

**MANUAL DE CONFIGURAÇÃO DAS
ESTAÇÕES DE TRABALHO WINDOWS**

CATEGORIA/REGISTRO:

MPO.076

CLASSIFICAÇÃO:

OSTENSIVO

PROCESSOS:

N/A

VERSÃO:

7

FASE:

PRODUÇÃO

DATA VIGÊNCIA:

31/05/2022

ELABORADOR:

IGOR FERREIRA

ÁREA RESPONSÁVEL:

INFRAESTRUTURA

DIRETORIA RESPONSÁVEL:

TI



Sumário

1. INTRODUÇÃO.....	3
2. REQUISITOS DO SISTEMA OPERACIONAL.....	3
3. CRITÉRIOS MÍNIMOS DE SEGURANÇA.....	3
4. CONFIGURANDO A ESTAÇÃO DE TRABALHO.....	3
4.1 Criptografia de disco.....	3
4.2 Usuários.....	9
4.3 Não exibir o último nome de usuário.....	12
4.4. Diretiva de senha.....	13
4.5. Diretiva de bloqueio de conta.....	14
4.6. Logon seguro.....	14
4.7. Serviço de log e auditoria.....	15
4.8. Diretivas de log.....	17
4.9. Proteção de tela.....	18
4.10. Serviço ntp.....	20
4.11. Antivírus.....	21
4.12. Firewall.....	22
4.13. Atualizações do Windows.....	22
4.14. Software autêntico.....	22
4.15. Acesso remoto.....	23

1. INTRODUÇÃO

Este manual visa orientar o usuário a executar as configurações de Segurança Lógica nas estações de trabalho do sistema operacional Windows seguindo os requisitos mínimos de segurança exigidos no DOC-03.01.

2. REQUISITOS DO SISTEMA OPERACIONAL

As configurações abaixo descritas neste manual somente funcionam nas seguintes versões do sistema operacional Windows.

- Windows 8 Profissional ou Enterprise 32bit ou 64bit
- Windows 8.1 Profissional ou Enterprise 32bit ou 64bit
- Windows 10 Profissional ou Enterprise 32bit ou 64bit
- Windows 11 Profissional ou Enterprise 32bit ou 64bit

OBS: Este manual foi baseado na versão do Windows 10 Profissional e serve também para as versões citadas acima, qualquer outra versão do Windows não é compatível com este manual.

3. CRITÉRIOS MÍNIMOS DE SEGURANÇA

3.1 A manutenção preventiva/corretiva das estações de trabalho deve ser realizada apenas por agentes autorizados (pelo fabricante, por assistência técnica autorizada ou por pessoa designada pela AC), dentro do período de manutenção recomendado. Os eventos de manutenção devem ser documentados.

3.2 A partição dos discos rígidos das estações devem ser criptografadas.

3.3 As estações de trabalho da AR, incluindo equipamentos portáteis, devem estar protegidas contra ameaças e ações não-autorizadas, bem como contra o acesso, uso ou exposição indevidos.

3.4 O Agente de Registro não deve possuir perfil de administrador ou senha de root dos equipamentos ou com privilégios especiais do sistema, ficando essa tarefa delegada a outros da própria organização, para permitir segregação de funções.

3.5 As estações de trabalho da AR deverão conter apenas aplicações e serviços que sejam suficientes e necessários para as atividades corporativas.

4. CONFIGURANDO A ESTAÇÃO DE TRABALHO

As estações de trabalho de uso do Agente de Registro e da AR devem seguir as seguintes configurações de segurança:

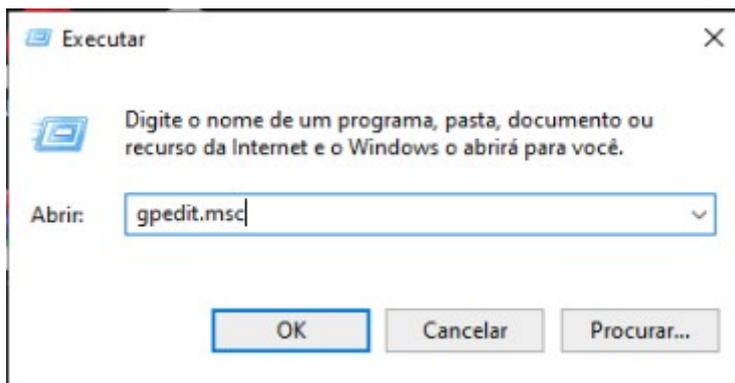
4.1 Criptografia de disco

Configurar política para habilitar criptografia de disco Bitlocker

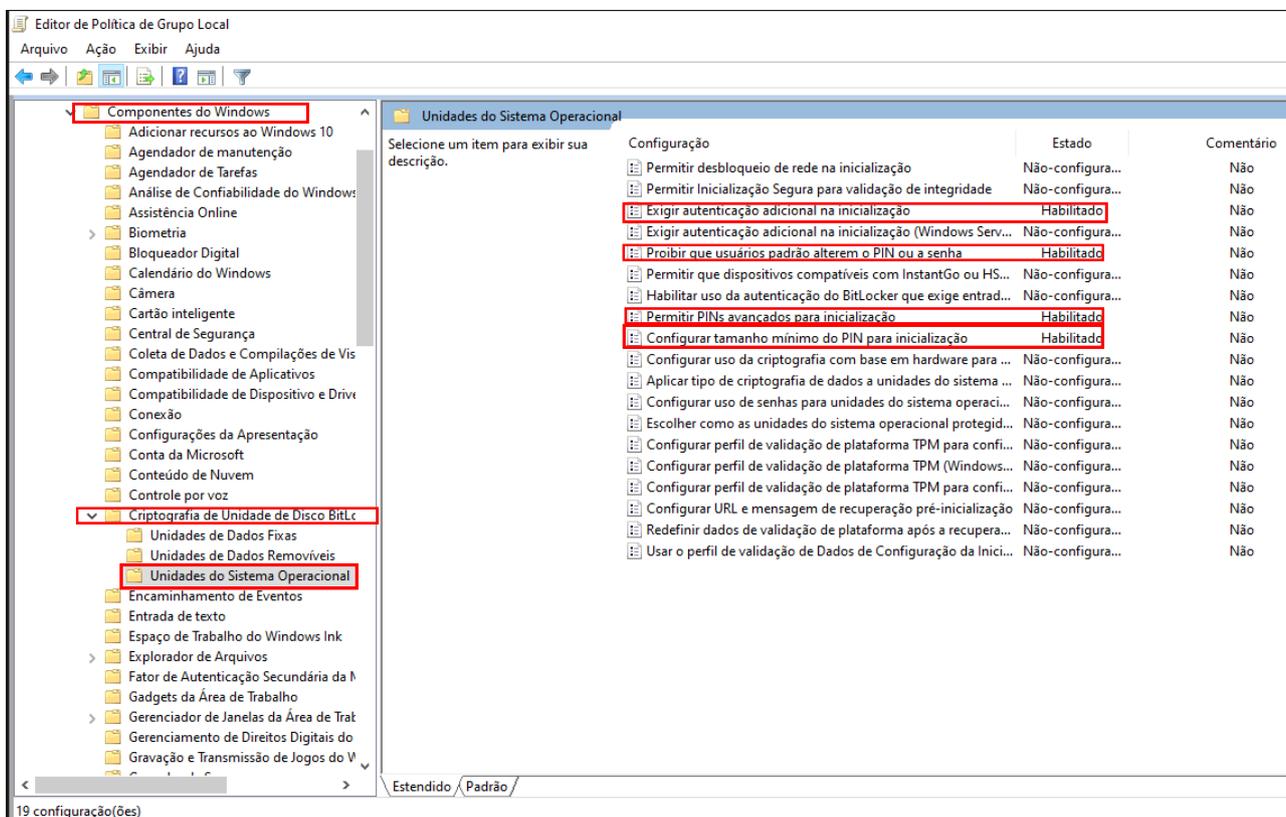
Clique no Menu iniciar > Busque por Executar > digite **“gpedit.msc”**



Continua na próxima página...

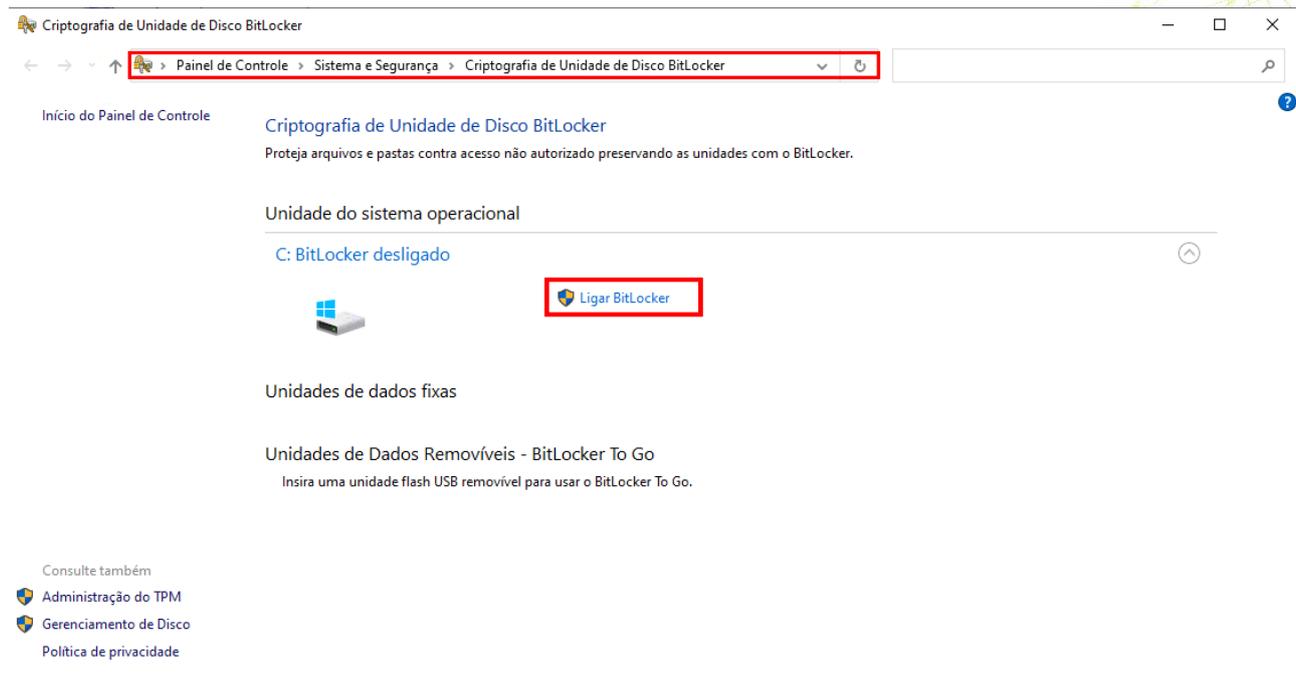


Acesse o caminho: Configuração do Computador > Modelos Administrativos > Criptografia de Unidade de Disco BitLocker > Unidades do Sistema Operacional.

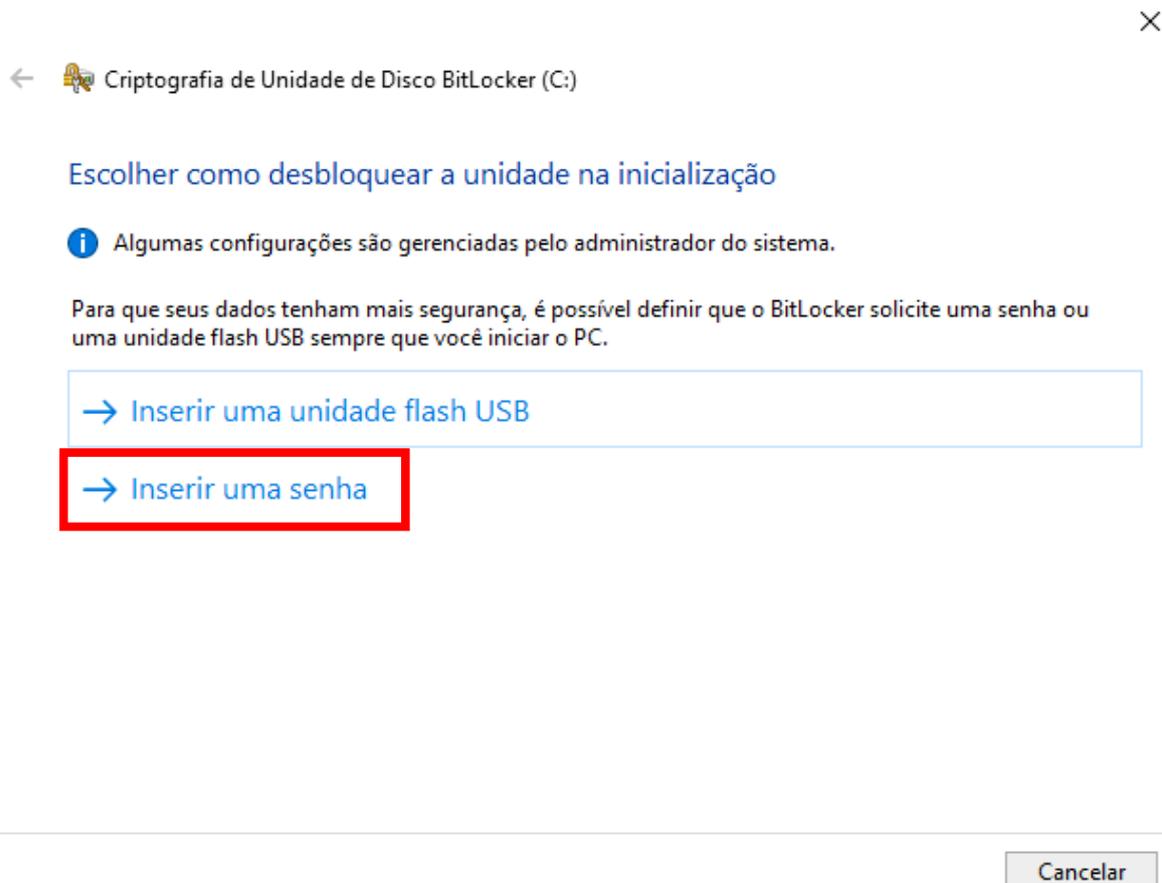


Obs.: Mantenha as configurações de acordo com a imagem.

Acesse o Painel de Controle > Sistema e Segurança > Criptografia de Unidade de Disco BitLocker.



Clique em “Ligar BitLocker” > inserir um PIN > Defina uma senha PIN forte.



Continua na próxima página...

Clique em “**Imprimir a chave de Recuperação**” > Armazene em um local confiável que não seja na própria máquina local, para caso de necessidade de recuperação se esquecer ou bloquear o PIN. > Depois clique em Avançar.

← Criptografia de Unidade de Disco BitLocker (C:)

Como deseja fazer o backup da chave de recuperação?

i A chave de recuperação foi impressa.

Uma chave de recuperação pode ser usada para acessar seus arquivos e pastas se você estiver com problemas para desbloquear o seu PC. Convém ter mais de uma e manter cada uma em um local seguro que não seja o seu PC.

→ Salvar em uma unidade flash USB

→ Salvar em um arquivo

→ **Imprimir a chave de recuperação**

[Como posso encontrar minha chave de recuperação mais tarde?](#)

Avançar

Cancelar

Selecione a opção “**Criptografar a unidade inteira (mais lento, mas melhor para Pcs e unidades já em uso)**” > Depois clique em Avançar.

← Criptografia de Unidade de Disco BitLocker (C:)

Escolher que parte da unidade deve ser criptografada

Se estiver configurando o BitLocker em uma nova unidade ou um novo PC, você só precisará criptografar a parte da unidade que está sendo usada. O BitLocker criptografa os novos dados automaticamente à medida que você os adiciona.

Se estiver habilitando o BitLocker em um PC ou em uma unidade que já esteja em uso, considere criptografar a unidade inteira. Criptografar a unidade inteira garante a proteção de todos os dados excluídos por você, mas ainda pode conter informações que podem ser recuperadas.

Criptografar apenas espaço em disco usado (mais rápido e melhor para novos PCs e unidades)

Criptografar a unidade inteira (mais lento, mas melhor para PCs e unidades já em uso)

Avançar

Cancelar

Selecione a opção “**Novo modo de criptografia**” > Depois clique em Avançar.

←  Criptografia de Unidade de Disco BitLocker (C:)

Escolha o modo de criptografia a ser usado

O Windows 10 (Versão 1511) apresenta um novo modo de criptografia de disco (XTS-AES). Esse modo dá suporte adicional a integridade, mas não é compatível com versões anteriores do Windows.

Se você for usar uma versão anterior do Windows em uma unidade removível, escolha Modo compatível.

Caso se trate de uma unidade fixa, ou se você usar essa unidade somente em dispositivos com o Windows 10 (Versão 1511) ou posterior, escolha o novo modo de criptografia.

Novo modo de criptografia (indicado para unidades fixas neste dispositivo)

Modo compatível (indicado para unidades que podem ser movidas deste dispositivo)

Avançar

Cancelar

Mantenha a opção “**Executar verificação do sistema BitLocker**”> Depois clique em Continua.

←  Criptografia de Unidade de Disco BitLocker (C:)

Você está pronto para criptografar essa unidade?

A criptografia pode levar algum tempo dependendo do tamanho da unidade.

Você pode continuar trabalhando enquanto a unidade está sendo criptografada, mas o PC pode ter um desempenho mais lento.

Executar verificação do sistema BitLocker

A verificação do sistema garante que o BitLocker pode ler as chaves de recuperação e de criptografia corretamente antes de criptografar a unidade.

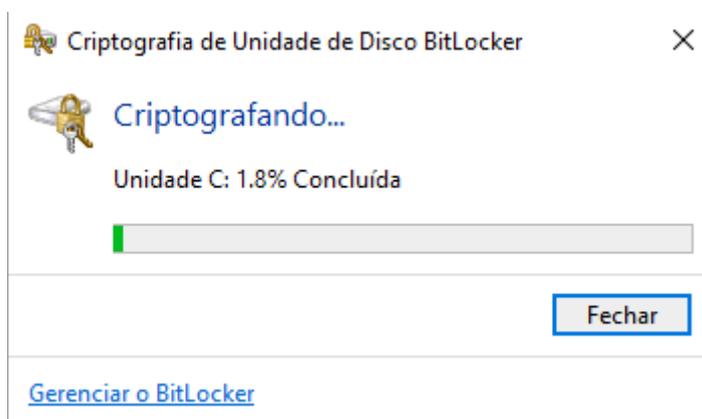
O BitLocker reiniciará o computador antes de iniciar a criptografia.

Observação: essa verificação pode demorar um pouco, mas é recomendada para garantir que o método de desbloqueio selecionado funcione sem a chave de recuperação.

Continuar

Cancelar

Obs.: Após clicar em continuar, será necessário reiniciar o computador para verificar se a chave PIN e de recuperação estão corretas antes de iniciar a criptografia automaticamente.



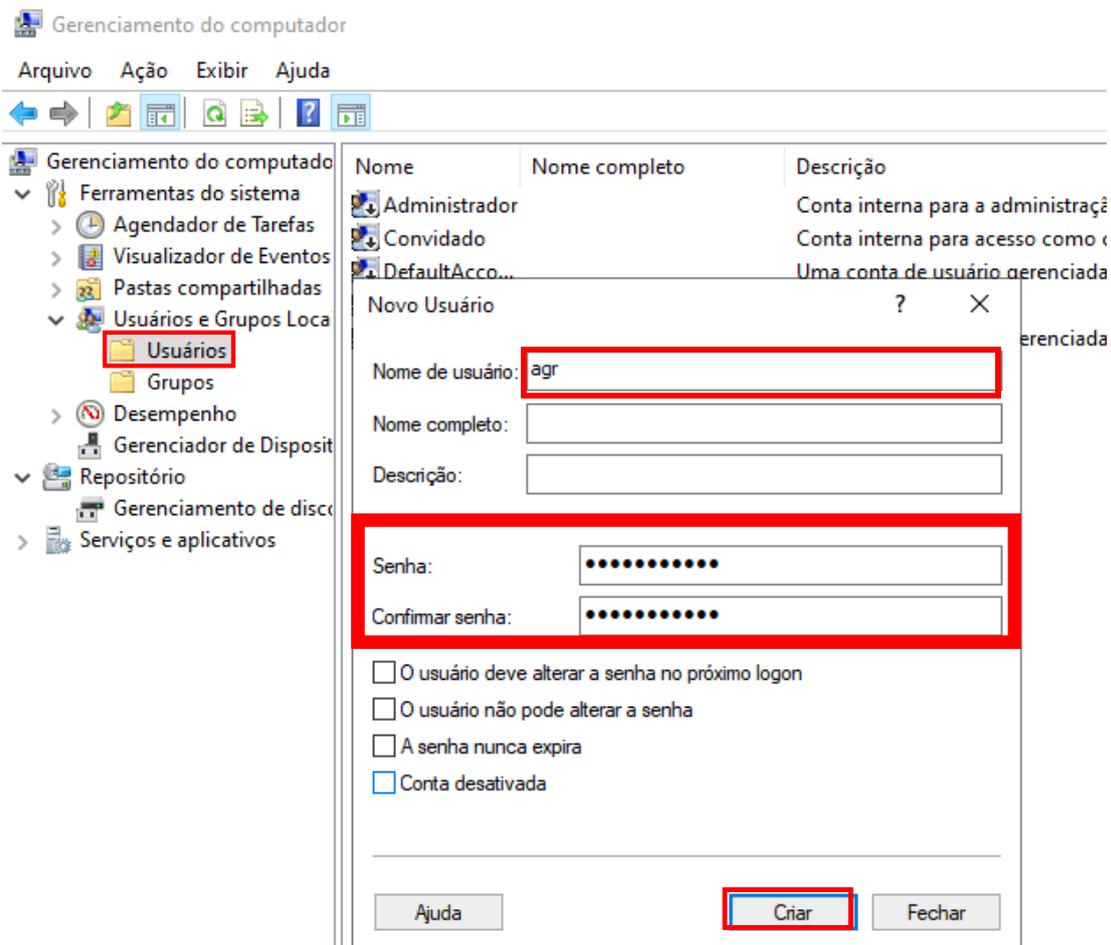
4.2 Usuários

Todas as estações devem possuir acesso através de senha, e dois usuários, um padrão usado por um agente de registro e outro com perfil de administrador para o suporte.

Crie um usuário para o agente de registro e defina uma senha:

Clique Menu iniciar > Executar > digitar “**compmgmt.msc**”.

Acesse o Gerenciamento do computador > Usuários e Grupos Locais > Usuários > Criar um novo usuário.



Gerenciamento do computador

Arquivo Ação Exibir Ajuda

Gerenciamento do computador

- Ferramentas do sistema
 - Agendador de Tarefas
 - Visualizador de Eventos
 - Pastas compartilhadas
 - Usuários e Grupos Locais
 - Usuários**
 - Grupos
 - Desempenho
 - Gerenciador de Dispositivos
- Repositório
 - Gerenciamento de discos
- Serviços e aplicativos

Nome	Nome completo	Descrição
Administrador		Conta interna para a administração
Convidado		Conta interna para acesso como convidado
DefaultAcco...		Uma conta de usuário gerenciada automaticamente

Novo Usuário

Nome de usuário: agr

Nome completo:

Descrição:

Senha:

Confirmar senha:

O usuário deve alterar a senha no próximo logon

O usuário não pode alterar a senha

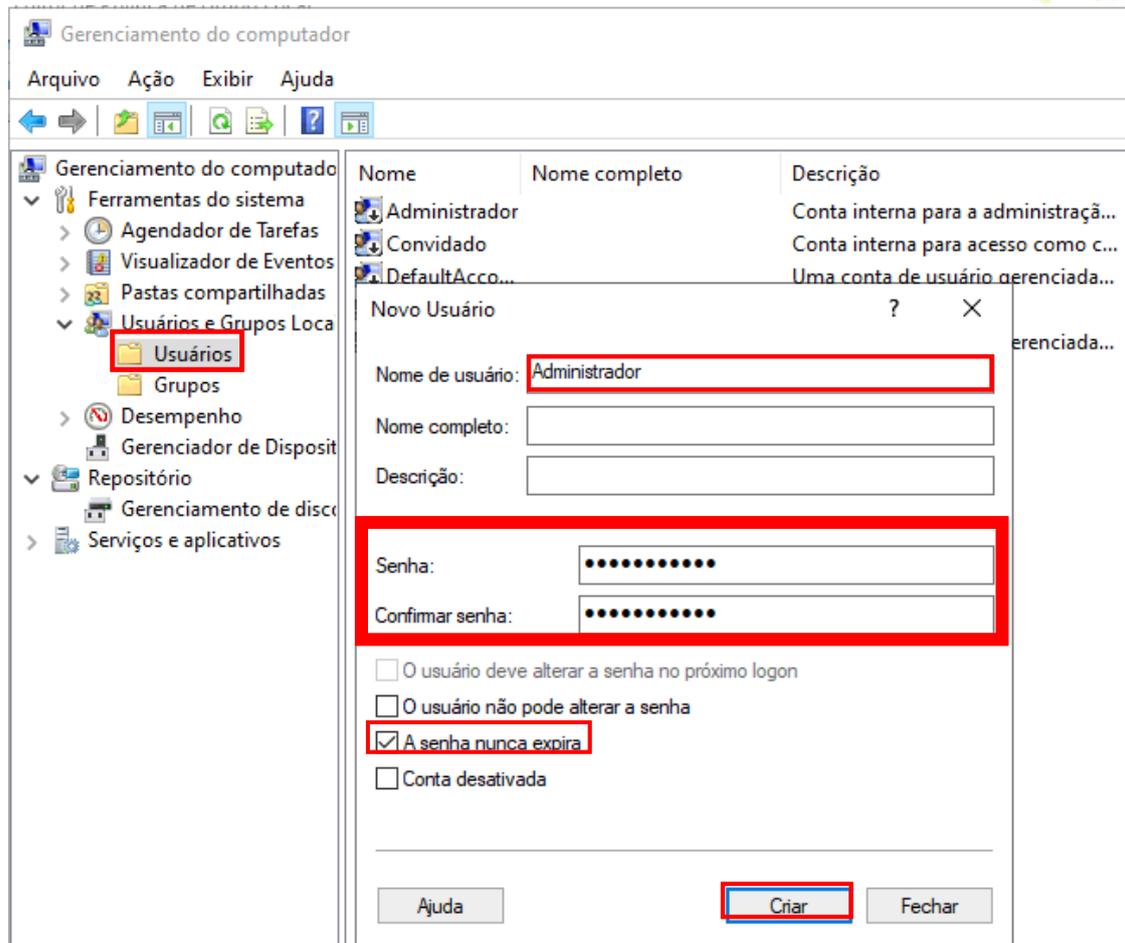
A senha nunca expira

Conta desativada

Ajuda Criar Fechar

Continua na próxima página...

Crie um usuário Administrador e defina uma senha:

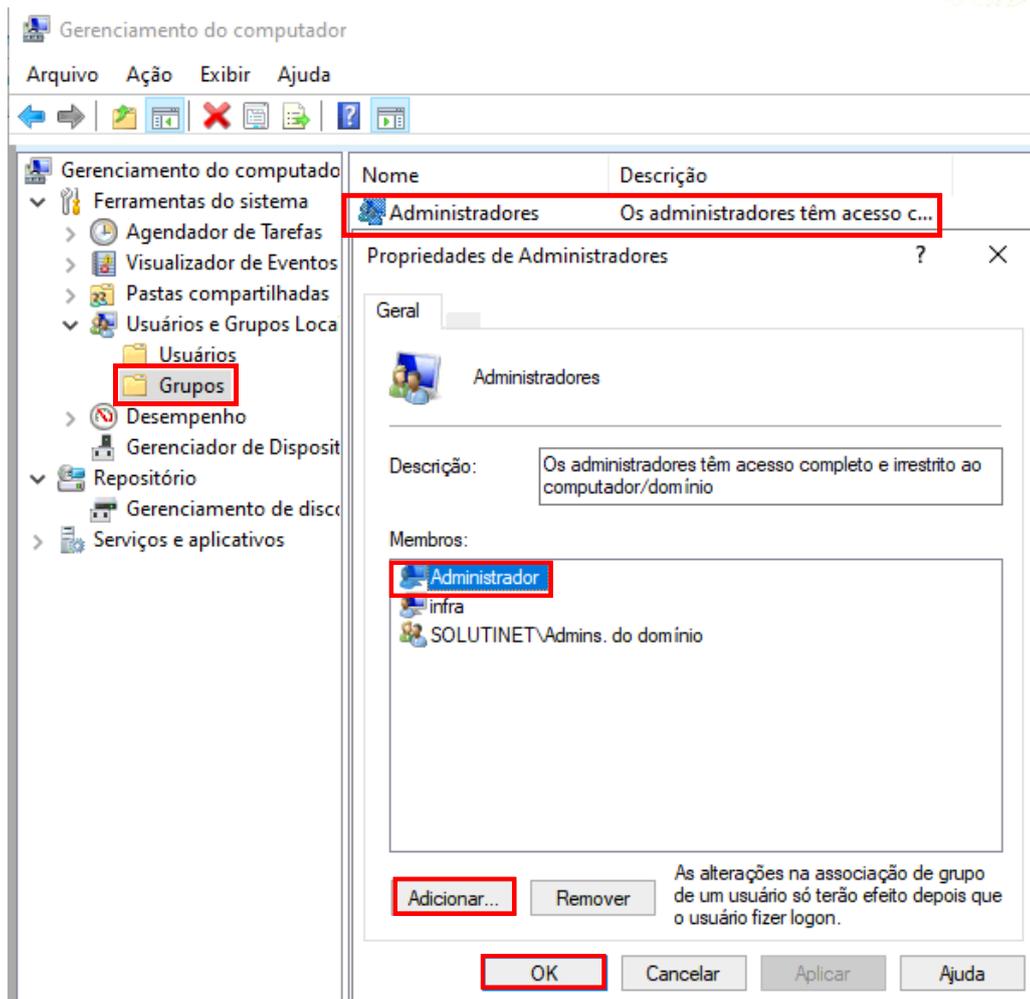


Obs.: Marcar a opção "A senha nunca expira".

Para adicionar o usuário Administrador no grupo de Administradores do sistema:

Acesse o Gerenciamento do computador > Usuários e Grupos Locais > Grupos > Administradores > Adicionar.

Continua na próxima página...



The screenshot shows the Windows 'Gerenciamento do computador' (Computer Management) console. The left-hand tree view is expanded to 'Grupos' (Groups). The main pane displays a table of groups:

Nome	Descrição
Administradores	Os administradores têm acesso c...

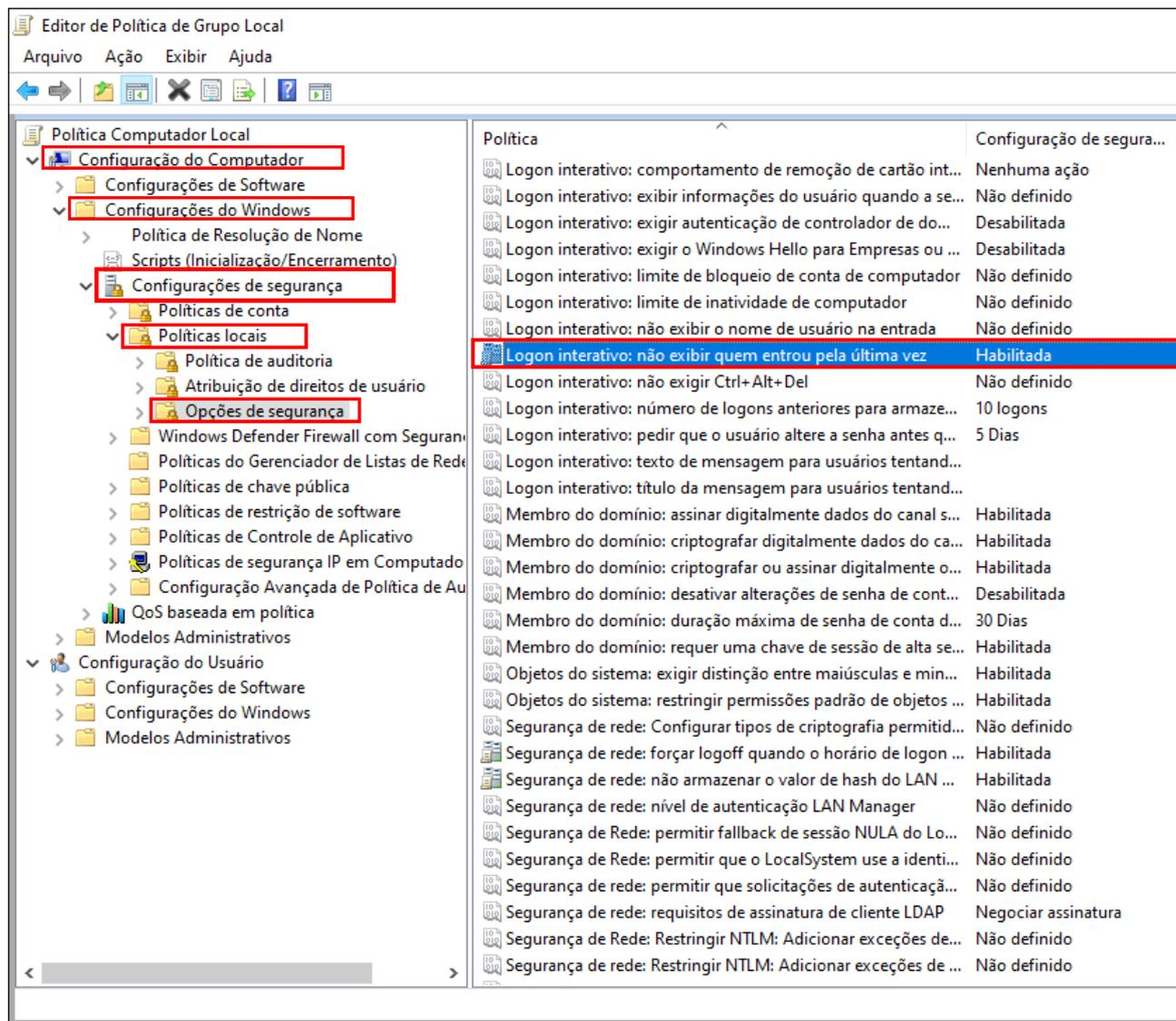
The 'Administradores' group is selected, and its 'Propriedades de Administradores' (Administrators Properties) dialog box is open. The 'Geral' (General) tab is active, showing the group name 'Administradores' and its description: 'Os administradores têm acesso completo e irrestrito ao computador/domínio'. The 'Membros' (Members) list includes 'Administrador', 'infra', and 'SOLUTINET\Admins. do domínio'. The 'Adicionar...' button is highlighted. At the bottom of the dialog, the 'OK' button is also highlighted.

4.3 Não exibir o último nome de usuário

Habilite a opção de não exibir o último nome do usuário a ter realizado logon.

Clique em Menu iniciar > Executar > digitar “gpedit.msc”.

Acesse o caminho: Configuração do Computador > Configuração do Windows > Configurações de segurança > Políticas locais > Opções de segurança.



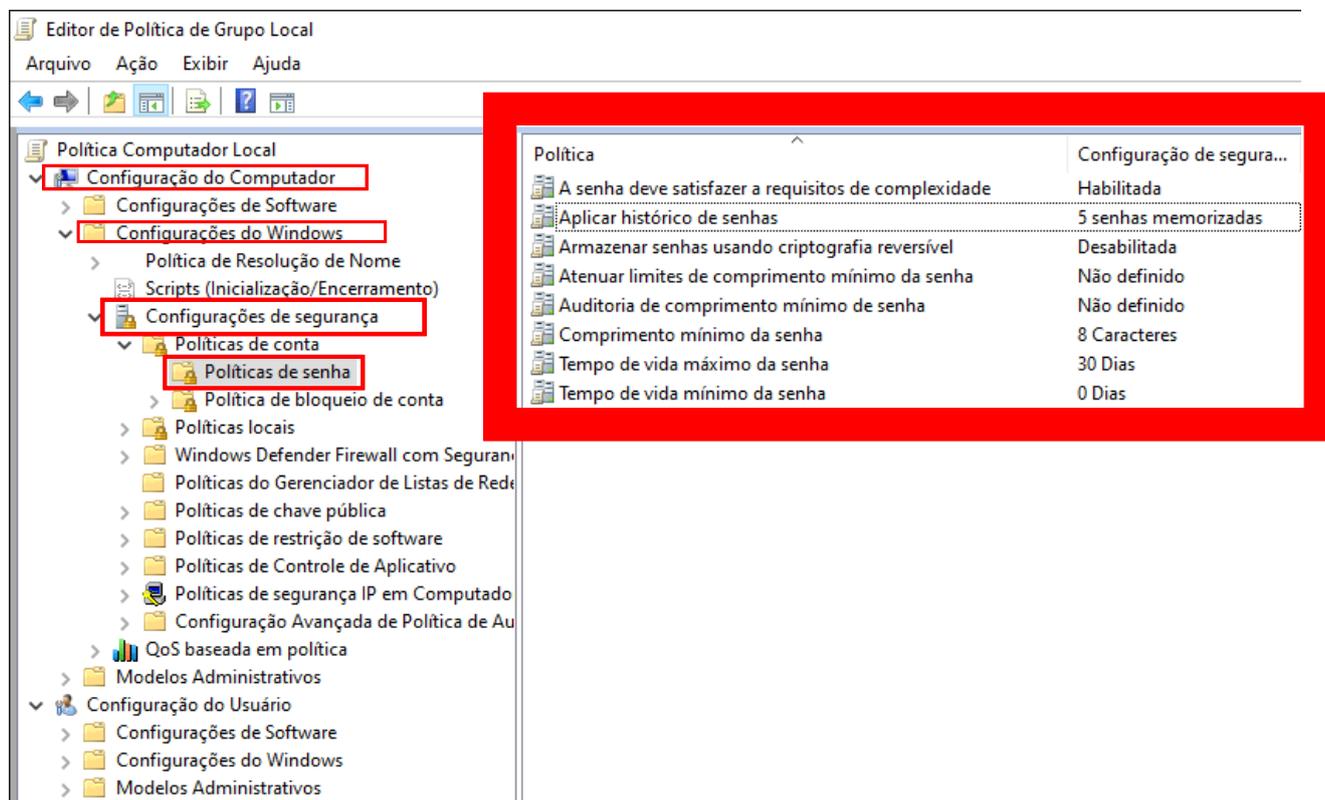
Obs.: Mantenha as configurações de acordo com a imagem.

4.4. Diretiva de senha

As senhas devem ser fortes.

Clique em Menu iniciar > Executar > digitar "gpedit.msc".

Acesse o caminho: Configuração do Computador > Configurações do Windows > Configurações de segurança > Políticas de conta > Políticas de senha.



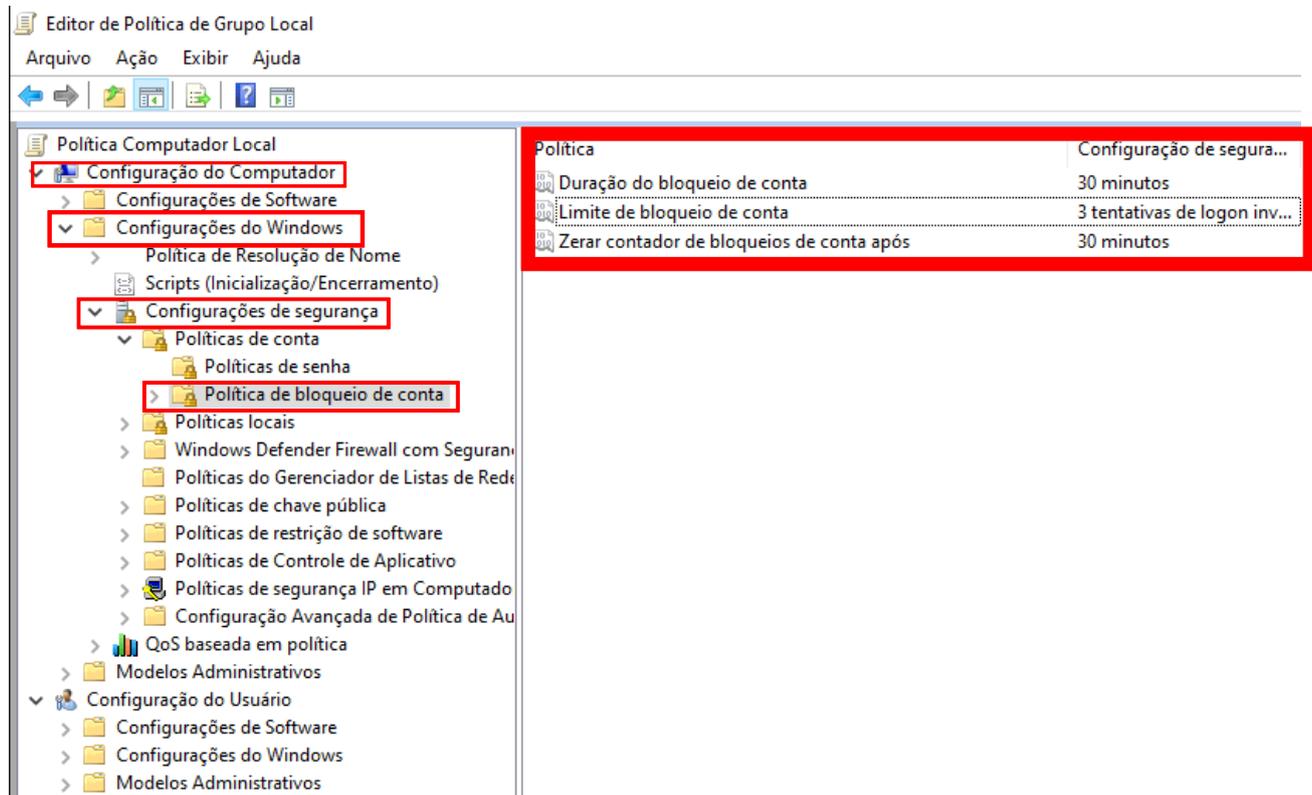
Obs.: Mantenha as configurações de acordo com a imagem.

4.5. Diretiva de bloqueio de conta

Caso o usuário erre a senha por mais de 3 vezes, a conta do mesmo permanecerá bloqueada por 30 minutos, após esse período o usuário poderá tentar fazer o logon novamente.

Clique em Menu iniciar > Executar > digitar “gpedit.msc”.

Acesse o caminho: Configuração do Computador > Configurações do Windows > Configurações de segurança > Políticas de conta > Políticas de bloqueio da conta.



Obs.: Mantenha as configurações de acordo com a imagem.

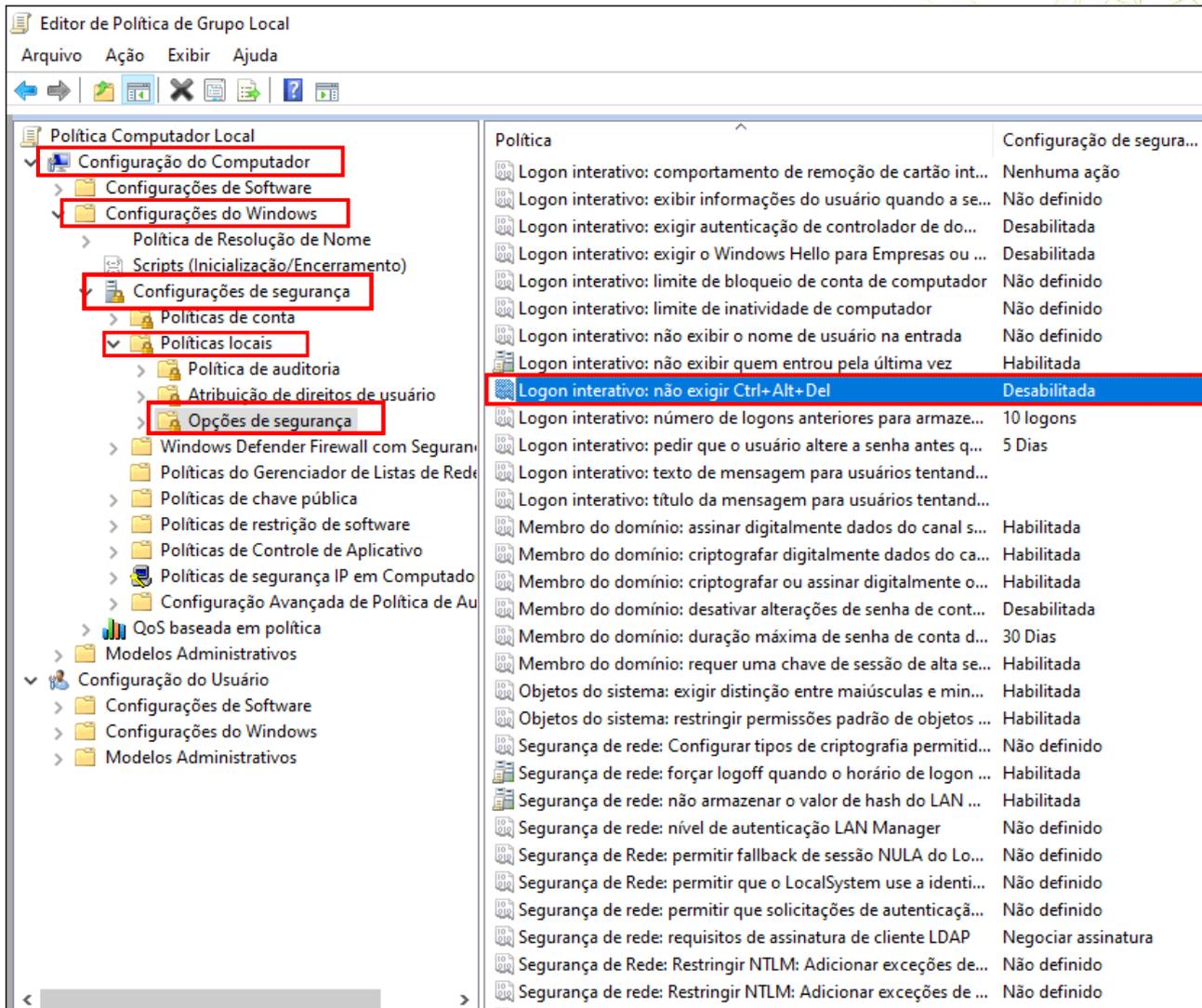
4.6. Logon seguro

Desative a opção para ser exigido que o usuário pressione CTRL+ALT+DEL para fazer logon.

Clique em Menu iniciar > Executar > digitar “gpedit.msc”.

Acesse o caminho: Configuração do Computador > Configurações do Windows > Configurações de segurança > Políticas locais > Opções de segurança.

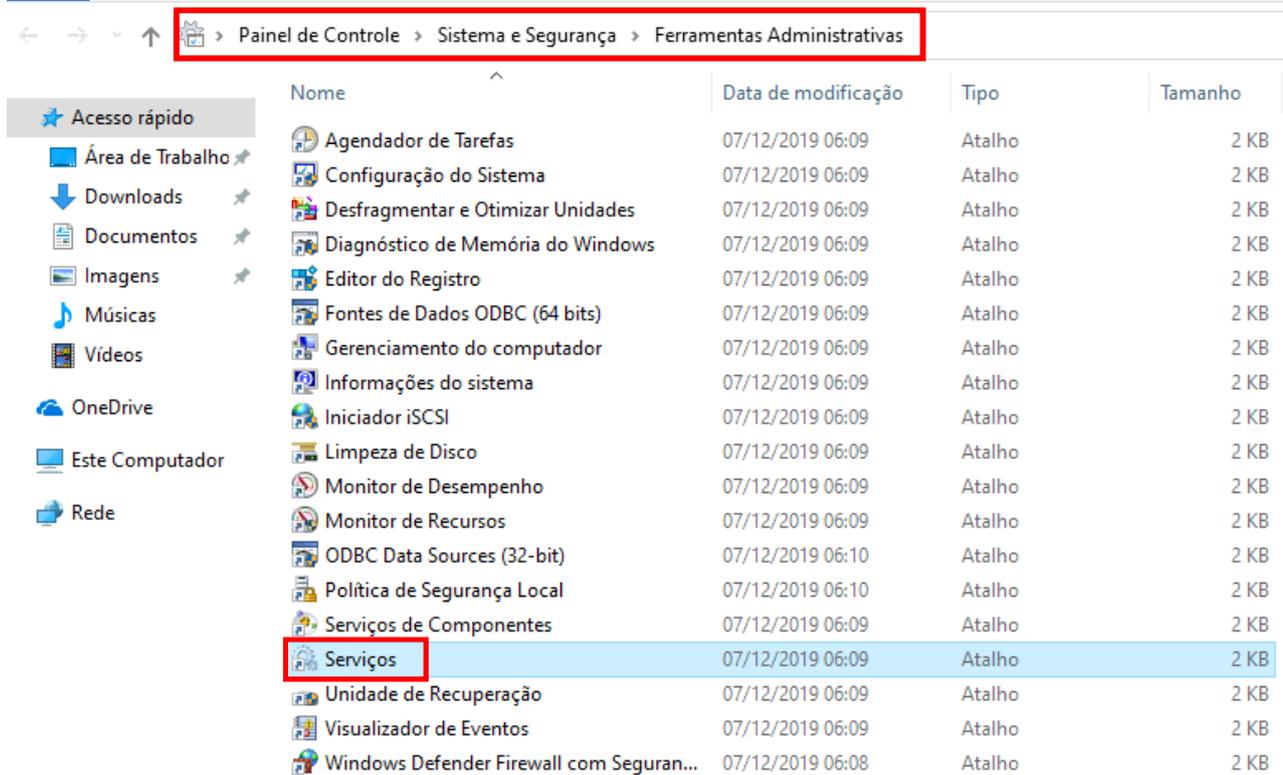
Continua na próxima página...



Obs.: Mantenha as configurações de acordo com a imagem.

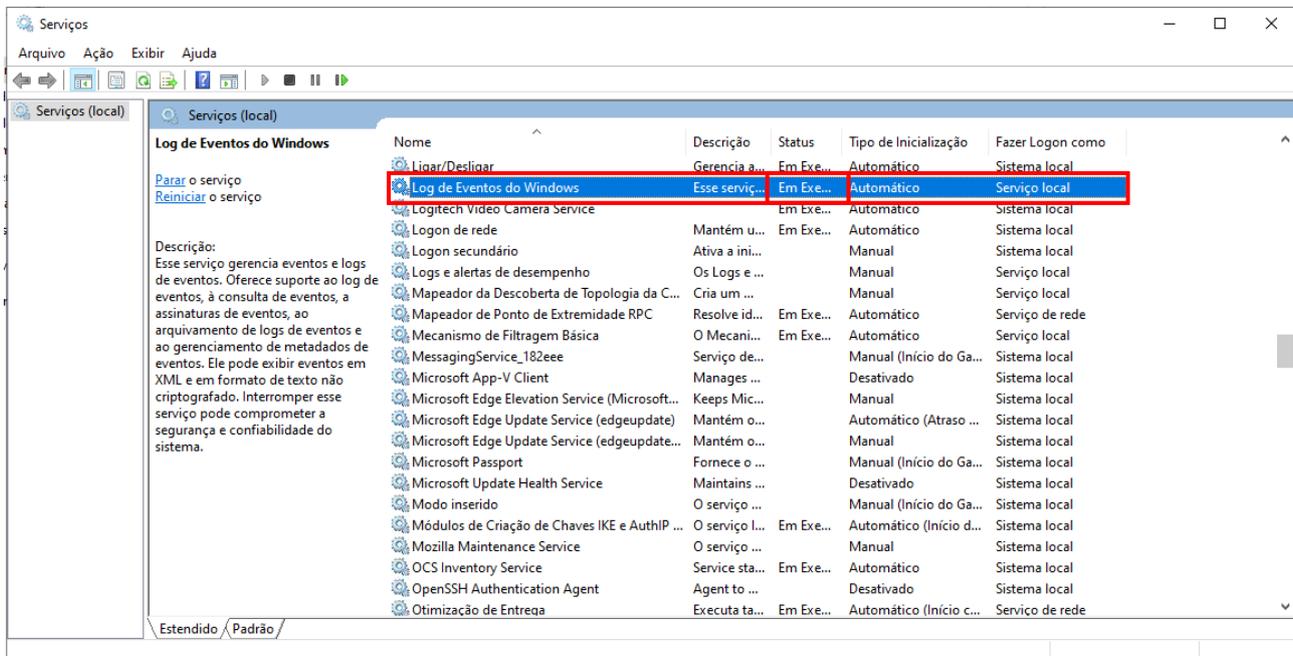
4.7. Serviço de Log e Auditoria

Acesse o Painel de Controle > Sistema de segurança > Ferramentas Administrativas > Serviços.



Nome	Data de modificação	Tipo	Tamanho
Agendador de Tarefas	07/12/2019 06:09	Atalho	2 KB
Configuração do Sistema	07/12/2019 06:09	Atalho	2 KB
Desfragmentar e Otimizar Unidades	07/12/2019 06:09	Atalho	2 KB
Diagnóstico de Memória do Windows	07/12/2019 06:09	Atalho	2 KB
Editor do Registro	07/12/2019 06:09	Atalho	2 KB
Fontes de Dados ODBC (64 bits)	07/12/2019 06:09	Atalho	2 KB
Gerenciamento do computador	07/12/2019 06:09	Atalho	2 KB
Informações do sistema	07/12/2019 06:09	Atalho	2 KB
Iniciador iSCSI	07/12/2019 06:09	Atalho	2 KB
Limpeza de Disco	07/12/2019 06:09	Atalho	2 KB
Monitor de Desempenho	07/12/2019 06:09	Atalho	2 KB
Monitor de Recursos	07/12/2019 06:09	Atalho	2 KB
ODBC Data Sources (32-bit)	07/12/2019 06:10	Atalho	2 KB
Política de Segurança Local	07/12/2019 06:10	Atalho	2 KB
Serviços de Componentes	07/12/2019 06:09	Atalho	2 KB
Serviços	07/12/2019 06:09	Atalho	2 KB
Unidade de Recuperação	07/12/2019 06:09	Atalho	2 KB
Visualizador de Eventos	07/12/2019 06:09	Atalho	2 KB
Windows Defender Firewall com Seguran...	07/12/2019 06:08	Atalho	2 KB

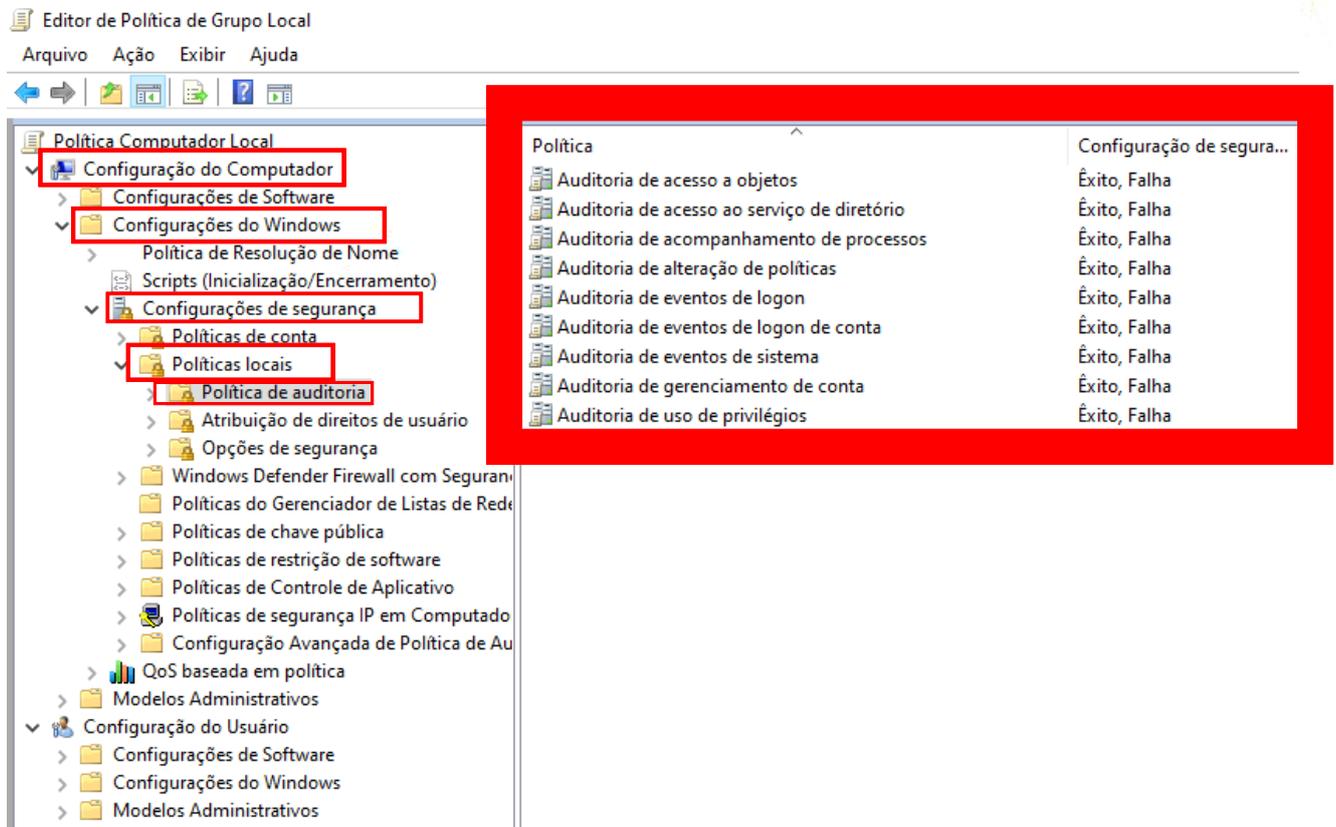
Verifique se o serviço de log de eventos do Windows não foi parado ou desabilitado.



Nome	Descrição	Status	Tipo de Inicialização	Fazer Logon como
Ligar/Desligar	Gerencia a...	Em Exe...	Automático	Sistema local
Log de Eventos do Windows	Esse serviç...	Em Exe...	Automático	Serviço local
Logitech Video Camera Service		Em Exe...	Automático	Sistema local
Logon de rede	Mantém u...	Em Exe...	Automático	Sistema local
Logon secundário	Ativa a ini...		Manual	Sistema local
Logs e alertas de desempenho	Os Logs e ...		Manual	Serviço local
Mapeador da Descoberta de Topologia da C...	Cria um ...		Manual	Serviço local
Mapeador de Ponto de Extremidade RPC	Resolve id...	Em Exe...	Automático	Serviço de rede
Mecanismo de Filtragem Básica	O Mecani...	Em Exe...	Automático	Serviço local
MessagingService_182eee	Serviço de...		Manual (Início do Ga...	Sistema local
Microsoft App-V Client	Manages ...		Desativado	Sistema local
Microsoft Edge Elevation Service (Microsoft...	Keeps Mic...		Manual	Sistema local
Microsoft Edge Update Service (edgeupdate)	Mantém o...		Automático (Atraso ...	Sistema local
Microsoft Edge Update Service (edgeupdate...	Mantém o...		Manual	Sistema local
Microsoft Passport	Fornece o ...		Manual (Início do Ga...	Sistema local
Microsoft Update Health Service	Maintains ...		Desativado	Sistema local
Modo inserido	O serviço ...		Manual (Início do Ga...	Sistema local
Módulos de Criação de Chaves IKE e AuthIP ...	O serviço l...	Em Exe...	Automático (Início d...	Sistema local
Mozilla Maintenance Service	O serviço ...		Manual	Sistema local
OCS Inventory Service	Service sta...	Em Exe...	Automático	Sistema local
OpenSSH Authentication Agent	Agent to ...		Desativado	Sistema local
Otimização de Entrega	Executa ta...	Em Exe...	Automático (Início c...	Serviço de rede

Clique em Menu iniciar > Executar > digitar "gpedit.msc".

Acesse o caminho: Configurações do Computador > Configurações do Windows > Configurações de segurança > Políticas locais > Políticas de auditoria.



Obs.: Mantenha as configurações de acordo com a imagem.

4.8. Diretivas de log

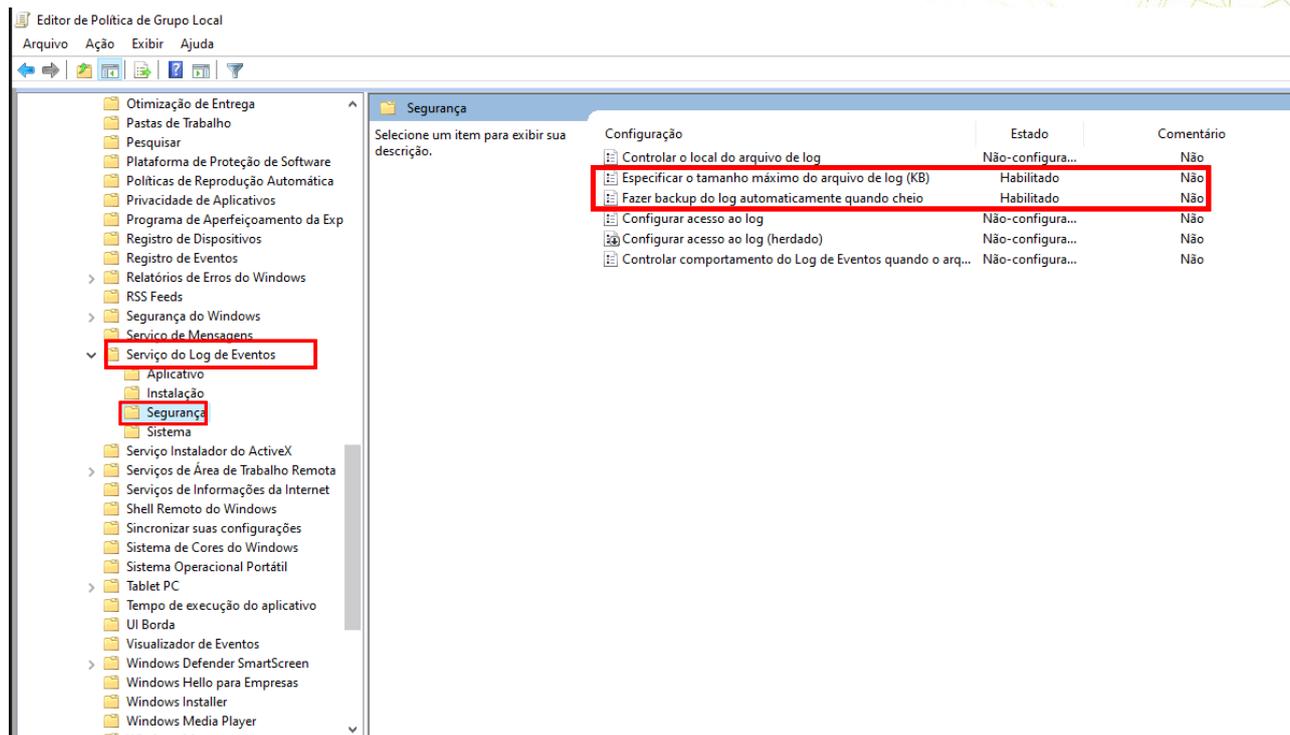
Habilitar as diretivas:

Tamanho Máximo de log (KB) e Fazer backup de log automaticamente quando completo.

Clique em Menu iniciar > Executar > digitar "gpedit.msc".

Acesse o caminho: Configuração do Computador > Modelos Administrativos > Componentes do Windows > Serviço do Log de Eventos > Segurança.

Continua na próxima página...



Obs.: Mantenha as configurações de acordo com a imagem.

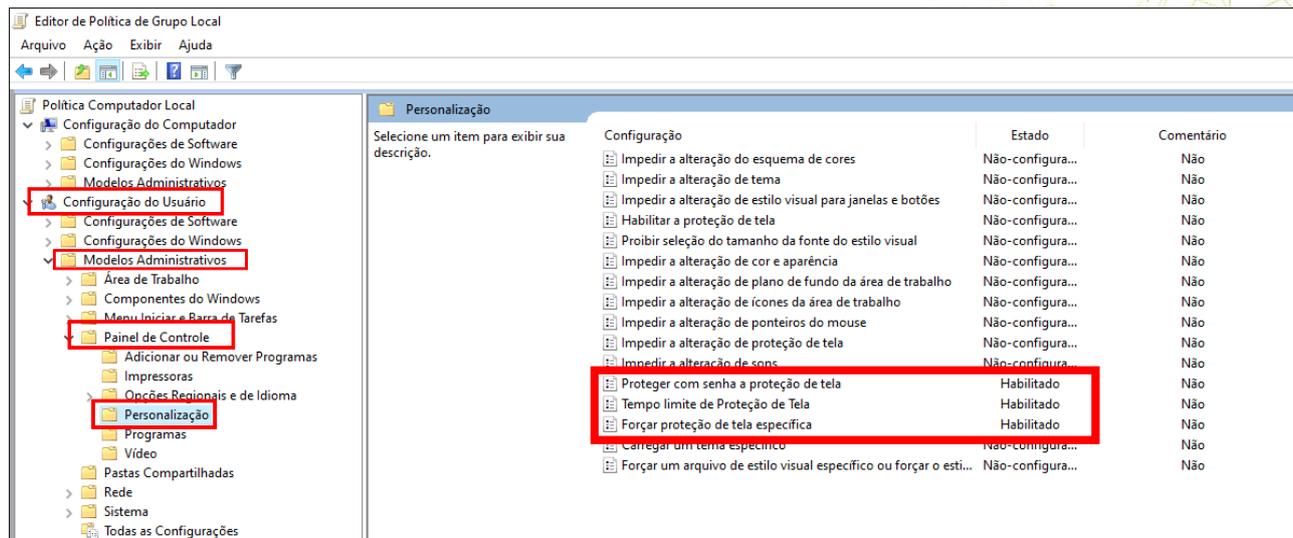
4.9. Proteção de tela

Habilitar bloqueio de tela com tempo de 2 minutos e proteger com senha.

Clique em Menu iniciar > Executar > digitar "**gpedit.msc**".

Acesse o caminho: Configuração do Usuário > Modelos Administrativos > Painel de Controle > Personalização.

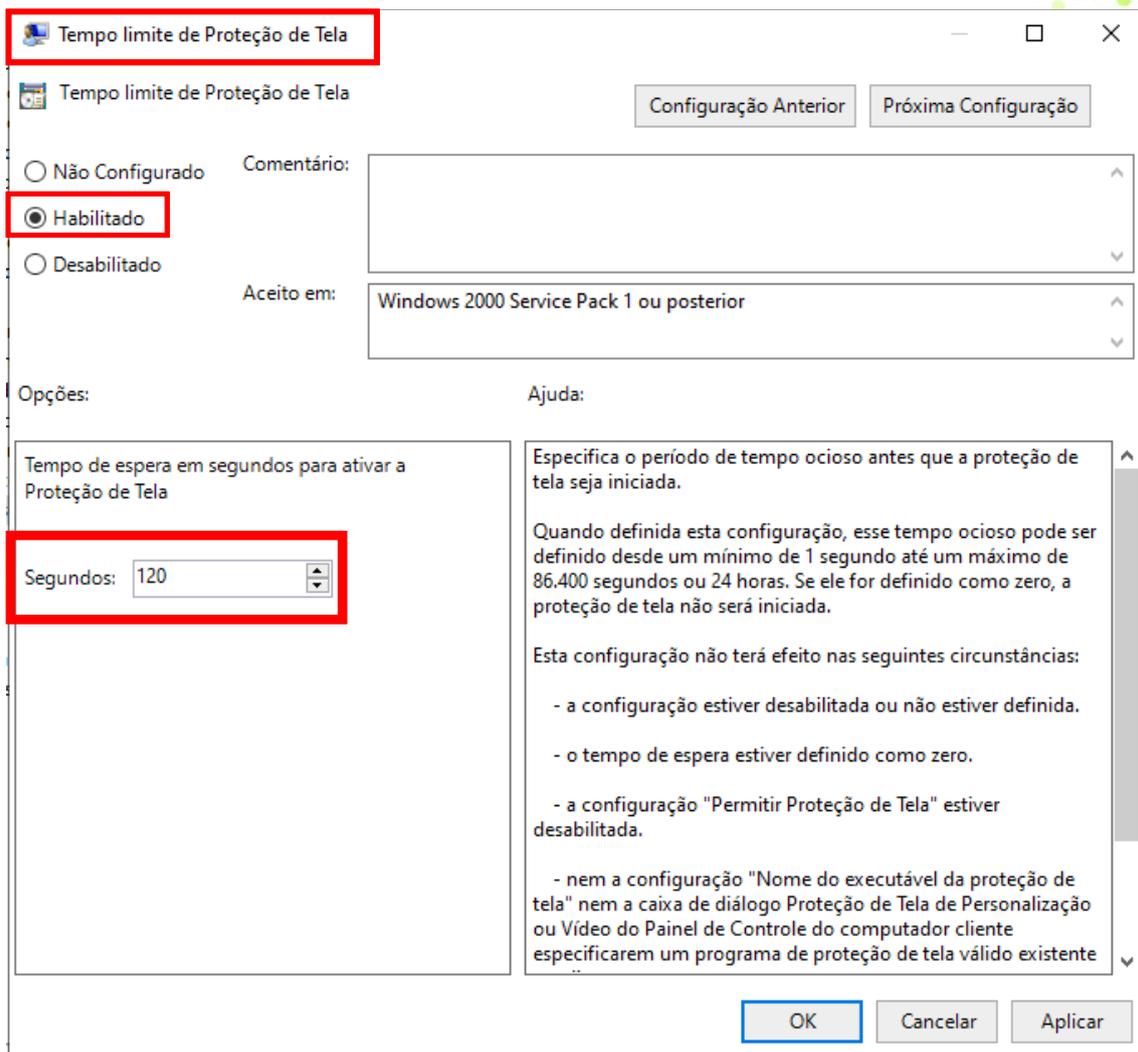
Continua na próxima página...



Obs.: Mantenha as configurações de acordo com a imagem.

Continua na próxima página...

Determinando o tempo limite de Proteção de Tela



Tempo limite de Proteção de Tela

Configuração Anterior Próxima Configuração

Não Configurado Comentário:

Habilitado

Desabilitado

Aceito em: Windows 2000 Service Pack 1 ou posterior

Opções:

Tempo de espera em segundos para ativar a Proteção de Tela

Segundos: 120

Ajuda:

Especifica o período de tempo ocioso antes que a proteção de tela seja iniciada.

Quando definida esta configuração, esse tempo ocioso pode ser definido desde um mínimo de 1 segundo até um máximo de 86.400 segundos ou 24 horas. Se ele for definido como zero, a proteção de tela não será iniciada.

Esta configuração não terá efeito nas seguintes circunstâncias:

- a configuração estiver desabilitada ou não estiver definida.
- o tempo de espera estiver definido como zero.
- a configuração "Permitir Proteção de Tela" estiver desabilitada.
- nem a configuração "Nome do executável da proteção de tela" nem a caixa de diálogo Proteção de Tela de Personalização ou Vídeo do Painel de Controle do computador cliente especificarem um programa de proteção de tela válido existente

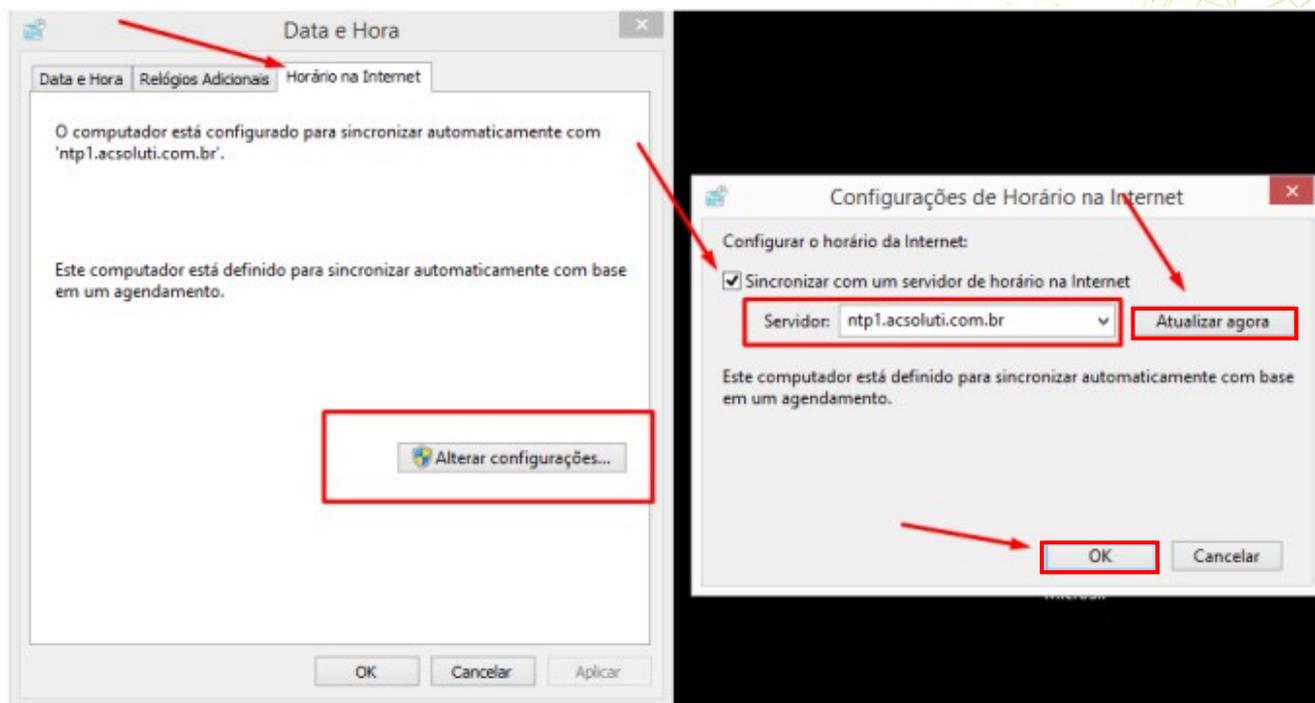
OK Cancelar Aplicar

4.10. Serviço NTP

Configure o relógio para sincronizar horário com o servidor da AC ntp1.acsoluti.com.br ou ntp2.acsoluti.com.br.

Acesse o caminho: Painel de Controle > Relógio e Região > Definir a hora e a data > Horário da Internet > Alterar configurações.

Continua na próxima página...



4.11. Antivírus

Deve possuir um antivírus de qualidade em cada estação. Caso não tenha adquirido algum antivírus, poderá utilizar o Windows Defender.

Obs.: O antivírus deve ser ativado e se manter sempre atualizado com a vacina mais atual.

Segurança em um relance

Veja o que está acontecendo com a segurança e a integridade do seu dispositivo e execute as ações necessárias.



Proteção contra vírus e ameaças
Nenhuma ação necessária.



Proteção de contas
Nenhuma ação necessária.



Firewall e proteção de rede
Nenhuma ação necessária.



Controle de aplicativos e do navegador
Nenhuma ação necessária.



Segurança do dispositivo
Exibir status e gerenciar recursos de segurança de hardware



Desempenho e integridade do dispositivo
Nenhuma ação necessária.

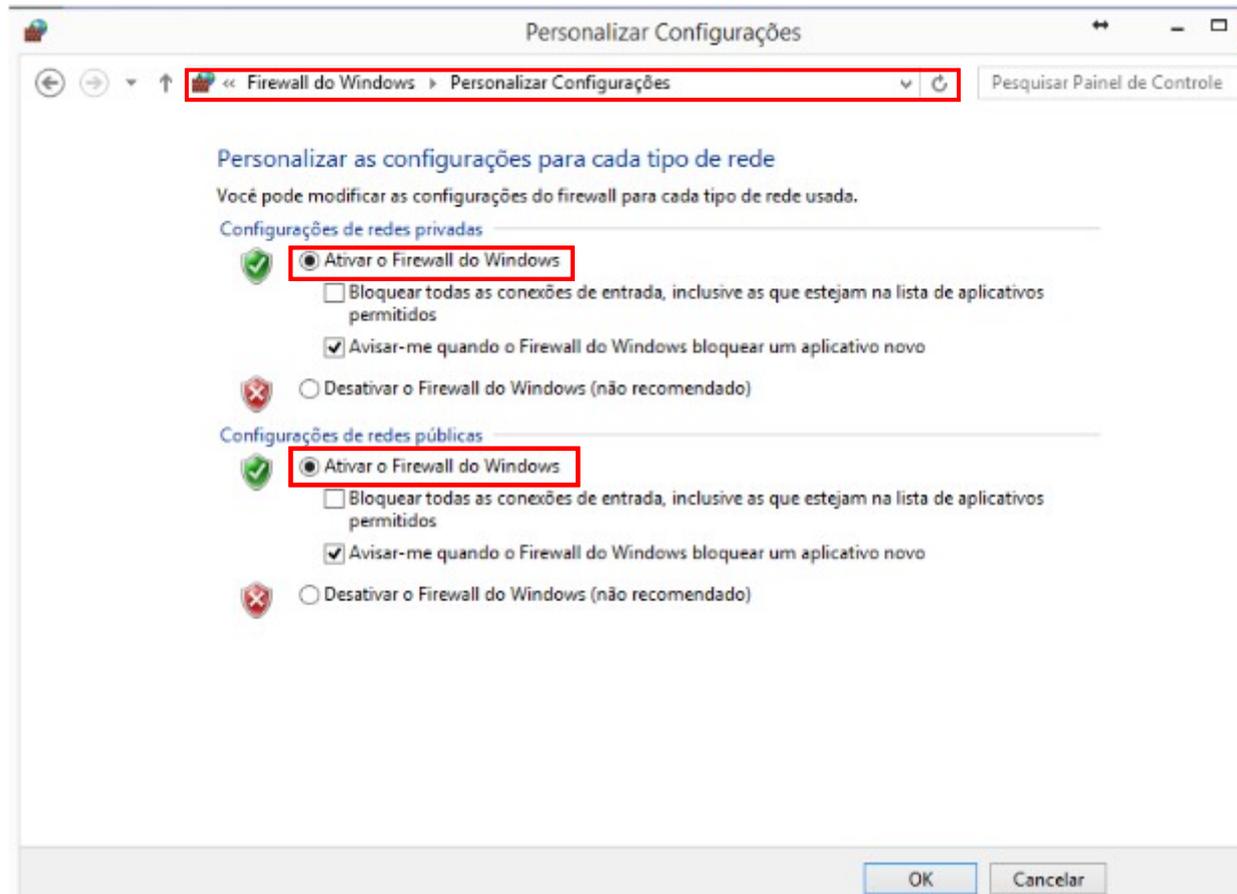


Opções da família
Gerencie o modo como sua família usa os dispositivos.

4.12. Firewall

Verifique se o Firewall do Windows está habilitado.

Acesse o Painel de Controle > Sistemas e segurança > Firewall do Windows > Ativar e Desativar o Firewall do Windows.



4.13. Atualizações do Windows

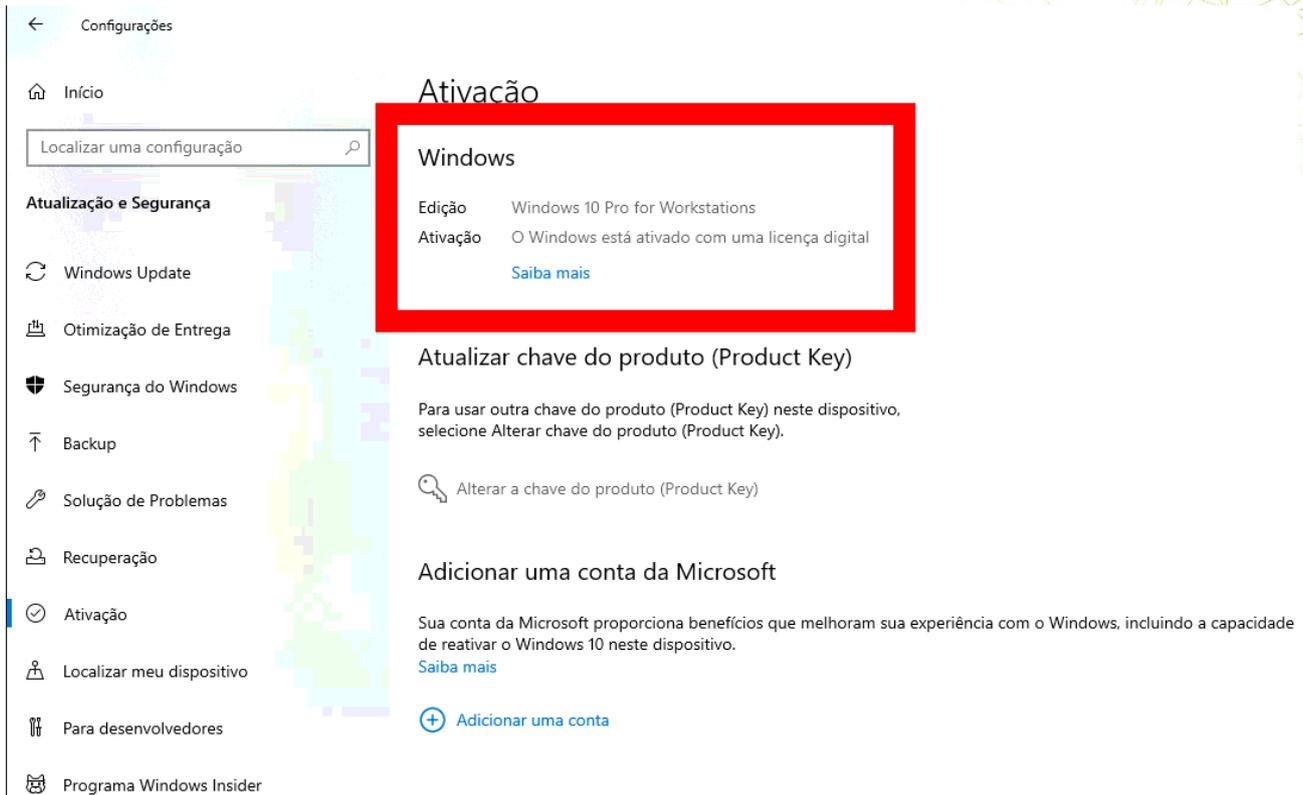
Certifique-se que o Windows esteja sempre atualizado!

4.14. Software autêntico

A licença do Windows instalado deve ser genuína, não deve ser utilizado nenhum software pirata.

Acesse o Painel de Controle > Sistema e segurança > Sistema > Alterar chave do produto (Product Key) ou atualizar a edição do Windows.

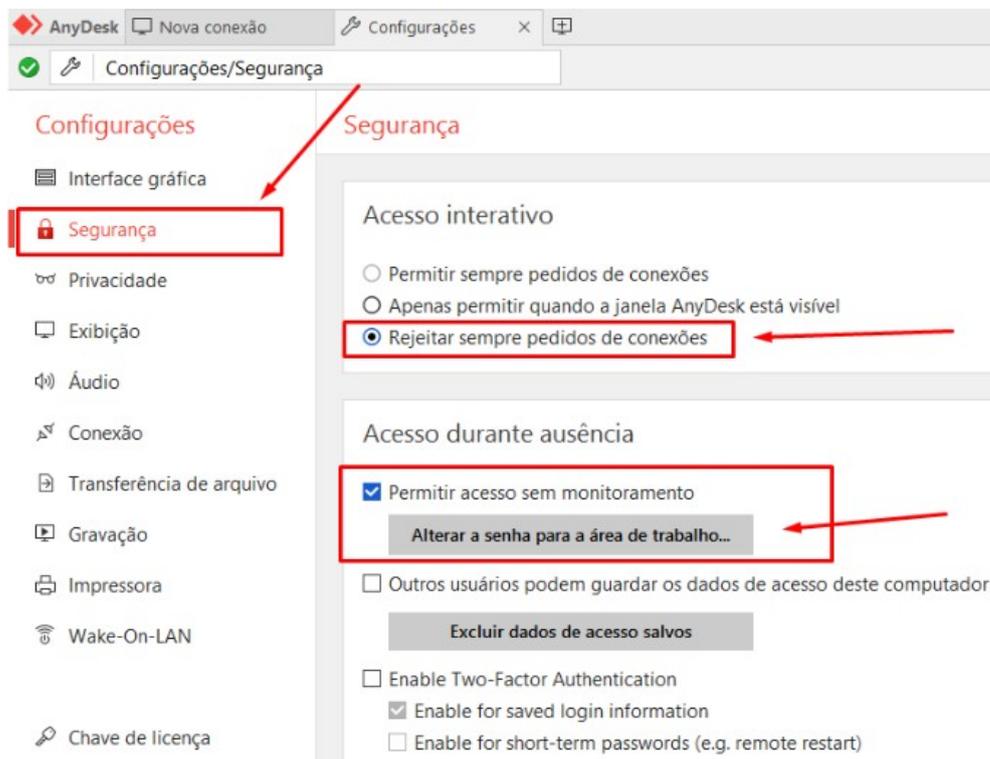
Continua na próxima página...



4.15. Acesso remoto

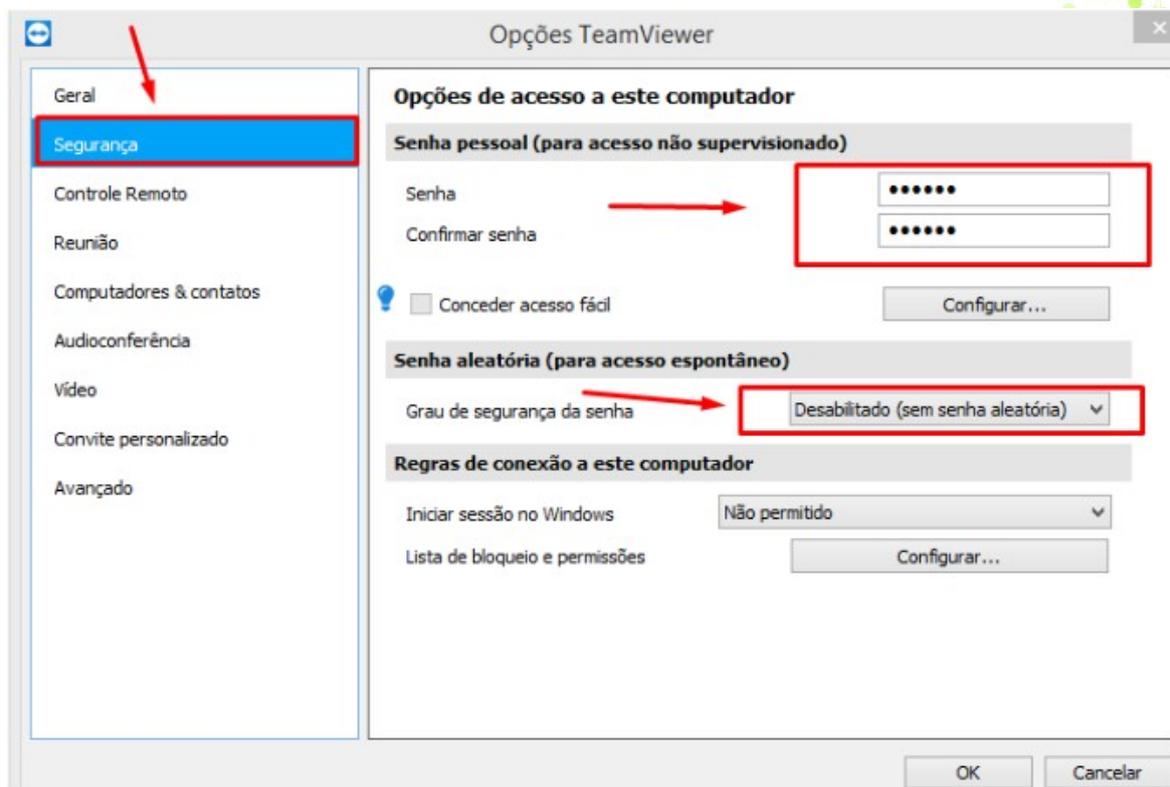
O acesso remoto às estações de trabalho deve ser feito somente para suporte técnico se necessário, definindo uma senha e limitando o acesso a usuários que não a possuem.

Exemplo Anydesk:



Continua na próxima página...

Exemplo Teamviewer:



HISTÓRICO DE REVISÕES

VERSÃO	DATA	DESCRIÇÃO DA REVISÃO	RESPONSÁVEL	ÁREA/DPTO
1	19/05/2015	- Versão inicial;	Jessé	Suporte
2	20/09/2016	- Alteração nas informações;	Marcos Marques Pícolo Júnior	Suporte AR's
3	14/08/2019	- Alteração de conteúdo no documento;	Marcos Marques Pícolo Júnior	Suporte AR's
4	14/08/2019	- Alteração de Layout;	Marcos Marques Pícolo Júnior	Suporte AR's
5	11/03/2021	- Atualização total de conteúdo do DOC;	Wincius Leal	Infraestrutura
6	26/05/2022	- Alteração de conteúdo no documento;	Igor Ferreira de Jesus Pereira	Infraestrutura
7	31/05/2022	- Adição de configuração BitLocker;	Igor Ferreira de Jesus Pereira	Infraestrutura

<small>REVISOR(ES):</small> IGOR FERREIRA DE JESUS PEREIRA	<small>DATA:</small> 31/05/2022	
<small>APROVADOR(ES):</small> MARCOS MARQUES PICOLO JUNIOR	<small>DATA:</small> 31/05/2022	