# *DOCUMENTAÇÃO DE GPO*

## BLOQUEANDO O ACESSO AO POWERSHELL NAS MÁQUINAS

Nessa documentação estarei mostrando como podemos bloquear o acesso ao PowerShell utilizando o Group Policy (GPO) em um domínio Windows Server.

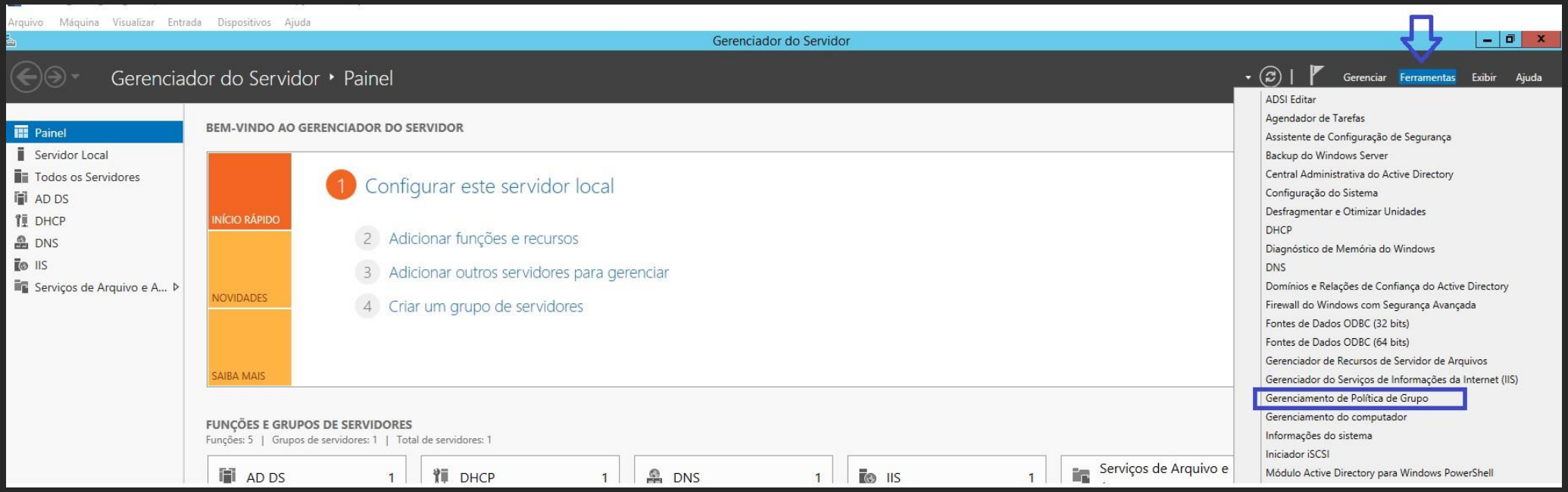
Muitos administradores estão procurando formas de barras os ataques e eliminando buracos de segurança em seus cenários, com isso diminuir esse risco.

Vamos ver na prática como fazer:

Os passos abaixo foram executados no Windows Server 2012 r2

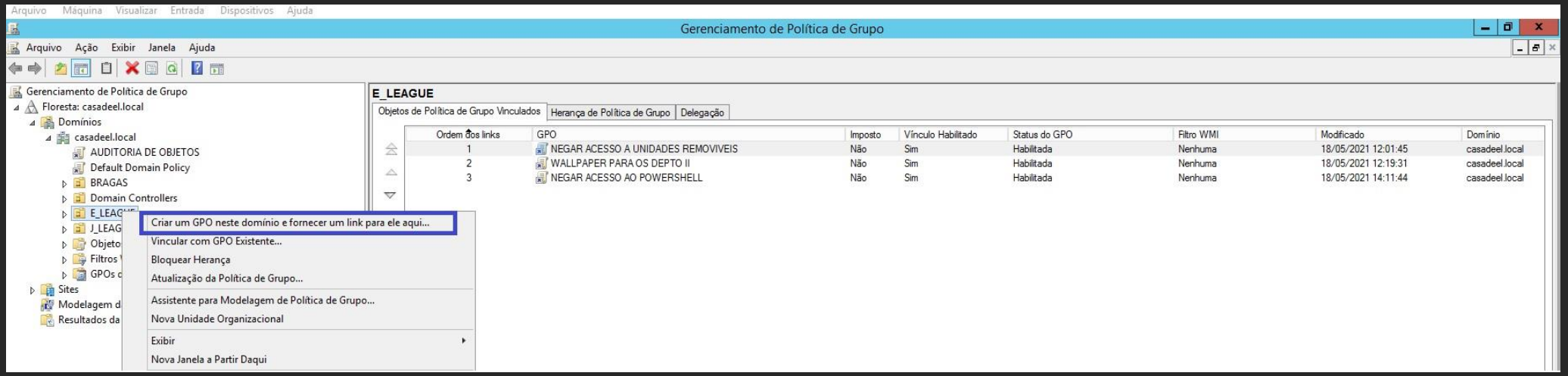
1º PASSO – Acessar a GPO

Ao abrir o Gerenciador de servidor > Painel, acessar “Ferramentas” e em seguida acessa “Gerenciamento de Política de Grupo”



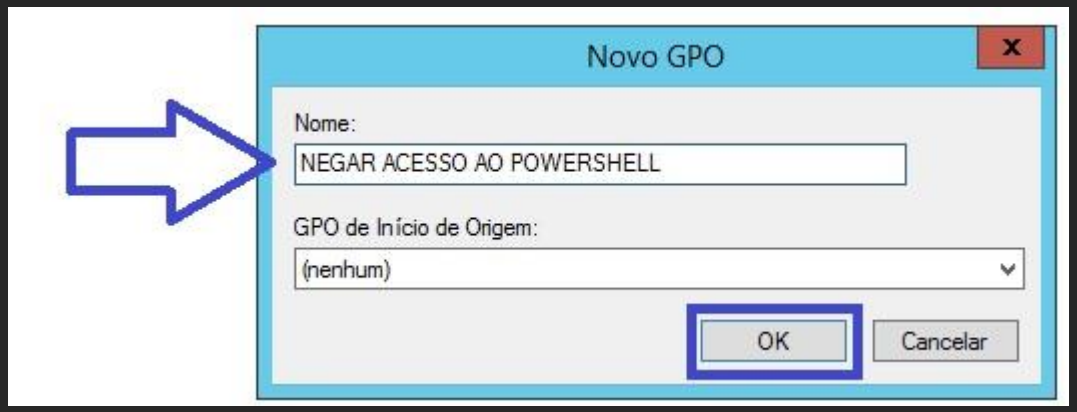
## 2º PASSO - Criar a GPO na Unidade Organizacional (OU) desejada

Clicar com o botão direito do mouse na OU que deseja criar a GPO, em seguida clicar em “Criar um GPO nesse domínio e fornecer um link para ela aqui...”



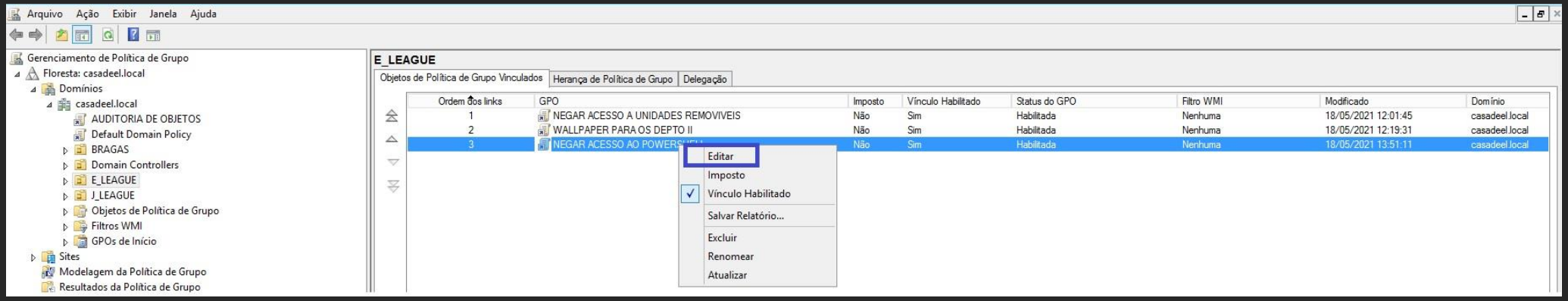

## 3º PASSO – Nomeando a GPO

No campo Nome, incluir o nome da GPO e em seguida clicar em “ok”



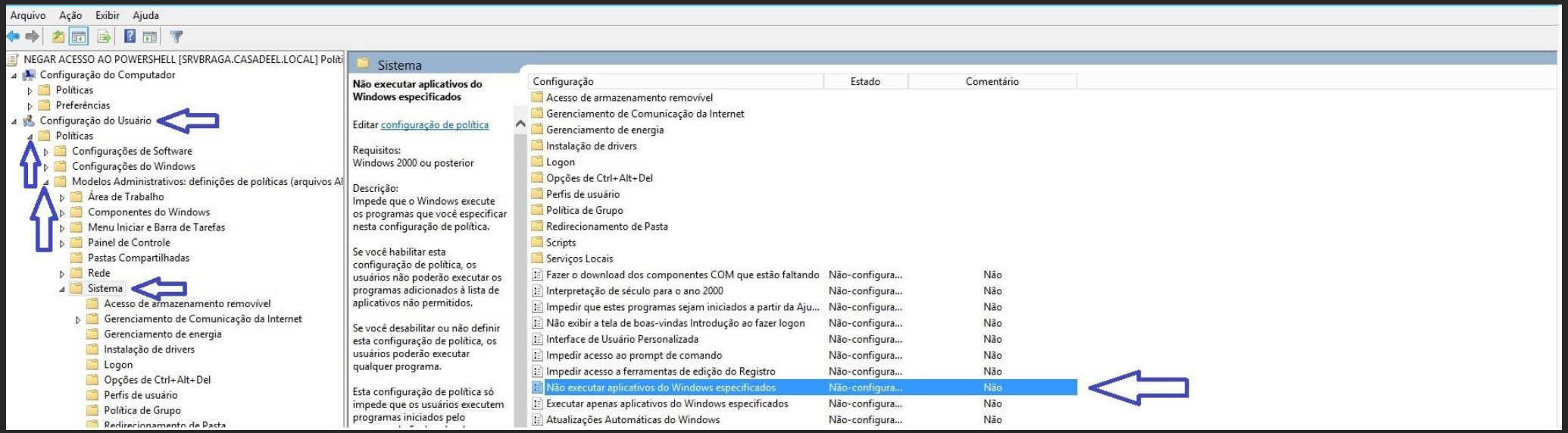
4º PASSO – Acessar o editor da GPO

Clicar com o botão direito do mouse e em seguida em “Editar”




5º PASSO – Acessar a GPO que iremos criar.

Seguir o passo abaixo, e clicar duas vezes na GPO “Não executar aplicativos do Windows específicos”



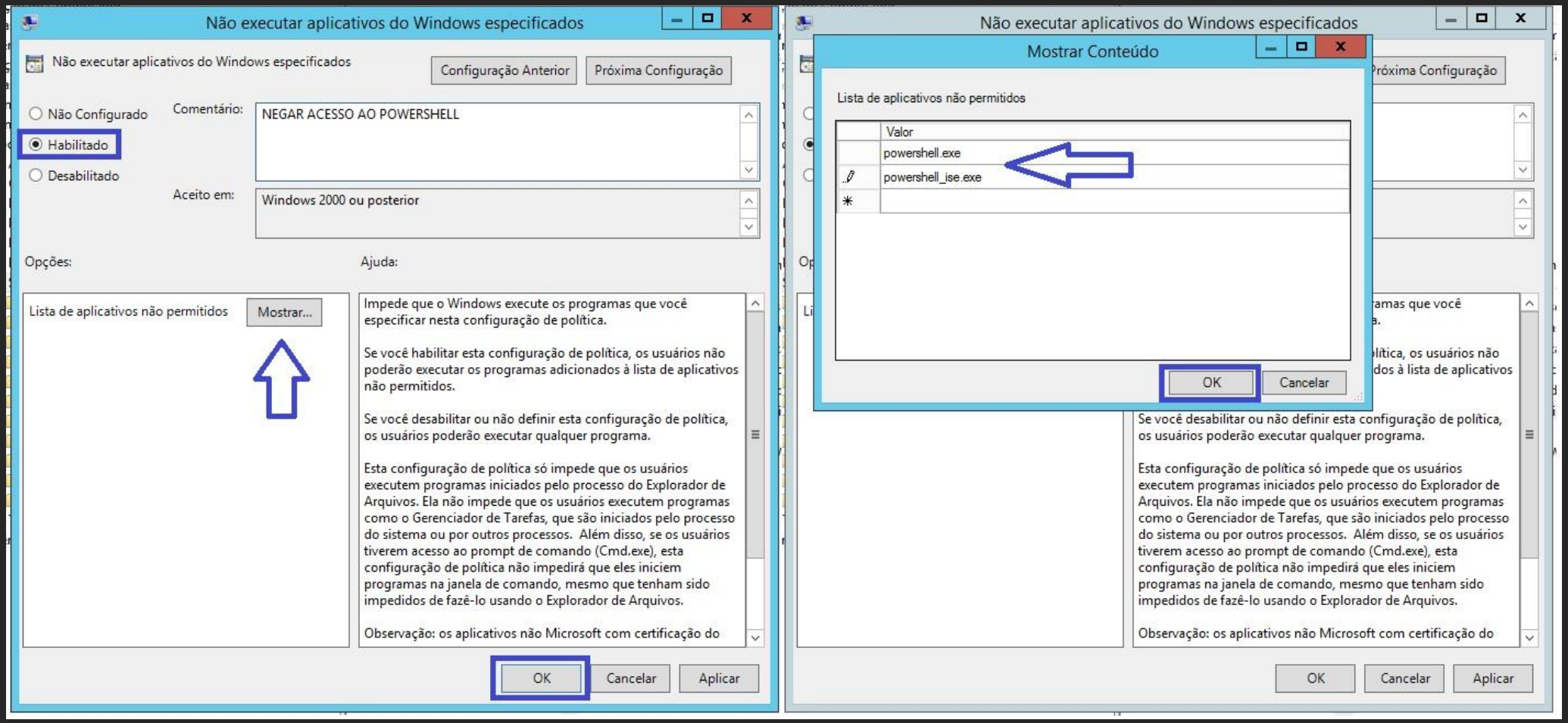
6º PASSO – Configurar a GPO

Após a GPO aberta, seguir a sequência.

Selecionar a opção “Habilitado” – Comentário: é opcional

Clicar em “Mostar...” – digitar o nome do programa, *powershell.exe* e *powershell_ise.exe*

Clicar em “ok” e “ok” novamente



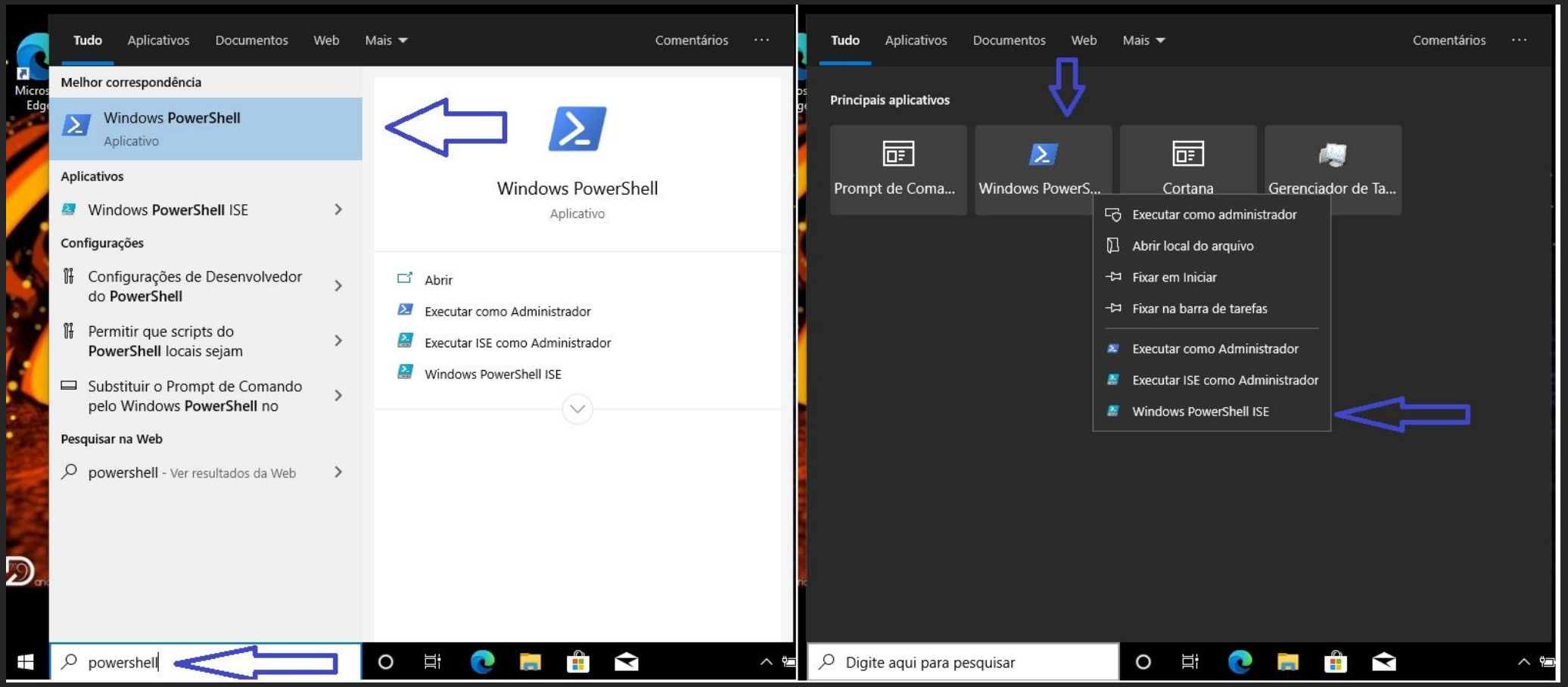

GPO criada.

Testando em uma estação de trabalho.

Na barra de tarefa do Windows no campo de “pesquisa” ao lado do iniciar digite *Powershell* e clique no programa.

Na imagem a esquerda digitar *powershell* no campo de de pesquisa

Na imagem a direita deixar o cursos no campo de pesquisa nesse momento o Windows irá demostrar as últimas pesquisas, clicar com o botão direito do mouse no Windows Powershell e em seguida em Powershell_ise




*Ambos os casos não irão executar o programa.*