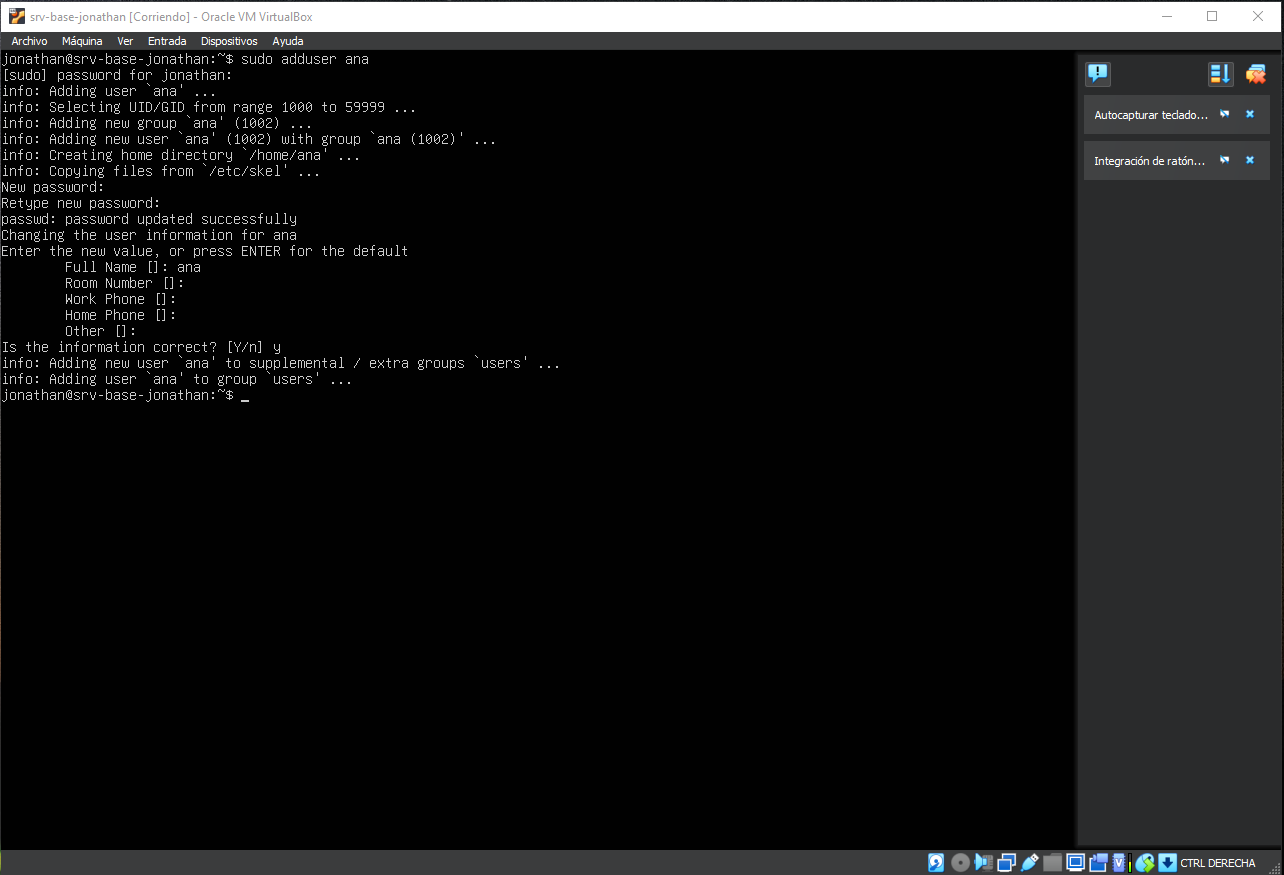
**Control de usuarios, grupos y permisos en Linux**

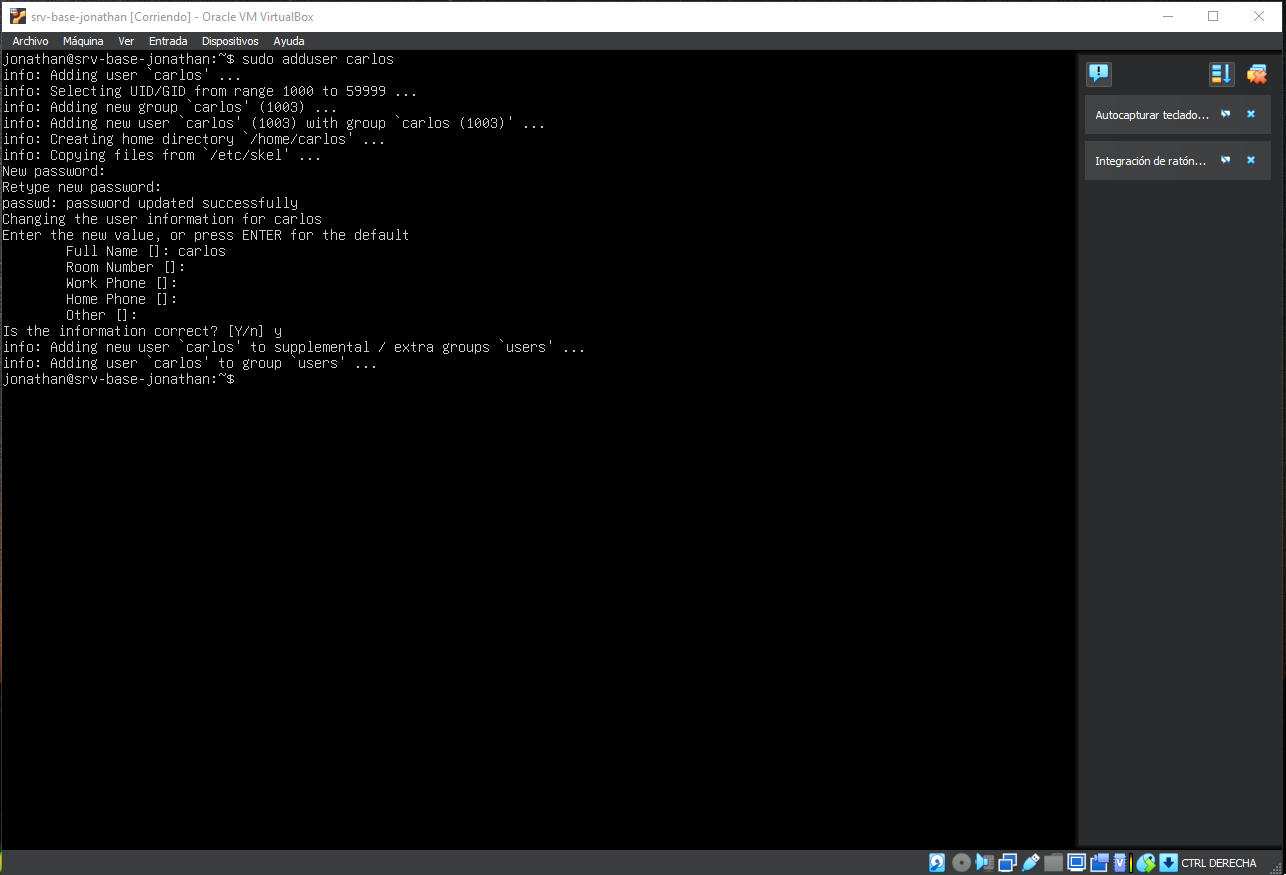
# **Fase 1: Creación y organización de usuarios**

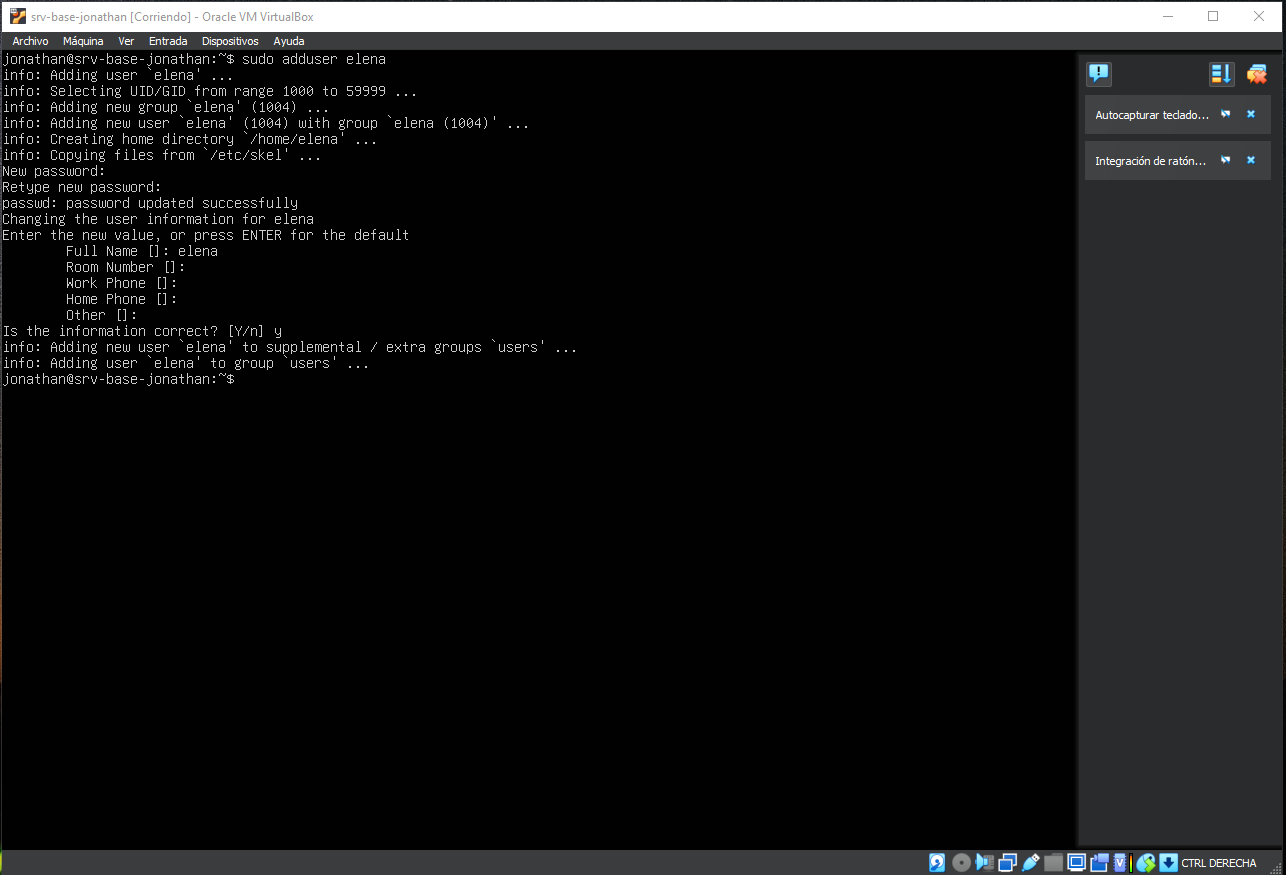
**1.1. Crear usuarios**

Nos vamos a dirigir a la terminal y ejecutaremos los siguientes comando para realizar la creación de usuarios.

* sudo adduser ana
* sudo adduser carlos
* sudo adduser elena





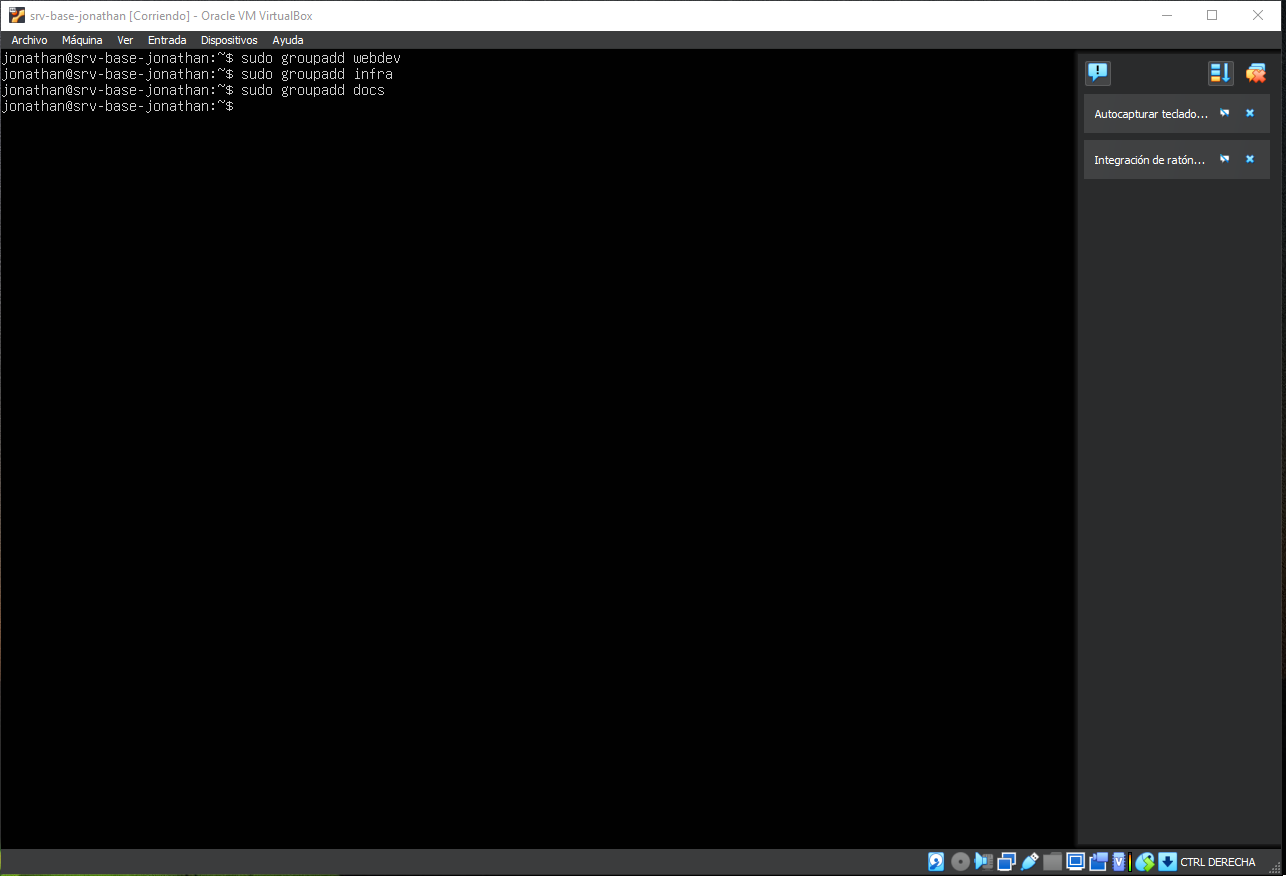


En cada comando nos pedirá una contraseña segura para cada usuario y algunos datos adicionales que podemos rellenar o dejar en blanco.

**1.2. Crear grupos**

Vamo a crear los grupos correspondientes que vamos a utilizar, para ello usaremos los siguientes comandos:

* sudo groupadd webdev
* sudo groupadd infra
* sudo groupadd docs

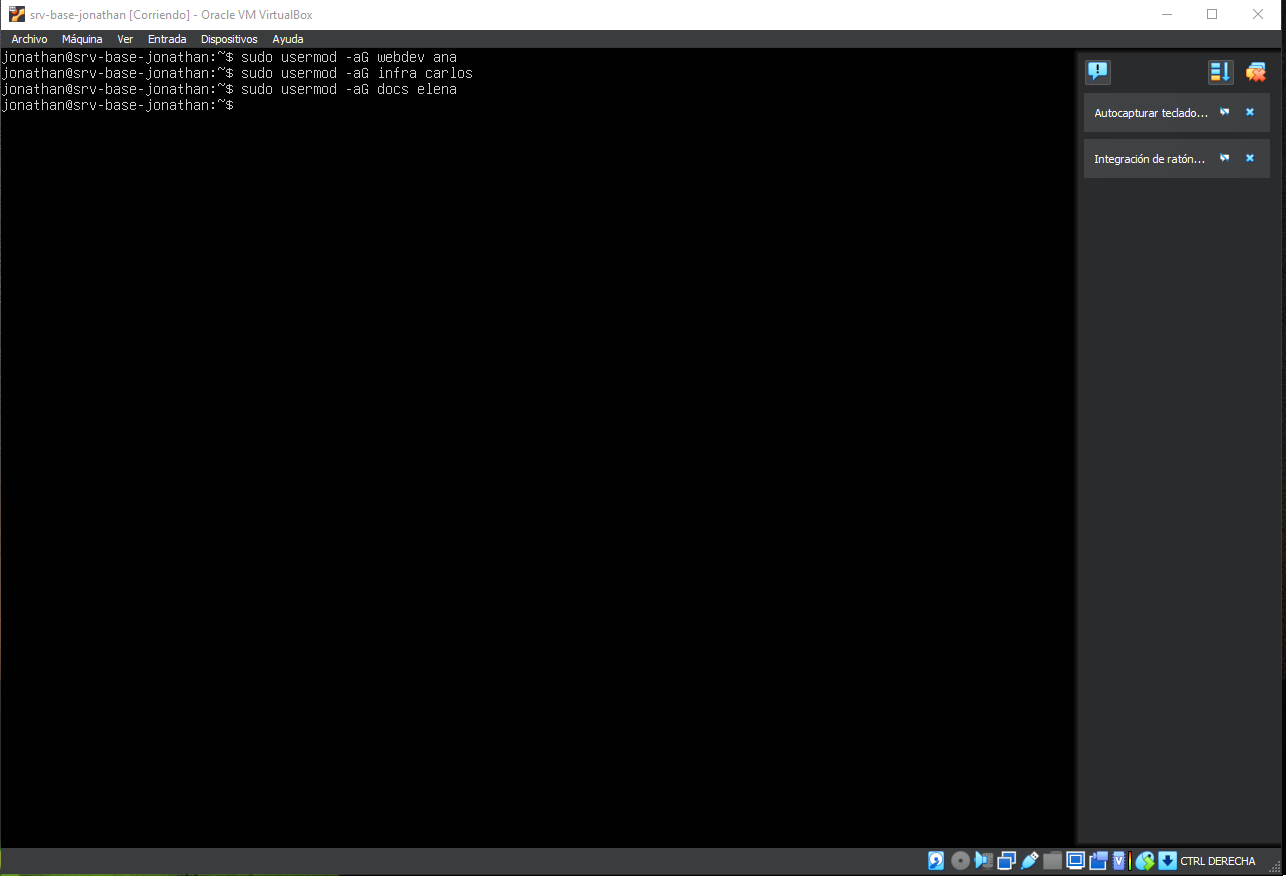


**1.3. Asignar usuarios a sus grupos**

Agregamos a cada usuario a su grupo correspondiente:

* sudo usermod -aG webdev ana
* sudo usermod -aG infra carlos
* sudo usermod -aG docs elena

-aG significa añadir a un grupo sin eliminarlo de otro grupo que tenga.

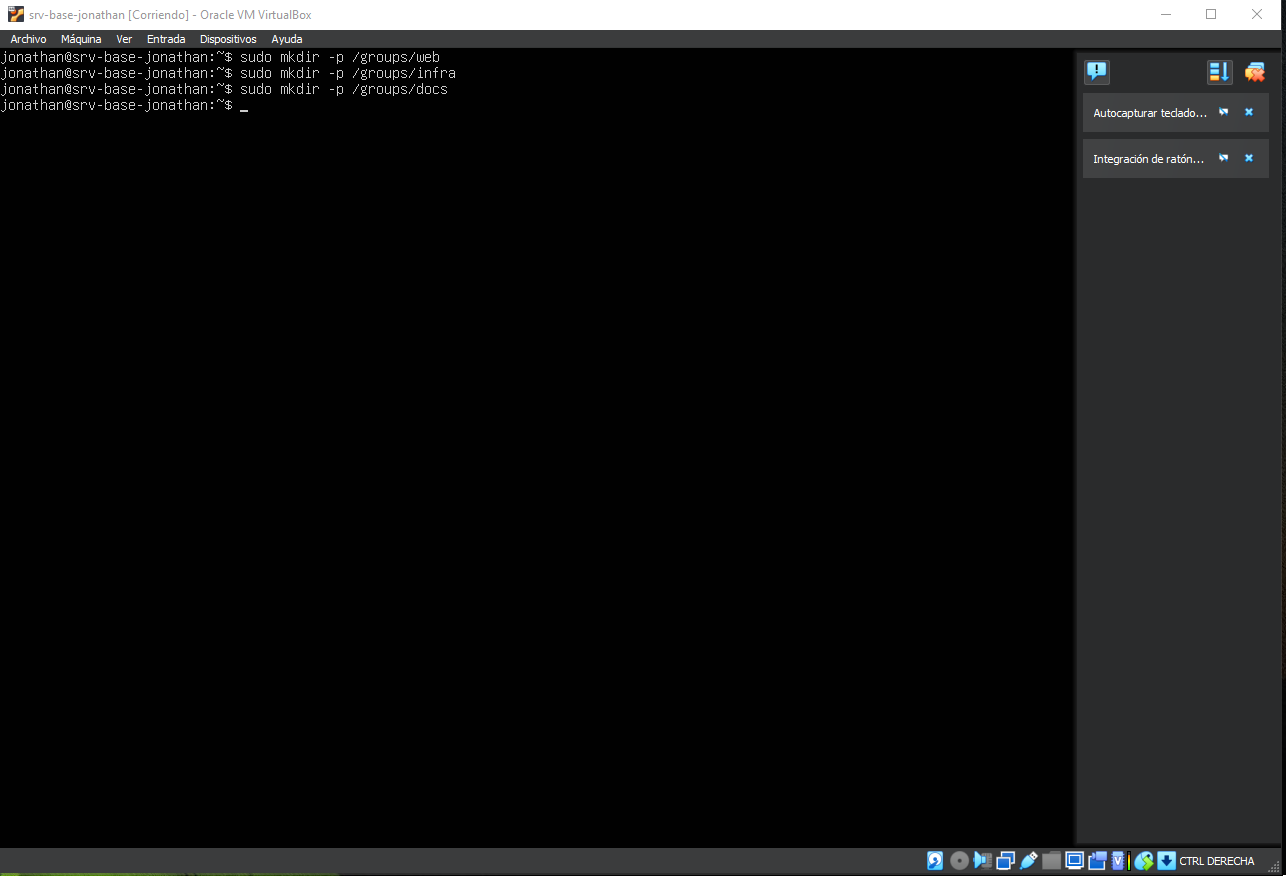


# Fase 2: Estructura de directorios y control de acceso

**2.1. Crear carpetas compartidas**

Creamos las siguientes carpetas para cada grupo.

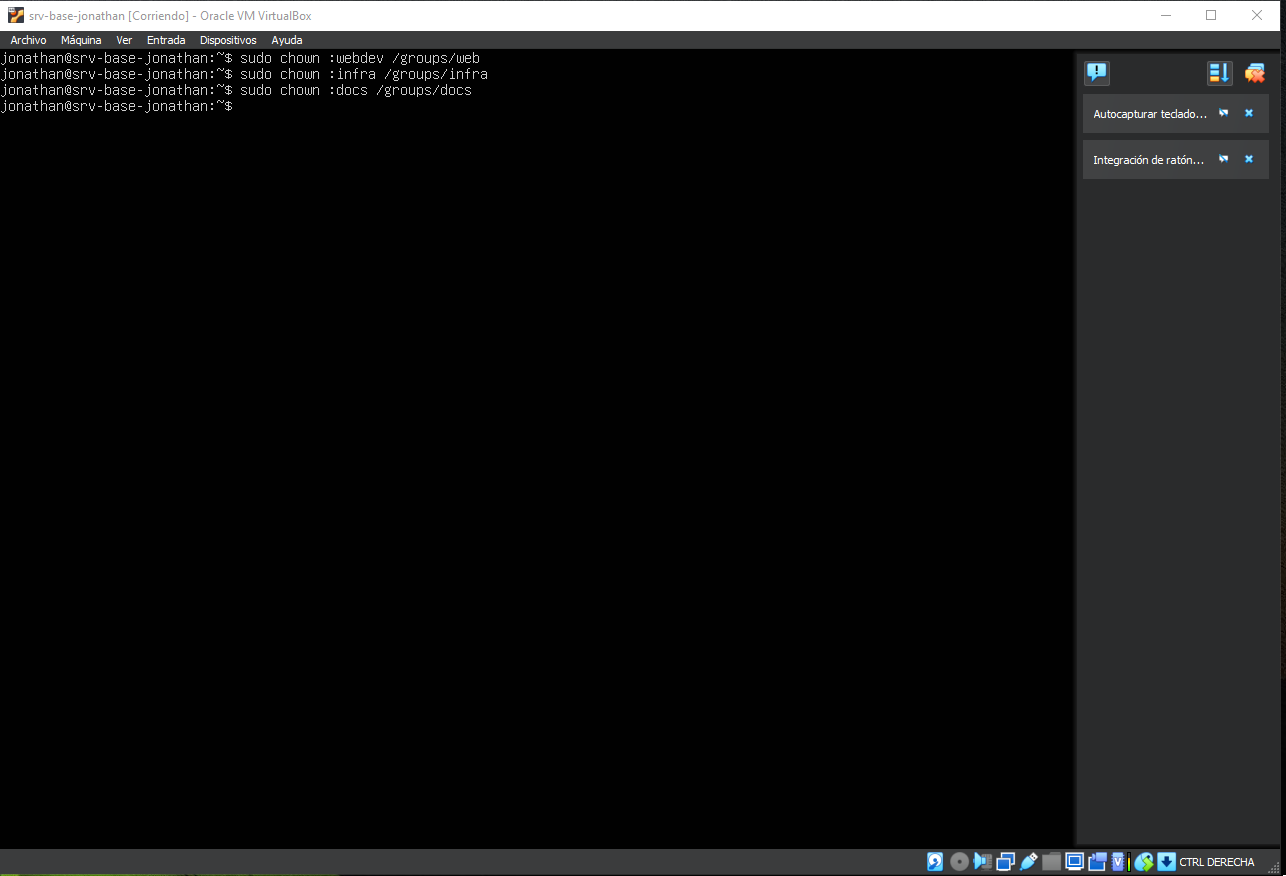
* sudo mkdir -p /grupos/web
* sudo mkdir -p /grupos/infra
* sudo mkdir -p /grupos/docs



**2.2. Cambiar el grupo dueño de las carpetas**

Asignamos el grupo correspondiente a cada carpeta:

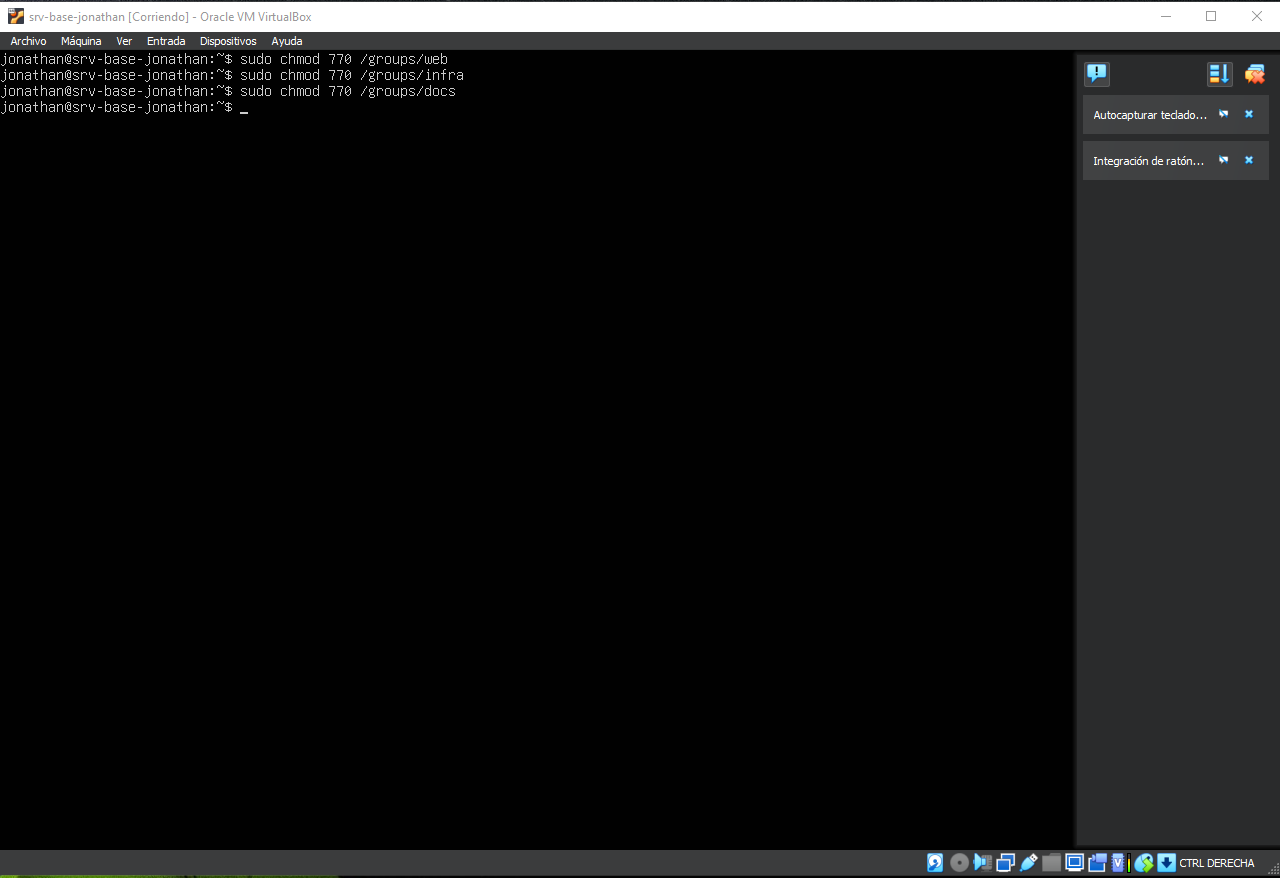
* sudo chown :webdev /grupos/web
* sudo chown :infra /grupos/infra
* sudo chown :docs /grupos/docs

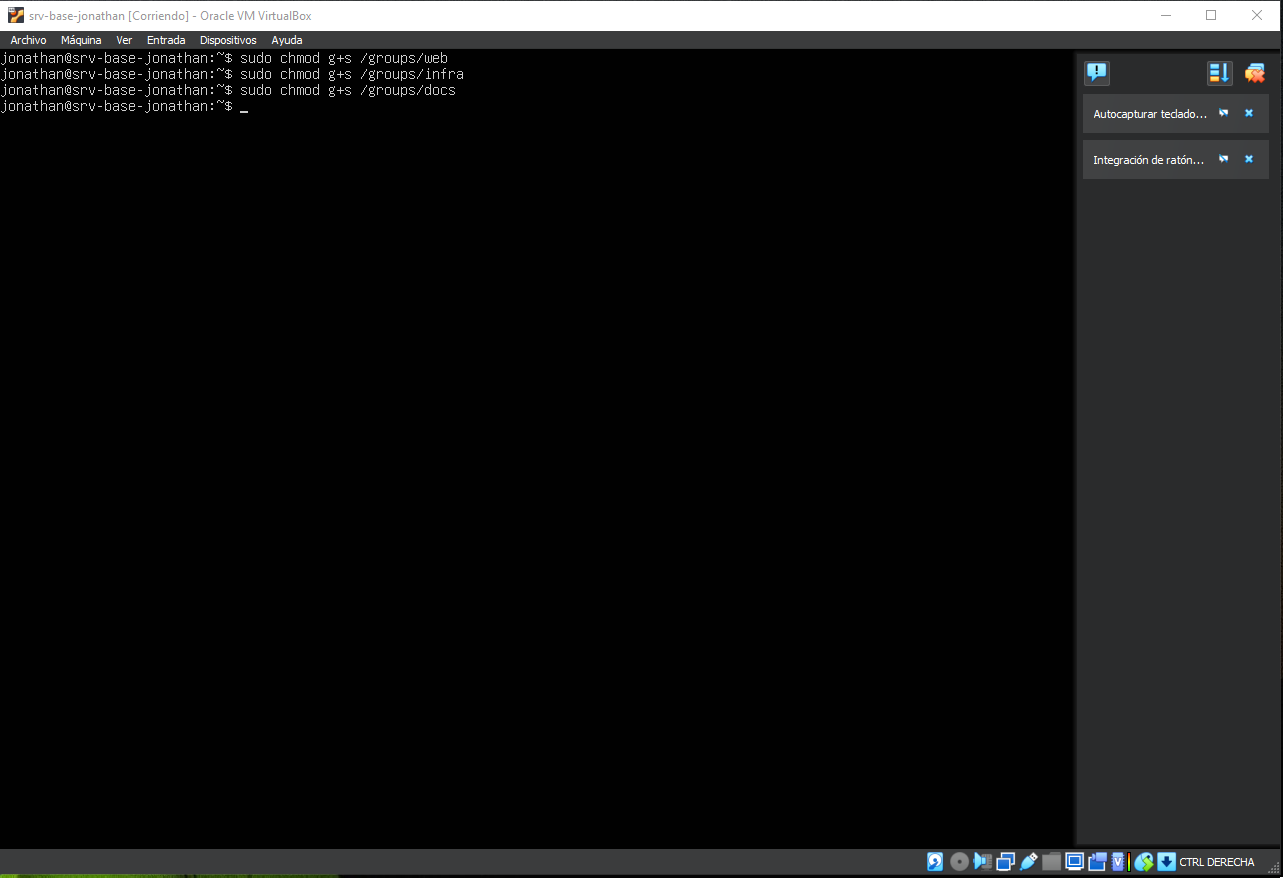


#### **2.3. Asignar permisos**

Establecemos los permisos 770 y activamos el setgit para que los nuevos archivos heeren el grupo.

* sudo chmod 770 /grupos/web
* sudo chmod 770 /grupos/infra
* sudo chmod 770 /grupos/docs
* sudo chmod g+s /grupos/web
* sudo chmod g+s /grupos/infra
* sudo chmod g+s /grupos/docs





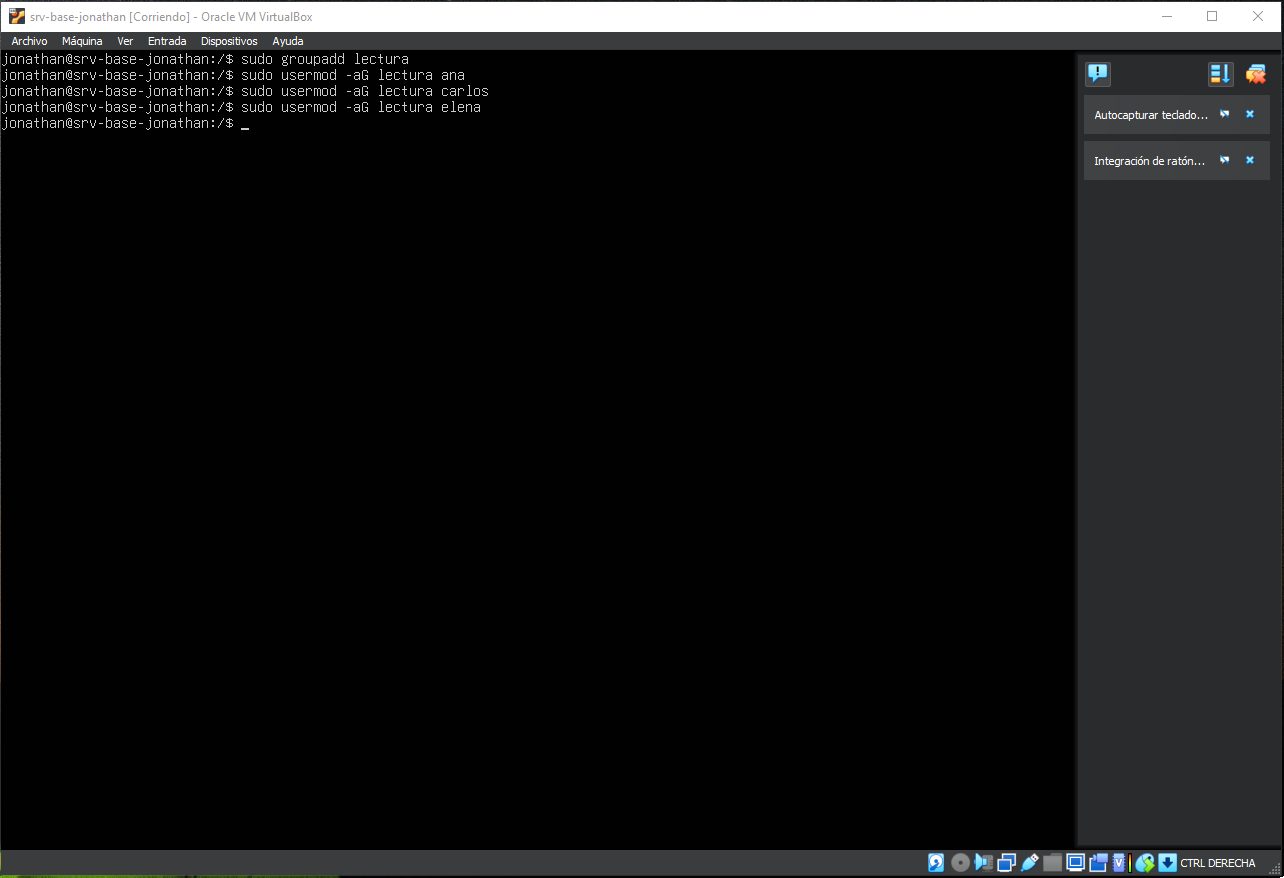
# Fase 3: Configuración avanzada de permisos y restricciones

**3.1 Crear en /grupos/docs un archivo llamado plant.txt**

Entraremos en la carpeta de docs y creamos el archivo con los siguientes comandos:

* sudo touch /grupos/docs/plan.txt
* sudo usermod -aG lectura ana
* sudo usermod -aG lectura carlos
* sudo usermod -aG lectura elena

# 



**3.2. Instalar ACL si es necesario**

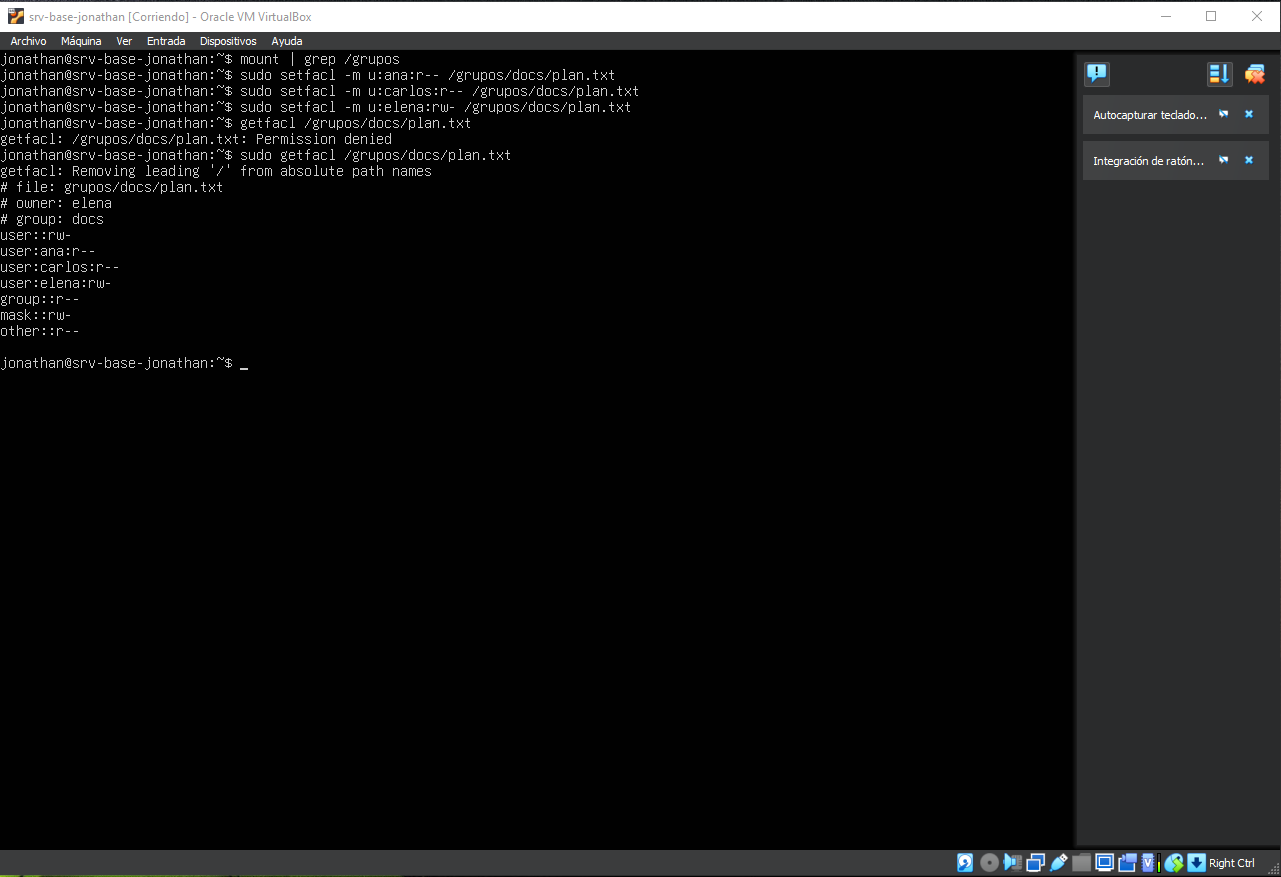
En algunos sistemas ACL no está instalado por defecto así que vamos a proceder a la instalación con:

* sudo apt update
* sudo apt install acl

**3.3. Establecer ACL para permisos especiales**

Vamos a dar los permisos para que Elena pueda editar el archivo pero que Ana y Carlos solo puedan leerlo, ejecutamos:

* sudo setfacl -m u:ana:r /grupos/docs/plan.txt
* sudo setfacl -m u:carlos:r /grupos/docs/plan.txt
* sudo setfacl -m u:elena:rw /grupos/docs/plan.txt

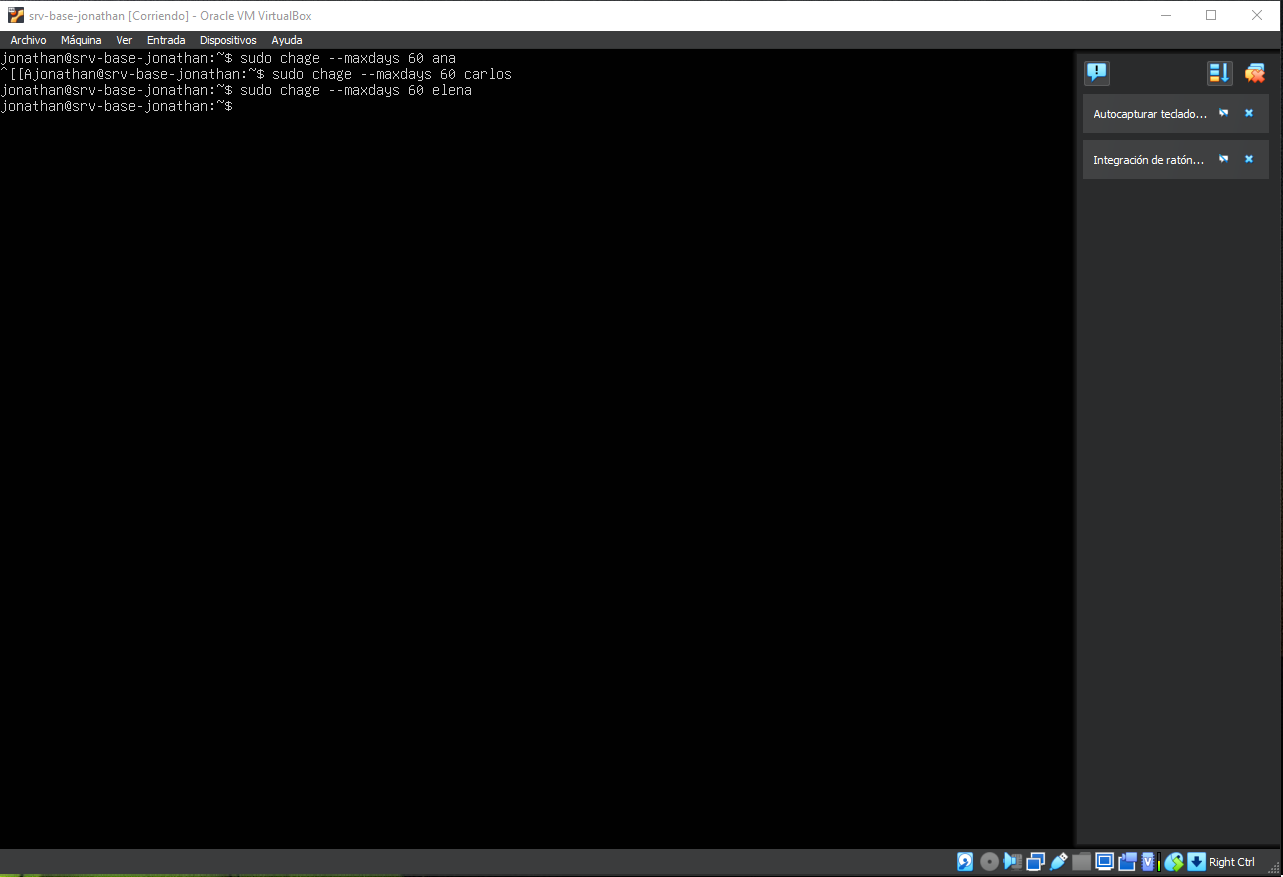


# Fase 4: Buenas prácticas y seguridad básica

**4.1. Política de caducidad de contraseña 60 días.**

Hacemos que las contraseñas de los usuarios creados caduquen cada 60 dias:

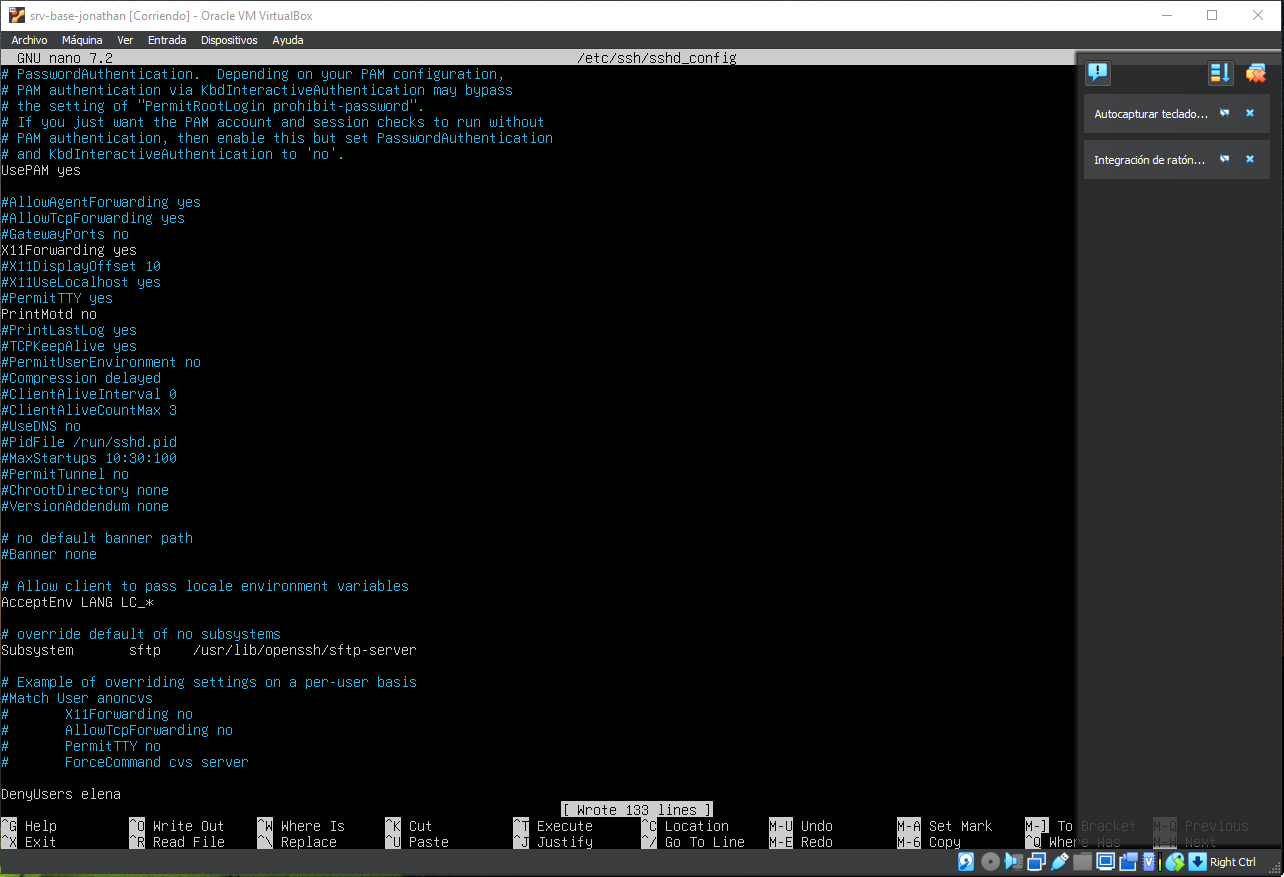
* sudo chage --maxdays 60 ana
* sudo chage --maxdays 60 carlos
* sudo chage --maxdays 60 elena



**4.2. Bloquear el acceso SSH a Elena**

**Editamos el archivo /etc/ssh/sshd\_config y agregamos al final de la linea:**

* **DenyUsers elena**

****

Reiniciamos el servicio SSH para aplicar cambios:

* **sudo systemctl restart ssh**

**4.3. Creación de ALIAS**

Editamos el esqueleto de bashrc para la personalización de un mensaje de bienvenida:

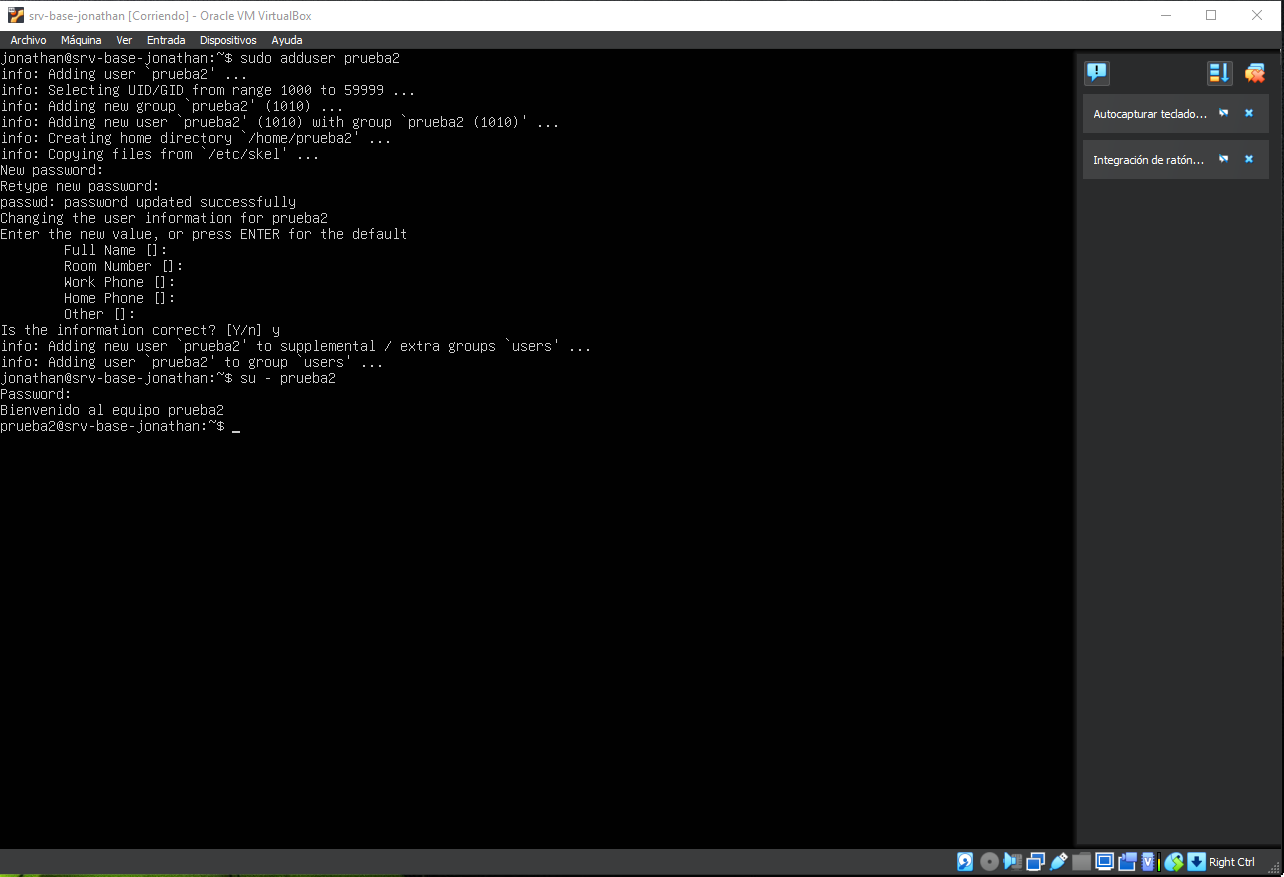
* sudo nano /etc/skel/.bashrc

Y agregamos al final del archivo:

echo "Bienvenido al equipo, $USER"

Hacemos una prueba creando un nuevo usuario:

* sudo adduser prueba2
* su - prueba2



**TABLA**

| Usuario | Grupos | Acceso /grupos/webs | Acceso /grupos/infra | Acceso /grupos/docs | Acceso plan.txt |
| --- | --- | --- | --- | --- | --- |
| ana | webdev | rw | - | - | solo leer |
| carlos | infra | - | rw | - | solo leer |
| elena | docs | - | - | rw | leer y escribir |