FURB

FERRAMENTA DE CONTROLE DE E-MAILS E ANTI-*SPAM*

Guilherme Luís Eberhardt

Prof. Francisco Adell Péricas- Orientador

Roteiro da Apresentação

- Introdução
- Objetivos
- Fundamentação teórica
- Ferramenta Atual
- Trabalhos Correlatos
- Desenvolvimento do Sistema
- Resultados e discussões
- Conclusão
- Extensões

Introdução

- Administração da área de correio eletrônico;
- *SPAMS*;
- POSTFIX.

Objetivos do Trabalho

- desenvolver uma ferramenta que colete as informações, como destinatário, remetente, assunto, data, hora, entre outras, dos e-mails que entram e saem de uma organização armazenando-os em uma base de dados, integrada no gerenciador de caixa postal do *Mail Transfer Agent* (MTA) Postfix;
- desenvolver uma ferramenta de anti-*spam* com base nos e-mails coletados operando integrado ao Postfix;
- gerenciar e-mails que entram e saem de uma organização, podendo assim ser feita uma possível auditoria.

E-MAILS

E-mail é uma ferramenta de trabalho e, principalmente, um meio de comunicação.

História:

- o surgimento do e-mail é anterior ao da Internet;
- em 1965, tem-se notícia do primeiro sistema criado de troca de mensagens entre computadores;
- acredita-se que os primeiros sistemas criados com tal funcionalidade foram o Q32 da *System Development Corporation* (SDC) e o CTSS do *Massachusetts Institute of Technology* (MIT);
- Em 1971, Ray Tomlinson iniciou o uso do sinal @ (arroba) para separar os nomes do usuário e da máquina no endereço de correio eletrônico.

Terminologias utilizadas:

- *auto-responders* (resposta automática) — O software do receptor responde automaticamente após receber a mensagem;
- *bulk, bulking* ("baciada"): Sinônimo de *spam*, utilizado principalmente pelos *spammers;*
- *commercial e-mail* (e-mail comercial): e-mail enviado com finalidade comercial;
- *false positives* (positivo falso): e-mails identificados erroneamente como *spam* pelo filtro do receptor;
- *list broker* (revendedor de listas): revendedor de listas de endereços de e-mails, conhecido também como *spammer*;
- *spam* ou UCE (*Unsolicited Commercial E-mail*): e-mail encaminhado sem o consentimento do receptor;
- *spam filter*: software utilizado para filtrar e-mails, evitando ou anunciando a presença de *spam*;
- *subject line* (assunto): campo destinado a dizer qual a finalidade da correspondência.

Protocolos:

Os protocolos para Internet formam o grupo de protocolos de comunicação que implementam a pilha de protocolos sobre a qual a internet e a maioria das redes comerciais funcionam. Entre eles: POP3, IMAP e SMTP.

- *Post Office Protocol* (POP3) é o protocolo que é utilizado para acesso remoto a uma caixa de correio eletrônico;

- *Simple Mail Transfer Protocol* (SMTP) é um protocolo baseado em texto simples, onde um ou vários destinatários de uma mensagem são especificados e, no caso do *Mail Transfer Agent* (MTA) Postfix validando estes destinatários sendo, depois, a mensagem transferida;

- *Internet Message Access Protocol* (IMAP) é um protocolo de gerenciamento de correio eletrônico no qual as mensagens ficam armazenadas no servidor e o usuário pode ter acesso a suas pastas e mensagens em qualquer computador, tanto por webmail como por cliente de correio eletrônico;

Problemas:

Algumas das desvantagens do uso de e-mail encontram-se na falta de conhecimento da grande maioria dos internautas e, ainda, os spammers ou geradores de spam, grandes remetentes de vírus.

- *Spam*;
- Vírus.

POSTFIX

Postfix é um MTA, responsável pelo envio e recebimento das mensagens entre servidores, e é configurado para responder por um domínio, porém não entrega as mensagens aos clientes de e-mail (POP3), não baixa as mensagens de outros servidores, recebe mensagens quando enviadas diretamente a ele mas não vai buscar em outros servidores, não tem anti-vírus e nem outros filtros utilizados em servidores de e-mail, precisando de outros pacotes que se integram ao Postfix para configurar o que se chama de um servidor de e-mail.

Sub-programas e parâmetros:

postfix: programa que inicia ou interrompe o processo *master* e os *daemons* que auxiliam no seu funcionamento, que pode utilizar os seguintes parâmetros:

- *start*: inicia o serviço do *postfix*;
- *stop*: interrompe o serviço do *postfix*;
- *reload*: relê as configurações do *postfix*;
- *abort*: para o *postfix* no ato;
- *check*: verifica sintaxe dos arquivos;
- *flush*: parâmetro para o programa *postfix* no qual move todas as mensagens contidas nos diretórios “HOLD” dos usuários e coloca na pasta *incoming* e ainda força o reenvio de todos os e-mails na fila;

postcat: programa parecido com o *cat* do *shell*, exibe o conteúdo de um arquivo de e-mail;

postsuper: ferramenta de manutenção de fila do Postfix que utiliza os seguintes parâmetros:

- –H <mensagem>: marca a mensagem especificada como apta a ser movida para o diretório *incoming* do usuário;
- –d <mensagem>: deleta a mensagem especificada;
- –d ALL: deleta todas as mensagens;

postconf: ferramenta de configuração do Postfix.

MailDir:

O formato Maildir trata cada mensagem como um arquivo independente dentro de um diretório, por isso MAIL+DIR. Esse formato é bastante interessante porque agrega muitas vantagens:

- dispensa o uso de *LockFiles*, travamento de arquivos, ou seja, permite que o *MailBox* pode estar sendo escrito por vários programas ao mesmo tempo;

- não existe problemas com indexação do mailbox;

- torna-se desnecessário abrir e indexar o mailbox inteiro para extrair uma única mensagem, pois os e-mail são separados por arquivos;

- não existe a corrupção do *MailBox* pois é um diretório, ao máximo pode-se corromper uma única mensagem.

SPAM

Spam é o termo usado para se referir aos e-mails não solicitados, que geralmente são enviados para um grande número de pessoas. Quando o conteúdo é exclusivamente comercial, este tipo de mensagem também é referenciada como Unsolicited Commercial E-mail (UCE).

Os tipos mais comuns de *spam* são:

- boatos e correntes;
- propagandas;
- ameaças e/ou brincadeiras.

Como atuam os *Spammers*:

- listas de e-mails;

- através de servidores de e-mails mau configurados, esses servidores são chamados de open relay, algo como servidores de retransmissão de e-mails liberada;

- uso de falsos remetentes;

- uso de ferramentas capazes de enviar e-mails em grandes quantidades e outras que permitem falsificar o cabeçalho e outros campos de e-mail.

Trabalhos Correlatos

- Santos elaborou sua monografia voltada a programas e técnicas contra spam. Diante do grande crescimento de envio de e-mails não autorizados pelo usuário, caso de roubo de informação, envio de vírus e trojans, fez uma análise de mecanismos para combater spam, através de configuração, de filtros ou de programas de proteção.

- Dalazen, professor da UnB, publicou uma matéria referente ao controle de e-mail nas empresas, tendo como tema principal a dúvida se o empregador pode monitorar o e-mail do funcionário ou não.

Requisitos Funcionais

- O sistema deverá interpretar todos os e-mails que entram ou saem de um determinado servidor.
- O sistema deverá gerar uma lista com os assuntos mais utilizados para uma lista de spam.
- O sistema deverá emitir um relatório contendo os e-mails que entraram e saíram do servidor.
- O sistema deverá permitir que o administrador cadastre palavras chaves que determinem se um e-mail é spam ou não.
- O sistema deverá bloquear todos os e-mails que identifique como spam.
- O sistema deverá listar todos os e-mails bloqueados como SPAM para liberação dos usuários se necessário.
- O sistema deverá permitir o cadastro de usuários.
- O sistema deverá permitir que o administrador cadastre palavras chaves que determinem se um e-mail é um e-mail bloqueado ou não.

Requisitos Não Funcionais

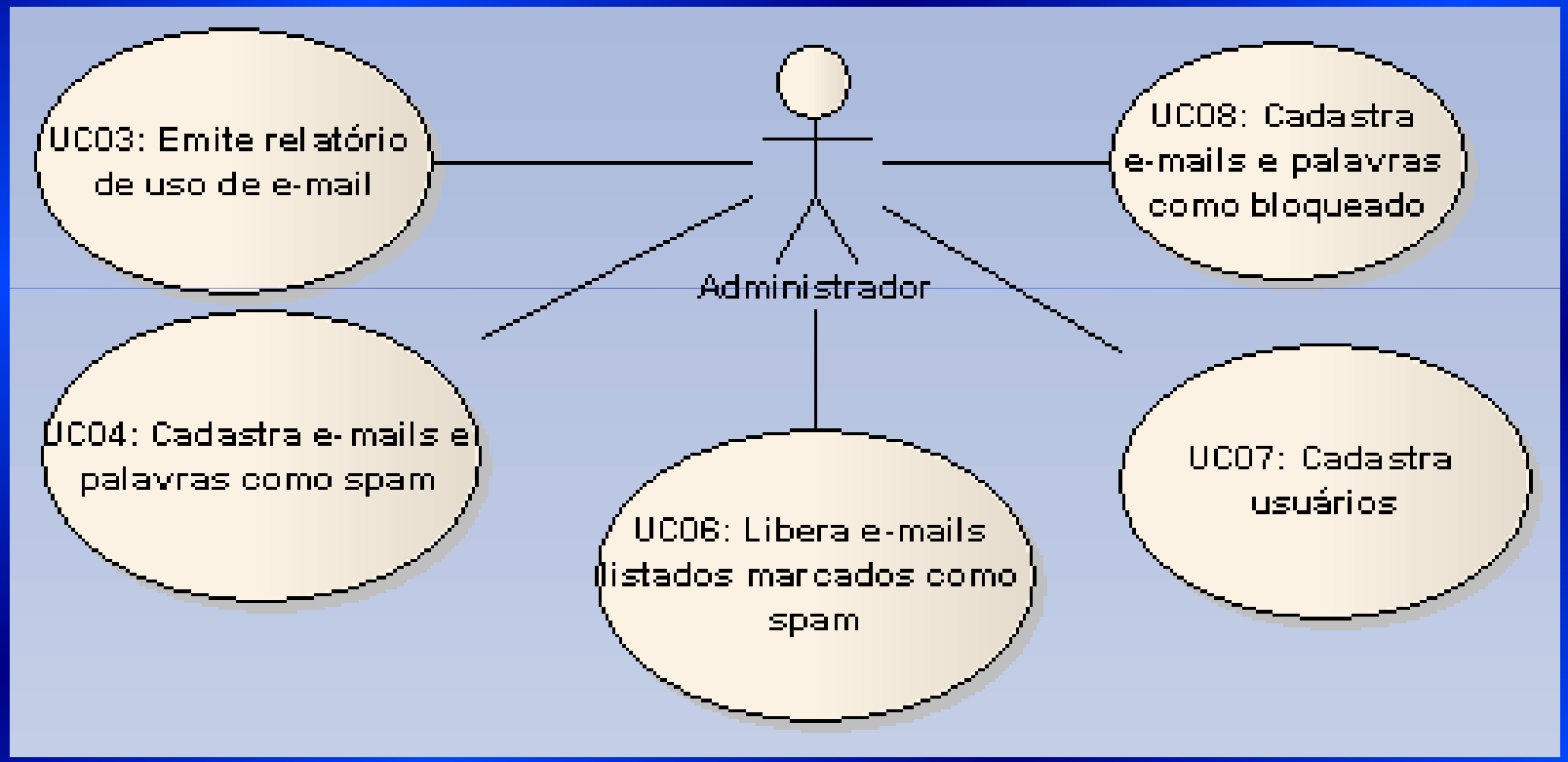
- O sistema deverá utilizar como linguagem de desenvolvimento o Perl.
- O sistema deverá utilizar como base de dados o MySQL.
- O sistema deverá utilizar como servidor de transporte de e-mail o Postfix.
- O sistema deverá ter como sistema operacional base qualquer distribuição Linux.

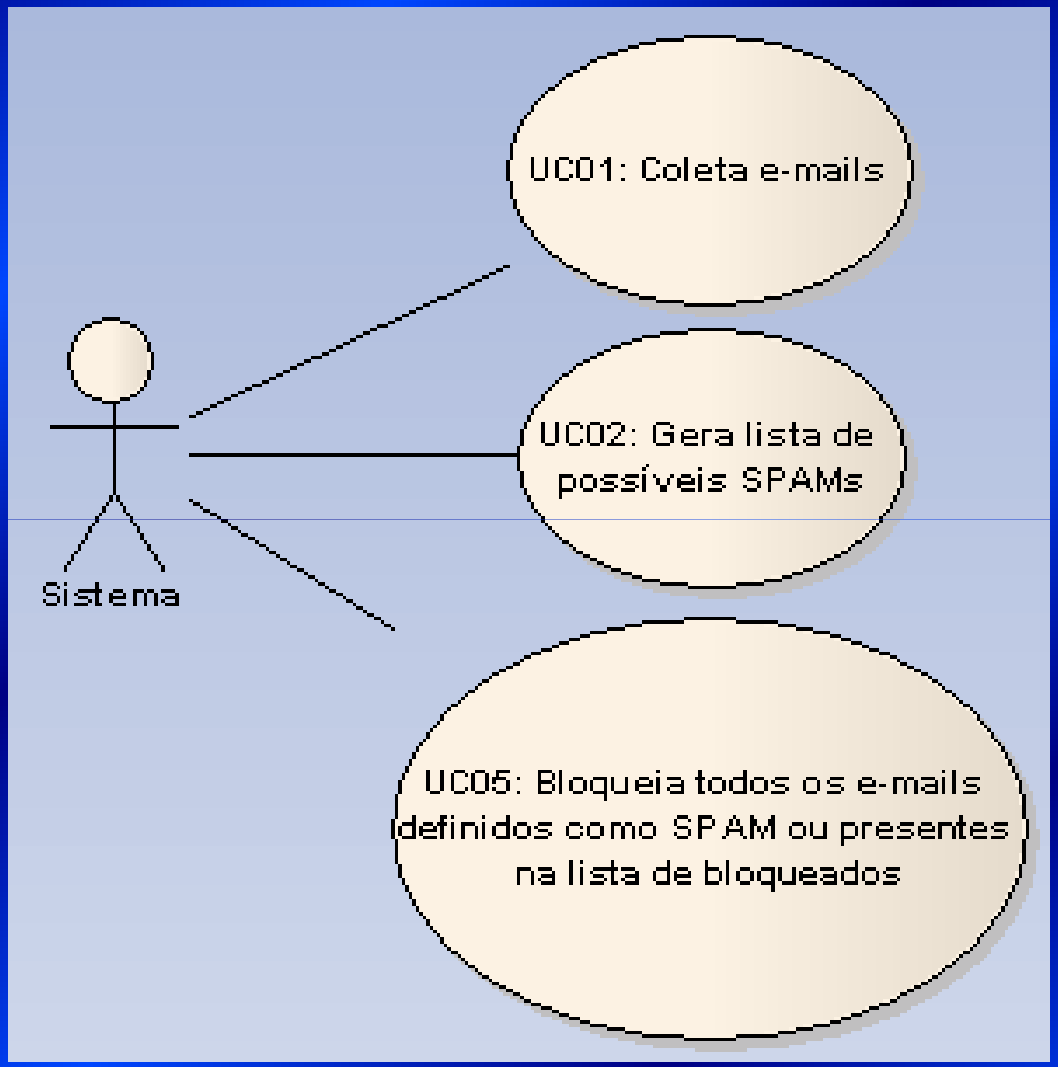
Especificação

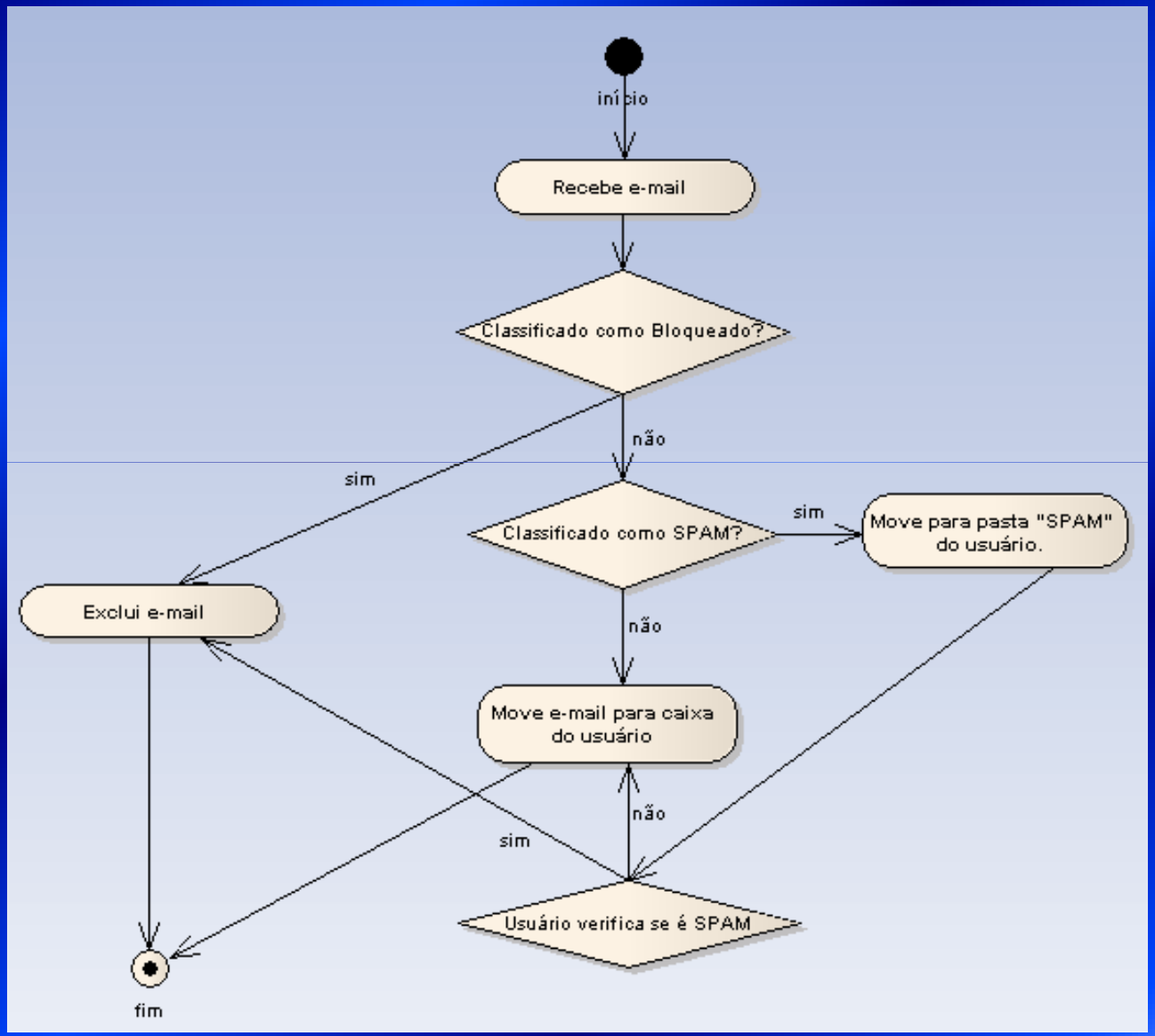
- Diagrama de casos de uso
- Diagrama de atividades
- Modelo de dados

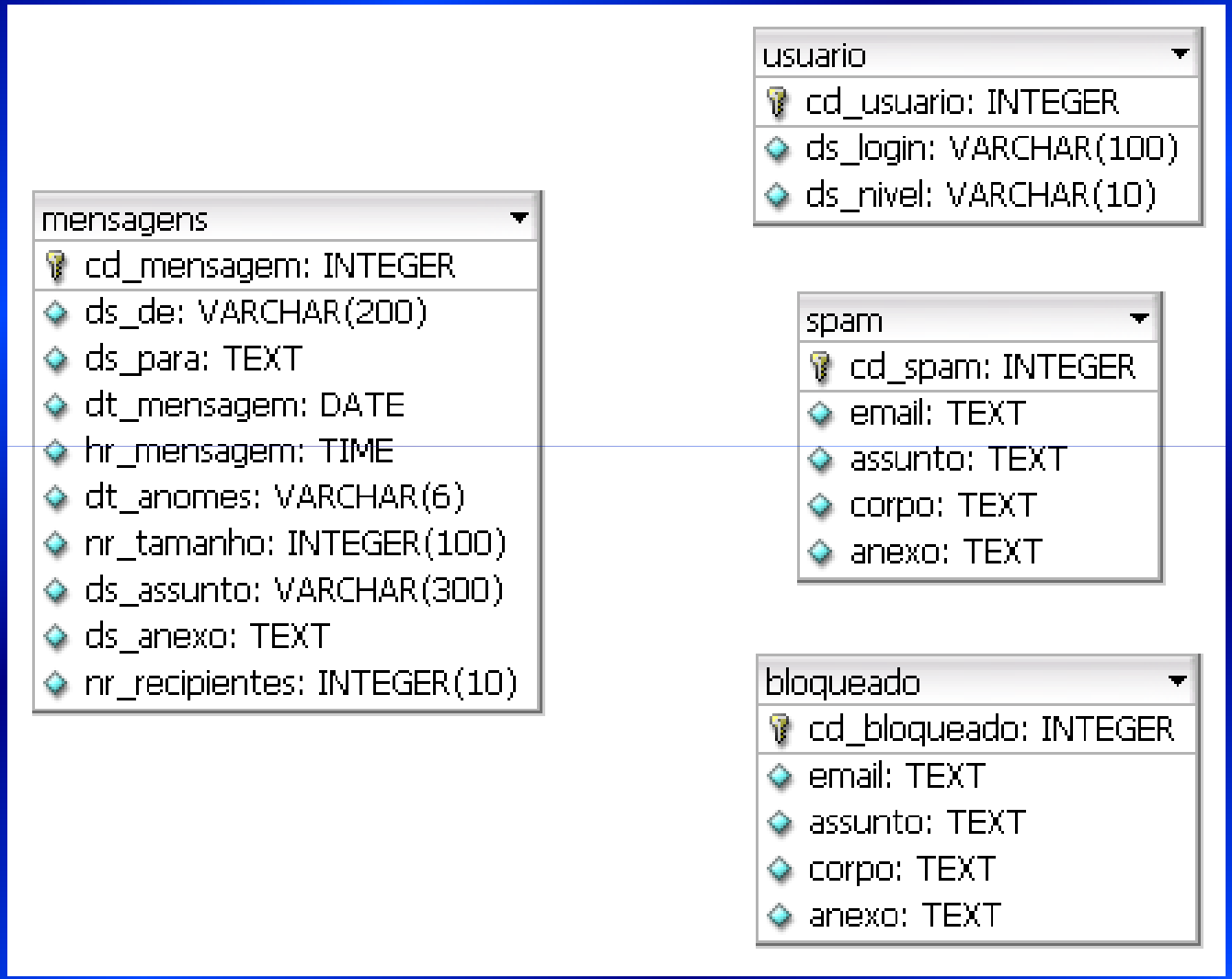
Ferramentas utilizadas

- Enterprise Architect
- DBDesigner


UC03: Emite relatório de uso de e-mail
UC08: Cadastra e-mails e palavras como bloqueado
Administrador
UC04: Cadastra e-mails e palavras como spam
UC06: Libera e-mails listados marcados como spam
UC07: Cadastra usuários


UC01: Coleta e-mails
UC02: Gera lista de possíveis SPAMs
Sistema
UC05: Bloqueia todos os e-mails definidos como SPAM ou presentes na lista de bloqueados

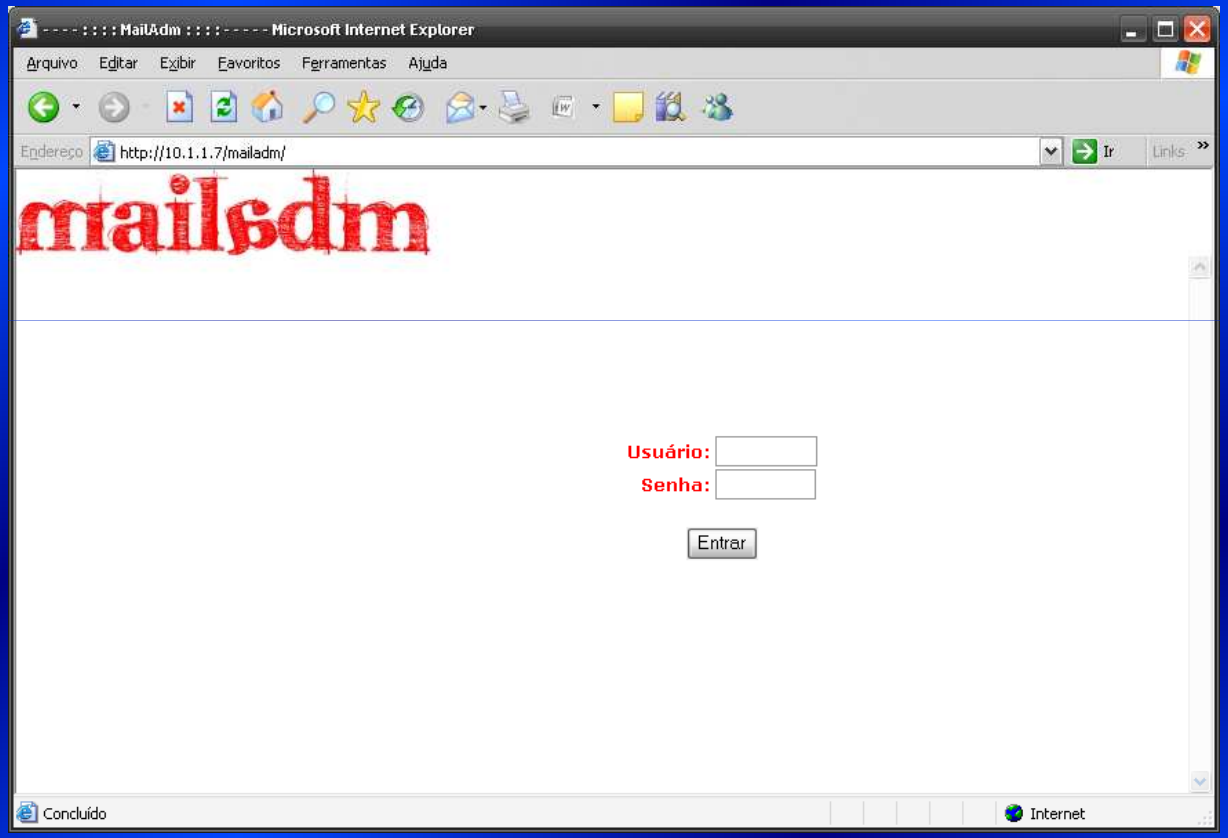

início
Recebe e-mail
Classificado como Bloqueado?
sim
não
Classificado como SPAM?
sim
Move para pasta "SPAM" do usuário.
Exclui e-mail
não
Move e-mail para caixa do usuário
não
sim
Usuário verifica se é SPAM
fim


usuario
cd_usuario: INTEGER
ds_login: VARCHAR(100)
ds_nivel: VARCHAR(10)
mensagens
cd_mensagem: INTEGER
ds_de: VARCHAR(200)
ds_para: TEXT
dt_mensagem: DATE
hr_mensagem: TIME
dt_anomes: VARCHAR(6)
nr_tamanho: INTEGER(100)
ds_assunto: VARCHAR(300)
ds_anexo: TEXT
nr_recipientes: INTEGER(10)
spam
cd_spam: INTEGER
email: TEXT
assunto: TEXT
corpo: TEXT
anexo: TEXT
bloqueado
cd_bloqueado: INTEGER
email: TEXT
assunto: TEXT
corpo: TEXT
anexo: TEXT

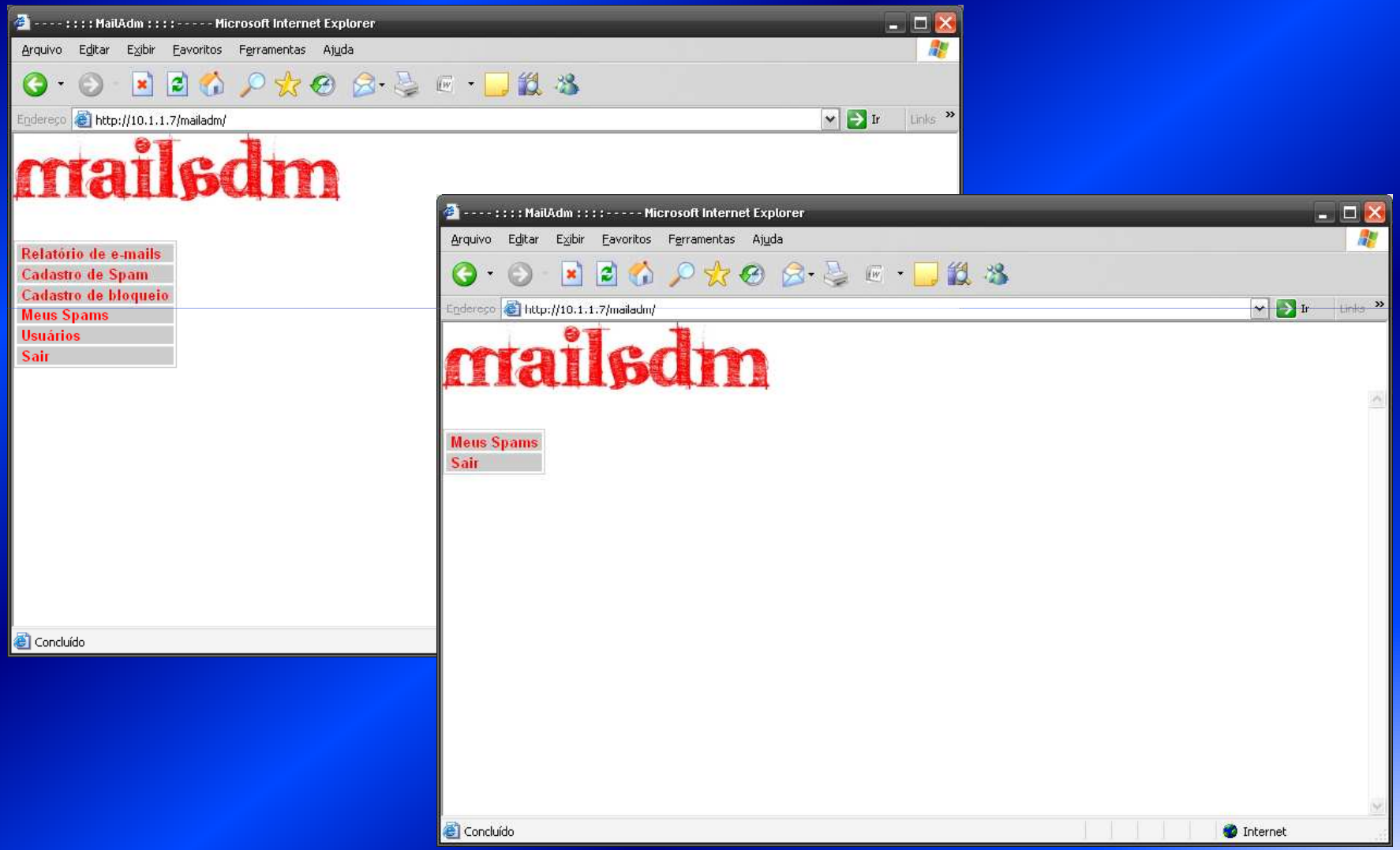
Implementação

- Desenvolvimento em Perl
- Banco de dados MySQL

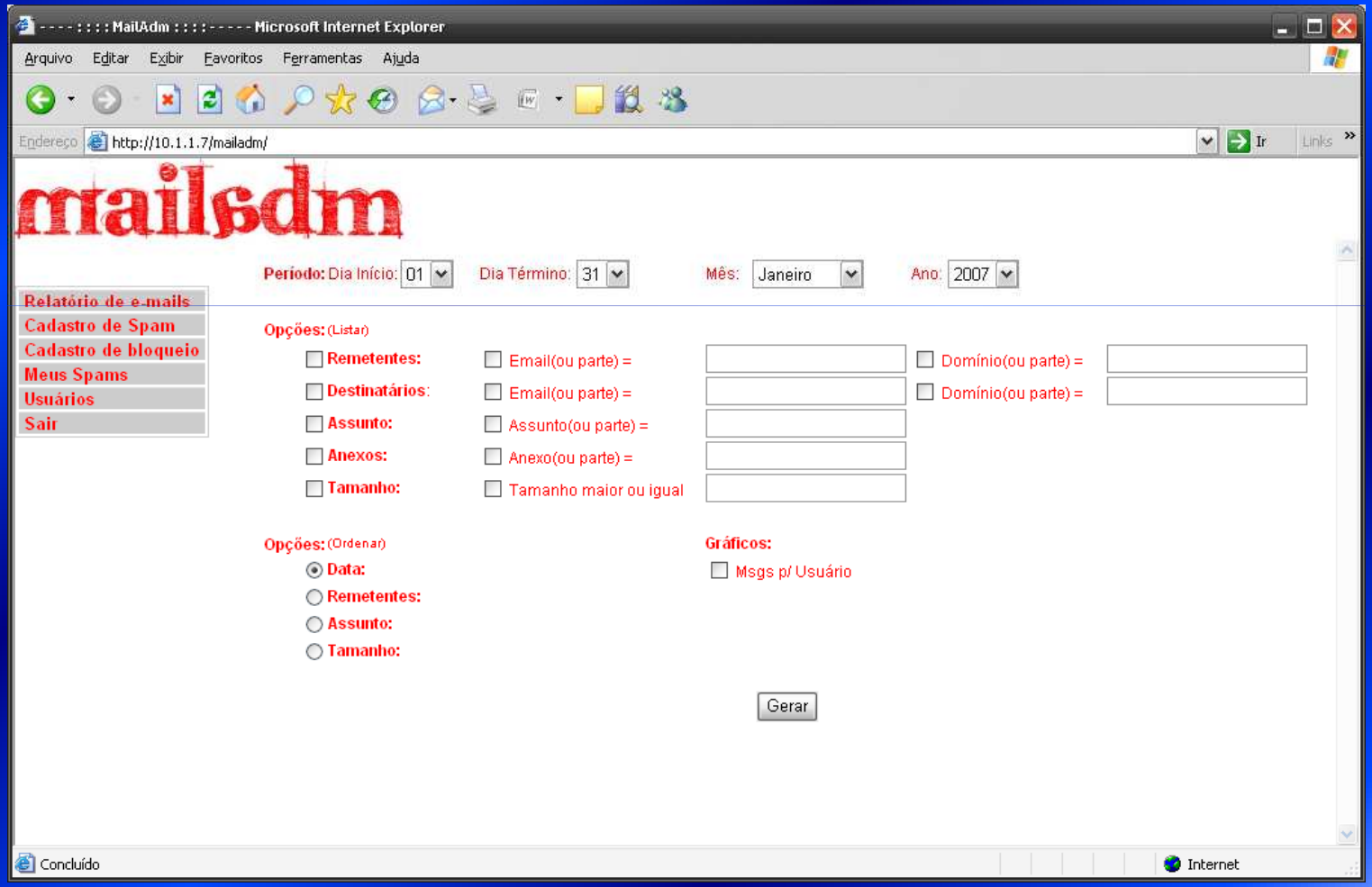
Operacionalidade



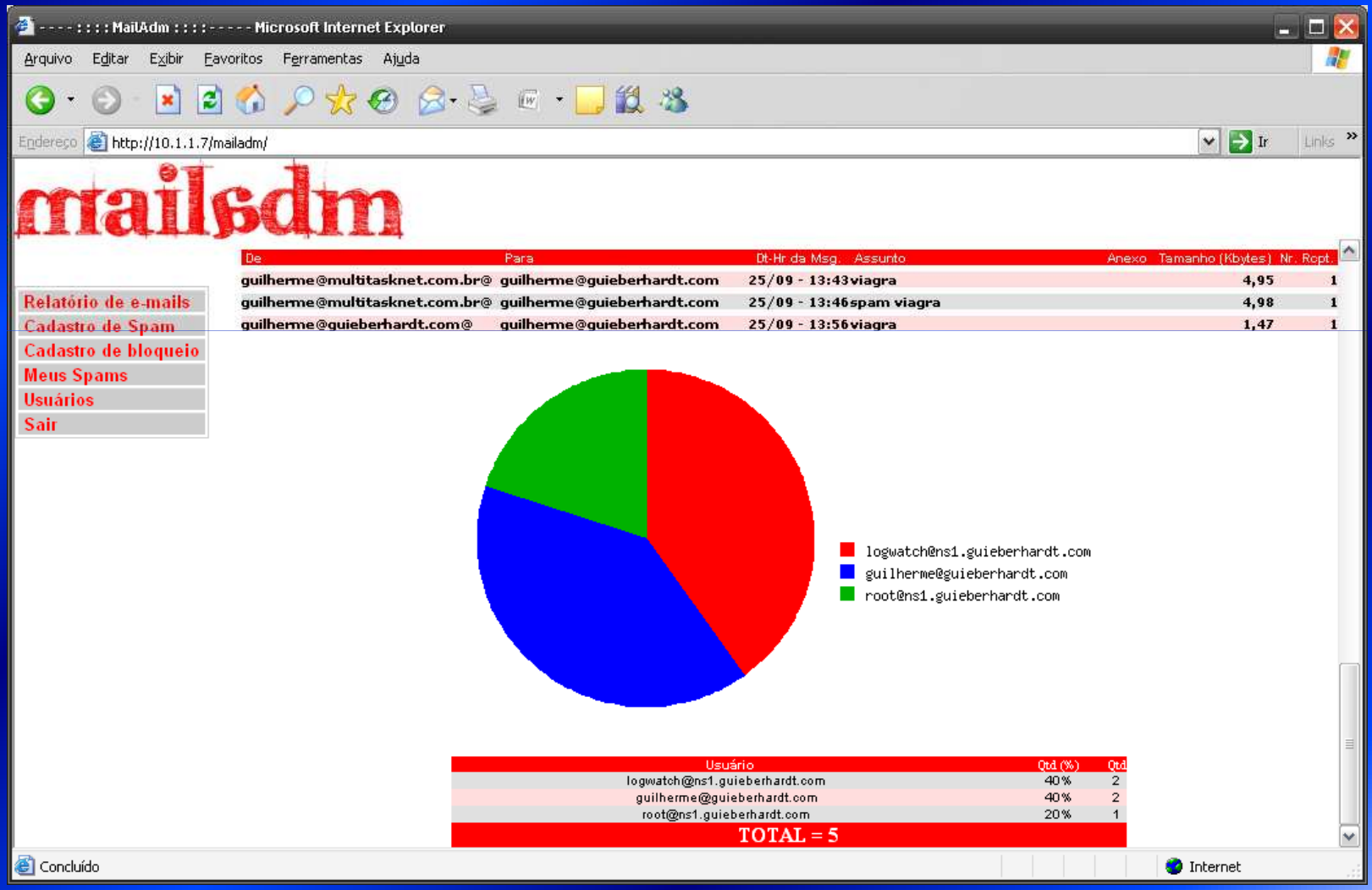
Operacionalidade



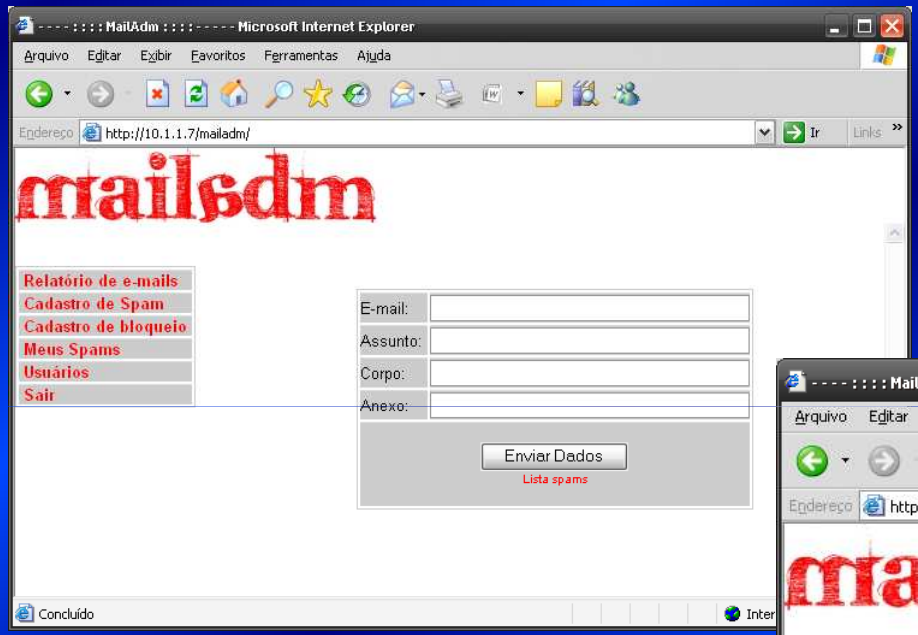
Operacionalidade

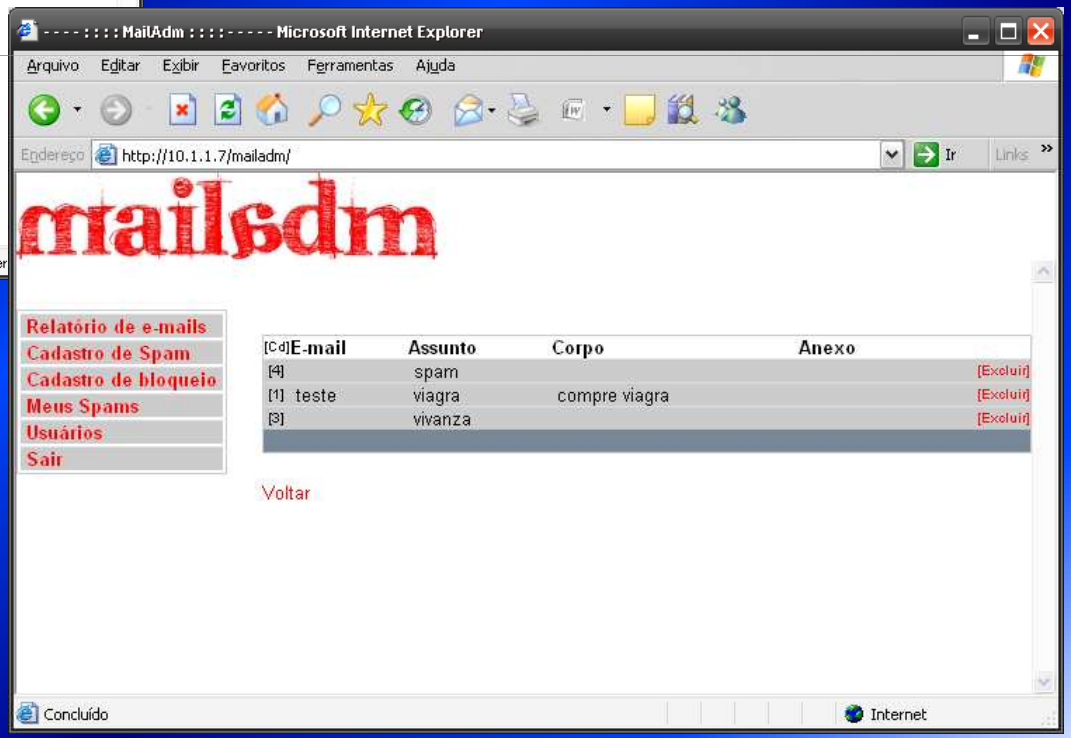


Operacionalidade

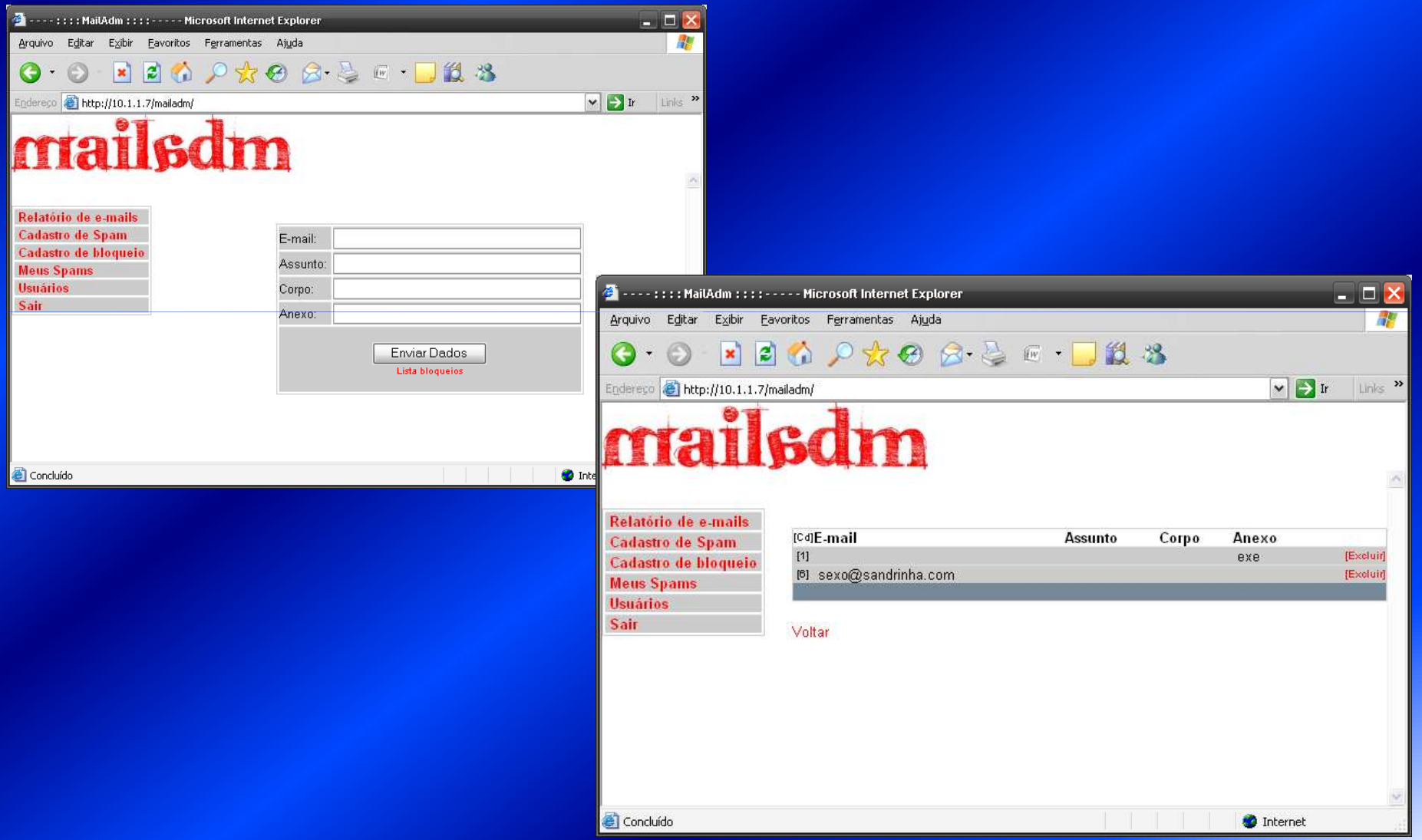


Operacionalidade

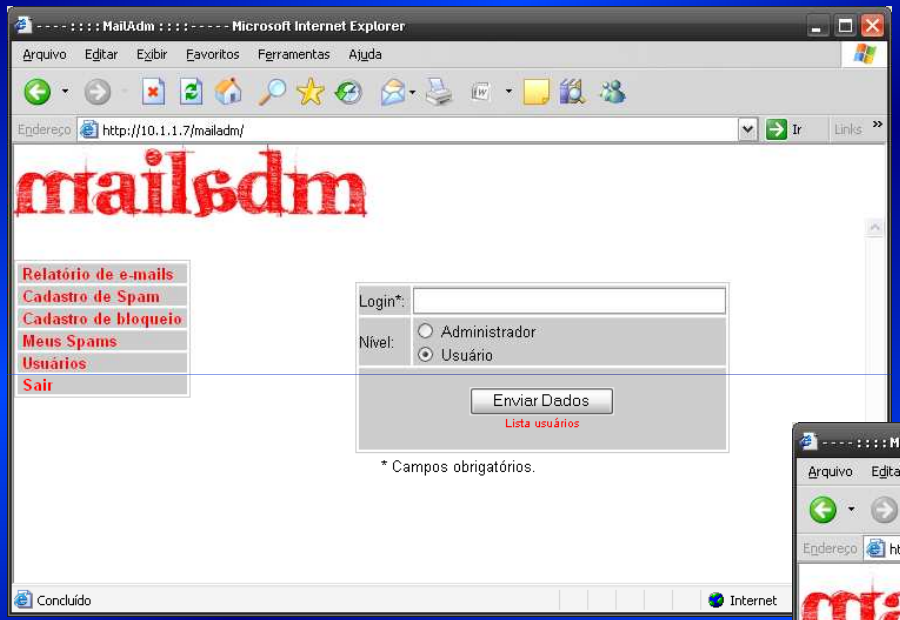


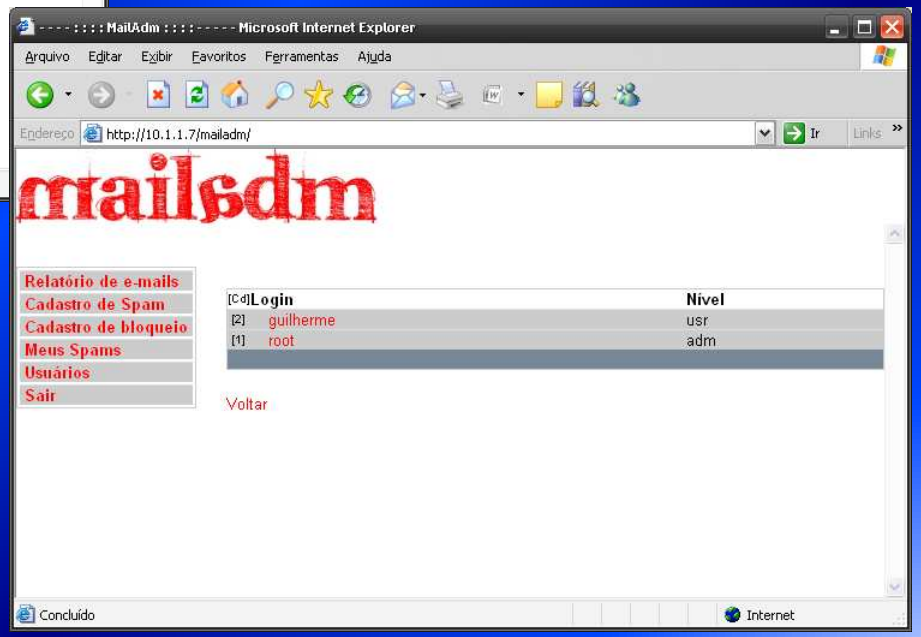


Operacionalidade

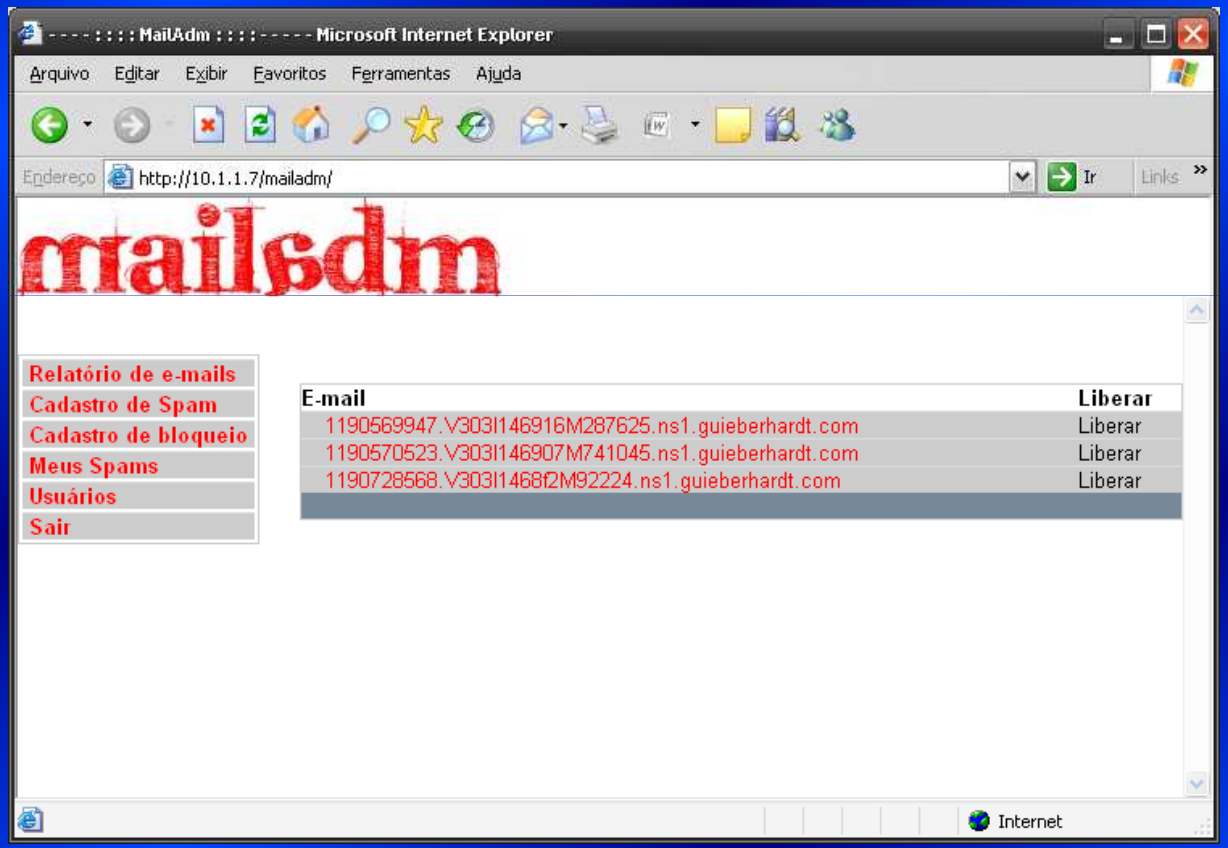


Operacionalidade





Operacionalidade



Resultados e discussões

- Proporcionou o controle de e-mails de entrada e saída do servidor por usuário
- Auxiliou no combate ao *spam*
- Facilitou o cadastro de regras de e-mails para combate a *spam* e bloqueio de mensagens
- Auxiliou na filtragem de e-mails com extensões ou arquivos que possam ser vírus

Conclusão

- Objetivos atingidos
- Dificuldades
- Limitações

Extensões

- Atualizações do sistema devido às atualizações dos servidores de e-mail
- Controle de regras de firewall via *browser*
- Implementação de inteligência artificial no sistema de anti-*spam*

Agradecimentos