Configuración de la Casa LANnister.

David Tardío Montoya, 2 GM B, para Servicios en Red (Sistemas Microinformáticos y Redes).

Índice de imágenes

[Configuración Windows 7 1](#_Toc86335504)

[XFCE: IP y nombre- Administrador 2](#_Toc86335505)

[Debian 10: IP y nombre- Bastión 2](#_Toc86335506)

[Debian 10: IP y nombre- Interno 2](#_Toc86335507)

[SSH-keygen 3](#_Toc86335508)

[Creación del archivo Authorized Keys 3](#_Toc86335509)

[Archivo configurado 4](#_Toc86335510)

[Cambiado correctamente 4](#_Toc86335511)

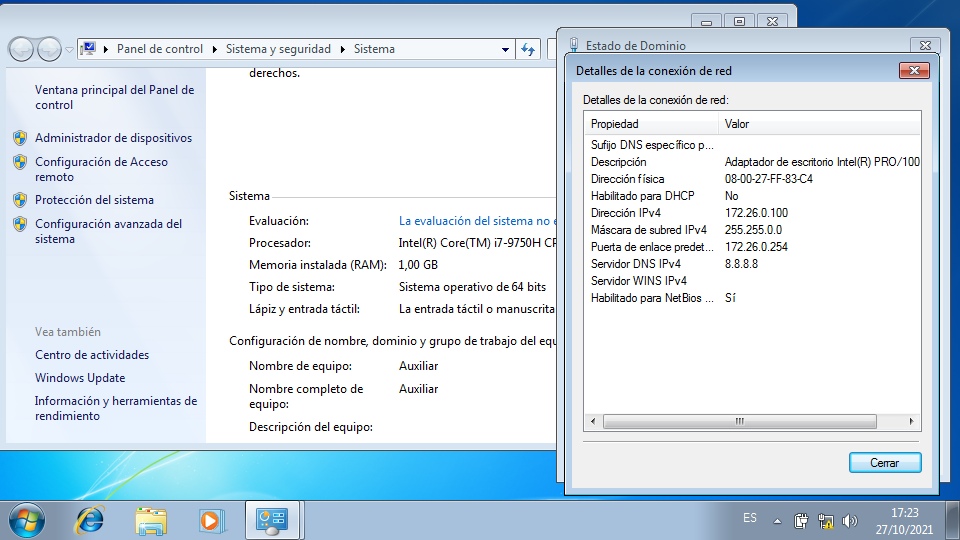
[Configuración de sshd\_config 5](#_Toc86335512)

[Mensaje de ssh 5](#_Toc86335513)

Empezaremos creando 4 máquinas virtuales: Un Debian XFCE, un Windows 7, y 2 Debian 11. El XFCE se llamará Administrador, un Debian 11 se llamará Bastión, el otro Debian 11 se llamará Interno, y el Windows 7 se llamará Auxiliar.

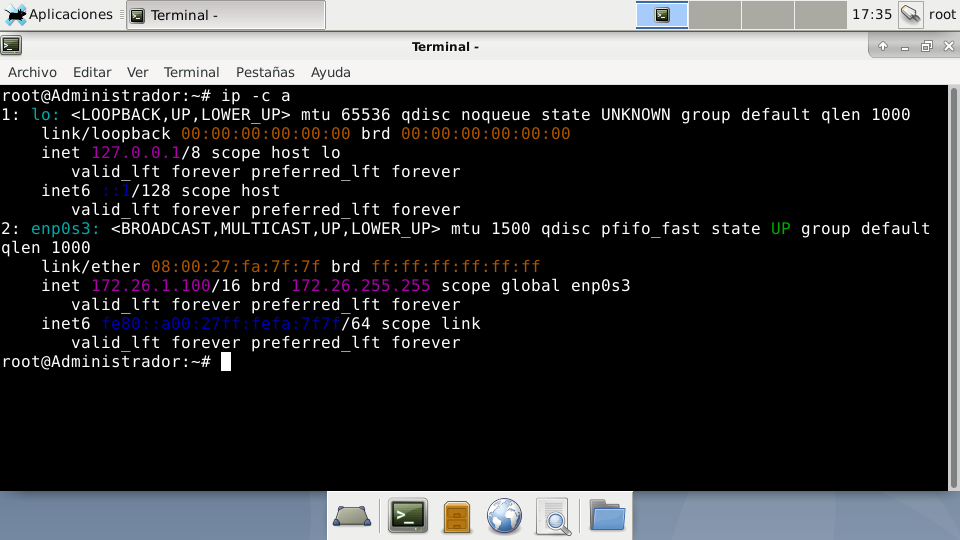
Auxiliar, Administrador y Bastión estarán conectados a una red NAT, mientras que Interno y Bastión estarán conectados a una red interna. Bastión contará con dos tarjetas de red.

Ahora, configuraremos el Windows 7. Le pondremos de nombre “Auxiliar”, y le pondremos la IP requerida.

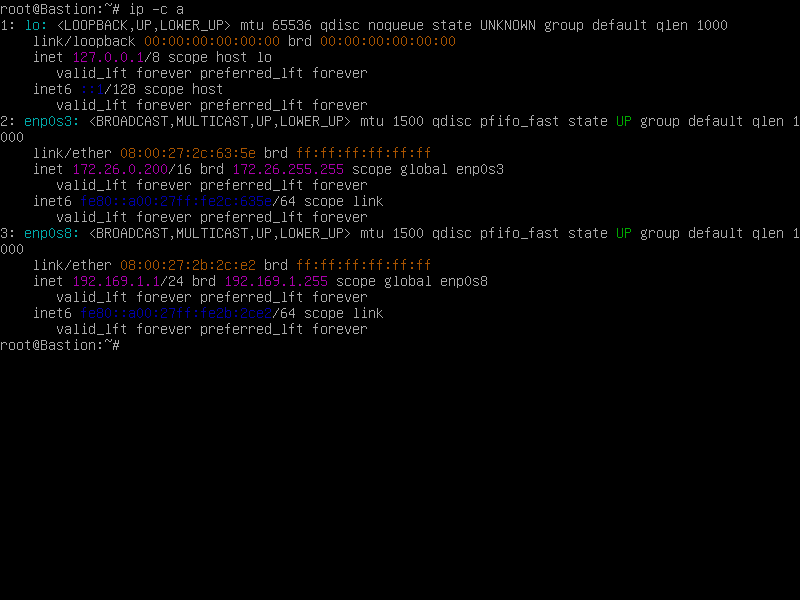


### Configuración Windows 7

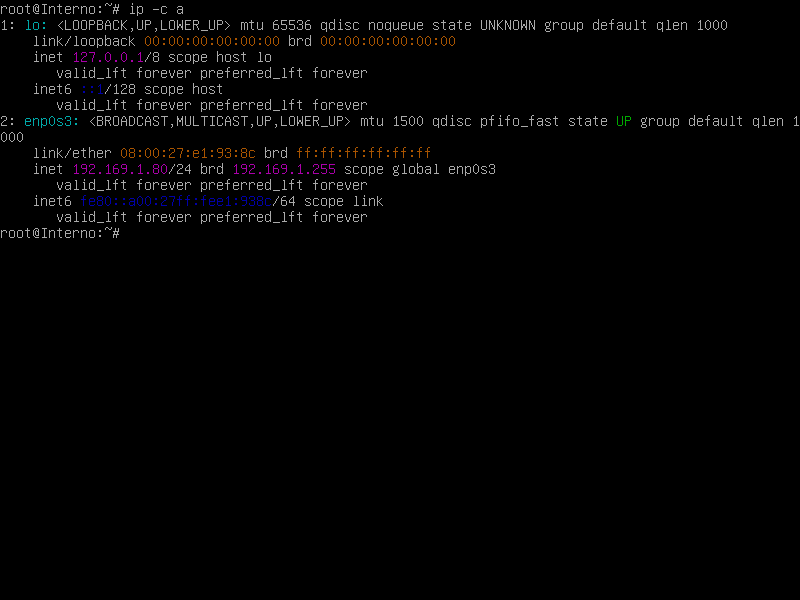
A continuación, configuraremos el resto de máquinas con sus nombres e IPs correspondientes.



### XFCE: IP y nombre- Administrador

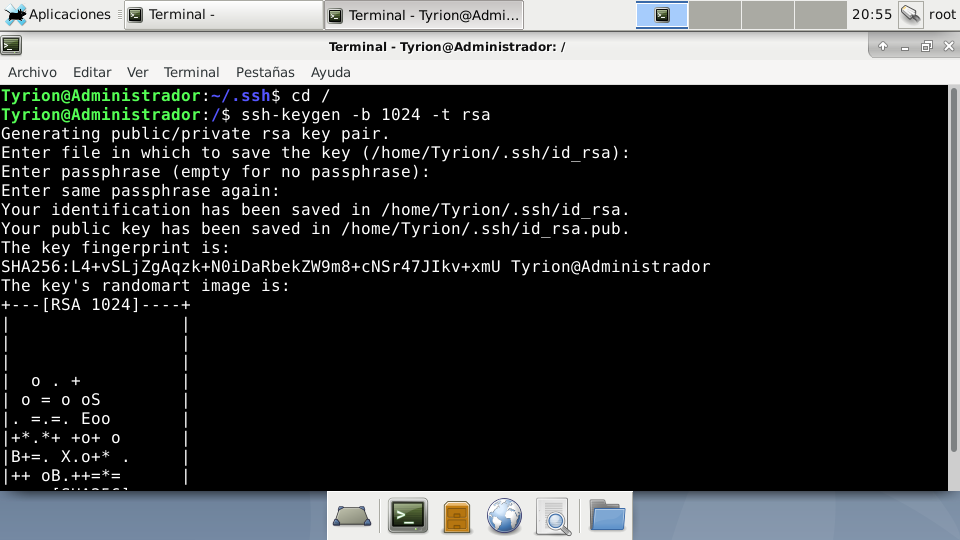


### Debian 10: IP y nombre- Bastión



### Debian 10: IP y nombre- Interno

A continuación, se crearán los usuarios Jaime y Tyrion en sus respectivas máquinas. Para ello, se usará la interfaz gráfica para aumentar la productividad. También configuraremos el SSH en Bastión e Interno. Para ello, nos aseguraremos de tener instalado SSH en Bastión, y en Administrador, y usaremos el comando *ssh-keygen -b 1024 -t rsa* dentro del cliente*.* Además, crearemos los usuarios Jaime y Tyrion en Bastión e Interno.



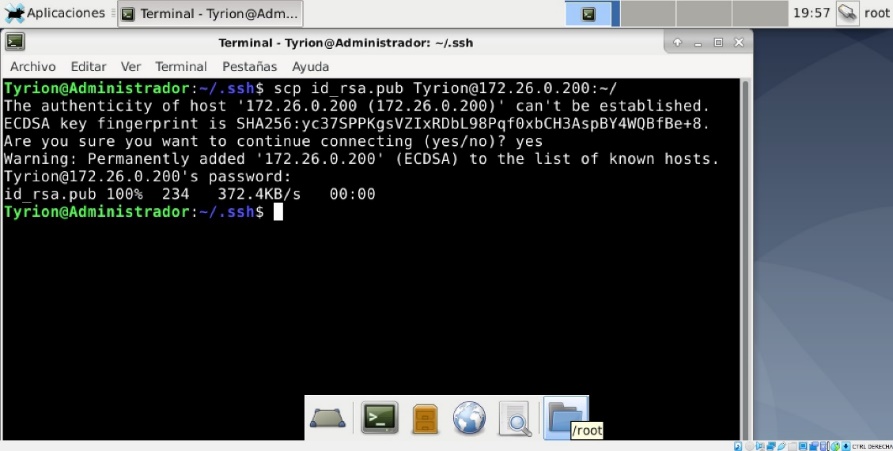
### SSH-keygen

Tras esto, accedemos al archivo ~/.ssh en el servidor SSH (Bastión), y crearemos un documento llamado “authorized\_keys”. Hecho esto, iremos al cliente (Tyrion).



### Creación del archivo Authorized Keys

En el cliente, iremos al directorio ~/.ssh, y usaremos el comando *scp id\_rsa-pub* [*Tyrion@172.26.0.200:~/*](mailto:Tyrion@172.26.0.200:~/).



### Archivo configurado

Ahora volveremos al servidor, iremos al directorio .ssh, ( tras haber iniciado sesión como Tyrion) y usaremos el comando *cat id\_rsa.pub >> ~/.ssh/authorized\_keys.*

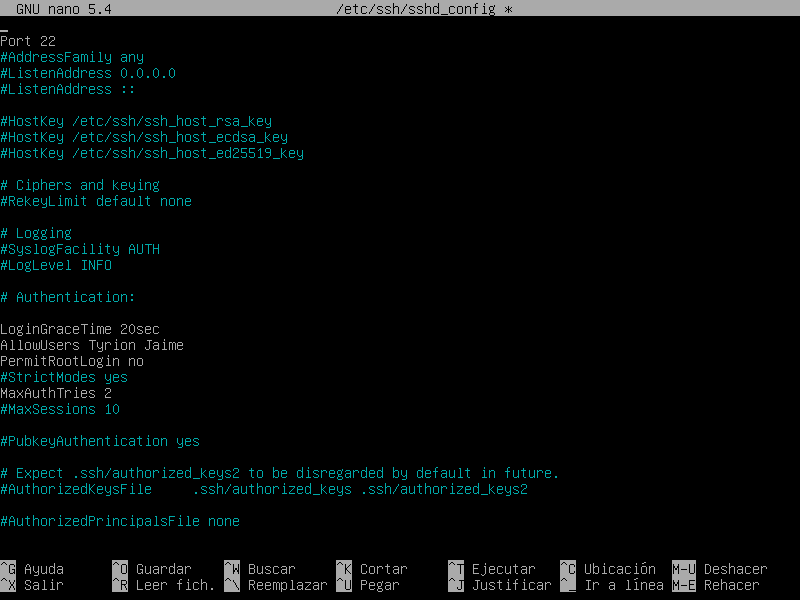


### Cambiado correctamente

Tras esto, podremos acceder al SSH desde Administrados sin necesidad de usar contraseña.

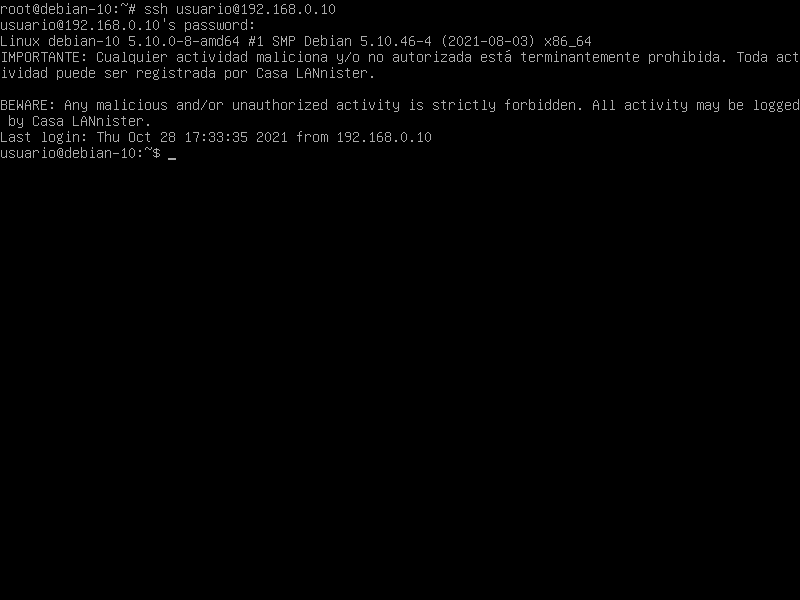
**Nota importante: a partir de este punto, todas mis máquinas virtuales, y todo el progreso en ellas se perdieron por motivos que desconozco, por lo que usaré “simulaciones” en máquinas creadas para ilustrar la explicación.**

Ahora, tendremos que entrar en Bastión en el documento /etc/ssh/sshd\_config, y modificar cosas como “PermitRootLogin no”, entre otras cosas.



### Configuración de sshd\_config

A continuación, haremos que aparezca un mensaje al conectarse por ssh. Para ello, entraremos en sshd\_config, y bajaremos hasta donde dice “Banner”. Ahí pondremos una ruta de un documento que crearemos, en el que pondremos el mensaje que deseemos. Además, podemos editar el archivo /etc/motd con nano para poder editar el mensaje.



### Mensaje de ssh

Al haber habilitado las claves de acceso, sólo Tyrion debería poder conectarse sin necesidad de contraseña, mientras que Jaime, teóricamente, necesitará utilizarla.