Ampliación: Permisos y drechos de usuario

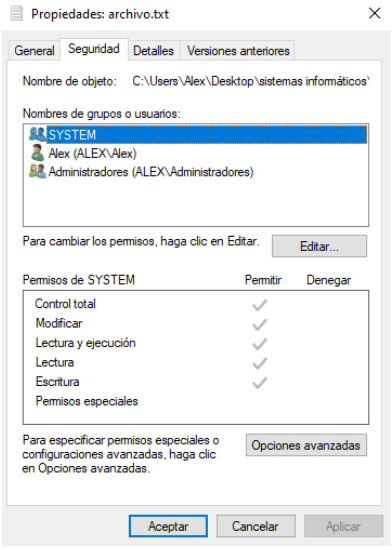
Sistemas Informáticos

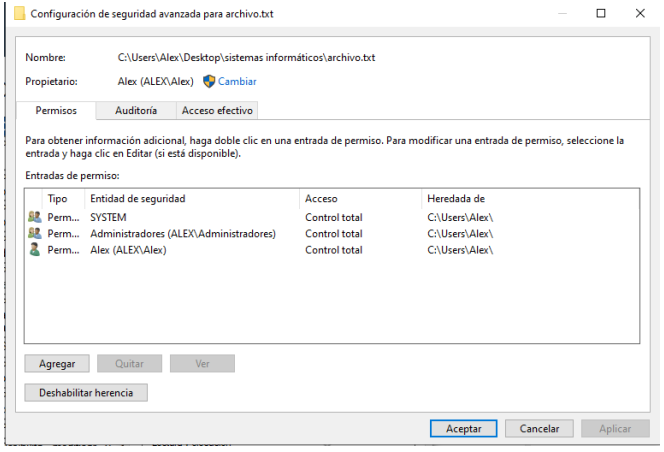
Permisos

permisos básicos

Tipos	Permisos	Descripción
Permisos en carpetas	Mostrar el contenido de la carpeta	Posibilita listar el contenidos de la carpeta
	Lectura	Permite ver el contenido de la carpeta, permisos, propietario y atributos
	Escritura	Posibilita crear nuevos archivos y subcarpetas, ver el propietario, modificar atributos y permisos
	Lectura y ejecución	Permite navegar por las subcarpetas más los permisos de lectura y mostrar el contenido
	Modificar	Posibilita eliminar la carpeta más los permisos de lectura y ejecución
	Control Total	Permite cambiar permisos, eliminar subcarpetas y archivos, tomar posesión y todos los permisos anteriores
	Permisos especiales	Se habilita cuando se activa uno de ellos
Permisos en archivos	Lectura	Permite ver el contenido del archivo, propietarios, permisos y atributos
	Escritura	Posibilita modificar su contenido y sus atributos, así como ver el propietario, permisos y atributos
	Lectura y ejecución	Permite ejecutar el archivo más el permiso de lectura
	Modificar	Posibilita modificar y eliminar el archivo más los permisos de escritura, lectura y ejecución
	Control Total	Permite cambiar permisos, tomas posesión más todos los permisos anteriores
	Permisos especiales	Se habilita cuando se activa uno de ellos

Para acceder a los permisos de un archivo o carpeta, pulsamos botón derecho sobre ellos y elegimos propiedades. En la pestaña seguridad lo podemos ver:





opciones avanzadas de seguridad

Permisos

Permiso especial	Descripción
Atravesar carpeta/ejecutar archivo	Posibilita moverse por carpetas, aunque no se tenga permiso de acceso. En archivos, permite su ejecución
Mostrar carpeta/leer datos	Permite visualizar los nombres de ficheros y subcarpetas de una carpeta. En archivos, posibilita leer su contenido
Leer atributos	Permite ver los atributos de un archivo o carpeta como lectura y oculto
Leer atributos extendidos	Permite ver los atributos extendidos de un archivo o carpeta. Los atributos extendidos están definidos por los programas y pueden variar según estos
Crear archivos/escribir datos	En carpetas, permite crear archivos. En archivos, permite modificar su contenido
Crear carpetas/anexar datos	En carpetas, permite crear carpetas. En archivos, posibilita añadir datos sin modificar los existentes
Escribir atributos	Permite modificar los atributos del archivo o carpeta
Escribir atributos extendidos	Permite modificar los atributos extendidos del archivo o carpeta
Eliminar	Permite eliminar el archivo o carpeta
Permisos de lectura	Permite leer los permisos del archivo o carpeta
Cambiar permisos	Permite modificar los permisos del archivo o de la carpeta
Tomar posesión	Permite tomar posesión de un archivo o carpeta

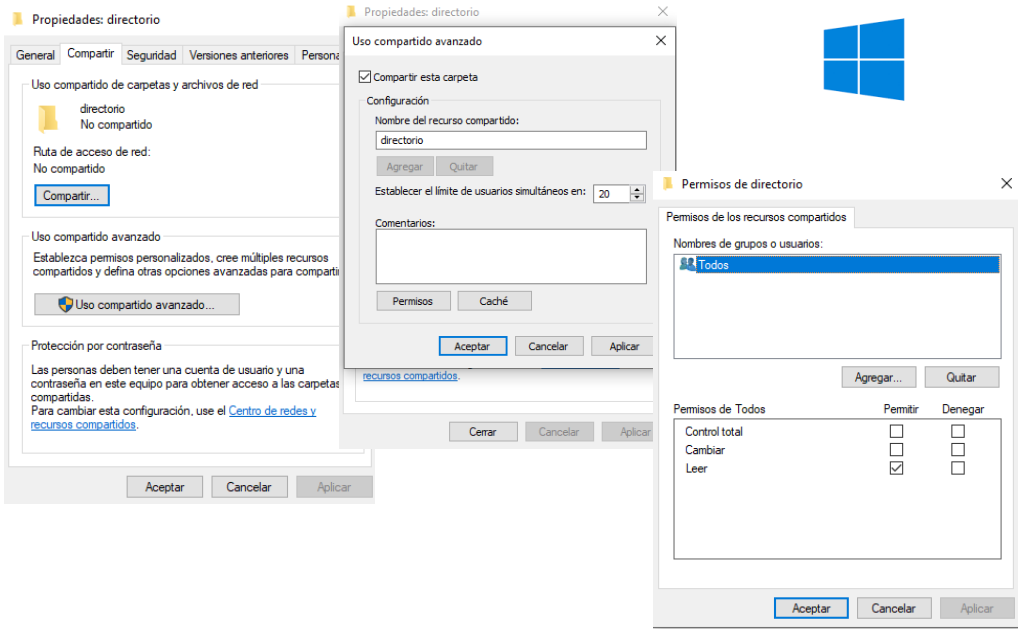
Cuando un **usuario** forma parte de un **grupo de usuarios**, este tiene los **mismos permisos** del grupo sobre un **objeto**. Por eficiencia del sistema, es recomendable asignar permisos a grupos de usuarios, en lugar de a usuarios sueltos si es posible.

Permisos. Permisos de red y locales

Para aplicar permisos de red en carpetas, vamos a la pestaña compartir. Indicaremos los usuarios con quien compartir y el nivel de permiso sobre estos

En uso compartido avanzado se puede modificar el nombre del recurso compartido y otras opciones más concretas como:

- Indicar el número máximo de usuarios que pueden acceder simultáneamente al recurso compartido
- Establecer un comentario sobre el recurso compartido para su correcta documentación
- Asignar permisos a usuarios y grupos de usuarios a través de Permisos

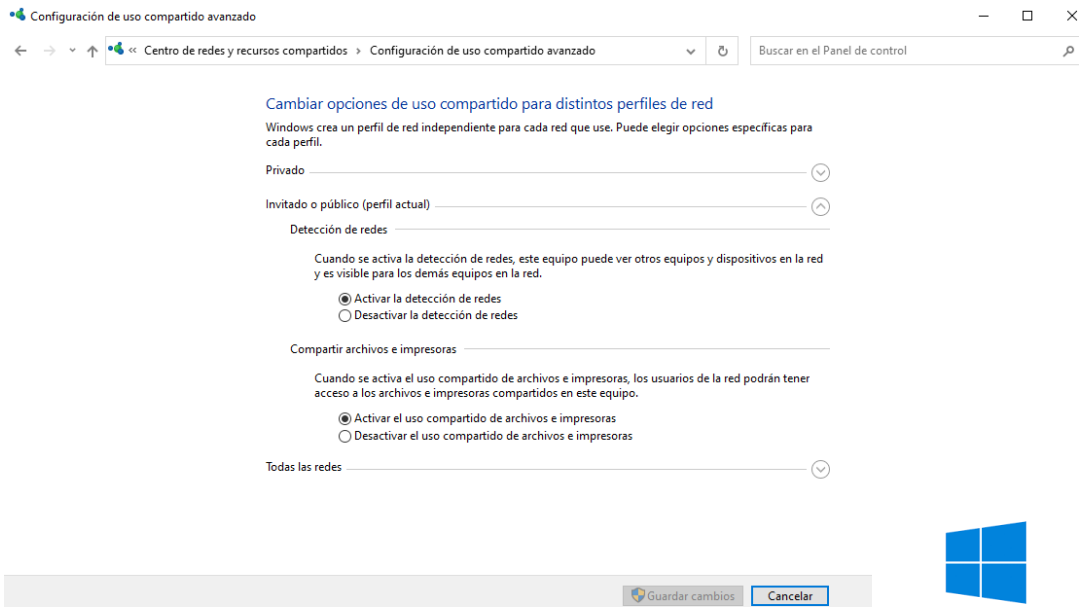


Se pueden compartir archivos a través de la opción **compartir con** y **Usuarios específicos** al pulsar botón secundario sobre ellos.

Permisos. Compartir archivos o carpetas

A la hora de compartir archivos o carpetas entre distintos equipos de Windows, suponemos que **los usuario disponen siempre de contraseña por seguridad**, y debemos asegurarnos:

- Que los equipos se encuentren en la **misma subred** lógica establecida por el administrador de red.
- **Activar la detección de redes y el uso compartido de archivos**. (Opciones de uso compartido en Red e Internet dentro de Configuración)
- Que se encuentran en el mismo grupo de trabajo el equipo con el recurso compartido y el equipo que desea hacer uso de aquel. **Comprobar mediante ping** que los dos equipos comunican entre sí.



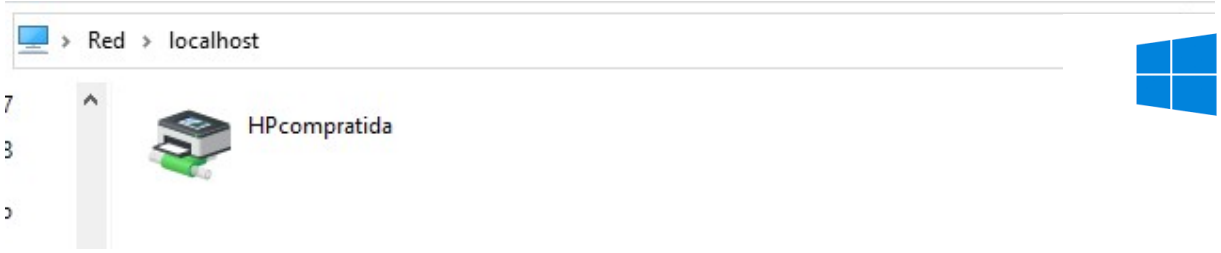
Permisos. Compartir archivos o carpetas

(a)“Red” del **“Explorador de Windows”**. En “Red” aparecerán los equipos accesibles desde el equipo actual. Podemos acceder a ellos introduciendo las credenciales, para más tarde acceder a sus recursos de red compartidos.

(b) Su especificación en formato UNC (convención de nomenclatura universal). Es decir, a través del **“Explorador de Windows”** podemos indicar, mediante el siguiente formato, el acceso al recurso: \\nombreEquipo\nombrerecurso

(c) Una unidad asignada. Mediante la opción **“Conectar a un unidad de red”** se configura el acceso a un equipo y a una ruta determinada. Se conectará al equipo remoto mediante unas credenciales, que pueden ser cambiadas por otras en caso de así desearlo en **“Conectar usando otras credenciales”**

Se puede ver los recursos compartidos de un equipo especificando **\\localhost** en la barra del **“Explorador de Windows”** .



Permisos. Herencia

Cuando trabajamos con carpetas y subcarpetas

objetos primarios, o contenedores

objetos secundarios (Subcarpetas y archivos dentro de la carpeta principal).

permisos

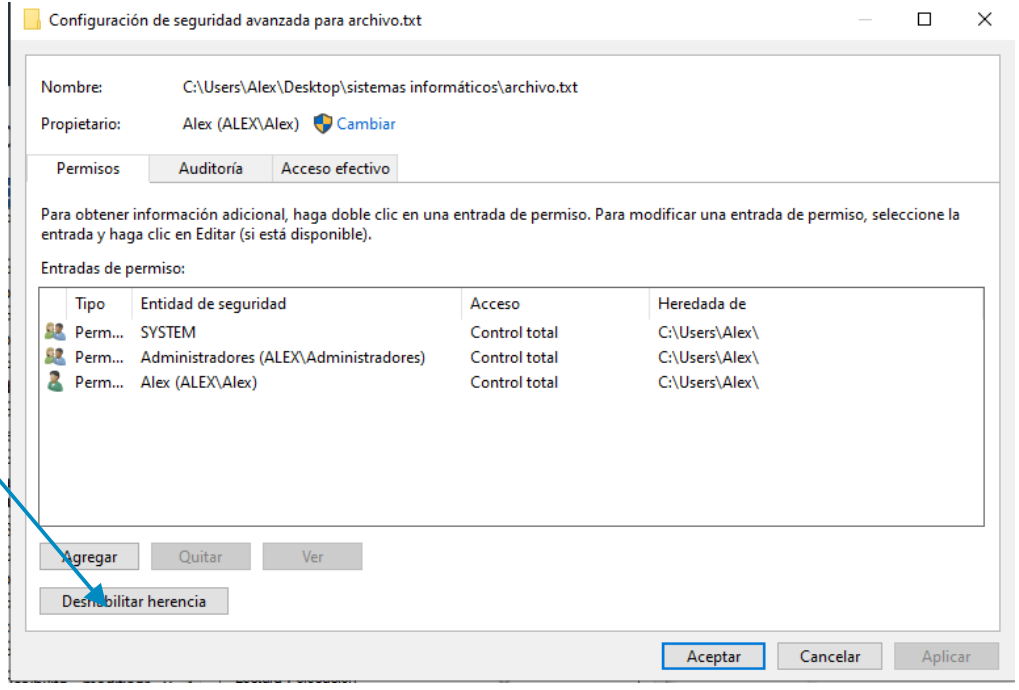
Windows permite **la herencia de permisos de objetos primarios a secundarios**. A los permisos que se heredan de los primarios se les conoce como permisos heredados, siendo el propietario quien controla como se heredan los permisos.

Los permisos de carpetas o archivos pueden heredar, implícitamente, permisos de la carpeta que los contienen. No obstante, estos pueden tener, además, permisos explícitos (establecidos directamente sobre ellos). La herencia de permisos es dinámica, por lo que la modificación de un permiso en una carpeta afectará a los archivos y carpetas que contenga.

Permisos. Herencia

En **“Opciones de seguridad avanzadas”** podemos habilitar o deshabilitar la herencia de un contenedor pulsando sobre el botón **“deshabilitar herencia”,** habilitada por defecto. Si se deshabilita la herencia, se puede optar por convertir los permisos heredados en explícitos o quitarlos. En cualquier caso, ya no afectarán las modificaciones de permisos del objeto primario sobre el secundario.

la herencia de permisos se puede editar para cada entrada de permiso, seleccionando la entrada y pulsando en **“Editar”** e indicando el tipo y a qué objetos les afectarán los permisos del objeto primario.

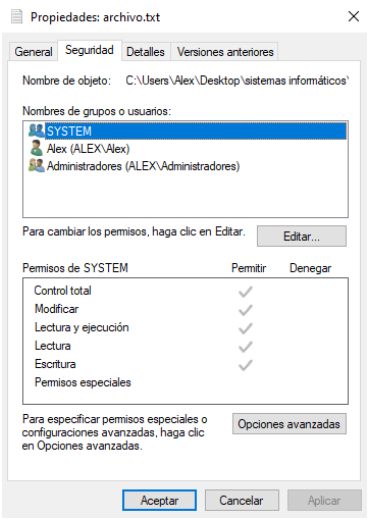


Permisos. ACL

El sistema de archivos NTFS implementa los permisos utilizando listas de control de acceso (ACL). Estas listas contienen los usuarios, grupos y equipos que tienen acceso permitido al archivo o carpeta y qué tipo de acceso.

Cada objeto tiene asociada una ACL, donde se indican los permisos de usuarios y grupos de usuarios. Para cada usuario o grupo de usuarios con permisos (denegados o concedidos) establecidos sobre un objeto, existe una entrada de control de acceso (ACE) en su ACL.

Windows representa gráficamente las ACL de un archivo o carpeta a través de la pestaña **“Seguridad”** de “ **Propiedades”**.



GNU/Linux

**En GNU/Linux se pueden aplicar ACL para adecuar y hacer más flexible los accesos o restricciones de usuarios y grupo de usuarios sobre los recursos. De esta manera, se pueden aplicar permisos más flexibles a usuarios o grupos de forma diferente del establecimiento de permisos regulares.*

Derechos de usuarios

Privilegios→ determinan las acciones que pueden realizar usuarios o grupos de usuarios en un sistema, ya sea en un equipo o en un dominio (administración centralizada de los recursos de una organización).

Se asocian con usuarios y no con objetos.

Pueden ser:

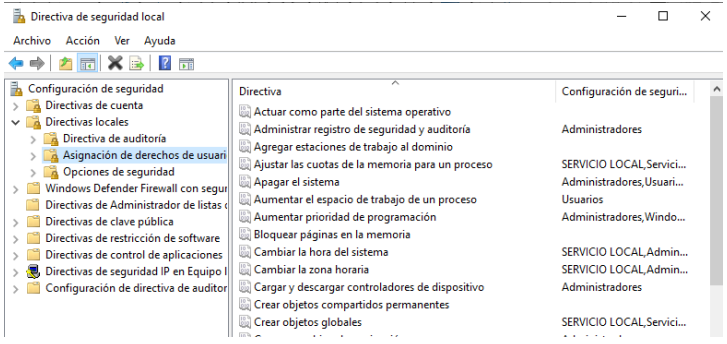
(a) **Derechos de inicio de sesión**: determinan de qué modo y quién inicia la sesión en un sistema.

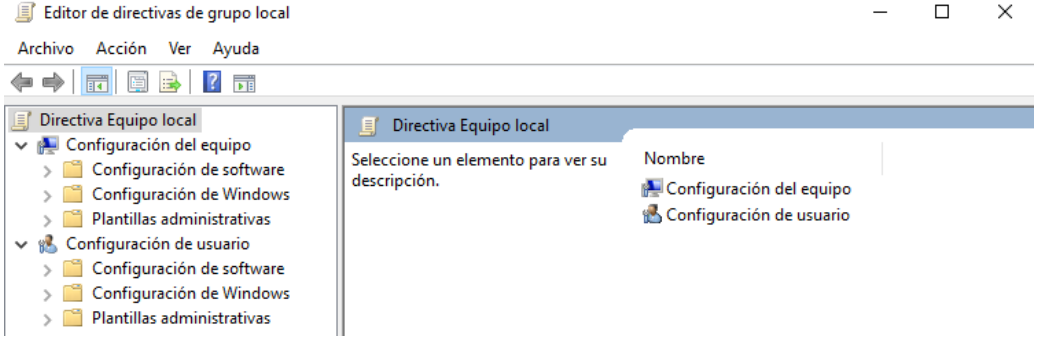
(b) **Privilegios específicos**: establecen los derechos de los usuarios una vez que han accedido al sistema, como, por ejemplo, realizar copias de seguridad de archivos y directorios, apagar el sistema, etc

Estos prevalecen sobre los permisos de los objetos.

Derechos de usuarios

Se administran mediante la herramienta **“Directiva de seguridad local”** de **“Herramientas administrativas”**, en **“Asignación de derechos de usuario”** dentro de **“Directivas locales”**.





También mediante la herramienta **“Editor de directivas de grupo local”** de las versiones más avanzadas de Windows 10, que incluye a **“Directiva de seguridad local”** dentro de los niveles **“Configuración de equipo”**, **“Configuración de Windows”** y **“Configuración de seguridad”**.

Derechos de usuarios.
Directivas de seguridad. Objetos y ámbito de directivas

Las directivas de seguridad establecen un conjunto de reglas de seguridad para administrar usuarios y equipos. Se definen mediante **objetos de directivas de grupo** (**GPO**). Una GPO contiene parámetros que definen políticas del sistema. De esta manera, se pueden centralizar políticas sobre usuarios y equipos, estableciendo permisos, bloqueos o controles. Ejemplos:

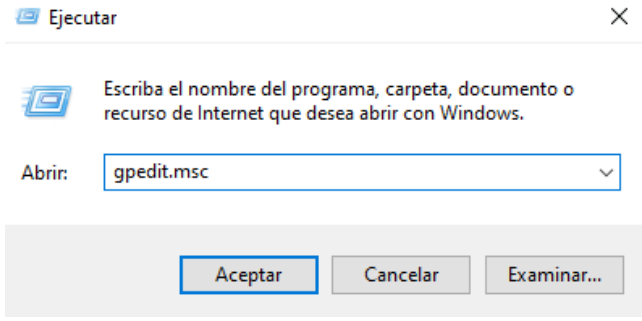
- Configurar el entorno gráfico
- Automatizar tareas
- Evitar que un usuario pueda instalar y desinstalar programas
- Fortalecer las contraseñas de inicio de sesión.
- Evitar el uso de memorias flash USB

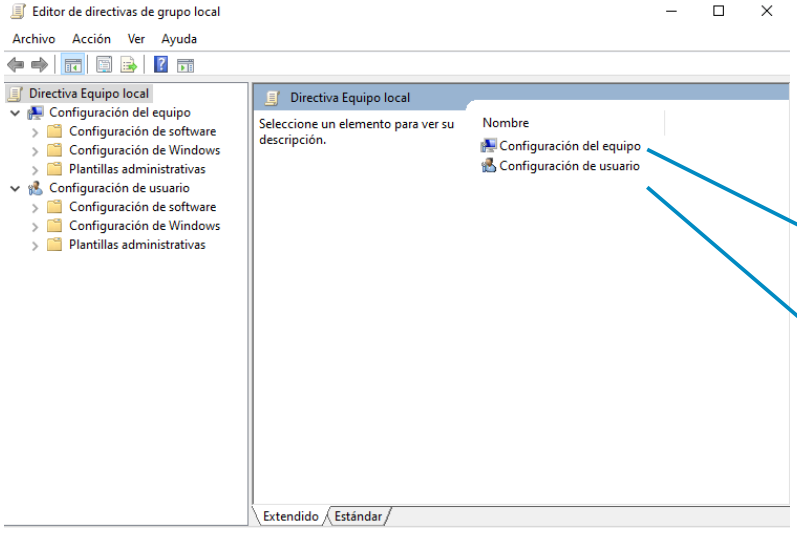
Podemos distinguir dos tipos:

- **GPO locales:** utilizadas para los equipos que no forman parte de un dominio. *Son las que estamos viendo*.
- **GPO no locales:** orientadas al servicio de directorio de Microsoft, Active directory (Windows Server)

Derechos de usuarios.
Directivas de seguridad. Objetos y ámbito de directivas

Para la gestión de GPO se emplea el **“Editor de directivas de grupo Local”**, el cual se puede ejecutar en las versiones avanzadas de Windows mediante el **“editor de directivas de grupo”** (o ejecutando gpedit.msc)





- **Directivas de configuración del equipo**: que aglutinan las políticas de configuración a nivel de equipo. Las modificaciones se aplican en el arranque del sistema.
- **Directivas de configuración de usuario**: donde se agrupan las políticas de configuración a nivel de usuario del equipo. Se aplican en cada inicio de sesión de usuario.

Derechos de usuarios.
Directivas de seguridad. Objetos y ámbito de directivas

A su vez, cada una se divide en las siguientes partes (aunque con diferentes políticas):

- **Configuración de Software:** permite la configuración del software ya instalado y la instalación automática de un nuevo software.
- **Configuración de Windows:** relacionado con el entorno de Windows, es decir, la configuración de seguridad, la ejecución de scripts, etc.
- **Plantillas administrativas:** incluyen políticas basadas en la configuración y ajustes del equipo, como el inicio y apagado, el panel de control la red, los componentes de Windows, etc.

El ámbito de las GPO es el equipo Local. Si se implementa el Active Directory el dominio.

Para llevar un control de las GPO establecidas, podemos listar **“Todos los valores”** dentro de **“Plantillas administrativas”**, tanto en **“Configuración de usuario”** como en **“Configuración de equipo”.**

Derechos de usuarios

Derechos de usuarios

Derechos de usuarios

Derechos de usuarios

Derechos de usuarios