WTR
WORKSHOP
DE TECNOLOGIA DE REDES DO POP-RS
07 a 09 de novembro de 2018

Registro no SGIS/RNP

Diego Ribeiro Torres

PoP-RS
Ponto de Presença da RNP no Rio Grande do Sul

RNP

Sumário

- SGIS
- Registro no SGIS
- Relatórios
- Desafios

SGIS

- Sistema disponível para todos clientes da RNP
- Gestão de incidentes
- Fomentar a cultura de segurança

SGIS – Página Inicial

- Wiki
- Detalhes
- Relatórios
- Incidentes
  - Origem
  - Destino
- Vulnerabilidades
- Histórico
- Permissões
- Redes
- Contatos
- Editar
- Criar Filho
- Remover

PoP-RS: Detalhes

Detalhes da Organização

Título:	PoP-RS (pop-rs)
Sigla:	PoP-RS
Criador:	CAIS RNP
Estado:	Rio Grande do Sul
Criado em:	30 de Outubro de 2014 às 18:27
Última modificação em:	11 de Setembro de 2018 às 14:50

Estrutura:	• **PoP-RS**
	  ◦ Associação Riograndense de Empreendimentos de Assistência Técnica e Extensão Rural
	  ◦ Centro de Excelência em Tecnologia Eletrônica Avançada
	  ◦ Centro de Preparação de Oficiais da Reserva
	  ◦ Centro Universitário La Salle
	  ◦ Colégio Militar de Porto Alegre
	  ◦ Embrapa - Clima Temperado
	  ◦ Embrapa Escritório de Negócios de Capão do Leão
	  ◦ Embrapa Pecuária Sul (CPPSUL)(Bagé)
	  ◦ Embrapa Trigo Passo Fundo
	  ◦ Embrapa Uva e Vinho Bento Goncalves
	  ◦ Escola Superior de Redes

SGIS – Mensagem

Antes de encerar este incidente junto ao CAIS, certifique-se que:
1. O incidente foi investigado e identificado:
2. O incidente foi corrigido, garantindo que ele não voltará a acontecer.

Para encerar o incidente, acesse o sistema SGIS (link abaixo) e atualize o status do incidente:
"https://sgis.rnp.br/incidents/[redacted]"

O incidente pode também ser encerrado mediante resposta dessa mensagem, conforme segue:

Para incidentes tratados e corrigidos, substitua o campo "Assunto"/"Subject" por:
[CAIS #[redacted]] - [RESOLVIDO]

Para incidentes com informações insuficientes ou cujo host denunciado não pertença a Instituição, substitua o campo "Assunto"/"Subject" por:
[CAIS #[redacted]] - [CAIS-AJUDA]

Aguardamos seu retorno, certos de sua colaboração, e nos colocamos a disposição
para quaisquer esclarecimentos.

Caso você não seja a pessoa apropriada para receber este tipo de mensagem, por
favor nos informe a quem devemos contactar para resolver este incidente.

Atenciosamente,

CAIS/RNP

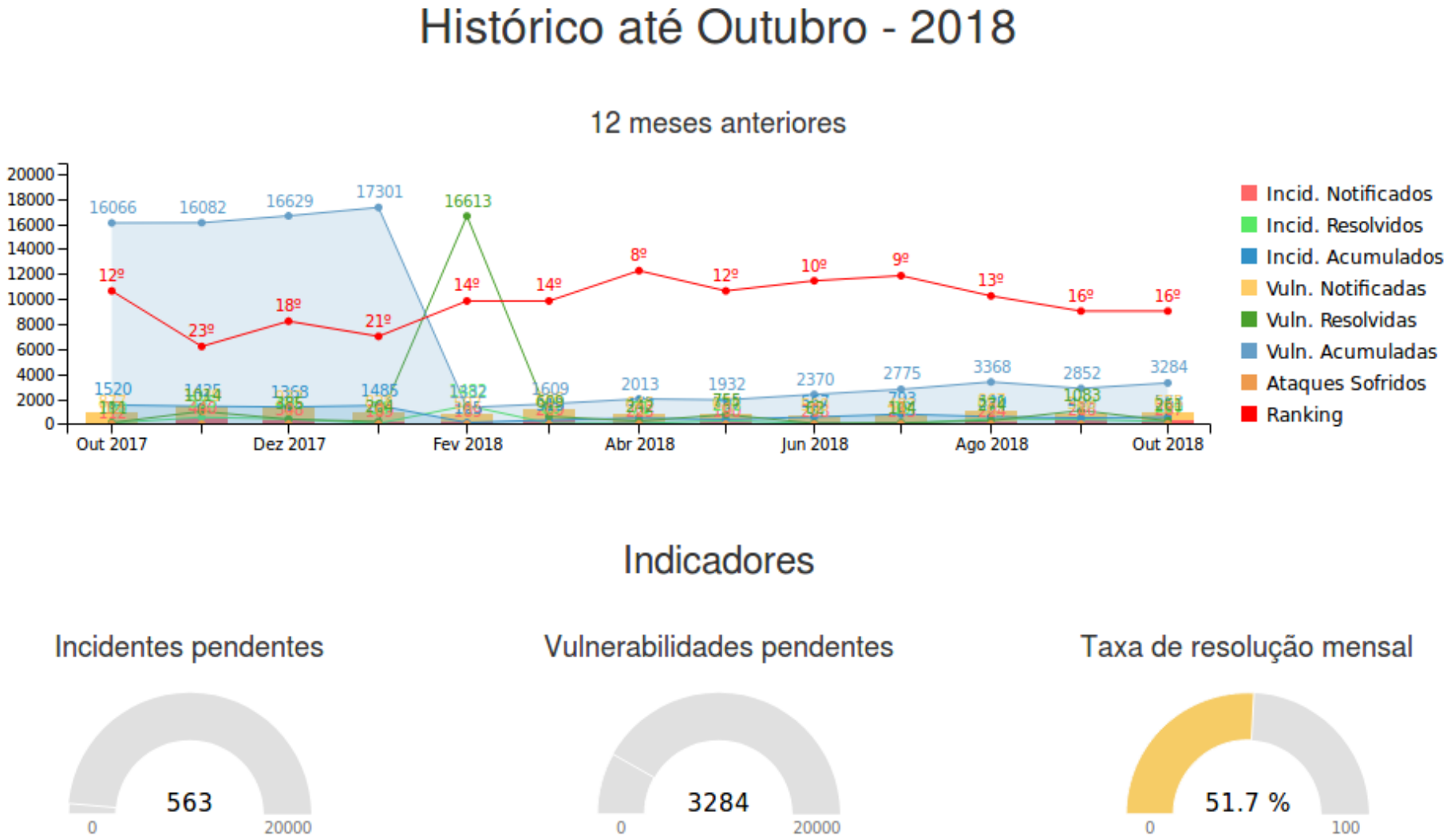
```
#################################################################
#   CENTRO DE ATENDIMENTO A INCIDENTES DE SEGURANCA (CAIS)      #
#       Rede Nacional de Ensino e Pesquisa (RNP)                #
#                                                               #
# cais@cais.rnp.br       http://www.rnp.br/servicos/seguranca   #
# Tel. 019-37873300      Fax. 019-37873301                      #
# Chave PGP disponivel   http://www.rnp.br/cais/cais-pgp.key    #
#################################################################

-------------------------------------------------------------------------------
Data e hora UTC(+0),IP Origem, Porta Origem, Protocolo, WebServer, Vulnerabilidade
[redacted]
```

Registro no SGIS

- Usuário e Contato
- Perfis de Acesso

Relatórios – 12 meses e indicadores



Indicadores

Incidentes pendentes

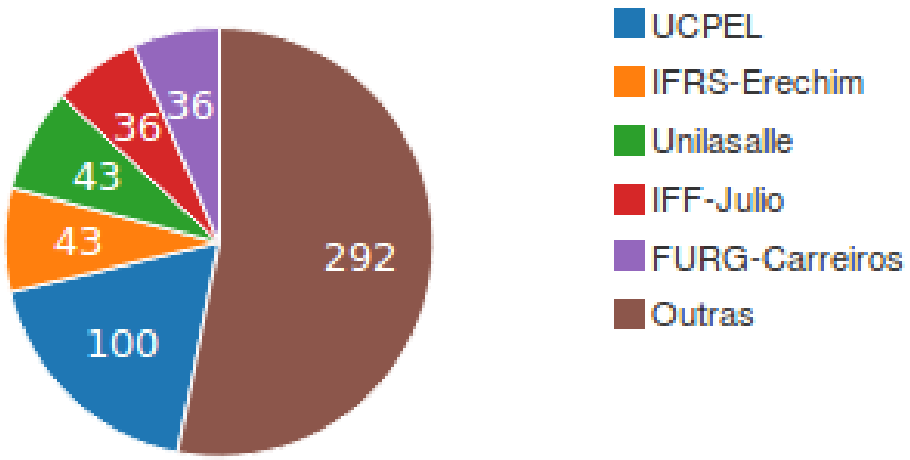
Vulnerabilidades pendentes

Taxa de resolução mensal

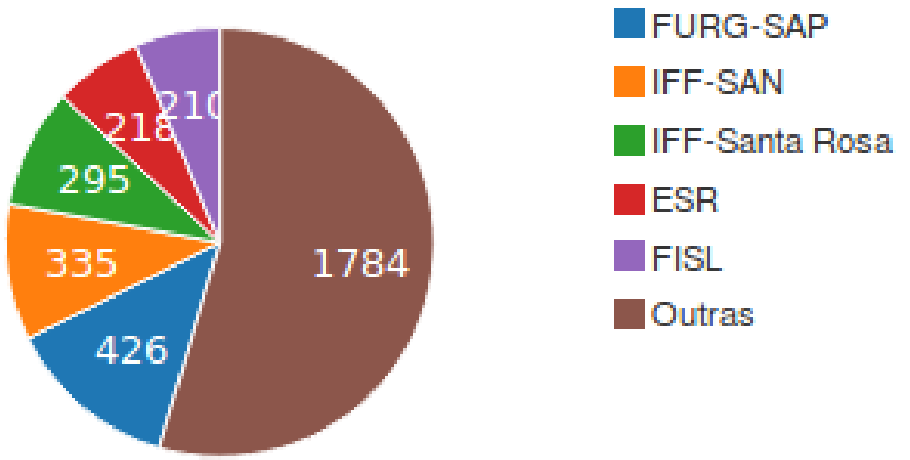
Relatórios – Pendentes

Distribuição por organização

Incidentes pendentes



Vulnerabilidades pendentes



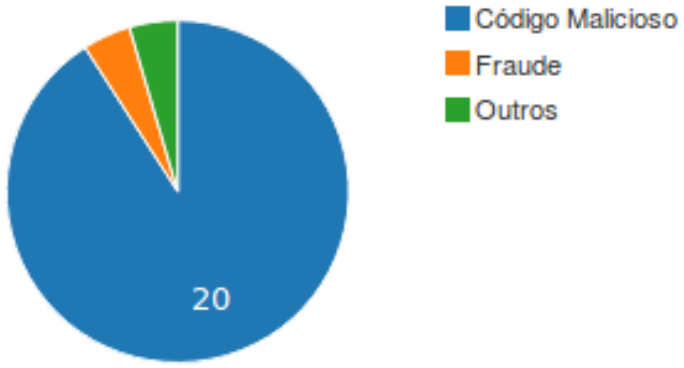
Relatórios – Incidentes

Top 10 IPs

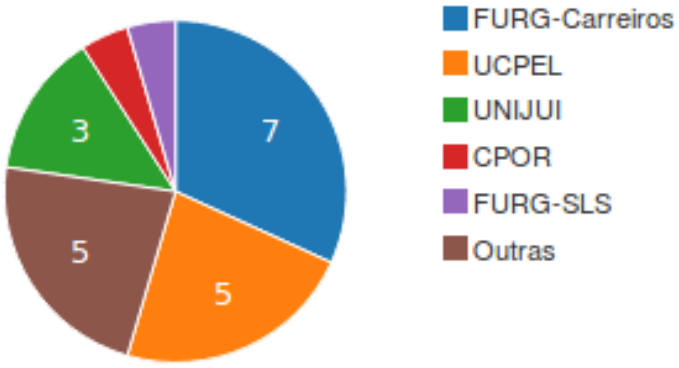
Origem	#
200.17.82.130	3
200.17.82.98	2
200.132.214.210	2
2804:0:5420:a:54a7:1d50:7dca:d58d	1
200.19.255.222	1
200.18.33.235	1
200.17.86.104	1
200.17.86.101	1
200.17.86.10	1
200.17.173.18	1

Incidentes

Por categorias



Por organizações



Desafios

- Redução de bots – desestimular uso de NAT (78,8%)
- Vulnerabilidade SSLv3 – Poodle attack (49,2%)
- Tempo para resolução de chamados

Obrigado(a)!

Diego Ribeiro Torres

diego@pop-rs.rnp.br