

# Administración de software base II.

## Caso práctico



[Alain Bachellier \(CC BY-NC-SA\)](#)

En la empresa **BK Sistemas Informáticos**, necesitarán utilizar los ordenadores todos los empleados ya que su actividad está relacionada con tareas de asesoría; **Juan** junto a **Laro** y **Vindio** ya habrán configurado los ordenadores que forman el sistema aplicando los conocimientos adquiridos en las unidades anteriores.

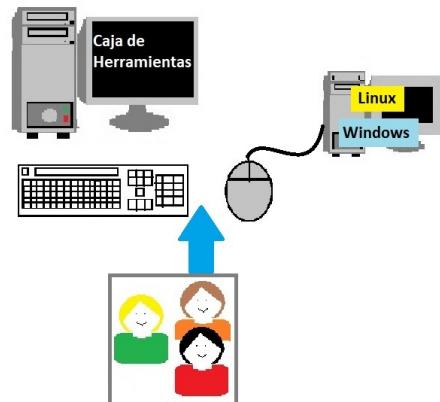
**Juan** administra las cuentas de los usuarios para los diferentes sistemas operativos instalados en los equipos, que en un principio trabajarán formando una estructura de red en grupo de trabajo, y que posteriormente pasarán a formar parte de un dominio. Todos los empleados tendrán la posibilidad de 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 **Juan** junto a **Laro** y **Vindio** realizarán 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.

En esta unidad continuaremos como en la unidad anterior administrando el software base. Aprenderemos a crear y configurar los usuarios y grupos tanto en Windows como en Linux. Lo haremos tanto de forma gráfica como con comandos.

Se recomienda estudiar los contenidos con el ordenador como elemento de consulta y realizar los ejemplos explicados en cada apartado, con el fin de facilitar la comprensión de los conceptos teórico/prácticos.



Antonio López (Elaboración propia)

# 1.- Administración de usuarios y grupos locales.

## Caso práctico

Juan le comenta a Vindio y Laro que tienen que elaborar un listado con la relación de compañeros de trabajo y su actividad dentro de la empresa.

¿Para qué es esa lista?, preguntan Vindio y Laro.

Tenemos que 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.

Entonces ¿tendremos que crear grupos y añadir los usuarios a esos grupos?, — pregunta Vindio.

Sí, tenemos que realizar las tareas administrativas relacionadas con las altas, bajas de usuarios y modificaciones de las características que necesitan los usuarios dentro del sistema, — responde Juan.

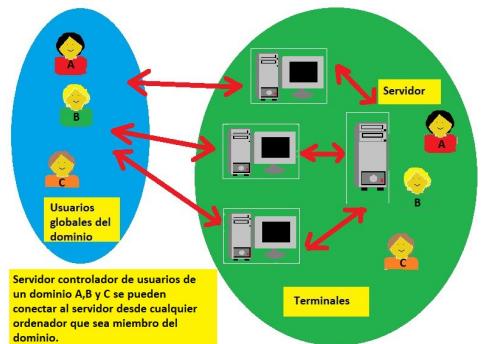


Jonny Goldstein (CC BY)



Antonio López (Elaboración propia)

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:**



Antonio López (Elaboración propia.)

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.

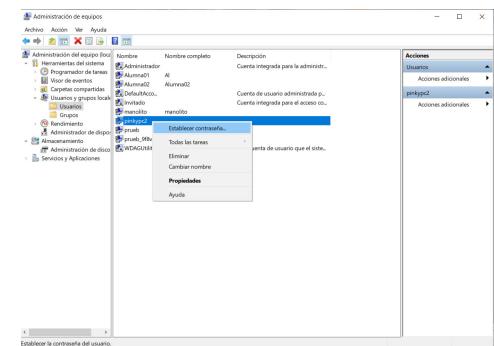
**Usuarios de un dominio:** un ordenador que cumpla la función de controlador de dominio es capaz de validar usuarios globales de dominio para que inicien sesión desde equipos clientes unidos al dominio o de forma local en el servidor para utilizar los recursos y servicios de software/hardware que comparte un ordenador servidor.

# 1.1.- Introducción a la administración de usuarios y grupos de usuarios locales en Windows 10.

Una cuenta de usuario en Windows 10 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.



Windows 10 (Elaboración propia)

## Autoevaluación

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

Sugerencia

- Verdadera
- Falsa

Incorrecto. Vuelve a leer el apartado.

Muy bien. Vas por buen camino.

## Solución

1. Incorrecto
2. Opción correcta

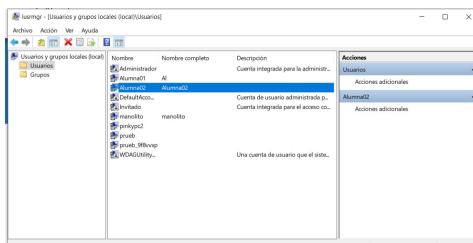
## 1.1.1.- Configuración de usuarios y grupos de usuarios locales en Windows 10.

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 Administración de equipos. Para acceder a ella, escribimos en el panel de búsqueda Administración de equipos. Dentro de ella, a la izquierda tenemos Usuarios y grupos locales.



Alex E. / sampler (CC0)

También podemos acceder directamente a la herramienta *Usuarios y grupos locales*, escribiendo en el panel de búsqueda lo siguiente: **lusrmgr.msc**.



Windows 10 (Elaboración propia)

Desde este recurso podemos realizar todas las tareas relacionadas con la administración de usuarios, como son:

**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 *Sí*. 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 las 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.

### Cuentas de usuario y grupos locales en PowerShell

Cmdlet	Finalidad
Get-LocalUser	Obtener información sobre las cuentas de usuario locales.

Get-LocalUser	Listas las cuentas de usuarios locales
Get-LocalGroup	Listar las cuentas de grupos locales
Get-LocalGroupMember	Listar los miembros de un grupo local
New-LocalUser	Crear una nueva cuenta de usuario local
New-LocalGroup	Crear una nueva cuenta de grupo local
Add-LocalGroupMember	Hacer miembro de un grupo local a un usuario
Remove-LocalUser -Name "nombre usuario"	Eliminar un usuario local
<em>Remove-LocalGroup "nombre de grupo"</em>	Eliminar un grupo local

## Trabajar con cuentas de usuario con PowerShell

### Crear un usuario local

Abrimos PowerShell, para ello, escribimos en el panel de búsqueda **PowerShell** y escribimos lo siguiente:

```
Get-LocalUser "nombre de usuario"
```

### Eliminar un usuario

Escribimos Lo siguiente:

```
Remove-LocalUser -Name "nombre de usuario"
```

### Listar los usuarios locales

Escribimos Lo siguiente:

```
Get-LocalUser
```

## Debes conocer

Crear un usuario desde la administración avanzada de cuentas de Windows

[Crear cuentas desde la administración avanzada de Windows](#)

## Autoevaluación

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

Sugerencia

- Verdadera
- Falsa

Incorrecto. Vuelve a leer el apartado.

Muy bien. Veo que vas avanzando.

## Solución

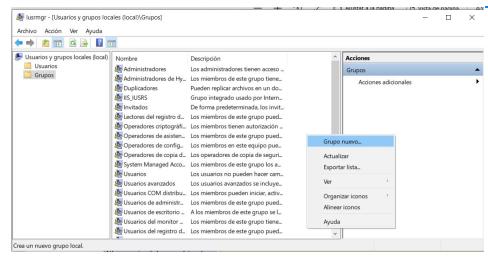
1. Incorrecto
2. Opción correcta

## 1.1.2.- Operaciones con grupos de usuarios en Windows 10.

Los grupos locales de usuarios se administran en Usuarios y grupos locales se encuentran definidos en la consola MMC Administración de equipos. Para acceder a ella, escribimos en el panel de búsqueda Administración de equipos. Dentro de ella, a la izquierda tenemos Usuarios y grupos locales.

También podemos acceder directamente a la herramienta Usuarios y grupos locales, escribiendo en el panel de búsqueda lo siguiente: <i>lusrmgr.msc</i>.

Las tareas que podemos realizar desde este lugar son:



Windows 10 (Elaboración propia)

**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.

### Trabajar con grupos desde la línea de comandos

#### Eliminar un grupo

Abre la ventana del símbolo del sistema, en el campo de *Buscar* escribir <i>cmd</i>. Luego ejecutar:

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

#### Identificar los miembros de un grupo

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 <i>cmd</i>. Luego ejecutar:

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

#### Añadir un 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 <i>cmd</i>. Luego ejecutar:

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

## Trabajar con grupos usando PowerShell

### Crear un grupo local

Abrimos PowerShell, para ello, escribimos en el panel de búsqueda **PowerShell** y escribimos lo siguiente:

```
New-LocalGroup "nombre de grupo"
```

### Listar los miembros de un grupo local

Escribimos el siguiente comando:

```
Get-LocalGroup "Nombre del grupo"
```

### Añadir usuarios como miembros de grupo local

Escribimos el siguiente comando:

```
Add-LocalGroupMember -Member "nombre de usuario" -Group "nombre del grupo"
```

### Eliminar un grupo local

Escribimos el siguiente comando:

```
Remove-LocalGroup "nombre de grupo"
```

## Debes conocer

Cómo trabajar con usuarios y grupos en PowerShell

[Usuarios y grupos en PowerShell](#)

Comando net user (crear usuarios desde el CMD)

[Comando NET USER](#)

Comando net localgroup (crear grupos desde el CMD)

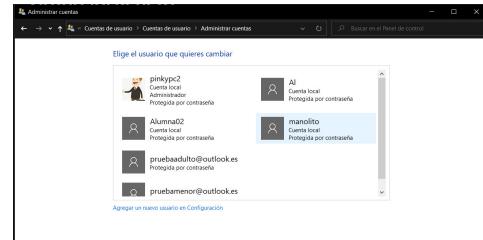
[Comando NET LOCALGROUP](#)

## 1.1.3.- Gestión de usuarios y grupos de usuarios desde el Panel de control de Windows 10.

Windows 10 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 al panel de búsqueda y escribimos *Panel de control*, pinchamos sobre panel de control -> *Cuentas de usuario* -> *Cuentas de usuario*. Para realizar esta tarea debemos de ser usuario del grupo de administradores. Desde este lugar podemos:



Windows 10 (Elaboración propia)

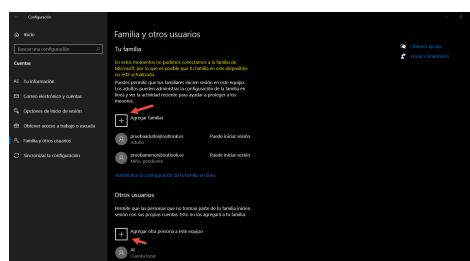


Windows 10 (Elaboración propia)

**Crear cuenta de usuario:** en el panel de búsqueda escribimos *Panel de control*, pinchamos sobre panel de control -> *Cuentas de usuario* -> *Cuentas de usuario* -> *Administrar cuentas* -> *Agregar un nuevo usuario en Configuración*. Esto nos lleva a la misma ventana que si entramos haciendo clic en el *botón de Inicio* -> *Configuración* -> *Cuentas* -> *Familia y otros usuarios*. Aquí podemos agregar varios tipos de usuario:

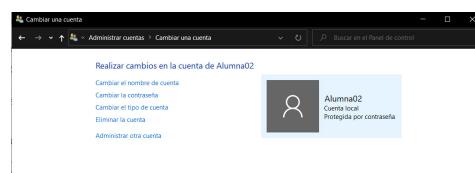
**Agregar familiar:** podemos agregar otros usuarios que son familiares nuestros. Aquí podemos crear cuentas de adultos y de niños. Los padres pueden usar el control parental sobre los niños. En los siguientes enlaces se explica como agregar cuentas de tipo familiar. [Agregar un miembro a tu grupo familiar por Microsoft](#). Aquí tenemos otro enlace sobre [Cómo añadir a los miembros de tu familia a tu PC con Windows 10](#).

**Agregar otra persona a este equipo:** en esta opción nos permite crear un usuario que no es un familiar. Para ella se abre un asistente donde podemos crear el usuario iniciando sesión con una cuenta de Microsoft (para ello necesitamos un correo electrónico o teléfono) o tenemos la opción de no iniciar sesión con una cuenta de Microsoft pulsando en el enlace *No tengo datos de inicio de sesión de esta persona*. En la siguiente ventana otra vez insiste en que escribamos el correo de Microsoft, si no queremos hay que pulsar en el enlace *Agregar un usuario sin cuenta de Microsoft*. Si pulsamos en esta última opción, nos pedirá el nombre de usuario y su contraseña por dos veces. Seguimos el asistente. En el siguiente enlace podemos ver como se [crea una cuenta de usuario local, no enlazada a una cuenta de Microsoft](#).



Windows 10 (Elaboración propia)

**Modificar o eliminar una cuenta de usuario:** desde el panel de búsqueda escribimos *Panel de control*, pinchamos sobre *panel de control* -> *Cuentas de usuario* -> *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:

Desde el panel de búsqueda escribimos *Panel de control*, pinchamos sobre *panel de control* -> *Cuentas de usuario* -> *Administrador de credenciales*.

En el panel de la derecha nos aparecen dos opciones: *credenciales web* y *credenciales Windows*.

Seleccionamos una de las dos opciones anteriores para obtener acceso a las credenciales que quieras administrar.

Seleccionamos *Credenciales de Windows*, hacemos 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.

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” que dispone Windows 10 permite gestionar grupos de usuarios.**

Sugerencia

- Verdadera
- Falsa

Incorrecto. Vuelve a leer el apartado.

Muy bien. Veo que vas avanzando.

## Solución

1. Incorrecto
2. Opción correcta

## Para saber más

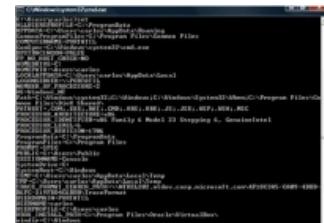
Que son y cómo administrar las credenciales de Windows

[Administrar credenciales de Windows](#)

## 1.1.4.- Variables de entorno relacionadas con usuarios y grupos en Windows 10.

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%
```



Windows 10 (Elaboración propia)

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

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

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

<b>set Nombre_variable</b>	Para que se muestre una variable
<b>set Nombre_variable=valor</b>	Para crear y asignar valor a una variable
<b>set Nombre_variable=</b>	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.- En el panel de búsqueda escribimos *Panel de control*, pinchamos sobre *panel de control* -> *Cuentas de usuario* -> *Cuentas de usuarios* -> *Cambiar las variables de entorno*. En el 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.

### Variables de entorno en PowerShell

Cmdlet	Función

Get-ChildItem Env:	Mostrar las variables de entorno
\$env:nombre_variable="Valor de la variable"	Crear una variable de entorno
Get-ChildItem Env:\nombre_variable	Mostrar el contenido de una variable de entorno creada por el usuario
\$env:COMPUTERNAME	Mostrar el contenido de una variable de entorno
\$nombre_variable=\$env:COMPUTERNAME	Guardar el contenido de una variable en otro variable

## Debes conocer

Como personalizar y añadir variables de entorno

[Añadir o personalizar variables de entorno](#)

Lista de variables de entorno en Windows

[Lista de variables de entorno en Windows](#)

## Para saber más

Configuración de variables de entorno con PowerShell

[Variables de entorno con PowerShell](#)

Como documentación podemos acceder a los enlaces:

[Administración de usuarios Windows 10 enlace 1](#)

[Administración de usuarios Windows 10 enlace 2](#)

## 1.2.- Introducción a la administración de usuarios y grupos locales en Windows Server 2019.

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:

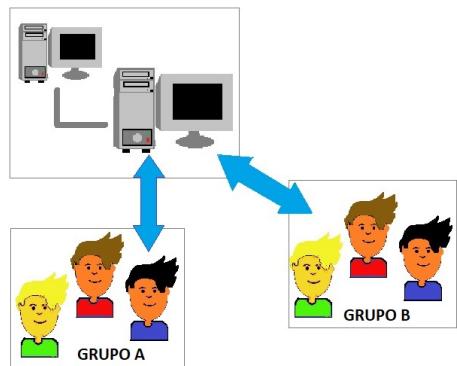
**Iniciar sesión en un dominio** (se verá en la Unidad 6) para acceder a los recursos de toda la red.

**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, permitiéndoles 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.



Antonio López (Elaboración propia)

## 1.2.1.- Configuración de usuarios y grupos locales en Windows Server 2019.

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**):

Hacemos clic en la lupa y escribimos **lusrmgr.msc** que es la aplicación de **Usuarios y grupos locales**. Pinchamos sobre ella, ya tenemos abierta esta aplicación.

Para **crear cuentas de usuario local** seguir los siguientes pasos:

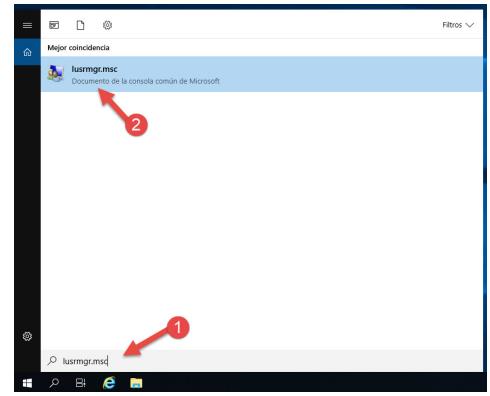
Abrimos la aplicación *Usuarios y grupos locales*. En el panel de la izquierda pulsamos en *Usuarios*, en el panel central nos aparecen los usuarios creados.

Si no hemos creado ningún usuario, nos aparecen los usuarios predeterminados el *Administrador*, *Invitado*, *DefaultAccount* y *WDAGUtilityAccount* (si tiene una flecha hacia abajo indica que por seguridad está deshabilitado).

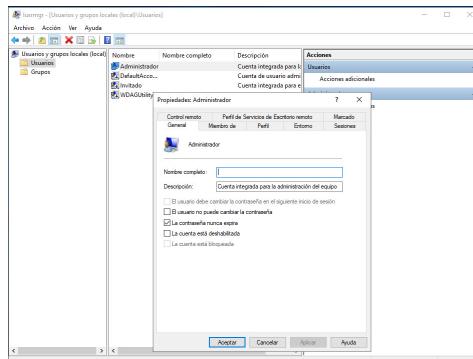
Pulsamos el botón derecho del ratón desde zona blanca del panel central, del menú seleccionar *Usuario nuevo*. Del formulario completar los campos y dar al botón *Crear*.

Para **dar de baja de usuario local** del servidor seguir los pasos siguientes:

Abrimos la aplicación *Usuarios y grupos locales*. En el panel de la izquierda pulsamos en *Usuarios*. Con el botón derecho seleccionamos el usuario a dar de baja. Seleccionamos la opción *Eliminar*. De la ventana de confirmación pulsar *Sí*. No se puede recuperar una cuenta de usuario eliminada. No es posible eliminar las cuentas *Administrador* e *Invitado*.



Windows Server 2019 (Elaboración propia)



Windows Server 2019 (Elaboración propia)

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

Abrimos la aplicación *Usuarios y grupos locales*. En el panel de la izquierda pulsamos en *Usuarios*. Con el botón derecho seleccionamos el usuario a modificar y seleccionamos la opción *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 escritorio remoto (permite que los usuarios pueden conectarse de forma remota usando el servicio de escritorio remoto 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 servicios de escritorio remoto. Permite indicar, por seguridad, en qué tiempo se fuerza a desconectar una sesión sin actividad o activa.

**Control remoto:** configura el control remoto de los Servicios de escritorio remoto.

*Perfil de Servicios servicios de escritorio remoto:* permite configurar la ruta de acceso al perfil de usuario de los servicios de escritorio remoto o para denegar el inicio de sesión a los servicios de escritorio remoto.

*Marcado:* para permitir o denegar el acceso a redes, las opciones de devolución de llamadas y para asignar direcciones IP estáticas.

## Debes conocer

Configuración de usuarios y grupos locales en Windows Server

[Configuración de usuarios y grupos locales en Windows Server](#)

## 1.2.2.- Operaciones con grupos de usuarios locales en Windows Server 2019.

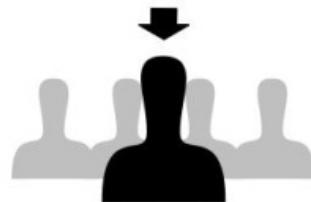
Si deseamos **gestionar grupos locales** debemos realizar con usuarios locales (**para consultar la descripción de los campos de los diferentes formularios acceder a la propia ayuda en la ventana mostrada por Windows**):

Hacemos clic en la lupa y escribimos **Iusrmgr.msc** que es la aplicación de Usuarios y grupos locales. Pinchamos sobre ella, ya tenemos abierta esta aplicación.

Si deseamos gestionar el **alta de un grupo local** debemos realizar los siguientes pasos :

1.- Abrimos la aplicación *Usuarios y grupos locales*. En el panel de la izquierda pulsamos en *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*.



Frédéric Moser (Dominio público)

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 <i>cmd</i>. 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.- Abrimos la aplicación *Usuarios y grupos locales*. En el panel de la izquierda pulsamos en *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 *Sí*. No se puede recuperar un grupo eliminado. 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.- Abrimos la aplicación *Usuarios y grupos locales*. En el panel de la izquierda pulsamos en *Grupos*.

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_grupos"
```

## Debes conocer

Cómo trabajar con usuarios y grupos en PowerShell

[Usuarios y grupos en PowerShell](#)

Comando net user (crear usuarios desde el CMD)

[Comando NET USER](#)

Comando net localgroup (crear grupos desde el CMD)

[Comando NET LOCALGROUP](#)

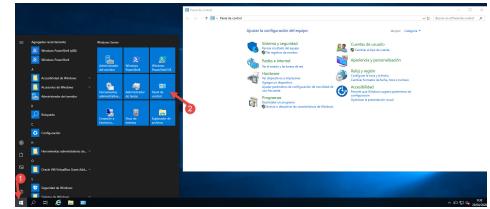
## 1.2.3.- Gestión de usuarios y grupos desde el Panel de control en Windows Server 2019.

Windows Server 2019 está diseñado para poder acceder a las herramientas y recursos por diferentes caminos o accesos, de una forma muy parecida a Windows 10 desde *Inicio-Configuración-Cuentas-Otros usuarios*, **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.

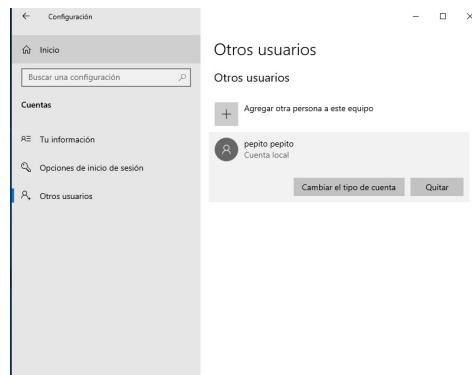
Desde este lugar podemos:

**Crear cuenta de usuario:** desde *Inicio-Configuración-Cuentas-Otros usuarios-Agregar otra persona a este equipo*. Nos aparece la ventana donde podemos gestionar los usuarios y grupos locales. Esto lo tenéis explicado en el apartado 1.2.1 *Configuración de usuarios y grupos locales en Windows Server 2019*.

**Cambiar el tipo de cuenta o eliminar una cuenta de usuario:** *Inicio-Configuración-Cuentas-Otros usuarios*. Aquí pinchamos sobre el usuario y nos aparece dos opciones: cambiar el tipo de cuenta, donde podemos elegir: usuario estándar o usuario administrador. También podemos eliminar la cuenta pulsando en el botón *Quitar*.



Windows (Elaboración propia)



Windows Server (Elaboración propia)

### Para saber más

Puedes consultar dudas y utilizar como bibliografía el propio manual de ayuda interactiva, aportado por la licencia instalada de Windows Server 2019 de Microsoft.

Documentación de Windows Server

[Documentación de Windows Server](#)

Tutorial de Windows Server

[Tutorial de Windows Server](#)

### Autoevaluación

**Un usuario de tipo o grupo estándar puede:**

Sugerencia

- 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.

Incorrecto. Repasa la unidad

Correcto. Veo que vas por buen camino.

Incorrecto. Vuelve a leer los contenidos de la unidad

No es correcta. Repasa los contenidos de la unidad.

## Solución

1. Incorrecto
2. Opción correcta
3. Incorrecto
4. Incorrecto

## 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.

Incorrecto. Medita mejor tu respuesta

Incorrecto. Repasa la unidad

Correcto

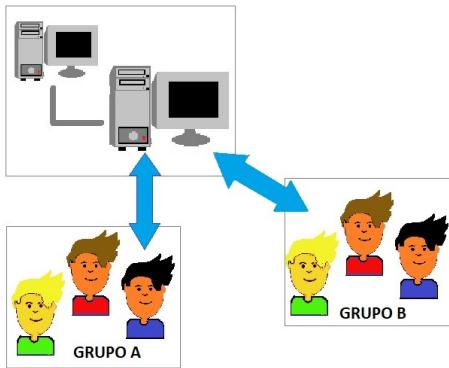
Incorrecto. Vuelve a leer los contenidos de la unidad

## Solución

1. Incorrecto

2. Incorrecto  
3. Opción correcta  
4. Incorrecto

## 1.3.- Introducción a la administración de usuarios y grupos en Linux.



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.**

Antonio López (Elaboración propia)

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

## 1.3.1.- 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** podriamos iniciar sesión como root. Esto por defecto, esta desactivado, porque no es recomendable iniciar sesión por motivos de seguridad. Para realizar la configuración desde Linux Ubuntu seguir los siguientes pasos:

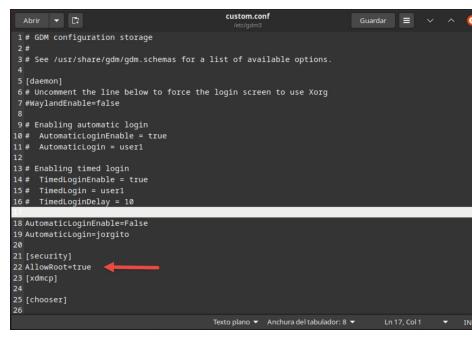
Abrimos un terminal. Escribimos el siguiente comando:

```
sudo gedit /etc/gdm3/custom.conf
```

En este fichero buscamos la categoría *[Security]* que no tiene ningún contenido. Debajo de ella escribimos el siguiente texto:

```
AllowRoot=true
```

El fichero queda como se ve en la siguiente imagen:



```
custom.conf
/etc/gdm3

1 # GDM configuration storage
2 # See /usr/share/gdm/gdm.schemas for a list of available options.
3 [daemon]
4 # Uncomment the line below to force the login screen to use Xorg
5 #keylandEnable=false
6
7 # Enabling automatic login
8 #AutomaticLoginEnable=true
9 # AutomaticLogin= user1
10
11 # Enabling timed login
12 #TimedLoginEnable=true
13 # TimedLogin= 10
14 # TimedLoginDelay = 10
15
16 # AutomaticLoginEnable=false
17 #AutomaticLogin=jorgeito
18
19 [security]
20
21 [security]
22 AllowRoot=true ←
23 [xdmcp]
24
25 [chooser]
26
```

Ubuntu (Elaboración propia)

Guardamos los cambios.

Editamos el fichero gdm-password. Para ello escribimos el siguiente comando en el terminal:

```
sudo gedit /etc/pam.d/gdm-password
```

En el fichero buscamos la línea siguiente:

```
auth required pam_succeed_if.so user != root quiet_success
```

Esta línea estará al principio del fichero. Al principio de la línea escribimos una (#), de manera que la línea que así:

```
# auth required pam_succeed_if.so user != root quiet_success
```

Guardamos los cambios.

Abrimos el fichero .profile. Para ello escribimos en el terminal:

```
sudo gedit /root/.profile
```

Buscamos la línea:

```
msg n || true
```

Sustituimos la línea anterior por:

```
if `tty -s`; then  
mesg n  
fi
```

Guardamos los cambios. Cerramos la sesión y hacemos clic sobre el enlace *¿No está en la lista?*. Nos aparece una pantalla donde tenemos que escribir el nombre del usuario. En este caso *root* y su contraseña. Pulsamos la tecla Intro. Como hemos iniciado sesión por primera vez con el usuario *root*, nos aparece un asistente donde nos ofrece información sobre diferentes aspectos del sistema. Avanzamos en el asistente pulsando en el botón *Siguiente*. Al final pulsamos la tecla *Hecho* y se cerrar la ventana. A partir de este momento estamos trabajando como usuario *root* y nos volverá a pedir la contraseña de administrador para hacer ninguna tarea de administración.

Como se ha comentado al principio esto no es recomendable por motivos de seguridad, por lo que solo se recomienda hacerlo si resulta imprescindible.

En Linux se pueden gestionar usuarios globales del dominio, de manera que con ellos se puede iniciar sesión desde cualquier equipo cliente que esté unido al dominio, de la misma forma que en un controlador de dominio Windows Server 2019. 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.

Incorrecto. Repasa la unidad

Incorrecto. Vuelve a leer la unidad

Efectivamente, vamos por buen camino.

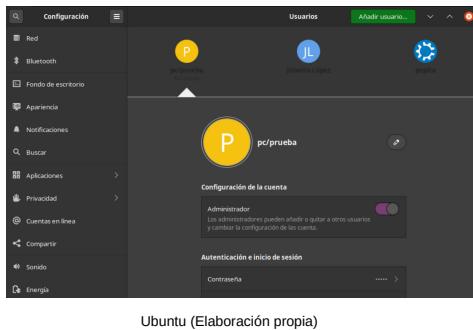
Incorrecto. Vuelve a repasar los contenidos vistos hasta ahora

## Solución

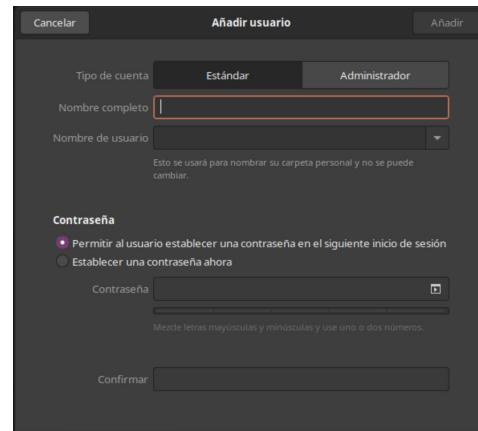
1. Incorrecto
2. Incorrecto
3. Opción correcta
4. Incorrecto

## 1.3.2.- Operaciones con usuarios en Linux.

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



Ubuntu (Elaboración propia)



Ubuntu (Elaboración propia)

### Alta de usuarios:

Pinchamos en *Mostrar aplicaciones*, escribimos *usuarios* y hacemos clic en *Añadir o quitar usuarios y cambiar su contraseña*. Veremos la lista de usuarios dados de alta en el sistema.

Pulsamos en el botón *Desbloquear*.

Una vez desbloqueado, aparece el botón *Añadir usuario*. Pulsamos en él y nos muestra un formulario donde se recogerán los datos del usuario que vamos a crear:

*Tipo de cuenta*: elegimos si la cuenta es estándar o de tipo administrador.

#### Contraseña:

*Permite al usuario establecer una contraseña en el siguiente inicio de sesión*. Cuando el usuario inicie sesión tendrá que introducir su contraseña.

*Establecer una contraseña ahora*: tenemos que introducir una contraseña por dos veces que cumpla los criterios de complejidad (uso de mayúsculas, minúsculas, números, caracteres especiales, etc). Pulsamos el botón *Añadir*.

### Modificación de los datos de usuario:

Pinchamos en *Mostrar aplicaciones*, escribimos *usuarios* y hacemos clic en *Añadir o quitar usuarios y cambiar su contraseña*. Veremos la lista de usuarios dados de alta en el sistema.

Pulsamos en el botón *Desbloquear*.

Una vez desbloqueado, aparece la lista de los usuarios creados en el sistema. Pulsamos sobre uno de ellos.

Nos aparecen las siguientes opciones:

*Cambiar el nombre del usuario*: para ello hacemos clic en el lápiz que aparece al lado del nombre del usuario.

*Cambiar la imagen del usuario*: para ello hacemos clic encima del círculo al lado del nombre del usuario.

*Configuración de la cuenta*: nos permite dar a nuestra cuenta el rol de administrador. También podemos elegir el idioma.

*Autenticación e inicio de sesión*: tiene las siguientes opciones:

*Contraseña*: al pinchar en esta opción permite al usuario establecer una contraseña en el siguiente inicio de sesión o establecer una contraseña ahora. Una vez elegida una opción pulsamos en el botón *Cambiar*.

*Iniciar sesión automáticamente*: si pinchamos en este botón el usuario inicia sesión sin introducir una contraseña.

*Actividad de la cuenta*: nos muestra un pantalla con la actividad de esta semana de la cuenta seleccionada.

*Quitar usuario*: nos permite eliminar el usuario.

### Baja de un usuario en el sistema:

Pinchamos en *Mostrar aplicaciones*, escribimos *usuarios* y hacemos clic en *Añadir o quitar usuarios y cambiar su contraseña*. Veremos la lista de usuarios dados de alta en el sistema.

Pulsamos en el botón *Desbloquear*.

Una vez desbloqueado, aparece la lista de los usuarios creados en el sistema. Pulsamos sobre uno de ellos.

Al final de todas las opciones, nos aparece el botón *Quitar usuario*.

Al pinchar sobre él, se abre una ventana que nos pregunta si eliminamos los archivos, mantenemos los archivos o cancelamos. Si pinchamos en eliminar archivos, se elimina el directorio Home del usuario y todos sus ficheros de configuración, si elegimos mantener archivos solo no se elimina su directorio Home.

# Autoevaluación

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

- Verdadera
- Falsa

Vuelve a leer la Unidad

Muy bien

## Solución

1. Incorrecto
2. Opción correcta

## Debes conocer

Administrar cuentas de usuario en Ubuntu

[Administrar cuentas de usuario en Ubuntu](#)

### 1.3.3.- Operaciones con grupos de usuarios en Linux.

Desde hace varias versiones, la distribuciones de Ubuntu no incluyen la gestión de grupos desde la herramienta gráfica de creación de usuarios. Esto es porque los creadores de Ubuntu pensaron que era necesario y que se podía hacer desde el terminal. Para solucionar esto tenemos que instalar el paquete gnome-system-tools.

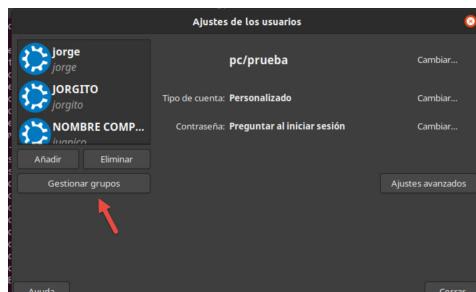
Para instalar este paquete abrimos un terminal y escribimos el siguiente comando:

```
prueba@prueba:/home/prueba$ sudo apt install gnome-system-tools
```

Nos pedirá la contraseña del administrador y que confirmemos la instalación. Pulsamos Y. Hecho esto la herramienta ya tenemos agregada la gestión de grupos en la herramienta gráfica. Para abrir la herramienta gráfica, hacemos clic en *Mostrar aplicaciones*, escribimos usuarios y ya nos aparece Usuarios y grupos..., pinchamos sobre su ícono.



Ubuntu (Elaboración propia)

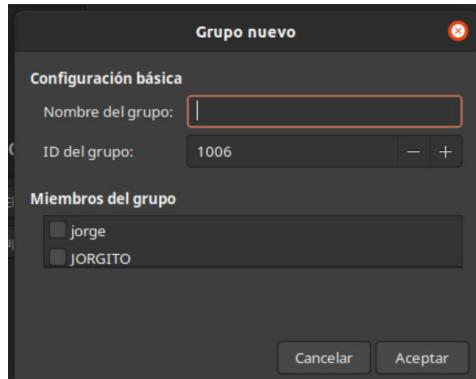


Ubuntu (Elaboración propia)

**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 <i>root, users, admin, ssh</i>, etc.



Ubuntu (Elaboración propia)



Ubuntu (Elaboración propia)

#### Crear un grupo de usuarios:

- 1.- Abrir la herramienta de 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:
  - 2.1.- *Nombre del grupo*: escribimos el nombre que tendrá el grupo en el sistema. No puede disponer de caracteres especiales, no espacios en blanco.
  - 2.2.- *Id del grupo*: es el número interno de identificación del grupo.
  - 2.3.- (*GID*) para los procesos del sistema que será un número igual o superior al que asigna el sistema por defecto
  - 2.4.- *Miembros del grupo*: marcamos las casillas de verificación de la lista para seleccionar los usuarios que vayan a pertenecer al grupo.
- 3.- Una vez rellenados los datos, pulsamos en *Aceptar*.

#### Modificación de grupos:

- Abrir la herramienta de usuarios y grupos. Pulsar el botón *Gestionar grupos*. Aparecerá una ventana con la lista de grupos creados en el sistema.
- 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:

- Abrir la herramienta de usuarios y grupos. Pulsar el botón *Gestionar grupos*. Aparecerá una ventana con la lista de grupos creados en el sistema.
- 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.

## Autoevaluación

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

- Un grupo con el mismo nombre que el usuario.
- root.
- estándar.
- invitado

Muy bien. Seguimos avanzando.

Incorrecto. Repasa la unidad

Incorrecto. Vuelve a leer los contenidos de la unidad

Incorrecto. Medita tu respuesta

## Solución

1. Opción correcta
2. Incorrecto
3. Incorrecto
4. Incorrecto

## 1.3.4.- Operaciones en modo comando con usuarios en Linux.

Hacemos clic en *Mostrar aplicaciones*, escribimos *Terminal*, pinchamos en terminal. También podemos abrir un terminal tecleando **CRI+ALT+Supr** desde el escritorio. Se abre una consola, donde podemos escribir comandos o ejecutar scripts. Hay comando que no tendremos permisos para poder ejecutarlos, porque se necesitan permisos de usuario root. Para poder ejecutar estos comandos tenemos que escribir el comando sudo su, nos pedirá la contraseña de root (es la misma que la del usuario que creamos durante la instalación del sistema) y aparece el prompt de entrada para el administrador identificado con el símbolo #:

```
prueba@prueba:~$ sudo su  
Contraseña:  
root@prueba:/home/prueba#
```

También, podemos ejecutar los comandos con el formato de la orden <i>sudo</i>, de la siguiente manera:

```
prueba@prueba:~$ sudo nombre_de_comando  
[sudo] password for prueba:
```

Mediante el comando <i>man</i> podemos obtener la ayuda interactiva de un comando de Linux mediante el formato siguiente:

```
root@prueba:/home/prueba# man nombre_comando
```

Con <i>useradd</i> o <i>adduser</i> **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 <i>/home/nombre\_de\_usuario</i> 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@prueba:/home/prueba# useradd nombre_de_usuario
```

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

```
root@prueba:/home/prueba# passwd nombre_de_usuario  
  
Introduzca la nueva contraseña de UNIX:  
Vuelva a escribir la nueva contraseña de UNIX:  
passwd: contraseña actualizada correctamente  
  
root@prueba:/home/prueba#
```

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 <i>passwd</i> sin ningún parámetro. El comando <i>passwd</i> tiene varias opciones que establecen los valores de la cuenta en /etc/shadow. **Con <i>usermod</i> podemos modificar o actualizar un usuario o cuenta ya existente**. Si quisieramos cambiar el nombre de usuario escribimos:

```
root@prueba:/home/prueba# usermod -l nombre_actual_de_usuario nuevo_nombre_de_usuario
```

**Con <i>userdel</i> elimina una cuenta del sistema.** Puede ser invocado de tres maneras:



Ubuntu (Elaboración propia)

Comando	Función
userdel nombre_de_usuario	Sin opciones elimina la cuenta del usuario de /etc/passwd y de /etc/shadow, pero no elimina su directorio de trabajo ni archivos contenidos en el mismo
userdel -r nombre_de_usuario	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.
userdel -f nombre_de_usuario	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

Crear usuarios en Linux

[Crear usuarios](#)

Administrar usuarios en Linux

[Administrar usuarios](#)

## 1.3.5.- 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:

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

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

*.bash\_profile:<code>* aquí podremos indicar alias, variables, configuración del entorno, etc. que deseamos indicar al principio de la sesión.

*.bash\_logout:<code>* aquí podremos indicar acciones, programas, scripts , etc., que deseemos ejecutar al salir de la sesión.

*.bashrc:<code>* es igual que *.bash\_profile<code>*, se ejecuta al principio de la sesión, en este archivo se indican los programas o scripts a ejecutar, a diferencia de *.bash\_profile<code>* 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** (en Ubuntu 20.04 se llama *aplicaciones al inicio*), para acceder a el pulsamos en mostrar aplicaciones y escribimos aplicaciones al inicio. Con este programa es posible establecer qué aplicaciones o scripts queremos que arranquen en el entorno gráfico (es similar al fichero *bashrc*).

Antonio López (Elaboración propia)

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<code>* o *.kde<code>* 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 *chpassw<code>* y *newuser<code>* 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](#) que ofrece una interfaz web. Entre muchas otras cosas te permiten un control total de la administración de usuarios y grupos local y remotamente.

### Debes conocer

Administración de usuarios y grupos en GNU/Linux

[Administración de usuarios y grupos en Linux](#)

### Para saber más

Como fuente de documentación consultar:

[Administración de Linux](#)

Documentación oficial de Ubuntu

[Documentación oficial de Ubuntu](#)

## 2.- Usuarios y grupos predeterminados.

### Caso práctico



Alain Bachellier (CC BY-NC-SA)

Chicos, sabéis que cuando se realiza el proceso de instalación de un sistema operativo, por defecto, el propio sistema crea una serie de usuarios y grupos predeterminados, —comenta **Juan**.

Como administrador de sistema siempre se debe comprobar las directivas de seguridad más adecuadas para los usuarios y grupos.

Nos pondremos en seguida a investigar todo esto, —responden **Laro** y **Vindio**.

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.

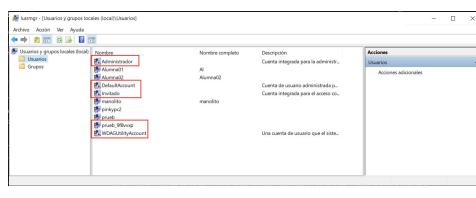


[LAN-Party pictogram](#). Autor: Katzenbaer (Dominio público)

## 2.1.- Usuarios y grupos locales predeterminados en Windows 10.

**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 10, existen de entrada las siguientes cuentas de usuario predeterminadas:**

Cuenta	Descripción
Administrador	<p>La cuenta de Administrador tiene las siguientes características:</p> <p>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.</p> <p>Nunca se puede eliminar ni quitar del grupo Administradores, pero es posible cambiarle el nombre o deshabilitarla.</p> <p>Aunque la cuenta Administrador esté deshabilitada de forma predeterminada, siempre puede usarse para obtener acceso a un equipo con el modo seguro.</p> <p>Se recomienda configurarla de modo que use una contraseña segura.</p>
DefaultAccount	<p>Se trata de una cuenta neutra para el usuario que se puede usar para ejecutar procesos que sean compatibles con varios usuarios o que sean independientes del usuario.</p>
Invitado	<p>La cuenta Invitado tiene las siguientes características:</p> <p>No requiere ninguna contraseña y la pueden utilizar usuarios que no disponen de cuenta en el equipo.</p> <p>La cuenta Invitado está deshabilitada de forma predeterminada, pero puede habilitarla.</p> <p>Es miembro del grupo predeterminado Invitados.</p> <p>Dispone de privilegios mínimos en el sistema.</p>
WDAGUtilityAccount	<p>Es una cuenta de usuario que es administrada y utilizada por el sistema para escenarios de Windows Defender Application Guard.</p> <p><b>WDAGUtilityAccount&lt;code&gt;</b> es parte de la Protección de aplicaciones de Windows Defender.</p> <p>Permanece deshabilitado hasta que Application Guard esté habilitado en su sistema.</p>



Windows 10 (Elaboración propia)

Los Usuarios y grupos locales se encuentran definidos en la consola MMC Administración de equipos. Para acceder a ella, escribimos en el panel de búsqueda Administración de equipos. Dentro de ella, a la izquierda tenemos Usuarios y

grupos locales. También podemos acceder directamente a la herramienta Usuarios y grupos locales, escribiendo en el panel de búsqueda lo siguiente: lusrmgr.msc<code>. 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.

**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 del grupo 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 *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.** Para acceder a la página que nos permite acceder al modo seguro de Windows 10 pincha [aquí](#). Donde podemos acceder a una serie de opciones para solucionar problemas en caso de fallo en nuestro sistema.



Windows10 (Elaboración propia)

## Para saber más

Cuentas locales en Windows

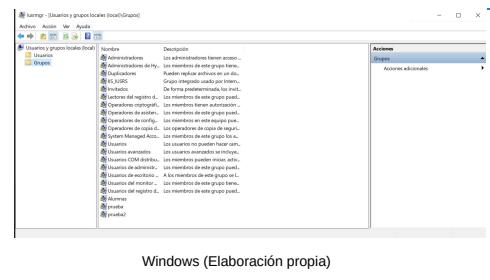
[Cuentas locales en Windows](#)

## 2.1.1- Clasificación de Grupos de usuarios locales predeterminados en Windows 10.

Para gestionar grupos de usuarios locales predeterminados tenemos escribir en el panel de búsqueda Administración de equipos y pulsamos sobre el resultado Administración de equipos. También podemos acceder directamente a la herramienta Usuarios y grupos locales, escribiendo en el panel de búsqueda lo siguiente: lusrmgr.msc. Dentro de *Usuarios y grupos locales* hacemos clic 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:

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

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.

*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*.

*Usuarios del registro de rendimiento:* Los miembros del grupo usuarios del registro de rendimiento pueden administrar los contadores de rendimiento, los registros y las alertas de forma local en el servidor y desde clientes remotos sin ser miembros del grupo administradores.

*Usuarios de administración remota:* Los miembros del grupo usuarios de administración remota pueden tener acceso a los recursos WMI por protocolos de administración (como WS-Management a través del servicio de administración remota de Windows).

*Usuarios del registro de eventos:* Los miembros de este grupo pueden leer registros de eventos de equipos locales. El grupo se crea cuando el servidor se promueve a controlador de dominio.

*Administradores de Hyper-V:* Los miembros del grupo administradores de Hyper-V tienen acceso completo y sin restricciones a todas las características de Hyper-V. Agregar miembros a este grupo ayuda a reducir el número de miembros necesarios en el grupo administradores y, además, separa el acceso.

## Para saber más

Grupos de seguridad de Windows

[Grupos de seguridad de Windows](#)

## 2.1.2.- El grupo de usuarios especial Hogar de Windows 10.

En los equipos que ejecutan Windows 10 se ha quitado el Grupo Hogar de Windows 10. De todas formas, aunque se haya quitado el grupo hogar, todavía se puede compartir impresoras y archivos usando características que están integradas en Windows 10.

En el siguiente enlace podéis tener mas información sobre esto: [aquí](#).



Windows 10 (Elaboración propia)

A continuación tenéis como se utiliza el grupo hogar en 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* y, a continuación, seguimos las instrucciones del asistente. Si ya existe un grupo en el hogar en la red, Windows te preguntará si deseas unirte a ese grupo en lugar de crear uno nuevo.
- 3.- Despues 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:
  - 3.1.- Desde *Inicio-Panel de control* (poner si no está, en el campo ver por: *Iconos pequeños*)-*Grupo Hogar*
  - 3.2.- 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*, hacer clic en el nombre de la cuenta de usuario de la persona a cuyos archivos deseas obtener acceso.
- 2.- En la lista de archivos, hacer doble clic en la biblioteca a la que deseas obtener acceso y, a continuación, doble clic en el archivo o la carpeta en la que deseas 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 hace 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 deseas obtener acceso. Buscar la carpeta que deseas 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*.

## 2.2.- Usuarios y grupos locales predeterminados en Windows Server 2019.

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.

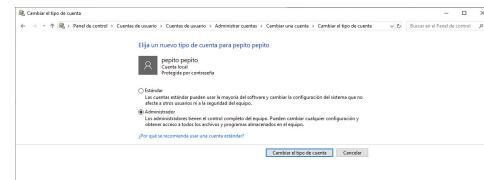
Para gestionar cuentas de usuario de forma fácil, debemos ir desde *Inicio-Panel de control-Cuentas de usuario-Cuentas de usuario-Administrar cuentas*. Aquí tenemos dos opciones:

Si hacemos clic sobre una cuenta, podemos realizar cambios sobre la cuenta como: cambiar su nombre, cambiar la contraseña, cambiar el tipo de cuenta, eliminar cuenta y administrar otra cuenta.

Si pinchamos sobre el enlace *Agregar una cuenta de usuario*, podemos crear una cuenta nueva. Cuando se crea una cuenta de usuario el sistema nos preguntará por el nombre de usuario y contraseña. Por defecto se crea una cuenta de usuario de tipo estándar.

**En el proceso de instalación del sistema Windows Server crearán 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.



Windows Server (Elaboración propia)

### Autoevaluación

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

- Administrador.
- Invitado.
- Administrador e Invitado.
- DefaultAccount

Incorrecto. Vuelve a leer la Unidad

Incorrecto. Repasa la Unidad

Muy bien. Vas por buen camino.

Incorrecto. Debes repasar los contenidos de la Unidad

## Solución

1. Incorrecto
2. Incorrecto
3. Opción correcta
4. Incorrecto

## 2.2.1.- Clasificación de Grupos de usuarios locales predeterminados en Windows Server 2019.

**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.



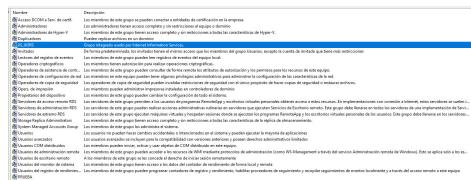
Autor Daniel Hansson / neocreo (Dominio público)

**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 administrar grupos de usuarios locales iremos desde** usamos **Usuarios y grupos locales** que se encuentran definidos en la consola MMC de la herramienta Administración de equipos. Para acceder a ella, escribimos en el panel de búsqueda Administración de equipos. Dentro de ella, a la izquierda tenemos Usuarios y grupos locales.

También podemos acceder directamente a la herramienta Usuarios y grupos locales, escribiendo en el panel de búsqueda lo siguiente: <i>lusrmgr.msc</i>.

Al hacer clic en la carpeta Grupos aparecen los grupos locales predeterminados, que se crean automáticamente al instalar el sistema operativo. **La lista de grupos de los grupos predeterminados y los derechos de usuario predeterminados para cada grupo son los mismos que los estudiados en Windows 10 en el apartado 2.1.1 del tema: Clasificación de Grupos de usuarios locales predeterminados en Windows 10 (puedes acceder y repasar la lista).** Para facilitar las tareas de administración de red, el uso de los servicios o recursos y organizar coherentlymente 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.

**Podemos concluir diciendo** que los usuarios y grupos predeterminados de Windows Server 2019 son los mismos que para Windows 10 Pro, es decir, son usuarios de ámbito local al sistema operativo del ordenador. En Windows Server 2019, 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 Escritorio remoto, los usuarios podrán ser usuarios del Escritorio remoto, (dependiendo de las licencias contratadas y disponibles para este servicio ya comentado en la unidad 1 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.

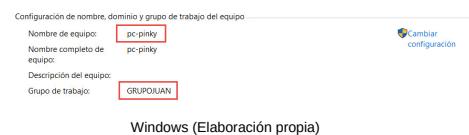
## 2.3.- Diferencias entre grupos de equipos de Windows.

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	DOMINIO
<p>Ningún equipo tiene el control sobre otro.</p> <p>Para iniciar sesión en cualquier equipo del grupo de trabajo, debe disponer de una cuenta en el equipo.</p> <p>Un grupo de trabajo no está protegido con contraseña.</p> <p>Todos los equipos deben encontrarse en la misma red local o subred.</p>	<p>Uno o más equipos son servidores.</p> <p>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.</p> <p>Un dominio puede incluir muchos de los equipos que pueden encontrarse en diferentes redes locales.</p>

El grupo hogar estaba disponible en Windows 7 en Windows 10 ya no esta disponible.

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 10](#)

### Autoevaluación

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

Sugerencia

- 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.

Incorrecto. Vuelve a leer la unidad

Muy bien

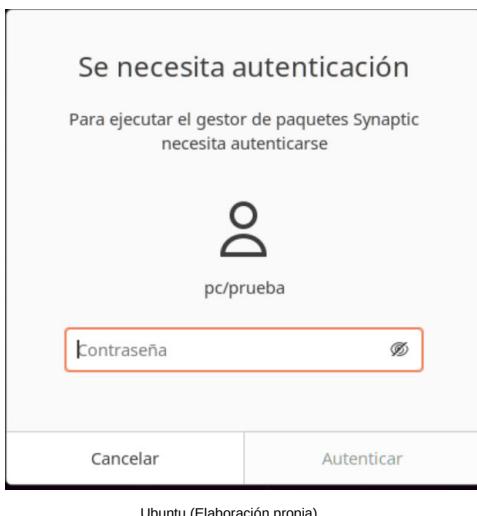
Incorrecto. Repasa la unidad

Incorrecto. Vuelve a leer los contenidos de la unidad

## Solución

1. Incorrecto
2. Opción correcta
3. Incorrecto
4. Incorrecto

## 2.4.- Usuarios y grupos locales predeterminados en Linux.



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 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

¿Cual de los siguientes ficheros guarda la contraseña encriptada?

- /home/passwd.
- /etc/passwd
- /var/passwd
- /etc/shadow

Incorrecto. Vuelve a leer la unidad

Incorrecto. Repasa la unidad

Incorrecto. Vuelve a leer los contenidos de la unidad

Muy bien. Vas por buen camino.

## Solución

1. Incorrecto
2. Incorrecto
3. Incorrecto
4. Opción correcta

## 2.4.1.- 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:

root daemon bin sys, sync games man lp mail news	uucp proxy www-data backup list irc gnats nobody systemd-timesync	systemd-network systemd-resolve messagebus syslog _apt tss uuid tcpdump avahi-autoipd	usbmux rtkit dnsmasq cups-pk-helper speech-dispatcher avahi kermoops saned nmopenvpn	hplip whoopsie colord geoclue pulse gdm vboxadd sddm 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:

root daemon byn sys adm tty disk lp mail news uucp man proxy kmem dialout fax voice cdrom floppy	tape sudo audio dip www-data backup operator list irc src gnats shadow utmp video sasi plugdev staff games users	nogroup systemd-journal systemd-timesync systemd-network systemd-resolve crontab messagebus input kvm render syslog tss bluetooth ssl-cert uuid tcpdump avahi-autoipd rtkit ssh	netdev lpadmin avahi scanner saned nm-openvpn whiipsie colord geoclue pulse pulse-access gdm lxd sambashare system-coredump vboxsf sddm mlocate
--	--	---	--

### 3.- Seguridad de cuentas y contraseñas de usuario.

#### Caso práctico



[Alain Bachellier \(CC BY-NC-SA\)](#)

**Vindio** y **Laro** han cogido la responsabilidad de gestionar la seguridad del sistema, pero quieren que las tres chicas de FCT (**Noiba**, **Naroba** y **Jana**), les ayuden en dicha labor.

¿Entonces vamos a aprender a realizar el control de dicha seguridad para que no se produzcan posibles alteraciones en el sistema que perjudiquen la actividad empresarial? -- responde **Laro**.

Efectivamente, debemos crear políticas de acceso que obliguen a los usuarios a modificar la contraseña cada cierto tiempo y que su escritura cumpla con las especificaciones necesarias de seguridad, —

responde **Vindio**.

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.



[warszawianka \(Dominio público\)](#)

# 3.1.- Seguridad de cuentas y contraseñas de usuario Windows 10.

Windows 10 permite centrar la tarea de administración del equipo desde el Panel de control y Configuración del menú de Inicio, 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 a la gestión de cuentas de usuario, escribiendo en el panel de búsqueda *Panel del control* y luego haciendo clic en *Cuentas de usuario* -> *Cuentas de usuario* seleccionar la 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:

Desde *Panel de control-Cuentas de usuario-Administrar credenciales*. Hacer clic en *Agregar una credencial de Windows*.

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.iesalisa.es).

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*.

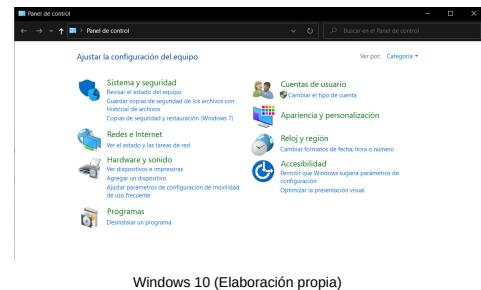
Podemos ejecutar desde una ventana de comandos, el comando **control userpasswords2** que nos mostrará la ventana de Cuentas de usuarios y entre una de las muchas opciones que da, te muestra la Administración de contraseñas.

**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 ayudarte 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



Windows 10 (Elaboración propia)

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 dónde buscar archivos ejecutables, donde almacenar los archivos temporales, etc. Puedes comprobar las variables existentes en el apartado Administración de usuarios y grupos locales de la unidad.

## Para saber más

Control de cuentas de usuario

[Control de cuentas de usuario](#)

## 3.1.1.- El control de cuentas de usuario UAC en Windows 10.

**Control de cuentas de usuario (UAC)** es una característica de Windows, que te ayuda a controlar el equipo informándote cuando un programa realice un cambio que requiera permiso de nivel de administrador. UAC funciona ajustando el nivel de permiso de tu cuenta de usuario. Cuando se vayan a realizar cambios en el equipo que requieran permiso de nivel de administrador, UAC te lo notificará. Si es administrador, haces clic en Sí para continuar. Si no eres administrador, alguien con cuenta de administrador en el equipo tendrá que escribir su contraseña para continuar. En conclusión, control de cuenta de usuario te pide permiso antes de instalar software o de abrir determinados tipos de programas que podrían dañar el equipo o hacerlo vulnerable a amenazas de seguridad.

En Windows 10 puedes ajustar la frecuencia con la que UAC te notifica los cambios en el equipo, atendiendo a los siguientes niveles de control de cuentas:

**Nivel 1 de UAC** no notificar nunca (no se recomienda) cuando:

Las aplicaciones intenten instalar software o hacer cambios en el equipo.  
Realice cambios en la configuración de Windows.

**Nivel 2 de UAC** notificarme solo cuando una aplicación intente realizar cambios en el equipo (no atenuar el escritorio). No notificará cuando realice cambios en la configuración de Windows.

**Nivel 3 de UAC** notificarme solamente cuando una aplicación intente realizar cambios en el equipo (opción predeterminada en Windows 10). No se notificará cuando realice cambios en la configuración de Windows.

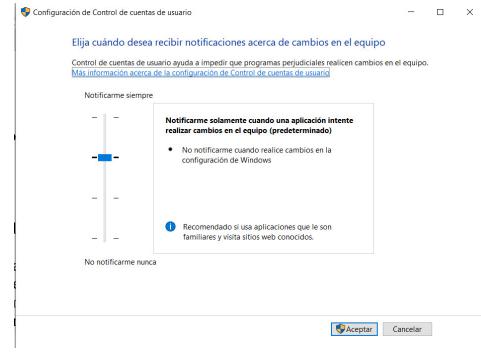
**Nivel 4 de UAC** se notificará siempre cuando:

Las aplicaciones intentan instalar software o hacer cambios en el equipo.  
Realice cambios en la configuración de Windows.

Para desactivar el control de cuentas de usuario, puesto que puede resultar incómodo ya que cada vez que abrimos un programa (Internet Explorer, Firefox u otro), siempre tendremos que confirmar. Para poder acceder al programa o a la Web sin confirmaciones previas, hay que seguir los siguientes pasos:

Desde Panel de control-Cuentas de usuario-Cambiar la configuración de Control de cuentas de usuario.

Deslizamos la barra hasta *No notificarme nunca* y hacemos clic en *Aceptar*.



Windows 10 (Elaboración propia)

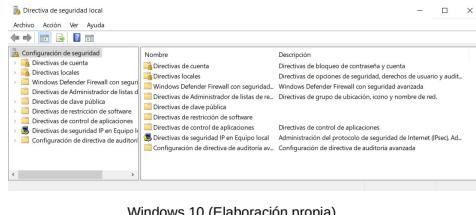
### Para saber más

Control de cuentas de usuario

[Control de cuentas de usuario](#)

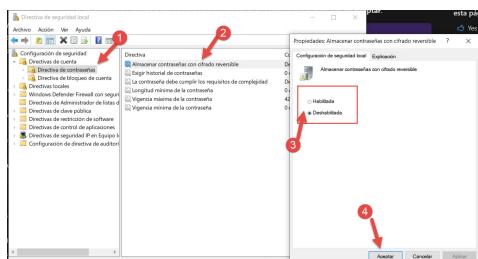
## 3.1.2.- Introducción a las directivas de seguridad de usuarios en Windows 10.

Las directivas de seguridad son un conjunto de reglas de seguridad, referentes a características y permisos que se pueden configurar con el fin de garantizar el acceso a los recursos del sistema.



El sistema aporta desde la instalación unas directivas de seguridad predeterminadas, que son suficientes para la mayoría de las situaciones, los administradores pueden modificarla o personalizarla para que se ajuste a las necesidades específicas de la organización del sistema.

Para acceder a la gestión de directivas iremos al panel de búsqueda y escribimos *Editor de directivas de grupo local* (el comando que se ejecuta para entrar en este modo es <i>secpol.msc</i> que se encuentra en <i>%windir%\System32\secpol.msc</i>). Para gestionar una regla de directiva, se hace doble clic sobre una directiva, a la derecha nos muestra las directivas que hay. Para modificar una de ellas, hacemos doble clic sobre ellas y seleccionamos la opción elegida. Pulsamos el botón *Aceptar* para confirmar los cambios. También podemos hacer, clic en el botón derecho del ratón y pulsamos la opción *Propiedades* y de la ventana de asistente de configuración *Activar/desactivar* o completar los campos deseados.



Windows 10 (Elaboración propia)

### Debes conocer

Configurar la directiva de contraseñas de usuario en Windows 10

[Configurar la directiva de contraseñas de usuario](#)

Cómo usar el editor de directivas de grupo local

[Usar el editor de directivas de grupo local](#)

### Para saber más

Configuración de las directivas de seguridad

[Configuración de las directivas de seguridad](#)

Directiva de cuenta

[Directiva de cuenta](#)

### 3.1.3.- Clasificación de directivas de seguridad de usuarios y contraseñas en Windows 10.

Dentro de la directiva de seguridad local relacionada con usuarios y contraseñas tenemos:

En Directivas de cuenta: se clasifican en:

Directivas de contraseña: podemos encontrar las reglas:

Almacenar contraseñas con cifrado reversible: Es prácticamente lo mismo que almacenar versiones de texto simple de las contraseñas. Por esta razón, esta directiva no debería habilitarse nunca, a menos que los requisitos de la aplicación tengan más importancia que la necesidad de proteger la información de contraseñas.

Exigir historial de contraseñas: Esta configuración de seguridad determina el número de nuevas contraseñas únicas, que deben asociarse a una cuenta de usuario antes de poder reutilizar una contraseña antigua. El valor debe estar comprendido entre 0 y 24 contraseñas.

La contraseña debe cumplir los requisitos de complejidad: No contener el nombre de cuenta del usuario o partes del nombre completo del usuario en más de dos caracteres consecutivos

Tener una longitud mínima de seis caracteres

Incluir caracteres de tres de las siguientes categorías: mayúsculas (de la A a la Z), minúsculas (de la a a la z) y dígitos de base 10 (del 0 al 9)

Caracteres no alfanuméricos (por ejemplo, !, \$, #, %)

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.

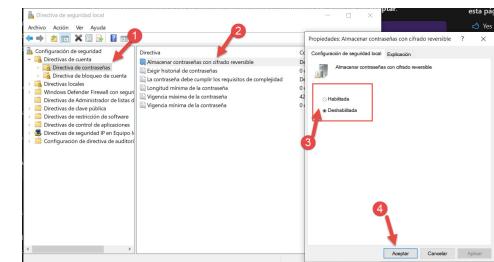
En Directivas de bloqueo de cuenta: podemos encontrar las siguientes reglas:

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 desbloquea explícitamente.

Restablecer el boqueo 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: se encarga de controlar las directivas de auditoría, asignación de derechos de usuario y opciones de seguridad.



Windows 10 (Elaboración propia)

## Autoevaluación

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

- Verdadera
- Falsa

Muy bien. Vas por buen camino.

Incorrecto. Vuelve a leer la Unidad

## Solución

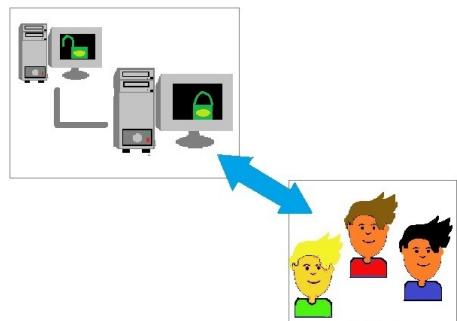
1. Opción correcta
2. Incorrecto

### 3.1.4.- Las directivas de seguridad de grupos locales de usuarios en Windows 10.

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 MMC). Este complemento MMC se abre escribiendo en el panel de búsqueda *Editor de directivas de grupo local* y pinchamos sobre su resultado.

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



1.- Abrimos: *Editor de directivas de grupo local* como se ha comentado antes.

Windows 10 (Elaboración propia)

2.- Pulsar en panel izquierdo nos aparecen las siguientes directivas:

2.1.- Configuración del equipo: nos permite realizar y establecer ajustes a los parámetros de la máquina local.

2.2.- Configuración de usuario: nos permite establecer la configuración necesaria para el software instalado en la máquina local.

2.2.1.- Las dos opciones anteriores están subdivididas en varias opciones:

2.2.1.1.- Configuración de software: permite establecer la configuración necesaria para el software instalado en la máquina local.

2.2.1.2.- Configuración de Windows: podemos establecer los parámetros relacionados con el entorno de Windows, por ejemplo, directivas de seguridad, scripts, resolución de nombres, etc; Esta ficha es de mucho cuidado porque algún ajuste mal establecido puede afectar el rendimiento del sistema.

2.2.1.3.- Plantillas administrativas: es la opción que más usaremos ya que desde allí está prácticamente todos los ajustes del equipo, panel de control, inicio de sesión, apagado, etc.

Vamos a ver como se quita el icono de la papelera de reciclaje de Windows, para ello:

1.- Abrimos: *Editor de directivas de grupo local* como se ha comentado antes.

2.- Pulsamos en el panel izquierdo en la opción, *configuración de usuario* hacemos doble clic.

3.- Doble clic en *Plantillas administrativas*.

4.- Clic en *Active Desktop*.

5.- En el panel de la derecha, hacemos clic en la opción *Quitar del escritorio el ícono de la papelera de reciclaje*. Al pinchar en cada opción a la derecha nos aparece una descripción de la acción a realizar y los requisitos que tiene que tener el sistema para poder aplicarlo. Hacemos doble clic, y seleccionamos la opción *Habilitada*.

6.- Pulsamos en *Aplicar y Aceptar*.

7.- En el panel de búsqueda escribimos *gpupdate* que permite actualizar las directivas.

8.- Hay que veces que hay que reiniciar el sistema para que alguna de estas acciones surjan efecto.

Podemos hacer otras opciones como *bloquear todas las opciones de la barra de tareas*, *impedir el acceso al símbolo del sistema*, etc.

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 el *Editor de directivas de grupo-Configuración de equipo-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:

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

[Preferencias de directivas de grupo](#)

Manual del editor de directivas de grupo local

[Editor de directivas de grupo](#)

## Debes conocer

Crear y gestionar políticas de grupos en Windows Server 2019

[Políticas de grupos en Windows Server 2019](#)

Vídeo tutorial de como usar el editor de directivas de grupo

[Usar el editor de directivas de grupo](#)

## Autoevaluación

**El comando que nos permite actualizar las directivas del Editor de directivas de grupo local es update.**

- Verdadera
- Falsa

Muy bien. Vas por buen camino.

Incorrecto. Vuelve a leer la Unidad

## Solución

1. Opción correcta
2. Incorrecto

## 3.2.- Seguridad de cuentas y contraseñas de usuario Windows server 2019.

La seguridad de cuentas y contraseñas de usuarios locales de Windows Server 2019, se basa en la misma teoría que en Windows 10, 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.

Windows Server 2019 (Elaboración propia)

*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 10 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 nunca expira.*

*La cuenta esta deshabilitada.*

*La cuenta esta bloqueada.*

### Autoevaluación

¿Cuál de las siguientes opciones sobre contraseñas de usuarios en Windows 10 no está disponible?

Sugerencia



El usuario no puede cambiar la contraseña

- La contraseña nunca expira
- La cuenta está bloqueada.
- La cuenta esta desactivada.

Incorrecta. Vuelve a leer la unidad

Incorrecta. Repasa la unidad

Muy bien. Vas por buen camino

Incorrecta. Vuelve a leer los contenidos de la unidad

## Solución

1. Incorrecto
2. Incorrecto
3. Opción correcta
4. Incorrecto

## 3.2.1.- Directivas de seguridad local en Windows Server 2019.

Las directivas de seguridad local referentes a usuario y grupos son idénticamente iguales a las de Windows 10. Un listado de las directivas de cuenta es:

Directiva de contraseñas	
Exigir 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 el bloqueo de cuenta después de...	
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:

- 1.- **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).
- 2.- **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.
- 3.- **Dominios de Active Directory o directiva de grupo de dominio:** se aplican a todos los equipos y/o usuarios de dominio.
- 4.- **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 2019 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 <i>SystemRoot\System32\GroupPolicy</i>. 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](#)

Cómo crear y gestionar GPO en Windows Server

[Gestionar GPO en Windows Server](#)

## **3.2.2.- Introducción a las copias de seguridad y restauración de archivos en Windows Server 2019.**

---

**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:

La interfaz de usuario de **MMC(WBADMIN.MCS)**

El conjunto de cmdlets de **Windows PowerShell**.

Desde el administrador del servidor, pulsando en el menú herramientas y seleccionando **Copias de seguridad de Windows Server**.

**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 crearse 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 2019, 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).

Para poder realizar copias de seguridad en Windows Server 2019, primero tenemos que activar la característica de Copias de seguridad de Windows Server. Para ello lo hacemos desde el Administrador del servidor y seleccionamos la opción Agregar Roles y características. [Aquí](#) tenéis un enlace donde explica como hacerlo.

**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.

Windows Server 2019 (Elaboración propia)

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.

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.

Windows Server (Elaboración propia)

## Para saber más

Por qué necesita una copia de seguridad Windows Server

[¿Necesita una copia de Seguridad?](#)

Hacer copias de seguridad con PowerShell

[Copias de seguridad con PowerShell](#)

## Debes conocer

Como hacer copias de Seguridad en Windows Server

[Como hacer copias de Seguridad](#)

Agregar la característica copia de seguridad

[Agregar la característica copia de seguridad](#)

### 3.2.3.- Configuración de copias de seguridad y restauración de archivos en Windows Server 2019.

Para poder realizar copias de seguridad en Windows Server 2019, primero tenemos que activar la característica de *Copias de seguridad de Windows Server*. Para ello lo hacemos desde el *Administrador del servidor* y seleccionamos la opción *Agregar Roles y características*. Seguimos las instrucciones del asistente, seleccionamos la característica *Copias de seguridad de Windows Server* y seguimos las instrucciones del asistente. [Aquí](#) tenéis un enlace donde explica como hacerlo.

Windows Server (Elaboración propia)

Windows Server (Elaboración propia)

#### Podemos realizar una copia de seguridad de varias formas:

Abrir el Administrador del servidor, pinchamos en el menú Herramientas y seleccionar *Copias de seguridad de Windows Server*. También podemos abrir la herramienta de copias de seguridad, haciendo clic en la lupa y escribimos WBADMIN, hacemos clic en *Copias de seguridad de Windows Server*.

Para realizar una copia de seguridad realizamos los siguientes pasos:

- 1.- En la ventana *Copias de seguridad de Windows Server (local)*, hacemos clic sobre la opción copia de seguridad local del panel izquierdo.
- 2.- Se abre el asistente para realizar una copia de seguridad una vez. Tenemos que elegir entre:
  - 2.1.- Si hacemos una copia de seguridad siguiendo los valores elegidos en una copia de seguridad programada anterior. Esta opción esta inactiva si aún no hemos realizado ninguna copia programada.
  - 2.2.- Si queremos realizar una copia de seguridad con parámetros diferentes a los de la copia programada.
- 3.- Elegimos la segunda opción.
- 4.- En el siguiente paso, decidiremos si la copia es del *Servidor completo* (incluyendo todos los volúmenes, e incluso el estado del propio sistema) o *Personalizada* (donde podremos excluir los volúmenes que queramos).
- 5.- Elegimos la opción personalizada.
- 6.- Ahora tenemos que indicar qué volúmenes estarán incluidos en la copia de seguridad. No podremos incluir el volumen que utilizaremos como destino de la copia, en este caso, el que tiene la etiqueta *Disco Local (C:)*.
- 7.- Comprobamos que el elemento elegido aparece en la lista (ahora mismo con un solo objeto). Si queremos añadir nuevos orígenes de datos para la copia, sólo hay que repetir los puntos 5 y 6 todas las veces que sea necesario. Pulsamos en el botón *Siguiente*.
- 8.- El siguiente paso consistirá en elegir un destino para la copia de seguridad. Podemos escoger entre una unidad local y una carpeta compartida en la red por otro servidor donde tengamos los permisos adecuados. En nuestro caso, hemos preparado la unidad Datos (E): para que sea el destino de nuestras copias, por lo que elegiremos *Unidades locales*. Nos muestra un resumen con el espacio que tenemos libre en esta unidad. Si hubiésemos indicado *Carpeta compartida remota*, tendríamos que especificar la ubicación de dicha carpeta. Pulsamos en el botón *Siguiente*.
- 9.- El asistente nos muestra un resumen de los valores que hemos elegido hasta ahora. Pulsamos en el botón *Copia de seguridad*. En versiones anteriores, podíamos elegir dos modos diferentes de hacer la copia de seguridad. Ahora, la opción predeterminada es *Copia de seguridad de copia de VSS*.

Desde el símbolo del sistema. Abrimos símbolo del sistema en modo administrador y escribimos la orden:

```
wbadmin /?
```

Este comando nos muestra la ayuda de wbadmin. **Podemos acceder a realizar una copia de seguridad y recuperación de la siguiente forma:**

Creamos una copia de seguridad del estado del sistema, escribimos el comando:

```
Wbadmin start systemstatebackup
```

Recuperamos el estado del sistema, escribimos el comando:

```
Wbadmin start systemstaterecovery
```

Con PowerShell. Abrimos PowerShell, haciendo clic en el botón de Inicio, en la parte derecha seleccionamos Windows PowerShell ISE. Pulsa [Aquí](#) para hacer Backup en Windows Server 2019

## Restaurar una copia de seguridad

Abrimos el *Administrador del servidor*, abrir el menú *Herramientas* y hacer clic sobre la opción *Copias de seguridad de Windows Server*. En el panel central, podremos ver la lista con todas las copias que hemos ido haciendo, ordenadas por fecha y hora.

Windows Server (Elaboración propia)

Para recuperar una de las copias o cualquiera de los archivos contenidos en ellas, hacemos lo siguiente:

- 1.- Hacemos clic en el enlace *Recuperar* que encontramos en el panel derecho. Se abrirá un asistente que nos guiará en el proceso de recuperación.
- 2.- En la primera pantalla elegimos si vamos a recuperar datos de una copia en el equipo local o de otro equipo de la red local. Hacemos clic en *siguiente*.
- 3.- Elegimos la fecha y hora de la copia que queremos reestablecer. Al seleccionar podemos ver información sobre donde esta almacenada y si está disponible. Hacemos clic en *siguiente*.
- 4.- Elegimos que es lo que vamos a recuperar. Podremos elegir entre recuperar volúmenes completos, aplicaciones o archivos de datos individuales. Esta última opción es particularmente útil cuando necesitamos una versión antigua de un documento que hemos modificado. Una vez elegida la opción, hacemos clic en *siguiente*.
- 5.- Seleccionamos los elementos que vamos a recuperar. Cuando los encontramos, los seleccionaremos en el panel de la derecha. Se pueden seleccionar archivos individuales o carpetas.
- 6.- Una vez seleccionados, hacemos clic en *siguiente*.
- 7.- Elegimos como vamos a realizar la recuperación:
  - 7.1.- *Destino de la recuperación*:
    - 7.1.1.- *Ubicación original*: los archivos se recuperarán en su ubicación original.
    - 7.1.2.- *Otra ubicación*: elegir otra lugar donde recuperar los archivos separados de la ubicación original.
  - 7.2.- *Cuando se encuentren elementos en la copia de seguridad que ya estén en el destino*: que hace la aplicación cuando intente recuperar un archivo que ya existe en el lugar de destino (ejemplo: recuperar una versión antigua de un archivo que se ha modificado después de realizar la copia de seguridad). Tenemos tres opciones:
    - 7.2.1.- *Crear copias para tener ambas versiones*: tenemos a la vez la versión antigua y la nueva.
    - 7.2.2.- *Sobreescribir las versiones existentes con las recuperadas*.

- 7.2.3.- *No recuperar los elementos ya existentes en el destino de recuperación.* En esta opción no se recuperan los valores que ya se encuentran en el sistema.
- 7.3.- *Configuración de seguridad:* aquí se indica si, además de los archivos, se recuperan también sus características de seguridad, como: permisos, propietarios,etc.
- 7.4.- Seleccionadas las opciones anteriores, hacemos clic en *siguiente*.
- 8.- El asistente nos muestra un resumen con todas las opciones seleccionadas. Si hay algo que esta mal, podemos pulsar en el botón *Anterior*. Si esta todo bien, hacemos clic en *Recuperar*.
- 9.- Esperamos hasta que el proceso termine. Si no hemos cerrado el asistente, cuando termine la restauración, la barra de progreso será sustituida por un mensaje informativo.
- 10.- Al terminal el proceso, en la ventana principal, quedará registrada la restauración realizada.

Windows Server (Elaboración propia)

Windows Server (Elaboración propia)

## Debes conocer

Hacer una copia de seguridad y restaurarla en Windows Server.

[Copia de seguridad y restaurarla en Windows Server.](#)

[Backup en Windows Server](#)

Copias de seguridad a través de PowerShell en Windows Server.

[Vídeo tutorial de Copias de seguridad a través de PowerShell en Windows Server.](#)

[Backup en Windows Server con PowerShell](#)

## Para saber más

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

[Herramienta para hacer copias de Seguridad](#)

## 3.3.- 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 `<i>su</i>` y `<i>sudo</i>`.

**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.

Antonio López (Elaboración propia)

### 3.3.1.- 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*, pinchamos en mostrar aplicaciones, escribimos *terminal* y pinchamos sobre *Terminal*. También podemos acceder pulsando la combinación de teclas *CTRL+ALT+Supr*. Se abre un terminal y ejecutamos la orden:

```
root@prueba:/home/prueba# more /etc/passwd
root:x:0:0:root:/root:/bin/bash
prueba:x:1000:1000:prueba,,,:/home/prueba:/bin/bash
```

Ubuntu (Elaboración propia)

#### Campos del fichero /etc/passwd

<b>Campo 1</b>	Nombre de la cuenta del usuario.
<b>Campo 2</b>	Contraseña del usuario.
<b>Campo 3</b>	UID (Identificador de usuario, 0 es para root).
<b>Campo 4</b>	Identificador numérico de grupo. De la misma manera que con el UID, el cero es siempre para root.
<b>Campo 5</b>	Descripción opcional de la cuenta. Se suele usar para dejar constancia del nombre real del usuario.
<b>Campo 6</b>	Otros campos como: nombre completo, número de habitación, teléfono del trabajo, teléfono de la casa y otros campos.
<b>Campo 7</b>	Directorio principal del usuario.
<b>Campo 8</b>	Interprete de comando por defecto.

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@prueba:/home/prueba# more /etc/shadow
prueba:$6$pSwsW.b0$5uCoovxVZ5YTq.YnuxYIG9fgrdxgfdgvbfg43434534534534YbabuLSB1:14642:0:99999:7:::
```

La información obtenida en dicho fichero es:

Ubuntu (Elaboración propia)

## Campos del fichero /etc/shadow

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

### Para saber más

Administración de usuarios

[Administración de usuarios](#)

### 3.3.2.- 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 jorge 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:

Ubuntu (Elaboración propia)

```
root@prueba:/home/prueba# chage -M 0 -W 560 jorge
```

De otra forma cualquier usuario puede ver cuando vence su contraseña con el comando `chage -l<code>`, por ejemplo para el usuario jorge sería:

```
root@prueba:/home/prueba# chage -l jorge
Último cambio de contraseña : abr 29, 2020
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 : 10
Número de días de aviso antes de que caduque la contraseña : 7
```

Con el comando `pwunconv` se elimina el fichero `shadow` pasando las contraseñas cifradas al fichero `passwd`, como el ejemplo siguiente:

```
root@prueba:/home/prueba# pwunconv
root@prueba:/home/prueba# more /etc/passwd
root:dfjsdfj48345345mnfdgm dfgmdfgp:0:0:root:/root:/bin/bash
jorge:$6$pSwsW.b0$5uCoovxVZ5YTq.YnuxYIG9fgrdxgfdgvbfg43434534534534YbabuLSB1:510:520:Jorge Marco:/home/jorge:/bin/bash
...
root@prueba:/home/prueba# more /etc/shadow
/etc/shadow: No such file or directory
```

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

```
root@prueba:/home/prueba# pwconv
root@prueba:/home/prueba# more /etc/shadow
jorge:$6$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:

<b>PASS_MAX_DAYS</b>	Número máximo de días que una contraseña es válida
<b>PASS_MIN_LEN</b>	El número mínimo de caracteres en la contraseña
<b>UID_MIN</b>	Valor mínimo para usuarios normales cuando se usa <code>useradd</code>
<b>UMASK</b>	El valor umask por defecto
<b>CREATE_HOME</b>	Si el comando <code>useradd</code> debe crear el directorio home por defecto

<b>MOTD_FILE</b>	El contenido de este fichero de texto se muestra a todos los usuarios tras identificarse
<b>LOGIN_RETRIES</b>	Número máximo de intentos si se escribe mal la contraseña en la entrada al sistema
<b>SU_WHEEL_ONLY</b>	Limitar permisos de "su" a determinados usuarios al estar en yes sólo grupo root

## Debes conocer

Uso del comando <span lang="en">chage</span>

[Comando Chage](#)

### 3.3.3.- 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/auth.log.** Con el comando `<i>less</i>` 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:

**Brutus:** es una herramienta de descifrado de contraseñas.

**Aircrack-ng:** analiza los paquetes cifrados inalámbricos y descifra sus contraseñas mediante su propia algoritmo. Mas información [aquí](#).

**Rainbow Crack:** descifra los hash de las contraseñas. Mas información [aquí](#).

**John the Ripper:** herramienta de descifrado de passwords. Mas información [aquí](#).

Usar el comando `<span title="en"><em>Last</em></span>`, que nos permite listar los acceso al sistema, las salidas, si reiniciaron la maquina, accesos a un archivo en particular, etc, y todo ello indicando fecha y hora.

Tenemos herramientas como **Audit** que permite realizar una auditoría de Linux. Es capaz de grabar los siguientes datos:

Fecha, hora, tipo y resultado de un evento.

Etiquetas de sensibilidad de sujetos y objetos.

Asociación de un evento con la identidad del usuario que ejecuto el evento.

Desplegar todas las modificaciones a la configuración de auditoría e intento de acceso a los archivos de registro de auditoría.

Almacenar todos los usos de los mecanismos de autenticación, como SSH, Kerberos y otros.

Es posible cambiar a cualquier base de datos de confianza, como /etc/passwd.

Registra cualquier intento de importar o exportar información hacia o desde el sistema.

Incluye o excluye eventos basados en identidad de usuario, etiquetas de sujeto y objeto y otros atributos.

**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** 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 `<i>pam_cracklib</i>` 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 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 pincha [aquí](#).

## Para saber más

Como fuente de documentación acceder a:

[Administración de Linux 1](#)

[Autenticación](#)

Gestión de contraseñas en Linux usando passwd

[Administración de Linux 2](#)

PAM. ¿Qué es y cómo ayuda a proteger tus archivos digitales?

[PAM](#)

Cómo auditar Linux con Audit Tool y Ausearch

[Auditar Linux](#)

## Debes conocer

Uso del comando *Last*

[Comandos \*Last\* y \*Lastb\*](#)

## 4.- Administración de perfiles locales de usuario.

### Caso práctico

Es importante preparar los sistemas operativos 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.

Entonces, ¿tendremos que aplicar todas las posibilidades que nos ofrece el sistema para gestionar los perfiles de usuarios? —pregunta **Jana**.

Sí, con la finalidad de realizar la actividad de responsable del sistema como usuario administrador, —responde **Vindio**.

Pongamos manos a la obra, —indica **Laro**.

[Alain Bachellier \(CC BY-NC-SA\)](#)

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 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.

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.

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.

### Para saber más

Perfiles de usuarios móviles

[Perfiles de usuarios móviles](#)



## 4.1.- Perfiles de usuarios locales en Windows.

Los perfiles de usuario en Windows 10 y Windows Server se localizan en `<i>c:\Users (usuarios)\nombre_usuario</i>` e incluye todos los ajustes de la cuenta como fondo de escritorio, salvapantallas, opciones de Explorador de archivos y muchas otras opciones y configuraciones. Cuando el perfil de usuario está dañado, Windows 10 muestra el mensaje *No puedes iniciar sesión con tu cuenta. Inicio de sesión temporal* e inicia un perfil temporal.

Un *perfil temporal* es una nueva sesión de usuario en la que cualquier modificación que el usuario realice se perderá después de cerrar la sesión. Además no existe ni rastro de nuestra información (documentos, imágenes, vídeos, configuraciones...). Este perfil temporal se guarda en la carpeta **C:\Users\Temp**.

El perfil genérico de Windows es *Default*, 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:

1.- *ntuser.dat* (registro del perfil móvil de usuario, los cambios se guardan al finalizar la sesión).

Windows (Elaboración propia)

2.- *ntuser.dat.log* (se guardan temporalmente los cambios, hasta que termina la sesión que se grabarán en el disco).

3.- *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 al *Panel de control-Cuentas de usuario-Cuentas de usuario-Configurar las propiedades avanzadas del perfil de usuario*. En la ventana que se abre, ahí verás todos los perfiles, su tamaño y el estado de los mismos.

### Debes conocer

Perfiles de usuario

[Perfiles de usuario](#)

Acceder a perfiles de usuario

[Acceder a los perfiles de usuario](#)

### Para saber más

Administrar perfiles de usuario en Windows 10 con Powershell

[Administrar perfiles de usuario en Windows 10 con Powershell](#)

Administrar perfiles de usuario en Windows

[Administrar perfiles de usuario con PowerShell](#)

# Autoevaluación

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

- C:\users\nombre\_usuario.
- C:\usuarios\generico.
- C:\users\default.
- C:\users\generic

Incorrecto. Vuelve a leer la unidad.

Incorrecto. Repasa los contenidos de la unidad.

Muy bien. Sigue avanzando.

Incorrecto. Deberías volver a leer la unidad.

## Solución

1. Incorrecto
2. Incorrecto
3. Opción correcta
4. Incorrecto

#### **4.1.1.- Operaciones con la configuración del perfil de usuarios locales en Windows.**

## Algunas operaciones con perfiles de usuarios:

Podemos **crear una copia de seguridad de tu perfil** para pulsa [aquí](#).

Para borrar un perfil de usuario en Windows, ejecutamos el comando `sysdm.cpl`, pinchamos en la lengüeta *Opciones avanzadas* -> *Configuración*, seleccionamos el perfil y pulsar en el botón *Eliminar*.

**Para copiar los archivos desde un perfil existente** a otro perfil de usuario seguimos los pasos que se indican [aquí](#).

**Reparar un perfil dañado.** Para poder reparar un perfil dañado, tenemos que 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 con otro usuario o acceder en modo seguro (En el siguiente video se explica como acceder en modo seguro. [Aquí](#).)
  - 2.- Abrir el registro, ejecutando el registro. Para ello, pulsamos las teclas **WINDOWS+R** y escribimos *regedit*. Pulsamos **Aceptar**.
  - 3.- Nos vamos hasta la clave: **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList**. Ahí veremos una serie de carpetas con un nombre que incluyen unas series numéricas y que están relacionadas con las cuentas de usuario del sistema. Para saber cuál es la que se corresponde con el perfil de usuario dañado, tenemos que entrar en cada una de ellas y fijarnos en los datos del valor de cadena con el nombre **ProfileImagePath**, que nos mostrará el nombre de usuario al que corresponde.
  - 4.- Localizada la entrada que corresponde al perfil del usuario dañado, hacemos doble clic sobre el valor **State** y le asignamos el valor **0**.
  - 5.- Buscamos un valor que se llama **RefCount** dentro de esa misma ruta y en caso de que no exista hacemos clic con el botón derecho del ratón sobre el panel y seleccionamos **Nuevo - Valor de DWORD (32 bits)**. Le ponemos el nombre **RefCount** y hacemos doble clic sobre el valor que acabamos de crear, nos aseguramos de asignarle también el valor **0**.
  - 6.- Cerramos el registro de Windows 10, reiniciamos el equipo para que los cambios sean efectivos y comprobamos que ya podemos entrar en el sistema con el perfil de usuario dañado.

Windows (Elaboración propia)

*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 por defecto. Antes hay que crear las carpetas. 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 `<i>\nombre_usuario_dominio.nombre_NetBios_dominio</i>`. 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:

*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 2019, una nueva directiva te permite establecer perfiles móviles para varios usuarios en un GPO.

## Debes conocer

Eliminar un perfil de usuario

[Eliminar un perfil de usuario en Windows](#)

Pasar archivos entre cuentas de usuarios

[Pasar archivos entre cuentas de usuarios en Windows](#)

Crear una copia de seguridad de tu perfil de usuarios de Windows

[Cómo crear una copia de seguridad de tu perfil de usuarios de Windows](#)

## Para saber más

Cómo cambiar, ocultar o eliminar la imagen de cuenta de usuario Windows 10

[Cómo cambiar, ocultar o eliminar la imagen de cuenta de usuario Windows 10](#)

Migrar información de un usuario local a otro

[Migrar información de un usuario local a otro](#)

Cómo reparar un perfil de usuario dañado en Windows

[Reparar un perfil de usuario dañado](#)

[Repara un perfil dañado](#)

## 4.2.- 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:

Ubuntu (Elaboración propia)

1	<code>&lt;i&gt;/etc/profile&lt;/i&gt;</code>	Ejecutar el perfil genérico para todos los usuarios
2	<code>&lt;i&gt;/home/nombre_usuario/.profile&lt;/i&gt;</code>	Ejecuta el .bashrc
3	<code>&lt;i&gt;/home/nombre_usuario/.bashrc&lt;/i&gt;</code>	Contiene comandos que se ejecutan al inicio del Shell de forma interactiva
4	<code>&lt;i&gt;/home/nombre_usuario/.bash_history&lt;/i&gt;</code>	Almacena el histórico de comandos que introduce el usuario en consola
5	<code>&lt;i&gt;/home/nombre_usuario/.bash_logout&lt;/i&gt;</code>	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:

<code>&lt;i&gt;prueba@prueba:/home/prueba\$ &lt;i&gt;ls -lta   grep .profile&lt;/i&gt;</code>	Busca los fichero <code>&lt;i&gt;.profile&lt;/i&gt;</code> en la ubicación actual
<code>&lt;i&gt;prueba@prueba:/home/prueba\$ &lt;o:p&gt;&lt;/o:p&gt;&lt;i&gt;ls -a&lt;/i&gt;</code>	Lista todos los ficheros ocultos
<code>&lt;i&gt;prueba@prueba:/home/prueba\$ &lt;o:p&gt;&lt;/o:p&gt;&lt;i&gt;more .profile&lt;/i&gt;</code>	Visualizamos el contenido del fichero <code>.profile</code>
<code>&lt;i&gt;prueba@prueba:/home/prueba\$ &lt;o:p&gt;&lt;/o:p&gt;&lt;i&gt;gedit .profile&lt;/i&gt;</code>	Editamos el fichero <code>.profile</code>
<code>&lt;i&gt;prueba@prueba:/home/prueba\$ &lt;o:p&gt;&lt;/o:p&gt;&lt;i&gt;su - nombre_usuario&lt;/i&gt;</code>	Cambiamos de usuario y se ejecuta su <code>.profile</code>
<code>&lt;i&gt;prueba@prueba:/home/prueba\$ &lt;o:p&gt;&lt;/o:p&gt;&lt;i&gt; su nombre_usuario&lt;/i&gt;</code>	Cambiamos de usuario pero no ejecuta el <code>.profile</code>

Debemos de tener en cuenta que cada vez que modificuemos el fichero `.profile` y ejecutemos el comando `su - Nombre de 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>&lt;i&gt;prueba@prueba:/home/prueba\$&lt;o:p&gt;&lt;/o:p&gt;&lt;i&gt; gedit .profile&lt;/i&gt;</code>	Editar el fichero <code>.profile</code>
2	<code>echo "Hola ya estas en el sistema" echo "estás en el directorio" &lt;i&gt;pwd&lt;/i&gt;</code>	Añadir al final las líneas siguientes

3		Guardar el archivo y salir
4	<i>exit</i>	Salir de la sesión del usuario
5	<i>prueba@prueba:/home/prueba\$ <o:p></o:p></i> <i>su – prueba</i>	Entrar al sistema como usuario carlos

## Autoevaluación

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

Sugerencia

- 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.
- Edita el fichero que configura el perfil de todos los usuarios del sistema.

Incorrecto. Deberías leer de nuevo la unidad.

Muy bien. Vas progresando.

Incorrecto. Vuelve a leer la Unidad.

Incorrecto. Repasa los contenidos vistos en la unidad.

## Solución

1. Incorrecto
2. Opción correcta
3. Incorrecto
4. Incorrecto

# Condiciones y términos de uso de los materiales

Materiales desarrollados inicialmente por el Ministerio de Educación, Cultura y Deporte y actualizados por el profesorado de la Junta de Andalucía bajo licencia Creative Commons BY-NC-SA.

Antes de cualquier uso leer detenidamente el siguiente [Aviso legal](#)

## Historial de actualizaciones

Versión: 01.00.01	Fecha de actualización: 03/11/21
Actualización de materiales y correcciones menores.	
Versión: 01.00.00	Fecha de actualización: 23/07/20
Versión inicial de los materiales.	

