CLAVE RSA EN DRAGO CON PUTTY

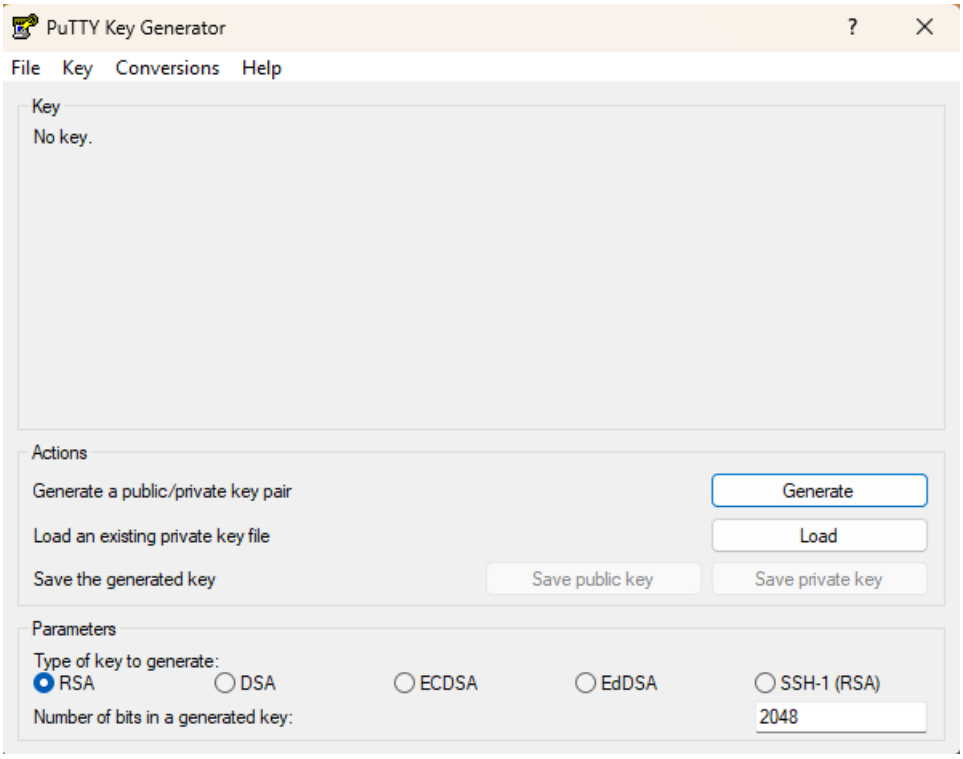
Dependiendo de la plataforma utilizada (Windows, Mac o Linux) para conectarse al HPC Drago, los pasos generales a seguir para la generación y uso de una clave RSA están publicados en el Portal Documentación AIC (SGAI)

https://docaic.rstools.csic.es/es/home

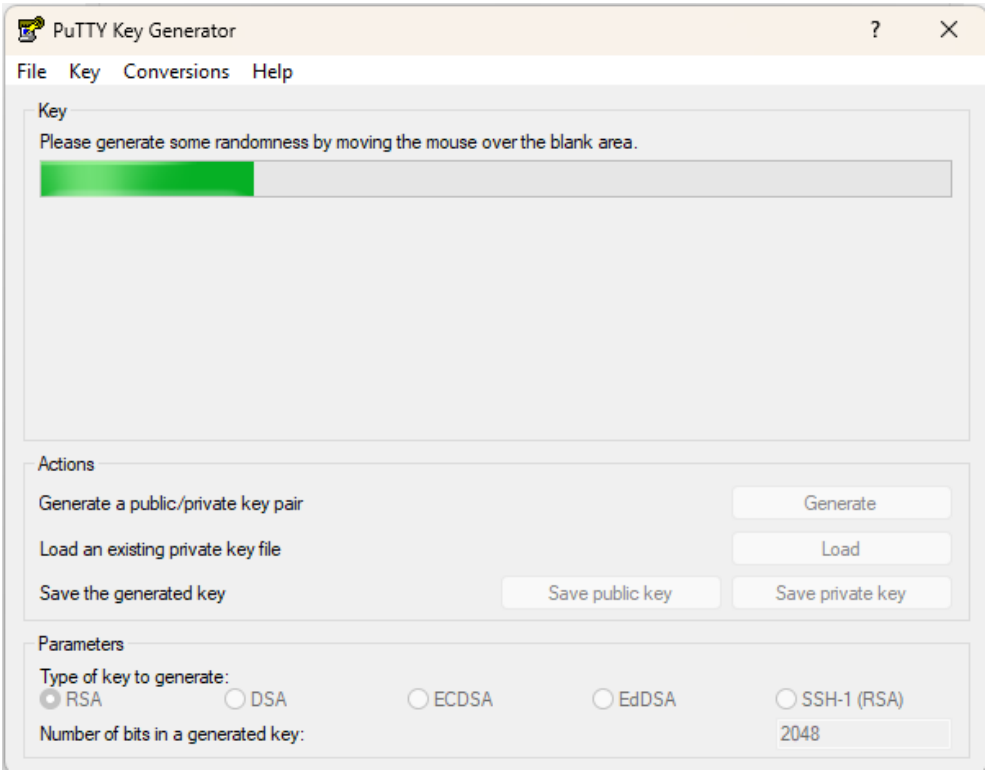
Este manual explica los pasos específicos a seguir en este proceso para realizarlo mediante el uso del software PuTTY/PuTTYgen que el usuario debe tener instalado en el PC.

1. GENERACION DE LAS CLAVES

El primer paso consiste en generar las claves publica (la que se copia en Drago) y privada (la que el usuario utiliza para identificarse) mediante PuTTYgen. Para ello, abrimos el software y presionamos el botón de “Generate”

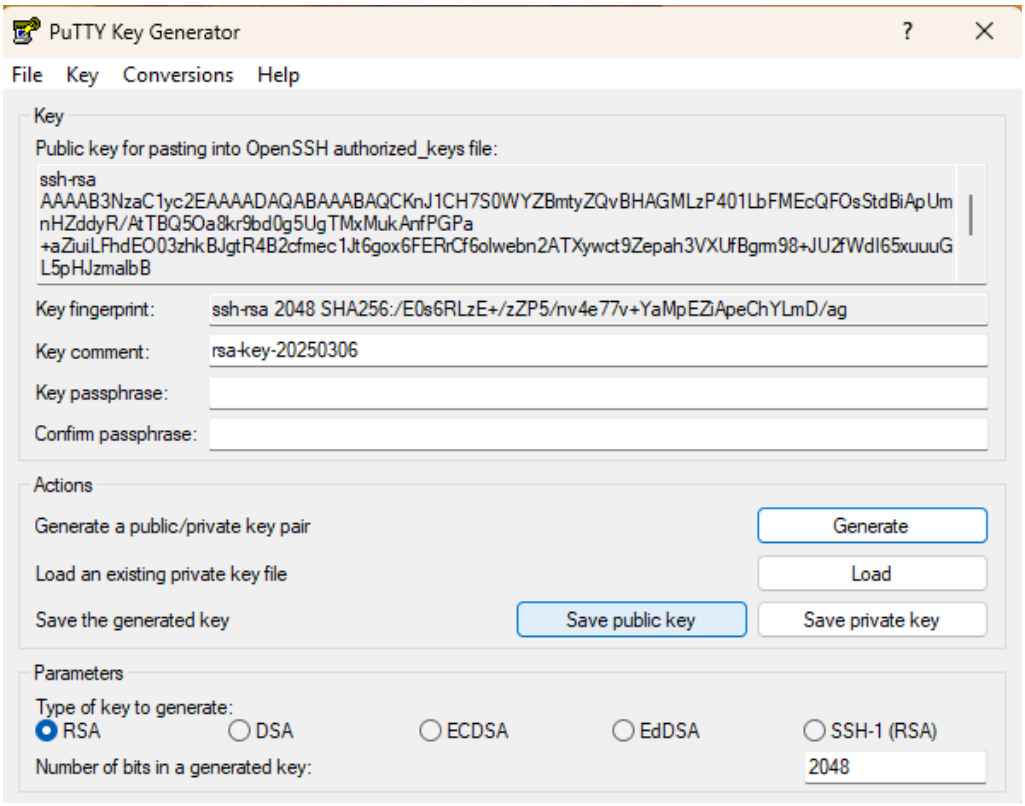


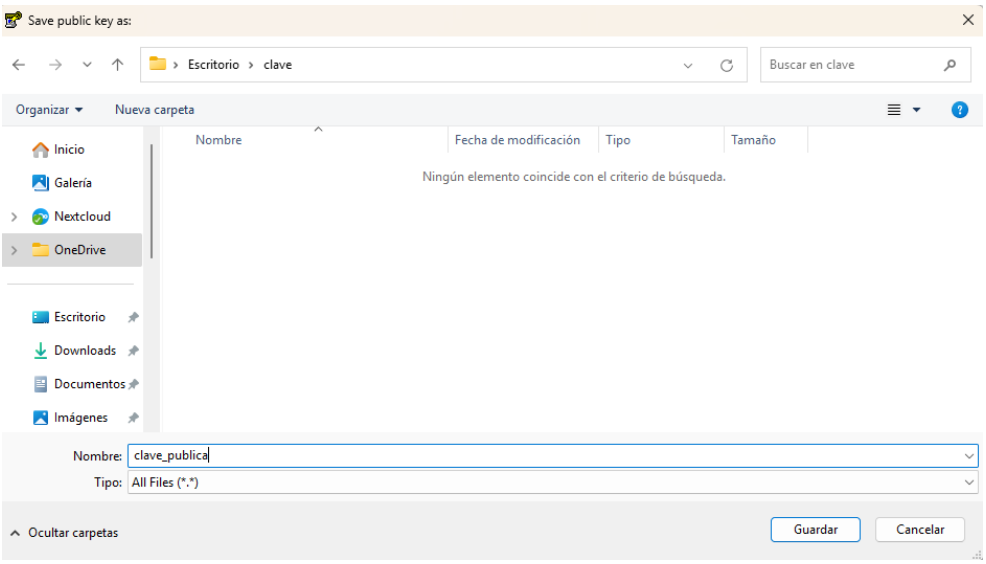
A continuación, se abrirá una ventana en la que debemos mover el ratón de forma aleatoria para que se vayan generando las claves.



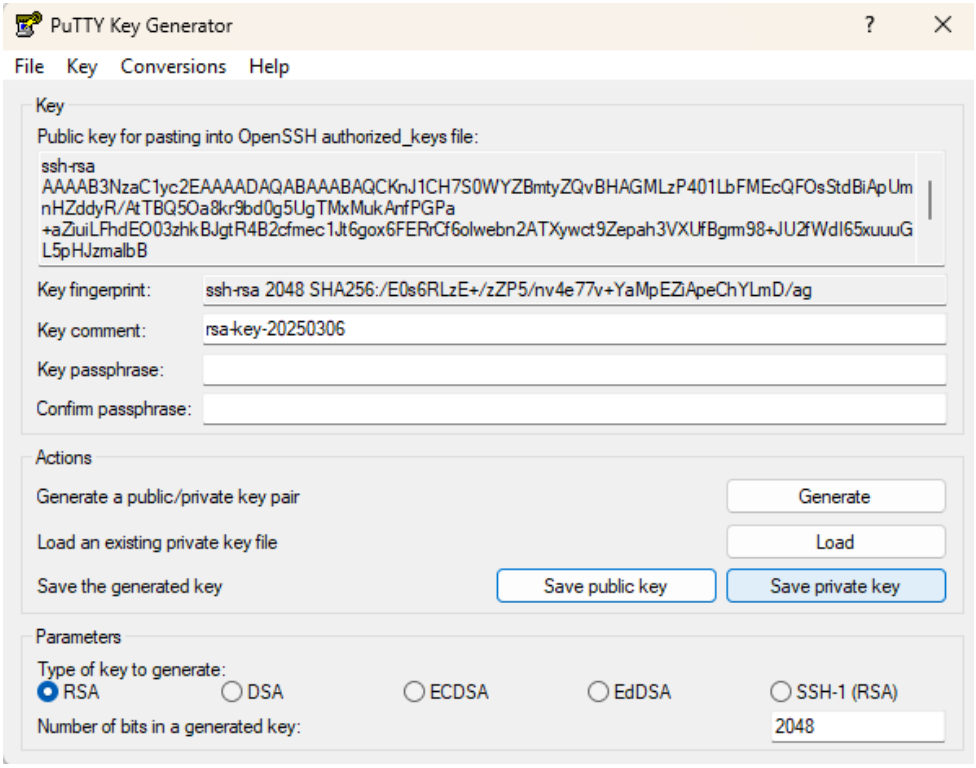
Una vez generadas las claves, que aparecen en el apartado “Key” de la ventana, es necesario exportar ambas claves (pública y privada) a sendos ficheros.

Para guardar la clave publica, pulsamos sobre el botón “Save public key” y guardamos la clave con el nombre de fichero que nos permita reconocerlo.





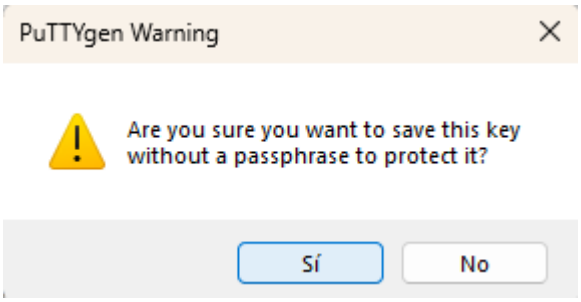
Para guardar la clave privada, pulsamos sobre el botón “Save private key”



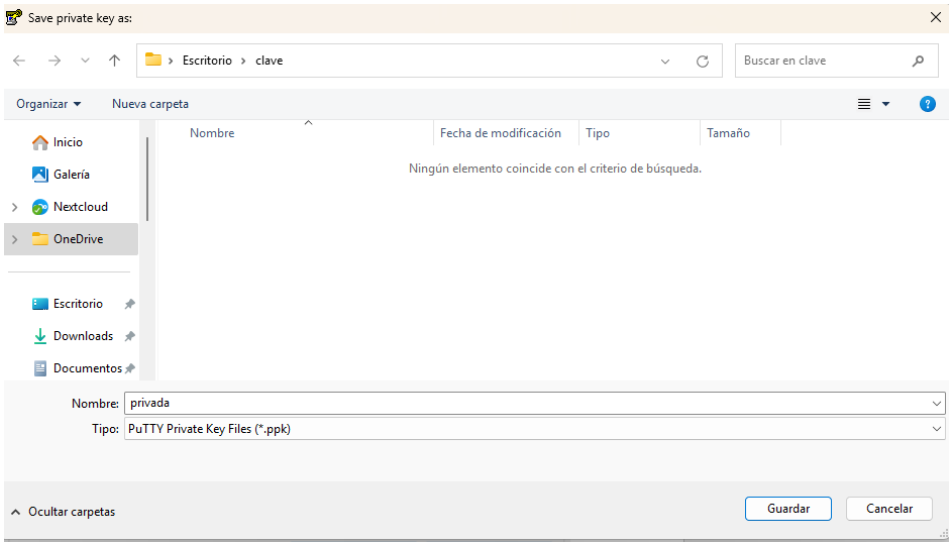
En este caso, dado que la clave privada únicamente debe tenerla y usarla el usuario que se identifica, se puede proteger mediante una contraseña rellenando el apartado de “Key passphrase” y su réplica “Confirm passphrase”.

Hay que tener en cuenta que esta contraseña será necesario introducirla cada vez que se utilice la clave para identificarse por lo que, si estamos en un PC que solo utilizamos nosotros, se puede dejar en blanco. En caso contrario, es recomendable rellenarlo para evitar que otros usuarios se identifiquen en Drago con nuestro

usuario. Si la “Key passphrase” se deja vacía, el programa nos preguntara si queremos seguir sin esa protección.



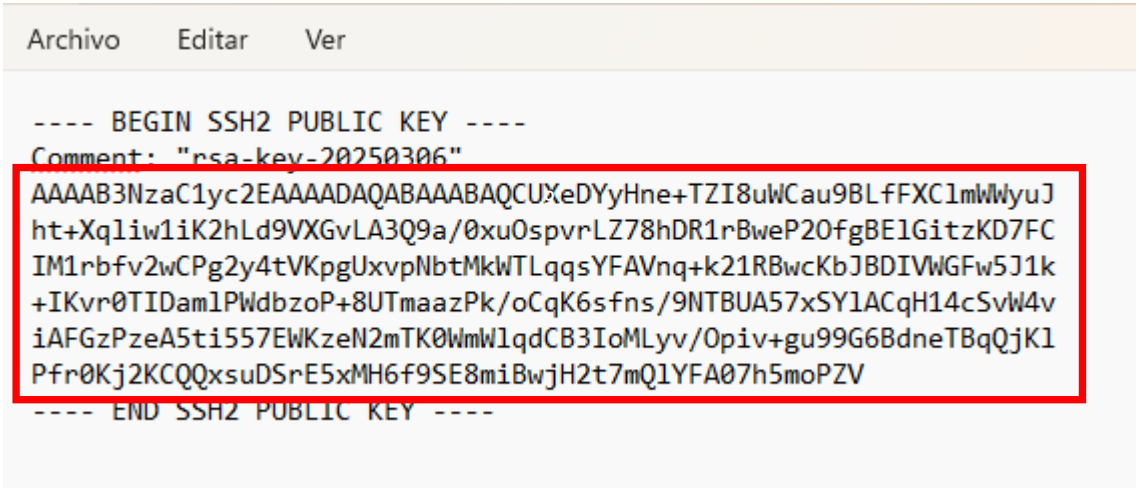
A continuación, guardamos la clave con el nombre de fichero que nos permita reconocerlo.



2. CONFIGURACION DE LA CLAVE EN DRAGO

Una vez disponemos de las claves, es necesario copiar la clave publica en nuestro usuario de Drago. Para ello:

- En nuestro PC, abrimos el fichero con la clave publica que hemos generado con el Notepad y copiamos únicamente la clave (en la imagen, sería lo que está dentro del recuadro rojo)



- Iniciamos sesión en Drago
- Nos aseguramos de estar en nuestra carpeta home con el comando

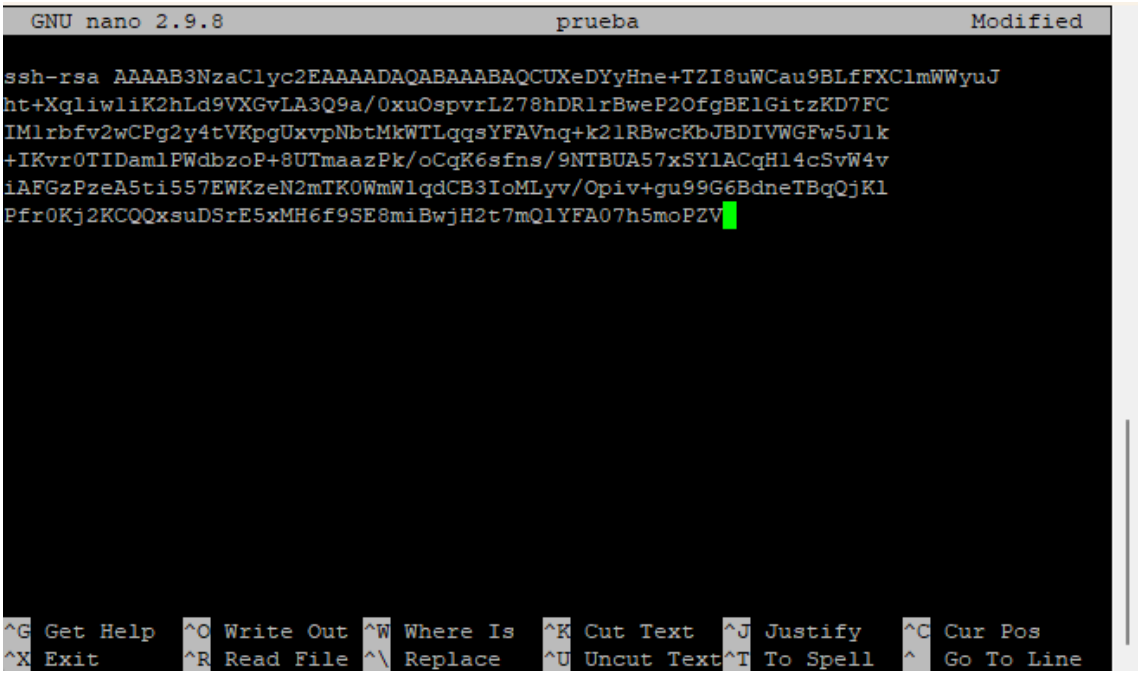
```
cd
```

- Ejecutamos el siguiente comando

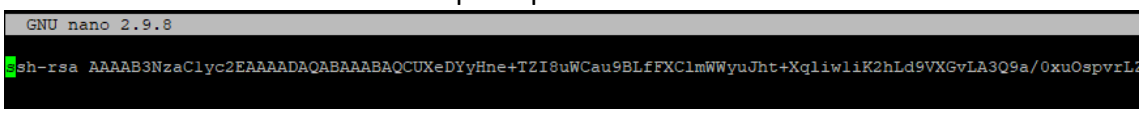
```
nano .ssh/authorized_keys
```

Esto abrirá el fichero “authorized_keys” si existe. Si no existe, se creará al editarlo y guardarlo.

- En este editor, comenzamos escribiendo una nueva línea con “ssh-rsa ” y a continuación, pegamos la clave que previamente hemos copiado



- Eliminamos los saltos de línea para que todo esté en una única línea

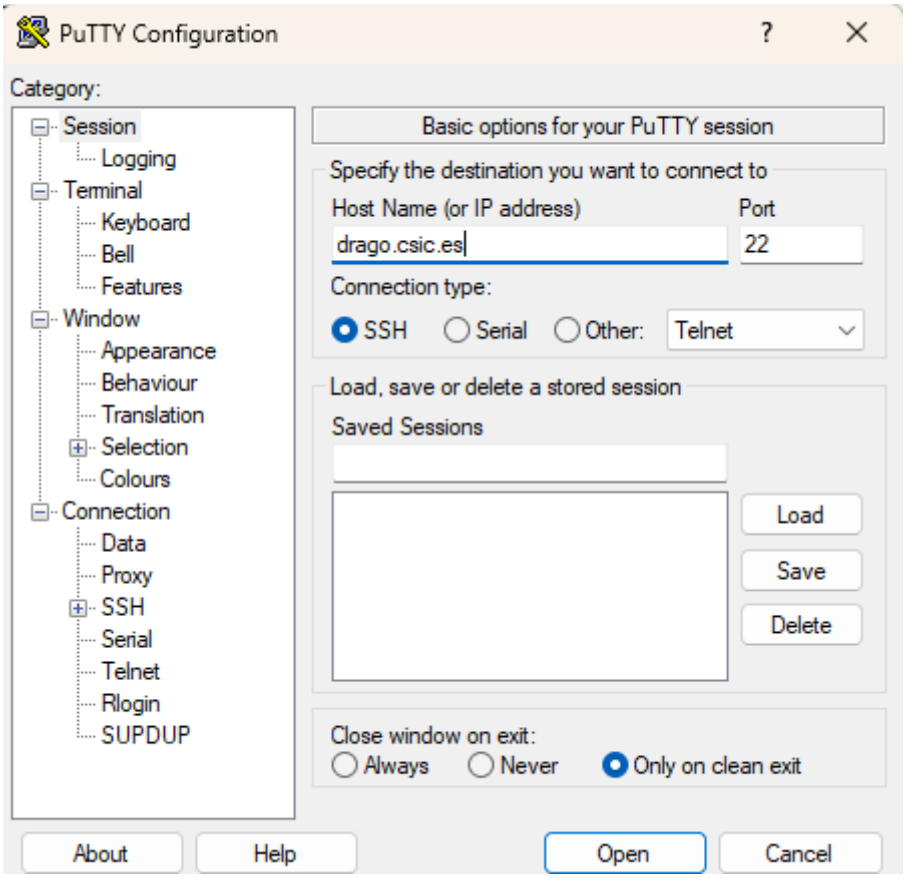


- Guardamos el fichero y salimos del editor.
- Modificamos los permisos del fichero para que solo pueda acceder el propietario mediante el comando

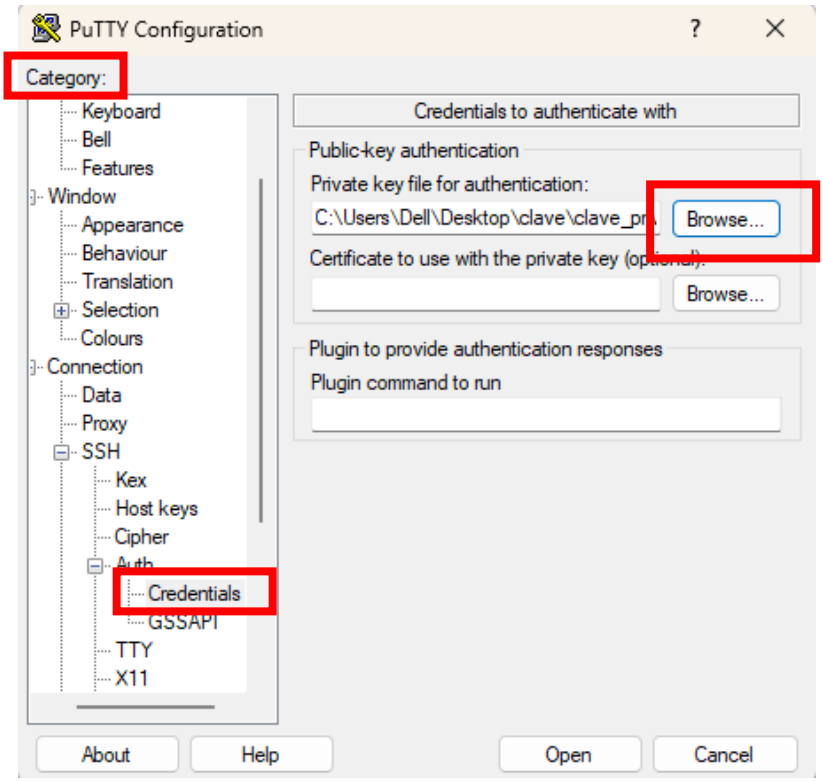
```
chmod 600 .ssh/authorized_keys
```

3. CONFIGURACION DE LA SESION EN PUTTY

Una vez disponemos de la clave publica en Drago, solo es necesario configurar nuestra sesión en PuTTY para conectarnos. Para ello, abrimos el PuTTY y rellenamos los datos de la sesión.

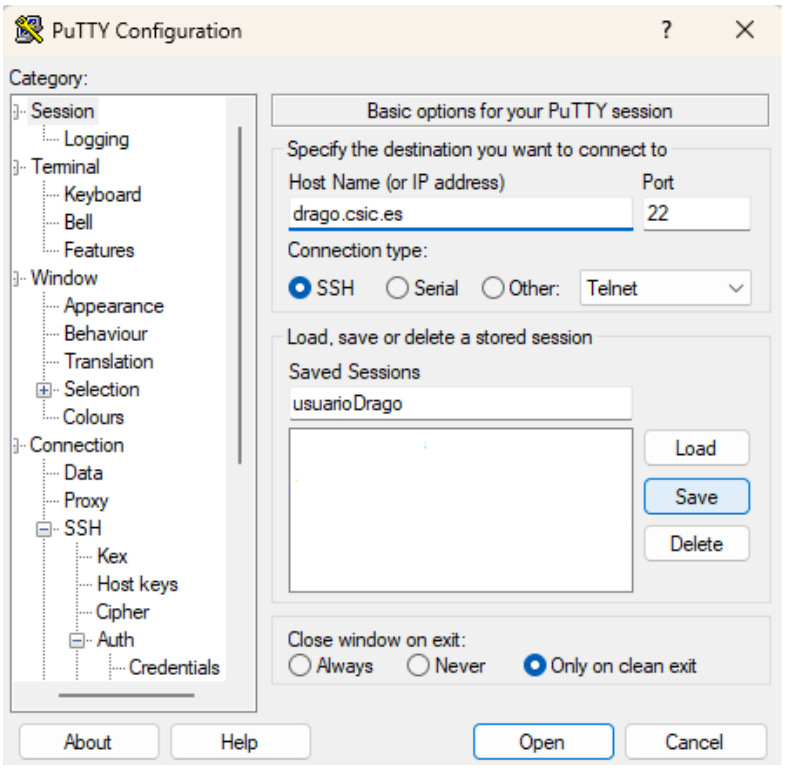


Configuramos la clave privada, seleccionando “Connection / SSH / Auth / Credentials” en la ventana de “Category”



Y pulsamos sobre le boto “Browse” en “Private key file for authenticate”. Esto nos permite seleccionar el fichero donde se encuentra almacenada la clave privada.

Una vez seleccionado, volvemos a la pestaña de “Session” y guardamos la configuración de la sesión con un nombre.



Y pulsamos sobre “Open” para conectarnos a Drago mediante la clave RSA.