Melhorias no Tratamento de Incidentes através do Sistema de Gestão de Incidentes de Segurança(SGIS)

Rildo Antonio de Souza

Edilson Lima

Alan Santos

RNP

Ministério da **Cultura**

Ministério da **Saúde**

Ministério da **Educação**

Ministério da **Ciência, Tecnologia e Inovação**

GOVERNO FEDERAL BRASIL PÁTRIA EDUCADORA

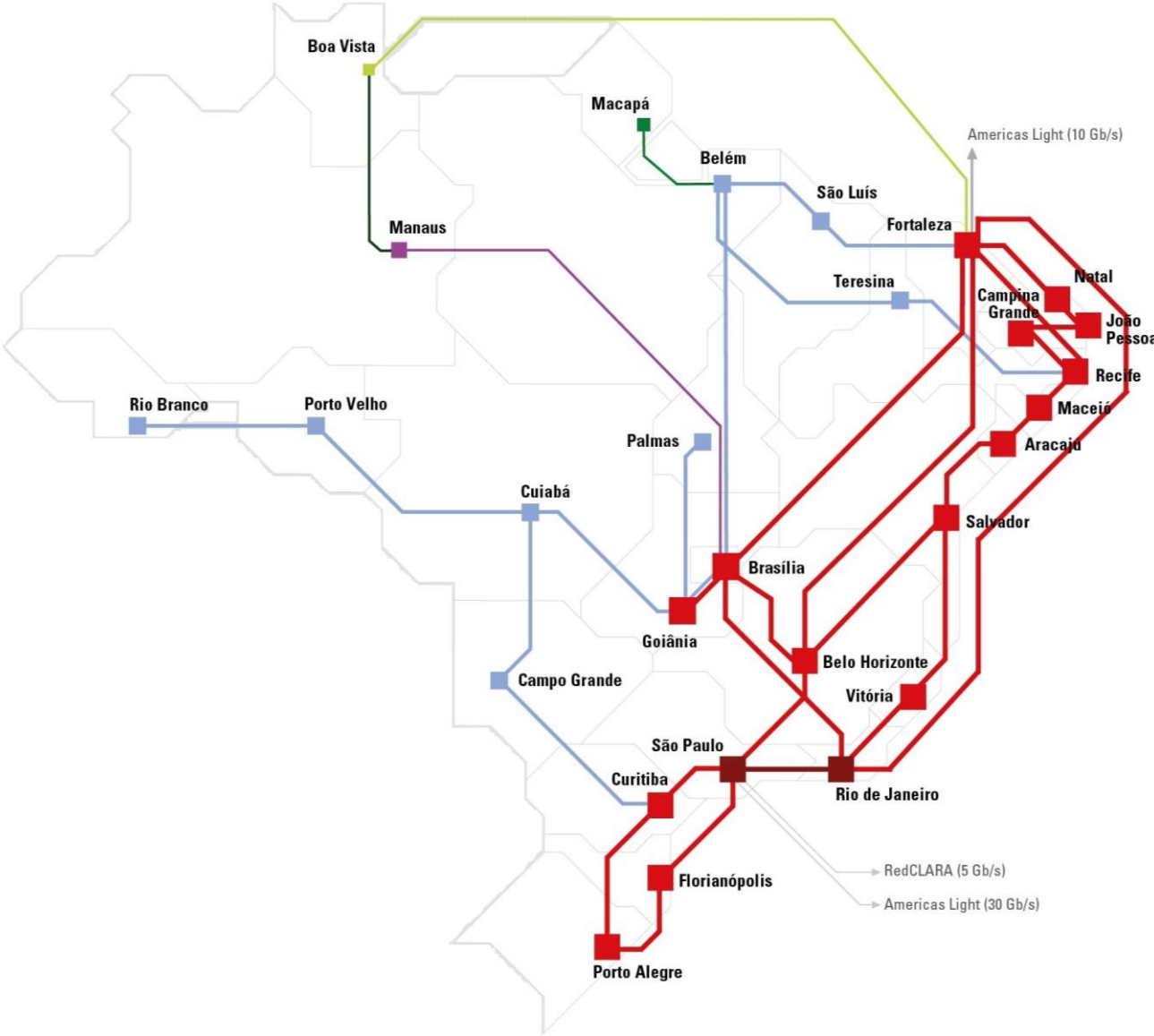
Agenda

- A RNP
- O CAIS
- Gestão de Incidentes de Segurança
- A Reestruturação no Tratamento de Incidentes
- O SGIS
- Resultados
- Apresentação da Ferramenta

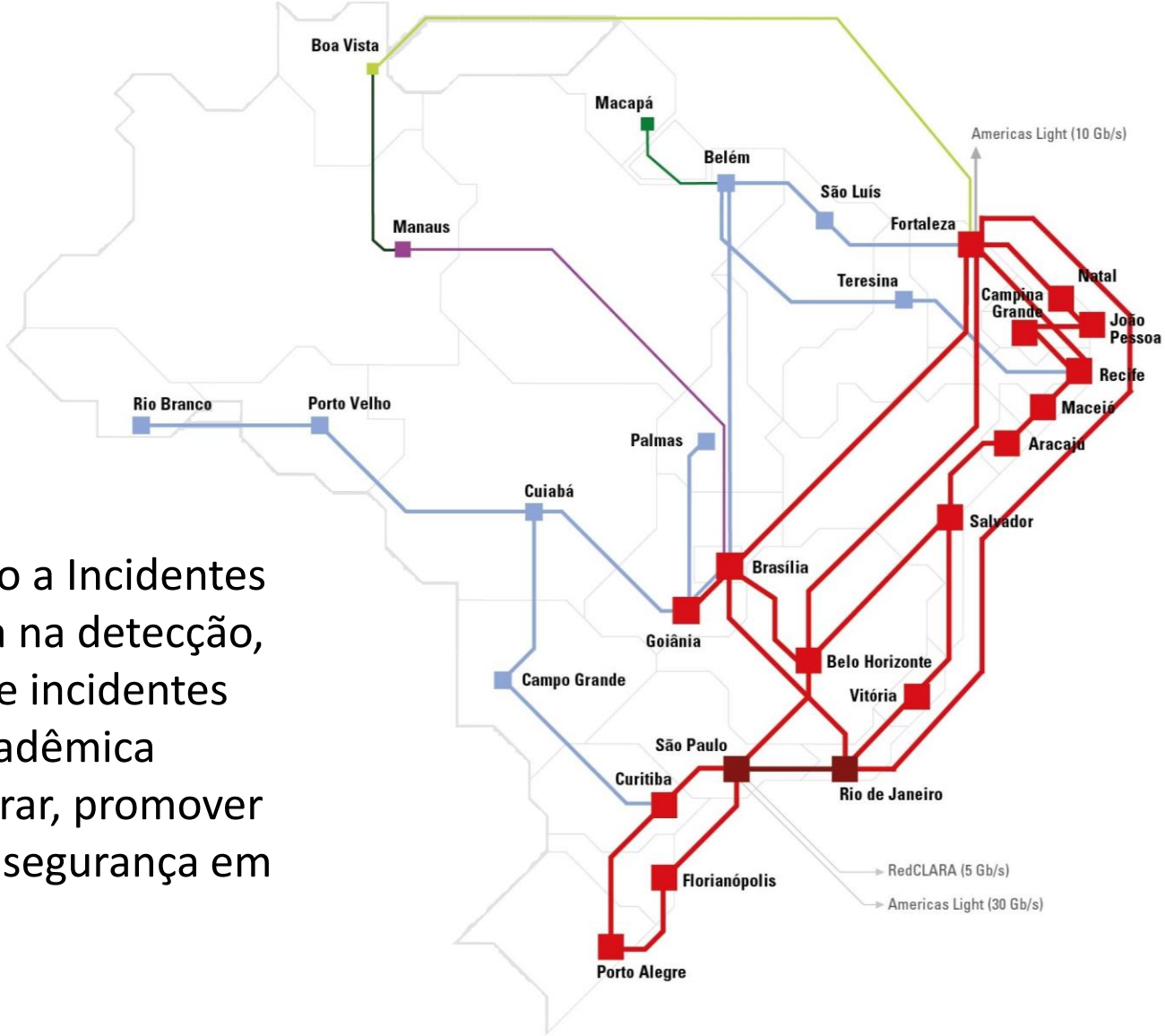
A RNP

27
PoPs

Cerca de
1.160
Instituições



O CAIS



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 .

Gestão de Incidentes de Segurança

- Papel de coordenação e suporte aos clientes
- Atuação nas unidades da RNP e no backbone
- 1 coordenador de área
- 3 analistas de segurança

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

- Incidentes reportados para e-mail 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

Tratamento de Incidentes no CAIS

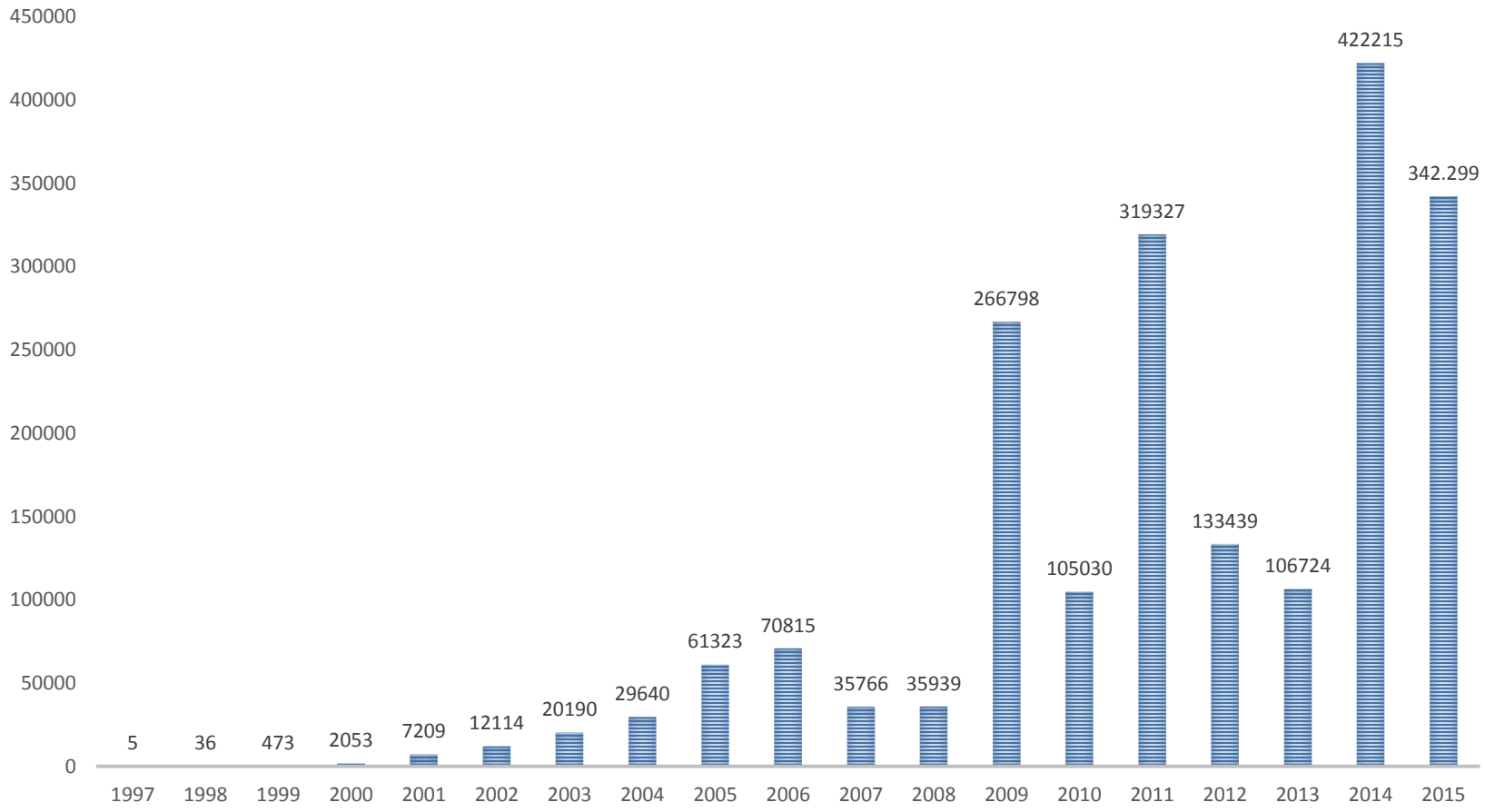
- Durante os oito primeiros meses de 2015, o CAIS tratou mais 342.000 mil notificações de incidentes/vulnerabilidades;

- Durante este período foram tratados cerca de 80 incidentes relacionados a negação de serviço (DoS);

- Monitoramento de eventos críticos relacionados ao Ministério da Educação (ex.: Sisu);

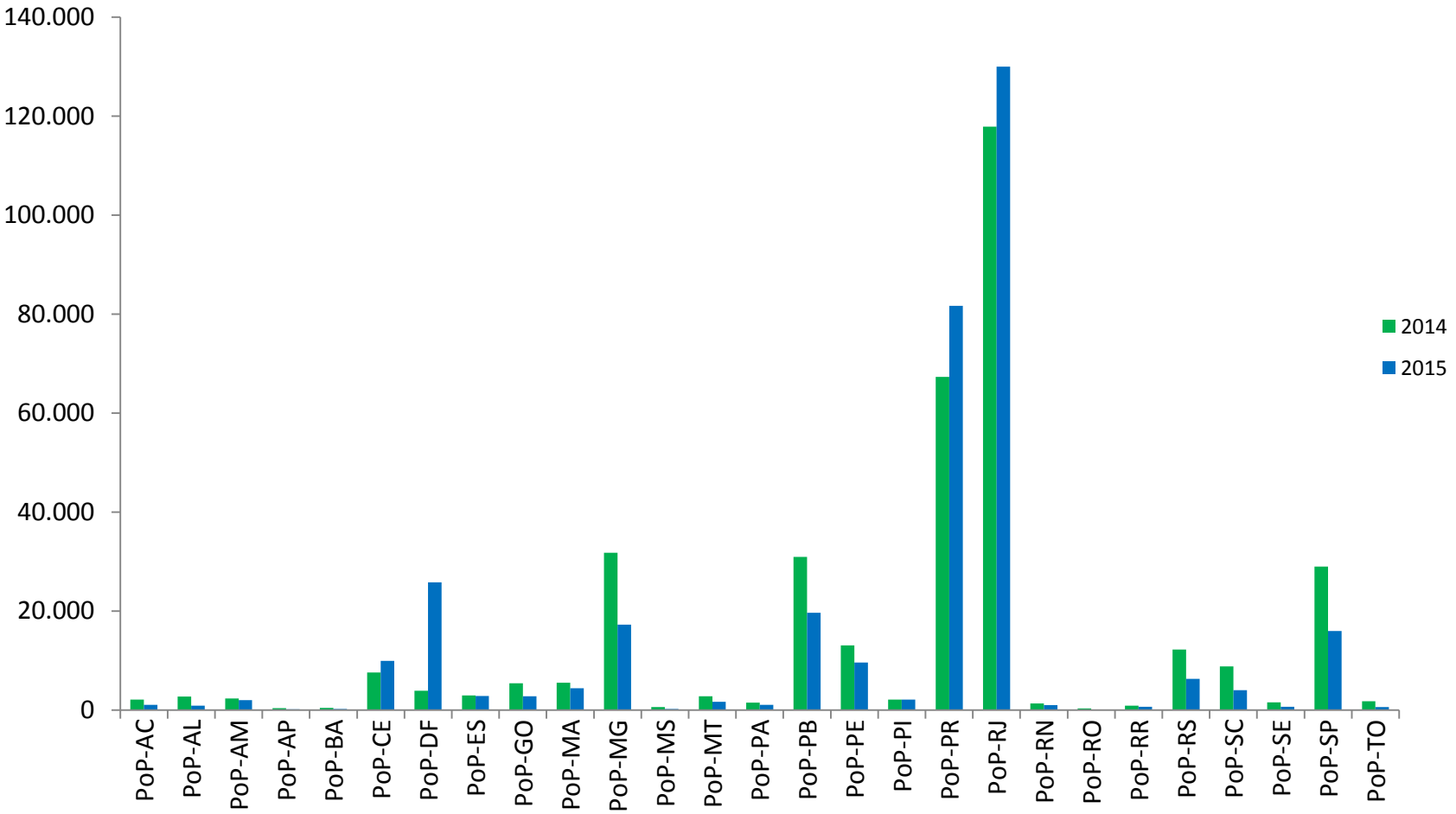
http://www.rnp.br/servicos/seguranca/tratamento-incidentes/estatisticas
http://www.brasil.gov.br/ciencia-e-tecnologia/2015/01/rnp-participa-da-operacao-de-monitoramento-do-sisu

Estatísticas Anuais de Incidentes/Vulnerabilidades

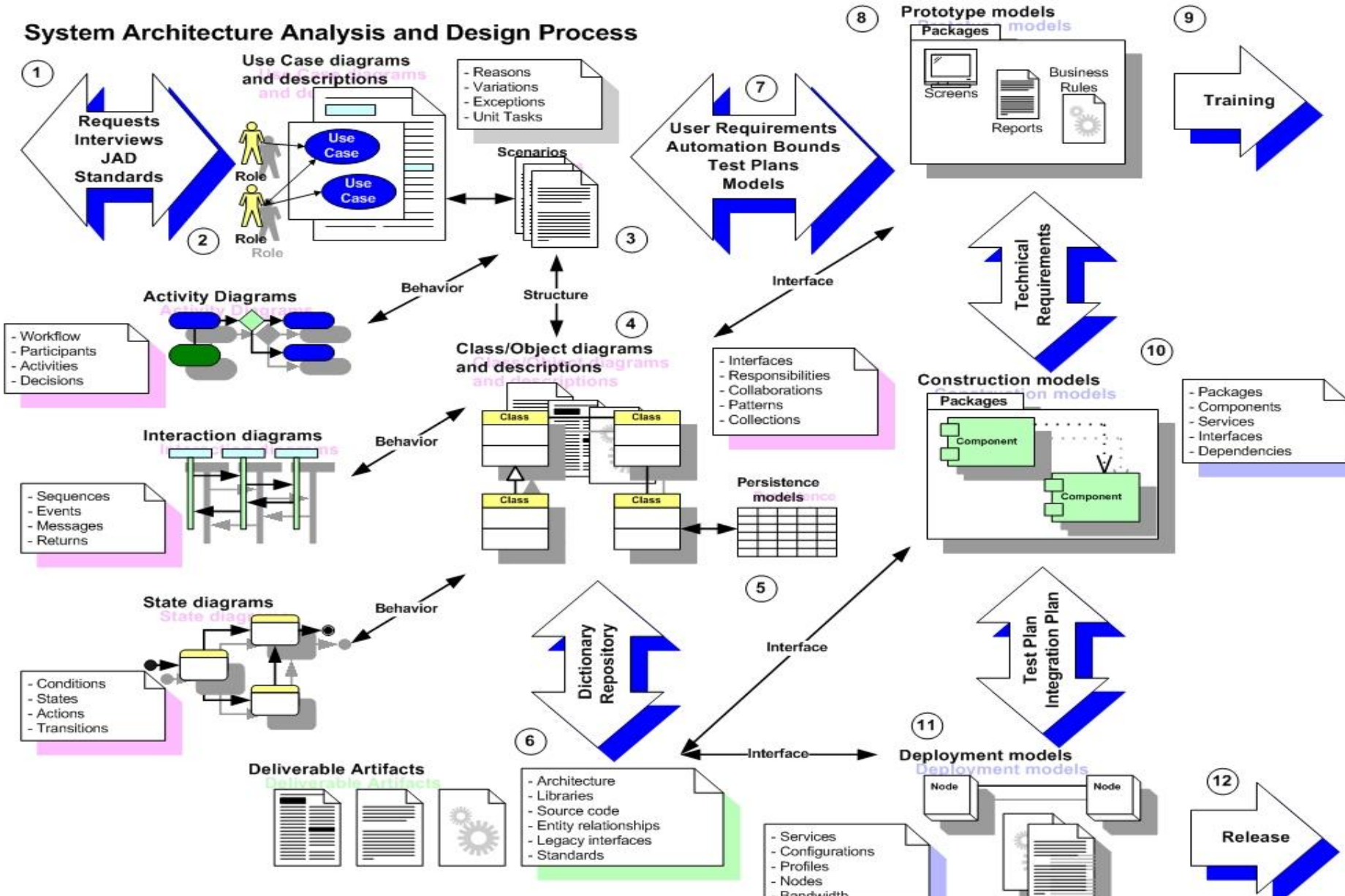


* Dados até 31/08

Número de Notificações por Estado



Antes do SGIS (Sistema Antigo)



Motivação

- Processo de tratamento de incidentes estabelecido
- Número crescente de instituições utilizando backbone da RNP
- Baixo número de incidentes solucionados
- Ferramenta não era escalável
- Fornecer uma ampla visão sobre os incidentes nas instituições
- Carência de relatórios mais detalhados e on-line
- Controle de status dos incidentes por flags

Objetivos

- Aumentar a porcentagem de incidentes resolvidos
- Reduzir o número de incidentes nas instituições
- Fornecer uma ferramenta web para acompanhamento/resolução dos incidentes da instituição
- Gerar de indicadores de apoio a criação de políticas de segurança

Desafios

- Criar um sistema para atender ambientes heterogêneos
- Permitir integração com ferramentas internas desenvolvidas pelas instituições
- Fomentar o compartilhamento de conhecimento entre as instituições
- Lidar com a alta rotatividade de funcionários nas instituições clientes

Proposta

- Criação de um sistema que atendesse todas as organizações usuárias na gestão dos incidentes de segurança da Rede Ipê, de forma eficaz e coordenada.

- Um sistema que permitisse o acompanhamento e análise de incidentes, a redução do custo operacional e o apoio na tomada de decisões estratégicas de segurança.

Sistema Atual

CAIS

- Detecção
- Triagem
- Notificação
- Suporte
- Gestão

Organização Usuária

- Mitigação
- Resolução
- Resposta
- Controle

Sistema de Gestão de Incidentes

Principais Recursos

- Sistema disponível para todas as Organizações Usuárias
- Facilidade no tratamento de incidentes
- Uso de certificados digitais
- Informações detalhadas sobre origem e destino dos incidentes

Mais que um sistema de encerramento incidentes, é uma ferramenta de gestão.

Concessão de acessos baseados em Cadeia de Confiança.

Sistema de acesso restrito aos profissionais que participam do processo.

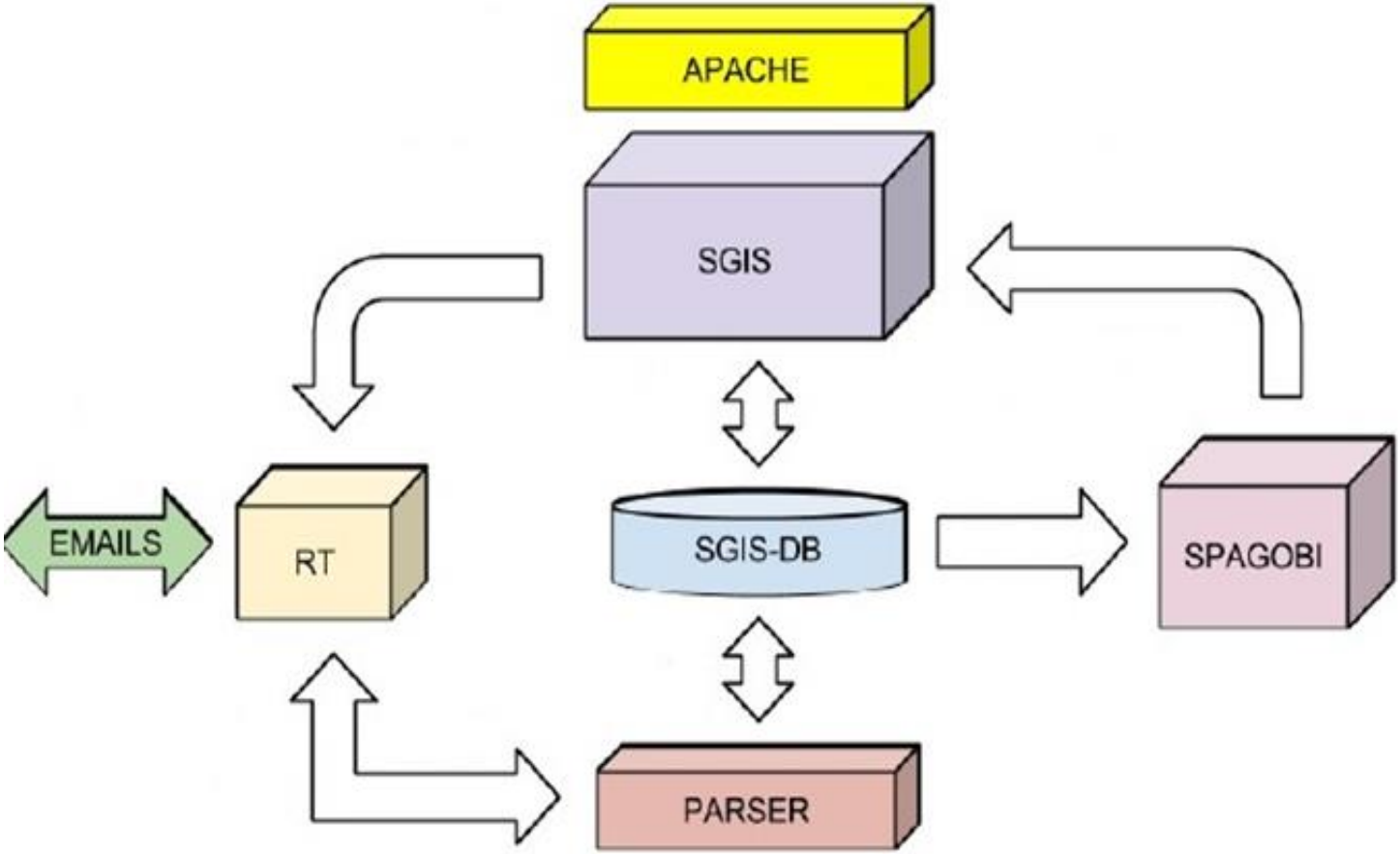
Perfis do Sistema

- Perfil A (Instituições): Visualizar Relatórios, Visualização de Incidentes, Encerramento de Incidentes Individuais e Acesso Base de Conhecimento (Wiki)

- Perfil B (Instituições) : Configurações de redes, contatos, permissões, Criação e Remoção de Instituições, Cadastro de novos Usuários e Encerramento de Incidentes em Lote e todas ações do Perfil A.

- Perfil C (RNP - Superuser) : Visualização Global de Incidentes e Relatórios, Criação de Grupos de Organizações, Criação de Parsers, Revisão e Aprovação de Usuários e todas as ações do Perfil A e B.

Estrutura do Sistema SGIS



RESULTADOS

O SGIS, 06 meses de uso...

- Tratamento de notificações duplicadas

$$\text{if} \qquad d^*(f,g) = \int_a^b \left| f(t) - g(t)\,\mathrm{d}t \right| < \delta$$

$$\text{then} \quad \left| \int_a^b f(t) - g(t)\,\mathrm{d}t \right| = \left| \lim_{n\to\infty} \sum_{i=1}^{n} M_i(t_i - t_{i-1}) \right| \leq$$

$$\text{if} \qquad d^*(f,g) = \int_a^b \left| f(t) - g(t)\,\mathrm{d}t \right| < \delta$$

$$\text{then} \quad \left| \int_a^b f(t) - g(t)\,\mathrm{d}t \right| = \left| \lim_{n\to\infty} \sum_{i=1}^{n} M_i(t_i - t_{i-1}) \right| \leq \quad - g(t)\,\mathrm{d}t \Big| < \delta = \varepsilon$$

$$\lim_{n\to\infty} \sum_{i=1}^{n} \left| M_i(t_i - t_{i-1}) \right| = \int_a^b \left| f(t) - g(t)\,\mathrm{d}t \right| < \delta = \varepsilon$$

- Interface de acesso para as instituições

O SGIS, 06 meses de uso...

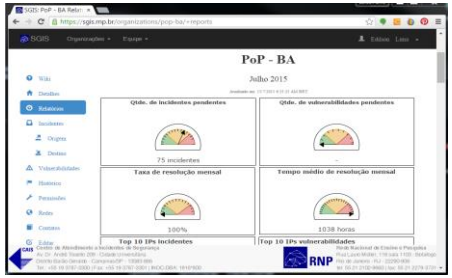
Principais benefícios

- Perfis de acesso por função
- Indicadores e Relatórios gerenciais on-line
- Envio de notificações para os clientes com arquivo em anexo baseado no padrão IODEF
- Ferramenta colaborativa (wiki)

O SGIS, 06 meses de uso...

Principais Números

909 Instituições



1 Sistema

218 contatos

INCIDENT REPORTING

342.299

Notificações de Incidentes/Vulnerabilidades

1116 Usuários

Apresentação da Ferramenta

Próximos Passos

- Aumentar a utilização do sistema
- Aumentar com outras fontes de notificações
- Melhorar a base de conhecimento do sistema
- Melhorar os relatórios gerenciais
- Melhorar o processo de gerenciamento de redes
- Integrar com CAFe(Certificados Digitais)

Dúvidas

Rildo Souza – rildo.souza@rnp.br

Alan Santos – alan.santos@rnp.br

Edilson Lima – edilson.lima@rnp.br

RNP

Ministério da
Cultura

Ministério da
Saúde

Ministério da
Educação

Ministério da
Ciência, Tecnologia e Inovação

GOVERNO FEDERAL
BRASIL
PÁTRIA EDUCADORA