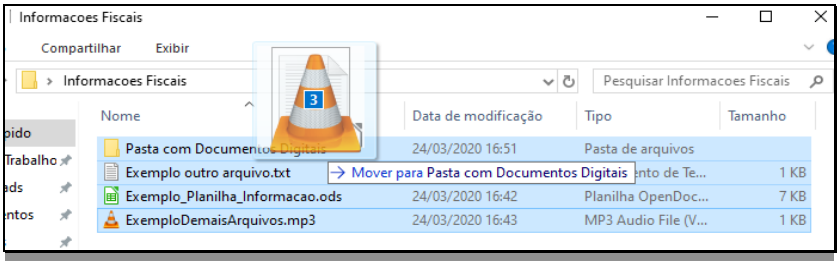
ANEXO ÚNICO

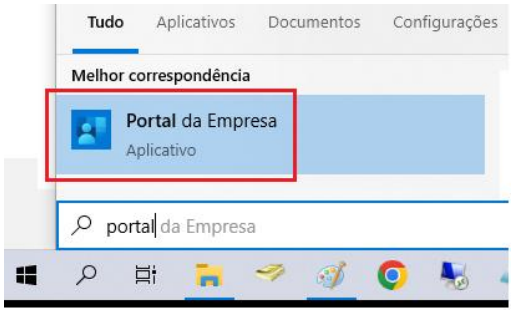
COMPACTAÇÃO E CRIPTOGRAFIA DE DOCUMENTO DIGITAL

MÉTODO 1 – USO DO VERACRYPT

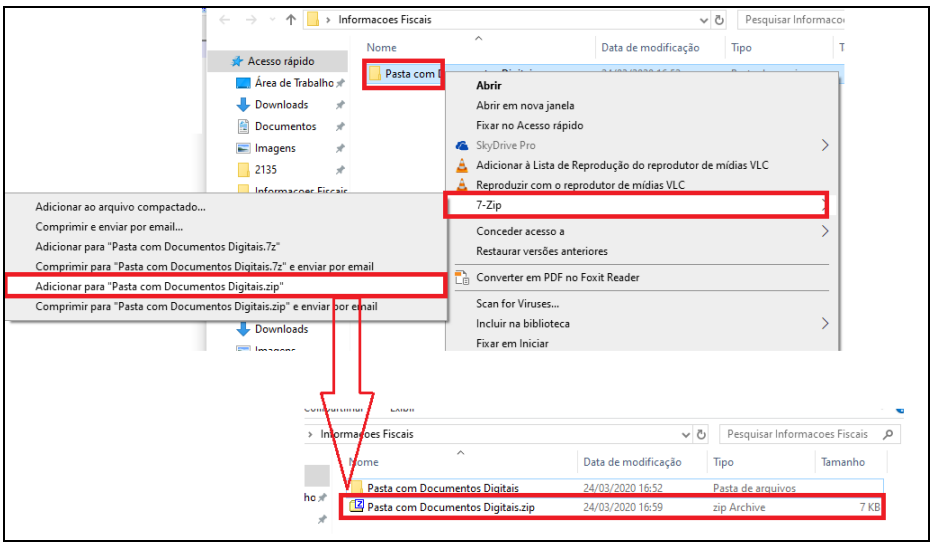
1. Antes de iniciar a compactação, se for o caso, e criptografia dos documentos digitais, recomenda-se a criação de uma pasta que receberá todos os documentos digitais. Neste exemplo, a pasta foi criada com o nome “Pasta com Documentos Digitais”.



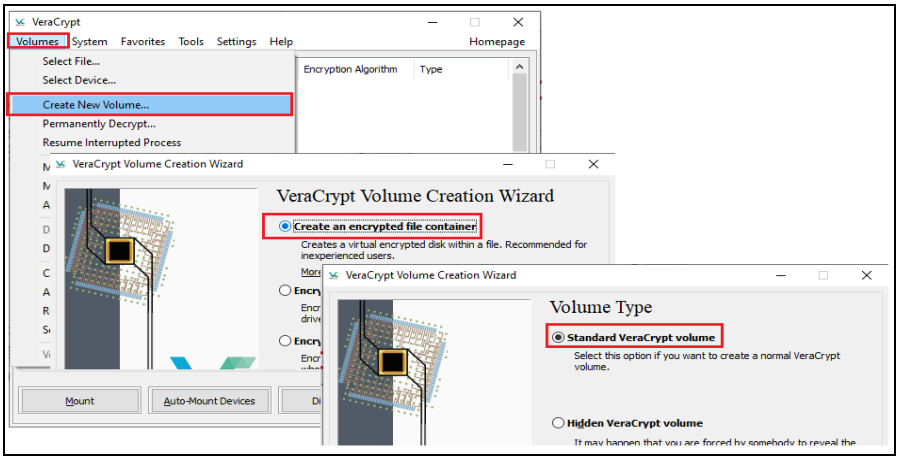
2. Caso o software 7-Zip não esteja instalado, solicite a instalação pelo Portal da Empresa:



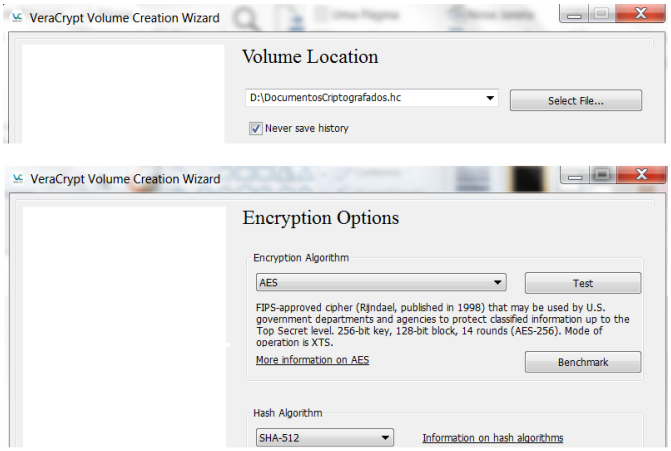
3. Clique com botão direito em cima da pasta com os documentos digitais, escolha a opção 7-Zip e, em seguida, selecione a opção “Adicionar para a ‘Pasta com Documentos Digitais.zip’”. Ao final do procedimento, será criado um arquivo compactado:



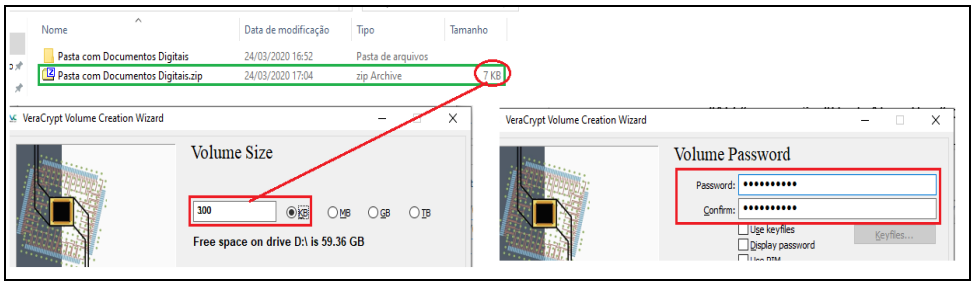
4. Para criptografia, é necessário ter o software Veracrypt instalado. Caso não tenha, solicite a instalação por meio do Portal da Empresa. Ao abrir o Veracrypt pela primeira vez, clique em “Volumes”; em seguida, em “Create New Volume”; selecione “Create an encrypted file container”; clique em “Next”; selecione “Standard VeraCrypt Volume”; e clique em “Next”.



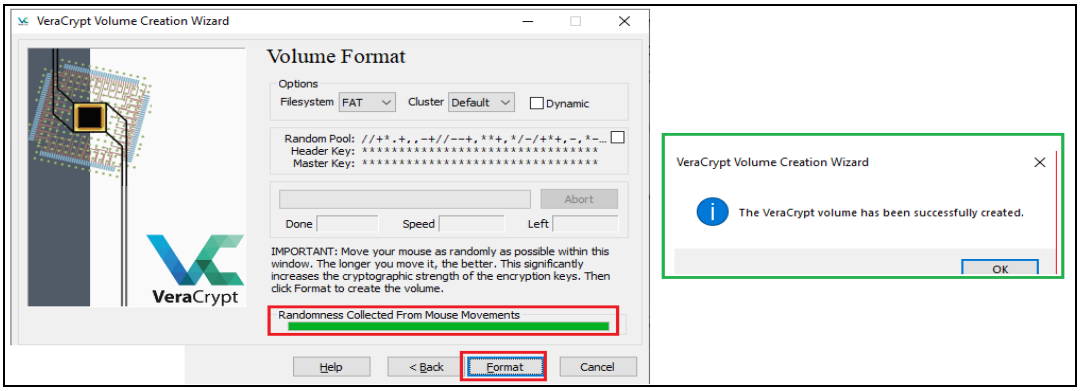
5. Em seguida, selecione uma unidade do seu computador para criar o Volume para armazenar os futuros arquivos criptografados. Nesse exemplo, foi criado o arquivo “Documentos Criptografados.hc” em “D:”. Defina a opção “Encryption Algorithm” com valor “AES” e a opção “Hash Algorithm” com valor “SHA-512”, em seguida, clique em “Next”.



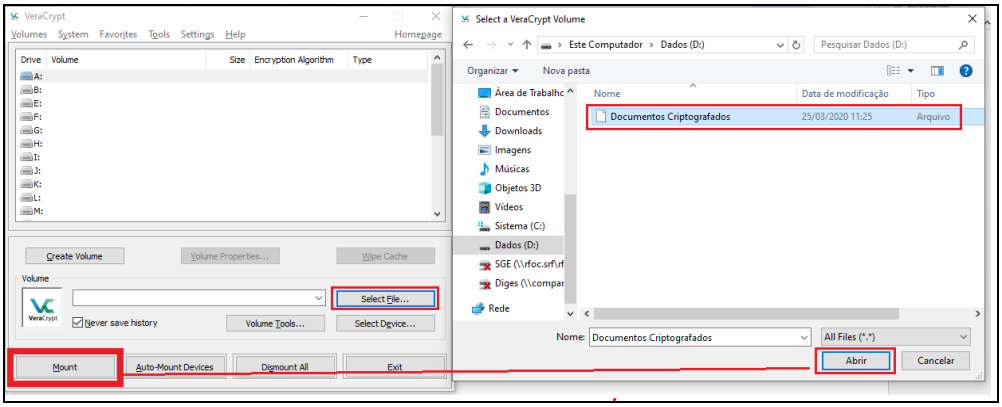
6. Defina um espaço de armazenamento para esse Volume (“Documentos Criptografados.hc”) que conterá os futuros arquivos criptografados, com base no arquivo a ser enviado ao destinatário, e clique em “Next”. Neste exemplo, o arquivo possui 7KB compactado, e, portanto, foi definido um espaço de armazenamento de 300 KB (por ser o tamanho mínimo). Defina a senha que protege esse volume e confirme essa senha, clicando em “Next” em seguida. **A senha deve conter letras maiúsculas e minúsculas, com caracteres especiais, números e com no mínimo 20 caracteres**, não sequenciais. Essa será a senha utilizada para Criptografia e Descriptografia.



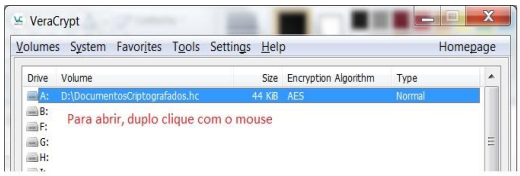
7. Na nova tela, faça movimentos aleatórios com o mouse até a barra de progresso ficar verde e, em seguida, clique em “Format”. Ao final, será exibida mensagem de confirmação. Clique em “Ok” e “Exit”.

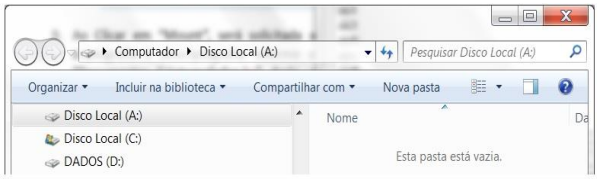


8. Finalizada a criação do Volume “Documentos Criptografados.hc”, o próximo passo é adicionar o arquivo digital compactado (“Pasta com Documentos Digitais.zip”) no Volume criptografado. Para isso, no Veracrypt, selecione o drive (drive A neste exemplo), clique em “Select File”, e abra o Volume “Documentos Criptografados” criado nas etapas anteriores. Após, clique em “Mount”.

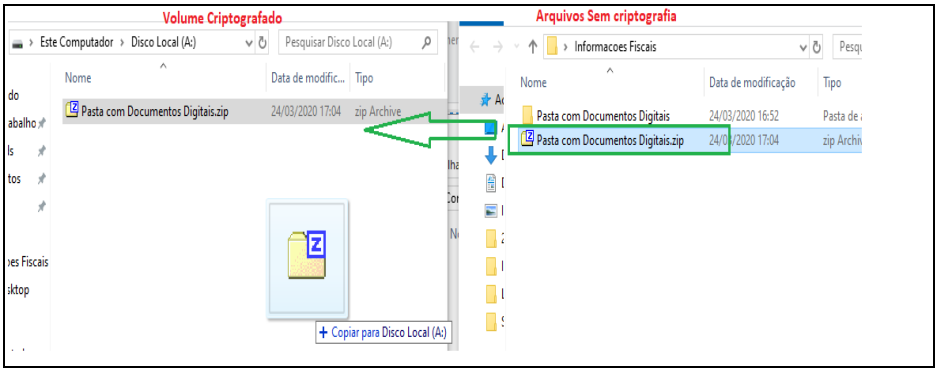


9. Ao Clicar em “Mount”, será solicitada a senha criada no passo 5. Essa é a senha de criptografia e descriptografia. Informe a senha. Após, será descriptografado o Volume “Documentos Criptografados.hc”. Após, abra o Volume para inserção do arquivo digital compactado para ser criptografado, conforme indicado na figura a seguir:





10. Aberto o drive (A neste exemplo), insira nele o arquivo digital compactado (“Pasta com Documentos Digitais.zip”). Após, retorne ao Veracrypt e clique em “Dismount”.



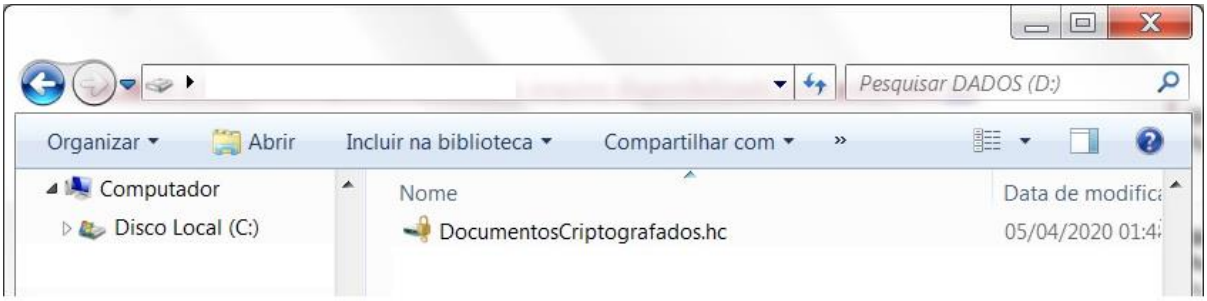
11. Realizados esses procedimentos, o Volume “Documentos Criptografados.hc” estará criptografado com os arquivos digitais compactados (“Pasta com Documentos Digitais.zip”) a ser enviado ao destinatário. A Senha criada no passo 5 deverá ser disponibilizada ao destinatário conforme procedimentos descritos no Anexo I ou de forma presencial.

12. O arquivo “Documentos Criptografados.hc” será enviado ao destinatário, que deverá ter o Veracrypt instalado para realizar a descriptografia com a utilização da senha disponibilizada.

PROCEDIMENTOS PARA AUXILIAR O DESTINATÁRIO

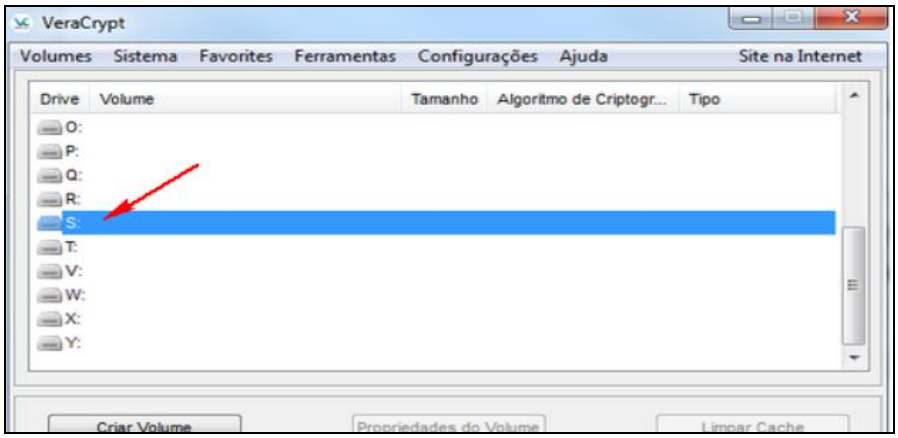
13. Instalar o VeraCrypt, caso não esteja instalado (http://www.veracrypt.fr)

14. Abrir o Windows Explorer e localizar o arquivo disponibilizado (com extensão.hc)

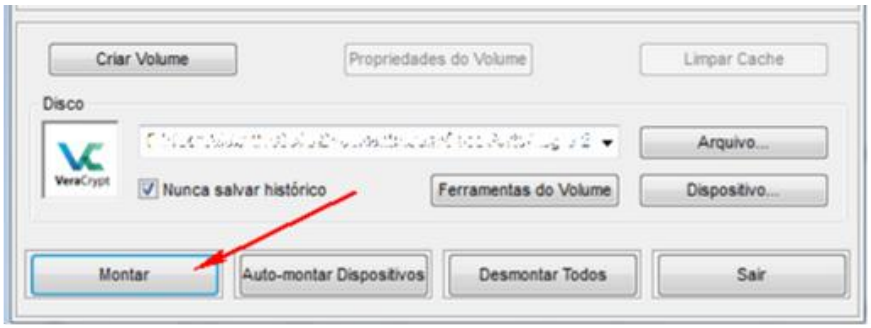


15. Clicar duas vezes no arquivo (se a extensão estiver associada corretamente no sistema operacional o VeraCrypt será aberto)

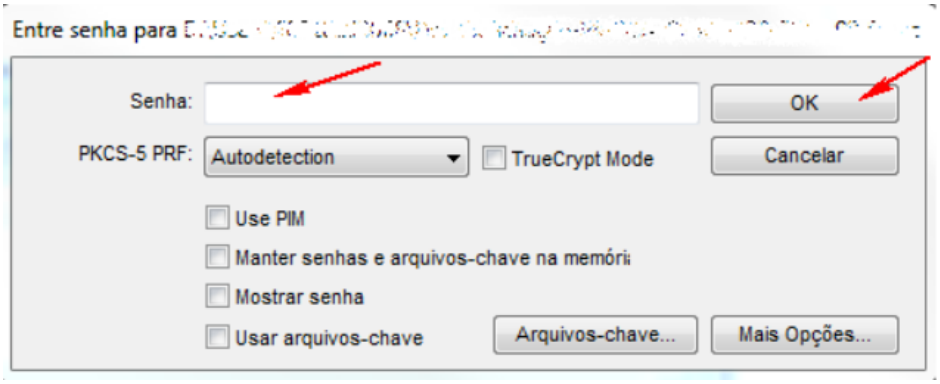
16. Se não aparecer uma letra (Drive) selecionada, clicar em uma (por exemplo, no S: ou T:)



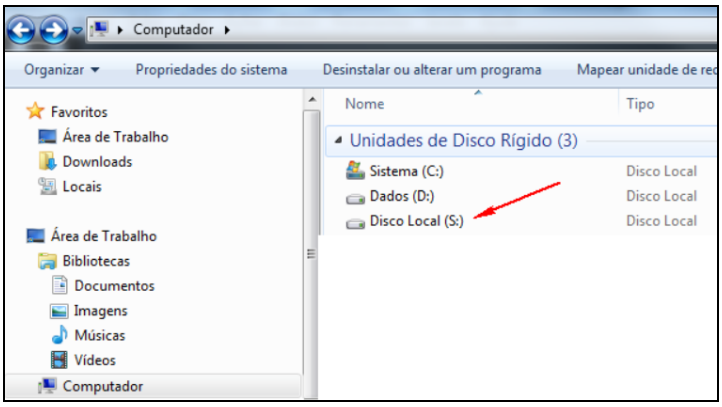
17. Clicar em Montar (deverá aparecer uma tela solicitando a senha).



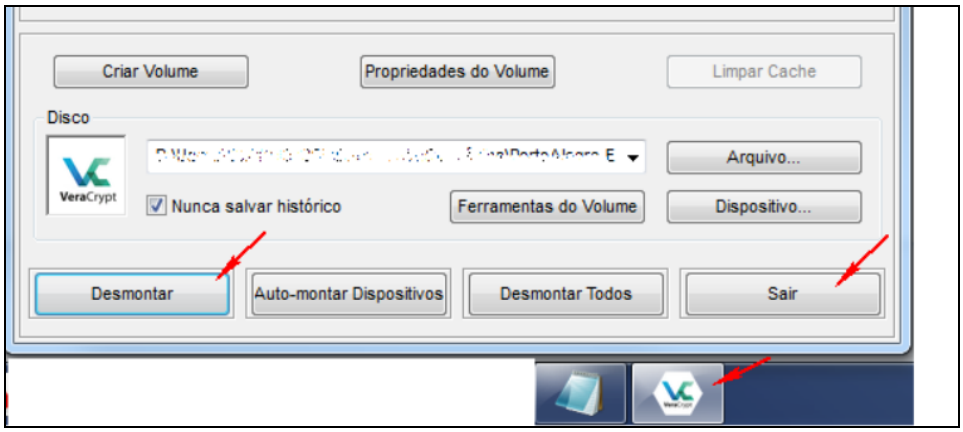
18. Abrir o arquivo que contém a senha e foi disponibilizado pela RFB.
19. Digitar a senha no campo "Senha:" do VeraCrypt e clicar em OK.



20. Minimizar o VeraCrypt.
21. Abrir o Windows Explorer e localizar a letra que foi selecionada anteriormente. Clicar na letra para acessar os arquivos.



22. Ao final da utilização dos arquivos, voltar ao VeraCrypt, clicar em “Desmontar” e depois em “Sair”.



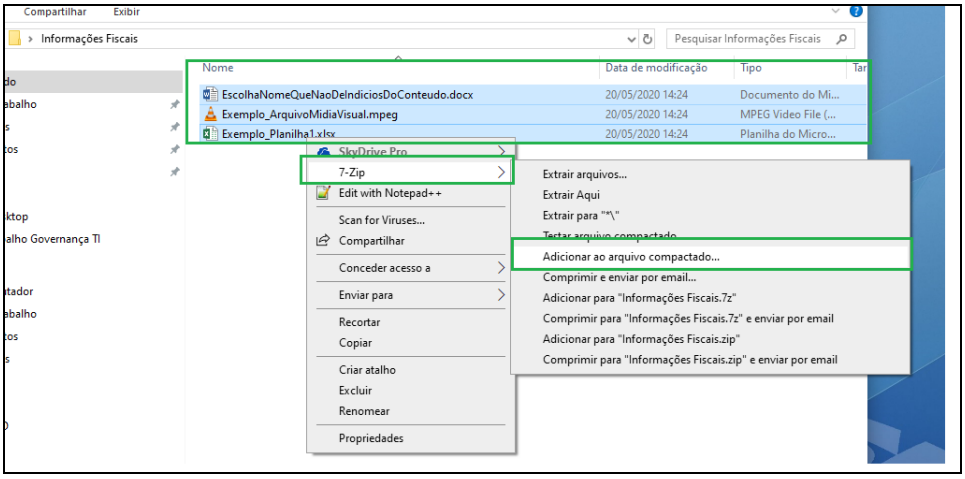
COMPACTAÇÃO E CRIPTOGRAFIA DE DOCUMENTO DIGITAL

MÉTODO 2 – USO DO 7-ZIP

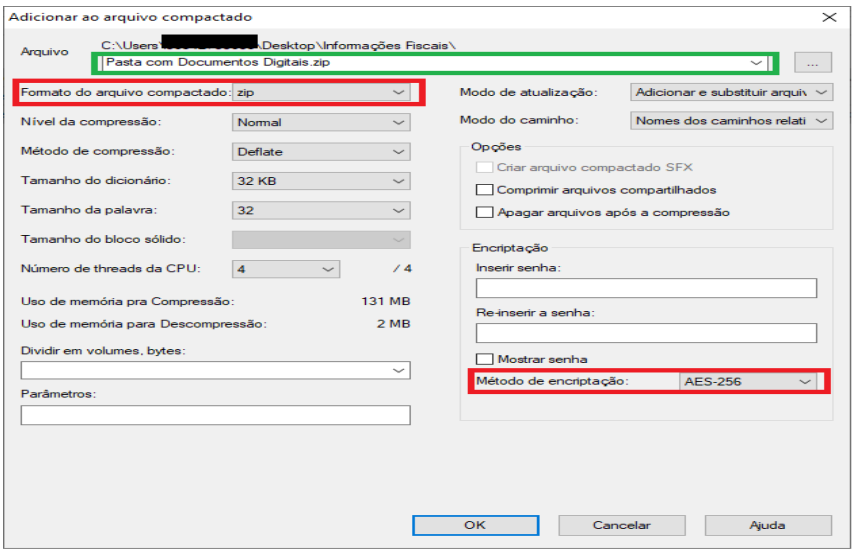
1. Para realizar a criptografia dos documentos digitais pelo Método 2, é necessário realizar a compactação, por meio do software 7-Zip. Caso não tenha instalado, solicite a instalação por meio do Portal da Empresa.

2. Selecione os documentos digitais com as informações sigilosas, clique com o botão direito, escolha a opção “7-Zip” e escolha a opção “Adicionar ao arquivo compactado”.

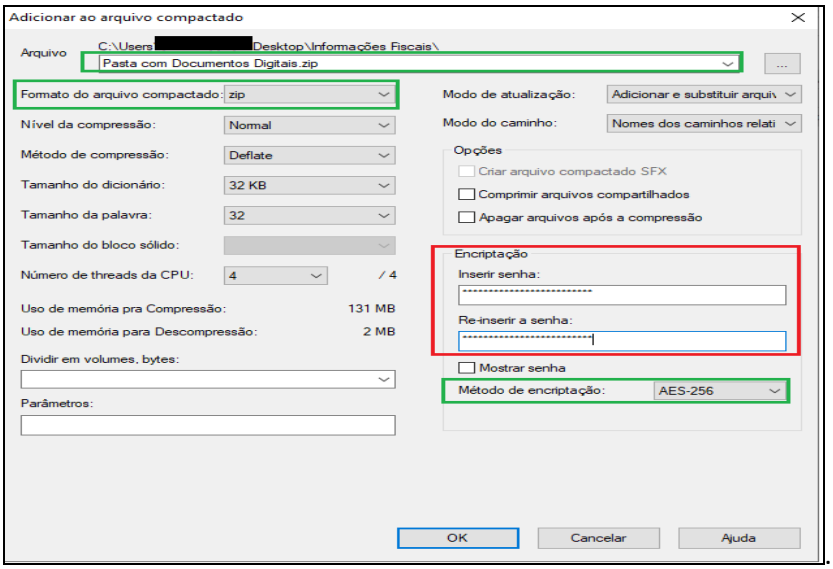
Importante: Escolha nomes para os documentos digitais com informações sigilosas que não guardem relação com os respectivos conteúdos.



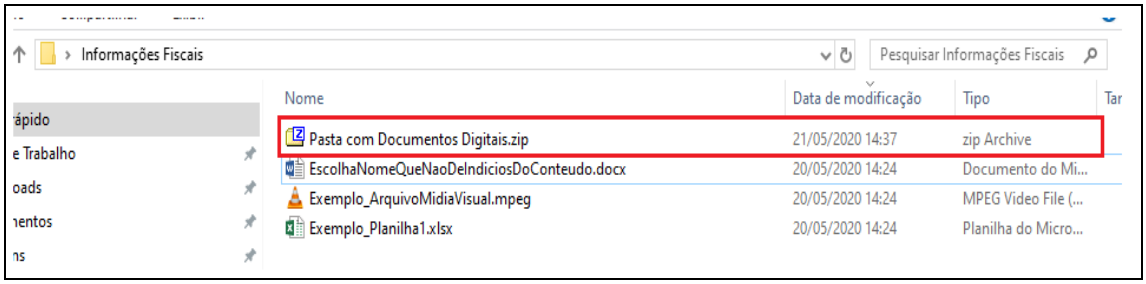
3. Na janela que se abriu, defina o nome para o arquivo digital compactado. Neste exemplo, foi utilizado Pasta com Documentos Digitais.zip. Modifique a opção “formato do arquivo compactado para “zip”. Modifique também que a opção método de encriptação para “AES-256”.



4. Em seguida, defina **e insira a senha de 20 caracteres**, no mínimo, que contenha letras maiúsculas e minúsculas, com caracteres especiais e números. Em seguida, insira novamente a senha e selecione “OK”



5. Realizados esses procedimentos, será criado o arquivo digital compactado e criptografado com o nome “Pasta com Documentos Digitais.zip a ser enviado ao destinatário. A Senha criada no passo 4 deverá ser disponibilizada ao destinatário conforme procedimentos descritos no Anexo I ou de forma presencial.

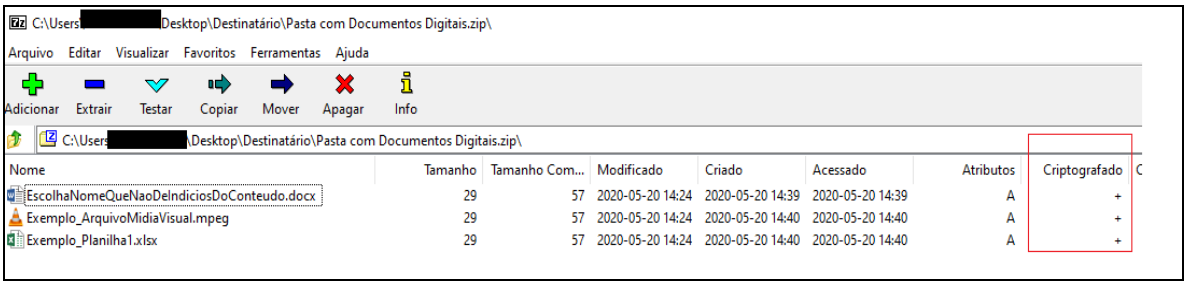


6. O arquivo “Pasta com Documentos Digitais. zip” será enviado ao destinatário, que deverá ter o software 7-Zip ou Winzip ou PKZip instalado para realizar a descriptografia com a utilização da senha disponibilizada.

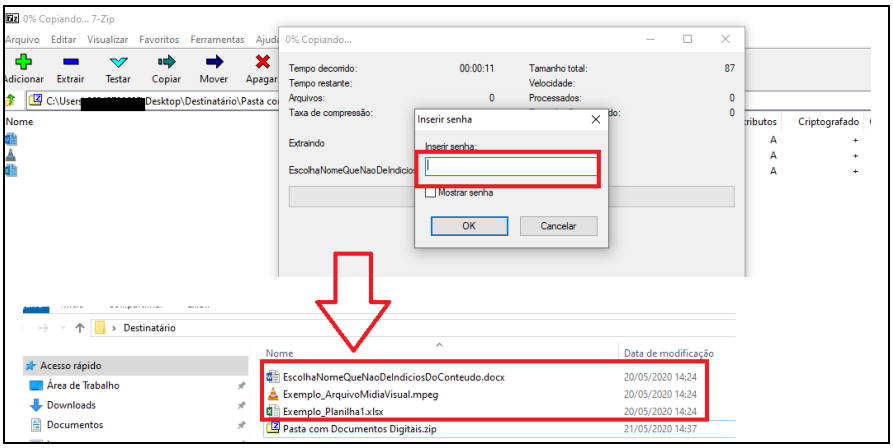
PROCEDIMENTOS PARA AUXILIAR O DESTINATÁRIO

7. Instale o software 7-Zip, caso não esteja instalado (https://www.7-zip.org/). Em regra, esse procedimento também pode ser executado com softwares como Winzip, PKZip e demais do gênero.

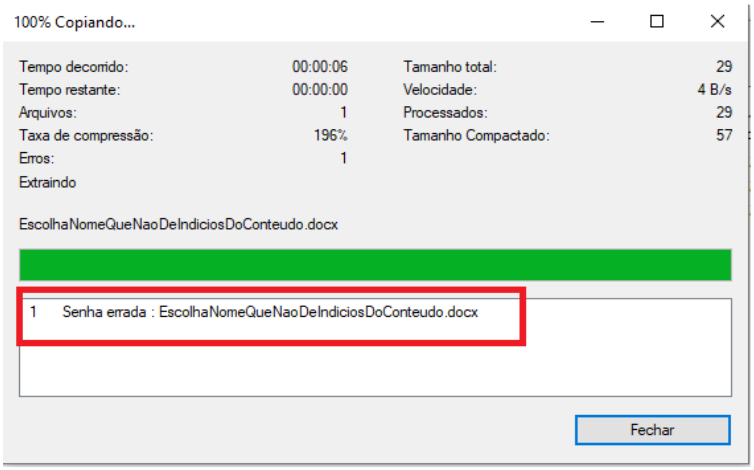
8. Localize o arquivo digital compactado e criptografado recebido, clique duas vezes no arquivo. Na nova janela, será apresentada a lista dos documentos digitais.



9. Clique duas vezes no arquivo que se deseja abrir ou selecione os arquivos e escolha a opção “Extrair”. Será solicitado informar a senha para descriptografia enviada pela Receita Federal. Informando a senha correta, o arquivo será descriptografado e descompactado.



10. Informando a senha incorreta, será apresentada mensagem de erro.

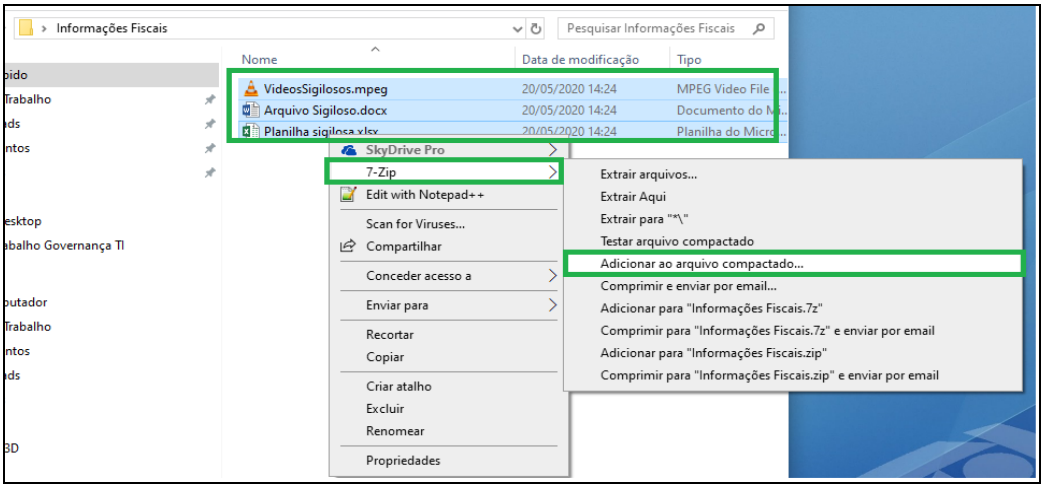


COMPACTAÇÃO E CRIPTOGRAFIA DE DOCUMENTO DIGITAL

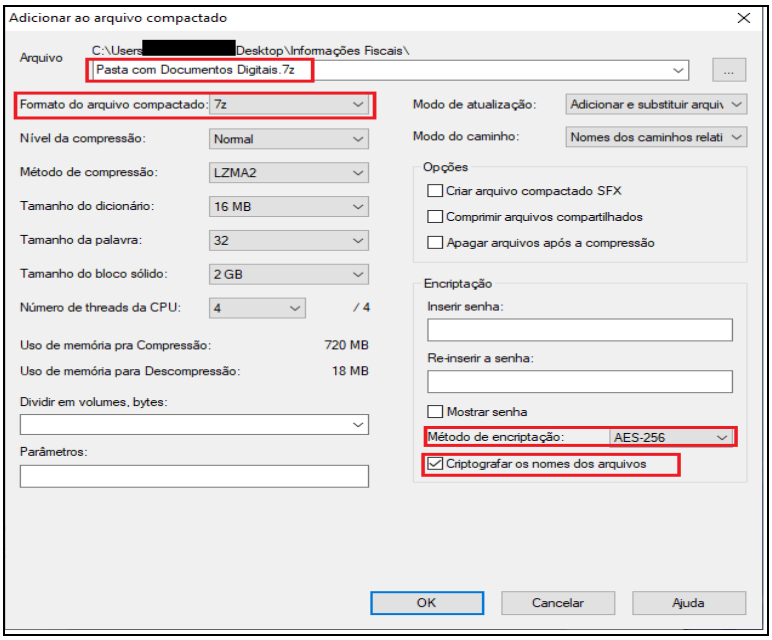
MÉTODO 3 - USO DO 7-ZIP

1. Para realizar a criptografia dos documentos digitais pelo Método 3, é necessário realizar a compactação, por meio do software 7-Zip. Caso não tenha instalado, solicite a instalação por meio Portal da Empresa.

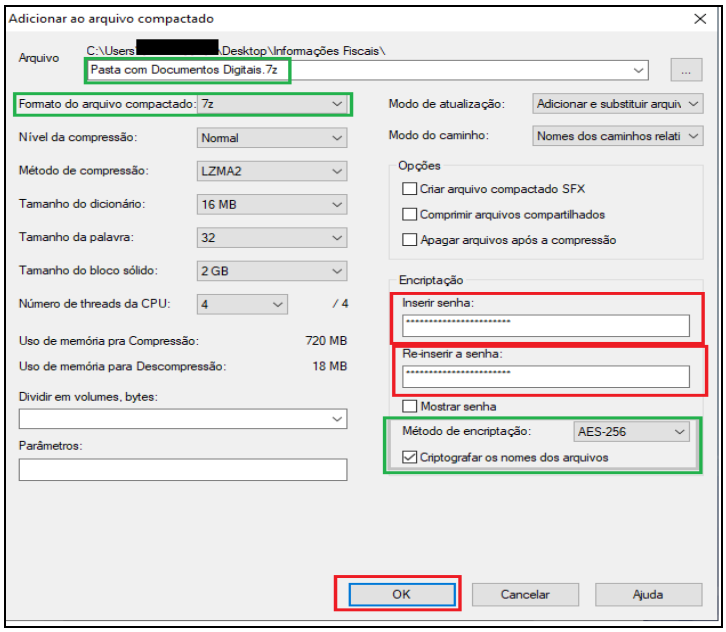
2. Selecione os documentos digitais com as informações sigilosas, clique com o botão direito, escolha a opção "7-Zip" e escolha a opção "Adicionar ao arquivo compactado".



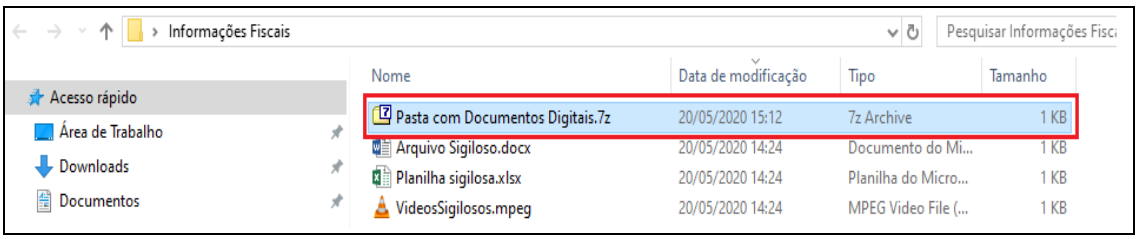
3. Na janela que se abriu, defina o nome para o arquivo digital compactado. Neste exemplo, foi utilizado Pasta com Documentos Digitais.7z. Certifique-se que a opção “formato do arquivo compactado seja “7z”. Certifique-se também que a opção método de encriptação seja “AES-256” e que a opção “Criptografar os nomes dos arquivos” esteja selecionada.



4. Em seguida, **defina e insira a senha de 20 caracteres**, no mínimo, que contenha letras maiúsculas e minúsculas, com caracteres especiais e números. Em seguida, insira novamente a senha e selecione “OK”.



5. Realizados esses procedimentos, será criado o arquivo digital compactado e criptografado com o nome “Pasta com Documentos Digitais.7z” a ser enviado ao destinatário. A Senha criada no passo 4 deverá ser disponibilizada ao destinatário conforme procedimentos descritos no Anexo I ou de forma presencial.

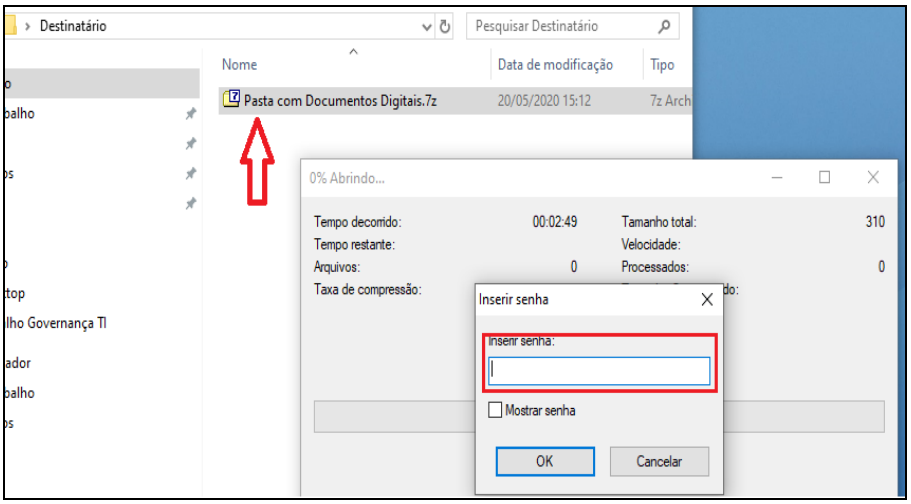


6. O arquivo “Pasta com Documentos Digitais.7z” será enviado ao destinatário, que deverá ter o software 7-Zip instalado para realizar a descriptografia com a utilização da senha disponibilizada.

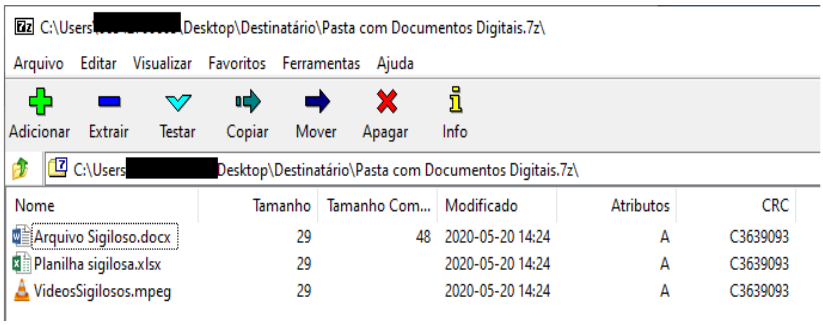
PROCEDIMENTOS PARA AUXILIAR O DESTINATÁRIO

7. Instale o software 7-Zip, caso não esteja instalado (https://www.7-zip.org/)

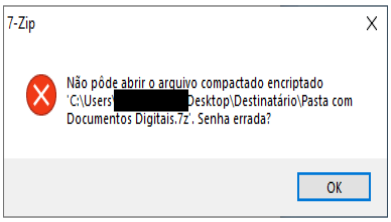
8. Localize o arquivo digital compactado e criptografado recebido, clique duas vezes no arquivo. Na nova janela, será solicitado informar a senha para descriptografia do arquivo.



9. Informando a senha correta, o arquivo será descriptografado e descompactado.



10. Informando a senha incorreta, será apresentada mensagem de erro.



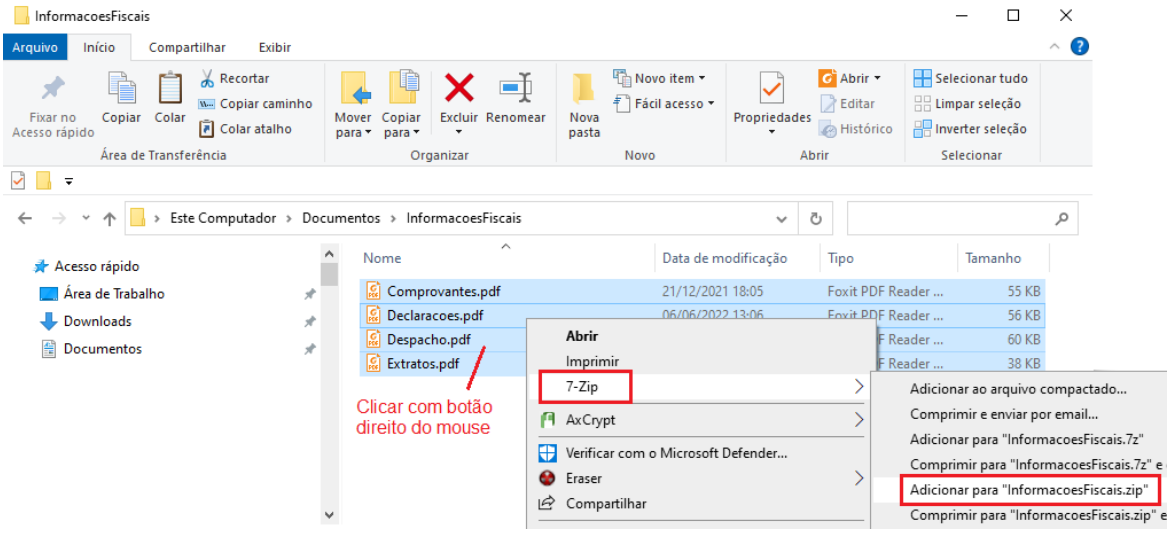
COMPACTAÇÃO E CRIPTOGRAFIA DE DOCUMENTO DIGITAL

MÉTODO 4 - USO DO BITLOCKER – PARA PENDRIVE OU HD

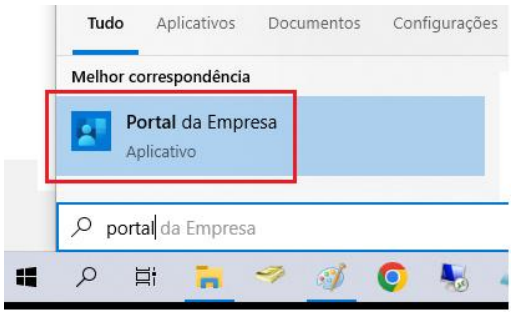
Compactação dos arquivos

1. Antes de iniciar a compactação, se for o caso, e criptografia dos documentos digitais, recomenda-se a criação de uma pasta que receberá todos os documentos digitais. Neste exemplo, a pasta foi criada com o nome “InformacoesFiscais”.

2. Clique com botão direito nos arquivos e pastas com os documentos digitais, escolha a opção 7-Zip e, em seguida, a opção “Adicionar para a ‘InformacoesFiscais.zip’” conforme exemplo. Ao final do procedimento, será criado um arquivo compactado.



3. Caso o software 7-Zip não esteja instalado, solicite a instalação pelo Portal da Empresa.



Solicitação do perfil “Criptografia BitLocker”

4. Para gravar dados em mídias removíveis no ambiente da RFB, o servidor deve possuir o perfil “Criptografia BitLocker” no sistema “Escrita Mídia Removível”. Esse perfil deve ser solicitado por meio do sistema eletrônico de controle de solicitações de cadastramento e habilitação de usuários da RFB (e-Fau), com o preenchimento do formulário conforme segue:

Tipo da solicitação: Habilitação

Solicitação de: Sistema

Segmento: WINDOWS

Ambiente: PRODUÇÃO

Sistema: Escrita Mídia Removível

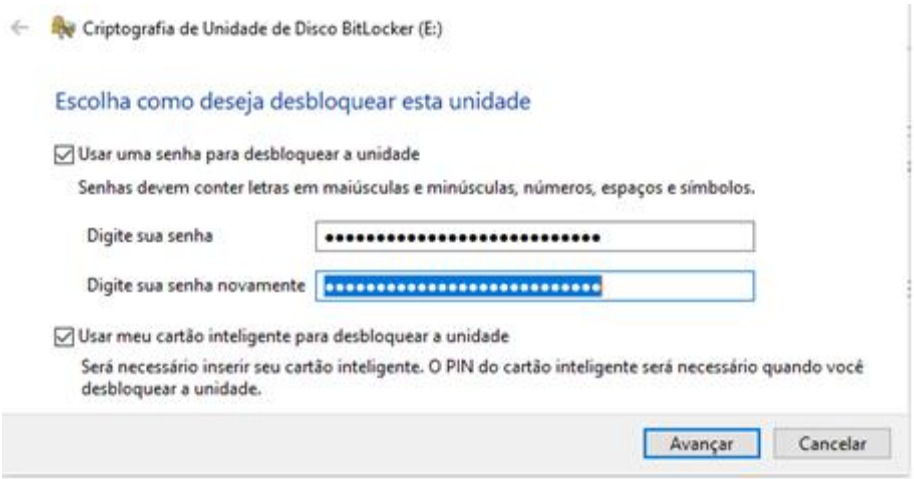
Perfil: Criptografia BitLocker

Gravação de arquivos em mídias removíveis

5. Para gravar arquivos em mídias removíveis, é necessário criptografar a mídia removível. Para criptografar a mídia removível em seu primeiro uso, siga os passos abaixo:

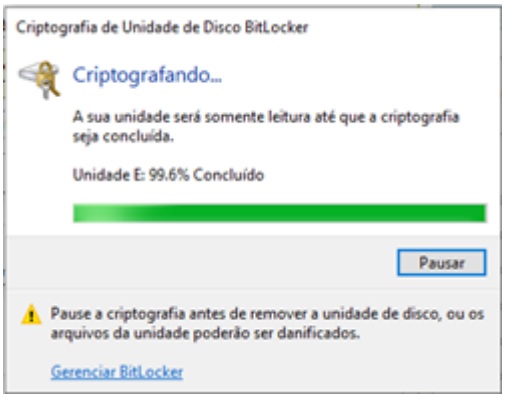
A. Conecte a mídia removível à porta USB do computador. Na mensagem que será exibida, selecione a opção “Criptografar esta unidade usando a Criptografia de Disco BitLocker”:

B. Na tela seguinte, informe uma senha para a mídia removível. A senha será utilizada para desbloquear a mídia, mesmo em casos de perda, extravio, furto, renovação ou bloqueio do token (certificado digital). A senha deverá ter, **no mínimo, 20 caracteres, entre letras maiúsculas, minúsculas, números e caracteres especiais**. Preenchidas e selecionadas as opções, clique em “Avançar”:



C. Clique em “Iniciar a Criptografia”:

D. O sistema exibirá uma tela de progresso da criptografia até informar “Criptografia concluída”:



E. A mídia removível está pronta para gravação e pode ser utilizada normalmente por meio do Windows Explorer.

Obs.1: Após a conclusão desse procedimento, as mídias removíveis criptografadas aparecem no Windows Explorer com um símbolo de cadeado.

Obs.2: É possível realizar o procedimento em mídias removíveis que já contenham dados.

Obs.3: No caso de preparação da mídia, deve-se utilizar a opção “Usar uma senha para desbloquear a unidade”. Esta será a senha prevista no art. 9º da Portaria. A senha deve conter letras maiúsculas e minúsculas, com caracteres especiais, números e com no mínimo 20 caracteres, não sequenciais. Essa será a senha utilizada para desbloquear o acesso à mídia pelo BitLocker.

Obs.4: Caso necessite suporte, abra um chamado via SoliCorp (Tema “Estação de Trabalho, Periféricos e Atendimento Remoto”, Serviço “Atendimento remoto a computador/notebook ou periféricos e a instalação de software”).

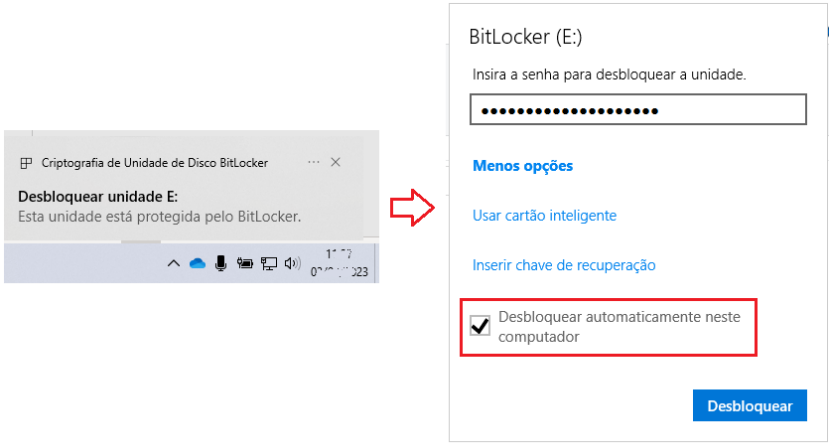
6. Copiar os arquivos para o pendrive ou HD criptografado e remover o dispositivo da estação de trabalho.

Disponibilização da senha

7. A senha criada no passo 5 deverá ser disponibilizada ao destinatário conforme procedimentos descritos no Anexo I ou de forma presencial.

PROCEDIMENTOS PARA AUXILIAR O DESTINATÁRIO

8. Conectar a mídia removível (pendrive ou HD) na estação de trabalho com Windows 7 ou superior.
9. O Windows deve mostrar uma mensagem para desbloquear a mídia conforme tela abaixo. Digitar a senha informada pela Receita Federal. Se for seguro manter a mídia liberada na estação em uso, selecionar “Desbloquear automaticamente neste computador”:



10. Se a mensagem apresentada no item 9 não aparecer, deve-se abrir o Windows Explorer, localizar a mídia, clicar com o botão direito do mouse e selecionar a opção “Desbloquear Unidade”. Seguir o previsto no item 9.

NOTA SOBRE O BITLOCKER

O BitLocker é uma ferramenta de criptografia da Microsoft disponível no sistema operacional Windows a partir da versão 7. O Linux não possui compatibilidade nativa com o BitLocker, mas existem pacotes que permitem acessar as mídias criptografadas como, por exemplo, o Dislocker. A gravação de dados em mídias removíveis na RFB exige a criptografia prévia da mídia, com algumas exceções.