**Desafío # 3:**

**Parte I: Comandos de Linux**

1. Crea un fichero que contenga una lista de provincias llamado provincias.txt. Después visualiza el contenido
2. Añade mediante comandos la Provincia de "Buenos Aires" y "Mendoza"

**$ mkdir Bootcamp-Devops-Engineer**

**$ cd Bootcamp-Devops-Engineer/**

**$ mkdir Desafio\_3**

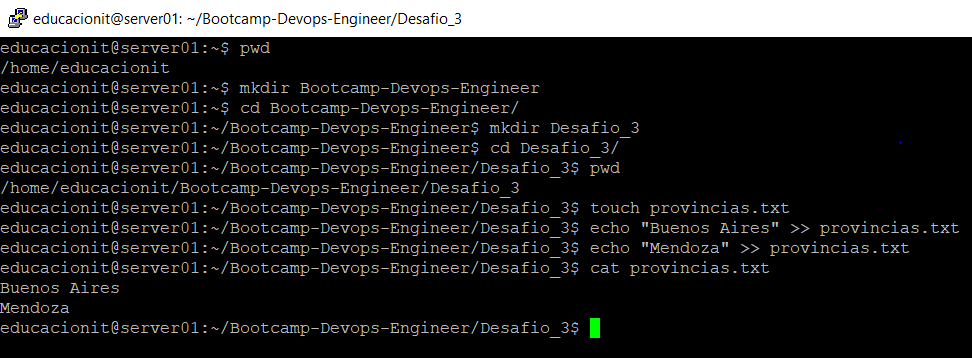
**$ cd Desafio\_3/**

**$ touch provincias.txt**

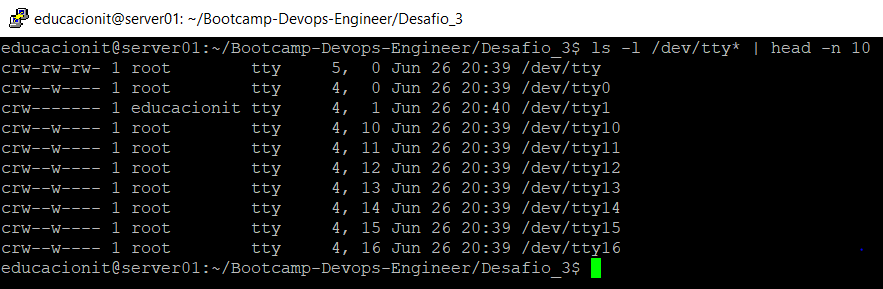
**$ echo "Buenos Aires" >> provincias.txt**

**$ echo "Mendoza" >> provincias.txt**

**$ cat provincias.txt**



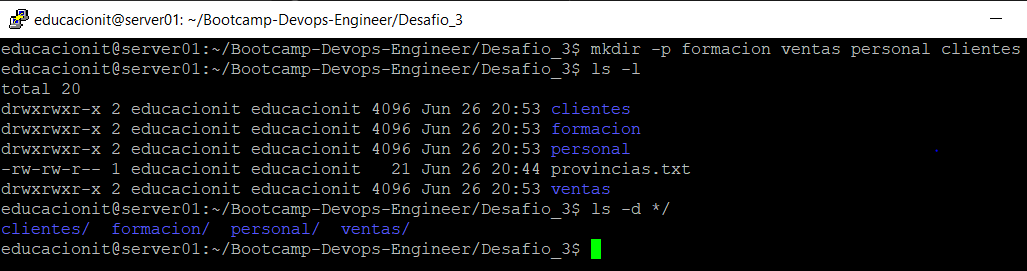
1. Lista los archivos del directorio /dev que empiecen por tty



1. Crea cuatros subdirectorios llamados formación, ventas, personal, clientes ¿Puedes hacerlo con un sólo comando?

**$ mkdir -p formacion ventas personal clientes**

**$ ls -l**



1. Crea cuatro archivos dentro de ventas que sean (mayo, junio, julio) con cualquier contenido en su interior.

**$ pwd**

**$ touch mayo junio julio**

**$ ls**

**$ echo "Información de mayo" > mayo**

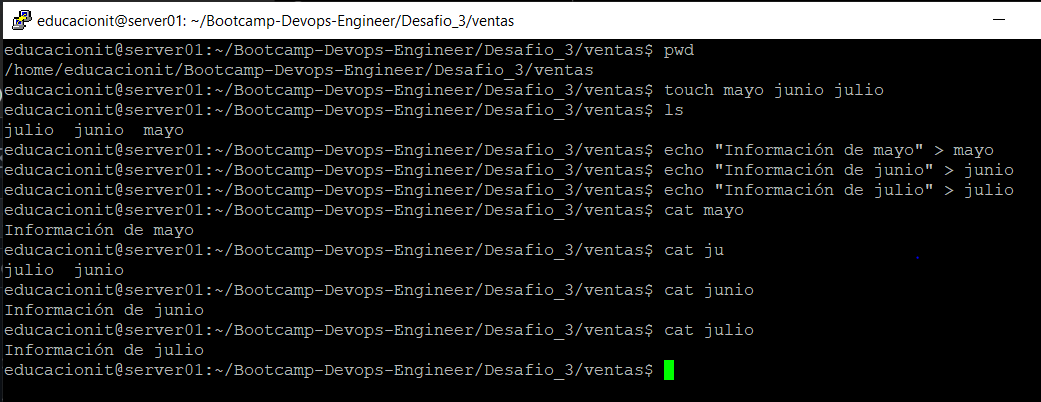
**$ echo "Información de junio" > junio**

**$ echo "Información de julio" > julio**

**$ cat mayo**

**$ cat junio**

**$ cat julio**



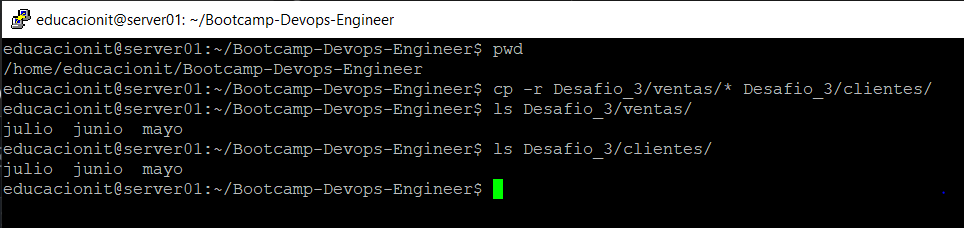
1. Sitúate en el directorio principal y copia en clientes todos los archivos que has creado en ventas

**$ pwd**

**$ cp -r Desafio\_3/ventas/\* Desafio\_3/clientes/**

**$ ls Desafio\_3/ventas/**

**$ ls Desafio\_3/clientes/**

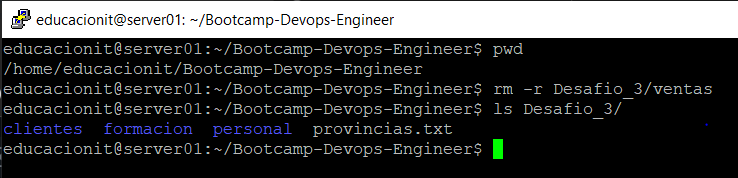


1. Ahora borra el directorio ventas.

**$ pwd**

**$ rm -r Desafio\_3/ventas**

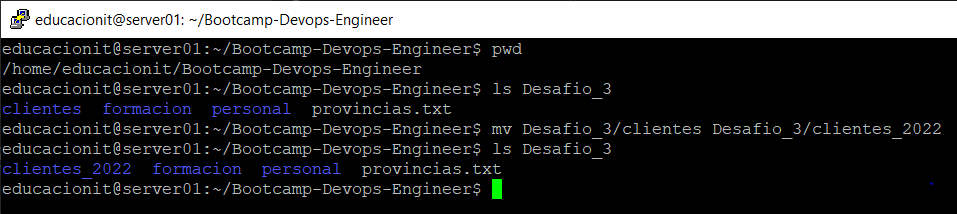
**$ ls Desafio\_3**



1. Renombra el directorio clientes a clientes\_2022

**$ pwd**

**$ mv Desafio\_3/clientes Desafio\_3/clientes\_2022**



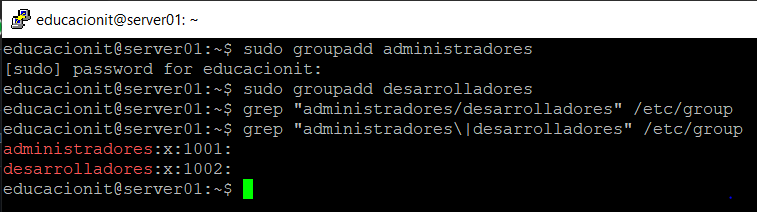
**Parte II: Usuarios/Grupos y Permisos**

1. Crea los grupos administradores y desarrolladores. Comprueba qué GID les asigna.

**$ sudo groupadd administradores**

**$ sudo groupadd desarrolladores**

**$ grep "administradores\|desarrolladores" /etc/group**



1. Crea los usuarios web y app. Estos usuarios deben pertenecer únicamente al grupo desarrolladores. Mira el fichero de definición de usuarios y comprueba que el grupo primario de estos usuarios es el que toca.

**$ sudo useradd -m -G desarrolladores -s /bin/bash web**

**$ sudo useradd -m -G desarrolladores -s /bin/bash app**

**$ sudo passwd web**

New password:

Retype new password:

passwd: password updated successfully

**$ sudo passwd app**

New password:

Retype new password:

passwd: password updated successfully

Texto

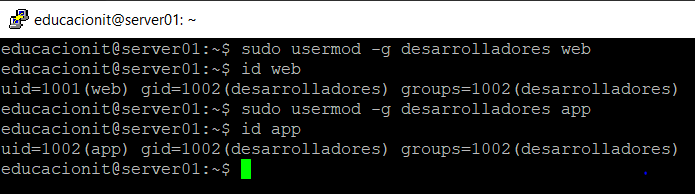
Descripción generada automáticamente

**$ sudo usermod -g desarrolladores web**

**$ id web**

**$ sudo usermod -g desarrolladores app**

**$ id app**



1. Logueate como usuario web y crea el archivo administracion.txt al que únicamente tenga acceso web como lectura y escritura.

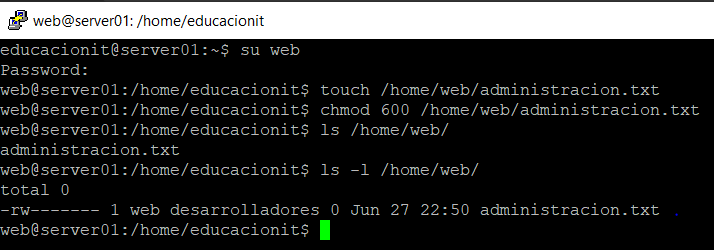
**$ su web**

Password:

**$ touch /home/web/administracion.txt**

**$ chmod 600 /home/web/administracion.txt**

**$ ls -l /home/web/**



1. Como usuario app crea el directorio compartido en su directorio de trabajo, y crea los ficheros archivo1.txt, archivo2.txt, archivo3.txt

**$ su app**

**$ mkdir /home/app/compartir**

**$ touch /home/app/compartir/archivo1.txt /home/app/compartir/archivo2.txt /home/app/compartir/archivo3.txt**

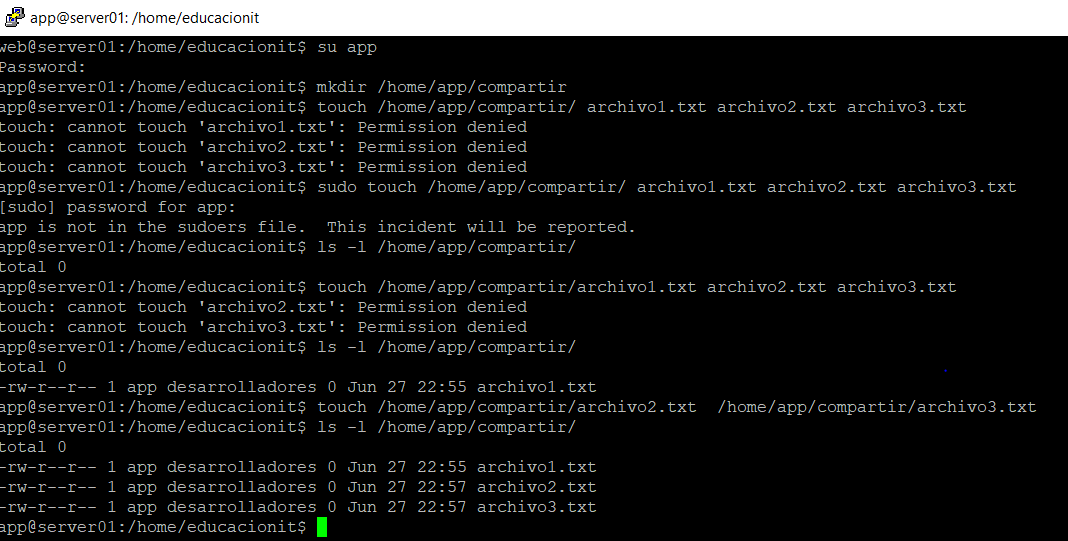
**$ ls -l /home/app/compartir/**

Texto

Descripción generada automáticamente

1. Cambia el grupo propietario de archivos2.txt a desarrolladores.

Cuando se creo el archivo archivos2.txt ya estaba asi.

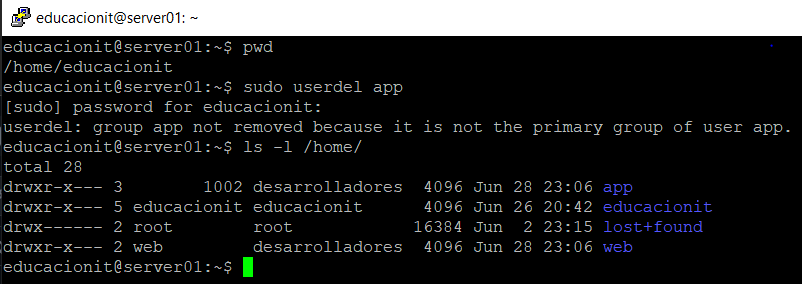


1. Elimina el usuario app sin quitar su directorio personal y observa quién es el

**$ pwd**

**$ sudo userdel app**

**$ ls -l /home/**



1. Steve es el líder de un equipo de trabajo para una compañía que realiza Auditorías Externas. Él ha creado un archivo llamado Lista\_Precios en su directorio /home. El archivo es altamente confidencial, pero resulta que existe un alto riesgo de que su archivo sea vulnerado porque otros empleados utilizan su equipo al finalizar su turno. Actualmente, Steve posee una contraseña segura, pero él necesita resguardar los datos de ese archivo y no desea que nadie más que solamente él tenga acceso al mismo.

¿Qué solución le propondría como equipo a Steve?

Considere lo siguiente para solucionar el problema.

Para proveer una solución apropiada para restringir accesos no autorizados al archivo, se necesita realizar lo siguiente:

* Identificar las medidas de seguridad a implementarse.
* Identificar el tipo de usuarios para quienes los permisos >serán cambiados.
* Identificar el tipo de permiso que necesita ser cambiado.
* Verificar los permisos de acceso al archivo.

Respuestas:

Identificar las medidas de seguridad a implementarse:

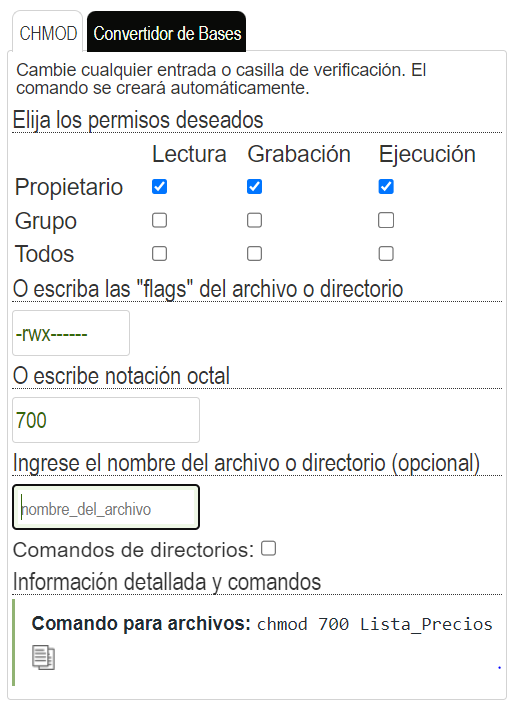
Implementar Google Authenticator en Linux, esto sirve como doble autenticación dedo le pedirá un código que solo lo va tener Steven, asi tengan la contraseña de usuario de Linux, sin este código no podrá ingresar, cambiar los permisos de acceso, cambiar el propietario del archivo o encriptar el archivo.

Identificar el tipo de usuarios para quienes los permisos >serán cambiados:

La idea es restringir el acceso no autorizado al archivo Lista\_Precios a todos los usuarios menos a Steven, por tal motivo los permisos se deben de modificar según esta necesidad.

Identificar el tipo de permiso que necesita ser cambiado:

El archivo deberá de tener los permisos 700 para que solo el propietario tenga acceso total de él, como se muestra en la siguiente imagen:



Verificar los permisos de acceso al archivo:

Para verificar la configuración de los permisos del archivo debemos de ejecutar la línea de comandos: **ls -l** , en caso tal si hay que modificar nuevamente se hace uso del comando **chmod**