

GUIA COMPLETO

Configuração de Computador de AR

INFORMAÇÕES

Cliente: ACERTSIS
Tipo de Documento: Guia
Última Revisão: 28/07/2022
Versão do Template: 1.0

ÍNDICE GERAL

1	Apresentação.....	3
2	Verificando ativação do Windows.....	4
3	Cadastrando o computador no TeamViewer.....	5
4	Alterando o nome do computador	14
5	Criando Contas de Usuário	17
6	Aplicativos a instalar	28
6.1	OCS.....	28
6.2	Gerenciadores de Certificados.....	31
6.3	Drivers de dispositivos	31
6.4	Complementos do Windows	31
6.4.1	Editor de Política de Grupo	31
6.4.2	Pacotes de Redistribuíveis do Visual C++.....	32
7	Cadeias de Certificados	33
8	Políticas de segurança	38
9	Sincronia da Data e Hora	45
10	Configurando o perfil do usuário	47
10.1	BG Info	48
10.2	Device Server.....	49
10.3	SPID Client.....	51
10.4	Navegadores e Favoritos	53
10.4.1	Google Chrome.....	54
10.4.2	Mozilla Firefox.....	57
11	Antivírus	64
12	Criptografia	65
12.1	BitLocker	65
12.2	VeraCrypt	69
13	Padrão de Nomenclatura.....	81
13.1	Hostnames	81
13.2	Grupos de Trabalho	82
14	Comandos recorrentes	83
14.1	Prompt de comandos	83
14.2	Teclas de Atalho.....	83
14.3	Consoles	84
14.4	Endereços comuns no Windows Explorer	86
15	Links	87
15.1	Diretórios no SharePoint	87
16	Glossário.....	88
17	Histórico da Revisão.....	89

1 Apresentação

O guia a seguir apresenta passo a passo como instalar diversas aplicações utilizados na AC Digital, mas tem como objetivo guiar a forma de configuração para configurar o computador de atendimento numa Agência de Registro.

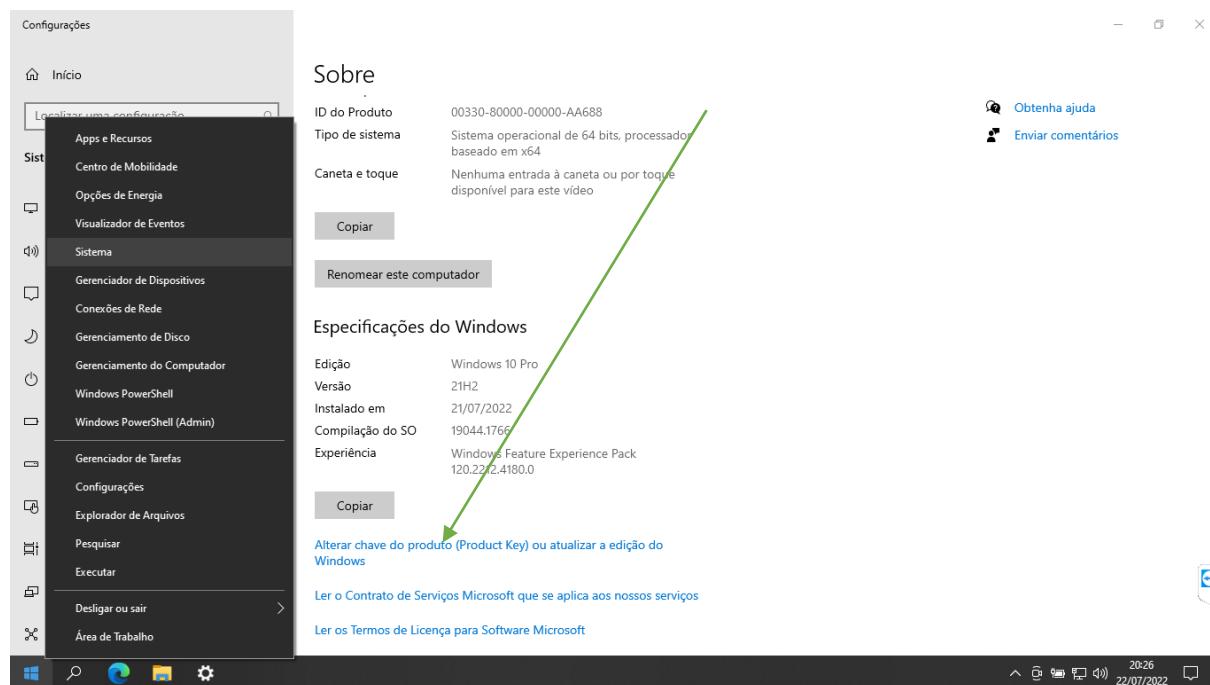
Há várias regras explicadas durante o guia, havendo um padrão facilmente identificável para se obedecer.

Muito do conteúdo deste guia, está presente na [Wiki](#) do canal Configuração para AGR da equipe do Suporte Técnico.

Fique atento!

2 Verificando ativação do Windows

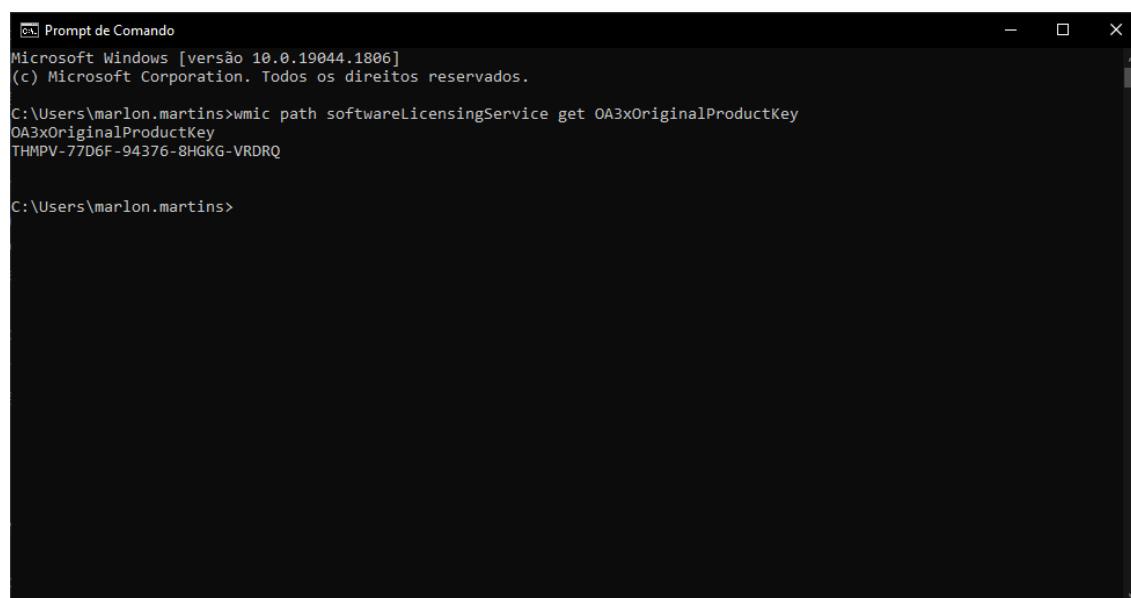
Após o responsável pelo computador na AR enviar a ID e senha do TeamViewer, executado como administrador, verifique se o computador possui chave original do Windows. Este procedimento pode ser feito verificando as informações do sistema clicando com o **botão direito** no Menu Iniciar e após em **Sistema** ou pressionando **WINKEY+PAUSE** e acessando o menu **Alterar chave do produto** (imagem),



ou executando o seguinte comando:

```
wmic path softwareLicensingService get OA3xOriginalProductKey
```

Este comando informa a chave utilizada no sistema:



```
C:\Prompt de Comando
Microsoft Windows [versão 10.0.19044.1806]
(c) Microsoft Corporation. Todos os direitos reservados.

C:\Users\marlon.martins>wmic path softwareLicensingService get OA3xOriginalProductKey
THMPV-77D6F-94376-8HGKG-VRDRQ

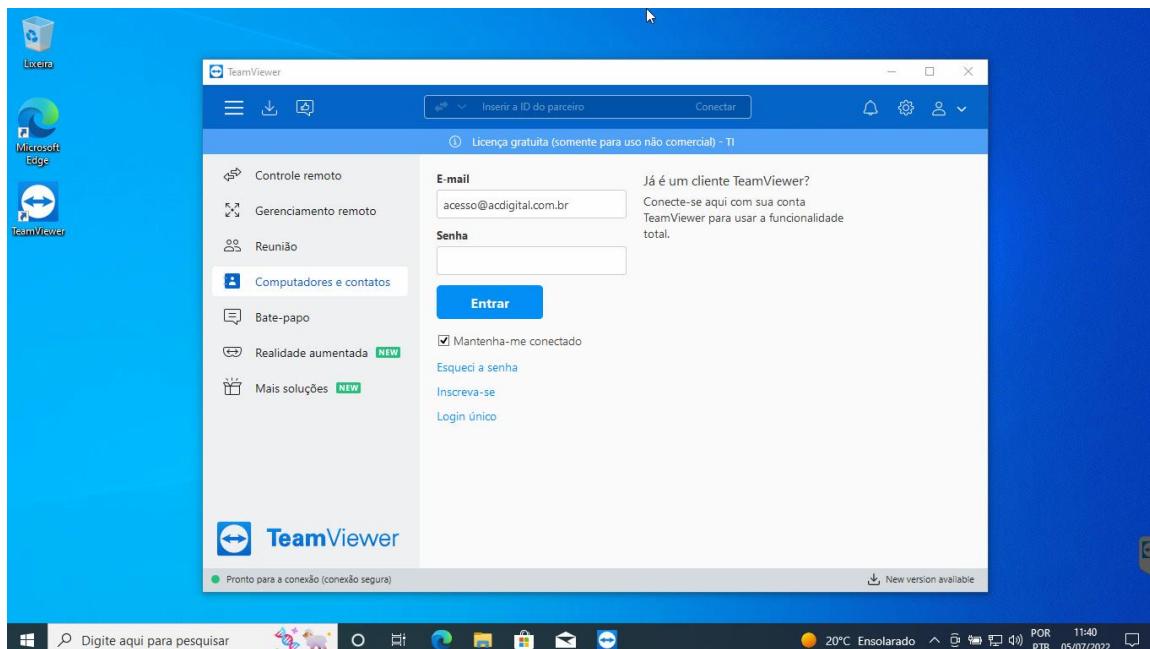
C:\Users\marlon.martins>
```

Se não houver uma chave original válida para o computador, a configuração não deve proceder e a AR deve ser informada da necessidade da ativação do sistema operacional.

3 Cadastrando o computador no TeamViewer

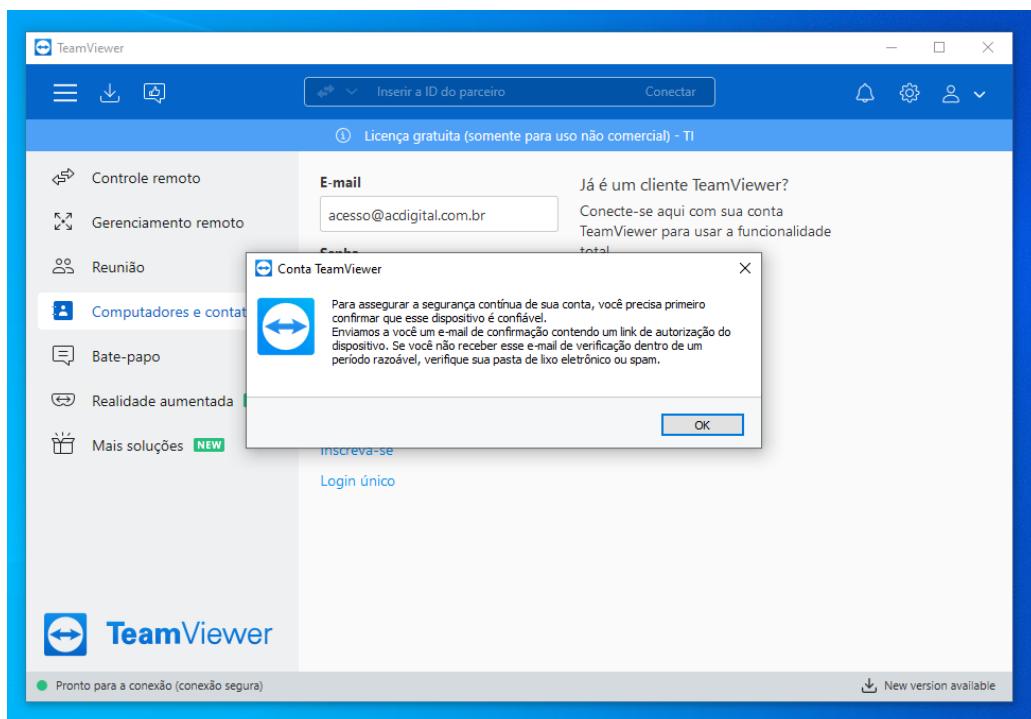
Estando o sistema operacional ativado com uma licença original, já vamos cadastrar o equipamento no TeamViewer conforme o procedimento a seguir para não se perder o acesso remoto durante a configuração, lembrando que o aplicativo deve ser aberto como administrador.

Acessando o computador remoto, abra o TeamViewer no menu **Computadores e contatos**, acesse com a credencial **acesso@acdigital.com.br***. A senha está no [SysPass](#).

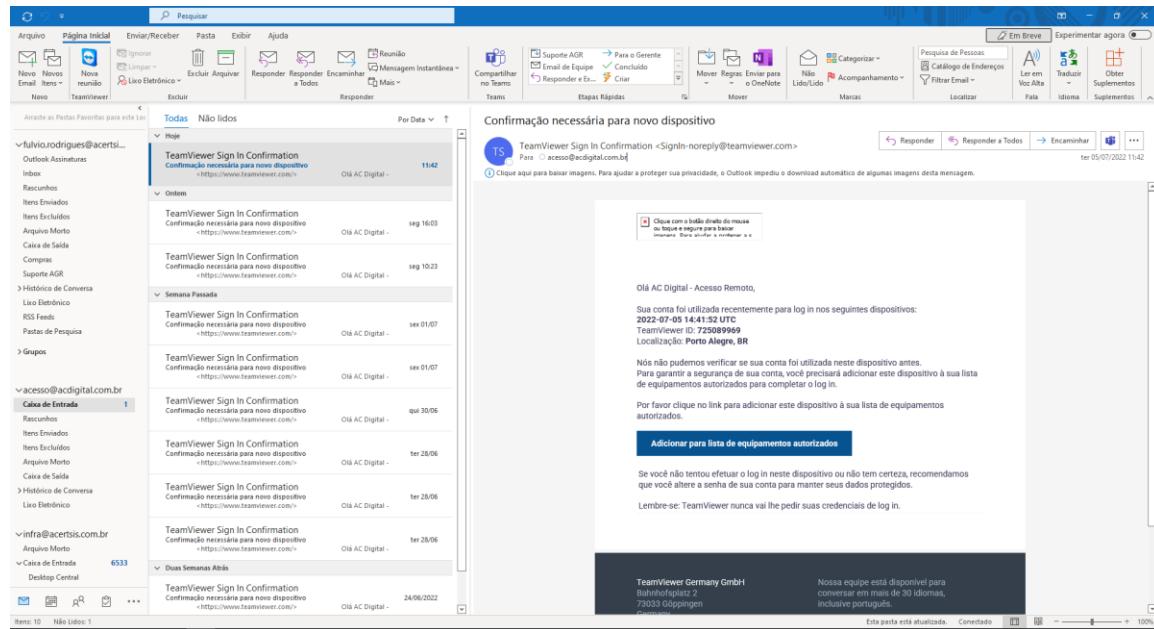


***Esta credencial é apenas para o cadastro. Não deve jamais ser utilizada para realizar acessos ou atendimentos!**

Na primeira tentativa de login, será exibido o seguinte aviso:



Sendo então enviado para a caixa de entrada do e-mail desta conta o link de confirmação para permitir o login.

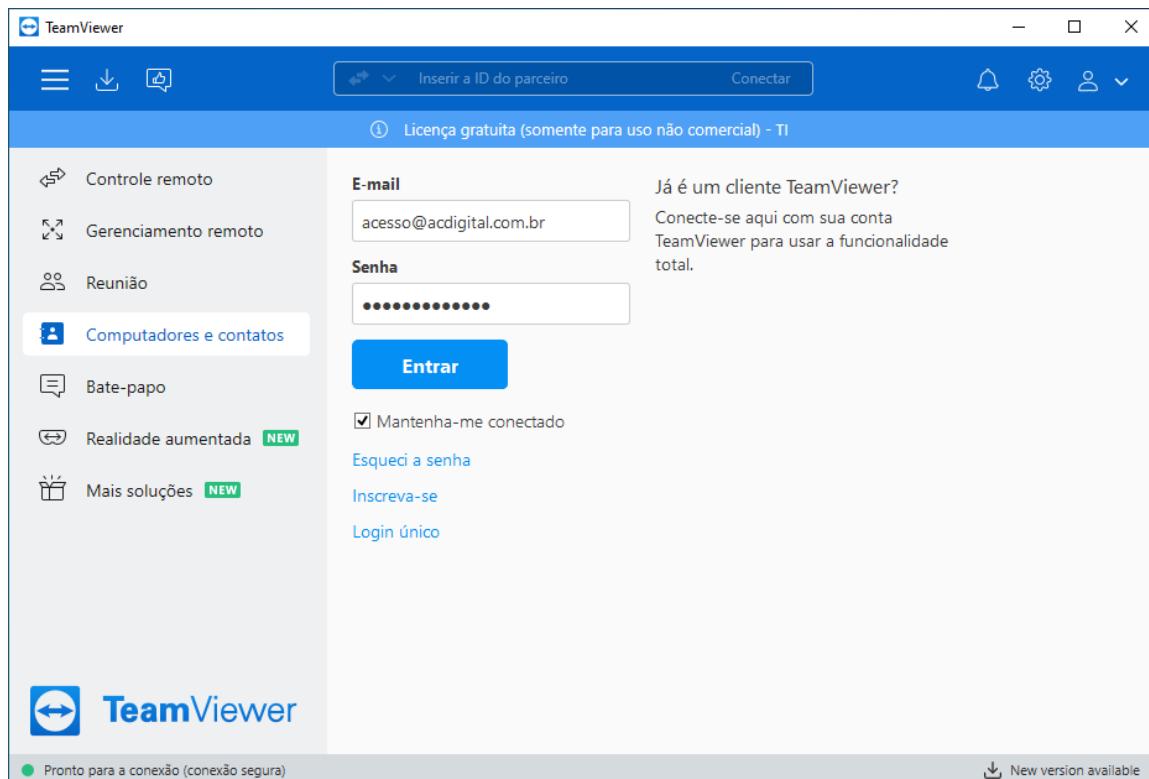
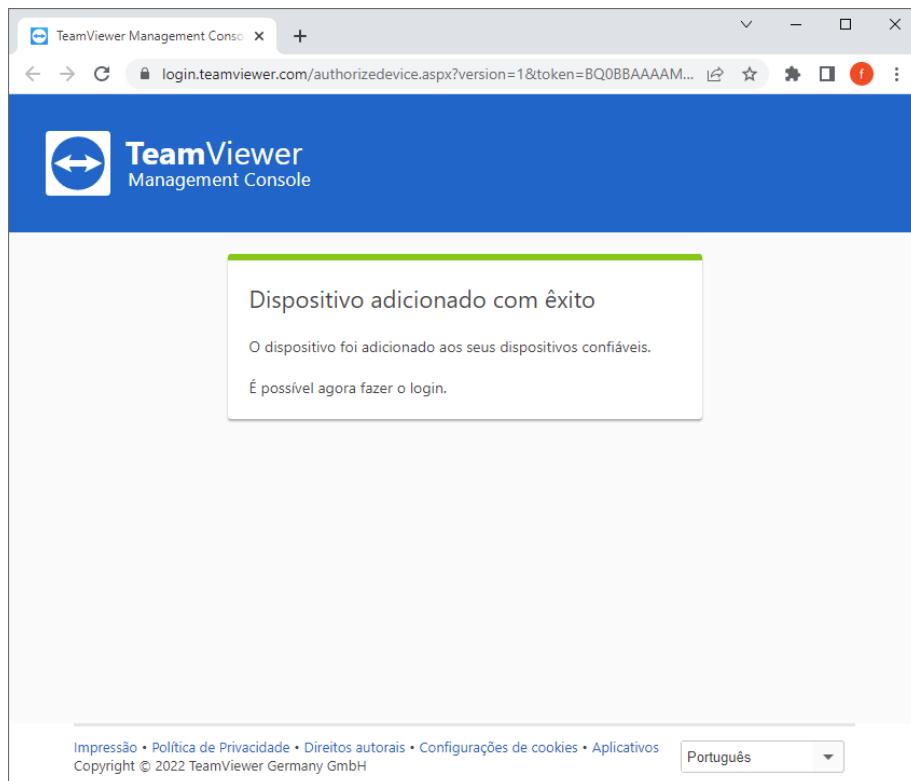


Clique em **Adicionar para a lista de equipamentos autorizados**. Será aberto o link onde você vai autorizar:

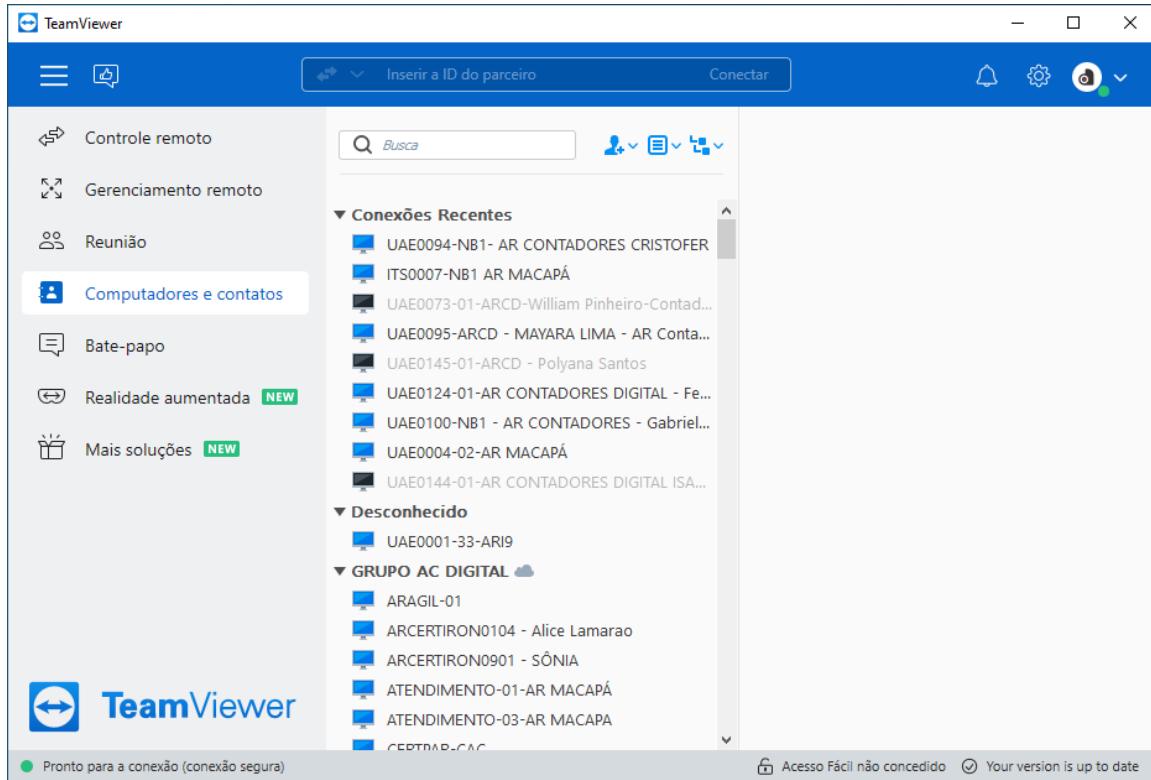
The screenshot shows a browser window for the "TeamViewer Management Console" at login.teamviewer.com/authorizeddevice.aspx?version=1&ttoken=BQ0BAAAAM.... A modal dialog box displays the message: "Sua conta foi usada para fazer o login com êxito no seguinte dispositivo:" followed by the date and time "ter 05 jul 2022 2:41 UTC", the "ID do TeamViewer: 725 089 969", the "IP Address: 200.182.176.50", and the "Local (aproximado): Porto Alegre, BR". It also states: "Não foi possível verificar se sua conta foi usada neste dispositivo anteriormente." Below this, a question asks: "Você deseja confiar nesse dispositivo ou no endereço IP permanentemente?", with options "Sim, esse dispositivo" (selected), "Confiável" (button), and "Recusar". At the bottom, a link "O que são dispositivos confiáveis?" is visible.

Clique em **Confiável** e o computador estará autorizado a efetuar login com esta conta. Acesse novamente com a conta **acesso@acdigital.com.br** e senha, para listar os computadores cadastrados e possibilitar o cadastro deste.

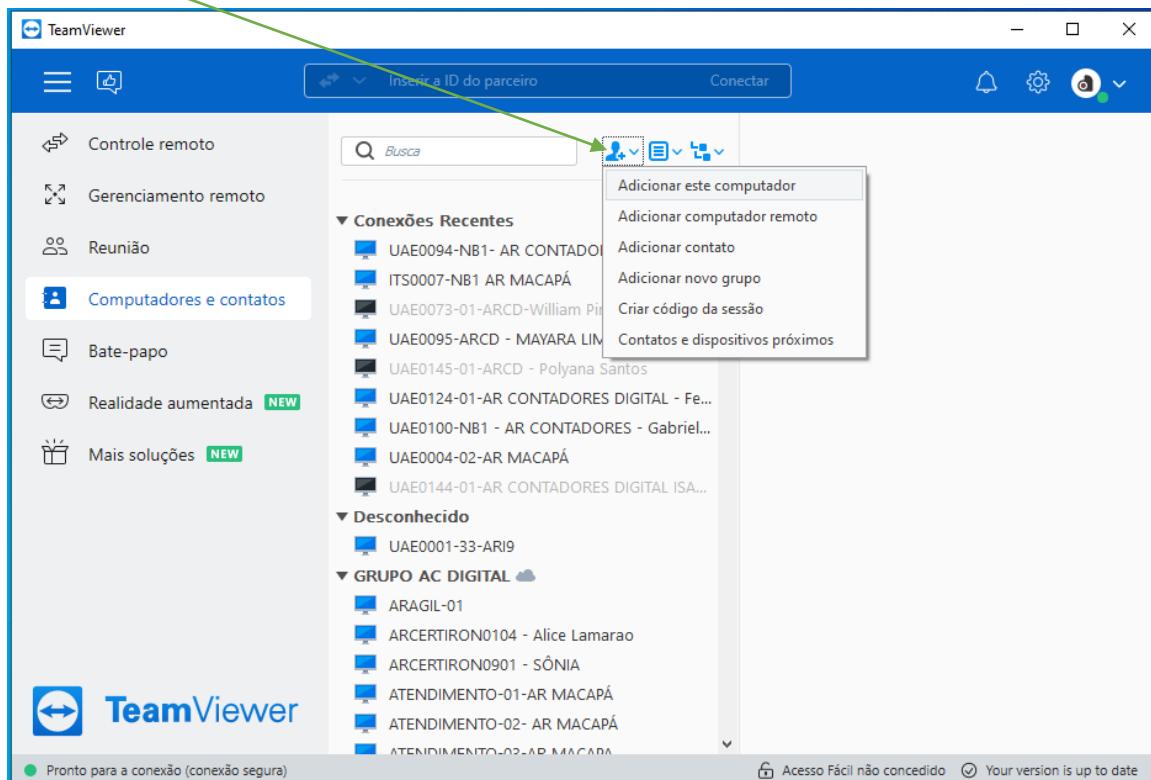




A tela exibida será a seguinte:

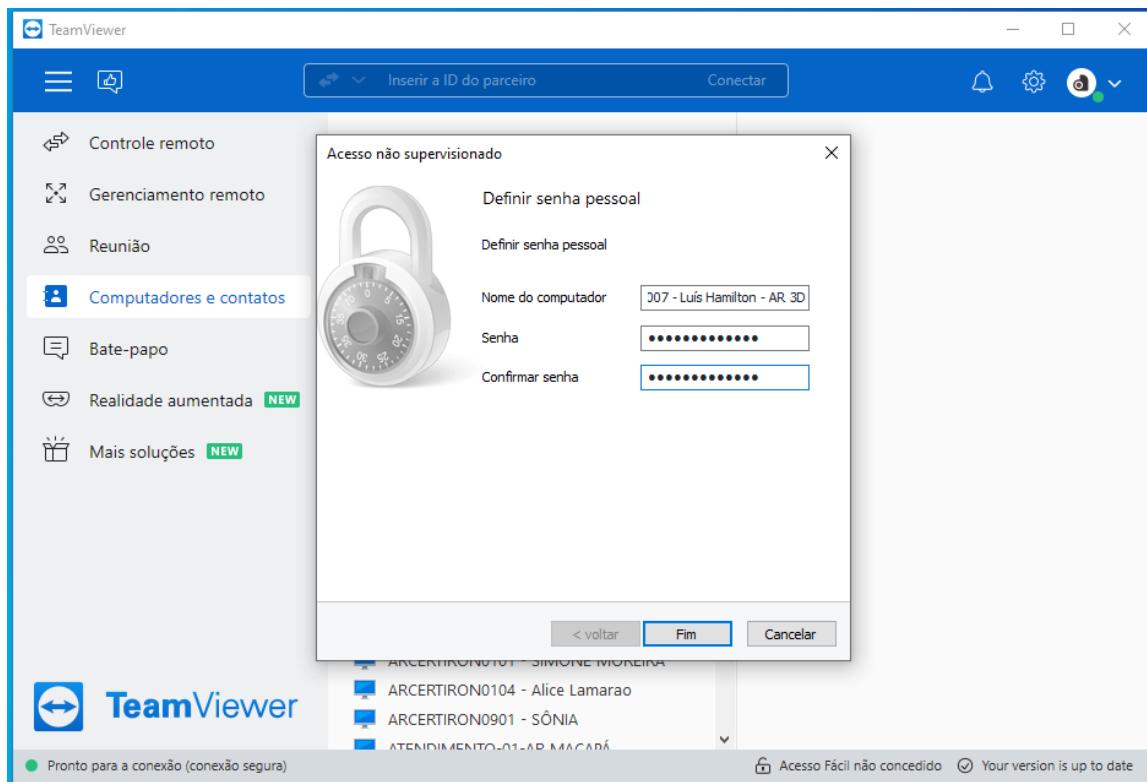


Clique em  e após clique em Adicionar este computador.

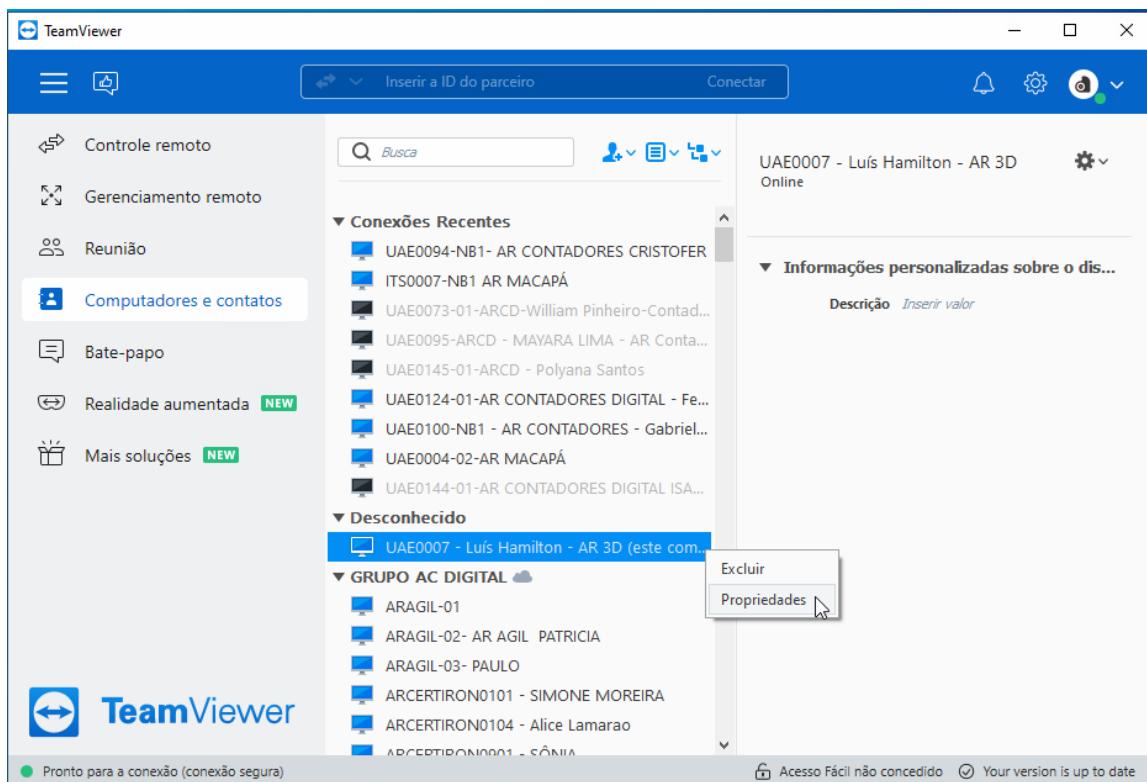


Nesta etapa, cadastre de acordo com o seguinte padrão: **HOSTNAME – Nome da AGR – Nome da Loja.**

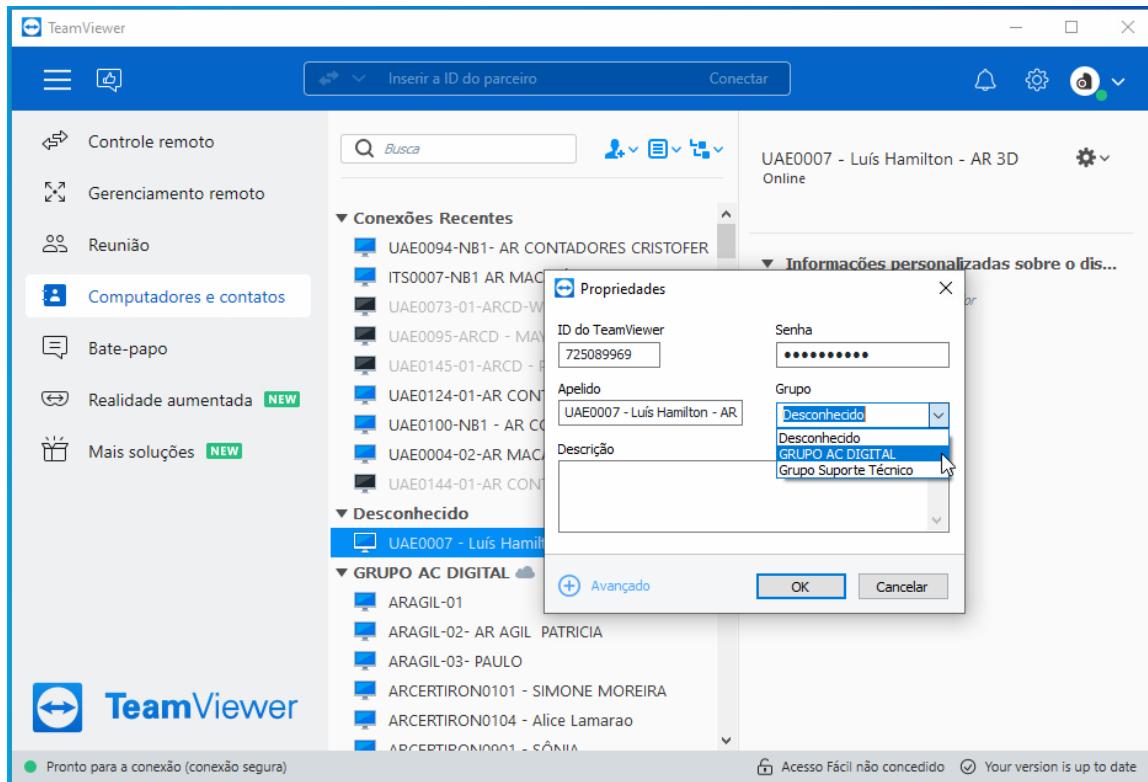
O hostname já deve estar definido de acordo com o padrão de nomenclaturas ([disponível também na Wiki](#)).



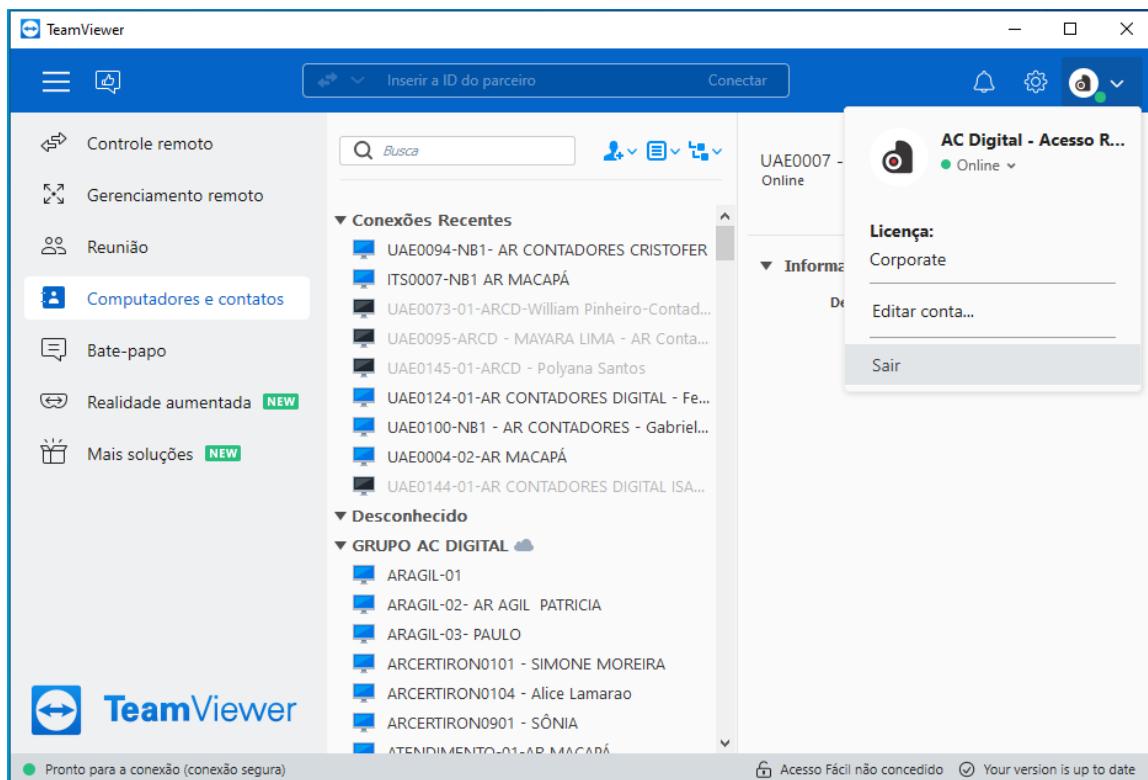
Clique em **Fim** e após clique com o botão direito no computador cadastrado e clique em **Propriedades**.



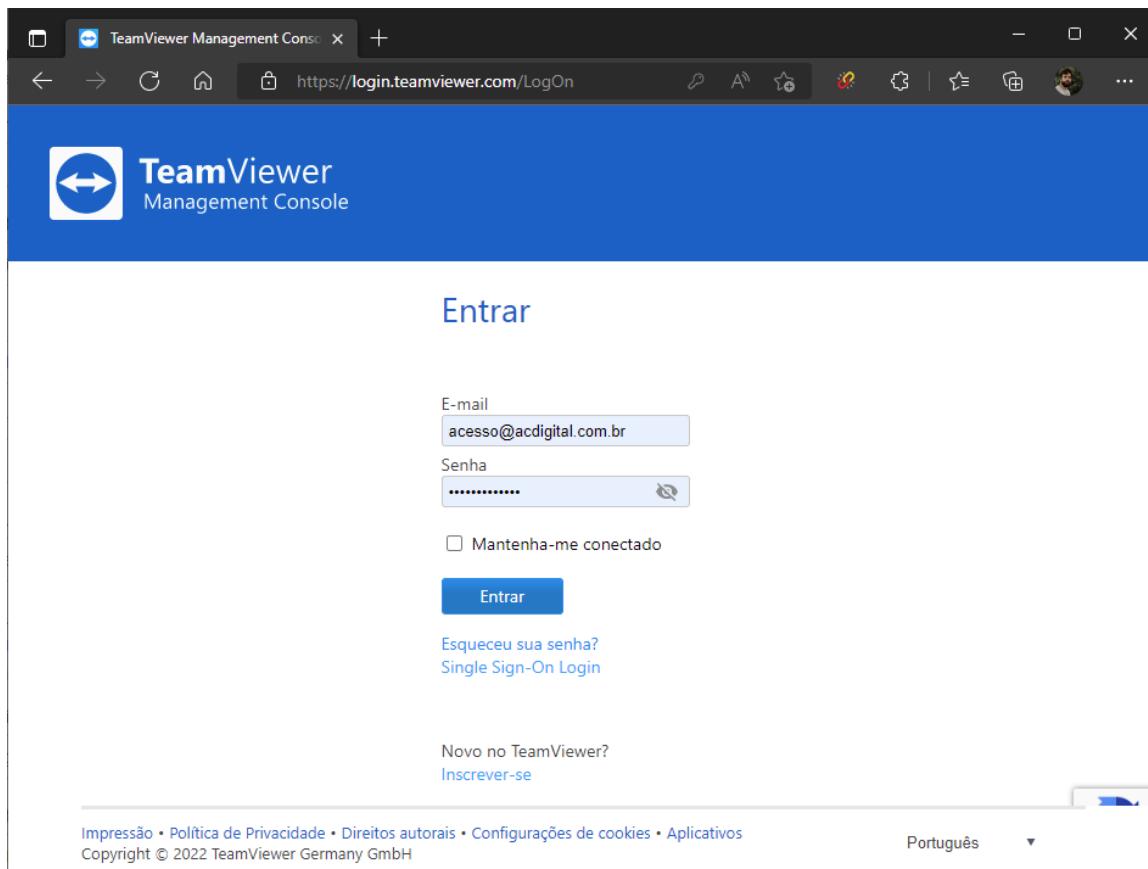
Nas propriedades, altere o grupo para **GRUPO AC DIGITAL** e clique em **OK**.



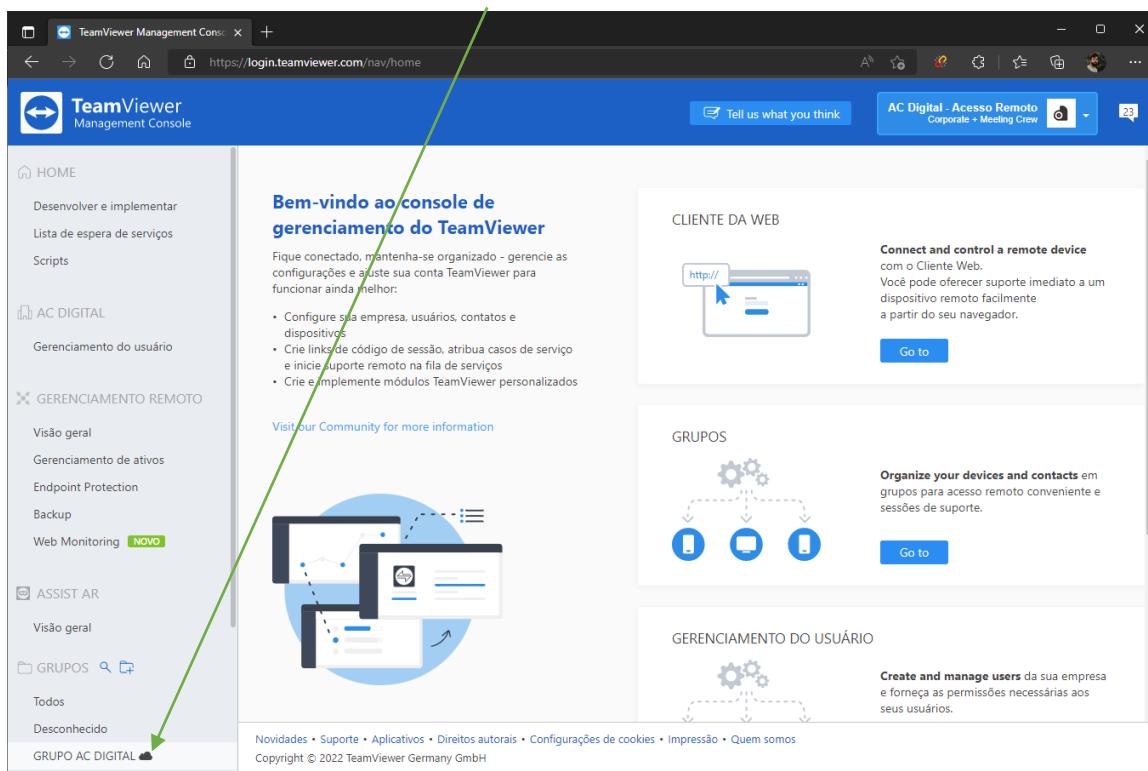
Após cadastrar, clique no menu do perfil e saia da conta clicando em **Sair**.



Após o cadastro, vamos importar as políticas do aplicativo no console do TeamViewer na web. Acesse login.teamviewer.com com as mesmas credenciais (acesso@acdigital.com.br).

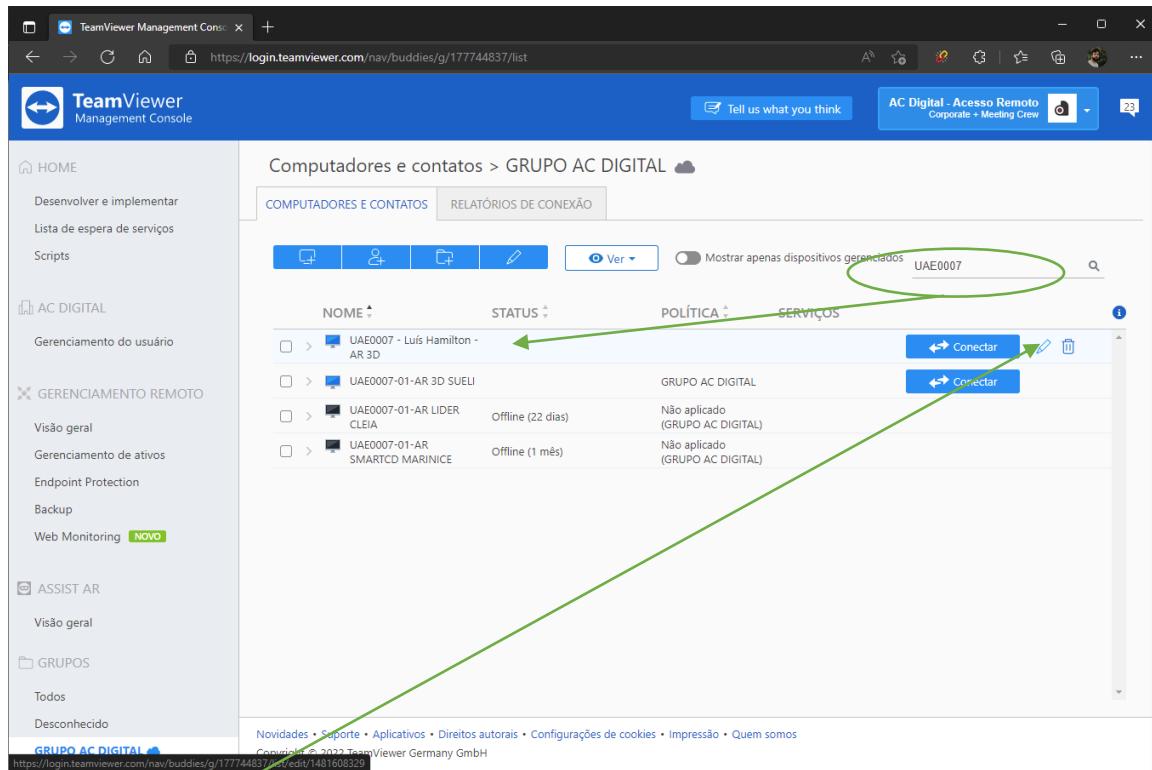


No console na web, clique no **GRUPO AC DIGITAL** no canto inferior esquerdo da tela.



The screenshot shows the TeamViewer Management Console interface. On the left, there's a sidebar with navigation links like 'HOME', 'AC DIGITAL', 'GERENCIAMENTO REMOTO', 'ASSIST AR', and 'GRUPOS'. The 'GRUPOS' section has a link labeled 'GRUPO AC DIGITAL'. The main content area is titled 'Bem-vindo ao console de gerenciamento do TeamViewer' and contains sections for 'CLIENTE DA WEB', 'GRUPOS', and 'GERENCIAMENTO DO USUÁRIO'.

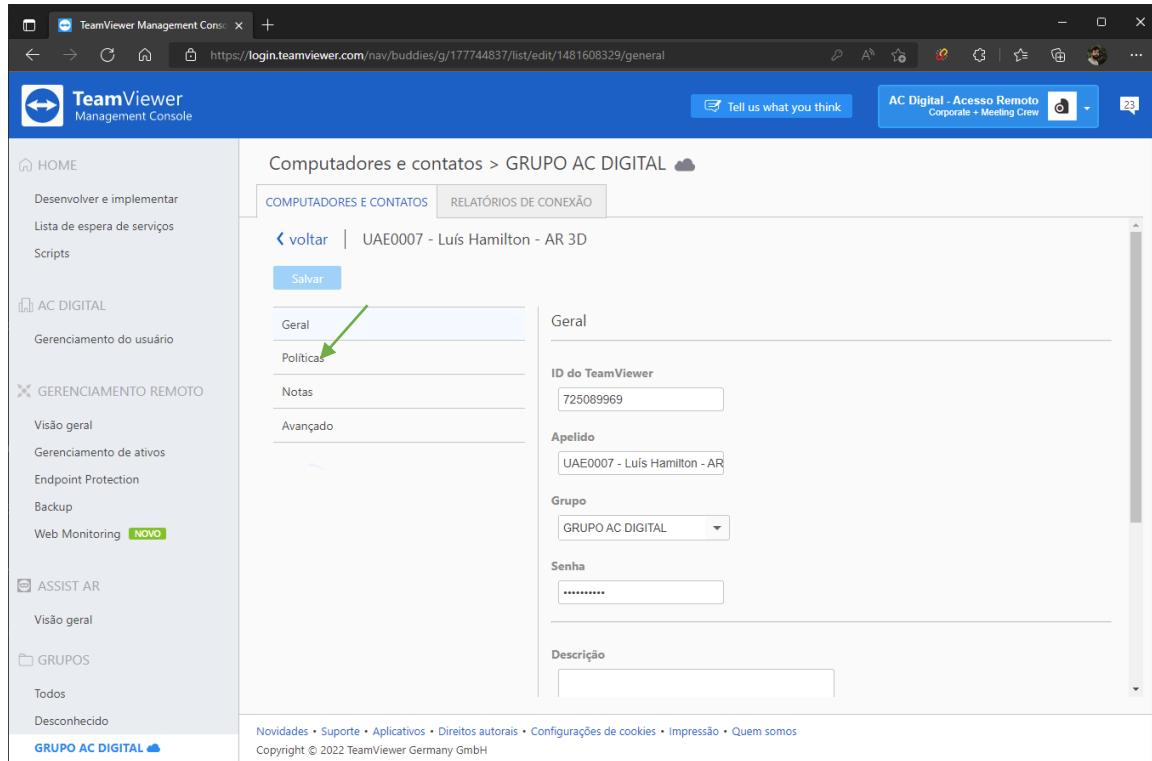
Na caixa de pesquisa, procure o computador que você acaba de cadastrar.



Computadores e contatos > GRUPO AC DIGITAL

NOME	STATUS	POLÍTICA	SERVIÇOS
UAE0007 - Luis Hamilton - AR 3D	Online	GRUPO AC DIGITAL	
UAE0007-01-AR 3D SUELI	Online	Não aplicado (GRUPO AC DIGITAL)	
UAE0007-01-AR LIDER CLEIA	Offline (22 dias)	Não aplicado (GRUPO AC DIGITAL)	
UAE0007-01-AR SMARTCD MARINICE	Offline (1 mês)	Não aplicado (GRUPO AC DIGITAL)	

Clique então em ao lado do computador cadastrado para editar a política. Após, clique em **Políticas**.

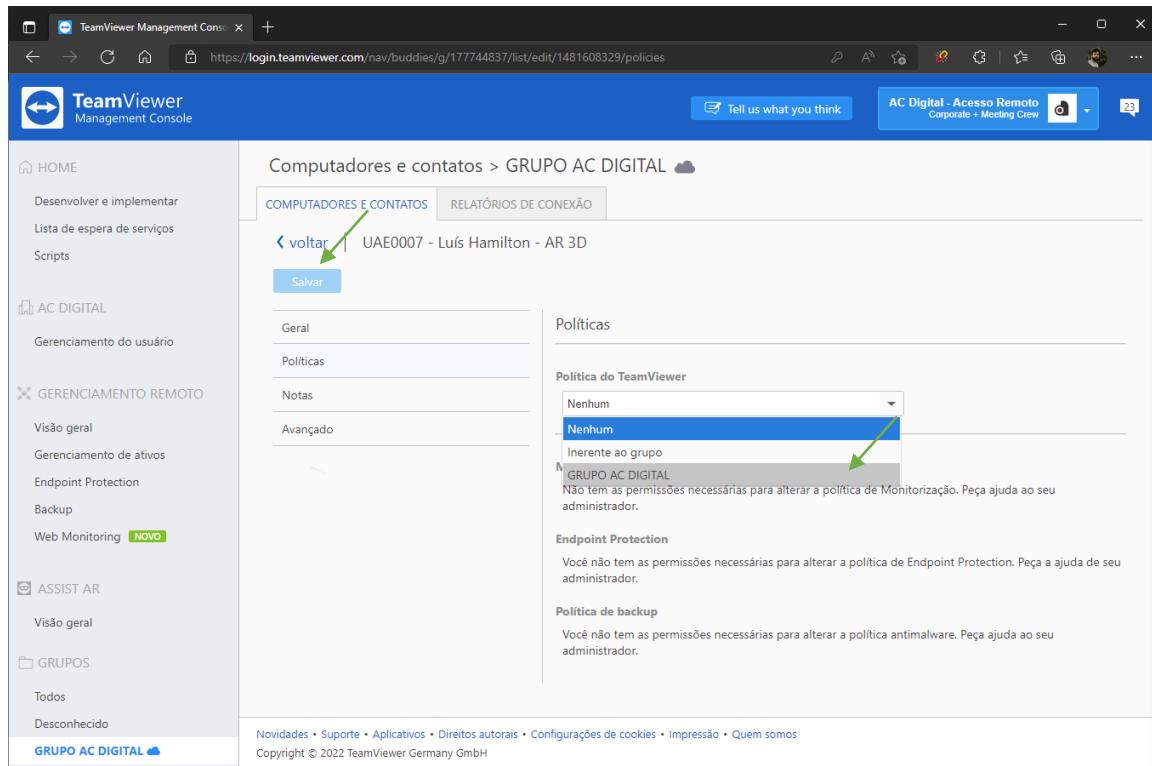


Computadores e contatos > GRUPO AC DIGITAL

UAE0007 - Luis Hamilton - AR 3D

Políticas

Altere a política para **GRUPO AC DIGITAL** e clique em **Salvar**.

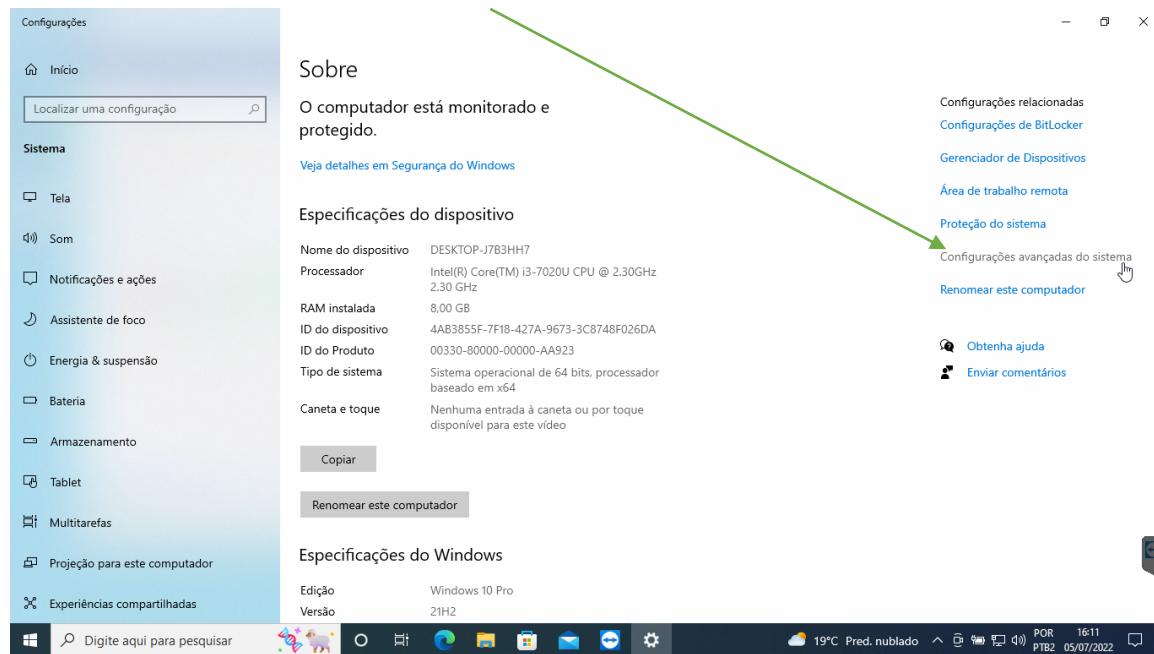


The screenshot shows the TeamViewer Management Console interface. On the left, there's a sidebar with categories like HOME, AC DIGITAL, GERENCIAMENTO REMOTO, ASSIST AR, GRUPOS, and GRUPO AC DIGITAL. The main area is titled 'Computadores e contatos > GRUPO AC DIGITAL'. It has tabs for 'COMPUTADORES E CONTATOS' and 'RELATÓRIOS DE CONEXÃO'. Below the tabs, there's a 'voltar' button and a 'Salvar' button. The 'Políticas' section contains a dropdown menu with options: 'Nenhum', 'Inerente ao grupo', and 'GRUPO AC DIGITAL'. The 'GRUPO AC DIGITAL' option is highlighted with a blue background and white text. To the right of the dropdown, there are sections for 'Política do TeamViewer', 'Endpoint Protection', and 'Política de backup', each with a note about permissions.

Feito isso, o computador está cadastrado no TeamViewer, com as políticas aplicadas, que forçam o aplicativo a iniciar junto com o sistema e impede o usuário de encerrar o processo, facilitando o acesso remoto com permissão de administrador.

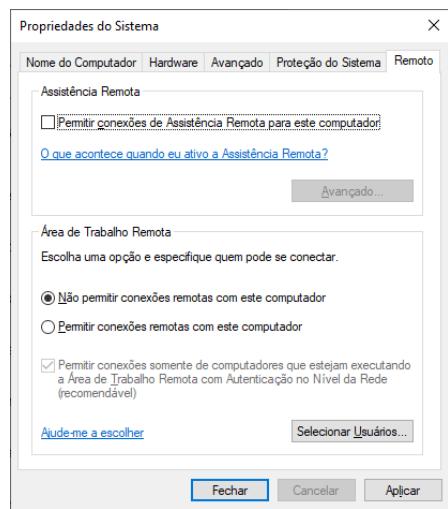
4 Alterando o nome do computador

Acesse as propriedades do Sistema pressionando **WINKEY+PAUSE** para mudar o hostname. Clique em **Configurações avançadas do sistema**.



Clique na aba **Remoto** e desmarque a opção **Permitir conexões de Assistência Remota para este computador** e garanta que a opção **Não permitir conexões remotas com este computador** esteja marcada.

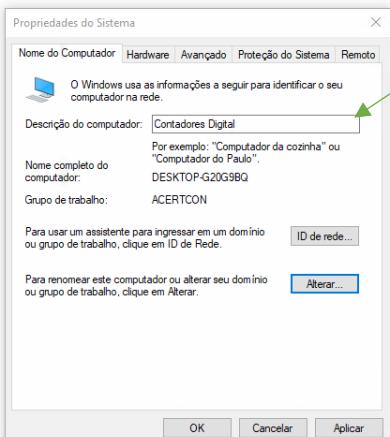
Após, clique na aba **Nome do Computador**.



Nesta etapa, siga os [padrões de nomenclatura](#).

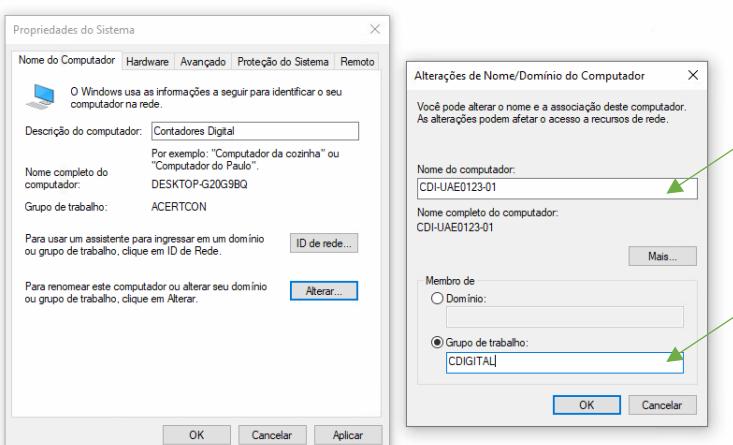
No campo **Descrição do Computador**, digite o **nome da loja**.

Clique em **Alterar**.

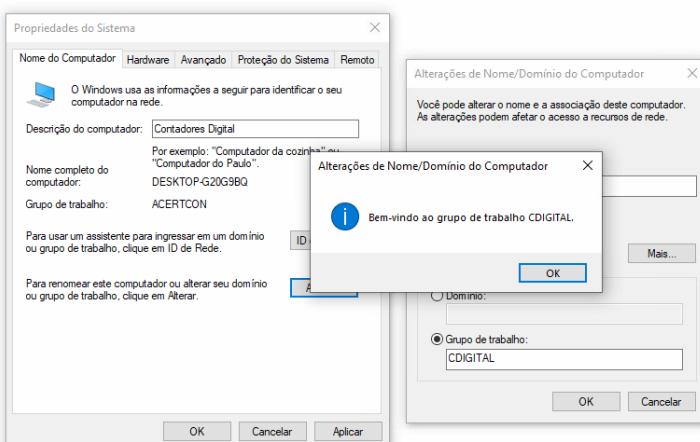


No campo **Nome do computador** digite o **HOSTNAME**.

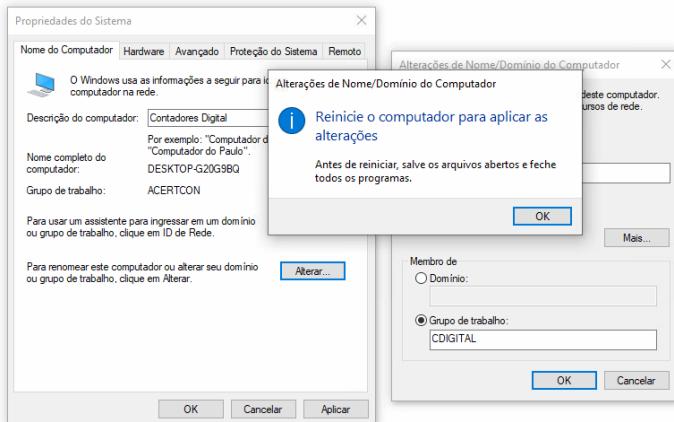
No campo **Grupo de trabalho** digite o **WORKGROUP** e clique em **OK**.



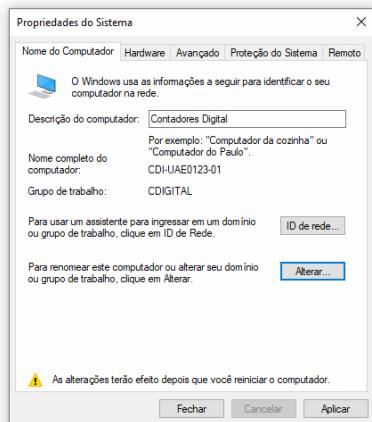
Clique em **OK**.



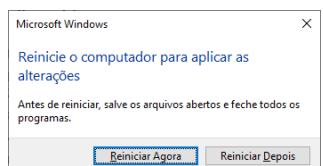
Clique em **OK**.



Clique em **Aplicar** e será solicitado reiniciar o computador.



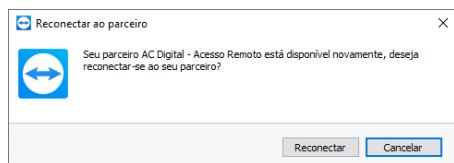
Clique em **Reiniciar Agora**.



O TeamViewer poderá questionar se você deseja retomar a conexão após o reinício. Clique em **Esperar por parceiro** para reconectar quando o computador reiniciar.



Quando reiniciar, será exibido o menu seguinte. Clique em **Reconectar**.



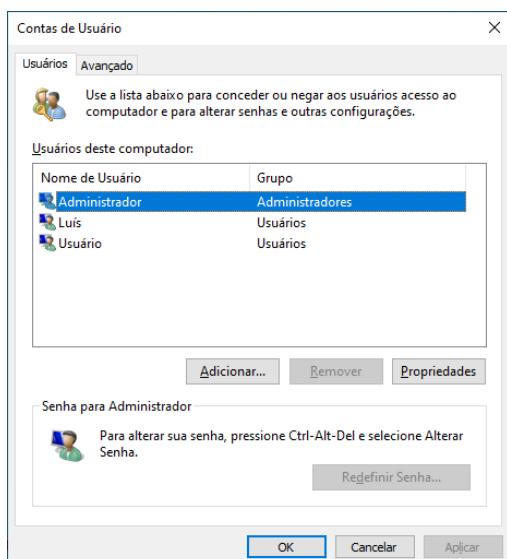
Caso não ocorra essa reconexão automática, busque o computador na aba **Computadores e contatos** do seu TeamViewer e acesse novamente para prosseguir.

5 Criando Contas de Usuário

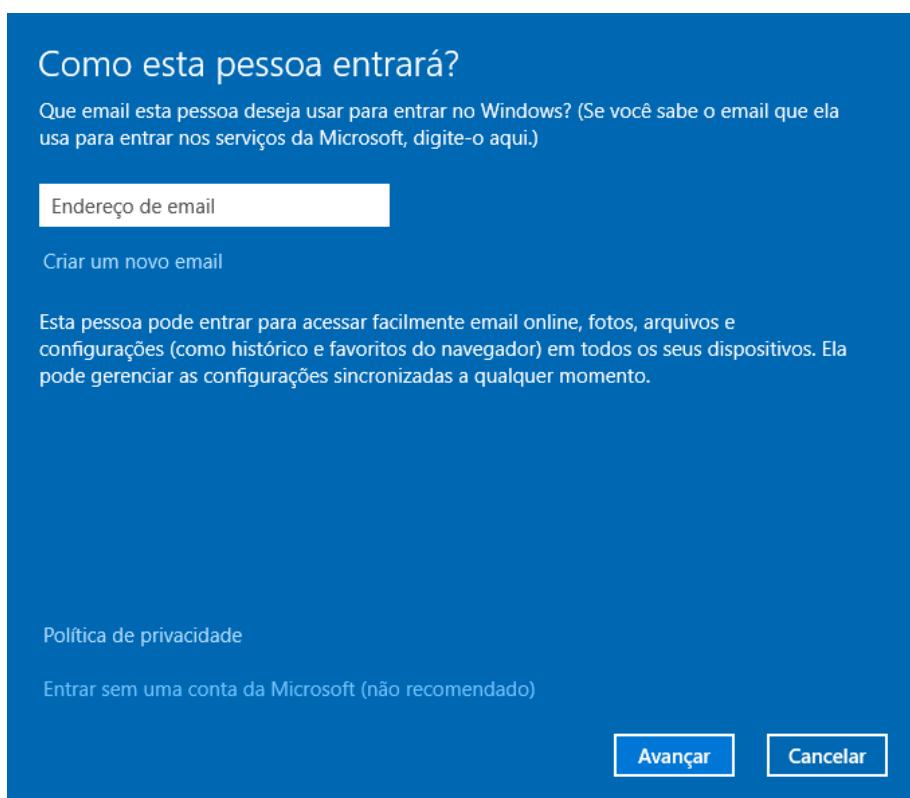
Vamos criar a conta de usuário administrador para seguir a configuração e a conta de usuário do AGR para sua futura utilização.

Execute o comando **NETPLWIZ** para abrir o painel de controle de contas de usuário.

Clique em **Adicionar** para criar a conta de usuário **Suporte**.



Clique em **Entrar sem uma conta Microsoft**.



Clique em **Conta local**.

➊ Adicionar um usuário

Há duas opções para entrar:

Conta da Microsoft

Entrar em computadores com seu endereço de email permite que você:

- Baixar aplicativos da Windows Store.
- Acessar seu conteúdo online nos aplicativos da Microsoft automaticamente.
- Sincronizar configurações online para que os computadores tenham a mesma aparência, como o histórico do navegador, a imagem da conta e as cores.

Conta local

Entrar em uma conta local significa:

- É necessário criar um nome de usuário e uma conta para cada computador que você usar.
- Você precisará de uma conta da Microsoft para baixar aplicativos, mas pode configurá-la mais tarde.
- Suas configurações não serão sincronizadas nos computadores que você usa.

Contas da Microsoft **Conta local** **Cancelar**

Preencha os campos com o nome do usuário **Suporte**, gere uma senha aleatória de 11 caracteres, **digite e repita a senha** e clique em **Avançar**. Você pode usar o [Gerador de Senhas do Norton](#).

➋ Adicionar um usuário

Escolha uma senha que seja fácil de lembrar, mas difícil de adivinhar. Se você esquecer, vamos mostrar a dica.

Nome do usuário	Suporte
Senha	•••••••••••
Confirmar senha	•••••••••••
Dica de senha	SysPass 

Avançar **Cancelar**

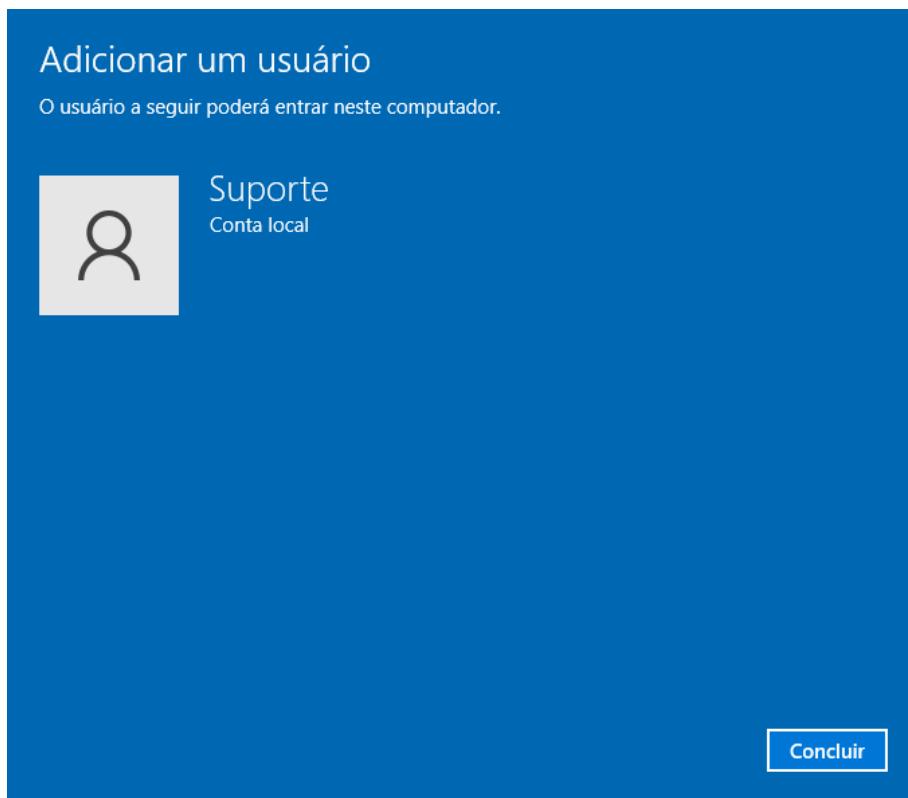


Cadastre a senha no [SysPass](#) conforme o padrão (vide documentação de cadastro de senha no SysPass)

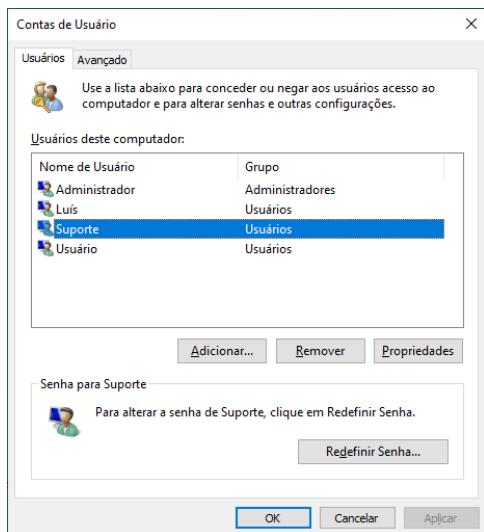
+ New Account

	ACCOUNT	PERMISSIONS
Name	Account name AR Poa - Andresa Vasques	
Client	AR POA	
Category	AGR	
URL / IP	Access URL or IP NBARPAAGR0835	
User	Access user Suporte	
Password	***** 	

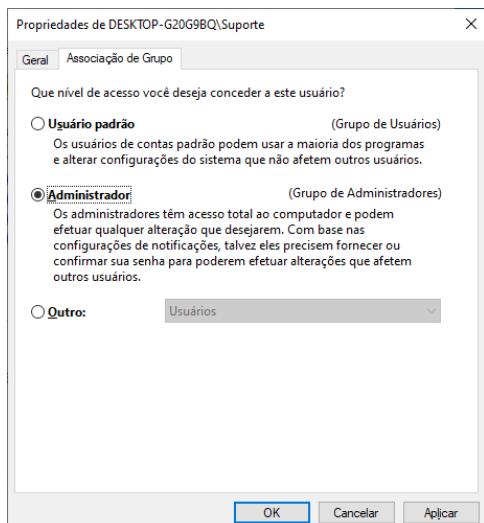
A conta do usuário Suporte terá sido criada.



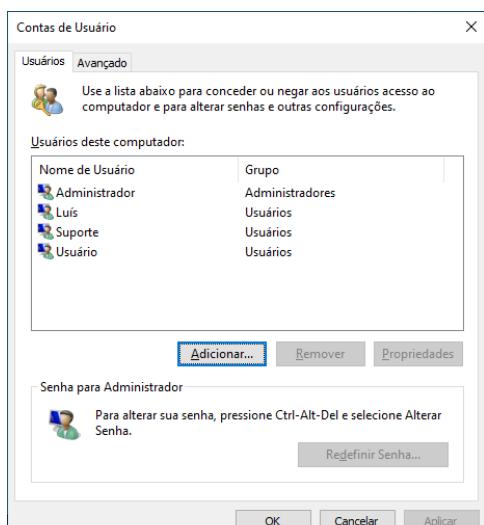
Defina o usuário **Suporte** como **Administrador** do computador. Para isso, clique duas vezes na conta de usuário **Suporte**.



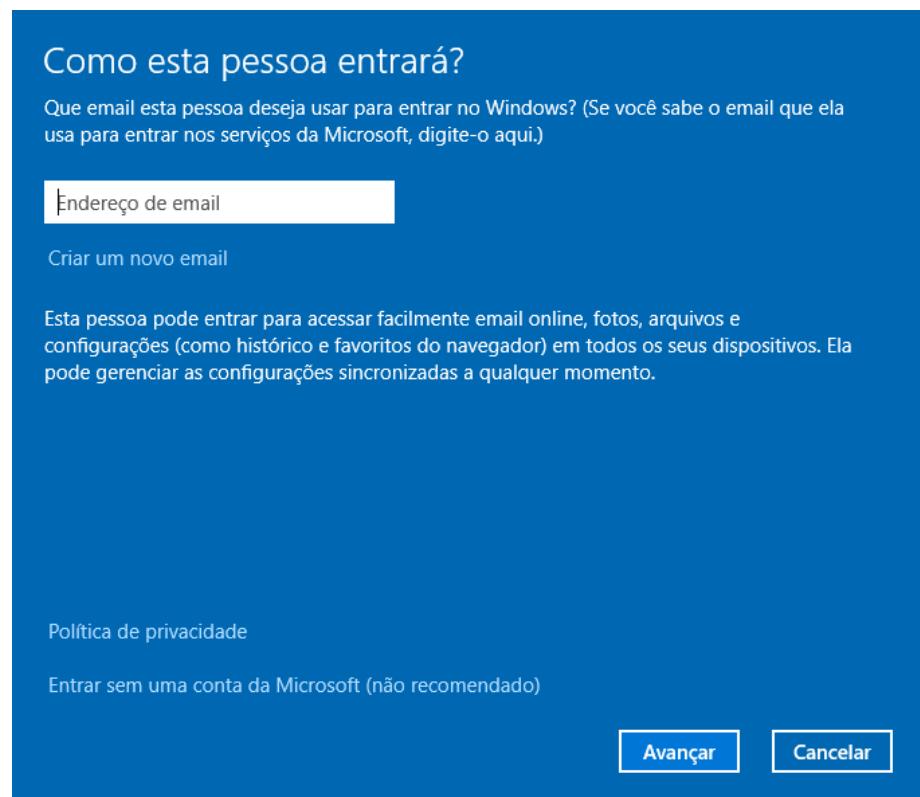
Clique em **Associação de Grupo**, marque a opção **Administrador** e clique em **OK**.



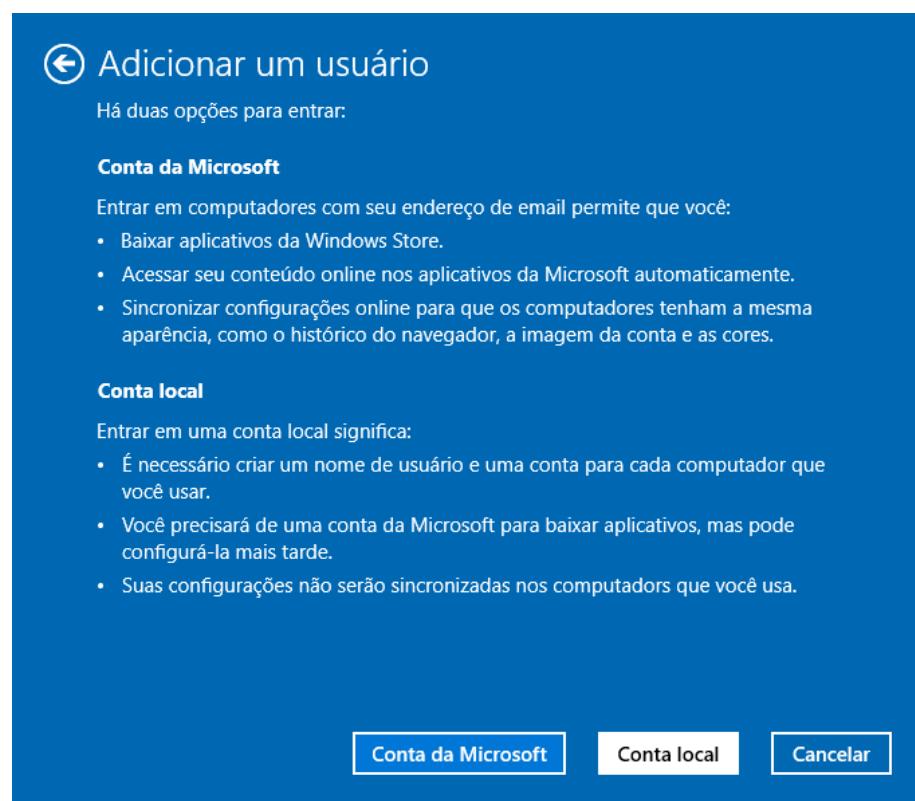
Sendo necessário ainda criar a conta de usuário do AGR, clique novamente em **Adicionar**.



Assim como feito anteriormente, selecione as mesmas opções, clicando em **Entrar sem uma conta Microsoft**.



Clique em **Conta local**.



Para criar a conta do usuário do AGR existem regras a serem seguidas:

- O usuário deve conter **apenas** o Nome e Sobrenome
- O usuário **não deve conter caracteres especiais**, como acentos ou til (‘, ^, ~, ¸, ´)
- A senha inicial deve ser **Q1W2e3r4**

Exemplo: se o AGR se chama *João da Silva*, o usuário será **Joao Silva**. Conforme o exemplo da imagem em que o usuário se chamaria *Luís Hamilton*, o usuário não possuirá acento: **Luis Hamilton**.

➊ Adicionar um usuário

Escolha uma senha que seja fácil de lembrar, mas difícil de adivinhar. Se você esquecer, vamos mostrar a dica.

Nome do usuário	Luis Hamilton
Senha	*****
Confirmar senha	*****
Dica de senha	Senha padrão <input type="button" value="X"/>

A conta foi criada.

Adicionar um usuário

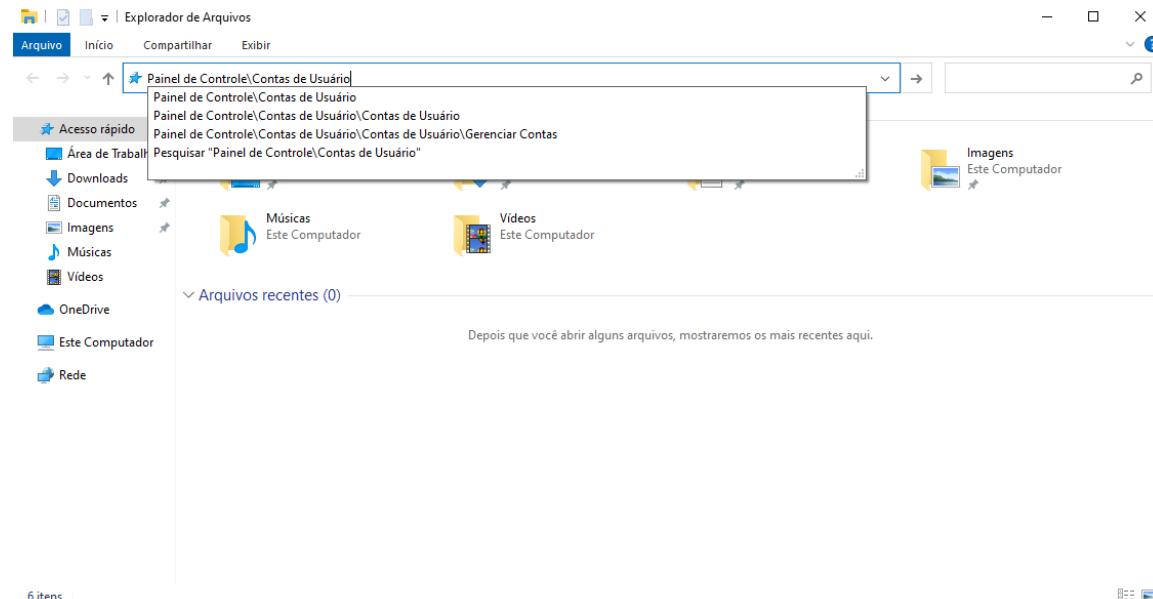
O usuário a seguir poderá entrar neste computador.

	Luis Hamilton Conta local
---	------------------------------

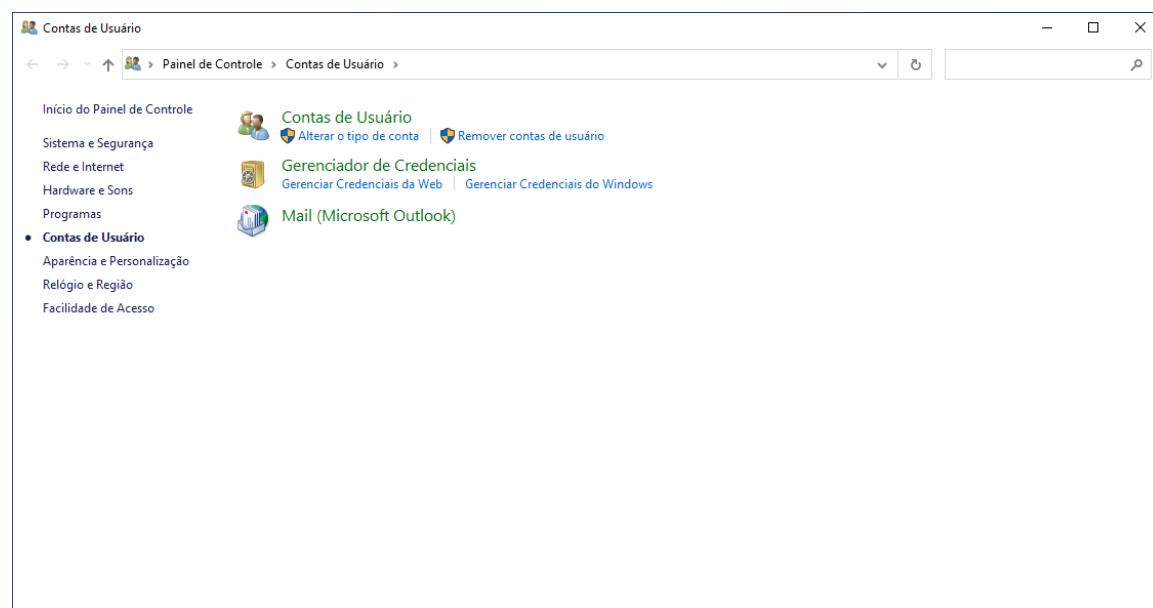
Além do usuário do AGR, o computador deve ter **apenas um usuário administrador** chamado **Suporte**, sendo assim, **remova os privilégios de administrador de outros possíveis usuários encontrados, realize backup dos dados destes usuários** e desative ou exclua estes usuários.

Antes de prosseguir com a exclusão de um usuário, é necessário assegurar que ele não está com nenhuma sessão aberta. Para garantir isso, a melhor forma é apenas reiniciar o computador antes de excluir. **Reinic peace e acesse com a conta Suporte criada.**

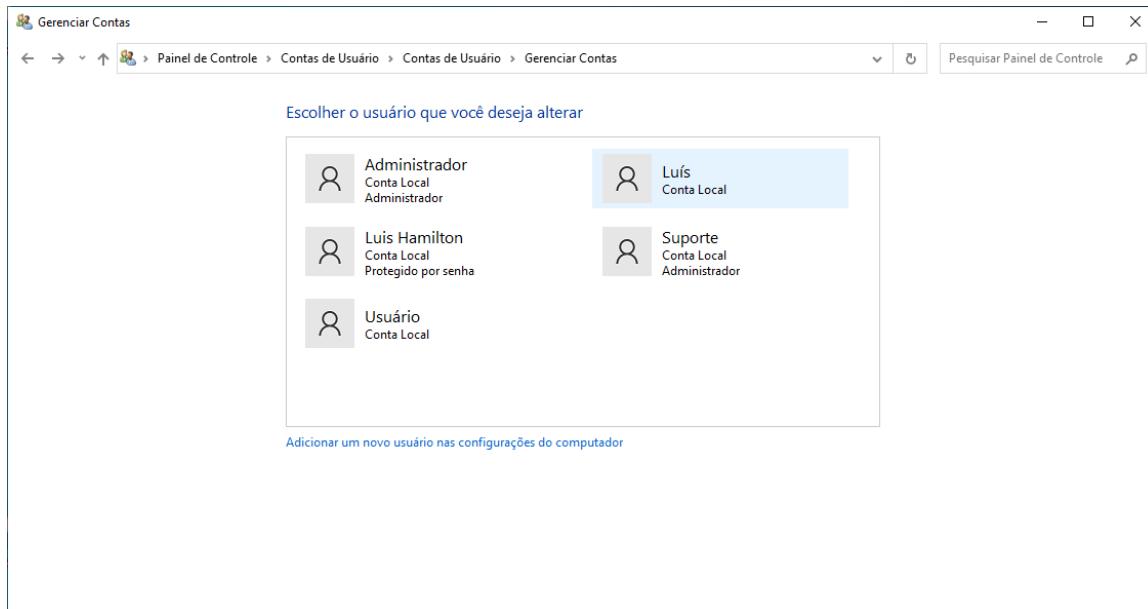
Para verificar os usuários atualmente em uso, abra o Windows Explorer (WINKEY+E) e na barra de endereços digite **Painel de Controle\Contas de Usuário** e pressione **ENTER**.



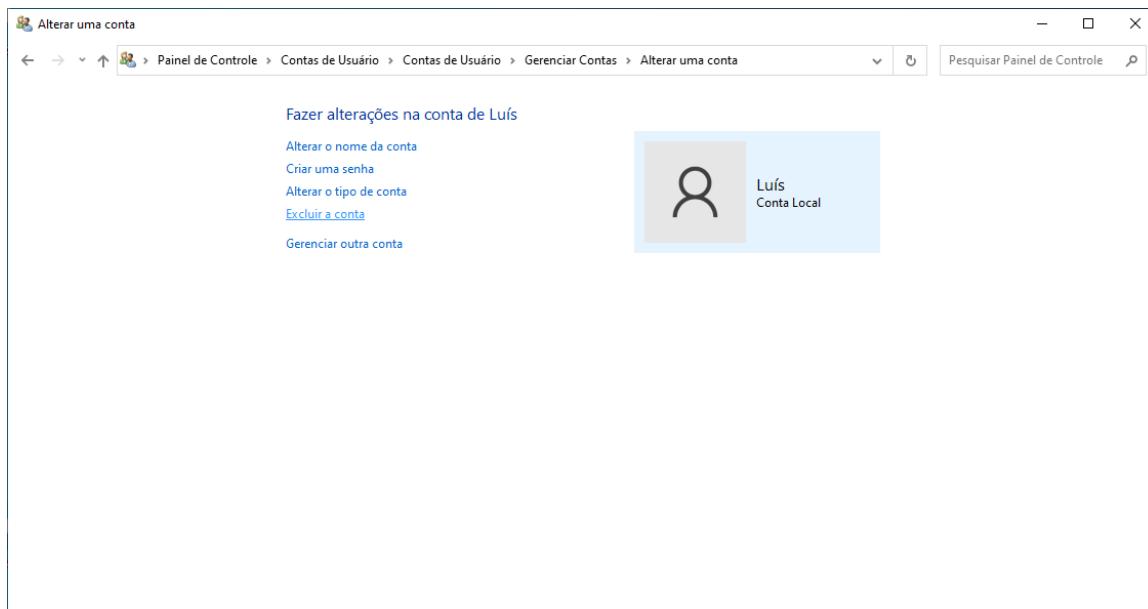
Clique em Remover contas de usuário.



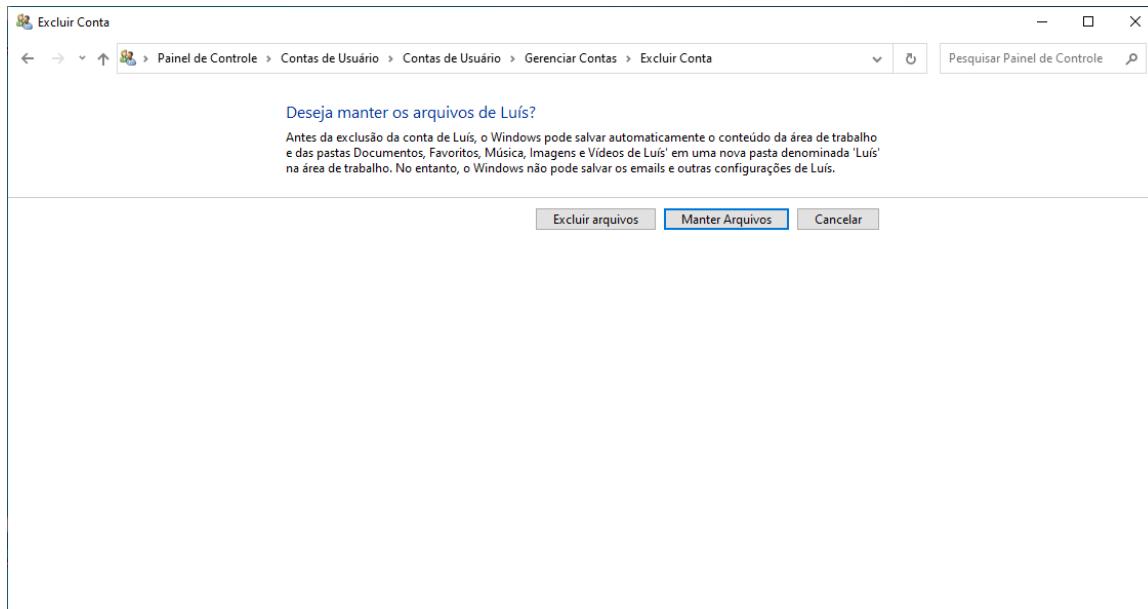
Clique na conta a ser excluída.



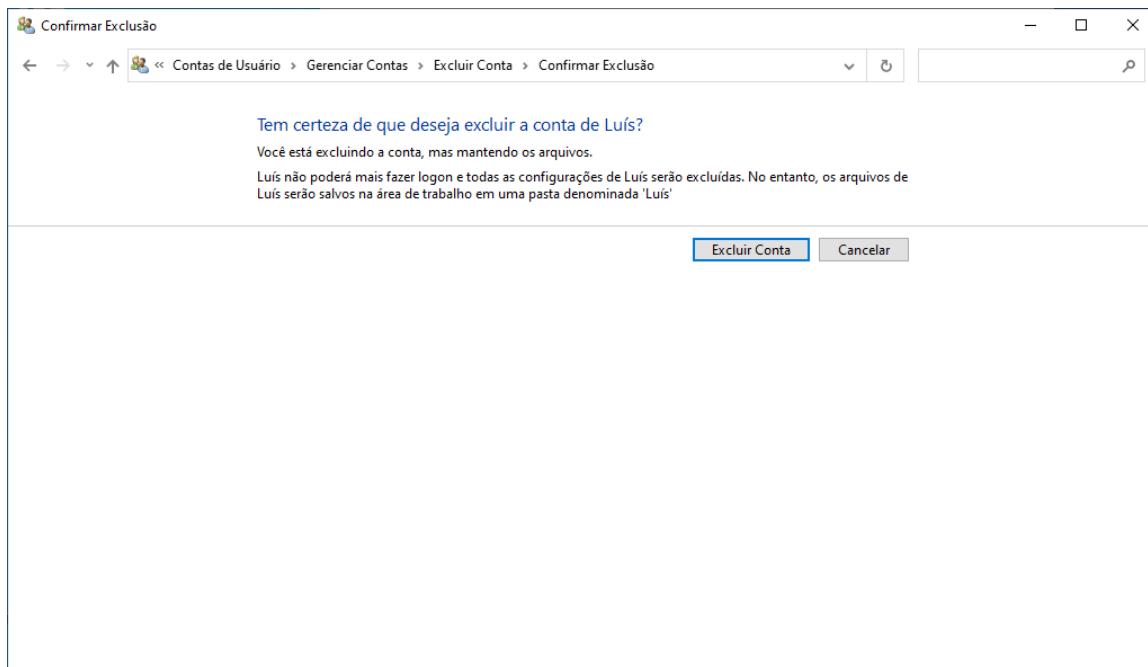
Clique em **Excluir a conta**.



Clique em **Manter Arquivos**.



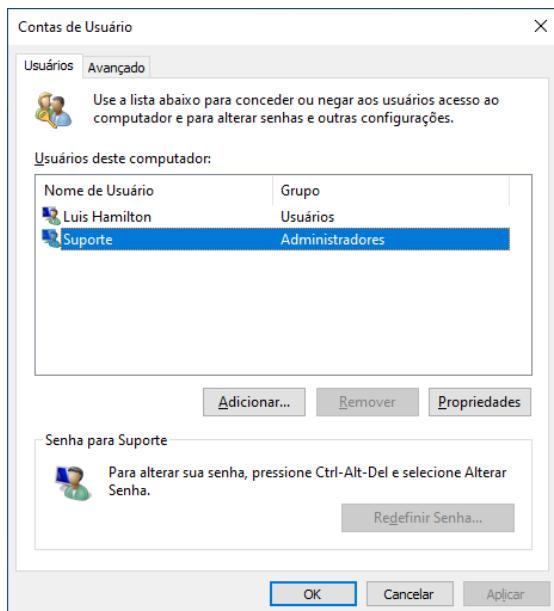
Confirme clicando em **Excluir Conta**.



Neste momento esta tela poderá demorar um tempo para prosseguir, pois estará realizando o backup do usuário na Área de Trabalho do usuário atual.

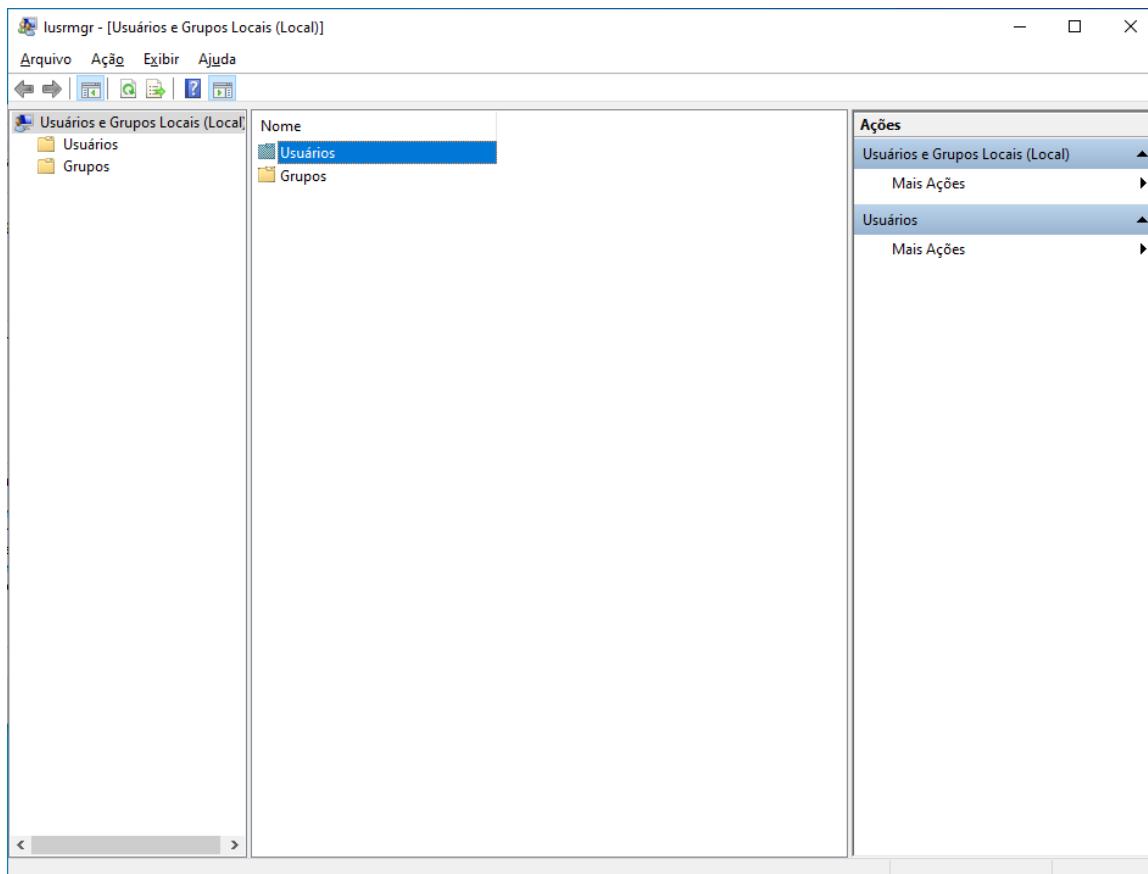


Após a devida configuração da conta de Suporte e de AGR e exclusão das demais contas, a tela do menu de contas de usuário deverá ficar assim:

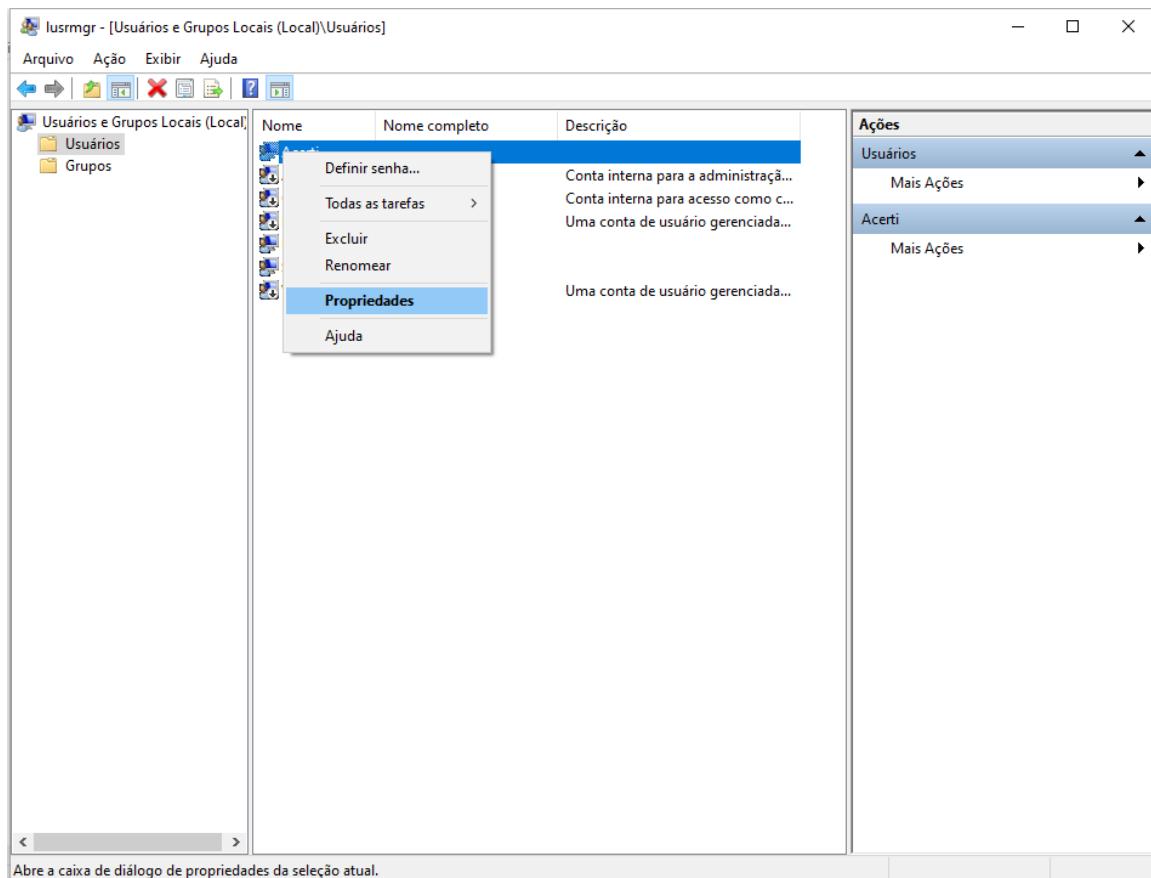


Se a distribuição do sistema operacional for Windows 10 Pro, é possível apenas desativar a conta de usuário, executando o comando **LUSRMGR.MSC** para abrir o Gerenciamento avançado de usuários.

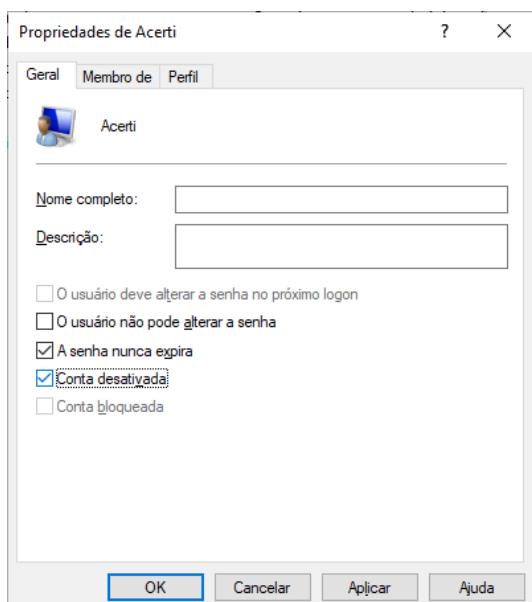
No console do gerenciamento avançado de usuários, abra a unidade **Usuários**.



Selecione o usuário a ser desativado e clique em **Propriedades**.



Marque a opção **Conta desativada** e clique em **OK**. A conta estará desativada.



6 Aplicativos a instalar

Com o usuário **Suporte**, vamos começar a instalar os aplicativos do computador.

Todos os aplicativos homologados estão no diretório do [SharePoint](#). Você pode acessar e fazer download no computador remoto para facilitar a instalação.

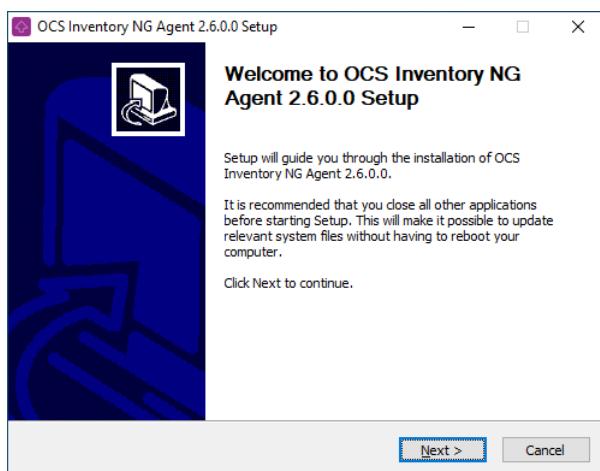
Instale na seguinte ordem:

1. 7-Zip
2. Desktop Central
3. Java 32 bits
4. Acrobat Reader
5. Microsoft Office ou LibreOffice e Thunderbird
6. Google Chrome
7. Firefox

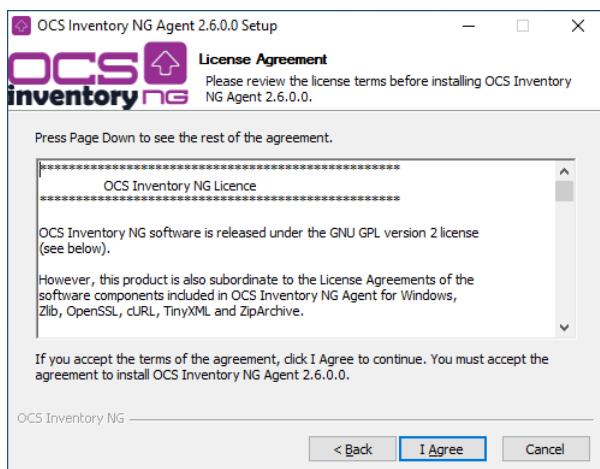
IMPORTANTE! Ao instalar todos estes aplicativos, fique atento para desmarcar todas as opções que oferecem plugins, extensões de navegadores ou outros elementos adicionais desnecessários!!!

6.1 OCS

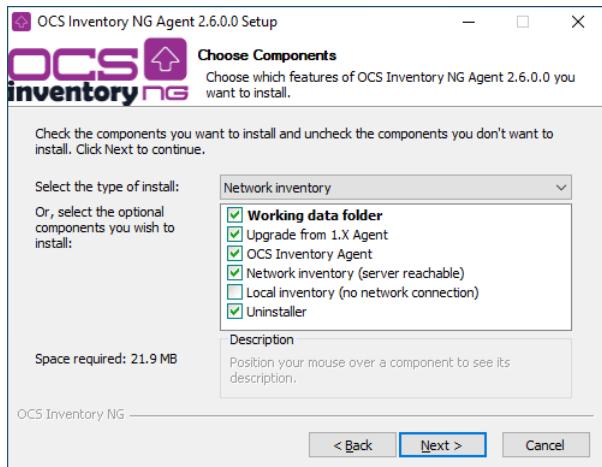
Execute o instalador e clique em **Next** na primeira tela.



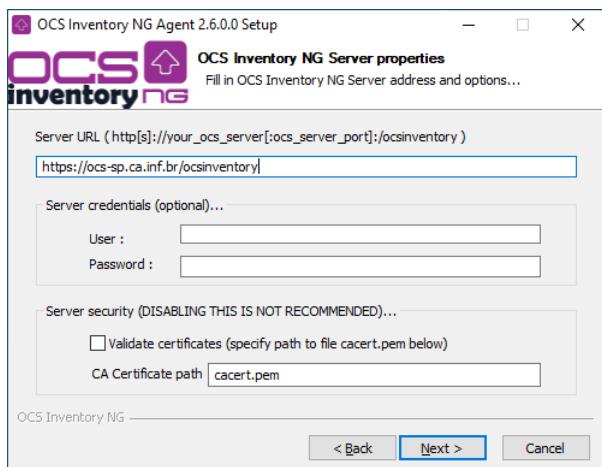
Clique em **I Agree**.



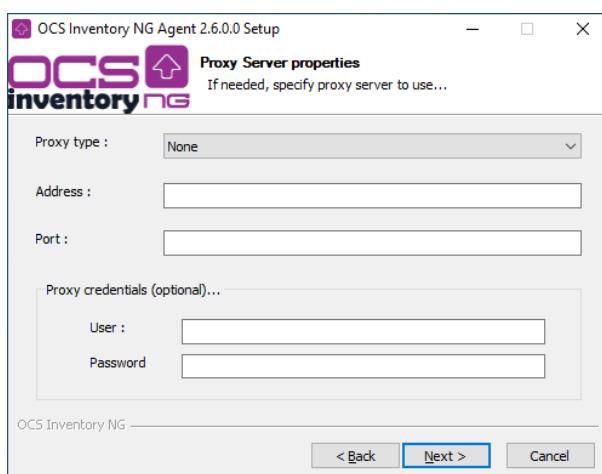
Clique em **Next**.



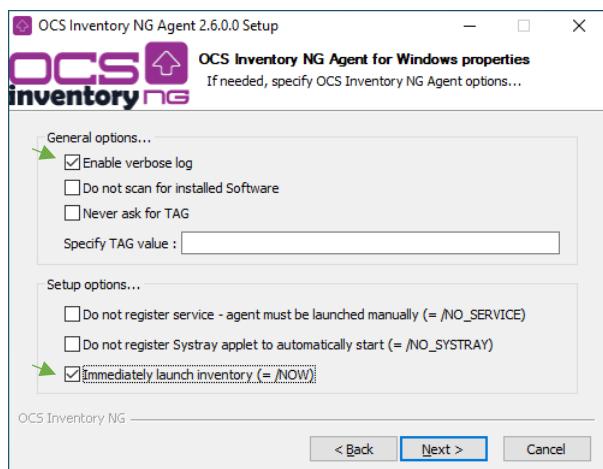
Nesta tela, **digite o endereço do servidor e desmarque a opção Validate certificates**. O endereço é: <https://ocs-sp.ca.inf.br/ocsinventory>



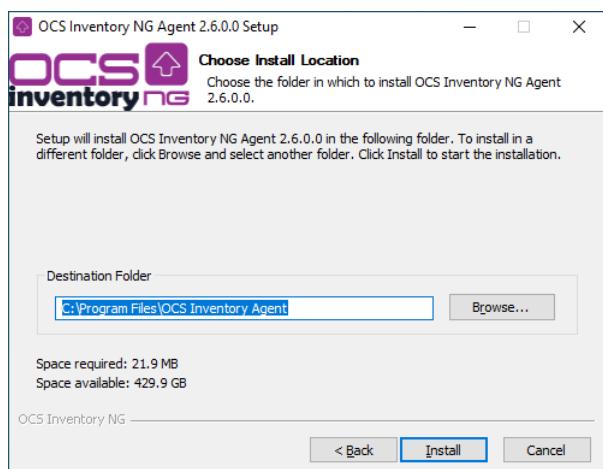
Pressione **Next**.



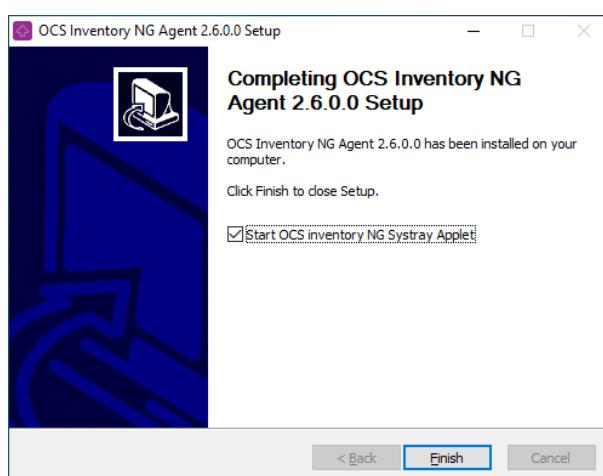
Nesta tela, marque a primeira e a última opção: **Enable verbose log** e **Immediately lauch inventory (=NOW)** e clique em **Next**.



Clique em **Install**.



Clique em **Finish** para concluir a instalação.



6.2 Gerenciadores de Certificados

Após instalar estes aplicativos, instale os [gerenciadores de certificados](#). Os gerenciadores são:

- AWP
- ePass2003
- StarSign
- PC-CCID
- Omnikey
- SafeNet
- SafeSign

6.3 Drivers de dispositivos

Após instalar os gerenciadores, instale os drivers de dispositivos. São eles:

- Leitora biométrica Futronic FS80
- Leitora de cartões Smart Card
- Webcam Logitech
- Token Morpho

6.4 Complementos do Windows

Após instalar os drivers, vamos instalar alguns complementos que podem ser necessários dependendo do Windows.

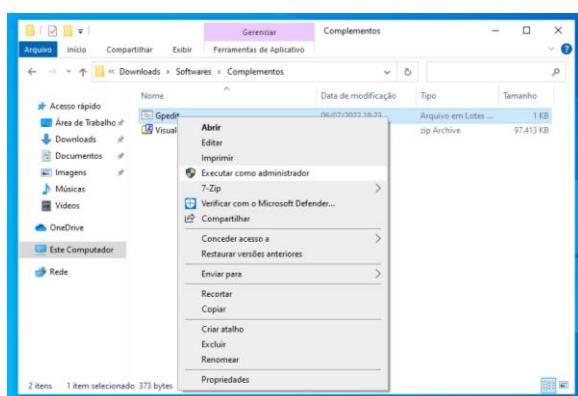
6.4.1 Editor de Política de Grupo

Não é necessário instalar se a versão do sistema for Windows 10 Pro. Se a distribuição for Windows 10 Home, Home Single Language, outras), será necessário incorporar o editor de política de grupo. Para verificar se é necessário, tente abrir o editor executando **GPEDIT.MSC** ou verificando a distribuição do Windows, que pode ser checada nas propriedades do sistema, pressionando **WINKEY+PAUSE**, conforme exibido anteriormente:

Especificações do Windows

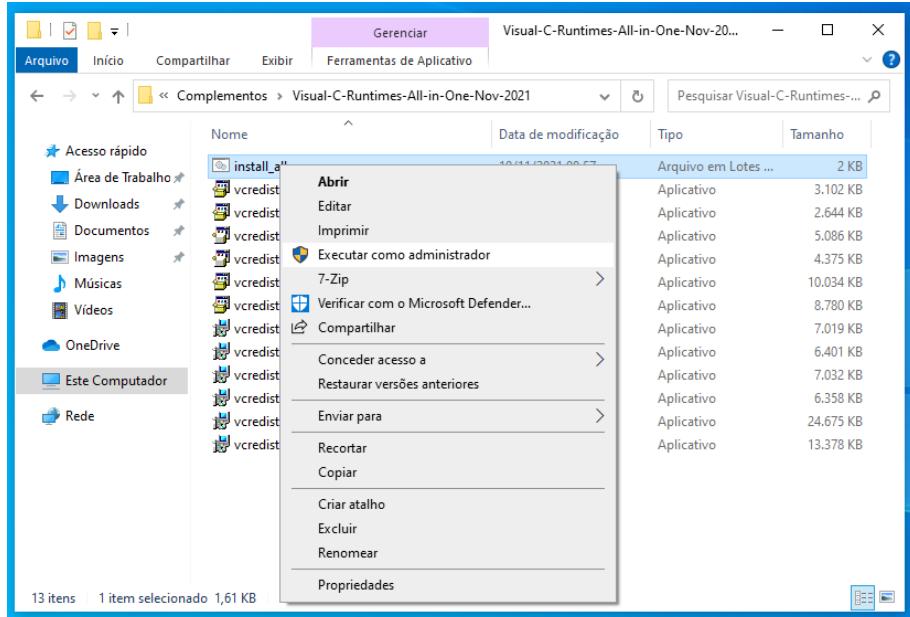
Edição	Windows 10 Pro
Versão	21H2
Instalado em	10/05/2022
Compilação do SO	19044.1620
Experiência	Windows Feature Experience Pack 120.2212.4170.0

Sendo necessário instalar o editor, execute a [bat](#) como **administrador** conforme a imagem.

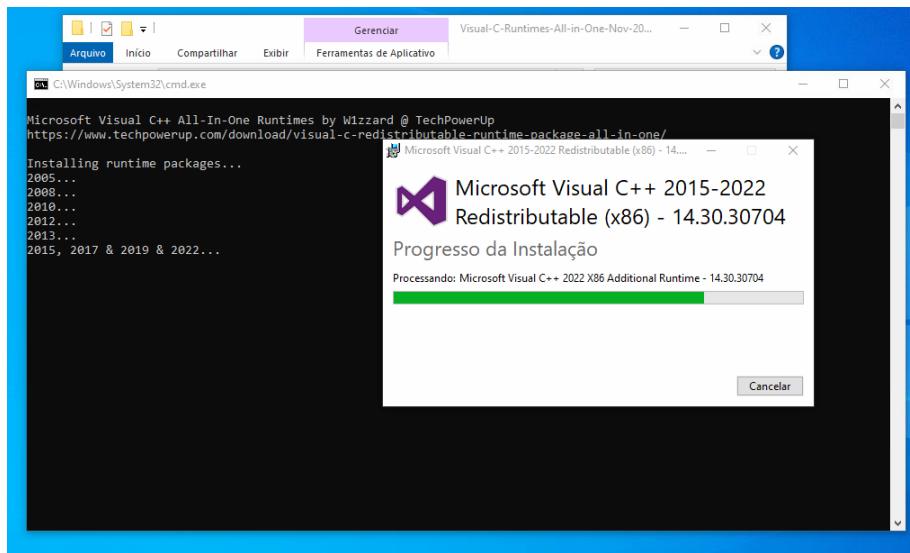


6.4.2 Pacotes de Redistribuíveis do Visual C++

Extraia todos os instaladores e execute a **bat** de instalação do Visual C++ Runtime **como administrador**, conforme a imagem.



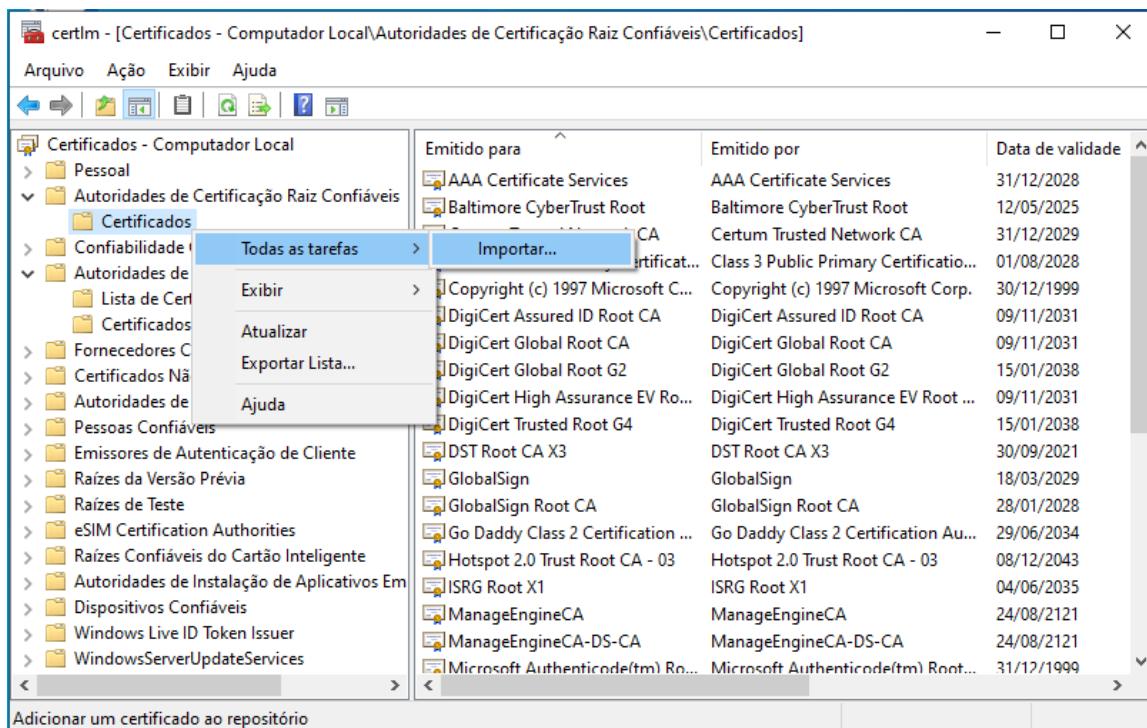
Os pacotes redistribuíveis do Visual C++ serão instalados e a janela fechará automaticamente.



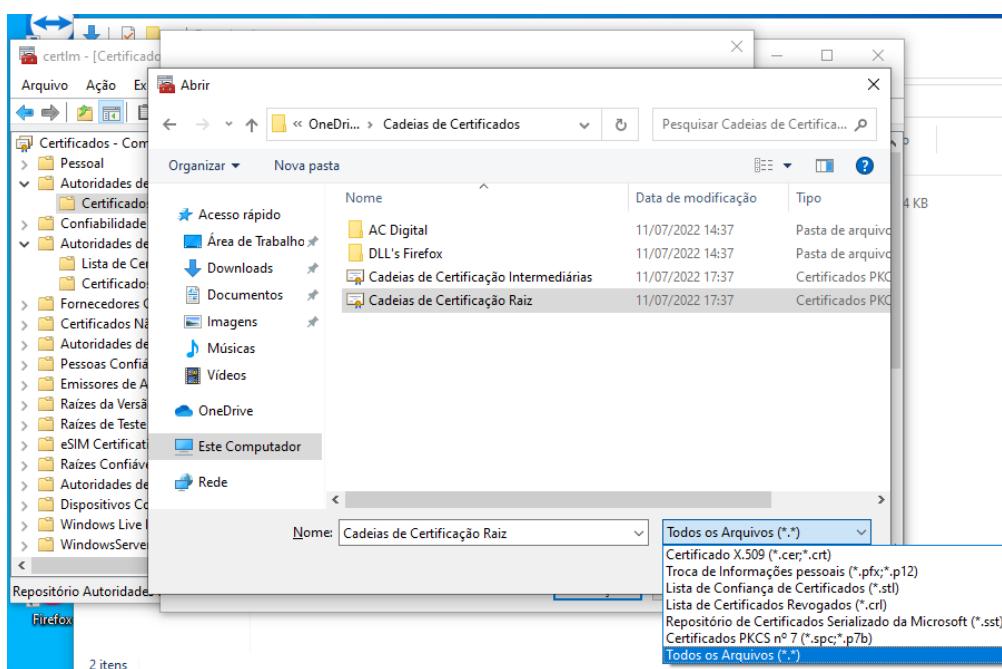
7 Cadeias de Certificados

Vamos agora importar as [cadeias de certificados](#). Abra o gerenciador de certificados do computador executando o comando **CERTLM.MSC**.

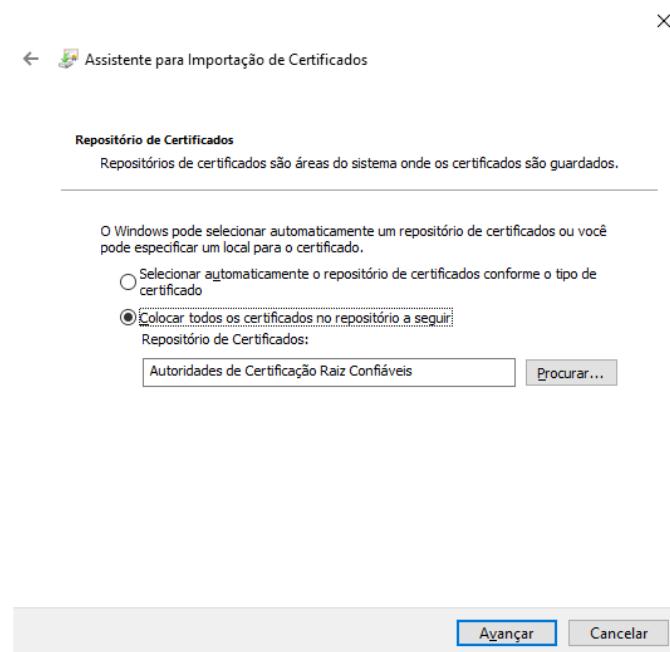
No gerenciador de certificados, expanda a guia **Autoridades de Certificação Raiz Confiáveis**, clique com o botão direito em **Certificados** > **Todas as tarefas** > **Importar...**



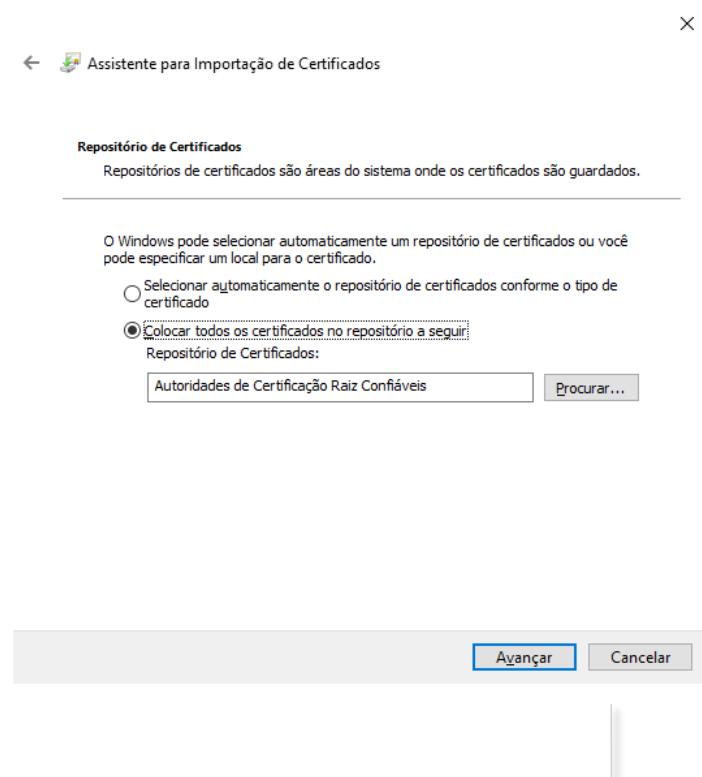
No assistente de importação de certificados, clique em **Avançar**. Clique em **Procurar** e na janela para abrir, selecione o tipo de arquivo para **Todos os Arquivos (*.*)** e selecione as **Cadeias de Certificação Raiz.p7b**:



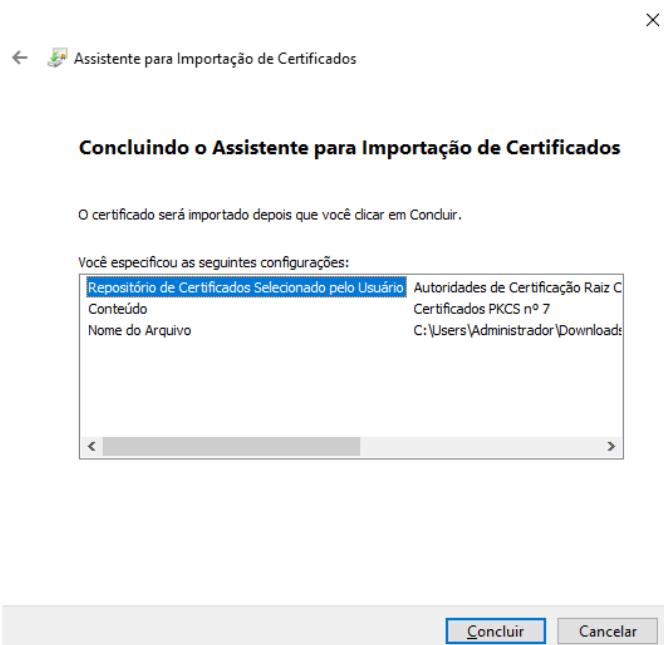
Clique em **Avançar**.



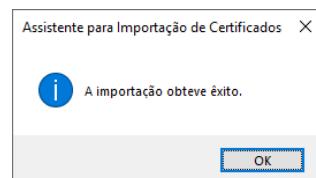
Clique novamente em **Avançar** para importar ao repositório correto.



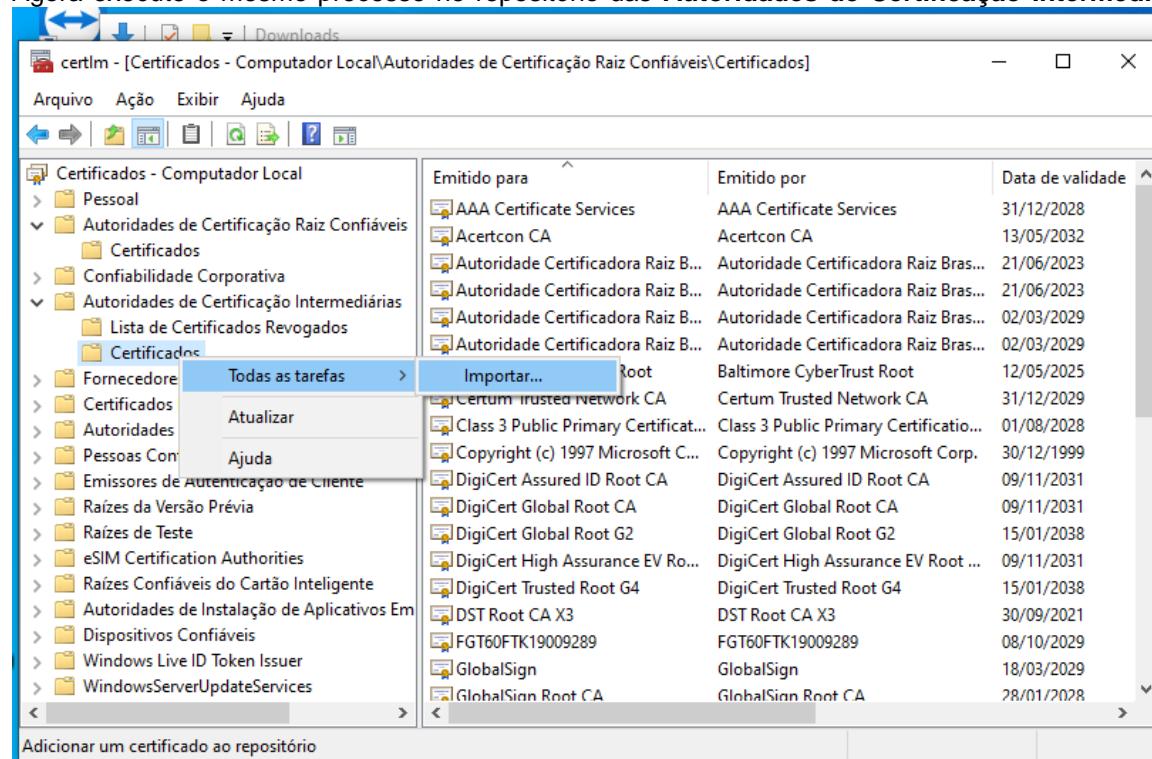
Clique em **Concluir** para finalizar a importação.



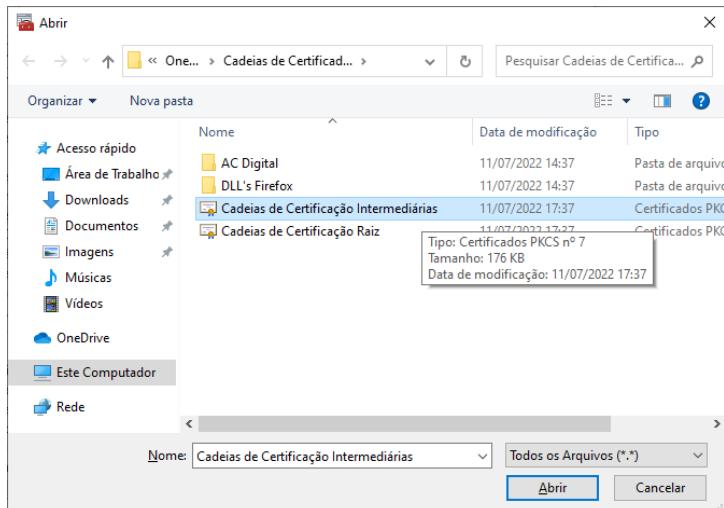
Clique em **OK** para encerrar.



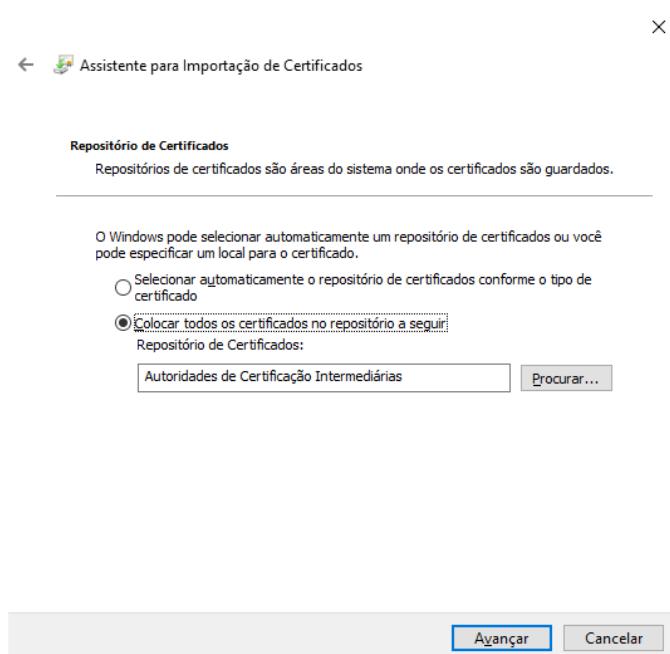
Agora execute o mesmo processo no repositório das **Autoridades de Certificação Intermediárias**.



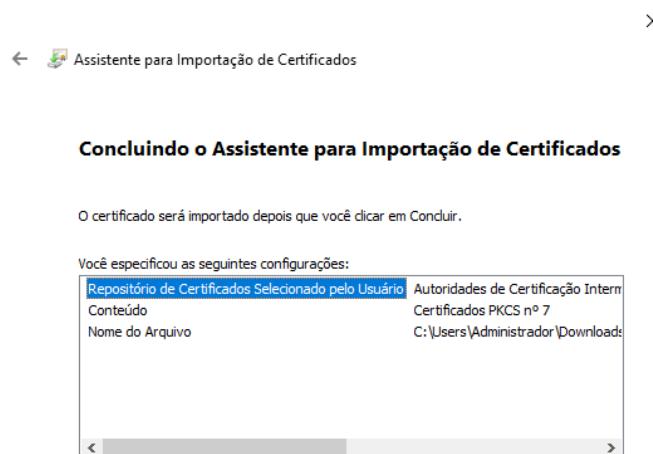
Emitido para	Emitido por	Data de validade
AAA Certificate Services	AAA Certificate Services	31/12/2028
Acertcon CA	Acertcon CA	13/05/2032
Autoridade Certificadora Raiz B...	Autoridade Certificadora Raiz Bras...	21/06/2023
Autoridade Certificadora Raiz B...	Autoridade Certificadora Raiz Bras...	21/06/2023
Autoridade Certificadora Raiz B...	Autoridade Certificadora Raiz Bras...	02/03/2029
Autoridade Certificadora Raiz B...	Autoridade Certificadora Raiz Bras...	02/03/2029
Baltimore CyberTrust Root	Baltimore CyberTrust Root	12/05/2025
Certum Trusted Network CA	Certum Trusted Network CA	31/12/2029
Class 3 Public Primary Certificat...	Class 3 Public Primary Certificatio...	01/08/2028
Copyright (c) 1997 Microsoft C...	Copyright (c) 1997 Microsoft Corp.	30/12/1999
DigiCert Assured ID Root CA	DigiCert Assured ID Root CA	09/11/2031
DigiCert Global Root CA	DigiCert Global Root CA	09/11/2031
DigiCert Global Root G2	DigiCert Global Root G2	15/01/2038
DigiCert High Assurance EV Root...	DigiCert High Assurance EV Root ...	09/11/2031
DigiCert Trusted Root G4	DigiCert Trusted Root G4	15/01/2038
DST Root CA X3	DST Root CA X3	30/09/2021
FGT60FTK19009289	FGT60FTK19009289	08/10/2029
GlobalSign	GlobalSign	18/03/2029
GlobalSign Root CA	GlobalSign Root CA	28/01/2028

Importe as Cadeias de Certificação Intermediárias.p7b


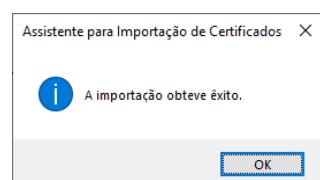
Clique em **Avançar** após confirmar o repositório correto.



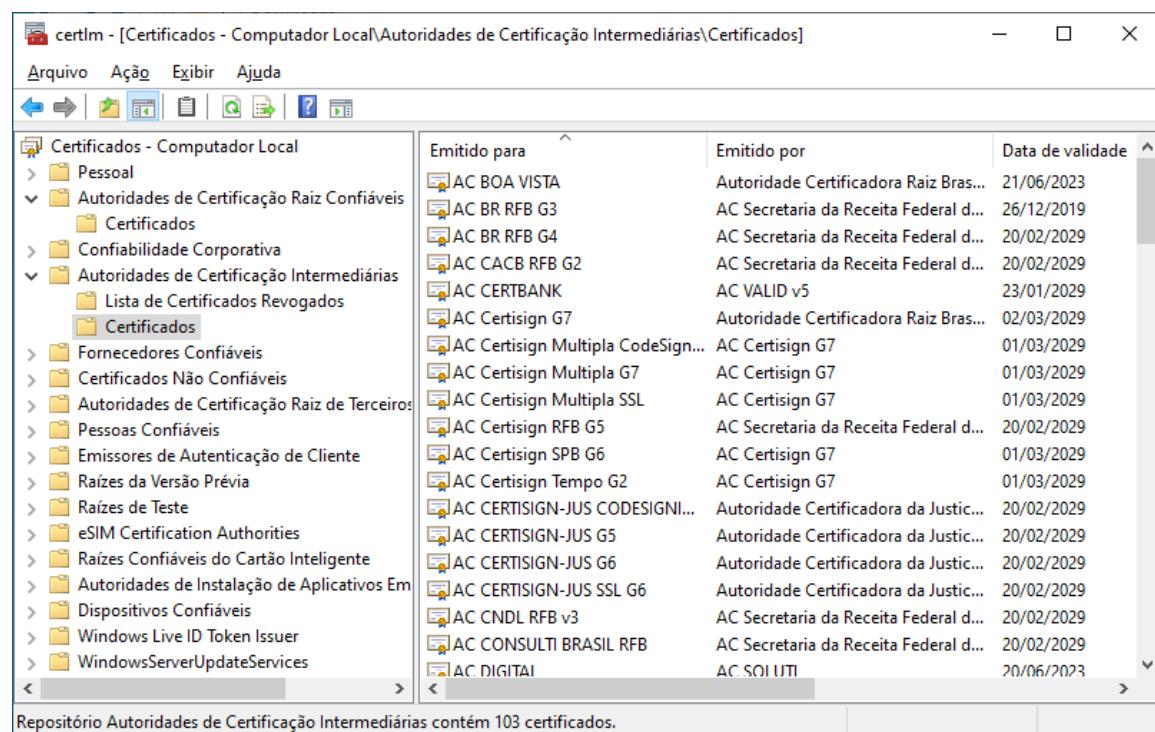
Clique em **Concluir**.



Clique em **OK**.



As cadeias foram importadas.



Emitido para	Emitido por	Data de validade
AC BOA VISTA	Autoridade Certificadora Raiz Bras...	21/06/2023
AC BR RFB G3	AC Secretaria da Receita Federal d...	26/12/2019
AC BR RFB G4	AC Secretaria da Receita Federal d...	20/02/2029
AC CACB RFB G2	AC Secretaria da Receita Federal d...	20/02/2029
AC CERTBANK	AC VALID v5	23/01/2029
AC Certisign G7	Autoridade Certificadora Raiz Bras...	02/03/2029
AC Certisign Multipla CodeSign...	AC Certisign G7	01/03/2029
AC Certisign Multipla G7	AC Certisign G7	01/03/2029
AC Certisign Multipla SSL	AC Certisign G7	01/03/2029
AC Certisign RFB G5	AC Secretaria da Receita Federal d...	20/02/2029
AC Certisign SPB G6	AC Certisign G7	01/03/2029
AC Certisign Tempo G2	AC Certisign G7	01/03/2029
AC CERTSIGN-JUS CODESIGNI...	Autoridade Certificadora da Justic...	20/02/2029
AC CERTSIGN-JUS G5	Autoridade Certificadora da Justic...	20/02/2029
AC CERTSIGN-JUS G6	Autoridade Certificadora da Justic...	20/02/2029
AC CERTSIGN-JUS SSL G6	Autoridade Certificadora da Justic...	20/02/2029
AC CNDL RFB v3	AC Secretaria da Receita Federal d...	20/02/2029
AC CONSULTI BRASIL RFB	AC Secretaria da Receita Federal d...	20/02/2029
AC DIGITAL	AC SOI UTI	20/06/2023

Repositório Autoridades de Certificação Intermediárias contém 103 certificados.

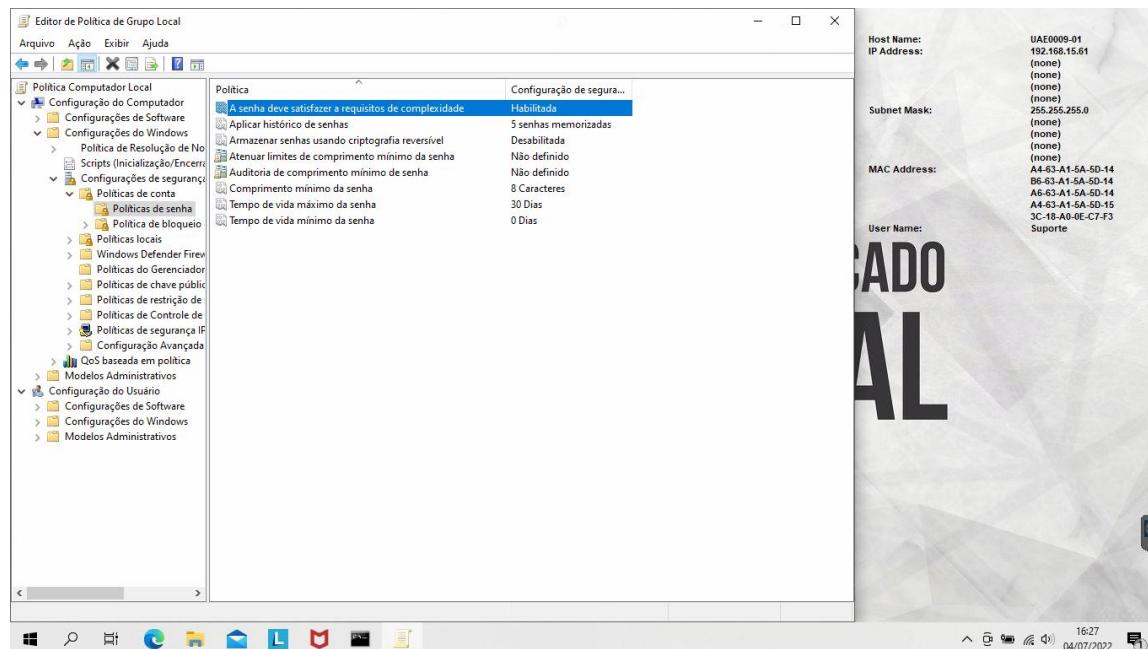
8 Políticas de segurança

Agora vamos editar as políticas de segurança do Windows.

Pressione WINKEY+R para executar e digite **GPEDIT.MSC** e pressione **ENTER** para abrir o **Editor de Política de Grupo**.

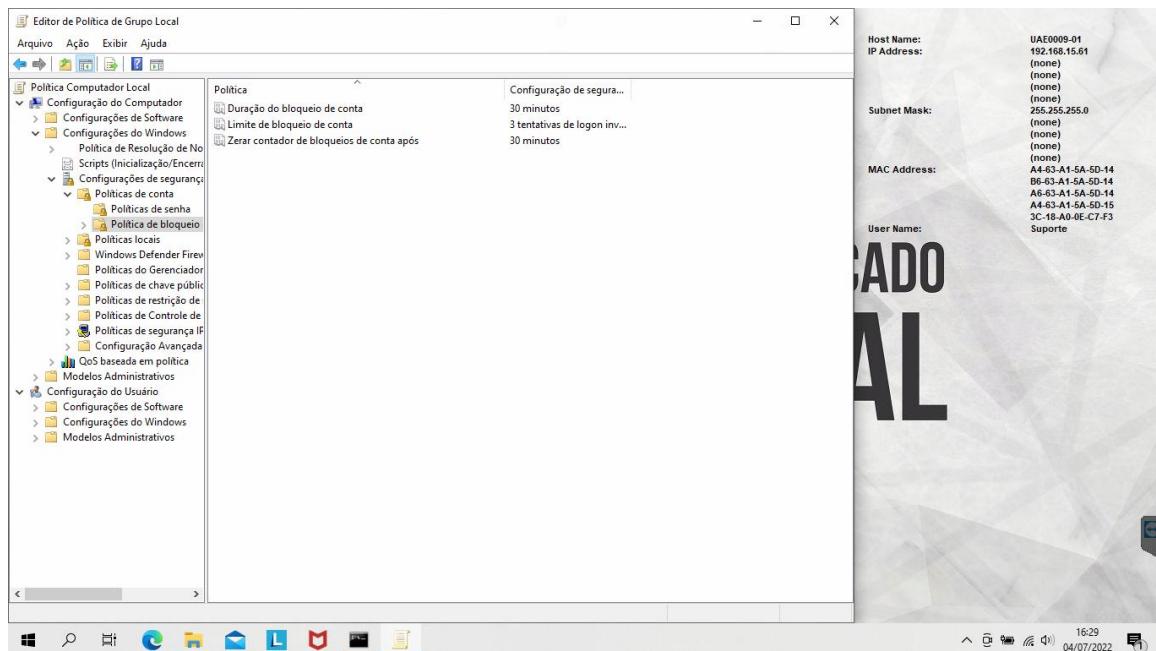
Configuração do Computador > Configurações do Windows > Configurações de Segurança > Políticas de conta > **Políticas de senha**

- A senha deve satisfazer os requisitos de complexidade: **Habilitada**
- Aplicar histórico de senhas: **5 senhas memorizadas**
- Armazenar senhas usando criptografia reversível: **Desabilitada**
- Comprimento mínimo da senha: **8 caracteres**
- Tempo de vida máxima da senha: **30 dias**
- Tempo de vida mínimo: **0 dias**



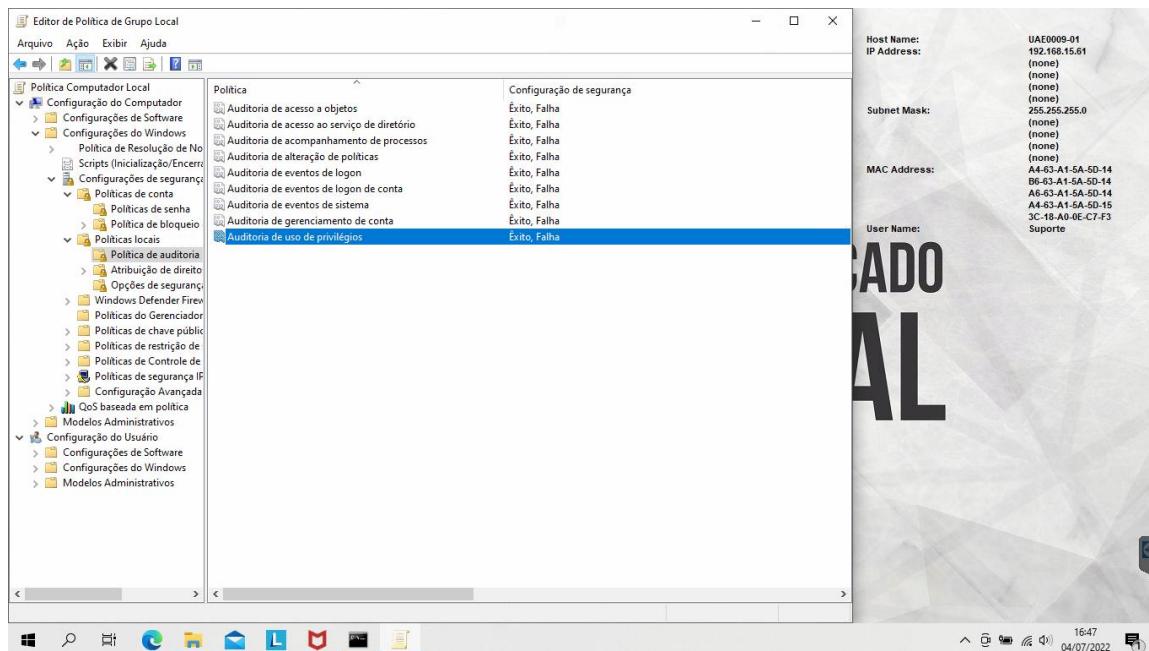
Configuração do Computador > Configurações do Windows > Configurações de Segurança > Políticas de Conta > **Política de bloqueio de conta**

- Limite de bloqueio de conta: **3 tentativas**
- Duração do bloqueio de conta: **30 minutos**
- Zerar contador de bloqueios de conta após: **30 minutos**



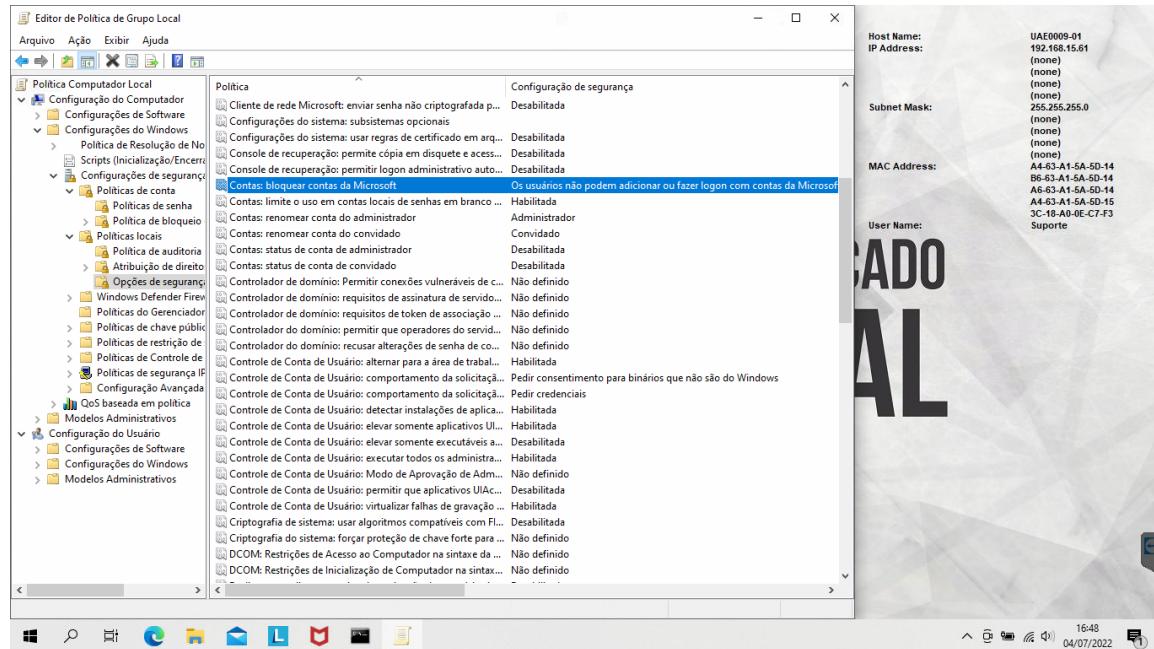
Configuração do Computador > Configurações do Windows > Configurações de Segurança > Políticas locais > **Política de auditoria**

- Auditoria de acesso a objetos: **Êxito, Falha**
- Auditoria de acesso ao serviço de diretório: **Êxito, Falha**
- Auditoria de acompanhamento de processos: **Êxito, Falha**
- Auditoria de alteração de políticas: **Êxito, Falha**
- Auditoria de eventos de logon: **Êxito, Falha**
- Auditoria de eventos de logon de conta: **Êxito, Falha**
- Auditoria de eventos de sistema: **Êxito, Falha**
- Auditoria de gerenciamento de conta: **Êxito, Falha**
- Auditoria de uso de privilégios: **Êxito, Falha**

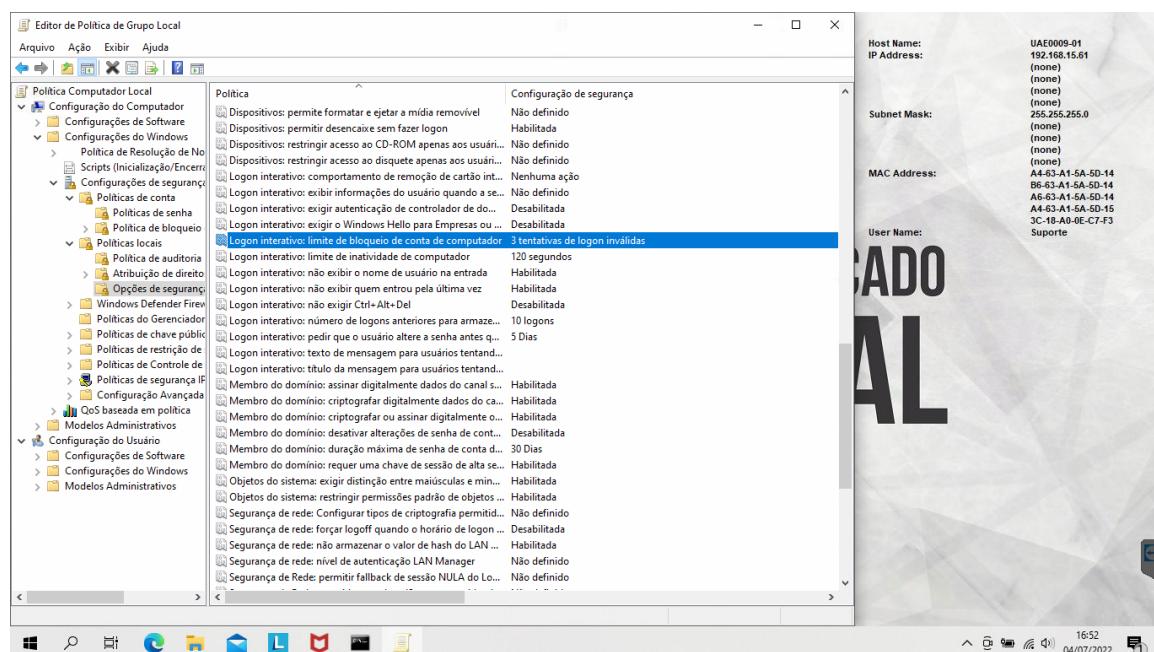


Configuração do Computador > Configurações do Windows > Configurações de Segurança > Políticas locais > **Opções de segurança**

- Contas: bloquear contas Microsoft: **Os usuários não poderão adicionar ou fazer logon com contas Microsoft**
- Contas: status de conta de administrador: **Desabilitada**
- Contas: status de conta de convidado: **Desabilitada**

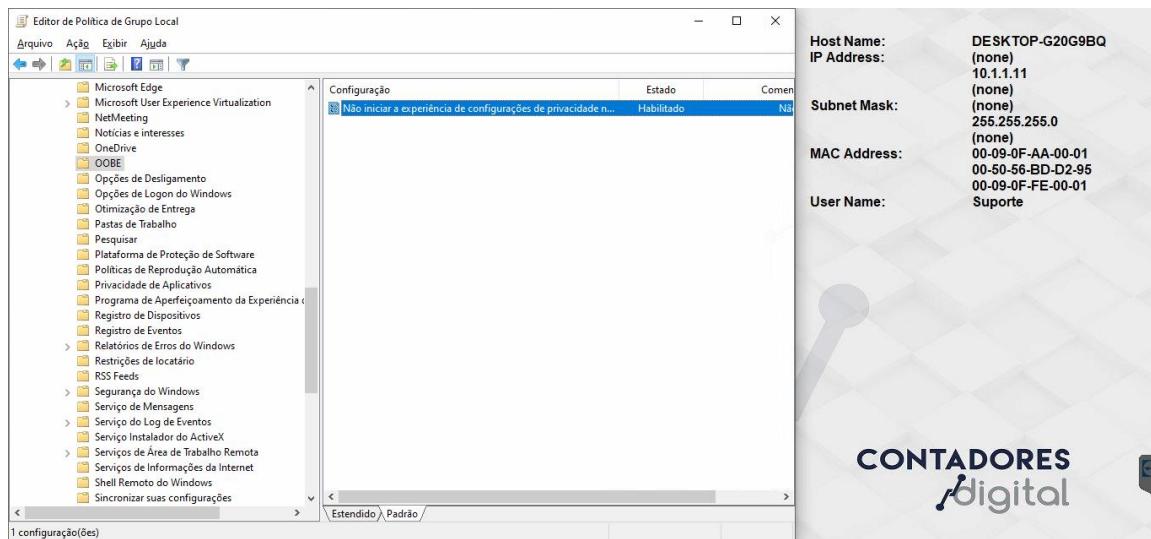


- Logon interativo: limite de bloqueio de conta de computador: **3 tentativas**
- Logon interativo: limite de inatividade do computador: **120 segundos**
- Logon interativo: não exibir o nome de usuário na entrada: **Habilitada**
- Logon interativo: não exibir quem entrou pela última vez: **Habilitada**
- Logon interativo: não exigir CTRL+ALT+DEL: **Desabilitada**

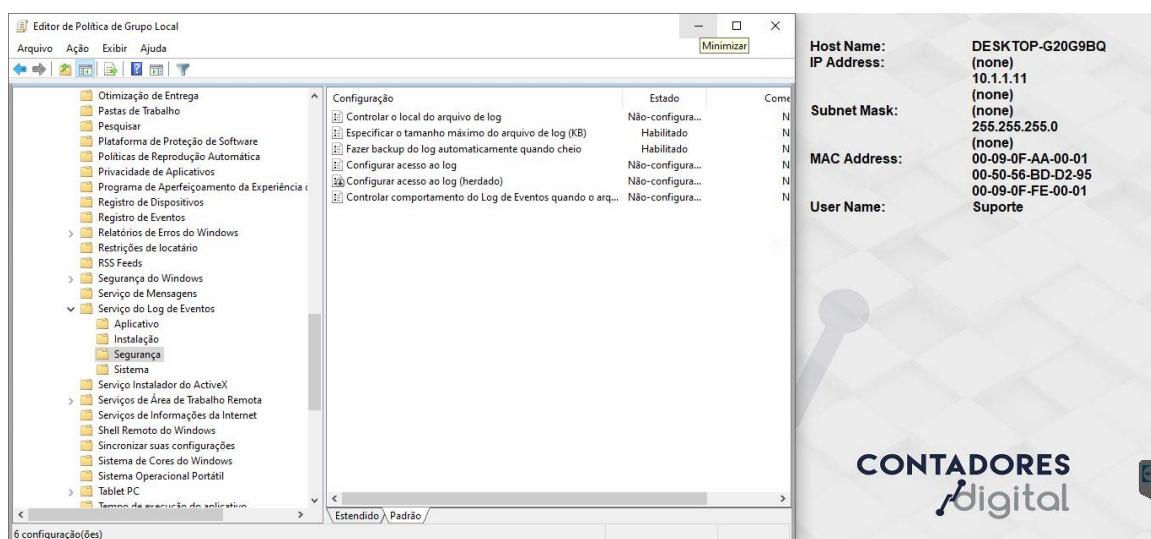


Configuração do Computador > Modelos Administrativos > Componentes do Windows > OOBE

- Não iniciar a experiência de configurações de privacidade no logon do usuário: **Habilitado**

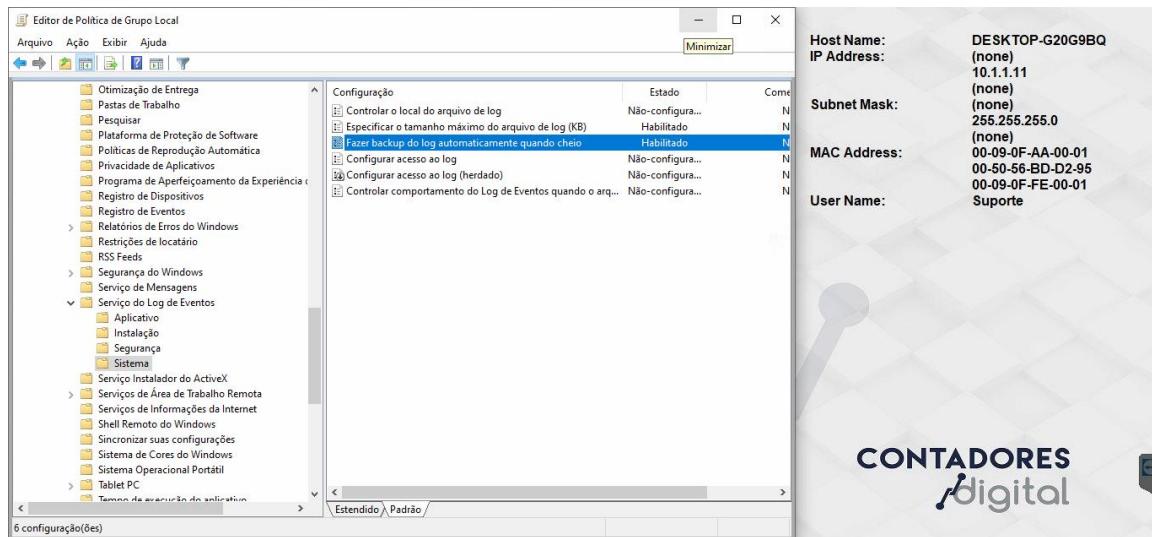

Configuração do Computador > Modelos Administrativos > Componentes do Windows > Serviço do Log de Eventos > Segurança

- Especificar o tamanho máximo do arquivo de log (KB): **Habilitado**
- Fazer backup do log automaticamente quando cheio: **Habilitado**



Configuração do Computador > Modelos Administrativos > Componentes do Windows > Serviço do Log de Eventos > **Sistema**

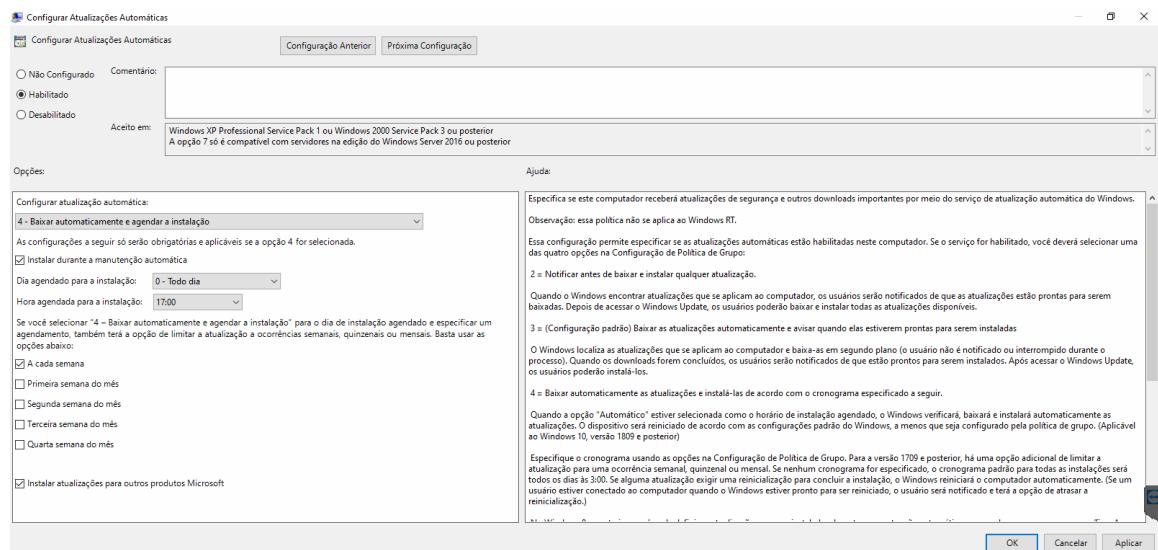
- Especificar o tamanho máximo do arquivo de log (KB): **Habilitado**
- Fazer backup do log automaticamente quando cheio: **Habilitado**



CONTADORES

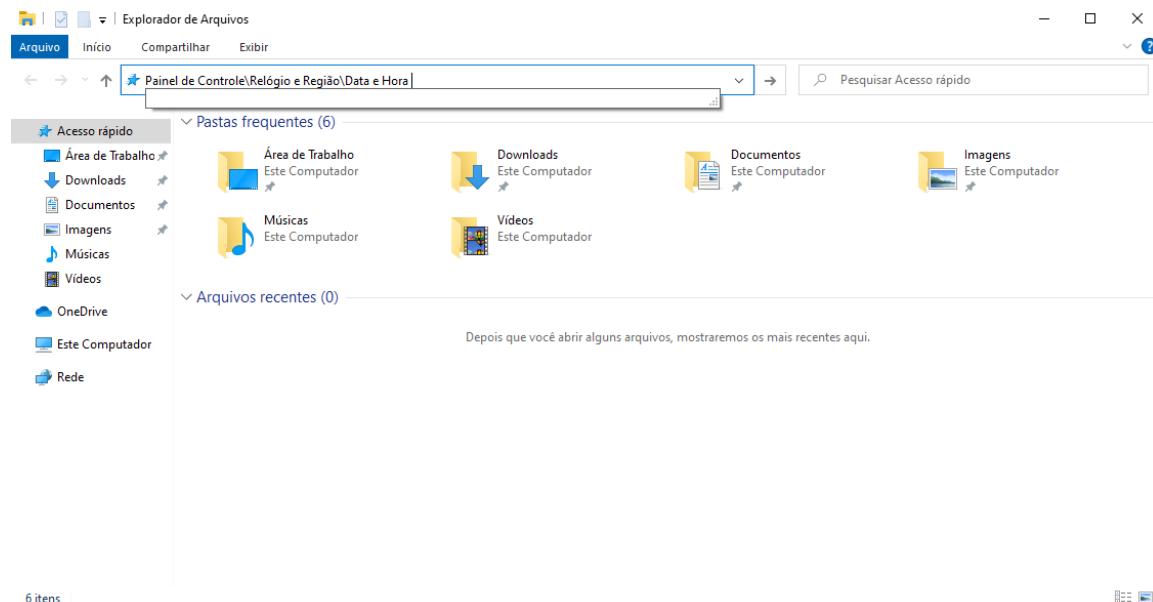

Configuração do Computador > Modelos Administrativos > Componentes do Windows > Windows Update

- Habilitando o Gerenciamento de Energia do Windows Update para ativar automaticamente o sistema e instalar atualizações agendadas: **Habilitado**
- Configurar atualizações automáticas: **4 – Baixar automaticamente e agendar a instalação**
 - Instalar durante a manutenção automática: ✓
 - **0 – Todo dia**
 - **17:00**
 - A cada semana: ✓
 - Instalar atualizações para outros produtos Microsoft: ✓
- Remover acesso ao recurso “Pausar atualizações”: **Habilitado**
- Não há reinicializações automáticas para usuários conectados, referentes às instalações de atualizações automáticas agendadas: **Habilitado**

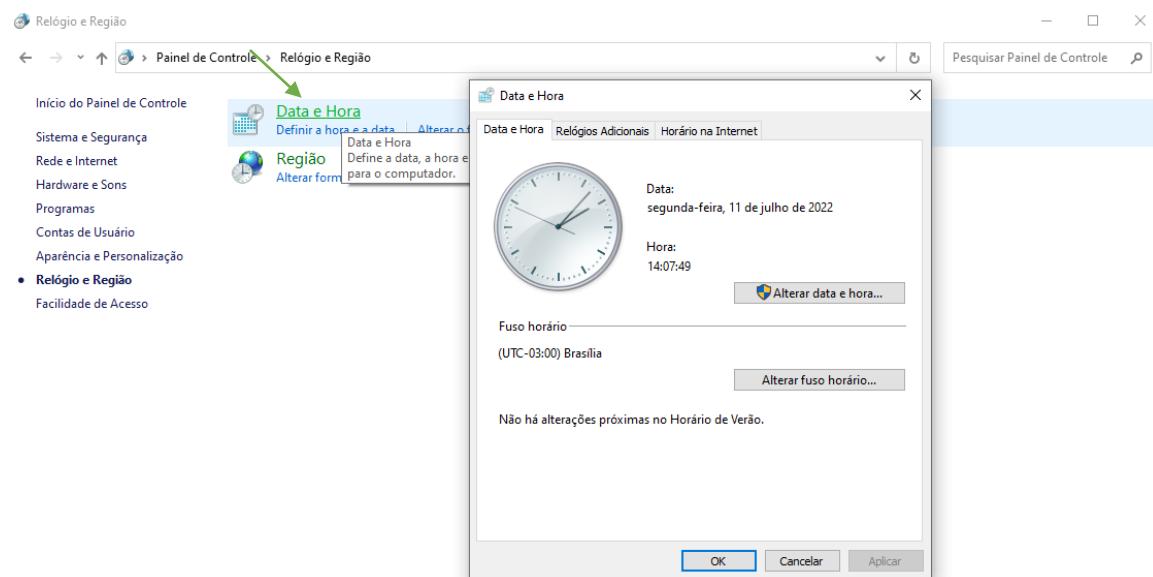

Como esta política deve ficar:

9 Sincronia da Data e Hora

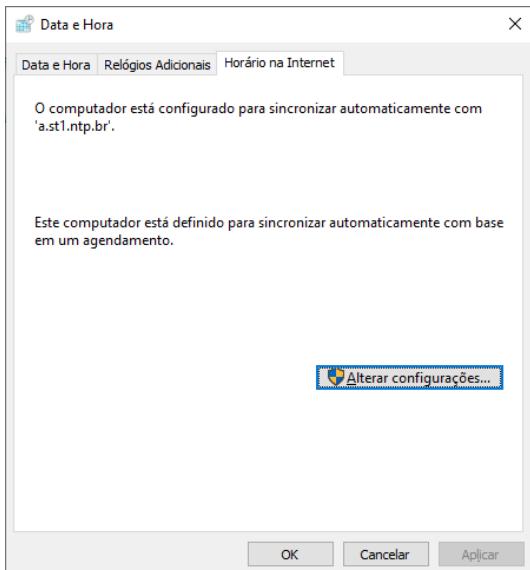
Após configurar o backup do log de eventos, vamos configurar a sincronia do relógio do Windows. Para isso, abra o **Windows Explorer** e na barra de endereços digite **Painel de Controle\Relógio e Região\Data e Hora** e pressione **ENTER** para abrir as configurações de data e hora (imagens).



Ou abra o **Painel de Controle**, clique em **Relógio e Região** e após em **Data e Hora**



Clique em **Horário na Internet** e após em **Alterar configurações...**



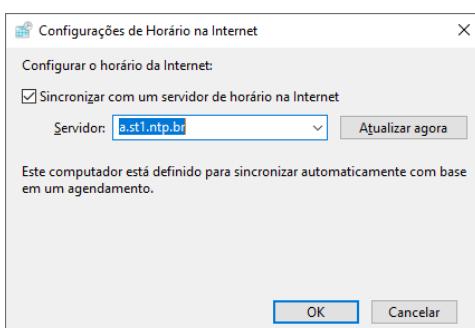
Em **servidor**, digite o endereço para sincronizar o horário, clique em **Atualizar agora** e confirme em **OK**.

O endereço é:

a.st1.ntp.br

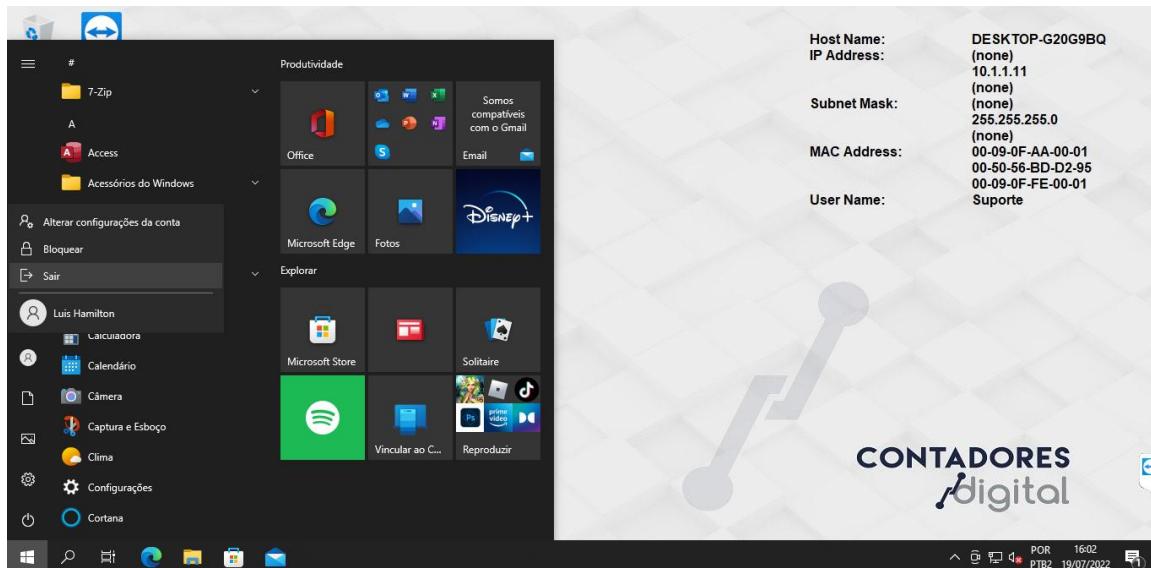
O endereço para configurar a sincronia do relógio para outras Autoridades Certificadoras, como a Soluti, é:

ntp.acsoluti.com.br

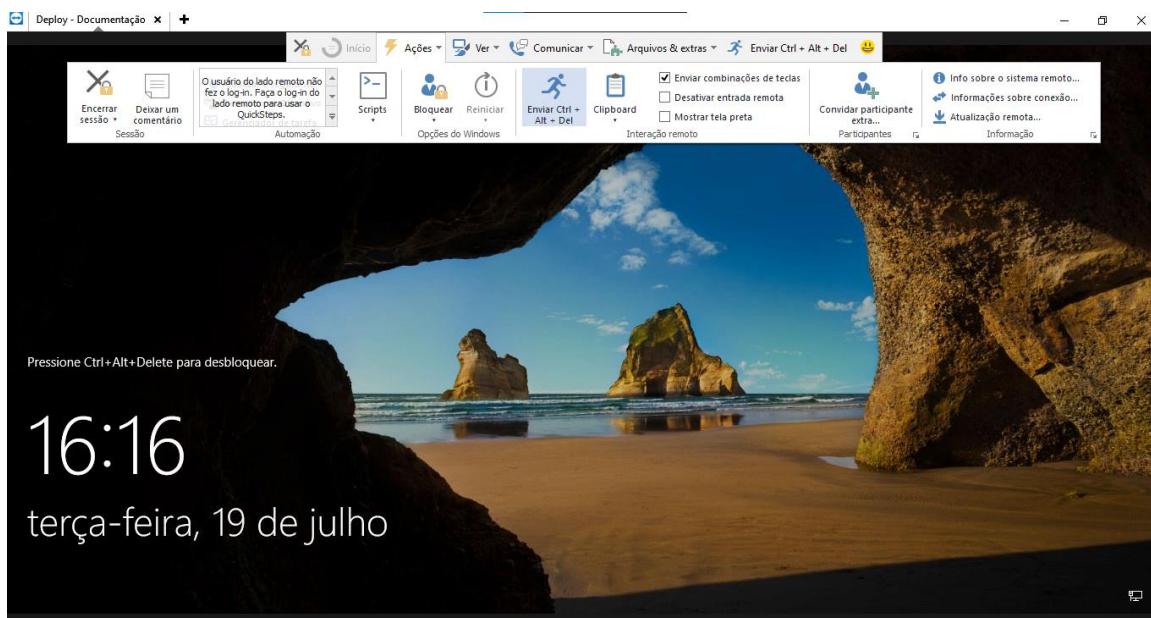


10 Configurando o perfil do usuário

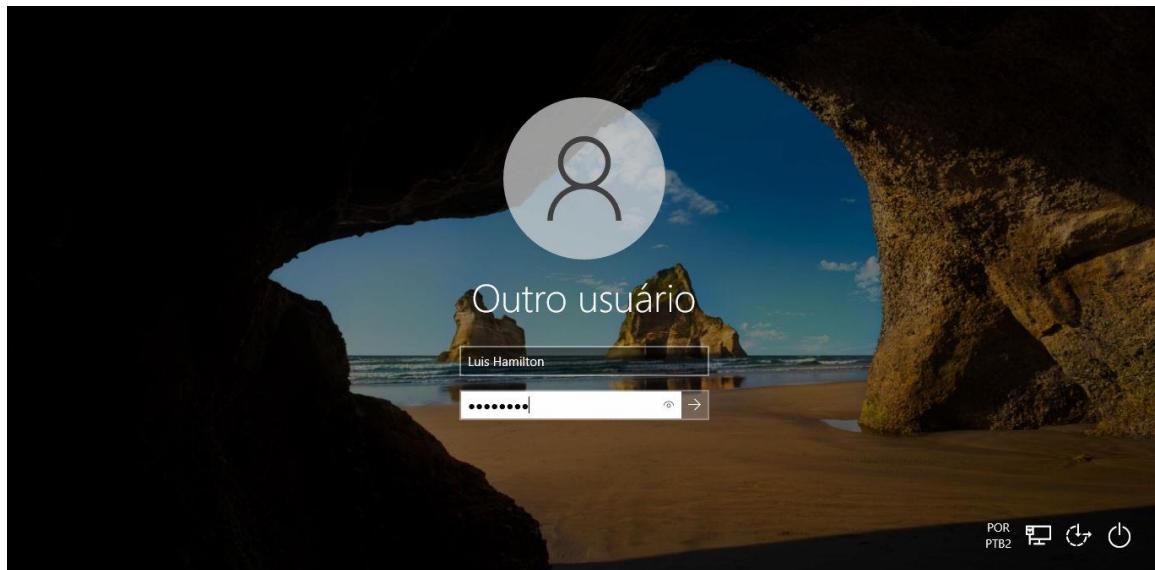
Agora iremos configurar o perfil do usuário. Saia do usuário **Suporte** abrindo o menu Iniciar, clicando na figura do perfil e depois em **Sair**.



Na tela de logon interativo, use a opção **Enviar Ctrl + Alt + Del**, ou clique em **Ações** e depois em **Enviar Ctrl + Alt + Del** para poder digitar as credenciais.



Digite as credenciais criadas para o AGR e se logue no usuário para configurar.



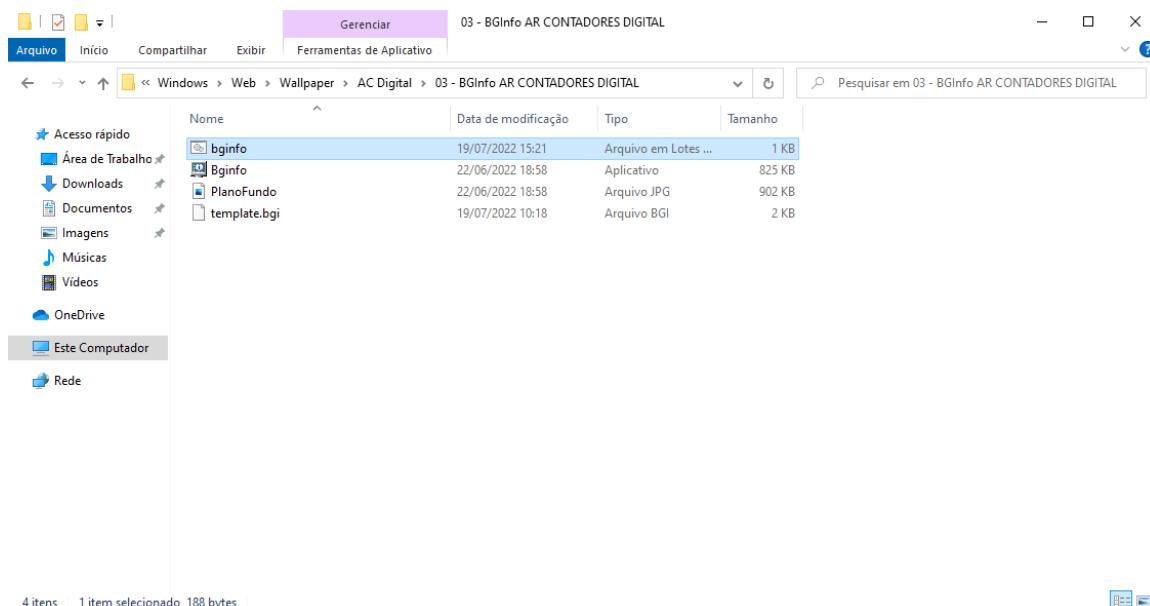
10.1 BG Info

Com a tela do usuário iniciada, vamos configurar o plano de fundo através do BG Info.

Copie para a área de trabalho do usuário [a pasta do BG Info referente a AR](#) que está sendo configurada, depois mova a pasta para o diretório **%SYSTEMROOT%\Web\Wallpaper\AC Digital**.

Pode ser necessário criar a pasta **AC Digital** neste diretório.

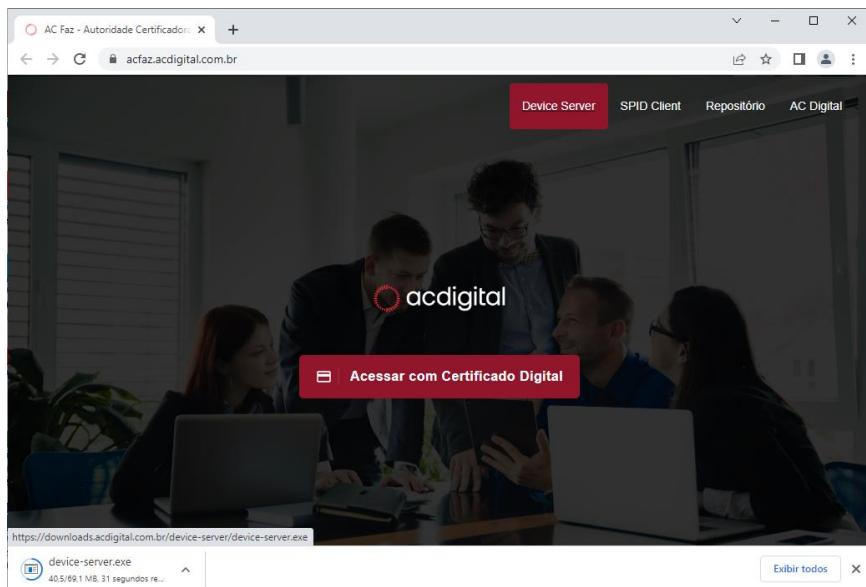
Execute a bat **bginfo** e o plano de fundo estará configurado.



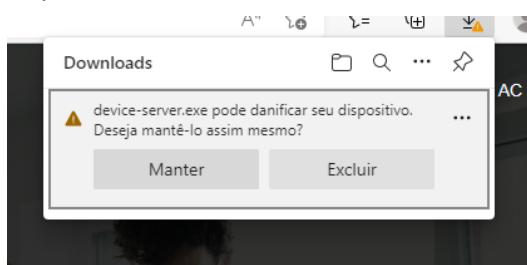
10.2 Device Server

Acesse a página do [AC Faz](#) para realizar o download da versão atual: acfaz.acdigital.com.br.

No canto superior direito, clique em **Device Server** para realizar o download do instalador.



Alguns navegadores podem exibir a mensagem informando que o aplicativo é inseguro. Neste caso, clique em **Manter**



Após o download, execute o instalador.

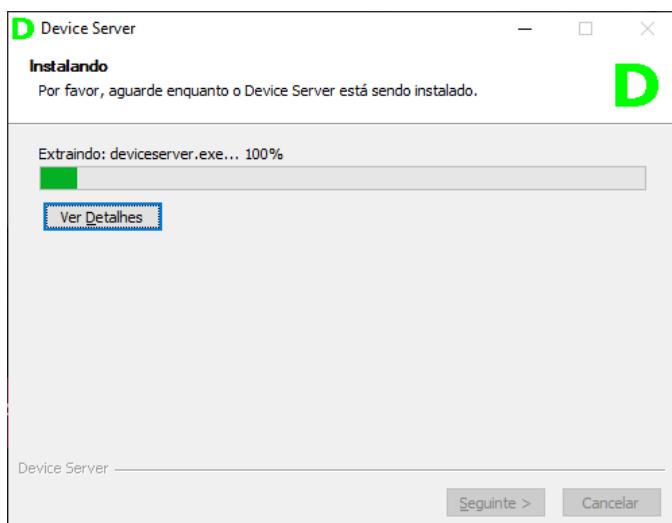
Dependendo da configuração do sistema, pode ocorrer o alerta informando que a aplicação não é segura. Clique em **Mais informações**.



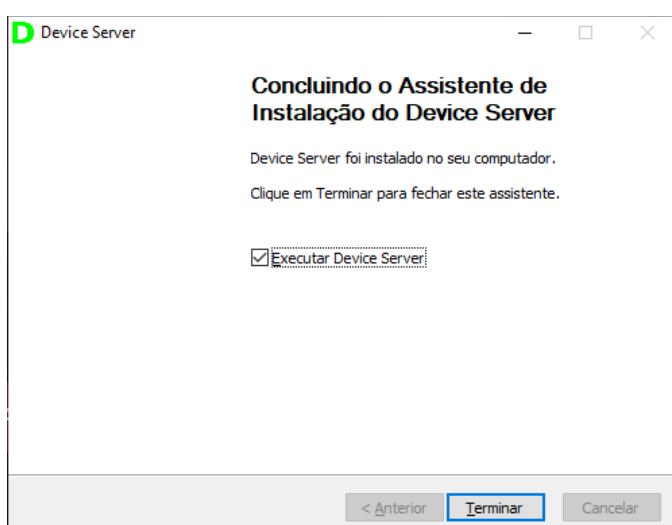
Clique agora em **Executar assim mesmo.**



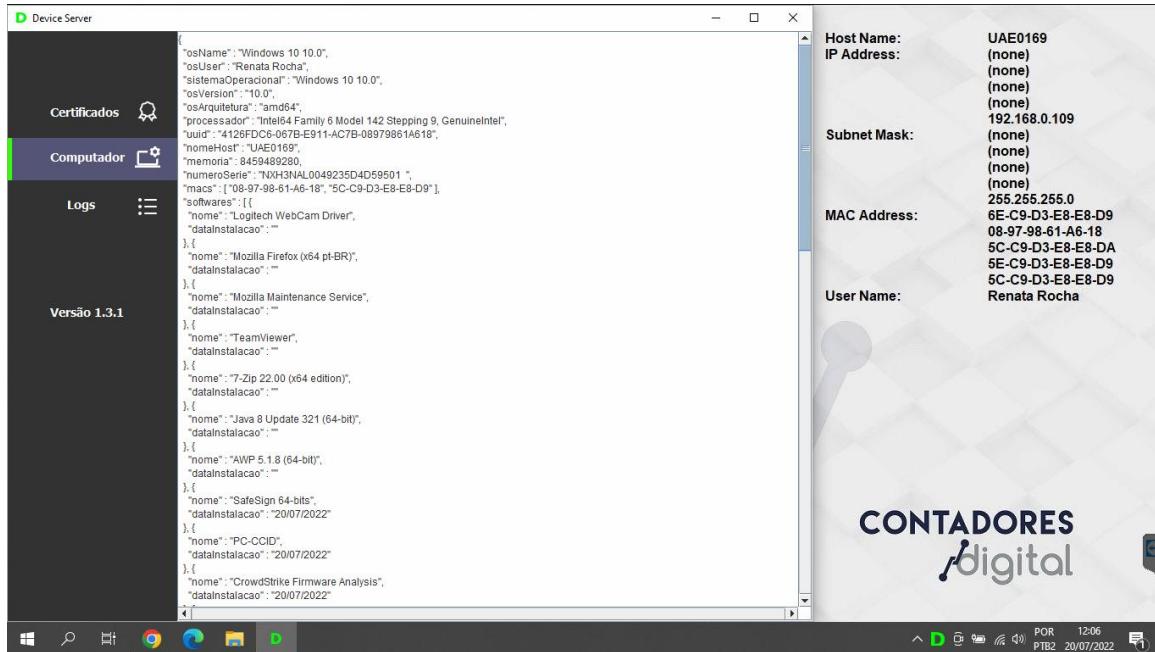
A instalação é automática.



Após o término da instalação, clique em **Terminar**.

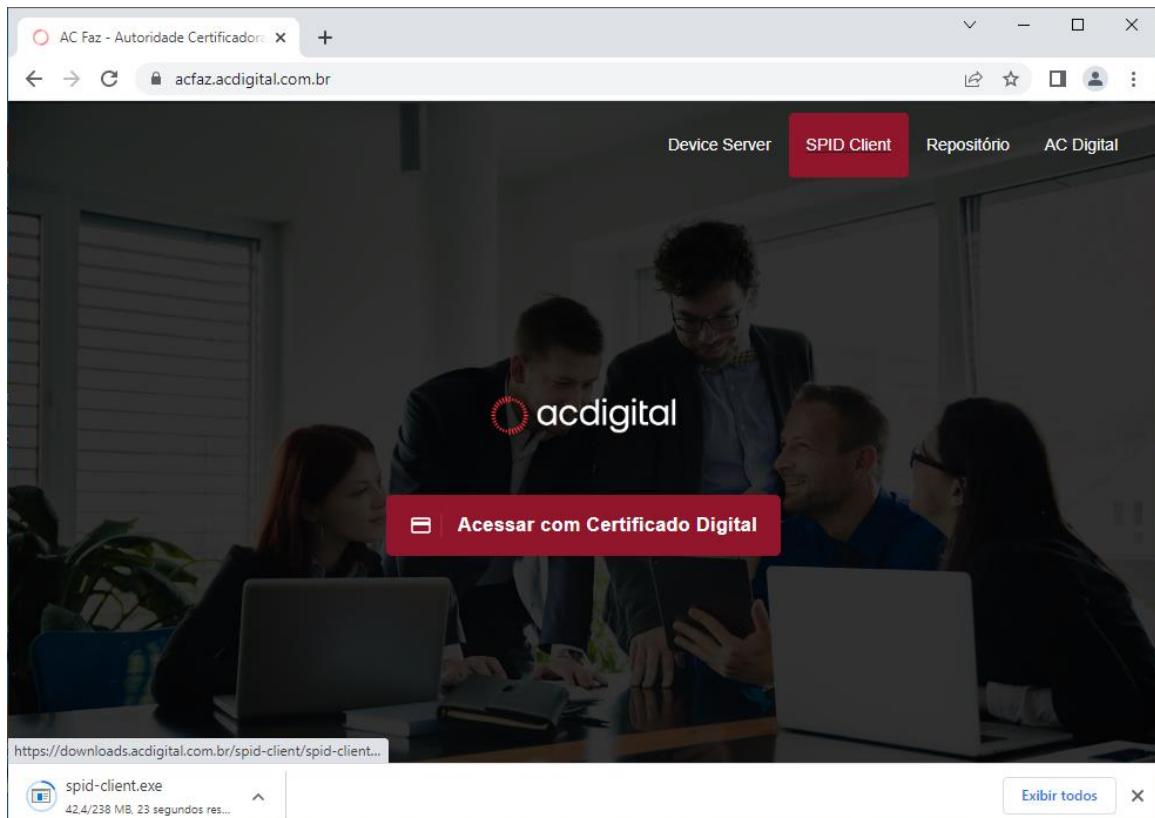


O Device Server estará instalado.



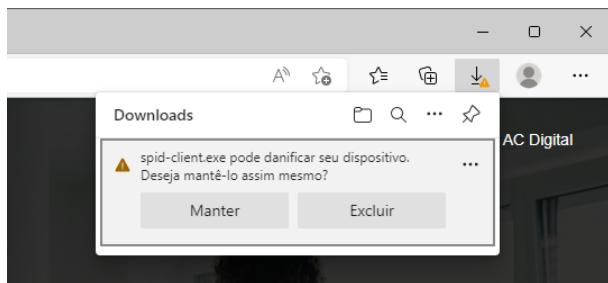
10.3 SPID Client

Volte a página da AC Faz para realizar o download do **SPID Client**, clicando em Spid Client.

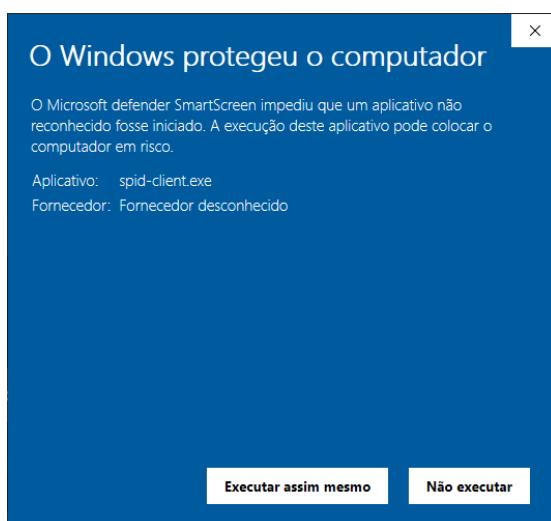


CONTEÚDO INTERNO

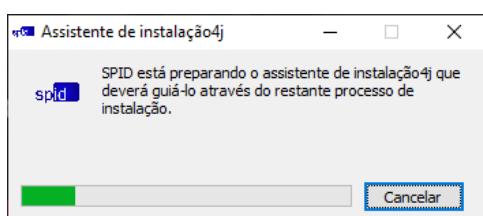
Assim como o Device, alguns navegadores podem informar que o SPID não é seguro. Clique em manter e execute o instalador.



O Spid também pode ser detectado como inseguro pelo Windows. Assim como anteriormente, clique em **Mais informações** e após em **Executar assim mesmo**.

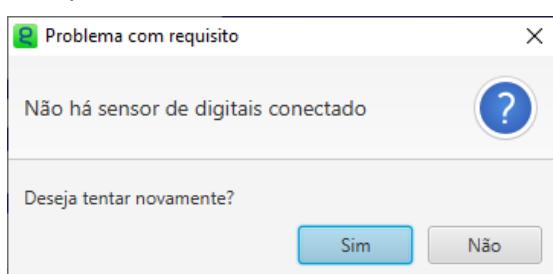


A instalação ocorrerá de forma automática.



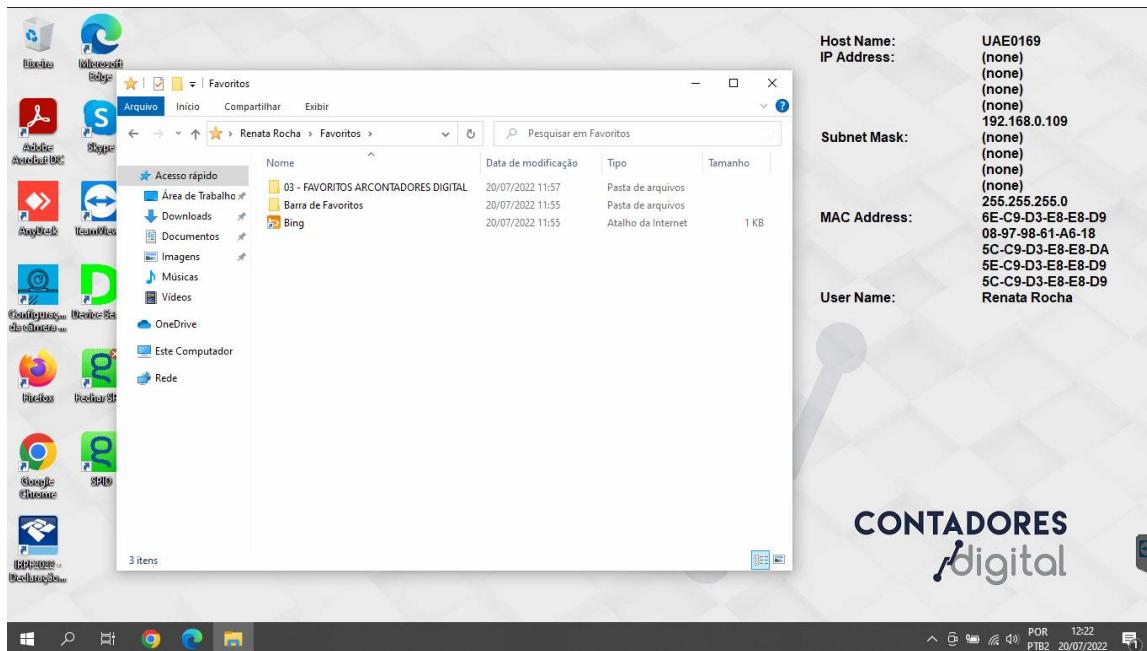


Não havendo dispositivos biométricos detectados, a informação seguinte será exibida. Clique em **Não** e o Spid estará instalado.



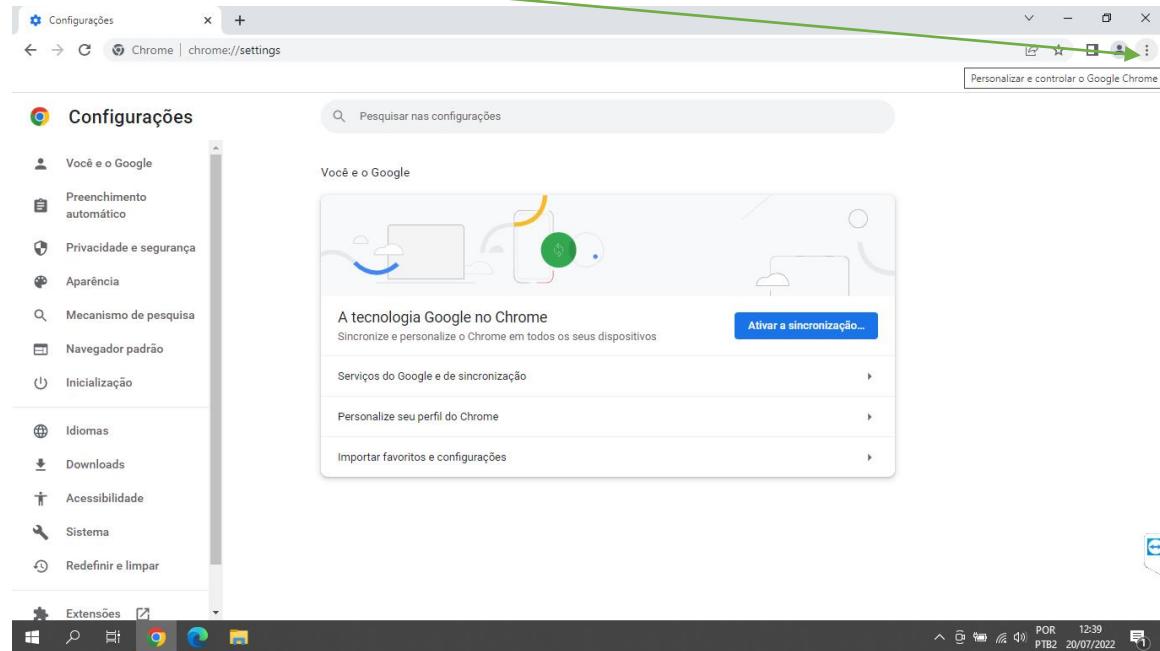
10.4 Navegadores e Favoritos

Resta agora configurar os favoritos do Google Chrome e Firefox. Copie para o diretório de favoritos do usuário a pasta respectiva a AR que está sendo configurada, conforme a imagem.

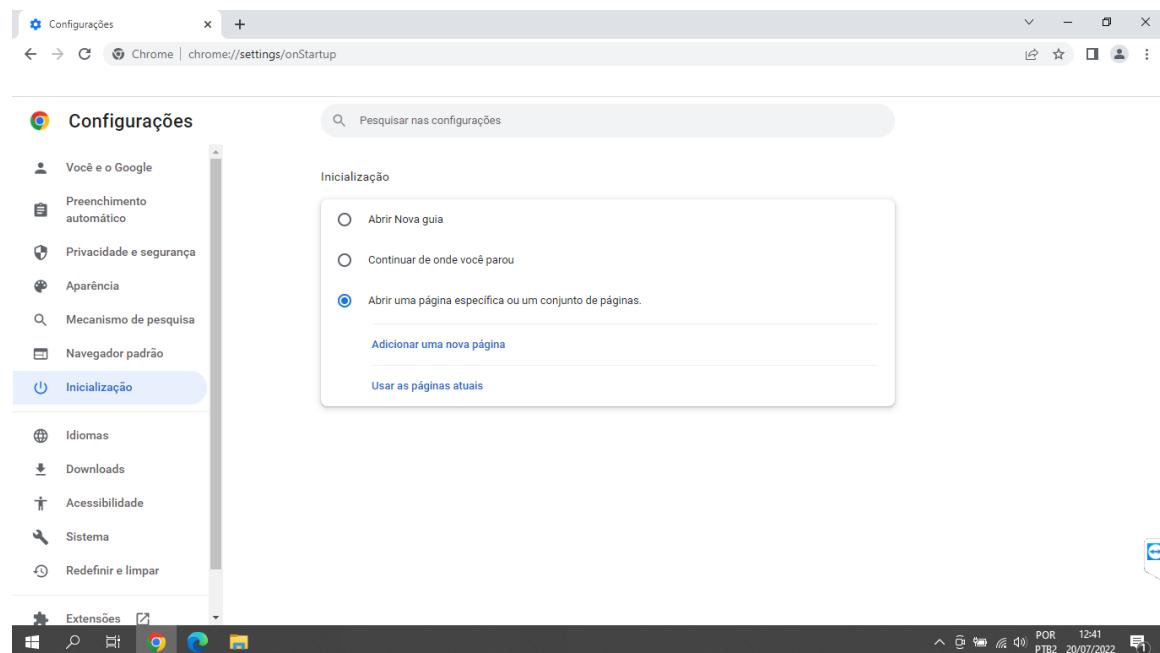


10.4.1 Google Chrome

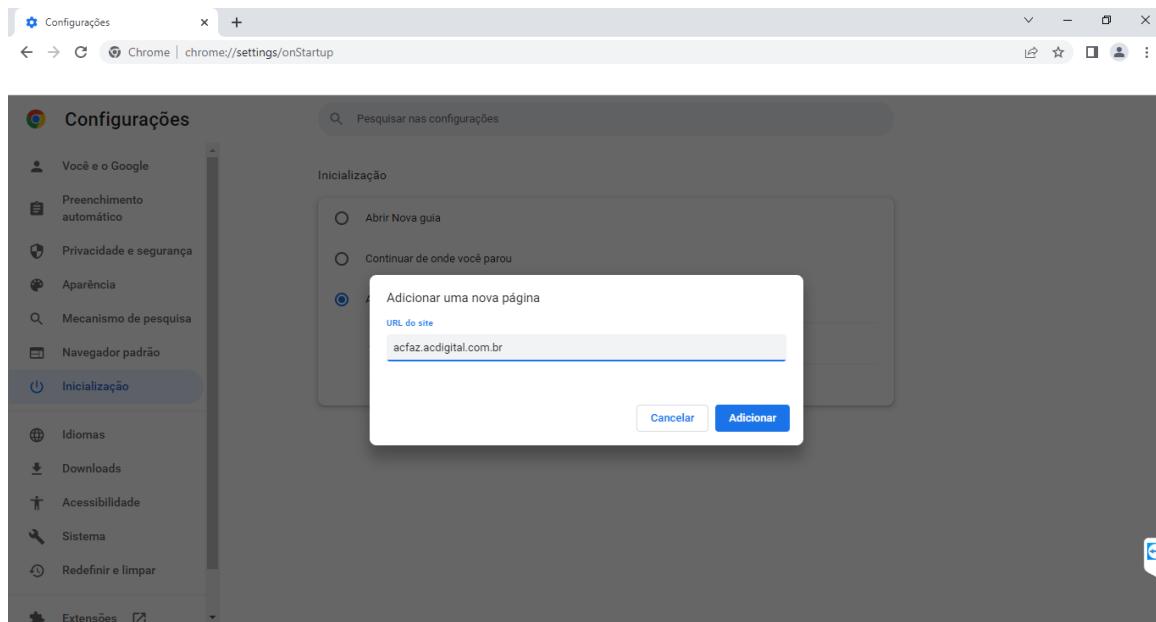
Abra o Google Chrome, clique em  > **Configurações**.



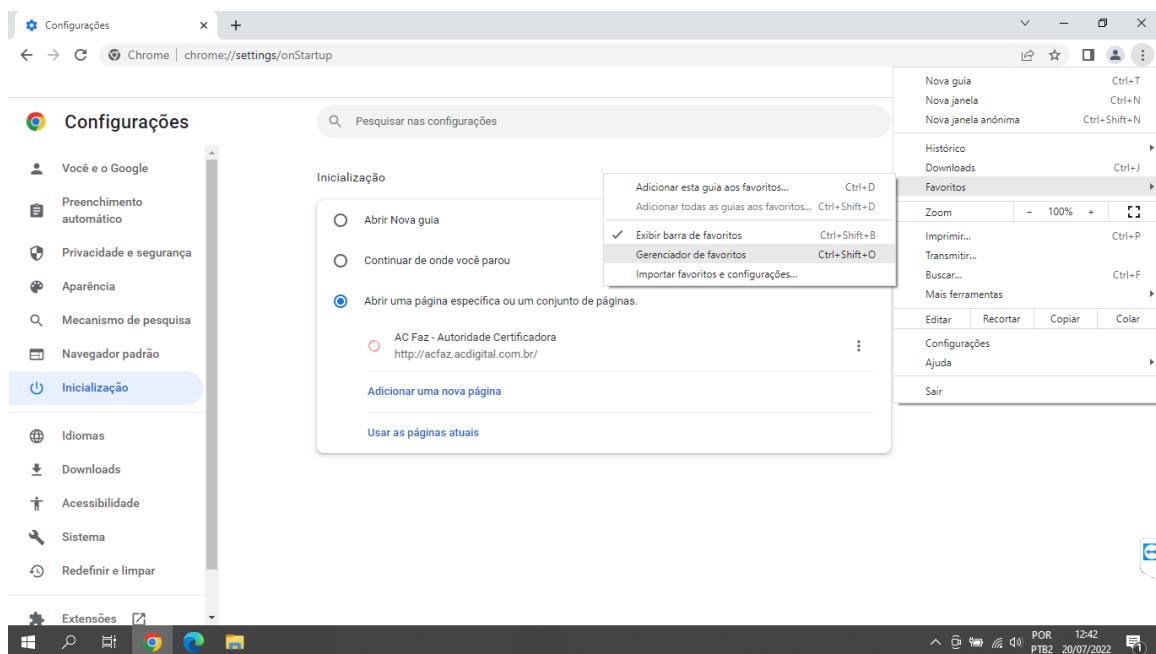
Na lateral esquerda, clique em **Inicialização** e após, selecione a opção **Abrir uma página específica ou um conjunto de páginas**.



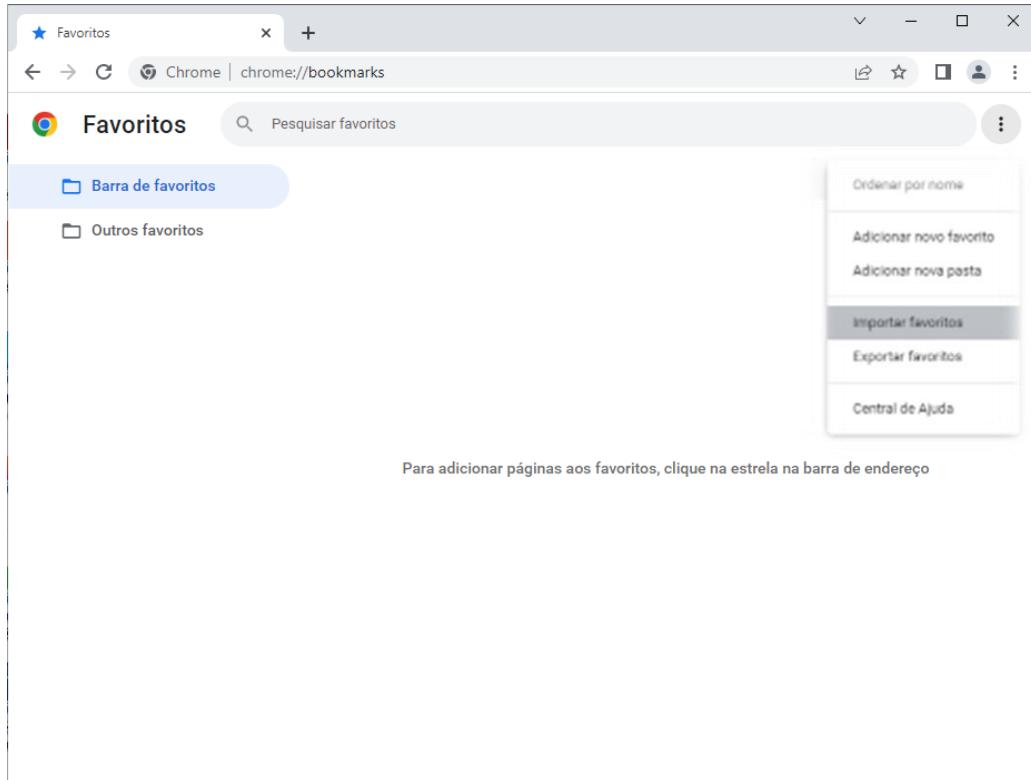
Clique em **Adicionar uma nova página** e digite o endereço da AC Faz: **acfaz.acdigital.com.br** e clique em **Adicionar**.



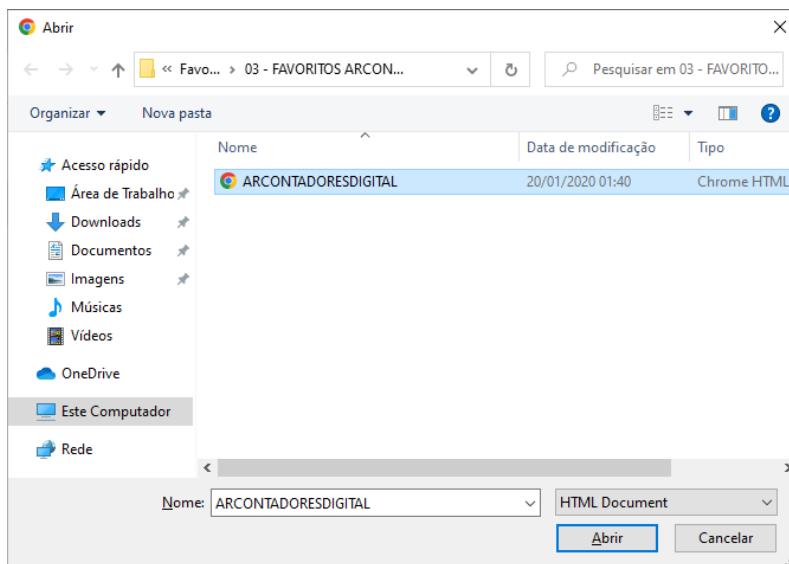
Clique novamente em  **Favoritos > Gerenciador de favoritos** ou pressione **Ctrl+Shift+O**.



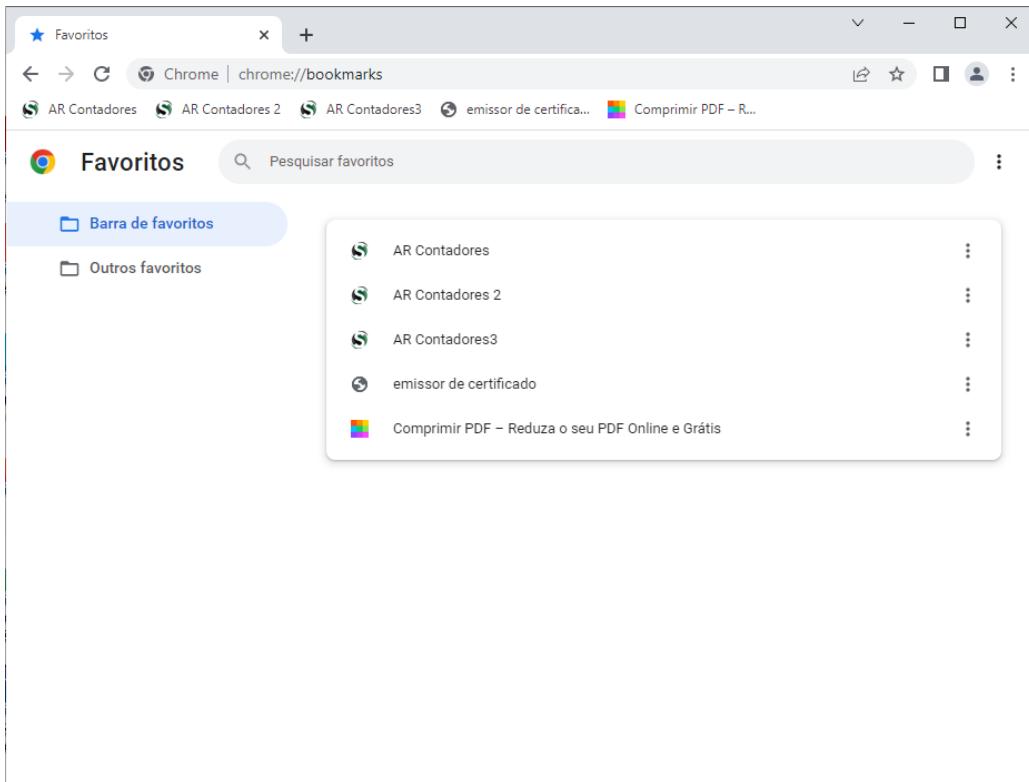
No gerenciador de favoritos do Google Chrome, clique em  > Importar favoritos.



Vá até o diretório onde os favoritos foram alocados, selecione o arquivo HTML a importar e clique em **Abrir**.

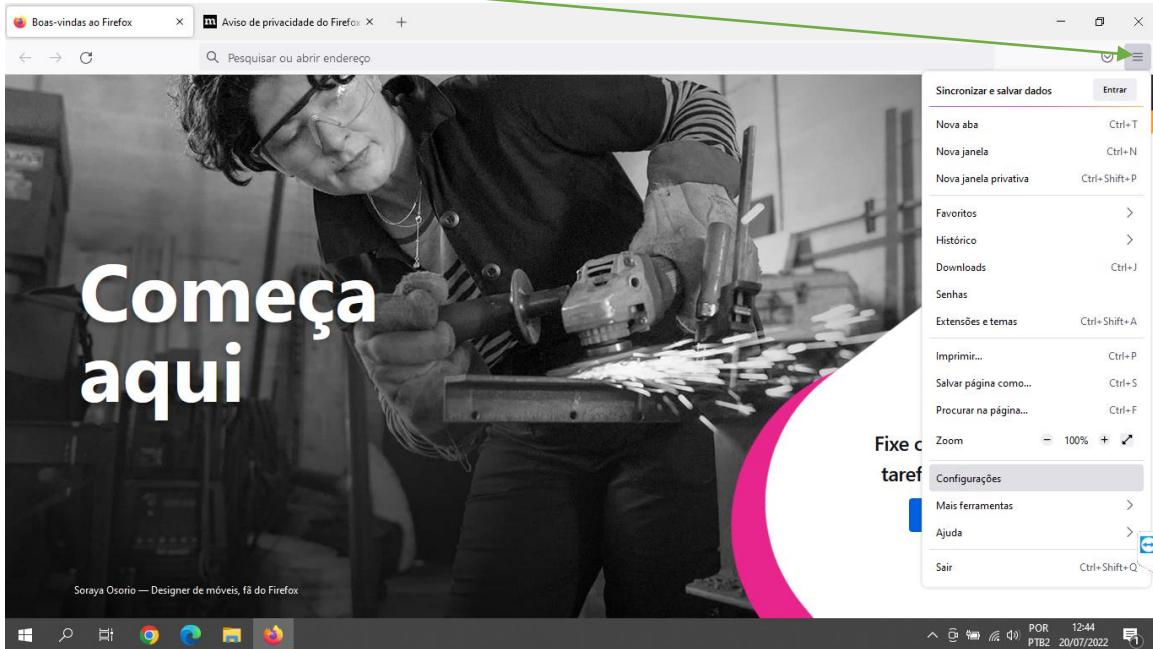


Os favoritos foram importados no Google Chrome.

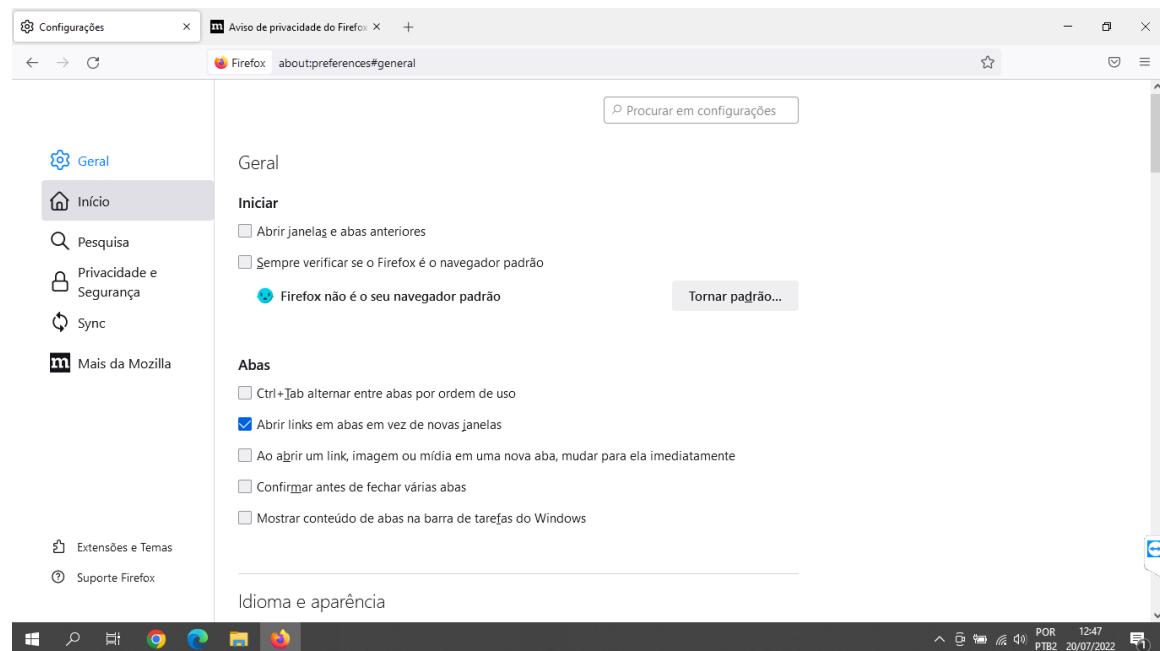


10.4.2 Mozilla Firefox

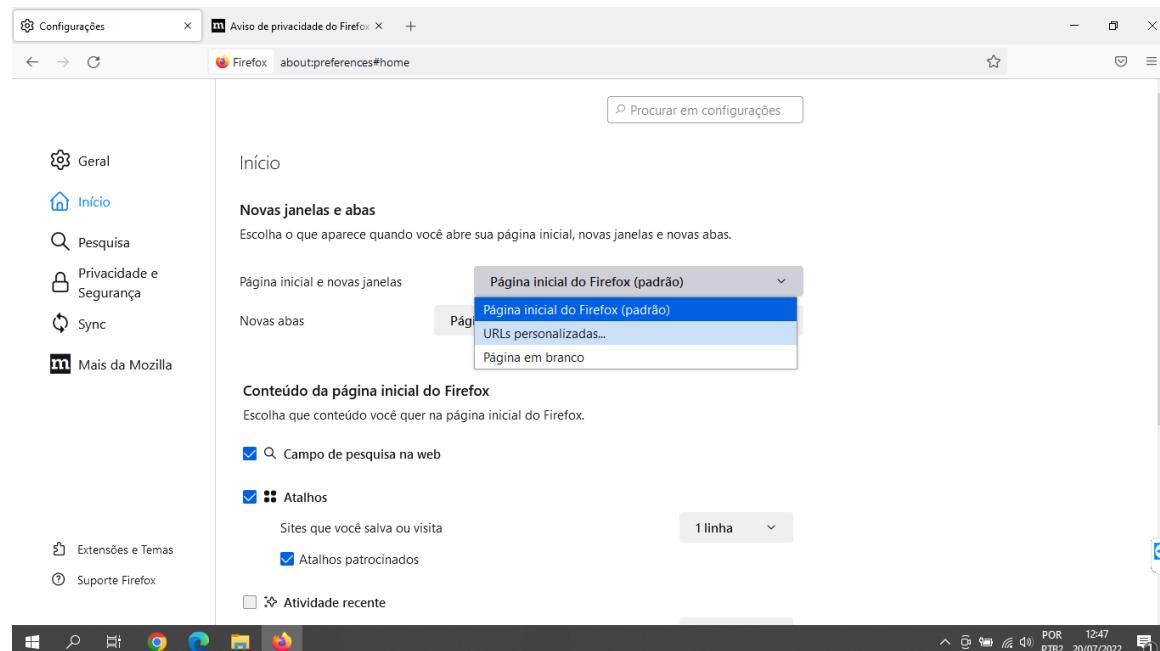
Abra agora o Firefox, clique em  > Configurações.



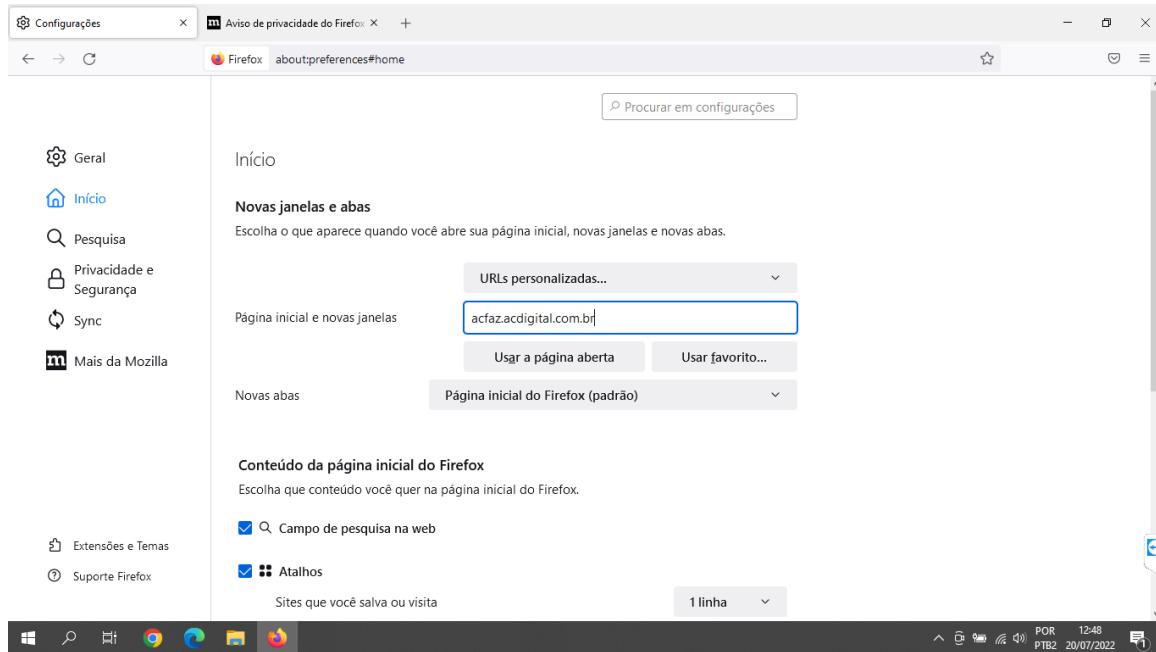
Desmarque a opção **Sempre verificar se o Firefox é o navegador padrão** e na lateral esquerda clique em **Início**.



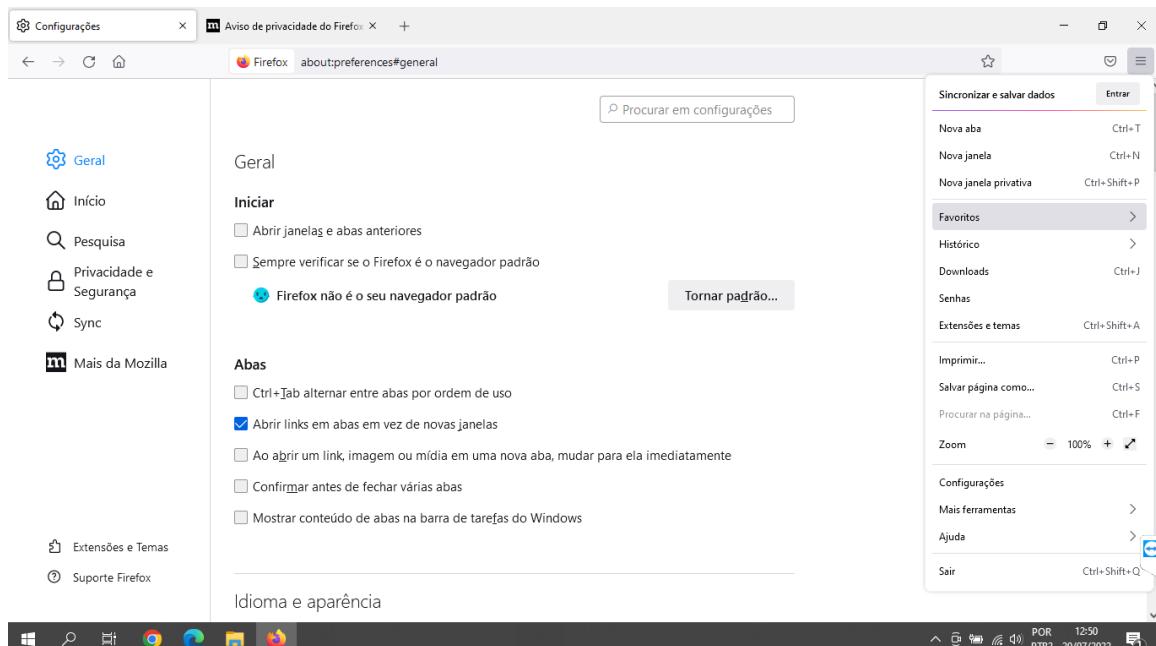
Em Página inicial e novas janelas, clique em **URLs personalizadas**.

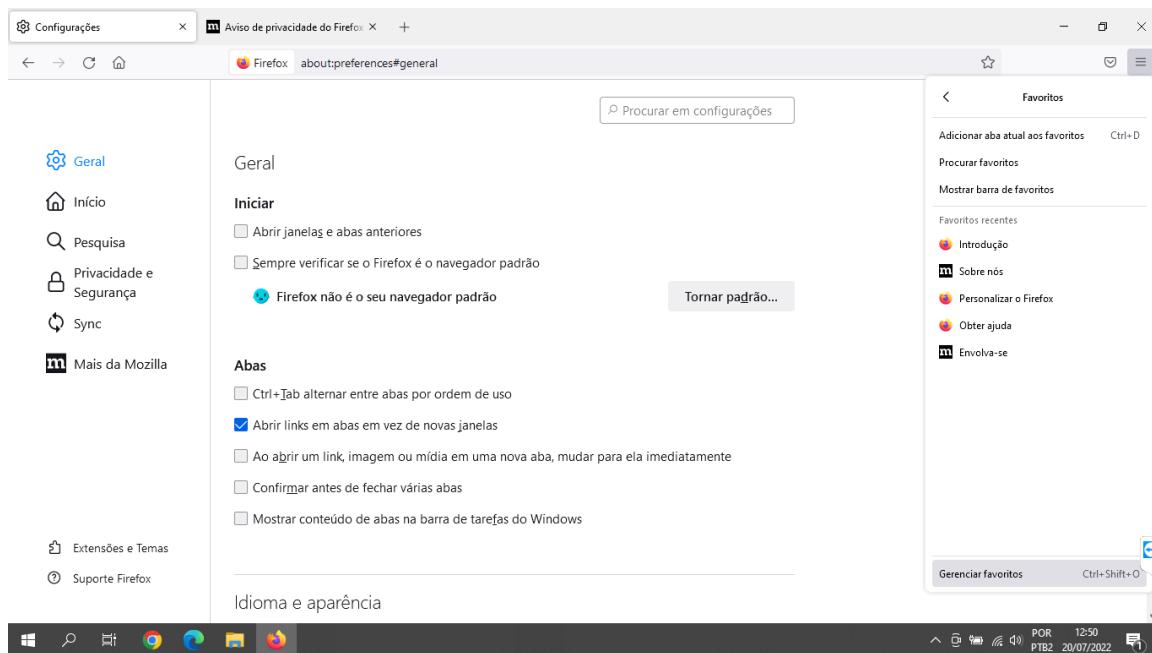


Digite o endereço da AC Faz: acfaz.acdigital.com.br.

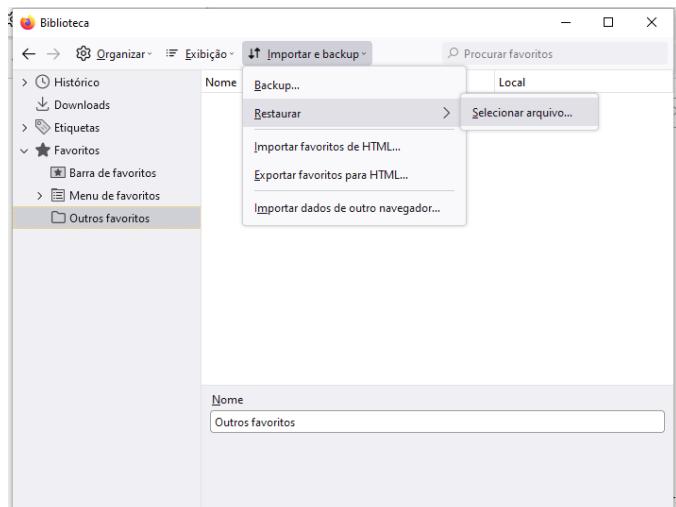


Após, clique novamente em  > **Favoritos** e clique em **Gerenciar favoritos**, ou pressione **Ctrl+Shift+O**.

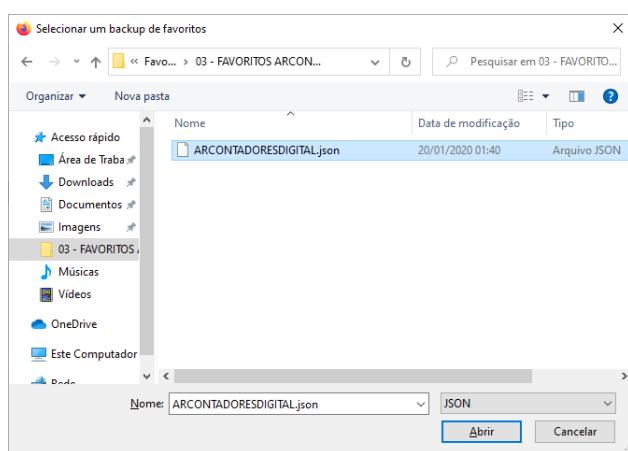




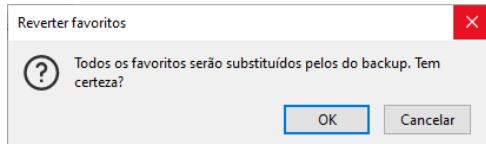
Na biblioteca de favoritos do Firefox, clique em **Importar e backup > Restaurar > Selecionar arquivo**.



Navegue até o diretório onde foram alocados os favoritos da AR, e selecione o arquivo JSON para importar os favoritos do Firefox.



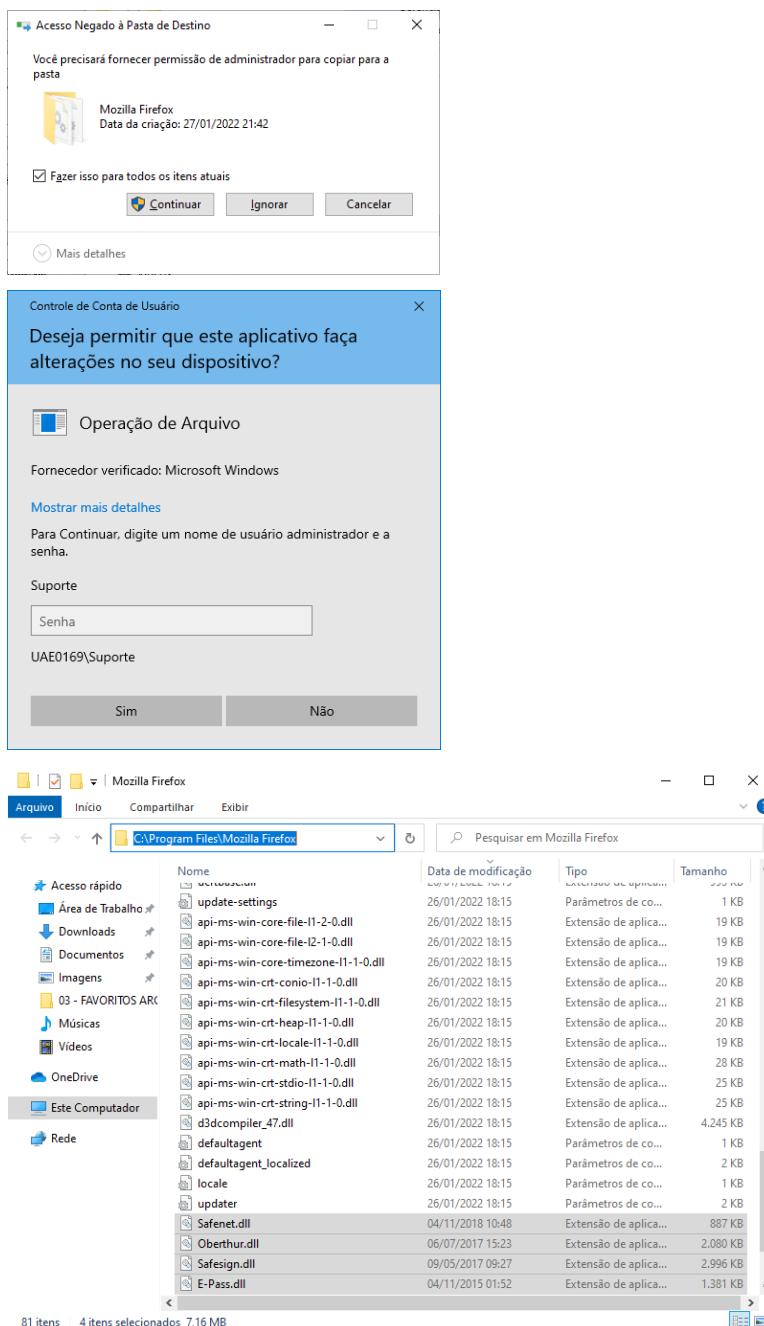
Confirme clicando em **OK**.



Os favoritos estarão importados, restando apenas configurar as bibliotecas dos gerenciadores de certificados no Firefox.

10.4.2.1 Bibliotecas dos gerenciadores de certificados no Firefox

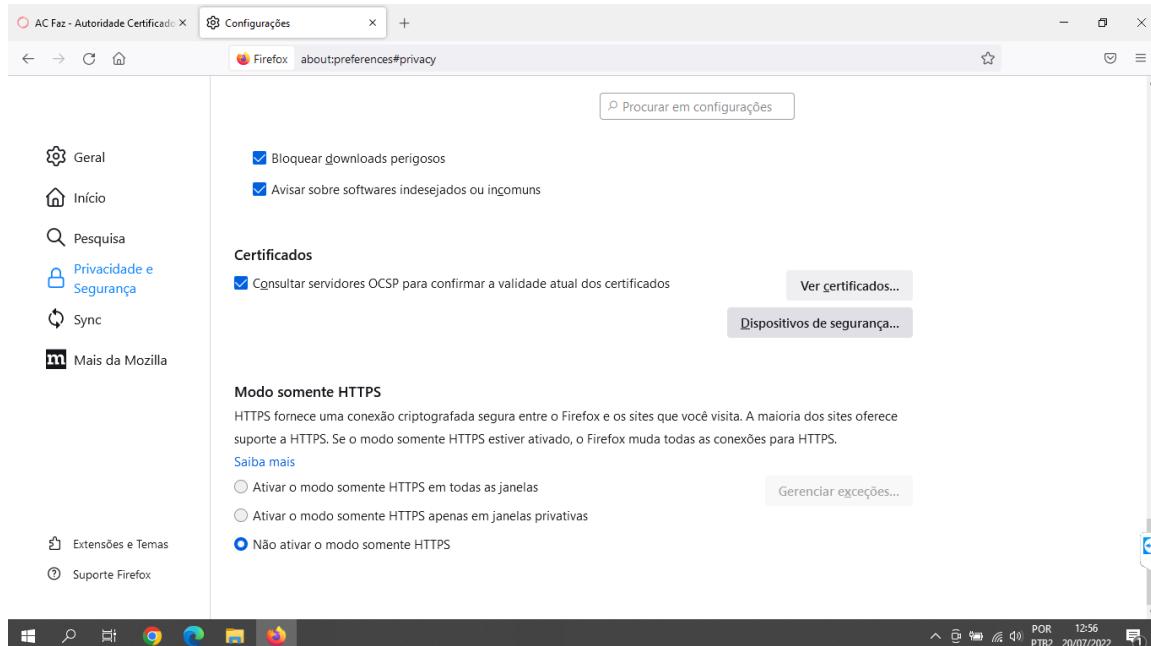
Para importar, cole as bibliotecas [DLL dos gerenciadores](#) (disponível no SharePoint) no diretório onde foi instalado o Firefox, sendo geralmente **C:\Program Files\Mozilla Firefox**. Serão necessários privilégios de Administrador (credenciais do usuário Suporte).



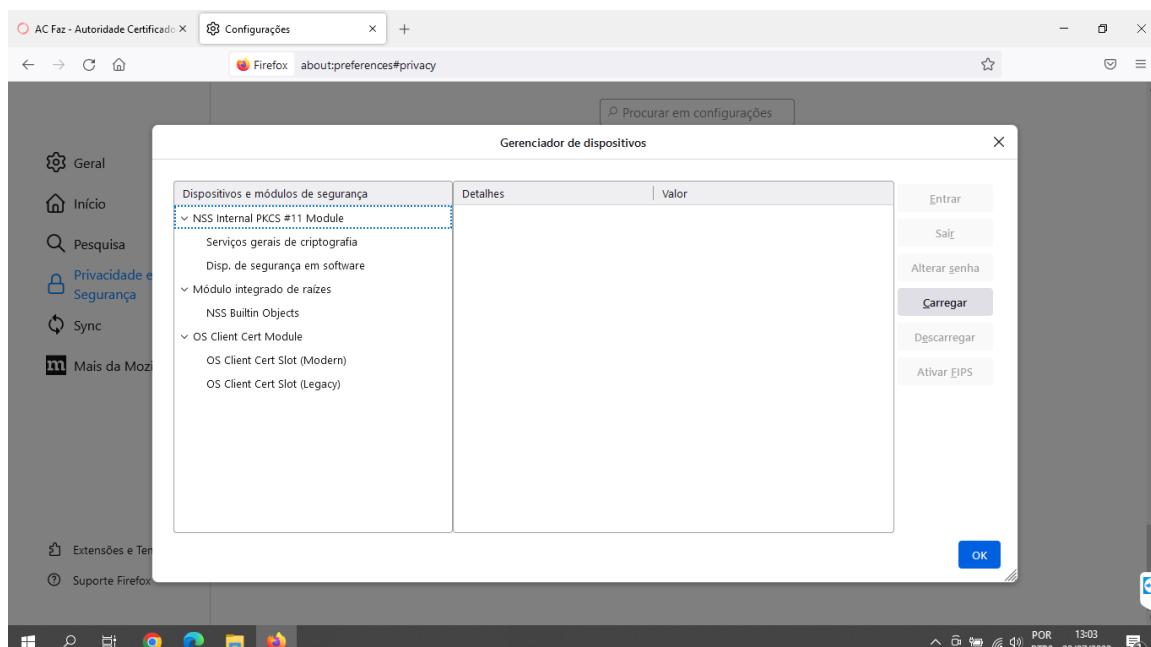
Nome	Data de modificação	Tipo	Tamanho
update-settings	26/01/2022 18:15	Parâmetros de co...	1 KB
api-ms-win-core-file-l1-2-0.dll	26/01/2022 18:15	Extensão de aplica...	19 KB
api-ms-win-core-file-l2-1-0.dll	26/01/2022 18:15	Extensão de aplica...	19 KB
api-ms-win-core-timezone-l1-1-0.dll	26/01/2022 18:15	Extensão de aplica...	19 KB
api-ms-win-crt-conio-l1-1-0.dll	26/01/2022 18:15	Extensão de aplica...	20 KB
api-ms-win-crt-fs-l1-1-0.dll	26/01/2022 18:15	Extensão de aplica...	21 KB
api-ms-win-crt-heap-l1-1-0.dll	26/01/2022 18:15	Extensão de aplica...	20 KB
api-ms-win-crt-locale-l1-1-0.dll	26/01/2022 18:15	Extensão de aplica...	19 KB
api-ms-win-crt-math-l1-1-0.dll	26/01/2022 18:15	Extensão de aplica...	28 KB
api-ms-win-crt-studio-l1-1-0.dll	26/01/2022 18:15	Extensão de aplica...	25 KB
api-ms-win-crt-string-l1-1-0.dll	26/01/2022 18:15	Extensão de aplica...	25 KB
d3dcompiler_47.dll	26/01/2022 18:15	Extensão de aplica...	4.245 KB
defaultagent	26/01/2022 18:15	Parâmetros de co...	1 KB
defaultagent_localized	26/01/2022 18:15	Parâmetros de co...	2 KB
locale	26/01/2022 18:15	Parâmetros de co...	1 KB
updater	26/01/2022 18:15	Parâmetros de co...	2 KB
Safenet.dll	04/11/2018 10:48	Extensão de aplica...	887 KB
Oberthur.dll	06/07/2017 15:23	Extensão de aplica...	2.080 KB
Safesign.dll	09/05/2017 09:27	Extensão de aplica...	2.996 KB
E-Pass.dll	04/11/2015 01:52	Extensão de aplica...	1.381 KB

Após colar, abra o Firefox, clique em  > **Configurações > Privacidade e Segurança**.

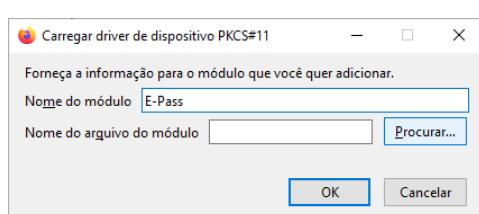
Role até o final da página e clique em **Dispositivos de segurança**.



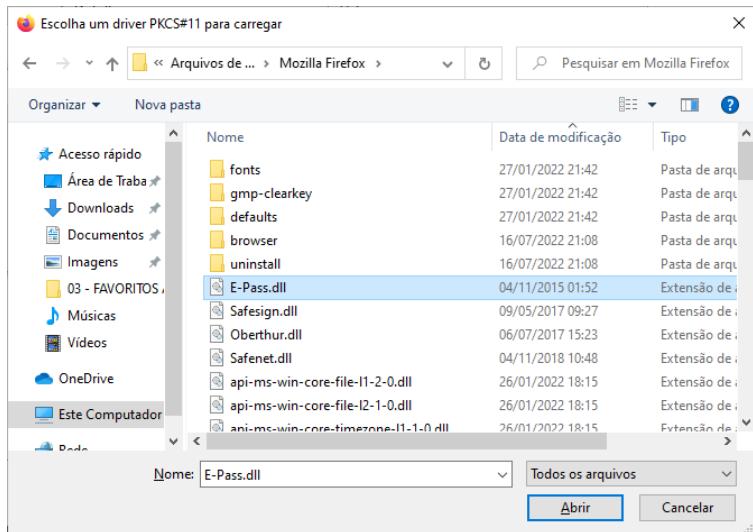
No menu de gerenciador de dispositivos do Firefox, clique em **Carregar**



Digite o nome da biblioteca a ser incluída, clique em **Procurar** e vá até o diretório onde foram coladas as DLL's.

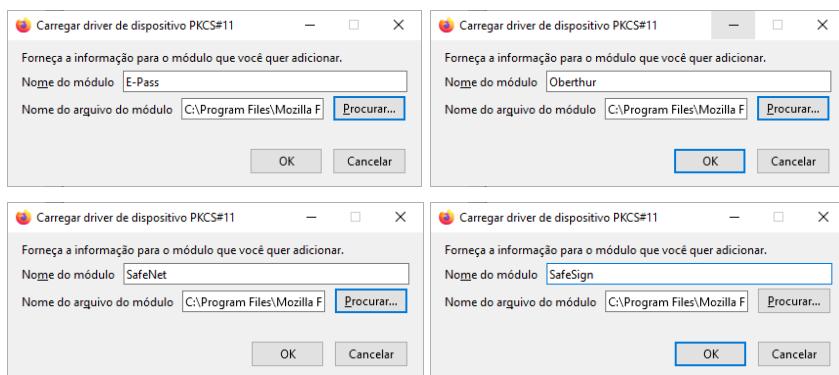


Selecione a **DLL** correspondente e clique em **Abrir**.



Repita o passo para as demais bibliotecas, elas são:

- E-Pass
- Oberthur
- SafeNet
- SafeSign

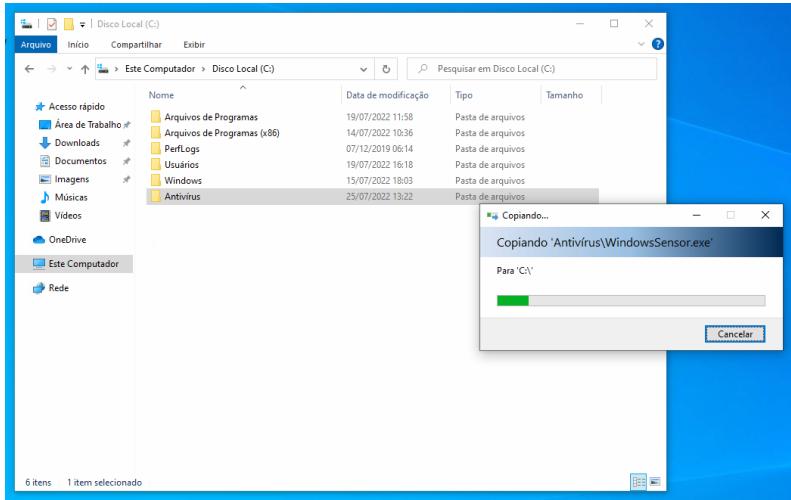


O perfil do usuário está completamente configurado, restando apenas a criptografia do computador.

11 Antivírus

Todos os computadores de AR devem possuir antivírus instalado. Dependendo da AR, o antivírus a ser instalado será o Falcon CrowdStrike, disponível no [SharePoint](#).

Para instalar o Falcon, cole a pasta com a bat e instalador no disco C do sistema.



Abra o Prompt de Comandos como administrador e navegue até a raiz da pasta onde estão os instaladores e, **pelo prompt, execute a bat**.

```
Administrator: Prompt de Comando - falcon.bat
Microsoft Windows [versão 10.0.19044.1826]
(c) Microsoft Corporation. Todos os direitos reservados.

C:\Windows\system32>cd..
C:\Windows>cd..
C:\>cd Antivirus
C:\Antivirus>falcon.bat
C:\Antivirus>WindowsSensor.exe /install /quiet /norestart CID=F6129D632C8C4B1B8EDBC9F38B35EB22-E8 ProvToken=C65322C5
```

O antivírus Falcon CrowdStrike estará instalado ao término da execução deste comando.

```
Administrator: Prompt de Comando
Microsoft Windows [versão 10.0.19044.1826]
(c) Microsoft Corporation. Todos os direitos reservados.

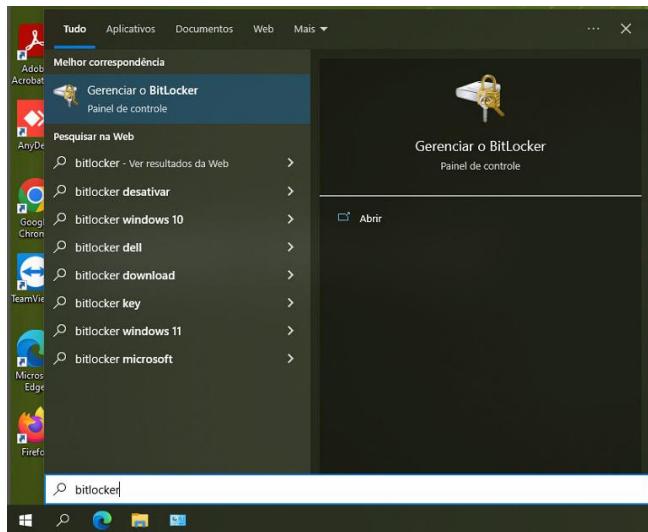
C:\Windows\system32>cd..
C:\Windows>cd..
C:\>cd Antivirus
C:\Antivirus>falcon.bat
C:\Antivirus>WindowsSensor.exe /install /quiet /norestart CID=F6129D632C8C4B1B8EDBC9F38B35EB22-E8 ProvToken=C65322C5
C:\Antivirus>
```

Não sendo uma loja própria, o antivírus a utilizar é o **Windows Defender**, nativo no Windows 10.

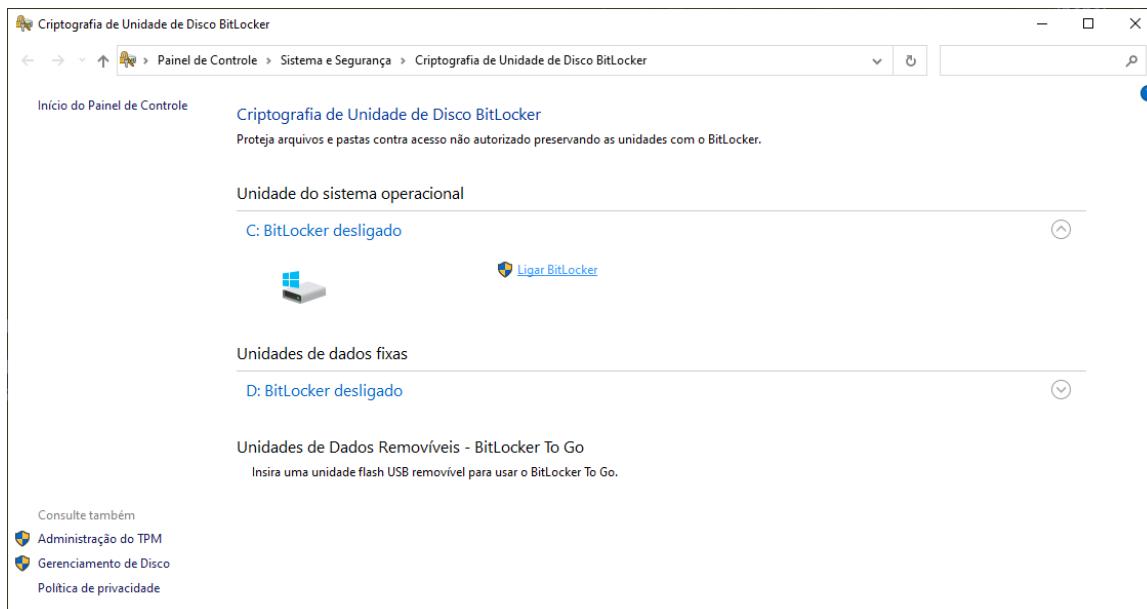
12 Criptografia

12.1 BitLocker

Ao final da configuração, precisaremos criptografar o disco do computador. Verifique se o computador dispõe do **BitLocker**. Para isso, abra o iniciar e digite **BitLocker** e pressione **Enter**.



Na tela do BitLocker, clique em **Ligar BitLocker**. Serão necessárias as credenciais de administrador (usuário Suporte).



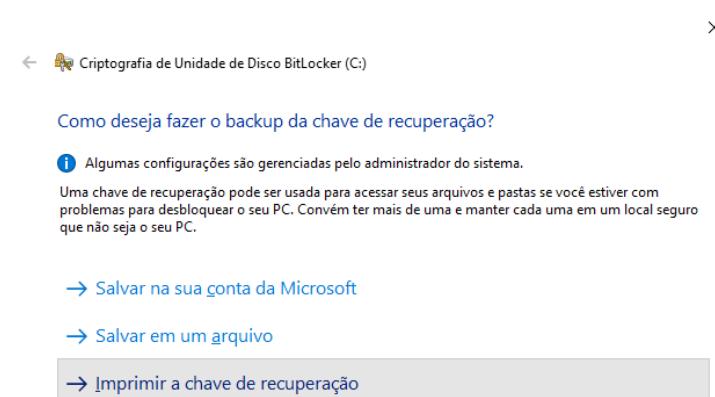
O BitLocker será carregado.



[Quais são os requisitos de sistema do BitLocker?](#)

[Cancelar](#)

Nesta tela, selecione a terceira opção: **Imprimir a chave de recuperação**.

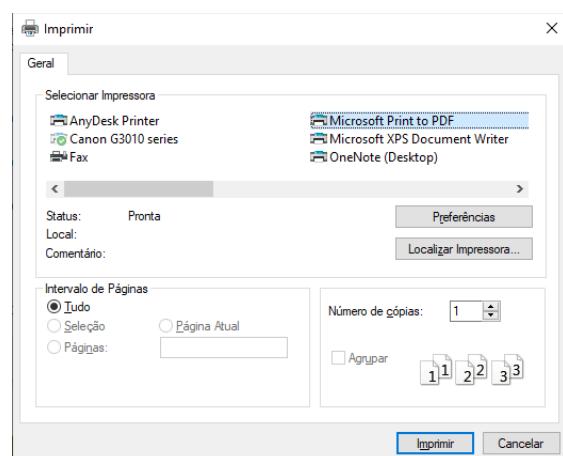


[Como posso encontrar minha chave de recuperação mais tarde?](#)

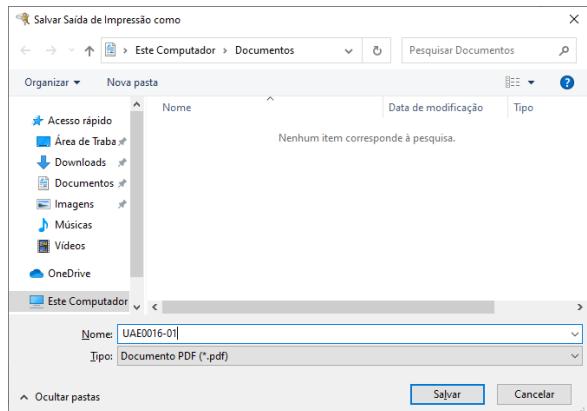
[Avançar](#)

[Cancelar](#)

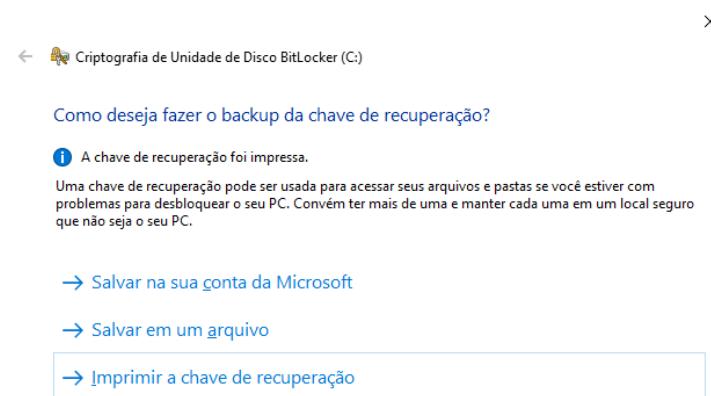
Imprima como **PDF**. Para isso, você pode selecionar imprimir com a impressora **Microsoft Print to PDF**.



Salve a **chave de recuperação** com o hostname do computador.



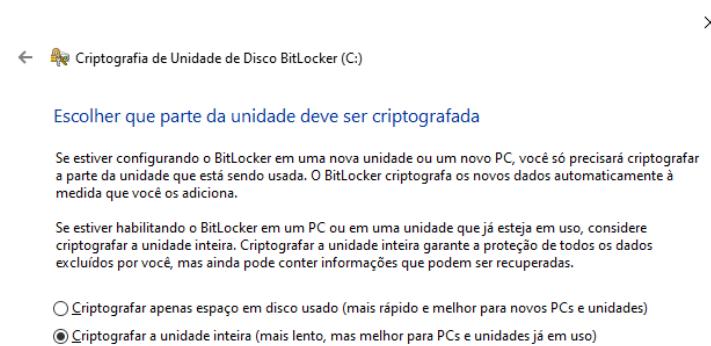
Após salvar, copie a **chave de recuperação para seu computador** e inclua o documento no **SysPass**, junto com a senha de administrador. Feito isso, clique em **Avançar**.



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

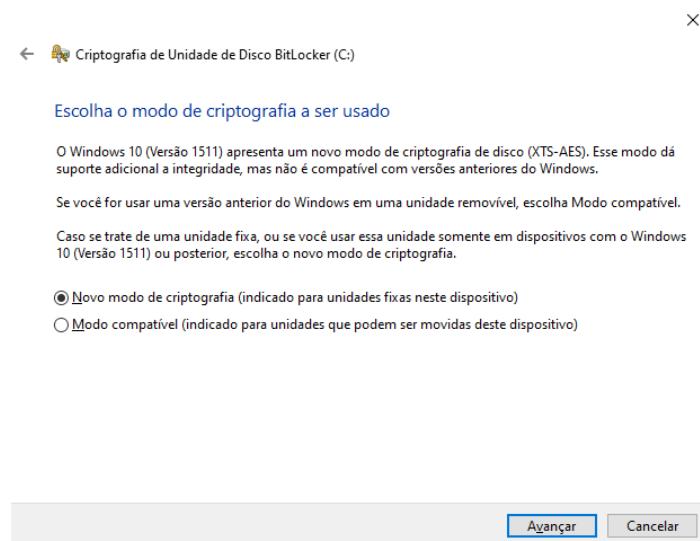
[Avançar](#) [Cancelar](#)

Selecione a opção de baixo: **Criptografar a unidade inteira (mais lento, mas melhor para PCs e unidades já em uso).**

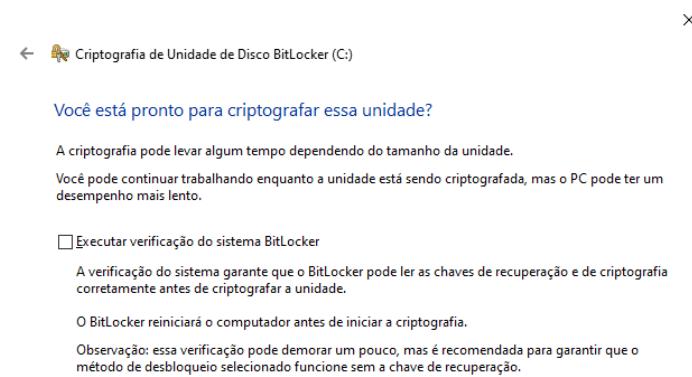


[Avançar](#) [Cancelar](#)

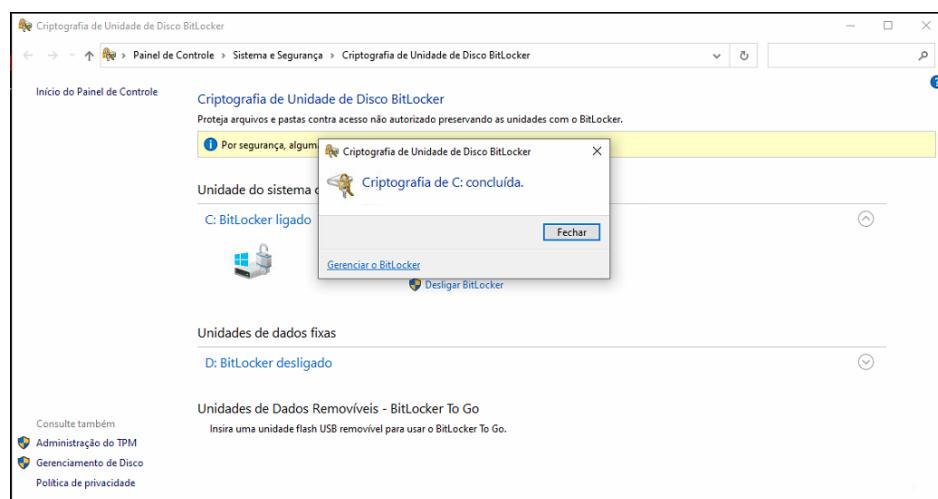
Nesta tela, selecione a primeira opção: **Novo modo de criptografia (indicado para unidades fixas neste dispositivo).**



Clique em Iniciar criptografia.



Criptografia concluída.

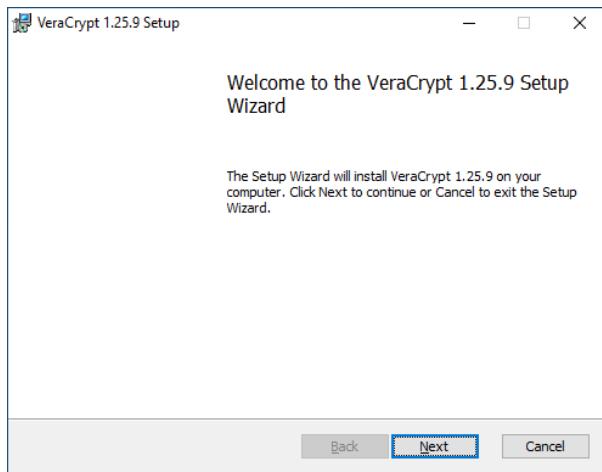


12.2 VeraCrypt

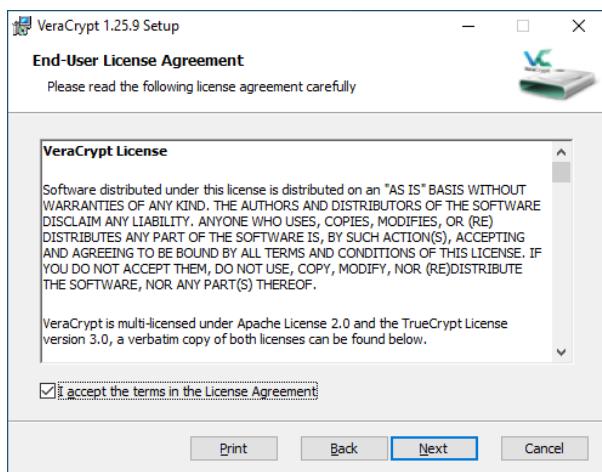
Porém, os requisitos de hardware para permitir o uso do BitLocker podem não ser atendidos dependendo do computador acessado, sendo necessária outra alternativa para a criptografia.

Neste caso, vamos utilizar o VeraCrypt para criptografar.

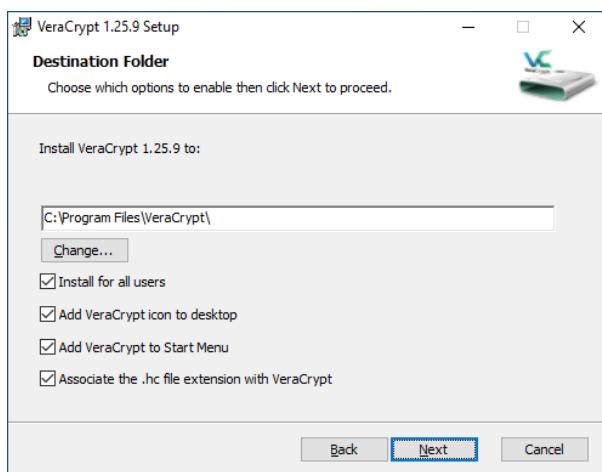
Como Administrador, execute o instalador do VeraCrypt e clique em **Next**.



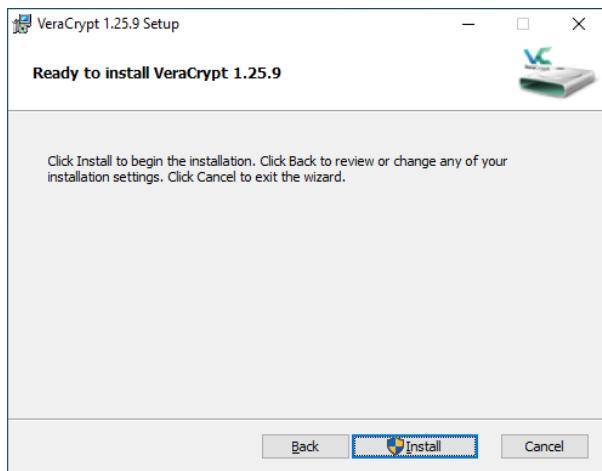
Aceite os termos de uso e clique em **Next**.



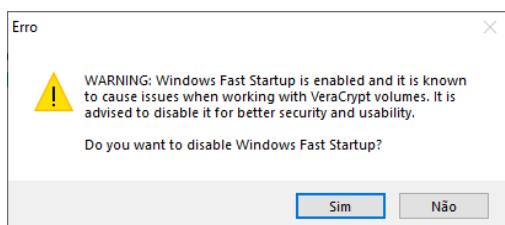
Clique novamente em **Next**.



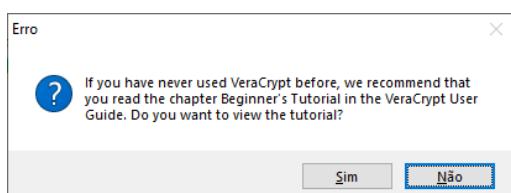
Clique em **Install**.



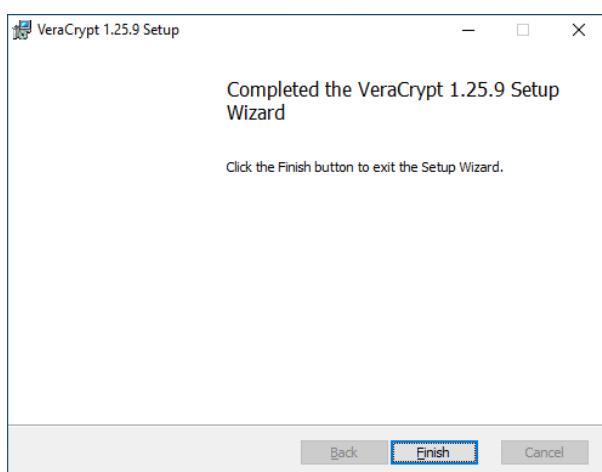
Dependendo do computador, pode ser perguntado se você quer desativar o início rápido do Windows. Clique em **Sim**.



Nesta etapa, clique no **Não** para dispensar a leitura do tutorial.



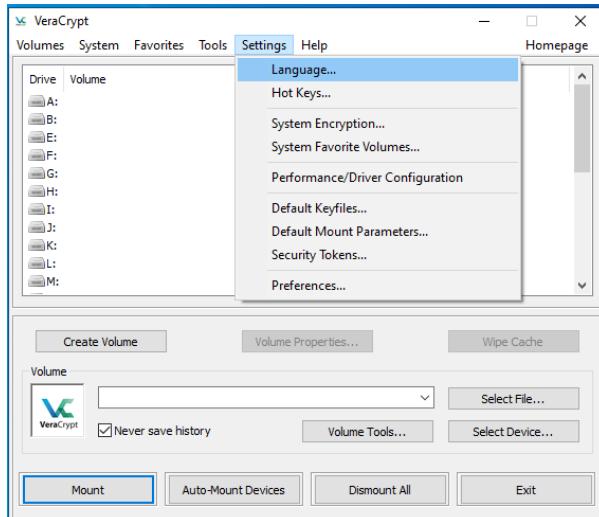
Clique em **Finish** e abra o **VeraCrypt** para iniciar a configuração.



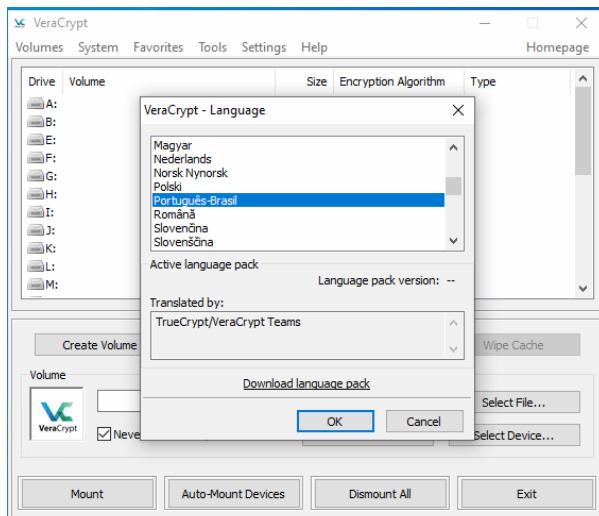
Execute o **VeraCrypt**.



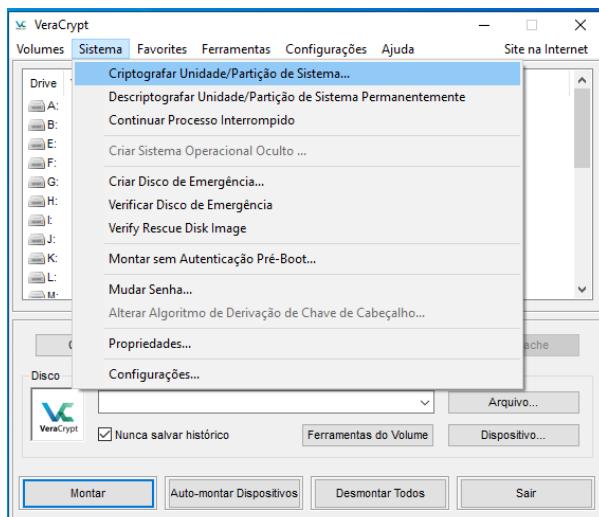
Com o VeraCrypt aberto, clique em **Settings** e após em **Language** para alterar o idioma.



Selecione **Português-Brasil** e clique em **OK**.



Clique em **Sistema** e após em **Criptografar Unidade/Partição de Sistema**.



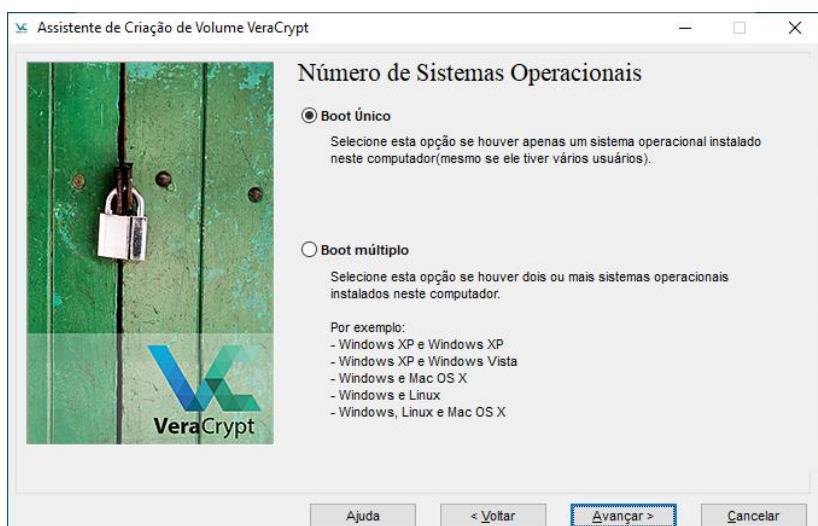
Clique em **Avançar**.



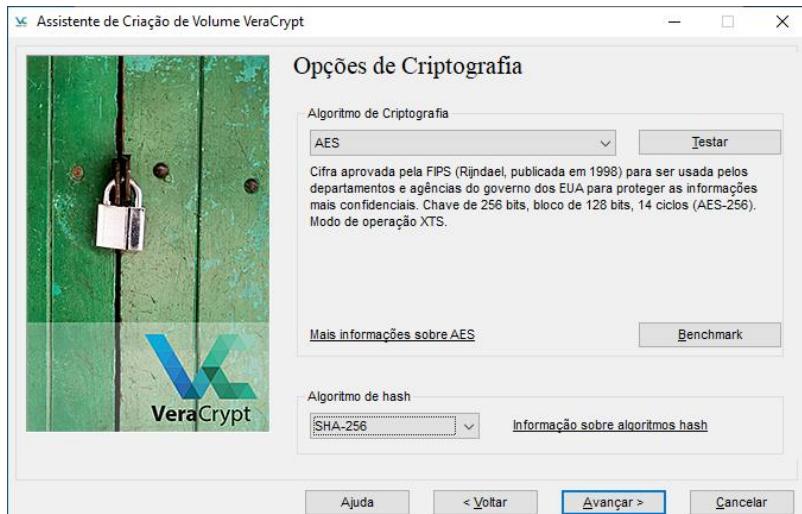
Com a opção **Criptografar a partição de sistema do Windows** selecionada, clique em **Avançar**.



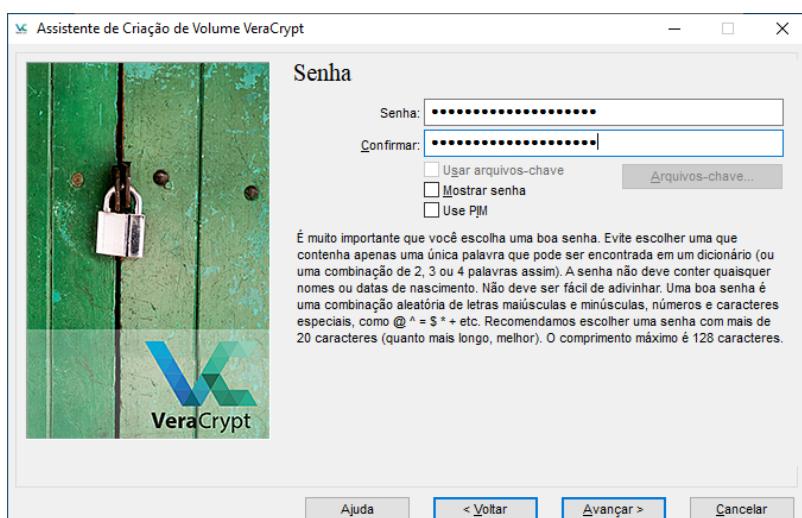
Selecione a opção **Boot Único** e clique em **Avançar**.



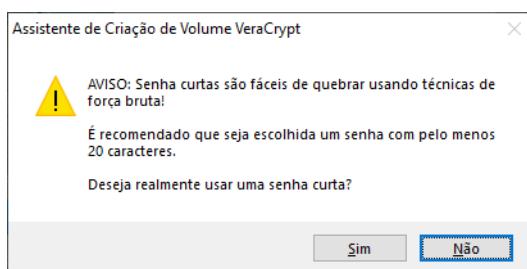
Altere o algoritmo de hash para **SHA-256** e clique em **Avançar**.



Com a opção Use PIM desmarcada, digite e repita a senha de criptografia padrão do VeraCrypt disponível no [SysPass](#) e clique em **Avançar**.



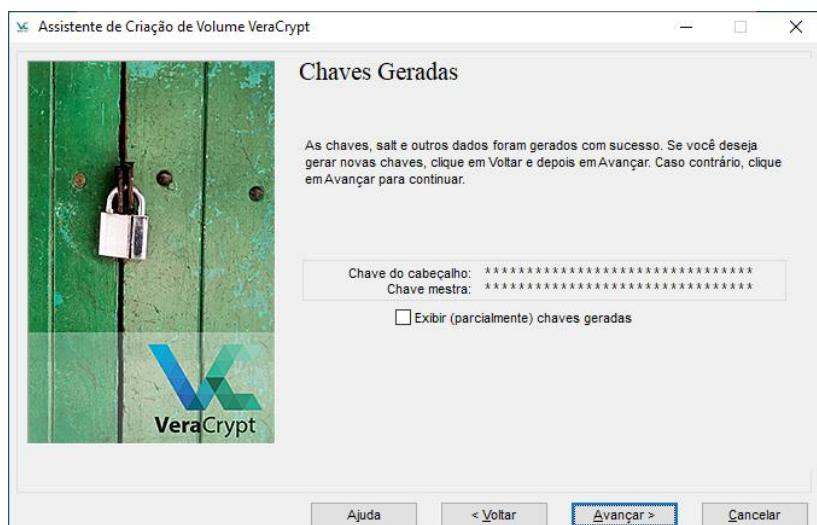
Pode ser exibida a mensagem informando que a senha é fraca. Confirme clicando em **Sim**.



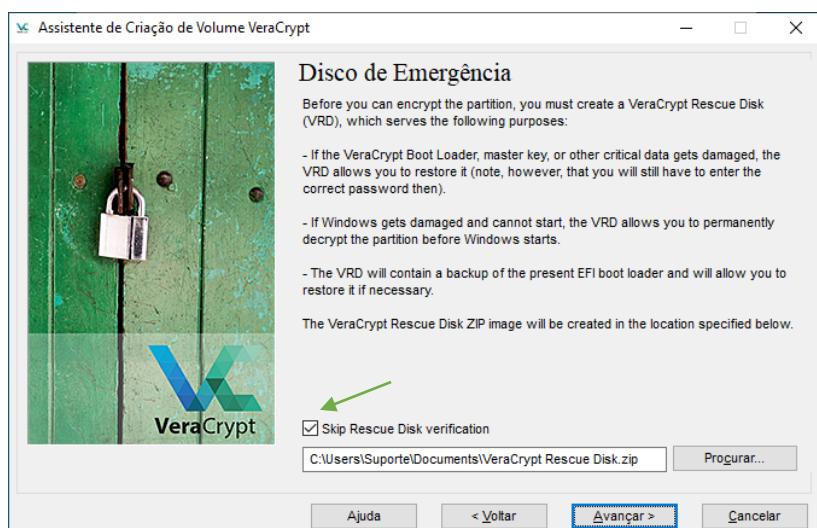
Mova o cursor do mouse em sentidos aleatórios para gerar o par de chaves da criptografia e clique em **Avançar**.



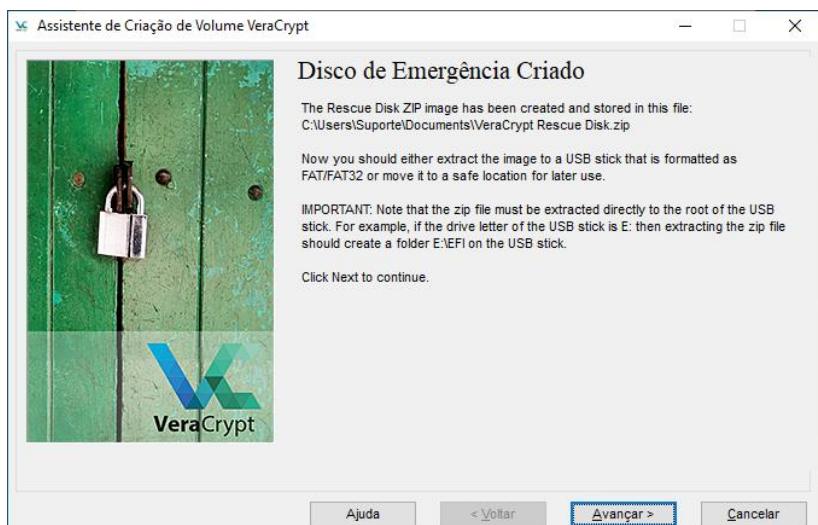
Com o par de chaves gerada, clique em **Avançar**.



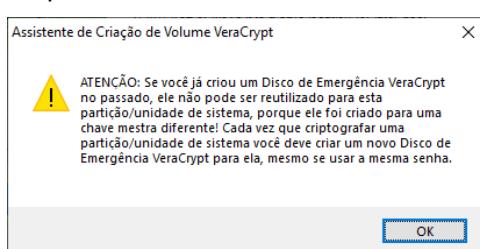
Marque a opção **Skip Rescue Disk Verification** e clique em **Avançar**.



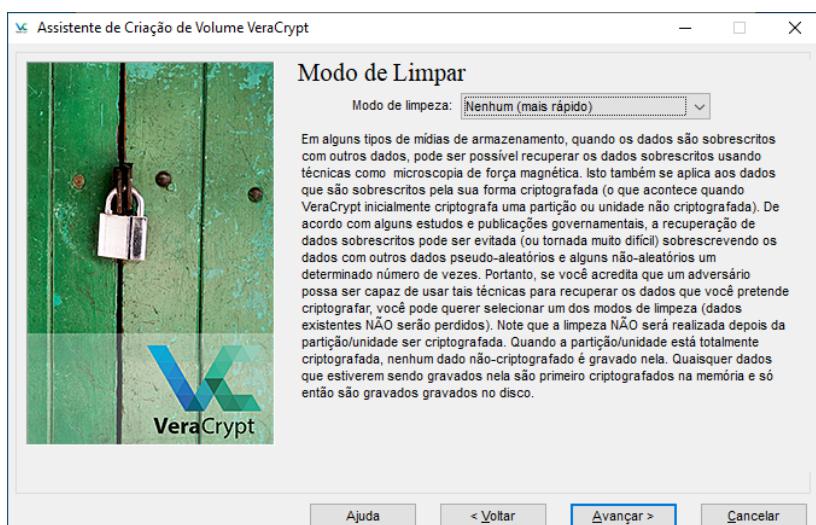
O disco de recuperação será gerado na pasta **Documentos**. Copie e adicione o arquivo no cadastro da senha da máquina no **SysPass**. Clique em **Avançar**.



Clique em **OK**.



Com o modo **Nenhum (mais rápido)** selecionado, clique em **Avançar**.



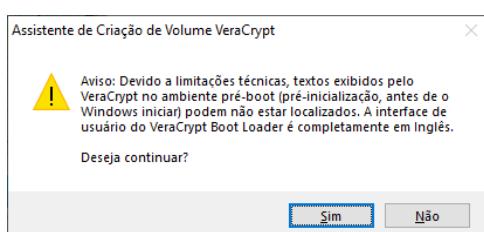
Dependendo da versão do Windows, pode ser exibida a mensagem solicitando a desativação do início rápido do Windows. Clique em **Sim**.



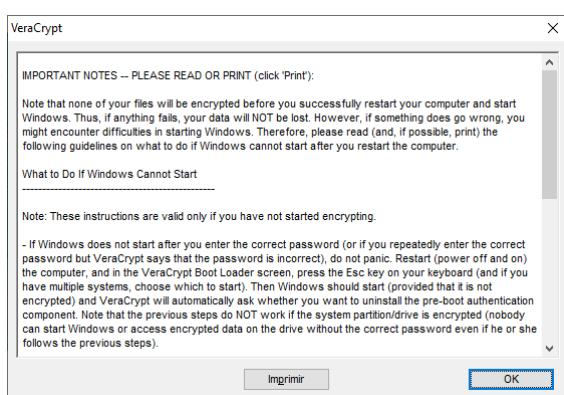
Será solicitado o Pré-Teste para avaliar se o equipamento permite a criptografia do sistema. Clique em **Testar** para dar seguimento.



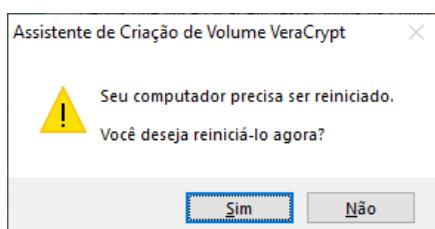
Clique em **Sim** para continuar.



Clique em **OK**.

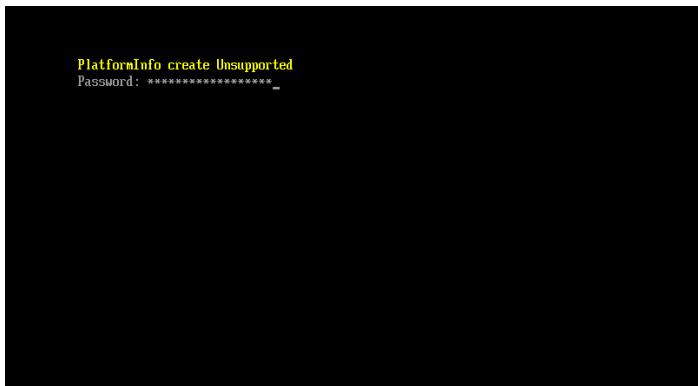


Clique em **Sim** para iniciar o teste.



Nesta etapa, vamos depender do **AGR** para a continuidade do teste, pois o computador será reiniciado e exigirá a senha pela primeira vez no durante o **boot**, sendo necessário que o **AGR digite a senha e deixe o PIM em branco** para concluir o teste e que o Windows inicialize.

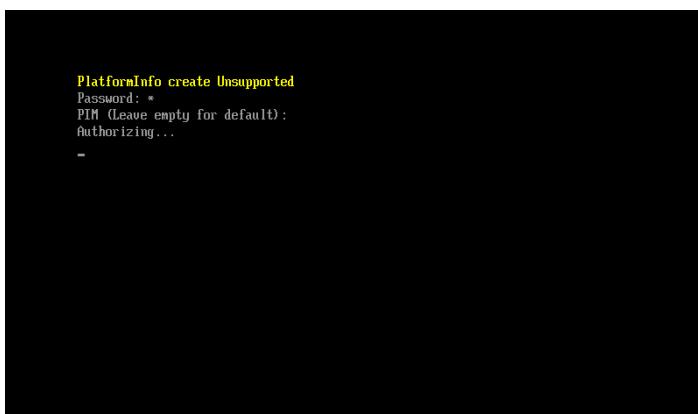




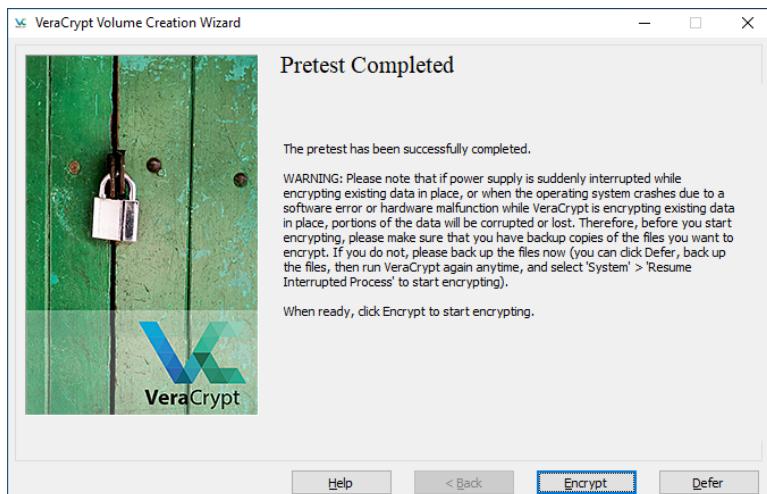
Portanto, **solicite ao AGR e solicite que digite a senha, deixe o PIM em branco e pressione ENTER.**



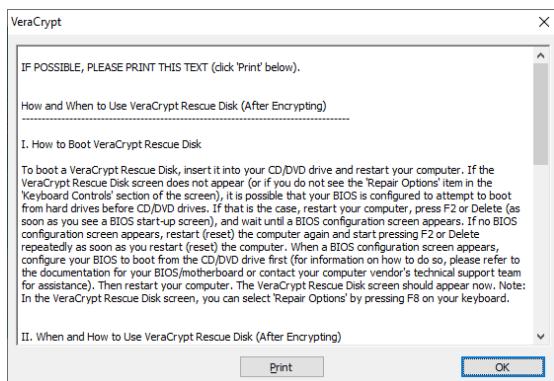
O VeraCrypt irá validar os testes e iniciar o Windows.



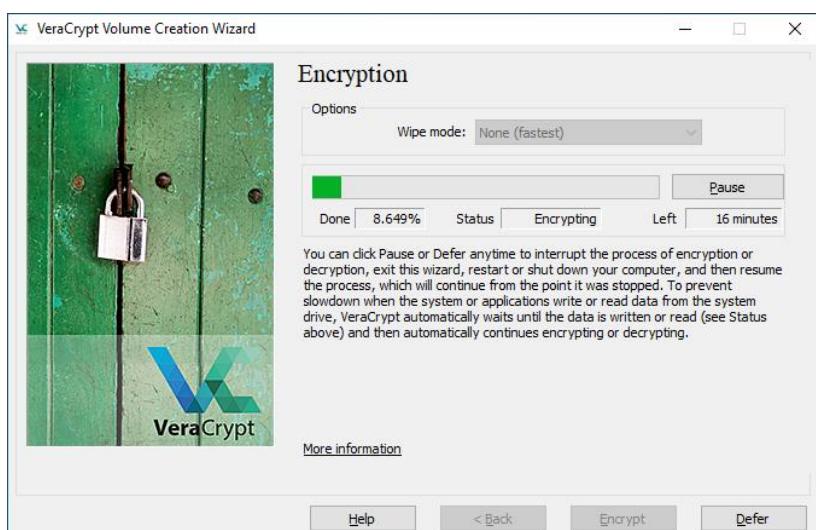
Ao iniciar, o VeraCrypt irá abrir confirmando que o teste foi executado com sucesso e permitindo o início da criptografia. Clique em **Encrypt** para iniciar.



Confirme em **OK**.



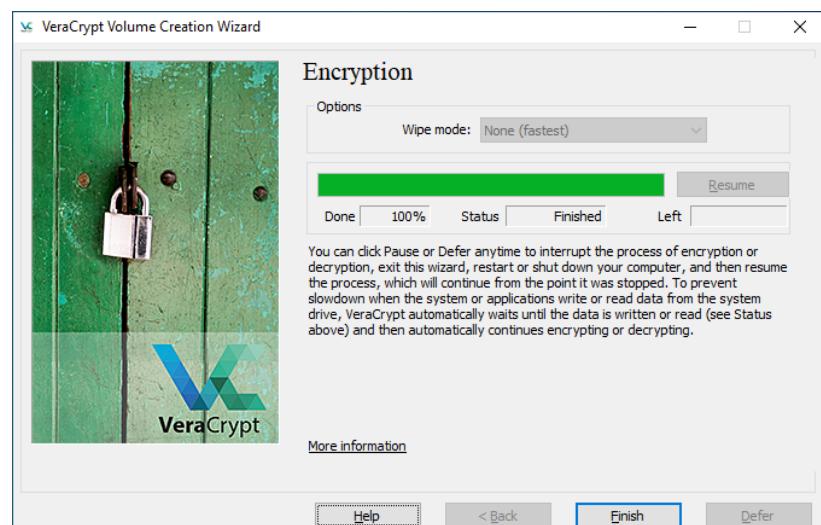
Será iniciado o processo de criptografia. Este procedimento é demorado e depende da capacidade do hardware, podendo levar de vários minutos a algumas horas.



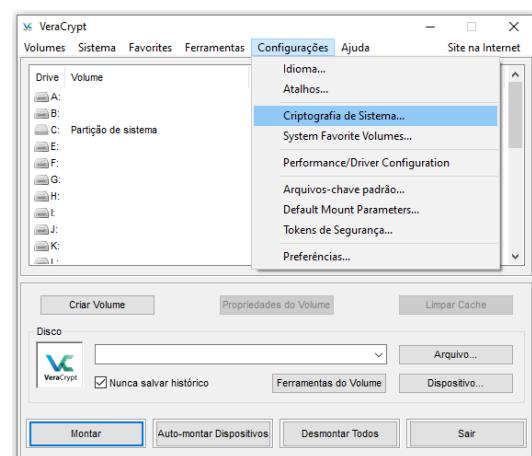
Após o término da criptografia, clique em **OK**.



Clique em **Finish** para concluir a configuração.

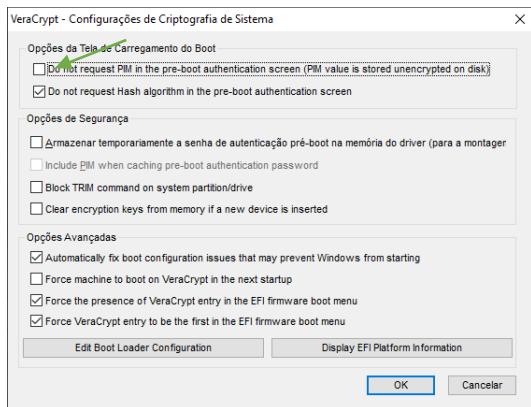


Por fim, abra o VeraCrypt e clique em **Configurações > Criptografia de Sistema**

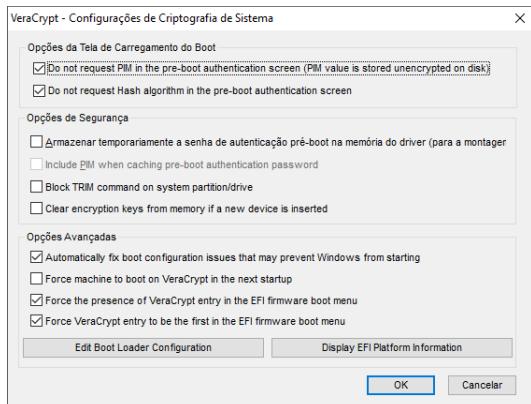
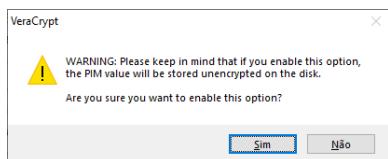


CONTEÚDO INTERNO

Marque a opção **Do not request PIM in the pre-boot authentication screen (PIM value is stored unencrypted on disk)**.



Clique em **Sim** para confirmar.



Clique em **OK** e a criptografia estará encerrada.

13 Padrão de Nomenclatura

13.1 Hostnames

Para definir o nome de um computador, utilizaremos o seguinte padrão:

SIGLA DA LOJA – NÚMERO DA UAE - NÚMERO DO COMPUTADOR LOCAL

O “número do computador local” se refere a quantos computadores existem na loja, para que não haja conflito na rede. **Confirme os outros hostnames da loja antes de definir o número pra evitar este conflito!**

Exemplo:

Uma loja da Contadores Digital, cuja UAE é a 0039 e existem 2 computadores, o hostname seria:

CDI-UAE0039-02

Abaixo a tabela com as siglas de cada loja.

LOJA	SIGLA
AR 3D Serviços Digitais	3DS
AC Digital	DIG
AR Ágil	AGI
AR Ativo	ATI
AR Bah	BAH
AR Certifica	CER
AR Certpar	PAR
AR Contadores	CON
AR Gol	GOL
AR i9 Digital	I9D
AR Líder Digital	LID
AR Macapá	MAC
AR Mineira	MIN
AR Poa	POA
AR Wclick	WCL
AR Ascel	ASC
Certiflex	FLE
Certiron	RON
Contadores Digital	CDI
Safe Digital	SAF
Smart CD	SCD
TecSegCert	TEC

Sendo uma loja própria, desconsiderar a tabela acima, pois neste caso é utilizado o [padrão interno da TI](#).

13.2 Grupos de Trabalho

Seguir o padrão conforme a tabela:

LOJA	Grupo de Trabalho
AR 3D Serviços Digitais	AR3D
AC Digital	ACDIGITAL
AR Ágil	ARAGIL
AR Ativo	ARATIVO
AR Bah	ARBAH
AR Certifica	ARCERTIFICA
AR Certpar	ARCERTPAR
AR Contadores	ARCONTADORES
AR Gol	ARGOL
AR i9 Digital	ARI9
AR Líder Digital	ARLIDER
AR Macapá	ARMACAPA
AR Mineira	ARMINERA
AR Poa	ARPOA
AR Wclick	ARWCLICK
AR Ascel	ARASCEL
Certiflex	CERTIFLEX
Certiron	CERTIRON
Contadores Digital	CDIGITAL
Safe Digital	SAFEDIGITAL
Smart CD	SMARTCD
TecSegCert	TECSEG

14 Comandos recorrentes

14.1 Prompt de comandos

wmic path softwareLicensingService get OA3xOriginalProductKey

Exibe a chave de ativação do Windows.

wmic bios get serialnumber

Exibe o serial do computador.

hostname

Exibe o nome do computador.

ipconfig /all

Exibe todas as informações dos dispositivos de rede.

getmac

Exibe o endereço físico do dispositivo de rede conectado no momento.

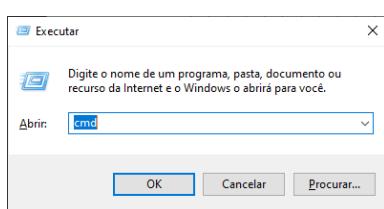
s1mgr /xpr

Exibe o status de ativação do Windows.

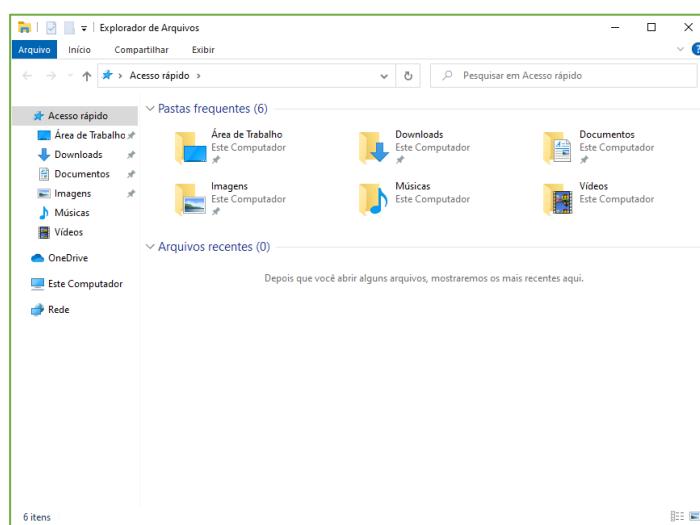
14.2 Teclas de Atalho

WINKEY – Abre o Menu Iniciar.

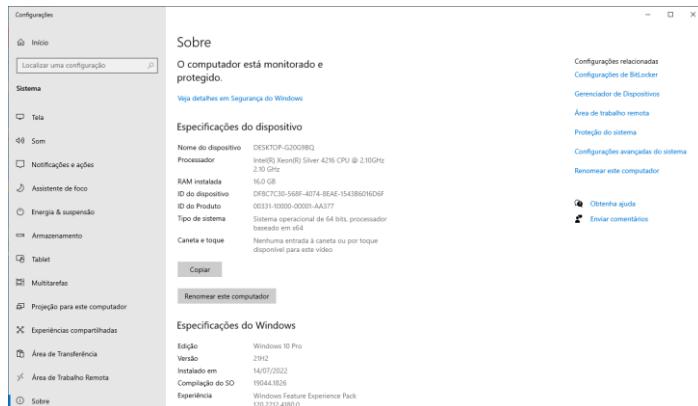
WINKEY + R – Abre o Executar.



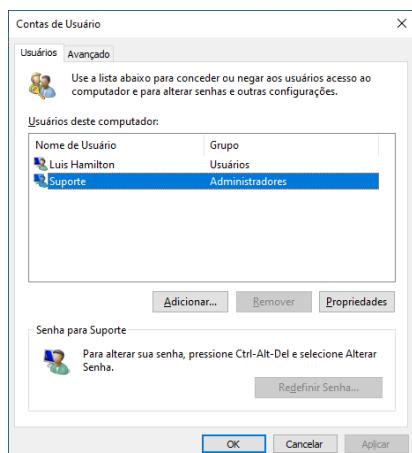
WINKEY + E – Abre o Windows Explorer.



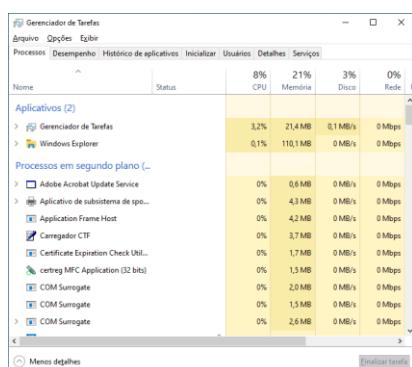
WINKEY + PAUSE – Abre as Configurações do Sistema.



NETPLWIZ – Abre o painel de controle de Contas do Usuário.



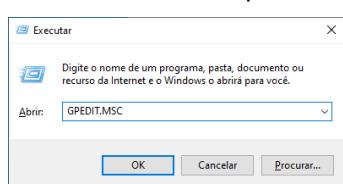
CTRL + SHIFT + ESC – Abre o gerenciador de tarefas.



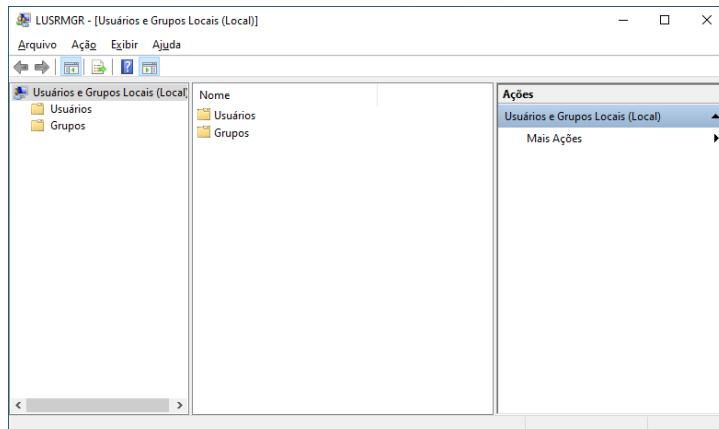
CTRL + ALT + DEL – Abre a tela de login .

14.3 Consoles

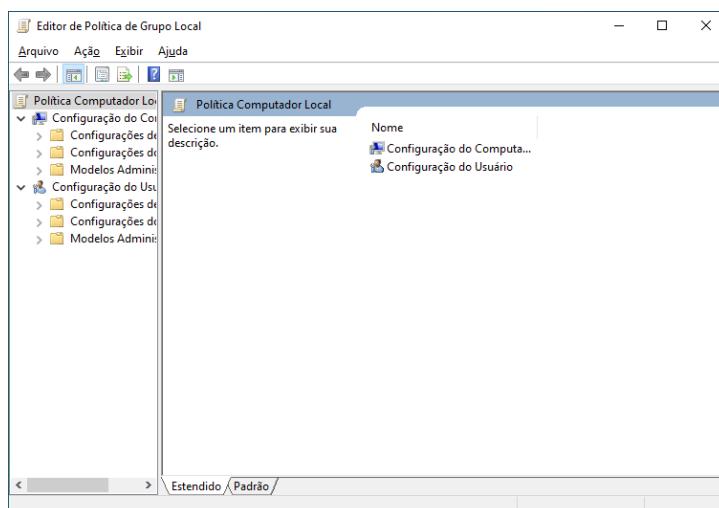
Nome de sistemas que ao Executar, abrem consoles de configuração avançada.



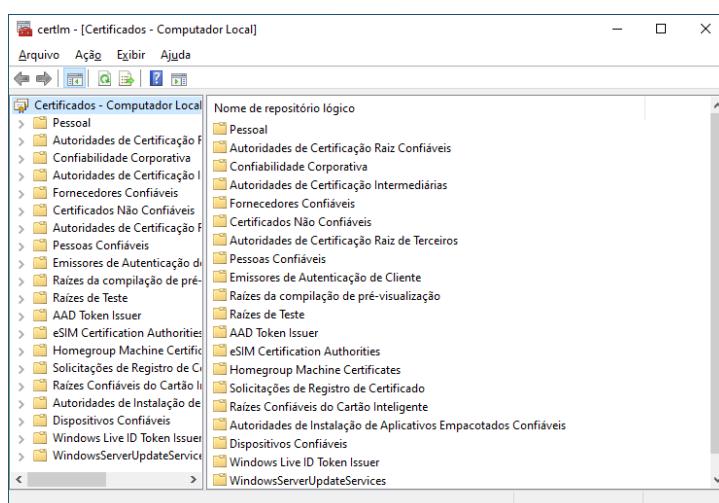
LUSRMGR.MSC - Gerenciamento Avançado de Usuários



GPEDIT.MSC - Editor de Política de Grupo

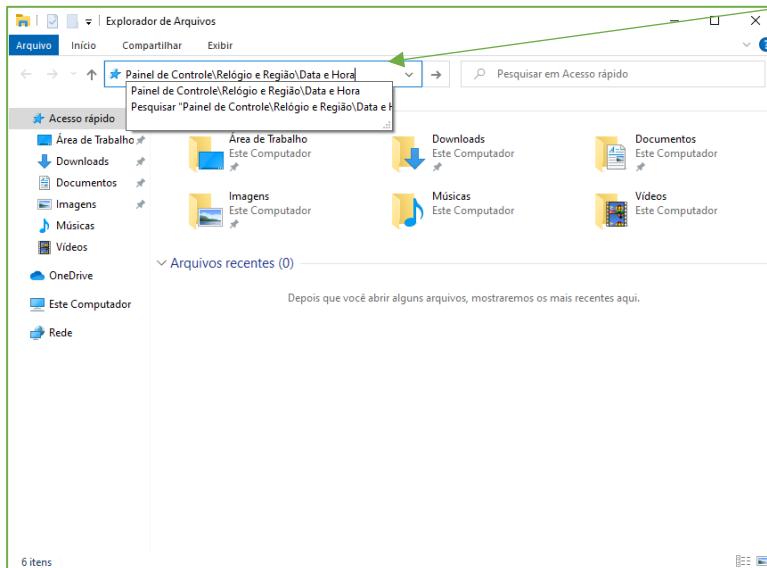


CERTLM.MSC - Certificados do Computador

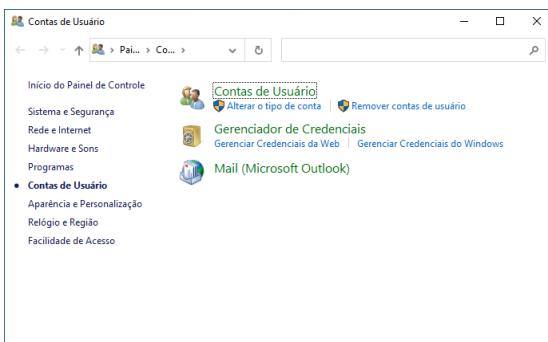


14.4 Endereços comuns no Windows Explorer

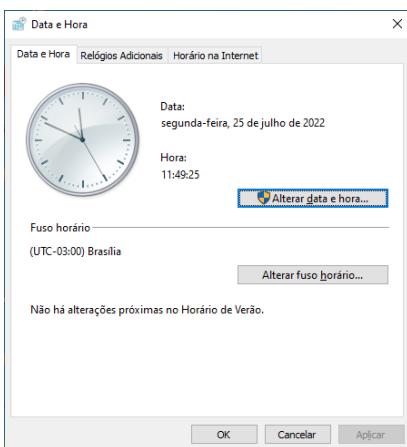
Endereço de painéis de configuração que são acessados ao serem executados na **barra de endereços** do Windows Explorer, conforme imagem:



Painel de Controle\Contas de Usuário



Painel de Controle\Relógio e Região\Data e Hora



15 Links

Endereços de páginas e sistemas comuns durante a configuração.

<https://acfaz.acdigital.com.br> - Página do AC Faz.

a.st1.ntp.br – Link da sincronia de tempo de data e hora do Windows.

ntp.acsoluti.com.br - Link da sincronia de tempo de data e hora do Windows para Soluti.

<https://ocs-sp.ca.inf.br/ocsinventory> - Endereço de configuração do OCS.

<https://syspass.idm.acertweb.com.br/> - SysPass

<https://login.teamviewer.com/> - TeamViewer

<https://my.norton.com/extspa/passwordmanager> - Gerador de Senhas do Norton

%SYSTEMROOT%\Web\Wallpaper\AC Digital\ - Diretório local do papel de parede AC Digital

15.1 Diretórios no SharePoint

Diretórios com conteúdo necessário para realizar as configurações descritas neste guia.

[Configuração para AGR](#)

[Softwares](#)

[Drivers](#)

[Gerenciadores de Certificados](#)

[Complementos](#)

[BG Info](#)

[Cadeias de Certificados](#)

[Manuais](#)

16 Glossário

AR – Agência de Registro, uma loja onde há um AGR e emite certificados

AGR – Agente de Registro, o funcionário que opera o computador e emite os certificados

AC – Autoridade Certificadora

Hostname – nome do computador

Workgroup – grupo de trabalho, descrito junto ao hostname, organiza computadores em uma rede

Administrador – conta de usuário do computador que permite instalar e alterar configurações do sistema operacional.

Sistema operacional – sistema principal do computador onde são instalados e rodados todas as demais aplicações, programas, bem como armazenamento.

Windows Explorer – Navegador do sistema operacional Windows, permite navegar pelos diretórios do Windows

TeamViewer – aplicativo de acesso remoto, permite acessar remotamente a tela de um computador e interagir nele.

SysPass – sistema de armazenamento de senhas utilizado pela AC Digital.

Backup – procedimento de guardar arquivos importantes de um usuário para evitar perdê-los

SharePoint – diretório de armazenamento na internet

Driver – programa que gerencia e permite o funcionamento adequado de um dispositivo de hardware

Hardware – parte física de um computador

Bat – Batche, um executável com uma lista de comandos integrado que junto com os arquivos necessários na mesma pasta, pode executar e instalar um ou vários programas e configurações

Wiki – Página colaborativa contendo informações úteis, em que qualquer membro pode editar

17 Histórico da Revisão

Descrição	Autor
Criação do documento	
Revisão técnica	