CAIS: CSIRT da Rede Acadêmica Brasileira

V WORKSHOP do PoP-RS

Porto Alegre, RS

Brasil

Outubro/2014

CAIS

RNP

Ministério da **Cultura**

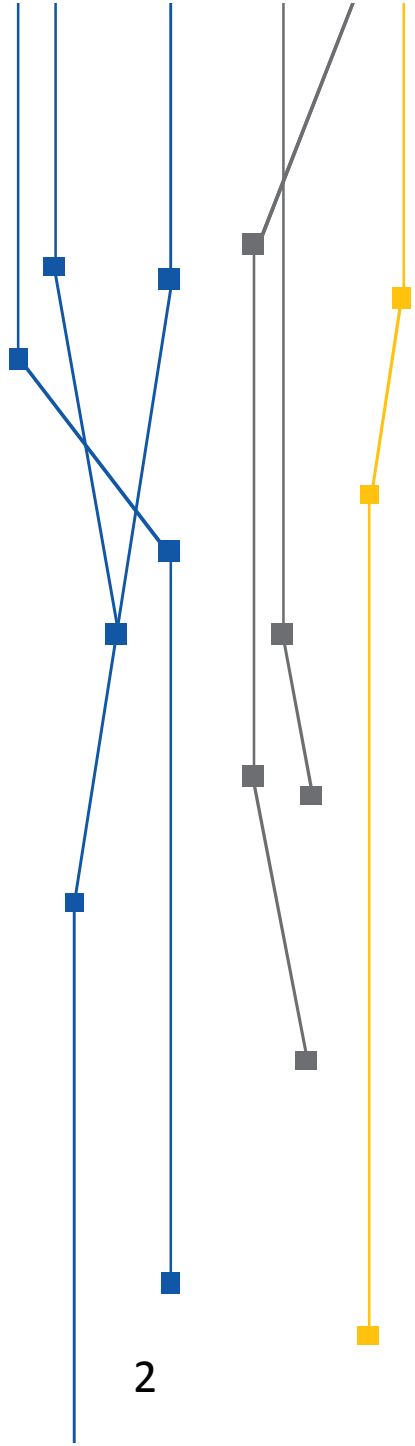
Ministério da **Saúde**

Ministério da **Educação**

Ministério da **Ciência, Tecnologia e Inovação**

Agenda

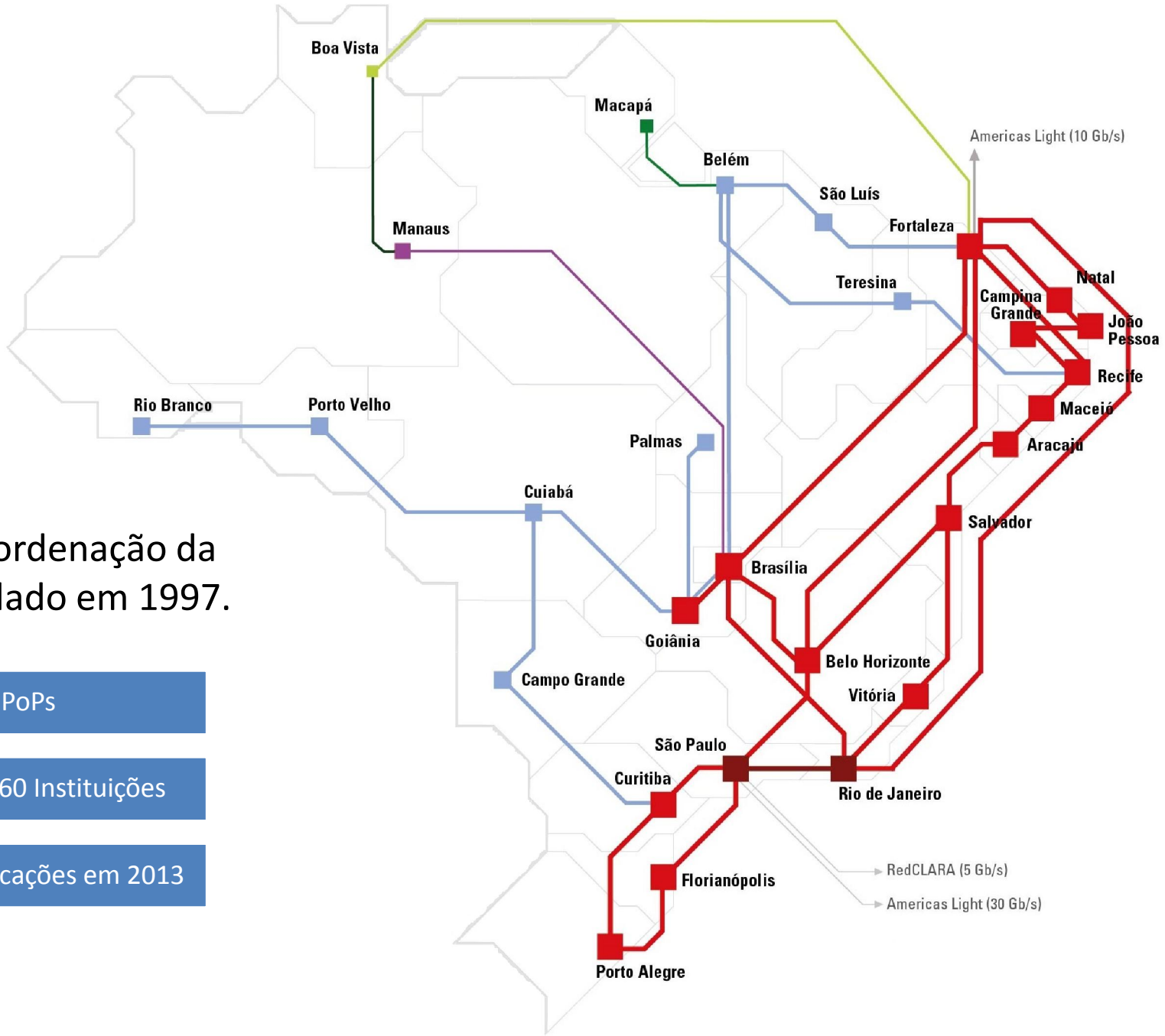
- Sobre o CAIS
- Ataque de Negação de Serviço na RNP: Detecção e Mitigação
- SGIS - O Novo Sistema de Gestão de Incidentes de Segurança



CAIS

O CSIRT de coordenação da Rede Ipê, fundado em 1997.

- 27 PoPs
- Cerca de 1.160 Instituições
- 106.724 notificações em 2013



Ataques de Negação de serviço: Detecção e mitigação

RNP

Ministério da **Cultura**

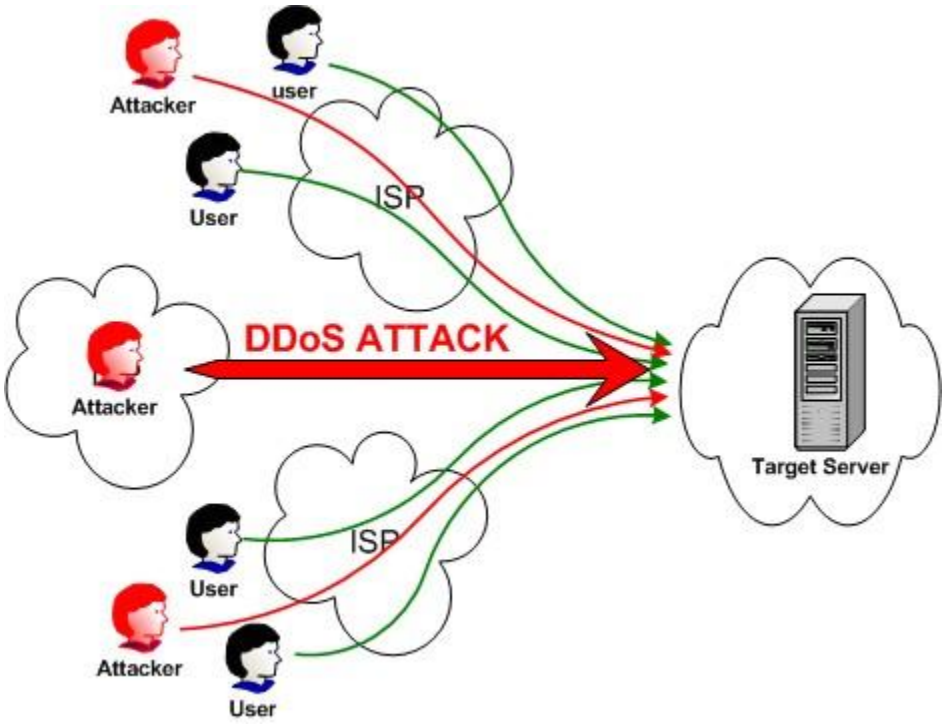
Ministério da **Saúde**

Ministério da **Educação**

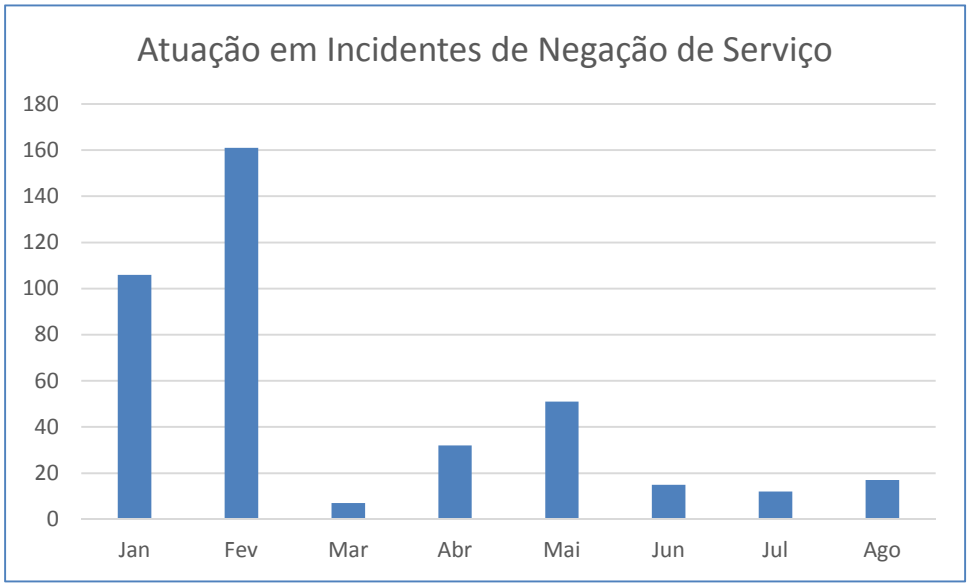
Ministério da **Ciência, Tecnologia e Inovação**

Ataques de Negação de Serviço

Vários acessos efetuados de forma simultânea.



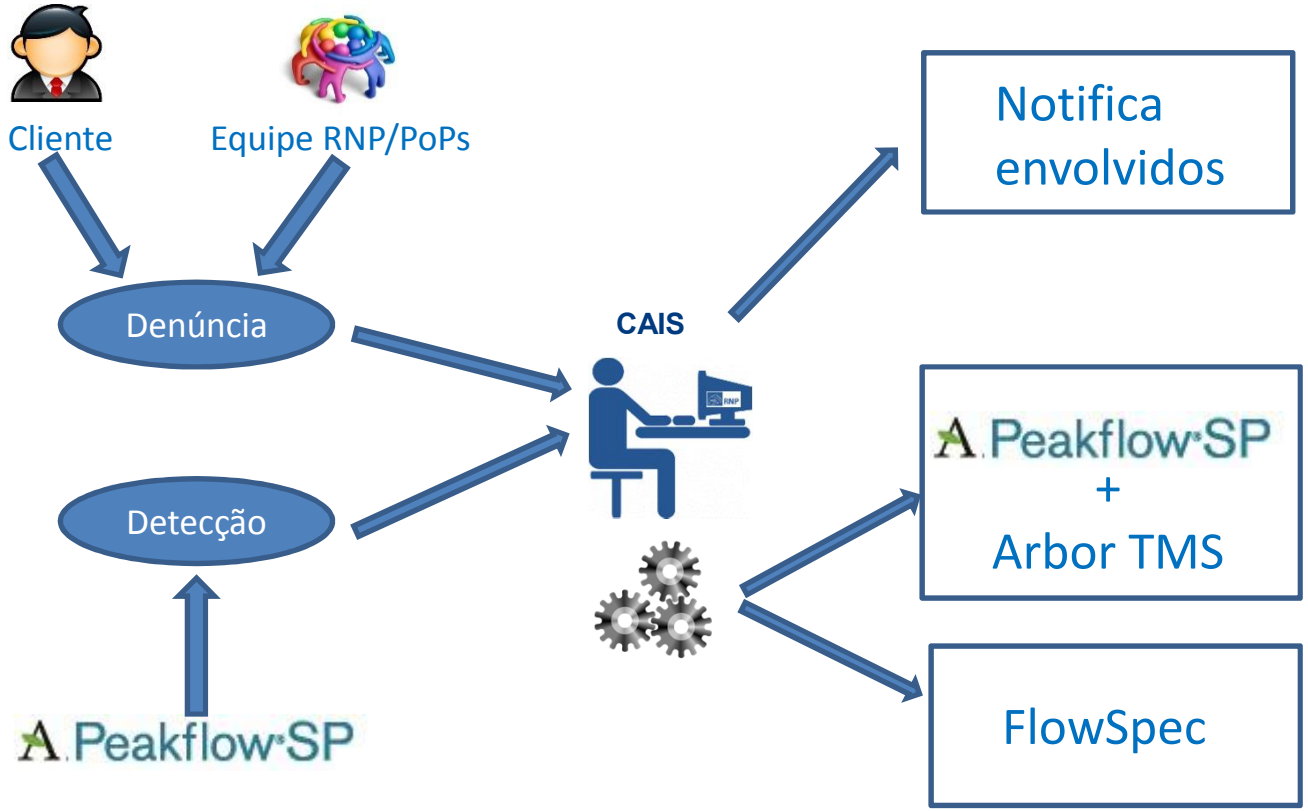
Cenário atual de atuação em ataques DDOS



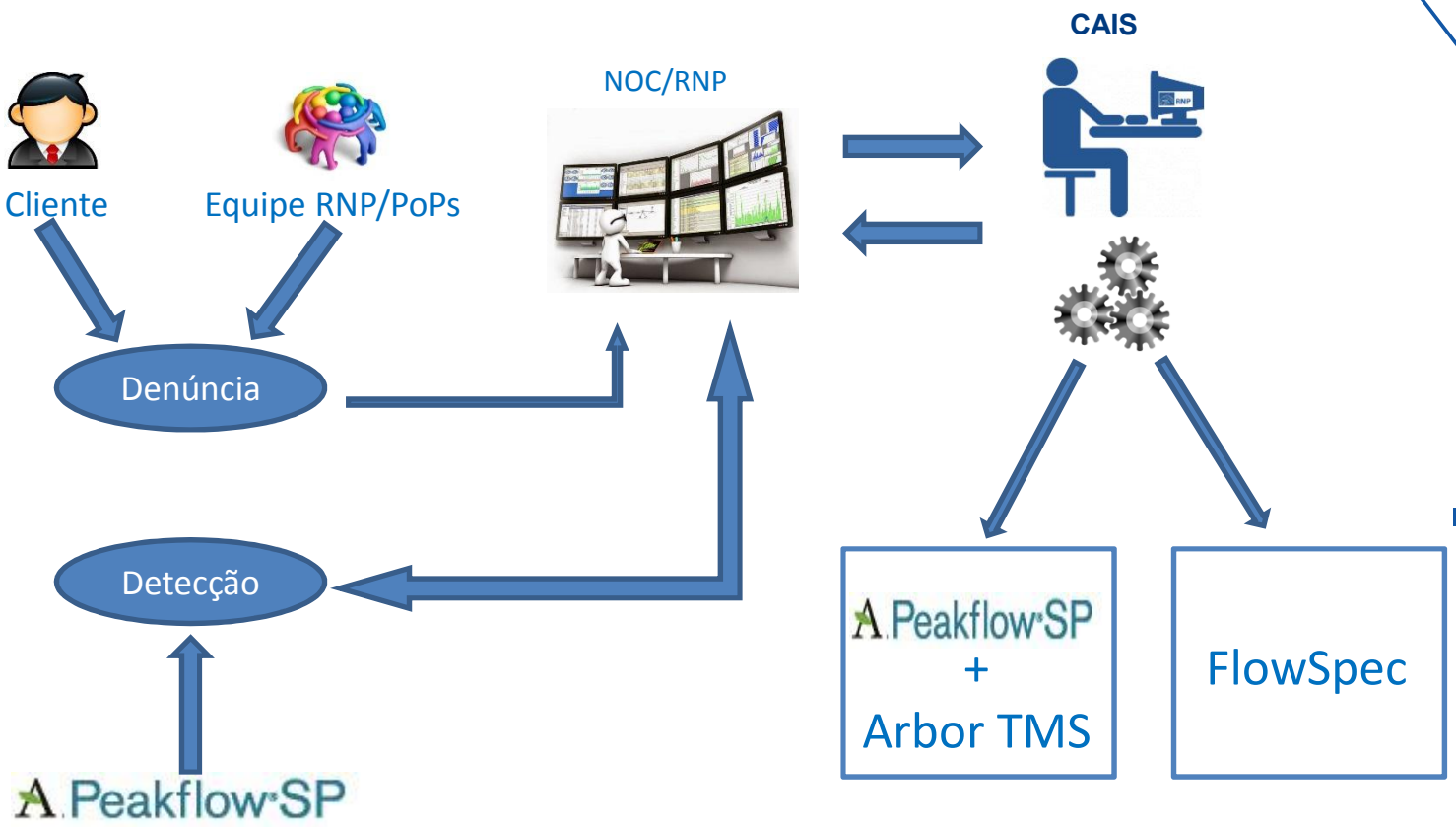
Dificuldades

- Natureza dos ataques
- Variedades de ataques
- Clientes com poucos mecanismos de detecção
- Erros na mitigação podem ser mais impactantes que o próprio ataque

Macro-processo para tratamento de incidentes DDOS (Horário comercial)



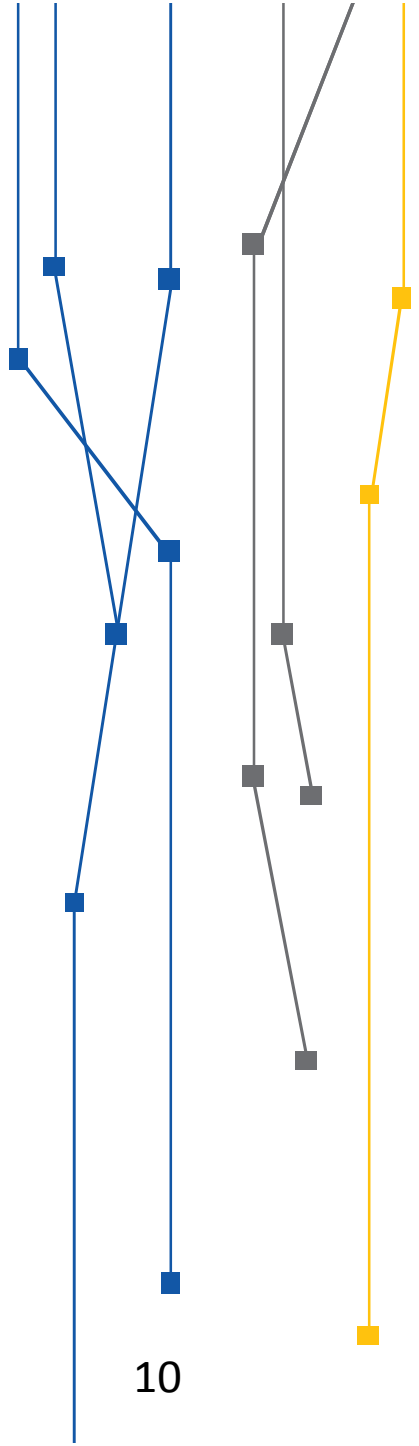
Macro-processo para tratamento de incidentes DDOS (Regime extraordinário)



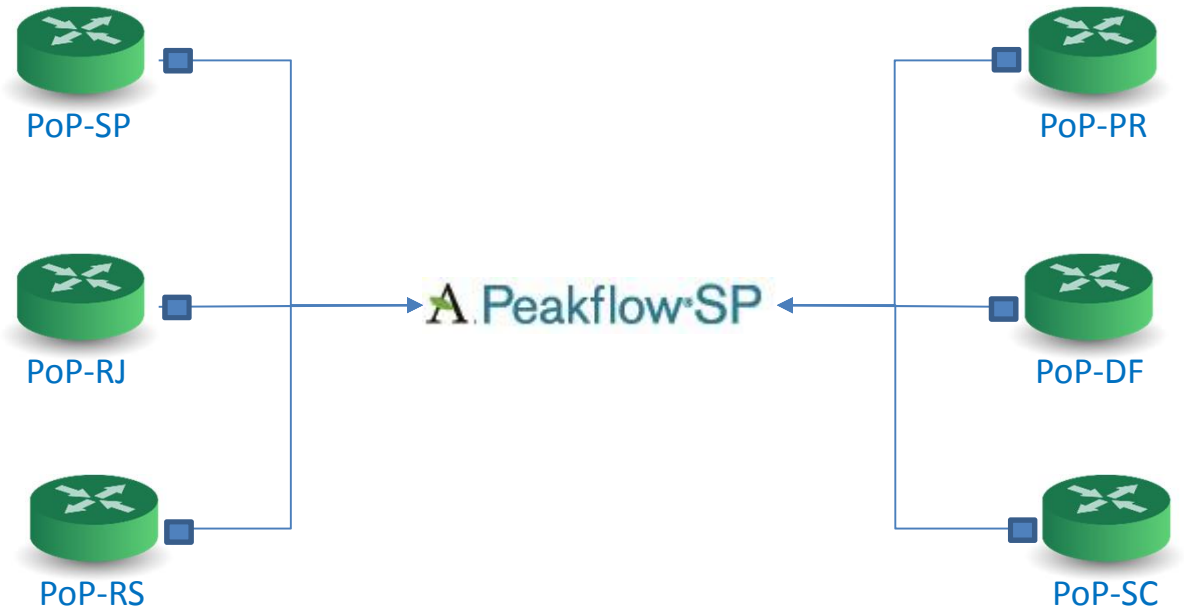
Ferramenta de detecção

Peakflow SP

- Ferramenta da Arbor
- Baseada em coleta de Flows por amostragem
- Ferramenta passiva e transparente

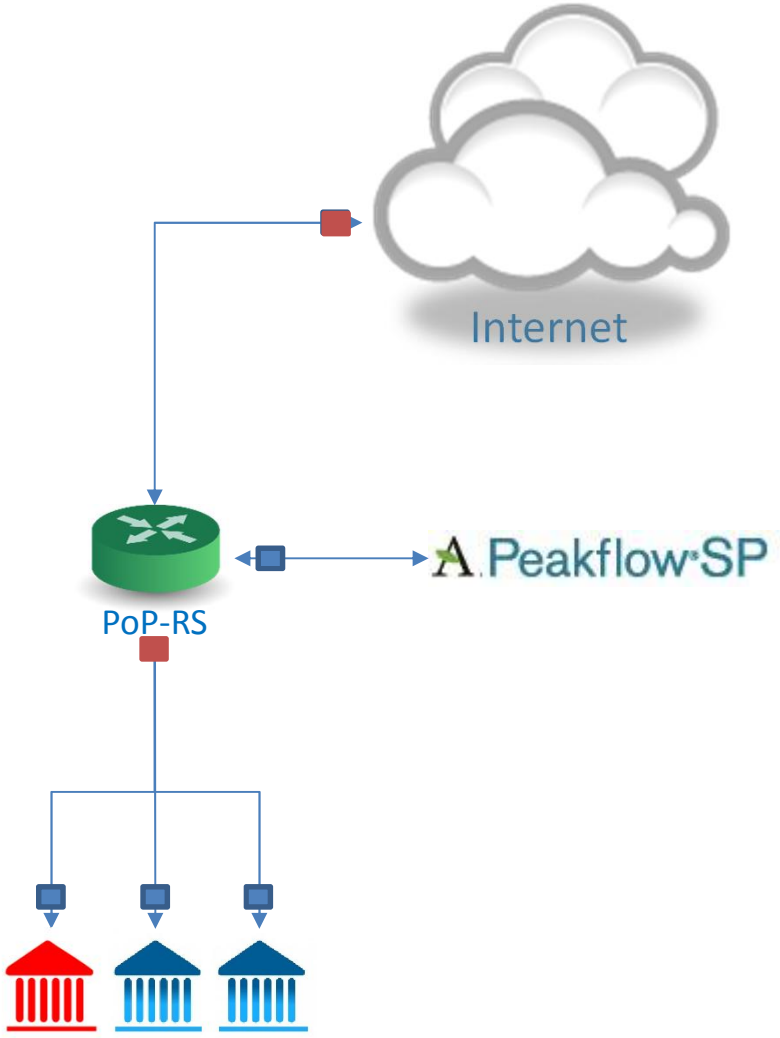


Ferramenta de detecção



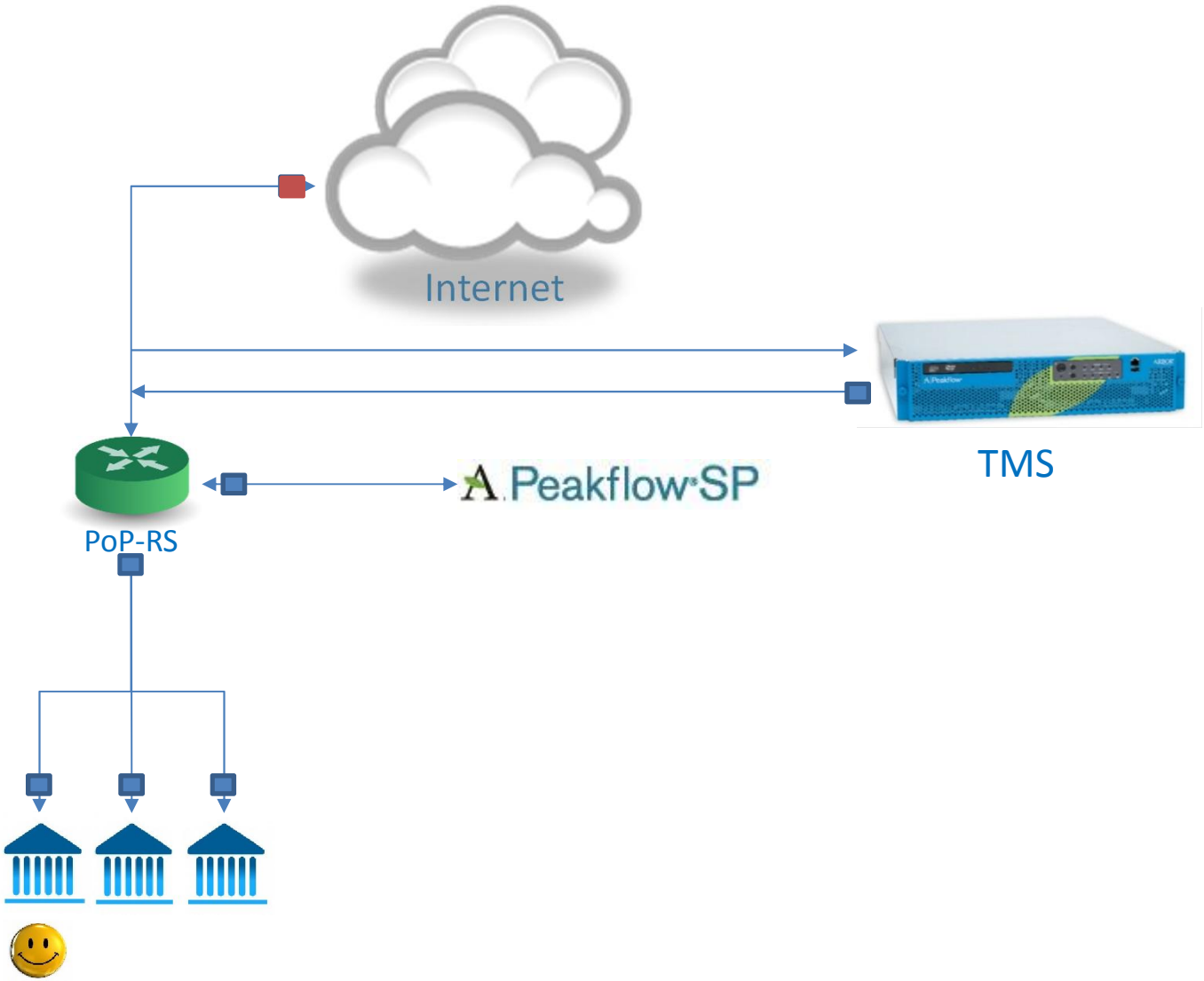
Taxa de amostragem: 1/1000

Ferramenta de detecção

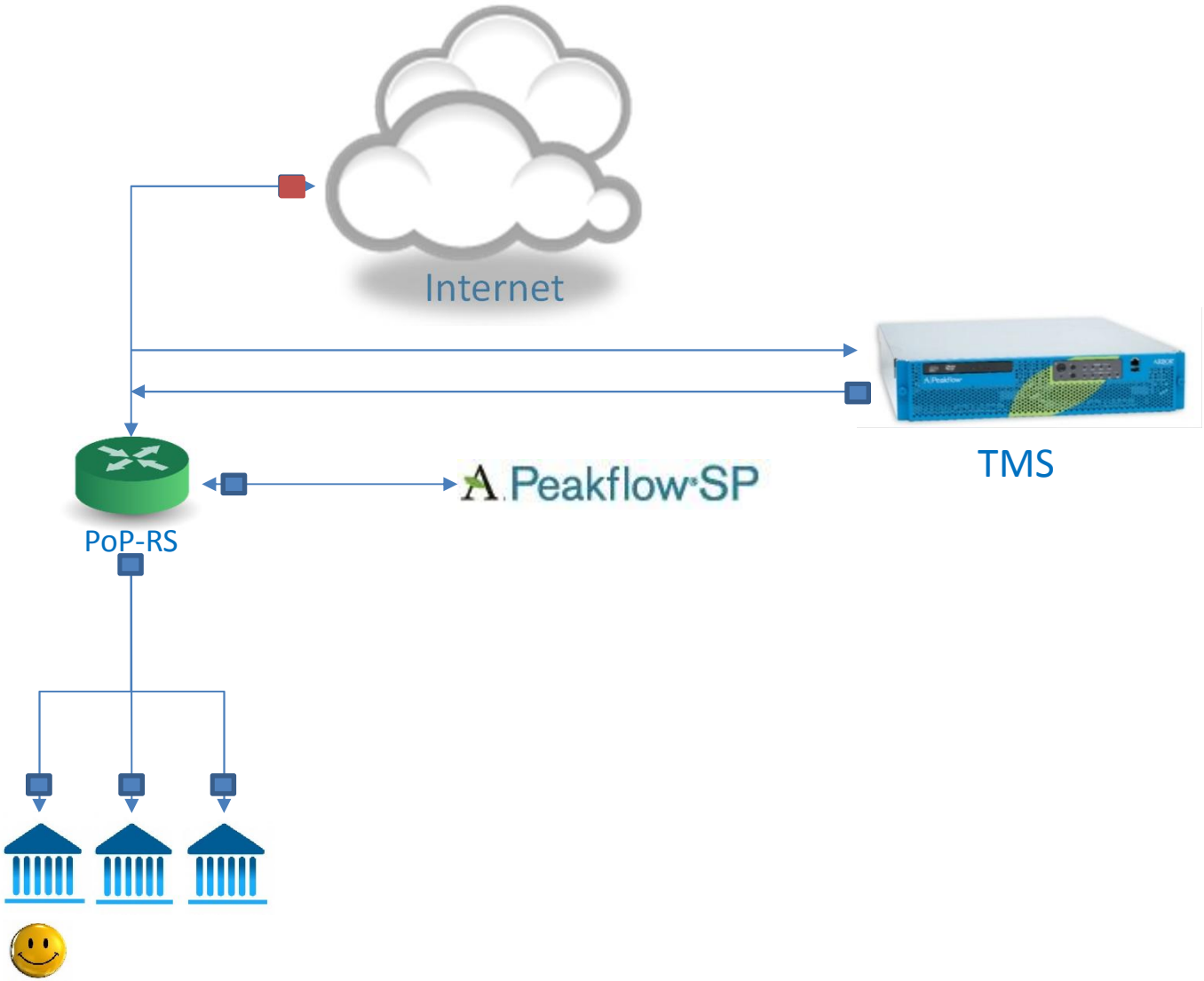


- Baseline de tráfego
- Pacotes Mal formados
- TCP SYN
- Características suspeitas

Ferramenta de Mitigação: TMS

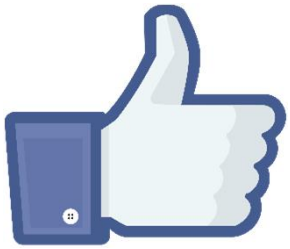


Ferramenta de Mitigação: TMS



Ferramenta de Mitigação:
TMS - Vantagens

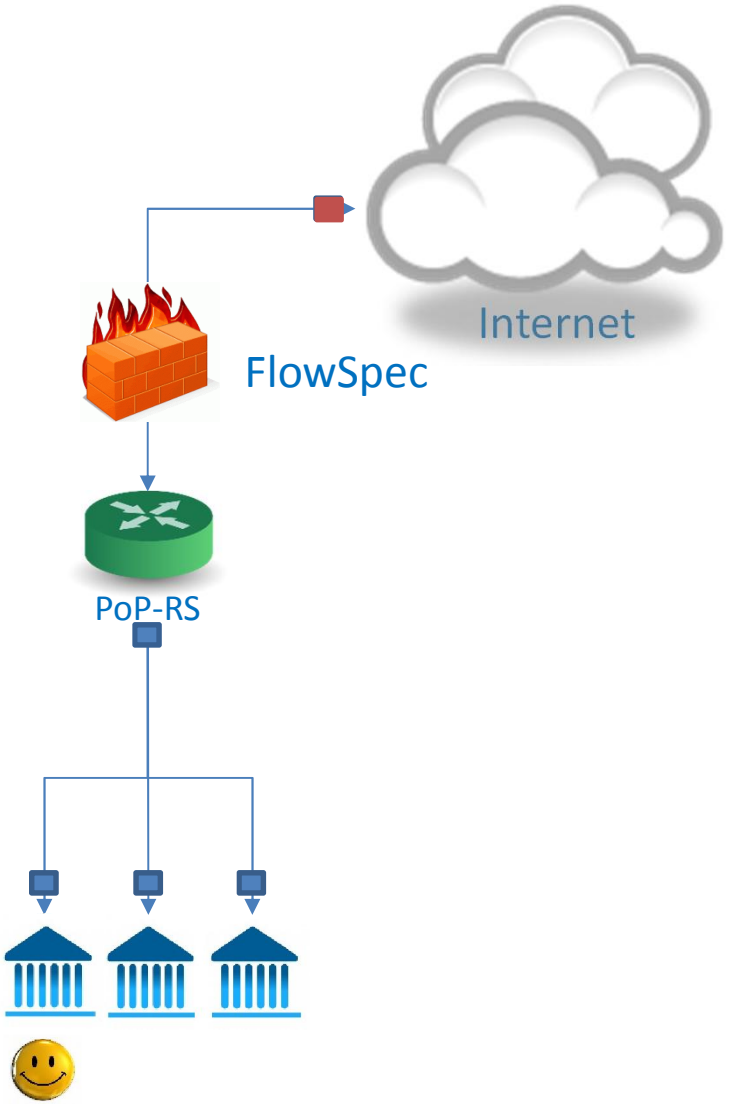
- Filtro inteligente
- Flexibilidade
- Amostra de pacotes bloqueados
- Estatísticas



Ferramenta de Mitigação:
TMS - Dificuldades

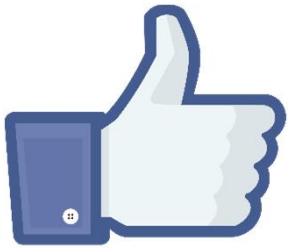
- Limite de throughput
- Mais intrusivo

Ferramenta de Mitigação: FlowSpec



Ferramenta de Mitigação: FlowSpec - Vantagens

- Melhor performace
- Requer menos recursos

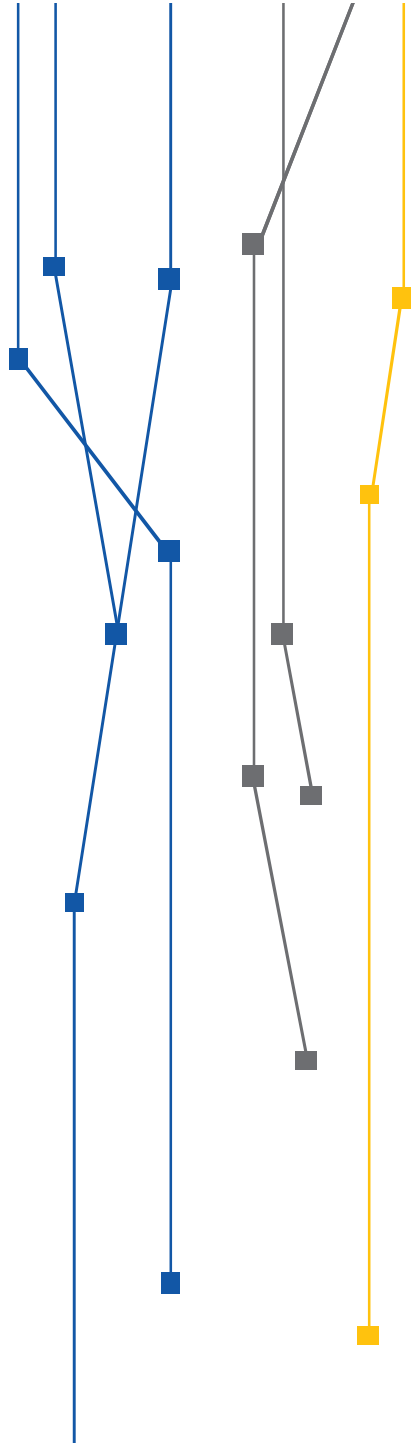


Ferramenta de Mitigação: FlowSpec - Dificuldades

- Filtro “Binário”
- Pouca flexibilidade
- Pouca visibilidade sobre o resultado da mitigação

Próximos passos...

- Projeto de atendimento integrado RNP (24x7)
- Upgrade da solução da Arbor
- Projeto de combate a atividade maliciosa com distribuição de sensores



Dúvidas

SGIS - Sistema de Gestão de Incidentes de Segurança

RNP

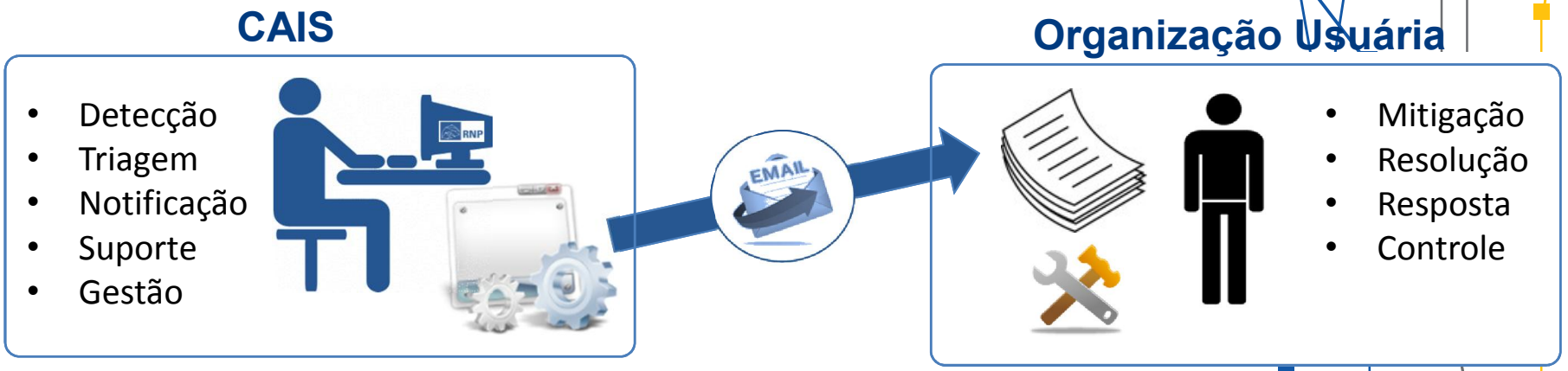
Ministério da **Cultura**

Ministério da **Saúde**

Ministério da **Educação**

Ministério da **Ciência, Tecnologia e Inovação**

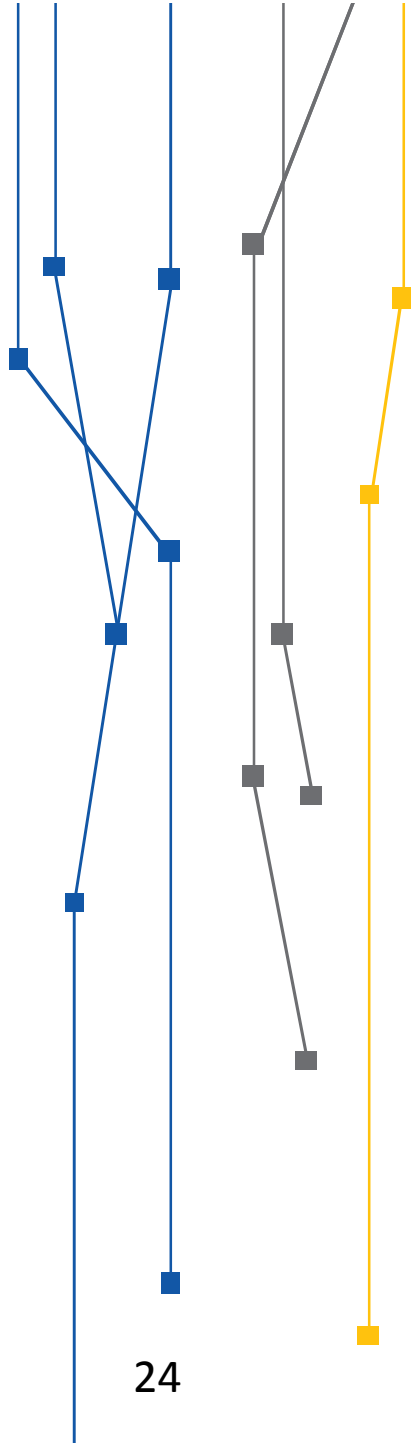
Processo (Sistema) Atual



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.

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

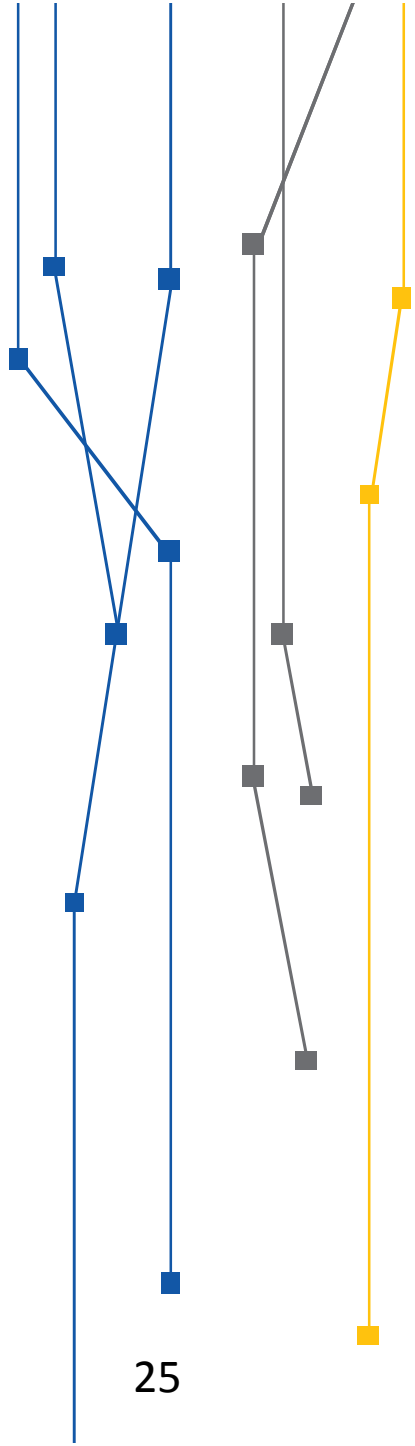


SGIS

Sistema de Gestão de Incidentes

Principais Recursos

- Sistema disponível para todas as Organizações Usuárias
- Facilidade no tratamento de incidentes
- Indicadores e Relatórios gerenciais on-line
- Segregação entre Incidentes e Vulnerabilidades
- Informações sobre Origem e Destino dos incidentes

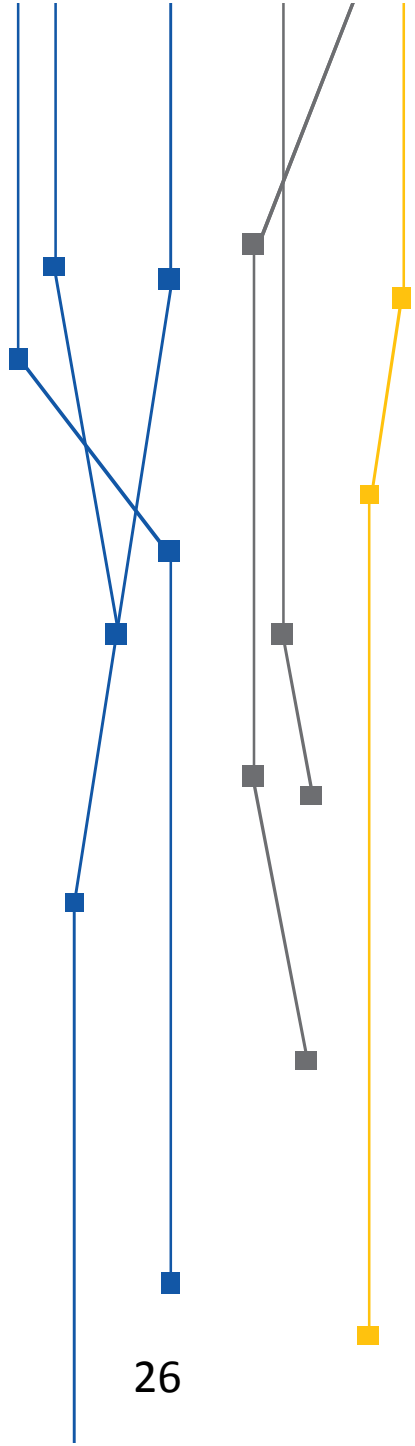


SGIS

Sistema de Gestão de Incidentes

Principais Recursos

- Tratamento de notificações duplicadas
- Perfis de acesso por função
- Envio de arquivo XML com dados das notificações
- Ferramentas colaborativas (Wiki e Instant Messaging)
- Integração com o CAFe (*em implantação*)

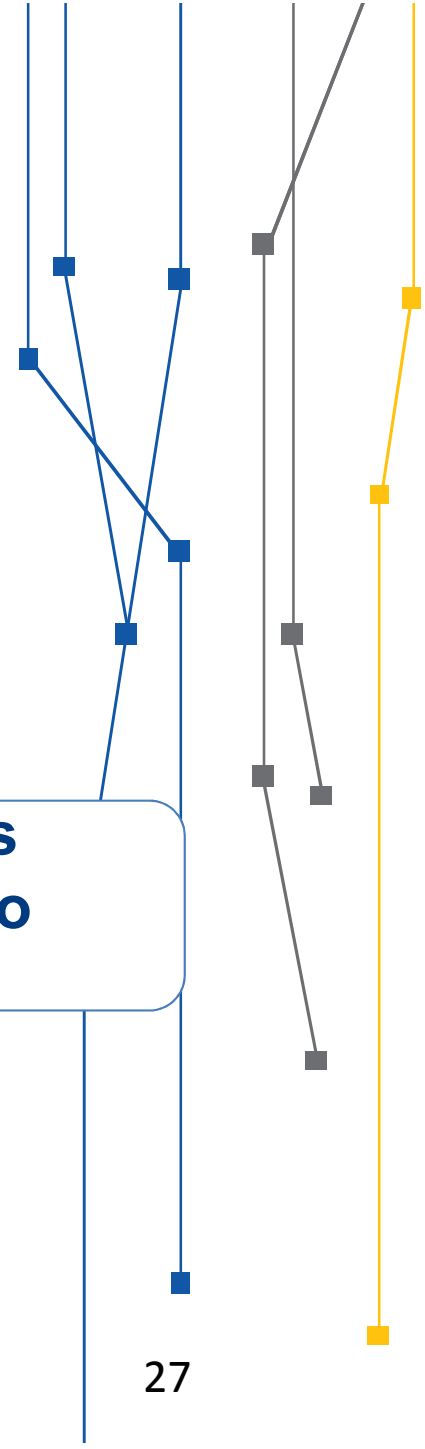


SGIS

Sistema de Gestão de Incidentes

Concessão de acessos baseados em Cadeia de Confiança.

Sistema de acesso restrito aos profissionais que participam do processo.



SGIS

Sistema de Gestão de Incidentes

sgis.rnp.br

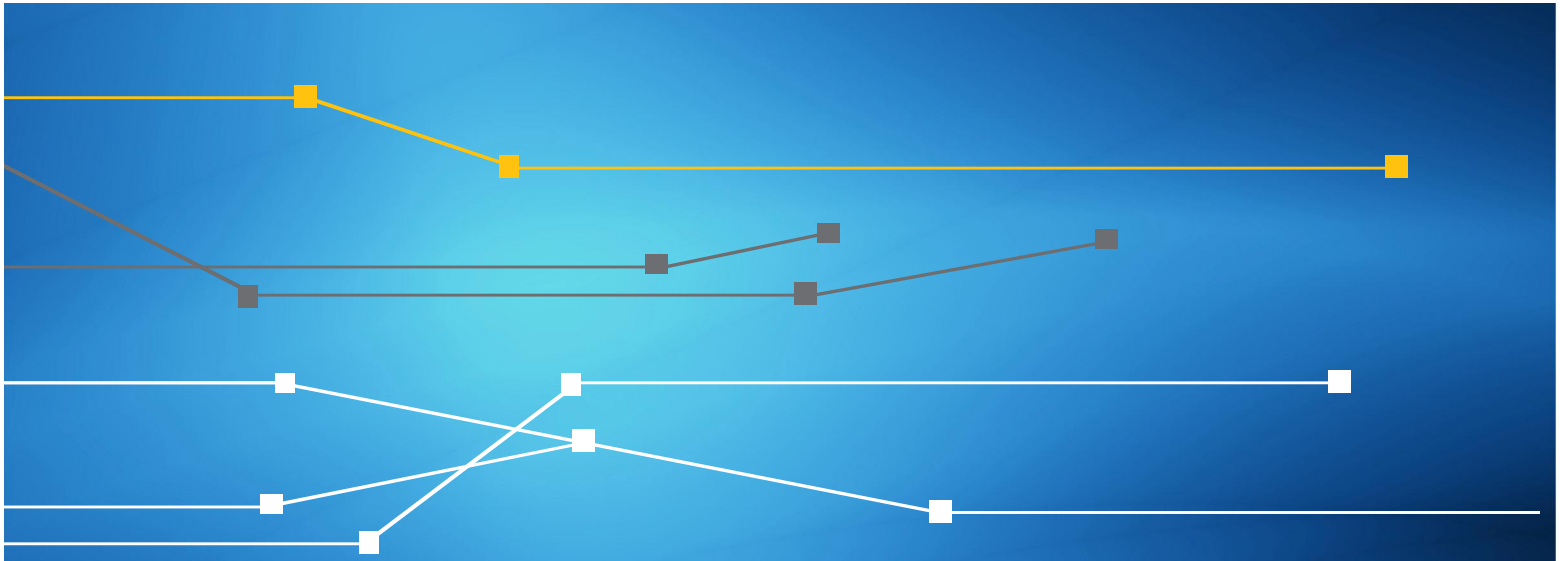
SGIS

Sistema de Gestão de Incidentes

Implantação

Atividade	Data
Concessão de acesso aos PoPs	até 31/10
Concessão de acesso aos gestores de TI e de segurança	até 14/11
Validação de blocos IPs e usuários do sistema - Gestores	14/11 a 28/11
Concessão de acesso aos demais usuários	14/11 a 28/11
Inicio da Produção	**01/12/2014**

Dúvidas



Obrigado!

Alan Santos

alan.santos@rnp.br

RNP

Ministério da **Cultura**

Ministério da **Saúde**

Ministério da **Educação**

Ministério da **Ciência, Tecnologia e Inovação**