

Grupo de Resposta a Incidentes de Segurança

Algumas práticas para proteger o seu Windows

por: Guilherme Alves Cardoso Penha

guilherme@gris.dcc.ufrj.br
gris@gris.dcc.ufrj.br

Grupo de Resposta a Incidentes de Segurança
Departamento de Ciência da Computação
Instituto de Matemática
Universidade Federal do Rio de Janeiro



Conteúdo

- **Analisar o Windows**
- **Testar a exposição do Windows**
- **Aplicar algumas medidas**
- **Dicas de boas práticas**

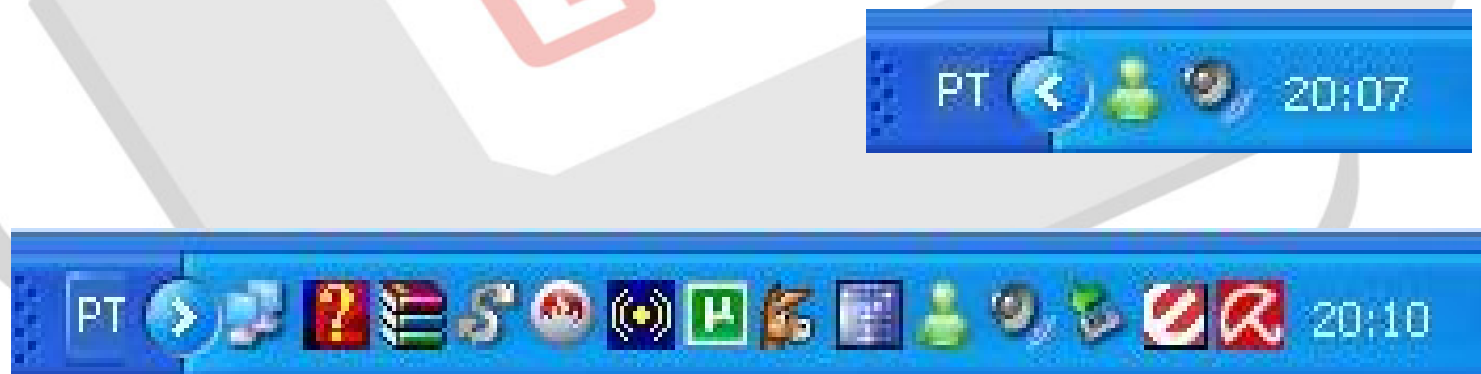
guilherme@gris.dcc.ufrj.br
gris@gris.dcc.ufrj.br

Grupo de Resposta a Incidentes de Segurança
Departamento de Ciência da Computação
Instituto de Matemática
Universidade Federal do Rio de Janeiro



Analizando o Windows

- Fique de olho na Barra de Tarefas perto do relógio
- Certifique-se de expandi-la
- Analise as opções dos ícones com um clique no botão direito do mouse



Analizando o Windows

- Fique de olho no Gerenciador de Tarefas
- Abra-o com “Ctrl + Shift + Esc”



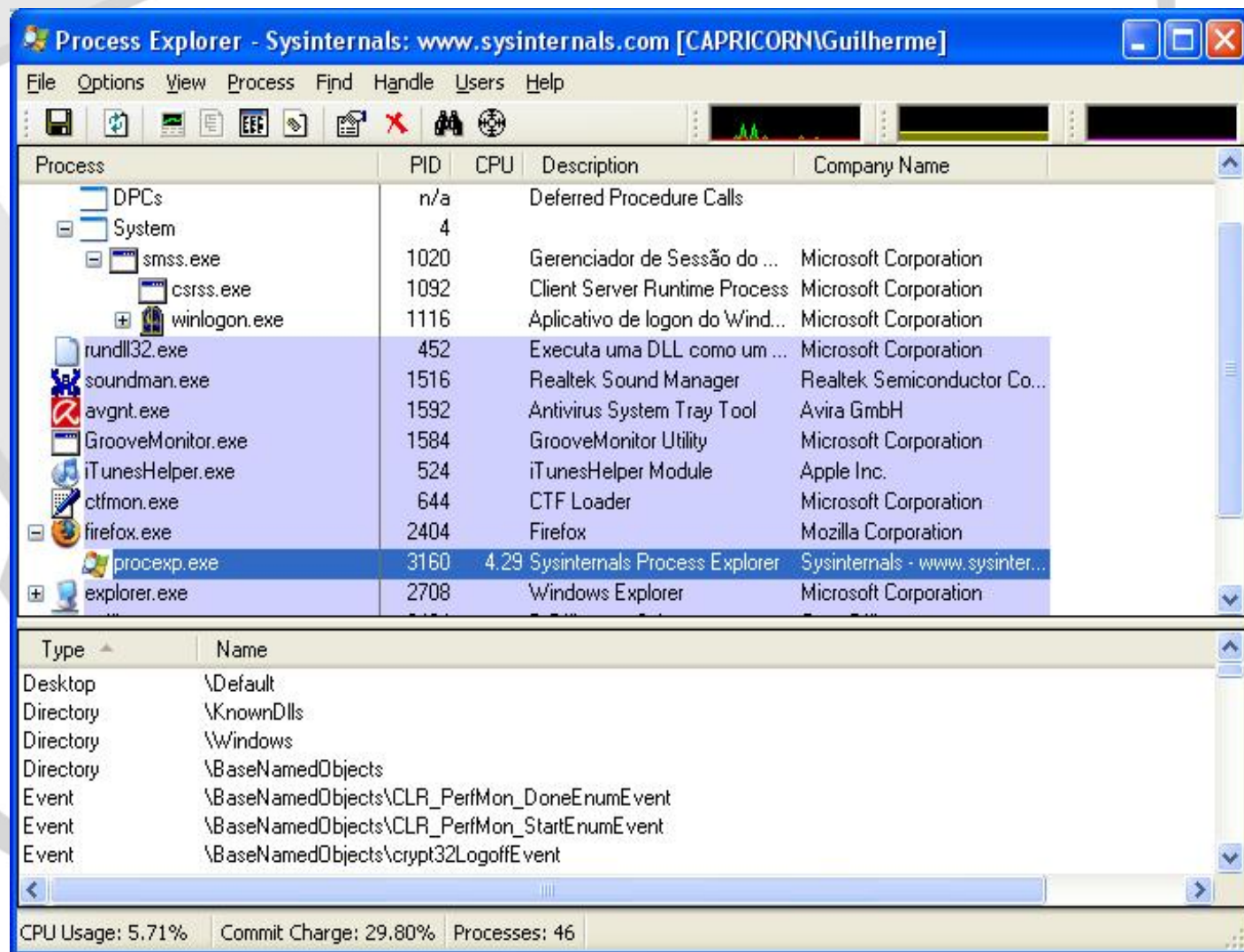
Analizando o Windows

- **Analise os aplicativos e finalize os desconhecidos/maliciosos**
- **Analise também a aba processos**
- **Nunca se assuste com a interface dos utilitários**



Analizando o Windows

- Utilize também o Process Explorer



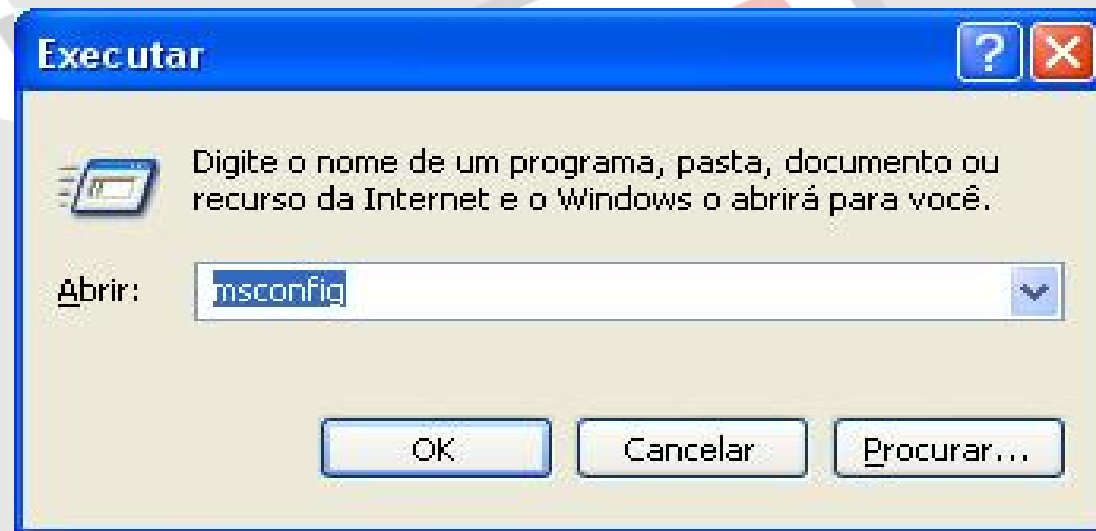
Analizando o Windows

- Analise quais aplicativos tem o seu início automático na inicialização do sistema
- Locais:
 - Registro (não abordado aqui)
 - Arquivo *win.ini* (não abordado aqui)
 - MSconfig



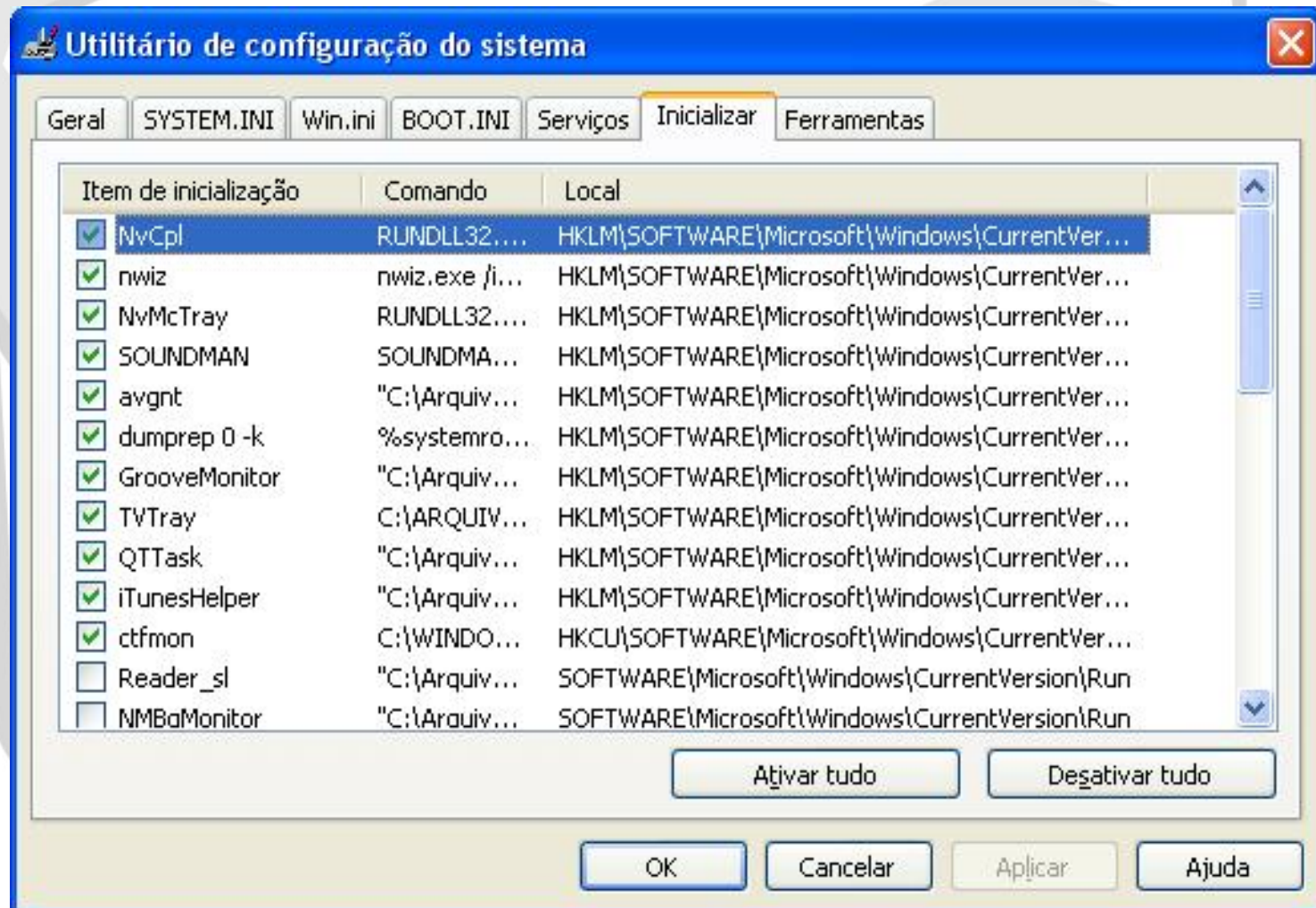
Analizando o Windows

- Execute o “msconfig” através do Executar do Windows
- Pode ser chamado com “Win + r”



Analizando o Windows

- Analise a aba Inicializar



Analizando o Windows

- **Faça pesquisa sobre processos desconhecidos**
- **Desabilite os desnecessários e indesejados**
- **Processos não catalogados na rede devem ser tratados com cautela**



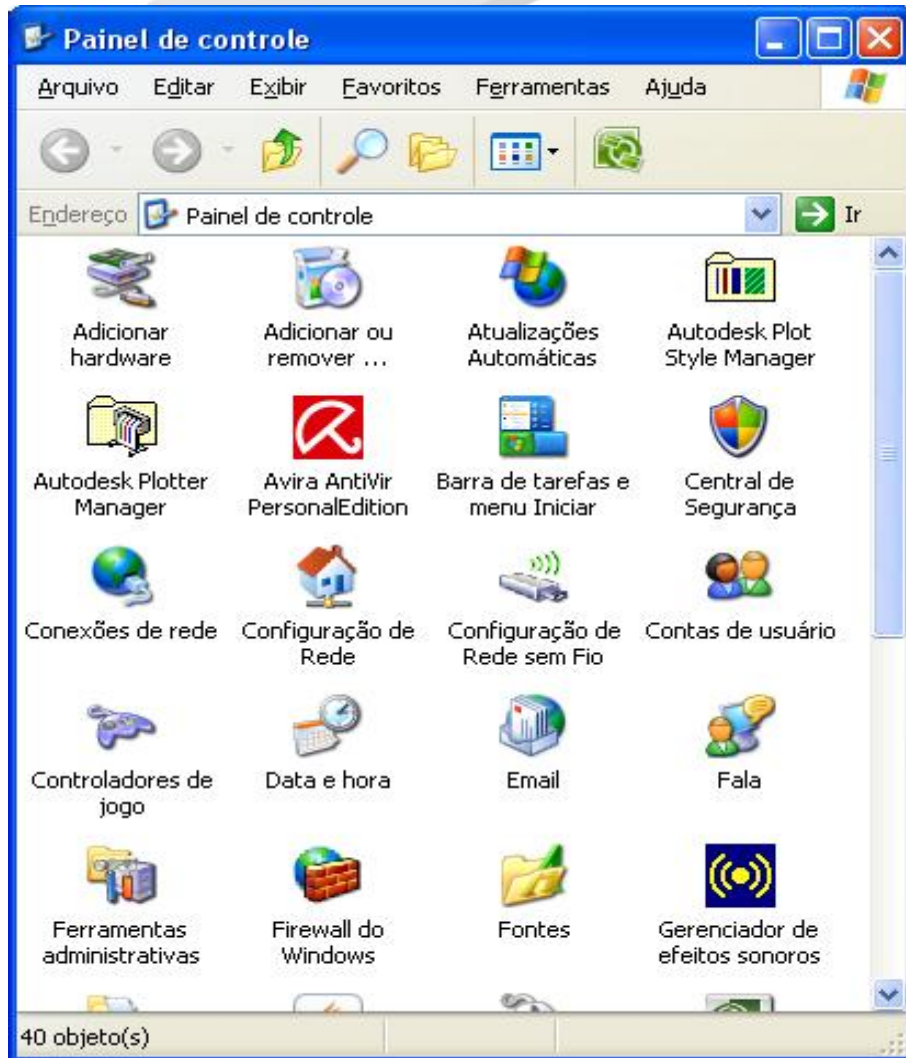
Analizando o Windows

- **Remova programas indesejados**
- **Utilize o Painel de Controle**
- **Pode ser acessado através do Iniciar**
- **Existem dois modos de exibições do Painel**



Analizando o Windows

Modo Clássico



Modo Categoria

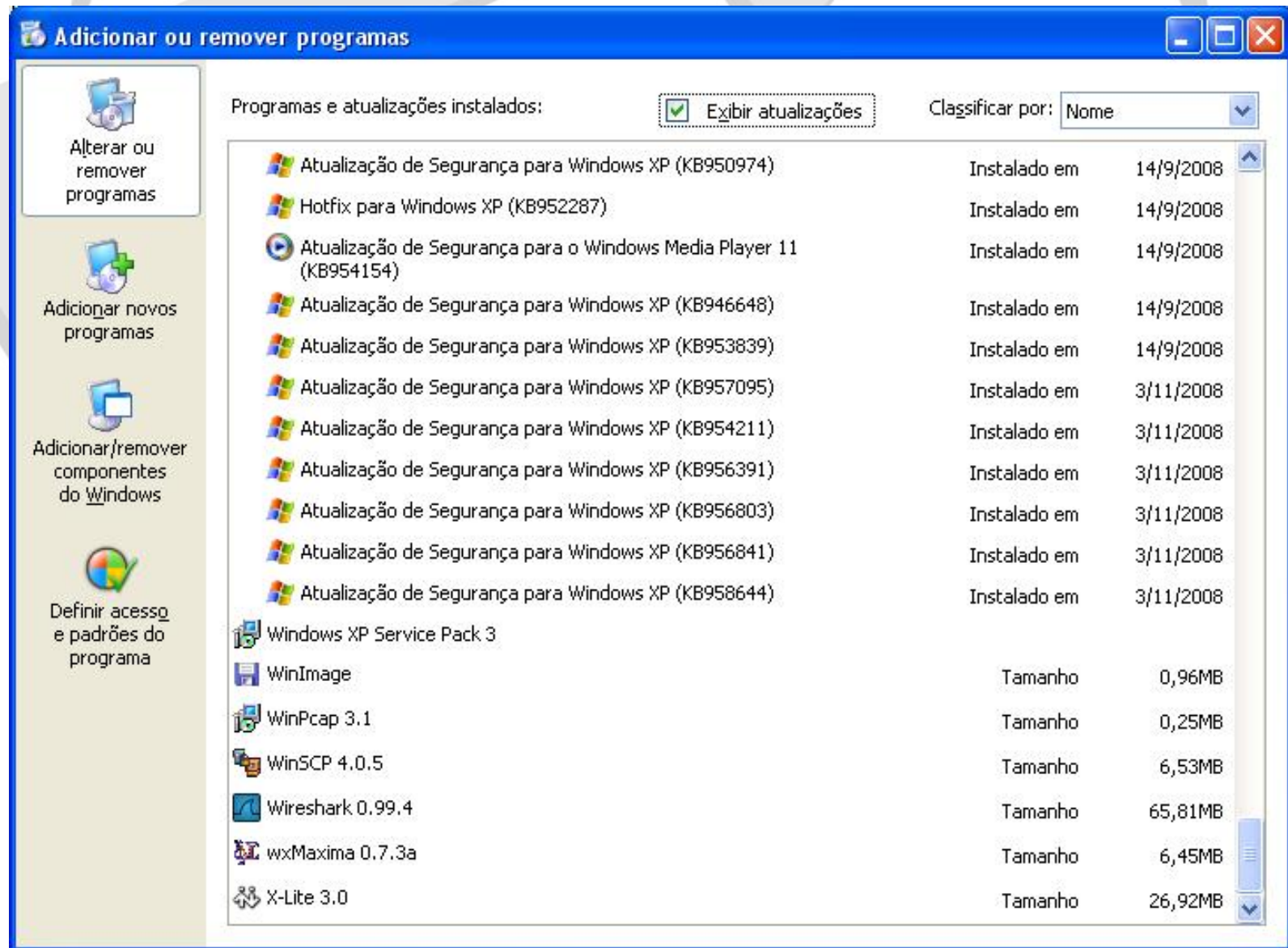


Analizando o Windows

- **Utilize o Adicionar ou remover programas**
- **Escolha exibir atualizações**
- **Nunca delete a pasta de um programa para tentar removê-lo**



Analizando o Windows



Analizando o Windows

Boas Práticas para atualizações de Programas

- **Nunca execute atualizações recebidas por email**
- **Visite os sites oficiais e/ou utilize as ferramentas de atualizações oficiais**
- **Para facilitar, guarde uma lista com o nome e site dos programas instalados**



Analizando o Windows

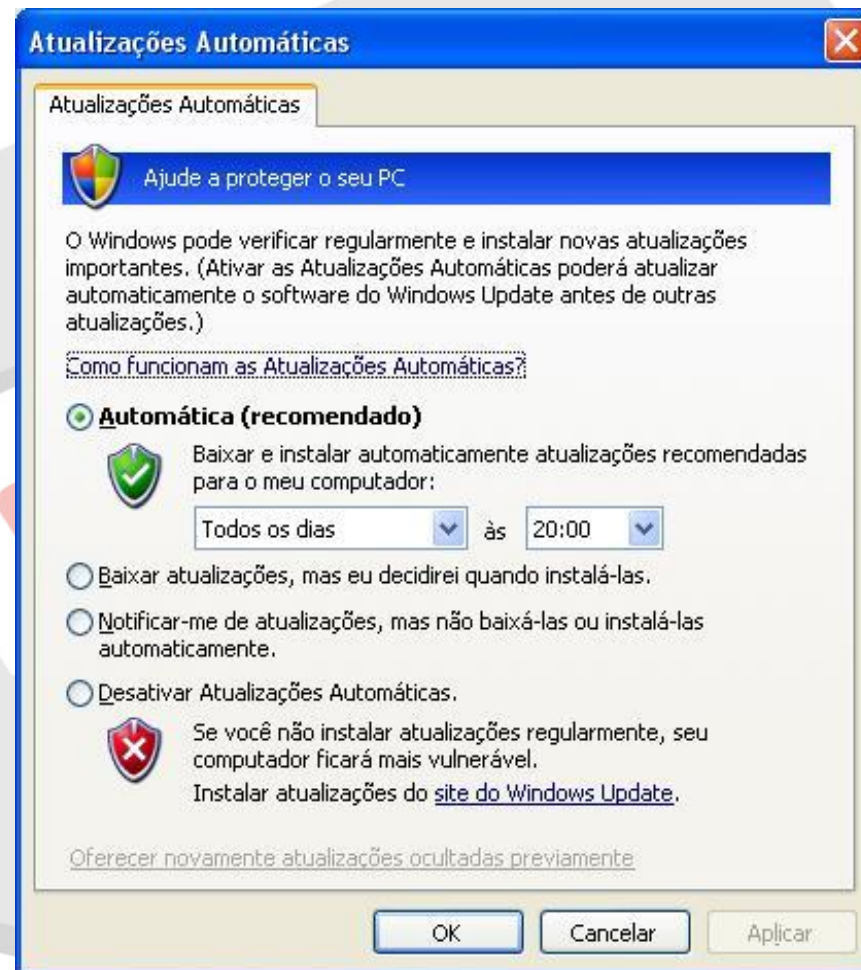
- **Certifique-se de que o Windows está atualizado**
 - **Execute o aplicativo “Atualizações Automáticas” no painel de controle**
 - **nunca desabilite as atualizações**
 - **escolha a opção mais adequada**



Analizando o Windows

- **Certifique-se de que o Windows está atualizado**

“Atualizações Automáticas”



Analizando o Windows

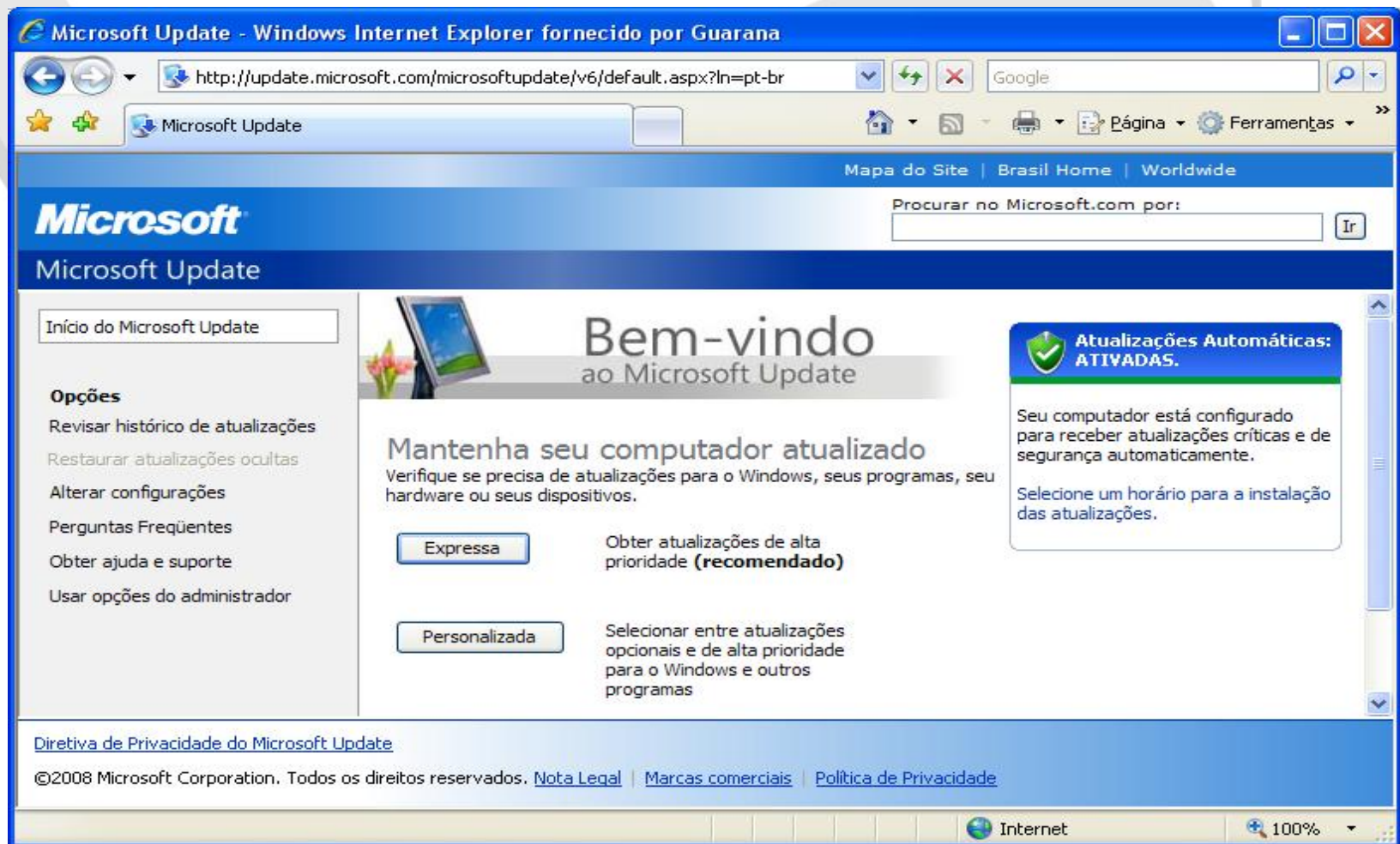
- **Certifique-se de que o Windows está atualizado**
 - **Execute o aplicativo “Microsoft Update” no menu Iniciar**
 - **faça uma busca online por atualizações**
 - **nunca deixe de instalar as críticas**



Analizando o Windows

- Certifique-se de que o Windows está atualizado

“Microsoft Update”



Testando a exposição do Windows

- **Faça testes online:**
 - na máquina
 - nos processos
 - no navegador
 - com Antivírus online

GRIS



Testando a exposição do Windows

- na máquina

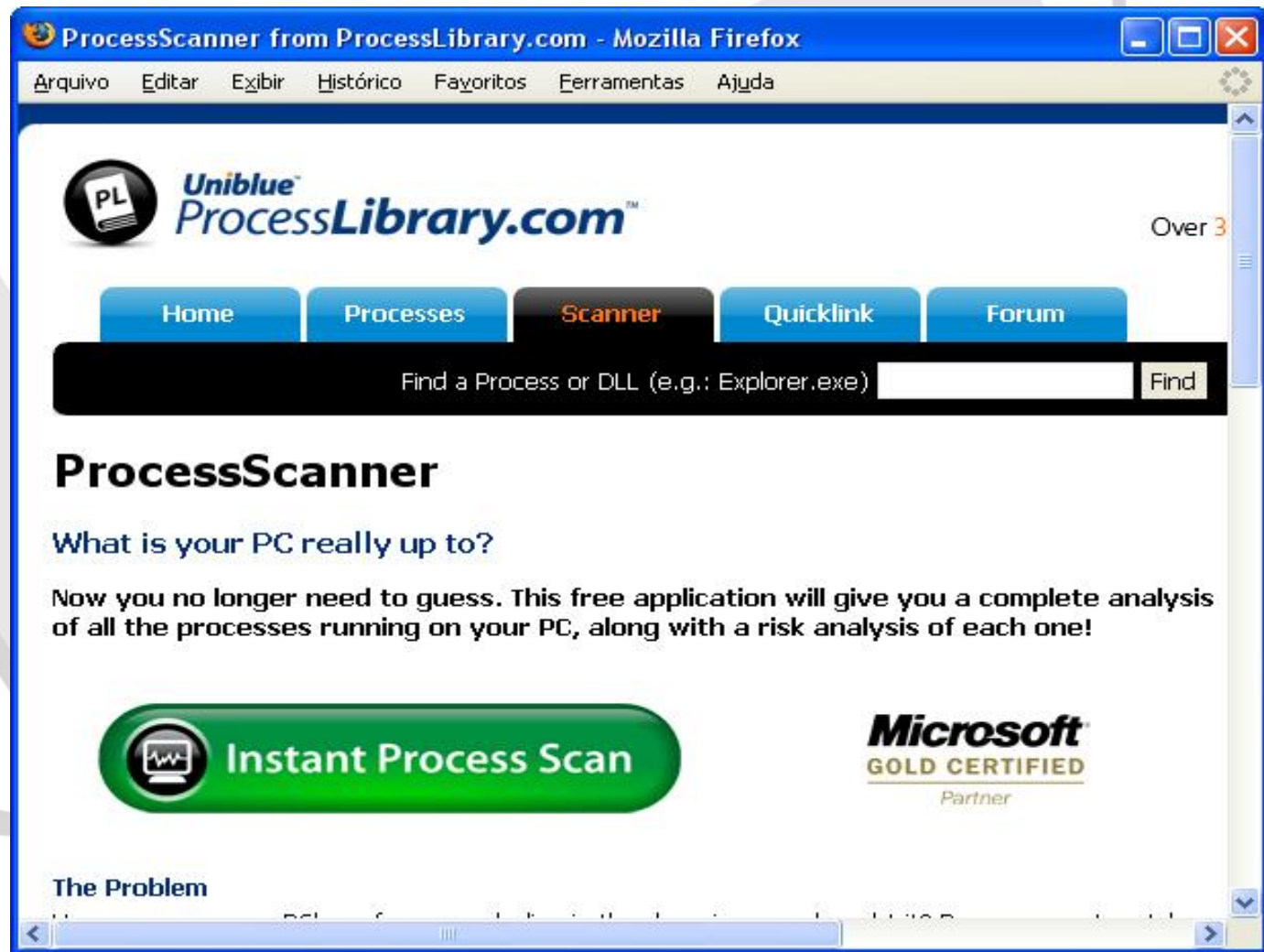
<http://www.grc.com/intro.htm>



Testando a exposição do Windows

- nos processos

<http://www.processlibrary.com/processscan/>



Testando a exposição do Windows

- no navegador

<http://bcheck.scanit.be/bcheck/>



The screenshot shows a Mozilla Firefox browser window titled "Browser Security Test - Mozilla Firefox". The address bar shows the URL <http://bcheck.scanit.be/bcheck/>. The page features the Scanit logo (a polar bear) and the text "browser security test".

Test Your Browser's Security Now

Careful! The test will try to crash your browser! Close all other browser windows before starting and bookmark this page. If your browser crashes during the test, restart it and return to this page. It will show which vulnerability crashed your browser and offer you to continue the test or view the results.

The test requires persistent cookies to be enabled. The cookie is used to restore your session after browser crash.

Your browser reports to be: "Mozilla/5.0 (Windows; U; Windows NT 5.1; pt-BR; rv:1.8.1.11) Gecko/20071127 Firefox/2.0.0.11 GoogleToolbarFF GoogleToolbarFF GoogleToolbarFF GoogleToolbarFF GoogleToolbarFF"

Browser name: Firefox
Version: 2.0.0.11
Platform: Windows XP

☒ Only test for bugs specific to my type of browser

scanit
The security company

About Browser Test

- [Browser test home](#)
- [Feedback](#)
- [Browser test FAQ](#)
- [What vulnerabilities we test](#)
- [Test statistics](#)
- [Help! My browser is hijacked](#)
- [Get notified about new tests](#)

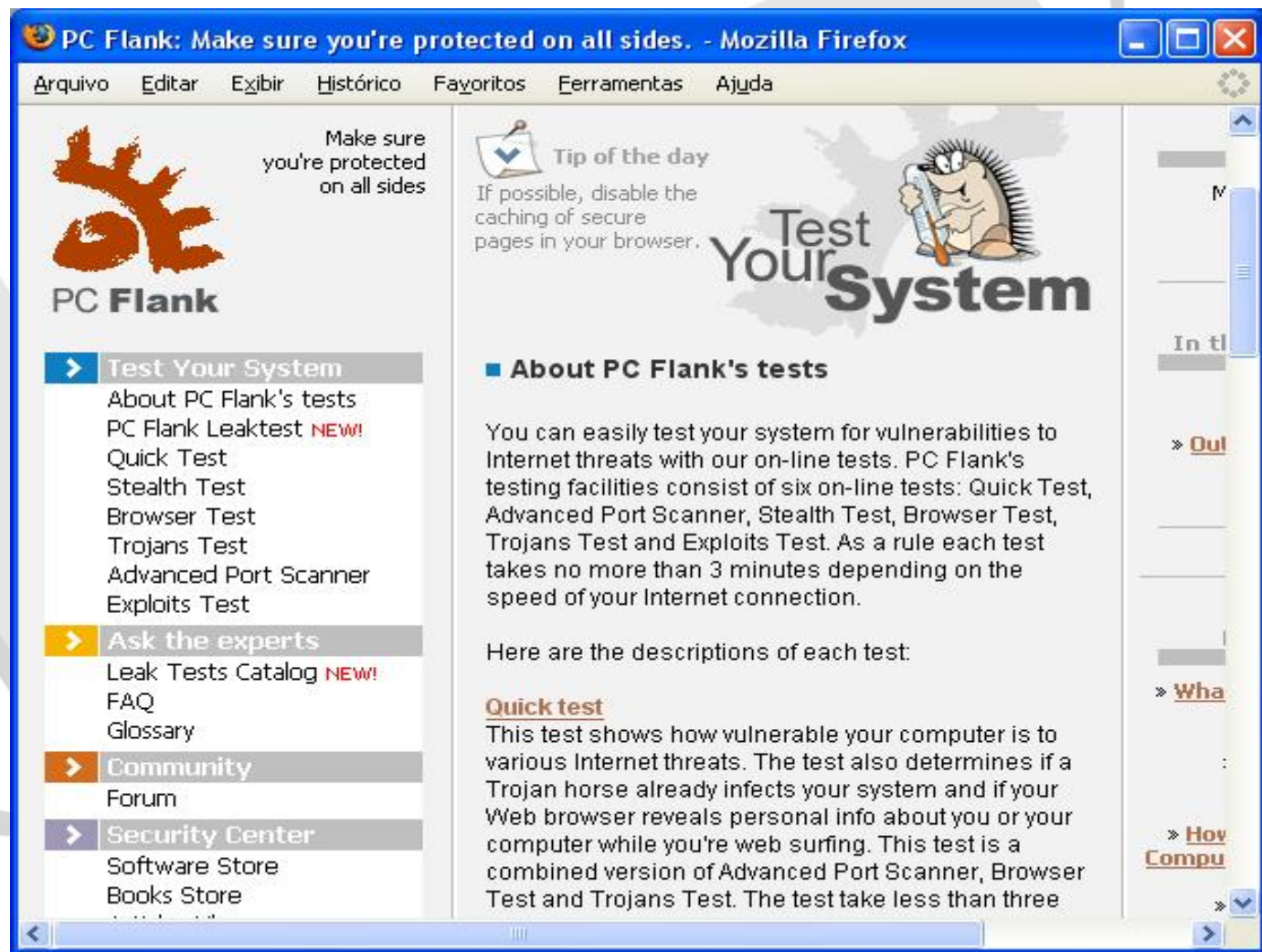
Security testing
Scanit offers penetration tests, vulnerability assessments and web application audits.

Learn ethical hacking.
Scanit offers 5-day training on ethical hacking.



Testando a exposição do Windows

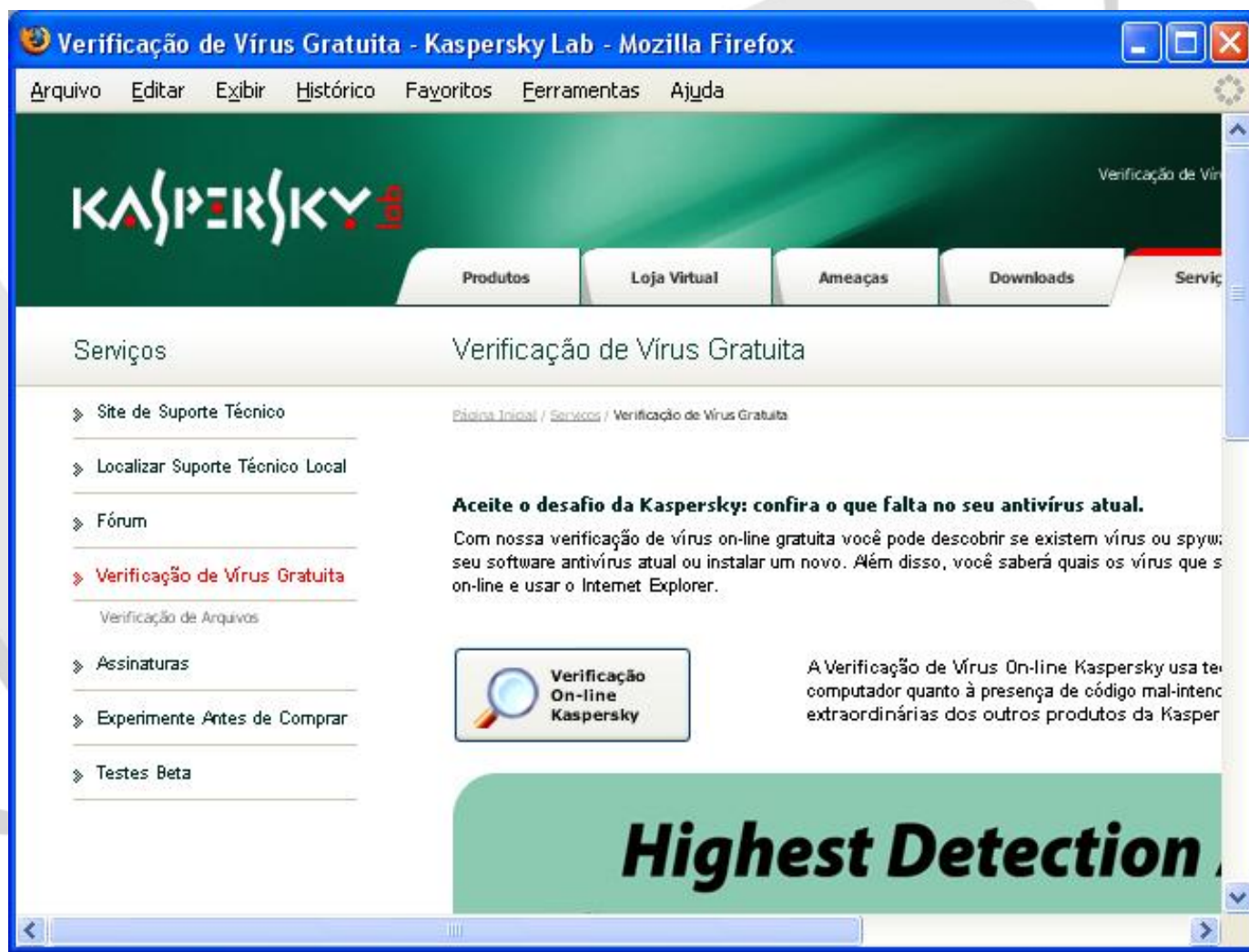
- no navegador e na máquina
<http://www.pcflank.com/>



Testando a exposição do Windows

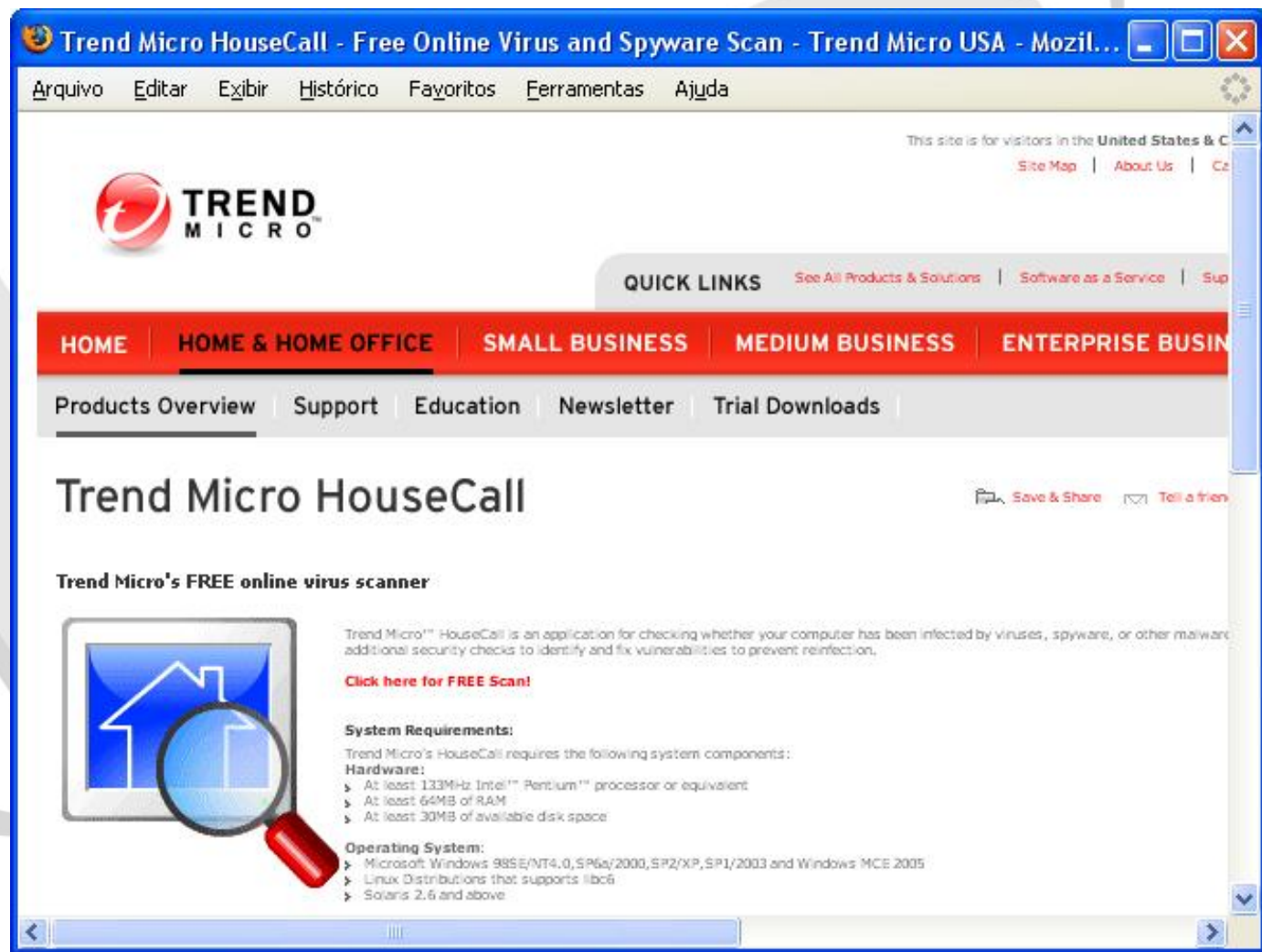
- com Antivírus Online

<http://www.kaspersky.com.br/virusscanner/>



Testando a exposição do Windows

- com Antivírus Online (2ª opção)
<http://housecall.trendmicro.com/>



Testando a exposição do Windows

- **Faça testes offline:**
 - **enumerando compartilhamentos de rede**
 - **enumerando portas abertas**
 - **enumerando conexões ativas**
 - **executando antivírus offline**
 - **executando anti-rootkits**



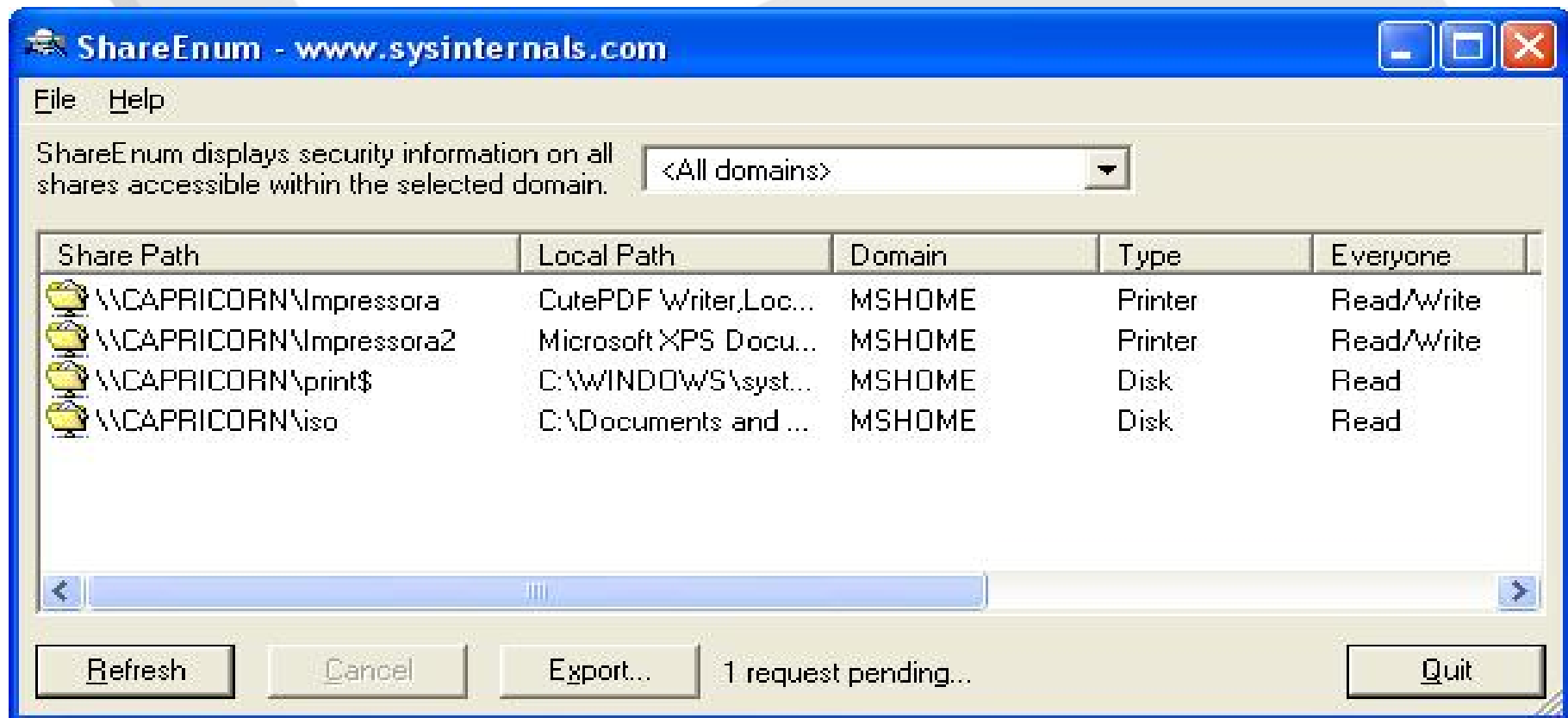
Testando a exposição do Windows

- **Enumerando compartilhamentos de rede**
 - só habilite quando necessário
 - nunca compartilhe pastas do sistema
 - utilize o ShareEnum



Testando a exposição do Windows

- Utilizando o ShareEnum
 - busca por domínios
 - busca por IP's



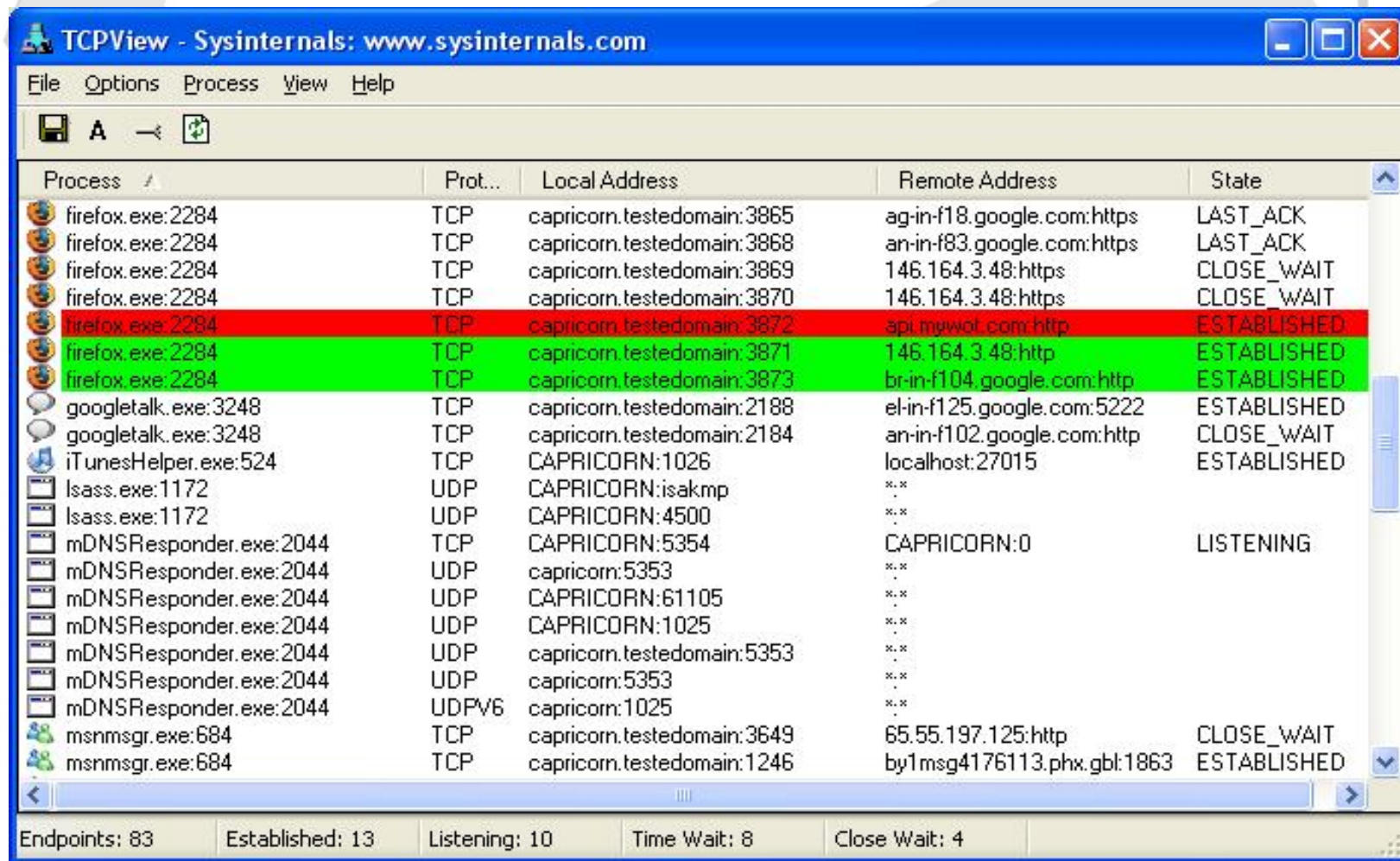
Testando a exposição do Windows

- **Enumerando portas abertas e conexões ativas**
 - só abra portas quando necessário
 - sempre utilize um Firewall
 - utilize o TCPView



Testando a exposição do Windows

- Utilizando o TCPView
- finalize os processos indesejados



The screenshot shows the TCPView application window from Sysinternals. The window title is "TCPView - Sysinternals: www.sysinternals.com". The menu bar includes "File", "Options", "Process", "View", and "Help". The toolbar has icons for saving, refreshing, and other functions. The main table displays network connections with columns for Process, Protocol, Local Address, Remote Address, and State. The table is filtered to show connections for the process "A". The status bar at the bottom shows summary statistics: Endpoints: 83, Established: 13, Listening: 10, Time Wait: 8, Close Wait: 4.

Process	Prot...	Local Address	Remote Address	State
firefox.exe:2284	TCP	capricorn.testedomain:3865	ag-in-f18.google.com:https	LAST_ACK
firefox.exe:2284	TCP	capricorn.testedomain:3868	an-in-f83.google.com:https	LAST_ACK
firefox.exe:2284	TCP	capricorn.testedomain:3869	146.164.3.48:https	CLOSE_WAIT
firefox.exe:2284	TCP	capricorn.testedomain:3870	146.164.3.48:https	CLOSE_WAIT
firefox.exe:2284	TCP	capricorn.testedomain:3872	api.mywot.com:http	ESTABLISHED
firefox.exe:2284	TCP	capricorn.testedomain:3871	146.164.3.48:http	ESTABLISHED
firefox.exe:2284	TCP	capricorn.testedomain:3873	br-in-f104.google.com:http	ESTABLISHED
googletalk.exe:3248	TCP	capricorn.testedomain:2188	el-in-f125.google.com:5222	ESTABLISHED
googletalk.exe:3248	TCP	capricorn.testedomain:2184	an-in-f102.google.com:http	CLOSE_WAIT
iTunesHelper.exe:524	TCP	CAPRICORN:1026	localhost:27015	ESTABLISHED
lsass.exe:1172	UDP	CAPRICORN:isakmp	..	
lsass.exe:1172	UDP	CAPRICORN:4500	..	
mDNSResponder.exe:2044	TCP	CAPRICORN:5354	CAPRICORN:0	LISTENING
mDNSResponder.exe:2044	UDP	capricorn:5353	..	
mDNSResponder.exe:2044	UDP	CAPRICORN:61105	..	
mDNSResponder.exe:2044	UDP	CAPRICORN:1025	..	
mDNSResponder.exe:2044	UDP	capricorn.testedomain:5353	..	
mDNSResponder.exe:2044	UDP	capricorn:5353	..	
mDNSResponder.exe:2044	UDPV6	capricorn:1025	..	
msnmsgr.exe:684	TCP	capricorn.testedomain:3649	65.55.197.125:http	CLOSE_WAIT
msnmsgr.exe:684	TCP	capricorn.testedomain:1246	by1msg4176113.phx.gbl:1863	ESTABLISHED

Endpoints: 83 Established: 13 Listening: 10 Time Wait: 8 Close Wait: 4



Testando a exposição do Windows

- **Executando Antivírus offline**
 - **certifique-se de que o Antivírus está atualizado**
 - **configure o seu nível de detecção**
 - **escolha um que possua scanner em real-time**



Testando a exposição do Windows

- **Executando Antivírus offline**
- **alguns bons antivírus grátis:**
 - **Avira Antivir** – Eleito o melhor pela Av-Test.org (9/2008)
 - **AVG Free**
 - **Avast Antivirus**
 - **ClamWin**



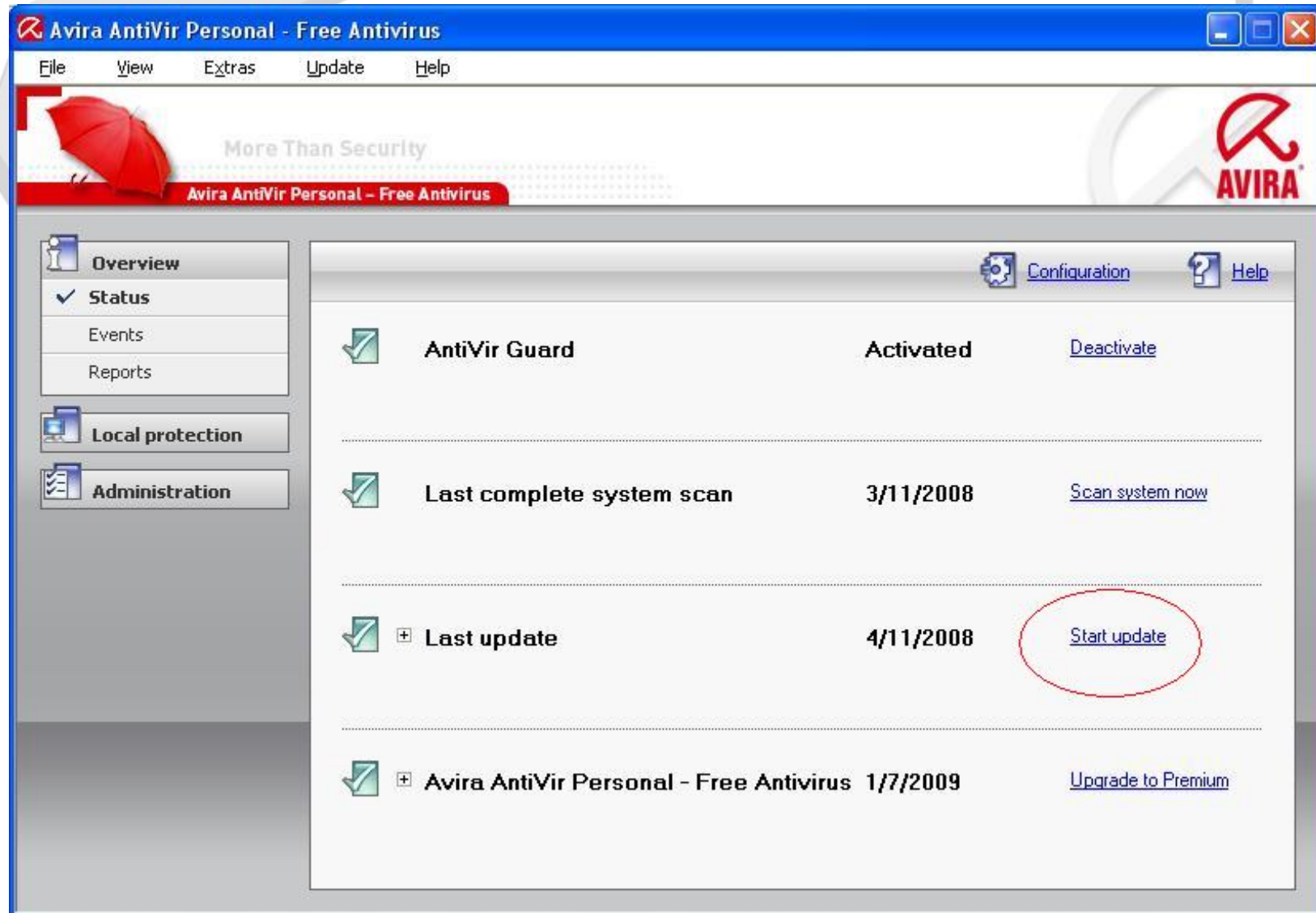
Testando a exposição do Windows

- **Executando Antivírus offline**
- **Usaremos o Antivir**
- **3 Passos:**
 - 1) **Atualizar o programa**
 - 2) **Configurar alto nível de detecção**
 - 3) **Executar**



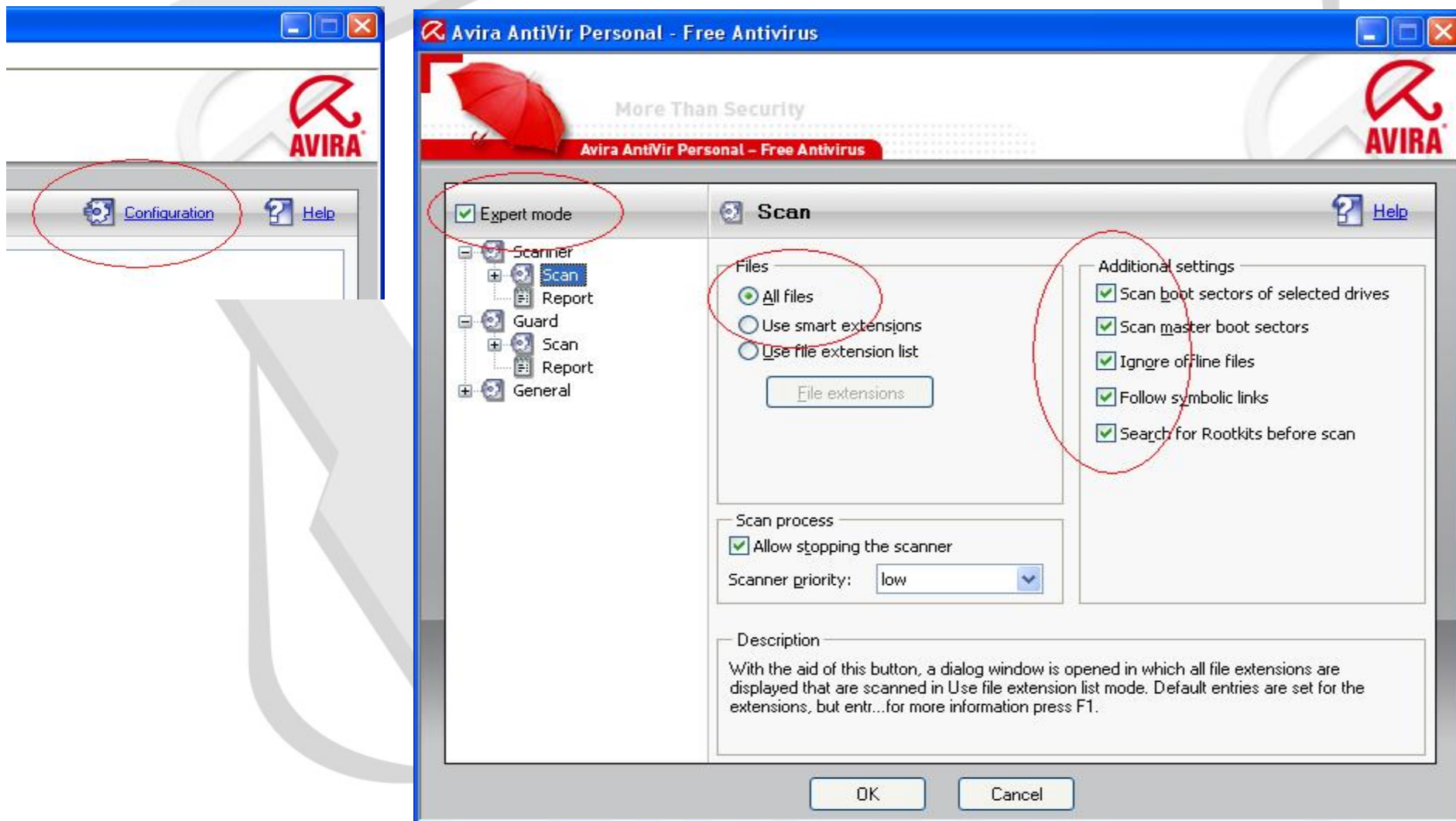
Testando a exposição do Windows

1) Atualizando o programa



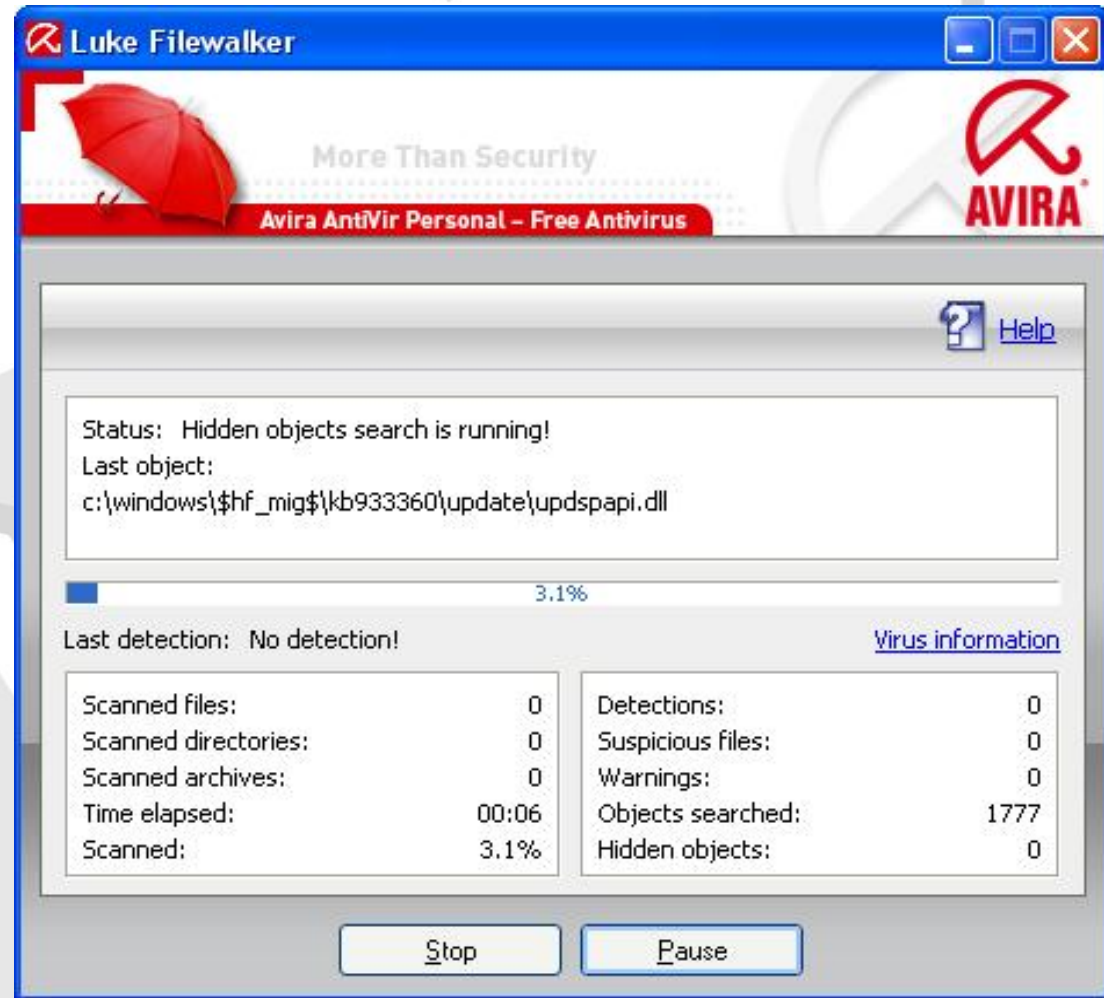
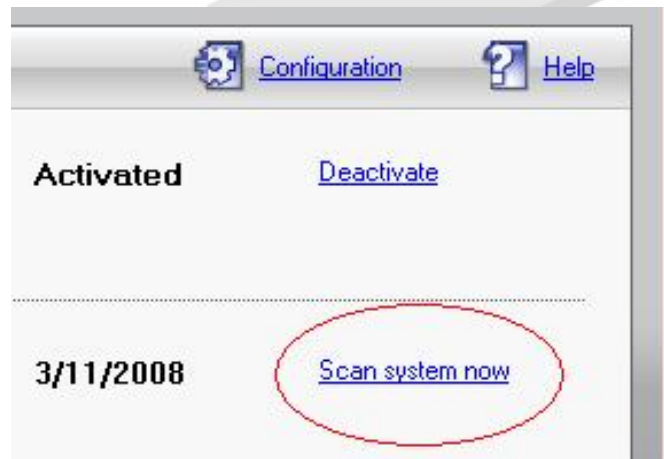
Testando a exposição do Windows

2) Configurando alta detecção



Testando a exposição do Windows

3) Executando o programa



Testando a exposição do Windows

3) Executando o programa



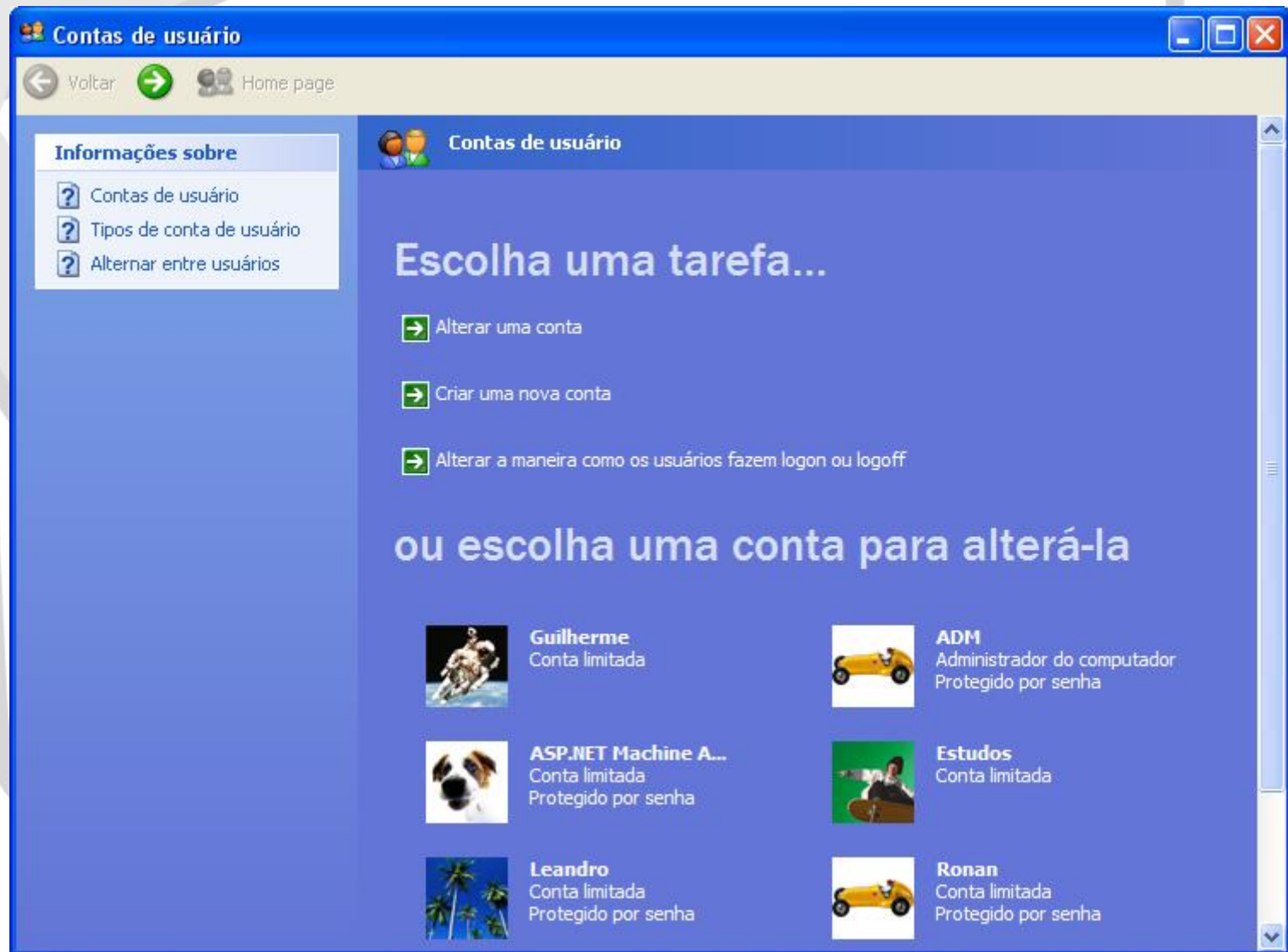
Boas práticas para o Windows

- **Gerenciando contas de usuários**
 - **sempre que possível, utilize contas limitadas**
 - **coloque senhas fortes para os usuários**
 - **execute o aplicativo “Contas de Usuários” pelo Painel de Controle**
 - **dicas de como escolher uma senha em <http://www.gris.dcc.ufrj.br/artigos.php>**



Boas práticas para o Windows

- Gerenciando contas de usuários



Boas práticas para o Windows

- Removendo arquivos de forma segura

ENQUETE:

“É possível apagar seguramente com “Shift + Delete”? ”



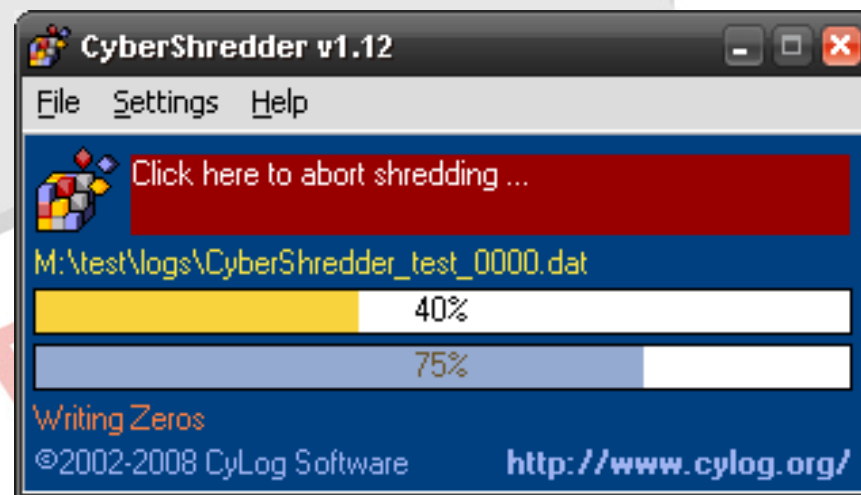
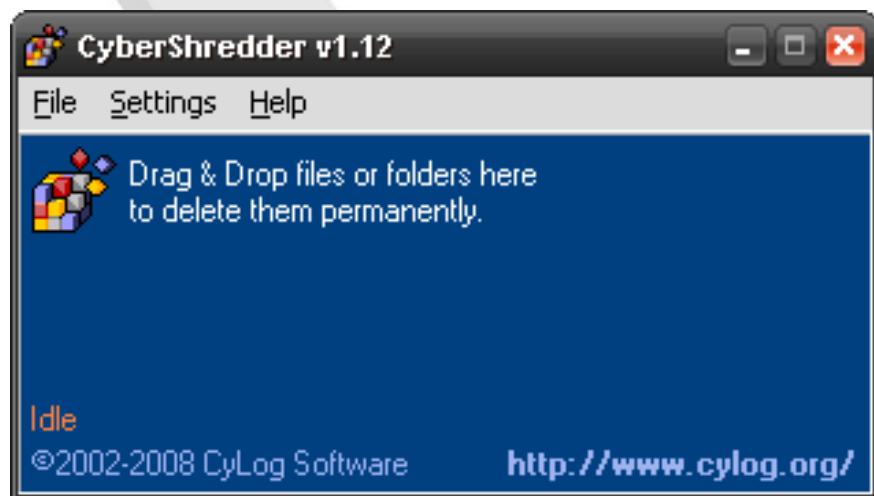
Boas práticas para o Windows

- **Removendo arquivos de forma segura**
 - **cuidado ao deletar arquivos sigilosos**
 - **sempre use programas que sobrescrevam o arquivo no disco**
 - **um exemplo é o CyberShredder**



Boas práticas para o Windows

- Removendo arquivos de forma segura
- muito cuidado ao utilizar estes programas



Boas práticas para o Windows

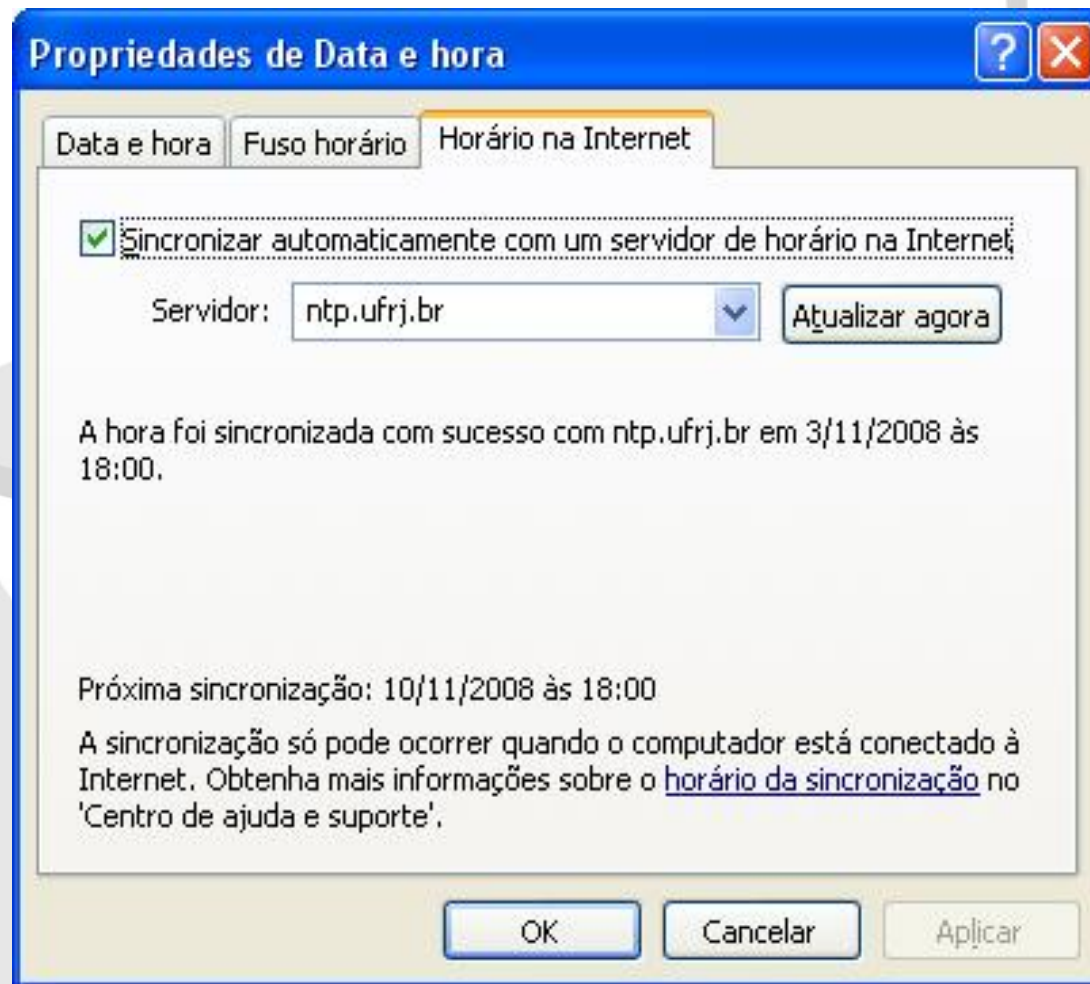
- **Acertando a hora do Windows**
 - **acesse através do relógio**
 - **utilize sempre servidores de NTP confiáveis**
 - **insira na aba “Horário na Internet” o seu servidor preferido**



Boas práticas para o Windows

- **Acertando a hora do Windows**

ntp.ufrj.br
a.ntp.br
b.ntp.br
c.ntp.br
d.ntp.br



Contatos GRIS

Caso não obtenha informações sobre algum processo ou esteja com dúvidas, envie um email, com ou sem os arquivos relacionados, para o email gris@gris.dcc.ufrj.br

Utilize também o formulário disponibilizado em <https://www.gris.dcc.ufrj.br/ri.php> para nos informar sobre incidentes



Conclusão

- **É fácil deixar o Windows mais seguro**
- **É fácil deixar de ser um simples usuário**
- **Utilize ferramentas de busca em caso de dúvidas**
- **Conheça algumas alternativas ao Windows**



Grupo de Resposta a Incidentes de Segurança

Documentos de apoio:

Cartilha de segurança para internet - <http://cartilha.cert.br>

15 Minute Security Guide: Windows XP LOCKDOWN! Por Jonny - <http://johnny.ihackstuff.com>

A Home User's Security Checklist for Windows por Scott - <http://www.securityfocus.com/columnists/220>

Microsoft Website - <http://www.microsoft.com>

Microsoft TechNet - <http://technet.microsoft.com/pt-br/library/default.aspx>

Av-Test Documents - <http://www.av-test.org/>



Grupo de Resposta a Incidentes de Segurança

Programas utilizados:

Process Explorer – SysInternals

<http://live.sysinternals.com/procexp.exe>

ShareEnum – SysInternals

<http://live.sysinternals.com/ShareEnum.exe>

TCPView – SysInternals

<http://live.sysinternals.com/Tcpview.exe>

Avira Antivir Personal

<http://www.free-av.com/>

Avast Antivirus Home Edition

<http://www.avast.com/por/download-avast-home.html>

AVG Antivirus Free Edition

<http://free.avg.com/>

Grupo de Resposta a Incidentes de Segurança
Departamento de Ciência da Computação
Instituto de Matemática
Universidade Federal do Rio de Janeiro



Grupo de Resposta a Incidentes de Segurança

Programas utilizados:

Cyber Shredder - Cylog

<http://www.cylog.org/utilities/cybershredder.jsp>

Ferramentas da SysInternals

<http://technet.microsoft.com/en-us/sysinternals/default.aspx>

OBS: Ferramentas similares às da SysInternals podem ser encontradas também em

<http://www.foundstone.com/us/resources-free-tools.asp>

