Unidad 6

Administración de acceso al dominio

Implantación de sistemas operativos

Índice

Introducción

En las unidades anteriores vimos cómo se gestionaban los principales objetos de un dominio, pero como sabíamos su función principal era la de poder dotar de recursos a los equipos que estén en la misma red, por lo que hay que gestionar el acceso a estos recursos del dominio.

Durante esta unidad hablaremos sobre los distintos permisos que se establecen en los recursos compartidos y como asignarlos.

Distinguiremos entre permisos y derechos y en los primeros distinguiremos los permisos de recursos de los permisos NTFS.

Además, como pequeña introducción para futuros temas se hablarán de las acreditaciones de los usuarios y sus directivas para controlar otros aspectos de seguridad.

Al finalizar esta unidad

- Seremos capaces de distinguir entre derechos y permisos de los usuarios.
- Sabremos la diferencia entre los permisos de los recursos compartidos y los permisos NTFS.
- Podremos compartir archivos y directorios.
- Estaremos preparados para compartir impresoras en la red.
- Sabremos como se configuran los permisos de los recursos compartidos.

6.1. Los permisos y los derechos

Los derechos o privilegios de los usuarios son atributos que afectan a una cuenta de usuario o a un grupo con la función de permitir realizar ciertas acciones sobre todo el sistema y no un solo recurso.

Por otra parte, los permisos son características propias de cada recurso en concreto (o conjuntos de recursos aglomerados en otro), en el que se dirá que usuarios o grupos pueden trabajar con estos recursos y que acciones pueden realizar sobre estos.

6.1.1. La acreditación de los usuarios

Cada vez que damos autorización a un usuario para que pueda conectarse a un sistema Windows, el propio sistema le construye una acreditación única que se llama **Security Access Token (SAT)**.

Esta es la identificación que realmente el sistema usa para saber quién está generando cada proceso en cada momento y así poder saber si tiene permitido realizar dicho proceso sobre dicho recurso concreto.

Dentro del SAT encontramos los siguientes atributos de protección:

- El SID que se usa para que el usuario esté identificado de manera única.
- La lista de los SID de cada uno de los grupos en los que está el usuario incluido.
- La lista de los derechos que tiene el usuario al completo ya sea por sí mismo o por los grupos a los que pertenece.

6.1.2. Los derechos de los usuarios

Como hemos mencionado anteriormente, los **derechos o privilegios** indican que acciones pueden o no realizar los usuarios que se encuentren iniciados en el sistema. Esta lista de derechos viene dada en el SAT, como se vio en el punto anterior.

En Windows existen principalmente dos tipos de derechos:

- **Derechos de conexión**, mediante los que se establecen las diferentes formas en las que un usuario puede acceder a un sistema. Destacan:
  - Denegar el acceso desde la red a este equipo. Si no está activo. Se permitirá que el usuario se pueda conectar con un equipo remoto a otro a través de la red.
  - Permitir el inicio de sesión local. Nos permite que se inicie sesión físicamente en el equipo en cuestión.
- **Los privilegios** (estos solo se pueden llamar así, no derechos también) mediante los cuales definimos el resto de las acciones que el usuario puede realizar dentro del sistema. Destacan (por ejemplo);
  - Añadir equipos a un dominio.
  - Realizar copias de seguridad del sistema de directorios.
  - Restaurar dichas copias de seguridad.
  - Cambiar la configuración del sistema.
  - Impedir la instalación de controladores de dispositivos.
  - Apagar el sistema.

Los derechos tienen prioridad sobre los permisos, es decir, si hay un conflicto, siempre se tendrán en cuenta los primeros.

6.1.3. Las directivas de seguridad

Los derechos en Windows se pueden agrupar en una serie de reglas a las que llamamos directivas de seguridad y donde definimos el comportamiento que tendrá el sistema dependiendo de la acción que se quiera o vaya a ejecutar.

Tenemos tres tipos principales:

- **Directiva de seguridad local.** Se usa para la modificación de las configuraciones de seguridad en equipos clientes propios o servidores donde no está instalado el directorio activo.
- **Directiva de seguridad de dominio.** Son las directivas que se pueden usar en Windows Server cuando tenemos un controlador de dominio instalado y queremos que se modifiquen las configuraciones de seguridad prestablecida para todos los miembros del dominio (también a algunos grupos en concreto).
- **Directiva de seguridad del controlador de dominio.** Es la directiva de seguridad que debemos usar cuando tenemos un controlador de dominio instalado y además queremos modificar la configuración de seguridad de varios controladores de dominio a la vez.

6.1.4. Los atributos de protección de los recursos

En todos los sistemas Windows con archivos NTFS, cada uno de los archivos o directorios que tenemos posee los siguientes atributos de protección:

- **El SID del propietario:** se trata el usuario que en primera instancia creó el archivo o carpeta, pero puede que se haya modificado esto en algún momento.
- **La lista de control de acceso de protección (ACL):** aquí incluiremos los permisos que se usan para regular que usuarios pueden acceder o no a los recursos del sistema y que acciones pueden hacer sobre estos. No hay un número definido de entradas en esta lista. Esta a su vez se divide en dos listas de manera real que se llaman:
  - Lista de Control de Acceso Discrecional (DACL). Cada uno de sus elementos se llaman **Entrada de control de Acceso (ACE)** y se usa para unir un SID de una cuenta con la adjudicación de una serie de permisos.
  - Un archivo tiene dos DACL en vez de una debido a que en los sistemas Windows existe la **herencia de permisos**, es decir, permisos que se han concedido en carpetas superiores y que por defecto se aplican a todo lo que cuelgue de estas. Entonces, en una DACL tendremos los permisos heredados y en otra los permisos explícitos del archivo.
- **La lista de control de acceso de seguridad (SACL):** aquí se nos indicarán que acciones debe de auditar o registrar el sistema en caso de se hagan. (sobre el archivo o carpeta).

NOTA

La herencia de las carpetas en Windows puede ser deshabilitada, aunque en muchas ocasiones no suele hacerse para que no se generen conflictos.

Por lo general, conforme nos vamos adentrando en el árbol de directorios los permisos van de más a menos restricción.

6.1.5. La asociación de los permisos a los recursos

Cuando vayamos a asignar permisos a los recursos compartidos, debemos de seguir una serie de reglas prestablecidas:

- Cuando creemos un nuevo objeto del directorio, no tendrá ningún permiso explícito y solo contará con los permisos heredados de la carpeta superior.
- Todos los usuarios que tengan poder total sobre el objeto en cuestión podrán modificar todos sus permisos. Este suele ser por defecto el propietario y el administrador.
- El control de la herencia de permisos se lleva a cabo en dos niveles:
  - Cada objeto del directorio puede heredar o no los permisos del directorio padre, pero defecto será que sí.
  - A la hora de definir los permisos explícitos, también se puede especificar que objetos los heredaran y cuáles no.
- Copiar archivos a una nueva ubicación es a efectos del sistema lo mismo que crear, por lo que de primeras tendrá los permisos heredados. Tenemos dos opciones de como contemplar este caso:
  - Si el movimiento entre directorios se produce dentro de un mismo volumen de almacenamiento, la herencia se desactiva y se mantienen los permisos explícitos que tenía.
  - Si se mueve a un volumen distinto, se adaptarán a los permisos heredados.

6.1.6. Los permisos NTFS estándar y especiales

En Windows distinguimos dos tipos de permisos NTFS:

- **Los permisos NTFS especiales.** Estos permisos controlan que acciones se pueden llevar a cabo sobre las carpetas y archivos.
- **Los permisos NTFS estándar.** Son combinaciones de permisos NTFS especiales que vienen predefinidos en el sistema.

Estos permisos predefinidos son necesarios para que cuando el administrador comience con la administración de nuestro sistema tenga más facilidad, pero por lo general después sufrirá cambios y se optará por los permisos NTFS especiales.

Cuando se cambian los permisos de las carpetas o archivos en Windows debemos de seguir en la medida de lo posible una serie de reglas:

- Debemos tener en cuenta que a veces, un único proceso puede que conlleve ejecutar acciones sobre distintas carpetas o archivos. Esto quiere decir, que, si ese proceso necesita de permisos específicos en esas carpetas o archivos, debe de tenerlos concedidos, en caso contrario tendremos un error de ejecución genérico por falta de permisos.
- Los permisos de Windows son acumulativos, es decir, un usuario puede ejecutar todos los permisos que tenga disponibles como cuenta de usuario, pero también todos los que tengan los grupos a los que pertenezca.
- No es necesario que haya una denegación de permisos (que también se puede hacer), porque su ausencia ya implica que no se pueden ejecutar esas acciones.
- Si sí que se han denegado permisos, pero a la vez también tenemos activados los mismos, estamos en la tesitura de un conflicto de permisos. En este caso siempre priman los permisos de denegación o negativos. Esto es parecido a lo que pasaba con los permisos explícitos y heredados.

6.1.7. Los permisos de los recursos compartidos

Los permisos que se establecen para un recurso compartido solo tienen validez para los usuarios que acceden a través de la red. En caso de que también se le quiera aportar seguridad de manera local habrá que establecer los permisos anteriormente dichos.

Como pasaba de manera local, los permisos de un recurso compartido tienen una cierta herencia y por lo tanto se aplican a todos los permisos que haya en la red, de manera que, cuando se tenga acceso a un recurso compartido, se tendrá además a las carpetas y archivos que se contienen.

Para controlar el acceso a los recursos compartidos en red, se usan principalmente tres métodos:

- Usar los permisos de recursos compartidos, estos son relativamente sencillos de aplicar y administrar.
- Usar los permisos NTFS que tienen algo más de control sobre los recursos compartidos.
- Usar una combinación de los dos, que suele ser la opción más recomendada.

Si por lo que sea, se usa una combinación de permisos de recursos y NTFS, siempre primará el permiso más restrictivo.

6.2. La compartición de directorios

De manera automática, cuando instalamos Windows Server, se crean dos directorios en la raíz del sistema que se usarán como recurso compartido. Estos directorios son:

- C:\Windows\SYSVOL\SYSVOL
- C:\Windows\SYSVOL\sysvol\nombre_dominio\scripts

Imagen 1. Directorio SYSVOL.

Dentro de C:\Windows\SYSVOL, tenemos 4 directorios, pero debemos de fijarnos en el último, el cual se comparte. Además, dentro de este tenemos el directorio que nos redirige al dominio y dentro del último, otras dos carpetas, Policies y Scripts.

Imagen 2. Directorio universae.lan.

La carpeta de scripts cambiará su nombre y a la hora de ser un recurso compartido su nuevo nombre será **NETLOGON**.

Para poder ver la administración de los recursos compartidos de Windows hacemos lo siguiente:

1. En el centro de administración, nos vamos a la esquina superior derecha, a Herramientas.
2. Una vez aquí, si desplegamos y vemos todas las opciones, elegimos la segunda, Administración de equipos.

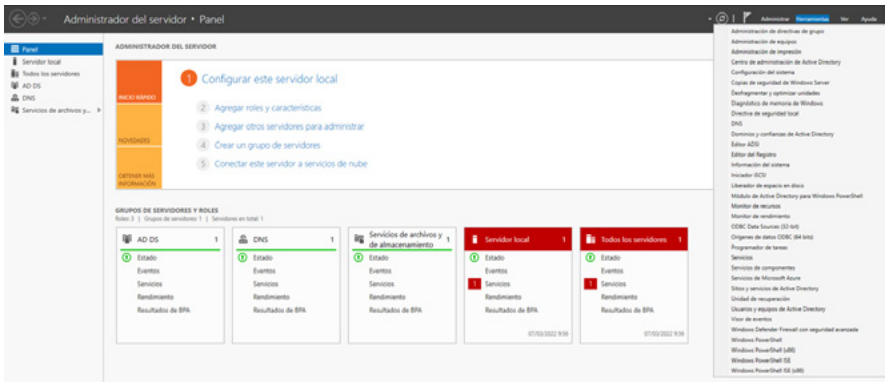

Imagen 3. Administrador del servidor.

3. Se nos despliega el Administrador de equipos disponible, donde vemos que a la izquierda tenemos numerosas opciones, pero tenemos que seguir la siguiente:

   » Herramientas del sistema → Carpetas compartidas → Recursos compartidos

   » Entonces ahora veremos que se nos muestran todos los recursos compartidos y una serie de atributos que se muestran, como en la imagen siguiente:

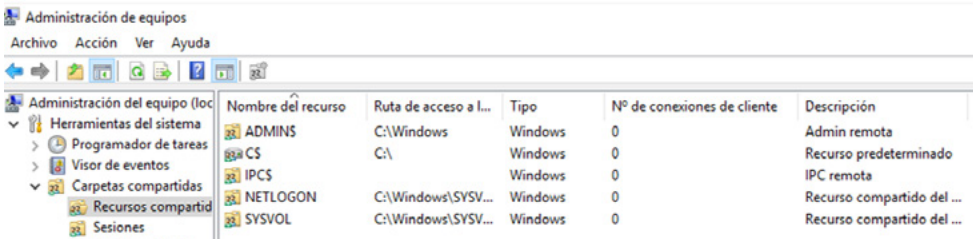

Imagen 4. Administrador de equipos.

NOTA

Podemos ver en la imagen anterior, que el directorio C:\Windows y C: también están compartidos como recurso, pero con nombres distintos. Estos recursos están compartidos para pura administración remota, por eso no se habla de ellos en profundidad.

6.2.1. Como compartir un directorio

Para compartir un directorio tenemos dos maneras de cómo actuar:

- Compartir el directorio desde las propiedades de la carpeta.
- Compartir el directorio desde Administración de equipos.

Para compartir un directorio desde las propiedades de la carpeta debemos:

1. Lo primero que haremos será crear la carpeta en cuestión:

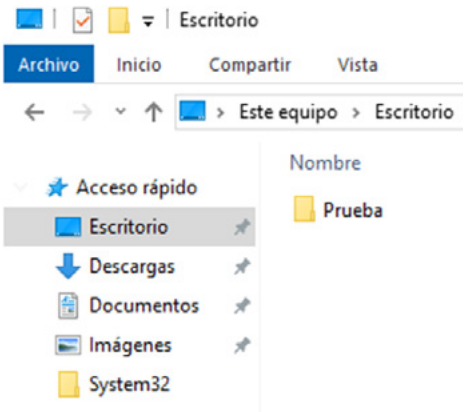

Imagen 5. Compartir directorios 1.

2. Cuando esté creado, hacemos clic derecho sobre la carpeta y seleccionamos Propiedades.

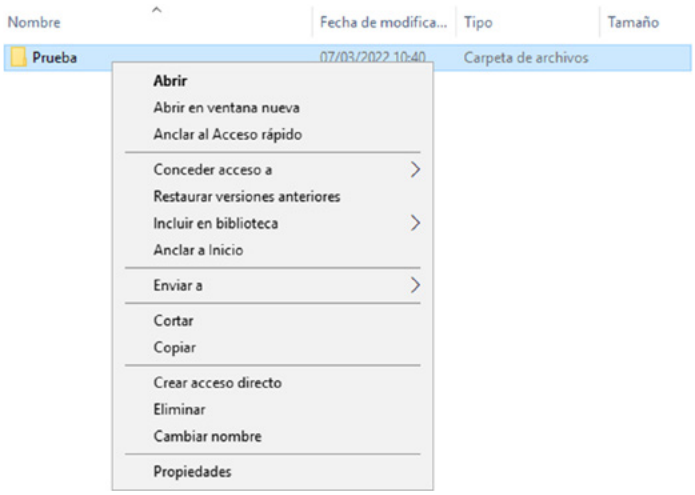

Imagen 6. Compartir directorios 2.

3. Dentro de las propiedades, nos dirigimos a la pestaña Compartir.

4. Una vez aquí elegiremos la opción Uso compartido de carpetas y archivos de red → Compartir.

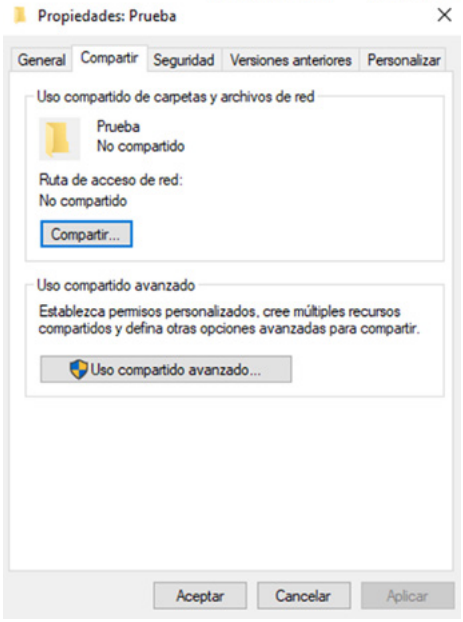

Imagen 7. Compartir directorios 3.

5. Nos aparecerá entonces un cuadro de diálogo donde nos dirá que seleccionemos que usuarios tienen acceso a esta carpeta, en nuestro caso hemos seleccionado a Alumno1.

6. Una vez elegidos los usuarios, en la parte derecha se pueden editar los permisos del usuario.

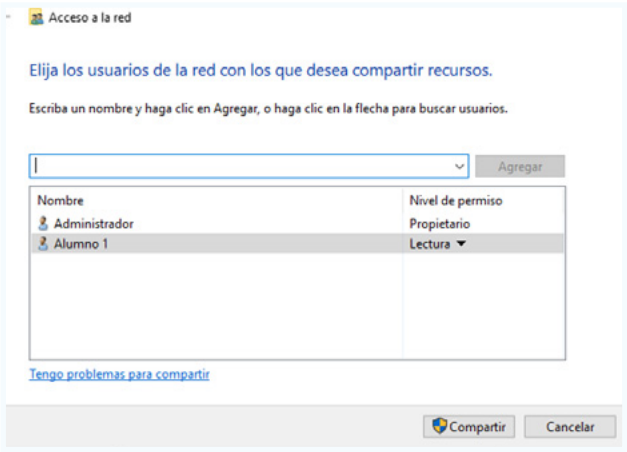

Imagen 8. Compartir directorios 4.

7. Acto seguido el sistema nos avisará de que la carpeta ha sido creada y su nombre y ruta de acceso.

8. Si estamos de acuerdo seleccionamos Listo.

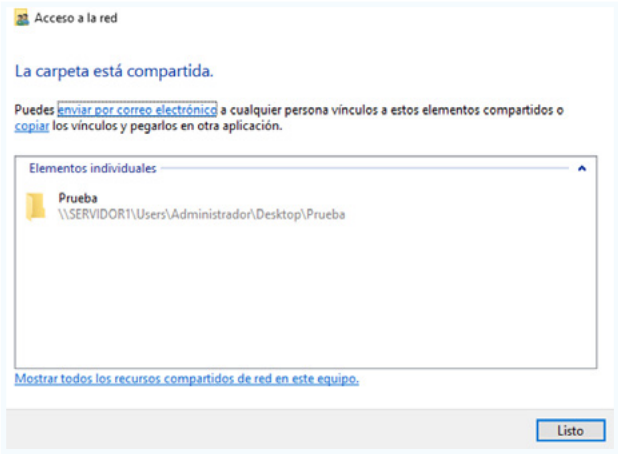

Imagen 9. Compartir directorios 5.

9. Si volvemos ahora las propiedades, veremos que ya aparece la carpeta como compartida y su ruta de acceso.

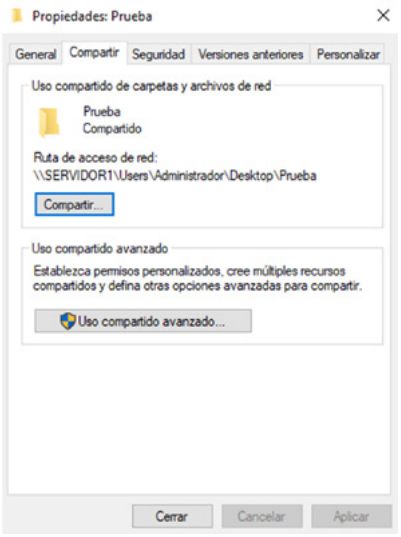

Imagen 10. Compartir directorios 6.

10. Por último, si en vez de seleccionar la primera opción, hubiésemos seleccionado la segunda, nos saldría una ventana como la de más abajo, pero esta opción es parecida a la que vamos a hacer a continuación, por lo que no se va a hacer en este apartado.

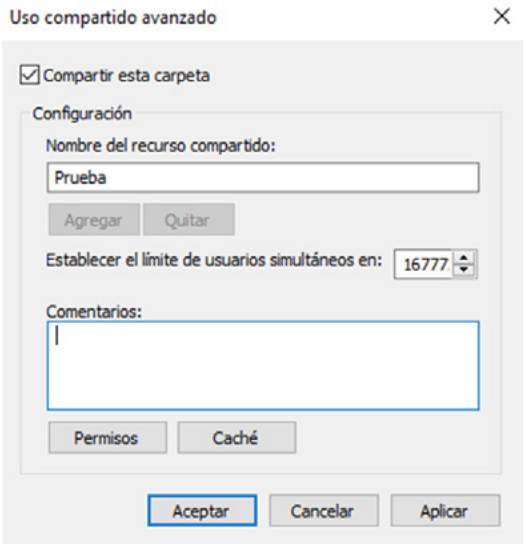

Imagen 11. Compartir directorios 7.

11. Si nos dirigimos ahora a un equipo cliente y seleccionamos la pestaña Red del explorador de archivos, nos aparecerán las máquinas visibles, pero no el recurso compartido, por lo que habrá que buscarlo.

12. En la ruta de las carpetas escribimos nosotros:

```
\\SERVIDOR1
```

13. Se nos mostrarán los recursos que ya dijimos se compartían de manera automática.

Imagen 12. Compartir directorios 8.

14. Si ahora escribimos la ruta completa que se nos planteaba antes, vemos que se ha compartido correctamente dicho recurso.

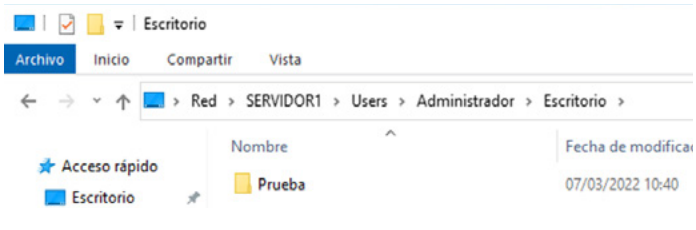

Imagen 13. Compartir directorios 9.

IMPORTANTE

Aunque no se hayan compartido los directorios padres del recurso creado, estos se crean de manera automática y se comparten para poder llegar hasta el recurso deseado.

NOTA

Para poder realizar esta tarea es necesario que el usuario tenga el permiso requerido o sea administrador del sistema.

Para realizar esta operación, desde el administrador de equipos, hacemos lo siguiente:

1. Creamos la carpeta que queremos compartir como recurso.
2. Abrimos Administración de equipos.
3. En Recursos compartidos, hacemos clic derecho y seleccionamos Recurso compartido nuevo...

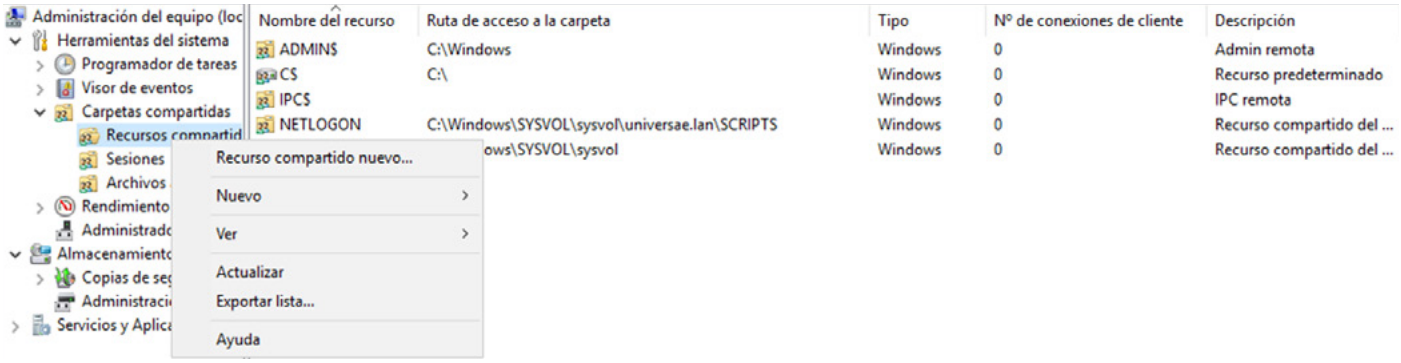

Imagen 14. Compartir directorios v2 1.

4. En el cuadro que se nos abre, nos pide la ruta de la carpeta que se quiere compartir, ya sea poniéndola nosotros o buscando en el equipo.
5. Seleccionamos, por lo general, la opción Examinar y hacemos la búsqueda de la carpeta moviéndonos entre directorios.
6. Seleccionamos la carpeta y damos al siguiente paso.

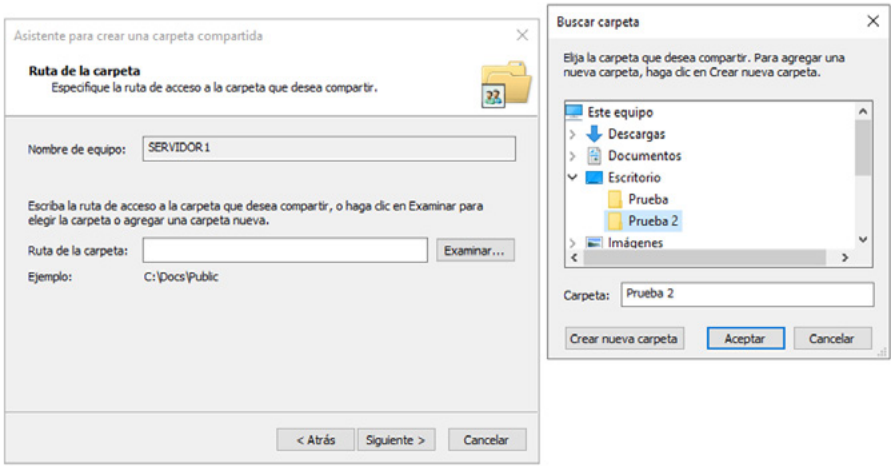

Imagen 15. Compartir directorios v2 2.

7. Una vez que se ha seleccionado la carpeta, nos aparecerá un cuadro en el que pide varios datos que se pueden modificar, nosotros los dejamos por defecto.

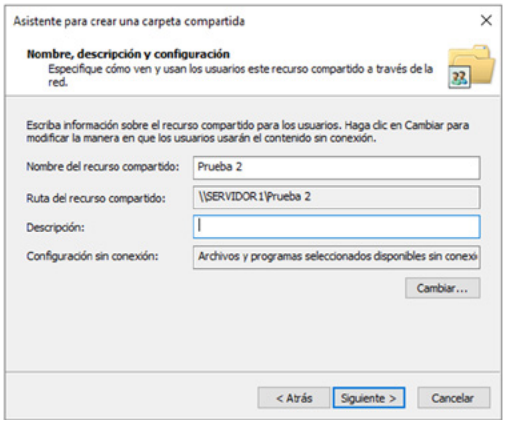

Imagen 16. Compartir directorios v2 3.

8. Nos piden ahora que definamos cuales son en principio los permisos que tendrá este recurso, nosotros lo dejamos solo para administradores.

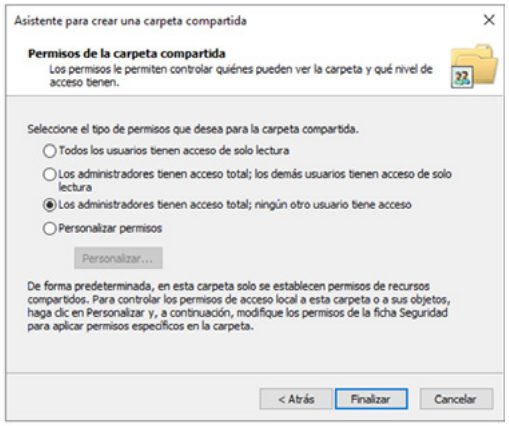

Imagen 17. Compartir directorios v2 4.

NOTA

Podemos ver que el recurso compartido creado en la primera instancia no se ha añadido a los recursos del sistema en Administración de equipos, esto es porque se ha creado desde la carpeta, pero su funcionamiento es el mismo.

Por otro lado, el segundo que hemos creado si se verá reflejado en las propiedades de la carpeta.

9. Una vez que se ha creado el recurso, podemos ver que aparece en la lista de recursos compartidos,

Nombre del recurso	Ruta de acceso a la carpeta	Tipo	Nº de conexiones de cliente	Descripción
ADMIN$	C:\Windows	Windows	0	Admin remota
C$	C:\	Windows	0	Recurso predeterminado
IPC$		Windows	0	IPC remota
NETLOGON	C:\Windows\SYSVOL\sysvol\universae.lan\SCRIPTS	Windows	0	Recurso compartido del ...
Prueba 2	C:\Users\Administrador\Desktop\Prueba 2	Windows	0	
SYSVOL	C:\Windows\SYSVOL\sysvol	Windows	0	Recurso compartido del ...
Users	C:\Users	Windows	0	

Imagen 18. Compartir directorios v2 5.

Las capturas o imágenes que no se muestran, pero cuando realicemos el proceso se verán, se dejan por defecto*

Para poder realizar esta acción es necesario ser administrador del sistema.

6.2.2. Como conectar los recursos compartidos como unidad de red

Hay ocasiones en las que tener que conectarnos a los recursos compartidos escribiendo toda la ruta puede resultar tedioso, sobre todo en las ocasiones en las que la ruta es muy larga.

Para poder facilitar esto, se puede conectar como una unidad de red la ubicación de un recurso compartido, y trabajar con ellas como una ubicación más de nuestro equipo.

Para poder realizar esta acción, seguimos el siguiente proceso:

1. En el equipo cliente nos vamos al explorador de archivos.
2. En Este equipo, en la parte superior desplegamos equipo.
3. Ahora seleccionamos la opción Conectar a una unidad de red.

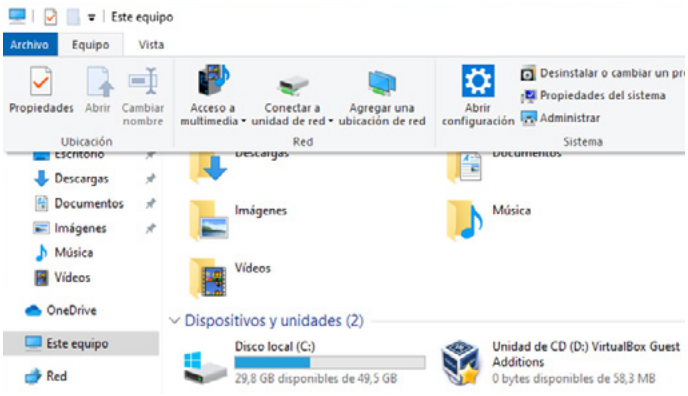

Imagen 19. Conectar unidades de red 1.

4. En la siguiente imagen vemos como nos pide que digamos que letra asignamos, y que ruta queremos seleccionar.
5. Al igual que hicimos antes, si damos a Examinar, podremos llegar.
6. Seleccionamos Finalizar y ya estaría listo.

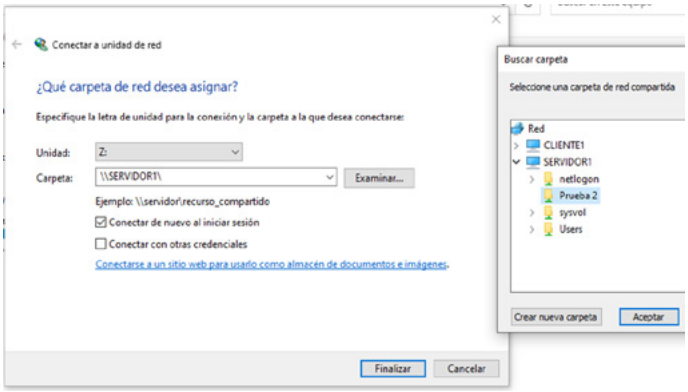

Imagen 20. Conectar unidades de red 2.

7. Si volvemos a mostrar el explorador, vemos la ruta en cuestión.

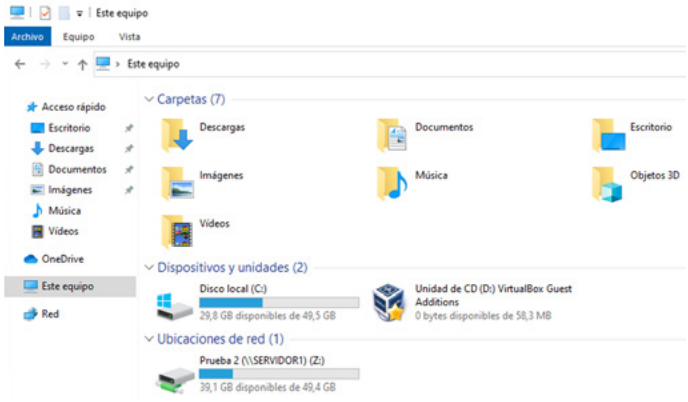

Imagen 21. Conectar unidades de red 3.

IMPORTANTE

Se podrá llegar a la ruta deseada a través de la opción Examinar siempre y cuando sea una unidad de red creada con el administrador de equipos. Si ha sido desde las carpetas directamente, no nos aparece inmediatamente y puede que tengamos que escribir la ruta a mano.

6.3. Los permisos de las carpetas compartidas

Los permisos de las carpetas compartidas se aplican a todos los directorios y subdirectorios del recurso compartido y regulan las acciones que se pueden ejecutar sobre los archivos al mismo tiempo que limitar el número de conexiones de usuarios que puede haber.

Siempre que queramos editar estos permisos, la única condición para poder hacerlo es pertenecer al grupo de Administradores del sistema.

En las últimas versiones se ha incorporado una serie de privilegios de grupo que permitirían que otros grupos también tengan la capacidad de editar permisos, aún así, no es lo recomendable.

Los permisos que se pueden dar en las carpetas compartidas:

- **Leer.** Se pueden ver los nombres que tienen los archivos y los directorios que se comprenden en el recurso. También se pueden ejecutar programas y leer el contenido de los archivos, pero no crear nuevos o modificar su contenido.
- **Modificar.** Se continúa teniendo todo lo que se tenía en Leer y, además, se pueden crear nuevos archivos y directorios y modificar su contenido.
- **Control total.** Se tienen todos los permisos sobre los archivos y directorios, pero además se puede modificar los permisos que tienen estos. Es recomendable que solo lo tengan los administradores.

6.3.1. Como establecer los permisos de las carpetas compartidas

Vamos a ver ahora como establecer los permisos de un recurso compartido.

1. Abrimos Administración de equipos.
2. Una vez aquí, nos movemos hasta Recursos compartidos y seleccionamos el recurso del cual queremos editar los permisos.
3. Accedemos a sus propiedades.

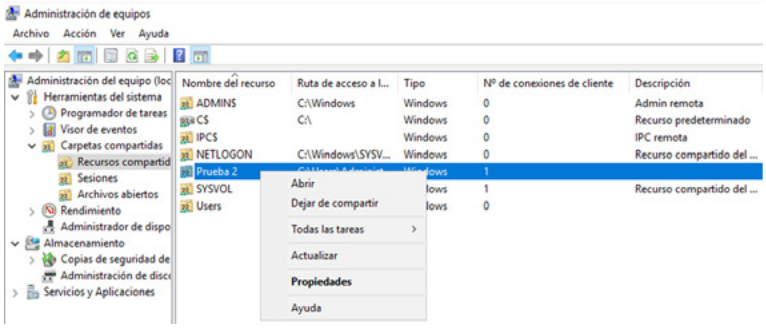

Imagen 22. Permisos de carpetas 1.

4. En la primera pestaña, General, se puede limitar el número de usuarios que pueden acceder al recurso.

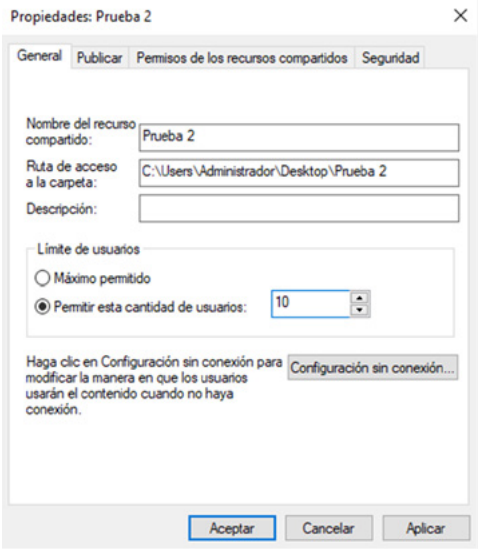

Imagen 23. Permisos de carpetas 2.

5. La siguiente pestaña, Publicar, nos indica si queremos que el recurso se comparta o no en Active Directory. Realmente esta acción hace que podamos desde el mismo AD cerrar los archivos de la carpeta, ver quien lo tiene abierto, etc.

Imagen 24. Permisos de carpetas 3.

6. La pestaña que nos interesa es la siguiente, Permisos de los recursos compartidos, donde nos aparecen los usuarios que tienen permisos y que tipo de permisos tienen.

7. Seleccionamos Agregar y elegimos que usuarios queremos que accedan al recurso.

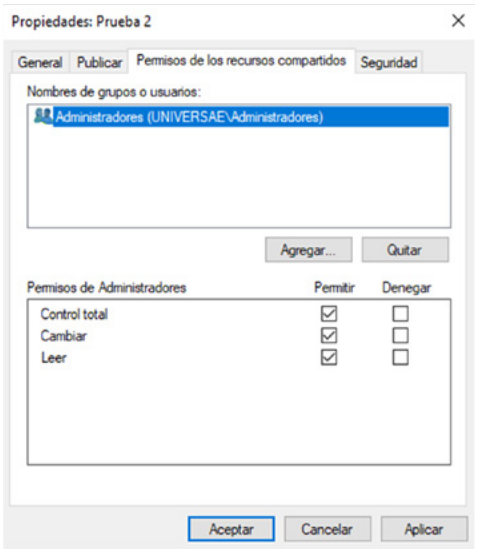

Imagen 25. Permisos de carpetas 4.

8. Una vez que ya hemos seleccionado el usuario, le concedemos los permisos que queremos que tenga.

9. Seleccionamos Aplicar para que se ejecuten los cambios y posteriormente Aceptar para guardar el resultado.

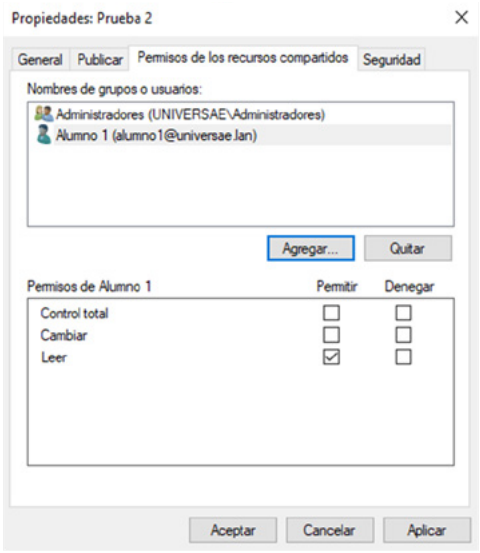

Imagen 26. Permisos de carpetas 5.

IMPORTANTE

Aunque estos permisos ya están establecidos, para poder acceder al recurso también deberá tener permisos NTFS el usuario en cuestión. Estos se manejan desde Seguridad y los veremos más adelante, que será cuando hagamos la comprobación de los permisos del usuario.

6.3.2. Los recursos compartidos especiales

Como hemos visto al principio del tema, hay una serie de recursos compartidos que se han creado automáticamente sin que nosotros realicemos ninguna acción, estos son:

- **ADMIN$.** Este recurso se usa para la administración remota del equipo y se ubica en la raíz del sistema. Su ubicación suele ser **C:\Windows**.
- **C$.** Se trata del recurso que comparte todo el disco, no suele estar disponible y también se usan para tareas de administración, su ubicación es **C:**.
- **IPC$.** Se trata del recurso predeterminado que comparte las canalizaciones connombre esenciales para la comunicación entre programas. No se suele usar mucho.
- **NETLOGON.** Ya vimos anteriormente su ubicación, aquí se almacena el servicio de Inicio de sesión para los controladores de dominio.
- **SYSVOL.** Se vio anteriormente su ubicación. Su función es la misma que la de **NETLOGON**.
- **Users.** Para tareas de administración, se componen de las carpetas de los usuarios del servidor donde se encuentra el directorio activo. Su ubicación es **C:\Users**.

6.4. Los permisos NTFS

Al principio del tema ya hicimos una pequeña introducción sobre lo que eran los permisos NTFS en sistemas Windows, pero ahora vamos a verlos en más profundidad.

Como recordaremos, estos permisos se basaban en la **herencia** de permisos para aplicar los mismos a todos los archivos y directorios que comprendiese el editado. Para realizar cambios en los permisos heredados, tenemos tres modos:

- Realizar cambios en la carpeta principal para que se cambien los heredados,
- Seleccionar la denegación de los permisos heredados en los archivos que así deseemos.
- Usar permisos explícitos que se contrapongan a los heredados.
- Deshabilitar la herencia. Para eso debemos de hacer lo siguiente:

1. Lo primero es abrir de nuevo las propiedades del recurso.
2. Ahora en la pestaña Seguridad, seleccionamos Opciones avanzadas.

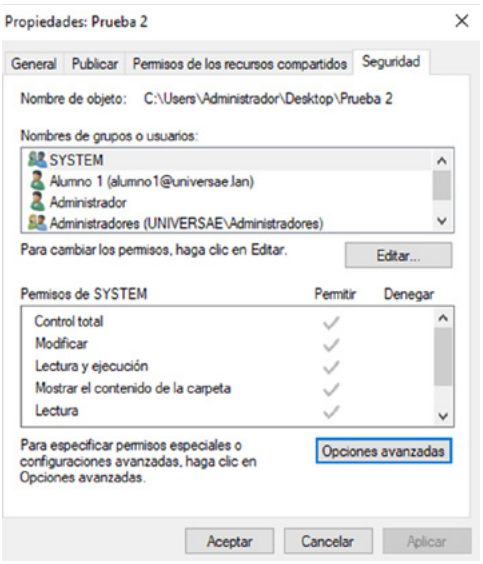

Imagen 27. Propiedades de seguridad.

3. Una vez que lo hemos seleccionado, nos aparecerá una ventana para editar de manera más avanzada ciertos permisos.
4. Seleccionamos la opción Deshabilitar herencia y se nos dirá que queremos que hagamos con los permisos. Elegiremos opción dependiendo de cual nos interesa más.
5. Aplicamos y registramos los cambios.

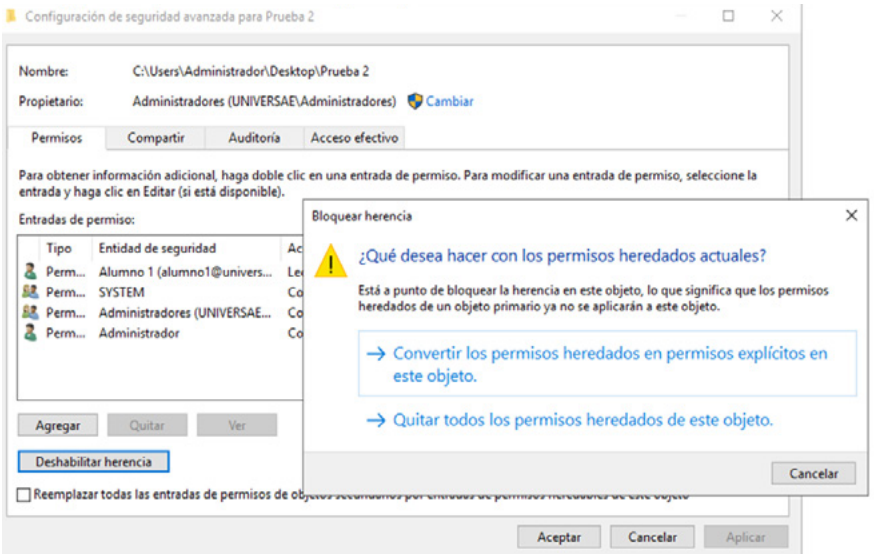

Imagen 28. Deshabilitar la herencia.

Los permisos NTFS que tenemos par poder trabajar con usuarios son:

- **Control total.** Funciona igual que en los permisos de recursos compartidos.
- **Modificar.** Funciona igual que en los permisos de recursos compartidos. Además, puede modificar los permisos.
- **Lectura y ejecución.** Es lo correspondiente a Leer de los permisos de recursos compartidos.
- **Mostrar el contenido de la carpeta.** Solo nos deja ver que tenemos en las carpetas, pero no abrir el contenido, porque para poder atravesar directorios es necesario el permiso de ejecución. En algunas versiones se llama también Listar.
- **Lectura.** Nos permite ver el contenido de algunos archivos, pero no atravesar directorios, para lo que serán necesarios los dos anteriores.
- **Escritura.** Permite realizar cambios en los archivos y directorios, pero no puede modificar permisos.
- **Permisos especiales.** Permisos que gestionan otros atributos y que veremos a continuación.

6.4.1. Como establecer los permisos NTFS estándar

La manera de cambiar los permisos NTFS de una carpeta es un proceso bastante sencillo. Se describe a continuación:

1. Abrimos las propiedades del recurso desde el servidor, ya sea en el administrador de equipos o desde el explorador de archivos.
2. Nos dirigimos a la pestaña Seguridad, y aquí seleccionamos en Editar.

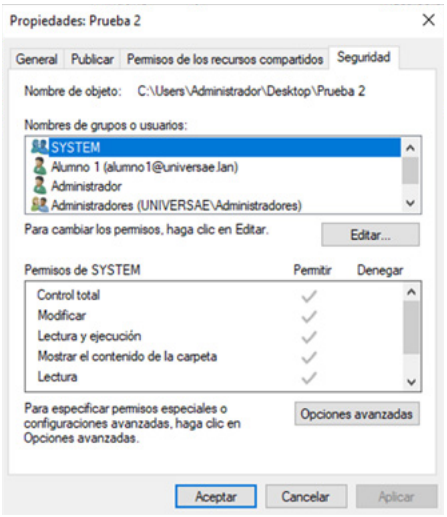

Imagen 29. Permisos NTFS estándar 1.

3. Una vez abierta la siguiente ventana, se nos da la opción de agregar o quitar un usuario de los permisos y de editar los que tenga. Seleccionamos Agregar.
4. Si ya hemos añadido al usuario, entonces editamos los permisos que creamos necesarios para que el usuario realice su trabajo.
5. Aplicamos y guardamos los cambios.

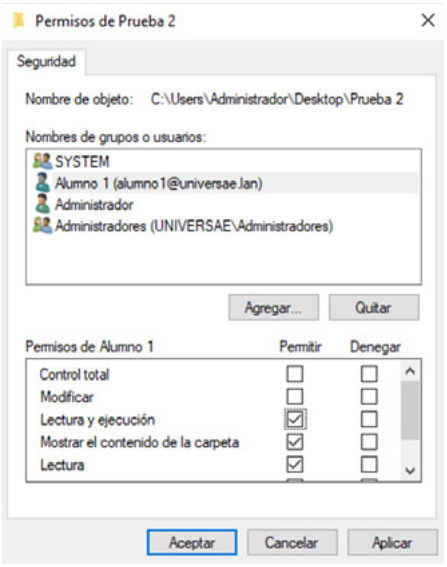

Imagen 30. Permisos NTFS estándar 2.

6. Ahora si podemos ir a nuestro cliente y probar.
7. Vemos que nos deja acceder a la carpeta, pero si intentamos crear una carpeta nueva no nos es posible.

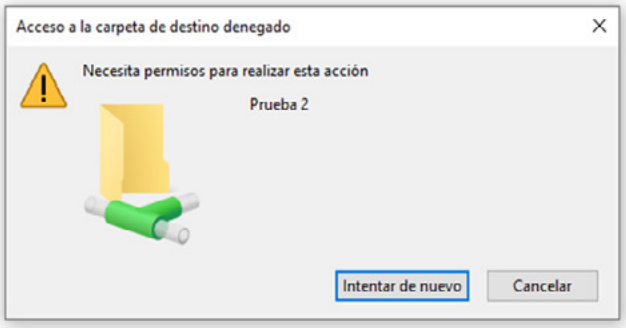

Imagen 31. Permisos NTFS estándar 3.

6.4.2. Como establecer los permisos NTFS especiales

Los permisos especiales NTFS de un recurso compartido son una serie de permisos muy específicos que se ejecutan desde las opciones avanzadas de seguridad.

Estos permisos no se usan muy comúnmente y solo debe de editarlos un administrador experto, por lo que simplemente se verá aquí una pequeña introducción de cuales son.

Pestaña Permisos

- En esta pestaña se editan los permisos que ya teníamos antes, pero además se puede cambiar el nivel de herencia que queremos que tengan estos permisos.

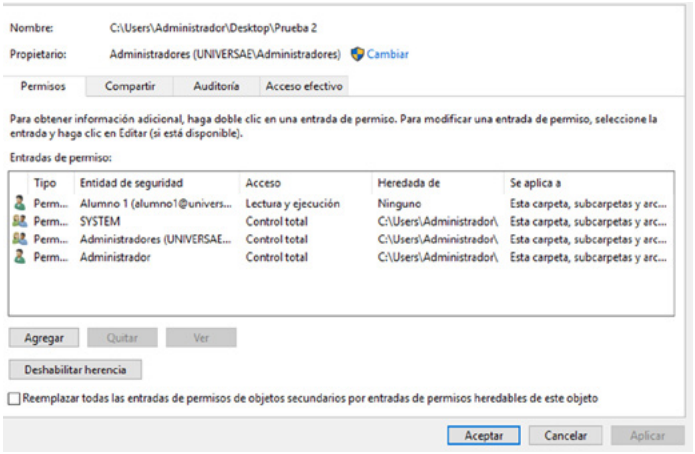

Imagen 32. Pestaña permisos.

Pestaña Compartir

- Son los permisos que administran el recurso compartido, ya los vimos anteriormente.

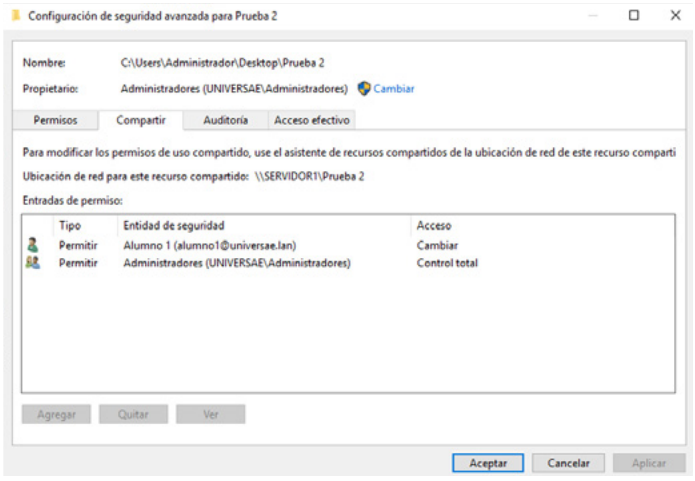

Imagen 33. Pestaña Compartir.

Pestaña Auditoría

> En esta pestaña se puede editar que usuarios están auditados, es decir, que usuarios tendrán un registro exhaustivo de su actividad en cuanto a permisos se refiere.

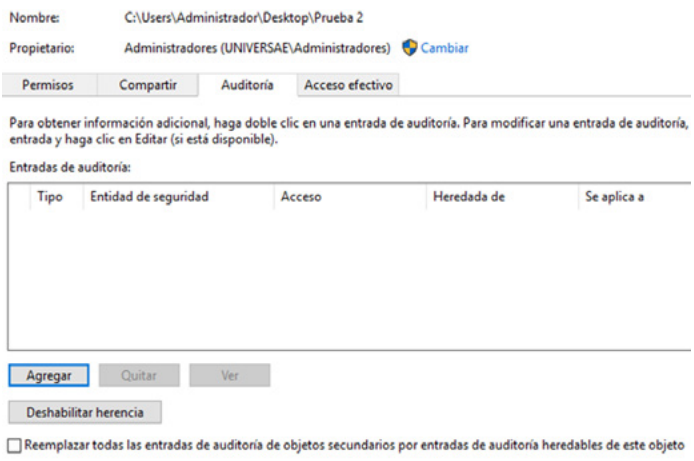

Imagen 34. Pestaña Auditoría.

Pestaña Acceso efectivo

> La última de las pestañas, el acceso efectivo nos permite que sepamos que permisos son efectivos para las cuentas con acceso a los recursos, es decir, cuales tiene realmente efecto y cuales no sobre los recursos editados.

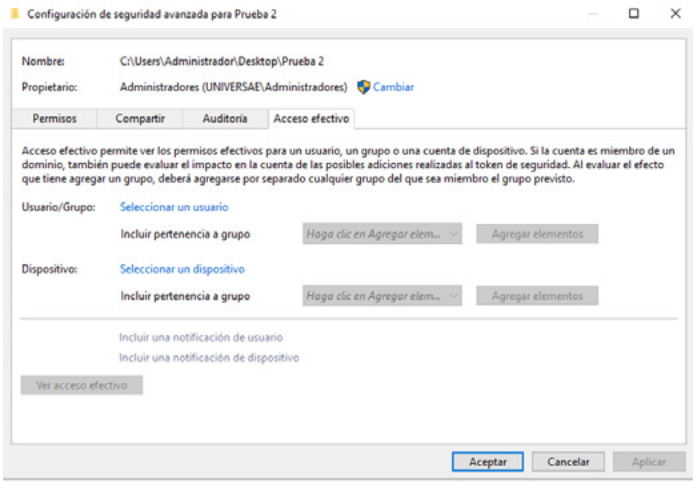

Imagen 35. Pestaña acceso efectivo.

6.4.3. El propietario de un directorio o un archivo

Cada vez que un usuario crea un objeto en el sistema de archivos, de manera automática se convierte en su propietario.

Ser el propietario de un objeto quiere decir que se tiene control total sobre este y sus permisos. Lo único que no puede hacer sobre el objeto es cambiarse a sí mismo como propietario por otro, pero esto se puede solucionar con el permiso de **Toma de posesión**.

Como establecer el permiso de toma de posesión

Para otorgar el permiso de toma de posesión debemos de realizar lo siguiente:

1. Lo primero es acceder a las opciones avanzadas de los permisos del recurso.
2. Una vez aquí seleccionamos al usuario que queremos editar sus permisos

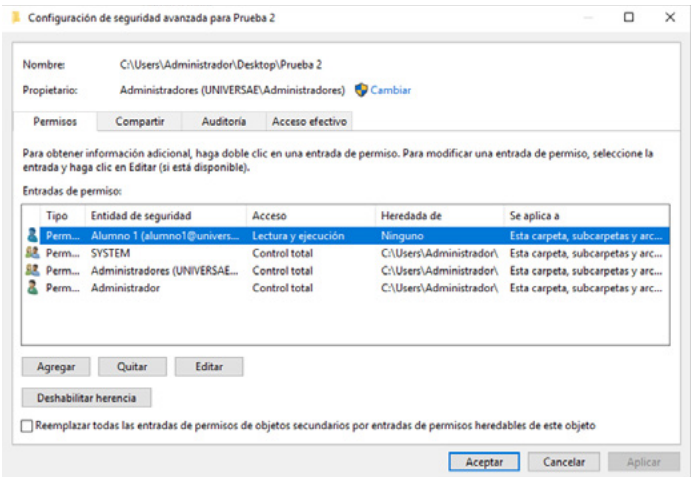

Imagen 36. Toma de posesión 1.

3. Una vez aquí, se nos muestran los permisos que ya sabemos que se pueden editar, pero a la izquierda tenemos la opción Mostrar permisos avanzados. Seleccionamos esta opción.

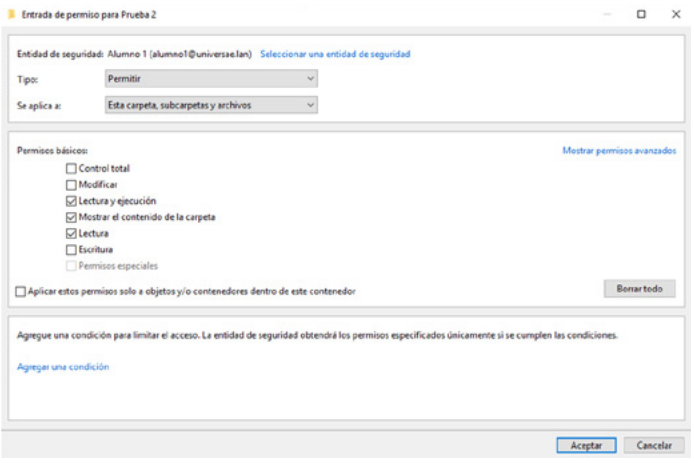

Imagen 37. Toma de posesión 2.

4. Cuando se nos muestren todos los permisos, tendremos que seleccionar el siguiente: **Tomar posesión**.

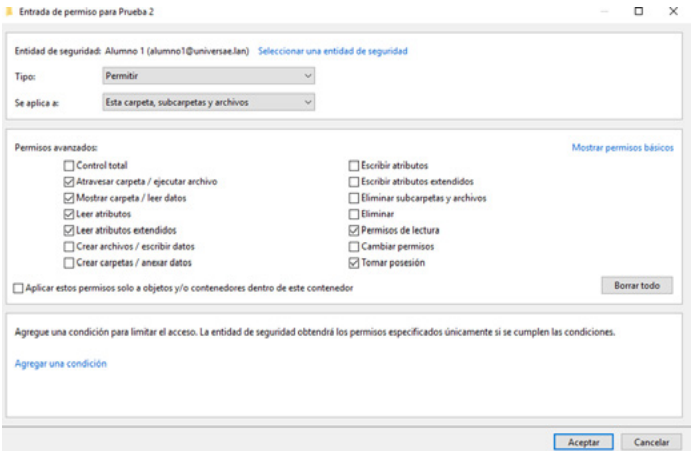

Imagen 38. Toma de posesión 3.

5. Aplicamos y guardamos.

6. Podemos ver ahora, que se han marcado los permisos especiales como permitidos.

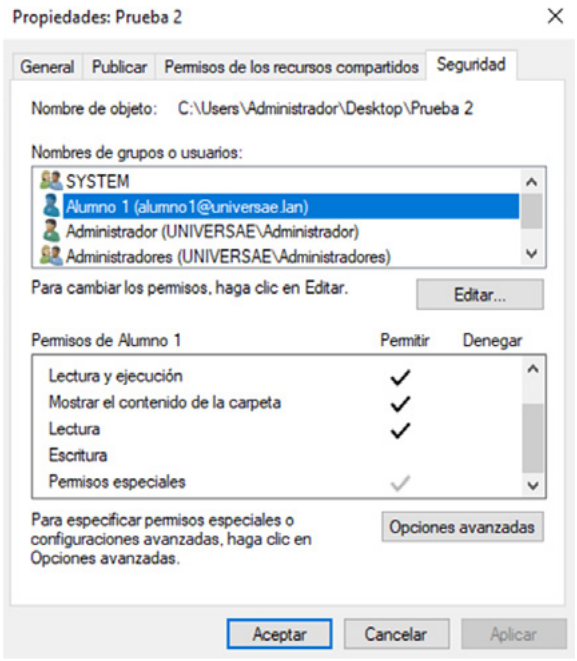

Imagen 39. Toma de posesión 4.

www.universae.com