

**MP0483.  
Sistemas informáticos**

**UF4. Configuración de  
sistemas operativos**

## **4.2. Administración de la seguridad**

# Índice

---

≡	Objetivos	3
≡	Seguridad de las cuentas	4
≡	Herramientas de seguridad	5
≡	Buenas prácticas de seguridad	7
≡	Control de acceso	9
≡	Política de contraseñas	10
≡	Ejemplo de cambio de contraseña	12
≡	Habilitar y deshabilitar cuentas de usuario	14
≡	Ejemplo: activar o desactivar cuentas en Windows 10	19
≡	Algoritmos para contraseñas seguras	21
≡	Opciones de contraseña	23
≡	Cómo saber si mi contraseña es segura	28
≡	Resumen	29

# Objetivos

---

Organizar la seguridad de las cuentas de usuario es una misión principal para un administrador del sistema. La seguridad de la cuenta tiene que ver, tanto con asegurar que el acceso al sistema del usuario se realiza asegurando su identidad (normalmente a través de algún sistema de autenticación), como también con sus privilegios de ejecución y los grupos a los que pertenece el usuario.

En esta unidad perseguimos los siguientes objetivos:

1

Conocer los conceptos básicos para que los usuarios puedan utilizar el sistema de forma segura.

2

Aprender cómo habilitar y deshabilitar cuentas de usuario y cómo gestionar la utilización de sus contraseñas de cuenta.

3

Conocer las condiciones que debe cumplir una contraseña para ser eficaz y segura.

---

¡Ánimo y adelante!

# Seguridad de las cuentas

---

A la hora de hablar de seguridad conviene recordar que la seguridad puede aplicarse a:

- 1 **El sistema operativo.** Seguridad intrínseca del propio sistema operativo que estemos utilizando: Windows, Linux, Mac OS X, etc.
- 2 **Las aplicaciones y servicios.** La seguridad de los programas y procesos ejecutados en la máquina (aplicaciones ofimáticas, servidores, gestores de correo electrónico y cualquier otro).
- 3 **Las redes.** Seguridad de los datos transmitidos a través de las redes de comunicaciones a las que estemos conectados y también la seguridad de todos los dispositivos que conforman la red: *routers*, *firewalls*, etc.
- 4 **Los datos.** Se trata de asegurar una adecuada protección de los datos del sistema (sistema de ficheros, datos de funcionamiento del propio S.O., etc.).
- 5 **Seguridad física.** A menudo nos olvidamos de ella, pero aunque no entra en el alcance de este capítulo es importante tenerla en mente. Por mucha seguridad que implementemos por SW, si los equipos son sensibles a caídas u otros agentes, podemos obtener desastres como resultado.

# Herramientas de seguridad

---

---

Existe una gran variedad de herramientas de seguridad que nos ayudan a garantizar que los usuarios pueden trabajar adecuadamente sobre el sistema, esto es, **"que pueden hacer lo que necesitan hacer y no hacen lo que no deben hacer"**.

---

Algunas de estas herramientas de seguridad pueden ser, por ejemplo:

## **Cortafuegos ("firewalls")**

Dispositivos de control y filtrado del tráfico que se colocan entre la red y el exterior.

## **Verificadores de integridad**

Programas que realizan una imagen del sistema o de un conjunto de datos, y que puede ser empleada en otro momento para comprobar si se han producido cambios sobre ella.

## **Analizadores de históricos ("logs")**

Facilitan el análisis de los **registros de acceso y actividad del sistema** en busca de actividad inusual. Algunos son capaces de generar alarmas si se producen determinados errores o eventos.

## **Sistemas de detección de intrusos (IDS - "Intrusión Detection Systems")**

Verifican los datos que circulan por la red para detectar posibles ataques, y si se producen generan una alarma y/o bloquean al atacante.

### **Analizadores de puertos**

Nos dicen los puertos que el sistema tiene abiertos, de forma que podemos detectar posibles riesgos y cerrar aquellos que no deban estar abiertos.

### **Analizadores de vulnerabilidades**

Herramientas que realizan comprobaciones automáticas sobre el sistema, detectando vulnerabilidades. Algunas pueden corregir ciertos fallos de seguridad.

### **Analizadores de tráfico (“sniffers”)**

Capturan todo el tráfico de un segmento de red y permiten analizarlo. Algunos también son empleados para detectar contraseñas o robar datos que no estén siendo transmitidos encriptados.

## **El principio del mínimo privilegio**

En general, las medidas de seguridad aplicadas a la configuración de las cuentas de usuario deben seguir el "**principio del mínimo privilegio**", que dice que:

---

Los usuarios, sus aplicaciones y los servicios a los que acceden no deben disponer de permisos y privilegios más allá de los necesarios para realizar eficientemente su trabajo.

Es decir, un usuario “normal” no necesitará pertenecer a un grupo de administración, ni poder supervisar los estados de un servidor o cualquier otro dispositivo no asignado a él, ni poder controlar colas de impresión o priorización de trabajos, ni tener permiso de lectura sobre directorios que no le sea necesario ver, etc.

# Buenas prácticas de seguridad

---

---

Aunque pueden variar según el S.O. y están sujetas al criterio del administrador, es importante tener en cuenta algunas prácticas determinadas, sobre todo en el caso de equipos servidores.

---

Algunas de estas **buenas prácticas** pueden ser:

- **Cambiar el nombre de la cuenta “admin”** (administrador), no dejarla con el nombre por defecto.
- **Crear una cuenta falsa de administración** para combatir intentos de acceso malintencionados.
- **Deshabilitar el usuario “invitado” (“guest”)** o al menos poner una contraseña compleja y limitar el número de accesos/día.
- **Limitar el número de cuentas en el equipo/servidor** y eliminar cualquier usuario innecesario.
- **Limitar los accesos de la cuenta de administración**, no usarla para actividades que no requieran los máximo privilegios.
- **Revisar los privilegios por defecto de los grupos de usuarios** para evitar que los asignados por defecto entrañen riesgos.
- **Elegir un sistema de ficheros más seguro (NTFS)**. Los sistemas FAT y FAT32 tienen menores niveles de seguridad.

- **Desactivar los servicios innecesarios en el equipo/servidor.** Algunos vienen activados por defecto y entrañan riesgos.
- **Cerrar los puertos que no estén siendo utilizados** y limitar los protocolos (TCP, UDP, ICMP, etc.) a los esenciales.
- **Habilitar la auditoría en el equipo/servidor** creando alertas sobre eventos como accesos de usuario, uso de privilegios, etc.
- **Proteger los archivos de registro de eventos.** Por omisión no suelen estarlo y deben restringirse a los administradores.
- **Desactivar la opción de mostrar “ultimo usuario” en la pantalla de inicio** para dificultar que se conozca el nombre del usuario administrador.
- **Mantener la actualización del sistema y sus parches de seguridad.** Tratar las actualizaciones de forma sistemática.
- **Desactivar las carpetas compartidas no necesarias** limitando el acceso de los usuarios solamente a las que necesitan.
- **Desactivar la opción de creación de un archivo “dump”** o limitar el acceso solamente a los administradores. Un archivo "dump" o "archivo de volcado de memoria" se crea cuando se produce algún evento crítico y almacena información de depuración para tratar luego el problema.
- **Configurar las políticas de seguridad en el equipo y en la organización** de forma que sean coherentes y lógicas.



# Control de acceso

---

---

La primera medida de seguridad que suele implementarse en todos los sistemas es el “control de acceso/autenticación” de los usuarios que quieren operar sobre el equipo.

El control de acceso incluye todo el conjunto de medidas tomadas para controlar la operación de los usuarios sobre el sistema, desde su inicio de sesión hasta su acceso a los directorios y recursos del sistema durante su operación.

Lo usual es que este control se lleve a cabo **estableciendo un sistema de permisos asociado a los usuarios y a los grupos**, de forma que si un usuario no tiene el permiso para realizar una acción, el sistema no le permitirá realizarla.

El primer mecanismo de control de acceso suele ser la necesidad de introducir una **contraseña** para poder “entrar” (acceder) al sistema. No es el único medio, y en los modernos sistemas también podemos encontrar mecanismos de control de acceso basados en:

- **Certificados digitales**, mecanismos de criptografía de seguridad por clave pública.
- Control de acceso mediante el uso de una **tarjeta física de acceso**.
- Control mediante **seguridad biométrica**, por ejemplo la huella digital o incluso un escáner de retina.

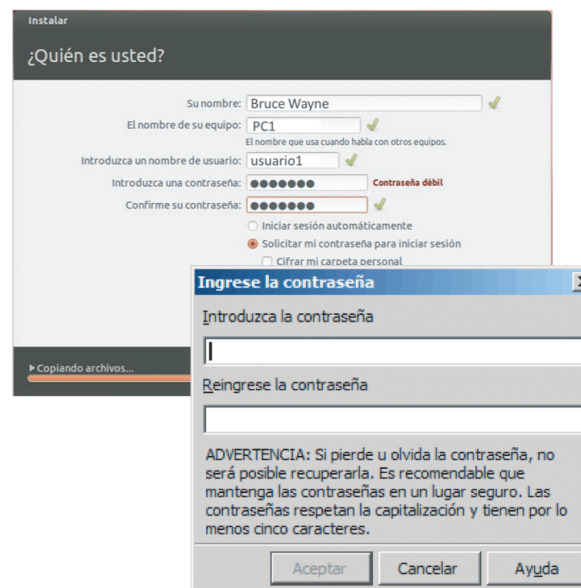
## Política de contraseñas

---

Lo más común y usual es la medida de seguridad más simple: la necesidad de introducir una contraseña para acceder al sistema.

La clave de acceso puede ser establecida por el administrador del sistema y luego permitirle al usuario cambiarla o no, incluso obligarle a cambiarla en el primer acceso, etc., y se pueden establecer normas de cómo debe ser el formato de la contraseña para aumentar la seguridad del sistema.

La forma en la que se gestionan en general las contraseñas de los sistemas es lo que se suele llamar **“política de contraseñas”**, y contiene el **conjunto de normas** por las que se rigen tanto los usuarios como los administradores para establecer y utilizar las contraseñas de acceso al sistema.



## Ejemplo de política de contraseñas

- Todas las contraseñas de sistema (*root*, cuentas de administración, aplicaciones, etc.) deben ser cambiadas al menos una vez cada seis meses.
- Las contraseñas de usuario (cuentas de sistema, e-mail, servicios web, etc.) deben ser cambiadas al menos una vez cada doce meses, pero se recomienda cambiarlas con mayor frecuencia y siempre que se sospeche que la seguridad de la contraseña actual pueda estar en duda.
- Las cuentas de usuario con privilegios de sistema (por pertenecer a grupos, por ejemplo) tendrán contraseñas distintas de las del resto de cuentas de ese usuario.
- Nunca se deben incluir las contraseñas en mensajes de correo electrónico o de otro tipo, ni ser compartidas en conversaciones telefónicas.
- Las contraseñas se generarán por primera vez de forma automática con el formato recomendado, y se comunicarán a los usuarios siempre en estado “expirado”, para obligar al usuario a cambiarla en el primer acceso que hagan a su cuenta.
- Las contraseñas por defecto asociadas a nuevos sistemas o aplicaciones deberán cambiarse obligatoriamente antes de que los sistemas se ofrezcan a los usuarios.
- Se desactivarán todas aquellas cuentas establecidas de forma predeterminada o “por defecto” que no sean imprescindibles.

## Ejemplo de cambio de contraseña

---

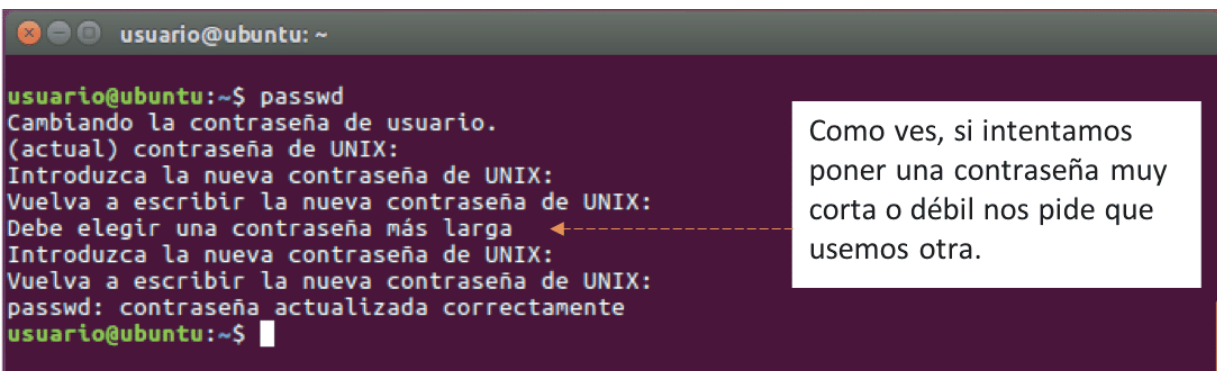
Cambiar nuestra contraseña es algo que siempre debemos saber hacer, y es una práctica recomendable, no sólo para cumplir con las indicaciones del administrador, sino por nuestra propia comodidad y seguridad.

### Cambiar nuestra contraseña en Windows 10

El proceso es extremadamente sencillo. Te lo mostramos en [el siguiente vídeo](#).

### Cambiar la contraseña en Ubuntu

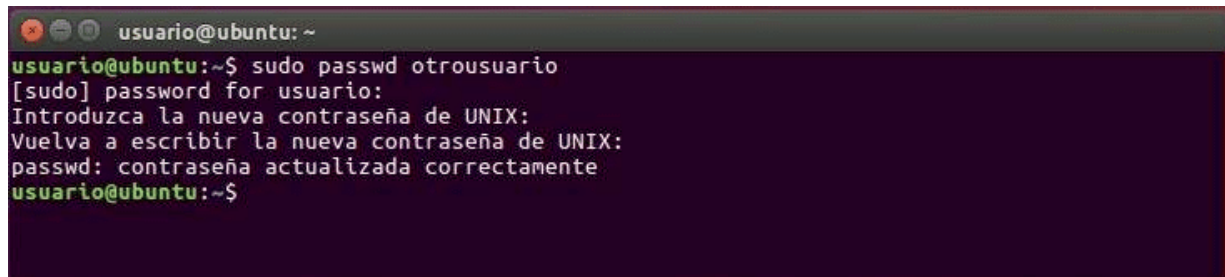
Si estamos trabajando con Ubuntu, el proceso de **cambiar nuestra contraseña** también es fácil. Basta ejecutar desde un terminal el comando "`passwd`". Por ejemplo:



```
usuario@ubuntu: ~  
usuario@ubuntu:~$ passwd  
Cambiando la contraseña de usuario.  
(actual) contraseña de UNIX:  
Introduzca la nueva contraseña de UNIX:  
Vuelva a escribir la nueva contraseña de UNIX:  
Debe elegir una contraseña más larga  
Introduzca la nueva contraseña de UNIX:  
Vuelva a escribir la nueva contraseña de UNIX:  
passwd: contraseña actualizada correctamente  
usuario@ubuntu:~$
```

Como ves, si intentamos poner una contraseña muy corta o débil nos pide que usemos otra.

De igual forma, si tenemos privilegios de administrador, podemos usar el mismo comando para cambiar la contraseña de otro usuario. Veámoslo:

A terminal window with a dark purple background and light green text. The window title is 'usuario@ubuntu: ~'. The user enters the command 'sudo passwd otrousuario'. The prompt changes to '[sudo] password for usuario:'. The user enters a password (not visible). The prompt changes to 'Introduzca la nueva contraseña de UNIX:'. The user enters the password again (not visible). The prompt changes to 'Vuelva a escribir la nueva contraseña de UNIX:'. The user enters the password a third time (not visible). The prompt changes to 'passwd: contraseña actualizada correctamente'. The user enters the command 'usuario@ubuntu:~\$' and the prompt returns to 'usuario@ubuntu:~\$'.

```
usuario@ubuntu: ~
usuario@ubuntu:~$ sudo passwd otrousuario
[sudo] password for usuario:
Introduzca la nueva contraseña de UNIX:
Vuelva a escribir la nueva contraseña de UNIX:
passwd: contraseña actualizada correctamente
usuario@ubuntu:~$
```

---

También puedes realizar esta operación a través del entorno gráfico, pero es interesante que aprendas a utilizar los comandos.

# Habilitar y deshabilitar cuentas de usuario

---

---

Entendemos por deshabilitar (o desactivar) una cuenta, a dejarla inaccesible para el usuario y, en general, impedir que desde ella se puedan realizar acciones sobre el sistema.

En algunos casos la cuenta deshabilitada no deja ni siquiera acceder al usuario. En otros puede mostrarle un mensaje de advertencia y permitirle un servicio limitado (por ejemplo, sólo la visualización de ciertos datos).

La **habilitación o activación** es lo contrario, es decir, **poner la cuenta en servicio**.

Normalmente la cuenta puede quedar habilitada de forma predeterminada después de su creación, o al revés, crearse en un estado de desactivación y requerir la acción de “habilitar la cuenta”.

Tanto la activación y desactivación de las cuentas de usuarios siempre podrán hacerse de forma manual por parte del administrador, pero es posible que éste desee establecer reglas para controlar el buen uso de las cuentas y detectar acciones peligrosas, de forma que se pueda bloquear automáticamente la cuenta en la que se realizan.

El ejemplo más conocido es **limitar el número de intentos de acceso**, de forma que si en una cuenta se introduce la clave de entrada de forma errónea más de un número consecutivo de veces, la cuenta se bloquea automáticamente y para habilitarla de nuevo es necesaria normalmente la acción del administrador (también puede reactivarse de forma automática pasado un tiempo).



La inhabilitación de una cuenta de usuario no siempre es debida a una mala práctica. Por ejemplo, si un empleado abandona la compañía puede ser aconsejable conservar su cuenta pero inhabilitarla en el sistema.

Veamos un par de ejemplos en Linux:

#### DESHABILITAR EN UNA FECHA

Si la habilitación/deshabilitación la realiza el administrador de forma manual, podrá hacerla a través de la línea de comandos o también a través de la interfaz gráfica si el sistema dispone de esa facilidad.

En el caso de Linux, por ejemplo, un comando a usar es “*usermod*”, con el que podemos asignar a una cuenta de usuario una fecha de vencimiento (si esa fecha es pasada la cuenta quedará desactivada). Por ejemplo:

***usermod -e 2017-01-01 nombreusuario***

Lo cual provocará que la próxima vez que el usuario intente acceder se le muestre un mensaje tipo:

***“Your account has expired please contact your system administrator”***

Evidentemente también podemos bloquear la cuenta de forma inmediata con el mismo comando:

***usermod -L nombreusuario***

Y para desbloquearla:

***usermod -U nombreusuario***

```

usuario@ubuntu:~$ sudo chage -l otrousuario
Último cambio de contraseña           : nunca
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 contraseña : 99999
Número de días de aviso antes de que caduque la contraseña : 7
usuario@ubuntu:~$ sudo usermod -e 2018-05-01 otrousuario
usuario@ubuntu:~$ sudo chage -l otrousuario
Último cambio de contraseña           : abr 02, 2018
La contraseña caduca                    : nunca
Contraseña inactiva                     : nunca
La cuenta caduca                        : may 01, 2018
Número de días mínimo entre cambio de contraseña : 0
Número de días máximo entre cambio de contraseña : 99999
Número de días de aviso antes de que caduque la contraseña : 7
usuario@ubuntu:~$

usuario@ubuntu:~$ sudo usermod -L otrousuario
usuario@ubuntu:~$ sudo grep -E --color 'otrouusuario:!' /etc/shadow
otrouusuario:!!$6$ZKYfCbed$8Kyhr5QkV1vqrB56Aa5saA9kaIM598Y.LW9WzkbwLq1uRgpI7zd6khVs1SjPAPwauK9qYnB1LuHz91.k8YE78.:17623:0:99999:7::17652:
usuario@ubuntu:~$ sudo usermod -U otrousuario
usuario@ubuntu:~$ sudo grep -E --color 'otrouusuario:!' /etc/shadow
otrouusuario:$6$ZKYfCbed$8Kyhr5QkV1vqrB56Aa5saA9kaIM598Y.LW9WzkbwLq1uRgpI7zd6khVs1SjPAPwauK9qYnB1LuHz91.k8YE78.:17623:0:99999:7::17652:
usuario@ubuntu:~$
usuario@ubuntu:~$
usuario@ubuntu:~$

```

Con el comando **chage** podemos ver el estado de caducidad de la cuenta y contraseña de un usuario.

Y con **usermod** le ponemos una fecha de expiración a la cuenta.

Si queremos bloquear una cuenta, podemos hacerlo con el comando **usermod** y la opción **-L**.

Las cuentas que están bloqueadas tienen un "!" delante de su clave encriptada en el fichero **/etc/shadow**.  
Con estos comandos visualizamos la línea en el fichero **/etc/shadow** correspondiente al usuario "otrouusuario".

## DESHABILITAR CUENTAS FICTICIAS

En el caso de que en el sistema tengamos dadas de alta **cuentas de usuario ficticias**, como una falsa cuenta de administrador, por ejemplo, para atraer hacia ella posibles ataques de intrusos, **estas cuentas deben estar deshabilitadas**, para de esa forma evitar cualquier posible entrada u operación.

En este caso, en vez de ponerles una fecha de vencimiento, resulta mejor bloquear su clave de acceso asignándole en el intérprete de comandos **"/sbin/nologin"** o **"/sbin/false"** (más restrictivo, pues cierra la entrada por consola, SSH y FTP, aunque no muestra mensaje de respuesta como la otra opción).

```

usuario@ubuntu:~$ sudo grep -E --color 'administrador' /etc/shadow
administrador:$6$J0UKvb.a0kXl0mrs$FPR9L/zsN95AXpLW7VwnuESLAXPB8YvWYstMj0oRxTELAsFdGHEHJCJKp4L3jR.fX0kxN/9c7LRxdflC05WtJ0:17623:0:99999:7:::
usuario@ubuntu:~$ sudo usermod -L administrador
usuario@ubuntu:~$ sudo grep -E --color 'administrador' /etc/shadow
administrador:!!$6$J0UKvb.a0kXl0mrs$FPR9L/zsN95AXpLW7VwnuESLAXPB8YvWYstMj0oRxTELAsFdGHEHJCJKp4L3jR.fX0kxN/9c7LRxdflC05WtJ0:17623:0:99999:7:::
usuario@ubuntu:~$
usuario@ubuntu:~$ sudo usermod -s /sbin/nologin administrador
usuario@ubuntu:~$

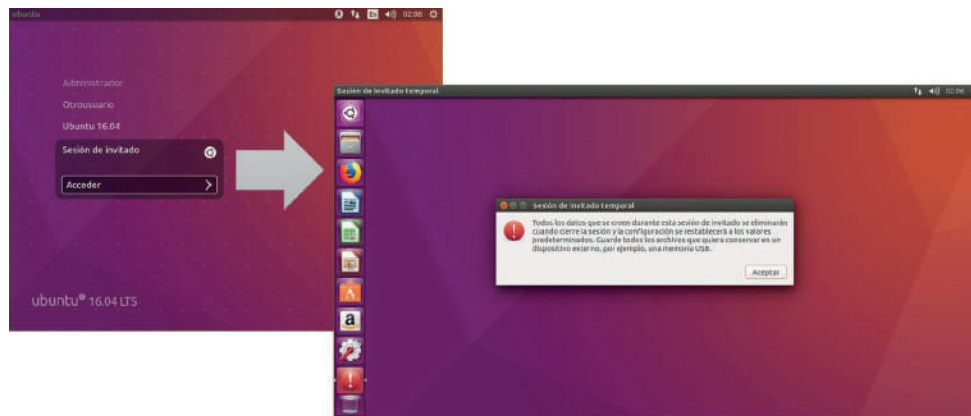
```

En este ejemplo, primero bloqueamos la cuenta ficticia "administrador" y además le asignamos como Shell "nologin" para mayor seguridad.



## Ejemplo: la cuenta de invitado en Linux Ubuntu

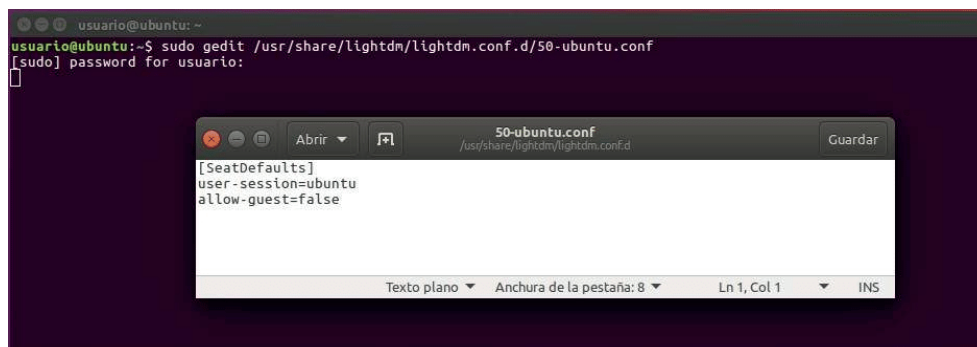
En muchos sistemas operativos, y entre ellos en Linux, se puede tener una cuenta de "invitado" para que las personas que no tienen declarado un usuario en el sistema puedan abrir una sesión temporal y usar el ordenador. Esta cuenta, también conocida como "guest", es independiente de cualquier otra que hayamos creado con el nombre de "Invitado".

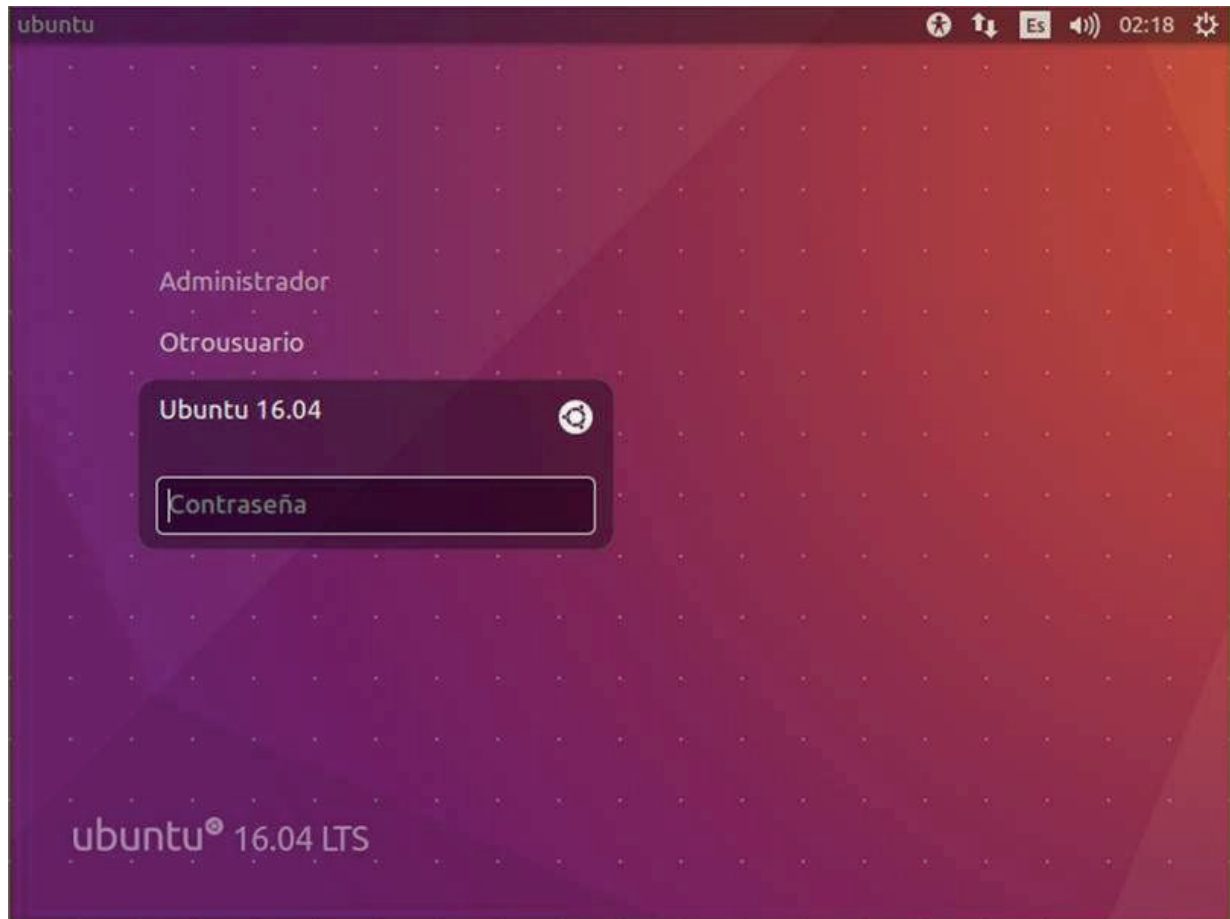


Sin embargo, una medida que se suele tomar por motivos de seguridad es la desactivación de la cuenta de "usuario invitado" ("guest") del sistema. Para desactivarla debemos modificar los archivos de configuración del S.O.

En nuestro caso, sobre Ubuntu 16.04, para **deshabilitar la cuenta de invitado** deberemos editar (con privilegios de administrador) el fichero "50-ubuntu.conf" del directorio "/usr/share/lightdm/lightdm.conf.d/", y añadir la línea "allow-guest=false".

Te lo mostramos en una imagen:





Una vez añadida la línea indicada y guardado el fichero, si reiniciamos el sistema ya no nos ofrecerá la opción de abrir sesión como usuario invitado, y deberemos conocer la clave de alguna de las cuentas activas para poder "entrar" al equipo.

# Ejemplo: activar o desactivar cuentas en Windows 10

Vamos a ver cómo podemos habilitar y deshabilitar cuentas de usuario desde nuestra cuenta de administrador.

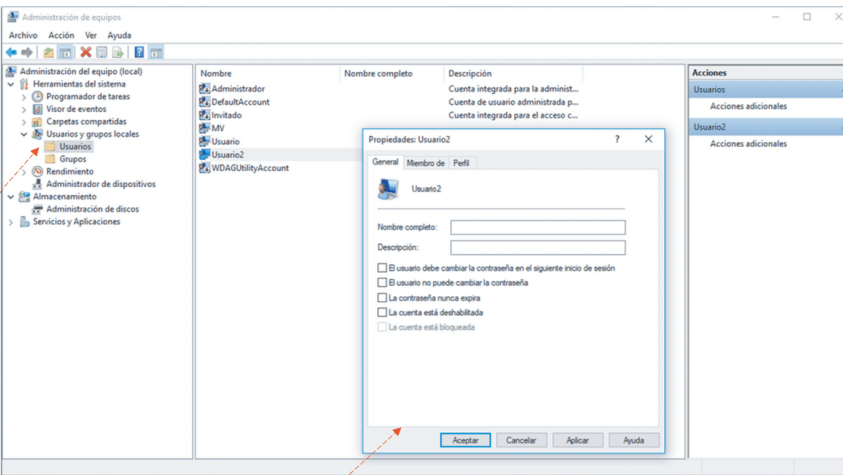
## Habilitar y deshabilitar cuentas en Windows 10

Controlar el estado de una cuenta desde el administrador es fácil, basta con ir a "Administración de equipos" y elegir la opción de gestión de los usuarios del sistema. Te lo mostramos en la siguiente imagen:

**Habilitar y deshabilitar una cuenta de usuario en Windows 10**

Para habilitar/deshabilitar una cuenta de usuario basta con abrir la ventana de "Administración de equipos", y dentro de ella seleccionar "Usuarios y grupos locales", luego pulsar en "Usuarios", y en el centro de la ventana elegir el usuario sobre el que queremos actuar.

- Haciendo doble click sobre el usuario no sale otra ventana donde podremos...
- Habilitar o deshabilitar la cuenta.
- Permitirle al usuario cambiar o no su contraseña.
- Hacer que el usuario tenga que cambiar la contraseña en el próximo inicio de sesión o que la contraseña nunca expire.



The screenshot shows the 'Administración de equipos' (Administrative Tools) window. On the left, the 'Usuarios' (Users) folder is selected under 'Administración del equipo (local)'. The main pane displays a list of users: Administrador, DefaultAccount, Invitado, Usuario, Usuario2, and WDAGUtilityAccount. The 'Propiedades: Usuario2' (Properties: Usuario2) window is open, showing the 'General' tab. It includes fields for 'Nombre completo' and 'Descripción', and several checkboxes: 'El usuario debe cambiar la contraseña en el siguiente inicio de sesión', 'El usuario no puede cambiar la contraseña', 'La contraseña nunca expira', 'La cuenta está deshabilitada', and 'La cuenta está bloqueada'. The 'Aceptar' (OK) button is highlighted with a red arrow.

En esta ventana también tenemos la opción de quitar el bloqueo de una cuenta, por ejemplo cuando se ha bloqueado por un número excesivo de intentos fallidos de introducción de la contraseña. En este caso, como la cuenta no está bloqueada, la opción no está activa.

Sin embargo, en la versión **Windows 10 Home**, el administrador de equipos no suele soportar la opción de gestión de usuarios, y aunque podemos crearlos a través de "Configuración", si queremos modificar sus detalles de cuenta debemos recurrir a la consola de comandos. Concretamente utilizar el comando "**NET User**", que tiene muchas opciones. Te lo mostraremos a través de un ejemplo:

Administrador: Símbolo del sistema

```
C:\WINDOWS\system32>net user
```

Nos muestra los usuarios que hay en el sistema.

Cuentas de usuario de \\AMD-ROJO

Administrador	DefaultAccount	Invitado
PC	Usuario2	WDAGUtilityAccount

Se ha completado el comando correctamente.

```
C:\WINDOWS\system32>net user angel Clave1234 /add /passwordreq:yes /fullname:"Angel Ito"
```

Se ha completado el comando correctamente.

```
C:\WINDOWS\system32>net user
```

Este comando crea el usuario "angel", le asigna la contraseña "Clave1234", configura que sea obligatorio introducirla, y lo relaciona en el sistema con su nombre completo "Angel Ito".

Administrador	angel	DefaultAccount
Invitado	PC	Usuario2

El usuario ha sido creado.

Se ha completado el comando correctamente.

C:\WINDOWS\system32>

Si nuestro interfaz gráfico no soporta la gestión de usuarios, podemos hacerlo con el comando "NET User". Es un comando con muchas opciones, que puedes ver tecleando "Net User /help", o una versión abreviada con "Net user help?".

Aquí te lo mostramos a través de ejemplos...

Administrador: Símbolo del sistema

```
C:\WINDOWS\system32>net user angel
```

También podemos visualizar todas las características del usuario.

Vemos que su cuenta ya está activa, que la contraseña es requerida para iniciar sesión, aunque aun no ha iniciado sesión porque acabamos de crearlo.

Nombre de usuario	Nombre completo	Comentario	Comentario del usuario	Código de país o región	Cuenta activa	La cuenta expira	Ultimo cambio de contraseña	La contraseña expira	Cambio de contraseña	Contraseña requerida	El usuario puede cambiar la contraseña	Estaciones de trabajo autorizadas	Script de inicio de sesión	Perfil de usuario	Directorio principal	Ultima sesión iniciada	Horas de inicio de sesión autorizadas	Miembros del grupo local	Miembros del grupo global
angel	Angel Ito			000 (Predeterminado por el equipo)	Sí	Nunca	29/03/2018 21:51:04	10/05/2018 21:51:04	29/03/2018 21:51:04	Sí	Sí	Todas			Nunca		Todas	*Usuarios	*Ninguno

Se ha completado el comando correctamente.

C:\WINDOWS\system32>

Administrador: Símbolo del sistema

```
C:\WINDOWS\system32>net user angel /active:no
```

Y con el mismo comando y la opción "/active:no" procedemos a deshabilitar la cuenta.

Si la visualizamos de nuevo lo comprobamos.

```
C:\WINDOWS\system32>net user angel
```

Nombre de usuario	Nombre completo	Comentario	Comentario del usuario	Código de país o región	Cuenta activa	La cuenta expira	Ultimo cambio de contraseña	La contraseña expira	Cambio de contraseña	Contraseña requerida	El usuario puede cambiar la contraseña	Estaciones de trabajo autorizadas	Script de inicio de sesión	Perfil de usuario	Directorio principal	Ultima sesión iniciada	Horas de inicio de sesión autorizadas	Miembros del grupo local	Miembros del grupo global
angel	Angel Ito			000 (Predeterminado por el equipo)	No	Nunca	29/03/2018 21:51:04	10/05/2018 21:51:04	29/03/2018 21:51:04	Sí	Sí	Todas			Nunca		Todas	*Usuarios	*Ninguno

Se ha completado el comando correctamente.

C:\WINDOWS\system32>

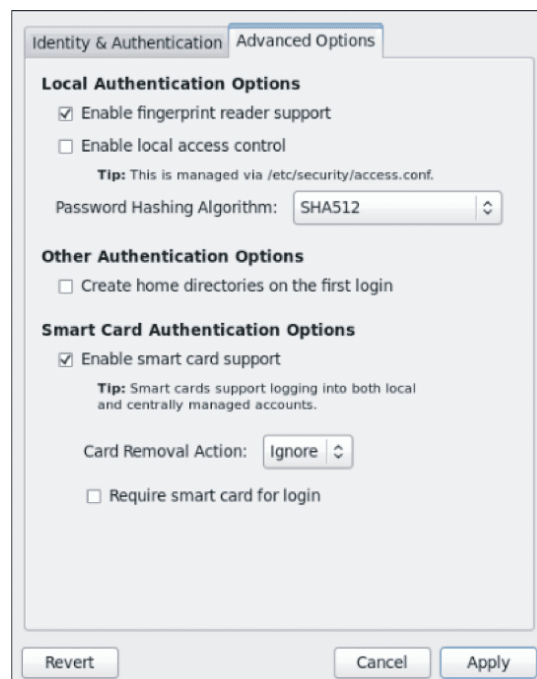
# Algoritmos para contraseñas seguras

Normalmente las claves de acceso se codifican con “algoritmos de sentido único”.

Esto quiere decir que **no pueden descodificarse directamente**, de forma que cuando un usuario introduce su contraseña, esta se codifica y se compara con la clave válida encriptada, y si es correcta se le permite la conexión.

Los sistemas modernos utilizan algoritmos de codificación muy potentes, como **MD5** o **SHA**, que permiten claves extensas y difíciles de averiguar. El algoritmo **MD5** usa claves de 128 bits, mientras que **SHA512** llega hasta los 512 bits.

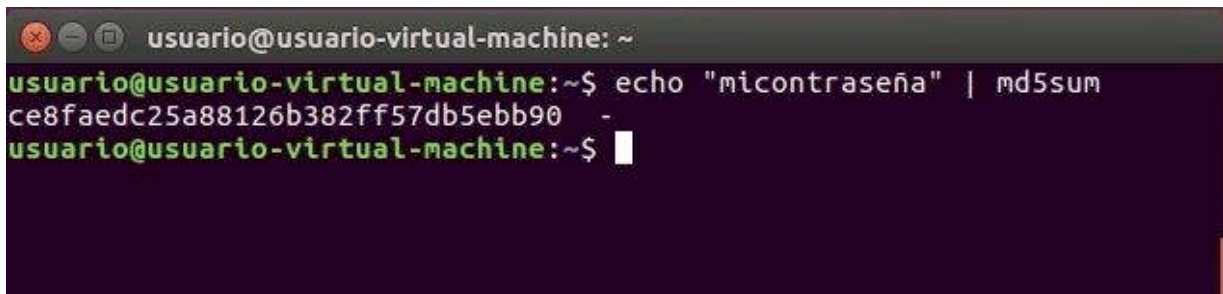
Por ejemplo, en el sistema Oracle Solaris las contraseñas de usuario se cifran de forma predeterminada con el algoritmo Crypt\_SHA256, pero el administrador puede cambiar este algoritmo y elegir otros de entre una serie de opciones: MD5, Blowfish, SHA256, SHA512, etc.



## Un ejemplo de codificación de contraseñas

Estas funciones de codificación que utilizan algoritmos de sentido único toman como entrada un conjunto de datos (que puede ser el contenido de un fichero por ejemplo, o en nuestro caso una contraseña) y haciendo una serie de operaciones matemáticas producen una salida alfanumérica de longitud fija, que se puede usar para comprobar los datos originales (porque cualquier variación en ellos produce un resultado diferente al hacer las operaciones).

Veamos un ejemplo sencillo y que puedes realizar en la mayoría de los sistemas Linux (y por supuesto en tu máquina virtual de Ubuntu). Imaginemos que tenemos una clave de entrada que es "micontraseña" y vamos a codificarla empleando un algoritmo **md5**. Para hacerlo introduciremos el comando de la imagen:



```
usuario@usuario-virtual-machine: ~  
usuario@usuario-virtual-machine:~$ echo "micontraseña" | md5sum  
ce8faedc25a88126b382ff57db5ebb90 -  
usuario@usuario-virtual-machine:~$
```

Como ves, lo que hacemos es utilizar la salida de otro comando (*echo "micontraseña"*) y decirle con `"|"` que la utilice como entrada del siguiente comando (*md5sum*), que calcula el **md5** de "micontraseña" (sin las comillas) y genera el código de 128 bits que ves en la figura anterior.

Si nuestro S.O. utilizase el algoritmo md5 para codificar las contraseñas de usuario, lo que haría sería **guardar en el sistema este resultado cifrado (con 128 bits) y cada vez que el usuario introduzca su contraseña volver a calcular el md5 y comparar el resultado**, y si coincide es que ha introducido la contraseña correctamente.

## Opciones de contraseña

---

El administrador puede indicar a los usuarios ciertas normas (en su política de seguridad) a la hora de establecer las contraseñas de acceso.

Algunas de ellas podrán ser **reglas verificadas por el propio sistema** a la hora de admitir la introducción de una nueva clave. Por ejemplo, la longitud o la necesidad de contener ciertos caracteres. Otras tendrán que ser **recomendaciones de buenas prácticas**, por ejemplo, para que sean difíciles de averiguar por terceras personas o programas de descifrado.

Algunas de las recomendaciones más habituales son:

- No usar palabras comunes (ciudades, direcciones) o números asociados a la persona (fechas de cumpleaños, etc.).
- No reutilizar las mismas contraseñas en distintos sistemas.
- Usar claves de “n” caracteres como mínimo (p. ej. mínimo 8) y que deban tener caracteres no alfabéticos (por ejemplo <>&%\$()=?¿) y combinar mayúsculas y minúsculas.
- No usar secuencias de teclado.
- Cambiar la contraseña periódicamente (controlado por el sistema) y no reutilizar claves anteriores.
- No anotar la contraseña y por supuesto no dejarla a la vista (el típico “*post-it*” amarillo pegado en la pantalla).
- No compartir la contraseña con otras personas.

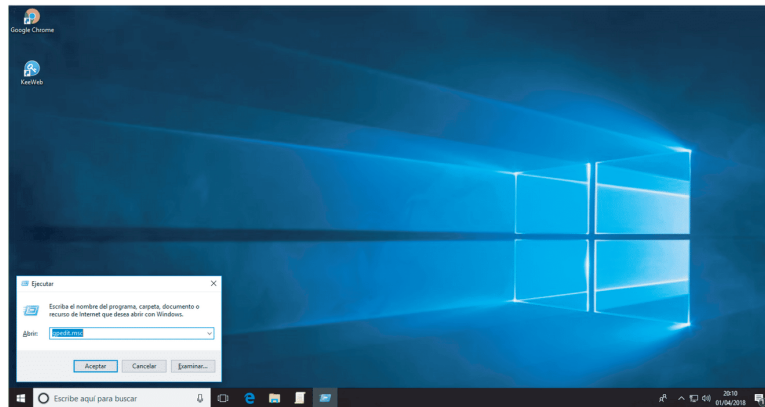


## Cómo establecer requisitos de contraseña en Windows 10

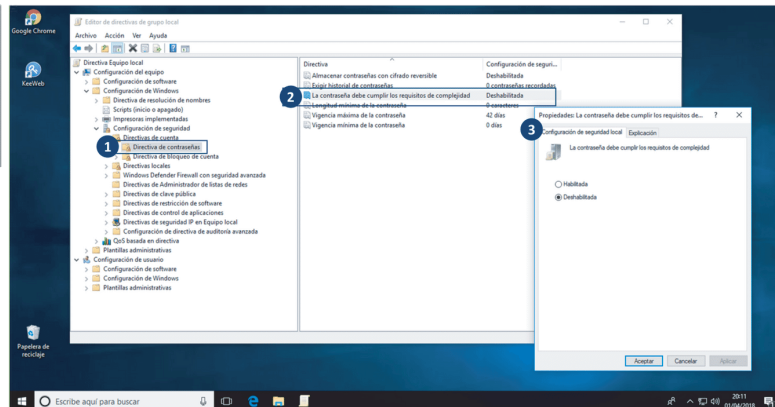
En este punto, ésto puede depender de la versión de Windows 10 que tengamos en nuestro equipo. Si nuestra versión lo contempla (p. ej. versión Windows 10 PRO o Enterprise) podemos acceder a modificar la directiva de contraseñas, por ejemplo, ejecutando "**gpedit.msc**" para editar las directivas de seguridad locales (más adelante volveremos sobre lo que es una directiva y para que sirven), y dentro de la opción "directiva de contraseñas" primero habilitar que la contraseña cumpla con requisitos de seguridad y luego programar el resto de opciones. Te lo mostramos en las imágenes siguientes.

### Directiva de contraseña en Windows

Con el botón derecho sobre el símbolo de Windows accedemos a la opción de "ejecutar" y ahí introducimos "gpedit.msc".

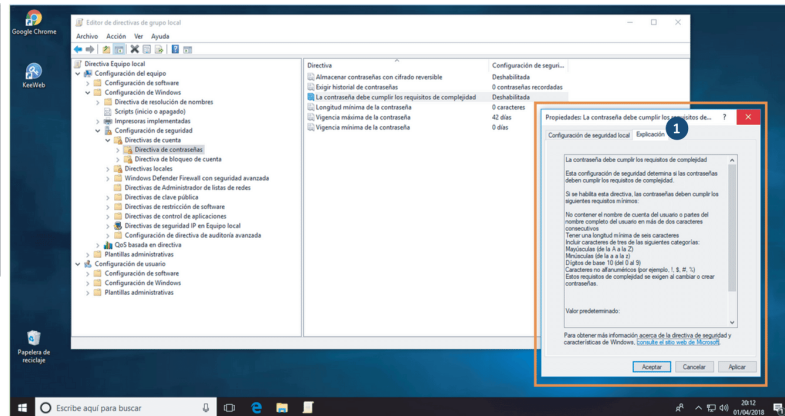


Elegimos la opción "Directiva de contraseñas", y dentro de ella podemos hacer que la contraseña tenga que cumplir requisitos especiales y luego fijar además otras condiciones.





Si en la ventana de requisitos de contraseña elegimos la pestaña de "Explicación" podemos obtener una lista de cuales son los requisitos que a partir de ese momento se pedirán a las contraseñas que se vayan a asignar a los usuarios (podemos comprobarlo creando un usuario nuevo y viendo que nos solicita estas condiciones).



También resulta muy útil, de cara a aumentar la seguridad, limitar el **número de intentos fallidos en que los se puede introducir una contraseña**. Para ello podemos ir a la "directiva de bloqueo de cuenta" y establecer un comportamiento en caso de que se realicen varios intentos fallidos de iniciar sesión ("hacer login") en el sistema, y que se tenga que esperar cierto tiempo antes de volver a intentarlo.

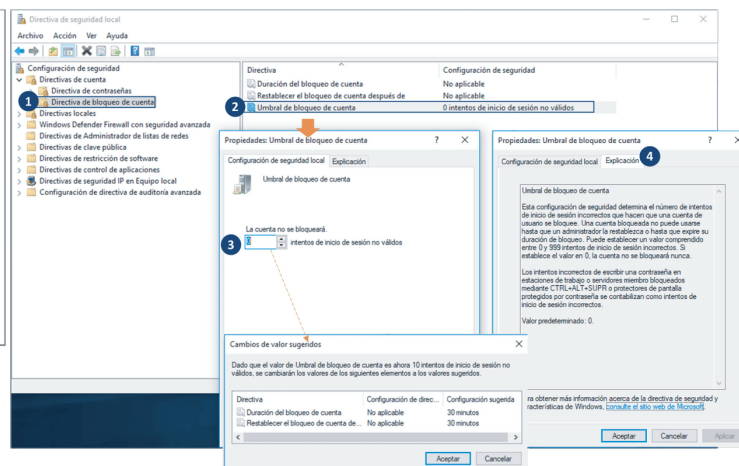
Para acceder a la directiva de cuenta podemos usar el editor "*gpedit.msc*" que acabamos de ver o también introducir en el cuadro de diálogo de Windows "directiva de seguridad local" y nos aparece la ventana que te mostramos:

**Umbral de bloqueo de cuenta en Windows 10 PRO o Enterprise**

En la ventana de configuración de la seguridad local del sistema podemos establecer una directiva de bloqueo de la cuenta si se realizan varios intentos fallidos de "login".

Si lo activamos podremos configurar también durante cuánto tiempo se bloquea la cuenta, o el periodo de tiempo para poner a cero el "contador de intentos fallidos".

En cada una de las ventanas de cada opción puedes ver una pestaña de "explicación" que te dice lo que significa y cómo usarla.



## ¿Y qué pasa si estoy en Windows 10 Home?

Bueno, la versión "doméstica" de Windows 10 nos ofrece menos posibilidades, pero si investigas un poco verás que hay ciertos trucos que a veces cuesta encontrar en la información pero que podemos probar. En este caso te sugerimos que pruebes con el comando "net accounts" dentro de una ventana de consola como administrador. Míralo:

```
C:\WINDOWS\system32\net accounts
Tiempo antes del cierre forzado:
Duración mín. de contraseña (días):
Duración máx. de contraseña (días):
Longitud mínima de contraseña:
Duración del historial de contraseñas:
Umbral de bloqueo:
Duración de bloqueo (minutos):
Ventana de obs. de bloqueo (minutos):
Rol del servidor:
Se ha completado el comando correctamente.

Nunca
0
42
0
Ninguna
Nunca
30
30
ESTACION DE TRABAJO

C:\WINDOWS\system32\net accounts /lockoutthreshold:7
Se ha completado el comando correctamente.

C:\WINDOWS\system32\net accounts /lockoutduration:45
Se ha completado el comando correctamente.

C:\WINDOWS\system32\net accounts /lockoutwindow:15
Se ha completado el comando correctamente.

C:\WINDOWS\system32\net accounts
Tiempo antes del cierre forzado:
Duración mín. de contraseña (días):
Duración máx. de contraseña (días):
Longitud mínima de contraseña:
Duración del historial de contraseñas:
Umbral de bloqueo:
Duración de bloqueo (minutos):
Ventana de obs. de bloqueo (minutos):
Rol del servidor:
Se ha completado el comando correctamente.

Nunca
0
42
0
Ninguna
7
45
15
ESTACION DE TRABAJO

C:\WINDOWS\system32>
```

En principio, parece que Windows 10 HOME no admite la gestión de directivas de contraseña ni bloqueo de cuentas, al no ofrecernos la opción de abrir la ventana de gestión en el entorno gráfico...

Sin embargo, si ejecutamos al consola de comandos (en modo administrador) puedes ver con el comando "NET ACCOUNTS" que si aparecen los datos en el sistema, y que nos deja modificarlos con las opciones adecuadas.

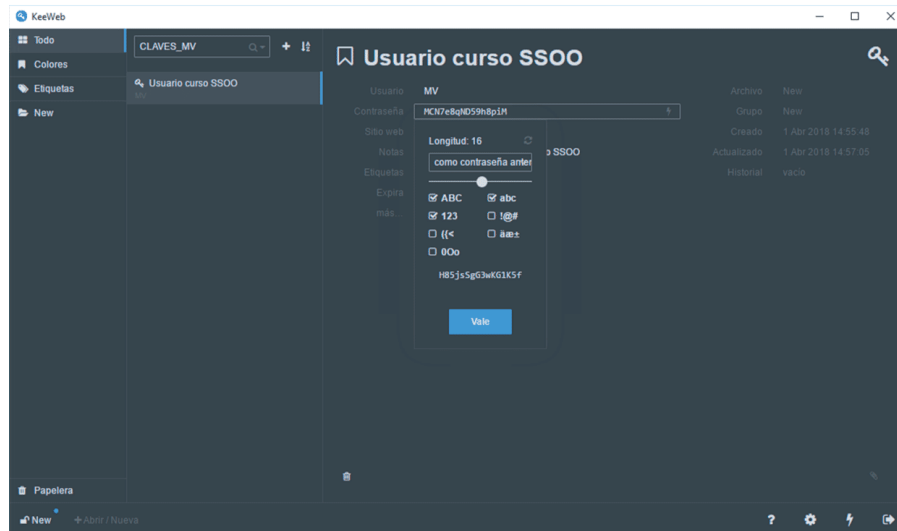
Te mostramos un ejemplo de cómo visualizamos el estado de estos parámetros antes de introducir el comando y después, en un entorno Windows 10 HOME.

## Aplicaciones de terceros para gestión de contraseñas

Uno de los problemas que a menudo nos surgen es generar y recordar las múltiples contraseñas de acceso a los diferentes servicios, páginas web, aplicaciones, etc. Puede resultar útil usar una aplicación que nos ayude a gestionar nuestras contraseñas, desde generar contraseñas seguras para utilizarlas, a guardarlas localmente o en la nube de forma segura para nosotros.

Existen múltiples aplicaciones para realizar estas funciones. Puede estar bien que les eches un vistazo y, aprovechando que tienes unas estupendas máquinas virtuales, pruebes a instalar alguna y ver si te interesa utilizarlas en tu trabajo diario.

Un ejemplo puede ser "Keeweb". Su manejo es sencillo, y si la instalas puedes ver que tiene diferentes opciones para generar contraseñas de varias longitudes.



Keeweb – <https://github.com/keeweb/keeweb/releases>.



Para que trabajes un poco sobre cómo elegir y gestionar contraseñas seguras te proponemos que profundices a través de los siguientes enlaces:

**Aprende a gestionar tus contraseñas - OSI**

<https://www.osi.es/es/contrasenas>

**Documento sobre contraseñas en la PYME de Incibe**

<https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/contrasenas.doc>

## Cómo saber si mi contraseña es segura

Lo ideal es que como administradores del sistema seamos nosotros los que fijemos las condiciones que deben cumplir las claves de los usuarios, de forma que cumpliendo la política de contraseñas sabemos que estamos usando claves adecuadas.

Por otro lado, si usamos alguna aplicación de gestión o generación de contraseñas, estas ya están preparadas con las principales opciones para generar claves fuertes.

Pero también existen numerosas web que analizan una contraseña y nos dicen si tiene suficiente fortaleza o no basándose en los principales criterios que se suelen adoptar. Puedes encontrarlas fácilmente, pero a modo de ejemplo te mostramos una:

<https://password.es/comprobador/>

Si vas introduciendo la contraseña en el cuadro superior de "Prueba tu contraseña", el sistema te irá dando una estimación de lo segura que es en función de su complejidad.

**Comprobador de Contraseñas/Password**

Inicio | Email Marketing | Juegos | test de velocidad adsl

Google ha cerrado el anuncio  
Denunciar este anuncio | ¿Por qué este anuncio? |>

Change language: castellano | english | italiano | aleman | catalan | frances | portugues

Prueba tu Contraseña		Requerimientos mínimos
Contraseña:	*****	<ul style="list-style-type: none"><li>Tamaño mínimo de 8 caracteres</li><li>Contener al menos 3-4 de las siguientes cosas:<ul style="list-style-type: none"><li>- Letras en Mayúsculas</li><li>- Letras en Minúsculas</li><li>- Números</li><li>- Símbolos</li></ul></li></ul>
Ocultar:	<input checked="" type="checkbox"/>	
Resultado:	100%	
Complejidad:	Very Strong	

<https://password.es/comprobador/>

## Resumen

---

---

Has finalizado esta lección. Repasemos los contenidos más importantes:

Como puedes ver, la labor del administrador no es "solamente" asegurarse de que "todo funciona", sino también establecer las medidas oportunas para intentar prevenir malas prácticas de los usuarios, ataques y vulneraciones de la seguridad o simplemente evitar que por error se produzcan daños al sistema.

Dentro de esta responsabilidad está el establecer una adecuada **política de seguridad**, y dentro de ella una buena **política de gestión de contraseñas**, no solamente con normas para asegurar su fortaleza, sino también la obligación de cambiarla cada cierto tiempo, etc.

Además, la estructura de grupos de usuario, sus privilegios y la pertenencia a ellos de los usuarios del sistema, es algo que debemos pensar y planificar antes de configurarlo, por un lado para asegurarnos de que cumplimos con el "**principio del mínimo privilegio**" y por otro, para facilitar en lo posible tanto nuestro trabajo como administradores como el de los propios usuarios del sistema.

**unir** LA UNIVERSIDAD  
EN INTERNET | FORMACIÓN  
PROFESIONAL

**PROEDUCA**