SISTEMAS INFORMÁTICOS UD-6

GESTIÓN DE RECURSOS EN RED DE UN SISTEMA INFORÁTICO

ÍNDICE

[PERMISOS 3](#_Toc133680045)

[PERMISOS BÁSICOS 3](#_Toc133680046)

[PERMISOS ESPECIALES 5](#_Toc133680047)

[PERMISOS DE RED Y LOCALES 5](#_Toc133680048)

[COMPARTIR ARCHIVOS O CARPETAS 6](#_Toc133680049)

[HERENCIA 8](#_Toc133680050)

[ACL 9](#_Toc133680051)

[DERECHOS DE USUARIOS (PRIVILEGIOS) 9](#_Toc133680052)

[DIRECTIVAS DE SEGURIDAD. OBJETOS Y ÁMBITO 10](#_Toc133680053)

[PLANTILLAS 12](#_Toc133680054)

# PERMISOS

Los objetos son estructuras de datos que representan recursos, como archivos, carpetas, impresoras, procesos, etc.

Los permisos definen el tipo de acceso concedido a un usuario o grupo de usuarios sobre un objeto.

En Windows los recursos tienen un propietario que concede o deniega permisos a usuarios o grupos de usuarios (*Security Principals* 🡪 identificados por un SID: Identificador de Seguridad Único).

El propietario de los objetos es el creador del objeto. Éste se puede modificar si se dispone del permiso de Tomar posesión (lo tienen el administrador y el propietario), este permiso se refiere a que puede cambiar a quién pertenece ese objeto creado, el propietario por defecto es el creador.

# PERMISOS BÁSICOS

|  |  |  |
| --- | --- | --- |
| Tipo | Nombre | Definición |
| Carpetas | Mostar el contenido de la carpeta | Posibilita listar el contenido de la carpeta. |
| Lectura | Ver el contenido de la carpeta, permisos, propietario y atributos |
| Escritura | Crear nuevos archivos y subcarpetas, ver propietario, modificar atributos y permisos. |
| Lectura y ejecución | Navegar por las subcarpetas más los permisos de lectura y mostrar contenido. |
| Modificar | Eliminar la carpeta más los permisos de lectura y ejecución. |
| Control total | Cambiar permisos, eliminar subcarpetas y archivos, tomar posesión y todos los permisos anteriores. |
| Permisos especiales | Se habilitan cuando se activa uno de ellos. |
| Archivos | Lectura | Ver el contenido del archivo, permisos, propietario y atributos. |
| Escritura | Modificar su contenido y sus atributos, ver propietario, atributos y permisos. |
| Lectura y ejecución | Ejecutar el archivo más permiso de lectura. |
| Modificar | Modificar y eliminar el archivo más los permisos de escritura, lectura y ejecución. |
| Control total | Cambiar permisos, tomar posesión y todos los permisos anteriores |
| Permisos especiales | Se habilitan cuando se activa uno de ellos. |

Los permisos de un archivo o carpeta los podemos ver desde la opción “Propiedades” del menú contextual. En la pestaña “Seguridad” podremos cambiarlos.

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamenteInterfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

En opciones avanzadas 🡪 Ver 🡪 “Mostrar permisos avanzados” podemos ver los permisos especiales.

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

# PERMISOS ESPECIALES

|  |  |
| --- | --- |
| Tipo permiso | Descripción |
| Atravesar carpeta / ejecutar archivo | Moverse por carpetas, aunque no se tenga permiso de acceso. En archivos permite su ejecución. |
| Mostar carpeta / leer datos | Visualizar los nombres de ficheros y subcarpetas de una carpeta. En archivos, leer su contenido. |
| Leer atributos | Ver atributos de un archivo o carpeta como lectura y oculto. |
| Leer atributos extendidos | Ver atributos extendidos de un archivo o carpeta. Estos atributos están definidos por los programas y pueden variar según éstos. |
| Crear archivos / escribir datos | En carpetas, crear archivos. En archivos, modificar su contenido. |
| Crear carpetas / anexar datos | En carpetas, crear carpetas. En archivos, añadir datos sin modificar los existentes. |
| Escribir atributos | Modificar atributos del archivo o carpeta. |
| Escribir atributos extendidos | Modificar atributos extendidos del archivo o carpeta. |
| Eliminar | Eliminar el archivo o carpeta. |
| Permisos de lectura | Leer los permisos del archivo o la carpeta. |
| Cambiar permisos | Modificar los permisos del archivo o la carpeta. |
| Tomar posesión | Tomar posesión de un archivo o carpeta. |

# Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico Descripción generada automáticamentePERMISOS DE RED Y LOCALES

Para aplicar permisos de red en carpetas, debemos seleccionar la pestaña “Compartir” en las “Propiedades” de la carpeta en el explorador de Windows.

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamenteEn “Uso compartido avanzado” se puede modificar el nombre del recurso compartido y otras opciones como:

* Indicar el número máximo de usuarios que pueden acceder a la vez al recurso.
* Indicar un comentario sobre el recurso compartido para su documentación.
* Asignar permisos y grupos de usuarios desde “Permisos”.

También hay accesos directos para compartir recursos directamente desde el menú contextual: “conceder acceso a” 🡪 “Usuarios específicos”.

Interfaz de usuario gráfica

Descripción generada automáticamente

# COMPARTIR ARCHIVOS O CARPETAS

A la hora de compartir archivos o carpetas entre distintos equipos suponemos que los usuarios tienen contraseña por seguridad y debemos verificar:

* Que los equipos se encuentran en la misma subred lógica establecida por el administrador.
* Activar la detección de redes y el uso compartido de archivos.

Texto

Descripción generada automáticamente con confianza baja

* Que se encuentran en el mismo grupo de trabajo el equipo con el recurso compartido y el equipo que desea hacer uso de aquel.

Para acceder a un recurso compartido lo podemos hacer desde: “Red” del “Explorador de Windows” 🡪 aparecerán los equipos accesibles del equipo actual. Podemos acceder a ellos introduciendo las credenciales.

Su nombre de formato universal (UNC) es \\nombreEquipo\nombreRecurso.

Una unidad asignada. Por la opción “Conectar a una unidad de red” del menú contextual al situarnos en “Red”.

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Podemos ver los recursos compartidos de un equipo especificando \\localhost en la barra del explorador de Windows.

También desde Panel de Control 🡪 Sistema y seguridad 🡪 Herramientas administrativas 🡪 Administrador de equipos 🡪 Carpetas compartidas 🡪 Recursos compartidos.

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamenteInterfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

De manera automática se comparten:

* Interfaz de usuario gráfica, Aplicación

  Descripción generada automáticamente con confianza mediaLas unidades con el formato letraUnidad$, por ejemplo, C$ y D$.
* El directorio del sistema cuyo nombre de recurso compartido es ADMIN$, siendo normalmente la ruta C:\Windows.
* Agrupación de tuberías de comunicación de procesos mediante el recurso compartido con nombre IPC$.

Por seguridad, los recursos compartidos terminados en $ quedan ocultos, aunque se puede acceder a ellos indicando el nombre del recurso compartido completo, es decir, con la terminación $. Por eso no aparecen desde \\localhost.

# HERENCIA

Microsoft Windows permite la herencia de permisos de objetos primarios o contenedores (carpetas y subcarpetas) a objetos secundarios (subcarpetas y archivos dentro de la carpeta principal).

A estos permisos heredados de objetos primarios se les conoce como permisos heredados. El propietario controla cómo se heredan los permisos.

La herencia de permisos es dinámica, es decir la modificación de un permiso en el objeto principal afectará a los secundarios.

En “Opciones de seguridad avanzadas” podemos habilitar o deshabilitar la herencia de un contenedor.

Por defecto la herencia está habilitada. Si se deshabilita se puede optar por convertir los permisos heredados en explícitos o quitarlos.

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Se puede editar para cada entrada de permiso indicando el tipo y a qué objetos afectaría.

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

En caso de conflicto, los permisos explícitos (propios del objeto) tienen prioridad sobre los heredados.

# Interfaz de usuario gráfica, Texto, Aplicación Descripción generada automáticamenteACL

Las listas de control de acceso (**ACL**) 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. Para cada usuario o grupo de usuarios existe una entrada de control de acceso (**ACE**) en su ACL.

Esta información se puede ver en la pestaña “**Seguridad**” de las **propiedades** del objeto.

En GNU/Linux también se pueden establecer listas ACL para la gestión de permisos.

# DERECHOS DE USUARIOS (PRIVILEGIOS)

A diferencia de los permisos, que se asocian a objetos, los privilegios se asocian a usuarios.

Distinguimos:

* **Derechos de inicio de sesión**: determina de qué modo y quién inicia sesión en un sistema.
* **Privilegios específicos**: establecen derechos de los usuarios una vez que han accedido al sistema.

Los derechos de usuario prevalecen sobre los permisos de los objetos.

También existe herencia de privilegios, un usuario hereda los privilegios que tenga el grupo al que pertenece.

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

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

O mediante el “**Editor de directivas de grupo local**” en Configuración del equipo -> Configuración de Windows -> Configuración de seguridad -> Directivas locales – **Asignación de derechos de usuario**

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

# DIRECTIVAS DE SEGURIDAD. OBJETOS Y ÁMBITO

Establecen un conjunto de reglas de seguridad para administrar usuarios y equipos. Se definen mediante **objetos de directivas de grupo** (**GPO**), que contienen parámetros que definen políticas del sistema.

Ejemplos de uso:

* Configuración del entorno gráfico.
* Automatización de tareas.
* Evitar instalación y desinstalación de programas por parte de un usuario.
* Evitar el uso de memorias flash USB.

Distinguimos:

* **GPO locales**: utilizadas para equipos que no forman parte de un dominio.
* **GPO no locales**: orientadas a Active Directory (servicio de directorio de Microsoft).

Se gestionan desde el “**Editor de directivas de grupo local**” (gpedit.msc)

Interfaz de usuario gráfica, Texto, Aplicación, Word

Descripción generada automáticamente

Se dividen en:

* Directivas de configuración **del equipo**: las modificaciones se aplican en el arranque del equipo.
* Directivas de configuración **de** **usuario**: las modificaciones se aplican en cada inicio de sesión de usuario.

Interfaz de usuario gráfica, Texto, Aplicación, Word

Descripción generada automáticamente

Cada una de las anteriores se divide en:

* **Configuración de software**: afecta a programas ya instalados y la instalación de nuevos programas.
* **Configuración de Windows**: afecta a la seguridad, ejecución de scripts, etc.
* **Plantillas administrativas**: relacionadas con la configuración y ajustes del equipo. Es la categoría más amplia e importante.

El ámbito de actuación de las GPO es el propio equipo local. En caso de tener implementado Active Directory el ámbito sería mayor.

Desde la consola podemos listar las directivas establecidas:

* gpresult /r 🡪 Políticas aplicadas al sistema en general
* gpresult /USER usuario /V 🡪 Políticas aplicadas sobre un usuario

# PLANTILLAS

Permiten definir la configuración para administrar aplicaciones o características del propio sistema operativo o de aplicaciones de terceros. Se pueden agregar o quitar plantillas de la lista actual.

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente