

CURSO 2025/2026

ADMINISTRACIÓN REMOTA DE SISTEMAS EN RED

ASO

Objetivo de la actividad	2
Criterios de evaluación	2
Infraestructura	2
PARTE1 – Acceso remoto seguro por SSH	3
Servicio SSH.....	3
Usuario exclusivo para acceso SSH.....	3
Configuración inicial del acceso por clave	3
Configuración inicial del acceso por clave	4
Bloqueo del acceso por contraseña	5
Prueba final de acceso autorizado.....	6
Comprobación de acceso denegado	6
Documentación.....	6
Evidencias.....	6
PARTE2 – Administración remota gráfica (RDP).....	6
Habilitar escritorio remoto en el equipo	6
Usuario remoto dedicado para RDP.....	7
Permitir conexiones solo con autenticación de nivel de red	7
Acceso RDP desde Windows 11	7
Comprobación de acceso denegado	7
Documentación.....	7
Evidencias.....	7

Objetivo de la actividad

Configurar y utilizar **mecanismos reales de acceso y administración remota** entre sistemas **Windows y Linux**, aplicando **criterios de seguridad, usuarios dedicados, cifrado de las comunicaciones y documentación técnica**, propios de un entorno profesional.

Criterios de evaluación

Esta práctica evalúa los siguientes criterios del **RA4**:

- CE 4.3
- CE 4.4
- CE 4.5
- CE 4.6
- CE 4.7
- CE 4.8
- CE 4.9

Infraestructura

- **Windows Server 2025** (servidor)
- **Ubuntu Server 24.04** (servidor)
- **Windows 11** (equipo administrador)
- Red privada

Todas las conexiones se realizan **desde la máquina Windows 11**.

PARTE1 – Acceso remoto seguro por SSH

Configurar **acceso remoto seguro por SSH** a un servidor Linux, empleando un **usuario dedicado y autenticación por clave pública**. La conexión se realizará desde Windows 11 utilizando PuTTY (equipo administración).

Servicio SSH

Comprobar que el servicio SSH está instalado y activo en Ubuntu Server.

```
user@user-manager:~$ sudo apt install openssh-server
No VM guests are running outdated hypervisor (qemu) binaries on this host.
user@user:~$ sudo apt install openssh-server -y
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
openssh-server ya está en su versión más reciente (1:9.6p1-3ubuntu13.14).
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 0 no actualizados.
user@user:~$ sudo apt install openssh-server
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
openssh-server ya está en su versión más reciente (1:9.6p1-3ubuntu13.14).
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 0 no actualizados.
user@user:~$ sudo systemctl start ssh
user@user:~$ sudo systemctl enable ssh
Synchronizing state of ssh.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable ssh
Created symlink /etc/systemd/system/ssh.service → /usr/lib/systemd/system/ssh.service.
Created symlink /etc/systemd/system/multi-user.target.wants/ssh.service → /usr/lib/systemd/system/ssh.service.
user@user:~$
```

Usuario exclusivo para acceso SSH

Crear un usuario dedicado únicamente al acceso remoto por SSH, *remoto_ssh*. No se permite usar: root, administrador u otro usuario habitual.

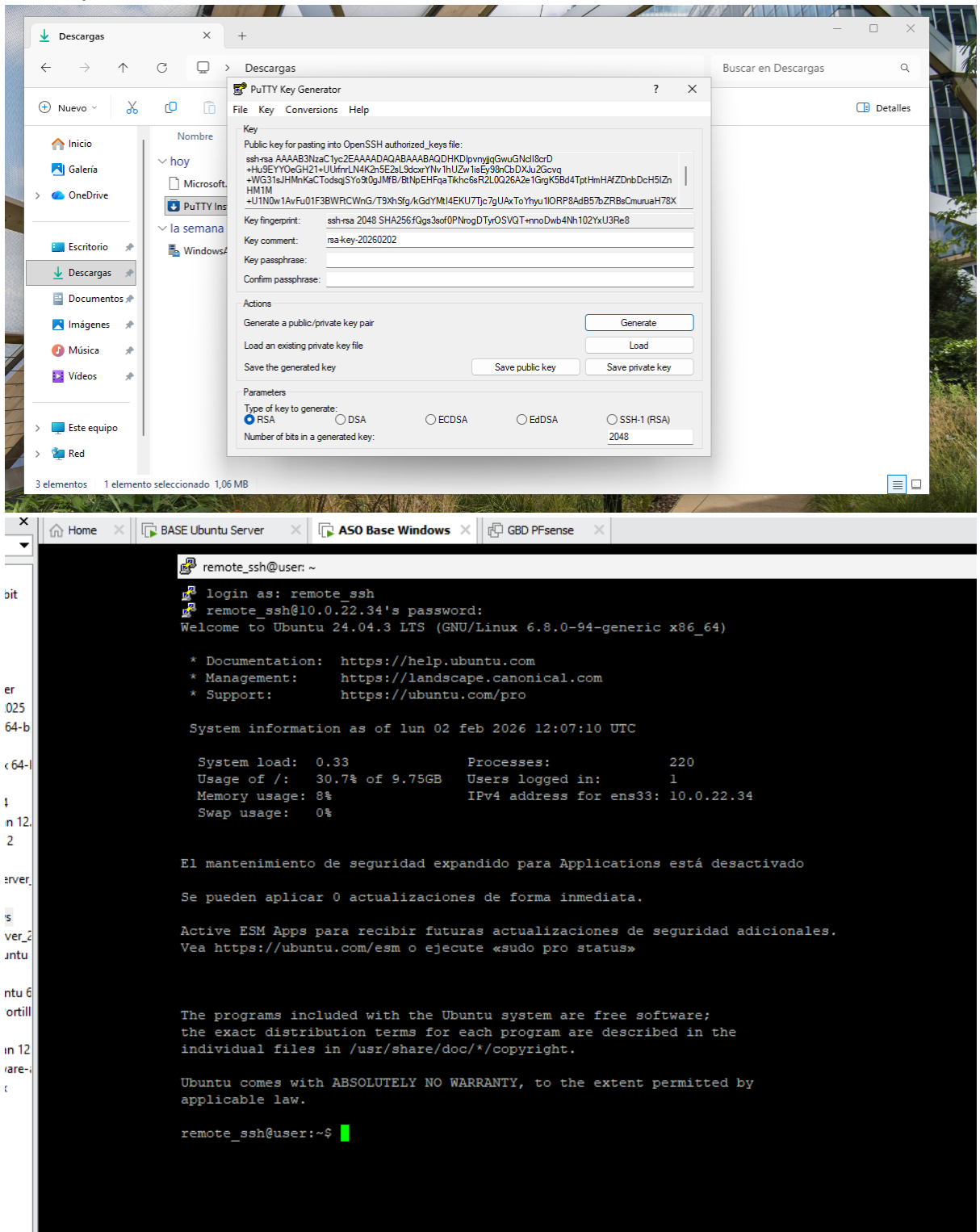
```
user@user:~$ sudo adduser remote_ssh
info: Adding user `remote_ssh' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `remote_ssh' (1001) ...
info: Adding new user `remote_ssh' (1001) with group `remote_ssh (1001)' ...
info: Creating home directory `/home/remote_ssh' ...
info: Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for remote_ssh
Enter the new value, or press ENTER for the default
  Full Name []:
    Room Number []:
    Work Phone []:
    Home Phone []:
    Other []:
Is the information correct? [Y/n] y
info: Adding new user `remote_ssh' to supplemental / extra groups `users' ...
info: Adding user `remote_ssh' to group `users' ...
user@user:~$
```

Configuración inicial del acceso por clave

Mientras la autenticación por contraseña siga permitida:

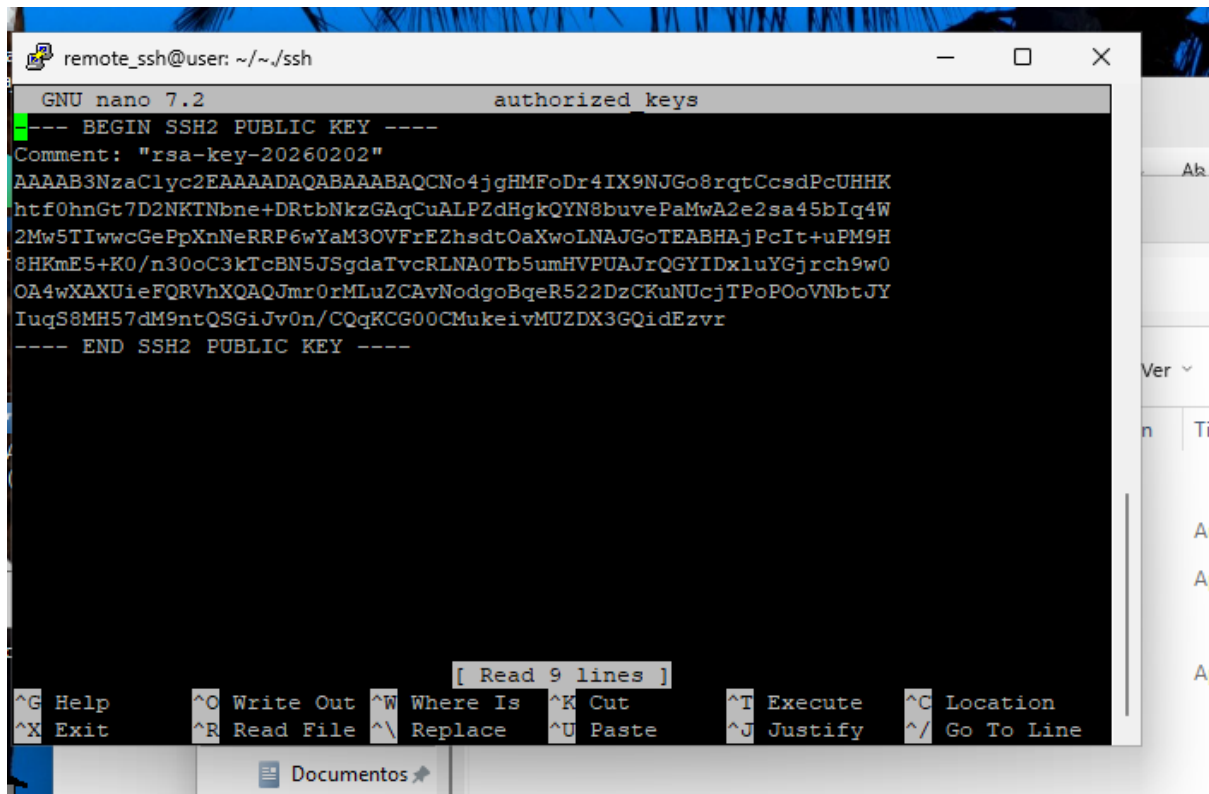
- Generar un par de claves en Windows 11
- Copiar la clave pública al servidor Ubuntu

- Configurar el usuario *remote_ssh* para que el servidor reconozca la clave pública



Configuración inicial del acceso por clave

Antes de aplicar medidas adicionales de seguridad, comprobar el acceso por ssh usando el usuario *remote_ssh* mediante clave pública. Verificar que el acceso funciona correctamente.

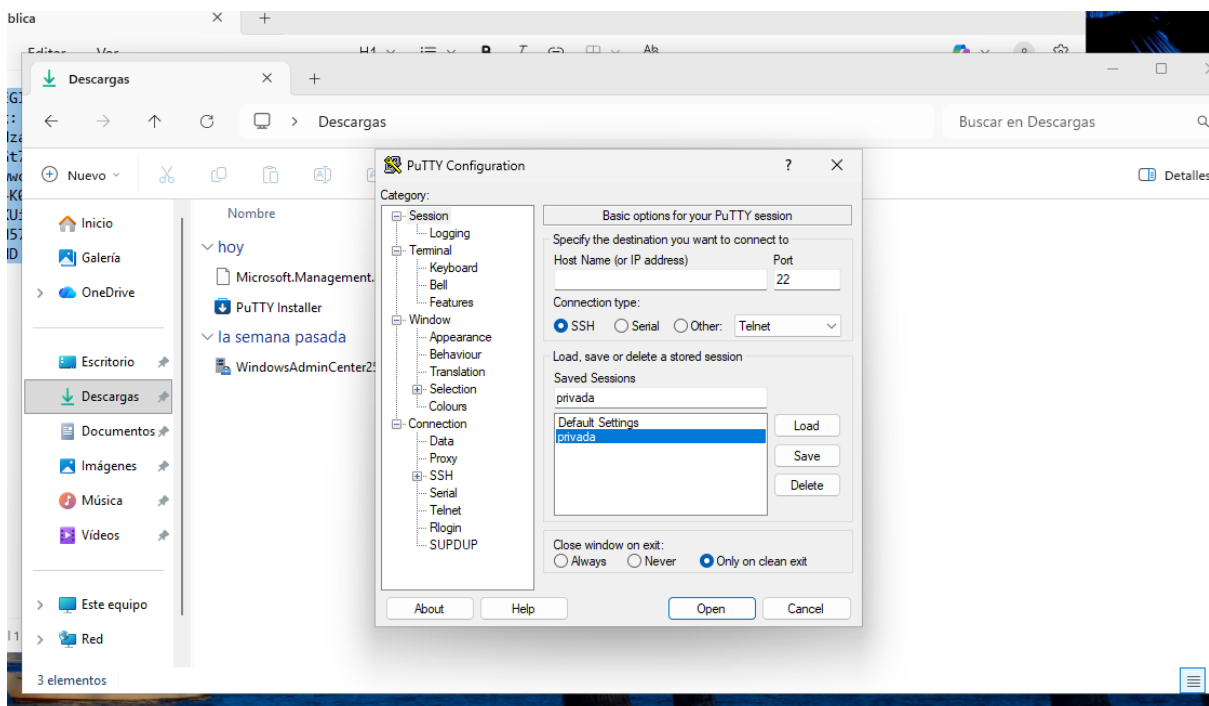


```
remote_ssh@user: ~/~/ssh
GNU nano 7.2 authorized_keys
--- BEGIN SSH2 PUBLIC KEY ---
Comment: "rsa-key-20260202"
AAAAB3NzaClyc2EAAAADAQABAAQCN04jgHMFoDr4IX9NJGo8rqtCcscPcUHHK
htf0hnGt7D2NKTnbne+DRtbNkzGAqCuALPZdHgkQYN8buvePaMwA2e2sa45bIq4W
2Mw5TIwccGePpXnNeRRP6wYam3OVFrEZhsdtOaXwoLNAJGoTEABHAjPcIt+uPM9H
8HKmE5+K0/n30oC3kTcBN5JSgdaTvcRLNA0Tb5umHVPUAJrQGYIDxluYGjrch9w0
OA4wXAXUieFORVhXQAQJmr0rMLuZCAvNodgoBqeR522DzCKuNUcjTPoPOoVNbtJY
IugS8MH57dM9ntQSGiJv0n/CQqKCG00CMukeivMUZDX3GQidEzvr
---- END SSH2 PUBLIC KEY ----
[ Read 9 lines ]
^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify   ^_ Go To Line
```

Bloqueo del acceso por contraseña

Una vez verificado que el acceso por clave funciona, deshabilitar la autenticación por contraseña en el servicio SSH.

Este paso debe realizarse **solo después** de comprobar el acceso por clave, para evitar perder el acceso al servidor.



Prueba final de acceso autorizado

Acceder al servidor Ubuntu desde PuTTY, demostrando que se utiliza el usuario *remoto_ssh*, no se solicita contraseña y el acceso se realiza mediante clave pública.

Comprobación de acceso denegado

Comprobar que otro usuario distinto de *remoto_ssh* NO puede acceder por SSH, al no disponer de clave pública configurada. Esto demuestra que la contraseña está bloqueada y el acceso está correctamente restringido.

Documentación

En Github crear una carpeta para la documentación de la práctica. En el readme incluir los datos relevantes de la práctica. Ejemplo:

```
## Acceso SSH

Usuario autorizado: remoto_ssh
Cliente: PuTTY
Autenticación: clave pública
Contraseña por SSH: deshabilitada
Usuarios no autorizados: acceso denegado
```

Evidencias

1. Usuario creado
2. Servicio SSH activo
3. Claves generadas. Captura donde se vean las claves generadas en el directorio final con los permisos adecuados.
4. Acceso por contraseña deshabilitado.
5. Acceso SSH desde PuTTY con *remoto_ssh*.
6. Acceso denegado a otro usuario. Captura del intento fallido con un usuario distinto de *remoto_ssh*.

PARTE2 – Administración remota gráfica (RDP)

Administrar un **Windows Server** de forma remota desde **Windows 11**, utilizando **RDP**, con **control explícito del acceso mediante usuarios dedicados**.

Habilitar escritorio remoto en el equipo

En Windows Server, habilitar el escritorio remoto para permitir conexiones remotas a la máquina.

<https://learn.microsoft.com/es-es/windows-server/remote/remote-desktop-services/remotepc/remote-desktop-allow-access>

Usuario remoto dedicado para RDP

Crear un usuario exclusivo *remoto_rdp* para acceso por escritorio remoto y añadirlo al grupo *Usuarios de Escritorio remoto*. No usar el usuario Administrador.

<https://learn.microsoft.com/es-es/windows-server/identity/ad-ds/manage/understand-security-groups>

Permitir conexiones solo con autenticación de nivel de red

Habilitar la autenticación de nivel de red (NLA) para agregar una capa adicional de seguridad en las conexiones de escritorio remoto.

Acceso RDP desde Windows 11

Desde el equipo Windows 11, acceder al Windows Server mediante escritorio remoto usando únicamente el usuario dedicado creado, *remoto_rdp*. Comprobar que la sesión gráfica funciona correctamente.

Comprobación de acceso denegado

Comprobar que otro usuario distinto de *remoto_rdp* NO puede acceder por RDP. Esto demuestra que el acceso está correctamente restringido.

Documentación

En Github en la carpeta para la documentación de la práctica. En el readme incluir los datos relevantes de la práctica. Ejemplo:

```
## Acceso RDP

Usuario RDP: rdp_srv
Sistema administrado: Windows Server 2022
Protocolo: RDP
Grupo de acceso: Usuarios de Escritorio remoto
Cifrado: Sí
```

Evidencias

1. Usuario *remoto_rdp* creado y añadido al grupo. Captura donde se vea el usuario dentro del grupo Usuarios de Escritorio remoto.
2. Autenticación de nivel de red para la conexión habilitada.
3. Sesión RDP activa donde se vea escritorio del servidor y usuario *remoto_rdp* conectado.
4. Acceso denegado a otro usuario. Captura del intento fallido con un usuario distinto de *remoto_rdp*.