Webmail Seguro

José Gracia Neto *zegracia@cbpf.br*
Marita Maestrelli *marita@cbpf.br*

Outubro 2001

Prefácio

Aprimorando os recursos da Rede computacional do CBPF, acrescentamos maior mobilidade para o usuário com a instalação de uma interface para transmissão e recepção de mensagens capaz de ser acessada de qualquer computador cliente da Internet. Esta garante não apenas praticidade, mas também segurança e privacidade das mensagens dos usuários.

Uma das formas utilizadas para isto é o serviço de *Webmail* acrescido de encriptação de dados. Possuidor de uma interface simples e intuitiva, ele nada requer do usuário além de um *web browser*.

Esta Nota Técnica visa expor a importância e a praticidade de um serviço deste tipo em uma rede integrada à Internet, utilizando como exemplo o atualmente disponível na rede do CBPF.

Sumário

1 Organização deste documento

Visando o melhor entendimento deste documento, as seguintes variações tipográficas foram utilizadas:

- *Palavras em itálico* – correspondem aos termos técnicos e em língua inglesa utilizados. Todos contém explicação no **Glossário**;
- **Palavras em negrito** – são utilizadas para destacar itens e avisos importantes que o leitor deverá ter em mente;
- `Textos em tipo de letra não-proporcional` – reproduzem todo e qualquer texto que o leitor deverá poder visualizar em um terminal. Quando precedidos do tipo #, devem ser encarados como comandos a serem executados pelo leitor como *root* no console do sistema;
- `Textos envoltos em moldura` – possuem esta aparência para reproduzir trechos de arquivos a serem criados ou alterados.

Ao final deste documento, o leitor deverá ser capaz de julgar a necessidade de se utilizar tal serviço, bem como implementá-lo em ambientes UNIX e semelhantes.

2 Introdução

O serviço de correio eletrônico é uma das formas mais difundidas de manter a comunicação entre os participantes de uma rede de computadores, desde uma rede local (Intranet) à rede global (Internet).

A popularização (ainda recente) da Internet tornou este serviço vital para a forma contemporânea de fazer negócios. Infelizmente, tal importância o tornou um dos principais alvos de todos aqueles que desejam causar prejuízos, desde manipulação e roubo de informações à disseminação de diversas categorias de vírus, capazes de causar o caos nos computadores de suas vítimas.

Tal perspectiva leva administradores de redes a procurar por formas práticas aos usuários, que garantam o sigilo das informações, bem como certifiquem sua origem e seu destino.

Uma das formas utilizadas para este propósito é o serviço de *Webmail*, acoplado a uma forma de encriptação da transmissão de dados.

No que se diz respeito à rede do CBPF, foi recém-implementado um serviço deste tipo, o qual permite aos usuários acessarem suas mensagens eletrônicas diretamente de suas contas no servidor de correio eletrônico, a partir de qualquer computador que possua um navegador de páginas HTML (como o *Netscape* e o *Internet Explorer*, por exemplo, conhecidos genericamente como *web browsers*).

Este *Webmail* é baseado no programa IMP, um projeto *Open Source* (de código aberto) desenvolvido pela comunidade da Internet, inteiramente feito em linguagem PHP.

Este *Webmail* faz uso de SSL (*Secure Socket Layer*) sobre o serviço de conexão ao servidor de páginas da *web* e sobre o serviço transporte de mensagens do servidor ao cliente. Tal condição promove de forma transparente ao usuário encriptação de dados, evitando que terceiros se apropriem de mensagens e senhas de acesso.

3 Topologia do *Webmail*

Para melhor entendermos o *Webmail*, apresentamos o diagrama funcional abaixo (fig. 1). Ao longo deste capítulo veremos cada um dos seus elementos e como se relacionam.

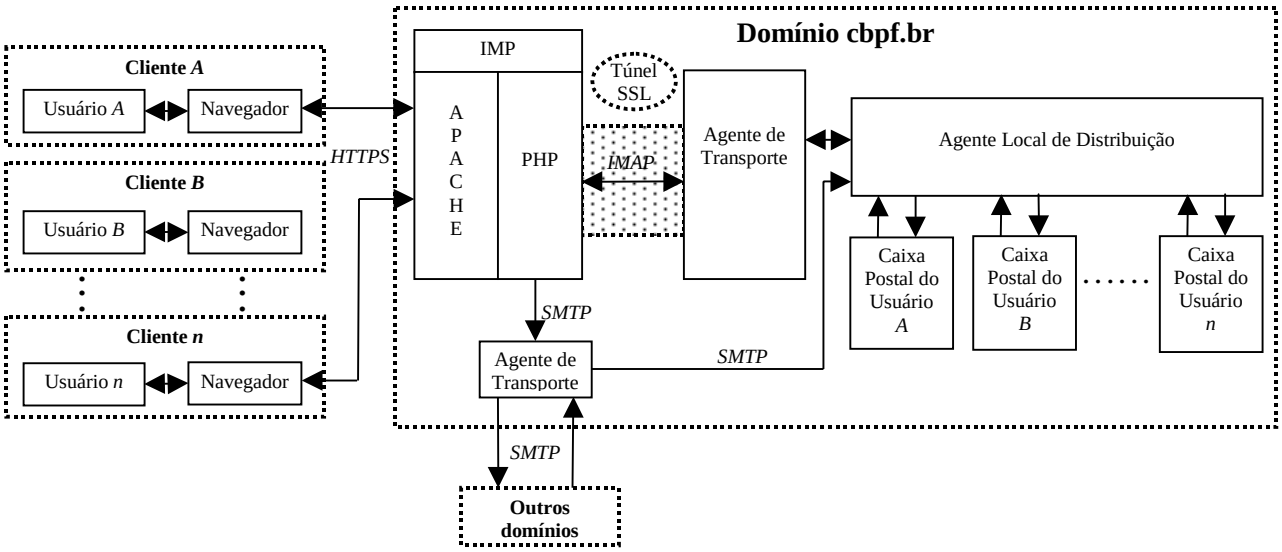

Figura 1

Focalizando a atenção nos blocos representados em linhas pontilhadas, verificamos a representação mais geral possível. Estes blocos representam:

- **Clientes** – são os usuários conectados à Internet através de outras redes ou **ISPs** (*Internet Service Providers* – Provedores de Acesso à Internet). Eles podem pertencer a qualquer domínio conectado à rede global, inclusive ao domínio do próprio CBPF.

- **Domínio cbpf.br** – pertence a este todo computador do CBPF, incluindo os servidores de correio e de *Webmail*. Estes permitem conexão simultânea de diversos clientes.

- **Outros domínios** – todo e qualquer domínio da Internet além do **cbpf.br**.

Um *Webmail* precisa suportar uma série de operações básicas. Dedicaremos o resto deste capítulo a explicar cada uma delas.

3.1 Manipulação de mensagens da caixa postal

Digamos que o usuário **A** deseja ler suas mensagens e organizá-las em sua caixa postal. Seu primeiro passo é conectar-se ao serviço de *Webmail*. Para tal, o usuário **A** utiliza se navegador para acessar a página https://mail.cbpf.br e se conectar ao serviço. O programa do *Webmail* (o IMP) entra em execução assim que a página principal do *site* é acessada.

Durante a etapa de conexão, o usuário **A** adquire o status de cliente, e interage com o servidor através do protocolo HTTPS (HTTP sobre SSL). O servidor – no caso o Apache – recebe os comandos do cliente, passando-os ao IMP. Este é interpretado como script PHP pelo servidor Apache, que responde ao cliente com páginas HTML.

Havendo sucesso na conexão, o servidor de *Webmail* – o conjunto formado pelo IMP, o Apache e o PHP – entra em contato com um agente de transporte via protocolo IMAP. O enlace de dados estabelecido é encriptado por SSL, que pode ser representado abstratamente como um túnel, um invólucro protetor dessa conexão. O agente local de distribuição de mensagens da rede do CBPF é então acionado para que, enfim, o servidor possa acessar o conteúdo da caixa postal do usuário **A** e manipulá-lo de acordo com os comandos que receber do respectivo cliente.

3.2 Envio de mensagens a outros usuários do CBPF

Digamos que o usuário **A** agora quer enviar uma mensagem ao usuário **B** em seu endereço de *e-mail* do CBPF. Através do IMP, ele irá acessar a interface de composição de mensagem, preencherá os campos necessários e o mandará executar o envio.

Agora, o servidor deverá entrar em contato com um outro agente de transporte via protocolo SMTP, que irá acionar o agente local de distribuição do CBPF para depositar a mensagem na caixa postal do usuário **B**.

3.3 Envio de mensagens a usuários externos ao CBPF

O usuário **A** deseja enviar uma mensagem a um endereço de *e-mail* não pertencente ao domínio do CBPF. Este tipo de operação se dá de forma similar à anterior, completamente transparente ao usuário. A diferença se dá no fato de que o agente de transporte selecionado fará uma conexão SMTP com o agente de transporte do servidor de correio do domínio ao qual o destinatário da mensagem pertence.

Vale ressaltar que este agente de transporte também é responsável pelo recebimento de mensagens externas, que são direcionadas ao agente local de distribuição, que trata de depositá-las nas respectivas caixas postais.

4 *Webmail* versus programas clientes locais

Acabamos de ver o modelo básico do *Webmail* do CBPF. Ao analisá-lo, e compará-lo ao método clássico de visualização de *e-mail* (os programas clientes locais), podemos assinalar as vantagens que um tem sobre o outro em uma tabela.

	Cliente local	*4.1 Webmail*
Quanto ao armazenamento, as mensagens	são depositadas no computador cliente e removidas do servidor	permanecem no servidor
Quanto à mobilidade	o usuário deve instalar e configurar um cliente em cada computador em que desejar consultar suas mensagens	o usuário pode visualizar suas mensagens em qualquer computador capaz de se conectar e acessar conteúdo HTML da rede
Quanto à coesão da caixa postal	o usuário geralmente espalha suas mensagens em vários computadores diferentes, precisando fazer cópias constantes para atualizá-los	como a única caixa postal se encontra no servidor, não há dispersão das mensagens.
Quanto à disponibilidade *off-line*	o usuário pode acessar mensagens anteriormente recebidas sem realizar uma nova conexão com o servidor	o usuário necessita conectar-se ao servidor para visualizar quaisquer mensagens
Quanto à velocidade de acesso	o usuário deve aguardar que mensagens e anexos – às vezes volumosos – sejam transmitidas ao seu computador local sem poder determinar previamente se os deseja	o usuário pode visualizar e remover quaisquer mensagens e anexos indesejados sem ter que gravá-los em seu computador
Quanto à segurança	o computador do usuário fica sujeito à contaminação por vírus e *worms* toda vez que visualiza uma mensagem	o usuário pode visualizar o conteúdo sem contaminar seu computador e decidir se grava localmente ou não quaisquer anexos recebidos nas mensagens
Quanto ao espaço de armazenagem	o usuário pode aumentar esse espaço em seu computador local	o espaço de armazenagem é fixo pela cota do servidor

Tabela 1

Podemos combinar as vantagens dos dois sistemas.O *Webmail* pode ser utilizado para visualizar mensagens em diversos computadores, filtrando as que forem indesejadas. O cliente local, então, fica sendo utilizado para receber as mensagens em um único computador local (talvez o computador residencial do usuário) e liberar seu espaço no servidor.

5 Programas necessários para implementar um *Webmail* em ambiente Sun

Este capítulo se preocupa em listar os programas necessários para a instalação de um *Webmail* em uma rede de máquinas Sparc Sun. Todos os programas listados abaixo foram compilados utilizando o **GNU C Compiler** - **gcc**. Também foram utilizados os utilitários

auxiliares de compilação chamados: **autoconf**, **automake** e **bison**. A linguagem **Perl**, presente na rede Sun do CBPF, é necessária para a execução de certos *scripts* de instalação.

5.1 Web server (Apache)

Como o *Webmail* é uma interface HTML acessada por um navegador *web*, ele necessita de um servidor *web*, ou seja, um programa que disponibilize essas páginas HTML. Em nossa aplicação foi escolhido o *web server* **Apache**, um projeto de código aberto (*open source*), desenvolvido pela comunidade da Internet.

5.2 Mod-SSL (módulo para o Apache)

Este programa adiciona a capacidade de prover conexões criptografadas via tecnologia SSL (*Secure Socket Layer*) ao Apache. Isto evita que terceiros se apropriem da senha do usuário.

5.3 OpenSSL

Este é outro exemplo de um projeto de código aberto. Ele implementa uma série de ferramentas para criar e manipular chaves e certificados digitais baseados na tecnologia SSL.

5.4 SSLeay

Para gerar chaves e certificados digitais criptografados é necessário fazer uso de um programa que gere números aleatórios. Diversos programas, comerciais e livres, existem para esta tarefa. O SSLeay, que outrora fazia parte do navegador *web* **Netscape** e recentemente foi separado e destinado para uso livre, foi o escolhido.

5.5 PHP

Cada vez mais popular na Internet, o PHP é uma linguagem de programação de scripts que são executados no lado do servidor, existente em várias plataformas. Isso quer dizer que quando um cliente (um navegador *web*) requisita a execução de um script PHP, este executa no servidor no qual se localiza e responde ao navegador cliente apenas HTML.

Desta forma, o cliente não precisa ter o PHP ou qualquer tipo de suporte instalado localmente, não tem seu desempenho prejudicado (já que não processa o script ele mesmo) e não pode ler ou interferir no código-fonte (visto que o PHP não envia nenhum código seu ao cliente, mas apenas HTML).

5.6 Um banco de dados (MySQL)

O *Webmail* do CBPF pode ter certas características personalizadas. O idioma em que se apresenta, por exemplo, vale por computador, e por isso é armazenado no compudador do usuário na forma de um *cookie*.

Outros dados (lista de contatos, assinatura) são particulares para cada usuário. Estes são dados que precisam ser armazenados no servidor. Existem outros dados que também precisam ser armazenados no servidor, visto que são únicos durante toda uma sessão do usuário (como seu código de identificação, por exemplo). Para tal, o *Webmail* precisa utilizar ou um servidor

LDAP, ou memória compartilhada, ou um banco de dados. A última opção foi a escolhida, visto ser a mais recomendada pelos administradores de *Webmail*.

O servidor de banco de dados utilizado nesta aplicação é o MySQL, visto que tem boa performance e é muito difundido no mercado, sendo que vários programas suportam por padrão interação com este.

5.7 IMAP

O *Internet Message Access Protocol* - IMAP, é o protocolo utilizado pelo *Webmail* para ler as mensagens do servidor de correio eletrônico. Apesar de o POP (*Post Office Protocol*) ser o mais comum, o IMAP foi o escolhido, devido as seguintes vantagens:

- Permite opção de encriptação de canal via SSL – não é necessário um *wrapper* SSL externo, ou seja, um programa que crie um "túnel" criptografado entre o servidor e o cliente; o IMAP tem um *wrapper* interno, e seu funcionamento é completamente transparente para o cliente: o *software* cliente não precisa possuir nenhuma funcionalidade extra para lidar com o canal codificado;

- PHP possui módulos nativos para este protocolo – desta forma o protocolo pode ser acessado internamente pelo script, sem a necessidade de artifícios, como CGIs, por exemplo, o que favorece à performance do *Webmail*;

- Maior performance para manipular pastas remotas – ao contrário do POP, que foi desenvolvido apenas para mover mensagens do servidor para o cliente, o IMAP possui a capacidade de manipular múltiplos acessos a múltiplas pastas de mensagem, permitindo ao usuário organizar as mensagens remotamente antes de obtê-las por um programa cliente convencional. Para realizar o mesmo com o POP, seriam necessários certos artifícios que resultariam em uma queda de performance e insatisfação dos usuários.

5.8 Horde

O *Horde Project* é um projeto de código aberto com a finalidade de desenvolver uma base de código comum para diversas aplicações baseadas na *web*, as quais foram ou estão sendo desenvolvidas. Estas são capazes de interagir entre si, compartilhar bibliotecas e fazer uso de uma interface ao usuário comum a todas. O programa do *Webmail* foi desenvolvido por este projeto.

5.9 IMP

Este é o *Webmail* propriamente dito. Conhecido anteriormente como *IMAP webMail Program* e mais atualmente como *Internet Mail Program*, ele é um programa totalmente desenvolvido em PHP que age como um cliente de *e-mail* cuja interface se dá via um navegador de páginas da *web*.

O IMP é um projeto de código aberto. Como tal, ele pode ser totalmente adaptado às necessidades de seus usuários. Os motivos de sua escolha como o programa do *Webmail* são os mesmos de seus pré-requisitos, ou sejam:

- Independente de plataforma – como é feito em PHP, possui todas as vantagens oferecidas por essa linguagem;

- Permite encriptação de canal – por usar IMAP e este permitir esta funcionalidade;

- Possibilita integração futura com outros serviços *web* – por ser um programa desenvolvido para a interface Horde, permite que todos os outros projetos de mesma origem interajam com ele. Desta forma, à medida que estes forem sendo disponibilizados, será possível anexar ao *Webmail* uma série de outros serviços, como por exemplo uma agenda, um *webchat*, um gerenciador administrativo para contas de usuários etc.

6 Descompactando os arquivos

Primeiramente, deve-se garantir que os programas de manipulação de arquivos compactados estejam disponíveis. São eles:

- Gzip
- Bzip2
- Tar

Com relação ao `tar`, a versão que vem no Solaris possui alguns problemas quando se trata de nomes de arquivos extremamente longos. Recomendamos o uso da versão **GNU** deste programa, denominado `gtar` para diferenciá-lo da versão nativa do sistema.

Devemos descompactar todos arquivos que contém os fontes dos programas selecionados, menos os que contêm o **Horde** e o **IMP**. Para tanto, basta copiá-los para um diretório, que na nossa aplicação é o diretório `/opt/src` e fazer uso do comando apropriado, que é:

```
gtar zxvf arquivofonte.tar.gz
```

para os arquivos com extensão `.tar.gz`, e:

```
gtar yxvf arquivofonte.tar.bz2
```

para os arquivos compactados com Bzip2. Os arquivos que não possuem o nome `tar` na extensão deverão ser descompactados com os respectivos programas:

`gunzip arquivofonte.gz` e `bunzip arquivofonte.bz2`

Para facilitar o processo de instalação, renomeamos os diretórios que foram criados para os fontes dos programas para:

- `/opt/local/src/apache`
- `/opt/local/src/SSLeay`
- `/opt/local/src/openssl`
- `/opt/local/src/mysql`
- `/opt/local/src/mod_ssl`

- /opt/local/src/imap
- /opt/local/src/php

7 Instalando os programas de suporte

7.1 MySQL

Utilizar os comandos:

```
#   cd /opt/local/src/mysql
#   ./configure --prefix=/opt/local/mysql --
    localstatedir=/opt/local/data/mysql
#   make
#   make install
#   Seguir com configuração do MySQL
#   cp /src/mysql/support-files/mysql.server
    /etc/init.d/mysql.server
```

Para iniciar o MySQL automaticamente no boot, veja os arquivos do diretório /etc/rc3.d (diretório dos scripts que são executados quando o sistema entra no *runlevel* 3). Eles são *links* dos respectivos processos do diretório /etc/init.d. O **S** na frente indica que é um script de inicialização (*start*) e o número representa a ordem de inicialização.

Em nosso exemplo, o número 94 foi utilizado por ser o mais alto no diretório, tornando a inicialização do MySQL a última a ser realizada durante o carregamento deste *runlevel*. Para criar o devido *link*, execute o comando:

```
#   ln –s /etc/init.d/mysql.server S94mysql.server
```

Adicione estas linhas no início do arquivo `/etc/init.d/mysql.server`, ou o server não iniciará no Solaris 8:

```
PATH=$PATH:/sbin:/usr/sbin:/bin:/usr/bin
export PATH
LD_LIBRARY_PATH=/opt/local/openssl/lib/opt/local/openssl/ssl/
lib:/opt/local/lib:/usr/lib:/usr/local/lib:/usr/local/lib:/us
r/lib:/lib
export LD_LIBRARY_PATH
```

Motivo: Até este ponto da inicialização do *runlevel* 3, o sistema não possui a variável de ambiente `LD_LIBRARY_PATH`**. Este comportamento é diferente do Linux e dos *BSD, que não necessitam desta alteração do script de inicialização do servidor de banco de dados.**

Inicie o serviço digitando:

```
#   /etc/init.d/mysql.server start
```

```
#   /opt/local/mysql/bin/mysqladmin -u root password
    'uma_nova_senha'
```

7.2 OpenSSL

Utilizar os comandos:

```
#   cd /opt/local/src/openssl
#   ./config --prefix=/opt/local/openssl threads shared
```
Editar o `Makefile` apos o config e procurar por `gnu-shared`. Substituir por `solaris-shared`.
```
#   make
#   make test
#   make install
#   LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/opt/local/openssl/lib:
    /opt/local/openssl/ssl/lib:/opt/local/lib
#   export LD_LIBRARY_PATH
```

7.3 SSLeay

Utilizar os comandos:

```
#   cd /opt/local/src/SSLeay
#   perl util/perlpath.pl /usr/bin
#   perl util/ssldir.pl /opt/local/openssl/ssl
#   make -f Makefile.ssl links
#   ./Configure solaris-sparc-gcc
#   make clean
#   make
#   make rehash
#   make test
#   make install
```

7.4 IMAP

Os procedimentos abaixo referem-se à compilação do **UW-IMAP** (o IMAP da Universidade de Washington):

Utilize o comando:

```
#   cd /opt/local/src/imap
```

Edite o arquivo `/opt/src/imap/Makefile` e altere as seguintes linhas para:

```
EXTRAAUTHENTICATORS=
EXTRADRIVERS=
PASSWDTYPE=std
SSLTYPE=unix
```

Edite o arquivo `/opt/src/imap/src/osdep/unix/Makefile` e altere as seguintes linhas para:

```
SSLDIR=/opt/local/openssl
SSLCERTS=$(SSLDIR)/ssl/certs
SSLINCLUDE=$(SSLDIR)/include
SSLLIB=$(SSLDIR)/lib
EXTRAAUTHENTICATORS=
EXTRADRIVERS=
PASSWDTYPE=std
SSLTYPE=unix
```

Utilize o comando:

```
#  make gso SSLTYPE=unix
```

Edite o arquivo /etc/inetd.conf e trocar as seguintes linhas por:

```
#imap    stream  tcp     nowait  root
/opt/local/src/imap/imapd/imapd   imapd
imaps   stream  tcp     nowait  root
/opt/local/src/imap/imapd/imapd    imapd
```

A primeira linha deverá estar comentada com # para não abrir a porta IMAP que não utiliza encriptação via SSL.

No arquivo `/etc/services`, altere, se necessário, as seguintes linhas para:

```
imap            143/tcp
imaps           993/tcp
```

Gere a chave para criptografia através do comando:

```
#  /opt/local/openssl req -new -x509 -nodes -out
   /opt/local/openssl/ssl/certs/imapd.pem -keyout
   /opt/local/openssl/ssl/certs/imapd.pem -days 3650
```

Edite o arquivo `/etc/init.d/inetsvc` e altere o final do arquivo para:

```
# Codigo inserido para imap-ssl ser carregado corretamente
LD_LIBRARY_PATH=/opt/local/openssl/lib:/opt/local/openssl/ssl
/lib:/opt/local/lib
:/usr/local/lib:/usr/lib:/lib
export LD_LIBRARY_PATH
# Fim de codigo para imap-ssl

/usr/sbin/inetd -s &
```

Reinicie o processo `inetd`

Para testar seu servidor IMAP, digite:

```
#   /opt/local/openssl/bin/openssl s_client –host
    seuhost.seudominio –port 993
```

Você deverá ver uma negociação de certificados, juntamente com o estabelecimento de uma conexão encriptada. Ao final, a interface do protocolo IMAP deverá aparecer. Para testar um *login*, digite:

```
O login seulogin suasenha
```

Uma mensagem de confirmação deverá aparecer. Saia da interface digitando:

```
O logout
```

7.5 Mod-SSL

Utilizar os comandos:

```
#   cd /opt/local/src/mod_ssl
#   ./configure --with-apache=/opt/local/src/apache
#   cd ../apache
#   ./configure --prefix=/opt/local/apache_ssl
```

7.6 PHP

Utilize os comandos:

```
#   cd /opt/src/php
```

Crie um arquivo chamado `config.nice` e adicione:

```
#! /bin/sh
#
# Created by configure

"./configure" \
"--prefix=/opt/local" \
"--with-apache=/opt/local/src/apache" \
"--with-mysql=/opt/local/mysql" \
"--with-openssl=/opt/local/openssl" \
"--with-imap=/opt/local/src/imap" \
"--with-imap-ssl=/opt/local/src/imap/c-client" \
"--with-zlib" \
"--enable-shared=imap.so" \
"--enable-track-vars" \
"--enable-debug=no" \
"--enable-memory-limit=yes" \
"$@"
```

Execute:

```
#   make
#   make install
#   cp php.ini-dist /opt/local/lib/php.ini
```

7.7 Apache

Utilize os comandos:

```
#   SSL_BASE=/opt/local/openssl
#   export SSL_BASE
#   ./configure --prefix=/opt/local/apache_ssl "--with-
    perl=/usr/local/bin" –enable-module=so --enable-module=ssl
    --activate-module=src/modules/php4/libphp4.a --enable-
    module=php4
#   make
#   make certificate
```

Quando for requisitado o nome da máquina, lembre de utilizar o nome completo listado no DNS (exemplo: mail.cbpf.br). No final será oferecida a oportunidade de definir uma senha (*pass phrase*). Se esta for implementada, será necessário digitá-la para iniciar o *daemon* do Apache com suporte a SSL. Como isto torna inviável uma ativação automática em caso de *reboot* do servidor, é aconselhado não ativar esta opção.

```
#   make install
```

Caso o arquivo `/etc/init.d/apache` já exista, altere as linhas:

```
LD_LIBRARY_PATH=/opt/local/openssl/lib:/opt/local/openssl/ssl
/lib:/opt/local/lib:/usr/local/lib:/usr/lib:/lib
export LD_LIBRARY_PATH

APACHE_HOME=/opt/local/apache_ssl
CONF_FILE=/opt/local/apache_ssl/conf/httpd.conf
PIDFILE=/opt/local/apache_ssl/logs/httpd.pid
```

Motivo: Para disponibilizar o suporte a criptografia (protocolo HTTPS), o Apache precisa localizar as bibliotecas do OpenSSL. Caso isto não seja feito, ocorrerá falha de inicialização. Ademais, caminhos para outras bibliotecas são necessários para alguns processos a serem inicializados posteriormente no *boot*.

Caso não exista, crie-o, escrevendo nele:

```
#!/sbin/sh
#
# Copyright (c) 1999 by Sun Microsystems, Inc.
# All rights reserved.
#
#ident  "@(#)apache.sh  1.3     99/11/10 SMI"
```

```
LD_LIBRARY_PATH=/opt/local/openssl/lib:/opt/local/openssl/ssl
/lib:/opt/local/lib:/usr/local/lib:/usr/lib:/lib
export LD_LIBRARY_PATH

APACHE_HOME=/opt/local/apache_ssl
CONF_FILE=/opt/local/apache_ssl/conf/httpd.conf
PIDFILE=/opt/local/apache_ssl/logs/httpd.pid

if [ ! -f ${CONF_FILE} ]; then
        exit 0
fi

case "$1" in
start)
        /bin/rm -f ${PIDFILE}
        cmdtext="starting"
        ;;
restart)
        cmdtext="restarting"
        ;;
stop)
        cmdtext="stopping"
        ;;
*)
        echo "Usage: $0 {start|stop|restart}"
        exit 1
        ;;
esac

echo "httpd $cmdtext."

status=`${APACHE_HOME}/bin/apachectl $1 2>&1`

if [ $? != 0 ]; then
        echo "$status"
        exit 1
fi
exit 0
```

Edite o arquivo `/opt/local/apache_ssl/bin/apachectl` e modifique as seguintes linhas:

```
#    start)
#    if [ $RUNNING -eq 1 ]; then
#        echo "$0 $ARG: httpd (pid $PID) already running"
#        continue
#    fi
#    if $HTTPD ; then
#        echo "$0 $ARG: httpd started"
```

```
#    else
#        echo "$0 $ARG: httpd could not be started"
#        ERROR=3
#    fi
#    ;;
    start|startssl|sslstart|start-SSL)
```

Também crie o devido *link*:

```
#  ln –s /etc/init.d/apache /etc/rc3.d/S50apache
```

Inicie o processo do Apache:

```
#  /etc/init.d/apache start
```

Para testar seu servidor Apache, digite:

```
#  /opt/local/openssl/bin/openssl s_client –host
   seuhost.seudominio –port 443
```

Você deverá ver uma negociação de certificados, juntamente com o estabelecimento de uma conexão encriptada. Ao final, a interface do protocolo HTTP deverá aparecer.

Saia da interface digitando:

```
bye
```

8 Instalando o IMP

O IMP é baseado no Horde. Este é uma base de código para desenvolvimento de aplicativos para Internet, que compreende uma coletânea de bibliotecas, bem como uma interface comum para tais aplicações.

O Horde faz uso da PHPlib, que é onde ficam armazenados os *includes* para interfaceamento do Horde com bancos de dados e gerenciamento de sessões, e o arquivo de *prepends*, que é o código que deve se carregado pelo PHP antes de processar quaisquer comandos

8.1 Localização dos programas

O Horde deve ser descompactado no diretório desejado para raiz do servidor *web*. Tal diretório é inicialmente, em nosso exemplo, `/opt/local/apache_ssl/htdocs`, portanto o Horde deve ser instalado em `/opt/local/apache_ssl/htdocs/horde`.

O diretório da PHPlib deve ser movido para fora do escopo do servidor *web*. Isso garante que somente o Horde, através dos canais apropriados, será capaz de acessar suas informações, evitando assim conflitos com outros aplicativos PHP. Em nosso exemplo, utilizamos o diretório `/opt/local/phplib`.

O IMP deve ser descompactado diretamente dentro do diretóriodo Horde, de forma que em nosso exemplo seu caminho passa a ser :

`/opt/local/apache_ssl/htdocs/horde/imp.`

8.2 Configurando a PHPlib

Edite o arquivo `/opt/local/lib/php.ini`, procure e altere as seguintes linhas para:

```
auto_prepend_file = "/opt/local/phplib/prepend.php3"
include_path = "/opt/local/phplib:."
magic_quotes_gpc = Off
upload_tmp_dir = "/tmp"
display_errors = Off
log_errors = On
extension=imap.so
extension=mysql.so
```

Edite o arquivo `/opt/local/phplib/local.inc` e descomente as linhas referentes ao banco de dados escolhido, que neste exemplo é o MySQL.

Verifique se há necessidade de alterar o arquivo `/opt/local/phplib/prepend.php3`. Normalmente ele já vem configurado, mas em algumas versões do Horde, ele vem com suas opções comentadas.

8.3 Configurando o Horde

Vá para o diretório `/opt/local/apache_ssl/htdocs/horde/config`, copie o arquivo `horde.php3.dist` para `horde.php3` e edite-o, alterando a linha:

```
$default->horde_root_url = ‘/horde’;
```

8.4 Configurando o Apache para o Webmail

Edite o arquivo `/opt/local/apache_ssl/conf/httpd.conf`, procure e altere as seguintes linhas para:

```
ServerName seuhost.seudominio
DocumentRoot
"/opt/local/apache_ssl/htdocs/horde/imp/redirect"

<IfModule mod_dir.c>
    DirectoryIndex index.html index.cgi index.php index.php3
</IfModule>
AddType application/x-httpd-php .php .php3
AddType application/x-httpd-php-source .phps
AddHandler cgi-script .cgi
```

```
<IfDefine SSL>

##
## SSL Virtual Host Context
##

<VirtualHost _default_:443>

#  General setup for the virtual host DocumentRoot
"/opt/local/apache_ssl/htdocs/horde/imp"
Alias /horde/ /opt/local/apache_ssl/htdocs/horde/

SSLCertificateFile
/opt/local/apache_ssl/conf/ssl.crt/server.crt
#SSLCertificateFile
/opt/local/apache_ssl/conf/ssl.crt/server-dsa.crt

#   Server Private Key:
SSLCertificateKeyFile
/opt/local/apache_ssl/conf/ssl.key/server.key
#SSLCertificateKeyFile
/opt/local/apache_ssl/conf/ssl.key/server-dsa.key

#   Server Certificate Chain:
SSLCertificateChainFile
/opt/local/apache_ssl/conf/ssl.crt/ca.crt

#   Certificate Authority (CA):
#SSLCACertificatePath /opt/local/apache_ssl/conf/ssl.crt
#SSLCACertificateFile /opt/local/apache_ssl/conf/ssl.crt/ca-
bundle.crt

#   Certificate Revocation Lists (CRL):
#SSLCARevocationPath /opt/local/apache_ssl/conf/ssl.crl
#SSLCARevocationFile /opt/local/apache_ssl/conf/ssl.crl/ca-
bundle.crl
```

Crie o diretório /opt/local/apache_ssl/htdocs/horde/imp/redirect. Neste diretório, crie um arquivo index.html e nele coloque:

```
<html>
<head><title></title>
<meta http-equiv="Refresh" content="0;
URL=https://seuhost.seudominio/index.php3"></head>
<body>
</body>
</html>
```

Renicie o processo do Apache:

```
#   /etc/init.d/apache restart make install
```

8.5 Criando o banco de dados

O Horde já vem com instruções para criar o banco de dados MySQL necessário para nossa aplicação. Para criá-lo, primeiramente vá para o diretório:

```
#   cd /opt/local/apache_ssl/htdocs/horde/scripts/database
```

Uma vez lá, basta executar:

```
#   /opt/local/mysql/bin/mysql –u root –p < mysql_create.sql
```

Ele criará um banco de dados chamado **horde**.

8.6 Configurando o IMP

O IMP pode ser configurado via uma interface gráfica. Basta para isso executar:

```
#   cd /opt/local/apache_ssl/htdocs/horde
#   sh install.sh
```

Agora, entre no seu navegador de páginas *web* e entre com o endereço do script de configuração, que em nosso exemplo é https://seuhost.seudomínio/horde/setup.php3.

Preencha atentamente o formulário e, quando acabar, execute:

```
#   cd /opt/local/apache_ssl/htdocs/horde
#   sh secure.sh
```

Isso impedirá que qualquer um acesse a configuração do IMP via *web*.

Edite o arquivo `/opt/local/apache_ssl/htdocs/horde/imp/config/defaults.php3` e altere a seguinte linha para:

```
$default->port = '993/imap/ssl/novalidate-cert';
```

Isso irá configurar o IMP para conectar-se à porta 993 utilizando protocolo IMAP, com suporte a SSL e aceitando o certificado digital criado sem requerer que este seja um certificado de um CA (*Certificate Authority*) comercial conhecido. Tal artifício é necessário quando se utiliza um certificado gerado e assinado localmente.

9 Usando o *Webmail* do CBPF

9.1 Conectando pela primeira vez

Conectando pela primeira vez, o usuário percebe que o *Webmail* vem no idiome Ingles. Caso deseje que sua interface seja em outra linguagem, basta selecionar a de sua preferência em **Language** (**Idioma**). Para o resto da apresentação, vamos considerar a interface em Português Brasileiro. A figura 2 mostra a tela de entrada:

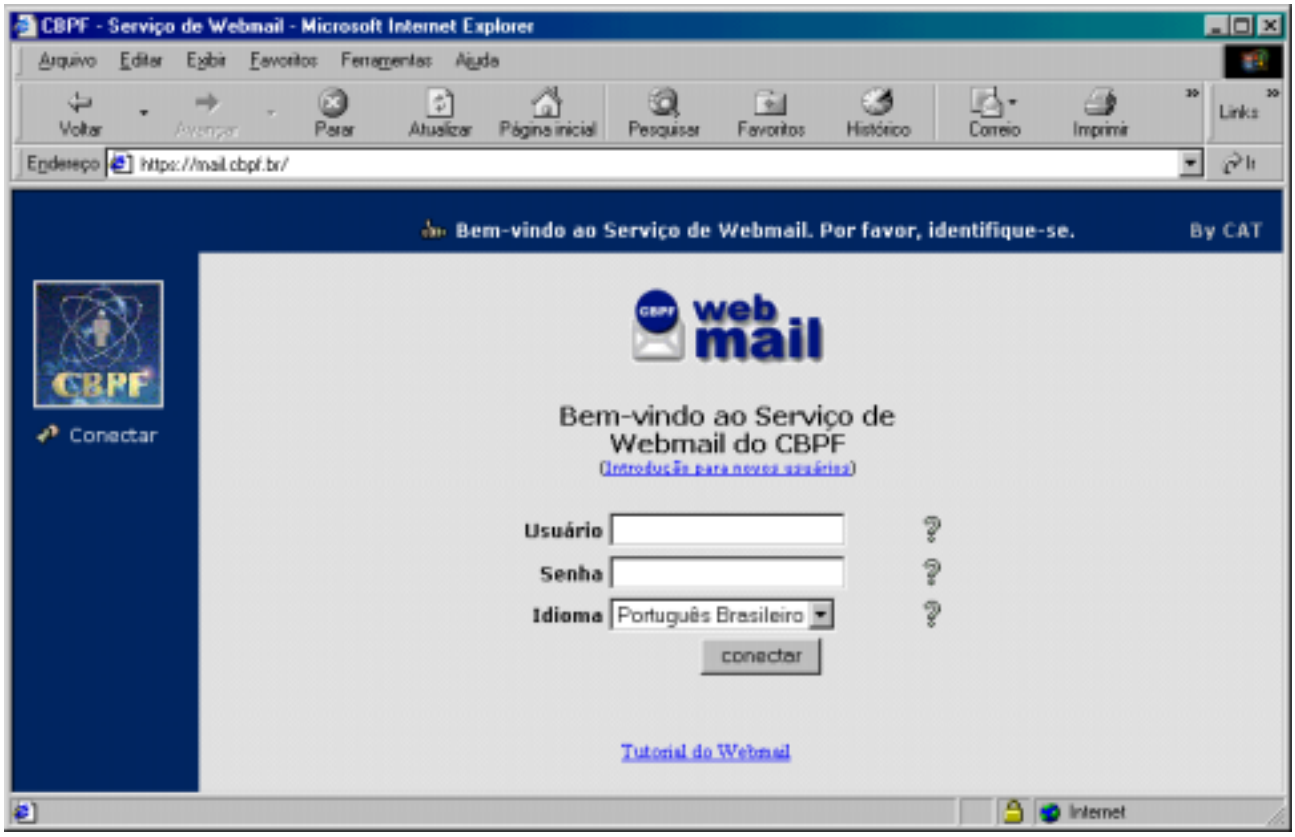

Figura 2

O usuário se conecta ao entrar com o seu *login* no campo **Usuário** e sua senha no campo **Senha**. A conexão se dá ao clicar, então, no botão **conectar**. Em caso de dúvida, os ícones em forma de pontos de interrogação fornecem uma breve explanação sobre cada campo.

O *link* **Introdução para novos usuários** fornece uma boa noção àqueles que nunca utilizaram um serviço de *Webmail*. Se este for o seu caso, não deixe de lê-lo, a fim de evitar dúvidas.

9.2 Lendo mensagens

Após a tela de conexão, aparece a tela de manipulação de mensagens (fig. 3). Esta automaticamente exibe a pasta **INBOX**, que contém as mensagens recebidas.

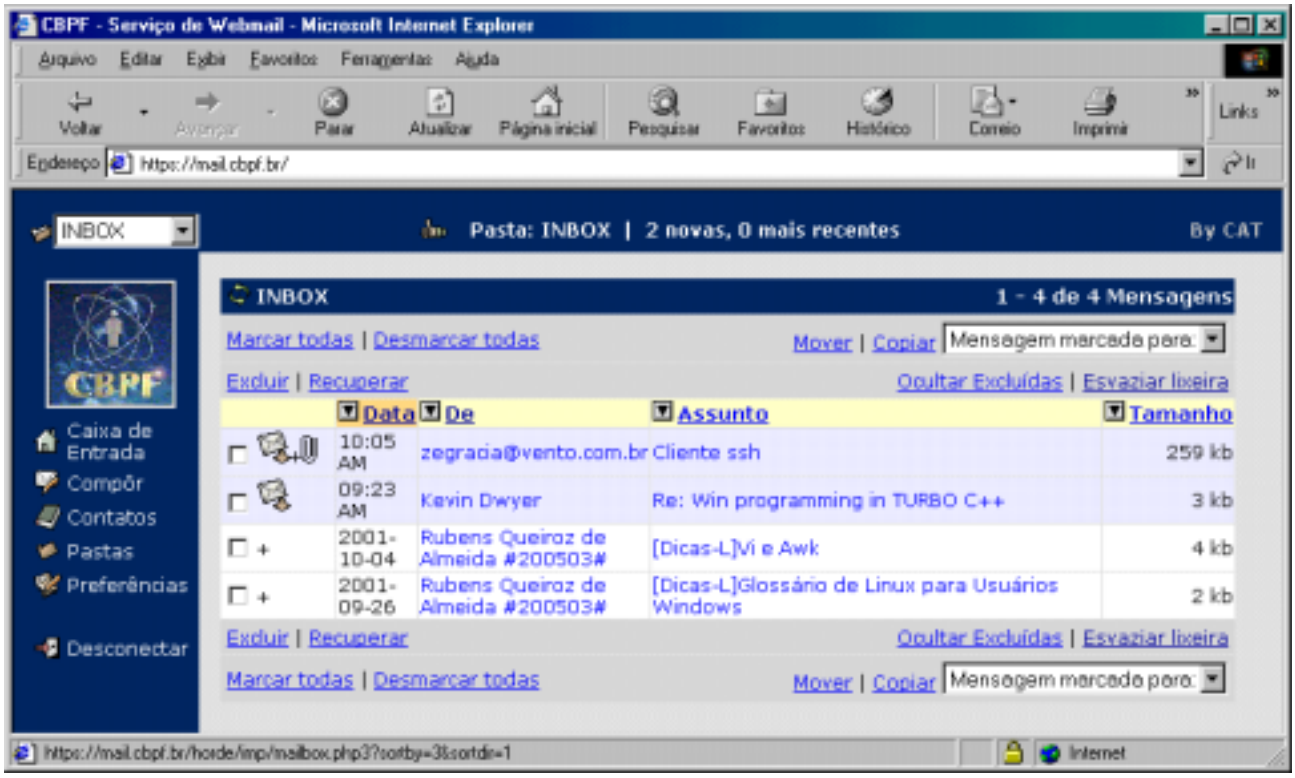

Figura 3

As mensagens aparecerão listadas em ordem de data, da mais recente para a mais antiga. Para alterar essa ordem, basta que o usuário clique no campo em que se desejar ordenar. Por exemplo, se ele quiser visualizar todas as mensagens por ordem de remetente, basta clicar em **De**.

Outra opção de ordenação é a em ordem crescente ou decrescente. Para selecionar a ordem, basta clicar no botão com desenho de seta localizado à esquerda de cada campo.

O primeiro campo representa os *status* de cada mensagem. Aquelas nas quais aparecer neste campo um ícone de uma carta são mensagens ainda não lidas (para reforçar a atenção para essa condição, toda a linha que representa a mensagem é representada em cor diferente). O ícone de um grampo representa que a respectiva mensagem contém um arquivo em anexo.

Caso haja muitas mensagens, o *Webmail* apresentará vinte itens por tela, sendo possível navegar entre as telas da lista através destes botões (fig. 4):

Figura 4

Estes aparecem logo acima da lista de mensagens e também logo após estas quando há a necessidade de se trabalhar com múltiplas páginas. As setas mais externas retornam ao usuário a primeira e a última página da lista de mensagens. As setas menores, mais interiores, avançam ou retrocedem na lista de uma em uma página. Ainda é possível especificar a página desejada através do campo texto disponível: apenas coloque o número da página e aperte *Enter*.

Para ler uma mensagem, clique no valor do campo **Assunto** ou do campo **De** da mensagem desejada.

A interface de leitura de mensagem (fig. 5) é bem intuitiva; os campos em fundo amarelo representam o cabeçalho da mensagem, enquanto que o em branco representa a mensagem propriamente dita.

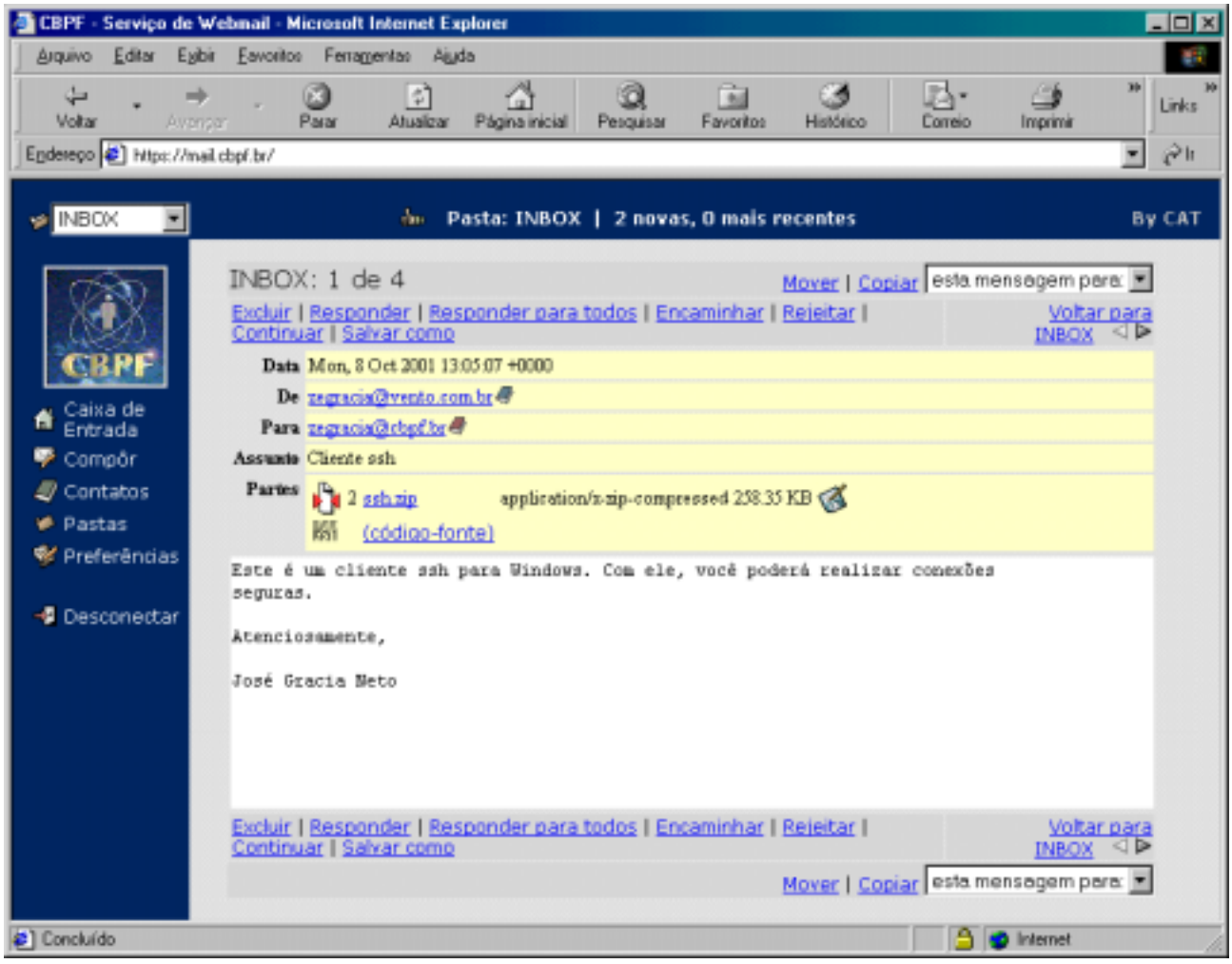

Figura 5

O campo **Partes** representa os arquivos em anexo à mensagem. Caso o usuário queira salvar o arquivo em anexo no seu computador local, basta clicar no ícone de um lápis escrevendo em um disquete representa o botão de gravar.

O *Webmail* é capaz de visualizar alguns tipos de arquivo. Na figura acima, vemos que existe um ícone representando um arquivo comprimido chamado **ssh.zip**. O conteúdo desse tipo de arquivo pode ser exibido sem a necessidade de primeiro salvar o arquivo no computador

local. Ao clicar no nome do arquivo, uma nova janela aparecerá listando diversos detalhes de seu conteúdo.

Para retornar à tela de manipulação de mensagens, basta clicar em **Voltar para INBOX**.

9.3 Excluindo e recuperando mensagens

Quando desejar excluir uma mensagem, o usuário deve fazer o seguinte:

- selecionar as mensagens que desejar excluir clicando na caixa de seleção que fica no primeiro campo de cada mensagem na janela principal;
- clicar em **Excluir**.

As mensagens excluídas aparecerão com um risco por cima de cada palavra do cabeçalho, e com o ícone de lata de lixo no campo de *status* da mensagem. A figura 6 exemplifica a situação:

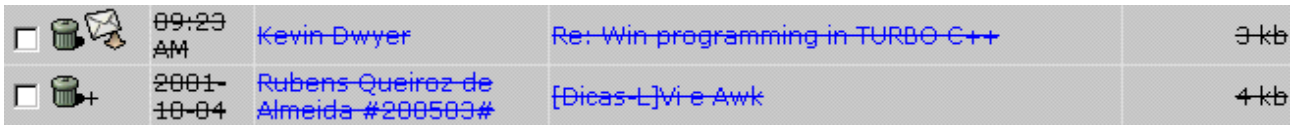

Figura 6

Note que esta exclusão não é definitiva. As mensagens ainda existem e podem ser recuperadas. Esta é uma medida preventiva contra erros ou arrependimentos de exclusão de mensagens.

Quando desejar recuperar uma mensagem, o usuário deve fazer o seguinte:

- selecionar as mensagens que desejar recuperar clicando na caixa de seleção que fica no primeiro campo de cada mensagem na janela principal;
- clicar em **Recuperar**.

Quando desejar esvaziar permanentemente a lixeira, o usuário deve clicar em **Esvaziar lixeira**.

AVISO: ESVAZIANDO A LIXEIRA, TODAS AS MENSAGENS MARCADAS COMO EXCLUÍDAS SERÃO PERDIDAS E NÃO PODERÃO MAIS SER RECUPERADAS!

9.4 Selecionando suas preferências

O *Webmail* permite que o usuário personalize alguns aspectos. Para tanto, basta clicar na opção **Preferências**, que aparece na lista de comandos à esquerda. A figura 7 mostra a interface de **Preferências**.

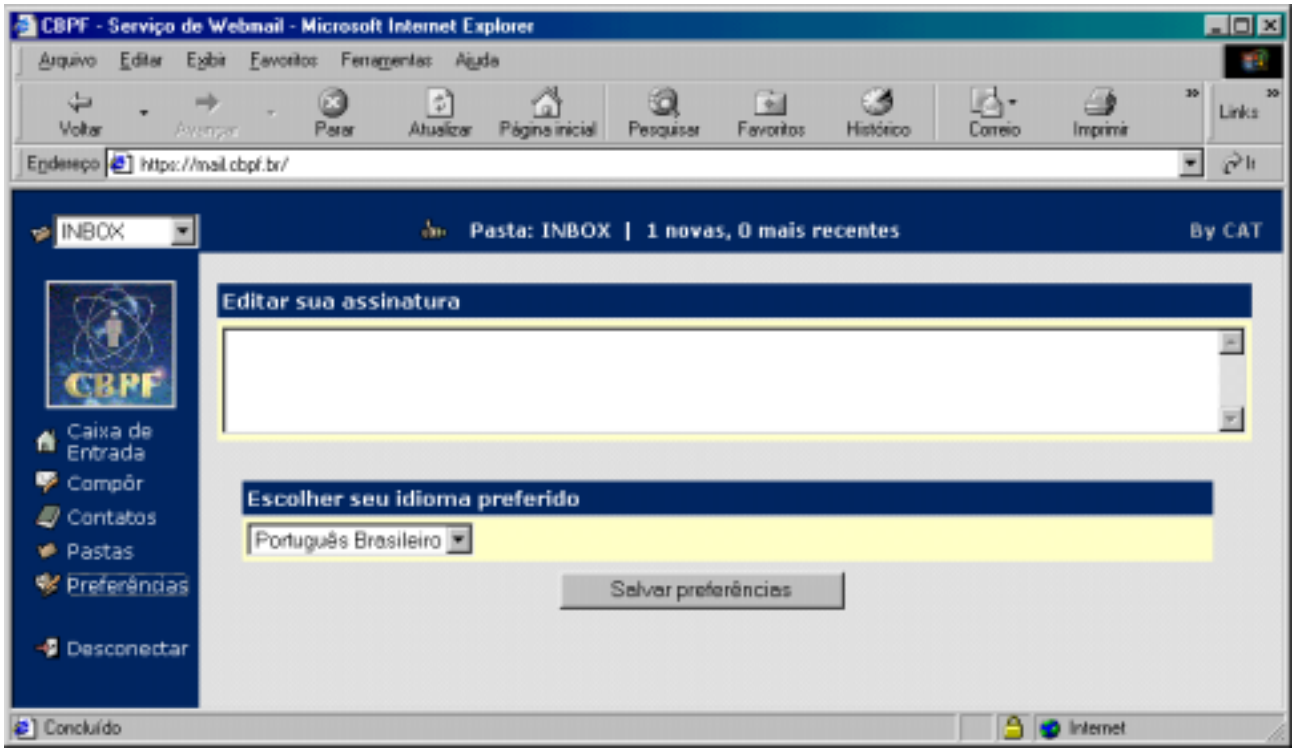

Figura 7

O primeiro aspecto personalizável é a assinatura. Tudo que o usuário escrever no campo texto abaixo de **Editar sua assinatura** será automaticamente incluído como rodapé de toda mensagem que for composta no *Webmail* a partir da aplicação das preferências.

O segundo aspecto personalizável é o idioma. Caso o usuário deseje trocar o idioma no qual *Webmail* se apresenta sem ter que desconectar da atual sessão e retornar, basta que ele seleciona o idioma desejado em **Escolher seu idioma preferido**.

Para aplicar as alterações das preferências, basta clicar em **Salvar preferências**.

9.5 Compondo mensagens

Em todo momento de navegação pelo *Webmail* o usuário deverá ser capaz de compôr uma mensagem. Para tal, basta clicar na opção **Compôr**, que aparece na lista de comandos à esquerda.

A janela de composição (fig. 8) é semelhante à dos mais conhecidos programas gráficos de e-mail do mercado.

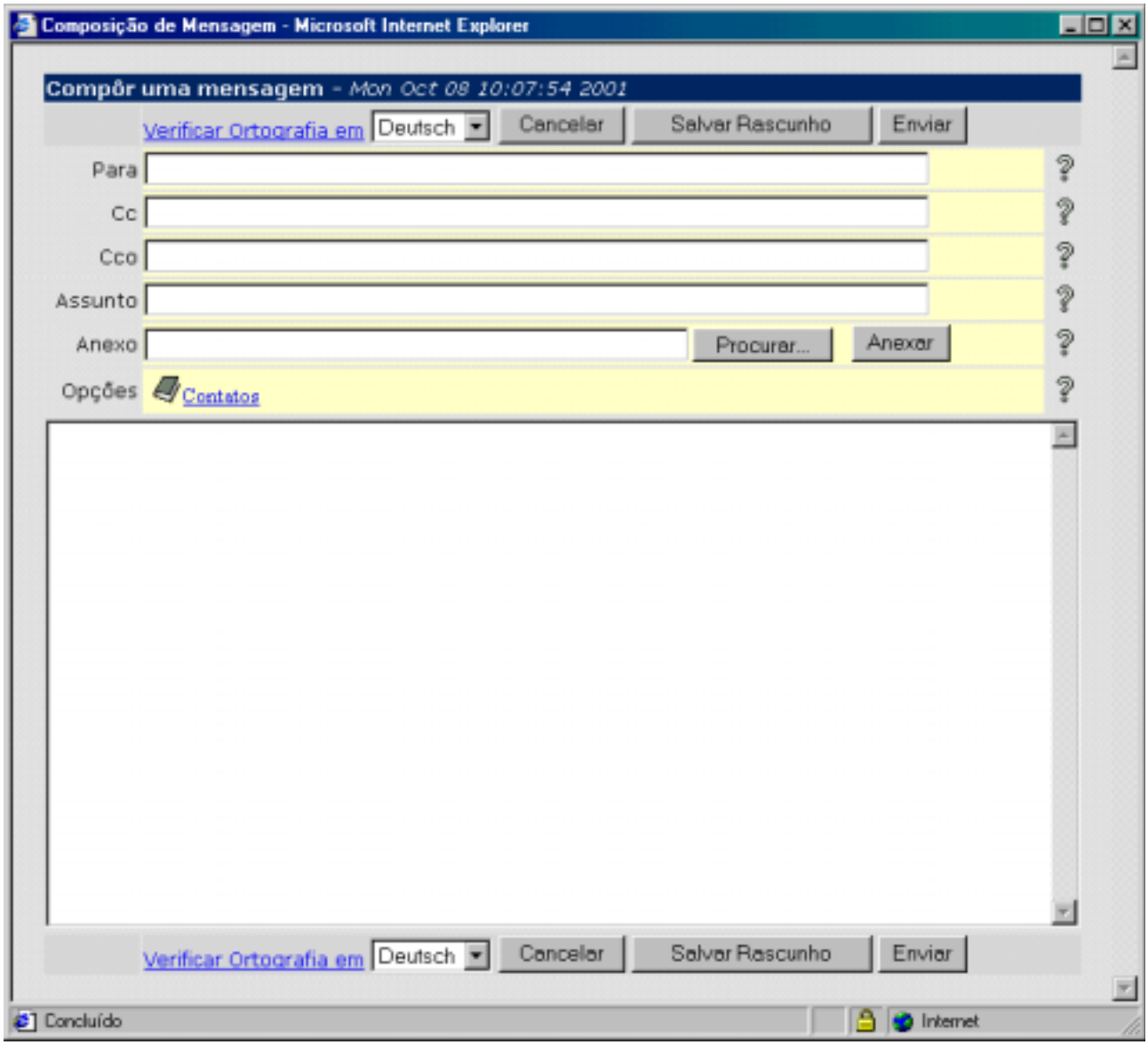

Figura 8

O usuário deve preencher o campo **Para** com o endereço do e-mail do destinatário. Em caso de múltiplos destinatários, preencher os campos **CC** e **Cco** com os outros endereços. Caso necessite incluir mais destinatários, digitar todos os endereços no campo **Para** separados por um **;** (ponto-e-vírgula).

O usuário também pode fazer uso da opção **Contatos**. Esta facilidade será explicada no próximo tópico.

Caso queira salvar esta mensagem para enviar posteriormente, ou utilizá-la novamente para outro destinatário, ou em outra época, ou qualquer outra opção na qual deseje utilizar esta mensagem como um rascunho, basta clicar no botão **Salvar Rascunho**.

É recomendado ao usuário ter por hábito preencher o campo **Assunto**. O motivo é que alguns clientes de correio não lidam bem mensagens sem assunto e algum destinatário pode estar utilizando um destes clientes.

Ao clicar em **Enviar**, a mensagem é automaticamente enviada e uma confirmação de sucesso de envio aparece na barra superior de *status* da tela principal.

9.6 Usando a lista de contatos

A lista de contatos é uma facilidade criada para que o usuário não tenha que memorizar e digitar extensos e confusos endereços. Também é uma ajuda quando houver a necessidade de enviar o mesmo e-mail a muitos endereços simultâneos.

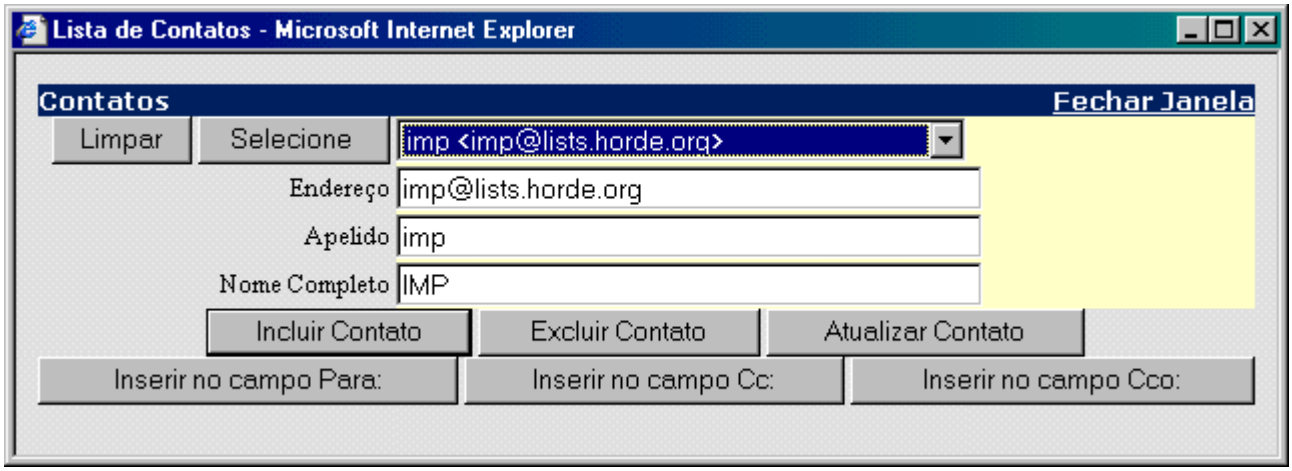

Figura 9

Sua interface (fig. 9) é bem intuitiva. Ela pode ser chamada clicando na opção **Contatos**, que aparece na lista de comandos à esquerda, ou da opção de mesmo nome que aparece na janela de composição de mensagens. Os botões de inserção de endereço no campo desejado funcionam apenas quando ela é chamada da janela de composição de mensagem.

9.7 Anexando arquivos às mensagens

Para o usuário apenas quando ela é chamada da janela de composição de mensagem anexar arquivos à sua mensagem, basta clicar em **Procurar** na janela de composição de mensagem. Uma janela surgirá com a lista de diretórios e arquivos. O usuário deve selecionar o arquivo desejado e clicar em **Abrir**. Agora o nome arquivo (com o caminho completo) aparecerá no campo **Anexo** da janela de composição. Para confirmar, clique em **Anexar**.

O usuário deve repetir a operação para cada arquivo que desejar anexar à mesma mensagem. A figura 10 exemplifica uma lista de anexos.

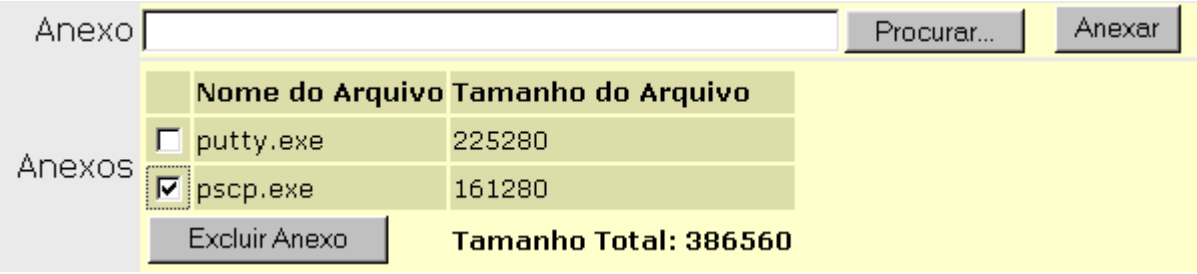

Figura 10

Caso o usuário mude de idéia e deseje retirar um arquivo da lista de anexos sem ter que recomeçar, basta marcar na caixa de seleção o que desejar remover e clique em **Excluir Anexo**.

9.8 Trabalhando com pastas

O *Webmail* permite o gerenciamento de pastas, o que é uma ótima forma de organizar suas mensagens. É possível visualizar a pasta desejada clicando na caixa de seleção (fig. 11).

Figura 11

Note que algumas pastas são padrão para o *Webmail*. Elas são:

- INBOX – esta pasta é a sua caixa de entrada de mensagens. Ela **nunca** pode ser apagada ou renomeada;
- Enviados – esta é a pasta padrão para armazenar uma cópia das mensagens enviadas. Originalmente não existe, e é criada automaticamente quando a primeira mensagem que o usuário compuser for enviada;
- Rascunho – esta é a pasta padrão para guardar as mensagens que o usuário escolher salvar sem enviar. Originalmente não existe, e é criada automaticamente na primeira vez que o usuário clicar no botão **Salvar Rascunho**.

Para copiar ou mover mensagens de uma pasta para outra, basta selecionar as desejadas, selecionar a pasta desejada na caixa de seleção **Mensagem marcada para** (fig. 12), e clicar em **Copiar** ou **Mover**.

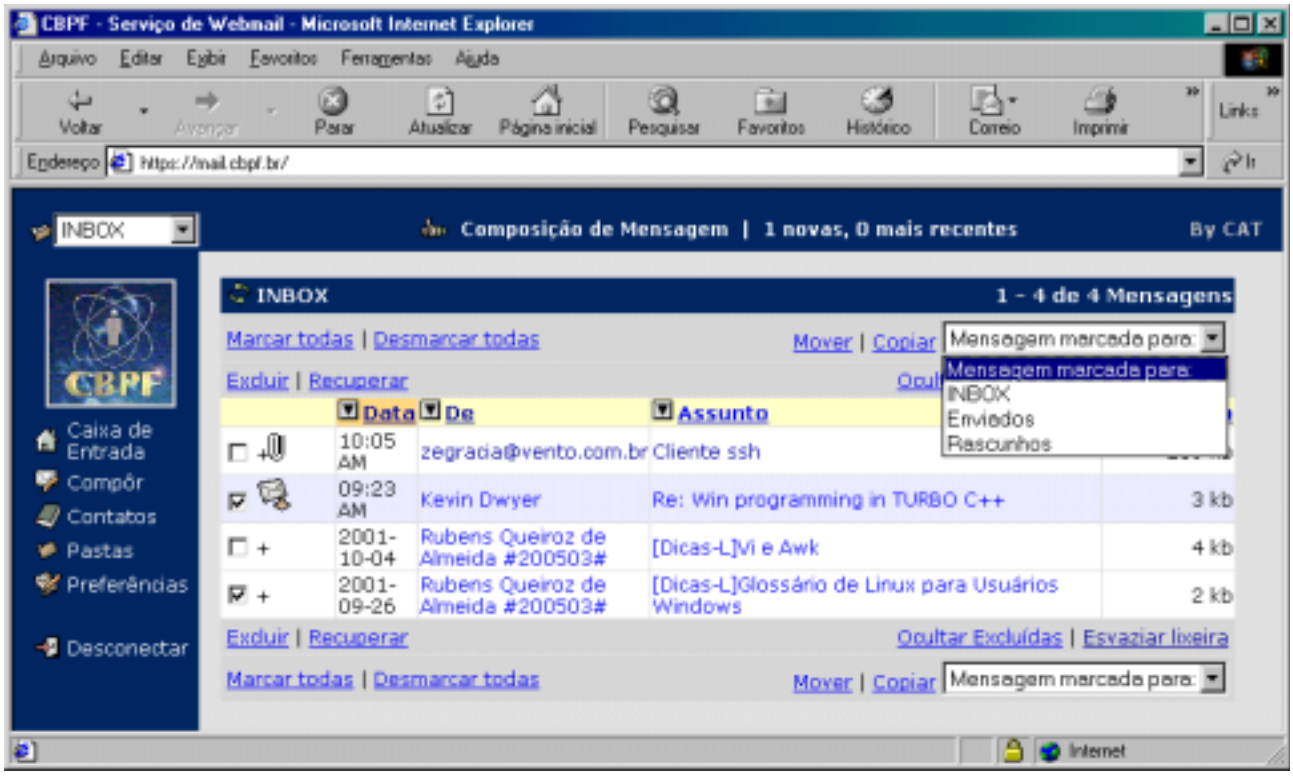

Figura 12

Quando movidas de pasta, as mensagens apresentam na pasta de origem a aparência de mensagem excluída. Caso o usuário mude de idéia quanto a mover as mensagens e deseje mesmo copiar, basta que ele selecione as mensagens excluídas e clique em **Recuperar**. A cópia feita para a nova pasta ainda estará lá.

9.9 Manipulando pastas

Para selecionar esta função, basta clicar na opção **Pastas**, que aparece na lista de comandos à esquerda. O gerenciamento de pastas deverá ter a aparência da figura 13.

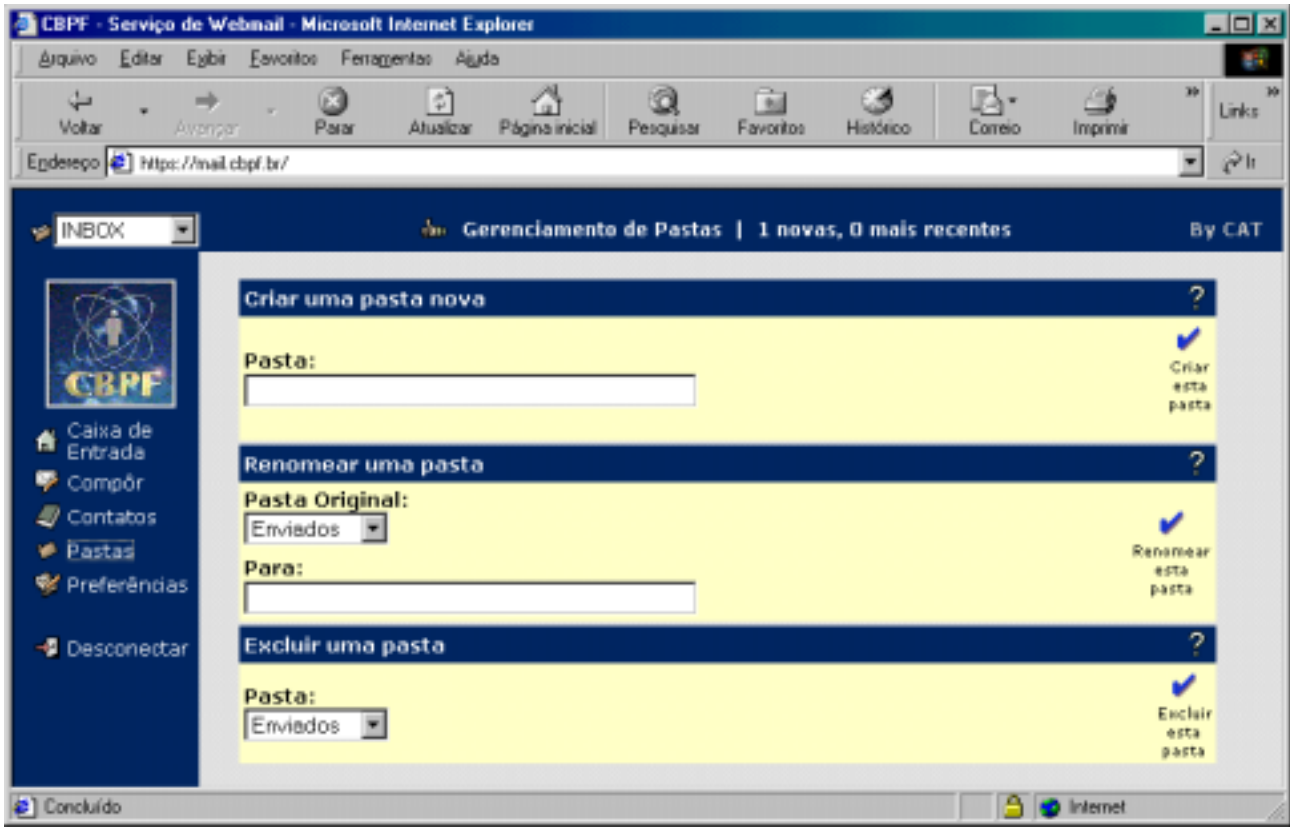

Figura 13

Para criar uma pasta nova, basta escrever o nome desejado para ela no campo de **Criar uma pasta nova** e após isso clicar em **Criar esta pasta**.

Para renomear uma pasta, basta selecionar a pasta desejada na caixa de seleção **Pasta Original**, escrever o novo nome no campo **Para** e clicar em **Renomear esta pasta**.

Para excluir uma pasta, basta selecionar a pasta desejada na caixa de seleção **Pasta** e clicar em **Excluir esta pasta**.

AVISO: EXCLUINDO UMA PASTA, TODAS AS MENSAGENS EXISTENTES NA PASTA APAGADA SERÃO IRREMEDIAVELMENTE PERDIDAS!

9.10 Desconectando do Webmail

Ao encerrar a consulta ao *Webmail*, o usuário deve clicar em **Desconectar** ou então fechar a janela do navegador. O usuário deve lembrar que nunca deve abandonar uma sessão do *Webmail* conectada, pois qualquer pessoa com acesso ao computador poderia ler suas mensagens ou enviar mensagens em seu nome.

10 Dúvidas e soluções

10.1 O que significa o alerta de segurança que aparece no início de uma sessão

Como já mencionado, o *Webmail* utiliza uma conexão segura com o usuário através do protocolo HTTPS. Tal protocolo exige que o *site* seja capaz de identificar-se, via um certificado digital.

Um certificado digital pode ser gerado localmente ou comprado de uma autoridade certificadora profissional (*Certificate authority*). No caso do *Webmail* do CBPF, preferiu-se gerar o certificado localmente.

O alerta de segurança tem o intuito de apresentar ao usuário este certificado, indicando que este não é um certificado comercial. Para ser capaz de se comunicar com o servidor, o cliente precisa responder afirmativamente a este aviso.

10.2 Não consigo mais enviar mensagens

A pasta **Enviados** contém uma cópia de todas as mensagens transmitidas. Com o tempo, esta pasta pode ficar muito cheia. Isso pode fazer com que o **script** PHP que realiza a cópia fique maior que o permitido, o que o impede de executar.

Para resolver isto, crie uma pasta pessoal com qualquer nome e mova o conteúdo da pasta Enviados para ela. Este procedimento, inclusive, é muito utilizado por clientes locais de *e-mail*, entre eles o *Outlook* e o *Pine*.

Conselho: Para aumentar a performance de sua sessão de *Webmail*, retire sempre que possível as mensagens não mais necessárias das pastas, ou então mova-as para a pasta INBOX e baixe-as para seu computador através de um cliente local. Isso liberará espaço em sua conta no servidor e diminuirá o volume de informações a serem processadas.

10.3 Mensagem com arquivo anexo não é transmitida

Existem duas situações nas quais uma mensagem com arquivos em anexo não pode ser transmitida:

Uma delas é se o tamanho do arquivo anexo exceder ao tamanho da área livre disponível na conta do usuário. Visto que para todo *e-mail* enviado é feita uma cópia na pasta **Enviados**, o usuário deve ter certeza de que possui espaço livre em sua conta de pelo menos o dobro do tamanho do arquivo anexo a ser enviado. Em caso negativo, o usuário deve livrar espaço, seja apagando arquivos via um acesso remoto à sua conta, seja via removendo *e-mails* antigos, que não mais são necessários.

A outra situação é se o tamanho do arquivo exceder ao máximo permitido pelo protocolo de envio de mensagem, o SMTP. Tal valor é de 10000 KB (dez mil kilobytes). Neste caso, o usuário não será capaz de enviar este arquivo pelo *Webmail* sob nenhuma hipótese. O que ele pode fazer é se valer de um cliente de *e-mail* local, como o *Outlook*, dotado da capacidade de partir um arquivo anexo grande em quantas mensagens menores forem necessárias para transmití-lo. O destinatário poderá concatenar as partes do arquivo anexo quando as receber, recuperando sua integridade.

10.4 O *Webmail* sempre retorna em inglês ao invés de lembrar o idioma escolhido

Preferências como o idioma ficam armazenadas em um *cookie* no computador local do usuário. Este deverá se certificar de que seu navegador suporta *cookies* e que os mesmos são aceitos. Alguns navegadores removem os *cookies* quando o usuário o manda remover os arquivos temporários. O usuário deverá verificar se seu navegador possui este comportamento.

11 Notas sobre segurança

Devemos ter em mente que a segurança provida pelo servidor de *Webmail* é voltada à privacidade e genuidade da conexão a seus usuários. Não obstante, sendo um membro de uma rede, este servidor pode sofrer outros tipos de interferência que se encontram fora de seu escopo de ação.

A fim de ampliar a estabilidade do servidor, a implementação de filtros anti-SPAM é recomendada. O próprio CBPF possui tal tipo de filtro em sua rede.

Além disso, o uso de sistemas IDS (*Intrusion Deteccion Systems*) pode aumentar a segurança de um servidor de *Webmail*, evitando possíveis tentativas de invasão e de ataques ao mesmo. Novamente, a rede do CBPF possui sistemas deste tipo implementados, como por exemplo o *Snort*.

12 Conclusão

Ao final deste documento, vemos que o *Webmail* acrescido de encriptação de dados é um serviço ideal para empresas e outras entidades que possuam rede conectada à Internet e possuam muitos usuários.

O *Webmail* implementado no CBPF, por exemplo, oferece uma interface intuitiva e prática, além de estabilidade e segurança de conexão.

Devemos ainda salientar que, apesar do *Webmail* do CBPF funcionar em uma plataforma **Sun**, este pode ser implementado em outras, como **Linux**, outros **UNIX** ou **Windows**, por exemplo. Qualquer sistema moderno pode ser utilizado, desde que sejam feitas as substituições de programas necessárias para a devida plataforma.

13 Bibliografia

Sites:

- The IMAP Connection – " http://www.imap.org ".
- MySQL – " http://www.mysql.com ".
- The Apache Software Foundation – " http://www.apache.org ".
- PHP – " http://www.php.net ".
- Mod_ssl: The Apache Interface to OpenSSL – " http://www.modssl.org ".
- OpenSSL: The Open Source toolkit for SSL/TLS – " http://www.openssl.org ".
- SSLeay – " ftp://ftp.psy.uq.oz.au/pub/Crypto/SSL/ ".
- The Horde Project@horde.org - " http://www.horde.org ".
- IMP 2.2@horde.org - " http://www.horde.org/imp/2.2/ ".
- Freeware for Solaris – " http://www.sunfreeware.com ".
- RFC-INDEX. All RFC's at the same place – " http://rfc.x42.com ".

Artigos:

- "Comparing Two Approaches to Remote Mailbox Access: IMAP vs. POP" – Gray, Terry – University of Washington, gray@cac.washington.edu, 18 de setembro de 1995.
- "Message Access Paradigms and Protocols" – Gray, Terry – University of Washington, gray@cac.washington.edu, 28 de setembro de 1995.
- "RFC1733: Distributed Electronic Mail Models in IMAP4" – Crispin, Mark R. – University of Washington, MRC@cac.washington.edu, dezembro de 1994.
- "Scalable webmail HOW-TO" – Belich, Jason – macmaster@pobox.com, v1.0, 11 de agosto de 1999.

Listas de discussão:

- IMP – imp@lists.horde.org .

14 Glossário

- **BSD** – significa *Berkeley Software Design*, e representa uma categoria à qual vários sistemas operacionais UNIX e clones UNIX pertencem;

- **Certificado digital** – é um arquivo criptografado que garante a identidade de um *site*. Pode ser gerado pelo próprio *site*, ou adquirido de uma empresa certificadora;

- **Certificate Authority** – autoridade responsável pela distribuição de certificados digitais. Pode ser um serviço residente em determinado computador para uma empresa, ou uma empresa especializada em comercializar certificados;

- **Cliente** – classificação de todo computador que usufrui de algum serviço disponibilizado por um servidor. É uma denominação circunstancial, ou seja, nada impede que um cliente aja como servidor para outro cliente;

- **Cookie** – pequeno arquivo que um *site* distribui a um usuário que armazena certos valores que podem ser reutilizados em uma conexão posterior com este *site*. Geralmente são usados para armazenar informações individuais que são freqüentemente utilizadas por cada usuário;

- **Criptografia** – é a prática de codificar uma informação;

- **Daemon** – aplicativo de controle de serviço, capaz de ser executado automaticamente pelo sistema;

- **Domínio** – para a Internet, representa o conjunto de IPs de rede que uma empresa ou entidade tem direito de uso, de acordo com seu órgão regulamentador de domínios local;

- **E-mail** – significa correio eletrônico, e se refere a um formato de mensagem que pode ser enviada através de uma rede;

- **Encriptação** – no que diz respeito a informações eletrônicas, é a prática de criptografar um dado;

- **HTML** – significa *Hypertext Markup Language*. É o padrão da Internet para escrita de informações em hipertexto;

- **HTTP** – significa *Hypertext Transfer Protocol*. É o protocolo utilizado para a transferência de documentos HTML.

- **HTTPS** – é a implementação de um túnel SSL sobre o prolocolo HTTP;

- **IDS** – sigla de *Intrusion Deteccion System*. É uma classe de programas dedicados a monitorar uma rede buscando indícios de tráfego ilegal e possíveis tentativas de invasão;

- **IMAP** – significa *Internet Message Access Protocol*, o protocolo de acesso a mensagens na Internet;

- **Includes** – são arquivos necessários para a compilação de um programa. Fornecem a capacidade de um programa acessar certas funções;

- **ISP** – significa *Internet Service Provider* (Provedor de Acesso à Internet), e é a forma mais comum de acesso à Internet de um usuário comum;

- **LDAP** – significa *Lightweight Directory Access Protocol*, e é um protocolo utilizado para acessar um serviço de diretório remoto;

- **Link** – é uma funcionalidade do HTML. Permite que o usuário acesse um conteúdo em um *site* a partir de uma referência em outro;

- **Linux** – é um sistema operacional clone do UNIX para plataforma Intel de 32 bits. Sua maior característica é a de ser inteiramente composto de código aberto. Está disponível no mercado em inúmeras distribuições, como por exemplo a Conectiva, o RedHat, o Mandrake, a Caldera, o SuSE, o Slackware e o Debian;

- **Login** – é a desegnação do usuário requerida para fornecer acesso a um serviço em específico;

- **Número IP** – IP significa *Internet Protocol*. O número IP fornece o endereço de um determinado computador na rede;

- **Off-line** – estado de não-conexão com determinado serviço;

- **Open Source** – significa código aberto ao público. É uma característica de alguns programas, cujas empresas fornecem seu código, permitindo que usuários comuns tornem-se desenvolvedores ao invés de apenas consumidores finais;

- **Pass phrase** – é uma senha composta de mais de uma palavra, da qual muitos utilitários SSL se valem para aumentar a segurança de certos serviços;

- **POP** – significa *Post Office Protocol*, e é um protocolo utilizado para a transferência de *e-mail* de um servidor a um cliente;

- **Porta de acesso** – é um endereço específico atribuído a um serviço. Algumas portas são padronizadas, como por exemplo: porta 80 – HTTP, porta 443 – HTTPS, porta 143 – IMAP, porta 993 – IMAPS (IMAP com SSL);

- **Reboot** – é o ato de reiniciar o sistema operacional de um computador;

- **RFC** – significa *Request For Comments*, e é um documento que determina o significado de termos e padroniza a funcionabilidade de protocolos;

- **Root** – é o superusuário, ou seja, aquele que pode tomar qualquer atitude em um sistema de um computador sem ser restringido por níveis de segurança e autorização;

- **Runlevel** – é o nível de execução em que o sistema operacional se encontra. O runlevel 3, por exemplo, é o nível no qual o computador suporta multitarefas e multiusuários;

- **Servidor** - classificação de todo computador que dispõe algum serviço a um cliente. É uma denominação circunstancial, ou seja, nada impede que um servidor aja como cliente de outro servidor;

- **Site** – para a Internet, é a localização de todos os documentos HTML de um servidor;

- **Software** – é o mesmo que programa;

- **Solaris** – é o sistema operacional UNIX fabricado pela empresa Sun Microsystems;

- **SMTP** – significa *Simple Mail Transfer Protocol*, e é o protocolo responsável pelo envio de *e-mail* do cliente para o servidor de correio eletrônico;

- **SPAM** – é o termo designado a mensagens indevidas, que têm como intuito espalhar desinformação e altos níveis de tráfego em servidores de *e-mail*. Provocam lentidão nesses servidores, chegando até mesmo a provocar negação de serviço. Disseminar SPAM é ilegal

em diversos países e passível de multa àté prisão. Apesar disso é uma prática extremamente comum nos dias de hoje e deve ser sempre observada pelos administradores de rede;

- **SSL** – significa *Secure Socket Layer*, que tem por função promover privacidade e certificação de identidade entre dois computadores quando estes estabelecem uma transação de dados. O SSL se dá de forma automática e transparente ao usuário, ou seja, este não precisa dispender nenhuma atenção especial ao seu funcionamento;

- **Script** – é uma forma de linguagem, que é interpretada e executada linha a linha diretamente do código fonte ao invés de compilada antes da execução;

- **Túnel SSL** – é a implementação de SSL para garantir a privacidade da conexão entre um servidor e um cliente;

- **UNIX** – é um tipo de sistema operacional com diversas distribuições no mercado. Como exemplo temos o AIX (criado pela IBM), o IRIX (Sgi), o UNIXWARE (Novell) e o Solaris (Sun Microsystems). Este último é o utilizado no *Webmail* da rede do CBPF;

- **Web browser** – é um programa que um usuário utiliza para visualizar páginas HTML de um servidor. É também conhecido como navegador;

- **Webchat** – é uma interface HTML para conversação em tempo real entre diversas pessoas;

- **Webmail** - é uma interface HTML que age como cliente de *e-mail*;

- **Windows** – tipo de sistema operacional criado pela Microsoft Inc., muito popular devido à sua facilidade de uso. Existe em diversas versões, desde para servidores (Windows NT e 2000), computadores pessoais (Windows 95, 98 e Millenium) àté computadores de bolso (Windows CE).