Ministério da Saúde
Secretaria de Vigilância em Saúde e Ambiente
Departamento de Análise Epidemiológica e Vigilância de Doenças não Transmissíveis

NOTA INFORMATIVA Nº 3/2025-DAENT/SVSA/MS

1. ASSUNTO

1.1. Informa acerca do compartilhamento e da manipulação segura dos dados dos sistemas de Informação sob gestão do Departamento de Análise Epidemiológica e Vigilância de Doenças não Transmissíveis da Secretaria de Vigilância em Saúde e Ambiente do Ministério da Saúde (DAENT/SVSA/MS).

2. CONTEXTUALIZAÇÃO

2.1. O DAENT/SVSA/MS é responsável pela gestão de informação e de negócio (Portarias DATASUS nº 68 - 91 de 08.07.24 - Gestor de negócio e de informação DAENT) dos seguintes sistemas:

- Sistema de Informações sobre Nascidos Vivos (SINASC);
- Sistema de Informação de Agravos de Notificação (SINAN);
- e-SUS SINAN;
- Sistema de Registro de Eventos em Saúde Pública (RESP - Microcefalia);
- Sistema de Notificação dos Casos de Síndrome Respiratória Leve (e-SUS Notifica);
- Sistema de Informações sobre Mortalidade (SIM).

2.2. Para garantir o compartilhamento seguro dos dados desses sistemas, recomenda-se que as informações sejam criptografadas e enviadas por meio de um link exclusivo, destinado ao operador responsável pelo recebimento, conforme previsto no termo de compromisso para uso dos dados. Após a confirmação do recebimento pelo operador, o link deverá ser desativado. Em seguida, a senha para descriptografar o arquivo deverá ser enviada por meio de um canal diferente de compartilhamento. Recomenda-se, preferencialmente, o uso do telefone institucional para o envio dessa senha.

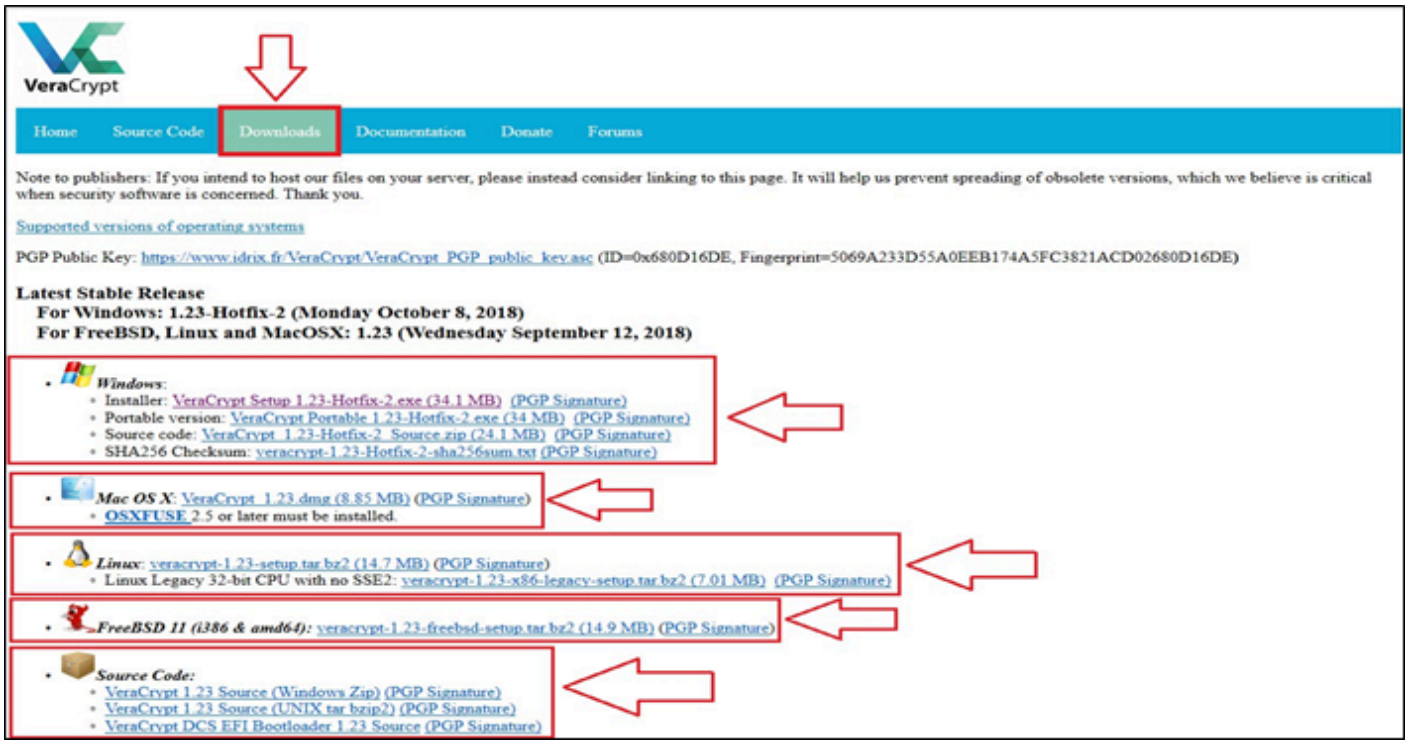
2.3. Para a execução deste fluxo, é necessário que ambas as partes, tanto o remetente quanto o destinatário dos dados, possuam o software VeraCrypt devidamente instalado em seus equipamentos. Nas unidades do Ministério da Saúde, a instalação deverá ser requerida à equipe do DATASUS.

2.4. Para assegurar a manipulação segura dos dados, recomenda-se a criação de uma unidade criptografada no computador do operador. No caso de o operador ser colaborador do Ministério da Saúde, tal unidade deverá ser criada na estação de trabalho. Ressalta-se que dados sensíveis somente poderão ser manipulados nas estações de trabalho pertencentes a rede do Departamento de Informação e Informática do SUS (DataSUS). No caso de unidades vinculadas a outros órgãos públicos, a manipulação dos dados deverá ocorrer exclusivamente dentro do ambiente físico de segurança institucional do órgão solicitante, respeitando os mesmos requisitos de proteção e sigilo.

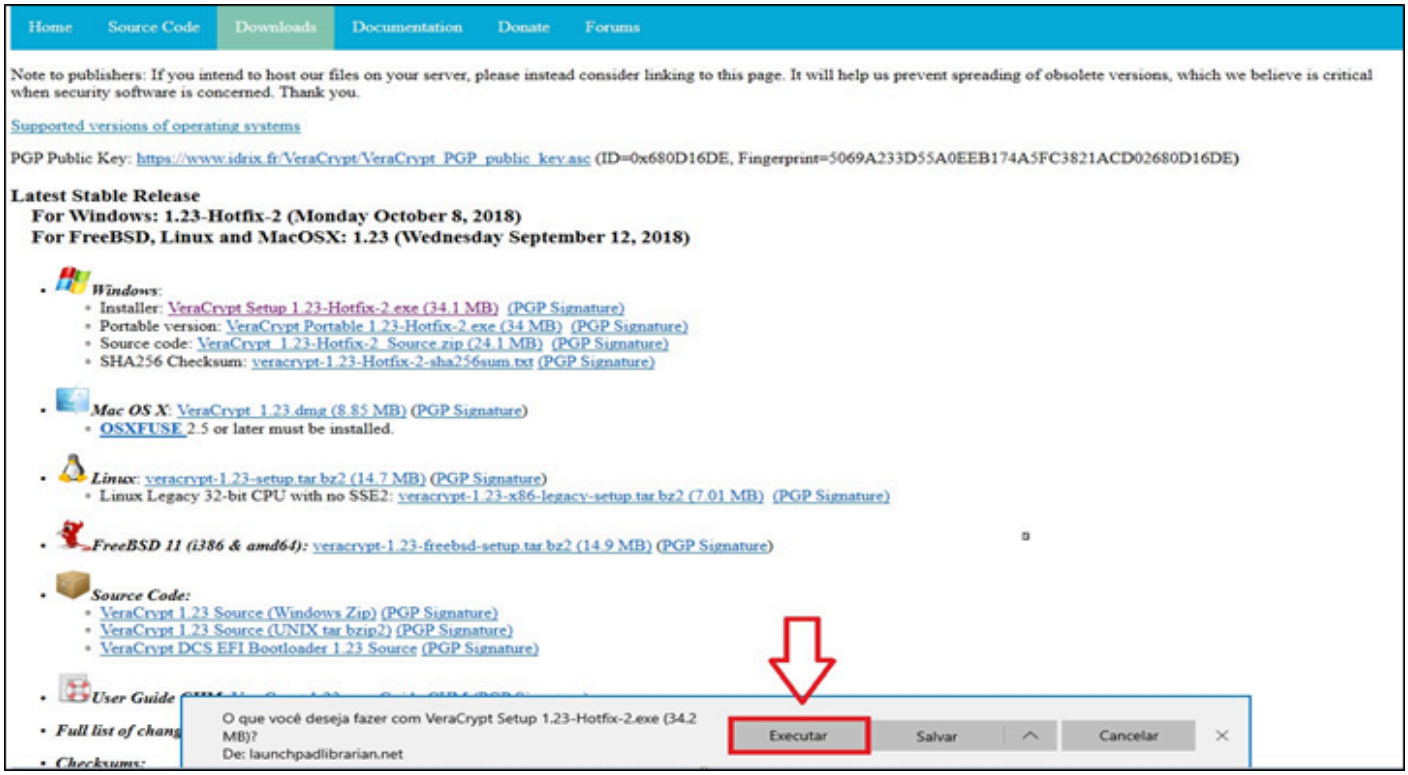
2.5. Procedimentos referente a criptografia, compartilhamento e manipulação de forma segura serão apresentados a seguir:

3. COMO INSTALAR O VERACRYPT

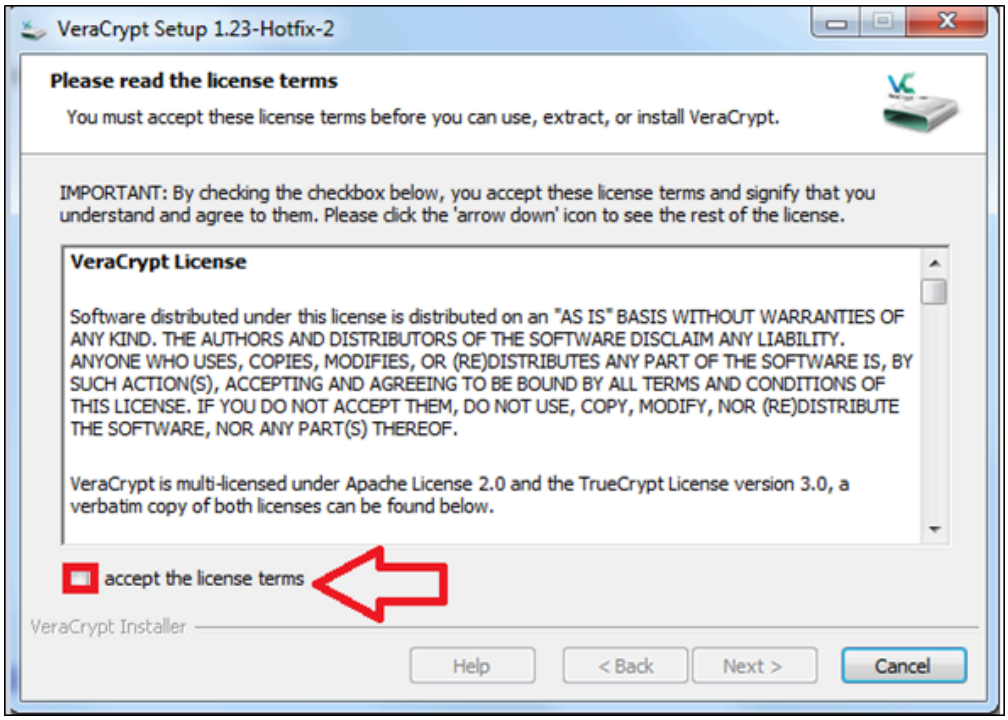
3.1. Acesse o site oficial https://www.veracrypt.fr/en/Downloads.html. Clique no sistema operacional de seu computador (Windows, MacOs, Linux) para iniciar o download do programa:



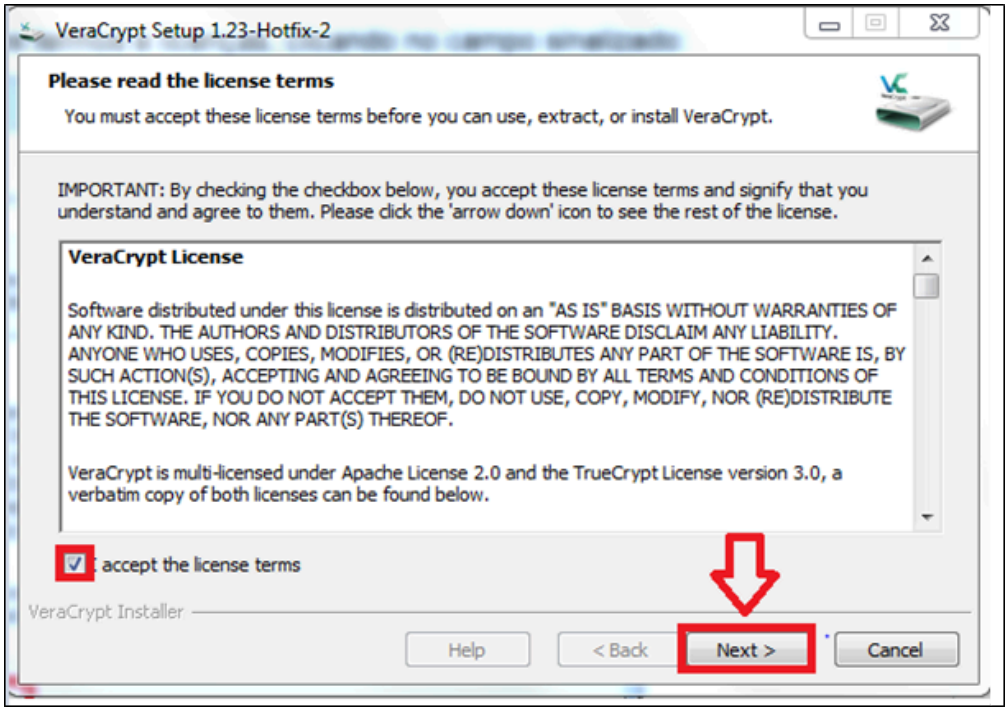
3.2. Clique em "***Executar***";



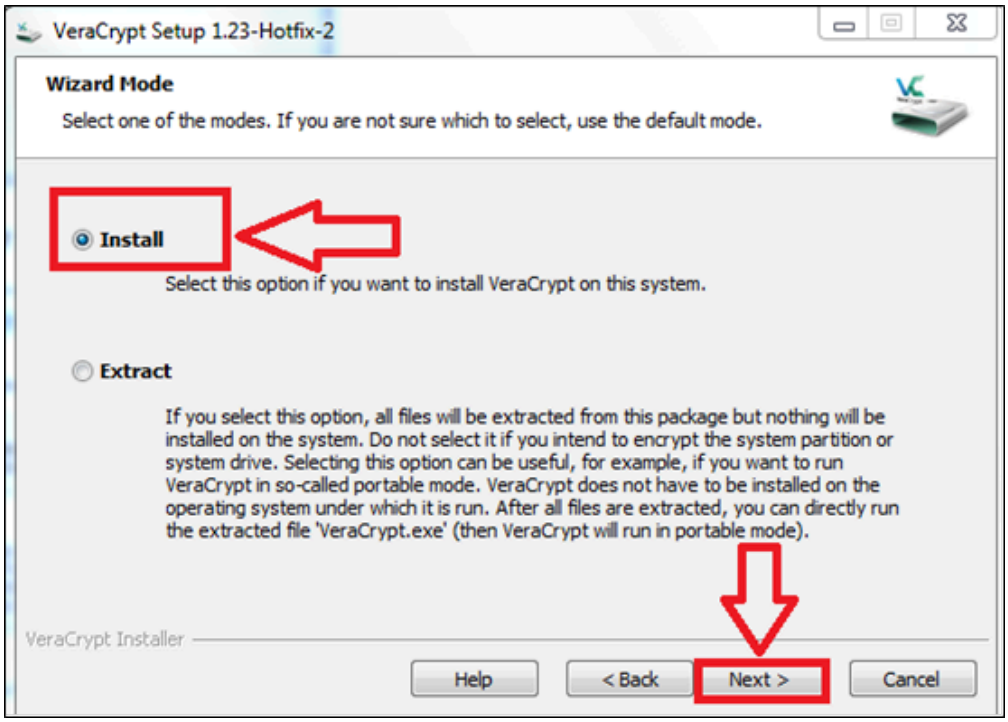
3.3. Aceite os termos e licenças marcando a caixa de aceite;



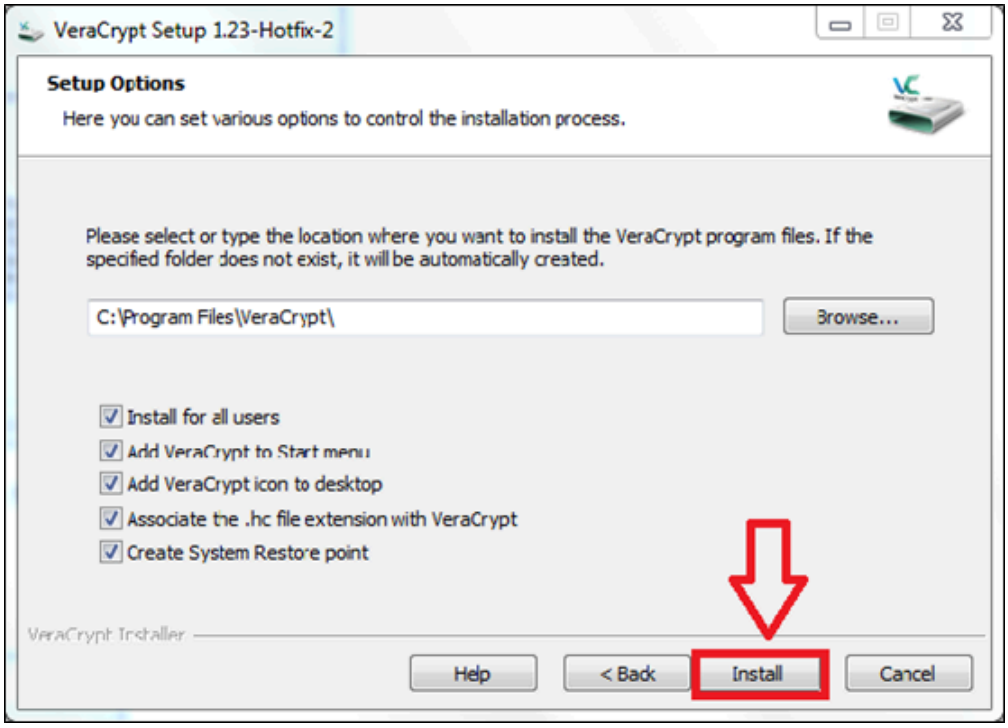
3.4. Depois, clique em "***Next***";



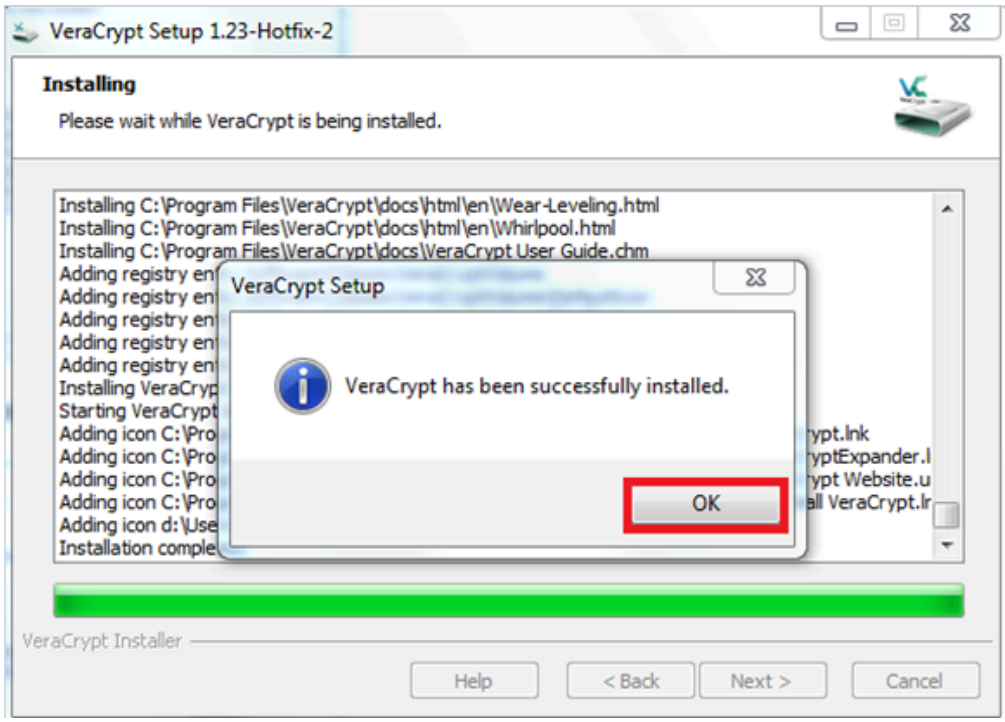
3.5. Marque a opção "***Install***" e depois clique em "***Next***";



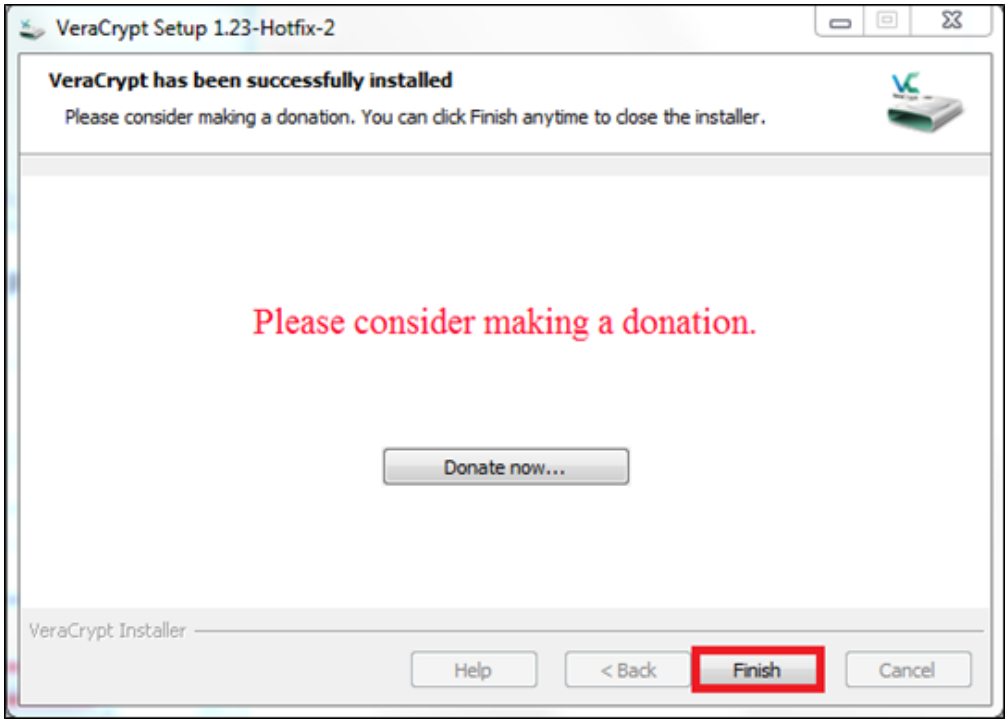
3.6. Clique em "***Install***";



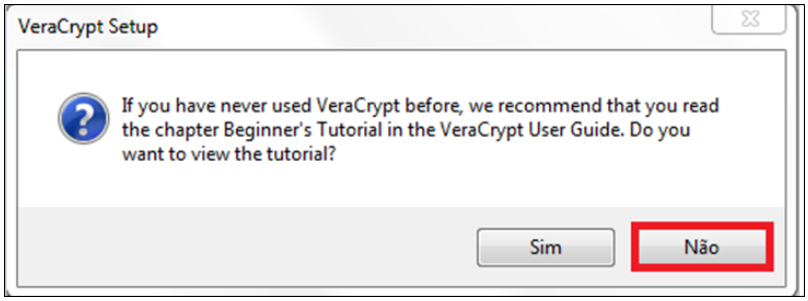
3.7. Após a instalação do programa, clique em "***OK***";



3.8. Clique em "***Finish***";



3.9. Aparecerá uma janela sugerindo o download do tutorial do "***VeraCrypt***". Clique em "***Não***";

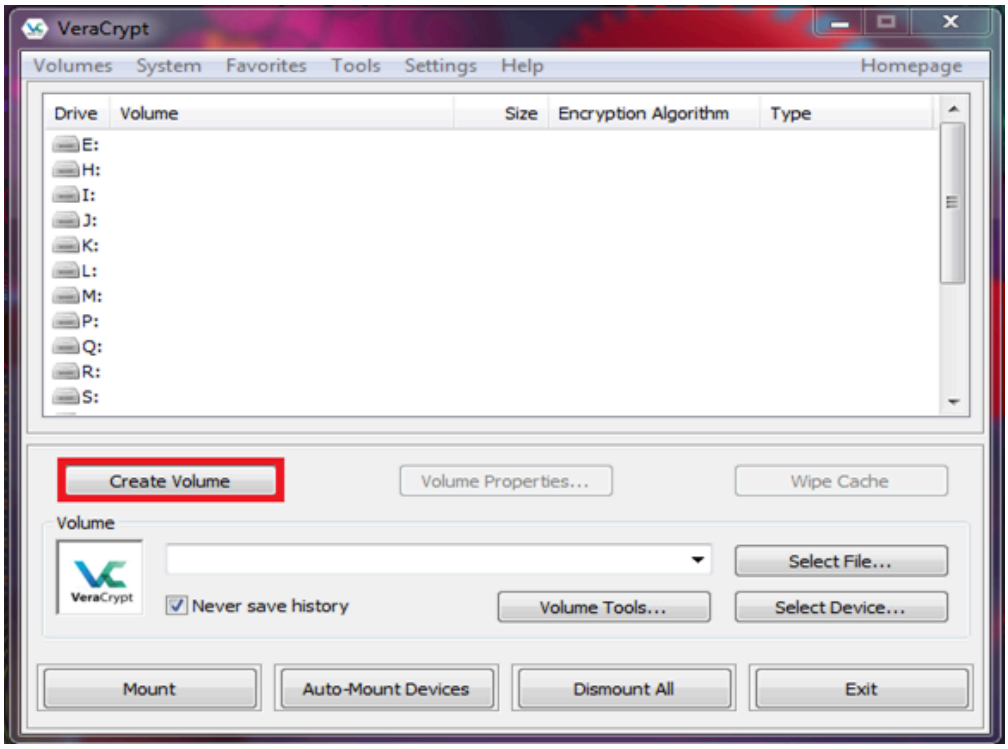


3.10. A instalação do programa foi concluída.

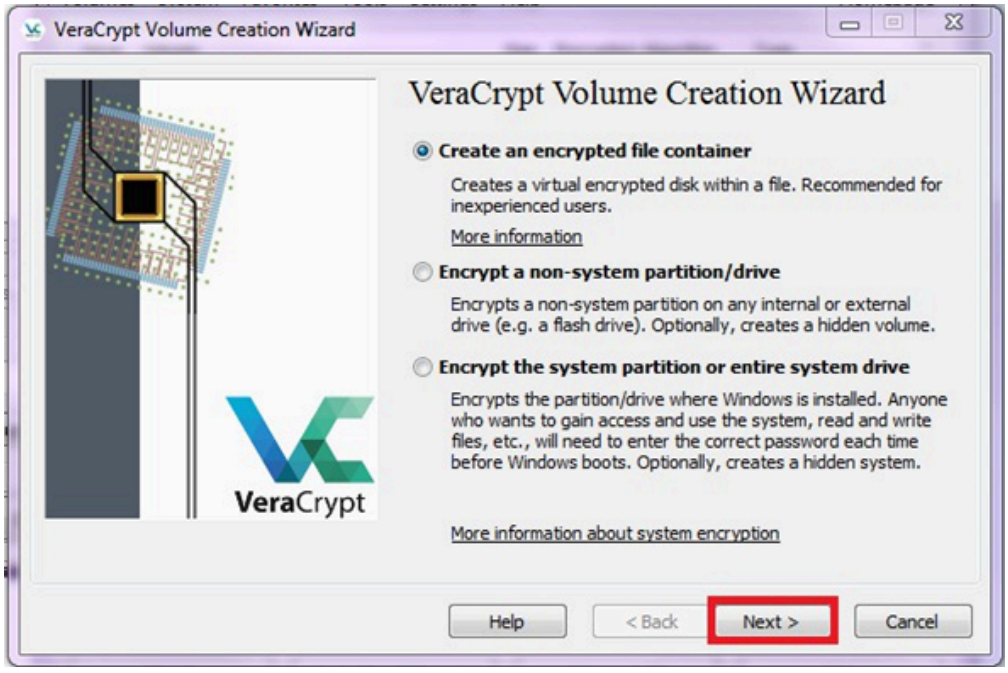
4. COMO CRIAR VOLUME/UNIDADE E INCLUSÃO DO ARQUIVO A SER CRIPTOGRAFADO

Toda vez que desejar criptografar um dado para envio, será necessário criar um volume.

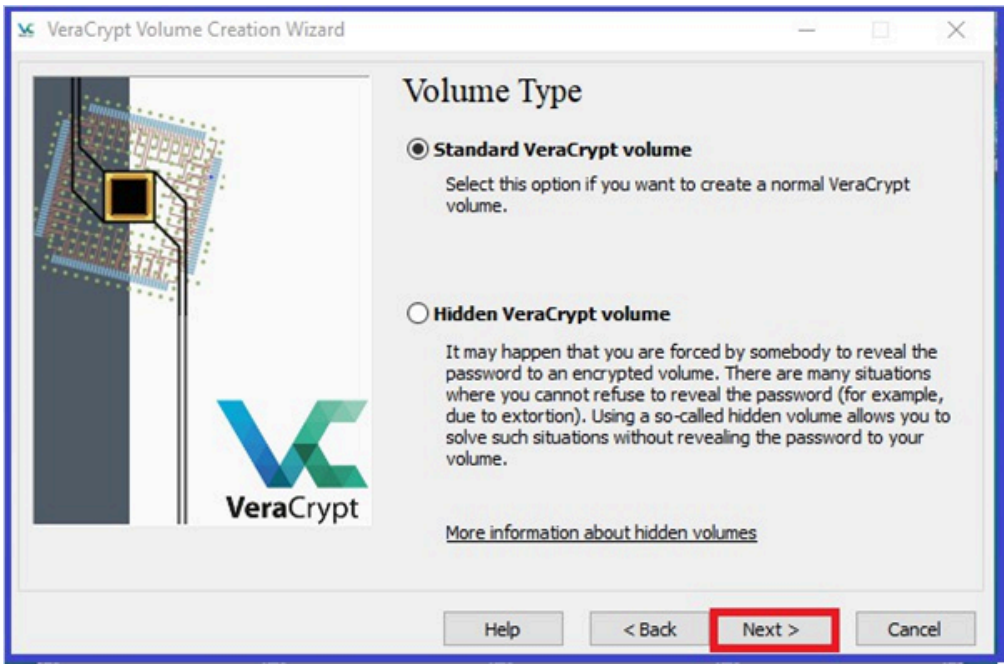
4.1. Abra o **"*Veracrypt*"** e clique em **"*Create Volume*";**



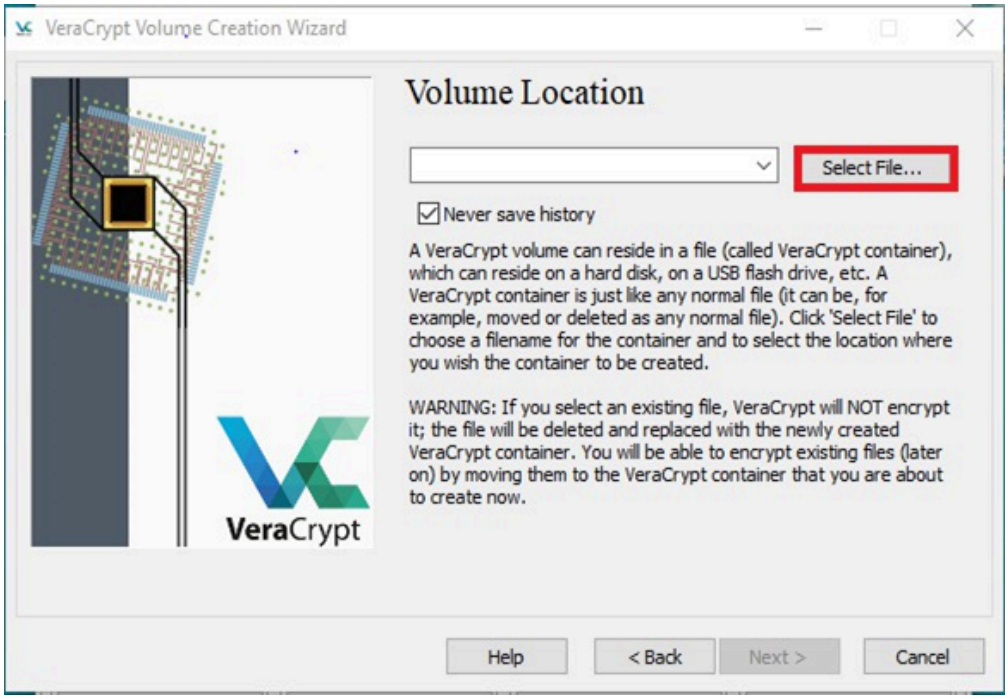
4.2. Clique em ***"Create an encrypted file container"*** e depois em "***Next***";



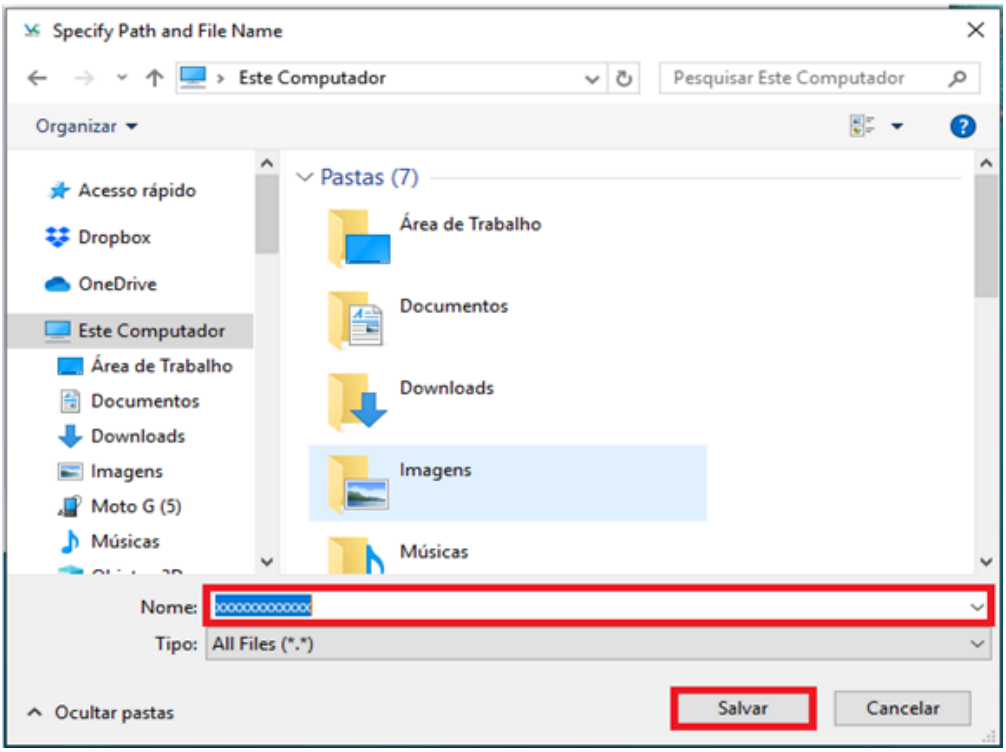
4.3. Clique em ***"Standard VeraCrypt volume"*** e depois em "***Next***";



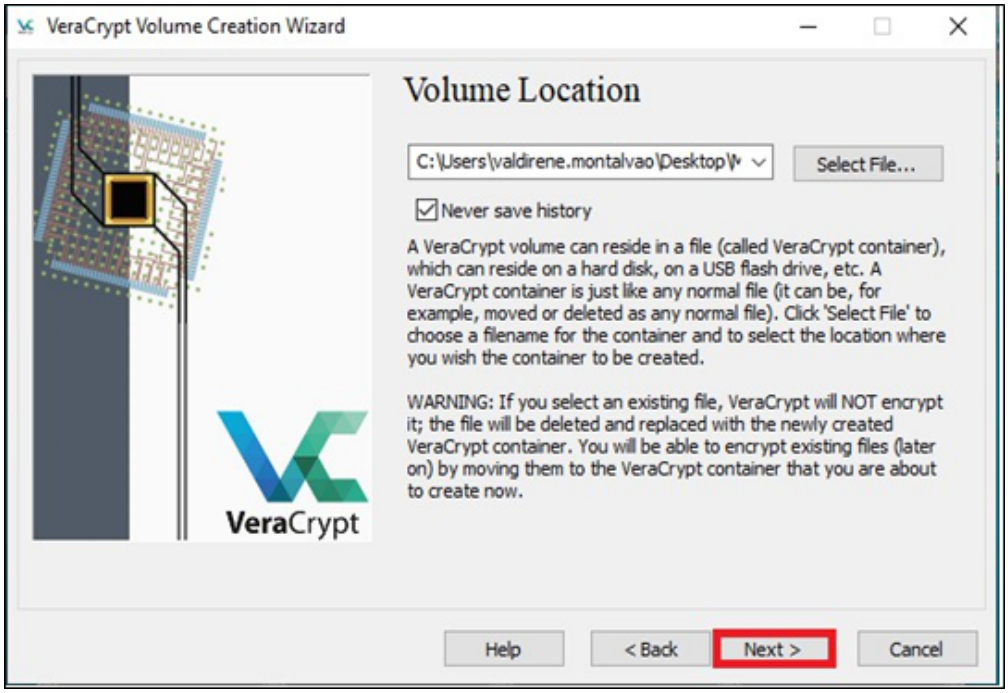
4.4. Clique em "***Select File***... ";



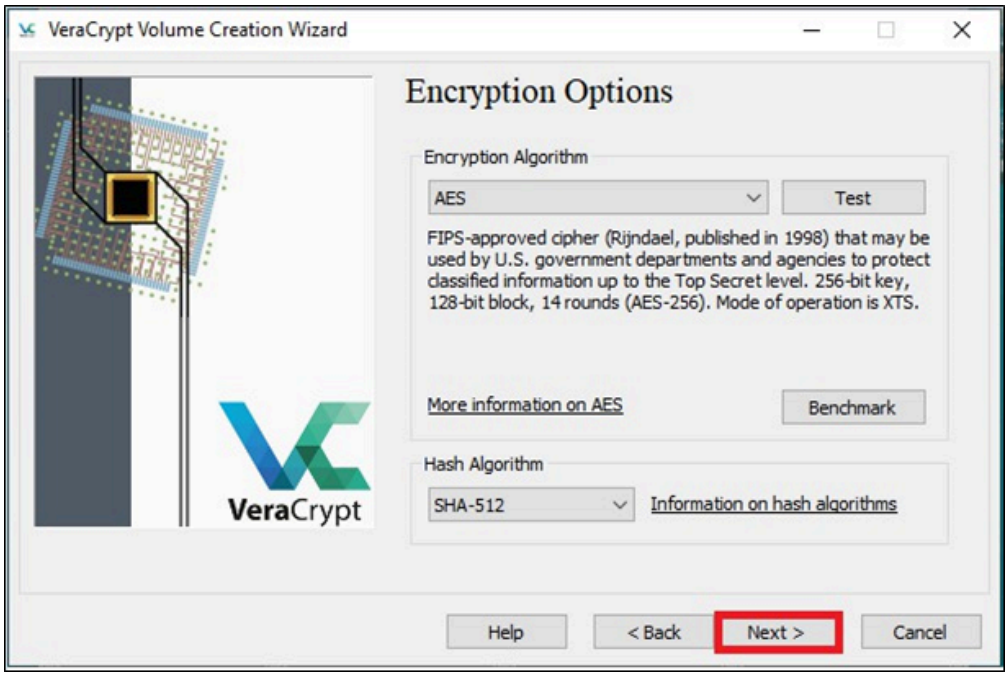
4.5. Selecione um local para salvar o volume (por exemplo: área de trabalho), crie um nome para esse volume e depois clique em "***Salvar***";



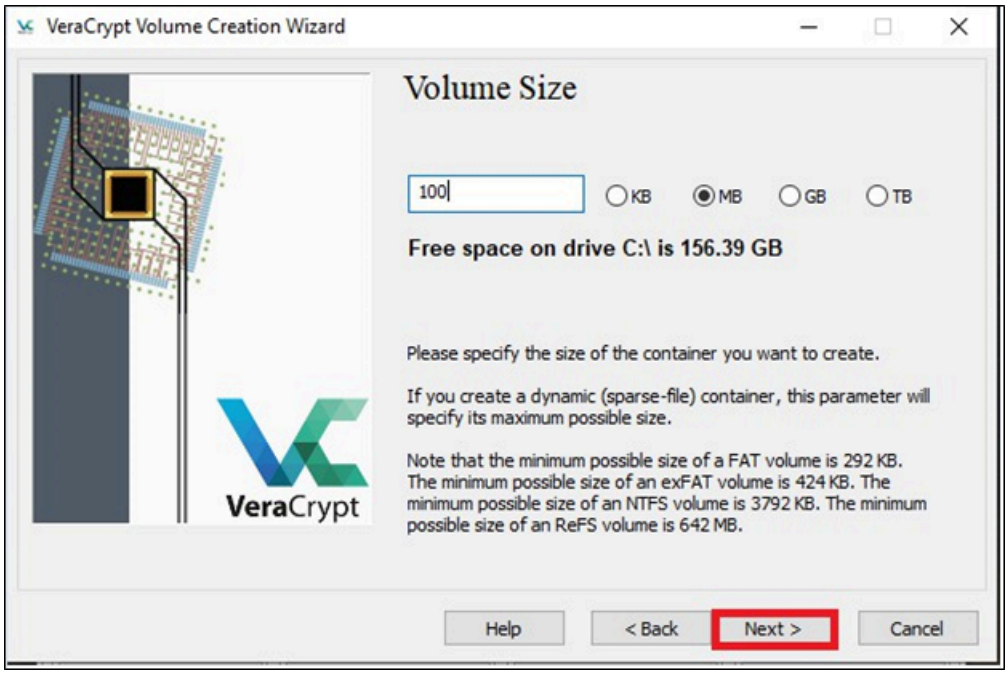
4.6. Clique em "***Next***";



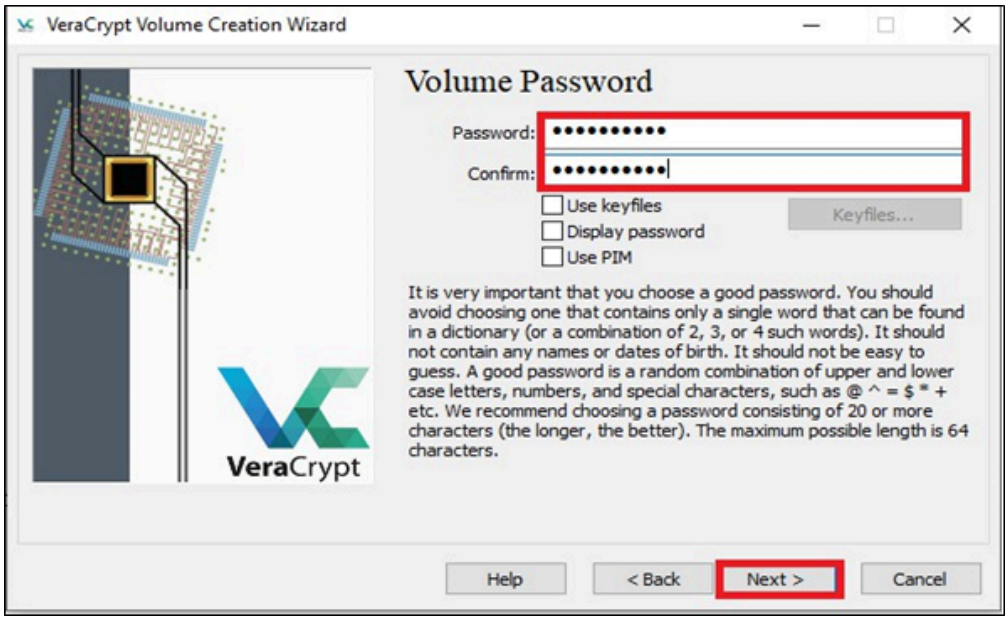
4.7. Na próxima tela chamada **"*Encryption Options*"**, clique em "***Next***";



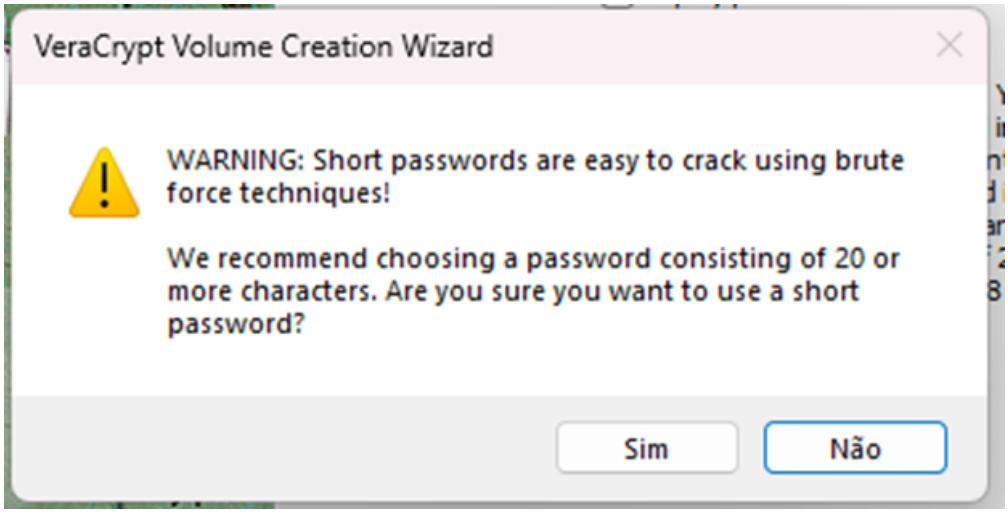
4.8. Na tela ***"Volume Size"*** escolha o tamanho da unidade que será criada. Se você pretende criptografar um arquivo de 80 MB, crie um volume maior (100 MB por exemplo). Depois clique em ***"Next"***;



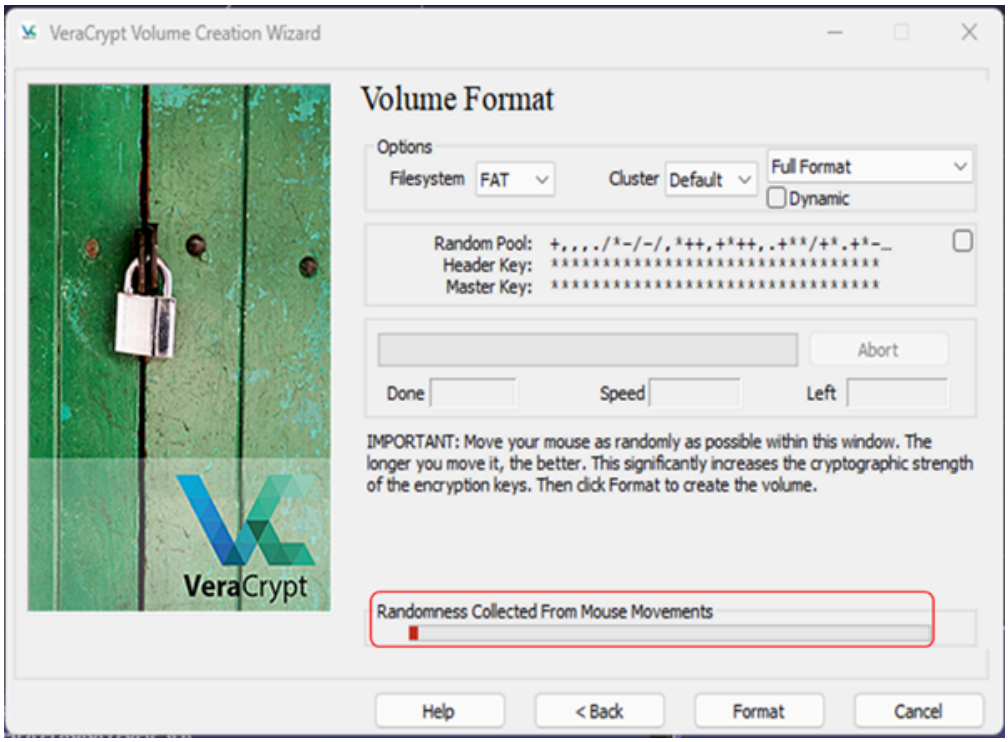
4.9. Crie uma senha de sua escolha e digite em ***"Password"*** e ***"Confirm"***. Clique em "***Next***". Existe a recomendação de que a senha seja maior do que 20 caracteres, caso sua senha seja menor que isso, existe a possibilidade de quebra da senha. Uma boa senha e a combinação aleatória entre letras maiúsculas e minúsculas, número e caracteres especiais, como @^=$+ etc;



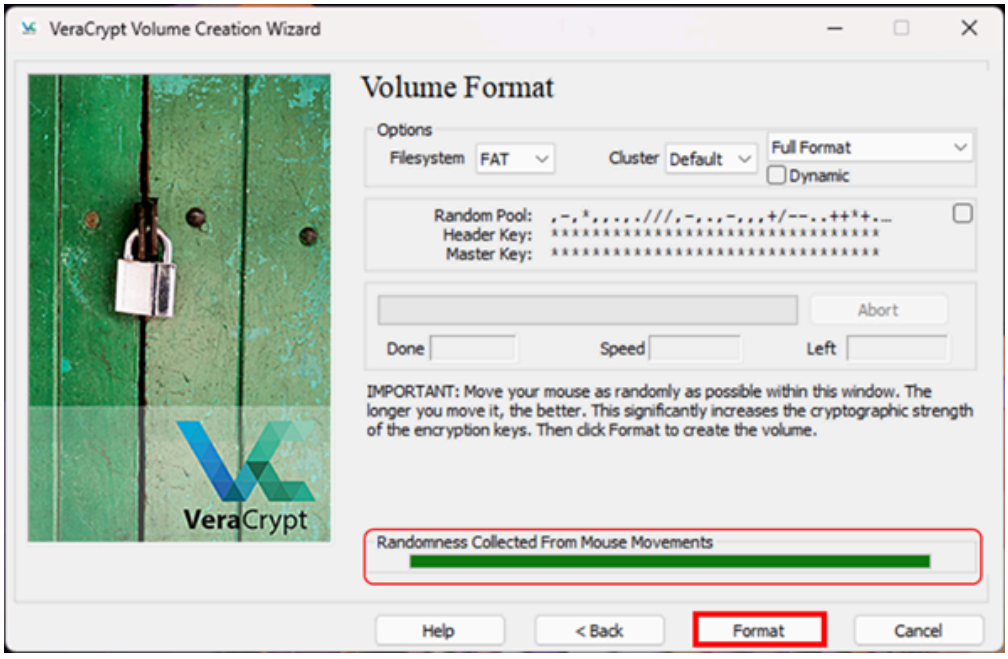
4.9.1. Caso sua senha seja menor que 20 caracteres ira aparecer uma mensagem avisando da fragilidade da senha e se deseja realmente usar uma senha curta, clique em "**não**" e aumente o tamanho da sua senha;



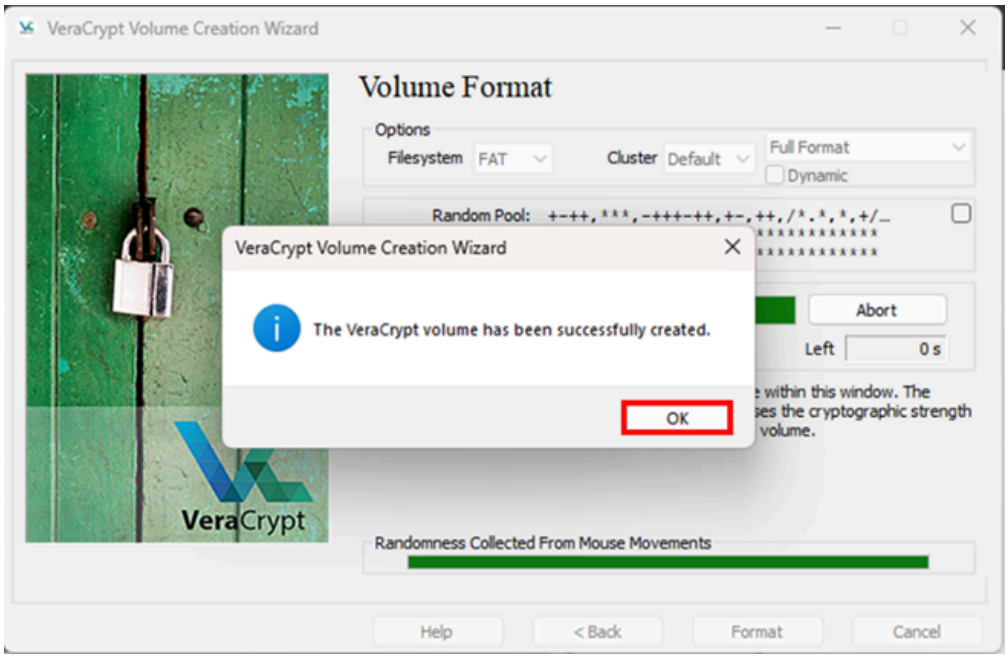
4.10. Irá abrir essa caixa, observe que o campo "***Randomness Collected From Mouse Movements***" tem uma barra de carregamento, realize movimentos circulares com o mouse em cima da tela, até terminar de preencher o campo;



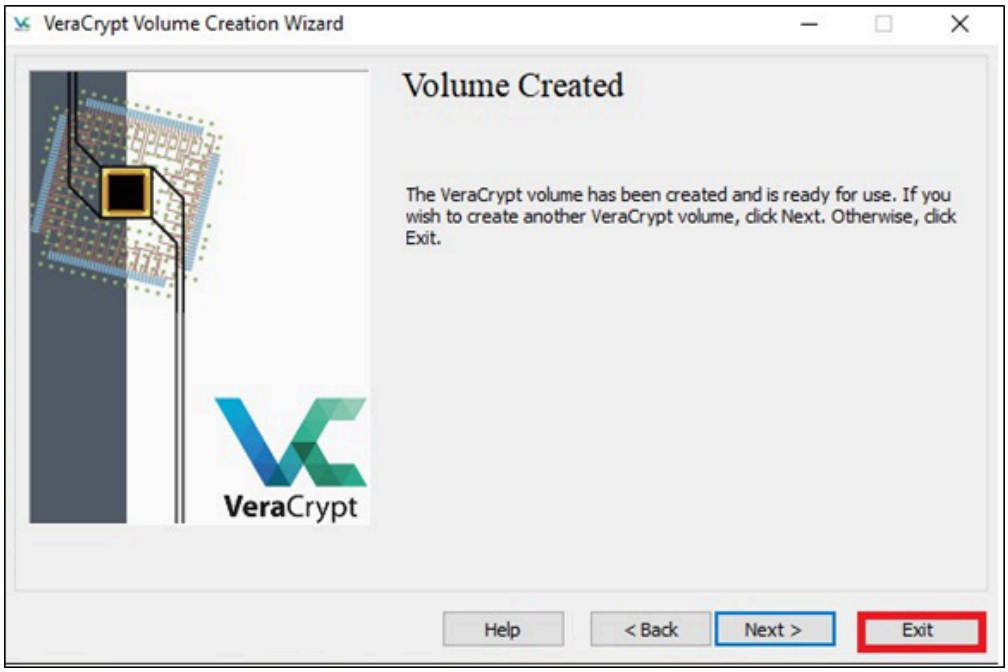
4.11. Quando a barra estiver totalmente preenchida clique em "***Format***";



4.12. Aparecerá a informação de que o arquivo foi criado com sucesso, ***"The VeraCrypt volume has been successfully created"***, clique em "***ok***";

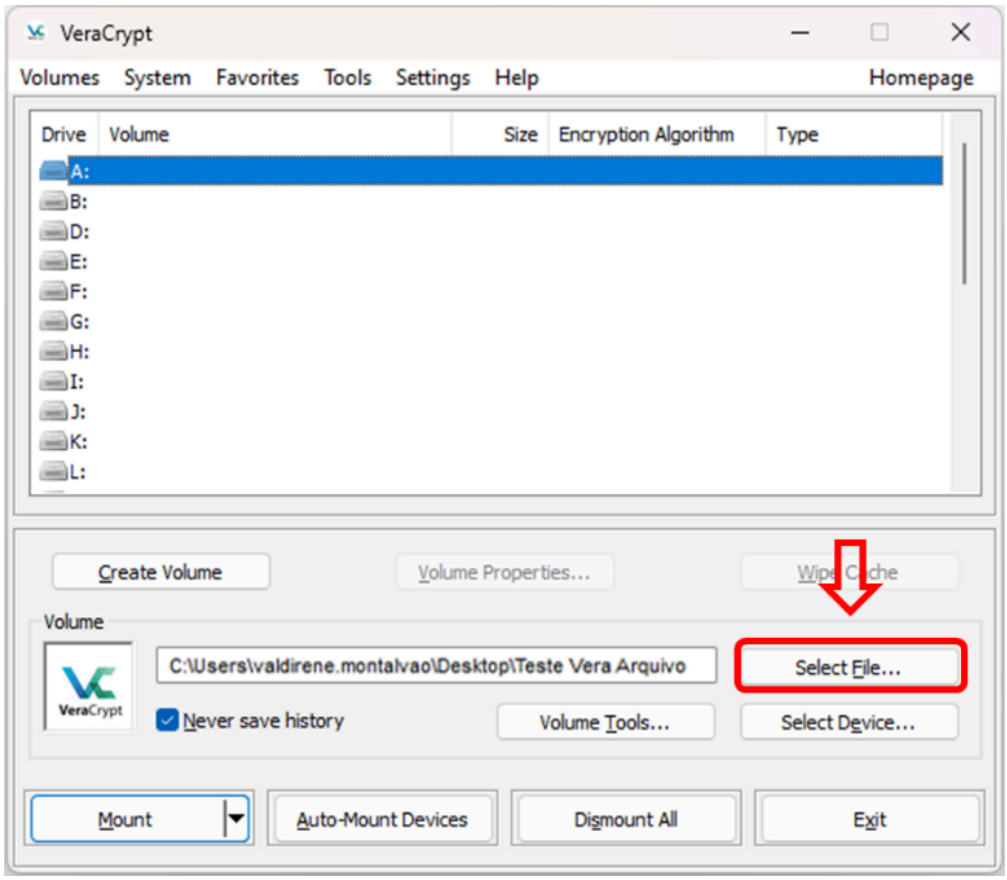


4.13. Clique em “***Exit***”.

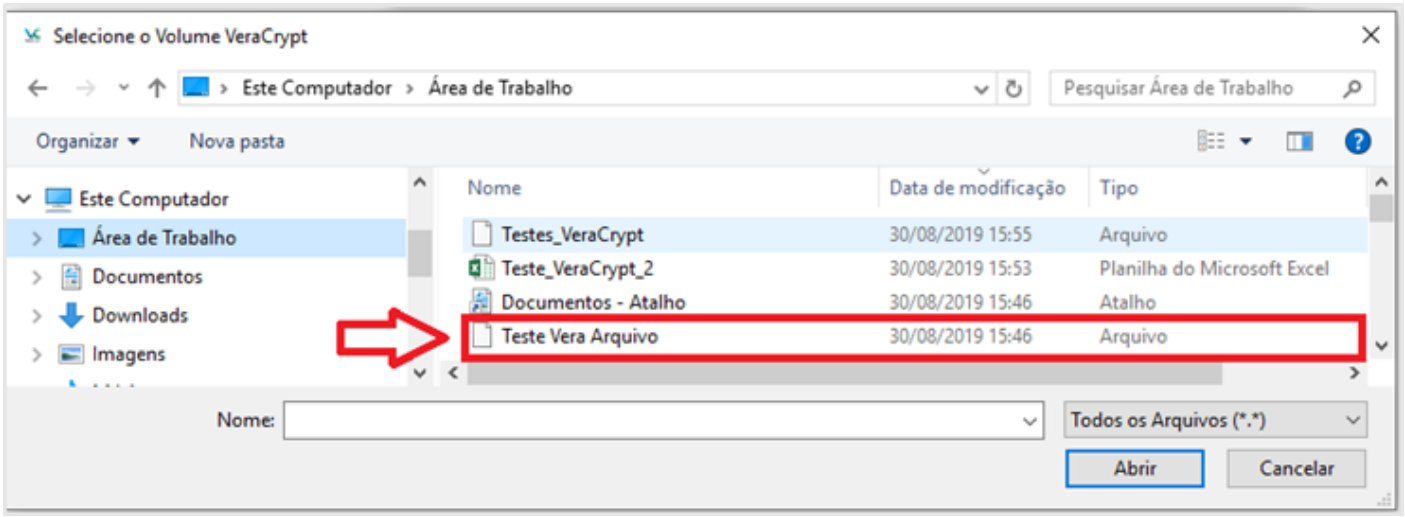


5. COMO INCLUIR O ARQUIVO A SER CRIPTOGRAFADO NO VOLUME/UNIDADE CRIADA ANTERIORMENTE

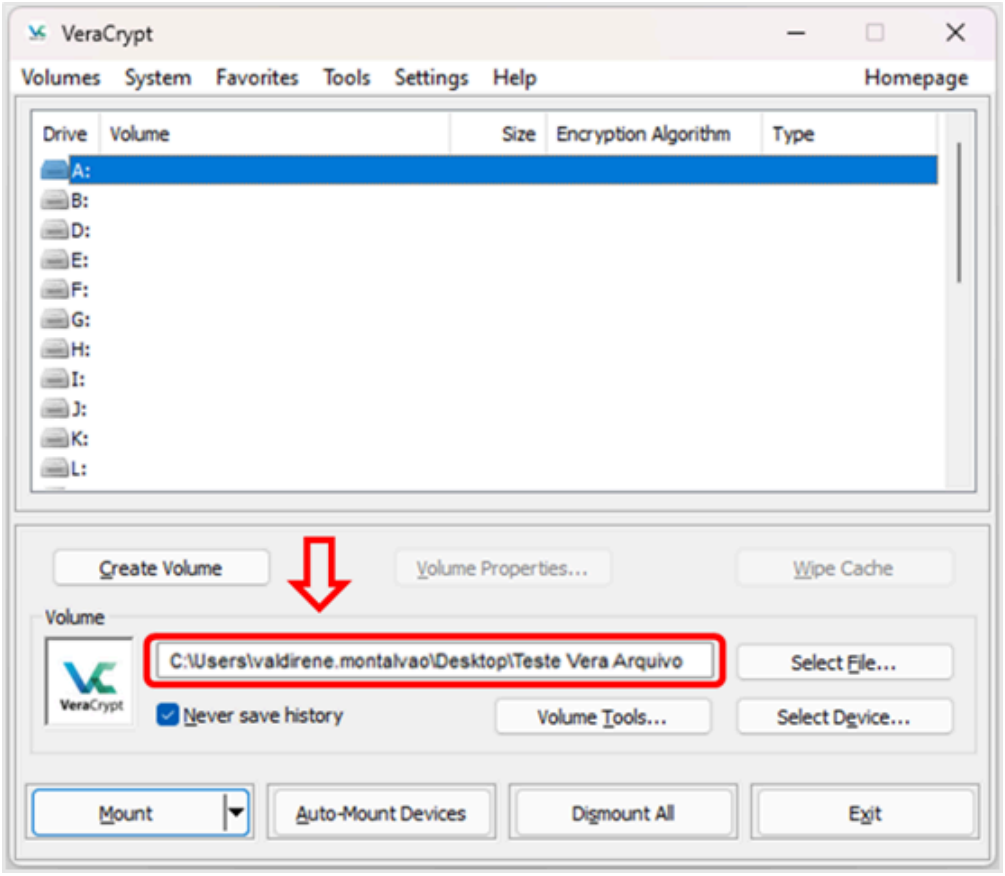
5.1. Abra o VeraCrypt e clique em “***Select File***”;



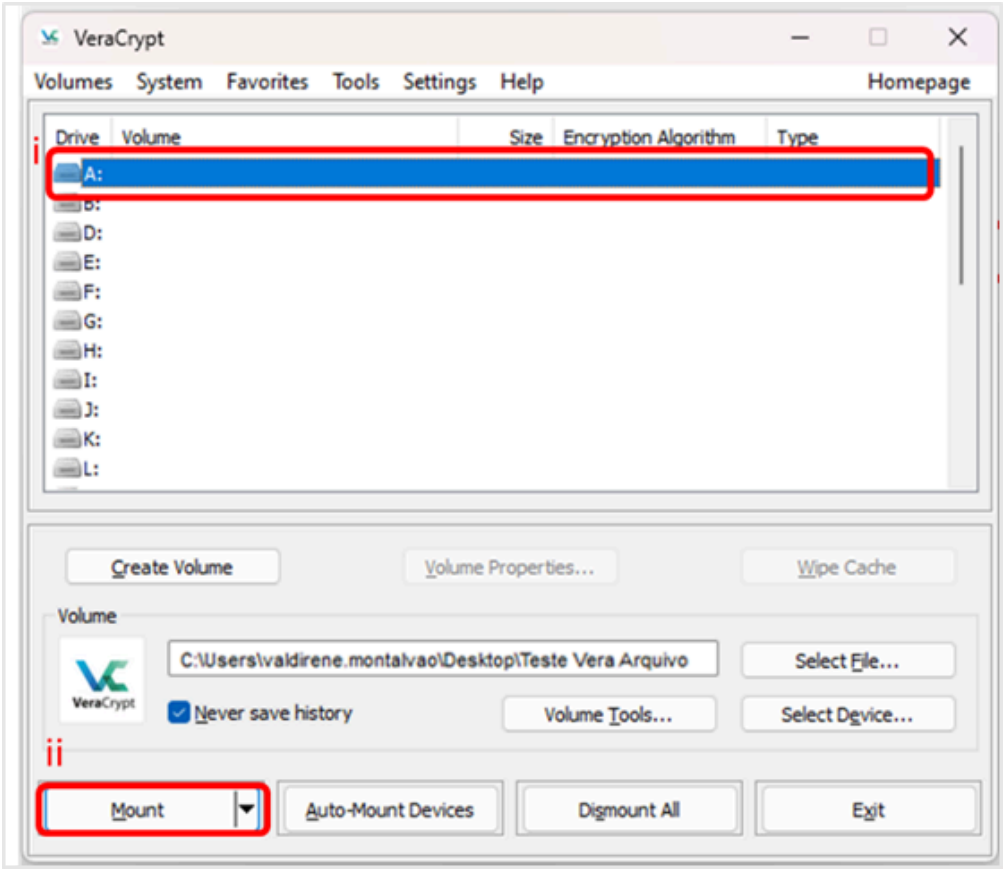
5.2. Localize o volume criado anteriormente, no exemplo abaixo o volume se chama **"Teste Vera Arquivo"**. Clique duas vezes sobre o arquivo;



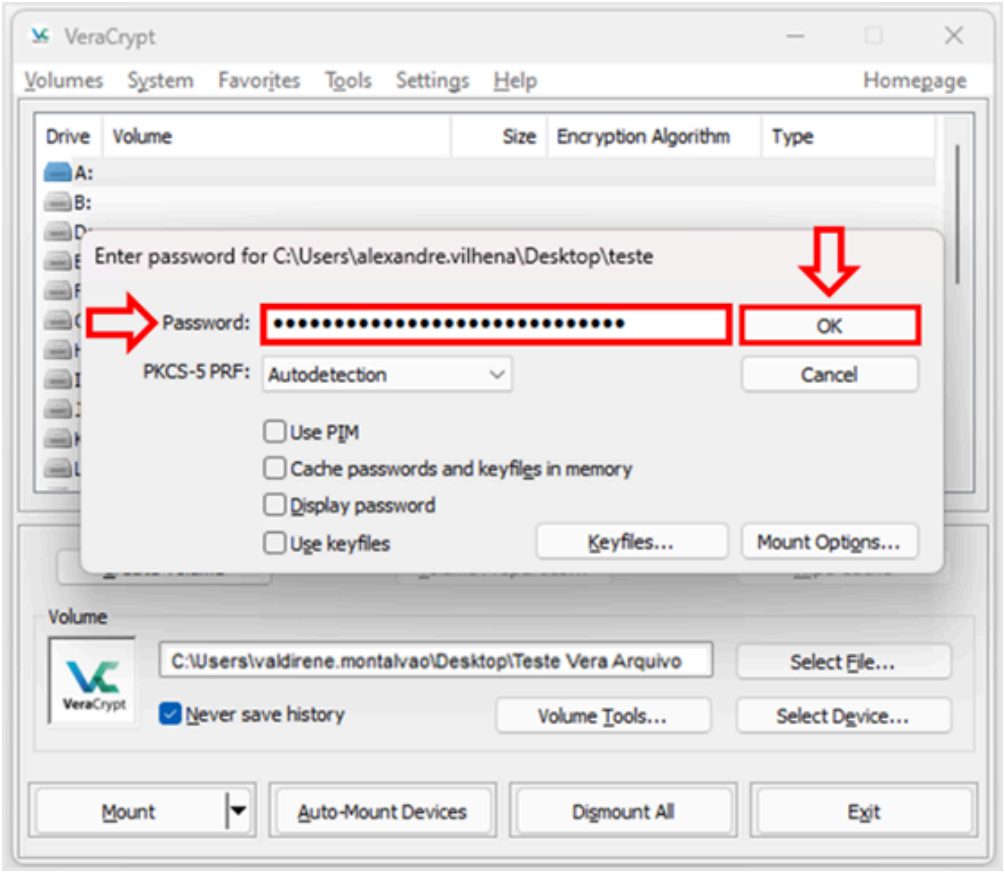
5.3. O volume será carregado na janela do Veracrypt;



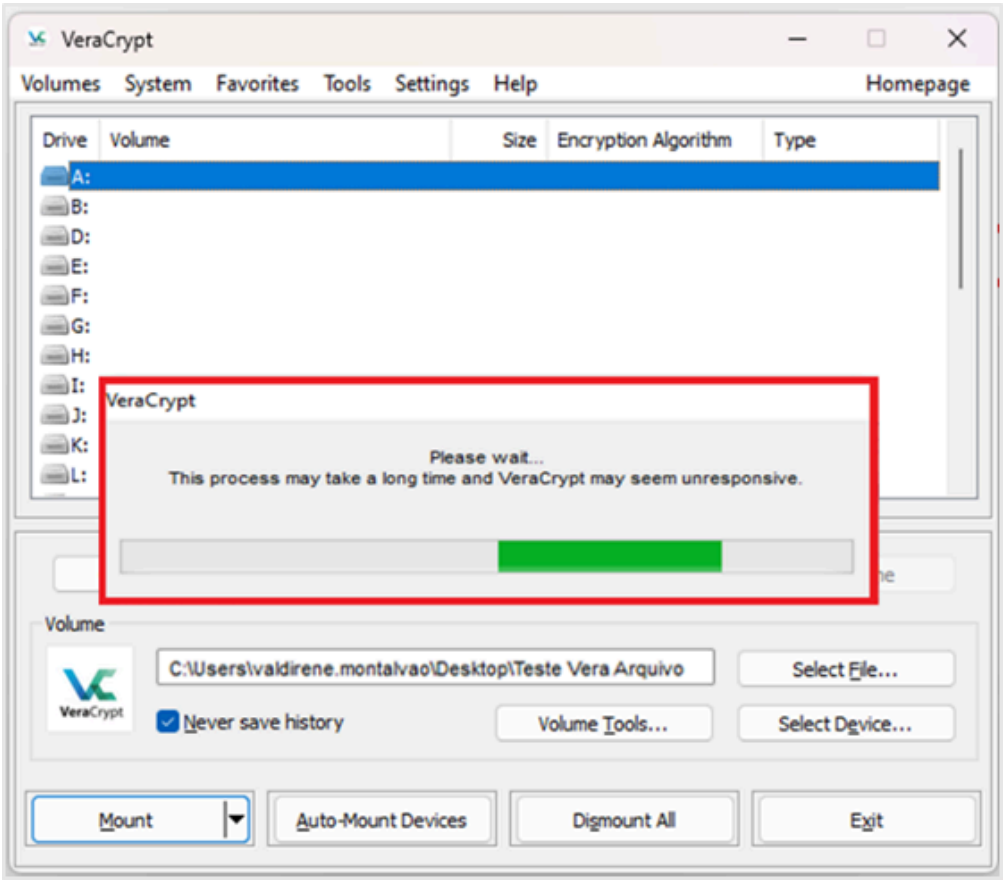
5.4. Selecione um diretório para colocar o volume criptografado, por exemplo "***Drive A***". Para rezalizar a seleção do diretório clique duas vezes sobre o diretório "***Drive A***" ou clique uma vez em "***Drive A***" e depois em "***Mount***";



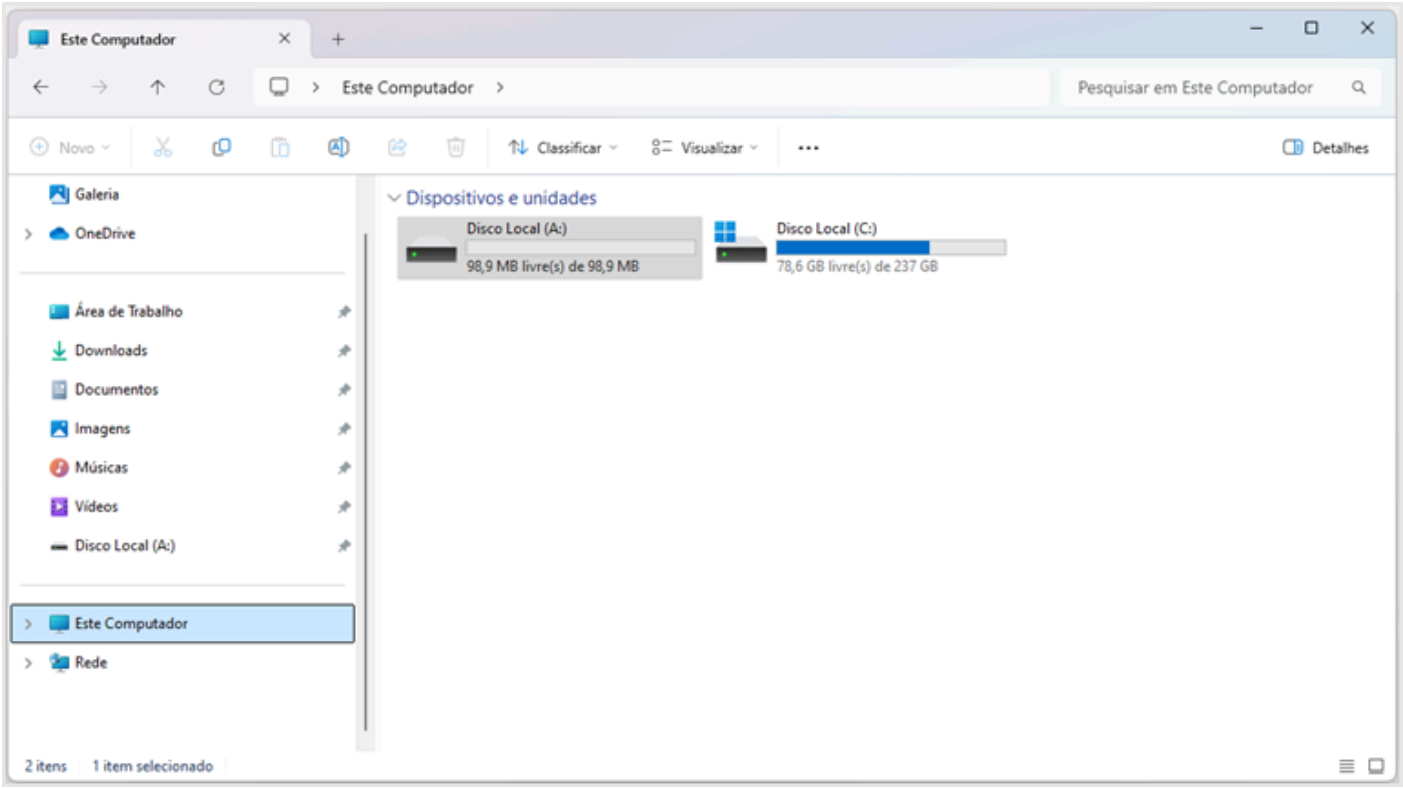
5.5. Digite a senha criada anteriormente e clique em "***OK***";



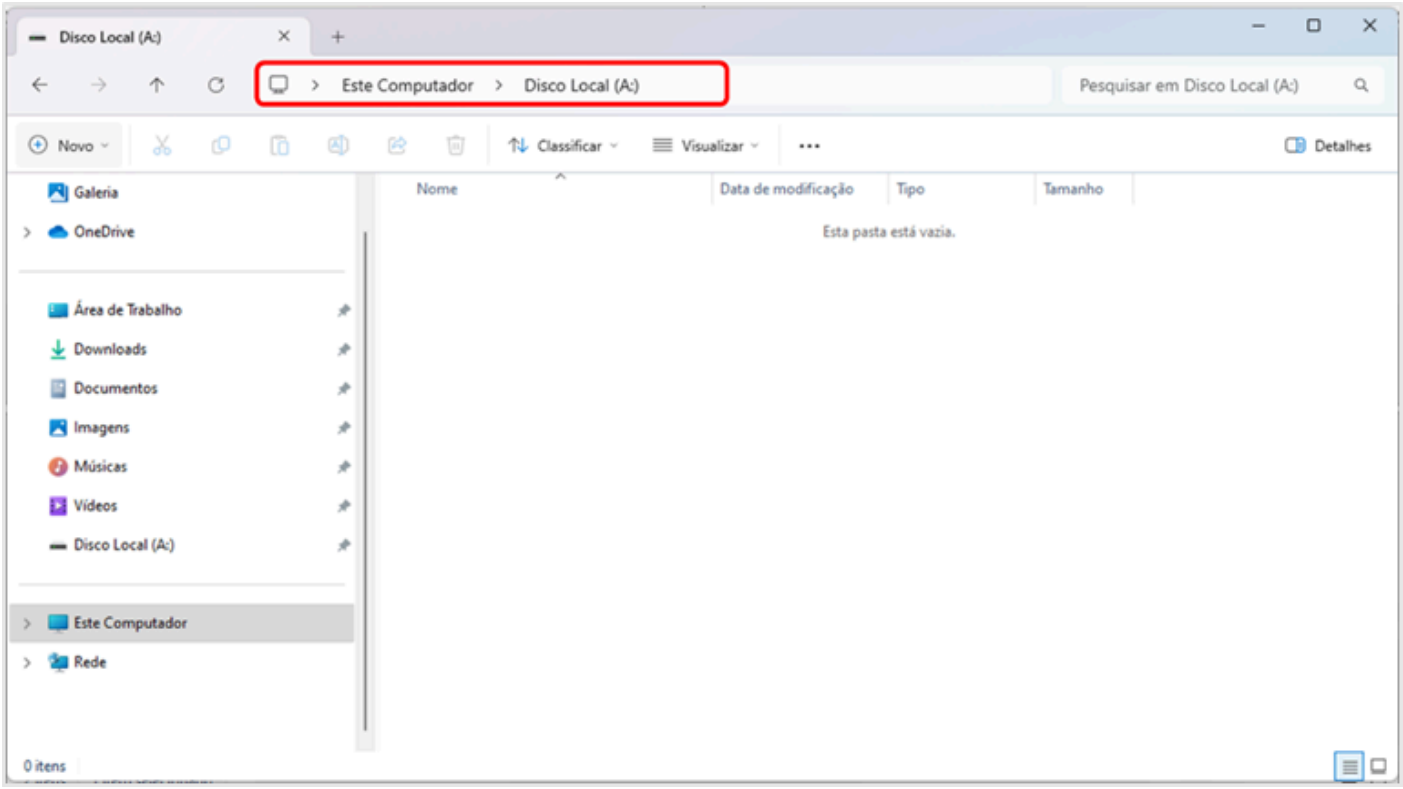
5.6. Aguarde o processamento;



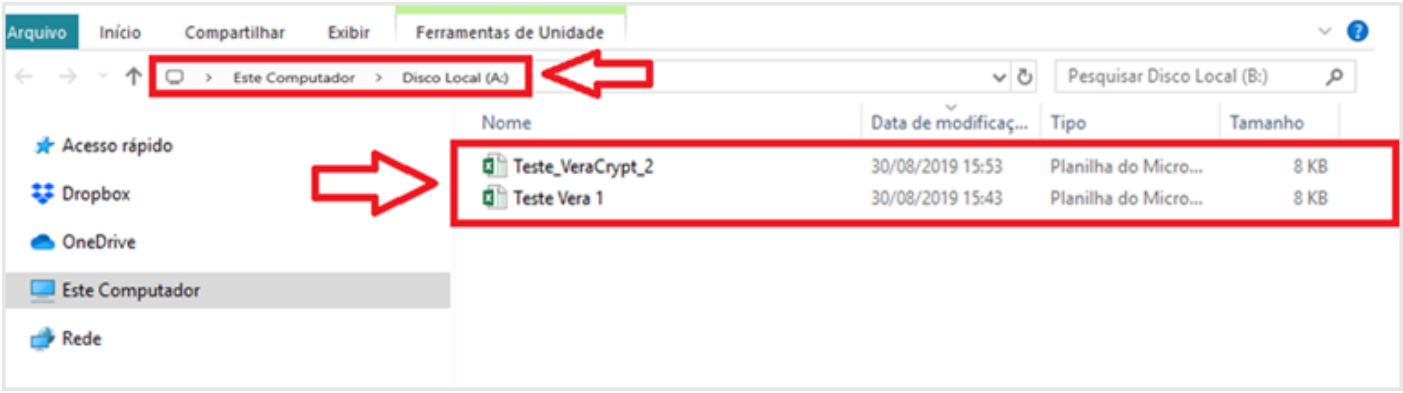
5.7. Abra o explorador de arquivos do computador, clique em "***Este Computador***". Neste local será possível localizar o diretório criado anteriormente;



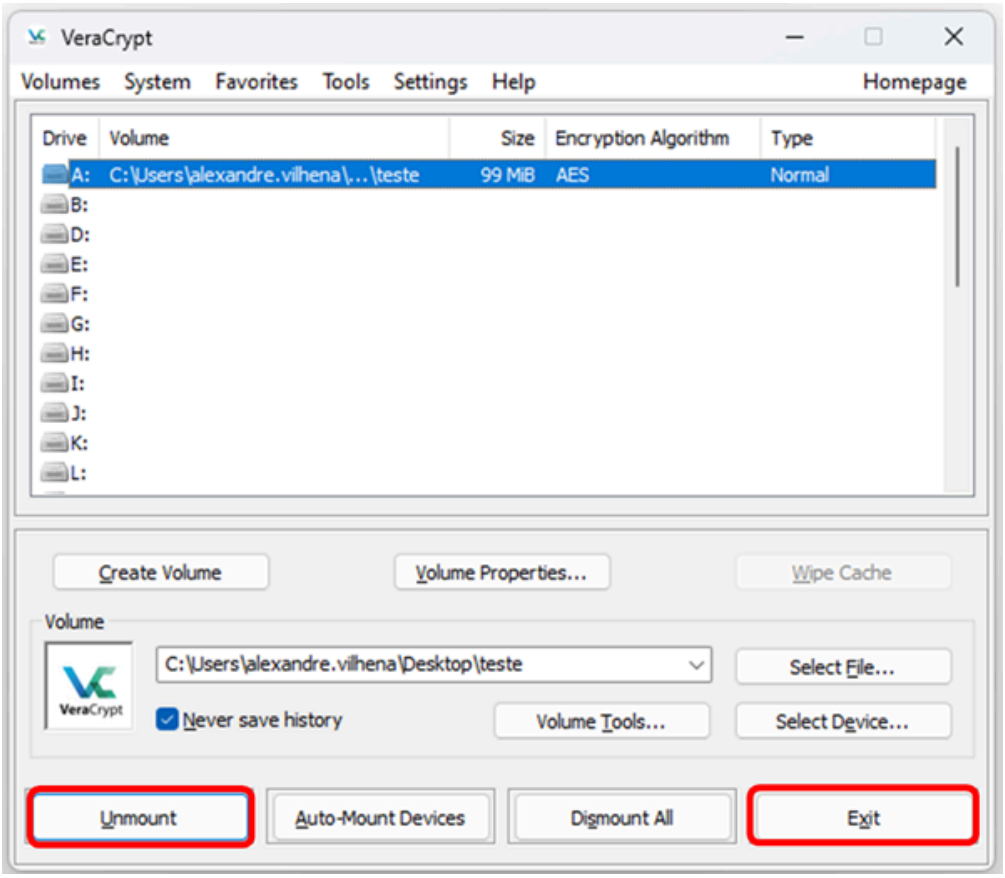
5.8. Abra o disco criado (Ex: "***Drive A:***") note que ele está vazio;



5.9. Cole os arquivos que pretende criptografar dentro do diretório (Ex. "***Drive A:"***);



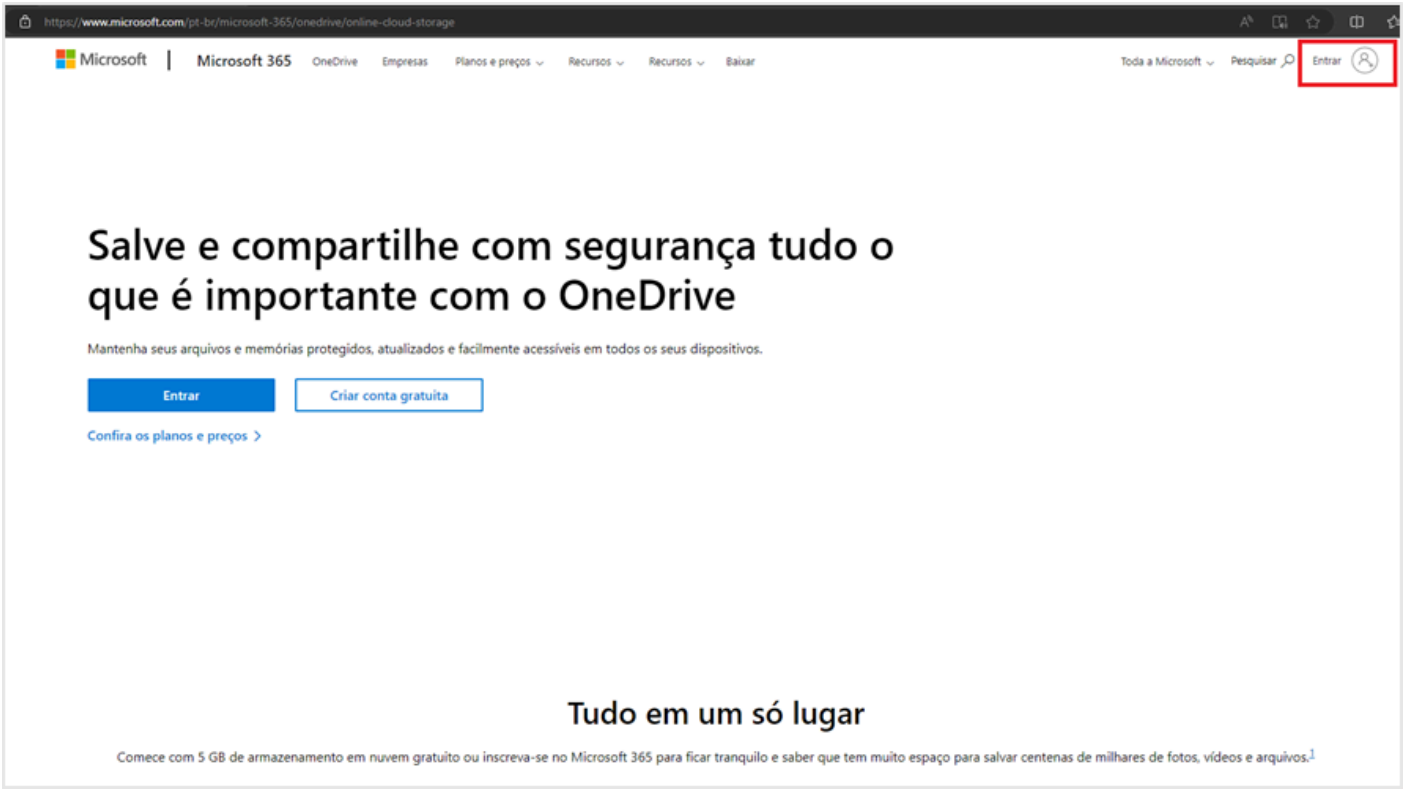
5.10. Na tela do VeraCrypt clique em "***unmount***", para que este diretório seja fechado, e posteriormente clique em "***Exit***".



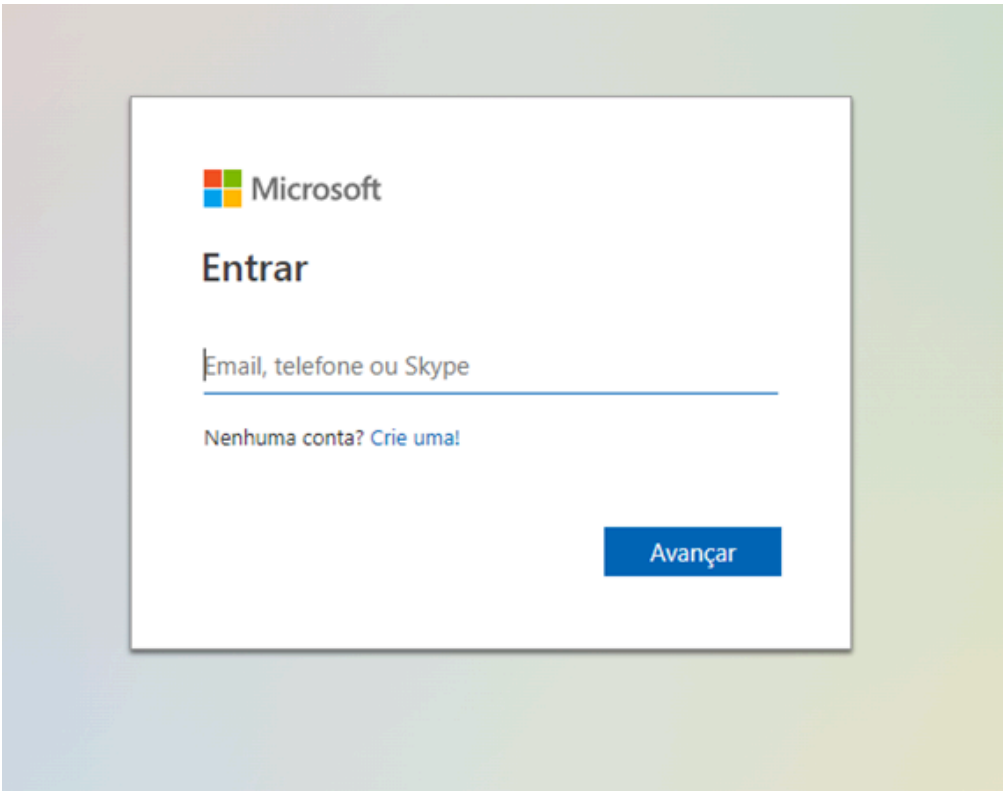
6. **COMO ENVIAR O ARQUIVO CRIPTOGRAFADO POR LINK RESTRITO NO ONEDRIVE**

6.1. Acesse o site: Armazenamento em nuvem pessoal – Microsoft OneDrive

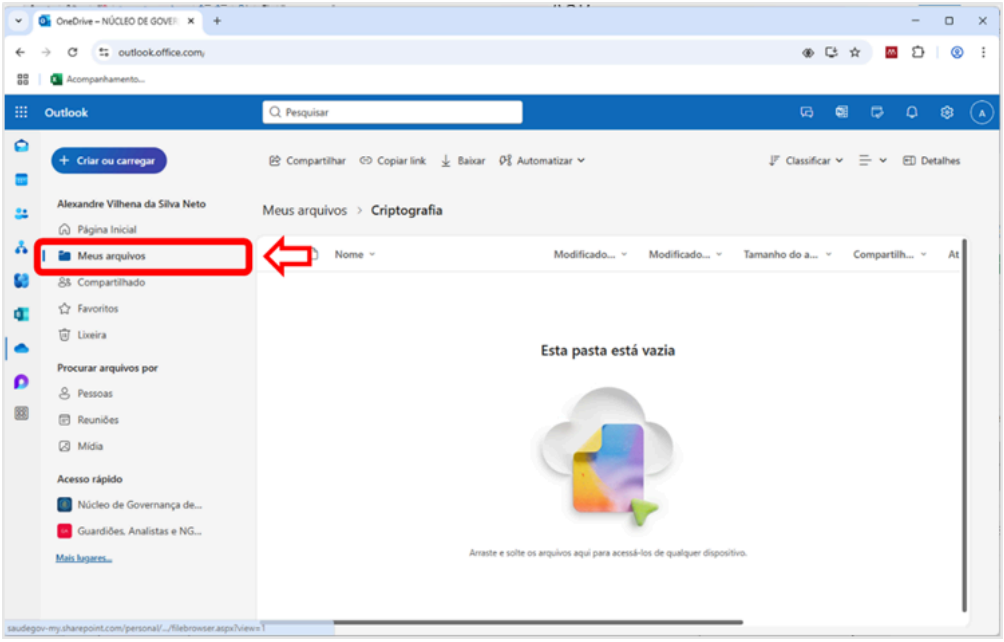
6.2. Clique no menu "**Entrar**" no canto superior direito da página;



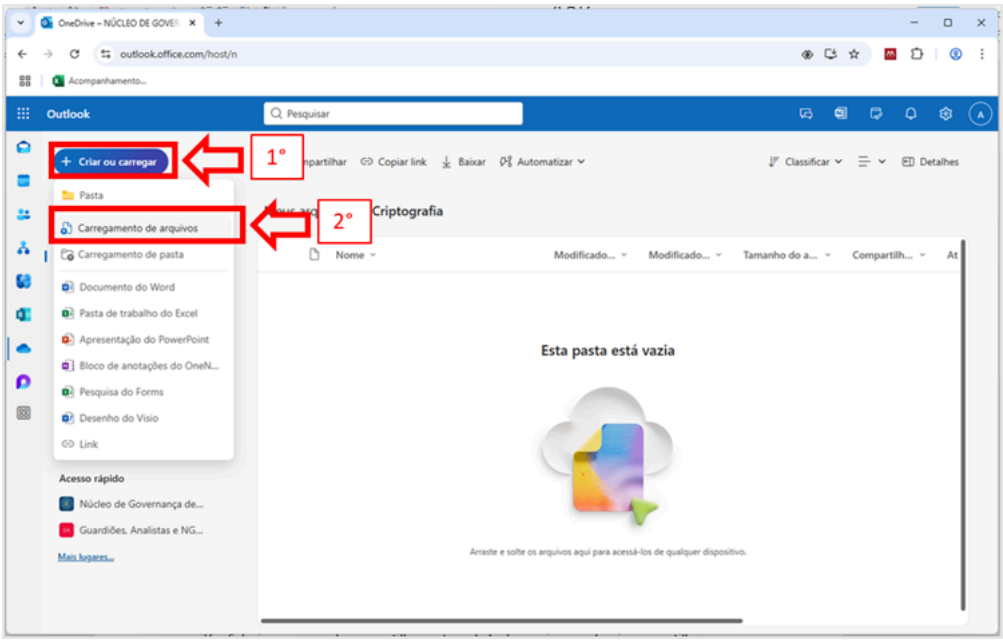
6.3. Realize o login com o seu e-mail e senha (institucional);



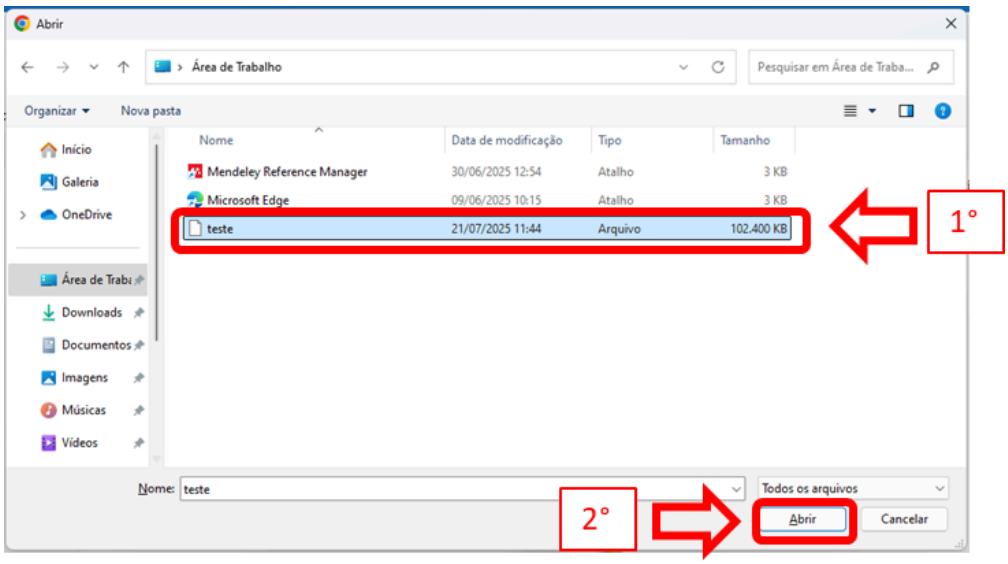
6.4. No lado esquerdo clique em "**Meus arquivos**";



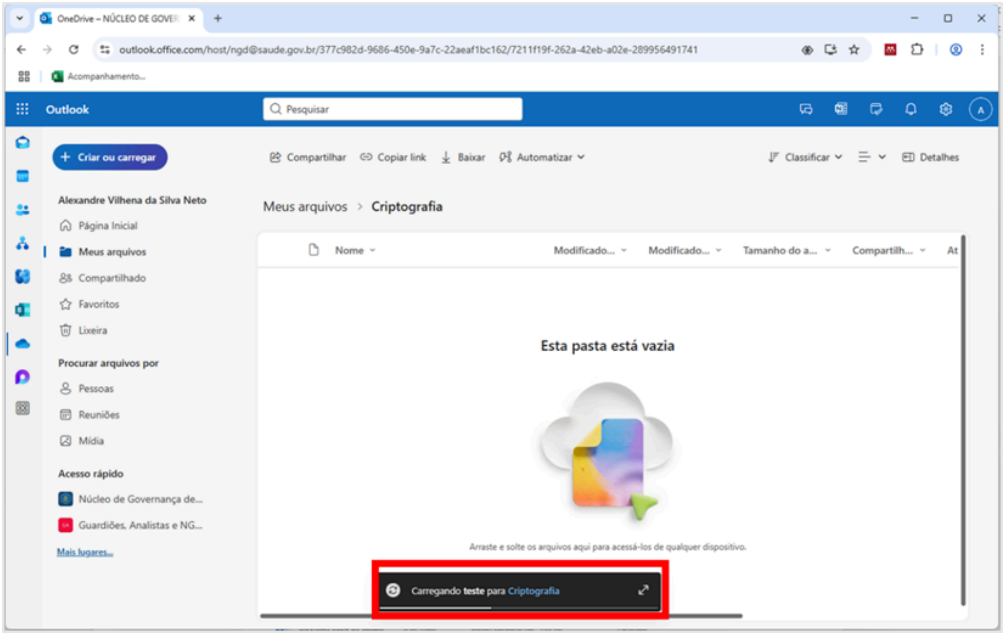
6.5. Faça o upload do arquivo criptografado no drive, clicando em "***Criar ou carregar***", e depois em "***carregamento de arquivo***";



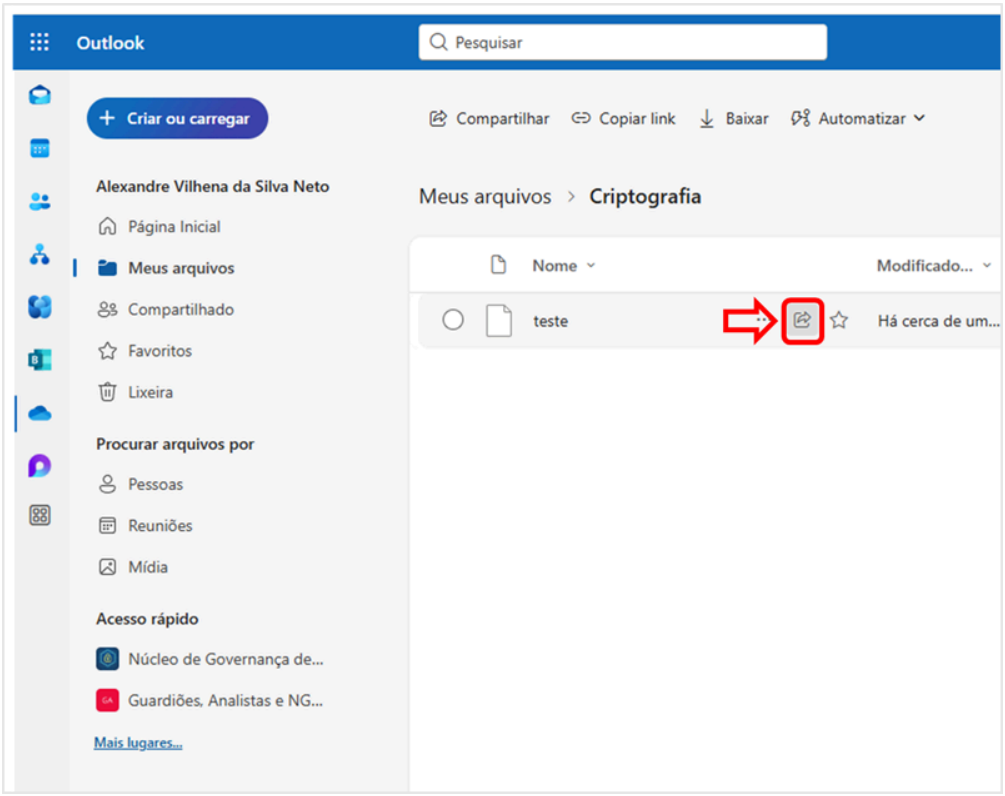
6.6. Selecione o arquivo criptografado e seguida em "***Abrir***";



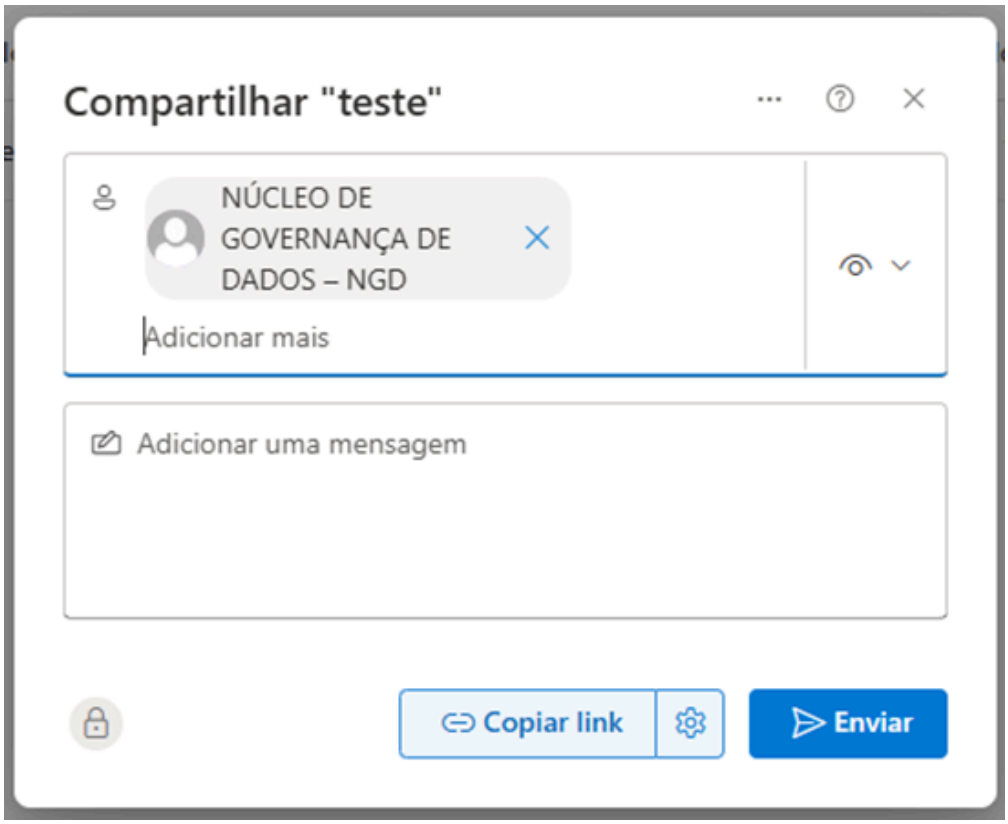
6.7. O arquivo será carregado;



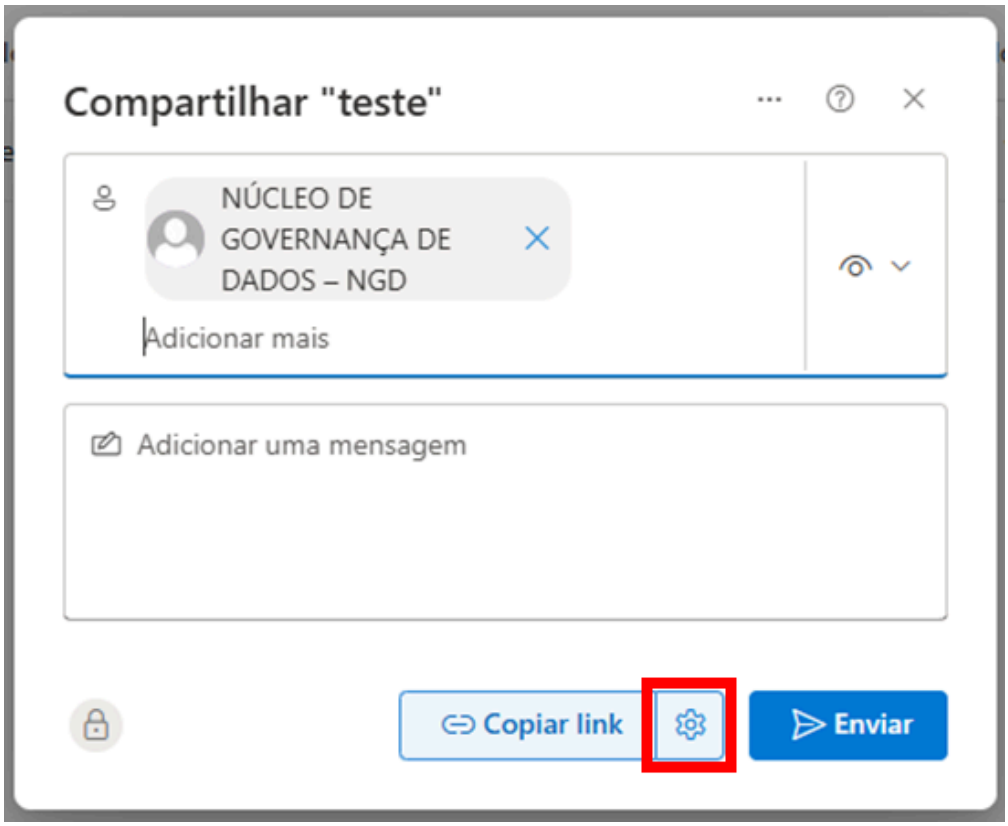
6.8. Selecione o menu de compartilhamento ao lado do arquivo que deseja compartilhar;



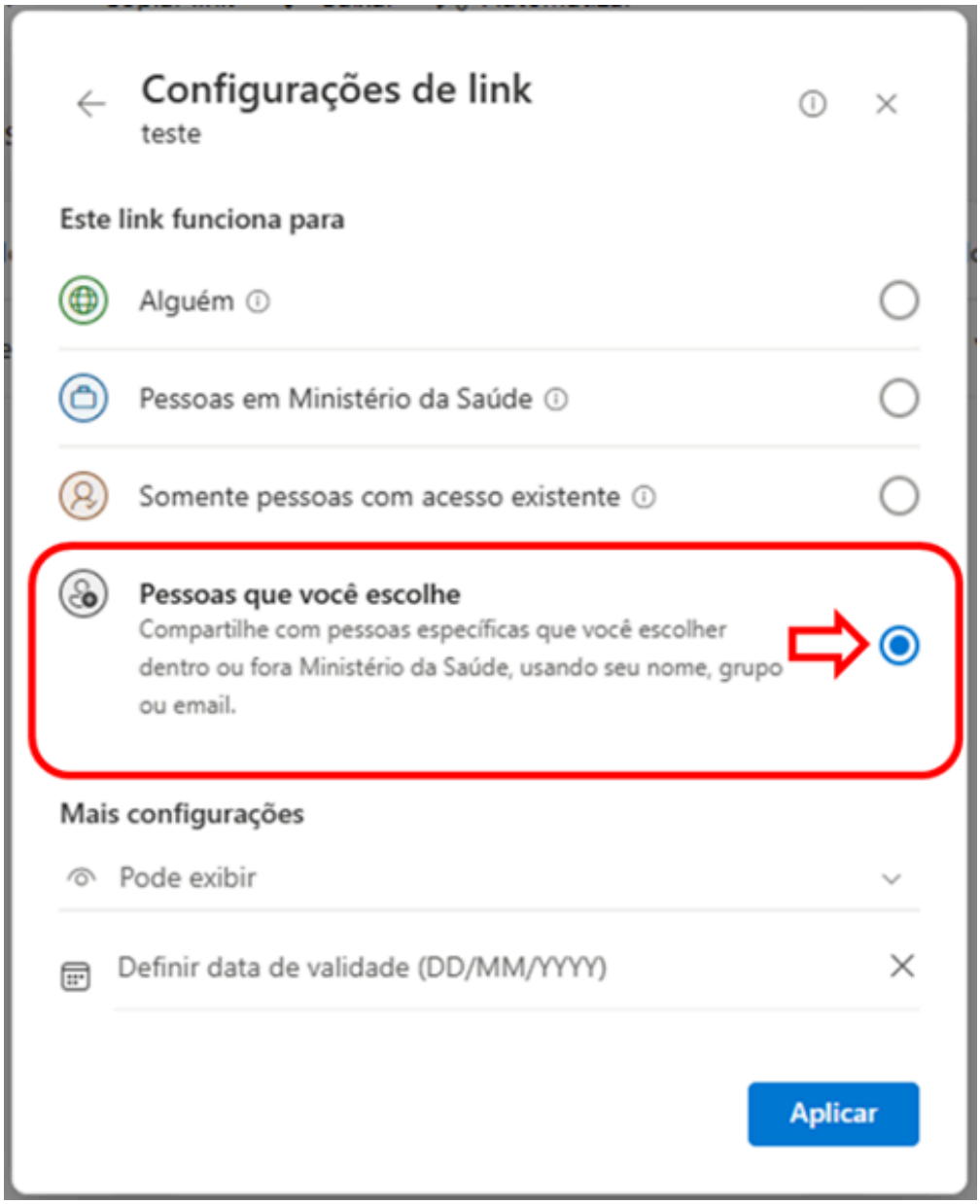
6.9. Irá aparecer em sua tela. Adicione o e-mail da(s) pessoa(s) que deseja compartilhar o arquivo;



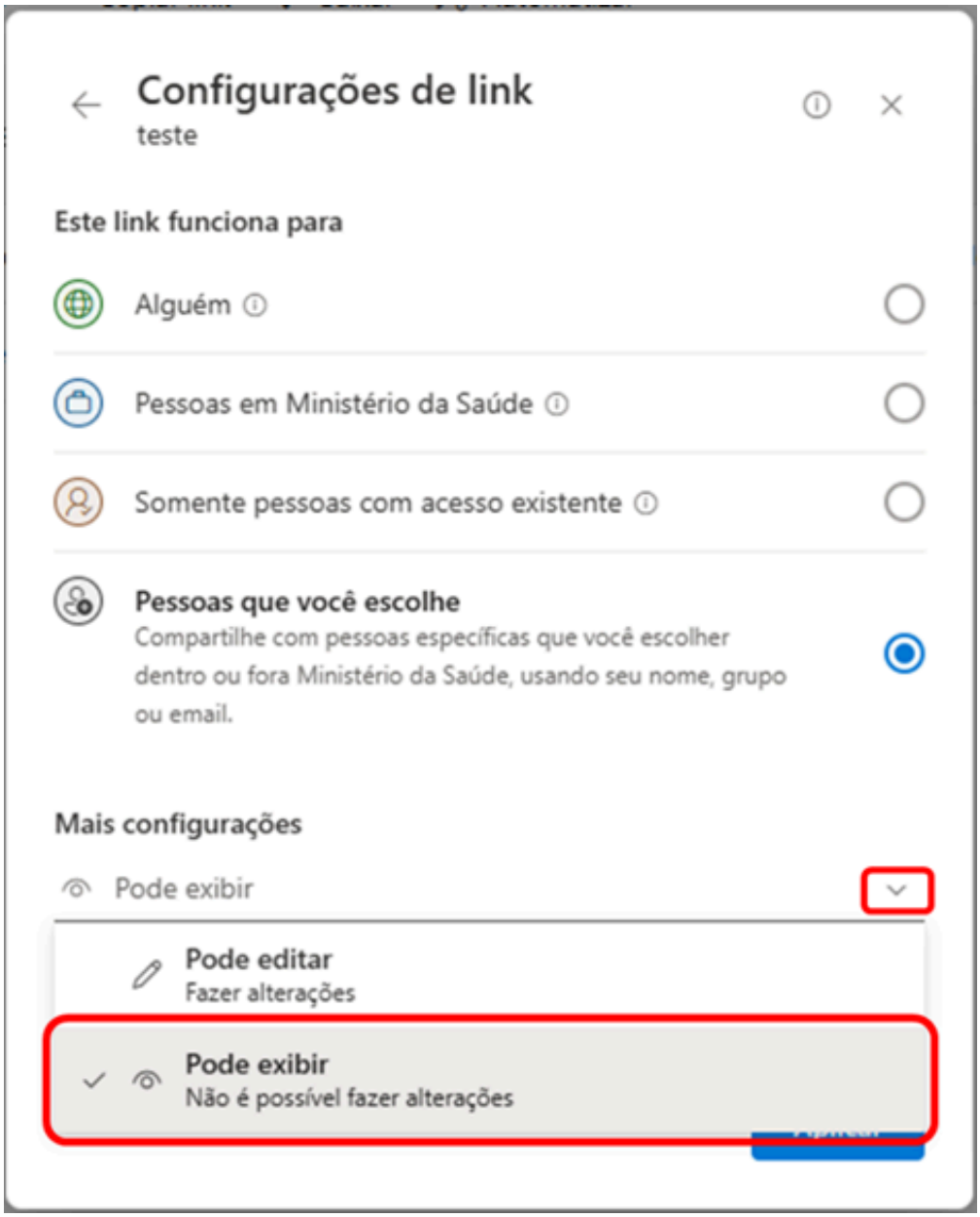
6.10. Caso deseje compartilhar um link exclusivo diretamente no e-mail que está redigindo, clique no menu configurações ao lado de "***Copiar link***";



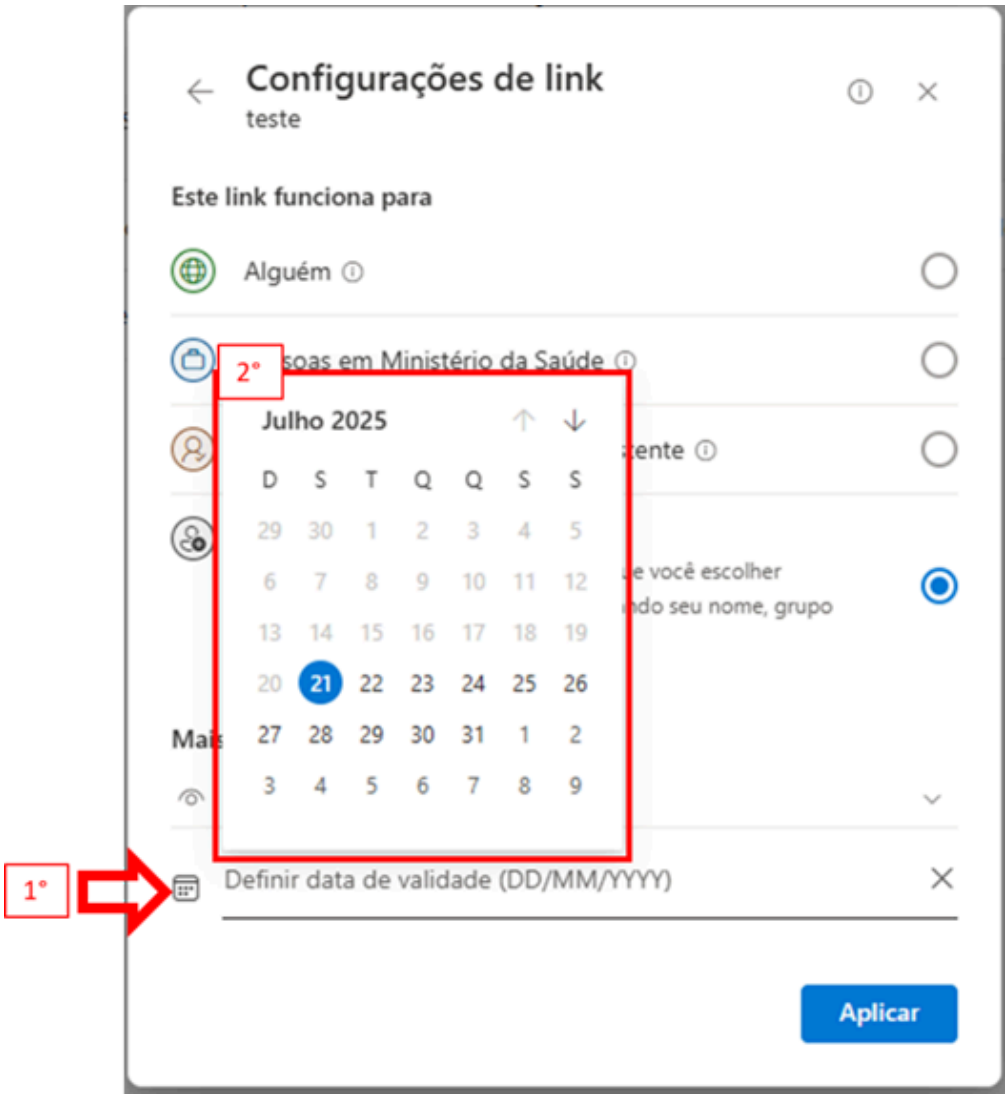
6.11. Aparecerá um novo pop-up. Selecione a opção "***Pessoas que você escolhe***";



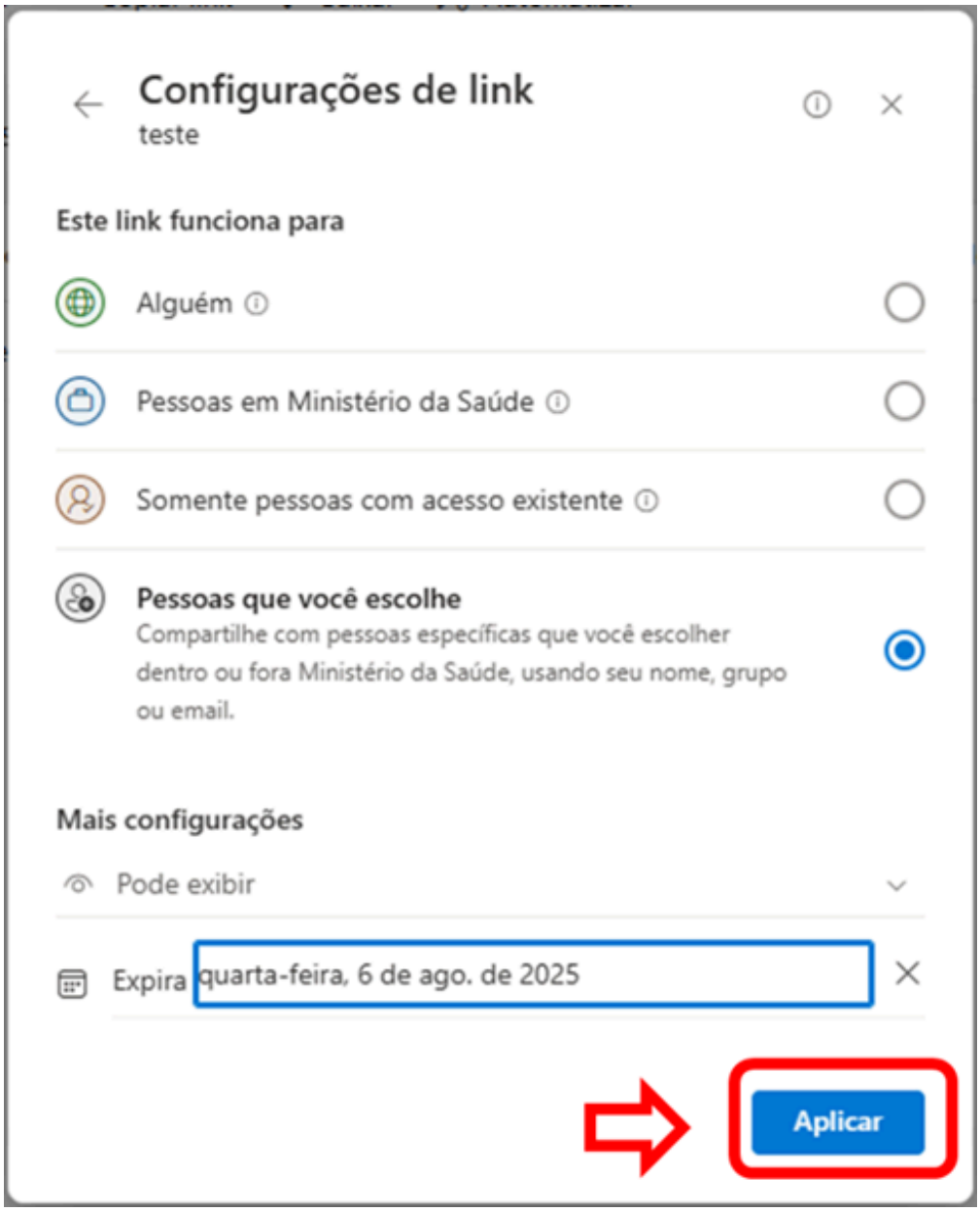
6.12. Em "***Mais Configurações***" selecionar a opção "***Pode Exibir***" (não é possível fazer alterações);



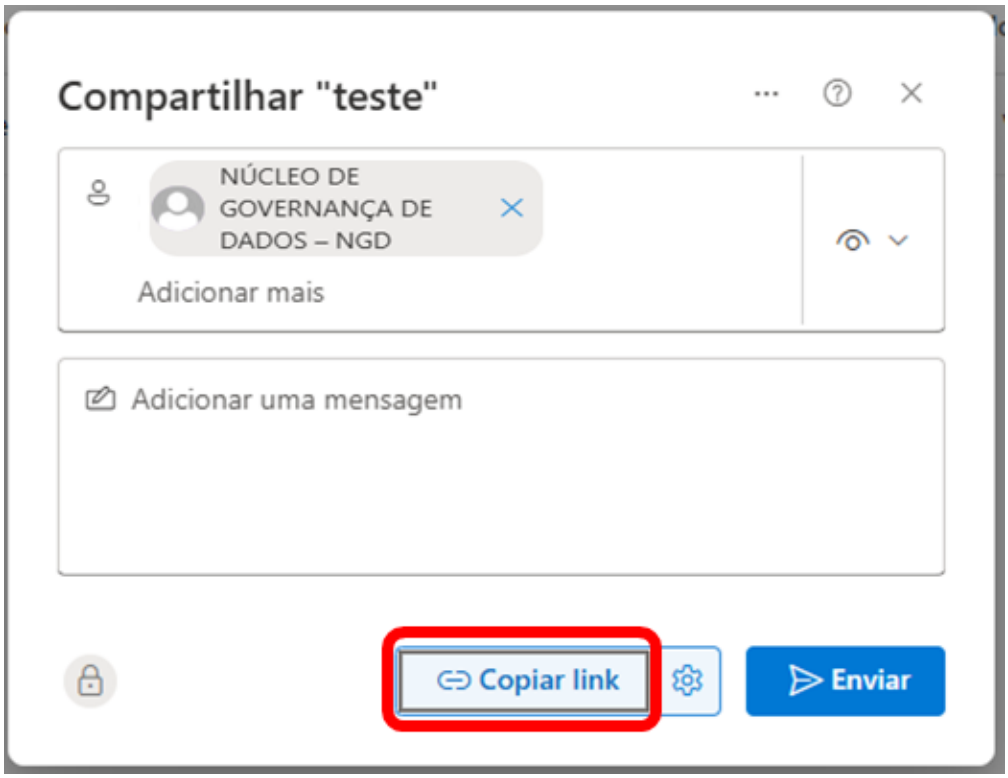
6.13. Em "***Mais Configurações***" é possível agendar o período que o link ficara disponível. Realize um agendamento com tempo de 15 dias. Essa data possui o intuito de evitar que dados, após compartilhados, continuem disponíveis;



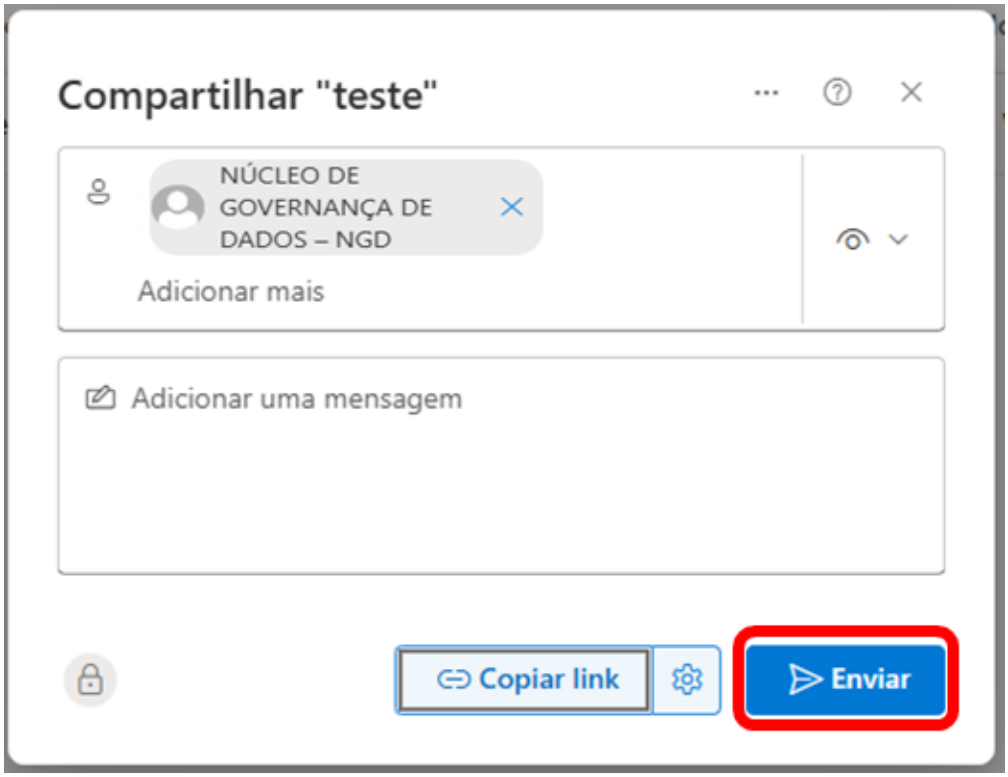
6.14. Agora clique em “***Aplicar***”;



6.15. Agora clique no menu "***Copiar Link***" para copiar o link e colá-lo no e-mail que será enviado ao operador;



6.16. Finalmente, clique no menu “**Enviar**” para finalizar o compartilhamento.



7. COMUNICAÇÃO E ENVIO DE SENHA

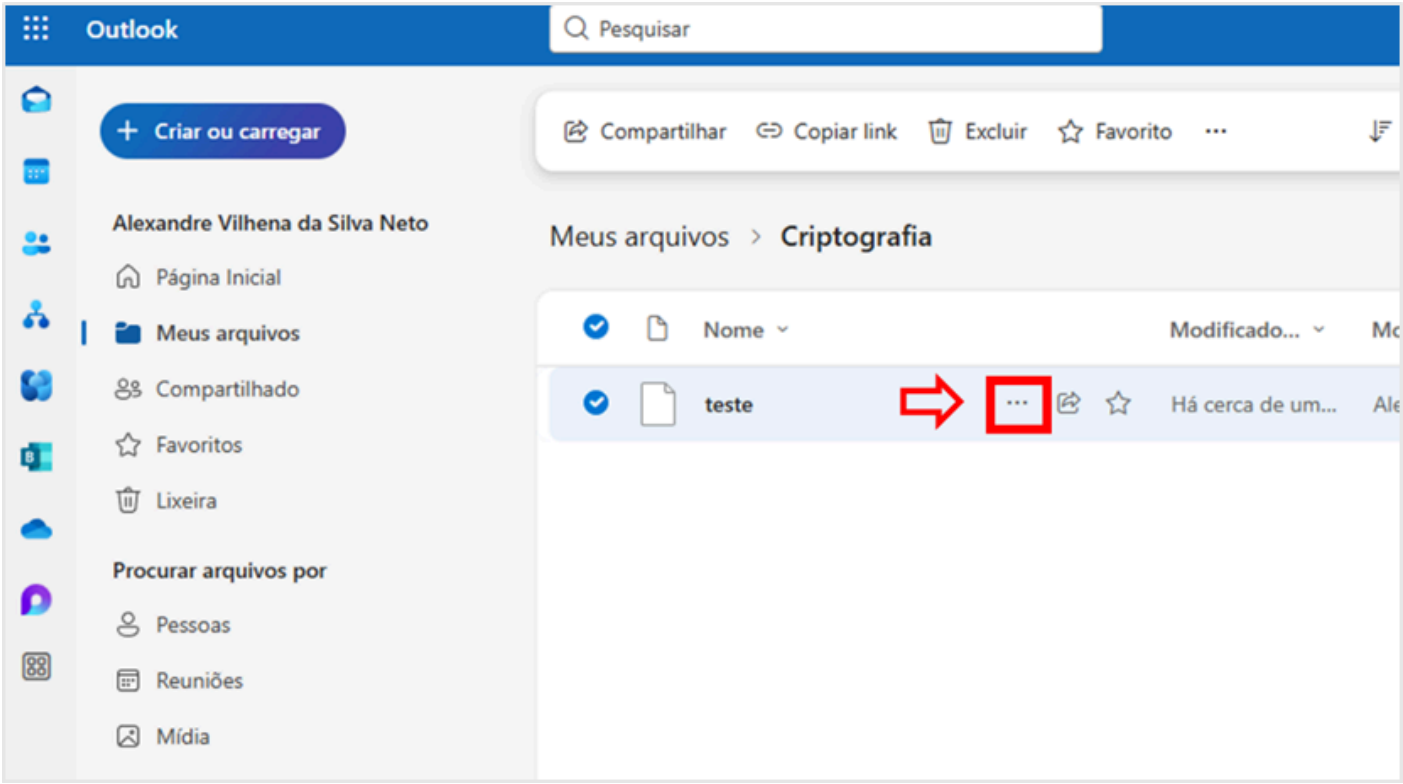
7.1. Será encaminhado um e-mail que deve conter a seguintes informações:

- Ao operador informando o envio do link, que o documento está criptografado e somente terá acesso o e-mail registrado no termo de compromisso;
- O operador deve acusar recebimento e download do arquivo;
- Que a demora pode acarretar expiração do link de acesso após 15 dias do envio;
- Após confirmação do acesso ao link e download ele será retirado;

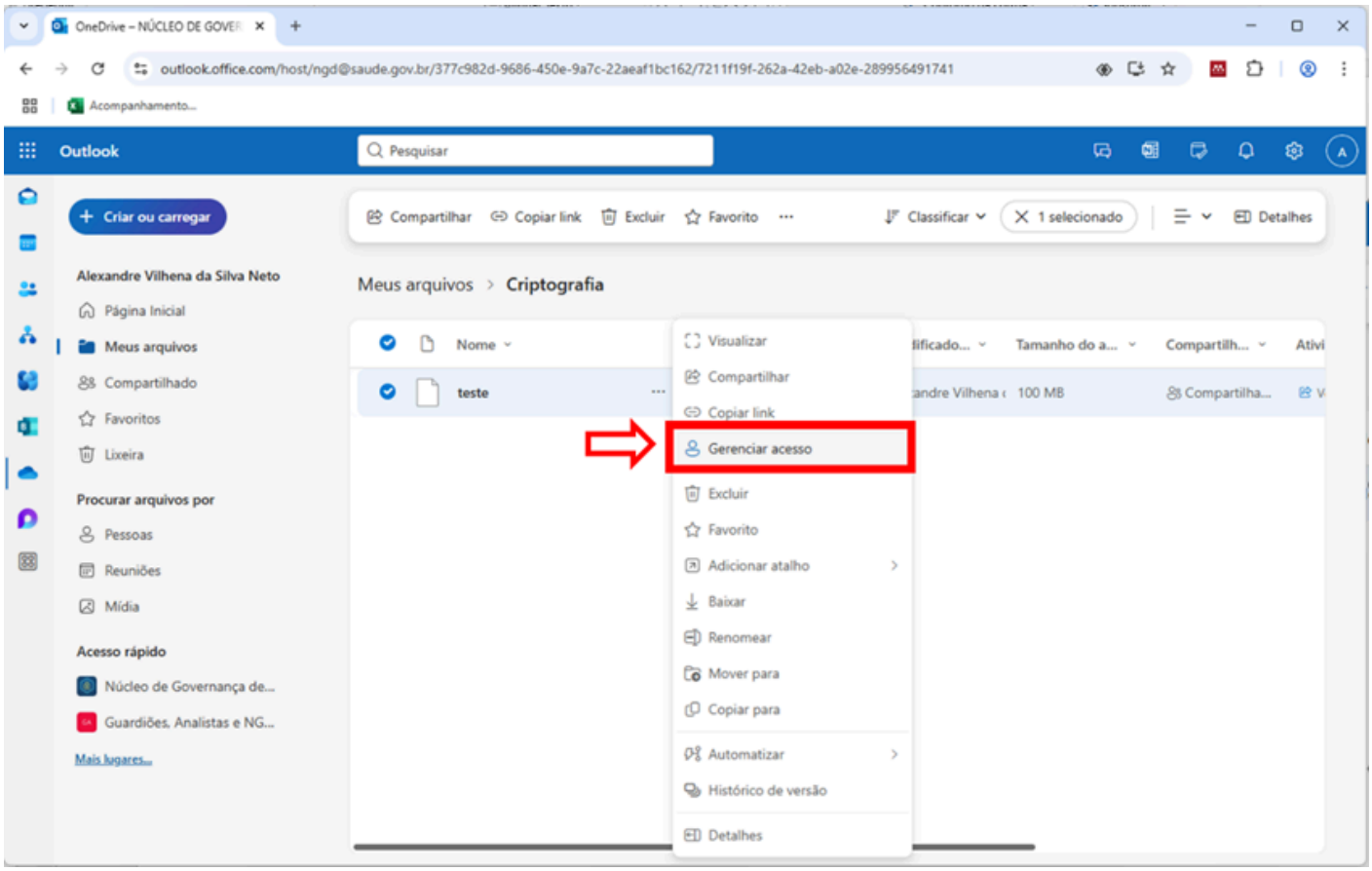
- Que a senha só será compartilhada após a assinatura do Termo transferência de dados, o qual estará em anexo no e-mail;
- Que o operador será contatado pelo telefone institucional para o envio da senha para descriptografar o arquivo, pelo contato informado no termo de compromisso.

7.2. Confirmado o recebimento de arquivo realizar a retirada do compartilhamento, entre novamente no Armazenamento em nuvem pessoal – Microsoft OneDrive. Conforme os passos 6.1 a 6.3;

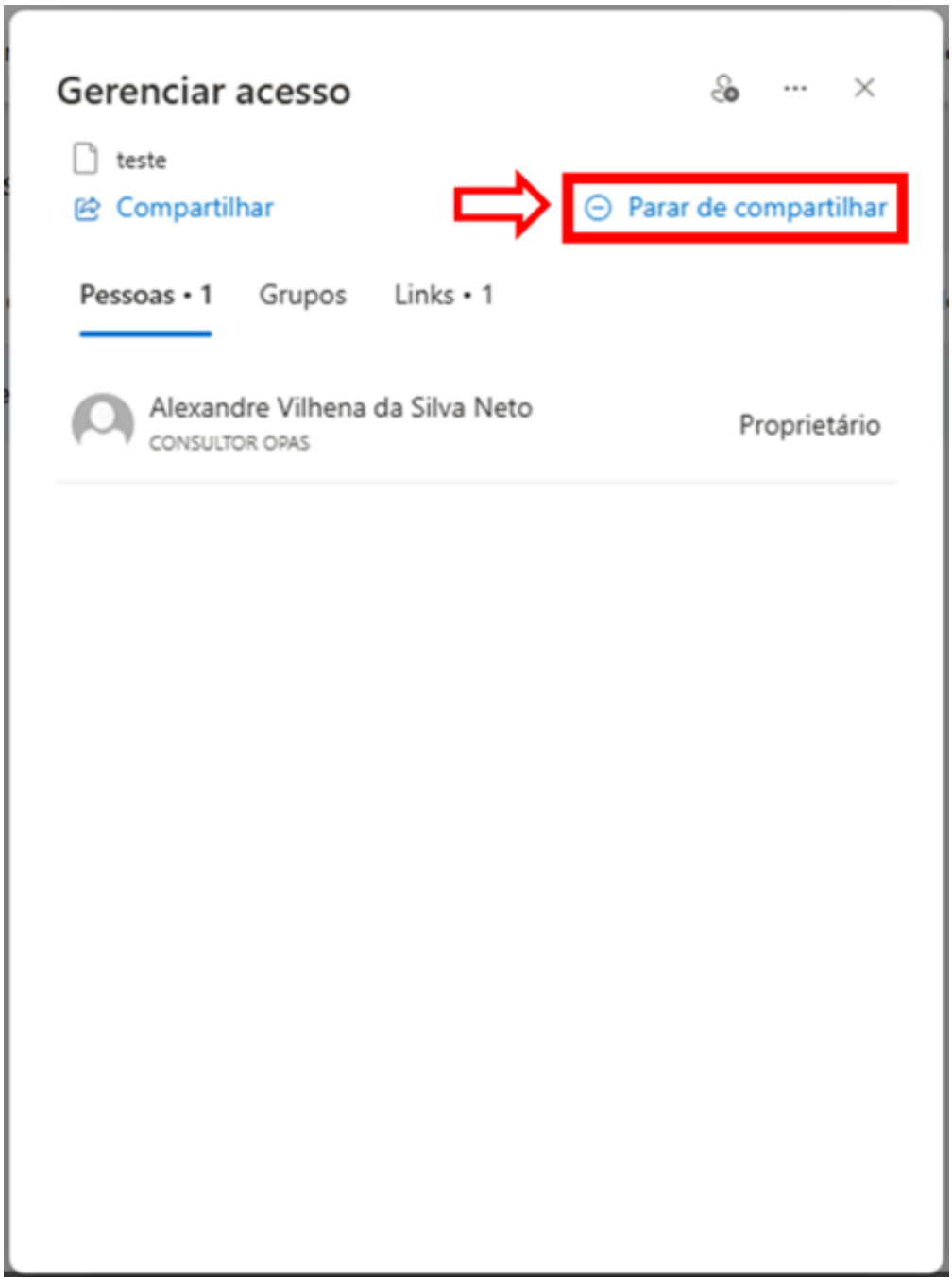
7.3. Encontre o arquivo que foi compartilhado anteriormente e clique nos três pontos "**...**";



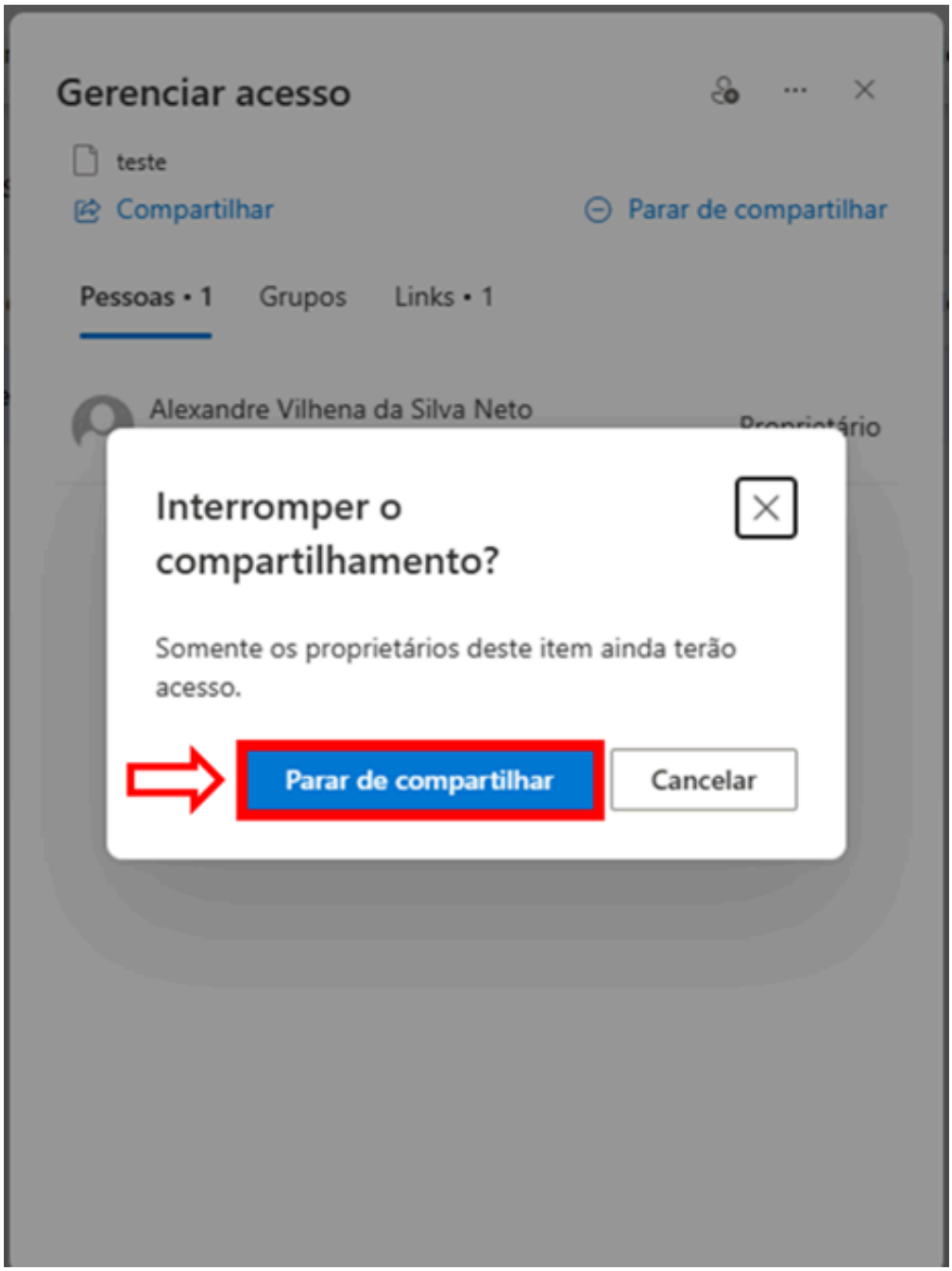
7.4. Clique em "***Gerenciar acesso***";



7.5. Ira abrir uma caixa e clique em “***Parar de compartilhar***”;



7.6. Ira abrir uma caixa de confirmação e clique em "***Parar de compartilhar***";

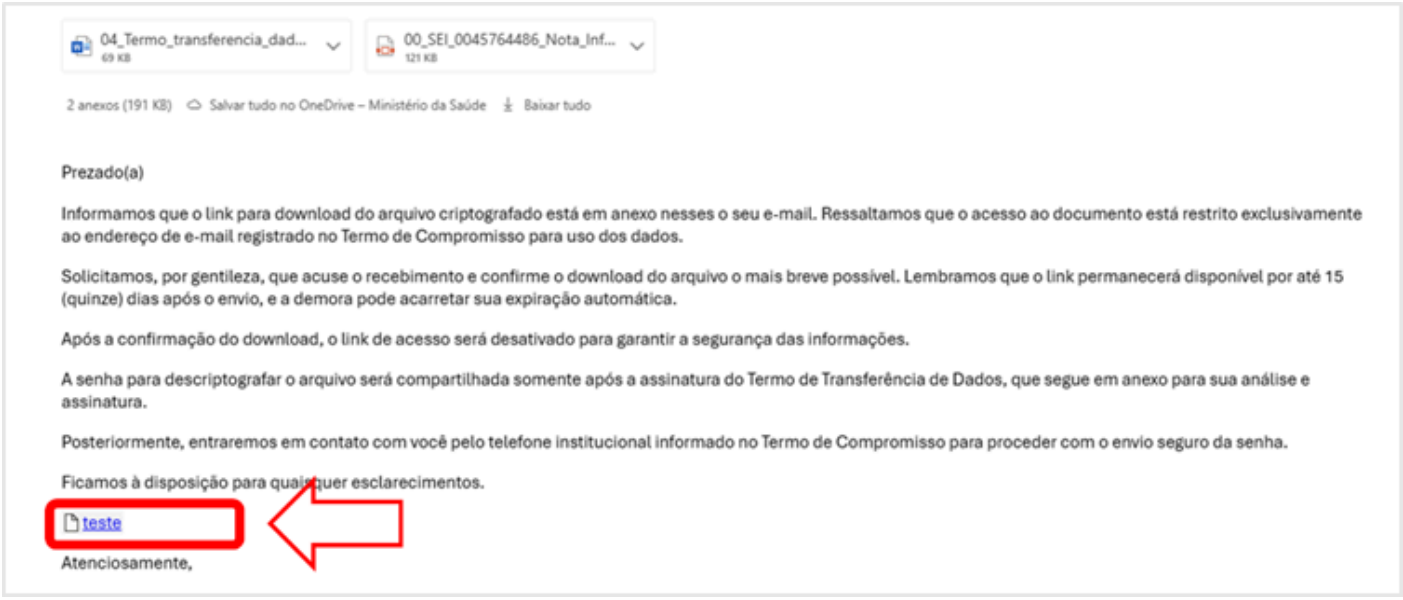


7.7. Confirme que o termo de recebimento do dado está em conformidade e se a assinatura e do operador presente no termo de compromisso;

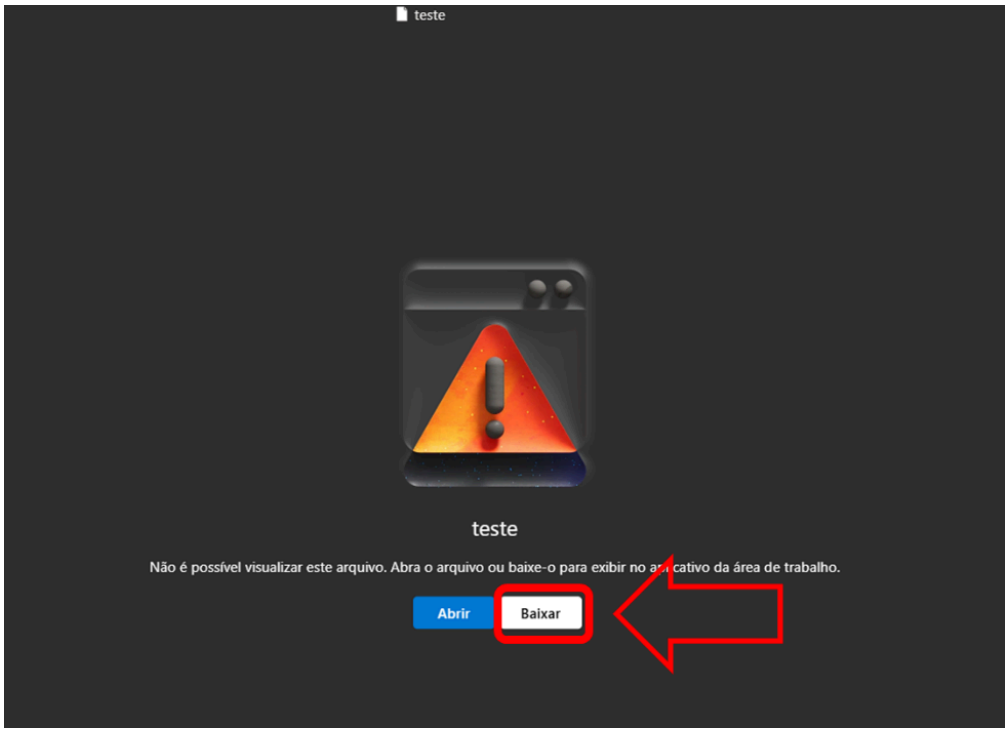
7.8. Realize a ligação para o contato no termo de recebimento, identifique o operador e realize o repasse da senha.

8. **DESCRIPTOGRAFAR UM ARQUIVO RECEBIDO**

8.1. Faça o download do link recebido no seu e-mail, clicando nele;

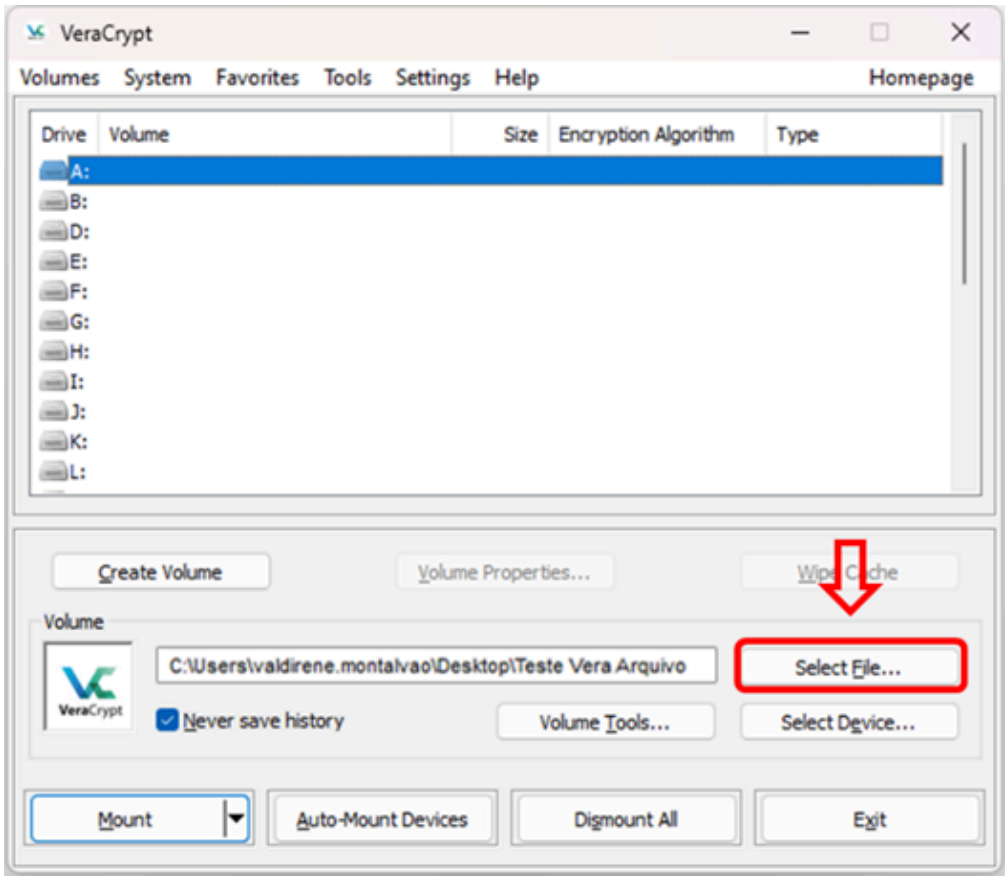


8.2. Ira abrir a seguinte guia no seu navegador, clique em baixar;

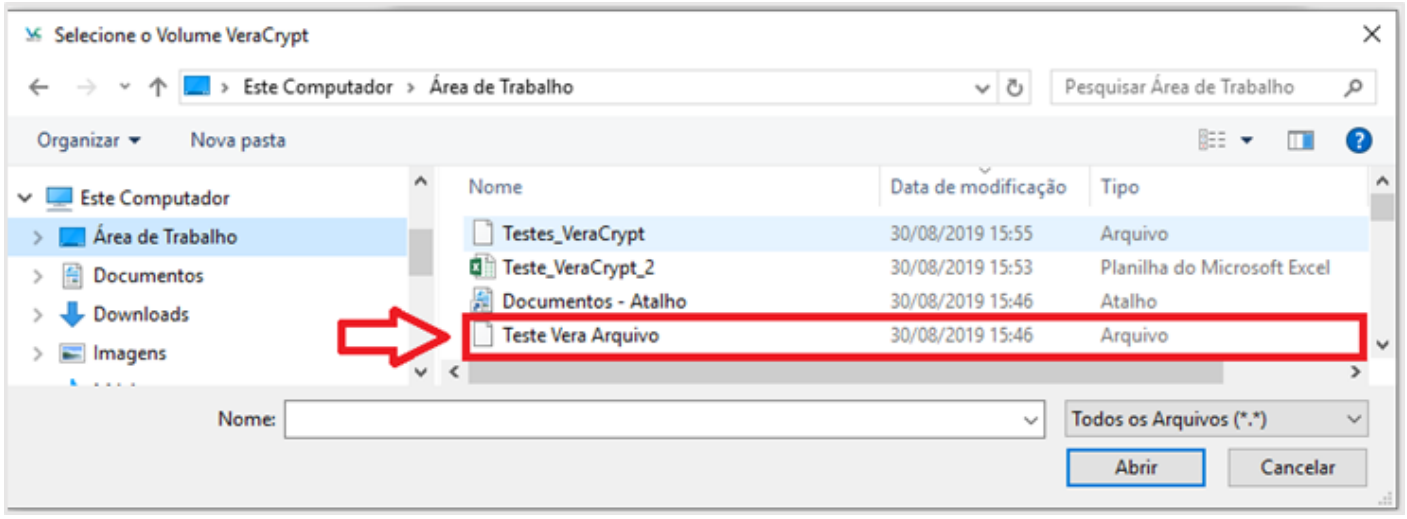


Ao receber a ligação proveniente do DAENT informe se pode tomar conhecimento da senha.

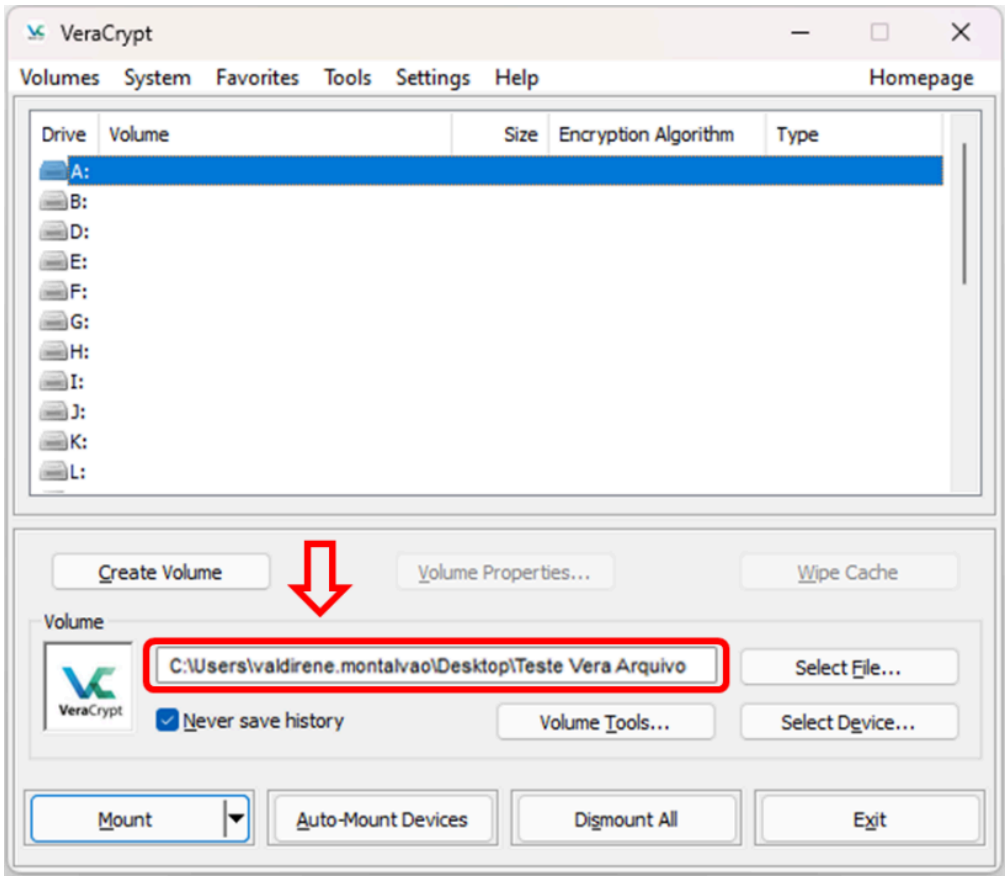
8.3. Abra o VeraCrypt e clique em “***Select File***”;



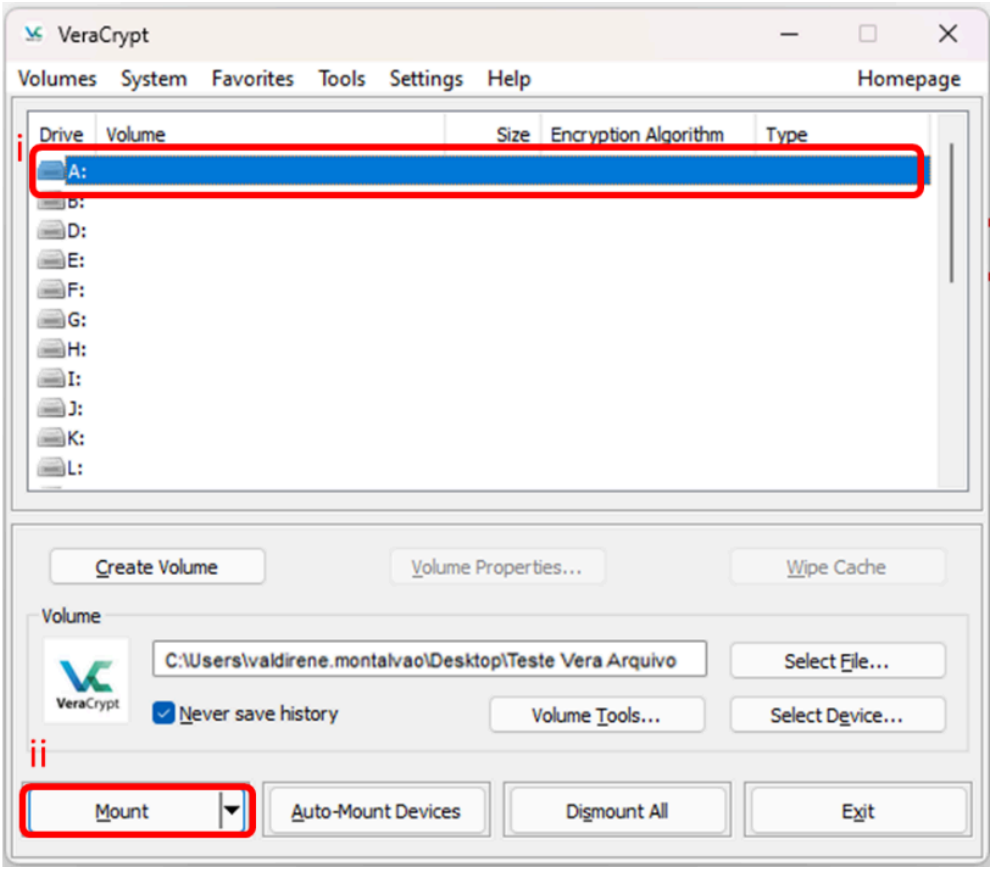
8.4. Localize o volume criado anteriormente, no exemplo abaixo o volume se chama **“teste”**. Clique duas vezes sobre o arquivo;



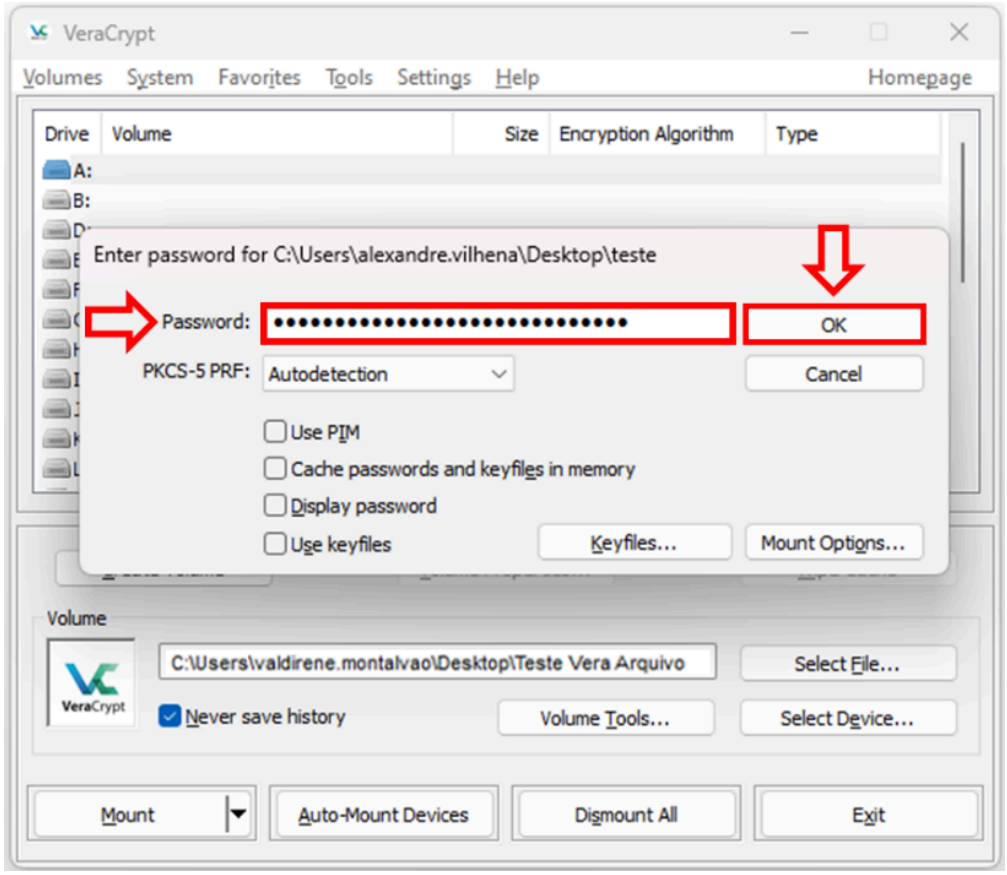
8.5. O volume será carregado na janela do Veracrypt;



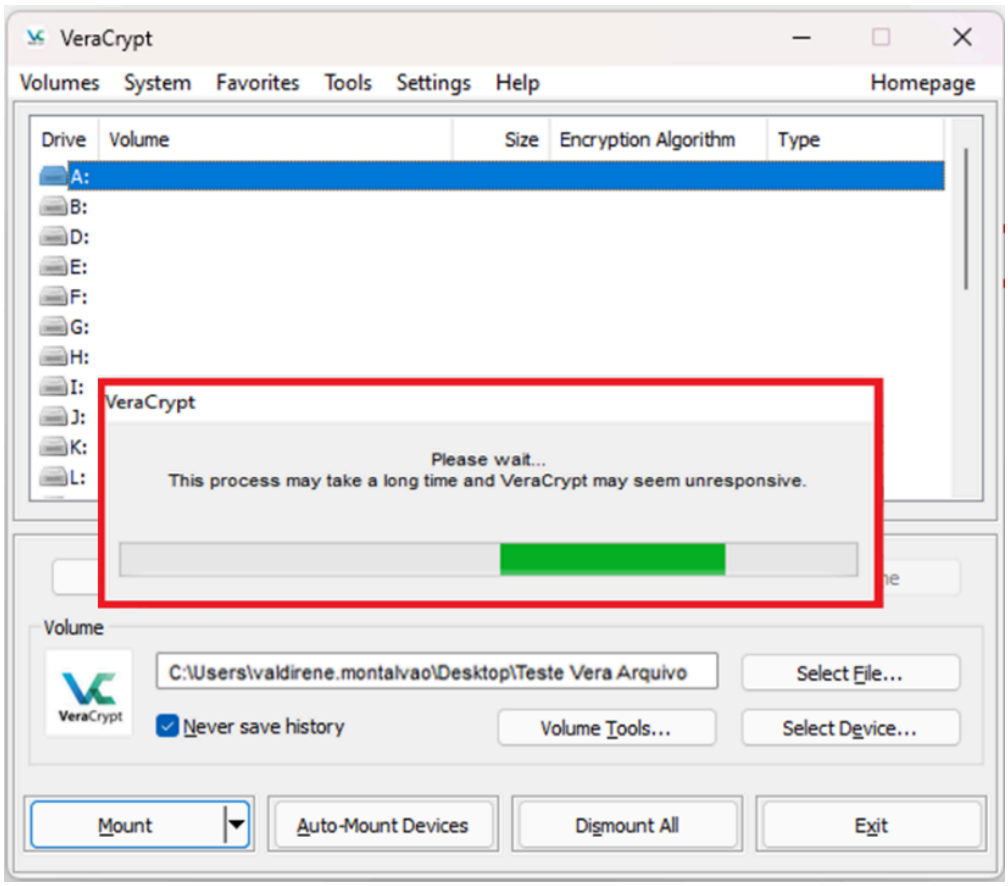
8.6. Selecione um diretório para colocar o volume criptografado para fins didático selecionado o "***Drive A***", (i) clicando duas vezes sobre o mesmo ou (ii) selecionando e clicando em "***Mount***";



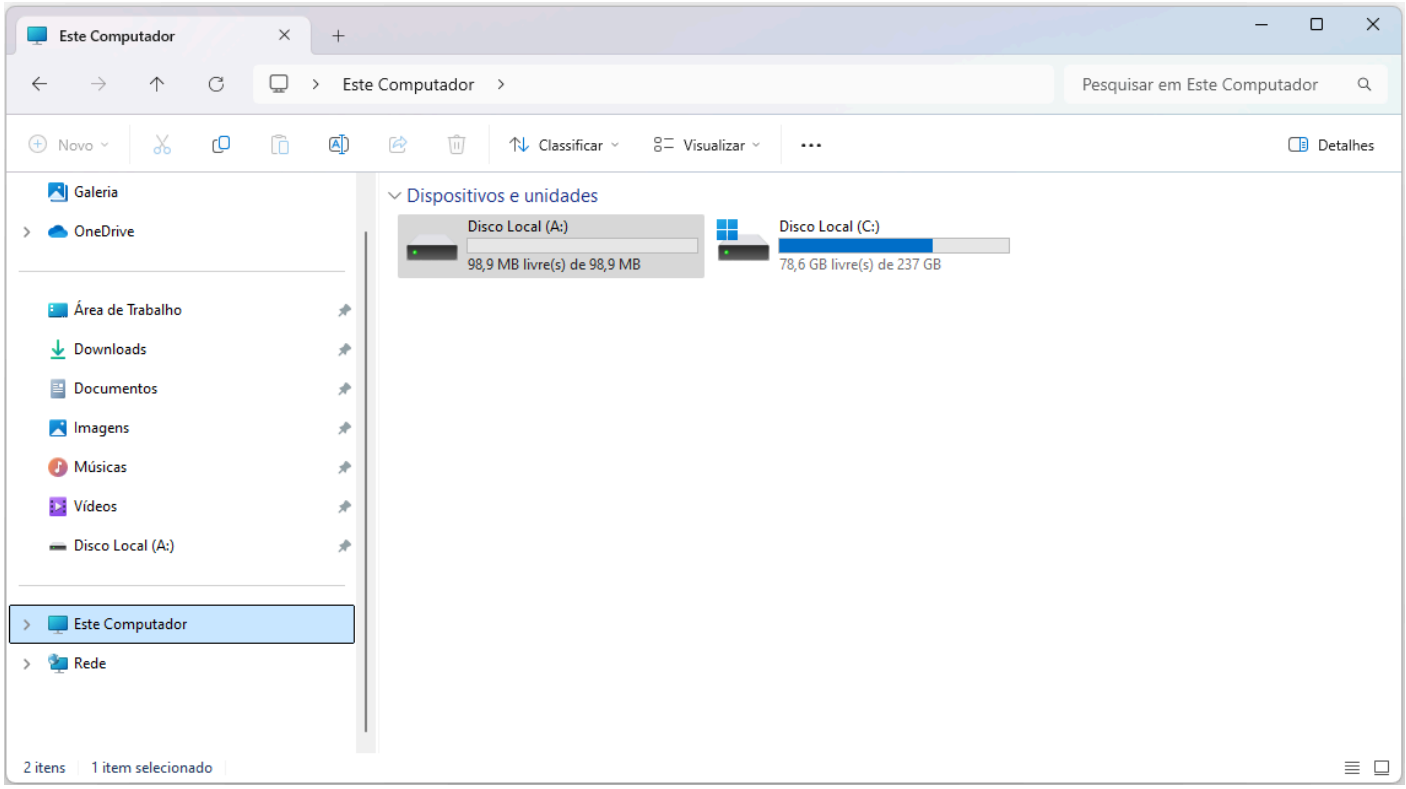
8.7. Digite a senha criada anteriormente e clique em "***OK***";



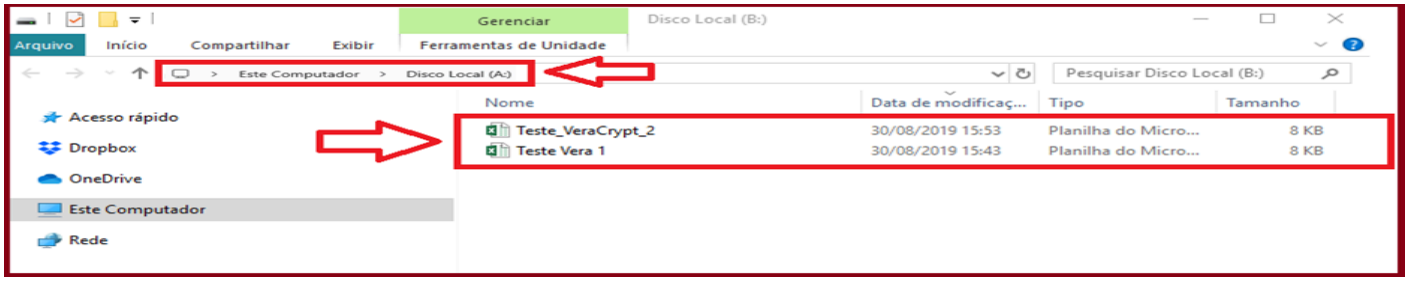
8.8. Aguarde o processamento;



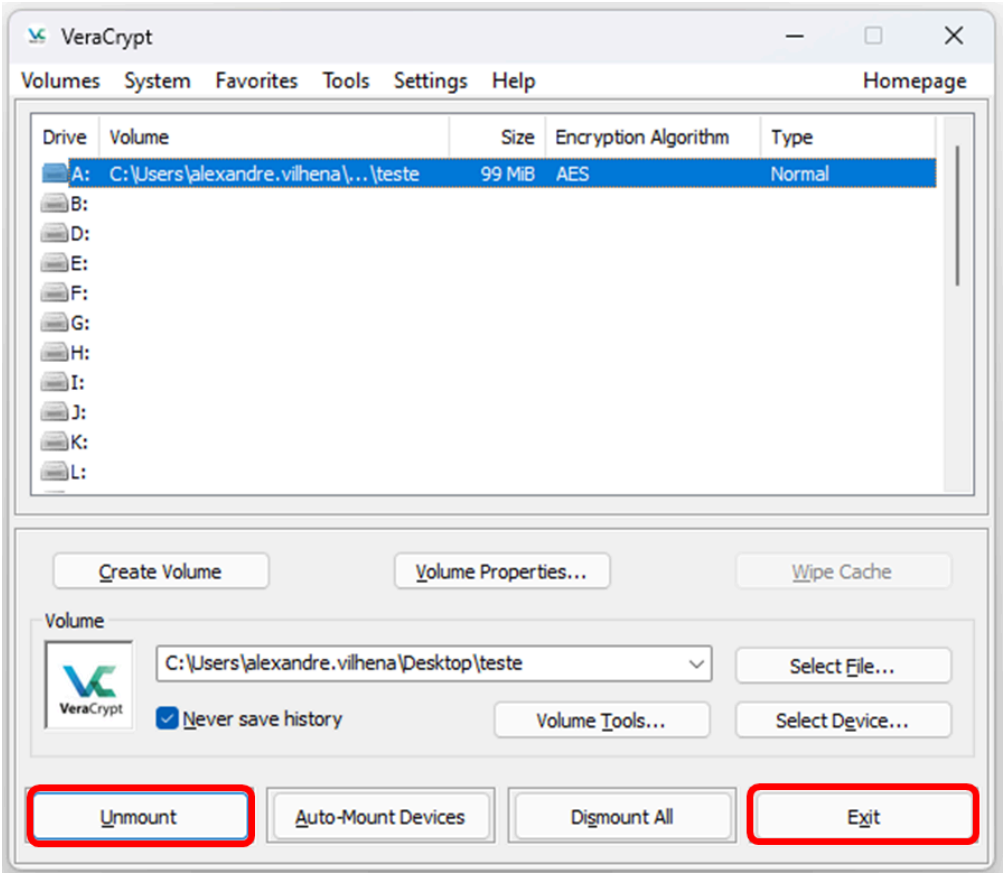
8.9. Abra o “Explorer” e em “***Este Computador***”, este computador ira encontra o drive criado, que para o fim didático utilizado “***Drive A:”;***



8.10. As arquivos estarão dentro do diretório (Ex. “***Drive A:”***);

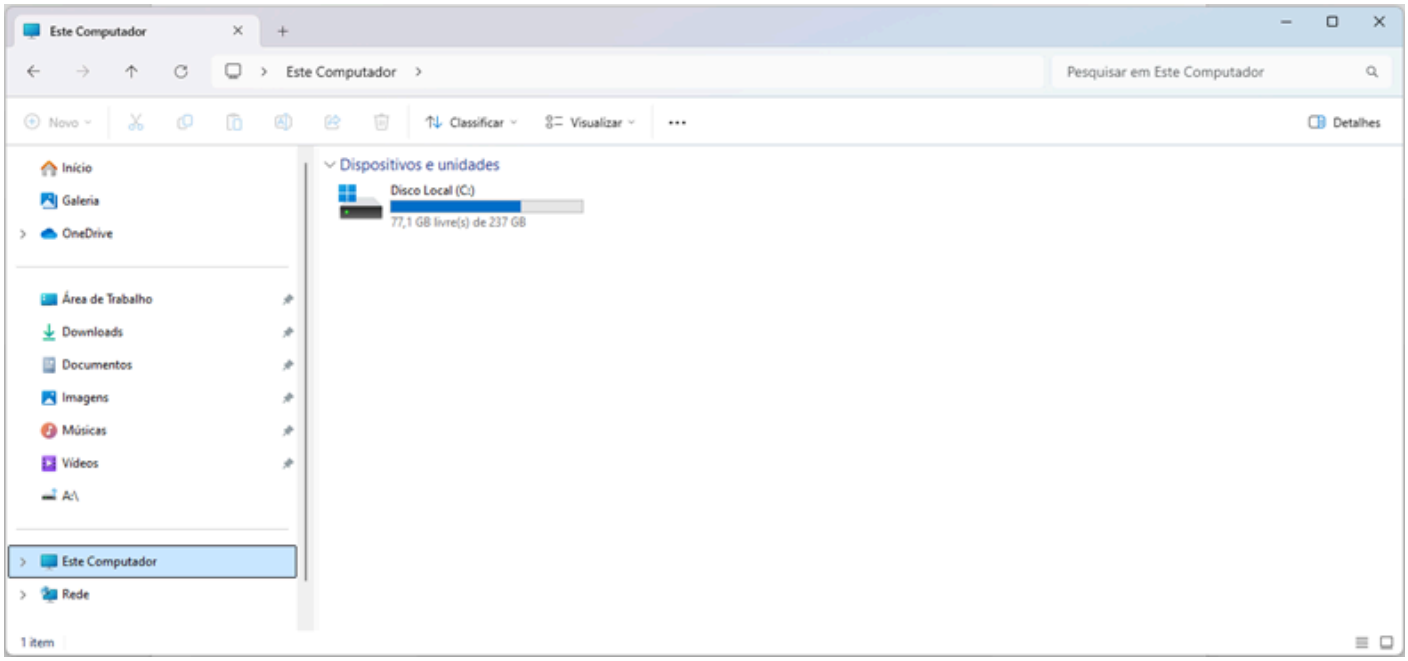


8.11. Na tela do VeraCrypt clique em “***Unmount***”, para que este diretório seja fechado, e posteriormente clique em “***Exit***”;



9. **CRIAÇÃO DE UMA UNIDADE CRIPTOGRAFADA**

9.1. Primeiramente verifique quando de memória de armazenamento (HD, SSD) existe em seu computador livre, abrindo o explore e clicando "***Este Computador***";

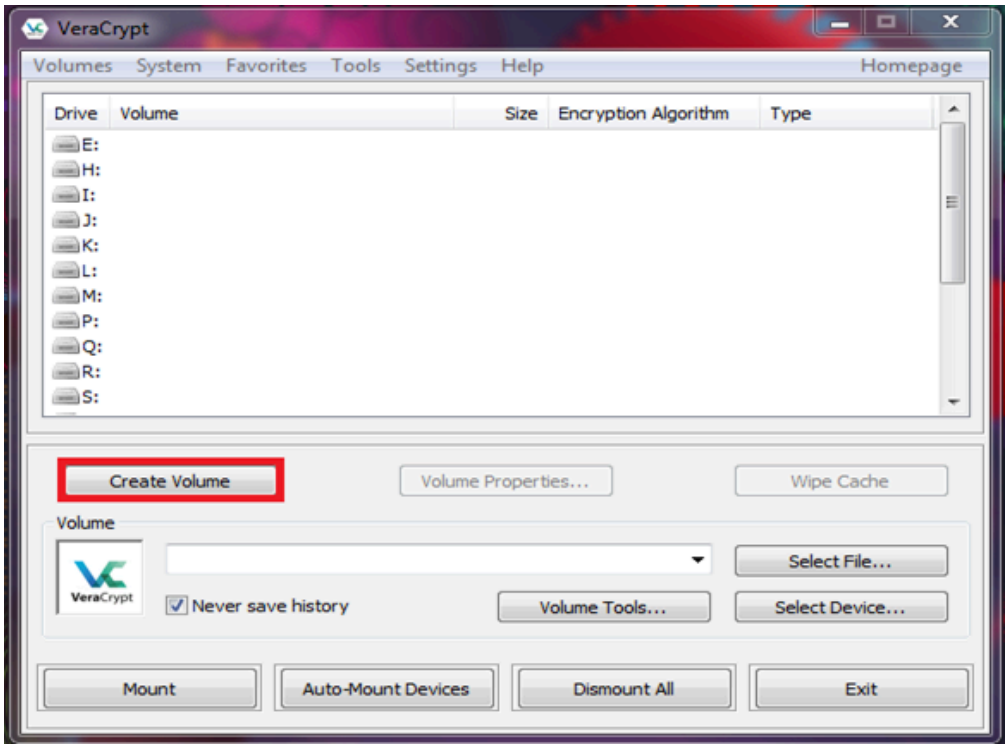


9.2. Este possui aproximadamente 77 Gb libres, o que significa que tenho essa quantidade de memória disponível para realizar a criptografia, recomenda-se nunca usar totalmente a memória para gerar o espaço criptografados, deixar sempre no mínimo 20 GB;

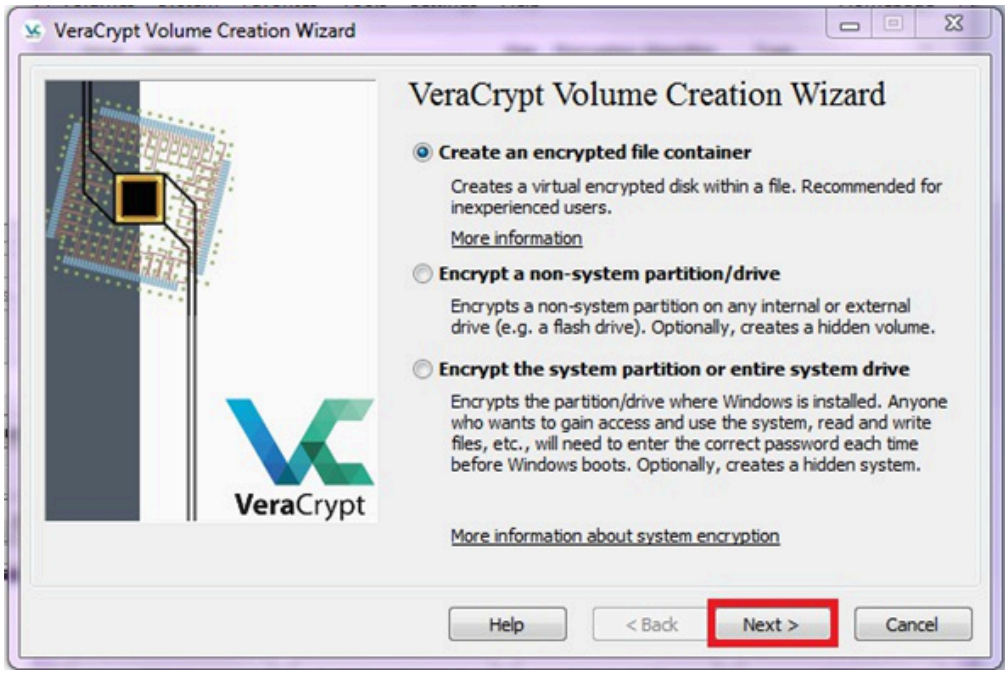
9.3. EX= 77-20=57Gb;

Logo 57 Gb seria o limite máximo de memória que poderá ser utilizado para realização de criptografia, ressaltando que se possível escolha tamanhos condizentes com o seu processamento.

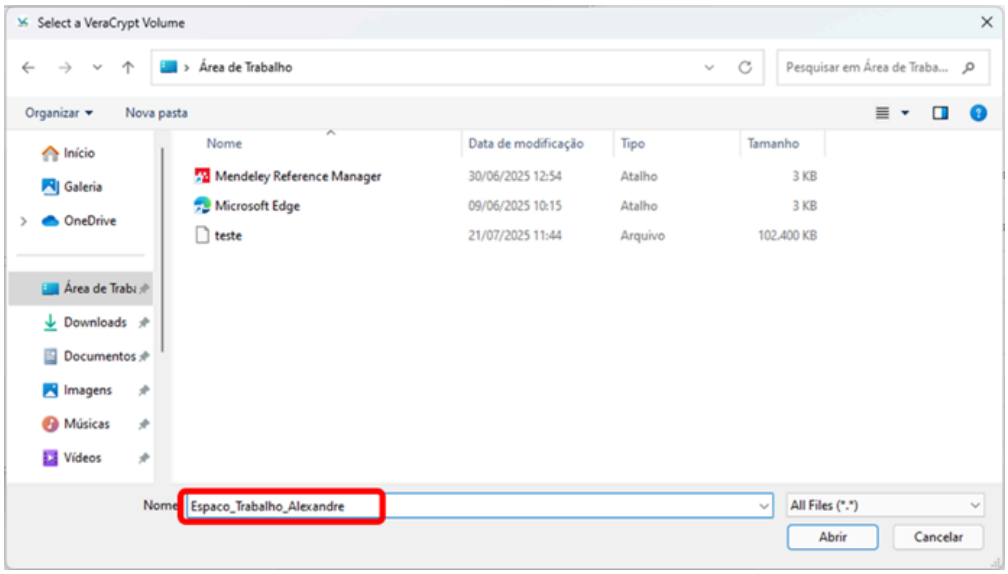
9.4. Abra o "***Veracrypt***" e clique em "***Create Volume***";



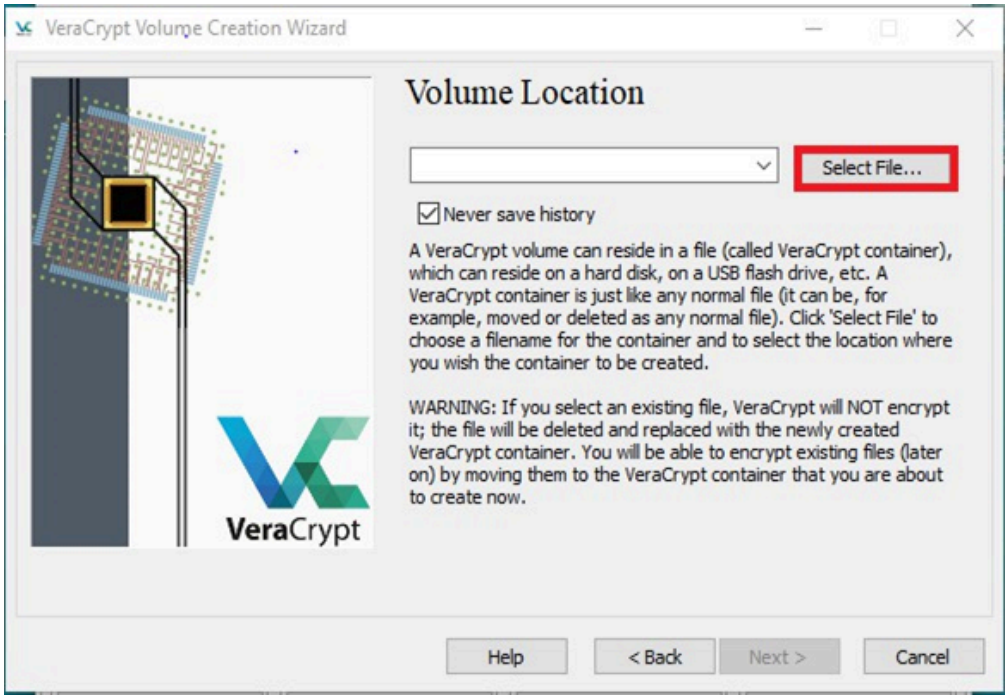
9.5. Clique em "***Create an encrypted file container***" e depois em "***Next***";



9.6. Clique em "***Standard VeraCrypt volume***" e depois em "***Next***";

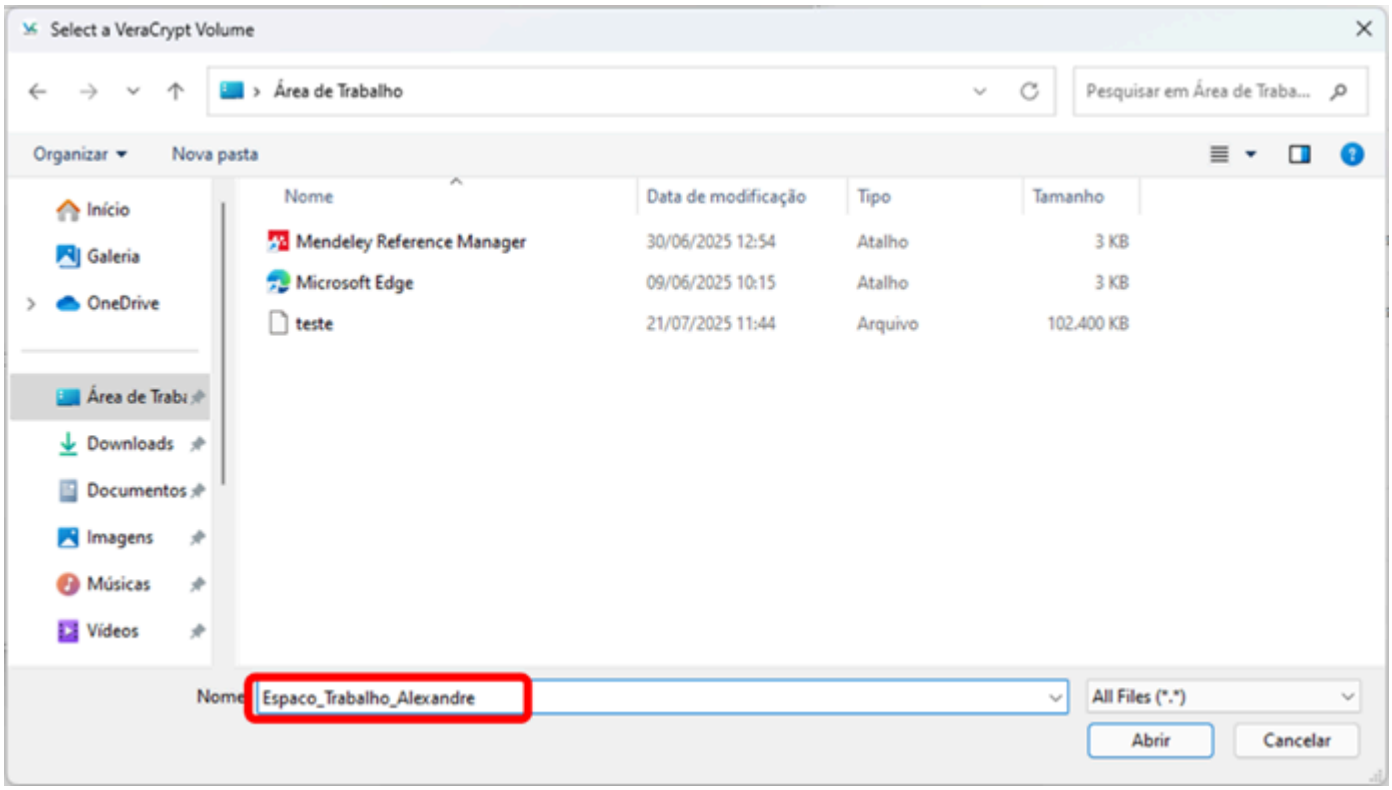


9.7. Clique em "***Select File...***";

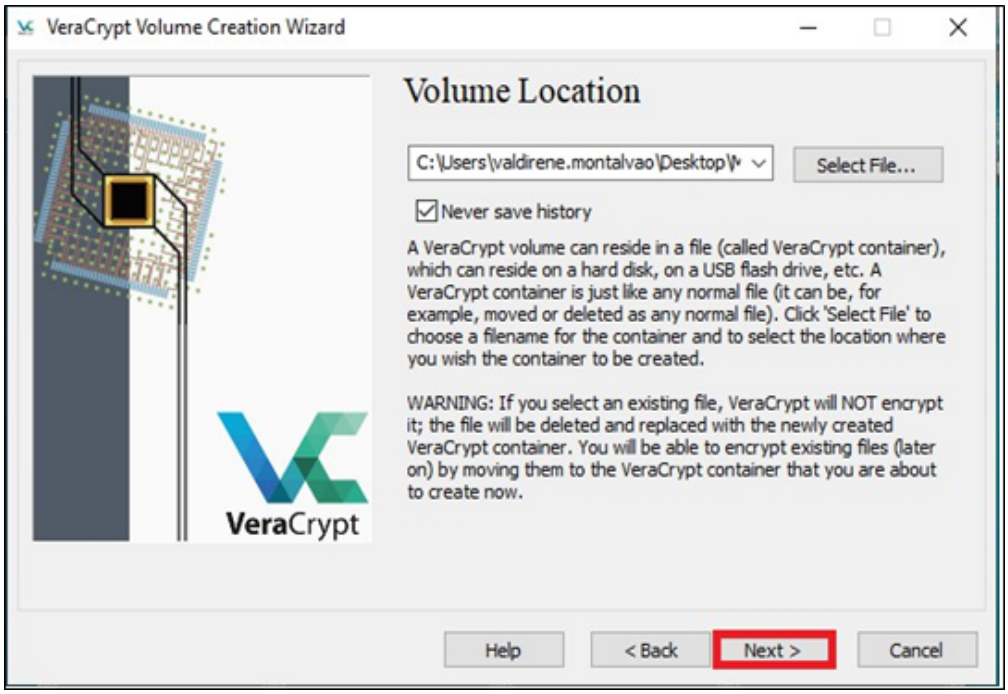


9.8. Selecione um local para salvar o volume (por exemplo: área de trabalho), crie um nome para esse volume recomendado que seja "***Espaco_Trabalho_nome***" e depois clique em "***Abrir***";

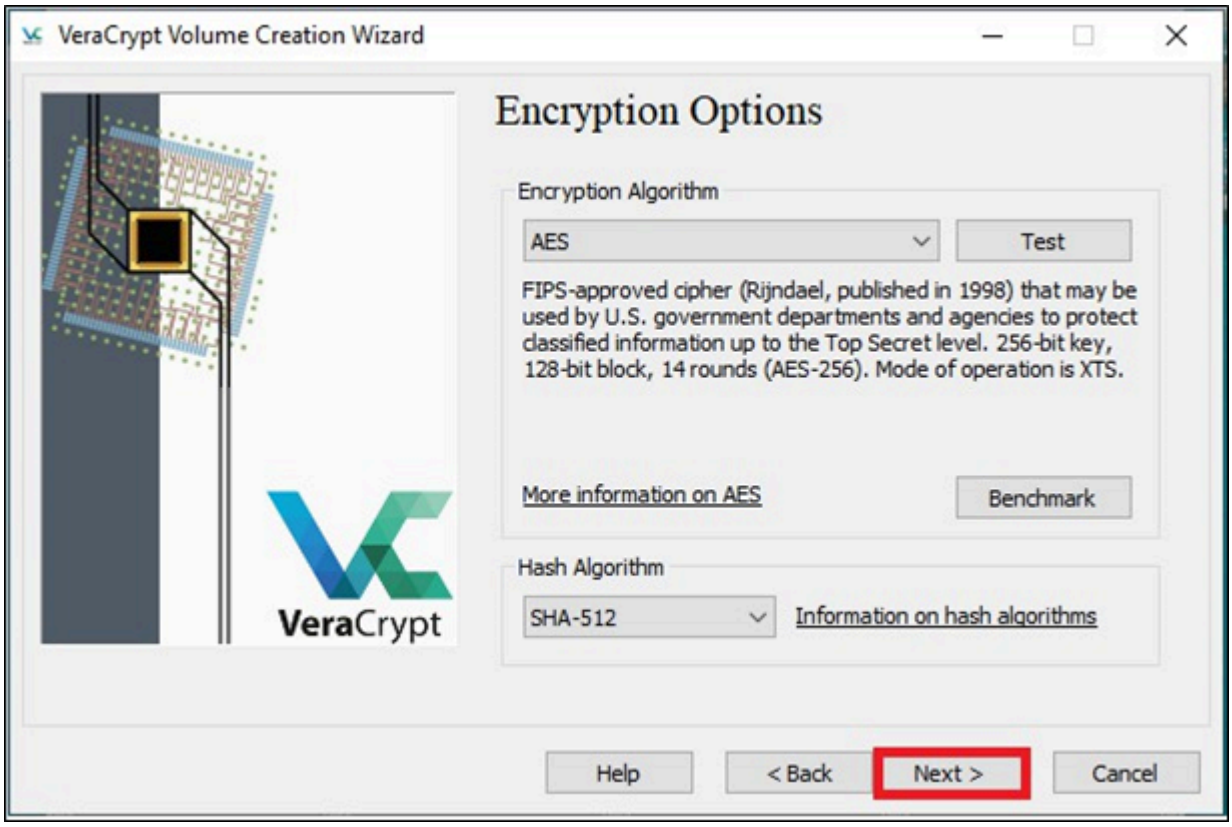
Obs: Sugere-se um nome sem espaço, caracteres especiais ou acentuação, por se tratar de processamento de dados, alguns softwares têm dificuldade quando o arquivo tem essas características.



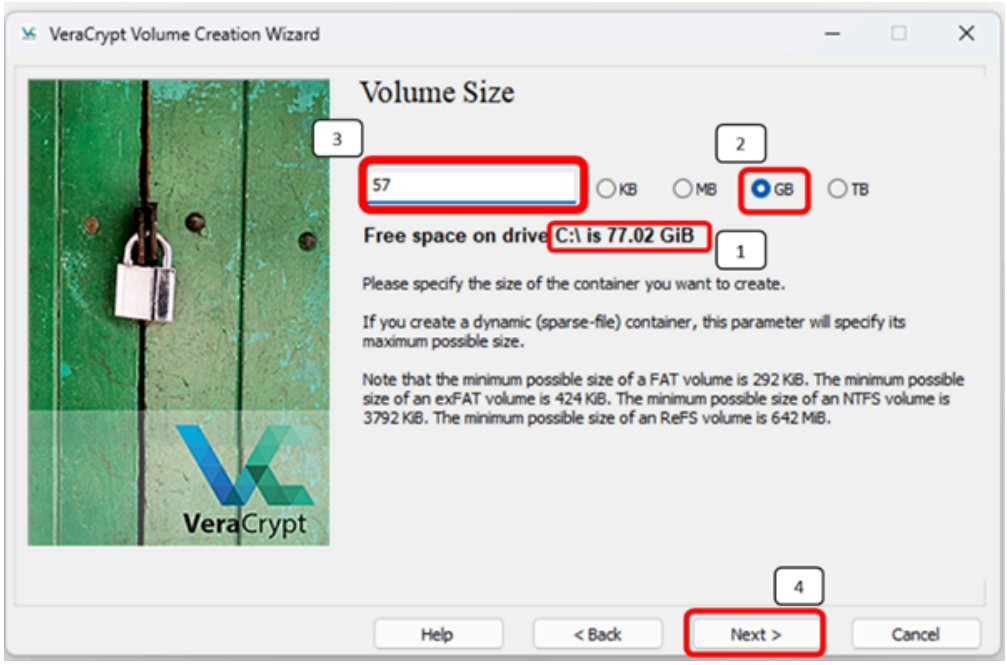
9.9. Clique em "***Next***";



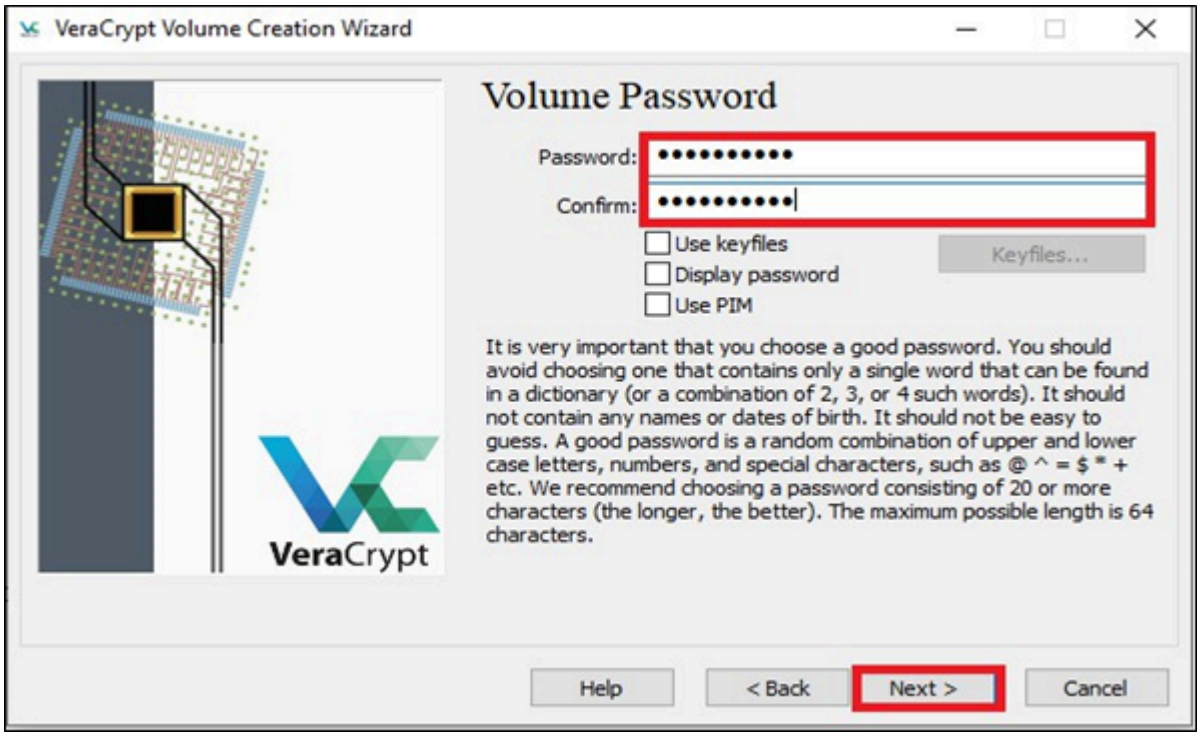
9.10. Na próxima tela chamada "***Encryption Options***", clique em "***Next***";



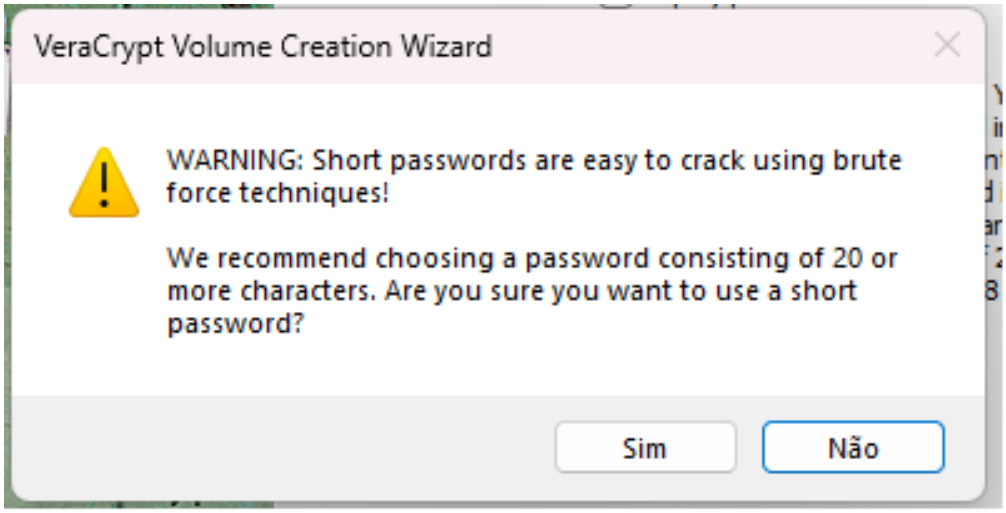
9.11. Na tela "***Volume Size***" escolha o tamanho da unidade que será criada, visualize a memória disponível (1) utilize sempre apenas o necessário recomendamos deixar pelo menos 20 gigas livre nesse caso criaremos um drive baseado em gigas devendo mudar a unidade de armazenamento (2) e adicionar o valor na caixa (3). Depois clique em "***Next***" (4);



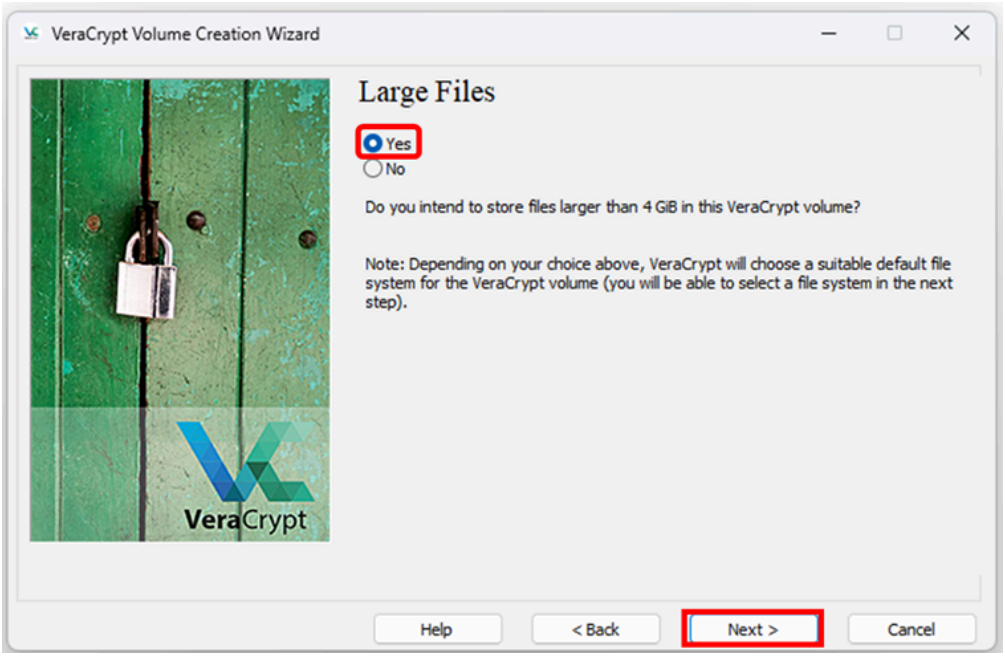
9.12. Crie uma senha de sua escolha e digite em "***Password***" e "***Confirm***". Clique em "***Next***". Existe a recomendação de que a senha seja maior do que 20 caracteres, caso sua senha seja menor que isso, existe a possibilidade de quebra da senha. Uma boa senha e a combinação aleatória entre letras maiúsculas e minúsculas, número e caracteres especiais, como @^=$+ etc;



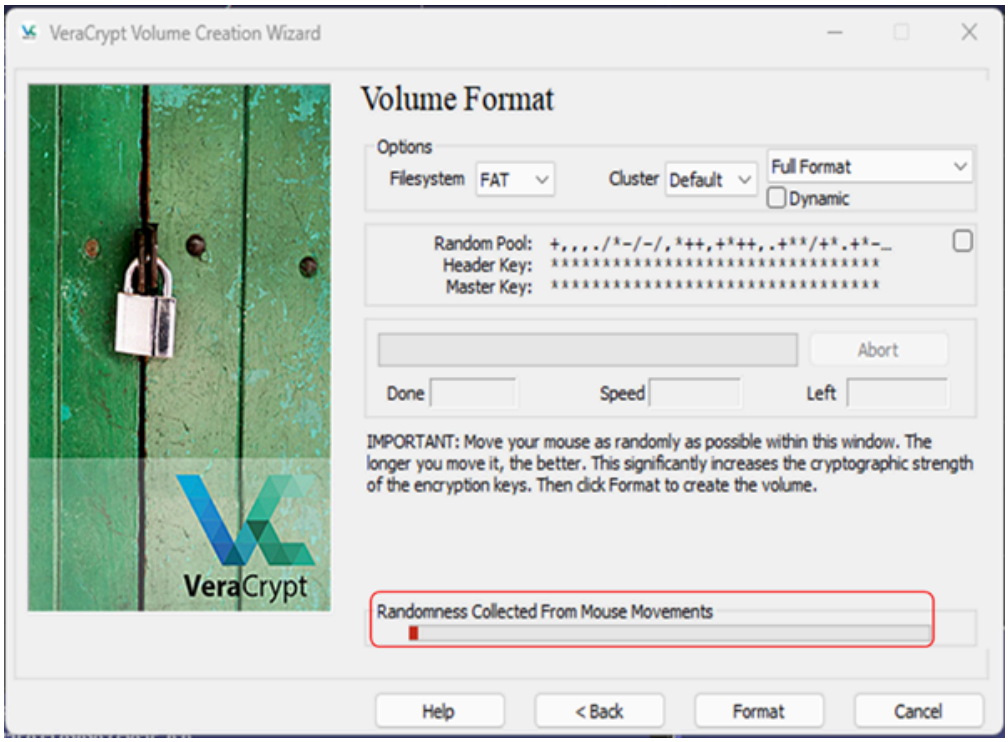
9.13. Caso sua senha seja menor que 20 caracteres irá aparecer uma mensagem avisando da fragilidade da senha e se deseja realmente usar uma senha curta, clique em "***Sim***" caso queira manter a senha ou "***Não***" e aumente o tamanho da sua senha;



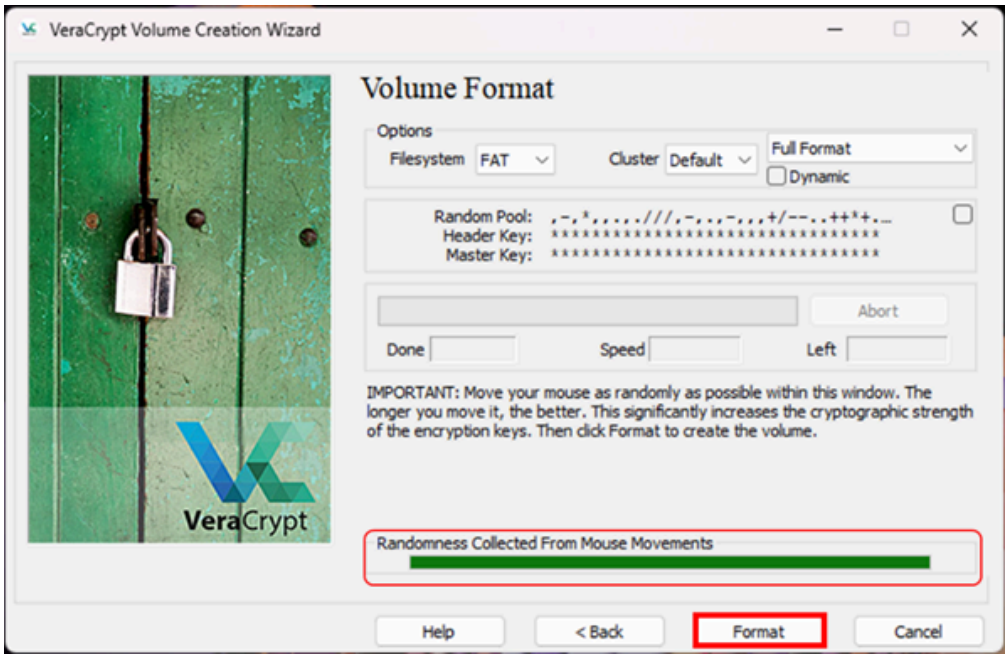
9.14. Por se tratar de um arquivo maior que 4 Gb, surgirá a seguinte mensagem. Selecione "***Yes***" e depois "***Next***";



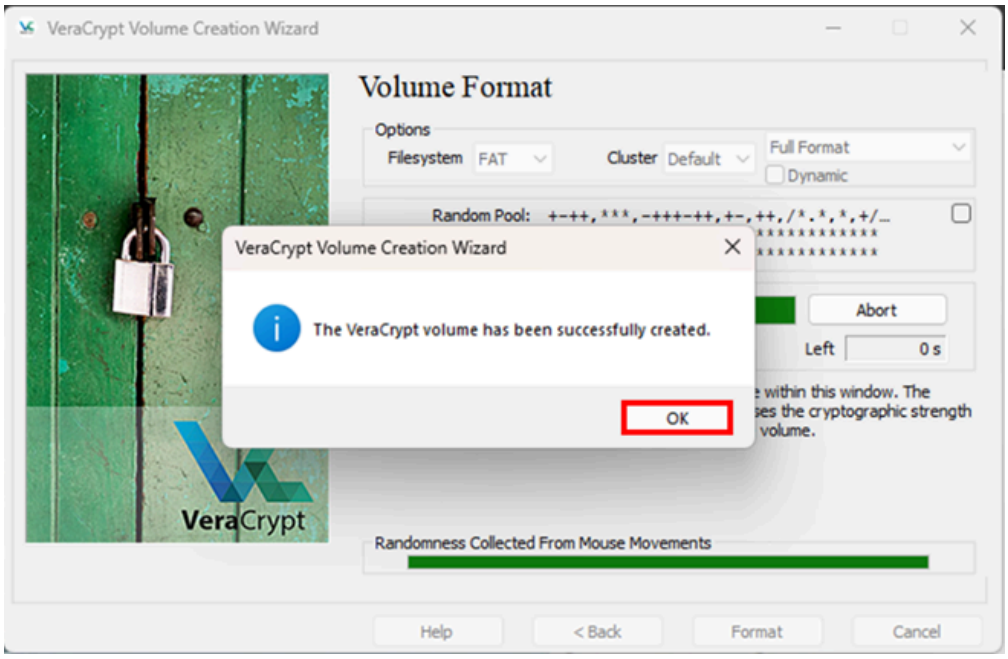
9.15. Irá abri essa caixa, observe que o campo "***Randomness Collected From Mouse Movements***" tem uma barra de carregamento, realize movimentos circulares com o mouse em cima da tela, até terminar de preencher o campo;



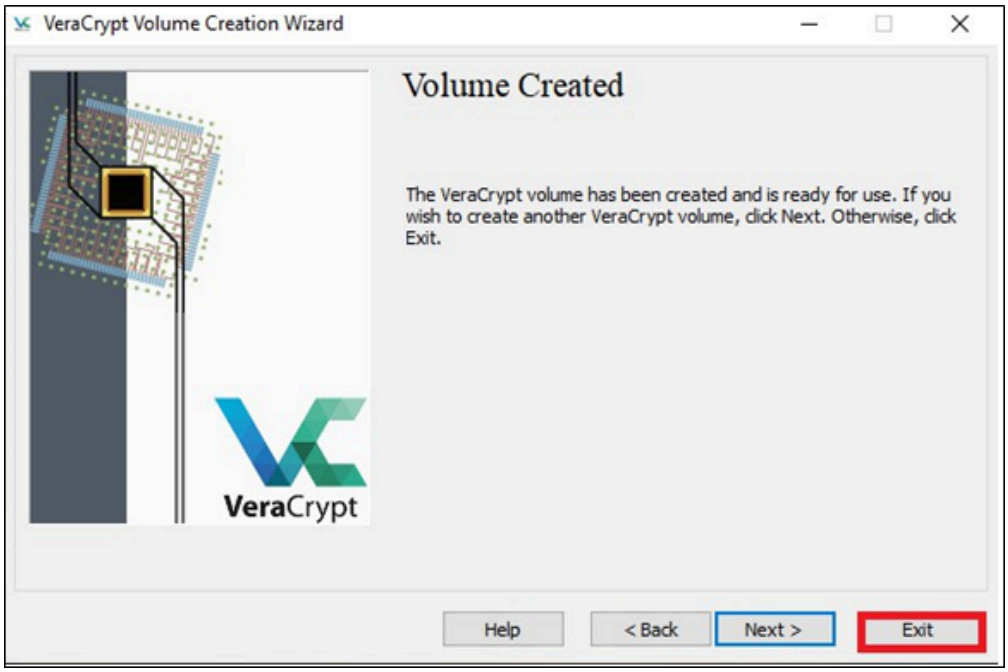
9.16. Em seguida clique, observe que o campo em "***Randomness Collected From Mouse Movements***" está totalmente preenchida e clique em "***Format***";



9.17. Assim o VeraCrypt criará um volume criptografado. Aparecerá a informação de que o arquivo foi criado com sucesso "***The VeraCrypt volume has been successfully created***", clique em "***ok***";

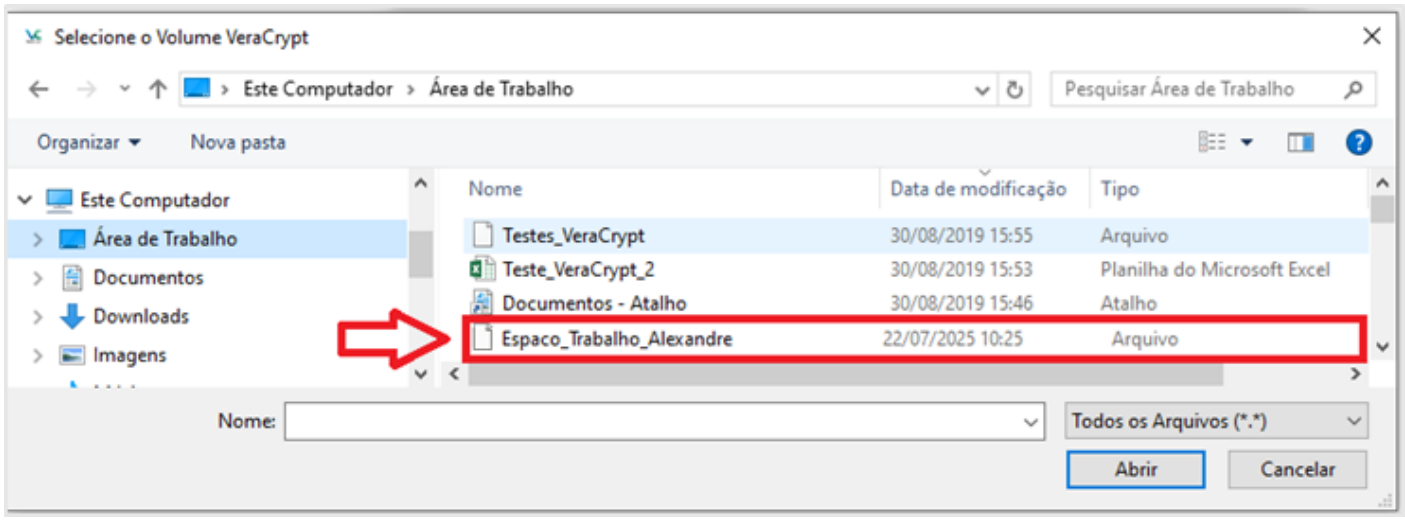


9.18. Clique em "***Exit***".

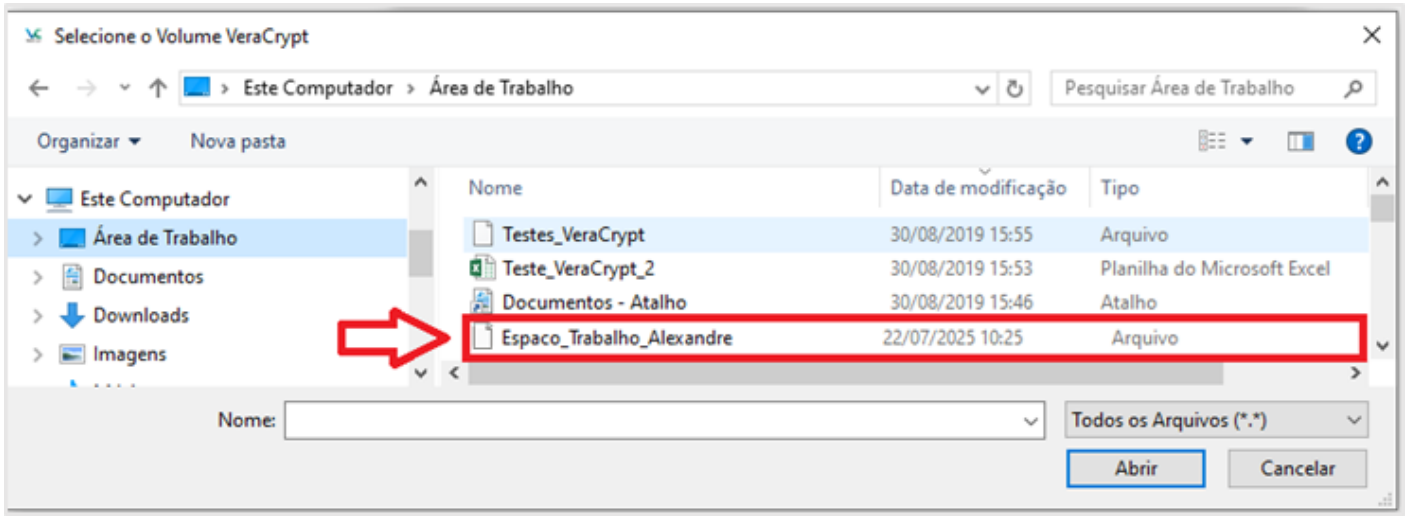


10. **ABRINDO O DRIVE CRIPTOGRAFADO PARA REALIZAÇÃO DE PROCESSAMENTO DE DADOS**

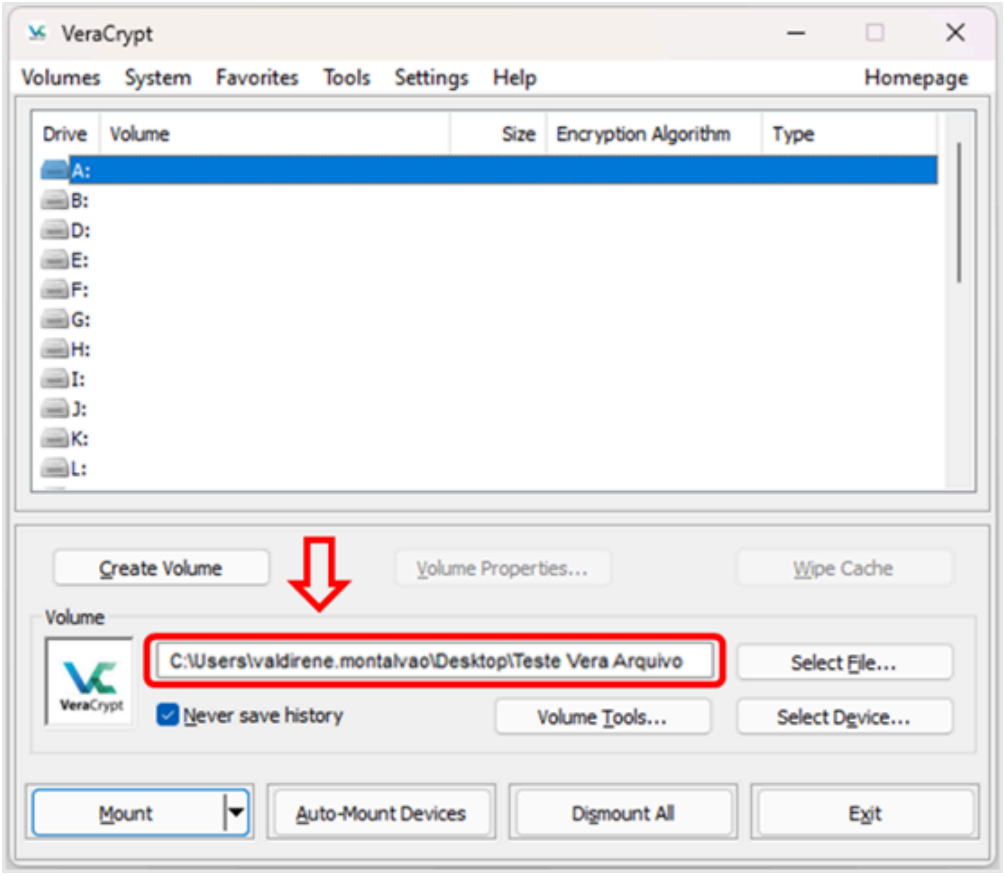
10.1. Abra o VeraCrypt e clique em "***Select File***";



10.2. Localize o volume criado anteriormente. No exemplo abaixo o volume se chama "***Teste Vera Arquivo***". Clique duas vezes sobre o arquivo;

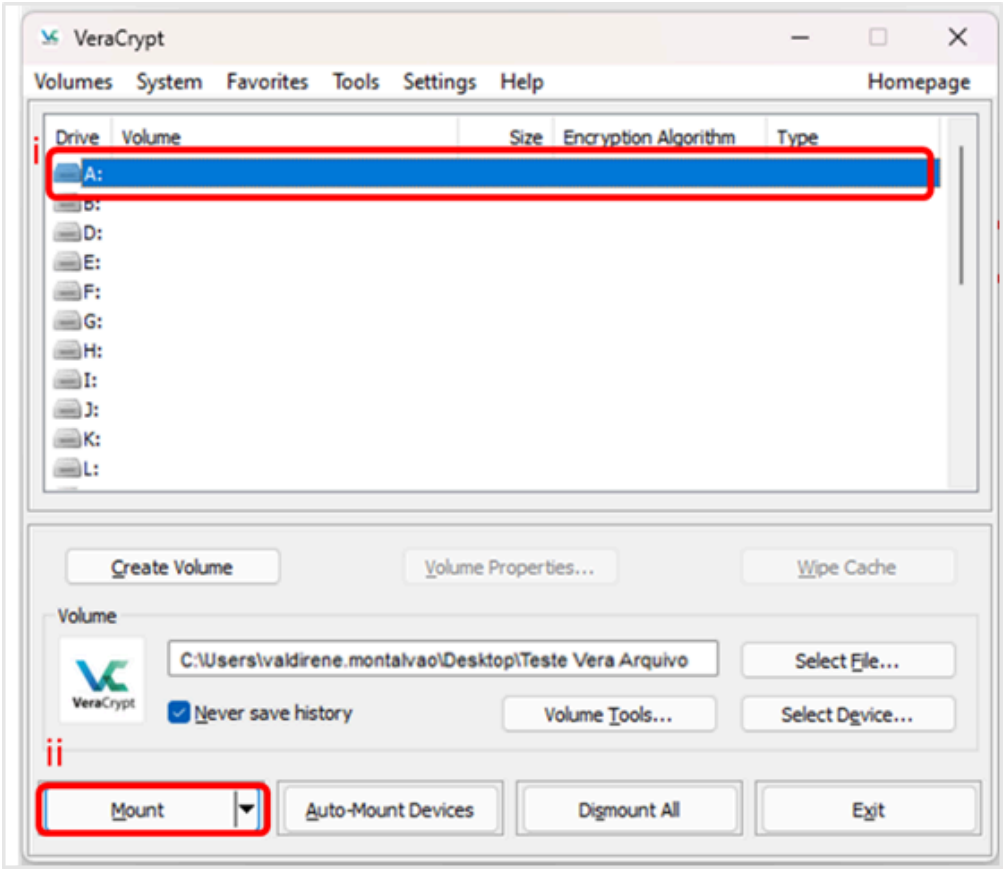


10.3. O volume será carregado na janela do Veracrypt;

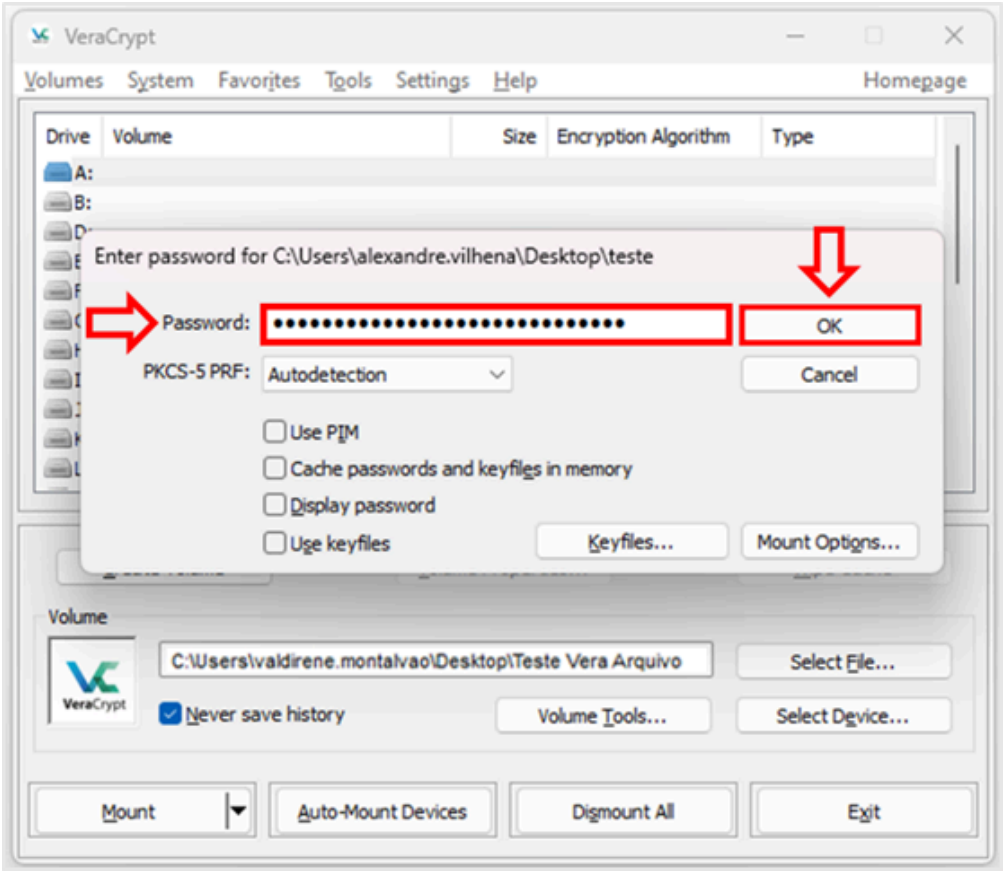


10.4. Selecione um diretório para colocar o volume criptografado importante definir sempre o mesmo driver para fim didáticos será selecionado o "***Drive A***", (i) clicando duas vezes sobre o mesmo ou (ii) selecionando e clicando em "***Mount***";

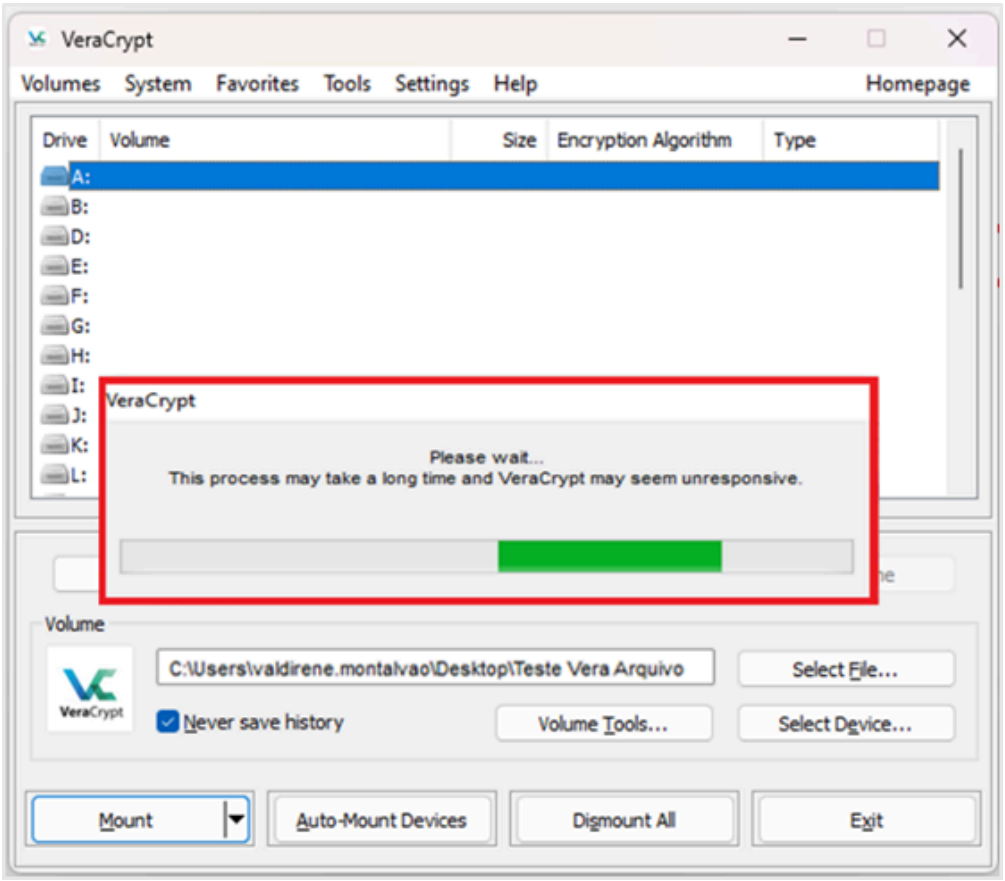
Obs: Por se tratar de uma criptografia para realização de processamento, é aconselhável que o diretório seja sempre o mesmo, no intuito de evitar a edição do caminho diretório de busca desse banco nos scripts de processamento.



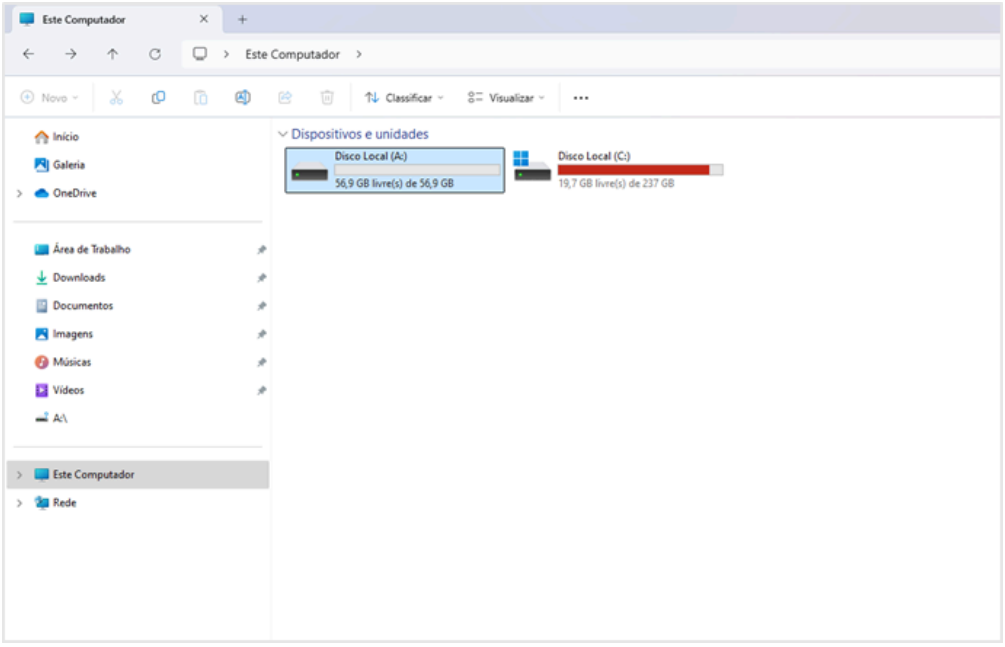
10.5. Digite a senha criada anteriormente e clique em "***OK***";



10.6. Aguarde o processamento;

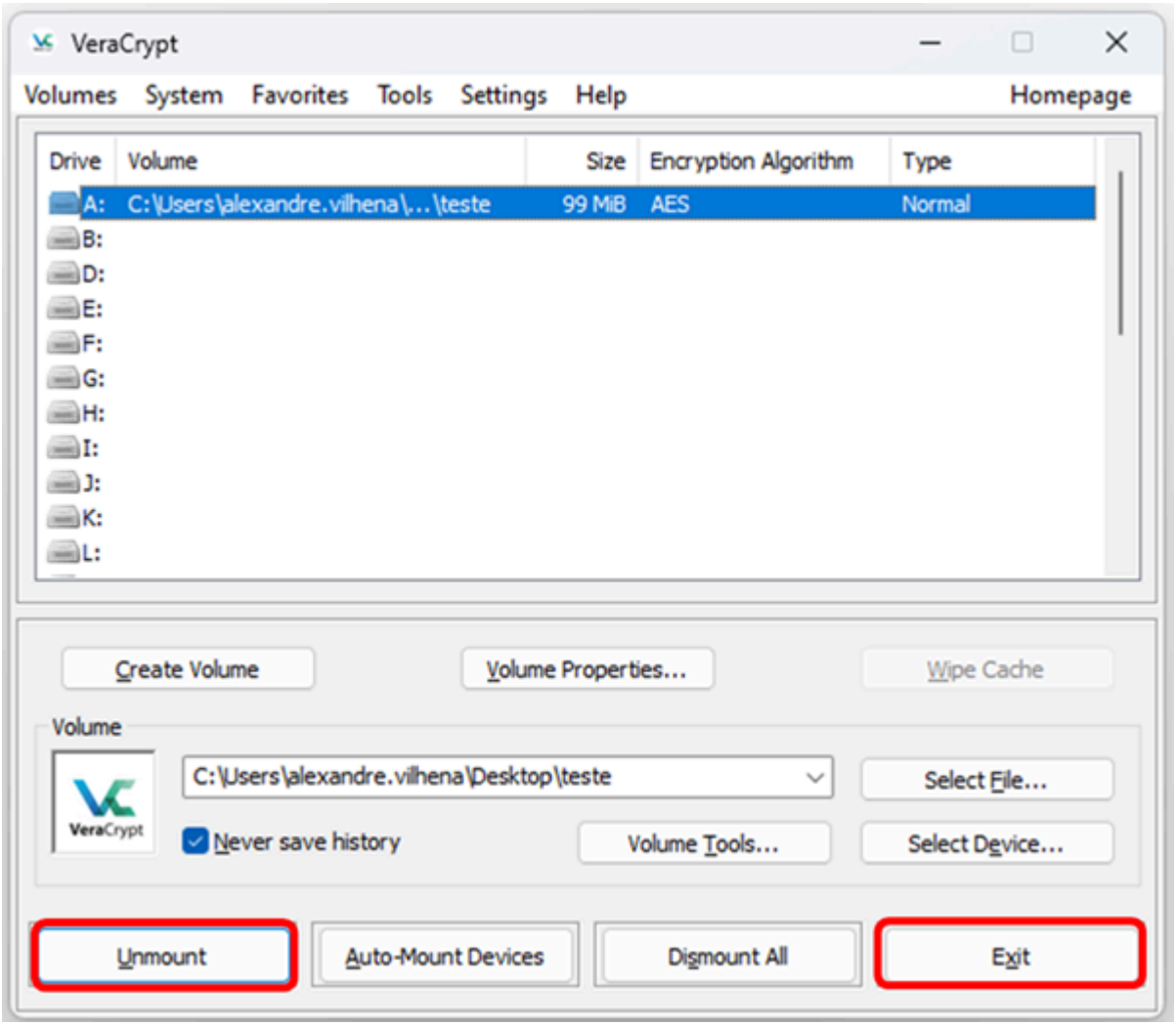


10.7. Abra o "***Explorer***" e em "***Este Computador***", este computador irá encontrar o drive criado, que para o fim didático utilizamos o "***Drive A:***", com o tamanho criado anteriormente e vazio;



10.8. Com o drive aberto, os dados serão aqui armazenados. Os scripts usados podem ser armazenados fora desse drive desde que não contenham nenhuma forma de identificar os titulares dos dados. Caso contrário o script também deverá ser armazenado no drive criptografado, assim como o copias e recortes do banco de dados deve ser direcionado para esse diretório;

10.9. Finalizando a atividade do dia na tela do VeraCrypt clique em "***unmount***", para que este diretório seja fechado, e posteriormente clicar em sair;



Brasília, 22 de julho de 2025.

Documento assinado eletronicamente por **Leticia de Oliveira Cardoso**, **Diretor(a) do Departamento de Análise Epidemiológica e Vigilância de Doenças não Transmissíveis**, em 14/08/2025, às 18:36, conforme horário oficial de Brasília, com fundamento no § 3º, do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020; e art. 8º, da Portaria nº 900 de 31 de Março de 2017.

Documento assinado eletronicamente por **Fabiano Geraldo Pimenta Junior**, **Secretário(a) de Vigilância em Saúde e Ambiente substituto(a)**, em 26/09/2025, às 04:06, conforme horário oficial de Brasília, com fundamento no § 3º, do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020; e art. 8º, da Portaria nº 900 de 31 de Março de 2017.

A autenticidade deste documento pode ser conferida no site http://sei.saude.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0049248423** e o código CRC **5217A589**.

Referência: Processo nº 25000.125910/2025-91 SEI nº 0049248423

Departamento de Análise Epidemiológica e Vigilância de Doenças não Transmissíveis - DAENT
SRTVN 701, Via W5 Norte Edifício PO700, 6º andar - Bairro Asa Norte, Brasília/DF, CEP 70723-040
Site - saude.gov.br