Valid Certificadora Digital LTDA

Infraestrutura

Controle da versão

Nome do responsável	Assunto/ Motivo	Revisão	Data
Marina Santos	Versão Inicial	1.0	10.08.2012
Marina Santos	Alteração no item 2.1 e no procedimento 5.	1.1	27.11.2012
Fabiano Silva de Souza	Alteração no item 2.15, 3.6; Alteração procedimento 4, 7, 8, 9 e 10.	1.2	11.01.2013
Rodrigo Lima	Criação dos itens Estrutura Lógica Sistemas Operacionais Homologados e Gestor Técnico. Atualização do item 2.4 e procedimento 4 sobre Internet Explorer 10.	1.3	29.07.2013
Rodrigo Lima	Alterado o item 2.14 de Pastas Valid Certificadora para Repositório de Softwares e arquivos digitalizados. Incluído no item 7 o ID Protect Versão 6.13.19, Valid CSP e Valid LOG Sender.	1.4	11.12.2013
Fabiano Silva de Souza	Remoção dos itens Valid CSP, Valid LOG Sender e procedimento 16.	1.5	25.08.2014
Alexandre Cerullo	Atualização de sistemas operacionais com inclusão do Windows 8.1 e alteração dos prints e configurações de Windows 7 para Windows 8.1	1.6	21.01.2015
Gabriel Fernando	Atualização de Sistemas Operacionais, inclusão do Windows 10 e alteração de prints e configurações de procedimentos.	1.7	20.04.2016
Ricardo Vidal	Inclusão de novas políticas baseado no DOC ICP 03.01 (Resolução 151).	1.8	09.10.2019
Ricardo Vidal	Atualização do Item 3 - SISTEMAS OPERACIONAIS HOMOLOGADOS. Inclusão dos itens 2.18 e 2.19.	1.9	01.06.2020

Índice

1. INTRODUÇÃO

De acordo com os requisitos propostos pelo ITI (Instituto Nacional de Tecnologia da Informação), este documento informa regras e padronização dos ambientes lógicos de uma Autoridade de Registro, disposto pelo DOC-ICP-03.01 - Versão 3.0.
Caso tenha alteração no documento, a Valid Certificadora se compromete divulgá-lo a todas suas Autoridades de Registro vinculadas, logo após a alteração. O Documento pode ser alterado sem aviso prévio.
Todo o procedimento deve ser executado como usuário administrador do Windows.
O gestor técnico é responsável pela configuração de máquina de AR.

2. ESTRUTURA LÓGICA

O ambiente da Autoridade de Registro (AR) poderá ser organizado através de Grupo de Trabalho Local ou através de Domínio via Microsoft Active Directory. No primeiro cenário as configurações contidas neste documento deverão ser realizadas através da edição de políticas locais em cada um dos equipamentos. No cenário com o Active Directory as mesmas configurações serão aplicadas nas políticas do servidor e replicadas a todas as máquinas que receberem esta política do domínio, sem a necessidade de configuração local.
Este documento demonstra apenas o detalhamento das configurações realizadas em disposição de Grupo de Trabalho Local.

3. SISTEMAS OPERACIONAIS HOMOLOGADOS

Os Sistemas Valid e o processo de emissão são homologados nos sistemas operacionais Windows 7, Windows 8.1 e Windows 10 na versão 64 bits. Os sistemas operacionais em questão apresentam diversas distribuições tais como Starter, Home, Professional, Enterprise e etc.
IMPORTANTE: Para o ambiente de emissão se faz necessário o uso da versão Professional.

Este manual tem como objetivo apresentar as configurações necessárias aos equipamentos envolvidos no processo de emissão. Apenas para facilitar o entendimento foram detalhadas as etapas de configuração utilizando como base um equipamento com Windows 10. Não serão desenvolvidos outros detalhamentos técnicos para os demais sistemas operacionais, pois as configurações são exatamente as mesmas em todos os sistemas operacionais, nos itens onde existem particularidades estes são demonstrados no documento.

4. GESTOR TÉCNICO

As configurações contidas neste documento deverão ser executadas pelo Gestor Técnico da AR, sendo todos os procedimentos citados neste documento relacionados ao entendimento técnico sobre ambientes operacionais Windows. Desta forma para aplicação e manutenção das configurações citadas neste manual é necessário conhecimento técnico em ambiente Windows.

Os **itens normativos** são obrigatórios e os **itens recomendados** são opcionais.

5. CONFIGURAÇÕES DE GRUPO (GPO)

2.1 Download de Softwares

Acessar o endereço https://docvalid.validcertificadora.com.br e efetuar o download dos softwares dentro da opção SUPORTE - Gestor Técnico de acordo com a configuração da máquina.

2.2 Sistema Operacional e Hostname

Sistemas operacionais homologados pela Valid Certificadora estão listados acima. É extremamente importante validar a distribuição (Home, Professional, Enterprise, etc.) para evitar problemas com o correto funcionamento dos recursos.
Sugerimos que todas as máquinas da AR utilizem hostname padrão, estabelecido através de siglas ou conjunto de informações através da qual seja possível identificar prontamente localidade e máquina. EX: VLDSPCAMP01 (VLD: Valid, SP: São Paulo, CAMP: Campinas, 01: numeração da máquina).

2.3 Atualizações Automáticas – *Item Normativo*

Atualizações Automáticas do sistema operacional (Windows Update) devem estar habilitadas.
Procedimento1

2.4 Auditorias – *Item Normativo*

As seguintes auditorias devem estar configuradas com (êxito e falha):

Auditoria de acesso a objetos (êxito e falha);
Auditoria de acesso ao serviço de diretório (êxito e falha);
Auditoria de acompanhamento de processos (êxito e falha);
Auditoria de alteração de políticas (êxito e falha);
Auditoria de eventos de logon (êxito e falha);
Auditoria de eventos de logon de conta (êxito e falha);
Auditoria de eventos de sistema (êxito e falha);
Auditoria de gerenciamento de conta (êxito e falha);
Auditoria de uso de privilégios (êxito e falha).
Procedimento2

2.5 Visualizador de Eventos (Event Viewer) – *Item Normativo*

Os logs de auditoria do sistema operacional devem registrar os acessos aos equipamentos e devem ficar armazenados localmente por um período mínimo de 60 dias. A análise desses logs somente precisa ser realizada em caso de suspeitas quanto a acessos não autorizados ou para dirimir outros tipos de dúvidas que possam surgir sobre a utilização dos equipamentos.
Procedimento3

2.6 Data e hora – *Item Normativo*
Todos os computadores designados para operação da Autoridade de Registro devem configurar o sincronismo de data e hora via Internet. Para os casos onde existe um servidor de domínio este deverá refletir a mesma configuração.

Servidores NTP.br	
a.st1.ntp.br	200.160.7.186 e 2001:12ff:0:7::186
b.st1.ntp.br	201.49.148.135
c.st1.ntp.br	200.186.125.195
d.st1.ntp.br	200.20.186.76
a.ntp.br	200.160.0.8 e 2001:12ff::8
b.ntp.br	200.189.40.8
c.ntp.br	200.192.232.8
gps.ntp.br	200.160.7.193 e 2001:12ff:0:7::193

Procedimento4

2.7 Firewall – *Item Normativo*
As estações de trabalho da AR, devem possuir firewall pessoal ativado, com permissões de acesso mínimas necessárias às atividades, podendo esse ser substituído por firewall corporativo, para equipamentos instalados em redes que possuam esse dispositivo.
A AR pode optar por utilizar o firewall do Windows ou por utilizar os diversos Firewalls pessoais disponíveis no mercado.
Atenção: Deve-se ficar atento à questão do licenciamento dos softwares.
Procedimento5

2.8 Proteções Tela de AR – *Item Normativo*
Todas as estações de trabalho da Autoridade de Registro devem possuir a proteção de tela com no máximo 2 minutos de inatividade, solicitando logon para desbloqueio.
Procedimento6

2.9 Sites confiáveis via GPO – *Recomendável*
Os sites listados no procedimento devem estar configurados como sites confiáveis:
Procedimento7

2.10 Internet Explorer
O IE deve estar na versão 11.

2.11 Papel de parede padrão – *Recomendável*
Para padronizar os equipamentos de emissão recomenda-se a padronização do papel de parede. A ferramenta BGinfo que faz parte do pacote de softwares oferece esse recurso.
Procedimento8

2.12 Repositório de Softwares e arquivos Digitalizados – *Recomendável*
Criar uma pasta com o nome “Softwares” no disco local C:, onde deve conter todos os aplicativos/ferramentas/material da Valid Certificadora.

Criar uma segunda pasta no disco local C: com o nome “Digitalizacao” esta pasta deve ser compartilhada por todos os usuários do computador, ou seja, deve estar disponibilizada na área de trabalho de All Users/Public.

2.13 Configuração de usuário de Windows – *Item Normativo*
Por questões de segurança o usuário Administrador, deverá ser renomeado. Deve ser definida pelo menos uma conta de administrador.
Usuários Autenticados devem possuir perfil de “operadores de configuração de rede” das estações de trabalho da AR.
Apenas contas de administrador e de Agente de Registro devem estar cadastradas e disponíveis, as demais devem ser excluídas ou desativadas.
As contas devem ser configuradas individualmente, cada AGR deve possuir sua conta de usuário.
Procedimento9

2.14 Política de senha forte – *Item Normativo*
Todos os computadores designados para operação da Autoridade de Registro devem exigir senhas fortes para login, Ex: valid@1234
Cada Agente de Registro deve possuir login e senha individual para execução da atividade.

Senha deve satisfazer requisitos de complexidade
Aplicar histórico de 5 senhas memorizadas
Desativar recurso de armazenar senha usando criptografia reversível
Comprimento mínimo da senha de 8 caracteres
Duração máxima da senha de 30 dias
Duração mínima da senha de 0 dias

Procedimento10

2.15 Diretivas de Bloqueio de Conta – *Item Normativo*
As estações de trabalho da AR, incluindo equipamentos portáteis, devem possuir diretivas de senha e de bloqueio de conta.

Duração do bloqueio de conta em 60 minutos
Limite de bloqueio de conta de 5 tentativas sem sucesso
Zerar contador de bloqueios de conta após 60 minutos

Procedimento11

2.16 Bloqueio de aplicativo Loja e logon com contas Microsoft – *Item Normativo*
As estações de trabalho da AR deverão conter apenas aplicações e serviços que sejam suficientes e necessários para as atividades corporativas.
Procedimento12

2.17 Criptografia de Disco – *Item Normativo*
As estações de trabalho da AR que contém componentes da aplicação da AC/AR ou que armazenem dados de solicitantes de certificados digitais devem ser criptografadas;
Procedimento13

2.18 Desabilitar Área de Trabalho Remota – *Item Normativo*
Impedimento de login remoto, via outro equipamento ligado à rede de computadores utilizada pela AR, exceto para as atividades de suporte remoto.
Procedimento17

2.19 Não mover arquivos excluídos para lixeira – *Item Normativo*
Os arquivos e pastas que forem excluídos através do Explorador de Arquivos não serão colocados na Lixeira e, portanto, serão excluídos permanentemente.
Procedimento16

6. DRIVERS/APLICATIVOS/FERRAMENTAS

3.1 Antivírus e Anti-Spyware – *Item Normativo*
Em todos os computadores designados para operação da Autoridade de Registro é obrigatório à instalação de uma ferramenta de antivírus, antitrojan instalados, atualizados e habilitados.

3.2 Cadeias ICP-Brasil e Valid AC – *Recomendável*
Para o correto funcionamento do certificado digital é necessário que o computador confie nele, para isso é necessária à instalação das Cadeias ICP-Brasil e AC Valid.
Procedimento14

3.3 Scanner/Impressora
Os respectivos drivers devem ser instalados de acordo com os equipamentos adquiridos em cada localidade.

3.4 Sistema de Biometria Valid – *Recomendável*
Pedimos que o Gestor Técnico instale a aplicação biométrica da Valid. O sistema de biometria funciona de forma local, ou seja, deve ser instalado no perfil de cada usuário do computador.
Procedimento15

7. APLICATIVOS COMPLEMENTARES

Gerador de PDF
Adobe Reader Atualizado
Flash Player Atualizado
Java atualizado
Editor de texto e planilhas
Compactador de arquivos (ZIP)
Microsoft Visual C++ 2015 (x86/x64)
SafeSign 3.0.124
Safenet 10.3
ID Protect 6.32.01
Leitora de Cartão
Driver do Token GIESECKE & DEVRIENT
.NET Framework 4
WebScoket - VAgent

OBS: NET Framework 4 já está integrado aos sistemas operacionais Windows 8.1 e Windows 10, sendo necessária sua instalação somente em versões anteriores.

8. PROCEDIMENTOS

Procedimento 1

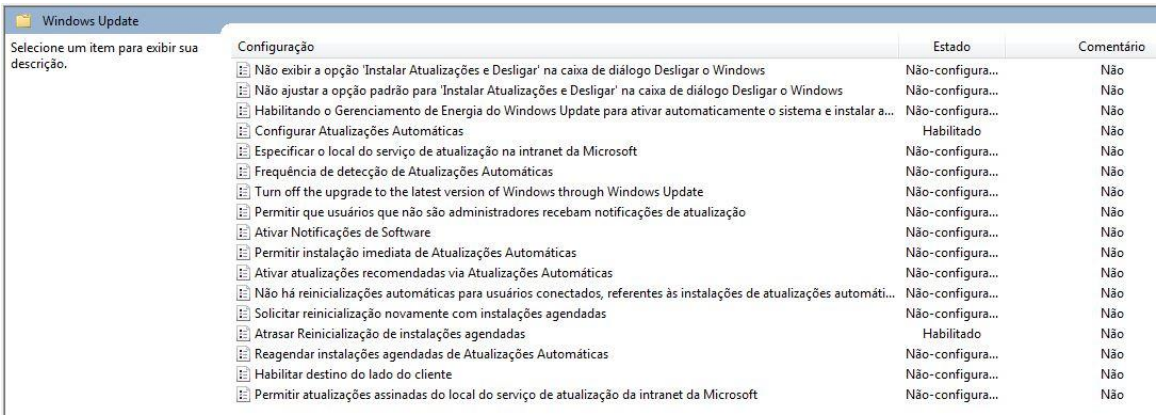
Procedimento para atualização do Sistema Operacional – Windows 7, 8 e 8.1

Manter o sistema operacional atualizado.

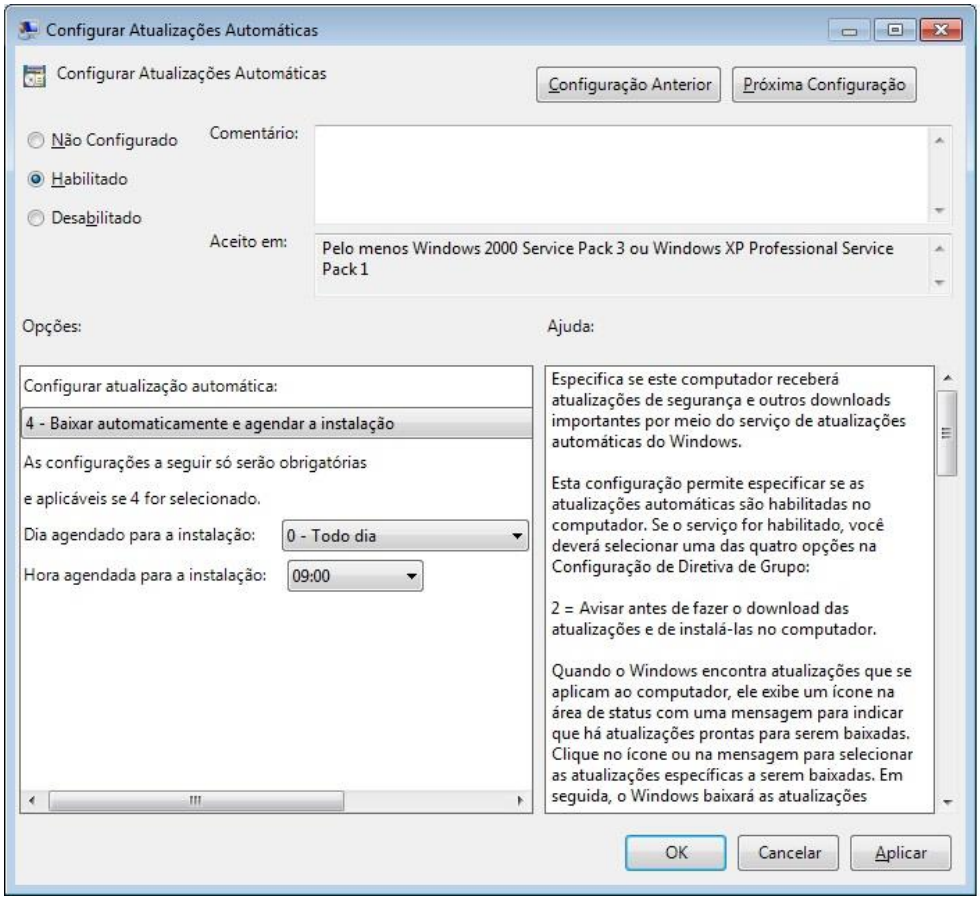
As seguintes configurações devem ser executadas:

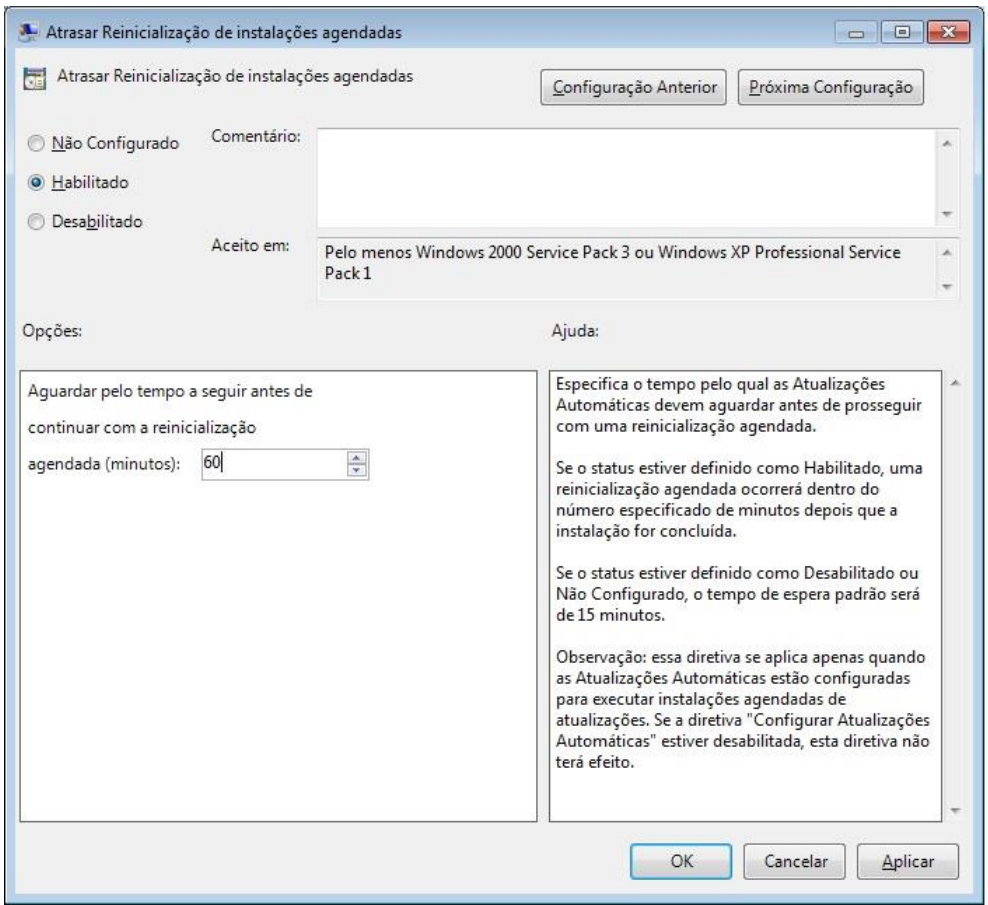
1. Iniciar -> pesquisar "**Gpedit.msc"** -> **Gpedit.msc**
Clicar em **OK.**

2. CONFIGURAÇÃO DO COMPUTADOR -> MODELOS ADMINISTRATIVOS -> COMPONENTES DO WINDOWS -> WINDOWS UPDATE.



3. Modificar os parâmetros de acordo com as figuras a seguir:





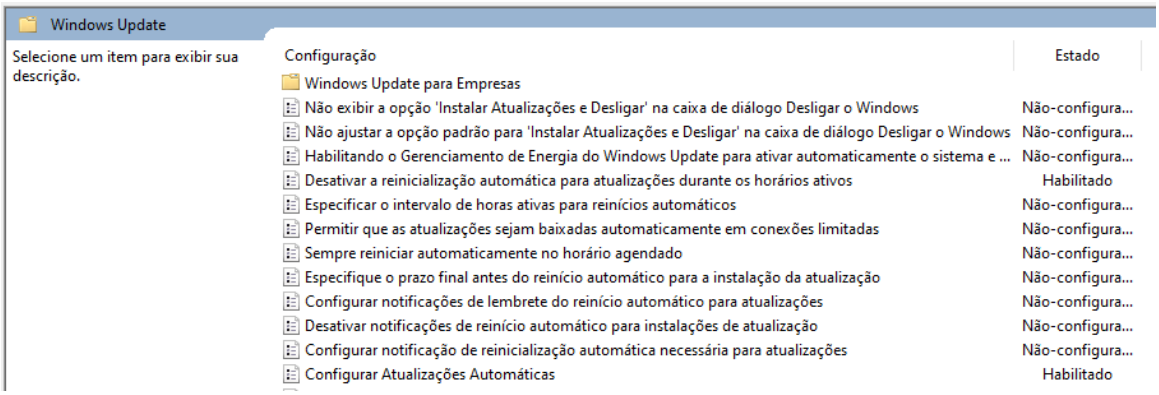
Procedimento 1 - Windows 10

Procedimento para atualização do Sistema Operacional

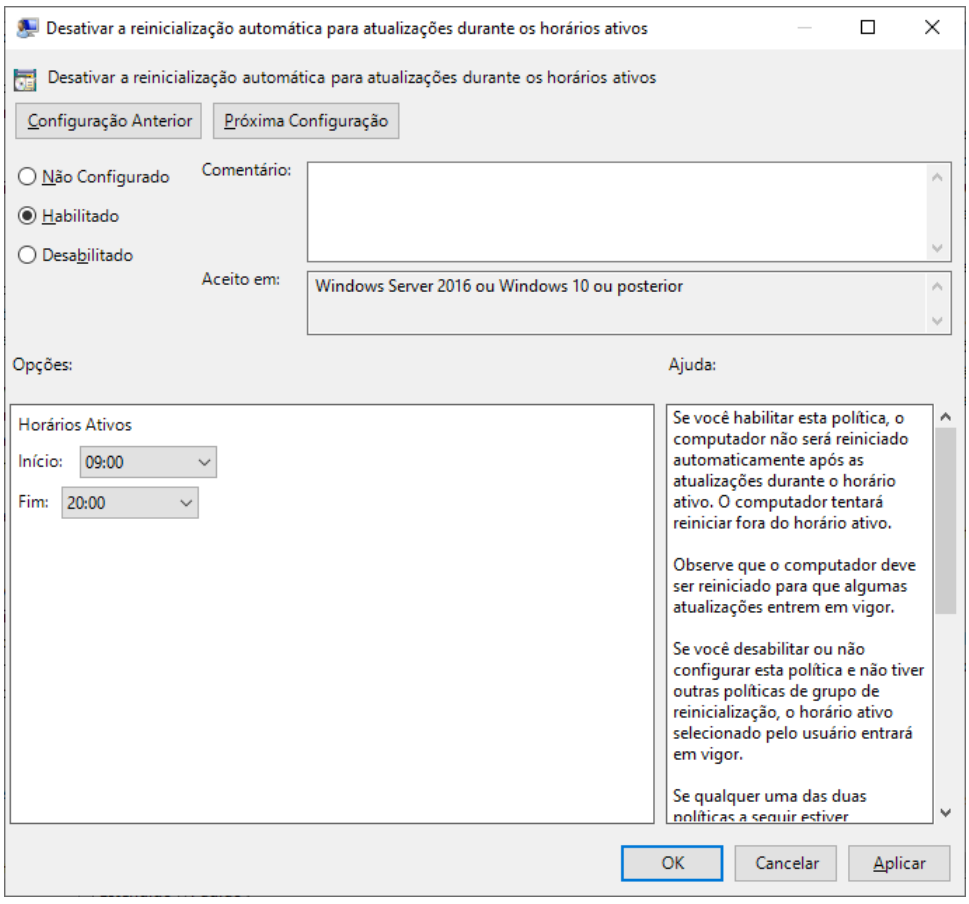
As seguintes configurações devem ser executadas:

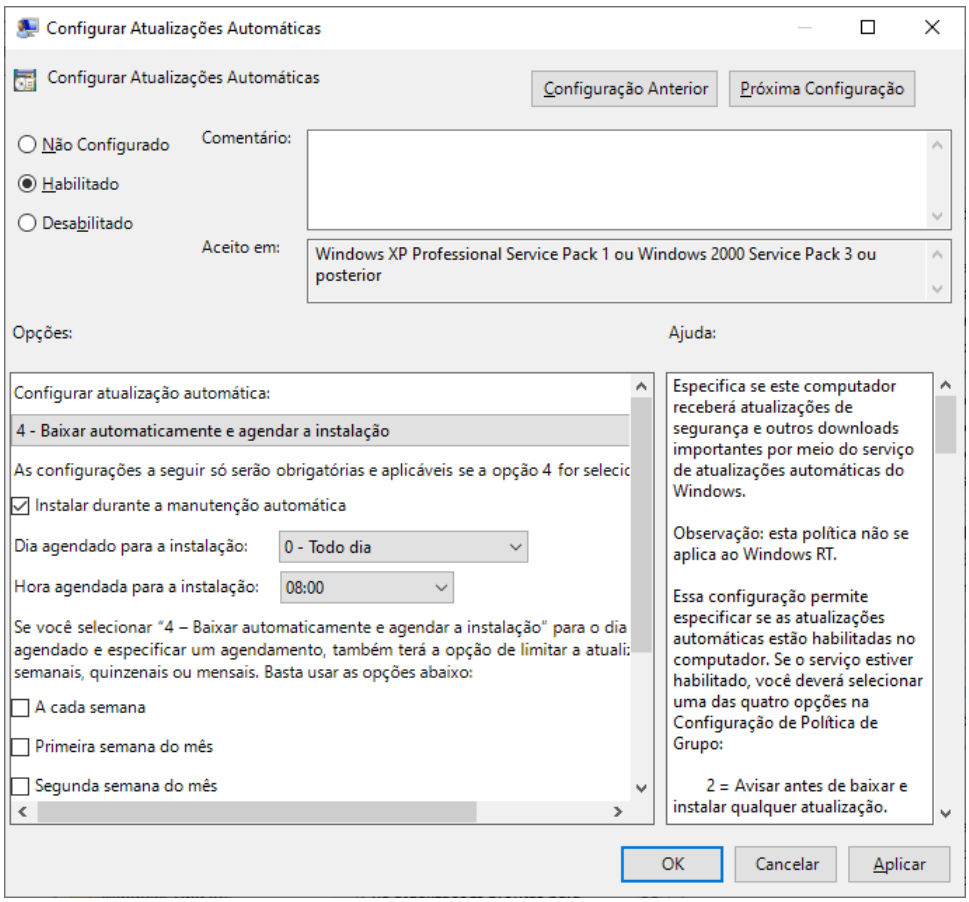
1. Iniciar -> pesquisar "**Gpedit.msc**" -> **Gpedit.msc**
Clicar em **OK.**

2. CONFIGURAÇÃO DO COMPUTADOR -> MODELOS ADMINISTRATIVOS -> COMPONENTES DO WINDOWS -> WINDOWS UPDATE.



3. Modificar os parâmetros de acordo com as figuras a seguir:





Procedimento 2

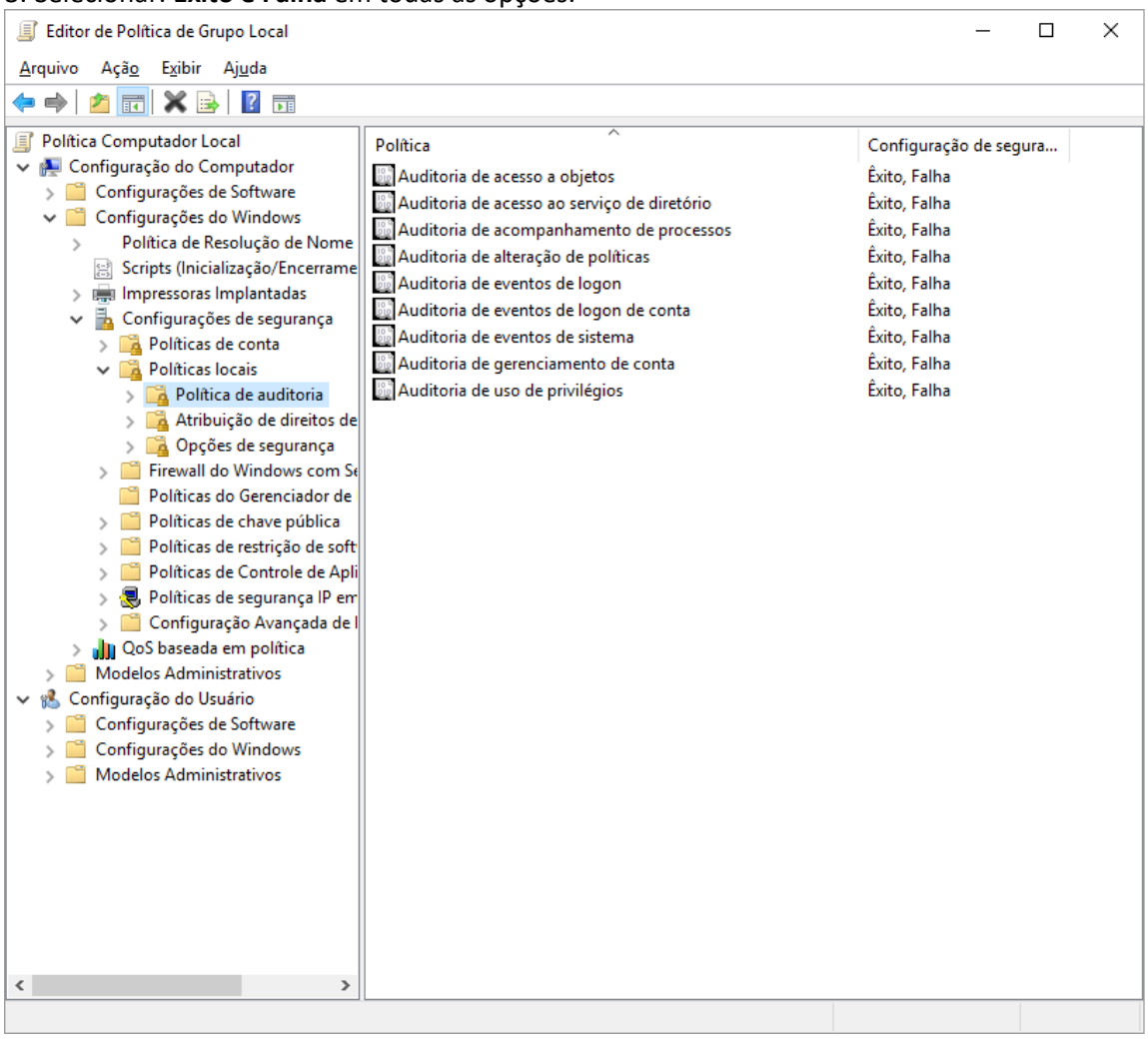
Procedimento para configuração de logs de auditoria na estação da AR.

1. Executar o aplicativo "Diretiva de Grupo".

Iniciar -> pesquisar "**Gpedit.msc"** -> **Gpedit.msc**
Clicar em **OK.**

2. Modificar os parâmetros referentes à Diretiva de Auditoria, de acordo com a figura abaixo:
Configuração do Computador -> Configurações do Windows -> Configurações de Segurança -> Políticas Locais -> Política de Auditoria

3. Selecionar: **Êxito e Falha** em todas as opções.



Procedimento 3

Procedimento para configurar as opções do Event Viewer

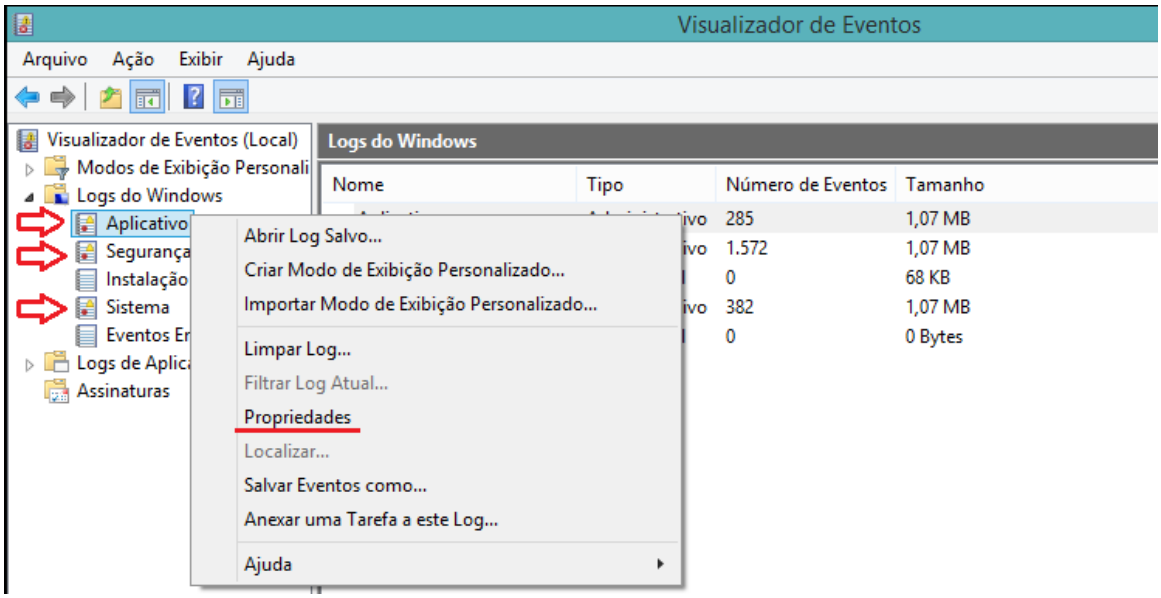
1. Executar o aplicativo “Visualizador de Eventos”.

Iniciar -> Pesquisar “eventvwr “-> eventvwr.exe.

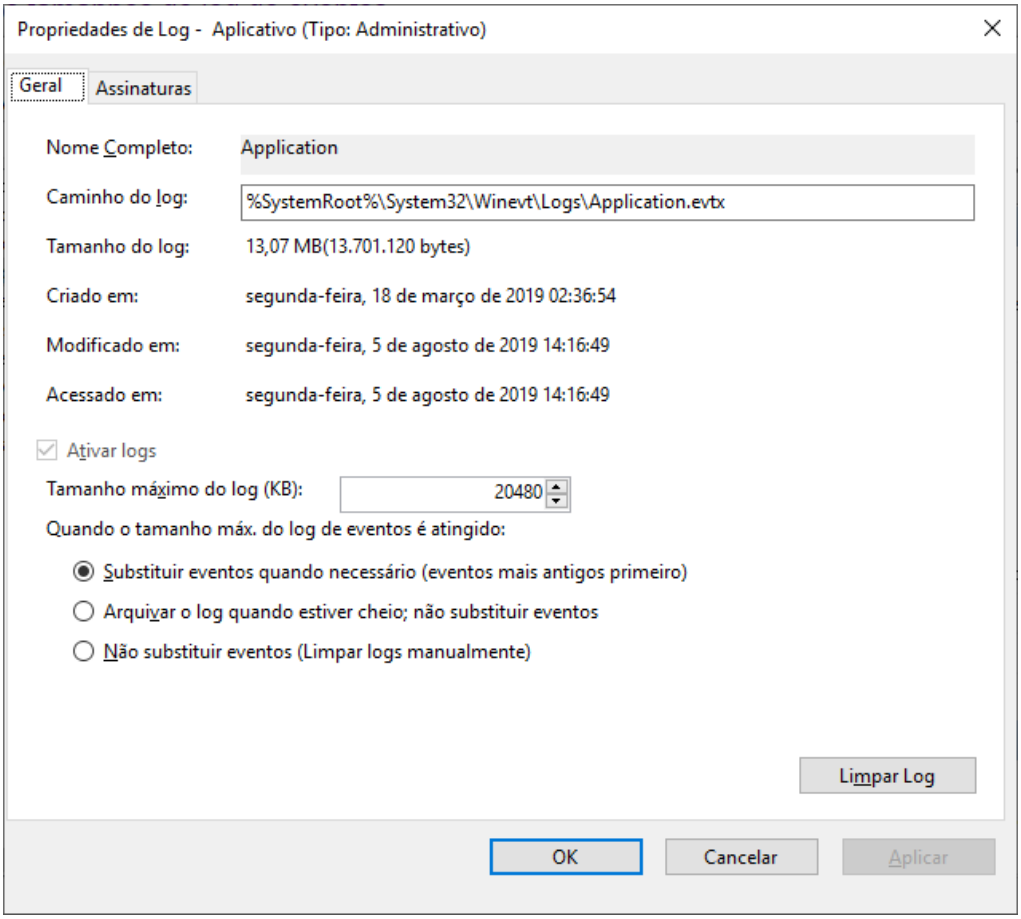
Clicar em OK.

2. Modificar os parâmetros das “Propriedades de Log”, de acordo com as figuras abaixo:

Clicar com o botão da direita sobre o “Log de Aplicativo” e selecionar a opção “Propriedades”.



Configurar o sistema conforme descrito abaixo, essa configuração deve ser replicada para os **"Logs de Segurança"** e **"Logs de Sistema"**:



2. Clicar em OK.

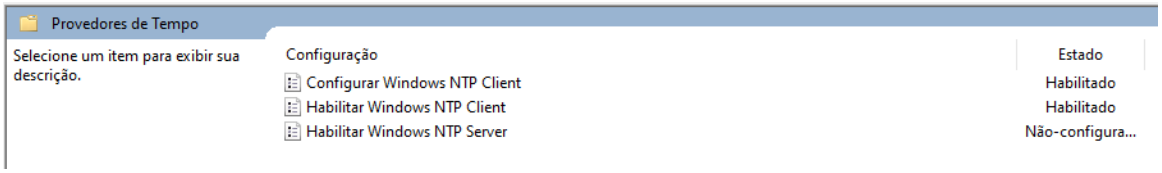
Procedimento 4

Procedimento para sincronismo de data e hora

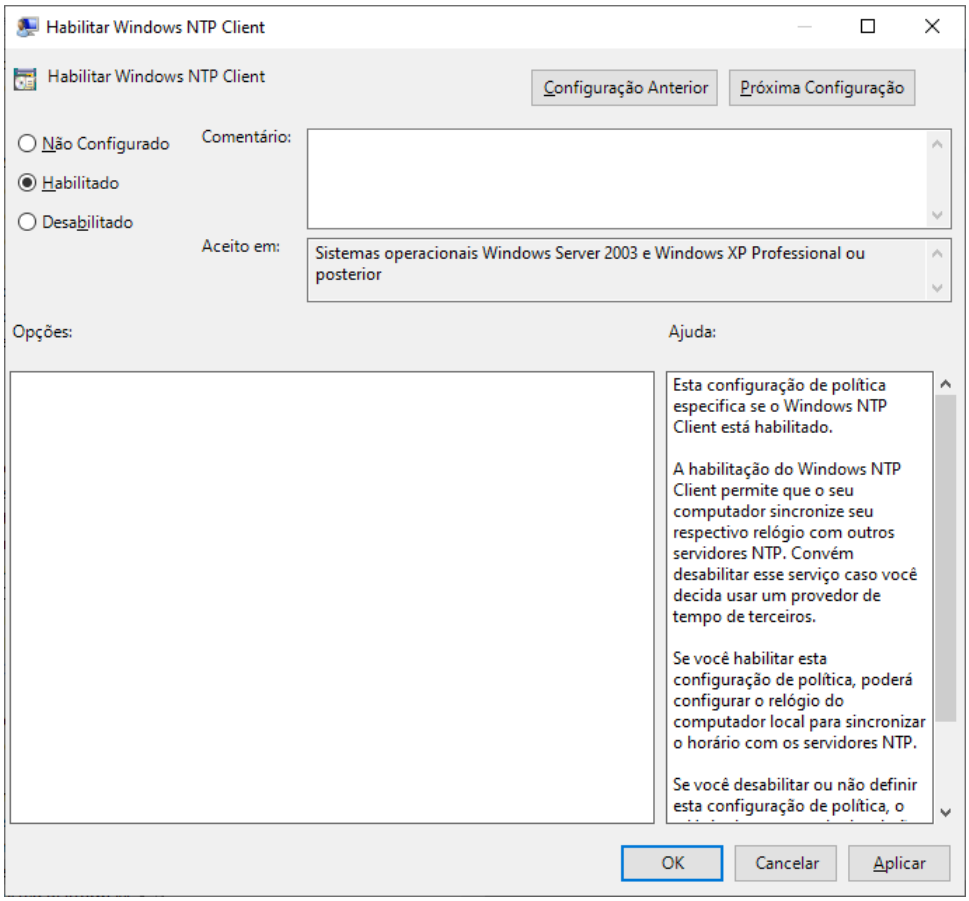
As seguintes configurações devem ser executadas:

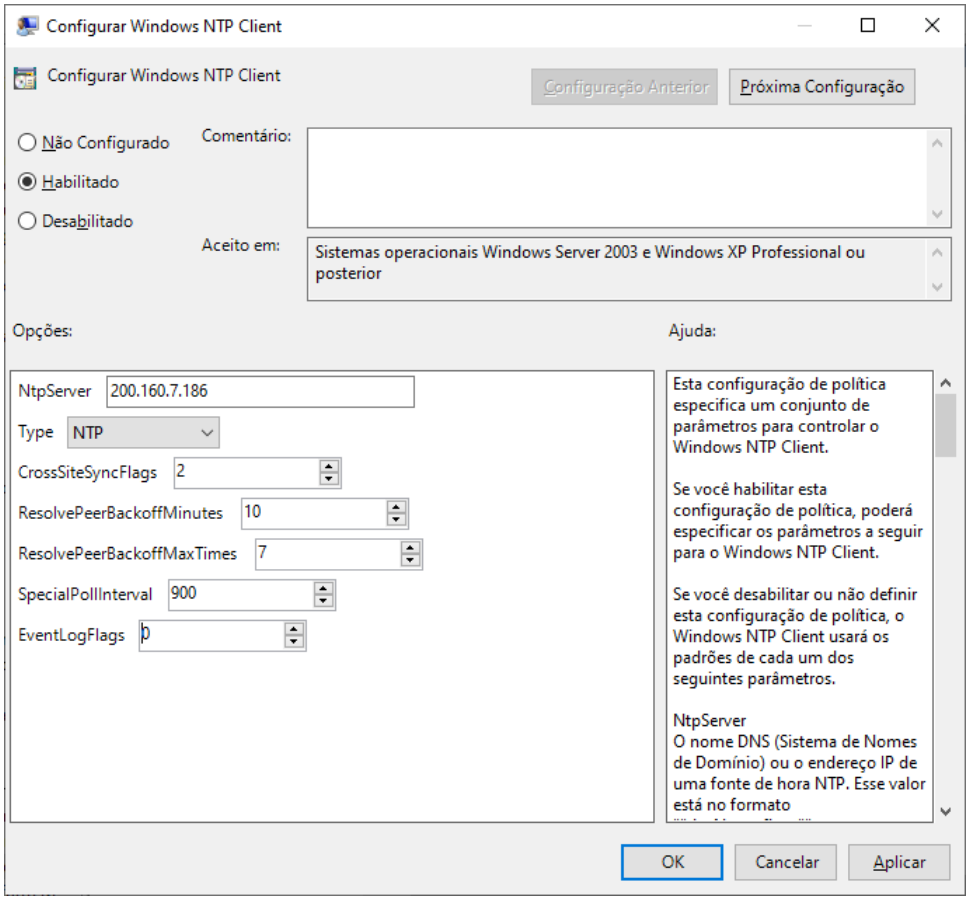
1. Iniciar -> pesquisar "**Gpedit.msc"** -> **Gpedit.msc**
Clicar em **OK.**

2. CONFIGURAÇÃO DO COMPUTADOR -> MODELOS ADMINISTRATIVOS -> SISTEMA -> SERVIÇO DE TEMPO DO WINDOWS -> PROVEDORES DE TEMPO.



3. Modificar os parâmetros de acordo com as figuras a seguir:

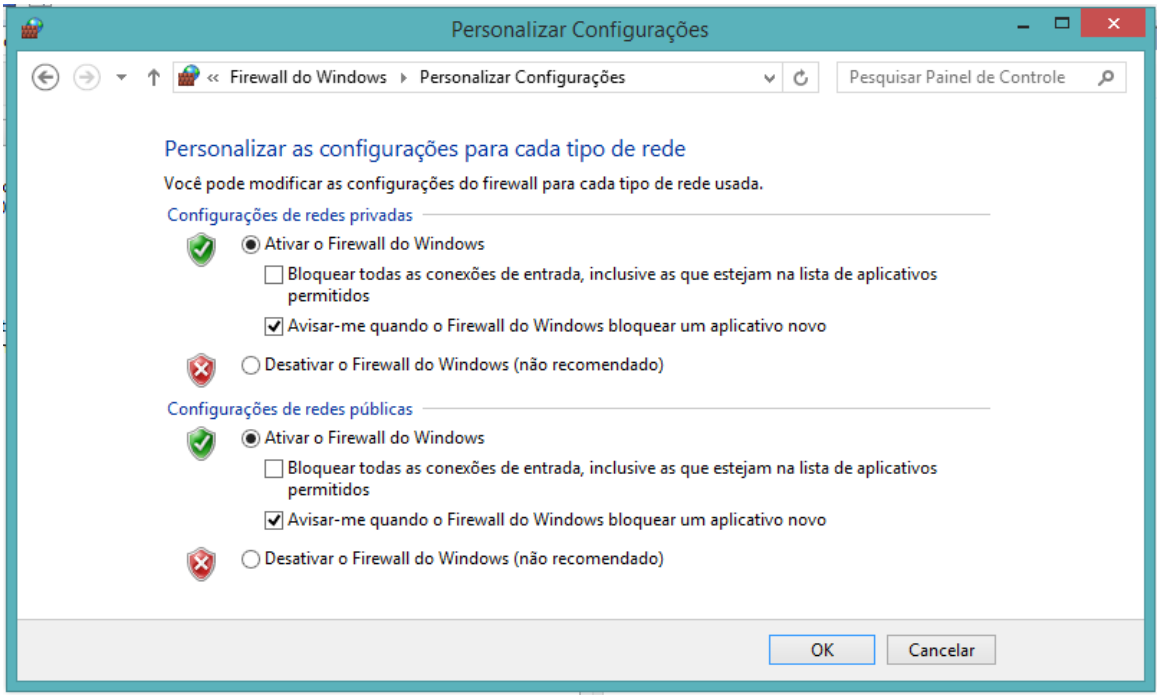




Procedimento 5

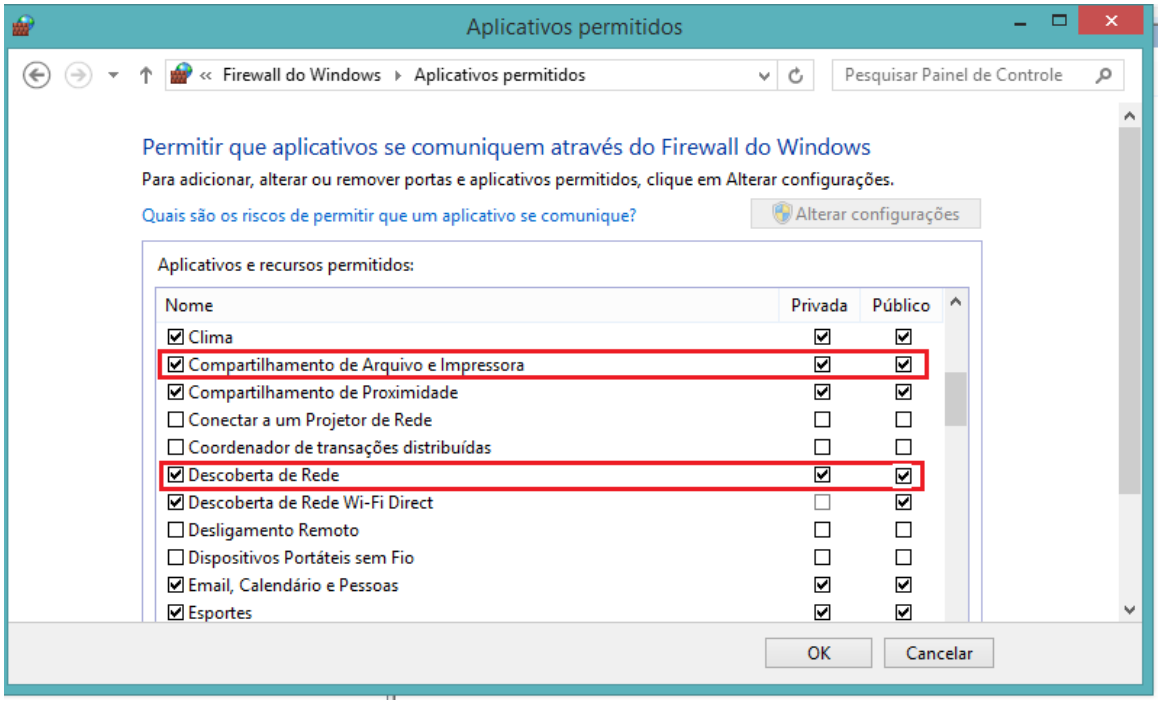
Procedimento para Ativação do Firewall do Windows.

1. Iniciar ->Pesquisar ”Painel de Controle” -> Painel de controle -> Firewall do Windows.
2. Acessar a opção “Ativar ou Desativar Firewall do Windows”
3. Modificar os parâmetros de acordo com a figura a seguir:



4. Clicar em OK.

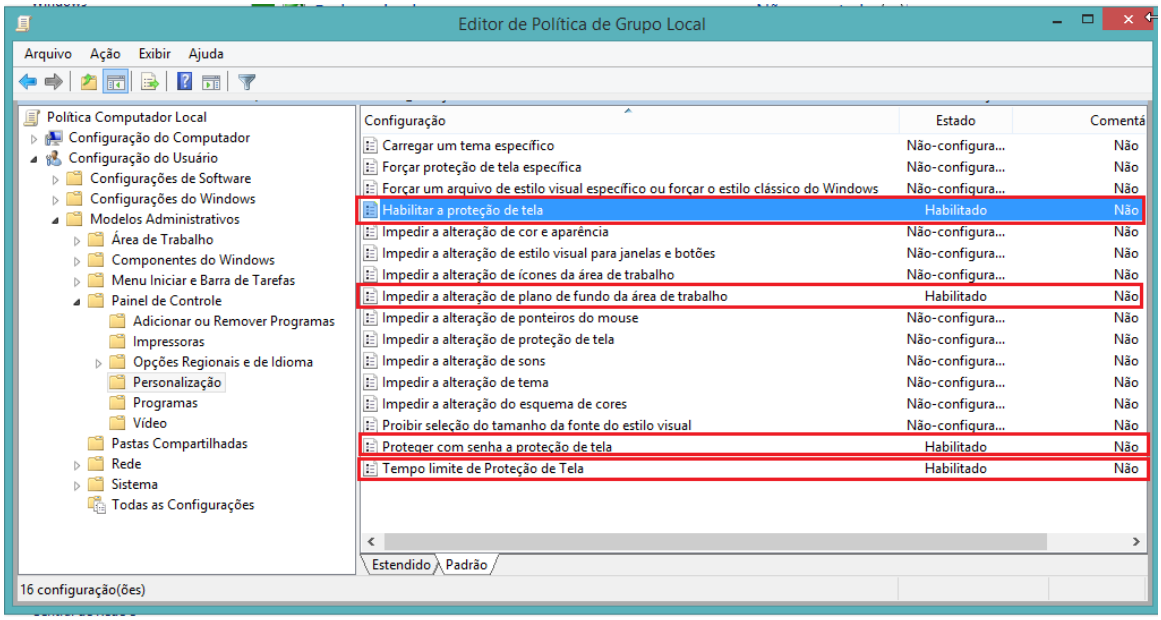
5. Selecionar: Permitir um programa ou recurso pelo firewall do Windows.
Selecione as opções: Descoberta de Rede e Compartilhamento de arquivos e impressoras conforme a imagem abaixo.



Procedimento 6

Procedimento para configuração de proteção de tela na estação da AR.

1. Iniciar -> Pesquisar "**Gpedit.msc"** -> **Gpedit.msc**.
2. Selecione: CONFIGURAÇÃO DO USUÁRIO -> MODELOS ADMINISTRATIVOS -> PAINEL DE CONTROLE -> PERSONALIZAÇÃO.
3. Habilitar as opções: Habilitar a proteção de tela, Impedir a alteração de plano de fundo da área de trabalho, Proteger com senha a proteção de tela e Tempo limite de Proteção de Tela.

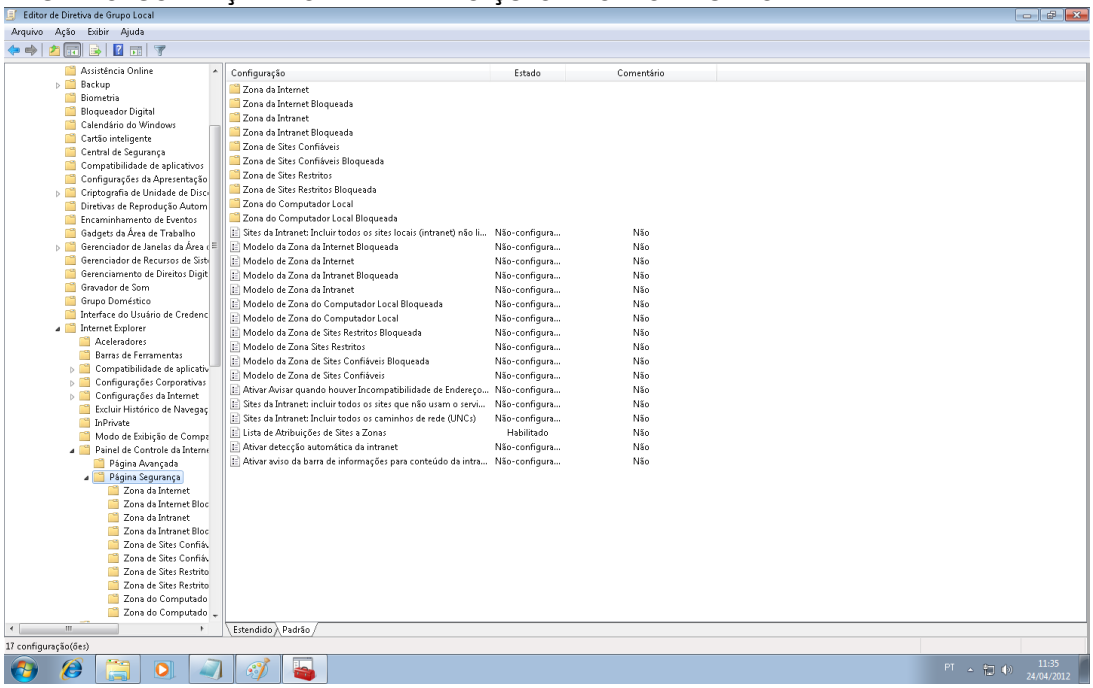


Na opção *Tempo limite de Proteção de Tela* além definir habilitado, defina o tempo com o valor de 120 segundos.

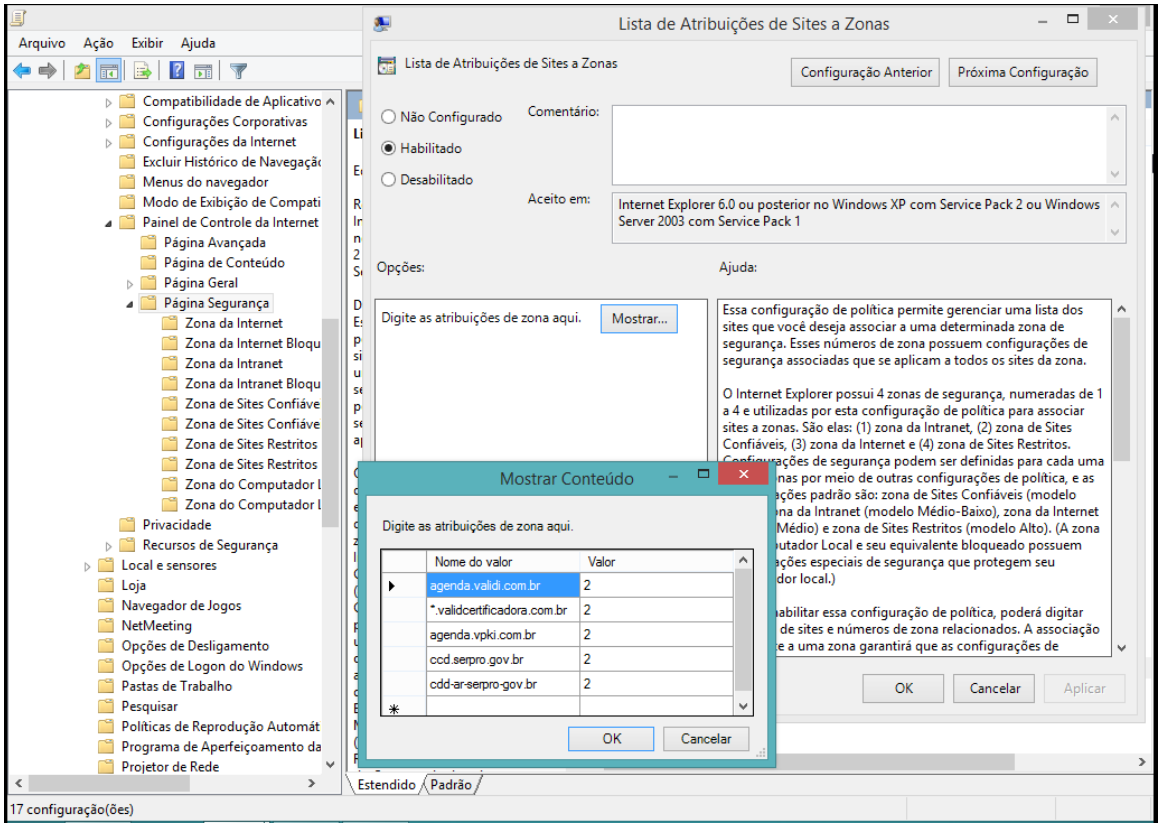
Procedimento 7

Procedimento para configurar listas de sites confiáveis via GPO.

1. Iniciar -> Pesquisar "**Gpedit.msc"** -> **Gpedit.msc**.
2. Selecione: CONFIGURAÇÃO DO COMPUTADOR -> MODELOS ADMINISTRATIVOS -> COMPONENTES DO WINDOWS > INTERNET EXPLORER -> PAINEL DE CONTROLE DA INTERNET -> PÁGINA SEGURANÇA > LISTA DE ATRIBUIÇÕES DE SITES A ZONAS



4. Selecione: LISTA DE ATRIBUIÇÕES DE SITES A ZONAS através de dois cliques sobre a opção.
5. Habilitar: LISTA DE ATRIBUIÇÕES DE SITES A ZONAS.
6. Clique no botão MOSTRAR.
7. Inserir os sites listados como confiáveis,
8. Inserir na coluna nome do valor os seguintes endereços:
    - agenda.validi.com.br
    - *.validcertificadora.com.br
    - agenda.vpki.com.br
    - ccd.serpro.gov.br
    - ccd-ar.serpro.gov.br
    - ccdhom.serpro.gov.br
    - *.conectividade.caixa.gov.br/
    - *.dataprev.gov.br/
    - *.detran.*
    - *.receita.fazenda.gov.br/
    - *.valid.educatec.org/login/index.php
    - *.intranet.valid.com.br
    - *.agenda.vpki.com.br
    - *.ar-icp-brasil.validcertificadora.com.br/
    - *.agenda-icp-brasil.validcertificadora.com.br
    - *.vpki.com.br
9. Inserir o valor 2 no campo VALOR.
10. As modificações devem estar conforme a imagem:

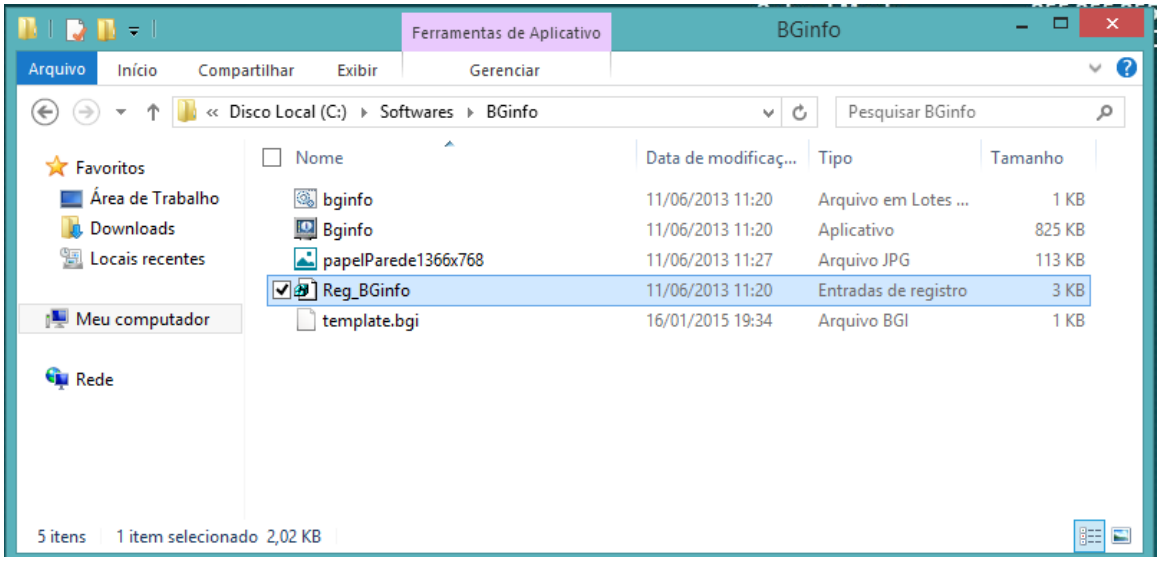


11. Clicar em OK.

Procedimento 8

Procedimento para Papel de parede, instalação BGinfo (sugestão)

1. Acessar o diretório C:\SOFTWARES\BGINFO;
2. Copiar os seguintes arquivos; Bginfo.exe, bginfo.bat e template.bgi;
3. Colar no diretório: C:\Windows\System32\GroupPolicy\Machine\Scripts\Startup;
4. Após realizar a cópia, acessar novamente o diretório C:\SOFTWARES\BGINFO e executar o seguinte arquivo: Reg_Bginfo.reg.
5. As demais configurações de apontamento da imagem são realizadas através do arquivo template.bgi

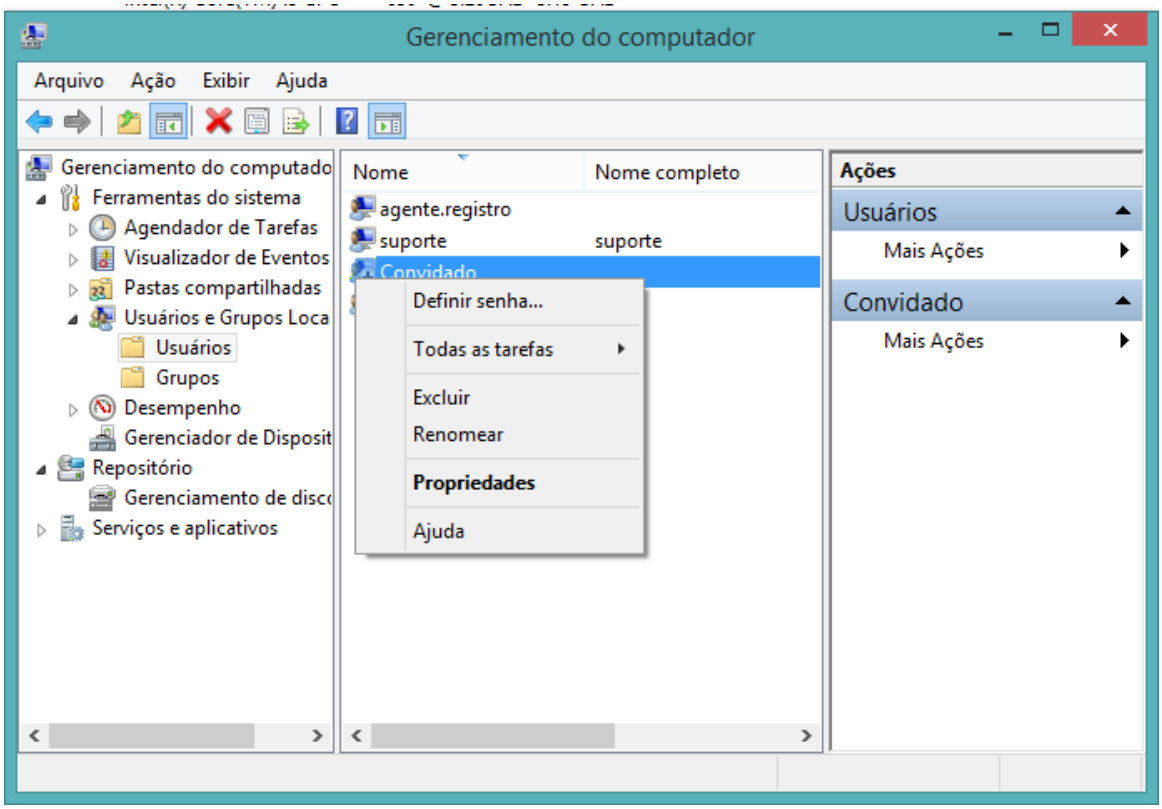


Procedimento 9

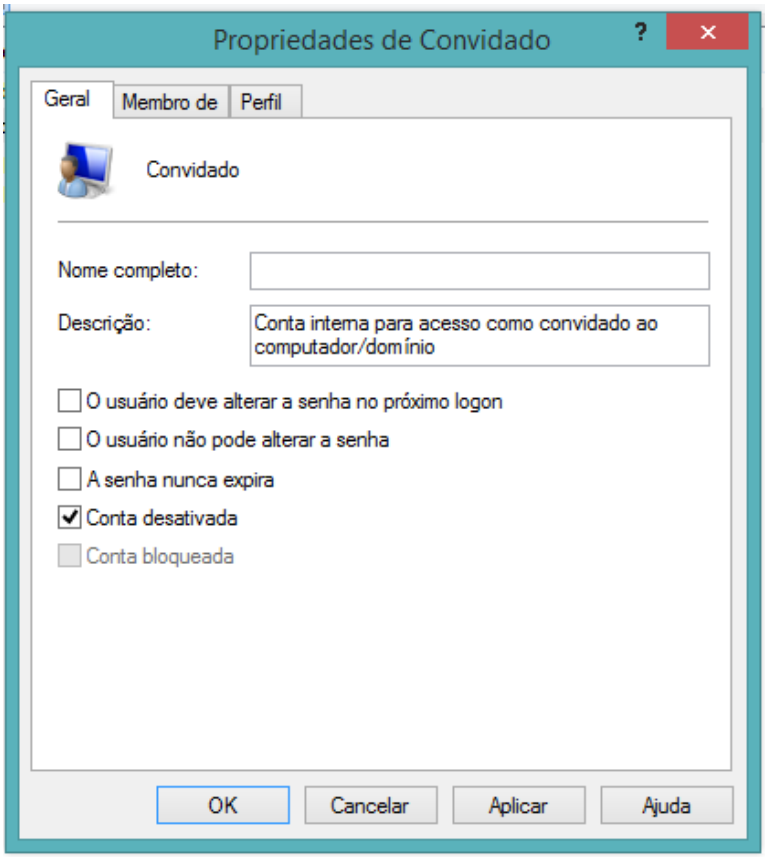
Procedimento para configurar as contas dos usuários.

Apenas contas de administrador e de Agente de Registro devem estar cadastradas e disponíveis, demais contas devem ser excluídas ou desativadas.

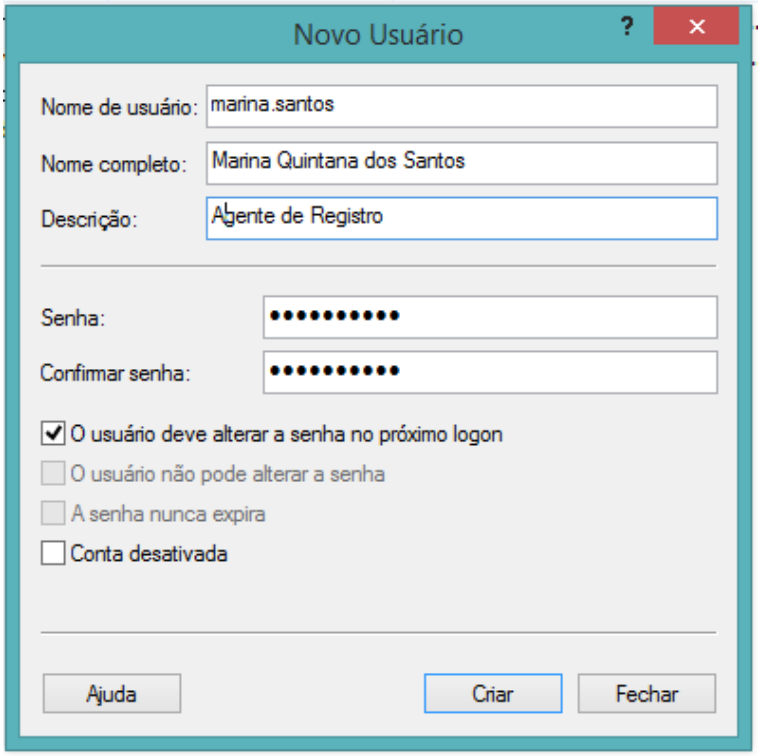
1. Iniciar -> Configurações -> Painel de Controle;
2. Acessar: Sistema e Manutenção;
3. Executar: Ferramentas Administrativas;
4. Executar: Gerenciamento do Computador;
5. Acessar: Usuários e Grupos Locais
6. Acessar: Usuários
7. Desabilitar o usuário “convidado” na estação da AR;
8. Clicar com o botão direito do mouse em “Convidado”;
9. Selecionar: Propriedades



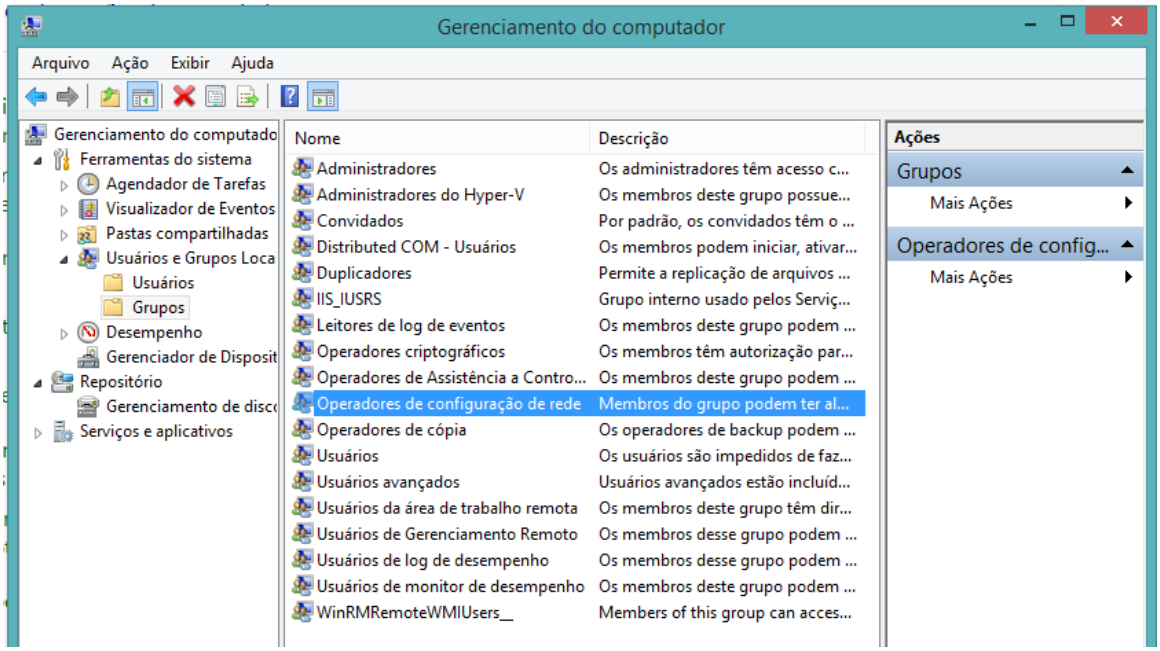
10. Desativar a conta, conforme mostrado na figura a seguir:



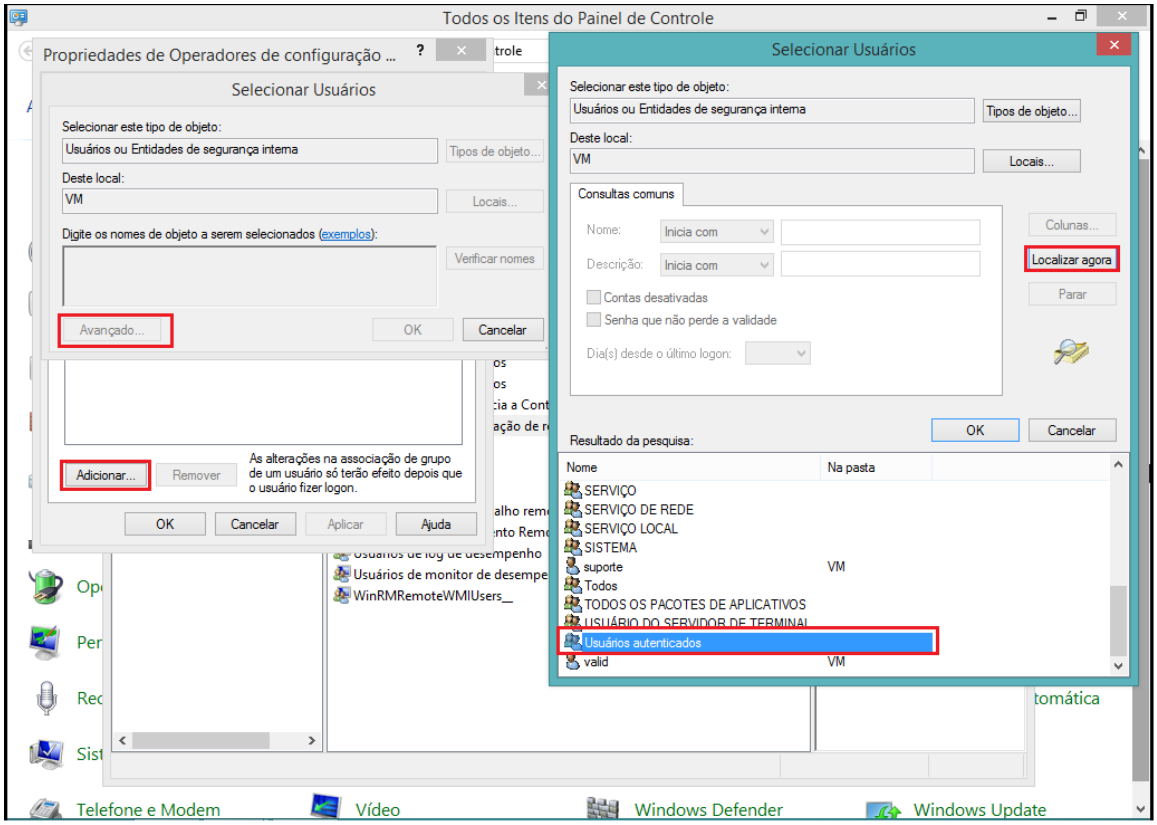
11. Clicar em Ok.
12. **Contas de Agentes de Registro (Usuários Ativos)**
13. Clicar com o botão direito do mouse em cima de Computador, escolher a opção Gerenciar >Usuários e Grupos Locais->Usuários.
14. Clicar com o botão direito do mouse em uma parte limpa, escolher a opção “Novo usuário”;
15. **As contas devem ser configuradas individualmente, cada AGR deve possuir sua conta de usuário nomeada conforme o exemplo nome.ultimosobrenome;**
16. Digitar a senha padrão por exemplo: valid@1234;
17. Selecionar: “Usuário deve alterar senha no próximo logon” para que o Agente de Registro possa alterar a senha no primeiro acesso conforme a imagem abaixo.



18. Adicionar Usuários Autenticados como operadores de configuração de rede.
19. Clicar: Grupos
20. Clicar com botão direito em OPERADORES DE CONFIGURAÇÃO DE REDE.

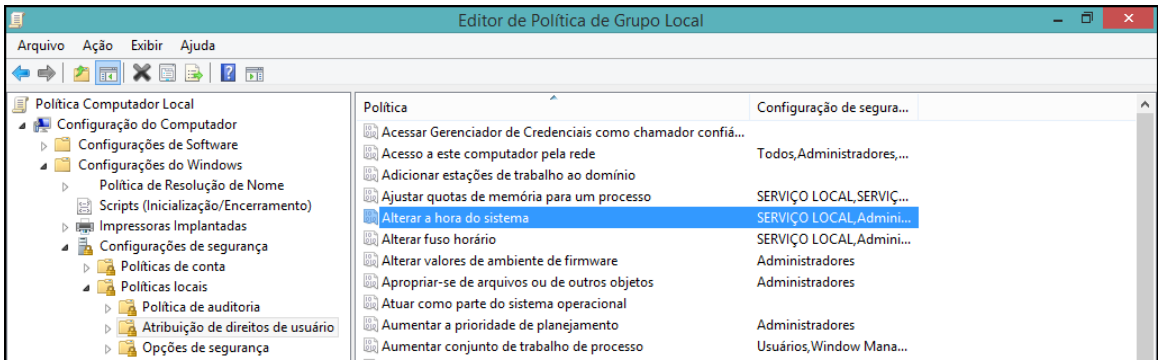


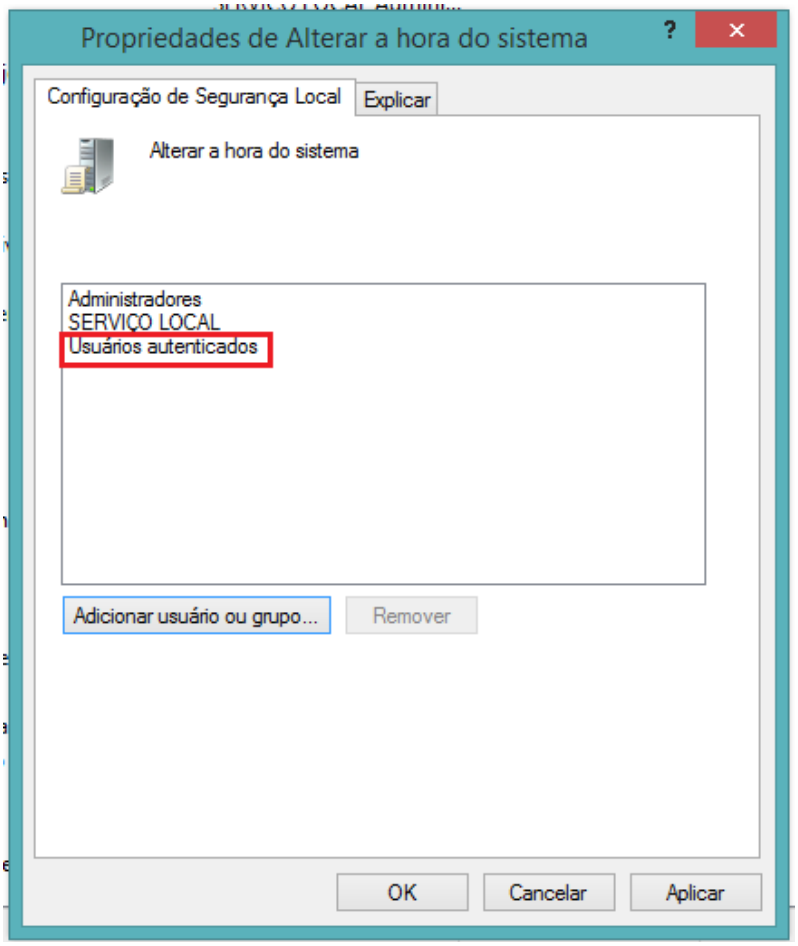
21. Clicar: Adicionar
22. Clicar : Avançado
23. Clicar: Localizar agora
24. Selecionar: Usuários Autenticados
25. Clicar: Ok.



Atribuir diretiva de alterar hora do sistema para USUÁRIOS AUTENTICADOS.

1. Iniciar -> Pesquisar "**Gpedit.msc"** -> **Gpedit.msc**.
2. Configuração do Computador -> Configuração do Windows -> Configurações de Segurança -> Políticas Locais -> Atribuição de Direitos de Usuários
3. Modificar os parâmetros referentes a "Alterar a hora do Sistema", de acordo com as figuras seguintes:

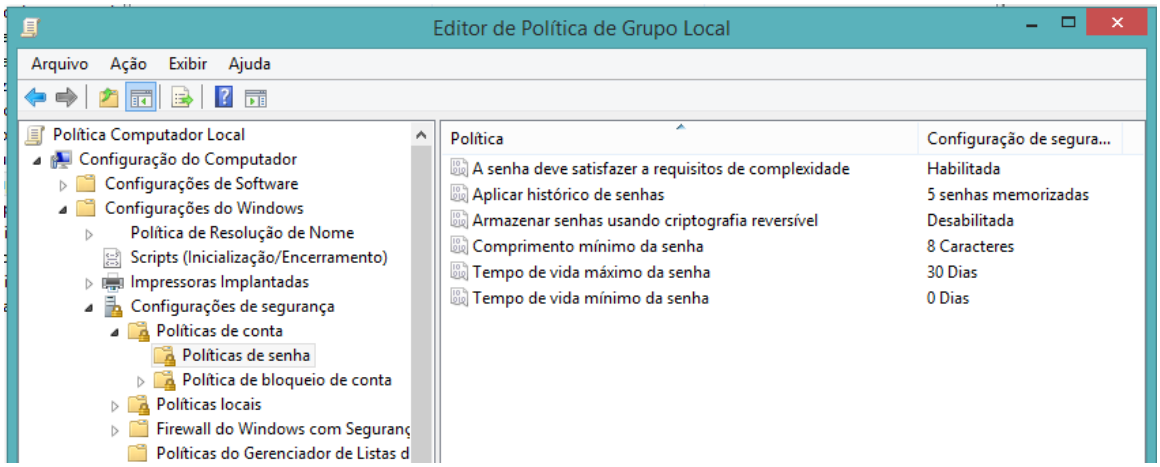




Procedimento 10

Procedimento para configuração de senha forte na estação da AR

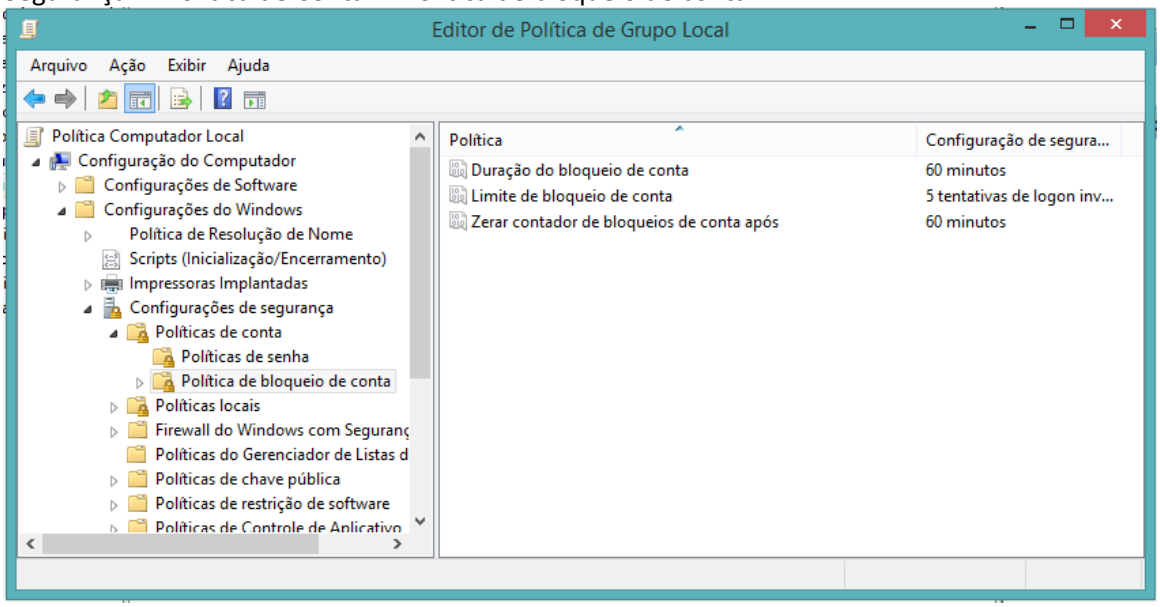
1. Iniciar -> Pesquisar "**Gpedit.msc"** -> **Gpedit.msc**.
2. Configuração do Computador -> Configuração do Windows -> Configurações de Segurança -> Politicas de Conta -> Politicas de Senha
3. Modificar os parâmetros referentes a Diretivas de Senha, de acordo com as figuras seguintes:



Procedimento 11

Procedimento para configuração das diretivas de bloqueio de conta.

1. Iniciar -> Pesquisar "**Gpedit.msc"** -> **Gpedit.msc**.
2. Configuração do Computador -> Configurações do Windows -> Configurações de Segurança -> Política de Conta -> Política de bloqueio de conta.



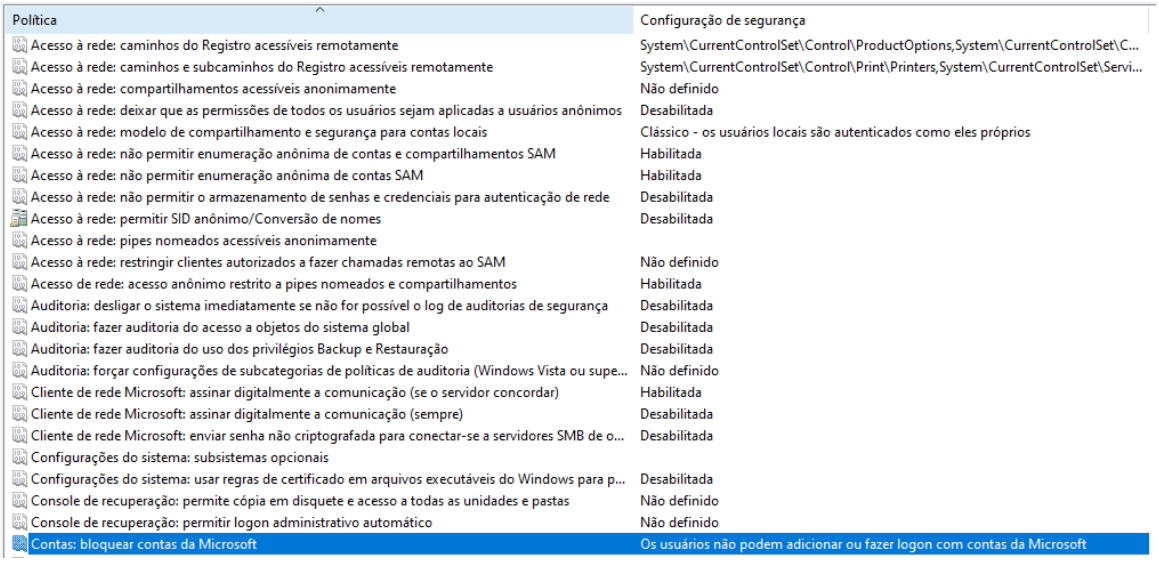
Procedimento 12

Bloqueio de aplicativo Loja e logon com contas Microsoft – Windows 8.1 e 10.

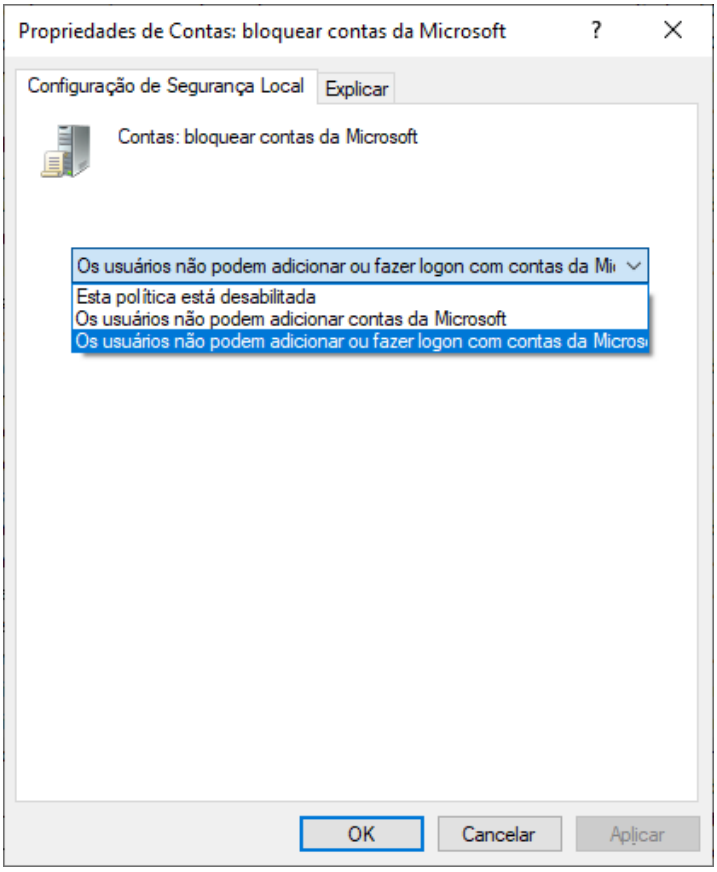
Bloqueio de Logon com conta Microsoft

1. Iniciar -> Pesquisar "**Gpedit.msc"** -> **Gpedit.msc**.

2. CONFIGURAÇÃO DO COMPUTADOR -> CONFIGURAÇÃO DO WINDOWS -> CONFIGURAÇÕES DE SEGURANÇA -> POLÍTICAS LOCAIS -> OPÇÕES DE SEGURANÇA.

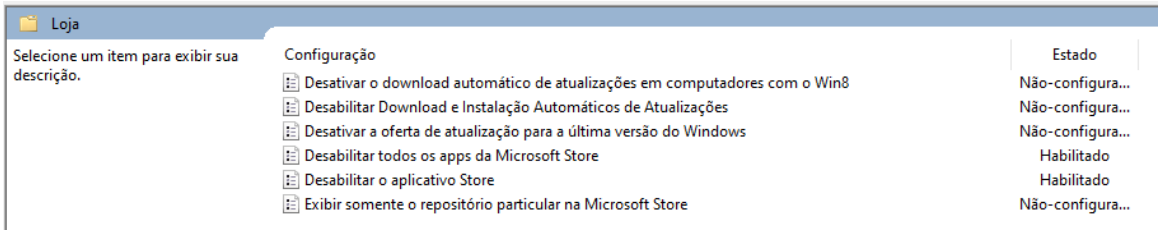


3. Modificar o parâmetro referente a Contas: bloquear contas Microsoft, de acordo com a figura seguinte:

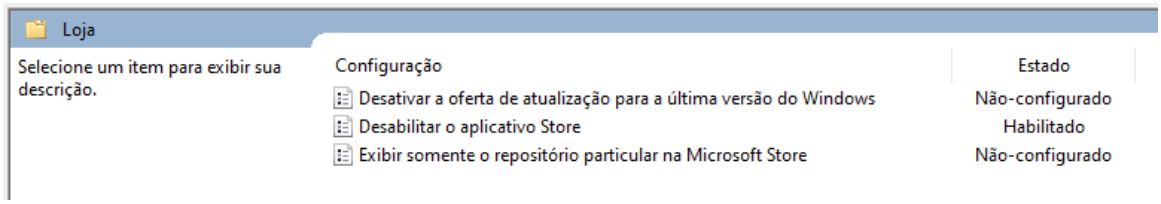


Bloqueio da Loja do Windows 10

1. Iniciar -> Pesquisar "**Gpedit.msc"** -> **Gpedit.msc**.
2. Selecione: CONFIGURAÇÃO DO COMPUTADOR -> MODELOS ADMINISTRATIVOS -> COMPONENTES DO WINDOWS -> LOJA:
3. Configurar conforme imagem abaixo as políticas: **Desabilitar todos os apps da Microsoft Store** e **Desabilitar o aplicativo Store.**

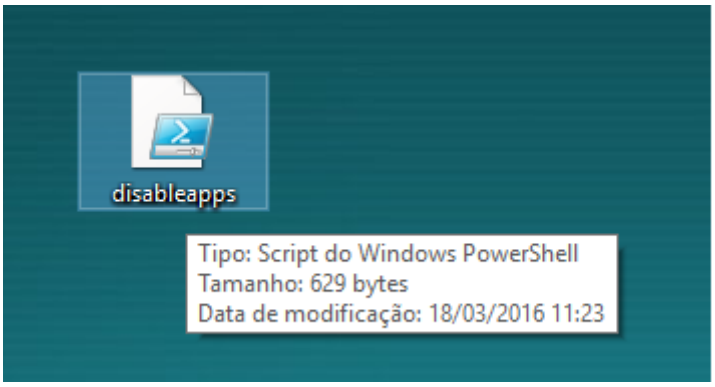


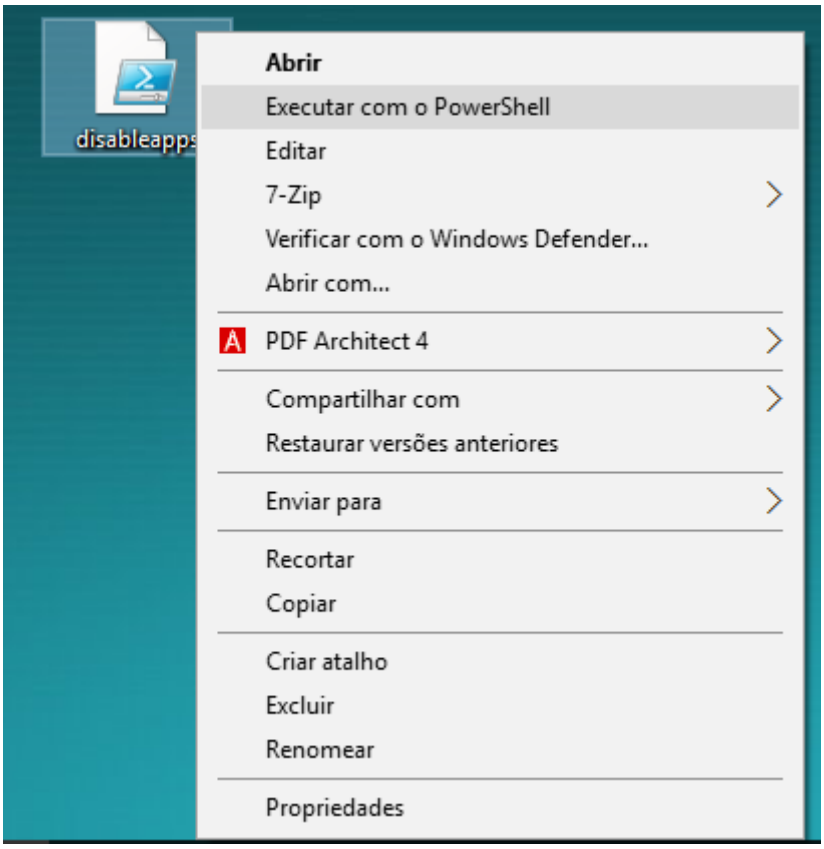
4. Selecione: CONFIGURAÇÃO DO USUARIO -> MODELOS ADMINISTRATIVOS -> COMPONENTES DO WINDOWS -> LOJA:
5. Configurar conforme imagem abaixo a política: ***Desabilitar o aplicativo Store***:



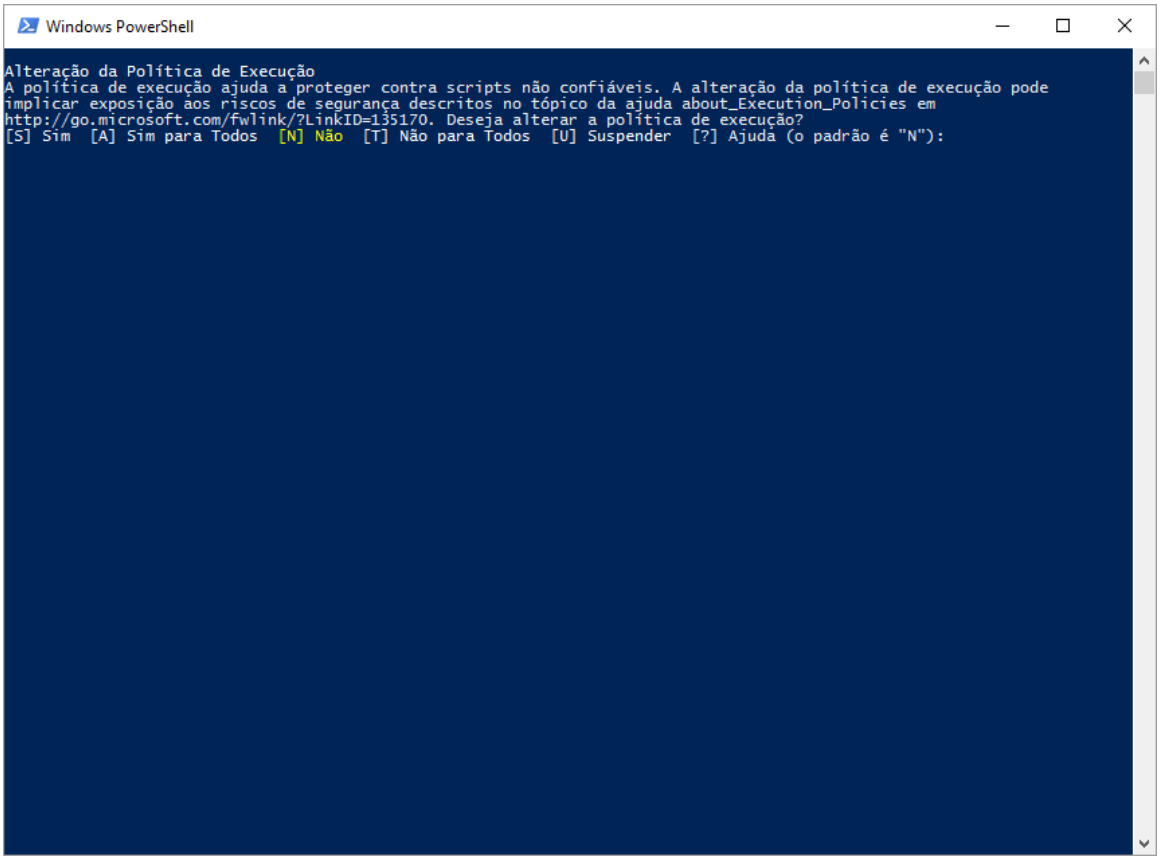
Procedimento para remoção de aplicações pré-instaladas do Windows 10.

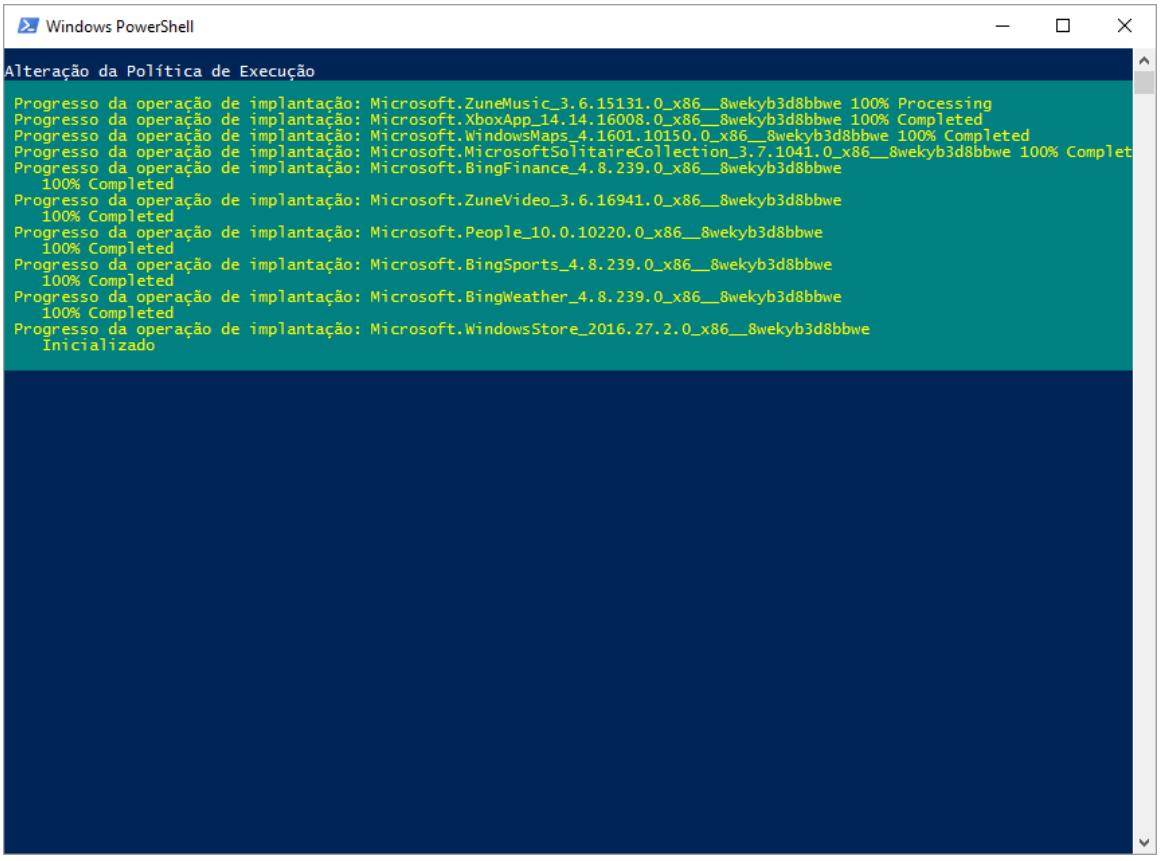
1. Abra a pasta de Softwares.
2. Clique com o botão direito do mouse em: “Disableapps.ps1”





3. Aceitar a alteração via PowerShell, vide imagem abaixo.





Aguardar o término da atividade.

No fim as aplicações pré-instaladas de fábrica pela Microsoft serão desinstaladas.

Note que nem todas são desinstaladas, são desinstaladas apenas as aplicações que não competem em um ambiente de Autoridade de Registro.

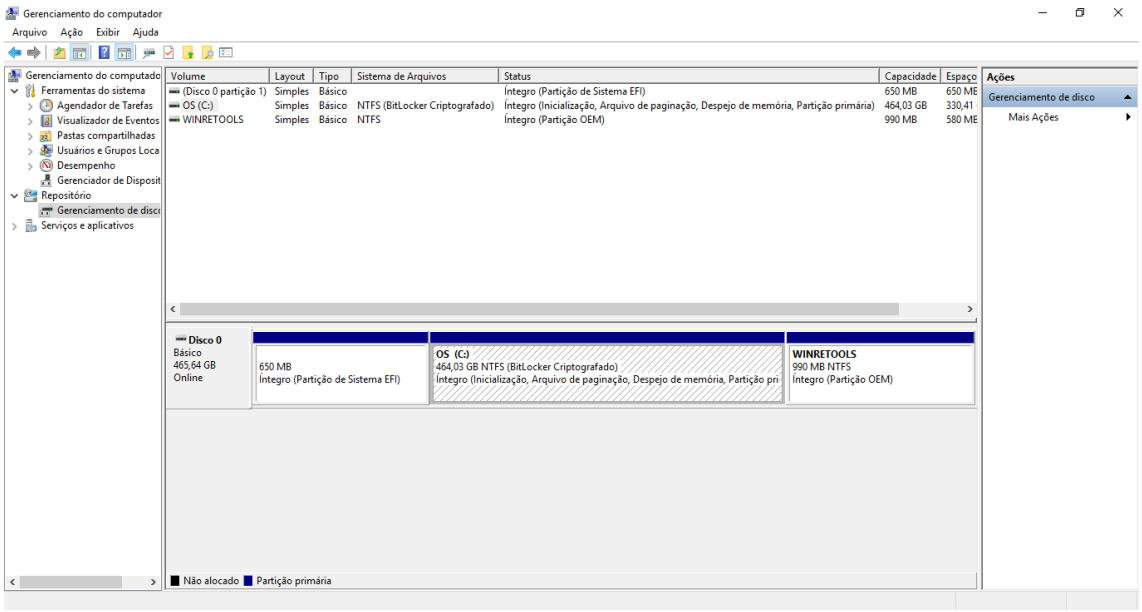
Os Aplicativos removidos são:

Aplicativo Xbox.
Aplicativo Groove de música.
Aplicativo Mapas.
Aplicativo de Jogo Paciência.
Aplicativo Dinheiro.
Aplicativo Filmes e TV.
Aplicativo Notícias.
Aplicativo Pessoas.
Aplicativo Esportes.
Aplicativo Clima.
Aplicativo Loja.
Aplicativo Twitter.
Aplicativo Candy Crush.
Aplicativo Store (Loja).

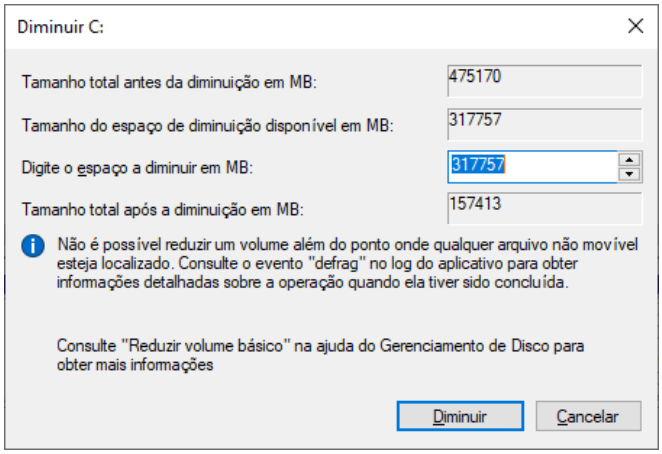
Procedimento 13

Procedimento para ativação da ferramenta de criptografia VeraCrypt.

O primeiro passo é criar uma partição no disco rígido, esta partição é onde ficará os documentos relacionados a emissão do certificado.
Vá para o menu iniciar, digite "Meu Computador", clique com o botão direito na opção e clique em "Gerenciar", a seguinte tela precisa estar aberta.

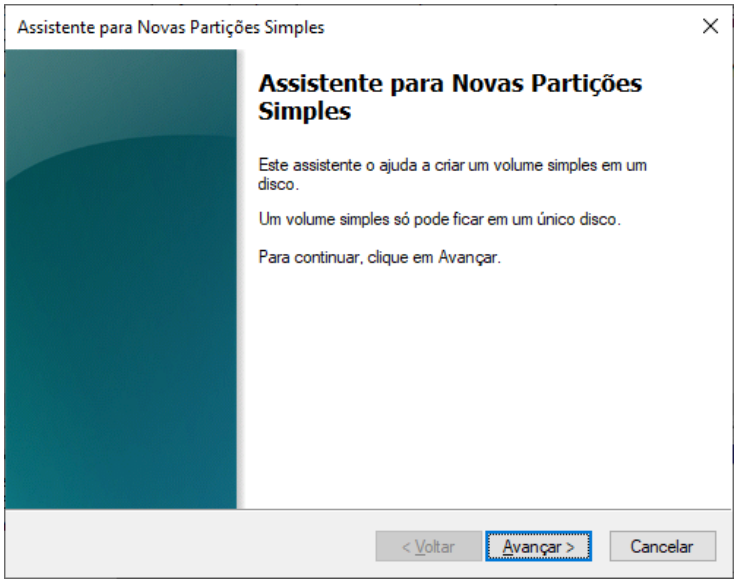


Após isso, clique com o botão direito na partição onde quer criar e clique em "Diminuir Volume". Após isso, é necessário definir o tamanho da partição. Este tamanho precisa ser definido pelo gestor técnico, de acordo com o tamanho do disco.

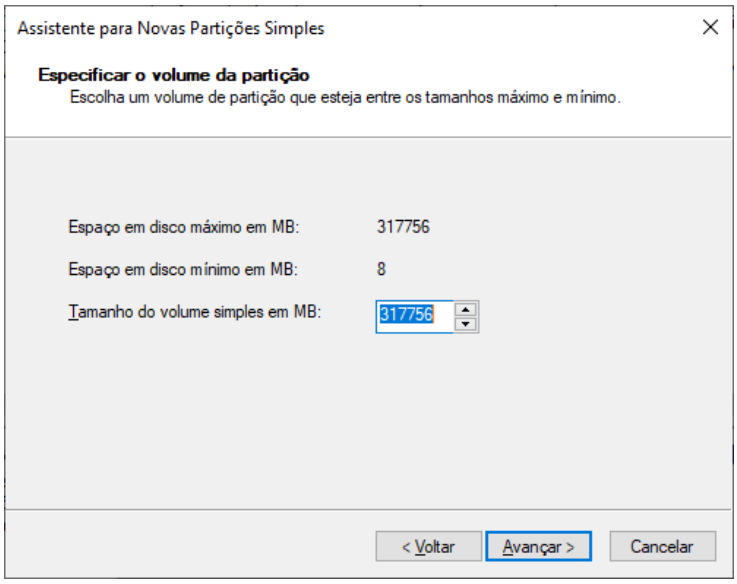


Após isto, clique com o botão direto na partição criada e depois clique em "Novo volume simples".

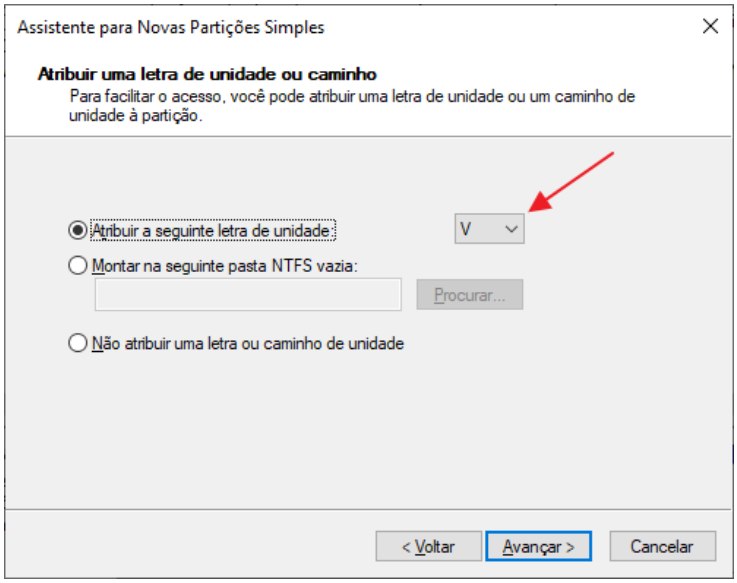
Após isto, clique em "Avançar".



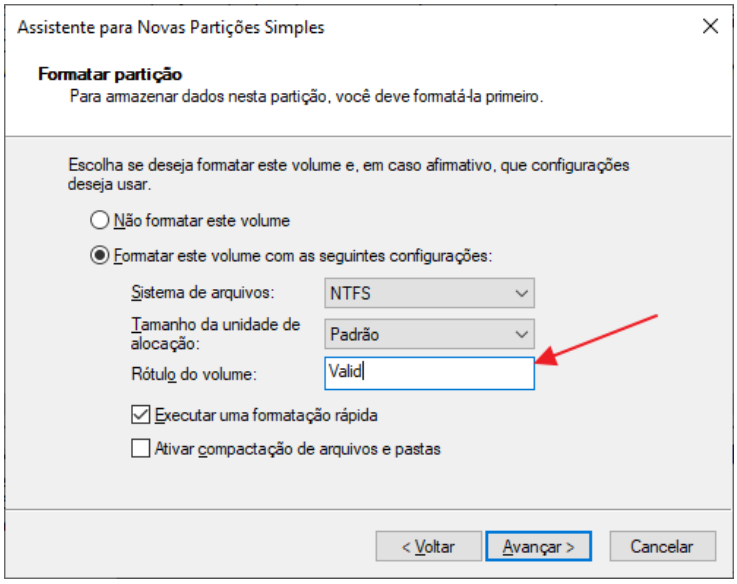
Clique em avançar para definir o tamanho da partição.



Nesta etapa, selecione a opção "Atribuir a seguinte letra de unidade" e selecione a letra "V".



Na opção a seguir, selecione a opção "Formatar este volume com as seguintes configurações", "Sistema de arquivos: NTFS", "Tamanho da unidade de alocação: Padrão" e "Rótulo do volume: VALID" (LETRA MAIÚSCULA).



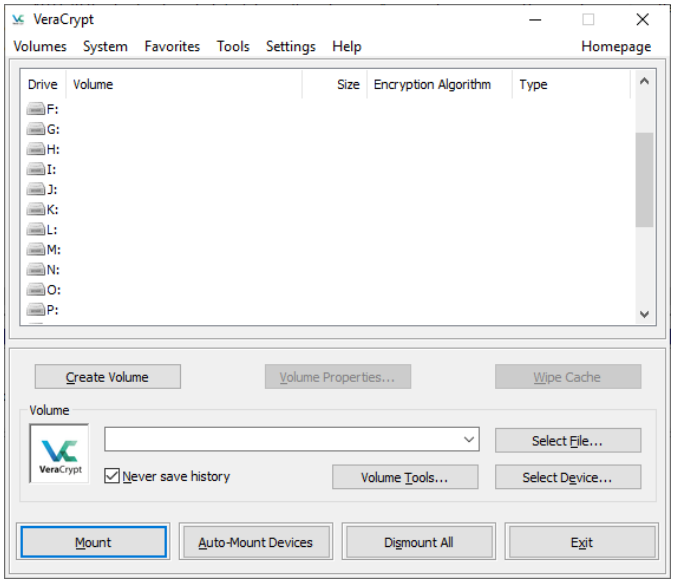
Clique em "Concluir" para terminar esta etapa.

Acesse o seguinte site para fazer o download do Veracrypt, realize a instalação conforme informado no site. https://www.veracrypt.fr/en/Downloads.html

Após instalar o programa, deve-se criar um volume, selecionar seu local de destino, o tipo de algoritmo criptográfico que será utilizado e seu tamanho. Após isso, o usuário deve escolher uma senha e criar uma cópia para segurança.

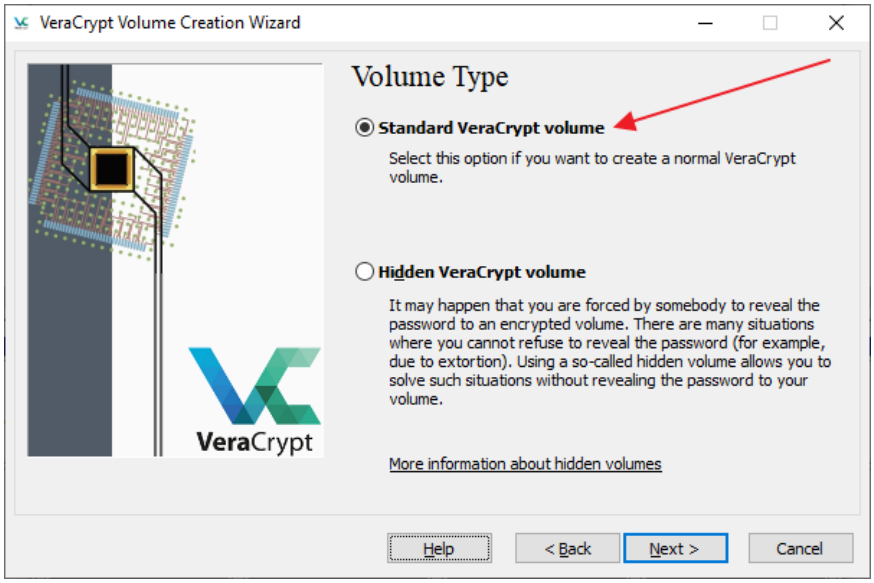
Este procedimento fará a encriptação completa do disco rígido. Importante além do agente de registro ter a senha, o gestor técnico ter o controle de todas as senhas das máquinas.

Abra o aplicativo e clique em "Create Volume".

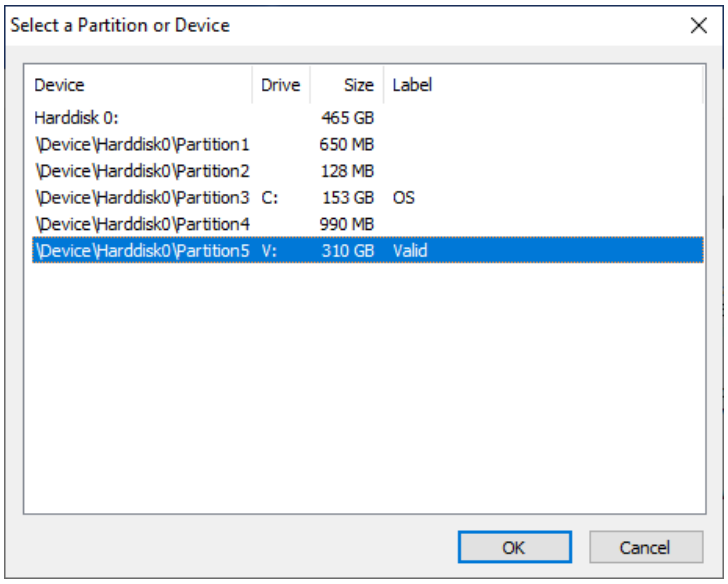


Selecione a opção "Encrypt a non-system partition/drive".

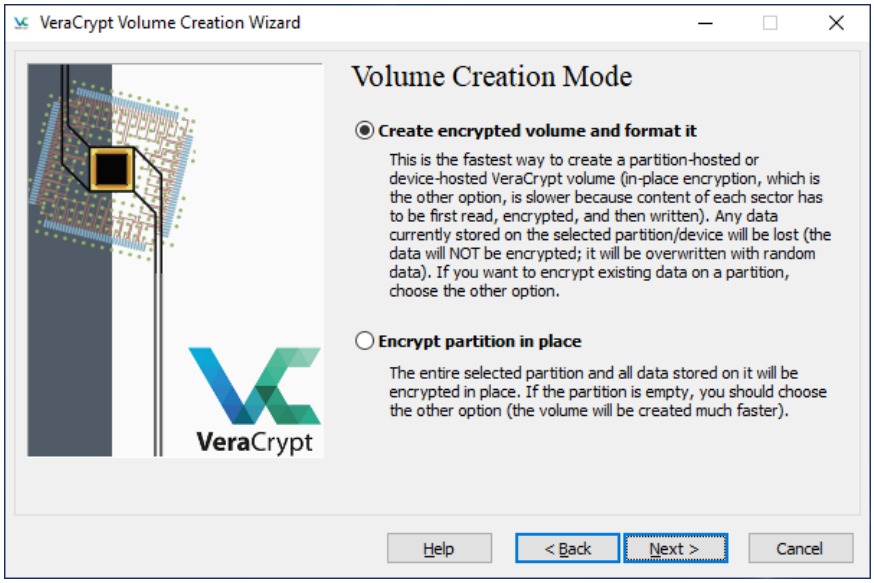
Clique em "Standard Veracrypt Volume".



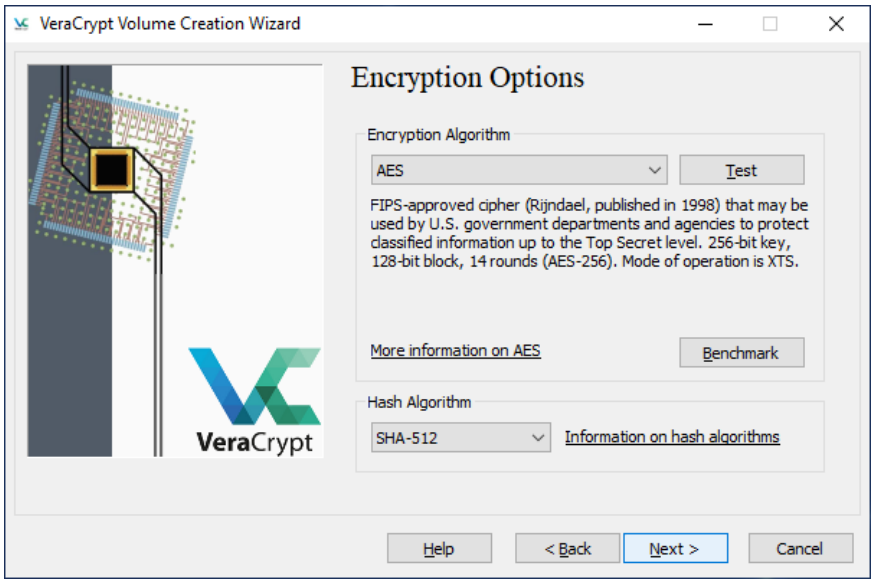
Clique em "Select Device" e seleciona a partição criada para os dados.



Selecione a opção "Create encrypt volumr and format it".



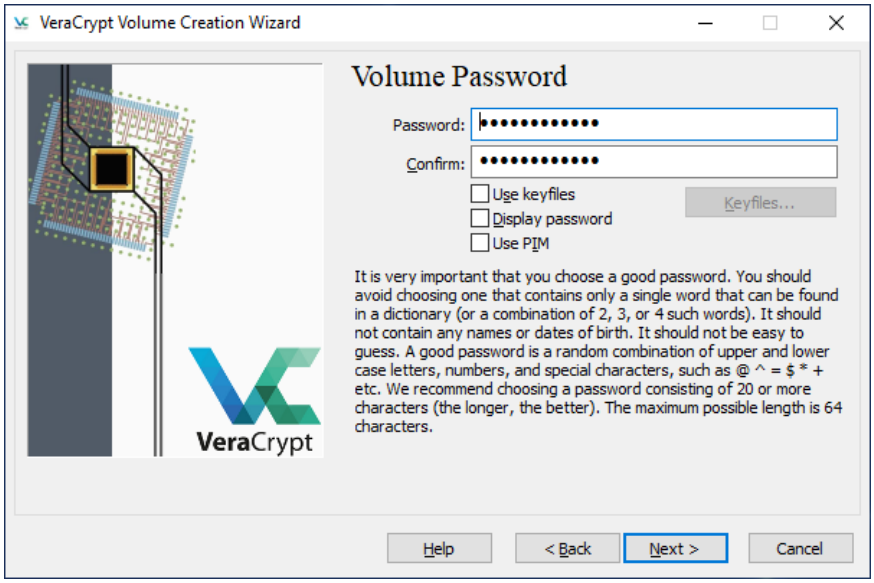
Clique em "Next" para utilizar as definições padrão.



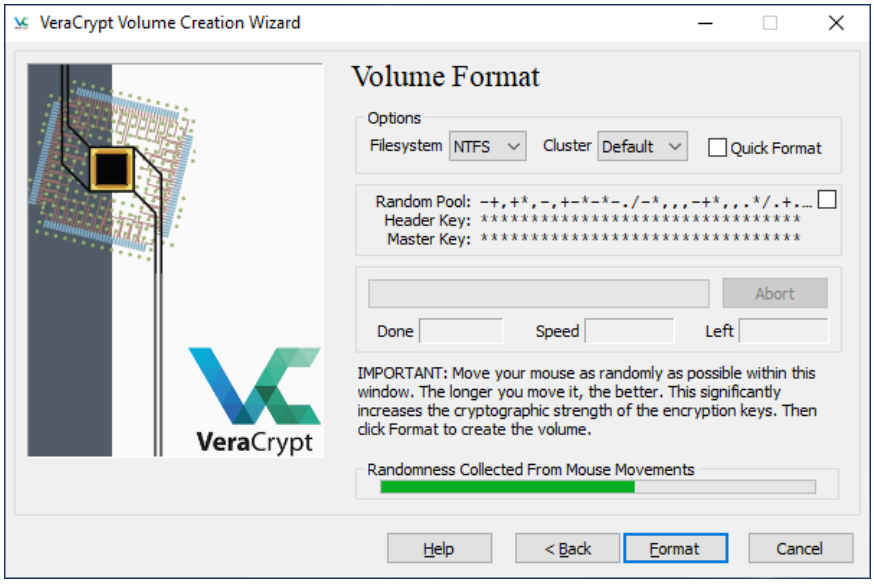
Clique em "Next" novamente para continuar com a encriptação.

A etapa a seguir, é a criação de senha para a utilização da partição.

É de extrema importância a senha ser complexa e única. Apenas o agente de registro e o gestor técnico precisa ter acesso a senha. Caso a AR perca a senha, é necessário formatar a partição e fazer todo o procedimento de novo.

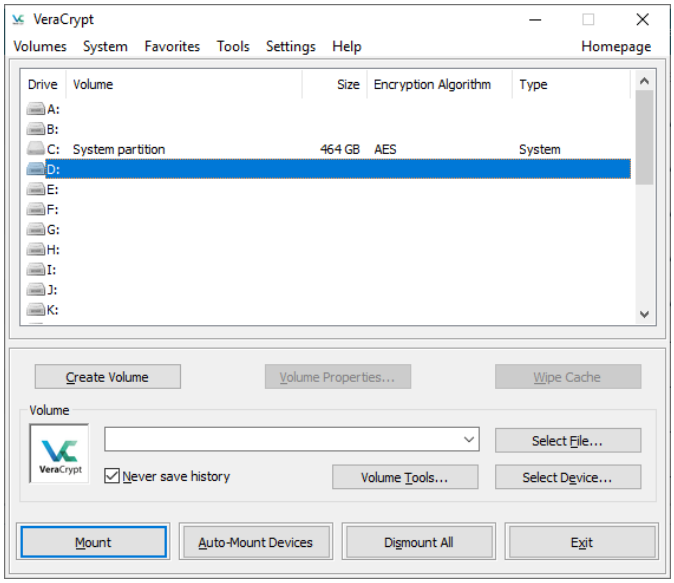


Selecione a opção "NO", para não permitir arquivos maiores que 4GB. A etapa a seguir é a criação da chave, necessário fazer movimentos aleatórios com o mouse para coletar informações para a criptografia, faça movimentos até a barra ficar na cor verde, clique em "Format" para concluir.

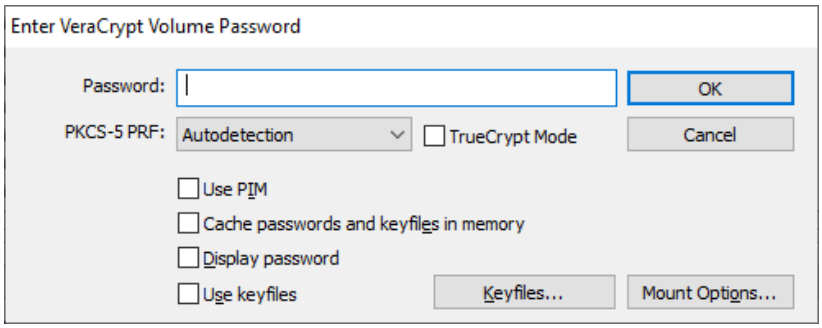


Esta etapa é para concluir o acesso da criptografia. É importante fazer este procedimento todas as vezes para acessar a partição.

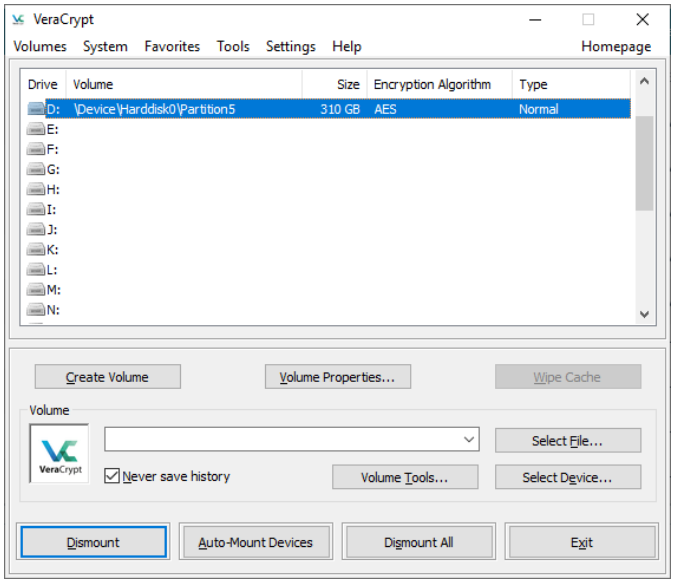
Após concluir, clique em "Next" e feche a janela. Com o programa inicial selecione uma letra e clique em "Auto-Mount-Devices".



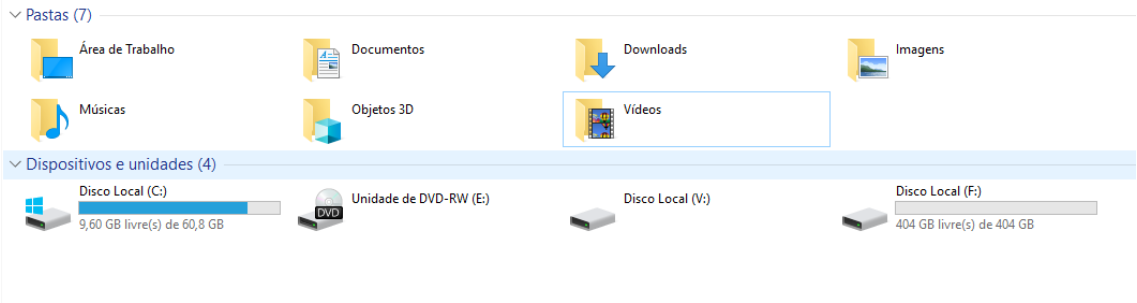
Digite a senha cadastrada e clique em "OK".



Pronto, a partição está pronta para uso.



Para verificar se a partição foi montada, acesse o "Meu computador" e verifique se possui uma partição a mais. Conforme a imagem abaixo.

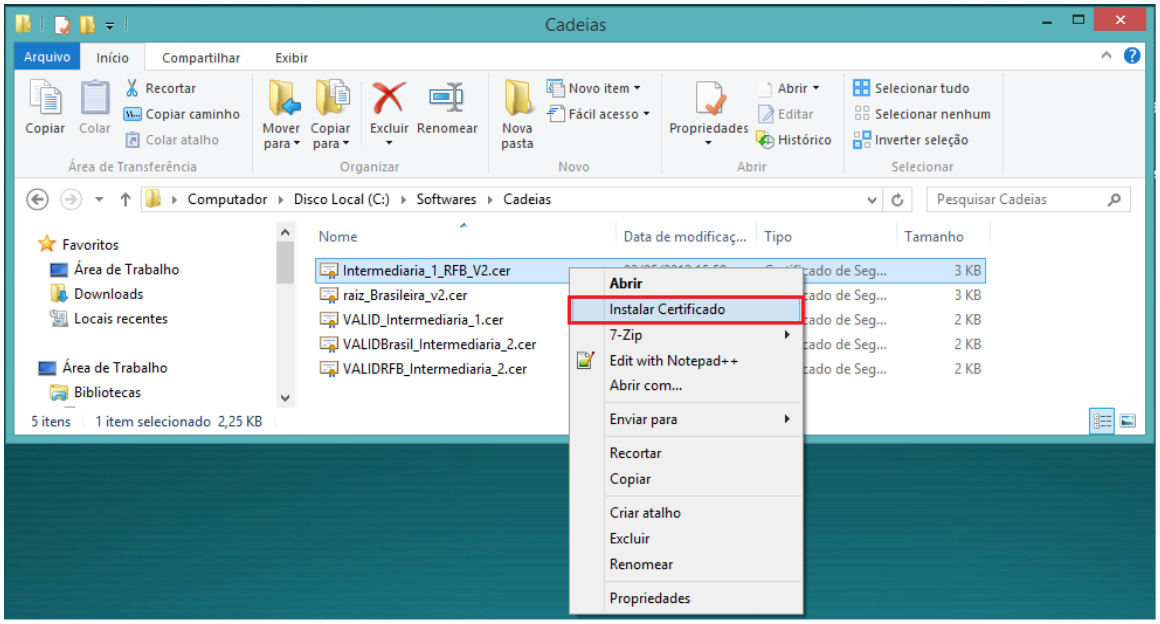


Procedimento 14

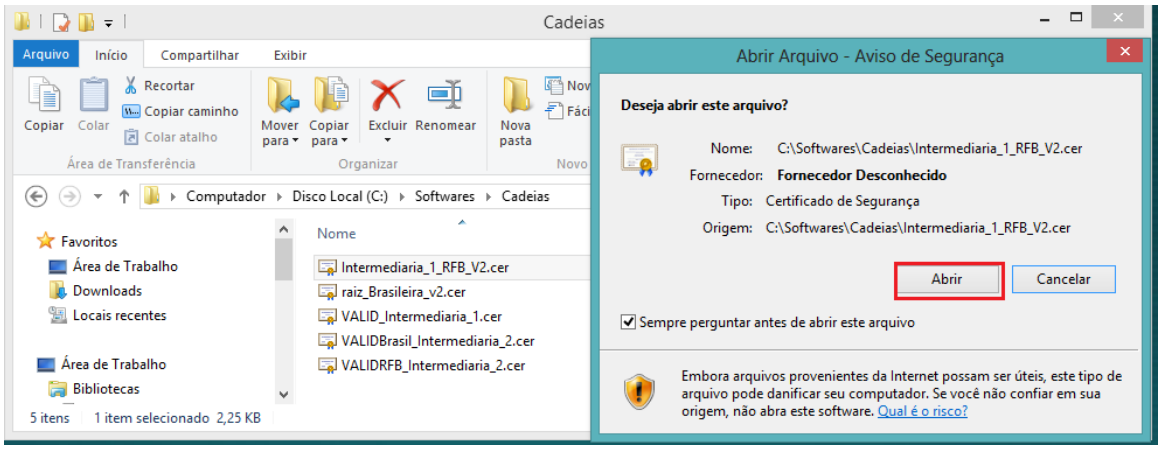
Procedimento para instalação das cadeias.

1. Acessar o diretório: C:\Softwares\Cadeias
2. Clicar com o botão direito do mouse sobre o arquivo e seguir as seguintes:

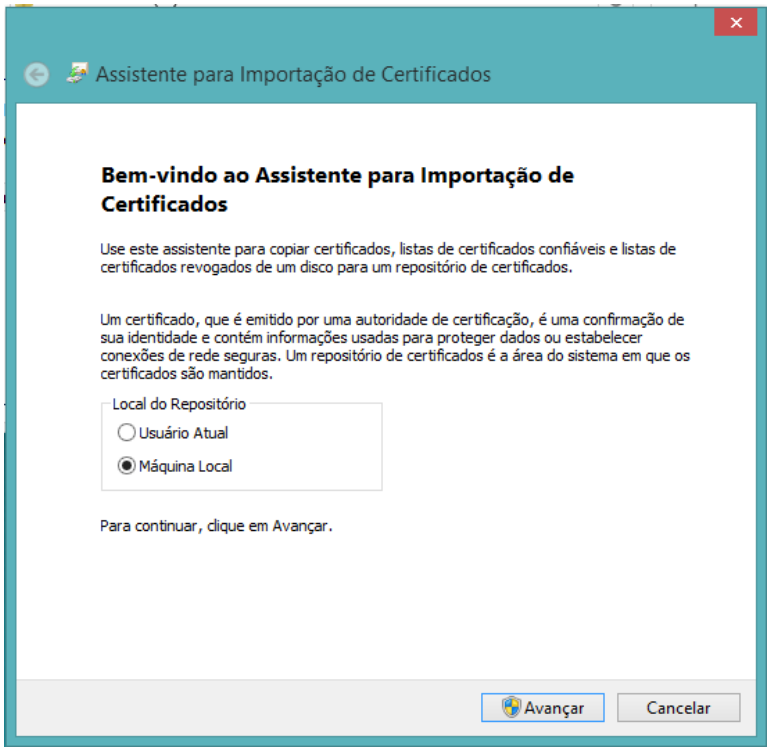
Instalar Certificado:



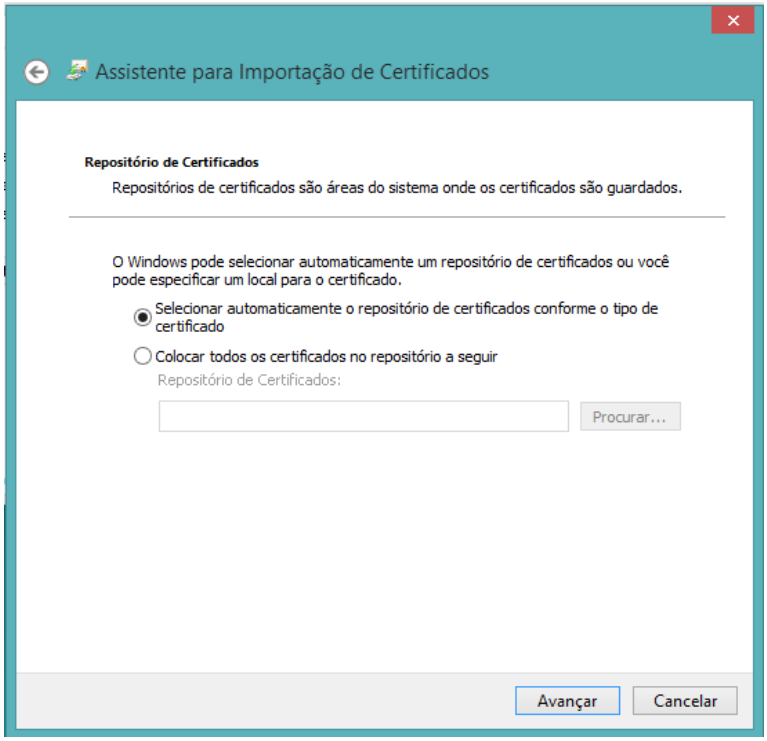
3. Clicar em Abrir:



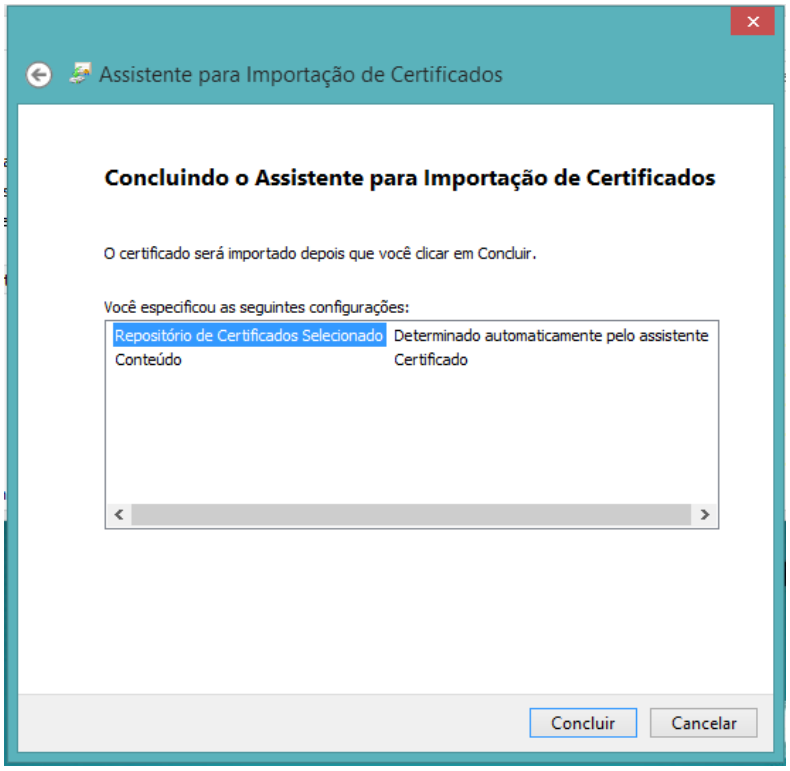
4. Clicar em Avançar:



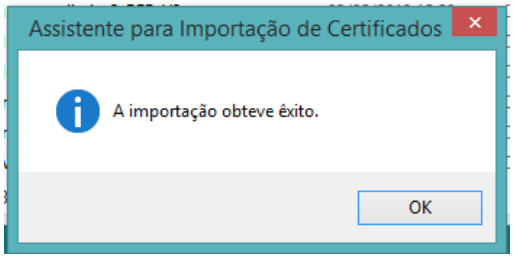
5. Clicar em Avançar novamente:



6. Clicar em Concluir:



7. Clicar em OK.



8. Este procedimento deverá ser executado para todos os arquivos existentes no diretório.

Procedimento 15

Procedimento para instalação do sistema de biometria Valid.

Para coleta biométrica do cliente e validação biométrica do Agente de Registro é necessário a instalação de dois módulos, necessário executar o download dos dois arquivos abaixo:

1. 1ª Instalação: https://s3-sa-east-1.amazonaws.com/share-validcertificadora/vc-ivs-bio-1.0.1.1-jar-with-dependencies.jar

2. 2ª Instalação: https://s3-sa-east-1.amazonaws.com/share-validcertificadora/vc-ivs-bio-1.0.1.1.exe

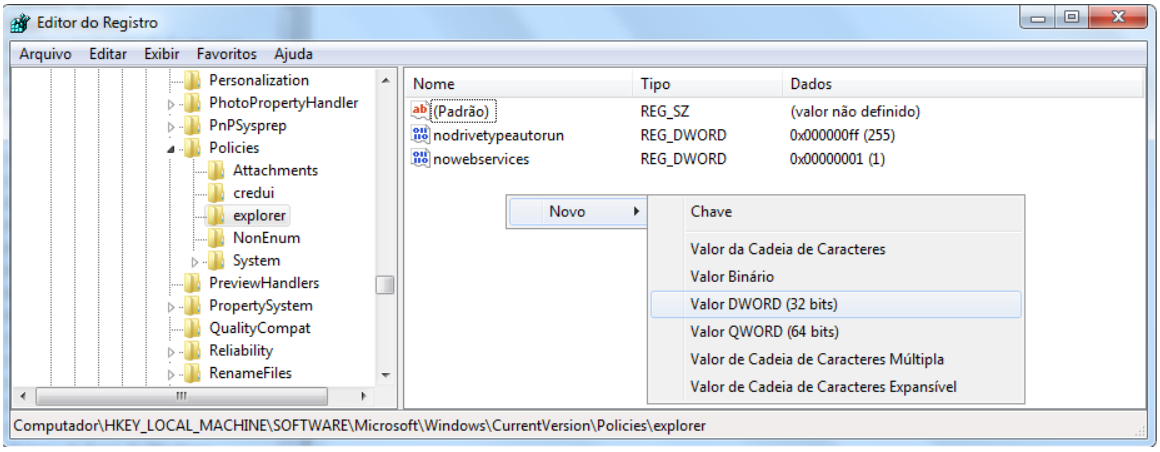
Importante: Após a instalação é criado uma pasta do vc-ivs-bio dentro do perfil do usuário logado (%userprofile%\AppData\Local\vc-ivs-bio\).

Caso o equipamento seja utilizado por mais de um agente, será necessário executar os dois arquivos em cada usuário.

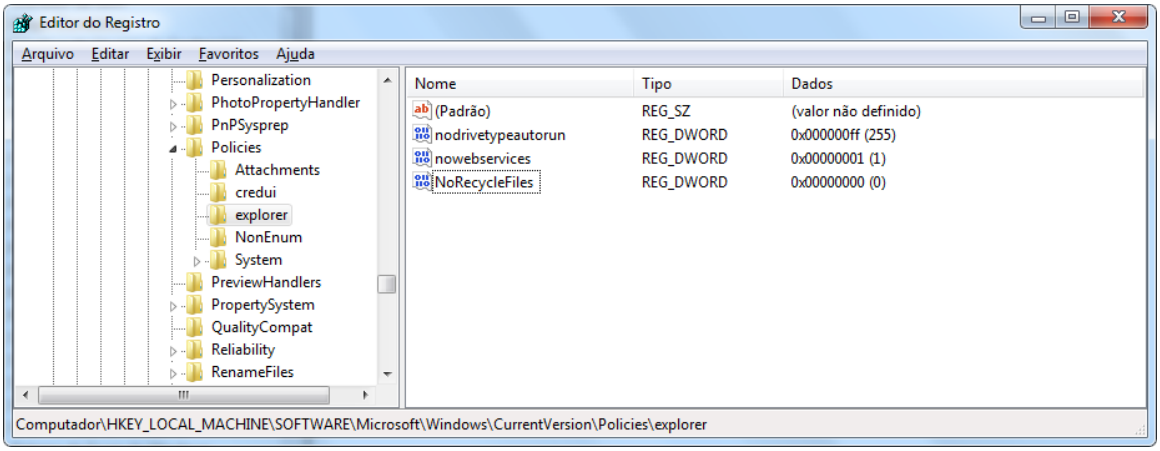
Procedimento 16 – Windows 7

Não mover arquivos excluídos para lixeira.

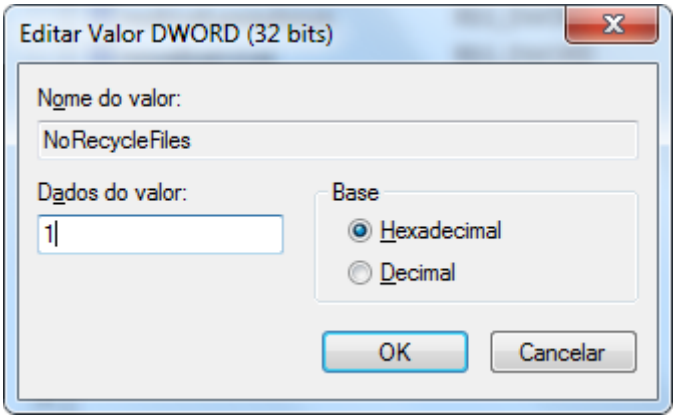
1. Iniciar -> Pesquisar "**regedit".**
2. Selecione: HKEY_LOCAL_MACHINE -> SOFTWARES -> Microsoft -> CurrentVersion -> Policies -> Explorer.
3. Novo -> Valor DWORD (32 bits).



4. Preencher com o nome: NoRecycleFiles.



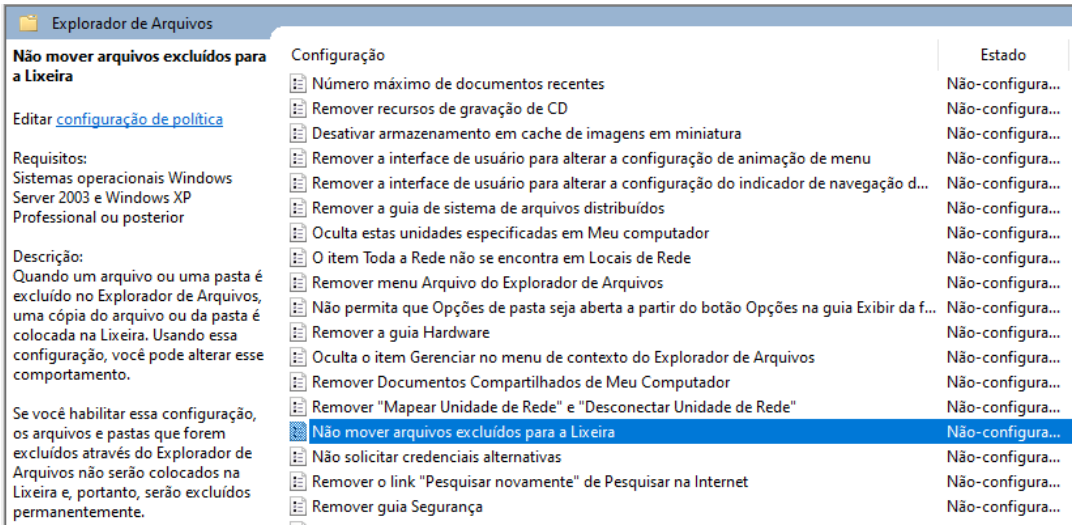
5. Selecione: NoRecycleFiles e altere o valor de **0** para **1**, clique em OK.

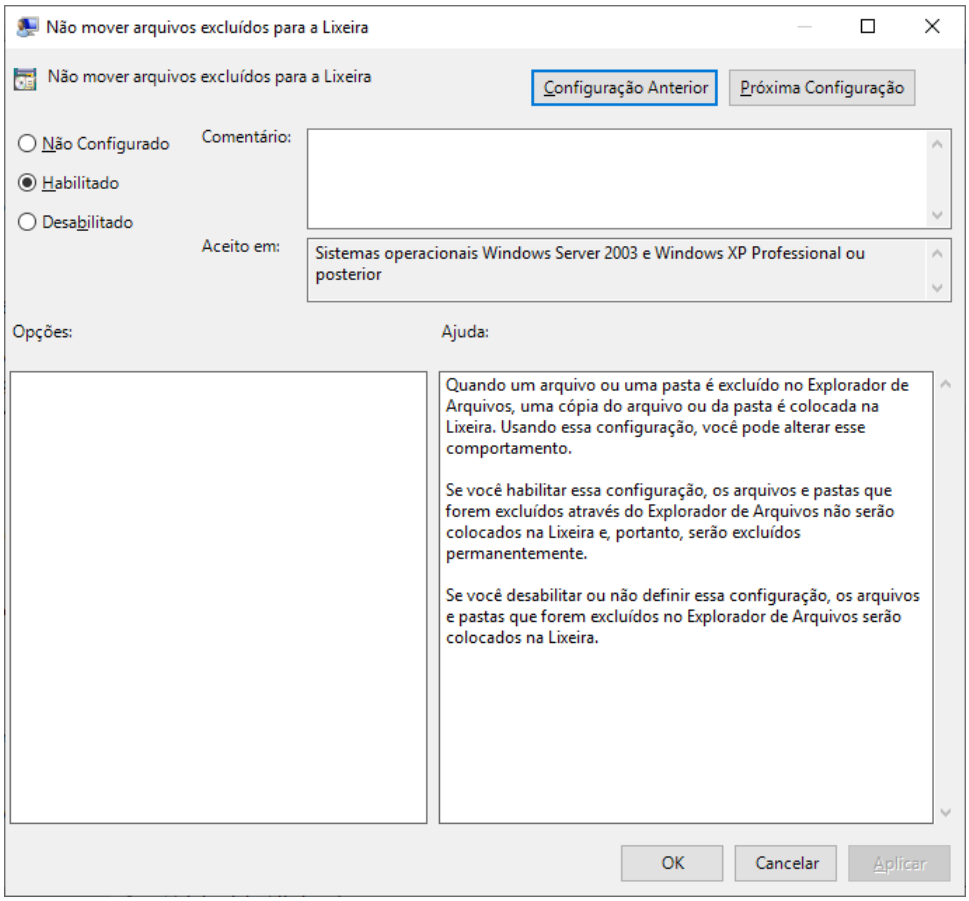


Procedimento 16 – Windows 10

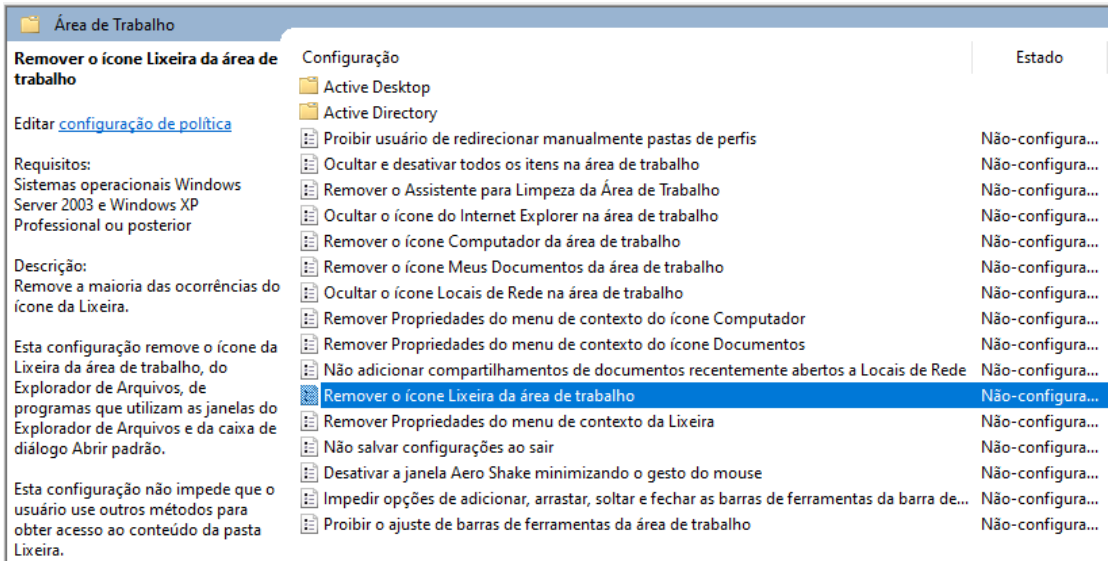
Não mover arquivos excluídos para lixeira.

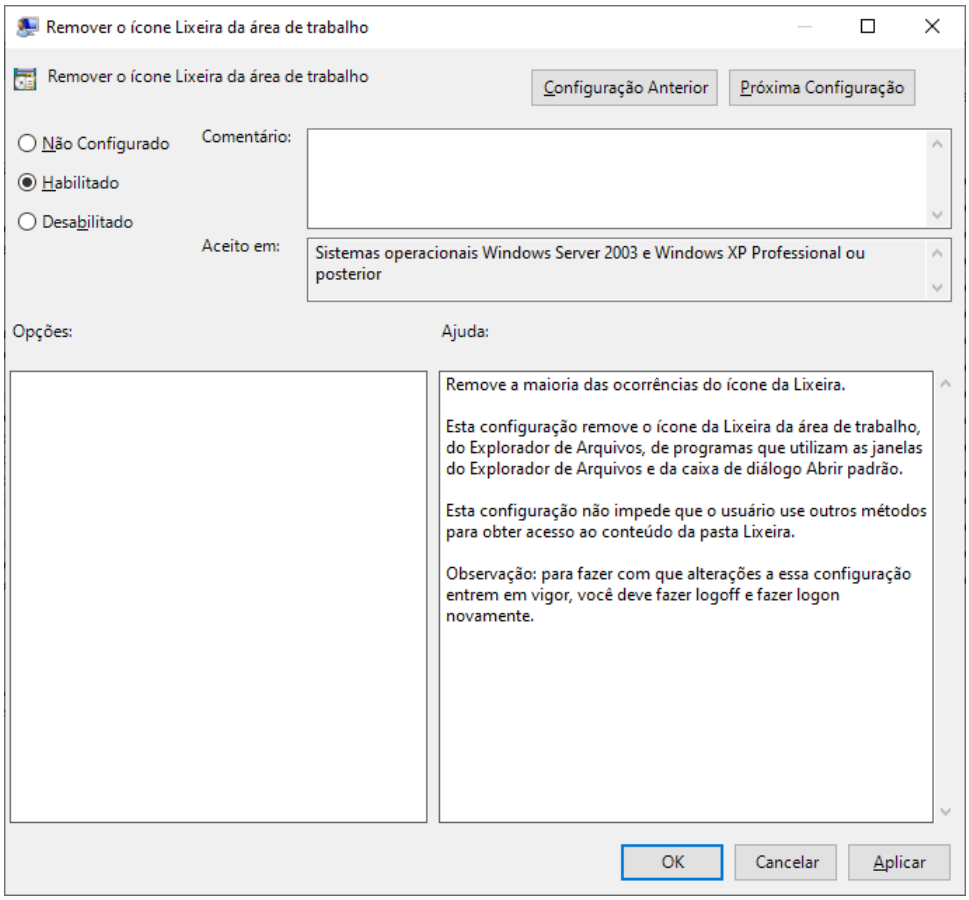
6. Iniciar -> Pesquisar "**Gpedit.msc"** -> **Gpedit.msc**.
7. Selecione: CONFIGURAÇÃO DO USUARIO -> MODELOS ADMINISTRATIVOS -> COMPONENTES DO WINDOWS -> EXPLORADOR DE ARQUIVOS:
8. Configurar conforme imagem abaixo a política: "***Não mover arquivos excluídos para a Lixeira".***





9. Selecione: CONFIGURAÇÃO DO USUARIO -> MODELOS ADMINISTRATIVOS -> ÁREA DE TRABALHO:
10. Configurar conforme imagem abaixo a política: "***Remover o ícone Lixeira da área de trabalho.".***





Procedimento 17

Desativar área de trabalho remota.

1. Iniciar -> Pesquisar "**Gpedit.msc"** -> **Gpedit.msc**.
2. Selecione: CONFIGURAÇÃO DO COMPUTADOR -> MODELOS ADMINISTRATIVOS -> COMPONENTES DO WINDOWS -> SERVIÇOS DE ÁREA DE TRABALHO REMOTA -> HOST DE SESSÃO DA ÁREA DE TRABALHO REMOTA -> CONEXÕES:
3. Configurar conforme imagem abaixo a política: "***Permitir que os usuários se conectem remotamente usando os Serviços de Área de Trabalho Remota".***