LUKS

Linux Unified Key Setup

Instalando o Debian em disco criptografado com LUKS

Debian Day Brasil 2023

Thiago Andrade - 17 Ago 23

SUMÁRIO

SUMÁRIO

O QUE É LUKS (Linux Unified Key Setup)

- Especificação de criptografia de disco criada por Clemens Fruhwirth em 2004, originalmente destinada ao Kernel Linux.

- Implementada pelo módulo de Kernel dm-crypt.
- Administrada no Debian pelo conjunto de ferramentas do pacote cryptsetup

  # apt install cryptsetup

O QUE É LUKS (Linux Unified Key Setup)

- LUKS é o padrão para criptografia de disco do Linux. Ao fornecer um formato padronizado em disco, não só facilita a compatibilidade entre as distribuições, mas também permite o gerenciamento seguro de várias passphrase de usuário.
- O LUKS armazena todas as informações de configuração necessárias no cabeçalho da partição, que permite aos usuários transportar ou migrar dados sem problemas.

SUMÁRIO

POR QUE UTILIZAR LUKS?

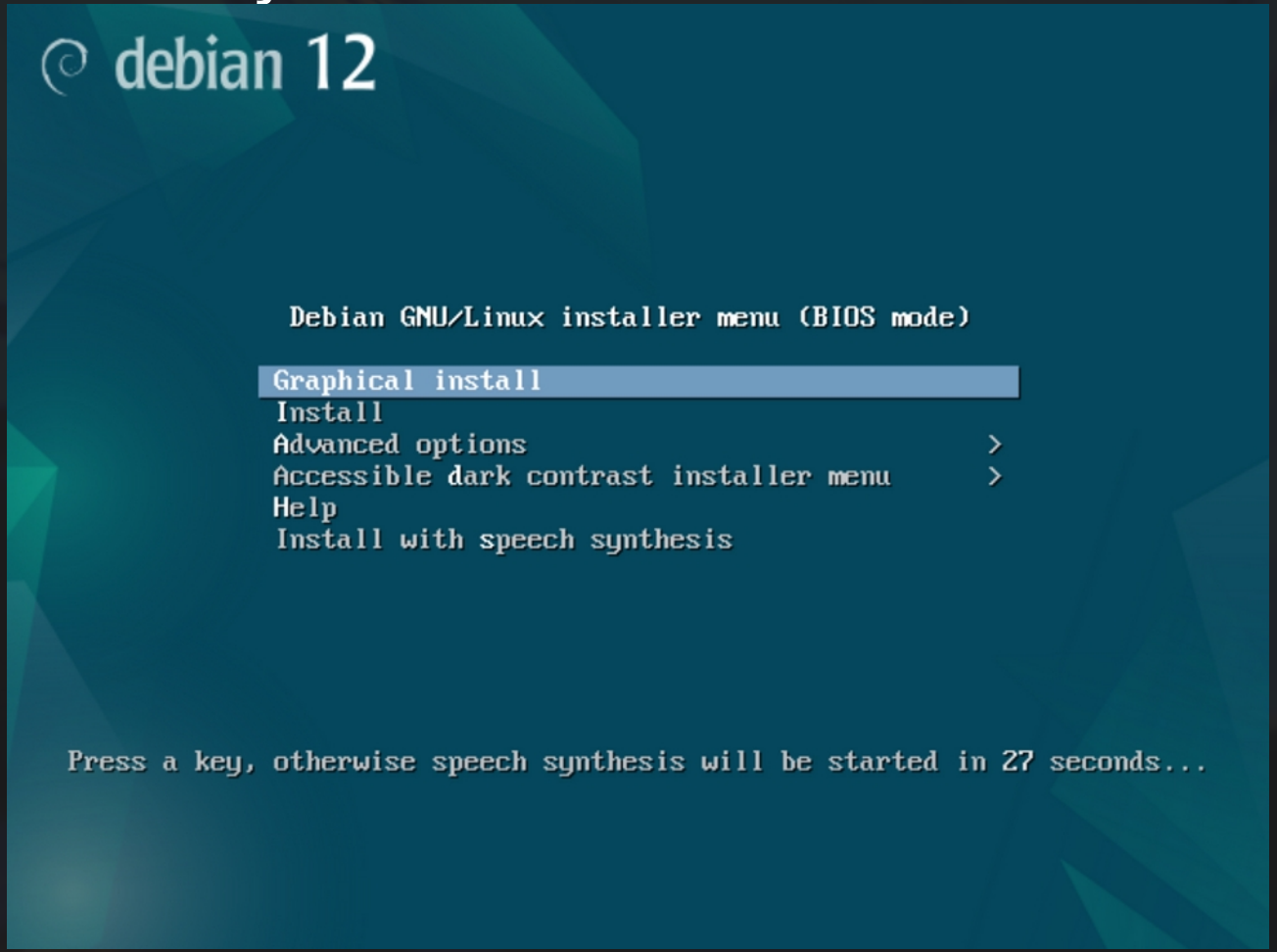
- Por ser software livre, estar empacotado no Debian e fazer parte do Instalador do Debian.
- Para dificultar que pessoas má intencionados leiam seus arquivos pessoais (casa / trabalho).
- Utiliza por padrão criptografia ‘forte’ aes-xts-plain64 com chave de 512 bits.
- Pode criptografar todo o disco, inclusive o swap, com exceção da partição que contêm o initrd (bootloader).

POR QUE UTILIZAR LUKS?

- Permite que os usuários incluam chaves ou passphrases de backup, o padrão LUKS2 suporta 32 slots de chave enquanto o LUKS1 suporta 8 slots.
- É compatível com LVM (Logical Volume Management) e RAID.
- É compatível com APPLE MACOS FILEVAULT2 e com WINDOWS BITLOCKER.

SUMÁRIO

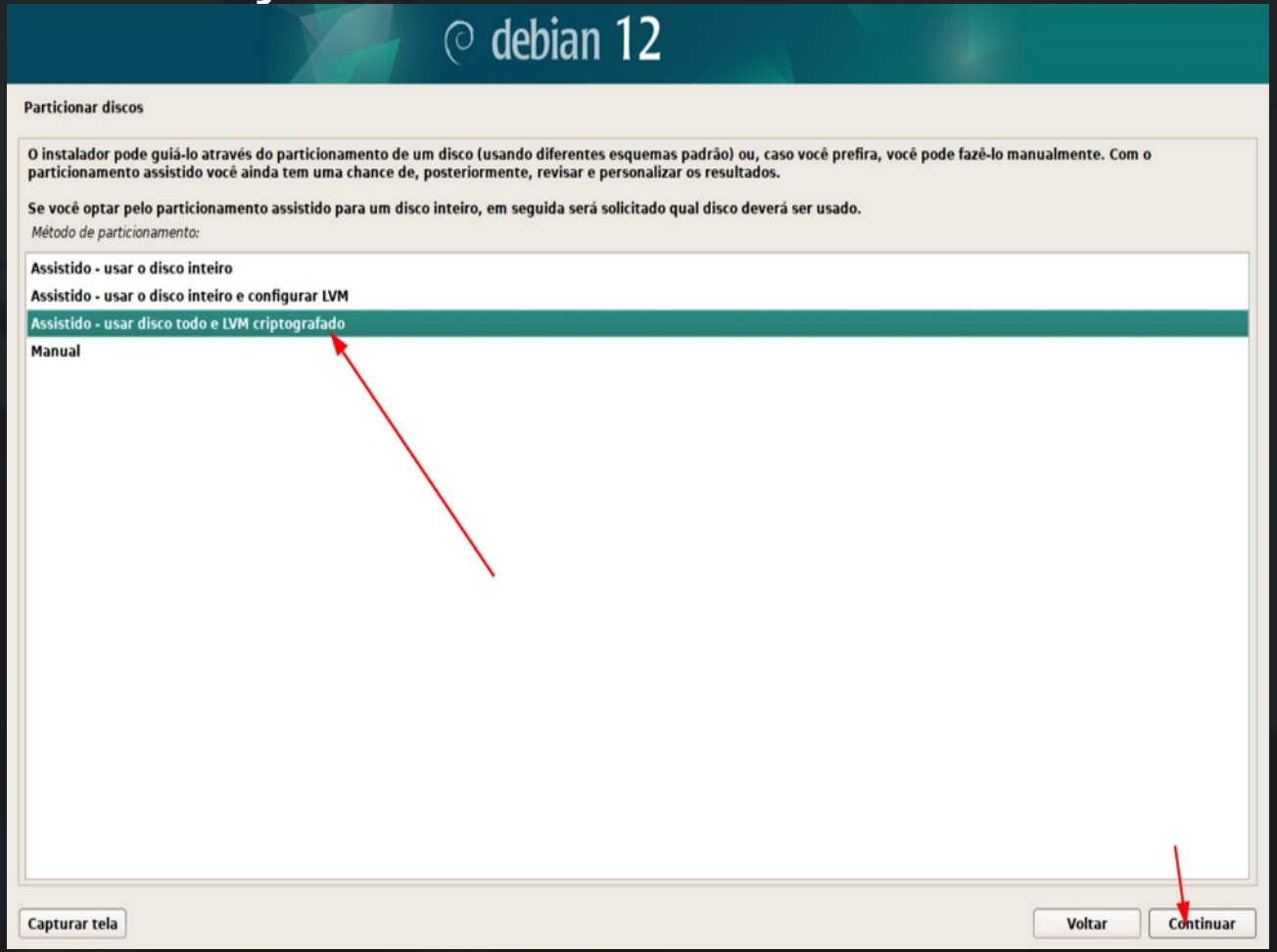
INSTALAÇÃO DO DEBIAN 12 COM LUKS



Debian Brasil

30 years debian

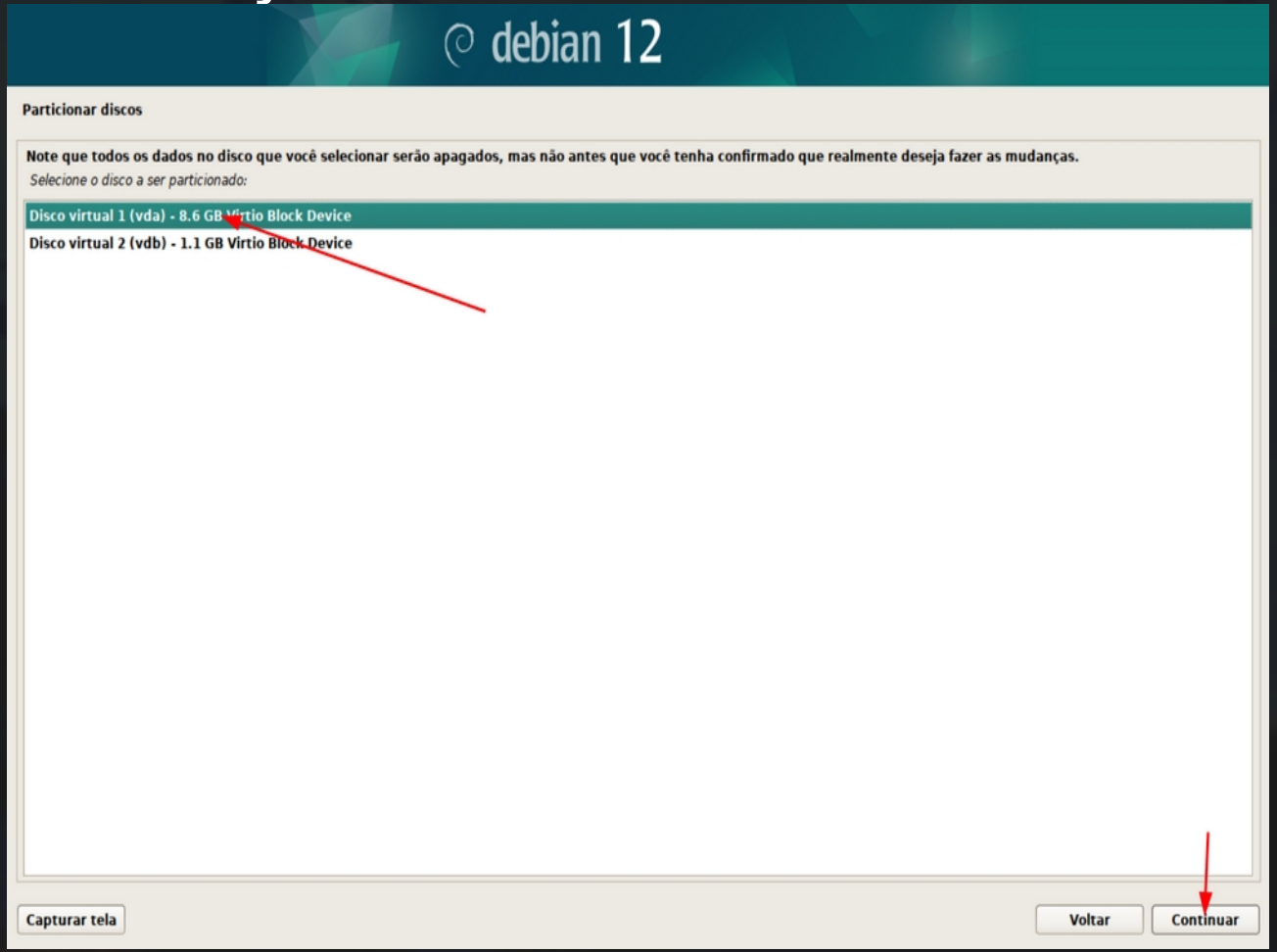
INSTALAÇÃO DO DEBIAN 12 COM LUKS



Debian Brasil

30 years debian

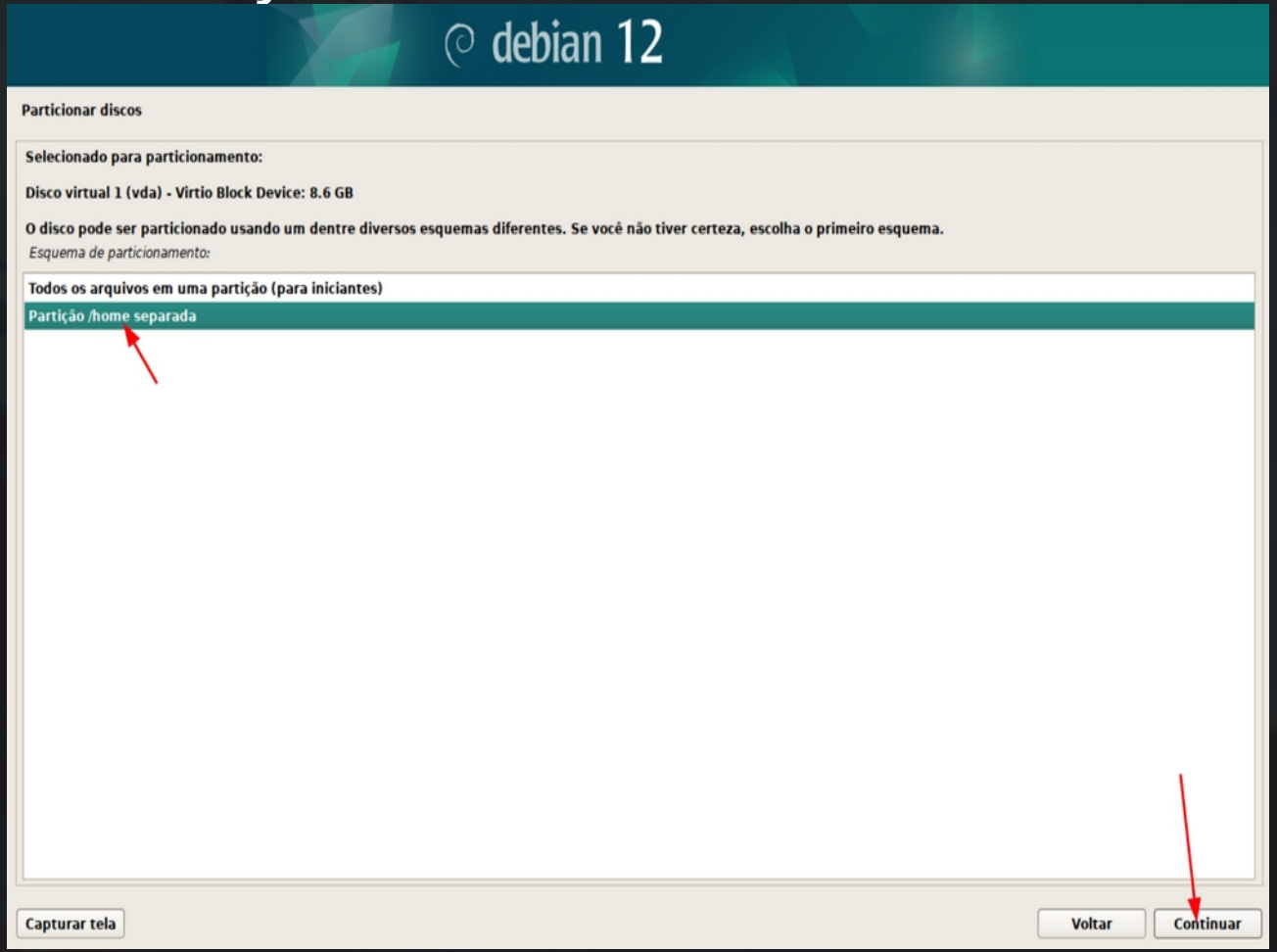
INSTALAÇÃO DO DEBIAN 12 COM LUKS



Debian Brasil

30 years debian

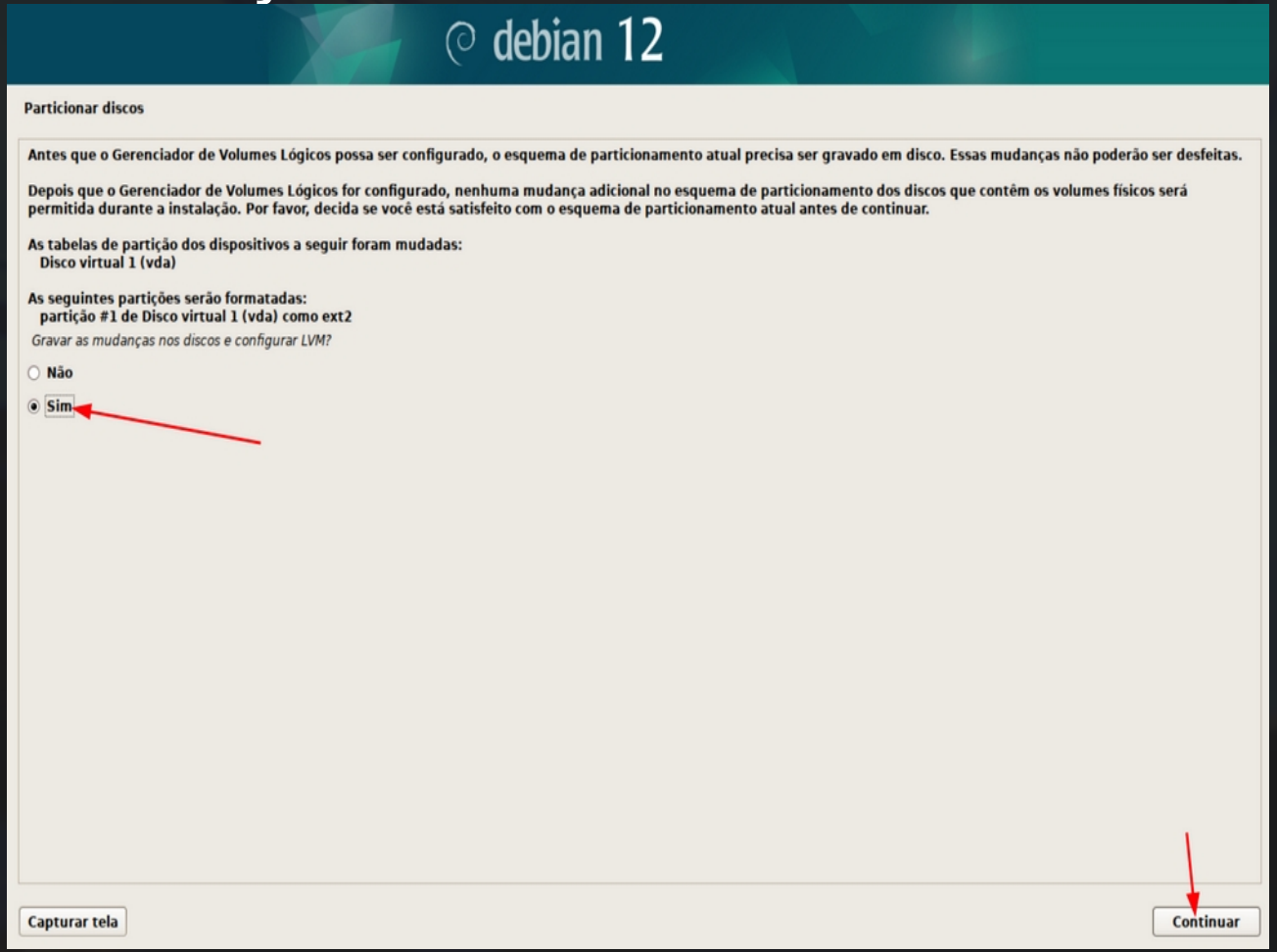
INSTALAÇÃO DO DEBIAN 12 COM LUKS



Debian Brasil

30 years debian

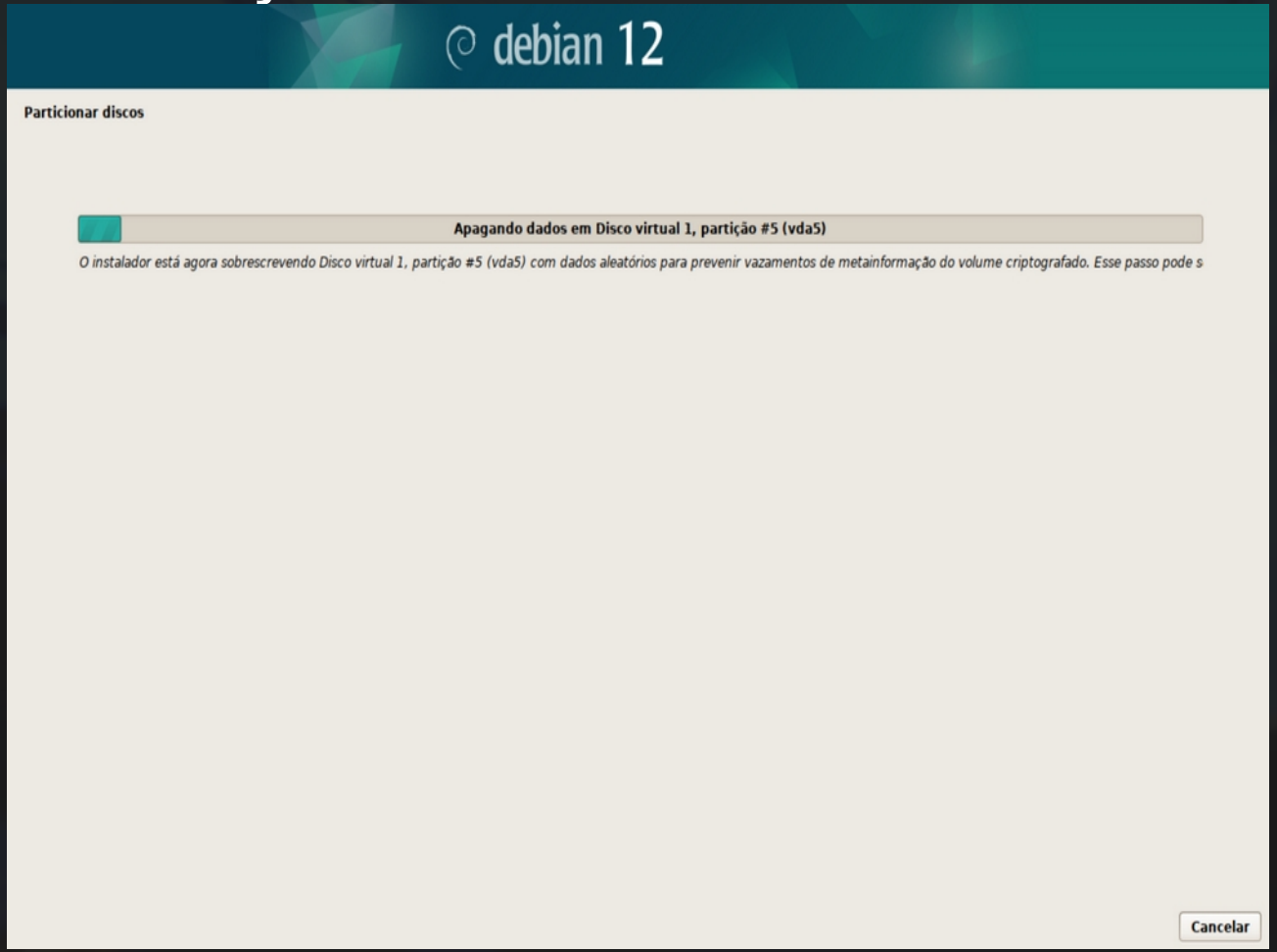
INSTALAÇÃO DO DEBIAN 12 COM LUKS



Debian Brasil

30 years debian

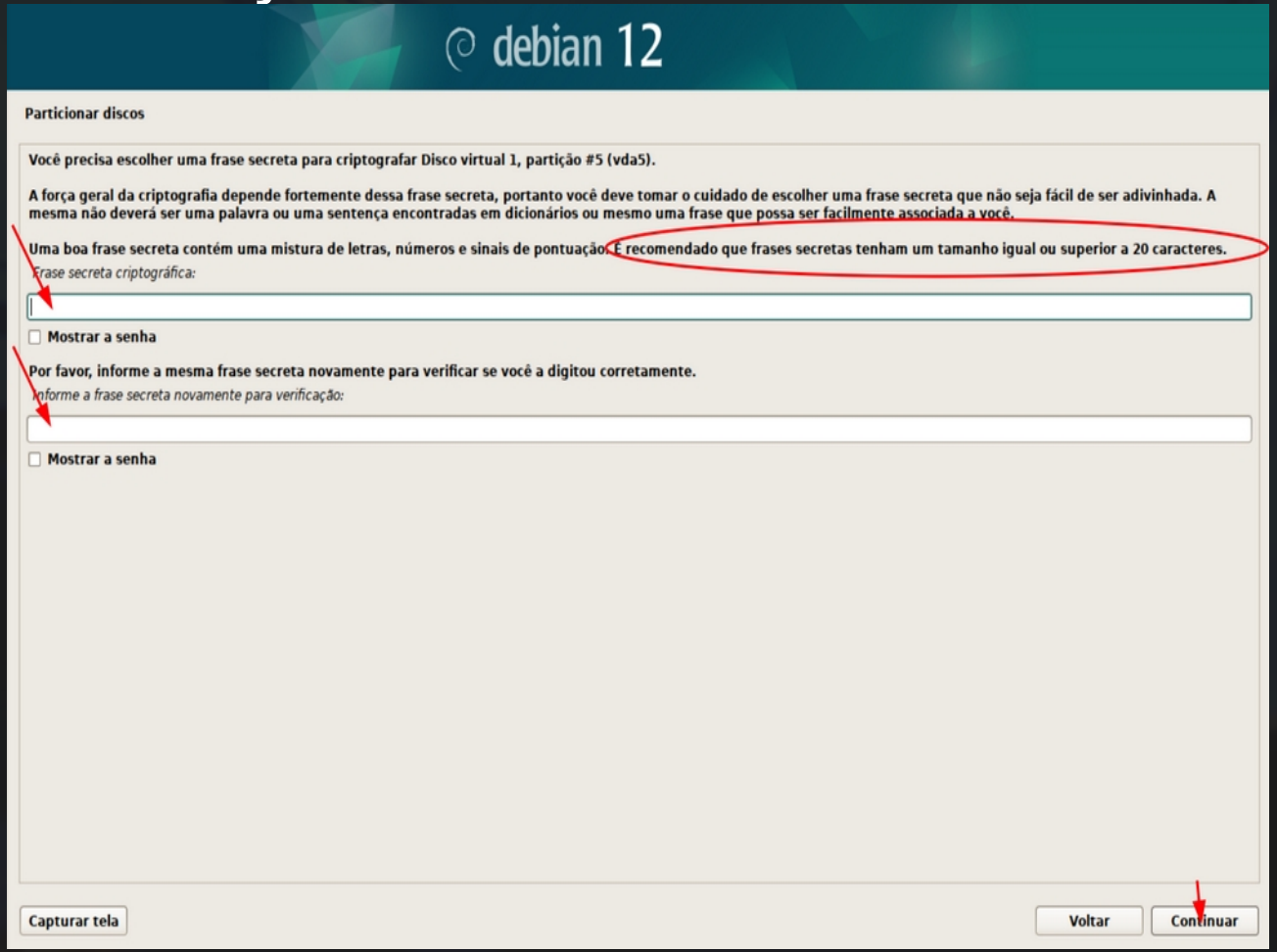
INSTALAÇÃO DO DEBIAN 12 COM LUKS



Debian Brasil

30 years debian

INSTALAÇÃO DO DEBIAN 12 COM LUKS

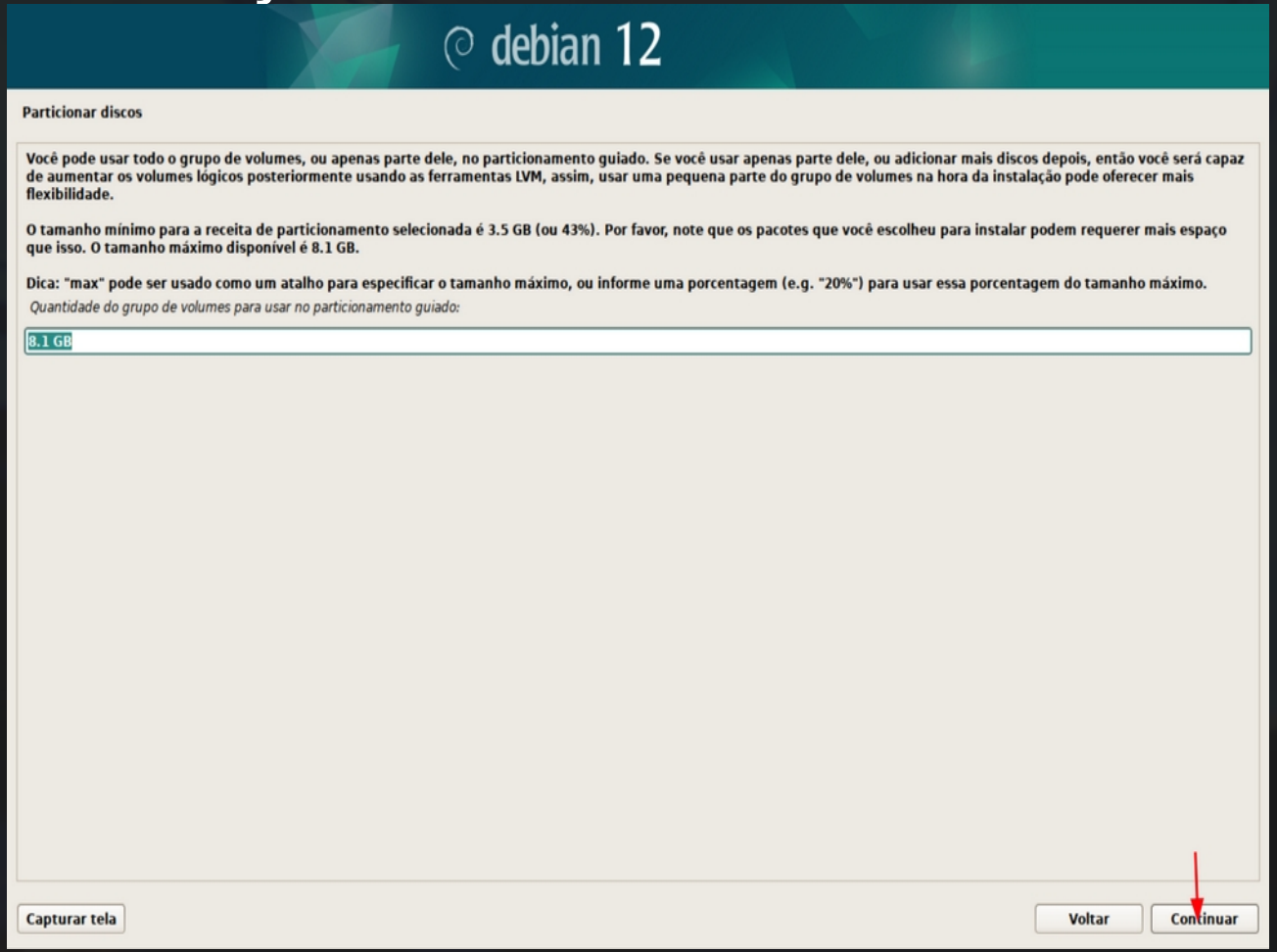


Debian Brasil

Andrade - Ago 23

30 years debian

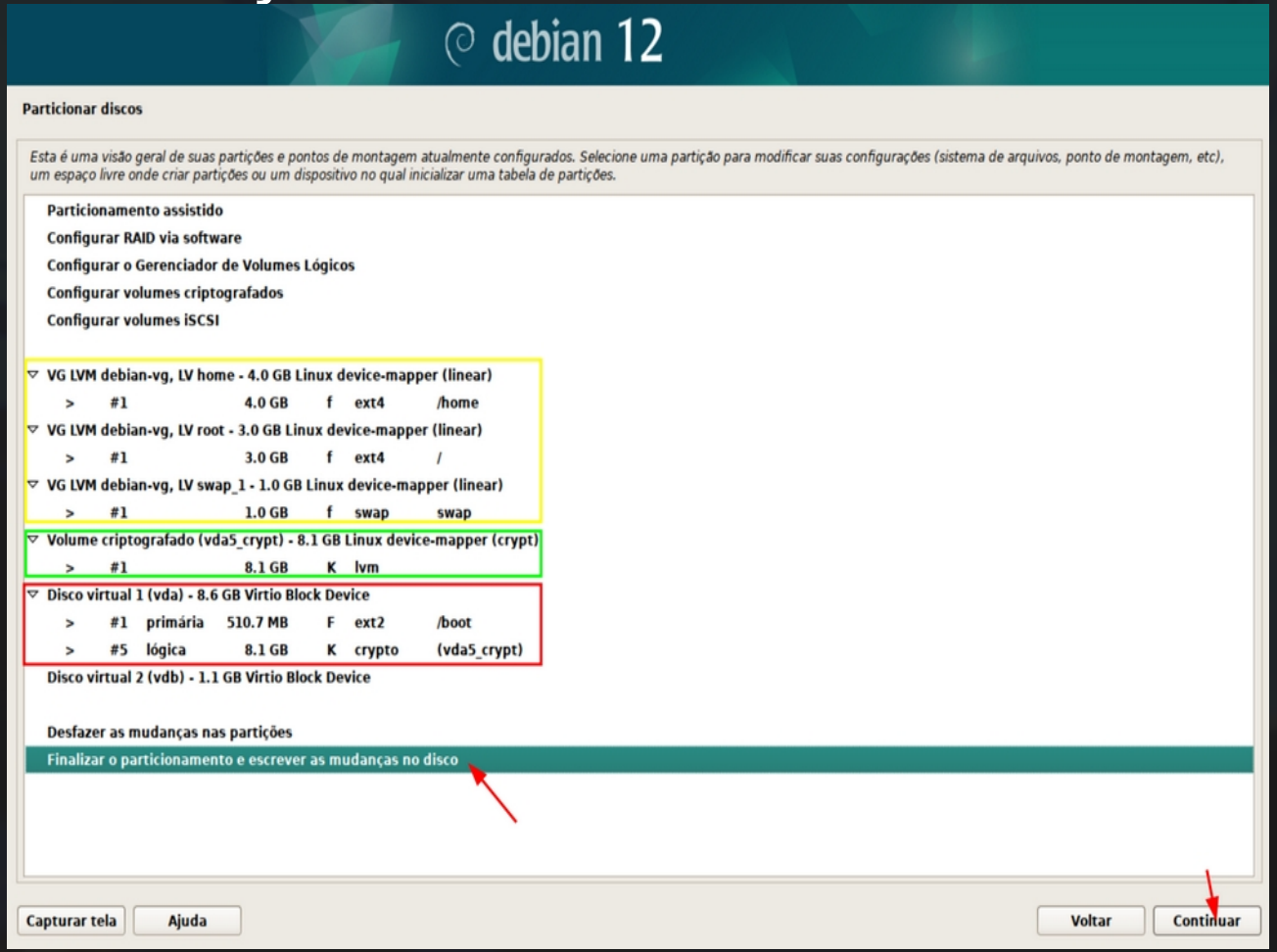
INSTALAÇÃO DO DEBIAN 12 COM LUKS



Debian Brasil

30 years debian

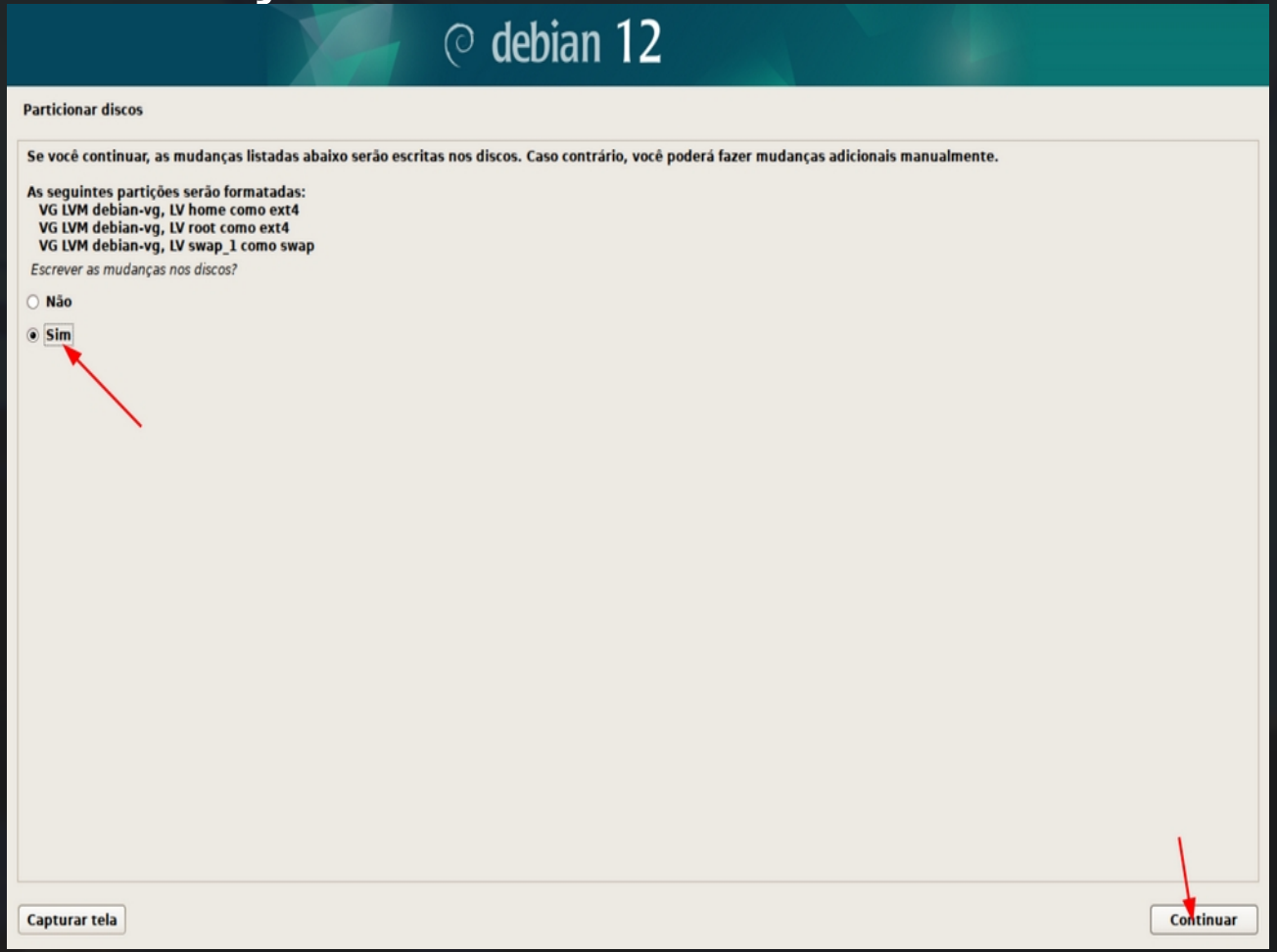
INSTALAÇÃO DO DEBIAN 12 COM LUKS



Debian Brasil

30 years debian

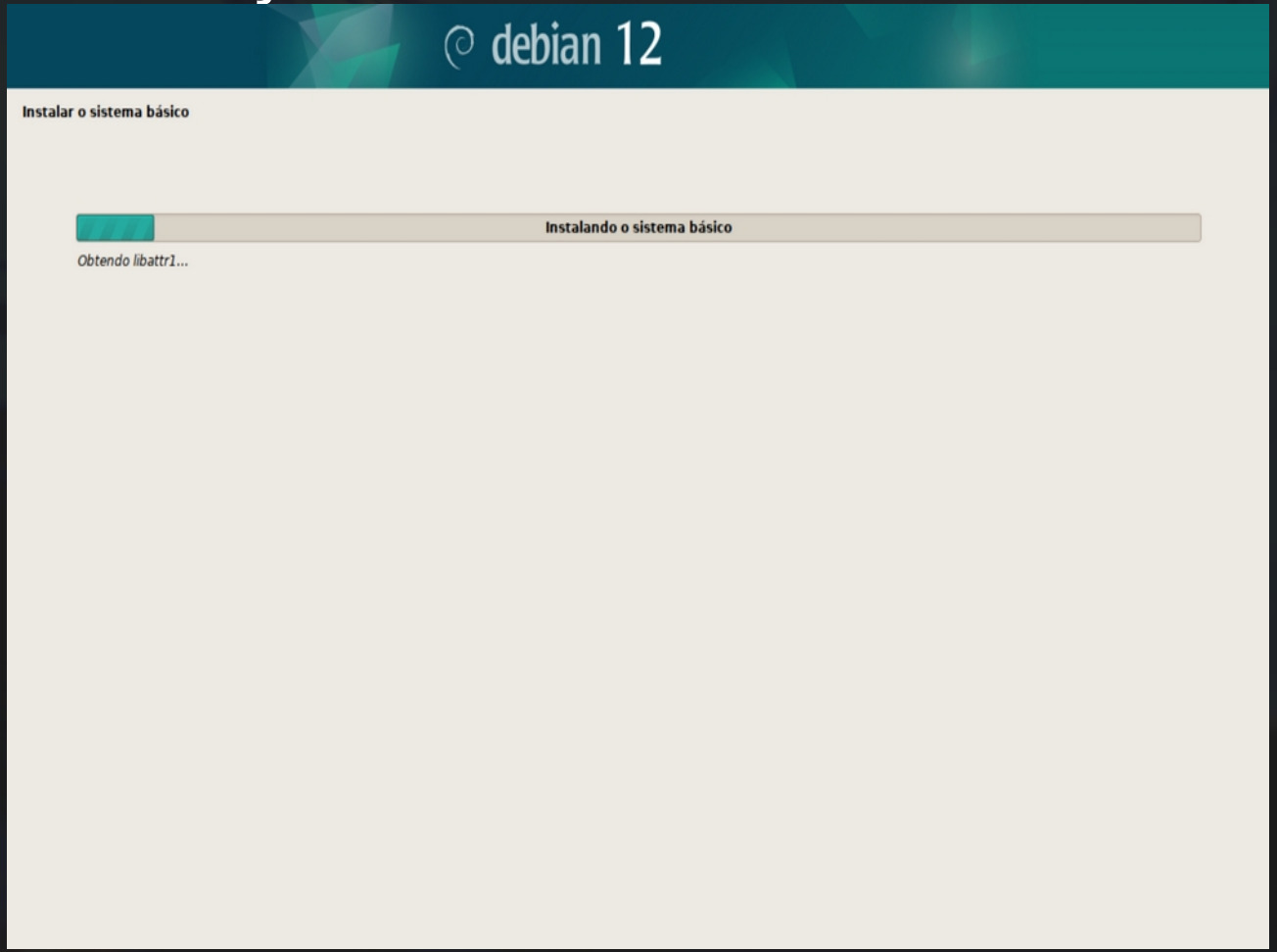
INSTALAÇÃO DO DEBIAN 12 COM LUKS



Debian Brasil

30 years debian

INSTALAÇÃO DO DEBIAN 12 COM LUKS



Debian Brasil

30 years debian

INSTALAÇÃO DO DEBIAN 12 COM LUKS

```
root@debian:~# lsblk
NAME                    MAJ:MIN RM  SIZE RO TYPE  MOUNTPOINTS
sr0                      11:0    1  3.7G  0 rom
vda                     254:0    0    8G  0 disk
├─vda1                  254:1    0  487M  0 part  /boot
├─vda2                  254:2    0    1K  0 part
└─vda5                  254:5    0  7.5G  0 part
  └─vda5_crypt          253:0    0  7.5G  0 crypt
    ├─debian--vg-root   253:1    0  2.8G  0 lvm   /
    ├─debian--vg-swap_1 253:2    0  976M  0 lvm   [SWAP]
    └─debian--vg-home   253:3    0  3.8G  0 lvm   /home
vdb                     254:16   0    1G  0 disk
```

SUMÁRIO

CRIANDO PARTIÇÕES E CRIPTOGRAFANDO O DISCO

Criação básica de partição com LUKS

```
apt install cryptsetup
lsblk
apt install hexyl
hexyl /dev/vdb | head
cryptsetup -v luksFormat /dev/vdb
hexyl /dev/vdb | head
cryptsetup open /dev/vdb pendrive-cripto
cryptsetup status pendrive-cripto
mkfs.ext4 /dev/mapper/pendrive-cripto
mkdir /mnt/pendrive
mount /dev/mapper/pendrive-cripto /mnt/pendrive/
touch lista
echo "arquivo de teste luks" >> lista
```

CRIANDO PARTIÇÕES E CRIPTOGRAFANDO O DISCO

Automatizar o processo de montagem

```
vi /etc/crypttab
pendrive-cripto /dev/vdb none luks,discard

vi /etc/fstab
/dev/mapper/pendrive-cripto /mnt/pendrive ext4  defaults    0   0

reboot
```

CRIANDO PARTIÇÕES E CRIPTOGRAFANDO O DISCO

Criando uma chave para montagem automática do bloco

```
dd if=/dev/urandom of=/root/key bs=4096 count=1
cryptsetup luksAddKey /dev/vdb /root/key
chmod 000 /root/key
vi /etc/crypttab
pendrive-cripto /dev/vdb /root/key luks,discard

reboot e verficar a partição montada
```

SUMÁRIO

CONCLUSÃO

- Instalar o Debian / Linux GNU com criptografia é simples e deve ser realizado sempre que possível.
- A criptografia não substitui backup!
- Fazer backup do HEADER da partição LUCKS é uma boa prática de segurança dos seus dados.

```
# cryptsetup luksHeaderBackup /dev/DEVICE --header-backup-file /path/to/backup
```

```
# cryptsetup luksHeaderRestore /dev/DEVICE --header-backup-file /path/to/backup
```

REFERÊNCIAS

- https://gitlab.com/cryptsetup/cryptsetup/
- https://gitlab.com/cryptsetup/LUKS2-docs/blob/main/luks2_doc_wip.pdf
- https://en.wikipedia.org/wiki/Linux_Unified_Key_Setup
- https://wiki.archlinux.org/title/dm-crypt/Device_encryption

  Benchmark do disco criptografado
- https://www.phoronix.com/review/ubuntu-1804-encrypt

Palestra disponível em *https://andrade.wiki.br/palestras/*

debian

Debian Day
Brasil 2023

Debian
Brasil

30 years
debian

Andrade - Ago 23