MANUAL DA MENSAGERIA
HUMANUS x eSocial Release V

Sumário

- *Comunicação e-Social (Mensageria)* 2
- *Funções necessária do Internet Information Services* 2
- *Instalação do WebService*..... 4
- *Pasta para geração dos arquivos XML'S* 6
- *Configuração de Internet Information Services (IIS)*..... 7
- *Consultar a versão da Mensageria* 9
- *Teste de Comunicação Mensageria x Banco de Dados* 10
- *Instalação Certificado digital no Servidor Web Service:*..... 12
- *Instalação do certificado Digital nas estações de trabalho (se houver)*..... 24
- *Windows Resource Kits:*..... 36
- *Instalação do HWinService:* 42

Comunicação e-Social (Mensageria)

Premissas:

- Sistema operacional compatível:

- Windows Server 2008 R2 (x86 e x64)
- Windows Server 2012 (x86 e x64)
- Windows Server 2012 R2 (x86 e x64)
- Windows Server 2016 (x86 e x64)

Versão IIS:

- IIS 7.0 / IIS 7.5

Versão .NET Framework:

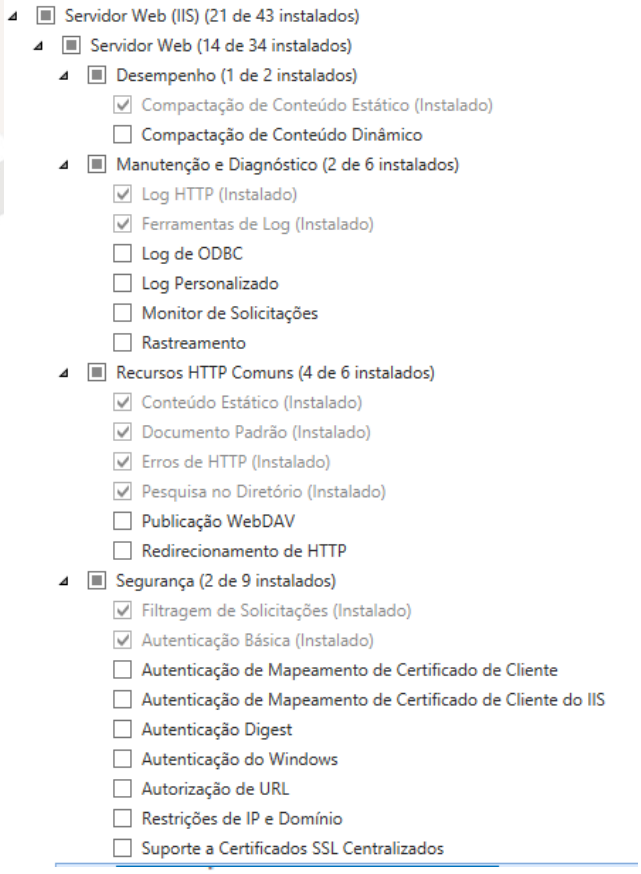
- .NET Framework 2.0, 3.0 e 4.5

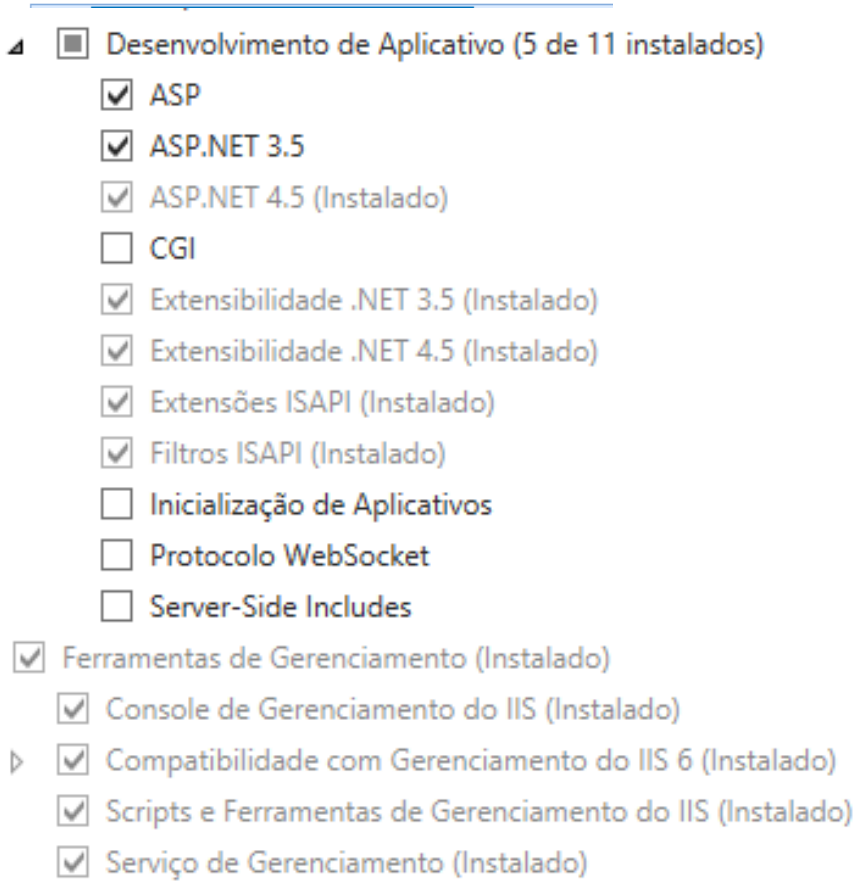
Certificado para Assinatura XML:

- Possuir o certificado digital A1 de empresa

Funções necessária do Internet Information Services

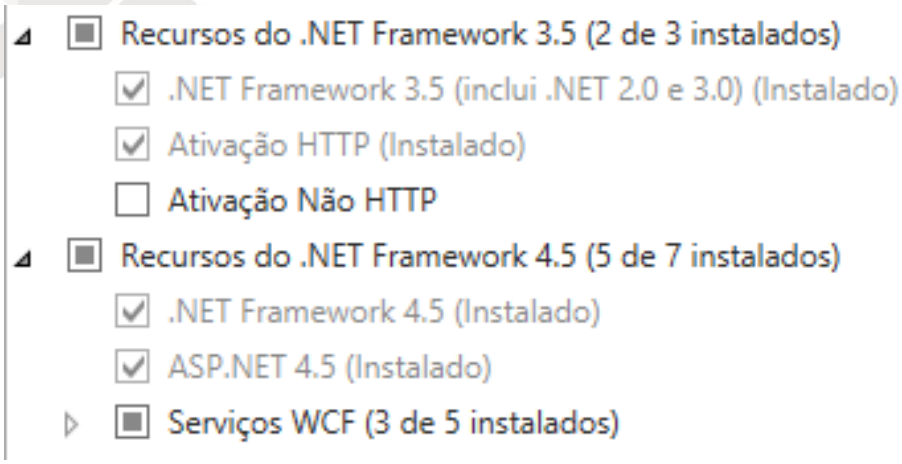
- Para que as funções do Webservice funcionem corretamente, abaixo a lista de funções necessárias que precisam estar habilitadas no servidor.





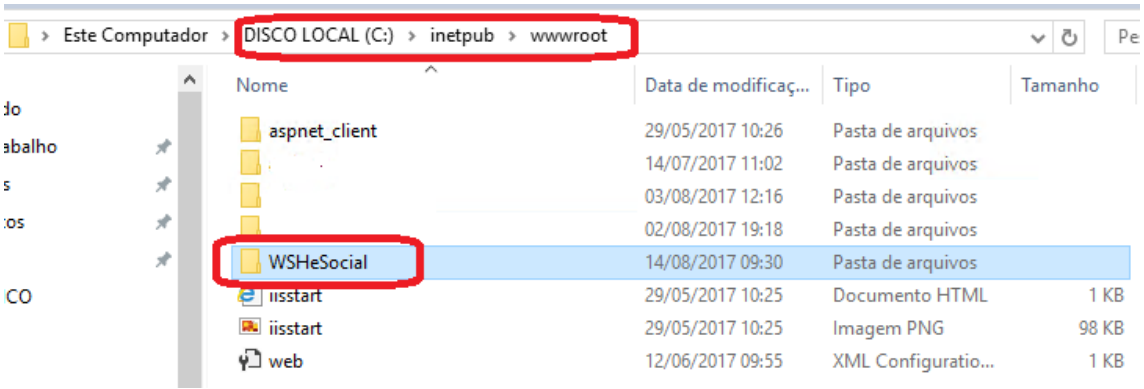
SISTEMA **HUMANUS**
PARA GESTÃO DE PESSOAS

Humanus

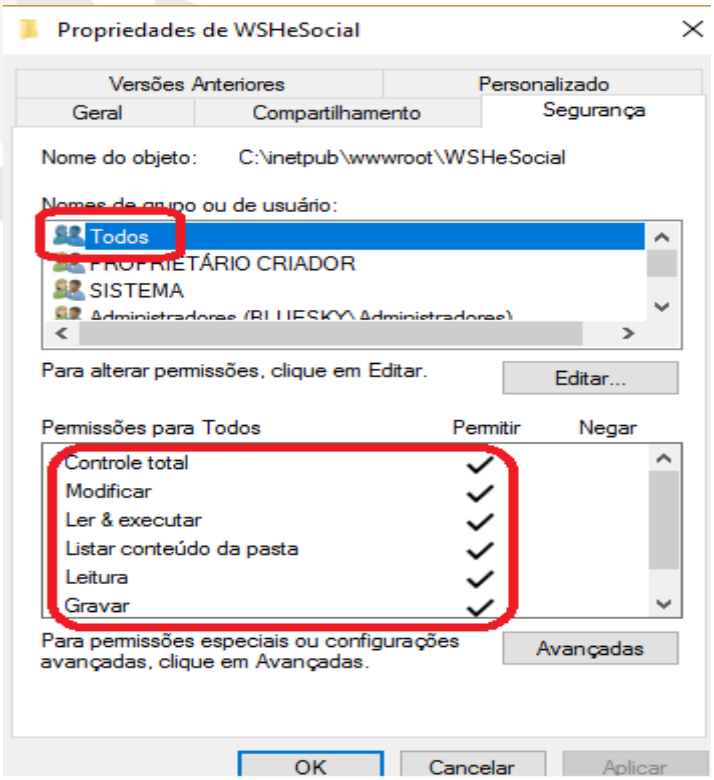


Instalação do WebService

- Descompacte o conteúdo da pasta WSHESOCIAL no diretório wwwroot das aplicações no Internet Information Services do seu servidor.



- Adicione permissões de leitura e gravação na pasta, processo muito importante para o correto funcionamento do WebService, no exemplo adicionamos leitura e gravação para todos.



- Abra o arquivo de configuração "Web_template.config" e informe sua forma de conexão na tag "connectionStrings".

Exemplo de conexão em SQL Server:

<add name="DbConnectionODBC" connectionString="DSN=FONTE_ODBC;User ID=USUARIO;Password=SENHA;" providerName="**System.Data.SqlClient**" />

* Onde:

DSN - Criar uma fonte de dados ODBC 32bits (DSN de sistema) com conexão ao banco de dados do Humanus;

UserID - Informar o usuário de acesso ao banco;

Password - Informar a senha de acesso ao banco;

```
<connectionStrings>
  <!-- <add name="DbConnection_SQL" connectionString="Data Source=localhost;Initial Catalog=SQL_eSocial;User ID=;Password=;" providerName="System.Data.SqlClient"/>-->
  <!--<add name="DbConnectionODBC" connectionString="DSN=SQL_eSocial;User ID=web;Password=123456;" providerName="System.Data.SqlClient"/>-->
  <add name="DbConnectionODBC" connectionString="DSN=ORA_REMOTO;User ID=humanus;Password=123456;" providerName="System.Data.SqlClient" />
  <!--<add name="DbConnectionODBC" connectionString="DSN=ORA_LOCAl;User ID=sertarh;Password=123456;" providerName="Oracle.DataAccess.Client"/>-->
  <!--<add name="DbConnectionODBC" connectionString="DSN=ACCHUMANUS77;User ID=;Password=;" providerName="Oracle.DataAccess.Client"/>-->
</connectionStrings>
```

Exemplo de conexão em bases ORACLE:

<add name="DbConnectionODBC" connectionString="DSN=FONTE_ODBC;User ID=USUARIO;Password=SENHA;" providerName=" **Oracle.DataAccess.Client**" />

Exemplo utilizando uma conexão ORACLE.

```
<connectionStrings>
  <!-- <add name="DbConnection_SQL" connectionString="Data Source=localhost;Initial Catalog=SQL_eSocial;User ID=;Password=;" providerName="System.Data.SqlClient"/>-->
  <!--<add name="DbConnectionODBC" connectionString="DSN=SQL_eSocial;User ID=web;Password=123456;" providerName="System.Data.SqlClient"/>-->
  <add name="DbConnectionODBC" connectionString="DSN=ORA_REMOTO;User ID=humanus;Password=123456;" providerName="Oracle.DataAccess.Client" />
  <!--<add name="DbConnectionODBC" connectionString="DSN=ORA_LOCAl;User ID=sertarh;Password=123456;" providerName="Oracle.DataAccess.Client"/>-->
  <!--<add name="DbConnectionODBC" connectionString="DSN=ACCHUMANUS77;User ID=;Password=;" providerName="Oracle.DataAccess.Client"/>-->
</connectionStrings>
```

Atenção:

1. A sua conexão deve ser a única fora do comentário Html " **<! --** ..... **-->** "

2. Após as configurações de conexão, renomear o arquivo **Web_template.config** para **web.config**

*Observação Banco de dados ORACLE

Para clientes que utilizam banco de dados Oracle é necessário adicionar permissões à 2 views internas ao *User ID* configurado no arquivo ***web.config***.

Para isto, deve-se conectar com o usuário *System do Oracle* e adicionar as Grants abaixo:

```
GRANT SELECT ON V$SESSION TO "seu usuário";
GRANT SELECT ON V$PROCESS TO "seu usuário";
```
→ **remover aspas**
→ **remover aspas**

Pasta para geração dos arquivos XML'S

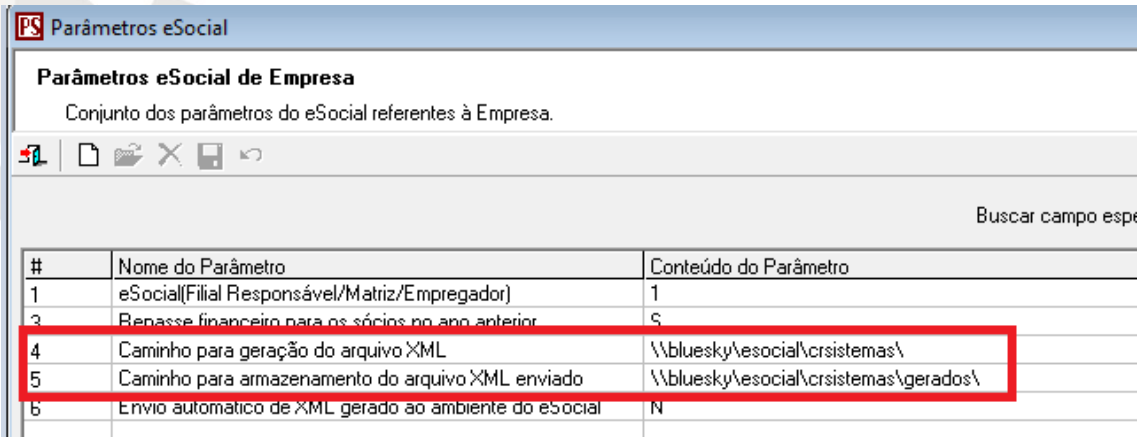
Criar uma pasta LOCAL (compartilhada) para geração dos arquivos, a mesma precisa de permissões "*Full Control*" respeitando a seguinte estrutura.

- eSocial
  - NomeDaEmpresa
    - Gerados

C:\eSocial\NomeDaEmpresa\Gerados

No Humanus, cadastrar o caminho das pastas, utilizar os seguintes parâmetros.

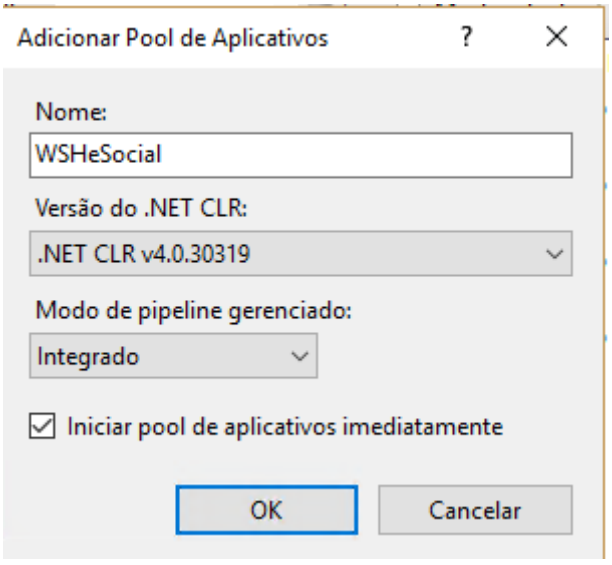
- Modulo Processos legais
  - Cadastros
    - Parâmetros de Empresa



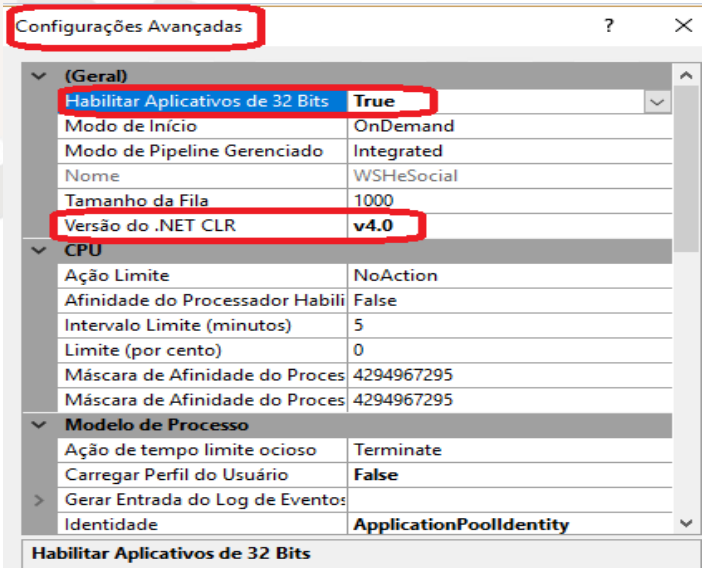
Lembrando que, o diretório do parâmetro 4 e 5, são pastas físicas do próprio servidor do Internet Information Services, são as que foram criadas e compartilhadas na rede anteriormente.

Configuração de Internet Information Services (IIS)

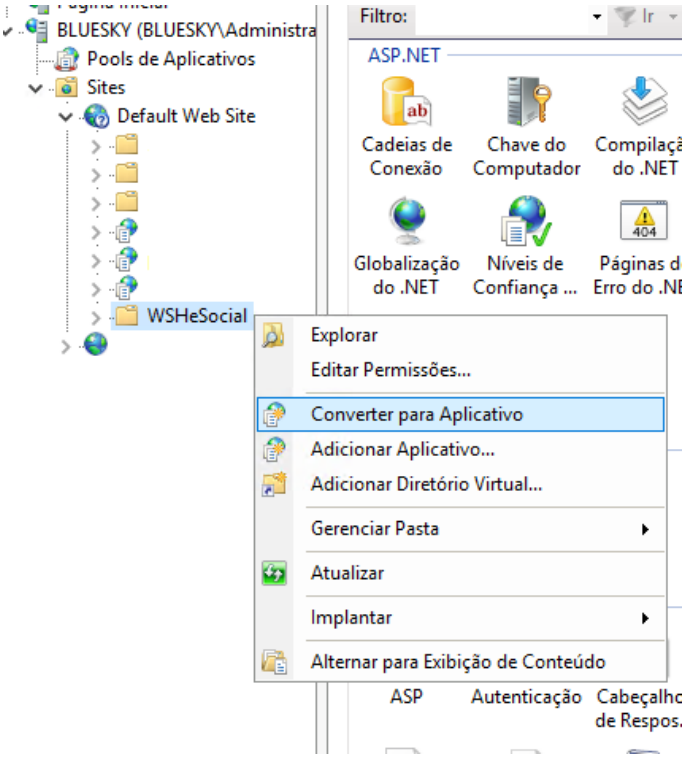
- Criar um pool de aplicação de forma "Integrada", habilitado para 32bits e .NET Framework 4 ou superior.

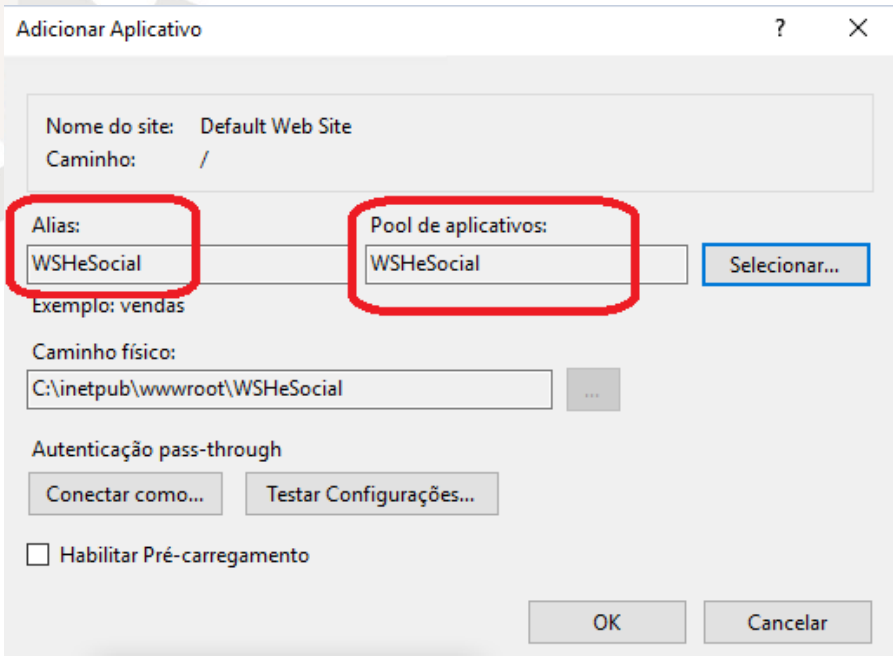


- Nas configurações avançadas do pool de aplicações, certifique-se que o mesmo esteja habilitado para aplicações 32bits, e confirme a utilização do Framework 4.0 ou superior.



- Converta o diretório do WS “**WSHeSocial**” basta clicar com o botão direito do mouse e "Converter em Aplicação" e confirme o caminho físico da aplicação WS.





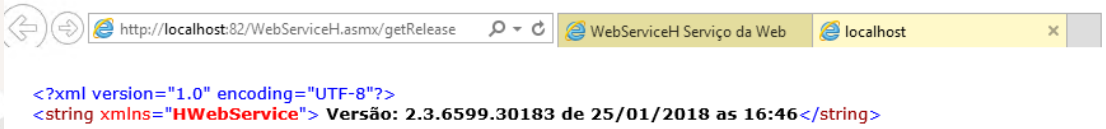
Consultar a versão da Mensageria

- Após os passos acima o Web Service deverá estar ativo e funcionando. Cerifique-se acessando a página diretamente pelo protocolo http do IIS.



Para verificar a versão da Mensageria instalada, basta clicar no último link “getRelease”, após isto você será direcionado a outra página, clicar no botão “Chamar” ou “Invoke”.

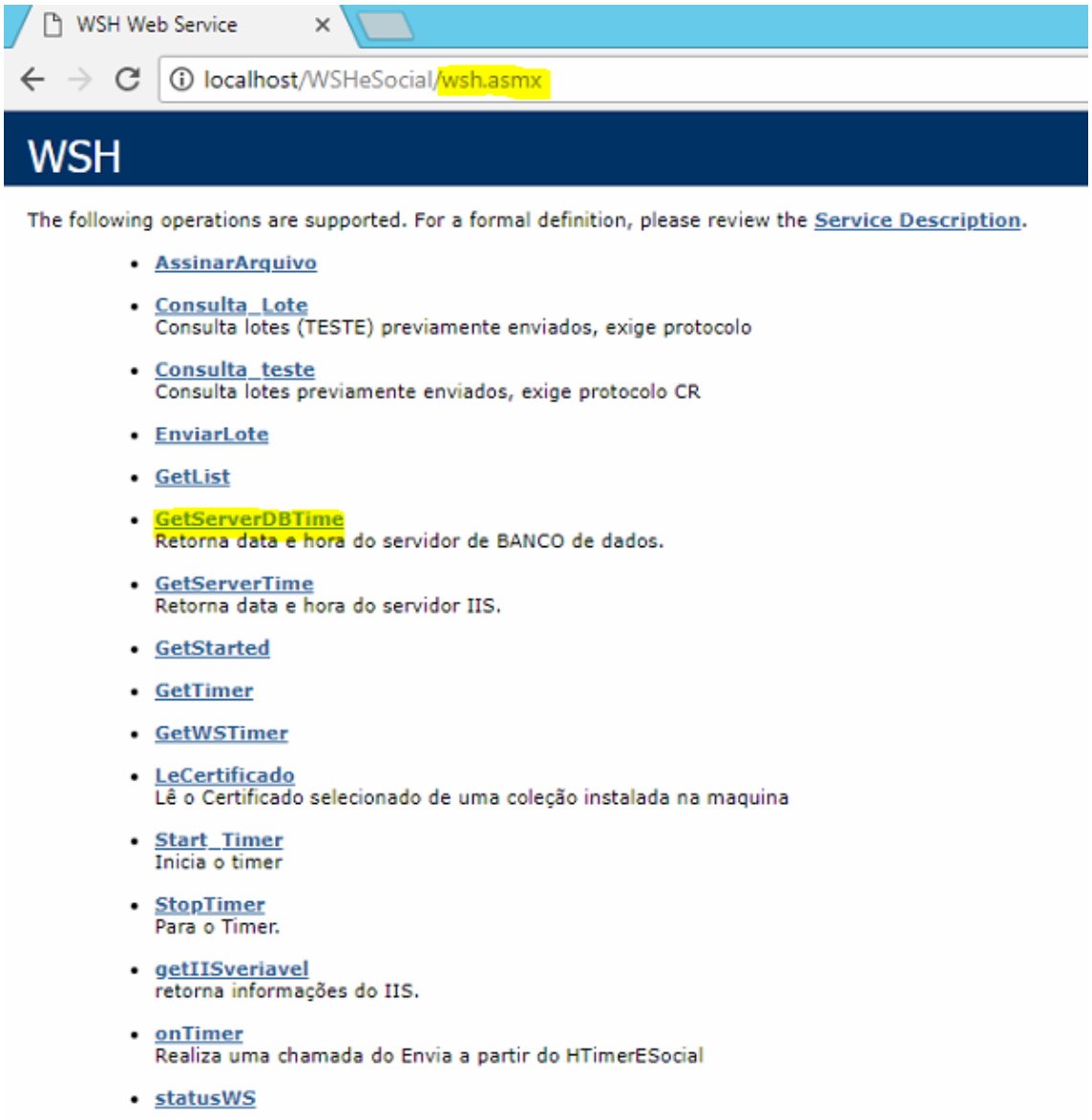
Exemplo:



A versão acima é apenas um exemplo.

Teste de Comunicação Mensageria x Banco de Dados

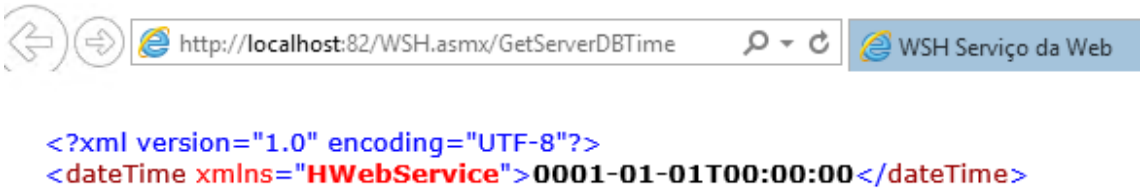
Acessar o diretório conforme a imagem abaixo e clicar no hyper-link "GetServerBDTime", após isto você será direcionado à outra página, clicar no botão "Chamar" ou "Invoke".



Mensagem de Sucesso: Se a conexão com o banco de dados for realizada com sucesso será exibido a data e hora atual:



Mensagem de Falha: Se a conexão com o banco de dados falhar as informações de data e hora será exibida da seguinte maneira:



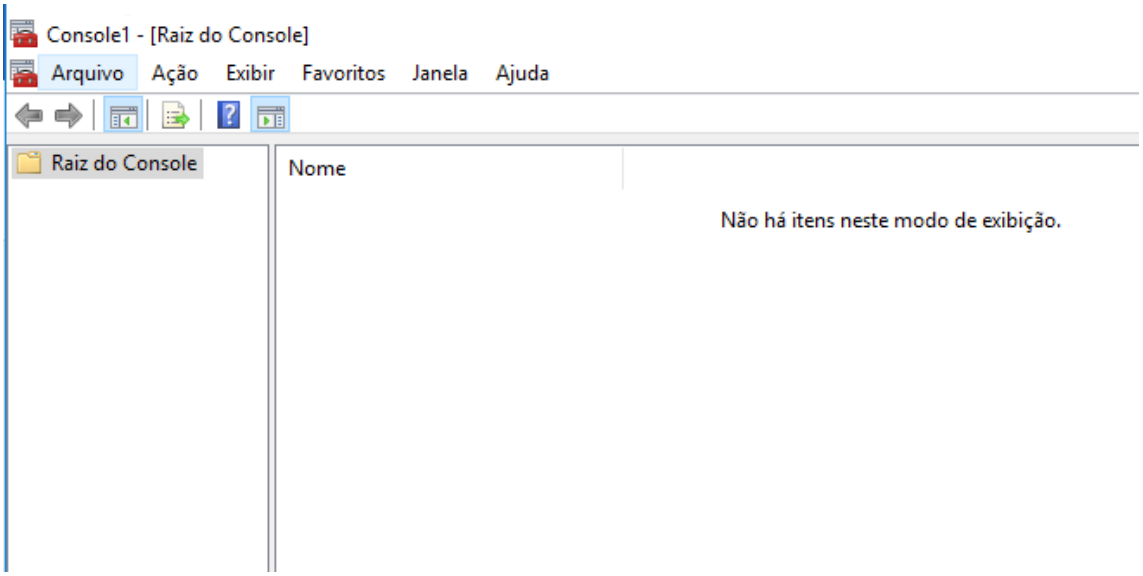
Se **mensagem de falha** for exibida o arquivo ***Web.config*** deve ser analisado novamente. *Verificar as orientações da Página 4 deste manual*, principalmente os dados de conexão com o banco de dados.

Instalação Certificado digital no Servidor Web Service:

- Para que os arquivos XML possam ser enviados pelo WEB SERVICE, se faz necessário a assinatura digital do lote, que utiliza do certificado A1. Obrigatoriamente a empresa precisa do certificado configurado corretamente no servidor e também nas estações de trabalho.

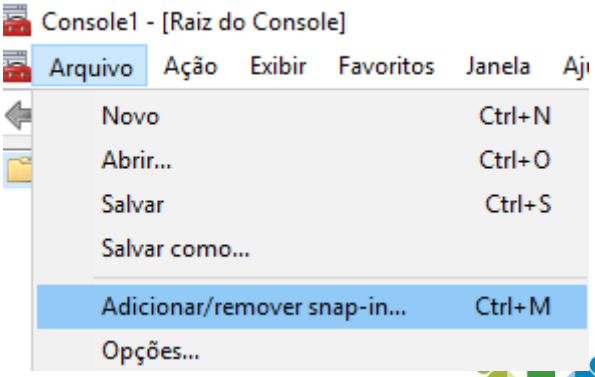
- Execute o console de gerenciamento do servidor.

C:\Windows\System32\ mmc.exe

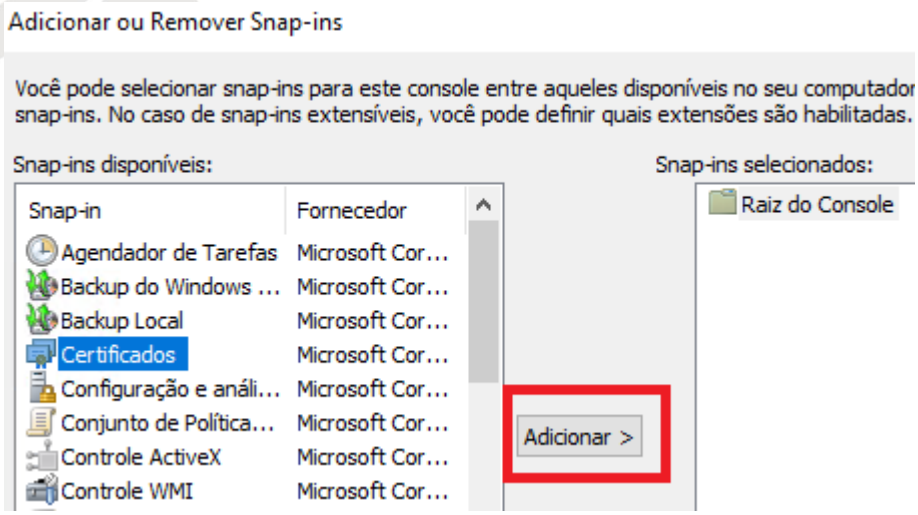


Se faz necessário adicionar a “Snap-ins” de certificado, para isso selecione.

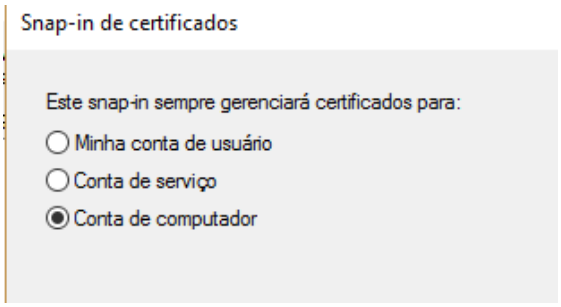
- Arquivo
  - Adicionar/remover Snap-ins



- Selecione “certificados” após clique em adicionar, para que o mesmo seja passível de configuração.



- Selecione a opção “conta do computador”

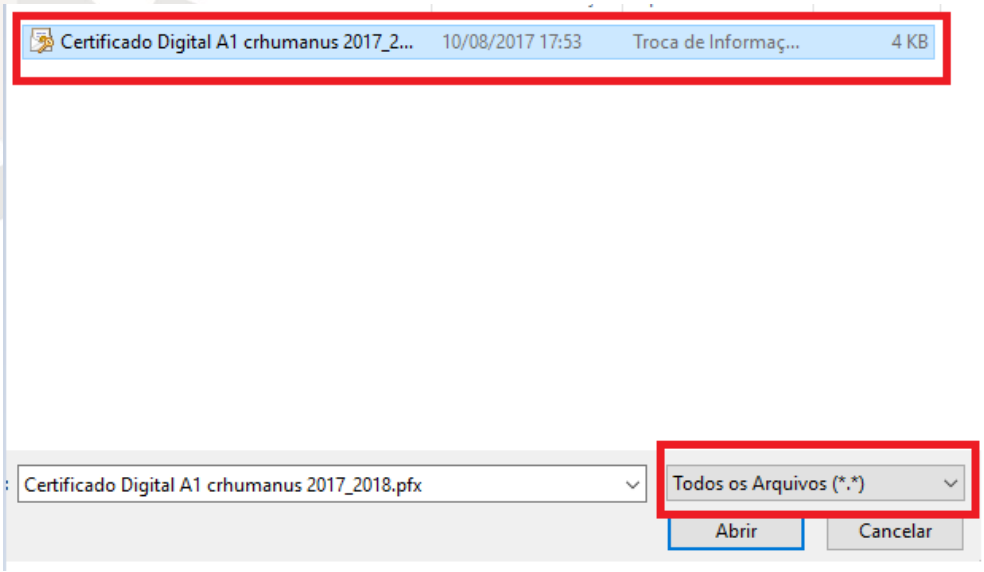


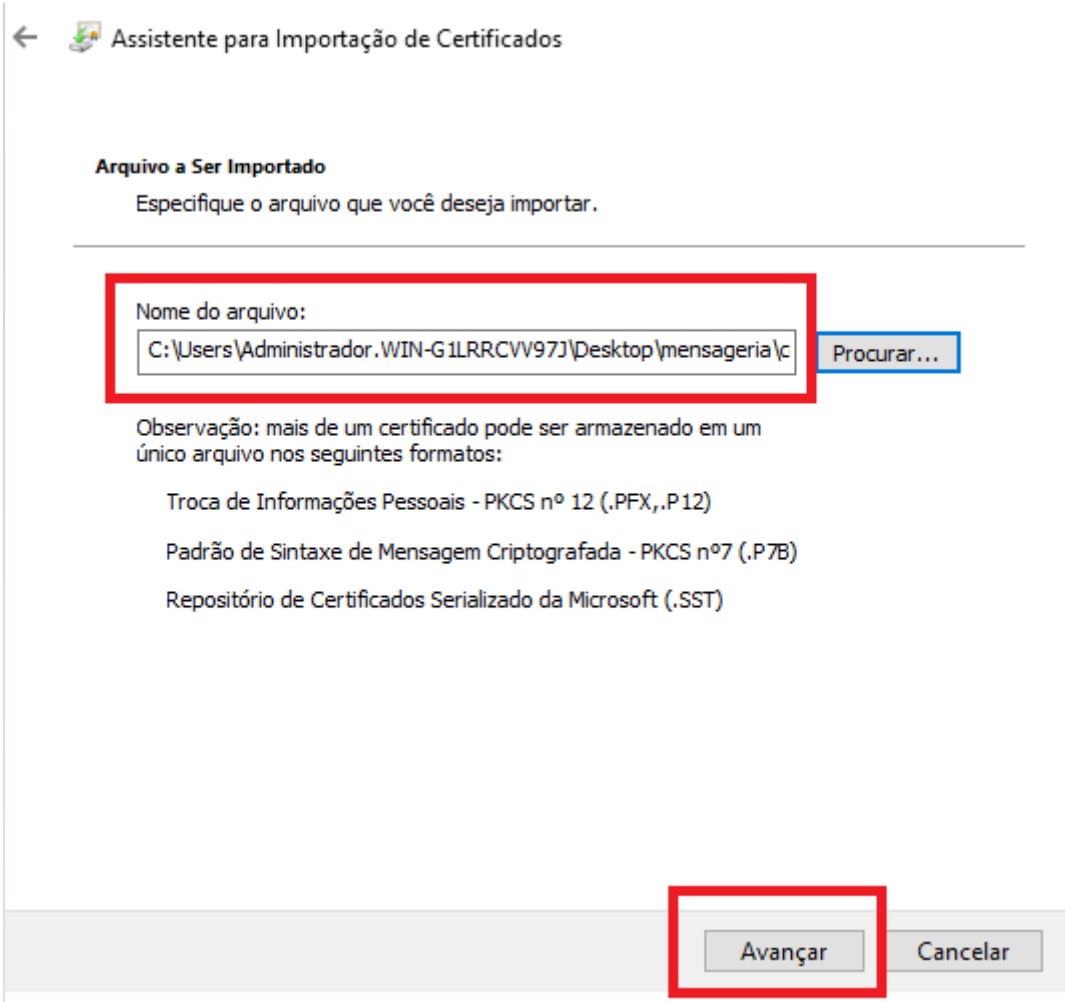
- Será exibida uma lista de opções para configuração do certificado, vamos adicionar o certificado da empresa.

Selecione:
- Pessoas confiáveis
  - Todas as tarefas
    - Importar

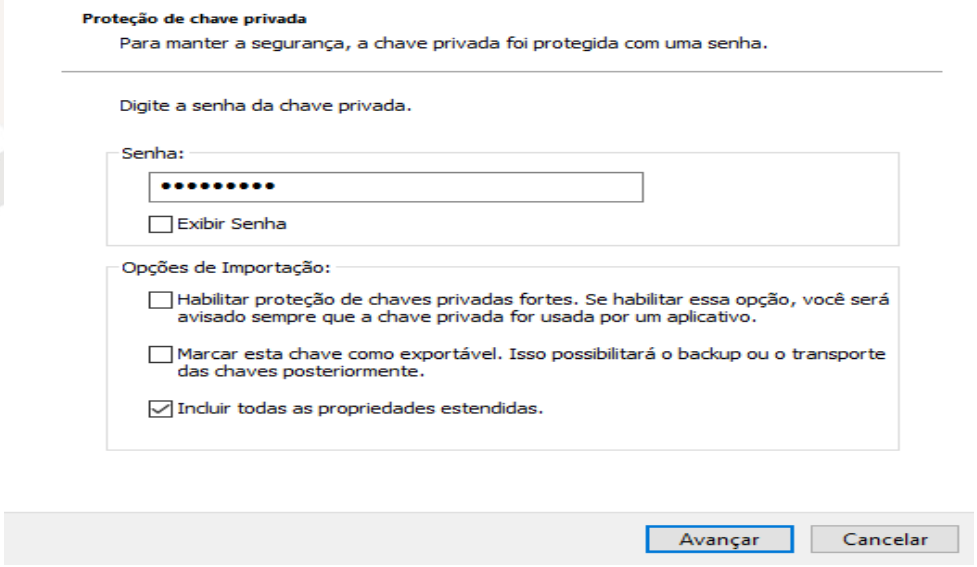
O assistente para adicionar o certificado será exibido.

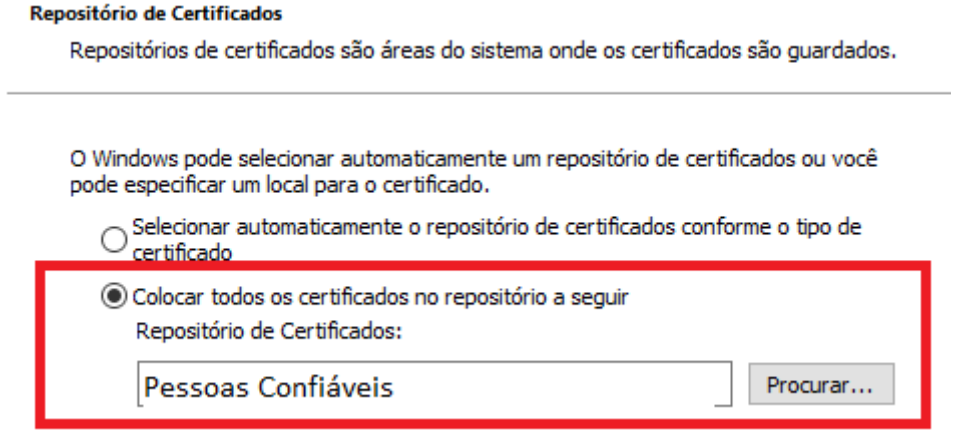
Clique em avançar e vá até a pasta onde se encontra o certificado da empresa, escolha a opção de visualização *todos os arquivos (*.*) para exibição do certificado.



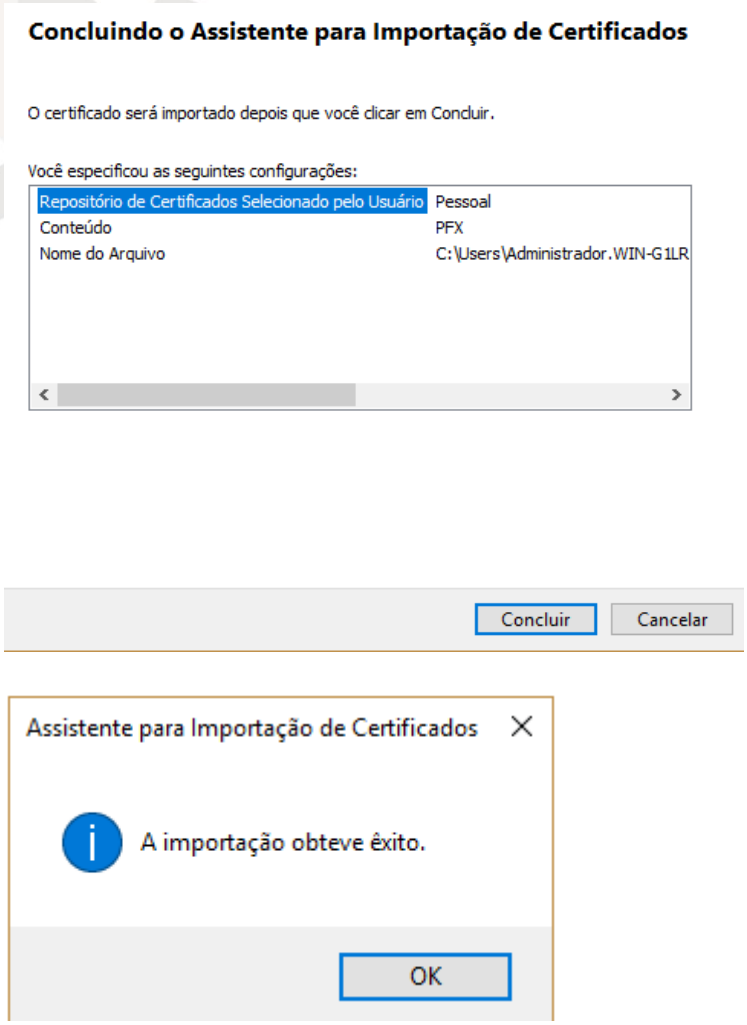


- Informe a senha referente ao seu certificado e clique em avançar.



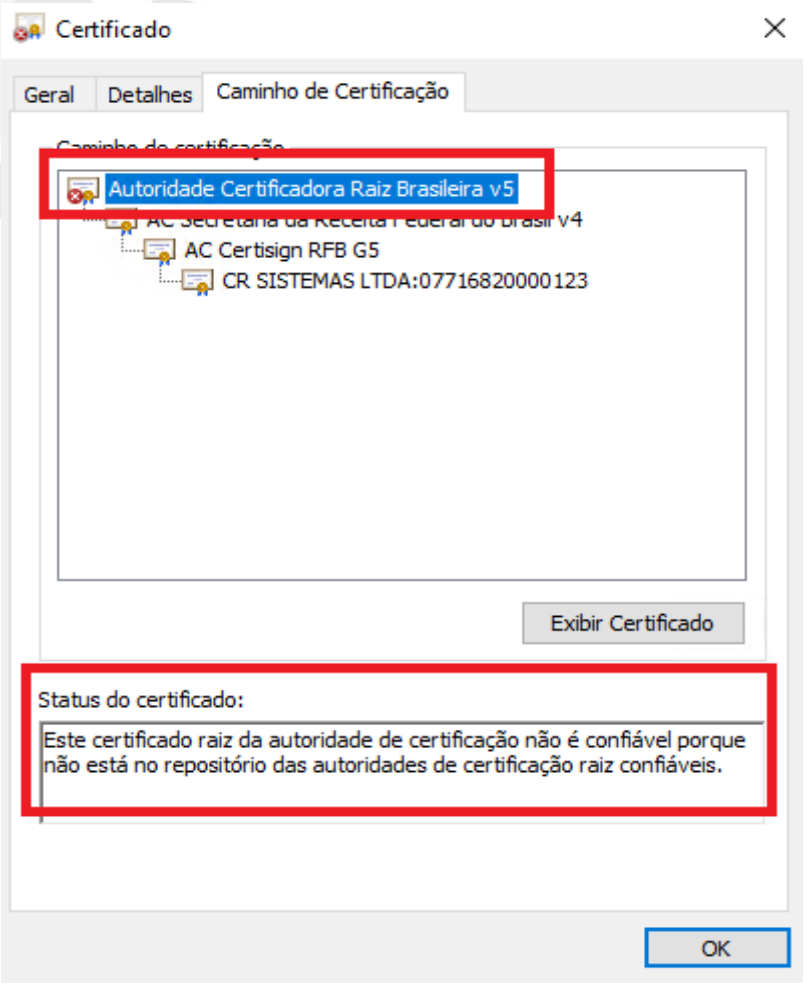


- Feitos todas as etapas, e conclua o assistente.



- Após a conclusão, verifique a cadeia de conexão do certificado recém instalado.

Selecione:
- Pessoas Confiáveis
    - Certificados
        - Duplo clique no certificado recém instalado (empresa)
            - Caminho de certificação



- Caso exiba a mensagem acima, será necessário a inclusão da certificadora de raiz confiável.
Ao contrário do certificado da empresa que é de uso pessoal, o da certificadora se encontra disponível na pasta “certificado” que se encontra na pasta WSESOCIAL:

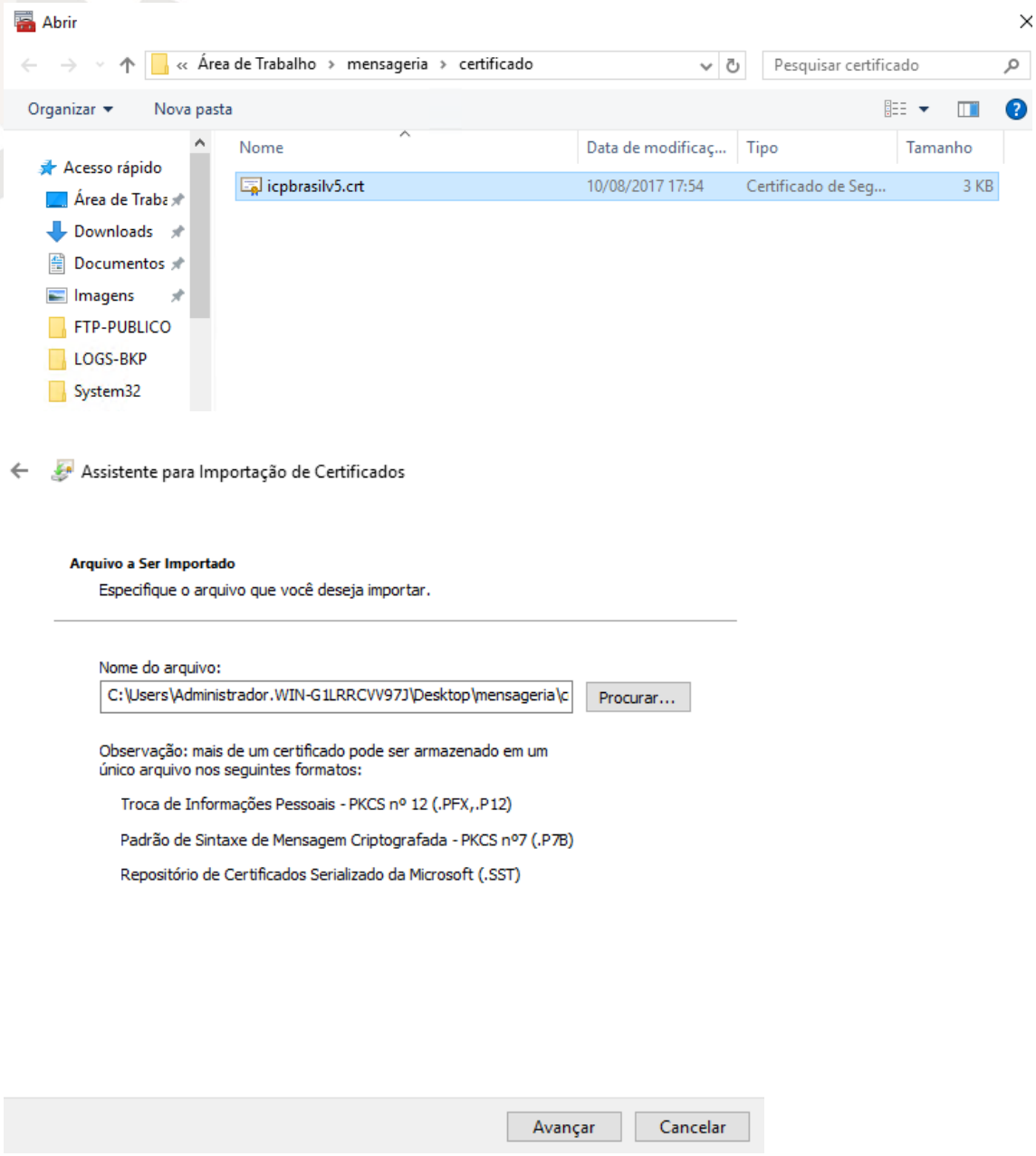
- “icpbrasilv5.crt”
- “acserprov4.crt”

Selecione:
- Autoridades de Certificação Raiz Confiáveis
  - Todas as tarefas
    - Importar

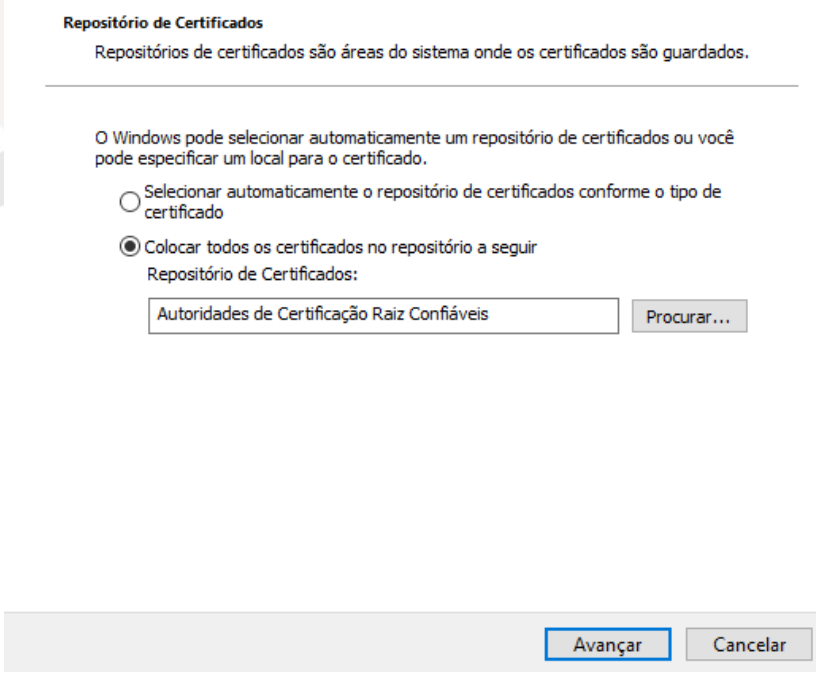
O assistente para adicionar o certificado será exibido.

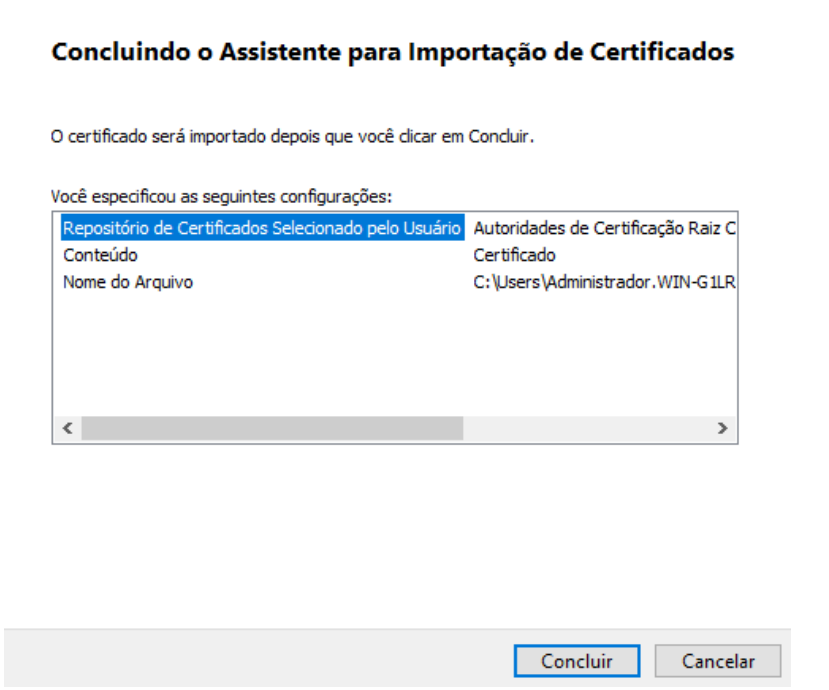
Clique em avançar e vá até a pasta onde se encontra os certificados de raiz confiável, escolha a opção de visualização *todos os arquivos (*.*) para exibição do certificado.

Selecione o certificado “icpbrasilv5.crt”

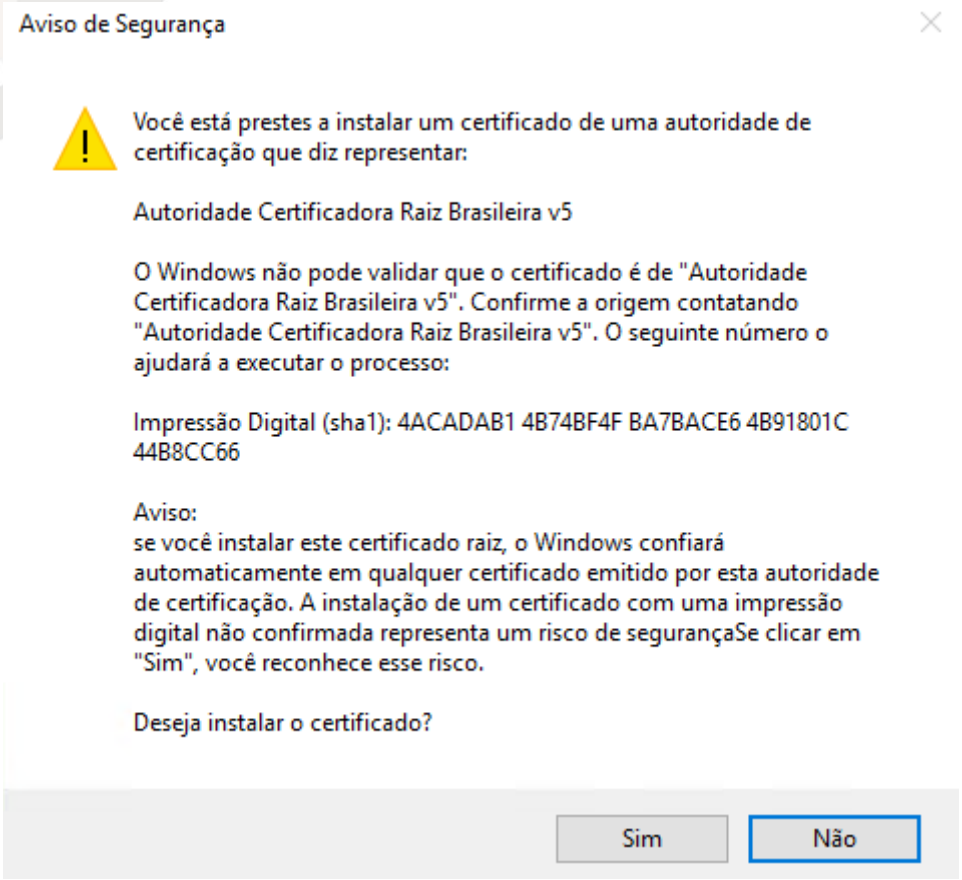

Abrir
« Área de Trabalho › mensageria › certificado
Pesquisar certificado
Organizar
Nova pasta
Acesso rápido
Área de Traba
Downloads
Documentos
Imagens
FTP-PUBLICO
LOGS-BKP
System32
Nome
Data de modificaç...
Tipo
Tamanho
icpbrasilv5.crt
10/08/2017 17:54
Certificado de Seg...
3 KB

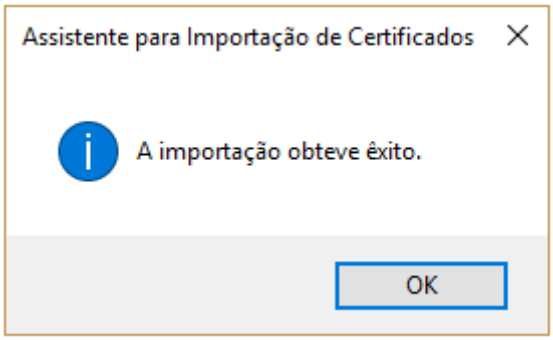
Assistente para Importação de Certificados
Arquivo a Ser Importado
Especifique o arquivo que você deseja importar.
Nome do arquivo:
C:\Users\Administrador.WIN-G1LRRCVV97J\Desktop\mensageria\c
Procurar...
Observação: mais de um certificado pode ser armazenado em um único arquivo nos seguintes formatos:
Troca de Informações Pessoais - PKCS nº 12 (.PFX,.P12)
Padrão de Sintaxe de Mensagem Criptografada - PKCS nº7 (.P7B)
Repositório de Certificados Serializado da Microsoft (.SST)
Avançar
Cancelar


Repositório de Certificados
Repositórios de certificados são áreas do sistema onde os certificados são guardados.
O Windows pode selecionar automaticamente um repositório de certificados ou você pode especificar um local para o certificado.
Selecionar automaticamente o repositório de certificados conforme o tipo de certificado
Colocar todos os certificados no repositório a seguir
Repositório de Certificados:
Autoridades de Certificação Raiz Confiáveis
Procurar...
Avançar
Cancelar


Concluindo o Assistente para Importação de Certificados
O certificado será importado depois que você clicar em Concluir.
Você especificou as seguintes configurações:
Repositório de Certificados Selecionado pelo Usuário
Autoridades de Certificação Raiz C
Conteúdo
Certificado
Nome do Arquivo
C:\Users\Administrador.WIN-G1LR
Concluir
Cancelar

- Caso a mensagem de segurança pedindo a confirmação seja exibida, clique em SIM.

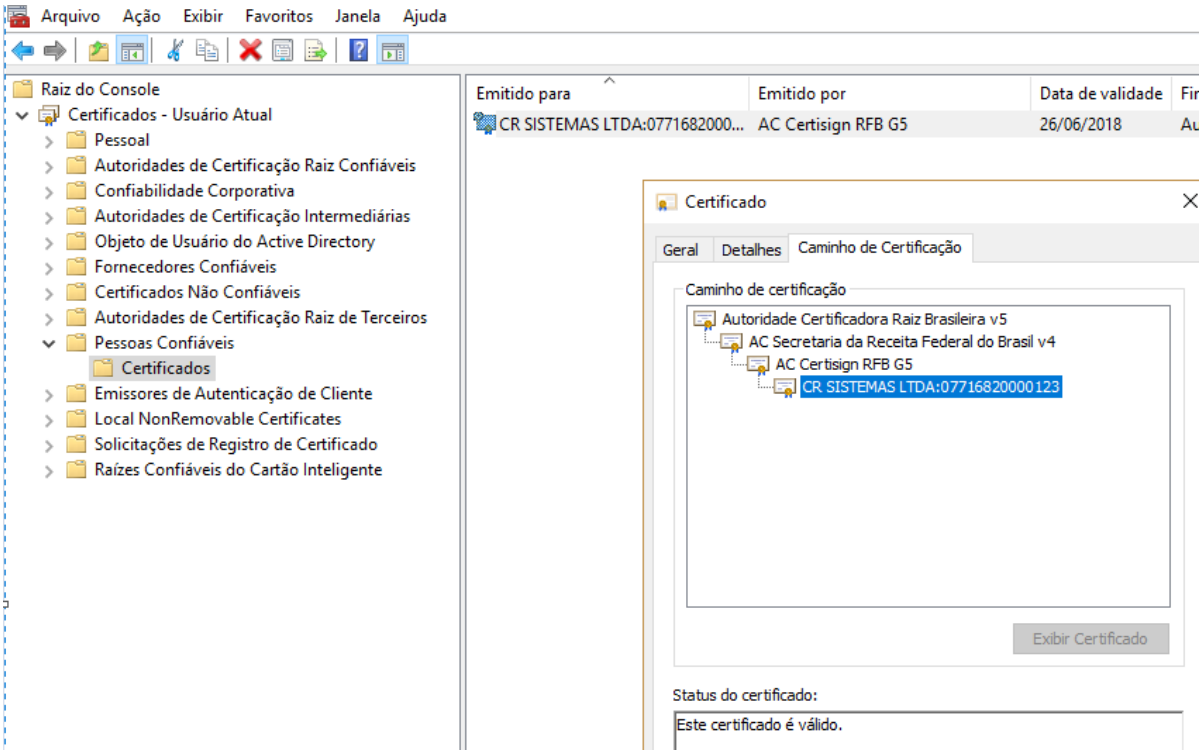




- Repita o processo, agora selecionando o certificado “acserprov4.crt”

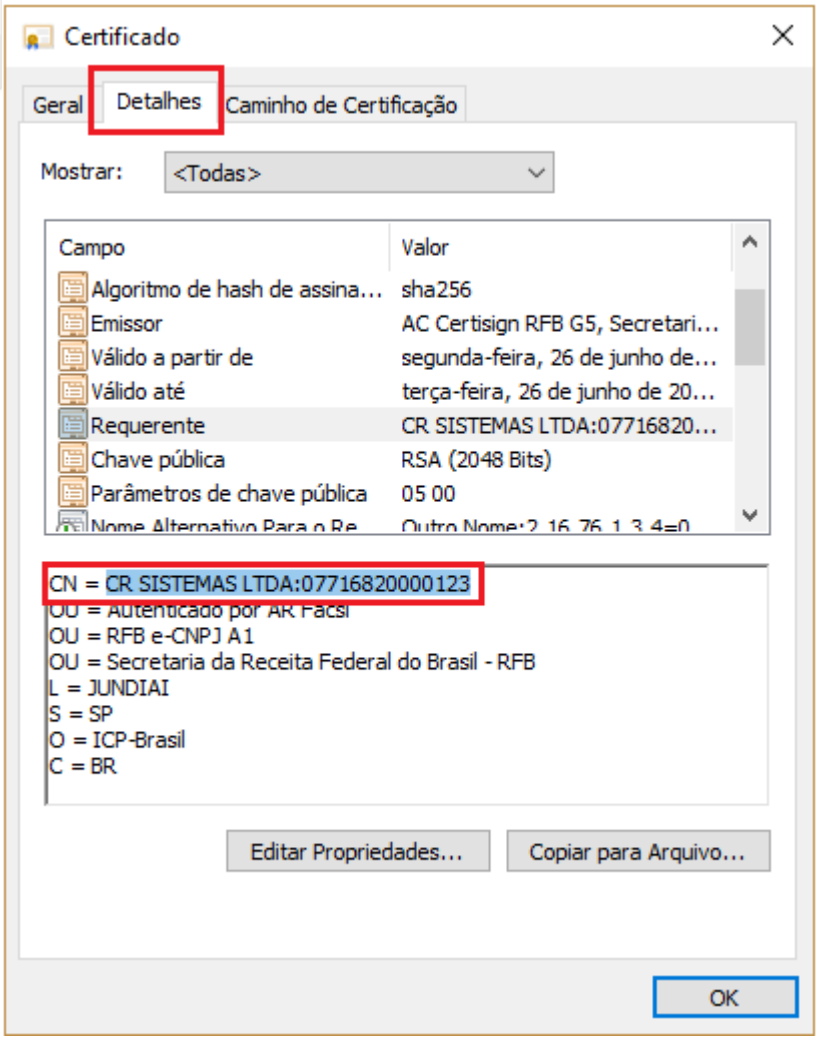
- Volte até o certificado da empresa em pessoas confiáveis, para constatar que o mesmo esteja validado por uma certificadora confiável.

Selecione:
- Pessoas Confiáveis
  - Certificados
    - Duplo clique no certificado recém instalado (empresa)
      - Caminho de certificação

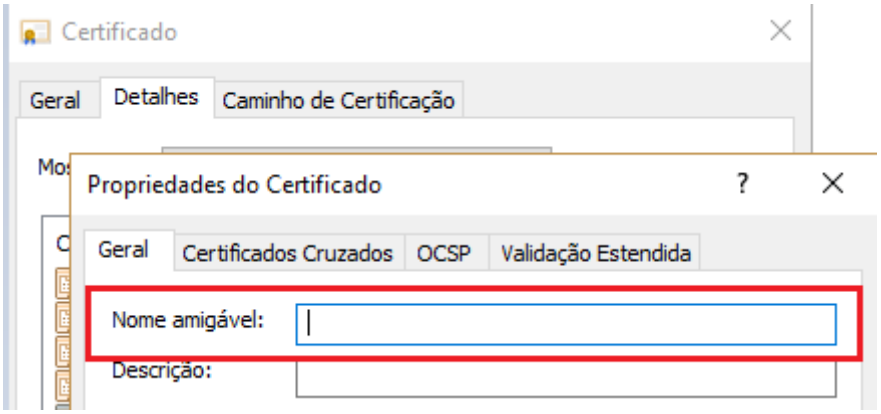


- Caso a mensagem “Este certificado é valido” seja exibida, o mesmo está operacional.

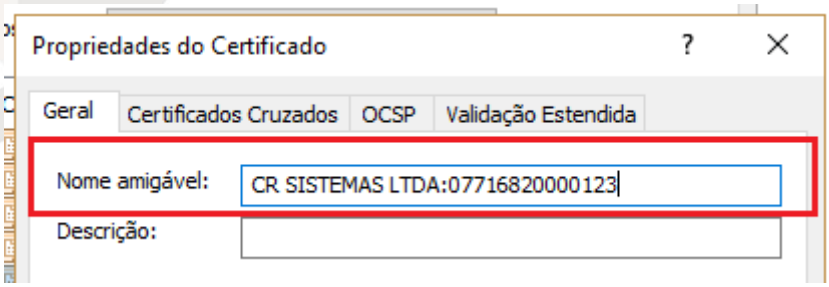
- Vá até a aba “Detalhes” “Requerente” selecione o “CN” após pressione as teclas CRTL+C



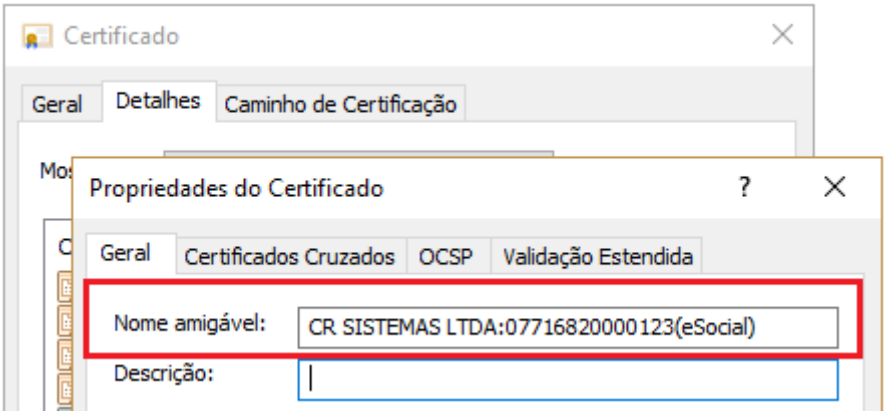
Clique no botão abaixo “Editar Propriedades...” caso o campo “Nome amigável” esteja vazio conforme modelo abaixo.



Pressione as teclas CRTL+V para preencher a informação do nome como no “CN”.

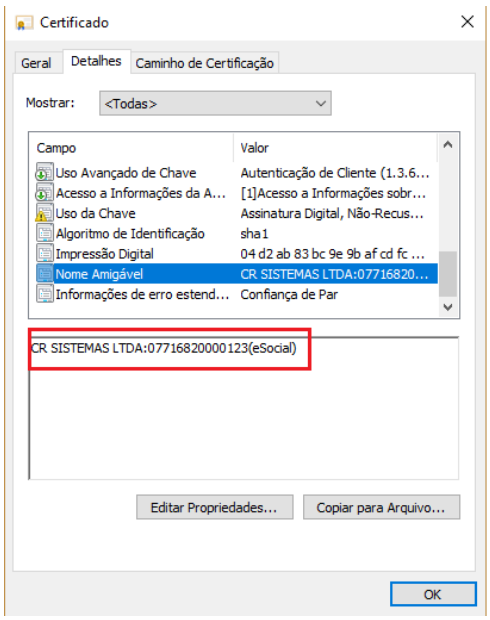


No final do nome adicione a TAG (eSocial) ficando conforme modelo abaixo.



Caso o nome da empresa com o CNPJ fique extenso truncando o campo, pode abreviar o nome a empresa, o importante é ao final do nome respeitar a TAG (eSocial)

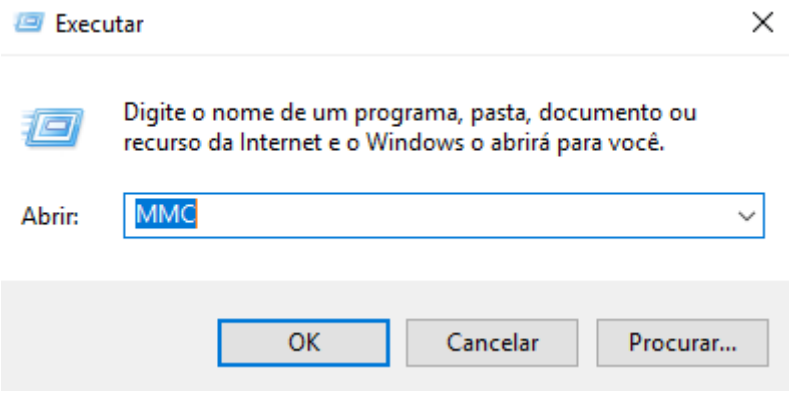
Confirme se o nome amigável ficou parametrizado corretamente, voltando para a aba “Detalhes”



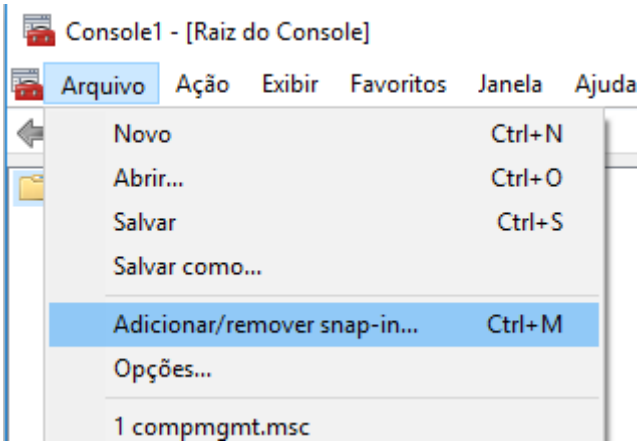
Instalação do certificado Digital nas estações de trabalho (se houver)

- Nas estações de trabalho, onde serão gerados os XML'S também será preciso a instalação do certificado A1, isso se deve ao fato de que cada arquivo XML precisa estar devidamente assinado. (Requisito do e-Social)

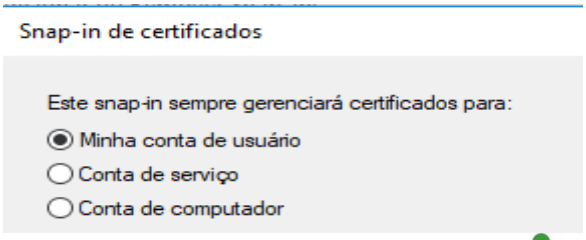
Abra o console de gerenciamento para adicionar o certificado.



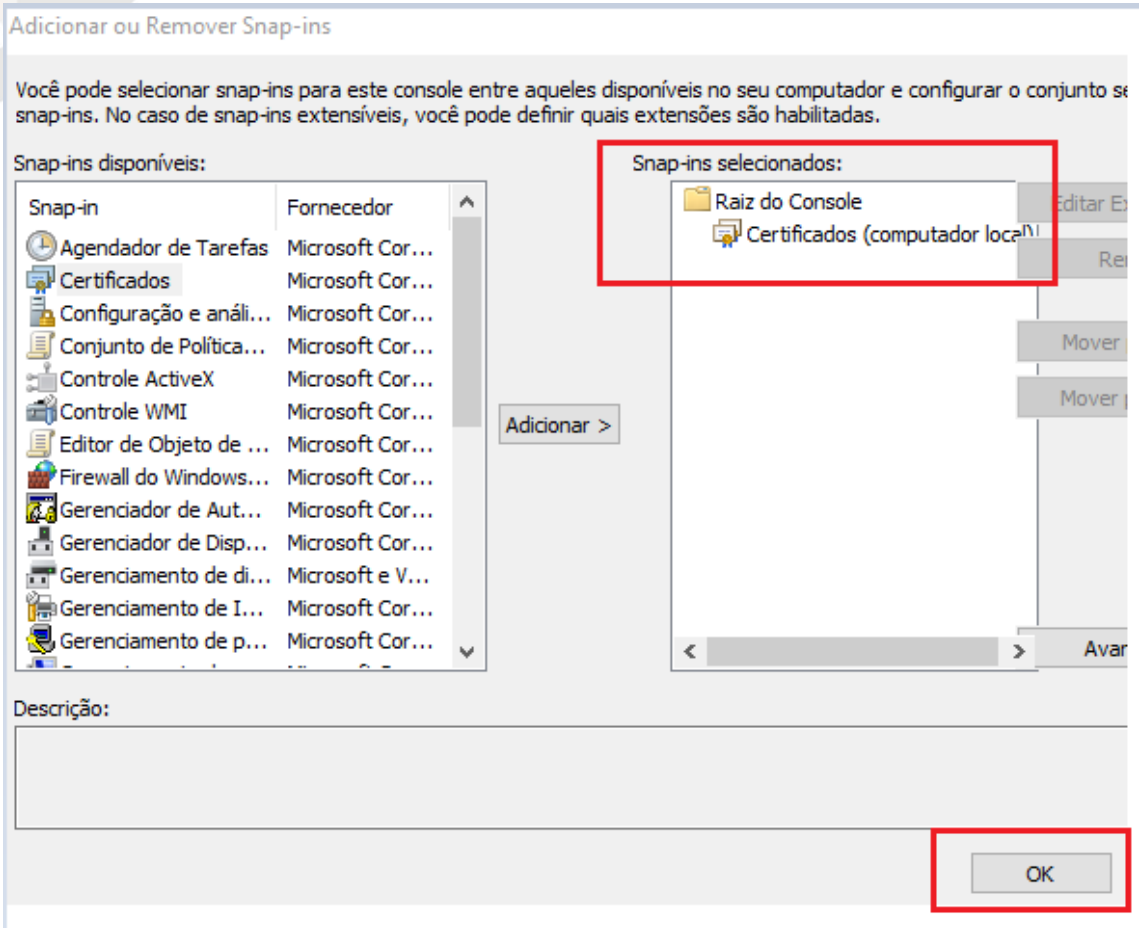
Adicionar ou remover "snap-ins"



- Selecione "Minha conta de usuário"

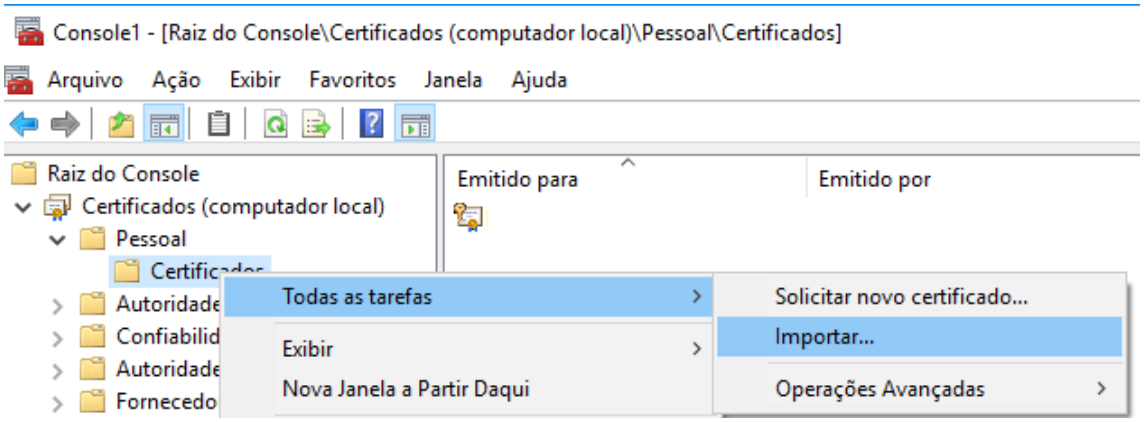


- Certifique-se das configurações selecionadas e clique em “OK”

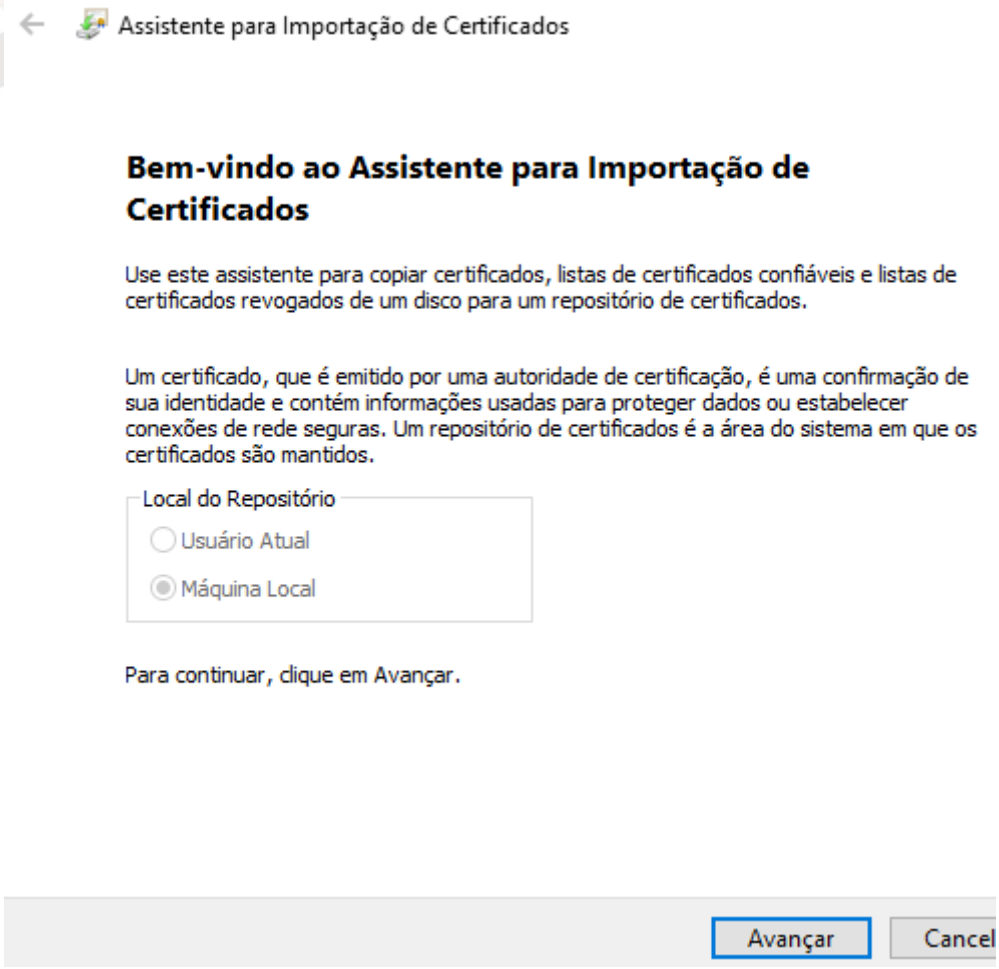


- Instale o certificado na raiz pessoal.

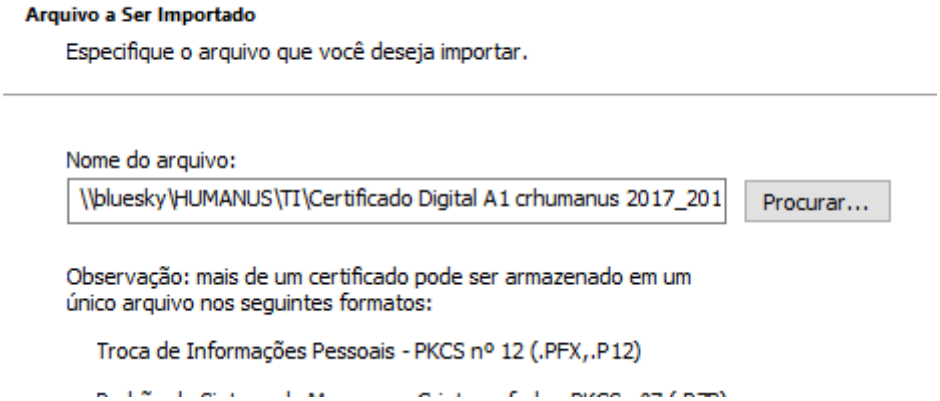
- Pessoal
  - Todas as tarefas
    - Importar



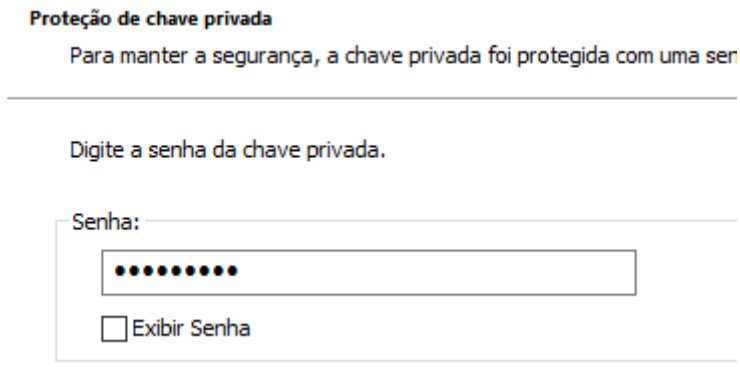
- Inicie o assistente para importar o certificado.



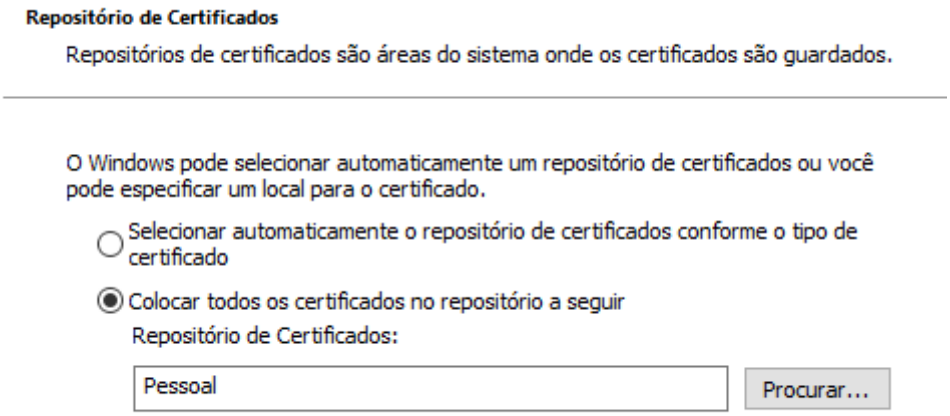
- Especifique o caminho onde se encontra o certificado.



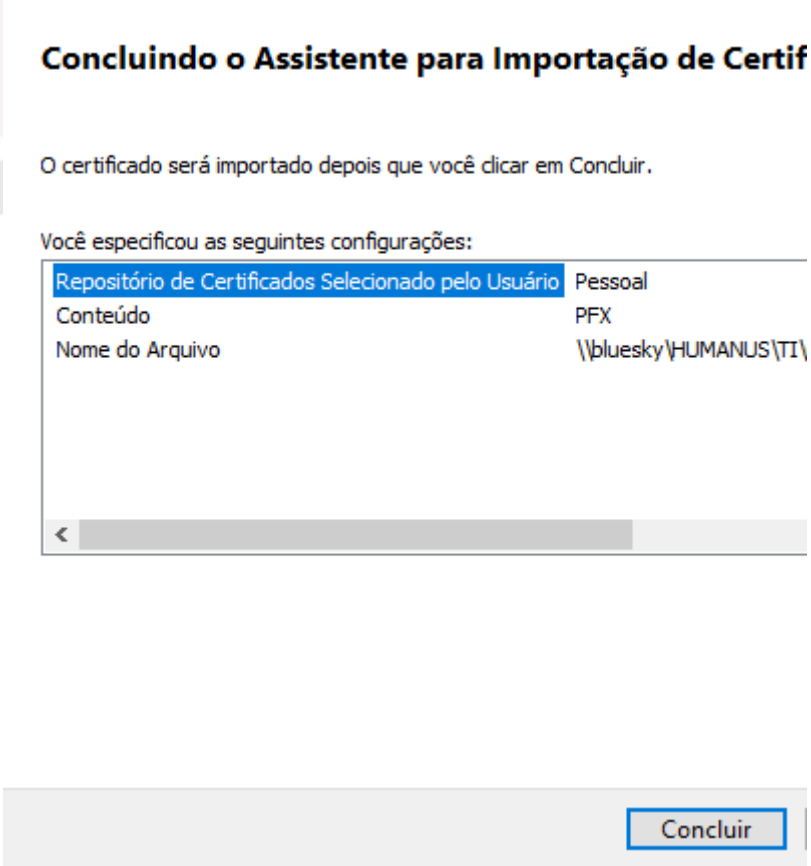
- Informe a senha do certificado.

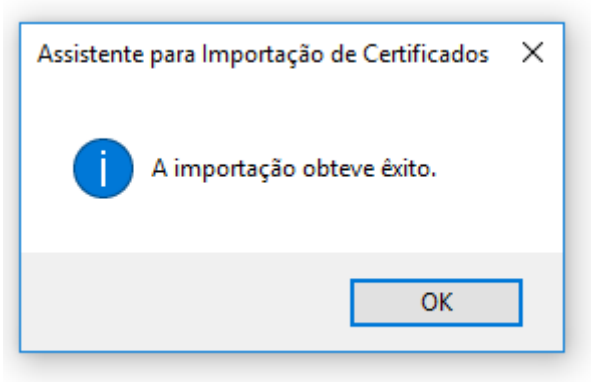


- Confirme a raiz onde o mesmo será instalado.



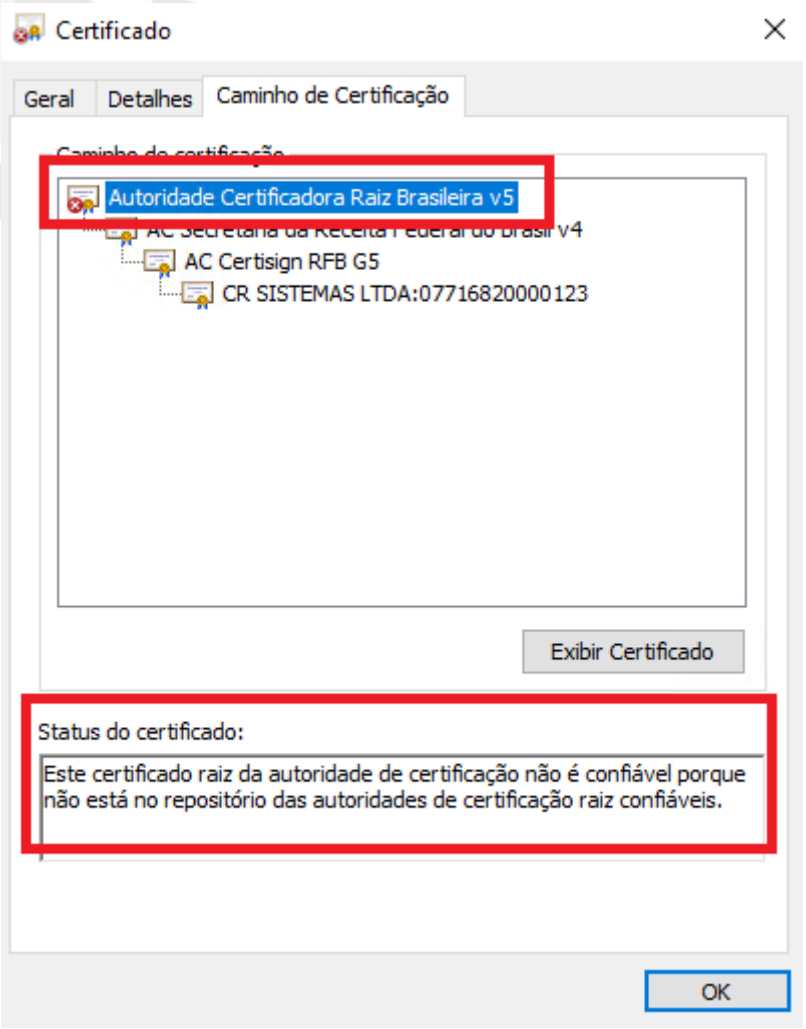
- Conclua o assistente.





- Após a conclusão, verifique a cadeia de conexão do certificado recém instalado.

Selecione:
- Pessoal
  - Certificados
    - Duplo clique no certificado recém instalado (empresa)
      - Caminho de certificação



- Mesmo procedimento anterior, caso seja exiba a mensagem acima, será necessário a inclusão da certificadora de raiz confiável.
Ao contrário do certificado da empresa que é de uso pessoal, o da certificadora se encontra disponível na pasta “certificado” que se encontra na pasta WSESOCIAL:

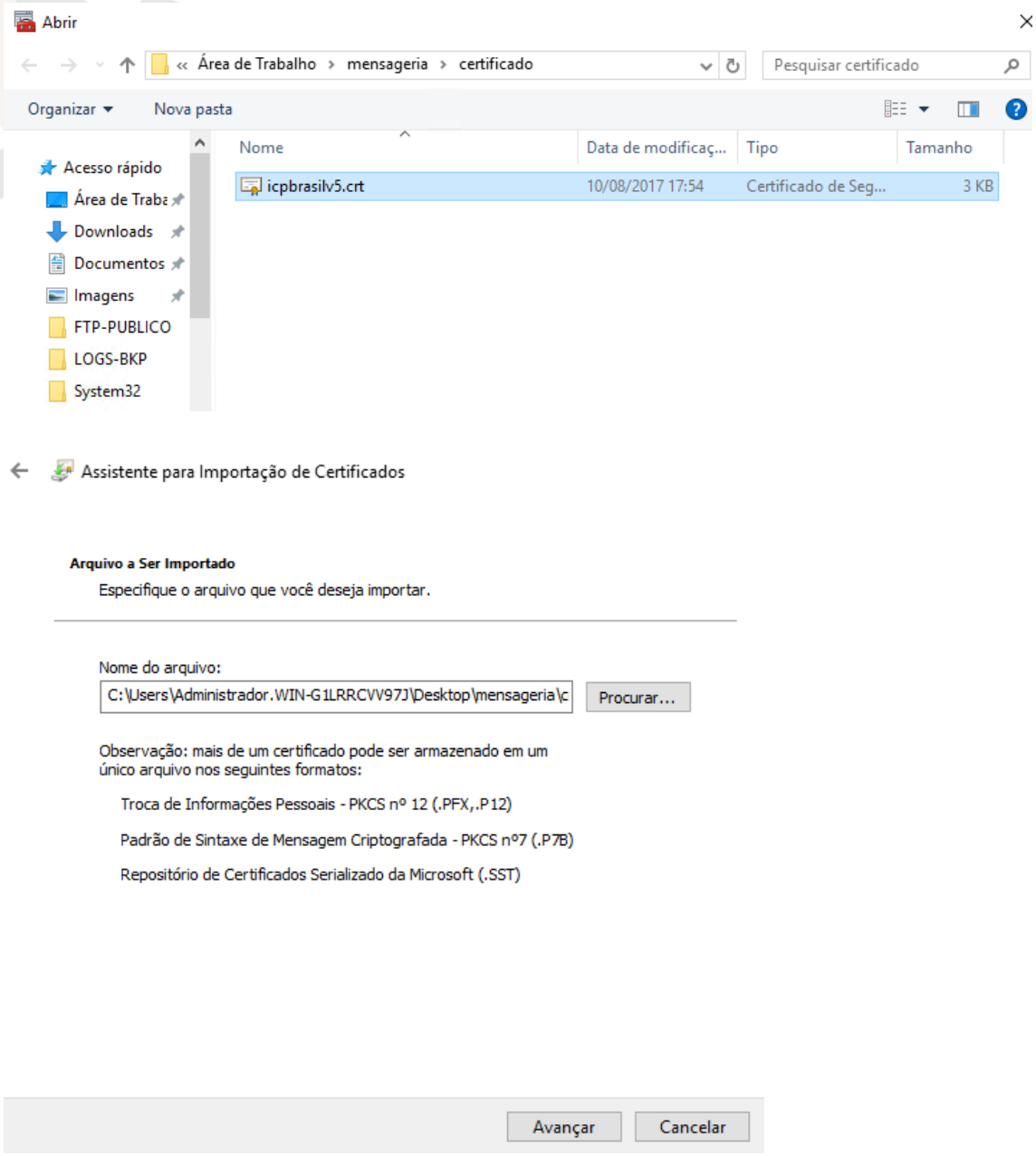
- “icpbrasilv5.crt”
- “acserprov4.crt”

Selecione:
- Autoridades de Certificação Raiz Confiáveis
  - Todas as tarefas
    - Importar

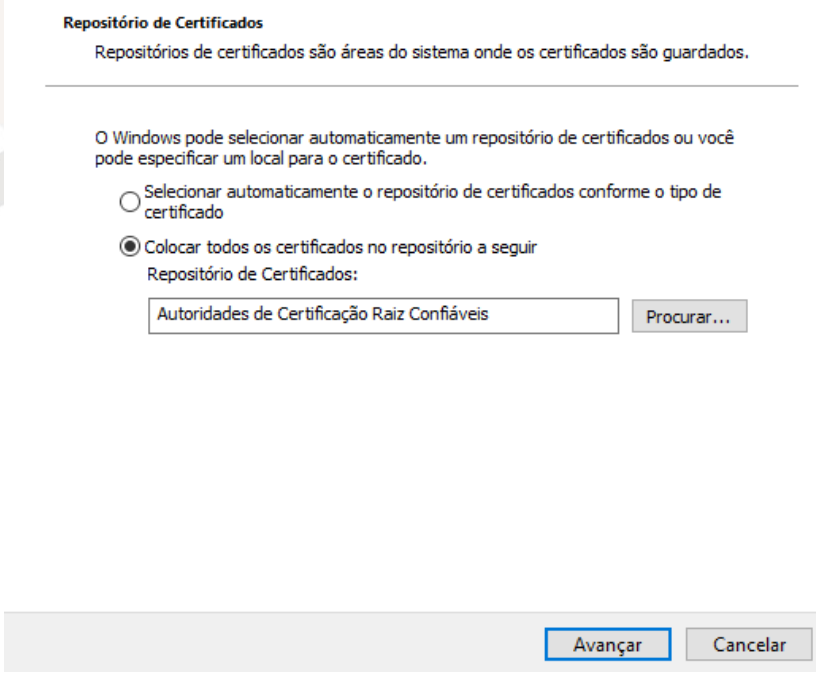
O assistente para adicionar o certificado será exibido.

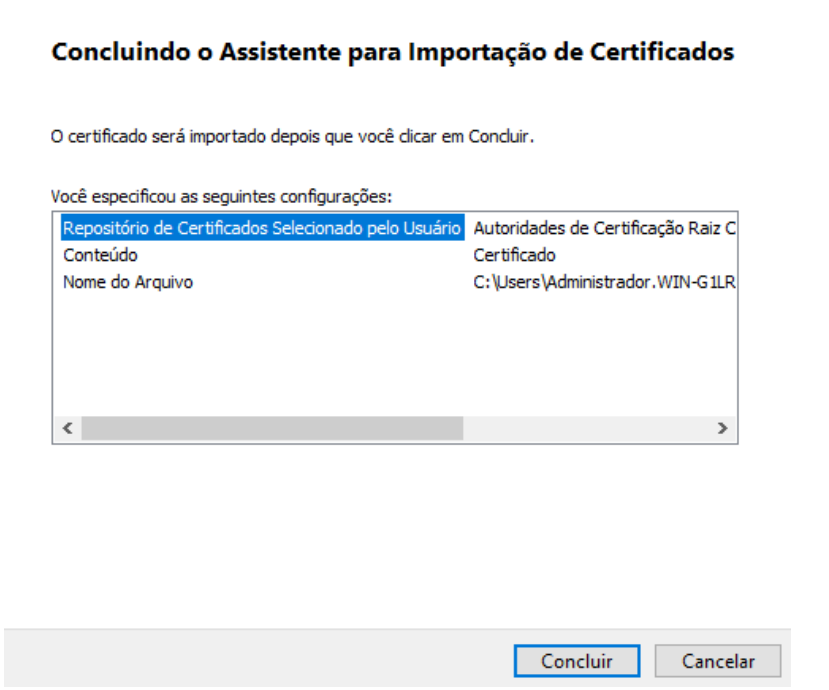
Clique em avançar e vá até a pasta onde se encontra os certificados de raiz confiável, escolha a opção de visualização *todos os arquivos (*.*) para exibição do certificado.

Selecione o certificado “icpbrasilv5.crt”

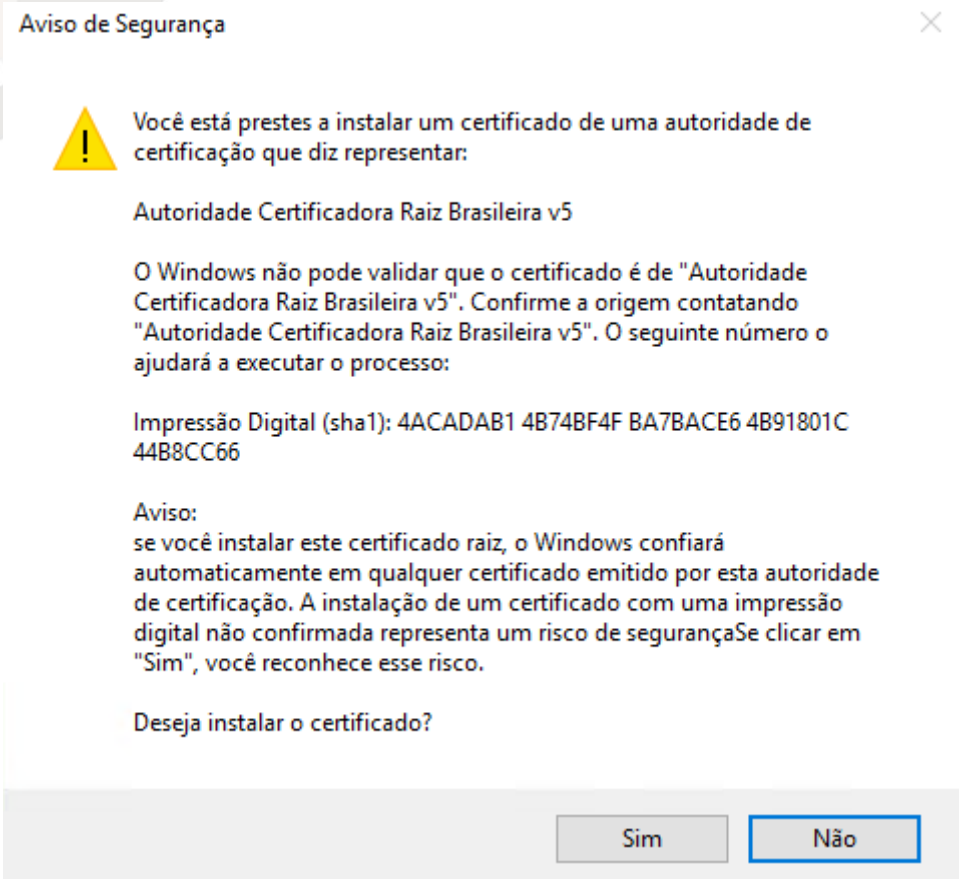

Abrir
« Área de Trabalho › mensageria › certificado
Pesquisar certificado
Organizar
Nova pasta
Acesso rápido
Área de Traba
Downloads
Documentos
Imagens
FTP-PUBLICO
LOGS-BKP
System32
Nome
Data de modificaç...
Tipo
Tamanho
icpbrasilv5.crt
10/08/2017 17:54
Certificado de Seg...
3 KB

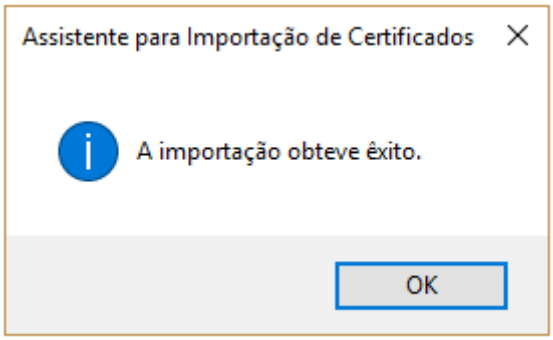
Assistente para Importação de Certificados
Arquivo a Ser Importado
Especifique o arquivo que você deseja importar.
Nome do arquivo:
C:\Users\Administrador.WIN-G1LRRCVV97J\Desktop\mensageria\c
Procurar...
Observação: mais de um certificado pode ser armazenado em um único arquivo nos seguintes formatos:
Troca de Informações Pessoais - PKCS nº 12 (.PFX,.P12)
Padrão de Sintaxe de Mensagem Criptografada - PKCS nº7 (.P7B)
Repositório de Certificados Serializado da Microsoft (.SST)
Avançar
Cancelar


Repositório de Certificados
Repositórios de certificados são áreas do sistema onde os certificados são guardados.
O Windows pode selecionar automaticamente um repositório de certificados ou você pode especificar um local para o certificado.
Selecionar automaticamente o repositório de certificados conforme o tipo de certificado
Colocar todos os certificados no repositório a seguir
Repositório de Certificados:
Autoridades de Certificação Raiz Confiáveis
Procurar...
Avançar
Cancelar


Concluindo o Assistente para Importação de Certificados
O certificado será importado depois que você clicar em Concluir.
Você especificou as seguintes configurações:
Repositório de Certificados Selecionado pelo Usuário
Autoridades de Certificação Raiz C
Conteúdo
Certificado
Nome do Arquivo
C:\Users\Administrador.WIN-G1LR
Concluir
Cancelar

- Caso a mensagem de segurança pedindo a confirmação seja exibida, clique em SIM.

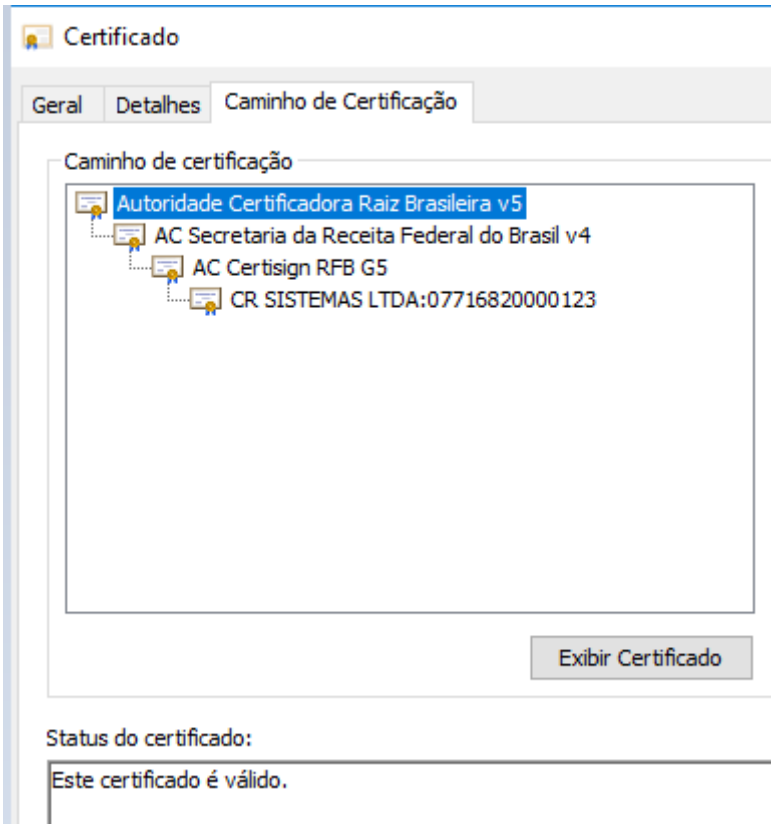




- Repita o processo, agora selecionando o certificado “acserprov4.crt”

- Volte até o certificado da empresa em pessoal, para constatar que o mesmo esteja validado por uma certificadora confiável.

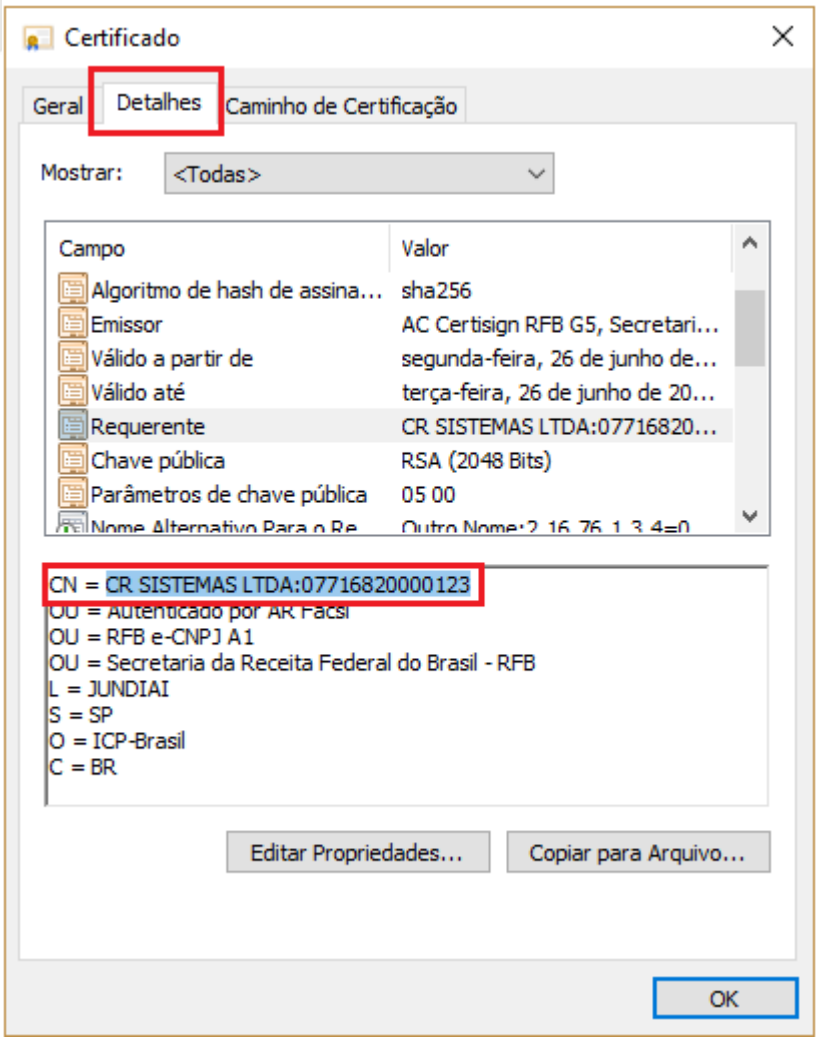
Selecione:
- Pessoal
  - Certificados
    - Duplo clique no certificado recém instalado (empresa)
      - Caminho de certificação



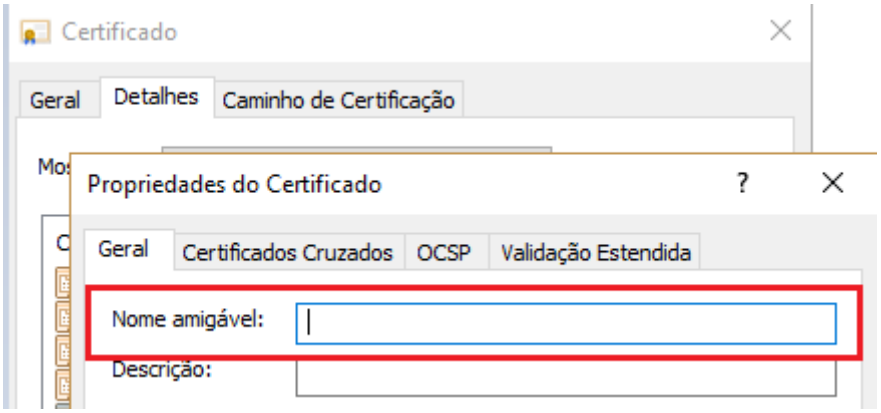
- Caso a mensagem “Este certificado é valido” seja exibida, o mesmo está operacional.

- Será necessário repetir o procedimento de adicionar a TAG (eSocial) no nome amigável do certificado, repita os passos abaixo.

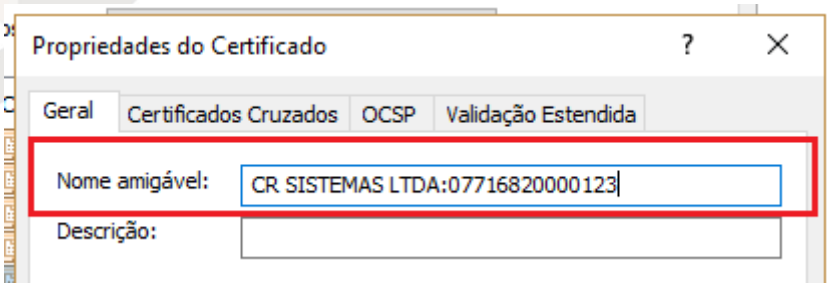
- Vá até a aba “Detalhes” “Requerente” selecione o “CN” após pressione as teclas CRTL+C



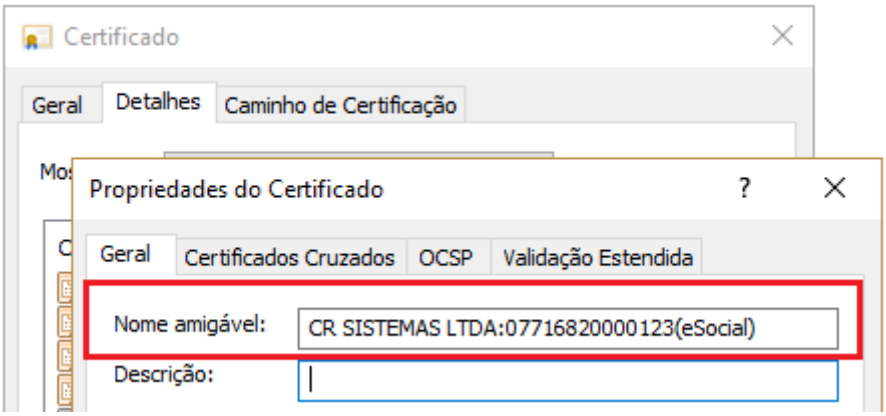
Clique no botão abaixo “Editar Propriedades...” caso o campo “Nome amigável” esteja vazio conforme modelo abaixo.



Pressione as teclas CRTL+V para preencher a informação do nome como no “CN”.

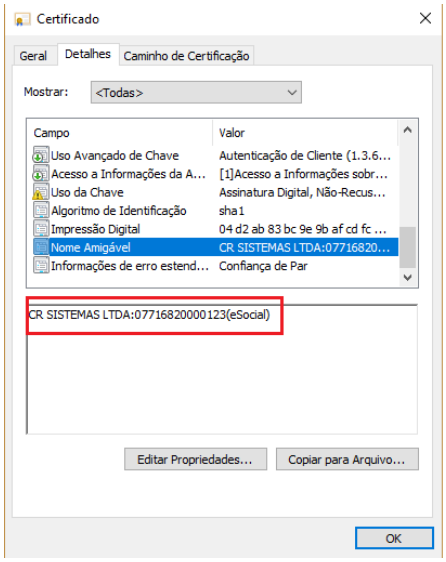


No final do nome adicione a TAG (eSocial) ficando conforme modelo abaixo.



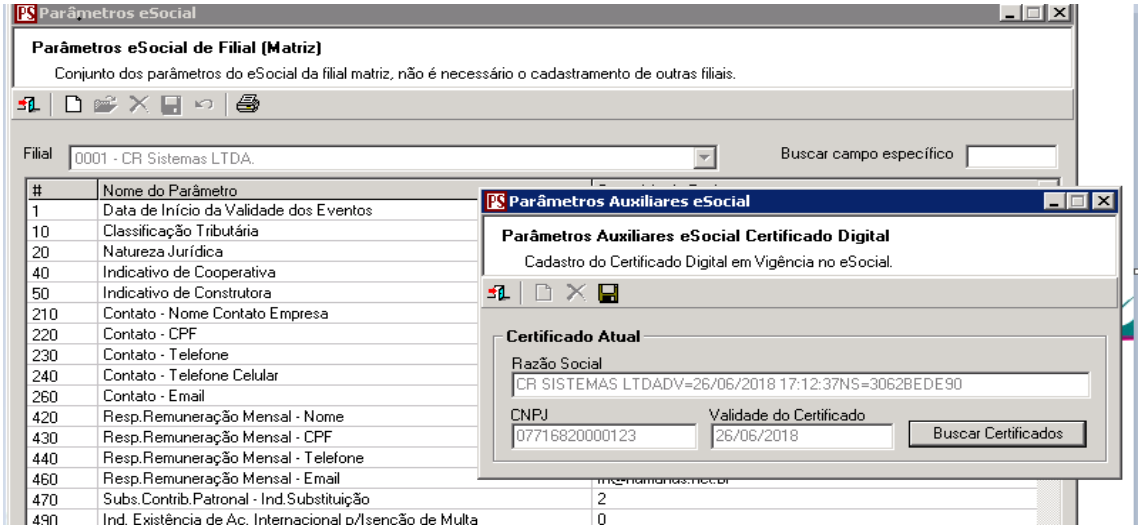
Caso o nome da empresa com o CNPJ fique muito extenso truncando o campo, pode abreviar o nome a empresa, o importante é ao final do nome respeitar a TAG (eSocial)

Confirme se o nome amigável ficou parametrizado corretamente, voltando para a aba “Detalhes”



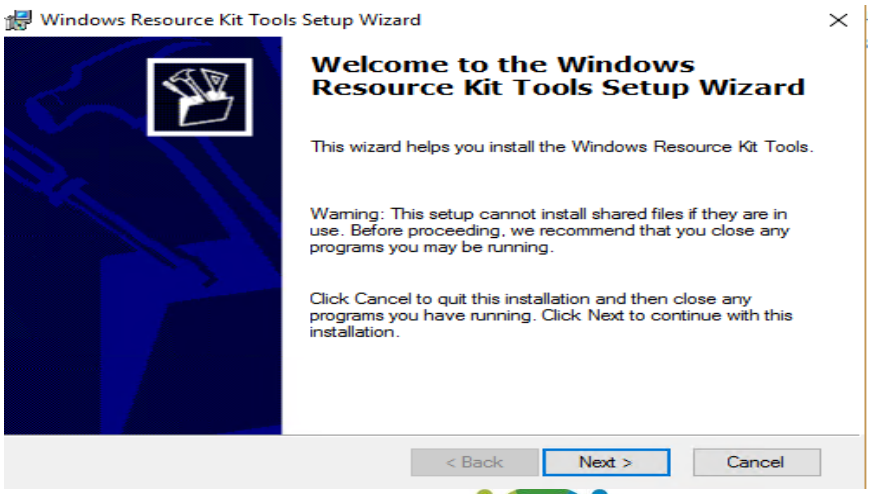
Após concluir a importação dos certificados no Windows, também se faz necessário importar os mesmos no Humanus, em:

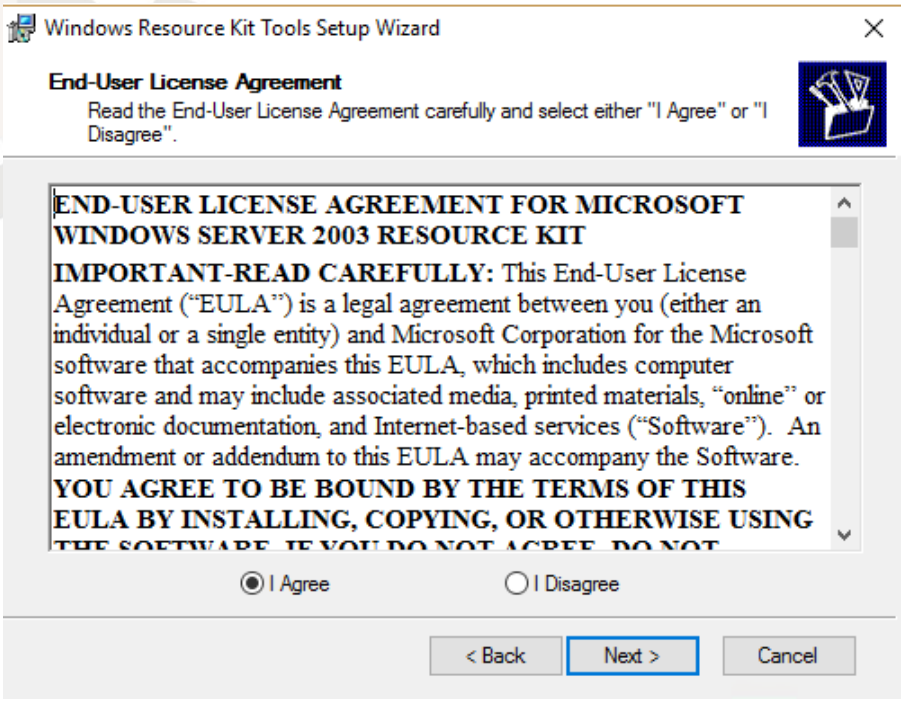
- Modulo Processos legais
  - Cadastros
    - Parâmetros de Filial

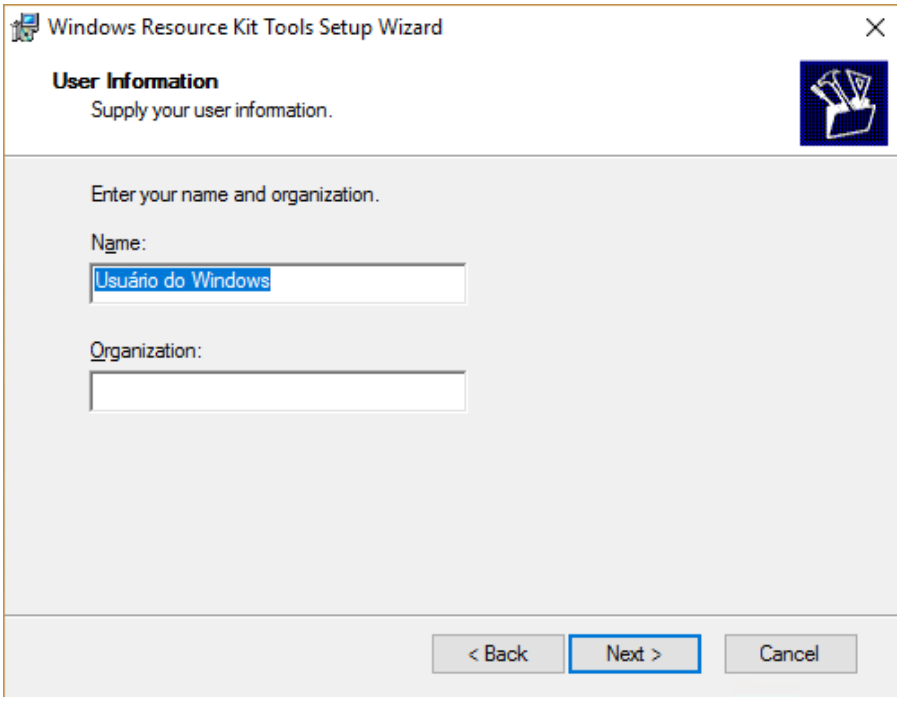


Windows Resource Kits:

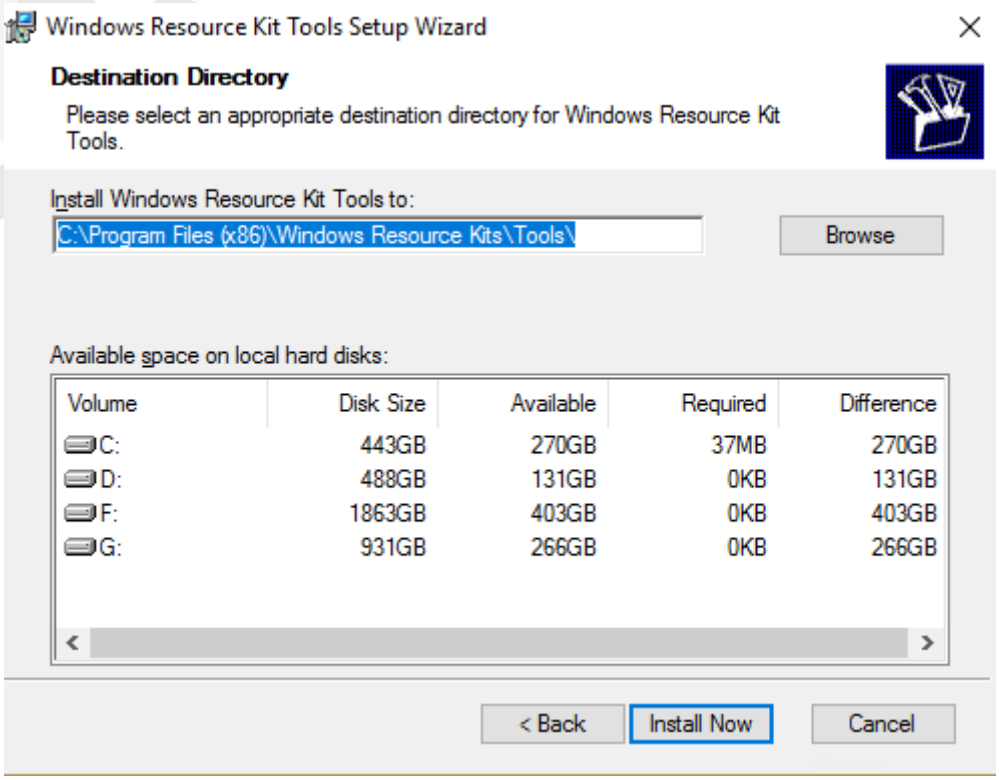
- Dentro da pasta “WSESOCIAL” se encontra o setup do “Windows Resource Kits” “winCertHTTPtools.exe” o mesmo é necessário apenas no **SERVIDOR**, este programa é utilizado para autorizar o uso do protocolo HTTP com o certificado para determinados usuários.
O processo de instalação é padrão (não há necessidades especiais de parametrizações) basta ir avançando conforme as telas a seguir (NEXT)

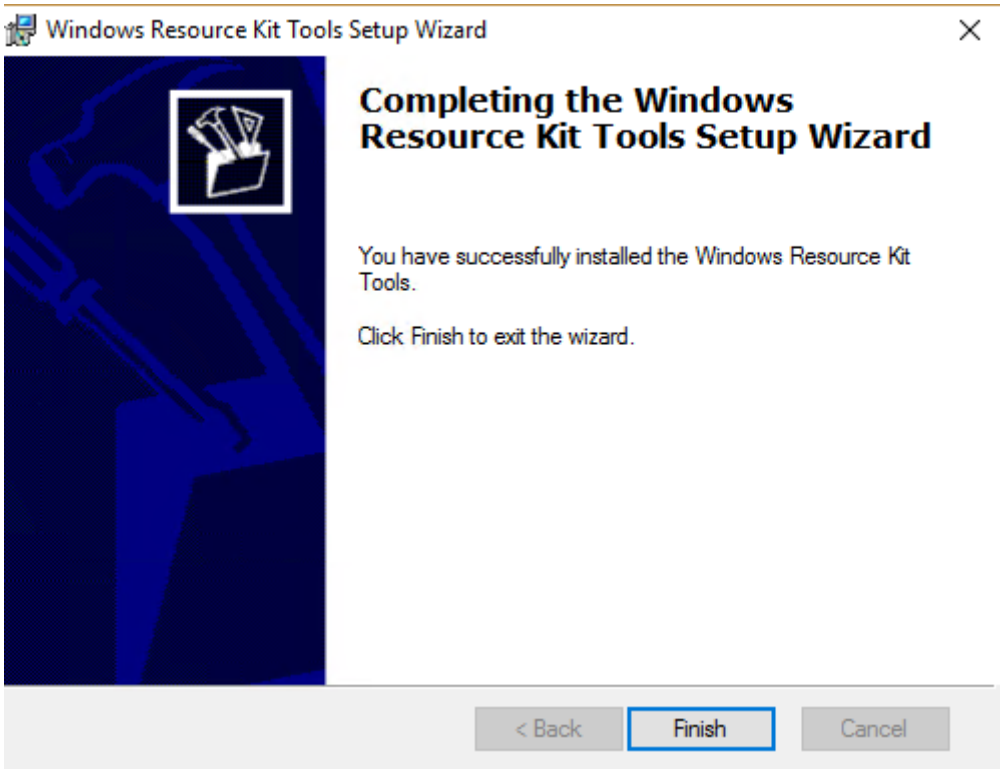




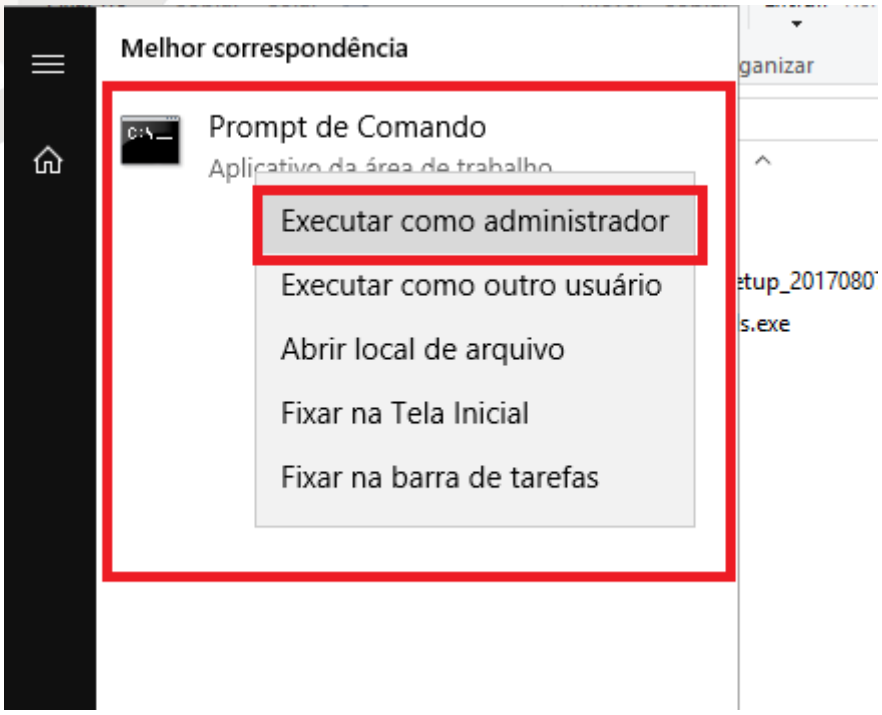


- Recomendamos manter o diretório padrão sugerido pelo instalador.


Windows Resource Kit Tools Setup Wizard
Destination Directory
Please select an appropriate destination directory for Windows Resource Kit Tools.
Install Windows Resource Kit Tools to:
C:\Program Files (x86)\Windows Resource Kits\Tools\
Browse
Available space on local hard disks:
Volume Disk Size Available Required Difference
C: 443GB 270GB 37MB 270GB
D: 488GB 131GB 0KB 131GB
F: 1863GB 403GB 0KB 403GB
G: 931GB 266GB 0KB 266GB
< Back
Install Now
Cancel


Windows Resource Kit Tools Setup Wizard
Completing the Windows Resource Kit Tools Setup Wizard
You have successfully installed the Windows Resource Kit Tools.
Click Finish to exit the wizard.
< Back
Finish
Cancel

- Execute o “Prompt de comando” como Administrador



- No prompt seguir até o caminho “Program Files (x86)\Windows Resource Kits\Tools”

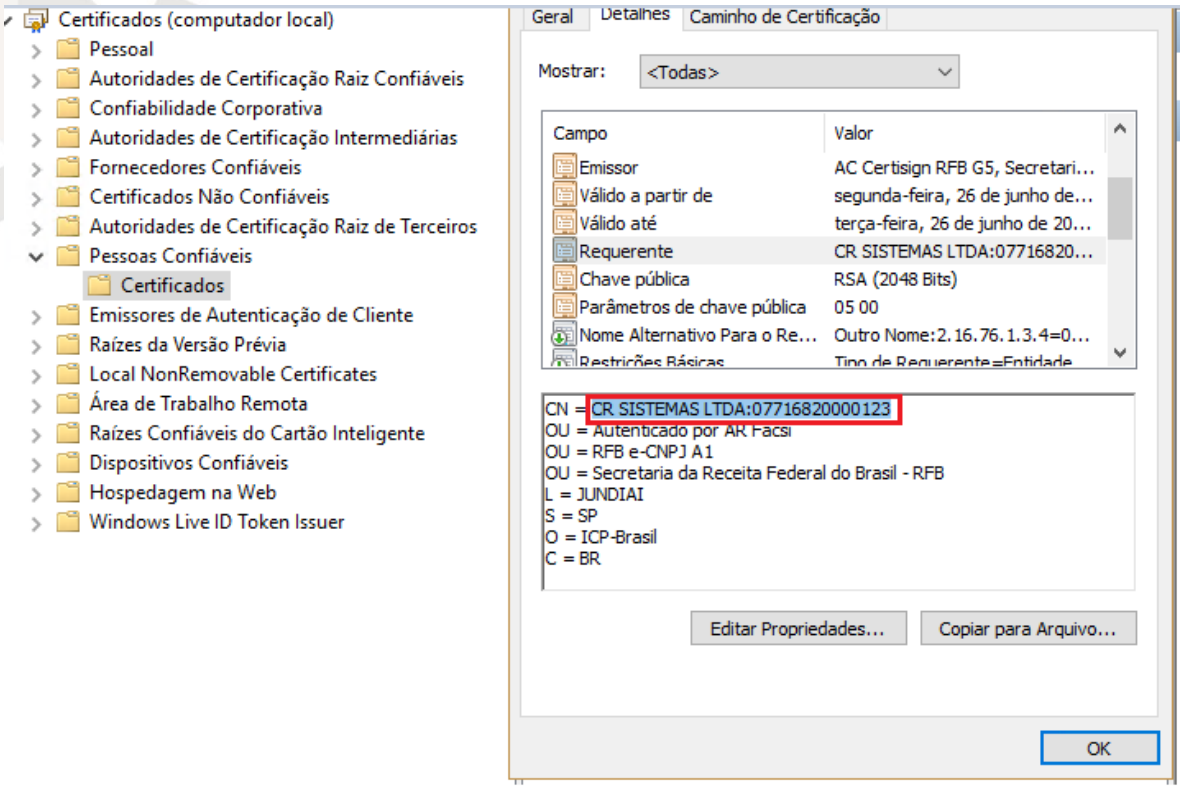
- Execute o comando:

winhttpcertcfg.exe -g -c local_machine\TrustedPeople -s "**CN DO SEU CERTIFICADO**" -a todos

Veja o nome correto do CN do certificado da empresa, no seguinte caminho.

C:\Windows\System32\ mmc.exe

Selecione:
- Pessoas Confiáveis
  - Certificado
    - Selecione o certificado da empresa com um duplo clique
      - Aba detalhes
        - Campo Requerente
          - Opção CN



No exemplo o nome do nosso certificado é “CR SISTEMAS LTDA:07716820000123”

Obs. Selecione e copie o nome CN com cuidado, para não ficar com espaçamento no início e no final do nome.

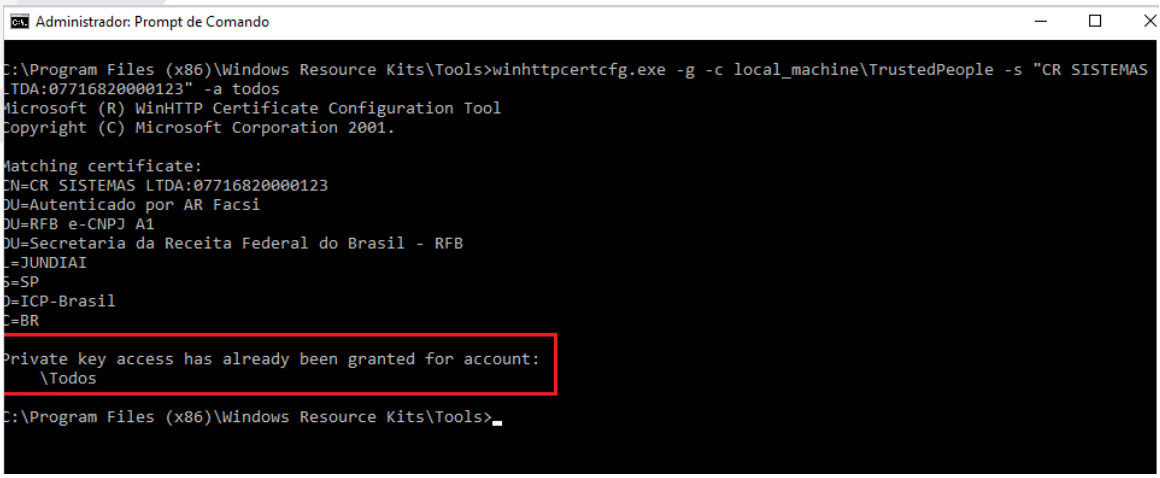
- Agora que sabemos o nome CN o comando fica dessa maneira.

winhttpcertcfg.exe -g -c local_machine\TrustedPeople -s "CR SISTEMAS LTDA:07716820000123" -a **todos**

Caso o idioma do sistema operacional esteja em inglês, substituir **todos** por **everyone**.

winhttpcertcfg.exe -g -c local_machine\TrustedPeople -s "CR SISTEMAS LTDA:07716820000123" -a **everyone**

- Caso o comando seja executado com sucesso a mensagem abaixo é exibida.



Esse processo é necessário para habilitar os usuários do autenticado do Windows a utilizar o certificado.

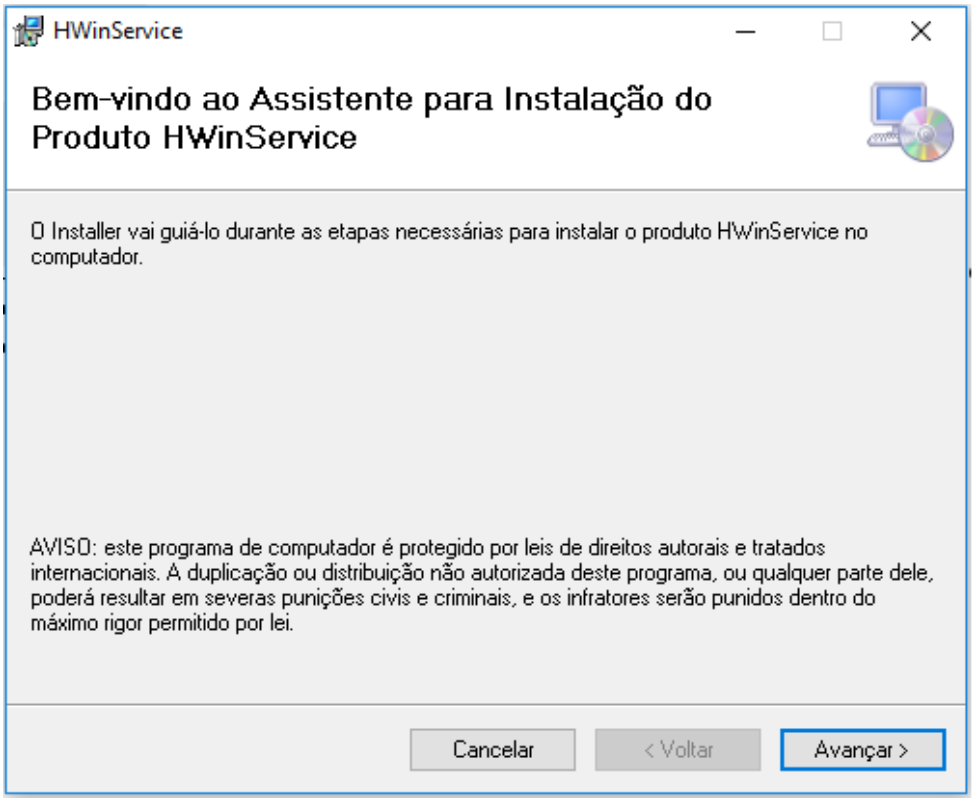
É possível visualizar a lista de usuários já autenticados com o seguinte comando:

winhttpcertcfg.exe -l -c local_machine\TrustedPeople -s " **CN DO SEU CERTIFICADO** "

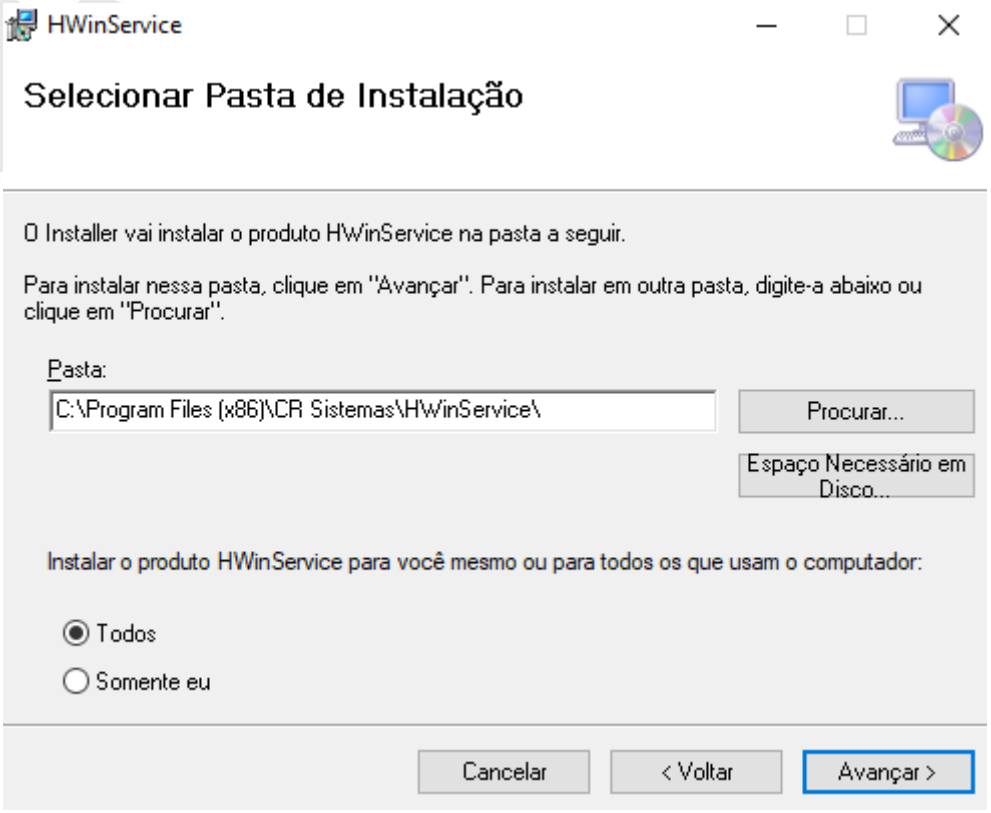
Esse procedimento é apenas para o certificado da empresa, não há necessidade de realizar esse processo para os certificados de raiz v4 e v5 (os mesmos enviados no pacote)

Instalação do HWinService:

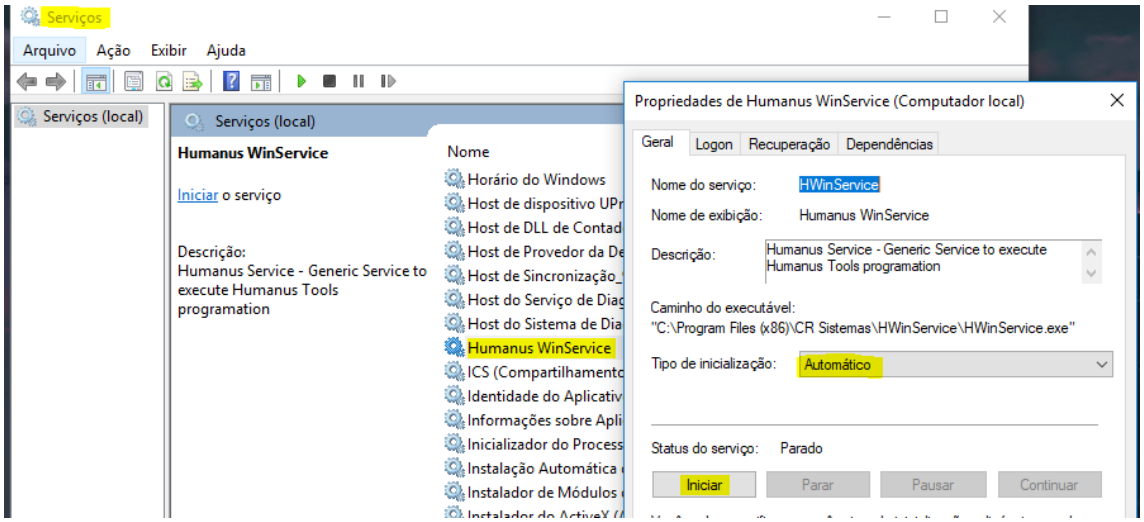
- Executar o arquivo "**HWinService.msi**", escolhendo o local de instalação de sua preferência, lembrando que deve ser um diretório de comum acesso a todos usuários.



No exemplo abaixo, vamos instalar no diretório C:\Program Files (x86)\CR Sistemas\HWinService\



Após a instalação, será criado um serviço da Humanus no Windows, basta inicia-lo conforme a imagem abaixo:



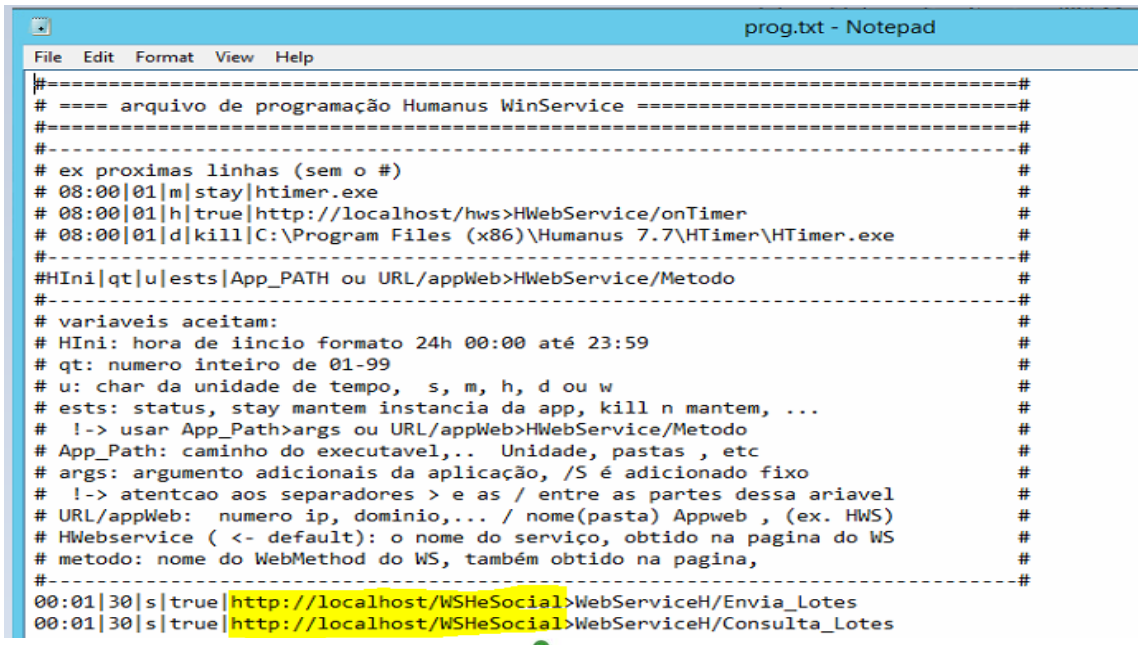
O HWinService possui um arquivo de configuração **prog.txt** que acompanha o setup de instalação, este arquivo deve ser copiado para a pasta de instalação, neste caso, em: “C:\Program Files (x86)\CR Sistemas\HWinService\ “.

Em seguida, nas 2 últimas linhas do arquivo prog.txt, basta configurar o diretório principal da página do Web Service.

1. Abrir a página principal do Web Service e copiar o diretório destacado:



2. Colar o diretório conforme destacado abaixo:



Versão: 4.0
Data: 15/03/2018
Autor: Bruno Oliveira

SISTEMA **HUMANUS**
PARA GESTÃO DE PESSOAS

Humanus

www.humanus.net.br • marketing@humanus.net.br • Rua Hilda Del Nero Bisquolo, 102, 1º andar sala 106 • Tel:. (11) 4583-3232• Jd. Flórida • 13208-703 • Jundiaí - SP
CNPJ: 07.716.820/0001 - 23