

	<b>Configuração de Máquina de AR</b>	<b>Versão</b>	<b>Data</b>	<b>Página</b>
		1.9	01/06/2020	1 de 53

## **Valid Certificadora Digital LTDA**

### **Infraestrutura**

*Este documento é de propriedade da Valid Certificadora e elaborado especialmente para servir de instrumento de apoio aos procedimentos da Estrutura de Certificação Digital, não podendo ser reproduzido nem comunicado, transmitido ou de qualquer forma ter seu conteúdo informado, total ou parcialmente, a pessoas estranhas às negociações com a Valid Certificadora.*

	<b>Configuração de Máquina de AR</b>			
		<b>Versão</b>	<b>Data</b>	<b>Página</b>
		1.9	01/06/2020	2 de 53

### 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

*Este documento é de propriedade da Valid Certificadora e elaborado especialmente para servir de instrumento de apoio aos procedimentos da Estrutura de Certificação Digital, não podendo ser reproduzido nem comunicado, transmitido ou de qualquer forma ter seu conteúdo informado, total ou parcialmente, a pessoas estranhas às negociações com a Valid Certificadora.*

	<b>Configuração de Máquina de AR</b>	<b>Versão</b>	<b>Data</b>	<b>Página</b>
		1.9	01/06/2020	3 de 53

## Índice

CONTROLE DA VERSÃO.....	2
<b>1. INTRODUÇÃO .....</b>	<b>4</b>
<b>2. ESTRUTURA LÓGICA .....</b>	<b>4</b>
<b>3. SISTEMAS OPERACIONAIS HOMOLOGADOS.....</b>	<b>4</b>
<b>4. GESTOR TÉCNICO .....</b>	<b>4</b>
<b>5. CONFIGURAÇÕES DE GRUPO (GPO).....</b>	<b>5</b>
2.1 DOWNLOAD DE SOFTWARES .....	5
2.2 SISTEMA OPERACIONAL E HOSTNAME.....	5
2.3 ATUALIZAÇÕES AUTOMÁTICAS – <i>ITEM NORMATIVO</i> .....	5
2.4 AUDITORIAS – <i>ITEM NORMATIVO</i> .....	5
2.5 VISUALIZADOR DE EVENTOS (EVENT VIEWER) – <i>ITEM NORMATIVO</i> .....	5
2.6 DATA E HORA – <i>ITEM NORMATIVO</i> .....	6
2.7 FIREWALL – <i>ITEM NORMATIVO</i> .....	6
2.8 PROTEÇÕES TELA DE AR – <i>ITEM NORMATIVO</i> .....	6
2.9 SITES CONFIÁVEIS VIA GPO – <i>RECOMENDÁVEL</i> .....	6
2.10 INTERNET EXPLORER.....	6
2.11 PAPEL DE PAREDE PADRÃO – <i>RECOMENDÁVEL</i> .....	6
2.12 REPOSITÓRIO DE SOFTWARES E ARQUIVOS DIGITALIZADOS – <i>RECOMENDÁVEL</i> .....	6
2.13 CONFIGURAÇÃO DE USUÁRIO DE WINDOWS – <i>ITEM NORMATIVO</i> .....	7
2.14 POLÍTICA DE SENHA FORTE – <i>ITEM NORMATIVO</i> .....	7
2.15 DIRETIVAS DE BLOQUEIO DE CONTA – <i>ITEM NORMATIVO</i> .....	7
2.16 BLOQUEIO DE APLICATIVO LOJA E LOGON COM CONTAS MICROSOFT – <i>ITEM NORMATIVO</i> .....	7
2.17 CRIPTOGRAFIA DE DISCO – <i>ITEM NORMATIVO</i> .....	7
2.18 DESABILITAR ÁREA DE TRABALHO REMOTA – <i>ITEM NORMATIVO</i> .....	8
2.19 NÃO MOVER ARQUIVOS EXCLUÍDOS PARA LIXEIRA – <i>RECOMENDÁVEL</i> .....	8
<b>6. DRIVERS/APLICATIVOS/FERRAMENTAS .....</b>	<b>8</b>
3.1 ANTIVÍRUS E ANTI-SPYWARE – <i>ITEM NORMATIVO</i> .....	8
3.2 CADEIAS ICP-BRASIL E VALID AC – <i>RECOMENDÁVEL</i> .....	8
3.3 SCANNER/IMPRESSORA.....	8
3.4 SISTEMA DE BIOMETRIA VALID – <i>RECOMENDÁVEL</i> .....	8
<b>7. APLICATIVOS COMPLEMENTARES .....</b>	<b>8</b>
<b>8. PROCEDIMENTOS.....</b>	<b>9</b>
PROCEDIMENTO 1.....	9
PROCEDIMENTO 2.....	13
PROCEDIMENTO 3.....	14
PROCEDIMENTO 4.....	16
PROCEDIMENTO 5.....	18
PROCEDIMENTO 6.....	20
PROCEDIMENTO 7.....	21
PROCEDIMENTO 8.....	23
PROCEDIMENTO 9.....	24
PROCEDIMENTO 10.....	30

*Este documento é de propriedade da Valid Certificadora e elaborado especialmente para servir de instrumento de apoio aos procedimentos da Estrutura de Certificação Digital, não podendo ser reproduzido nem comunicado, transmitido ou de qualquer forma ter seu conteúdo informado, total ou parcialmente, a pessoas estranhas às negociações com a Valid Certificadora.*

	<b>Configuração de Máquina de AR</b>	<b>Versão</b>	<b>Data</b>	<b>Página</b>
		1.9	01/06/2020	4 de 53

PROCEDIMENTO 11.....	31
PROCEDIMENTO 12.....	32
PROCEDIMENTO 13.....	37
PROCEDIMENTO 14.....	46
PROCEDIMENTO 15.....	49
PROCEDIMENTO 16.....	51
PROCEDIMENTO 17.....	53

## 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 detalhes 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

*Este documento é de propriedade da Valid Certificadora e elaborado especialmente para servir de instrumento de apoio aos procedimentos da Estrutura de Certificação Digital, não podendo ser reproduzido nem comunicado, transmitido ou de qualquer forma ter seu conteúdo informado, total ou parcialmente, a pessoas estranhas às negociações com a Valid Certificadora.*

	<b>Configuração de Máquina de AR</b>	<b>Versão</b>	<b>Data</b>	<b>Página</b>
		1.9	01/06/2020	5 de 53

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](#)

*Este documento é de propriedade da Valid Certificadora e elaborado especialmente para servir de instrumento de apoio aos procedimentos da Estrutura de Certificação Digital, não podendo ser reproduzido nem comunicado, transmitido ou de qualquer forma ter seu conteúdo informado, total ou parcialmente, a pessoas estranhas às negociações com a Valid Certificadora.*

	<b>Configuração de Máquina de AR</b>	<b>Versão</b>	<b>Data</b>	<b>Página</b>
		1.9	01/06/2020	6 de 53

## 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.

*Este documento é de propriedade da Valid Certificadora e elaborado especialmente para servir de instrumento de apoio aos procedimentos da Estrutura de Certificação Digital, não podendo ser reproduzido nem comunicado, transmitido ou de qualquer forma ter seu conteúdo informado, total ou parcialmente, a pessoas estranhas às negociações com a Valid Certificadora.*

	<b>Configuração de Máquina de AR</b>	<b>Versão</b>	<b>Data</b>	<b>Página</b>
		1.9	01/06/2020	7 de 53

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](#)

*Este documento é de propriedade da Valid Certificadora e elaborado especialmente para servir de instrumento de apoio aos procedimentos da Estrutura de Certificação Digital, não podendo ser reproduzido nem comunicado, transmitido ou de qualquer forma ter seu conteúdo informado, total ou parcialmente, a pessoas estranhas às negociações com a Valid Certificadora.*

	<b>Configuração de Máquina de AR</b>	<b>Versão</b>	<b>Data</b>	<b>Página</b>
		1.9	01/06/2020	8 de 53

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

*Este documento é de propriedade da Valid Certificadora e elaborado especialmente para servir de instrumento de apoio aos procedimentos da Estrutura de Certificação Digital, não podendo ser reproduzido nem comunicado, transmitido ou de qualquer forma ter seu conteúdo informado, total ou parcialmente, a pessoas estranhas às negociações com a Valid Certificadora.*

	<b>Configuração de Máquina de AR</b>			
		<b>Versão</b>	<b>Data</b>	<b>Página</b>
		1.9	01/06/2020	9 de 53

## 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.



Configuração	Estado	Comentário
<input type="checkbox"/> Não exibir a opção 'Instalar Atualizações e Desligar' na caixa de diálogo Desligar o Windows	Não-configura...	Não
<input type="checkbox"/> Não ajustar a opção padrão para 'Instalar Atualizações e Desligar' na caixa de diálogo Desligar o Windows	Não-configura...	Não
<input type="checkbox"/> Habilitando o Gerenciamento de Energia do Windows Update para ativar automaticamente o sistema e instalar a...	Não-configura...	Não
<input type="checkbox"/> Configurar Atualizações Automáticas	Habilitado	Não
<input type="checkbox"/> Especificar o local do serviço de atualização na intranet da Microsoft	Não-configura...	Não
<input type="checkbox"/> Frequência de detecção de Atualizações Automáticas	Não-configura...	Não
<input type="checkbox"/> Turn off the upgrade to the latest version of Windows through Windows Update	Não-configura...	Não
<input type="checkbox"/> Permitir que usuários que não são administradores recebam notificações de atualização	Não-configura...	Não
<input type="checkbox"/> Ativar Notificações de Software	Não-configura...	Não
<input type="checkbox"/> Permitir instalação imediata de Atualizações Automáticas	Não-configura...	Não
<input type="checkbox"/> Ativar atualizações recomendadas via Atualizações Automáticas	Não-configura...	Não
<input type="checkbox"/> Não há reinicializações automáticas para usuários conectados, referentes às instalações de atualizações automati...	Não-configura...	Não
<input type="checkbox"/> Solicitar reinicialização novamente com instalações agendadas	Não-configura...	Não
<input type="checkbox"/> Atrasar Reinicialização de instalações agendadas	Habilitado	Não
<input type="checkbox"/> Reagendar instalações agendadas de Atualizações Automáticas	Não-configura...	Não
<input type="checkbox"/> Habilitar destino do lado do cliente	Não-configura...	Não
<input type="checkbox"/> Permitir atualizações assinadas do local do serviço de atualização da intranet da Microsoft	Não-configura...	Não

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

**Configurar Atualizações Automáticas**

Configurar Atualizações Automáticas

Não Configurado    Comentário:

**Habilitado**

Desabilitado

Aceito em: Pelo menos Windows 2000 Service Pack 3 ou Windows XP Professional Service Pack 1

Opções:

Configurar atualização automática:

**4 - Baixar automaticamente e agendar a instalação**

As configurações a seguir só serão obrigatórias e aplicáveis se 4 for selecionado.

Dia agendado para a instalação: 0 - Todo dia

Hora agendada para a instalação: 09:00

Ajuda:

Especifica se este computador receberá atualizações de segurança e outros downloads importantes por meio do serviço de atualizações automáticas do Windows.

Esta configuração permite especificar se as atualizações automáticas são habilitadas no computador. Se o serviço for habilitado, você deverá selecionar uma das quatro opções na Configuração de Diretiva de Grupo:

2 = Avisar antes de fazer o download das atualizações e de instalá-las no computador.

Quando o Windows encontra atualizações que se aplicam ao computador, ele exibe um ícone na área de status com uma mensagem para indicar que há atualizações prontas para serem baixadas. Clique no ícone ou na mensagem para selecionar as atualizações específicas a serem baixadas. Em seguida, o Windows baixará as atualizações

OK    Cancelar    Aplicar

**Atrasar Reinicialização de instalações agendadas**

Atrasar Reinicialização de instalações agendadas

Não Configurado    Comentário:

**Habilitado**

Desabilitado

Aceito em: Pelo menos Windows 2000 Service Pack 3 ou Windows XP Professional Service Pack 1

Opções:

Aguardar pelo tempo a seguir antes de continuar com a reinicialização agendada (minutos): 60

Ajuda:

Especifica o tempo pelo qual as Atualizações Automáticas devem aguardar antes de prosseguir com uma reinicialização agendada.

Se o status estiver definido como Habilitado, uma reinicialização agendada ocorrerá dentro do número especificado de minutos depois que a instalação for concluída.

Se o status estiver definido como Desabilitado ou Não Configurado, o tempo de espera padrão será de 15 minutos.

Observação: essa diretiva se aplica apenas quando as Atualizações Automáticas estão configuradas para executar instalações agendadas de atualizações. Se a diretiva "Configurar Atualizações Automáticas" estiver desabilitada, esta diretiva não terá efeito.

OK    Cancelar    Aplicar

	<b>Configuração de Máquina de AR</b>			
		<b>Versão</b>	<b>Data</b>	<b>Página</b>
		1.9	01/06/2020	11 de 53

## Procedimento 1 - Windows 10

### Procedimento para atualização do Sistema Operacional

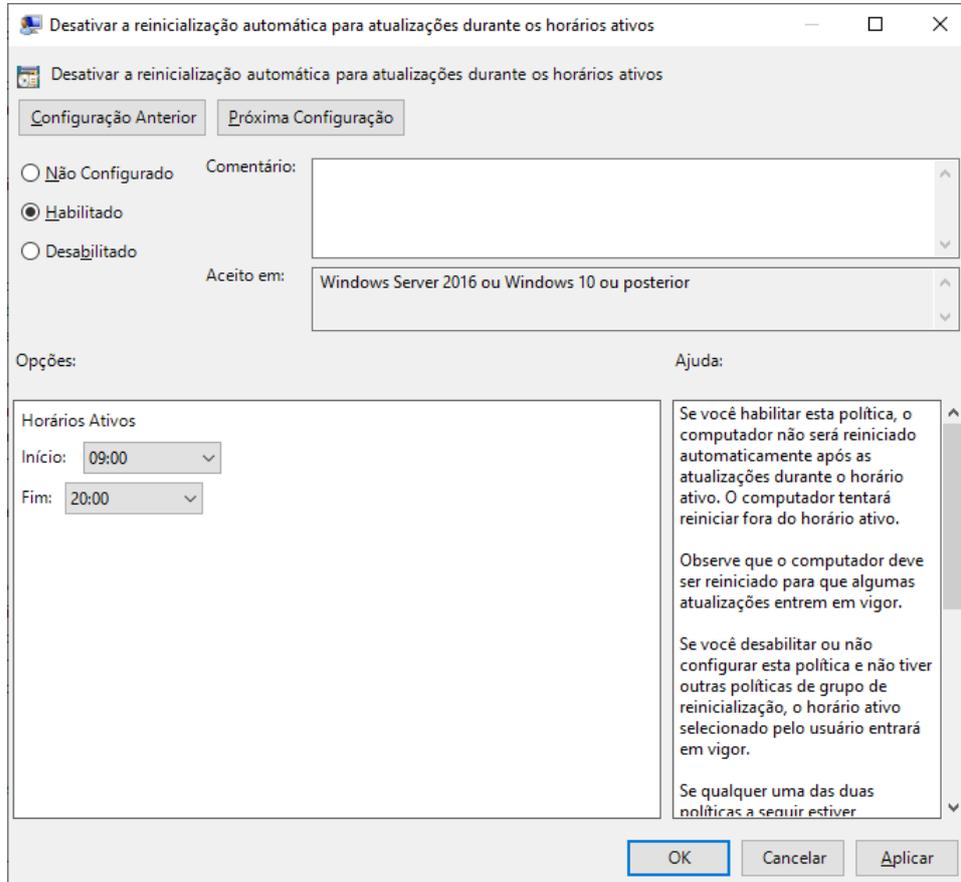
As seguintes configurações devem ser executadas:

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

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

Seleção de item para exibir sua descrição.	Configuração	Estado
	Windows Update para Empresas	
	Não exibir a opção 'Instalar Atualizações e Desligar' na caixa de diálogo Desligar o Windows	Não-configura...
	Não ajustar a opção padrão para 'Instalar Atualizações e Desligar' na caixa de diálogo Desligar o Windows	Não-configura...
	Habilitando o Gerenciamento de Energia do Windows Update para ativar automaticamente o sistema e ...	Não-configura...
	Desativar a reinicialização automática para atualizações durante os horários ativos	Habilitado
	Especificar o intervalo de horas ativas para reinícios automáticos	Não-configura...
	Permitir que as atualizações sejam baixadas automaticamente em conexões limitadas	Não-configura...
	Sempre reiniciar automaticamente no horário agendado	Não-configura...
	Especifique o prazo final antes do reinício automático para a instalação da atualização	Não-configura...
	Configurar notificações de lembrete do reinício automático para atualizações	Não-configura...
	Desativar notificações de reinício automático para instalações de atualização	Não-configura...
	Configurar notificação de reinicialização automática necessária para atualizações	Não-configura...
	Configurar Atualizações Automáticas	Habilitado

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



**Desativar a reinicialização automática para atualizações durante os horários ativos**

Desativar a reinicialização automática para atualizações durante os horários ativos

Configuração Anterior | Próxima Configuração

Não Configurado  
 **Habilitado**  
 Desabilitado

Comentário:

Aceito em: Windows Server 2016 ou Windows 10 ou posterior

Opções:

Horários Ativos

Início: 09:00

Fim: 20:00

Ajuda:

Se você habilitar esta política, o computador não será reiniciado automaticamente após as atualizações durante o horário ativo. O computador tentará reiniciar fora do horário ativo.

Observe que o computador deve ser reiniciado para que algumas atualizações entrem em vigor.

Se você desabilitar ou não configurar esta política e não tiver outras políticas de grupo de reinicialização, o horário ativo selecionado pelo usuário entrará em vigor.

Se qualquer uma das duas políticas a seguir estiver

OK Cancelar Aplicar

Configurar Atualizações Automáticas

Configurar Atualizações Automáticas

Configuração Anterior Próxima Configuração

Não Configurado    Comentário:

**Habilitado**

Desabilitado

Aceito em: Windows XP Professional Service Pack 1 ou Windows 2000 Service Pack 3 ou posterior

Opções:

Ajuda:

Configurar atualização automática:

**4 - Baixar automaticamente e agendar a instalação**

As configurações a seguir só serão obrigatórias e aplicáveis se a opção 4 for selecionada.

Instalar durante a manutenção automática

Dia agendado para a instalação: 0 - Todo dia

Hora agendada para a instalação: 08:00

Se você selecionar "4 - Baixar automaticamente e agendar a instalação" para o dia agendado e especificar um agendamento, também terá a opção de limitar a atualização a:

A cada semana

Primeira semana do mês

Segunda semana do mês

Especifica se este computador receberá atualizações de segurança e outros downloads importantes por meio do serviço de atualizações automáticas do Windows.

Observação: esta política não se aplica ao Windows RT.

Essa configuração permite especificar se as atualizações automáticas estão habilitadas no computador. Se o serviço estiver habilitado, você deverá selecionar uma das quatro opções na Configuração de Política de Grupo:

2 = Avisar antes de baixar e instalar qualquer atualização.

OK Cancelar Aplicar

	<b>Configuração de Máquina de AR</b>			
		<b>Versão</b>	<b>Data</b>	<b>Página</b>
		1.9	01/06/2020	13 de 53

## Procedimento 2

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

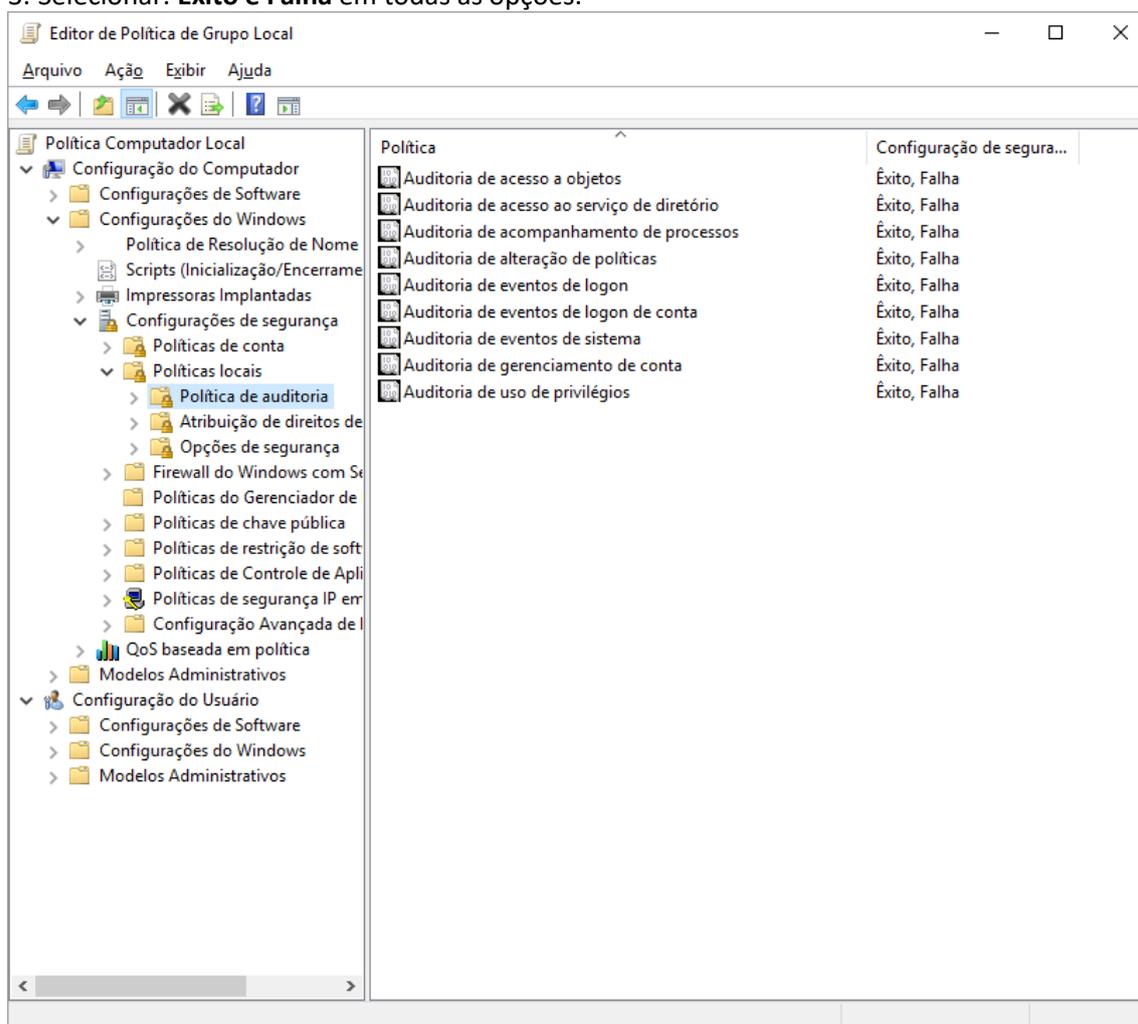
1. Executar o aplicativo “Diretiva de Grupo”.

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**

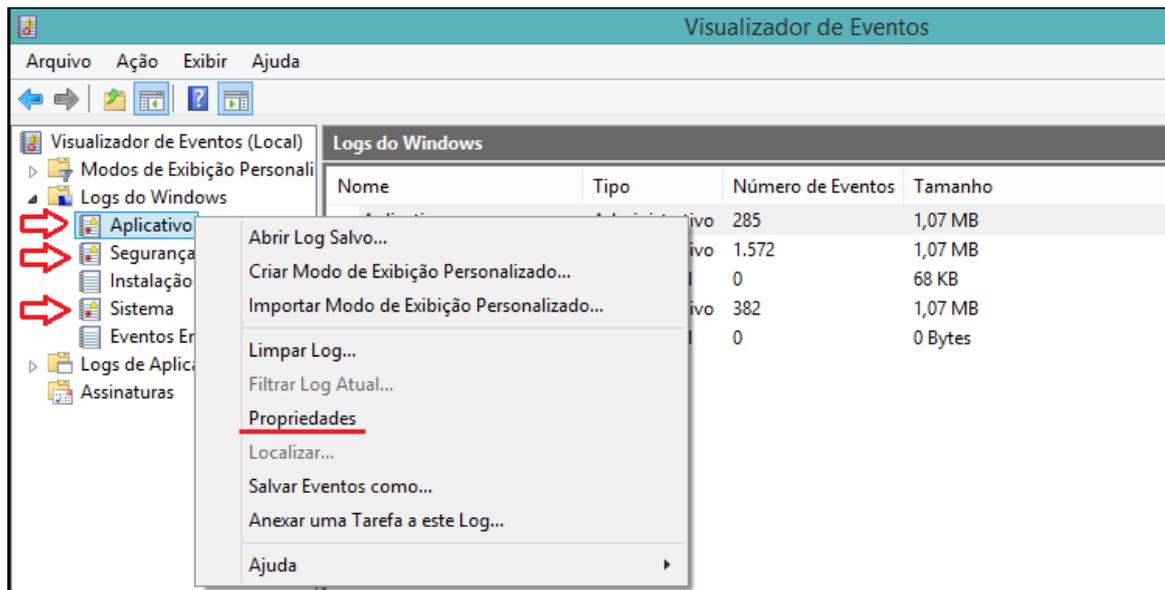
#### **Procedimento para configurar as opções do Event Viewer**

1. Executar o aplicativo “Visualizador de Eventos”.

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

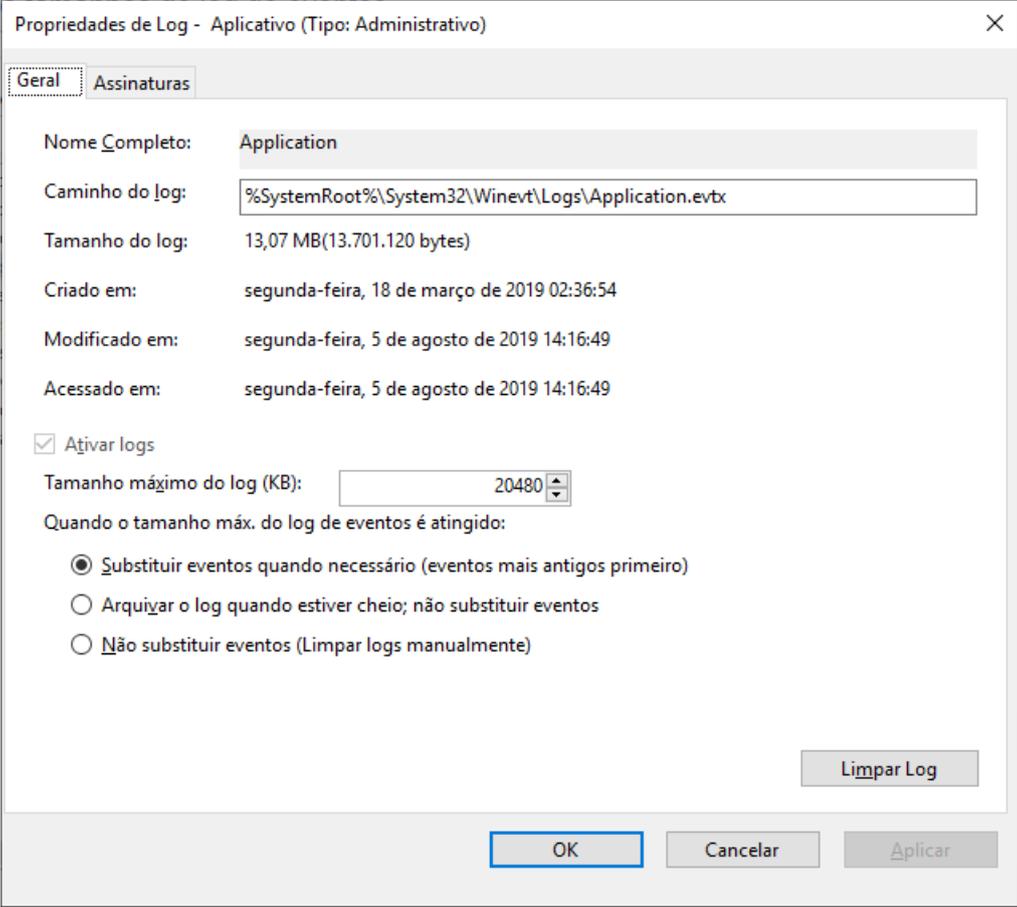
Clicar em OK.

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”.



	<b>Configuração de Máquina de AR</b>			
		<b>Versão</b>	<b>Data</b>	<b>Página</b>
		1.9	01/06/2020	15 de 53

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



Propriedades de Log - Aplicativo (Tipo: Administrativo)

**Gerar** Assinaturas

Nome Completo: Application

Caminho do log: %SystemRoot%\System32\Winevt\Logs\Application.evtx

Tamanho do log: 13,07 MB(13.701.120 bytes)

Criado em: segunda-feira, 18 de março de 2019 02:36:54

Modificado em: segunda-feira, 5 de agosto de 2019 14:16:49

Acessado em: segunda-feira, 5 de agosto de 2019 14:16:49

Ativar logs

Tamanho máximo do log (KB): 20480

Quando o tamanho máx. do log de eventos é atingido:

- Substituir eventos quando necessário (eventos mais antigos primeiro)
- Arquivar o log quando estiver cheio; não substituir eventos
- Não substituir eventos (Limpar logs manualmente)

Limpar Log

OK Cancelar Aplicar

2. Clicar em OK.

	<b>Configuração de Máquina de AR</b>			
		<b>Versão</b>	<b>Data</b>	<b>Página</b>
		1.9	01/06/2020	16 de 53

#### **Procedimento 4**

##### **Procedimento para sincronismo de data e hora**

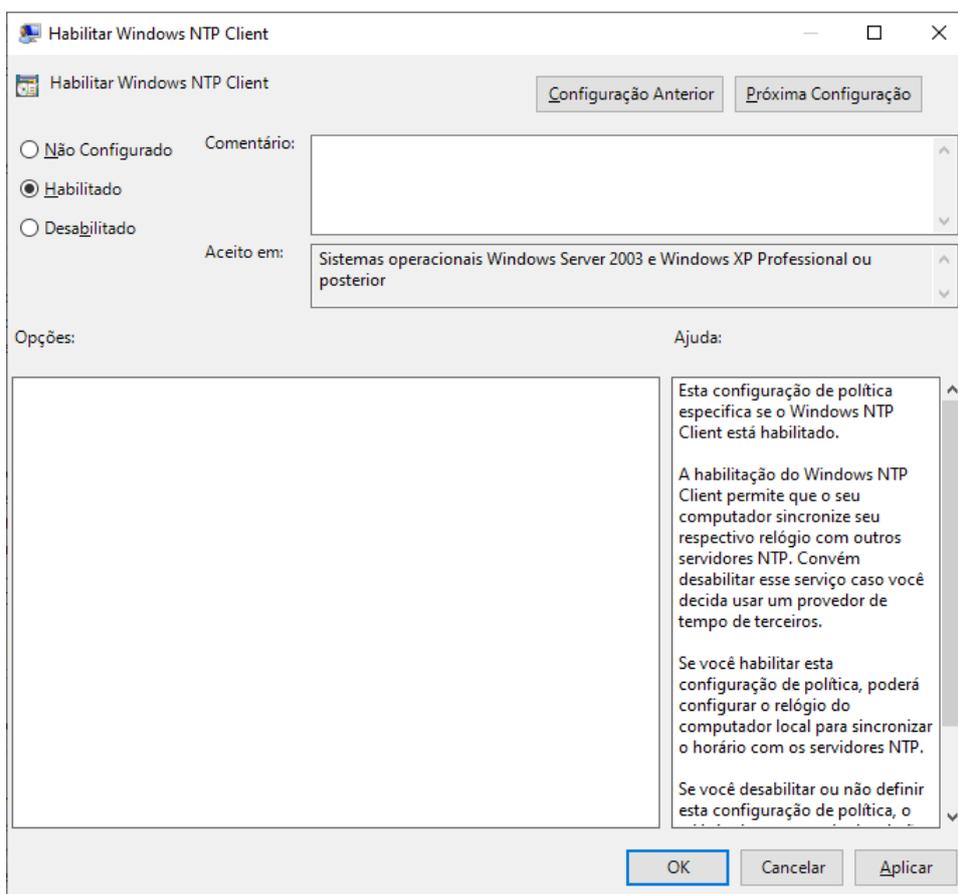
As seguintes configurações devem ser executadas:

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:



Configurar Windows NTP Client

Configurar Windows NTP Client

Não Configurado    Comentário:

**Habilitado**

Desabilitado

Aceito em: Sistemas operacionais Windows Server 2003 e Windows XP Professional ou posterior

Opções:

Ajuda:

NtpServer: 200.160.7.186

Type: NTP

CrossSiteSyncFlags: 2

ResolvePeerBackoffMinutes: 10

ResolvePeerBackoffMaxTimes: 7

SpecialPollInterval: 900

EventLogFlags: 0

Esta configuração de política especifica um conjunto de parâmetros para controlar o Windows NTP Client.

Se você habilitar esta configuração de política, poderá especificar os parâmetros a seguir para o Windows NTP Client.

Se você desabilitar ou não definir esta configuração de política, o Windows NTP Client usará os padrões de cada um dos seguintes parâmetros.

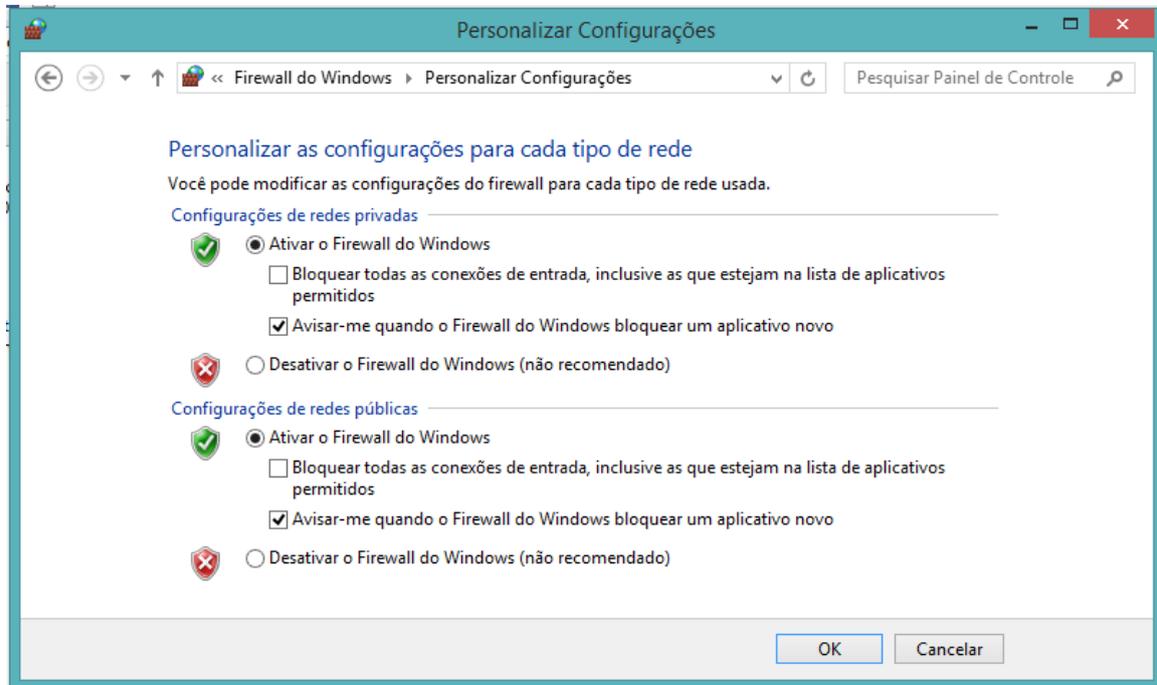
NtpServer  
O nome DNS (Sistema de Nomes de Domínio) ou o endereço IP de uma fonte de hora NTP. Esse valor está no formato

	<b>Configuração de Máquina de AR</b>			
		<b>Versão</b>	<b>Data</b>	<b>Página</b>
		1.9	01/06/2020	18 de 53

### Procedimento 5

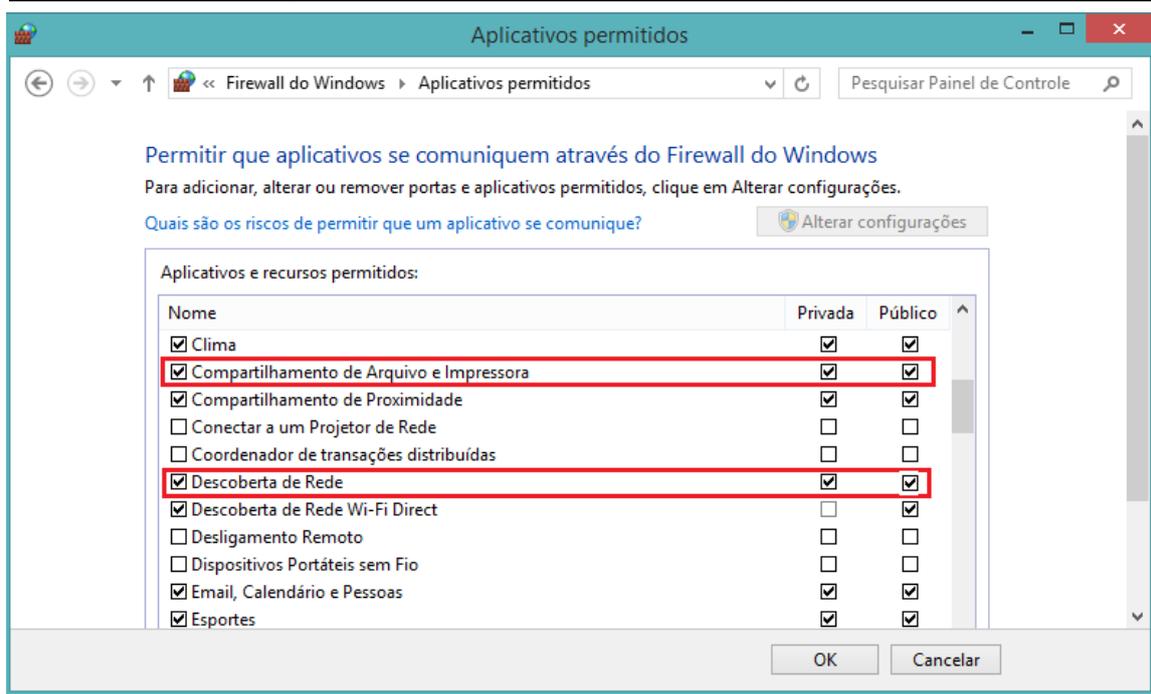
#### **Procedimento para Ativação do Firewall do Windows.**

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. Seleccione as opções: Descoberta de Rede e Compartilhamento de arquivos e impressoras conforme a imagem abaixo.

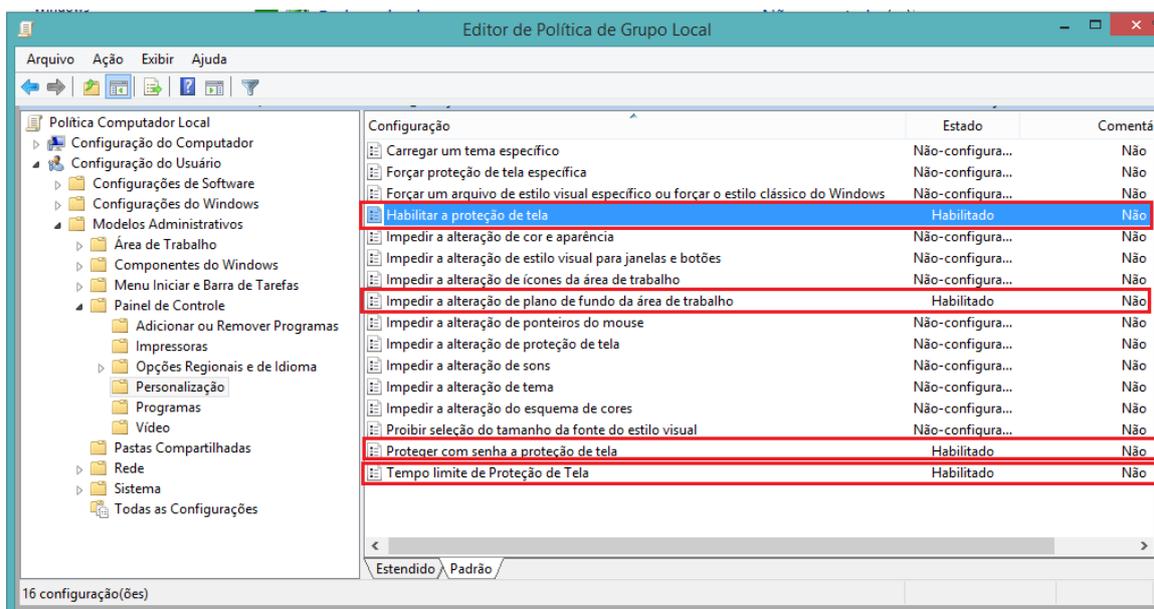


	<b>Configuração de Máquina de AR</b>			
		<b>Versão</b>	<b>Data</b>	<b>Página</b>
		1.9	01/06/2020	20 de 53

## 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.

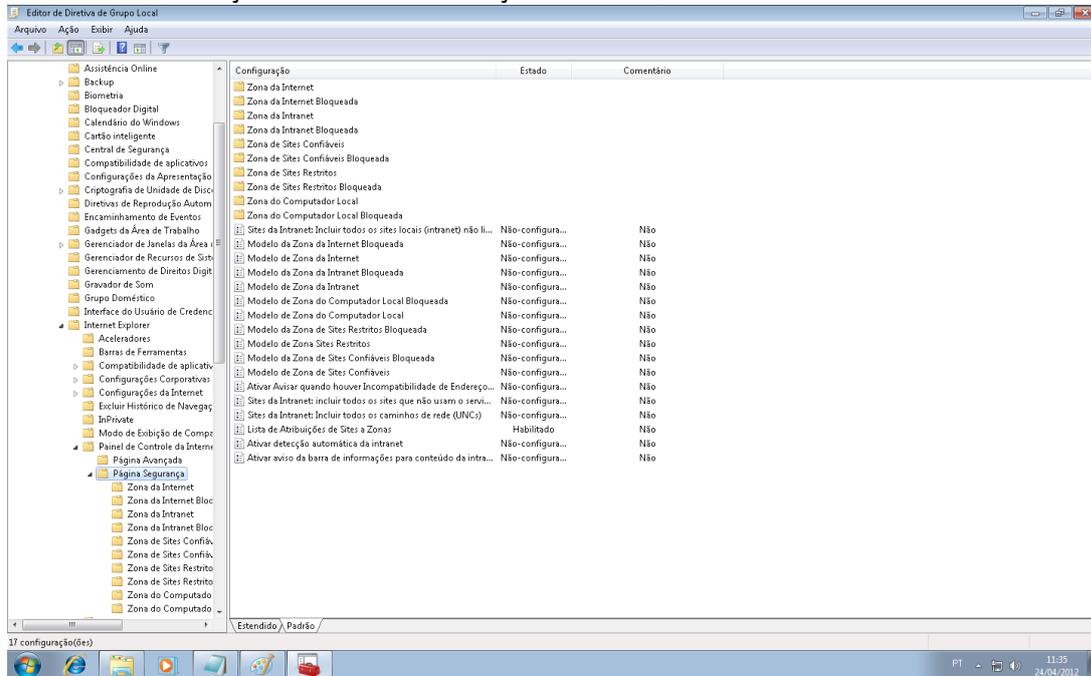


Na opção *Tempo limite de Proteção de Tela* além definir habilitado, defina o tempo com o valor de 120 segundos.

## 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.

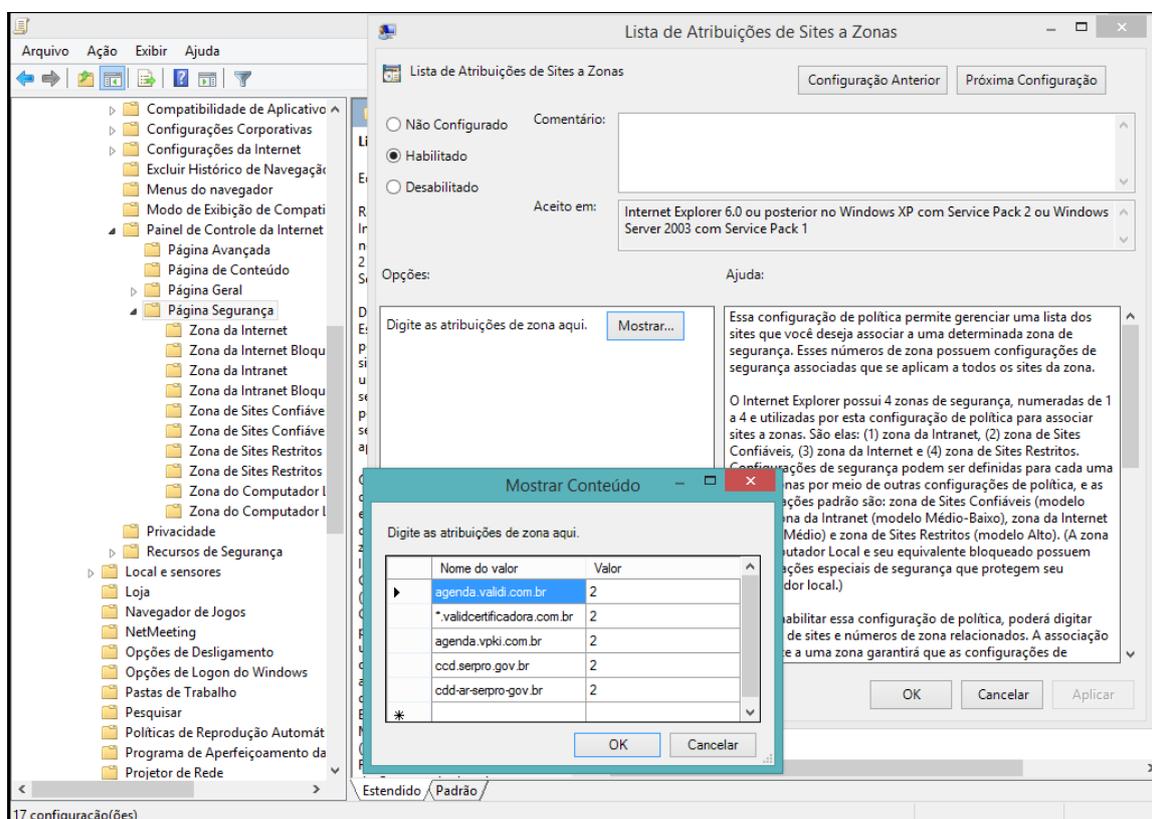
7. Inserir os sites listados como confiáveis,

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:



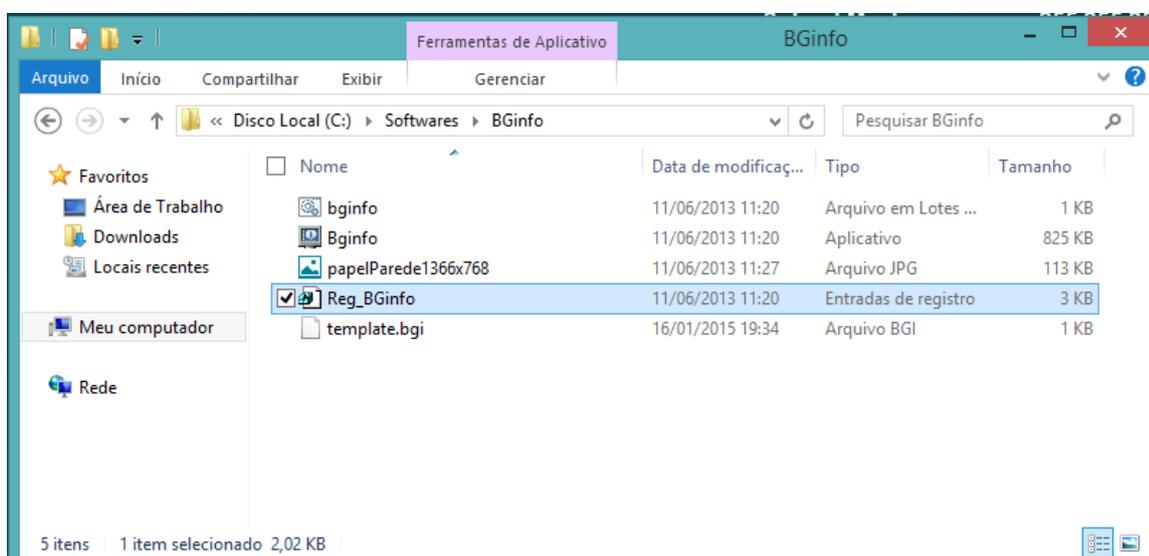
11. Clicar em OK.

	<b>Configuração de Máquina de AR</b>			
		<b>Versão</b>	<b>Data</b>	<b>Página</b>
		1.9	01/06/2020	23 de 53

## 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



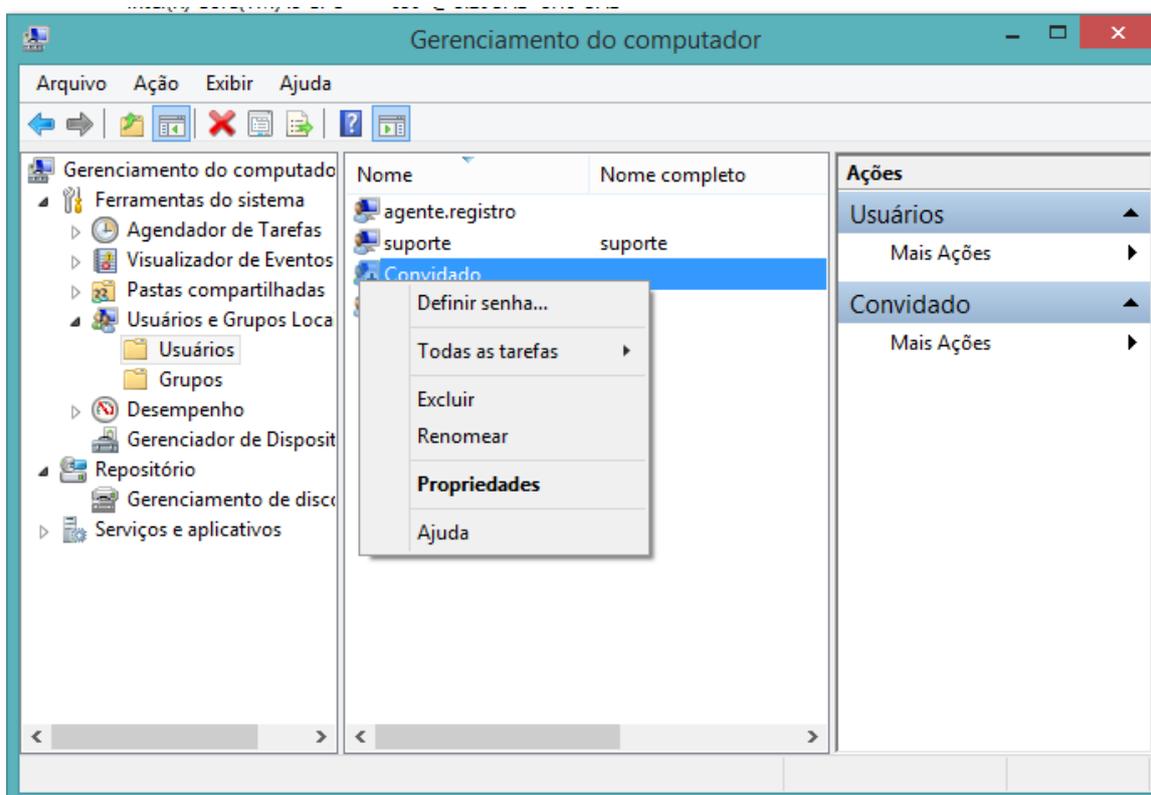
	<b>Configuração de Máquina de AR</b>			
		<b>Versão</b>	<b>Data</b>	<b>Página</b>
		1.9	01/06/2020	24 de 53

## Procedimento 9

### **Procedimento para configurar as contas dos usuários.**

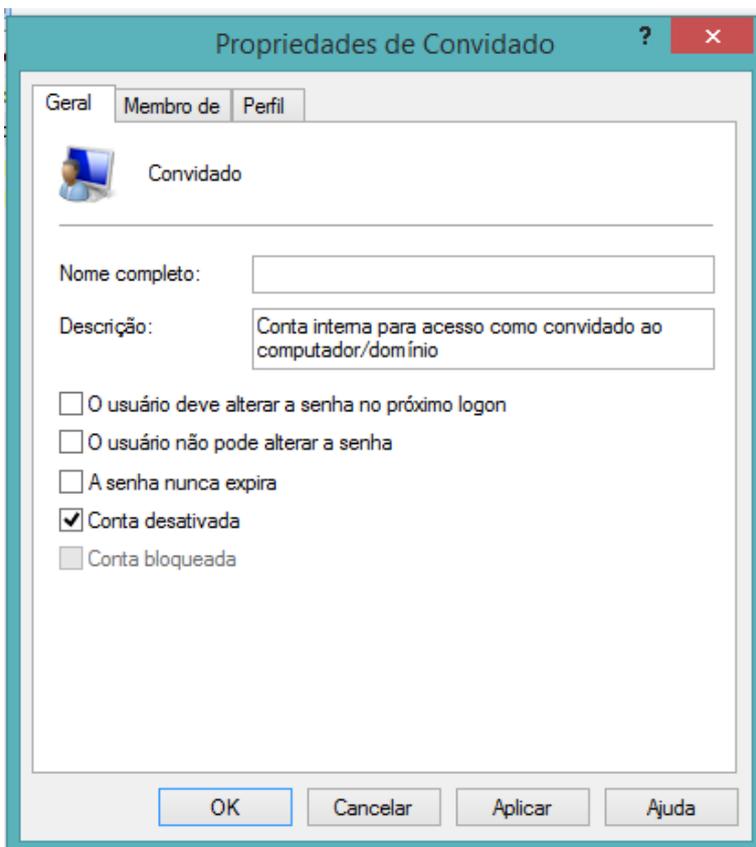
Apenas contas de administrador e de Agente de Registro devem estar cadastradas e disponíveis, demais contas devem ser excluídas ou desativadas.

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



	<b>Configuração de Máquina de AR</b>			
		<b>Versão</b>	<b>Data</b>	<b>Página</b>
		1.9	01/06/2020	25 de 53

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.

Novo Usuário ? x

Nome de usuário: marina.santos

Nome completo: Marina Quintana dos Santos

Descrição: Agente de Registro

---

Senha: ●●●●●●●●

Confirmar senha: ●●●●●●●●

O usuário deve alterar a senha no próximo logon

O usuário não pode alterar a senha

A senha nunca expira

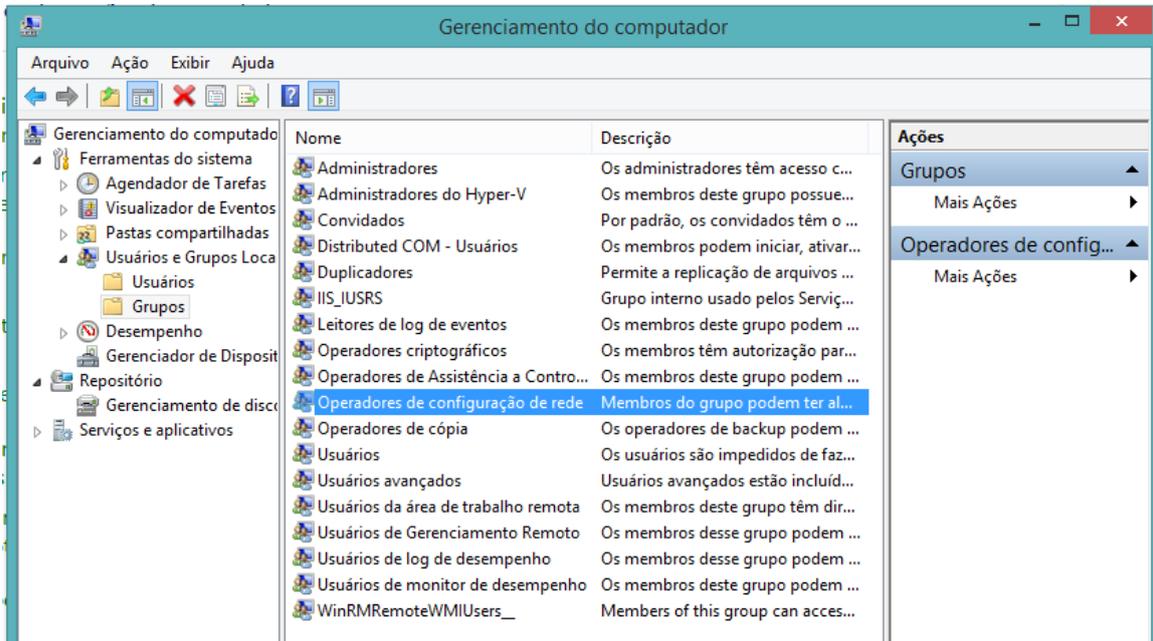
Conta desativada

---

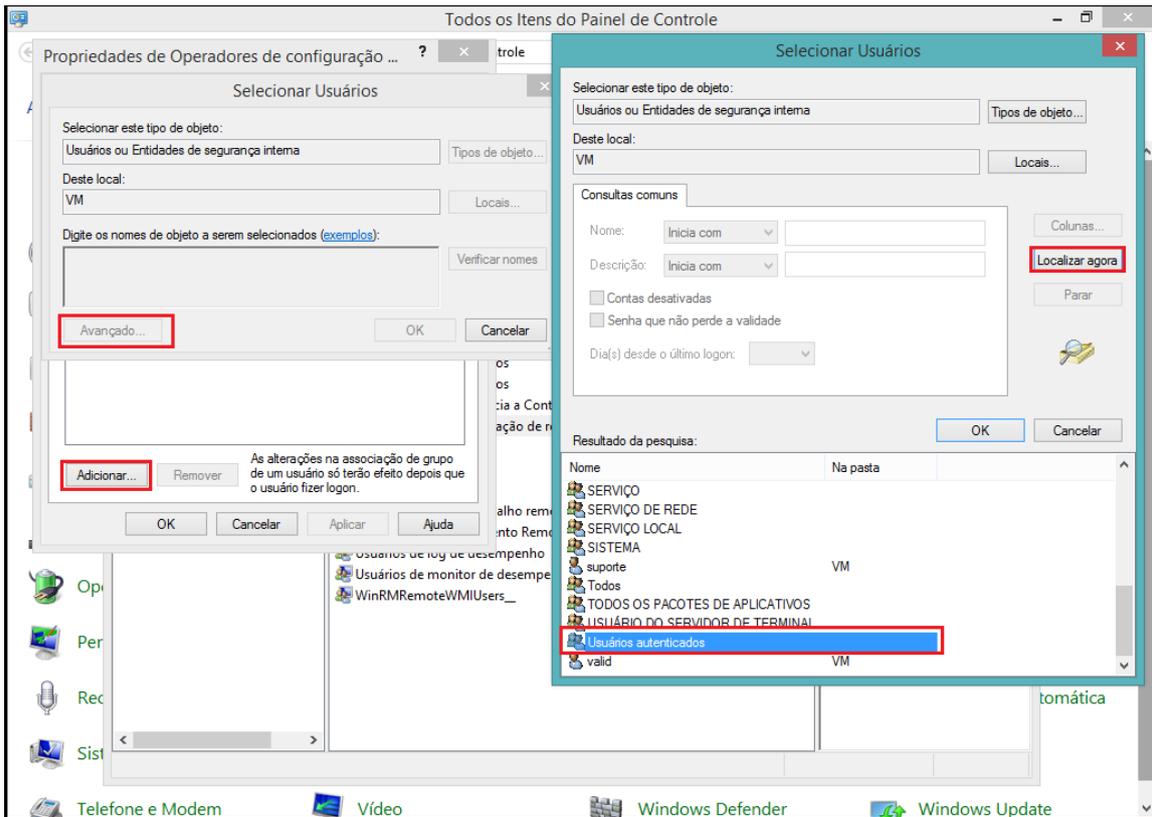
Ajuda Criar Fechar

	<b>Configuração de Máquina de AR</b>			
		<b>Versão</b>	<b>Data</b>	<b>Página</b>
		1.9	01/06/2020	27 de 53

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

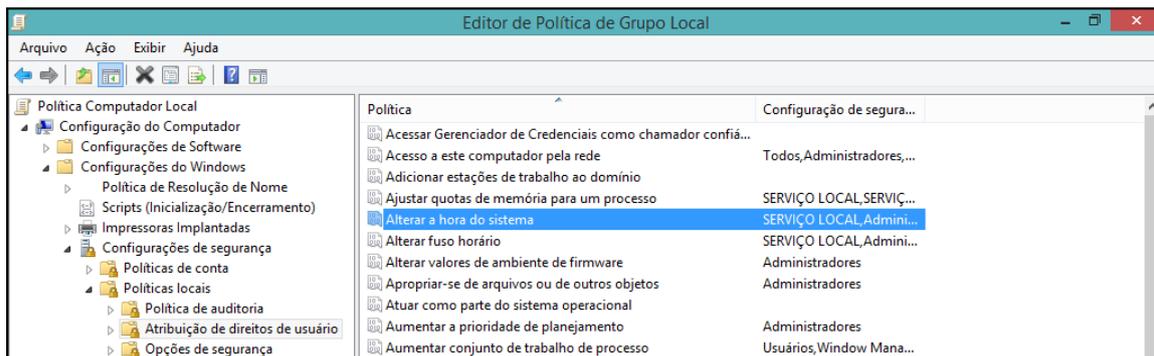


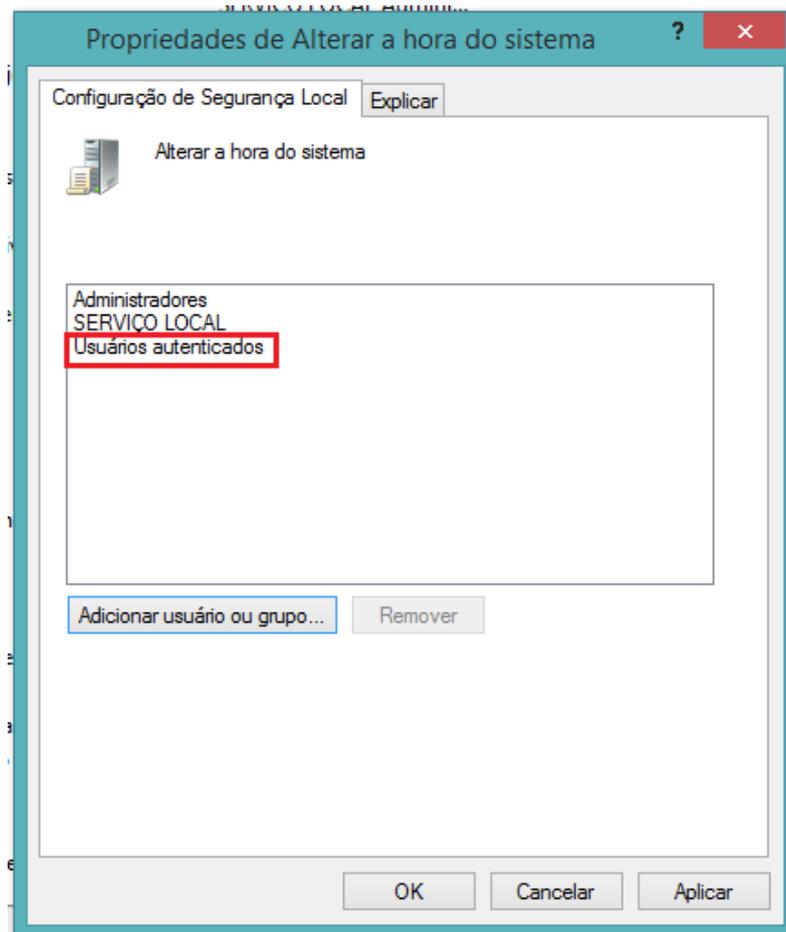
21. Clicar: Adicionar
22. Clicar : Avançado
23. Clicar: Localizar agora
24. Selecionar: Usuários Autenticados
25. Clicar: Ok.



### 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:



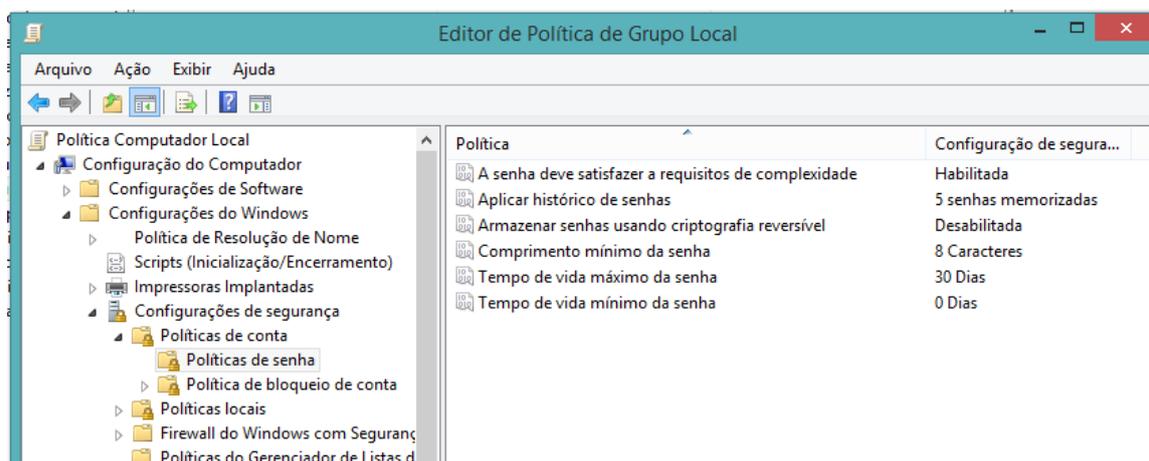


	<b>Configuração de Máquina de AR</b>			
		<b>Versão</b>	<b>Data</b>	<b>Página</b>
		1.9	01/06/2020	30 de 53

## 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 -> Políticas de Conta -> Políticas de Senha
3. Modificar os parâmetros referentes a Diretivas de Senha, de acordo com as figuras seguintes:

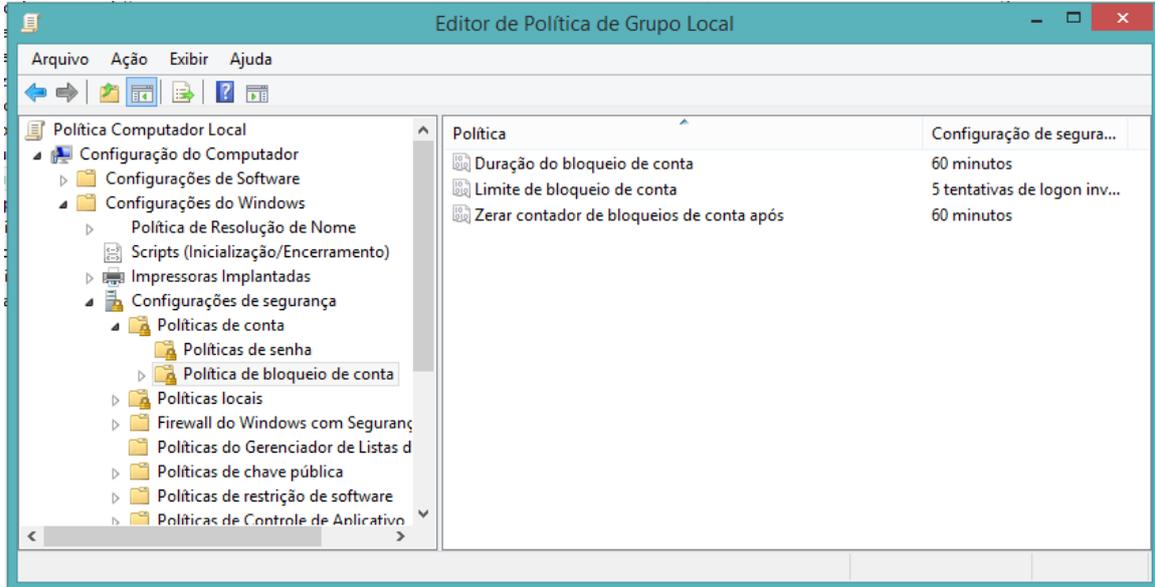


	<b>Configuração de Máquina de AR</b>			
		<b>Versão</b>	<b>Data</b>	<b>Página</b>
		1.9	01/06/2020	31 de 53

## 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

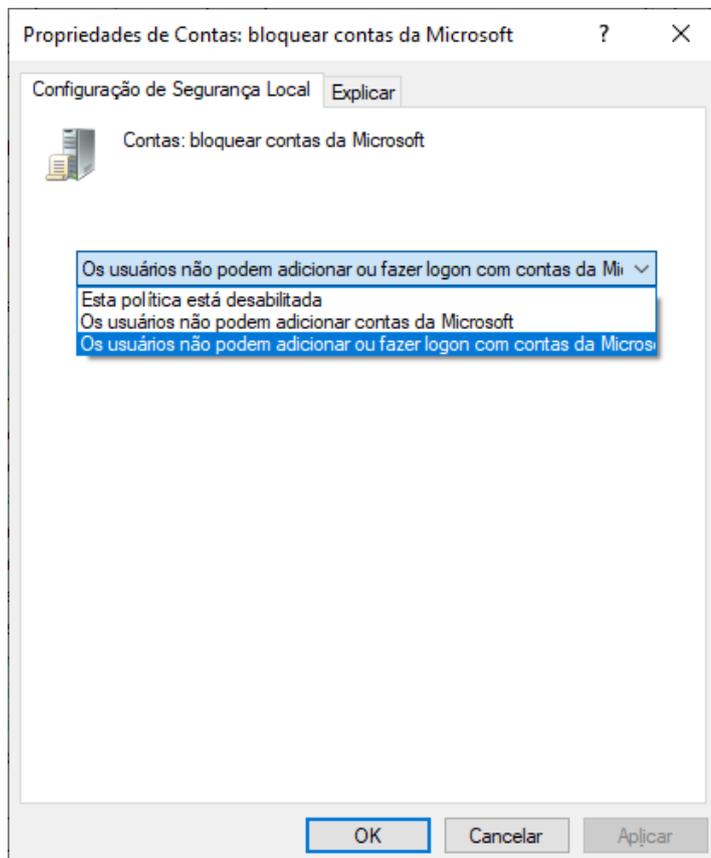
### Bloqueio de aplicativo Loja e logon com contas Microsoft – Windows 8.1 e 10.

#### 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.

Política	Configuração de segurança
Acesso à rede: caminhos do Registro acessíveis remotamente	System\CurrentControlSet\Control\ProductOptions,System\CurrentControlSet\C...
Acesso à rede: caminhos e subcaminhos do Registro acessíveis remotamente	System\CurrentControlSet\Control\Print\Printers,System\CurrentControlSet\Servi...
Acesso à rede: compartimentos acessíveis anonimamente	Não definido
Acesso à rede: deixar que as permissões de todos os usuários sejam aplicadas a usuários anônimos	Desabilitada
Acesso à rede: modelo de compartilhamento e segurança para contas locais	Clássico - os usuários locais são autenticados como eles próprios
Acesso à rede: não permitir enumeração anônima de contas e compartilhamentos SAM	Habilitada
Acesso à rede: não permitir enumeração anônima de contas SAM	Habilitada
Acesso à rede: não permitir o armazenamento de senhas e credenciais para autenticação de rede	Desabilitada
Acesso à rede: permitir SID anônimo/Conversão de nomes	Desabilitada
Acesso à rede: pipes nomeados acessíveis anonimamente	Não definido
Acesso à rede: restringir clientes autorizados a fazer chamadas remotas ao SAM	Habilitada
Acesso de rede: acesso anônimo restrito a pipes nomeados e compartilhamentos	Habilitada
Auditoria: desligar o sistema imediatamente se não for possível o log de auditorias de segurança	Desabilitada
Auditoria: fazer auditoria do acesso a objetos do sistema global	Desabilitada
Auditoria: fazer auditoria do uso dos privilégios Backup e Restauração	Desabilitada
Auditoria: forçar configurações de subcategorias de políticas de auditoria (Windows Vista ou supe...	Não definido
Cliente de rede Microsoft: assinar digitalmente a comunicação (se o servidor concordar)	Habilitada
Cliente de rede Microsoft: assinar digitalmente a comunicação (sempre)	Desabilitada
Cliente de rede Microsoft: enviar senha não criptografada para conectar-se a servidores SMB de o...	Desabilitada
Configurações do sistema: subsistemas opcionais	Não definido
Configurações do sistema: usar regras de certificado em arquivos executáveis do Windows para p...	Desabilitada
Console de recuperação: permite cópia em disquete e acesso a todas as unidades e pastas	Não definido
Console de recuperação: permitir logon administrativo automático	Não definido
Contas: bloquear contas da Microsoft	Os usuários não podem adicionar ou fazer logon com contas da Microsoft

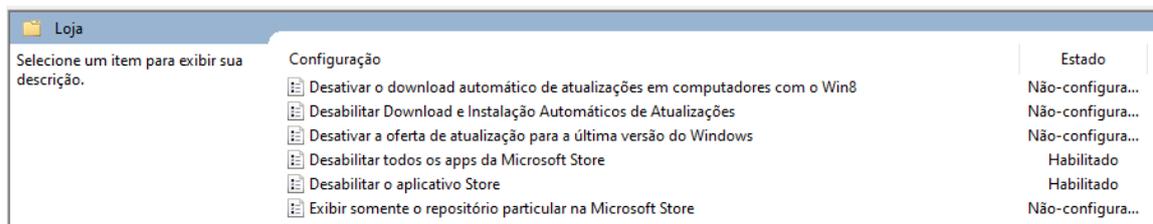
3. Modificar o parâmetro referente a Contas: bloquear contas Microsoft, de acordo com a figura seguinte:



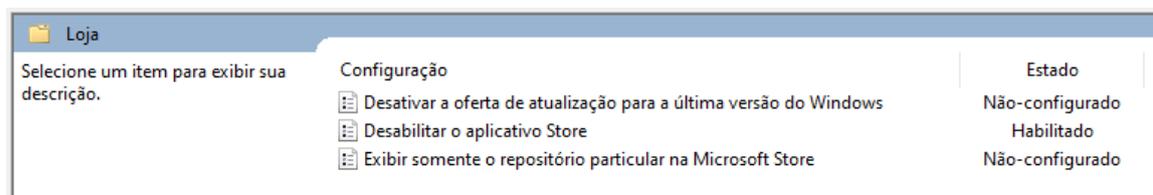
	<b>Configuração de Máquina de AR</b>			
		<b>Versão</b>	<b>Data</b>	<b>Página</b>
		1.9	01/06/2020	33 de 53

### 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**.



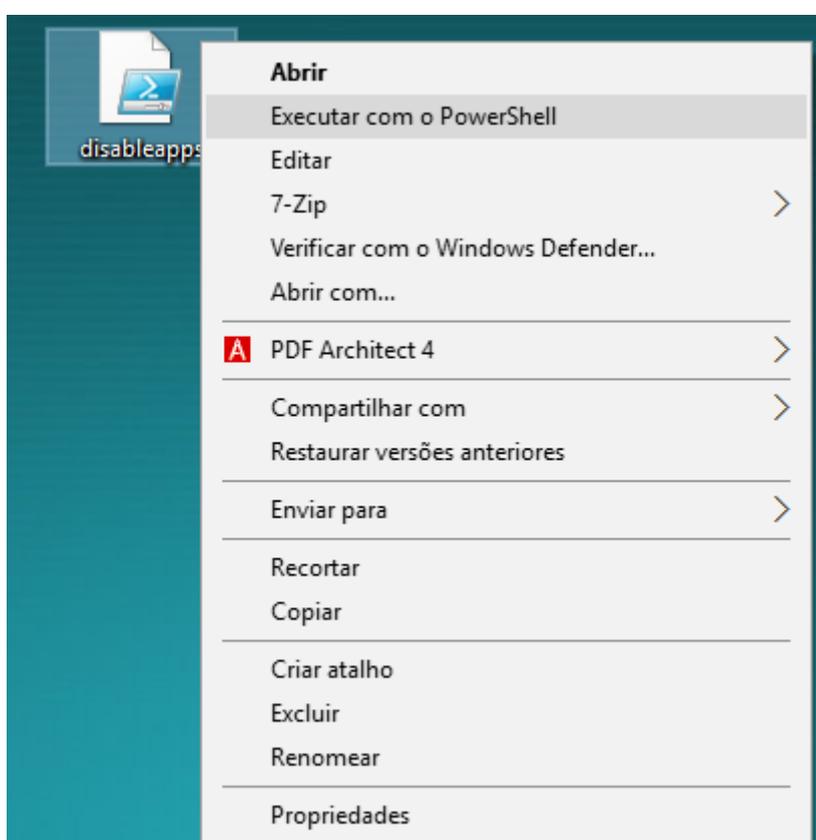
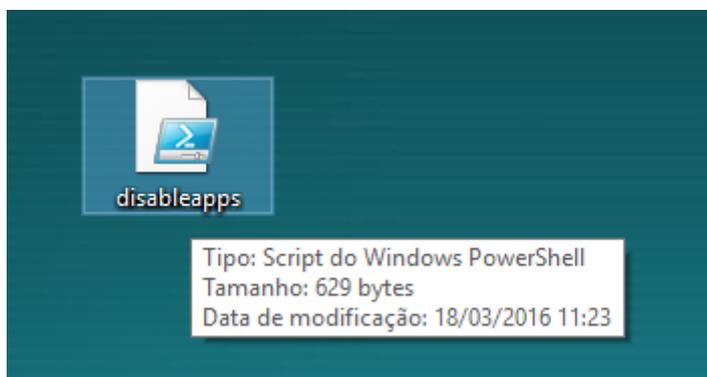
4. Selecione: CONFIGURAÇÃO DO USUARIO -> MODELOS ADMINISTRATIVOS -> COMPONENTES DO WINDOWS -> LOJA:
5. Configurar conforme imagem abaixo a política: **Desabilitar o aplicativo Store**:



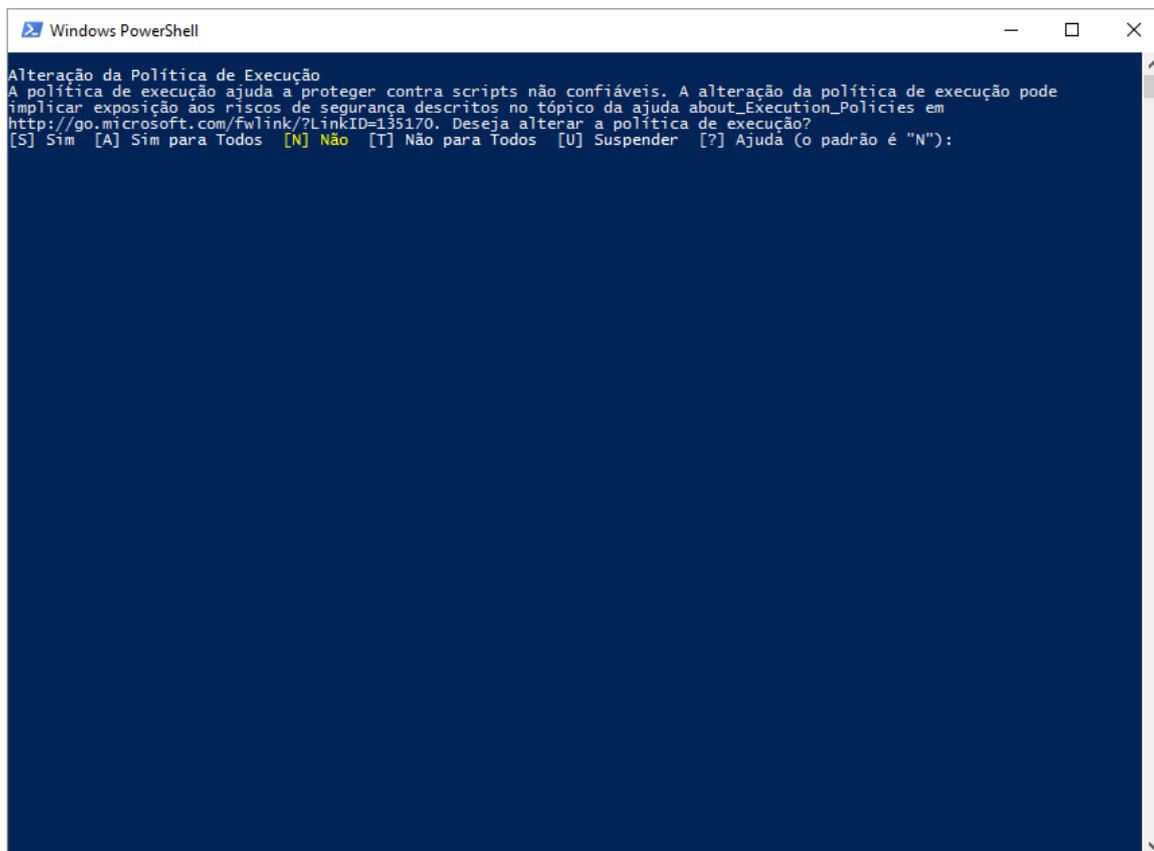
	<b>Configuração de Máquina de AR</b>			
		<b>Versão</b>	<b>Data</b>	<b>Página</b>
		1.9	01/06/2020	34 de 53

**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”

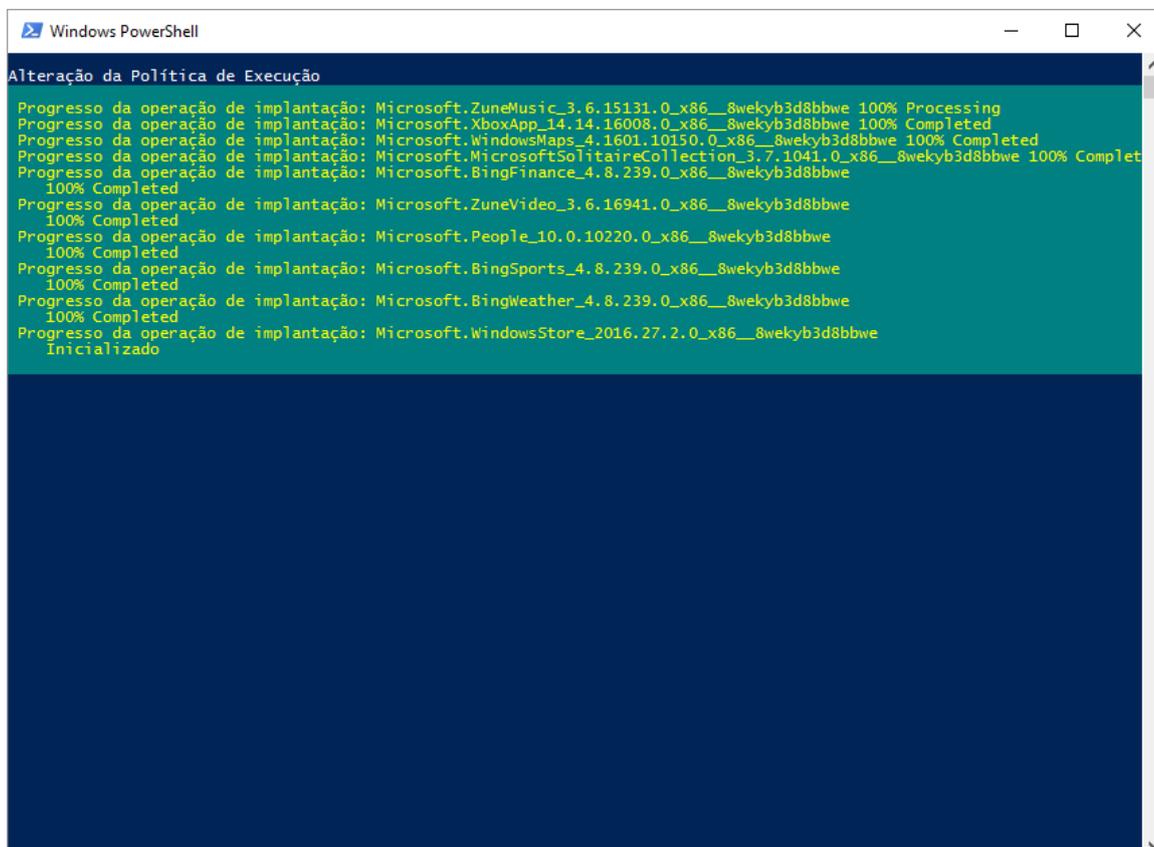


3. Aceitar a alteração via PowerShell, vide imagem abaixo.



```
Windows PowerShell

Alteração da Política de Execução
A política de execução ajuda a proteger contra scripts não confiáveis. A alteração da política de execução pode implicar exposição aos riscos de segurança descritos no tópico da ajuda about_Execution_Policies em http://go.microsoft.com/fwlink/?LinkID=135170. Deseja alterar a política de execução?
[S] Sim [A] Sim para Todos [N] Não [T] Não para Todos [U] Suspender [?] Ajuda (o padrão é "N"):
```



```
Windows PowerShell

Alteração da Política de Execução

Progresso da operação de implantação: Microsoft.ZuneMusic_3.6.15131.0_x86__8wekyb3d8bbwe 100% Processing
Progresso da operação de implantação: Microsoft.XboxApp_14.14.16008.0_x86__8wekyb3d8bbwe 100% Completed
Progresso da operação de implantação: Microsoft.WindowsMaps_4.1601.10150.0_x86__8wekyb3d8bbwe 100% Completed
Progresso da operação de implantação: Microsoft.MicrosoftSolitaireCollection_3.7.1041.0_x86__8wekyb3d8bbwe 100% Completed
Progresso da operação de implantação: Microsoft.BingFinance_4.8.239.0_x86__8wekyb3d8bbwe 100% Completed
Progresso da operação de implantação: Microsoft.ZuneVideo_3.6.16941.0_x86__8wekyb3d8bbwe 100% Completed
Progresso da operação de implantação: Microsoft.People_10.0.10220.0_x86__8wekyb3d8bbwe 100% Completed
Progresso da operação de implantação: Microsoft.BingSports_4.8.239.0_x86__8wekyb3d8bbwe 100% Completed
Progresso da operação de implantação: Microsoft.BingWeather_4.8.239.0_x86__8wekyb3d8bbwe 100% Completed
Progresso da operação de implantação: Microsoft.WindowsStore_2016.27.2.0_x86__8wekyb3d8bbwe 100% Completed
Inicializado
```

	<b>Configuração de Máquina de AR</b>			
		<b>Versão</b>	<b>Data</b>	<b>Página</b>
		1.9	01/06/2020	36 de 53

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).

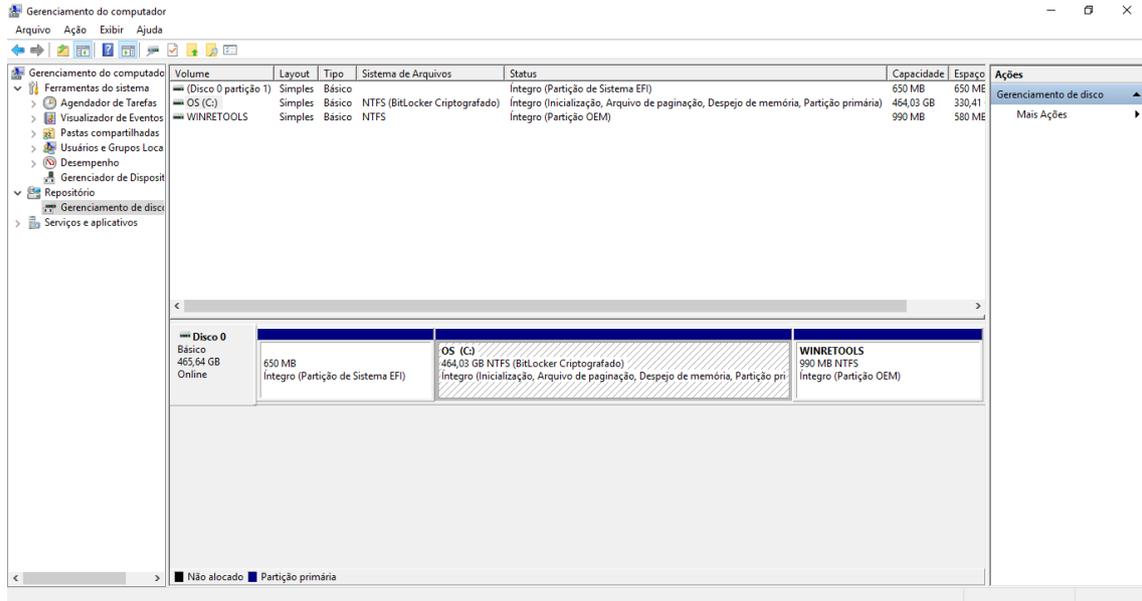
	<b>Configuração de Máquina de AR</b>			
		<b>Versão</b>	<b>Data</b>	<b>Página</b>
		1.9	01/06/2020	37 de 53

### Procedimento 13

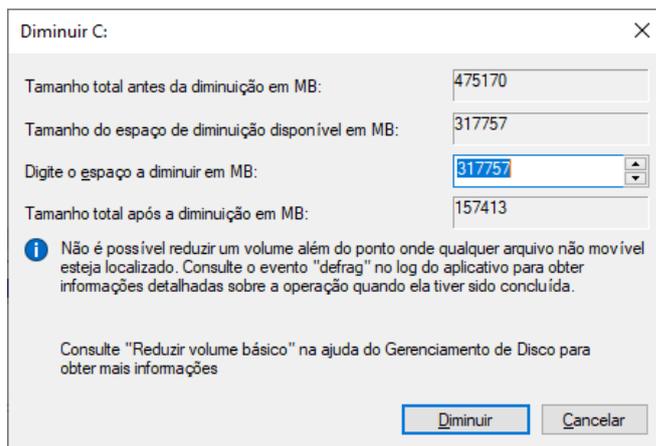
#### Procedimento para ativação da ferramenta de criptografia VeraCrypt.

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.

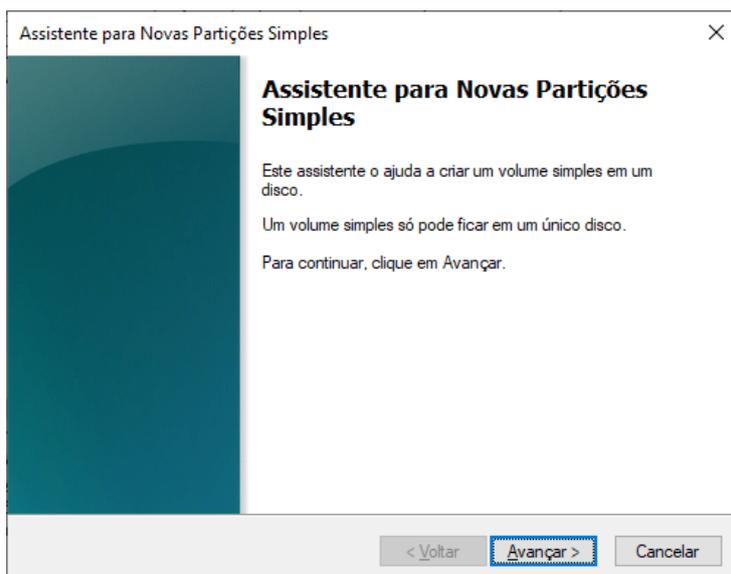


Após isso, clique com o botão direito na partição onde quer criar e clique em "Diminuir Volume". Após isso, é necessário definir o tamanho da partição. Este tamanho precisa ser definido pelo gestor técnico, de acordo com o tamanho do disco.

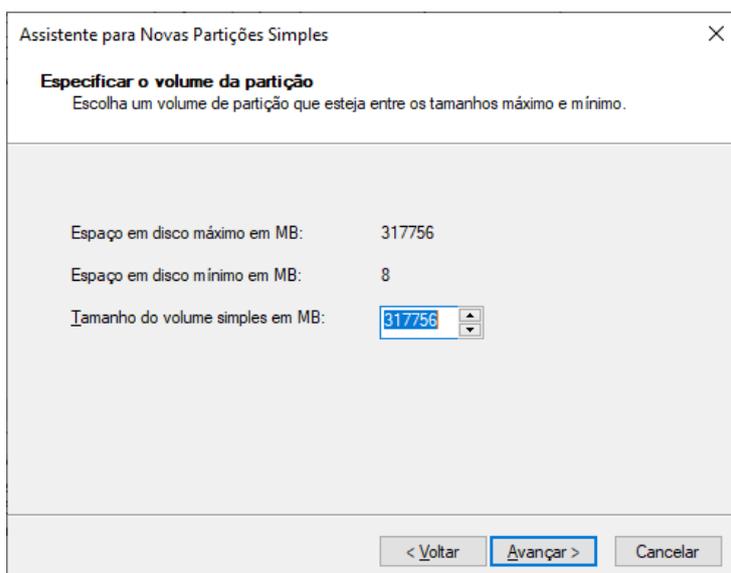


Após isto, clique com o botão direito na partição criada e depois clique em "Novo volume simples".

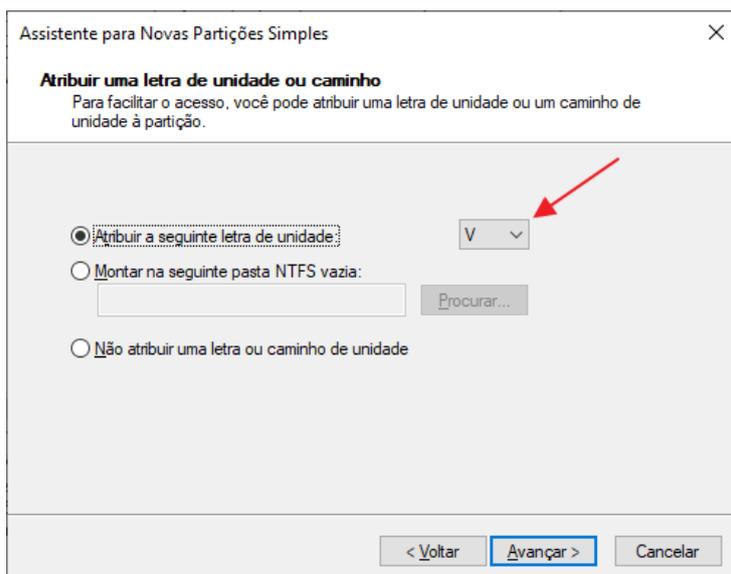
Após isto, clique em "Avançar".



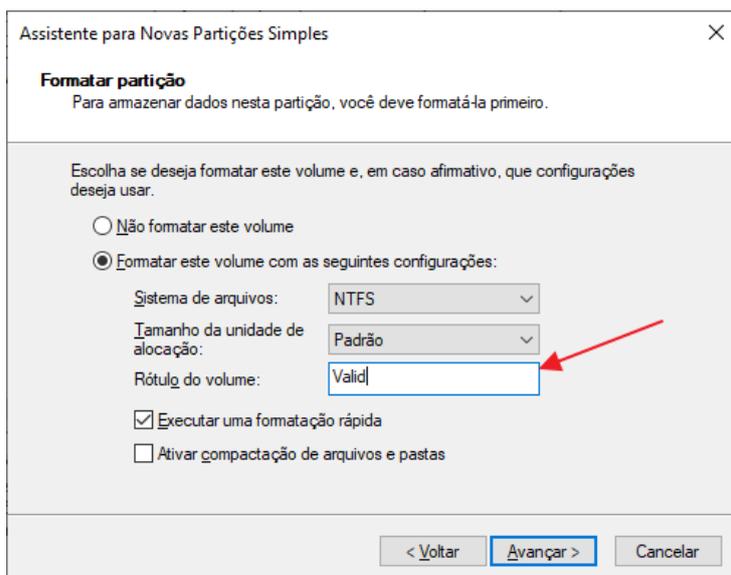
Clique em avançar para definir o tamanho da partição.



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).



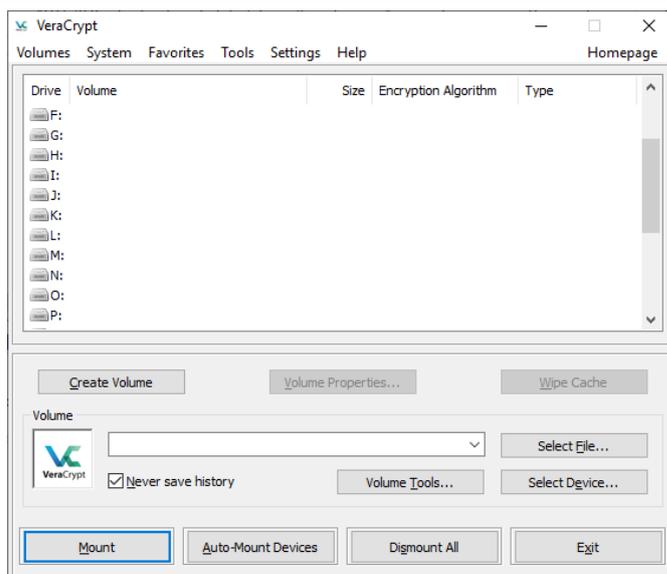
Clique em “Concluir” para terminar esta etapa.

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

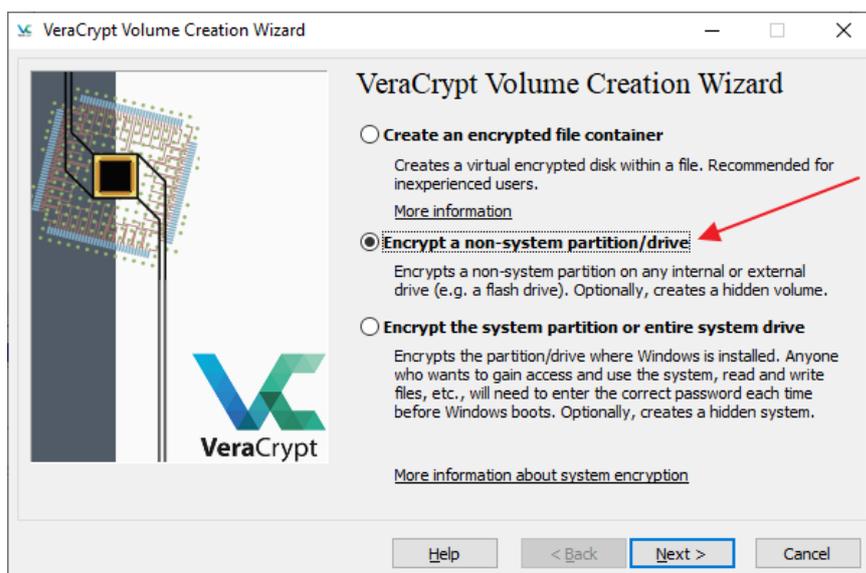
Após instalar o programa, deve-se criar um volume, selecionar seu local de destino, o tipo de algoritmo criptográfico que será utilizado e seu tamanho. Após isso, o usuário deve escolher uma senha e criar uma cópia para segurança.

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.

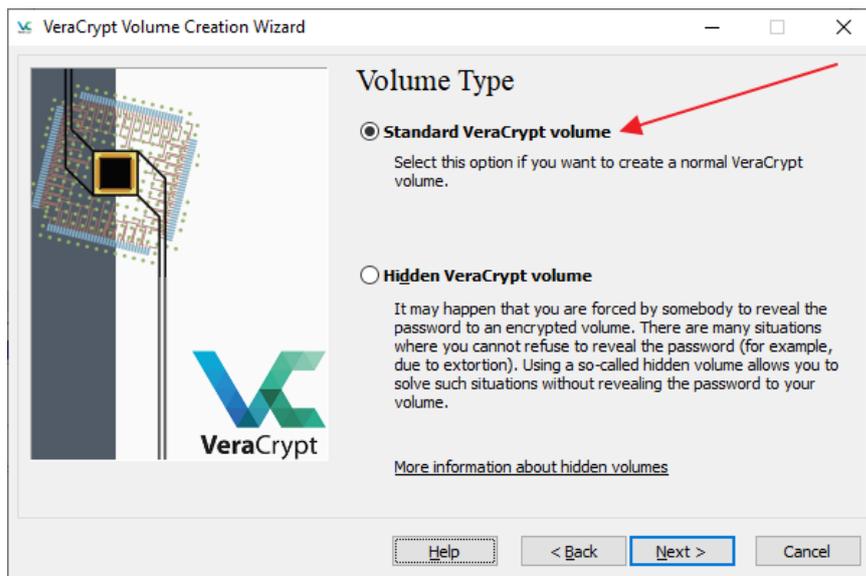
Abra o aplicativo e clique em “Create Volume”.



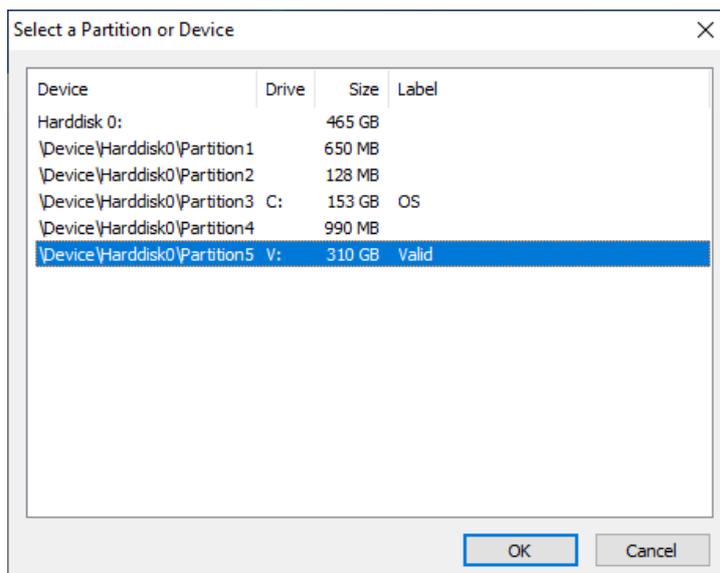
Selecione a opção "Encrypt a non-system partition/drive".



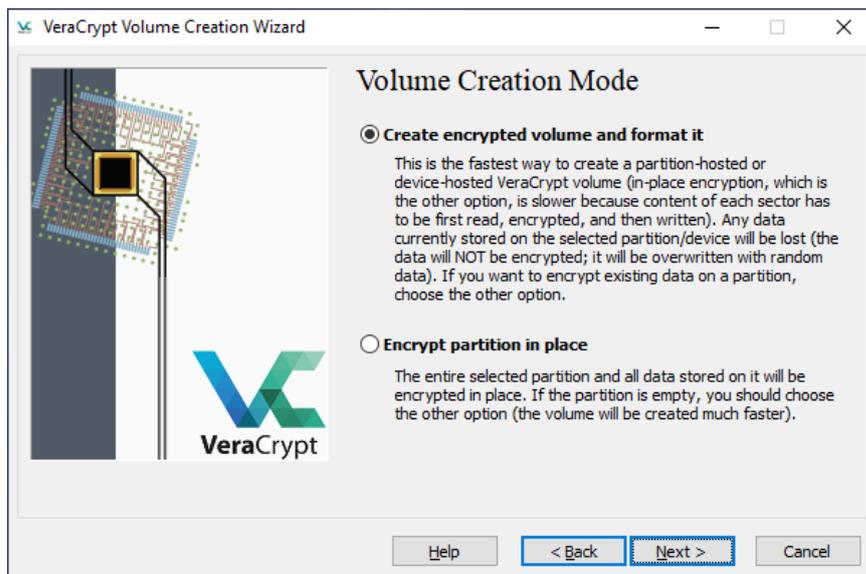
Clique em "Standard Veracrypt Volume".



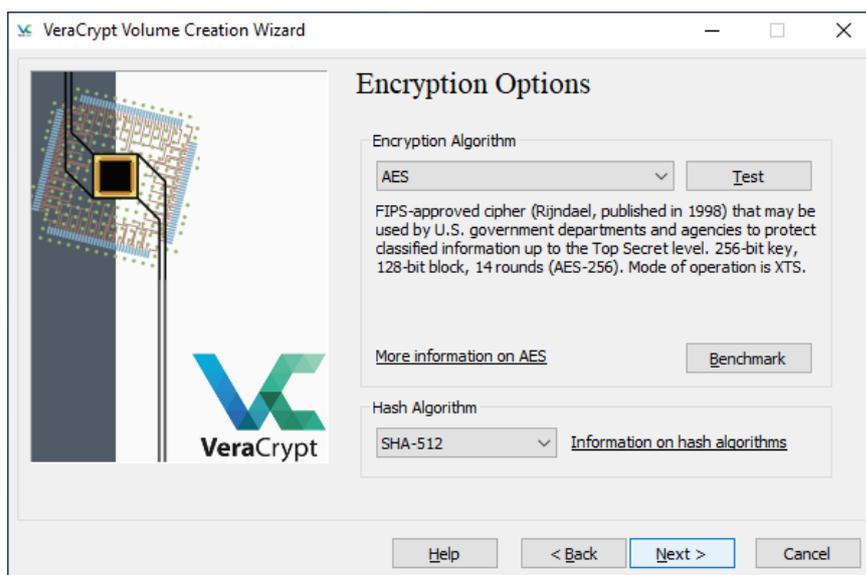
Clique em "Select Device" e seleciona a partição criada para os dados.



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



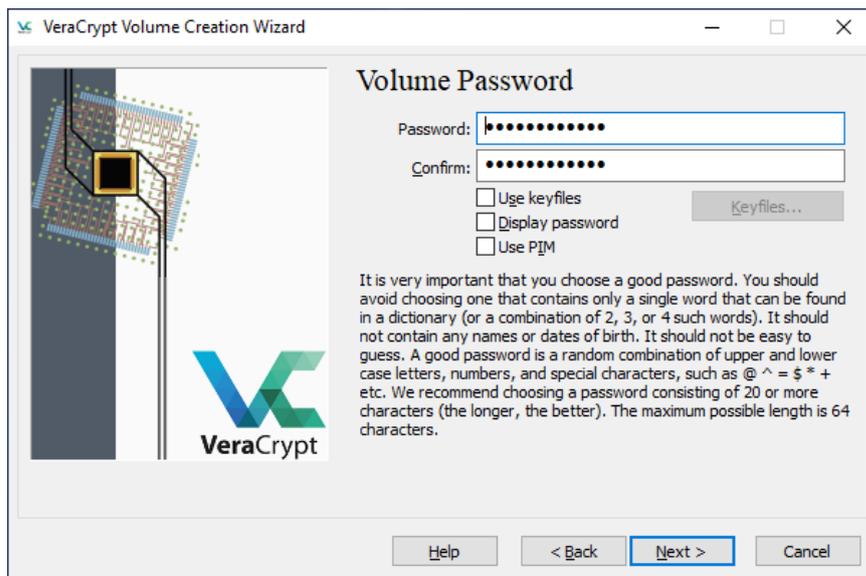
Clique em "Next" para utilizar as definições padrão.



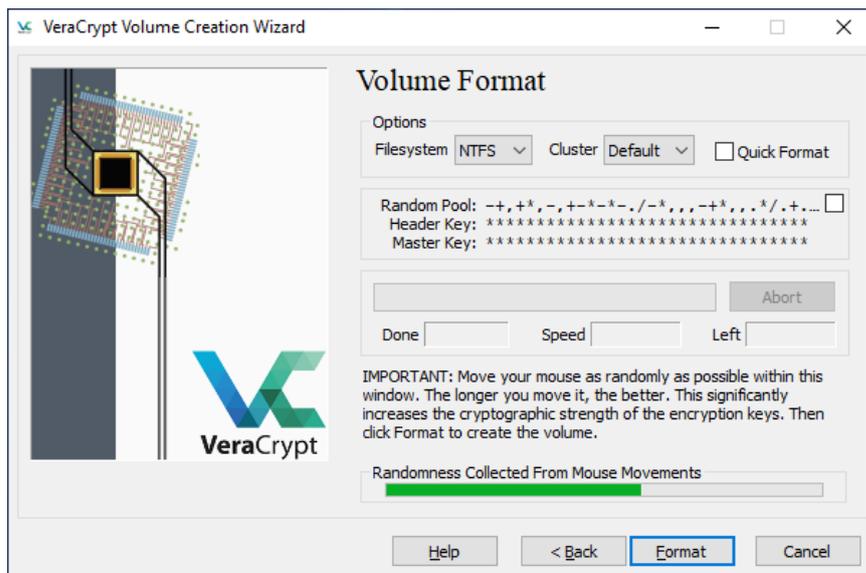
Clique em "Next" novamente para continuar com a encriptação.

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.**

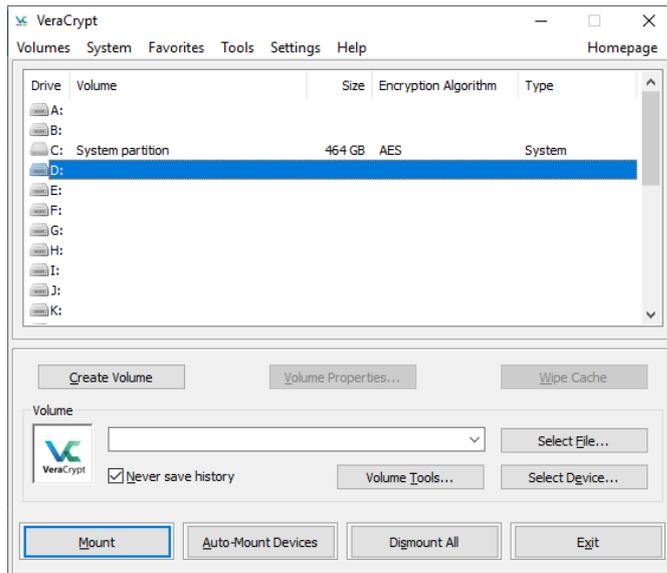


Selecione a opção "NO", para não permitir arquivos maiores que 4GB. A etapa a seguir é a criação da chave, necessário fazer movimentos aleatórios com o mouse para coletar informações para a criptografia, faça movimentos até a barra ficar na cor verde, clique em "Format" para concluir.

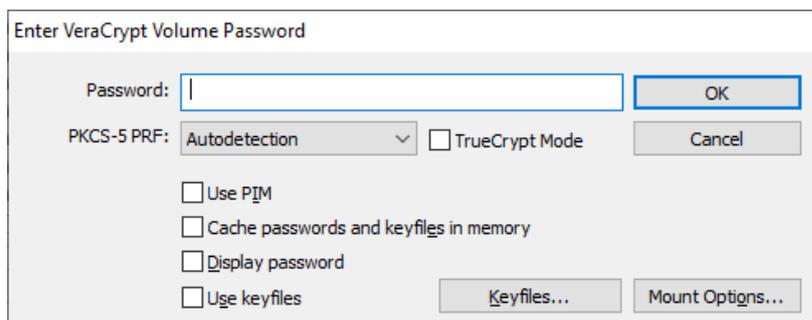


Esta etapa é para concluir o acesso da criptografia. É importante fazer este procedimento todas as vezes para acessar a partição.

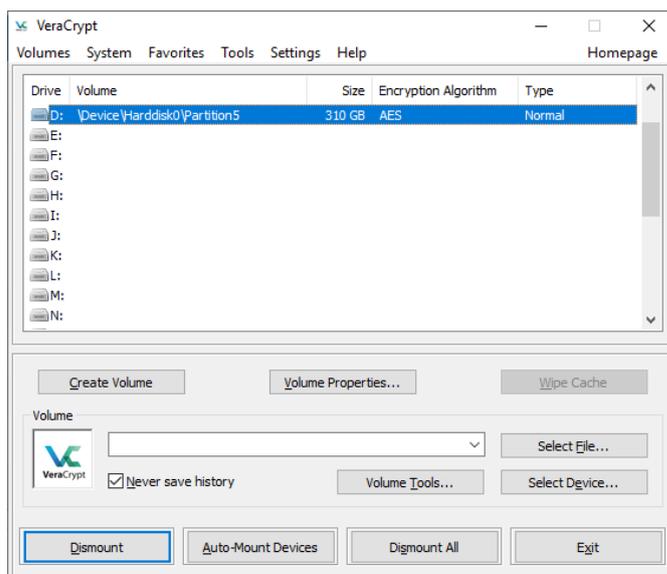
Após concluir, clique em "Next" e feche a janela. Com o programa inicial selecione uma letra e clique em "Auto-Mount-Devices".



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.

## Pastas (7)



## Dispositivos e unidades (4)



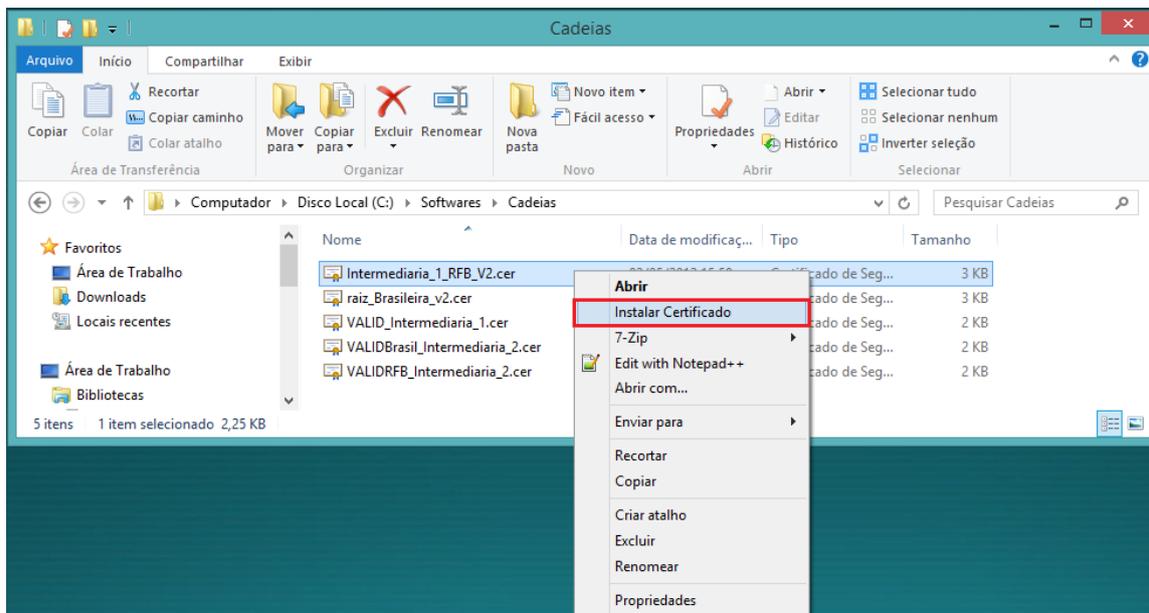
	<b>Configuração de Máquina de AR</b>		
		1.9	01/06/2020

## Procedimento 14

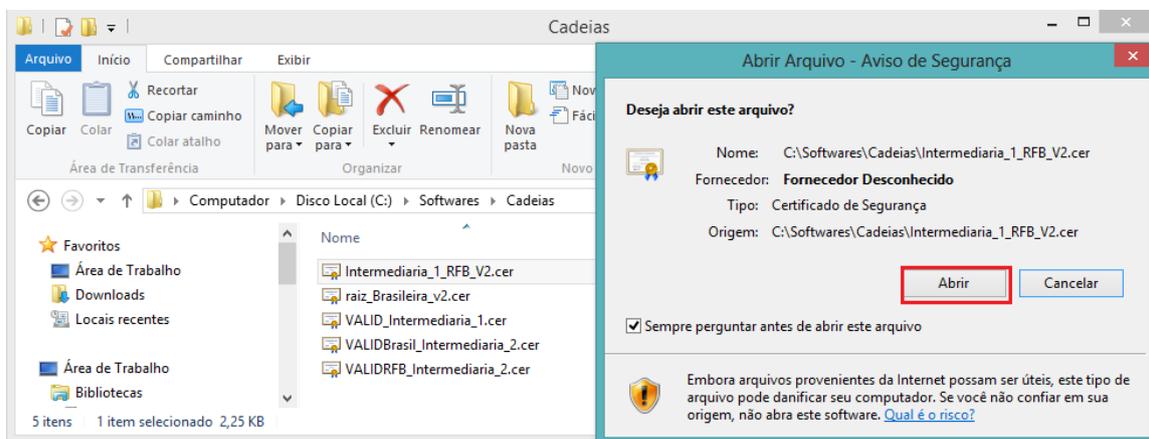
### Procedimento para instalação das cadeias.

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

Instalar Certificado:



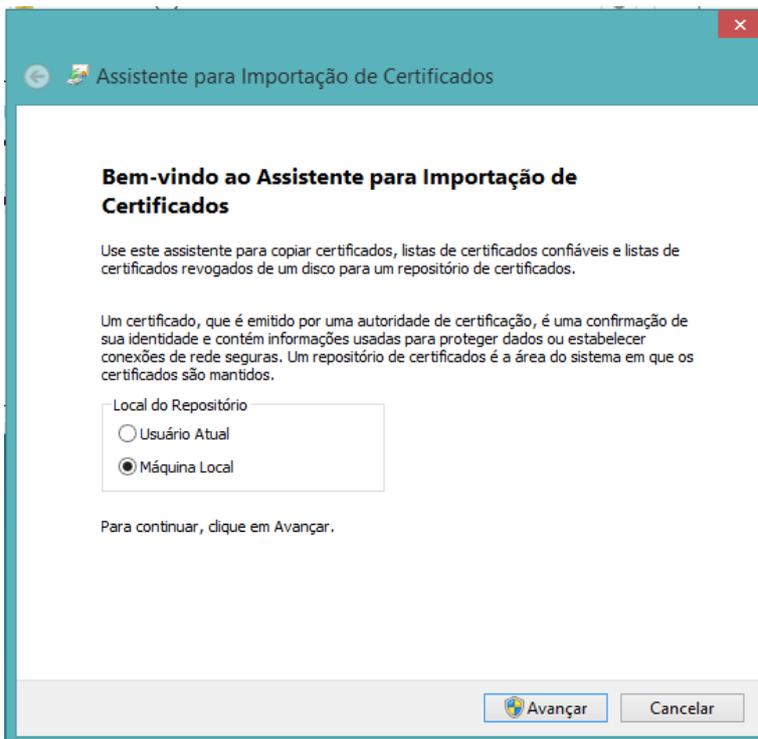
3. Clicar em Abrir:



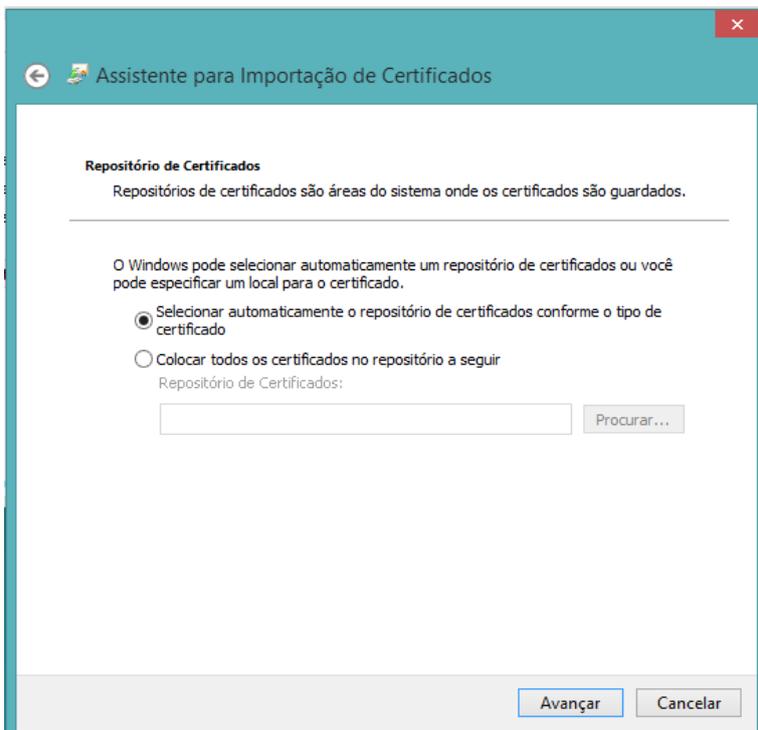
*Este documento é de propriedade da Valid Certificadora e elaborado especialmente para servir de instrumento de apoio aos procedimentos da Estrutura de Certificação Digital, não podendo ser reproduzido nem comunicado, transmitido ou de qualquer forma ter seu conteúdo informado, total ou parcialmente, a pessoas estranhas às negociações com a Valid Certificadora.*

	<b>Configuração de Máquina de AR</b>			
		<b>Versão</b>	<b>Data</b>	<b>Página</b>
		1.9	01/06/2020	47 de 53

4. Clicar em Avançar:

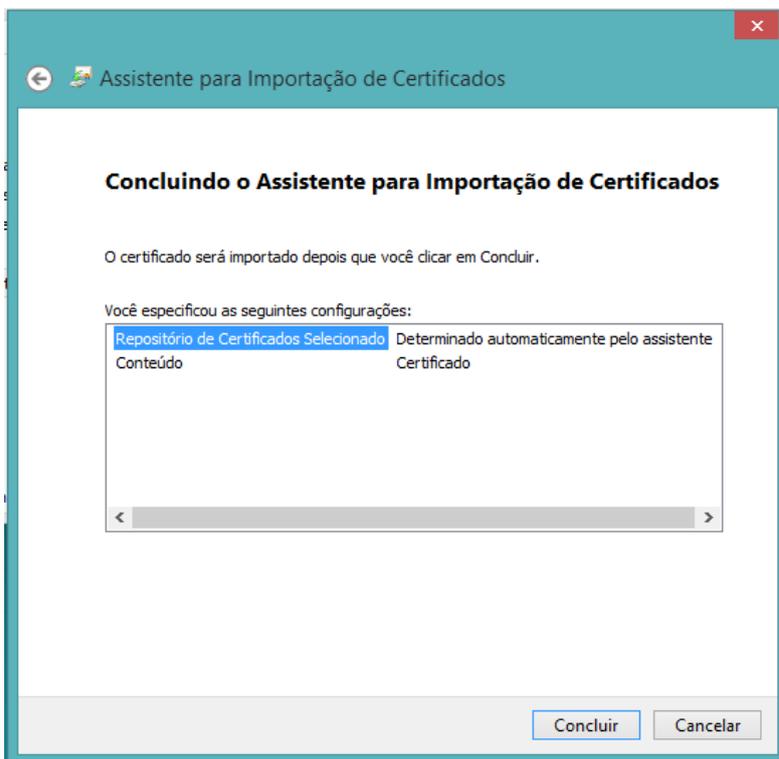


5. Clicar em Avançar novamente:

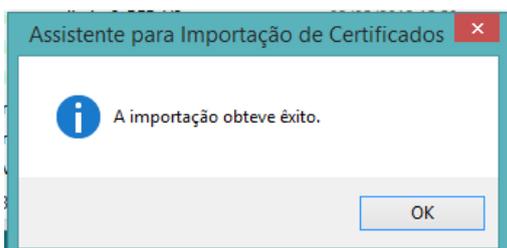


	<b>Configuração de Máquina de AR</b>			
		<b>Versão</b>	<b>Data</b>	<b>Página</b>
		1.9	01/06/2020	48 de 53

6. Clicar em Concluir:



7. Clicar em OK.



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

	<b>Configuração de Máquina de AR</b>			
		<b>Versão</b>	<b>Data</b>	<b>Página</b>
		1.9	01/06/2020	49 de 53

### **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>

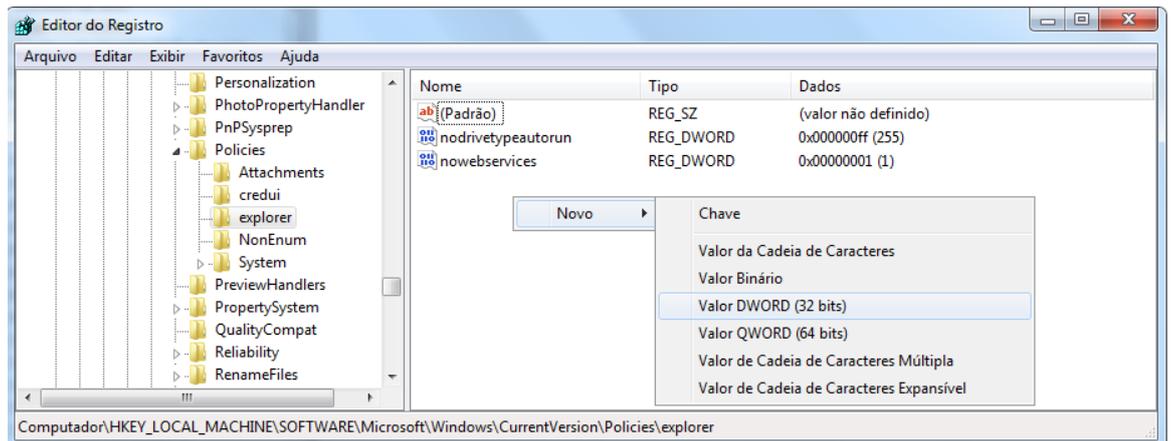
Importante: Após a instalação é criado uma pasta do vc-ivs-bio dentro do perfil do usuário logado (%userprofile%\AppData\Local\vc-ivs-bio\).

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

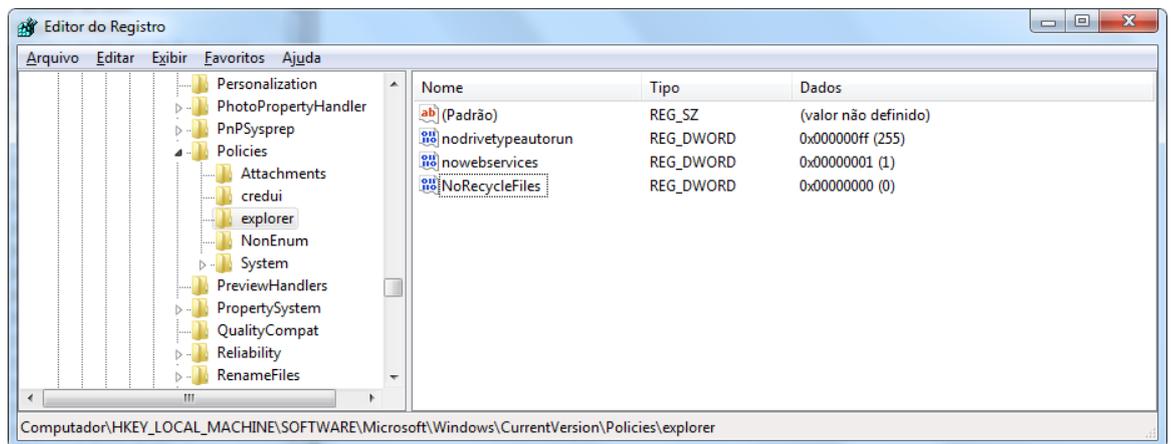
### Procedimento 16 – Windows 7

Não mover arquivos excluídos para lixeira.

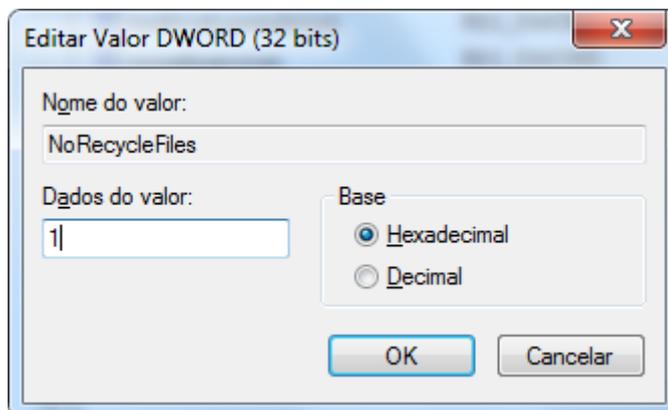
1. Iniciar -> Pesquisar “regedit”.
2. Selecione: HKEY\_LOCAL\_MACHINE -> SOFTWARES -> Microsoft -> CurrentVersion -> Policies -> Explorer.
3. Novo -> Valor DWORD (32 bits).



4. Preencher com o nome: NoRecycleFiles.



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

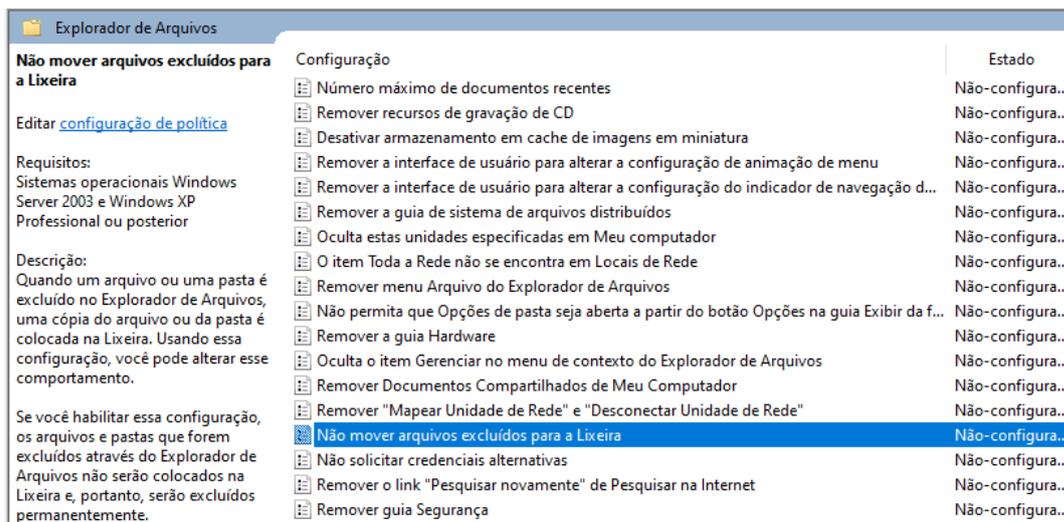


	<b>Configuração de Máquina de AR</b>			
		<b>Versão</b>	<b>Data</b>	<b>Página</b>
		1.9	01/06/2020	51 de 53

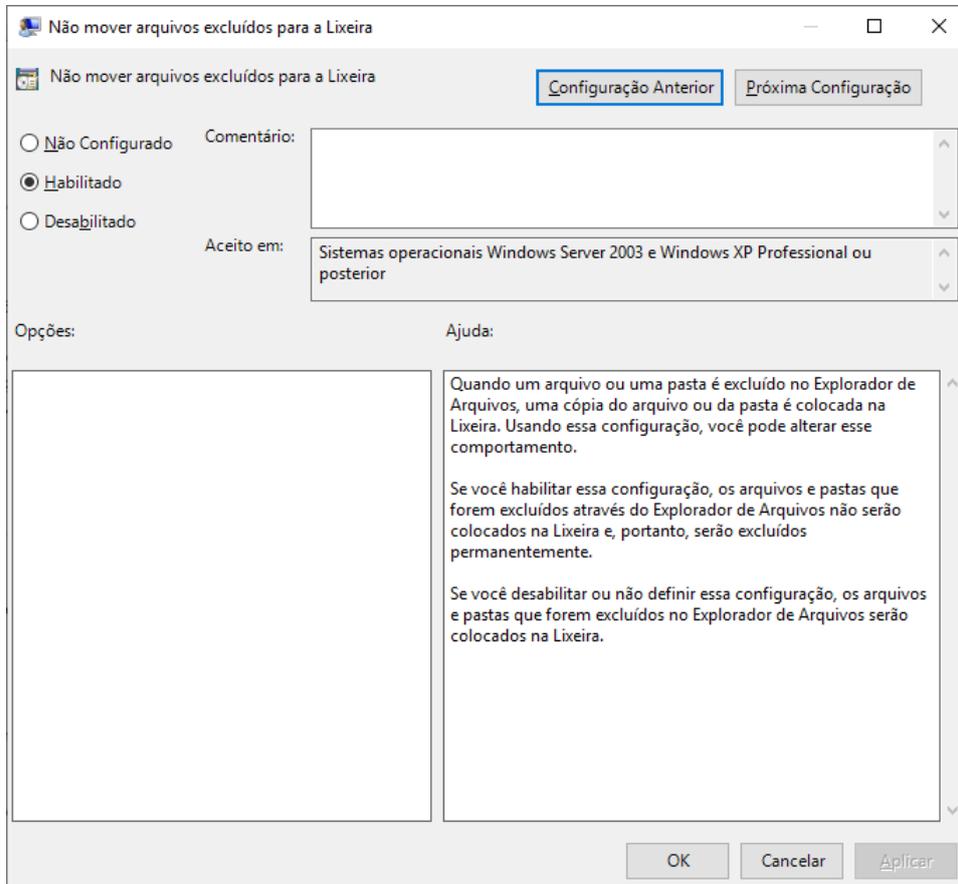
## Procedimento 16 – Windows 10

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*”.



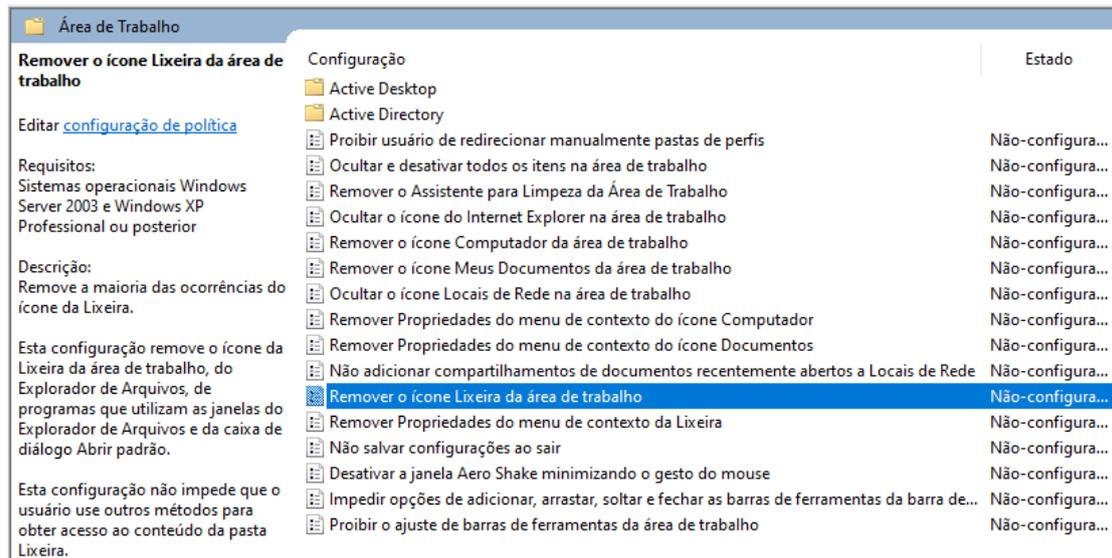
The screenshot shows the Windows Explorer interface with the 'Configuração' (Configuration) pane open. The policy 'Não mover arquivos excluídos para a Lixeira' is selected and highlighted in blue. The 'Estado' (Status) column shows 'Não-configura...' for this policy. The left pane shows the policy name and a link to edit the configuration. The right pane lists various configuration options, with the selected policy being the one to be configured.



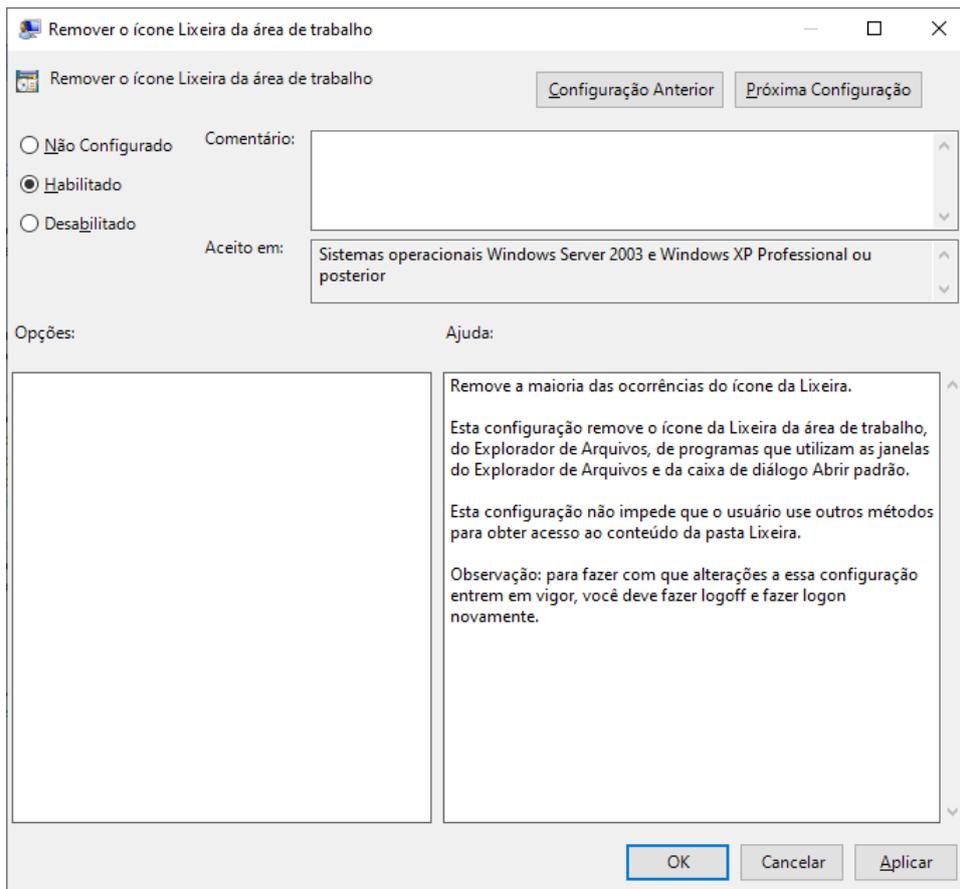
The screenshot shows the configuration dialog box for the policy 'Não mover arquivos excluídos para a Lixeira'. The dialog has a title bar with the policy name and standard window controls. Below the title bar, there are buttons for 'Configuração Anterior' and 'Próxima Configuração'. The main area contains three radio buttons: 'Não Configurado', 'Habilitado' (which is selected), and 'Desabilitado'. To the right of these buttons is a 'Comentário:' text box. Below the radio buttons is an 'Aceito em:' dropdown menu showing 'Sistemas operacionais Windows Server 2003 e Windows XP Profissional ou posterior'. At the bottom, there are 'Opções:' and 'Ajuda:' sections. The 'Ajuda:' section contains text explaining the policy's behavior: 'Quando um arquivo ou uma pasta é excluído no Explorador de Arquivos, uma cópia do arquivo ou da pasta é colocada na Lixeira. Usando essa configuração, você pode alterar esse comportamento. Se você habilitar essa configuração, os arquivos e pastas que forem excluídos através do Explorador de Arquivos não serão colocados na Lixeira e, portanto, serão excluídos permanentemente. Se você desabilitar ou não definir essa configuração, os arquivos e pastas que forem excluídos no Explorador de Arquivos serão colocados na Lixeira.' At the bottom right, there are 'OK', 'Cancelar', and 'Aplicar' buttons.

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.”**.



The screenshot shows the Windows Group Policy Editor window for the 'Área de Trabalho' (Desktop) folder. The policy 'Remover o ícone Lixeira da área de trabalho' is selected and highlighted in blue. The policy status is 'Não-configurad...' (Not configured). The left pane shows the policy name and a link to 'Editar configuração de política'. The right pane shows a list of other policies, all with a status of 'Não-configurad...'.



The screenshot shows the configuration dialog box for the 'Remover o ícone Lixeira da área de trabalho' policy. The dialog has a title bar with the policy name and standard window controls. It contains the following elements:

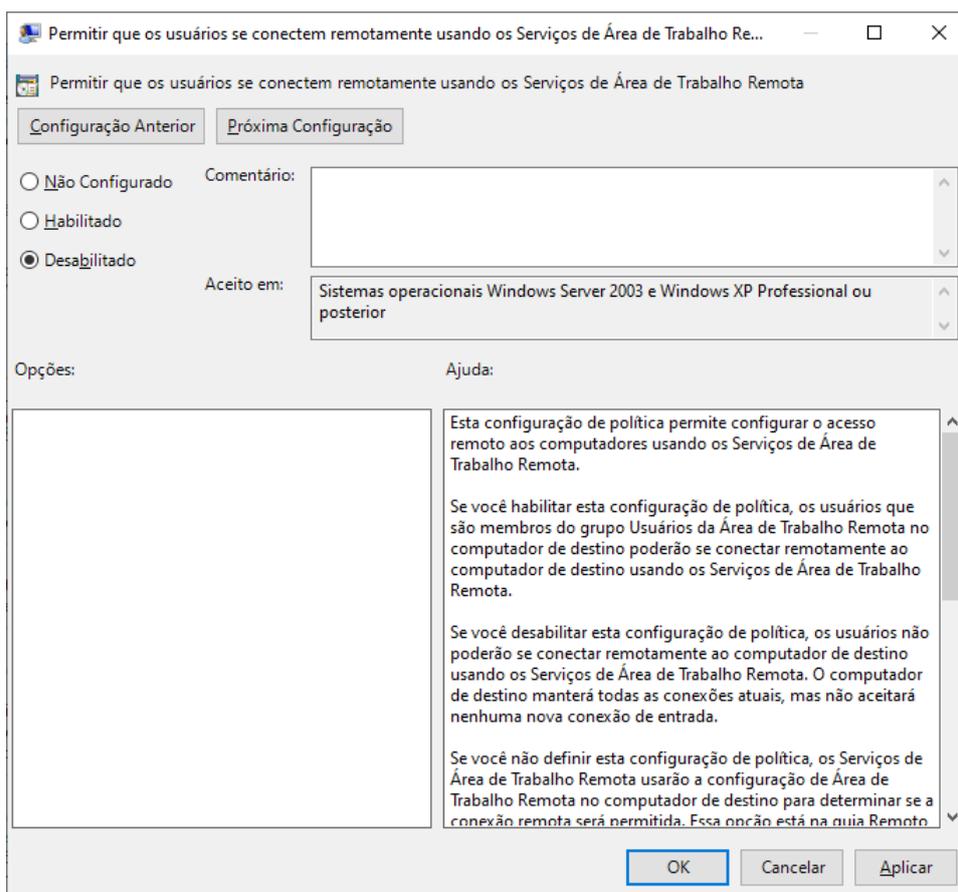
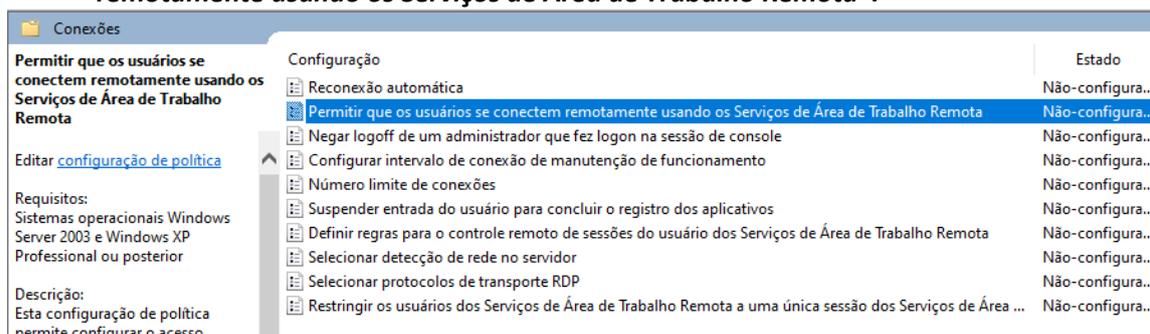
- Buttons for 'Configuração Anterior' and 'Próxima Configuração'.
- Radio buttons for 'Não Configurado', 'Habilitado' (selected), and 'Desabilitado'.
- A 'Comentário:' text box.
- An 'Aceito em:' dropdown menu showing 'Sistemas operacionais Windows Server 2003 e Windows XP Professional ou posterior'.
- 'Opções:' and 'Ajuda:' sections, both currently empty.
- 'OK', 'Cancelar', and 'Aplicar' buttons at the bottom.

	<b>Configuração de Máquina de AR</b>			
		<b>Versão</b>	<b>Data</b>	<b>Página</b>
		1.9	01/06/2020	53 de 53

## 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”**.



**VALID Certificadora Digital**

Classificação: **RESTRITO**

Para maiores informações acesse

[www.validcertificadora.com.br](http://www.validcertificadora.com.br)

Junho de 2020

*Este documento é de propriedade da Valid Certificadora e elaborado especialmente para servir de instrumento de apoio aos procedimentos da Estrutura de Certificação Digital, não podendo ser reproduzido nem comunicado, transmitido ou de qualquer forma ter seu conteúdo informado, total ou parcialmente, a pessoas estranhas às negociações com a Valid Certificadora.*