



**nic.br**

Núcleo de Informação  
e Coordenação do  
Ponto BR

**egi.br**

Comitê Gestor da  
Internet no Brasil

**registro.br cert.br cetic.br ceptro.br ceweb.br ix.br**

# Melhores Práticas de Segurança para ISPs

## Programa por uma Internet mais segura

Gilberto Zorello | [gzorello@nic.br](mailto:gzorello@nic.br)

**Provedor em Foco - ABRINT - Edição Vitória**

Vitória, ES | 22/10/25

**nic.br**

**Quem são o NIC.br e o CGI.br  
e por que padrões técnicos,  
boas práticas e colaboração  
são importantes para a Internet?**



# Como a Internet começou?

- Projeto da DARPA
- Redes resilientes
- Chegou ao Brasil na década de 1990
- Eco 92
- Abertura comercial
- CGI.br e NIC.br







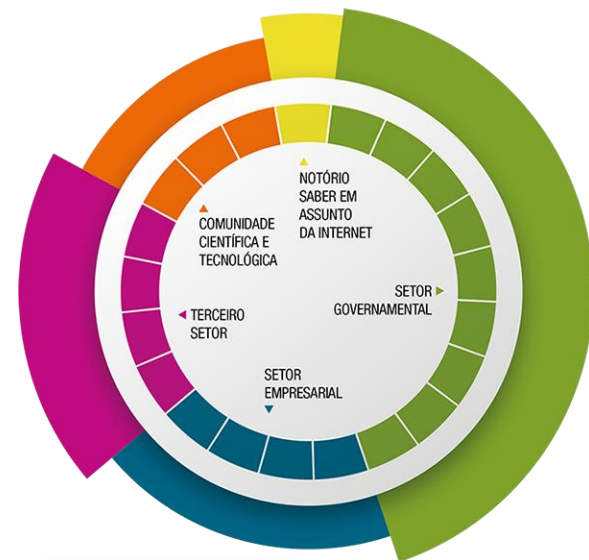
## NIC.br e CGI.br

- CGI.br: criado em 1995
- Decreto em 2003
- Diretrizes para o desenvolvimento da Internet no Brasil
- NIC.br: organização privada sem finalidade de lucro
- Braço executivo do CGI.br

<https://cgi.br/>

<https://nic.br/>

# NIC.br e CGI.br



membros e ex-membros do CGI.br  
(somente os atuais membros têm direito a voto)

## ASSEMBLEIA GERAL

7 membros eleitos pela Assembleia Geral

CONSELHO DE  
ADMINISTRAÇÃO

CONSELHO  
FISCAL

ADMINISTRAÇÃO  
JURÍDICO  
COMUNICAÇÃO  
ASSESSORIAS:  
CGI.br e PRESIDÊNCIA

DIRETORIA  
EXECUTIVA

1 2 3 4 5



- 1 Diretor presidente
- 2 Diretor administrativo e financeiro
- 3 Diretor de serviços e de tecnologia
- 4 Diretor de projetos especiais e de desenvolvimento
- 5 Diretor de assessoria às atividades do CGI.br





# Padrões técnicos e colaboração

- RFCs
- IETF
- Padrões Abertos
- ~ 75 mil redes na Internet
- ~ 8,5 mil no Brasil
- Colaboração

<https://ietf.org/>  
<https://bgp.potaroo.net/>  
<https://mapadeas.ceptro.br/>



# Programa por uma Internet mais Segura

Nossa agenda



## Objetivo / Plano de Ação

Interação com Provedores e Operadoras

## Ações do Programa

Notificação de Amplificadores

MANRS

KINDNS

TOP – Teste os Padrões



MANRS



PROGRAMA  
INTERNET  
+SEGURA



TESTE OS PADRÕES



KINDNS





# Objetivos do Programa

- Reduzir ataques DDoS
- Melhorar a segurança de roteamento
- Reduzir vulnerabilidades e falhas de configuração
- Divulgar melhores práticas de segurança
- **Aumentar a cultura de segurança**

<https://bcp.nic.br/i+seg>







# Configuração de serviços expostos na Internet

- Usados para amplificação em DDoS
- Portas UDP: DNS (53), SNMP (161), NTP (123), e várias outras!
- Notificações do CERT.br

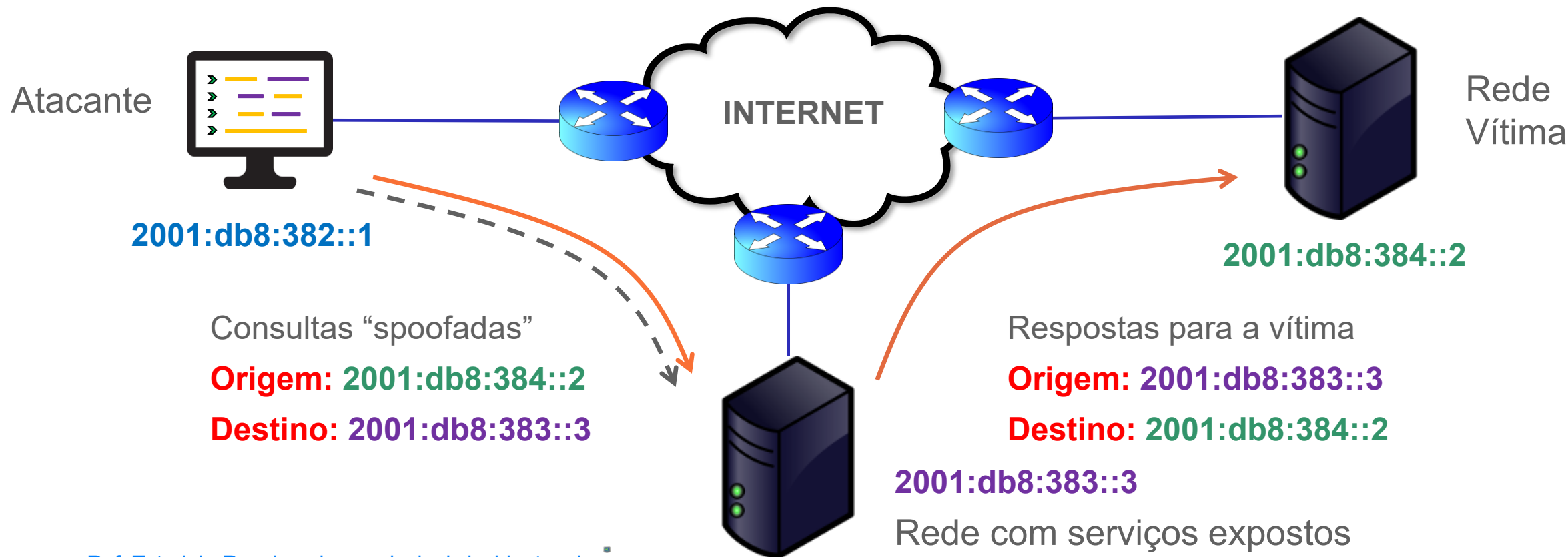
<https://bcp.nic.br/i+seg/acoes/amplificacao/>



# Programa por uma Internet mais Segura

## Negação de Serviço Reflexivo com Amplificação

Utiliza um terceiro para fazer o ataque



[Ref. Tutorial - Resolvendo os principais incidentes de segurança](#)

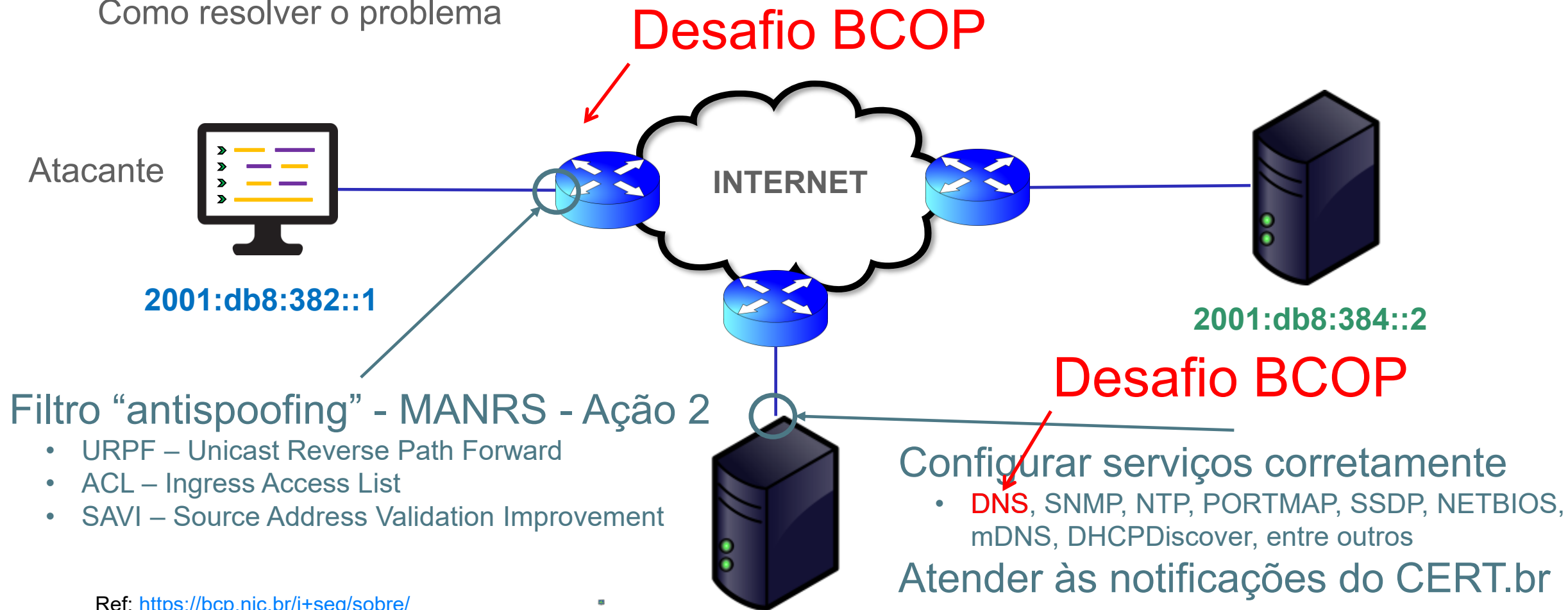


# Programa por uma Internet mais Segura

## Negação de Serviço Reflexivo com Amplificação



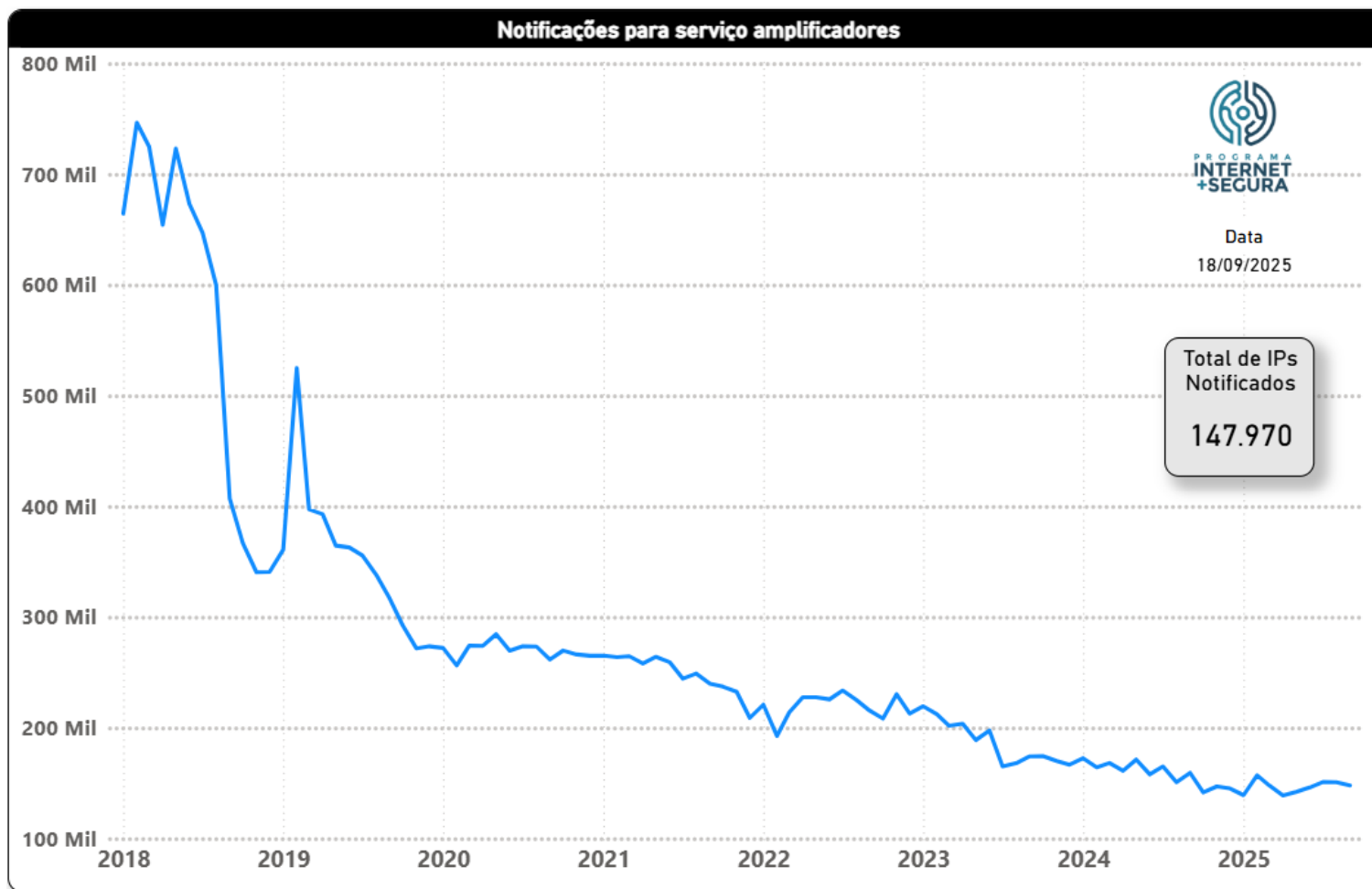
Como resolver o problema



Ref: <https://bcp.nic.br/i+seg/sobre/>

# Programa por uma Internet mais Segura

## Notificação de amplificadores - evolução



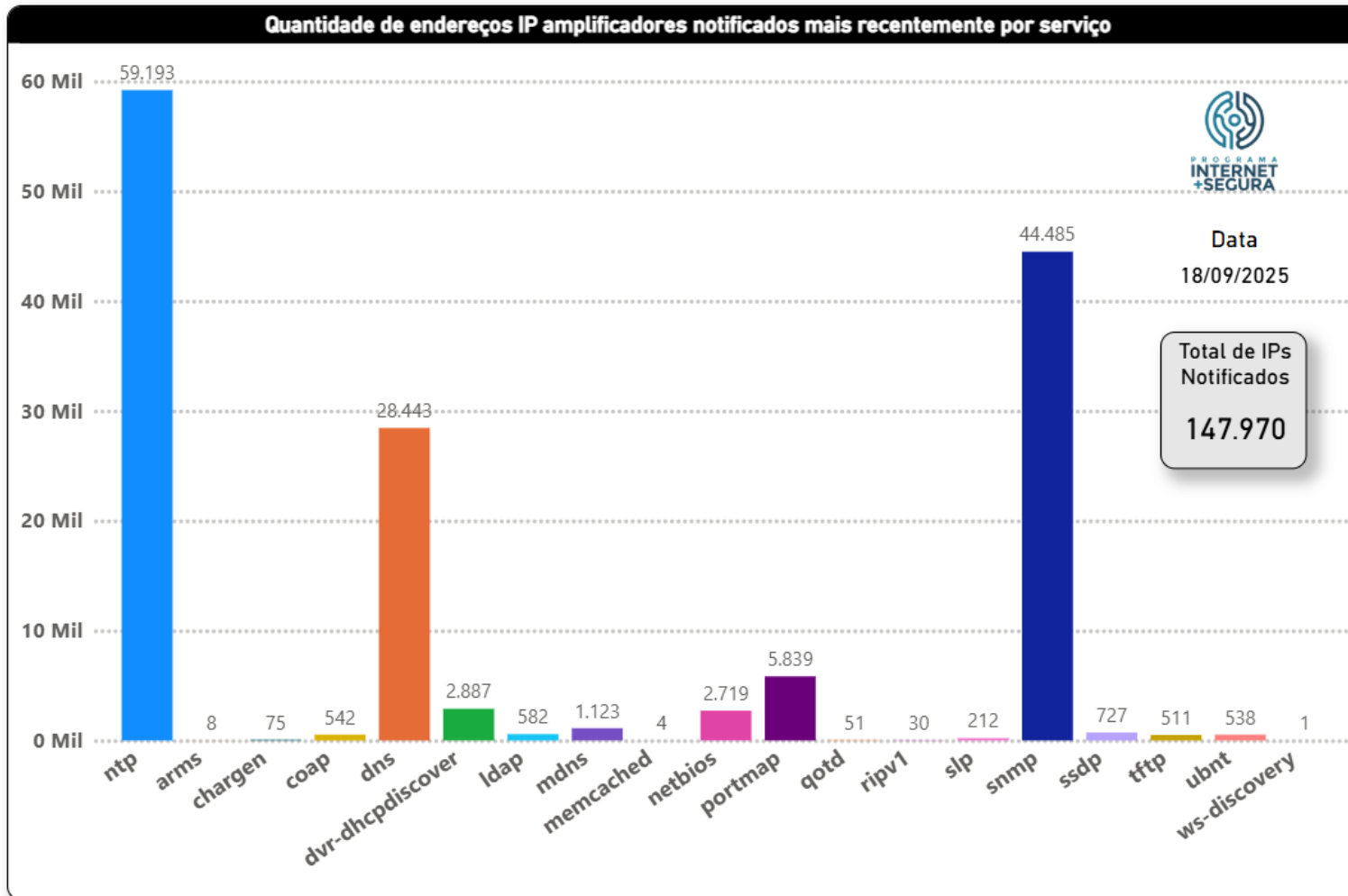
### Brasil

- Início (fev/2018)
  - Endereços IP: 746.508
  - Serviços: 5
- Atual:
  - Endereços IP: 147.970
  - Serviços: 19
  - **Redução de 80%**



# Programa por uma Internet mais Segura

## Notificação de amplificadores - serviços

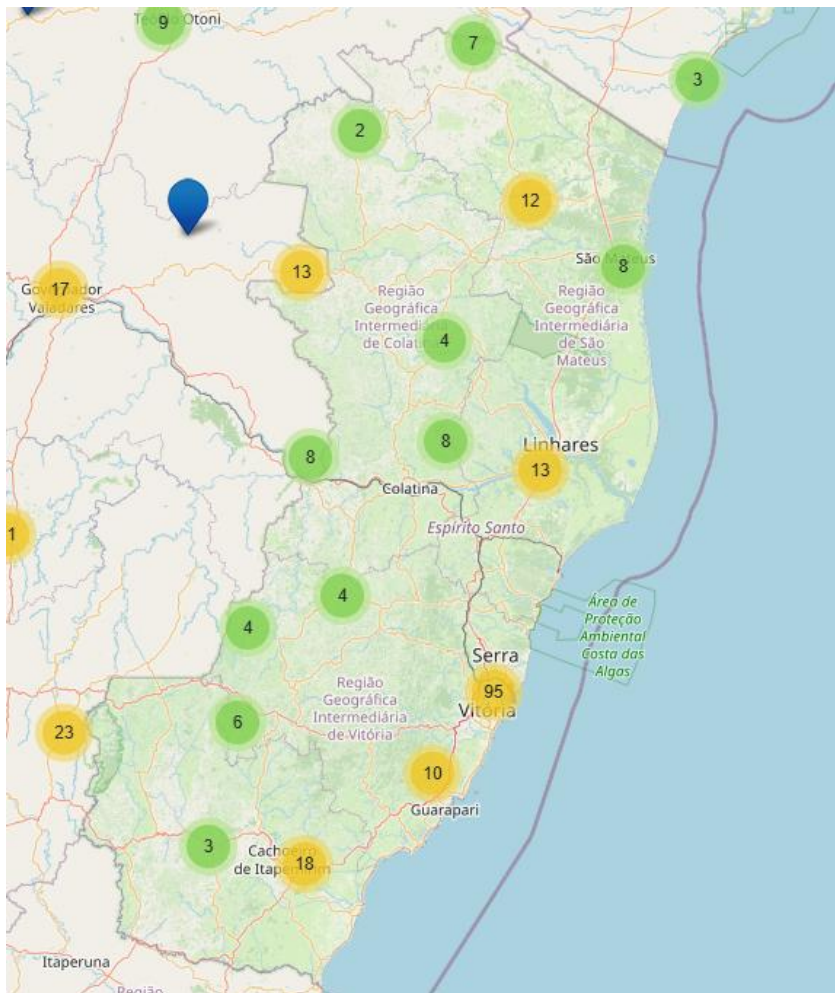


### Brasil

- 9.053 AS
- 5.138 AS notificados
- 147.970 endereços IP mal configurados
- **NTP 59.193**
- **SNMP 44.485**
- **DNS 28.443**

# Programa por uma Internet mais Segura

## Notificação de amplificadores - serviços



### Espírito Santo (206 AS)

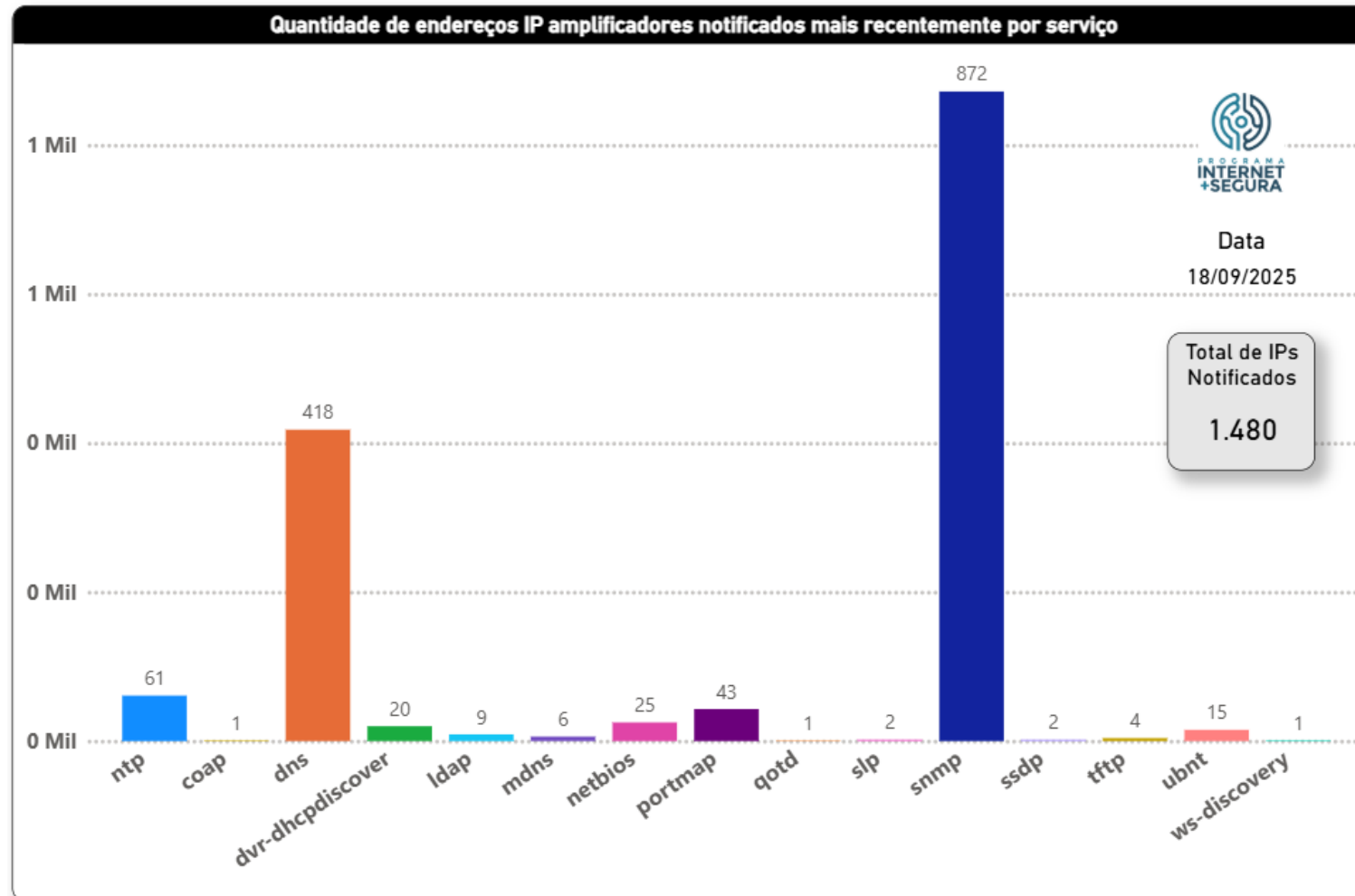
- Serra (30)
- Cariacica (23)
- Vila Velha (23)
- Vitória (18)
- Cachoeiro de Itapemirim (8)
- São Mateus (8)
- Guarapari (7)
- Aracruz (5)
- Baixo Guandu (4)
- Linhares (4)
- Pedro Canário (4)
- Colatina (3)
- Itapemirim (3)
- Nova Venécia (3)
- Rio Bananal (3)
- São Gabriel da Palha (3)
- Afonso Cláudio (2)

Ref. <https://mapadeas.ceptro.br>



# Programa por uma Internet mais Segura

## Notificação de amplificadores - serviços



### Espírito Santo

- 206 AS
- 92 AS conectados ao IX
- 121 AS notificados
- 1 AS com mais de 300 IP notificados
- 1.480 endereços IP mal configurados
  - DNS 418
  - SNMP 872
  - NTP 61



# MANRS

## Mutually Agreed Norms for Routing Security

<http://manrs.org>

<https://bcp.nic.br/i+seg/acoes/manrs/>



# Programa por uma Internet mais Segura



## Boas práticas de roteamento global

- MANRS - Internet Society (trocadilho em inglês)
- BGP é inseguro!
- Filtros BGP
- Filtro Anti Spoofing (endereço de origem)
- Pontos de contato de segurança no Peering DB, whois, IRR
- Cadastro da política de roteamento no IRR e RPKI



MANRS

<https://bcp.nic.br/i+seg/acoes/manrs/>



# Programa por uma Internet mais Segura

## Sequestro de prefixos (Hijacking)

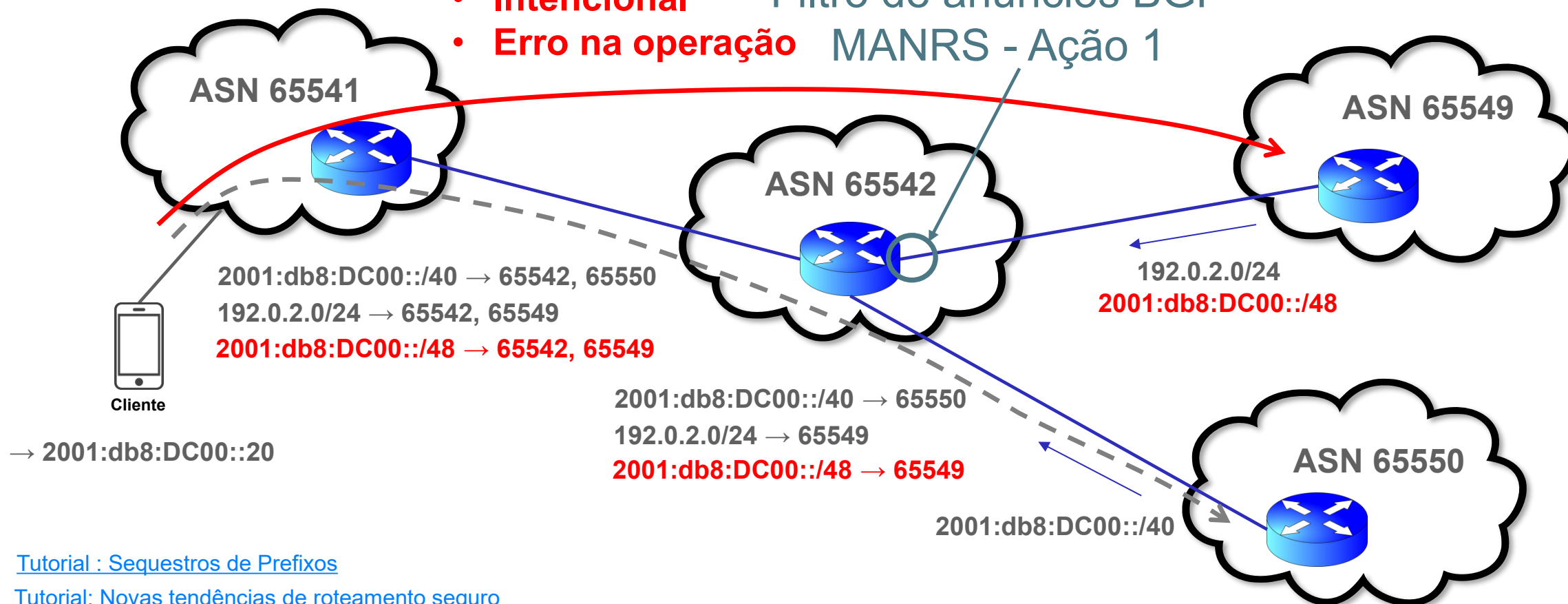
### Anúncio de prefixos não autorizados:

- Intencional

Filtro de anúncios BGP

- Erro na operação

MANRS - Ação 1



[Tutorial : Sequestros de Prefixos](#)

[Tutorial: Novas tendências de roteamento seguro](#)

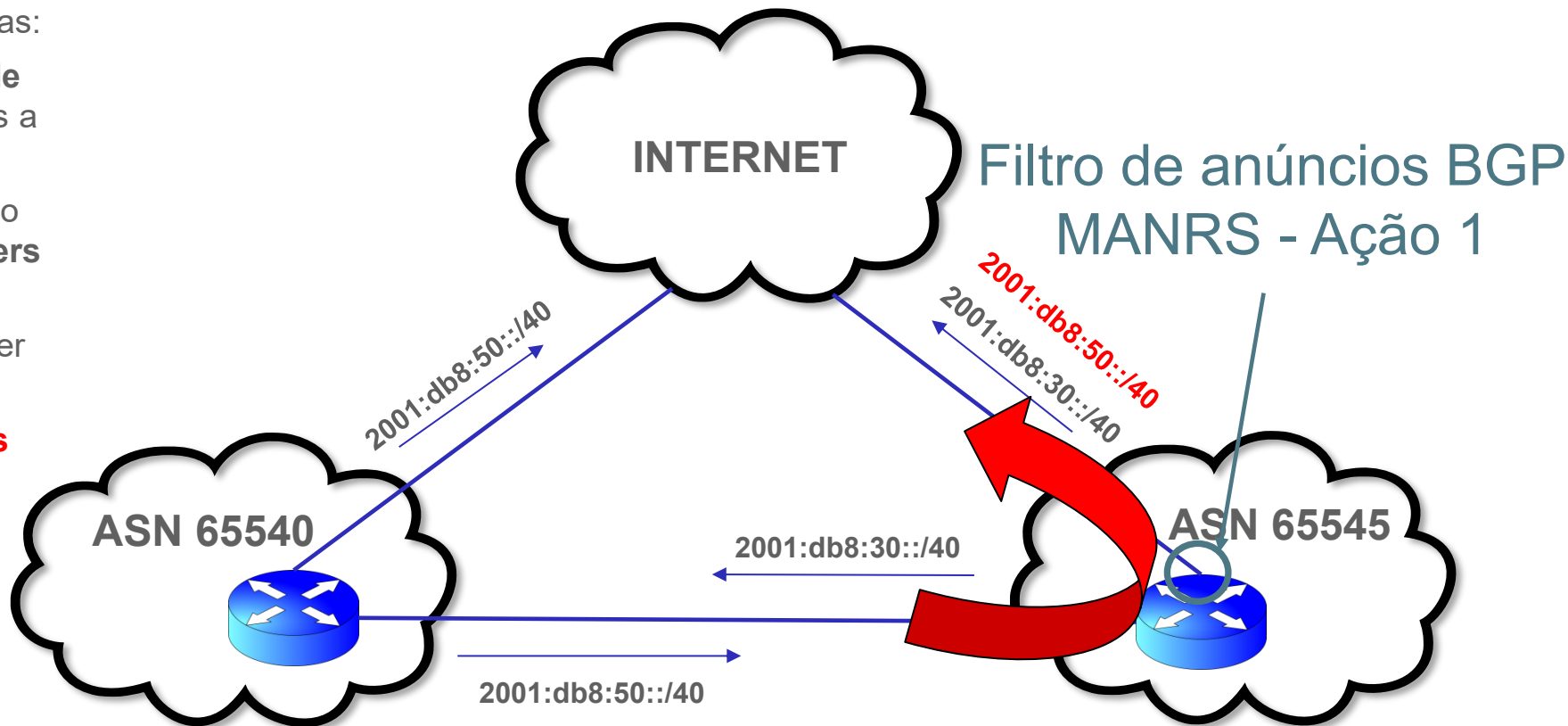


# Programa por uma Internet mais Segura

## Vazamento de rotas (Route Leak)

- Algumas **regras** devem ser cumpridas:
- Prefixos aprendidos do **provedor de trânsito** não devem ser anunciados a **outro provedor** ou a **peer** da rede
- Prefixos aprendidos de um **peer** não devem ser anunciados a outros **peers** nem ao **provedor de trânsito**
- Estes prefixos somente deveriam ser **anunciados a clientes**
- **Se as regras não forem cumpridas pode ocorrer vazamento de rotas**

**Leak!**  
**Normalmente são**  
**erros operacionais**





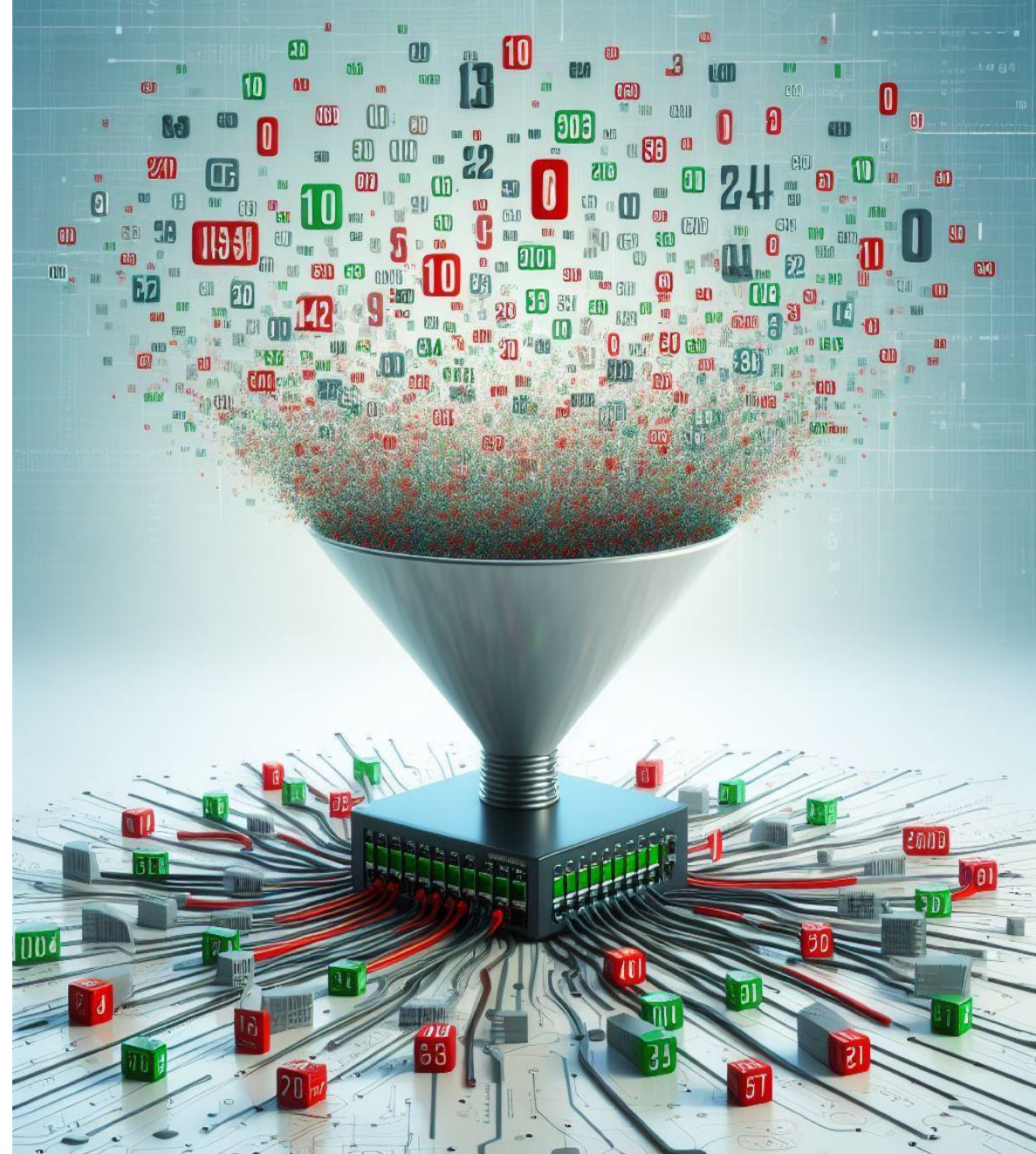
# Programa por uma Internet mais Segura



## MANRS - Ação 1 - Impedir a propagação de informações incorretas no BGP

- Implemente filtros no BGP para os seus prefixos e dos seus clientes

<https://bcp.nic.br/i+seg/acoes/manrs/#filtragem-de-rotas>





# Programa por uma Internet mais Segura



## MANRS - Ação 2 - Filtro Anti-spoofing

- Bloqueie pacotes com **origem** em IPs diferentes daqueles do seu bloco, eles **não podem sair de sua rede** (não podem ser originados na sua rede)!



<https://bcp.nic.br/antispoofing/>





# Programa por uma Internet mais Segura



## MANRS - Ação 3 - Pontos de Contato

- Contatos de roteamento e abuse no Registro.br devem estar atualizados e serem de grupos de pessoas. Ex.: [noc@seuprovedor.com.br](mailto:noc@seuprovedor.com.br)
- Registro.br está validando os e-mails de abuse e a não resposta pode causar a **recuperação** (perda) dos endereços IP
- Mensagens do CERT.br estão indo para o SPAM em alguns casos!
- Atualizar contatos no **PeeringDB** e **IRR**



MANRS

<https://bcp.nic.br/i+seg/acoes/manrs/#coordenacao>



# Programa por uma Internet mais Segura



## MANRS - Ação 4 - Cadastro da Política de Roteamento

- IRR - Internet Routing Registry
  - RADB
  - TC (gratuito)

Desafio BCOP

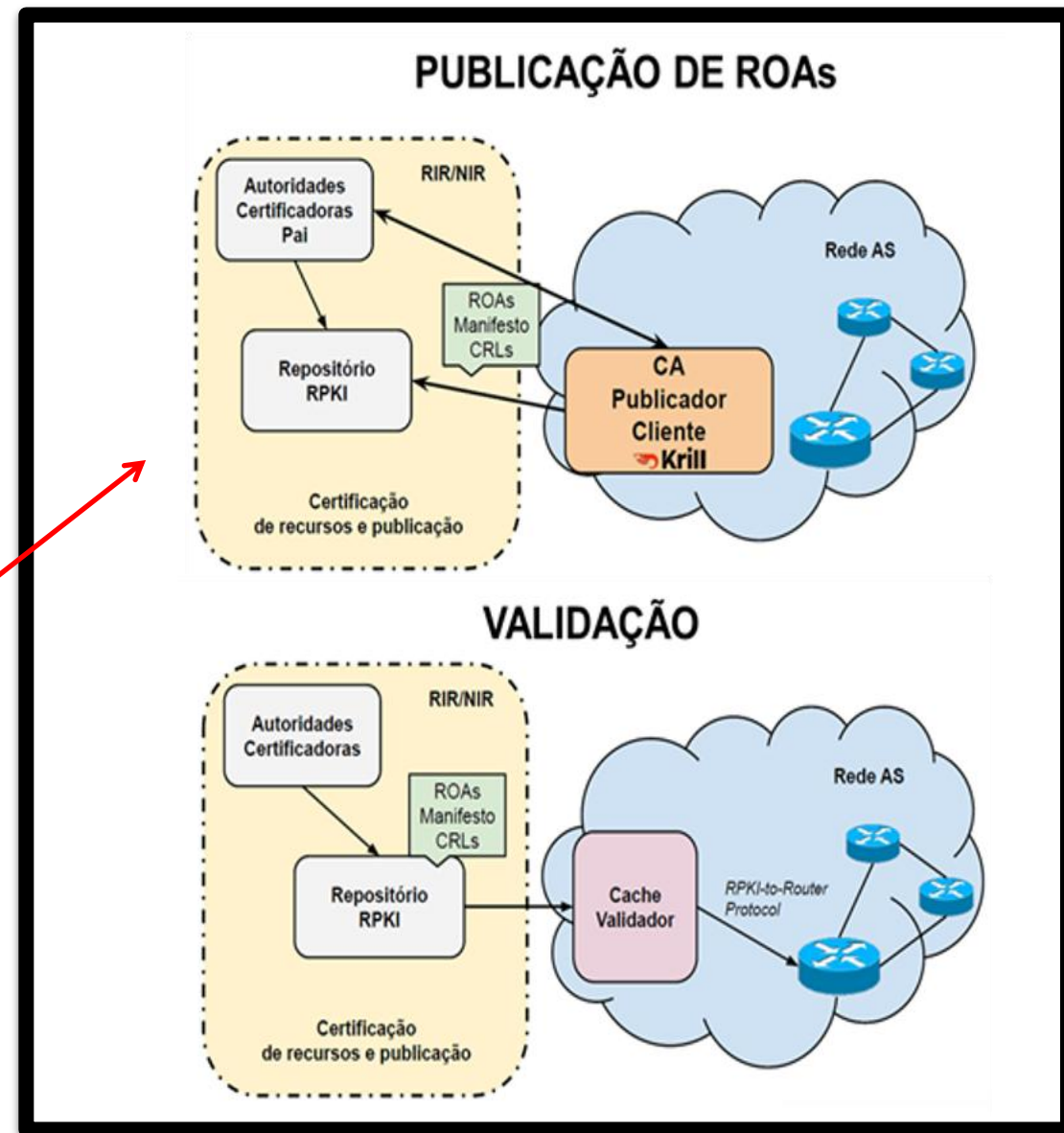
- RPKI - Resource Public Key Infrastructure

<https://bcp.nic.br/i+seg/acoes/>



Tutorial: [IRR na prática](#)

Tutorial: [Segurança no roteamento com RPKI](#)





# Programa por uma Internet mais Segura



## MANRS Observatory - Espírito Santo - 201 AS

Resumo

21-out-25



### MANRS - Status da Segurança de Roteamento

#### Incidentes

|                   |   |
|-------------------|---|
| Sequestro de Rota | 0 |
| Vazamento de Rota | 0 |
| Anúncio inválido  | 0 |
| Total             | 0 |

■ Sequestro de Rota ■ Vazamento de Rota  
■ Anúncio inválido

#### Responsáveis

|                 |   |
|-----------------|---|
| AS responsáveis | 0 |
|-----------------|---|

■ AS responsáveis

#### Informação de Roteamento

##### IRR

|                |       |       |
|----------------|-------|-------|
| Não registrado | 30    | 1,3%  |
| Registrado     | 2.193 | 98,7% |



■ Não registrado ■ Registrado

##### RPKI

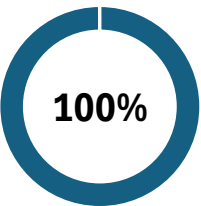
|              |       |       |
|--------------|-------|-------|
| Válido       | 912   | 41,0% |
| Desconhecido | 1.310 | 58,9% |
| Inválido     | 1     | 0,0%  |



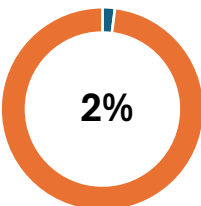
■ Válido ■ Desconhecido ■ Inválido

### MANRS - Prontidão

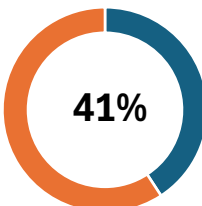
#### Filtros BGP



#### Anti-spoofing

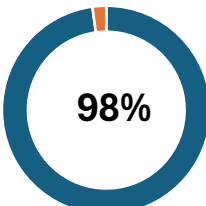


#### Coordenação

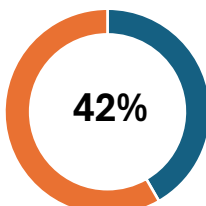


#### Informação de Roteamento

##### IRR



##### RPKI



# Programa por uma Internet mais Segura

## MANRS Observatory - 201 AS – ES

| ASN     | Holder | Country | UN Regions | UN Sub-Regions                  | RIR Regions | Filtering | Anti-spoofing | Coordination | Routing Information (IRR) | Routing Information (RPKI) | Participante MANRS | Status abuse  | Status Notificações CERT.br |
|---------|--------|---------|------------|---------------------------------|-------------|-----------|---------------|--------------|---------------------------|----------------------------|--------------------|--------------------------------------------------------------------------------------------------|-----------------------------|
| ASN 2   | ---    | BR      | Americas   | Latin America and the Caribbean | LACNIC      | 100%      | 0%            | 100%         | 100%                      | 0%                         |                    | PEND                                                                                             |                             |
| ASN 36  | ---    | BR      | Americas   | Latin America and the Caribbean | LACNIC      | 100%      | 0%            | 100%         | 100%                      | 0%                         |                    | PEND                                                                                             |                             |
| ASN 40  | ---    | BR      | Americas   | Latin America and the Caribbean | LACNIC      | 100%      | 0%            | 0%           | 100%                      | 0%                         |                    | PEND                                                                                             |                             |
| ASN 47  | ---    | BR      | Americas   | Latin America and the Caribbean | LACNIC      | 100%      | 0%            | 100%         | 100%                      | 100%                       |                    | PEND                                                                                             |                             |
| ASN 50  | ---    | BR      | Americas   | Latin America and the Caribbean | LACNIC      | 100%      | 0%            | 0%           | 100%                      | 0%                         |                    | BLOCK                                                                                            |                             |
| ASN 56  | ---    | BR      | Americas   | Latin America and the Caribbean | LACNIC      | 100%      | 0%            | 100%         | 100%                      | 100%                       |                    | PEND                                                                                             |                             |
| ASN 65  | ---    | BR      | Americas   | Latin America and the Caribbean | LACNIC      | 100%      | 0%            | 0%           | 100%                      | 0%                         |                    | PEND                                                                                             |                             |
| ASN 84  | ---    | BR      | Americas   | Latin America and the Caribbean | LACNIC      | 100%      | 0%            | 100%         | 100%                      | 0%                         |                    | PEND                                                                                             |                             |
| ASN 92  | ---    | BR      | Americas   | Latin America and the Caribbean | LACNIC      | 100%      | 0%            | 100%         | 100%                      | 0%                         |                    | PEND                                                                                             |                             |
| ASN 98  | ---    | BR      | Americas   | Latin America and the Caribbean | LACNIC      | 100%      | 0%            | 100%         | 100%                      | 100%                       |                    | PEND                                                                                             |                             |
| ASN 101 | ---    | BR      | Americas   | Latin America and the Caribbean | LACNIC      | 100%      | 0%            | 0%           | 100%                      | 0%                         |                    | PEND                                                                                             |                             |
| ASN 104 | ---    | BR      | Americas   | Latin America and the Caribbean | LACNIC      | 100%      | 0%            | 100%         | 100%                      | 0%                         |                    | PEND                                                                                             |                             |
| ASN 107 | ---    | BR      | Americas   | Latin America and the Caribbean | LACNIC      | 100%      | 0%            | 0%           | 100%                      | 100%                       |                    | PEND                                                                                             |                             |
| ASN 113 | ---    | BR      | Americas   | Latin America and the Caribbean | LACNIC      | 100%      | 0%            | 0%           | 100%                      | 0%                         |                    | PEND                                                                                             |                             |
| ASN 120 | ---    | BR      | Americas   | Latin America and the Caribbean | LACNIC      | 100%      | 0%            | 0%           | 100%                      | 100%                       |                    | PEND                                                                                             |                             |
| ASN 125 | ---    | BR      | Americas   | Latin America and the Caribbean | LACNIC      | 100%      | 0%            | 100%         | 100%                      | 100%                       |                    | PEND                                                                                             |                             |
| ASN 137 | ---    | BR      | Americas   | Latin America and the Caribbean | LACNIC      | 100%      | 0%            | 100%         | 100%                      | 100%                       |                    | PEND                                                                                             |                             |
| ASN 167 | ---    | BR      | Americas   | Latin America and the Caribbean | LACNIC      | 100%      | 0%            | 0%           | 100%                      | 0%                         |                    | PEND                                                                                             |                             |
| ASN 175 | ---    | BR      | Americas   | Latin America and the Caribbean | LACNIC      | 100%      | 0%            | 0%           | 100%                      | 0%                         |                    | BLOCK                                                                                            |                             |
| ASN 178 | ---    | BR      | Americas   | Latin America and the Caribbean | LACNIC      | 100%      | 0%            | 0%           | 100%                      | 0%                         |                    | PEND                                                                                             |                             |
| ASN 183 | ---    | BR      | Americas   | Latin America and the Caribbean | LACNIC      | 100%      | 0%            | 0%           | 100%                      | 0%                         |                    | PEND                                                                                             |                             |
| ASN 189 | ---    | BR      | Americas   | Latin America and the Caribbean | LACNIC      | 100%      | 0%            | 0%           | 100%                      | 0%                         |                    | BLOCK                                                                                            |                             |
| ASN 196 | ---    | BR      | Americas   | Latin America and the Caribbean | LACNIC      | 100%      | 0%            | 0%           | 100%                      | 0%                         |                    | PEND                                                                                             |                             |
| ASN 200 | ---    | BR      | Americas   | Latin America and the Caribbean | LACNIC      | 100%      | 0%            | 0%           | 0%                        | 0%                         |                    | PEND                                                                                             |                             |



# Programa por uma Internet mais Segura



## Participantes por país

- Total: 1.087
- Participantes no Brasil → 311



MANRS

2024 → 292

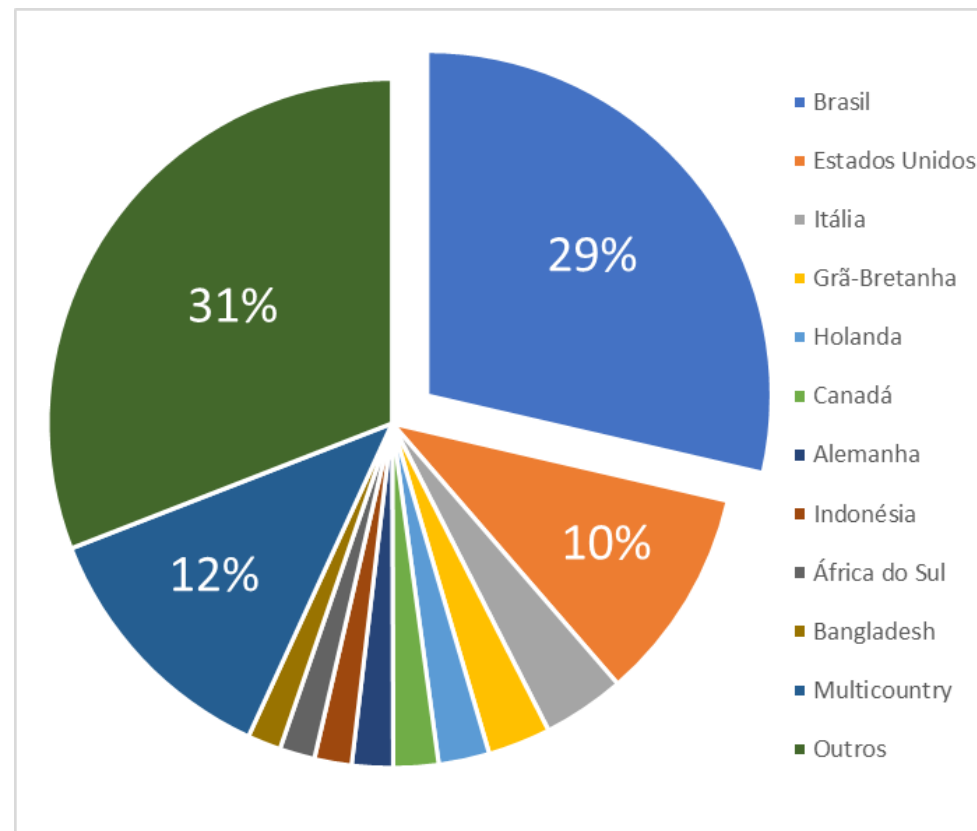
2023 → 258

2022 → 206

2021 → 174

2020 → 140

## % de Participantes



Fonte: <https://www.manrs.org/netops/participants/> Acesso 01/09/25

# Programa por uma Internet mais Segura

## MANRS Observatory - 201 AS – ES

| ASN     | Holder | Country | UN Regions | UN Sub-Regions                  | RIR Regions | Filtering | Anti-spoofing | Coordination | Routing Information (IRR) | Routing Information (RPKI) | Participante MANRS | Status abuse-c |
|---------|--------|---------|------------|---------------------------------|-------------|-----------|---------------|--------------|---------------------------|----------------------------|--------------------|----------------|
| ASN 19  | ---    | BR      | Americas   | Latin America and the Caribbean | LACNIC      | 100%      | 0%            | 100%         | 100%                      | 100%                       | 61583              | OK             |
| ASN 46  | ---    | BR      | Americas   | Latin America and the Caribbean | LACNIC      | 100%      | 0%            | 100%         | 100%                      | 0%                         | 263462             | OK             |
| ASN 58  | ---    | BR      | Americas   | Latin America and the Caribbean | LACNIC      | 100%      | 0%            | 100%         | 100%                      | 0%                         | 264297             | OK             |
| ASN 62  | ---    | BR      | Americas   | Latin America and the Caribbean | LACNIC      | 100%      | 0%            | 100%         | 100%                      | 100%                       | 264513             | OK             |
| ASN 123 | ---    | BR      | Americas   | Latin America and the Caribbean | LACNIC      | 100%      | 100%          | 100%         | 100%                      | 100%                       | 268235             | OK             |
| ASN 126 | ---    | BR      | Americas   | Latin America and the Caribbean | LACNIC      | 100%      | 0%            | 100%         | 100%                      | 0%                         | 268377             | OK             |
| ASN 128 | ---    | BR      | Americas   | Latin America and the Caribbean | LACNIC      | 100%      | 0%            | 100%         | 100%                      | 100%                       | 268508             | OK             |



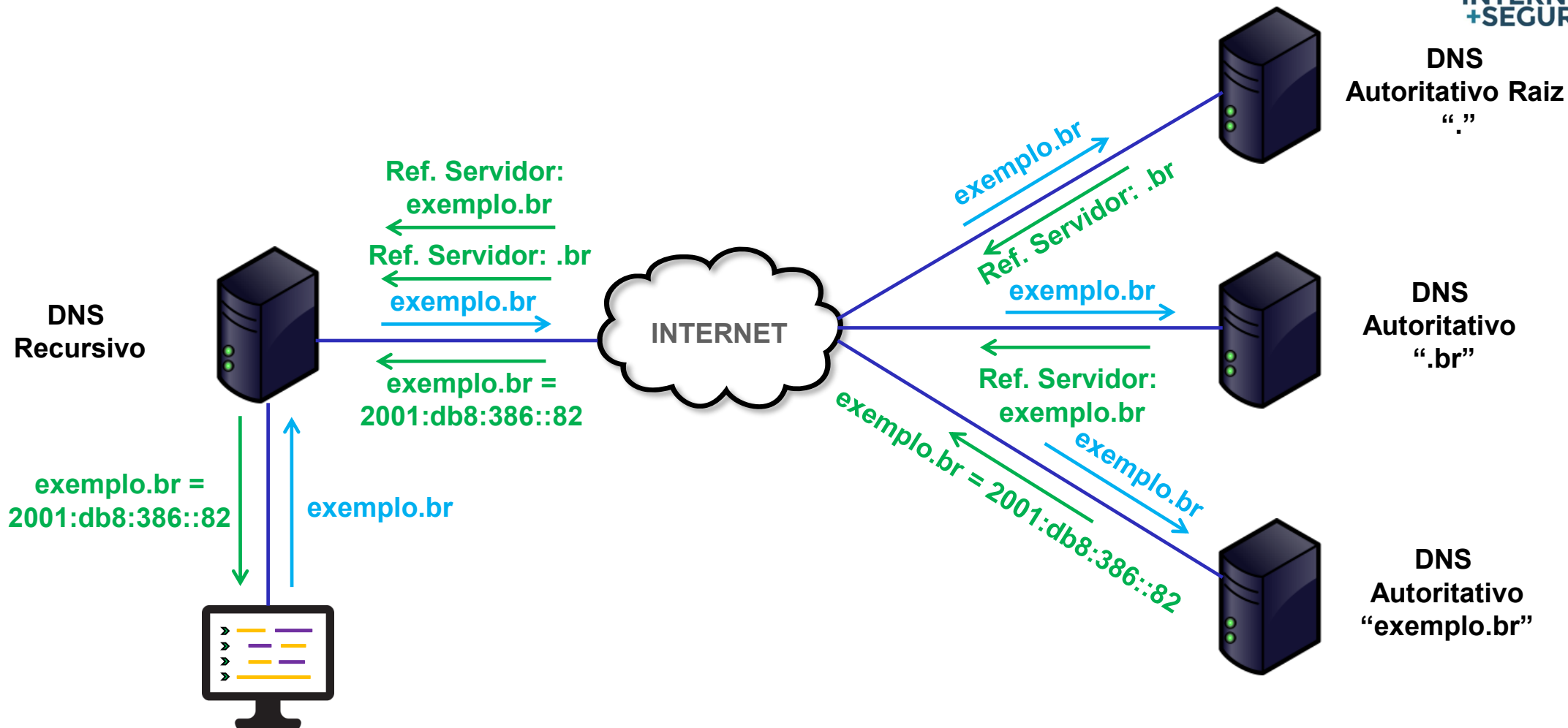


Stands for **K**nowledge-Sharing and  
**I**ntantiating **N**orms for **D**NS and **N**aming  
**S**ecurity

<https://kindns.org/>

# Programa por uma Internet mais Segura

## Processo de Recursão DNS



Tutorial: [Configurando o seu DNS de forma simples e segura – Ataque DNS Poisoning](#)

# Programa por uma Internet mais Segura

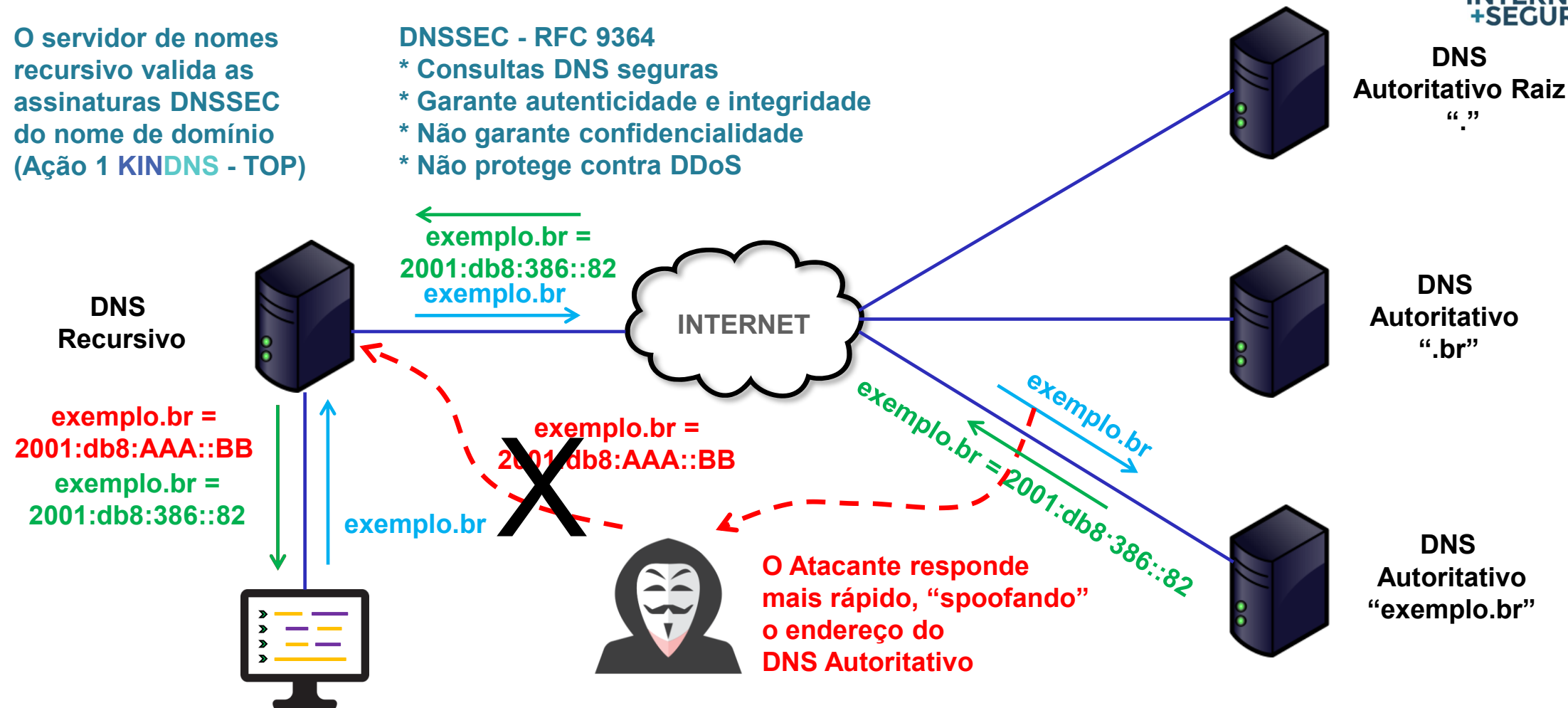
## Ataque DNS - Poisoning



O servidor de nomes recursivo valida as assinaturas DNSSEC do nome de domínio (Ação 1 KINDNS - TOP)

DNSSEC - RFC 9364

- \* Consultas DNS seguras
- \* Garante autenticidade e integridade
- \* Não garante confidencialidade
- \* Não protege contra DDoS



Tutorial: [Configurando o seu DNS de forma simples e segura – Ataque DNS Poisoning](#)





# Programa por uma Internet mais Segura



## Boas práticas para DNS

- KinDNS da ICANN (trocadilho em inglês)
- Configuração correta do recursivo somente para seus usuários
- Validação do DNSSEC no recursivo
- Configuração do autoritativo do seu nome de domínio com DNSSEC

<https://kindns.org/>

Tutorial: [Configurando o seu DNS de forma simples e segura](#)





<https://top.nic.br>



The screenshot shows the TOP website with a header containing the logo and navigation links. The main content area features a introductory text and three test modules: Site, E-mail, and IPv6/DNSSEC. Each module includes a description, a text input field for a domain, and a button to start the test. The URL <https://top.nic.br> is displayed at the bottom.

**TOP**  
TESTE OS PADRÕES

Quem é TOP Sobre Referências Comunicados

Os padrões técnicos modernos de Internet aumentam a confiabilidade e permitem o crescimento da rede. Você está usando esses padrões?

**Teste TOP - Site**  
Endereço IP moderno?  
Domínio assinado? Conexão segura? Opções de segurança?

Nome de domínio do seu site:

Iniciar o teste

**Teste TOP - E-mail**  
Endereço IP moderno?  
Domínio assinado? Proteção contra phishing? Conexão segura?

Nome de domínio do seu e-mail:

Iniciar o teste

**Teste TOP - IPv6 e DNSSEC da sua rede**  
Endereços modernos acessíveis? Assinaturas de domínio validadas?

Iniciar o teste

<https://top.nic.br>

# Programa por uma Internet mais Segura



## Teste os padrões

- Teste do DNS recursivo na sua rede (DNSSEC)!
- Teste do IPv6 na sua rede!
- Teste do seu site!
- Teste do seu e-mail!
- Mostra o que está errado e links com informações para corrigir!



# Programa por uma Internet mais Segura

## Testes realizados

- Teste TOP Site ← **Desafio BCOP**
  - IPv6, DNSSEC, HTTPS, Opções de Segurança, RPKI, Security.txt (RFC 9116)
- Teste TOP E-mail
  - IPv6, DNSSEC, STARTTLS, DMARC, RPKI
- Teste TOP IPv6 e DNSSEC do recursivo da sua rede

↖  
**Desafio BCOP**

[Tutorial: Teste para padrões técnicos e modernos de Internet](#)



# Programa por uma Internet mais Segura

## Testes realizados

- Teste TOP Site ← **Desafio BCOP**
  - IPv6, DNSSEC, HTTPS, Opções de Segurança, **RPKI\***, **Security.txt (RFC 9116)\***
- Teste TOP E-mail
  - IPv6, DNSSEC, STARTTLS, DMARC, **RPKI\***
- Teste TOP IPv6 e **DNSSEC** do recursivo da sua rede

\* Novos testes

**Desafio BCOP**

[Tutorial: Teste para padrões técnicos e modernos de Internet](#)

**TOP**  
TESTE OS PADRÕES

Quem é TOP Sobre Referências Comunicados

PROGRAMA INTERNET + SEGURA

Os padrões técnicos modernos de Internet aumentam a confiabilidade e permitem o crescimento da rede. Você está usando esses padrões?

**Teste TOP - Site**  
Endereço IP moderno?  
Domínio assinado? Conexão segura? Opções de segurança?

Nome de domínio do seu site:  
www.exemplo.com.br

Iniciar o teste

**Teste TOP - E-mail**  
Endereço IP moderno?  
Domínio assinado? Proteção contra phishing? Conexão segura?

Nome de domínio do seu e-mail:  
@exemplo.com.br

Iniciar o teste

**Teste TOP - IPv6 e DNSSEC da sua rede**  
Endereços modernos acessíveis? Assinaturas de domínio validadas?

Iniciar o teste

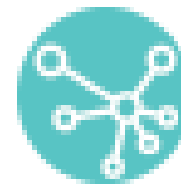
<https://top.nic.br>

# Programa por uma Internet mais Segura

## Implemente as melhores práticas - Selos



MANRS



KINDNS



# Reuniões on-line com os responsáveis pelos AS (KPI)

- Serviços notificados mal configurados \*
- Adoção do MANRS
- Adoção do KINDNS
- Testes do TOP: conexão, site e e-mail

<https://bcp.nic.br/i+seg>

<https://kindns.org/>

<https://top.nic.br>

\* Relatório mensal



# Camada 8 - NIC.br

- Podcast sobre a infraestrutura da Internet
- Edição Novembro/24

<https://www.nic.br/podcasts/camada8/episodio-57>



The image is a promotional graphic for a podcast. It features a man, Gilberto Zorello, with grey hair, wearing a dark blue blazer over a light blue shirt, standing with his arms crossed. He is positioned in the center-right of the frame. The background is a stylized, isometric illustration in shades of blue and teal, depicting a network infrastructure with server racks, data flows, and people working. In the top left corner, the text 'CAMADA 8' is written in a large, white, sans-serif font, with '« nic.br »' in a smaller font below it. In the bottom right corner, the text 'INTERNET MAIS SEGURA' is written in a large, white, sans-serif font, with 'COM GILBERTO ZORELLO, COORDENADOR DE PROJETOS NO NIC.BR' in a smaller font below it. The overall design is modern and tech-oriented.

CAMADA 8  
« nic.br »

INTERNET  
MAIS SEGURA

COM GILBERTO ZORELLO,  
COORDENADOR DE PROJETOS NO NIC.BR

# Programa por uma Internet mais Segura

## APOIO



A CONECTIVIDADE AO SEU ALCANCE





# Obrigado

**Gilberto Zorello**

@ [gzorello@nic.br](mailto:gzorello@nic.br)

22 de outubro de 2025

**nic.br** **cgi.br**

[www.nic.br](http://www.nic.br) | [www.cgi.br](http://www.cgi.br)

