Rede de sensores distribuídos do CAIS

Edilson Lima

5º Fórum brasileiro de CSIRTs

Agenda

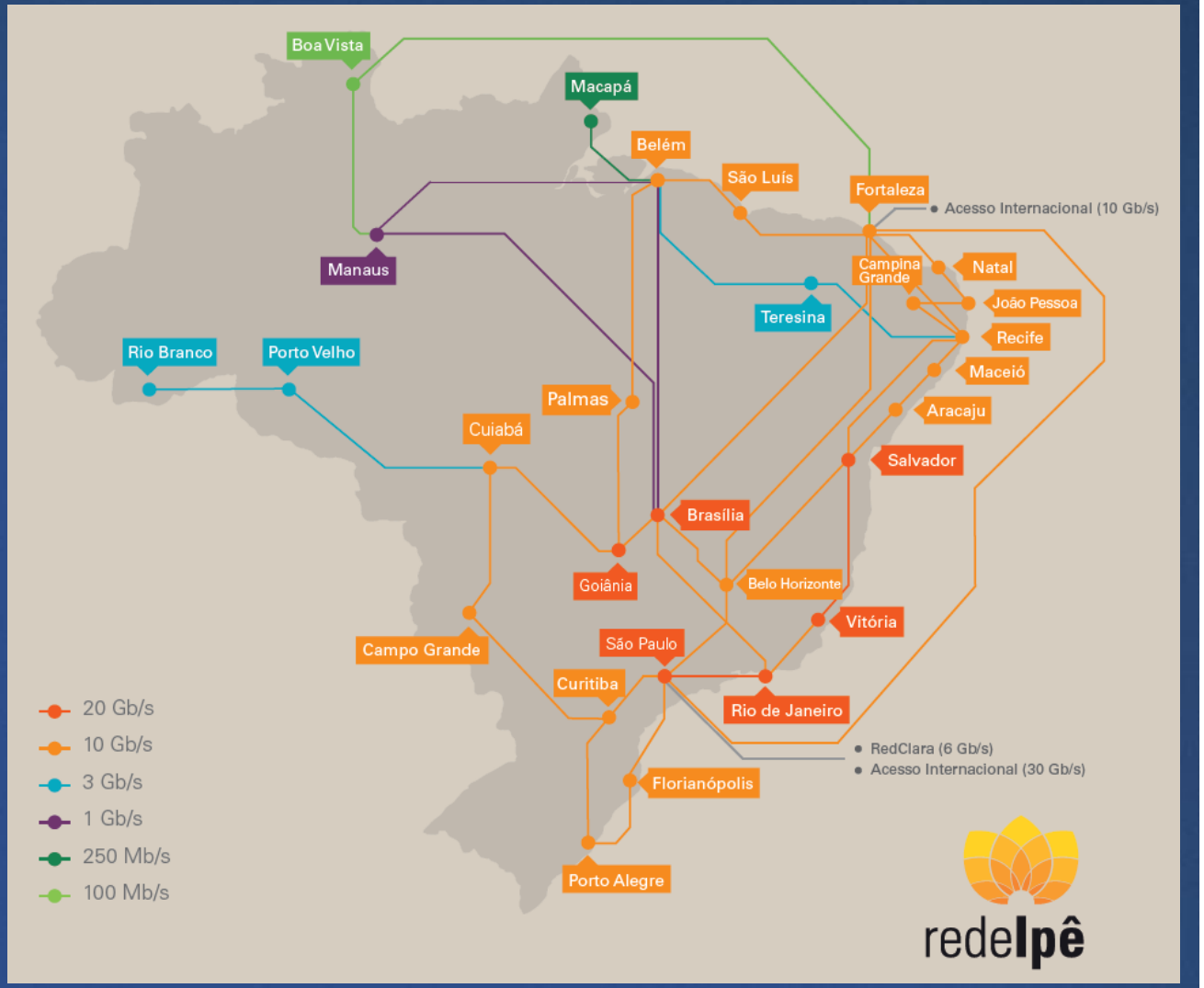
- [ ] Apresentação
- [x] O Projeto
- [ ] Principais números
- [ ] Integração com o sistema SGIS
- [ ] Encerramento

Apresentação

RNP

Rede Nacional de Ensino e Pesquisa (RNP), criada pelo MCTI em 1989, para construir uma infraestrutura de internet acadêmica.

Desde então, participa do desenvolvimento da internet no Brasil, com a introdução de novas tecnologias e a implantação da primeira rede óptica acadêmica da América Latina, em 2005, batizada de Ipê.



Apresentação

CSIRT de coordenação da rede acadêmica brasileira, a Rede Ipê, desde 1997.

Atua na detecção, resolução e prevenção de incidentes de segurança de rede, além de elaborar, promover e disseminar práticas de segurança na RNP e instituições a ela vinculadas.

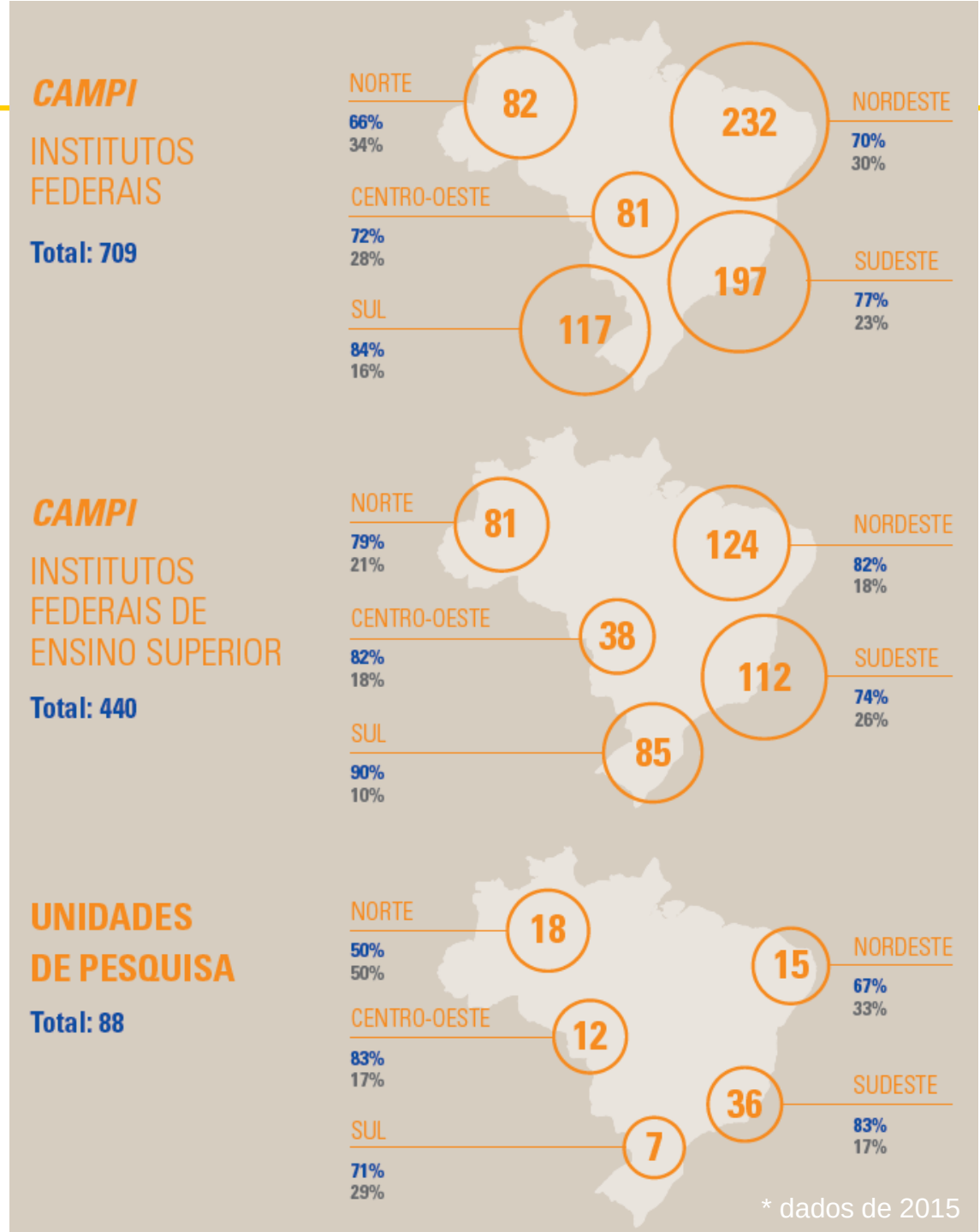
Projeto - Contexto

Rede Ipê, backbone da rede acadêmica.
Capacidade integrada de 345,45 Gb/s.

Interliga 1.237 *campi* de Organizações Usuárias (IFs, IFEs, Unidades de Pesquisa).

Ambiente altamente diversificado em redes, tecnologias e maturidade das equipes de segurança.

Dificuldades para uma detecção eficiente.



* dados de 2015

Projeto - Objetivo

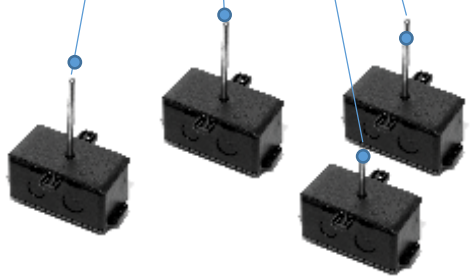
Criar uma rede se sensores na rede acadêmica.

Projeto - O sistema

Projeto - O sistema

Master

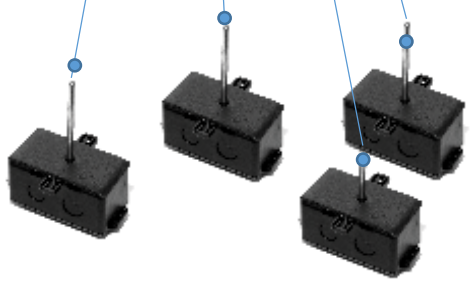
Sensor



Projeto - O sistema

Master

Sensor

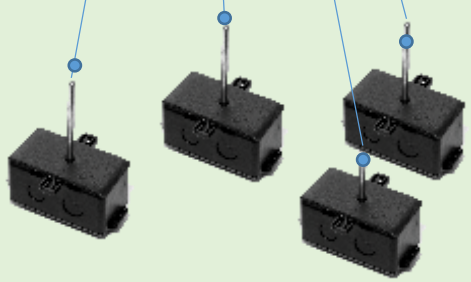


- Gerenciamento dos sensores e instituições
- Gerenciamento das atualizações
- Estatísticas do sistema geral e dos sensores
- Classificação das atividades maliciosas
- Administração geral do sistema

Projeto - O sistema

Master

Sensor



- Interface friendly user
- Plug and play
- Exige pouco conhecimento técnico
- Pouca manutenção e suporte
  - Envio das detecções por e-mail
  - Envio de dados estatísticos e de status
  - Solicitação de atualizações

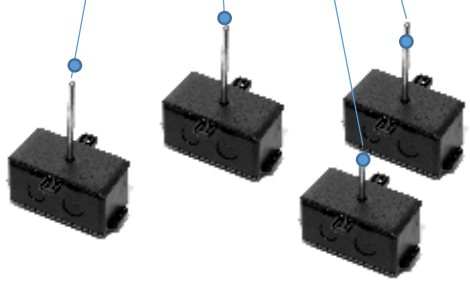
Projeto - O sistema

Master

Conexão

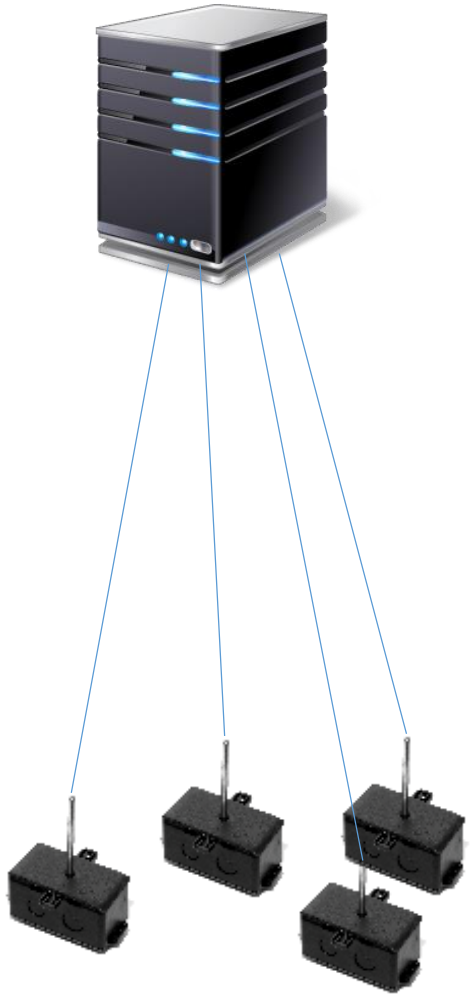
- HTTPS
- Autenticação

Sensor



Projeto - O sistema

Master

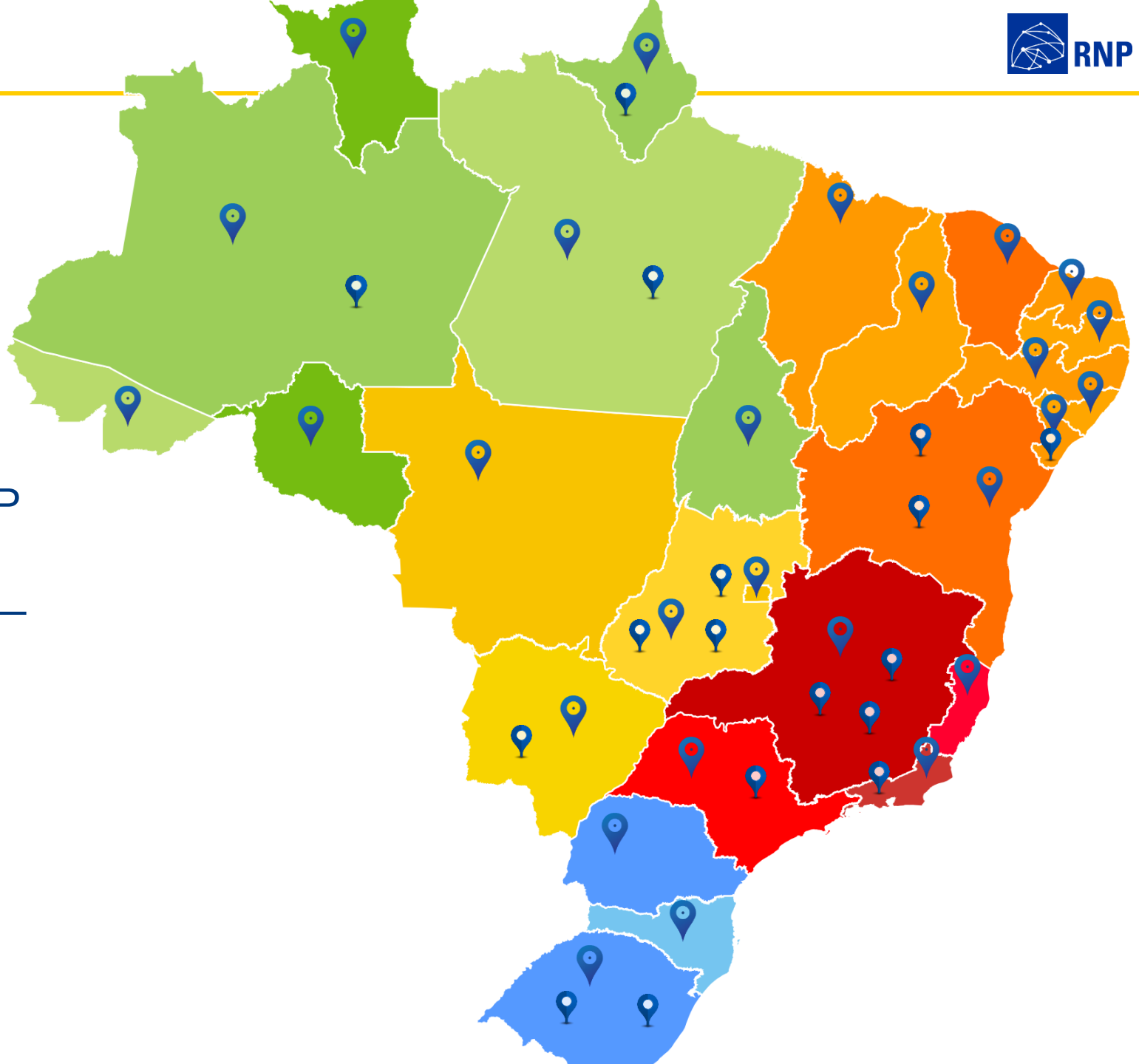


Sensor

Tipos de atualizações

Tipo	Finalidade
Regras gerais	Prover as regras gerais.
Regras customizadas	Prover regras específicas, sob demanda.
Exceções de regras	Desativar regras, sem a necessidade de gerar nova release.
Blacklist URLs	Identificar acessos a URLs maliciosas
Blacklist de IPs	Identificar acessos a IPs maliciosos, como C&C.
Redes	Cada cliente possui sua própria rede, portanto a HOME_NET de cada um deve ser única, para maior assertividade.
Atualizações de Sistema	Novas versões do sensor, correções e features.

Projeto - Implantação



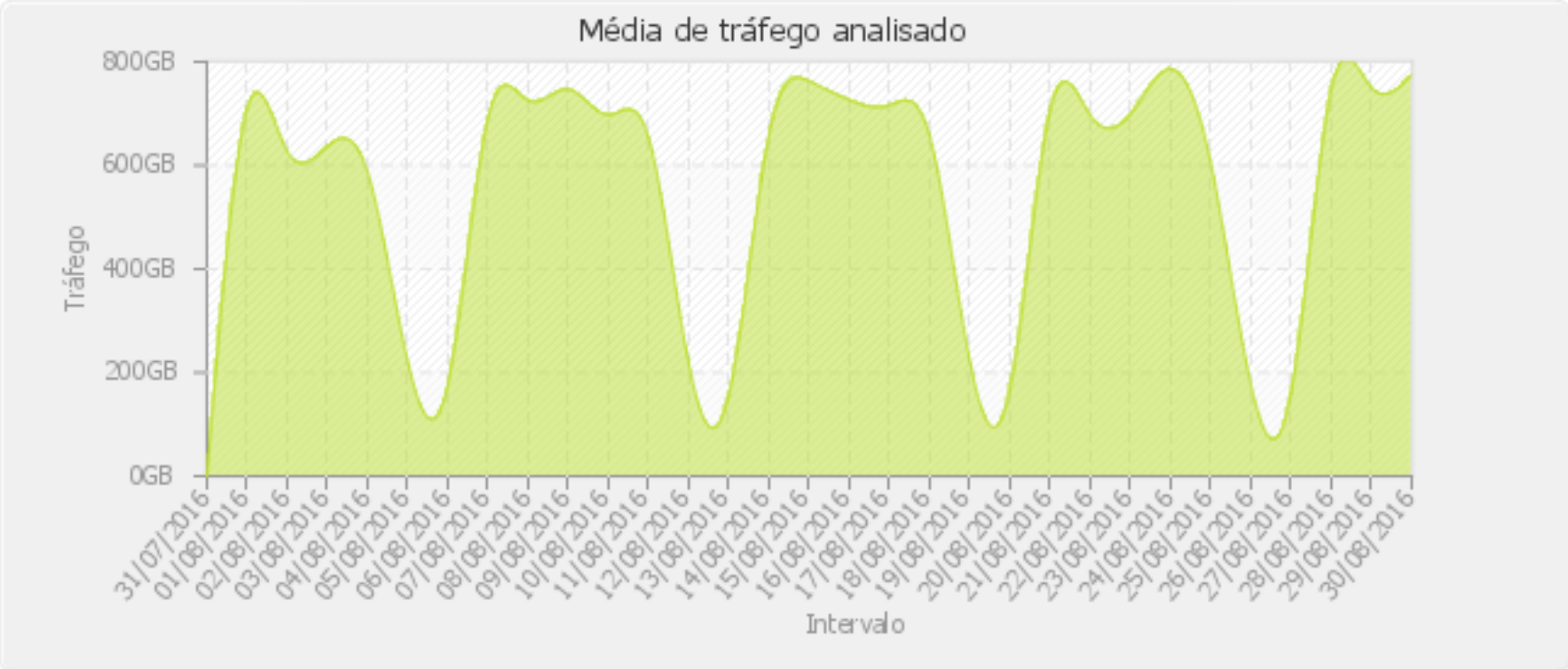
- ✓ 27 Pontos de Presença da RNP
- ✓ 17 Organizações Usuárias

---

44 Sensores Instalados

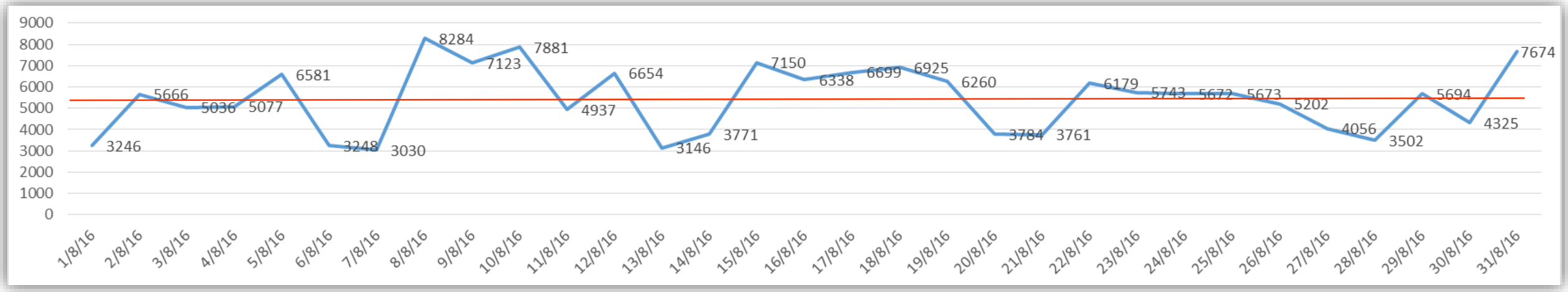
Principais números

Tráfego analisado



Principais números

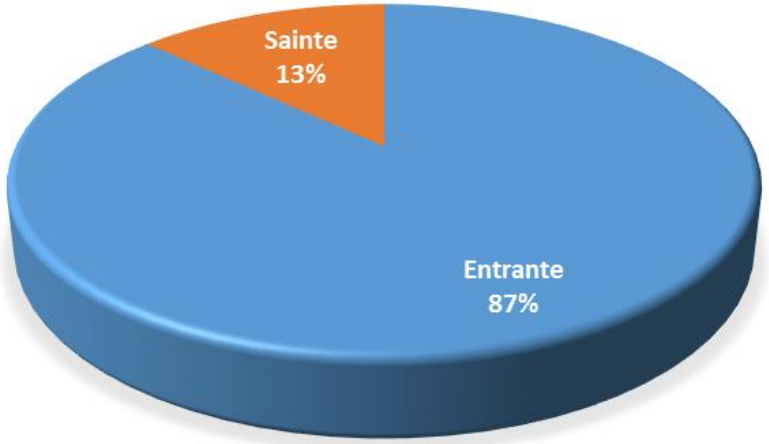
Quantidade de detecções x dia



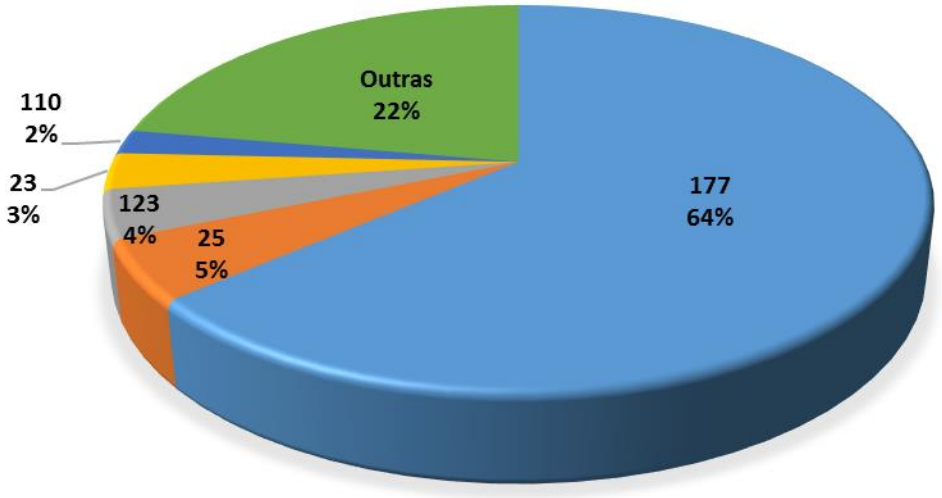
---- Média: 5.430

Principais números

Fluxo da atividade maliciosa



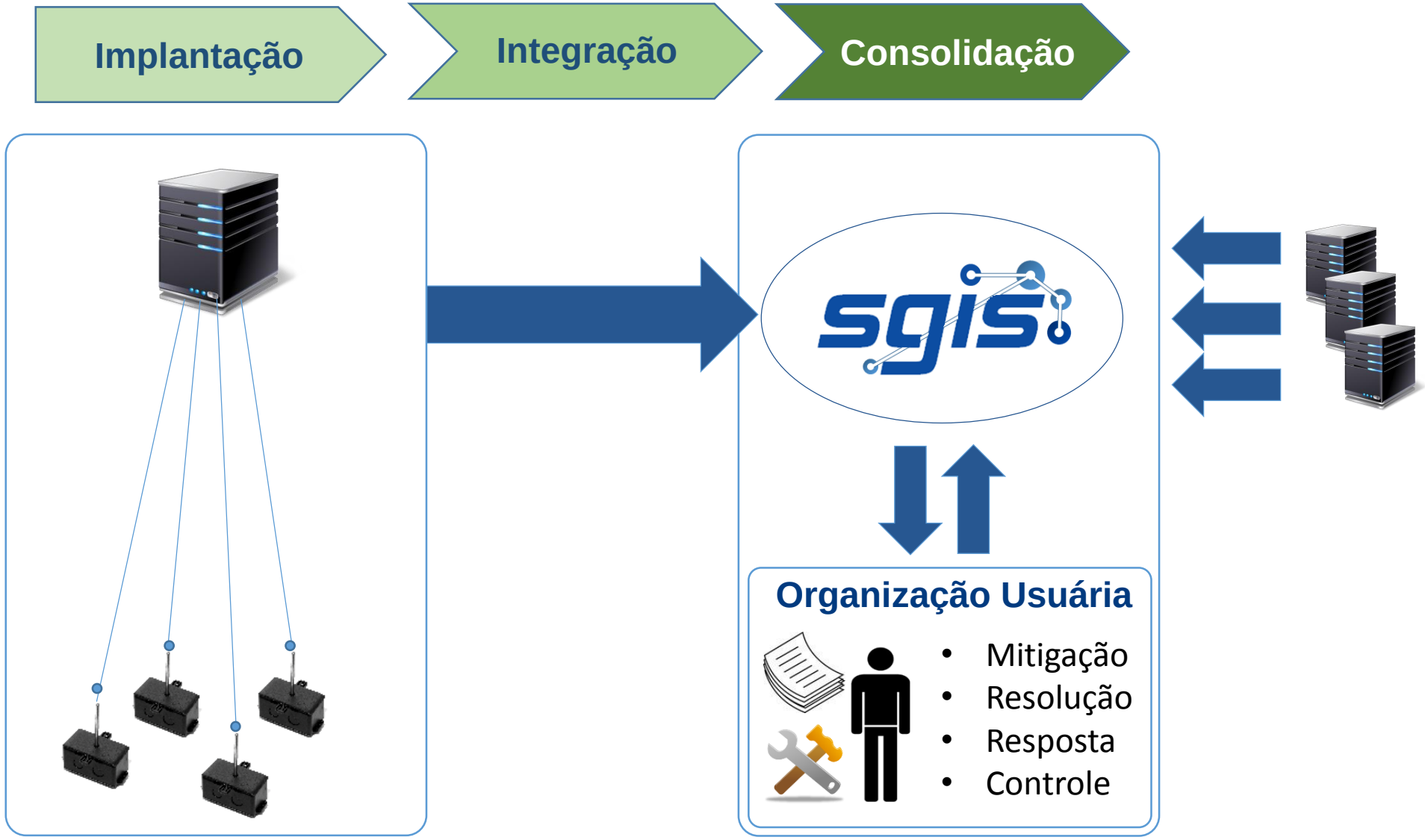
Portas utilizadas



Principais números

Principais atividades maliciosas detectadas

Integração com o SGIS



Encerramento

Encerramento

Muito obrigado,

Edilson Lima
edilson.lima@rnp.br