 Confidencialidade	Tipo de Documento:	Procedimento
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Procedimento para Uso de Criptografia

Sumário

1.	OBJETIVO.....	1
2.	ÂMBITO DE APLICAÇÃO	1
3.	DEFINIÇÕES.....	1
4.	DOCUMENTOS DE REFERÊNCIA	2
5.	RESPONSABILIDADES.....	2
6.	REGRAS BÁSICAS.....	2
7.	CONTROLE DE REGISTROS	29
8.	ANEXOS.....	29
9.	REGISTRO DE ALTERAÇÕES.....	29

1. OBJETIVO

Esta norma tem o objetivo de assegurar o uso efetivo e adequado da criptografia para proteger a confidencialidade, autenticidade e/ou a integridade da informação.

2. ÂMBITO DE APLICAÇÃO

2.1. Empresa

Esta norma é aplicável ao **Grupo CPFL Energia** e a todas as suas controladas diretas e/ou indiretas, excetuadas as empresas com modelo de gestão e governança próprio.


2.2. Área

Todas as áreas do **Grupo CPFL Energia**.

3. DEFINIÇÕES

- **CERTIFICADO DIGITAL:** O Certificado Digital é a identidade digital da pessoa física e jurídica no meio eletrônico.
- **BITLOCKER:** O BitLocker é a ferramenta de criptografia da Microsoft, disponível no Windows Vista, Windows 7, Windows 8 e Windows 10.
- **ASSINATURA DIGITAL:** A assinatura eletrônica permite que você assine um documento em meio digital.

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18934	Instrução	1.0	Emerson Cardoso	08/09/2021	1 de 29

 Confidencialida	Tipo de Documento:	Procedimento
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Procedimento para Uso de Criptografia

- **DATA ENCRYPTION KEY (DEK):** Chave que é utilizada para criptografar os dados, sejam eles arquivos de um sistema de arquivos, dados trafegando em uma conexão entre duas máquinas ou registros de um banco de dados, por exemplo.
- **KEY ENCRYPTION KEY (KEK):** Chave que é utilizada para criptografar uma outra chave. Muito utilizada em criptografia híbrida, onde a KEK criptografa a DEK e a DEK criptografa os dados.

4. DOCUMENTOS DE REFERÊNCIA

- ABNT/ISO 27001-2013;
- ABNT/ISO 27002-2013;
- Política de Segurança da Informação do **Grupo CPFL Energia**;
- Norma de Classificação da Informação do **Grupo CPFL Energia**;
- Código de Ética e de Conduta Empresarial do **Grupo CPFL Energia**;
- Esta Norma é complementada pela Política, e demais Normas e Procedimentos do **Grupo CPFL Energia**.


5. RESPONSABILIDADES

- **Infraestrutura**
Implementar os controles criptográficos definidos, além disso recomendar novas tecnologias e atualizar este documento sempre que aplicável. Cabe também a infraestrutura do **Grupo CPFL Energia** manter a infraestrutura de chaves necessária, bem como os softwares necessários e instruções detalhadas nos servidores de rede para que a criptografia possa ser realizada.
- **Segurança da Informação**
Selecionar os algoritmos, protocolos, processos e tecnologias utilizadas para se obter uma proteção eficiente da informação através do uso de criptografia forte, além de assegurar a confidencialidade das chaves utilizadas.
- **Desenvolvimento**
Desenvolver e manter as aplicações de acordo com as especificações.

6. REGRAS BÁSICAS

Criptografia é um recurso que é amplamente utilizado com o intuito de evitar invasões de pessoas mal-intencionadas às mensagens e arquivos salvos em diferentes formatos. A criptografia também é eficiente para impossibilitar o roubo de dados ou de senhas que circulam em dispositivos computacionais com acesso à Internet. O uso desse poderoso mecanismo de

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18934	Instrução	1.0	Emerson Cardoso	08/09/2021	2 de 29

 Confidencialidade	Tipo de Documento:	Procedimento
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Procedimento para Uso de Criptografia

segurança pode ocorrer em diversas ocasiões em que haja a necessidade de proteção do usuário da rede.

Por meio do uso da criptografia você pode:

- ✓ Proteger os dados sigilosos armazenados em seu computador, como o seu arquivo de senhas e a sua declaração de Imposto de Renda;
- ✓ Criar uma área (partição) específica no seu computador, na qual todas as informações que forem lá gravadas serão automaticamente criptografadas;
- ✓ Proteger seus backups contra acesso indevido, principalmente aqueles enviados para áreas de armazenamento externo de mídias;
- ✓ Proteger as comunicações realizadas pela Internet, como os e-mails enviados/recebidos e as transações bancárias e comerciais realizadas.

Termos geralmente utilizados quando falamos de criptografia na tabela abaixo:


Termo	Significado
Texto claro	Informação legível (original) que será protegida, ou seja, que será codificada
Texto codificado (cifrado)	Texto ilegível, gerado pela codificação de um texto claro
Codificar (cifrar)	Ato de transformar um texto claro em um texto codificado
Decodificar (decifrar)	Ato de transformar um texto codificado em um texto claro
Método criptográfico	Conjunto de programas responsável por codificar e decodificar informações
Chave	Similar a uma senha, é utilizada como elemento secreto pelos métodos criptográficos. Seu tamanho é geralmente medido em quantidade de <i>bits</i>
Canal de comunicação	Meio utilizado para a troca de informações
Remetente	Pessoa ou serviço que envia a informação
Destinatário	Pessoa ou serviço que recebe a informação

6.1 Assinatura digital

A assinatura digital permite comprovar a autenticidade e a integridade de uma informação, ou seja, que ela foi realmente gerada por quem diz ter feito isto e que ela não foi alterada.

A assinatura digital baseia-se no fato de que apenas o dono conhece a chave privada e que, se ela foi usada para codificar uma informação, então apenas seu dono poderia ter feito isto. A verificação da assinatura é feita com o uso da chave pública, pois se o texto foi codificado com a chave privada, somente a chave pública correspondente pode decodificá-lo.

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18934	Instrução	1.0	Emerson Cardoso	08/09/2021	3 de 29

 Confidencialidade	Tipo de Documento:	Procedimento
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Procedimento para Uso de Criptografia

Para contornar a baixa eficiência característica da criptografia de chaves assimétricas, a codificação é feita sobre o hash e não sobre o conteúdo em si, pois é mais rápido codificar o hash (que possui tamanho fixo e reduzido) do que a informação toda.

6.2 Certificado digital

A chave pública pode ser livremente divulgada. Entretanto, se não houver como comprovar a quem ela pertence, pode ocorrer de você se comunicar, de forma cifrada, diretamente com um impostor.

Um impostor pode criar uma chave pública falsa para um amigo seu e enviá-la para você ou disponibilizá-la em um repositório. Ao usá-la para codificar uma informação para o seu amigo, você estará, na verdade, codificando-a para o impostor, que possui a chave privada correspondente e conseguirá decodificar. Uma das formas de impedir que isto ocorra é pelo uso de certificados digitais.

O certificado digital é um registro eletrônico composto por um conjunto de dados que distingue uma entidade e associa a ela uma chave pública. Ele pode ser emitido para pessoas, empresas, equipamentos ou serviços na rede (por exemplo, um site Web) e pode ser homologado para diferentes usos, como confidencialidade e assinatura digital.

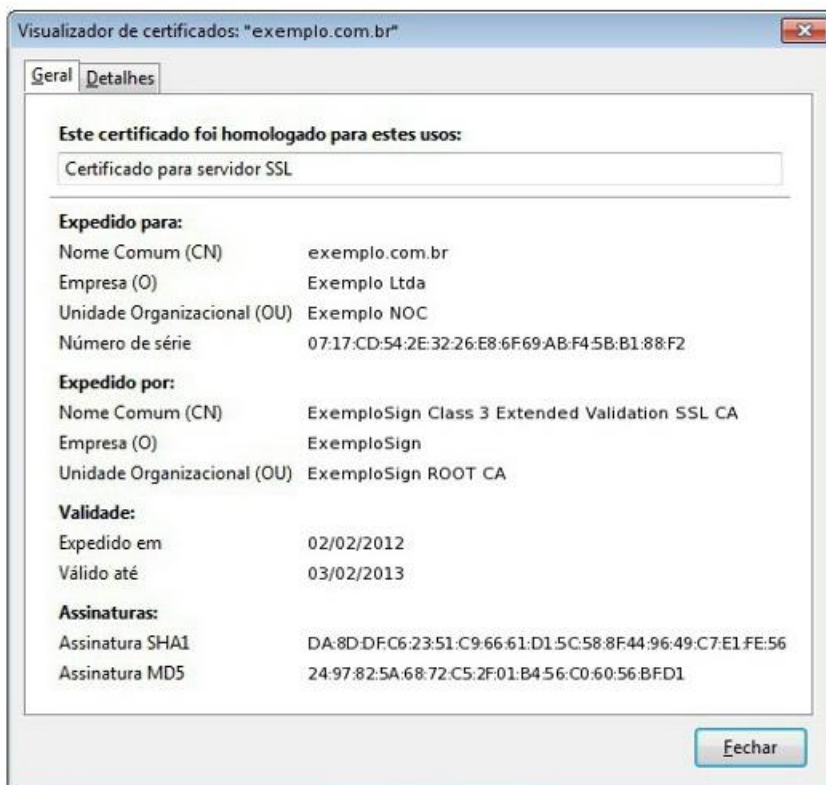
Um certificado digital pode ser comparado a um documento de identidade, por exemplo, o seu passaporte, no qual constam os seus dados pessoais e a identificação de quem o emitiu. No caso do passaporte, a entidade responsável pela emissão e pela veracidade dos dados é a Polícia Federal. No caso do certificado digital esta entidade é uma Autoridade Certificadora (AC).

6.3 AC emissora é também responsável por publicar informações sobre certificados que não são mais confiáveis. Sempre que a AC descobre ou é informada que um certificado não é mais confiável, ela o inclui em uma "lista negra", chamada de "Lista de Certificados Revogados" (LCR) para que os usuários possam tomar conhecimento. A LCR é um arquivo eletrônico publicado periodicamente pela AC, contendo o número de série dos certificados que não são mais válidos e a data de revogação.

As Figuras abaixo ilustram como os certificados digitais são apresentados nos navegadores Web. Note que, embora os campos apresentados sejam padronizados, a representação gráfica pode variar entre diferentes navegadores e sistemas operacionais. De forma geral, os dados básicos que compõem um certificado digital são:

- ✓ Versão e número de série do certificado;
- ✓ Dados que identificam a AC que emitiu o certificado;
- ✓ Dados que identificam o dono do certificado (para quem ele foi emitido);
- ✓ Chave pública do dono do certificado;
- ✓ Validade do certificado (quando foi emitido e até quando é válido);
- ✓ Assinatura digital da AC emissora e dados para verificação da assinatura.

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18934	Instrução	1.0	Emerson Cardoso	08/09/2021	4 de 29

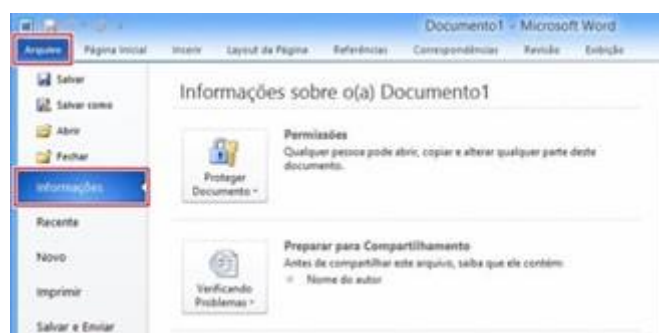





6.4 Protegendo documentos do Office

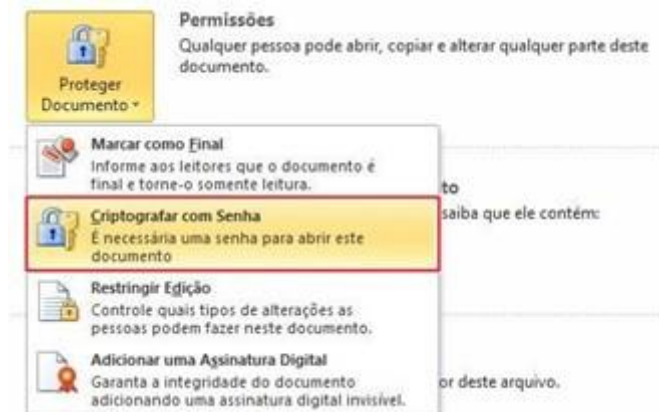
Os programas do pacote Office da Microsoft possuem uma maneira de você criptografar o documento pelas próprias opções dos arquivos. Para isso, primeiro clique no botão “Arquivo” e escolha a alternativa “Informações”.

“Arquivo” e escolha a alternativa “Informações”.



Em seguida, no setor “Permissões”, selecione “Proteger Documento” e clique na opção “Criptografar com senha”.

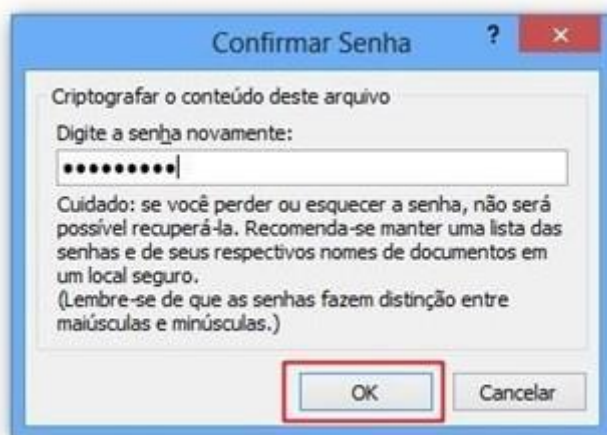
 Confidencialidade	Tipo de Documento:	Procedimento
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Procedimento para Uso de Criptografia



Feito isso, uma nova janela é mostrada na tela e, nela, você deve preencher a combinação desejada no campo “Senha” e clicar em “OK”.




Então, será preciso confirmar a senha e clicar em “OK” para completar a operação.



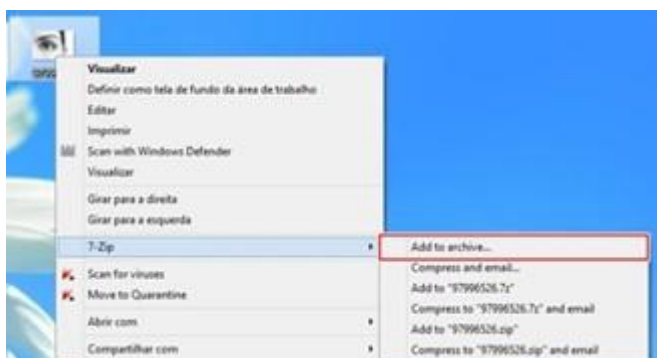
Embora nossas imagens tenham sido capturadas a partir do Word, a operação também vale para as outras ferramentas do pacote Office. Uma vez concluído o procedimento, será exigida a inserção da senha previamente cadastrada para a abertura do arquivo.

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18934	Instrução	1.0	Emerson Cardoso	08/09/2021	7 de 29

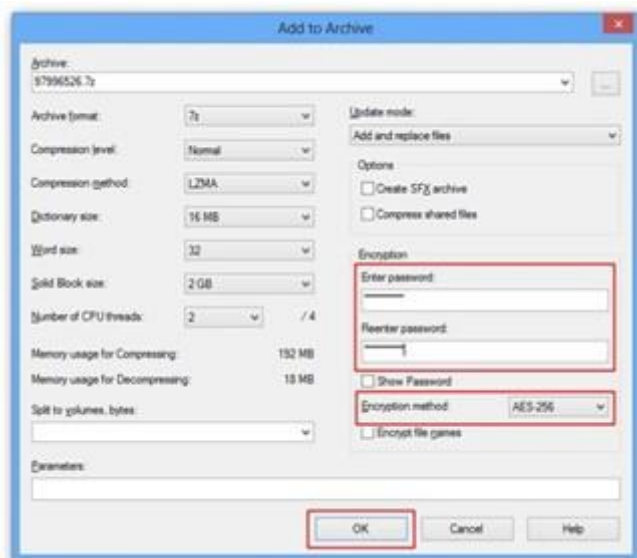
 Confidencialida	Tipo de Documento:	Procedimento
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Procedimento para Uso de Criptografia


6.5 Compactando e criptografando

Se você precisa enviar um ou mais arquivos para uma pessoa, mas quer mantê-los seguros, você pode utilizar um programa completamente gratuito e de código aberto para a tarefa, o 7-Zip, o primeiro passo é utilizá-lo para criar um arquivo, o que pode ser feito abrindo o software propriamente dito ou via menu de contexto no documento.



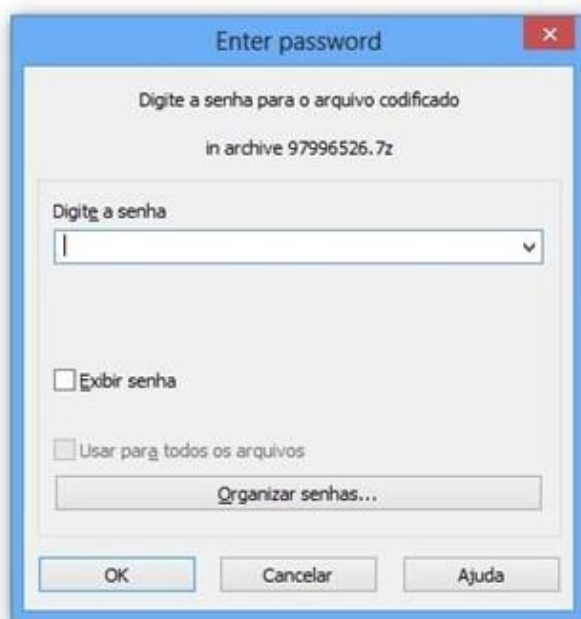
Em seguida, no setor “Encryption”, observe que há um campo para você adicionar uma senha (e outro para confirmá-la). Aqui, tudo o que você precisa fazer é digitar a sequência desejada e garantir que a caixa de seleção “Encryption method” esteja preenchida com a opção “AES-256”. Quando tudo estiver conforme o desejado, clique em “OK” para confirmar.



 Confidencialida	Tipo de Documento:	Procedimento
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Procedimento para Uso de Criptografia

Vale apenas lembrar-se de que é possível adicionar mais de um arquivo ou até mesmo uma pasta inteira na hora de fazer a compactação.

Concluído esse procedimento, o seu arquivo já estará criptografado e será exigida uma senha em uma tentativa de abri-lo.

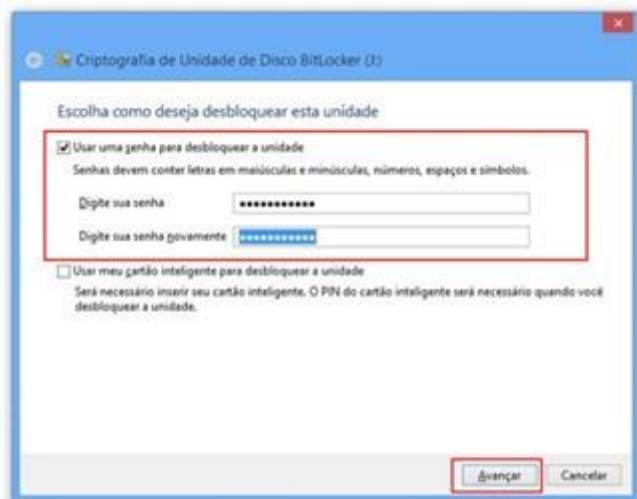


6.6 Bitlocker

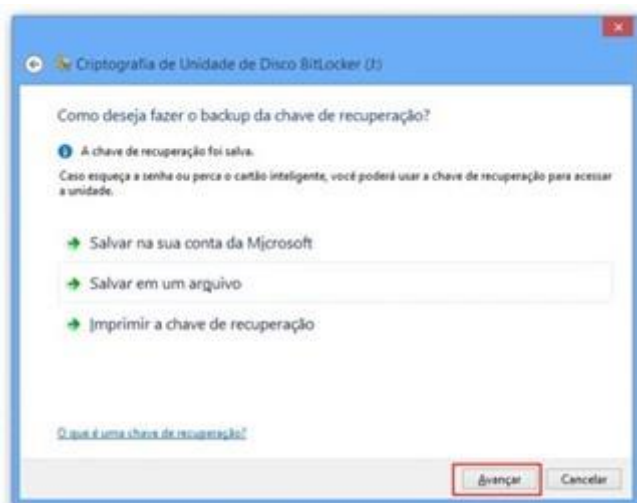
O Bitlocker pode ser utilizado para criptografar unidades inteiras, incluindo HDs externos e pendrives. Inclusive, você pode até mesmo aplicar a proteção na partição na qual o sistema operacional está instalado. Para utilizá-lo, clique na partição desejada com o botão direito do mouse e selecione a alternativa “Ligar BitLocker”.




Em seguida, na nova janela aberta, marque a opção “Usar uma senha para desbloquear a unidade”. Então, observe que há um campo para você adicionar uma senha (e outro para confirmá-la). Aqui, você deve digitar a sequência desejada e clicar em “Avançar”.



Feito isso, uma nova janela é aberta solicitando que você crie uma chave de recuperação. Isso é feito para o caso de você se esquecer da senha utilizada para proteger a unidade. Para prosseguir, basta escolher o método desejado e clicar em “Avançar”.



Agora, você deve escolher se deseja criptografar apenas o que está em uso na unidade ou ela inteira. A primeira alternativa é ideal para computadores novos, enquanto a segunda é recomendada para um dispositivo que já esteja há algum tempo em uso. Quando tudo estiver conforme o desejado, clique em “Avançar”.

 Confidencialidade	Tipo de Documento:	Procedimento
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Procedimento para Uso de Criptografia



Uma vez executados esses passos, o processo é iniciado e, posteriormente, será necessário utilizar a senha configurada para abrir a unidade protegida.

No anexo I é apresentado como podemos utilizar o Bitlocker em larga escala e centralizando as chaves criptográficas.

6.7 Criptografia no Windows

O sistema operacional Windows já vem há algum tempo trazendo uma funcionalidade que permite a criptografia de disco Bitlocker, que foi introduzido originalmente com o Windows Vista.

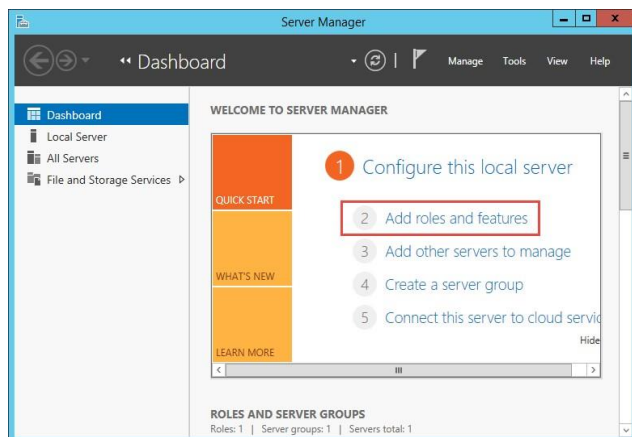
É recomendável que o chip TPM seja usado pelo Bitlocker para manter segura a chave de criptografia usada. Todavia é possível utilizar essa ferramenta de criptografia nativa do Windows sem esse chip.

O Bitlocker trabalha com algoritmos de criptografia AES-128 bits e AES-256 bits e pode ser usado para proteger o boot e a integridade da configuração do servidor.

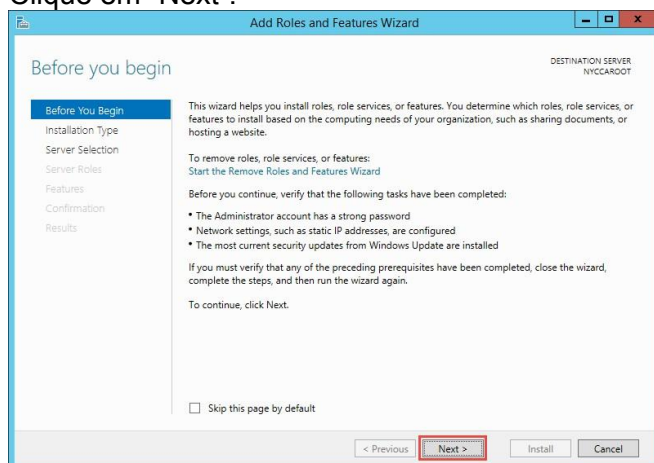
6.8 Instalando e usando o Bitlocker

Para usar o Bitlocker, a primeira coisa que precisamos fazer é instalar a funcionalidade "Bitlocker Drive Encryption". Para esse fim, é preciso executar o Server Manager e clicar em "Add roles and features", conforme a Figura "Server Manager".

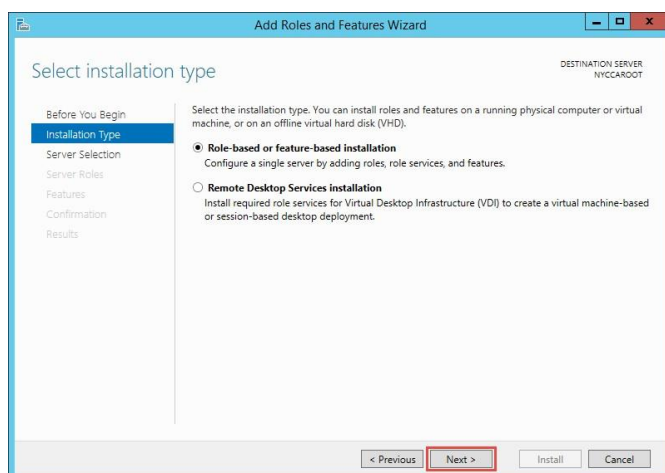
N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18934	Instrução	1.0	Emerson Cardoso	08/09/2021	11 de 29



Clique em “Next”.

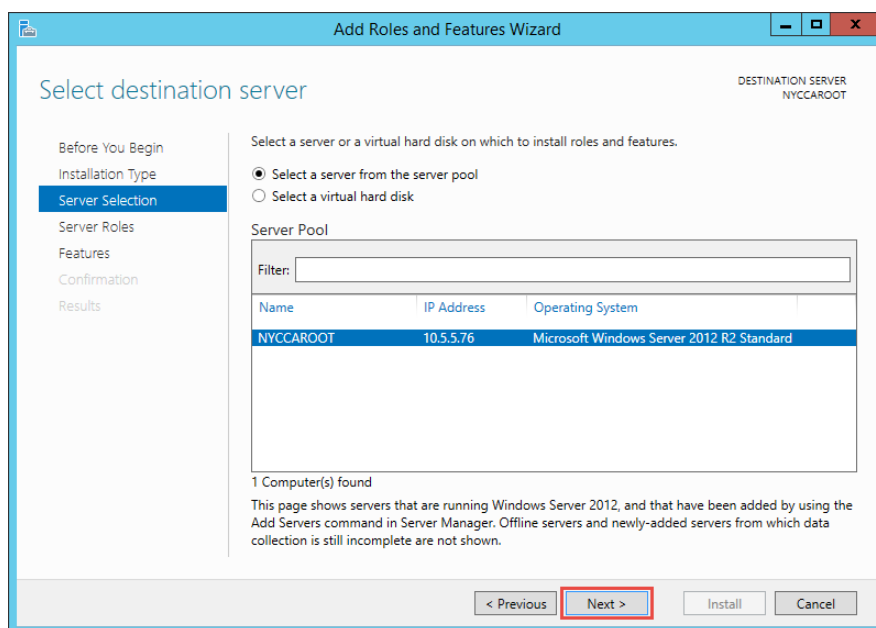


Clique em “Next”

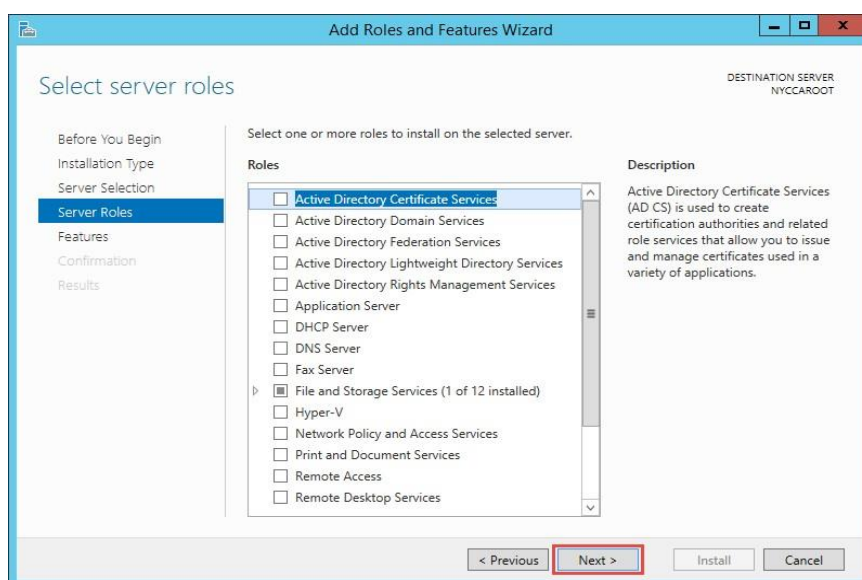



Clique em “Next”

Na próxima tela, o leitor deve selecionar o nome do servidor. Se ele é um servidor standalone, aparecerá apenas o nome desse servidor. Se é parte de um grupo, deve-se selecionar o servidor adequado dentre as opções apresentadas.

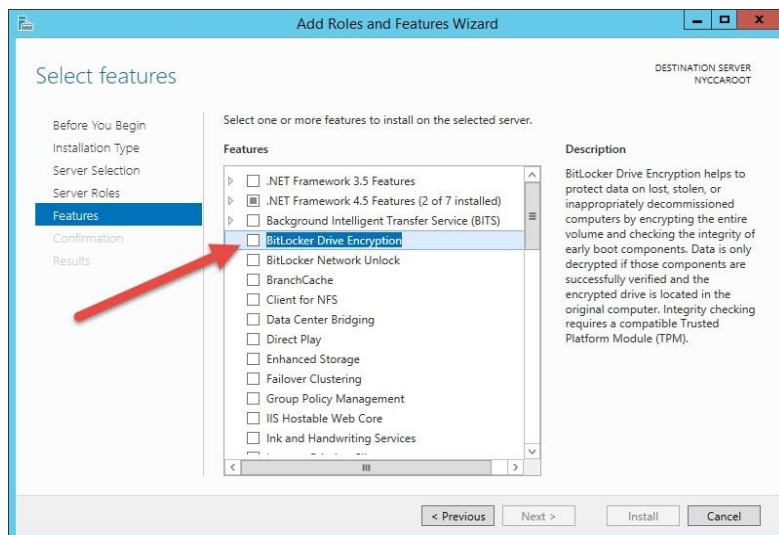


Clicando em “Next”, escolha a opção “Server Roles”. Note que não estamos instalando um “role” (papel) para o servidor, mas uma feature.

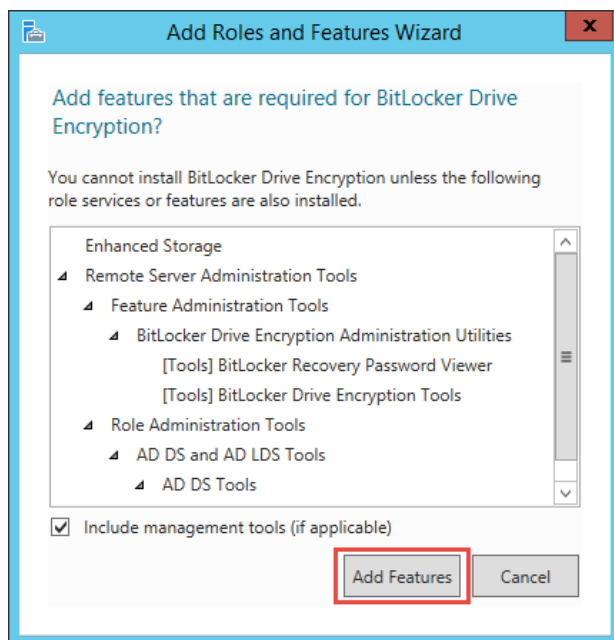


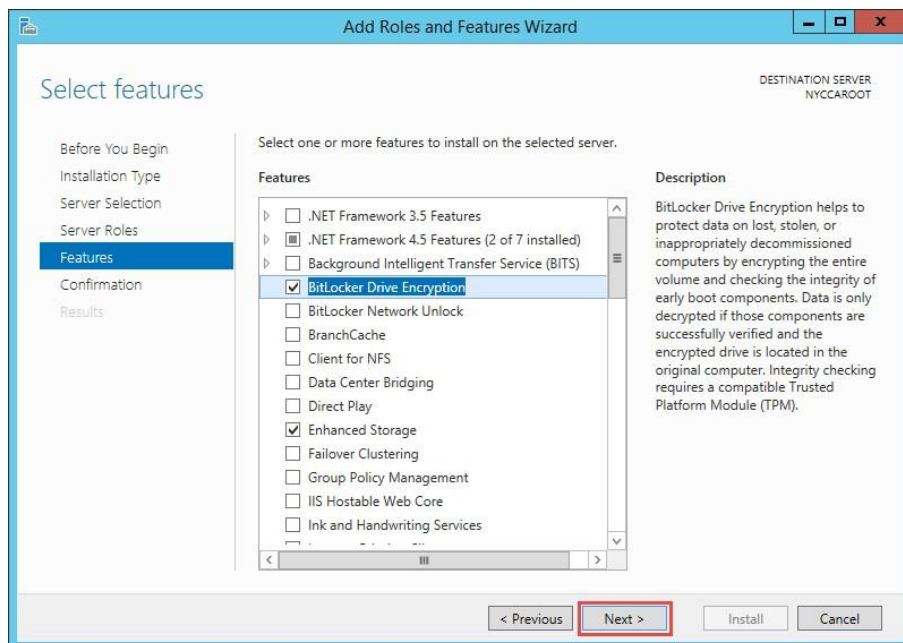
 Confidencialida	Tipo de Documento:	Procedimento
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Procedimento para Uso de Criptografia

Finalmente, clique em “BitLocker Drive Encryption”, como mostrado na tela da Figura “Seleção da funcionalidade BDE”.

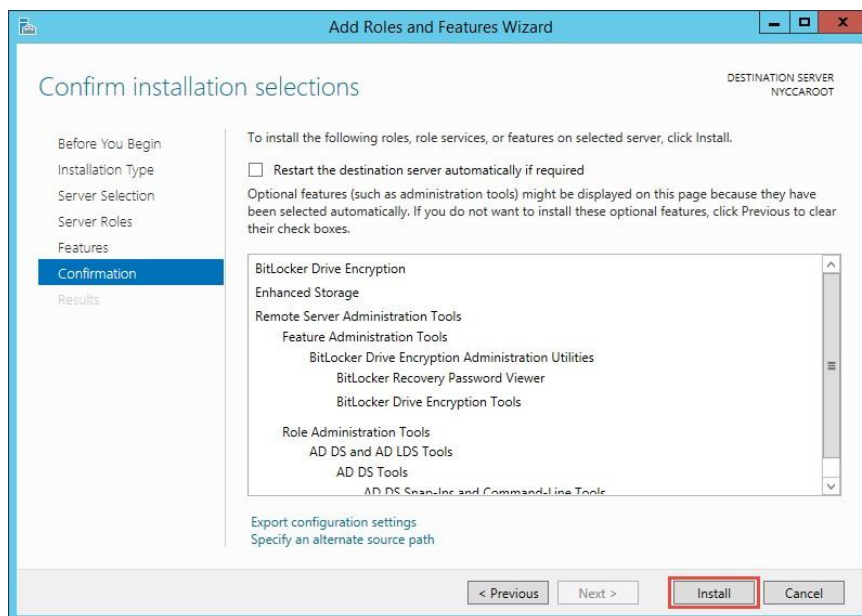


O popup abaixo aparecerá. Clique então em “Add Features”.

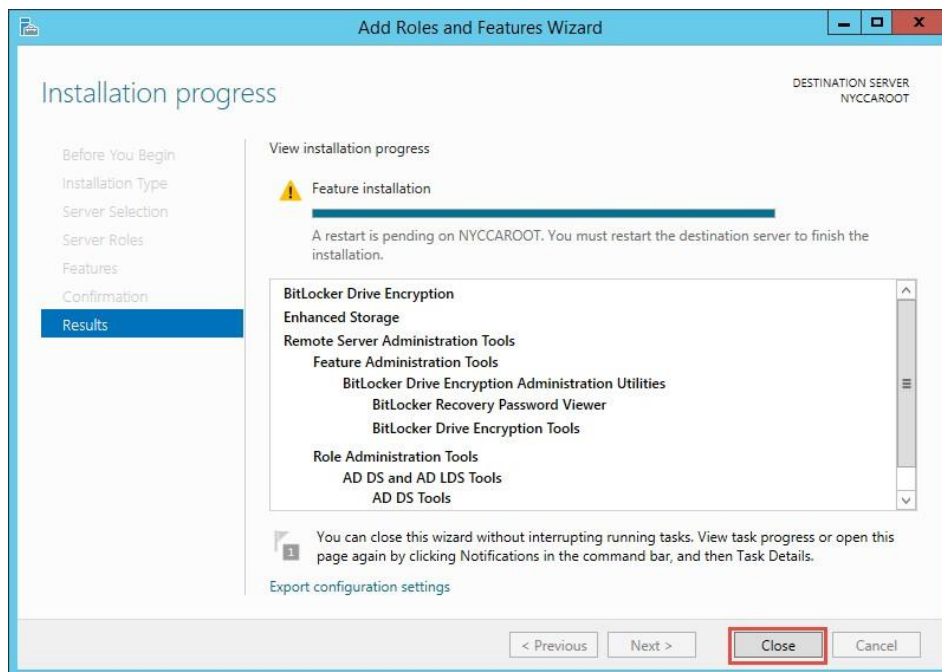




Clique em “Next”.



Clique em “Install” para adicionar a feature.



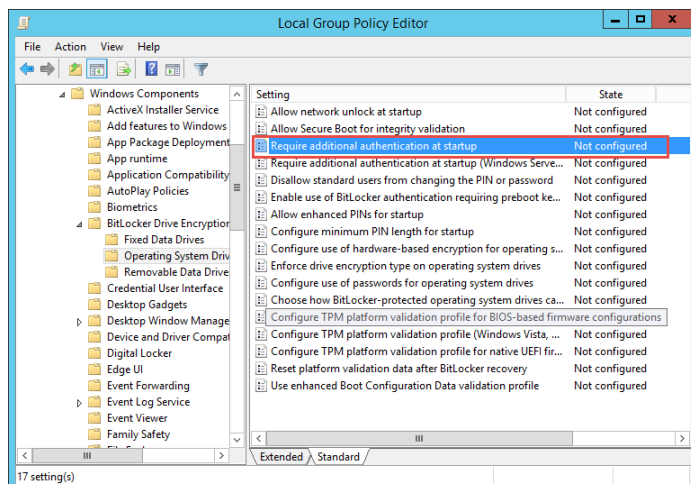
A instalação pode demorar alguns minutos. Clique em “Close” quando ela terminar.


Uma vez que isso termine, será preciso reinicializar o computador. Antes que isso seja feito, porém, é importante configurar uma política de grupo local, conforme a Figura “Local Group Policy Editor”.

Execute o editor de política de grupos local (gpedit.msc) e navegue por:

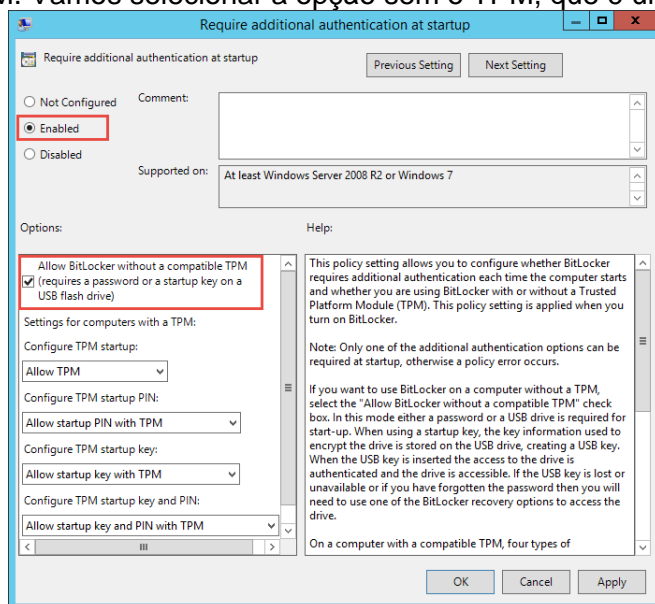
Computer Configuration > Administrative Templates > Windows Components > BitLocker Drive Encryption > Operating System Drives > Require additional authentication at startup.

Veja a Figura “Local Group Policy Editor” abaixo.



 Confidencialida	Tipo de Documento:	Procedimento
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Procedimento para Uso de Criptografia

Clique na opção marcada acima para habilitar a política. Vamos marcar a opção “Allow BitLocker without a compatible TPM”. Caso o leitor queira usar o chip TPM, o que é mais recomendado caso ele esteja presente no hardware usado, selecione uma das opções com o TPM. Vamos selecionar a opção sem o TPM, que é um pouco mais trabalhosa.

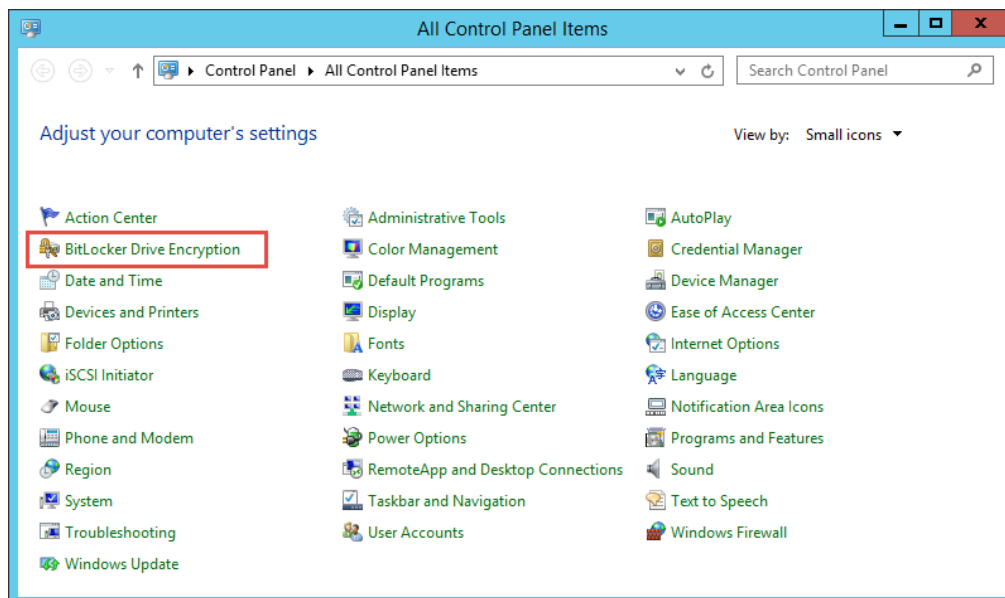


As opções para a configuração usando o chip TPM são:

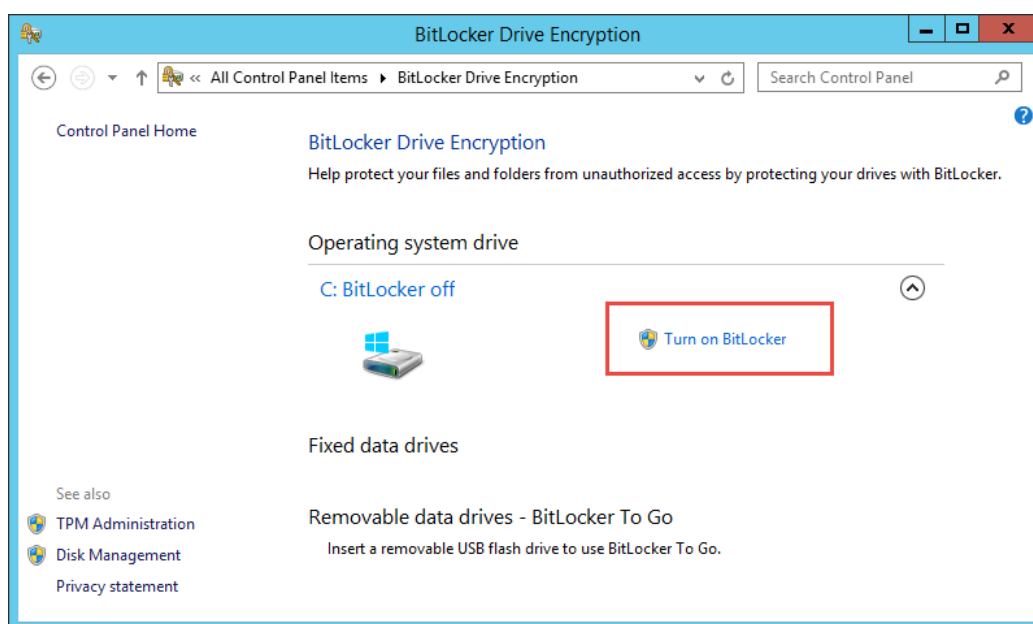
- ✓ TPM sem qualquer proteção: essa opção parece não agregar qualquer segurança. No entanto, o chip TPM poderá fazer a guarda segura da chave usada para criptografia do disco da máquina. Isso garante a proteção do servidor contra os ataques em que ele estiver off-line.
- ✓ Startup PIN: nesse caso, um PIN é necessário no momento do boot para autenticação do usuário antes da recuperação da chave usada para cifrar o disco.
- ✓ Startup Key: nesse caso, uma chave deve ser usada para autenticação. Essa chave pode estar armazenada em um pendrive, que deverá estar conectado ao servidor durante sua inicialização.
- ✓ Startup Key e PIN: a combinação dos itens (2) e (3).

Depois desse último passo, a máquina deve ser reinicializada para que as novas configurações passem a fazer efeito. Depois da reinicialização do sistema, abra o control panel e na sequência vá em BitLocker Drive Encryption.


N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18934	Instrução	1.0	Emerson Cardoso	08/09/2021	17 de 29

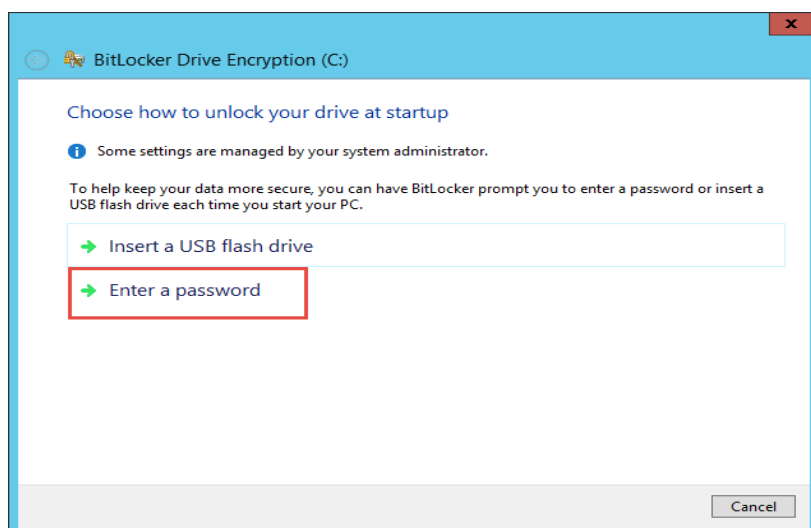


Clique em “Turn on BitLocker”.



Lembre-se de que estamos usando o Bitlocker sem o chip TPM. Podemos utilizar a proteção da chave com uma password ou inserindo um pendrive sempre que iniciar o servidor. Vamos escolher o uso da password na tela mostrada na Figura “Seleção de Mecanismo de Autenticação”.


 Confidencialida	Tipo de Documento:	Procedimento
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Procedimento para Uso de Criptografia

Escolha uma senha legal e clique em “Next”

Agora vamos fazer um backup da chave de recuperação que pode ser usada a qualquer momento para desbloquear o Bitlocker se a senha for esquecida. Essa chave de recuperação pode ser armazenada em um flash drive/pendrive, em um arquivo ou pode ser impressa.

Na tela mostrada na Figura “Chave de Recuperação”, estamos salvando essa chave em um arquivo. Nesse caso, o leitor deverá obviamente copiar esse arquivo para um local seguro fora do servidor. Caso ele seja salvo em um pendrive e o volume criptografado esteja em uma máquina virtual, é importante verificar se a chave de recuperação foi

 Confidencialidade	Tipo de Documento:	Procedimento
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Procedimento para Uso de Criptografia

realmente salva para o dispositivo de armazenamento externo. De qualquer forma, em todas essas situações, a chave de recuperação deve ser protegida fisicamente.



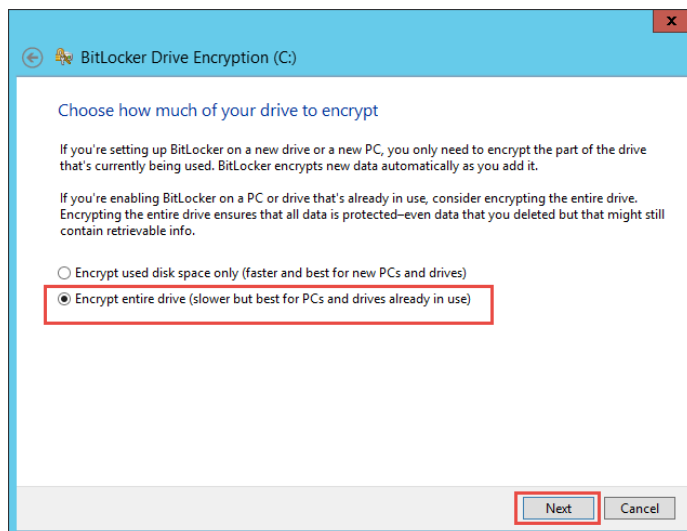
Agora vamos definir o que precisa ser criptografado na unidade. Nesse caso, temos que escolher entre duas opções:

Podemos cifrar apenas o espaço já utilizado.

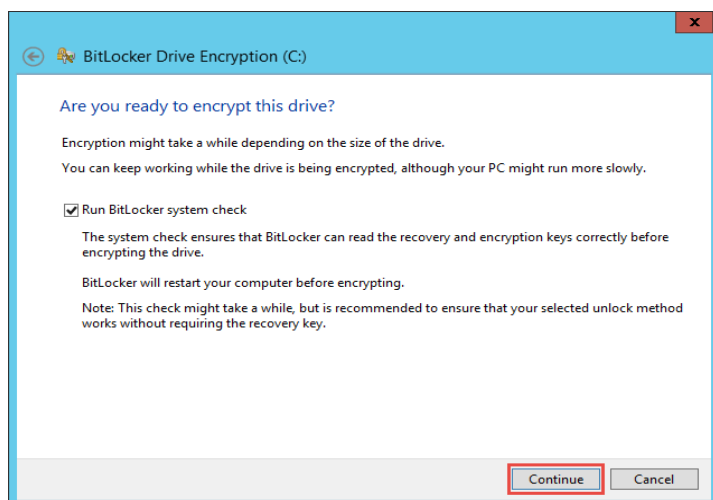
Podemos cifrar todo o disco.

Em discos mais novos, a opção (1) parece mais interessante, pois não há chances de encontrarmos dados em slack spaces do disco, ou seja, restos de dados que ficaram no disco após a deleção de arquivos. Para discos já em uso há algum tempo, a melhor opção pode ser de fato a (2), pois quaisquer resquícios de dados no disco poderão ser protegidos. Na tela mostrada na Figura “Opção da Criptografia do Disco”, selecionaremos a opção “Encrypt entire drive”. Depois clicaremos em “Next” para iniciar a criptografia do disco. O processo pode levar algum tempo, dependendo do tamanho do volume que será cifrado.

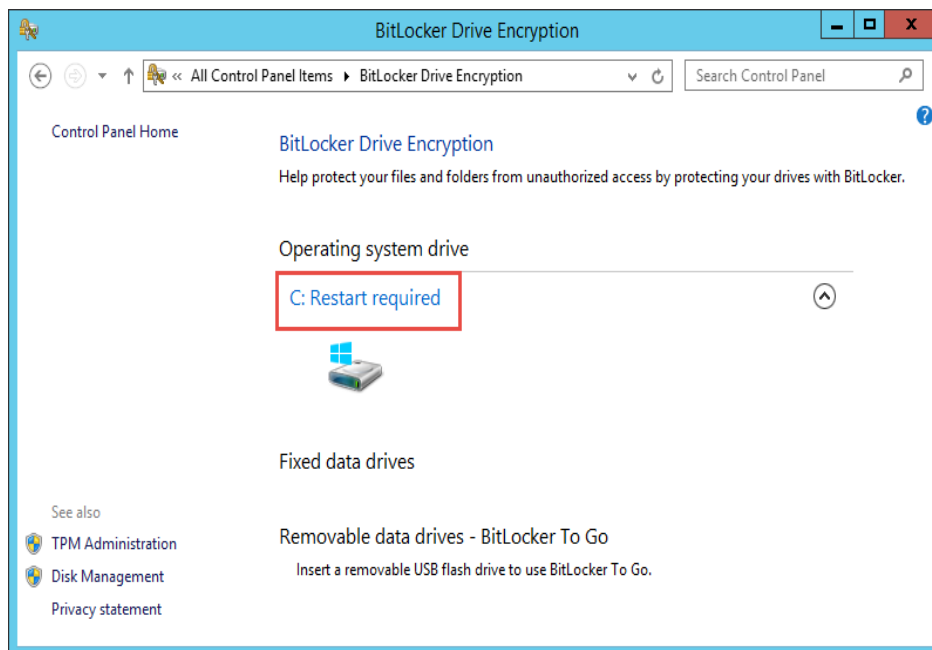
N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18934	Instrução	1.0	Emerson Cardoso	08/09/2021	20 de 29



Marque a opção “Run BitLocker Check” para garantir que o bitlocker consiga ler e recuperar a chave de criptografia, antes de começar o processo de criptografia do disco.



Depois disso, clique em “Continue”. Você precisará reiniciar o computador para habilitar a criptografia BitLocker.



Operating system drive

C: Restart required




Fixed data drives

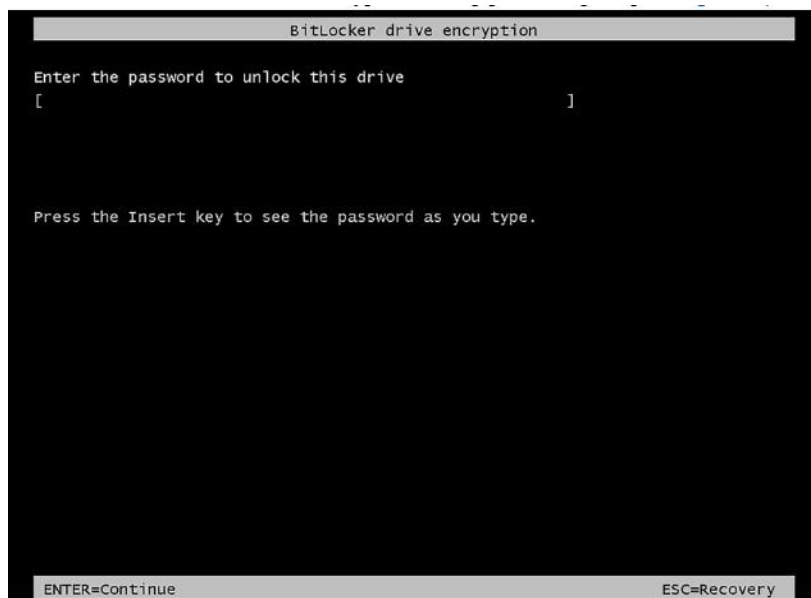
Removable data drives - BitLocker To Go

Insert a removable USB flash drive to use BitLocker To Go.

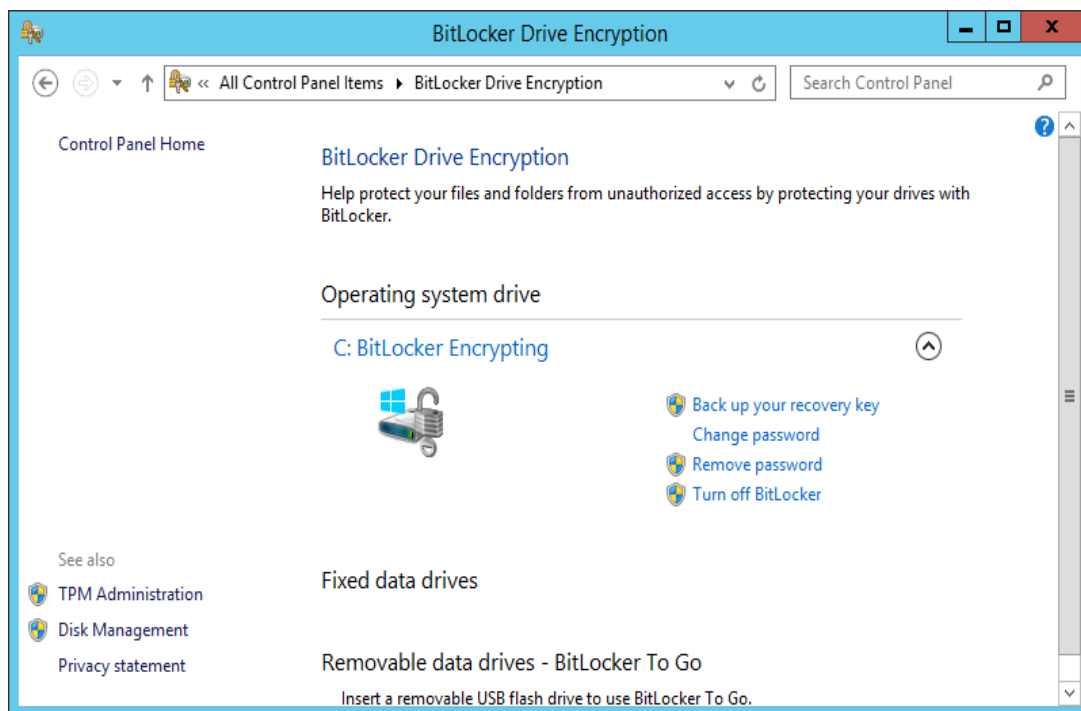


 Confidencialidade	Tipo de Documento:	Procedimento
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Procedimento para Uso de Criptografia


Depois da reinicialização, será preciso usar a senha previamente definida para a autenticação e proteção da chave de criptografia.



Depois do login, o processo de criptografia do disco realmente começa. Você pode navegar no applet “BitLocker Drive Encryption” para assegurar que o processo foi iniciado. Você verá o status de “Encrypting” quando ele começar.



N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18934	Instrução	1.0	Emerson Cardoso	08/09/2021	23 de 29

 Confidencialidade	Tipo de Documento:	Procedimento
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Procedimento para Uso de Criptografia

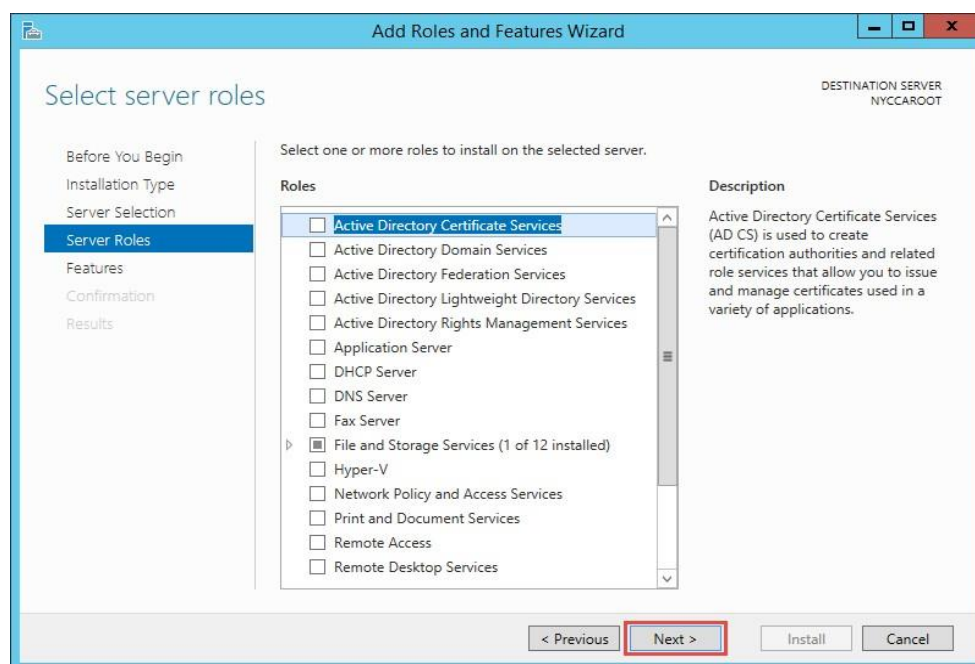
6.9 Desbloqueando o Bitlocker pela rede

Pode ser complicado, em algumas situações, ter alguém fisicamente próximo aos servidores para digitar a password a fim de desbloquear o Bitlocker. Nesse caso, a possibilidade de fazer essa atividade remotamente pode ser muito necessária. Felizmente, é possível fazer isso com o Bitlocker.

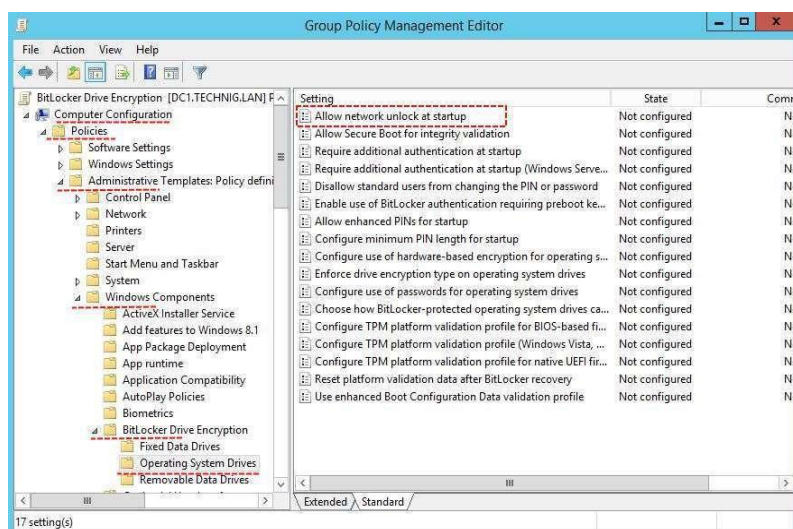
Primeiro, deve-se instalar alguns papéis (roles) no servidor:

- ✓ Active Directory
- ✓ DNS Server
- ✓ DHCP Server
- ✓ WDS Server

A janela apresentada na Figura “Ativando roles para o servidor” mostra onde essa instalação deve ser feita. Selecione os roles e faça a instalação.



Em seguida, no Group Policy Management Editor, expanda “Computer Configuration” para “Operating System Drives”. Clique em “Allow network unlock at startup” e habilite a política (Figura “Ativação do BitLocker pela rede”).

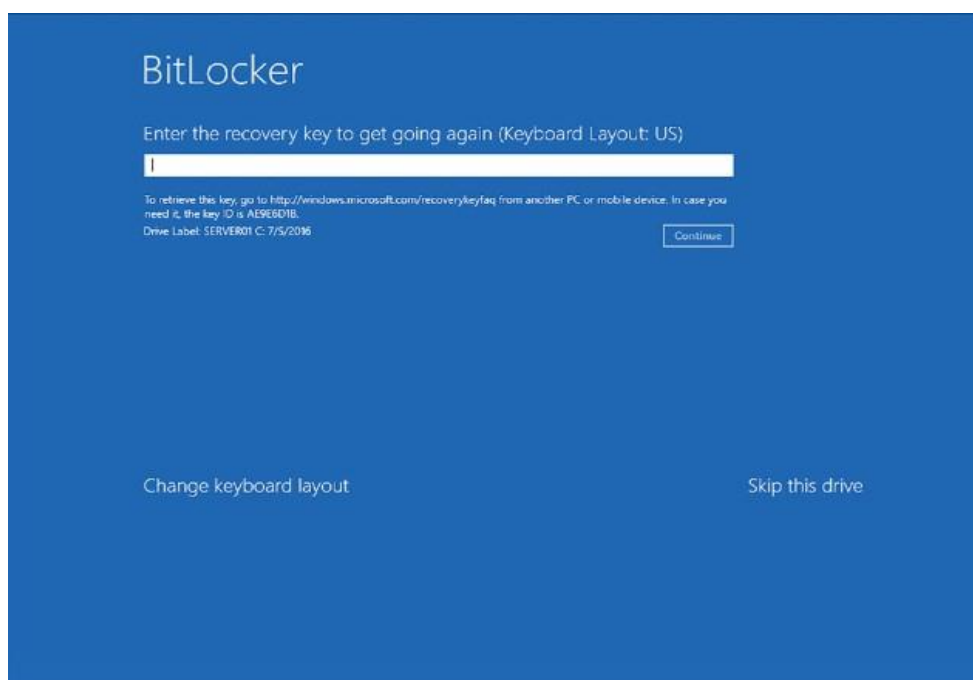
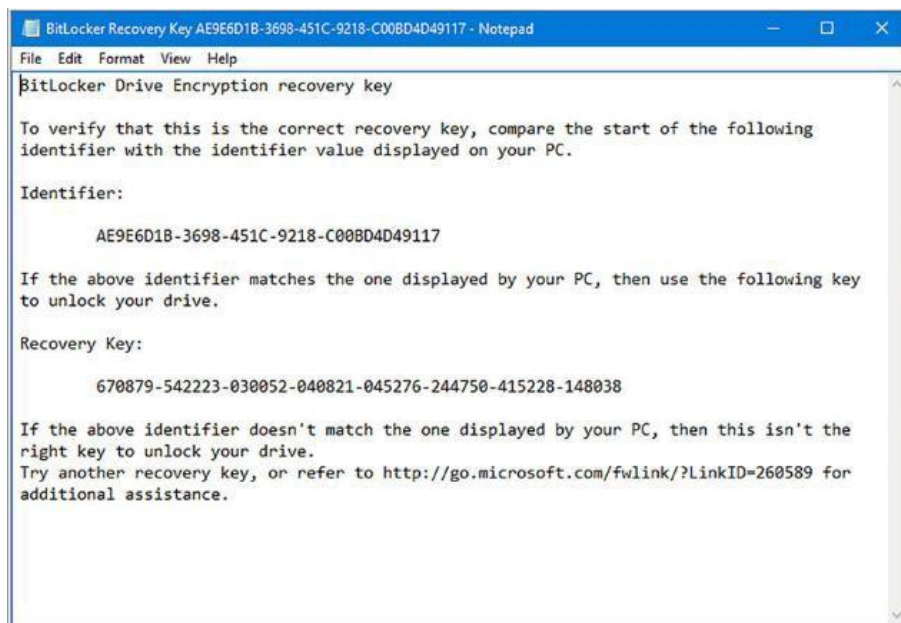


6.10 Uso da chave de recuperação


O que acontece se esqueço a senha ou perco?

o pendrive com a chave para desbloquear o Bitlocker? Não é um problema trivial tentar abrir um disco cifrado com AES-256 bits, por exemplo, sem a chave simétrica. Felizmente, durante o processo de criptografia do disco, explicado anteriormente, vimos que há a geração de uma chave de recuperação de 48 bits salva em algum local seguro. A Figura “Chave de recuperação” mostra um arquivo com essa chave.

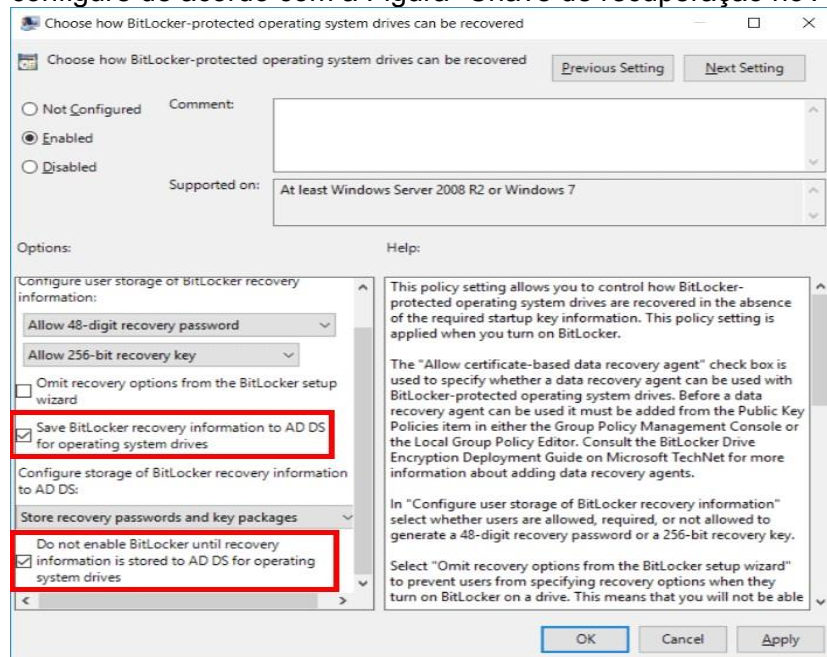
Portanto, essa é a forma mais direta para desbloqueio. No momento em que a senha for solicitada, o usuário pode pressionar a tecla ESC para inserir a chave de recuperação.



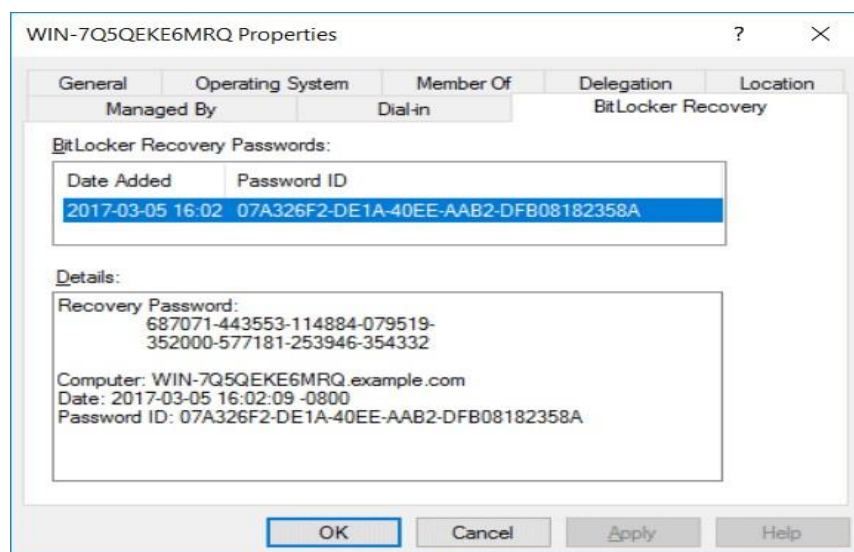
Mas essa gestão de chaves de recuperação pode ficar mais complicada com o aumento do número de servidores. Uma forma interessante de resolver isso é usar o AD (Active Directory) para a guarda dessas chaves dos diferentes servidores e sua recuperação automática. Para que isso aconteça, precisamos habilitar a funcionalidade pelo Group Policy Management Editor.

 Confidencialida	Tipo de Documento:	Procedimento
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Procedimento para Uso de Criptografia

Navegue no editor em: Computer Configuration > Policies > Administrative Templates > Windows Components > BitLocker Drive Encryption > Operating System Drives. Habilite a política “Choose how BitLocker protected operating system drives can be recovered” e a configure de acordo com a Figura “Chave de recuperação no AD”.

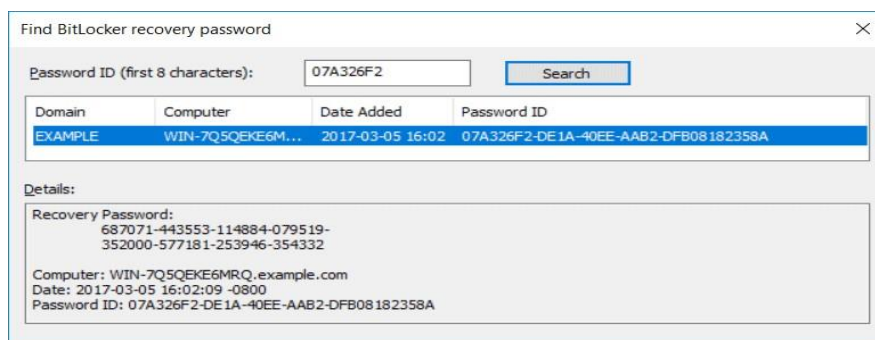
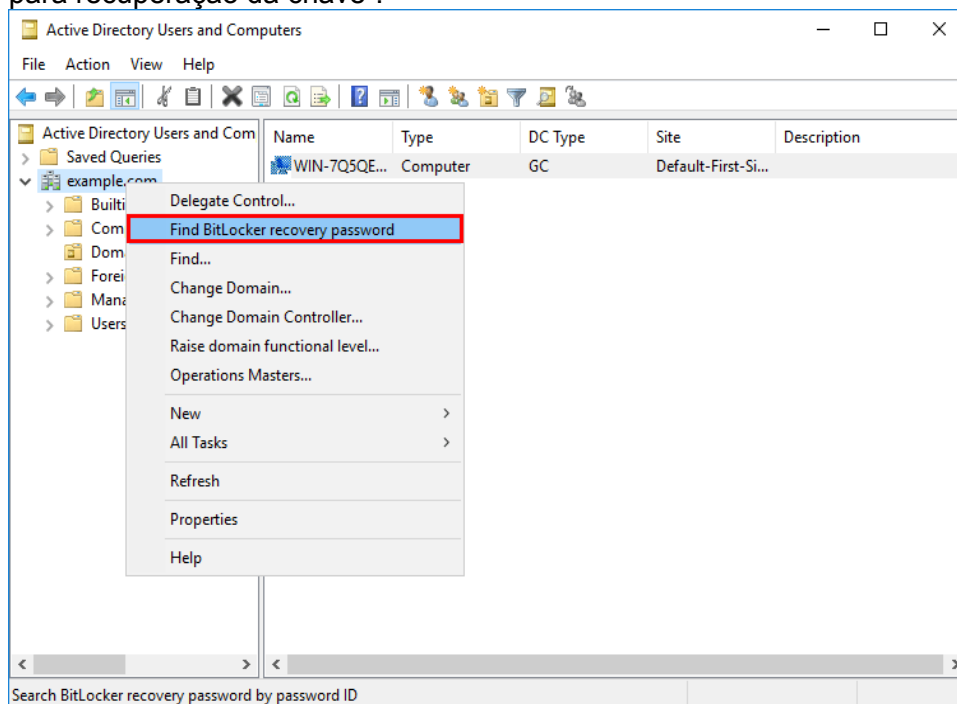


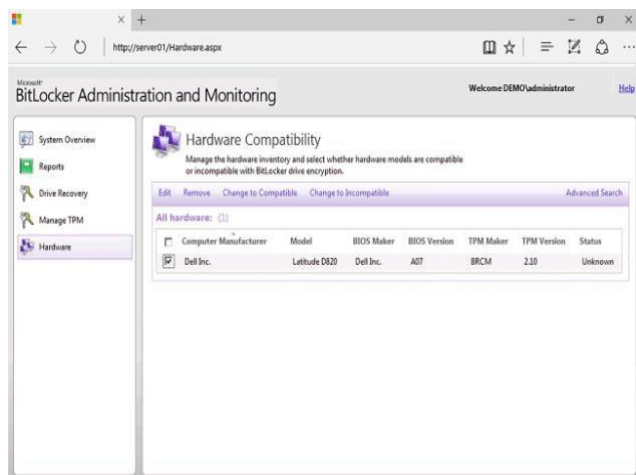
Portanto, é muito conveniente ter essas chaves de recuperação armazenadas no AD. No entanto, a recuperação deve ser manual do controlador do domínio. Para recuperar essa chave, é preciso ver as propriedades do computador e ir para a tab “Bitlocker Recovery”.



N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18934	Instrução	1.0	Emerson Cardoso	08/09/2021	27 de 29

Também é possível recuperar a chave manualmente na ferramenta administrativa Active Directory Users and Computers, como pode ser visto na Figura “Mecanismo alternativo para recuperação da chave”.





Para grandes empresas, uma boa solução é usar toolset MBAM. Essa é uma solução que permite fazer o gerenciamento central das chaves de recuperação do Bitlocker. Ela permite que usuários consigam obter suas chaves de recuperação por eles mesmos de forma automática e segura. Você pode ver a tela principal dessa solução na Figura “Tela do MBAM”.

7. CONTROLE DE REGISTROS

Identificação	Armazenamento e Preservação	Proteção (acesso)	Recuperação e uso	Retenção	Disposição
Norma de SI	Eletrônico (GED)	Restrição de acesso	Por tema ou título	Até a próxima atualização do documento	Substituição

8. ANEXOS

Não aplicável

9. REGISTRO DE ALTERAÇÕES

9.1. Colaboradores

Empresa	Área	Nome
NAVA	Segurança da Informação	Mateus Rocha

9.2. Alterações

Versão Anterior	Data da Versão Anterior	Alterações em relação à Versão Anterior
Não Aplicável	Não Aplicável	Documento em versão inicial