Casos pràctics:

Administració remota basada en la linea d'ordres.

CAS PRÀCTIC 1: **Instal·lació de servei ssh**.

Objectiu general: Instal·lar el servei ssh (openssh) al servidor Ubuntu.

Accions a fer:

1. Instal·leu el programa client i el servidor SSH: *openssh-server*.

2. Accediu al terminal del equip remot. Quina pregunta apareixerà la primera vegada que us connecteu a l'equip remot?

3. Escolliu un fitxer de l'equip local i copieu-lo a l'equip remot. Documenteu les accions realitzades.

CAS PRÀCTIC 2: **Inici de sessió ssh amb autenticació per contrasenya**

Objectiu general: Comprovar el procés d'una connexió ssh autenticada amb contrasenya.

Accions a fer:

1. Assegureu-vos que al servidor ssh el fitxer /etc/ssh/sshd_config conté:

   Port 22
   Protocol 2
   HostKey /etc/ssh/ssh_host_rsa_key
   PubkeyAuthentication yes
   PasswordAuthentication yes
   X11Forwarding yes

2. Què indiquen cadascuna de les línies?

3. Assegureu-vos que al client ssh el fitxer /etc/ssh/ssh_config conté:
   Host *

   Port 22 Protocol 2
   StrictHostKeyChecking ask
   PasswordAuthentication yes
   IdentityFile ~/.ssh/id_rsa
   ForwardX11 yes

4. Què indiquen cadascuna de les línies?
5. Inicia la connexió ssh: ssh usuari@www.serveisM07.net

6. Documenteu les accions que heu fet en aquesta primera connexió.

7. Documenteu les accions a fer en successives connexions.

CAS PRÀCTIC 3: Inici de sessió ssh amb autenticació de clau pública.

Objectiu general: Comprovar el procés d'una connexió ssh autenticada per clau pública.

Accions a fer:

1. Generar al client les claus pública-privada: ssh-keygen -t rsa

2. Copieu la clau pública a al directori de l'usuari1 al servidor, a l'arxiu ~/.ssh/authorized_keys. Tanqueu la connexió.

3. Connecteu-vos ara i documenteu les passes.