Tratamento de incidentes de segurança na Rede Acadêmica Brasileira

Frederico Costa
Atanaí Sousa Ticianelli

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

CAIS

RNP

Ministério da Educação

Ministério da Ciência e Tecnologia

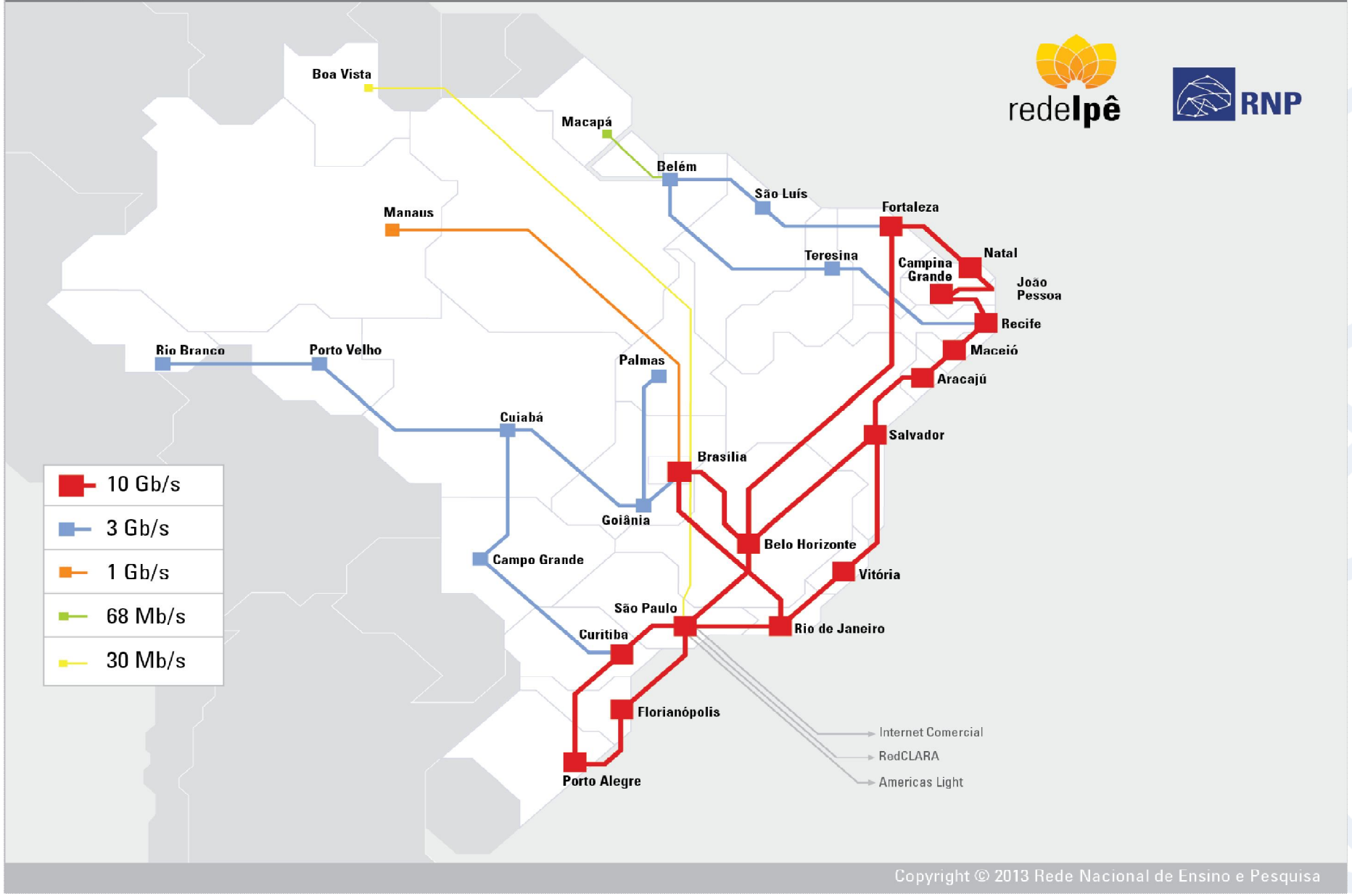
BRASIL UM PAÍS DE TODOS GOVERNO FEDERAL

Agenda

- RNP e CAIS
- Detalhamento do processo de RI
- Histórico do atendimento a incidentes
- Números e incidentes em destaque
- Iniciativas em prevenção
- Desafios e visão de futuro
- Parcerias

RNP

Situação em maio de 2013



Centro de Atendimento a Incidentes de Segurança

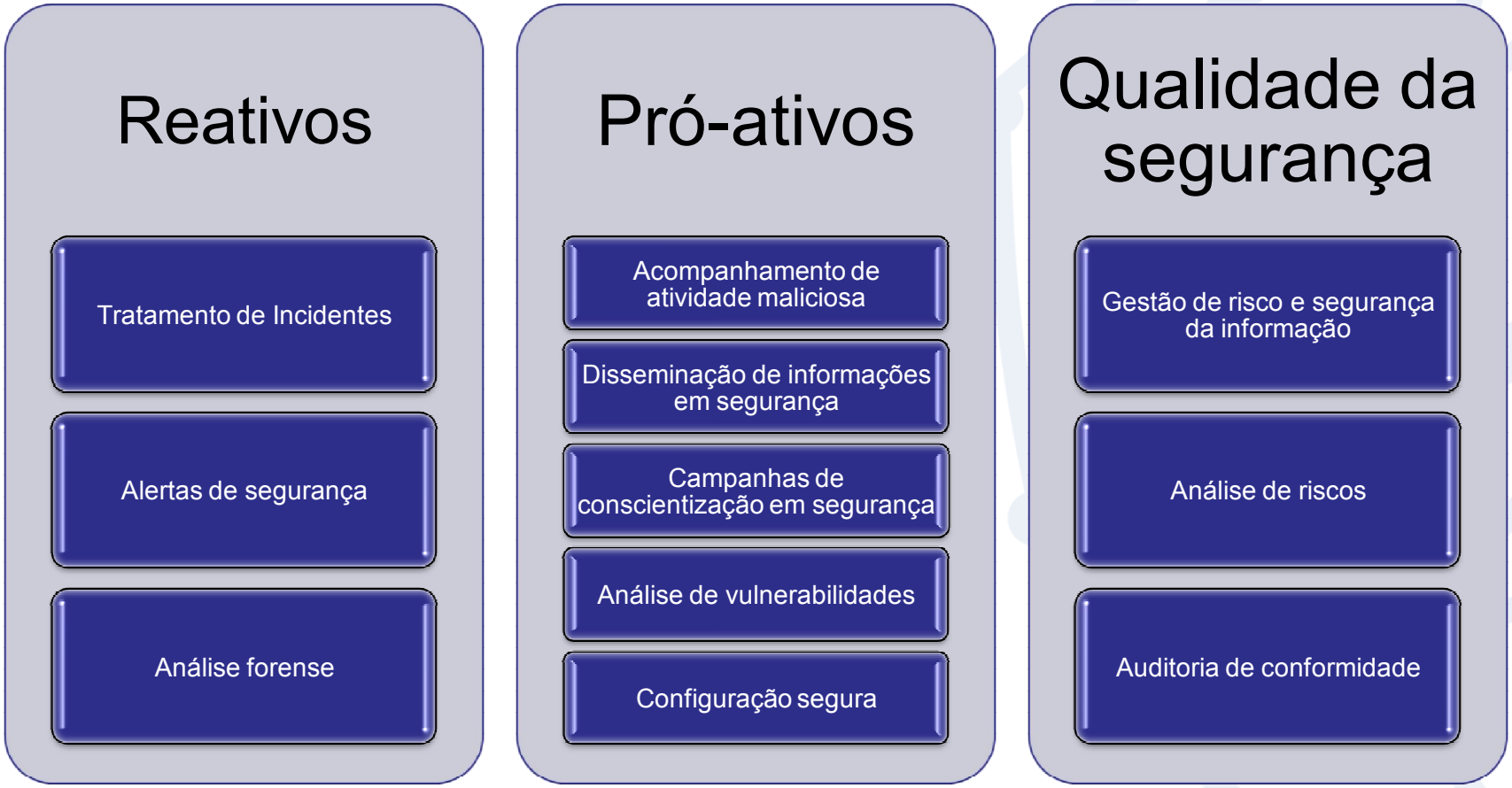
- Maio de 1997 – CAIS inicia suas operações

"... atua na detecção, resolução e prevenção de incidentes de segurança na rede acadêmica brasileira, além de elaborar, promover e disseminar práticas de segurança em redes."

- 7 pessoas atuando em quatro áreas principais

  - **GIS** : Gestão de Incidentes de Segurança
  - **DCS** : Disseminação da Cultura de Segurança
  - **GRSI** : Gestão de Riscos e Segurança da Informação
  - **INFRA** : Infraestrutura e Serviços à Comunidade Acadêmica

- **Serviços**


Reativos
Tratamento de Incidentes
Alertas de segurança
Análise forense
Pró-ativos
Acompanhamento de atividade maliciosa
Disseminação de informações em segurança
Campanhas de conscientização em segurança
Análise de vulnerabilidades
Configuração segura
Qualidade da segurança
Gestão de risco e segurança da informação
Análise de riscos
Auditoria de conformidade

CAIS - Detalhamento do processo de GIS

– Operar o serviço de atendimento a incidentes de segurança identificados no backbone, nos PoPs, em instituições conectadas à RNP ou em clientes através da prestação de serviço (ação reativa).

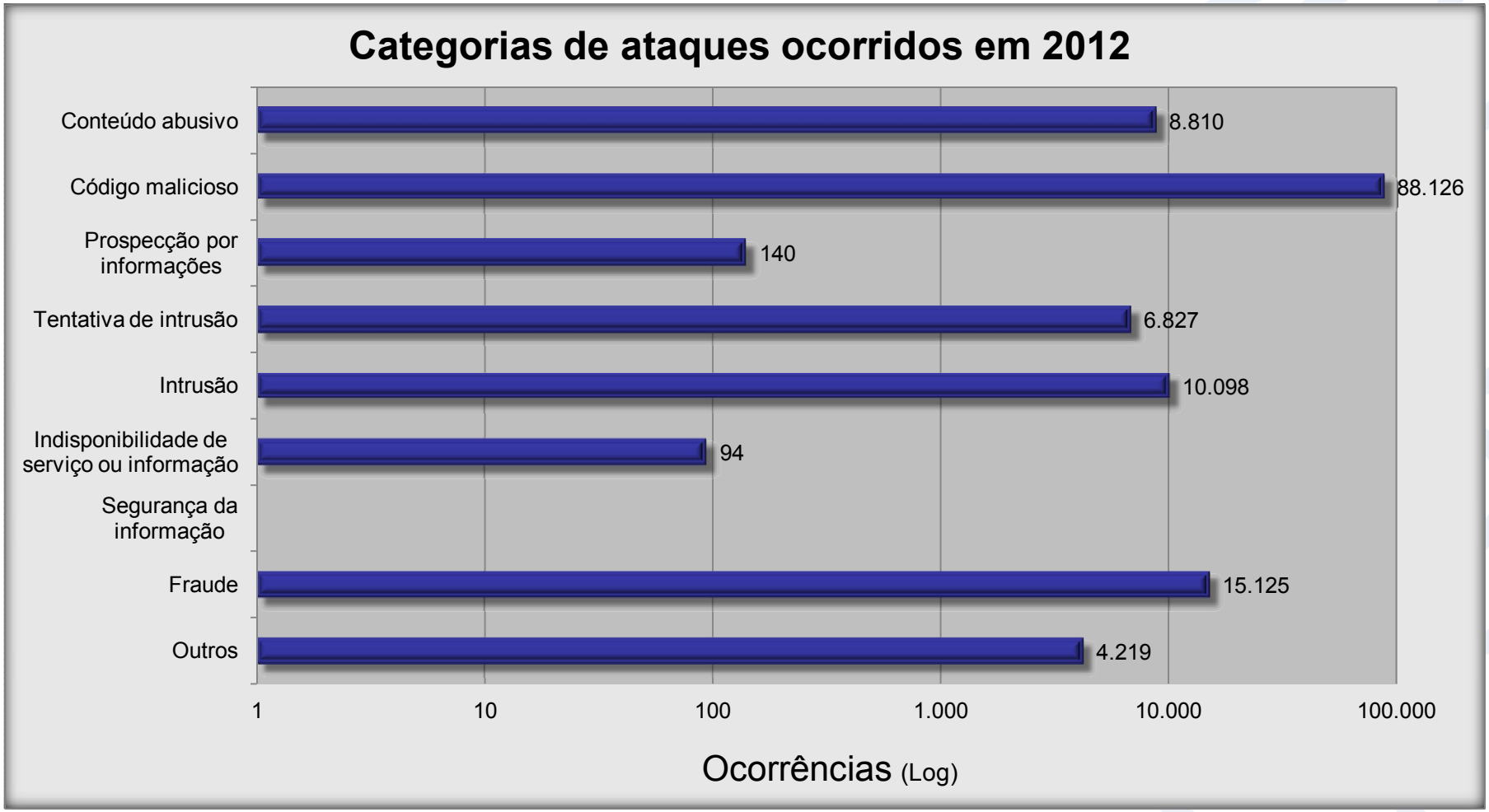
– Gerar documentação, relatórios estatísticos, manutenção e iniciativas de melhoria no processo

CAIS - Detalhamento do processo de GIS

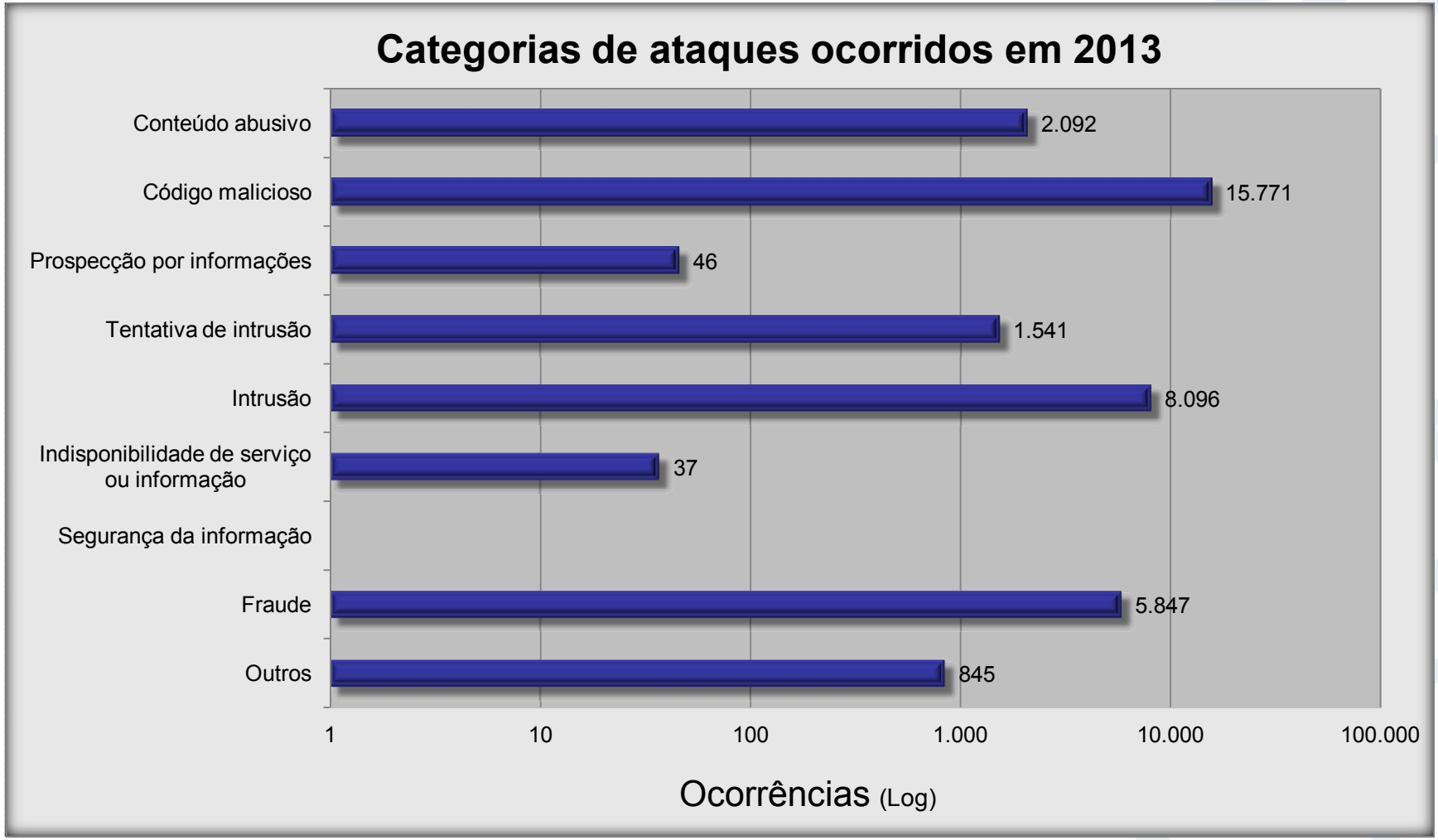
- Ponto de contato de segurança para toda a rede acadêmica
- Notificações de incidentes oriundas de
  - Parcerias no monitoramento de atividade maliciosa
  - Monitoramento do backbone
  - Grupos de pesquisa/resposta a incidentes (spamcop, shadowserver)
  - Notificações de clientes

Histórico do atendimento a incidentes

Histórico do atendimento a incidentes



Números e incidentes em destaque



Números e incidentes em destaque

- **2011 – DDoS “fashion year”**
  - Ataques de negação de serviço se tornam “armas” para grupos hackers e para outros grupos auto-denominados de “cyberativistas”;
  - Diversos grupos “recrutam” usuários pela Internet em prol de uma causa ou objetivo em comum;
  - Instituições e corporações das mais diversas áreas foram afetadas por este “movimento”.

** Imagens coletadas diretamente do Twitter*

*** http://webtrends.about.com/od/profile1/tp/Rage-Faces-Internet-Meme-Faces-And-Funny-Memes.htm*

- **Ataques contra os clientes da RNP**
  - Um cliente importante sofreu um ataque de aproximadamente 900Mbps, indisponibilizando o acesso às informações em um momento crítico
    - Este ataque foi mitigado e contido
  - Uma instituição foi citada para ser atacada, em uma conversa em um canal IRC de um grupo de “cyberativistas”
    - Este ataque não chegou a ocorrer ou não foi suficientemante significativo

```
<hlbbit> pacota esse 150.162.2.10
* AttaXX (bels@AN-d77.tua.qj9f10.IP) has joined #LulzSecBrazil
* _0RL0FF_ (_0RL0FF_@AN-6j1.1l5.rnpprb.IP) has joined #LulzSecBrazil
<shibi> esse ip é de onde?
<hlbbit> universidade federal
<Lefioda> ufsc
<hlbbit> de santa catarina
```

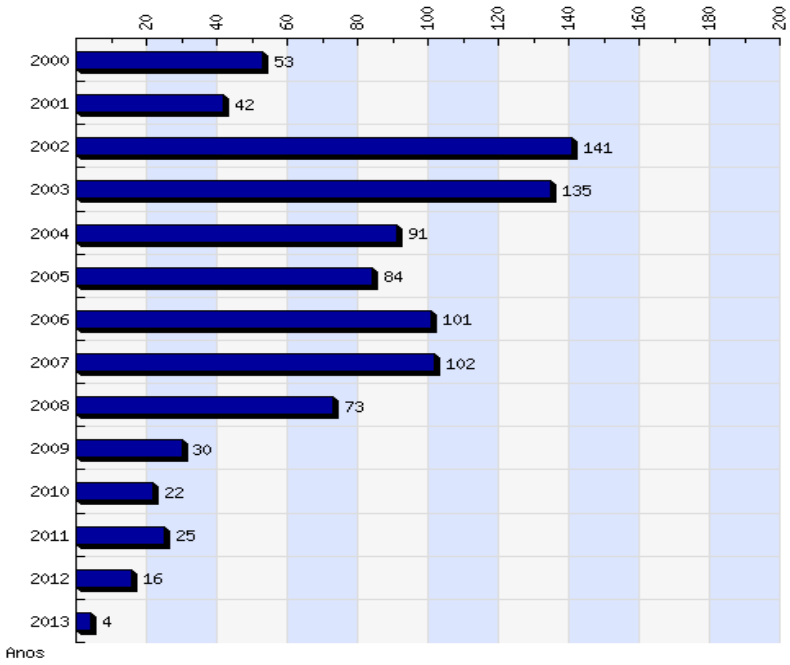
Números e incidentes em destaque

- **Utilização de computadores conectados à RNP para participar de ataques**
  - Dados coletados em atividades de monitoramento e informações enviadas por parceiros mostram que indivíduos supostamente ligados a grupos como Anonymous e Lulzsec pretendiam utilizar o backbone da RNP em seus ataques.
    - Esta utilização do backbone não ocorreu

```
Jun 22 13:03:51 <JC_muahaha>    as conexoes do brasil, ainda que
pontuais
Jun 22 13:03:53 <JC_muahaha>    passam por backbones
Jun 22 13:04:07 <JC_muahaha>    ou seja, eles roteiam as informacoes
que entram no pais
Jun 22 13:04:54 <JC_muahaha>    podemos usar um DDOS mais potente
Jun 22 13:04:56 <JC_muahaha>    e deixar o brasil inteiro
Jun 22 13:04:57 <JC_muahaha>    isolado
Jun 22 13:04:59 <JC_muahaha>    da internet mundial
Jun 22 13:05:01 <JC_muahaha>    por exemplo
Jun 22 13:05:08 <JC_muahaha>    hackers fizeram isso na espanha
Jun 22 13:05:09 <JC_muahaha>    ha uns 6 anos
...
Jun 22 13:17:35 <pr0teus>       JC_muahaha:  ate tenho uma solucao
Jun 22 13:18:04 <pr0teus>       JC_muahaha: parte da RNP eh ligada ao
exterior por backbones proprios...
Jun 22 13:18:29 <pr0teus>       JC_muahaha: basta só ter acesso a
alguns servidores da RNP
Jun 22 13:19:19 <JC_muahaha>    pr0teus, esse eh um bom caminho
```

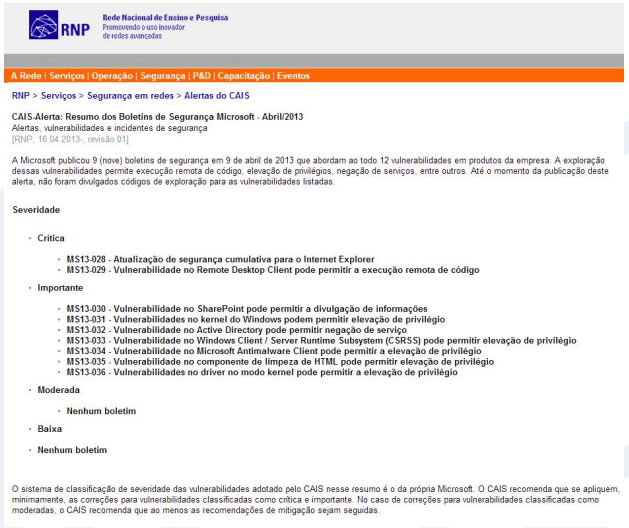
Iniciativas em prenvenção

- **Divulgação de alertas de segurança**
  - Alertas
    - rnp-alertas@cais.rnp.br | http://www.rnp.br/cais/alertas/
      - 16 Alertas em 2012
      - 4.000 inscritos
      - Vulnerabilidades em software e temas diversos



Iniciativas em prenvenção

- **Publicações**
  - CAIS-Resumo
    - Alertas, vulnerabilidades, incidentes, notícias
    - Periodicidade quadrimestral
    - Veículo de divulgação das ações do CAIS/RNP


RNP Rede Nacional de Ensino e Pesquisa
Promovendo o uso inovador de redes avançadas

A Rede | Serviços | Operação | Segurança | P&D | Capacitação | Eventos

RNP > Serviços > Segurança em redes > Alertas do CAIS

CAIS Alerta: Resumo dos Boletins de Segurança Microsoft - Abril/2013
Alertas, vulnerabilidades e incidentes de segurança
[RNP, 16.04.2013-, revisão 01]

A Microsoft publicou 9 (nove) boletins de segurança em 9 de abril de 2013 que abordam ao todo 12 vulnerabilidades em produtos da empresa. A exploração dessas vulnerabilidades permite execução remota de código, elevação de privilégios, negação de serviços, entre outros. Até o momento da publicação deste alerta, não foram divulgados códigos de exploração para as vulnerabilidades listadas.

Severidade

- **Crítica**
  - **MS13-028 - Atualização de segurança cumulativa para o Internet Explorer**
  - **MS13-029 - Vulnerabilidade no Remote Desktop Client pode permitir a execução remota de código**
- **Importante**
  - **MS13-030 - Vulnerabilidade no SharePoint pode permitir a divulgação de informações**
  - **MS13-031 - Vulnerabilidades no kernel do Windows podem permitir elevação de privilégio**
  - **MS13-032 - Vulnerabilidade no Active Directory pode permitir negação de serviço**
  - **MS13-033 - Vulnerabilidade no Windows Client / Server Runtime Subsystem (CSRSS) pode permitir elevação de privilégio**
  - **MS13-034 - Vulnerabilidade no Microsoft Antimalware Client pode permitir a elevação de privilégio**
  - **MS13-035 - Vulnerabilidade no componente de limpeza de HTML pode permitir elevação de privilégio**
  - **MS13-036 - Vulnerabilidades no driver no modo kernel pode permitir a elevação de privilégio**
- **Moderada**
  - **Nenhum boletim**
- **Baixa**
- **Nenhum boletim**

O sistema de classificação de severidade das vulnerabilidades adotado pelo CAIS nesse resumo é o da própria Microsoft. O CAIS recomenda que se apliquem, minimamente, as correções para vulnerabilidades classificadas como crítica e importante. No caso de correções para vulnerabilidades classificadas como moderadas, o CAIS recomenda que ao menos as recomendações de mitigação sejam seguidas.

  - Pesquisa de segurança
    - Panorama de segurança nas redes acadêmicas.
    - Escopo inicial: IFES (parceria com Andifes)
    - Periodicidade annual

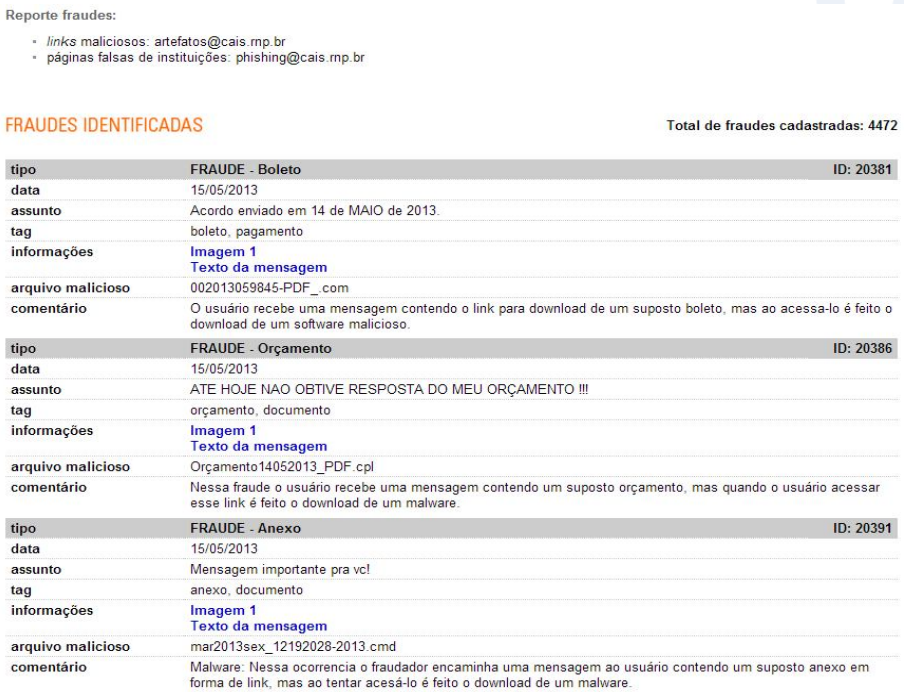
  - Cartilhas de segurança:
    - Segurança em redes sociais
    - Segurança em dispositivos móveis

Iniciativas em prevenção

- **Educação e treinamento**
  - Palestras
    - Eventos nacionais e internacionais
      - GTS, FIRST, CLARA, OEA
  - Cursos/treinamentos
    - Eventos nacionais e internacionais
      - Ex: SCI/RNP, WRNP, CLARA-TEC

Iniciativas em prevenção

- **Catálogo de fraudes**
  - **http://www.rnp.br/cais/fraudes.php**
    - Informar, exemplificar e analisar os modelos de fraude mais comuns em circulação na internet.
    - Grande colaboração da comunidade.
    - 4.472 fraudes cadastradas
      - Colaborações: **phishing@cais.rnp.br**



Reporte fraudes:

- *links* maliciosos: artefatos@cais.rnp.br
- páginas falsas de instituições: phishing@cais.rnp.br

FRAUDES IDENTIFICADAS — Total de fraudes cadastradas: 4472

tipo	FRAUDE - Boleto	ID: 20381
data	15/05/2013	
assunto	Acordo enviado em 14 de MAIO de 2013.	
tag	boleto, pagamento	
informações	Imagem 1 Texto da mensagem	
arquivo malicioso	002013059845-PDF_.com	
comentário	O usuário recebe uma mensagem contendo o link para download de um suposto boleto, mas ao acessa-lo é feito o download de um software malicioso.	
tipo	FRAUDE - Orçamento	ID: 20386
data	15/05/2013	
assunto	ATE HOJE NAO OBTIVE RESPOSTA DO MEU ORÇAMENTO !!!	
tag	orçamento, documento	
informações	Imagem 1 Texto da mensagem	
arquivo malicioso	Orçamento14052013_PDF.cpl	
comentário	Nessa fraude o usuário recebe uma mensagem contendo um suposto orçamento, mas quando o usuário acessar esse link é feito o download de um malware.	
tipo	FRAUDE - Anexo	ID: 20391
data	15/05/2013	
assunto	Mensagem importante pra vc!	
tag	anexo, documento	
informações	Imagem 1 Texto da mensagem	
arquivo malicioso	mar2013sex_12192028-2013.cmd	
comentário	Malware: Nessa ocorrencia o fraudador encaminha uma mensagem ao usuário contendo um suposto anexo em forma de link, mas ao tentar acesá-lo é feito o download de um malware.	

Iniciativas em prevenção

- Promoção de eventos
  - Dia Internacional de Segurança em Informática

    http://www.rnp.br/eventos/disi

    - Evento promovido desde 2005
    - Voltado ao usuário final de computadores
    - Discutir temas atuais sobre segurança no uso das tecnologias de informação, com palestras transmitidas pela Internet
    - **Cybercrime – Como não passar de vítima a vilão (30 de Agosto de 2013)**

Iniciativas em prevenção

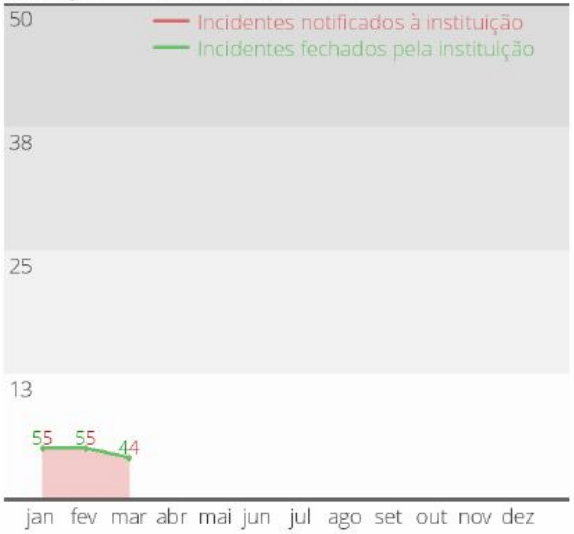
- Promoção de eventos
  - EnCSIRT: Encontro de CSIRT acadêmicos
    - Evento voltado para os CSIRTs das instituições conectadas ao backbone acadêmico
    - Discussão de temas de interesse as atividades de um CSIRT e para a interação entre grupos
    - Comumente ocorre junto com o SCI
  - SCI – Seminário de Capacitação e Inovação
    - Participação regular:
      - Treinamento em segurança
      - Workshop de Segurança

Relatório Mensal de Incidentes de Segurança

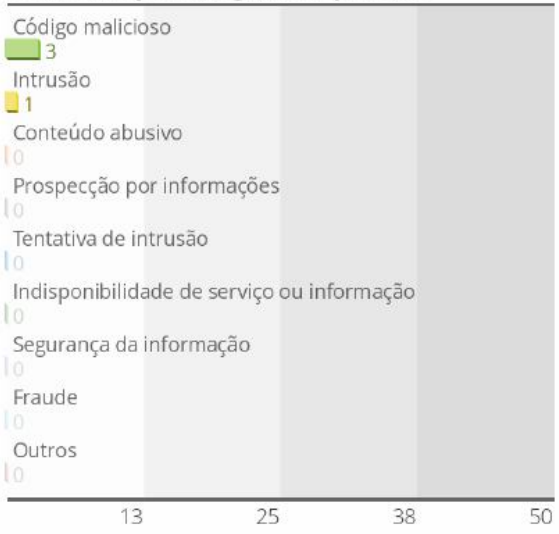
Instituição: **Universidade** [redacted]
Período: **Março de 2013** (gerado em 25/04/2013)

Gestor: –
Contato de segurança: [redacted]
PoP: **SP**

Evolução de incidentes no ano



Incidentes por categoria no período



Posição no Ranking

Incidentes notificados
128 em 273
Incidentes fechados
100,00%

TOP 10 IPs	Qtde.
[redacted]	1
	1
	1
	1

Contabilização de incidentes

Categoria	Tipo	Status					Total
		APC	AEA	ANR	F	FE	
1. Conteúdo abusivo	1.1. Spam	0	0	0	0	0	0
	1.2. Assédio/discriminação	0	0	0	0	0	0
	1.3. Outros	0	0	0	0	0	0
	Total por categoria	**0**	**0**	**0**	**0**	**0**	**0**
2. Código malicioso	2.1. Bot	0	0	0	3	0	3

Parcerias

- Entende-se que há espaço para colaboração entre CAIS/RNP, DSIC, CTIR.Gov e outros CSIRTs governamentais:

- Resposta coordenada a incidentes de segurança
  - CAIS/RNP e CTIR.Gov: Interseção entre "constituencies"

    Instituições de ensino e pesquisa que fazem parte da administração pública (ex. IFES, IFs e UPs)

  - CAIS/RNP e CSIRTs de provedores governamentais

    Clientes com mais de um upstream: RNP e ANSP, RNP e Serpro (GRA)

  - Monitoramento de atividade maliciosa em períodos críticos

    Exemplo: ENEM, Declaração IR, etc

    Carência de coordenação de ações conjuntas

  - Como pode ser aprimorado o processo de resposta?

Parcerias

– Normatização, conformidade e promoção de boas práticas

- RNP e Governo Federal: Interseção entre "constituencies"

  2013: Início do Programa de Fortalecimento da SI nas Organizações Usuárias

  Programa plurianual

  Conta-se com o apoio do trabalho conjunto entre DSIC, TCU e RNP

Centro de Atendimento a Incidentes de Segurança – CAIS/RNP

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

 @cais_rnp

Frederico Costa – frederico.costa@cais.rnp.br
cais@cais.rnp.br