TEMA 6

Usuarios

se utilizan para iniciar sesiones en la red y tener acceso a los recursos.

Una cuenta de usuario permite que un usuario inicie sesiones en equipos y/o dominios con una identidad que se puede autenticar y autorizar para tener acceso a los recursos del dominio.

Por tanto, una cuenta de usuario se utiliza para:

* Autenticar la identidad del usuario.
* Autorizar o denegar el acceso a los recursos del dominio.
* Auditar las acciones realizadas con la cuenta de usuario.

USUARIO LOCAL

Un usuario local es una cuenta a la que se pueden conceder permisos y derechos para el equipo en donde se está creando la cuenta.

En el proceso de instalación, se crean cuentas de usuario predefinidas y pueden usarse para iniciar una sesión y tener acceso a los recursos. Estas cuentas son:

* **La cuenta de usuario del Administrador** que le permite administrar el equipo en el que se creó. Esta cuenta puede ser renombrada o deshabilitada pero no puede ser borrada ni quitada del grupo local de Administradores. Es importante renombrar y proteger esta cuenta con una contraseña especial, así como crear otras cuentas de administradores para proteger mejor la seguridad del equipo.
* **La cuenta de usuario del Invitado.** Normalmente, esta cuenta está deshabilitada (y debería permanecer de esta manera) pero puede habilitarse si se desea que alguien pueda conectarse al equipo o dominio con ella (tenga en cuenta que no precisa ninguna contraseña). Esta cuenta puede borrarse y renombrarse.
* **Cuenta del usuario inicial**. Nombre del usuario introducido durante la instalación del SO y que tiene casi los mismos privilegios que el administrador.

Los grupos

agregar a los usuarios de forma que se puedan **asignar privilegios más fácilmente a dichos usuarios y hacer más sencilla su administración.**

se puede incorporar un usuario a uno o a varios grupos teniendo, en cada uno de ellos, **unos permisos determinados que le permitirán realizar distintas funciones**.

Un grupo local es una cuenta a la que se pueden conceder permisos y derechos para el equipo donde se está creando y a la que se pueden agregar usuarios locales, así como usuarios, grupos y equipos de un dominio al que pertenezca el equipo.

Los permisos de directorios

Cuando se establecen los permisos sobre un directorio, se define el acceso de un usuario o de un grupo a dicho directorio y sus archivos.

Estos permisos solo pueden establecerlos y cambiarlos el propietario o aquel usuario que haya recibido el permiso del propietario.

Una vez establecidos los permisos, afectarán a los archivos y subdirectorios que dependan de él (herencia) Si no desea que se hereden, deberá indicarse expresamente cuando se indiquen los permisos



Administración de discos

Herramientas de los discos

Liberar espacio en disco. La liberación de espacio en disco puede mejorar el rendimiento de un equipo y ayuda a liberar espacio en el disco duro. Para ello, identifica los archivos que se pueden eliminar de forma segura y, después, permite elegir entre la eliminación de todos los archivos o de algunos.

Agilizar el acceso a los datos. Con la fragmentación del disco se disminuye el rendimiento global del sistema. Cuando un archivo está fragmentado, al abrirlo el sistema deberá buscar en el disco duro los distintos fragmentos para poder reconstruirlo

Comprobación de errores. Con el uso, se pueden dañar algunos sectores del disco duro. Los sectores defectuosos afectan al rendimiento del disco duro y en ocasiones dificultan e, incluso, imposibilitan la escritura de datos.

Las directivas locales

En Windows, los derechos se agrupan en un conjunto de reglas de seguridad y se han incorporado en unas consolas de administración denominadas directivas de seguridad que definen el comportamiento del sistema en temas de seguridad.

VENTAJAS

* La principal ventaja es que, por medio de las directivas de seguridad local, un administrador dispone herramientas que le permiten incrementar la seguridad.
* Con las directivas puede establecer parámetros de seguridad para todos los usuarios.
* Brindan seguridad al sistema operativo y al hardware del equipo, restringiendo la instalación de software y controladores al sistema.
* Seguridad al acceso de una cuenta de usuario.
* Seguridad en el inicio y cierre de una cuenta de usuario.
* Seguridad en el apagado de sistema operativo.
* Auditorias y monitoreo a cuentas de usuarios.
* Asignación de derechos a cuentas de usuarios.
* Protección a contraseñas de cuentas de usuarios.

**Directivas de cuentas:** en este apartado se puede establecer cuál es la política de cuentas o de contraseñas que se seguirá.

1. Contraseñas: cómo deben ser las contraseñas en el equipo (longitud mínima, vigencia máxima, historial, etc.).
2. Bloqueo: cómo se debe bloquear una cuenta que haya alcanzado un cierto máximo de intentos fallidos de conexión.

**Directiva local:** la Auditoría del equipo, que permite registrar en el visor de sucesos ciertos eventos que sean interesantes, a criterio del administrador (por ejemplo, los inicios de sesión local), y los derechos y privilegios que pueden tener los usuarios en el equipo.

**Directivas de clave pública:** en este apartado se pueden administrar las opciones de seguridad de las claves públicas emitidas por el equipo.

Administrando el equipo

* Visor de sucesos o Visor de eventos
* Carpetas compartidas
* Usuarios y grupos locales
* Registros y alertas de rendimiento o Rendimiento
* Administrador de dispositivos
* Administración de discos
* Servicios y aplicaciones