

En este capítulo nos centraremos en los aspectos del dominio relacionados con los clientes. Comenzaremos por detallar cómo unir un cliente, con un sistema operativo *Windows* de escritorio, al dominio que implementamos en el Capítulo 6.

Después aprenderemos a compartir con los equipos cliente el espacio de almacenamiento del servidor, asignaremos derechos a los usuarios y grupos del sistema y crearemos perfiles móviles y obligatorios para las cuentas de usuario.

También aprenderemos a unir al dominio otros sistemas operativos del lado cliente que hoy día son muy habituales en los entornos de red, me refiero a *Ubuntu* y a versiones algo más antiguas de *Windows*.

Por último, aprenderemos a instalar y configurar las herramientas de administración remota que permiten controlar un dominio con *Windows Server* desde equipos cliente. En concreto, instalaremos *Remote Server Administration Tools (RSAT)* sobre un sistema *Windows* de escritorio. Una vez que hemos establecido nuestros objetivos, iniciemos la marcha...

Lo primero que tenemos que hacer para utilizar los recursos de un dominio es añadirle los ordenadores que puedan actuar como clientes. En este caso, comenzaremos por un ordenador que está ejecutando *Microsoft Windows*. Básicamente, el proceso consistirá en establecer las características de red, para que coincidan con las necesidades del dominio, ajustar el nombre del equipo cliente, unir el equipo al dominio y, finalmente, iniciar sesión utilizando una cuenta de usuario de las que ya tenemos definidas en el dominio.

Aunque aquí añadiremos el cliente utilizando una cuenta de equipo que ya existe en el dominio, también se pueden añadir equipos que aún no dispongan de una cuenta. Ésta se creará en el momento de unir el equipo al dominio.

El primer paso, para comenzar a utilizar los recursos que ofrece un dominio, consiste en añadir a dicho dominio los ordenadores que puedan actuar como clientes.

En este caso, comenzaremos por un ordenador que está ejecutando *Microsoft Windows 10*.

Básicamente, el proceso consistirá en realizar los siguientes pasos:

- Establecer las características de red, para que coincidan con las necesidades del dominio.
- Ajustar el nombre del equipo cliente.
- Unir el equipo al dominio.

Al final del proceso, iniciaremos sesión en el equipo cliente usando una cuenta de usuario de las que ya tenemos definidas en el dominio. Con esto comprobaremos que el proceso se ha realizado correctamente.

Así es que, si estás listo, pongamos manos a la obra.

Configurar la red en el equipo cliente

Para conseguir que un cliente pueda unirse a un dominio, antes deberemos asegurarnos de que las características de su configuración de red sean coincidentes con las necesidades del dominio.

En [SomeBooks.es](#) ya aprendimos a configurar la red de un ordenador con *Windows 10* en el artículo [Asignar una dirección IP fija en Windows 10](#). La diferencia es que, ahora, podemos dejar

habilitada la asignación automática de *IP*, pero debemos asegurarnos de que el *Servidor DNS preferido* hace referencia a la *dirección IP* del controlador del dominio (para nuestros ejemplos, 192.168.1.5)

En definitiva, podemos dejar una configuración como la que muestra la siguiente imagen:

Obtenemos la dirección IP automáticamente, pero asignamos el *Servidor DNS preferido* de forma manual.

Comprobar que la configuración de red es correcta.

Después de completar el apartado anterior, debemos comprobar que no hemos cometido ningún error. Esto es tan sencillo como abrir una ventana de comandos y hacer un *ping* al Servidor.

Si utilizamos el *nombre del servidor* en lugar de su *dirección IP*, no sólo estaremos comprobando que el equipo cliente está en la misma red que el servidor. También comprobaremos que la configuración *DNS* del cliente es correcta y que el *servidor DNS* del controlador de dominio está funcionando adecuadamente.

Si la respuesta no es correcta, deberemos repasar nuestras últimas acciones.

Para comenzar, hacemos clic, con el botón derecho del ratón, sobre el botón *Inicio*.

En el menú que aparece, elegimos la opción *Símbolo del sistema*.

Una vez que se abra la ventana de la *Línea de comandos*, escribimos una orden como esta:

```
ping server-2016-a
```

Lógicamente, *server-2016-a* es el nombre de nuestro servidor de dominio y deberemos sustituirlo por el que usemos en cada caso.

Cuando estemos listos, pulsamos la tecla *Intro*.

Si todo es correcto, el servidor responderá y la salida será parecida a lo que muestra la imagen anterior.

Cambiar el nombre del equipo y unirlo al dominio

El siguiente paso consistirá en ajustar el nombre del equipo cliente, para que coincida con un nombre de equipo definido en el dominio. Al indicar el nombre del dominio, el sistema procederá a establecer el vínculo. Recuerda que, en artículos anteriores, ya teníamos una cuenta de equipo en el dominio con el nombre *CLIENTE-W10-01* (puedes consultar el artículo [Administrar cuentas de equipo del dominio desde la interfaz gráfica de Windows Server 2016](#)).

Para comenzar, hacemos clic, con el botón derecho del ratón, sobre el botón *Inicio*.

En el menú que aparece, elegimos la opción *Sistema*.

Al hacerlo, aparecerá una ventana con información del sistema. En la parte inferior, además de algunos detalles sobre el hardware del equipo, podemos encontrar su nombre (tanto el nombre *NetBIOS* como el nombre *DNS*), la descripción y el nombre del grupo de trabajo o dominio al que pertenece.

En la imagen puedes observar que, en estos momentos, el nombre del equipo es el predeterminado que asigna *Windows* durante su proceso de instalación. Además, también pertenece al grupo de trabajo predeterminado (*WORKGROUP*), que se asigna a todos los equipos con *Windows* desde hace innumerables versiones.

Para cambiar estos datos, sólo tenemos que hacer clic en el enlace *Cambiar configuración*.

En la ventana *Propiedades del sistema*, que aparece a continuación, podríamos escribir un texto para la descripción (si te fijas, en la imagen anterior aparecía en blanco). Sin embargo, lo dejaremos así.

Lo que sí haremos será un clic sobre el botón *Cambiar*, para escribir el nuevo nombre del equipo y nombre del dominio.

Lo haremos en la ventana que aparece a continuación. En el campo *Nombre de equipo*, debemos asegurar de escribir el nombre de la cuenta del dominio. Además, en el área *Miembro del*, elegiremos la opción *Dominio* y debajo escribiremos el nombre del dominio al que queremos unir el equipo (recuerda que, para nuestros ejemplos, estamos utilizando *somebooks.local*)

Cuando los datos sean correctos, hacemos clic en *Aceptar*.

En ese momento, *Windows 10* busca en la red el dominio especificado. Si no lo encuentra, aparecerá un mensaje de aviso (probablemente habremos cometido algún error en los datos introducidos).

Si lo encuentra, deberemos escribir un nombre de usuario y una contraseña, perteneciente al dominio, que tenga privilegios suficientes para unir el equipo cliente.

Una vez introducidos los datos, hacemos clic en *Aceptar*.

La ventana de autenticación se cierra y en su lugar aparece un mensaje indicando que el equipo se ha unido correctamente al dominio. Si cometemos algún error en el nombre de usuario o en la contraseña, en lugar del mensaje siguiente, aparecerá uno de error y tendremos que volver a intentarlo.

Hacemos clic sobre *Aceptar*.

A continuación, aparece una nueva ventana informativa indicando que deberemos reiniciar el equipo para que se apliquen los cambios, pero que antes deberemos cerrar todos los programas y guardar todos los archivos que tengamos abiertos.

Hacemos clic sobre *Aceptar*.

Cuando cerremos la ventana de *Propiedades del sistema*, detectará que ya no hay programas en ejecución y nos dará la oportunidad de reiniciar en ese momento.

Hacemos clic sobre *Reiniciar ahora*.

Iniciar sesión en el dominio

Cuando haya concluido el reinicio, procederemos a iniciar sesión con una de las cuentas de usuario del dominio (por ejemplo, la cuenta *Bernard*, que creamos en un artículo anterior).

De forma predeterminada, el sistema nos ofrece iniciar sesión con el último usuario con el que hayamos trabajado. Sin embargo, en este caso se trata del usuario local (en nuestro ejemplo, se llamaba *usuario*).

Sabemos que es una cuenta local porque, antes del nombre de usuario, aparece el nombre del equipo.

La pantalla cambiará para mostrarnos un cuadro de texto donde escribir el nombre de la cuenta y, debajo, la contraseña de dicha cuenta en el dominio.

Observa que, como el equipo ya es miembro del dominio, bajo el cuadro de texto de la contraseña aparece un mensaje indicándonos que se iniciará sesión en el dominio *SOMEBOOKS* (el nombre *NetBIOS* de *somebooks.local* que estamos utilizando como ejemplo).

Si quisiéramos iniciar sesión en otro dominio de la red, usaríamos el enlace *¿Cómo puedo iniciar sesión en otro dominio?*, pero de momento, este no es el caso.

Después de esto, se iniciará la sesión de la forma estándar, aunque notarás que tarda un poco más, debido a que se está creando la información de perfil del nuevo usuario. Mientras tanto, nos mantendrá ocupados mostrándonos mensajes en la pantalla.

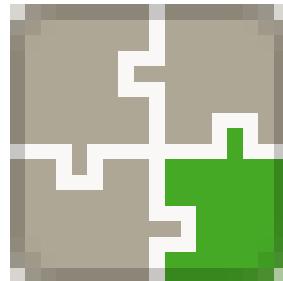
Cuando termine de arrancar, el aspecto del área de trabajo será el predeterminado, aunque la cuenta de usuario lo hubiese tenido cambiado.

Al hacerlo, se desplaza un panel hacia la derecha con opciones de apagado, configuración... Y el nombre de la cuenta de usuario con la que hemos iniciado sesión.

Si queremos comprobar que el equipo está realmente unido al dominio, también podemos volver a consultar las propiedades del sistema.

Obtendremos la ventana con información sobre el sistema que vimos más arriba, pero ahora los datos se corresponden con los nuevos parámetros que hemos usado para unir el equipo al dominio.

Una de las ventajas de *GNU/Linux* es su capacidad para adaptarse a multitud de contextos. Un ejemplo de ello es el artículo de hoy, donde aprenderemos a unirlo, como cliente, a un dominio de *Windows Server 2019*.



En particular, lo uniremos al dominio que hemos venido creando y configurando a lo largo de diferentes artículos desde hace un tiempo.

Antes de poner en práctica el contenido de este artículo deberás tener instalado *Active Directory* en un equipo con *Windows Server 2019*. Si aún no lo tienes, puede resultarte de ayuda el contenido de los siguientes artículos:

- [Instalar un dominio desde la interfaz gráfica de Windows Server 2019 \(parte 1\)](#).
- [Instalar un dominio desde la interfaz gráfica de Windows Server 2019 \(parte 2\)](#).
- [Crear una cuenta de usuario del dominio en la interfaz gráfica de Windows Server 2019](#).
- [Operaciones frecuentes sobre cuentas de usuario en un dominio Windows Server 2019 \(Parte I\)](#).
- [Operaciones frecuentes sobre cuentas de usuario en un dominio Windows Server 2019 \(Parte II\)](#).

La tarea no es muy complicada, pero sí un poco larga. Por ese motivo, la dividiremos en dos partes. La primera, que cubriremos en el artículo de hoy, resolverá los siguientes aspectos:

- Configurar las características del equipo.
- Instalar el software necesario.
- Configurar *Kerberos*.
- Comprobar el funcionamiento de *Kerberos*.
- Unir el cliente al dominio.

Y la segunda, que resolveremos en un próximo artículo, se encargará de lo siguiente:

- Configurar *SSSD*.
- Ajustar el comportamiento de *PAM* para iniciar sesión con usuarios del dominio.
- Convertir al administrador del dominio en administrador local.
- Reiniciar el equipo y comprobar el inicio de sesión gráfico.

- Iniciar sesión con cualquier cuenta del dominio.

De cualquier modo, el proceso debe entenderse como un todo y los pasos deberán completarse en su totalidad, y en el orden indicado, para obtener los resultados esperados. Así es que, si estás listo, comencemos...

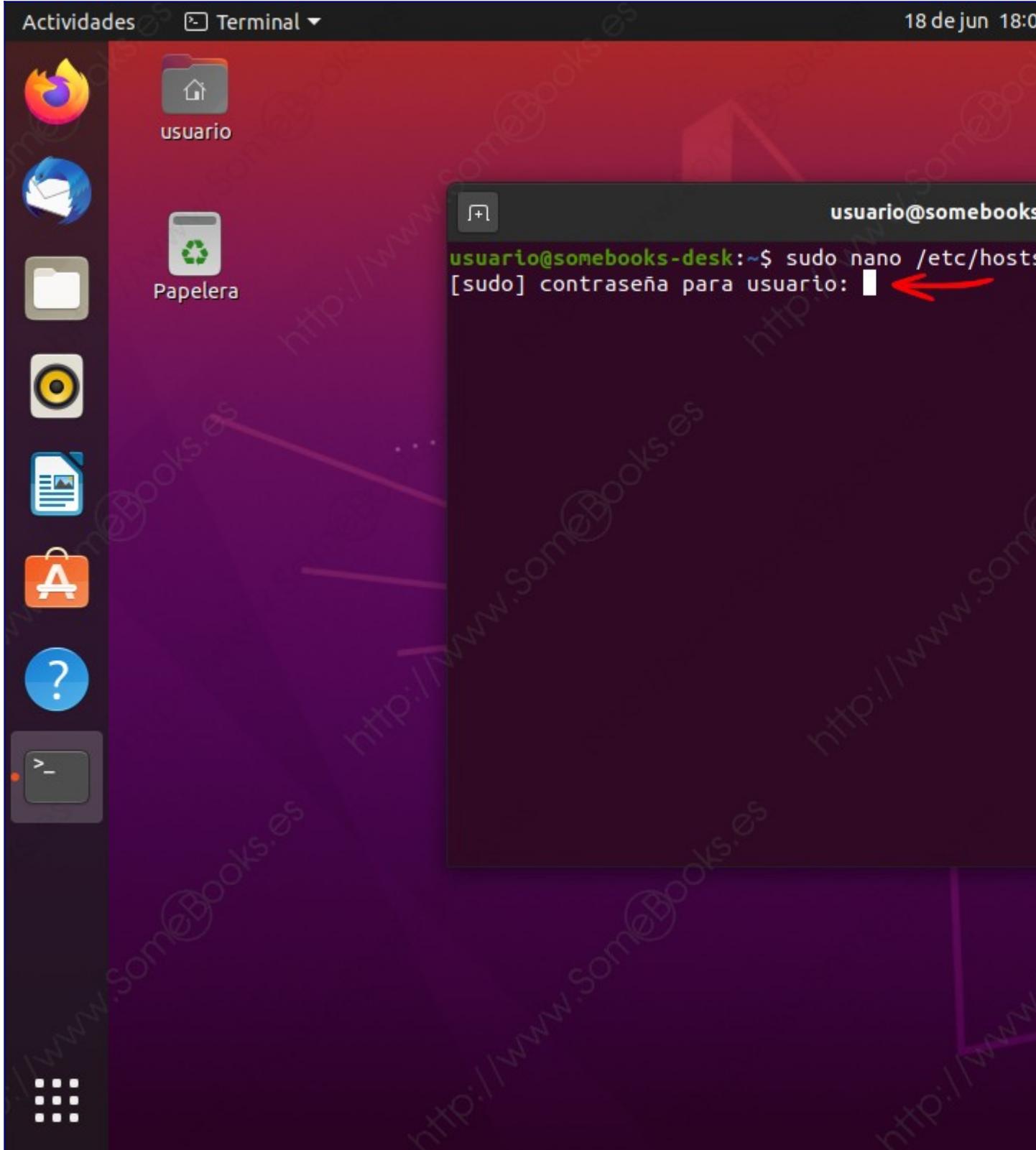
Configurar las características del equipo

Lo primero será asegurarnos de que el cliente puede hacer *ping* al servidor utilizando su nombre. Como en nuestro caso no estamos utilizando *Windows Server* con una configuración *DNS* completa, podemos limitarnos a configurar el archivo *hosts* del equipo *Ubuntu* con el fin de conseguir el mismo objetivo.

Por lo tanto, comenzamos editando en archivo */etc/hosts* con el editor de textos *nano*.

```
sudo nano /etc/hosts
```

Como es lógico, debemos utilizar privilegios administrativos



Lo siguiente será añadir una nueva línea que relacione la *dirección IP* del servidor con su nombre de equipo, incluyendo también el nombre completo dentro del dominio:

```
192.168.1.5      server-2019-a server-2019-a.somebooks.local
```

Cuando estemos listos, pulsamos la combinación de teclas **Ctrl + X** para cerrar el editor de textos.

Cuando el editor nos pregunte si queremos guardar los cambios, pulsamos la tecla **S**.

Actividades

Terminal ▾

18 de jun 18:00



usuario



Papelera



usuario@somebooks

GNU nano 4.8

/etc/hosts

127.0.0.1 localhost

127.0.1.1 somebooks-desk

192.168.1.5 server-2019-a server-2019-a.s

```
# The following lines are desirable for IPv6
::1      ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

¿Guardar el búfer modificado?

S Sí

N No

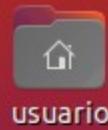
^C Cancelar

... Y, a continuación, pulsamos la tecla Intro para conservar el mismo nombre de archivo.

Actividades

Terminal ▾

18 de jun 18:0



usuario



Papelera



usuario@somebooks

GNU nano 4.8

/etc/hosts

```
127.0.0.1      localhost
127.0.1.1      somebooks-desk
192.168.1.5    server-2019-a server-2019-a.s
```

```
# The following lines are desirable for IPv6
::1      ip6-localhost ip6-loopback
fe00::0  ip6-localnet
ff00::0  ip6-mcastprefix
ff02::1  ip6-allnodes
ff02::2  ip6-allrouters
```

Nombre del archivo a escribir: /etc/hosts

^G Ver ayuda

M-D Formato DOS

M-A A

^C Cancelar

M-M Formato Mac

M-P A

Finalmente, para comprobar que los cambios han tenido éxito, probamos a ejecutar la orden *ping* con el nombre del servidor:

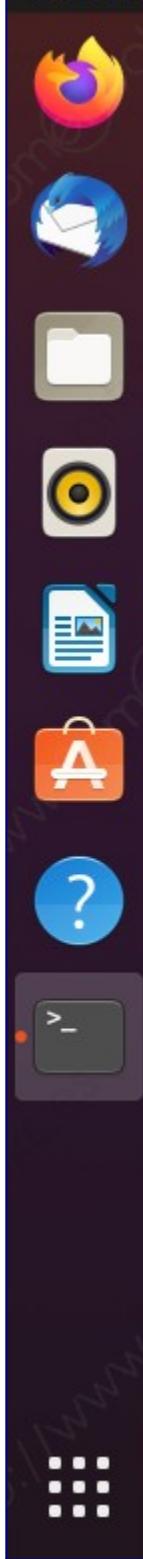
```
ping server-2019-a
```

... Y comprobamos que funciona correctamente.

Actividades

Terminal ▾

18 de jun 18:0



```
usuario@somebooks-desk:~$ sudo nano /etc/hosts  
[sudo] contraseña para usuario:  
usuario@somebooks-desk:~$ ping server-2019-a  
PING server-2019-a (192.168.1.5) 56(84) bytes  
64 bytes from server-2019-a (192.168.1.5): icmp  
^C  
--- server-2019-a ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss  
rtt min/avg/max/mdev = 0.520/0.583/0.687/0.064  
usuario@somebooks-desk:~$
```

Para detener la salida de la orden *ping*, necesitaremos pulsar la combinación de teclas **Ctrl + C**.

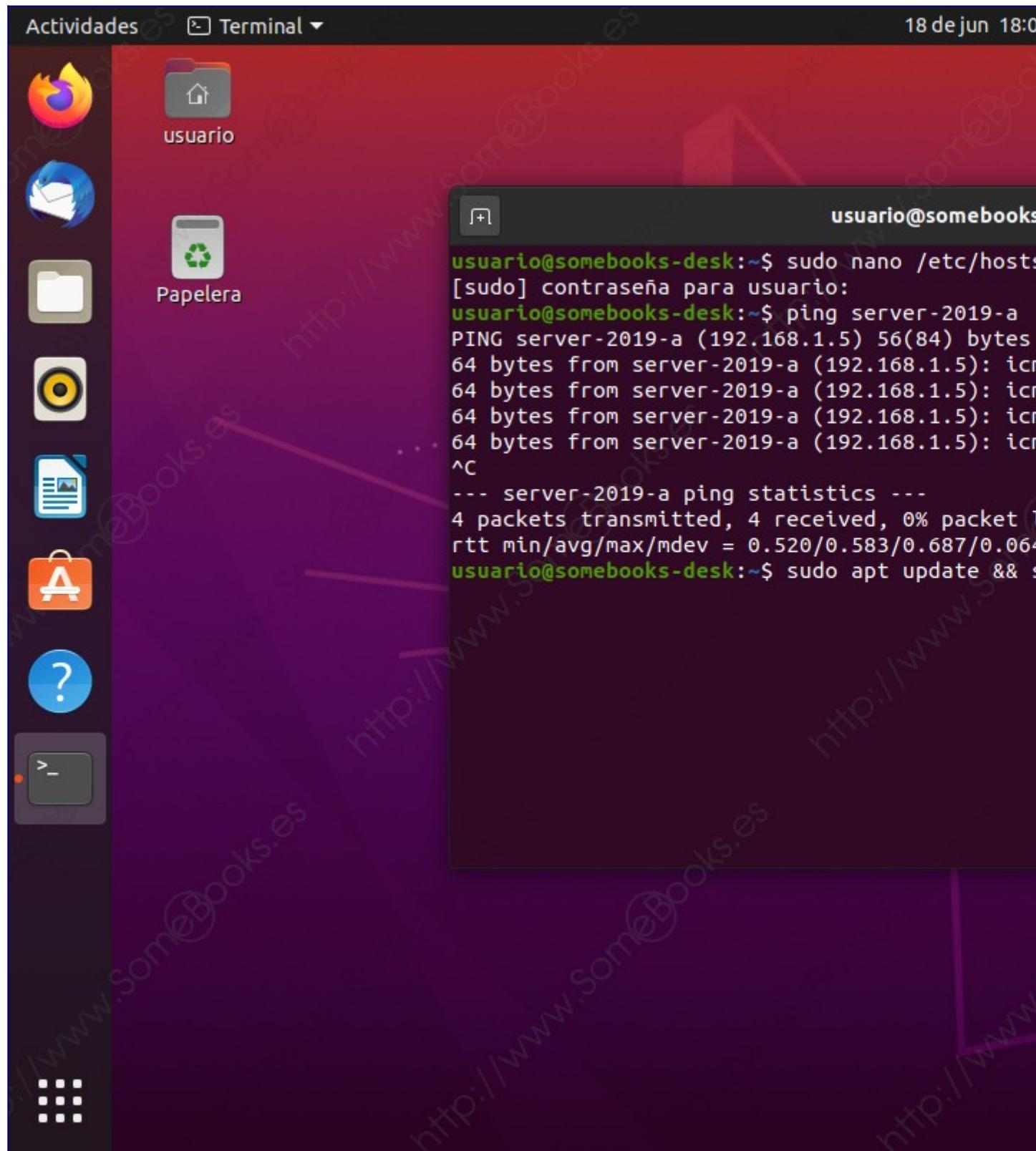
Instalar el software necesario

Una vez que estamos seguros de que la comunicación entre el cliente y el servidor funciona correctamente, el siguiente paso consistirá en instalar el software necesario para realizar la tarea.

Para lograrlo, comenzaremos por actualizar el sistema operativo con las últimas versiones de los paquetes disponibles en los repositorios. Algo tan sencillo como utilizar la siguiente orden:

```
sudo apt update && sudo apt upgrade
```

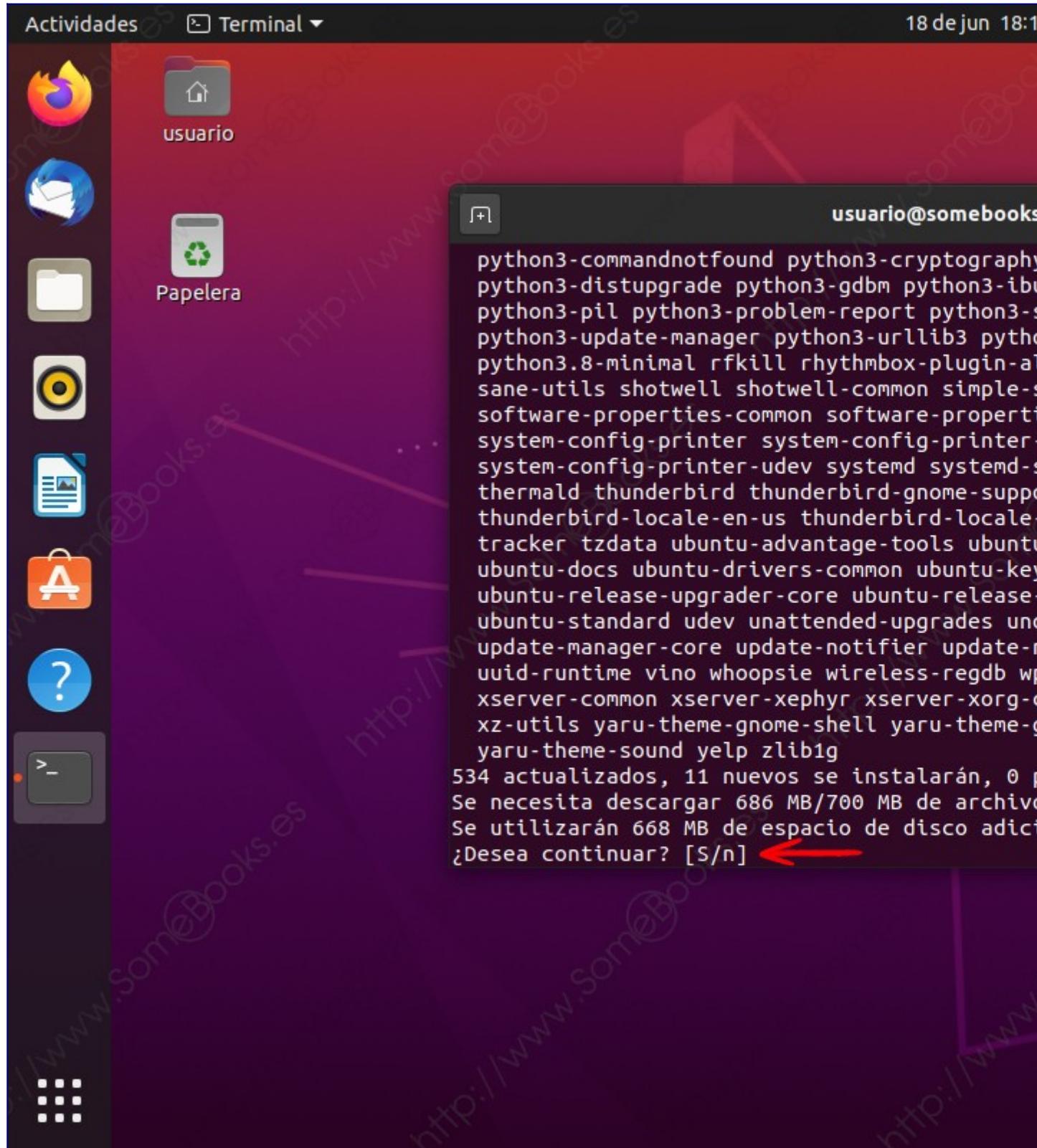
La escribimos y pulsamos la tecla **Intro**.



Al hacerlo, recibiremos un detalle con todos los paquetes que van a actualizarse y un resumen final con el numero de paquetes que se actualizarán, los paquetes nuevos que se instalarán y los que se

eliminarán de la instalación. También se incluye la cantidad de información que se descargará de los repositorios y la capacidad final que se utilizará en nuestro disco duro.

Si estamos de acuerdo con todo, pulsaremos la tecla S para continuar.



Cuando acabe la actualización, estaremos listos para instalar los paquetes que necesitamos. En particular, añadiremos los siguientes paquete:

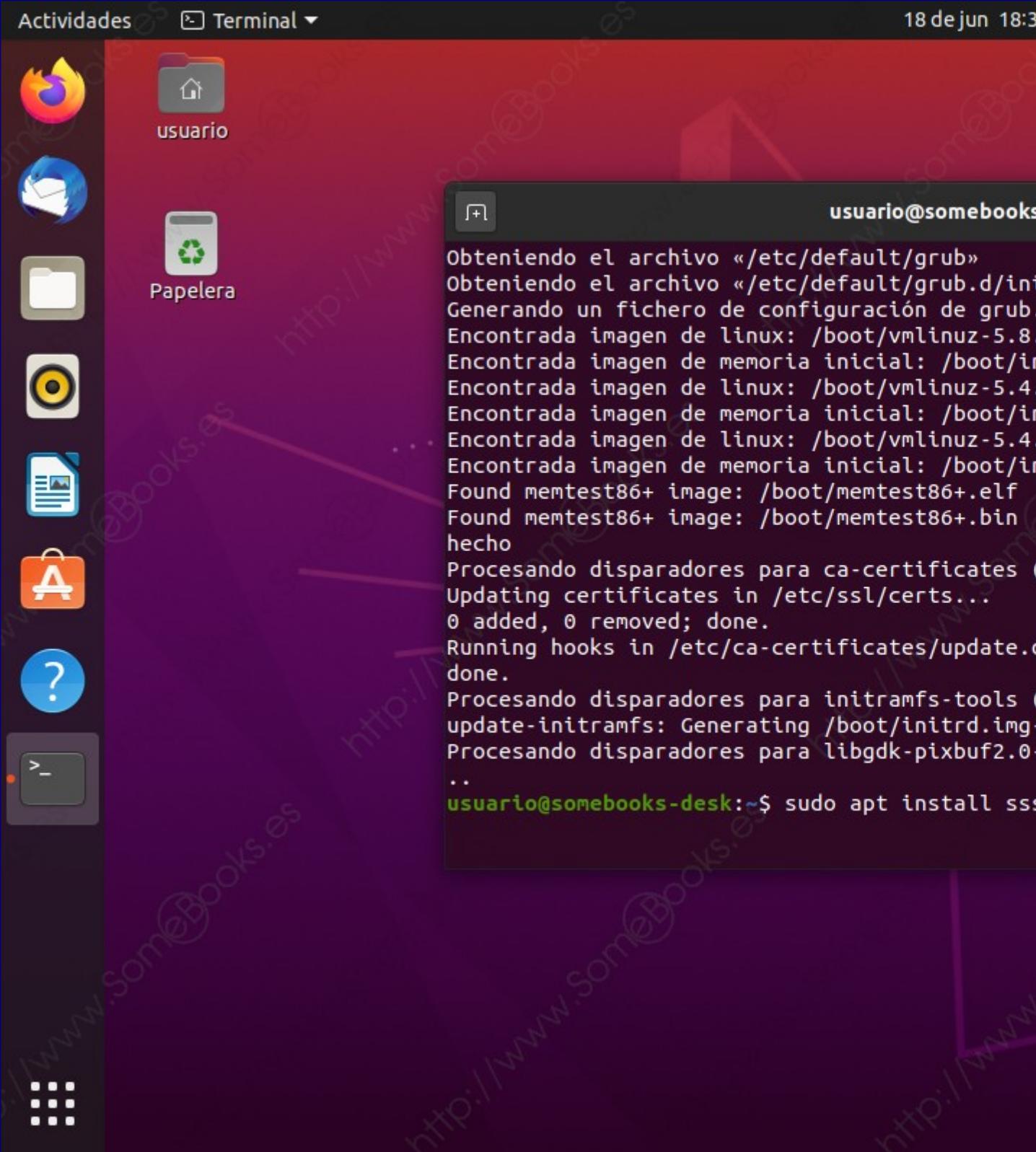
- *sssd* (*System Security Services Daemon*): Administra los mecanismos de autenticación y el acceso a directorios remotos. Sustituye al clásico *Winbind* aportando más velocidad y estabilidad.
- *heimdal-clients*: Se trata de una implementación libre de *Kerberos 5* creada con la intención de ser compatible con el protocolo *Kerberos* implementado por el *MIT*.
- *msktutil*: La utilidad que obtiene y administra los *keytabs* de *Kerberos* en un entorno de *Microsoft Active Directory*.

Un *keytab* es un archivo que contiene parejas de entidades de seguridad y claves cifradas de *Kerberos*. Se utilizar para autenticarse en un sistema remoto que use el protocolo *Kerberos*.

Para instalar todos los paquetes en una sola operación, sólo tenemos que utilizar la siguiente orden:

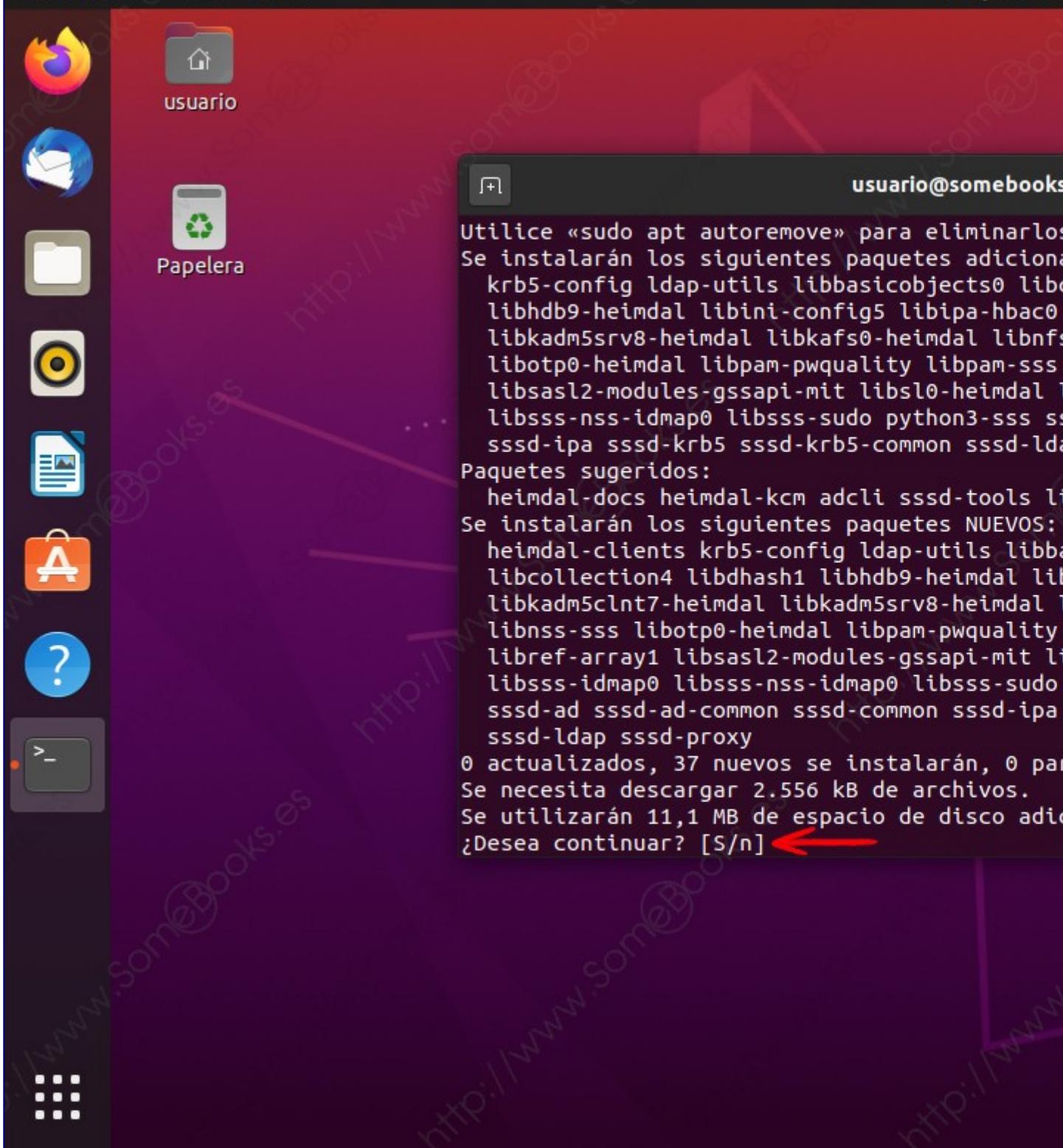
```
sudo apt install sssd heimdal-clients msktutil
```

Como antes, escribimos la orden y pulsamos la tecla **Intro**.



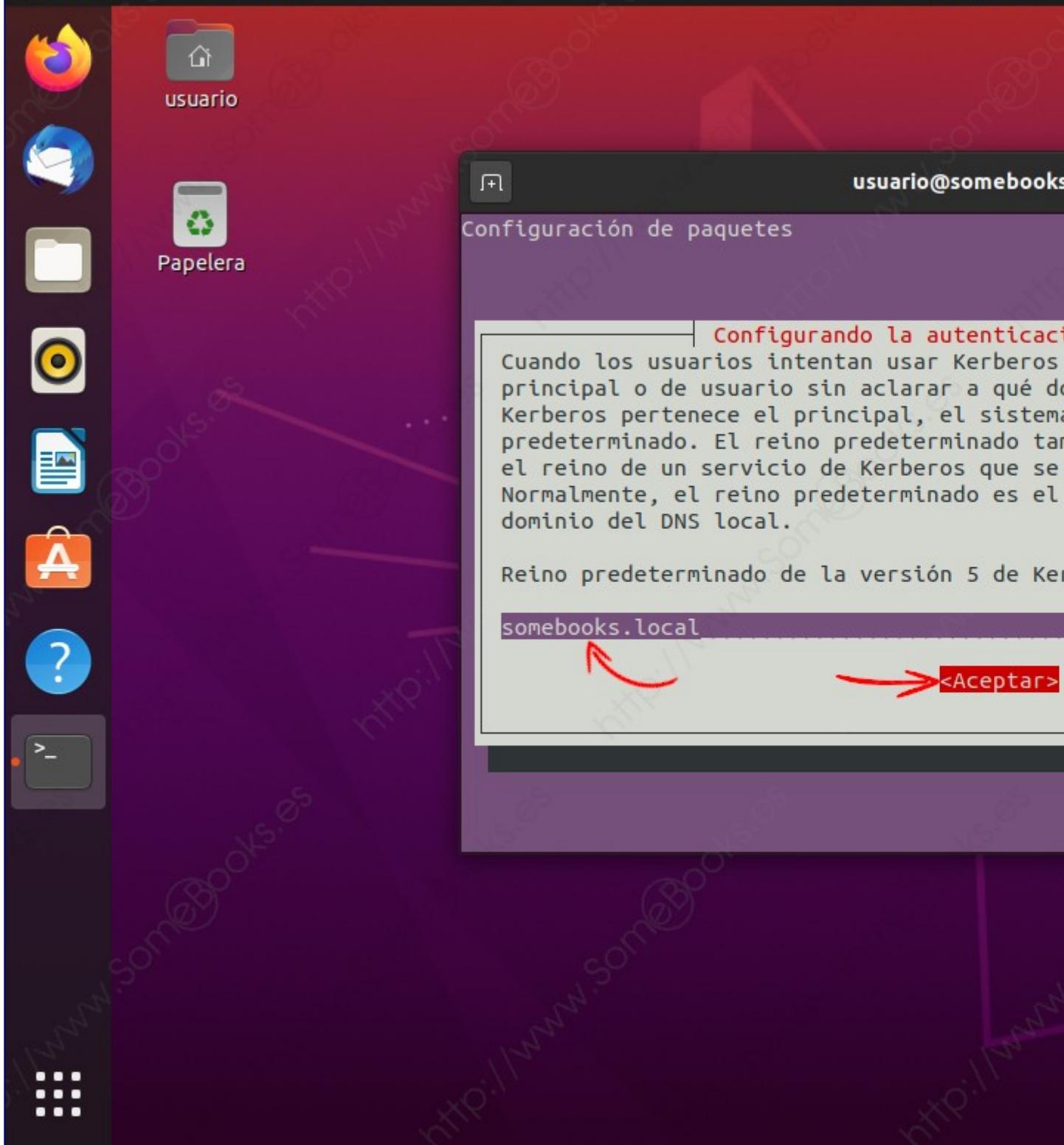
También ahora nos aparece un listado con todos los paquetes que van a actualizarse y un resumen final con el numero de paquetes que se actualizarán, los paquetes nuevos que se instalarán y los que se eliminarán de la instalación. Y de nuevo se incluye la cantidad de información que se descargará de los repositorios y la capacidad final que se utilizará en nuestro disco duro.

De nuevo, si estamos de acuerdo con todo, pulsaremos la tecla S para continuar.



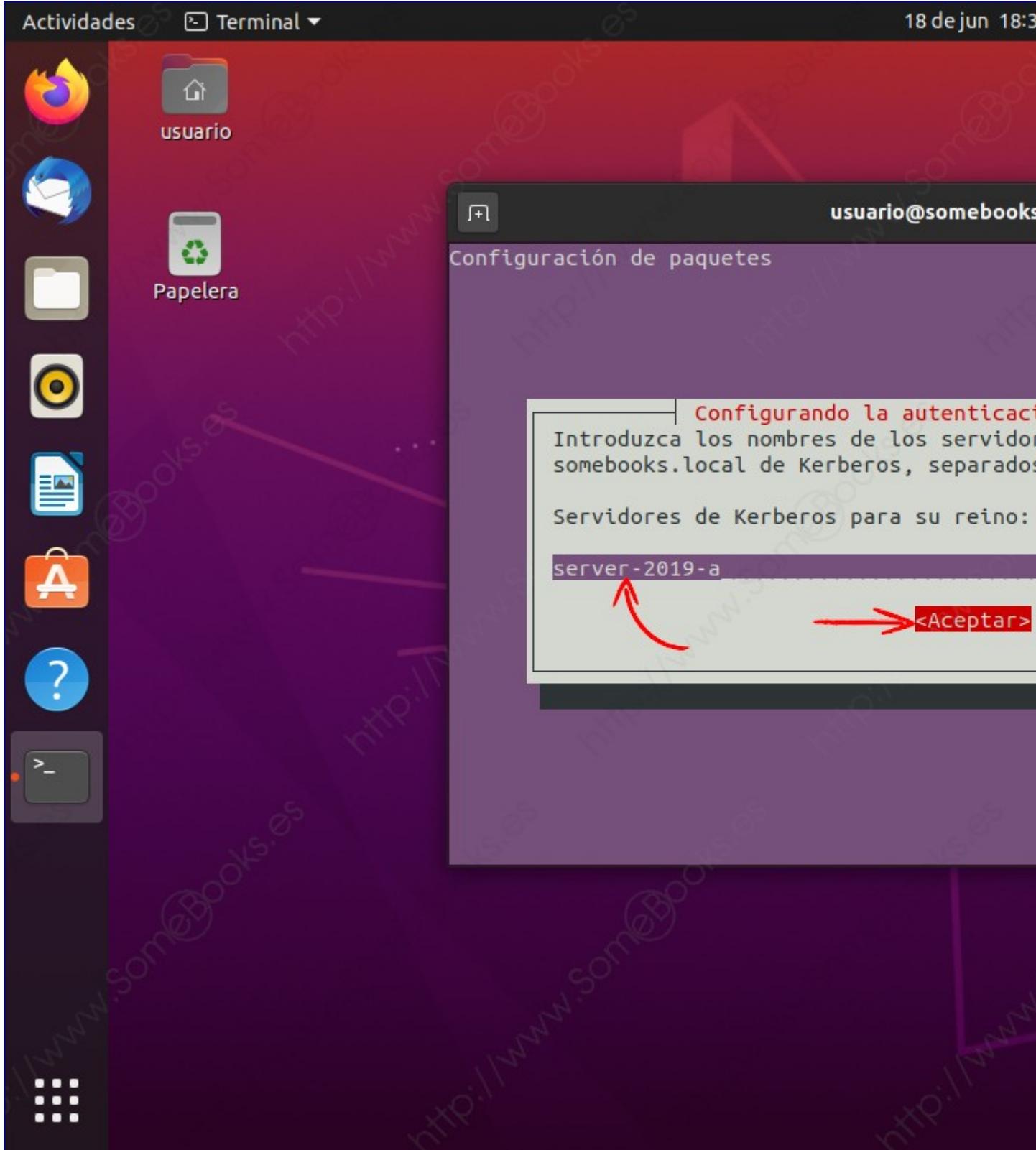
Cuando llegue el momento de instalar *Kerberos*, nos preguntará por el reino (realm en inglés). En realidad, se refiere al nombre del dominio al que vamos a unirnos. Para nuestro ejemplo, debemos escribir el nombre del dominio que hemos venido usando para los artículos mencionados al principio: *somebooks.local*.

Después, pulsamos la tecla de tabulación (Tab) para seleccionar *Aceptar* y a continuación la tecla Intro.



Después, el instalador nos solicita el nombre de los servidores de *Kerberos* para nuestro reino. En este caso, se refiere al controlador de dominio, que en nuestro ejemplo se llama *server-2019-a*, por lo que procedemos a escribir su nombre.

Como antes, una vez relleno el valor correcto, nos desplazamos hasta *Aceptar* y pulsamos la tecla **Intro**.



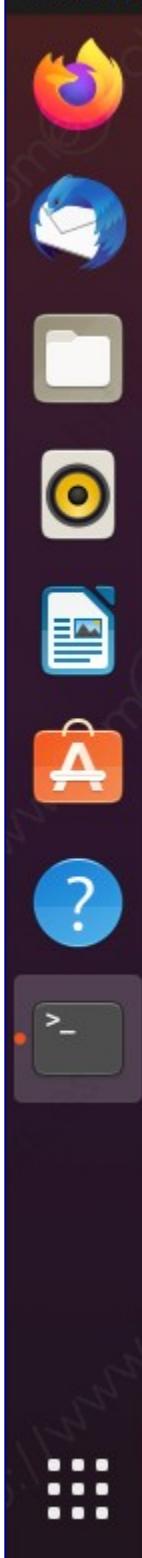
Por último, nos solicita el nombre del equipo que actúa como servidor administrativo para la autenticación en el dominio. Como en nuestro caso es el mismo, volvemos a escribir el nombre del servidor.

... Y de nuevo nos desplazamos hasta *Aceptar* y pulsamos la tecla **Intro**.

Actividades

Terminal ▾

18 de jun 18:3



usuario@somebooks

Configuración de paquetes

Configurando la autenticación Kerberos
Introduzca el nombre del servidor administrativo para el reino somebooks.local de Kerberos.

Servidor administrativo para su reino de Kerberos:

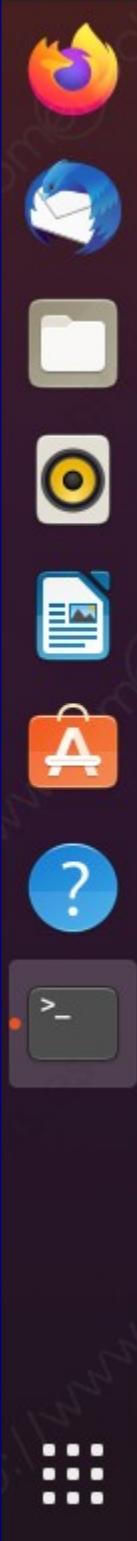
server-2019-a



→ <Aceptar>

Después de esto, la instalación continuará un poco más, pero sin necesitar que aportemos más información.

Solo tenemos que esperar hasta que se complete.



+

usuario@somebooks

```
Desempaquetando libnss-sss:amd64 (2.2.3-3ubuntu0.4) ... Seleccionando el paquete libpam-sss:amd64 previamente desempaquetado. Preparando para desempaquetar .../22-libpam-sss:amd64 ... Desempaquetando libpam-sss:amd64 (2.2.3-3ubuntu0.4) ... Seleccionando el paquete libsss-certmap0 previamente desempaquetado. Preparando para desempaquetar .../23-libsss-certmap0 ... Desempaquetando libsss-certmap0 (2.2.3-3ubuntu0.4) ... Seleccionando el paquete libsss-idmap0 previamente desempaquetado. Preparando para desempaquetar .../24-libsss-idmap0 ... Desempaquetando libsss-idmap0 (2.2.3-3ubuntu0.4) ... Seleccionando el paquete libsss-nss-idmap0 previamente desempaquetado. Preparando para desempaquetar .../25-libsss-nss-idmap0 ... Desempaquetando libsss-nss-idmap0 (2.2.3-3ubuntu0.4) ... Seleccionando el paquete libsss-sudo previamente desempaquetado. Preparando para desempaquetar .../26-libsss-sudo ... Desempaquetando libsss-sudo (2.2.3-3ubuntu0.4) ... Seleccionando el paquete python3-sss previamente desempaquetado. Preparando para desempaquetar .../27-python3-sss ... Desempaquetando python3-sss (2.2.3-3ubuntu0.4) ...
```

■ Progreso: [36%] [#####.....]

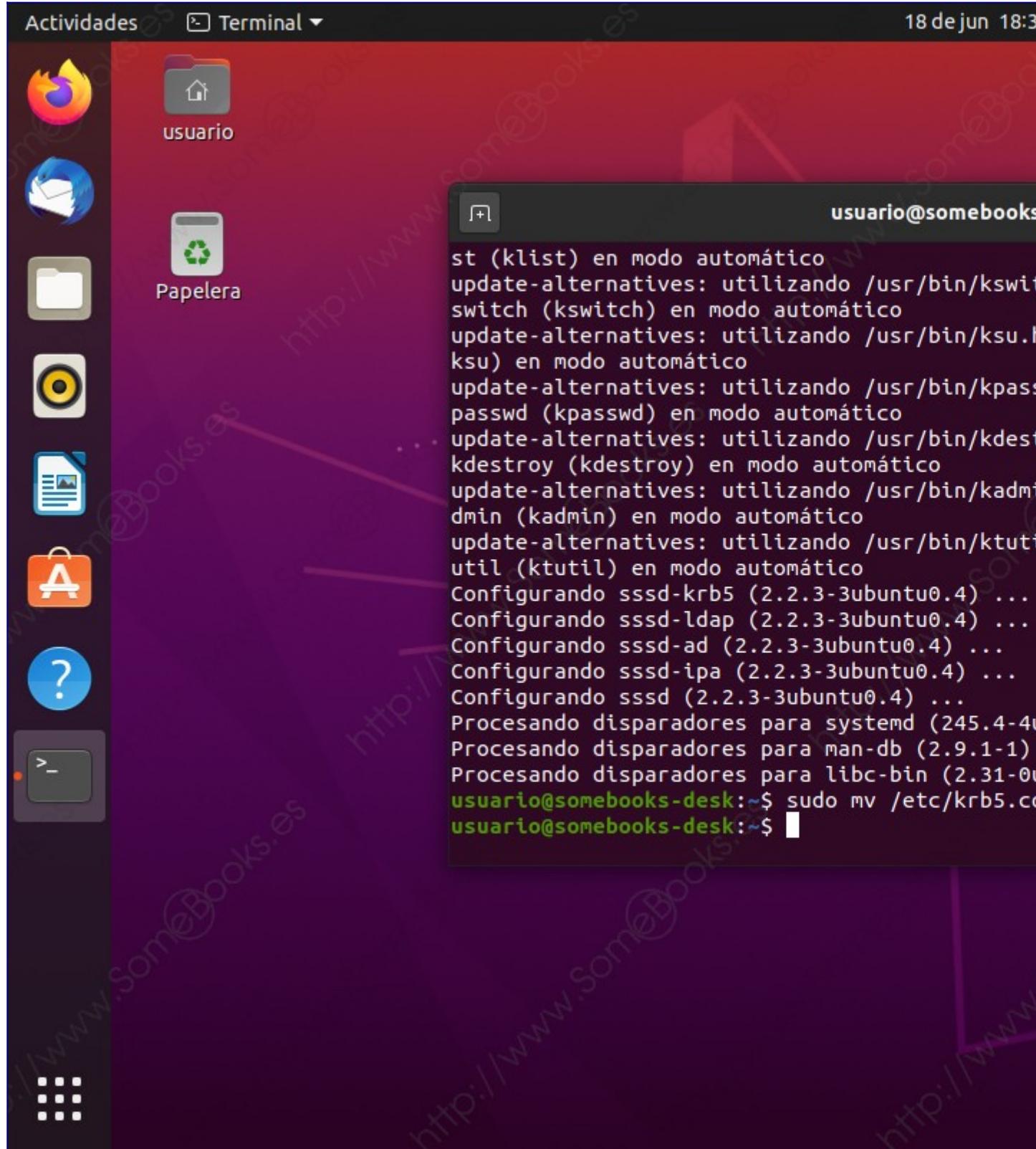
Configurar Kerberos

Con la información que hemos aportado durante la instalación (el nombre del dominio, o reino en la terminología *Kerberos* y el nombre del equipo que actúa como controlador de dominio), debería ser suficiente. Sin embargo, debemos añadir más información a la configuración de *Kerberos* para que se comporte de forma adecuada en el dominio.

Comenzaremos por cambiar el nombre del archivo de configuración, para poder volver a los parámetros originales si fuese preciso. Y lo conseguiremos con una orden como esta:

```
sudo mv /etc/krb5.conf /etc/krb5.conf.default
```

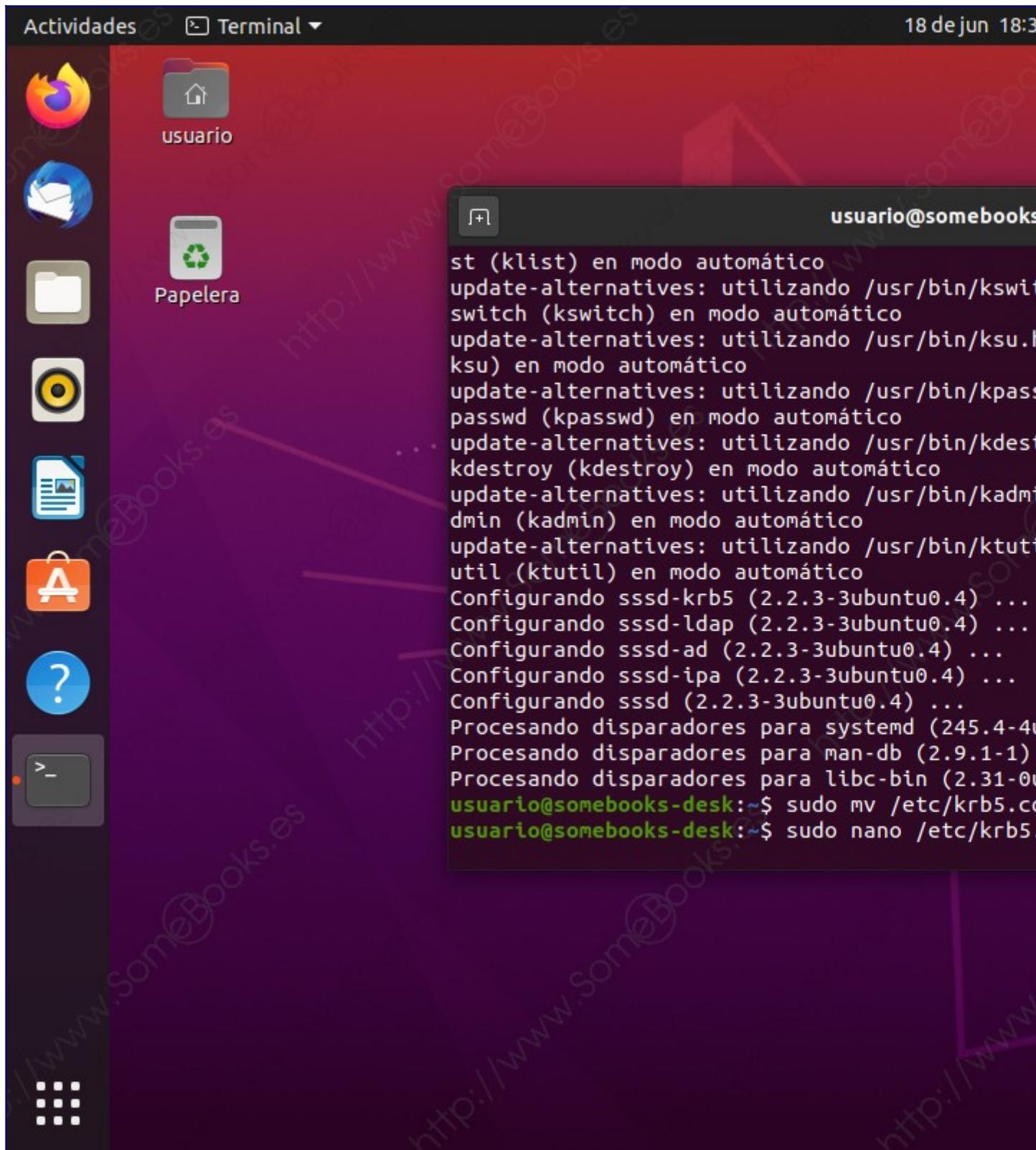
La escribimos y pulsamos la tecla **Intro**.



A continuación, volveremos a utilizar el editor *nano* para crear un nuevo archivo de configuración:

```
sudo nano /etc/krb5.conf
```

Como antes, solo tenemos que escribir la orden y pulsar la tecla Intro.



Al hacerlo, conseguiremos un documento vacío, donde escribiremos lo siguiente:

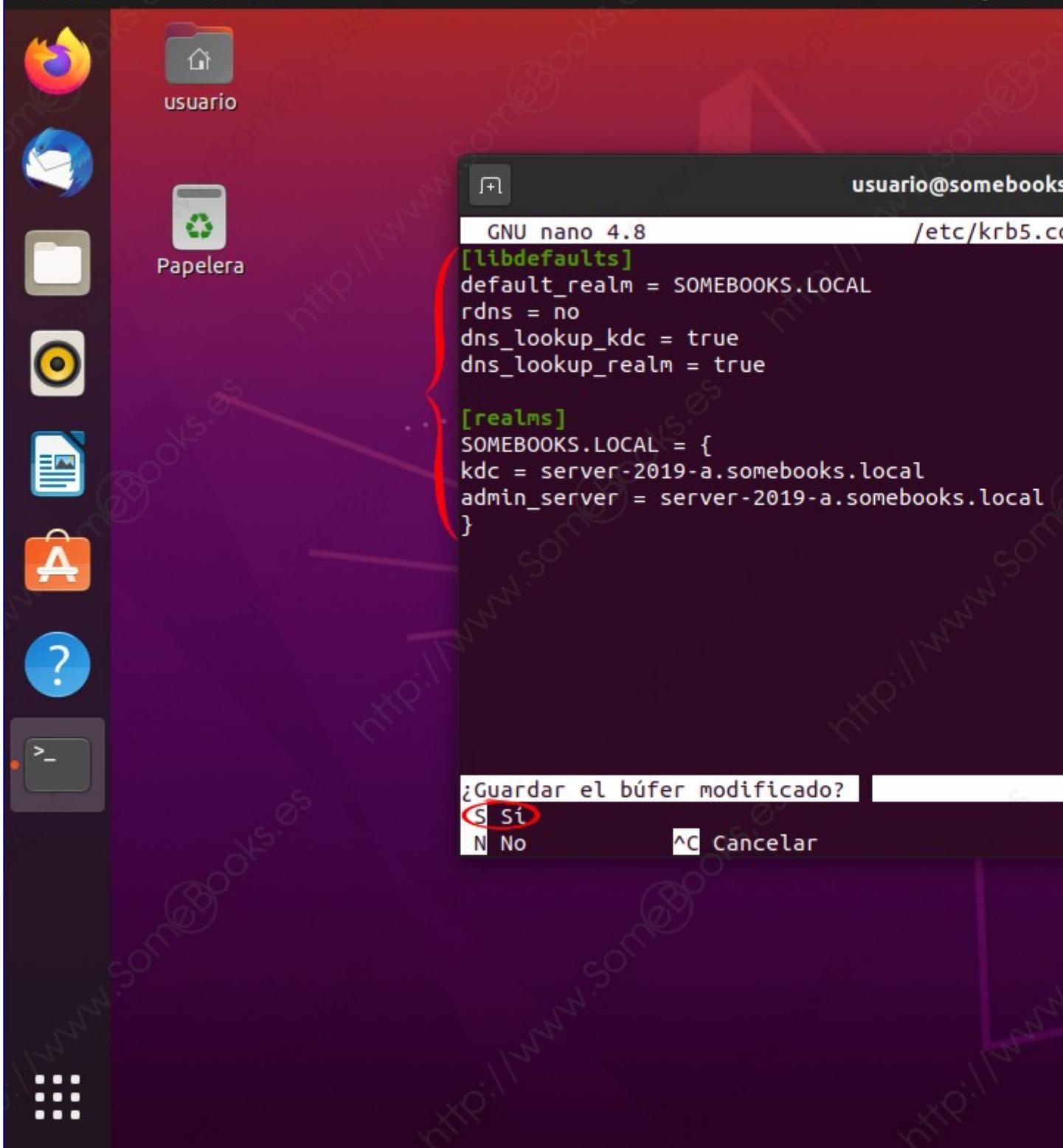
```
[libdefaults]
default_realm = SOMEBOOKS.LOCAL
rdns = no
dns_lookup_kdc = true
```

```
dns_lookup_realm = true

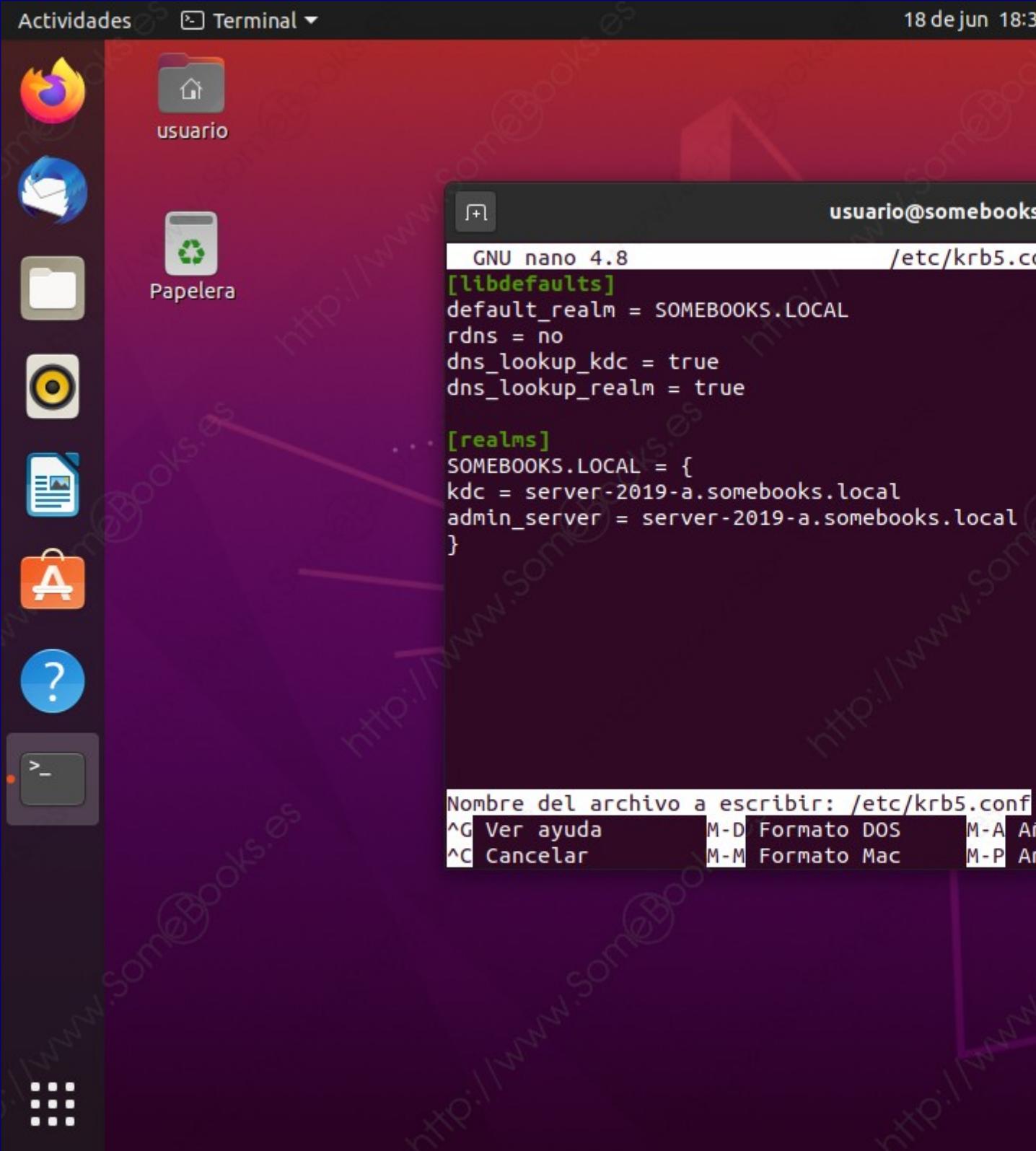
[realms]
SOMEBOOKS.LOCAL = {
kdc = server-2019-a.somebooks.local
admin_server = server-2019-a.somebooks.local
}
```

Cuando estemos listos, pulsamos la combinación de teclas **Ctrl + X** para cerrar el editor de textos.

Cuando el editor nos pregunte si queremos guardar los cambios, pulsamos la tecla **S**.



... Y, a continuación, pulsamos la tecla Intro para conservar el mismo nombre de archivo.



Comprobar el funcionamiento de Kerberos

Para comprobar que la autenticación en el dominio, utilizando Kerberos, se produce de forma satisfactoria, utilizaremos el comando **kinit** y la cuenta *Administrador* del propio dominio:

```
kinit administrador
```

Si todo va bien, *Kerberos* nos pedirá la contraseña de la cuenta. Observa que nos muestra el nombre *dns* de la cuenta (*Administrador@SOMEBOOKS.LOCAL*), lo que nos permite confirmar que se trata de la cuenta correcta.

Escribimos la contraseña y pulsamos la tecla **Intro**.

The screenshot shows a Linux desktop environment with a dark theme. On the left is a vertical dock containing icons for a browser, file manager, terminal, and other applications. The main desktop has several desktop icons: a folder labeled 'usuario', a trash can labeled 'Papelera', and a system tray icon. A terminal window is open in the top right corner, displaying the following text:

```
Actividades Terminal ▾ 18 de jun 18:3
usuario@somebooks:~$ update-alternatives: utilizando /usr/bin/kswitch
switch (kswitch) en modo automático
update-alternatives: utilizando /usr/bin/ksu
ksu) en modo automático
update-alternatives: utilizando /usr/bin/kpasswd
passwd (kpasswd) en modo automático
update-alternatives: utilizando /usr/bin/kdestroy
kdestroy (kdestroy) en modo automático
update-alternatives: utilizando /usr/bin/kadm
dmin (kadmin) en modo automático
update-alternatives: utilizando /usr/bin/ktut
util (ktutil) en modo automático
Configurando sssd-krb5 (2.2.3-3ubuntu0.4) ...
Configurando sssd-ldap (2.2.3-3ubuntu0.4) ...
Configurando sssd-ad (2.2.3-3ubuntu0.4) ...
Configurando sssd-ipa (2.2.3-3ubuntu0.4) ...
Configurando sssd (2.2.3-3ubuntu0.4) ...
Procesando dispositores para systemd (245.4-4)
Procesando dispositores para man-db (2.9.1-1)
Procesando dispositores para libc-bin (2.31-0
usuario@somebooks-desk:~$ sudo mv /etc/krb5.co
usuario@somebooks-desk:~$ sudo nano /etc/krb5
usuario@somebooks-desk:~$ kinit administrador
administrador@SOMEBOOKS.LOCAL's Password: ↵
```

Si la salida no nos ofrece ningún tipo de error, es porque el proceso de autenticación ha funcionado correctamente. No obstante, utilizaremos el comando **klist** para estar completamente seguros.

klist muestra la información sobre el *ticket de autenticación*, incluida la fecha y hora de concesión, de caducidad, la cuenta y el dominio que estamos empleando.

klist

Ejecución del comando Ejecución del comando klist..

The screenshot shows a Linux desktop environment with a dark theme. On the left is a vertical dock containing icons for various applications like a browser, file manager, and system tools. A terminal window titled "Terminal" is open in the center, displaying the output of the "klist" command. The terminal shows the user "usuario" at "somebooks" has run several configuration scripts for "sssd-krb5", "sssd-ldap", "sssd-ad", and "sssd-ipa". It then proceeds to run "sudo mv" and "sudo nano" commands on the "/etc/krb5.conf" file. Finally, it runs "kinit administrador" and "klist" to check the credentials cache. A red arrow points from the bottom right towards the "klist" command in the terminal. A red curly brace is placed over the configuration steps, highlighting the initial setup phase.

```
update-alternatives: utilizando /usr/bin/kadmin en modo automático
update-alternatives: utilizando /usr/bin/ktutil en modo automático
Configurando sssd-krb5 (2.2.3-3ubuntu0.4) ...
Configurando sssd-ldap (2.2.3-3ubuntu0.4) ...
Configurando sssd-ad (2.2.3-3ubuntu0.4) ...
Configurando sssd-ipa (2.2.3-3ubuntu0.4) ...
Configurando sssd (2.2.3-3ubuntu0.4) ...
Procesando disparadores para systemd (245.4-4)
Procesando disparadores para man-db (2.9.1-1)
Procesando disparadores para libc-bin (2.31-0)
usuario@somebooks-desk:~$ sudo mv /etc/krb5.conf /etc/krb5.conf.bak
usuario@somebooks-desk:~$ sudo nano /etc/krb5.conf
usuario@somebooks-desk:~$ kinit administrador
administrador@SOMEBOOKS.LOCAL's Password:
usuario@somebooks-desk:~$ klist ←
Credentials cache: FILE:/tmp/krb5cc_1000
Principal: administrador@SOMEBOOKS.LOCAL
          Issued                         Expires
Jun 18 18:36:09 2021  Jun 19 04:36:09 2021  k
AL
usuario@somebooks-desk:~$ █
```

Unir el cliente al dominio

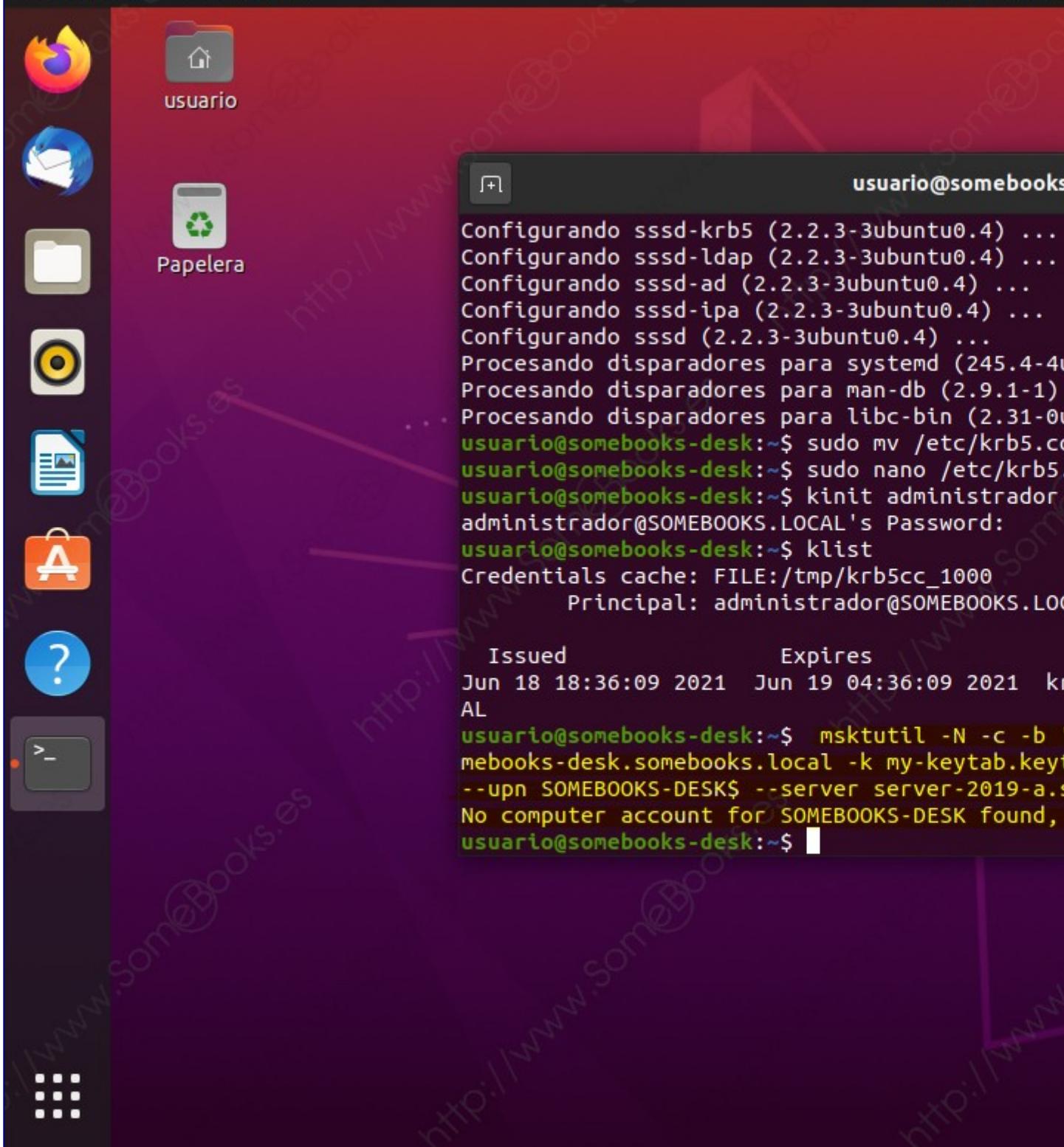
Una vez que nos hemos asegurado del funcionamiento de kerberos, la comprobación definitiva será unir el equipo al dominio de *Windows Server 2019*. Para lograrlo, usaremos el comando **msktutil** con la siguiente sintaxis:

```
msktutil -N -c -b 'CN=COMPUTERS' -s SOMEBOOKS-DESK/somebooks-
desk.somebooks.local -k my-keytab.keytab --computer-name SOMEBOOKS-DESK --upn
SOMEBOOKS-DESK$ --server server-2019-a.somebooks.local --user-creds-only
```

Como el comando es un poco largo, haremos un resumen con la función de los argumentos empleados, para que entiendas lo que estamos haciendo:

- **-N** le dice al comando que no realiza búsquedas DNS inversas para canonizar el nombre del dominio (recuerda que no hemos configurado la red para utilizar el DNS del servidor).
- **-c** indica que debe crearse un *keytab* predeterminado.
- **-b** establece el contenedor donde debe crearse la cuenta para el equipo dentro del dominio. En nuestro caso será dentro de *COMPUTERS*.
- **-s** incluye el equipo responsable de servicio para añadir a la cuenta. Tiene la forma <servicio>/<nombre de host>. En nuestro caso, será *SOMEBOOKS-DESK/somebooks-
desk.somebooks.local*.
- **-k** contiene el nombre del archivo que se usará para almacenar el *keytab*. Para nuestro ejemplo, será *my-keytab.keytab*.
- **--computer-name** indica el nombre con el que se creará la cuenta del equipo en el directorio.
- **--upn** establece el nombre de usuario principal del equipo. En su lugar usaremos el nombre del equipo, lo que se especifica incluyéndolo seguido de un carácter \$ como hemos incluido en nuestro ejemplo (*SOMEBOOKS-DESK\$*).
- **--server** identifica al controlador de dominio. En nuestro caso, *server-2019-
a.somebooks.local*.
- **--user-creds-only** fuerza a que se utilicen las credenciales de usuario. En este caso, las de kinit.

Una vez escrito el comando, pulsamos la tecla **Intro**.



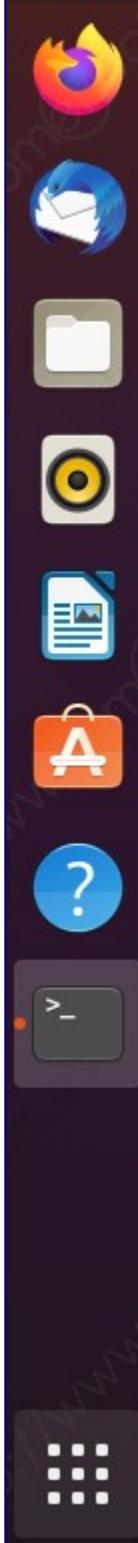
Como en el argumento `-s` hemos incluido el *nombre DNS* del equipo (para nuestro ejemplo, `somebooks-desk.somebooks.local`), a continuación, repetiremos la misma orden usando el *nombre NetBIOS* (en nuestro caso, `somebooks-desk`):

```
msktutil -N -c -b 'CN=COMPUTERS' -s SOMEBOOKS-DESK/somebooks-desk -k my-keytab.keytab --computer-name SOMEBOOKS-DESK --upn SOMEBOOKS-DESK$ --server server-2019-a.somebooks.local --user-creds-only
```

Volvemos a escribir el comando y pulsamos de nuevo la tecla **Intro**.

Actividades Terminal ▾

18 de jun 18:3



```
Configurando sssd-ipa (2.2.3-3ubuntu0.4) ...
Configurando sssd (2.2.3-3ubuntu0.4) ...
Procesando disparadores para systemd (245.4-4)
Procesando disparadores para man-db (2.9.1-1)
Procesando disparadores para libc-bin (2.31-0
usuario@somebooks-desk:~$ sudo mv /etc/krb5.co
usuario@somebooks-desk:~$ sudo nano /etc/krb5
usuario@somebooks-desk:~$ kinit administrador
administrador@SOMEBOOKS.LOCAL's Password:
usuario@somebooks-desk:~$ klist
Credentials cache: FILE:/tmp/krb5cc_1000
Principal: administrador@SOMEBOOKS.LOCAL
          Issued                         Expires
Jun 18 18:36:09 2021  Jun 19 04:36:09 2021  kr
AL
usuario@somebooks-desk:~$ msktutil -N -c -b
mebooks-desk.somebooks.local -k my-keytab.keyt
--upn SOMEBOOKS-DESK$ --server server-2019-a.s
No computer account for SOMEBOOKS-DESK found,
usuario@somebooks-desk:~$ msktutil -N -c -b 'c
ebooks-desk -k my-keytab.keytab --computer-na
ESK$ --server server-2019-a.somebooks.local --
usuario@somebooks-desk:~$
```

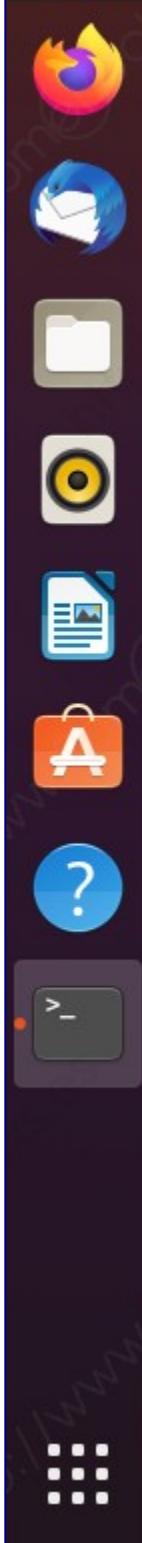
Para completar la tarea, eliminaremos los *tickets de autorización* de kerberos que activamos al ejecutar **kinit**. Para lograrlo, basta con utilizar el comando **kdestroy**.

kdestroy

Escribimos el comando y pulsamos la tecla **Intro**.

Actividades Terminal

18 de jun 18:3



usuario
Papelera

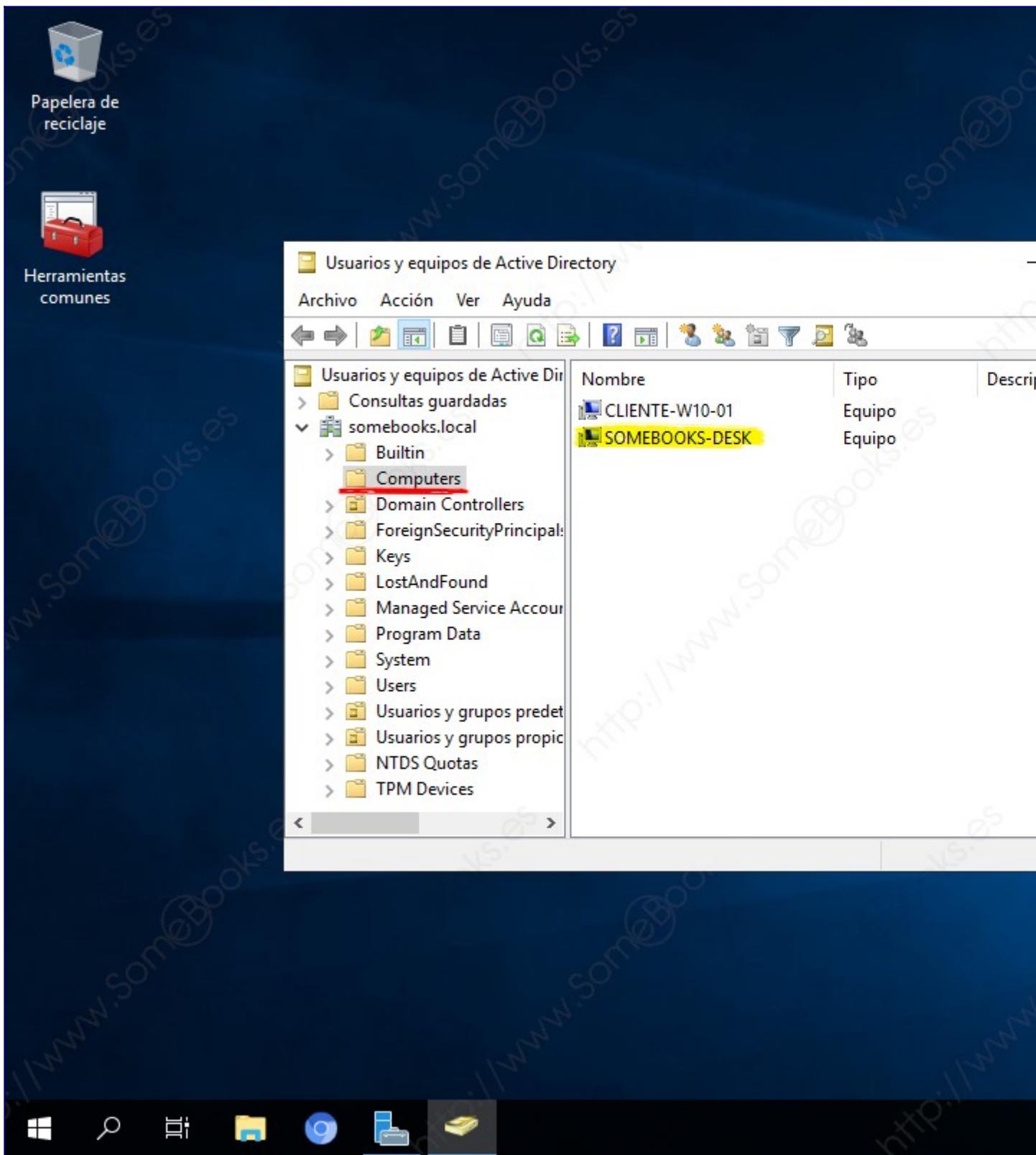
```
Configurando sssd (2.2.3-3ubuntu0.4) ...
Procesando disparadores para systemd (245.4-4)
Procesando disparadores para man-db (2.9.1-1)
Procesando disparadores para libc-bin (2.31-0)
usuario@somebooks-desk:~$ sudo mv /etc/krb5.conf /etc/krb5.conf.bak
usuario@somebooks-desk:~$ sudo nano /etc/krb5.conf
usuario@somebooks-desk:~$ kinit administrador
administrador@SOMEBOOKS.LOCAL's Password:
usuario@somebooks-desk:~$ klist
Credentials cache: FILE:/tmp/krb5cc_1000
Principal: administrador@SOMEBOOKS.LOCAL

Issued                                         Expires
Jun 18 18:36:09 2021   Jun 19 04:36:09 2021  krb5cc_1000@SOMEBOOKS-DESK
AL

usuario@somebooks-desk:~$ msktutil -N -c -b
mebooks-desk.somebooks.local -k my-keytab.keytab
--upn SOMEBOOKS-DESK$ --server server-2019-a.somebooks.local
No computer account for SOMEBOOKS-DESK found,
usuario@somebooks-desk:~$ msktutil -N -c -b 'O
ebooks-desk -k my-keytab.keytab --computer-name=ESK$ --server server-2019-a.somebooks.local
usuario@somebooks-desk:~$ kdestroy
usuario@somebooks-desk:~$ █
```

Por último, podemos comprobar que el equipo se ha unido correctamente al dominio usando la herramienta *Usuarios y equipos de Active Directory* en el *controlador de dominio* de Windows Server.

En el contenedor *Computers* debe aparecer el equipo *Ubuntu* que acabamos de incorporar.



Con esto, damos por concluida la primera parte del trabajo, pero no olvides que la tarea no estará completa hasta que no apliques el resto de los cambios, que te explicaremos el próximo artículo.

Configurar SSSD

Como dijimos al principio del artículo anterior, *SSSD* (*System Security Services Daemon*) es un conjunto de demonios que se encarga de administrar la autenticación y el acceso a los recursos remotos mediante *LDAP* y *Kerberos*, entre otros.

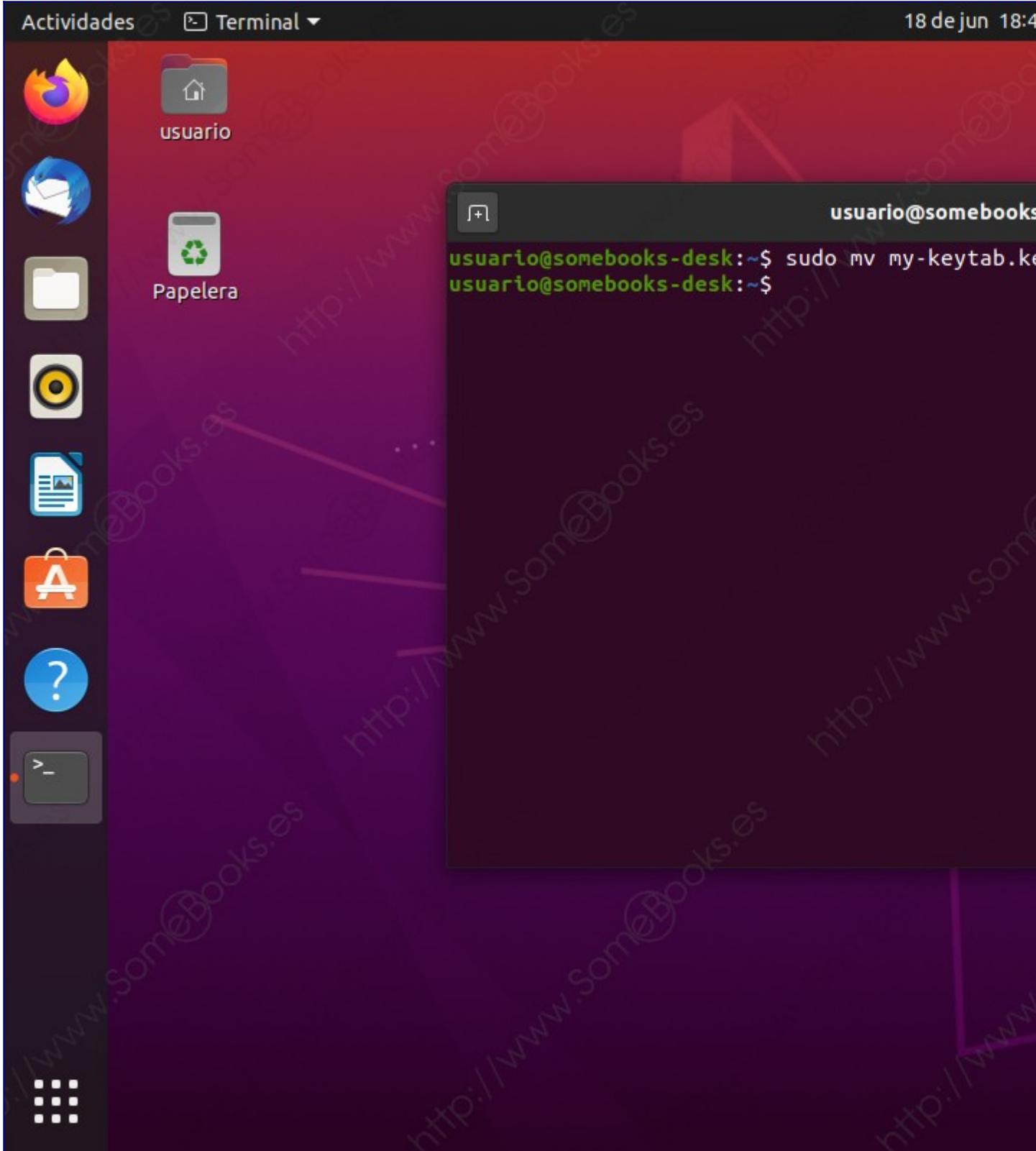
Como veremos más adelante, gracias a *SSSD*, podremos iniciar sesión en el equipo utilizando los datos de autenticación de una cuenta del dominio en lugar de hacerlo con una cuenta local.

SSSD ya debe encontrarse instalado en el sistema (lo incluimos en el conjunto de paquetes que instalamos al principio), pero ahora debemos configurarlo para que se comporte del modo adecuado.

Lo primero será mover el archivo *keytab* que generamos al unir el cliente *Ubuntu* al dominio, dentro de la carpeta adecuada para la configuración de *SSSD* (*/etc/sssd*). Lo conseguiremos con una orden como esta:

```
sudo mv my-keytab.keytab /etc/sssd/my-keytab.keytab
```

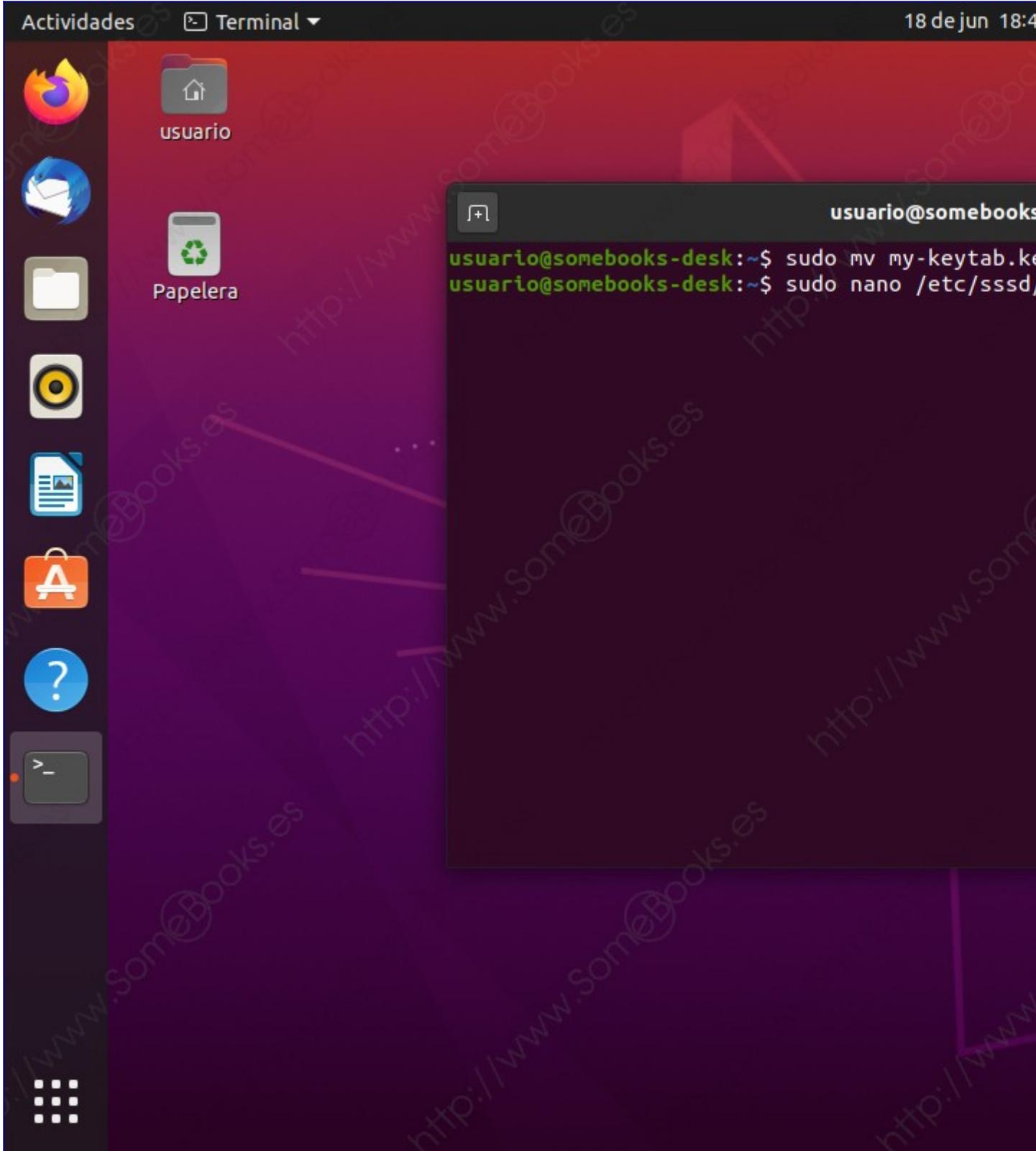
Escribimos el comando y pulsamos la tecla **Intro**.



A diferencia de *Kerberos*, para *SSSD* no tenemos un archivo de configuración predeterminado que debamos poner a salvo antes de comenzar. En este caso, solo tendremos que usar el editor de textos para crear uno nuevo con el contenido adecuado:

```
sudo nano /etc/sssd/sssd.conf
```

De nuevo, escribimos el comando y pulsamos la tecla **Intro**.



A continuación, copiaremos las siguientes líneas en el área de trabajo del editor... Pero no olvides modificar los valores que te indicamos en color rojo, para adaptarlos a los datos concretos de tu instalación:

```
[sssd]
services = nss, pam
config_file_version = 2
domains = somebooks.local
```

```
[nss]
entry_negative_timeout = 0
#debug_level = 5

[pam]
#debug_level = 5

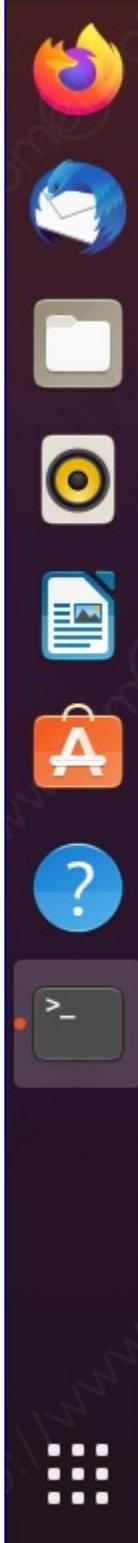
[domain/somebooks.local]
#debug_level = 10
enumerate = false
id_provider = ad
auth_provider = ad
chpass_provider = ad
access_provider = ad
dyndns_update = false
ad_hostname = somebooks-desk.somebooks.local
ad_server = server-2019-a.somebooks.local
ad_domain = somebooks.local
ldap_schema = ad
ldap_id_mapping = true
fallback_homedir = /home/%u
default_shell = /bin/bash
ldap_sasl_mech = gssapi
ldap_sasl_authid = SOMEBOOKS-DESK$
krb5_keytab = /etc/sssd/my-keytab.keytab
ldap_krb5_init_creds = true
```

Cuando estemos listos, pulsamos la combinación de teclas **Ctrl + X** para cerrar el editor de textos.

Cuando el editor nos pregunte si queremos guardar los cambios, pulsamos la tecla **S**.

Actividades Terminal ▾

18 de jun 18:4



usuario
Papelera

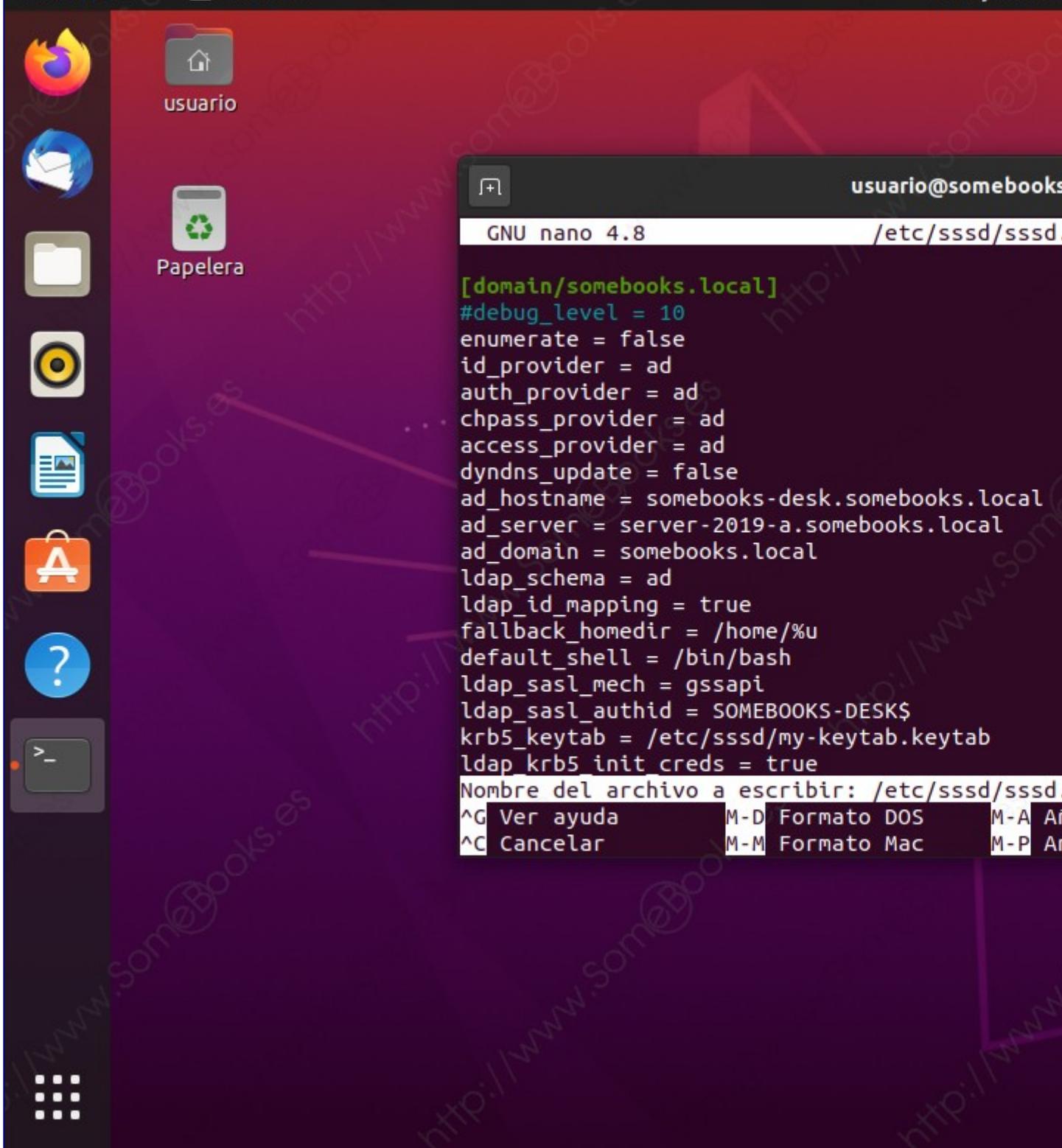
GNU nano 4.8 /etc/sssd/sssd.conf

```
[domain/somebooks.local]
#debug_level = 10
enumerate = false
id_provider = ad
auth_provider = ad
chpass_provider = ad
access_provider = ad
dyndns_update = false
ad_hostname = somebooks-desk.somebooks.local
ad_server = server-2019-a.somebooks.local
ad_domain = somebooks.local
ldap_schema = ad
ldap_id_mapping = true
fallback_homedir = /home/%u
default_shell = /bin/bash
ldap_sasl_mech = gssapi
ldap_sasl_authid = SOMEBOOKS-DESK$
krb5_keytab = /etc/sssd/my-keytab.keytab
ldap_krb5_init_creds = true
```

¿Guardar el búfer modificado?

S Sí N No ^C Cancelar

... Y, a continuación, pulsamos la tecla Intro para conservar el mismo nombre de archivo.



Antes de abandonar el archivo *sssd.conf*, deberemos asegurarnos de que sus permisos son los adecuados. El propietario es el único que debe tener permisos de lectura y escritura sobre el archivo, y para lograrlo, sólo tenemos que escribir lo siguiente:

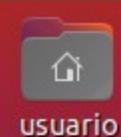
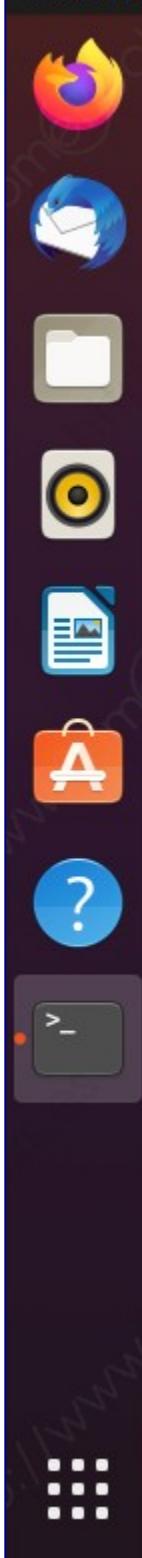
```
sudo chmod 0600 /etc/sssd/sssd.conf
```

Una vez más, escribimos el comando y pulsamos la tecla Intro.

Actividades

Terminal ▾

18 de jun 18:4



usuario@somebooks

```
usuario@somebooks-desk:~$ sudo mv my-keytab.keytab /etc/sss
usuario@somebooks-desk:~$ sudo nano /etc/sssd
usuario@somebooks-desk:~$ sudo chmod 0600 /etc/sss
usuario@somebooks-desk:~$ █
```

Puedes comprobar que el cambio ha surtido efecto recurriendo al comando ls:

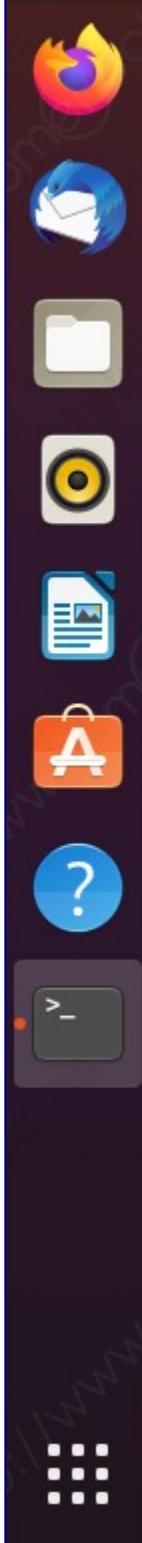
```
sudo ls -al /etc/sssd
```

Efectivamente, solo el propietario tiene permisos de lectura y escritura sobre el archivo...

Actividades

Terminal ▾

18 de jun 18:4



```
usuario@somebooks-desk:~$ sudo mv my-keytab.keytab /etc/sss...
usuario@somebooks-desk:~$ sudo nano /etc/sssd...
usuario@somebooks-desk:~$ sudo chmod 0600 /etc/sss...
usuario@somebooks-desk:~$ sudo ls -al /etc/sss...
total 28
drwx--x--x  3 sssd      sssd      4096 jun 18 18:18 .
drwxr-xr-x 131 root      root     12288 jun 18 18:18 ..
drwxr-xr-x  2 root      root     4096 feb 11 2018 .
-rw-----  1 usuario   usuario   2188 jun 18 18:18 my-keytab.keytab
-rw-----  1 root      root      651 jun 18 18:18 sssd.conf
usuario@somebooks-desk:~$ █
```

Ajustar el comportamiento de PAM para iniciar sesión con usuarios del dominio

En los años 90, la empresa *Sun Microsystems* desarrolló un *framework* llamado *Pluggable Authentication Modules (PAM)* que ofrecía una capa de abstracción para diferentes métodos de autenticación (contraseña, tarjeta, parámetros biométricos, etc.)

Tienes más información sobre la configuración de *PAM* en http://www.linux-pam.org/Linux-PAM-html/Linux-PAM_SAG.html

En *Ubuntu*, uno de los archivos de configuración de *PAM* es *common-session*, que contiene parámetros generales sobre el inicio de sesión. Entre ellos, la necesidad de crear un directorio de inicio para las cuentas de usuario.

Esto lo conseguiremos, para las cuentas que pertenecen al dominio, añadiendo el argumento **pam_mkdhomedir.so** en el archivo *common-session*. Al hacerlo, indicamos que se cree el directorio local, para cada cuenta, la primera vez que se inicie sesión con ella.

Para lograrlo, comenzaremos por editar el archivo de configuración:

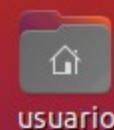
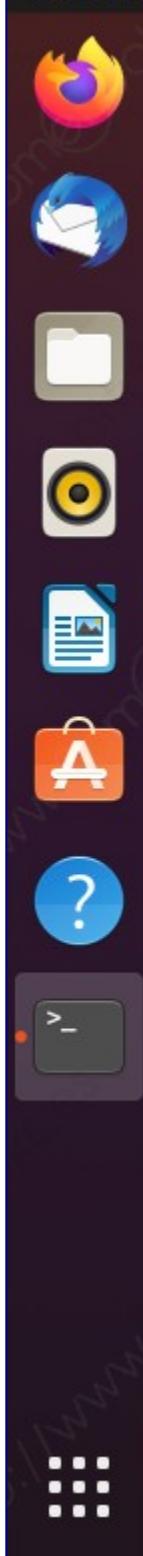
```
sudo nano /etc/pam.d/common-session
```

Como antes, escribimos el comando y pulsamos la tecla **Intro**.

Actividades

Terminal ▾

18 de jun 18:4



usuario@somebooks

```
usuario@somebooks-desk:~$ sudo mv my-keytab.keytab /etc/sss
usuario@somebooks-desk:~$ sudo nano /etc/sssd.conf
usuario@somebooks-desk:~$ sudo chmod 0600 /etc/sss
usuario@somebooks-desk:~$ sudo ls -al /etc/sss
total 28
drwx--x--x  3 sssd      sssd      4096 jun 18 18:42 .
drwxr-xr-x 131 root      root     12288 jun 18 18:42 ..
drwxr-xr-x  2 root      root     4096 feb 11 2018 .
-rw-----  1 usuario   usuario   2188 jun 18 18:42 my-keytab.keytab
-rw-----  1 root      root      651 jun 18 18:42 pam.conf
usuario@somebooks-desk:~$ sudo nano /etc/pam.conf
```



Cuando se haya abierto el editor de textos, buscamos una línea con el siguiente aspecto:

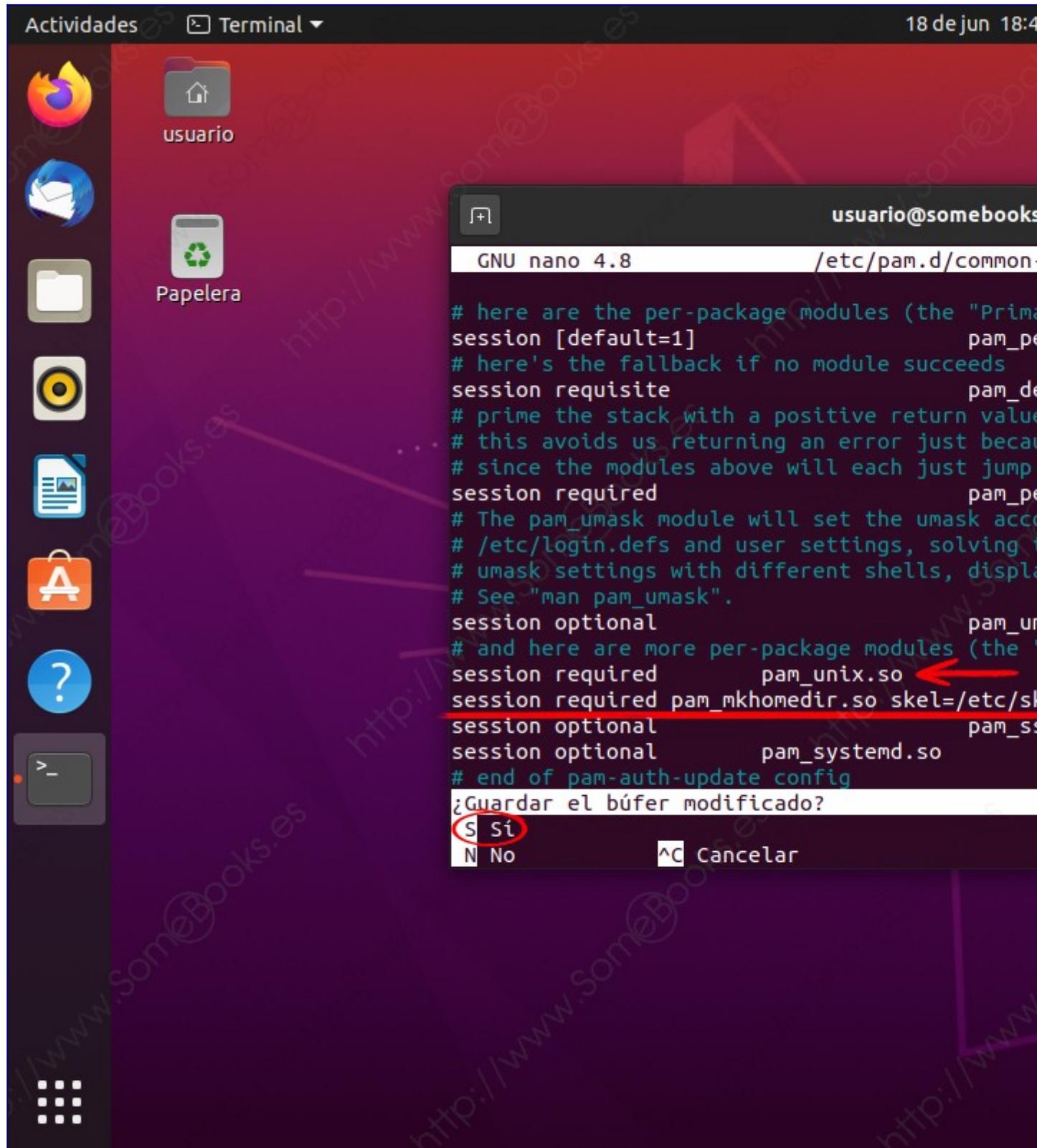
```
session required      pam_unix.so
```

Y justo debajo escribimos, o copiamos, la siguiente línea:

```
session required pam_mkhomedir.so skel=/etc/skel umask=0077
```

Como en ocasiones anteriores, cuando estemos listos, pulsamos la combinación de teclas **ctrl + X** para cerrar el editor de textos.

Cuando el editor nos pregunte si queremos guardar los cambios, pulsamos la tecla **S**.



... Y, a continuación, pulsamos la tecla **Intro** para conservar el mismo nombre de archivo.

Actividades

Terminal ▾

18 de jun 18:4



usuario@somebooks:

GNU nano 4.8

/etc/pam.d/common

```
# here are the per-package modules (the "Primary" modules)
session [default=1] pam_per
# here's the fallback if no module succeeds
session requisite pam_de
# prime the stack with a positive return value
# this avoids us returning an error just because
# since the modules above will each just jump
# session required pam_pe
# The pam_umask module will set the umask according to
# /etc/login.defs and user settings, solving the
# umask settings with different shells, displayed
# See "man pam_umask".
session optional pam_u
# and here are more per-package modules (the "Secondary" modules)
session required pam_unix.so
session required pam_mkhomedir.so skel=/etc/skel
session optional pam_s
session optional pam_systemd.so
# end of pam-auth-update config
```

Nombre del archivo a escribir: /etc/pam.d/common

^G Ver ayuda

M-D Formato DOS

M-A Ai

^C Cancelar

M-M Formato Mac

M-P Ar

... Y para que se apliquen los cambios, reiniciamos el servicio `sssd`:

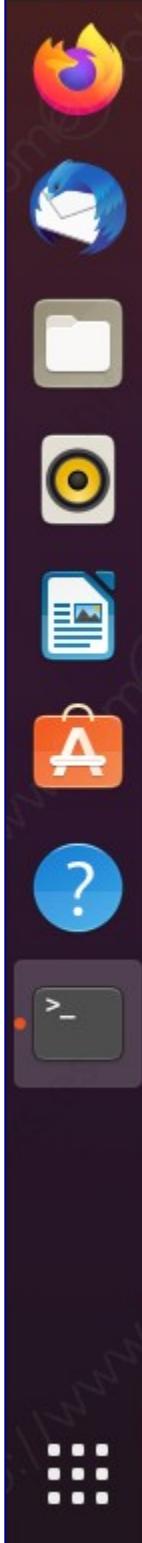
```
sudo systemctl restart sssd
```

Si no aparece ningún mensaje, el reinicio se ha producido de forma satisfactoria.

Actividades

Terminal ▾

18 de jun 18:42



```
usuario@somebooks-desk:~$ sudo mv my-keytab.keytab /etc/sss
usuario@somebooks-desk:~$ sudo nano /etc/sssd/sssd.conf
usuario@somebooks-desk:~$ sudo chmod 0600 /etc/sss/sssd.conf
usuario@somebooks-desk:~$ sudo ls -al /etc/sss
total 28
drwx--x--x  3 sssd      sssd      4096 jun 18 18:42 .
drwxr-xr-x 131 root      root     12288 jun 18 18:42 ..
drwxr-xr-x  2 root      root     4096 feb 11 2018 .
-rw-----  1 usuario   usuario   2188 jun 18 18:42 my-keytab.keytab
-rw-----  1 root      root      651 jun 18 18:42 sssd.conf
usuario@somebooks-desk:~$ sudo nano /etc/pam.d/common-auth
usuario@somebooks-desk:~$ sudo systemctl restart sssd
usuario@somebooks-desk:~$ █
```

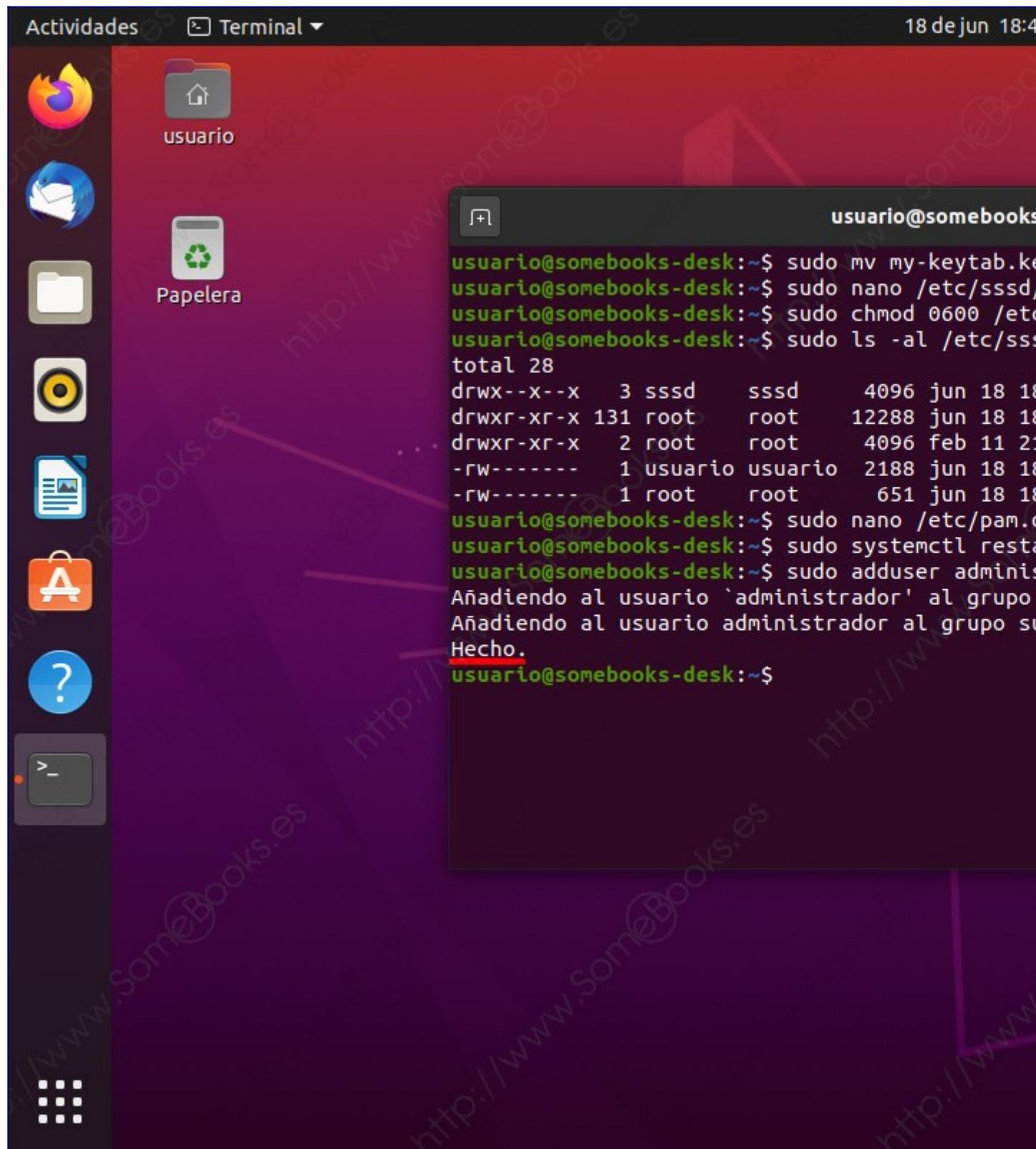
Convertir al administrador del dominio en administrador local

Si vamos a iniciar sesión con la cuenta *Administrador* del dominio de forma local en el equipo cliente, parece lógico que esta cuenta también tenga privilegios administrativos en el propio equipo.

Para lograrlo, solo tenemos que incluir dicha cuenta en el grupo sudo, para lo que podemos utilizar la siguiente orden:

```
sudo adduser administrador sudo
```

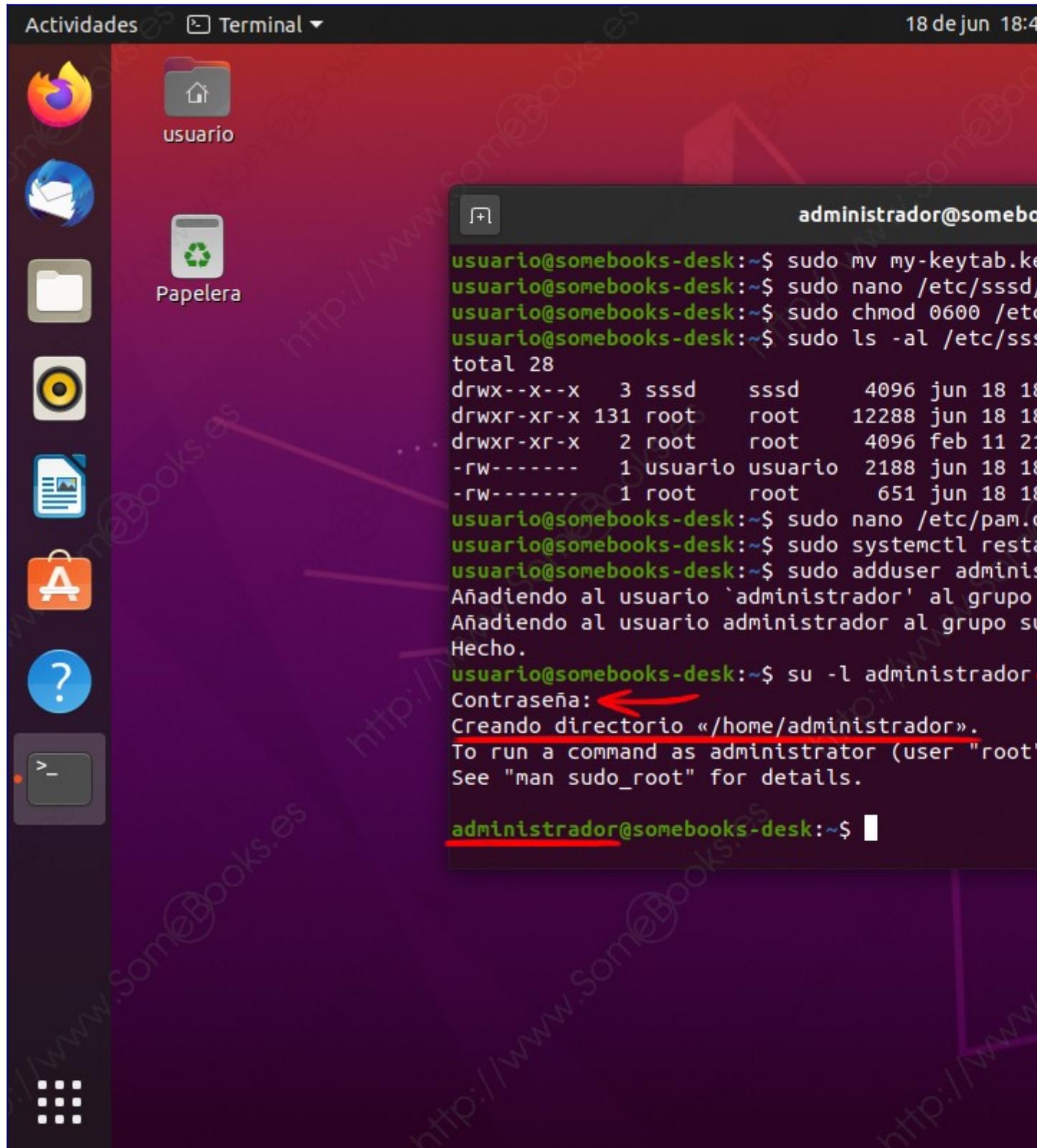
... Y comprobamos que la tarea se ejecuta correctamente.



A continuación, comprobamos que podemos autenticarnos con el usuario Administrador (recuerda que esta cuenta no existe localmente y que se trata de una cuenta del dominio). Para lograrlo, basta con escribir la orden:

```
su -l administrador
```

Al hacerlo, comprobamos que incluso se crea una nueva carpeta para la cuenta dentro de `/home`.

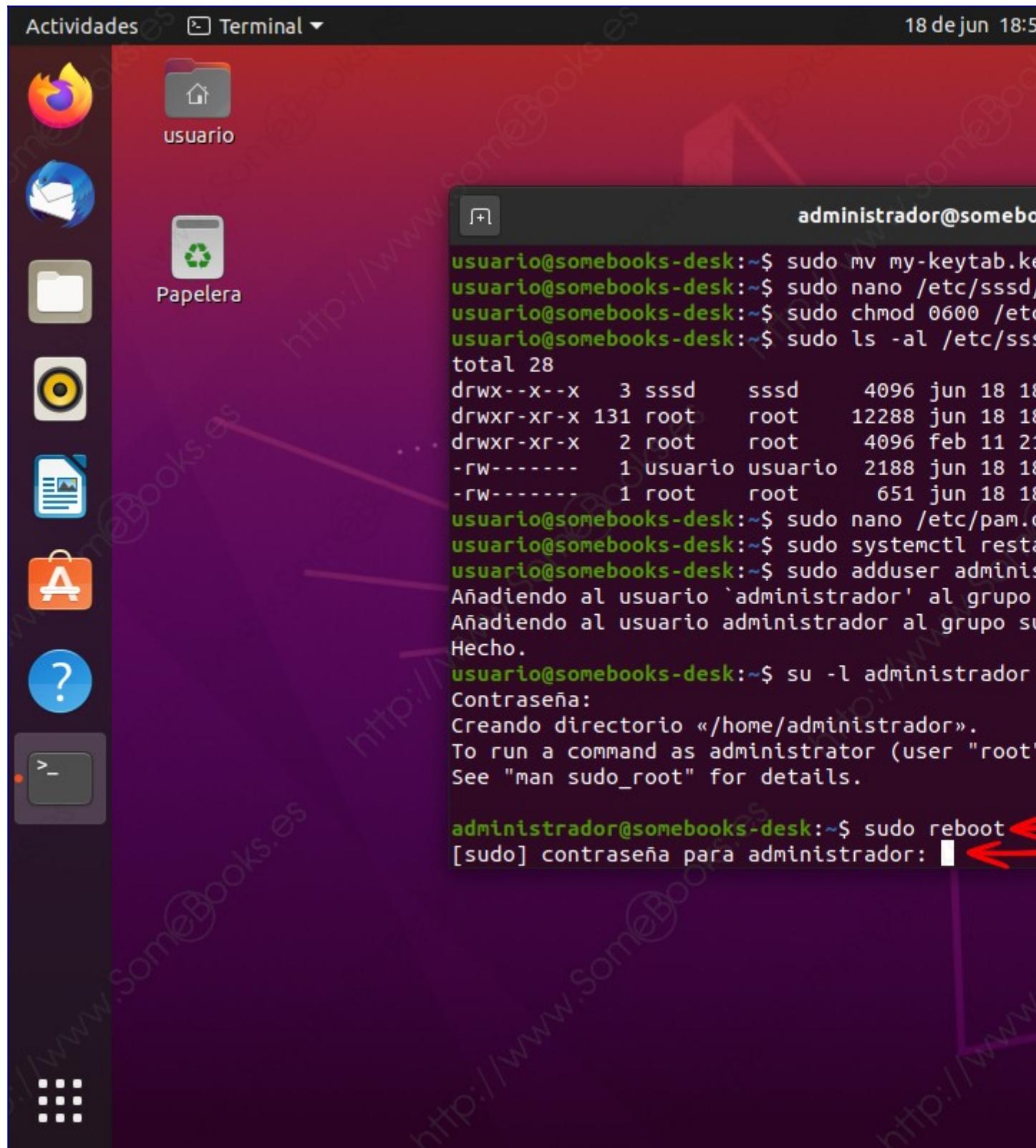


Reiniciar el equipo y comprobar el inicio de sesión gráfico

Para reiniciar el equipo, solo tenemos que recurrir a la orden:

```
sudo reboot
```

Escribimos el comando y pulsamos la tecla Intro.



Observa que ni siquiera tenemos que abandonar la cuenta *administrador*, ya que ahora forma parte del grupo *sudo*.

Al completar el reinicio, la interfaz gráfica nos muestra únicamente las cuentas de usuario que conoce. Sin embargo, si queremos iniciar sesión gráfica con la cuenta administrador, solo tenemos que usar la opción *¿No está en la lista?*.

Hacemos clic sobre *¿No está en la lista?*.



Esto nos ofrece la posibilidad de escribir el nombre de la cuenta de usuario que queremos utilizar. En nuestro caso, la cuenta *administrador*.

Ten en cuenta que *Windows Server* no diferencia entre mayúsculas y minúsculas, y suele mostrar el nombre de la cuenta con la primera letra en mayúscula (*Administrador*). Sin embargo, *Ubuntu* sí que diferencia y utiliza el nombre de la cuenta escrito completamente en minúscula (*administrador*)

Observa que ponemos delante el nombre del dominio para que *gdm* sepa donde encontrar la información de autenticación.



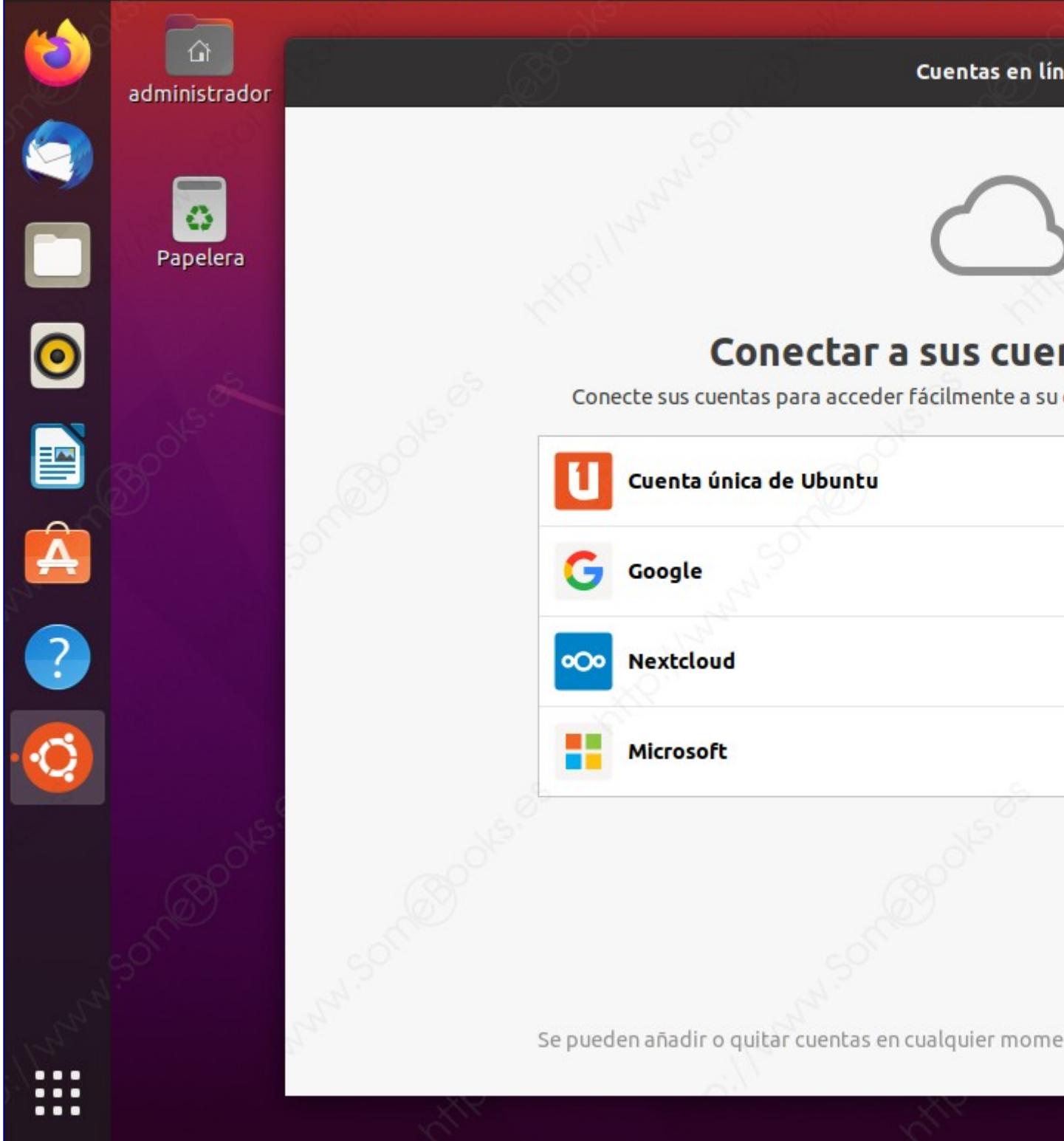
Al pulsar la tecla **Intro**, se nos pedirá también la contraseña.

Escribiremos la contraseña de la cuenta *Administrador* en el dominio *Windows Server*.



Inmediatamente veremos cómo se inicia sesión en la interfaz gráfica.

Y, como es la primera vez que iniciamos sesión gráfica con esa cuenta, nos aparecerá el asistente de bienvenida.



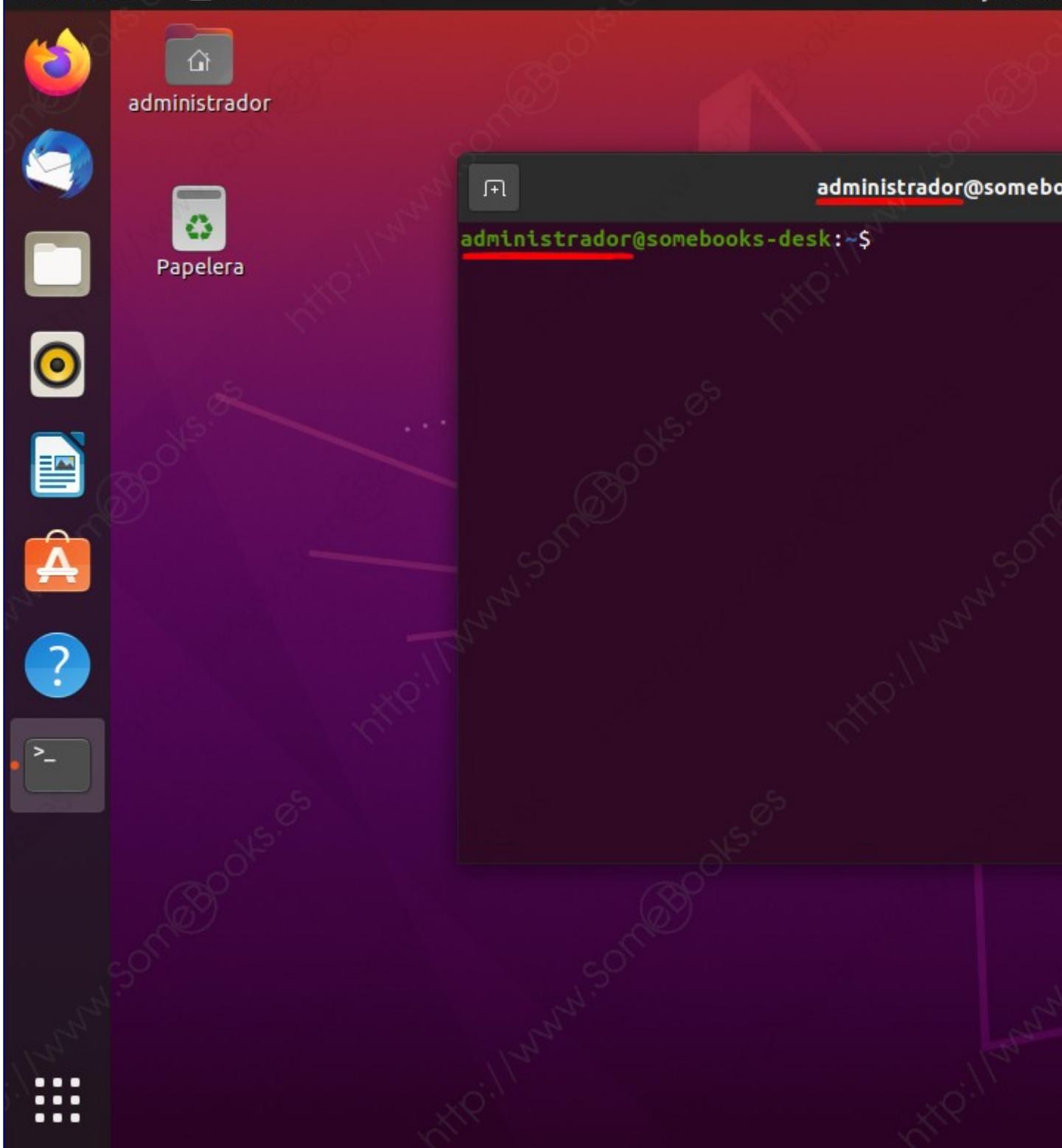
Cuando hayamos completado el asistente, si abrimos una ventana de *Terminal* (*Alt + Control + T*), podemos comprobar que nos encontramos en la cuenta correcta.

Solo tenemos que fijarnos en el título de la ventana o en el *prompt* del sistema.

Actividades

Terminal ▾

18 de jun 19:00



Si ahora cerramos la sesión, comprobaremos que en la pantalla de autenticación ya sí aparece la cuenta *Administrador*... Incluso con la inicial en mayúscula, al estilo *Windows*.

Ya no tendremos que volver a escribir el nombre de la cuenta.

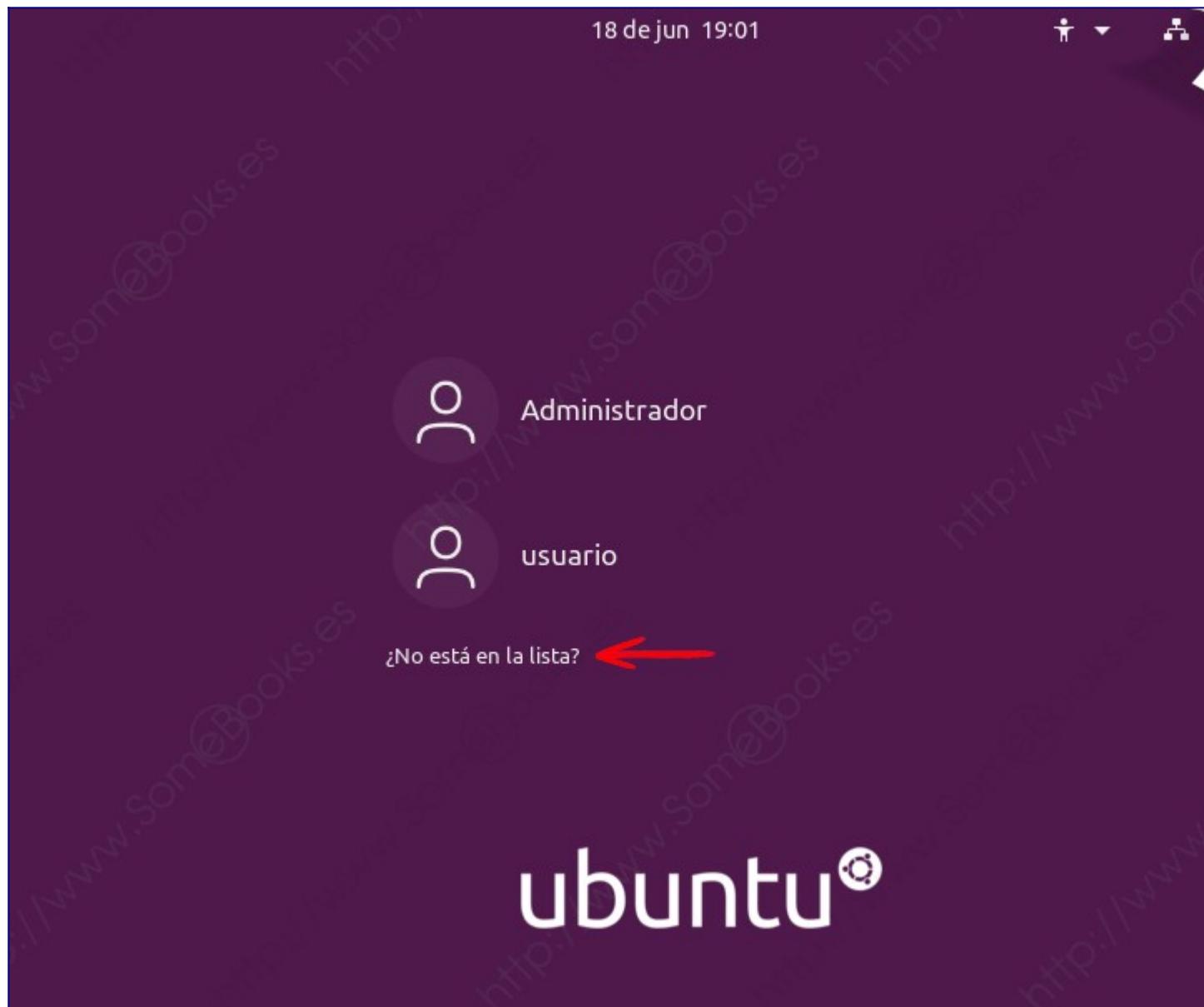


Iniciar sesión con cualquier cuenta del dominio

Como cabe esperar, a partir de este momento, podremos repetir los pasos anteriores para iniciar sesión en el equipo cliente con cualquier cuenta de usuario que se encuentre definida en *Windows Server*, sin necesidad de que exista de forma local en el cliente *Ubuntu*.

Solo habrá que hacer clic, de nuevo, sobre *¿No está en la lista?*.

18 de jun 19:01



... Y escribir el nombre de la cuenta que vayamos a usar.



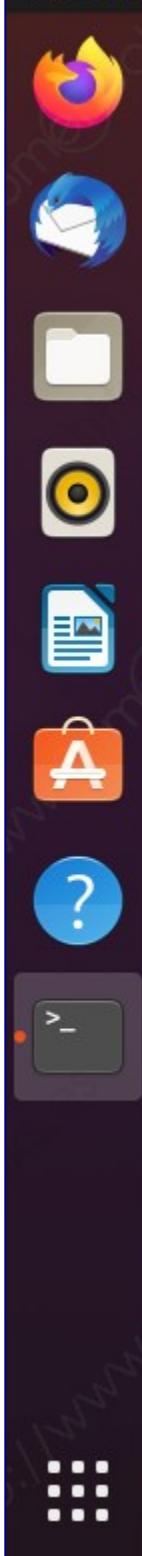
Una vez escrita la contraseña, podremos volver a comprobar, en el área de notificación del sistema, que hemos iniciado sesión con la cuenta adecuada.

Comprobamos el nombre de la cuenta.

Actividades

Terminal ▾

18 de jun 19:00



marius@somebooks

marius@somebooks-desk:~\$

Y con esto podemos dar por concluida la tarea. Espero que te haya resultado útil.