idserpro.gov.br

Manual de Configuração

Diretivas de Segurança para Estações AR Vinculadas

Serviço: Certificação Digital

Cliente: AR IDFEDERAL

Versão 1.0

Superintendência de Serviços e Produtos – Operações (SUPOP)

Histórico de Versões

Versão	Data	Autor/Revisor	Alterações da Versão
1.0	02/03/20	Francisca Juscivania Mendes Janine Silva da Costa Maria Lilian Santos da Costa Sueli Pinheiro Vila Real	– Versão inicial.

Resumo do Documento

Descrição:	Este documento apresenta as configurações de segurança para estações de trabalho AR vinculadas se adequarem às recomendações do ITI.
Local de Publicação:	http://rit.documenta.serpro
Validade da Versão:	02/03/21
Modelo de Publicação Versão 3.0	

Sumário

1. Introdução

Este documento tem por objetivo orientar os procedimentos mínimos de segurança da estação de trabalho a serem adotados pelas Autoridades de Registro – AR Vinculadas ao SERPRO, de forma a atender aos requisitos apresentados pelo ITI através do documento DOC-ICP-03.01 – Versão 3.1.

1.1. Premissas

A estação de trabalho do AR:

- deve possuir sistema operacional Windows 10 Professional ou superior;
- deve estar atualizada com todas as atualizações de segurança necessárias;
- deve estar com o antivírus instalado e configurado para ser atualizado automaticamente.

2. Procedimentos de segurança para estações AR

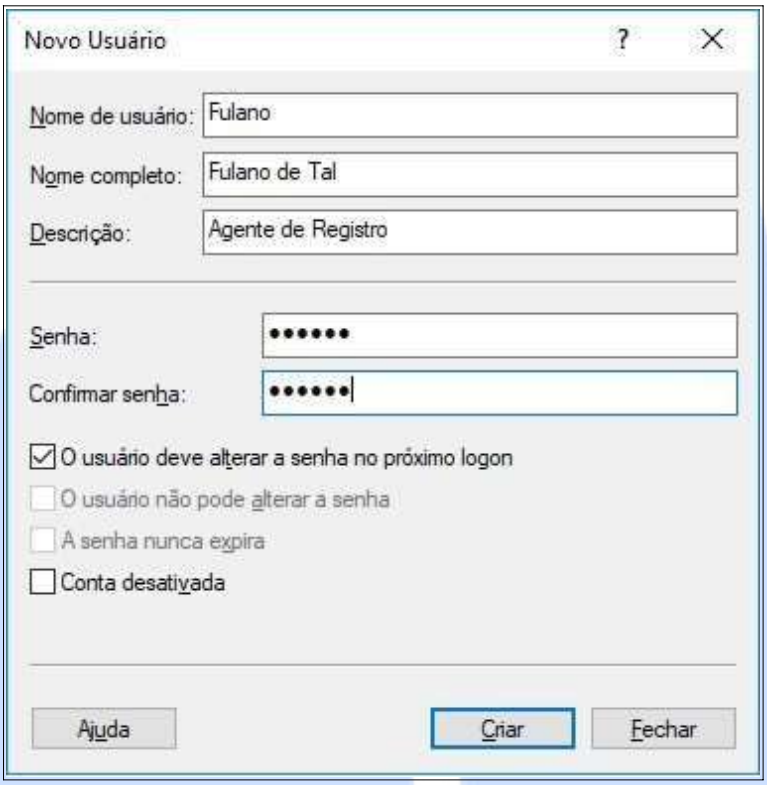
Este tópico descreve as configurações que deverão ser aplicadas às estações de trabalho das AR's parceiras do SERPRO para atender aos requisitos de segurança recomendados pelo ITI.

2.1. Controle de Acesso Lógico ao Sistema Operacional

Devem ser configurados os controles de acesso conforme orientações a seguir.

- Renomear a conta do usuário local "Administrador" das estações.
- Definir que apenas o usuário local Administrador (renomeado) pertença ao grupo de Administradores.
  - Clique com o botão direito sobre "Meu Computador" e em seguida "Gerenciar". Acesse a opção "Usuários e Grupos Locais", clique na pasta "Grupos" e em seguida clique com botão direito sobre "Administradores". Caso sejam exibidos outros usuários além do Administrador (renomeado) os mesmos devem ser removidos.
- Desativar a conta do usuário local "Convidado" das estações.
  - Clique com o botão direito sobre "Meu Computador" e em seguida "Gerenciar". Acesse opção "Usuários e Grupos Locais", clique na pasta "Usuários" e em seguida clique com botão direito sobre "Convidado" e "Propriedades". Marque somente "Conta desativada" e clique OK, conforme a tela a seguir.
- Definir conta para cada Agente de Registro.
  - Clique com o botão direito sobre "Meu Computador" e em seguida "Gerenciar". Acesse a opção "Usuários e Grupos Locais", clique com botão direito sobre "Usuários" e depois em "Novo Usuário". Preencha as informações, defina uma

senha, marque "O usuário deve alterar a senha no próximo logon" e depois clique em "Criar" conforme tela a seguir.



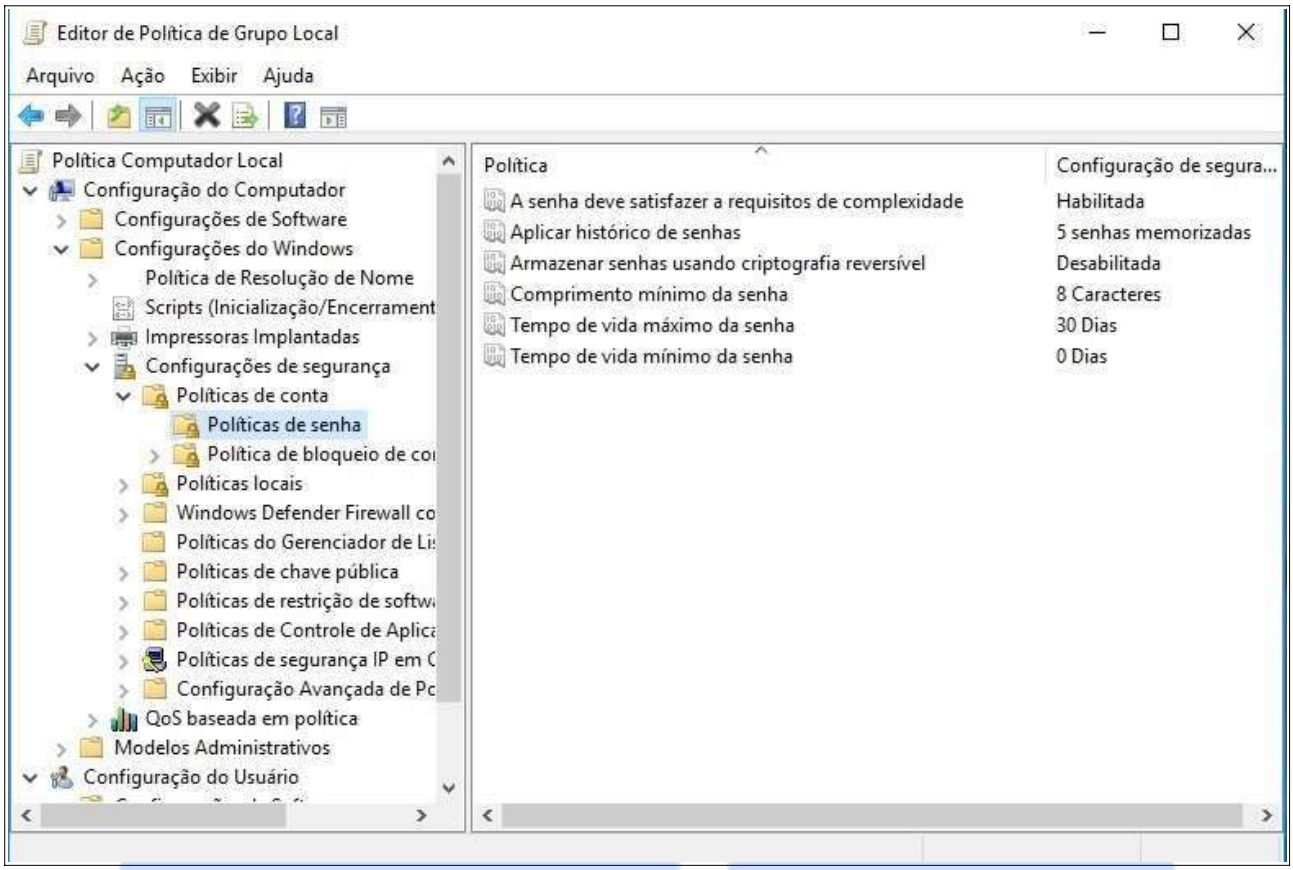
2.2. Diretivas de Senha e de Bloqueio de Conta

2.2.1. Exigência de uso de senhas fortes

Devem ser configurados os parâmetros de Diretivas de Senha conforme orientações abaixo.

- Definir que as senhas dos usuários do domínio devem satisfazer a requisitos de complexidade.
- Definir que as últimas 5 senhas utilizadas pelos usuários não poderão ser novamente utilizadas.
- Desativar o armazenamento de senhas usando criptografia reversível.
- Definir para 8 caracteres o comprimento mínimo de uma senha.
- Definir para 30 dias o tempo de vida máximo de uma senha.
- Definir para 0 (zero) dias o tempo de vida mínimo de uma senha.
  - No menu Iniciar do Windows digite "**gpedit**" e abra "Editar Política de Grupo" (Painel de Controle). Na janela aberta clique em "Configuração do Computador", depois em "Configurações do Windows" e "Configurações de segurança". Clique 2xem "Políticas de conta" e após clique em "Políticas de senha", onde devem ser

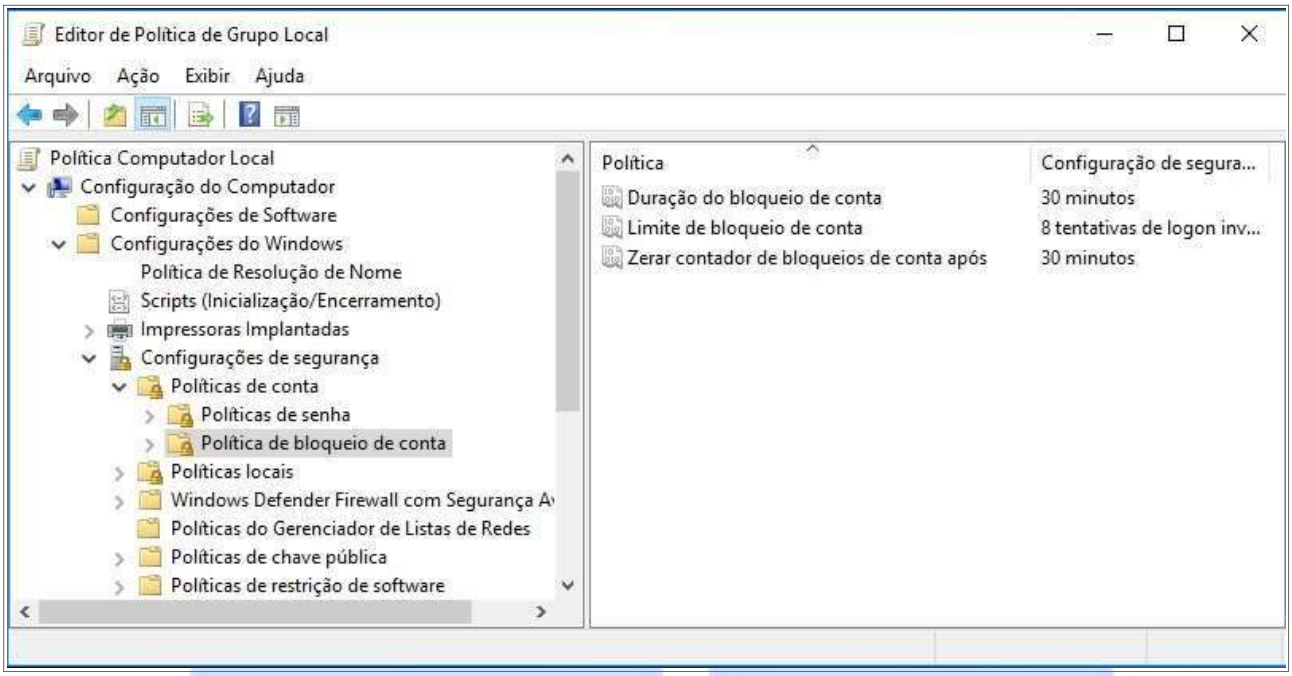
definidos os parâmetros conforme tela abaixo.



2.2.2. Diretivas de Bloqueio de conta

Devem ser configurados os parâmetros de Diretivas de Bloqueio de conta conforme orientações abaixo.

- Definir que uma conta bloqueada poderá ser desbloqueada após 30 minutos.
- Definir que uma conta será bloqueada após 8 tentativas de logon inválidas.
- Definir que o contador de bloqueio de contas será zerado a cada 30 minutos.
    - No menu Iniciar do Windows digite **"gpedit"** e abra "Editar Política de Grupo" (Painel de Controle). Na janela aberta clique em "Configuração do Computador", depois em "Configurações do Windows" e "Configurações de segurança". Clique 2xem "Políticas de conta" e após clique em "Política de bloqueio de conta", onde devem ser definidos os parâmetros conforme tela a seguir.



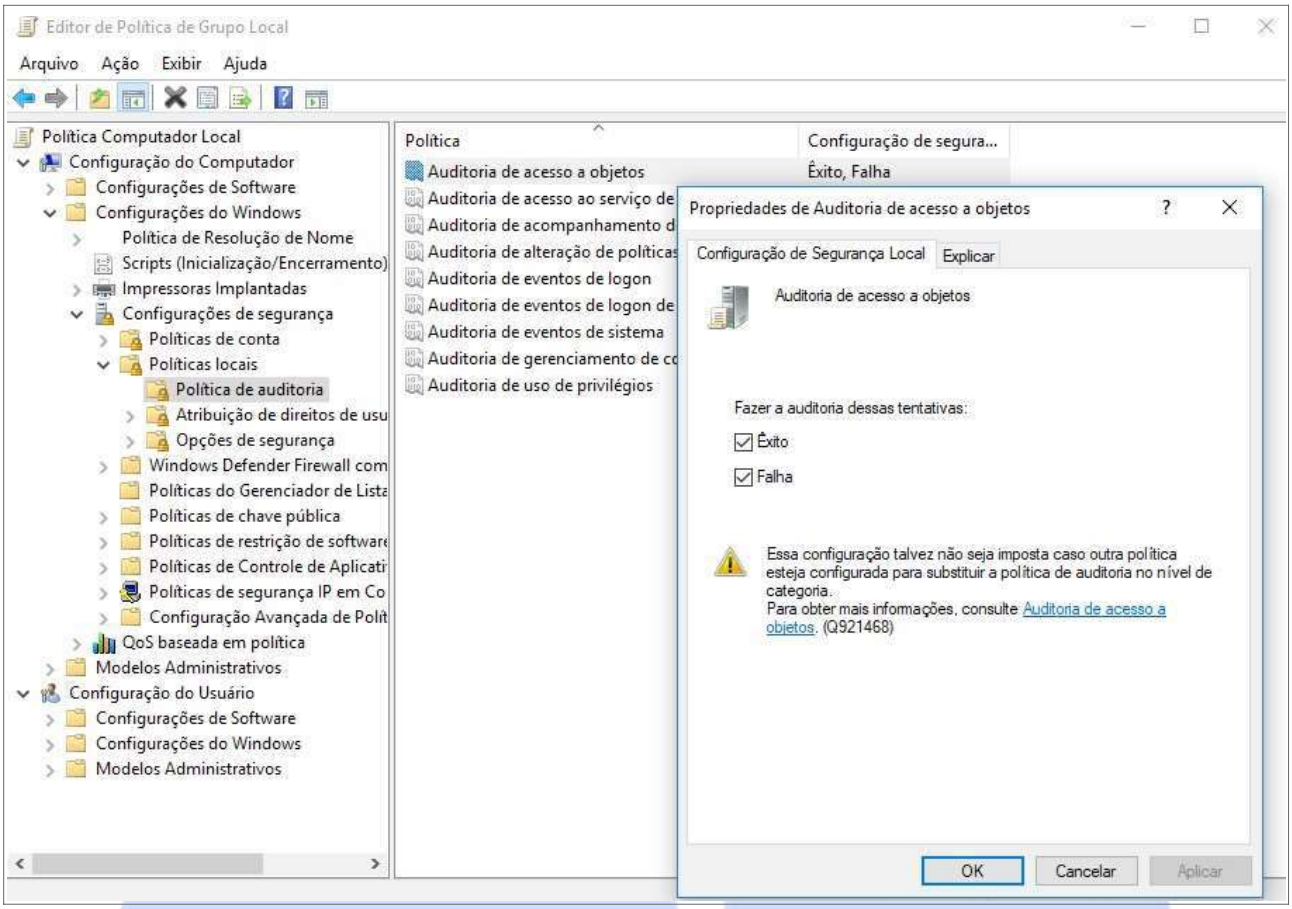
2.3. Logs de auditoria do sistema operacional

Devem ser configuradas as auditorias de eventos de sucesso ou falha relacionados ao acesso a objetos, alteração de diretivas, logon de conta de auditoria, eventos de logon, gerenciamento de contas e uso de privilégios.

- No menu Iniciar do Windows digite **"gpedit"** e abra "Editar Política de Grupo" (Painel de Controle). Em seguida acesse "Configuração do Computador", clique em "Configurações do Windows" e depois em "Configurações de segurança". Clique em "Políticas locais" e abaixo clique 2x para abrir "Política de auditoria".

- Clique 2x em "Auditoria de acesso a objetos", e em "Fazer a auditoria dessas tentativas" marque "Êxito" e "Falha" e depois clique em "Aplicar" conforme tela a seguir.

Repita esse procedimento para Auditoria de alteração de políticas, Auditoria de eventos de logon, Auditoria de eventos de logon de conta, Auditoria de gerenciamento de conta e Auditoria de uso de privilégios.



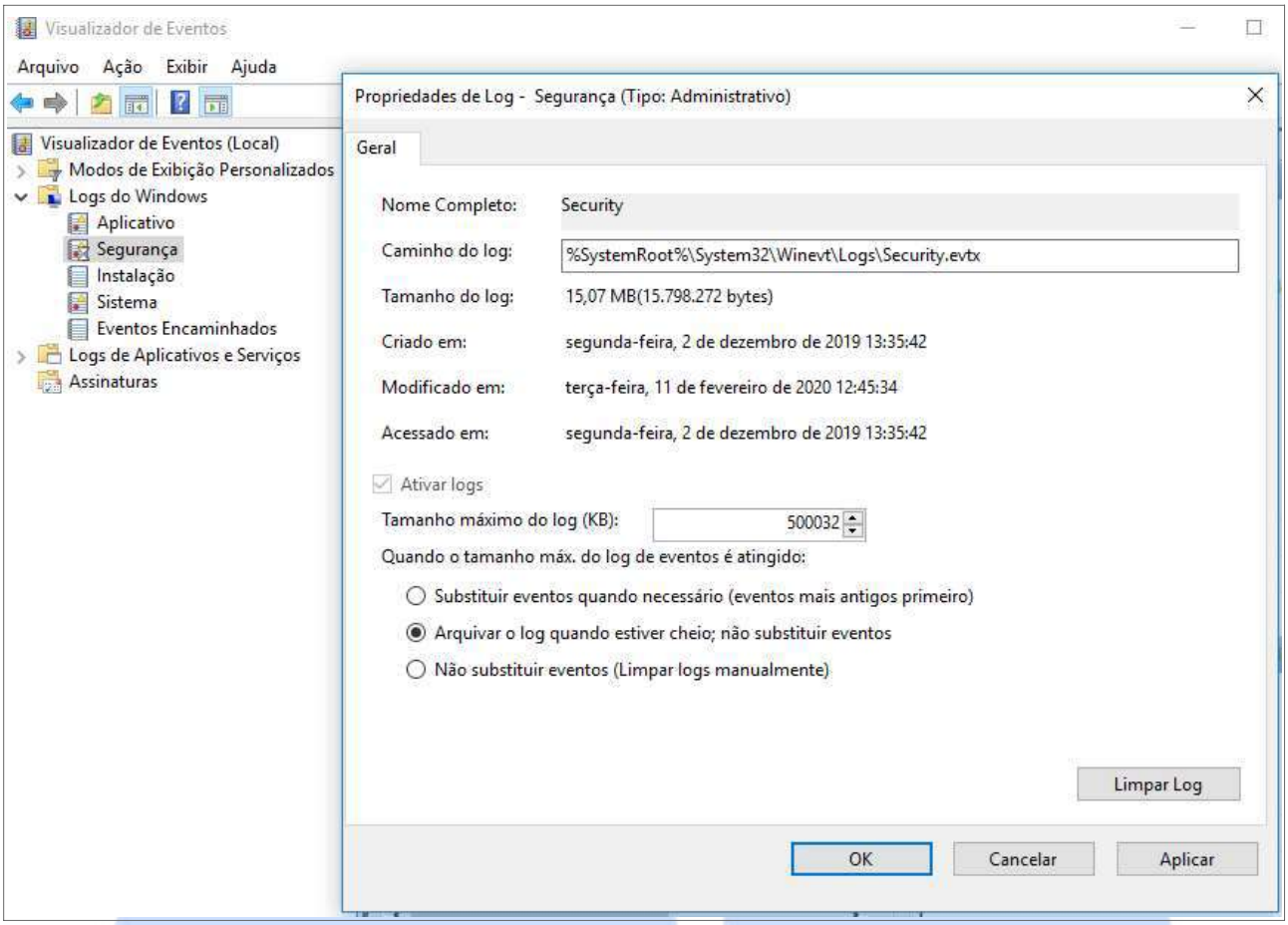
2.4. Armazenamento do log localmente por período mínimo de 60 dias

Deve ser configurada a retenção dos logs para 60 dias, e definido o tamanho máximo do log Segurança para 500 MB e do log de Aplicativo e Sistema para 50MB cada.

- No menu Iniciar do Windows digite **"event"** e abra "Visualizador de Eventos" (Aplicativo). Em seguida clique 2x em "Logs do Windows", clique com botão direito em "Segurança" e selecione "Propriedades".

- Na janela aberta configure o tamanho máximo do log (KB) para 500.000KB e marque a opção "Arquivar o log quando estiver cheio", clique em "Aplicar" conforme tela a seguir.

Repita esse procedimento para Aplicativo e para Sistema, definindo o tamanho máximo do log para 50.000KB.



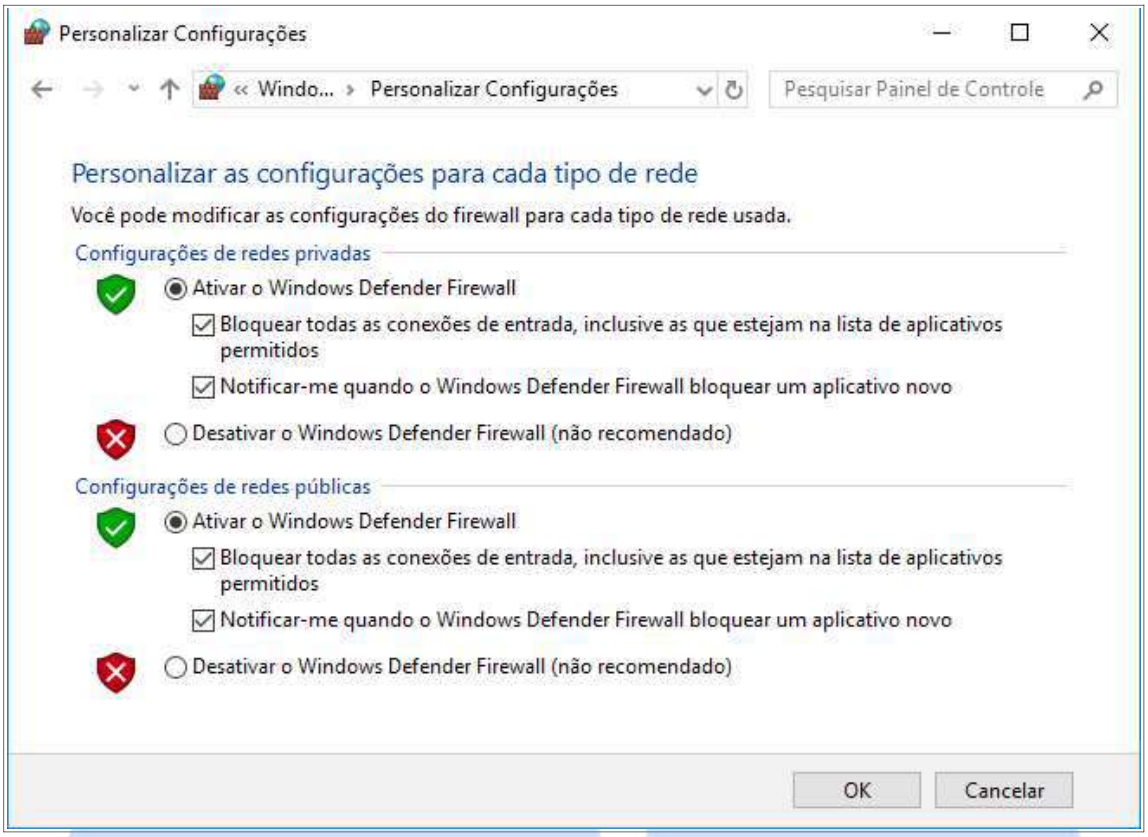
2.5. Antivírus, Antitrojan e Antispyware

Deve ser instalada uma solução de antivírus com capacidade para detectar e eliminar ameaças como vírus, trojans, spywares e outros tipos de códigos maliciosos, a qual deverá serconfigurada para atualização automática.

2.6. Firewall Pessoal

Deve ser ativado o firewall do Windows e configurado para não permitir exceções, de forma que serão bloqueadas todas as conexões de entrada não solicitadas. O log do firewall deverá ser configurado para registrar as conexões à estação e terá tamanho máximo de 50MB.

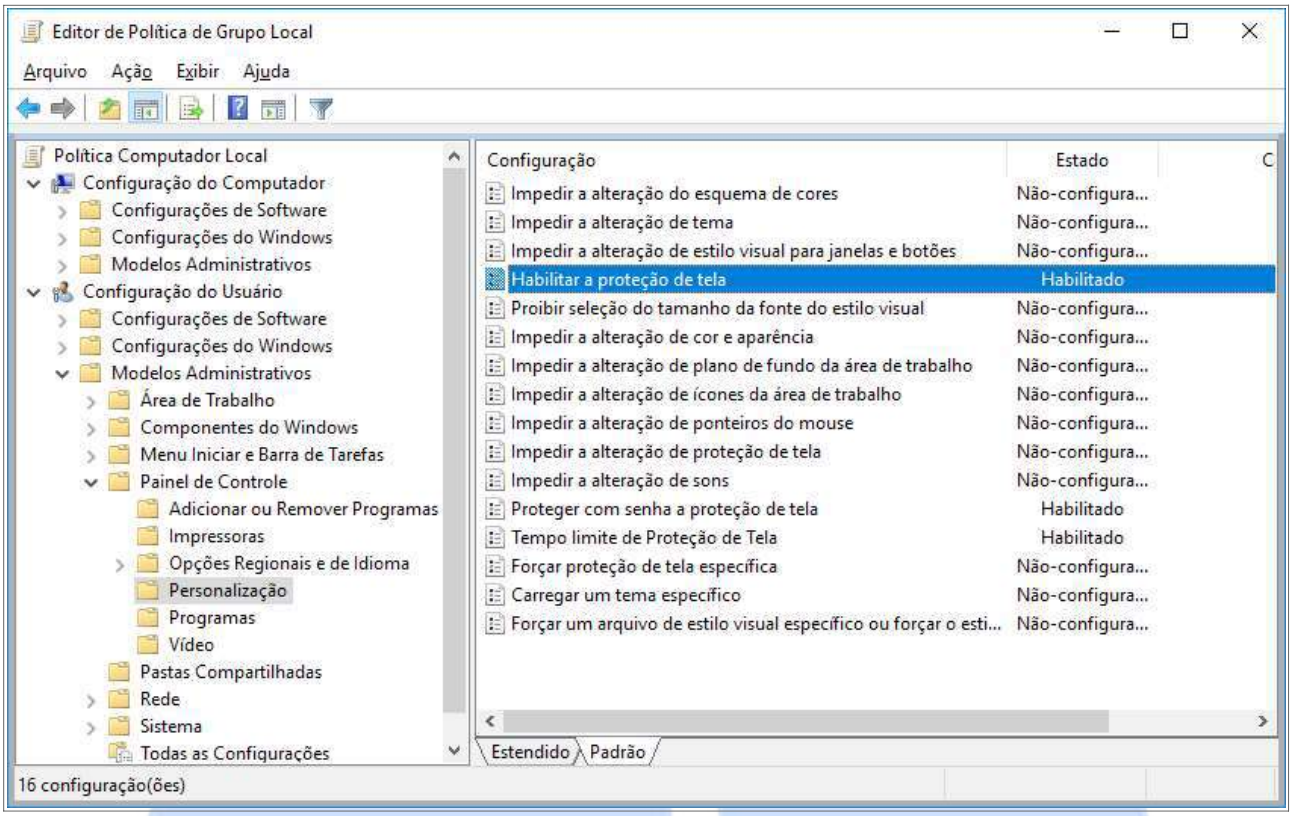
- No menu Iniciar do Windows digite **"firewall"** e abra "Windows Defender Firewall" (Configurações). Na janela aberta, clique na barra lateral esquerda em "Ativar ou Desativar Windows Defender Firewall", e marque as opções "Ativar o Windows Defender Firewall" e "Bloquear todas as conexões de entrada", tanto para Configurações de redes privadas como Configurações de redes públicas conforme tela a seguir.



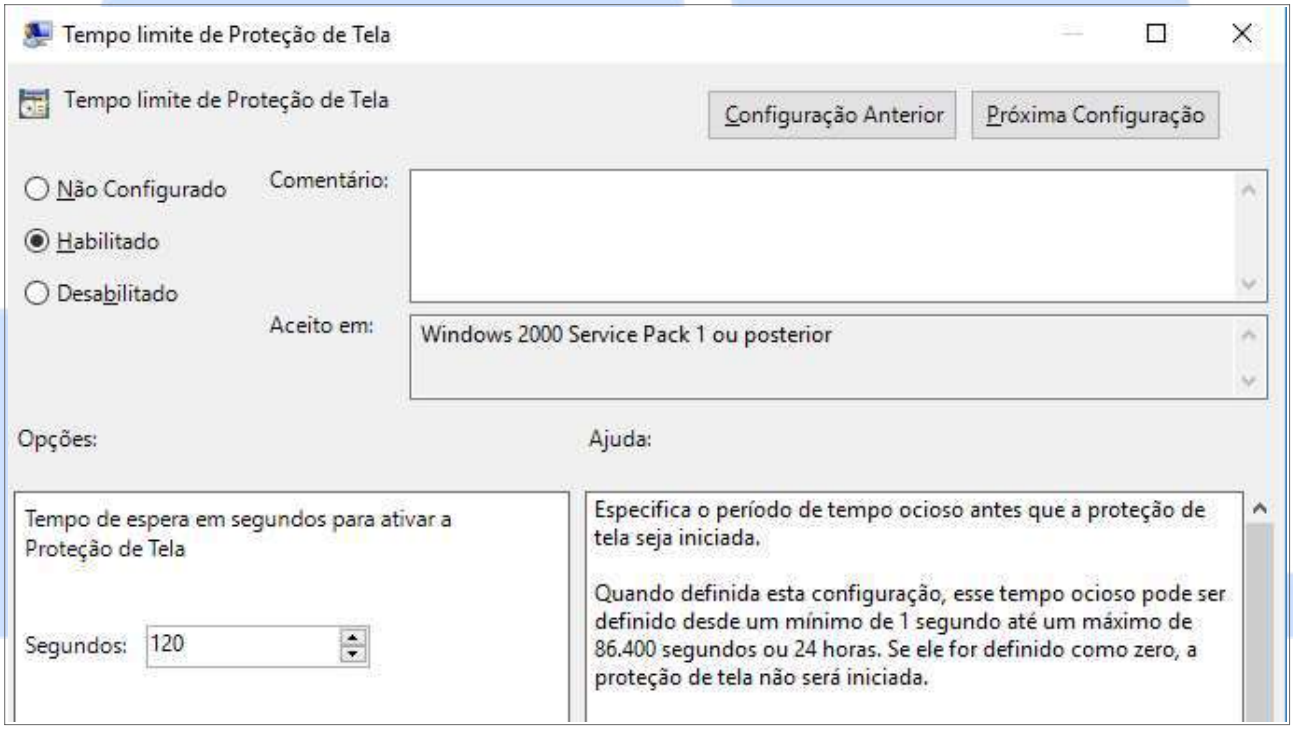
2.7. Proteção de Tela

Deve ser habilitada a proteção de tela com senha e definido tempo de 120 segundos para inatividade.

- No menu Iniciar do Windows digite **"gpedit"** e abra "Editar Política de Grupo" (Painel de Controle). Em seguida clique para abrir "Configurações do usuário", depois clique em "Modelos Administrativos", em seguida clique em "Painel de controle" e "Personalização".
- Clique 2x na Configuração "Habilitar a proteção de tela", e na janela aberta clique em "Habilitado", e depois em "Aplicar" conforme tela a seguir. Repita o procedimento para "Proteger com senha a proteção de tela".



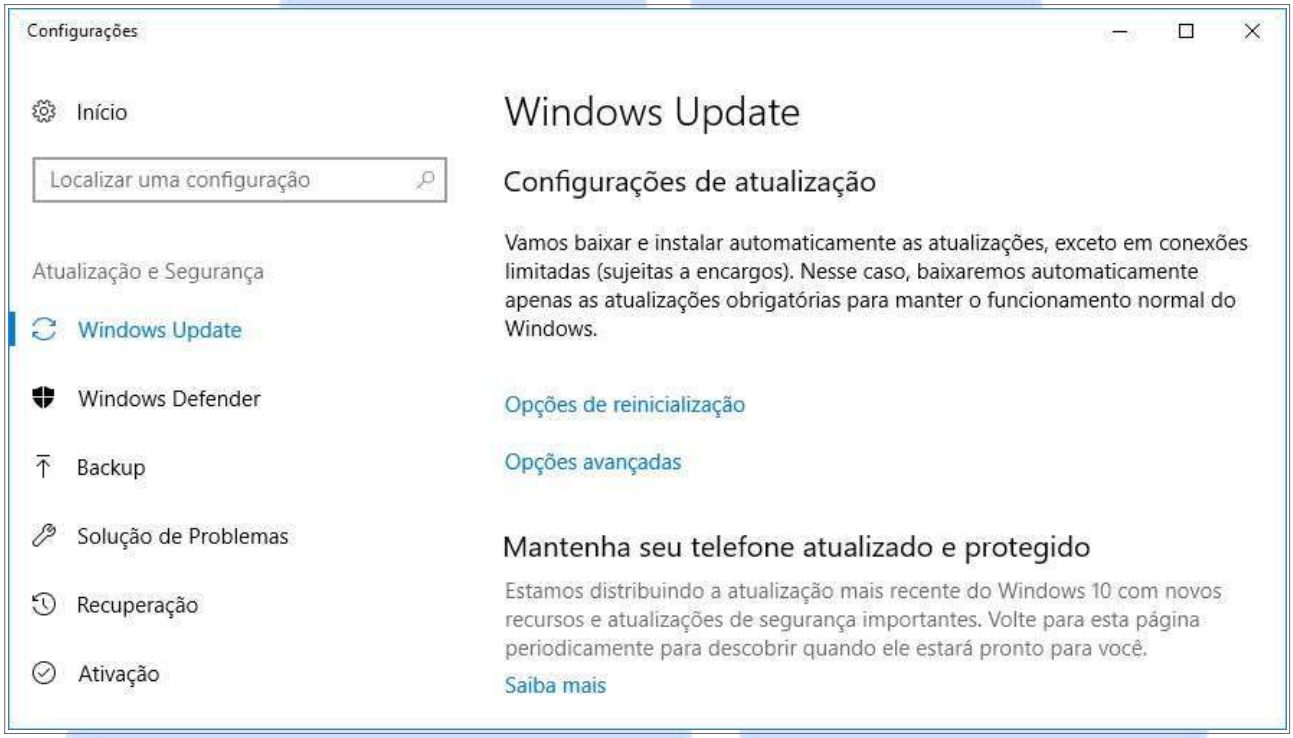
- Em seguida clique 2x na Configuração "Tempo limite de Proteção de Tela", e na janela aberta clique em "Habilitado", e em "Segundos" configure 120, e depois clique em "Aplicar" conforme tela a seguir.



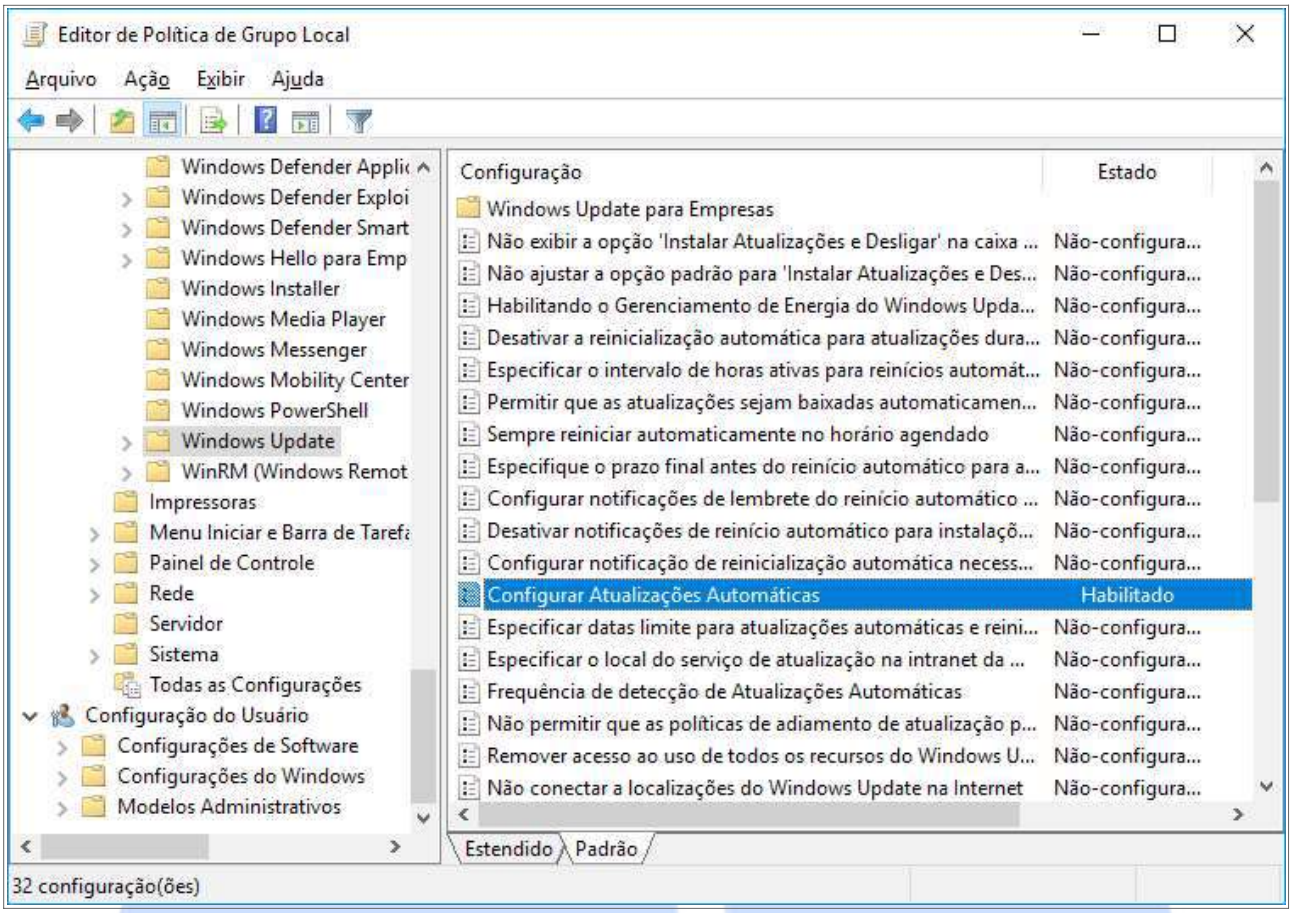
2.8. Atualização Automática do Sistema Operacional

Deve ser configurado o serviço de Atualização Automática do Windows.

- No menu Iniciar do Windows digite **"windows update"** e abra "Configurações do Windows Update" (Configurações do Sistema), e verifique a mensagem "Vamos baixar e instalar automaticamente as atualizações" conforme tela abaixo.



- Caso não esteja com a mensagem de baixar e instalar automaticamente as atualizações, no menu Iniciar do Windows digite **"gpedit"** e abra "Editar Política de Grupo" (Painel de Controle). Em seguida clique para abrir "Configurações do Computador", depois clique em "Modelos Administrativos", depois em "Componentes do Windows" e "Windows Update". Selecione "Configurar Atualizações Automáticas" e clique em "Habilitado" conforme tela a seguir.



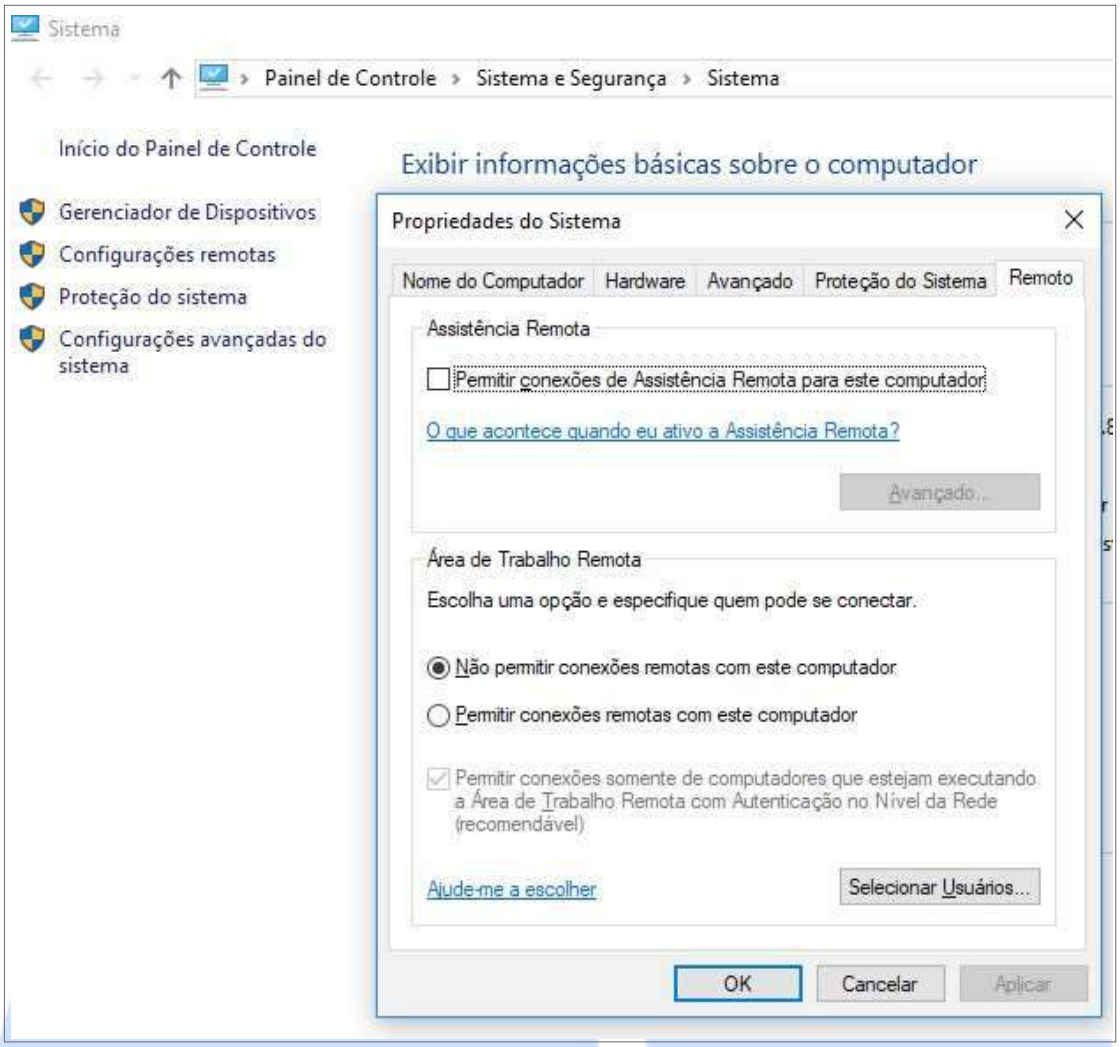
2.9. Softwares Licenciados

Deve ser configurado o usuário local do AR apenas no grupo local Usuários para que este não tenha permissão de instalação de softwares não autorizados.

2.10. Desativação de Logon Remoto

Devem ser desativadas as ferramentas de acesso remoto à estação Área de Trabalho Remota e Assistência Remota, bem como negar logon pelos serviços de terminal.

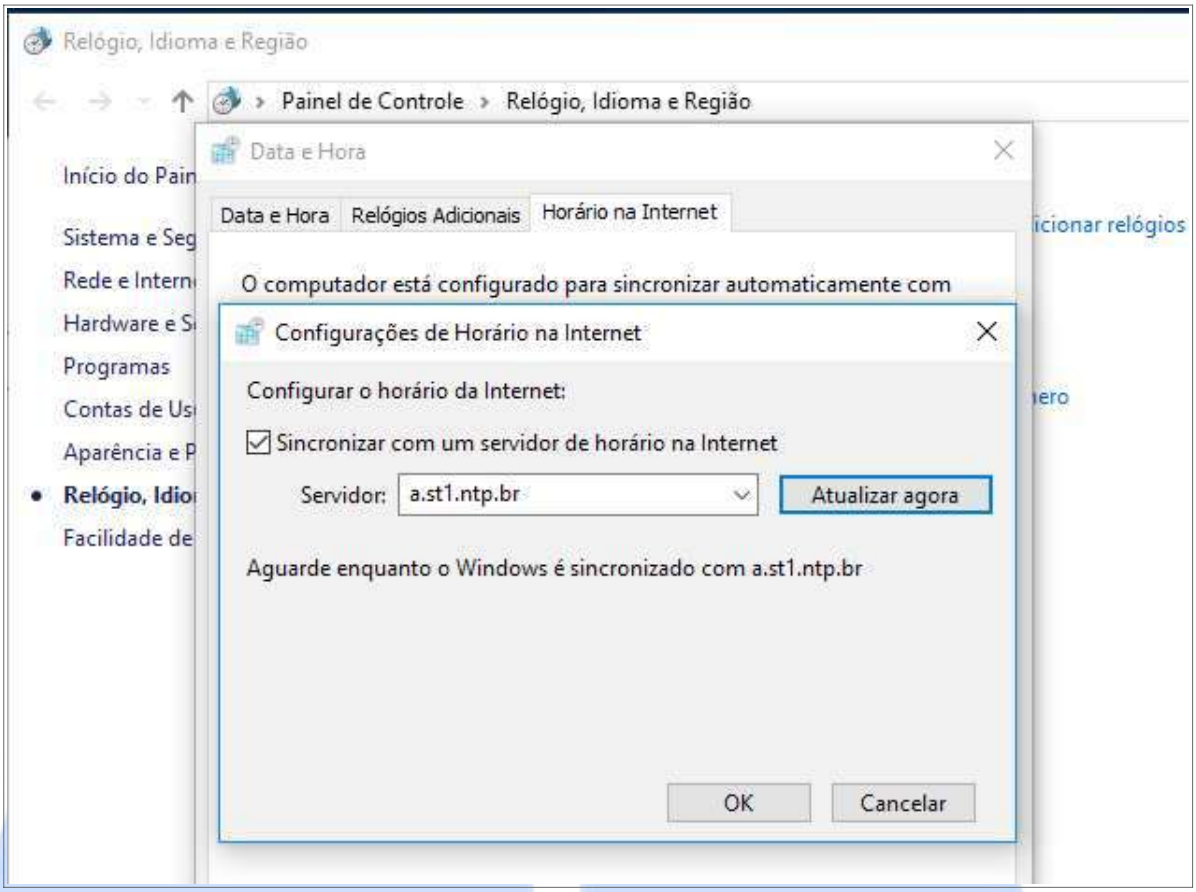
- No menu Iniciar do Windows digite **"sistema"** e abra "Sistema" (Painel de Controle). Na barra lateral clique em "Configurações Remotas". Na janela aberta de propriedades do sistema desmarque "Permitir conexões de Assistência Remota para este computador" e marque "Não permitir conexões remotas com este computador" conforme tela a seguir.



2.11. Utilização de Data e Hora de Fonte Confiável do Tempo (FCT)

Deve ser utilizado um servidor de horário na internet para sincronizar o horário da estação, o qual poderá ser um servidor do NTP.br ou outro servidor de tempo.

- Abra o Painel de Controle e clique em "Relógio, Idioma e Região", e em seguida clique em "Definir a hora e a data". Na janela aberta clique na aba "Horário na Internet" e em "Alterar configurações".
- Habilite a opção "Sincronizar com um servidor de horário na internet" e emservidor digite **a.st1.ntp.br**. Em seguida clique em "Atualizar agora" e OK, conformetela a seguir.

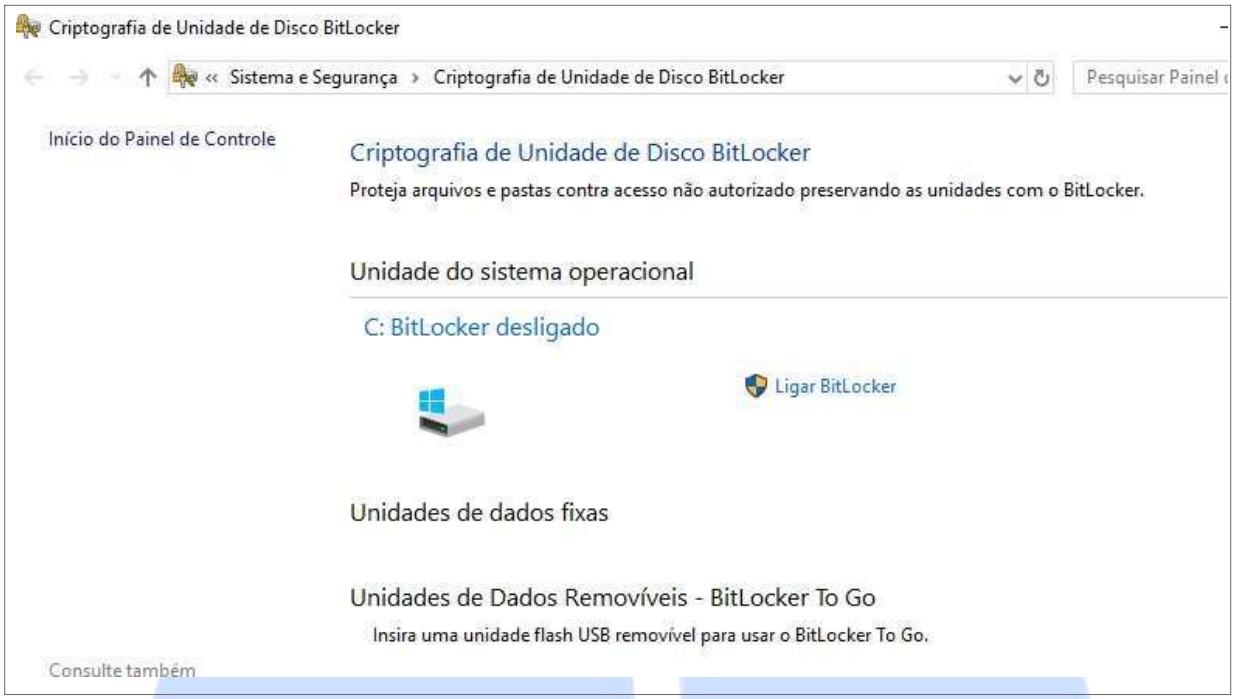


2.12. Criptografia de Disco

Devem ser criptografadas as partições do disco rígido que armazenam dados de solicitantes de certificados.

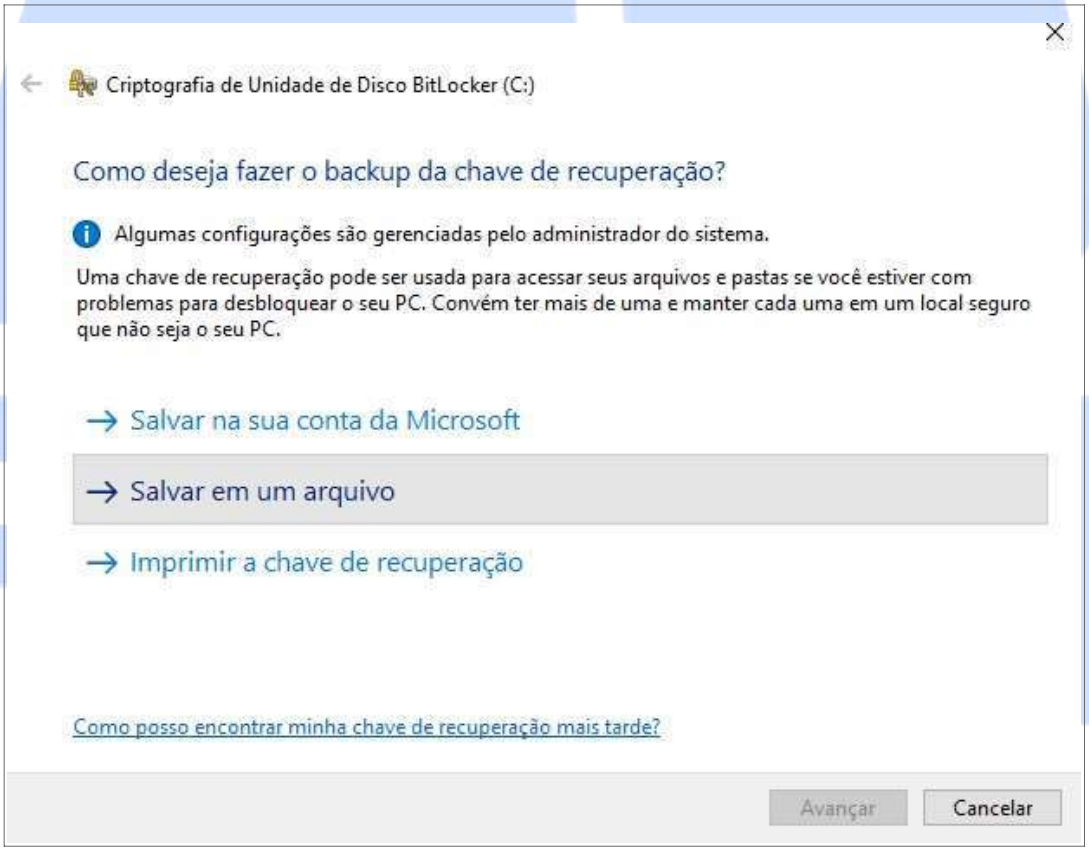
ATENÇÃO: Antes de inciar os procedimentos de criptografia de disco certifique-se de realizar um backup dos dados.

- No menu Iniciar do Windows digite **"BitLocker"** e abra "Gerenciar BitLocker" (Painel de Controle). Na janela aberta clique na opção "Ligar BitLocker" conforme tela a seguir, e siga as instruções.



ATENÇÃO: A chave de recuperação do BitLocker é uma senha numérica de 48 dígitos que pode ser usada para desbloquear o acesso, e sem a qual não será possível acessar o sistema.

- No momento em que for solicitado um backup da chave de recuperação, conforme tela abaixo, clique na opção "Salvar em um arquivo" e utilize um pendrive.



2.13. Equipamentos de Coleta Biométrica

Os equipamentos e softwares de identificação biométrica deverão ser instalados conforme documentação específica.

Ficha Técnica

SERVIÇO FEDERAL DE PROCESSAMENTO DE DADOS

Diretor-Presidente
Caio Mário Paes de Andrade

Diretor de Operações
Antonino dos Santos Guerra Neto

Superintendente de Operações – SUPOP
Gilberto de Oliveira Netto

Departamento de Gestão do Serviço de Certificação Digital
Pedro Moacir Rigo Motta

Divisão de Gestão das Aplicações e Inovação em Certificação Digital
Ronald Carvalho Ribeiro de Araújo

Elaboração
Francisca Juscivania Mendes – DIOPE/SUPOP/OPCDI/OPGAC
Janine Silva da Costa – DIOPE/SUPOP/OPCDI/OPGAC
Maria Lilian Santos da Costa – DIOPE/SUPOP/OPCDI/OPGAC
Sueli Pinheiro Vila Real – DIOPE/SUPOP/OPCDI/OPGAC

Versão 1.0
março/2020