1 INTRODUÇÃO

O sistema operacional utilizado para realizar esta atividade foi o Linux Mint, utilizei também o software Virtual Box e duas VM instaladas: Windows 10 e Windows Server. Nesta atividade será demonstrado na prática uma forma de utilização das GPO.

2 DESENVOLVIMENTO

1º passo: Depois de instalar e configurar o Windows Server 2019 corretamente, vá para o canto superior direito e clique em “tools” e depois em “Group Policy Management”.

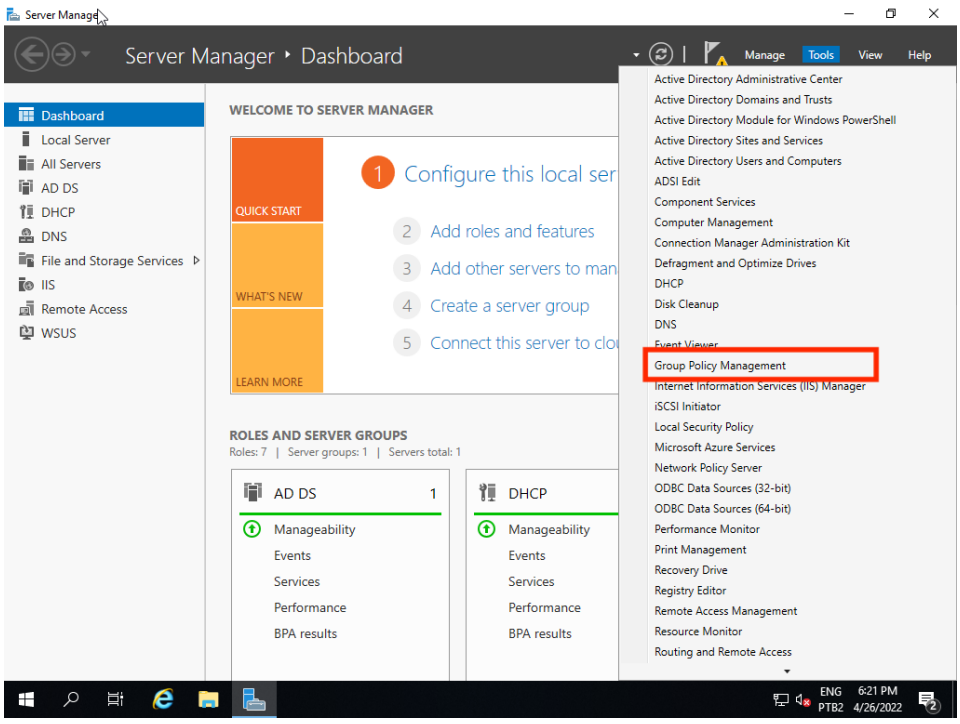

Figure 1

O objetivo da atividade é mostrar as GPO’s funcionando e o processo de configurações, portanto a partir de agora irei demonstrar cada configuração de cada GPO criada e depois seu funcionamento.

- **GPO que se refere ao bloqueio do painel de controle**: na coluna da esquerda, observamos que o bloqueio está direcionado para usuário “user

configuration” e não para computador “computer configuration”. Na coluna da direita podemos observar que a configuração “prohibt acces to Control Panel and PC settings” está ligada isto significa que esta GPO tem a função de bloquear o acesso ao painel de controle e configurações do PC que está no domínio que esta GPO trabalha.

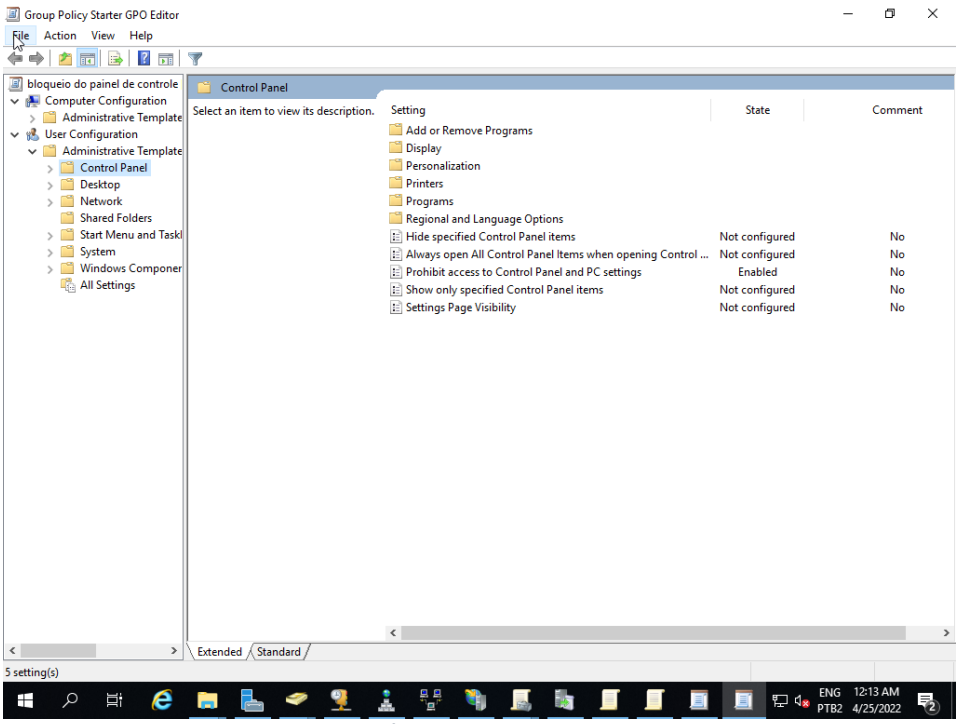

Figure 2

- **GPO que se refere ao Bloqueio da configuração que o sistema seja reiniciado automaticamente após uma atualização (Windows Update):** Observemos que o bloqueio está direcionado para um computador “computer configuration” e não para um usuário. Na coluna da direita podemos observar que a configuração “Do not adjust default option to 'Install Updates and Shut Down' in Shut Down Windows” está ligada isso significa que quando houver alguma atualização, não será feito como escolha padrão instalar as atualizações e desligar o Windows para reiniciar.

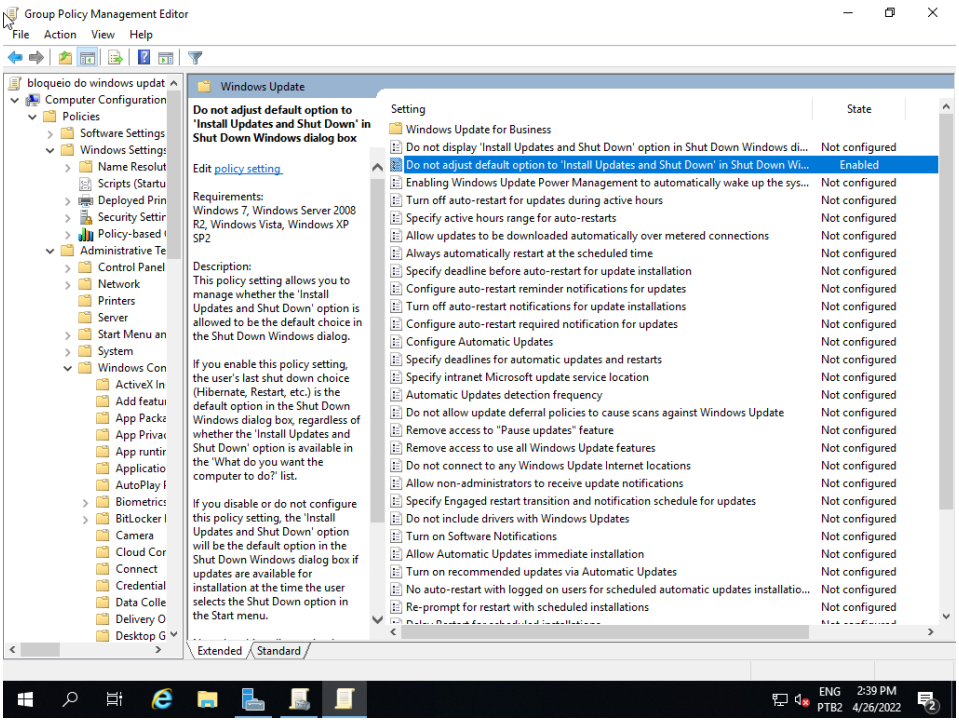

Figure 3

- **GPO que se refere ao bloqueio de instalação de novos softwares:** Observemos as configurações feitas para o computador “computer configuration” e não usuário, elas estão descritas em “Executable Rules”. Na figura 5 observamos outra configuração, neste caso referente ao sistema em que automatiza a identificação de aplicações. Clique em “Aplication identity” e efetue a edição. Após a edição da GPO o computador não permitirá a instalação de novos softwares.

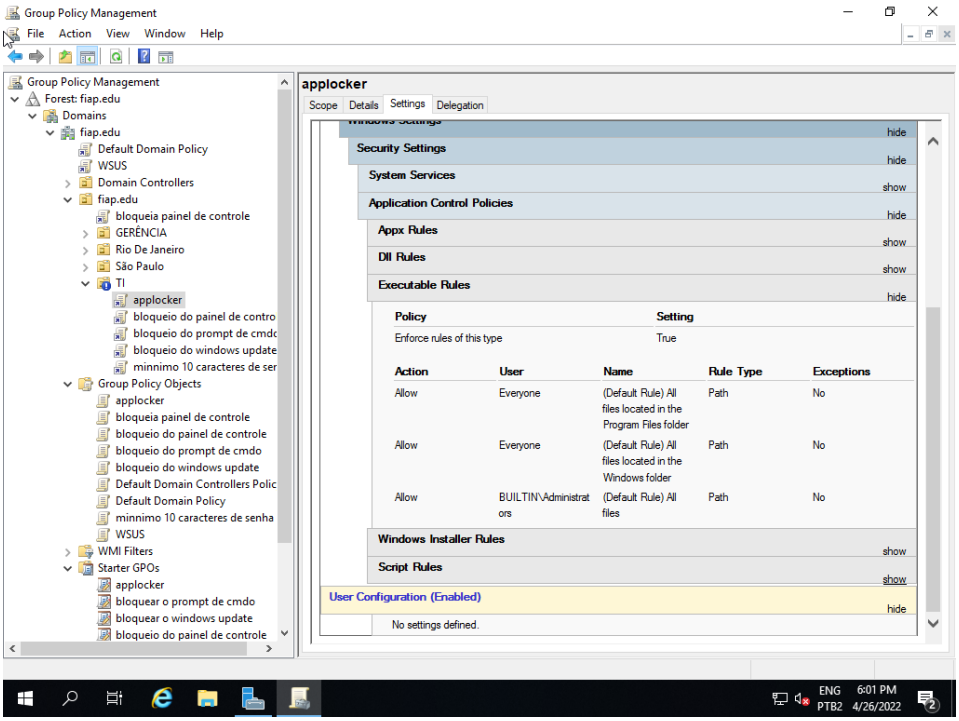

Figure 4

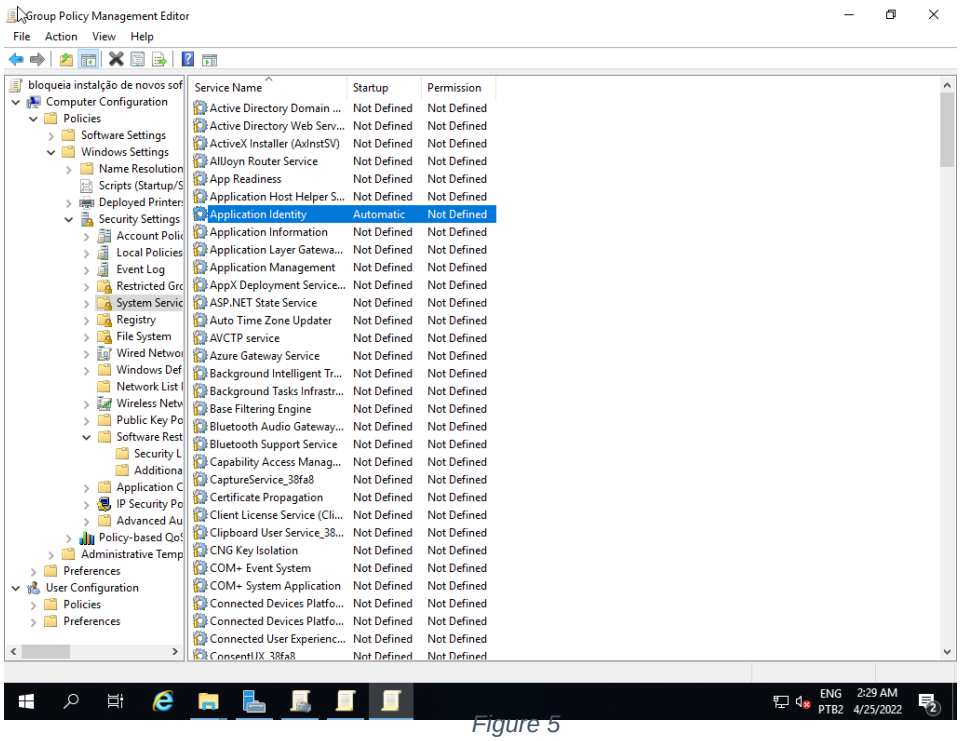

Figure 5

- **GPO referente ao bloqueio do prompt de comando:** podemos observar que as configurações são ligadas ao usuário e não ao computador, na coluna da esquerda. Na coluna da Direita podemos observar que a configuração “A Prevent access to the command prompt” está “enable”, neste caso com esta forma de configuração, o usuário não conseguirá acessar o prompt de comando.

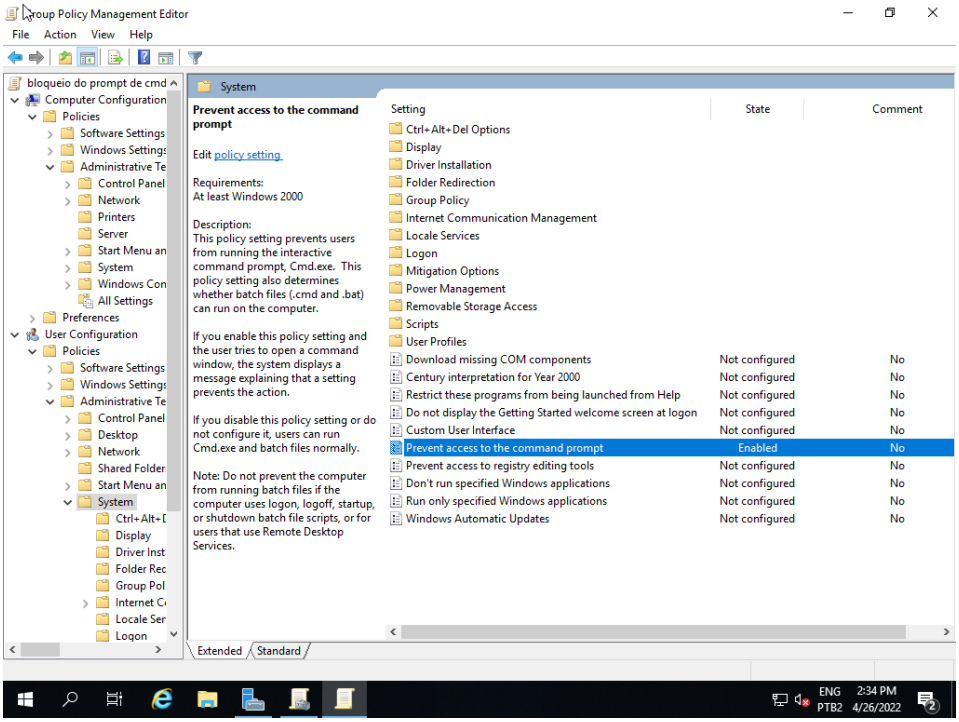

Figure 6

- **GPO que determina o número mínimo de 10 caracteres para uma senha:** agora observamos que as configurações são destinadas ao computador e não ao usuário, elas estão descritas em “System/PIN Complexity” que tem uma política que exige um número mínimo de 10 caracteres para a senha e esta política está “enable”.

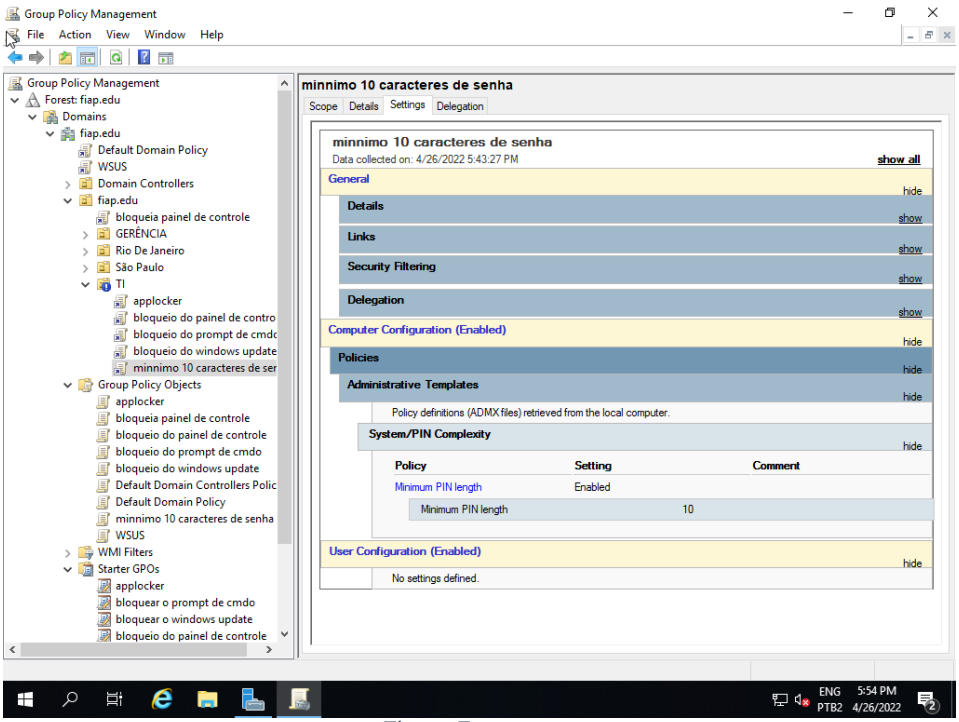

Figure 7

- A seguir demonstrarei com capturas de tela o funcionamento de cada GPO:

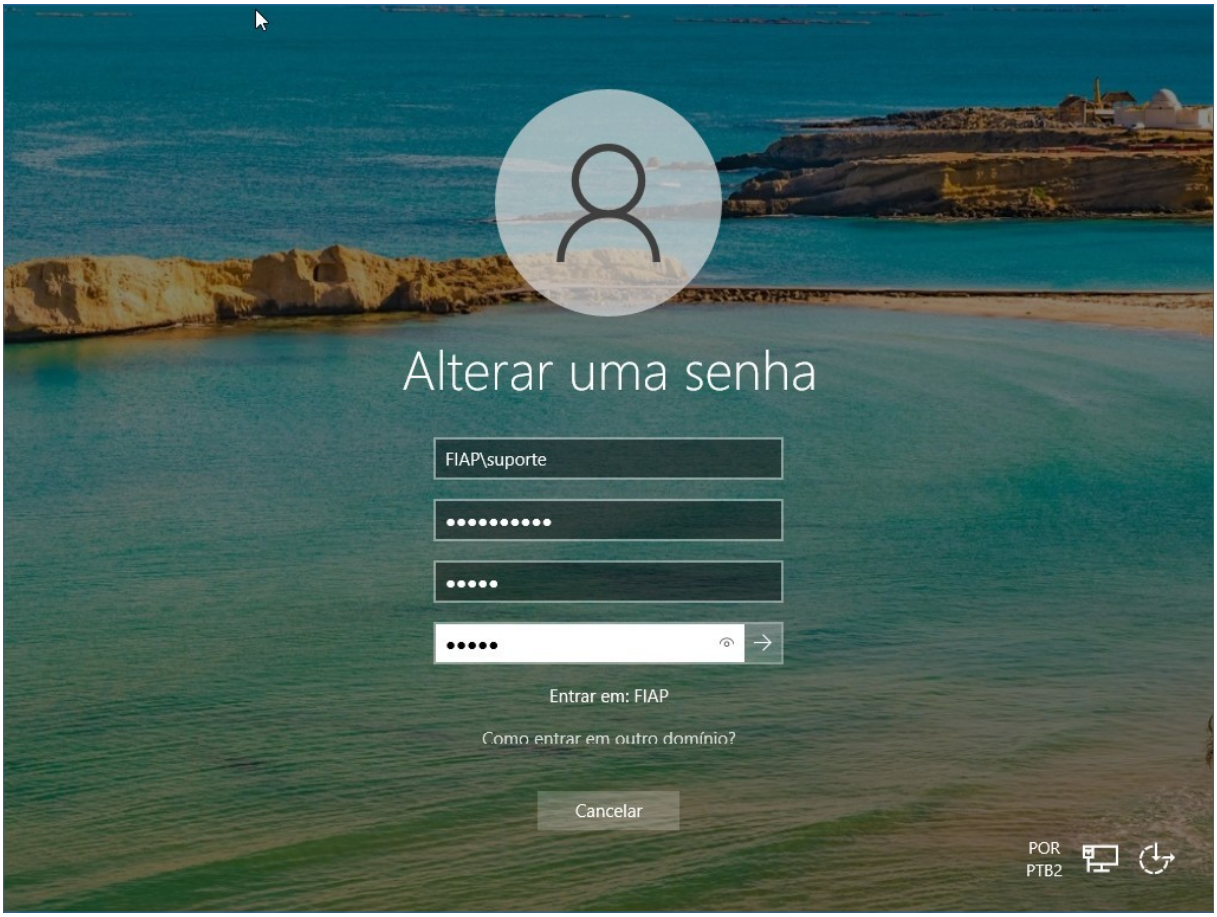

Figure 1: tentativa de trocar a senha com 5 caracteres

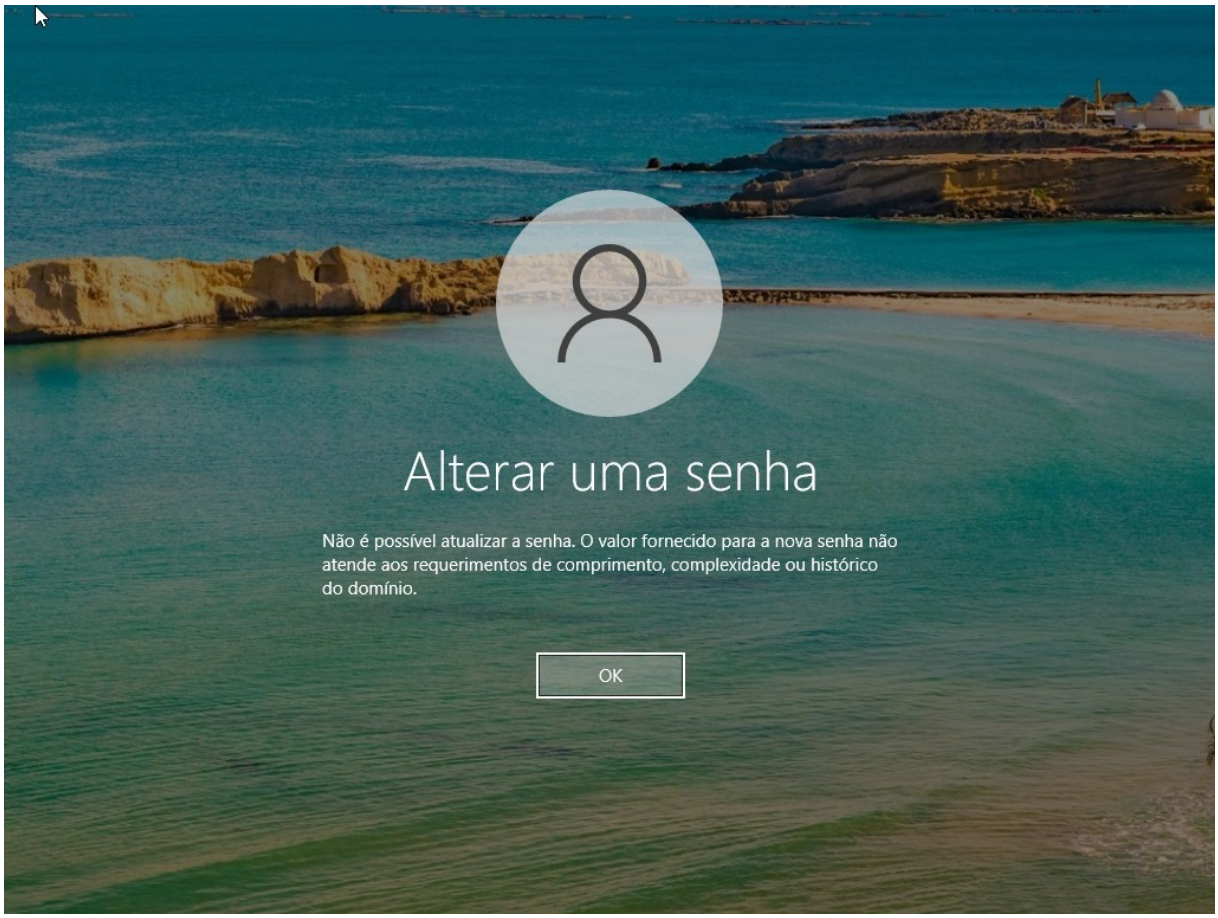

Figure 2: resultado

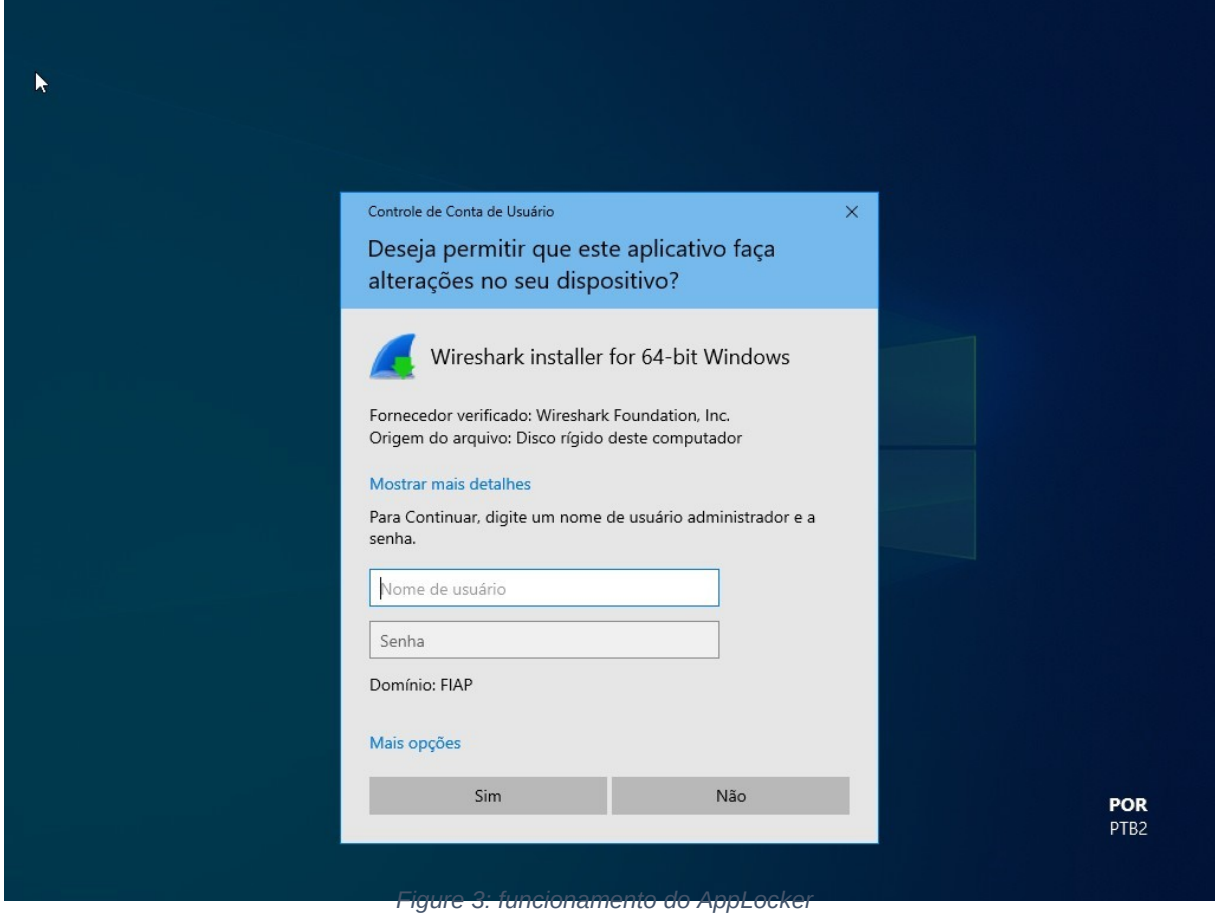

Figure 3: funcionamento do AppLocker

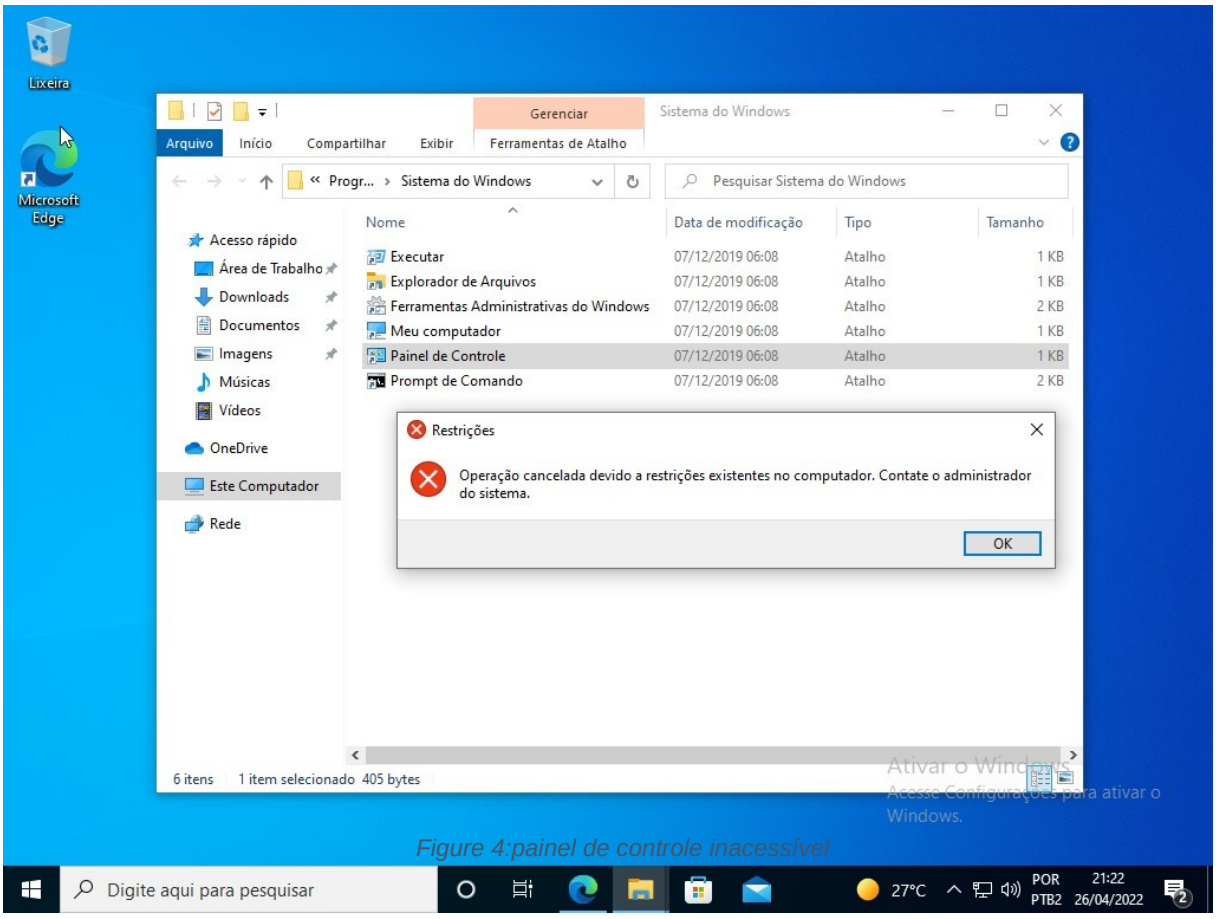

Figure 4:painel de controle inacessível

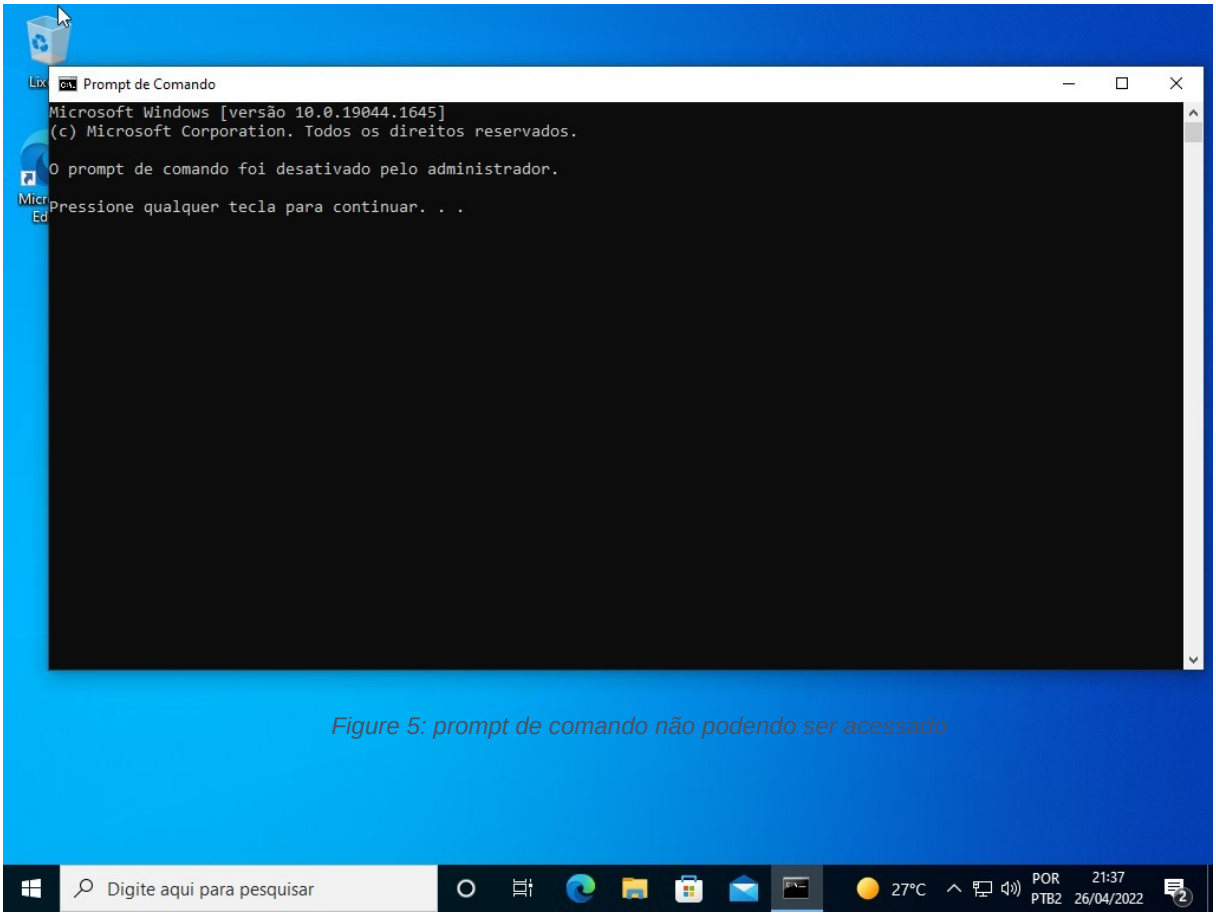

Figure 5: prompt de comando não podendo ser acessado

Obs: Não consegui demonstrar tão bem o bloqueio de instalação de novos softwares, utilizei o wireshark como base.