**Desafío 3**

**Parte 1: 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**

**$ touch provincias.txt**

**$ echo “Buenos Aires” >> provincias.txt**

**$ echo “Mendoza” >> provincias.txt**

**$ cat provincias.txt**



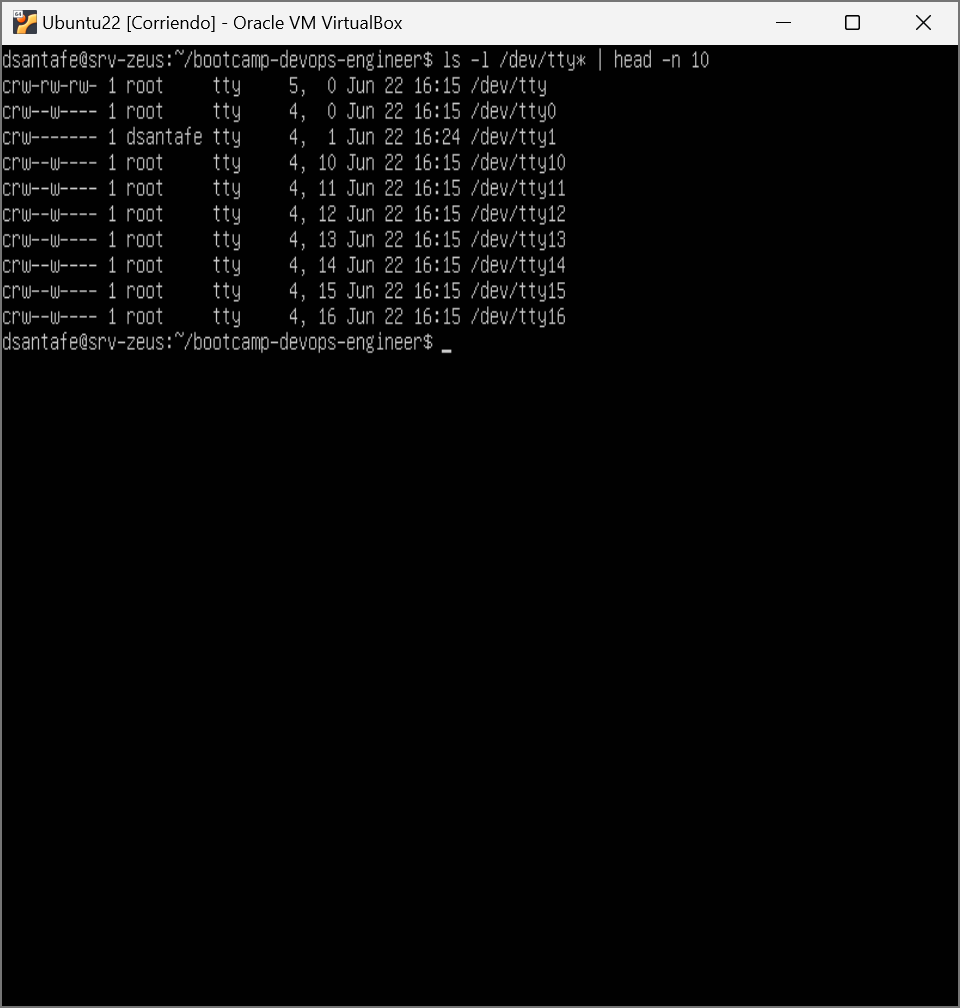
1. Lista los archivos del directorio /dev que empiecen por tty

**$ ls -l /dev/tty\***

Nota: listar los archivos que empiezan por tty en el directorio /dev, con sus detalles como permisos, propietario, tamaño, etc.

**$ ls -l /dev/tty\* | head -n 10**

Nota: limitar el resultado de la búsqueda a 10 archivos.



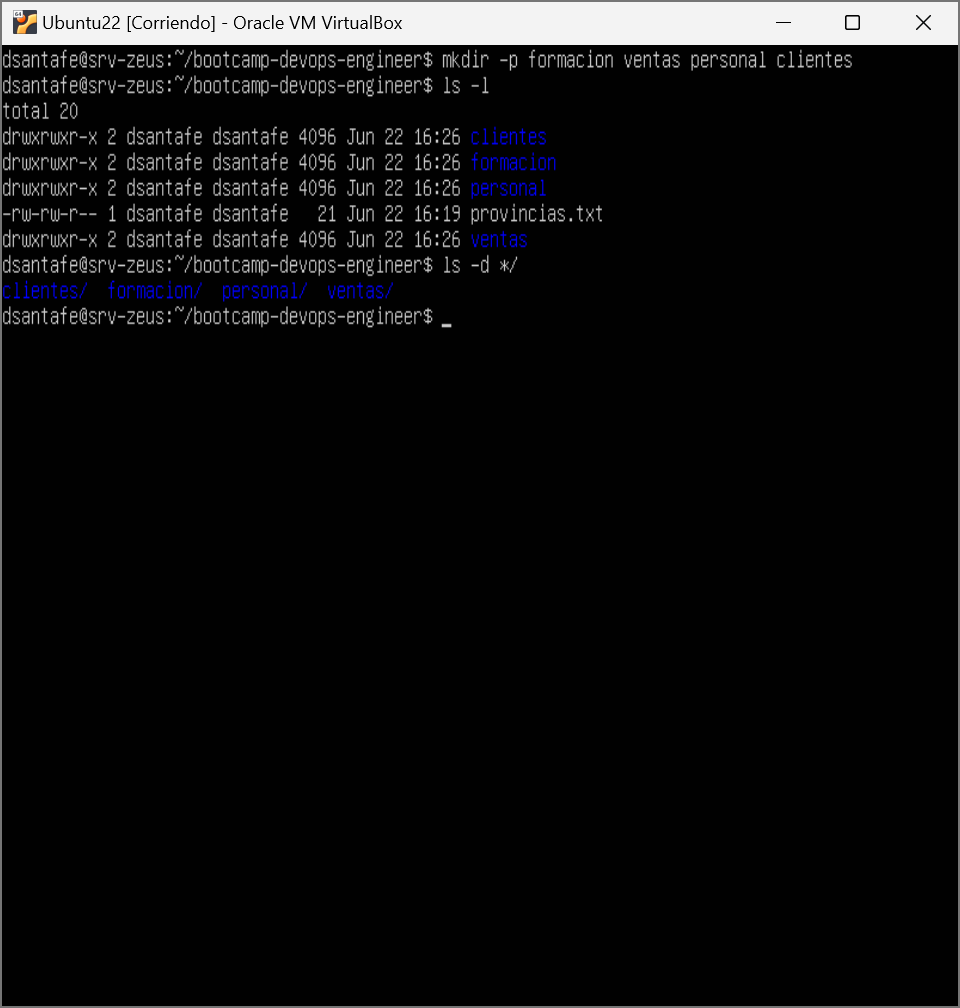
1. Crea cuatros subdirectorios llamados formación, ventas, personal, clientes ¿Puedes hacerlo con un sólo comando?

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

**$ ls -l**

**$ ls -d \*/**

Nota: utilizar el comando mkdir con la opción -p para crear los directorios de forma recursiva.



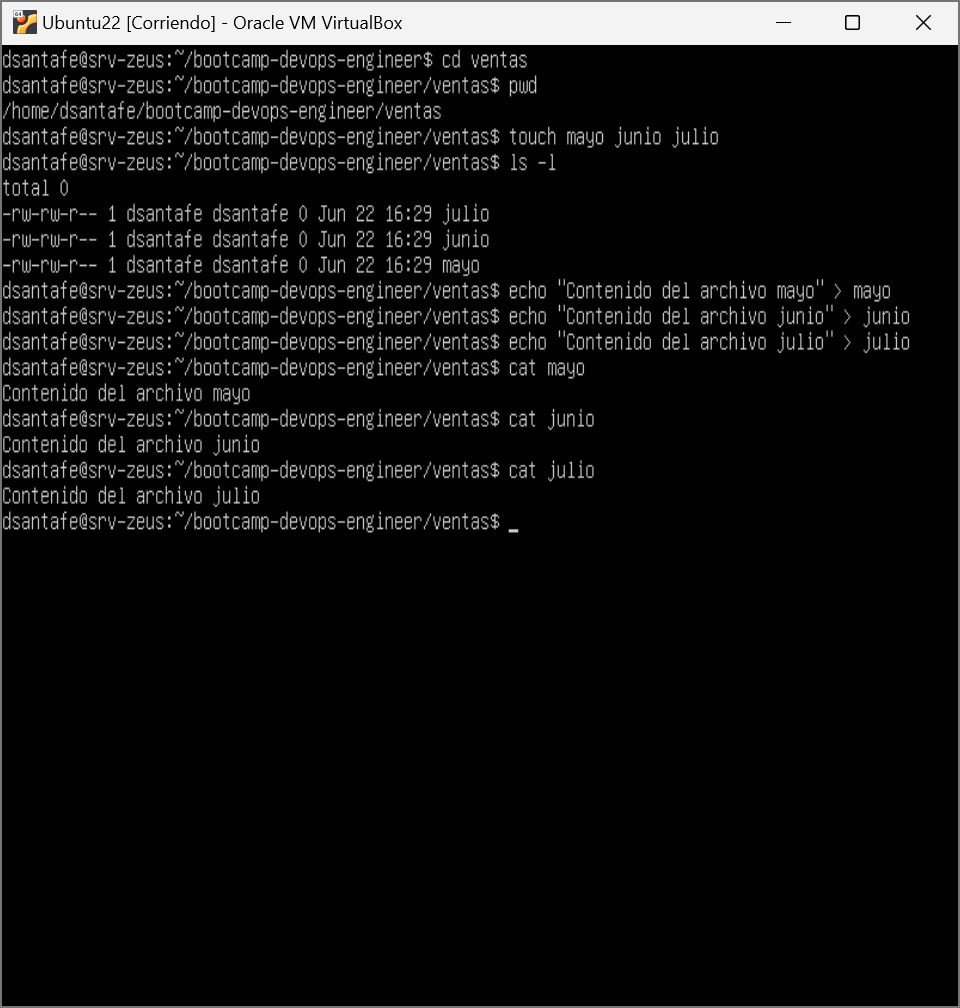
1. Crea cuatro archivos dentro de ventas que sean (mayo, junio, julio) con cualquier contenido en su interior.

**$ cd ventas**

**$ touch mayo junio julio**

**$ echo “Contenido del archivo mayo” > mayo**

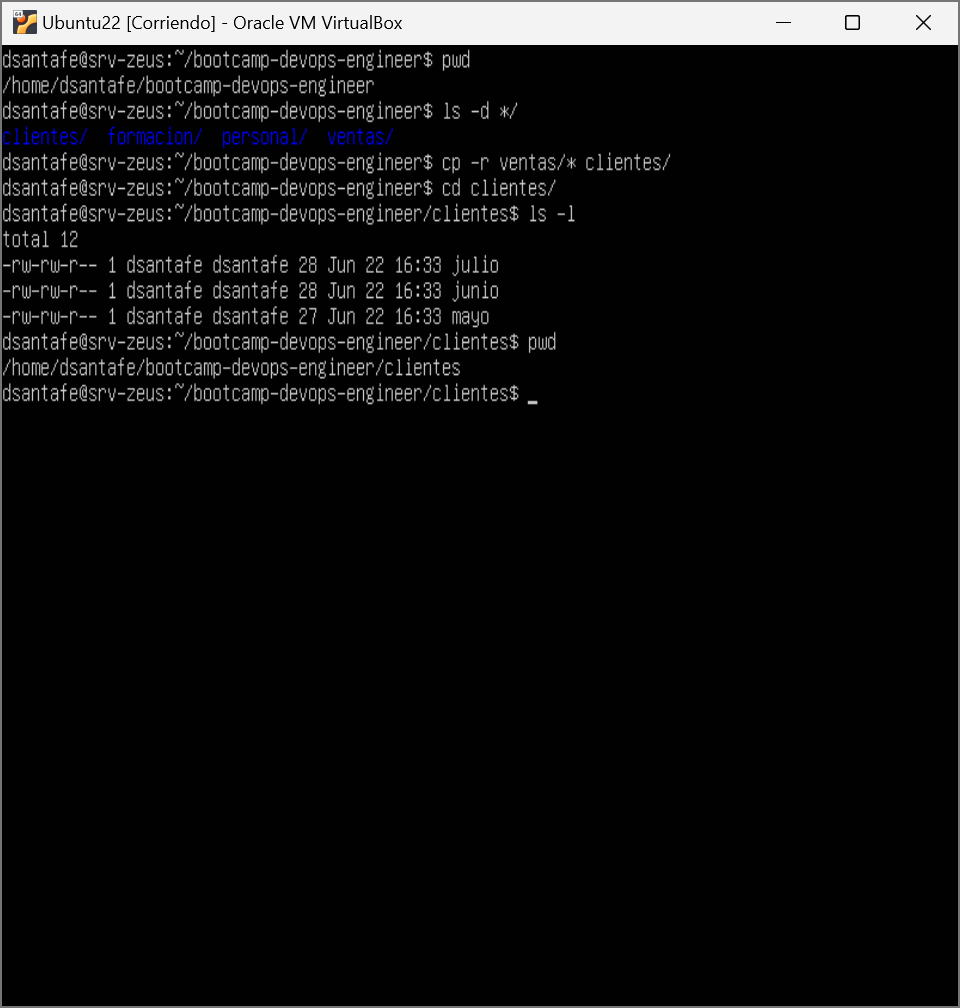
**$ echo “Contenido del archivo junio” > junio**

**$ echo “Contenido del archivo julio” > julio**

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

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

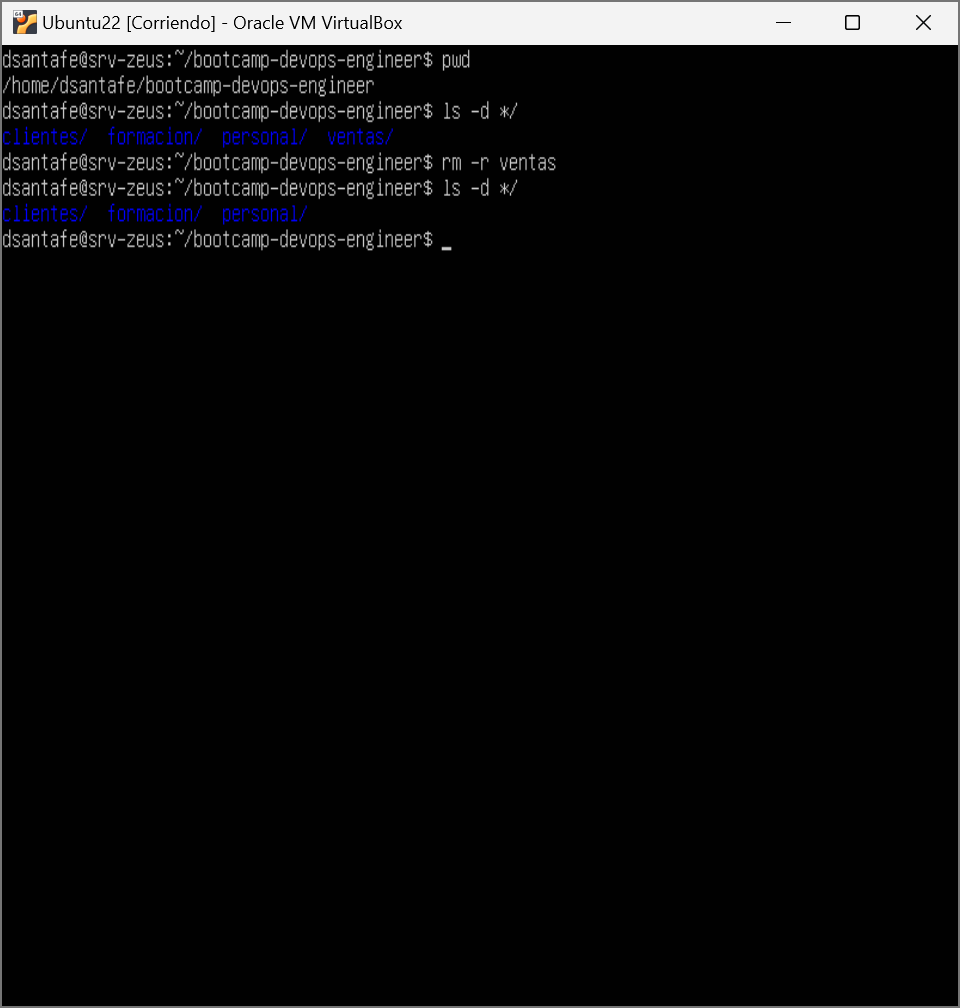
Nota: utilizar el comando cp con el argumento -r para copiar los archivos de forma recursiva.



1. Ahora borra el directorio ventas.

**$ rm -r ventas**

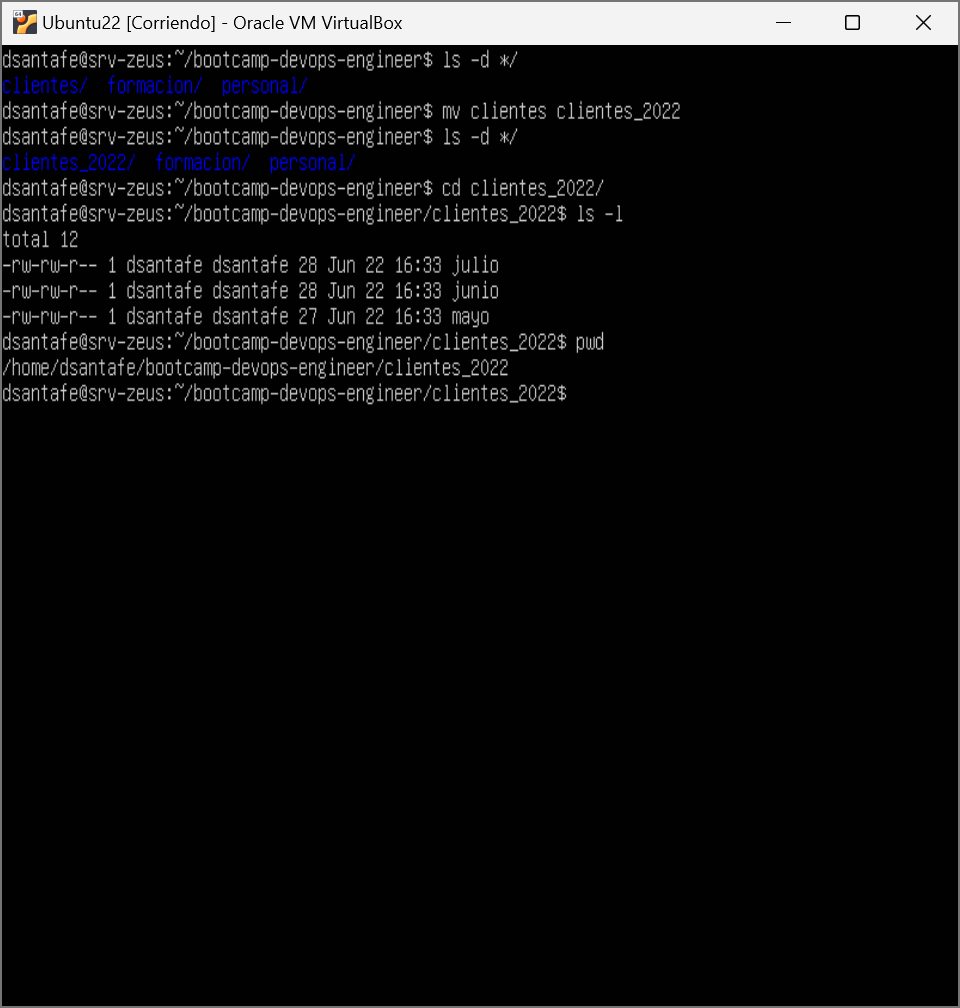
Nota: utilizar el comando rm con el argumento -r para eliminar el directorio y su contenido de forma recursiva.



1. Renombra el directorio clientes a clientes\_2022

**$ mv clientes clientes\_2022**

Nota: utilizar el comando mv para mover o renombrar el directorio.



**Parte 2: Usuarios/Grupos y permisos**

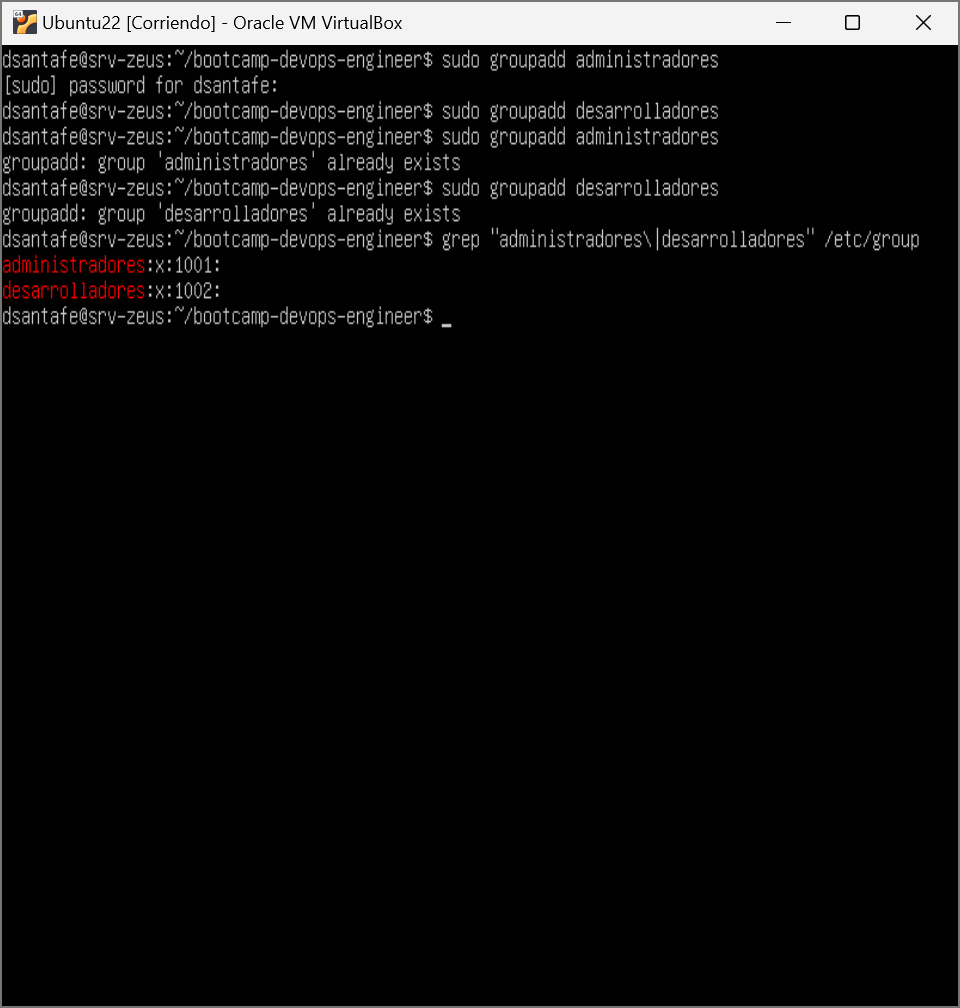
1. Crea los grupos administradores y desarrolladores. Comprueba qué GID les asigna.

**$ sudo groupadd administradores**

**$ sudo groupadd desarrolladores**

**$ grep “administradores\|desarrolladores” /etc/group**

Nota: utilizar el comando groupadd para crear los grupos y el comando grep para buscar y mostrar la información del archivo /etc/group, que contiene la lista de grupos y sus GID asignados.



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.

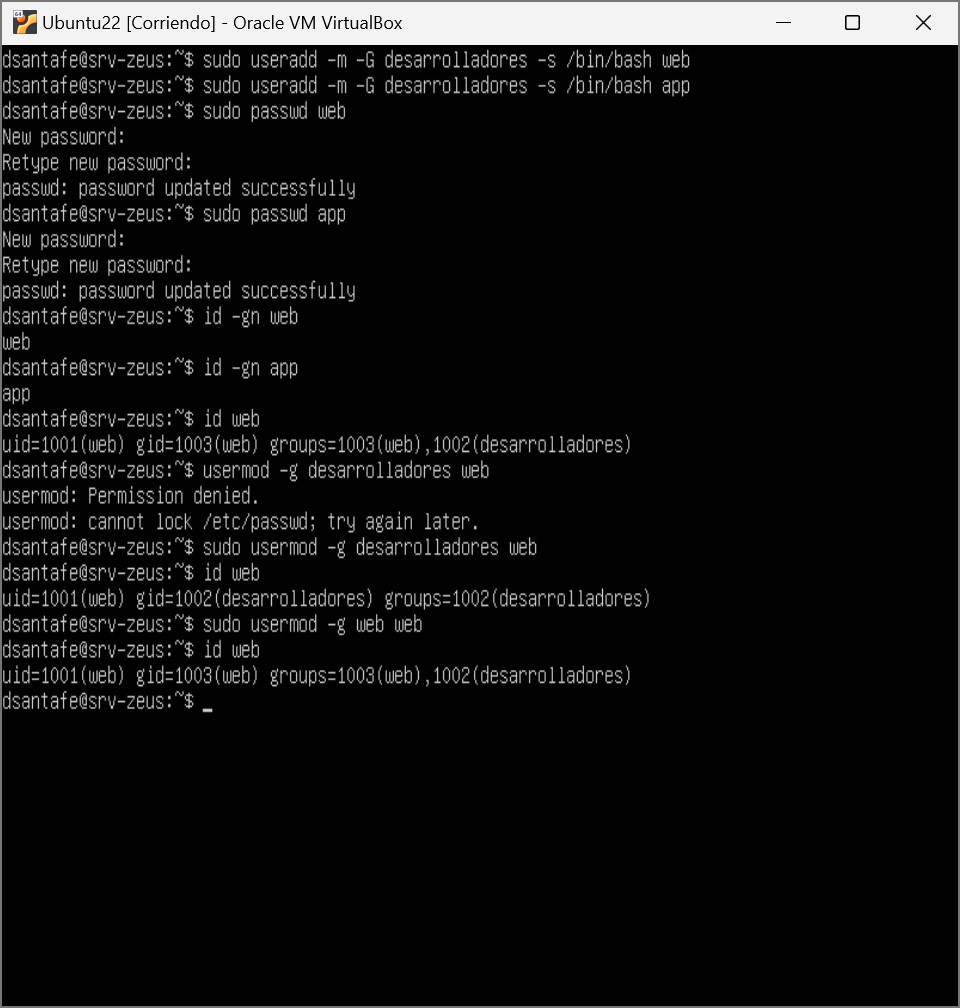
**$ sudo useradd -m -G desarrolladores -s /bin/bash web**

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

**$ sudo passwd web** (asignar password para el usuario web)

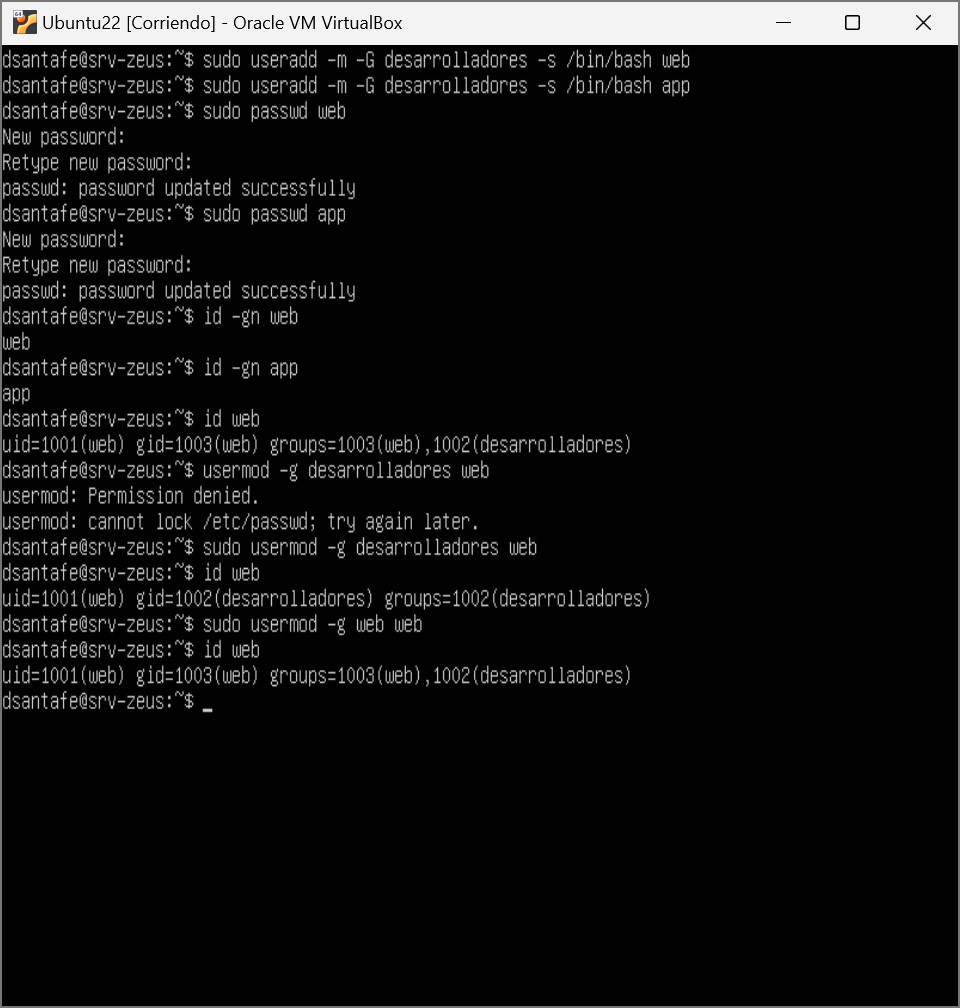
**$ sudo passwd app** (asignar password para el usuario app)

Nota: utilizar el comando useradd para crear los usuarios y el comando usermod para modificar sus propiedades, incluyendo el grupo primario.



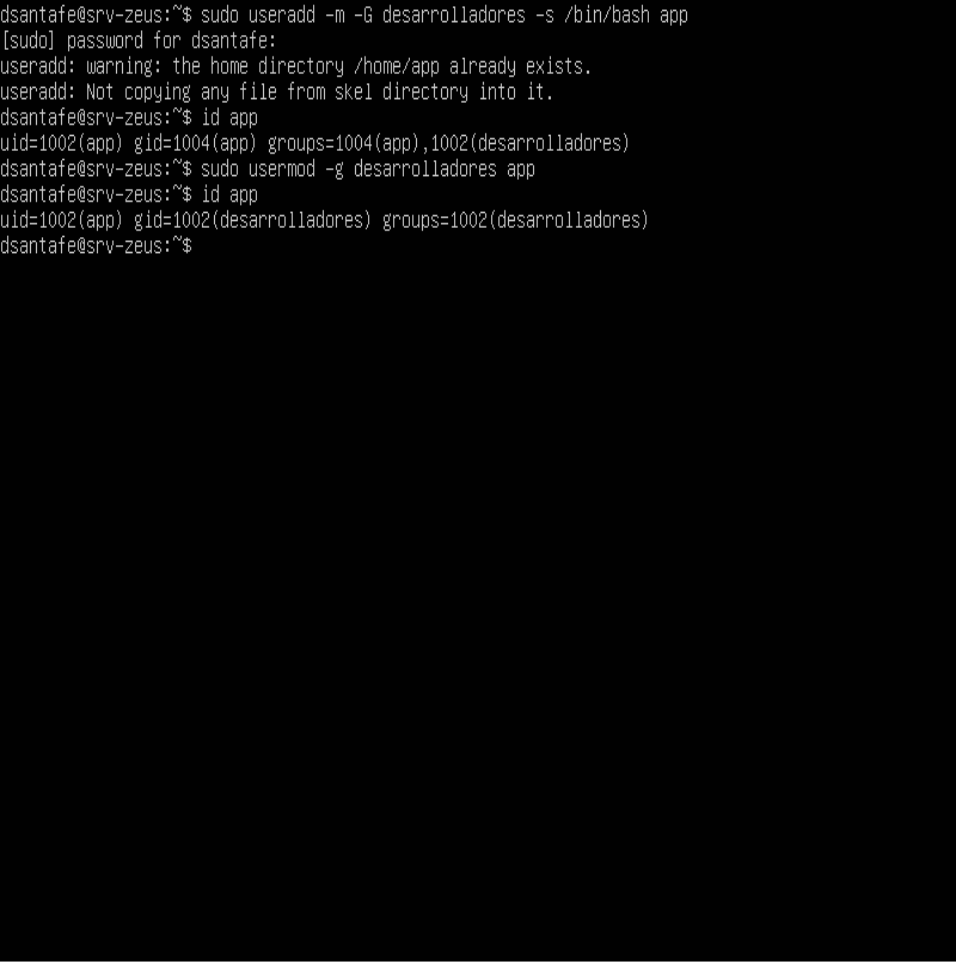
**$ sudo usermod -g desarrolladores web**

**$ 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**

**$ cd ~web**

**$ touch administracion.txt**

**$ chmod 600 administracion.txt**

**$ ls -l**

Nota: utilizar el comando touch para crear el archivo y el comando chmod para establecer los permisos adecuados.



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

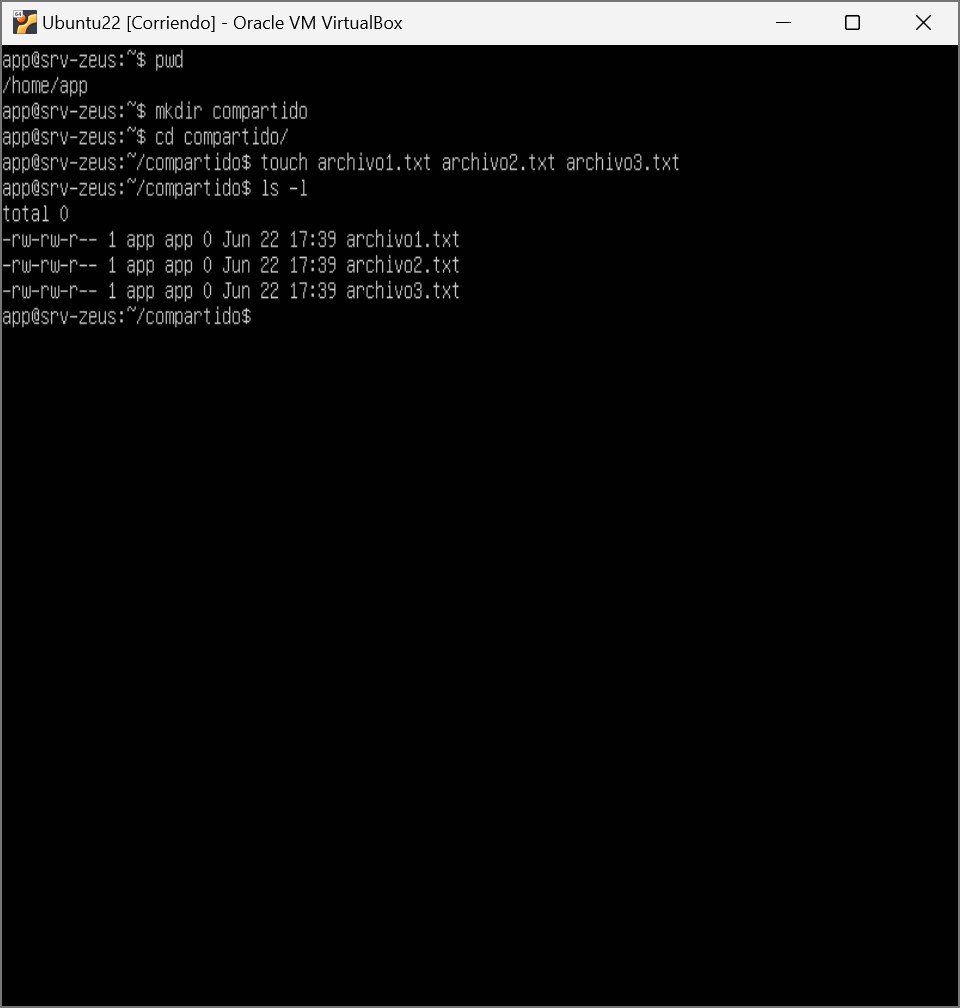
**$ su app**

**$ cd ~app**

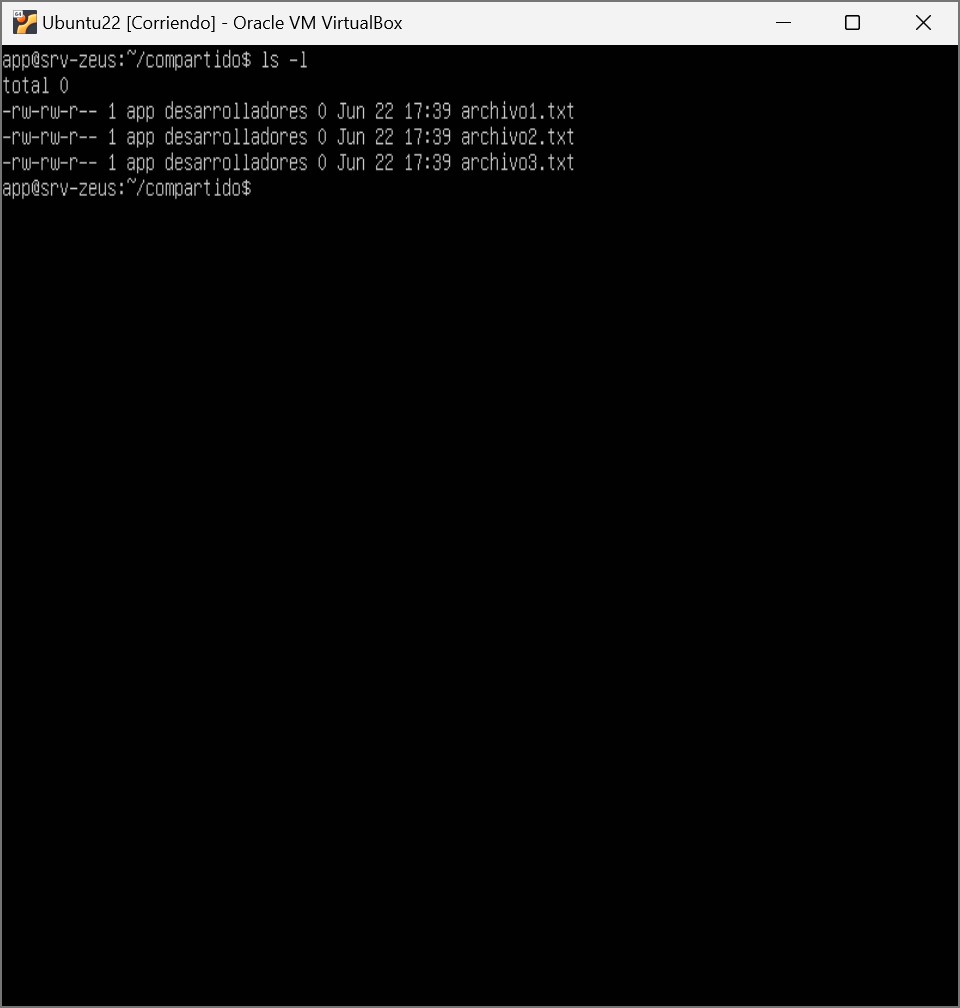
**$ mkdir compartido**

**$ cd compartido**

**$ touch archivo1.txt archivo2.txt archivo3.txt**



**$ ls -l**

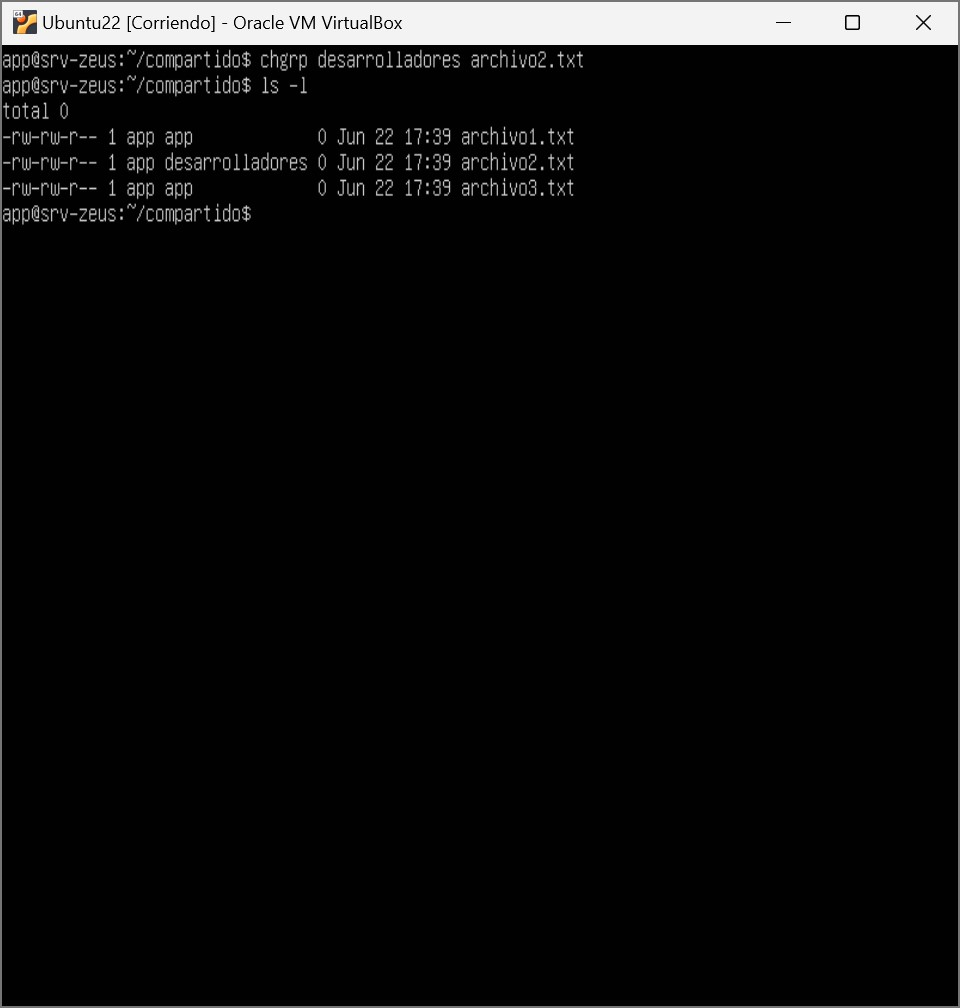


1. Cambia el grupo propietario de archivo2.txt a desarrolladores.

**$ chgrp desarrolladores archivo2.txt**

**$ ls -l**

Nota: Para cambiar el grupo propietario del archivo, utilizar el comando `chgrp` seguido del nombre del grupo y el nombre del archivo.



1. Elimina el usuario app sin quitar su directorio personal y observa quién es el usuario propietario de la carpeta /home/app

**$ su dsantafe**

**$ cd ~dsantafe**

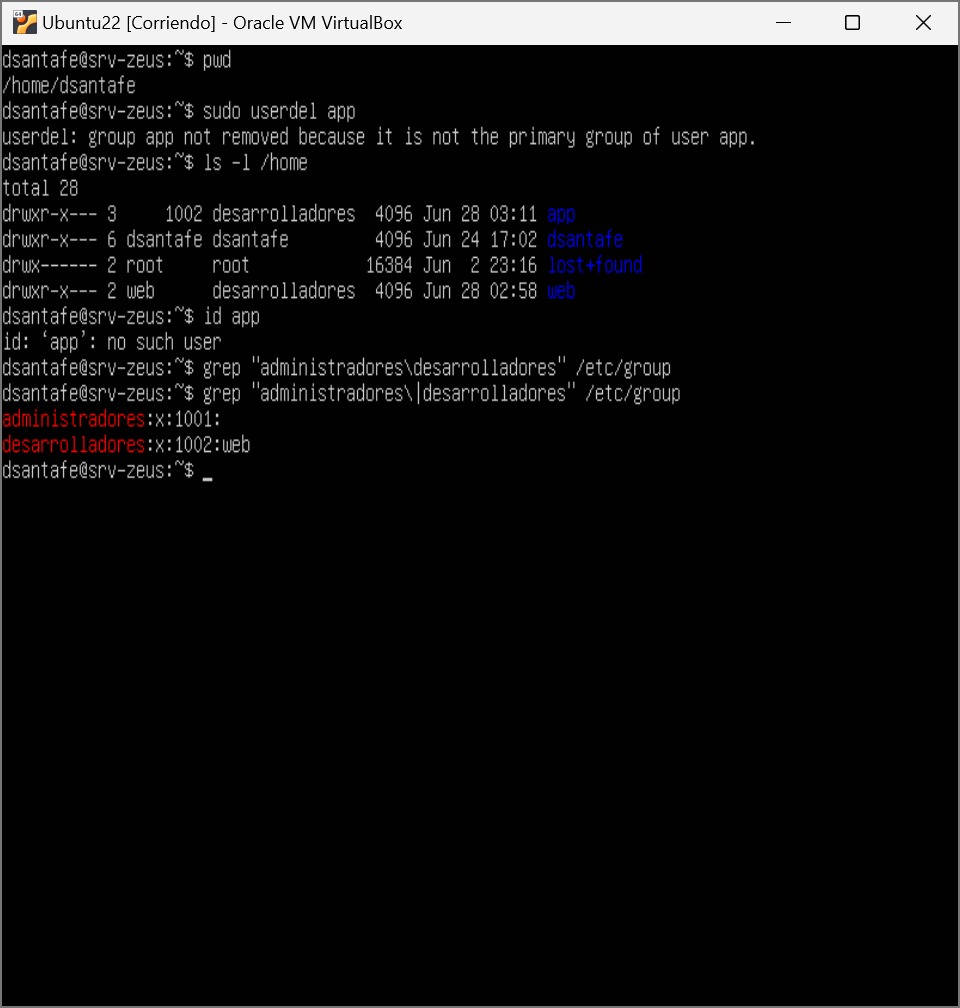
**$ pwd**

**$ sudo userdel app**

**$ ls -l /home**

**$ id app**

Nota: Si utilizas el comando `userdel` con la opción `-r`, elimina al usuario y su directorio personal. Utilizar el comando `userdel`, elimina la entrada del usuario en los archivos /etc/passwd, /etc/shadow y /etc/group. Sin embargo, no eliminará su directorio personal.



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.

Como equipo, le propondríamos a Steve las siguientes medidas de seguridad para restringir el acceso no autorizado al archivo "Lista\_Precios":

* Identificar las medidas de seguridad a implementarse: En primer lugar, es importante identificar las medidas de seguridad necesarias para proteger el archivo. Esto puede incluir cambiar los permisos de acceso, cambiar el propietario del archivo, encriptar el archivo, entre otras medidas.
* Identificar el tipo de usuarios para quienes los permisos serán cambiados: En este caso, el objetivo es restringir el acceso al archivo "Lista\_Precios" a todos los usuarios, excepto a Steve. Por lo tanto, los permisos deben ser modificados para que solo Steve tenga acceso al archivo.
* Identificar el tipo de permiso que necesita ser cambiado: Para restringir el acceso al archivo, se deben cambiar los permisos del archivo para que solo el propietario tenga acceso de lectura y escritura. Esto se puede lograr estableciendo los permisos del archivo en 600, lo que significa que solo el propietario tiene permisos de lectura y escritura.
* Verificar los permisos de acceso al archivo: Antes de implementar las medidas de seguridad, es importante verificar los permisos de acceso actuales del archivo "Lista\_Precios". Esto se puede hacer utilizando el comando `ls -l` para mostrar los permisos del archivo. Si los permisos actuales no son adecuados, se pueden modificar utilizando el comando `chmod`.

En resumen, como equipo, le propondríamos a Steve cambiar los permisos del archivo "Lista\_Precios" para que solo él tenga acceso de lectura y escritura (600), y también cambiar el propietario del archivo a su usuario. Además, se puede considerar encriptar el archivo para agregar una capa adicional de seguridad. Es importante verificar los permisos actuales del archivo antes de implementar estas medidas.