

**MANUAL DE CONFIGURACIÓN DEL CLIENTE**

Administración de Servicios en Red

Equipo 5:

Campos Gómez Fernanda Ivette

Hernández López César Erick

Ruiz Pérez Alejandro

# 

# 

# ÍNDICE

[**CLIENTES GRÁFICOS**](#_o4n479m76zxh) **3**

[Windows](#_6k5dttuzpf0e) 3

[Linux](#_qe0z6lth7zdb) 6

[**Configuración de las llaves**](#_chhiqa8dm4bp) **7**

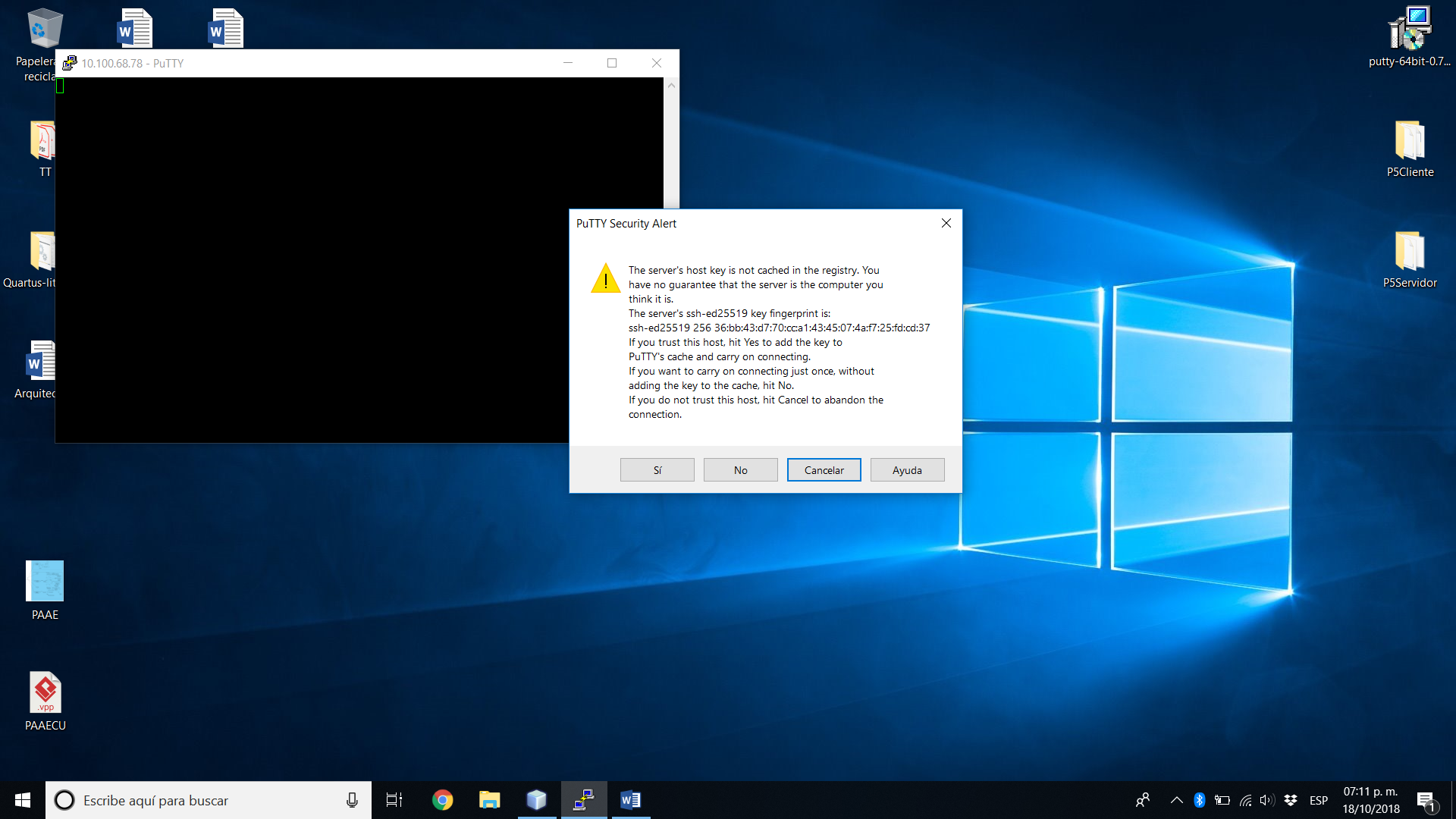
[Copia de la llave pública usando ssh-copy-id](#_grwnf21e8tq5) 8

# 

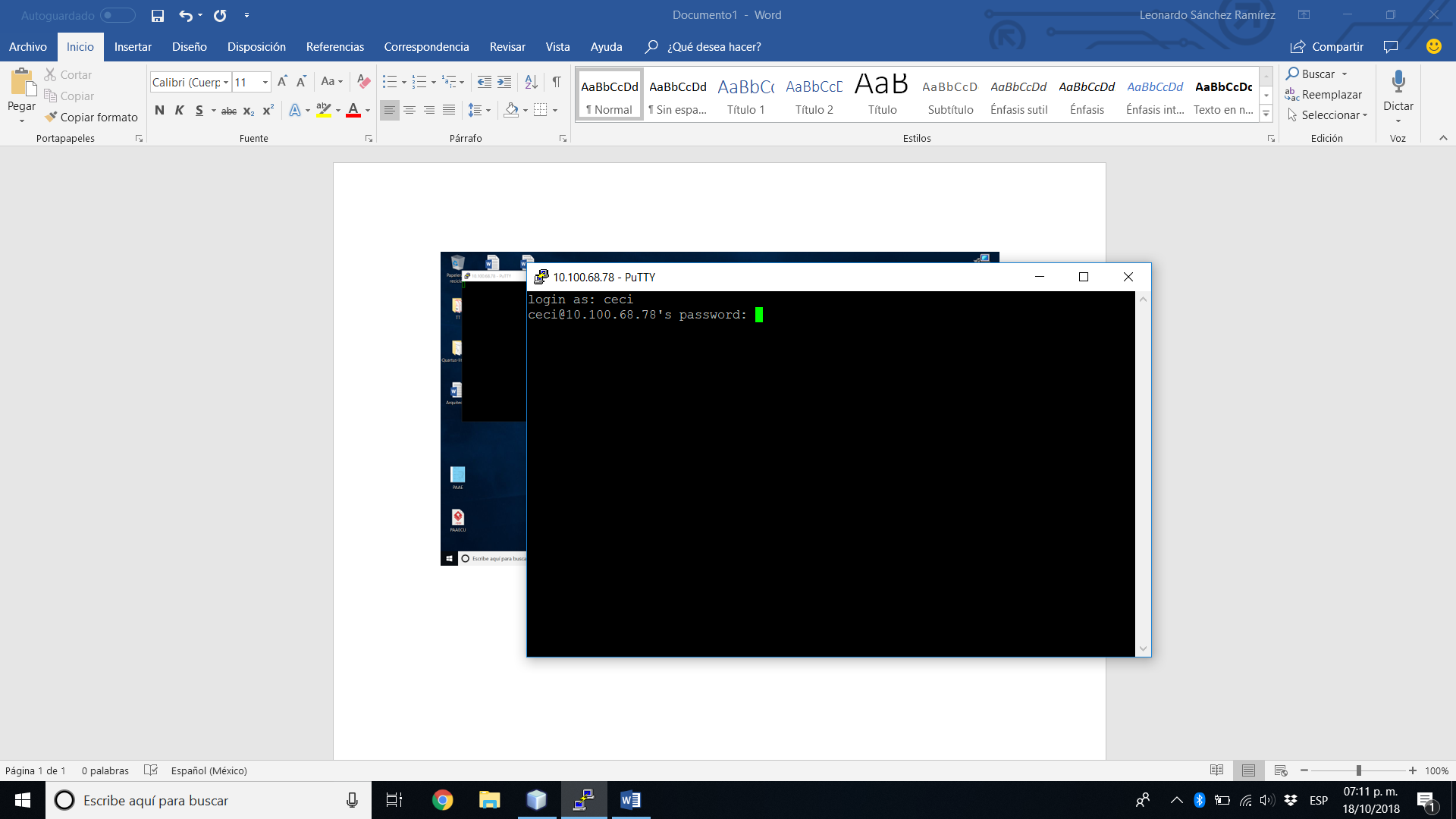
# CLIENTES GRÁFICOS

## Windows

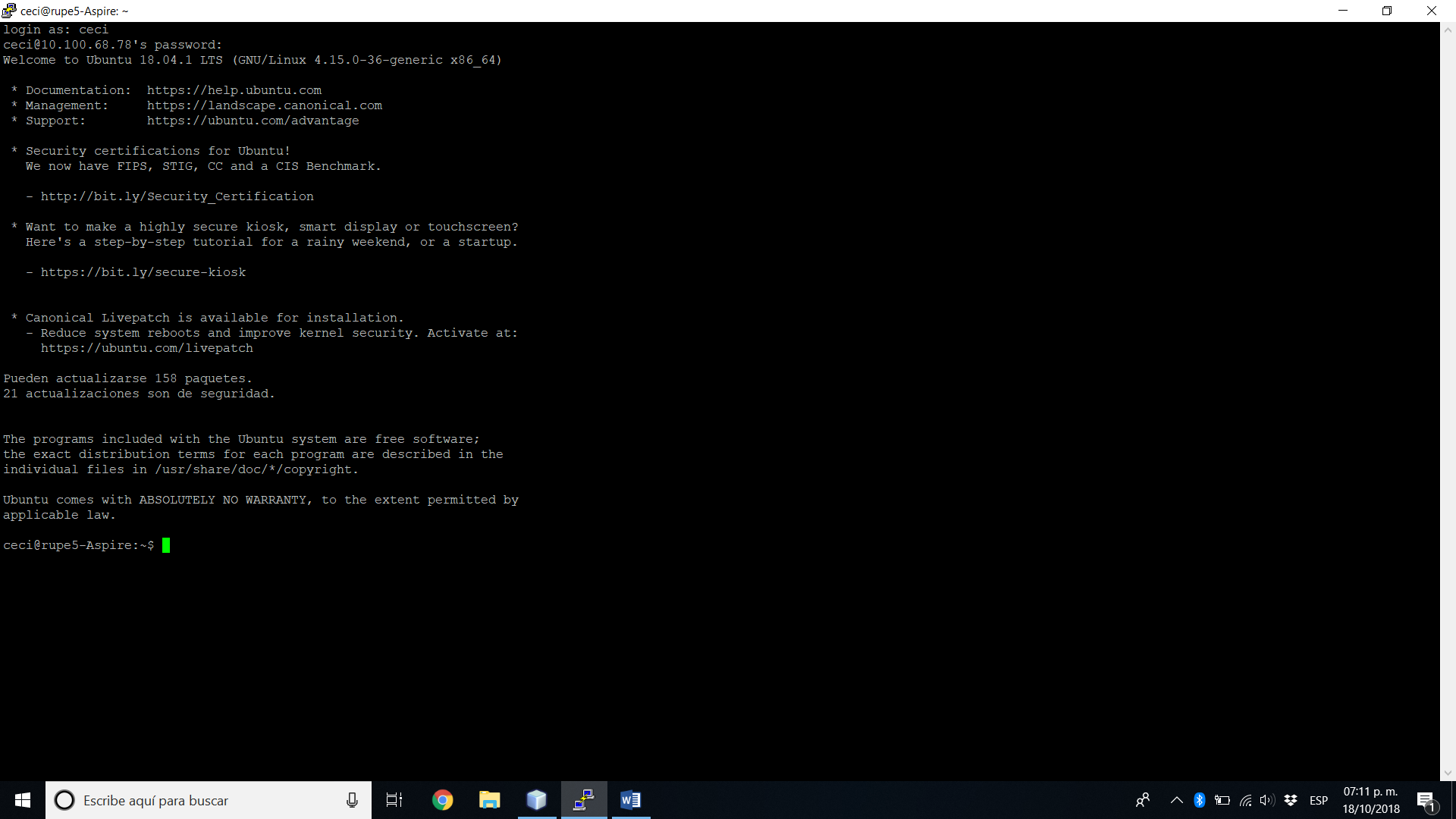
Cuando ingresamos en el cliente PuTTY te muestra la llave SSH simplemente se le da clic en “sí” para poder desplegar el cliente en el sistema operativo Windows.



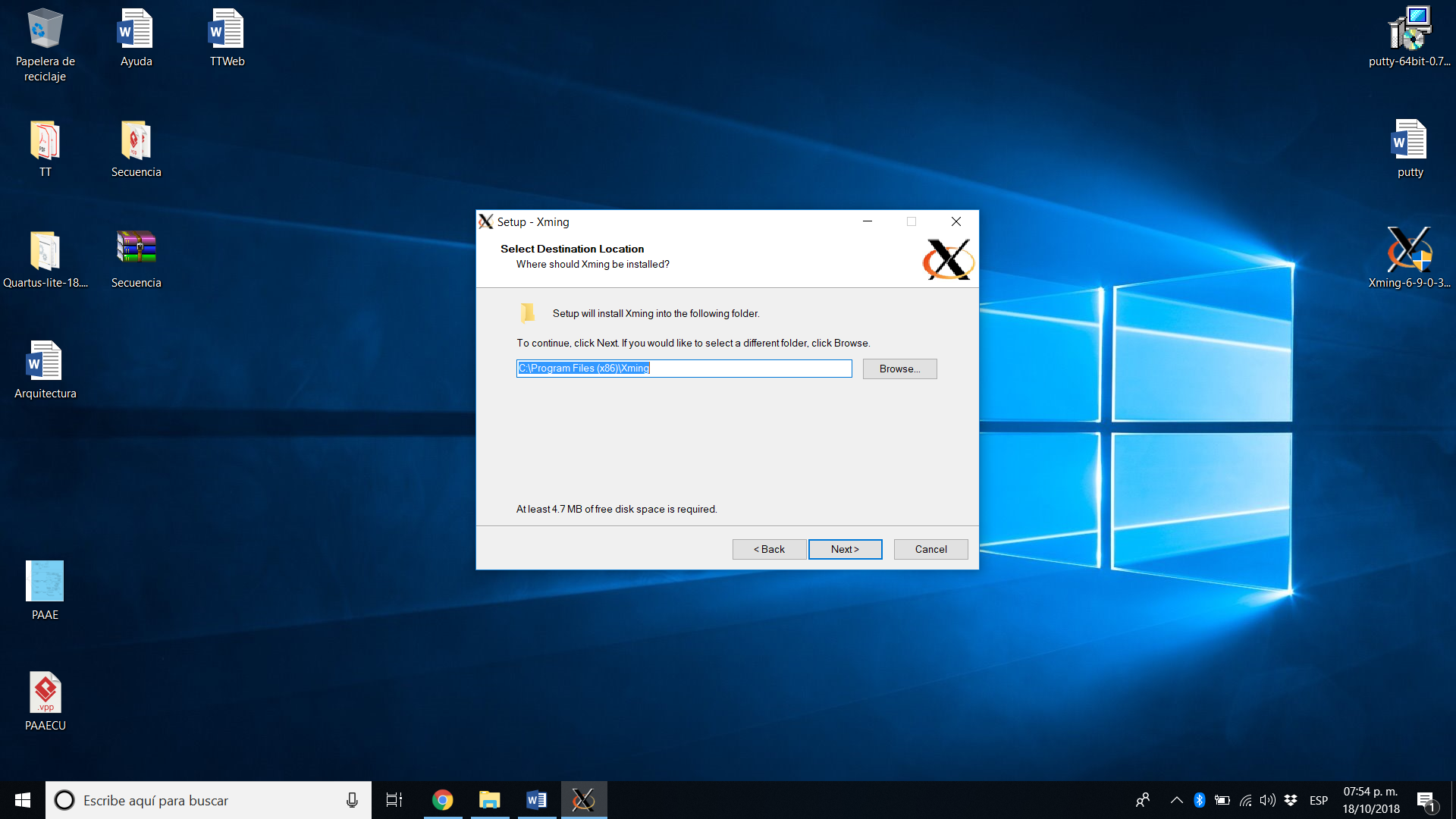
Una vez dentro del sistema se ingresan las credenciales que le ha otorgado el su administrador, en este caso se hará intento de ingreso con las siguientes credenciales: usuario: cesi, ip: 10.100.68.78 y password: 12345



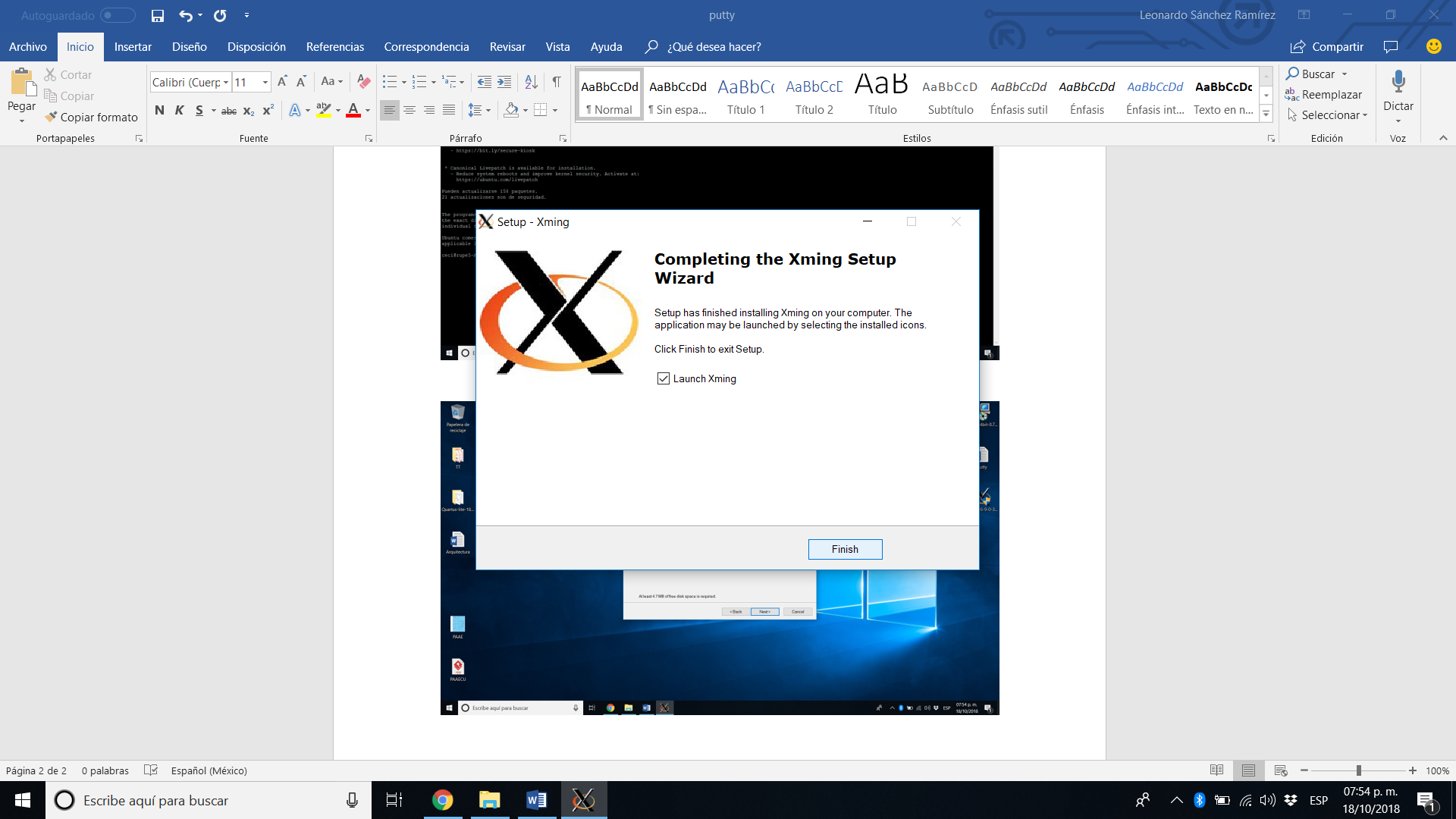
En la siguiente imagen se puede apreciar el ingreso exitoso al servidor “rupe-Aspire”



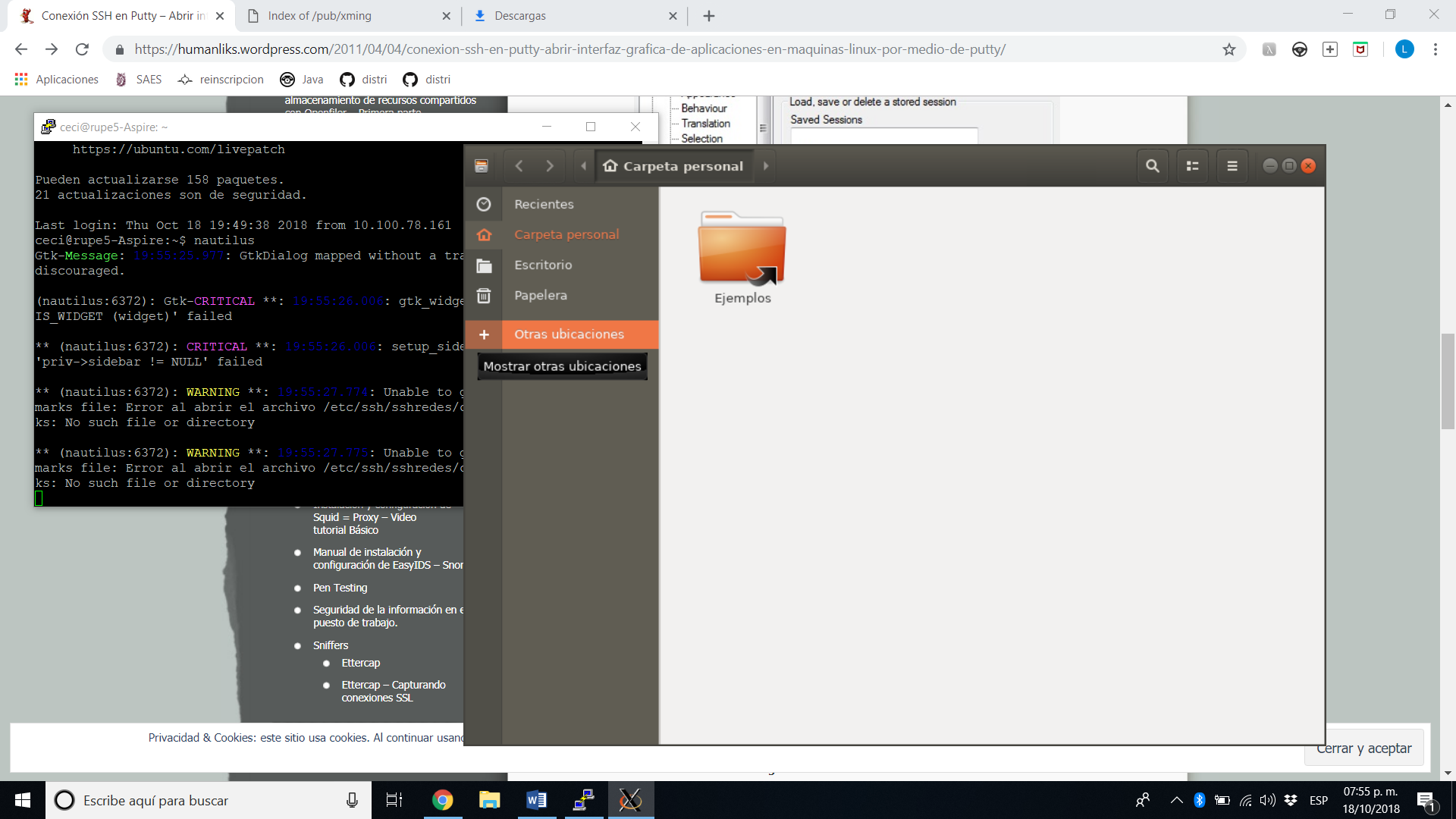
Para configurar el cliente gráfico, necesitamos descargar *X11,* indicamos el fichero donde vamos a instalar.



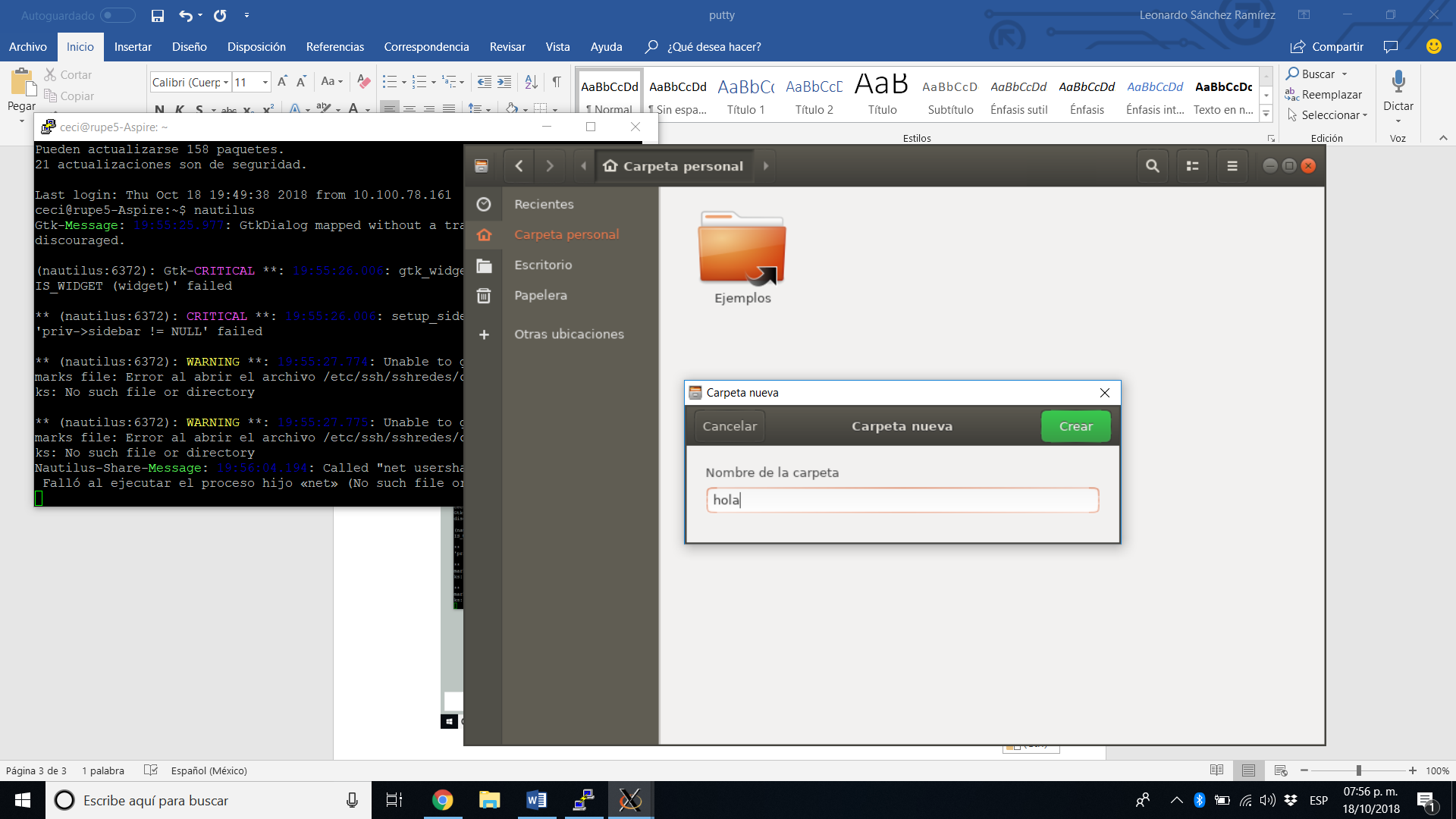
Damos click en aceptar, para iniciar la instalación.



Podemos ver que en el cliente de Windows se ejecuta el administrador de archivos *Nautilus*.

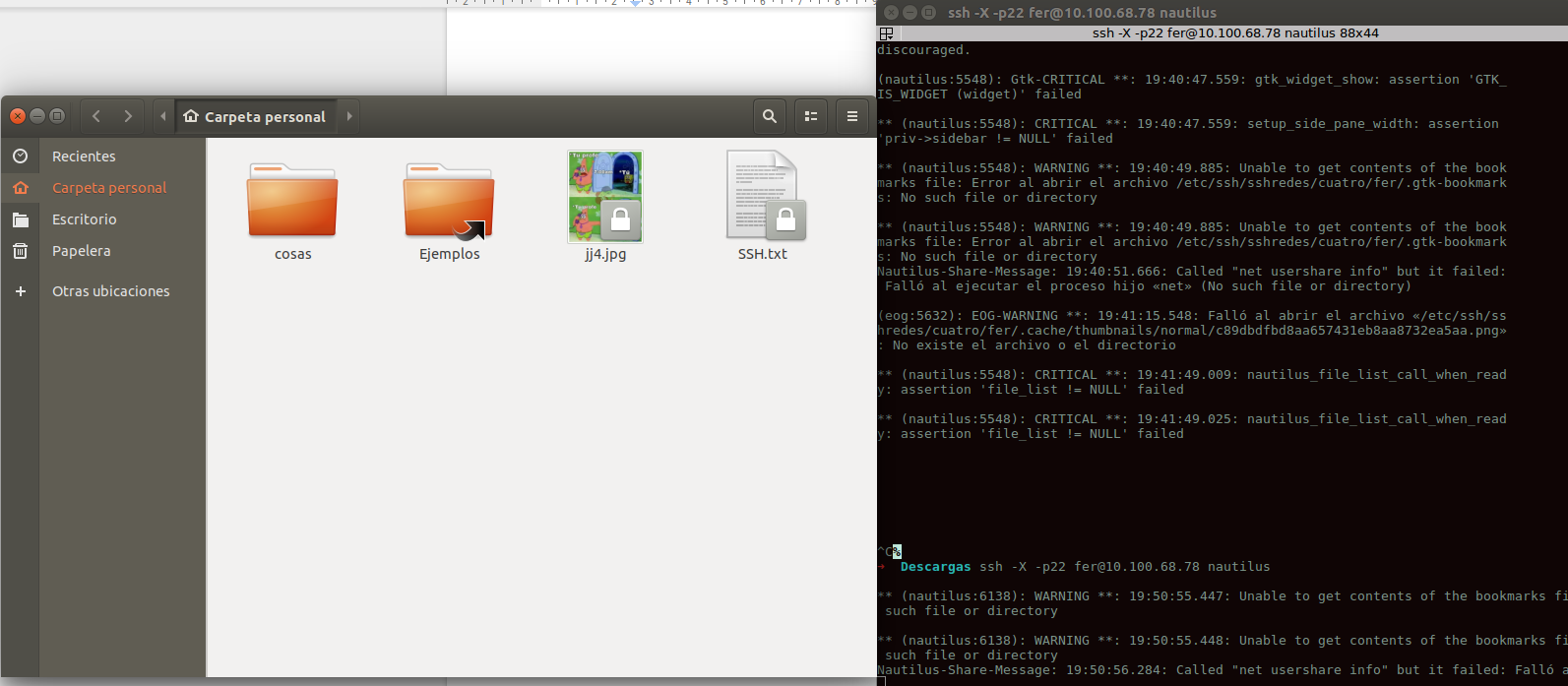


Para ingresar, nos pide ingresar la contraseña de los usuarios.

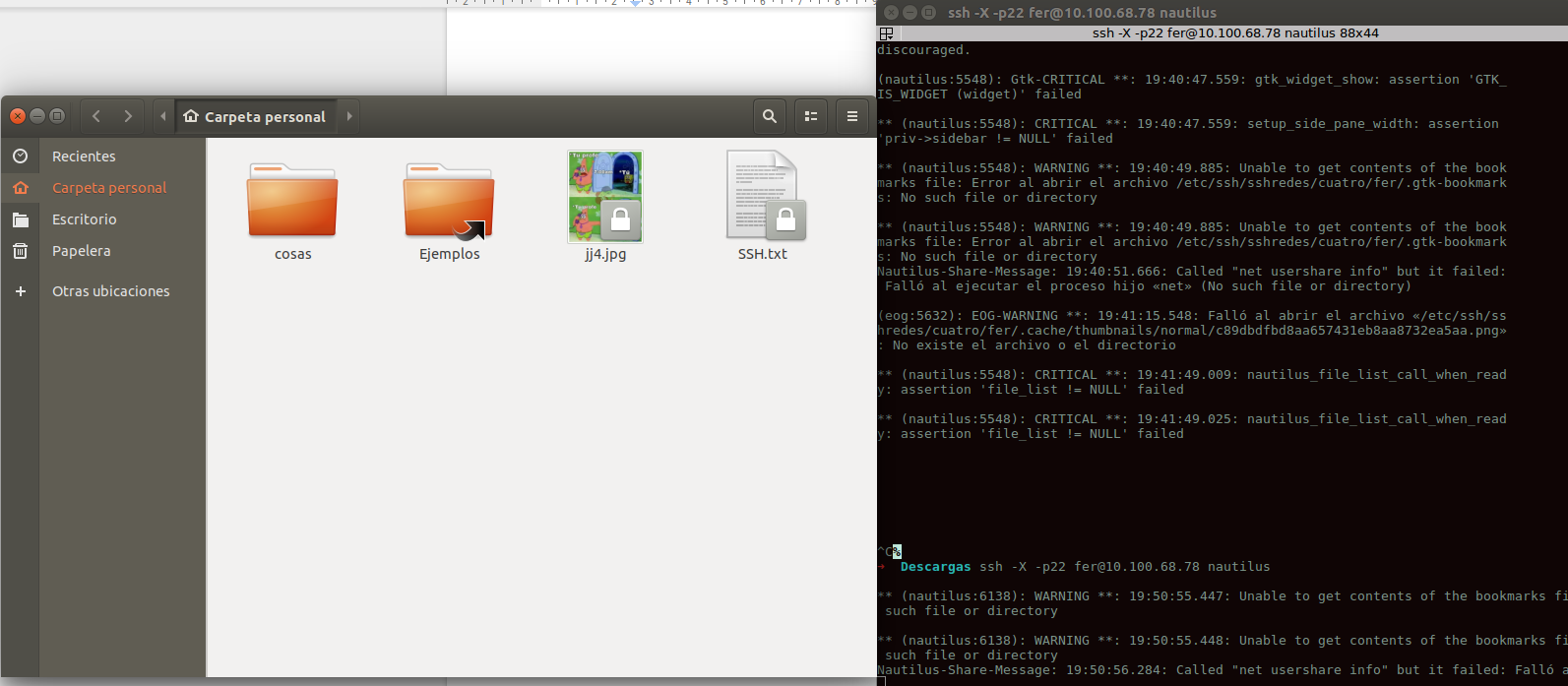


## Linux

Para iniciar sesión desde un cliente, en la terminal ejecutamos el comando *ssh -X -p22 usuario@host aplicación*



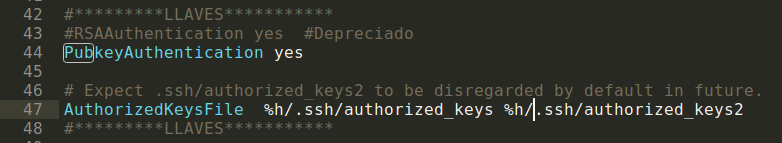
Podemos ver que abre la pantalla del nautilus, pero desde nuestro cliente de Linux.



# Configuración de las llaves

Cada cliente que desee utilizar este método debe generar en su equipo su certificado y su llave correspondiente:

Se utilizarán llaves RSA. En el servidor se debe permitir la autenticación por medio de llaves RSA e indicar la ruta de las llaves autorizadas para acceder, de la siguiente manera (esto se encuentra en el archivo de configuración del servidor):



El indicador “%h” referencía el directorio home. De esta forma cada usuario habilitado para iniciar sesión por llave, deberá colocar la llave generada en su equipo, en la respectiva carpeta .ssh/ dentro del servidor ssh.

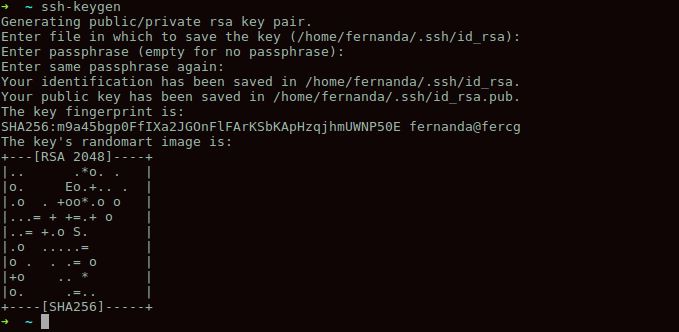
## Copia de la llave pública usando ssh-copy-id

La herramienta ssh-copy-id se encuentra incluida de manera predeterminada en varios sistemas operativos, por lo cual existe la posibilidad que esté disponible en tu sistema local. Para que este método funcione es necesario que ya se cuente con acceso por contraseña mediante SSH dentro de tu servidor.

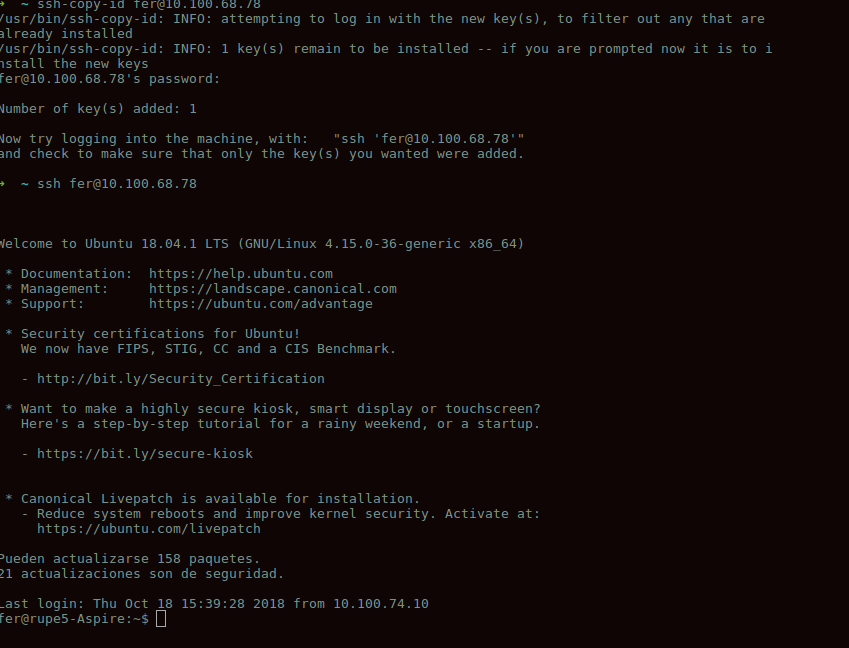
Para usar este método, simplemente se debe especificar el servidor remoto al cual te quieres conectar, así como la cuenta de usuario y su contraseña con acceso SSH. Esta cuenta es a la cual se copiará tu llave SSH pública.

La sintaxis es:

* ssh-copy-id username@remote\_host



Una vez creada la llave, cuando el usuario deseé ingresar al servidor, ya no será necesario que escriba su contraseña.



Al copiar las llaves al servidor, se copiará la carpeta .ssh



Al ingresar a la carpeta podemos ver el archivo .*key* correspondiente a la llave.

