# Relatório Mensal de Incidentes de Segurança como instrumento de melhoria contínua

Rildo Souza
Centro de Atendimento a Incidentes de Segurança (CAIS)

redeIpê

RNP

Ministério da Cultura
Ministério da Saúde
Ministério da Educação
Ministério da Ciência, Tecnologia e Inovação

BRASIL
PAÍS RICO É PAÍS SEM POBREZA

WTR 2013 PoP-SC
Workshop de tecnologia de redes

# Agenda

- Sobre o CAIS
  Estatísticas
- Relatório de Incidentes de Segurança
  Visão Geral
  Incidentes envolvendo clientes do PoP-SC
  Estatísticas de fechamento anual
- Notificações do CAIS
  Entendendo as notificações do CAIS
  Fechando Incidentes – 1 MD5
  Fechando Incidentes – N MD5s
- Relatório de Incidentes como instrumento de melhoria contínua
- Próximos Passos

# CAIS

- Centro de Atendimento a Incidentes de Segurança
- 16 anos de atuação na área de segurança
- Clientes: instituições conectadas à RNP

*"O Centro de Atendimento a Incidentes de Segurança (CAIS) 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."*

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

# Gestão de Incidentes de Segurança

- Papel de coordenação e suporte aos clientes
- Atuação nos núcleos da RNP e no backbone
- 1 coordenador de área
- 2 analistas dedicados em regime de plantão

# Gestão de Incidentes de Segurança

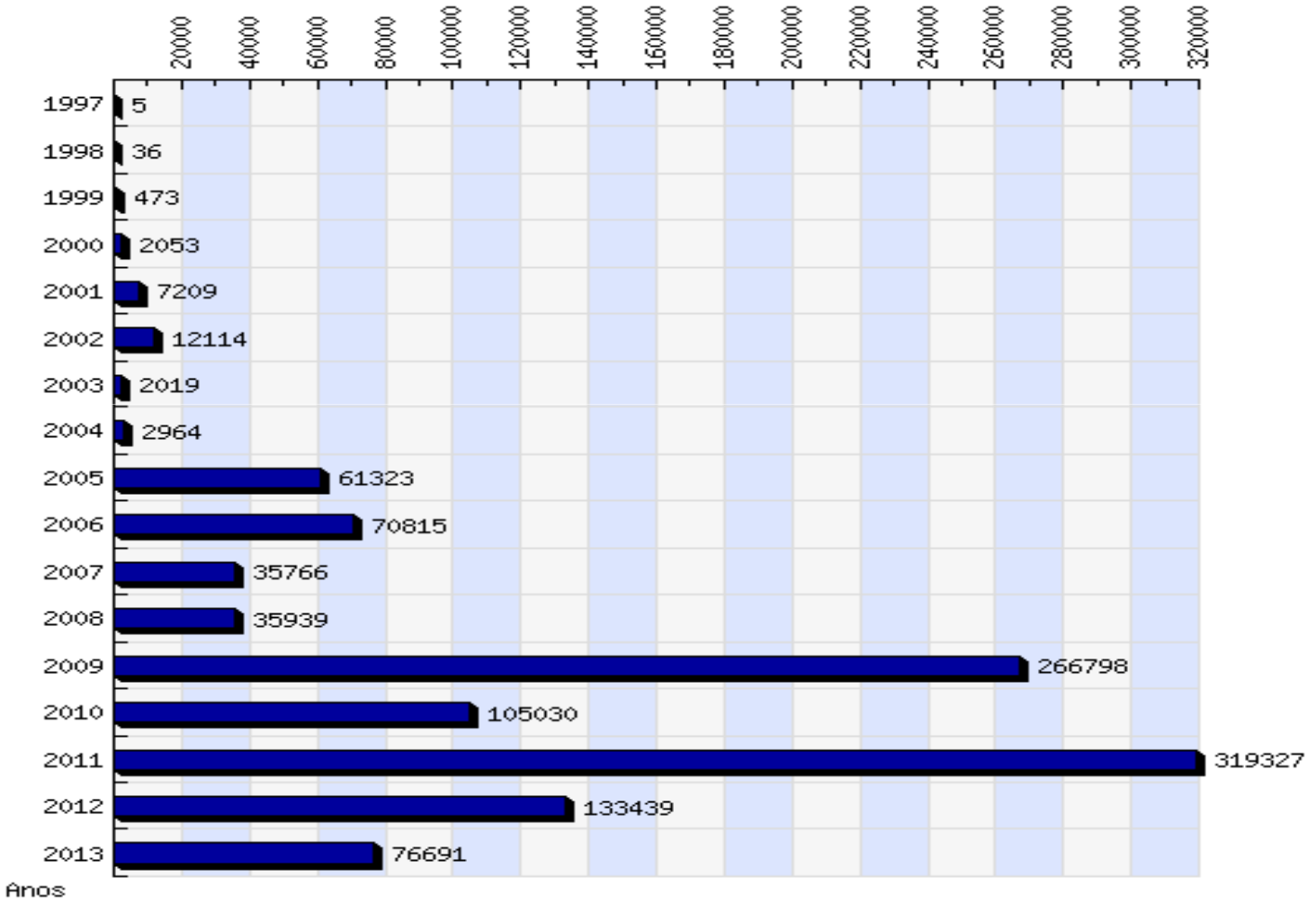
- Incidentes de segurança que envolvem o backbone da RNP – AS1916 e aproximadamente 19 clientes
  (AS1251, AS2715, AS2716, AS10412, AS10715, AS10881, AS11097, AS11156, AS11242, AS11751, AS13522, AS14553, AS19200, AS19611, AS19763, AS21506, AS21612, AS22819, AS28579)

- Conta **cais@cais.rnp.br**

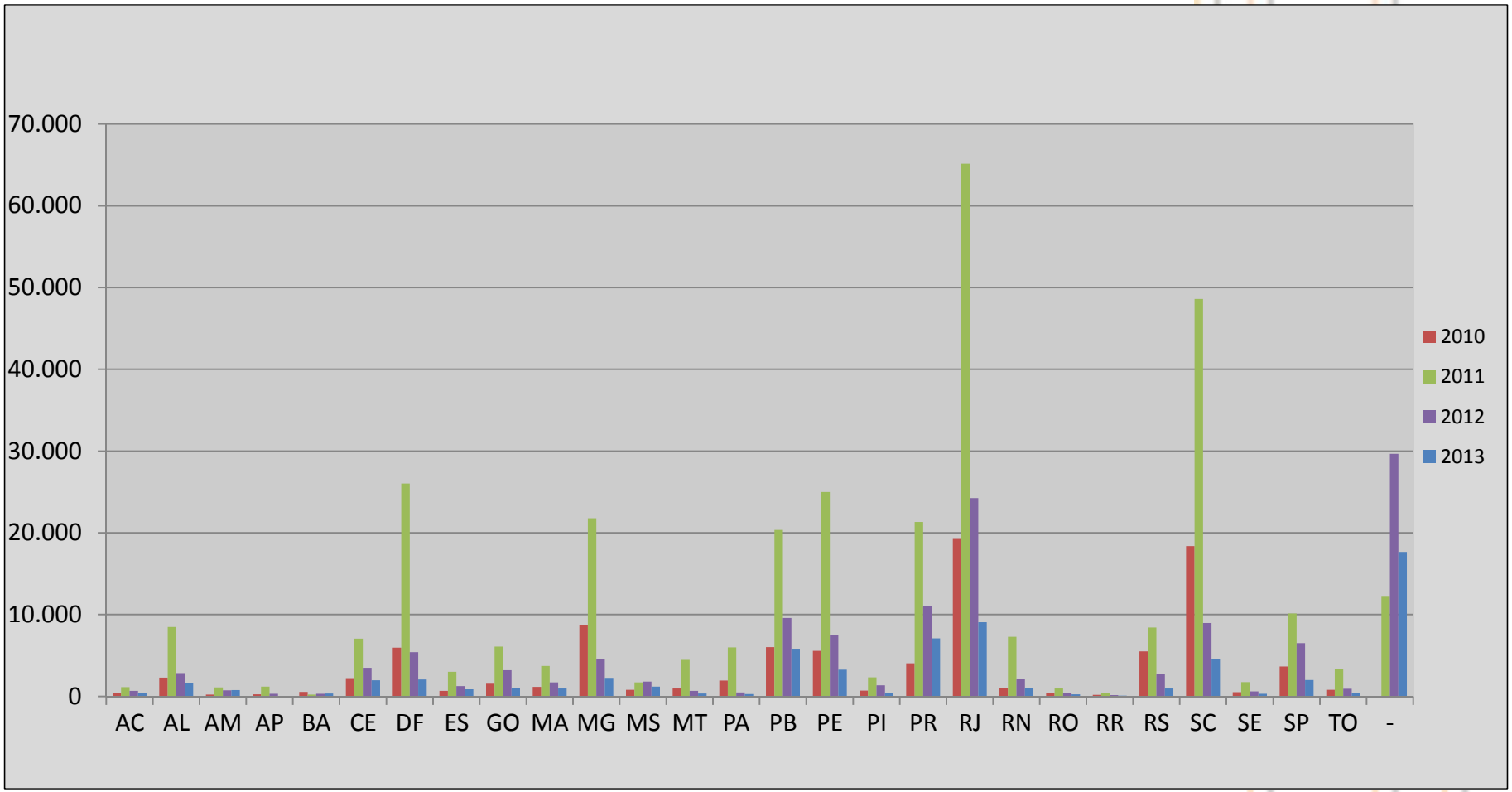
- Os incidentes são reportados por parceiros, CSIRTs, usuários, provedores ou são identificados pelo CAIS através dos sistemas de detecção de atividade maliciosa:

  * trocas de páginas (defacements)
  * botnets/malware
  * phishing
  * spam
  * sistemas comprometidos

# Incidentes notificados ao CAIS



# Número de incidentes por Estado



# Relatório Mensal de Incidentes

# Motivação para criação do Relatório

- Classificação dos incidentes pelo CAIS
- Número crescente de instituições utilizando backbone da RNP
- Aumento no número de incidentes tratados
- Número baixo de incidentes resolvidos
- Fornecer uma visão executiva sobre os incidentes nas instituições

# Objetivos

- Resolução de 30% dos incidentes notificados
- Redução no número de incidentes
- Fornecer um “mecanismo” para acompanhamento/melhoria dos incidentes da instituição
- Evidenciar a preocupação do CAIS em combater a atividade maliciosa na rede Ipê

# Desafios no desenvolvimento do Relatório

- Modificação nos templates de notificação
- Contabilização automática dos status dos incidentes
- Resposta das instituições recebidas em diferentes formatos
- Rotatividade de funcionários nas instituições clientes

# Soluções Encontradas

- Criação de diversos scripts pela equipe do CAIS
- Alteração nos templates de notificação
- Padronização das respostas dos incidentes
- Aproximação dos responsáveis técnicos dos PoPs

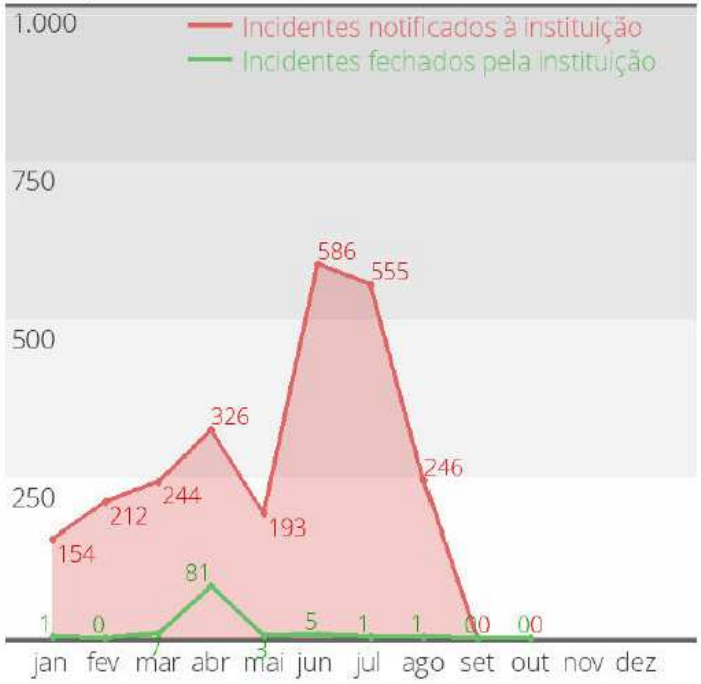
# Visão Geral

**Relatório Anual de Incidentes de Segurança**

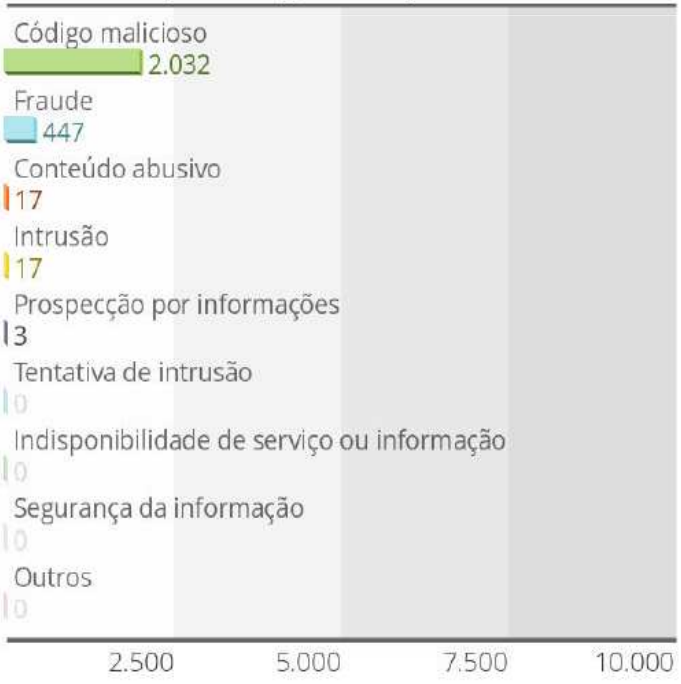
Instituição: **Universidade Federal de Santa Catarina – UFSC**
Período: **2013** (gerado em 10/10/2013)

Gestor: **Edison Tadeu Lopes Melo**
Contato de segurança: **Jaime**
PoP: **SC**

**Evolução de incidentes no ano**




**Incidentes por categoria no período**



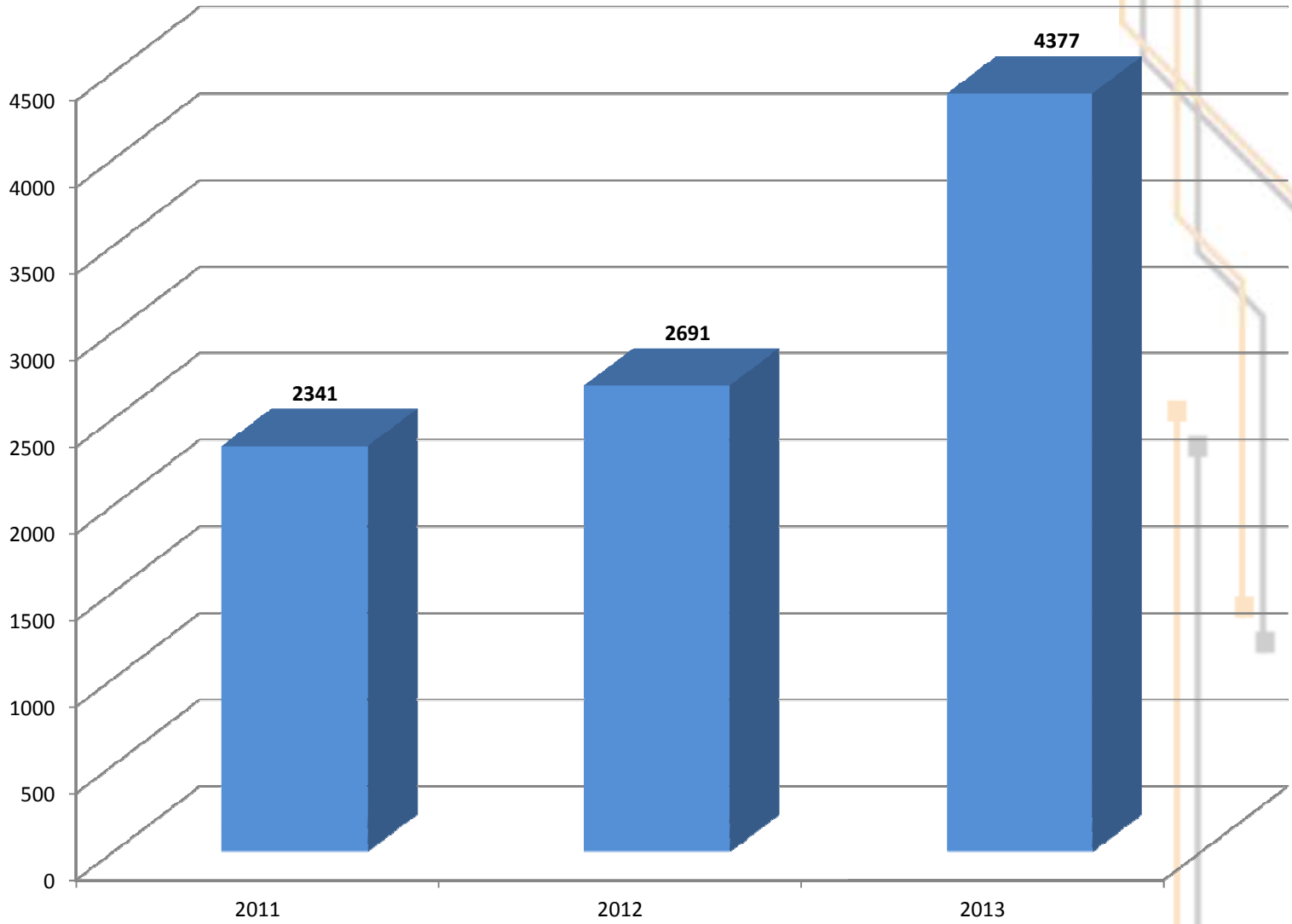

Posição no ranking

Incidentes notificados
6 de 371

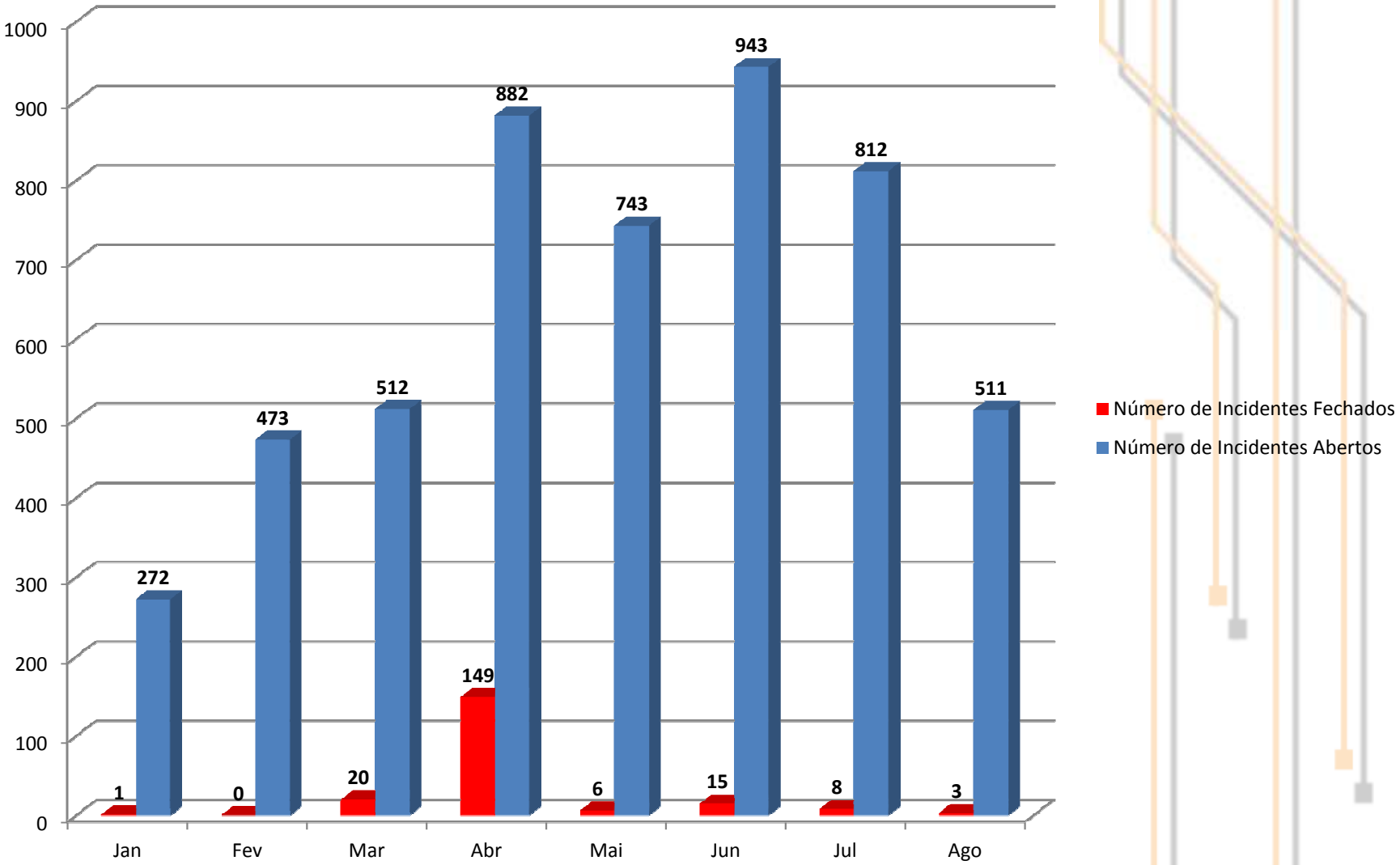
Incidentes fechados
3,93%

| TOP 10 IPs | Qtde. |
|---|---|
| 150.162.173.61 | 67 |
| 150.162.138.67 | 62 |
| 150.162.67.15 | 59 |
| 150.162.138.200 | 49 |
| 150.162.162.25 | 49 |
| 150.162.162.75 | 49 |
| 150.162.162.76 | 49 |
| 150.162.162.77 | 49 |
| 150.162.162.87 | 49 |
| 150.162.162.105 | 49 |

# Número de incidentes fechados Anualmente



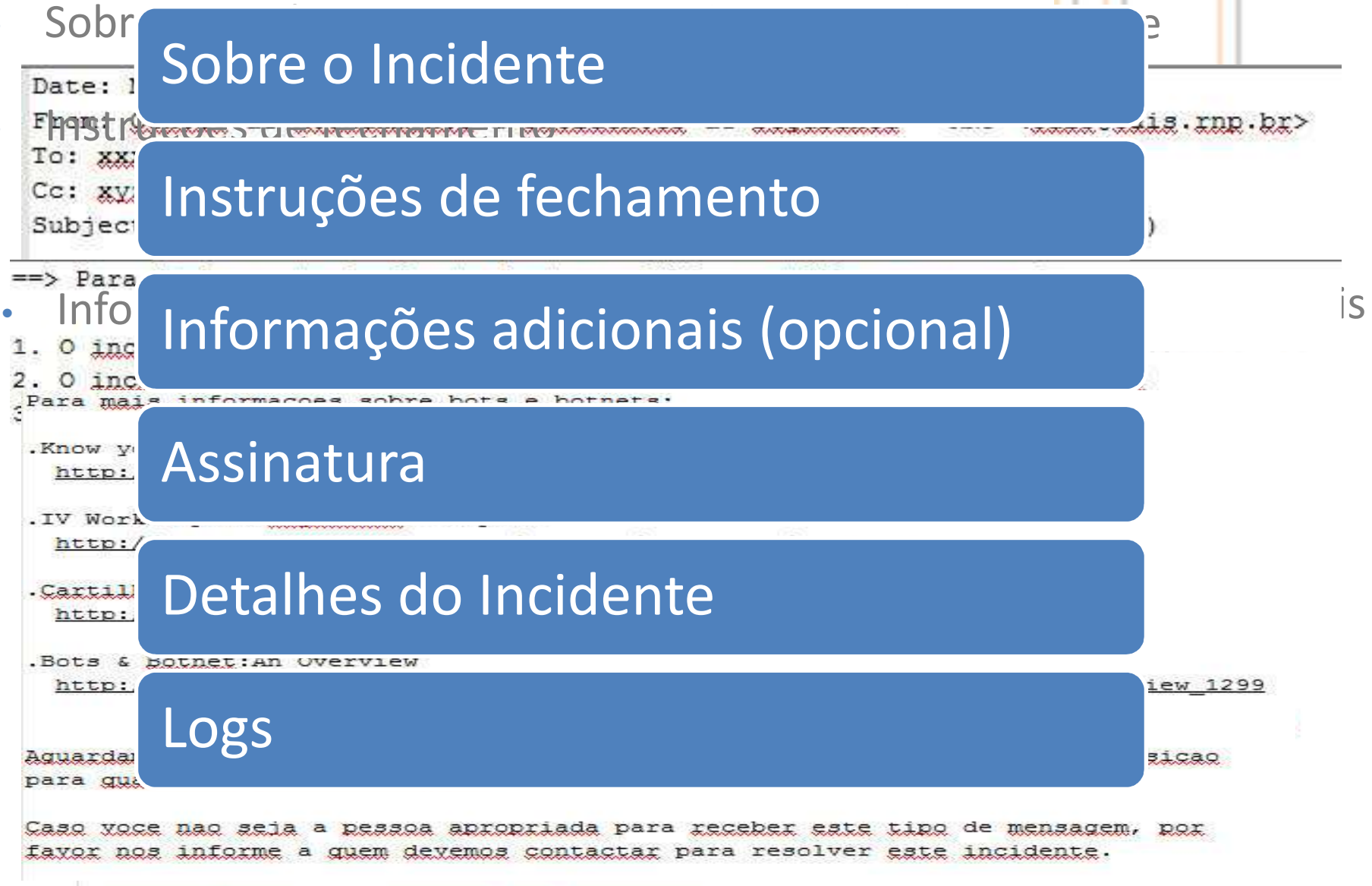
# Número de incidentes envolvendo clientes PoP-SC



# Notificações do CAIS

# Entendendo as notificações do CAIS

- Sobre o Incidente
- Instruções de fechamento
- Informações adicionais (opcional)
- Assinatura
- Detalhes do Incidente
- Logs



# Entendendo as notificações do CAIS

- Assinatura do CAIS

Atenciosamente,

Rildo Souza
CAIS/RNP

```
#####################################################################
#    CENTRO DE ATENDIMENTO A INCIDENTES DE SEGURANCA (CAIS)         #
#                                                                   #
```

Detalhes_do_Incidente:

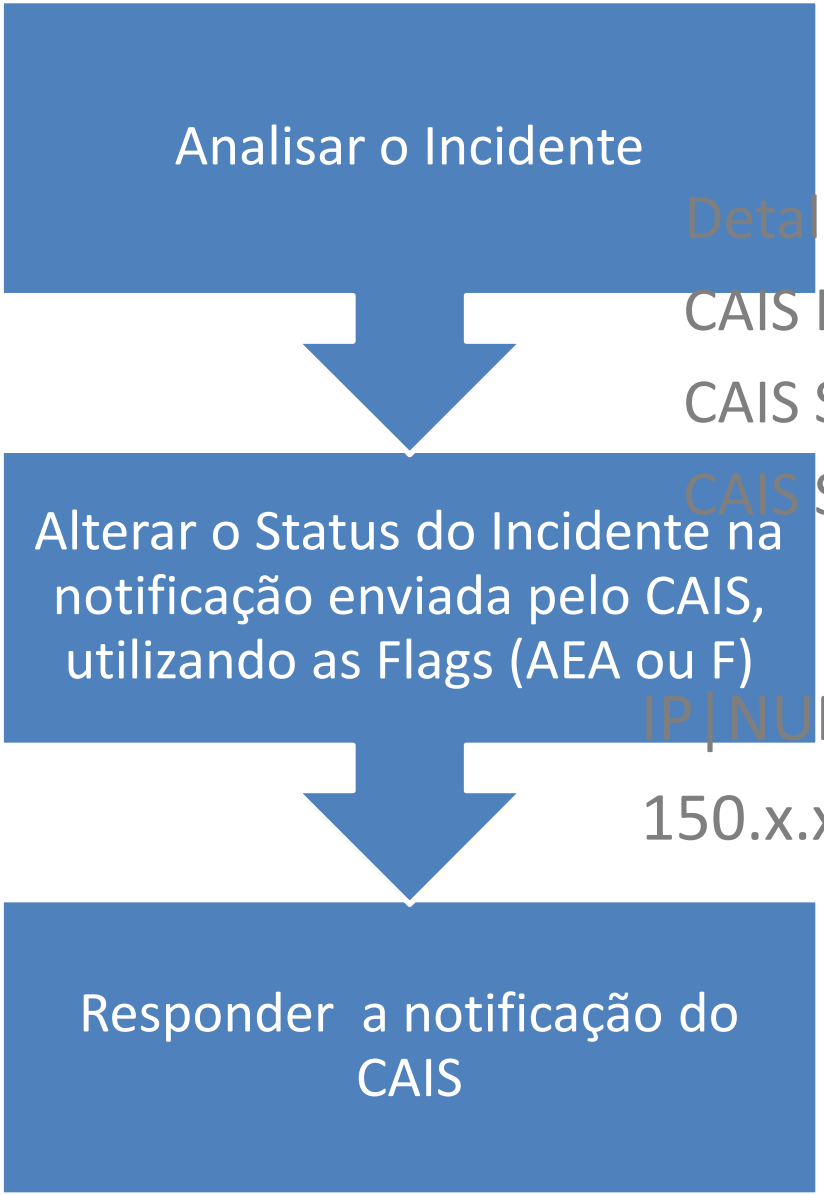
Data e hora UTC+0,IP do bot,Porta origem,ASN,Pais,Estado,Cidade,Hostname,IP_BlockList,UDP/TCP,Tipo de infeccao,URL de conexao,Agente HTTP,IP CC,Porta CC,ASN CC,Pais CC,DNS Reverso CC,
Nro de conexoes do bot,Conexao por proxy
"2013-10-06 23:35:08","x.y.z.w",50684,1916,"BR","RIO DE JANEIRO","RIO DE JANEIRO","h200137223134.xxx.br","udp","ZeroAccess",,,"68.226.196.56",16470,22773,"US",
"ip68-226-196-56.lf.br.cox.net",1,,,,

==========

Data e hora UTC+0,IP do bot,Porta origem,ASN,Pais,Estado,Cidade,Hostname,IP_BlockList,UDP/TCP,Tipo de infeccao,URL de conexao,Agente HTTP,IP CC,Porta CC,ASN CC,Pais CC,DNS Reverso CC,
Nro de conexoes do bot,Conexao por proxy
"2013-10-06 23:35:08","x.y.z.w",50684,1916,"BR","RIO DE JANEIRO","RIO DE JANEIRO","h200137223134.xxx.br","udp","ZeroAccess",,,"68.226.196.56",16470,22773,"US",
"ip68-226-196-56.lf.br.cox.net",1,,,,

==========

# Fechando um incidente – 1 MD5




Detalhes_do_Incidente:

CAIS Incidente ID:”MD5”

CAIS Status inicial:[ ANR ]

CAIS Status resposta:[ AEA ]

IP|NUMERO DO AS|DATA HORA(GMT 00:00)

150.x.x.x|1916|2013-09-29 12:17:03

# Fechando um incidente – N MD5s

Detalhes_do_Incidente:

CAIS Incidente ID:9e9908361f6fa91fb8e080a78cbc022a

CAIS Status inicial:[ ANR ]

CAIS Status resposta:[ AEA ]

IP|NUMERO DO AS|DATA HORA(GMT 00:00)|NOME DO AS

10.0.0.1|1916|2013-09-29 12:17:03|RNP

Detalhes_do_Incidente:

CAIS Incidente ID: 9f2589c984304a17c38e900e8a9a5c97

CAIS Status inicial:[ ANR ]

CAIS Status resposta:[ F ]

IP|NUMERO DO AS|DATA HORA(GMT 00:00)|NOME DO AS

10.0.0.2|1916|2013-09-30 15:10:45|RNP

# Relatório de Incidentes como instrumento de melhoria contínua

- Sensibilizar a Alta direção
- Definir prioridades (incidentes)
- Orientar investimentos(Recursos humanos, hardware)
- Identificar eventuais necessidades de capacitação

# Próximos Passos

- Implementar ajustes solicitados pelas instituições
- Levar aprendizado para o desenvolvimento de novo sistema
- Integrar relatórios com SGIS ( sistema em desenvolvimento )
- Realizar webconferes para ajudar os clientes

**Rildo Souza**

(rildo.souza@cais.rnp.br)

**Centro de Atendimento a Incidentes de Segurança**

(cais@cais.rnp.br)

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

redeIpê

RNP

Ministério da Cultura

Ministério da Saúde

Ministério da Educação

Ministério da Ciência, Tecnologia e Inovação

GOVERNO FEDERAL BRASIL PAÍS RICO É PAÍS SEM POBREZA