IMPLANTACIÓN DE SISTEMAS OPERATIVOS

TEMA GESTIÓN DE WINDOWS

Contenido

[1 INSTALACIÓN Y ADMINISTRACIÓN DE UN S.O. CLIENTE TIPO WINDOWS 3](#_Toc155559717)

[1.1 VERSIONES DE WINDOWS 10 3](#_Toc155559718)

[2 LA PARTICIÓN DE 500 MB. 5](#_Toc155559719)

[3 Principios de Seguridad en Windows 6](#_Toc155559720)

[3.1 Gestión de Cuentas de Usuario y Grupos. 6](#_Toc155559721)

[ Asistente para cuentas de usuario desde Panel de Control 8](#_Toc155559722)

[ Gestión de cuentas de usuarios locales y grupos mediante consola. 8](#_Toc155559723)

[ Gestión de Cuentas de Usuario desde el Interfaz de línea de comandos de Windows (CLI). 19](#_Toc155559724)

[ Gestión de las contraseñas. 23](#_Toc155559725)

[ Bloqueo de las cuentas. 26](#_Toc155559726)

[3.2 IDENTIFICADOR DE SEGURIDAD O SID. 27](#_Toc155559727)

[3.3 Recursos Locales. Gestión de ACL 34](#_Toc155559728)

# INSTALACIÓN Y ADMINISTRACIÓN DE UN S.O. CLIENTE TIPO WINDOWS

Entendemos como sistema operativo cliente al sistema que no está diseñado para actuar como servidor en un sistema informático, sino que desempeña el papel de sistema cliente conectado a un servidor. Estos sistemas operativos permiten trabajar tanto de forma separada sin conectarse a un servidor, como de forma conjunta uniéndose a un sistema informático mayor que cuente con un servidor.

Como sistemas operativos clientes típicos podemos citar entre muchos a los siguientes:

* Windows 10
* Windows Vista
* Windows 7
* Windows 8
* Linux (Ubuntu, Linux Mint, etc.).
* Mac OS

## VERSIONES DE WINDOWS 10

Para comprobar nuestra versión actual de Windows 10 tenemos que acceder al panel de control, sistema y seguridad, sistema o bien pulsando botón derecho del ratón sobre Mi PC (o equipo) y eligiendo la opción Propiedades, o bien pulsando la combinación de teclas Windows + Pausa.

Texto

Descripción generada automáticamente con confianza media

Pasos a hacer para ver esta pantalla, antigua.

Interfaz de usuario gráfica

Descripción generada automáticamente

explorer.exe shell:::{BB06C0E4-D293-4f75-8A90-CB05B6477EEE}

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Las seis versiones principales de Windows 10 son las siguientes:

**Windows 10 Home** es la edición de escritorio centrada en el consumidor.

**Windows 10 Mobile** está diseñado para ofrecer la mejor experiencia de usuario en los dispositivos más pequeños, como teléfonos inteligentes y tabletas pequeñas táctiles. Es el sucesor de Windows Phone e incluirá nuevas versiones de Office optimizadas para dispositivos móviles.

**Windows 10 Pro** es una edición de escritorio para PCs, tabletas y 2-en-1 s. Será el equivalente a Windows 8 Pro, orientado para empresas y con acceso al programa de actualización Windows Update for Business, la versión para profesionales y programadores y uso comercial.

Con el fin de evitar las molestias que generalmente ha causado Windows Update, como por ejemplo **iniciarse en el momento menos oportuno** mientras se está trabajando o incluso **reiniciar el ordenador**. Los usuarios podrán **marcar las horas para actualizarse (noche o fuera de horario)**. para interrumpir lo menos posible con su trabajo diario.

**Windows 10 Enterprise** Está pensada en empresas de tamaño medio y grande. Se basa en Windows 10 Pro, por lo que ofrece todas las funciones del mismo y además otras específicamente diseñadas para los usuarios de empresas de mayor tamaño. Estará disponible mediante **licencias por volumen**, y quienes adquieran esta versión también podrán elegir la velocidad a la que recibir futuras actualizaciones del sistema operativo (una característica muy demandada en entornos corporativos).

**Windows 10 Mobile Enterprise** . Está orientada a las grandes empresas para que todos los «smartphones» y «tablets» compartan la licencia del sistema operativo, por lo tanto, estará disponible a través de las licencias por volumen. La premisa es que haya «formas flexibles de que las empresas gestionen las actualizaciones»

**Windows 10 Education** Es una adaptación de la Entreprise y orientada a entidades educativas y académicas. Esta edición estará disponible con licencias por volumen para educación.

# LA PARTICIÓN DE 500 MB.

Si instalamos Windows 10 en un disco duro sin particiones, veremos que crea una partición de 500 MB y la reserva para el sistema. A esta pequeña partición no se le asigna ninguna letra de unidad así que el usuario normalmente ni siquiera se da cuenta de que esta creada a menos que usemos el gestor de discos (DISKMGMT.MSC).

Esta partición sirve para dos funciones. En primer lugar, almacena los ficheros de inicio del sistema y la base de datos de configuración del inicio (BCD). En segundo lugar, almacena la información requerida para usar la encriptación de volúmenes.

# Principios de Seguridad en Windows

En la mayoría de los sistemas operativos actuales, aparecen dos conceptos relacionados con la seguridad del sistema: Autentificación y Autorización.

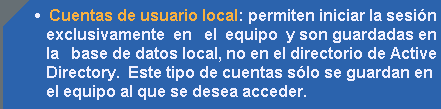
* **Autentificación:** Para usar el sistema es necesario abrir una sesión de trabajo (login) para lo cual tendremos que autentificarnos, proporcionando al sistema un nombre de usuario y una contraseña. En caso de no tener una cuenta de usuario abierta en el sistema, será imposible entrar en el mismo.
* **Autorización**: Una vez que el usuario se ha autentificado y abierto sesión, cada vez que quiera usar un recurso (un fichero, una carpeta, una impresora, etc) el sistema comprobará si esta autorizado o no para realizar esa acción. Los administradores del sistema pueden modificar estas autorizaciones mediante unas listas de acceso.

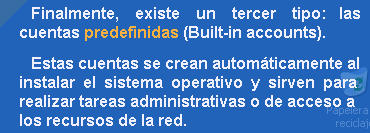
## Gestión de Cuentas de Usuario y Grupos.

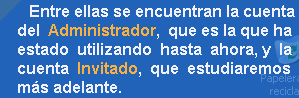
Podemos crear, borrar y modificar cuentas de usuario en Windows usando varios programas distintos.

* Asistente para cuentas de usuario desde Panel de Control.
* Gestión de cuentas de usuarios locales y grupo mediante consola.
* Gestión de cuentas de usuarios mediante consola especial.
* Desde el shell de texto.
* **Usuarios locales.**

Un usuario local es una cuenta a la que se puede conceder permisos y derechos para el equipo donde se está creando la cuenta. Está disponible en equipos que no son controladores de dominio, no pueden usarse para conectarse a ningún dominio..







### Asistente para cuentas de usuario desde Panel de Control

Para abrir la herramienta Cuentas de usuarios, hay que abrir el Panel de control desde el menú Inicio y, a continuación Cuentas de usuario.

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamenteDesde aquí podemos crear cuentas, modificarlas, cambiar contraseñas, gráficos asociados a la cuenta, etc.

Nota: No se puede borrar una cuenta de un usuario si tiene sesión abierta en el sistema.

Aunque con distintas prestaciones, básicamente esta aplicación es igual entre Windows 2008 server, windows 10, windows 2012 server etc.

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

### Gestión de cuentas de usuarios locales y grupos mediante consola.

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamenteLa segunda opción que tenemos para gestionar cuentas de usuario, es la opción más interesante de todas las que nos ofrece Windows, y la más potente. Es la consola de usuarios locales y grupos. Podemos llegar a dicha consola de varias formas, aunque la más rápida es\_

* Inicio – Ejecutar y escribir ó tecla de Windows+R **LUSRMGR.MSC**

Lleguemos desde donde lleguemos, veremos que tenemos dos carpetas, una para los usuarios y otra para los grupos.

Podemos crear usuarios nuevos accediendo a las propiedades de la carpeta usuarios (botón derecho sobre ella) y seleccionando la opción de Usuario Nuevo. Podemos modificar un usuario accediendo a sus propiedades. Del mismo modo podemos crear nuevos grupos y modificar los ya existentes.

Podemos tanto asignar a un usuario varios grupos, como asignar a un grupo varios usuarios.

Podemos crear todas las cuentas de usuarios que deseemos, pero aparte de estas cuentas normales, existen dos cuentas de usuario especiales en Windows, ya creadas y que no pueden (no deben) ser modificadas o eliminadas.

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

* La cuenta del Administrador del sistema (Administrador). Todos los sistemas Windows tienen una cuenta especial conocida como Administrador. Esta cuenta tiene todos los derechos sobre todo el equipo. Puede crear otras cuentas de usuario y es el responsable de gestionar el sistema. Muchas funciones del sistema están limitadas para que solo puedan ser ejecutadas por el Administrador. Es posible crear cuentas de usuario y darles los mismos derechos que la cuenta Administrador (integrándolas como miembros del grupo Administradores), aunque Administrador solo puede haber uno. Esta cuenta siempre debe contar con contraseña y se crea en el momento de la instalación del sistema.
* La cuenta de Invitado. (Guest). Es la contraria a la cuenta de Administrador, está totalmente limitada, no cuenta apenas con ningún permiso o derecho, pero permite que cualquier usuario pueda entrar en nuestro sistema sin contraseña (lo que se denomina acceso anónimo) y darse un “paseo” por el mismo. Por defecto, en Windows esta cuenta esta desactivada. Es altamente recomendable nunca activar dicha cuenta, ya que representa un riesgo altísimo de seguridad.

Si comprobáis el título de esta última consola, veréis que aparece la palabra local en el mismo. Esto es así porque se distinguen dos ámbitos al hablar de usuarios:

Los usuarios locales y los usuarios de dominio. Mientras no tengamos instalado un dominio (para lo cual necesitaremos algún servidor Windows como 2008,2012,2016,2019 server) siempre estaremos trabajando con cuentas locales.

**CÓMO CREAR usuarios locales.**

Para crear usuarios locales, siga los pasos siguientes:

* Seleccione**: InicioHerramientas Administrativas Administrador del servidor.**

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

* Despliegue **Configuración,** después Usuarios y grupos locales y verá su contenido, Usuarios y Grupos.
* Pulsa el botón izquierdo del ratón sobre Usuarios y, en el panel derecho, le mostrará los usuarios que hay dados de alta en el equipo.

Interfaz de usuario gráfica, Texto, Aplicación

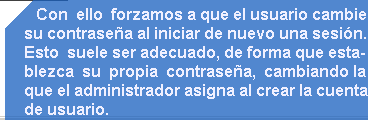
Descripción generada automáticamente

* **Seleccione Usuario nuevo** del menú contextual de Usuarios y le mostrará la siguiente pantalla:

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

* **Indica el nombre** que desea dar al usuario para conectarse, con un máximo de 20 caracteres; su nombre completo debe ser único en el dominio y tener 64 caracteres como máximo: es necesario seguir una norma ya que cuando se ordenen por el nombre completo será más fácil su búsqueda, por tanto, que todos empiecen por el nombre del usuario o todos empiecen por su primer apellido; una breve descripción; su contraseña, con un máximo de 14 caracteres distinguiendo entre mayúsculas y minúsculas; la confirmación de la contraseña y active las casillas que desee de las siguientes.
  1. **El usuario debe cambiar la contraseña en el siguiente inicio de sesión**. Esta opción obligará al usuario a cambiar la contraseña, que le puso al darle de alta en el equipo, la próxima vez que inicie una sesión. Cuando el usuario inicie sesión la próxima vez se verá obligado a cambiar su contraseña.



* 1. **El usuario no puede cambiar la contraseña**. Esta opción evita que los usuarios puedan modificar su contraseña.
  2. **La contraseña nunca expira**. Al activar esta casilla, se evita que la contraseña pueda caducar y, en consecuencia, que deba cambiarla el usuario.
  3. **Cuenta deshabilitada**. Al activar esta casilla, nadie puede iniciar una sesión con el nombre de este usuario (por ejemplo, cuando el usuario se va de vacaciones, puede deshabilitarla para que nadie pueda tener acceso a sus recursos).
* Cuando haya finalizado, pulse en **Crear** y ya estará creada la cuenta.

**CÓMO MODIFICARLOS.**

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamenteSi accedemos a las propiedades de un usuario, veremos cómo tenemos tres pestañas con las que trabajar, en windows 2008 server tenemos más pestañas.

* **General**: Podemos indicar el nombre completo de la cuenta, una descripción, e indicar algunas opciones de la cuenta.

El usuario debe cambiar la contraseña en el siguiente inicio de sesión. Cuando el usuario inicie sesión la próxima vez se verá obligado a cambiar su contraseña.

El usuario no puede cambiar la contraseña. Prohibimos que el usuario pueda cambiar su contraseña.

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamenteLa contraseña nunca caduca. Ya veremos cómo en Windows las contraseñas se consideran material fungible, es decir, que tras un cierto tiempo de uso el sistema obligará a cambiar dichas contraseñas. Mediante esta opción indicamos que la contraseña podrá usarse sin que caduque nunca.

Cuenta deshabilitada: No borra la cuenta, pero impide que sea usada. Es el estado por defecto de la cuenta Invitado.

La cuenta está bloqueada: Normalmente esta casilla está desactivada y, en caso de estar activada, se utiliza para desbloquear una cuenta que se ha bloqueado por haber intentado iniciar una sesión un número excesivo de veces sin introducir la contraseña correcta. No se puede utilizar para bloquearla; para ello está el apartado Cuenta deshabilitada.

* **Miembro de**: Desde esta pestaña podemos introducir al usuario en grupos. Los grupos se usan para dar permisos y derechos a los usuarios fácilmente, sin tener que ir usuario por usuario. Así, por ejemplo, si introducimos a un usuario como miembro del grupo Administradores, le estaremos dando todos los permisos del grupo Administradores.

Interfaz de usuario gráfica

Descripción generada automáticamenteEn la pestaña miembro de veremos todos los grupos a los que el usuario pertenece actualmente. Si le damos al botón **agregar** podremos escribir directamente el nombre de un grupo donde agregarlo. Si queremos escoger dicho grupo de una lista de los grupos posibles, hay que escoger la opción **Avanzada** y luego **Buscar ahora**, que nos mostrará una lista de todos los grupos del sistema. Basta con seleccionar el que queramos (o los que queramos) y pulsar aceptar.

* **Perfil**: Nos permite indicar la ruta del perfil, los archivos de inicio de sesión y las carpetas personales del usuario. Como en un apunte posterior veremos el tema de perfiles, de momento lo dejamos pendiente.
* Si marca en **Entorno**, verá una pantalla en la que se podrá configurar el entorno de inicio de los **Servicios de Terminal Server** del usuario.
* Si marca en **Sesiones**, verá una pantalla en donde se pueden configurar las opciones de tiempo de espera y reconexiones de los **Servicios de Terminal Server** del usuario.
* Si marca en **Control remoto**, verá una pantalla en donde se pueden configurar el control remoto de los **Servicios de Terminal Server** del usuario.
* Si marca en **Perfil de Servicios de Terminal Server**, verá una pantalla en donde se pueden configurar el perfil de usuario de los **Servicios de Terminal Server** del usuario.
* Si marca en **Marcado**, verá una pantalla en donde se pueden configurar el uso del **Acceso telefónico a redes** del usuario.

**CÓMO CAMBIAR SU NOMBRE.**

* Seleccione**: InicioHerramientas Administrativas Administrador del servidor.**
* Despliegue **Configuración,** después Usuarios y grupos locales y verá su contenido, Usuarios y Grupos.
* Pulsa el botón izquierdo del ratón sobre Usuarios y, en el panel derecho, le mostrará los usuarios que hay dados de alta en el equipo.
* Sitúese sobre el usuario al que desea cambiar el nombre, muestre su menú contextual, seleccione **Cambiar Nombre**, indique el nombre que desea darle.

**CÓMO MODIFICAR SU CONTRASEÑA.**

La manera mejor de cambiar la contraseña de los usuarios es con la opción **Cambiar una contraseña** que se obtiene pulsando [Ctrl]+[Alt]+[Supr], pero es necesario conocer la contraseña anterior del usuario. Si no se conoce la contraseña anterior no se puede utilizar dicha opción y se debe realizar siguiendo los pasos siguientes.

* Seleccione**: InicioHerramientas Administrativas Administrador del servidor.**
* Despliegue **Configuración,** después Usuarios y grupos locales y verá su contenido, Usuarios y Grupos.
* Pulsa el botón izquierdo del ratón sobre Usuarios y, en el panel derecho, le mostrará los usuarios que hay dados de alta en el equipo.
* Sitúese sobre el usuario al que desea cambiar su contraseña, muestre su menú contextual, y seleccione **Establecer Contraseña**, le mostrará un mensaje de aviso en el cual le indica que es mejor utilizar la opción **Cambiar una contraseña** que se obtiene pulsando [Ctrl]+[Alt]+[Supr], pulse en continuar y indique la nueva contraseña , confírmela y pulse aceptar.

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

**GESTIÓN DE CUENTAS DE USUARIO MEDIANTE CONSOLA ESPECIAL.**

Podemos también gestionar las cuentas de usuario mediante una consola especial, normalmente oculta. Para acceder a dicha consola, hay que ejecutar la siguiente orden desde una ventana del intérprete de comandos:

Control userpasswords2 o también se puede ejecutar NETPLWIZ.



Con este gestor de cuentas de usuario, tenemos un control especial sobre los usuarios, permitiéndonos realizar algunas acciones que no son accesibles desde ningún otro sitio.

La primera opción que vemos en pantalla, “Los usuarios deben escribir su nombre y contraseña para usar el equipo” nos permite indicar si queremos usar la autentificación o no.

Si lo desactivamos, obtendremos un Windows que se iniciará automáticamente con la cuenta que indiquemos sin mostrarnos siquiera la pantalla de bienvenida. Si tenemos varios usuarios, en el momento en que desactivemos dicha casilla y pulsemos aceptar o aplicar, nos preguntará el sistema por el usuario a cargar automáticamente.

Obviamente, esta opción solo debería usarse en ambientes domésticos donde solo un usuario usa el ordenador.

Para agregar cuentas de usuario usamos el botón agregar, para eliminar cuentas el botón quitar, etc. Si seleccionamos una cuenta de usuario y pulsamos el botón propiedades, pasamos a sus propiedades.

Desde esta pantalla de propiedades, podemos observar cómo podemos incluir al usuario en algún grupo de usuarios, bien uno de los dos incluidos en el gestor (usuarios estándar y usuarios restringidos) o bien seleccionando otro grupo como puede ser el de administradores, etc.

En la pestaña opciones avanzadas de este gestor, podemos ver opciones muy interesantes como la administración de nuestras contraseñas, un botón que nos lleva a LUSRMGR.MSC, obligar a utilizar el inicio de sesión seguro, etc.

Una opción muy interesante, (y muy peligrosa y poco segura) que nos podemos encontrar en la primera pantalla es la posibilidad de cambiar la contraseña de cualquier usuario, incluido el usuario administrador. Para hacerlo, basta con que nos hayamos autentificado con una cuenta de usuario que pertenezca al grupo Administradores. Esta opción ha sido incluida ya que a veces los usuarios olvidan con el tiempo la contraseña que le asignaron a la cuenta de Administrador en el momento de la instalación del equipo, y es a su vez la causante de que Microsoft oculte esta consola para que no sea ejecutada por los usuarios normales.



### Gestión de Cuentas de Usuario desde el Interfaz de línea de comandos de Windows (CLI).

La última opción para gestionar las cuentas de usuario, es hacerlo directamente desde el Shell de texto o interfaz de línea de comandos (CLI). Esta opción puede parecer la más engorrosa, pero resulta ser la más práctica y potente en muchísimas ocasiones, sobre todo si conocemos como hacer scripts de sistema.

**Desde una Shell de texto con el usuario administrador.**

**Texto

Descripción generada automáticamente**

Para ello disponemos de una orden que nos permiten gestionar las cuentas de usuario:

net user

Este comando nos permite consultar, agregar o modificar cuentas de usuario.

Su sintaxis es la siguiente:

* net user [***nombredeusuario*** [***contraseña*** | **\***] [opciones]]
* net user ***nombredeusuario*** [***contraseña*** | **\***] **/add** [*opciones*]
* net user [***nombredeusuario*** [**/delete**] [**/domain**]]

Expliquemos los parámetros de la orden que hemos visto en la sintaxis.

*Nombredeusuario:* Específica el nombre de la cuenta de usuario que se desea agregar, eliminar, modificar o consultar. El nombre de la cuenta de usuario puede tener hasta 20 caracteres.

*Contraseña:* Asigna o cambia una contraseña para la cuenta de usuario. Escribimos un asterisco (\*) si deseamos que se nos pida la contraseña. Los caracteres de la contraseña no se muestran en la pantalla a medida que los escribimos, así que hay que tener cuidado.

/add: Agrega el usuario al sistema.

/delete: Borra el usuario del sistema.

Si al ejecutar la orden desde la línea de comandos (CMD) obtenemos el error de sistema 5 (acceso denegado) es porque estamos ejecutando una línea de comandos sin ser administrador.

Para evitar esto, haced un acceso directo a CMD en el escritorio, y lanzadlo con botón derecho – Ejecutar como Administrador. (Truco: También podemos escribir CMD en el botón inicio (Windows – escribir CMD) y en lugar de pulsar INTRO pulsamos CONTROL – MAYUSCULAS – INTRO con lo que conseguiremos que lo que ejecutemos se ejecute como Administrador).

Ejemplo:

**COMANDOS NET:**

* **CLS🡪 Borrar pantalla**
* **Net help 🡪 ayuda nosotros veremos la parte de crear usuarios y crear grupos.**
* **Net share🡪 Es para ver las carpetas que tenemos compartidas**
* **Net user 🡪 Nos muestra los usuarios que tenemos creados ya.**
  + **Net user ana 🡪 visualiza la información del usuario indicado**
  + **Net user domain—> Nos visualiza los usuarios que tenemos creados en el dominio cuando tenemos un dominio.**

**AÑADIR O CREAR USUARIOS LOCALES.**

* **Net user Luis \* /ADD 🡪 Nos pide por teclado la contraseña que va a tener este usuario y asi no se ve en el fichero o en la orden tecleada.**
* **Net user Luis Prueba1. /ADD🡪 Se crea el usuario Luis con contraseña Prueba1.**
* **Net user mama P@ssw0rd /logonpasswordchg:yes /fullname:”cuenta de mama” /ADD 🡪 crea el usuario mama con password .**
  + - **/logonpasswordchg:yes /no Con esto establecemos que en el próximo inicio de sesión el usuario deberá cambiar la contraseña.**
    - **/fullname:”cuenta de mama” con esto establecemos que el nombre completo del usuario será lo que pongamos entre comillas.**

**BORRAR USUARIOS**

**Net user Luis /delete**

Vemos en la sintaxis, como además de los elementos anteriores podemos escribir algunas opciones. Las opciones más utilizadas son las siguientes:

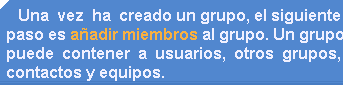
Tabla

Descripción generada automáticamente

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Obviamente la mayor potencia de la interfaz de línea de comandos, (shell de texto o CLI) aparece cuando usamos scripts. Estos scripts son pequeños programas que podemos realizar con un editor de texto y que se ejecutan directamente en nuestro sistema operativo.





**CREACIÓN DE GRUPOS.**

* Net localgroup familia /add 🡪 nos crea un grupo local con nombre familia
* Net localgroup 🡪 visualiza los grupos creados
* Net localgroup familia /delete 🡪 Eliminamos el grupo familia
* Net localgroup familia 🡪 Nos visualiza los usuarios que pertenecen al grupo familia

**AÑADIR USUARIOS AL GRUPO CREADO**

**Net localgroup “nombre del grupo” “nombre de los usuarios que queramos que pertenezcan a este grupo” /add**

Texto

Descripción generada automáticamente

### Gestión de las contraseñas.

Windows es un sistema operativo muy configurable por parte del usuario. Aunque estas configuraciones suelen estar algo ocultas para que no sean accesibles por los usuarios normales, y solo pueden ser modificadas desde las consolas del sistema.

* Interfaz de usuario gráfica, Texto, Aplicación

  Descripción generada automáticamenteEn concreto, desde la consola de Configuración de Seguridad Local, podemos gestionar varios aspectos sobre las contraseñas. Esta consola se denomina **SECPOL.MSC**, y para gestionar las contraseñas, debemos entrar en Configuración de Seguridad, Directivas de Contraseña. **: InicioHerramientas Administrativas Directiva de Seguridad local.**

Las configuraciones más útiles que podemos gestionar desde aquí son:

* Forzar el historial de contraseñas. Impide que un usuario cambie su contraseña por una contraseña que haya usado anteriormente, el valor numérico indica cuantas contraseñas recordará.

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

* Las contraseñas deben cumplir los requerimientos de complejidad. Obliga a que las contraseñas deban cumplir ciertos requerimientos, como son mezclar letras mayúsculas, minúsculas y números, no parecerse al nombre de la cuenta, etc.

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

* Longitud minina de la contraseña. Indica cuantos caracteres debe tener la contraseña como mínimo, un valor cero en este campo indica que pueden dejarse las contraseñas en blanco.

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

* Vigencia máxima de la contraseña. Las contraseñas de los usuarios caducan y dejan de ser validas después del número de días indicados en esta configuración, y el sistema obligará al usuario a cambiarlas. (Recordemos que al crear una cuenta de usuario podemos indicar que la contraseña nunca caduca para esa cuenta).
* Vigencia minina de la contraseña. Indica cuanto tiempo debe transcurrir desde que un usuario se cambio la contraseña, hasta que puede volver a cambiarla.

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

### Bloqueo de las cuentas.

* Desde la Configuración de seguridad local (secpol.msc) también podemos gestionar el comportamiento de las cuentas de usuario relacionado con las contraseñas, y por ejemplo bloquear las cuentas si se intenta acceder al sistema con las mismas, pero usando contraseñas incorrectas. Esta configuración la encontramos en Configuración de Seguridad – Directivas de Cuenta – Directivas de Bloqueo de Cuentas) **InicioHerramientas Administrativas Directiva de Seguridad local Directivas de bloqueo de cuentas.**

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Aquí podemos configurar:

* Duración del bloqueo de cuenta. (Durante cuanto tiempo permanecerá una cuenta bloqueada si se supera el umbral de bloqueo. Un valor cero indica que la cuenta se bloqueará hasta que un Administrador la desbloquee).
* Restablecer la cuenta de bloqueos después de. (Indica cada cuanto tiempo se pone el contador de intentos erróneos a cero).
* Umbral de bloqueo de la cuenta. (Indica cuantos intentos erróneos se permiten antes de bloquear la cuenta).

## IDENTIFICADOR DE SEGURIDAD O SID.

* Imaginad que creamos una cuenta en nuestro equipo con nombre PACO y contraseña P1c4. Creamos varias carpetas que solo le pertenecen a PACO, ciframos archivos para que solo los pueda leer PACO, etc. Un día por error borramos la cuenta PACO y todas esas informaciones quedan “huérfanas”.

Ni cortos ni perezosos decidimos crear otra vez la cuenta PACO con contraseña P1c4, para intentar acceder a dichos ficheros y carpetas. Pues bien, comprobaremos que nuestro sistema sabe perfectamente que ese nuevo PACO no tiene nada que ver con el antiguo PACO, y los considera usuarios totalmente distintos y no le deja acceder a los ficheros.

Esto es así porque el sistema operativo no usa para referirse a las cuentas su nombre y su contraseña, esos son campos que usamos nosotros, al igual que nos llamamos entre nosotros con nuestro nombre, pero la administración nos conoce por nuestro DNI.

El DNI que usa el sistema para referirse a las cuentas de usuario se denomina SID. (Security IDentifier o Identificador de Seguridad).

Un SID es algo parecido a lo siguiente:

S-1-5-21-448539723-413027322-839522115-1003

El último número, en este caso 1003 se conoce como RID (identificador relativo del usuario) y todo lo que está delante del mismo identifica el dominio al que pertenece ese usuario.

En concreto, esos tres grandes números que se observan (448539723-413027322-839522115) se generan automáticamente y al azar cada vez que instalamos un Windows, y aparecerán en todas las cuentas que creemos en dicho sistema.

En Windows anteriores a XP no se podía clonar un equipo debido al SID, sin embargo, Windows desde la versión Vista no presenta problemas en repetir el SID en varias máquinas.

La parte del SID S-1-5-21 nos da información sobre el objeto con el que estamos trabajando. Así por ejemplo si hablamos de algunos grupos o usuarios especiales tenemos:

S-1-1-0 es el SID del grupo Todos (Everyone)

S-1-2-0 es el SID del grupo Usuarios locales

S-1-3-1 es el SID de Creator – Owner

S-1-5 Este inicio de SID nos indica que estamos trabajando con un usuario o grupo normal. Dentro de este grupo algunos SID conocidos son:

S-1-5-32-544 SID del grupo Administradores

S-1-5-32-545 SID del grupo Usuarios

El RID del Administrador siempre es el 500.

Es posible ver los SID que se le asignan a nuestros usuarios y grupos con la orden **whoami.exe**. Si veis que Windows no reconoce este comando, se puede instalar desde el CD de Windows o bien desde Internet, aunque normalmente si se reconoce. Para ello, introducid el CD de Windows 10 en la unidad de CD con el sistema en marcha, explorad dicho CD y ejecutar el programa SETUP que está en la carpeta \SUPPORT\TOOLS. Esto instalará en vuestro sistema varias herramientas, entre las cuales estará el comando WHOAMI.EXE.

Una vez instalado, abrid un shell, y ejecutad la siguiente orden:

whoami /USER

Que os responderá algo como lo siguiente:

[User]="SIS\Joan" S-1-5-21-448539723-413027322-839522115-1003

Texto

Descripción generada automáticamente

Podemos ver aquí como nos dice el nombre de nuestro usuario actual y además nos indica que SID le ha sido otorgado por el sistema.

Si queremos ver no solo el SID que se le ha otorgado a nuestro usuario, sino el SID de todos los grupos a los que pertenece nuestro usuario, usad la orden con los parámetros /GROUPS.

Whoami solo nos muestra información sobre el usuario actual, así que, si queremos ver los SID de distintos usuarios, tendremos que ejecutar dicha orden como dichos usuarios.

Aprovecho aquí para comentaros una orden que a veces es muy útil. En lugar de tener que ir cerrando y abriendo sesión con cada usuario, podemos “hacernos pasar” por dicho usuario sin tener que cerrar sesión, ni abrir sesión, ni nada. Para ello usaremos la orden runas (ejecutar como si fuera).

Para ellos, abrid un shell y ejecutad la orden: RunAs /user:usuario\_a\_suplantar cmd

Texto

Descripción generada automáticamente

Con esto conseguiremos abrir una nueva shell en la que seremos el usuario que estamos suplantando, por lo que si ejecutamos en dicha ventana whoami nos responderá con el nuevo usuario.

Texto

Descripción generada automáticamente

Abrimos una nueva sesión de cmd ya que si ejecutamos directamente runas whoami se ejecutaría la orden, pero no veríamos nada.

En caso de que tampoco contemos con la orden runas en nuestro equipo, podemos instalarla con algunos de los métodos que explicamos para whoami.

**AUTOMATIZAR LA CREACIÓN DE USUARIOS**

Ahora que hemos aprendido a crear usuarios desde línea de comando, vamos a Automatizar el proceso.

Para ello con el notepad creamos un fichero con nombres de personas.

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Lo guardamos con codificación Unicode y con un nombre alumnos.txt.

Ahora creamos otro fichero llamado alta.cmd con el notepad con los siguientes datos. Tipo ANSI

Texto

Descripción generada automáticamente

UN BUCLE:

Sintaxis:

FOR **/F** ["*options*"] %%*parameter* IN (*filenameset*) DO *command*

FOR **/F** ["*options*"] %%*parameter* IN ("Text string to process") DO *command*

%%i es la variable I que va a ir tomando los distintos valores que se le van a pasar en el fichero alumnos.txt

Do detrás del do se le dice lo que queremos que ejecute con cada uno de los valores de i.

Tokens= es como decirle que tenemos dos campos definidos en el fichero de datos de alumnos

Delims= le decimos que carácter vamos a utilizar para separar un campo de otro, es decir para separar el nombre del alumno de la contraseña utilizo una ,

Usebackq= este delimitador es para decirle que en el type utilizo las comas invertidas.

Type alumnos.txt = le decimos que nos visualice el contenido del fichero indicado.

Interfaz de usuario gráfica, Texto

Descripción generada automáticamente

Para ejecutar el fichero ponemos alta.

Ya vemos en la imagen como nos coge los nombres del fichero y nos los muestra, ahora solo nos queda decirle que en vez de mostrar los nombres cree las cuentas de cada uno de los usuarios en el sistema.

Esto se lo decimo con el do( net user….. )

Texto

Descripción generada automáticamente

Texto

Descripción generada automáticamente

Si ahora nos vamos a usuarios, tendremos los usuarios creados

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Otra forma de crear usuarios sin tener un fichero con los nombres de los usuarios

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Texto

Descripción generada automáticamente

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

## Recursos Locales. Gestión de ACL

Llamamos recursos de un sistema a los distintos elementos con los que ese sistema cuenta para que sean usados por los usuarios.

Así, una impresora, una carpeta, un fichero, una conexión de red son recursos.

Bien, pues cada recurso cuenta con una lista donde aparecen los usuarios que pueden usar dicho recurso y de qué forma pueden usarlo.

Ya hemos visto que el sistema no ve usuarios y grupos, realmente ve Identificadores de Seguridad (SID), de modo que dicha lista realmente tendrá en su interior una serie de SIDs y los permisos que cada uno de esos SIDs tiene sobre el recurso.

Esta lista con la que cuenta cada recurso se conoce como **ACL** (Access Control List, o **Lista de Control de Acceso**).

Cuando un usuario intenta acceder a un recurso, pide autorización al recurso para hacerlo. El recurso comprobará entonces si en su ACL aparece el SID del usuario, y en caso contrario, comprobará si en su ACL aparece el SID de algún grupo al que pertenezca el usuario.

Si no aparece en la ACL ningún SID del usuario, el recurso niega el acceso al usuario.

Si aparece en la ACL algún SID del usuario, el recurso comprueba si la acción que quiere realizar el usuario (leer, borrar, escribir, etc.) está permitida para ese SID en su ACL, si lo está le autoriza para hacerlo, en caso contrario se lo impide.

Diagrama

Descripción generada automáticamente

Puede ocurrir que un usuario tenga permisos contradictorios… imaginemos que en el ACL de la carpeta margarita aparece que el SID del usuario PACO puede escribir en la carpeta, pero PACO pertenece al grupo PROFESORES que aparece en el ACL de margarita como que no tiene derecho a escribir. Bien, en este caso se aplica la siguiente regla:

Interfaz de usuario gráfica, Aplicación, Correo electrónico

Descripción generada automáticamente

1. Lo que más pesa en cualquier ACL es la denegación implícita de permisos. Si un permiso esta denegado, no se sigue mirando, se deniega inmediatamente.
2. Basta con que un permiso este concedido en cualquier SID para que se considere concedido. (A excepción de la regla 1, es decir, que no esté denegado implícitamente en ningún sitio)

Esto se entiende mejor gestionando el ACL de algún recurso.

Por ejemplo, creemos en la raíz de nuestro volumen (en NTFS) una carpeta con nombre MARGARITA. Una vez creada, accedemos a sus propiedades y en ellas a la pestaña Seguridad:

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Podemos ver como en la parte superior tenemos las SID a las que concedemos permisos (usuarios y grupos) y en la parte inferior tenemos los permisos concretos que le concedemos a dicha SID. Si veis las dos columnas por cada permiso, podemos tanto Permitir como Denegar un permiso.

La denegación de un permiso es la que más pesa, y se aplica inmediatamente. De hecho, se aconseja no denegar permisos NUNCA, a menos que sea absolutamente necesario.

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

Si damos al botón Editar.

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

Con los botones agregar y quitar podemos añadir o quitar SID de la

ACL.

En la parte inferior podemos pulsar en las casillas de Permitir y Denegar para dar y quitar permisos.

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

¿Pero… por que aparece la columna de Permitir en gris y no nos deja cambiarla?

Porque son permisos heredados de la carpeta superior. Bien, ha llegado el momento de hablar de la herencia.

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Imaginemos que creamos una carpeta por ejemplo CONTABLES, y la preparamos minuciosamente para que pueden leer y escribir en ella los usuarios que sean miembros del grupo CONTABLES, para que solo puedan leer los del grupo JEFES pero no escribir, y que los demás usuarios no puedan ni leer en ella ni escribir.

Bien, si ahora dentro de la carpeta CONTABLES creamos una nueva carpeta INFORMES, ¿no sería lógico que esta carpeta INFORMES “heredara” la ACL de su carpeta madre CONTABLES para que no tuviera que configurarla nuevamente?

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Interfaz de usuario gráfica, Texto, Correo electrónico

Descripción generada automáticamenteInterfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Interfaz de usuario gráfica, Texto, Correo electrónico

Descripción generada automáticamente

La carpeta Informes tiene los mismos permisos que contables.

Interfaz de usuario gráfica, Aplicación, Correo electrónico

Descripción generada automáticamente

Pues precisamente eso es lo que hace Windows, cualquier recurso que creemos, heredará automáticamente la ACL de su recurso padre si es que existe.

En nuestro caso, la carpeta MARGARITA ha heredado la ACL de la raíz de nuestro volumen. De modo que no podremos quitar usuarios, quitar permisos, etc.

Para realizar cambios en la ACL de nuestra carpeta MARGARITA, debemos indicarle que “rompa” la herencia, es decir, que deseamos retocar manualmente su ACL.

Para ello, accedemos al botón de **Opciones Avanzadas** que está en la pestaña Seguridad.

Interfaz de usuario gráfica, Texto

Descripción generada automáticamente

Podemos ver en estas opciones avanzadas cuatro pestañas, de momento nos quedamos en la primera, **permisos**.

Vemos como en la parte inferior de esta ventana, está marcada la opción de “Heredar del objeto principal las entradas de permiso relativas a los objetos secundarios. Incluirlas junto con las entradas indicadas aquí de forma explícita”. Si desmarcamos dicha opción mataremos la relación de herencia de nuestro recurso, y podremos gestionar su ACL “a pelo”. Hagámoslo.

Para ello nos vamos a cambiar permisos.

Interfaz de usuario gráfica, Texto, Correo electrónico

Descripción generada automáticamente

Cuidado ahora, una vez quitada la herencia, el sistema nos da a elegir entre dos opciones:

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Si escogemos la opción **convertir los permisos heredados en permisos explícitos en este objeto,** la herencia se interrumpirá, y podremos retocar la ACL como nos plazca, pero dicha ACL será la que ahora mismo tiene el recurso, heredada de su objeto principal.

Si escogemos la opción **Quitar todos los permisos heredados de este objeto**, la ACL se borrará totalmente, se interrumpirá la herencia y la podremos crear desde cero.

Si elegimos quitar y empezar desde cero, hay que tener en cuenta que en las ACL no solo deben aparecer nuestras SID normales, sino que grupos como Creator Owner o System son necesarios para que el sistema pueda trabajar sin problemas con dichas carpetas. Si quitamos estos SID tendremos problemas en el futuro (copias de seguridad, auditorias, etc.).

Vemos como debajo de la opción de Habilitar herencia, tenemos otra opción que nos permite activar que los objetos por debajo del nuestro hereden las modificaciones que hagamos en nuestra ACL. Esto es importante tenerlo en cuenta si queremos que los cambios que hagamos en la ACL se repliquen en los objetos hijos del nuestro, ya que hemos roto la herencia y a veces tendremos que forzar dichos cambios.

**Realizad los siguientes ejercicios:**

**Ejercicio1**

Creamos una carpeta en C llamada CARPETA1 y miramos los permisos que tiene.

Ahora dentro de esta carpeta creamos otra carpeta llamada CARPETA11 ¿Que permisos tiene?

Ahora modificamos los permisos de CARPETA1 ejemplo: quitamos usuarios y incluimos un usuario ana con permisos de lectura y escritura. Creamos otra carpeta llamada CARPETA22 ¿Que permisos tiene? ¿Que es la herencia?

PERMISOS

Diagrama

Descripción generada automáticamente

La DACL establece quien y como puede acceder a la carpeta o al archivo.

Internamente la DACL posee 0 o más entradas que pueden ser de dos tipos, heredadas de la carpeta padre o explicitas del propio objeto.

Y donde cada una de estas entradas asocia un permiso concreto a un usuario o grupo representado internamente por el SID.

Fichero informe1.txt tiene dos entradas heredadas y una explicita.

¿QUE PERMISOS EXISTEN?

Hay 2 tipos de permisos Explícitos y Heredados.

Explícitos: Son aquellos que se establecen de forma predeterminada, cuando se crea el objeto.

Heredados: Son aquellos que se propagan a un objeto desde un objeto principal. Los permisos heredados facilitan la tarea de administrar permisos y garantizar la coherencia de los permisos entre todos los objetos.

Interfaz de usuario gráfica

Descripción generada automáticamente con confianza baja

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Permiso de Lectura, permite listar el contenido de una carpeta y acceder en modo lectura a los archivos que contiene.

Interfaz de usuario gráfica, Texto, Aplicación, Chat o mensaje de texto

Descripción generada automáticamente

Permite añadir ficheros y carpetas a una carpeta, y sobre escribir el contenido de un fichero, pero no incluye internamente ningún permiso de lectura por tanto, si solamente tenemos el permiso de escritura, podemos añadir elementos a una carpeta pero no podremos acceder a ellos, así mismo podremos sobrescribir un fichero pero no podremos abrirlo para lectura.

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Este permiso autoriza listar y recorrer carpetas y leer y ejecutar ficheros.

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

En resumen, autoriza recorrer carpetas, crear y borrar carpetas y ficheros y leer, ejecutar y modificar ficheros.

Interfaz de usuario gráfica, Texto, Aplicación, Chat o mensaje de texto

Descripción generada automáticamente

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Finalmente tienes que saber que además de los permisos anteriores se incluye mostrar el contenido de la carpeta solo disponible para carpetas no incluye ningún permiso para los ficheros.



Texto

Descripción generada automáticamente

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Los distintos permisos que se pueden aplicar para cada SID en la ACL no son únicamente los que vemos en las propiedades de la carpeta, si entramos en opciones avanzadas y allí en permisos – agregar veremos cómo podemos indicar otro tipo de permisos.

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamenteEl permiso Recorrer o Atravesar carpeta permite o impide que el usuario pase de una carpeta a otra para llegar a otros archivos o carpetas, incluso aunque el usuario no tenga permisos para las carpetas recorridas (sólo se aplica a carpetas).

El permiso Atributos de lectura o leer atributos permite o impide que el usuario vea los atributos de un archivo o de una carpeta, como sólo lectura y oculto. Los atributos están definidos por el sistema de archivos NTFS..

Interfaz de usuario gráfica, Texto

Descripción generada automáticamente

El permiso Atributos de escritura o Escribir atributos permite o impide que el usuario cambie los atributos de un archivo o de una carpeta, como sólo lectura y oculto. Los atributos están definidos por el sistema de archivos NTFS.

El permiso Leer permisos o permisos de lectura permite o impide que el usuario lea permisos del archivo o de la carpeta, como Control total, Leer y Escribir.

El permiso Tomar posesión permite o impide que el usuario tome posesión del archivo o de la carpeta. El propietario de un archivo o de una carpeta puede cambiar los permisos correspondientes, cualesquiera que sean los permisos existentes que protegen el archivo o la carpeta.

Un permiso muy especial es el de Control Total. Si este permiso se lo otorgamos a un usuario en una carpeta, este usuario podrá eliminar cualquier cosa que haya en esa carpeta, incluso si le denegamos el permiso de eliminación en esos recursos. Hay que tener mucho cuidado al conceder este permiso.

EJEMPLOS:



Diagrama

Descripción generada automáticamente con confianza media

Grupos: (ACL\_Inf\_Mod) (ACL\_Inf\_Leer) (Administradores)

Solucion 1 es la mala.

Imagen que contiene Interfaz de usuario gráfica

Descripción generada automáticamente

Se le niega el permiso de Lectura en la carpeta confidencial al grupo ACL\_inf\_leer.

Imagen que contiene Texto

Descripción generada automáticamente

La segunda solución es la buena.

Interfaz de usuario gráfica, Texto

Descripción generada automáticamente

**Ejercicio2**

Creamos una carpeta llamada CARPETA2 y le dejamos los permisos siguientes:

Gasir: Asi11, Asi22. El grupo tiene los permisos de lectura y ejecución.

Además de asignar CARPETA2 el grupo el usuario Asi11 también se le asigna, pero con los permisos de escritura , lectura y ejecución.

Ahora entras con el usuario Asi22 y intentas crear un fichero en la CARPETA2 ¿Puedes hacerlo? no ¿Por qué? Porque el grupo no tiene permisos.

después entras con el usuario Asi11 y intentas crear un fichero en la CARPETA2 ¿Puedes hacerlo? SI ¿Por qué? Porque el usuario ASI11 tiene permisos de escritura Que es lo que prevalece.

Ahora modificamos los permisos del grupo Gasir. Le denegamos el permiso de escritura. después intentamos entrar con el usuario Asi11 y creamos un fichero ¿Puedes hacerlo? ¿Explica por qué?

**Ejercicio3**

Creamos dos grupos Grupo1: usuario11, usuario12

Grupo2: usuario21, usuario22

Creamos una carpeta en C MARGARITA1. Asignamos a esta carpeta el Grupo1.

Ahora salimos de la sesión del Administrador y entramos con un usuario del Grupo2, usuario21 o usuario22.

Comprobamos si podemos ver el contenido de MARGARITA1

¿Puedes hacerlo? ¿Por qué?

Como Administrador…

Nos vamos a la carpeta MARGARITA1 y quitamos de la ACL el grupo usuarios. ¿Puedes hacerlo? ¿Que tienes que hacer?

Ahora salimos de la sesión del Administrador y entramos con un usuario del Grupo2, usuario21 o usuario22.

Comprobamos si podemos ver el contenido de MARGARITA1

¿Puedes hacerlo? ¿Por qué?

Ahora salimos de la sesión del Administrador y entramos con un usuario del Grupo1, usuario11 o usuario12.

Comprobamos si podemos ver el contenido de MARGARITA1

¿Puedes hacerlo? ¿Por qué? ¿Puedes crear un fichero o carpeta? ¿Por qué?

Entramos como Administrador y modificamos lo necesario para que los usuarios del grupo1 puedan escribir.

Comprobar que los del grupo2 no pueden escribir solo los del grupo1.

**Realizad el siguiente ejercicio:**

Cread 4 usuarios con nombre MELINDA, BELINDA, ROSALINDA y DESIDERIA.

Introducid los 4 usuarios anteriores en el grupo DANZA.

Cread una carpeta en la raíz de vuestro volumen con nombre BAILE.

Modificad su ACL para que sólo puedan leer y escribir en dicha carpeta los miembros del grupo DANZA. Quitad el grupo Administradores, Usuarios, etc.

Dejad los que aparecen en mayúsculas (System) para que no tengamos problemas con la carpeta.

Comprobad abriendo sesión con los usuarios nuevos que efectivamente ellos pueden entrar y escribir en dicha carpeta y los demás usuarios del sistema no. (Podéis hacerlo bien cerrando y abriendo sesión o con Runas, lo que os resulte más cómodo).

Para ver que usuario creó la carpeta, nos vamos a: propiedades de la carpeta, seguridad, opciones avanzadas, propietario.

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Si una carpeta la creamos con usuario determinado X ese usuario tiene permisos sobre dicha carpeta.

Entrar con el usuario MELINDA y crear una carpeta llamada BAILAD.

Bien, ahora tendremos una carpeta “BAILE” donde ni los miembros del grupo Administradores ni el Administrador pueden entrar, leer o escribir.

Es solamente para los usuarios del grupo DANZA… ¿o no?

Es imposible que un usuario en un sistema impida que el Administrador realice alguna función, (siempre que el Administrador sepa lo que es Administrar un sistema, claro). En este caso como Administrador (o miembro del grupo Administradores) podemos hacer lo siguiente:

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamenteAccedemos a las propiedades de la carpeta “rebelde BAILAD”, si bien en ella no podemos modificar nada si podemos acceder a sus propiedades avanzadas, y dentro de dichas propiedades accedemos a Propietario.

Podéis ver como desde aquí podemos cambiar el propietario actual del objeto, e indicar que el propietario actual es el grupo Administradores (o el usuario actual si es del grupo Administradores).

Basta con que seleccionemos el grupo Administradores y marquemos abajo Reemplazar propietario en sub contenedores y objetos y demos aplicar – aceptar. Seremos propietarios de la carpeta.

IMPORTANTE. Siempre que hagamos algo así, dejad como propietario al GRUPO administradores, nunca al usuario Administrador. De esta forma la carpeta no se estropeará si es un perfil.

Basta con que actualicemos la ventana de permisos y ya podremos modificar la ACL del recurso como queramos.

**Realizad el siguiente ejercicio:**

Ya tenemos creados 4 usuarios con nombre MELINDA, BELINDA, ROSALINDA y DESIDERIA.

Introducid los 4 usuarios anteriores en el grupo DANZA.

Cread con el usuario MELINDA una carpeta en la raíz de vuestro volumen con nombre BAILAD.

Modificad su ACL para que sólo puedan leer y escribir en dicha carpeta los miembros del grupo DANZA. Quitad el grupo Administradores, Usuarios, etc.

Comprobar que MELINDA tiene acceso a las carpetas y que puede crear ficheros.

¿Entramos con el usuario Administrador?, ¿Puede ver el contenido de la carpeta? ¿Puede modificar y crear ?. NO puede hacerlo

Ahora tenemos una carpeta que ni el administrador y nadie del grupo administradores puede hacer algo sobre esta carpeta.

El administrador necesita siempre tener el control de todas las carpetas ¿Qué puede hacer?

Lo que puede hacer es modificar el propietario de la carpeta e indicar que el propietario actual es el grupo administradores

Otro ejercicio más para comprobar todo lo visto hasta ahora:

* Crear 2 usuarios con nombre AASIR\_01, AASIR\_02
* Crear un grupo AASIR e introducid dentro los 2 usuarios anteriores
* Abrid sesión como AASIR\_01 y cread una carpeta en la raíz de vuestro volumen con nombre ASI.
* Modificad sus permisos para que solo los miembros del grupo AASIR puedan leer, escribir, etc., en dicha carpeta. Quitad todas las demás SID de su ACL, incluidas las SID especiales.
* Comprobad que nadie fuera del grupo AASIR puede acceder a la carpeta ASI
* Cread un usuario con nombre HACKER y hacedlo miembro del grupo Administradores, pero no del grupo ASIR
* Abrid sesión como el usuario HACKER y modificar los permisos de ASI para que se DENIEGUE el acceso a los miembros del grupo AASIR y se permita el acceso total al grupo Todos.

También podemos gestionar las ACL desde shell de texto, con la instrucción CACLS.EXE y ICALS.EXE (mismo caso que runas y whoami).

Usando cacls al mismo tiempo que runas, podemos crear carpetas usando varios usuarios, modificar sus permisos, etc. Si esto mismo lo hacemos abriendo y cerrando las distintas sesiones nos ocupará mucho más tiempo. NO vamos a ver el CACLS ni el ICALS.

Uno de los principales poderes del Administrador del sistema (y de hecho, de cualquier miembro del grupo Administradores) es que puede tomar posesión de cualquier recurso. Es decir, que el Administrador puede indicarle a cualquier recurso que él es el creador o propietario del recurso, por lo que pasa a tener todos los poderes sobre el mismo.

Para conseguir esto, tenemos que entrar en las opciones avanzadas de la pestaña Seguridad del recurso, y allí irnos a la pestaña Propietario.

Veremos cómo, aunque no tengamos ningún permiso sobre el recurso, desde esta pestaña podemos indicar que el propietario del recurso será el grupo Administradores (recomendado antes que asignar el propietario al usuario individual), bastará entonces actualizar las propiedades del recurso para ver como pasamos a tener todos los poderes.

Como ejercicio, cread un usuario nuevo en el sistema, abrid sesión como dicho usuario (o usar runas), crear una carpeta cualquiera y configurad su ACL para que únicamente el usuario nuevo tenga algún permiso sobre dicha carpeta. Abrid sesión ahora como un miembro del grupo de Administradores y conseguid acceder a la carpeta, para por ejemplo crear un archivo dentro. (Tendremos que tomar posesión de la carpeta para el grupo Administradores, y posteriormente modificar su ACL para insertar nuestra cuenta con permisos de escritura).