

Crear y utilizar volúmenes LUKS cifrados

Cifrado de disco en Ubuntu

La **seguridad** es un aspecto que merece atención, incluso en Linux.

Es **muy recomendable que los usuarios de ordenadores y portátiles den un paso más y cifren el disco**. Y es que en caso contrario, ante la pérdida o robo del equipo, toda la información que contenga estaría al alcance de cualquiera.

En resumen, si en tu equipo guardas documentos, fotos personales, documentación de clientes...

Cifrado de disco en Ubuntu.

Cifrar el disco equivale a **proteger los datos almacenados con una contraseña** y cuanto más «fuerte» sea ésta, más difícil será romper el cifrado.

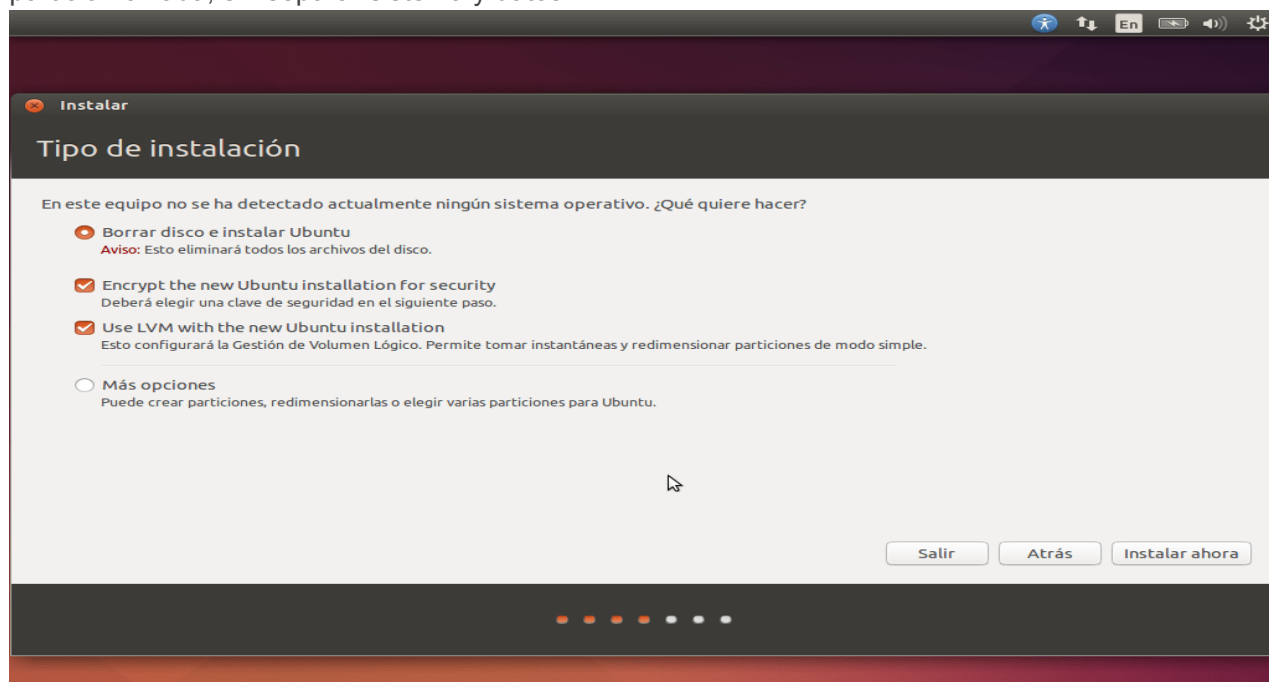
Cifrar el disco tiene la única pero importante ventaja de disfrutar de una mayor seguridad, pero también tiene alguna «contraindicación»:

- Afecta al rendimiento del equipo, aunque en la experiencia de usuario es imperceptible.
- La configuración postinstalación se complica en unidades SSD.
- Si se pierde la contraseña, se pierde el acceso y los datos.

Retomamos la **instalación de Ubuntu** en el punto del particionado, momento en el que se puede efectuar el cifrado de la instalación al completo o el cifrado de particiones.

1. Cifrado de instalación

Este es el método más sencillo y directo, pero **no es el recomendado**, ya que creará una única partición cifrada, sin separar sistema y datos.



- Al seleccionar «Cifrar la nueva instalación de Ubuntu» se seleccionará automáticamente la siguiente opción, «LVM» o el **administrador de volúmenes lógicos**.
- Para un cifrado más eficiente hay que elegir “Más opciones”.

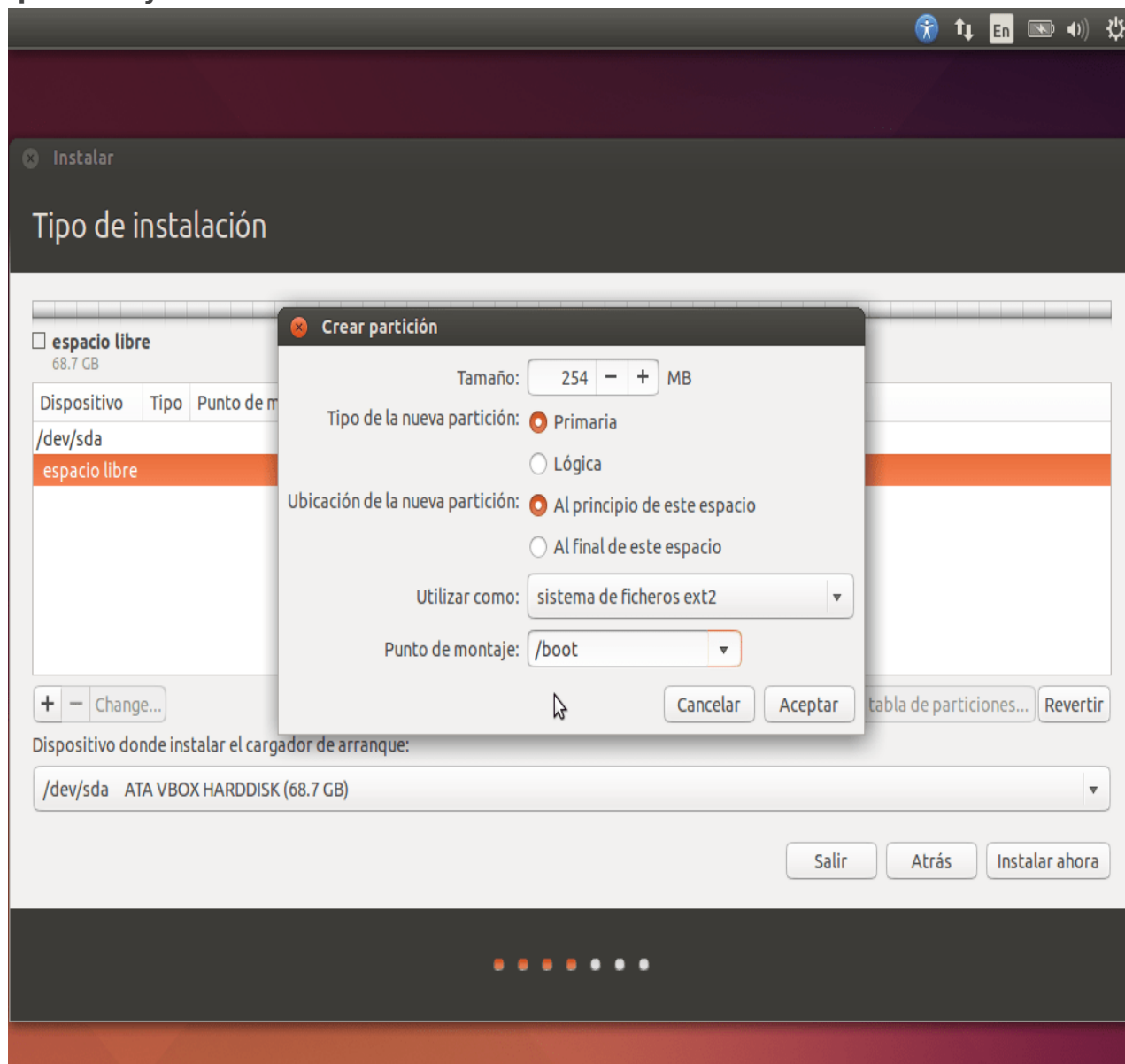
.....

2. Cifrado de particiones

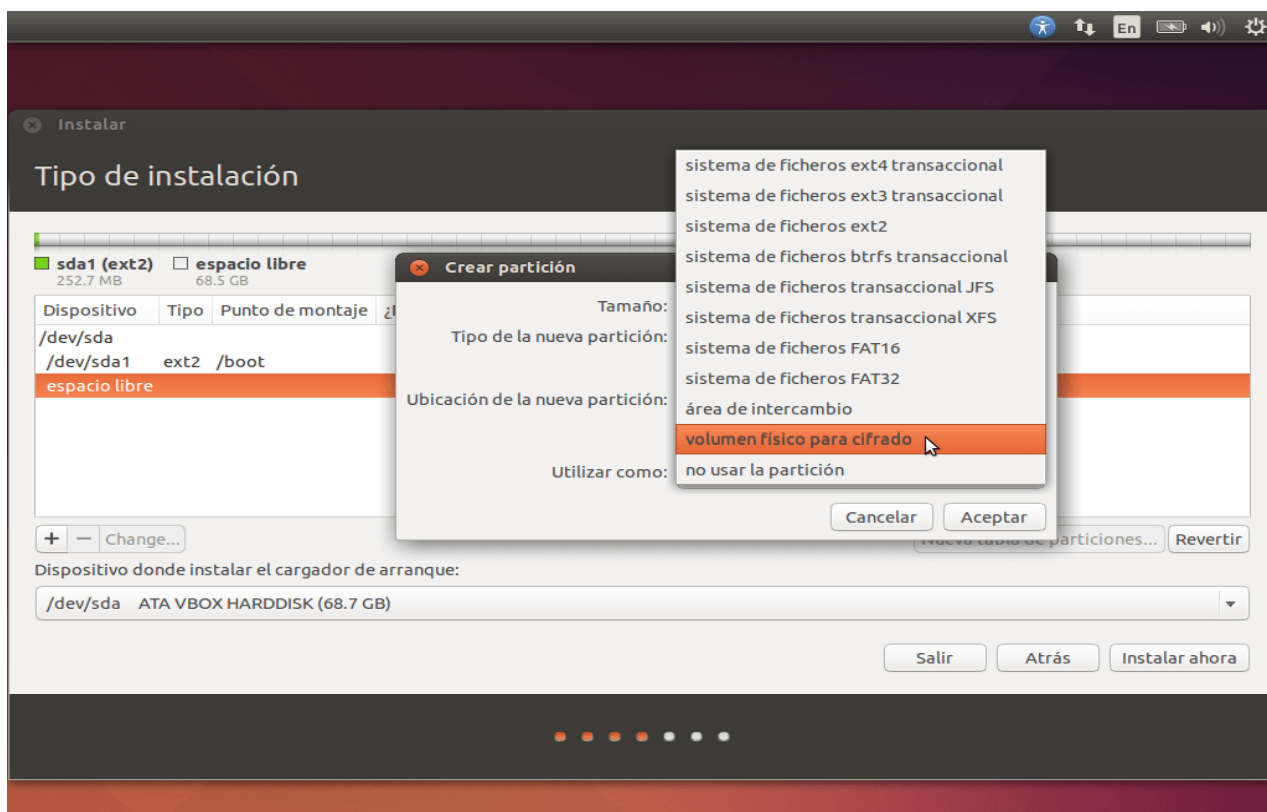
Este es el método más complejo por el planteamiento a considerar y los pasos a seguir, pero **es el recomendado** por ofrecer mayor control y menor incidencia en el rendimiento. La principal consideración es: ¿hay que cifrar todas las particiones, o basta con cifrar solo la partición de datos? Todo dependerá del nivel de seguridad que se busque.

Por ejemplo, si solo se cifra la partición de datos («/home») el instalador puede arrojar un error, ya que a través del área de intercambio («swap») se podría extraer información sensible e incluso recuperar partes de la clave de cifrado o la frase de contraseña. Asimismo, en la partición raíz («/») hay directorios que son susceptibles de albergar información confidencial.

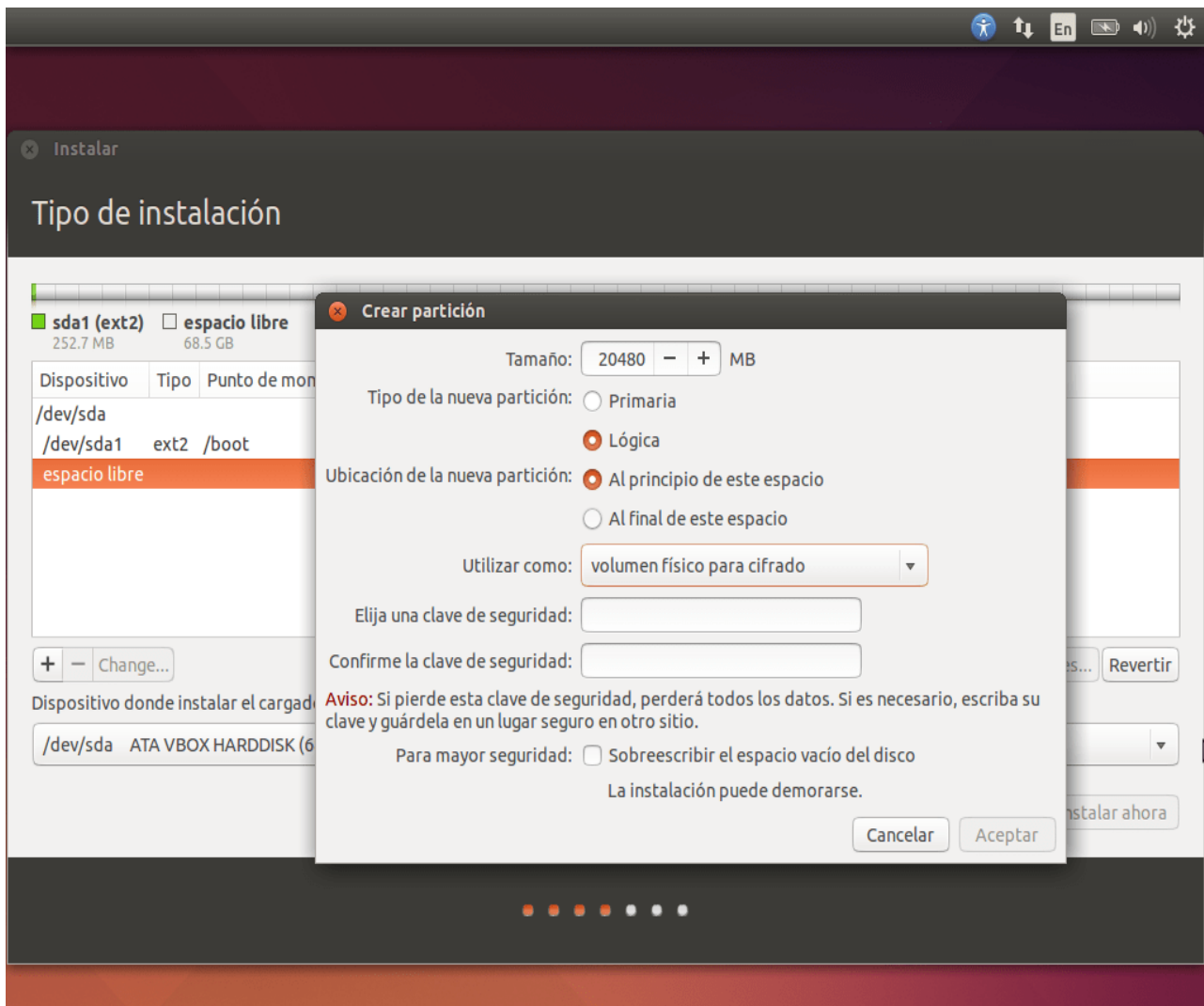
En cada arranque del sistema **habrá que introducir una contraseña por cada partición que se haya cifrado**.



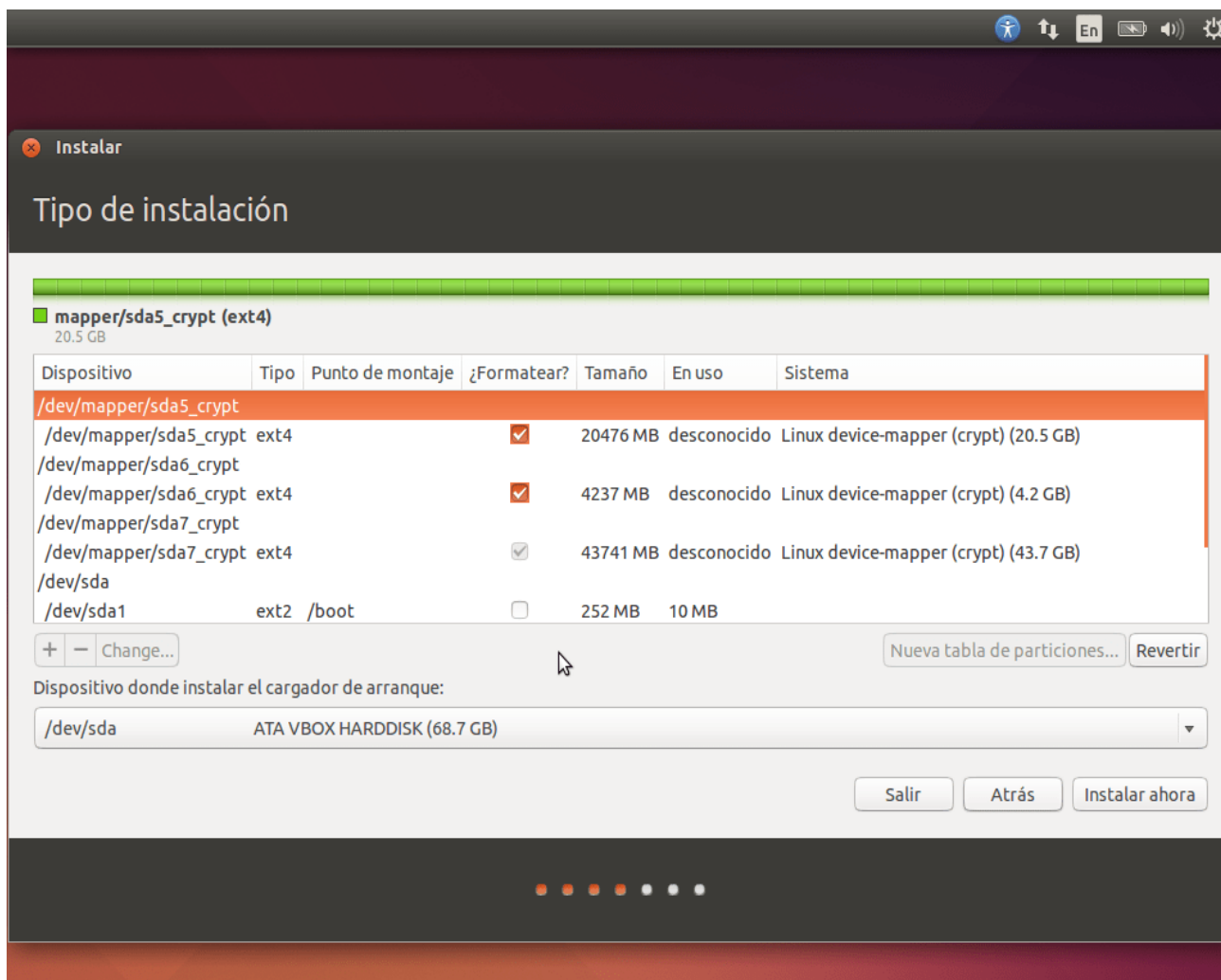
- Si se desea cifrar la partición del sistema («/»), es **imprescindible crear primero una partición para el arranque**, tal y como se muestra en la imagen.



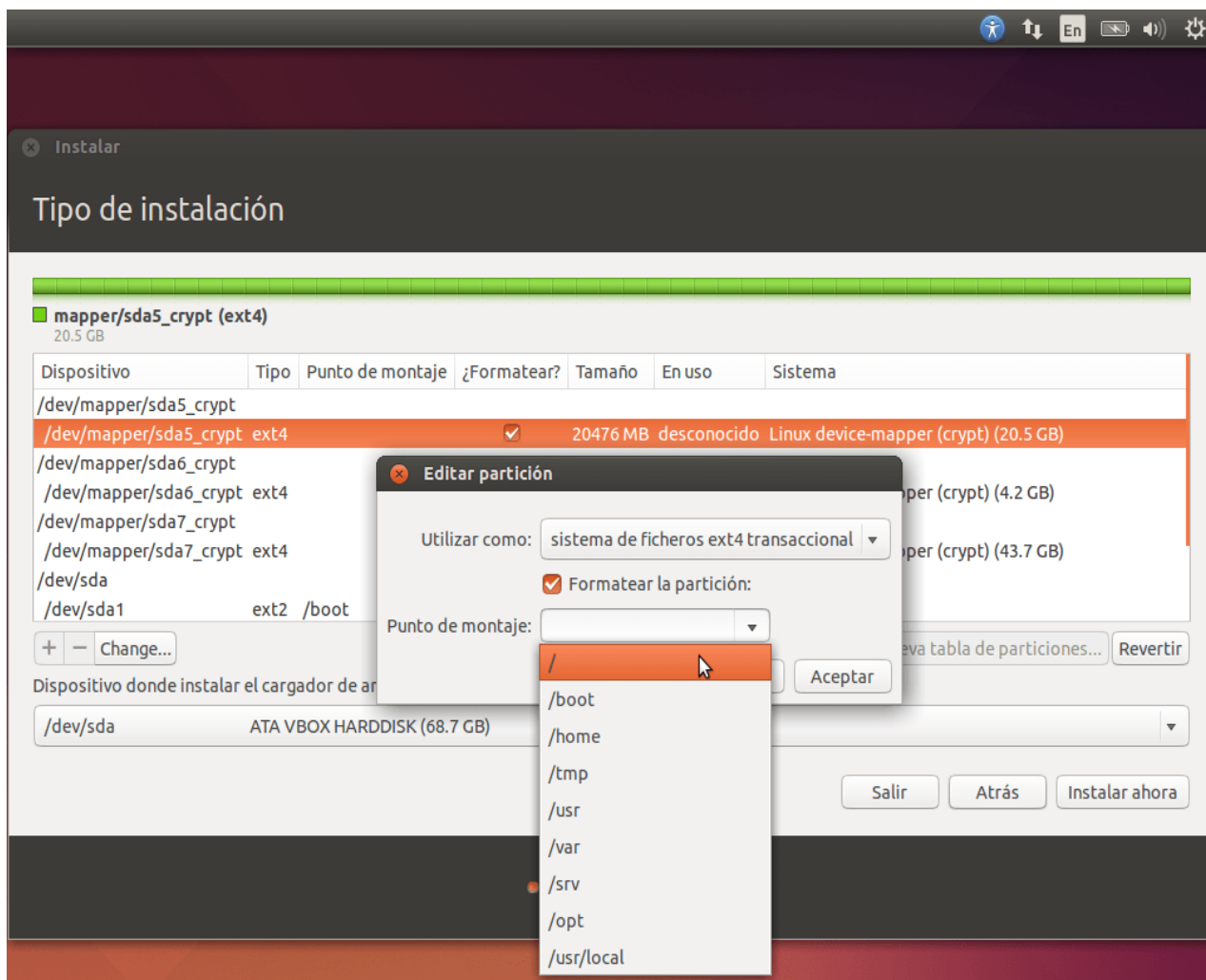
- El primer paso al crear una partición cifrada es **asignar el tamaño** y en «Utilizar como» elegir «volumen físico para cifrado». Lo mismo para la partición del sistema, la de datos y el área de intercambio.



- Al seleccionar utilizar como volumen físico para cifrado habrá que **introducir una contraseña** para completar la acción.



- Al terminar la creación de particiones cifradas se mostrará en la lista principal una **nueva serie de dispositivos** que, efectivamente, se corresponden con las particiones cifradas.

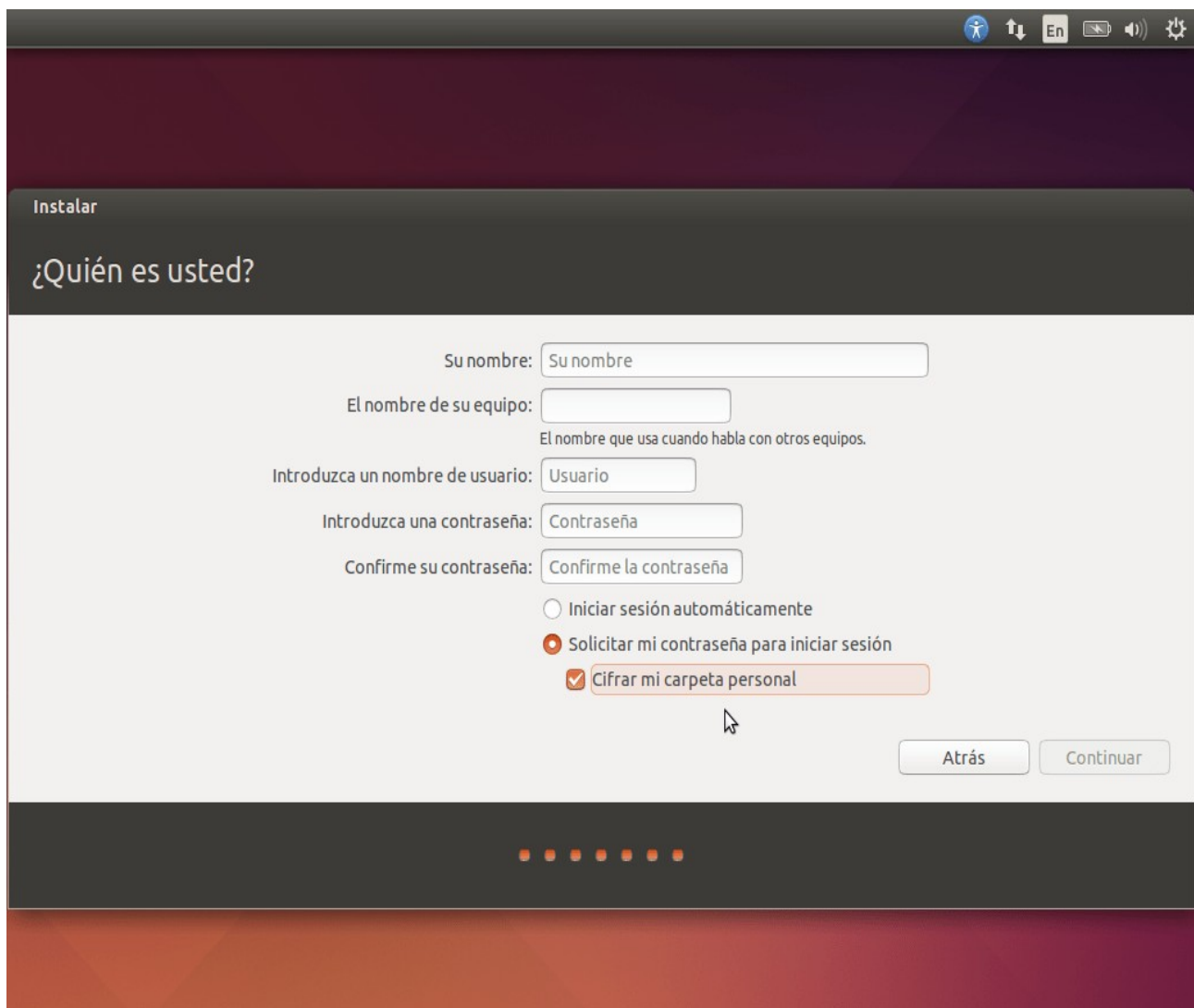


- El último paso consistirá en **asignar un punto de montaje** para la partición de sistema («/») y datos («/home») y seleccionar el **área de intercambio**, todo en los dispositivos señalados como «/dev/mapper/».

.....

3. Cifrado del directorio personal

Ubuntu ofrece un método de cifrado más sencillo que el de instalación y que contempla solo la carpeta personal del usuario, de manera que todos los archivos y configuraciones que haya en el directorio «/home/usuario» se cifren con la **contraseña de inicio de sesión**.

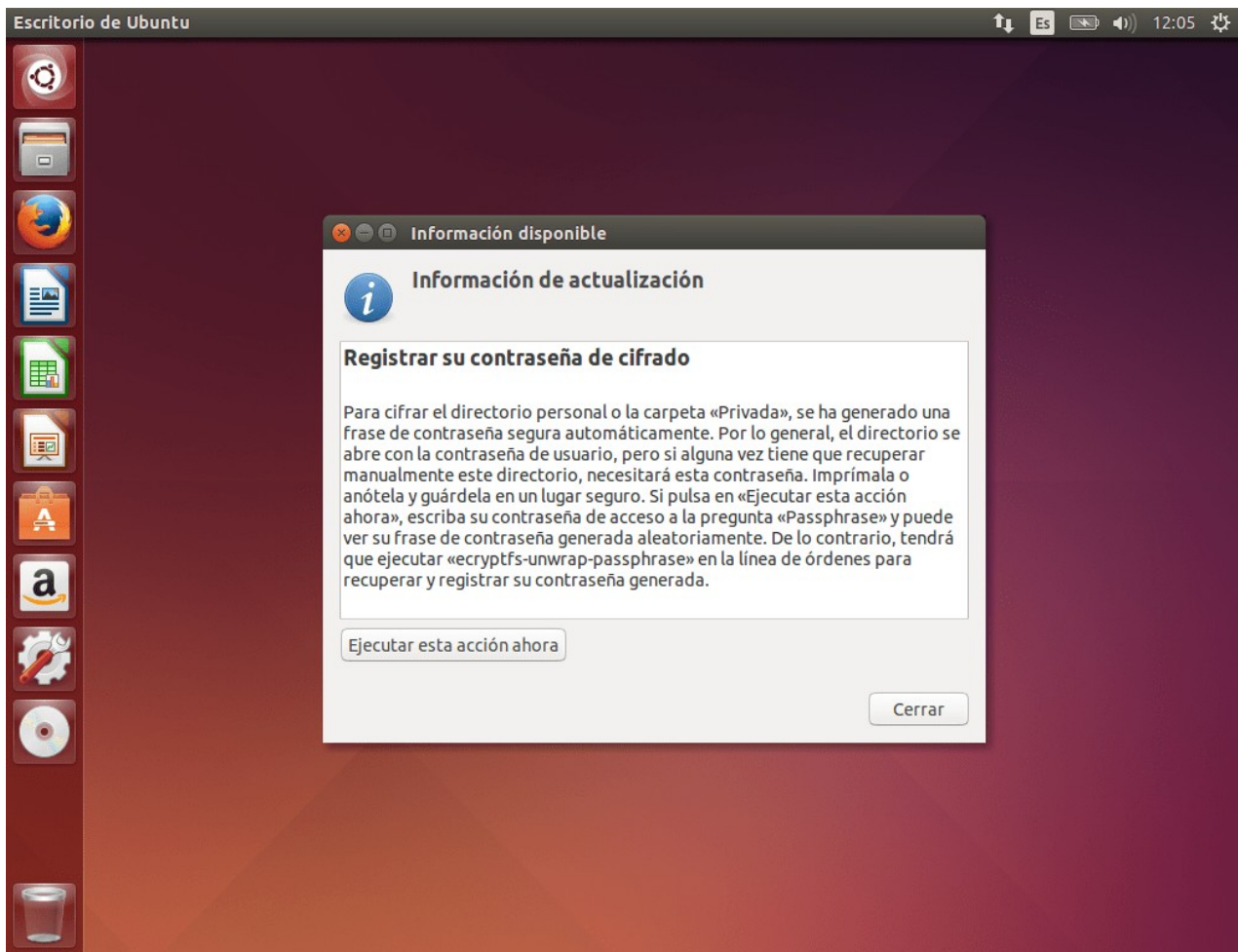


The image shows a screenshot of the Ubuntu installer window titled "¿Quién es usted?". The window has a dark header bar with the word "Instalar" on the left and system icons on the right. The main content area is light gray and contains the following fields and options:

- Su nombre:** A text input field with the placeholder "Su nombre".
- El nombre de su equipo:** A text input field with the placeholder "El nombre que usa cuando habla con otros equipos."
- Introduzca un nombre de usuario:** A text input field with the placeholder "Usuario".
- Introduzca una contraseña:** A text input field with the placeholder "Contraseña".
- Confirme su contraseña:** A text input field with the placeholder "Confirme la contraseña".
- ☐ Iniciar sesión automáticamente
- ☒ Solicitar mi contraseña para iniciar sesión
- ☒ Cifrar mi carpeta personal

At the bottom right of the form are two buttons: "Atrás" and "Continuar". Below the form, there is a progress bar consisting of seven dots, with the last dot being orange, indicating the current step. The window has a dark footer bar with a red and orange geometric pattern.

- Cifrar el directorio personal es la última opción a elegir en la instalación del sistema, en el apartado de creación de usuario.



- Al finalizar la instalación e iniciar sesión por primera vez, una de las acciones a completar será la de guardar la clave de cifrado.

Proteger por Contraseña y Cifrar Pendrive o Disco Duro

Hay muchas formas de **cifrar** o **proteger** con una contraseña un pendrive pero lo más eficiente es cifrar toda la partición ya que simplemente asignar una contraseña es bastante inseguro y fácil de saltar.

Al cifrar necesitaremos una contraseña para poder descifrar y acceder al contenido de nuestro pendrive dejando este bastante seguro.

Desde hace bastante tiempo disponemos de una herramienta para linux utilizando librerías GTK con la que podemos realizar las dos cosas a la vez y disponer de un cómodo acceso desde nuestro navegador de archivos favorito en vez de tener que estar abriendo un programa específicamente para este fin.

También es posible Gestionar directamente el cifrado desde una terminal aprovechando luks y dm-crypt

Para aclarar, este proceso tal como lo voy a explicar va dirigido a usarse en sistemas Linux.

Información General

- **Cryptsetup** es la utilidad con la que podemos cifrar una partición (ya sea de nuestro pendrive como un HDD) y utiliza volúmenes LUKS, loop-AES y formato compatible con **TrueCrypt**.
- **LUKS** es el estándar para **cifrado** de disco duro en Linux que proporciona compatibilidad entre sistemas operativos, seguridad en contraseñas multiusuarios y almacena la configuración necesaria en la cabecera de la partición pudiendo de esta forma transportar o migrar los datos sin tener problemas. Lo mejor de todo es que es open source.

Cifrar desde terminal

Al cifrar desde terminal no necesitamos en ningún momento de componente gráfico, es decir, podremos acceder al dispositivo cifrado mediante comandos en cualquier equipo **GNU/LINUX** incluso servidores que normalmente no disponen de interfaz para aprovechar todos los recursos hardware posible.

Requisitos

Tendremos que instalar solamente “cryptsetup”

```
sudo apt-get install cryptsetup cryptmount
```

Asegurar dispositivo

Podemos asegurar que no los datos del dispositivo son completamente borrados (para que nadie pueda recuperarlos) escribiendo de forma aleatoria todo el dispositivo de almacenamiento.

Tengan en cuenta que esto borrará el contenido del dispositivo.

Podemos identificar el dispositivo con el comando **fdisk** de esta forma:

```
sudo fdisk -l
```

Y cuando tengamos claro el objetivo, en mi caso pondré los ejemplos con “/dev/sdc1”, procederemos a sobrescribirlo:

```
sudo dd if=/dev/urandom of=/dev/sdc1 bs=1M
```

Con esto quedará totalmente destrozado lo que hubiese sido borrado anteriormente, nos garantiza seguridad en caso de pérdida o robo.

Formatear con LUKS

Ahora vamos a formatear la partición con un sistema de cifrado LUKS en una orden muy sencilla:

```
sudo cryptsetup luksFormat /dev/sdc1
```

Nos pedirá una contraseña, la introducimos y deberemos recordarla ya que en caso de olvidarla nuestros datos serán irrecuperables por completo.

Abrir dispositivo

Antes de poder usar un dispositivo **cifrado** debemos abrirlo, esto es introducir la clave y prepararlo para usar.

Al abrirlo indicamos que lo queremos abrir con luks, el dispositivo físico y por último el nombre que tendrá para identificarlo. En este caso lo llamaré “USB-LUKS”

Para abrir un dispositivo cifrado desde terminal podremos usar el siguiente comando adecuando a nuestro dispositivo:

```
cryptsetup luksOpen /dev/sdc1 USB-LUKS
```

Una vez introducido este comando se nos habrá creado un nuevo dispositivo nombrado **/dev/mapper/USB-LUKS**, el cual realmente será nuestro dispositivo externo abierto y renombrado de una forma amigable

Formatear

El formato también queda a nuestra elección.

Mi objetivo será usarlo solo en sistemas linux, por ello es más eficiente que lo use con un sistema de archivos ext4 pero si lo quieres usar también en windows podéis hacerlo en **fat**.

Para formatearlo lo haremos con el comando:

```
sudo mkfs.ext4 /dev/mapper/USB-LUKS
```

Para otro tipo de formatos consultad la herramienta mkfs (man mkfs)

Montar dispositivo

Para montar el dispositivo cifrado con LUKS usaremos el comando mount como si fuese una partición normal:

```
mount /dev/mapper/USB-LUKS /mnt/
```

Desmontar dispositivo

Para desmontar el dispositivo cifrado con LUKS usaremos umount como para una partición de almacenamiento normal:

```
umount /mnt/
```

Cerrar dispositivo cifrado

Cuando terminamos de usar un dispositivo es recomendable cerrarlo, esto es desmontarlo como unidad y que vuelva a pedir el cifrado para volver a usarse. Para poder cerrarlo es necesario que esté desmontado primero

```
cryptsetup luksClose USB-LUKS
```

Cifrar desde Utilidad de Discos (forma gráfica)

La herramienta en cuestión se llama “Utilidad de Discos de Gnome” y con ella junto unos paquetes que nos proporcionarán la capacidad de cifrado tendremos todo lo que necesitamos.

Aunque sea para gnome es posible instalarlo en cualquier entorno gráfico, eso si, requerirá ciertas dependencias para poder hacerlo, sobre todo librerías (no son demasiadas ni ocupan mucho) pero esta forma te puede dar mucha más seguridad frente a la opción de terminal.

Requisitos

Tendremos que instalar “cryptsetup” y “Utilidades de Disco” en sistemas derivados de debian sería así:

```
sudo apt-get install cryptsetup cryptmount gnome-disk-utility
```

Formatear con sistema de archivos LUKS cifrado

Ahora abrimos “Utilidad de Discos” también puede aparecer en el menú como “Disks” o “Discos”

Podemos abrirlo incluso desde terminal:

```
sudo gnome-disks
```

Una vez dentro de la “Utilidad de Discos” pulsamos sobre Formatear volumen (Todo será borrado, procura respaldar los datos existentes)

Debemos asegurarnos de marcar “Cifrar el dispositivo subyacente” ya que esto hará que la partición esté cifrada y necesite una clave para acceder a los datos.

Introducimos el nombre que tendrá como etiqueta nuestro pendrive y marcamos el tipo de partición correspondiente (normalmente FAT) pero podemos usar perfectamente ext4, además si el objetivo es solo usarlo bajo linux recomendaría usar ext4.

Pulsamos sobre “Formato” y comenzará el formateo y cifrado.

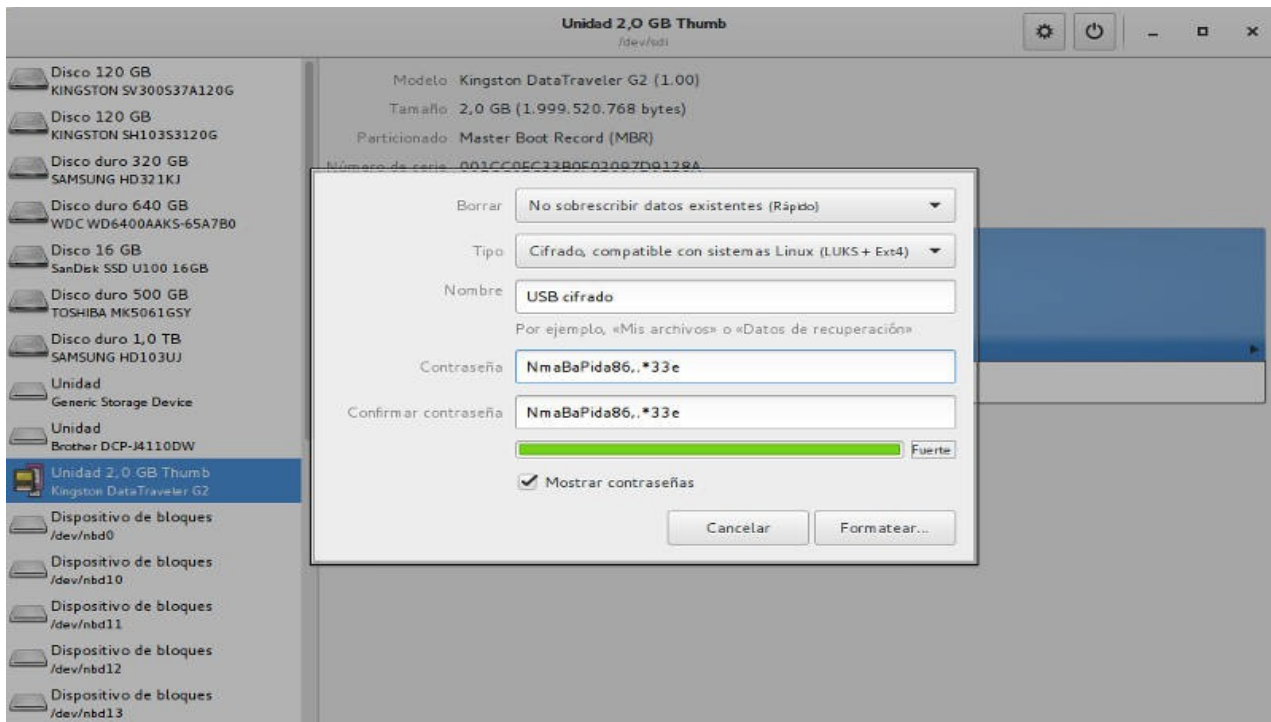
Comprobar que solicita contraseña para acceder

Nos aseguramos que es el pendrive correcto y la partición correcta antes de aplicar los cambios definitivamente.

Introducimos la clave que servirá para acceder a los datos de la partición cifrada.

Ahora podemos ver que en la partición aparece que está cifrada y nos lo representa con un candado.

Para comprobar que funciona añadimos algunos directorios o documentos, desmontamos el pendrive y lo volvemos a montar.



Quitar cifrado y contraseña

- 1.Extraemos el pendrive, lo desconectamos físicamente y volvemos a enchufar a nuestro ordenador.
- 2.Entramos de nuevo a “Utilidad de Discos”
- 3.Ahora le damos a “Formatear unidad”
- 4.Cuando termina pulsamos en “Crear partición”

Cambiar la contraseña de cifrado

- 1.Para cambiar la contraseña basta con entrar en “Utilidad de Discos”
- 2.En la parte inferior izquierda pulsar sobre “Cambiar contraseña”
- 3.Nos pedirá introducir la contraseña actual y la nueva contraseña.