Serviço de Respostas a Incidentes de Segurança da RedeRio

Marita Maestrelli
mm@rederio.br

I Encontro de CSIRTs Acadêmicos
Rio de Janeiro/RJ – 25 e 26 maio de 2006

Roteiro

- Apresentação da RedeRio
- Serviço de Respostas a Incidentes de Segurança
- Projetos
- Contato

Coordenação de Engenharia Operacional da Rede Rio

Backbone Acadêmico

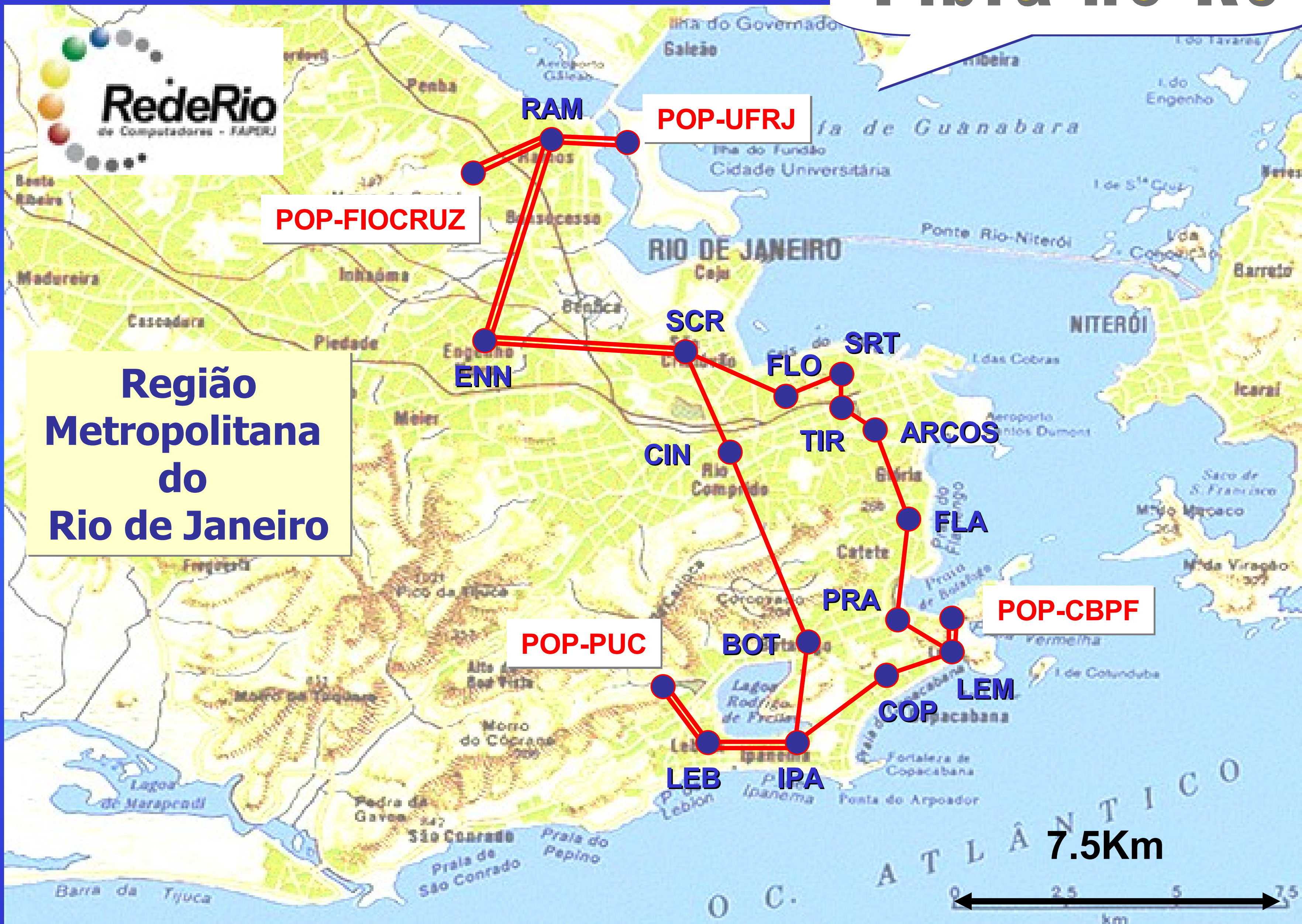
Apresentação RedeRio

A Rede Rio é uma rede de computadores, integrada por universidades, centros de pesquisa e entidades governamentais (municipais, estaduais e federais) localizados no Estado do Rio de Janeiro.

É um dos principais instrumentos de desenvolvimento científico e tecnológico, alem de oferecer serviços do governo ao cidadão do Estado do Rio de Janeiro.

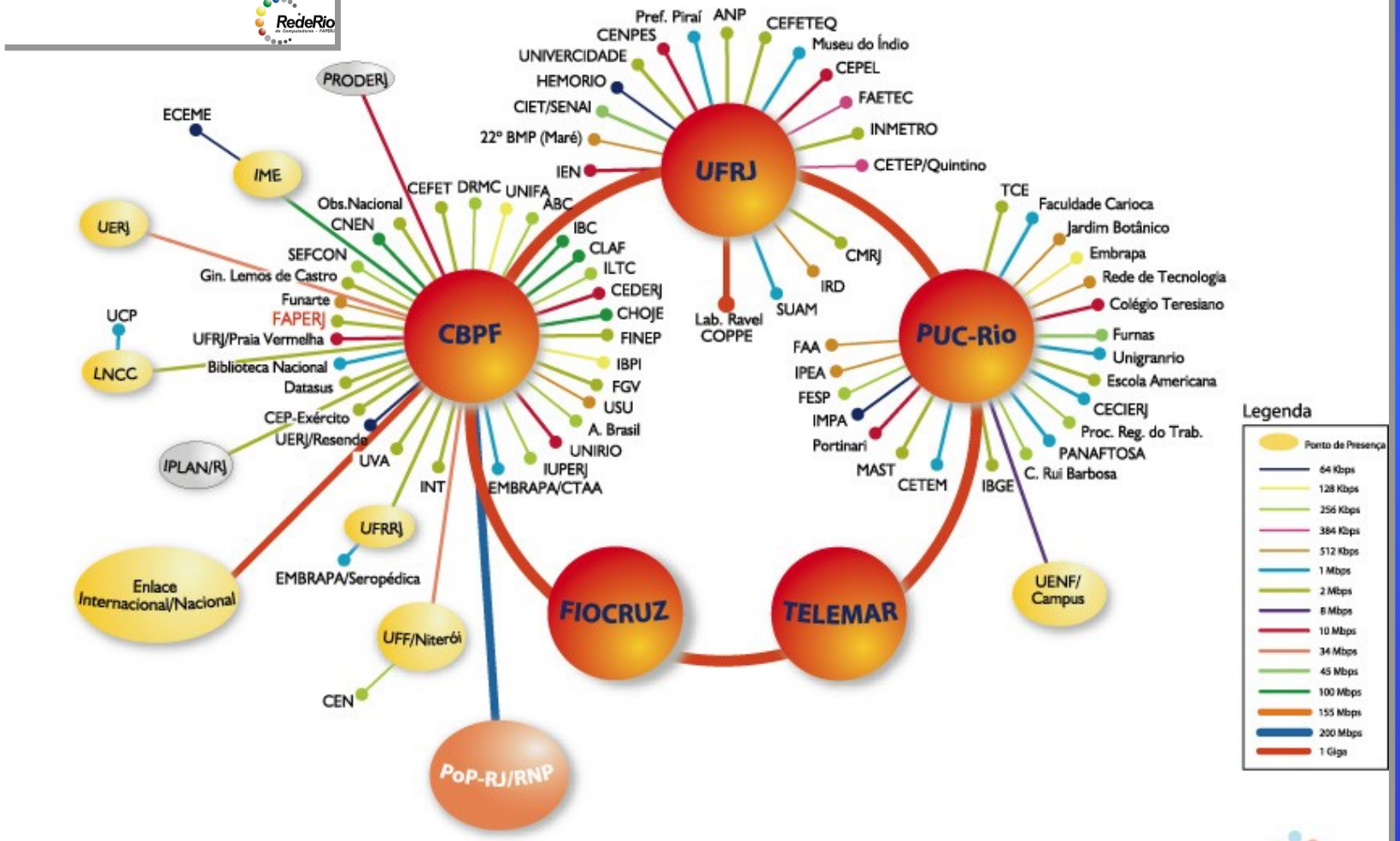
A FAPERJ é o órgão responsável pela sua coordenação e pelo seu financiamento.

Fibra no RJ


RedeRio de Computadores - FAPERJ
Região Metropolitana do Rio de Janeiro
RAM
POP-UFRJ
POP-FIOCRUZ
ENN
SCR
SRT
FLO
TIR
ARCOS
CIN
FLA
PRA
POP-CBPF
POP-PUC
BOT
LEM
COP
LEB
IPA
7.5Km
0
2.5
5
7.5
km

Mapa Topológico

RedeRio de Computadores - FAPERJ



CEO/RedeRio

Serviço de Respostas à Incidentes de Segurança
CEO – Coordenação de Engenharia Operacional

Início: Dezembro de 1999

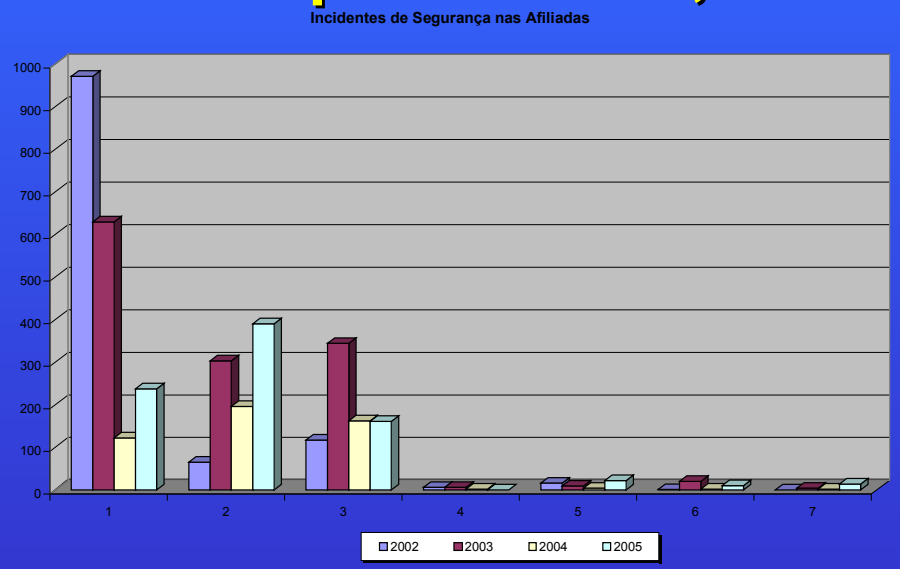
Constituency:
- Universidades, Institutos de Pesquisa e Órgãos do Governo no Estado do Rio de Janeiro conectados ao AS2715, alem dos AS21612 e AS14553;

Equipe:
- Um responsável e uma bolsista;
- Toda a equipe CEO;

Atuação

Serviço de Respostas à Incidentes de Segurança CEO/RedeRio:

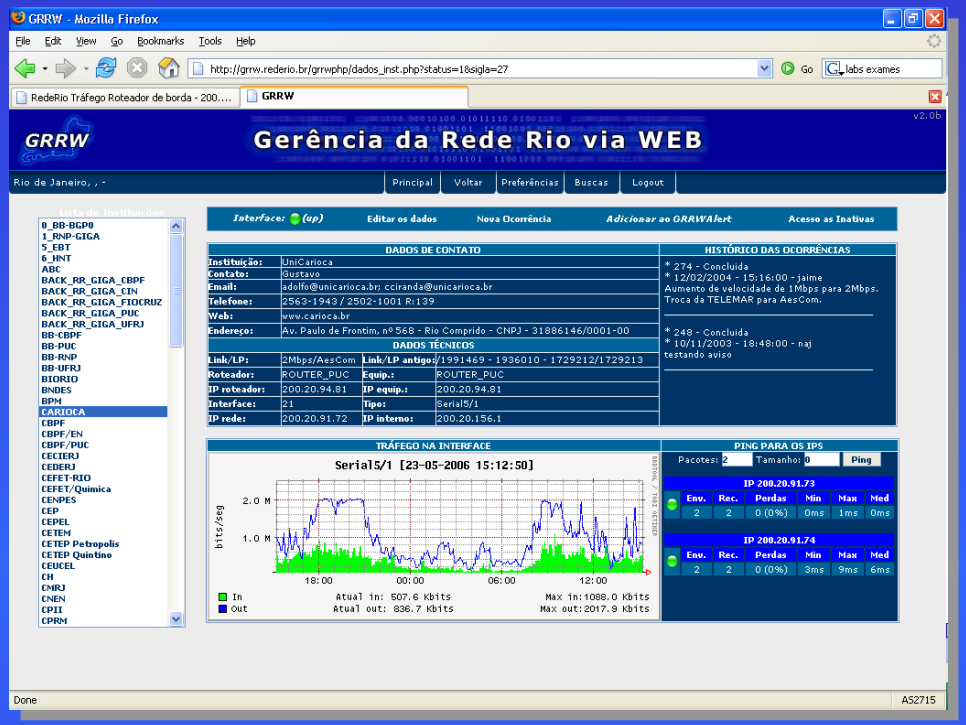
- Monitoramento e Alertas;
- Repasse para responsáveis e acompanhamento;
- Ajuda, se for necessário;
- Estatísticas;



Projetos

- GRRW – cadastramento das afiliadas
- GRRW2 – Alertas de falhas
- Fluxo do Tráfego – Monitoramento visual
- Consórcio Brasileiro de Honeypots

GRRW



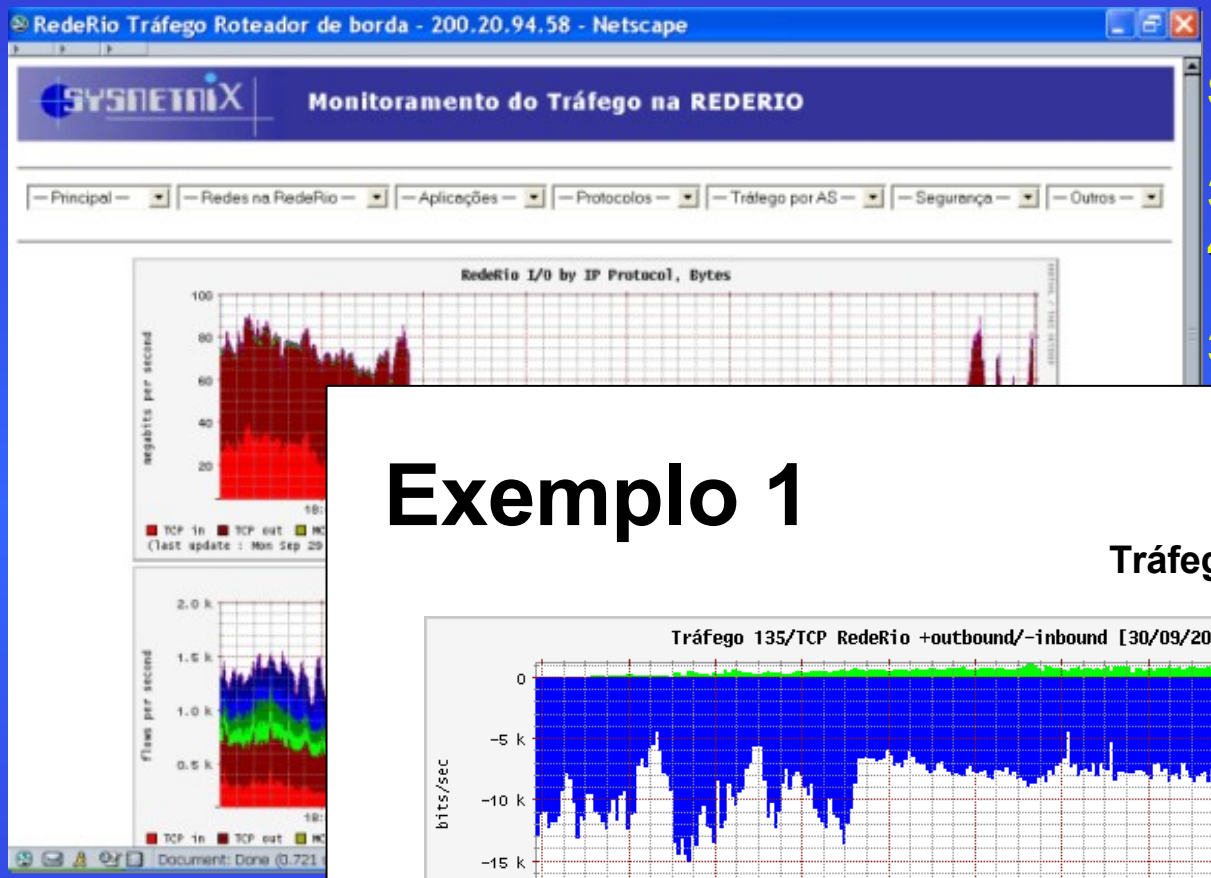
- Importante localizar os responsáveis pelas redes envolvidas.
- Cadastro atualizado constantemente.
- Gerencia Integrada.
- Autenticação de usuários.
- Documentação da Rede.
- Acesso restrito.

GRRW2

- Alertas de falhas: pode ser queda ou congestionamento no link;
- Sistema redundante;
- Gera relatórios WAP;
- Acesso restrito;

Fluxo do Tráfego

Facilidade em detectar incidentes visualmente

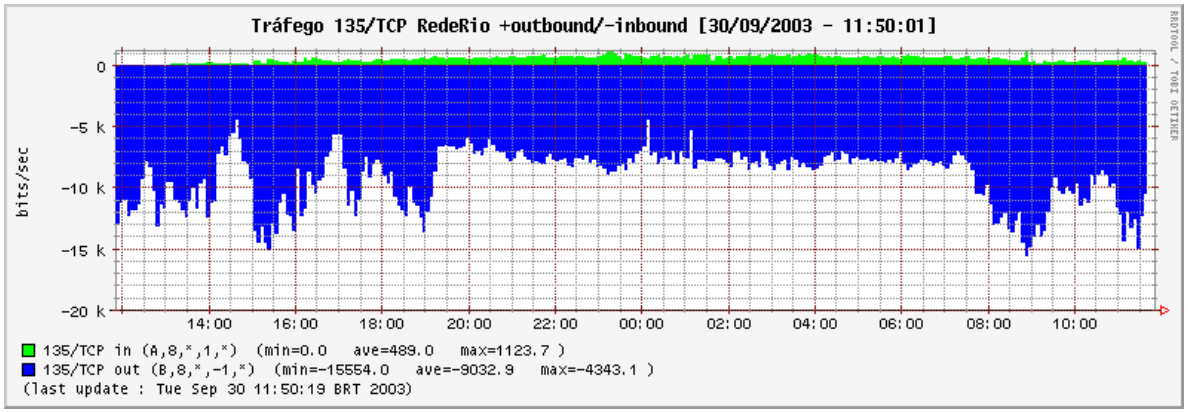


Sistema de Análise de Fluxo:

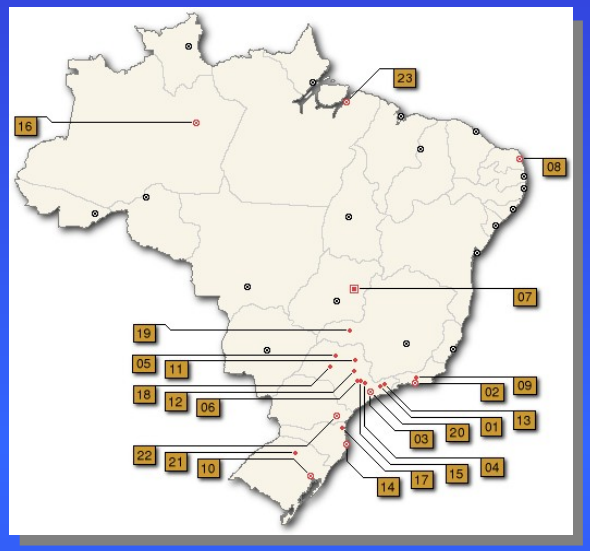
3) Por serviço
4) Por Rede (AS 2715)
   Top 10
3) Por AS

Exemplo 1

Tráfego: RPC MS-Windows



Honeypots



- Coordenação: CERT.br e CenPRA
- Diversas máquinas no espaço Internet brasileiro
- http://www.honeypots-alliance.org.br/index-po.html

- Honeypots de Baixa Interatividade
  Os sistemas e serviços de rede são emulados e o sistema REAL é inacessível.
- Arquitetura Sparc/Sun
- Emulam 4 redes diferentes

Contato

Serviço de Respostas à Incidentes de Segurança CEO/RedeRio:

- **Responsável: Marita Maestrelli**
- **E_mail: security@rederio.br**
- **Chave PGP: http://www.rederio.br/ceo/PGP/RedeRio.asc**
- **Telefone: 21-2141-7124**
- **INOC-DBA: 2715*800**

Coordenação de Engenharia Operacional da Rede Rio