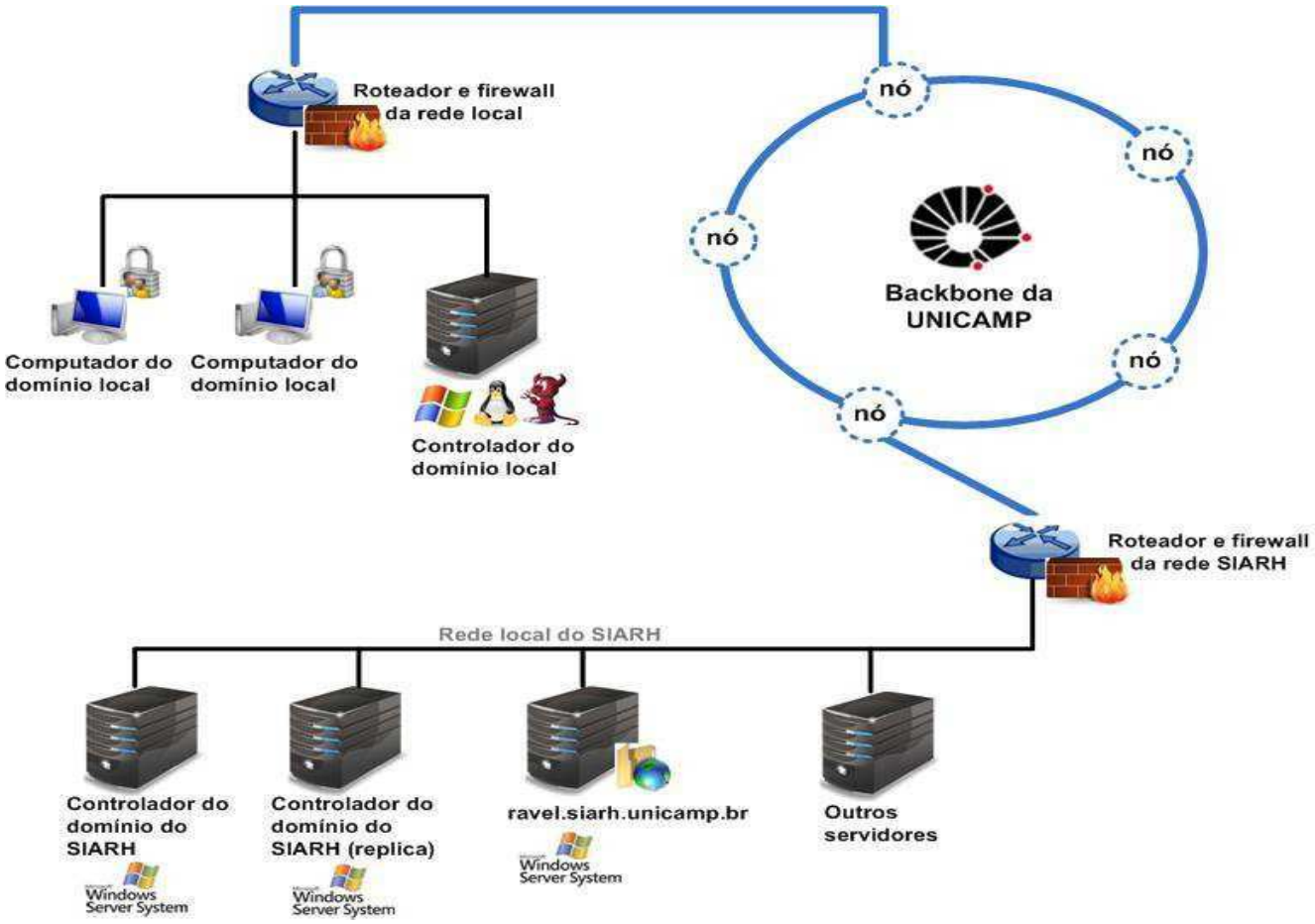
Manual para integração do domínio da rede local à rede corporativa de Recursos Humanos – versão 2.4

Objetivo:

Este manual tem por objetivo fornecer as informações necessárias do procedimento (conceitual e prático) aos administradores das redes locais da universidade que necessitam criar uma **relação de confiança**[i] entre o domínio local e o corporativo da DGRH (**siarh.unicamp.br**).

Este procedimento tem a finalidade de criar um canal de comunicação direta entre a rede local de sua Unidade, visando a instalação da versão **Cliente/Servidor** do software para administração de informações de Recursos Humanos (VETORH® de propriedade da Sênior Sistemas), nas máquinas clientes e responsáveis pelo gerenciamento das informações deste sistema na Unidade.

Esquema gráfico:



Participantes fundamentais do Processo de Interligação e suas funções

1) Representante da Administração de Redes da DGRH

Sua função será auxiliar a Administração de Rede Local nas tarefas de configuração dos filtros de entrada nas redes (*firewall*), criação do grupo global de clientes do sistema de RH na Unidade, estabelecer a senha para criação da Relação de Confiança entre o domínio local (*Windows Server* 2008/2012/2016/2019/2022) com o controlador do AD (*Active Directory*, raiz da floresta[ii]) da rede corporativa da DGRH (denominada SIARH), testar os canais de comunicação e seu funcionamento, instalação do banco *Oracle Client 11g* na estação cliente, instalação do software de Recursos Humanos e testar seu funcionamento.

2) Representante da Administração de Redes Local da Unidade

Sua função é utilizar os principais aspectos nativos do Sistema Operacional envolvido (arquivos, comandos, nomenclaturas, estrutura, serviços e protocolos) e fazer as alterações necessárias no filtro de entrada da rede local (*firewall*). Criar e administrar um grupo global **apenas com os usuários clientes do sistema de RH**, fazer as alterações necessárias nos arquivos do Controlador de Domínio Local, informar o endereço **IP dos Controladores** ao Administrador da DGRH, estabelecer a Relação de Confiança com o Servidor do SIARH através da senha recebida, testar a relação de confiança e os canais estabelecidos com manual recebido da DGRH, instalar o banco *Oracle Client 11g* na estação cliente e configurar seus arquivos, instalar o software para administração de Recursos Humanos (VETORH) no microcomputador do cliente local de RH, aplicar as permissões necessárias para sua execução e certificar que está tudo funcionando.

3) Representante (Usuário) do Sistema de Recursos Humanos

A função do usuário do Sistema de Recursos Humanos é verificar se a instalação foi executada com sucesso pela Administração da rede local, carregando os módulos do software que irá utilizar para a realização de suas tarefas administrativas, preferencialmente acessando todos os módulos, para que não haja dúvidas quanto ao procedimento de instalação.

Tarefas necessárias para integração das Redes Locais com o domínio SIARH

O objetivo agora no documento é apresentar uma seqüência de tarefas que deverão ser seguidas passo-a-passo, facilitando a compreensão das atividades que deverão ser realizadas ao longo do tempo, e em caso de falha pode-se voltar a estas **macro-atividades** para verificação se todas foram cumpridas devidamente.

Passos necessários:

1. Ler todas as instruções deste manual para compreensão da solução e adaptação à sua Unidade
2. Configurar as regras do filtro de entrada da rede local (*firewall*) para permitir a comunicação segura
3. Verificar os registros de DNS do AD local e do domínio do SIARH
4. Criação do Grupo Global no domínio da sua Unidade contendo apenas os clientes autorizados para o uso das ferramentas de sistema de RH
5. Estabelecer a Relação de Confiança unidirecional com o controlador do AD (*Active Directory*) do SIARH
6. Efetuar os testes para certificar que o caminho está ativo e os dados trafegam pelo canal criado entre as redes
7. Instalar o software VETORH e seus módulos da versão Cliente/Servidor no microcomputador local
8. Testar o uso dos módulos

Passo 2

Configurar as regras do filtro de entrada da rede local (firewall)

Todas as Unidades possuem um ponto de acesso à rede da Unicamp, em geral temos uma estrutura parecida, ou seja, um equipamento destinado a receber este sinal e distribuí-lo na rede local, um comutador de pacotes que geralmente possui também a função de filtro de entrada, melhor dizendo *gateway* com *firewall*. Podemos encontrar redes com equipamentos modernos destinados à esta função (roteadores CISCO, *Switches*, etc) mas o caso mais comum na universidade é termos um microcomputador com Sistema Operacional UNIX e suas variantes como FreeBSD, Linux, Solaris ou outros ainda.

Como não seria viável, e nem agradável para leitura, a criação de um documento que abrangesse todos os Sistemas Operacionais utilizados e equipamentos possíveis, partimos para o caso mais comum, ou seja, uma rede que possui um microcomputador com Sistema Operacional **FreeBSD** com a função de *Gateway* e *firewall*. Caso sua Unidade possua uma estrutura diferente podemos tratá-la especialmente, para que as mesmas regras que serão aplicadas no ambiente comum sejam aplicadas ao seu equipamento ou Sistema Operacional.

Observação: Não colocaremos aqui passos já supostamente conhecidos pelos administradores e inerentes a sua função do dia-a-dia, como efetuar *logon* no *Gateway*, usar o editor de textos "vi" ou caminhar na árvore de diretórios.

Começando...

Primeiramente precisamos modificar algumas regras do seu *firewall,* para permitir que os pacotes que sairão da rede corporativa da DGRH cheguem até a estação do cliente, basicamente serão necessárias regras para os pacotes de **Relação de Confiança**, **IPSec** para redes Microsoft e **NetBIOS over TCP** (compartilhamento de arquivos). Utilize o emulador de terminais **SSH** para acessar o **Gateway** da sua rede local, ou se preferir já diretamente ao console.

1) *Logue* no seu Gateway em uma conta com privilégio de "**root**".

2) Vá até o diretório **/etc** e edite o arquivo de firewall, normalmente com nome **rc.firewall**, ou aquele que você utiliza para criar as regras.

3) Nós aconselhamos criar variáveis no arquivo *rc.firewall* para facilitar sua administração, deste modo teremos 3 (três) tipos de variáveis. **Uma** para permitir o acesso aos diretórios compartilhados da servidora de arquivos do Sistema de RH. **Outra** já prevendo o uso de *IPSec*, e **uma última** variável com os endereços IP das servidoras responsáveis pela Relação de Confiança entre os domínios. Opcionalmente criamos uma variável com todas as portas TCP e UDP usadas no processo, com a finalidade de facilitar a manutenção e visualização.

A seguir temos um exemplo da criação das variáveis no arquivo **rc.firewall**.

 # cd /etc

 # vi rc.firewall

```
############
#  Comentários colocados pela Administração da Rede e GCNET
#
############
:…
############
# Flush out the list before we begin.
$fwcmd -f flush
:...
# $fwcmd add 65000 pass all from any to any

    # set these to your outside interface network and netmask and ip
    oif="sua placa para a rede externa (uninet)"
    onet="143.106.X.A"
    omask="255.255.255.224"     # Depende da mascara da Uninet
    oip="143.106.X.B"

    # Configuracoes para a rede da Unidade
    iif="sua placa para a rede interna"
    inet="143.106.X.yyy"
    iip="143.106.X.zzz"
    imask="255.255.255.128"    # A máscara da rede é sua definição

# Prototype setups.
if [ "${firewall_type}" = "open" -o "${firewall_type}" = "OPEN" ]; then
       $fwcmd add 65000 pass all from any to any
elif [ "${firewall_type}" = "simple" ]; then
    # A partir daqui você pode definir suas variáveis

    # set these to your networks (Identificação das suas redes e subredes)
    inets="143.106.xxx.0/25 143.106.xxx.128/25"

    :… mais a diante...

        ######################################################################
        # Maquinas de Arquivos do Sistema de RH no Ambiente Corporativo,
        # portas 135-139
        #
        ip_netbios_corp="143.106.119.0/25{5}"

        ######################################################################
        # Maquinas da Rede Corporativa da DGRH que respondem IPSEC
        # portas 445 (tcp) e 500 (udp)
        #
        ip_ipsec="143.106.119.0/25{7,9,10,18}"

        ######################################################################
        # IPs para estabelecimento da relacao de confianca da rede da Local
        # com a rede corporativa da DGRH (controlador de domínio W2k3/2k8)
        #
        ip_trust="143.106.119.0/25{7,9,10,18}"

        ######################################################################
        # Variaveis com o range de portas utilizadas na conexao dos
        # cliente do sistema de RH (via cliente/servidor) nas maquinas
        # que fornecem o acesso ao diretorio de arquivos
        #
        wsptcp="88,135-139,389,445,1025"          # mean: Windows Shared Ports TCP
        wspudp="88,135-139,389,445,500,1025"      # mean: Windows Shared Ports UDP
    :...
```

Mais adiante, no trecho das estruturas para a criação das regras...

```
  ....
################################################################################
# Conexão do Sistema para os Servidores de Arquivos (Máquinas Clientes da Rede Local)
# Substitua "a.b" pelos IPs das suas máquinas Clientes e Servidores Locais (PDC)
# ou pode liberar o acesso para todo a range de sua rede, substitua "a.b" por
# "a.0/sua_máscara_de_rede", exemplo : "aaa.0/26" para mascara de rede "255.192"
#
for vip in ${ip_netbios_corp}; do
    $fwcmd add pass log tcp from ${vip} to 143.106.a.b/xx ${wsptcp} in via ${oif} setup
    $fwcmd add pass log udp from ${vip} to 143.106.a.b/xx ${wspudp} in via ${oif}
done

################################################################################
# Regra que permite conexões em IPsec com as servidoras do Sistema de Recursos
# Humanos.
# Substitua "a.b" pelos IPs das suas máquinas Clientes e Servidores
# Ou pode liberar o acesso para todo a range de sua rede, substitua "a.b" por
# "aaa.0/sua_máscara_de_rede", exemplo : "aaa.0/26" para mascara de rede "255.192"
#
for vip in ${ip_ipsec}; do
    ${fwcmd} add pass log tcp from ${vip} to 143.106.a.b/xx ${wsptcp} in via ${oif} setup
    ${fwcmd} add pass log udp from ${vip} to 143.106.a.b/xx ${wspudp} in via ${oif}
done

################################################################################
# Permite a passagem para estabelecimento do relacionamento de confiança
# com domínio SIARH na rede DGRHCorp
# substitua "xxx.yyy" pelo IP do seu controlado de domínio primário (PDC)
#
################################################################################
# Permite a passagem para estabelecimento do relacionamento com dominio
# SIARH no rede RHCorp, com os IPs dos controladores de dominio da DGRH,
# listados na variavel ip_adrcsrvs.
#
ip_adrcsrvs="143.106.xxx.yyy/XX{a,b,c}"    # IPs dos controladores

for vip in ${ip_trust}; do
    $fwcmd add pass log esp from ${vip} to ${ip_adrcsrvs} in via ${oif}
    $fwcmd add pass log tcp from ${vip} ${wsptcp} to ${ip_adrcsrvs} in via ${oif} setup
    $fwcmd add pass log udp from ${vip} ${wspudp} to ${ip_adrcsrvs} in via ${oif}
    $fwcmd add pass log tcp from ${vip} ${hp} to ${ip_adrcsrvs} ${hp} in via ${oif} setup
done
```

4) Grave este arquivo e execute o comando para colocar as regras ativas. Exemplo:

 # sleep 15 ; sh /etc/rc.firewall >/tmp/saida.txt &

5) Verifique se as regras estão ativas, olhando o arquivo de saída gerado ou mesmo listando as regras que estão no ar.

 # ipfw list | grep 143.106.119. (por exemplo!!!)

```
26810 allow esp from 143.106.119.9 to 143.106.a.b/XX in recv de0
26910 allow tcp from 143.106.119.9 88 to 143.106.a.b/XX in recv de0
27010 allow tcp from 143.106.119.9 445 to 143.106.a.b/XX in recv de0
#
```

Após este procedimento o *firewall* da sua Unidade já está de configurado o caminho para a Administração de Rede Local possa configurar os arquivos do PDC e também criar a relação de confiança com o domínio do SIARH (siarh.unicamp.br).

Passo 3

Verificação dos registros SRV do domínio local e do domínio do SIARH

Este passo é de suma importância (para não dizer fundamental) para o sucesso do estabelecimento da relação de confiança, pois todos os registros e funcionamento do AD dependem da correta informação no DNS, ou seja, qualquer problema neste serviço ou na comunicação deste, impede a troca de informações entre os domínios. Sendo assim precisamos antes testar se todos os registros do tipo SRV constam no DNS e são exportados para fora de seu domínio para consulta.

Isso é necessário porque o mecanismo de estabelecimento da RC é feito via FQDN (f*ully qualified domain name*) permitindo que os domínios possam ser geridos internamente, sem a necessidade ou perda da RC quando da mudança na Unidade de um servidor do AD ou na rede Corporativa da DGRH.

Portanto vamos consultar primeiro se os registros SRV estão corretos e publicados. Vamos usar as ferramentas de consulta existentes e conhecidas pelos administradores o NSLOOKUP ou DIG. Para não prolongar este manual padronizaremos as consultas com NSLOOKUP, mas as mesmas funcionam com o DIG (feitos os devidos ajustes no comando para adaptar aos tipos de parâmetros usados neste executável).

1) Consultando os registros SRV do domínio do SIARH:

```
C:\Users\roque.DGRH>nslookup -type=SRV _ldap._tcp.dc._msdcs.siarh.unicamp.br
Servidor:  intrh.dgrh.unicamp.br
Address:  143.106.149.79
Não é resposta de autorização:
_ldap._tcp.dc._msdcs.siarh.unicamp.br    SRV service location:
          priority       = 0
          weight         = 100
          port           = 389
          svr hostname   = rossini.siarh.unicamp.br
_ldap._tcp.dc._msdcs.siarh.unicamp.br    SRV service location:
          priority       = 0
          weight         = 100
          port           = 389
          svr hostname   = vivaldi.siarh.unicamp.br
_ldap._tcp.dc._msdcs.siarh.unicamp.br    SRV service location:
          priority       = 0
          weight         = 100
          port           = 389
          svr hostname   = lebrun.siarh.unicamp.br
_ldap._tcp.dc._msdcs.siarh.unicamp.br    SRV service location:
          priority       = 0
          weight         = 100
          port           = 389
```

Veja que o DNS local respondeu que conhece as informações do registro SRV do domínio SIARH e localizou 4 máquinas que possuem o catálogo global do AD do SIARH. Essa resposta é muito importante, pois demonstra que sua rede local consegue localizar os controladores apenas pela busca no DNS.

Faça a mesma consulta para o seu domínio para aferir se os seus registros SRV constam no DNS, exemplo:

```
C:\Users\curti.DGRH>nslookup -type=SRV _ldap._tcp.dc._msdcs.dgrh.unicamp.br
```

Estou consultando os registros SRV do domínio da DGRH e a resposta deve ser algo como a anterior.

Caso não obtenha estas respostas você pode estar com problemas em seu DNS, por favor verifique junto ao pessoal do CCUEC (mantenedores do domínio unicamp.br) quais as medidas a serem tomadas para esta correção, pois lembre-se, apenas se os registros estiverem 100% corretos a RC poderá ser feita, portanto só passe adiante se isso estiver resolvido.

Passo 4

Criação do Grupo Global no domínio da sua Unidade contendo apenas os clientes autorizados para o uso das ferramentas de sistema de RH

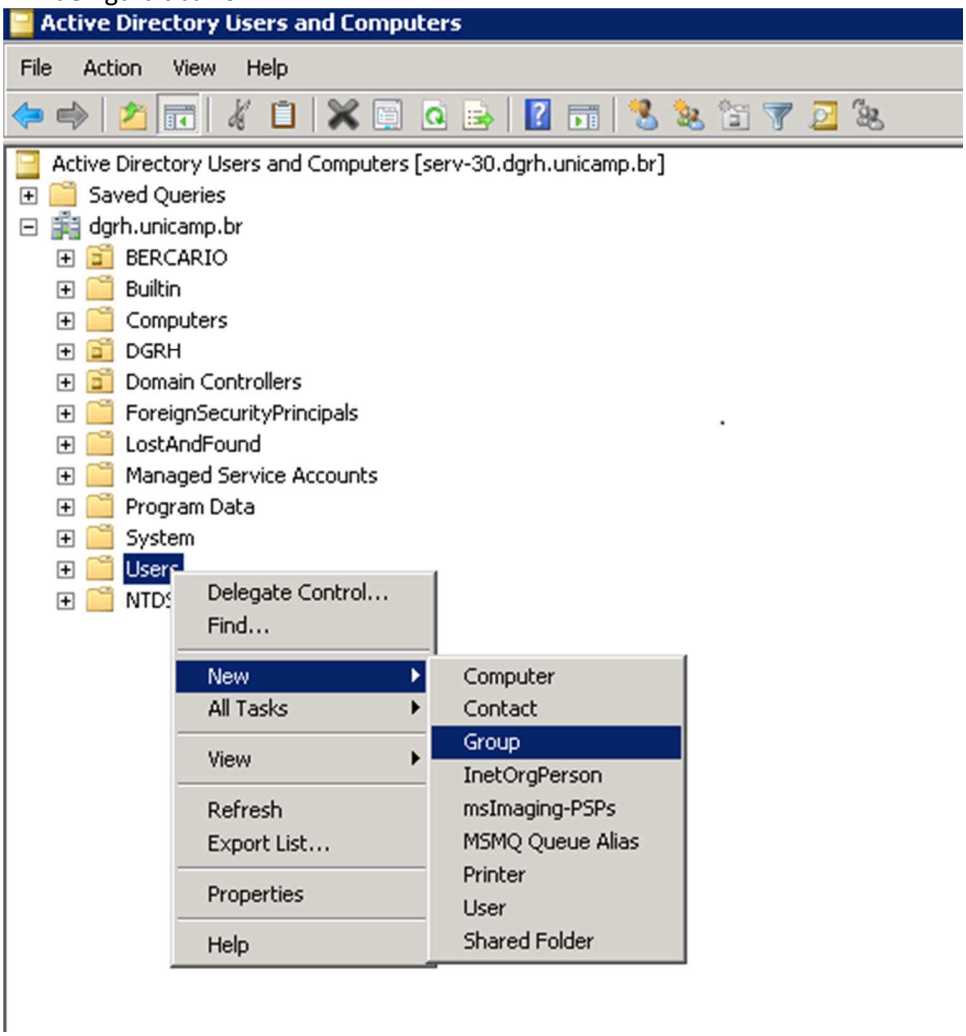
Neste próximo passo, contaremos com a habilidade do Administrador Local para criar um **Grupo Global** denominado **RHSIS-NOME_DA_SUA_UNIDADE**, por exemplo **RHSIS-CAISM**.

Os passos são os seguintes:

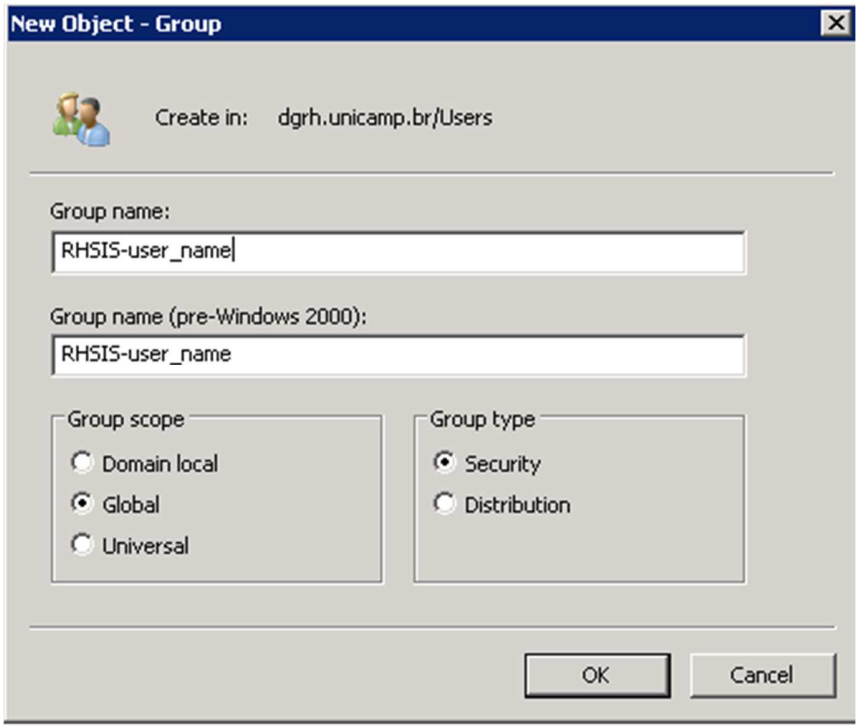
1) *Logue* em um de seus controladores do domínio com uma conta com privilégios de administrador do sistema de contas.

2) Em seguida clique sobre o botão "***Start***", vá até o item chamado "***Programs***", nele escolha a opção "***Administrative Tools***" e finalmente a opção "***Active Directory Users and Computers***".

Abra a lista do seu domínio local e clique na aba "***Users***", em seguida "***New***" e finalmente "***Group***", vide figura abaixo:

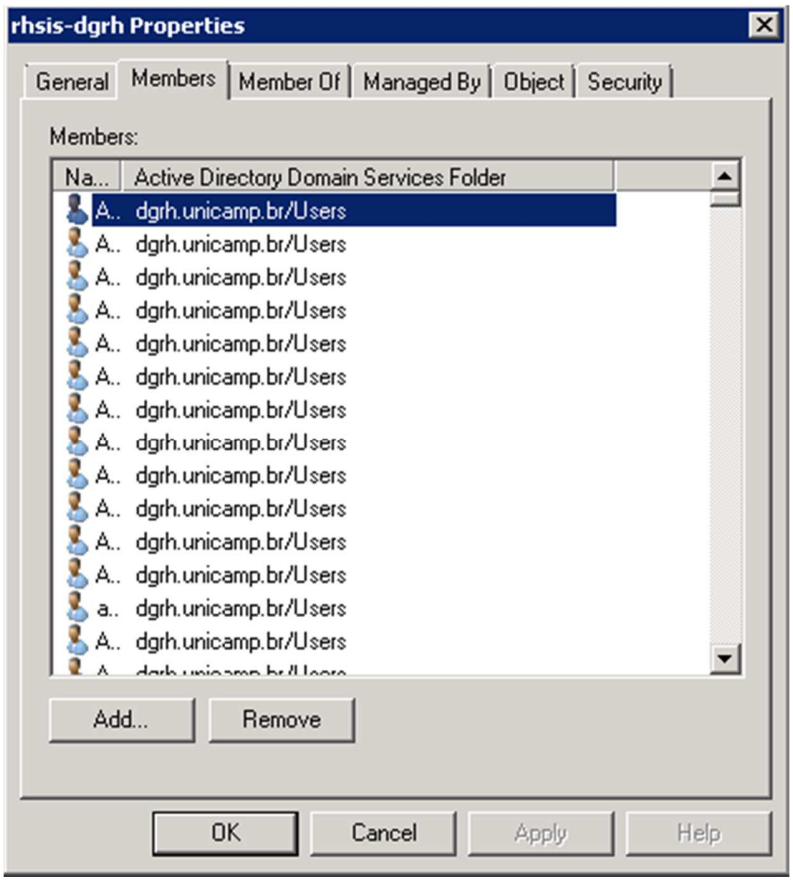


Você verá a janela aberta solicitando o nome do novo grupo e suas características, preencha conforme a tela a seguir, substituindo o texto "*sua_unidade*" pelo nome abreviado da sua unidade, exemplo: **RHSIS-CAISM** ou **RHSIS-REIT**.



Mantenha o escopo do grupo como '***Global***' e a segurança como '***Security***'. Em seguida '**Ok**' para confirmar a criação.

Após isso o grupo está criado. Basta agora adicionar os usuários do sistema de RH que farão o acesso ao servidor da DGRH neste grupo. Para isso continue na mesma janela e localize o grupo criado, clique com o botão direito na opção '**Propriedades**' em seguida na aba '**Members**' e use o botão '**Add**' para adicionar seus usuários.



Após a criação do grupo é necessário a criação de um usuário local no domínio da Unidade para o SIARH de forma que o administrador do SIARH possa usá-lo para fechar e testar a relação de confiança. ***Isso será feito com instruções trocadas através de mails, por uma questão de segurança.***

Passo 5

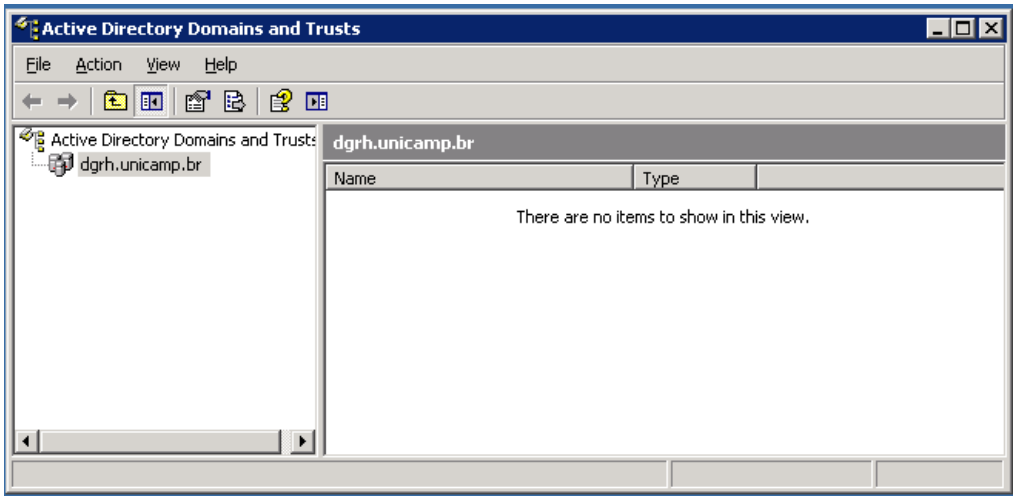
Estabelecer a Relação de Confiança unidirecional com o controlador do AD (*Active Directory*) do SIARH

Agora que temos a certeza que os registros SRV estão ok, tanto do domínio siarh.unicamp.br, quanto o seu local, poderemos **criar o seu lado** da RC, veja que a RC será unidirecional, isso significa que apenas o domínio siarh confiará em seus usuários, em outras palavras, ***nós confiaremos no seu domínio e daremos permissão para que acessem nosso servidor com a autenticação da rede local***. Isso implica que o administrador deve ser criterioso na colocação e retirada dos usuários quando de sua saída da Unidade, ou seja, ***a manutenção deste grupo é fundamental para a sua segurança, pois todos os acessos e ações no sistema são monitorados e armazenados em logs.***

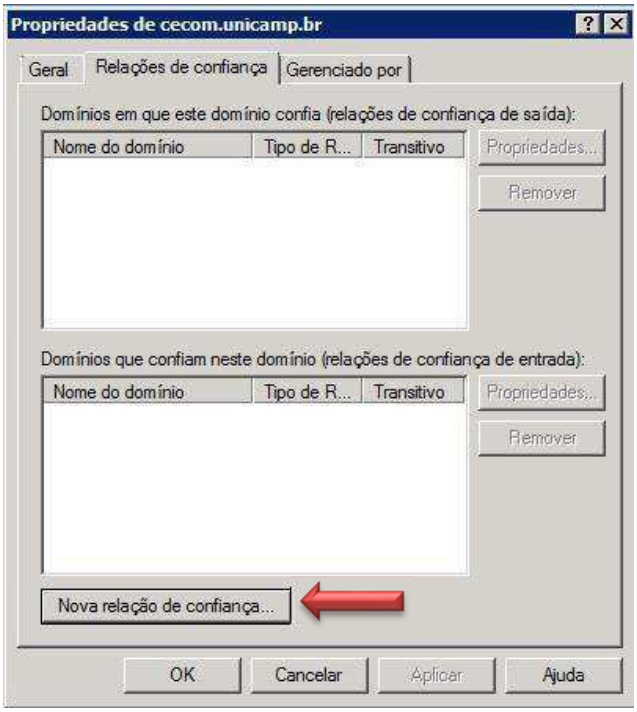
Criando a RC no domínio local para o siarh:

As telas a seguir foram feitas com um servidor Windows 2008 R2, mas servem também para servidores que estão com outras versões do Windows Server (*caso precisem nos avisem que encaminharemos as telas do passo-a-passo*). Portanto siga as seguintes etapas:

Acesse a ferramenta "**Active Directory Domains and Trusts**"



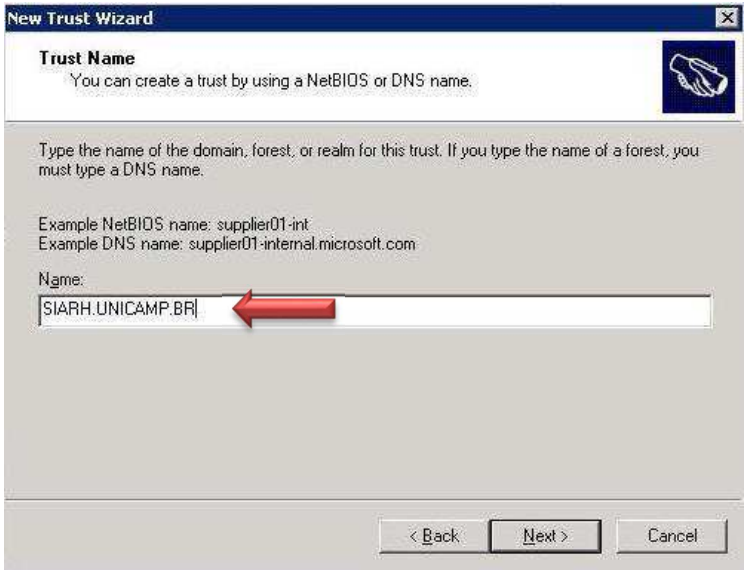
Clique com o botão direito sobre o seu domínio para acessar a opção '**Propriedades**', em seguida clique na aba '**Trust Relationship**'. Você receberá a janela conforme exposto na próxima figura.



Clique no botão '**New Trust Relationship**' e você será direcionado para um auxiliar de criação da RC.

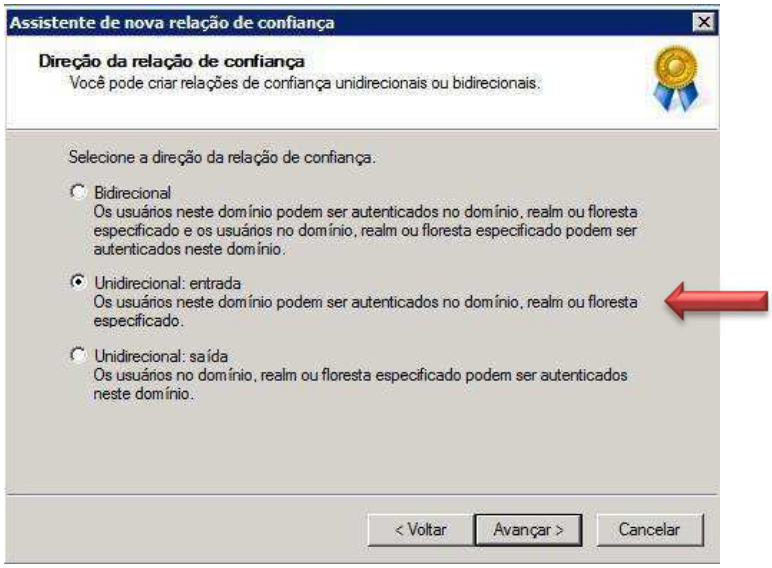
Em seguida preencha os campos solicitados conforme a sequencia:

Clique em '***Next***'.

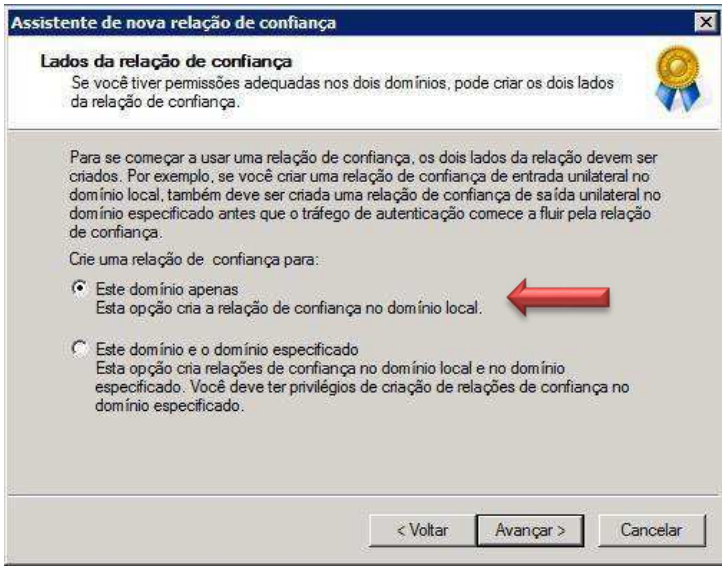


Insira o nome completo do domínio do siarh para a localização dos controladores do AD via DNS. No nosso caso o campo deve ser preenchido com '***siarh.unicamp.br***'.

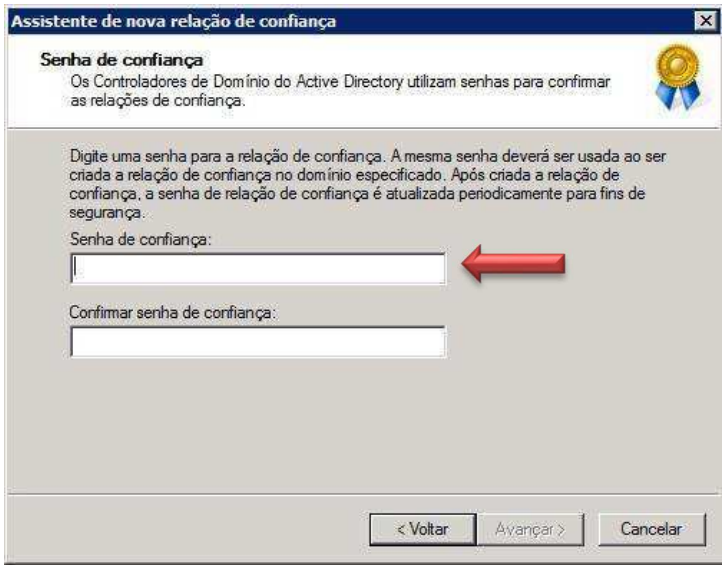
Escolha a RC como tipo '***External Trust'***.



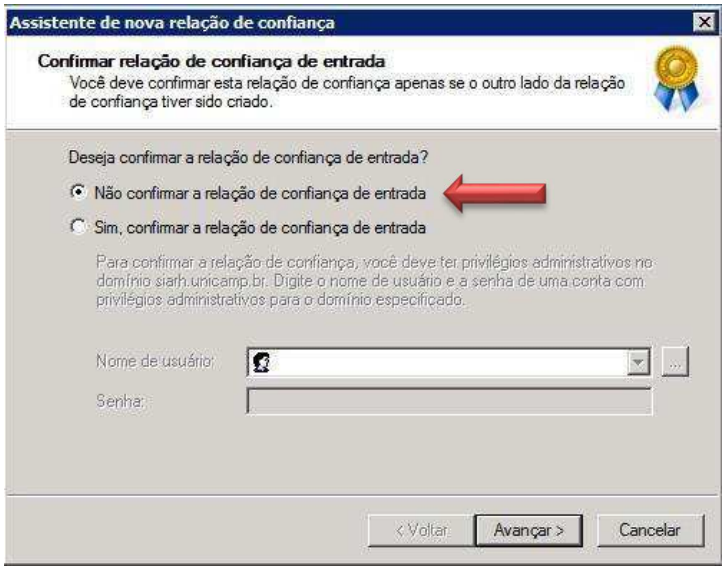
Definia a RC como **unidirecional de entrada**.



Defina que a RC ocorrerá com apenas o seu domínio principal, caso você tenha outros subdomínios.

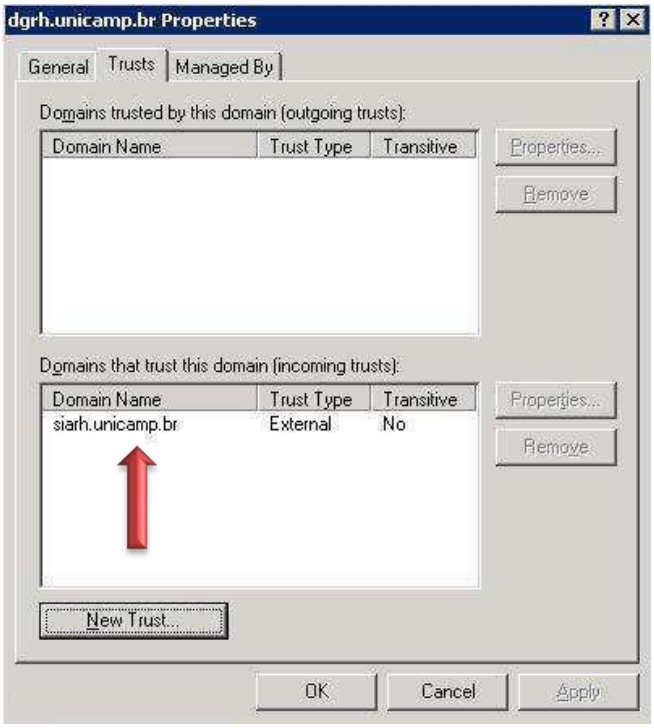


Insira a senha trocada com o administrador da DGRH para realizar a RC.



Se tudo ocorrer bem, ele irá solicitar a criação da RC também no domínio do SIARH, neste caso não é necessário, pois o administrador da DGRH é quem fará esta tarefa.

Pronto. Se conseguir incluir a RC no seu domínio a sua janela de RC deverá estar deste modo:



Ok, sendo assim o seu lado da RC está pronto, basta apenas que o lado do SIARH esteja completo, por isso é importante manter o contato com o administrador da DGRH para certificar se isso foi feito.

Passo 6

Efetuar os testes para certificar que o caminho está ativo e os dados trafegam pelo canal criado entre as redes

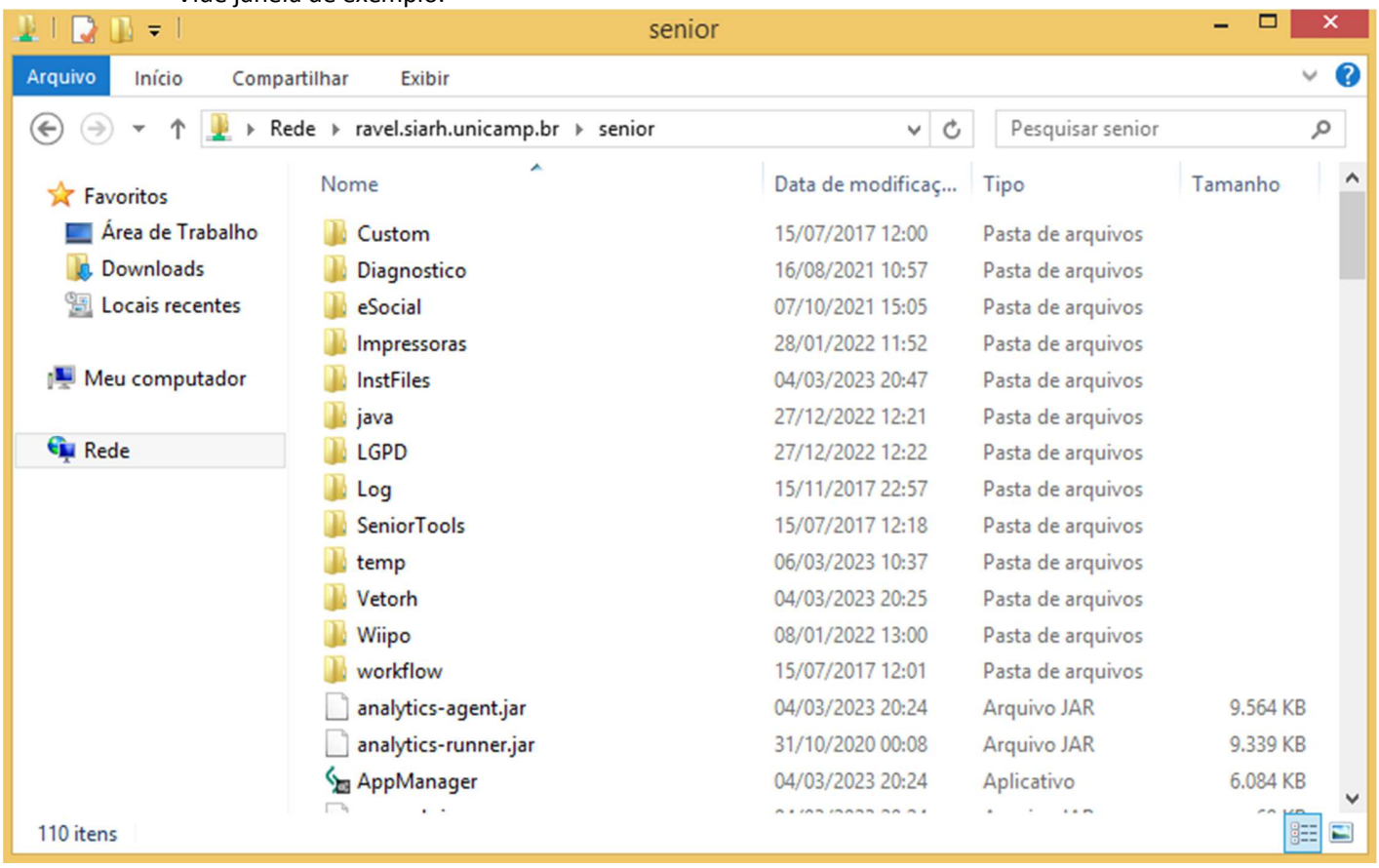
O teste do caminho ocorre de forma simples, será necessário certifica-se de que o usuário autenticado no microcomputador com Windows Profissional possui os privilégios necessários para instalação de software localmente, em geral pedimos que a conta usada neste momento seja do administrador do domínio.

Detalhe importante, o usuário administrador do domínio, além dos usuários locais do sistema de RH, deve constar no grupo criado no passo 4 a fim de permitir o acesso ao servidor remoto da DGRH. Caso contrário receberá uma mensagem de erro e solicitação de autenticação no domínio do SIARH.

O teste é feito verificando se você consegue conectar-se e acessar os arquivos do sistema. Um dos meios é através da janela de gerenciamento de arquivos do Windows o '**Windows Explorer**', verifique se consegue ler os arquivos do seguinte endereço de rede:

\\ravel.siarh.unicamp.br\senior

Vide janela de exemplo:



Se verificar uma janela como está o acesso está Ok

Passo 7

Instalar o software VETORH e seus módulos da versão Cliente/Servidor do microcomputador local

O procedimento de instalação ocorre em algumas fases, que são:

- Conexão com o servidor do **SIARH** (*Sistema Integrado de Administração de Recursos Humanos*), onde está localizado o arquivo de instalação do sistema;
- Execução do binário de instalação;
- Escolha das opções de armazenamento dos arquivos do VETORH e módulos usados pela equipe local de RH;
- Copia dos arquivos dos módulos escolhidos para a máquina local;
- Finalização do programa;

Procedimentos passo-a-passo:

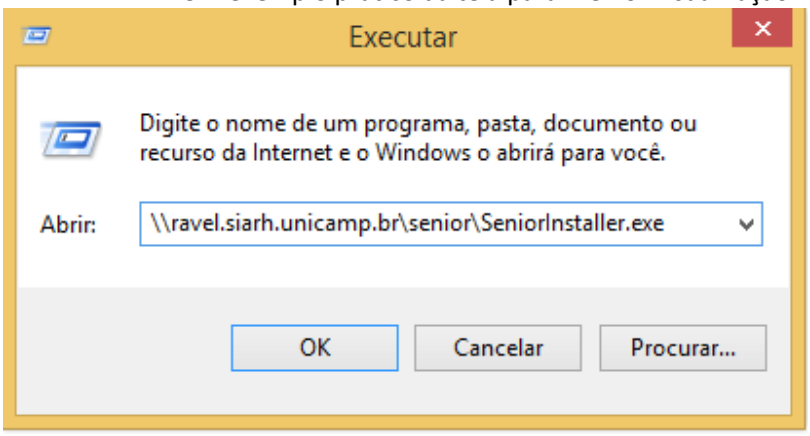
Inicialmente precisamos estabelecer uma conexão com o servidor com os arquivos de instalação do sistema, você pode fazer de várias maneiras, mas o importante é lembrar que o usuário que está autenticado (*logado*) na máquina local deve possuir privilégios de administrador para instalar o programa e realizar a inclusão e modificação de arquivos no sistema operacional da máquina.

Deste modo usamos para exemplificar o comando de execução de tarefas do Windows com as teclas "***Windows + R***" , mas você pode usar qualquer gerenciador de arquivos para indicar o caminho ao servidor, como o *Windows Explorer* e até mesmo um navegador internet.

Após chamado o comando de execução de tarefas, precisamos digitar na linha de comando o seguinte caminho:

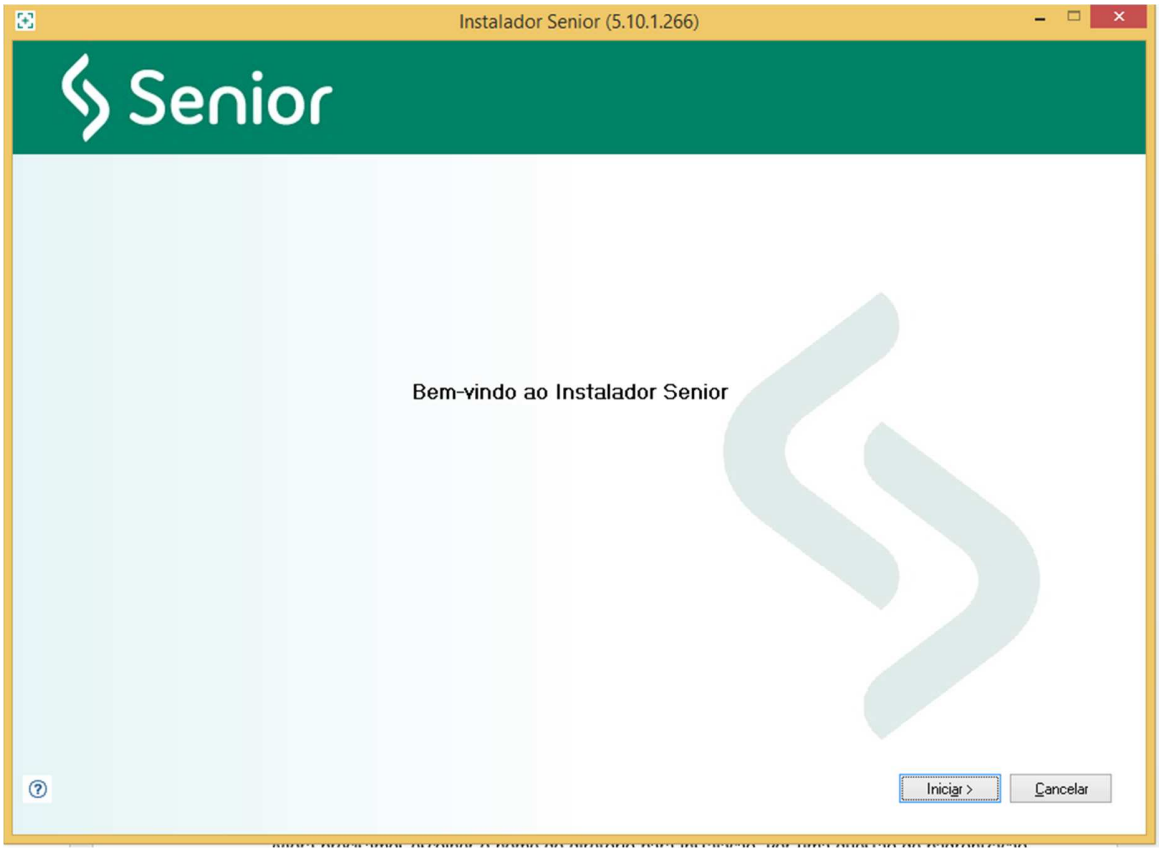
\\ravel.siarh.unicamp.br\senior\SeniorInstaller.exe

Um exemplo prático da tela para melhor visualização:



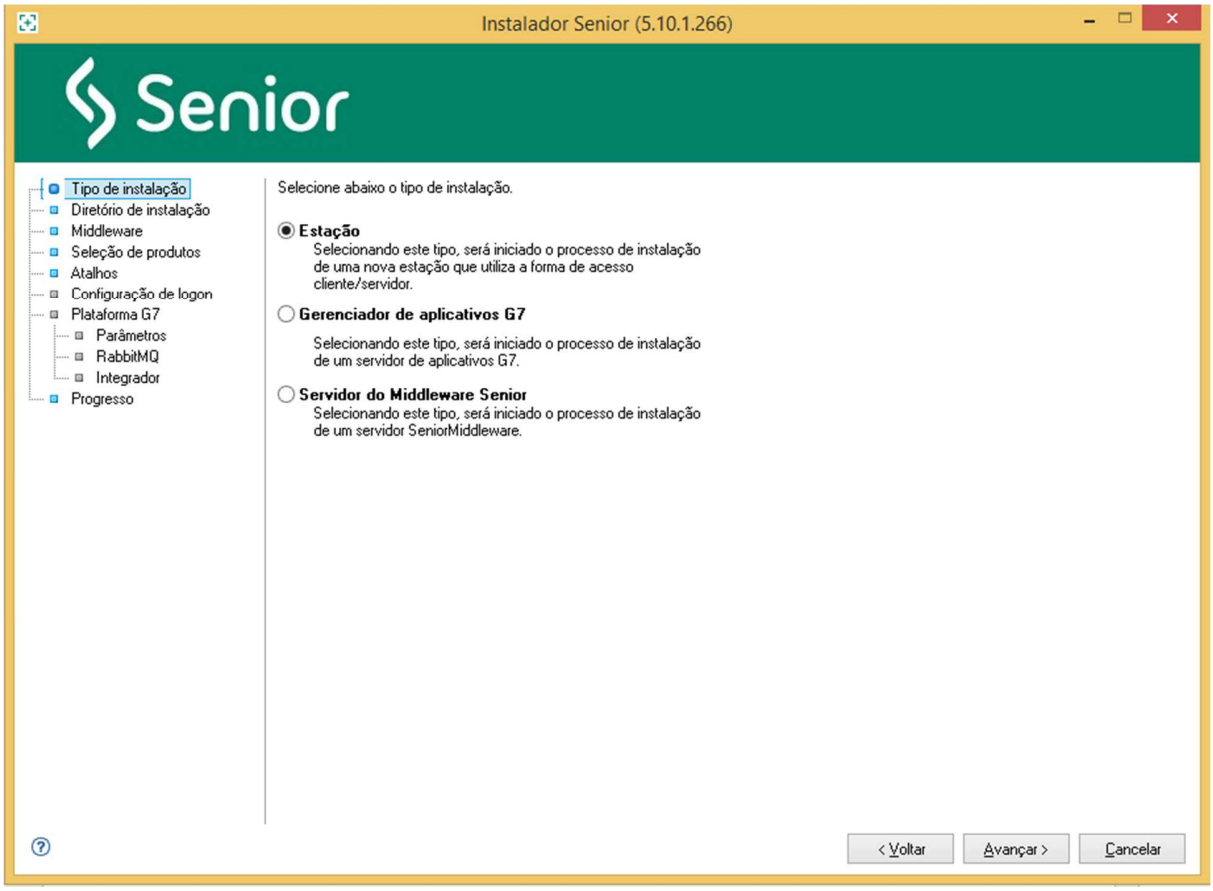
Clique em "Ok" para prosseguir.

Você será apresentado ao guia de instalação com a seguinte janela:



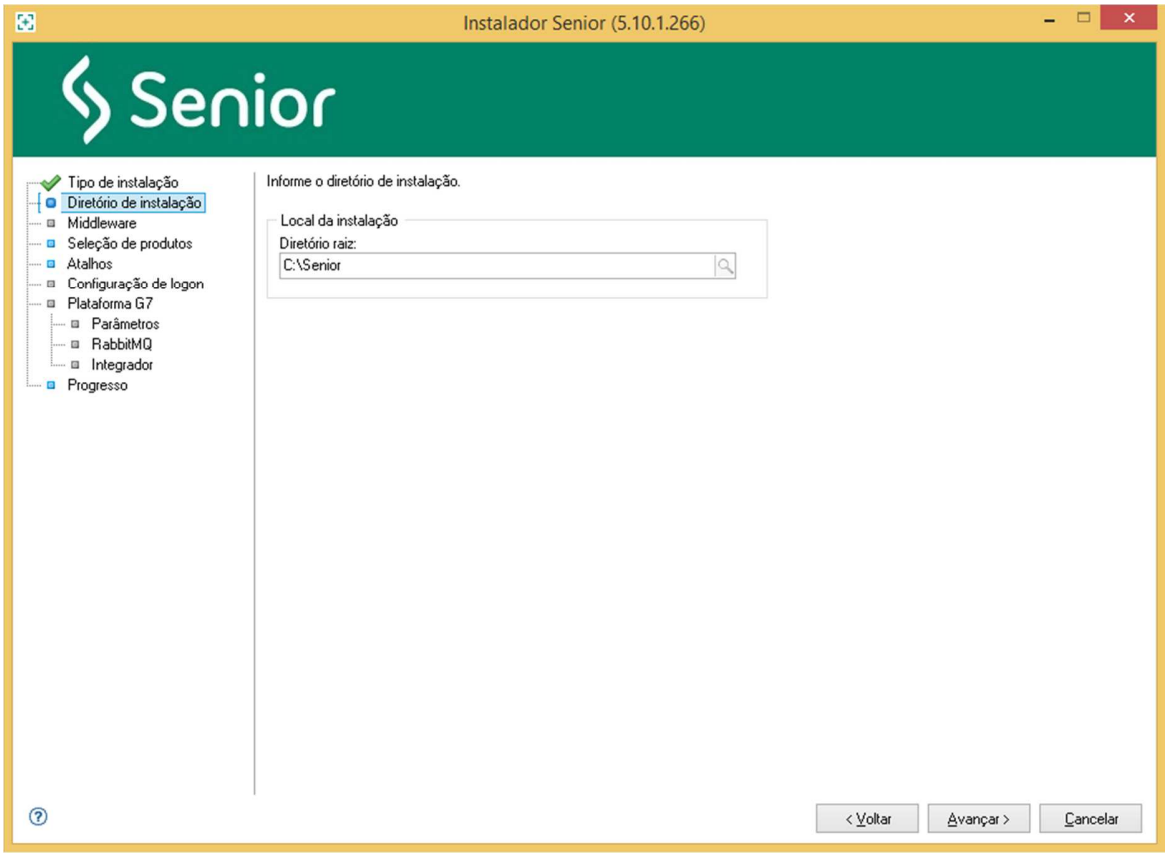
Clique em "**Iniciar**" para começar o processo de escolha dos locais de armazenamento dos arquivos do software e os módulos que serão instalados em sua Unidade.

Seguimos a sequencia, agora com um guia mais amigável.

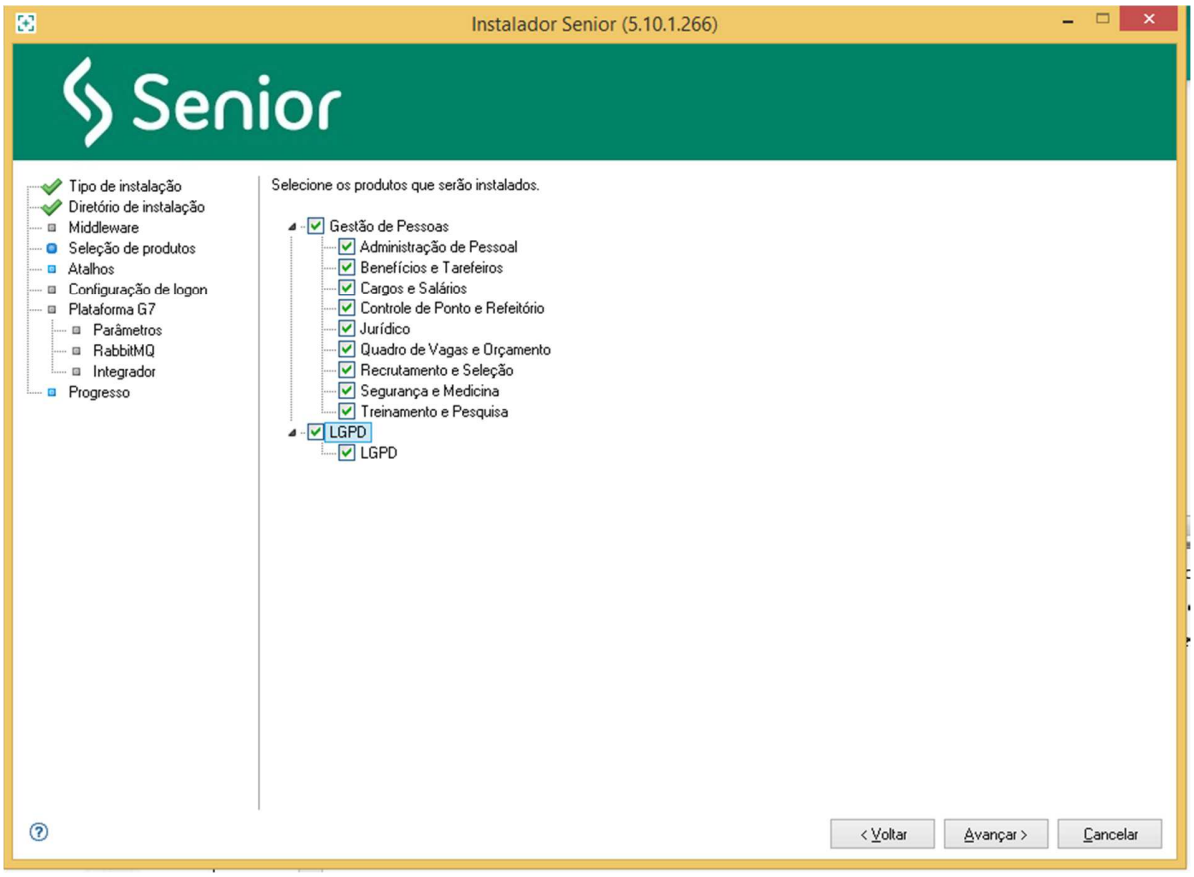


Para os usuários do sistema local, a opção não deve ser alterada, ou seja, a instalação padrão é a opção "**Estação**". Após a escolha será marcado um "verificado" em verde (✔), demostrando que o passo já foi realizado e está Ok.

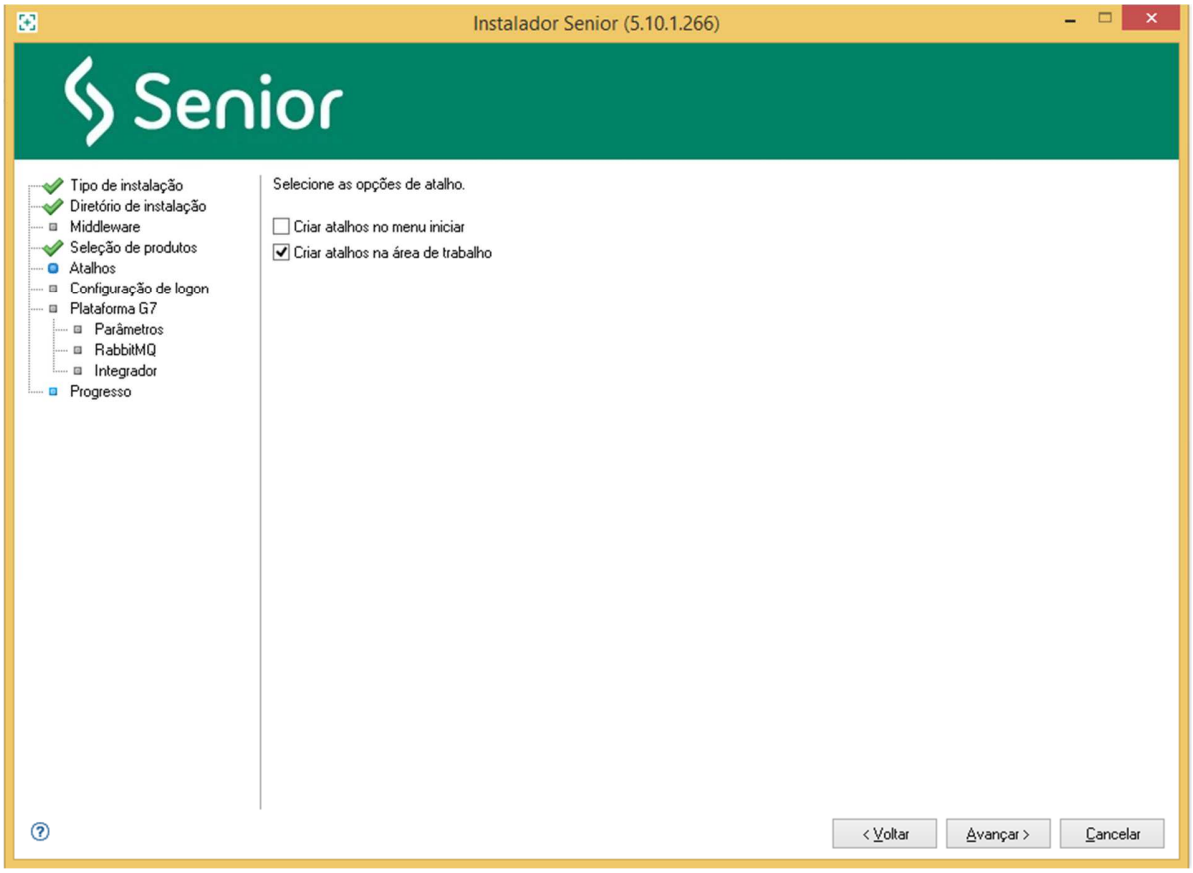
Agora precisamos escolher o nome do diretório para instalação. Por uma questão de padronização, deixe o nome da parta como "**C:\Senior**", pois em caso de alteração, eventuais problemas e alguns atendimentos poderão ser mais demorados, se o administrador não informar que o nome do local é diferente.



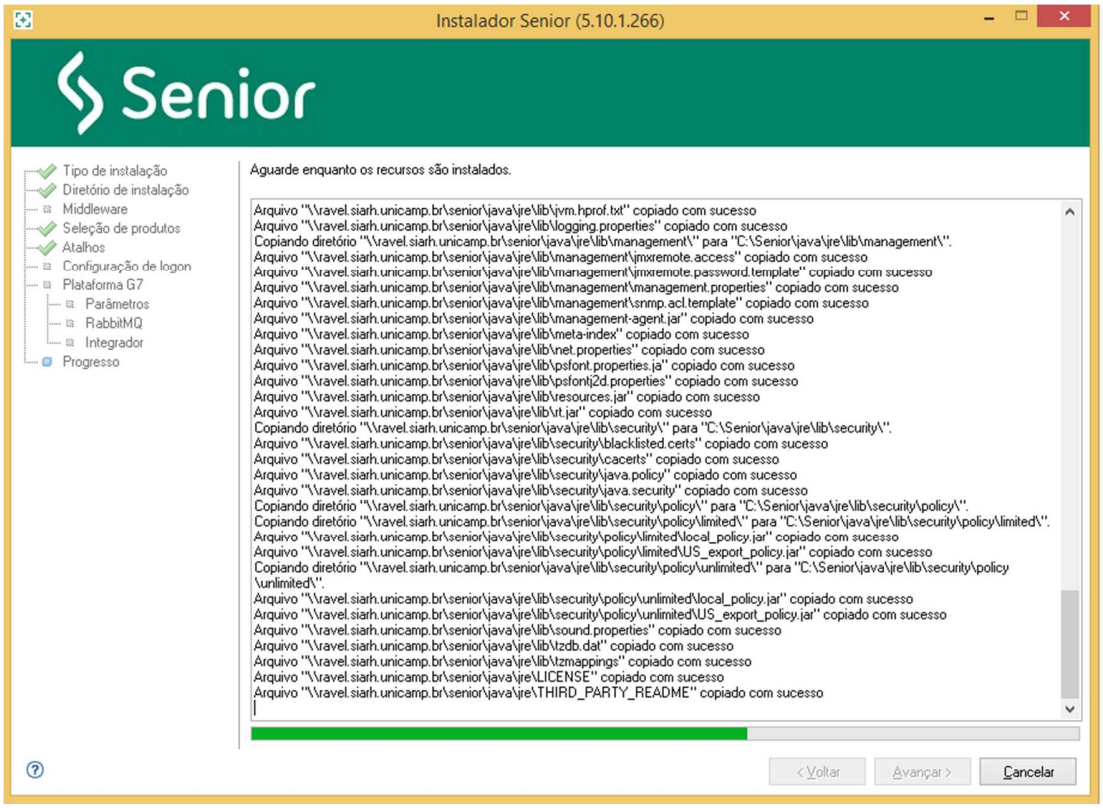
Vamos avançar. O próximo passo é a escolha dos produtos que serão instalados, marque as opções que o seu usuário utiliza. Neste nosso exemplo marcamos a instalação de todos eles, veja na janela abaixo.



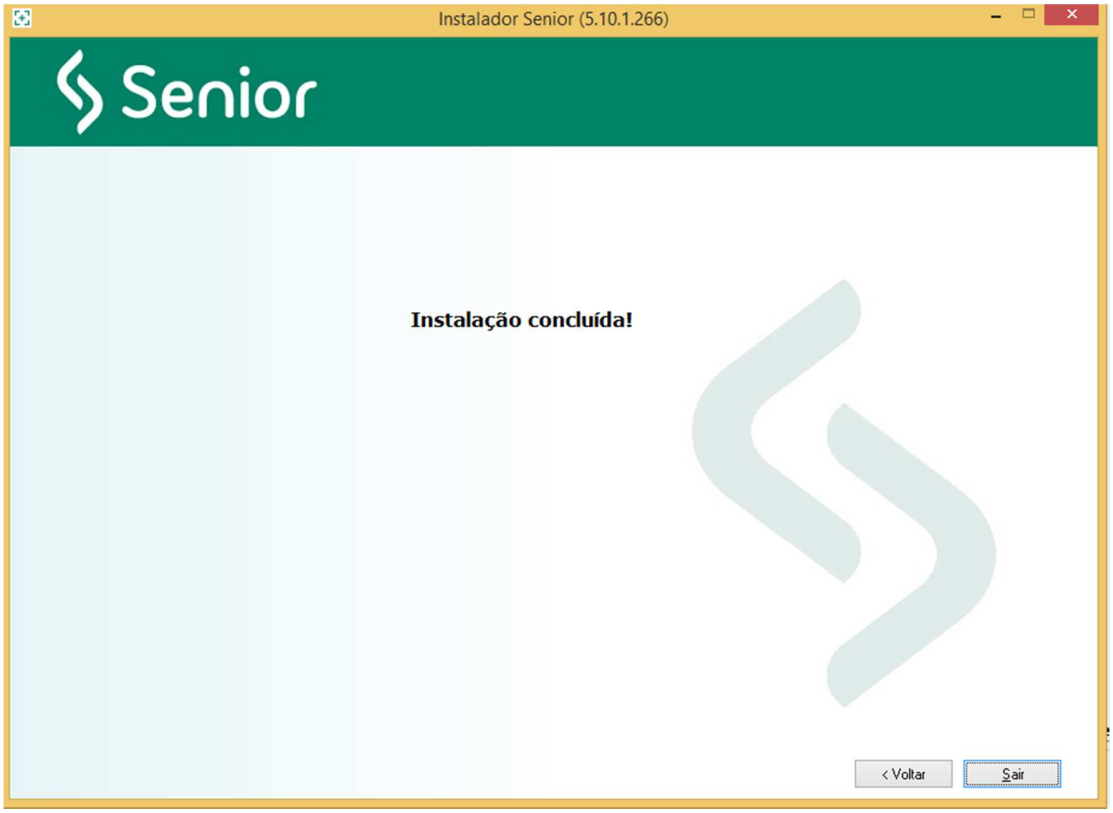
Após clicar no botão “Avançar”, precisamos escolher finalmente se vamos criar apenas os atalhos na área de trabalho e/ou o item no *menu* Iniciar. ***Aconselhamos que seja escolhida apenas a opção de criar atalhos na área de trabalho, pois o produto não cria uma entrada na lista de programas instalados no painel de controle do Windows.***



Após escolhidas todas as opções, clique em "**Instalar**" para iniciar o processo de cópia.



Após isso, a mensagem final de conclusão.



Testes de execução dos módulos:

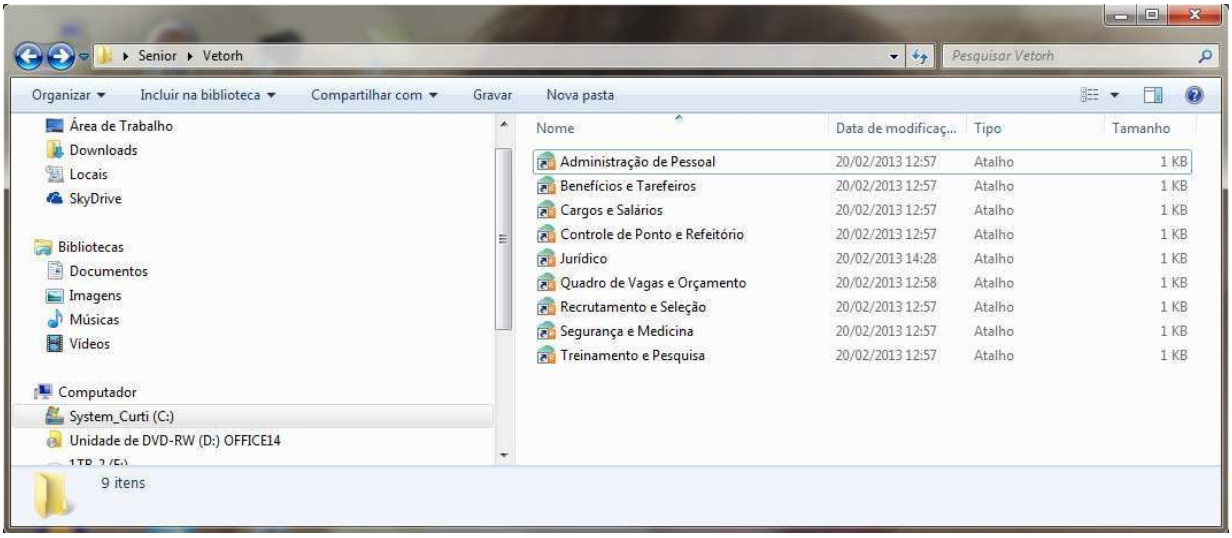
Após a instalação você perceberá que o ícone para acesso ao sistema foi modificado, antes tínhamos na área de trabalho uma pasta chamada "**Sênior Sistemas**" com os módulos diretamente apresentados. Na nova versão é criada na área de trabalho uma nova pasta chamada apenas de "**Sênior**", dentro dela temos o produto licenciado para a Unicamp que é o **VETORH**.

Antes, 

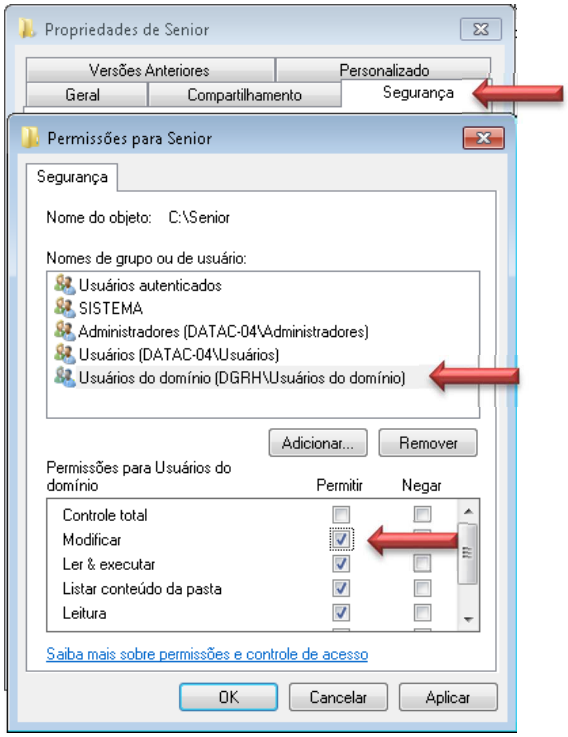
agora, 

.

Para executar um dos módulos, abrimos a pasta "**Sênior**" e temos a seguinte janela:



Antes de iniciar a execução do módulo verifique se **a conta do usuário de RH** possui privilégios de modificação de arquivos (aba de segurança) no diretório **c:\senior**, pois a cada nova atualização dos módulos os arquivos serão copiados automaticamente, como já ocorre atualmente.



Aplique as permissões para que tenham efeito. Agora você pode voltar à pasta da área de trabalho para que possa escolher o módulo que deseja executar.

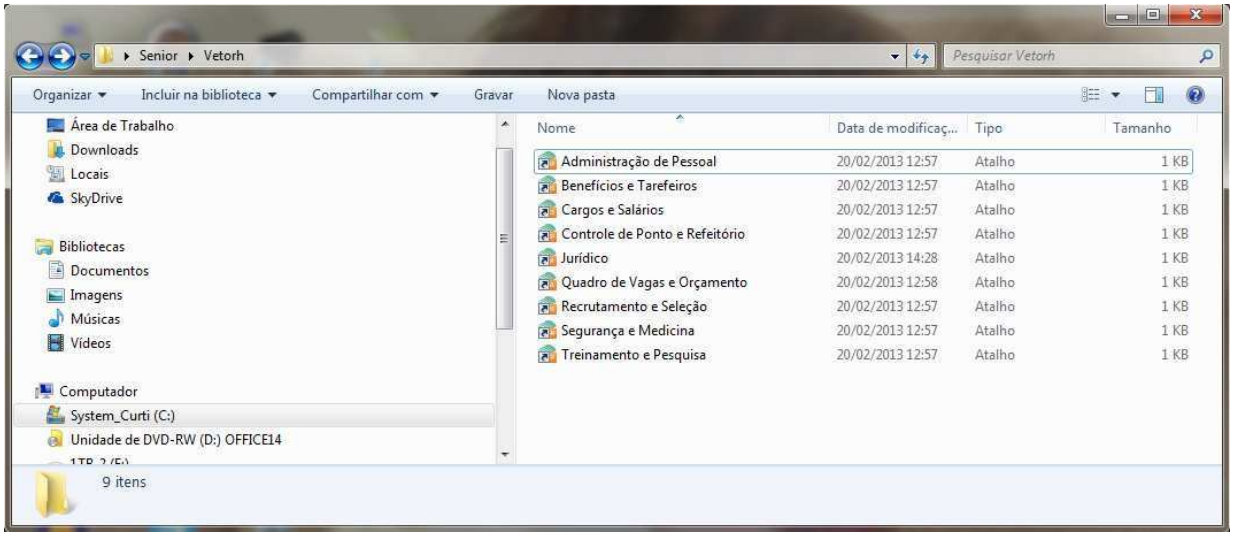
Uma vez que o usuário de RH local executou o sistema e chegou até este ponto, temos a garantia que toda a parte de configuração da rede e instalação foi executada com sucesso.

Passo 8

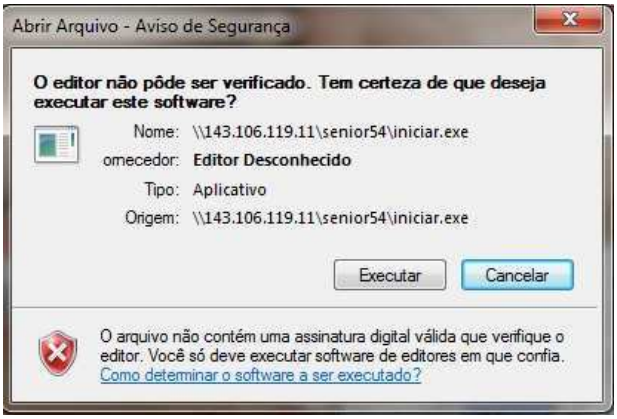
Testar o uso dos módulos do VETORH (Administração de Pessoal, Refeitório dentre outros)

Finalmente temos condições de testar os módulos instalados, você verá que na sua área de trabalho terá um novo ícone, denominado "**Sênior**", como abaixo.

Para acessar os programas do Sistema de Recursos Humanos abra a pasta "**Senior\vetorh**", e clicar sobre o ícone do módulo que precisa acessar.



Quando iniciamos os módulos, por exemplo, o Administração de Pessoal, uma janela de inicialização será apresentada, nela temos o andamento de carga para memória das tabelas do Sistema e dos arquivos usados no banco de dados. Pode-se também antes ocorrer a solicitação de confirmação da execução do programa, pois estes produtos não possuem assinatura junto ao sistema operacional.



Clique em '**Executar**' para carregar o módulo. Em seguida será mostrado o processo de inicialização que verifica se há necessidade de atualização dos arquivos que estão no servidor para sua máquina.

Após todos os arquivos carregados em memória o usuário receberá a janela de "**logon**" (entrada) no Sistema, a partir daí o cliente do sistema precisa se identificar com seu nome de usuário e senha, peça para alguém de RH local fazer um teste.

Depois de digitado o nome do usuário e senha, aguarde alguns instantes que o módulo que solicitou será apresentado na tela, a partir daí o cliente já poderá utilizar o produto.

Uma vez que o usuário de RH local executou o sistema e chegou até este ponto, temos a garantia que toda a parte de configuração da rede e instalação foi executada com sucesso.

Contatos com a equipe de suporte da DGRH

Estaremos à disposição dos usuários e clientes do Sistema de Recursos Humanos para esclarecer as dúvidas, receber comentários e sugestões para melhoria no atendimento.

Os contatos deverão ser feitos de acordo com a especificidade do problema, pois temos duas equipes distintas preparadas nas seguintes áreas:

Administração do Sistema de Recursos Humanos

Poderão ser esclarecidas dúvidas sobre ocorrências quando o cliente está utilizando um dos módulos do Sistemas (Relatórios, Telas, Senhas e outros). O contato deverá ser feito para:

SIARH -

Thiago Sbrici

✉ e-mail: thiago@unicamp.br

☎ Telefone : 0*19 3521-5186

Pessoalmente : Com prévio agendamento.

Solicitação de Serviços: Através do Site da DGRH

http://serv-20.dgrh.unicamp.br/solicitacoes/

Administração da Rede do DGRH e SIARH

Esta equipe está preparada para auxiliar as dúvidas relacionadas sobre tecnologia para funcionamento do Sistema (integração das redes, relacionamento de confiança, alteração de arquivos no cliente ou servidor, dúvidas na instalação, erros de conexão, etc). O contato deverá ser feito para:

Administração da Rede

Jurandir Roque Dutra da Silva, Christiane Zim Zapelini ou *Rodrigo Botelho Martimiano*

✉ e-mails: roque@unicamp.br, zapelini@unicamp.br ou botelhom@unicamp.br

☎ Telefone: 0*19 3521-4790 ou 0*19 3521-5186

Pessoalmente : Com prévio agendamento.

Localização da DGRH

Rua da Reitoria, prédio Reitoria IV, Térreo

[i] Conceitos básicos sobre Relações de Confiança: http://technet.microsoft.com/pt-br/library/cc759554(v=WS.10).aspx e http://technet.microsoft.com/pt-br/library/cc775736(v=WS.10).aspx

[ii] http://technet.microsoft.com/pt-br/library/cc783351(v=WS.10).aspx