CAIS/RNP: El CSIRT de la Red Académica Brasileña

Rede Nacional de Ensino e Pesquisa - RNP
Centro de Atendimento a Incidentes de Segurança - CAIS

1-7 Octubre de 2005

Liliana Velásquez Solha

Gerente do CAIS/RNP

Jornadas sobre Seguridad Informática

Resumen

- Misión
- Rango de acción
- Servicios ofrecidos
- Proyectos Especiales
- Interacción y cooperación con otros CSIRTs
- Colaboración y parcerías con otras organizaciones

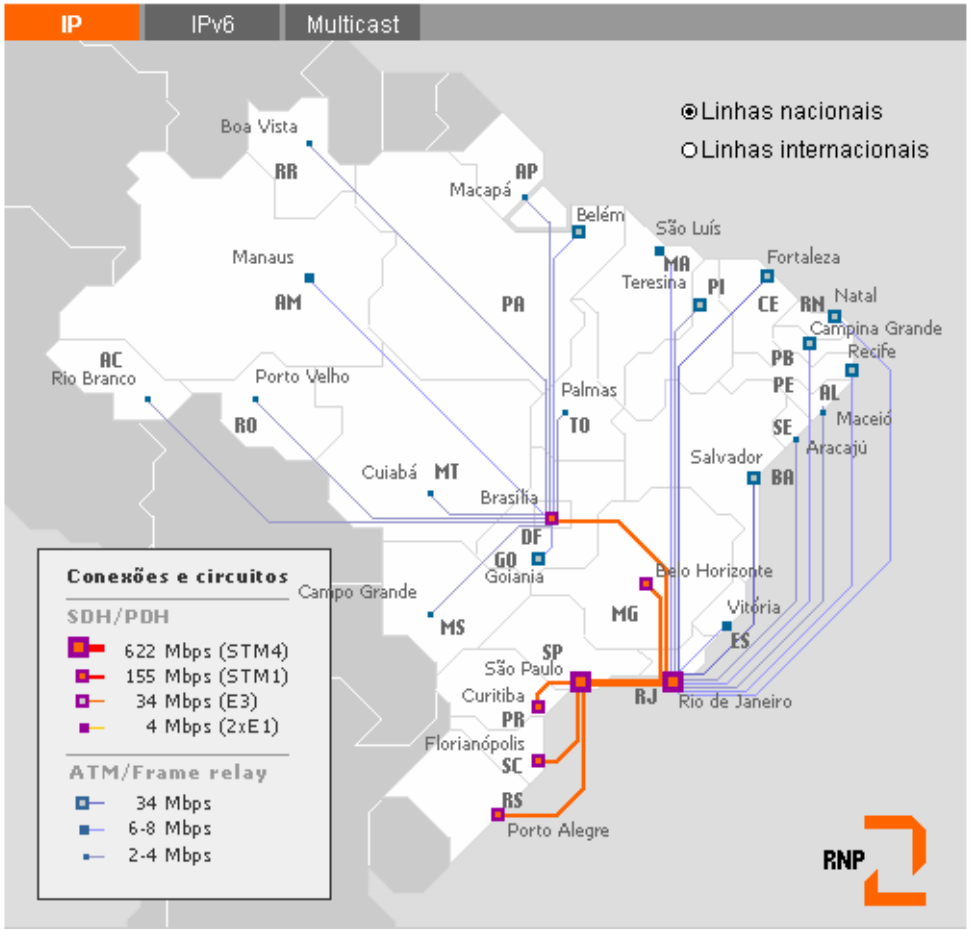
Misión

- [Mayo, 1997] - CAIS inicia sus operaciones
- Misión:

> "CAIS – El Centro de Respuesta a Incidentes de Seguridad actúa en la detección, resolución y prevención de los incidentes de seguridad en la red académica brasileña, además de elaborar, promover y diseminar prácticas de seguridad en redes.

http://www.rnp.br/cais/sobre.html

Rango de acción



- RNP conecta los 27 estados brasileños
- Comunidad académica y de investigación (300 instituciones).
  - Escuelas de educación superior y universidades federales
  - Centros de tecnología federales
  - Laboratorios nacionales
  - Institutos y centros de investigación
  - Museos
- Més de 1,3 millones de usuários

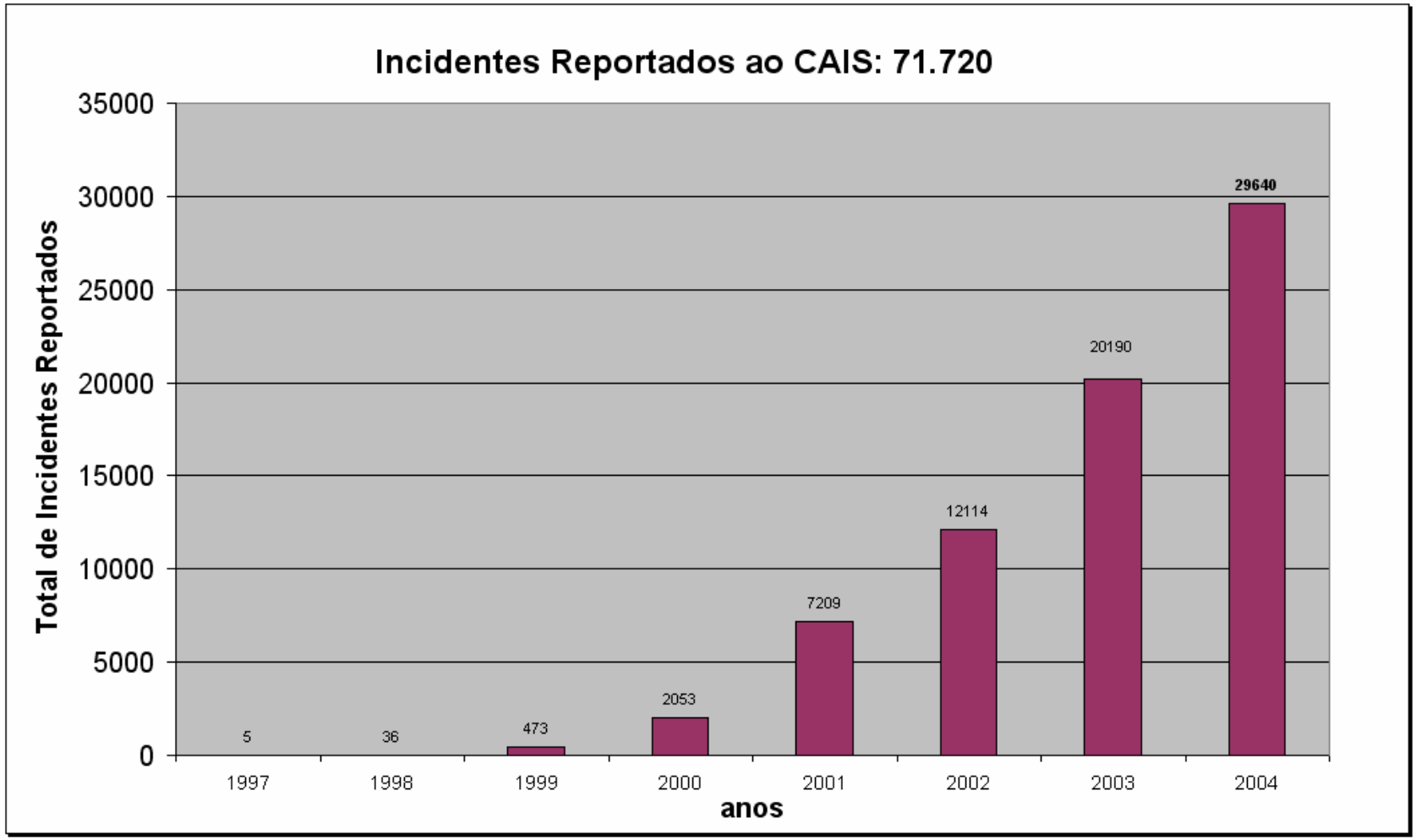
Staff y Operación

- **Staff**
  - 6 empleados (dedicación integral)
    - Gerente de Unida
    - 5 Analistas de Se
  - Capacitación contínua
    Usenix, FIRST Technica
- **Operación**: 24 x 7 (24 h

Servicios ofrecidos

- Tratamiento de incidentes
- Divulgación de informaciones
- Monitoreo y detección de intrusos
- Auditoría de sistemas y testes de penetración
- Educación y Entrenamiento

Servicios: Tratamiento de Incidentes



Tratamiento de Incidentes – Ejemplo: “Phishing Scam”

Servicios: Divulgación de informaciones (2005)

- **91** alertas de seguridad divulgados (**9** produzidos por CAIS) [RNP-ALERTA@cais.rnp.br → 3600 inscritos]
- **18** presentaciones en eventos nacionales e internacionales
- Aproximadamente **40** notícias y notas publicadas, citando el trabalho de CAIS. Cerca de **10** entrevistas concedidas a la prensa.
- Participación en **10** eventos nacionales y **7** internacionales.
- **13** cursos ofrecidos.

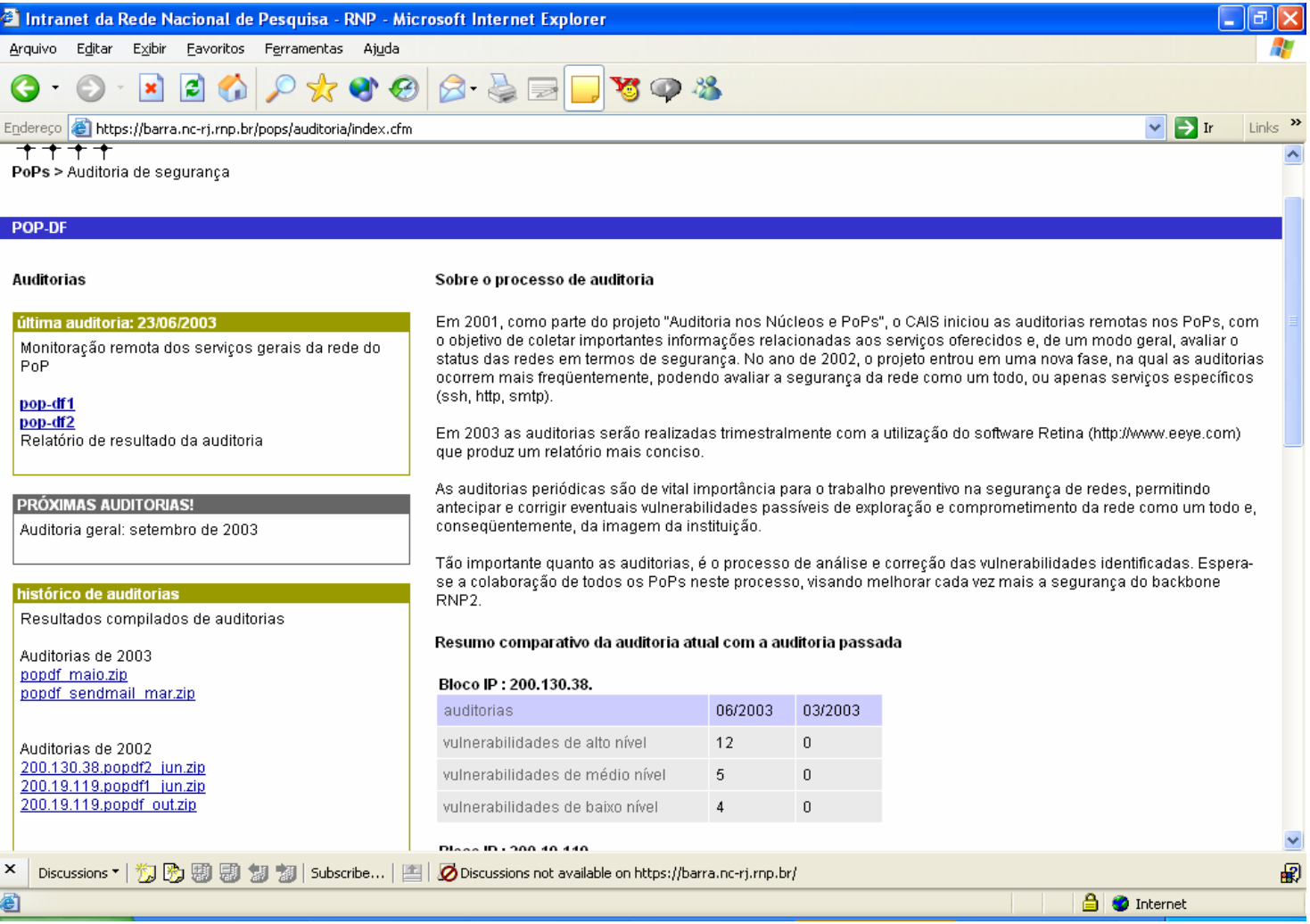
Servicios: Monitoreo y detección de intrusos

- Servidores críticos de la RNP (RNP/PoPs)
- Listas Negras “Blackhole lists”
- Honeynet/Honeypot/Darknet
- Sensores Distribuídos
- Atividade Hacker
- Vírus / Worms / Malware / Top-10 portas
- Webpage defacement mirrors

Servicios: Educación y Entrenamiento

- **41** cursos ministrados
- Participación en **68** eventos nacionales e internacionales

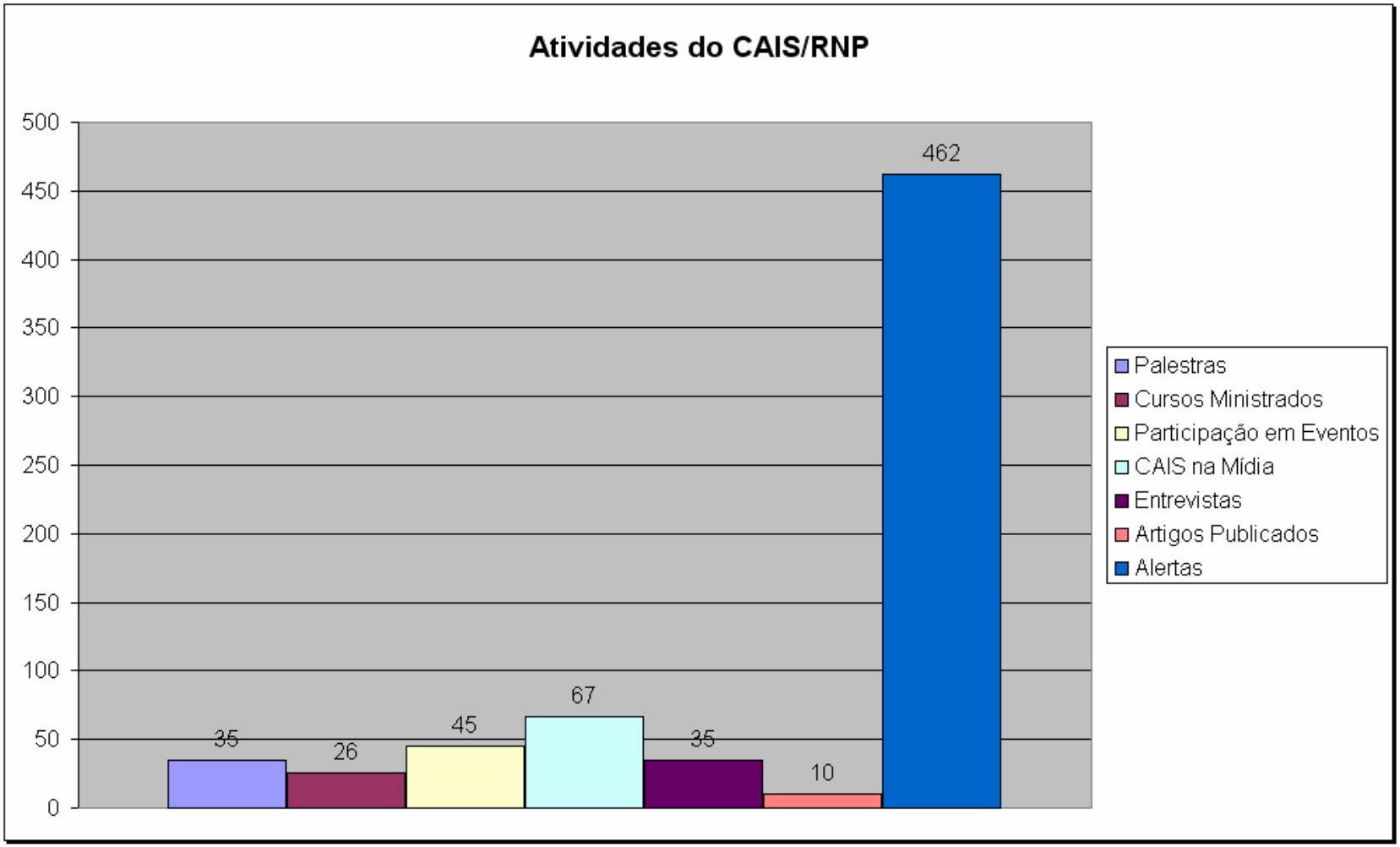
- **Servicios: Auditoría de Sistemas y Redes**



- Periódicas
  x
- Por demanda

- Remotas
  x
- On-site

CAIS en números



- **Proyectos Especiales**
  - Projeto NTP (Network Time Protocol) – Fase II
  - Políticas de Seguridad para la RNP (BS 7799)
  - Programa de Conscientización en Seguridad
  - “CAIS.Storm Center”
  - CSIRTs en Latino América -> CLARA
  - nsp-security-BR (RNP y Brasil Telecom)
  - PKI Académica

- **Interacción y cooperação con otros CSIRTs**
  - FIRST (**F**orum of **I**ncident **R**esponse **S**ecurity **T**eams)
    - 202 grupos de seguridad (CSIRTs)
    - CAIS es miembro desde setiembre de 2001
    - Gerente do CAIS, miembro del Steering Commitee desde 2002
    - Analista do CAIS, Hands-On Coordinator del FIRST
  - En particular: CERT/CC, Rediris, UNAM-CERT, CERT-BR, TERENA
    - ArCERT, CL-CERT (patrocínio ao FIRST)
    - APSIRT (Asia & Pacific)
    - TF-CSIRT (Europa)
  - “Desafío Forense” - versión 1 y 2 (Colaboración)

- **Interacción y cooperación con otras entidades**
  - Gobierno Federal
    - GT de Sincronismo
    - GT de Seguridad en sitios gobernamentales
    - GT – Respuesta a Incidentes de Seguridad en Redes Gobernamentales (CETIR.GOV)
    - GT Tratamiento de Incidentes – CBC-1 - Anatel
  - Órganos policiales
    - Polícía Federal
    - Polícía Civíl

- **Otras colaboraciones**
  - SANS – Security Administration Network Security – 2002

    “Las 20 vulnerabilidades de seguridad más críticas”
  - ITU (International Communication Union) - 2003

    “Creating Trust in Critical Network Infrastructures: The case of Brazil”
  - SANS – Security Administration Network Security – 2003

    “Mistakes people make that lead to Security Breaches”
  - *CERT/CC: State of the Practice of CSIRTs*

Contato com o CAIS: Notificação de Incidentes

Incidentes de segurança envolvendo redes conectadas ao backbone da RNP podem ser encaminhadas ao CAIS através de:

1. *E-mail*: **cais@cais.rnp.br**.

   Para envio de informações criptografadas, recomenda-se o uso da chave PGP pública do CAIS, disponível em: **http://www.rnp.br/cais/cais-pgp.key**

2. *Web*: Através do Formulário para Notificação de Incidentes de Segurança, disponível em: **http://www.rnp.br/cais/atendimento_form.html**

Telefone:

No horário comercial (09:00 – 18:00), através do telefone: **(19) 3787-3300** ou **INOC DBA 1916*800** (Voz sobre IP).

Atendimento Emergencial:

Contatos emergenciais fora do horário comercial devem ser feitos através do telefone: **(61) 3226-9465**.

Alertas do CAIS

O CAIS mantém a lista **rnp-alerta@cais.rnp.br**. Assinatura aberta à comunidade atuante na área. Inscrições através do formulário disponível em:

http://www.rnp.br/cais/alertas