U.T. 3: SISTEMAS OPERATIVOS PROPIETARIOS. WINDOWS.

Objetivos:

- Conocer que es un sistema de archivos y sus características principales.
- Conocer los requisitos y consideraciones para la instalación de un SO.
- Conocer la instalación de un SO Windows.
- Conocer lo que son las cuentas de usuario en un SO.
- Conocer los permisos locales en un SO Windows.
- Utilizar el administrador de equipos.
- Configurar el sistema.
- Conocer que son las directivas de seguridad local.

3 .1 EL SISTEMA DE ARCHIVOS.

En un sistema informático existe la necesidad por parte de los usuarios de almacenar datos en algún medio, a veces por periodos largos y a veces por instantes.

Cada aplicación y cada usuario debe tener ciertos derechos con sus datos, como son el poder crearlos y borrarlos, cambiarlos de lugar o mantener su privacidad.

El **sistema de archivos (FS) es el componente del SO** que se encarga de la **asignación de espacio** a los archivos, la **administración del espacio libre** y del **acceso a los datos en la memoria secundaria.**

Es el propio FS quien determina la estructura, nombre, forma de acceso, uso y propiedades de la información que se guardará en el disco, además de establecer el formato físico en el cual almacenará los datos.

Cada SO dispone de su propio **sistema de archivos**, pero el objetivo y función de todos ellos es el mismo, **permitir a los usuarios un manejo fácil y cómodo de sus archivos, abstrayéndose de las particularidades del HW en el que se guardan dichos archivos.**

Para administrar todo esto el FS utiliza dos tipos de objetos fundamentalmente: Los **archivos y** los **directorios.**

3.1.1 TIPOS DE SISTEMAS DE ARCHIVOS.

Los tipos de sistemas de archivos más conocidos para microordenadores son:

- **FAT32:** Se podía utilizar en SSOO como w95 osr2, w98, w2000, wXP, WVista, W2003S y W2008S. Admite particiones mayores de 2 GB, el tamaño máximo de un archivo es de 4 GB, un volumen puede tener hasta 2 TB.

- **NTFS 5:** Sus volúmenes pueden llegar casi a 16 TB y el tamaño máximo del archivo está limitado al tamaño del volumen. Es el sistema de ficheros usado por Windows hasta Windows 10.

- **ReFS:** Está diseñado por Microsoft para solucionar algunos problemas importantes de NTFS como una mayor resistencia a la corrupción de datos o para trabajar de manera más efectiva con sistemas de archivos muy grandes. Está pensado como la próxima generación de FS de Microsoft.

- **Ext3fs Sistema De Archivos Extendido 3:** Se usa en sistemas Linux. Permite nombres de archivo de hasta 256 caracteres. El tamaño máximo de un volumen es de 32 TB y el tamaño máximo de un archivo es de 2 TB. Dispone de un registro de diario (**Journal**).

- **Ext4fs Sistema De Archivos Extendido 4** Es uno de los más flexibles y eficientes. Se usa en sistemas Linux, es compatible con Ext3. Permite nombres de archivo de hasta 256 caracteres. El tamaño máximo de un volumen es de 1 EB (aproximadamente 1000000 TB) y el tamaño máximo de un archivo es de 16 TB. Dispone de un registro de diario (**Journal**)

3.1.2 ARCHIVOS O FICHEROS.

Los **ficheros o archivos** son un mecanismo de abstracción que permite almacenar información en un dispositivo y usarla posteriormente.

Los ficheros permiten que el usuario no tenga que preocuparse por la forma o el lugar físico de almacenamiento de los datos.

Un fichero es una colección de información que tiene un nombre.

Las reglas para nombrar archivos varían de un FS a otro. La estructura típica de un nombre de archivo en la mayoría de los FS suele ser: ***nombre.extensión***

Donde la extensión suele representar de alguna forma el tipo de archivo del que se trata.

Actualmente la mayoría de los FS pueden utilizar nombres de archivos de hasta 255 caracteres.

Junto con el nombre del fichero, el SO almacena información sobre algunos atributos que califican al archivo. Estos atributos varían también dependiendo del FS utilizado.

Generalmente se suelen encontrar los siguientes atributos de archivo.

- Atributo de sistema (S) system: Indica si un archivo pertenece al SO.
- Atributo de oculto (H) hidden: Indica si un fichero es visible o se oculta para protegerlo.
- Atributo de solo lectura (R). (read only): Indica si un fichero se puede modificar o solamente ser leído su contenido.
- Atributos sobre Fechas: Almacenan la fecha de creación, modificación o acceso.
- Atributos sobre Hora: Almacena la hora de creación, modificación o acceso.
- Tamaño: almacena el tamaño que ocupa el archivo en disco.

Existen, dependiendo del FS, otros atributos que pueden indicar la pertenencia del archivo a un determinado usuario o grupo de ellos. El tipo de archivo que es o los permisos que los distintos usuarios del sistema tienen sobre él.

3.1.3 LOS DIRECTORIOS.

Son un tipo de archivos especiales que **sirven para estructurar los ficheros almacenados** en un dispositivo de almacenamiento secundario, de forma que **se puedan guardar ficheros lógicamente relacionados en el mismo directorio.**

Los directorios **contienen archivos e información sobre los mismos**. Un directorio también **puede contener a su vez otros directorios** con lo que el sistema de archivos establece de esta manera una **estructura jerárquica** entre los diferentes archivos que contiene.

Los directorios sirven al sistema de archivos para llevar un control de los archivos.

Se puede visualizar un directorio como una tabla en la que cada archivo contenido en el directorio tiene una entrada. En esta entrada el SO guarda la información que necesita del archivo para su utilización.

Habitualmente la información sobre los archivos que contiene un directorio que se guarda en las entradas de directorio es:

- Nombre del archivo,
- Tipo de archivo,
- Tamaño del archivo,
- Propietario del archivo,
- Fecha de creación,
- Fecha de modificación,
- Localización del archivo en el almacenamiento secundario.

Existen, dependiendo del FS, otros atributos que pueden indicar la pertenencia de un directorio a un determinado usuario o grupo de ellos o los permisos que los distintos usuarios del sistema tienen sobre él.

La mayoría de los sistemas operativos proporcionan servicios para la creación y manipulación de directorios.

3.1.4 DIRECTORIOS ESPECIALES, RUTAS O TRAYECTORIAS.

En todo sistema de archivos existe un **directorio especial llamado raíz (root)**, que es el directorio que contiene a todos los demás.

Desde este directorio se puede identificar la situación lógica del fichero o directorio dentro del FS, esto es lo que se conoce como la ruta del fichero.

Existen en la mayoría de SSOO que usan un sistema jerárquico de archivos dos entradas especiales en los directorios para hacer referencia al directorio activo, que es el directorio en el que se está trabajando, nombrado por **"." y al directorio padre** del **directorio activo nombrado por "..".**

Un ruta o trayectoria es la expresión de la situación lógica en el sistema de archivos de un fichero o directorio.

Es decir, una **ruta o trayectoria** identifica la situación lógica de un fichero o directorio en el sistema de archivos.

Existen dos tipos habitualmente de rutas o trayectorias de ficheros:

Absoluta: Esta ruta parte del directorio raíz y llega a el directorio que queremos situar.

Ejemplo: C:\Windows\system32

Relativa: Esta ruta parte del directorio en el que el usuario está trabajando (directorio activo o actual) hasta el directorio que queremos situar.

Ejemplo: Si estamos en el directorio C:\Windows la ruta relativa de system32 sería: \system32

En Windows en las rutas los directorios están separados por el carácter \ mientras que en Linux se usa /.

3.1.5 LOS COMODINES.

En cualquier sistema de archivos existen formas de facilitar a los usuarios la manera de seleccionar ficheros al nombrarlos. Una de estas formas son los comodines. El tratamiento de estos depende del SO. Pero podemos generalizar el uso de dos tipos de comodines:

"*": Sustituye a todos los caracteres de un nombre por delante, por detrás o en medio del nombre.

Ejemplo: *.dat, d*tos.bat o datos.*

"?": Sustituye a un único carácter de un nombre por delante, por detrás o en medio del nombre.

Ejemplo: dato?.dat, d?tos.bat o datos.?

3 .2 UTILIZACIÓN DEL SISTEMA OPERATIVO.

Normalmente un SO se puede utilizar de dos formas distintas:

- En **modo comando o consola de comandos**: Es la interacción del usuario a través de una línea de comandos el usuario tiene que teclear la orden y pulsar intro para que el SO la ejecute. El uso de un modo comando está muy extendido entre los equipos servidores, los administradores suelen trabajar en modo comando. MS-DOS y las primeras versiones de Linux funcionaban únicamente en modo comando. Sin embargo, hoy en día la mayoría de los SSOO poseen un entorno gráfico.
- **Modo gráfico**: Se entiende por este modo a aquella interfaz que usa ventanas, iconos y ratón. En gran medida los desarrollos de entornos gráficos han contribuido al boom de la informática.

Para utilizar en Windows 10 el modo consola se puede usar el comando CMD para lanzar un terminal de línea de comandos.

3 .3 REQUISITOS PREVIOS A LA INSTALACIÓN.

Antes de empezar a instalar el SO hay una serie de cuestiones que hay que resolver:

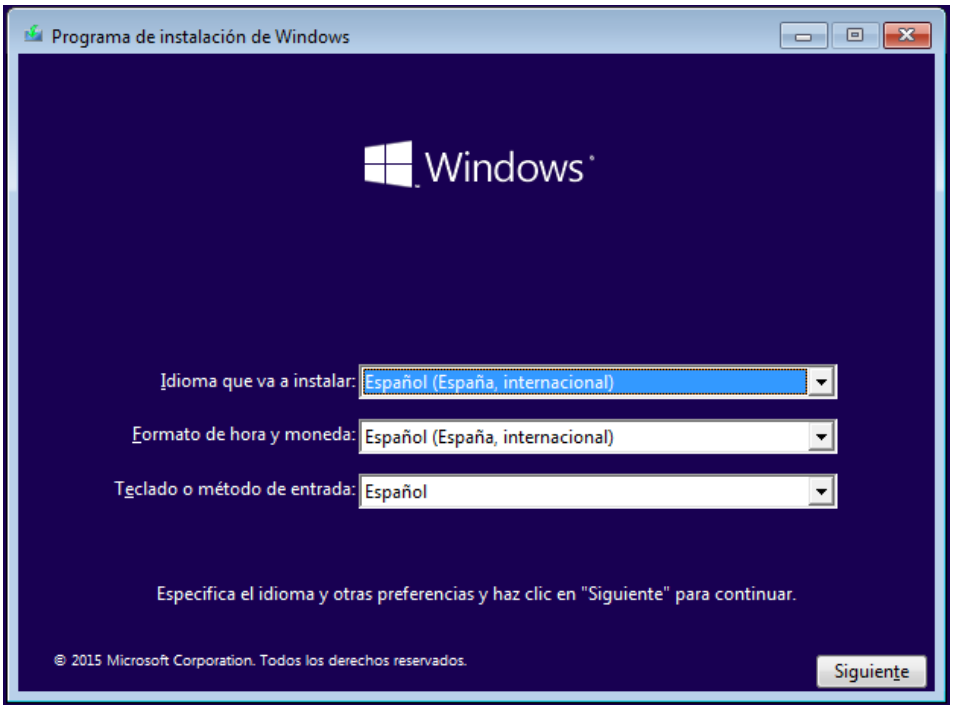
- Requisitos mínimos que necesita el SO que queremos instalar.
- Elegir el particionado del disco donde instalaremos el sistema.
- Qué sistema de archivos se va a utilizar.

Una vez resultas estas cuestiones se puede proceder a la instalación.

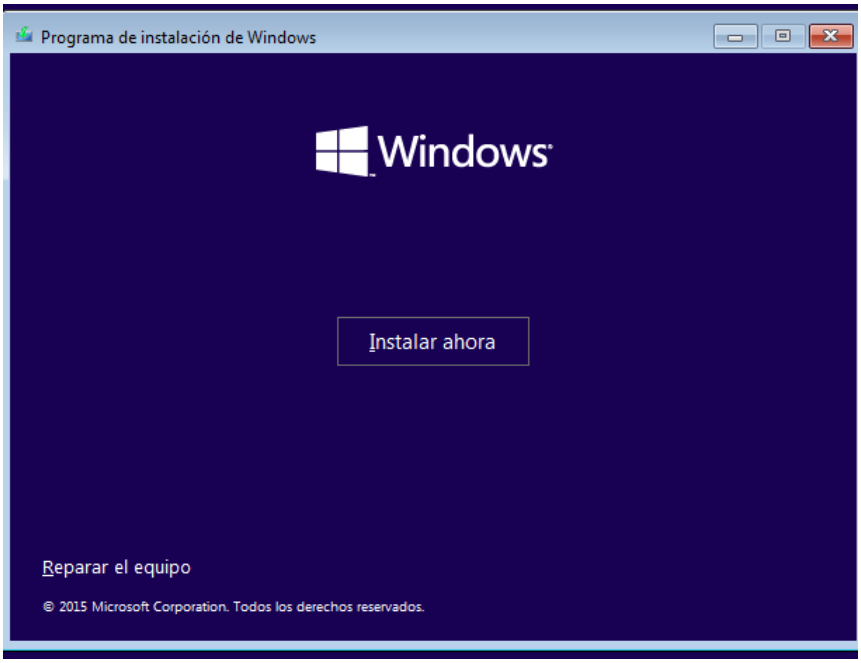
3.3.1 INSTALACIÓN WINDOWS 10.

Una vez el soporte de instalación está funcionando comienza el proceso de instalación.

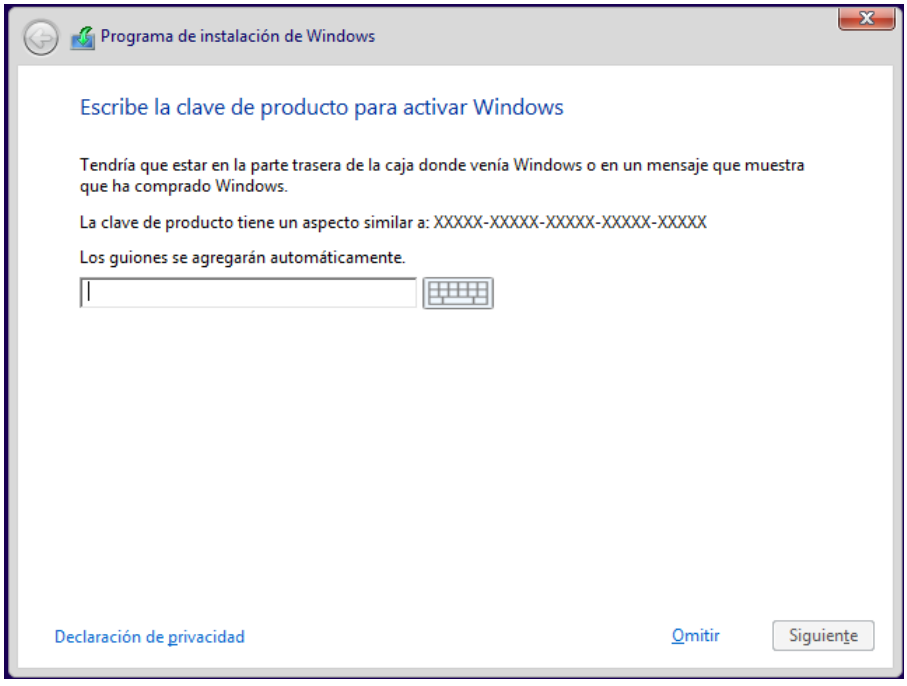
Elegimos el idioma de instalación, de teclado y el formato de fecha y hora y hacemos clic en *siguiente*



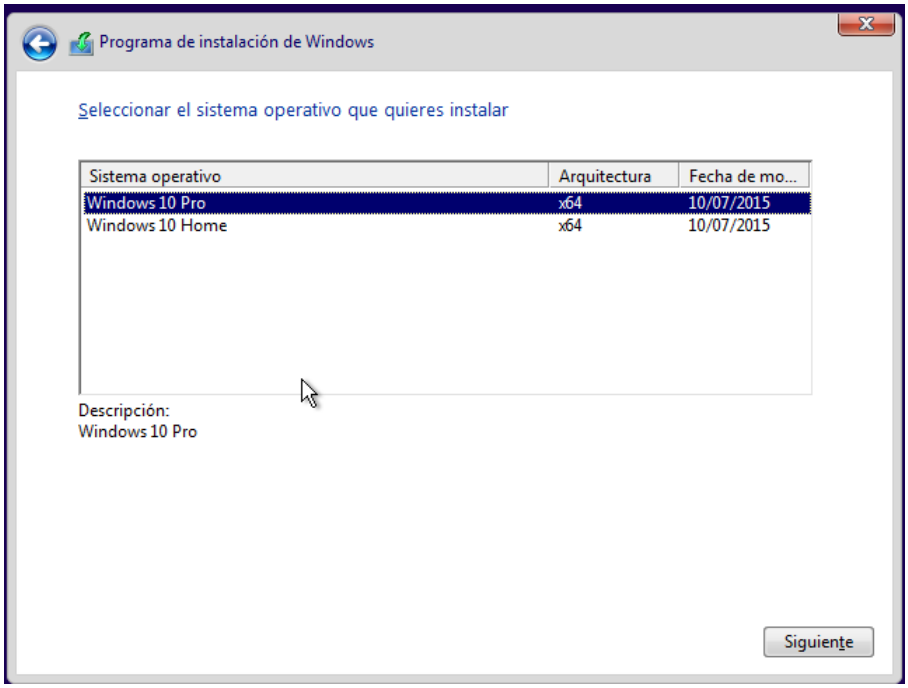
Elegimos instalar el sistema.



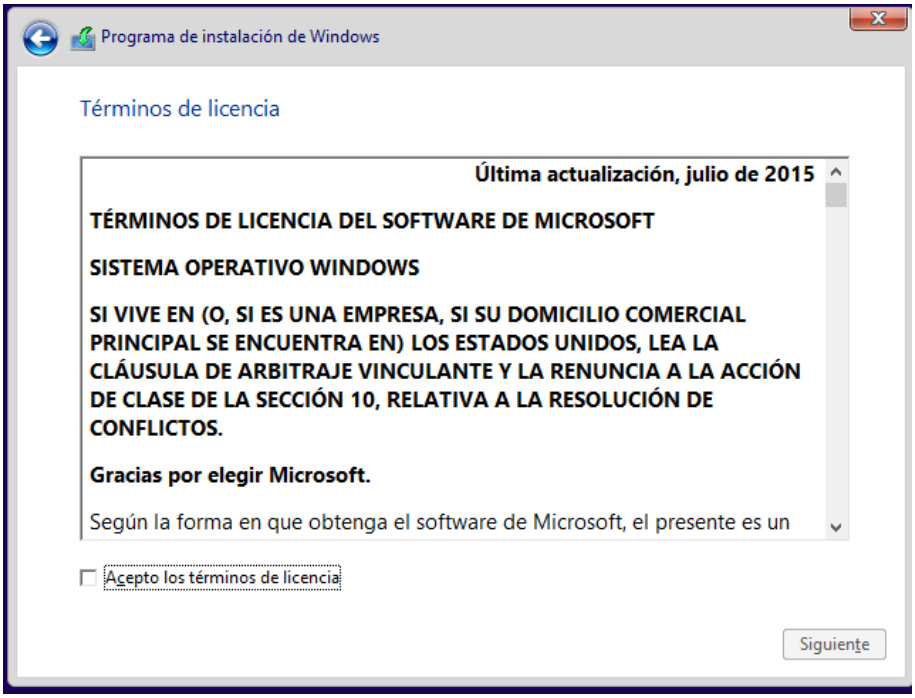
A continuación, nos pedirá la clave de producto para activar Windows. Se la proporcionamos y hacemos clic en siguiente.



Ahora nos da a elegir que edición del SO queremos instalar. Elegimos instalar Windows 10 Pro.

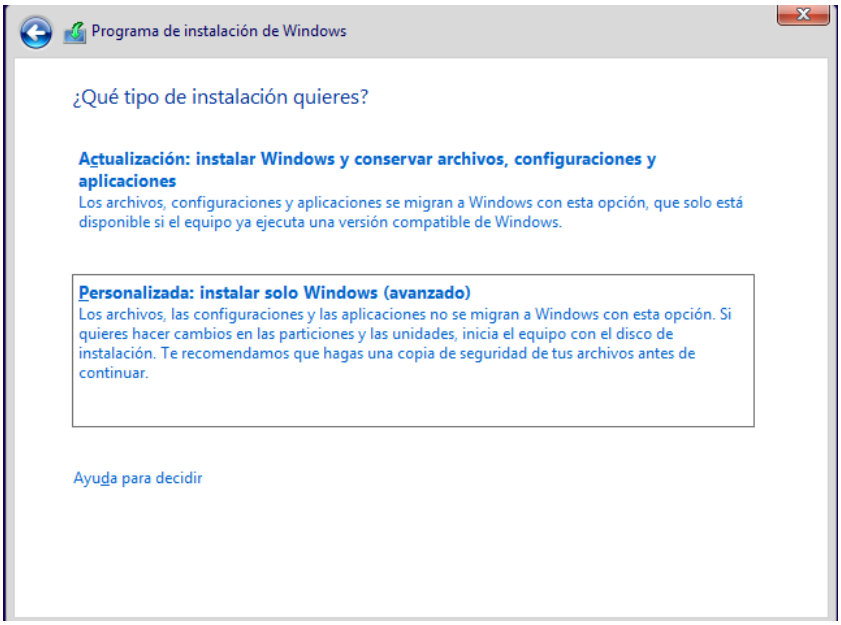


Leemos y aceptamos el contrato de licencia (CLUF)

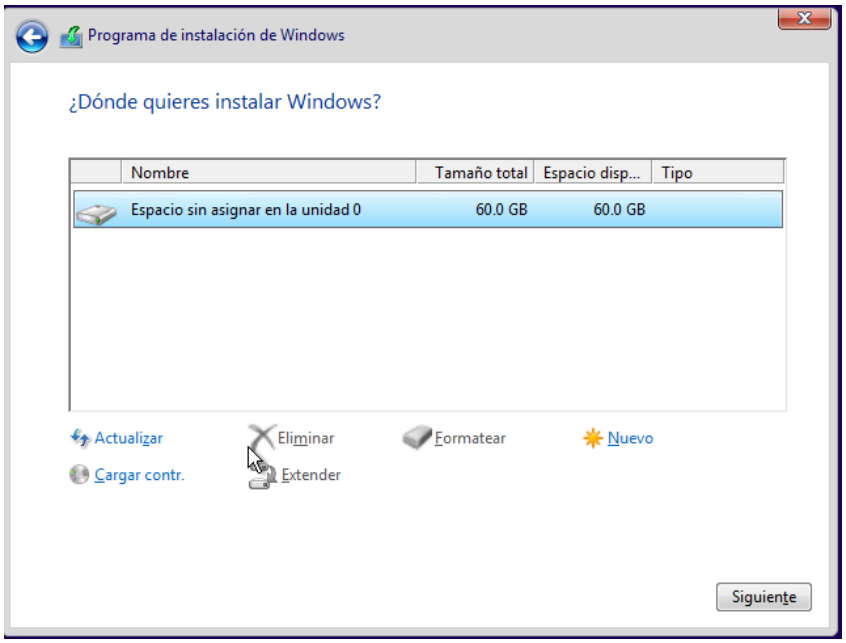


Elegimos si queremos una instalación limpia (personalizada) o queremos conservar los archivos y configuraciones que ya tiene el equipo con el anterior SO.

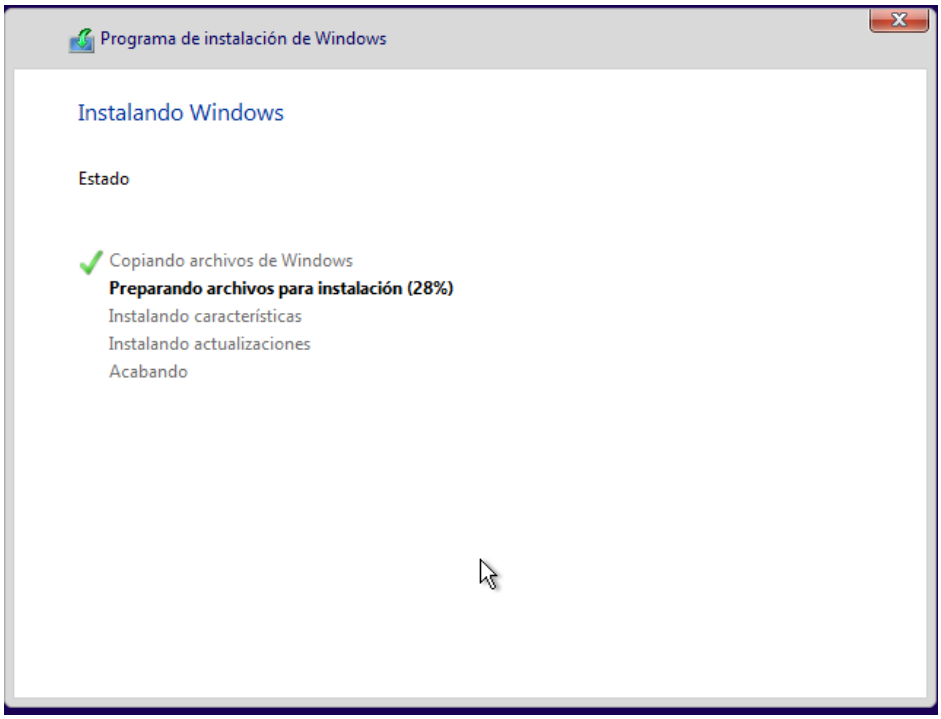
Elegimos una instalación personalizada, ya que no tenemos un SO en la maquina actualmente.



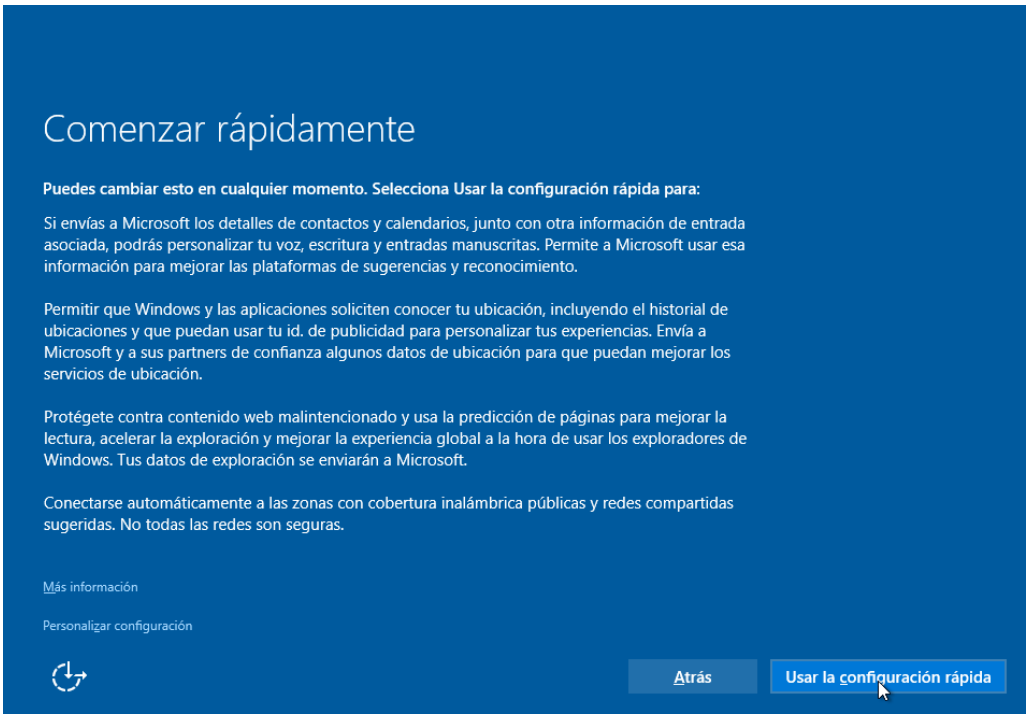
A continuación, nos muestra el espacio donde se puede instalar el SO. Elegimos instalar en el espacio sin asignar.



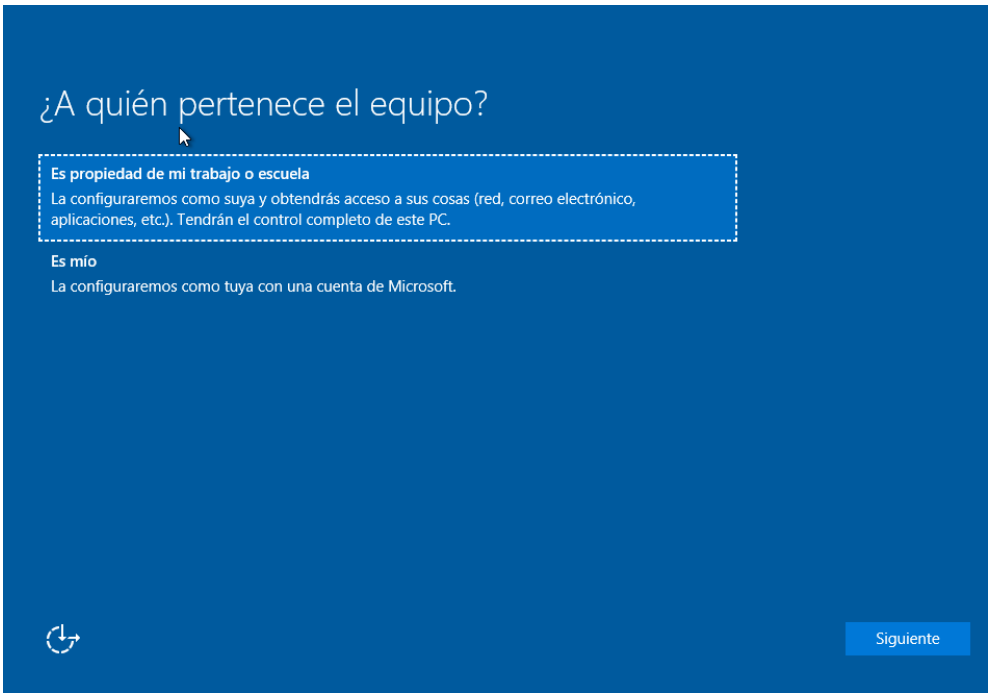
A partir de aquí el sistema tiene suficiente información para continuar de forma autónoma instalando el SO



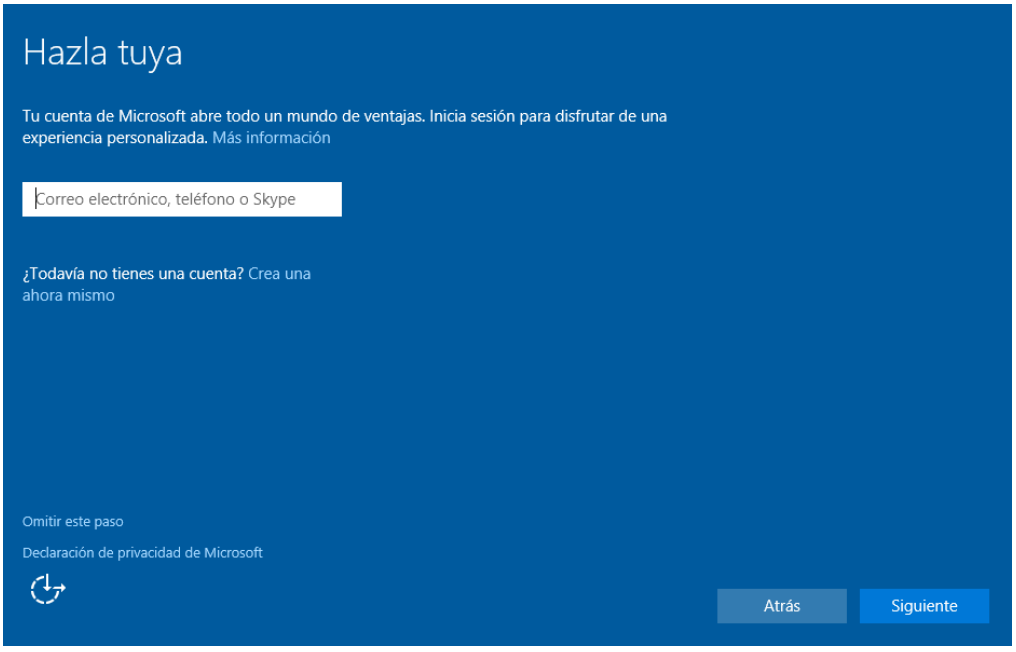
Una vez instalado faltan algunas configuraciones que nos pide ahora el sistema. Elegimos usar la configuración rápida.



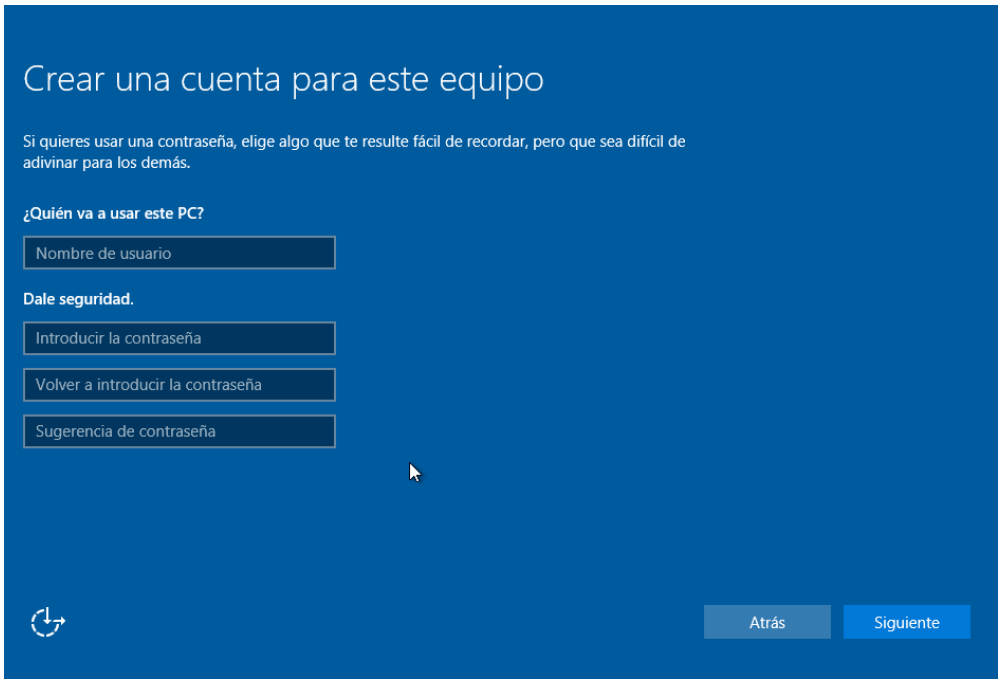
Ahora la máquina se reinicia y nos muestra la siguiente pantalla.



Elegimos usarlo como equipo personal y a continuación elegimos en la siguiente pantalla omitir este paso.

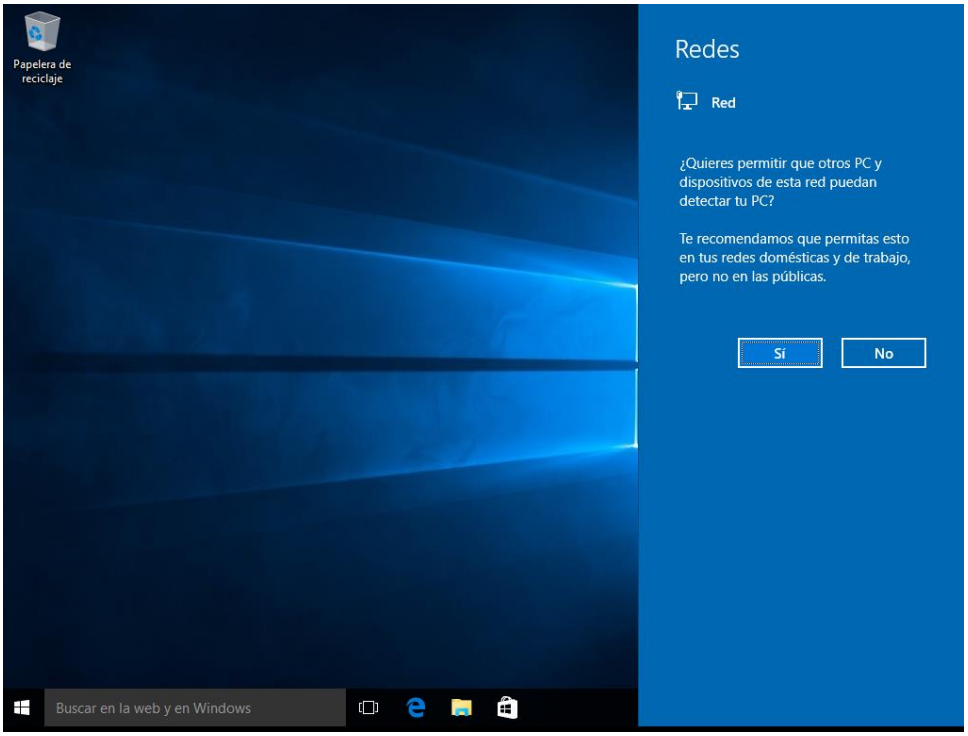


A continuación, nos pide un nombre de usuario para el equipo, su contraseña que tendremos que teclear dos veces y una sugerencia de seguridad por si se nos olvida la contraseña.



Y finalmente Windows se iniciará por primera vez mostrando el escritorio del usuario. tras la configuración final.

Seguidamente nos pregunta si queremos activar la detección de redes para que el equipo se pueda detectar por otros equipos y también pueda detectar a otros equipos de la red.



3 .4 LOS USUARIOS.

Una cuenta de usuario representa a una persona y se utiliza para iniciar sesiones en la red y para tener acceso a los recursos de esta.

Una cuenta de usuario contiene toda la información que define a ese usuario en particular dentro del entorno Windows. Todo lo que se necesita es asociarle un identificador de seguridad de usuario (SID).

La seguridad de las cuentas de usuario incluye un nombre único de usuario, una contraseña y los permisos que el usuario tiene para usar el sistema y acceder a sus recursos.

Las cuentas de usuario permiten que un usuario inicie sesión en equipos o dominios con una identidad que se puede autentificar y autorizar para tener acceso a los diferentes recursos que la red ofrece.

Cada usuario que se conecta a la red debe tener su propia cuenta de usuario y su propia contraseña.

La autenticación del usuario permite auditar las acciones de este en el sistema, reforzando así la seguridad del mismo.

Por tanto, una cuenta de usuario se utiliza para:

- Autentificar la identidad del usuario.
- Autorizar o denegar el acceso a los recursos de la red.
- Administrar la seguridad del sistema.
- Auditar las acciones realizadas con la cuenta de usuario.

Las cuentas de usuario pueden definirse en una máquina local o en un dominio.

Las cuentas definidas en un dominio pueden usarse en cualquier máquina que pertenezca a ese dominio o algún dominio de confianza.

Un usuario del dominio es una cuenta a la que se pueden conceder permisos y derechos para los equipos del dominio o de otros dominios de confianza.

Las cuentas definidas en una máquina local solo se pueden usar en esa máquina. Un usuario local es una cuenta a la que se pueden conceder permisos y derechos para el equipo en el que se crea.

Normalmente se proporcionan dos cuentas de usuario local predefinidas que se crean durante el proceso de instalación:

- **Administrador:** La cuenta de administrador posee control total sobre las operaciones y la seguridad del sistema completo. Cualquiera que puede iniciar sesión como administrador posee control total sobre la administración del sistema completo. Este es un punto importante debido a que los usuarios de las cuentas de administrador deben ser de total confianza. Esta cuenta puede ser renombrada o deshabilitada pero no puede ser borrada ni quitada del grupo local de Administradores.

Esta cuenta está pensada para el individuo o individuos que administran la configuración del sistema. Un mal uso de esta cuenta puede ser desastroso debido a los derechos y permisos asociados a la cuenta. Es recomendable usar esta cuenta solo para tareas administrativas.

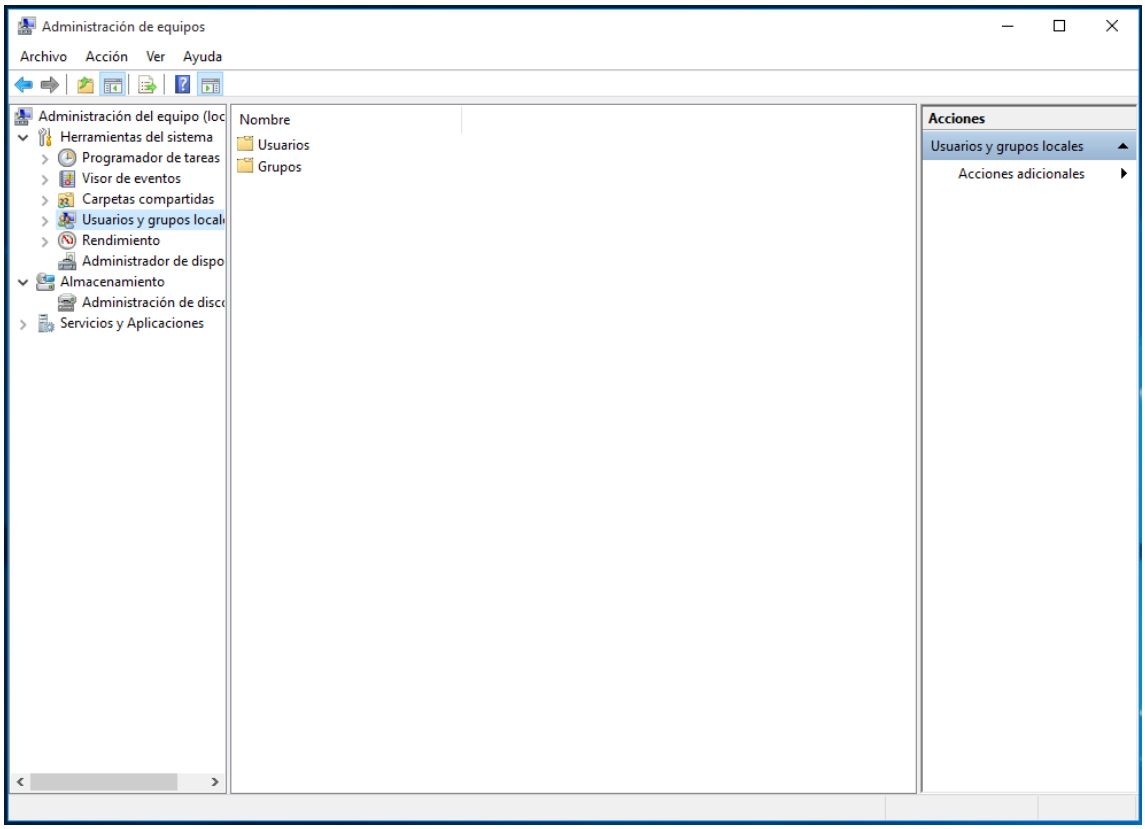
- **Invitado:** Está pensada para los usuarios que se conecten de forma ocasional al sistema. Sin embargo, no es recomendable usarla, sino que se deberían crear cuentas temporales que proporcionen unos controles de responsabilidad y auditorias adecuados.

Por defecto la cuenta de invitado está desactivada y configurada como miembro del grupo local invitados. Posee una contraseña vacía y no se puede cambiar su perfil por el perfil de un usuario determinado.

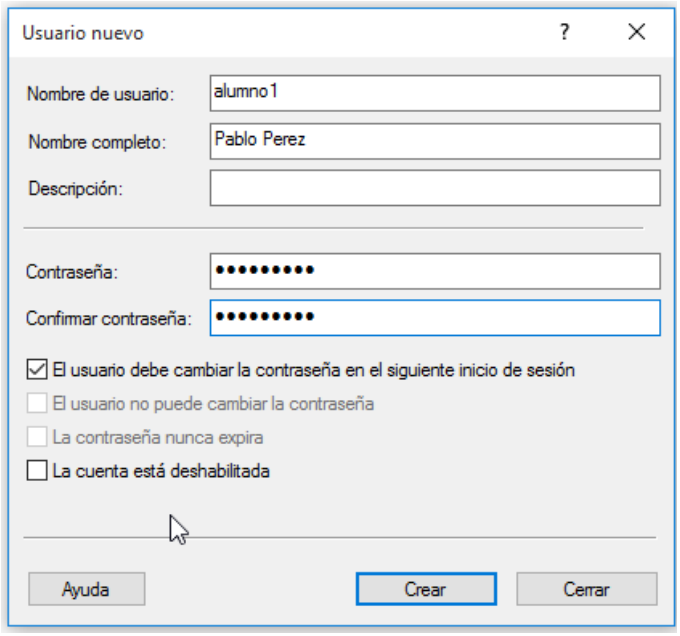
3.4.1 CREAR USUARIOS LOCALES

Para crear un usuario local en Windows 10 podemos hacerlo de distintas formas:

Desde administración de equipos: en la caja de búsqueda de Windows 10 buscamos Administración de equipos y se nos abrirá la siguiente ventana



Usando el botón derecho del ratón sobre usuarios nos aparecerá la opción *Usuario Nuevo* que nos mostrará el siguiente interfaz:



En la ventana que aparece habrá que indicar los datos de la nueva cuenta de usuario, siendo el único campo obligatorio el referente al nombre de usuario. El resto de los campos son: nombre completo, descripción, contraseña y confirmar contraseña.

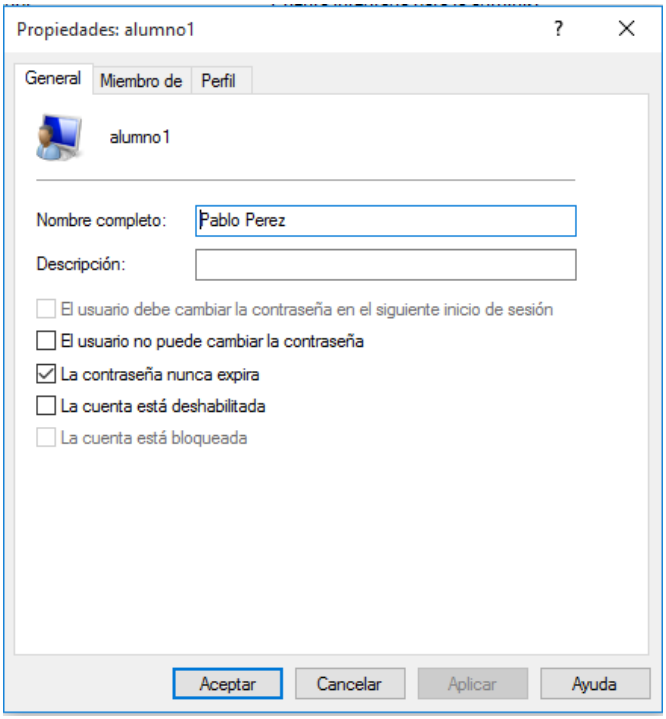
Además de estos campos existen algunas casillas de verificación en este cuadro de diálogo que tiene que ver con la configuración de la contraseña del usuario, referentes a si la contraseña puede o no caducar, si el usuario debe cambiarla al iniciar la siguiente sesión con esta cuenta o si la cuenta está deshabilitada.

3.4.1.1 PROPIEDADES DE UN USUARIO

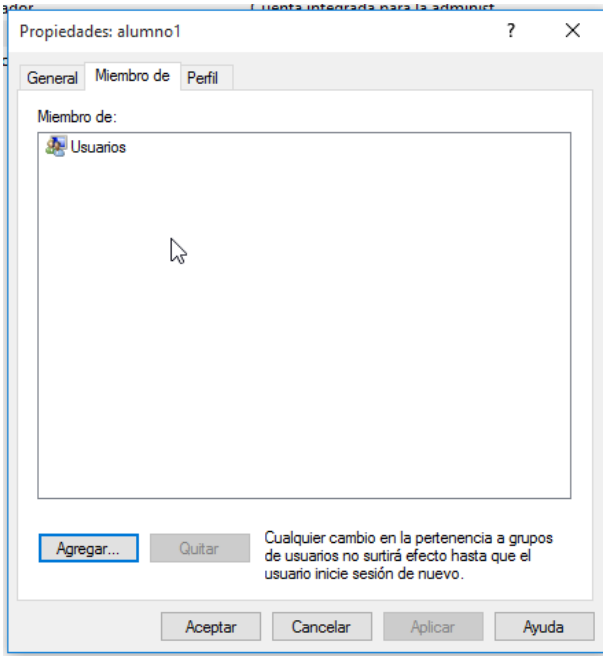
Si pulsamos dos veces sobre el usuario aparecerá la ventana de propiedades del usuario. El número de pestañas que esta ventana tenga dependerá de los servicios que tenga instalado el sistema.

Generalmente las pestañas más utilizadas son:

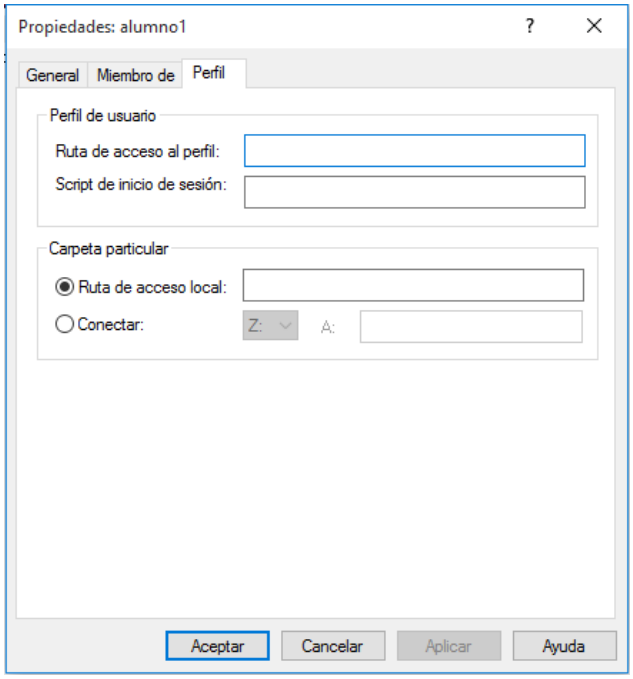
- **General:** Muestra la información suministrada a la hora de crear un usuario.



- **Miembro de:** Muestra el listado de grupos a los que pertenece el usuario. Para modificar los grupos a los que pertenecerá el usuario hay que utilizar los botones de *Agregar y quitar*.



- **Perfil:** Se puede establecer aquí el perfil y directorio particular de un usuario.



También se puede configurar la ruta de acceso al perfil, que no se usa para perfiles locales, sino para perfiles móviles y el script de inicio de sesión, en el que se puede configurar que cuando inicie sesión dicho usuario, se ejecute un script determinado.

Se puede también definir la carpeta particular de un usuario, donde puede almacenar sus archivos y programas. Este directorio es el predeterminado que se usará en el Símbolo del sistema y en todas las aplicaciones que no tienen definido un directorio de trabajo.

3.4.1.2 EL PERFIL DE USUARIO.

Un **perfil de usuario** es una de las herramientas más potentes de Windows para configurar el entorno de trabajo de los usuarios de la red. Se puede especificar el aspecto del escritorio, la barra de tareas, el contenido del menú Inicio, etc.

Cada usuario puede tener un perfil que esté asociado a su nombre de usuario y que se guarde en la estación de trabajo. Aquellos usuarios que acceden a distintas estaciones podrán tener un perfil en cada una de ellas, este perfil se llama **perfil local** porque solo se puede tener acceso a él desde la estación de trabajo en la que fue creado.

Además, existe un **perfil temporal** que se crea cuando se produce un error en la carga del perfil del usuario. Éste se elimina al final de la sesión y no se almacenan los cambios realizados por el usuario en la configuración del escritorio y los archivos.

Existe un tipo de perfil que permite guardar los datos de dicho perfil en un servidor de manera que se puede acceder al perfil independientemente del equipo en el que se inicie sesión. Este tipo de perfil se llama **perfil de red**.

Por cuestiones organizativas, los diferentes archivos que forman el perfil de cada usuario se organizan en carpetas.

Por ejemplo:

- Datos de programa: Contiene datos particulares de algunos programas, como pinceles de Gimp o diccionarios de LibreOffice Writer.
- Cookies: Guarda Información sobre el usuario y sus preferencias.
- Escritorio: Contiene todos los elementos que pueden verse en el escritorio del usuario.
- Favoritos: Almacena los marcadores creados por el usuario de sus sitios de Internet preferidos.
- Mis documentos: Contiene documentos del usuario.
- Documentos recientes: Contiene enlaces a los documentos y carpetas utilizados recientemente.
- Entorno de red: Almacena accesos directos a los elementos de Mis sitios de red.
- Impresoras: Contiene accesos directos a los elementos de la carpeta Impresoras.
- Menú Inicio: Guarda los accesos directos a los programas que mostrará el menú del sistema.

3.4.1.3 LOS GRUPOS.

Para facilitar la administración de los diferentes usuarios Windows nos ofrece el concepto de grupo. De manera que agrupando a los usuarios podemos asignarles privilegios y derechos más fácilmente. Se puede incorporar a un usuario a varios grupos, teniendo en cada uno de ellos unos permisos o derechos determinados que le permitirán realizar distintas funciones.

3.4.1.3.1 LAS IDENTIDADES ESPECIALES.

Cuando se instala el SO, se crean una serie de usuarios, grupos e identidades especiales a las que se puede asignar permisos y derechos.

Entre estas identidades especiales se encuentran:

- **Inicio de sesión anónimo (Anonymous logon): C**orresponde a un usuario que se ha registrado de forma anónima, es decir sin proporcionar ni usuario ni contraseña alguna. Por ejemplo, un usuario de FTP anónimo.
- **Grupo Creador (Creator Group):** Corresponde al grupo que creó el objeto o que tiene su propiedad.
- **Propietario Creador (Creator Owner).** Corresponde al usuario que creo el objeto o que tiene su propiedad.
- **Interactivo (Interactive):** Corresponde a usuarios que acceden de forma local o a través de una sesión de escritorio remoto.
- **Lotes (Batch):** corresponde a los usuarios que han iniciado sesión en un recurso de cola de procesos por lotes (por ejemplo, trabajos del programador de tareas).
- **Todos:** Corresponde a todos los usuarios estén o no autentificados.
- **Usuarios Autentificados (Authenticated Users):** Corresponde a todos los usuarios y equipos que han sido autentificados por el sistema.

3.4.1.3.2 LOS GRUPOS LOCALES.

Un grupo local es una cuenta a la que se pueden conceder permisos y derechos para el equipo donde se está creando y a la que pueden agregar usuarios locales, así como usuarios, grupos.

Para agregar miembros a los grupos hay que seguir los siguientes pasos:

- Seleccionar ***Administrar*** del menú contextual de ***Equipo*** y en ***Usuarios Y Grupos Locales***.
- Pulsar con el botón izquierdo del ratón sobre *Grupos* y en el panel derecho se mostrarán los grupos disponibles.
- Selecciona propiedades del grupo y sitúate en la pestaña *Miembros.* Aquí podemos agregar los usuarios que necesitemos.

3 .5 LOS PERMISOS Y LOS DERECHOS.

El modelo de protección de Windows establece la forma en que el sistema lleva a cabo el control de acceso de cada usuario o grupo de usuarios. Windows define dos conceptos distintos y complementarios: el concepto de derecho y el concepto de permiso, respectivamente.

Un **derecho**, es un atributo de un usuario (o grupo) que le permite realizar una acción que afecta al sistema en su conjunto (y no a un objeto o recurso en concreto). Existe un conjunto fijo y predefinido de derechos en Windows. Para determinar qué usuarios poseen qué derechos, cada derecho posee una lista donde se especifican los grupos o usuarios que tienen concedido ese derecho.

Un **permiso**, es una característica de cada recurso (carpeta, archivo, impresora, etc.) del sistema, que concede o deniega el acceso al mismo a un usuario o grupo concreto. Cada recurso del sistema posee una lista en la que se establece qué usuarios o grupos pueden acceder a dicho recurso y qué tipo de acceso puede hacer cada uno (lectura, modificación, ejecución, borrado, etc.)

Es importante destacar que cuando existe un conflicto entre lo que concede o deniega un permiso y lo que concede o deniega un derecho, este último tiene prioridad.

Por ejemplo, el administrador tiene el derecho de tomar posesión de cualquier archivo, incluso de aquellos archivos sobre los que no tenga ningún permiso.

3.5.1 LOS PERMISOS NTFS ESTÁNDAR Y ESPECIALES.

Windows distingue entre:

- Los **permisos NTFS especiales**, que son los que controlan cada una de las acciones que se pueden realizar sobre las carpetas o los archivos.

- Los **permisos NTFS estándar**, que son combinaciones de los permisos NTFS especiales que están predefinidas en el sistema. Los permisos NTFS estándar facilitan la labor del administrador y de cada usuario cuando administra los permisos de sus archivos.

Cuando la asignación de permisos no se ajusta al comportamiento de ninguno de los permisos NTFS estándar, se deberá recurrir a los permisos NTFS especiales.

Las principales reglas que controlan la aplicación de los permisos a las carpetas y archivos son las siguientes:

Una única acción de un proceso puede involucrar varias acciones individuales sobre varios archivos o carpetas. En este caso, el sistema verificará si el proceso tiene o no, permisos para todas ellas. Si le falta algún permiso, la acción se rechazará con un mensaje de error genérico.

Los **permisos en Windows son acumulativos**: un proceso de usuario posee implícitamente todos los permisos correspondientes a los SID de su acreditación, es decir, poseerá todos los permisos del usuario y de los grupos a los que pertenezca.

La ausencia de un determinado permiso sobre un objeto supone implícitamente la imposibilidad de realizar la acción correspondiente sobre el objeto.

Si se produce un conflicto en la comprobación de los permisos, los permisos negativos tendrán una prioridad sobre los positivos y los permisos explícitos sobre los heredados.

3.5.2 LOS PERMISOS NTFS.

Cuando se establecen los permisos NTFS sobre un directorio, se define el acceso de un usuario o de un grupo a dicho directorio y sus archivos. Estos permisos sólo pueden establecerlos y cambiarlos, el propietario o aquel usuario que haya recibido el permiso del propietario.

Una vez establecidos los permisos, afectarán a los archivos y subdirectorios que dependan de él, tanto los que se creen posteriormente como los que ya existían previamente; este hecho se denomina **herencia**. Si no se desea que se hereden, deberá indicarse expresamente cuando se establezcan los permisos.

Hay tres modos de realizar cambios en los permisos heredados:

- Realizar los cambios en la carpeta principal y entonces la carpeta secundaria heredará estos permisos.
- Seleccionar el permiso contrario (Permitir o Denegar) para sustituir al permiso heredado.
- Deshabilitando la herencia desde el interfaz en opciones avanzadas de la pestaña de seguridad del objeto. De esta manera, podrás realizar cambios en los permisos, ya que la carpeta no heredará los permisos de la carpeta principal.

Los permisos NTFS estándar para directorios y archivos que se pueden conceder o denegar son:

- **Control total**. Es el máximo nivel y comprende poder realizar todas las acciones, tanto a nivel de archivos como de directorios.
- **Modificar**. Comprende todos los permisos, menos eliminar archivos y subdirectorios, cambiar permisos y tomar posesión.
- **Lectura y ejecución**. Comprende la visualización de los nombres de los archivos y subdirectorios, de los datos de los archivos, de los atributos y permisos y la ejecución de programas.
- **Mostrar el contenido de la carpeta**. Comprende los mismos permisos que lectura y ejecución, pero aplicables sólo a las carpetas.
- **Lectura.** Comprende ver los nombres de los archivos y directorios, ver los datos de los archivos, así como ver los atributos y permisos.
- **Escritura**. Comprende crear archivos y subdirectorios, añadir datos a los archivos, modificar los atributos y leer los permisos.
- **Permisos especiales**. Se activa cuando se indican permisos más concretos (se indicará cómo hacerlo, posteriormente).

Estos permisos son acumulables, pero denegar el permiso Control total, elimina todos los demás.

3.5.3 LA ASOCIACIÓN DE LOS PERMISOS A LOS RECURSOS.

La asociación de los permisos a los archivos y carpetas sigue una serie de reglas:

Cuando se crea un nuevo archivo o carpeta, éste posee por defecto los permisos heredados de la carpeta o unidad donde se ubica y ningún permiso explícito.

Cualquier usuario que posea control total sobre el archivo o carpeta (por defecto, su propietario) podrá incluir nuevos permisos (positivos o negativos) en la lista de permisos explícita.

El control sobre la herencia de permisos (por ejemplo, qué objetos heredan y qué permisos se heredan) se realiza a dos niveles:

En cada objeto (archivo o carpeta), se puede decidir si se desea o no, heredar los permisos de su carpeta padre.

Cuando se define un permiso explícito en una carpeta, se puede también decidir qué objetos van a heredarlo. En este caso, se puede decidir entre cualquier combinación de la propia carpeta, las subcarpetas y los archivos.

Copiar un archivo o carpeta a otra ubicación se considera una creación, y, por tanto, el archivo copiado recibirá una lista de permisos explícitos vacía y se activará la herencia de la carpeta padre correspondiente a la nueva ubicación.

En el proceso de mover un archivo se distinguen dos casos:

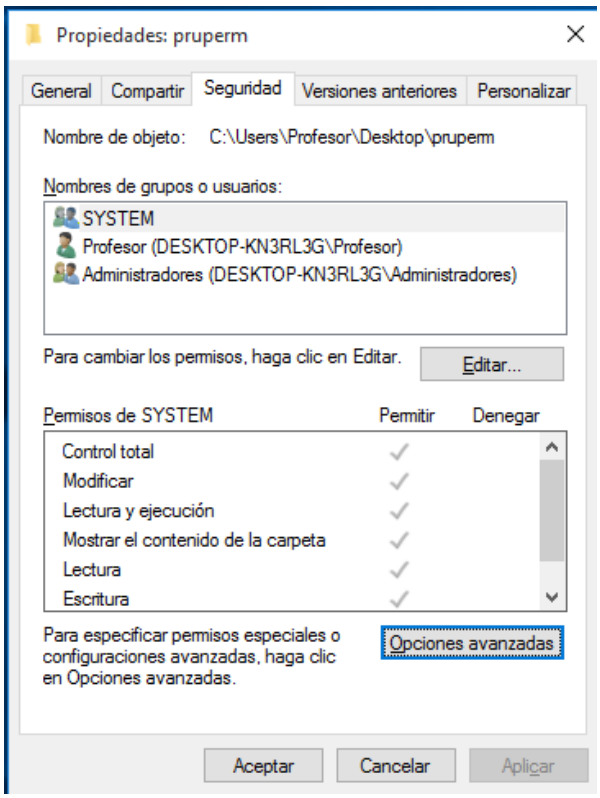
Si se mueve una carpeta o archivo a otra ubicación dentro del mismo volumen (o partición) NTFS, se desactivará la herencia y se mantendrán los permisos que tuviera como explícitos en la nueva ubicación. Además, se activará la herencia de la nueva ubicación del archivo o carpeta.

Si el volumen destino es distinto, entonces se actuará como en una copia, por tanto, sólo se tendrán los permisos heredados de la carpeta padre correspondiente a la nueva ubicación.

3.5.4 CÓMO ESTABLECER LOS PERMISOS NTFS ESTÁNDAR.

Para establecer los permisos NTFS estándar para un directorio o un archivo, sigue los pasos siguientes:

- Desde **Equipo** se selecciona el directorio o archivo que se desea. En el menú contextual, selecciona **Propiedades**, después **Seguridad** y verás la siguiente pantalla:



- En ella se encuentran los nombres de los usuarios, grupos e identidades especiales que tienen permisos sobre dicha carpeta y, debajo, los permisos estándar de directorio que posee cada uno de ellos.

- Si quieres consultar los permisos de alguno de ellos, sitúate sobre él y verás que, en la parte inferior, se muestran los permisos que tiene establecidos. Si hay marcas grises, corresponden a permisos heredados.

- Si deseas modificar los permisos de alguno de ellos, pulsa en **Editar**, sitúate sobre él y verás que, en la parte inferior, se muestran los permisos que tiene establecidos. Si hay casillas grises, corresponden a permisos heredados. Activa la casilla correspondiente al permiso deseado en la columna **Permitir**, se concede el permiso, o **Denegar**, se deniega el permiso.

- Si quieres añadir otros usuarios o grupos a la lista de nombres, pulsa en **Agregar**, en **Avanzadas** y en **Buscar ahora**. Se abrirá una ventana con todos los posibles usuarios, grupos e identidades especiales a los que puedes otorgar o denegar permisos.

- **Si seleccionas elementos de la lista y pulsas en Aceptar** dos veces, se añadirán a los grupos o usuarios que tienen permisos sobre la carpeta. Una vez que estén en la lista, indica los permisos que deseas conceder o denegar a cada uno de los usuarios que has añadido.

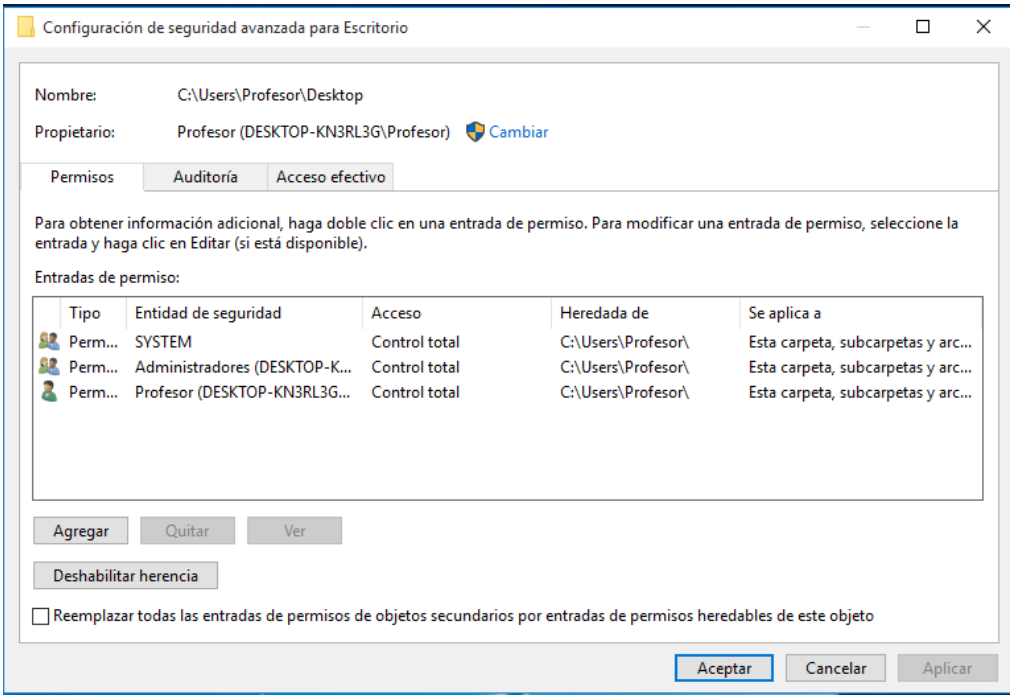
- Si quieres quitar algún usuario o grupo, sitúate sobre él, pulsa en **Quitar** (no se pedirá ninguna confirmación) y verás cómo se elimina de la lista.

3.5.5 CÓMO ESTABLECER LOS PERMISOS NTFS ESPECIALES.

Para establecer los **permisos NTFS especiales** de archivo o directorio, sigue los pasos siguientes:

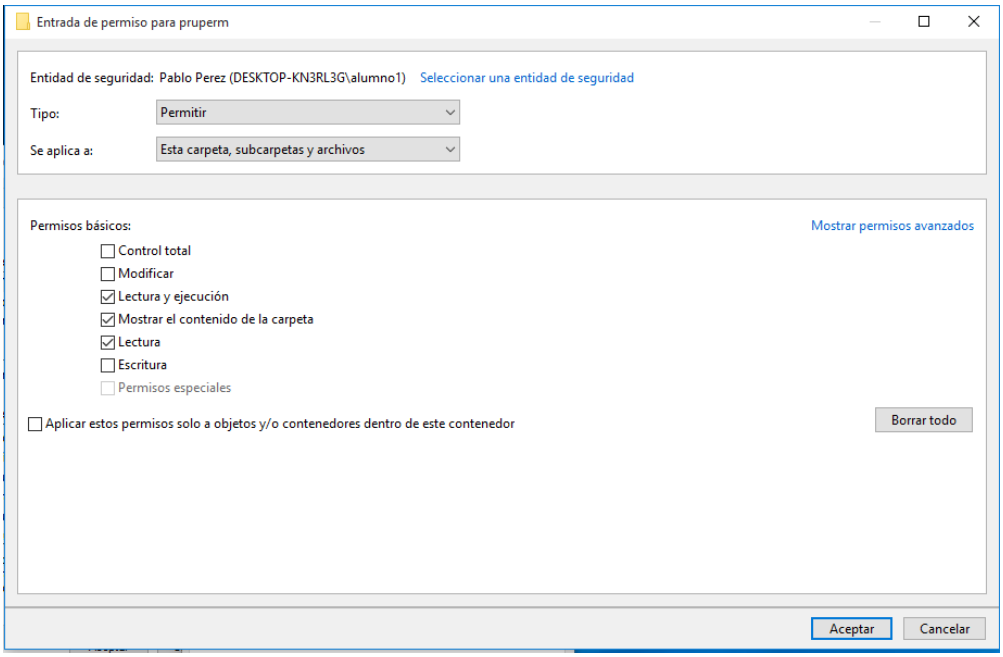
- Selecciona el directorio o archivo que desees, muestra su menú contextual, selecciona **Propiedades**, después **Seguridad** y verás la pantalla de **Propiedades** del directorio.

- Pulsa en **Opciones avanzadas** y verás una pantalla en donde se encuentran los nombres de los usuarios, grupos o identidades especiales, que tienen permisos sobre dicho directorio o archivo, junto con una descripción de los permisos y dónde se aplican.



- Para poder modificar los permisos establecidos, selecciona un usuario y si los permisos de dicho usuario no son heredados se habilitará el botón **editar.**

Muestra los permisos NTFS que tiene establecidos el usuario o grupo seleccionado. Si hay casillas grises, corresponden a permisos heredados. Se puede seleccionar ver los permisos

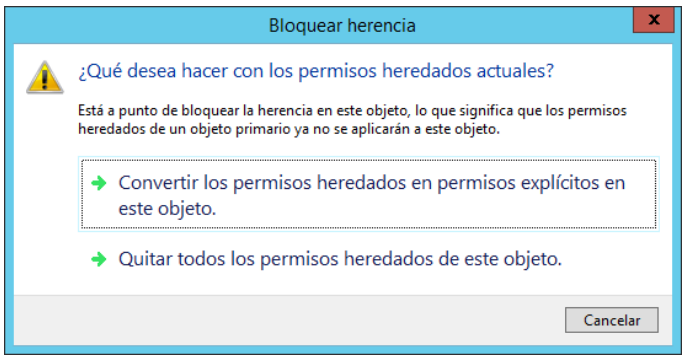


Puedes modificar los permisos que quieras activando en el desplegable la casilla correspondiente a Permitir, si quieres conceder el permiso, o Denegar, se quieres denegarlo.

Indica, en el desplegable asociado a ***Se aplica a***, el ámbito de los permisos que estás indicando. Si marcas el check **Aplicar estos permisos sólo a objetos y/o contenedores dentro de este contenedor**, evitarás que los archivos y subcarpetas hereden estos permisos.

- Si deseas quitar algún usuario o grupo, sitúate sobre él, pulsa en **Quitar** (no pedirá confirmación) y verás como se elimina de la lista.

- Si quieres que los permisos de la carpeta principal no se hereden a esta carpeta secundaria, haz clic en el botón **deshabilitar herencia** y se mostrará la siguiente pantalla:



- **Convertir los permisos heredados en permisos explícitos** de manera que concederás al objeto los permisos que tenía el objeto principal y podrán ser modificados.

- **Quitar todos los permisos heredados de este objeto** de esta forma el objeto no heredará los permisos del objeto principal y se quedará sin permisos (ni explícitos, ni heredados) y podrán añadirse nuevos permisos.

Si lo que quieres es que los permisos indicados en esta carpeta se hereden a todos los subdirectorios secundarios, deberás activas la casilla **Reemplazar todas las entradas de permisos de objetos secundarios por entradas de permisos heredables de este objeto**, de esta manera se eliminarán los permisos explícitos indicados en los subdirectorios y archivos que cuelgan de este directorio y se propagará de nuevo la herencia.

3 .6 ADMINISTRADOR DE EQUIPOS.

Para realizar distintas tareas de administración se dispone de la utilidad Administración de equipos que se encuentra en Administrar del menú contextual de Mi PC o de Equipo, con la que se pueden realizar, entre otras, las siguientes operaciones:

- Monitorizar sucesos del sistema como la hora de inicio de sesión y los errores de programas usando el **Visor de eventos**.
- Administrar usuarios y grupos del equipo con **Usuarios locales y grupos** o **Usuarios y grupos locales**.
- Ver la configuración de los dispositivos y agregar controladores de dispositivos nuevos desde **Administrador de dispositivos**.
- Iniciar y detener los servicios del sistema (**Servicios y aplicaciones**).

3.6.1 EL VISOR DE EVENTOS.

El **Visor de eventos** permite examinar y administrar los eventos ocurridos en el equipo.

Un **evento** o **suceso** es un acontecimiento significativo del sistema o de una aplicación que requiere una notificación al usuario.

Los registros de eventos que se muestran son:

- **Vistas personalizadas**. Una vez creado un filtro que muestre solo los registros que interesen, puede guardarlo con un nombre para utilizarlo después. Ese filtro guardado es una vista personalizada.
- **Registros de Windows**.
  - **Aplicación**: muestra los eventos generados por las aplicaciones o los programas.
  - **Seguridad**: muestra los eventos que se producen al hacer un seguimiento de los cambios en el sistema de seguridad o al detectar cualquier fallo.
  - **Instalación**: muestra los eventos relacionados con la instalación del sistema operativo o sus componentes.
  - **Sistema**: muestra los eventos que se producen en los distintos componentes de Windows.
  - **Eventos reenviados**: este registro se utiliza para almacenar los eventos recopilados de equipos remotos (para ello, se deberá crear previamente una suscripción de evento).
- **Registros de aplicaciones y servicios**: permiten almacenar eventos de una única aplicación o componente en lugar de eventos que pueden tener un impacto en todo el sistema.

- **Suscripciones**: el visor de eventos permite ver eventos en un único equipo remoto. Sin embargo, la solución de un problema puede requerir el examen de un conjunto de eventos almacenados en varios registros de diferentes equipos.

El visor de eventos puede mostrar los siguientes tipos de sucesos:

- **Crítico**: corresponde a un error del que no puede recuperarse automáticamente la aplicación o el componente que desencadenó el evento.

- **Error**: corresponde a un problema importante que puede afectar a la funcionalidad externa a la aplicación o al componente que desencadenó el evento.

- **Advertencia**: corresponde a un evento que no es importante necesariamente pero que indica la posibilidad de problemas en el futuro.

- **Información**: corresponde a un evento que describe el funcionamiento correcto de una aplicación, un controlador o un servicio.

- **Auditoria correcta**: indica que se ha realizado correctamente el ejercicio de los derechos de un usuario.

- **Error de auditoria**: indica que se ha producido un error en el ejercicio de los derechos de un usuario.

3.6.2 ADMINISTRAR LOS SERVICIOS DE UN EQUIPO.

Para administrar los servicios de un equipo, desde **Administración de equipos** y verás la pantalla principal de la utilidad.

Pulsa en el signo que hay a la izquierda de **Servicios y Aplicaciones** y se desplegarán sus nodos.

Pulsa el botón izquierdo del ratón sobre **Servicios** y en el panel derecho se mostrarán los servicios disponibles en el equipo.

Sitúate sobre el que desee, pulse el botón derecho del ratón para que muestre su menú contextual, seleccione **Propiedades.**

Se encuentra en la pestaña **General** y en ella se muestran los siguientes apartados:

- **Nombre de servicio**: nombre LDAP del servicio.

- **Nombre para mostrar**: nombre que aparecerá en la columna **Nombre** del panel de detalles.

- **Descripción**: breve comentario sobre el servicio.

- **Ruta de acceso al ejecutable**: nombre del archivo ejecutable correspondiente.

- **Tipo de inicio**: tipo de inicio del servicio seleccionado. Si pulsas en el triángulo que hay a la derecha del apartado, podrás seleccionar entre:
  - Automático:
  - Manual:
  - Deshabilitado:
- **Estado del servicio**: estado en que se encuentra en ese momento el servicio.
- **Iniciar**: al pulsar el botón, se iniciará el servicio.
- **Detener**: al pulsar el botón, se detendrá el servicio.
- **Pausa**: al pulsar el botón, se hará una pausa temporal en el servicio.
- **Reanudar**: al pulsar el botón, se volverá a reiniciar el servicio.
- **Parámetros de inicio**: se pueden indicar aquí los parámetros para el inicio del servicio.

En la pestaña **Iniciar sesión**, verás una pantalla en la que se encuentran entre otros los apartados siguientes:

- **Cuenta del sistema local**: al activar esta casilla, se indica que el servicio se inicie con la cuenta del sistema en lugar de con una cuenta de usuario.
- **Esta cuenta**: al activarla, se indica que el servicio se inicie con la cuenta de un usuario o una identidad especial

En la pestaña **Recuperación**, verás una pantalla en la que se encuentran entre otros los apartados siguientes:

- **Primer error:** se muestra la acción que se realizará durante el primer intento de recuperación al fallar el servicio
- **Segundo error;** se muestra la acción que se realizará durante el segundo intento de recuperación al fallar el servicio
- **Siguientes errores:** se muestra la acción que se realizará durante los siguientes intentos de recuperación al fallar el servicio
- **Programa:** se puede indicar la ubicación y el nombre del archivo que se ejecutará si falla el servicio.

En la pestaña **Dependencias**, verás una pantalla en la que se encuentran las dependencias del servicio seleccionado en las siguientes ventanas:

- En la superior, se muestran los servicios de los que depende el servicio seleccionado.
- En la inferior, se muestran los servicios que dependen del servicio seleccionado.

3.6.3 EL ADMINISTRADOR DE DISPOSITIVOS.

Windows dispone de una utilidad que permite ver la configuración de los dispositivos instalados en el equipo y añadir actualizar sus controladores.

Para ello, pulsa en **Sistema** del **Panel de control** del menú **Inicio**. Pulsa en la ficha **Hardware y sonido** y después, en el menú de **Dispositivos e impresoras** en **Administrador de dispositivos**. Verás una pantalla en donde se encuentran todos los dispositivos del sistema.

Si pulsas sobre el signo que hay a la izquierda de cualquier grupo de dispositivos, mostrará sus nodos. Si te sitúas sobre uno de los dispositivos, y en su menú contextual seleccionas **Propiedades**, verás una pantalla donde se muestra información diversa sobre el dispositivo y su estado.

Si el dispositivo tiene algún problema, se mostrará en el interfaz con algún símbolo como una señal de prohibido o una admiración.

En la pestaña Controlador, verás una pantalla en la que se muestra información diversa del controlador del dispositivo. Hay disponibles varios botones:

- **Detalles del controlador**: al pulsar en este botón, se mostrará diversa información sobre los archivos correspondientes al controlador del dispositivo.
- **Actualizar controlador**: al pulsarlo, se podrán actualizar los archivos del controlador del dispositivo.
- **Volver al controlador anterior** (en Windows 7, **Revertir al controlador anterior**): se podrá volver al controlador anterior si se han actualizado los archivos del controlador del dispositivo.
- **Deshabilitar** (únicamente en Windows 7): al pulsarlo, se podrá deshabilitar el dispositivo.
- **Desinstalar**: se podrá desinstalar el dispositivo.

En la pestaña Detalles, verás una pantalla en la que podrá ver o modificar el valor que desee para las propiedades.

En la pestaña Eventos se puede ver el historial de eventos sobre ese dispositivo.

En la pestaña **Recursos**, verás una pantalla en la que se muestra la configuración de los recursos del controlador y la lista de conflictos.

3.6.4 EL ADMINISTRADOR DE TAREAS.

El **Administrador de tareas** proporciona información acerca de los programas, procesos y servicios que se están ejecutando en el equipo. También, muestra medidas de rendimiento del equipo, así como otra información. Para ejecutar la utilidad siga los pasos siguientes:

Pulse las teclas [Ctrl] + [Alt] + [Supr]

Pulse en Iniciar el Administrador de tareas y accederá a la ficha Aplicaciones.

En ella se muestra el estado de los programas que se están ejecutando en el equipo. Desde ella se puede finalizar un programa, cambiar a otro de los programas en ejecución o iniciar uno nuevo.

En la ficha **Procesos**, se muestra información acerca de los procesos que se están ejecutando en el equipo (del usuario que ha iniciado sesión o de todos los usuarios). Si desea finalizar un proceso, selecciónelo y pulse en Finalizar proceso).

En la ficha **Servicios**, verás una pantalla en la que se muestra información acerca de los servicios que se están ejecutando en el equipo. Si pulsa en Servicios, podrás detener o iniciar los que desees.

En la ficha **Rendimiento**, verás una pantalla en la que se muestra información actualizada sobre el rendimiento del equipo.

En la ficha **Usuarios**, verás una pantalla en la que se muestra información sobre los usuarios que están conectados al equipo, el estado de la sesión, el nombre del equipo en el que están conectados y el nombre de la sesión.

3.6.5 LAS DIRECTIVAS LOCALES.

En Windows, los derechos se han agrupado en un conjunto de reglas de seguridad y se han incorporado en unas consolas de administración denominadas **directivas de seguridad** que definen el comportamiento del sistema en temas de seguridad. Entre ellas se encuentra la **Directiva de seguridad local** que es la que se debe utilizar si se desea modificar la configuración de seguridad que afecta a una estación de trabajo y a los usuarios locales de la misma.

Para poder ver las distintas opciones de la directiva local, accede a **Herramientas administrativas** que se encuentran en el **Panel de control** y selecciona **Directiva de seguridad local.** También se puede teclear en la caja de búsqueda o la línea de comandos **secpol.msc**

Desde dichas herramientas de administración se pueden establecer, entre otras, las siguientes directivas:

- **Directivas de cuentas**: en este apartado se puede establecer cuál es la política de cuentas o de contraseñas que se seguirá. Dentro de este apartado se pueden distinguir reglas en dos grupos: **Contraseñas y Bloqueo**. Entre ellas, hacen referencia a cómo deben ser las contraseñas en el equipo (longitud mínima, vigencia máxima, historial, etc.) y cómo se debe bloquear una cuenta que haya alcanzado un cierto máximo de intentos fallidos de conexión.

- **Directiva local**: en este apartado se encuentran: la **Auditoria** del equipo, que permite registrar en el visor de sucesos ciertos eventos que sean interesantes, a criterio del administrador (por ejemplo, los inicios de sesión local), y los derechos y privilegios que pueden tener los usuarios en el equipo.

- **Directivas de clave pública**: en este apartado se pueden administrar las opciones de seguridad de las claves públicas emitidas por el equipo.