



**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**

# Segurança de Redes

Programa por uma Internet mais segura

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

**IX Fórum Regional - Edição Sudeste - 2024**

Vitória, ES | 28/11/24

**nic.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





# Objetivos do Programa

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

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



PROGRAMA  
**INTERNET  
+SEGURA**

<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

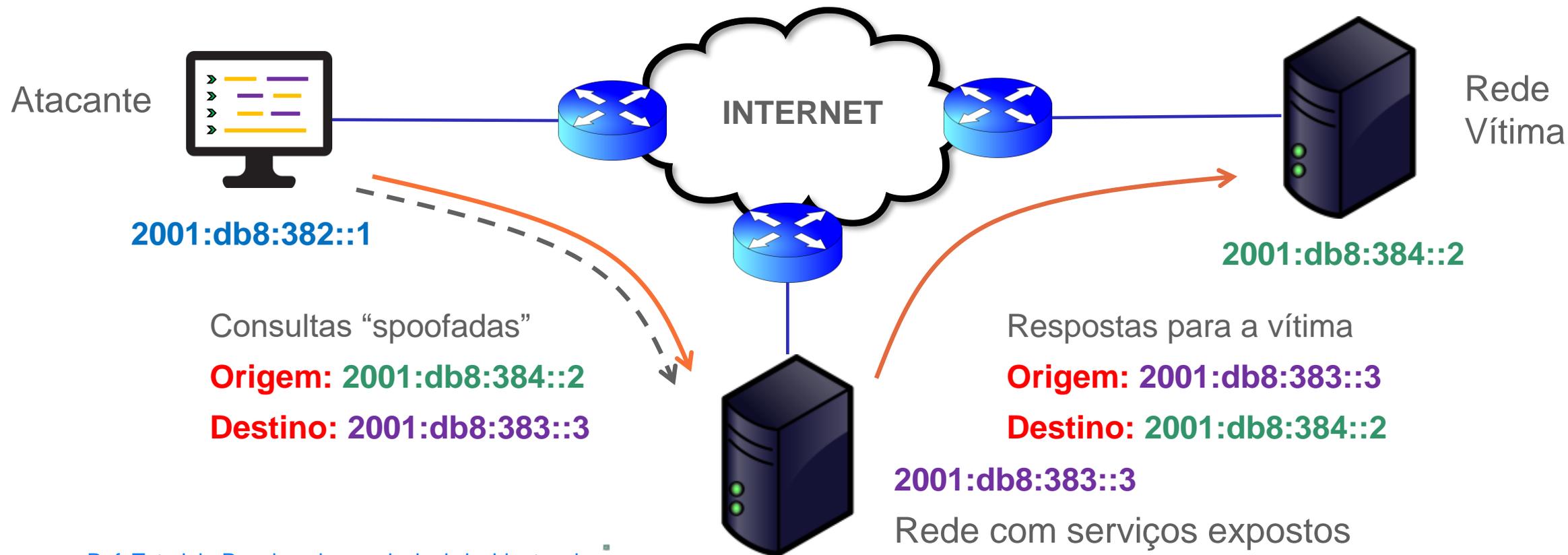
<https://bcp.nic.br/i+seg/acoes/amplificacao/>



# 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

Desafio BCOP 2024

~~Origens falsificadas~~

Atacante



2001:db8:382::1

INTERNET



2001:db8:384::2

~~DNS Recursivo aberto~~

Filtro “antispoofing” - MANRS - Ação 2

- URPF – Unicast Reverse Path Forward
- ACL – Ingress Access List
- SAVI – Source Address Validation Improvement

Configurar serviços corretamente

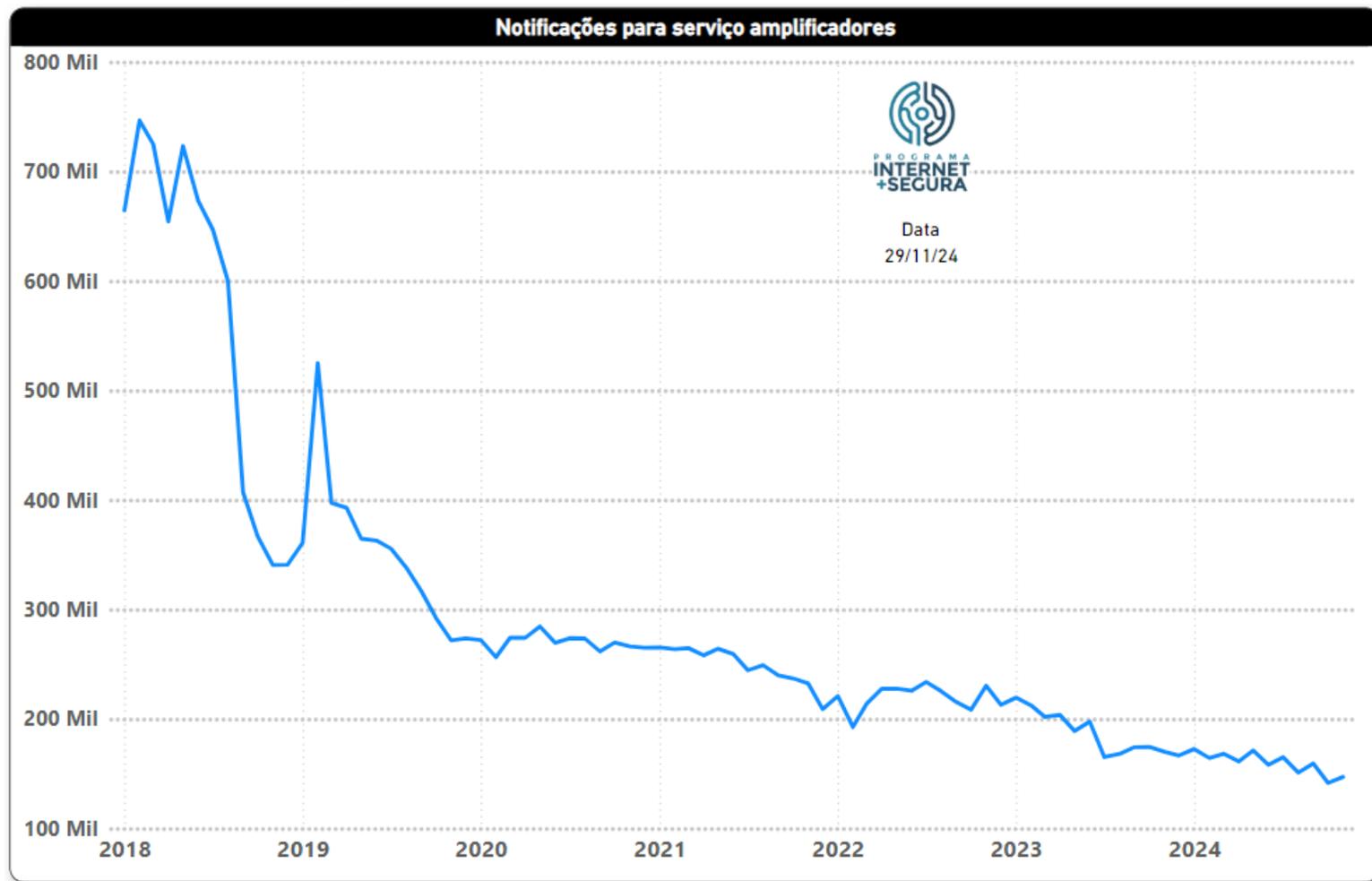
- DNS, SNMP, NTP, PORTMAP, SSDP, NETBIOS, mDNS, DHCPDiscover, entre outros

Atender às notificações do CERT.br

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

# Programa por uma Internet mais Segura

## Notificação de amplificadores - evolução

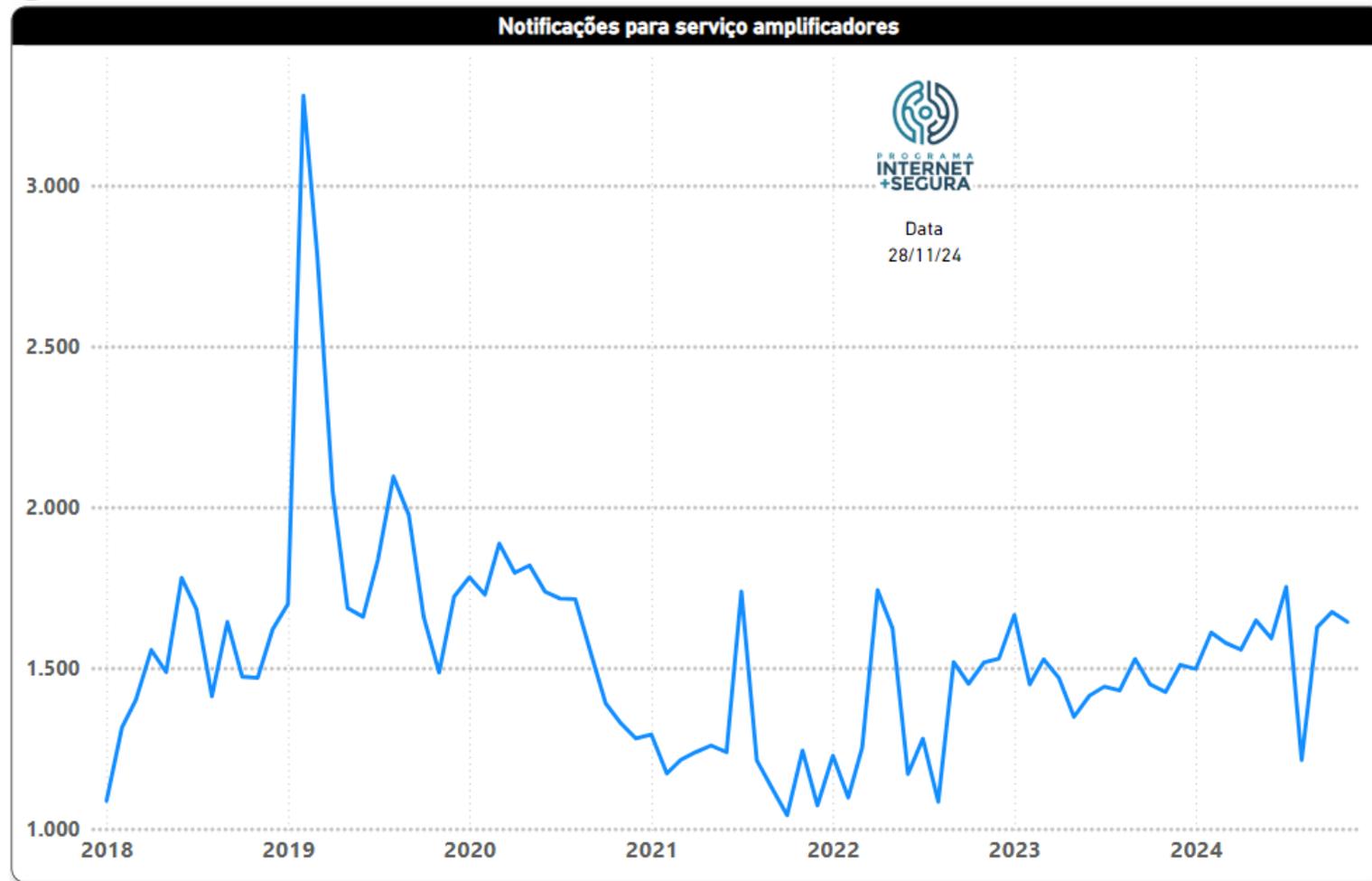


### Brasil

- Início (fev/2018)
  - Endereços IP: 746.508
  - Serviços: 5
- Atual:
  - Endereços IP: 141.557
  - Serviços: 19
  - **Redução de 80%**

# Programa por uma Internet mais Segura

## Notificação de amplificadores - evolução

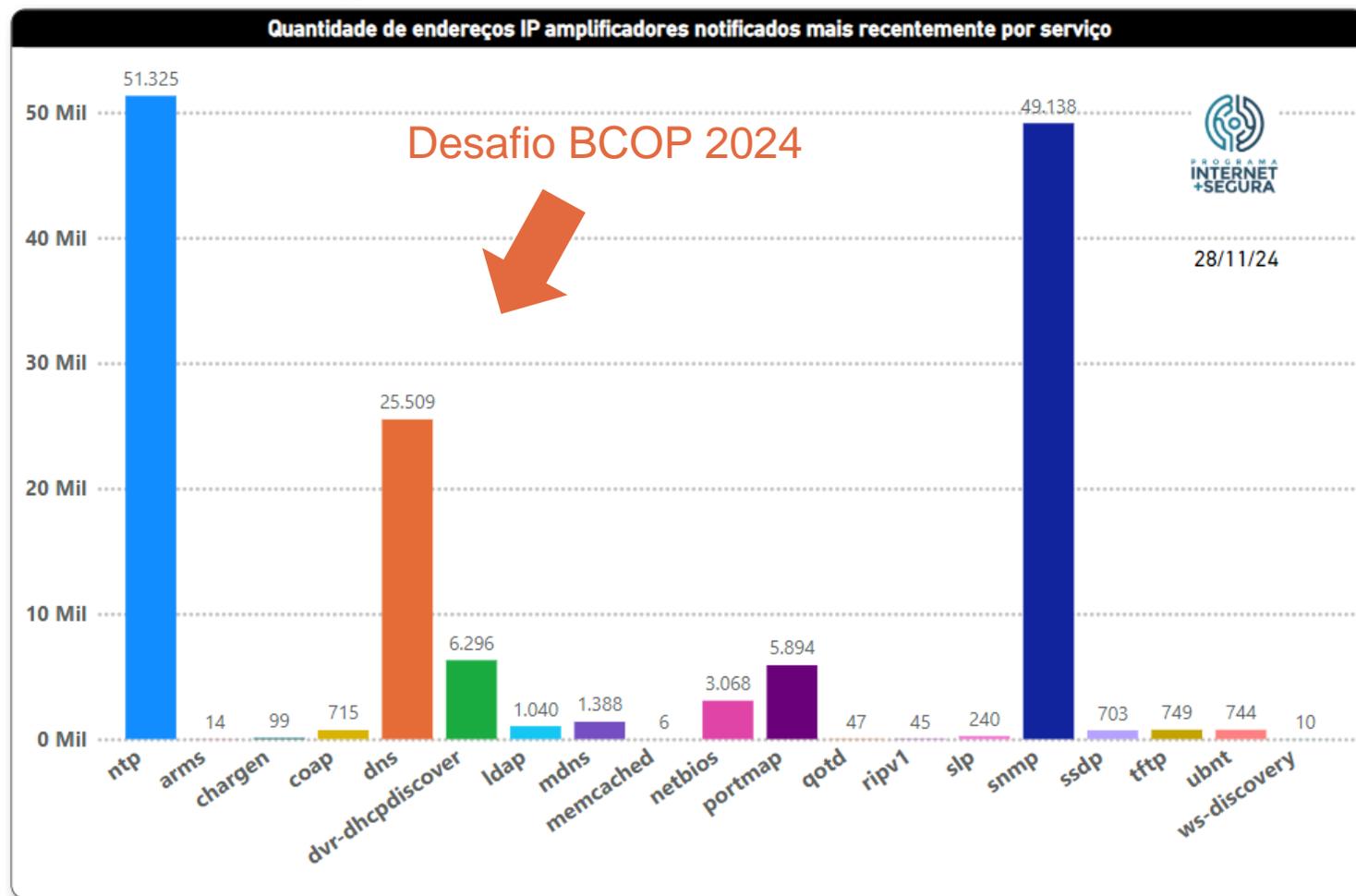


### Participantes IX Vitória

- Pico (fev/2019)
  - Endereços IP: 3.279
  - Serviços: 11
- Atual:
  - Endereços IP: 1.643
  - Serviços: 12

# Programa por uma Internet mais Segura

## Notificação de amplificadores - serviços

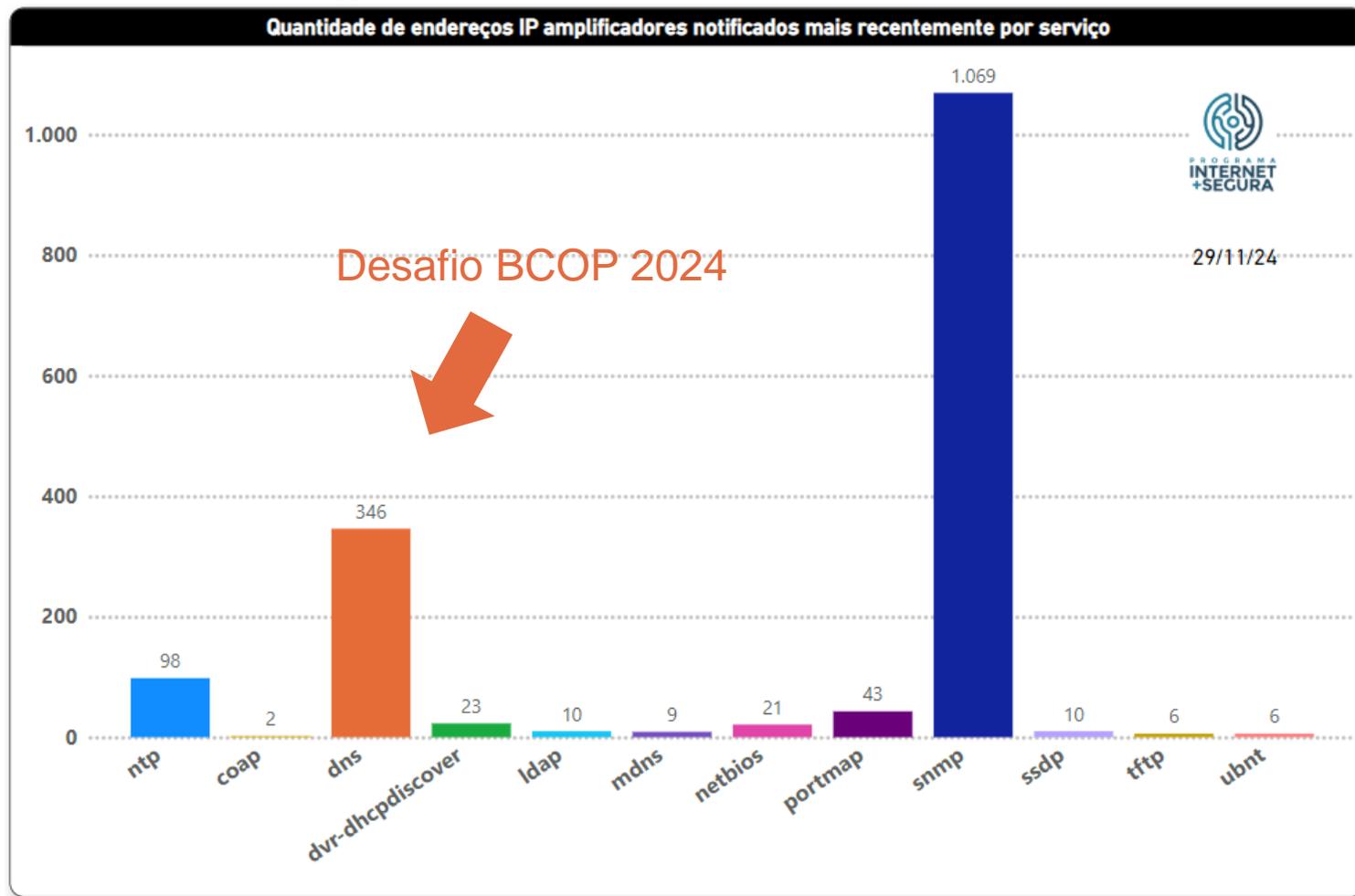


### Brasil

- 5.222 AS notificados
- 141.557 endereços IP mal configurados
- **SNMP 49.138**
- **DNS 25.509**
- **NTP 51.325**

# Programa por uma Internet mais Segura

## Notificação de amplificadores - serviços



### Participantes IX Vitória

- 75 AS participantes (< 400km)
- 57 AS notificados
- 1.643 endereços IP mal configurados
  - **SNMP 1.069**
  - **DNS 346**
  - **NTP 98**



# 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/>

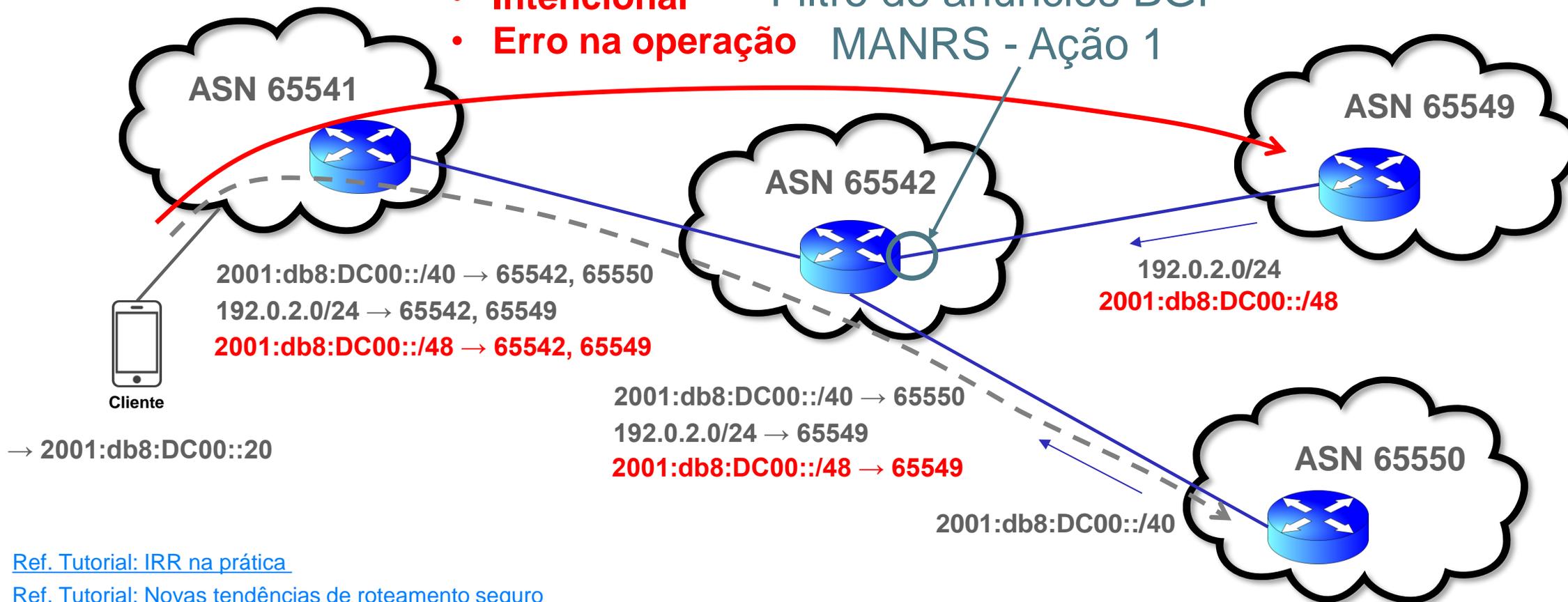


# Programa por uma Internet mais Segura

## Sequestro de prefixos (Hijacking)

**Anúncio de prefixos não autorizados:**

- **Intencional** Filtro de anúncios BGP
- **Erro na operação** MANRS - Ação 1



[Ref. Tutorial: IRR na prática](#)

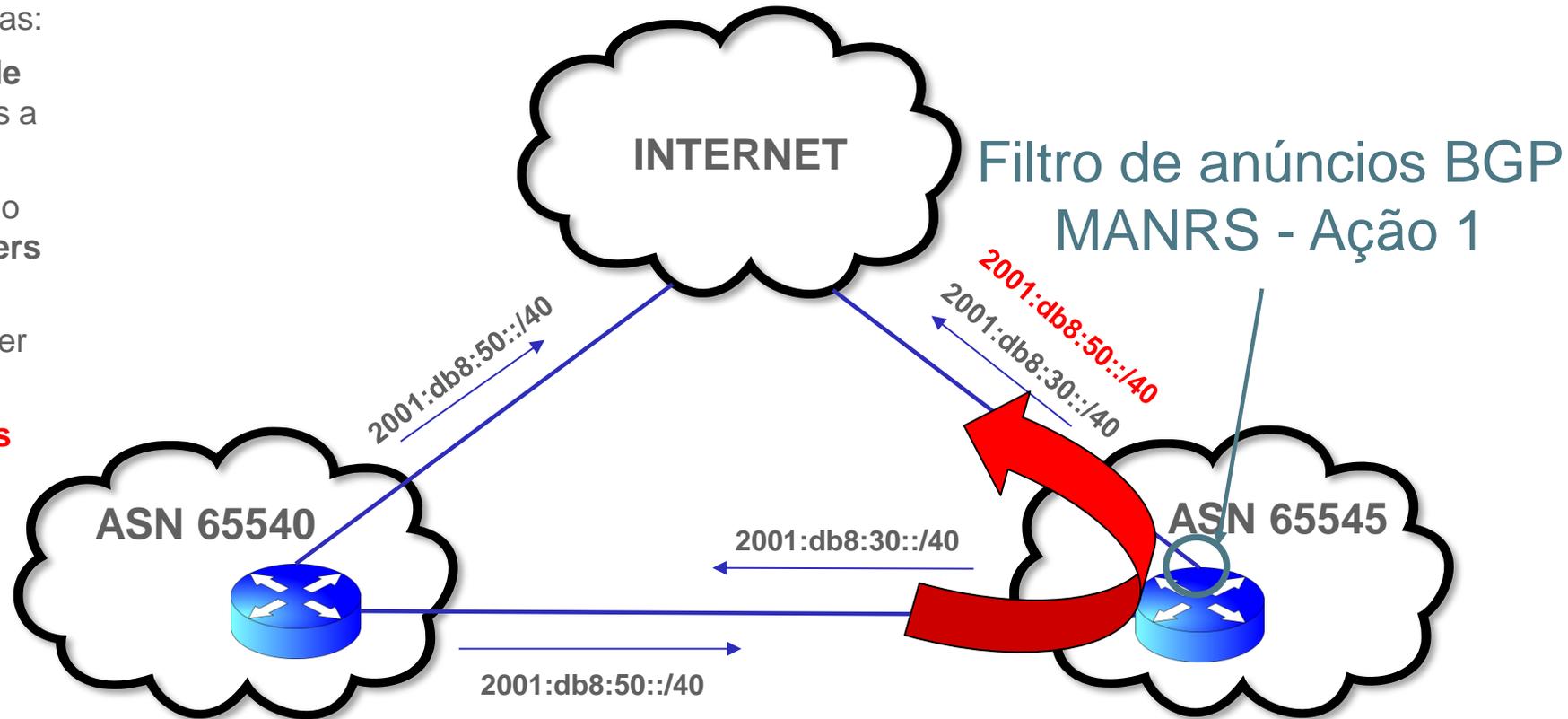
[Ref. Tutorial: Novas tendências de roteamento seguro](#)

# 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



[Ref. Tutorial: IRR na prática](#)

[Ref. Tutorial: novas tendências de roteamento seguro](#)

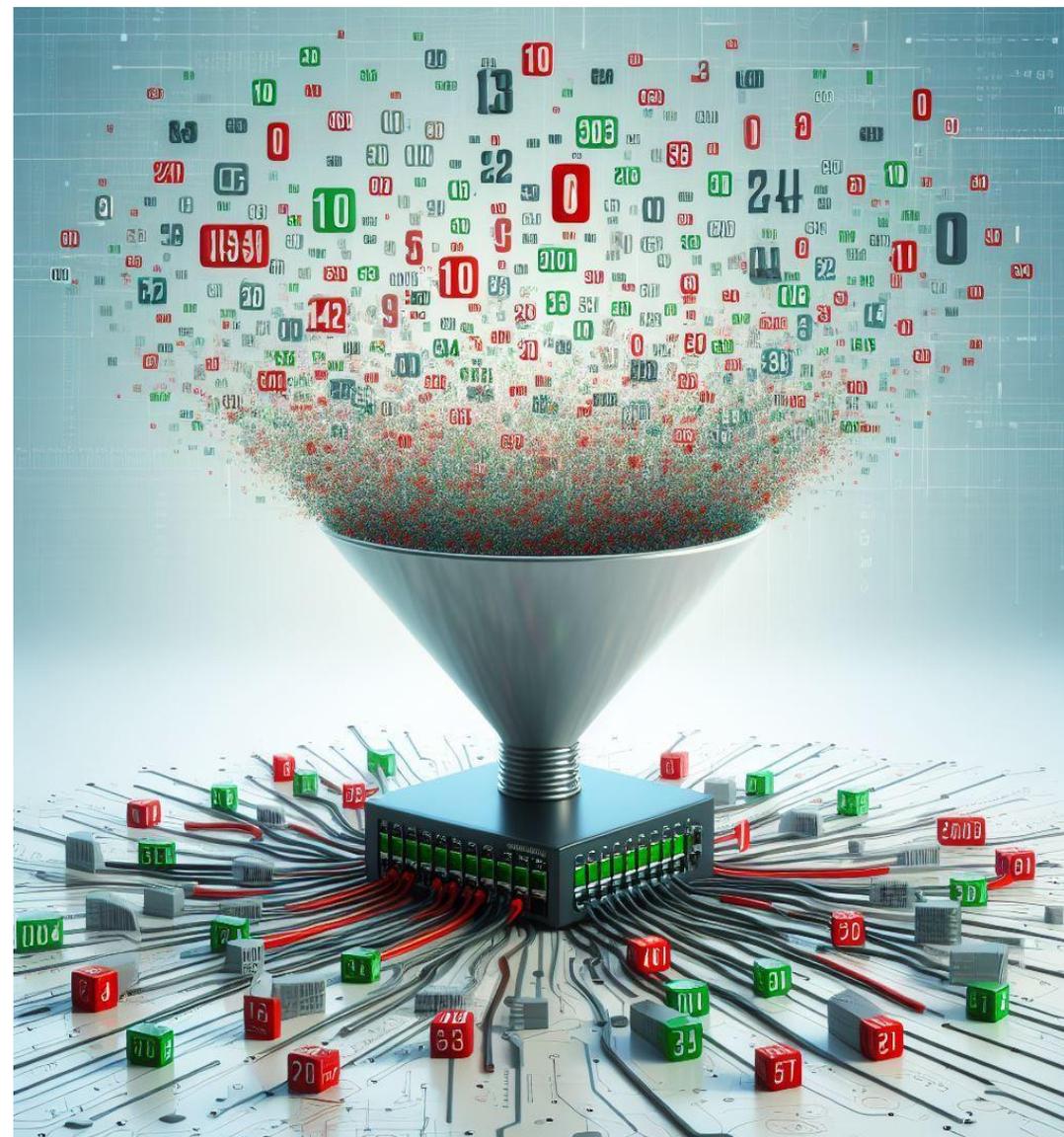
# Programa por uma Internet mais Segura



## 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

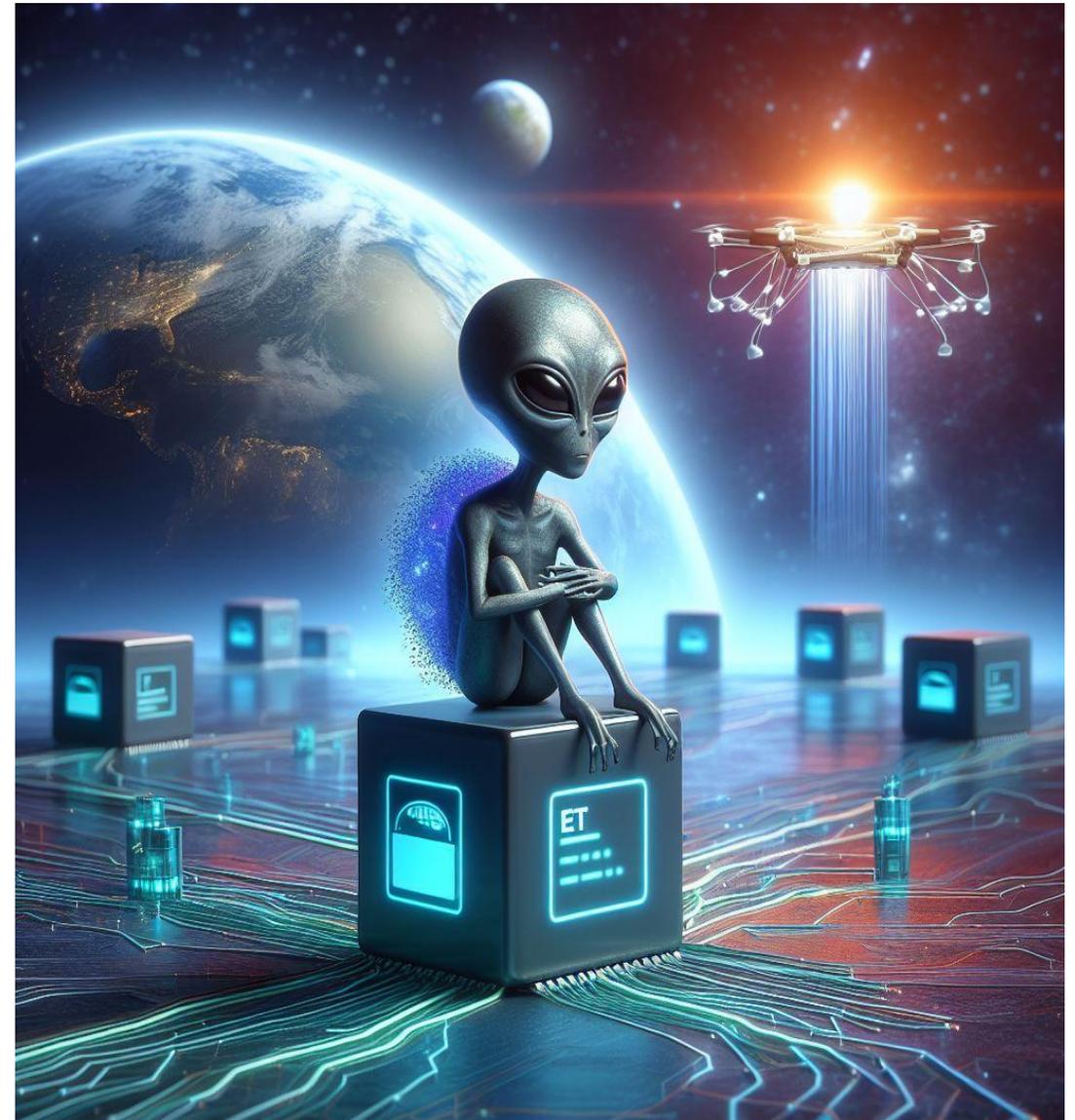


## MANRS - Ação 2 - Filtro Anti Spoofing

- 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



# 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



# Programa por uma Internet mais Segura

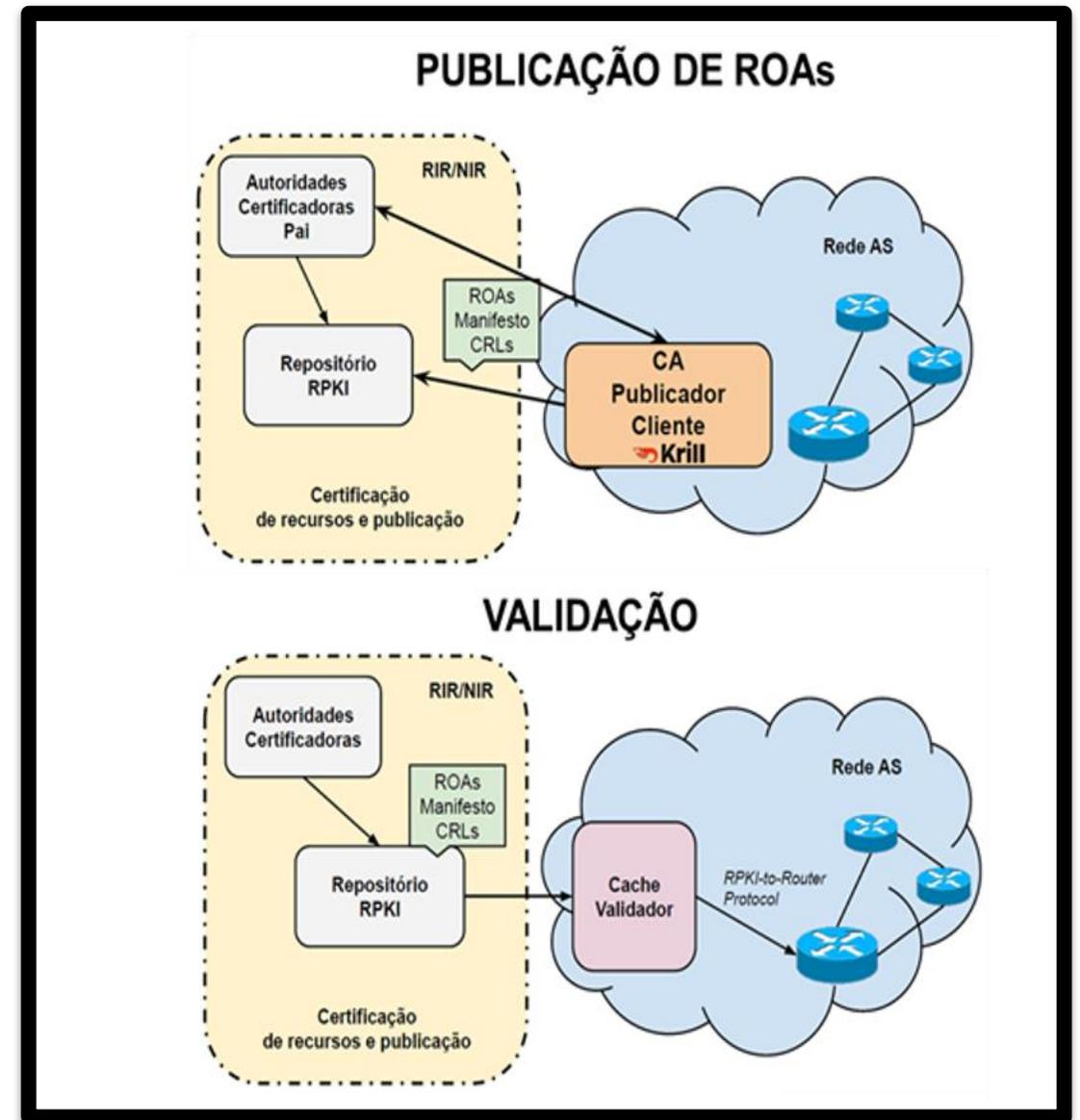


## MANRS - Ação 4 - Cadastro da Política de Roteamento

- **IRR** - Internet Routing Registry
  - RADB
  - TC (gratuito)
- **RPKI** - Resource Public Key Infrastructure



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



# Programa por uma Internet mais Segura

## MANRS Observatory – 75 AS – IX Vitória

### Overview

#### State of Routing Security

Number of incidents, networks involved and quality of published routing information in the IRR and RPKI in the selected region and time period

##### Incidents <sup>1</sup>

Route misoriginations	0
Route leaks	0
Bogon announcements	0
<b>Total</b>	<b>0</b>

##### Culprits <sup>1</sup>

Culprits	0
----------	---

##### Routing Information (IRR) <sup>1</sup>

Unregistered	33	2.6%
Registered	1,234	97.4%



MANRS

Route misoriginations Route leaks Bogon announcements

Culprits

Unregistered Registered

##### Routing Information (RPKI) <sup>1</sup>

Valid	773	61.0%
Unknown	493	38.9%
Invalid	1	0.1%

##### Route Origin Validation <sup>1</sup>

ROV-based Filtering Rate (%)	5.6%
------------------------------	------

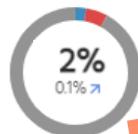
Valid Unknown Invalid

#### MANRS Readiness <sup>1</sup>

##### Filtering <sup>1</sup>



##### Anti-spoofing <sup>1</sup>



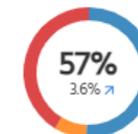
##### Coordination <sup>1</sup>



##### Routing Information (IRR) <sup>1</sup>



##### Routing Information (RPKI) <sup>1</sup>



Ready Aspiring Lagging No Data Available

**Desafio BCOP 2024**

# Programa por uma Internet mais Segura

## MANRS Observatory – 75 AS – IX Vitória

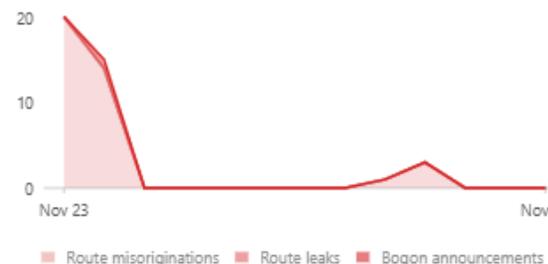
### History

November 2023 - November 2024

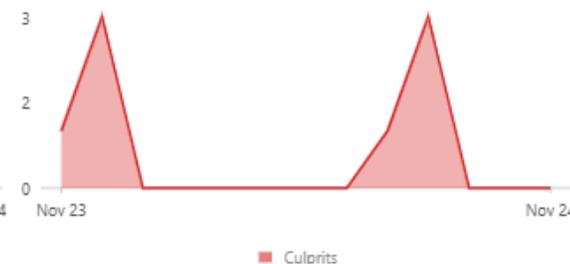


MANRS

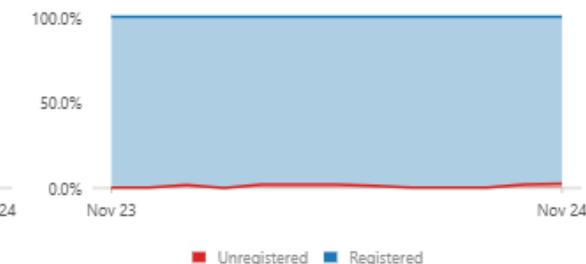
#### Incidents <sup>i</sup>



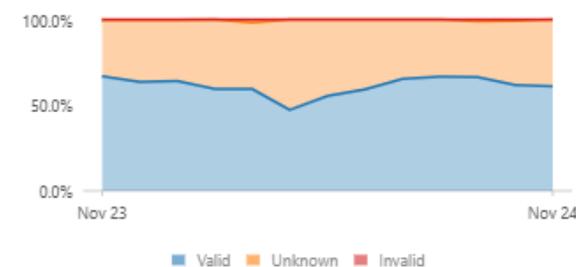
#### Culprits <sup>i</sup>



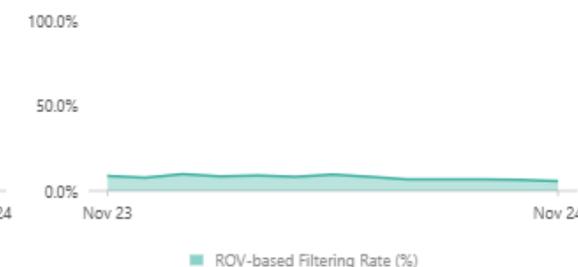
#### Routing Information (IRR) <sup>i</sup>



#### Routing Information (RPKI) <sup>i</sup>



#### Route Origin Validation <sup>i</sup>



# Programa por uma Internet mais Segura



## Participantes por país

- Total: 998
- Participantes no Brasil → 290 (out/24)

2023 → 258

2022 → 206

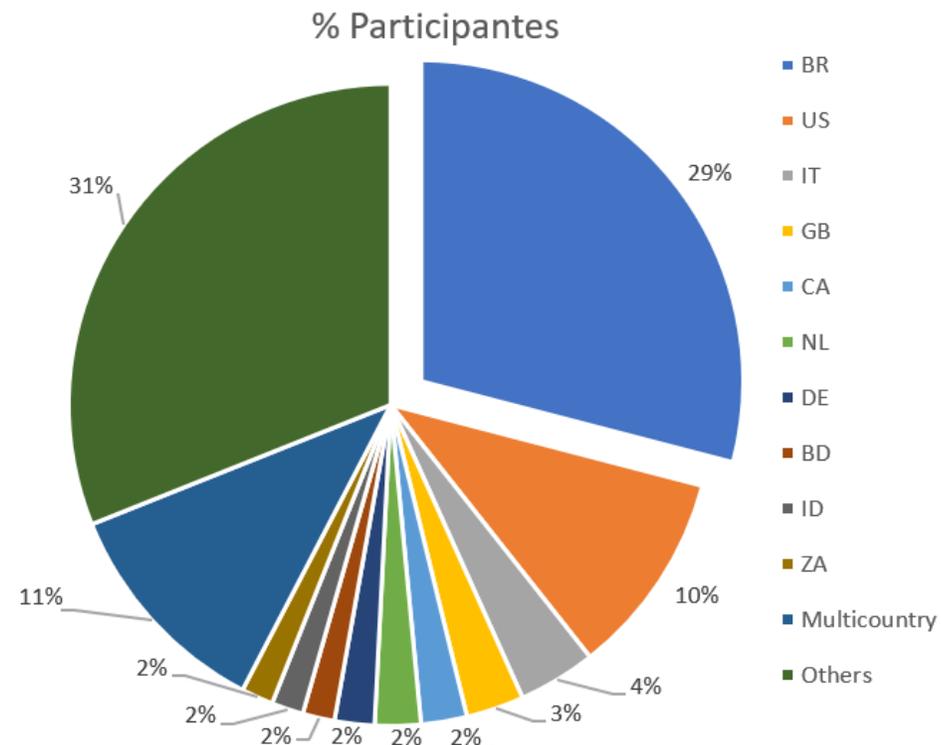
2021 → 174

2020 → 140



MANRS

## % de Participantes



Fonte: <https://www.manrs.org/netops/participants/> Acesso out/24

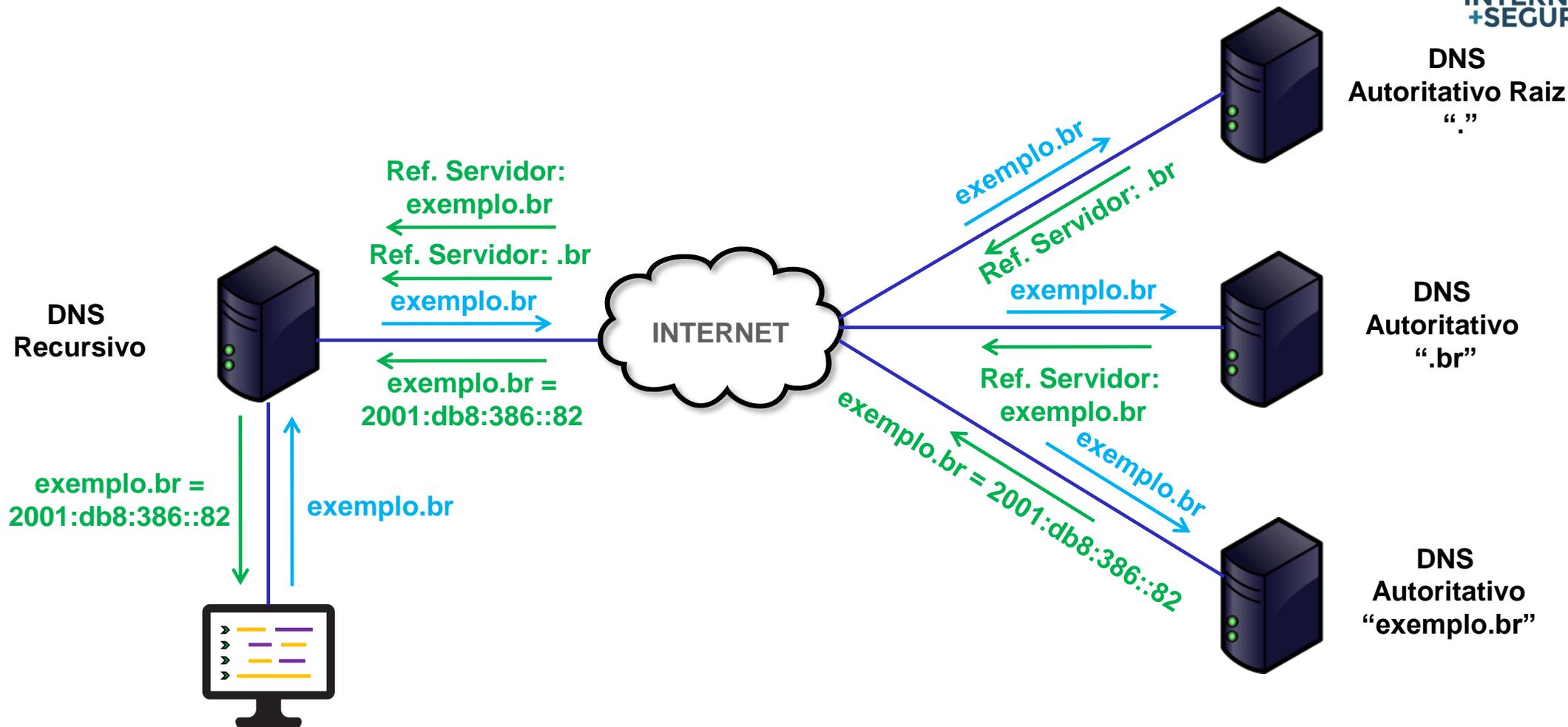


Stands for **K**nowledge-Sharing and  
**I**nstantiating **N**orms for **D**NS and **N**aming  
**S**ecurity

<https://kindns.org/>

# Programa por uma Internet mais Segura

## Processo de Recursão DNS



Fonte: [\[#SemanaCap 7\] Curso - Configurando o seu DNS de forma simples e segura – Ataque DNS Poisoning](#)

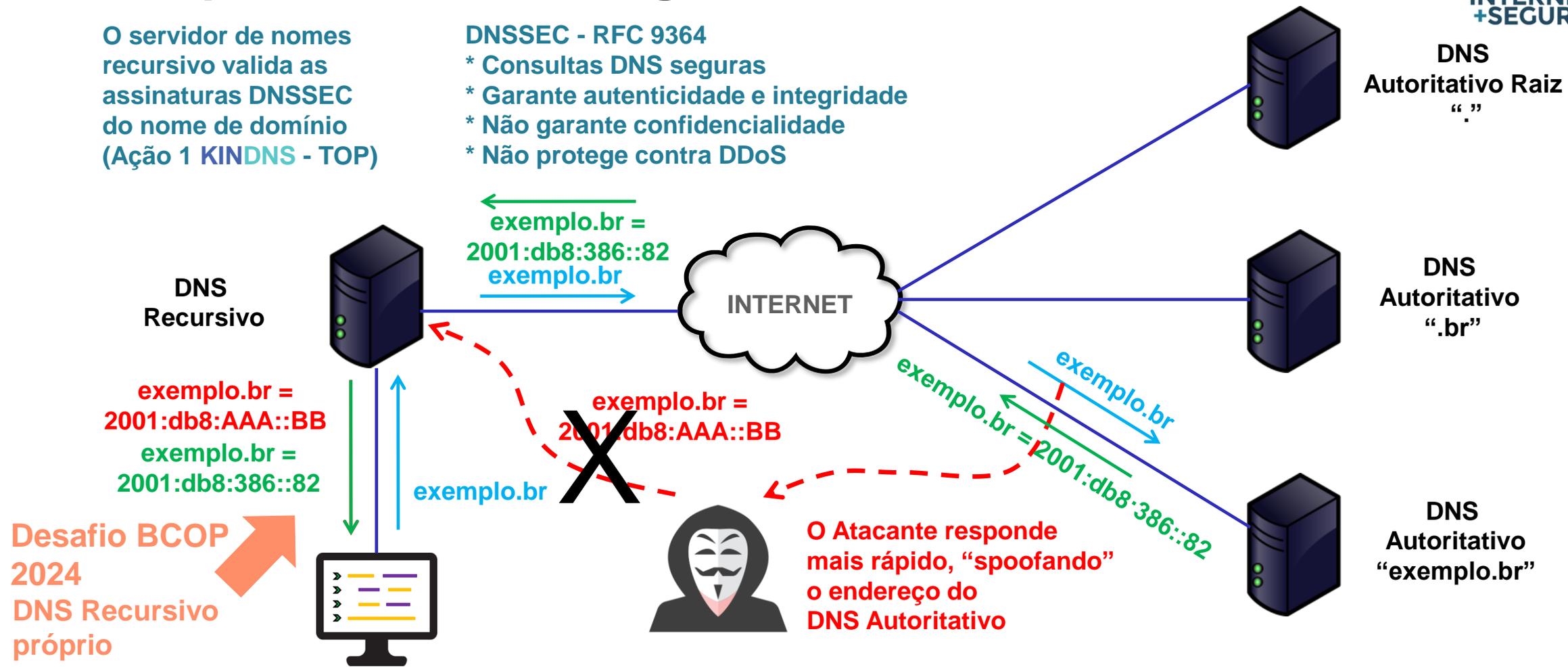
# Programa por uma Internet mais Segura

## 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



Fonte: [#SemanaCap 7] Curso - Configurando o seu DNS de forma simples e segura – Ataque DNS Poisoning

Esta Foto de Autor Desconhecido está licenciado em CC BY-NC



# 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/>



# TOP

TESTE OS PADRÕES

<https://top.nic.br>

**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:  
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

# Programa por uma Internet mais Segura



## TOP - 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!

<https://top.nic.br>

## Teste TOP - IPv6 e DNSSEC



30/10/24

274.441

Med. - IPv6 DNSSEC Final.

7.213

AS Únicos Testados

192.427

DNS Rec com DNSSEC Validado

70%

% DNS Rec c/ DNSSEC Validado

184.009

Usuários IPv6 100%

67%

% Usuários IPv6 100%

# Programa por uma Internet mais Segura



## TOP - Teste os padrões – Interface do usuário

- Operação IPv6 no usuário
- Validação DNSSEC pelo servidor DNS recursivo
- Resolução de nomes IPv6

<https://top.nic.br>

# Programa por uma Internet mais Segura

## TOP - Teste os padrões - Site

- Domínios únicos testados
- Quem é TOP Site
- IPv6
- Domínios Assinados
- Implementação HTTPS
- Opções de Segurança

<https://top.nic.br>

### Teste TOP - Site



39.489

Domínios Únicos Site

607

Quem é TOP Site

2%

% Quem é TOP Site

7.642

IPv6 100% Site

7.809

DNSSEC 100% Site

2.282

HTTPS 100% Site

19%

% IPv6 100% Site

20%

% DNSSEC Site

6%

% HTTPS Site

# Programa por uma Internet mais Segura



## TOP - Teste os padrões – *E-mail*

- Domínios únicos testados
- Quem é TOP *E-mail*
- IPv6
- Domínios Assinados
- Implementação de STARTTLS
- Marcas Segurança (DMARC, DKIM, SPF)

<https://top.nic.br>

### Teste TOP - *E-mail*



# Programa por uma Internet mais Segura

## Implemente as melhores práticas



MANRS



**BCP**

Portal de boas práticas  
para a Internet no Brasil

Desafio BCOP 2024



**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>



# Camada 8 - NIC.br

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

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



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)

28 de novembro de 2024

**nic.br egi.br**

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

