

# TRABAJO 2: CIFRADO DE LA INFORMACIÓN

LUIS ALBERTO ÁLVAREZ ZAVALETA

## Contenido

Introducción .....	2
Aplicaciones de cifrado de ficheros en Linux. ....	3
Tomb.....	3
Cryptmount .....	3
GnuPG .....	3
CryFS.....	4
VeraCrypt.....	4
Crear una clave PGP y compartirla en un servidor público de claves PGP. ....	5
Instalación de un sistema Linux sobre una partición cifrada con LUKS.....	7
Conclusión .....	10

## Introducción

Este trabajo consistirá en el análisis de las aplicaciones de cifrado que se encuentran disponibles en Linux. Se hablará un poco sobre las que se han encontrado y sobre su funcionamiento.

A continuación, crearemos una clave PGP y la publicaremos en un servidor público de claves. Por último, realizaremos la instalación de un sistema Linux, en concreto Debian sobre una partición cifrada mediante LUKS

## Aplicaciones de cifrado de ficheros en Linux.

A continuación, se describirán algunas de las aplicaciones de cifrado que he encontrado

### Tomb

Tomb se presenta como una solución que busca elevar los estándares de seguridad a través de la adopción y la aplicación de buenas prácticas en el almacenamiento de claves.

Este permite crear “tumbas”, un espacio de memoria cifrado para los cuales se debe crear una llave y “sellar” la tumba con la clave nueva que se ha creado, esta llave se necesitará usar de nuevo para poder abrir la tumba y poder modificar sus contenidos.

```
luis@luis-VirtualBox:~/Eael$ sudo tomb dig -s 30 tumba.tomb
tomb . Commanded to dig tomb
tomb (*) Creating a new tomb in tumba.tomb
tomb . Generating tumba.tomb of 30MiB
30+0 registros leídos
30+0 registros escritos
31457280 bytes (31 MB, 30 MiB) copied, 0,403043 s, 78,0 MB/s
-rw----- 1 luis luis 30M nov 24 13:32 tumba.tomb
tomb (*) Done digging tumba.tomb
tomb . Your tomb is not yet ready, you need to forge a key and lock it:
tomb . tomb forge tumba.tomb.key
tomb . tomb lock tumba.tomb -k tumba.tomb.key
```

*Ilustración 1. Creación de una tumba*

### Cryptmount

Cryptmount, diseñado específicamente para sistemas operativos GNU/Linux, permite a los usuarios montar archivos cifrados sin necesidad de privilegios de root. Utiliza el mecanismo devmapper más reciente, ofreciendo ventajas con funcionalidad mejorada en el kernel, soporte para particiones de intercambio cifradas para superusuarios y la capacidad de almacenar múltiples sistemas de archivos encriptados en un solo disco

```
luis@luis-VirtualBox:~/cryptmount$ sudo cryptmount-setup
-----
cryptmount setup script

This program will allow you to setup a secure filing-system that will
be managed by "cryptmount". You will be able to select basic features
such as the location and size of the filesystem - if you want more
advanced features, you should consult the cryptmount manual page.

cryptmount version 5.3.3, (C)Copyright 2007-2021 RW Penney
cryptmount comes with ABSOLUTELY NO WARRANTY.
This is free software, and you are welcome to redistribute it under
certain conditions - see the file 'COPYING' in the source directory.
-----

Each cryptmount filesystem is identified by a short name which is used
when mounting or configuring that filesystem. This name should be a
single word (without spaces), such as "opaque".
The following target names have already been used:      (NONE)

Please enter a target name for your filesystem
[opaque]: luis

Your new encrypted filesystem is now ready for use - to access, try:
  cryptmount luis
  cd /home/luis/crypt
After you have finished using the filesystem, try:
  cd
  cryptmount --unmount luis

Please take great care NOT to delete or damage your keyfile
("/etc/cryptmount/luis.key"). Without that file, and the associated
password, it will be virtually impossible to access your encrypted
filesystem. You may want to keep a separate backup copy of the
keyfile.
```

*Ilustración 2. Crear una partición con Cryptmount*

### GnuPG

GnuPG, una colección de herramientas criptográficas se presenta como un reemplazo del paquete de software criptográfico PGP de Symantec. Cumple con la especificación de

seguimiento de estándares IETF de OpenPGP y RFC 4889. GnuPG se posiciona como una opción confiable para usuarios que buscan herramientas de cifrado/descifrado en entornos Linux.

```
luis@luis-VirtualBox:~/gpg$ echo "hola que tal"> texto.txt
luis@luis-VirtualBox:~/gpg$ gpg -c texto.txt
luis@luis-VirtualBox:~/gpg$ ls
texto.txt  texto.txt.gpg
luis@luis-VirtualBox:~/gpg$ gpg -d texto.txt.gpg
gpg: datos cifrados AES256.CFB
gpg: cifrado con 1 frase contraseña
hola que tal
luis@luis-VirtualBox:~/gpg$
```

*Ilustración 3. Cifrar un archivo*

## CryFS

CryFS se presenta como una herramienta de cifrado gratuita y de código abierto diseñada para almacenar archivos de forma segura en la nube.

Destaca por su facilidad de configuración, ejecución en segundo plano y compatibilidad con diversos servicios en la nube, incluyendo Dropbox, OneDrive o iCloud.

CryFS permite que ningún dato, incluyendo la estructura del directorio, los metadatos y el contenido de los archivos, dejen la computadora en un formato sin cifrar, proporcionando así una capa adicional de seguridad para la información subida a la nube.

## VeraCrypt

VeraCrypt una herramienta gratuita y de código abierto, se destaca por proporcionar a los usuarios cifrado sobre la marcha.

Ofrece la posibilidad de cifrar dispositivos de almacenamiento extraíbles como tarjetas SD, incluso discos duros, USB o particiones seleccionadas mediante autenticación previa al arranque. Además, incluyen la creación de discos virtuales cifrados y la capacidad de montarlos como unidades reales

Además, está disponible no solo para Linux, sino también para Windows y Mac, permitiendo su compatibilidad con una gran gama de plataformas. Por esta razón es utilizado por muchas organizaciones de seguridad, para garantizar que el software es seguro y confiable.

## Crear una clave PGP y compartirla en un servidor público de claves PGP.

Podemos crear una clave PGP usando el paquete GPG , se nos pedirá varias opciones que tendremos que rellenar para crear nuestro par de claves.

```
luis@luis-VirtualBox:~/gpg$ gpg --full-generate-key
gpg (GnuPG) 2.2.27; Copyright (C) 2021 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Por favor seleccione tipo de clave deseado:
(1) RSA y RSA (por defecto)
(2) DSA y ElGamal
(3) DSA (sólo firmar)
(4) RSA (sólo firmar)
(14) Existing key from card
Su elección: 1
Las claves RSA pueden tener entre 1024 y 4096 bits de longitud.
¿De qué tamaño quiere la clave? (3072) 3072
El tamaño requerido es de 3072 bits
Por favor, especifique el período de validez de la clave.
0 = la clave nunca caduca
<n> = la clave caduca en n días
<n>w = la clave caduca en n semanas
<n>m = la clave caduca en n meses
<n>y = la clave caduca en n años
¿Validez de la clave (0)? 1y
La clave caduca lun 02 dic 2024 22:20:16 CET
¿Es correcto? (s/n) s
```

*Ilustración 4. Generar llave gpg*

Podemos observar la lista de claves secretas creadas usando el siguiente comando.

```
luis@luis-VirtualBox:~/gpg$ gpg --list-secret-keys
gpg: comprobando base de datos de confianza
gpg: marginals needed: 3 completes needed: 1 trust model: pgp
gpg: nivel: 0 validez: 1 firmada: 0 confianza: 0-, 0q, 0n, 0m, 0f, 1u
gpg: siguiente comprobación de base de datos de confianza el: 2024-12-02
/home/luis/.gnupg/pubring.kbx
-----
sec   rsa3072 2023-12-03 [SC] [caduca: 2024-12-02]
      CB653ED87A7A4E989DA90B126BDF6CE25B924C4E
uid   [ absoluta ] Luis Alberto Alvarez Zavaleta (Clave creada para CIB) <albertoalvaza@gmail.com>
ssb   rsa3072 2023-12-03 [E] [caduca: 2024-12-02]
```

*Ilustración 5. Listado de claves*

Podemos exportar la clave pública a partir del su id

```
luis@luis-VirtualBox:~/gpg$ gpg --armor --export CB653ED87A7A4E989DA90B126BDF6CE25B924C4E
-----BEGIN PGP PUBLIC KEY BLOCK-----

mQGNBGVs8UgBDADWV10D4fPbNFU4yYQvaRSOsPAWwpwk19K07Uc9g7U9gFR7vnMq
APRyGXYJHutjaCqA1e51Llj+8wPuMtoFLIM2nSEPlFokKC5zjxq3FU6GNsgisYoo
9HtDX20b4gRT26u5Fyw4YdL1QqNYqyUiHPbwQa3nMMWwMKFcNhCD98YX5fK9J3aH
iKPDq00xH6P7pbn0qE92ExNyryWBS+9HvUyFLHssECXvhaKn1kjKHCGLXDfUwmx
yuW3Lm0bK8oTKAUcKTWvQlupWLINT3CS7qTtrSAJVXoKk+z+PrK204nT7mBH2wDM
8NXD32RJEX6SBdGpRgi6IgVU7VfKscwPaG0ShAPHqzFT2uJtiWowpuz14mVR2wH/
03iGrGtSL1lXJ3XPZEevh4WSJA+T7HRPrFHaGG+BUaG04J0GU1Ief7gCTp4mJEP0
UcXidM4fIXdxgL4tCIjzenl0K4nbU3a2zJqseX2Npi3Hk3fgG5iNhp7YtOtqDbuE
2qQuXeB7wnsJGwsAEQEAAARPTHVpcyBBbGJlcnRvIEFsdmFyZXQwWmF2YWxldGEg
```

*Ilustración 6. Clave pública generada*

Podemos copiar la clave para subirla a un servidor público de llaves, en este caso usaremos:

<https://keyserver.ubuntu.com/>

```
pub (4)rsa3072/cb653ed87a7a4e989da90b126bdf6ce25b924c4e 2023-12-03T21:21:12Z

uid Luis Alberto Alvarez Zavaleta (Clave creada para CIB) <albertoalvaza@gmail.com>
sig sig 6bdf6ce25b924c4e 2023-12-03T21:21:12Z 2024-12-02T21:21:12Z [selfsig]

sub (4)rsa3072/ffe7726d7f56b4ece0d926a45e7609438d386cfd 2023-12-03T21:21:12Z
sig sbind 6bdf6ce25b924c4e 2023-12-03T21:21:12Z 2024-12-02T21:21:12Z []
```

Podemos comprobar que la clave se encuentra disponible en el servidor

<https://keyserver.ubuntu.com/> usando tanto el correo electrónico

[albertoalvaza@gmail.com](mailto:albertoalvaza@gmail.com) , el nombre vinculado a la clave, Luis Alberto Alvarez

Zavaleta o el id de la clave **CB653ED87A7A4E989DA90B126BDF6CE25B924C4E**

# Instalación de un sistema Linux sobre una partición cifrada con LUKS

Para realizar la instalación usaremos el sistema operativo Debian ya que nos permite crear la partición cifrada como una de las opciones de instalación del sistema operativo

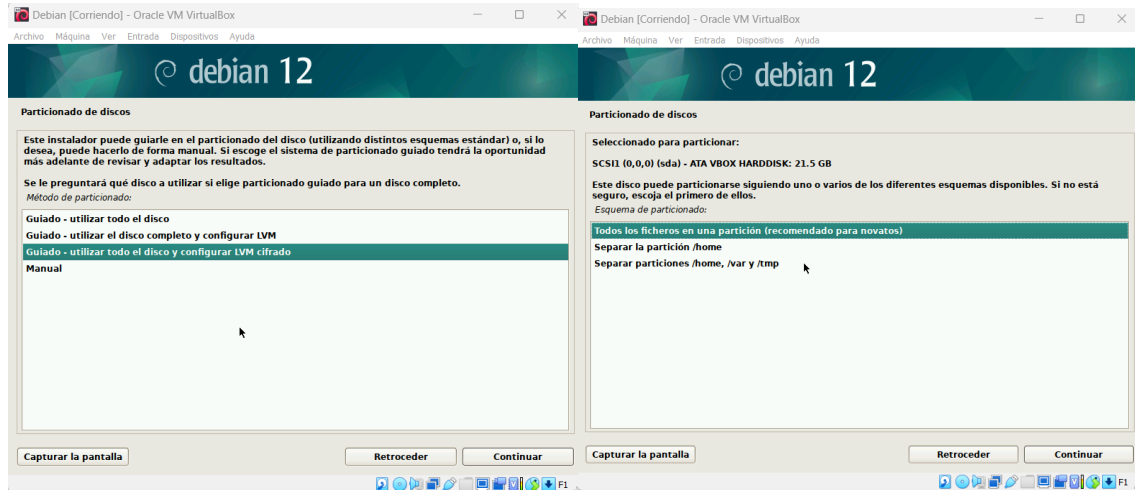


Ilustración 7. Crear partición de disco usando cifrado

Seleccionamos a guardar los cambios y configurar el LVM

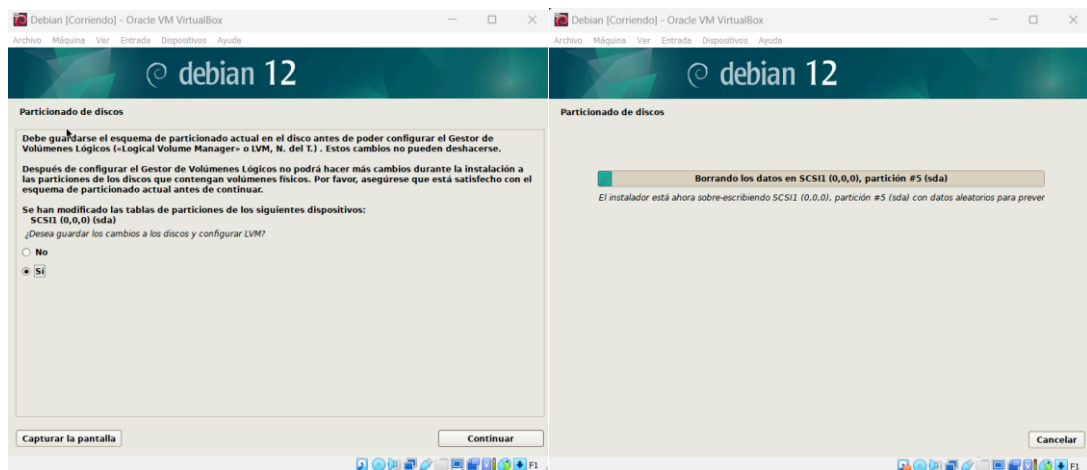


Ilustración 8. Cifrado usando LVM



A continuación nos pedirá una clave para cifrar la partición donde se instalará, su tamaño entre otras cosas.

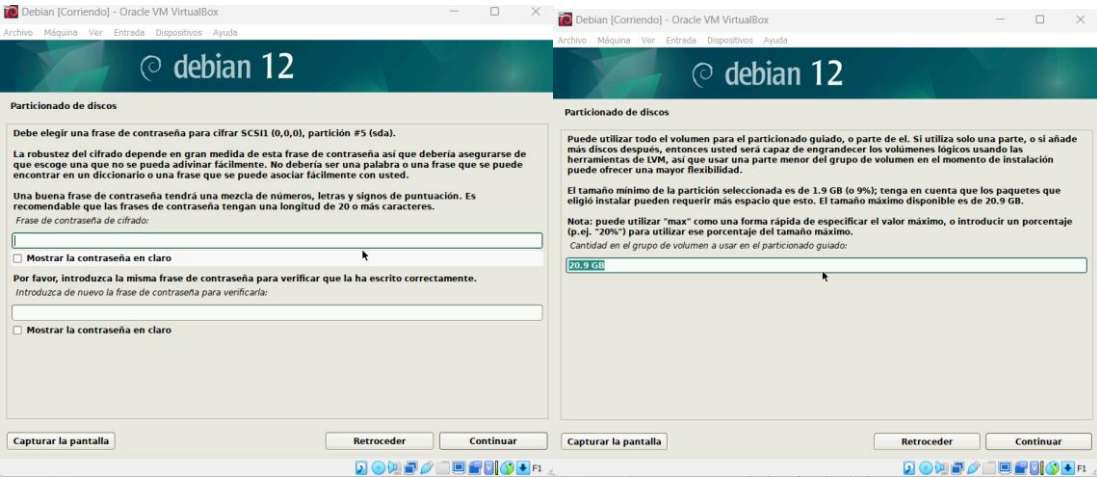


Ilustración 9. Contraseña de cifrado y tamaño de partición

Una vez terminado podemos observar como se terminará de cifrar y como quedarán las distintas particiones que hemos creado. Podemos ver que sda5 ha quedado cifrada.

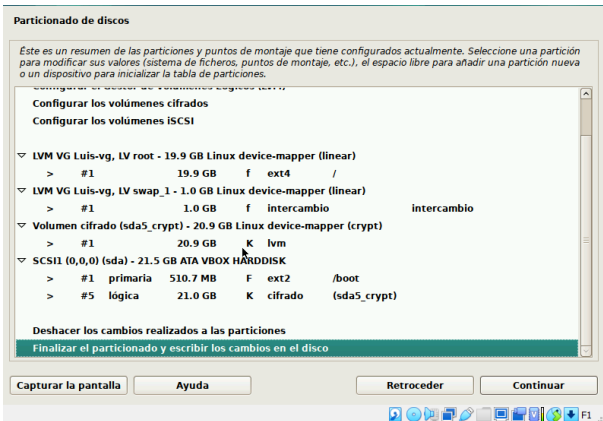


Ilustración 10. Estructura de particiones final

Una vez terminada la instalación tendremos el disco cifrado. Podemos observar que dado que la partición Linux se ha montado en el disco cifrado nos pide la contraseña para poder acceder a él y arrancar Linux.

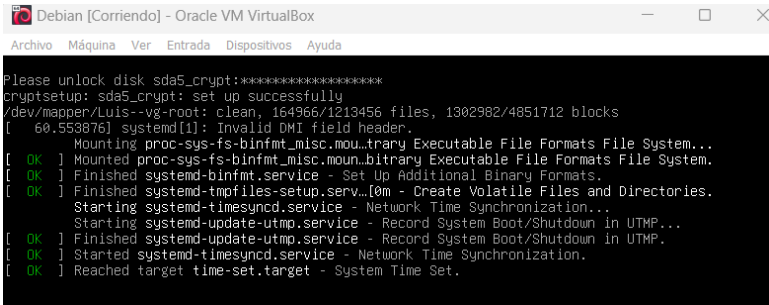


Ilustración 11. Clave para descryptar

Podemos observar la estructura de nuestros volúmenes usando la orden `lsblk -fs` y observar que el volumen sda5 que hemos creado este encriptado.

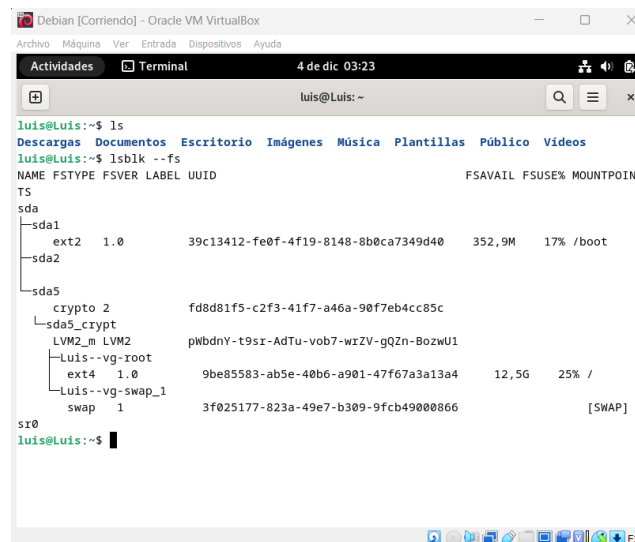


Ilustración 12. Estructura de particiones Linux

Además, podemos comprobar el algoritmo con el que se ha cifrado nuestra partición así como algunos detalles extra utilizando la función `lukDump` que viene en `cryptsetup` para analizar el volumen `sda5`.

```
luis@Luis:~$ sudo cryptsetup luksDump /dev/sda5
LUKS header information
Version:          2
Epoch:           3
Metadata area:    16384 [bytes]
Keyslots area:    16744448 [bytes]
UUID:             fd8d81f5-c2f3-41f7-a46a-90f7eb4cc85c
Label:            (no label)
Subsystem:        (no subsystem)
Flags:            (no flags)

Data segments:
  0: crypt
      offset: 16777216 [bytes]
      length: (whole device)
      cipher: aes-xts-plain64
      sector: 512 [bytes]

Keyslots:
  0: luks2
      Key:        512 bits
      Priority:    normal
      Cipher:     aes-xts-plain64
      Cipher key: 512 bits
      PBKDF:      argon2id

Cipher key: 512 bits
PBKDF:      argon2id
Time cost:  4
Memory:     716724
Threads:    2
Salt:       74 82 c5 cb 64 3a f2 37 15 bd 4a a4 64 ee b4 a6
            ab db 1d f2 d8 00 bd f3 e7 41 5d 18 fa aa af 91
AF stripes: 4000
AF hash:    sha256
Area offset: 32768 [bytes]
Area length: 258048 [bytes]
Digest ID:  0

Tokens:
Digests:
  0: pbkdf2
      Hash:      sha256
      Iterations: 105703
      Salt:       ac 95 47 c8 91 19 ec 9a 8b 37 92 d7 0f d6 14 9a
                  8d 8c a9 55 c4 a8 4b 64 32 ae 08 d0 b0 e2 b0 d5
      Digest:     9e 94 33 67 70 1b ce 71 4f 28 82 dc 62 ba 1e de
                  7a b2 6f b1 b8 96 c1 6d ce 39 c1 18 68 da a6 25
```

Ilustración 13. Estructura de sda5

## Conclusión

En este trabajo, se han explorado diversas aplicaciones de cifrado disponibles en el sistema operativo Linux, abordando sus funcionalidades y destacando algunas de sus características clave.

Este trabajo he conseguido tener una visión general sobre las herramientas de cifrado que existen en Linux, desde la creación de claves hasta la implementación de sistemas operativos con particiones cifradas. Estas medidas contribuyen significativamente a la protección de la información en un entorno digital cada vez más propenso a amenazas de seguridad.