

# 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





## Resumen

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



## Misión

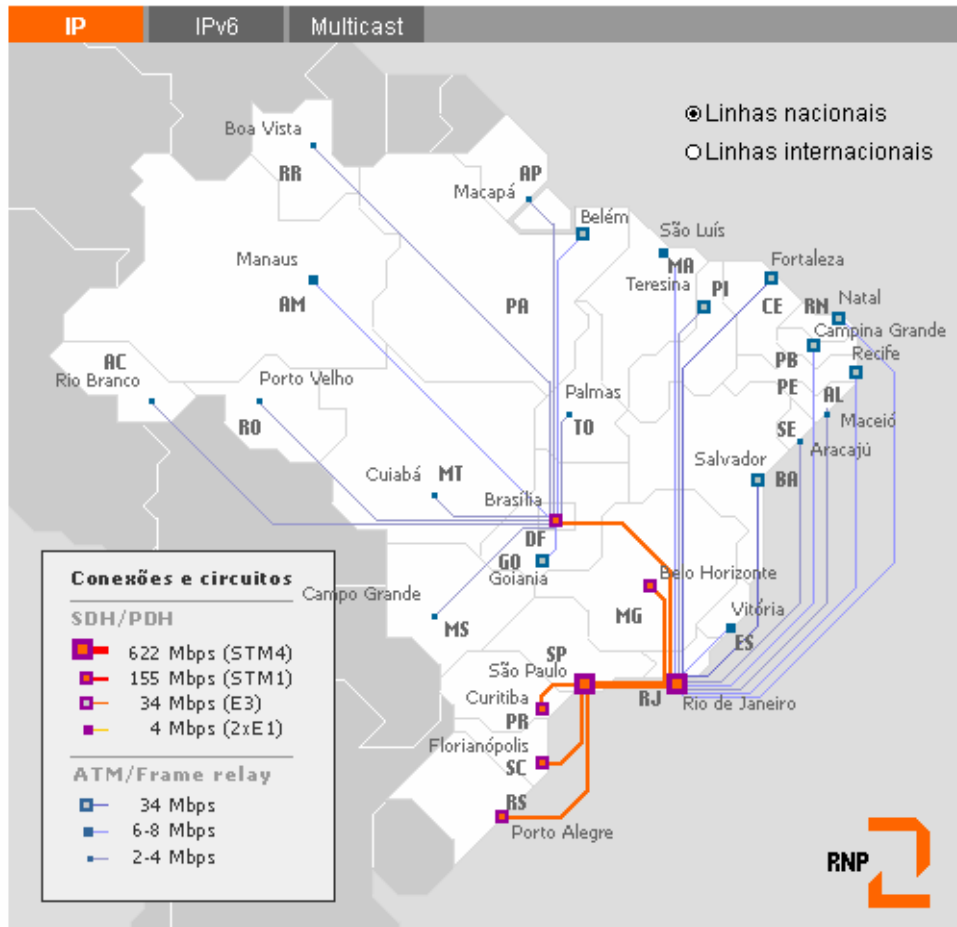
- [Mayo, 1997] - CAIS inicia sus operaciones
- Misión:

“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
- Más de 1,3 millones de usuarios

## Staff y Operación

- **Staff**
  - 6 empleados (dedicación integral)
    - Gerente de Unidad
    - 5 Analistas de Seguridad
  - Capacitación continua: Usenix, FIRST Technical
- **Operación:** 24 x 7 (24 h)



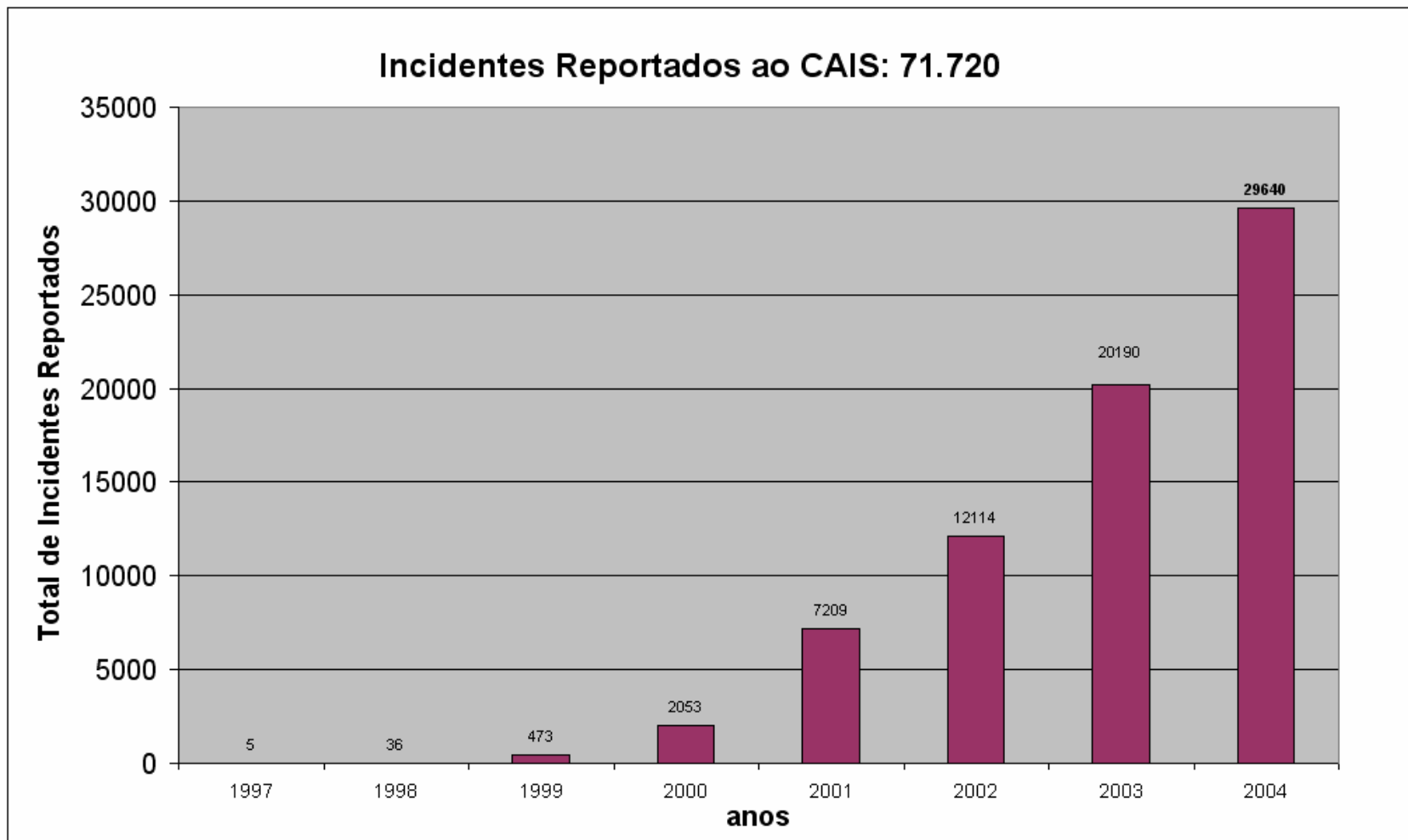


## Servicios ofrecidos

- 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”



The screenshot shows a web browser window titled "BB Internet E-Mail Banking - Microsoft Internet Explorer". The address bar shows the URL "http://www.obancodobrasil.com/login.php". The page layout includes a yellow header with the BB logo and navigation links. The main content area is divided into several sections:

- Sua Conta**: Navigation links for "Acesso", "Segurança", "Perguntas Frequentes", and "Certificação Digital".
- Novo teclado virtual**: A section with a graphic of an eye and a numeric keypad. Text: "Novo teclado virtual: somente para seus olhos." and "Sequência de números alterada a cada acesso." Below the keypad, it says: "Agora, a entrada das senhas será feita **exclusivamente** pelo teclado virtual, da seguinte forma:" followed by two bullet points:
  - Senha Auto-Atendimento (8 dígitos):** Somente nesta tela. As transações de consulta (saldos, extratos, etc..) não exigirão mais senha.
  - Senha cartão (6 dígitos):** Na confirmação de transações que envolvam movimentação financeira
- BB Internet E-Mail Banking - CADASTRO**: A registration form with fields for "Título" (dropdown), "1º Titular", "Agência", "Conta", "Senha", and "Senha do cartão". Buttons for "Entrar" and "Limpa" are present. A link "Problemas, clique aqui" is also visible.
- Conheça as Mudanças**: A blue box with text: "Simplificando o uso - A partir de agora você utilizará senhas apenas para entrar na sua conta e para transações com movimentação financeira. [Conheça os detalhes »](#)" and "Novo teclado virtual - O novo teclado virtual é muito mais amigável. As principais novidades são: botões numéricos maiores, sequência alterada, controle de luminosidade e posição centralizada na página. [Saiba mais »](#)".
- Informações Importantes**: A grey box with links: "Ajuda para quem é usuário Windows XP »", "BB não envia e-mail sem sua permissão »", and "Saiba como identificar um site seguro »".

The footer of the page contains the phone number "0800-785678" and links for "política de privacidade", "internet grátis", and "mapa do site".





## Servicios: Divulgación de informaciones (2005)

- **91** alertas de seguridad divulgados (**9** producidos por CAIS) [RNP-ALERTA@cais.rnp.br → 3600 inscritos]
- **18** presentaciones en eventos nacionales e internacionales
- Aproximadamente **40** noticias y notas publicadas, citando el trabajo 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



Anti-Phishing  
Working Group

## Servicios: Educación y Entrenamiento



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



## • Servicios: Auditoría de Sistemas y Redes

**POP-DF**

**Auditorias**

**última auditoria: 23/06/2003**  
Monitoração remota dos serviços gerais da rede do PoP  
[pop-df1](#)  
[pop-df2](#)  
Relatório de resultado da auditoria

**PRÓXIMAS AUDITORIAS!**  
Auditoria geral: setembro de 2003

**histórico de auditorias**  
Resultados compilados de auditorias  
Auditorias de 2003  
[popdf\\_mai0.zip](#)  
[popdf\\_sendmail\\_mar.zip](#)  
Auditorias de 2002  
[200.130.38.popdf2\\_jun.zip](#)  
[200.19.119.popdf1\\_jun.zip](#)  
[200.19.119.popdf\\_out.zip](#)

**Sobre o processo de auditoria**

Em 2001, como parte do projeto "Auditoria nos Núcleos e PoPs", o CAIS iniciou as auditorias remotas nos PoPs, com o objetivo de coletar importantes informações relacionadas aos serviços oferecidos e, de um modo geral, avaliar o status das redes em termos de segurança. No ano de 2002, o projeto entrou em uma nova fase, na qual as auditorias ocorrem mais frequentemente, podendo avaliar a segurança da rede como um todo, ou apenas serviços específicos (ssh, http, smtp).

Em 2003 as auditorias serão realizadas trimestralmente com a utilização do software Retina (<http://www.eeye.com>) que produz um relatório mais conciso.

As auditorias periódicas são de vital importância para o trabalho preventivo na segurança de redes, permitindo antecipar e corrigir eventuais vulnerabilidades passíveis de exploração e comprometimento da rede como um todo e, conseqüentemente, da imagem da instituição.

Tão importante quanto as auditorias, é o processo de análise e correção das vulnerabilidades identificadas. Espere-se a colaboração de todos os PoPs neste processo, visando melhorar cada vez mais a segurança do backbone RNP2.

**Resumo comparativo da auditoria atual com a auditoria passada**

**Bloco IP : 200.130.38.**

auditorias	06/2003	03/2003
vulnerabilidades de alto nível	12	0
vulnerabilidades de médio nível	5	0
vulnerabilidades de baixo nível	4	0

**Bloco IP : 200.19.119.**

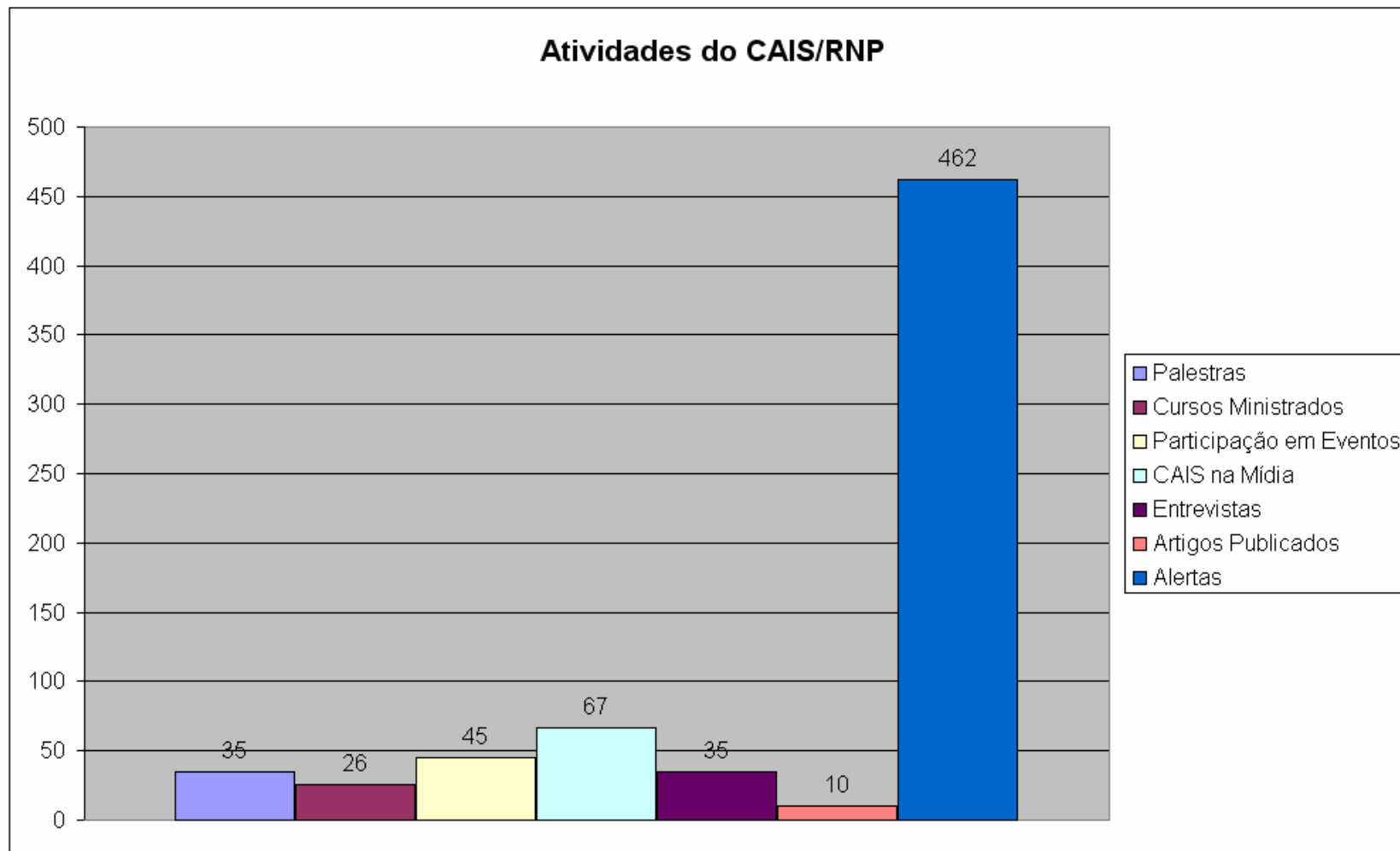
- Periódicas  
X
- Por demanda

- 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 Committee 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 gubernamentales
    - GT – Respuesta a Incidentes de Seguridad en Redes Gubernamentales (CETIR.GOV)
    - GT Tratamiento de Incidentes – CBC-1 - Anatel
  - Órganos policiales
    - Policía Federal
    - Policía Civil





- **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](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>**