WTR

WORKSHOP
DE TECNOLOGIA DE REDES DO POP-RS
2021

Ações de segurança na rede Tchê

Diego Ribeiro Torres

22 SET

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

RNP
ORGANIZAÇÃO SOCIAL DO MCTI

Introdução

- Centro de Resposta a Incidentes de Segurança (CERT-RS)
- Pioneiro – fundado em Agosto de 1997
- Sistema de Gestão de Incidentes de Segurança (SGIS)

Objetivos do CERT-RS

- Responder por incidentes na rede acadêmica gaúcha (rede Tchê)
- Auxiliar na resolução de incidentes e vulnerabilidades
- Aumentar a conscientização sobre a necessidade da segurança na internet
- Colaborar em equipe para deixar a internet mais saudável

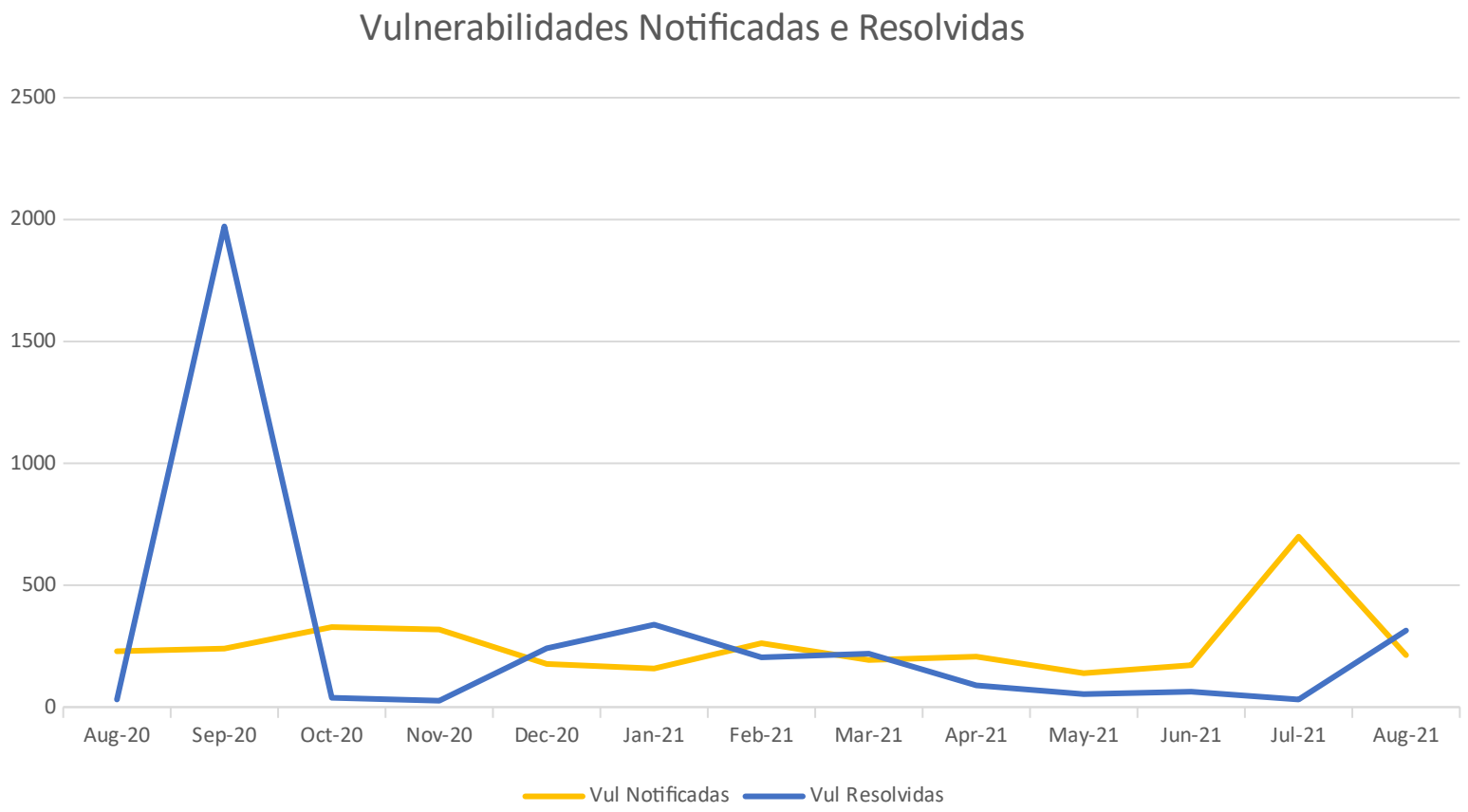
Vulnerabilidades e Incidentes

- **Vulnerabilidade**: é uma falha ou fraqueza no projeto, implementação, operação, ou gestão de um sistema que pode ser explorada para violar as políticas de segurança do sistema.

- **Incidente/violação de segurança**: é um ato, ou evento, que desobedece ou, de alguma forma, rompe com a política de segurança.

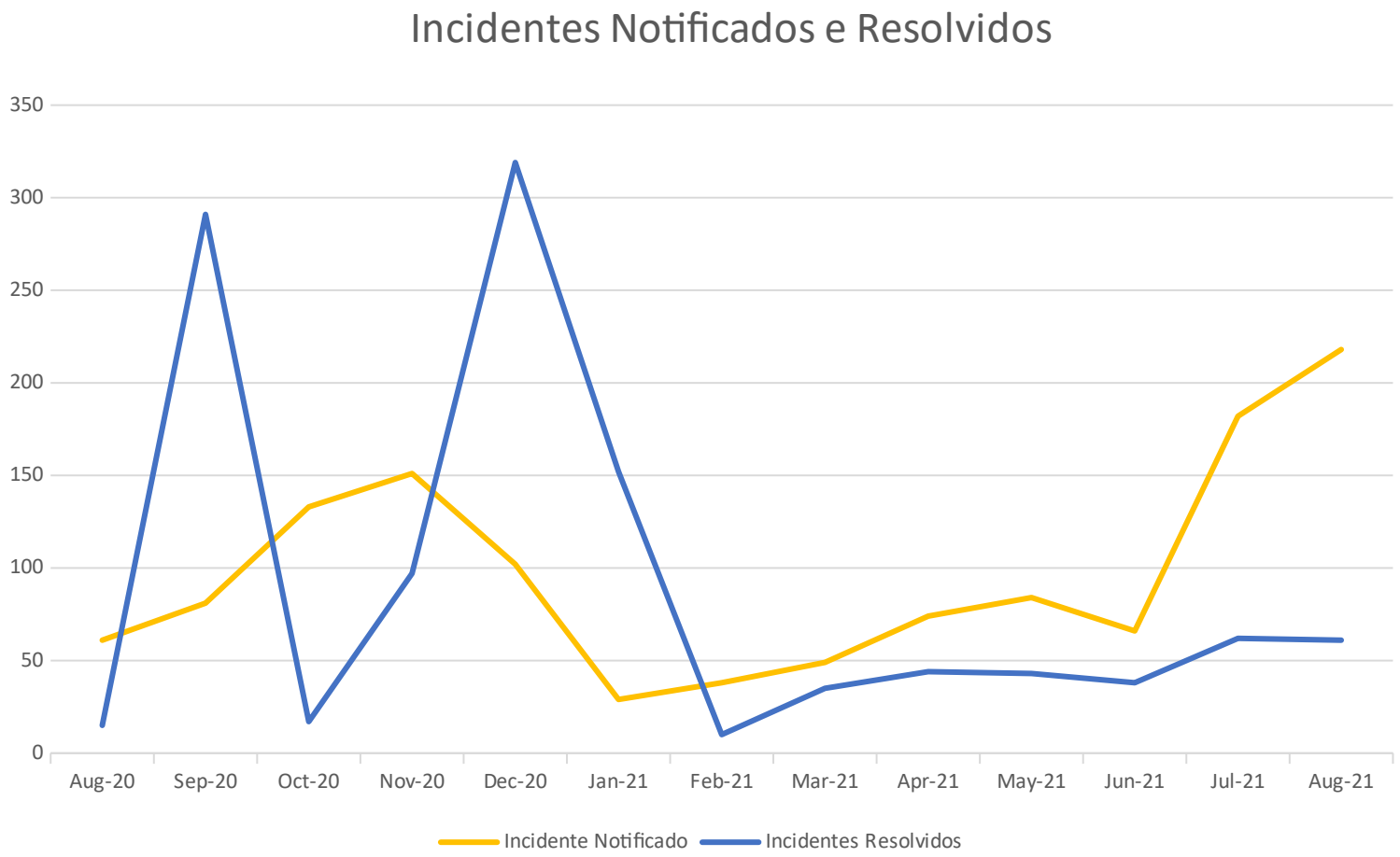
•*IETF RFC 2828 – tradução livre*

Vulnerabilidades e Incidentes



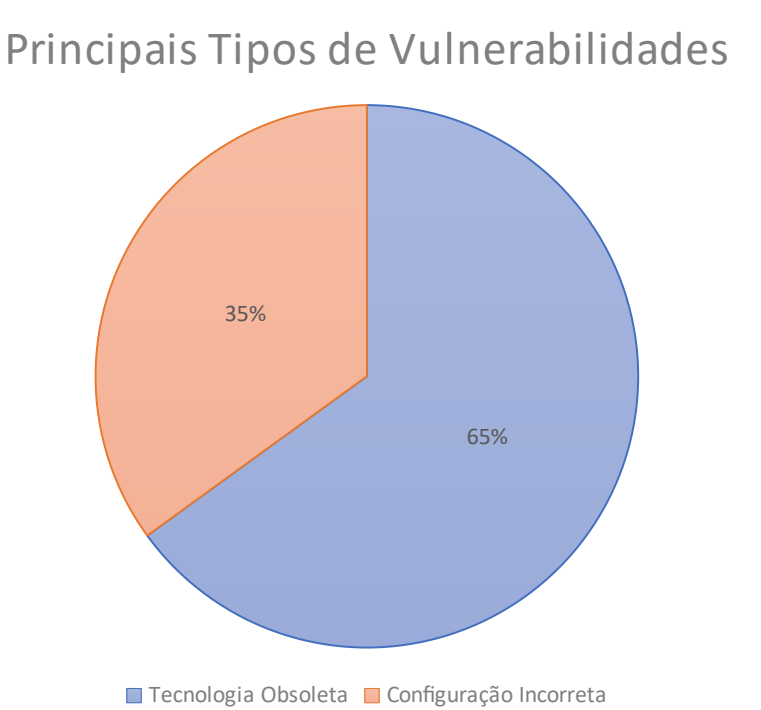
Fonte: https://sgis.rnp.br

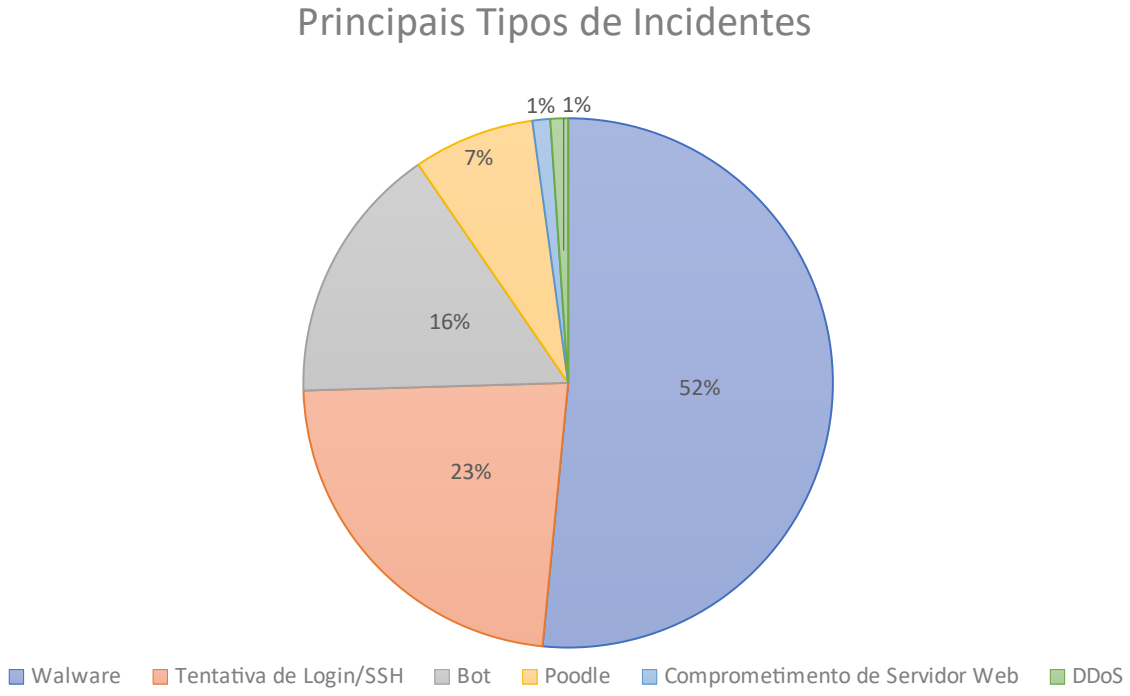
Vulnerabilidades e Incidentes



Fonte: https://sgis.rnp.br

Principais Tipos de Incidentes



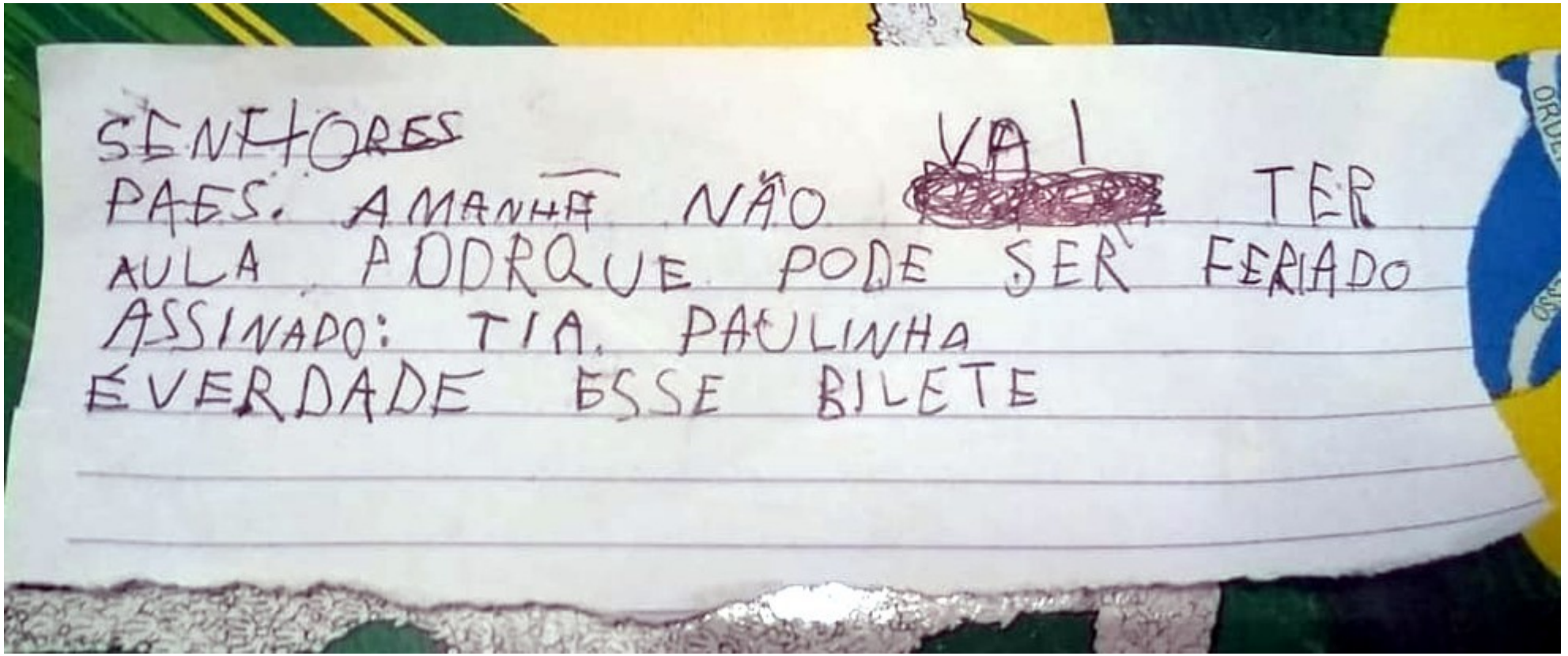


Fonte: https://sgis.rnp.br

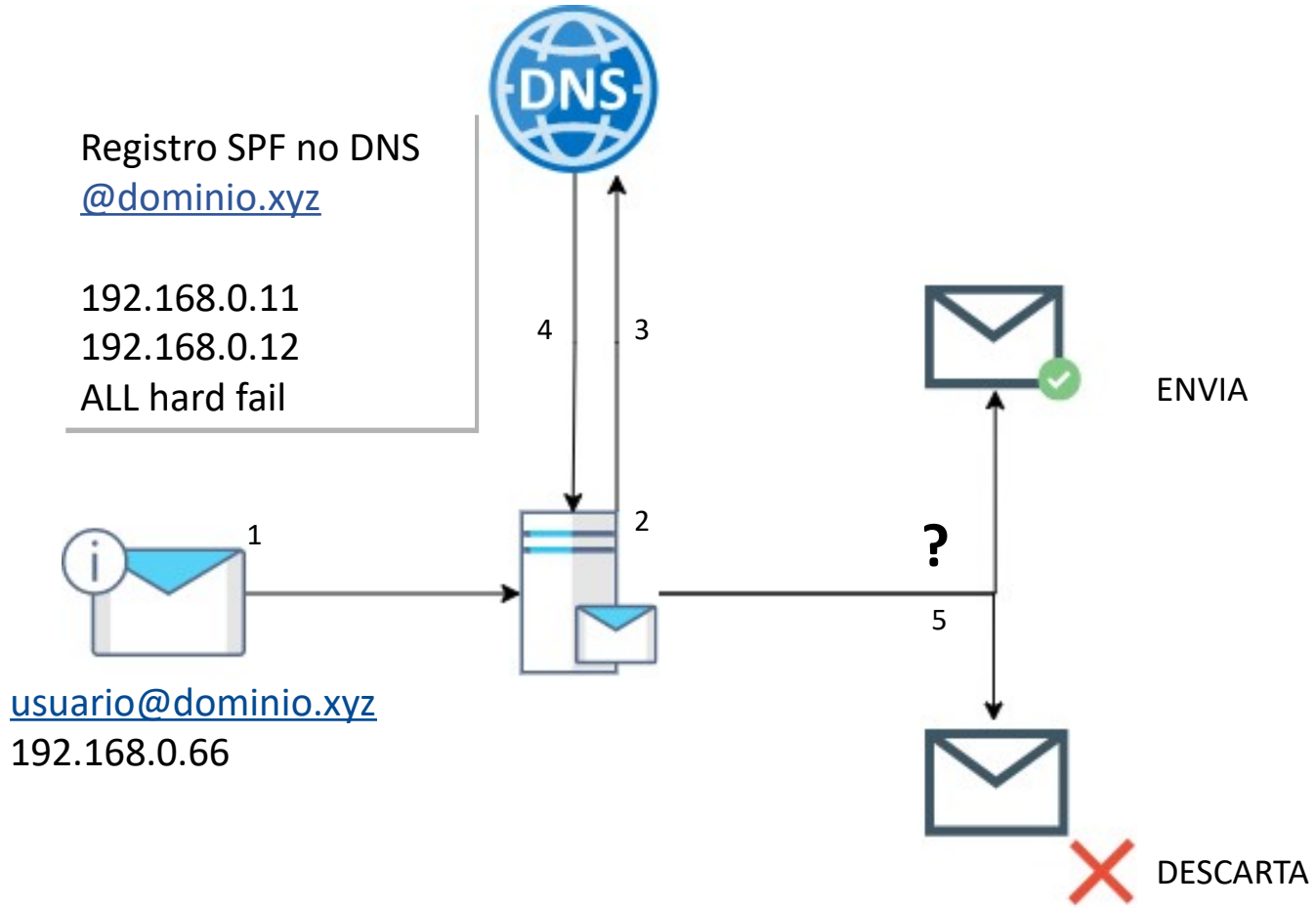
BLOQUEIO DE PREFIXOS DE REDE

O QUE É SPF?

Uma forma de evitar e-mails fraudulentos usando o seu domínio.



SPF – Sender Policy Framework



SPF – Sender Policy Framework

+Pass: significa que o IP está autorizado a enviar mensagens em nome do domínio

–Fail: este resultado pode ser utilizado para rejeitar a mensagem.

?Neutral: este resultado deve ser tratado exatamente como se não existisse um registro SPF.

~SoftFail: a mensagem não deve ser rejeitada apenas com base neste resultado, mas é recomendável submetê-la a outros testes.

include: usado para incluir endereços de terceiros, não pertencentes ao domínio.

Exemplos de configuração

v=spf1 –all

v=spf1 ip4: 123.0.0.1 ip6:fe80:: include:dominio.xyz

v=spf1 +all

v=spf1 ip4:192.168.0.0/16 ip6:fe80:cafe:/64 -all

Contatos

E-MAIL:

CERT-RS: cert-rs@pop-rs.rnp.br

CAIS: cais@rnp.br

TELEFONE:

CERT-RS (8hrs às 18hrs):

(51) 3308-5039

(51) 3308-5042

CERT-RS EMERGÊNCIAS (24 hrs):

(51) 3308-5036

(51) 3308-5205

Obrigado!

WTR
WORKSHOP
DE TECNOLOGIA DE REDES DO POP-RS
2021

APOIO

nic.br

REALIZAÇÃO

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

RNP
ORGANIZAÇÃO SOCIAL DO MCTI

MINISTÉRIO DO TURISMO
MINISTÉRIO DA DEFESA
MINISTÉRIO DA SAÚDE
MINISTÉRIO DAS COMUNICAÇÕES
MINISTÉRIO DA EDUCAÇÃO
MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÕES

PÁTRIA AMADA BRASIL
GOVERNO FEDERAL