Ministério da Agricultura, Pecuária e Abastecimento

Instruções Técnicas 4

ISSN
Outubro, 2001
Campinas, SP


# Instalação de Antivírus na Servidora de Mail: Uma Opção para Impedir Ataques de Vírus Anexados a E-mail

Marcelo Gonçalves Narciso[1]

Um dos grandes desafios dos administradores de redes é quanto à segurança de sua rede. Existem vários tipos de ataques a redes, e um dos mais comuns atualmente tem sido os vírus anexados a mensagens eletrônicas (e-mail). Casos em que os desastres ocorreram devido a vírus existem centenas registrados na Internet (Carnegie Mellon University, 2001a, 2001b).

Devido ao despreparo ou falta de conhecimento ou cuidados quanto a abertura de mensagens com arquivos anexados, os usuários muitas vezes são vítimas de vírus. Em alguns casos, o usuário só percebe a existência de vírus quando o mesmo já causou algum dano em seu micro. Assim, o ideal é evitar que a mensagem com vírus chegue ao usuário. Para isto, o vírus deverá ser detectado na servidora de mails e a mensagem deverá ser descartada. Existem alguns softwares livres (freeware) na Internet, para ambiente unix, que podem fazer este papel, tal como o Amavis (www.amavis.org). Para ambiente Microsoft Windows existem outros tipos de softwares (ver www.microsoft.com), porém não serão enfocados neste trabalho.

Uma vez que é colocado um software antivírus na servidora de mail e o software detecta a presença de vírus em arquivo anexado a mail, a rede local ficará protegida e o usuário final não será, conseqüentemente, atingido por vírus anexado a arquivos. Porém, é necessário que o antivírus na servidora esteja sempre atualizado.

Este trabalho visa descrever um mecanismo de defesa na servidora de mail quando esta recebe mensagem com arquivos anexados e com vírus. Este mecanismo é muito útil pois evita transtornos para os usuários, mesmo os mais leigos no assunto, e também permite ao administrador, além de prevenir problemas com vírus, verificar se sua rede tem sido alvo de ataques e também notificar os sites de onde os vírus têm sido enviados, ajudando assim a diminuir o tráfego de vírus na Internet.

## Antivírus no Servidor de Mail

Vírus que vem via arquivo anexado a mensagens eletrônicas têm se tornado um dos grandes problemas de segurança na Internet. Desta forma, uma política

[1] *Doutorado em Computação Aplicada, Pesquisador da Embrapa Informática Agropecuária, Caixa Postal 6041, Barão Geraldo, 13083-970 – Campinas, SP. (narciso@cnptia.embrapa.br)*

Embrapa

de uso de antivírus em um site é de suma importância. Um antivírus pode ser instalado nas máquinas clientes (a maneira mais usual) e também na servidora. O ideal é ter antivírus tanto nas máquinas clientes como na servidora.

Na servidora, os arquivos anexados podem ser analisados de duas maneiras: ou pela extensão do arquivo (.exe, .bat, .com, etc.) ou pela varredura do arquivo (scan) para verificar se existe algum vírus.

Na análise da extensão do arquivo anexado a e-mail, simplesmente são barrados arquivos anexados que têm potencial de conter vírus. Algumas das extensões de arquivos anexados a mail que já trouxeram vírus, conforme Microsoft Corporation (2001) e Procmail (2001), são:

.exe, .com, .vbs, .pps, .bat, .pif, .js, .shs, .scr, .chm, .dll, .hta, .bas, .lnk, .isn, .ade, .adp, .cmd, .cpl, .crt, .hlp, .inf, .ins, .isp, .jse, .mdb, .mde, .msc, .msi, .msp, .mst, .pcd, .reg, .sct, .url, .vb, .vbe, .wsc, .wsf, .wsh, .shl. Atualmente, tem-se afirmado que já existe arquivos .pdf que já tem catalogado vírus anexado (ver site http://idgnow.terra.com.br/idgnow/pcnews/2001/08/0035).

Um bom programa para fazer a função citada de análise de extensões de arquivos é o Procmail (www.procmail.org).

Na análise por varredura do arquivo e busca por vírus conhecido, o programa de varredura verifica se existe algum vírus anexado ao e-mail. Assim, se o arquivo não contiver vírus, o mesmo não será barrado, mesmo se a extensão for uma daquelas já citadas anteriormente (.exe, .bat, etc.). Um dos softwares para fazer este tipo de verificação que será enfocado neste trabalho é chamado de Amavis e é freeware (ver www.amavis.org). O Amavis contém um programa de varredura chamado scanmails, o qual divide a mensagem interna de um mail do arquivo anexado a este. Após a divisão dos conteúdos do mail, o scanmails ativa um programa de antivírus (por exemplo, NAI Virus Scan 4.x ou uvscan) que verifica se tem vírus conhecido anexado a e-mail. Após a verificação do uvscan, se não houver vírus, o scanmails prossegue no envio da mensagem. Se houver vírus anexado a arquivo, então o mail é barrado e arquivado em algum diretório na servidora, para verificação posterior do administrador do sistema, ou ainda, o mail é simplesmente apagado. O scanmails também funciona como um mailer local, isto é, um programa que entrega um mail, com auxílio do sendmail (ver www.sendmail.org), dentro de uma rede local.

O Amavis pode trabalhar em conjunto com o Procmail para aumentar a segurança de um site. Por exemplo, o vírus Sircam (Julho de 2001) apareceu e inundou a Internet através de mail com arquivos anexados. O vírus foi detectado, porém a vacina não apareceu logo em seguida. Demoraram alguns dias para a vacina estar disponível. Assim, neste ínterim, graças ao Procmail, muitos arquivos que tinham vírus Sircam foram barrados, impedindo assim que um site (por exemplo, a Embrapa Informática Agropecuária) sofresse conseqüências danosas. Naqueles dias, muitos sites da Embrapa foram infectados, causando transtornos a uma série de usuários.

## Configuração de antivírus na máquina servidora de mail

Para um melhor entendimento do processo de configuração do Amavis e Procmail, faz-se necessário discorrer um pouco sobre o Sendmail, software largamente empregado em sites para a entrega e recebimento de mails pela Internet e rede local.

### Funcionamento do programa responsável pela entrega e recebimento de mail - Sendmail

O Sendmail é um programa responsável pela entrega e envio de mail, de onde quer que ele venha (Sendmail Incorporation, 2001). As características principais do Sendmail são:

- Entrega imediata de mensagens para o endereço especificado.
- Interação com DNS (Domain Name Server, que resolve nomes de domínios da Internet) através de registros MX (mail exchange, variável configurada no DNS que determina o fato de uma máquina ser servidora de mail principal ou secundária da rede).
- Mensagens podem ser entregues por meio de programas que acessam outras redes, tais como UUCP e BITNET.

Quando um usuário qualquer (fulano@site.com.br, por exemplo), a partir de sua máquina da rede local, envia mail para outro usuário (beltrano@site1.gov.br, por exemplo), o processo do Sendmail que fica na servidora da rede, cujo domínio é site .com.br, deverá ler o endereço, determinar se é local ou não, e então enviar a mensagem para o endereço correto (beltrano@site1.gov.br). Para isto, o Sendmail tem uma série de regras, as quais estão cadastradas em seu arquivo de configuração, sendmail.cf. Este arqui-

vo de configuração é de suma importância para o bom funcionamento do Sendmail. Nele podem ser configurados uma série de parâmetros, tais como: diretórios onde ficam os arquivos de *aliases* da rede, *time out* de conexão, tempo limite para entregar uma mensagem, domínio da rede local, mecanismos para combater spam, etc. As regras que ficam no sendmail.cf têm o objetivo de fazer uma varredura no endereço do e-mail para onde vai a mensagem e escolher a forma como a mensagem vai ser enviada (se localmente ou para um site da Internet). Além disso, o sendmail.cf também tem regras para varrer o endereço de quem enviou a mensagem. Isto é útil para se combater spam, pois conforme o endereço, o mail poderá ser rejeitado ou não. Além disso, quem receber a mensagem deverá saber quem enviou.

De uma forma geral, o processo do sendmail da servidora recebe uma mensagem, identifica quem enviou e para quem a mensagem vai, verifica se o destinatário é da rede local ou não e, conforme o caso, escolhe um outro programa, chamado de mailer, para enviar a mensagem. Se a mensagem tiver destinatário com endereço da rede local, o sendmail escolhe o mailer local (usualmente são programas executáveis ou scripts, e os mais comuns são mail, mail.local, Procmail, ou scanmails) e envia a mensagem para o destinatário da rede local. Se a mensagem estiver endereçada para um usuário fora da rede local, o sendmail, através de uma série de rotinas (funções) que vem em seu pacote, envia o mail conforme os parâmetros estabelecidos no seu arquivo de configuração, o sendmail.cf (Costales & Allman, 1997). A Fig. 1 a seguir ilustra o funcionamento do sendmail.

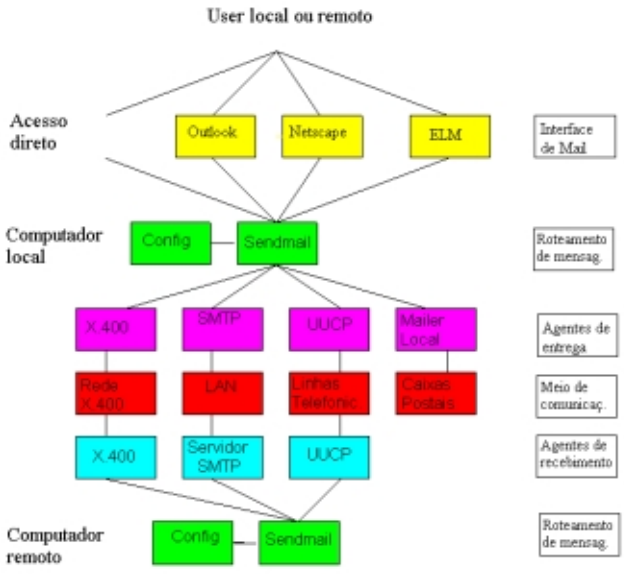


**Fig. 1.** Esquema do funcionamento do Sendmail.

Uma vez colocado um pequeno resumo sobre o sendmail, pode-se então discorrer sobre a instalação do mecanismo de se evitar vírus ou mails indesejáveis a partir da servidora de mail da rede local. O mecanismo é referenciado a partir do sendmail.cf. Quando uma mensagem chega a algum destinatário da rede local, o sendmail ativa o mailer local, o qual pode ser o Procmail ou Scanmails, conforme o que estiver configurado em sendmail.cf. Este mailer local, além da entrega do mail, irá fazer a verificação do arquivo anexado a mensagem, quando houver.

## Procmail

Conforme visto no item anterior, o Procmail é um mailer local. Para instalar o Procmail na máquina servidora de mail, é necessário que nesta esteja instalado a linguagem Perl, versão 5 (Perl Mongers, 2001) e um compilador C (gcc, por exemplo). O servidor de mail deverá então usar o Procmail para entrega local dos e-mails (mailer local). Em plataformas Solaris, AIX, HP e outros sistemas Unix, outros mailers locais são definidos inicialmente. Porém, basta instalar o Procmail e defini-lo como mailer local no sendmail.cf, para o caso do sistema estar usando o sendmail (ver www.sendmail.org). Neste trabalho, não será enfocado o postfix (similar ao sendmail), cujos detalhes podem ser vistos em www.postfix.org. No sendmail.cf, o trecho do programa onde ficará o Procmail é o seguinte:

```
Mlocal, P=/usr/bin/procmail, F=SAw5:/
|@glDFMPhsfn,
S=EnvFromL/HdrFromL, R=EnvToL/HdrToL,
          T=DNS/RFC822/X-Unix,
          A=procmail -Y -a $h -d $u
```

A instalação do Procmail (Versao 1.1, usada neste exemplo, ou superior) pode ser resumida da seguinte maneira:

1. obtenha o Procmail em www.procmail.org e descomprima o arquivo em algum diretório temporário (uncompress procmail.tar.Z e tar -xvf procmail.tar);
2. personalize o arquivo recusanexo.pl com seus dados e mensagens
   (ver site http://www.ppgia.pucpr.br/~borchardt/tools/; e
3. mova o diretório procmail.d para dentro do diretório /etc (o próprio pacote do Procmail sugere este passo). Não depende do sistema operacional visto que os scripts usados são em PERL;
4. pare o servidor de mail;
5. mova arquivo procmailrc para o diretório /etc (caso já exista o arquivo

/etc/procmailrc edite-o para incluir o conteúdo do arquivo novo no arquivo

/etc/procmailrc original)

Um exemplo de procmailrc para barrar vírus com as extensões citadas anteriormente seria:

```
# Versao 1.1, 25/04/2001. Uso e distribuicao de acordo com a licenca GNU.
#
:0 HB
*.filename*=?
*\".*\.(exe|com|vbs|pps|bat|mov|mpg|png|pif|js|shs|scr|chm|
dll|hta|bas|lnk|isn|ade|adp|cmd|cpl|crt|hlp|inf|ins|isp|j
se|mdb|mde|msc|msi|msp
|mst|pcd|reg|sct|url|vb|vbe|wsc|wsf|sh|wsh)
(=\?)?\"| /etc/procmail.d/recusanexo.pl
#
# fim do procmailrc
```

6. ajuste as permissões:
   cd /etc
   chmod 644 procmailrc
   chmod -R 755 procmail.d
   chown root.root procmailrc
   chown -R root.root procmail.d
7. reinicialize o servidor de mail;
8. envie um e-mail de teste para você mesmo, com qualquer uma das extensões existentes. Você deve receber os e-mails de aviso;
9. confira no arquivo /var/log/procmail.log o comportamento do procmail.

No arquivo sendmail.cf, o Procmail é definido como o mailer local. Assim, o Procmail sempre varre uma mensagem a procura de alguma extensão não permitida. Se encontrar alguma extensão não permitida, uma mensagem de aviso é enviada aos usuários (quem enviou e quem iria receber a mensagem, além do administrador do sistema). Um exemplo da mensagem é tal como abaixo:

*O e-mail abaixo foi descartado por conter um anexo executável.*
*Esta mensagem visa apenas sua informação; o remetente também foi informado do ocorrido.*
**_____*

** From: "Fulano da Silva" <fulano@cnptia.embrapa.br>*
** To: Beltrano*
** Subject: arquivos PAT*
** Date: Tue, 14 Aug 2001 17:24:41 -0300*
** File(s): PAT2000_d_dete.doc abono_pcs.rtf Backup de abono_pcs.wbk Backup de Índices_SISPEM 2001.wbk Backup de renquadramento_fapespv2.wbk Backup de renquadramento_fapespv3.wbk Boss_saad2000.doc Índices_SISPEM 2001.doc irpf2000.exe irpf2001.exe PAT2000_a_dete.doc PAT2000_b_dete.doc PAT2000_c_dete.doc*
**_____*

*Os arquivos anexados a mail que nao estao sendo aceitos pelo server de mail do CNPTIA sao aqueles que terminam com:*
*.exe, .com, .vbs, .pps, .bat, .pif, .js, .shs, .scr, .chm, .dll, .hta, .bas, .lnk, .isn, .ade, .adp, .cmd, .cpl, .crt, .hlp, .inf, .ins, .isp, .jse, .mdb, .mde, .msc, .msi, .msp, .mst, .pcd, .reg, .sct, .url, .vb,*
*.vbe, .wsc, .wsf, .wsh, .shl*
*SUPORTE-CNPTIA*
*(*mailto:postmaster@cnptia.embrapa.br*)*

Observe que os arquivos irpf2000.exe irpf2001.exe foram os responsáveis pelo Procmail ter impedido o mail de ter chegado a Beltrano.

## Amavis

Conforme citado anteriormente, o Amavis é um antivírus a ser instalado na servidora de mails. Os passos da instalação podem ser dados conforme a seguir:

1. obtenha a última versão do Amavis em www.amavis.org. No caso deste exemplo, a versão é 0.2.1;
2. Instale um antivírus na servidora. Como exemplo, existe o antivírus uvscan (NAI Virus Scan 4.x ). No site da McAfee tem os arquivos .dat (arquivos de definição de vírus), que são usados para capturar os vírus. Estes arquivos estão em ftp://ftp.mcafee.com/pub/datfiles/english. O arquivos .dat devem ser baixados diariamente ou semanalmente, pelo menos, para o antivírus não ficar desatualizado;
3. após descomprimir e aplicar o comando tar –xvf para a extração dos arquivos do pacote Amavis, execute o arquivo configure da seguinte maneira:

./configure —prefix=/usr —enable-exim —enable-exim-procmail –withnotifyreceiver

A opção —enable-exim-procmail faz com que o scanmails ative o procmail;

Após o configure ser executado com sucesso, execute os comandos:

- make (pode ser como um usuário qualquer
- make install (apenas como usuário root)

4. no arquivo sendmail.cf, troque o caminho do arquivo mail.local pelo caminho do scanmails e troque também mail.local por scanmails. Estes parâmetros estão na seção “Mlocal” do sendmail.cf;

5. com relação ao arquivo scanmails, um script escrito em perl, você deverá editá-lo e configurá-lo conforme as necessidades do site. Neste arquivo é configurado o antivírus. Aliás, o ./configure vai procurar onde está o antivírus na servidora e se ele é reconhecido pelo Amavis (ele reconhece vários). Alguns dos antivírus reconhecidos pelo Amavis são:

H+BEDV, Mcafee Antivirus, Dr. Solomon, Sophos Sweep, NAI Virus Scan 4.x, KasperskyLab AVP, KasperskyLab AVPDaemonClient, F-Secure Antivirus, Trend Micro FileScanner, CyberSoft vfind, e CAI InoculateIT (inocucmd).

Uma vez que o mailer local da servidora é o Scanmails, então este será sempre acionado quando um mail vier de fora da rede local para dentro da rede (ou da rede local para um outro usuário da rede local). O scanmails vai verificar os arquivos anexados para ver se tem vírus. Se tudo estiver bem, o scanmails vai passar o arquivo para o Procmail (conforme a extensão do arquivo, ele permite passar ou não). Se o Procmail permite a passagem do arquivo, então o arquivo é enviado ao seu destino. Se o Procmail não estiver configurado no Amavis (a opção —enable-exim-procmail não for atribuída ao comando ./configure), então, após a ação do scanmails, o mail é enviado ao destino ou então descartado, caso tenha vírus.

Quando um mail é barrado pelo Amavis, o usuário que iria receber a mensagem (recipient) e o usuário que mandou a mensagem (sender) são notificados pelo Amavis que um vírus foi enviado anexo a mensagem do mail e que a mensagem foi descartada. O administrador do sistema (rede local na qual o recipiente é um usuário) também recebe a notificação do sistema do que aconteceu. Segue um exemplo da mensagem que vai para o administrador.

*Subject: FOUND VIRUS IN MAIL from Beltrano@alterdata.com.br to fulano*
*Date: Tue, 14 Aug 2001 18:17:35 -0300 (EST)*
*From: postmaster*
*To: administrador do sistema*
*The attached mail has been found to contain a virus*
*Originally /usr/sbin/scanmails -f Beltrano@alterdata.com.br -Y -a -d fulano*
*The mail has been stored as /var/adm/virusmails/root/virus-20010814-1757*
*xxxxxxxxxxxxxxxxxxTue Aug 14 18:17:29 EST 2001xxxxxxxxxxxxxxxxxxxxxxxx*
*scanmails (0.2.1) called -f Beltrano@alterdata.com.br -Y -a -d fulano*
*FROM: Beltrano@alterdata.com.br*
*TO: fulano*
*maxlevel: 0*
*Contents of /var/tmp/scanmails1757/unpacked*
*/var/tmp/scanmails1757/unpacked:*
*total 3464*
*-rw-r—r— 1 root root 93 Aug 14 18:17 997823850.1775-0.sol*
*-rw-r—r— 1 root root 0 Aug 14 18:17 997823851.1775-1.sol*
*drwxr-xr-x 2 root root 512 Aug 14 18:17 SFX*
*-rw-r—r— 1 root root 1759744 Aug 14 18:17 WRHAGENDA.doc.com*

*/var/tmp/scanmails1757/unpacked/SFX:*
*total 4*
*Scanning /var/tmp/scanmails1757/unpacked/**
*Scanning file /var/tmp/scanmails1757/unpacked/997823850.1775-0.sol*
*Scanning file /var/tmp/scanmails1757/unpacked/WRHAGENDA.doc.com*
*/var/tmp/scanmails1757/unpacked/WRHAGENDA.doc.com*
*Found the W32/SirCam@MM virus !!!*
*Scanning file /var/tmp/scanmails1757/unpacked/997823851.1775-1.sol*
*/var/tmp/scanmails1757/unpacked/997823851.1775-1.sol*
*File too small to have a known virus.*

Observe que o arquivo WRHAGENDA.doc.com tinha o virus Sircam (na mensagem, tem a notificação Found the W32/SirCam@MM virus !!!). Este arquivo iria para fulano, enviado por Beltrano@alterdata.com.br.

Os arquivos .dat e outros arquivos importantes para o engine de varredura devem ser atualizados diariamente. Um possível script (em ambiente unix) para isto, supondo que os arquivos .dat sejam acessados do site da McAfee, seria:

```
#!/bin/sh –v

# Mudar para o diretório onde fica o antivírus
cd /usr/uvscan

/bin/rm -f .listing*
datdir="ftp://ftp.mcafee.com/pub/datfiles/english/"
uvdir=/usr/uvscan/mcafee

# Buscar o arquivo latest-dat.tar em ftp.mcafee.com
/usr/local/wget/bin/wget -q -O $uvdir/latest-dat.tar
$datdir/''/usr/local/wget/bin/wget -qnr $datdir && grep
tar .listing | awk {'print $4'}'

#extrair os arquivos para a atualização dos .dat e
outros arquivos
tar -xf $uvdir/latest-dat.tar
chmod -R 700 /usr/uvscan
/bin/rm /usr/uvscan/mcafee/latest-dat.tar
```

O programa citado (shell script) deverá estar sendo executado todos os dias, para então garantir que todas as atualizações feitas no dia no site da McAfee sejam efetuadas na servidora de mails.

## Conclusões

Vírus anexado a mensagens eletrônicas (e-mails) têm sido um dos ataques mais comuns a um site na Internet. Para combater estes ataques, deve-se instalar antivírus nas máquinas clientes e na servidora de mail. Isto aumenta consideravelmente a segurança de um site pois, antes da mensagem com arquivo anexado chegar ao usuário final, esta será analisada pelo antivírus da servidora, e só após passar pela servidora é que vai para o cliente, o qual também tem um antivírus em sua máquina, sendo uma segunda proteção. O limitante neste caso é a atualização do antivírus. Sem a atualização, vírus novos podem passar pelo servidor e pelas máquinas cliente.

Caso o antivírus esteja desatualizado, o Procmail entrará em ação e assim tem-se uma segurança extra contra possíveis vírus que possam estar anexados a e-mail e ainda não existam vacinas para o combate.

Este mecanismo também tem a vantagem de facilitar o trabalho do administrador de redes, evitando assim perda de horas de trabalho em remover vírus em máquina de usuários (isto quando houver vacina disponível). Além disso, o administrador pode saber de onde vem os arquivos com vírus anexados e informar ao site sobre o ocorrido e o administrador do site infectado por vírus então toma as devidas providências.

## Referências Bibliográficas

AMAVIS. **AMaViS - a mail virus scanner**. Disponível em: <http://www.amavis.org>. Acesso em: 15 ago. 2001.

CARNEGIE MELLON UNIVERSITY. Software Engineering Institute. **CERT Coordination Center**. Disponível em: <http://www.cert.org>. Acesso em: 12 nov. 2001a.

CARNEGIE MELLON UNIVERSITY. Software Engineering Institute**. CERT Coordination Center:** computer virus resources. Disponível em: <http://www.cert.org/other_sources/viruses.html>. Acesso em: 12 nov. 2001b.

COSTALES, B.; ALLMAN, E. **Sendmail**. 2. ed. rev. atual. Cambridge: O´Reilly, 1997. 997 p.

MICROSOFT CORPORATION. Microsoft Office. **Outlook e-mail security update - frequently asked questions**. Disponível em: <http://office.microsoft.com/assistance/2000/Out2ksecFAQ.aspx>. Acesso em: 28 set. 2001.

PERL MONGERS. **Pearl Mongers [homepage]**. Disponível em: <http://www.perl.org>. Acesso em: 28 set. 2001.

PROCMAIL. **Procmail homepage**: welcome to procmail.org: news flash: procmail version 3.22 released. Disponível em: <http://www.procmail.org>. Acesso em: 15 ago. 2001.

SENDMAIL INCORPORATION. **Sendmail homepage**: welcome to sendmail.org. Disponível em: <http://www.sendmail.org>. Acesso em: 15 ago. 2001.

**Instruções Técnicas, 4**

MINISTÉRIO DA AGRICULTURA, PECUÁRIA E ABASTECIMENTO

GOVERNO FEDERAL
Trabalhando em todo o Brasil

**Embrapa Informática Agropecuária**
**Área de Comunicação e Negócios**
Av. Dr. André Tosello s/nº
Cidade Universitária - "Zeferino Vaz"
Barão Geraldo - Caixa Postal 6041
13083-970 - Campinas, SP
Telefone/Fax: (19) 3789-5743
E-mail: sac@cnptia.embrapa.br

**1ª edição**