VERACRYPT

VOLUME 7/7

Proteção extra forte para arquivos confidenciais

maria d'ajuda

#07

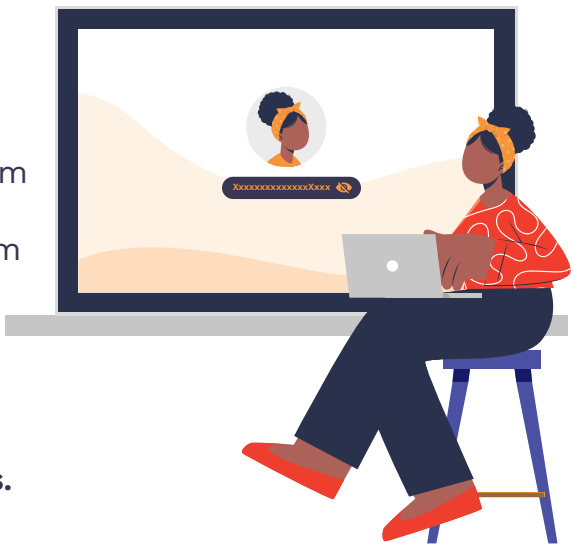
Criptografia para proteger aqueles arquivos mais que importantes

Oi, sou a Maria e vim te contar uma dica para ficar mais segura. Estou melhorando minha segurança digital e já avancei muito na minha proteção, mas às vezes fico com a pulga atrás da orelha com certas coisas que me enviam.

Documentos pessoais, nudes (recebidas ou enviadas) e todo tipo de arquivo que pode expor a mim ou a alguma companheira... Existe alguma proteção extra forte para o que é confidencial?

md'a

Perguntei para uma amiga que trabalha com segurança digital e ela me contou que existem programas que criam uma **camada forte de criptografia para proteger arquivos dentro de pastas secretas ou pen drives.**



Entendendo os riscos

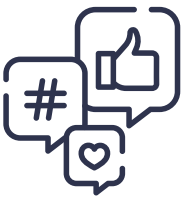
Possuir um arquivo confidencial seu ou de outra pessoa é uma responsabilidade importante. Há muitas maneira de ter dados digitais roubados de nossos dispositivos:

NO CELULAR

O risco maior é a perda ou a instalação de programas usados para nos espionar.

NO COMPUTADOR

Se alguém tiver acesso físico ao seu computador muito provavelmente vai conseguir ver todos os arquivos, mesmo que você use senha para entrar no sistema. Isso porque os sistemas operacionais como o Windows e o Mac por padrão não usam criptografia, o que permite qualquer pessoa com um pouco de conhecimento técnico facilmente ler os arquivos no HD.



NAS CONTAS ONLINE (e-mail, nuvem, redes sociais, etc)

Roubo de contas abusando de senhas fracas, falta de segundo fator de autenticação ou uso compartilhado.

Criptografia para proteger o computador

Nessa jornada eu aprendi: No que diz respeito à segurança digital todo risco tem uma ou mais proteções que podem me deixar mais segura.

Há 2 maneiras importantes de proteger os arquivos em nosso computador:

01 **Criptografar todo o disco ou**

02 **Criptografar os arquivos mais importantes.**

O Sistema operacional do computador pode ser Windows, Mac ou Linux. Cada um deles possui uma maneira de ativar a criptografia de disco. Uma vez ativada, não importa quanto conhecimento técnico uma pessoa tenha: para acessar seus arquivos ela vai precisar da sua **senha de criptografia.**

Windows:
Bitlocker - https://support.google.com/a/answer/9539590[1

Mac:
Filevault - https://support.apple.com/pt-br/guide/mac-help/mh11785

Linux:
Luks - https://pt.linux-console.net/?p=10126

É muito recomendado ativar essa proteção, mas ela **funciona como se fosse um cofre.**

Enquanto o computador está desligado o cofre está trancado e ninguém poderá ler os arquivos sem a sua senha.

Mas uma vez que a senha foi inserida e o computador está ligado, aí os arquivos ficam vulneráveis.

Criptografando arquivos confidenciais: Veracryptz

Pensando nisso há uma outra camada de segurança que podemos inserir:

Criptografia só naqueles arquivos super confidenciais.
Pra isso me recomendaram o Veracrypt, um programa gratuito e de código aberto que oferece versões não só para Windows, como também para macOS e Linux.

Com ele, é possível criar arquivos, pen drives ou discos criptografados, que ficam disponível apenas após digitar sua senha.

Achei bacana e resolvi testar. Olha lá o que eu fiz:

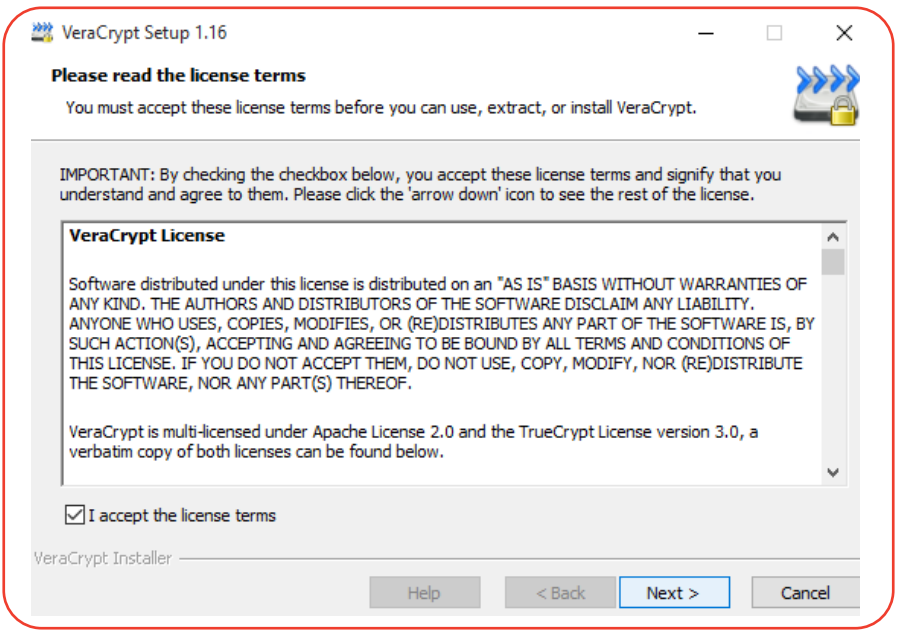
01 Entrei no site oficial e fiz o download (baixei)

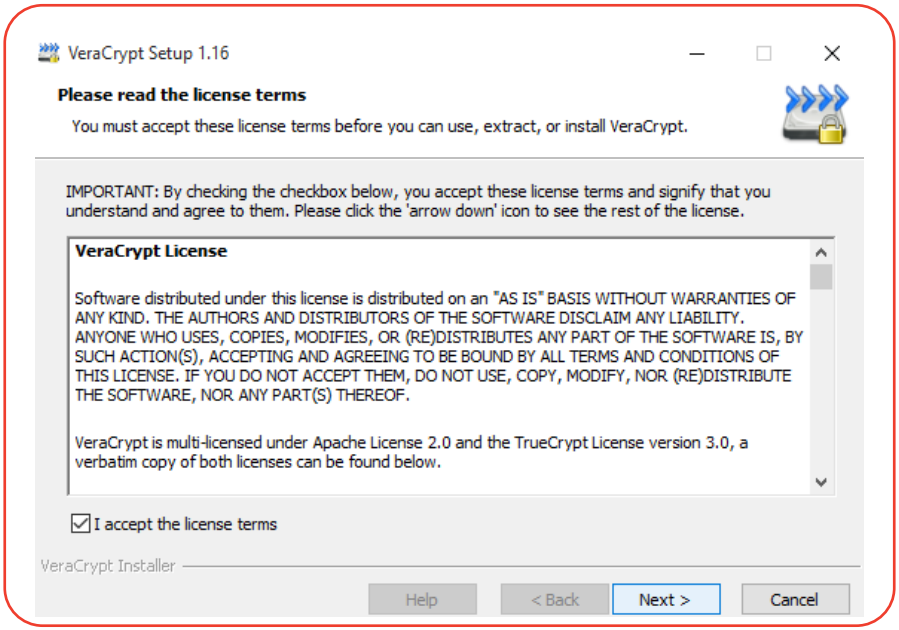
- ***macOS (Monterey 12 and later)***:
  - OSXFUSE compatible version : VeraCrypt_1.26.14.dmg (PGP Signature)

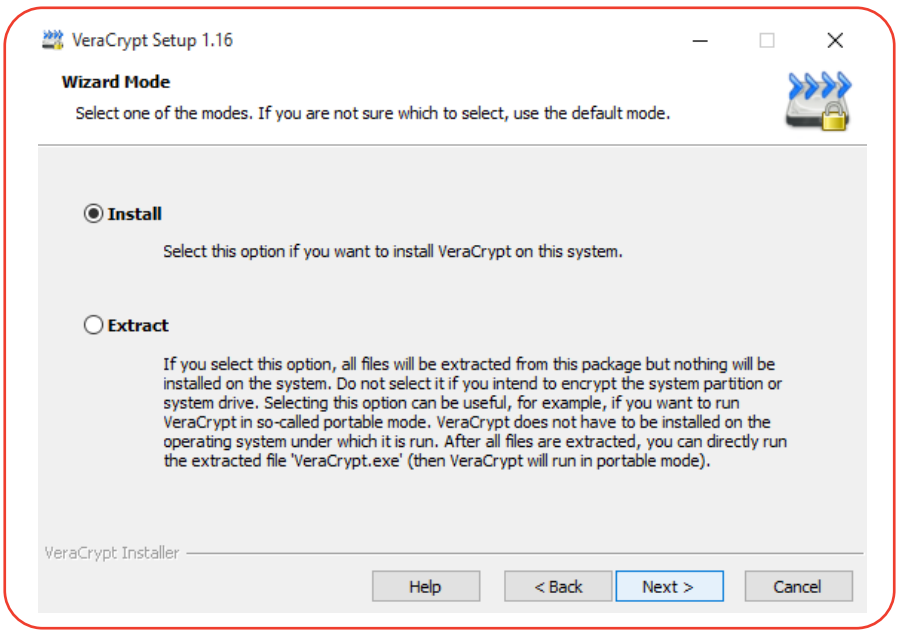
- ***Windows***:
  - EXE Installer: VeraCrypt Setup 1.26.15.exe (PGP Signature)

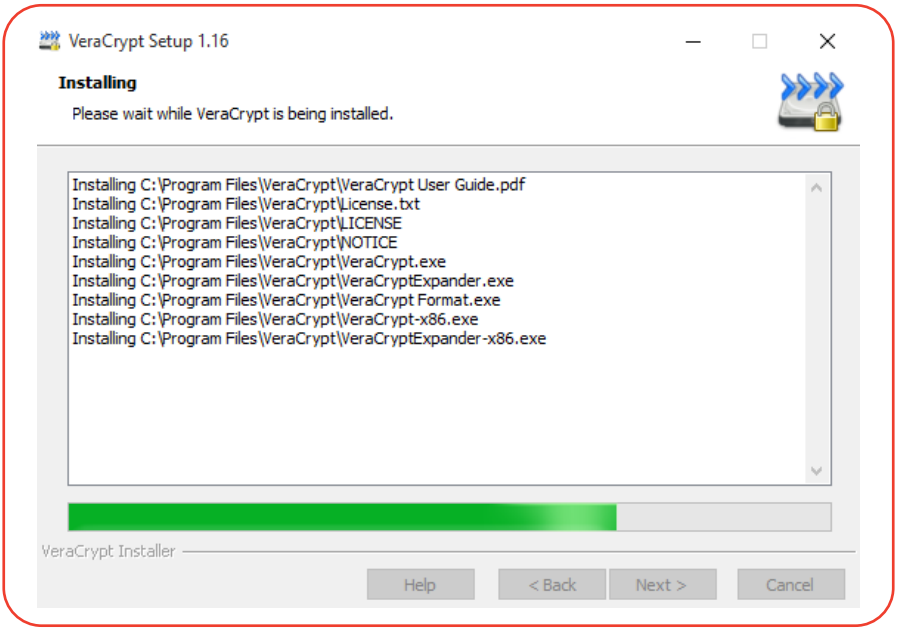
VeraCrypt Setup 1.26.15.exe
34,4 MB — launchpadlibrarian.net — 12:02

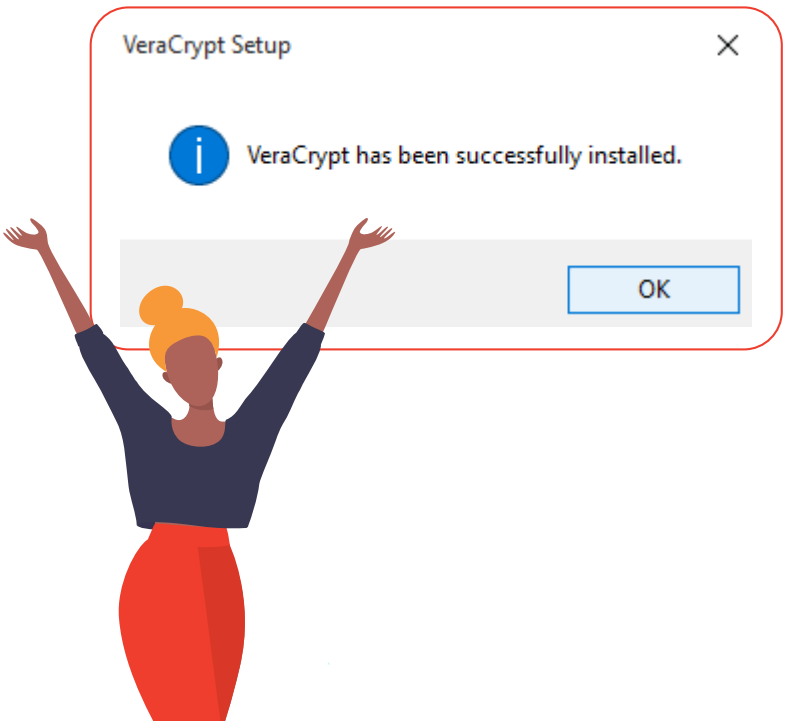
02 Instalei o Veracrypt no meu computador




VeraCrypt Setup 1.16
Please read the license terms
You must accept these license terms before you can use, extract, or install VeraCrypt.
IMPORTANT: By checking the checkbox below, you accept these license terms and signify that you understand and agree to them. Please click the 'arrow down' icon to see the rest of the license.
VeraCrypt License
Software distributed under this license is distributed on an "AS IS" BASIS WITHOUT WARRANTIES OF ANY KIND. THE AUTHORS AND DISTRIBUTORS OF THE SOFTWARE DISCLAIM ANY LIABILITY. ANYONE WHO USES, COPIES, MODIFIES, OR (RE)DISTRIBUTES ANY PART OF THE SOFTWARE IS, BY SUCH ACTION(S), ACCEPTING AND AGREEING TO BE BOUND BY ALL TERMS AND CONDITIONS OF THIS LICENSE. IF YOU DO NOT ACCEPT THEM, DO NOT USE, COPY, MODIFY, NOR (RE)DISTRIBUTE THE SOFTWARE, NOR ANY PART(S) THEREOF.
VeraCrypt is multi-licensed under Apache License 2.0 and the TrueCrypt License version 3.0, a verbatim copy of both licenses can be found below.
I accept the license terms
VeraCrypt Installer
Help
< Back
Next >
Cancel


VeraCrypt Setup 1.16
Wizard Mode
Select one of the modes. If you are not sure which to select, use the default mode.
Install
Select this option if you want to install VeraCrypt on this system.
Extract
If you select this option, all files will be extracted from this package but nothing will be installed on the system. Do not select it if you intend to encrypt the system partition or system drive. Selecting this option can be useful, for example, if you want to run VeraCrypt in so-called portable mode. VeraCrypt does not have to be installed on the operating system under which it is run. After all files are extracted, you can directly run the extracted file 'VeraCrypt.exe' (then VeraCrypt will run in portable mode).
VeraCrypt Installer
Help
< Back
Next >
Cancel


VeraCrypt Setup 1.16
Installing
Please wait while VeraCrypt is being installed.
Installing C:\Program Files\VeraCrypt\VeraCrypt User Guide.pdf
Installing C:\Program Files\VeraCrypt\License.txt
Installing C:\Program Files\VeraCrypt\LICENSE
Installing C:\Program Files\VeraCrypt\NOTICE
Installing C:\Program Files\VeraCrypt\VeraCrypt.exe
Installing C:\Program Files\VeraCrypt\VeraCryptExpander.exe
Installing C:\Program Files\VeraCrypt\VeraCrypt Format.exe
Installing C:\Program Files\VeraCrypt\VeraCrypt-x86.exe
Installing C:\Program Files\VeraCrypt\VeraCryptExpander-x86.exe
VeraCrypt Installer
Help
< Back
Next >
Cancel


VeraCrypt Setup
VeraCrypt has been successfully installed.
OK

03 Aprendi alguns fundamentos do Veracrypt

Agora vou ser sincera com vocês...esse programa não é nada intuitivo.

Diferente do Signal e do Keepass que até achei tranquilo, o Veracrypt não é muito amigável, nem em português ele é!

Mas depois que me explicaram eu peguei o jeito.

O caminho das pedras é o seguinte:

1

Criar um volume criptografado e protegido por senha.

Esse 'volume' pode ser um arquivo, uma partição do computador ou um pendrive/HD externo.

2

Selecionar o arquivo ou disco e 'montar'

No processo de 'montar' seu computador reconhece aquele volume criptografado como uma unidade (D:, E:, F:, etc...).

Isso é equivalente a 'abrir' a porta do seu cofre.

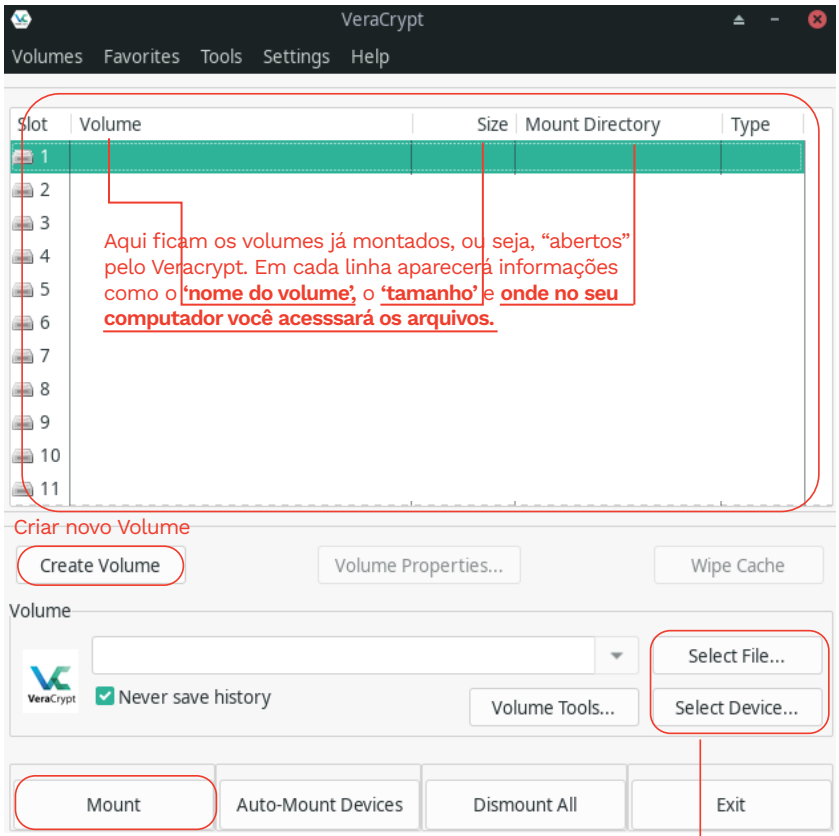
3

Desmontar o volume depois de usar

Uma vez que terminamos o uso é necessário 'desmontar' aquele volume. Ou seja, "fechar" a porta do cofre.

04 Aprendi para que serve cada coisa na tela principal

Vou explicar o que cada parte dessa tela significa:



“Montar” ou “Desmontar”
o volume selecionado.
Isso pedirá a senha e “abrirá”
ou “fechará” a porta do cofre.

Clique aqui para abrir volumes
veracrypts criados anteriormente.
Você pode selecionar
o arquivo ou dispositivo
(se for um disco ou pen drive)

05 Criei um novo arquivo criptografado

Agora sim podemos começar!

Cliquei em **Novo Volume** e abriu esse passo a passo.

É nessa tela que indicamos se queremos criar
um arquivo ou todo um pendrive/HD externo criptografado.

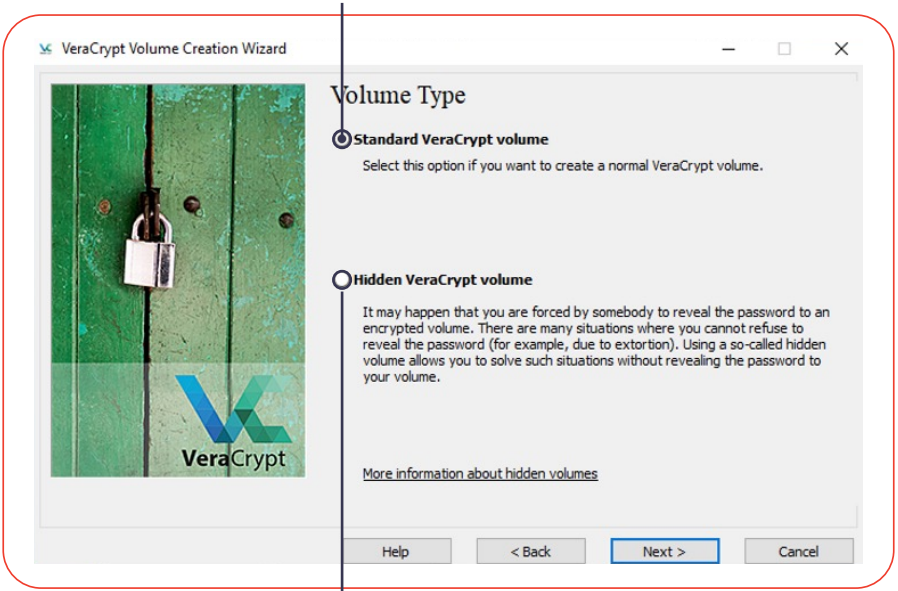
Me recomendaram começar com a 1a opção que é mais fácil, pois uma vez que temos o nosso arquivo criptografado é seguro armazená-lo em qualquer lugar.

06

Escolhi se quero um volume normal ou oculto

Aqui eu mantive volume comum e avancei.

Volume Veracrypt comum

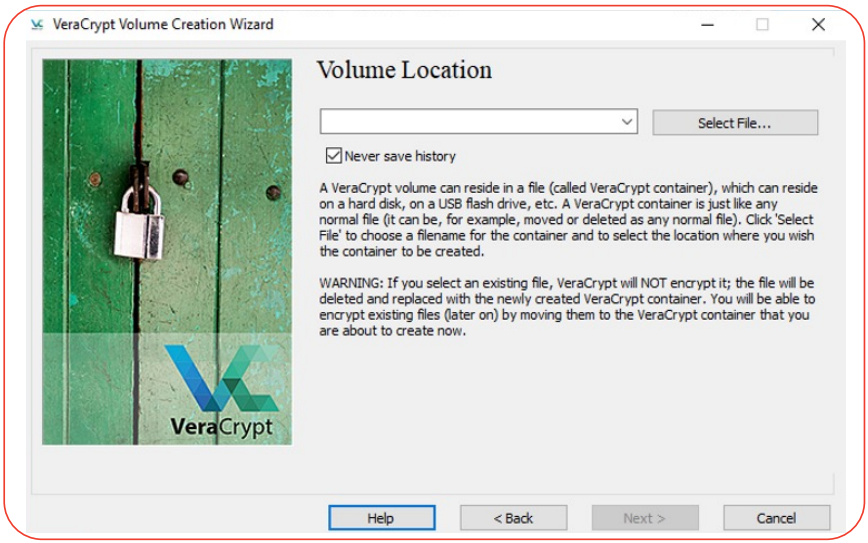


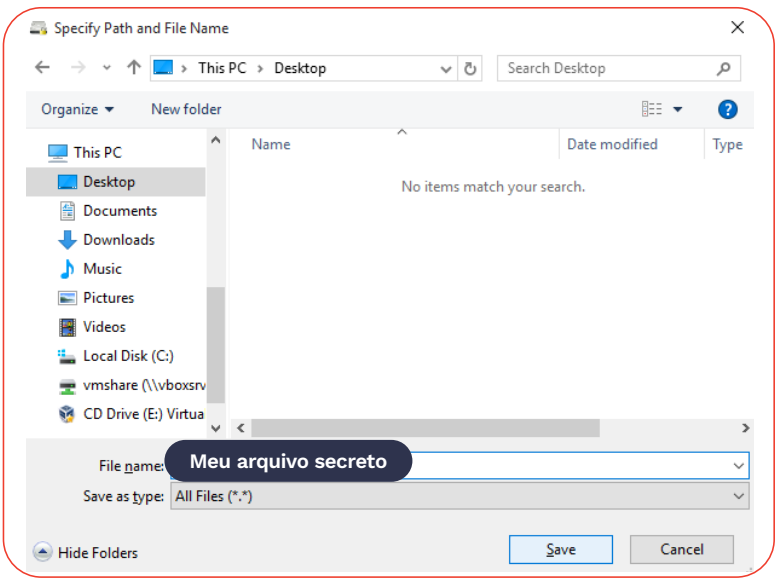
Volume Veracrypt escondido*

*Existe para casos graves onde precisamos enganar alguém que pode nos forçar a dar nossa senha. Nesse caso passaríamos uma senha “de mentira” que abriria uma pasta com arquivos “normais” e não os que realmente queremos proteger.

07 Escolhi o nome e o local do arquivo criptografado

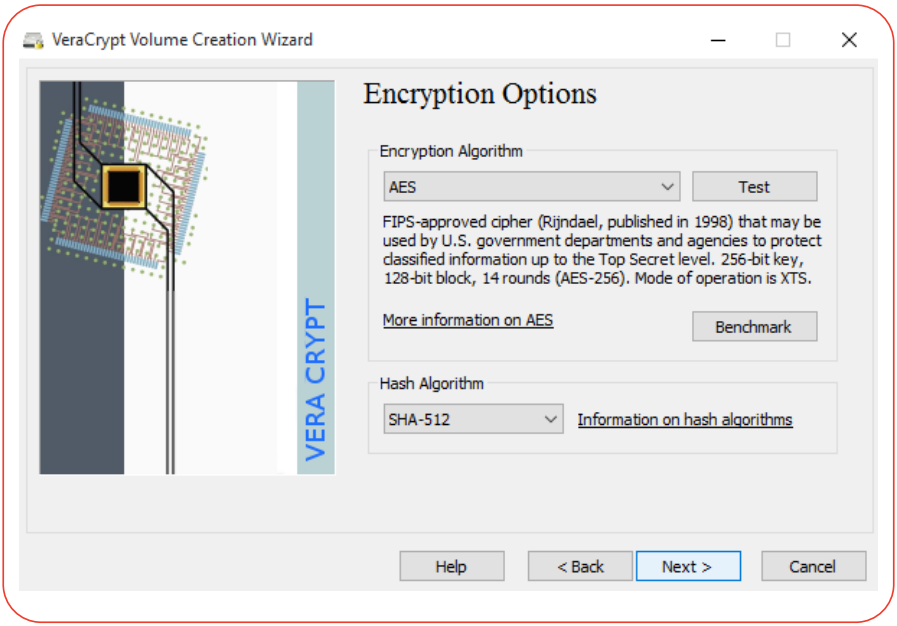
Cliquei em “Select File...” para escolher onde o arquivo será guardado no meu computador e qual o nome dele.





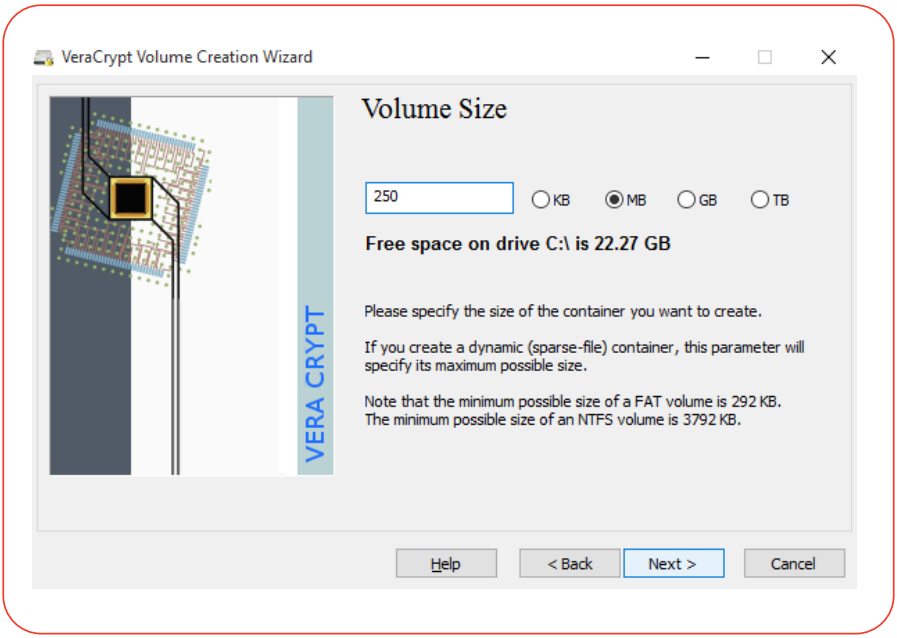
08 Mantive as opções avançadas como vieram

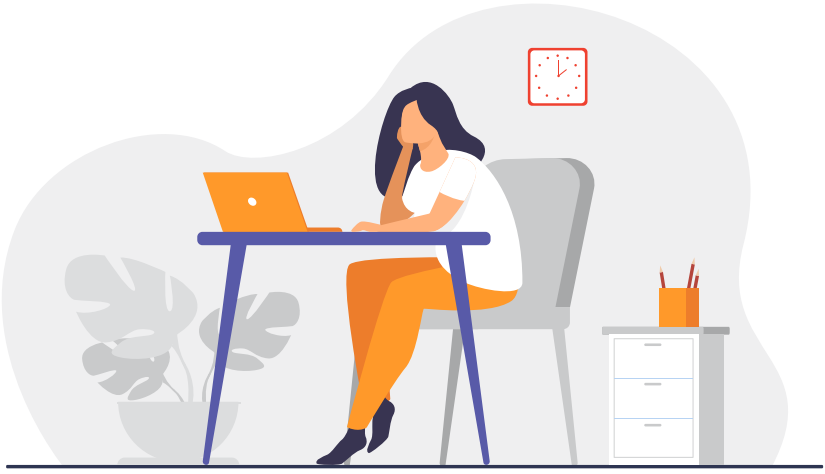
Nessa tela temos as 'opções de criptografia'. Como sou iniciante mantive como está e avancei, mas me garantiram que por padrão o Veracrypt usa uma criptografia forte e que não há maneira conhecida para quebrar essa proteção.



09 Escolhi o tamanho do meu arquivo Veracrypt

O tamanho total do arquivo que meu computador irá “montar” para guardar arquivos secretos. Aqui decidimos quantos MB, GB ou TB ele terá, desde que haja espaço no computador,





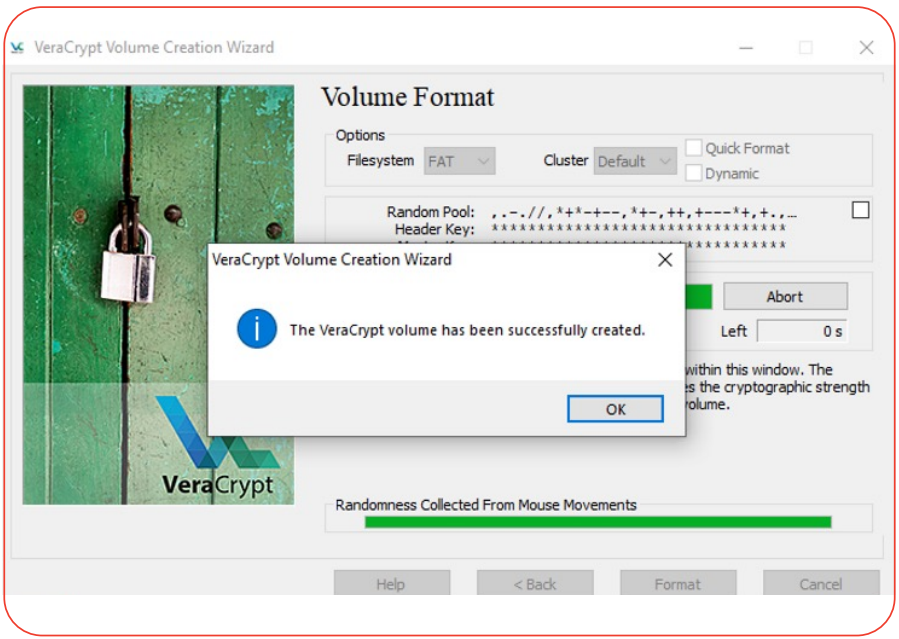
10 Escolhi a senha super-secreta do meu cofre de arquivos Veracrypt

Chegou a hora! Aqui inserimos a senha super forte e secreta do nosso arquivo criptografado (Não esqueça de salvar em seu Keepass, viu?)

11 Formatei o arquivo para aplicar a proteção

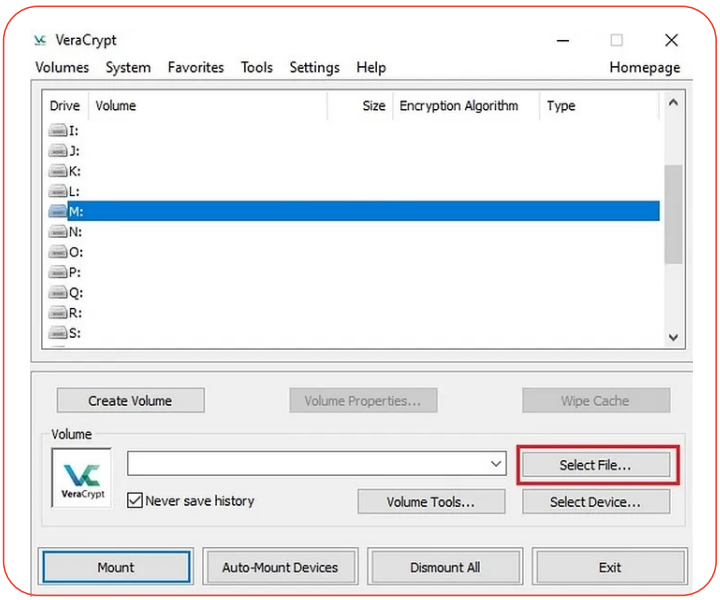
Essa é a última etapa na criação do nosso arquivo! E é uma tela meio estranha...eu quase não acreditei quando me explicaram: Veja bem, nesta tela deve-se mover o mouse bem rápido e aleatório até que a barra verde esteja cheia. Só depois disso clicamos em 'Format'.

E por que fazer isso?? Para gerar dados aleatórios que vão deixar a criptografia do seu Veracrypt ainda mais forte.

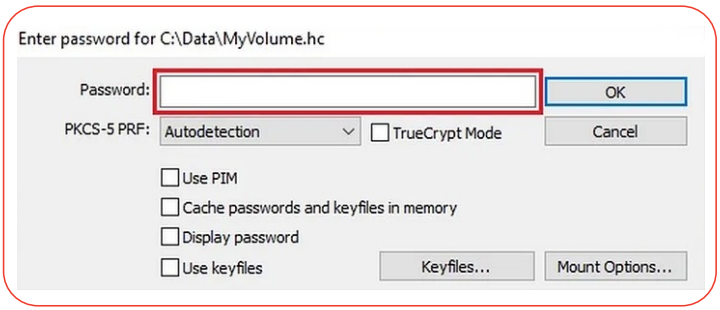


12 “Montei” o volume criado para abrir o cofre

O processo a seguir é o mesmo que deverá ser feito todas as vezes que desejamos acessar o nosso volume criptografado. De volta para a tela inicial do Veracrypt selecionei um dos volumes, no caso a linha M: e depois cliquei em ‘Select File’ para escolher o arquivo que criei e em seguida ‘Mount’.



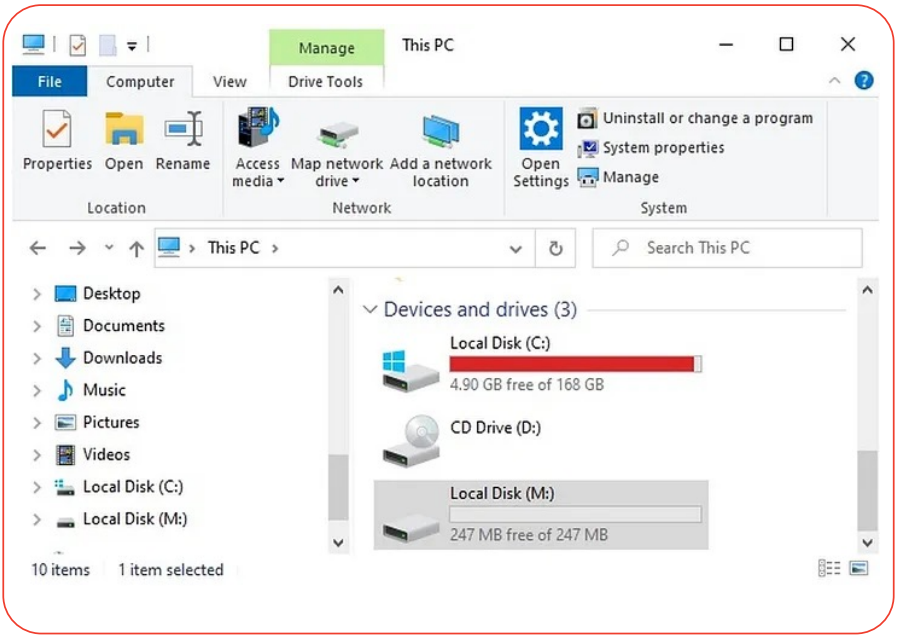
13 Coloque a senha



14 Agora é só usar!

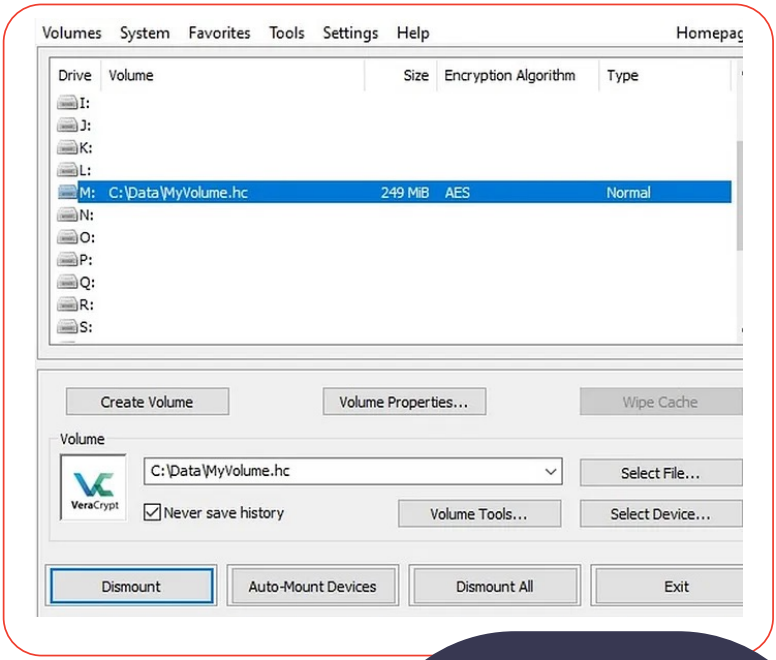
Pronto! Uma vez que a senha certa é colocada o Veracrypt vai “montar” o arquivo criptografado como sendo uma unidade.

Você pode abrir normalmente no Windows ou no MAC e começar a copiar ou salvar arquivos confidenciais dentro dela.



15 ...E depois de usar...é hora de 'desmontar'.

Assim como é recomendado sair ou fazer logoff de uma conta online após o uso, é necessário 'desmontar' o arquivo Veracrypt, fechando assim o cofre e fazendo o uso de toda sua proteção



Esse arquivo criptografado pode ser aberto e montado em qualquer computador, desde que tenha o Veracrypt instalado e a pessoa saiba a senha definida na criação do arquivo.

Não esqueça do Backup

Uma vez que nosso arquivo criptografado foi criado e salvo em nosso computador ele está protegido contra almas sebosas, mas não contra perda.

Perdas de dados podem acontecer com qualquer um, por isso é importante manter sempre uma cópia de segurança desse arquivo em outro lugar. A vantagem nesse caso é que o arquivo já está criptografado, então é mais tranquilo fazer backup dele em um pen drive comum, e-mail, nuvem, o que for.

O IMPORTANTE É FAZER PARA NÃO FICAR SEM :)

Na palma da mão

Infelizmente não existe o Veracrypt para celular, mas me recomendaram um programa igualmente seguro, feito para quem recebe ou cria informações sigilosas a partir celular, como é o caso de jornalistas, advogados e ativistas.

...Mas que também é excelente para guardar nudes, informações pessoais e o que mais eu quiser proteger! Esse aplicativo se chama Tella, pode ser instalado gratuitamente em celulares e tablets. Veja mais em:

https://tella-app.org/

Para ler mais sobre o Veracrypt e como proteger arquivos:

https://securityinabox.org/pt/tools/veracrypt/

https://escoladeativismo.org.br/veracrypt-como-instalar-e-porque-usar-pastas-criptografadas-no-computador/

https://tella-app.org/pt-BR/faq/

Para ler mais sobre segurança digital:

https://marialab.org/biblioteca
https://pratododia.org
https://blogueirasnegras.org/guia
https://digitalfirstaid.org/pt

REALIZAÇÃO:

maria [lab]

APOIO:

HEINRICH BÖLL STIFTUNG
RIO DE JANEIRO
Brasil