

GESTIÓN Y ADMINISTRACION EN WINDOWS



26 de marzo de 2020

LAS NAVES SALESIANOS

AARÓN CAÑAMERO MOCHALES

Desarrollo de la práctica en modo gráfico y texto

En esta práctica necesitarás una Máquina Virtual con Windows 10 instalado.

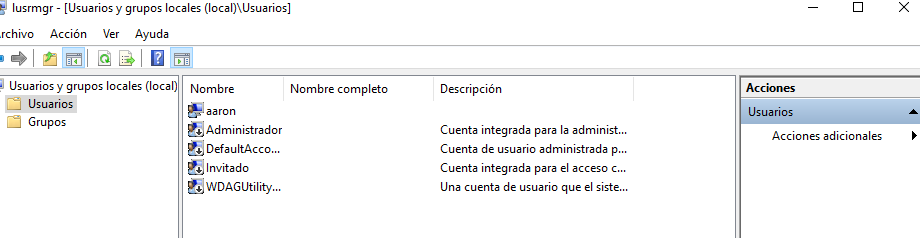
En esta práctica no utilizarás el usuario administrador, sino otro conjunto de usuarios que se crearán exclusivamente para esta práctica en el sistema.

En esta práctica se trabajarán conceptos que debes de añadir a tus conocimientos teóricos de la materia.

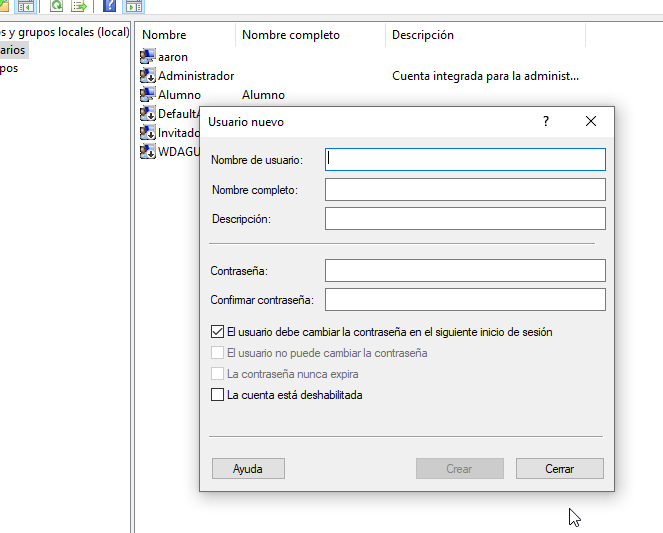
1 Inicio de sesión:

Crea los usuarios con el nombre Alumno, AlumnoGMA1 y AlumnoGMA2 y el grupo AlumnosGM, al que pertenecerán los usuarios, además Alumno debe de pertenecer el grupo de administradores.

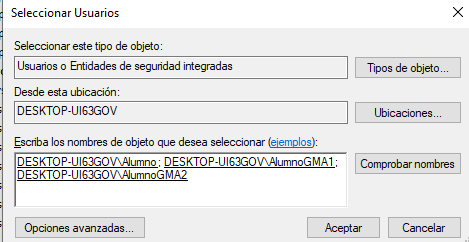
En primer lugar, vamos a crearlo en entorno gráfico, para ello abrimos el menú de **USUARIOS** Y **GRUPOS LOCALES**, una vez abierto nos saldrá dos carpetas una de **USUARIOS** y otra de **GRUPOS**, en ellas nos van a salir todos los creado previamente y haciendo clic derecho podemos crear nosotros nuevos, en primer lugar, vamos a crear los **USUARIOS**.



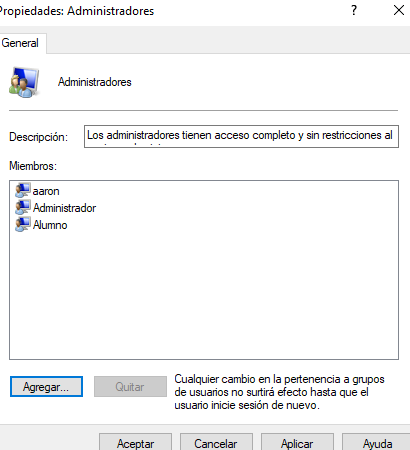
Aquí nos saldré como queremos crear el **USUARIO** y como queremos que se llame.



Para crear el **GRUPO** vamos a poner el nombre del mismo y ha decirle que **USUARIOS** queremos que estén dentro.

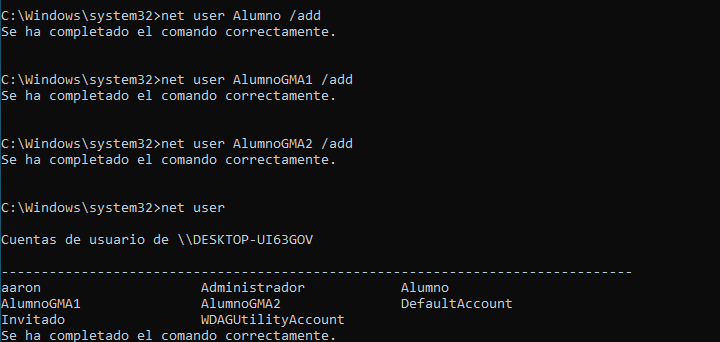


Haremos lo mismo con el **GRUPO ADMINISTRADORES** en este caso el GRUPO ya esta creado, pero igualmente añadiremos el **USUARIO ALUMNO**.



Ahora haremos lo mismo desde el aparto de texto, es decir desde el **CMD**.

Para crear usuarios usaremos el comando **NET USER ALUMNO /ADD**, lo haremos con todos los usuarios que queremos crear, una vez creado, realizaremos un **NET USER**, para comprobar que se han creado correctamente.



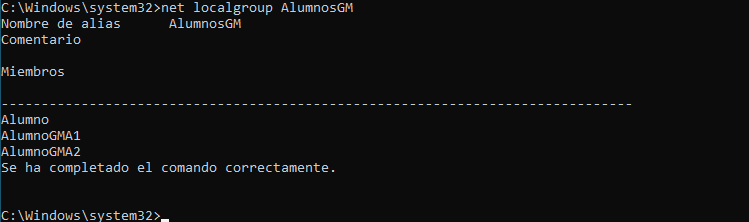
Ahora creamos el grupo con el comando **NET LOCALGROUP ALUMNOGM /ADD**.



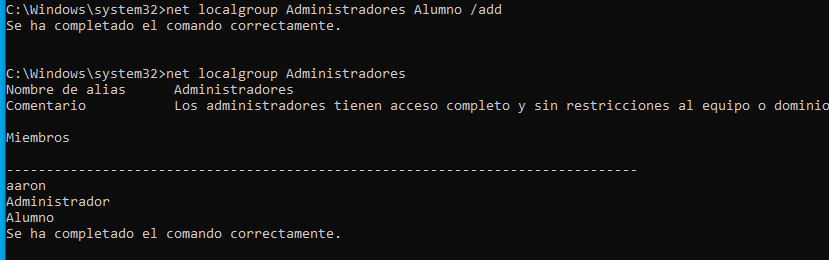
Después añadiremos los usuarios al grupo esto lo haremos con el comando **NET LOCALGROUP ALUMNOGM ALUMNO ALUMNOGMA1 ALUMNOGMA2 /ADD.**



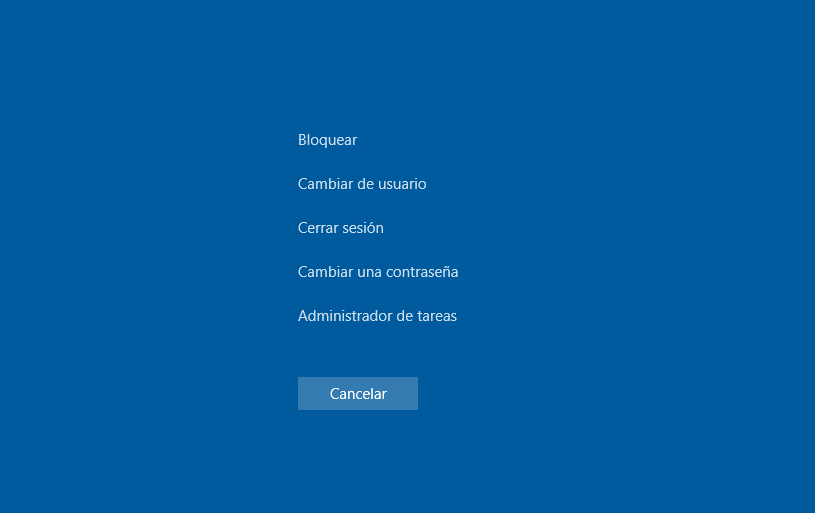
Para comprobar que se ha creado correctamente usaremos el comando **NET LOCALGROUP ALUMNOGM**.



Por último, añadiremos el **USUARIO ALUMNO** al **GRUPO ADMINISTRADORES** y volvemos a comprobar que se ha añadido correctamente con el comando **NET LOCALGROUP ADMINISTRADORES**



Arranca en la Máquina Virtual. Observa la pantalla de bienvenida. En este momento, el programa *Winlogon* tiene el control del escritorio. Nos encontramos en su escritorio privado. Introduce la combinación de teclas Ctrl-Alt-Supr.



Esta combinación es conocida como SAS (*Secure Attention Sequence*). SAS provoca la apertura de la ventana, que, entre otras cosas permite el cambio de usuario activo. Entra como AlumnoGMA1. Una vez que el usuario se ha autenticado en la VM (es decir, ha proporcionado un nombre y clave correctos), se abandona el escritorio de *Winlogon* y se conmuta al escritorio de las aplicaciones. En este momento se ha iniciado la sesión de trabajo.

*Winlogon* sigue disponible durante toda la sesión de trabajo. Podemos activarlo en cualquier momento introduciendo la SAS. Al activar *Winlogon* desaparece todo lo que tenemos en el escritorio actual, que es el escritorio de las aplicaciones. Esto es completamente lógico porque se produce una conmutación al escritorio privado de *Winlogon*. Vamos a repetir la operación poniendo en foco en otro sitio.

Teclea la SAS. Ahora te encuentras en el escritorio de *Winlogon*, sobre el que se representa la ventana denominada *Seguridad en Windows*.

1. Existen varios tipos de inicio de sesión, y, en función de ellos el literal que se pone aquí es distinto, Busca y pone en el hueco los literales de los distintos tipos de inicio de sesión existentes.

Tenemos varios tipos de inicio de sesión existentes, **EQUIPO/USUARIO** será la cuenta local de un equipo Monopuesto.

**DOMINIO/USUARIO** sería una cuenta de usuario de un dominio, puedes hacer desde cualquier dispositivo en la red con ese dominio con tu cuenta de usuario y ya tener toda una configuración echa.

Podemos inicia **USUARIO@DOMINIO** como un correo electrónico.

Haciendo SAS, *Winlogon* proporciona al usuario opciones para cerrar la sesión, bloquear la estación de trabajo, etc. Cabe destacar la opción *Cambiar contraseña*. *Winlogon* proporciona un medio seguro para llevar a cabo esta operación.

Como habrás podido darte cuenta, *Winlogon* es un programa fundamental del sistema, que solemos utilizar con bastante frecuencia.

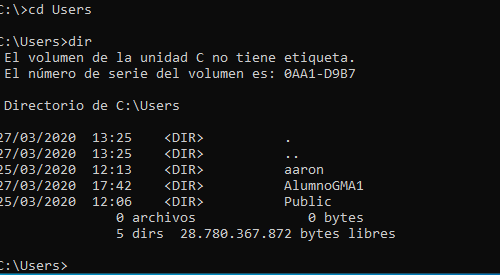
2 El perfil de usuario:

Windows 10 es un sistema con características de seguridad que permite realizar una gestión de los usuarios que utilizan el sistema. Esto implica proporcionar un espacio privado de almacenamiento para cada usuario registrado en el sistema, así como la posibilidad de que cada usuario configure a su gusto su entorno de trabajo en el sistema, es decir, su escritorio. Este espacio privado de almacenamiento y parámetros de configuración son los que conforman el perfil de usuario.

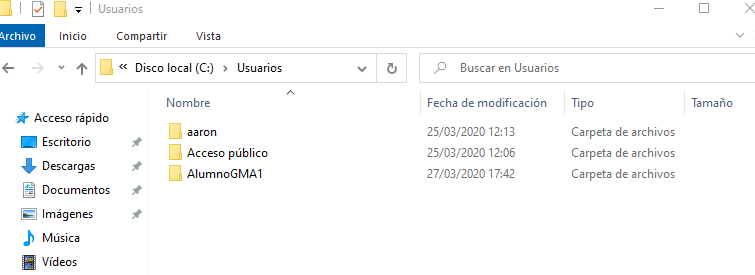
Los perfiles de usuario se almacenan, por defecto, en una carpeta denominada *Usuarios*, que en nuestro caso se ubica en la unidad C.

Abre la carpeta *Usuarios* y observa los nombres de las carpetas que están contenidas en ella. Las carpetas *Alumno*, *AlumnoGMA1*, *AlumnoGMA2* y *Administrador* contienen los perfiles de los usuarios correspondientes.

Para entrar desde el **CMD** a la carpeta **USERS** primero nos dirigiremos a ella, con el comando **CD USERS**, después realizaremos un **DIR** para comprobar que están los **USUARIOS**, en este caso no nos sale el **ALUMNOGMA2,** ni **ALUMNO** porque no se ha creado el perfil del mismo.



Desde el entorno grafico entremos en **DOCUMENTOS** y en la carpeta de **USUARIOS**.

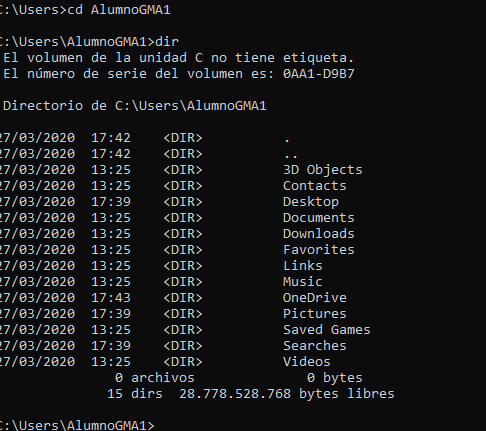


Veremos ahora el cometido de las carpetas almacenadas en el perfil de un usuario y, al mismo tiempo, iremos configurando su perfil, lo cual proporcionará unas determinadas características al entorno de trabajo de este usuario. Para ello utilizaremos el usuario *AlumnoGMA1*. Finalmente compararemos el entorno de trabajo de *AlumnoGMA1* con el de *AlumnoGMA2*, en cuyo perfil no hemos realizado ninguna modificación. Así comprobaremos cómo el perfil define el entorno de trabajo particular para cada usuario.

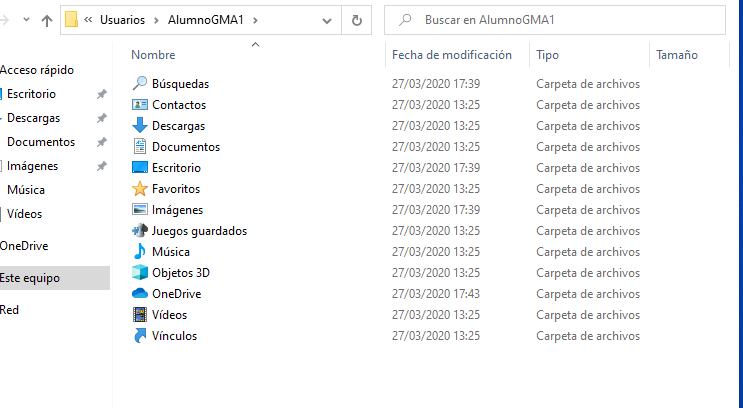
1. Empecemos viendo cuáles con las carpetas típicas que contiene el perfil de un usuario. Abre la carpeta *AlumnoGMA1* e indica a continuación los nombres de las carpetas que se encuentran ubicadas dentro de ella.

En modo texto lo primero que haremos es entrar en el la carpeta con un **CD ALUMNOGMA1** y a continuación realizaremos un **DIR**.

Aquí nos sale el perfil del **USUARIO ALUMNOGMA1**.



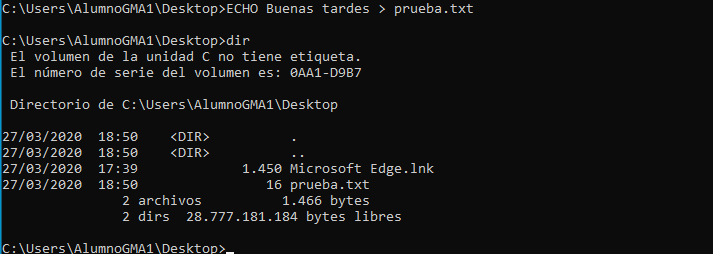
En modo grafico solo tendríamos que entrar en la carpeta.



Una de las carpetas anteriores es *Documentos*. Esta carpeta es la que se utiliza como lugar de almacenamiento privado para el usuario. Hay varios accesos directos a esta carpeta. Cada usuario tiene su propia carpeta *Documentos* en su perfil, de ahí que haya un espacio privado de almacenamiento para cada usuario. Vamos a colocar un fichero en la carpeta *Documentos* del usuario *AlumnoGMA1*.

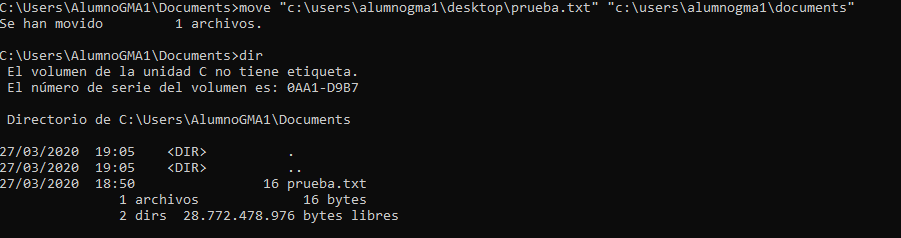
Crea un fichero de texto llamado **prueba.txt** en el escritorio. Escribe en él cualquier cosa. Usando uno de los accesos directos que existen, abre *Documentos*. Mueve **prueba.txt** a esta carpeta y ciérrala después. Ahora abre la carpeta *Usuarios*, después *AlumnoGMA1* y finalmente *Documentos*. Observa cómo el fichero prueba.txt se encuentra en esta carpeta.

Para crear un archivo de texto en el escritorio y añadir texto a la vez usaremos el comando **ECHO BUENAS TARDES > PRUEBA.TXT** primero añadimos el texto que queremos que tenga el archivo y luego el nombre del mismo, después realizamos un **DIR** para comprobar que se ha creado correctamente.

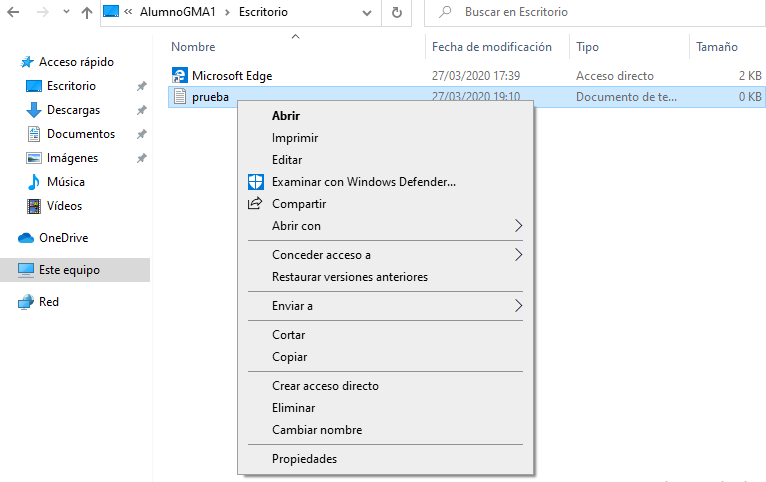


Después vamos a salir del **ESCRITORIO** y vamos a entrar en **DOCUMENTOS** con el comando **CD ..** para salir y **CD DOCUMENTS** para entrar.

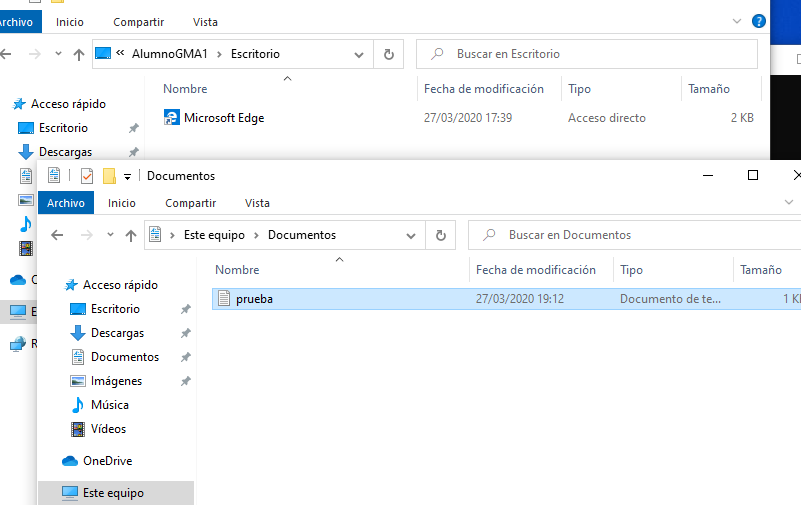
Con el comando MOVE **“C:\USERS\AALUMNOGMA1\DESKTOP\PRUEBA.TXT” “C:\USERS\ALUMNOGMA1\DOCUMENTS”** movemos el fichero de carpeta, es decir con este comando le decimos que queremos que nos mueva x fichero a otra carpeta, ruta del origen de la carpeta y ruta destino, después realizamos un **DIR** después de cerrarlo y veremos que se encuentra el fichero hay.



Desde el modo grafico lo primero que haremos es situarnos en el **ESCRITORIO**, creamos el archivo con clic derecho y nuevo, elegimos el tipo de archivo le damos un nombre y escribimos algo dentro de él.



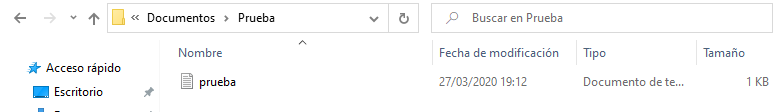
Con Windows E, podemos acceder al acceso directo de documentos una vez hay, después seleccionamos cortar en la carpeta de ESCRITORIO y pegamos en la carpeta de DOCUMENTOS y ya tendríamos el archivo movido de carpeta.



Ahora analizaremos el cometido de la carpeta *Escritorio.* El escritorio de todo usuario tiene por defecto un elemento, la *Papelera de reciclaje*. Este elemento viene definido en el sistema y puede ser el único que se encuentra el usuario cuando entra en el sistema por primera vez. Sin embargo, el usuario puede añadir a voluntad tantos objetos como desee a su escritorio. Normalmente, añadirá accesos directos a aquellas carpetas o programas que más utilice. Incluso puede utilizarse el escritorio para almacenar ficheros temporalmente. Todo lo que se añade al escritorio se almacena en la carpeta *Escritorio* del perfil del usuario.

En este momento tienes en *Documentos* el fichero **prueba.txt**. Crea en *Documentos* una carpeta denominada *Prueba* y mueve a ella el archivo prueba.txt. Ahora copia (copiar no mover) el archivo *Prueba* en el escritorio. Crea un acceso directo a la carpeta *Pruebas* y muévelo (mover no copiar) al escritorio. Abre la carpeta *Escritorio* de tu perfil y comprueba que los elementos que acabas de mover al escritorio se encuentran en ella. Minimiza la carpeta *Escritorio*. Borra del escritorio el fichero prueba.txt. Restaura la capeta *Escritorio*. Observa que el fichero prueba.txt ha desaparecido de la carpeta *Escritorio*.

En modo grafico primero creamos en **DOCUMENTOS** la carpeta **PRUEBA** luego movemos el archivo **PRUEBA** a la carpeta, con cortar y pegar.



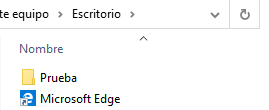
En modo texto primero creamos la carpeta con el comando **MD PRUEBA** y luego movemos el fichero **PRUEBA.TXT**.



Movemos el fichero con el comando **MOVE “PRUEBA.TXT” “PRUEBA”**.



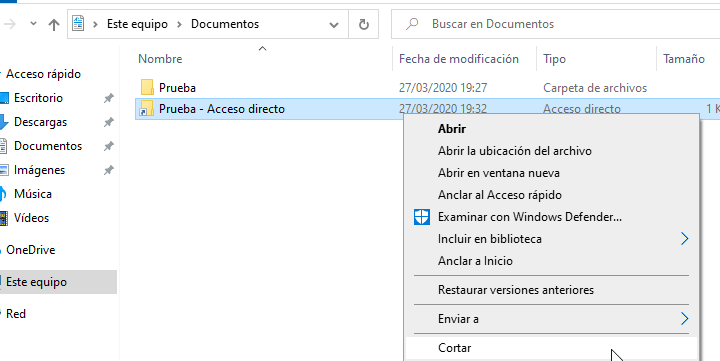
Con un Control c y Control v copiamos el archivo y lo pegamos en la carpeta **ESCRITORIO**.



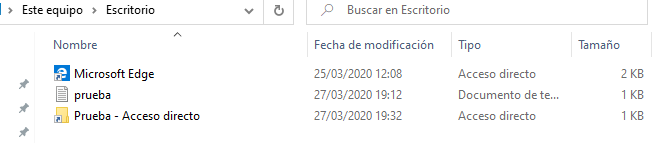
En modo texto realizamos el comando **XCOPY “C\USERS\ALUMNOGMA1\DOCUMENTS\PRUEBA” “C:\USERS\ALUMNOGMA1\DESKTOP”** lo que hacemos con este comando es copiar la carpeta **PRUEBA** al **ESCRITORIO**.



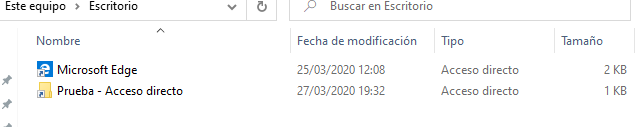
Después creamos un acceso directo de la carpeta **PRUEBA** y movemos el acceso directo a la carpeta **ESCRITORIO**.



Comprobamos que se ha movido todo correctamente.



Eliminamos el fichero y restauramos la carpeta **ESCRITORIO** después comprobamos que se ha eliminado el fichero.

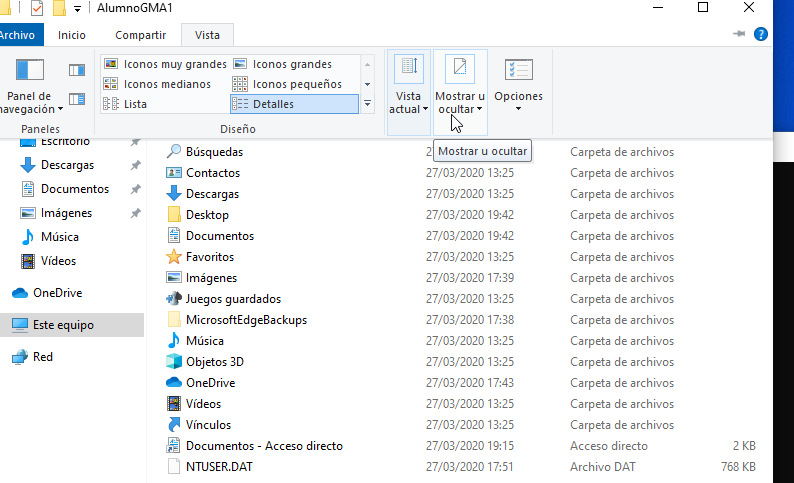


En resumen, los elementos que un usuario coloca en el escritorio se almacenan en la carpeta *Escritorio* de su perfil.

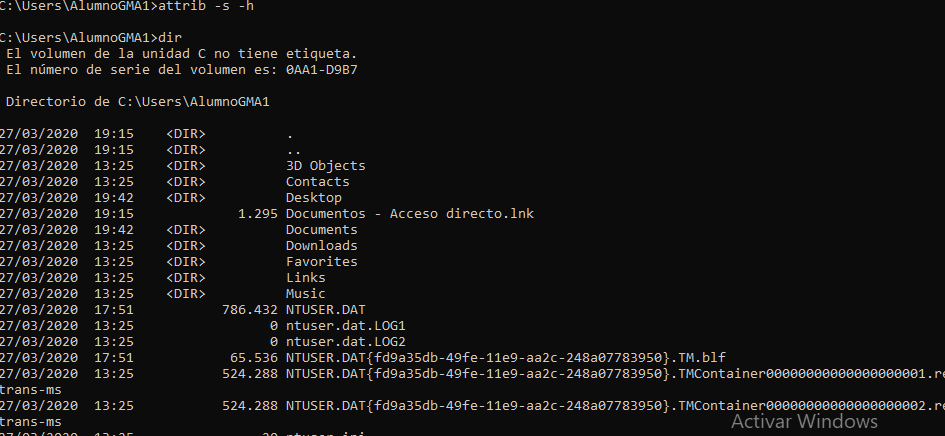
En todo perfil de usuario existen un conjunto de carpetas ocultas. Vamos a hacer visibles estas carpetas y a analizar el cometido de alguna de ellas.

Abre la carpeta *AlumnoGMA1*. Ahora haz que se muestren las carpetas ocultas y ficheros de sistema. Entonces observarás carpetas tales como *Appdata*, *Contactos, Entornos de red*, etc. También observarás el fichero NTUSER.

Desde el entorno gráfico, nos situamos en la carpeta **ALUMNOGMA1** y arriba a la derecha le damos a **VISTA** y seleccionamos la opción de mostrar.

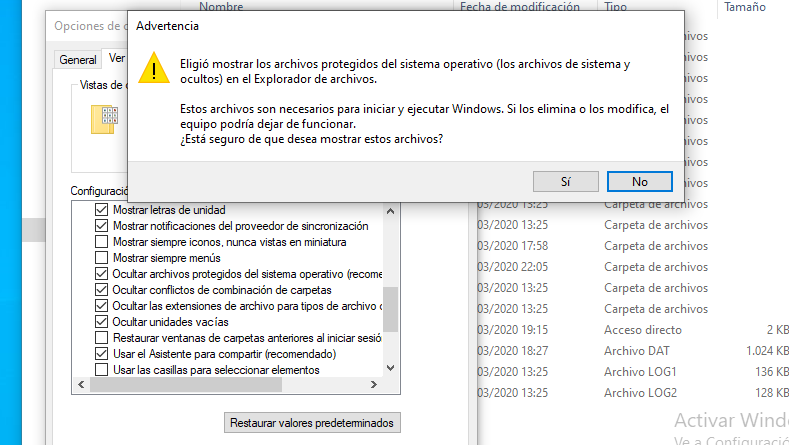


Con el entorno de texto escribimos el comando **ATTRIB -S -H** para que nos aparezcan todos los archivos y ficheros ocultos de la carpeta **ALUMNOGMA1**.



Ahora vas a analizar el funcionamiento de Acceso a Redes y *Documentos recientes*.

En la carpeta *Entorno de red* se almacenan los enlaces a las ubicaciones de red que crea el usuario.

Dichos enlaces son los que se muestran cuando el usuario utiliza la herramienta *Acceso a redes*, a la que se accede desde *Centro de Redes y Recursos Compartidos.* Para probar el uso de la carpeta *Entorno de red* vas a crear una carpeta, la vas a compartir, y accederás a ella a través de Acceso de redes y recursos compartiros -> redes e internet - >Ver equipos y dispositivos de red. Ahora crea un acceso directo a esta ubicación de red, en concreto la carpeta creada.

Desde el mismo punto del párrafo anterior ancla al inicio la conexión directa el recurso compartido.

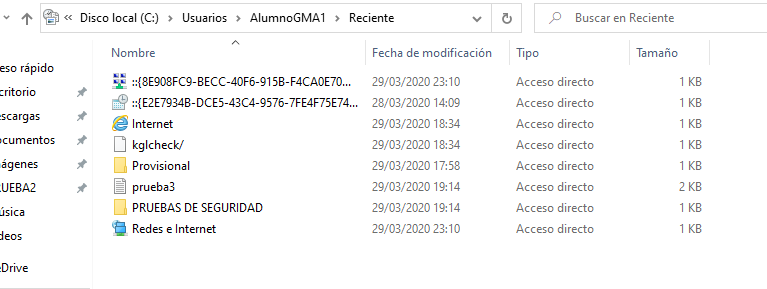


Finalmente analizaremos el cometido de la carpeta *Documentos Recientes*. En esta carpeta se almacenan enlaces a los ficheros (documentos, gráficos, etc.) a los que el usuario ha accedido recientemente.

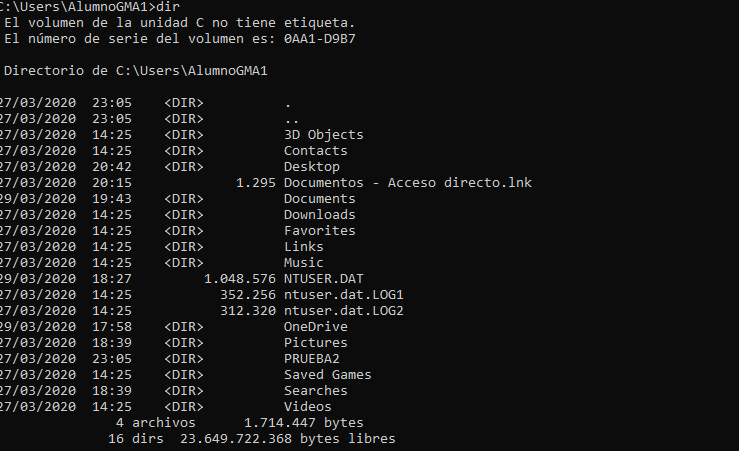
1. Indica a continuación los accesos Actividad reciente del usuario.

Podemos comprobar la actividad reciente del usuario después de haber des ocultado las carpetas y archivos ocultos anteriores.

En **CMD** nos valdría realizando un **DIR** sobre la carpeta, en modo texto.



Hay muchas opciones de configuración que no se guardan mediante accesos directos en las carpetas del perfil, sino en un fichero denominado NTUSER, que se encuentra en la carpeta raíz del perfil de todo usuario.

Abre la carpeta raíz del perfil de *AlumnoGMA1* y comprueba que en ella se encuentra el fichero NTUSER.

Gracias a toda la información de configuración que se guarda en este fichero, cada usuario podrá configurar a su gusto el aspecto de su escritorio y el comportamiento de su entorno de trabajo. Este fichero se maneja a través de la interfaz de usuario mediante diversas opciones. Por ejemplo, mediante la opción *Propiedades* de los menús contextuales de la barra de tareas y del escritorio.

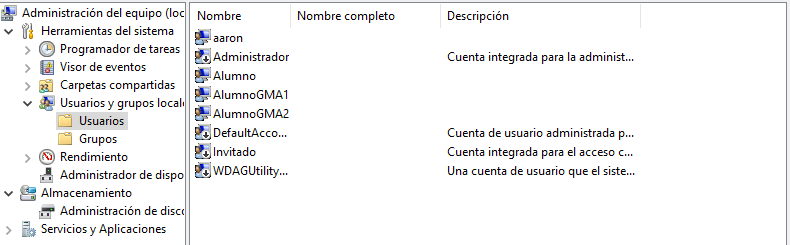
3 Usuarios y grupos:

Para llevar a cabo la gestión de usuarios y grupos se utiliza la herramienta *Administración de equipos*, a la que se accede desde el menú *Herramientas administrativas*. Utilizaremos esta herramienta para ver los usuarios y grupos registrados en el sistema.

Abre la herramienta *Administración de equipos*. Esta herramienta muestra en forma de árbol diversos aspectos relativos a la administración del sistema.

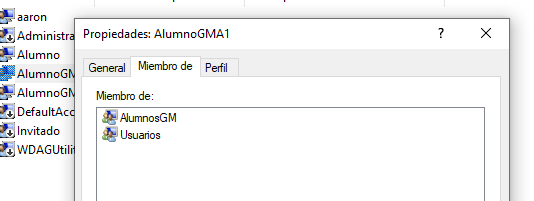


Elige *Usuarios y grupos locales*. Abre la carpeta *Usuarios*. Esto te muestra todos los usuarios registrados en el sistema. El usuario *Administrador* es creado durante la instalación del sistema operativo. Este usuario es el principal responsable de la administración del equipo y tendrá privilegios para acceder a todos los recursos del sistema. El *Administrador* es además el encargado de abrir las cuentas de todos los nuevos usuarios que se vayan registrando en el sistema. Además del Administrador puedes observar que se encuentran también registrados *Alumno*, *AlumnoGMA1* y *AlumnoGMA2*.

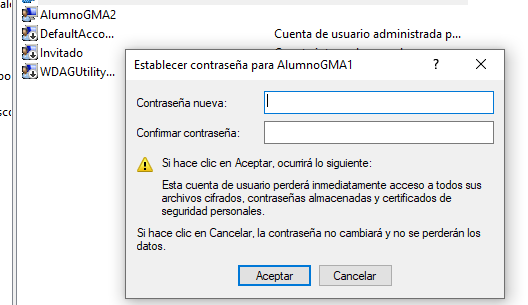


1. Para ver las propiedades de un usuario se pulsa sobre él. Pulsa sobre *AlumnoGMA1* y determina a qué grupo o grupos pertenece y cómo se encuentra configurado el comportamiento de su contraseña. Contesta a continuación.

Grupo(s): ALUMNOSGM, USUARIOS.

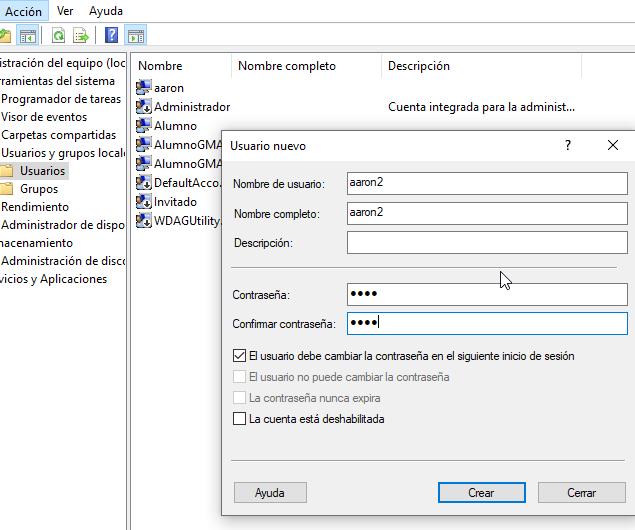


Configuración contraseña: Podemos cambiar la contraseña, pero a cambio perderemos todos los archivos cifrados y contraseñas almacenadas, del usuario.



Intenta ahora crear un nuevo usuario. Utiliza para ello el menú *Acción*, opción *Usuario nuevo*. Rellena los campos del cuadro de diálogo con valores ficticios y pulsa *Crear*. ¿Qué ocurre? ¿Esto se podría hacer con un usuario normal?

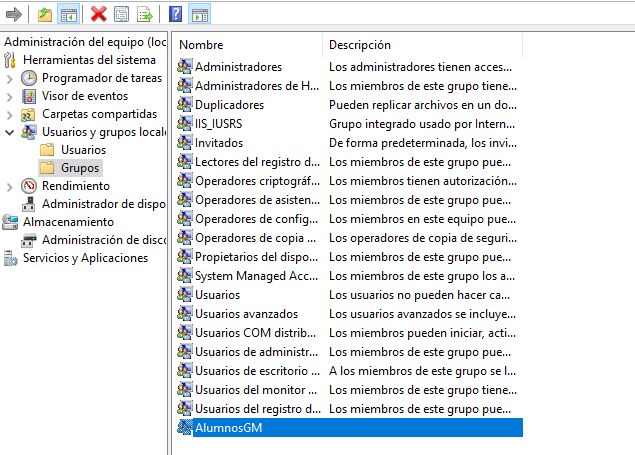
Podemos crear un nuevo usuario, pero con un usuario que no fuera administrador no podríamos crearlo, ya que, para ello, necesitamos ser administrador.



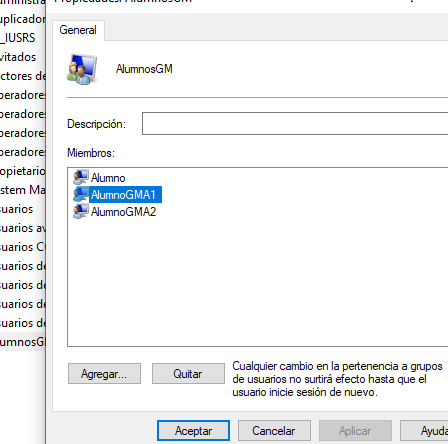
Grupos:

Los *grupos* representan colecciones de usuarios, pudiendo contener a su vez a otros grupos. En primera instancia, los grupos pueden organizarse en dos grandes categorías: *grupos administrables* y *grupos no administrables*. Los grupos administrables son aquellos que van a poder ser administrados por un usuario con privilegios de administración de grupos, el cual podrá determinar, a voluntad, los usuarios que son miembros de cada uno de estos grupos. Los grupos no administrables, como su propio nombre indica, no pueden ser administrados por ningún usuario del pc, ni siquiera por un administrador. Los grupos no administrables reciben el nombre de *grupos especiales*. Más adelante se verá el cometido de estos grupos.

Veamos en primer lugar los grupos administrables. Abre la carpeta *Grupos*. Todos los grupos que puedes observar en esta carpeta son administrables. Prueba que, siendo administrador, puedes añadir o quitar usuarios de ellos a voluntad, en cambio no siendo administrador, pedirá elevación de privilegios, y, lo más que puedes conseguir en llegar a ver sus miembros.



Siendo administrador podemos agregar o quitar usuarios del grupo, sin ser administrador solo podemos ver los miembros de cada grupo.



De todos los grupos que observas en la carpeta *Grupos*, todos, salvo *AlumnosGM*, son grupos predeterminados de Windows, es decir, son creados por el sistema operativo durante la instalación. A estos grupos se los conoce como *grupos integrados*. Por el contrario, el grupo *AlumnosGM* ha sido específicamente creado por el administrador del sistema para esta práctica. Sean estos grupos integrados o creados por el administrador, recuerda que todos ellos son administrables y por ello se muestran en la carpeta *Grupos*.

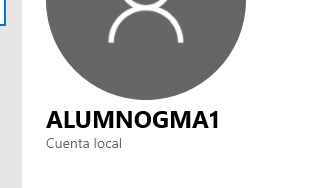
Los *grupos integrados* cuentan con permisos y privilegios predeterminados para propósitos de administración. Así estos grupos proporcionan un medio simple para asignar papeles administrativos a otros usuarios o grupos de usuarios. Por ejemplo, cualquier usuario que se asigne al grupo *Administradores* podrá llevar a cabo cualquier operación en el sistema. Sin embargo, un usuario asignado a *Invitados*, tendrá un acceso muy restringido a los objetos del sistema y las operaciones que se pueden hacer sobre ellos.

Además del grupo *Administradores*, el otro grupo más comúnmente utilizado es el de *Usuarios*. De hecho, cada vez que se crea un nuevo usuario en el ordenador, se asigna por defecto a este grupo. Un usuario del grupo *Usuarios* puede ejecutar programas y acceder a datos en el ordenador local y en otros ordenadores de la red, pero su capacidad de llevar a cabo tareas de administración se encuentra muy restringida. Los usuarios del grupo *Usuarios avanzados* tienen algunas capacidades más que los usuarios normales.

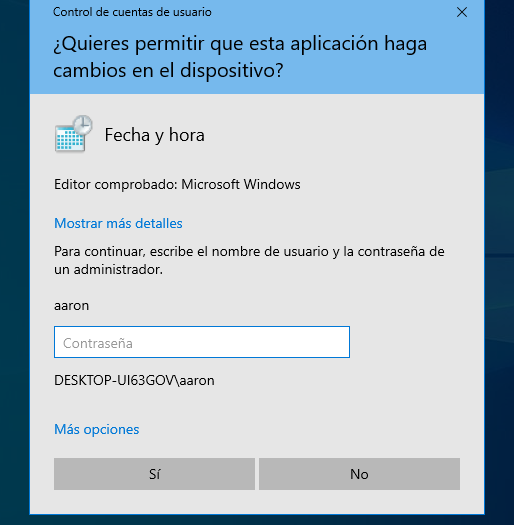
Por ejemplo, pueden crear nuevas impresoras y archivos compartidos en el ordenador y cambiar la hora del sistema. Ç

1. Comprueba que has iniciado sesión en el sistema como *AlumnoGMA1*. Para ello, introduce la SAS y mira el campo *ha iniciado la sesión como*. Recuerda que antes determinaste que *AlumnoGMA1* pertenece al grupo *Usuarios*. Intenta cambiar la hora del sistema. Para ello abre el *Panel de control* y pulsa sobre el comando *Fecha y hora*. ¿Qué ocurre? Indícalo a continuación.

Nos encontramos como **ALUMNOGMA1.**

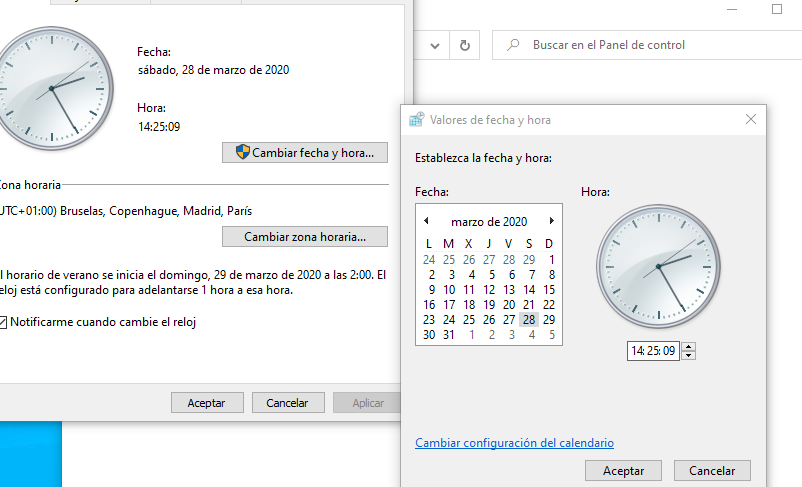


A continuación, intentamos cambiar la fecha y hora de nuestro sistema entrando en el **PANEL DE CONTROL** y después en el menú de **FECHA Y HORA**, pulsamos en la opción cambiar hora y fecha y nos saldrá la siguiente ventana, que quiere decir que no tenemos permiso para cambiar la fecha y la hora de nuestro sistema y que introduzcamos un **USUARIO ADMINISTRADOR** y su contraseña, para poder efectuar este cambio, esto paso porque **ALUMNOGMA1** no tiene los permisos necesarios, para realizar esta acción.



1. Cierra la sesión actual y comienza una nueva sesión como *Alumno*. Intenta ahora cambiar la hora del sistema. ¿Puedes hacerlo? ¿Por qué? Escribe tu respuesta a continuación.

Lo primero que haremos es iniciar sesión en nuestra cuenta de **ALUMNO**. A continuación, una vez iniciada la sesión nos iremos al panel de control, opciones de fecha y hora y cambiar fecha y hora, podemos observar que lógicamente podemos cambiar la fecha y hora de nuestro sistema, porque el **USUARIO ALUMNO**, pertenece al **GRUPO ADMINISTRADORES** y el **USUARIO** hereda los permisos del grupo.

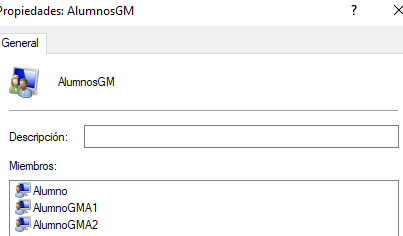


Además de asignar papeles administrativos a los usuarios, los grupos también cumplen otro cometido fundamental: proporcionar un medio simple para dar a una colección de usuarios una serie de permisos de acceso a uno o varios objetos. Por ejemplo, imagina que hay una serie de ficheros en el pc que deben poder ser accedidos por todos los alumnos. Imagina que cada alumno tiene una cuenta privada. Si hay treinta alumnos, deberíamos indicar en la ACL de cada fichero los treinta usuarios que tienen permiso para acceder a él. Esto es claramente inmanejable. La solución es crear el grupo *AlumnosGM*, e incluir en él a todos los alumnos. Entonces para dar permiso de acceso a los ficheros, utilizaremos el grupo *AlumnosGM*, en lugar de la lista de alumnos individuales.

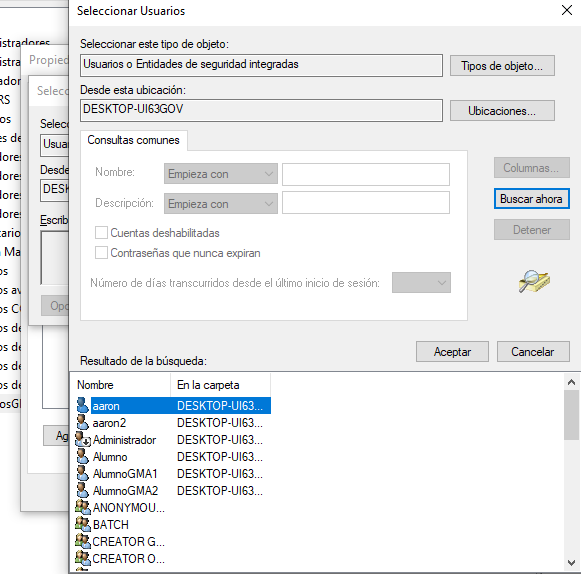
Veamos ahora qué miembros podemos incluir en un determinado grupo y cómo hacerlo. Por supuesto, esto sólo lo podemos hacer con esos grupos que hemos denominado *administrables*, que son los que aparecen en la carpeta *Grupos*.

Abre la carpeta *Grupos*. Pulsa sobre *AlumnosGM*. Observarás que este grupo cuenta con dos miembros, *AlumnoGMA1* y *AlumnoGMA2*.

Contiene 3 **USUARIOS**, **ALUMNO** está en dos grupos, en el grupo **ALUMNOSGM** y en el grupo **ADMINISTRADORES**.

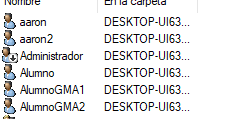


Imagina que quieres añadir otro usuario a *AlumnosGM*. Para ello pulsa *Agregar*. Se abre la ventana *Seleccionar Usuarios*. Esta ventana dispone de una opción de navegación que muestra los usuarios que podemos agregar al grupo. Para activar esta opción debes pulsar el botón *Avanzadas* y a continuación *Buscar ahora*. Entonces se muestra una lista con los usuarios y grupos que pueden hacerse miembros de *AlumnosGM*. Los usuarios se indican mediante un icono que representa una cabeza, los grupos mediante un icono que representa dos cabezas. Los usuarios que pueden hacerse formar parte de un grupo son todos los que se encuentran registrados en el sistema.



1. Indica a continuación cuáles son estos usuarios (solo usuarios, no grupos).

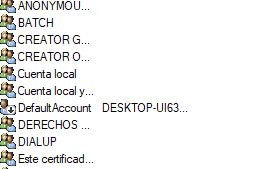
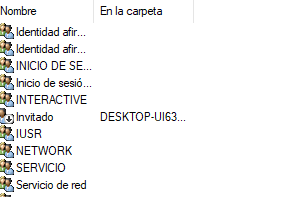
Estos usuarios son **AARON, AARON2, ADMINISTRADOR,ALUMNO, ALUMNOGMA1, ALUMNOGMA2.**

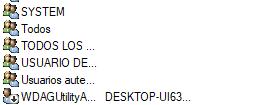


Además de los usuarios anteriores, observarás que hay un conjunto de grupos que pueden formar parte de *AlumnosTC…* Sin embargo, ninguno de los grupos que observas ahora pertenece a la categoría de grupos administrables que vimos antes. Así observarás que no está disponible ni el grupo *Administradores*, ni *Usuarios*, ni *Usuarios avanzados*, etc. Pues bien, los grupos que observas ahora en la ventana *Seleccionar usuarios* son los que se conocen como *Grupos especiales*, que están fuera de la categoría de *Grupos administrables*.

1. Aunque son unos cuantos, escribe a continuación cuáles son los grupos especiales disponibles en tu ordenador.

A continuación, podemos observar todos los grupos especiales disponibles en nuestro ordenador.





Del ejercicio anterior debes extraer una conclusión importante: **un grupo administrable sólo puede contener usuarios y grupos especiales. De esto se deduce que un grupo administrable no puede contener a otros grupos administrables.**

Intenta buscar en Internet una definición para los grupos *Inicio de sesión remoto interactivo* (el nombre de este grupo en la versión inglesa de Windows es *Remote interactive logon*), INTERACTIVE, y RED (NETWORK en la versión inglesa). Usa Google y un conjunto de palabras clave apropiadas, como por ejemplo “Windows 10”, Groups, INTERACTIVE, NETWORK, etc.

1. Anota a continuación las definiciones que has encontrado.

**Inicio de sesión remoto interactivo:**

Es el grupo al cual automáticamente cualquier usuario que ha iniciado sesión en el sistema mediante el escritorio remoto.

**Interactive:**

Es el grupo al que pertenece automáticamente todo usuario que ha iniciado sesión en el sistema, ya sea en la propia consola del sistema o utilizando el escritorio remoto.

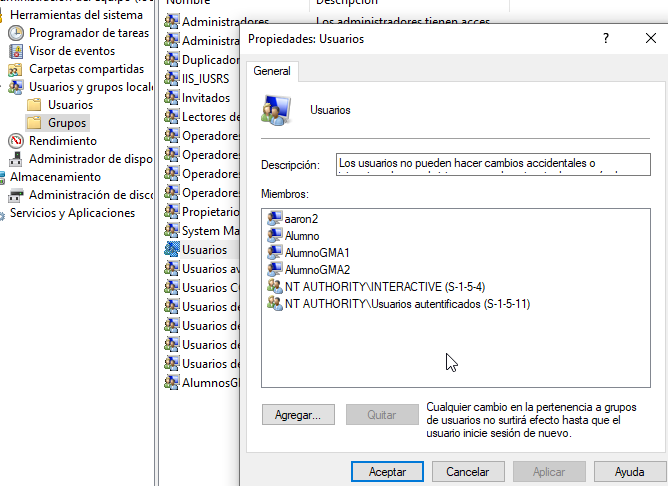
**RED:**

Es el grupo al cual automáticamente todo usuario que ha establecido una conexión con el sistema a través de red.

Cuando un grupo especial se hace formar parte de un grupo administrable, el sistema marca al grupo especial con el distintivo NT AUTHORITY, con objeto de diferenciarlo de los usuarios normales que formen parte del grupo.

1. Abre el grupo *Usuarios* e indica a continuación los grupos especiales que forman parte de él. Observarás que dichos grupos se encuentran precedidos por el distintivo NT AUTHORITY.

Dentro del grupo **USUARIOS** encontramos los grupos especiales.



4 Seguridad de ficheros y carpetas:

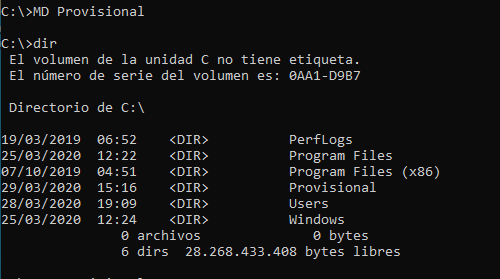
Todos los objetos de tipo fichero o carpeta se encuentran protegidos por un SD (Security Descriptor). Una parte de este elemento, la ACL (Access Control List), determina la lista de usuarios y grupos que tienen acceso a un determinado fichero o carpeta. Además, a cada usuario o grupo de la ACL se le pueden proporcionar permisos específicos. En este apartado vamos a trabajar con la ACL de ficheros y carpetas.

Como paso previo, vas a crear una carpeta en la que todos los usuarios del sistema puedan llevar a cabo cualquier operación. Para ello, necesitas ser el usuario Administrador.

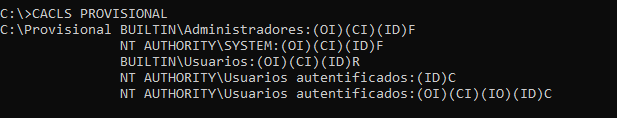
Cierra cualquier sesión que tengas abierta y abre una nueva sesión como Administrador. Crea en la unidad C: una carpeta llamada *Provisional.* Ahora vas a preparar esa carpeta para que todos los usuarios puedan escribir en ella. Abre las *Propiedades* de la carpeta, ficha *Seguridad*. Agrega el grupo *Todos* a la ACL de la carpeta. Activa el permiso *Control total* para este grupo y cierra *Propiedades*.

Lo primero que haremos es entrar en modo **ADMINISTRADOR** al **CMD** esto lo lograremos con un clic derecho sobre le herramienta y seleccionando la opción dicha antes.

A continuación, nos situamos en la unidad **C** y creamos una carpeta con el comando **MD PROVISIONAL**, después realizamos un **DIR** para comprobar que se ha creado correctamente.



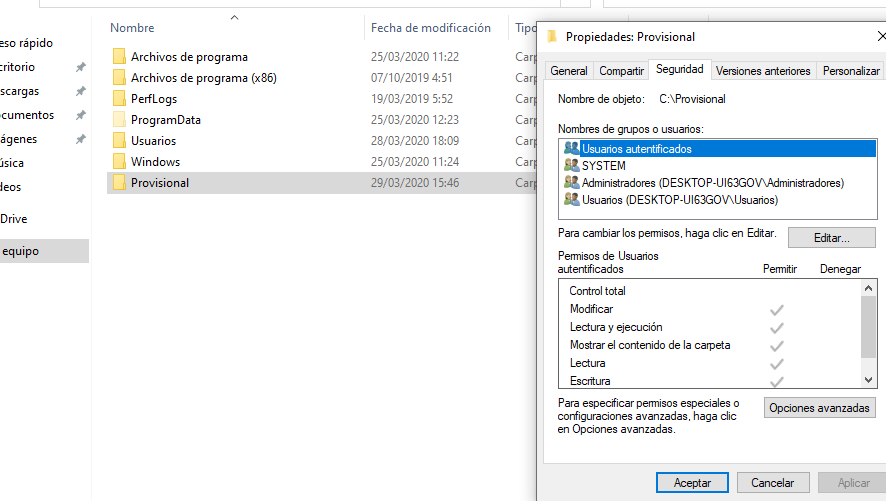
Ahora vamos a comprobar las ACLS de la carpeta con el comando **CACLS PROVISIONAL**.



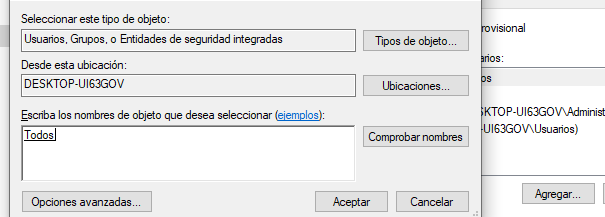
Con el comando **CACLS PROVISIONAL /G TODOS: F** añadimos el grupo **TODOS** y le decimos que puede tener todos los permisos.



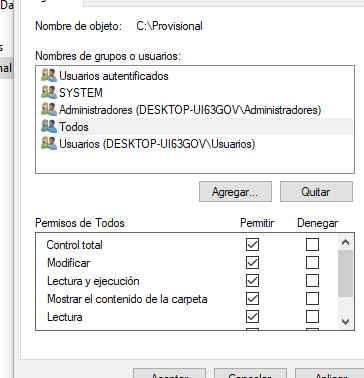
En modo grafico creamos la carpeta y damos clic derecho seleccionamos propiedades y luego seguridad.



Después seleccionamos opciones avanzadas y añadimos el grupo **TODOS**.



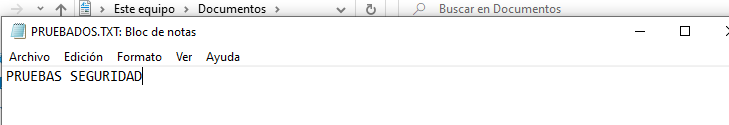
Después seleccionamos los permisos y le damos aplicar.



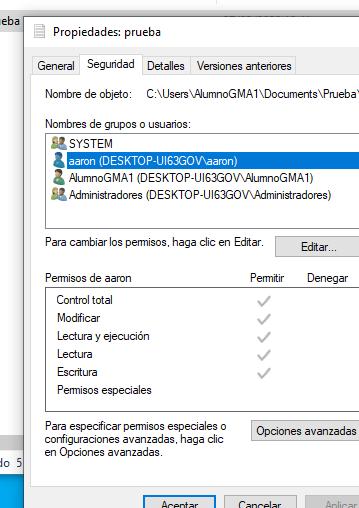
Tras esta operación inicial, vamos a ver más detenidamente el cometido y funcionamiento de la ACL.

Cierra la sesión del *Administrador*. Inicia una nueva sesión como *AlumnoGMA1*. Crea con el *Bloc de notas* un fichero que contenga la frase “Pruebas de seguridad”, dale el nombre pruebados.txt y almacénalo en *Documentos*. Ahora abre la hoja de propiedades de prueba.txt. Elige la ficha *Seguridad*. Esto te muestra la ACL del fichero.

En modo grafico creamos el fichero con el block de notas y luego lo guardamos en documentos.



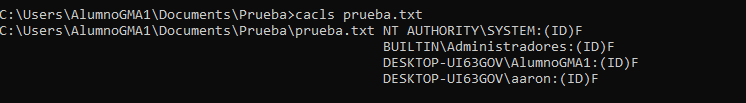
Entramos en las propiedades del fichero prueba.txt con el clic derecho y nos vamos a la parte de seguridad y vemos la **ACLS** del fichero.txt.



En modo texto entramos en el usuario **ALUMNOGMA1** y después creamos el fichero con el comando **ECHO PRUEBAS DE SEGURIDAD > PRUEBADOS.TXT** con este comando le decimos que vamos a crear un nuevo fichero y que queremos que tenga ese contenido.



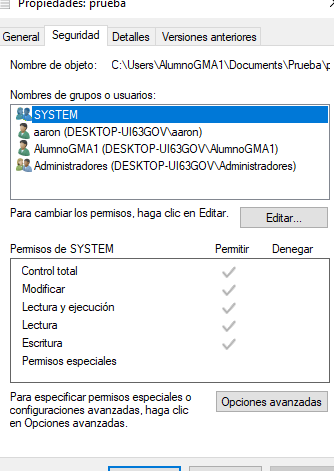
Para poder ver las ACLS que le corresponde al fichero **PRUEBA.TXT** vamos a realizar el comando **CACLS PRUEBA.TXT**



1. Anota a continuación los usuarios y grupos correspondientes a la ACL de este fichero.

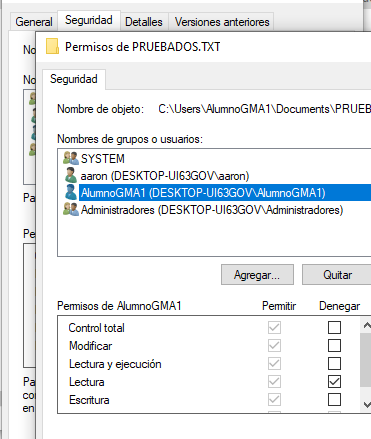
**Admistradores, AlumnoGMA1 y SYSTEM**, también tenemos el usuario Aaron que es mío creado personalmente.

Selecciona cualquiera de los usuarios o grupos de la ACL. En el cuadro de diálogo inferior, llamado *Permisos*, puedes observar los permisos con los que cuenta el grupo o usuario seleccionado sobre el objeto que estamos analizando.



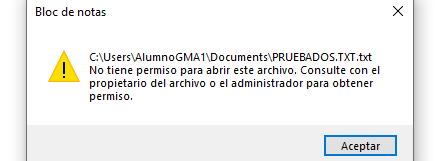
Selecciona *AlumnoGMA1* en la ACL. Puedes observar que cuenta con todos los permisos. Esta suele ser la situación por defecto, ya que normalmente los objetos heredan sus permisos de otros objetos. En este caso el fichero pruebados.txt ha heredado sus permisos de la carpeta *Documentos* del usuario *AlumnoGMA1*. En la situación actual *AlumnoGMA1* puede hacer cualquier cosa con pruebados.txt. Ahora deniega a *AlumnoGMA1* (o sea, a ti mismo) el permiso *Leer* sobre el fichero pruebados.txt.

Quitamos el permiso de leer al **ALUMNOGMA1** en el fichero.



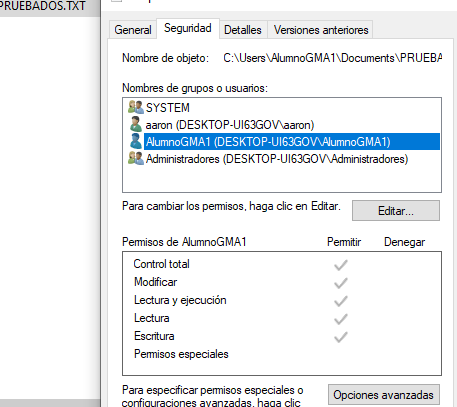
1. Cierra la hoja de propiedades de este fichero e intenta abrirlo. ¿Qué ocurre? Indícalo a continuación

A continuación, intentamos leer el fichero y podemos comprobar que no se puede leer, porque no tenemos permisos, ya que anteriormente los hemos cancelado.



Vuelve a abrir la hoja de propiedades de pruebados.txt y deja los permisos de *AlumnoTC1* como estaban. Cierra la hoja de propiedades y abre de nuevo el fichero, comprobando que ahora puedes acceder a él sin problema.

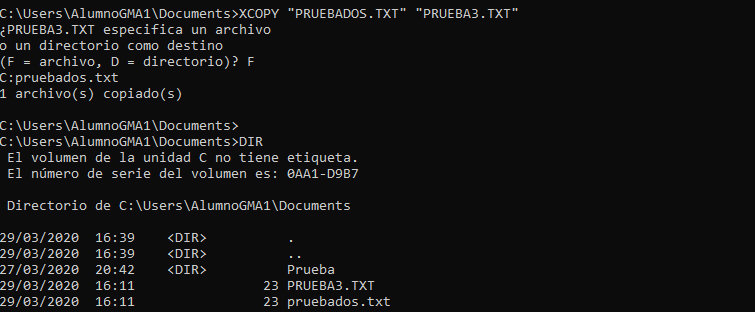
Dejamos la configuración de las ACLS anterior, para que nuestro usuario ALUMNOGMA1 pueda leer el fichero.



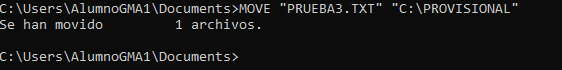
Mediante el ejercicio has comprobado cómo influyen los permisos concedidos a un usuario en su capacidad de acceso a un objeto, pero teniendo en cuenta que el usuario forma parte de la ACL del objeto. Veamos ahora qué ocurre cuando un usuario que no se encuentra en la ACL de un objeto intenta acceder a él.

Haz una copia de pruebados.txt, llámala prueba3.txt y almacénala también en *Documentos*. Mueve prueba3.txt a la carpeta *Provisional* (tiene que ser mover, no vale copiar). Comprueba que prueba3.txt conserva la misma ACL que tenía antes de moverlo. En su ACL deben estar los usuarios *Administradores*, *AlumnoGMA1* y *SYSTEM*. Ahora cierra la sesión y comienza una nueva sesión como *AlumnoGMA2*.

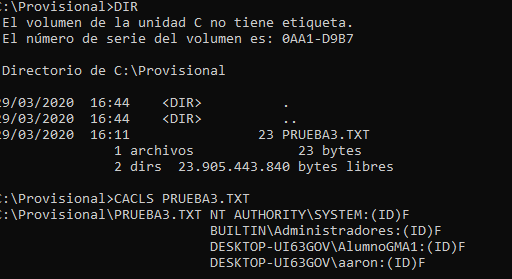
Desde la consola de comando realizamos el comando **XCOPY “PRUEBADOS.TXT” “PRUEBA3.TXT”** con este comando lo que le decimos es que nos copie ese fichero y nos lo pegue en la dirección **DOCUMENTOS** que es en la cual nos encontramos, después realizamos un **DIR** para comprobar que se ha copiado correctamente con otro nombre.



Con el comando **MOVE “PRUEBA3.TXT” “C:\PROVISIONAL”** movemos el fichero.

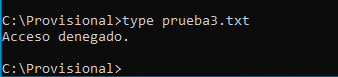


Una vez estemos en la carpeta **PROVISIONAL** realizamos un **DIR**, comprobamos que se ha movido correctamente el fichero y después realizamos un **CACLS PRUEBA3.TXT** y podemos comprobar que usuarios y grupos tienen permisos sobre el fichero.



1. Intenta abrir prueba3.txt. ¿Qué ocurre? Anótalo a continuación.

Al intentar abrir el fichero para ver el contenido que tiene dentro con el usuario ALUMNOGMA2, no podemos porque no tenemos permisos para poder abrirlo.



Debes extraer como conclusión que sólo pueden acceder a un objeto aquellos usuarios que formen parte de su ACL.

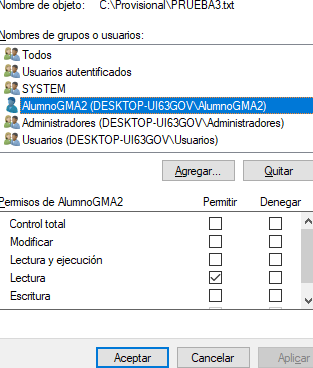
Imagina ahora que es necesario darle permiso de lectura a prueba3.txt al usuario AlumnoGMA2. Para ello es necesario que otro usuario que tenga permiso de acceso al objeto incluya en la ACL de éste al usuario AlumnoGMA2. Vamos a hacerlo.

Cierra la sesión en curso (ahora eres AlumnoGMA2) e inicia una nueva sesión como AlumnoGMA1. Abre la ficha Seguridad de la hoja de propiedades de prueba3.txt y añade AlumnoGMA2 a su ACL, dándole permiso de lectura. Para hacer esta operación utiliza el botón Agregar. Cierra la sesión y abre una nueva sesión como AlumnoGMA2. Comprueba que ahora este usuario es capaz de abrir el fichero. Intenta ahora modificar el contenido de este fichero.

Lo primero que haremos es iniciar sesión con el **ALUMNOGMA1** y a continuación entraremos en la carpeta **PROVISIONA**L y después cambiaremos las **ACL** del fichero, con el comando **CACLS PRUEBA3.TXT /G ALUMNOGMA2:R**

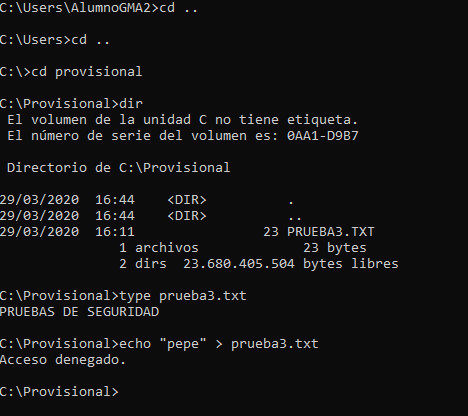


Desde el modo grafico entramos al fichero, vamos a propiedades, seguridad y añadimos el ALUMNOGMA2 y le otorgamos permisos de lectura.



1. ¿Por qué no puedes hacerlo? Responde a continuación.

Una vez entrados en el usuario **ALUMNOGMA2** intentamos leer el archivo y vemos que podemos hacerlo correctamente, después intentamos escribir o modificar el archivo y vemos que nos salta acceso denegado, porque no tenemos permisos para modificar el archivo, pero si para leerlo.



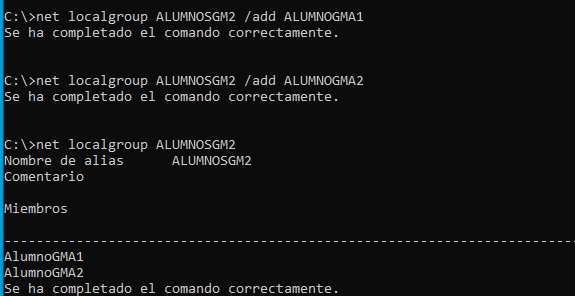
Ahora vas a probar la utilidad de los grupos para dar permisos de acceso a un fichero. En este momento, la ACL de prueba3.txt incluye a *AlumnoTGMA1* y *AlumnoGMA2*, que representan los alumnos de la asignatura SOMO. Imagina que, en lugar de haber dos alumnos, hubiera 50. Agregarlos todos a la ACL de prueba3.txt sería muy tedioso. Para facilitar este tipo de tareas de administración se utilizan los grupos. Se crea un grupo que contenga a todos los alumnos de la asignatura y se utiliza ese grupo para dar permiso de acceso sobre cualquier objeto que se requiera a todos los alumnos colectivamente. En nuestro caso hemos creamos el grupo *AlumnosGM2* que contendrá a los dos alumnos de la asignatura. Utilizaremos ahora *AlumnosGM2* para dar permiso de acceso colectivo sobre prueba3.txt.

Cierra la sesión actual e inicia una nueva sesión como *AlumnoGMA1*. Abre la ficha *Seguridad* de la hoja de propiedades de prueba3.txt. Agrega el grupo *AlumnosGM2* a la ACL del fichero y dale permiso de *Control total*. Borra *AlumnoGMA1* y *AlumnoGMA2* de la ACL y abandona la hoja de propiedades. Abandona la sesión. Ahora iniciarás la sesión como *AlumnoGMA1*, *AlumnoGMA2* y *Alumno* sucesivamente, intentando acceder a prueba3.txt en cada sesión.

Creamos primero el grupo **ALUMNOSGMA2** con el comando **NET LOCALGROUP ALUMNOSGM2 /ADD**

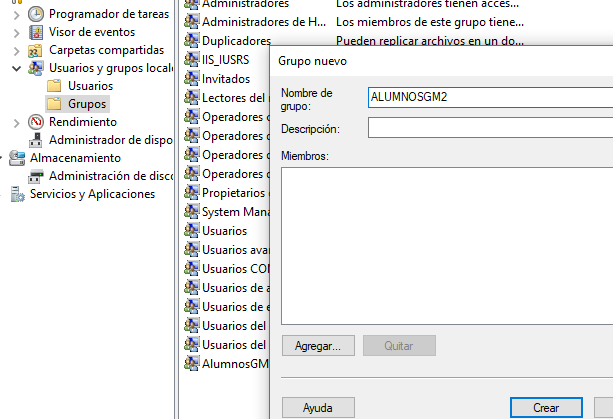


También añadimos los usuarios al grupo.



Desde el apartado grafico tendremos que crear el grupo desde las herramientas administrativas, después administración de equipo y añadir un nuevo grupo desde la opción de acciones.

Necesitaremos tener permisos para realizar estas acciones.



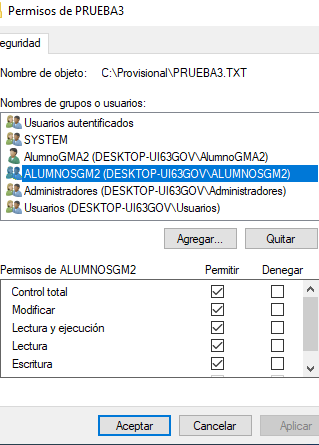
A continuación, vamos a añadir el **GRUPO ALUMNOSGM2** a las **AC**L de **PRUEBA3.TXT**, con el comando **CACLS PRUEBA3.TXT /G ALUMNOSGM2: F** para que tenga un control total.



Ahora vamos a eliminar a los usuarios con el comando **CACLS PRUEBA3.TXT /P ALUMNOGMA1:N ALUMNOGMA2:N** para que no tenga ningún permiso.



Desde modo grafico accedemos a la carpeta y nos vamos a propiedades des hay cambiamos los permisos

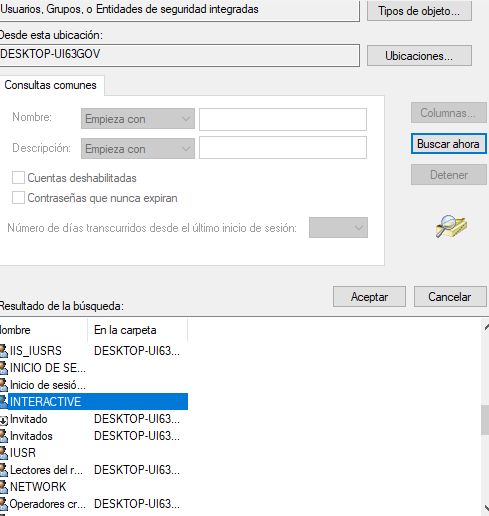


1. ¿Qué sucede en cada caso? Justifícalo.

Los dos alumnos tienen acceso a todo porque están en el grupo de **ALUMNOSGM2** y **ALUMNO** tiene acceso porque está en el grupo de administradores.

1. ¿Cómo podrías conseguir que *Alumno*, *AlumnoGMA1* y *AlumnoGMA2* tengan acceso a prueba3.txt, sin estar ninguno de ellos ni tampoco *AlumnosGM2* en la ACL de prueba3.txt? Responde a continuación y prueba tu respuesta.

Pues una de las formas seria añadiendo el grupo **INTERACTIVE**, para que cualquier usuario que pueda acceder a la consola **AUTENTIFICANDOSE** pueda acceder al fichero **PRUEBA3.TXT**.

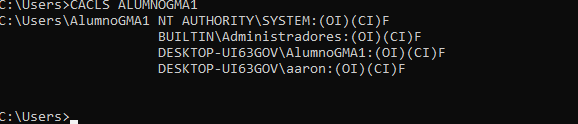


Carpetas:

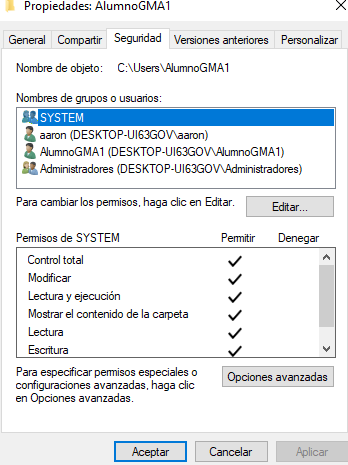
El funcionamiento de la seguridad de las carpetas es totalmente similar al de los ficheros. Su seguridad se basa en la ACL, que determina quién tiene acceso a la carpeta y con qué permisos cuenta. Empezaremos viendo la ACL de las carpetas de los perfiles de usuario.

1. Cierra la sesión en la que te encuentres e inicia una nueva como *AlumnoGMA1*. Visualiza la ACL de la carpeta raíz del perfil de *AlumnoGMA1*. Recuerda que los perfiles se almacenan en la carpeta *Usuarios*. Anota la lista de usuarios y grupos que aparecen en su ACL.

Desde el modo texto accedemos con el comando **CACLS** **ALUMNOGMA1** y hay nos saldrá los grupos y usuarios a los que perteneces en su **ACL**.



En modo grafico accedemos desde la carpeta de **USERS**.

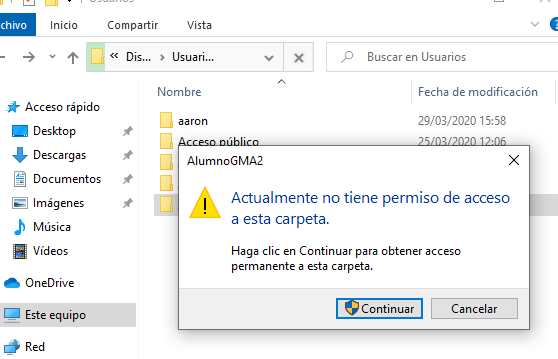


Comprueba que puedes abrir la carpeta raíz de tu perfil y hacer con ella cualquier operación.

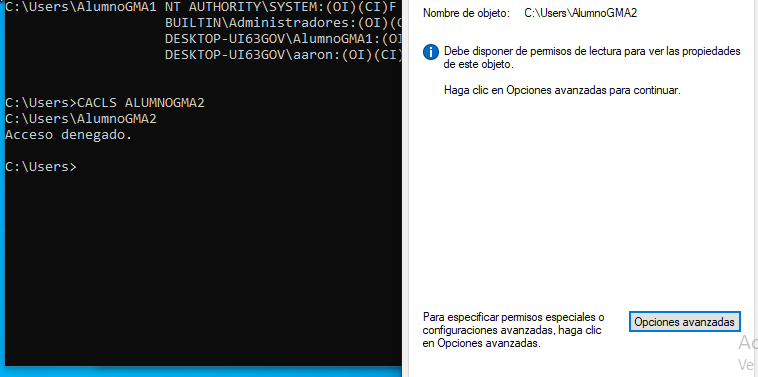
Podemos hacer cualquier cosa a nuestra carpeta raíz, ya que somos el dueño de la misma.

1. Ahora intenta abrir la carpeta raíz del perfil de *AlumnoGMA2*. ¿Qué ocurre? Anótalo a continuación.

Desde el modo grafico y el modo texto nos va salir lo mismo, vemos que no tenemos permisos para poder acceder a la carpeta raíz de **ALUMNOGMA2**.

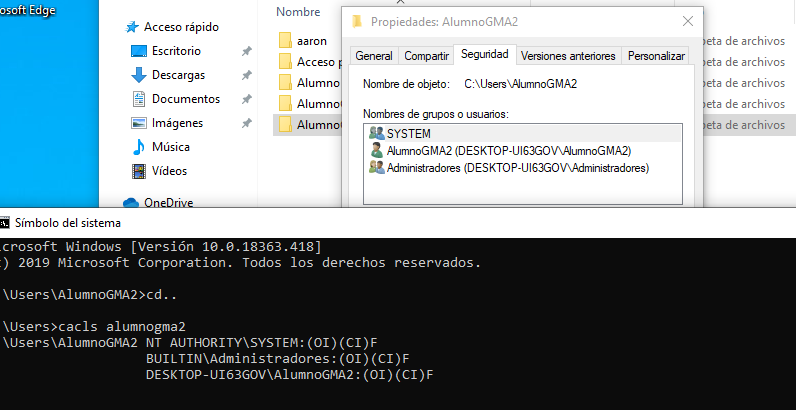


1. Abre su hoja de propiedades. ¿Qué observas?

Tenemos que tener permisos para poder ver las propiedades.

Ten en cuenta que el perfil de cada usuario se encuentra protegido para que sólo el propio usuario o un administrador puedan acceder a él.

Para hacer ya la última comprobación, cierra la sesión actual e inicia otra como AlumnoGMA2. Ahora tendrás acceso a la carpeta raíz del perfil de AlumnoGMA2. Observa su ACL, comprobando que en ella se encuentra AlumnoGMA2.

Accedemos al usuario **ALUMNOGMA2** y comprobamos que todo esta correctamente.

Herencias de permisos:

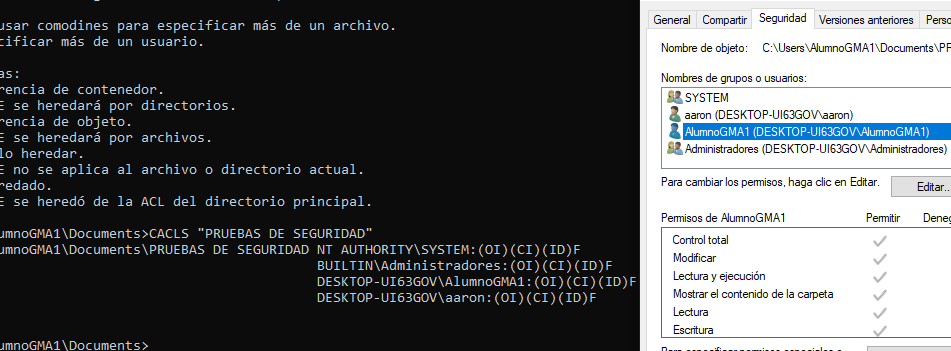
La herencia de permisos es una propiedad de los objetos, que les permite heredar permisos de otros objetos primarios. Así por ejemplo cuando se crea un fichero en una carpeta, normalmente el fichero heredará los permisos de la capeta, aunque debe indicarse que esto no tiene por qué ser siempre así. Vamos a comprobar ahora esta propiedad.

1. Inicia una nueva sesión como *AlumnoGMA1*. Crea en Documentos una carpeta llamada *Pruebas de seguridad.* Anota a continuación los usuarios y grupos de la ACL de esta carpeta.

Primero creamos la carpeta con el comando **MD “RPUEBAS DE SEGURIDAD”**, las comillas las ponemos para que se cree solo una carpeta y con sus espacios, sino se crearían 3 carpetas diferentes.

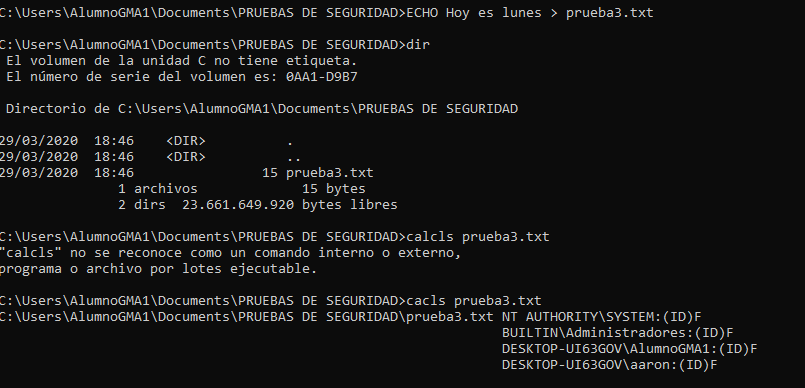


Después realizamos un **CACLS “PRUEBAS DE SEGURIDAD”** para comprobar los **ACL** de la carpeta.

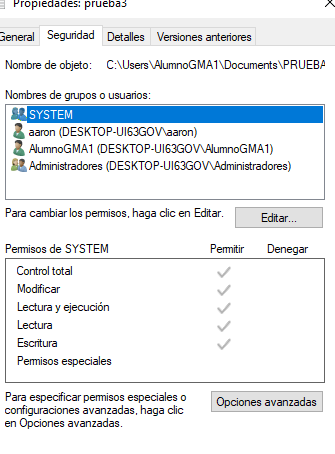


1. Abre el *Bloc de notas* y crea un archivo llamado prueba3.txt. Escribe en él cualquier cosa y almacénalo en la carpeta *Pruebas de seguridad*. Abre la hoja de propiedades del fichero y observa su ACL. ¿Coincide con la ACL de la carpeta *Pruebas de seguridad*?

Primero creamos el archivo con el comando **ECHO HOY ES LUNES > PRUEBA3.TXT** después realizamos un **DIR** para comprobar que se ha creado correctamente, después realizamos un **CACLS PRUEBA3.TXT** para comprobar que las **ACL** son las mismas que las de la carpeta a la cual pertenece, esto pasa por la heredarían.



En modo gráfico, veremos las **ACL** en las propiedades del archivo.

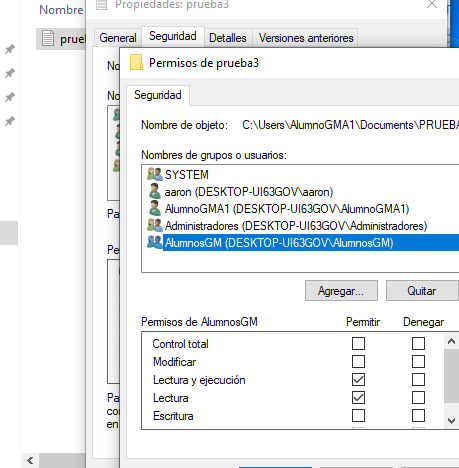


Observa que los permisos heredados están sombreados en gris.

Abre la ficha de *Seguridad* de prueba3.txt y agrega el grupo *AlumnosGMA* a su ACL. Ahora *AlumnosGMA* es el único elemento no heredado en la ACL de prueba3.txt. Observa que los permisos de *AlumnosGMA* no se encuentran sombreados en gris: esto es porque no son heredados. Comprueba que los permisos de los otros elementos de la ACL se encuentran sombreados en gris, como corresponde a permisos heredados. Dale a *AlumnosGMA* el permiso de control total.

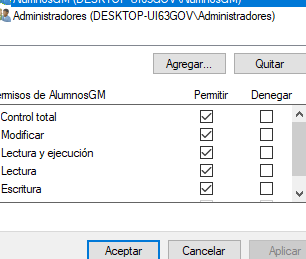
Añadimos **ALUMNOSGM** a archivo **PRUEBA3.TXT**.

En modo texto es con el comando **CACLS PRUEBA3.TXT /G ALUMNOSGM: R**



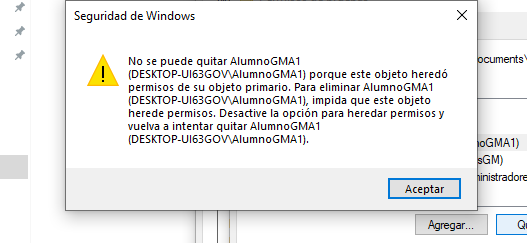
Damos todos los permisos a **ALUMNOSGM**, en el momento que lo cambiamos ya no salen sombreados en gris.

En modo texto seria con el comando **CACLS PRUEBA3.TXT /G ALUMNOSGM:F**, para tener un control total.



1. Intenta eliminar de la ACL de prueba3.txt algún elemento que no sea *AlumnosTC*. ¿Qué ocurre? ¿Por qué? Anótalo a continuación.

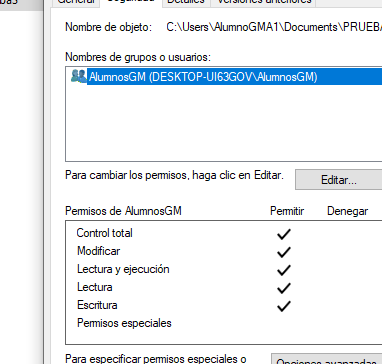
No se pueden quitar ningún elemento heredado de las **ACL** del archivo **PRUEBA3.TXT**.



Ahora veremos cómo se puede evitar que un objeto herede permisos de otro objeto primario.

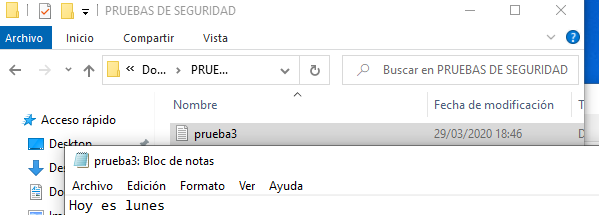
Abre la ficha Seguridad de prueba3.txt. Pulsa sobre Opciones avanzadas. Observa la opción Permitir que los permisos heredables del primario se propaguen a este objeto y a todos los objetos secundarios. En este momento debe encontrase activada. Precisamente por eso, prueba3.txt ha heredado los permisos de la carpeta Pruebas de seguridad. Desactiva esta opción. Se te plantean dos posibilidades: Copiar o Quitar. Elige Copiar. Mediante esta opción transformas los permisos heredados en permisos propios del objeto. Comprueba que dejan de estar sombreados en gris: esto es porque ya no son permisos heredados. Ahora borra de la ACL los elementos que acabas de copiar, o sea, todos salvo AlumnosGMA. Puedes hacerlo sin problema porque ahora, al no ser heredados, tienes control total sobre esos elementos. Cierra la hoja de propiedades del fichero.

Vemos que se ha eliminado, con las dos opciones anteriormente escritas.



1. ¿Tendrás a partir de este momento (recuerda que eres AlumnoGMA1) control sobre el fichero? ¿Por qué? Responde a continuación y comprueba tu respuesta.

Si, porque el **ALUMNOGMA1** está dentro del grupo **ALUMNOSGM**, entonces podremos tener control sobre el fichero.

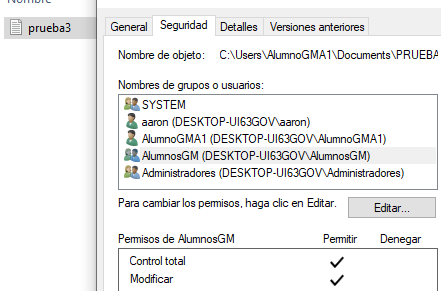


Abre de nuevo la ficha de *Seguridad* de prueba3.txt. Activa la opción *Permitir que los permisos heredables del primario se propaguen a este objeto y a todos los objetos secundarios*. De esta forma consigues que prueba3.txt vuelva a recuperar los permisos heredados.

Habilitamos la herencia de nuevo.

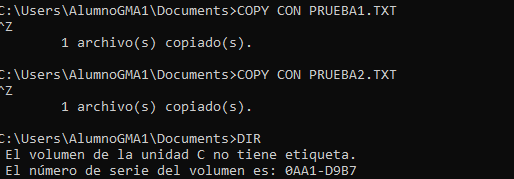


Y podemos comprobar que ha vuelto a la normalidad todos los permisos heredados.

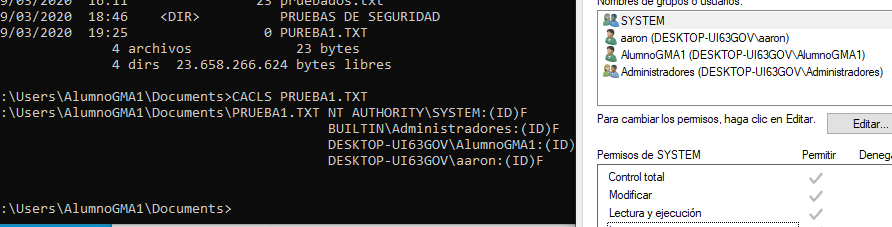


1. La ACL de ficheros y carpetas presenta un comportamiento diferente ante las operaciones *copiar* y *mover*. En este ejercicio se propone que realices un experimento para que observes dicha diferencia. Comprueba que eres *AlumnoGMA1*. Si no es así, comienza una nueva sesión utilizando este usuario. Crea, utilizando el *Bloc de notas*, los archivos prueba1.txt y prueba2.txt y almacénalos en la carpeta *Documentos (si existe alguno anterior, los eliminas antes)*. Comprueba que ambos ficheros tienen una ACL idéntica. Indica a continuación los miembros de sus ACLs:

Una vez que somos **ALUMNOGMA1**, entramos en el **CMD** y creamos los archivos de texto correspondientes en la carpeta DOCUMENTOS. Lo creamos con el comando **COPY CON PRUEBA1.TXT** y lo mismo con **PRUEBA2.TXT**.

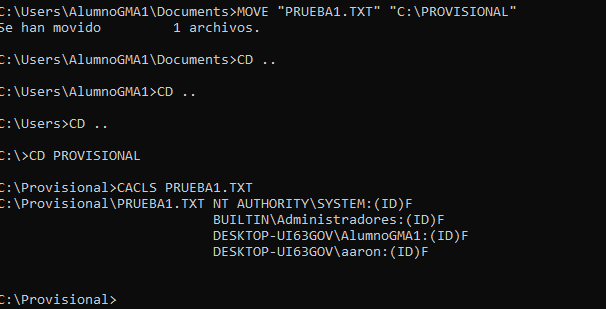


Comprobamos a continuación que los dos archivos tienen los mismos permisos, en el modo texto lo hacemos con el comando **CACLS PRUEBA1.TXT** y con el modo grafico accedemos a las propiedades y seguridad del archivo **PRUEBA2.TXT**, vemos que **ACL** son idénticas.

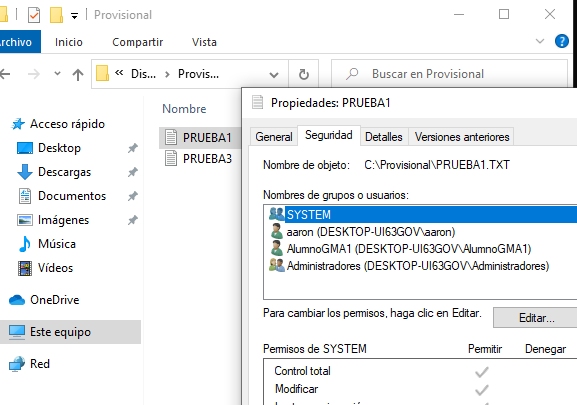


1. *Mueve prueba1.txt* a la carpeta *Provisional.* Observa su ACL e indica a continuación sus miembros:

Para mover un archivo utilizaremos el comando **MOVE “PRUEBA1.TXT” “C:\PROVISIONAL”,** para mover el archivo, después veremos sus **ACL** con el comando **CACLS PRUEBA1.TXT**.

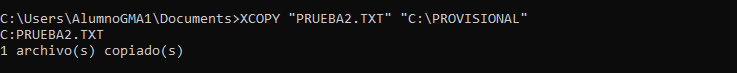


En modo grafico también lo podemos ver en propiedades y seguridad del archivo.

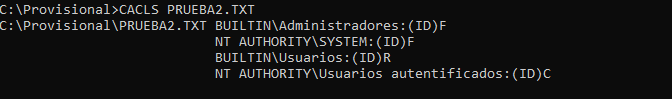


1. Ahora copia prueba2.txt a la carpeta *Provisional.* Observa su ACL y escribe a continuación sus miembros.

Primero copiamos el archivo con el comando **XCOPY “PRUEBA2.TXT” “C:\PROVISIONAL”**



Después vemos sus **ACL** con el comando **CACLS PRUEBA2.TXT**

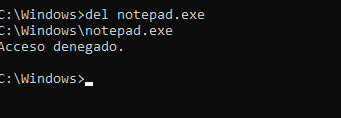


1. ¿Podrías explicar ahora la diferencia entre al comportamiento de mover y copiar?

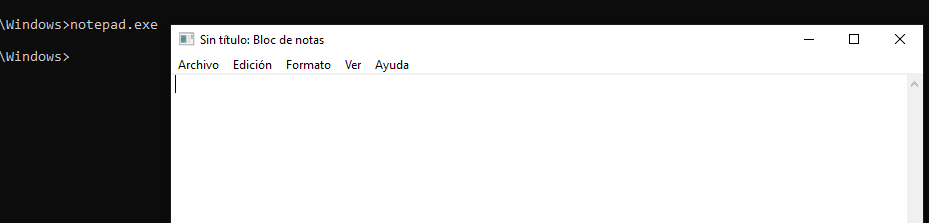
Es muy fácil de explicar y comprender, cuando movemos un archivo a otra carpeta las **ACL** de las mismas no se modifican, pero cuando copiamos el fichero pierde sus **ACL** y hereda las **ACL** de la nueva carpeta.

1. Busca en la unidad C: de tu sistema el fichero ejecutable correspondiente al Bloc de notas (notepad.exe). Intenta eliminarlo. Observarás que se te deniega el acceso. Sin embargo, comprueba que sí puedes ejecutarlo. Observa la ACL de este fichero. Ahora explica por qué puedes ejecutarlo, pero no borrarlo (recuerda que has iniciado la sesión como AlumnoGMA1):

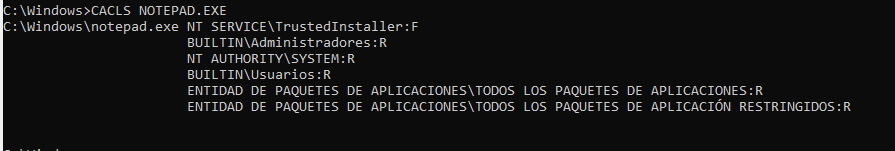
Primero tenemos que saber dónde se encuentra **NOTEPAD.EXE**, este se encuentra en la carpeta **WINDOWS**, vemos que no podemos eliminarlo.



Pero si podemos ejecutarlo.

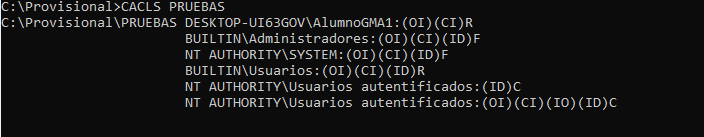


Podemos comprobar que no podemos eliminarla porque El grupo **USUARIOS** solo puede leer, y nosotros estamos en el grupo de **USUARIOS**, pero el **NT SERVIC**E si podría eliminarlo.



1. Crea dentro de la carpeta *Provisional* la carpeta *Pruebas*. Borra todas sus entradas de la ACL salvo *Administradores* y *AlumnoGMA1*. Se entiende que en este momento eres *AlumnoGMA1*. Da al usuario *AlumnoGMA1* todos los permisos salvo *Control total*. Ahora realiza los experimentos que consideres oportunos para observar las diferencias de comportamiento de esta carpeta cuando el permiso *Modificar* se encuentra activado o no. Indica a continuación las diferencias que has encontrado.

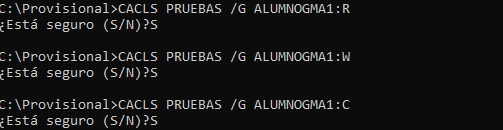
Lo primero que haremos, va ser crear la carpeta **PRUEBAS** y ver las **ACL** que tiene.



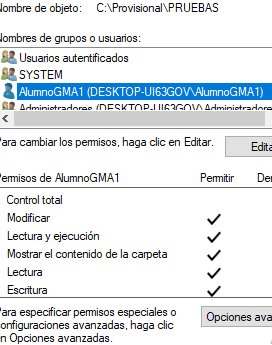
Después borramos todas sus **ACL** menos **ADMINSITRADORES** Y **ALUMNOGMA1**



Por último, le damos todos los permisos a **ALUMNOGMA1** menos el control total, con el comando **CACLS PRUEBAS /G ALUMNOGMA1: PERMISO**



Comprobamos en modo grafico que se ha configurado correctamente



Cuando el permiso **MODIFICAR** esta activo, podemos hacer cualquier operación con los ficheros, cuando **MODIFICAR** no está activo, podremos hacer de todo menos cambiar el nombre y borrarlos.