



Título del trabajo: **“Trabajo Integrador Sistemas Operativos”**

Farid Salomón, [faridsalomon90@gmail.com](mailto:faridsalomon90@gmail.com) - Gabriel Gonzalez, [gaby250995@gmail.com](mailto:gaby250995@gmail.com)

- Materia: **Arquitectura y Sistemas Operativos**
- Profesor/a: Martin Aristiaran, Mauricio Gabriel Pasti
- Fecha de Entrega: **21/06/2025**

---

## Índice

1. Introducción
  2. Marco Teórico
    - 2.1 Gestión de Permisos y Roles de Usuario
    - 2.2 Autenticación y Acceso
    - 2.3 Optimización del Uso de Recursos
  3. Caso Práctico: Entorno de Pruebas
  4. Caso Práctico: Creación de Usuarios
  5. Caso Práctico: Autenticación y Acceso
  6. Conclusiones
  7. Bibliografía
  8. Anexos
-

# 1. Introducción

En la actualidad, la seguridad de los sistemas operativos Linux es un pilar fundamental para proteger la integridad, confidencialidad y disponibilidad de la información. Más allá del control de permisos y la gestión de usuarios, existen herramientas básicas que refuerzan esta defensa:

- **Firewall:** Primer línea de filtrado de tráfico. Con soluciones como **iptables** o **firewalld** podemos definir reglas que permitan o bloqueen conexiones según puertos, interfaces y protocolos.
- **Antivirus (opcional):** Aunque Linux es menos propenso a malware, herramientas como **ClamAV** facilitan la detección y eliminación de amenazas conocidas.
- **Monitoreo de Actividad:** Utilizar sistemas de auditoría (**auditd**), monitorización de procesos y lectura de logs permite una **detección temprana de anomalías** y posibles ataques.

Además, una configuración segura del sistema operativo implica:

- **Configuración del Firewall en Linux:** Definir políticas de entrada/salida, zonas y reglas específicas con **iptables** o **firewalld** para asegurar que solo el tráfico legítimo acceda al equipo.
- **Gestión de Permisos y Roles de Usuario:** Asignar privilegios mínimos necesarios usando **chmod**, **chown**, **usermod** y **sudo** para limitar acciones no autorizadas.
- **Autenticación y Acceso:** Implementar contraseñas robustas, autenticación de dos factores (2FA) y asegurar servicios remotos (SSH) para controlar quién y cómo se conecta al sistema.
- **Optimización del Uso de Recursos:** Deshabilitar servicios innecesarios, aplicar **ulimit** para limitar consumo de CPU y memoria, y mantener un entorno liviano reduce puntos de ataque y mejora el rendimiento.

Este trabajo combina estos conceptos teóricos con un caso práctico reproducible en una máquina virtual Ubuntu en VirtualBox, sin requerir instalaciones adicionales, para que puedas aplicar de inmediato las buenas prácticas de seguridad.

## 2. Marco Teórico

### 2.1 Gestión de Permisos y Roles de Usuario

La asignación adecuada de permisos en archivos y directorios garantiza la confidencialidad e integridad de los datos. Una gestión de usuarios y grupos con políticas de privilegios mínimos ayuda a prevenir escalamiento de privilegios indeseados.

- **Uso de permisos (chmod, chown, umask):**
  - Permisos de solo lectura: `sudo chmod 444 archivo.txt`
  - Permitir escritura al propietario: `sudo chmod 755 /ruta/directorio`

- Cambiar propietario y grupo: `sudo chown usuario:grupo archivo.txt`
- **Roles y sudo:**
  - Agregar usuario a grupo: `sudo usermod -aG grupo usuario`
  - Ver grupos de un usuario: `groups usuario`
  - Dar acceso a sudo: `sudo usermod -aG sudo usuario`
  - Editar sudoers: `sudo visudo`

## 2.2 Autenticación y Acceso

Una autenticación robusta protege contra accesos no autorizados y vulnerabilidades.

- **Contraseñas seguras y 2FA:**
  - Cambiar contraseña: `sudo passwd usuario`
  - (Opcional) Google Authenticator: `sudo apt install libpam-google-authenticator`
- **SSH seguro:**
  - Deshabilitar root login en SSH: editar `/etc/ssh/sshd_config` y poner `PermitRootLogin no`, luego `sudo systemctl restart sshd`
  - Habilitar autenticación por clave pública: generar par RSA y copiar `id_rsa.pub` a `~/.ssh/authorized_keys`

## 2.3 Optimización del Uso de Recursos

La seguridad también implica eficiencia en la administración de recursos, reduciendo la superficie de ataque.

- **Deshabilitar servicios innecesarios:** `sudo systemctl disable servicio`
- **Limitar recursos por usuario:** configurar `ulimit` en `/etc/security/limits.conf`
- **Reducir vulnerabilidades operativas:** mantener solo servicios esenciales en ejecución

## 3. Caso Práctico: Entorno de Pruebas

- **Plataforma:** Ubuntu LTS en VirtualBox
- **Configuración:** cuenta con `sudo` por defecto
- **Alcance:** Instalando un paquete de google

## 4. Caso Práctico: Creación de Usuarios

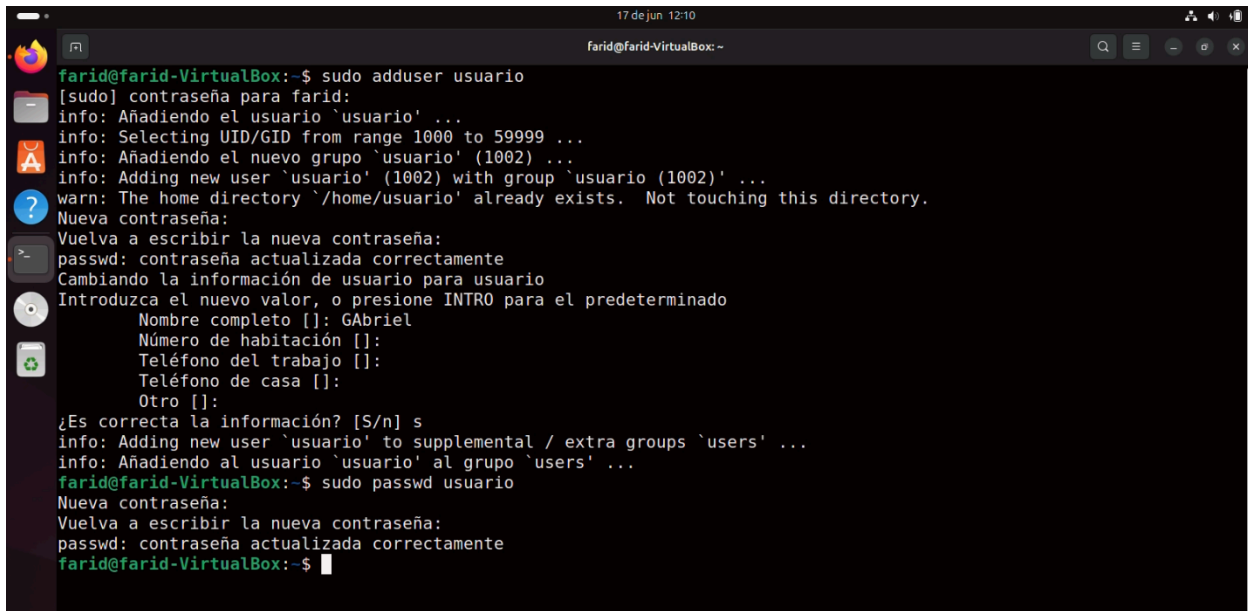
`sudo adduser usuario`

## 5. Caso Práctico: Autenticación y Acceso

Para probar la gestión de contraseñas y acceso, trabajaremos con el usuario “usuario”

### 1. Asignar o cambiar contraseña de usuarios

- Como sudoer (farid), establece la contraseña de cada usuario:
- `sudo passwd usuario`
- Esto definirá la contraseña inicial de ambos.




```

17 de jun 12:10
farid@farid-VirtualBox: ~
farid@farid-VirtualBox:~$ sudo adduser usuario
[sudo] contraseña para farid:
info: Añadiendo el usuario 'usuario' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Añadiendo el nuevo grupo 'usuario' (1002) ...
info: Adding new user 'usuario' (1002) with group 'usuario (1002)' ...
warn: The home directory '/home/usuario' already exists. Not touching this directory.
Nueva contraseña:
Vuelva a escribir la nueva contraseña:
passwd: contraseña actualizada correctamente
Cambiando la información de usuario para usuario
Introduzca el nuevo valor, o presione INTRO para el predeterminado
Nombre completo [:] Gabriel
Número de habitación [:]
Teléfono del trabajo [:]
Teléfono de casa [:]
Otro [:]
¿Es correcta la información? [S/n] s
info: Adding new user 'usuario' to supplemental / extra groups 'users' ...
info: Añadiendo al usuario 'usuario' al grupo 'users' ...
farid@farid-VirtualBox:~$ sudo passwd usuario
Nueva contraseña:
Vuelva a escribir la nueva contraseña:
passwd: contraseña actualizada correctamente
farid@farid-VirtualBox:~$

```

### 2. Cambio de contraseña propio

- Conéctate como alumno1 y cambia tu propia contraseña sin sudo:
- `su - usuario`
- `passwd` # cambia la contraseña del usuario actual



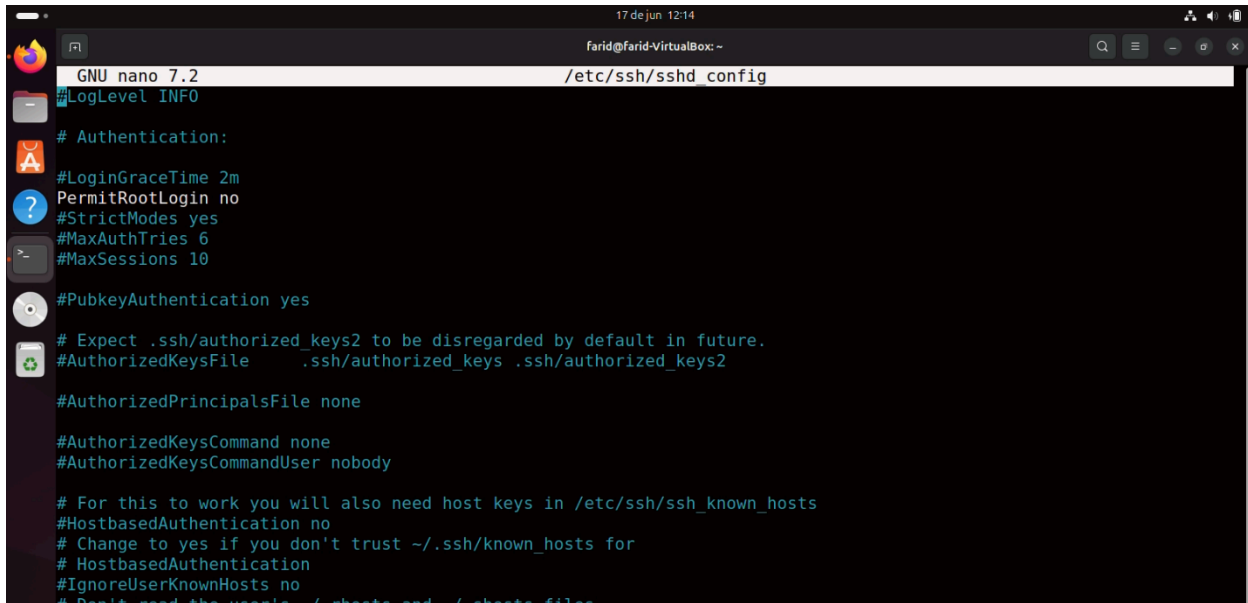
```

17 de jun 12:12
usuario@farid-VirtualBox: ~
farid@farid-VirtualBox:~$ su - usuario
Contraseña:
usuario@farid-VirtualBox:~$ passwd
Cambiando la contraseña de usuario.
Contraseña actual:
Nueva contraseña:
Vuelva a escribir la nueva contraseña:
passwd: contraseña actualizada correctamente
usuario@farid-VirtualBox:~$

```

### 3. SSH seguro

- Edita la configuración para deshabilitar login de root:
- `sudo nano /etc/ssh/sshd_config`
- # Cambiar o añadir:
- `PermitRootLogin no`



```

GNU nano 7.2 /etc/ssh/sshd_config
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
PermitRootLogin no
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#PubkeyAuthentication yes

# Expect .ssh/authorized_keys2 to be disregarded by default in future.
#AuthorizedKeysFile .ssh/authorized_keys .ssh/authorized_keys2

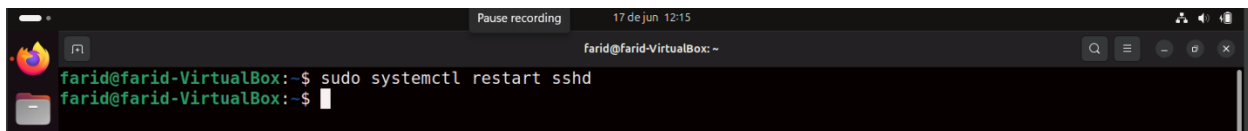
#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody

# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# HostbasedAuthentication
#IgnoreUserKnownHosts no
#Don't read the user's ~/.rhosts and ~/.shosts files

```

`sudo systemctl restart sshd`

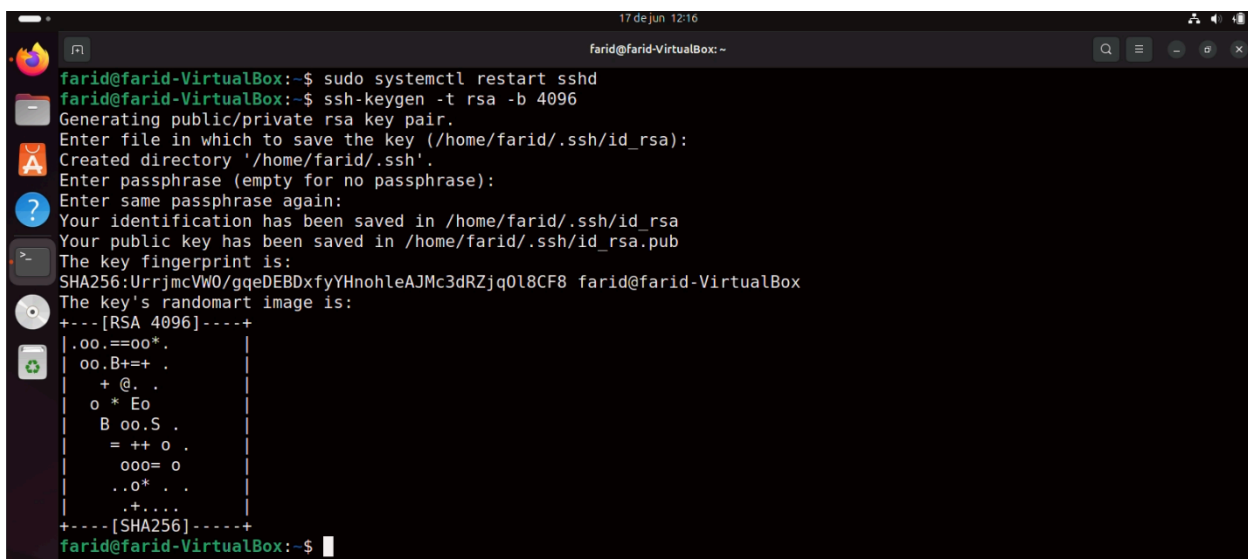


```

farid@farid-VirtualBox:~$ sudo systemctl restart sshd
farid@farid-VirtualBox:~$

```

- Autenticación por clave pública:
- `ssh-keygen -t rsa -b 4096`

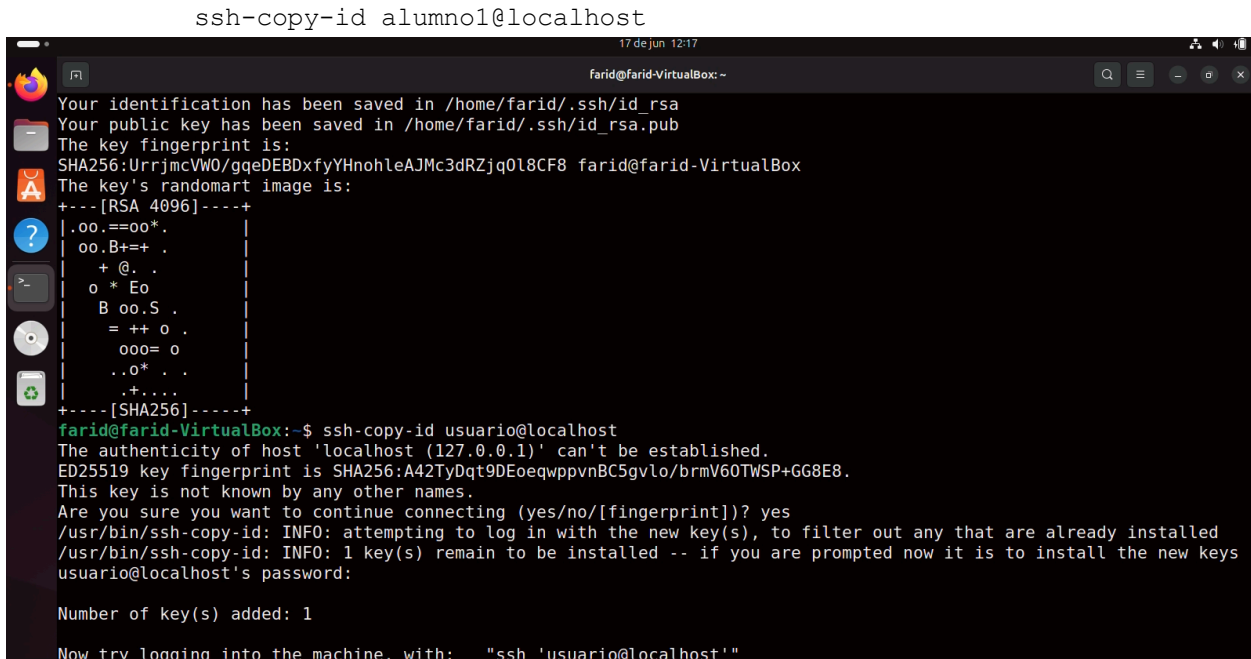


```

farid@farid-VirtualBox:~$ sudo systemctl restart sshd
farid@farid-VirtualBox:~$ ssh-keygen -t rsa -b 4096
Generating public/private rsa key pair.
Enter file in which to save the key (/home/farid/.ssh/id_rsa):
Created directory '/home/farid/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/farid/.ssh/id_rsa
Your public key has been saved in /home/farid/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:UrrjmcVW0/gqeDEBDxfyYHnohleAJMc3dRZjq0l8CF8 farid@farid-VirtualBox
The key's randomart image is:
+---[RSA 4096]-----+
|.oo.==oo*|.
|.oo.B+=+|.
|+@.|.
|o *Eo|.
|B oo.S|.
|= ++ o|.
|ooo= o|.
|..o*|.
|..+....|
+---[SHA256]-----+
farid@farid-VirtualBox:~$

```

```
ssh-copy-id alumno1@localhost
```



```

Your identification has been saved in /home/farid/.ssh/id_rsa
Your public key has been saved in /home/farid/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:UrrjmcVW0/gqeDEBDxfyYHnohleAJMc3dRZjq0l8CF8 farid@farid-VirtualBox
The key's randomart image is:
+---[RSA 4096]-----+
|.oo.=oo*|.
|oo.B+=+|.
|+@.|.
|o *Eo|.
|B oo.S|.
|=++o|.
|ooo= o|.
|..O*|.
|+. ....|
+---[SHA256]-----+
farid@farid-VirtualBox:~$ ssh-copy-id usuario@localhost
The authenticity of host 'localhost (127.0.0.1)' can't be established.
ED25519 key fingerprint is SHA256:A42TyDqt9DEoeqwppvnBC5gvlo/brmV60TWSP+GG8E8.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install the new keys
usuario@localhost's password:

Number of key(s) added: 1

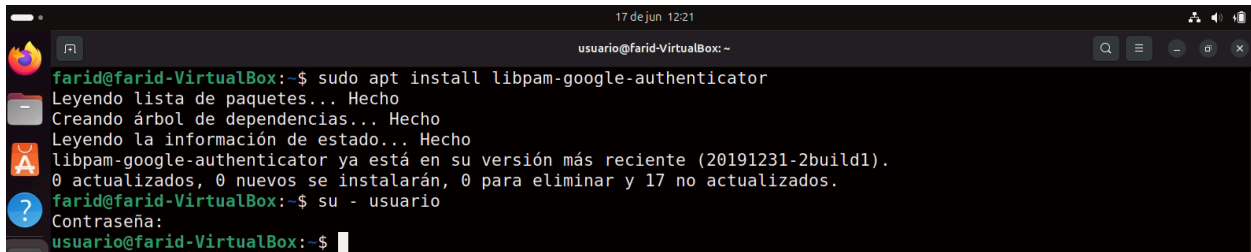
Now try logging into the machine, with: "ssh 'usuario@localhost'"

```

#### 4. Autenticación de dos factores (opcional)

- Instala el módulo PAM de Google Authenticator:

```
sudo apt install libpam-google-authenticator
```



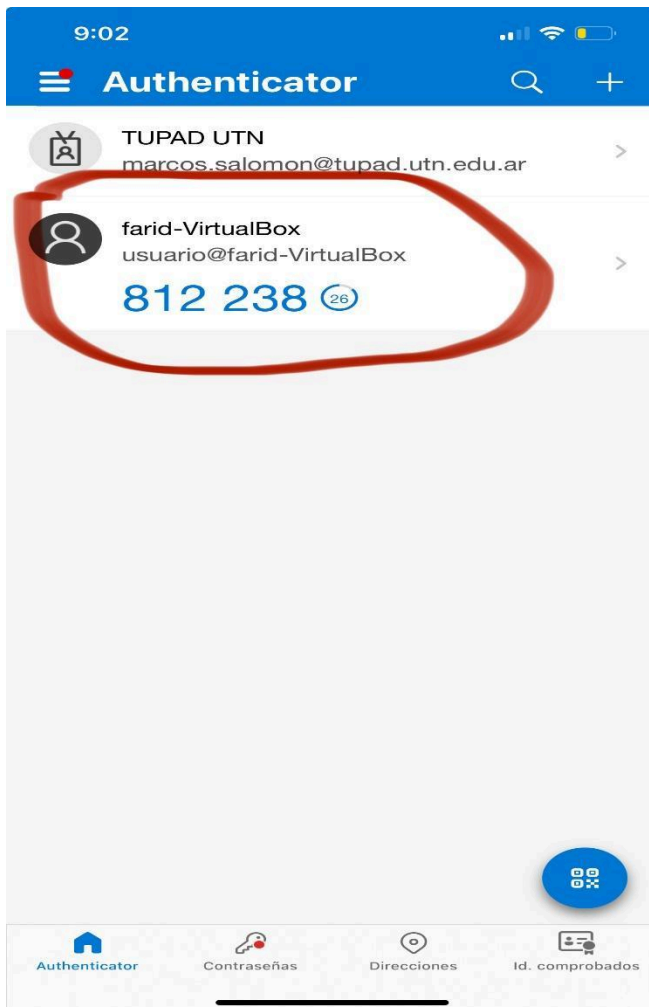
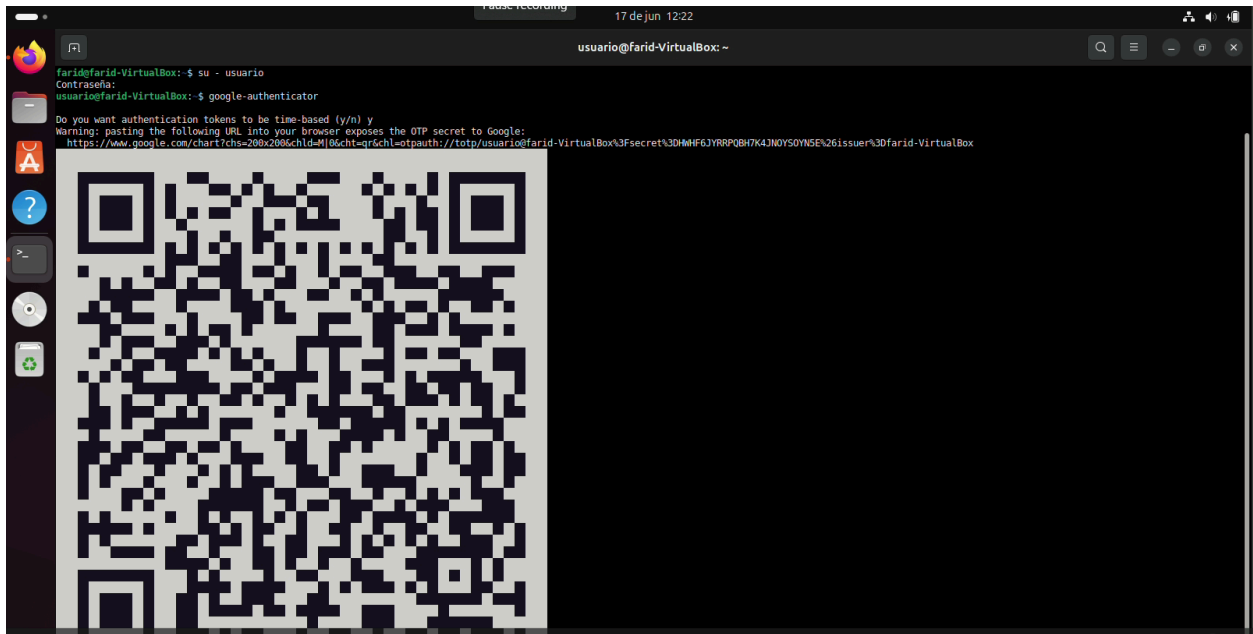
```

17 de jun 12:21
usuario@farid-VirtualBox: ~
farid@farid-VirtualBox:~$ sudo apt install libpam-google-authenticator
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
libpam-google-authenticator ya está en su versión más reciente (20191231-2build1).
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 17 no actualizados.
farid@farid-VirtualBox:~$ su - usuario
Contraseña:
usuario@farid-VirtualBox:~$

```

- Ejecuta como usuario1:

```
google-authenticator
```



## 6. Conclusiones

La combinación de firewalls, antivirus y monitoreo de actividad es esencial para mantener la seguridad de sistemas y redes. Mientras que el firewall actúa como una barrera de protección contra accesos no autorizados, el antivirus evita infecciones por malware y el monitoreo de actividad permite la detección temprana de amenazas. Implementar estas soluciones de manera conjunta es clave para una estrategia de ciberseguridad efectiva y proactiva.

Una adecuada configuración de seguridad en Linux es un pilar fundamental para la protección de los sistemas informáticos. En este proyecto hemos demostrado cómo, sin instalar paquetes adicionales, es posible reforzar la defensa de Ubuntu en VirtualBox mediante:

- **Reglas de firewall** con `iptables` o `firewalld` para filtrar tráfico entrante y saliente.
- **Gestión de permisos y roles de usuario**, asignando permisos con `chmod` y `chown`, y otorgando privilegios específicos con `sudo`.
- **Autenticación robusta**, incluyendo contraseñas fuertes, autenticación de dos factores y uso de claves SSH para acceder de forma segura.
- **Optimización de recursos**, deshabilitando servicios innecesarios y limitando uso de CPU/memoria con `ulimit`.

La implementación de estas medidas de forma integrada contribuye significativamente a reducir la superficie de ataque, prevenir incidentes de seguridad y mejorar la resiliencia de los sistemas frente a amenazas cibernéticas. A medida que las amenazas evolucionan, es crucial mantener y actualizar periódicamente la configuración de seguridad, asegurando así la estabilidad y confianza en el entorno de trabajo.

## 7. Bibliografía

- **The Linux Command Line** (William E. Shotts, Jr.) – guía completa de comandos y scripting en Linux.
- **Linux Security Cookbook** (Daniel J. Barrett, Richard Silverman, Robert G. Byrnes) – recetas prácticas para asegurar servicios y sistemas.
- **SELinux by Example** (Frank Mayer, Karl MacMillan, David Caplan) – para profundizar en Mandatory Access Control.
- **Linux Firewalls** (Michael Rash) – configuración avanzada con `iptables` y `firewalld`.
- **Documentación UTN**: "Apuntes de la Unidad de Seguridad en Sistemas Operativos" – apuntes del curso con ejemplos y prácticas.
- Artículos en línea:
  - "Securing Linux Servers" – Red Hat Security Blog (<https://www.redhat.com/en/blog>)
  - "Best Practices for SSH Hardening" – DigitalOcean Community (<https://www.digitalocean.com/community>)



## 8. Anexos

- A. Script `setup_basico.sh` con todos los comandos.
- B. Capturas de pantalla de las pruebas de permisos, sudo y SSH.
- C. Video Youtube: <https://www.youtube.com/watch?v=b1tnuIuGA4E>
- Github:  
<https://github.com/turkaym/Aquitectura-y-Sistemas-Operativos/tree/main/TP%20Integrador>
- D. Drive con evidencia del TP:  
[https://drive.google.com/drive/folders/1KX6zWLDZ3T-oxY2gqiNIItA7TVy8\\_fDRd?usp=sharing](https://drive.google.com/drive/folders/1KX6zWLDZ3T-oxY2gqiNIItA7TVy8_fDRd?usp=sharing)