

Administración de software base II.

Caso práctico



En la empresa "GESTISA", de nuestro caso, necesitarán utilizar los ordenadores todos los empleados ya que su actividad está relacionada con tareas de asesoría; Carlos ya habrá configurando los ordenadores que forman el sistema aplicando los conocimientos adquiridos en las unidades anteriores.

Él administra las cuentas de los usuarios para los diferentes sistemas operativos instalados en los equipos, que en un principio trabajarán formando una estructura de red en grupo de trabajo, y que posteriormente pasarán a formar parte de un dominio. Todos los empleados tendrán la posibilidad de acceder a trabajar localmente en sus estaciones de trabajo.

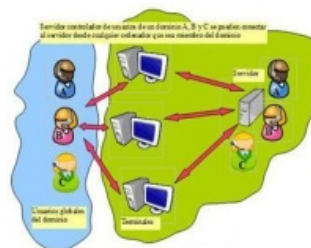
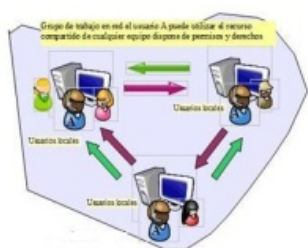
Los usuarios tendrán un perfil dentro del sistema dependiendo a los grupos de usuarios al que pertenezcan y de la actividad laboral que realicen.

En un principio Carlos realizará las pruebas prácticas necesarias en su ordenador "Caja de herramientas" donde tiene instalados las diferentes aplicaciones de forma virtual, antes de pasar a realizar las configuraciones necesarias en el sistema informático real de la empresa.

Administración de usuarios y grupos locales.

Caso práctico

Carlos realizará un listado con la relación de compañeros de trabajo y su actividad dentro de la empresa para poder gestionar y organizar los usuarios que necesitarán utilizar los ordenadores con el fin de que puedan trabajar con las aplicaciones instaladas y accedan a los servicios aportados por los servidores. Cada usuario dispondrá de un nombre y una clave para poder entrar en el sistema. Además, Carlos realiza las tareas administrativas relacionadas con las altas, bajas de usuarios y modificaciones de las características que necesitan los usuarios dentro del sistema.



La administración y gestión de los usuarios que acceden al sistema, es una de las tareas que controla el usuario administrador. El sistema operativo tiene que aportar funciones que permitan la seguridad del acceso mediante usuarios al sistema. **Las tareas que realiza el administrador de usuarios:**

- Añadir, modificar y eliminar usuarios en el sistema.
- Añadir, modificar y eliminar grupos locales o globales.
- Fijar el plan de cuentas y contraseñas en el equipo junto con una política de derechos de usuario.
- Establecer el sistema de auditorías.

Generalmente la **entrada al sistema o login** se realiza con la identificación del nombre de usuario y su contraseña de acceso (existen otros mecanismos como tarjeta inteligente identificativa, reconocimiento de huellas, voz, etc). Cada usuario, dentro del sistema, pertenece a un tipo de conjunto de usuarios denominado **grupo de usuario** y podrá pertenecer a tantos como sea necesario, adquiriendo los permisos de todos ellos.

El **sistema aporta grupos de usuarios predeterminados** como son Grupo Administrador, Grupo estándar, Grupo de invitado, etc. Además el sistema permite que el administrador cree sus propios grupos de usuarios, con un perfil de políticas de acceso a los diferentes recursos del sistema. Esta forma de administrar el sistema es mucho más flexible y potente que el establecimiento de permisos en base a usuarios individuales.

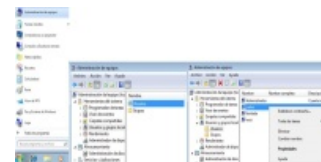
Los usuarios pueden **acceder a los recursos de un ordenador de forma local** y a los de **un servidor** desde un terminal o estación de trabajo mediante la identificación en el login ofrecido por el servidor y gestionado por un servicio. **Dentro de una estructura de red podemos encontrar diferentes tipos de usuarios:**

- **Usuarios locales al sistema operativo instalado en el terminal o servidor:** acceden directamente en el login del propio ordenador y utilizan los recursos del ordenador al que se han conectado. Pueden formar grupos de usuarios con características comunes. Para acceder a los recursos de un grupo de trabajo de ordenadores generalmente tienen que estar dados de alta en cada ordenador que forma parte del grupo o se debe identificar en el momento de tener que utilizar el recurso compartido.
- **Usuarios de un dominio:** un ordenador que cumpla la función de controlador de dominio es capaz de validar usuarios globales de dominio para que inicien sesión desde equipos clientes unidos al dominio o de forma local en el servidor para utilizar los recursos y servicios de software/ hardware que comparte un ordenador servidor.

Introducción a la administración de usuarios y grupos de usuarios locales en Windows 7.

Una **cuenta de usuario en Windows 7** guarda información que indica al sistema los archivos y carpetas a los que puede obtener acceso, los

privilegios que tiene para poder realizar cambios en el equipo y las preferencias personales. Las cuentas de usuario permiten compartir un equipo localmente con varias personas con el fin de mantener una propiedad de archivos y configuraciones. Cada persona obtiene acceso a su propia cuenta de usuario con un nombre de usuario y una contraseña. **Un usuario puede pertenecer a varios grupos, con privilegios adquiridos de la suma de todos ellos.**



Windows permite limitar la capacidad de los usuarios y los grupos para llevar a cabo determinadas acciones, mediante la asignación de derechos y permisos en su cuenta. **Un derecho autoriza a un usuario a realizar ciertas acciones en un equipo. Un permiso es una regla asociada con un objeto (normalmente un archivo, una carpeta o una impresora) que regula los usuarios que pueden tener acceso al objeto y de qué manera.**

Una carpeta o recurso particular, por ejemplo *Mis Documentos*, puede ser de acceso local o compartido mediante el acceso por red. Al asignar una carpeta particular a un usuario, se convierte en su carpeta predeterminada en los cuadros de diálogo *Abrir* y *Guardar como*, en las sesiones del símbolo de sistema y en todos los programas que no tienen una carpeta de trabajo definida. El usuario administrador puede cambiar la ubicación de dicha carpeta particular.



Autoevaluación

Un usuario solamente puede pertenecer a un grupo local de usuarios dentro del sistema operativo Windows.

- ☐ Verdadera
- ☐ Falsa

Configuración de usuarios y grupos de usuarios locales en Windows 7.

El usuario encargado de realizar la administración de cuentas tiene que pertenecer al grupo de administradores. Los Usuarios y grupos locales se encuentran definidos en la consola MMC en *Inicio-Administración de equipos-Usuarios y grupos locales*, desde este recurso podemos realizar todas las tareas relacionadas con la administración de usuarios, como son (el propio Windows ofrece una ayuda de descripción de los campos que aparecen en los diferentes formularios):



- **Altas de usuarios:** situar el ratón en el panel central (lista de usuarios y grupos) abrir la carpeta *Usuarios*, en una zona blanca (sin seleccionar ningún usuario) y pulsar el botón derecho, del menú seleccionar *Nuevo usuario*. Del formulario completar los campos y dar al botón *Crear* según la descripción de campos.
- **Baja de usuario:** situar el ratón en el panel central abrir la carpeta *Usuarios*, de la lista seleccionar el usuario a borrar y pulsar el botón derecho del ratón, hacer clic en la opción *Eliminar*. En la ventana de confirmación pulsar *Si*. No se puede recuperar una cuenta de usuario eliminada. No es posible eliminar las cuentas Administrador e Invitado.
- **Modificación datos de usuario:** situar el ratón en el Panel Central abrir la carpeta *Usuarios*, de la lista seleccionar el usuario a modificar y pulsar el botón derecho del ratón, hacer clic en la *Propiedades*. Aparece una ventana con las siguientes pestañas con formularios, donde se especifican los datos de los usuarios según los valores de campos:
 - *General:* están los datos que identifican a los usuarios. Como son el nombre y la contraseña y sus directivas de cuenta de acceso al ordenador.
 - *Miembro de:* permite indicar los grupos a los que pertenece el usuario. Un usuario puede pertenecer a varios grupos, con privilegios adquiridos de la suma de todos ellos. **Mediante la agrupación de usuarios en grupos podemos facilitar la administración de usuarios ya que todos ellos adquieren automáticamente las características de acceso a los recursos al ser incorporados al grupo, sin necesidad de tener que asignarlas usuario por usuario.** Para añadir el usuario a un grupo pulsamos en el botón *Agregar*, después pulsamos en *Opciones avanzadas*, en la ventana que aparece pulsamos en *Ubicación* para indicar, de la lista que aparece, el ordenador donde debe buscar los grupos a los que queremos pertenecer y seguidamente hacemos clic en el botón *Buscar ahora* para que en el panel inferior aparezcan todos los grupos, seleccionamos al que queremos pertenecer y pulsamos el botón *Aceptar*. Para quitar el usuario de un grupo, de la ventana inicial, seleccionamos el grupo y damos al botón *Quitar*.
 - *Perfil:* permite al usuario darle características indicadas en los campos del formulario como son su ruta de acceso, programa que se ejecuta al inicio, etc. **Para cambiar la contraseña o el nombre** debemos de situar el ratón en el panel central (lista de usuarios y grupos) abrir la carpeta *Usuarios*, de la lista seleccionar el usuario a modificar y pulsar el botón derecho del ratón, hacer clic en la opción deseada *Establecer contraseña* o *Cambiar de nombre*. El restablecimiento de una contraseña de cuenta local para un usuario puede ocasionar una pérdida de datos si dicho usuario tiene datos cifrados o contraseñas de Internet alternativas.

Todas las cuentas de usuario deben de ser únicas y cumplir con unas reglas de escritura como que deben de tener como máximo 20 caracteres, pueden contener letras mayúsculas y minúsculas, números, pero no se aceptan los siguientes caracteres especiales: /, |, :, ;, =, <, >, * y los espacios en blanco.

Debes conocer

Para consultar la descripción de los campos de los diferentes formularios que se utilizan para gestionar usuarios:

[Guía de referencia windows7. \(0.14 MB\)](#)



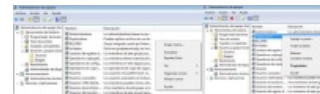
Autoevaluación

Cuando se elimina un grupo, también automáticamente se eliminan los usuarios que pertenecen al grupo en todo el sistema.

- ☐ Verdadera
- ☐ Falsa

Operaciones con grupos de usuarios en Windows 7.

Los grupos locales de usuarios se administran en *Inicio-Equipo*, botón derecho del ratón pulsar en *Administrar-Usuarios y grupos locales*. Las tareas que podemos realizar desde este lugar son (el propio Windows ofrece una ayuda de descripción de los campos que aparecen en los diferentes formularios):



- **Alta de un grupo local:** situar el ratón en el panel central (lista de usuarios y grupos) abrir la carpeta *Grupos*, en una zona blanca (sin seleccionar ningún grupo) y pulsar al botón derecho, del menú seleccionar *Nuevo grupo*. Del formulario completar los campos y dar al botón *Crear*. Los derechos y permisos de un grupo se asignan a todos sus miembros. Si el equipo se ha unido a un dominio, también veremos agregadas las cuentas de usuario, de equipo y de grupo de ese dominio y de los dominios de confianza en la consola de administración de usuarios en el equipo local.
- **Baja de un grupo:** situar el ratón en el panel central abrir la carpeta *Grupos*, de la lista seleccionar el grupo a borrar y pulsar el botón derecho del ratón, hacer clic en la opción *Eliminar*. De la ventana de confirmación pulsar *Si*. No se puede recuperar una cuenta de usuario eliminada. Los siguientes grupos predeterminados no se pueden eliminar: Administradores, Operadores de copia de seguridad, Operadores criptográficos, Usuarios avanzados, Usuarios, Usuarios de COM distribuido, Invitados, IIS_IUSRS, Usuarios de escritorio remoto, Operadores de configuración de red, Usuarios del registro de rendimiento, Usuarios del monitor de sistema y Replicador. Los grupos eliminados no se pueden recuperar. La eliminación de un grupo no elimina las cuentas de usuario, las cuentas de equipo o las cuentas de grupo que eran miembros de dicho grupo. Para **eliminar un grupo desde la línea de comandos**:
 - Abre la ventana del símbolo del sistema, desde *Inicio*, en el campo de *Buscar* escribir *cmd*. Luego ejecutar:

```
net localgroup "nombre_grupo" /delete
```

- Para **identificar los miembros de un grupo local:** situar el ratón en el panel central abrir la carpeta *Grupos*, de la lista seleccionar el grupo y pulsar el botón derecho del ratón, hacer clic en la *Propiedades*. Desde esta ventana podemos *Agregar o quitar usuarios del grupo*. Para **identificar usuarios desde la línea de comandos**:
 - Abre la ventana del símbolo del sistema, desde *Inicio*, en el campo de *Buscar* escribir *cmd*. Luego ejecutar:

```
net localgroup "<nombre_del_grupo">
```

- Para **añadir el usuario a un grupo** pulsamos en el botón *Agregar*, de la ventana pulsamos en *Opciones avanzadas*, pulsamos en *Ubicación* para indicar el ordenador donde debe buscar los grupos a los que queremos pertenecer y dar al botón *Buscar ahora*, para que en el panel inferior aparezcan todos los grupos, seleccionamos al que queremos pertenecer y pulsamos al botón *Aceptar*. Para quitar al usuario de un grupo, de la ventana inicial, seleccionamos el grupo y damos al botón *Quitar*. Para **agregar un usuario a un grupo desde la línea de comandos**:
 - Abre la ventana del símbolo del sistema, desde *Inicio*, en el campo de *Buscar* escribir *cmd*. Luego ejecutar:

```
net localgroup "nombre_del_grupo" "<nombre_de_usuario>" /add
```

Debes conocer

Para consultar la descripción de los campos de los diferentes formularios que aparecen en el apartado de esta

[Guía de referencia windows7. \(0.14 MB\)](#)

Para consultar ejemplos de comandos para la gestión de usuarios y grupos visitar el siguiente enlace:

[Gestión de usuarios y grupos en Windows. \(0.03 MB\)](#)

Gestión de usuarios y grupos de usuarios desde el Panel de control de Windows 7.

Windows 7 está diseñado para poder acceder a las herramientas y recursos por diferentes caminos o accesos. Podemos gestionar las cuentas de usuario de una manera fácil y rápida desde el **Panel de control**, para ello vamos a *Inicio-Panel de control-Cuentas de usuario y protección infantil*. Para realizar esta tarea debemos de ser usuario del grupo de administradores. Desde este lugar podemos:



- **Crear cuenta de usuario:** desde *Inicio-Panel de control-Cuentas de usuario y protección infantil- Cuentas de usuario- Administrar cuentas- Crear una nueva cuenta*. En la ventana escribimos el nombre de usuario y seleccionamos el tipo de cuenta *Usuario estándar* o *Administrador* (consultar tema de grupos de usuarios predeterminados).

- **Modificar o eliminar una cuenta de usuario:** desde *Inicio-Panel de control-Cuentas de usuario y protección infantil-Cuentas de usuario-Administrar cuentas*, damos doble clic con el ratón sobre una cuenta de la lista. Podemos realizar operaciones como: *Cambiar el nombre de cuenta, Cambiar la contraseña, Quitar la contraseña, Cambiar la imagen, Cambiar el tipo de cuenta, Eliminar cuenta*, etc.
- **El Administrador de credenciales:** permite almacenar los nombres de usuarios y sus contraseñas que usa para iniciar sesión en sitios web o en otros equipos de una red. Las credenciales o datos se guardan en carpetas del equipo llamadas almacenes. Windows y determinados programas (como los exploradores web) pueden proporcionar con seguridad las credenciales de los almacenes a otros equipos y sitios web. Para agregar una contraseña a su almacén de Windows, hay que seguir los siguientes pasos:
 1. Desde *Inicio-Panel de control-Cuentas de usuario y protección infantil-Cuentas de usuario*.
 2. En el panel izquierdo, hacer clic en *Administrar credenciales*.
 3. Hacer clic en *Agregar una credencial de Windows*. En el campo *Dirección de red o Internet*, escribir el nombre del equipo de la red al que desea obtener acceso.
 4. En los campos *Nombre de usuario* y *Contraseña*, escribir el nombre de usuario y la contraseña que se usan para ese equipo o sitio web y pulsa en *Aceptar*.



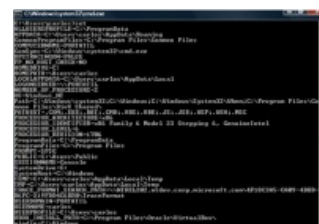
Autoevaluación

La utilidad del Panel de control “Cuentas de usuario y protección infantil” que dispone Windows 7 permite gestionar grupos de usuarios.

- ☐ Verdadera
- ☐ Falsa

Variables de entorno relacionadas con usuarios y grupos en Windows 7.

Una variable del entorno es un **valor dinámico** cargado en la memoria, y que puede ser utilizado por varios procesos de un ordenador. En Windows, las variables del entorno se ubican entre los caracteres "%". De esta forma, para mostrar el valor de una variable del entorno sólo se debe escribir desde la consola de entrada de comandos la orden:



echo %nombre_variable%

Una lista de las principales variables del entorno en un sistema Windows relacionadas con usuarios y grupos de usuarios es:

Nombre de Variable	Descripción
%ALLUSERSPROFILE%	Ruta de la carpeta con la configuración para todos los usuarios
%APPDATA%	Almacena una ruta de acceso al directorio predeterminado que contiene los programas del usuario
%HOMEDRIVE%	Contiene la letra de la unidad en la que está ubicado el directorio actual del usuario
%HOMEPATH%	Presenta la ruta de acceso completa al directorio actual del usuario
%USERNAME%	Almacena el nombre de usuario en sesión
%USERPROFILE%	Almacena la ubicación del perfil de usuario en sesión
%WINDIR%	Almacena el directorio de acceso del sistema

En Windows para crear, modificar y mostrar las variables del entorno se utiliza el comando **set**. La forma de utilizarlo es desde una consola, ejecutando el comando siendo *nombre_variable* la variable deseada:

set Nombre_variable	Para que se muestre una variable
set Nombre_variable=valor	Para crear y asignar valor a una variable
set Nombre_variable=	Para eliminar de memoria una variable

Para modificar, añadir o consultar las variables de entorno del usuario utilizando el entorno gráfico de ventanas, seguir estos pasos:

1. Hacer clic en *Inicio-Panel de control-Cuentas de usuario y protección infantil-Cuentas de usuario*, del panel izquierdo seleccionar la opción *Cambiar las variables de entorno*.
2. Realizar las modificaciones que desea en las variables de entorno del usuario correspondientes a su cuenta de usuario.

Debes conocer

Para consultar la descripción de las variables relacionadas con el sistema Windows 7 acceder al siguiente fichero adjunto:

[Guía de referencia windows7. \(0.14 MB\)](#)

Para saber más

Como documentación podemos acceder a los enlaces:

[Administración de usuarios Windows 7 enlace 1](#)

[Administración de usuarios Windows 7 enlace 2](#)

Introducción a la administración de usuarios y grupos locales en Windows Server 2008.

Caso práctico

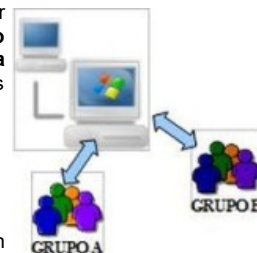
Carlos configura los usuarios de su empresa y los agrupa por el criterio de la actividad laboral que realizan en "GESTISA" tales como: *asesoría_contable* (todos los usuarios encargados de gestionar los asuntos contables de los clientes), *asesoría_laboral* (los empleados que mantienen la asesoría de asuntos laborales) y *asesoría_financiera* (los empleados que mantienen la asesoría de asuntos financieros de los clientes). También ha creado un grupo encargado resolver y manejar las aplicaciones relacionadas con la gestión empresarial de la propia empresa (contabilidad, facturación y nóminas) denominado *grupo_gestisa*.

Windows Server es un sistema multiusuario donde varios usuarios pueden iniciar sesión simultáneamente en el ordenador desde un entorno de trabajo en red, desde otros terminales o estaciones de trabajo. **Debemos estar como usuario administrador para poder configurar el servidor. Un servidor dispone de cuentas de acceso local para acceder por la red desde el propio servidor o global a un ordenador estación de trabajo o terminal.** Es decir, una cuenta de usuario es una identificación asignada de manera única al usuario para permitirle:

- **Iniciar sesión en un dominio** (se verá en la Unidad 6) para acceder a los recursos de toda la red.
- **Iniciar sesión en un equipo local** para acceder a los recursos locales o a un grupo de trabajo.

Cuando varios usuarios van a tener los mismos derechos y privilegios en el servidor, es conveniente crear un grupo con dicho perfil de acceso, permitiéndonos crear usuarios que se puedan añadir a un grupo definido, de este modo automáticamente adquieren los privilegios de acceso al grupo. Hay dos tipos diferentes de grupos:

- **Grupos locales:** Otorgan a los usuarios permisos para que accedan a un recurso de red. También sirven para conceder a los usuarios privilegios para gestionar tareas de sistema (como cambiar la hora, hacer copias de seguridad, recuperar archivos, etc.). Existen grupos locales predeterminados. **Mientras no se defina un dominio todas las cuentas junto con la de Administrador se consideran locales.** Podemos crear nuevas cuentas locales y asignarles diferentes permisos de acceso al sistema.
- **Grupos globales:** Se usan para organizar las **cuentas de usuario de dominio** (se verá en la Unidad 6). También se usan en redes de varios dominios, cuando los usuarios de un dominio necesitan tener acceso a recursos de otro dominio.



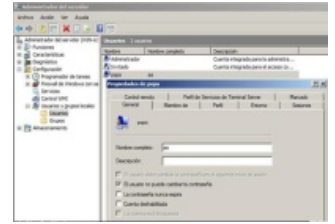
Configuración de usuarios y grupos locales en Windows Server 2008.

Operaciones que podemos realizar con usuarios locales (**para consultar la descripción de los campos de los diferentes formularios acceder a la propia ayuda en la ventana mostrada por Windows**):

- Para **crear cuentas de usuario local** seguir los siguientes pasos:
 1. Desde el menú *Inicio-Administrador del servidor*, del panel derecho seleccionar *Configuración*, pulsamos en *Usuarios y grupos locales*, en el panel central debemos seleccionar la carpeta *Usuarios*.
 2. Aparecen dos usuarios predeterminados el *Administrador e Invitado* (si tiene una flecha hacia abajo indica que por seguridad está deshabilitado).
 3. Pulsamos el botón derecho del ratón desde zona blanca del panel central, del menú seleccionar *Nuevo usuario*. Del formulario completar los campos y dar al botón *Crear*.
- Para **dar de baja de usuario local** del servidor seguir los pasos siguientes:
 1. Desde el menú *Inicio-Administrador del servidor*, del panel derecho seleccionar *Configuración*, pulsamos en *Usuarios y grupos locales*.
 2. Situar el ratón en el panel central abrir la carpeta *Usuarios*, de la lista seleccionar el usuario a borrar y pulsar el botón derecho del ratón, hacer clic en la opción *Eliminar*. De la ventana de confirmación pulsar *Si*. No se puede recuperar una cuenta de usuario eliminada. No es posible eliminar las cuentas *Administrador e Invitado*.

- Si necesitamos **modificar los datos de un usuario** debemos seguir las siguientes indicaciones:

1. Desde el menú *Inicio-Administrador del servidor*, del panel derecho seleccionar *Configuración*, pulsamos en *Usuarios y grupos locales*.
2. Situar el ratón en el panel Central abrir la carpeta *Usuarios*, de la lista seleccionar el usuario a modificar y pulsar el botón derecho del ratón, hacer clic en *Propiedades*. Aparece una ventana con las siguientes pestañas o formularios:
 - *General*: donde se pueden modificar los datos que identifican al usuario dentro del sistema como su nombre y directivas de seguridad de la cuenta.
 - *Miembro de*: permite ver o cambiar los grupos a los que pertenece el usuario. Un usuario puede pertenecer a varios grupos, con privilegios adquiridos de la suma de todos ellos. Para añadir el usuario a un grupo pulsamos en el botón *Agregar*, clic en *Opciones avanzadas*, clic en *Ubicación* para indicar de la lista que aparece, el ordenador donde debe buscar los grupos a los que queremos pertenecer y seguidamente dar al botón *Buscar ahora*. Para que en el panel inferior aparezcan todos los grupos seleccionamos al que queremos pertenecer y pulsamos *Aceptar*. Para quitar el usuario de un grupo, de la ventana inicial, seleccionamos el grupo y damos al botón *Quitar*.
 - *Perfil*: Define la ruta de acceso al perfil del usuario y el script de inicio de sesión.
 - *Entorno*: permite configurar el entorno de servicios de Terminal Server (permite que los usuarios pueden conectarse a un servidor de Terminal Server para ejecutar programas y usar los recursos de red de dicho servidor) y el modo de conexión de dispositivos al inicio de sesión. Indicamos el programa que se ejecutará al iniciar la sesión y las impresoras de las que podrá disponer el cliente.
 - *Sesiones*: podemos configurar el tiempo de espera y la reconexión a los servicios de Terminal server. Permite indicar, por seguridad, en que tiempo se fuerza a desconectar una sesión sin actividad o activa.
 - *Control remoto*: configura el control remoto de los Servicios de Terminal Server.
 - *Perfil de Servicios de Terminal Server*: permite configurar la ruta de acceso al perfil de usuario de los Servicios de Terminal Server o para denegar el inicio de sesión a Terminal Server.
 - *Marcado*: para permitir o denegar el acceso a redes, las opciones de devolución de llamadas y para asignar direcciones IP estáticas.



Debes conocer

Puedes consultar la descripción de los campos de los diferentes formularios del apartado de la unidad

[Guía de referencia windows server. \(0.12 MB\)](#)

Operaciones con grupos de usuarios locales en Windows Server 2008.

Si deseamos gestionar el **alta de un grupo local** debemos realizar los siguientes pasos (**podemos consultar la descripción de los campos de los diferentes formularios desde la propia ayuda en la ventana mostrada por Windows**):

1. Desde el Menú *Inicio-Administrador del servidor*, del panel derecho seleccionar *Configuración*, pulsamos en *Usuarios y grupos locales*, en el panel central debemos seleccionar la carpeta *Grupos*.
2. Aparecen los grupos predeterminados y los creados en el sistema. Dar el botón derecho del ratón desde zona blanca del panel central, del menú seleccionar *Grupo nuevo*. Del formulario completar los campos y clic en el botón *Crear*.



Para **añadir el usuario a un grupo** pulsamos en el botón *Agregar*, clic en *Opciones avanzadas*, clic en *Ubicación* para indicar el ordenador donde debe buscar los grupos a los que queremos pertenecer y dar al botón *Buscar ahora*, para que en el panel inferior aparezcan todos los grupos, seleccionamos al que queremos pertenecer y pulsamos en el botón *Aceptar*. Para quitar un usuario de un grupo, en la ventana inicial seleccionamos el grupo y clic en *Quitar*.

Es posible **agregar un usuario a un grupo desde la consola de línea de comandos** abriendo la ventana del símbolo del sistema, desde *Inicio*, en el campo de buscar escribir *cmd*. Ejecutar la orden:

```
net localgroup "nombre_grupo" "<nombre_usuario>" /add
```

Los derechos y permisos asignados a un grupo se asignan a todos sus miembros. Si el equipo se ha unido a un dominio, también puede agregar a un grupo local las cuentas de usuario, de equipo y de grupo de ese dominio y de los dominios de confianza.

Si deseamos **dar de baja un grupo** debemos de realizar los siguientes pasos:

1. Desde el menú *Inicio-Administrador del servidor*, del panel derecho seleccionar *Configuración*, pulsamos en *Usuarios y grupos locales*, en el panel central debemos seleccionar la carpeta *Grupos*.
2. De la lista seleccionar el grupo a borrar y pulsar el botón derecho del ratón, hacer clic en la opción *Eliminar*. De la ventana de confirmación pulsar *Si*. No se puede recuperar una cuenta de usuario eliminada. Los siguientes grupos predeterminados no se pueden eliminar: Administradores, Operadores de copia de seguridad, Operadores criptográficos, Usuarios avanzados, Usuarios, Usuarios de COM distribuido, Invitados, IIS_IUSRS, Usuarios de escritorio remoto, Operadores de configuración de red, Usuarios del registro de rendimiento, Usuarios del monitor de sistema y Replicador.

Los grupos eliminados no se pueden recuperar. La eliminación de un grupo no elimina las cuentas de usuario, las cuentas de equipo o las cuentas de grupo, de las que era miembro dicho grupo. Para **eliminar un grupo desde la línea de comandos**, abre la ventana del símbolo del sistema, desde *Inicio*, en el campo de buscar escribir *cmd* y Ejecutar:

```
net localgroup <nombre_grupo> /delete
```

Para **identificar los miembros de un grupo local**:

1. Desde el menú *Inicio-Administrador del servidor*, del panel derecho seleccionar *Configuración*, pulsamos en *Usuarios y grupos locales*.
2. Situar el ratón en el panel central (lista de usuarios y grupos) abrir la carpeta *Grupos*, de la lista seleccionar el grupo y pulsar el botón derecho del ratón, hacer clic en *Propiedades*. Desde esta ventana podemos *Agregar o quitar usuarios del grupo*.

Para **identificar usuarios desde la línea de comandos** abre la ventana del símbolo del sistema y ejecutar la orden:

```
net localgroup "nombre_del_grupo"
```

Debes conocer

Puedes consultar la descripción de los campos de los diferentes formularios del apartado de la unidad

[Guía de referencia windows server.](#) (0.12 MB)

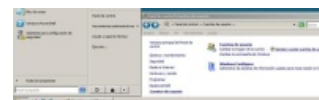
Gestión de usuarios y grupos desde el Panel de control en Windows Server 2008.

Caso práctico

Carlos, utiliza un servidor con el Sistema Windows Server 2008 con la idea de montar posteriormente un dominio en la empresa, previamente dará de alta los usuarios incluyéndolos en sus correspondientes grupos.

Windows Server 2008 está diseñado para poder acceder a las herramientas y recursos por diferentes caminos o accesos, de una forma muy parecida a Windows 7 desde *Inicio-Panel de control-Cuentas de usuario y protección infantil*, **podemos gestionar las cuentas de usuario de un modo fácil y rápido desde Panel de control**. Para realizar esta tarea debemos ser usuario del grupo de administradores.

Desde este lugar podemos:



- **Crear cuenta de usuario:** desde *Inicio-Panel de control-Cuentas de usuario-Agregar o quitar cuentas de usuario-Crear una nueva cuenta*. En la ventana escribimos el nombre de usuario y seleccionamos el tipo de *Usuario estándar* o *Administrador* (consultar tema de grupos de usuarios predeterminados).
- **Modificar o eliminar una cuenta de usuario:** desde *Inicio-Panel de control-Cuentas de usuario-Administrar cuentas*, damos doble clic con el ratón sobre la imagen de una cuenta de la lista. Podemos realizar operaciones como: *Cambiar el nombre de cuenta*, *Cambiar la contraseña*, *Quitar la contraseña*, *Cambiar la imagen*, *Cambiar el tipo de cuenta*, *Eliminar cuenta*, etc.

Para saber más

Puedes consultar dudas y utilizar como bibliografía el propio manual de ayuda interactiva, aportado por la licencia instalada de Windows Server 2008 de Microsoft.



Autoevaluación

Un usuario de tipo o grupo estándar puede:

- ☐ Eliminar su cuenta.
- ☐ Cambiar su nombre y contraseña.
- ☐ Cambiar el tipo de cuenta.
- ☐ Si no es administrador no puede hacer nada con su configuración de cuenta.



Autoevaluación

Para poder acceder desde un terminal con una cuenta de usuario creada en un servidor de Windows Server.

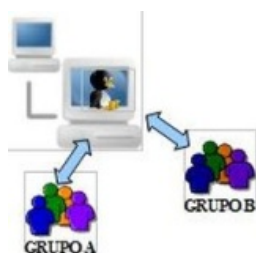
- ☐ La cuenta tiene que ser de tipo de acceso global.

- ☐ La cuenta tiene que ser de tipo de acceso local.
- ☐ En el terminal tiene que estar configurado que es miembro de un dominio y la cuenta tiene que estar configurada en el servidor de tipo global.
- ☐ En el terminal tiene que estar configurado que es miembro de un grupo de trabajo y la cuenta tiene que estar configurada en el servidor de tipo global.

Introducción a la administración de usuarios y grupos en Linux.

Caso práctico

Algunas aplicaciones de "Gestisa" corren en Linux, y Carlos va a dar de alta a ciertos usuarios y grupos en Linux para poder utilizar dichas herramientas.



Linux es un sistema multiusuario donde varios usuarios pueden iniciar sesión simultáneamente desde otros terminales o estaciones de trabajo a un ordenador siempre que estén en un entorno de trabajo en red. También, los usuarios creados en el sistema, pueden acceder localmente en el ordenador, abriendo diferentes sesiones.

Los usuarios en Linux se identifican por un número único de usuario (User ID o UID) y pertenecen a un grupo principal de usuario, identificado también por un número único de grupo (Group ID o GID). El usuario puede pertenecer a más grupos además del principal. **El usuario root es creado en el proceso de la instalación del sistema operativo, será el administrador de usuarios del sistema. Su UID es 0.**

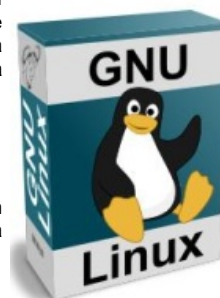
Los usuarios que crea el administrador root pueden acceder al sistema localmente mediante un login de entrada o remotamente por protocolos de comunicación como son el [telnet](#) por seguridad, ya en desuso o [ssh](#). También pueden trabajar en un entorno gráfico (mediante objetos de ventanas) o en modo texto (mediante consola de edición o entrada de comandos).

Cada usuario dispone de un directorio de trabajo con una ubicación predeterminada dentro del directorio `/home` del que tiene todos los derechos y privilegios para su uso. Cada usuario puede personalizar su entorno de trabajo o escritorio gráfico. A los usuarios creados por el administrador, el sistema se encarga de asignar a cada uno un UID superior a 500. **Los datos de los usuarios y grupos se encuentran en los siguientes ficheros:**

FICHERO	LOCALIZACION	DESCRIPCIÓN
<code>passwd</code>	<code>/etc/passwd</code>	Se encuentran definidas las cuentas de usuario
<code>shadow</code>	<code>/etc/shadow</code>	Contiene las contraseñas de usuario encriptadas
<code>group</code>	<code>/etc/group</code>	Contiene una relación de los grupos a los que pertenecen los usuarios
<code>login.defs</code>	<code>/etc/login.defs</code>	Están definidas las variables que controlan los aspectos de la creación de usuarios y de los campos de shadow usadas por defecto

Configuración de usuarios y grupos en Linux.


En la configuración predeterminada del sistema, y por seguridad, la cuenta del root está deshabilitada para el acceso remoto al sistema o para el login de entrada local, y su contraseña es la misma que la del usuario normal, creado en el proceso de instalación. Para poder trabajar sin que el sistema nos interrumpa solicitándonos la contraseña de root cada vez que se realiza una tarea de **administración en el entorno gráfico tendremos que asignar una contraseña a root y habilitarle la entrada desde el login del entorno gráfico.** Para realizar la configuración desde Linux Ubuntu seguir los siguientes pasos:



- Desde el menú *Sistema-Administración-Ventana de entrada*. Se abrirá una ventana con las siguientes pestañas:
 - General*: para indicar cuál será la interfaz gráfica que inicia el sistema por defecto.
 - Local*: para indicar que en la pantalla de login se muestren los usuarios del sistema con una imagen. También podemos indicar el tema con el que se inicia sesión en modo local, por seguridad este tipo de acceso está desactivado.
 - Remota*: para configurar el modo de iniciar sesión remotamente, desde otro ordenador.
 - Accesibilidad*: para poner colores y sonidos en la entrada de sesión local.
 - Seguridad*: podemos indicar que se inicie sesión automáticamente sin tener que indicar el nombre de usuario al iniciar sesión. También podemos permitir que el usuario root pueda iniciar sesión en entorno gráfico en el sistema, y permitir que pueda acceder de forma remota. También podemos configurar los permisos del usuario, grupo y otros sobre la carpeta personal de trabajo del usuario que inicie la sesión. Pulsando en el botón *Configurar servidor X* se puede configurar el inicio de sesión remoto en entorno gráfico.
 - Usuarios*: se puede seleccionar la lista de usuarios que se muestran en la pantalla de login (siempre que esté activada la opción de *Estilo Simple con face browser* en la pestaña *Local*). También podemos personalizar la imagen que se muestra en la pantalla inicial asociada a cada usuario del sistema.
- Pulsar en la pestaña *Seguridad* y activar la pestaña de *Permitir entrada local al administrador del sistema*, desmarcar *Activar entrada automática*, seleccionar *Activar entrada temporalizada* e indicar 15 segundos.
- Ahora para dar una contraseña a root debemos ir al menú *Sistema-Administración-Usuario y Grupos* y pulsar en el botón *Desbloquear e*

introducimos la contraseña de usuario con la que instalamos el sistema operativo y seguidamente ponemos la contraseña de root, para ello seleccionamos de la lista al usuario root y pulsamos en la opción *Propiedades*, en el campo *Contraseña de usuario* escribimos la nueva contraseña y la repetimos en el campo de *Confirmación*.

En Linux se pueden gestionar usuarios globales del dominio, de manera que con ellos se puede iniciar sesión desde cualquier equipo cliente que este unido al dominio, de la misma forma que en un controlador de dominio Windows Server 2008. Es decir, en Windows los usuarios locales de un Servidor, cuando pasa a ser controlador de dominio todos ellos pasan automáticamente a ser usuarios globales, que pueden acceder remotamente desde otro terminal o localmente en el propio servidor. A diferencia, Linux gestiona aparte los usuarios locales del equipo que pueden acceder localmente al equipo o remotamente sin necesidad de pertenecer al dominio, aunque el servidor estuviera configurado como controlador de dominio.



Autoevaluación

¿Cuál es el directorio particular de cada usuario en Linux?.

- ☐ Mis documentos.
- ☐ Documents and settings.
- ☐ home.
- ☐ /etc/passwd.

Operaciones con usuarios en Linux.

Para crear, modificar y eliminar usuarios locales debemos seguir los siguientes pasos:



- **Alta de usuarios:**

1. Ir al menú *Sistema-Administración-Usuarios y grupos*. Veremos la lista de usuarios dados de alta en el sistema.
2. Pulsar en el botón *Añadir usuario*, se mostrará una pantalla con las siguientes pestañas que recogerán los datos del usuario necesarios para su gestión en el sistema:
 - **Cuenta:** contiene la información esencial para registrarse en el sistema como son los datos de los campos siguientes:
 - **Usuario:** es el nombre con el que el usuario se valida en el sistema. Hay que tener en cuenta que **Linux distingue entre mayúsculas y minúsculas**. Los nombres no pueden contener caracteres especiales como (-, %, &, etc.) ni tampoco espacios en blanco.
 - **Nombre real:** es el nombre completo del usuario.
 - **Contraseña del usuario:** se escribe la contraseña del usuario para entrar al sistema.
 - **Confirmación:** se vuelve a escribir la contraseña.
 - **Contacto:** contiene información para contactar con el usuario como es el domicilio de trabajo, teléfono del trabajo y domicilio del usuario.
 - **Privilegios del usuario:** mediante la marcación o desmarcación de una serie de opciones de acceso a recursos que aparecen en un listado, podemos otorgar algunos privilegios al usuario como puede ser conectarse a redes, configurar impresoras, administrar el sistema, usar unidades de CDRom, compartir archivos en la red, etc. Según dichos privilegios serán añadidos a grupos predeterminados del sistema.
 - **Avanzado:** podemos configurar datos como son:
 - La ubicación del directorio personal en el sistema de ficheros, por defecto se le asignará `/home/nombre_de_usuario`.
 - El intérprete de comandos a utilizar, por defecto es `/bin/bash`.
 - El Grupo principal al que pertenece, cada vez que se crea un usuario se creará un grupo con su nombre.
 - El número ID que el sistema asigna al usuario (UID)

3. Rellenar los datos de la pestaña *Cuenta* y pulsar en *Aceptar*

- **Modificación de los datos de usuario:**

1. Ir al menú *Sistema-Administración-Usuarios y grupos*. Veremos la lista de usuarios dados de alta en el sistema.
2. Seleccionamos el usuario a modificar de la lista y pulsamos en el botón *Propiedades*.

3. Aparecerá la ventana con las pestañas *Cuenta*, *Contacto*, *Privilegios del Usuario* y *Avanzado*, que contienen los campos con los datos del usuario, donde podemos modificar la información que se desee. No podemos cambiar el login del usuario ya que si se hace se crearía un nuevo usuario.

- **Baja de un usuario en el sistema:**

1. Ir al menú *Sistema-Administración-Usuarios y grupos*. Veremos la lista de usuarios dados de alta en el sistema.
2. Seleccionamos el usuario a borrar de la lista y pulsamos en el botón *Borrar*. Al dar de baja a un usuario su carpeta personal, que estará dentro del directorio */home*, no se eliminará; esto es debido a que pueden existir usuarios del sistema que tengan derechos para usar dicha carpeta o parte de su contenido.

Autoevaluación

Podemos dar de alta a un usuario en Linux con el nombre **USu1distancia#**.

☐ Verdadera

☐ Falsa

Operaciones con grupos de usuarios en Linux.

Todos los usuarios tienen que pertenecer a un grupo de usuarios del sistema. Cuando se da de alta a un usuario, el sistema crea un grupo con el mismo nombre que el usuario y añade automáticamente a dicho grupo el usuario creado. El sistema creará una serie de grupos predeterminados como son *root*, *users*, *admin*, *ssh*, etc.



- **Crear un grupo de usuarios:**

1. Ir al menú *Sistema-Administración-Usuarios y grupos*. Pulsar el botón *Gestionar grupos*. Aparecerá una ventana con la lista de grupos creados en el sistema.
2. Pulsar en el botón *Añadir*. Completamos los siguientes campos del formulario:
 - *Nombre del grupo*: escribimos el nombre que tendrá el grupo en el sistema. No puede disponer de caracteres especiales, no espacios en blanco.
 - *Id del grupo*: es el número interno de identificación del grupo
 - (GID) para los procesos del sistema que será un número igual o superior al que asigna el sistema por defecto
 - *Miembros del grupo*: marcamos las casillas de verificación de la lista para seleccionar los usuarios que vayan a pertenecer al grupo.
3. Pulsamos en *Aceptar*.

- **Modificación de grupos:**

1. Ir al menú *Sistema-Administración-Usuarios y grupos*. Pulsar el botón *Gestionar grupos*. Aparecerá una ventana con la lista de grupos creados en el sistema.
2. De la lista seleccionamos un grupo y pulsamos en el botón de *Propiedades*. Podemos añadir o quitar usuarios que pertenezcan al grupo en el apartado *Miembros del grupo* marcando o desmarcando las casillas de verificación de la lista de usuarios del sistema.

- **Baja de un grupo de usuarios:**

1. Ir al menú *Sistema-Administración-Usuarios y grupos*. Pulsar el botón *Gestionar grupos*. Aparecerá una ventana con la lista de grupos creados en el sistema.
2. De la lista seleccionamos un grupo y pulsamos en el botón de *Borrar*. Cuando se borra un grupo, los usuarios que pertenecen exclusivamente a ese grupo, será necesario que se les añada a otro grupo para que no surjan problemas de acceso.

Si deseamos **ejecutar la aplicación que administra usuarios y grupos desde la consola** de entrada de comandos debemos de ejecutar el demonio:

```
root@sistemaubuntu:~# user -admin
```



Autoevaluación

¿Cuándo se crea un usuario nuevo en Linux, por defecto es miembro de grupo?

- ☐ users.
- ☐ root.
- ☐ estándar.
- ☐ Ninguno.

Operaciones en modo comando con usuarios en Linux.

Desde *Inicio-Accesorios-Terminal* ejecutar desde terminal de consola el comando `su` para identificarse como usuario `root` escribir la contraseña del usuario `root` y aparece el prompt de entrada para el administrador identificado con el símbolo `#`:

```

root@carlos-laptop:~# su
Introduzca la nueva contraseña de UNIX:
Vuelva a escribir la nueva contraseña de UNIX:
passwd: contraseña actualizada correctamente
root@carlos-laptop:~# su
Contraseña:
root@carlos-laptop:/home/carlos# mes useradd
root@carlos-laptop:/home/carlos# useradd alumnol
root@carlos-laptop:/home/carlos# passwd alumnol
Introduzca la nueva contraseña de UNIX:
Vuelva a escribir la nueva contraseña de UNIX:
passwd: contraseña actualizada correctamente
root@carlos-laptop:/home/carlos#

```

```

carlos@sistemaubuntu:~$ su
Contraseña:
root@carlos-laptop:/home/carlos#

```

También, podemos ejecutar los comandos con el formato de la orden `sudo`, de la siguiente manera:

```

carlos@sistemaubuntu:~$ sudo nombre_de_comando
[sudo] password for carlos:

```

Mediante el comando `man` podemos obtener la ayuda interactiva de un comando de Linux mediante el formato siguiente:

```

root@carlos-laptop:/home/carlos# man nombre_comando

```

Con `useradd` o `adduser` es el comando que permite añadir nuevos usuarios, se creará el usuario y su grupo, así como las entradas correspondientes en `/etc/passwd`, `/etc/shadow` y `/etc/group`. También se creará el directorio de inicio o de trabajo en `/home/nombre_de_usuario` y los archivos de configuración que van dentro de este directorio. Las fechas de expiración de contraseña, etc. El formato más simple del comando sería:

```

root@sistemaubuntu:~# useradd nombre_de_usuario

```

El segundo paso es asignarle una contraseña a ese usuario con el comando `passwd` que permitirá ingresar o cambiar la contraseña y su verificación:

```

root@sistemaubuntu:~# passwd nombre_de_usuario
Introduzca la nueva contraseña de UNIX:
Vuelva a escribir la nueva contraseña de UNIX:
passwd: contraseña actualizada correctamente
root@sistemaubuntu:~#

```

El usuario `root` es el único que puede indicar el cambio o asignación de contraseñas de cualquier usuario. Un usuario puede cambiar su propia contraseña mediante el comando `passwd` sin ningún parámetro. El comando `passwd` tiene varias opciones que establecen los valores de la cuenta en `/etc/shadow`. Con `usermod` podemos modificar o actualizar un usuario o cuenta ya existente. Si quisiéramos cambiar el nombre de usuario escribimos:

```

root@sistemaubuntu:~# usermod -l nombre_actual_de_usuario nuevo_nombre_de_usuario

```

Con `userdel` elimina una cuenta del sistema, `userdel` puede ser invocado de tres maneras:

<code>userdel nombre_de_usuario</code>	Sin opciones elimina la cuenta del usuario de <code>/etc/passwd</code> y de <code>/etc/shadow</code> , pero no elimina su directorio de trabajo ni archivos contenidos en el mismo
<code>userdel -r nombre_de_usuario</code>	Elimina la cuenta totalmente, y elimina su directorio de trabajo y archivos y directorios contenidos en el mismo. La cuenta no se podrá eliminar si el usuario esta logueado o en el sistema al momento de ejecutar el comando
<code>userdel -f nombre_de_usuario</code>	elimina todo lo del usuario, cuenta, directorios y archivos del usuario, pero además lo hace sin importar si el usuario está actualmente en el sistema trabajando

Debes conocer

Podemos consultar las opciones de formato de todos los comandos utilizados para la gestión de usuarios desde el fichero:

[Guía de referencia Linux.](#) (0.12 MB)

Gestión avanzada de usuarios en Linux.

Los usuarios normales y `root` en sus directorios de inicio tienen varios archivos que comienzan con "." ya que están ocultos. Pueden variar dependiendo de la distribución de Linux que se tenga, pero seguramente se encontrarán los siguientes o similares:

```
carlos@sistemaubuntu:~$ ls -la
total 788
drwxr-xr-x 44 carlos carlos 4096 2010-02-03 11:48 .
drwxr-xr-x 3 root root 4096 2010-01-22 11:58 ..
-rw-r--r-- 1 carlos carlos 220 2009-12-27 18:16 .bash_logout
-rw-r--r-- 1 carlos carlos 191 2009-12-27 18:54 .profile
-rw-r--r-- 1 carlos carlos 3115 2009-12-27 18:16 .bashrc
```

Utilizando terminales de textos podemos encontrar los siguientes ficheros de configuración de usuario:

- **.bash_profile**: aquí podremos indicar alias, variables, configuración del entorno, etc. que deseamos indicar al principio de la sesión.
- **.bash_logout**: aquí podremos indicar acciones, programas, scripts, etc., que deseemos ejecutar al salir de la sesión.
- **.bashrc**: es igual que **.bash_profile**, se ejecuta al principio de la sesión, en este archivo se indican los programas o scripts a ejecutar, a diferencia de **.bash_profile** que configura el entorno.



Si deseamos configurar archivos de inicio o de salida de la sesión gráfica entonces, en este caso, hay que buscar en el menú del entorno gráfico algún programa gráfico que permita manipular que programas se deben arrancar al iniciar la sesión. **En la mayoría de las distribuciones existe un programa llamado *sesiones* o *sessions*, que está ubicado dentro del menú de preferencias, con este programa es posible establecer que programas o scripts queremos que arranquen en el entorno gráfico**(es similar al fichero *bashrc*).

Linux permite que el usuario decida qué tipo de entorno *Xwindow* quiere utilizar, ya sea algún entorno de escritorio como KDE o Gnome. **Dentro del directorio *Home* del usuario, se creará un directorio o archivo oculto, como *.gnome* o *.kde* donde está la configuración personalizada del usuario para ese entorno gráfico. También, dentro de este directorio encontramos varios directorios y archivos de configuración del usuario** (se recomienda modificar estos archivos por las interfaces gráficas que permiten cambiar los fondos, protectores de pantalla, estilos de ventanas, tamaños de letras, etc.).

Algunos comando como *chpasswd* y *newuser* resultan muy útiles y prácticos para dar de alta a múltiples usuarios. Si usamos Linux con *Xwindow* (gnome, kde, etc.) podemos instalar el programa *webmin* (<http://www.webmin.com/>) basado en Web que entre muchas otras cosas te permiten un control total de la administración de usuarios y grupos local y remotamente.

Debes conocer

Para consultar un resumen de los comandos y ficheros referentes a la gestión y configuración de usuarios:

[Guia de referencia Linux.](#) (0.12 MB)

Para saber más

Como fuente de documentación consultar:

[Administración de Linux enlace 1](#) autor: Sergio González Durán

[Administración de Linux enlace 2](#)

Usuarios y grupos predeterminados.

Caso práctico

Cuando se realiza el proceso de instalación de un sistema operativo, por defecto, el propio sistema creará una serie de usuarios y grupos predeterminados. Carlos, como administrador de sistema comprobará dichos objetos para establece las directivas de seguridad más adecuadas para los usuarios y grupos dentro del sistema.

Durante el proceso de instalación de los sistemas operativos se crean automáticamente unos usuarios y grupos de usuarios predeterminados, como es el caso del grupo Administradores del sistema. Estos usuarios predefinidos permiten desde un principio el uso del sistema, el control de los accesos a los recursos, crear otros usuarios para delegar funciones específicas, etc.

En los siguientes apartados estudiaremos, en cada uno de los sistemas operativos, los diferentes usuarios y grupos predefinidos y las funciones que pueden realizar.

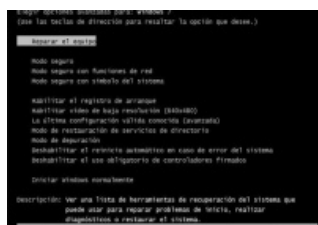


Usuarios y grupos locales predeterminados en Windows 7.

Los usuarios y grupos predeterminados del sistema organizan a los usuarios automáticamente en función del uso del sistema. No se puede cambiar el nombre ni eliminar ninguno de los grupos incorporados. Los privilegios de un tipo de usuario predeterminado determinan qué tareas puede

ejecutar un usuario o miembro de un grupo incorporado, como son: realizar copias de seguridad y restaurar datos, cambiar la hora y administrar los recursos del sistema. **Cuando en un equipo se instala Windows 7, existen de entrada las siguientes cuentas de usuario predeterminadas:**

Cuenta	Descripción
Administrador	<p>La cuenta de Administrador tiene las siguientes características:</p> <ul style="list-style-type: none"> • Pertenece al grupo Administradores en el equipo. • La cuenta Administrador tiene control total del equipo y se usa para administrar el sistema en todos aquellos aspectos en que éste es configurable: usuarios, grupos de usuarios, contraseñas, recursos, derechos, etc. • Nunca se puede eliminar ni quitar del grupo Administradores, pero es posible cambiarle el nombre o deshabilitarla. • Aunque la cuenta Administrador esté deshabilitada de forma predeterminada, siempre puede usarse para obtener acceso a un equipo con el modo seguro. • Se recomienda configurarla de modo que use una contraseña segura.
HomeGroupUser\$	<p>Cuenta integrada para el acceso de un grupo de hogar. Dispone de la contraseña que se da al grupo de hogar, y desde ahí pueden acceder todos los recursos compartidos de los ordenadores en red con el sistema operativo Windows 7, al conocer la contraseña y ser siempre el mismo usuario.</p>
Invitado	<p>La cuenta Invitado tiene las siguientes características:</p> <ul style="list-style-type: none"> • No requiere ninguna contraseña y la pueden utilizar usuarios que no disponen de cuenta en el equipo. • La cuenta Invitado está deshabilitada de forma predeterminada, pero puede habilitarla. • Es miembro del grupo predeterminado Invitados. • Dispone de privilegios mínimos en el sistema.



Durante el proceso de instalación el sistema te invita a crear una cuenta del grupo de Administradores con un nombre de usuario y una contraseña. Desde *Inicio-Administración de equipos-Usuarios y grupos locales de MMC*(Microsoft Management Console), en la carpeta *Usuarios*, se muestran las cuentas de usuarios predeterminados y las creadas por los usuarios. Estas cuentas de usuario predeterminadas se crean automáticamente al instalar el sistema operativo.

Cuando se crea una cuenta nueva puede pertenecer al tipo de cuenta de categoría de administrador o cuenta estándar (elección predeterminada) que puede usar la mayoría de software y puede cambiar la configuración que no afecte al resto de usuarios y a la configuración del equipo. **El tipo de usuario estándar, de forma predeterminada, es miembro de los grupos HomeUsers y Usuarios.** En el proceso de instalación, el sistema nos invita a crear una de administrador independiente de la ya creada por el sistema llamada

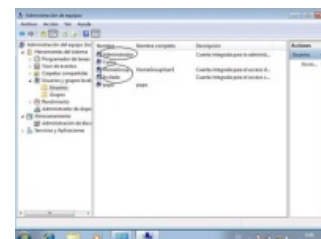
Administrador a la que debemos poner clave.

La cuenta del sistema llamada Administrador si deseamos habilitarla debemos de ir a *Inicio-Administración de equipos- Usuarios y grupos locales*, entrar en la carpeta de *Usuarios*, de la lista de usuarios del panel central seleccionar la cuenta de *Administrador* y pulsar el botón derecho del ratón elegir la opción *Propiedades* y de la ventana de formulario desactivar la opción *La cuenta está deshabilitada*, seguidamente se recomienda poner una contraseña volviendo a seleccionar el usuario y pulsando el botón derecho del ratón elegir la opción de *Establecer contraseña* rellenando los campos solicitados en el formulario.

Es aconsejable no habilitar la cuenta de Administrador, solamente se recomienda su uso para entrar el sistema en caso de fallo pulsando la tecla F8 durante el proceso de inicio del sistema. Donde nos aparecerá el menú que muestra la figura siguiente que nos permitirá seleccionar un modo de entrada al sistema en caso de producirse algún error o fallo en la entrada o acceso normal, si seleccionamos *Modo seguro* entraremos con la cuenta de *Administrador*.

Clasificación de Grupos de usuarios locales predeterminados en Windows 7.

Para gestionar grupos de usuarios locales predeterminados tenemos que ir desde Inicio-Administración de equipos-Usuarios y grupos locales de MMC en la carpeta *Grupos*, se muestran los grupos locales predeterminados y los creados por los usuarios. **Un usuario puede pertenecer a varios grupos y acumular la suma de privilegios en el sistema de todos ellos. Los grupos predeterminados del sistema son:**



- **Administradores:** los usuarios de este grupo tienen control total del equipo y pueden asignar derechos de usuario y permisos de control de acceso a los usuarios según sea necesario. Cuando un equipo se une a un dominio, el grupo Administrador de dominio se agrega automáticamente a este grupo. Los derechos que tienen los usuarios que pertenecen a este grupo son:

- Tener acceso a este equipo desde la red
- Ajustar las cuotas de la memoria para un proceso
- Permitir el inicio de sesión local
- Permitir el inicio de sesión mediante los Servicios de Escritorio remoto
- Hacer copias de seguridad de archivos y directorios
- Omitir comprobación de recorrido
- Cambiar la hora del sistema
- Cambiar la zona horaria
- Crear un archivo de paginación
- Crear objetos globales
- Crear vínculos simbólicos
- Depurar programas
- Forzar cierre desde un sistema remoto

- Suplantar a un cliente tras la autenticación
- Aumentar prioridad de programación
- Cargar y descargar controladores de dispositivo
- Iniciar sesión como proceso por lotes
- Administrar registro de seguridad y auditoría
- Modificar valores de entorno firmware
- Realizar tareas de mantenimiento del volumen
- Analizar un solo proceso
- Analizar el rendimiento del sistema
- Quitar equipo de la estación de acoplamiento
- Restaurar archivos y directorios
- Apagar el sistema

- Tomar posesión de archivos y otros objetos.

- **Operadores de copia de seguridad:** los usuarios de este grupo pueden hacer copias de seguridad y restaurar archivos de un equipo, independientemente de los permisos que protejan dichos archivos. Los miembros de este grupo no pueden cambiar la configuración de seguridad. Pueden realizar tareas como:

- | | |
|--|--|
| <ul style="list-style-type: none"> • Tener acceso a este equipo desde la red • Permitir el inicio de sesión local • Hacer copias de seguridad de archivos y directorios • Omitir comprobación de recorrido | <ul style="list-style-type: none"> • Iniciar sesión como proceso por lotes • Restaurar archivos y directorios • Apagar el sistema |
|--|--|

- **Operadores criptográficos:** los usuarios de este grupo están autorizados a realizar operaciones criptográficas.
- **Usuarios de COM distribuido:** este grupo pueden iniciar, activar y usar objetos DCOM en un equipo.
- **Invitados:** los usuarios de este grupo tienen un perfil temporal que se crea al iniciar la sesión y que se elimina cuando el miembro la cierra. La cuenta Invitado está deshabilitada de forma predeterminada.
- **IIS_IUSRS:** Es un grupo integrado que usa el servicio de publicación Web Internet Information Services (IIS).
- **Operadores de configuración de red:** Los miembros de este grupo pueden modificar la configuración TCP/IP, y renovar y liberar las direcciones TCP/IP. Este grupo no dispone de miembro predeterminado.
- **Usuarios del registro de rendimiento:** pueden administrar los contadores de rendimiento, los registros y las alertas de un equipo, tanto de forma local como desde clientes remotos.
- **Usuarios del monitor de sistema:** pueden supervisar los contadores de rendimiento de un equipo, tanto de forma local como desde clientes remotos, sin ser miembros de los grupos Administradores o Usuarios del registro de rendimiento.
- **Usuarios avanzados:** los usuarios de este grupo no tienen más derechos o permisos de usuario que una cuenta de usuario estándar. En el caso de las aplicaciones heredadas que requieren los mismos derechos y permisos del grupo Usuarios avanzados que se encontraban en versiones anteriores de Windows, los administradores pueden aplicar una plantilla de seguridad que los otorgue.
- **Usuarios de escritorio remoto:** Los miembros de este grupo pueden iniciar una sesión en el equipo de forma remota.
- **Replicador:** los usuarios de este grupo admiten funciones de réplica. El único miembro del grupo Replicador debe ser una cuenta de usuario de dominio que se use para iniciar sesión en los servicios de Replicador de un controlador de dominio. No agregue a este grupo cuentas de usuario de usuarios reales.
- **Usuarios:** los usuarios del grupo pueden realizar las tareas más habituales, como ejecutar aplicaciones, usar impresoras locales y de red, y bloquear el equipo. Los miembros de este grupo no pueden compartir directorios ni crear impresoras locales. Todas las cuentas de usuario que se crean en el dominio son miembros de este grupo. Pueden realizar mismas tareas como las descritas en **Operadores de copia de seguridad**.
- **Ofrecer aplicaciones auxiliares de asistencia remota:** Los miembros de este grupo pueden ofrecer Asistencia remota a los usuarios de este equipo.

El grupo de usuarios especial Hogar de Windows 7.

Los equipos que ejecutan Windows 7 en redes domésticas también pueden ser parte de un grupo especial denominado *Grupo en el hogar*, pero no es imprescindible. En Windows 7 Starter y Windows 7 Home Basic, puede unirse a un grupo en el hogar, pero no crear uno. **Cuando se instala un equipo con una versión de Windows 7, se creará un grupo en el hogar de forma automática. Si se desea crear, hay que seguir los siguientes pasos:**



1. Desde **Inicio-Panel de control-Grupo Hogar**.
2. En la página *Compartir con otros equipos domésticos que ejecutan Windows 7*, hacemos clic en **Crear un grupo en el hogar**, a continuación, seguimos las instrucciones del asistente. Si ya existe un grupo en el hogar en la red, Windows te preguntará si desea unirse a ese grupo en lugar de crear uno nuevo.
3. Después de crear un grupo en el hogar, debes agregarle otros equipos de manera que pueda tener acceso a las carpetas, ficheros e impresoras compartidas. **Mientras los demás equipos no se unan al grupo en el hogar, no podrá obtener acceso a sus recursos y archivos compartidos.** Para ello, debemos realizar los siguientes pasos:
 1. Desde **Inicio-Panel de control** (poner si no está, en el campo *ver por: Iconos pequeños*)-**Grupo Hogar**
 2. Hacer clic en **Unirse ahora** y, a continuación, completar el asistente.

Para comprobar si el equipo pertenece a un grupo en el hogar:

1. Desde **Inicio-Panel de control** (poner si no está, en el campo *ver por: Iconos pequeños*)-**Centro de redes y recursos compartidos**.
2. Si se especifica **Unido junto a Grupo Hogar**, el equipo pertenece a un grupo en el hogar.

Para obtener acceso a archivos o carpetas en otros equipos del grupo en el hogar:

1. Pulsar **Inicio** y escribir el nombre de usuario en el campo de **Búsqueda**. En el panel de navegación en la zona izquierda seleccionar el nombre de usuario y de la ventana pulsar del menú del panel izquierdo en la opción **Grupo Hogar**, haga clic en el nombre de la cuenta de usuario de la persona a cuyos archivos desea obtener acceso.
2. En la lista de archivos, hacer doble clic en la biblioteca a la que desea obtener acceso y, a continuación, doble clic en el archivo o la carpeta en la que desea Incluir una ubicación del grupo en el hogar en una biblioteca.

Para disponer de un acceso rápido a un recurso compartido de otro miembro del grupo del hogar:

1. Pulsar en **Inicio** y hacer clic en el nombre de usuario.
2. En el panel de navegación (panel izquierdo) dentro de la sección **Grupo en el hogar**, hacer doble clic en el equipo al que desea obtener acceso. Buscar la carpeta que desea incluir, seleccionarla y pulsar el botón derecho del ratón, pulsar en la opción **Incluir en biblioteca** y, a continuación, seleccionar la biblioteca de destino.

Acceder a una impresora del grupo en el hogar:

1. Hacer clic en el mensaje que aparece "Windows encontró una impresora del grupo en el hogar".

Instalar una impresora del grupo en el hogar:

1. En el equipo en el que está conectada físicamente la impresora, pulsar en *Inicio-Panel de control*, escribir grupo hogar en el campo de *Búsqueda* y, a continuación, pulsar en *Grupo Hogar*. Seleccionar la casilla *Impresoras*.
2. Desde el equipo que deseas imprimir. Pulsar en *Inicio-Panel de control*, escribir grupo hogar en el campo de *Búsqueda*, y pulsar en *Grupo Hogar*. Hacer clic en *Instalar impresora*. Si no tenemos un controlador instalado para la impresora, pulsar en *Instalar controlador*.

Usuarios y grupos locales predeterminados en Windows Server 2008.

Podemos distinguir tres tipos de cuentas de usuarios predeterminadas en Windows Server, que permiten al usuario un nivel diferente de control sobre el equipo y son las siguientes:

- **Estándar:** puede realizar funciones como la ejecución de las aplicaciones, pero no puede realizar operaciones de cambios en el sistema que afecten al resto de los usuarios y a la seguridad del equipo, como puede ser la instalación de software, hardware, alta/baja/modificación de usuarios, etc.
- **Administrador:** puede realizar cambios que afecten a otros usuarios como configurar la seguridad del sistema, instalar software y hardware, configurar usuarios (altas, bajas y modificaciones). En la instalación del sistema Windows solicita la clave del usuario Administrador que debe de cumplir una reglas de escritura como que disponga de letras en mayúscula, minúscula y números, además de una longitud de más de seis caracteres.
- **Invitado:** es una cuenta para los usuarios que no tiene asignada una cuenta en el equipo, permite usar el ordenador sin poder acceder a archivos personales, no pueden instalar software y hardware, ni cambiar la configuración y no pueden crearse una contraseña. Por seguridad está deshabilitada.



Para gestionar cuentas de usuario de forma fácil, debemos ir desde *Inicio-Panel de control-Cuentas de usuario-Agregar o quitar cuentas de usuario-Crear una cuenta*. Cuando se crea una cuenta de usuario el sistema nos preguntará si es un usuario de tipo *estándar* o *administrador*.

En el proceso de instalación del sistema Windows Server creará dos cuentas predeterminadas, la de *Administrador* y la de *Invitado* que por seguridad permanecerá deshabilitada. El *Administrador* es el encargado de crear el resto de las cuentas de los usuarios y puede hacer que cada una pertenezca a un grupo o grupos que estime conveniente. También puede crear nuevos grupos que tengan unos derechos y privilegios conforme a las necesidades particulares de la organización donde se ubique el sistema.

En sistemas integrados con dominios o servicios de directorio (Active Directory) es posible crear cuentas de acceso tanto en las estaciones de trabajo locales o terminales como para el dominio o directorio activo con el fin de que todas las cuentas sean válidas para todos los ordenadores y los recursos de toda la red que se administren o gestionen desde un controlador de ese dominio. Las cuentas de usuario de Active Directory representan entidades físicas, como personas. Las cuentas de usuario también se pueden usar como cuentas de servicio dedicadas para algunas aplicaciones.

Autoevaluación

¿Qué cuenta o cuentas se encuentran deshabilitadas al entrar en el sistema de Windows Server?

☐ Administrador.
 ☐ Invitado.
 ☐ Administrador e Invitado.
 ☐ Ninguna.

Clasificación de Grupos de usuarios locales predeterminados en Windows Server 2008.

Podemos distinguir en un servidor de Windows lo que son cuentas locales y cuentas de dominio. La cuenta local se utiliza para acceder desde la propia máquina a los recursos del equipo realizando una comprobación de su nombre de usuario y la contraseña, almacenados en una base de datos de seguridad local. La cuenta de acceso a un dominio, nos permite el acceso a los recursos de todo un dominio, considerando que un dominio es un conjunto de equipos (clientes y servidores) y dispositivos conectados en una estructura de red, que comparten una base de datos de seguridad del sistema, la cual contiene información de cuentas de usuarios y privilegios de acceso a los recursos y equipos.



Los grupos incorporados son aquellos que tienen privilegios predeterminados de usuario. Los privilegios de usuario determinan qué tareas puede ejecutar un usuario o miembro de un grupo incorporado. Estos son los tres tipos de grupos incorporados en Windows:

- **Grupos locales incorporados:** otorgan a los usuarios privilegios que les permiten ejecutar tareas de sistema como realizar copias de seguridad y restaurar datos, cambiar la hora y administrar los recursos del sistema. Se encuentran en todas los equipos que ejecutan Windows.
- **Grupos globales incorporados:** proporcionan a los administradores una forma sencilla de controlar a todos los usuarios del dominio. Los grupos globales se encuentran únicamente en los controladores de dominio.

- **Los grupos de sistema:** organizan a los usuarios automáticamente en función del uso del sistema. Los administradores no agregan usuarios a estos grupos. Los usuarios pueden ser miembros de estos grupos de forma predeterminada, o pueden convertirse en miembros a través de su actividad en la red. Se encuentran en todos los equipos que ejecutan Windows



Para facilitar las tareas de administración de red, el uso de los servicios o recursos y organizar coherentemente el acceso a la red, existen en los sistemas operativos de red otras entidades de administración denominadas cuentas de grupo o simplemente grupos. **Una cuenta de grupo es una colección de cuentas de usuario. Al conceder a un usuario la pertenencia a un grupo, se le asignan automáticamente todas las propiedades, derechos, características, permisos y privilegios de ese grupo.** En este sentido, las cuentas de grupo

proporcionan una forma sencilla de configurar los servicios de red para un conjunto de usuarios de características similares.

Para administrar grupos de usuarios locales iremos desde Inicio-Administrador del servidor, haciendo clic en el apartado *Configuración* del panel izquierdo de la consola MMC (Microsoft Management Console), se encuentra la opción *Usuarios y grupos locales* que al desplegar aparece la carpeta *Grupos* y al hacer doble clic sobre ellas aparecen los grupos locales predeterminados, que se crean automáticamente al instalar el sistema operativo. **La lista de grupos los grupos predeterminados y los derechos de usuario predeterminados para cada grupo son los mismos que los estudiados en Windows 7 en el apartado 2.1.1 del tema: Clasificación de Grupos de usuarios locales predeterminados en Windows 7 (puedes acceder y repasar la lista).**

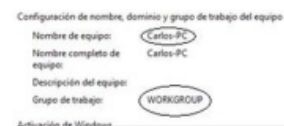
Podemos concluir diciendo que los usuarios y grupos predeterminados de Windows Server 2008 son los mismo que para Windows 7 Premium, es decir, son usuarios de ámbito local al sistema operativo del ordenador. En Windows Server 2008, cuando creamos el dominio en el servidor, los usuarios de ámbito local pasan automáticamente a ser usuarios y grupos de usuarios de ámbito global y pasan a formar parte de la estructura organizativa del llamado Active Directory. Posteriormente los usuarios dispondrán de privilegios y derechos de acceso a los diferentes servicios habilitados en el servidor y de los recursos que forman parte de la red. Por ejemplo cuando se instala el Terminal Server, los usuarios podrán ser usuarios de Servicio de terminal, (dependiendo de las licencias contratadas y disponibles para este servicio ya comentado en la unidad I apartado "Instalación/desinstalación de aplicaciones. Requisitos, versiones y licencias"), que permite que un usuario desde un equipo cliente pueda ejecutar aplicaciones Windows en un servidor.

Diferencias entre grupos de equipos de Windows.

Los equipos que ejecutan Windows en una red deben ser parte de un grupo de trabajo o de un dominio. Las diferencias de que un equipo pertenezca a un grupo u otro son:

GRUPO DE TRABAJO	GRUPO DE HOGAR	DOMINIO
<ul style="list-style-type: none"> -Ningún equipo tiene el control sobre otro. - Para iniciar sesión en cualquier equipo del grupo de trabajo, debe disponer de una cuenta en el equipo. - Un grupo de trabajo no está protegido con contraseña. - Todos los equipos deben encontrarse en la misma red local o subred. 	<ul style="list-style-type: none"> - Un grupo en el hogar permite compartir fácilmente imágenes, música, vídeos, documentos e impresoras con otras personas de una red doméstica. - El grupo en el hogar está protegido con contraseña, pero solo es necesario escribir la contraseña una vez, al agregar el equipo al grupo en el hogar 	<ul style="list-style-type: none"> - Uno o más equipos son servidores. - Con una cuenta de usuario en el dominio, se puede iniciar sesión en cualquier equipo del dominio sin necesidad de disponer de una cuenta en dicho equipo. - Un dominio puede incluir muchos de los equipos que pueden encontrarse en diferentes redes locales.

Podemos comprobar si un equipo está integrado dentro de un grupo de trabajo de ordenadores o en un dominio, (identificado dentro de un servidor que actúa como controlador de dominio) clic en Inicio seleccionamos *Equipo* y pulsamos el botón derecho del ratón, clic en *Propiedades* donde veremos la configuración de nombre, dominio y grupo de trabajo.



Para saber más

Como fuentes de documentación consultar:

[Administración de Windows 7](#)



Autoevaluación

¿La utilidad Grupo de hogar para compartir recursos dentro de una red de ordenadores?

- ☐ Funciona con ordenadores que tengan instalada cualquier distribución de Windows.
- ☐ Funciona con ordenadores que tengan instalada la versión de Windows 7.
- ☐ Funciona con ordenadores que tengan el grupo de trabajo hogar.
- ☐ Funciona con ordenadores que pertenezcan a un dominio llamado grupo hogar.

Usuarios y grupos locales predeterminados en Linux.

Linux dispone de un usuario predeterminado creado en el proceso de instalación por el propio sistema, su nombre es *root* (no es posible



modificar), adquiere la misma contraseña que el primer usuario creado. La cuenta root, por seguridad, no se permite su acceso en el login del sistema, ni desde el acceso remoto (mediante el comando *ssh*), aunque se puede configurar para habilitar ambos accesos desde *Sistema-Administración-Ventana de entrada*. En el caso de acceder al sistema con la cuenta de un usuario estándar, cuando se realiza una actividad de administración el propio sistema reclama la clave del administrador.

El sistema dispone de una serie de grupos predeterminados, que dependen de los recursos y servicios activados en el servidor. **Cuando se da de alta un usuario se crea un grupo con el mismo nombre que el usuario** y con los mismos derechos y privilegios que se conceden al usuario. De la misma forma, **cada vez que se instala un servicio en el ordenador se crea un grupo perteneciente al servicio, se considera que cuando se incluye un usuario a dicho grupo ya dispone de derechos para usar el servicio**. Por ejemplo, si se habilita el servicio *ssh* todos los usuarios que estén incluidos tienen derecho a acceder al servidor remotamente (desde otro terminal).

En el mundo Linux un **usuario es identificado** por un número de usuario, el *uid* (**user ID**) y por un número de grupo el *gid* (**group ID**), que le permite al sistema asociar los procesos mediante esos números identificativos.

La información de **las cuentas de usuario en Linux se almacena dos archivos**:

- */etc/passwd*: en cada línea representa un usuario con la siguiente información, separada por dos puntos:

nombre usuario:contraseña encriptada:uid:gid:descripción de la cuenta:el directorio local [home]:shell

- */etc/shadow*: en cada línea representa un usuario con la siguiente información separada por dos puntos sobre su contraseña:

nombre usuario:contraseña encriptada:último cambio de contraseña:días hasta el cambio permitido:días antes del cambio permitido:días de advertencia para expirar:días antes de inactividad de la cuenta:fecha cuando la cuenta expira

La información de **los grupos de usuario en Linux se almacena en el archivo**:

- */etc/group*: cada línea representa a un grupo con la siguiente información:

nombre grupo: contraseña encriptada o "x" si no tiene contraseña: gid o identif. del grupo:lista de los miembros del grupo

El fichero */etc/login.defs* configura las opciones del login de usuarios, es un fichero de texto en código ASCII.

El directorio */etc/skel* proporciona una forma de estar seguro de que todos los nuevos usuarios de tu sistema LFS tienen la misma configuración inicial. El administrador del sistema puede crear archivos dentro de */etc/skel* que proveerán un amable entorno predeterminado para los usuarios. Por ejemplo, puede crear un */etc/skel/.profile* que configura las variables de entorno de algún editor más amigable para los usuarios nuevos.

Autoevaluación

¿Estando en sesión como usuario root, mediante que comando podemos ver el contenido del fichero passwd?

☐ gedit /etc/passwd.
 ☐ cat /etc/passwd
 ☐ more /etc/passwd
 ☐ Todos los anteriores.

Clasificación de los usuarios y grupos locales predeterminados en Linux.

El sistema crea una serie de usuarios especiales encontrados en el fichero */etc/passwd*, generalmente generados por el sistema, (en nuestro caso en la distribución Ubuntu) durante el proceso de instalación. Dichos usuarios se encuentran incluidos dentro del resto de usuarios, y no aparecen en las aplicaciones de las ventanas gráficas que permitan su configuración, es decir, no se pueden modificar ni borrar, solamente representan ciertos privilegios en el sistema como puede ser el *path*, grupo al que pertenecen, número identificativo *uid*, etc. Podemos encontrar los siguientes **usuarios predeterminados**:

<ul style="list-style-type: none"> • root • daemon • bin • sysync • games • man 	<ul style="list-style-type: none"> • mailnews • uucp • proxy • www-data • backup • list 	<ul style="list-style-type: none"> • irc • gnats • nobody • libuuid • syslogkl • Kog 	<ul style="list-style-type: none"> • hplip: • avahi-autoipd • gdm • saned • pulse • messagebus 	<ul style="list-style-type: none"> • polkituser • avahi • haldaemon • vboxadd • jett
---	---	--	--	---



Los grupos de usuarios especiales encontrados en el fichero */etc/group*, generalmente generados por el sistema (distribución Ubuntu) durante el proceso de instalación son:

<ul style="list-style-type: none"> • root • users • libuuid • syslog • klog • fuse 	<ul style="list-style-type: none"> • ssl-cert • lpadmin • crontab • mlocate • ssh • avahi-autipd 	<ul style="list-style-type: none"> • gdm • netdev • saned • pulse • pulse-access • pulse-rt 	<ul style="list-style-type: none"> • messagebus • polkituser • avahi • haldaemon • admin • sambashare
--	--	---	---

Seguridad de cuentas y contraseñas de usuario.

Caso práctico

Carlos, como usuario administrador del sistema tiene la responsabilidad de gestionar la seguridad del sistema y en el apartado de cuentas de usuario tiene que aprender a realizar el control de dicha seguridad para que no se produzcan posibles alteraciones en el sistema que perjudiquen la actividad empresarial. Deberá de crear políticas de acceso que obligue a ciertos usuarios que tengan responsabilidad en los datos a tratar a modificar la contraseña cada cierto tiempo y que su escritura cumpla con las especificaciones necesarias de seguridad.



El administrador es el encargado de proteger las cuentas de usuario y las contraseñas de autenticación para el acceso al sistema. Además, el administrador tiene que analizar las necesidades de cada usuario y asignarle los privilegios justos y necesarios para realizar su tarea sin peligro de utilizar recursos no autorizados.

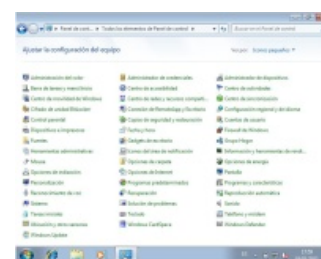
En los siguientes apartados, aprenderemos a gestionar los mecanismos necesarios para ofrecer una buena seguridad de cuentas y contraseñas de los usuarios en los diferentes sistemas operativos.

Seguridad de cuentas y contraseñas de usuario Windows 7.

Windows 7 permite centrar la tarea de administración del equipo desde *Inicio-Panel de control* donde aparecen utilidades de administración y configuración.

Muchas de las opciones que presenta el *Panel de control* se deben de realizar desde una cuenta de administrador. Las cuentas de administrador deben de estar protegidas, ya que su uso por terceras personas, puede acarrear que el equipo deje de funcionar o funcione mal. Por este motivo es aconsejable usar una cuenta de usuario estándar, en lugar de una cuenta de administrador. Con una cuenta estándar podemos realizar muchas tareas, pero si deseamos hacer algo que afecte a los demás usuarios del equipo, como instalar software o cambiar la configuración de seguridad, Windows nos pide una contraseña para una cuenta de administrador.

Un usuario puede acceder desde *Inicio-Panel de control-Cuentas de usuario* a su cuenta y realizar tareas como:



- **Administrar credenciales:** permite almacenar información que incluye la identificación para iniciar sesión automáticamente en sitios web o en otros equipos. Las credenciales se guardan en carpetas especiales del equipo llamadas almacenes. Para agregar una contraseña a tu almacén de Windows:
 1. Desde *Panel de control-Cuentas de usuario-Administrar credenciales*. Hacer clic en *Agregar una credencial de Windows*.
 2. En el cuadro *Dirección de red o Internet*, escribir el nombre del equipo de la red al que desea obtener acceso. Puede ser el nombre NetBIOS (ejemplo: equipo1) o el nombre DNS (ejemplo: equipo1.iesalisal.es)
 3. En los cuadros *Nombre de usuario* y *Contraseña*, escribir el nombre de usuario y la contraseña que se usan para ese equipo o sitio web y hacer clic en *Aceptar*.

Podemos ejecutar desde una ventana de comandos (CMD) el comando **control userpasswords2** que nos mostrara la ventana de Cuentas de usuarios y entre una de las muchas opciones que da, te muestra la Administración de contraseñas.

- **Crear un disco para restablecer contraseña:** crea un disco que puedes utilizar para iniciar sesión, por si se te olvida la contraseña de tu cuenta de usuario. El disco de recuperación solamente se creará una vez, (no cada vez que se cambia de contraseña) y un disco por cuenta de usuario. Se puede almacenar la información de recuperación de contraseña en una unidad flash de USB.
- **Vincular identificadores en línea:** permite agregar, eliminar o cambiar las contraseñas que han sido recordados por Windows para su uso en servidores remotos o sitios web. Una característica útil es que puedes hacer copias de estas claves en un disco y copiar a tu cuenta en otro equipo.
- **Administrar sus certificados de cifrado de archivo (EFS):** para cifrar los archivos con mayor seguridad, hay que disponer de un certificado de cifrado y una clave de descifrado asociada en el equipo o en una tarjeta inteligente. Para poder tener acceso a los archivos cifrados es necesario disponer del **certificado** y la **clave**. El cifrado, es la protección de mayor nivel que proporciona Windows, para ayudarlo a mantener la información a salvo.

Características destacadas de EFS	Operaciones que se pueden hacer con EFS
Para cifrar hay que activar una casilla en las propiedades del archivo o la carpeta	Descifrar los archivos ejecutando Cipher.exe en la ventana del símbolo del sistema como usuarios avanzados
El usuario controla quién puede leer los archivos	Modificar un archivo cifrado
Los archivos se cifran cuando se cierran, cuando se abren quedan automáticamente listos para su uso	Copiar un archivo cifrado como descifrado en el disco duro del equipo e Importar certificados y claves EFS
Para eliminar el cifrado de un archivo, desactiva la casilla en las propiedades del archivo	Hacer copias de seguridad de claves y certificados EFS ejecutando Cipher.exe en la ventana del símbolo del sistema como usuarios avanzados

- **Configurar las propiedades avanzadas de perfil de usuario:** los perfiles del usuario contienen la configuración de escritorio y otro tipo de información relacionada con tu cuenta de usuario. Se puede crear un perfil diferente en cada equipo que se use, o bien seleccionar un perfil móvil para usarlo en cualquier equipo y tener siempre el mismo entorno de trabajo. Si tu ordenador está conectado a una red de dominio, puedes seleccionar que tu perfil de usuario sea de ida y vuelta al servidor de archivos (un perfil móvil), o simplemente mantenerse en el equipo que te has logueado (un perfil local).
- **Cambiar las variables de entorno:** puedes personalizar las variables de entorno de tu cuenta. Las variables de entorno guardan la información como

- Estos requisitos de complejidad se exigen al cambiar o crear contraseñas.
- Longitud mínima de la contraseña: Puede establecer un valor comprendido entre 1 y 14 caracteres, o puedes establecer que no se exija contraseña alguna estableciendo el número de caracteres en 0. Valor predeterminado: 7 en controladores de dominio y 0 en servidores independientes.
- Vigencia máxima de la contraseña: como recomendación de seguridad debe ser los 30-90 días
- Vigencia mínima de la contraseña: Podemos configurar la vigencia mínima de la contraseña de modo que sea mayor que 0. Si deseamos que sea efectiva la configuración: Exigir historial de contraseñas.
- En *Directivas de bloqueo de cuenta*: podemos encontrar las siguientes reglas:
 - Duración del bloqueo de cuenta: El intervalo disponible oscila entre 0 y 99.999 minutos. Si la duración del bloqueo de cuenta se establece en 0, la cuenta se bloquea hasta que el administrador la desbloquee explícitamente.
 - Restablecer el bloqueo de cuenta después de: Esta configuración de seguridad determina el número de minutos que deben transcurrir tras un intento de inicio de sesión incorrecto para que el contador de intentos de inicio de sesión incorrectos se restablezca en 0.
 - Umbral de bloqueo de cuenta: Esta configuración de seguridad determina el número de intentos de inicio de sesión incorrectos, que hacen que una cuenta de usuario se bloquee. Una cuenta bloqueada no puede usarse hasta que un administrador la restablezca o hasta que expire su duración de bloqueo.
- *Directivas locales*: debido al amplio contenido se recomienda el acceso a la ayuda que aporta Windows interactivamente (se da doble clic sobre la directiva seleccionada y pulsamos sobre la pestaña explicación)



Autoevaluación

El comando que nos permite ejecutar la MMC que gestiona las directivas de seguridad local de usuarios es %windir%\System32\secpol.msc.

☐ Verdadera
 ☐ Falsa

Las directivas de seguridad de grupos locales de usuarios en Windows7.



Una directiva de grupo es una característica de Windows que permite a los administradores del sistema administrar el acceso de los usuarios a las características de Windows. Por ejemplo, si el equipo no forma parte de una red, es posible que un usuario con privilegios de administrador haya modificado la directiva de grupo en su equipo para quitar el acceso a la configuración.

Para la administración de la directiva de grupo podemos entrar en el editor de directiva (complemento de Microsoft Management Console o MMC). Este complemento MMC se encuentra en la siguiente ubicación: %windir%\System32\gpedit.msc. Para **abrir el Editor de directivas de grupo local**, hacer clic en *Inicio*, luego en *Ejecutar* y escriba *gpedit.msc*.

Por ejemplo, para cambiar el comportamiento de la herramienta de seguridad UAC (control de acceso de usuarios) mediante directivas de grupo:

1. Dar en *Inicio*, escribir *secpol.msc* en el cuadro *Buscar programas y archivos* y, pulsar en la tecla *Intro*.
2. Se verá el cuadro de diálogo *Control de cuentas de usuario*, confirmar si la acción que aparece es la que se desea, dar en *Sí*.
3. Pulsar en panel izquierdo en *Directivas locales* y clic en *Opciones de seguridad*.
4. En el panel de detalles hacer doble clic en la configuración de directivas de grupo que deseas cambiar. La configuración de directivas de UAC, que un administrador local puede modificar incluye: modo de aprobación de administrador para la cuenta predeterminada Administrador, permitir que las aplicaciones UIAccess pidan confirmación de elevación sin usar el escritorio de seguridad, comportamiento del indicador de elevación para los administradores en Modo de aprobación de administrador, comportamiento del indicador de elevación para los usuarios estándar, detectar instalaciones de aplicaciones y pedir confirmación de elevación, solo elevar ejecutables que estén firmados y validados, solo elevar aplicaciones UIAccess que estén instaladas en ubicaciones seguras, ejecutar todos los administradores en Modo de aprobación de administrador, cambiar al escritorio seguro cuando se pida confirmación de elevación, virtualización de archivos y errores de escritura de registro a ubicaciones definidas por cada usuario.
5. En la página *Propiedades*, realizar las selecciones y a continuación, pulsar en *Aceptar*.

También, es posible configurar la directiva de grupo del Cifrado de unidad BitLocker, para unidades protegidas por BitLocker específicas de la organización o en el equipo local si el equipo no forma parte de un dominio. Las opciones de configuración de la directiva de grupo de BitLocker en la *Consola de administración de directivas de grupo-Plantillas administrativas-Componentes de Windows-Cifrado de unidad BitLocker*. Esto permite a los administradores del sistema definir directivas basadas en el uso de las unidades. Estas opciones de configuración de directiva se pueden aplicar a lo siguiente:

- Todas las unidades: estas opciones de configuración de directiva se aplican a todas las unidades protegidas con BitLocker.

- Unidades de sistema operativo: se trata de la unidad del equipo local en la que está instalado el sistema operativo.
- Unidades de datos fijas: se trata de unidades instaladas permanentemente en el equipo local que no se pueden quitar cuando el equipo está en ejecución.
- Unidades de datos extraíbles: son unidades diseñadas para quitarlas de un equipo y usarlas en otro cuando el equipo está en ejecución.

Para saber más

Sobre las preferencias de directivas de grupo

[Administración de Windows 7](#)

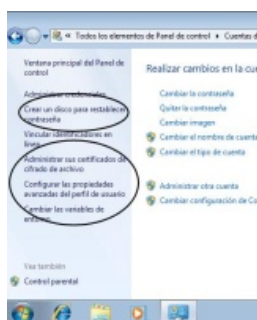


Autoevaluación

El comando que nos permite ejecutar el editor de directivas seguridad de grupos locales de usuarios es `windir%\System32\gpedit.msc`.

- ☐ Verdadera
- ☐ Falsa

Seguridad de cuentas y contraseñas de usuario Windows server 2008.



La seguridad de cuentas y contraseñas de usuarios locales de Windows Server 2008, se basa en la misma teoría que en Windows 2007, es decir, los usuarios locales pueden gestionar utilidades relacionadas con su cuenta desde **Inicio-Panel de control-Cuentas de usuario**, en las que encontramos:

- **Crear un disco para establecer contraseña:** permite generar un arranque desde disco externo o memoria flash USB para el caso de olvidarse la contraseña.
- **Administrar sus contraseñas de red:** para almacenar credenciales de inicio de sesión que permitirán iniciar sesión de forma automática.
- **Administrar sus certificados de cifrado de archivo:** permite generar un certificado de cifrado con una clave para cifrar archivos creando una mayor seguridad en su acceso.
- **Configurar las propiedades avanzadas de perfil de usuario:** mediante los perfiles de usuario se gestiona la información de escritorio y del entorno de trabajo del usuario, permitiendo exportar o importar dicho perfil a otros

entornos de trabajo.

- **Cambiar las variables de entorno:** cada usuario dispone de unas variables del sistema que contiene información importante (para conocer dichas variables repasar el apartado de Administración de usuarios y grupos locales en Windows 7 de esta Unidad).

Otro comentario relacionado con la seguridad de cuentas de usuario, como ya hemos comentado en otros apartados, es la existencia de un dato único que se asocia a cada cuenta, denominado identificador seguro (Secure Identifier, o SID), tanto cuando se crea una cuenta local como cuando se crea una cuenta en el dominio. Este identificador es interno y el sistema lo genera automáticamente cuando se crea una nueva cuenta.

Windows utiliza siempre el SID para controlar si un usuario tiene o no permisos suficientes para llevar a cabo cualquiera de sus acciones. Dado que cada cuenta dispone de un único SID y que está gestionado internamente por el sistema, resulta muy difícil suplantar marcando así un grado alto de seguridad. El SID es único en el dominio e incluye información relacionada con los grupos a los que pertenece el usuario y la configuración de seguridad. **Por seguridad es fundamental realizar las siguientes acciones de configuración:**

- Desactivar la cuenta de *invitado*, que permitiría que cualquier usuario inicie sesión en el sistema.
- Cambiar el nombre de la cuenta de *administrador* para reducir el riesgo de intrusión mediante esta cuenta. Debido a que la cuenta de *administrador* posee todos los permisos, es un objetivo prioritario de los posibles intrusos.
- También se debe completar, siguiendo la directiva de seguridad de contraseñas, todas las reglas existentes para las mismas.

Podemos establecer una serie de políticas o directivas por defecto asignadas a cada cuenta que mejoran su seguridad en el momento de su creación o alta en el sistema, estas condiciones también se pueden cambiar en cualquier momento. Entre ellas se encuentran las siguientes:

- *El usuario debe cambiar la contraseña en el siguiente inicio de sesión.*
- *El usuario no puede cambiar su contraseña.*
- *La contraseña no caducará nunca.*
- *La cuenta quedará desactivada en un plazo de tiempo.*
- *La cuenta se bloqueará si ocurre un número de fallos de presentación consecutivos previamente fijado.*



Autoevaluación

¿Cuál de las siguientes opciones sobre contraseñas de usuarios en Windows7 no está disponible?

- ☐ El usuario no puede cambiar la contraseña
- ☐ La contraseña nunca caduca
- ☐ La contraseña está bloqueada.
- ☐ Ninguna de las anteriores

Directivas de seguridad local en Windows Server 2008.

Las directivas de seguridad local referentes a usuario y grupos son idénticamente iguales a las de Windows 7. Un listado de las directivas de cuenta es:

Directiva de contraseñas
Aplicar el historial de contraseñas
Vigencia máxima de la contraseña
Vigencia mínima de la contraseña
Longitud mínima de contraseña
La contraseña debe cumplir requisitos de complejidad
Almacenar contraseñas con cifrado reversible
Directiva de bloqueo de cuenta
Duración del bloqueo de cuenta
Umbral de bloqueo de cuenta
Restablecer recuentos de bloqueo de cuenta tras...
Directiva Kerberos
Aplicar restricciones de inicio de sesión de usuario
Vigencia máxima del vale de servicio
Vigencia máxima del vale de usuario
Vigencia máxima de renovación de vales de usuario
Tolerancia máxima para la sincronización de los relojes de los equipos

La directiva de grupo es un conjunto de una o más políticas del sistema. Cada una de las políticas o reglas del sistema establece una configuración del objeto al que afecta. Gracias a las reglas de directiva de grupo podemos controlar los entornos de trabajo de los usuarios del dominio, los equipos y el comportamiento de los diferentes objetos y elementos que conforman la estructura del dominio en red. Por ejemplo, indicar los scripts que se ejecutan al inicio y final de sesión de equipo o usuario, cambiar la actuación de los permisos de usuarios y grupos, bloquear cuentas, limitar las funcionalidades de los equipos, etc.

Las políticas o directivas de grupo pueden estar contenidas en cuatro tipos de objetos:



- Equipos Locales o directiva de grupo local:** son aplicadas únicamente en el equipo que las tiene asignadas independientemente del dominio al que pertenezcan. Son modificadas con "gpedit.msc". Estas son las únicas políticas que se aplican a los equipos que no están en un dominio, como servidores independientes (stand alone) o clientes en redes de igual a igual (peer to peer).
- Sitios de Active Directory o directiva de sitio de grupo:** se aplican para todos los equipos y/o usuarios de un sitio, independientemente del dominio del mismo bosque al que pertenezcan.
- Dominios de Active Directory o directiva de grupo de dominio:** se aplican a todos los equipos y/o usuarios de dominio.
- Unidades Organizativas de Active Directory directiva de grupo de unidad organizativa:** se aplican únicamente a los equipos y/o usuarios que pertenezcan a la propia unidad organizativa (OU).

En el momento que en el sistema se crea el Dominio, los usuarios pasaran a ser usuarios del dominio y lo mismo ocurrirá con lo referente a la directiva de seguridad. Esto ocurre debido al modo en que la directiva de grupo se hereda mediante la estructura de Active Directory. Cuando se instala el Active Directory se crean un conjunto de directivas de grupo predeterminadas y editables (Estudiaremos este tema en la Unidad 6). La herramienta de administración que gestiona las directivas de grupo en Windows Server 2008 es el llamado complemento de Administración de directivas de grupo. En cada ordenador hay unos objetos de directiva grupo local (GPO) encontrada en el directorio `SystemRoot\System32\GroupPolicy`. En el controlador de dominio se encuentran los objetos de las directivas de grupo (GPO) de Active Directory (tienen prioridad sobre las directivas locales) y se guardan en el directorio `Sysvol`. A un equipo en red se le pueden aplicar directivas de grupo local y directivas de grupo de Active directory.

Para saber más

Para más documentación sobre seguridad de contraseñas consultar:

[Administración de contraseñas Windows Server I](#)

[Administración de contraseñas Windows Server II](#)

Introducción a las copias de seguridad y restauración de archivos en Windows Server 2008.

Caso práctico

Como medida preventiva en "Gestisa" para no perder datos importantes, ha adoptado la medida de programar copias de seguridad de forma periódica, y Carlos se encargará de ello.

Mediante las copias de seguridad podemos proteger los archivos y carpetas relacionados con usuarios y contraseñas, del registro del sistema, de la base de datos del Active Directory, etc. Cuando se hace una copia completa del sistema (System State) hacemos copia de todos los objetos y componentes que nos permitirán restaurar el servidor por completo, en caso de producirse un fallo o error en el sistema. **Se dispone de asistentes de ventanas que ayudan para configurar una programación de copia de seguridad automática, también podemos crear copias de seguridad manuales desde PowerShell** (consola de comandos) en caso necesario, y recuperar elementos o volúmenes enteros. Además, en caso de desastres como errores del disco duro, puede realizar una recuperación del sistema, que restaurará el sistema completo en el nuevo disco duro mediante una copia de seguridad del servidor completo y el Entorno de recuperación de Windows. La **Copia de seguridad** dispone de herramientas como:



- | | |
|---|---|
| <ul style="list-style-type: none"> La interfaz de usuario de MMC (WBADMIN.MCS) La interfaz de línea de comandos (WBADMIN.EXE) | <ul style="list-style-type: none"> El servicio de copias de seguridad (WBENGINE.EXE) El conjunto de cmdlets de Windows PowerShell |
|---|---|

Para usar Copias de seguridad debe ser miembro de los grupos *Operadores de copia de seguridad* o *Administradores*, los miembros de este grupo no pueden cambiar la configuración de seguridad. También, **es aconsejable crease una nueva unidad o partición para alojar las copias de seguridad de forma independiente a la unidad que contienen todos los programas que forman el sistema operativo**. En Windows Server 2008, el firewall está habilitado de manera predeterminada. Esto puede afectar si estamos administrando las copias de seguridad de otro equipo mediante el complemento Copias de seguridad de Windows Server de Microsoft Management Console (MMC)

Copias de seguridad de Windows Server incluye, las siguientes características:

- Copias de seguridad para hacer una copia de seguridad de un servidor entero o de volúmenes seleccionados.
- Se puede administrar copias de seguridad en servidores remotos. haciendo clic en Acción y, después, en Conectar a otro equipo.
- Tecnología de copia de seguridad nueva y más rápida.
- Podemos configurar Copias de seguridad para ejecutar de forma automática copias de seguridad incrementales que guarden únicamente los datos que han cambiado desde la última copia de seguridad.
- Podemos restaurar elementos eligiendo una copia de seguridad de la que recuperarlos y eligiendo a continuación los elementos para restaurar (para recuperar archivos específicos de una carpeta o todo su contenido).
- Puede recuperar en el mismo servidor o, si el hardware tiene un error, en un servidor nuevo que no tenga sistema operativo.
- Hay que instalar el complemento de Copias de seguridad para tener acceso a esta herramienta mediante el Administrador del servidor, o bien puede agregar el complemento a una consola MMC nueva o existente. Para ello debemos agregar una Característica al servidor
- También es posible automatizar las actividades de copia de seguridad mediante la creación de scripts, desde la consola de PowerShell en línea de comandos
- Podemos realizar copias manuales directas en un DVD.

Configuración de copias de seguridad y restauración de archivos en Windows Server 2008.

Para instalar herramientas de copia de seguridad y recuperación, debemos seguir los siguientes pasos:

- Desde Inicio . *Administrador del servidor* . *Características* . *Agregar característica*, seleccionar *Característica de Copias de seguridad de Windows Server* y activar las casillas *Copias de seguridad de Windows Server* y *Herramientas de línea de comandos*, nos aparece un mensaje que nos indica que también se instala en el PowerShell. Dar a *Siguiente* y pulsar en *Instalar* para confirmar el proceso.

Podemos acceder a realizar una copia de seguridad y recuperación de la siguiente forma:

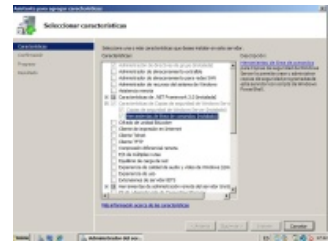
- Desde Inicio-Herramientas administrativas-Copias de seguridad de Windows Server o desde Inicio, pulsar el botón derecho de ratón en la opción *Símbolo del sistema* y elegimos *Ejecutar como Administrador*, en la línea de comandos escribir la orden `wbadmin /?`. También, con los



comandos podemos copiar y restaurar:

- Comando `Wbadmin start systemstatebackup`: creamos una copia de seguridad del estado del sistema.
- Comando `Wbadmin start systemstaterecovery`: recuperamos el estado del sistema.

El manual de PowerShell se encuentra en: `C:\>:\Windows\System32\WindowsPowerShell\v1.0\Documents\es-ES`

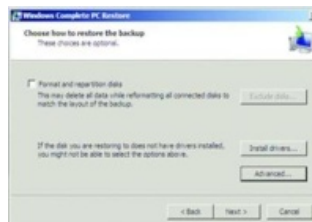


Podemos restaurar el sistema al arrancar Windows Server 2008

desde los medios de instalación, puedes elegir la opción *Reparar el equipo*, seguidamente en la pantalla de instalación, Windows te permite seleccionar una opción de restauración.

En este caso, podemos seleccionar *Restauración de Windows Complete PC*, que invoca el entorno de recuperación de Windows. Una vez selecciona el sistema operativo que deseamos reparar (normalmente sólo hay una opción), *WinRE* te permite seleccionar la copia de seguridad desde la que desea realizar la restauración. De forma

predeterminada, *WinRE* selecciona la copia de seguridad de sistema completa más reciente, aunque puede especificar otras copias de seguridad almacenadas en discos locales o buscar en la red copias de seguridad que se almacenan en recursos compartidos de archivos en otros servidores. Después de realizar dos afirmaciones, *WinRE* inicia el proceso de restauración y el servidor se vuelve a arrancar. De esta manera es posible llevar a cabo, sin problemas, una restauración completa en un servidor.



Debes conocer

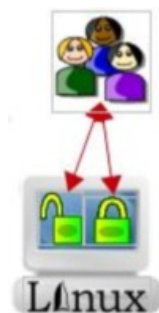
Consultar el documento siguiente que nos enseña a realizar copias de seguridad o backup y restauraciones en Windows Server 2008.

[Guía referencia copia de seguridad Windows Server \(0.14 MB\)](#)

Para saber más

Podemos obtener más documentación desde el Manual de ayuda interactivo del propio sistema operativo Windows Server instalado.

Seguridad de cuentas y contraseñas de usuario Linux.



La cuenta de root o cuenta de superusuario administrador es una cuenta presente en todos los sistemas Linux que usualmente no tiene ninguna restricción. El root puede hacer cualquier cosa. Por ese motivo, **usualmente es recomendable no hacer login y usar el sistema como root, a no ser que eso sea absolutamente necesario**. Por seguridad, es siempre mejor trabajar como un usuario normal en vez del usuario root, y cuando se requiera hacer uso de comandos solo de root, utilizar los comandos `su` y `sudo`.

Cada usuario del sistema tiene un identificador de usuario único, el UID, asociado a su nombre de usuario (es posible atribuir dos nombres de usuario a un mismo UID, aunque no es recomendable, creando una misma cuenta con dos nombres que pueden ser usados para hacer login).

Cada usuario pertenece por lo menos a un grupo de usuarios (tendrá su mismo nombre de usuario y se crea, por defecto, al dar de alta al usuario), **y cada grupo tiene un identificador único de grupo (GID) asociado al nombre del grupo**. El Shell por defecto es particularmente importante para cuentas del sistema. Si no hubiese un Shell válido asignado al usuario, este no podría hacer login en el sistema.

Como hemos comentado en apartados anteriores en todo sistema Linux hay tres archivos que ofrecen el nivel más básico de autenticación para el sistema local: `/etc/passwd`, `/etc/group` y `/etc/shadow`, el acceso a estos archivos debe de ser restringido a los usuarios del sistema, solamente el usuario root tendrá todos los derechos, mientras que el resto solamente de lectura e incluso en el archivo `shadow` ningún derecho ya que guarda las contraseñas cifradas de los usuarios.

La seguridad de los archivos passwd, shadow y group en Linux.

Dentro del directorio `/etc` se encuentra el fichero `passwd` donde se definen por cada línea de fichero una cuenta de usuario. Podemos ver el contenido del fichero como usuario root desde el menú del escritorio *Aplicaciones-Accesorio-Terminal*. En la línea de consola de comandos se ejecuta la orden:



```
root@sistemaubuntu:~# more /etc/passwd
root:x:0:0:root:/root:/bin/bash
```

```
carlos:x:1000:1000:carlos,,,:/home/carlos:/bin/bash.....
```

Las contraseñas cifradas no se suelen almacenar en el fichero *passwd* ya que puede ser leído por cualquier usuario y con programas de descifrado se pueden descubrir. Linux dispone del fichero *shadow* encargado de almacenar las contraseñas encriptadas y solamente puede ser leído y modificado por el usuario *root*, además dispone de campos de control de contraseñas. La información de cada usuario del fichero */etc/shadow* se encuentra en campos delimitados cada uno por dos puntos. Si queremos ver el contenido ejecutamos como usuario *root* el comando:

```
root@sistemaubuntu:~# more /etc/shadow
```

```
carlos:$6$pSwsW.b0$5uCoovxVZ5YTq.YnuxYIG9fgrdxgfdgvbfg43434534534534YbabuLSB1:14642:0:99999:7:::
```

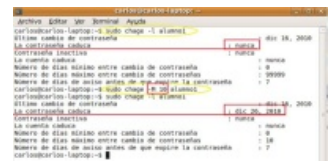
La información obtenida en dicho fichero es:

Campo 1	Nombre de la cuenta del usuario.
Campo 2	Contraseña cifrada o encriptada, un * indica cuenta de nologin .
Campo 3	Días transcurridos desde el 1/ene/1970 hasta la fecha en que la contraseña fue cambiada por última vez.
Campo 4	Número de días que deben transcurrir hasta que la contraseña se pueda volver a cambiar.
Campo 5	Número de días tras los cuales hay que cambiar la contraseña. (-1 significa nunca). A partir de este dato se obtiene la fecha de expiración de la contraseña.
Campo 6	Número de días antes de la expiración de la contraseña en que se le avisará al usuario al inicio de la sesión.
Campo 7	Días después de la expiración en que la contraseña se inhabilitara, si es que no se cambió.
Campo 8	Fecha de caducidad de la cuenta. Se expresa en días transcurridos desde el 1/Enero/1970.
Campo 9	Reservado.

Operaciones de configuración de seguridad de las cuentas de usuarios en Linux.

Algunas operaciones que podemos realizar con la seguridad de cuentas de usuarios:

- Podemos definir un período después del cual la contraseña debe ser cambiada con el comando *chage*. Por ejemplo si queremos obligar al usuario Carlos a modificar la contraseña cada sesenta días, y que le de aviso cinco días antes de que la contraseña va a caducar, puedo hacerlo con el comando:



```
root@sistemaubuntu:~# chage -M 0 -W 560 Carlos
```

De otra forma cualquier usuario puede ver cuando vence su contraseña con el comando *chage -l*, por ejemplo para el usuario carlos sería:

```
root@sistemaubuntu:~# chage -l carlos
```

```
Último cambio de contraseña : feb 03, 2010
```

```
La contraseña caduca : nunca
```

```
Contraseña inactiva : nunca
```

```
La cuenta caduca : nunca
```

```
Número de días mínimo entre cambio de contraseña : 0
```

```
Número de días máximo entre cambio de contraseñas : 99999
```

```
Número de días de avASIR_ISO antes de que expire la contraseña : 7
```

- Con el comando *pwunconv* elimina el fichero *shadow* pasando las contraseñas cifradas al fichero *passwd*, como el ejemplo siguiente

```
root@sistemaubuntu:~# pwunconv
```

```
root@sistemaubuntu:~# more /etc/passwd
```

```
root:dfjsdfj48345345mnfdgm dfgmdfgp:0:0:root:/root:/bin/bash
```

```
carlos:$6$pSwsW.b0$5uCoovxVZ5YTq.YnuxYIG9fgrdxgfdgvbfg43434534534534YbabuLSB1:510:520:Juan Carlos:/home/carlos:/bin/bash
```

```
...
```

```
root@sistemaubuntu:~# more /etc/shadow
```

```
/etc/shadow: No such file or directory
```

- Para reactivar la protección de *shadow*, con el comando *pwconv* que crea *shadow* desde *passwd*. Es conveniente periódicamente ejecutar la orden *pwconv* para asegurarnos de que todas las contraseñas tienen *shadow*

```
root@sistemaubuntu:~# pwconv
```

```
root@sistemaubuntu:~# more /etc/shadow
```

```
carlos:$6$pSwsW.b0$5uCoovxVZ5YTq.YnuxYIG9fgrdxgfdgvbfg43434534534534YbabuLSB1:14642:0:99999:7:::
```

- Las variables que controlan los aspectos de la creación de usuarios y de los campos de *shadow* usadas por defecto están definidas en el archivo de configuración */etc/login.defs*, se pueden usar para modificar aspectos del usuario con el entorno de trabajo en el sistema, algunas de sus variables son:

PASS_MAX_DAYS	Número máximo de días que una contraseña es válida
PASS_MIN_LEN	El número mínimo de caracteres en la contraseña

UID_MIN	Valor mínimo para usuarios normales cuando se usa <i>useradd</i>
UMASK	El valor umask por defecto
CREATE_HOME	Si el comando <i>useradd</i> debe crear el directorio home por defecto
MOTD_FILE	El contenido de este fichero de texto se muestra a todos los usuarios tras identificarse
LOGIN_RETRIES	Número máximo de intentos si se escribe mal la contraseña en la entrada al sistema
SU_WHEEL_ONLY	Limitar permisos de "su" a determinados usuarios al estar en yes sólo grupo <i>root</i>

Alternativas avanzadas de seguridad de cuentas de usuarios en Linux.

Algunas alternativas para la seguridad de contraseñas pueden ser:

- **Las modificaciones o intentos de modificaciones de las contraseñas quedan registradas en el archivo `/var/log/messages`.** Con el comando `less` y los filtros adecuados podemos consultar los mensajes correspondientes a estos cambios o intentos relacionados con las contraseñas, comprobando el terminal, día y hora del acceso al ordenador.
- Root puede periódicamente ejecutar programas que detectan las claves que pueden ser fácilmente descifrables para avisar el usuario a que sea cambiada, como son **Crack** (<http://www.crypticide.org/users/alecm/>) o **John the Ripper**(<http://openwall.com/john>).
- Con la herramienta **passwd+**: podemos realizar un log de todas las sesiones, errores, usuarios que han cambiado su contraseña, reglas que no cumplieran las contraseñas y si ha tenido éxito o no el cambio de contraseña. Podemos encontrar más información en la dirección: <ftp://ftp.dartmouth.edu/pub/security>.
- La aplicación **npasswd** sustituye al comando `passwd` del sistema, más completo y eficiente. Podemos encontrar más información en: <http://www.utexas.edu/cc/unix/software/npasswd>.
- **Control de acceso biométrico**: autentican a los usuarios en función de sus huellas dactilares, voz, etc.
- **Contraseña de un solo uso**: el servidor envía un número al cliente, y éste utiliza este número para generar un valor secreto que se devuelve.
- **En las últimas distribuciones Linux se han integrado los módulos de autenticación PAM** (Pluggable Authentication Modules) desarrollados inicialmente por Sun. **PAM permite decidir el método de autenticación que se requiere para cada servicio o en cada caso.** Cada método tiene sus módulos que son los que manejan cada tipo de petición. Es decir, para cada método de autenticación, como Kerberos, LDAP, etc, se han desarrollado los módulos correspondientes. Por ejemplo, una regla puede permitir que una clase de usuarios solo pueda hacer login en ciertos horarios.



Existen en Linux gran cantidad de módulos PAM disponibles, como por ejemplo el módulo *pam_cracklib.so* que puede ser utilizado por la orden `passwd` para hacer una comprobación contra la biblioteca *pam_cracklib* y determinar si la contraseña elegida por el usuario es débil. O también desactivar el uso en todo el sistema de archivos *.rhosts* en los home de los usuarios. Para ello habría que utilizar el modulo *pam_rhosts_auth.so*.

PAM viene "de serie" en diferentes sistemas Linux, y el nivel de abstracción que proporciona permite cosas tan interesantes como kerberizar (**Kerberos** es un protocolo de autenticación de redes de ordenador que permite a dos computadores en una red insegura demostrar su identidad mutuamente de manera segura) nuestra autenticación (al menos la parte servidora) sin más que cambiar la configuración de PAM, que se encuentra bien en el fichero */etc/pam.conf* o bien en diferentes archivos dentro del directorio */etc/pam.d/*.

El archivo */etc/pam.conf* está formado por una lista de reglas. Cada regla es un conjunto de campos separados por espacios. La sintaxis de los archivos bajo */etc/pam.d/* es igual salvo que no existe el campo "service". En este caso "service" es el nombre del archivo en el directorio */etc/pam.d/* (el nombre del archivo debe estar en minúsculas) Usualmente *service* es el nombre del servicio o aplicación comúnmente usado, ejemplo de esto son login, su y ssh. **Para más información podemos consultar la página:** <http://es.wikipedia.org/wiki/Autenticaci%C3%B3n>

Para saber más

Como fuente de documentación acceder a:

[Administración de Linux 1](#) autor: Sergio González Durán

[Administración de Linux 2](#)

[Administración de Linux 3](#) autor: Elvira Misfud "Seguridad básica en Linux"

Administración de perfiles locales de usuario.

Caso práctico

Los sistemas operativos están preparados para que cada usuario pueda disponer de su propia configuración y forma de trabajo dentro del sistema al que accede de manera que marque diferencia con otros usuarios, por lo general hay características comunes y otras que pueden ser configuradas por el propio usuario y por el superusuario del sistema. Carlos aplicará todas las posibilidades que le ofrece el sistema para gestionar los perfiles de usuarios con el fin realizar la actividad de responsable del sistema como usuario administrador.



Los perfiles de usuario guardan un conjunto de informaciones que permiten al usuario disponer de un entorno de trabajo en aspecto y funciones del sistema cada vez que inicie sesión en un equipo como son el modo de escritorio, la configuración de red, etc. Cada vez que se crea un usuario dispone de un perfil predeterminado por el sistema, que puede modificar en cada sesión y del que serán archivados sus cambios al salir. Los perfiles pueden ser configurados y gestionados por el usuario administrador o cualquier usuario autorizado.

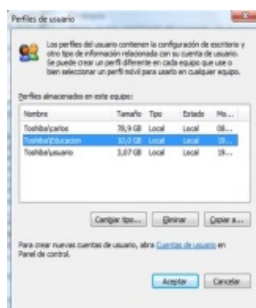
El disponer de perfiles hace que múltiples usuarios del sistema puedan utilizar el mismo equipo, con la configuración de cada uno recuperada al iniciar la sesión al mismo estado en que estaba cuando la cerró por última vez, además los cambios hechos por cada usuario no afectan a otros; Si el perfil está almacenado en un servidor los usuarios podrán conectarse al servidor desde cualquier estación de trabajo y recibirán como perfil el del servidor, este tipo de perfil móvil hace que siempre dispongas del mismo entorno de trabajo aunque la conexión se

realice desde cualquier terminal. Según esto **podemos distinguir los siguientes tipos de perfiles**:

- Perfil de usuario local: Perfiles creados en un equipo cuando un usuario inicia sesión. El perfil es específico de un usuario, local al equipo y se almacena en el disco duro del equipo local.
- Perfil de usuario móvil de red: los crea el usuario administrador del sistema y se almacenan en un servidor. Este perfil está disponible siempre que el usuario inicia una sesión en cualquier equipo de la red ya que recibe la configuración desde el servidor. Cada vez que se termina la sesión todas las modificaciones efectuadas en el perfil se archivan en el servidor, es decir, puede ser modificado por el usuario.
- Perfil de usuario obligatorio de red: son perfiles móviles que se utilizan para especificar configuraciones particulares de usuarios o grupos de usuarios. Sólo pueden ser modificados por un administrador, los cambios realizados por usuario no son guardados. Su principal ventaja que se asegura que todos los usuarios trabajan en un entorno común.
- Perfil de usuario temporal: es un tipo de perfil genérico que se inicia siempre que se produce un error en la entrada del perfil del usuario logueado. Siempre es el mismo y no se guardan los cambios efectuados al terminar la sesión.

Cada usuario dispone de un lugar del disco donde se guardan los datos de su perfil mediante carpetas, como pueden ser: carpeta de configuración local (ficheros de datos, historiales, etc), preferencias o cookies, entorno de red, escritorio, favoritos, templates o plantillas, sendto o accesos directos, etc. Algunas de estas informaciones se encuentran ocultas por seguridad.

Perfiles de usuarios locales en Windows.



Los perfiles de usuario en Windows 7 y Windows Server se localizan en `c:\Users (usuarios)\nombre_usuario`. El perfil genérico de Windows es *All Users*, de tal manera que si por ejemplo ponemos un acceso directo en el escritorio de ese usuario aparecerá en todos los escritorios de los usuarios.

Dependiendo del tipo de perfil podemos encontrar tres archivos que se encuentran ocultos por seguridad: *ntuser.dat* (registro del perfil móvil de usuario, los cambios se guardan al finalizar la sesión), *ntuser.dat.log* (se guardan temporalmente los cambios, hasta que termina la sesión que se grabarán en el disco) y *ntuser.man* (contiene perfil obligado de usuario, no se puede cambiar nada más que por el administrador). Cuando un usuario cierra su sesión, el sistema guarda la sección del registro específica de dicho usuario en la clave *HKEY_CURRENT_USER* y la actualiza.

Para obtener información sobre un perfil vamos *Inicio-Equipo*, botón derecho del ratón damos en *Propiedades*, de la Pestaña *Opciones avanzadas* pulsamos en el botón *Configuración del apartado Perfiles de usuario*, ahí verás todos los perfiles, su tamaño y el estado de los mismos.



Autoevaluación

¿Cuál es el directorio donde se encuentra el perfil genérico de todos los usuario de Windows 7?

- ☐ C:\users\nombre_usuario.
- ☐ C:/users/all users.
- ☐ C:\users\all users.
- ☐ Ninguna de las anteriores.

Operaciones con la configuración del perfil de usuarios locales en Windows.

Algunas operaciones con perfiles de usuarios:

- Podemos **copiar el perfil de un usuario** a otro, para ello seleccionamos el perfil del usuario que deseamos clonar y pulsamos en el botón *Copiar a...* y seguimos el asistente.
- **Para copiar los archivos desde un perfil existente** para que todos los usuarios tengan los mismos archivos de trabajo o para **reparar un perfil dañado**. Para poder completar estos pasos, debes tener al menos tres cuentas de usuario en el equipo, incluida la nueva cuenta recién creada y seguiremos los siguientes pasos:
 1. Debes de iniciar sesión en el ordenador como un usuario que no sea el nuevo usuario recién creado ni el usuario desde donde desea copiar los archivos. Pulsar en *Inicio-Documentos-Organizar*, hacer clic en *Opciones de carpeta y búsqueda*. Seleccionar la pestaña *Mostrar todos los archivos y carpetas ocultos*, seguidamente hacemos clic en la pestaña *Ver y Mostrar los archivos*, carpetas y unidades ocultos, seguidamente desactivamos *Ocultar archivos protegidos del sistema operativo* y damos en el botón *Aceptar*.
 2. Buscamos la carpeta `C:\Users\nombre_De_Usuario_antiguo`, donde `Ces` la unidad donde está instalado Windows y `ynombre_de_Usuario_antiguo` es el nombre del usuario desde el que desea copiar los archivos del perfil.

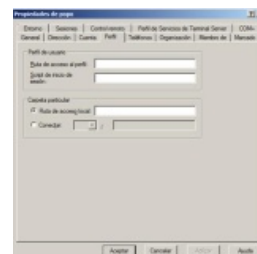
3. Seleccione todos los archivos y carpetas de esta carpeta, a excepción de los siguientes archivos: *Ntuser.dat*, *Ntuser.dat.log* y *Ntuser.ini*. Seguidamente haces clic en el menú *Edición* y en *Copiar*.
4. Buscamos la carpeta *C:\Users\nombre_de_usuario_nuevo*, donde *C* es la unidad donde está instalado Windows y *nombre_de_usuario_nuevos* el nombre del nuevo perfil de usuario creado. Hacemos clic en el menú *Edición* y en *Pegar*.
5. Cierra la sesión y, a continuación, vuelva a iniciar sesión como el nuevo usuario.

Las siguientes operaciones avanzadas podemos consultarlas en el enlace siguiente de Ayuda de soporte de Microsoft <http://support.microsoft.com/kb/973289>:

- Cómo personalizar un perfil de usuario local predeterminado en Windows 7
- Cómo convertir el perfil de usuario local predeterminado en un perfil de usuario de red predeterminado en Windows 7
- Cómo convertir el perfil de usuario local predeterminado en un perfil de usuario obligatorio en Windows 7.

Cuando desde un terminal te conectas a un servidor o dominio por primera vez en cada equipo local, se crea un usuario de dominio con un perfil local con respecto al servidor. Dentro de la carpeta Usuarios se crea una carpeta al usuario de tipo *nombre_usuario_dominio.nombre_NetBios_dominio*. Los usuarios disponen de una ficha o formulario que indica su perfil tanto en usuarios locales del servidor como configurar usuarios de *Active Directory* en la administración del servidor, podemos acceder desde *Inicio-Herramientas administrativas-Usuario y equipos del Active Directory*. Donde podemos especificar:

- **Ruta de acceso al perfil:** ruta de acceso en la red para activar el perfil móvil u obligado, *el\nombre_del_servidor\nombre_carpeta_compartida_de_perfiles\nombre_de_usuario*. Si no se especifica su perfil local será el que se creó en por defecto. Antes hay que crear las carpetas.
- **Script de inicio de sesión:** podemos especificar un fichero de secuencia de comando .bat que se ejecutará en el inicio de sesión, donde podemos indicar los lugares donde puede acceder, por ejemplo las unidades de red.
- **Ruta de acceso local:** indica el directorio particular donde almacena sus archivos, con el formato *c:\nombre_subdirectorio\nombre_del_usuario* (representado por la variable del sistema %USERNAME%). Antes hay que crear la carpeta.
- **Conectar:** permite conectarse a una letra de unidad de red compartida dentro del sistema de red, y tiene el formato *\\nombre_del_servidor\nombre_del_subdirectorio\nombre_usuario o %USERNAME%*



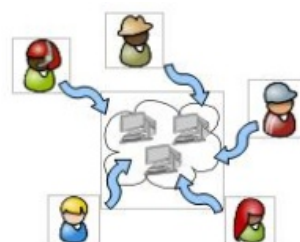
Para evitar que en cada terminal dispongas de un perfil de entrada al servidor diferente, se crea en la cuenta de usuario del servidor la característica de que el perfil sea móvil, para usarlo en cualquier equipo. En Windows Server 2008, una nueva directiva te permite establecer perfiles móviles para varios usuarios en un GPO.

Perfiles de usuario Linux.

Para cualquier usuario dado de alta en el sistema se creará una carpeta dentro del directorio */home* con el nombre del usuario que contendrá el perfil que se le aplicará cuando inicie sesión en Linux. El usuario será el único que tendrá todos los derechos de uso.

Por seguridad el usuario root tiene su propio perfil local de usuario ubicado en el directorio */root*. Se pueden crear scripts y ficheros de inicio que se ejecutarán al entrar en sesión un usuario de manera que podamos configurar el perfil de trabajo del usuario dentro del sistema.

Existe el fichero */etc/profile* que contiene el perfil igual para todos los usuarios, en su interior podemos poner comandos que se ejecutarán al iniciar sesión cualquier usuario, también ejecuta todos los script que se encuentran en el directorio */etc/profile.d*.



Cada vez que se inicia sesión de un usuario con el comando, se ejecutarán los siguientes ficheros ocultos (llevan el identificativo del punto) relacionados con el perfil de acceso al sistema de un usuario:

1	<i>/etc/profile</i>	Ejecutar el perfil genérico para todos los usuarios
2	<i>/home/nombre_usuario/.profile</i>	Ejecuta el .bashrc
3	<i>/home/nombre_usuario/.bashrc</i>	Contiene comandos que se ejecutan al inicio del Shell de forma interactiva
4	<i>/home/nombre_usuario/.bash_history</i>	Almacena el histórico de comandos que introduce el usuario en consola
5	<i>/home/nombre_usuario/.bash_logout</i>	Se ejecuta cuando el usuario sale de la sesión

Hay que destacar que cuando se inicia sesión desde un terminal para cambiar de usuario solamente se ejecuta el fichero *.bashrc*

Algunas operaciones con ficheros de perfil:

carlos@sistemaubuntu:~\$ ls -lta grep .profile	Busca los fichero .profile en la ubicación actual
carlos@sistemaubuntu:~\$ ls -a	Lista todos los ficheros ocultos
carlos@sistemaubuntu:~\$ more .profile	Visualizamos el contenido del fichero .profile
carlos@sistemaubuntu:~\$ gedit .profile	Editamos el fichero .profile
carlos@sistemaubuntu:~\$ su - nombre_usuario	Cambiamos de usuario y se ejecuta su .profile
carlos@sistemaubuntu:~\$ su nombre_usuario	Cambiamos de usuario pero no ejecuta el .profile

Debemos de tener en cuenta que cada vez que modifiquemos el fichero `.profile` y ejecutemos el comando `su - Nombre_usuario` se ejecutara lo que éste contenga ya que es un script de inicio de sesión del usuario. Un ejemplo para hacer que se muestre un mensaje de bienvenida cada vez que inicia sesión un usuario en el sistema puede ser el siguiente:

1	<code>carlos@sistemaubuntu:~\$ gedit .profile</code>	Editar el fichero <code>.profile</code>
2	<code>echo "Hola ya estas en el sistema"</code> <code>echo "estás en el directorio"</code> <code>pwd</code>	Añadir al final las líneas siguientes
3		Guardar el archivo y salir
4	<code>exit</code>	Salir de la sesión del usuario
5	<code>carlos@sistemaubuntu:~\$ su - carlos</code>	Entrar al sistema como usuario carlos



Autoevaluación

¿Qué realiza el siguiente comando `gedit /etc/profile`?

- ☐ Edita el fichero que configura el perfil del usuario conectado al sistema.
- ☐ Edita el fichero que configura el perfil común de todos los usuarios.
- ☐ Edita los ficheros ocultos dentro del directorio `/etc/profile`.
- ☐ Ninguna de las anteriores.