Universidade de São Paulo
Centro de Computação Eletrônica

"Ferramenta SiRI e sua utilização pela Equipe de Segurança da USP"

Apresentação:

Mauro Cesar Bernardes

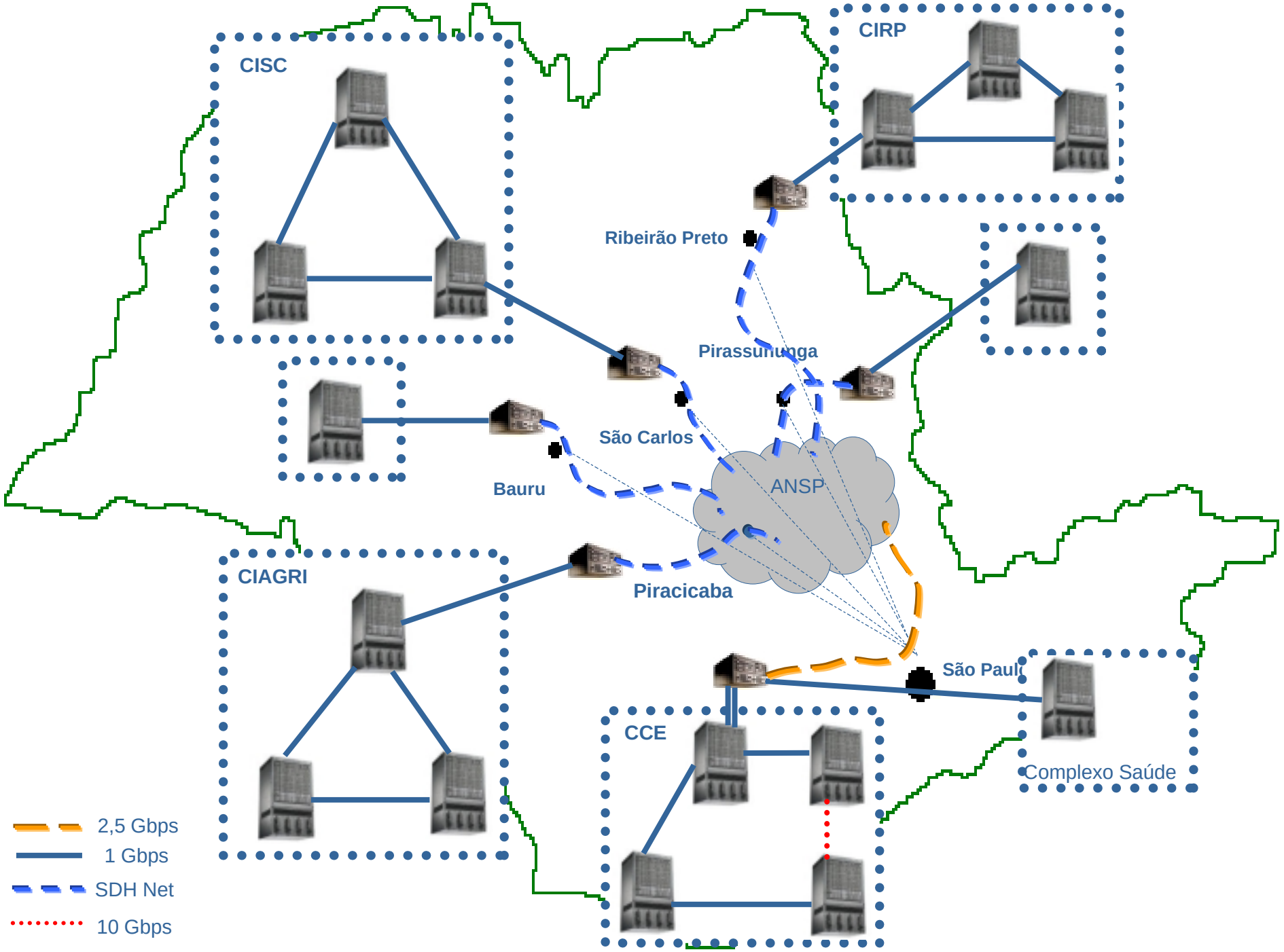
Rafael Nogueira Tavares

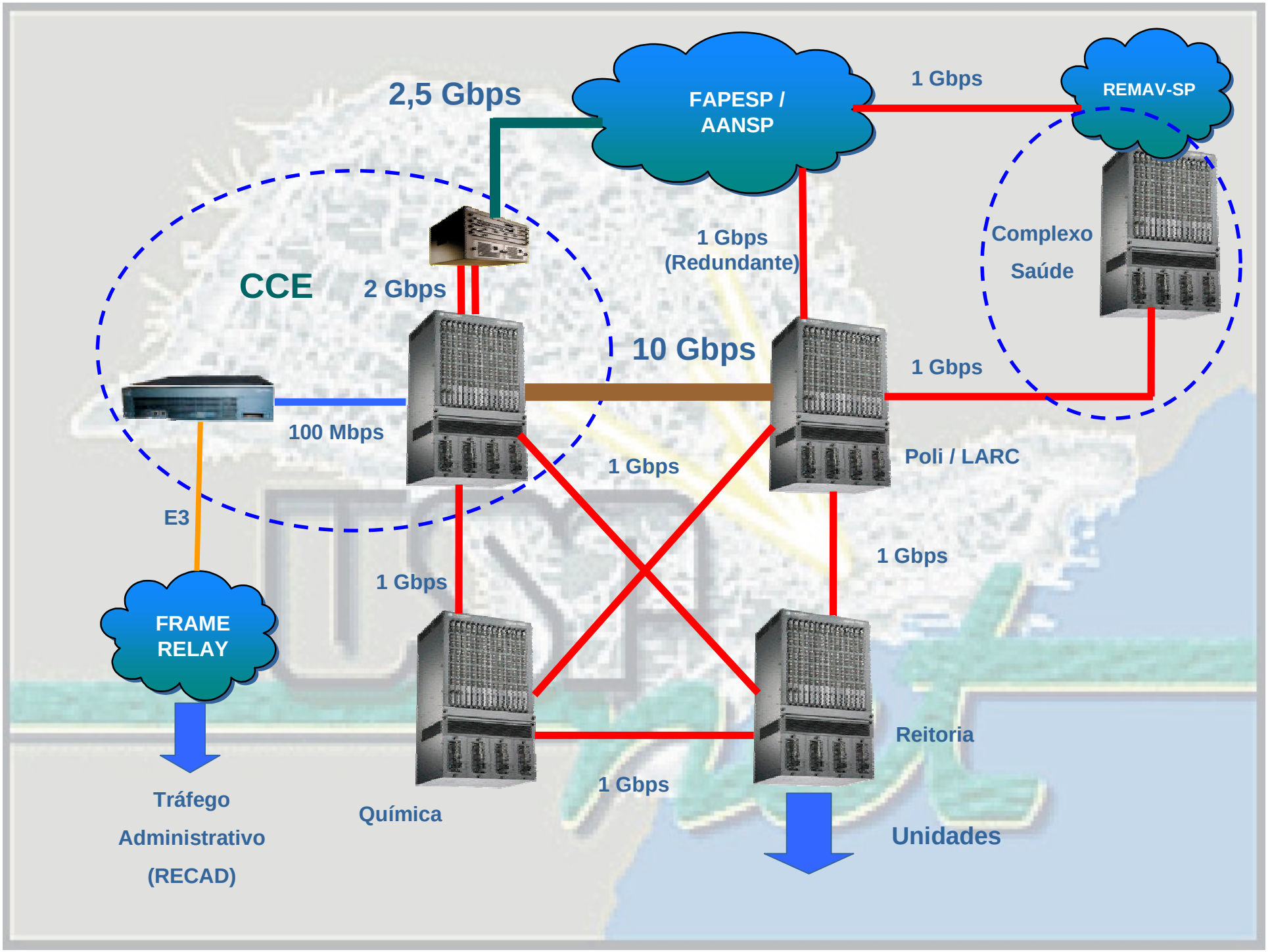
Abril de 2003

Estrutura da Apresentação

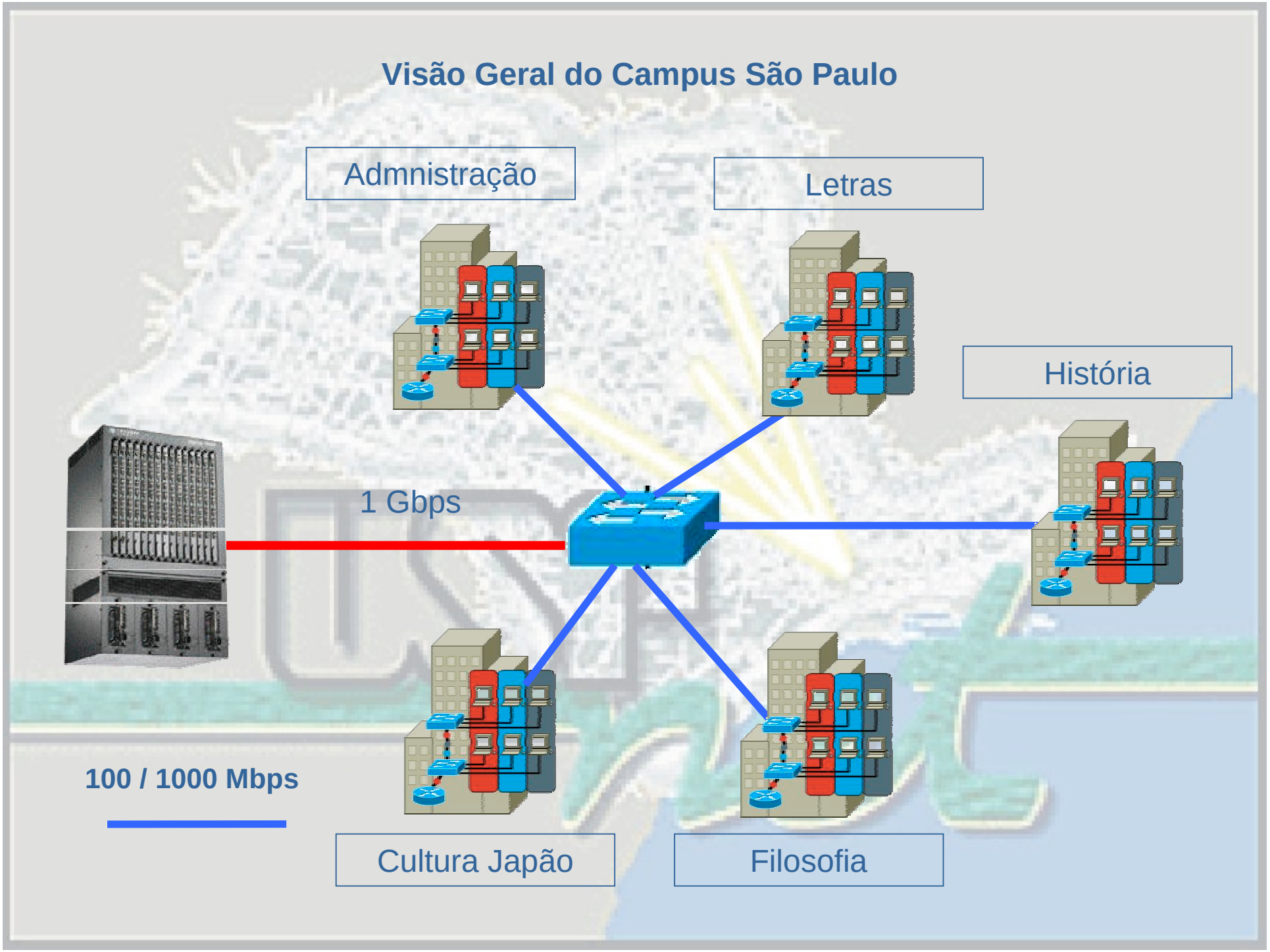
- Motivação
  - Uma visão geral da USPNet
  - A Equipe de Segurança
  - O cenário antigo
- A ferramenta SiRI
  - Funcionalidades da Ferramenta
  - O cenário atual
- Trabalhos futuros
- Debate.

Uma visão Geral da USPNet


CISC
CIRP
Ribeirão Preto
Pirassununga
São Carlos
Bauru
ANSP
CIAGRI
Piracicaba
São Paulo
CCE
Complexo Saúde
2,5 Gbps
1 Gbps
SDH Net
10 Gbps


2,5 Gbps
FAPESP / AANSP
1 Gbps
REMAV-SP
CCE
2 Gbps
1 Gbps (Redundante)
Complexo Saúde
10 Gbps
1 Gbps
100 Mbps
1 Gbps
Poli / LARC
E3
1 Gbps
1 Gbps
FRAME RELAY
Reitoria
1 Gbps
Tráfego Administrativo (RECAD)
Química
Unidades

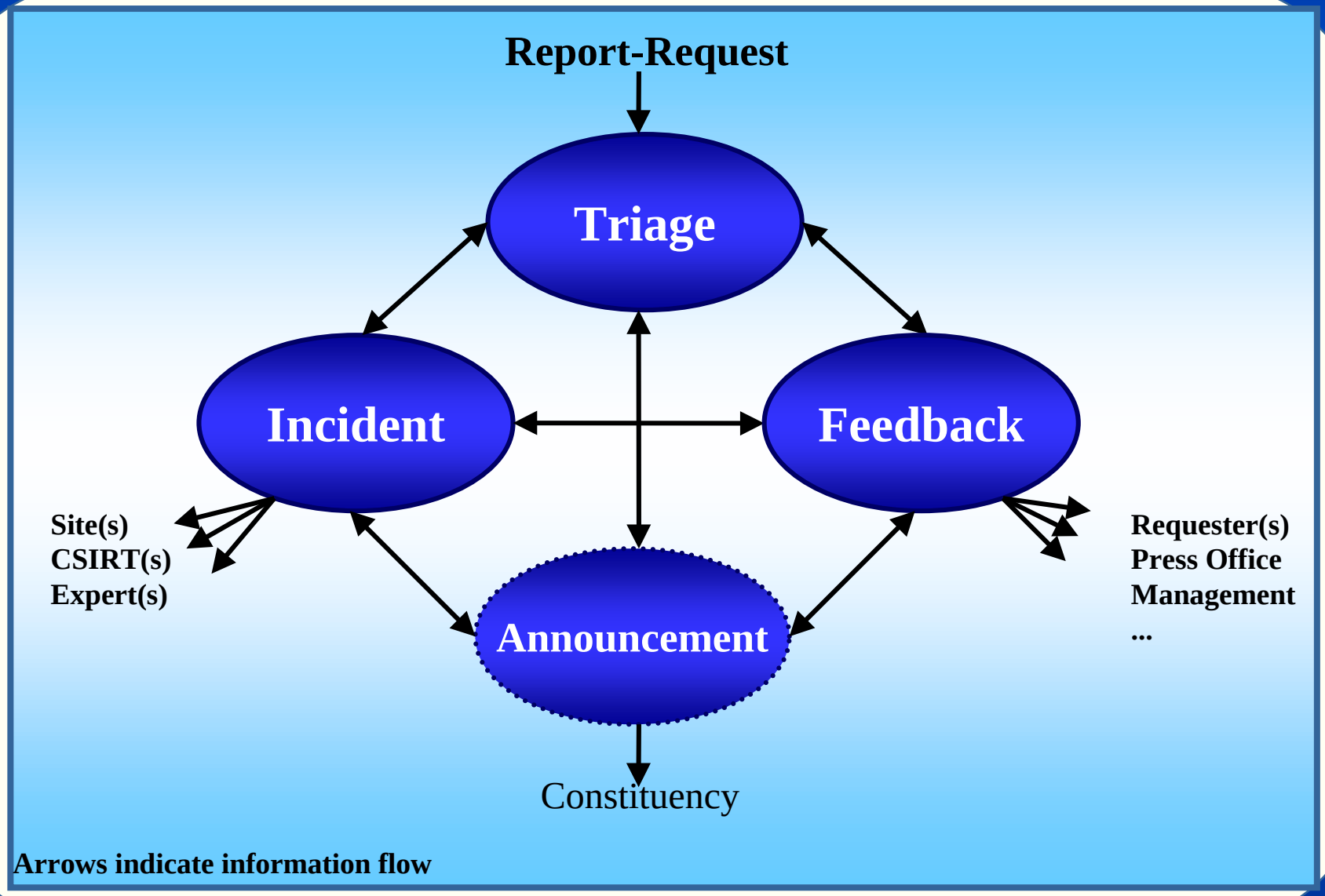
Visão Geral do Campus São Paulo



A Equipe de Segurança

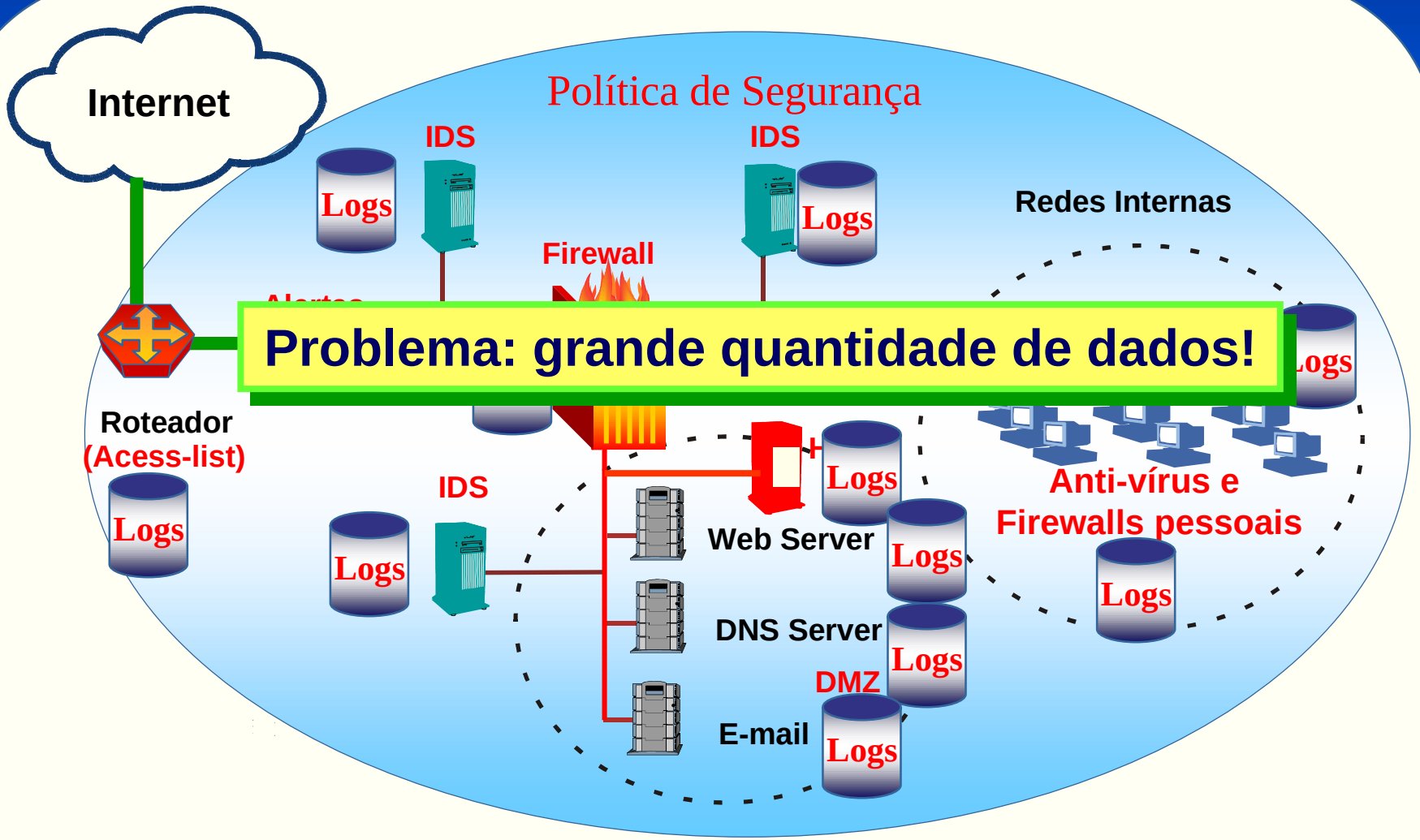
- **Centro de Computação Eletrônica**
  - Responsável pelo security@usp.br, abuse@usp.br, ...
  - 4 Analistas
  - 4 Ténicos/operadores
  - Atendimento 24x7
- **Administradores em cada Unidade**
- **Trabalho cooperativo e colaborativo**

IR Service Functions Overview



Fonte: http://www.sei.cmu.edu/publications/documents/98.reports/98hb001/98hb001abstract.html

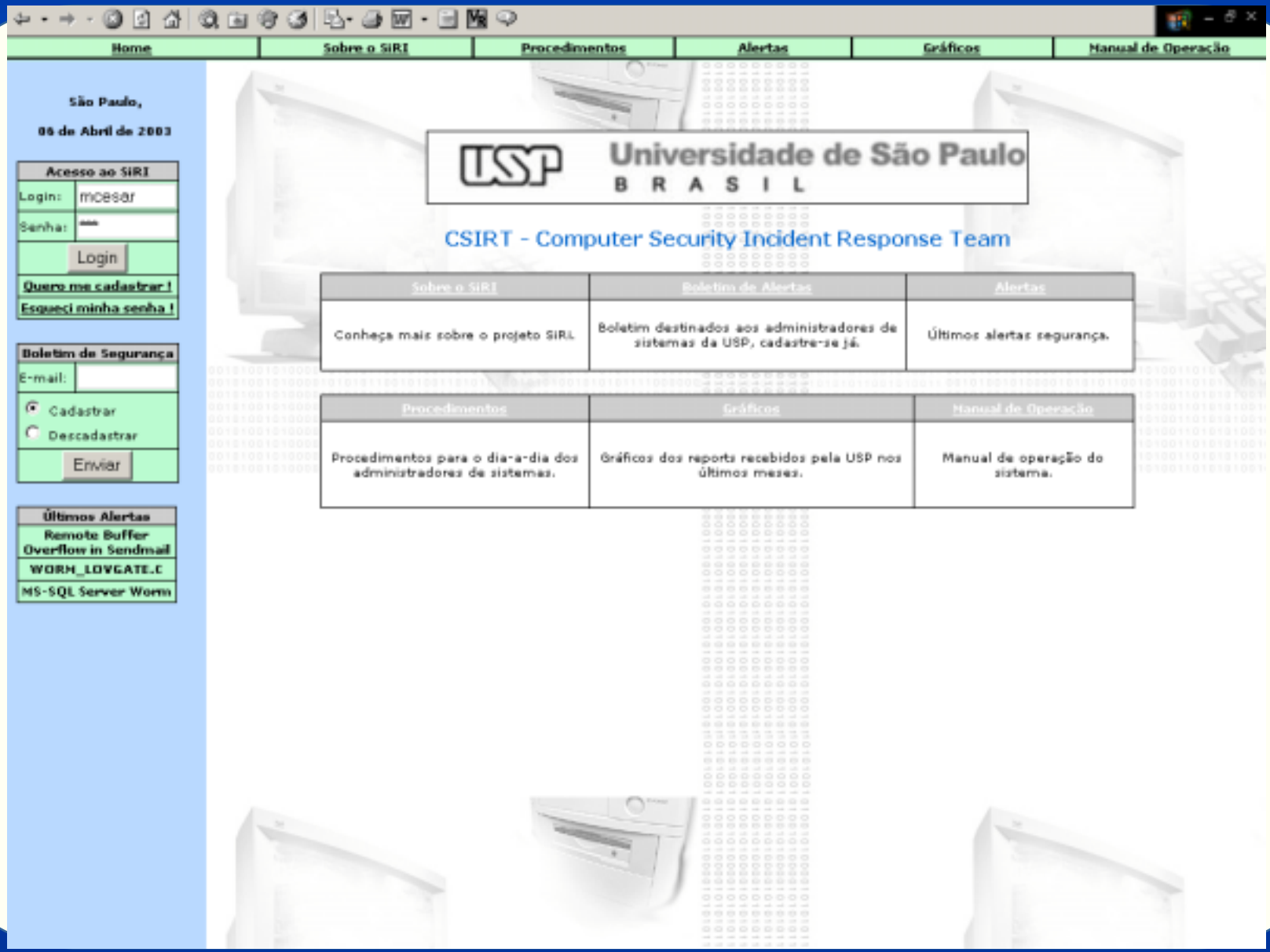
Problemas no cenário antigo



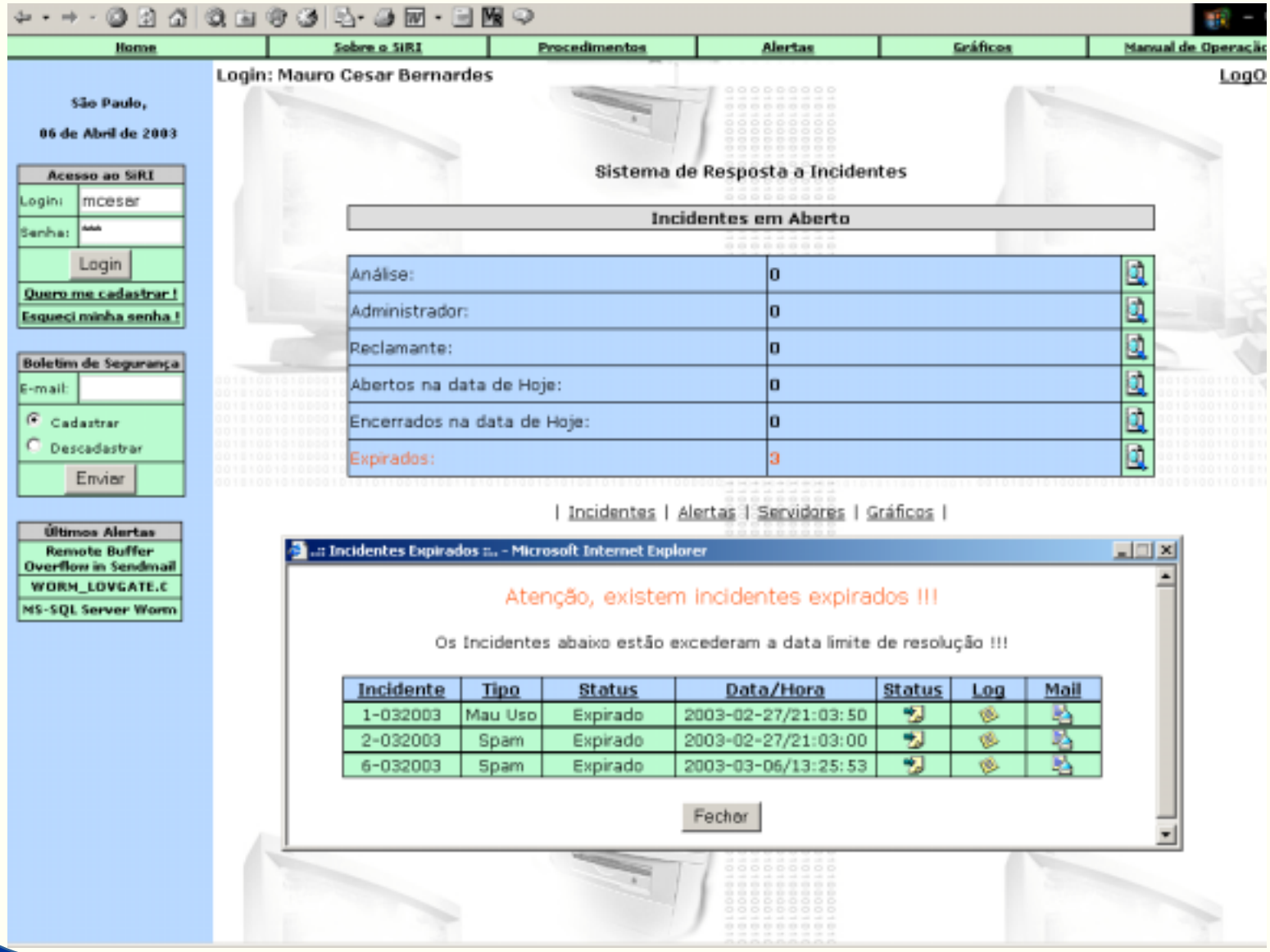
“O problema onde há um excesso de dados pode ser tão prejudicial quanto a sua falta”

A Ferramenta SiRI

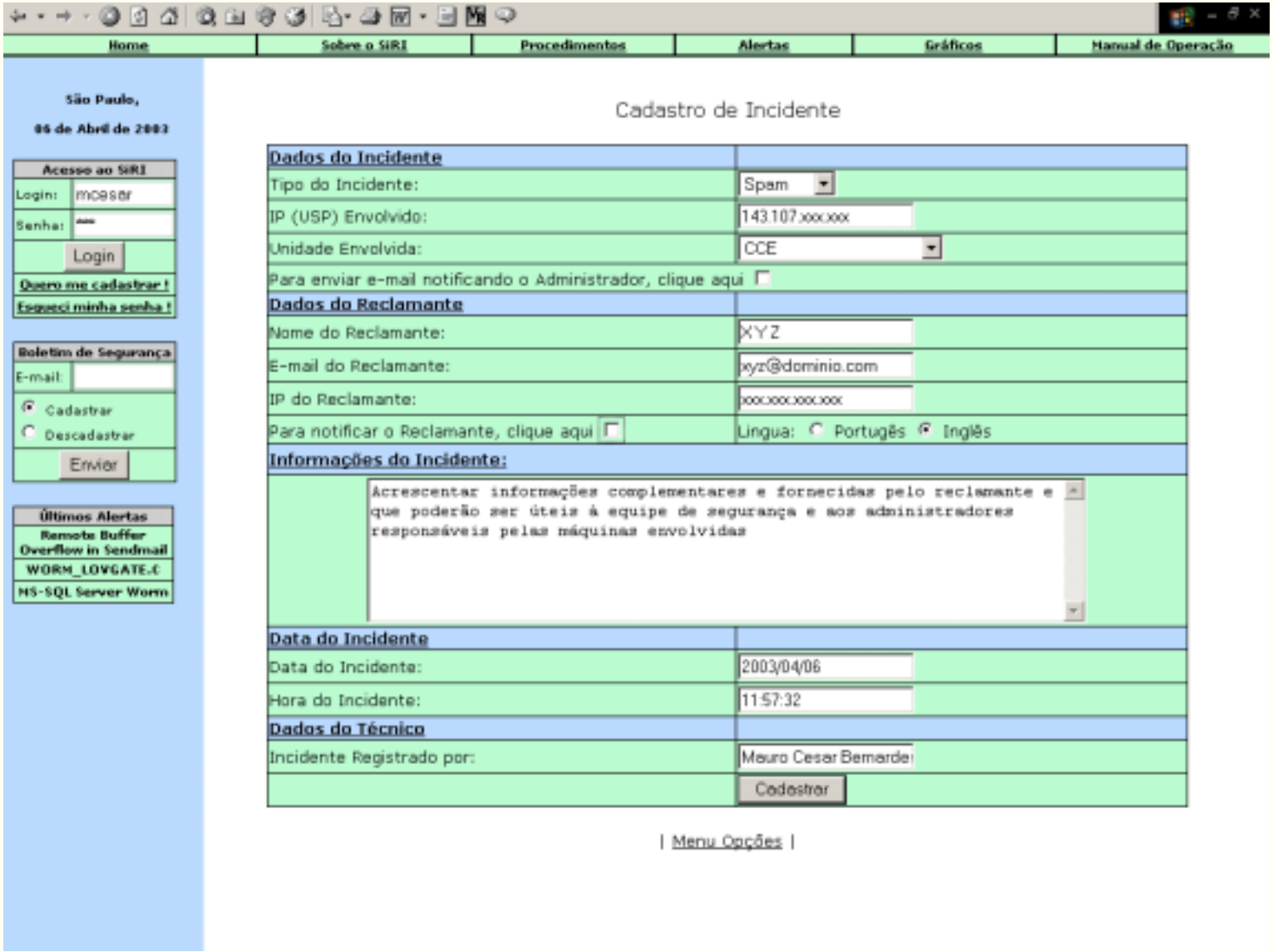
A Ferramenta SiRI



Minimização do Tempo de RI



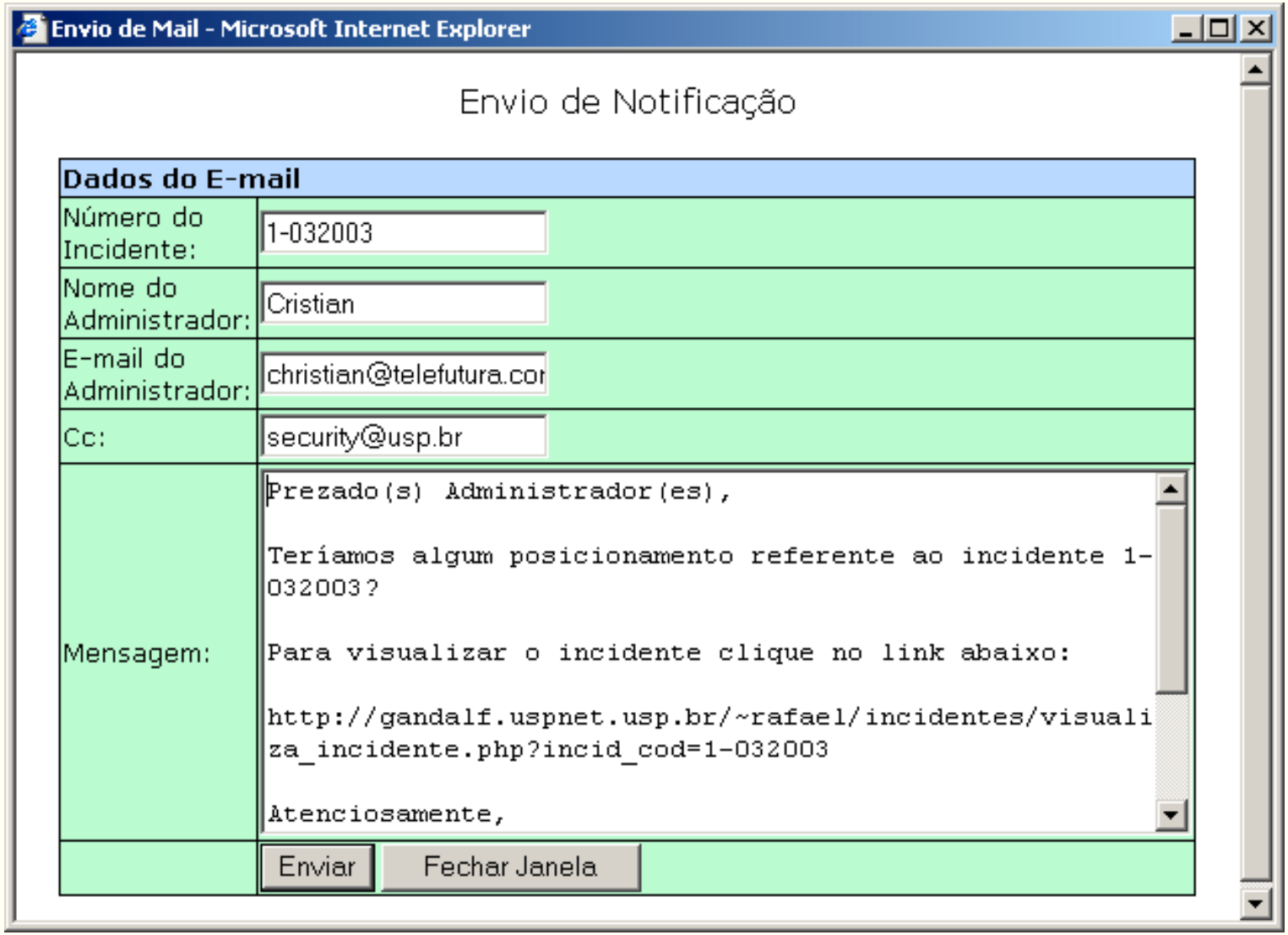
Triagem de um Incidente



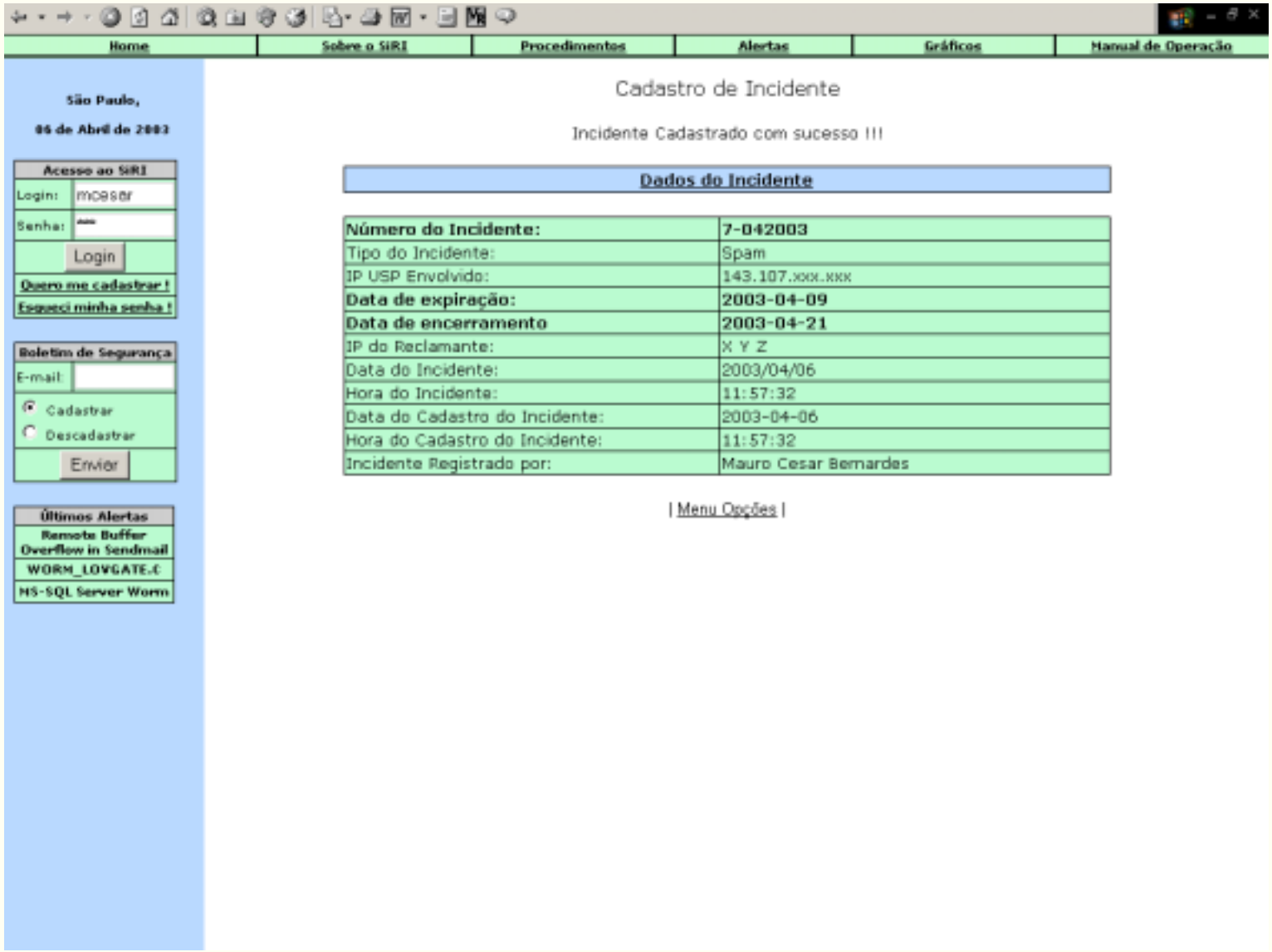
Ações Emergenciais

- **A partir da triagem do Incidente, pode-se adotar ações emergenciais.**

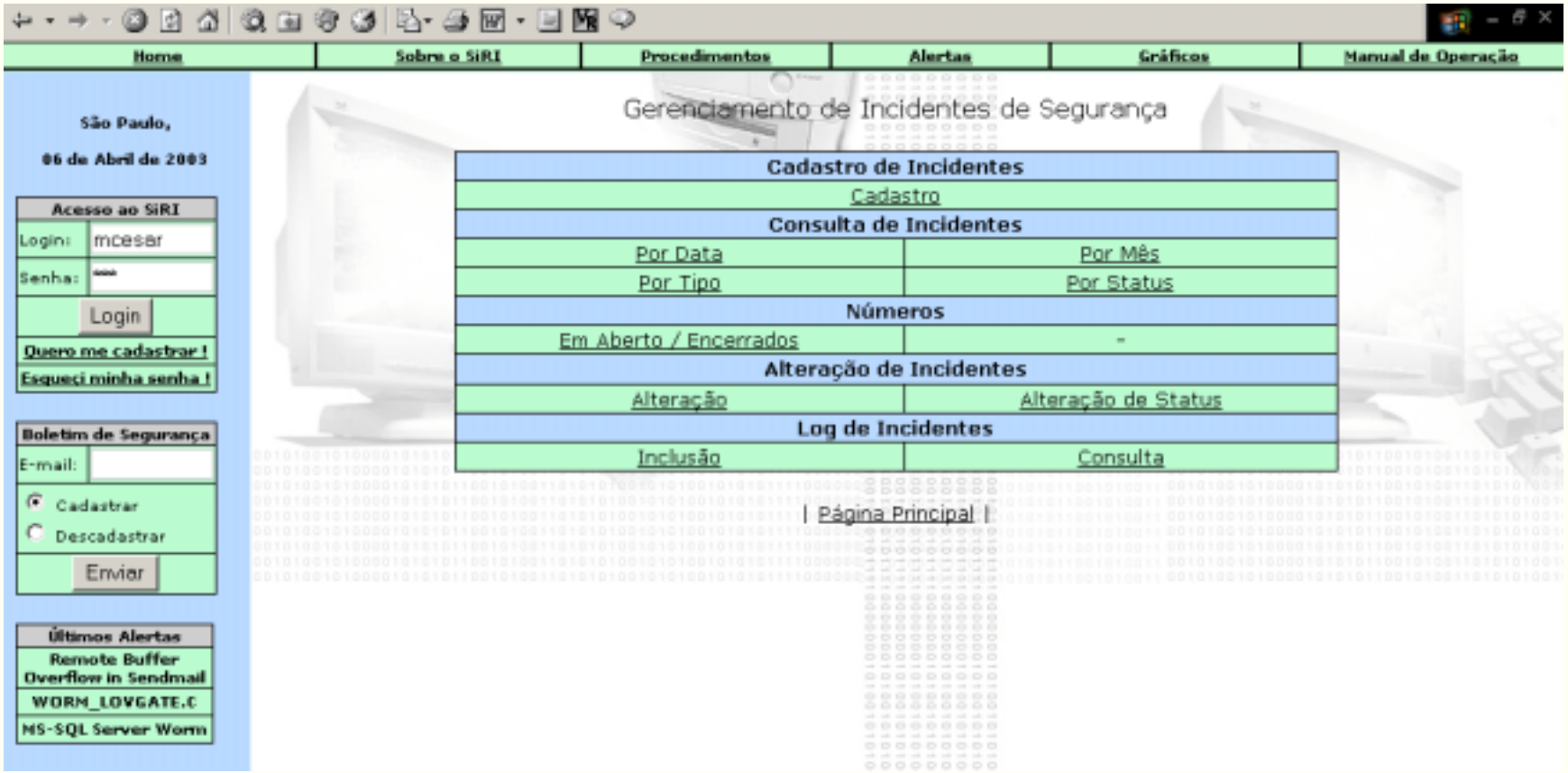
Notificações Personalizadas



Identificação única para cada Incidente



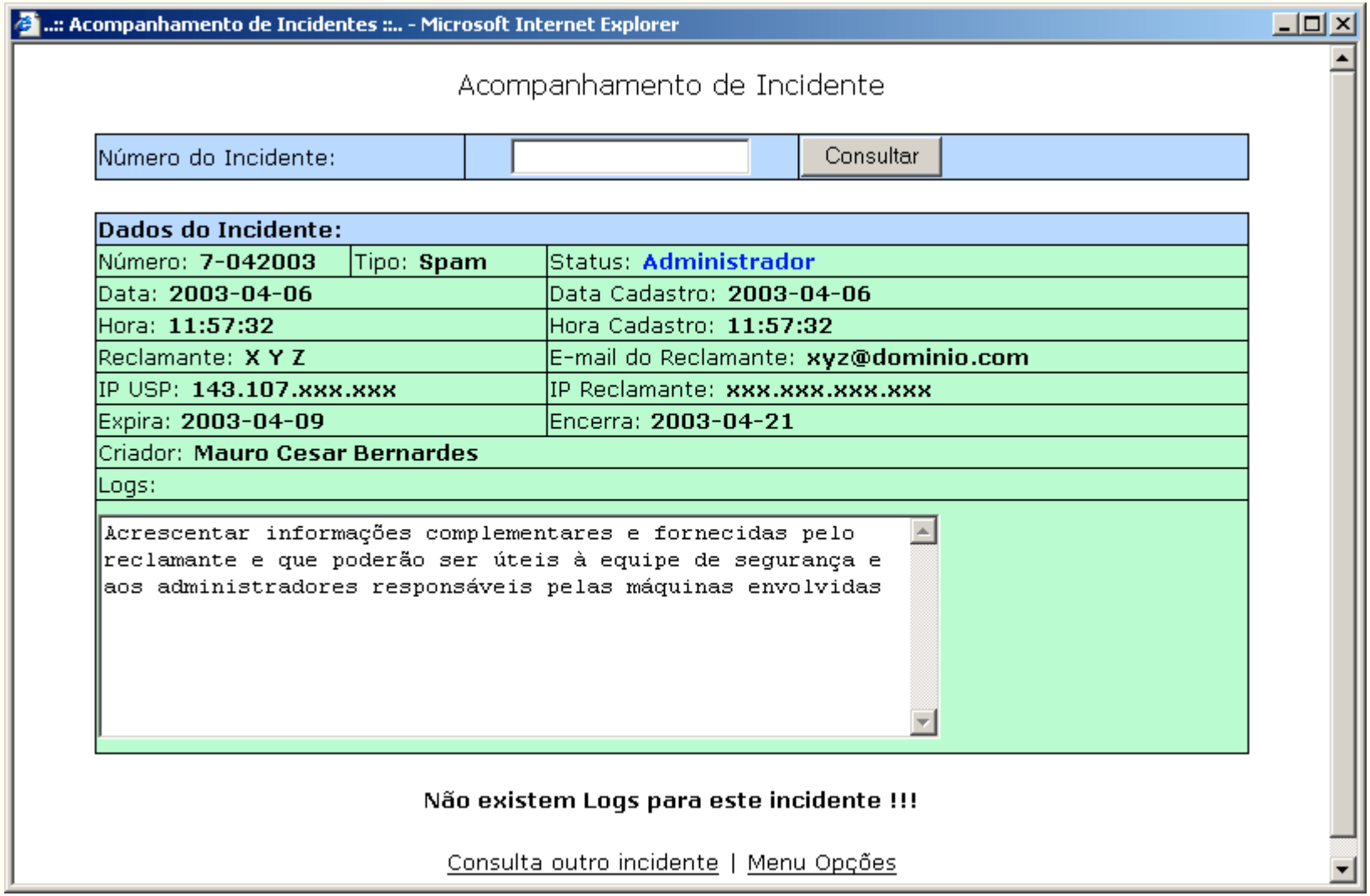
Visão Geral das Opções para Incidentes



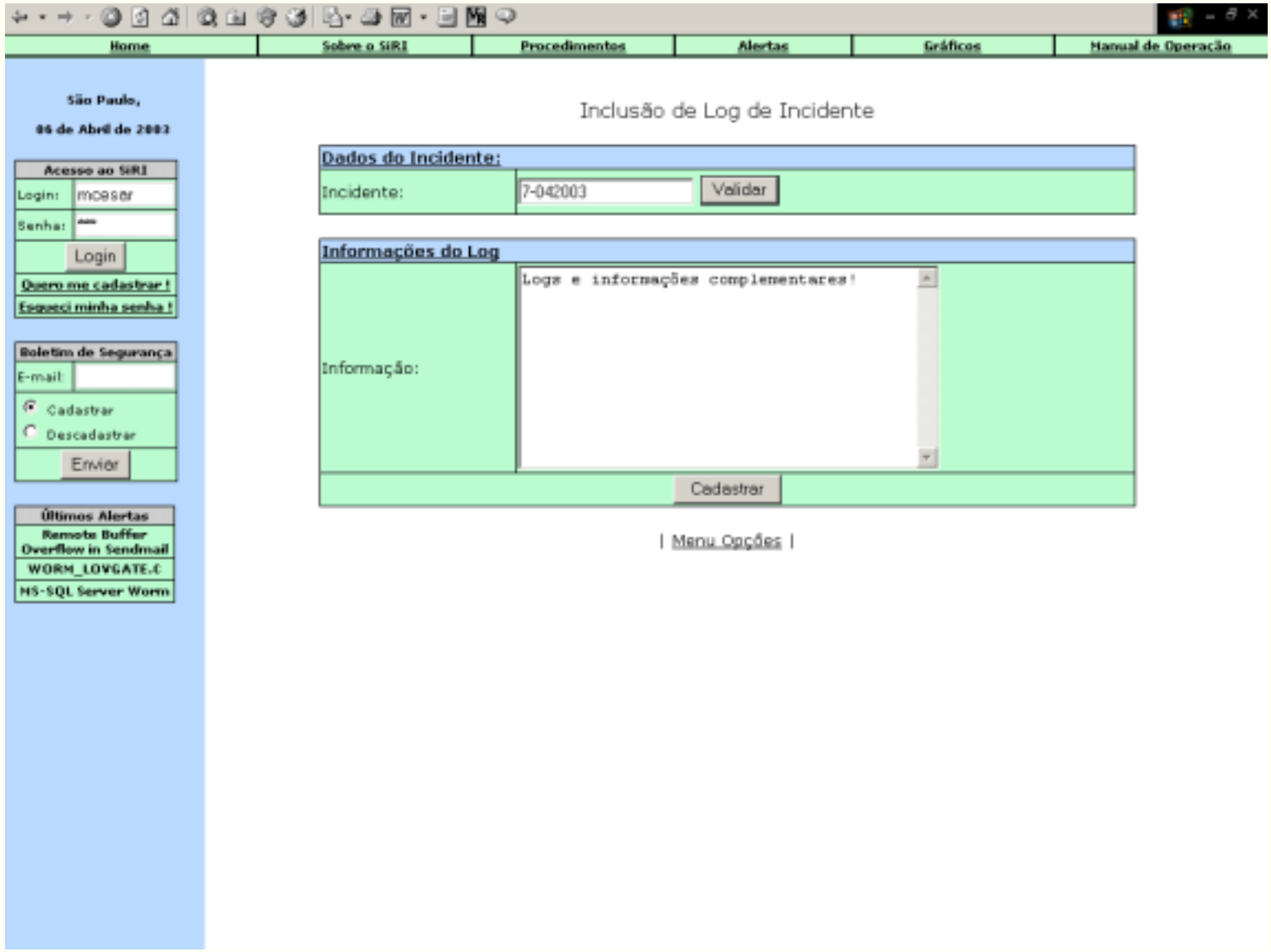
Acompanhamento do Incidente

Acesso Mediante Certificação

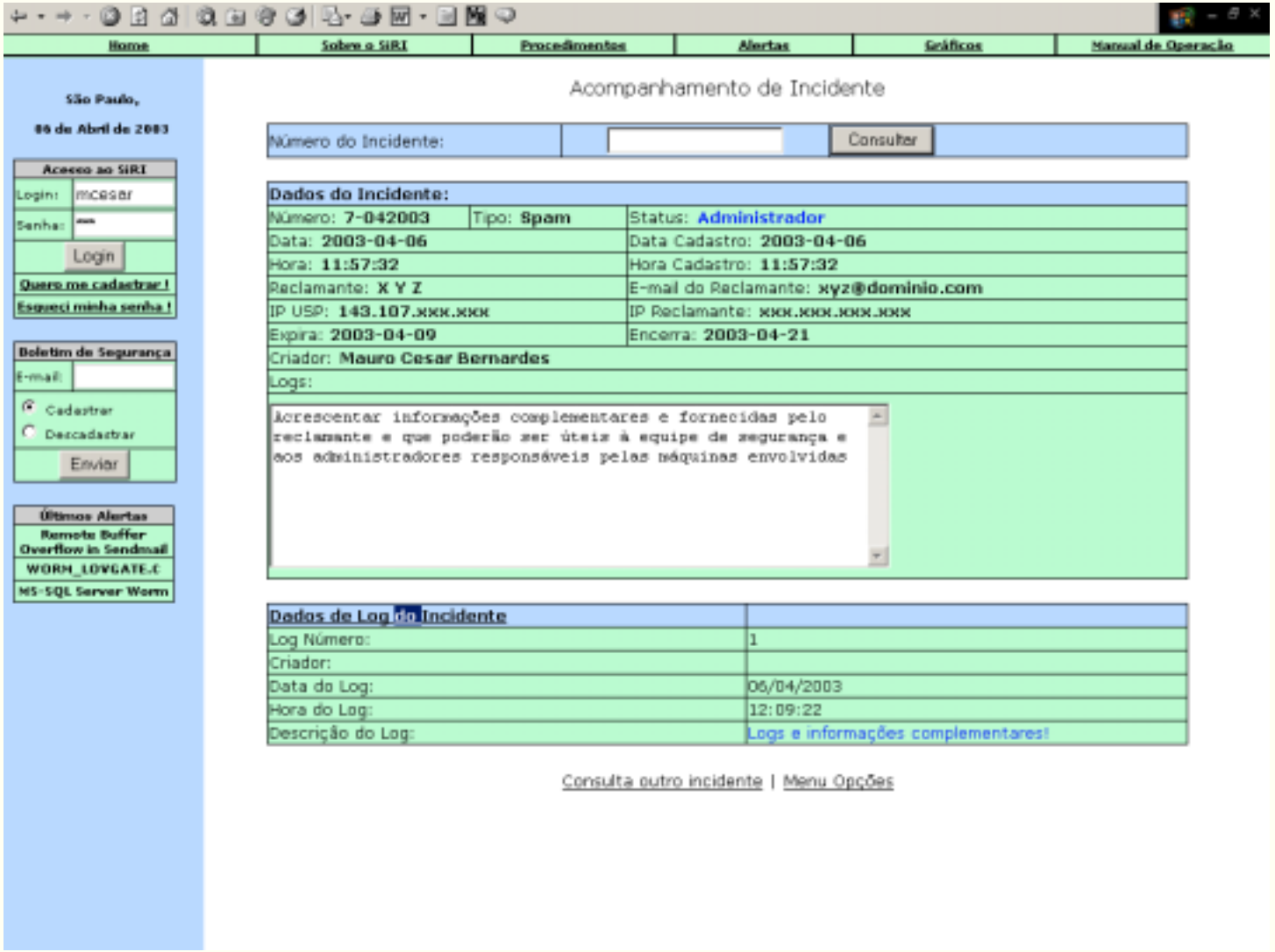
Acompanhamento do Incidente



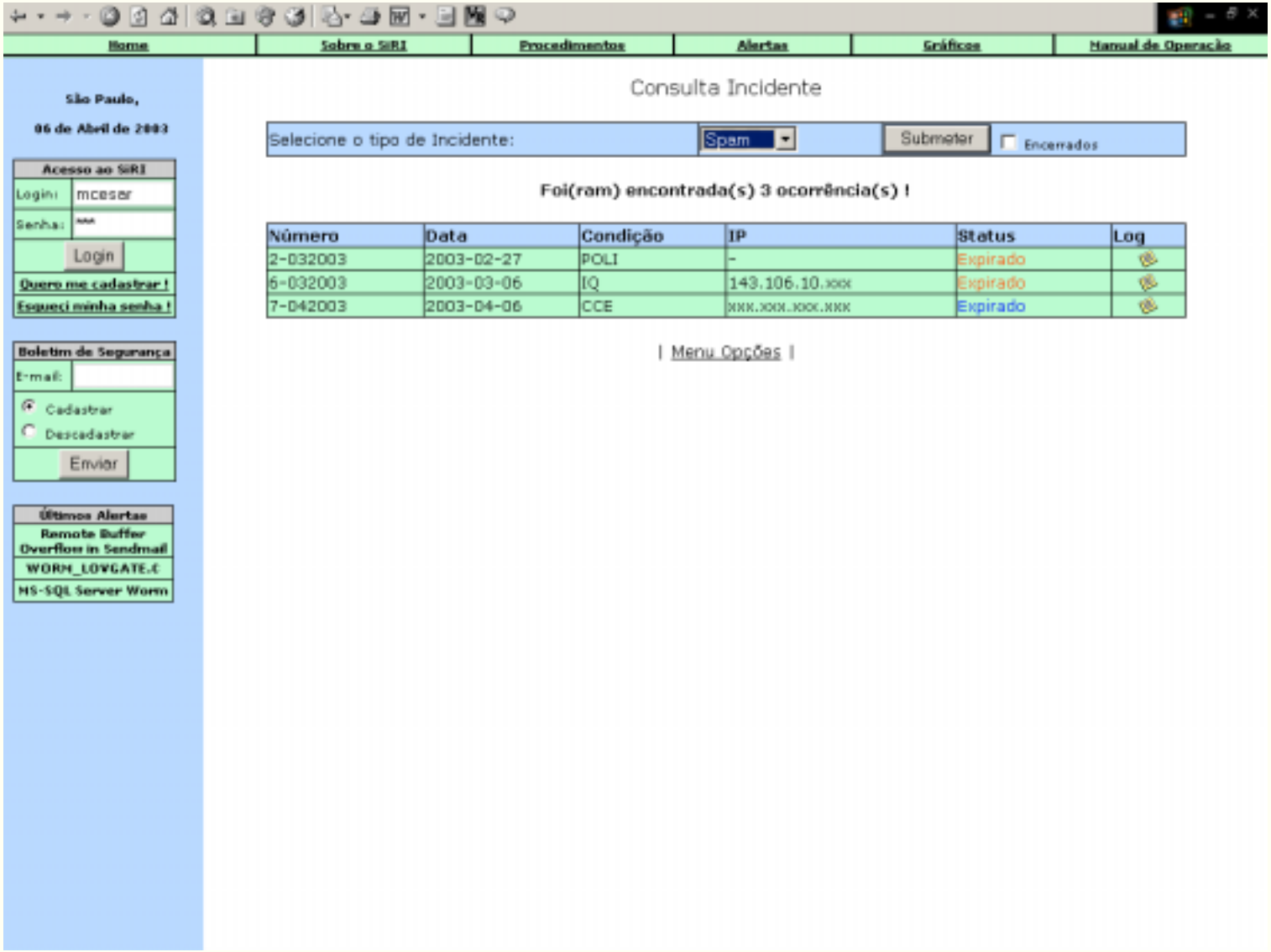
Informações de Acompanhamento



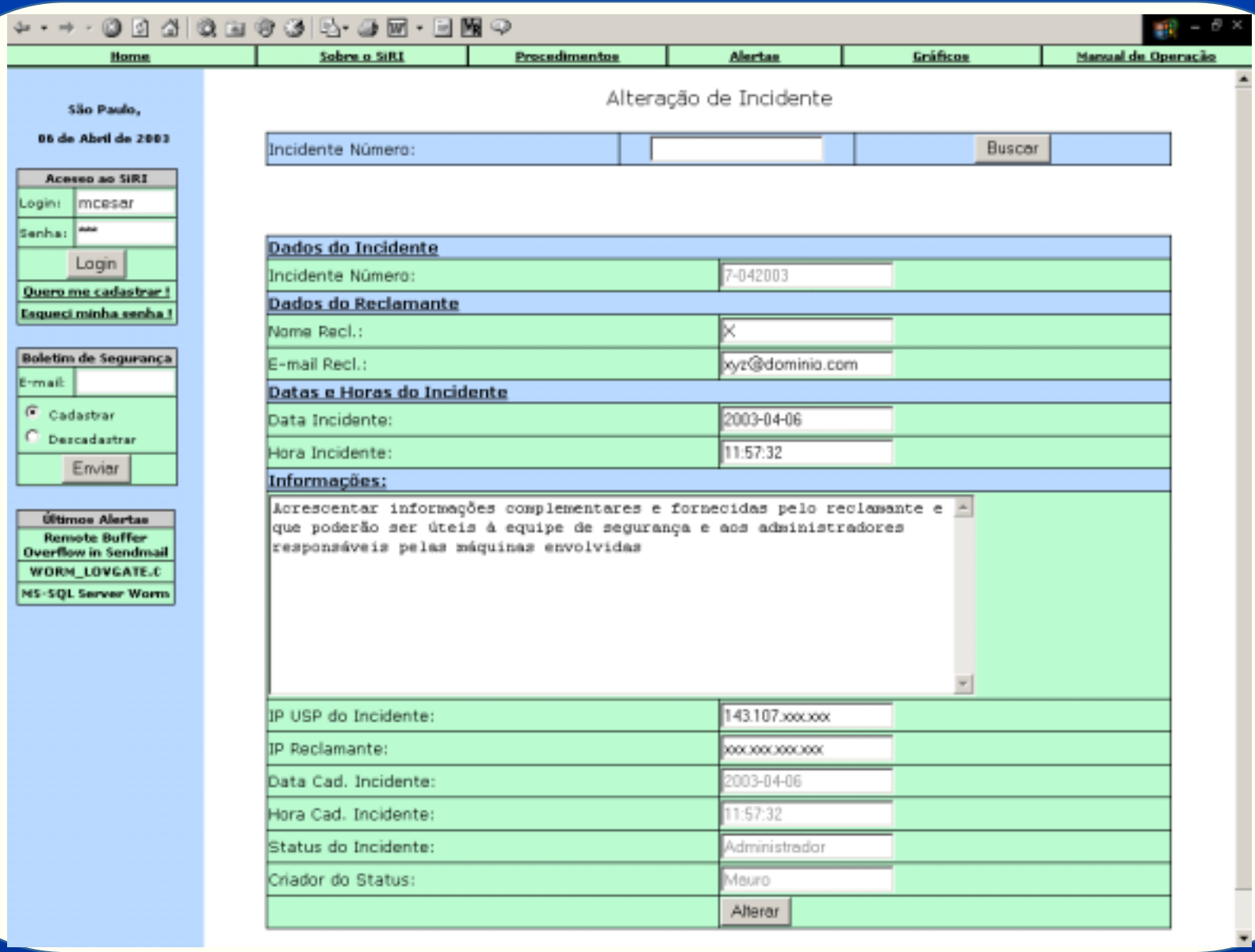
Informações de Acompanhamento



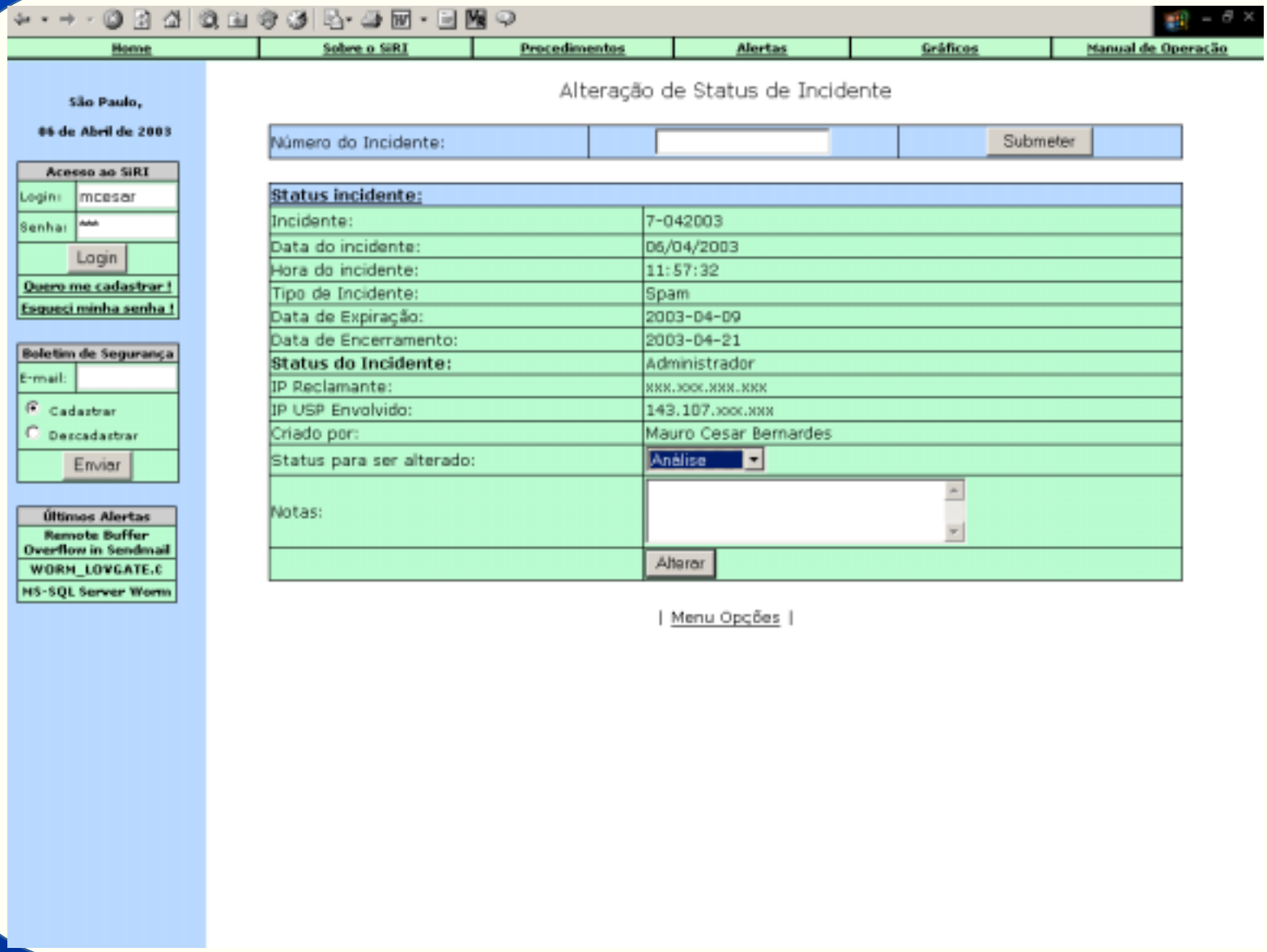
Consultas personalizadas para a Equipe



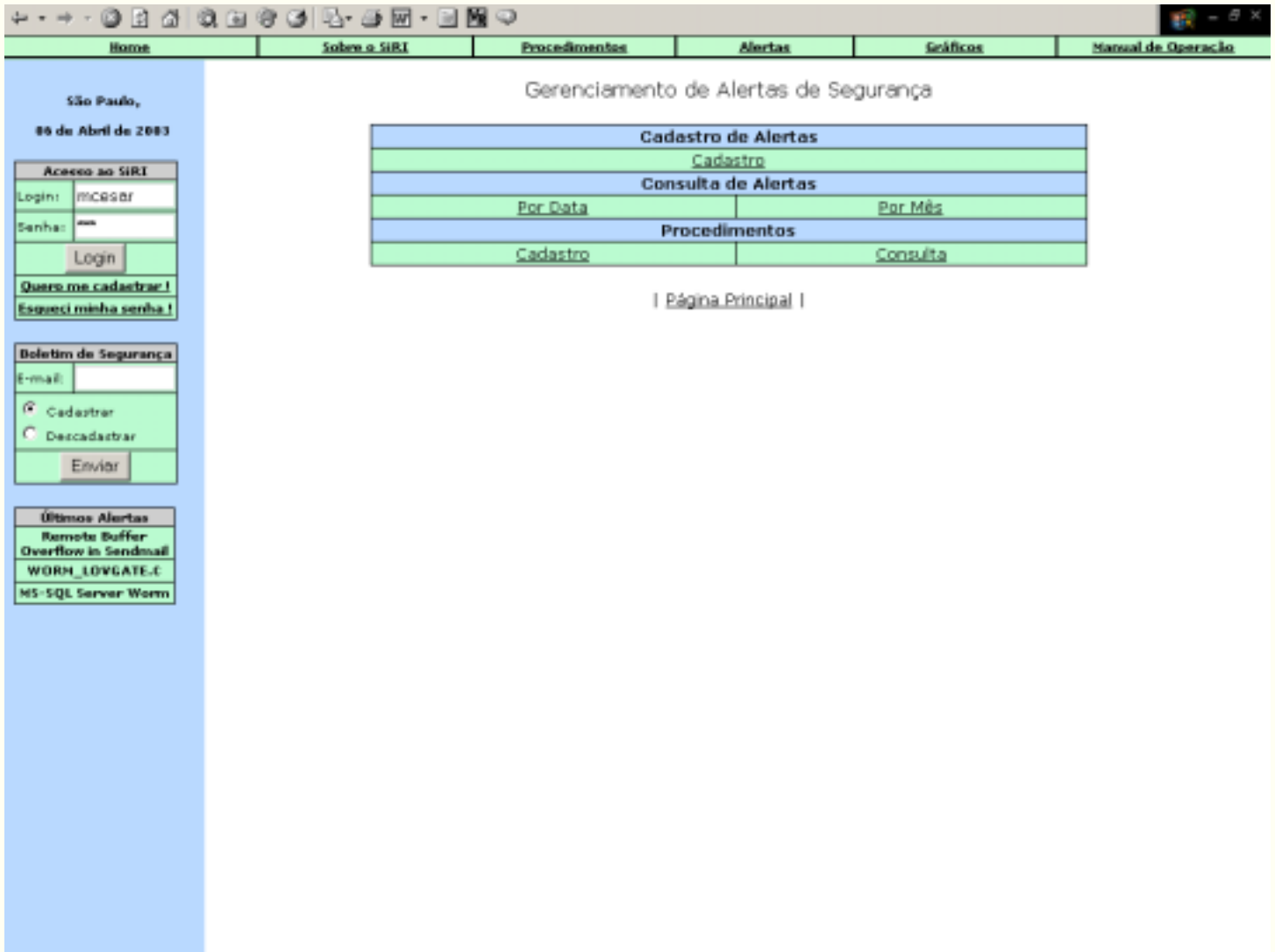
Refinamento das informações do Incidente



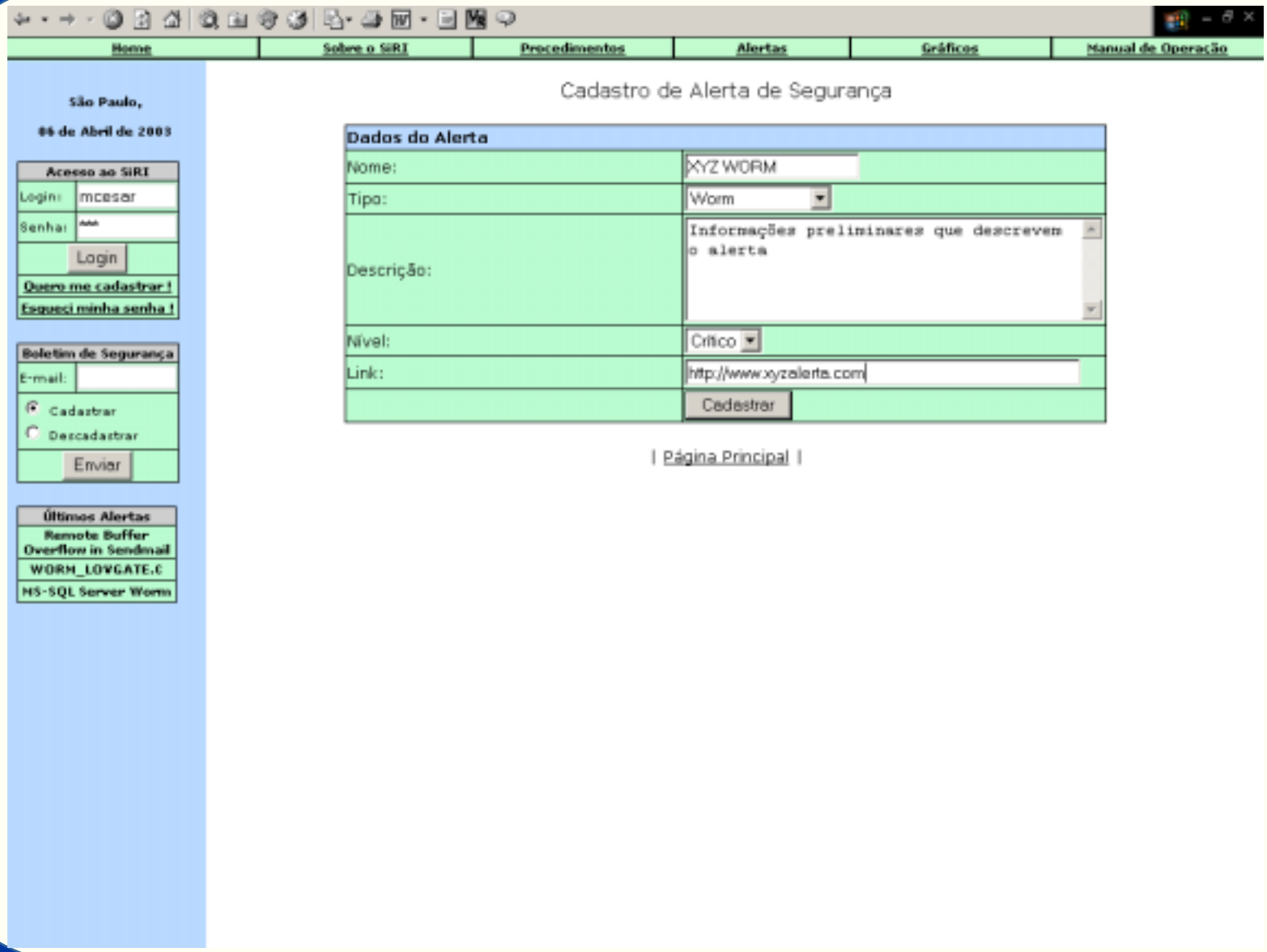
Alteração de Status



Gerenciamento de Alertas



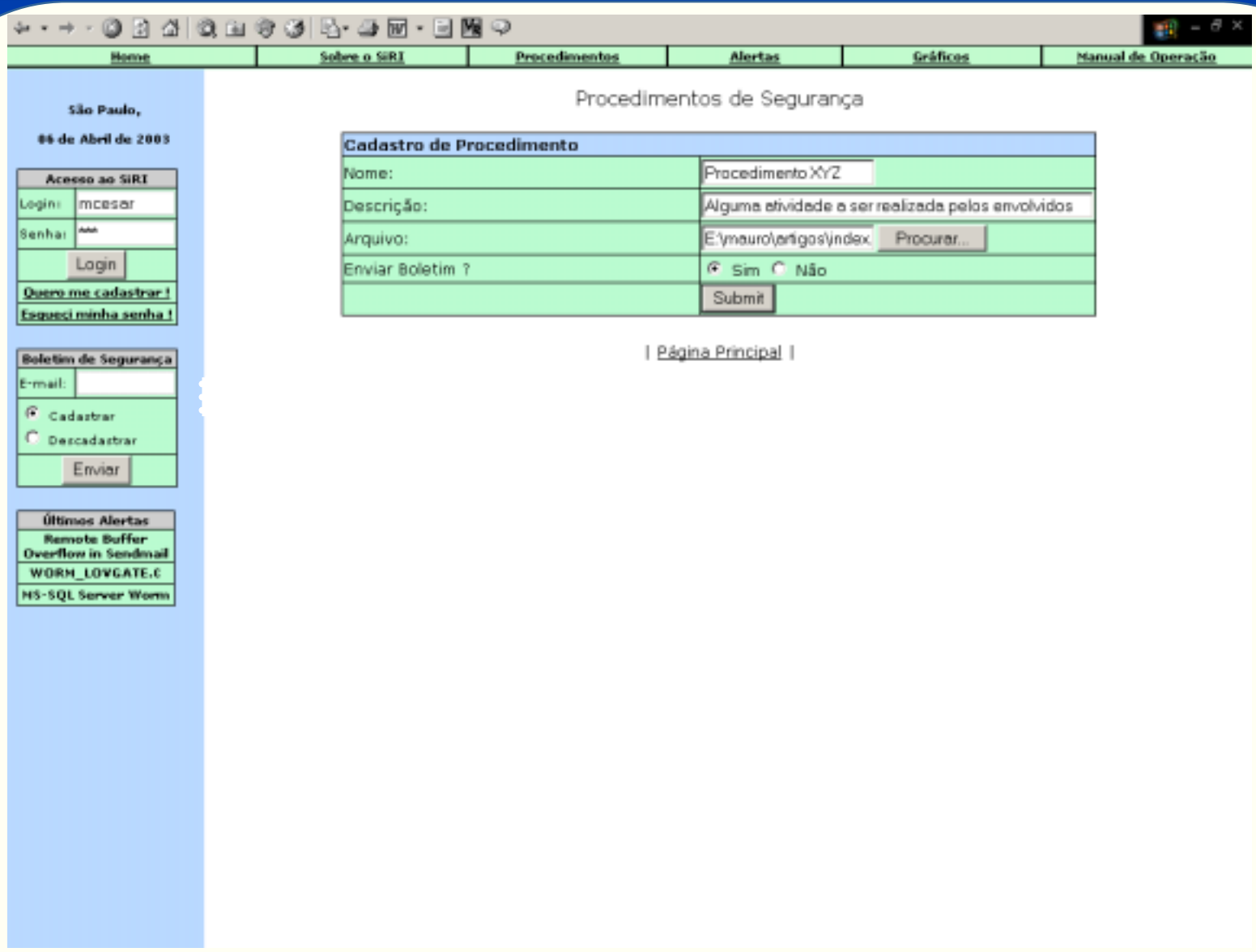
Cadastro de Alertas



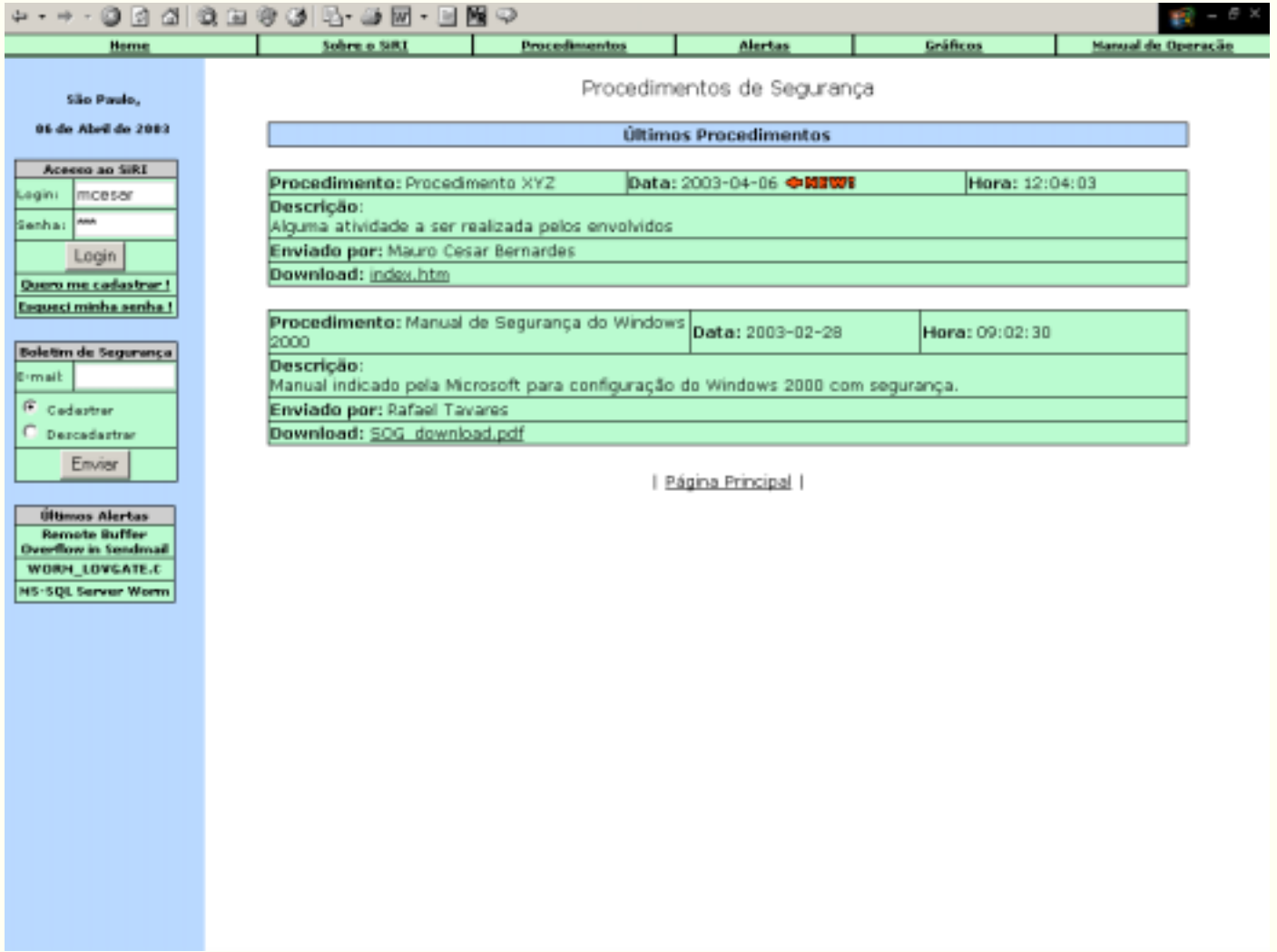
Encaminhamento de Alertas

- **Alertas Classificados;**
  - ⇨**Uso de Ontologias**
- **Alertas priorizados conforme necessidade dos usuários;**
  - ⇨**Listas de Discussão X SiRI: O diferencial;**
  - ⇨**Correlacionar alertas às necessidades;**
  - ⇨**Meta: Trabalhar informações prévias, Histórico e Extração de conhecimento;**

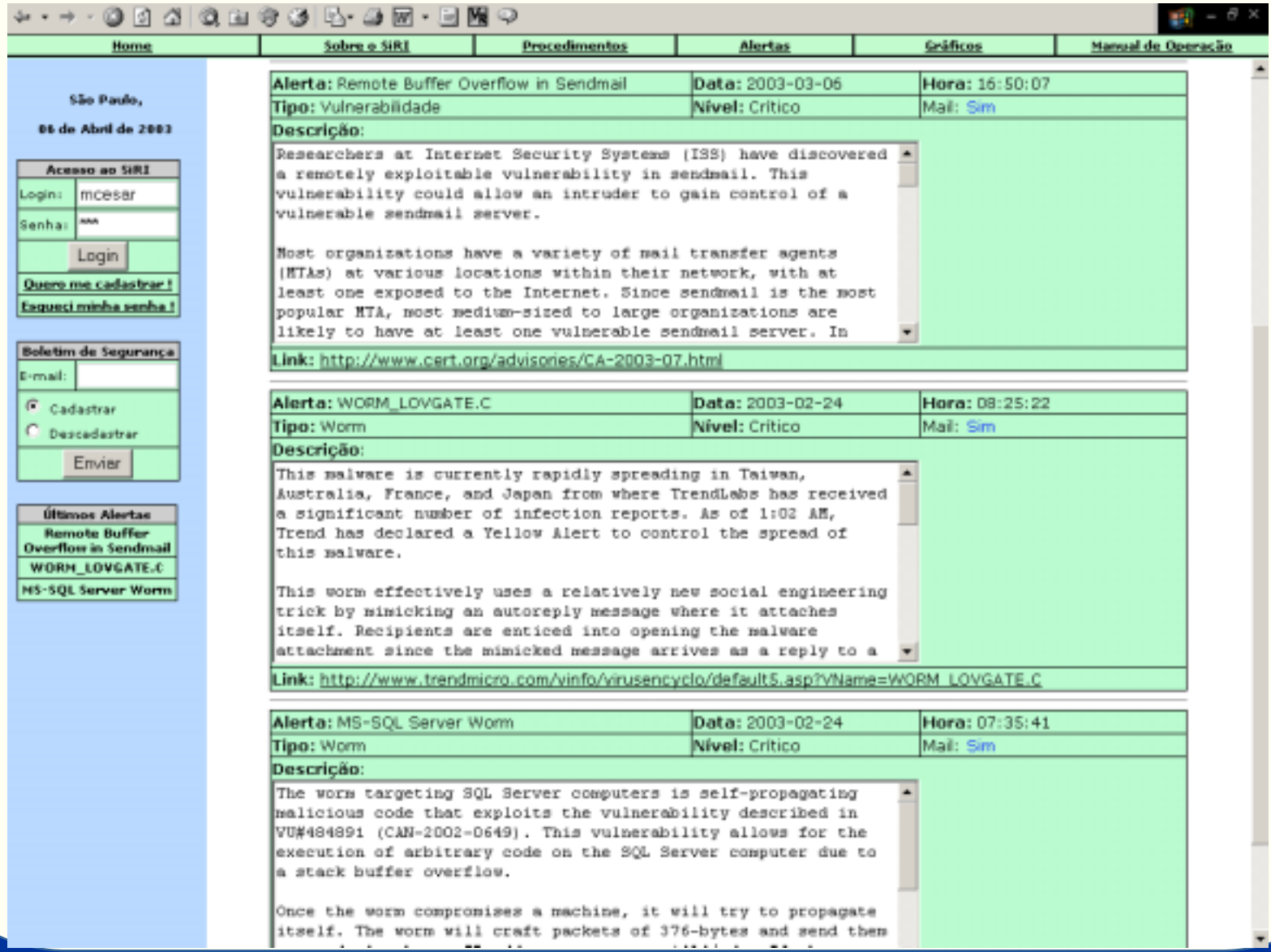
Cadastro de Procedimentos



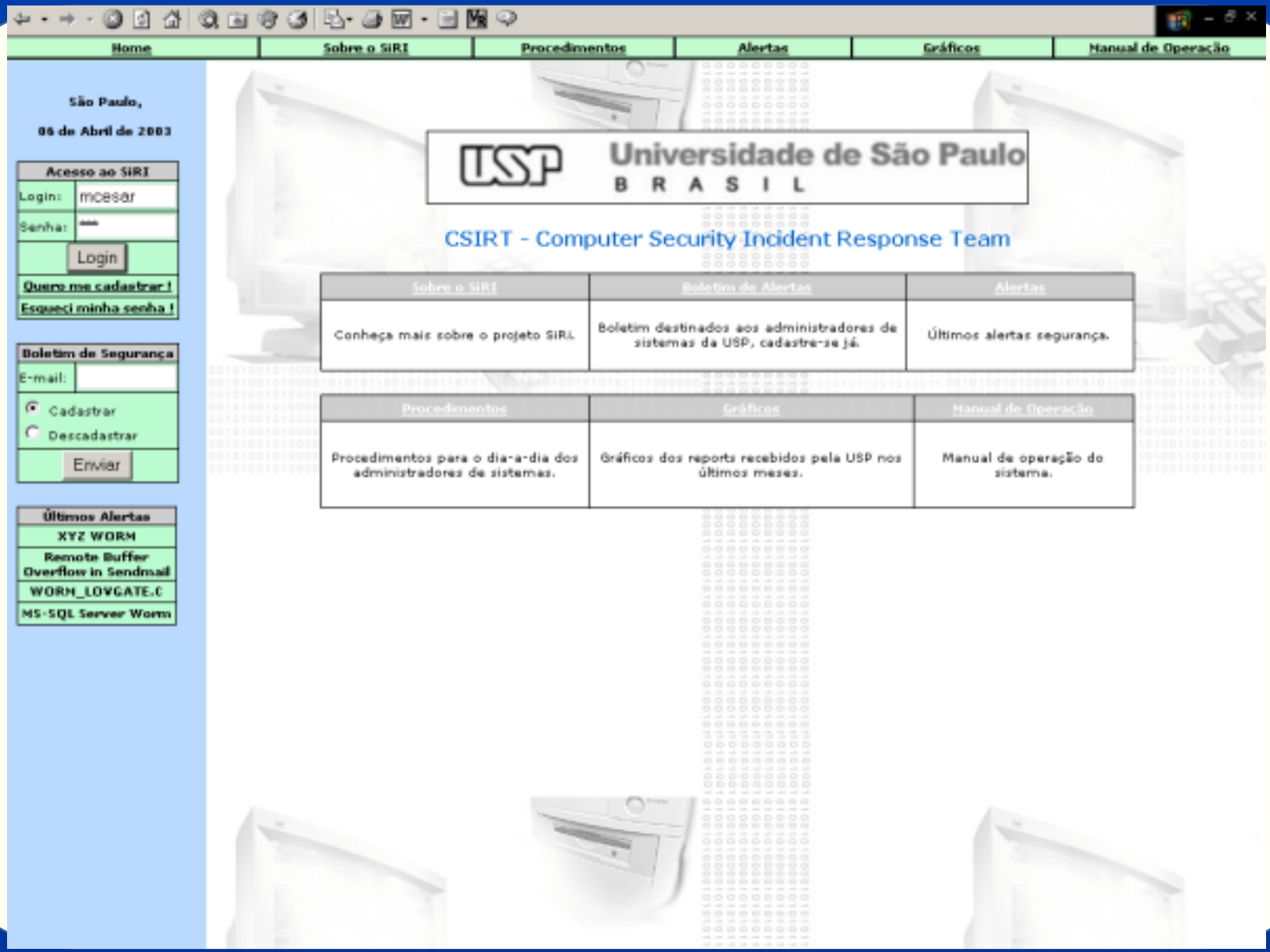
Correlação Alertas X Procedimentos



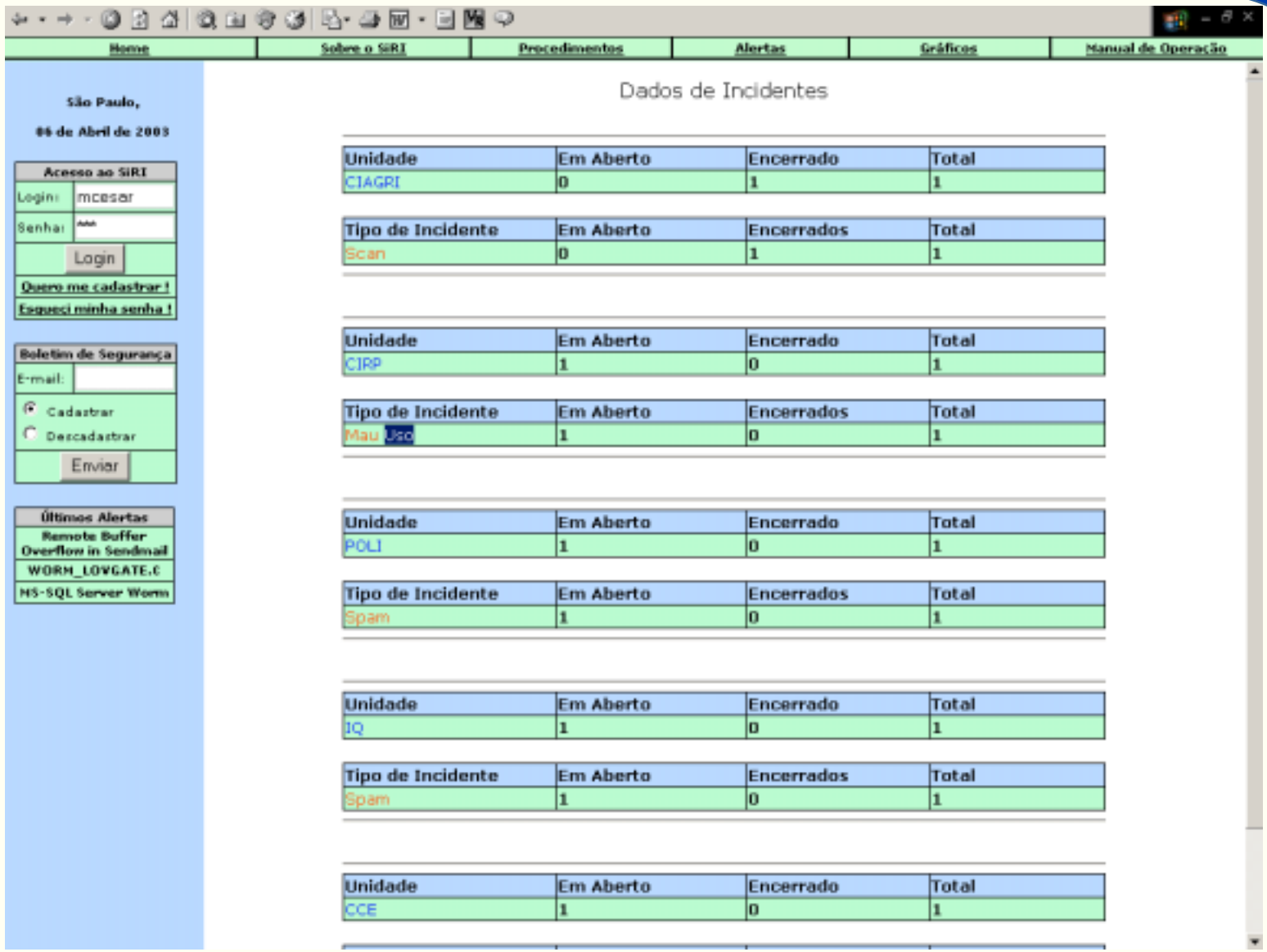
Correlação Alertas X Procedimentos



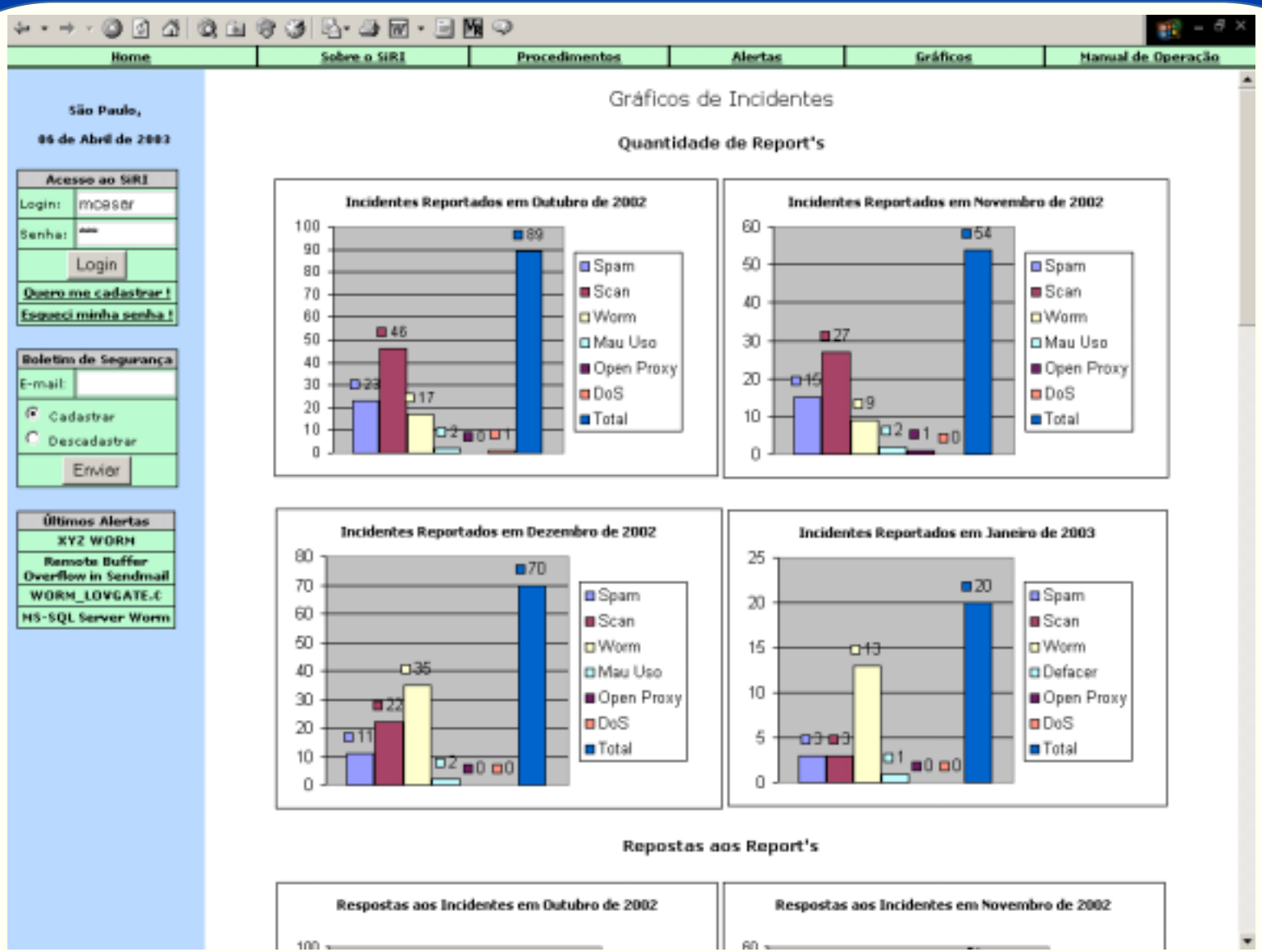
Estatísticas



Estatísticas Personalizadas



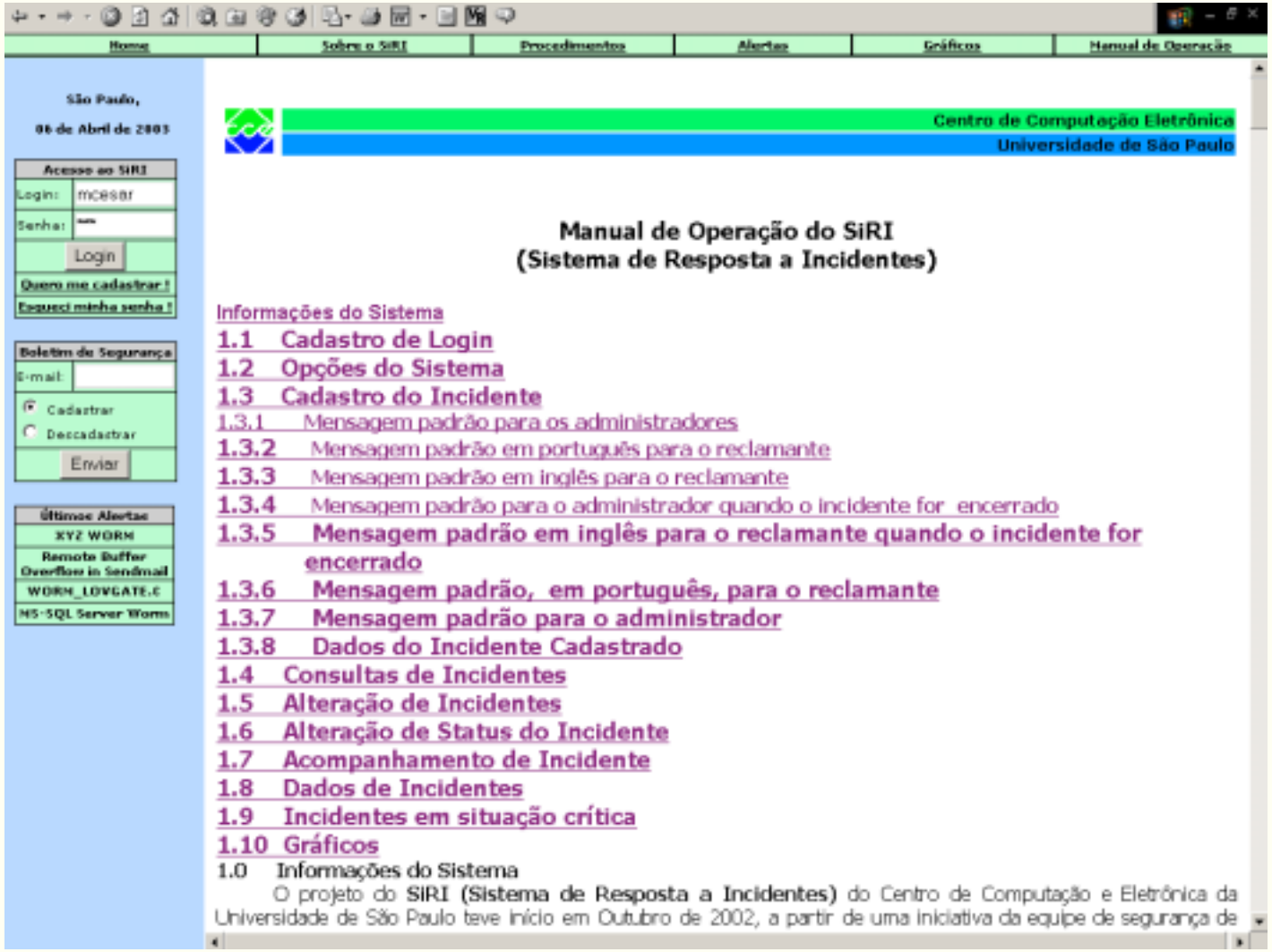
Gráficos Personalizados



Estatísticas

- O fator Psicológico;
- Repositório de Informações;
- Ajuda a redefinir requisitos de controle para a Política de Segurança.

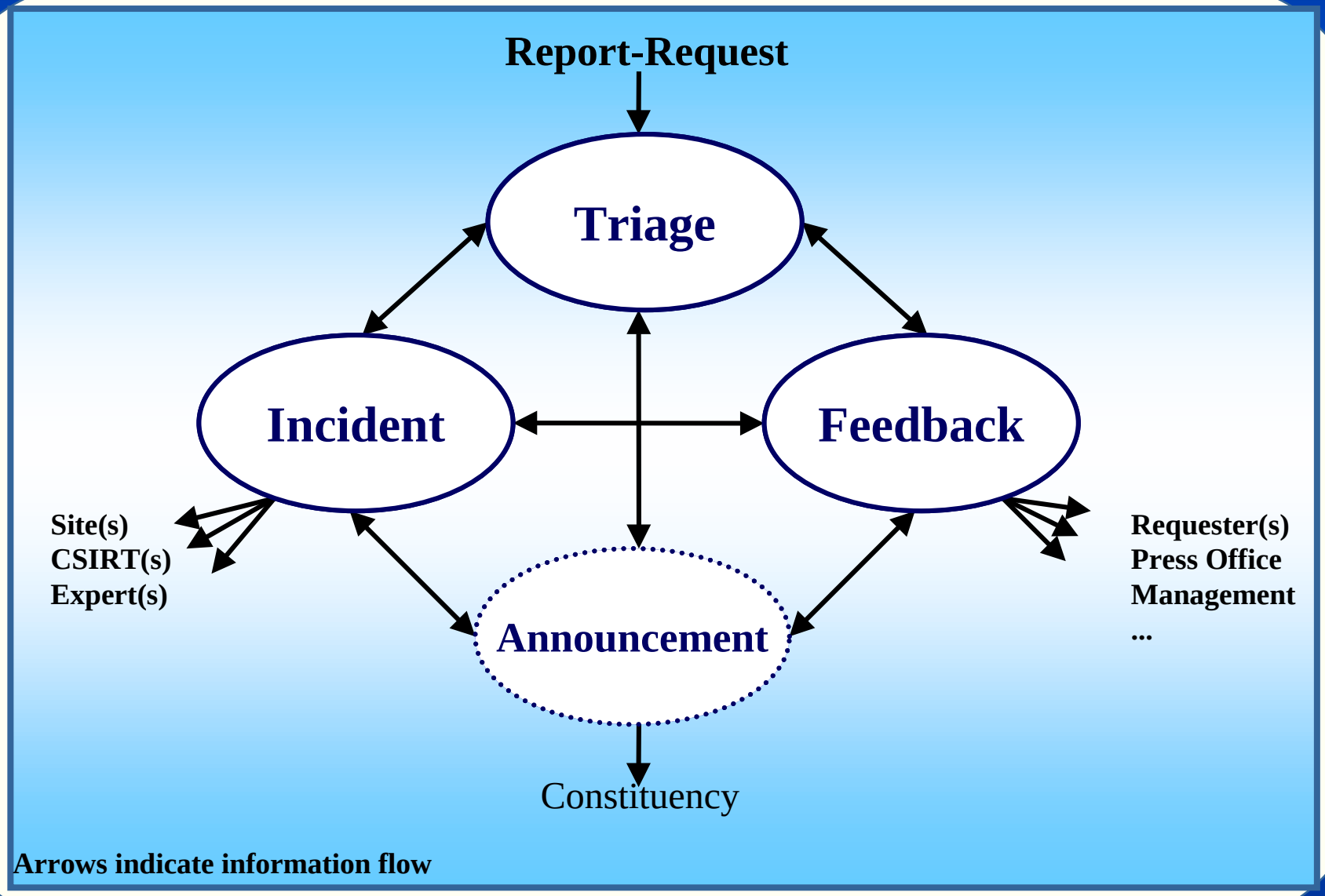
Manual de Documentação



O Cenário Atual

- Redução de 60% do tempo despendido no ciclo de vida de uma Resposta a Incidentes;
- Acompanhamento personalizado de cada incidente;
- Maior interação entre o reclamante, a equipe de segurança e os administradores responsáveis;
- Constituição de um Repositório de Informações.
- Ferramenta auxiliar para as etapas previstas para a atividade de Resposta a Incidentes;

IR Service Functions Overview



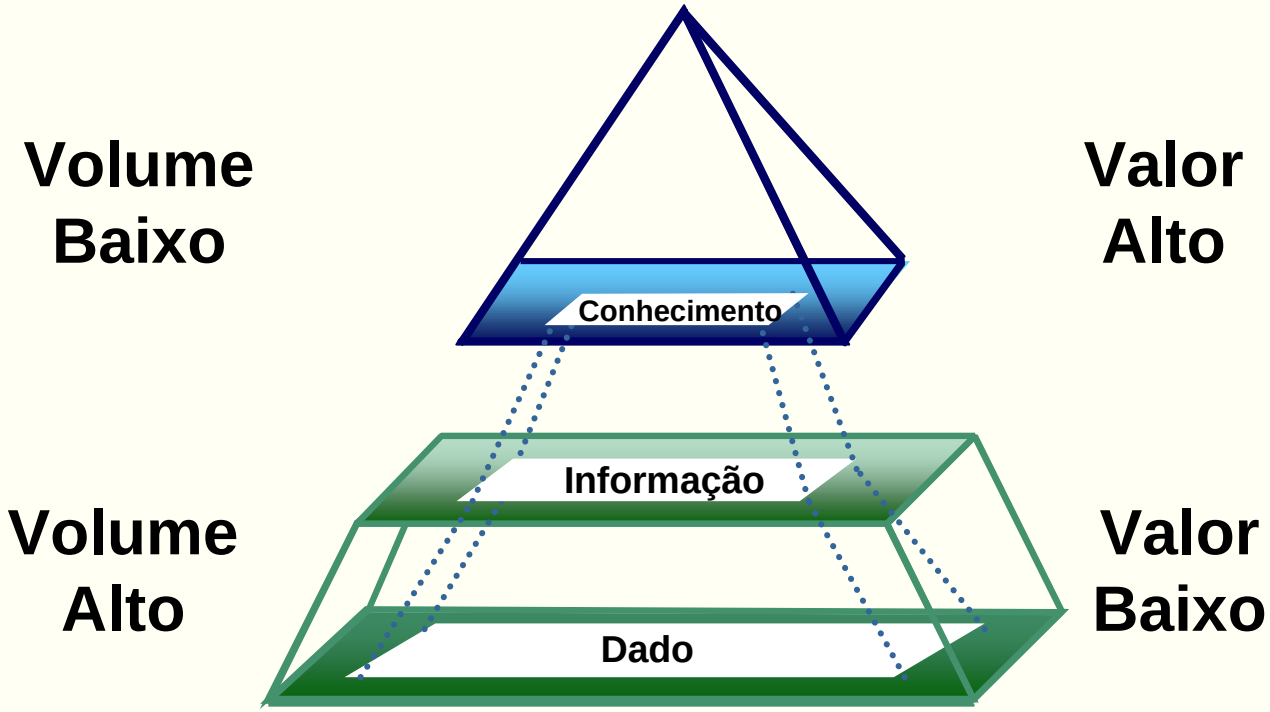
Fonte: http://www.sei.cmu.edu/publications/documents/98.reports/98hb001/98hb001abstract.html

Trabalhos Futuros

Constituição de um Sistema de Informações

- Trabalhar dados para produzir informação e conhecimento;
- Fornecer suporte à tomada de decisão;
- **Expectativa:** Um sistema integrado homem-máquina que provê informações para dar suporte às funções de operação, administração e tomada de decisão em relação à segurança computacional;
- Código aberto a contribuições.

Metodologia: Dados, Informação e Conhecimento



Aquisição de conhecimento (AC):
Extração, interpretação e representação do conhecimento de um dado domínio.
Tarefa difícil!

Sistemas de Informação e Estrutura de Decisão

Classificação dos Sistemas de Informação

Extração de conhecimento de Base de Dados

Objetivos:

Apoiar os especialistas do domínio na obtenção de conhecimento de base de dados;

KDD (Knowledge Discovery in Databases)

Elementos de Apoio ao Processo KDD

- *Data Warehouse*;
- Técnicas Estatísticas;
- Visualização de Dados

Expectativa

Utilização dos conceitos de sistemas de informação para modelar um ambiente que permita ao administrador de segurança computacional, metodicamente, gerar conhecimento para planejar e programar a tomada de decisão com a eficiência e a eficácia exigidas pelos sistemas/redes atuais.

Conclusões

- A ferramenta apresentada apresentou contribuições significativas no processo de RI;
- Entretanto, a ferramenta SiRI é apenas o início de um projeto para a constituição de um sistema de informação;
- Trabalho colaborativo é essencial!