Permisos de carpetas y archivos en sistemas Windows

Agustín Espinosa Minguet
Universitat Politècnica de València

Objetivo

- Explicar el mecanismo de aplicación de permisos de acceso a archivos y carpetas de los sistemas operativos Windows

Contenido

- Permisos estándar aplicados a archivos y carpetas
- Listas de control de acceso (ACLs)
- Mecanismo de autorización
- Buenas prácticas de diseño de ACLs

Permisos estándar aplicados a archivos

- Lectura
  - Leer el contenido del archivo
- Escritura
  - Cambiar el contenido del archivo
- Lectura y ejecución
  - Lectura + ejecutar el archivo si es un programa ejecutable
- Modificar
  - Lectura y ejecución + Escritura + eliminar el archivo
- Control Total
  - Modificar + tomar posesión + cambiar permisos

Permisos estándar aplicados a carpetas

- Mostrar
  - Ver la lista de elementos de la carpeta y sus subcarpetas (no implica poder acceder a ellos)
- Lectura
  - Mostrar
    + Lectura (aplicado a archivos *)
- Lectura y ejecución
  - Mostrar
    + Lectura y ejecución (aplicado a archivos *)

** los de la carpeta y cualquier subcarpeta*

Permisos estándar aplicados a carpetas

- Escritura
  - Crear subcarpetas y archivos en la carpeta y subcarpetas + Escritura (aplicado a archivos *)
- Modificar
  - Lectura y ejecución + Escritura + eliminar la carpeta y subcarpetas + Modificar (aplicado a archivos *)
- Control Total
  - Modificar
    + tomar posesión de la carpeta y subcarpetas *
    + cambiar permisos de la carpeta y subcarpetas *
    + eliminar subcarpetas y archivos aun sin tener permiso para ello + Control Total (aplicado a archivos *)

** los de la carpeta y cualquier subcarpeta*

Listas de control de acceso (ACLs) *Access Control Lists*

- Se utilizan para conceder o denegar permisos a usuarios y grupos
- Formadas por una lista de entradas de control de acceso (ACE) *Access Control Entries*
- Estructura de una ACE:

Permitir / Denegar	Usuario / Grupo	Permiso

- Ejemplo:

Permitir	Juan	Lectura
Permitir	Directores	Modificar
Denegar	Ejecutivos	Escritura

Listas de control de acceso (ACLs)

- Una lista de control de acceso tiene dos tipos de entradas, las heredadas y las explícitas
- Las entradas heredadas son las explícitas de las carpetas antecesoras

C:\			
Permitir	Directores	Modificar	Explícita

C:\TEMP			
Permitir	Directores	Modificar	Heredada de C:\
Permitir	Ejecutivos	Leer	Explícita

C:\TEMP\DATOS.TXT			
Permitir	Directores	Modificar	Heredada de C:\
Permitir	Ejecutivos	Leer	Heredada de C:\TEMP

Listas de control de acceso (ACLs)

- Es posible desactivar la herencia en un archivo o carpeta respecto a sus carpetas antecesoras.
- Se utiliza cuando los permisos de un archivo o carpeta deben ser más restrictivos que los heredados

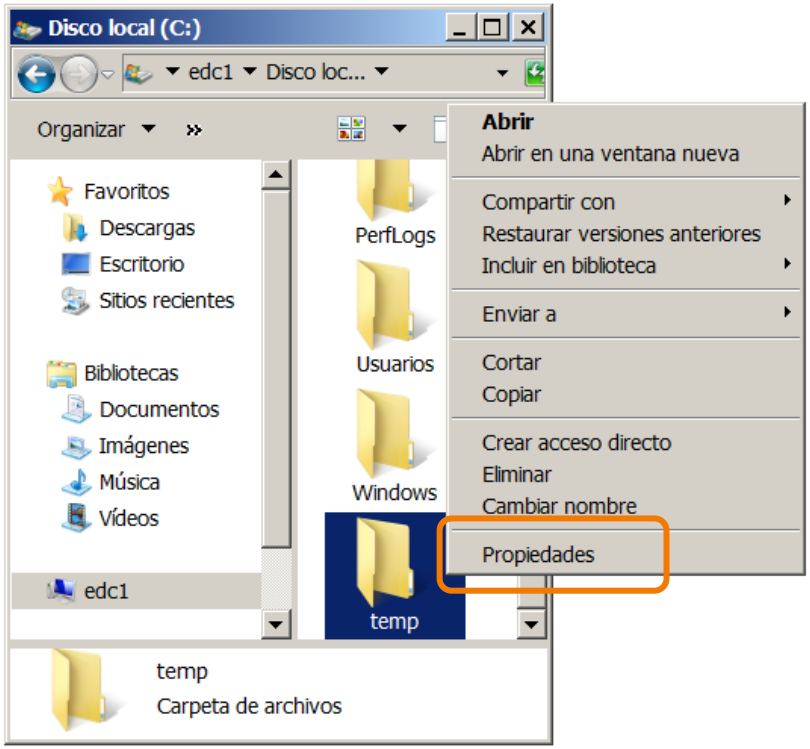
C:			
Permitir	Directores	Modificar	Explícita

C:\TEMP		**¡¡ Herencia Desactivada !!**	
Permitir	Ejecutivos	Leer	Explícita

C:\TEMP\DESCARGAS			
Permitir	Ejecutivos	Leer	Heredada de C:\TEMP

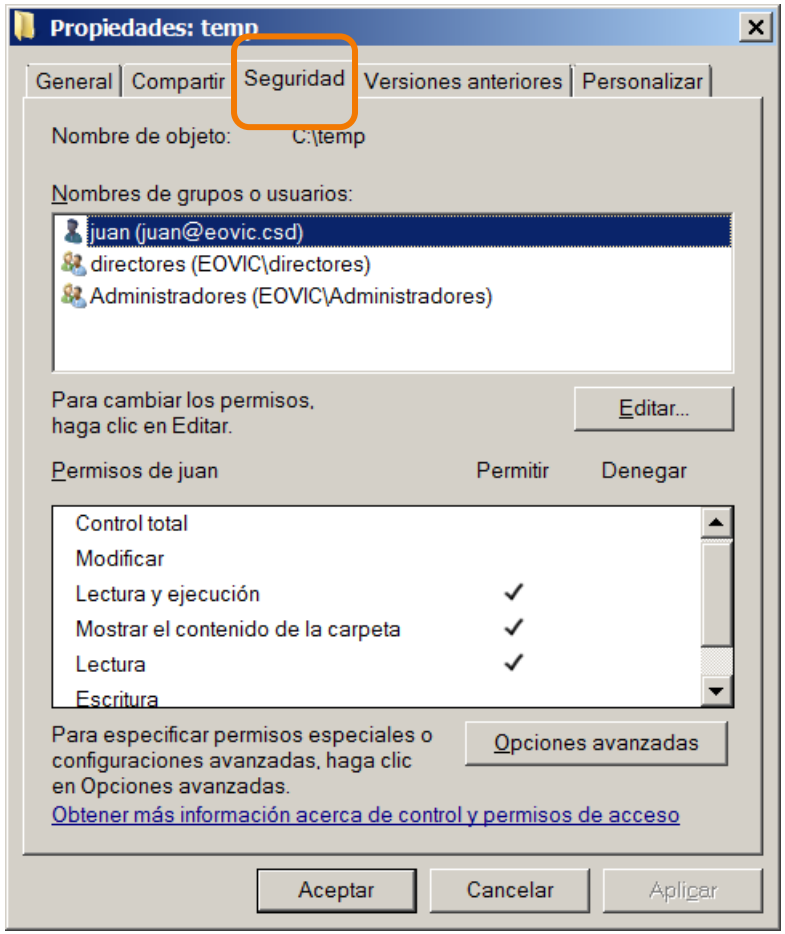
Interfaz de gestión de ACLs

- Se accede desde las Propiedades de la carpetas o archivos



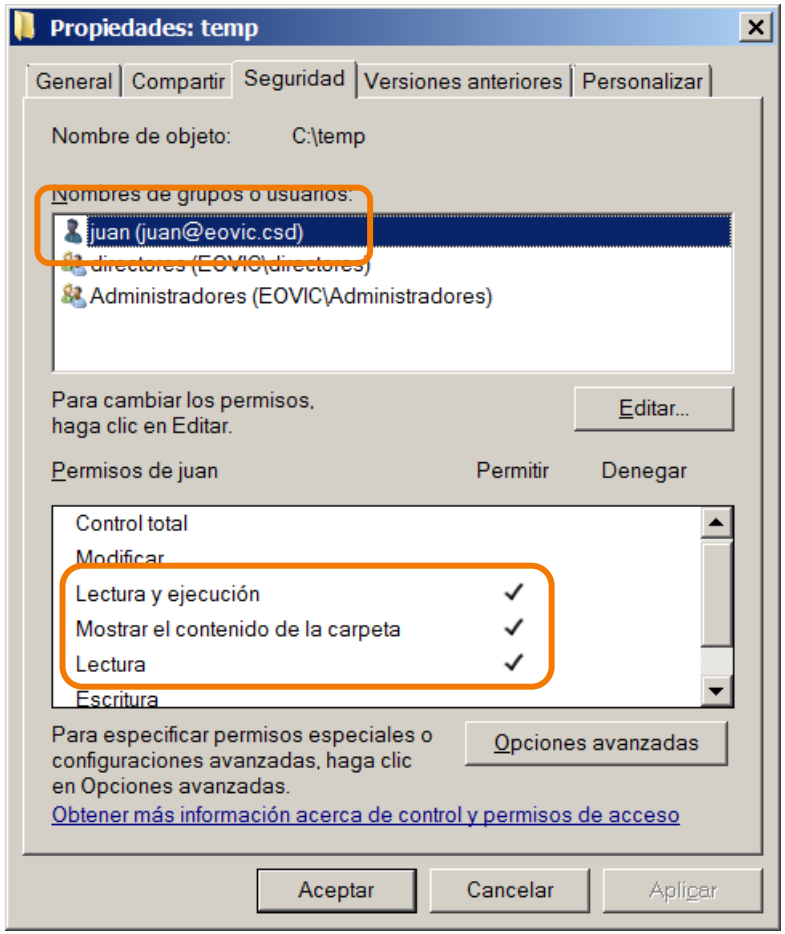
Interfaz de gestión de ACLs

- Lista de control de acceso en la pestaña de Seguridad



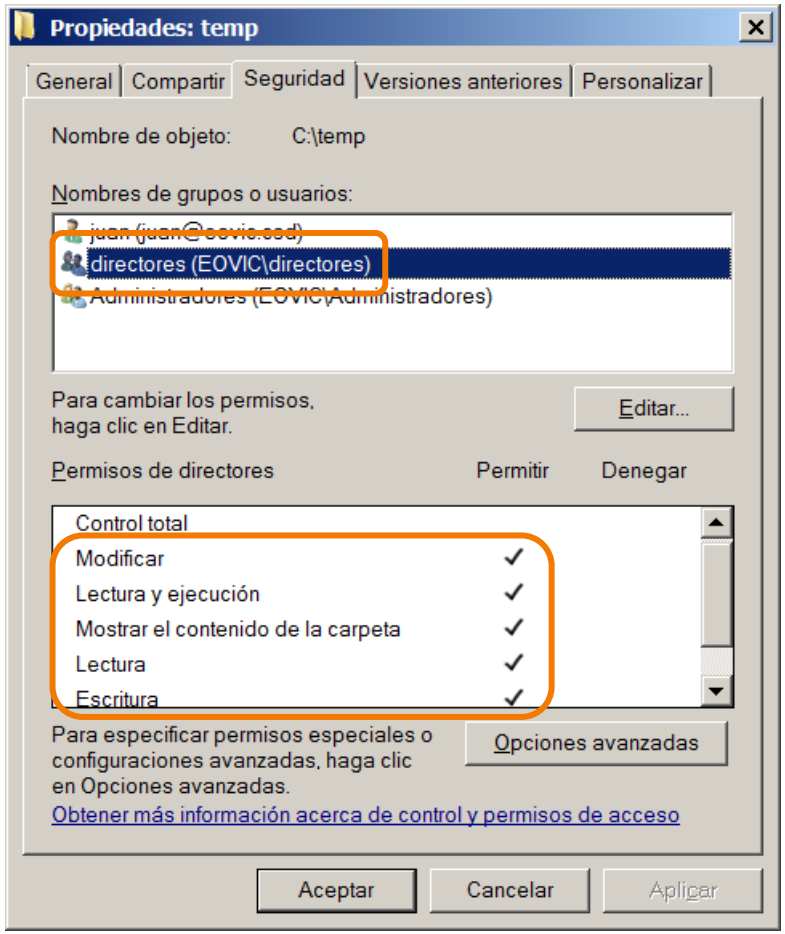
Interfaz de gestión de ACLs

- Permiso para juan
  - Lectura y Ejecución



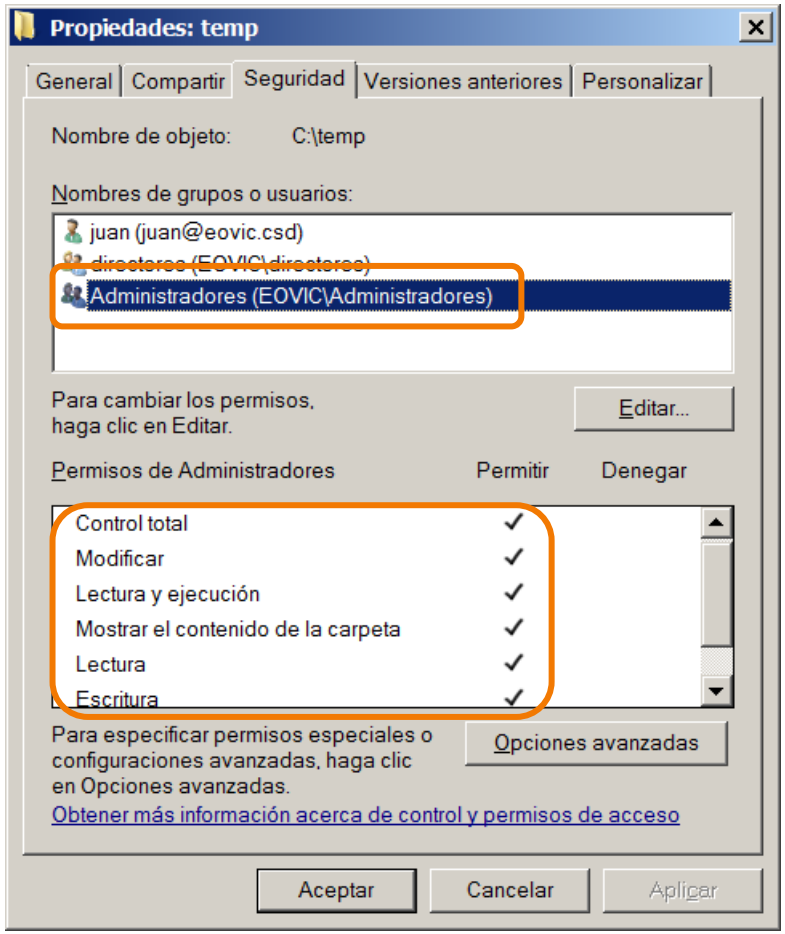
Interfaz de gestión de ACLs

- Permiso para directores
  - Modificar



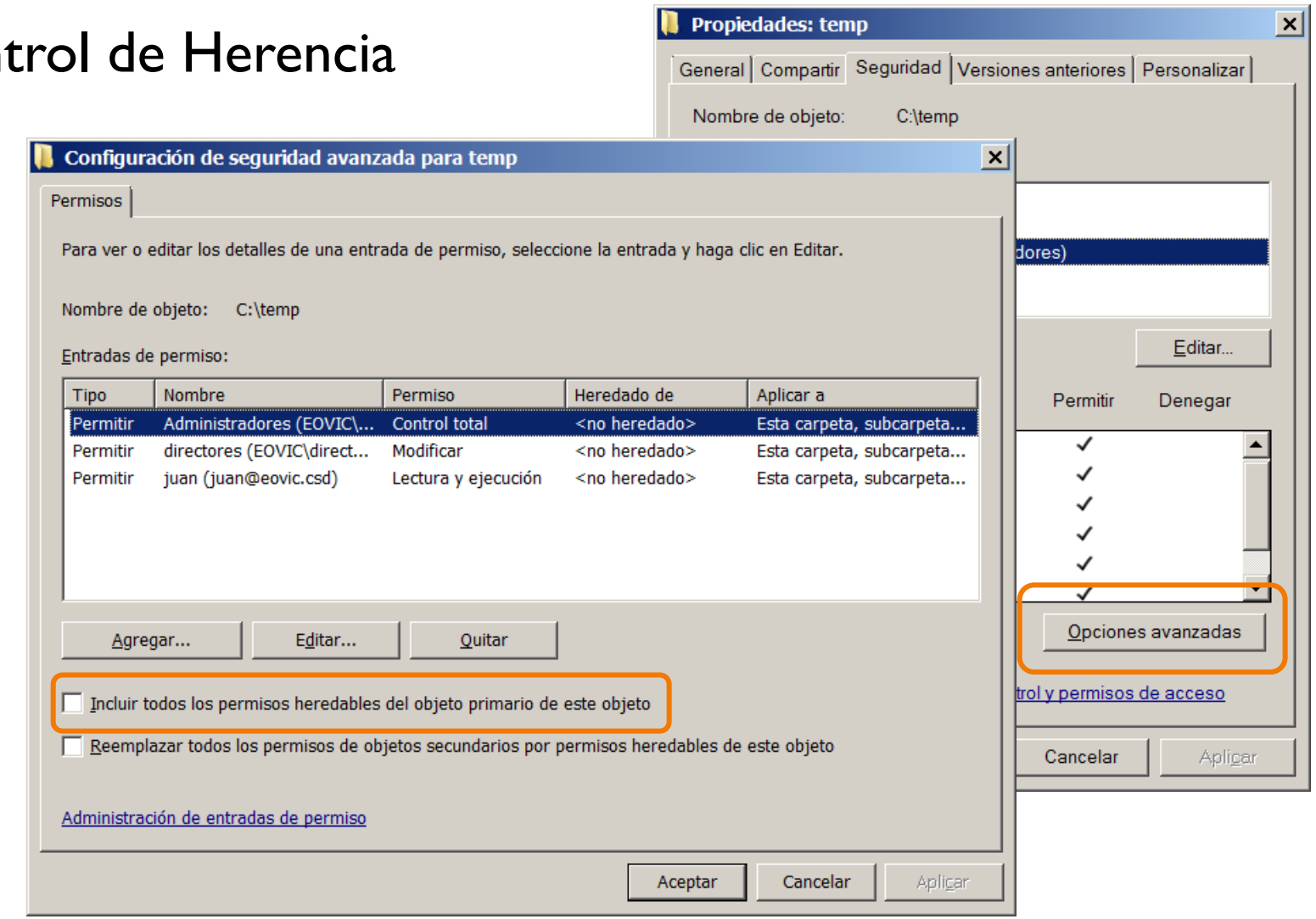
Interfaz de gestión de ACLs

- Permiso para Administradores
  - Control total



Interfaz de gestión de ACLs

- Control de Herencia



Mecanismo de autorización

- Se inicia cuando un usuario solicita realizar una acción sobre un archivo o carpeta.
  - Ejemplos: editar un archivo, mostrar una carpeta
- El sistema realiza los siguientes pasos para decidir si autoriza la acción:
  1. Determina el conjunto de permisos necesario para llevar a cabo la acción
     - Ejemplo: editar un archivo necesita lectura y escritura.
  2. Crea un conjunto de identidades formado por el usuario y los grupos a los que pertenece
     - Ejemplo: Juan, Directores, Todos

Mecanismo de autorización

- Pasos (continuación)
  3. Recorre la ACL en el siguiente orden:
     - ACEs explícitas que deniegan
     - ACEs explícitas que permiten
     - ACEs heredadas de la carpeta padre que deniegan
     - ACEs heredadas de la carpeta padre que permiten
     - …
     - ACEs heredadas de la carpeta antecesora más lejana que deniegan
     - ACEs heredadas de la carpeta antecesora más lejana que permiten
  4. Analiza sólo aquellas entradas que hacen referencia a alguna de las identidades del usuario

Mecanismo de autorización

- Pasos (continuación)
  5. Para cada entrada analizada
     - Si la entrada deniega **alguno** de los permisos de la solicitud, se deniega el acceso y se deja de recorrer la ACL
     - Si la entrada concede alguno de los permisos de la solicitud, se acumula a otros permisos previamente acumulados.
       Si **todos** los permisos solicitados forman parte de los permisos acumulados
       se concede el acceso y se deja de recorrer la ACL
  6. Si finalmente se recorre toda la ACL sin haber tomado ninguna de las decisiones anteriores
     se deniega el acceso.

Mecanismo de autorización

- Ejemplo 1:
  - `Ana`, cuyos grupos son `Proy2` y `Proy3` solicita una acción sobre `F:\D10\D11\D12\DATOS.TXT` que requiere los permisos: Lectura y Ejecución y Escritura

F:\D10\D11\D12\DATOS.TXT			
Tipo	Usuario/Grupo	Permiso	Heredada de
Permitir	Alicia	Modificar	No heredada
Denegar	Adrian	Lectura	F:\D10\D11\D12\
Permitir	Proy3	Escritura	F:\D10\D11\D12\
Permitir	Proy1	Lectura y Ejecución	F:\D10\D11\
Permitir	Proy2	Lectura y Ejecución	F:\D10\
Permitir	Administradores	Control Total	F:\

Petición Autorizada

Mecanismo de autorización

- Ejemplo 2:
  - `Adrian`, cuyos grupos son `Proy2` y `Proy3` solicita una acción sobre `F:\D10\D11\D12\DATOS.TXT` que requiere los permisos: Lectura y Ejecución y Escritura

F:\D10\D11\D12\DATOS.TXT			
Tipo	Usuario/Grupo	Permiso	Heredada de
Permitir	Alicia	Modificar	No heredada
Denegar	Adrian	Lectura	F:\D10\D11\D12\
Permitir	Proy3	Escritura	F:\D10\D11\D12\
Permitir	Proy1	Lectura y Ejecución	F:\D10\D11\
Permitir	Proy2	Lectura y Ejecución	F:\D10\
Permitir	Administradores	Control Total	F:\

Petición NO autorizada

Mecanismo de autorización

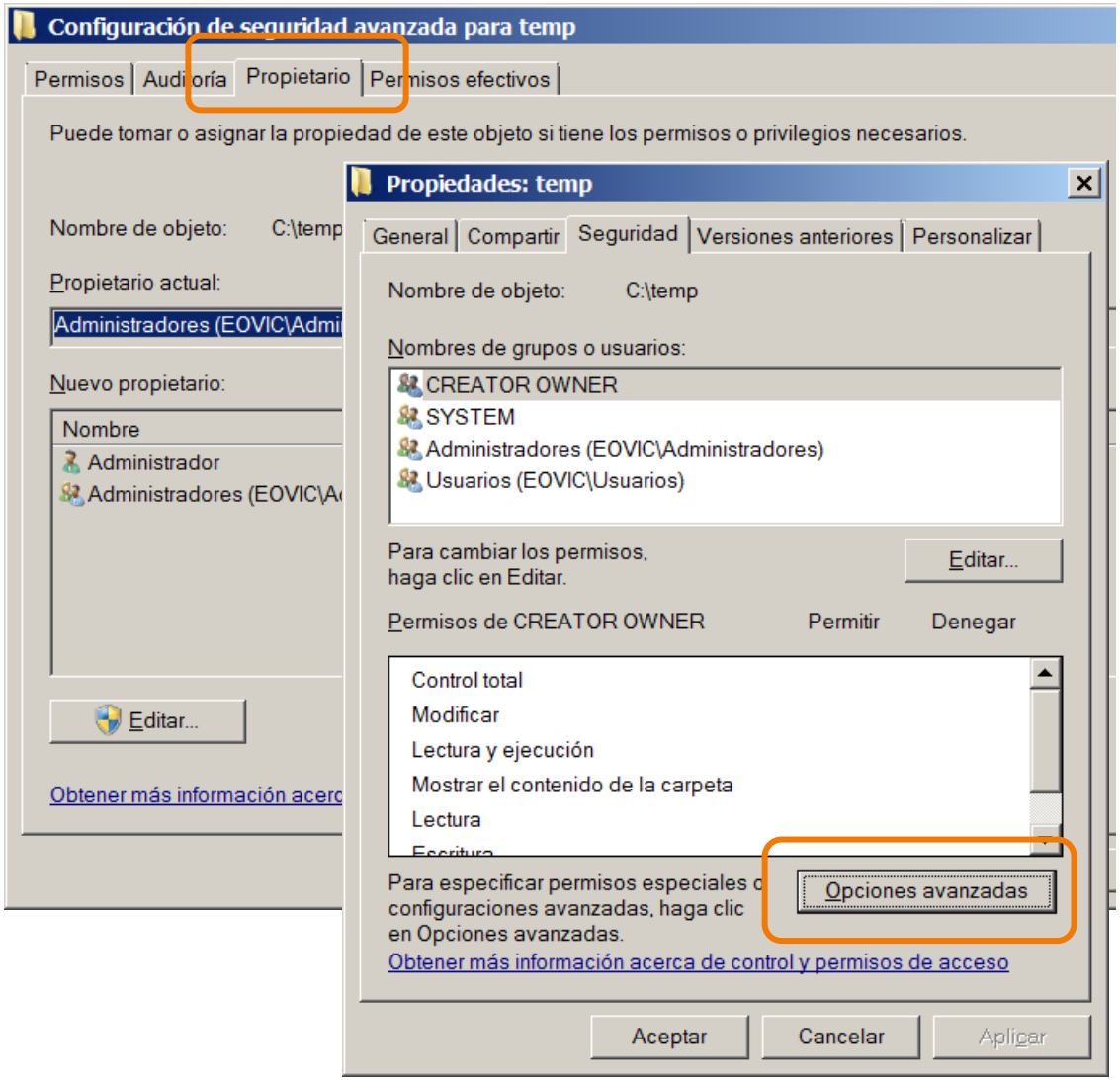
- Ejemplo 3:
  - `Antonio`, cuyos grupos son `Proy1` y `Proy5` solicita una acción sobre `F:\D10\D11\D12\DATOS.TXT` que requiere los permisos: Lectura y Ejecución y Escritura

F:\D10\D11\D12\DATOS.TXT			
Tipo	Usuario/Grupo	Permiso	Heredada de
Permitir	Alicia	Modificar	No heredada
Denegar	Adrian	Lectura	F:\D10\D11\D12\
Permitir	Proy3	Escritura	F:\D10\D11\D12\
Permitir	Proy1	Lectura y Ejecución	F:\D10\D11\
Permitir	Proy2	Lectura y Ejecución	F:\D10\
Permitir	Administradores	Control Total	F:\

Petición NO Autorizada

Mecanismo de autorización

- Propietario
  - Siempre puede cambiar los permisos
  - El permiso Control Total autoriza a cambiar el propietario, pero sólo a uno mismo
  - El administrador tiene el derecho de cambio general de propietario



Buenas prácticas en el diseño de ACLs

- Si los permisos heredados no son adecuados, desactiva la herencia antes que usar la denegación de permisos.
- En dominios, utiliza sólo grupos de Dominio Local
- Emplea sólo un grupo por cada permiso distinto
- Usa un convenio de nombrado que facilite la identificación del propósito de cada grupo de Dominio Local:
  - Convenio recomendado: ACL_nombre del objeto_permiso
  - Ejemplo para la carpeta datos:

F:\DATOS		
Permitir	ACL_datos_control total	Control Total
Permitir	ACL_datos_modificar	Modificar
Permitir	ACL_datos_lectura	Lectura

Resumen

- La herencia de permisos facilita que los permisos puedan aplicarse en base a carpetas y no a su contenido
- Los asignación de permisos tiene un carácter acumulativo consecuencia de los pasos que tienen lugar en el mecanismo de autorización
- Es importante seguir buenas prácticas para elegir la mejor forma de establecer permisos