

# Sessão 1: Fundamentos de segurança

## 1) Da divisão de grupos

Neste curso, os alunos serão divididos em dois grupos: **A** e **B**. Ao longo da semana, iremos realizar algumas atividades que vão envolver a intercomunicação entre máquinas virtuais dos alunos de cada grupo; para que as configurações de rede de dois alunos envolvidos em uma mesma atividade não conflitem, iremos adotar uma nomenclatura de endereços para cada grupo, como se segue:

*Tabela 1. Nomenclatura entre grupos*

Grupo	Sufixo de endereço
A	1
B	2

O que isso significa, na prática? Em vários momentos, ao ler este material, você irá se deparar com endereços como 172.16.G.20 ou 10.1.G.10 — que evidentemente são inválidos. Nesse momento, substitua o número do seu grupo pela letra **G** no endereço. Se você for membro do grupo **B**, portanto, os endereços acima seriam 172.16.2.20 e 10.1.2.10.

## 2) Topologia geral de rede

A figura abaixo mostra a topologia de rede que será utilizada durante este curso. Nos tópicos que se seguem, iremos verificar que a importação de máquinas virtuais, configurações de rede e conectividade estão funcionais antes de prosseguir. As configurações específicas de cada máquina/interface serão detalhadas na seção a seguir.

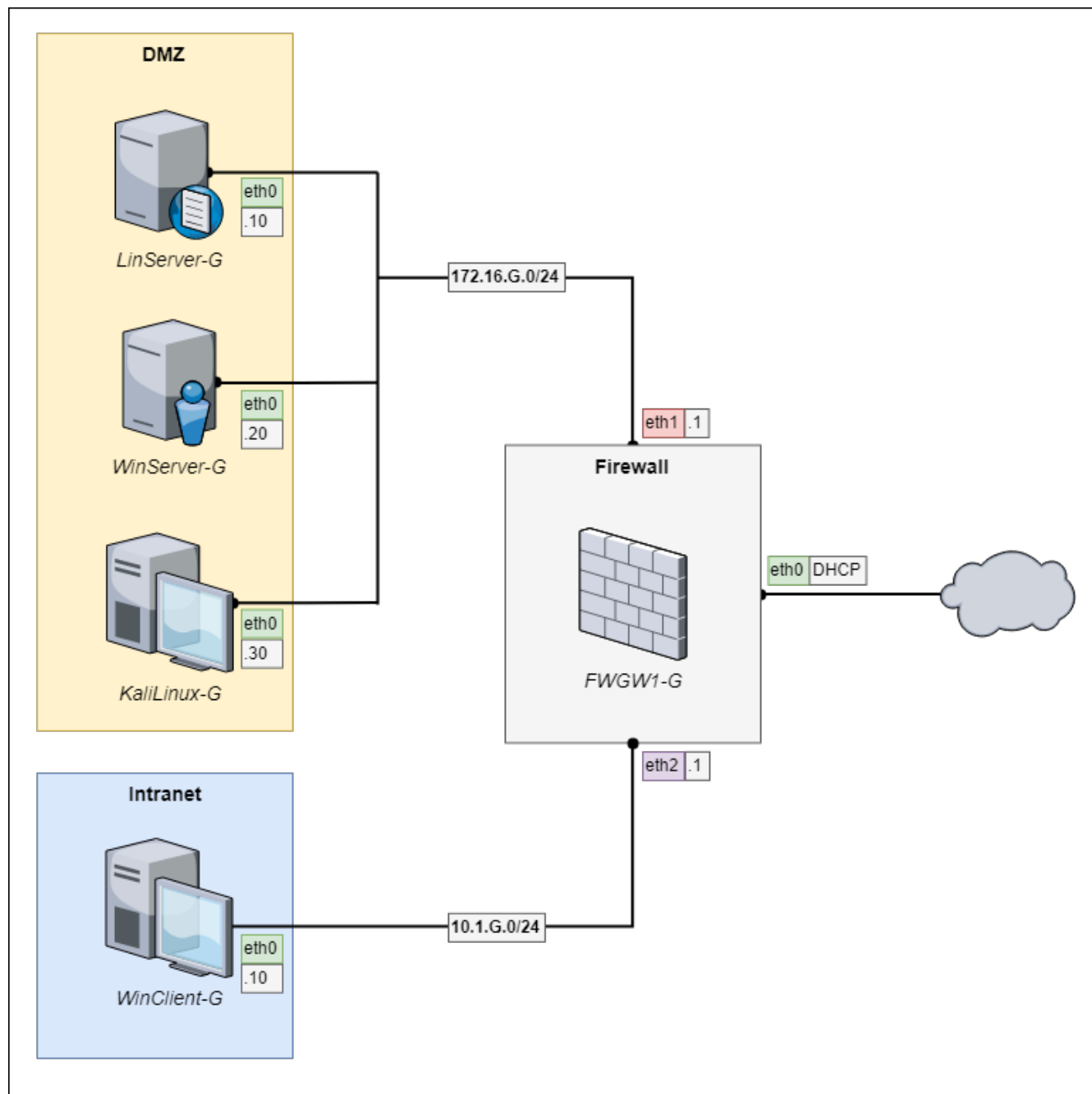


Figura 1. Topologia de rede do curso

### 3) Configuração do Virtualbox

1. Primeiramente, verifique se todas as máquinas virtuais foram importadas.

Se ainda não foram, importe-as manualmente através do menu *File > Import Appliance*. Navegue até a pasta onde se encontra o arquivo **.ova** com as imagens das máquinas virtuais e clique em *Next*. Na tela subsequente, marque a caixa *Reinitialize the MAC address of all network cards* e só depois clique em *Import*.

Ao final do processo, você deve ter cinco VMs com as configurações que se seguem. Renomeie as máquinas virtuais com os nomes indicados na tabela abaixo, substituindo o **G** pela letra do seu grupo. Para renomear máquinas virtuais no Virtualbox, acesse *Settings > General > Name* e altere o nome da VM (a mesma deve estar previamente desligada).

Tabela 2. VMs disponíveis no Virtualbox

Nome VM	Memória
FWGW1-G	2048 MB
LinServer-G	2048 MB
WinServer-G	2048 MB
KaliLinux-G	2048 MB
WinClient-G	2048 MB

Se a quantidade de RAM de alguma das máquinas for inferior aos valores estipulados, ajuste-a.

2. Agora, configure as redes do Virtualbox. Acesso o menu *File > Host Network Manager* e crie as seguintes redes:

Tabela 3. Redes host-only no Virtualbox

Rede	Endereço IPv4	Máscara de rede	Servidor DHCP
Virtualbox Host-Only Ethernet Adapter	172.16.G.254	255.255.255.0	Desabilitado
Virtualbox Host-Only Ethernet Adapter #2	10.1.G.254	255.255.255.0	Desabilitado

- Finalmente, configure as interfaces de rede de cada máquinas virtual. Para cada VM, acesse *Settings > Network* e faça as configurações que se seguem:

Tabela 4. Interfaces de rede das máquinas virtuais

VM Nome	Interface	Conectado a	Nome da rede
FWGW1-G	Adapter 1	Bridged Adapter	Placa de rede física do <i>host</i>
	Adapter 2	Host-only Adapter	Virtualbox Host-Only Ethernet Adapter
	Adapter 3	Host-only Adapter	Virtualbox Host-Only Ethernet Adapter #2
LinServer-G	Adapter 1	Host-only Adapter	Virtualbox Host-Only Ethernet Adapter
WinServer-G	Adapter 1	Host-only Adapter	Virtualbox Host-Only Ethernet Adapter
KaliLinux-G	Adapter 1	Host-only Adapter	Virtualbox Host-Only Ethernet Adapter
WinClient-G	Adapter 1	Host-only Adapter	Virtualbox Host-Only Ethernet Adapter #2

## 4) Detalhamento das configurações de rede

As configurações de rede realizadas internamente em cada máquina virtual foram apresentados de forma sucinta na figura 1. Iremos detalhar as configurações logo abaixo:

Tabela 5. Configurações de rede de cada VM

VM Nome	Interface	Modo	Endereço	Gateway	Servidores DNS
FWGW1-G	eth0	Estático	DHCP	Automático	Automático
	eth1	Estático	172.16.G.1/24	n/a	n/a
	eth2	Estático	10.1.G.1/24	n/a	n/a
LinServer-G	eth0	Estático	172.16.G.10/24	172.16.G.1	8.8.8.8 ; 8.8.4.4
WinServer-G	eth0	Estático	172.16.G.20/24	172.16.G.1	8.8.8.8 ; 8.8.4.4
KaliLinux-G	eth0	Estático	172.16.G.30/24	172.16.G.1	8.8.8.8 ; 8.8.4.4
WinClient-G	eth0	Estático	10.1.G.10/24	10.1.G.1	8.8.8.8 ; 8.8.4.4

A partir do Debian 9, a nomenclatura padrão de interfaces de rede foi alterada. Ao invés de denotarmos as interfaces como **eth0**, **eth1** ou **eth2**, o **systemd/udev** utiliza, a partir da versão v197, um método de nomenclatura de interfaces usando **biosdevnames**, como documentado oficialmente em <https://www.freedesktop.org/wiki/Software/systemd/PredictableNetworkInterfaceNames/> . Com efeito, esse novo sistema suporta cinco meios de nomeação de interfaces de rede:

- Nomes incorporando números de índice providos pelo firmware/BIOS de dispositivos *on-board* (p.ex.: **eno1**)

2. Nomes incorporando números de índice providos pelo firmware/BIOS de encaixes *hotplug* PCI Express (p.ex.: `ens1`)
3. Nomes incorporando localização física/geográfica do conector do hardware (p.ex.: `enp2s0`)
4. Nomes incorporando o endereço MAC da interface (p.ex.: `enx78e7d1ea46da`)
5. Nomes clássicos, usando nomenclatura não-previsível nativa do kernel (p.ex.: `eth0`)

Como as máquinas *FWGW1-G* e *LinServer-G* são instalações do Debian 9, isso significa dizer que as entradas de interface na tabela anterior ficam da seguinte forma:

Tabela 6. Nomenclatura de interfaces de máquinas Debian 9

VM Nome	Interface antiga	Interface nova
FWGW1-G	eth0	enp0s3
	eth1	enp0s8
	eth2	enp0s9
LinServer-G	eth0	enp0s3

Observe, por exemplo, como é feita a detecção de interfaces durante o *boot* da máquina *FWGW1-G*:

```
# hostname
FWGW1-A

# dmesg | grep 'renamed from'
[ 1.667147] e1000 0000:00:09.0 enp0s9: renamed from eth2
[ 1.667995] e1000 0000:00:08.0 enp0s8: renamed from eth1
[ 1.668885] e1000 0000:00:03.0 enp0s3: renamed from eth0
```

## 5) Configuração da máquinas virtuais

Agora, vamos configurar a rede de cada máquina virtual de acordo com as especificações da topologia de rede apresentada no começo deste capítulo.



Observe que as máquinas virtuais da **DMZ** e **Intranet** poderão ainda não ter acesso à Internet neste passo, pois ainda não configuramos o firewall. A próxima seção irá tratar deste tópico.



Para tangibilizar os exemplos nas configurações-modelo deste gabarito, iremos assumir que o aluno é membro do grupo **A**, ou seja, tem suas máquinas virtuais nas redes 172.16.1.0/24 e 10.1.1.0/24. Se você for membro do grupo **B**, tenha o cuidado de sempre adaptar os endereços IP dos exemplos para as suas faixas de rede.

1. Primeiramente, ligue a máquina *FWGW1-G* e faça login como usuário **root** e senha **rnpesr**. Verifique se o mapa de teclado está correto (teste com os caracteres **/** ou **ç**). Se não estiver, execute o comando:

```
# dpkg-reconfigure keyboard-configuration
```

Nas perguntas que se seguem, responda:

Tabela 7. Configurações de teclado

Pergunta	Parâmetro
Modelo do teclado	PC (Intl) Genérico de 105 teclas
Layout do teclado	Outro > Português (Brasil) > Português (Brasil)
Tecla para funcionar como AltGr	Alt Direito (AltGr)
Tecla Compose	Tecla Logo Direita

Finalmente, execute o comando que se segue. Volte a testar o teclado e verifique seu funcionamento.

```
# systemctl restart keyboard-setup.service
```

Se ainda não estiver funcional, reinicie a VM e teste novamente.

2. Ao longo do curso, iremos editar vários arquivos de texto em ambiente Linux. Há vários editores de texto disponíveis para a tarefa, como o **vi**, **emacs** ou **nano**. Caso você não esteja familiarizado com um editor de texto, recomendamos o uso do **nano**, que possui uma interface bastante amigável para usuários iniciantes. Para editar um arquivo com o **nano**, basta digitar **nano** seguido do nome do arquivo a editar — não é necessário que o arquivo tenha sido criado previamente:

```
# nano teste
```

Digite livremente a seguir. Use as setas do teclado para navegar no texto, e **DELETE** ou **BACKSPACE** para apagar texto. O **nano** possui alguns atalhos interessantes, como:

- **CTRL + G**: Exibir a ajuda do editor
- **CTRL + X**: Fechar o **buffer** de arquivo atual (que pode ser um texto sendo editado, ou o painel de ajuda), e sair do **nano**. Para salvar o arquivo, digite **Y** (*yes*) ou **S** (*sim*) para confirmar as mudanças ao arquivo, opcionalmente altere o nome do arquivo a ser escrito no disco, e digite **ENTER**.
- **CTRL + O**: Salvar o arquivo no disco sem sair do editor.
- **CTRL + W**: Buscar padrão no texto.
- **CTRL + K**: Cortar uma linha inteira e salvar no **buffer** do editor.
- **CTRL + U**: Colar o **buffer** do editor na posição atual do cursor. Pode ser usado repetidamente.

Para salvar e sair do texto sendo editado, como mencionado acima, utilize **CTRL + X**.

3. Ainda na máquina *FWGW1-G*, edite o arquivo **/etc/network/interfaces** como se segue, reinicie a rede e verifique o funcionamento:

```
# hostname  
FWGW1-A
```

```
# whoami  
root
```

```
# nano /etc/network/interfaces  
(...)
```

```
# cat /etc/network/interfaces  
source /etc/network/interfaces.d/*
```

```
auto lo enp0s3 enp0s8 enp0s9
```

```
iface lo inet loopback
```

```
iface enp0s3 inet dhcp
```

```
iface enp0s8 inet static  
address 172.16.1.1/24
```

```
iface enp0s9 inet static  
address 10.1.1.1/24
```

```
# systemctl restart networking
```

```
# ip a s | grep '^ *inet '  
    inet 127.0.0.1/8 scope host lo  
    inet 192.168.29.107/24 brd 192.168.29.255 scope global enp0s3  
    inet 172.16.1.1/24 brd 172.16.1.255 scope global enp0s8  
    inet 10.1.1.1/24 brd 10.1.1.255 scope global enp0s9
```



4. Se você for membro do grupo **B**, altere o nome de *host* da máquina *FWGW1-G* para refletir corretamente seu grupo. Primeiro, altere o arquivo */etc/hostname*:

```
# nano /etc/hostname  
(...)
```

```
# cat /etc/hostname  
FWGW1-B
```

Faça o mesmo com o arquivo */etc/hosts*:

```
# nano /etc/hosts  
(...)
```

```
# cat /etc/hosts  
127.0.0.1      localhost  
127.0.1.1      FWGW1-B.intnet  FWGW1-B  
  
# The following lines are desirable for IPv6 capable hosts  
::1           localhost ip6-localhost ip6-loopback  
ff02::1       ip6-allnodes  
ff02::2       ip6-allrouters
```

Agora, reinicie a máquina. Após o login como usuário **root**, você deverá ver que o *prompt* do terminal mudou, como se segue:

```
root@FWGW1-B:~# hostname  
FWGW1-B
```

```
# whoami  
root
```

Finalmente, vamos regerar as chaves de *host* do **ssh** com o novo *hostname*. Execute:

```
# rm /etc/ssh/ssh_host_*
```

```
# dpkg-reconfigure openssh-server
Creating SSH2 RSA key; this may take some time ...
2048 SHA256:NyWM8WE7wv2rWpPMN/w115eq4UeflK0m+jFSsHQ/Zwk root@FWGW1-B (RSA)
Creating SSH2 ECDSA key; this may take some time ...
256 SHA256:ZPxXhAgsnAdTuEbpggsxERp5WQNbQuNROAtatszYrLA root@FWGW1-B (ECDSA)
Creating SSH2 ED25519 key; this may take some time ...
256 SHA256:YBEQfhMSNz6sKvyDu/mRjNB/njj6PAim7xaLmGrcDEM root@FWGW1-B (ED25519)
```

```
# systemctl restart ssh
```

5. Ligue a máquina *LinServer-G* e faça login como usuário **root** e senha **rnpesr**. Se encontrar problemas com o teclado, aplique a mesma solução utilizada na etapa (1) desta atividade. Para alterar o *hostname* da máquina, siga os passos da etapa (4).

A seguir, edite as configurações de rede no arquivo **/etc/network/interfaces**, de DNS no arquivo **/etc/resolv.conf**, reinicie a rede e verifique se tudo está funcionando:

```
# hostname
LinServer-A
```

```
# whoami
root
```

```
# nano /etc/network/interfaces
(...)
```

```
# cat /etc/network/interfaces
source /etc/network/interfaces.d/*

auto lo enp0s3

iface lo inet loopback

iface enp0s3 inet static
address 172.16.1.10/24
gateway 172.16.1.1
```

```
# nano /etc/resolv.conf
(...)
```

```
# cat /etc/resolv.conf
nameserver 8.8.8.8
nameserver 8.8.4.4
```

```
# systemctl restart networking
```

```
# ip a s | grep '^ *inet '
    inet 127.0.0.1/8 scope host lo
    inet 172.16.1.10/24 brd 172.16.1.255 scope global enp0s3
```

6. Vamos para a máquina *WinServer-G*. Assim que a máquina terminar de ligar, clique em **OK** para entrar com uma nova senha, e informe a senha **rnpesr**. Na próxima tela, escolha "Activate Later".

Pelo *Control Panel* ou usando o comando **ncpa.cpl**, configure o endereço IP e servidores DNS de forma estática, como na foto abaixo, e verifique que suas configurações estão funcionais. Quando perguntado sobre o perfil da rede, escolha *Work*.

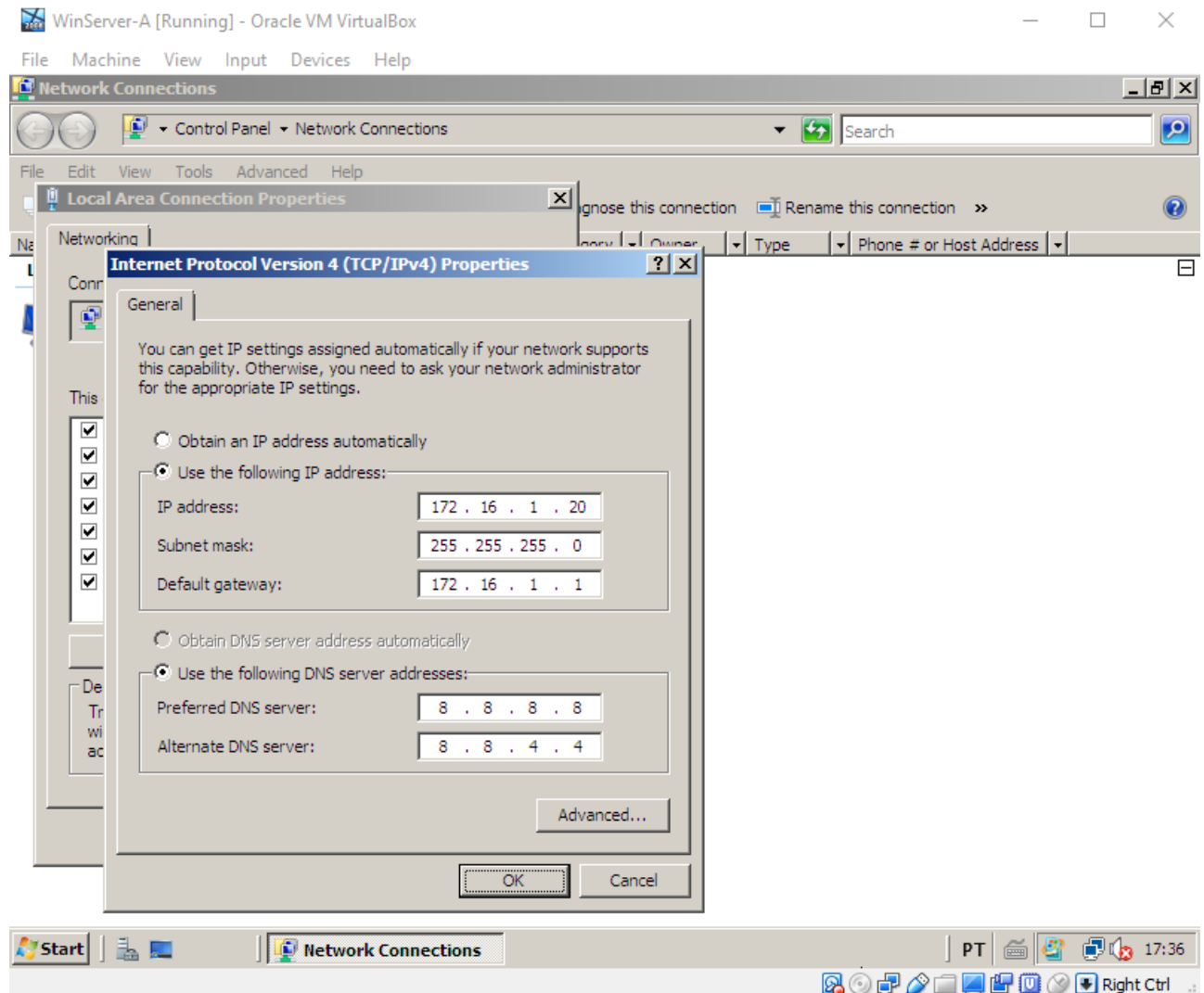


Figura 2. Configuração de rede da máquina *WinServer-G*

7. Prossiga para a máquina *KaliLinux-G*, e faça login como usuário **root** e senha **rnpsr**. Se encontrar problemas com o teclado, aplique a mesma solução utilizada na etapa (1) desta atividade, e reinicie a VM. Para alterar o *hostname* da máquina, siga os passos da etapa (4).

Em seguida, edite as configurações de rede no arquivo **/etc/network/interfaces** e de DNS no arquivo **/etc/resolv.conf**. Reinicie a rede e verifique se tudo está correto:

```
# hostname  
KaliLinux-A
```

```
# whoami  
root
```

```
# nano /etc/network/interfaces  
(...)
```

```
# cat /etc/network/interfaces  
source /etc/network/interfaces.d/*  
  
auto lo eth0  
  
iface lo inet loopback  
  
iface eth0 inet static  
address 172.16.1.30/24  
gateway 172.16.1.1
```

```
# nano /etc/resolv.conf  
(...)
```

```
# cat /etc/resolv.conf  
nameserver 8.8.8.8  
nameserver 8.8.4.4
```

```
# systemctl restart networking
```

```
# ip a s | grep '^ *inet '  
    inet 127.0.0.1/8 scope host lo  
    inet 172.16.1.30/24 brd 172.16.1.255 scope global eth0
```

8. Finalmente, vamos configurar a máquina *WinClient-G*: faça login como usuário **aluno** e senha **rnpesr**. Acesse o *Control Panel* ou use o comando **ncpa.cpl**, configure o endereço IP e servidores DNS de forma estática, como na foto abaixo, e verifique que suas configurações estão funcionais.

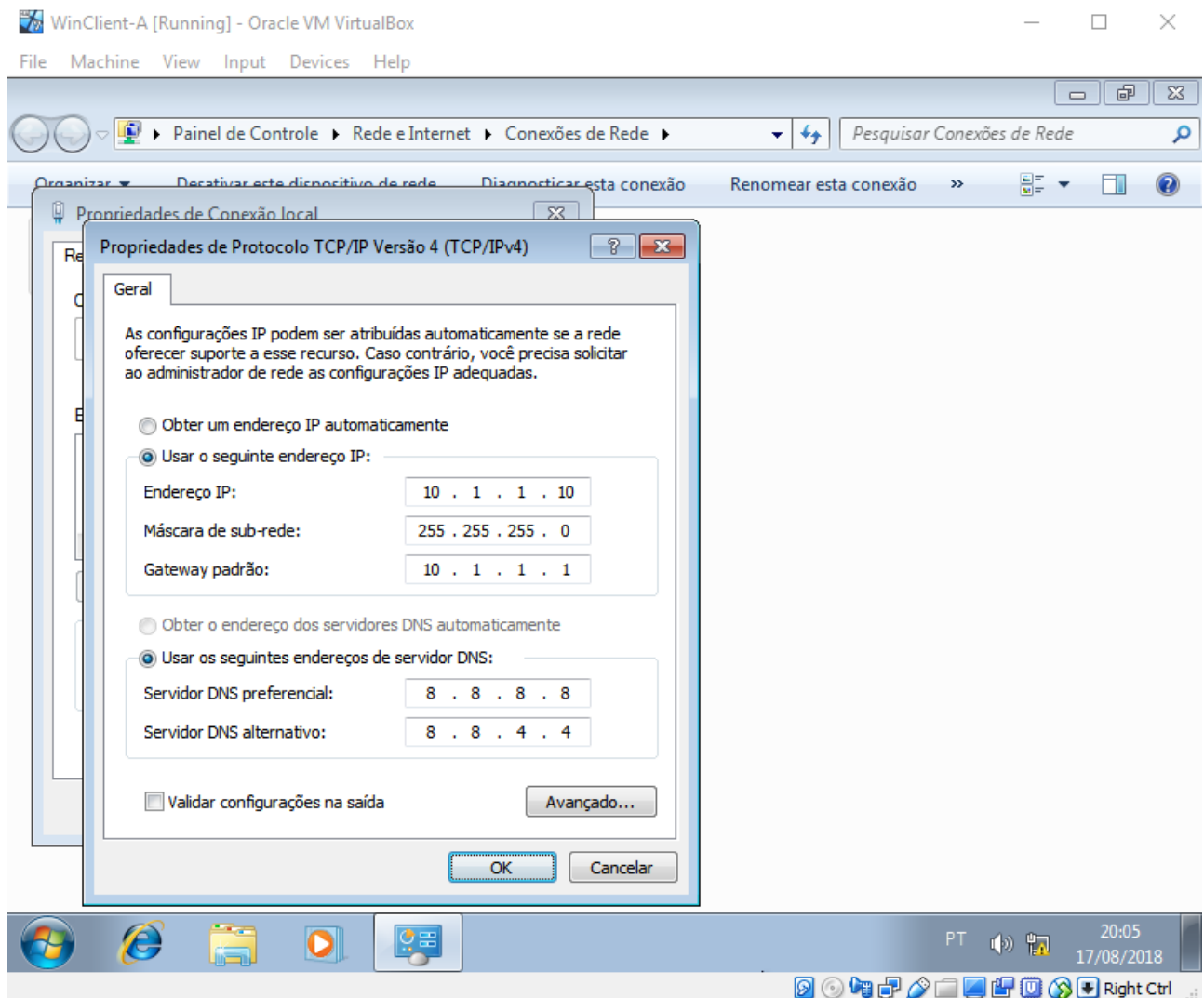


Figura 3. Configuração de rede da máquina *WinClient-G*

## 6) Configuração de firewall e NAT

O próximo passo é garantir que as VMs consigam acessar a internet através da máquina *FWGW1-G*, que é o firewall/roteador na topologia de rede do curso.

1. Antes de mais nada, observe que na máquina *FWGW1-G* já existe uma configuração de *masquerading* (um tipo de SNAT que veremos em maior detalhe na sessão 3) no arquivo */etc/rc.local*:

```
# hostname
FWGW1-A
```

```
# cat /etc/rc.local
#!/bin/sh -e

iptables -t nat -A POSTROUTING -o enp0s3 -j MASQUERADE
exit 0
```

2. Isto significa dizer que a tradução de endereços das redes privadas já está configurado. Verifique se o repasse de pacotes entre interfaces está habilitado—cheque se a linha *net.ipv4.ip\_forward=1* no arquivo */etc/sysctl.conf* está descomentada e, posteriormente, execute *# sysctl -p*:

```
# nano/etc/sysctl.conf
(...)
```

```
# grep 'net.ipv4.ip_forward' /etc/sysctl.conf
net.ipv4.ip_forward=1
```

```
# sysctl -p
net.ipv4.ip_forward = 1
```

3. Verifique que o *masquerading* está de fato habilitado no firewall:

```
# iptables -L POSTROUTING -vn -t nat
Chain POSTROUTING (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target      prot opt in      out     source        destination
 23  1640 MASQUERADE  all  --  *       enp0s3  0.0.0.0/0     0.0.0.0/0
```

## 7) Teste de conectividade das VMs

1. Vamos agora testar a conectividade de cada uma das VMs. Primeiro, acesse a máquina *FWGW1-G* e verifique o acesso à internet e resolução de nomes:

```
aluno@FWGW1-A:~$ hostname  
FWGW1-A
```

```
aluno@FWGW1-A:~$ ping -c3 8.8.8.8  
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.  
64 bytes from 8.8.8.8: icmp_seq=1 ttl=121 time=28.7 ms  
64 bytes from 8.8.8.8: icmp_seq=2 ttl=121 time=16.9 ms  
64 bytes from 8.8.8.8: icmp_seq=3 ttl=121 time=16.7 ms  
  
--- 8.8.8.8 ping statistics ---  
3 packets transmitted, 3 received, 0% packet loss, time 2005ms  
rtt min/avg/max/mdev = 16.776/20.832/28.757/5.606 ms
```

```
aluno@FWGW1-A:~$ ping -c3 esr.rnp.br  
PING esr.rnp.br (200.130.99.56) 56(84) bytes of data.  
64 bytes from 200.130.99.56: icmp_seq=1 ttl=54 time=37.9 ms  
64 bytes from 200.130.99.56: icmp_seq=2 ttl=54 time=36.4 ms  
64 bytes from 200.130.99.56: icmp_seq=3 ttl=54 time=37.1 ms  
  
--- esr.rnp.br ping statistics ---  
3 packets transmitted, 3 received, 0% packet loss, time 2004ms  
rtt min/avg/max/mdev = 36.474/37.168/37.931/0.636 ms
```

2. Em seguida, acesse cada uma das demais VMs, em ordem (*LinServer-G*, *WinServer-G*, *KaliLinux-G* e *WinClient-G*) e teste se é possível:
  - Alcançar o roteador da rede: **ping 172.16.1.1** (para máquinas da DMZ) ou **ping 10.1.1.1** (para máquinas da Intranet)
  - Alcançar um servidor na Internet: **ping 8.8.8.8**
  - Resolver nomes: comandos **nslookup**, **host** ou **ping** para o nome de domínio **esr.rnp.br**

## 8) Instalação do *Virtualbox Guest Additions* nas VMs Windows

Vamos agora instalar os adicionais de convidado para máquinas virtuais do Virtualbox, conhecido como *Virtualbox Guest Additions*. Esse adicionais consistem em *drivers* de dispositivo e aplicações de sistema que otimizam o sistema para rodar no ambiente virtual, proporcionando maior performance e estabilidade. Nesta atividade, iremos instalar os adicionais apenas nas máquinas *WinServer-G* e *WinClient-G*.



1. Na console da máquina *WinServer-G*, acesse o menu *Devices > Insert Guest Additions CD image*. Após algum tempo, a janela de *autorun* irá aparecer, como mostrado abaixo. Clique duas vezes na opção *Run VBoxWindowsAdditions.exe*.

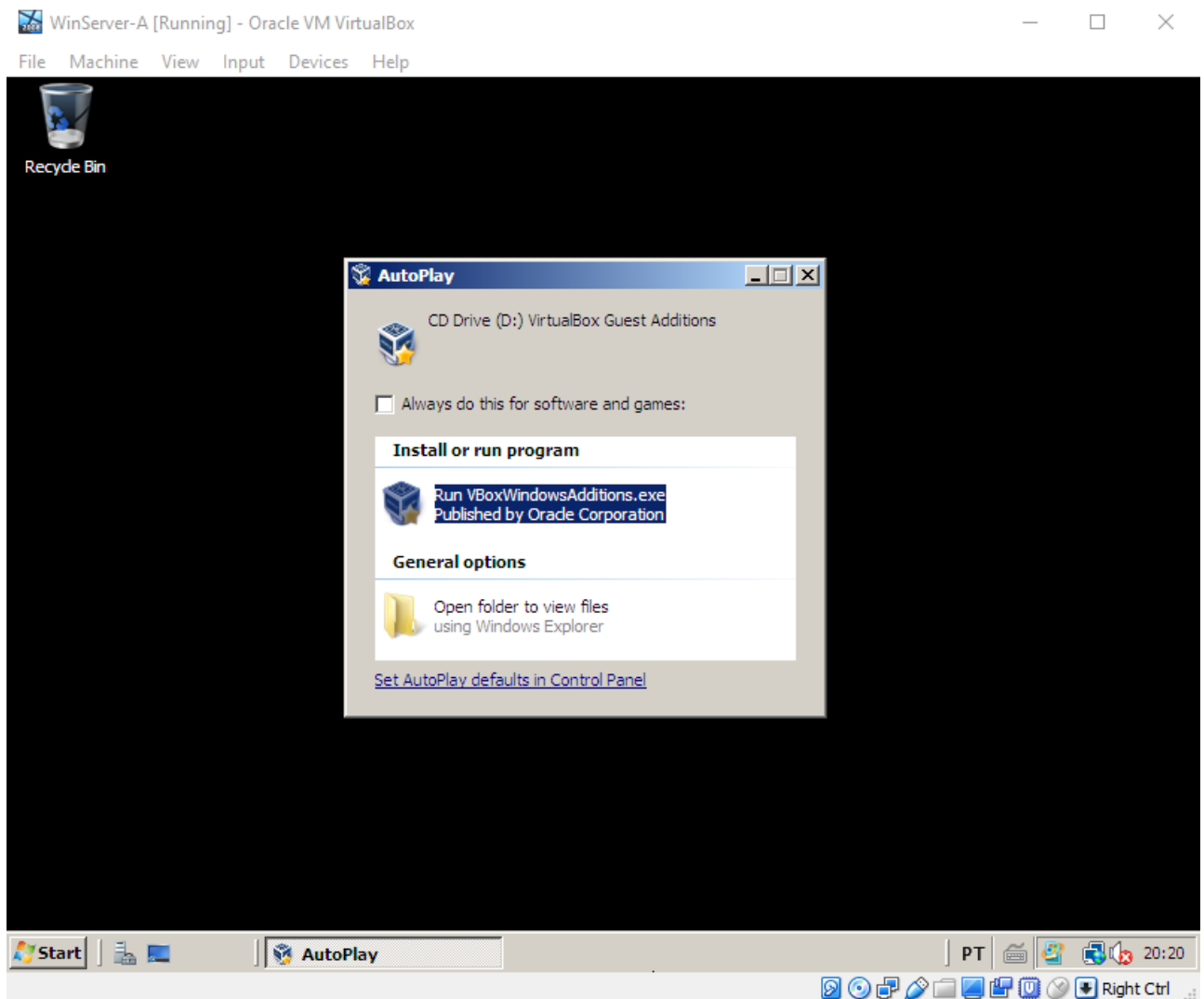


Figura 4. Janela de autorun do CD Virtualbox Guest Additions

2. No assistente de instalação, clique em *Next*, *Next*, e finalmente em *Install*. No meio da instalação o sistema irá avisar que a assinatura de quem publicou o software não é conhecida. Clique em *Install this driver software anyway*, como mostrado abaixo. A mesma janela irá aparecer logo depois, então escolha a mesma opção.

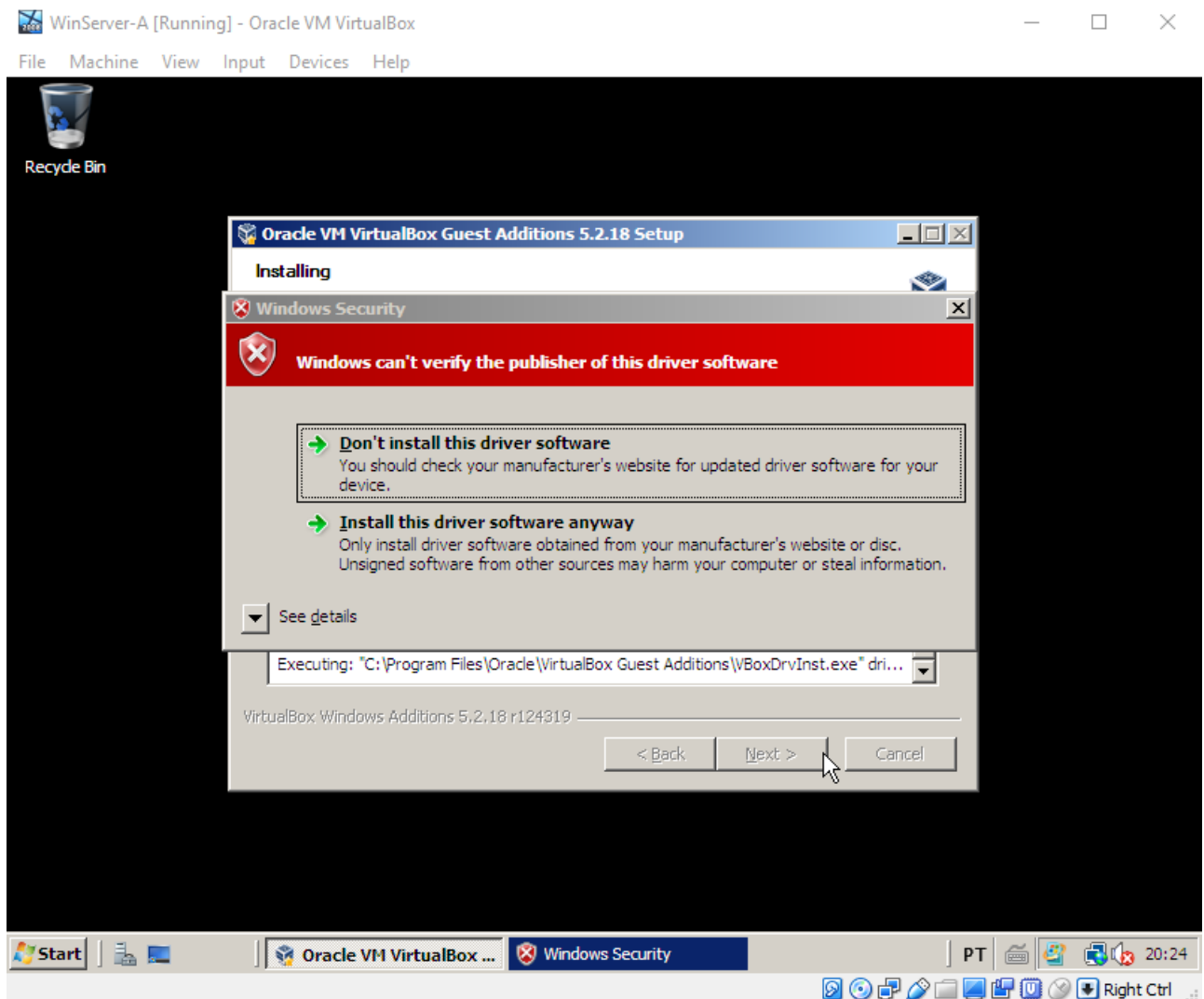


Figura 5. Aviso de publisher não verificado do Virtualbox Guest Additions

3. Ao final da instalação, o assistente irá solicitar que o computador seja reiniciado. Deixe a caixa *Reboot now* marcada e clique em *Finish*.
4. Após o reinício do sistema, maximize a janela do Virtualbox e faça login no sistema como o usuário **Administrator**. Observe que, agora, o *desktop* do Windows Server 2008 ocupa toda extensão do monitor, e não apenas uma pequena janela—indício de que a instalação do *Virtualbox Guest Additions* foi realizada com sucesso.
5. Repita o procedimento de instalação dos passos 1 - 4 na máquina *WinClient-G*.

## 9) Instalação do *Virtualbox Guest Additions* nas VMs Linux

A instalação do *Virtualbox Guest Additions* nas VMs Linux é um pouco diferente, mais manual. Siga os passos a seguir:

1. Vamos começar pela máquina *FWGW1-G*. Primeiro, faça login como **root** apague o conteúdo do arquivo `/etc/apt/sources.list`:

```
# echo "" > /etc/apt/sources.list
```

Em seguida, edite-o com o seguinte conteúdo:

```
# cat /etc/apt/sources.list
deb http://ftp.br.debian.org/debian/          stretch          main contrib non-
free
deb http://ftp.br.debian.org/debian/          stretch-updates main contrib non-
free
deb http://security.debian.org/debian-security stretch/updates main contrib non-
free
```

2. Em seguida, atualize os repositórios com o comando **apt-get update** e depois instale os pacotes **build-essential** e **module-assistant**, sem incluir recomendações:

```
# apt-get update
# apt-get install --no-install-recommends build-essential module-assistant
```

3. Agora, faça o download dos **headers** do kernel em execução no sistema:

```
# m-a prepare
```

4. Na console do Virtualbox da máquina *FWGW1-G*, acesse o menu *Devices > Insert Guest Additions CD image*. Em seguida, monte o dispositivo:

```
# mount /dev/cdrom /mnt/
```

5. Agora, execute o instalador do *Virtualbox Guest Additions*, com o comando:

```
# sh /mnt/VBoxLinuxAdditions.run
Verifying archive integrity... All good.
Uncompressing VirtualBox 5.2.18 Guest Additions for Linux.....
VirtualBox Guest Additions installer
Copying additional installer modules ...
Installing additional modules ...
VirtualBox Guest Additions: Building the VirtualBox Guest Additions kernel modules.
This may take a while.
VirtualBox Guest Additions: Starting.
```

6. Finalmente, reinicie a máquina. Após o *reboot*, verifique que os módulos do *Virtualbox Guest Additions* estão operacionais:

```
# reboot

(...)

# lsmod | grep '^vbox'
vboxsf          36413  0
vboxvideo       34226  1
vboxguest       221732  2 vboxsf
```

7. Instale os módulos do *Virtualbox Guest Additions* na máquina *LinServer-G*. O procedimento é idêntico ao que fizemos nos passos 1 - 6.

## 10) Configuração da VM WinServer-G

A máquina WinServer-G demanda uma pequena configuração adicional antes que estejamos prontos para começar os trabalhos. Vamos a ela:

1. Usando o 1) *Control Panel*, 2) clique direito em *Computer > Properties* no Windows Explorer ou 3) digitando **system** no menu iniciar, abra a tela de configuração do sistema como mostrado a seguir:

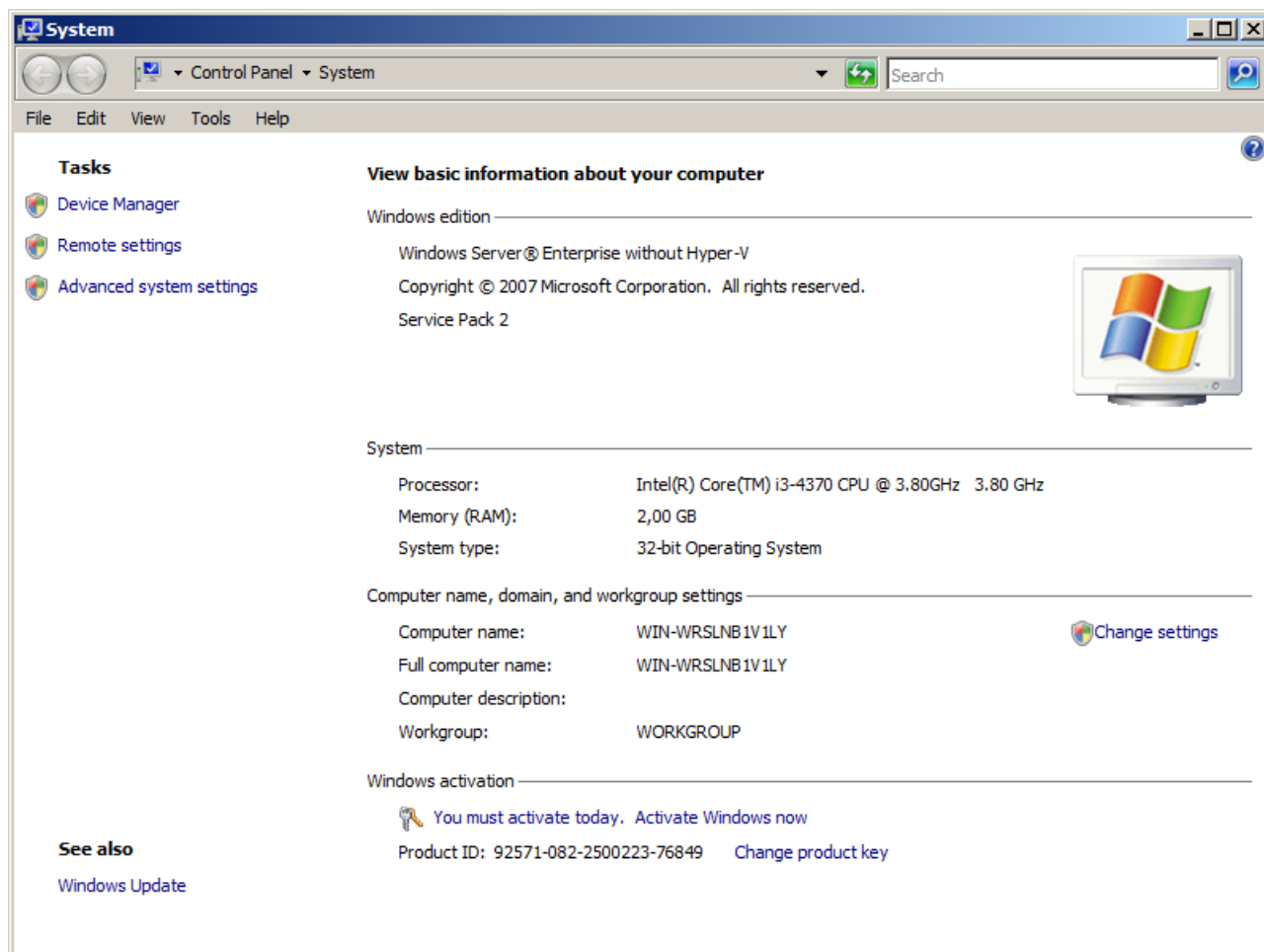


Figura 6. Tela de configuração do sistema do WinServer

2. Clique em *Change Settings*, e na aba *Computer Name*, no botão *Change....*. Altere o nome do computador para **WinServer-G** e o *Workgroup* para **GRUPO**, como se segue. Depois, clique em *OK*.

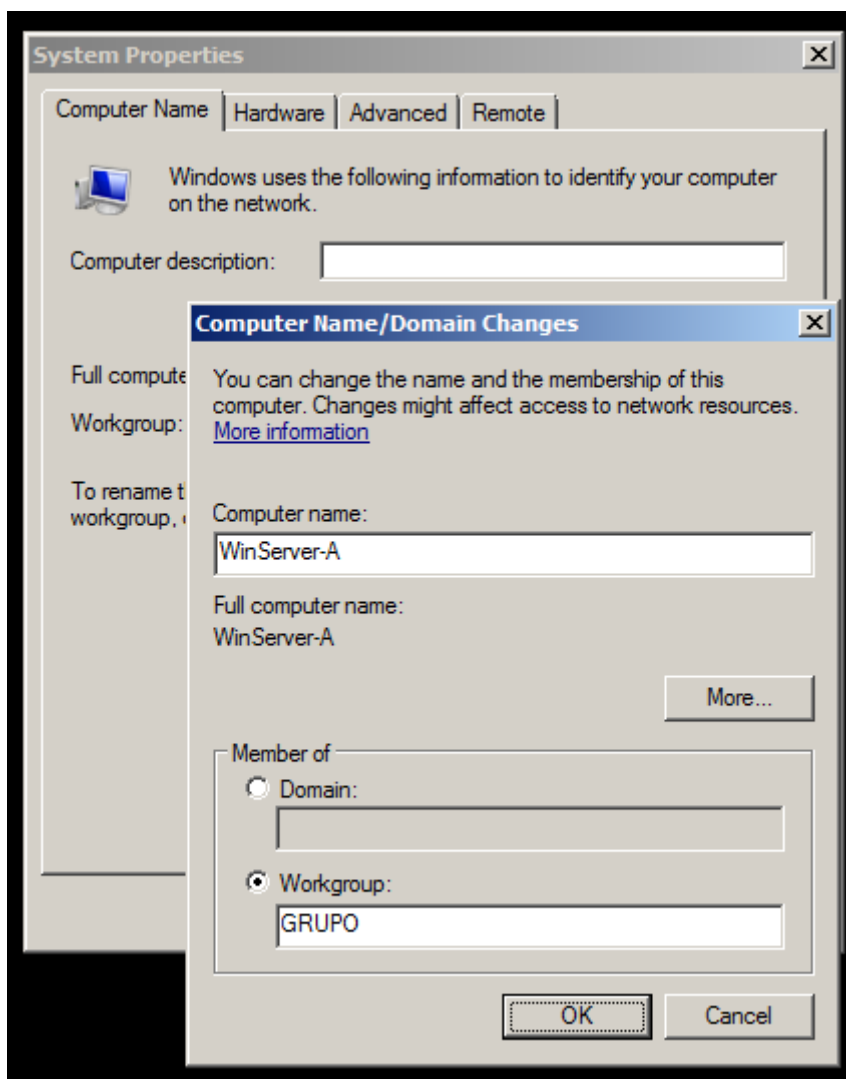


Figura 7. Alteração de nome de máquina do WinServer

3. Não reinicie o computador ainda. Na aba *Remote*, marque a caixa *Allow Connections from computers running any version of Remote Desktop (less secure)*, como na imagem abaixo. Depois, clique em *Apply* e em seguida em *Restart Later*.

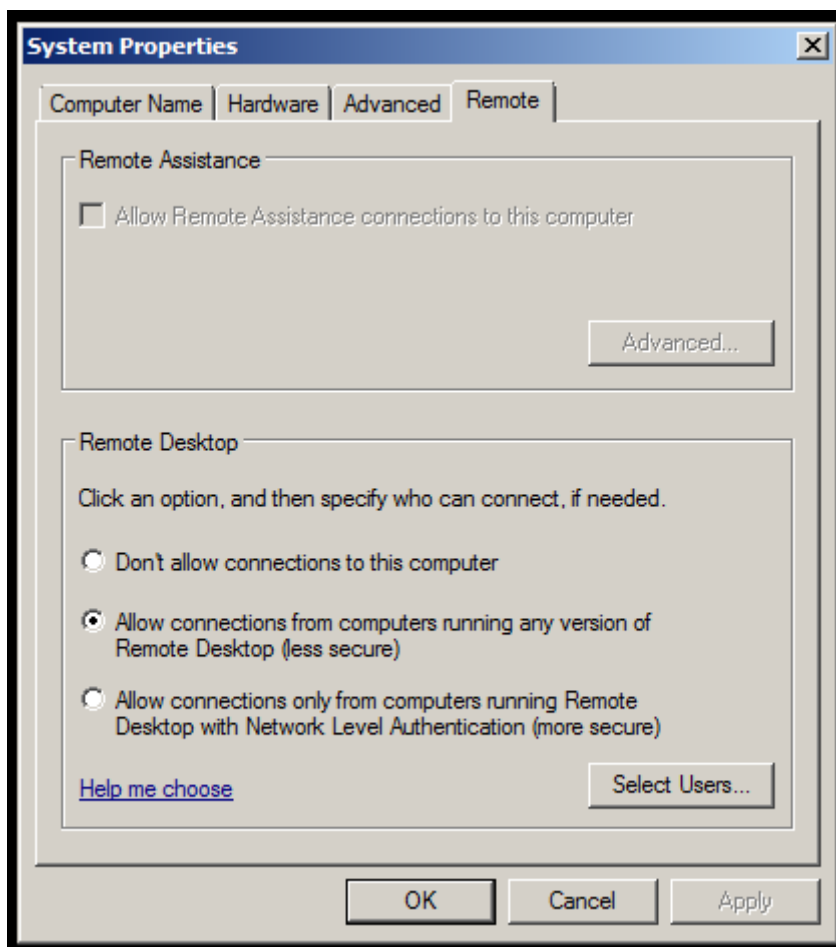


Figura 8. Configurações de Remote Desktop do WinServer

4. Agora, desabilite o firewall do Windows. Digite **firewall** no menu *Start* (alternativamente, clique em *Windows Firewall* no *Control Panel*), em seguida em *Turn Windows Firewall on or off*, e finalmente marque a caixa *Off*, como se segue:

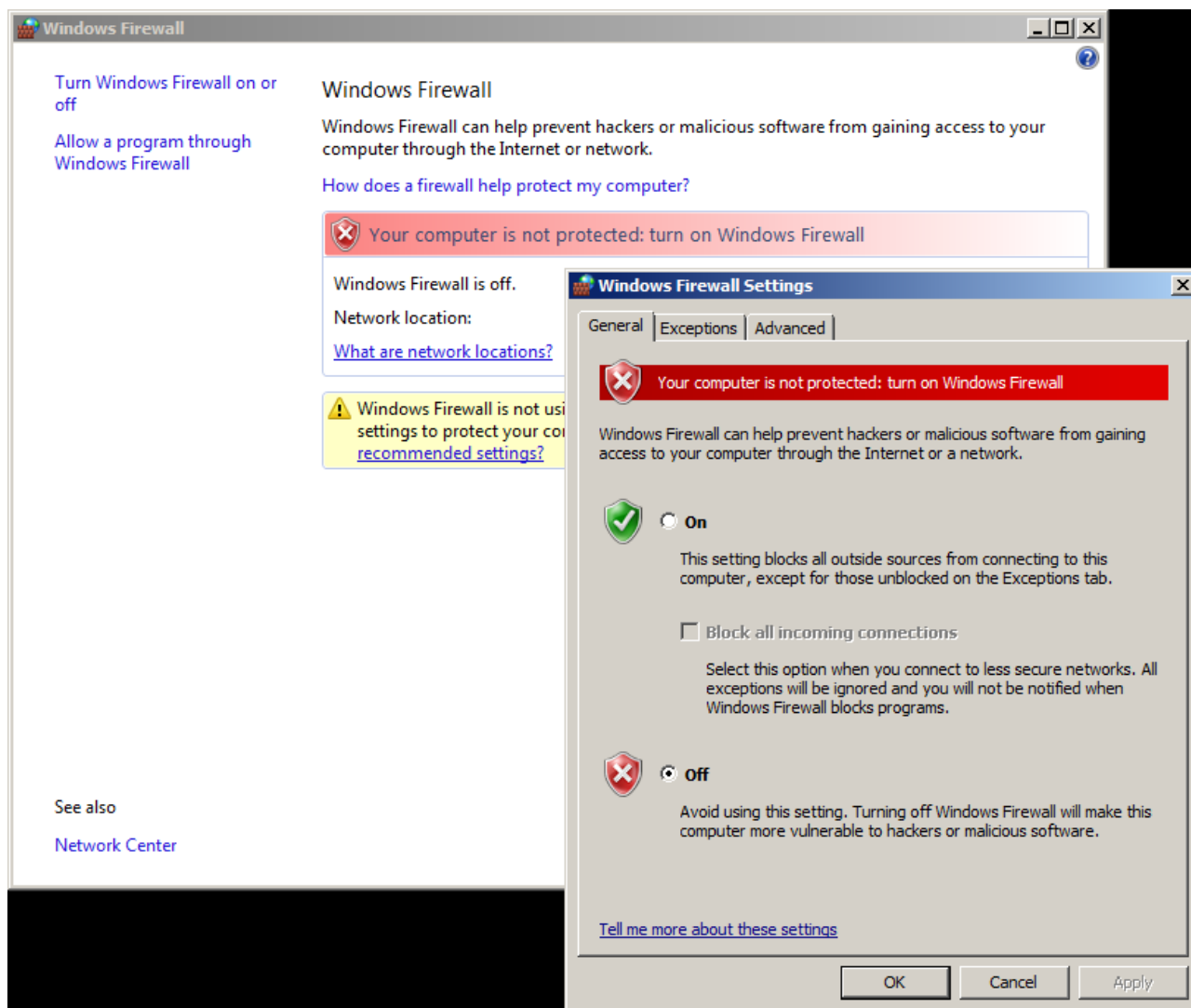


Figura 9. Desabilitar o firewall do WinServer

5. Clique em *OK* e reinicie a máquina *WinServer-G*.



6. Após o *reboot*, abra o *Server Manager* (é o primeiro ícone à direita do botão *Start*), e em seguida clique com o botão direito em *Roles*, selecionando *Add Roles*. Na janela subsequente, clique em *Next*. Depois, marque a caixa da *role Web Server (IIS)*, como se segue. Quando surgir a pergunta *Add features required for Web Server (IIS)?*, clique em *Add Required Features*, e depois em *Next*.

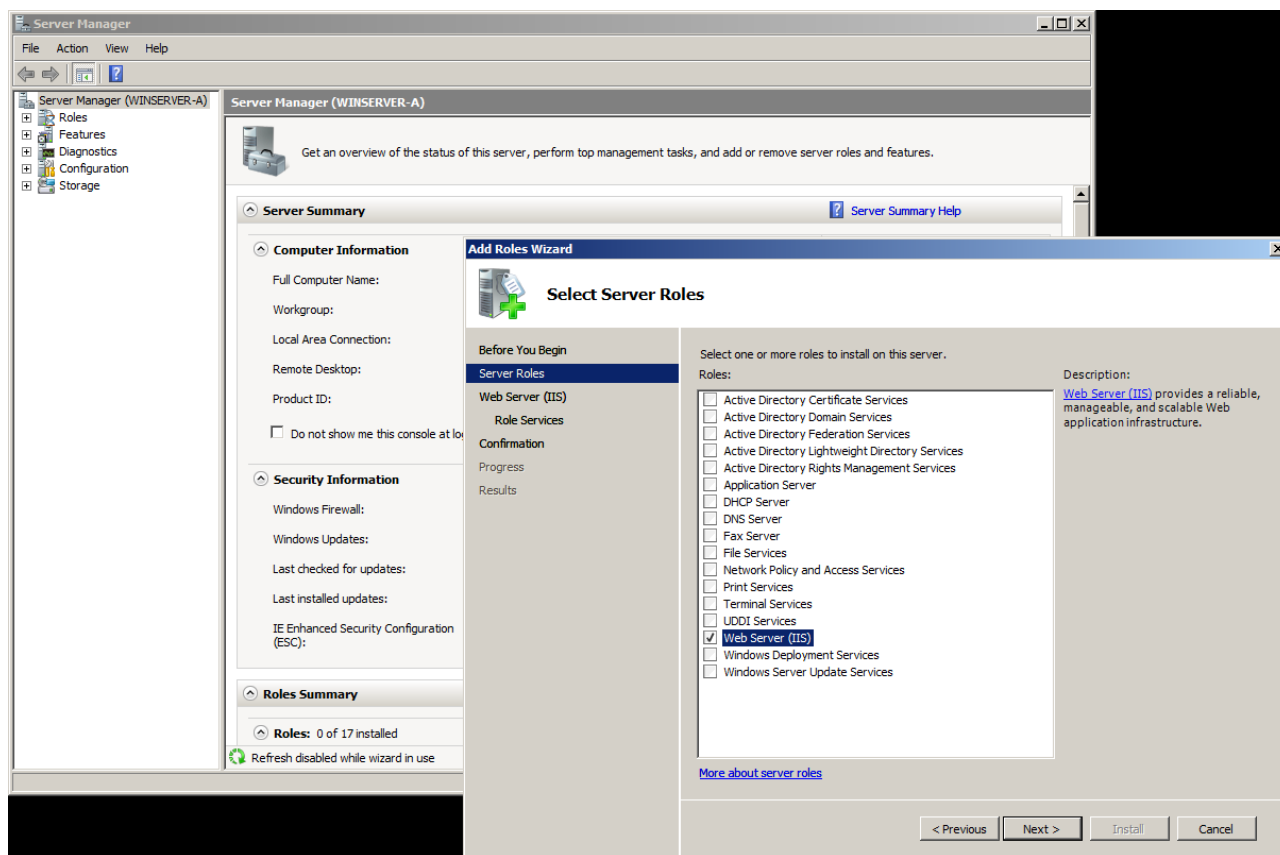


Figura 10. Instalando a role IIS no WinServer

7. Na janela *Introduction to Web Server (IIS)*, clique em *Next*. A seguir, na janela *Role services*, desça a barra de rolagem até o final e marque a caixa *FTP Publishing Service*, como se segue. Da mesma forma que antes, quando surgir a pergunta *Add features required for FTP Publishing Service?*, clique em *Add Required Features*, e depois em *Next*.

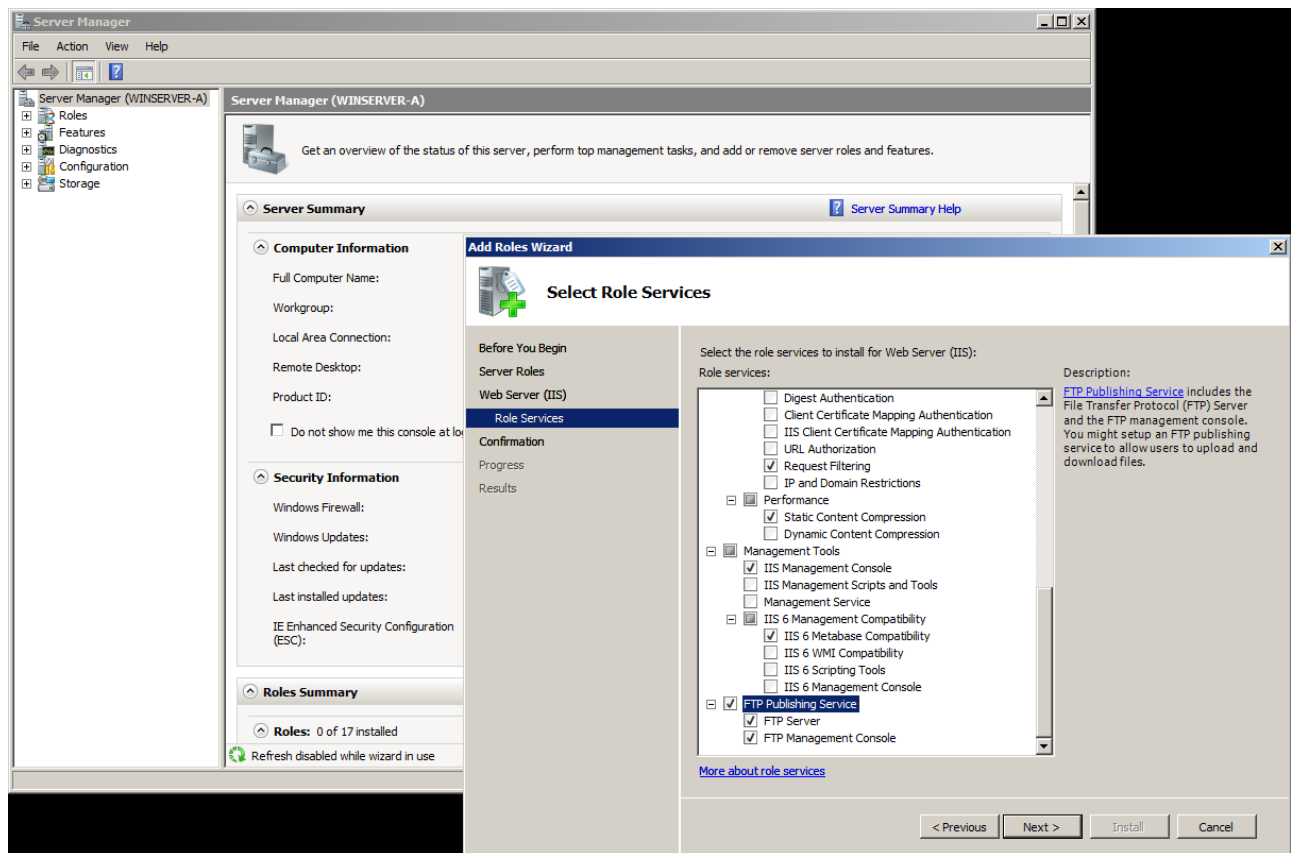


Figura 11. Instalando a feature FTP Server no WinServer

8. Finalmente, clique em *Install* e aguarde. Ao final do processo, clique em *Close*.

## 11) Exercitando os fundamentos de segurança

- Como vimos, o conceito de segurança mais básico apresentado consiste no CID (Confidencialidade, Integridade e Disponibilidade). Apresente três exemplos de quebra de segurança em cada um desses componentes, como por exemplo:
  - Planilha Excel corrompida.
  - Acesso não autorizado aos e-mails de uma conta de correio eletrônico.
  - Queda de um servidor web por conta de uma falha de energia elétrica.
- Associe cada um dos eventos abaixo a uma estratégia de segurança definida na parte teórica.
  - Utilizar um servidor web Linux e outro Windows 2016 Server para servir um mesmo conteúdo, utilizando alguma técnica para redirecionar o tráfego para os dois servidores.
  - Utilizar uma interface gráfica simplificada para configurar uma solução de segurança.
  - Configurar todos os acessos externos de modo que passem por um ponto único.
  - Um sistema de segurança em que caso falte energia elétrica, todos os acessos que passam por ele são bloqueados.

- Configurar um sistema para só ser acessível através de redes confiáveis, para solicitar uma senha de acesso e em seguida verificar se o sistema de origem possui antivírus instalado.
- Configurar as permissões de um servidor web para apenas ler arquivos da pasta onde estão as páginas HTML, sem nenhuma permissão de execução ou gravação em qualquer arquivo do sistema.

## 12) Normas e políticas de segurança

1. Acesse o site do DSIC em <http://dsic.planalto.gov.br/assuntos/editoria-c/instrucoes-normativas> e leia a Instrução Normativa GSI/PR nº 1, de 13 de junho de 2008 e as normas complementares indicadas. Elas são um bom ponto de partida para a criação de uma Política de Segurança, de uma Equipe de Tratamento de Incidentes de Segurança, de um Plano de Continuidade de Negócios e para a implementação da Gestão de Riscos de Segurança da Informação.
2. Leia o texto da Política de Segurança da Informação da Secretaria de Direitos Humanos da Presidência da República, de 2012 (disponível na seção *Links Úteis e Leituras Recomendadas* do AVA, pasta *PoSIC*), e procure identificar os principais pontos na estruturação de uma PoSIC. Faça uma crítica construtiva do documento com vistas a identificar as principais dificuldades encontradas na elaboração de uma PoSIC.