GPO para forçar a criptografia da unidade USB em dispositivos removíveis usando Bitlocker.

Bitlocker é uma ferramenta de criptografia do Windows disponível desde a sua versão do Windows Vista até a atual versão do Windows 10. Essa ferramenta permite a criptografia de mídias removíveis como USBs e HDs externos e até mesmo o próprio disco rígido do computador, impedindo assim que qualquer pessoa tenha acesso aos dados sem usar a chave definida para os usuários.

A intenção dessa GPO é aumentar o nível de segurança da empresa nos setores ao qual existe a necessidade de transporte de dados sensíveis e confidenciais, ao qual não podemos bloquear o acesso de salvar em determinados discos.

Requisitos; é necessário que os computadores da empresa estejam utilizando Windows 7 ou Windows 10 para aplicação desse GPO.

Tutorial

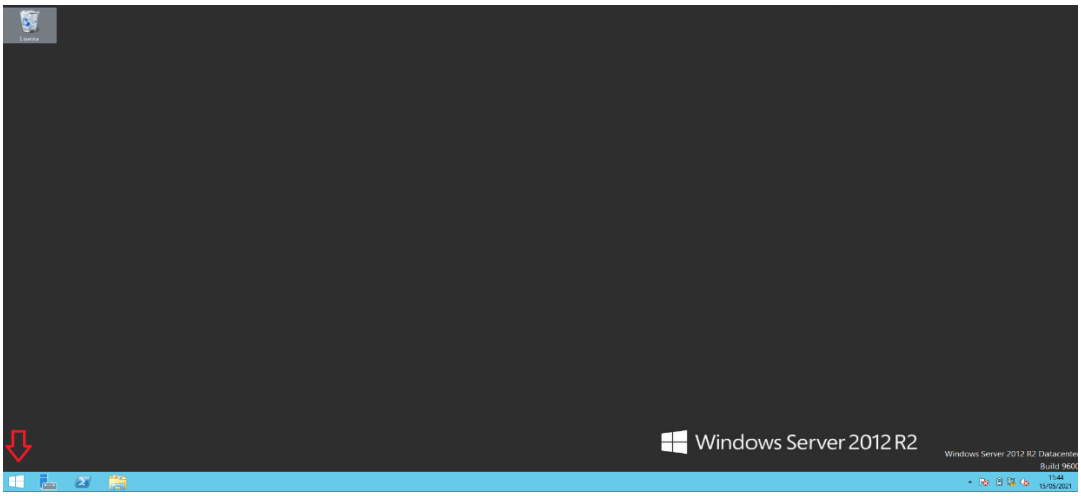
Utilizaremos o Windows 2012 R2 com AD para esse Tutorial;

Passo I – Criando a GPO

1 – Acessaremos a Ferramenta de Gerenciamento de Política de Grupo;

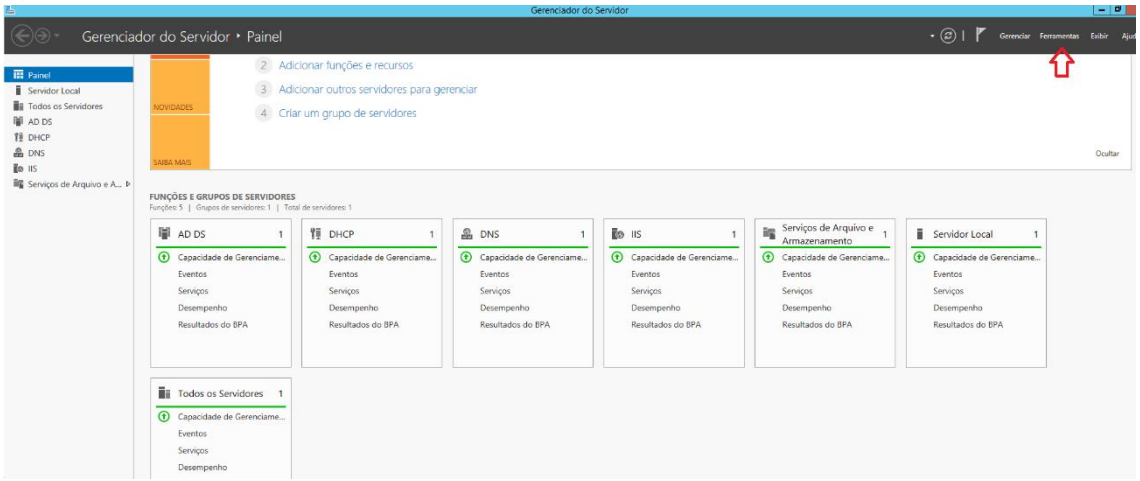
Iremos acessar o Gerenciador de Servidores através do botão Iniciar, na opção Ferramentas acessaremos o Gerenciamento de Politica de Grupo;

A) -

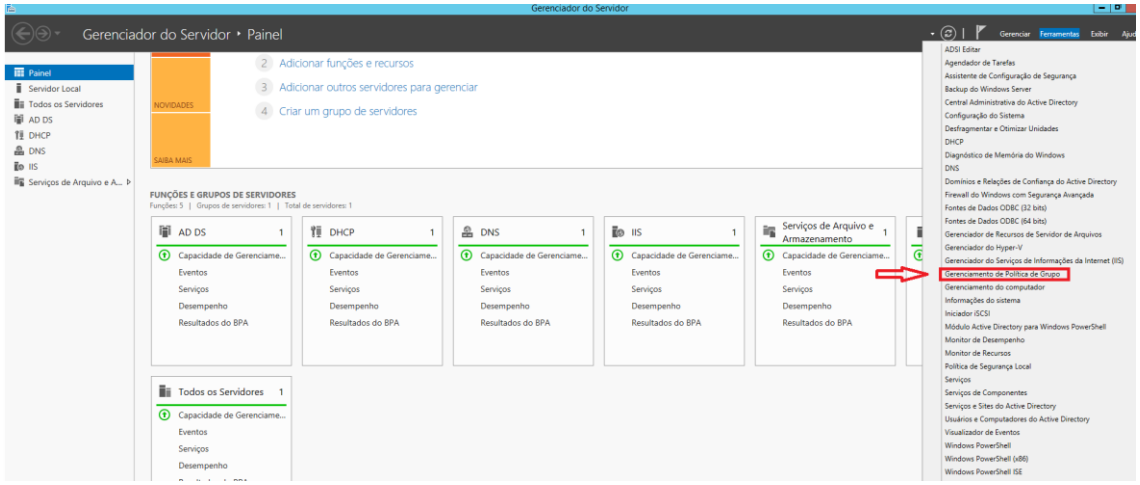


B) -

C) -

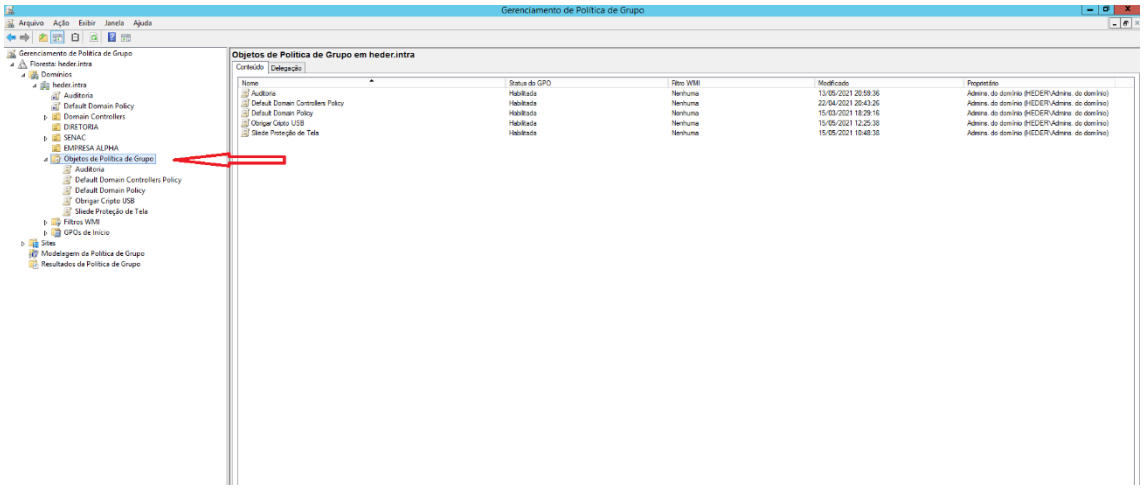

Gerenciador do Servidor
Gerenciador do Servidor • Painel
Gerenciar
Ferramentas
Exibir
Painel
Servidor Local
Todos os Servidores
AD DS
DHCP
DNS
IIS
Serviços de Arquivo e A...
2 Adicionar funções e recursos
3 Adicionar outros servidores para gerenciar
4 Criar um grupo de servidores
NOVIDADES
SAIBA MAIS
Ocultar
FUNÇÕES E GRUPOS DE SERVIDORES
AD DS
DHCP
DNS
IIS
Serviços de Arquivo e Armazenamento
Servidor Local
Todos os Servidores
Capacidade de Gerenciame...
Eventos
Serviços
Desempenho
Resultados do BPA

D) -


Gerenciador do Servidor
Gerenciador do Servidor • Painel
Gerenciar
Ferramentas
Exibir
2 Adicionar funções e recursos
3 Adicionar outros servidores para gerenciar
4 Criar um grupo de servidores
NOVIDADES
SAIBA MAIS
FUNÇÕES E GRUPOS DE SERVIDORES
AD DS
DHCP
DNS
IIS
Serviços de Arquivo e Armazenamento
Todos os Servidores
ADSI Editar
Agendador de Tarefas
Assistente de Configuração de Segurança
Backup do Windows Server
Central Administrativa do Active Directory
Configuração do Sistema
Desfragmentar e Otimizar Unidades
DHCP
Diagnóstico de Memória do Windows
DNS
Domínios e Relações de Confiança do Active Directory
Firewall do Windows com Segurança Avançada
Fontes de Dados ODBC (32 bits)
Fontes de Dados ODBC (64 bits)
Gerenciador de Recursos de Servidor de Arquivos
Gerenciador do Hyper-V
Gerenciador dos Serviços de Informações da Internet (IIS)
Gerenciamento de Política de Grupo
Gerenciamento do computador
Informações do sistema
Iniciador iSCSI
Módulo Active Directory para Windows PowerShell
Monitor de Desempenho
Monitor de Recursos
Política de Segurança Local
Serviços
Serviços de Componentes
Serviços e Sites do Active Directory
Usuários e Computadores do Active Directory
Visualizador de Eventos
Windows PowerShell
Windows PowerShell (x86)
Windows PowerShell ISE

2 – Dentro do Gerenciamento de Política de Grupo, iremos encontrar uma pasta denominada Objetos de Política de Grupo. Iremos selecioná-la, e com o botão direito do mouse iremos na opção Novo;

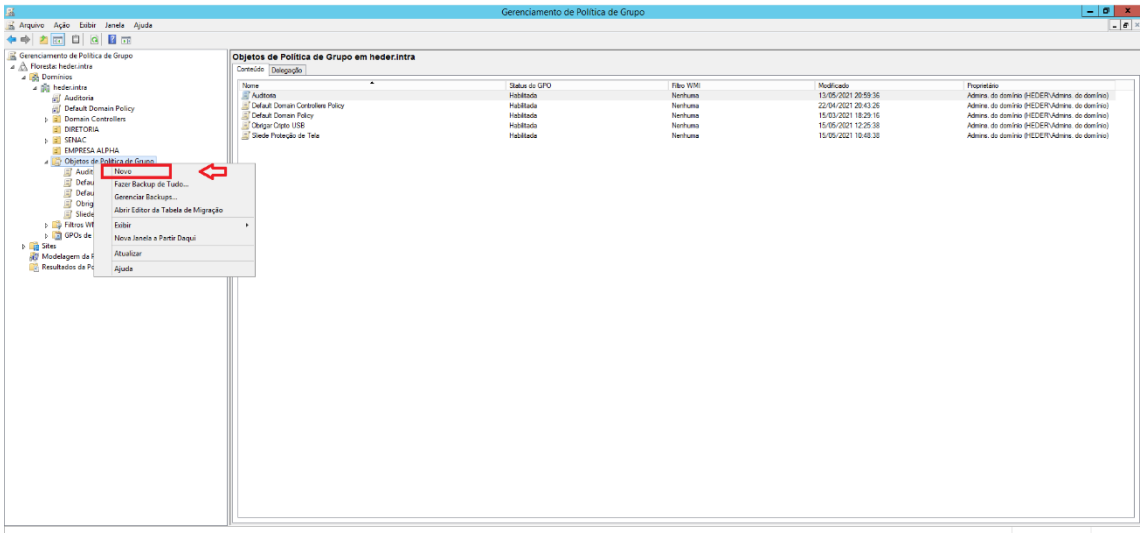
A) -



Importante observar que a pasta Objetos de Política de Grupos se encontra na seguinte sequência;

Floresta "Domínio" > Domínios > "Nome do Domínio" > Objetos de Políticas de Grupo

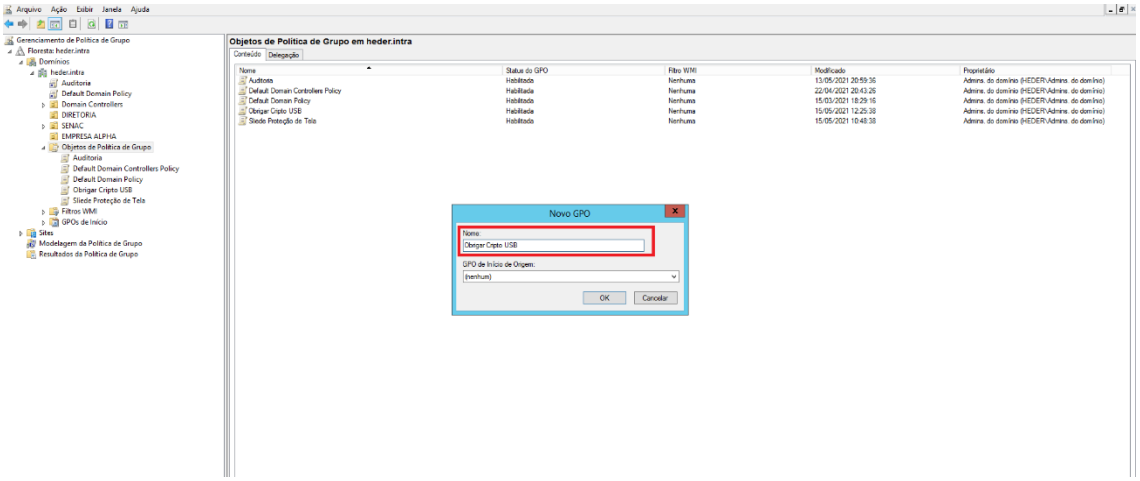
B) -



2.1 – Após clicar na opção Novo, iremos nomear a nossa GPO.

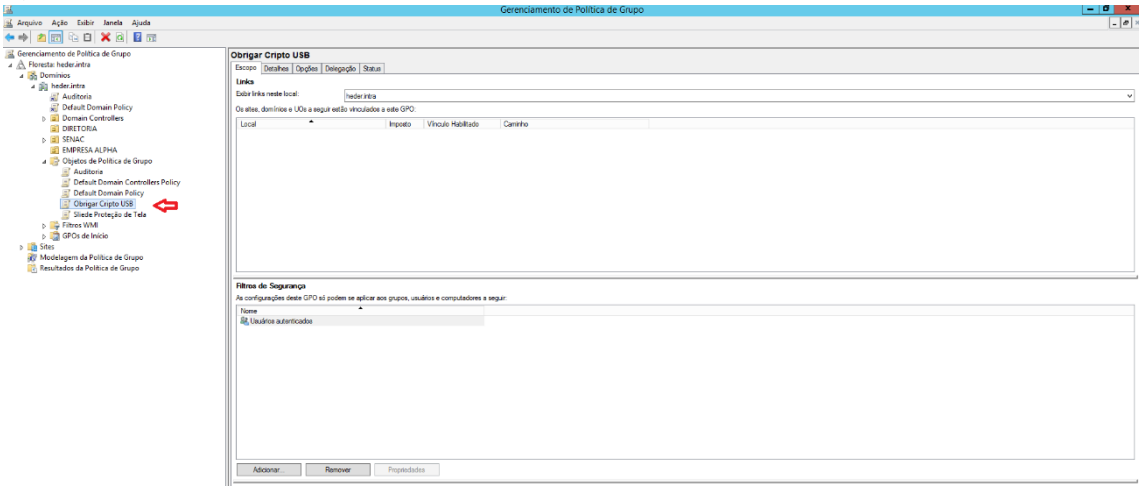
Em nosso exemplo usaremos o nome: Obrigar Cripto USB

A) –

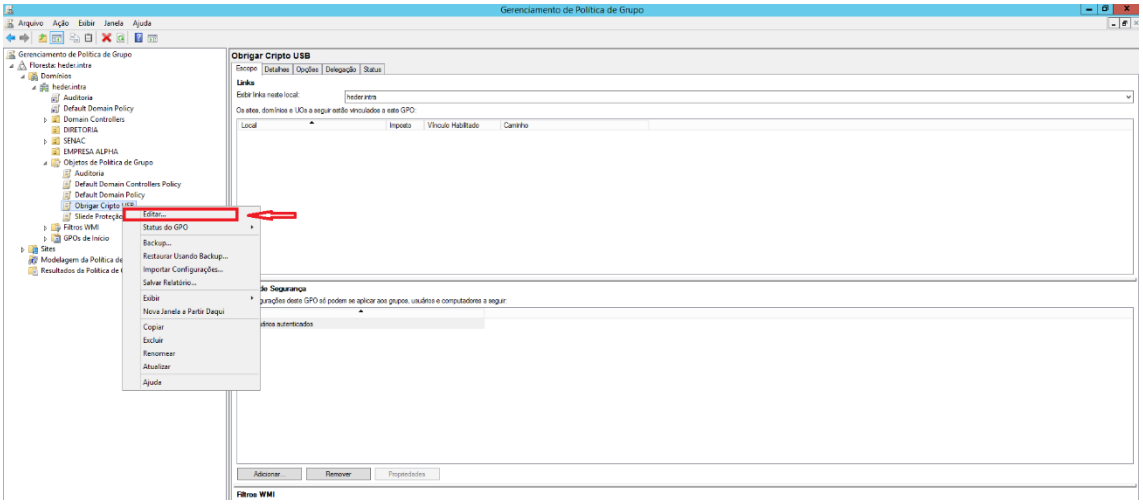


3 – Feito isso, na pasta Objetos de Política de Grupo agora deverá aparecer a nossa GPO. Clicaremos com o botão direito em cima dela e iremos na opção editar, para acessarmos o Editor de Gerenciamento de Política de Grupo;

A) -



B) -

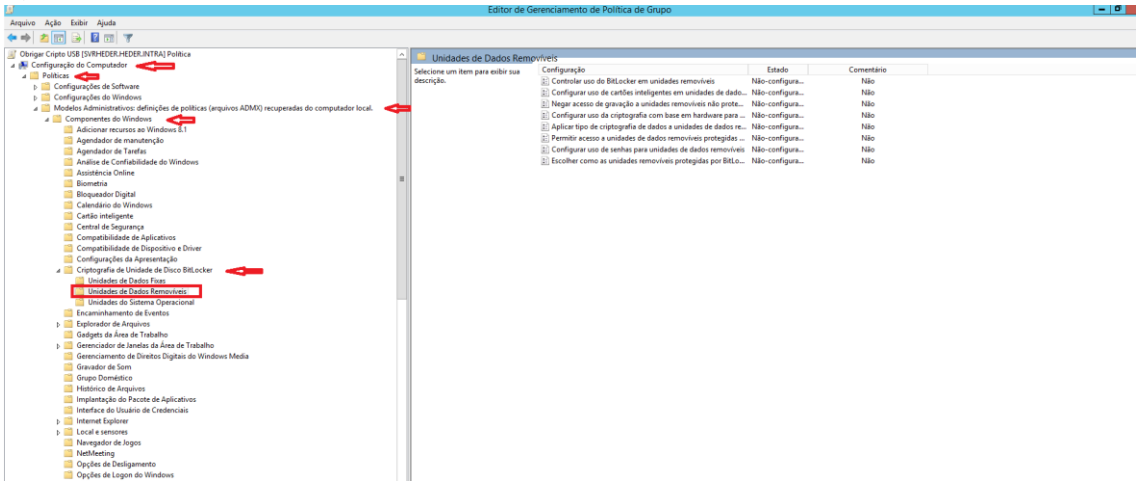


4 – Na tela do editor seremos apresentadas as configurações de Usuários e Computadores. Onde iremos alterar as configurações de Computadores, sem mexer em nada nas configurações de Usuários.

Iremos localizar a seguinte pasta de configuração Unidade de Dados Removíveis, dentro da seguinte sequência;

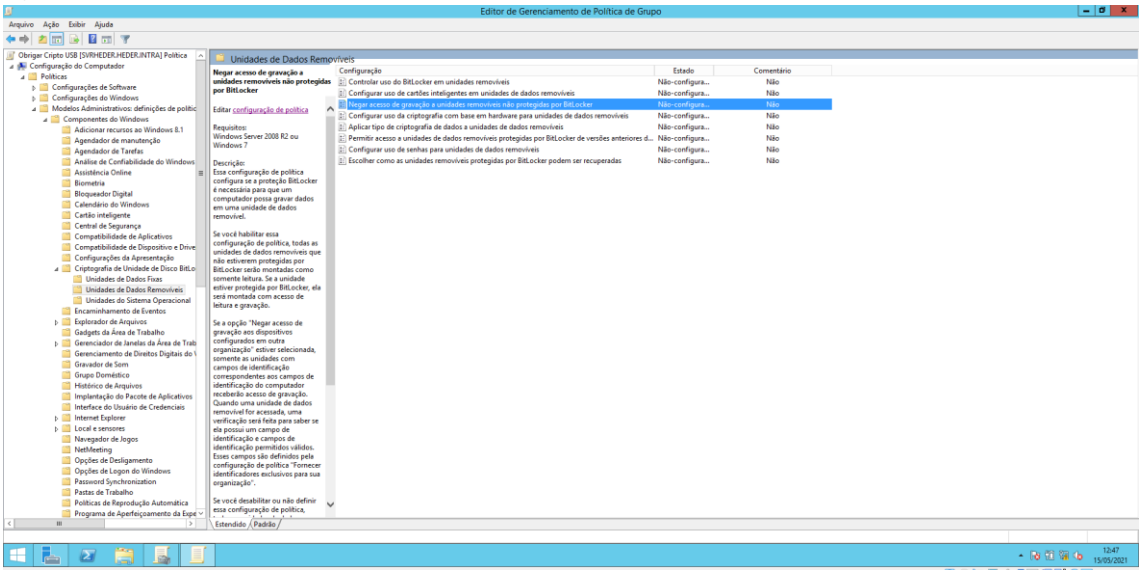
Configuração do Computador > Políticas > Modelos Administrativos: definições de políticas (arquivos ADMX) recuperadas do computador local > Componentes do Windows > Criptografia da Unidade de Disco Bitlocker > Unidade de Dados Removíveis

A) -

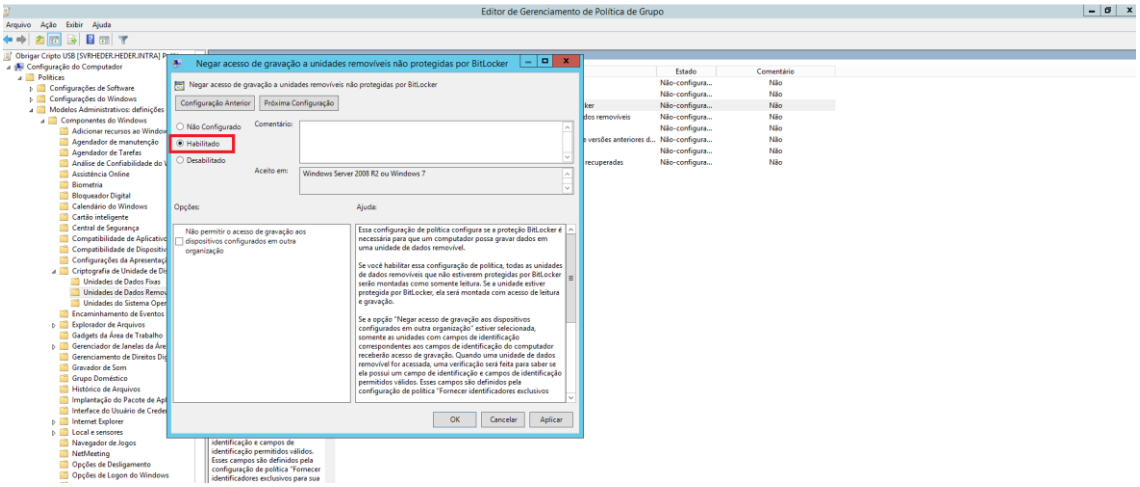


4.1 – No Menu do Lado direito será apresentado algumas opções de configurações que estão disponíveis. Iremos desativar o acesso de gravação a dispositivos USB não criptografados, clicando duas vezes no item de configuração**: Negar acesso de gravação a unidades removíveis não protegidas pelo Bitlocker** e depois ativando-a.

A) -



B) -



Como podemos observar, existe a opção de negar a gravação aos dispositivos configurados em outra organização. Restringindo assim a gravação apenas para dispositivos que foram correspondentes a organização do computador. O que não será aplicado em nosso cenário.

Após clicar em Ok e fechar a de diretiva de grupo, o sistema salvará as configurações estabelecidas e a GPO estará devidamente criada.

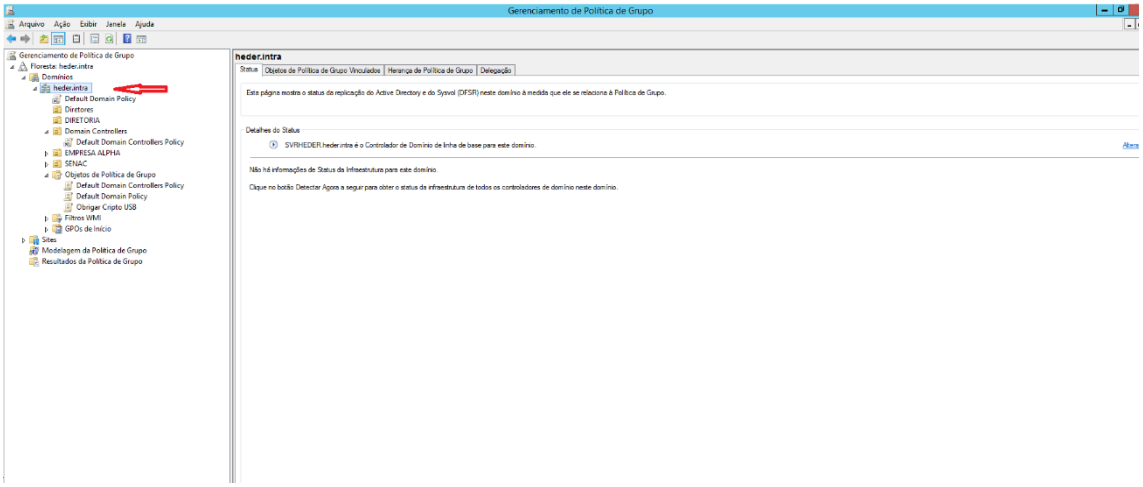
Passo II – Aplicando a GPO

Uma vez criada a GPO precisaremos agora habilitar o uso da nova Política de Grupo.

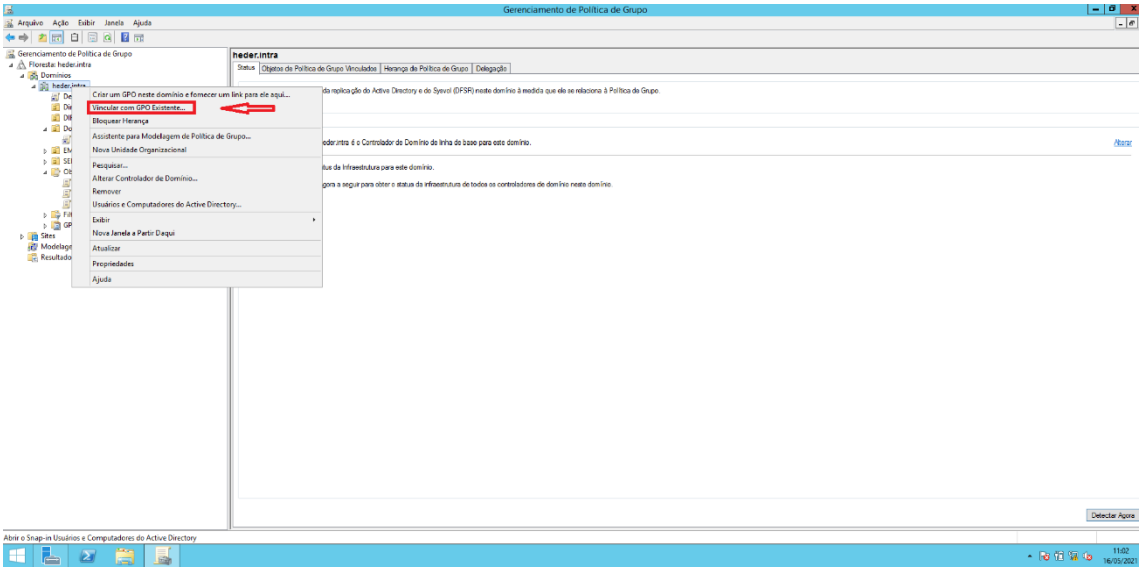
Iremos habilitá-la em nosso domínio, no meu caso; *heder.intra*

1 – Dentro do Gerenciador de Política de Grupo iremos selecionar o domínio com o nome HEDER.INTRA e clicaremos com o botão direito do mouse para acessar a opção *Vincular com GPO existente...* e selecionar a nossa GPO.

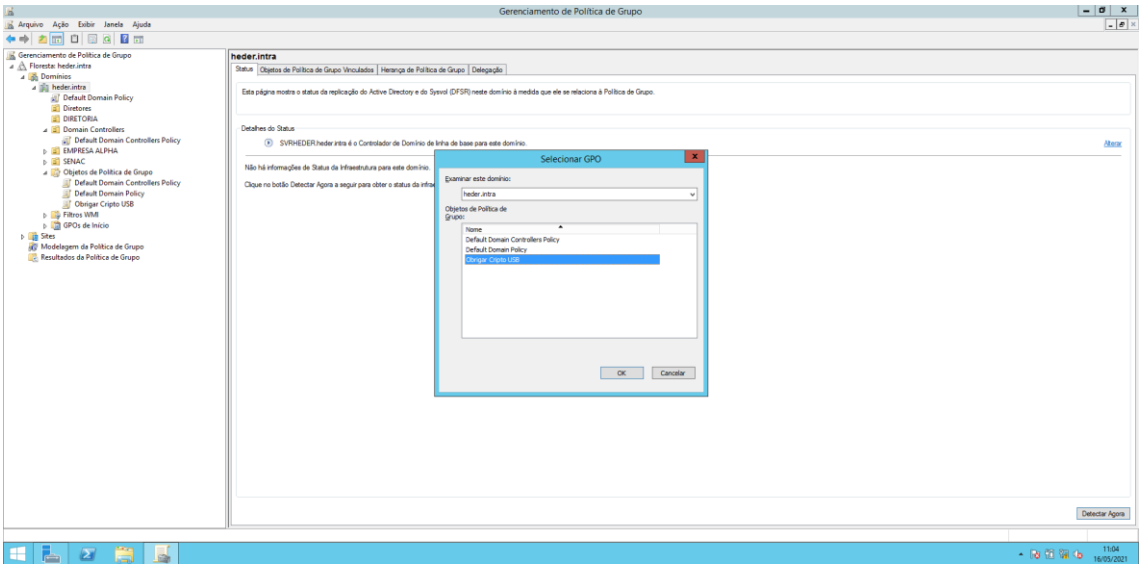
A) -



B) -



C) –

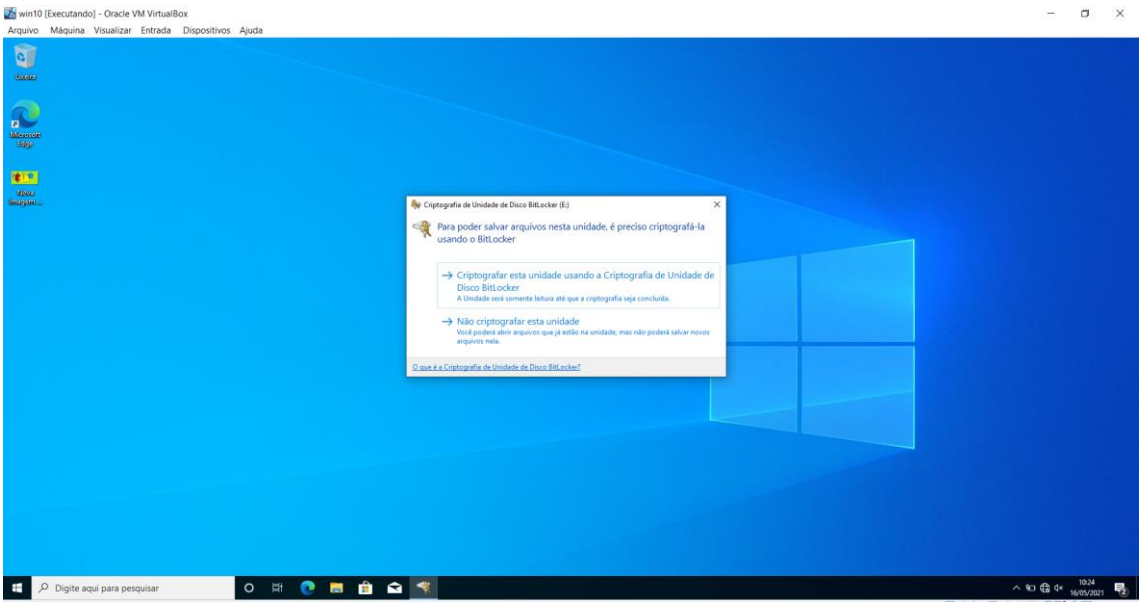


2 – Depois de selecionar a nossa GPO corretamente, pode ser necessário esperar de 10 a 20 minutos e reiniciar a máquina do usuário para aplicação dela.

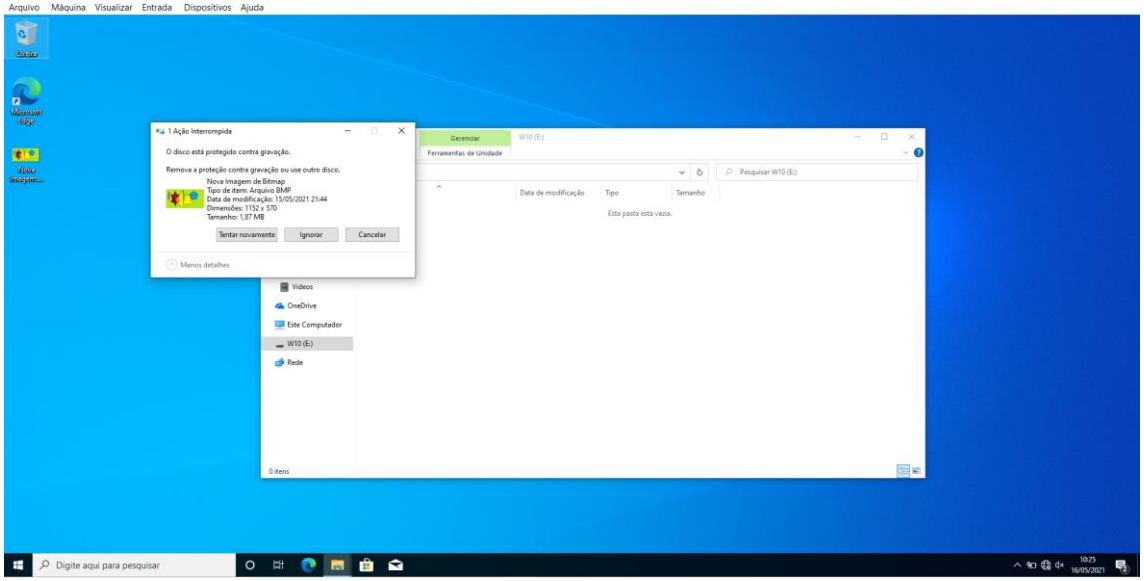
Para testar a configuração, é necessário conectar uma unidade de armazenamento USB ao computador e tentar salvar um arquivo. (O dispositivo só poderá ser reconhecido como ‘somente leitura’ quando não criptografado)

O computador deverá negar o acesso ao dispositivo não criptografado com Bitlocker e oferecer para criptografá-lo. Somente após encriptação o dispositivo será reconhecido para gravação.

A)-



B) – Caso de não aceitar a encriptação



Site de Documentação Microsoft: BitLocker Configurações da Política de Grupo (Windows 10) - Microsoft 365 Security | Microsoft Docs - (Negar o acesso de gravação a unidades removíveis não protegidas pelo BitLocker)

Observações finais; após testes realizados durante essa pesquisa, essa GPO só é aplicável ao domínio. Não funcionando ou executando quando aplicável apenas a uma OU escolhida.

Dessa forma, em nossa ideia original para aplicação em setor/áreas especificas, deveremos trabalhar com exceções as demais OU's.