**Tarea clase 12**

-Root es el nombre convencional de la cuenta de [usuario](https://es.wikipedia.org/wiki/Usuario) que posee todos los derechos en todos los modos ([monousuario](https://es.wikipedia.org/wiki/Monousuario) o [multiusuario](https://es.wikipedia.org/wiki/Multiusuario)). Normalmente es la cuenta de [administrador](https://es.wikipedia.org/wiki/Administrador_de_sistema).

El usuario root puede hacer muchas cosas que un usuario común no puede, tales como cambiar el dueño o permisos de archivos y enlazar a [puertos](https://es.wikipedia.org/wiki/Puerto_(computaci%C3%B3n)) de numeración pequeña.

No es recomendable utilizar el [usuario](https://es.wikipedia.org/wiki/Superusuario) root para una simple sesión de uso habitual, ya que pone en riesgo el sistema al garantizar acceso privilegiado a cada programa en ejecución. Es preferible utilizar una cuenta de usuario normal y utilizar el comando [su](https://es.wikipedia.org/wiki/Su_(unix)" \o "Su (unix)) para acceder a los privilegios de Root en caso de ser necesario.

 Es política de seguridad en [Ubuntu](https://www.ubuntu.com/) no tener activada la cuenta del usuario root o superusuario, que es el que tiene permisos totales sobre el sistema.

-Un [demonio](https://es.wikipedia.org/wiki/Demonio_%28inform%C3%A1tica%29) en Linux, y de manera general en cualquier sistema tipo UNIX, es un proceso que se ejecuta en segundo plano y es autónomo, de manera que no necesita interacción por parte de un usuario del sistema para arrancar y funcionar.

Los servidores web Apache o Nginx están controlados por demonios, por ejemplo.

Los demonios son útiles para hacer funcionar programas independientes de una sesión de usuario, procesos que se inicien de manera automática cuando el sistema arranca, servicios que permanecen a la escucha para ejecutar su tarea cuando son llamados.

-Casi todos los demonios tienen nombres que terminan con la letra “d”, por lo tanto, esa es una forma de identificarlos. Por ejemplo, httpd es el demonio que maneja el servidor Apache, o sshd el que maneja las conexiones de acceso remoto SSH. Linux a menudo inicia demonios en el momento del arranque.

-Debido al gran poder y peligro que tiene el usuario root, en Ubuntu y otras distribuciones basadas en Ubuntu viene deshabilitado por defecto.

En realidad no es necesario tener permisos root para las tareas diarias como navegar por internet, programar, editar vídeos, fotografías o audios. Si quisiéramos instalar cualquier programa o hacer algo que requiera más permisos de los que tiene nuestro usuario podríamos utilizar el comando sudo.

**-Cómo habilitar el usuario root**

Ahora que ya sabemos que el usuario root está deshabilitado por defecto, para habilitarlo simplemente tenemos que asignarle una contraseña con el siguiente comando, pero cuidado, no te recomiendo hacer este paso porque como se te olvide la contraseña de root podrías perder el acceso:

sudo passwd root  
Enter new UNIX password:  
Retype new UNIX password:  
passwd: password updated successfully

Introducimos la contraseña deseada dos veces y ya habremos terminado.

**Cómo deshabilitar el usuario root**

Para bloquear de nuevo el usuario root en Linux simplemente hay que introducir el siguiente comando:

sudo passwd -dl root