



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

CONECTA NET - FOZ DO IGUAÇU

Foz do Iguaçu, PR | 11/07/25

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



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

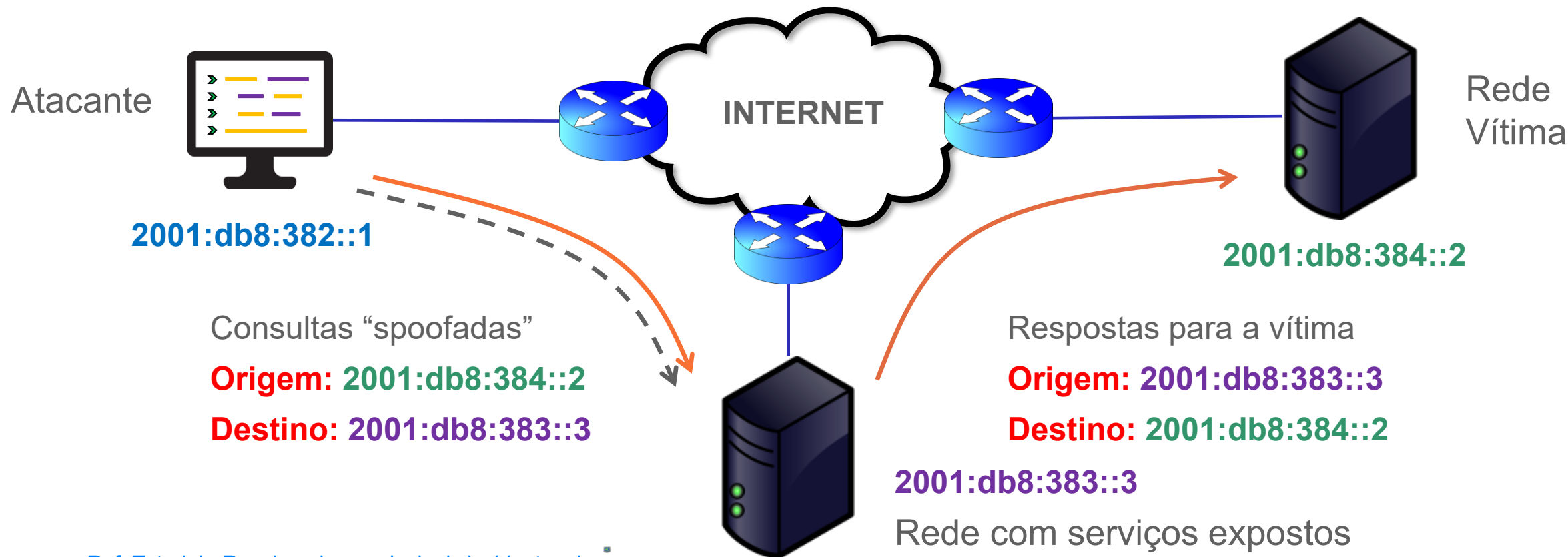
<https://bcp.nic.br/i+seg/acoes/amplificacao/>



Programa por uma Internet mais Segura

Negação de Serviço Reflexivo com Amplificação

Utiliza um terceiro para fazer o ataque



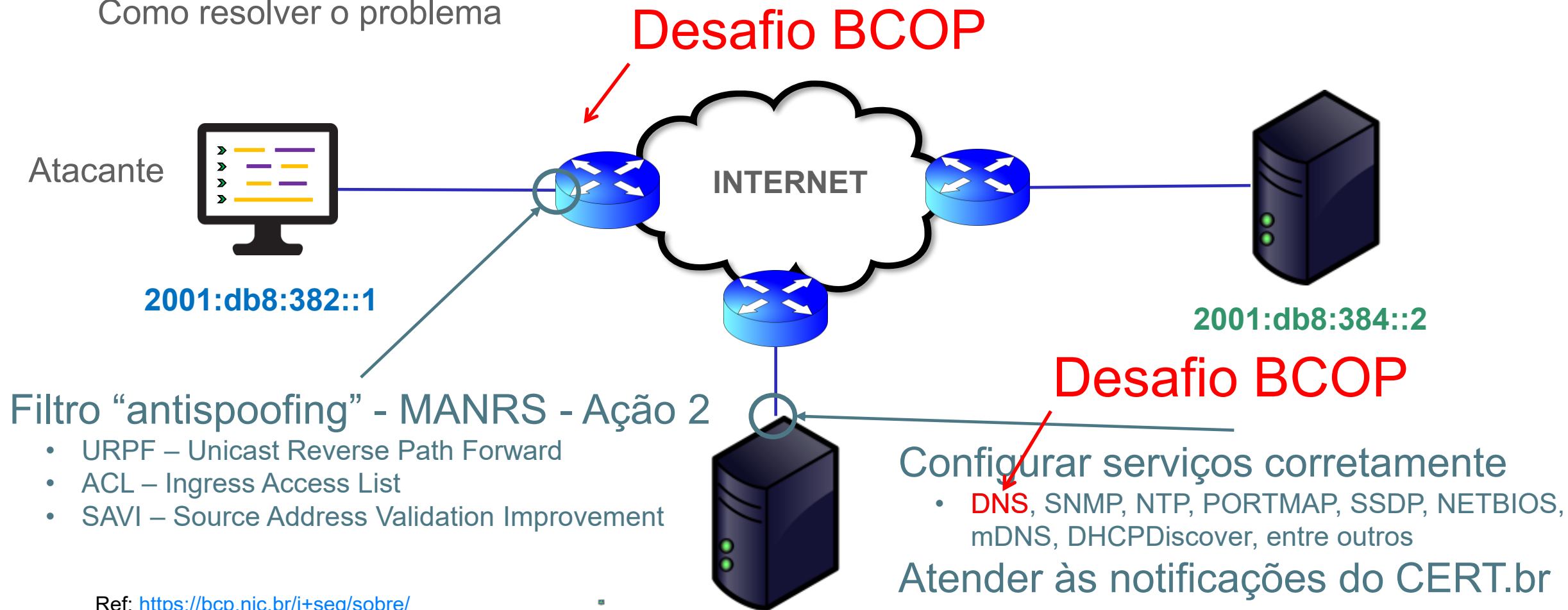
[Ref. Tutorial - Resolvendo os principais incidentes de segurança](#)

Programa por uma Internet mais Segura

Negação de Serviço Reflexivo com Amplificação



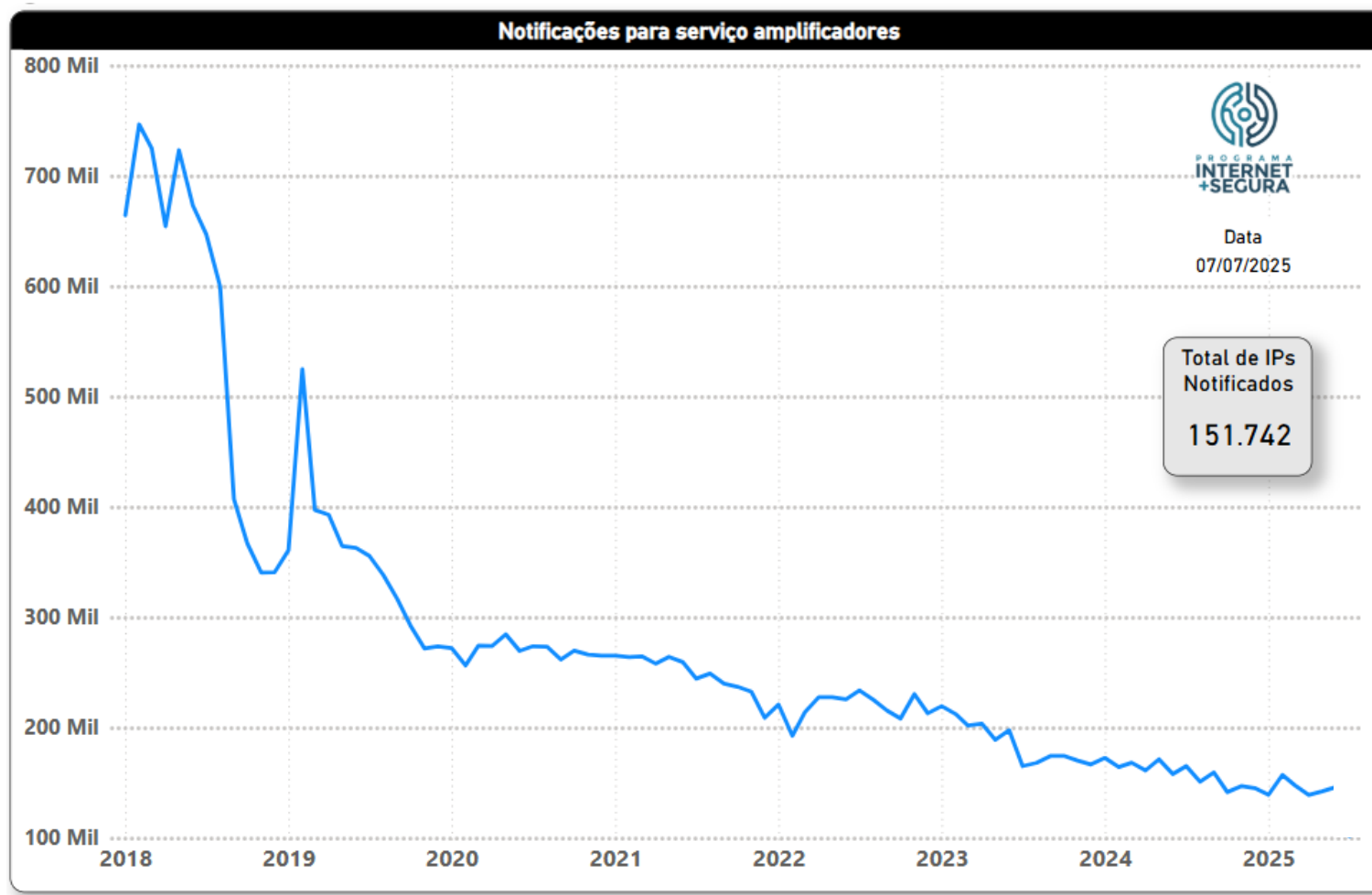
Como resolver o problema



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

Programa por uma Internet mais Segura

Notificação de amplificadores - evolução

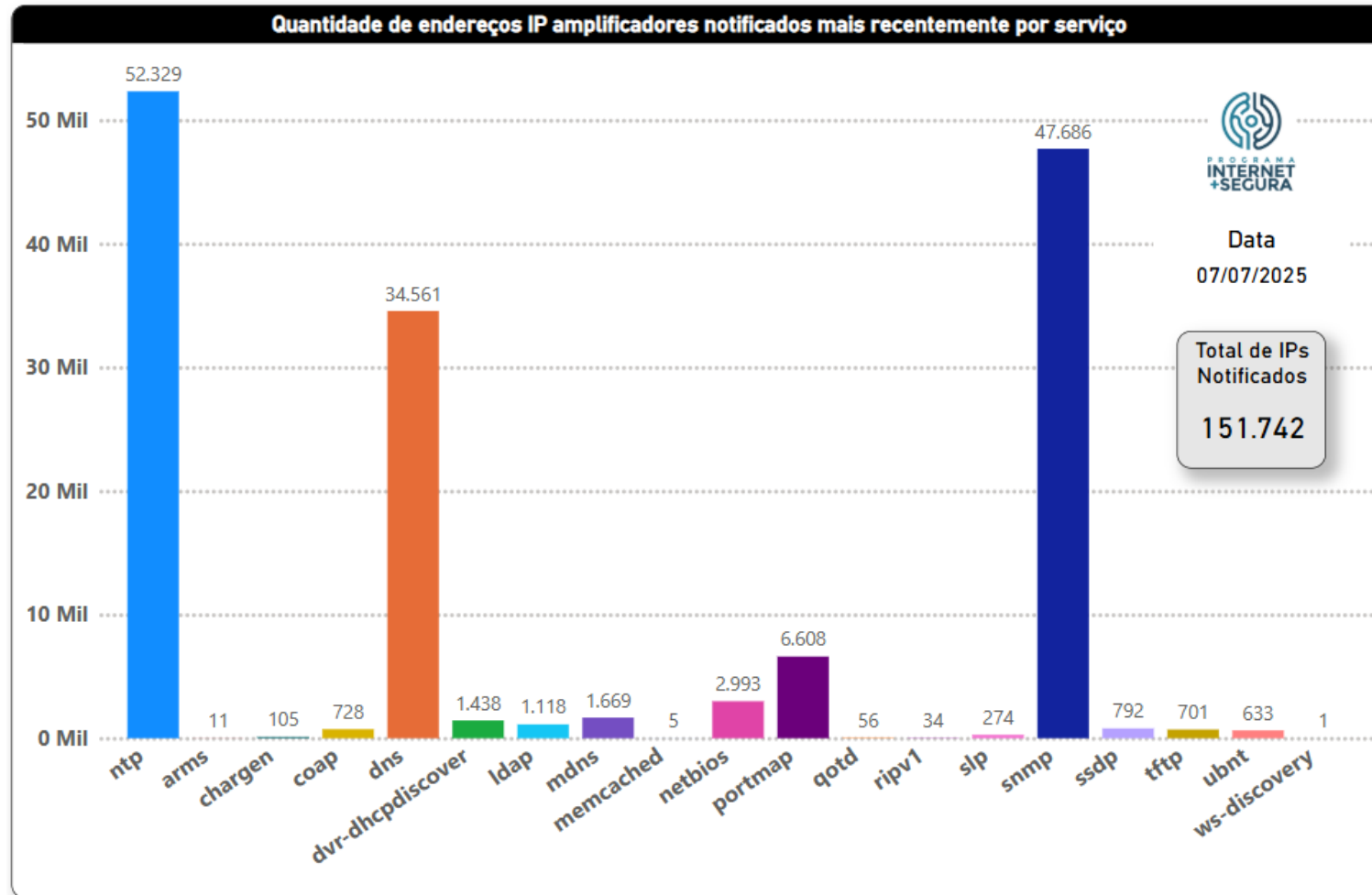


Brasil

- Início (fev/2018)
 - Endereços IP: 746.508
 - Serviços: 5
- Atual:
 - Endereços IP: 151.742
 - Serviços: 19
 - **Redução de 80%**

Programa por uma Internet mais Segura

Notificação de amplificadores - serviços

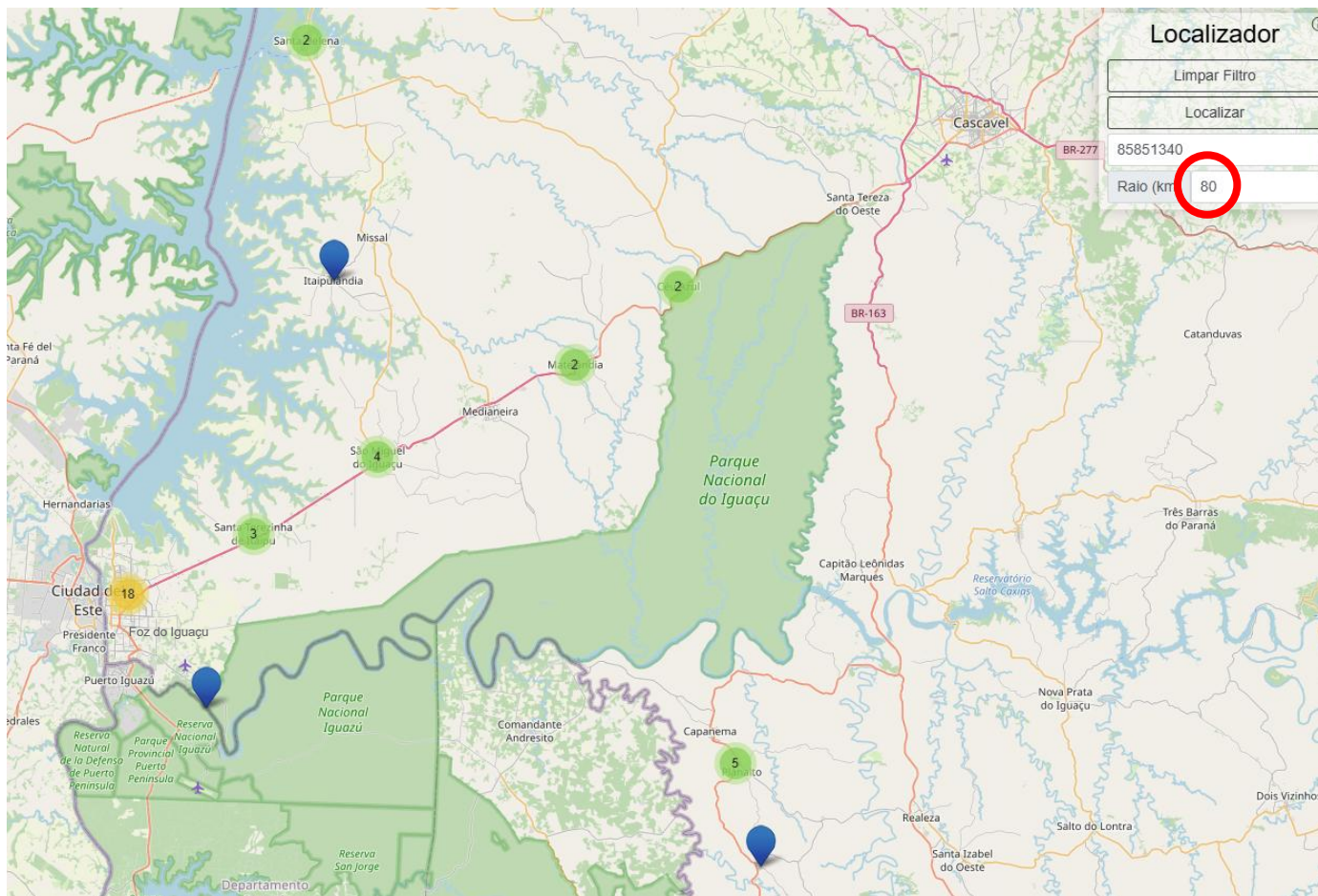


Brasil

- 9.015 AS
- 5.262 AS notificados
- 151.742 endereços IP mal configurados
- **NTP 52.329**
- **SNMP 47.686**
- **DNS 34.561**

Programa por uma Internet mais Segura

Notificação de amplificadores - serviços



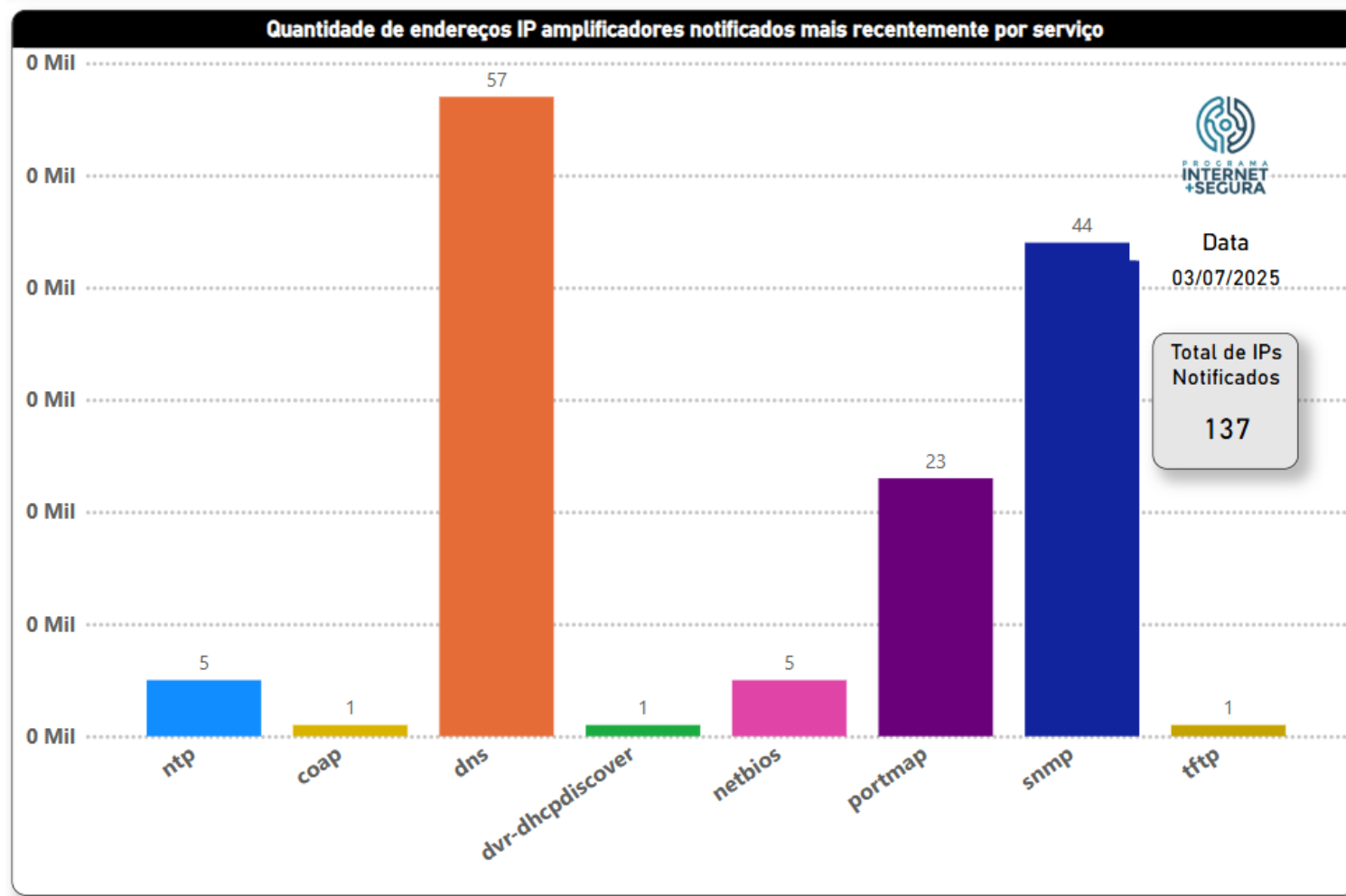
Foz do Iguaçu (39 AS)

- Foz do Iguaçu (19)
- Santa Terezinha do Itaipu (3)
- São Miguel do Iguaçu (4)
- Matelândia (2)
- Céu Azul (2)
- Planalto (5)
- Santa Helena (2)
- Itaipulândia (1)
- Capanema (1)

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

Programa por uma Internet mais Segura

Notificação de amplificadores - serviços



Foz do Iguaçu (80Km)

- 39 AS
- 26 AS notificados
- 137 endereços IP mal configurados
 - DNS 57
 - SNMP 44
 - PORTMAP 23



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



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



Programa por uma Internet mais Segura

Sequestro de prefixos (Hijacking)

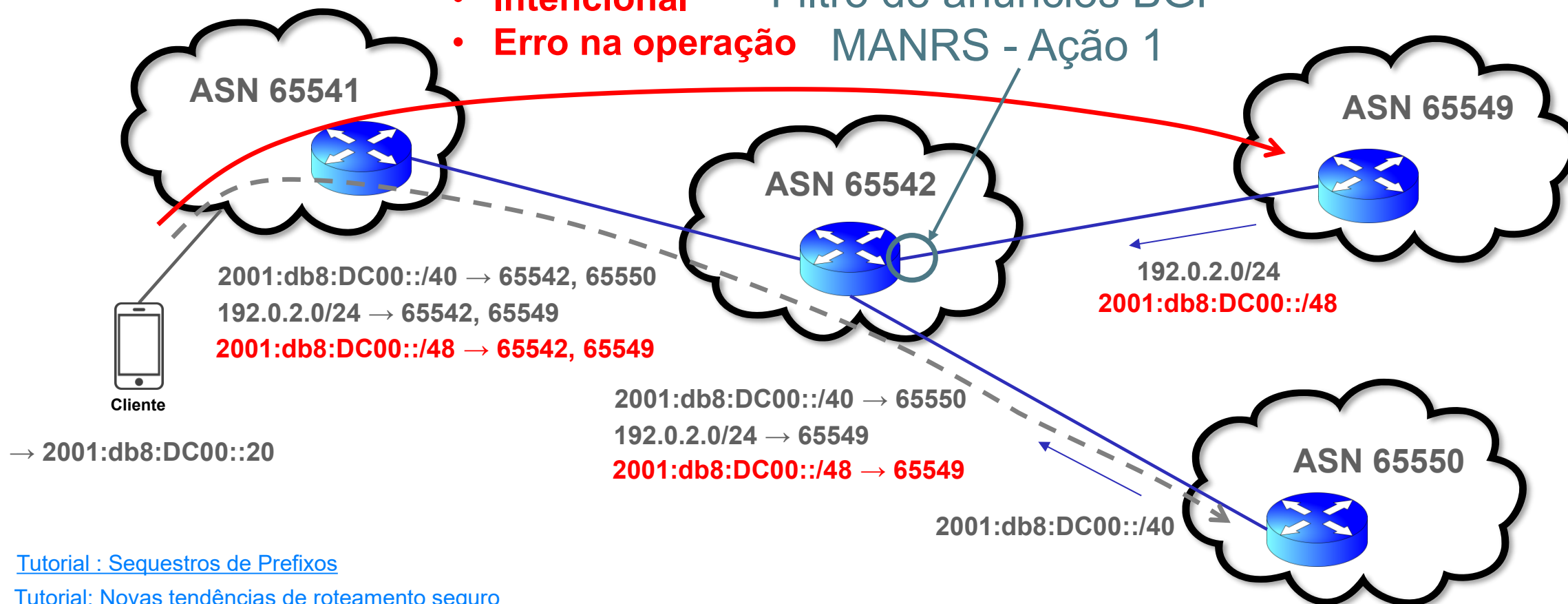
Anúncio de prefixos não autorizados:

- Intencional

Filtro de anúncios BGP

- Erro na operação

MANRS - Ação 1



[Tutorial : Sequestros de Prefixos](#)

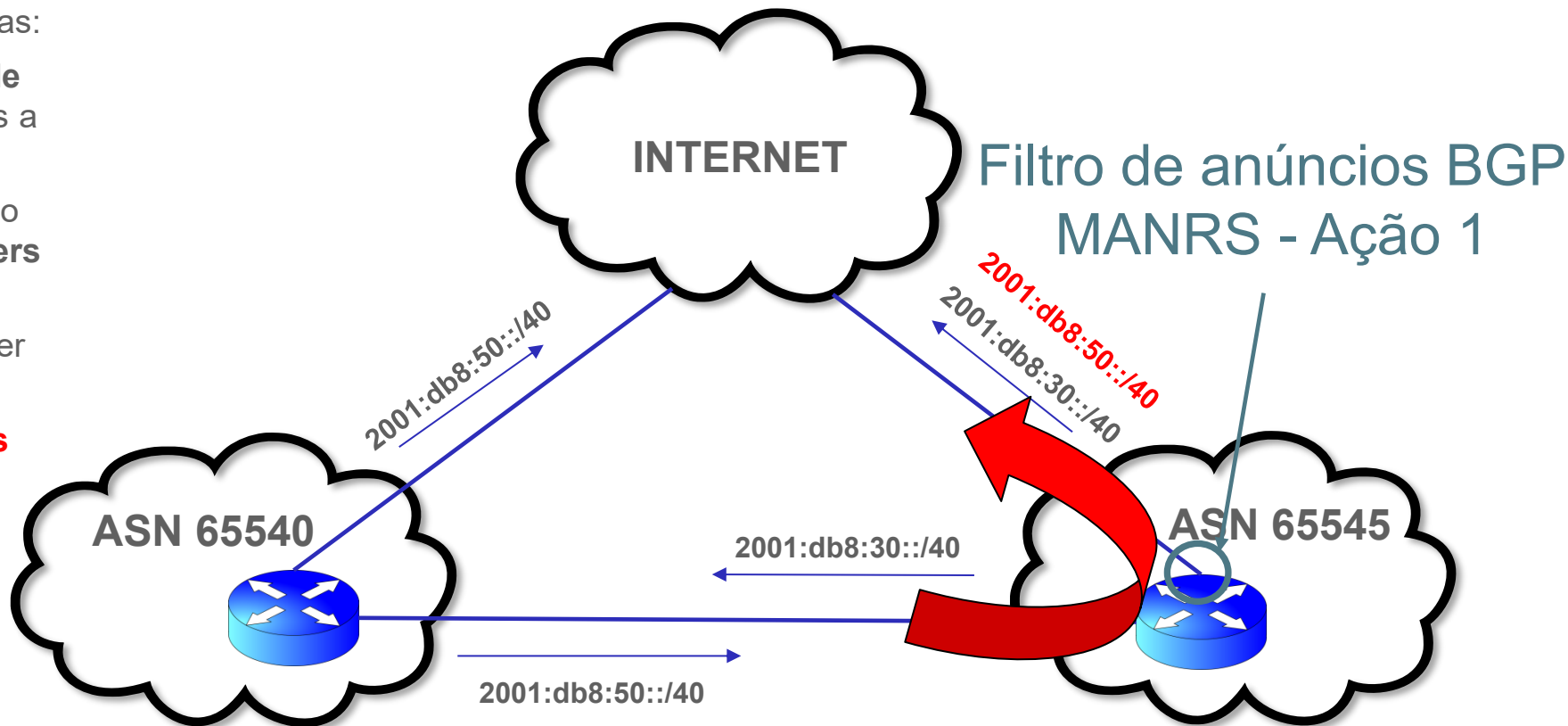
[Tutorial: Novas tendências de roteamento seguro](#)

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



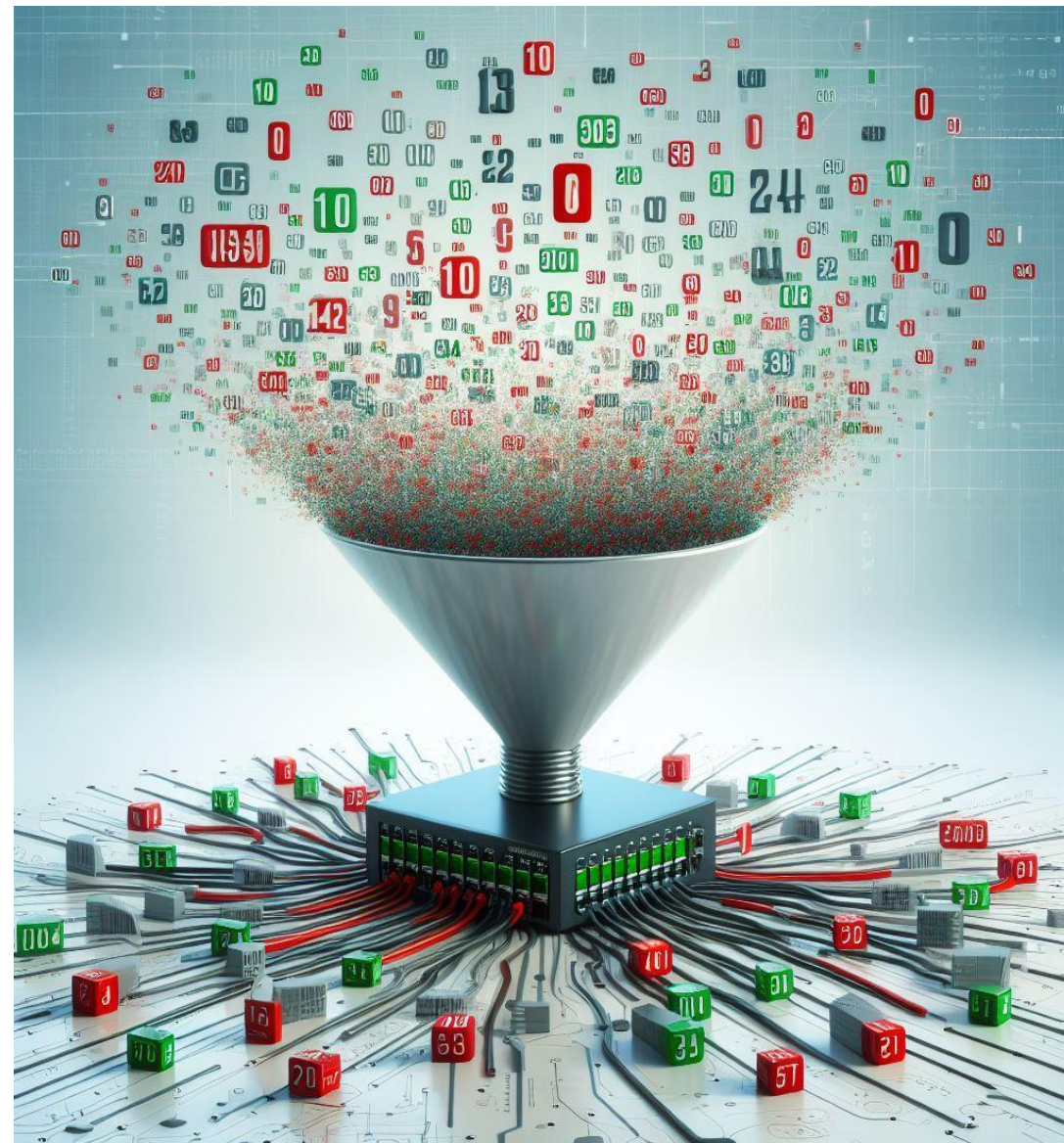
Programa por uma Internet mais Segura



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

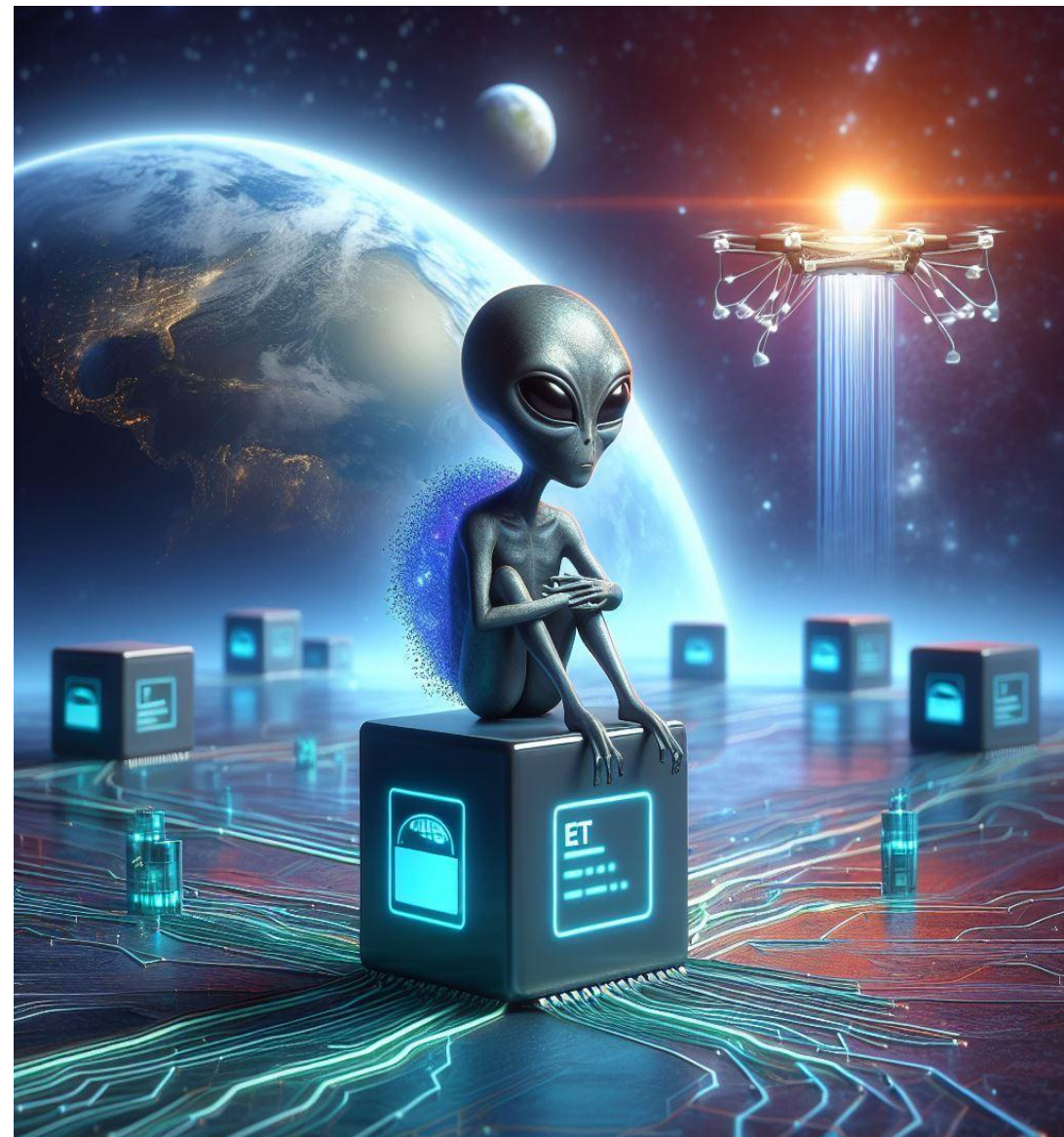


MANRS - Ação 2 - Filtro Anti-spoofing

- 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/>

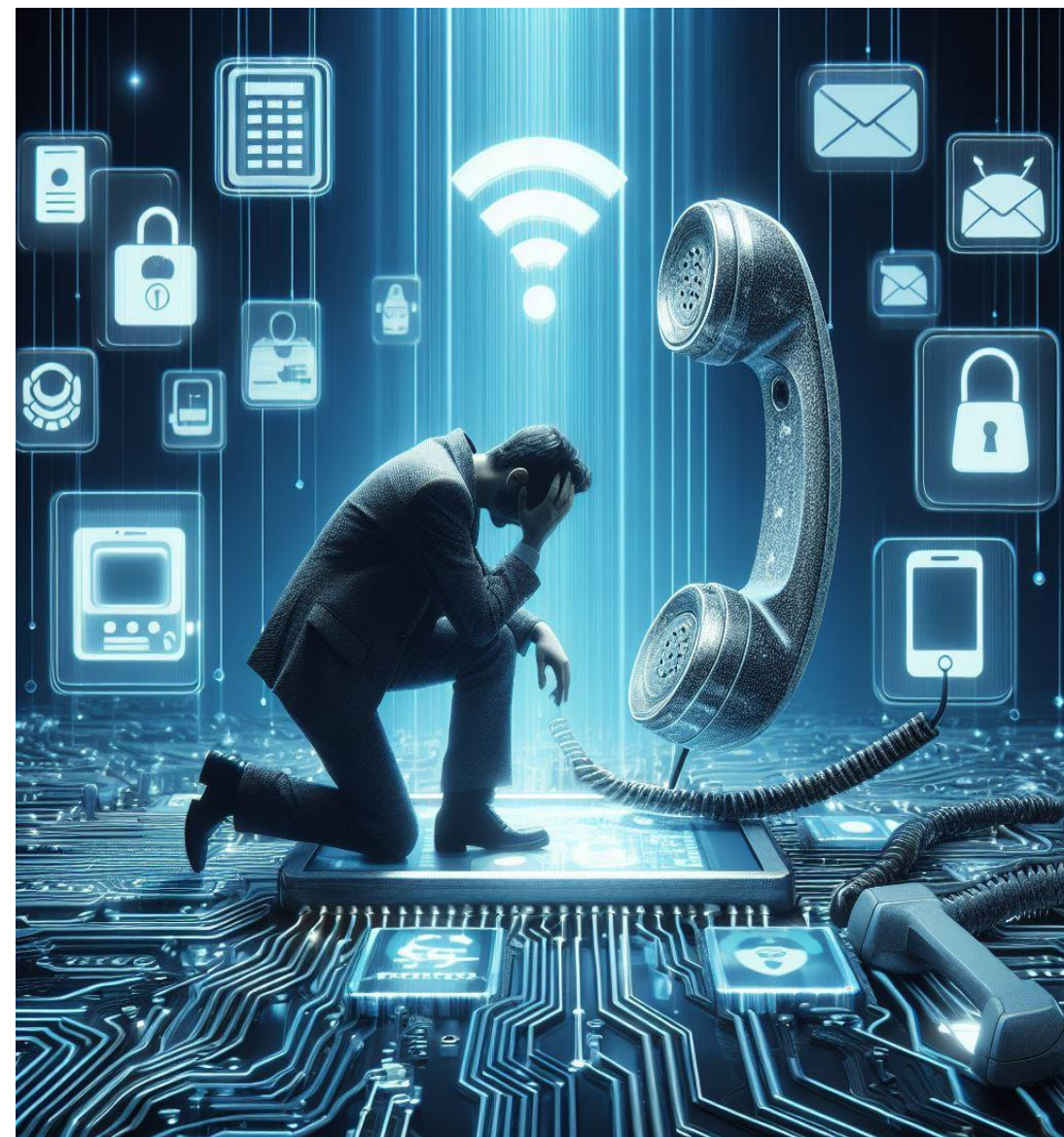


Programa por uma Internet mais Segura



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
- 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

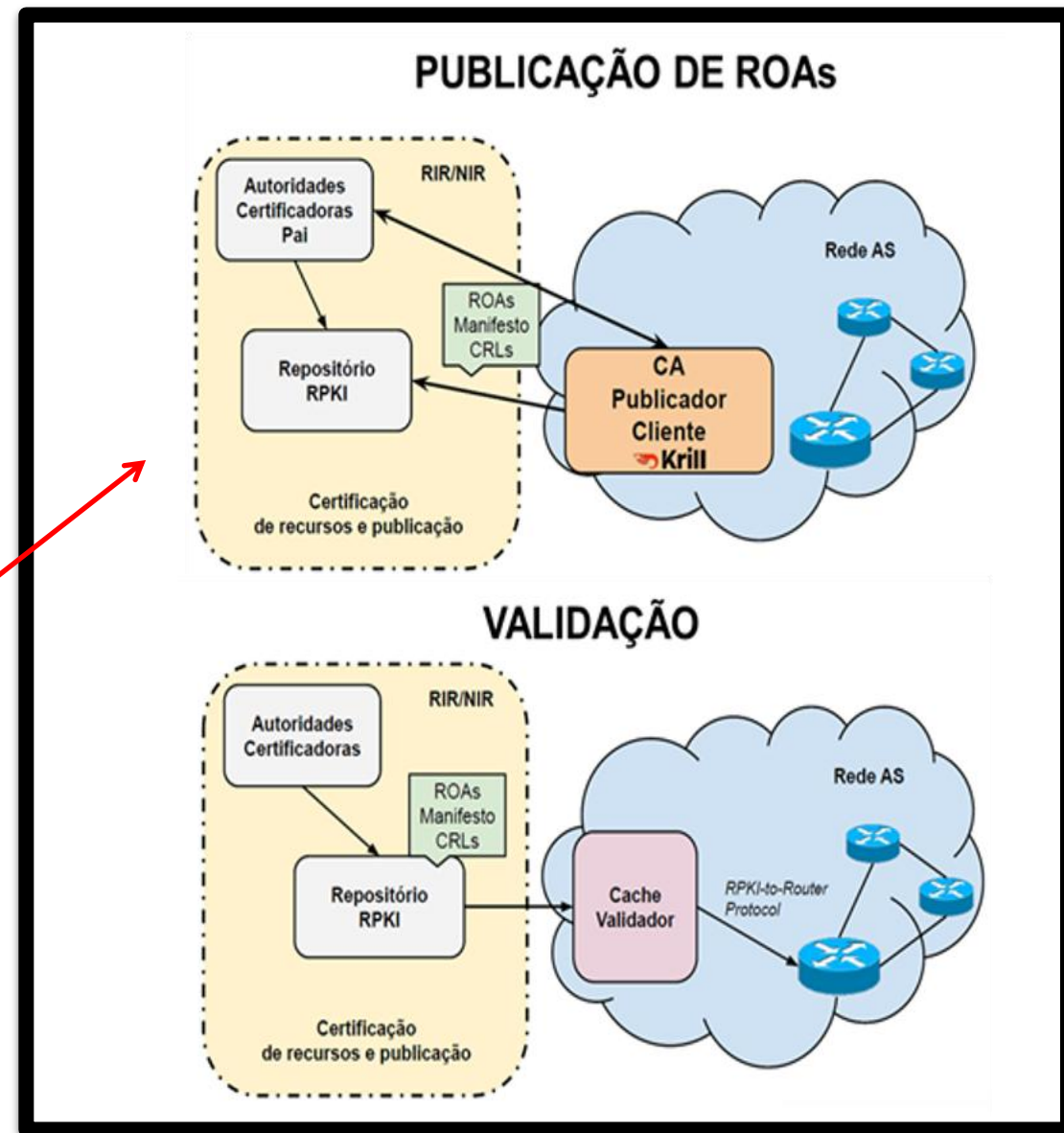
- RPKI - Resource Public Key Infrastructure

<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 - 14 AS – AP



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 ¹

Route misoriginations
Route leaks
Bogon announcements
Total

Culprits ¹

Culprits
Total

Routing Information (IRR) ¹

Unregistered 2 0.6%
Registered 342 99.4%

Routing Information (RPKI) ¹

Valid 247 71.0%
Unknown 101 29.0%
Invalid 0 0.0%

Route Origin Validation ¹

ROV-based Filtering Rate (%) 9.4%

Route misoriginations Route leaks Bogon announcements

Culprits

Unregistered Registered

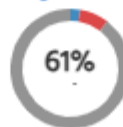
Valid Unknown Invalid

MANRS Readiness ¹

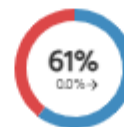
Filtering ¹



Anti-spoofing ¹



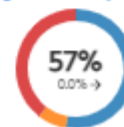
Coordination ¹



Routing Information (IRR) ¹



Routing Information (RPKI) ¹



Ready Aspiring Lagging No Data Available

Programa por uma Internet mais Segura

MANRS Observatory - 14 AS – AP

ASN	Holder	Country	UN Regions	UN Sub-Regions	RIR Regions	Filtering	Anti-spoofing	Coordination	Routing Information (IRR)	Routing Information (RPKI)
ASN 1	---	BR	Americas	Latin America and the Caribbean	LACNIC	100%		100%	100%	100%
ASN 3	---	BR	Americas	Latin America and the Caribbean	LACNIC	100%		0%	88%	50%
ASN 5	---	BR	Americas	Latin America and the Caribbean	LACNIC	100%		100%	100%	100%
ASN 6	---	BR	Americas	Latin America and the Caribbean	LACNIC	100%	49%	100%	100%	100%
ASN 11	---	BR	Americas	Latin America and the Caribbean	LACNIC	100%		0%	100%	0%
ASN 13	---	BR	Americas	Latin America and the Caribbean	LACNIC	100%		0%	100%	100%
ASN 14	---	BR	Americas	Latin America and the Caribbean	LACNIC	100%		0%	100%	0%
ASN 15	---	BR	Americas	Latin America and the Caribbean	LACNIC	100%	100%	100%	100%	100%
ASN 16	---	BR	Americas	Latin America and the Caribbean	LACNIC	100%	49%	100%	100%	0%
ASN 18	---	BR	Americas	Latin America and the Caribbean	LACNIC	100%		100%	94%	94%
ASN 19	---	BR	Americas	Latin America and the Caribbean	LACNIC	100%		100%	100%	100%
ASN 20	---	BR	Americas	Latin America and the Caribbean	LACNIC	100%		0%	100%	0%
ASN 22	---	BR	Americas	Latin America and the Caribbean	LACNIC	100%		100%	100%	100%
ASN 23	---	BR	Americas	Latin America and the Caribbean	LACNIC	100%		100%	100%	70%
ASN 24	---	BR	Americas	Latin America and the Caribbean	LACNIC	100%	49%	100%	100%	0%
ASN 25	---	BR	Americas	Latin America and the Caribbean	LACNIC	100%		0%	100%	100%
ASN 26	---	BR	Americas	Latin America and the Caribbean	LACNIC	100%		0%	100%	0%
ASN 28	---	BR	Americas	Latin America and the Caribbean	LACNIC	100%		100%	100%	100%
ASN 29	---	BR	Americas	Latin America and the Caribbean	LACNIC	100%		0%	100%	0%
ASN 31	---	BR	Americas	Latin America and the Caribbean	LACNIC	100%		100%	100%	0%
ASN 32 *	---	BR	Americas	Latin America and the Caribbean	LACNIC	100%		0%	100%	0%
ASN 33	---	BR	Americas	Latin America and the Caribbean	LACNIC	100%		100%	100%	100%
ASN 34	---	BR	Americas	Latin America and the Caribbean	LACNIC	100%		100%	100%	0%
ASN 35	---	BR	Americas	Latin America and the Caribbean	LACNIC	100%		0%	100%	100%
ASN 36 #	---	BR	Americas	Latin America and the Caribbean	LACNIC	100%		0%	100%	0%
ASN 38	---	BR	Americas	Latin America and the Caribbean	LACNIC	100%		0%	100%	50%

* - ASN com status pendente junto ao registro.br

- ASN com status bloqueio junto ao registro.br

Programa por uma Internet mais Segura



Participantes por país

- Total: 1.070
- Participantes no Brasil → 308 (jun/25)

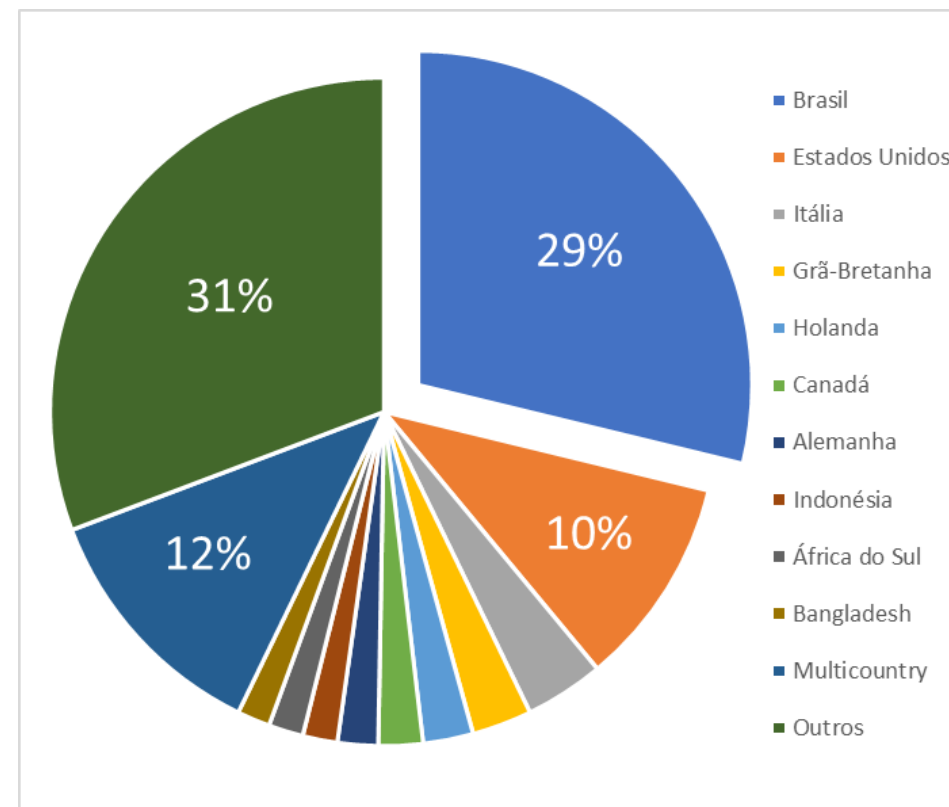


MANRS

2024 → 292
2023 → 258
2022 → 206
2021 → 174
2020 → 140

- Participantes Foz: AS28145, AS269347, AS28223

% de Participantes



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

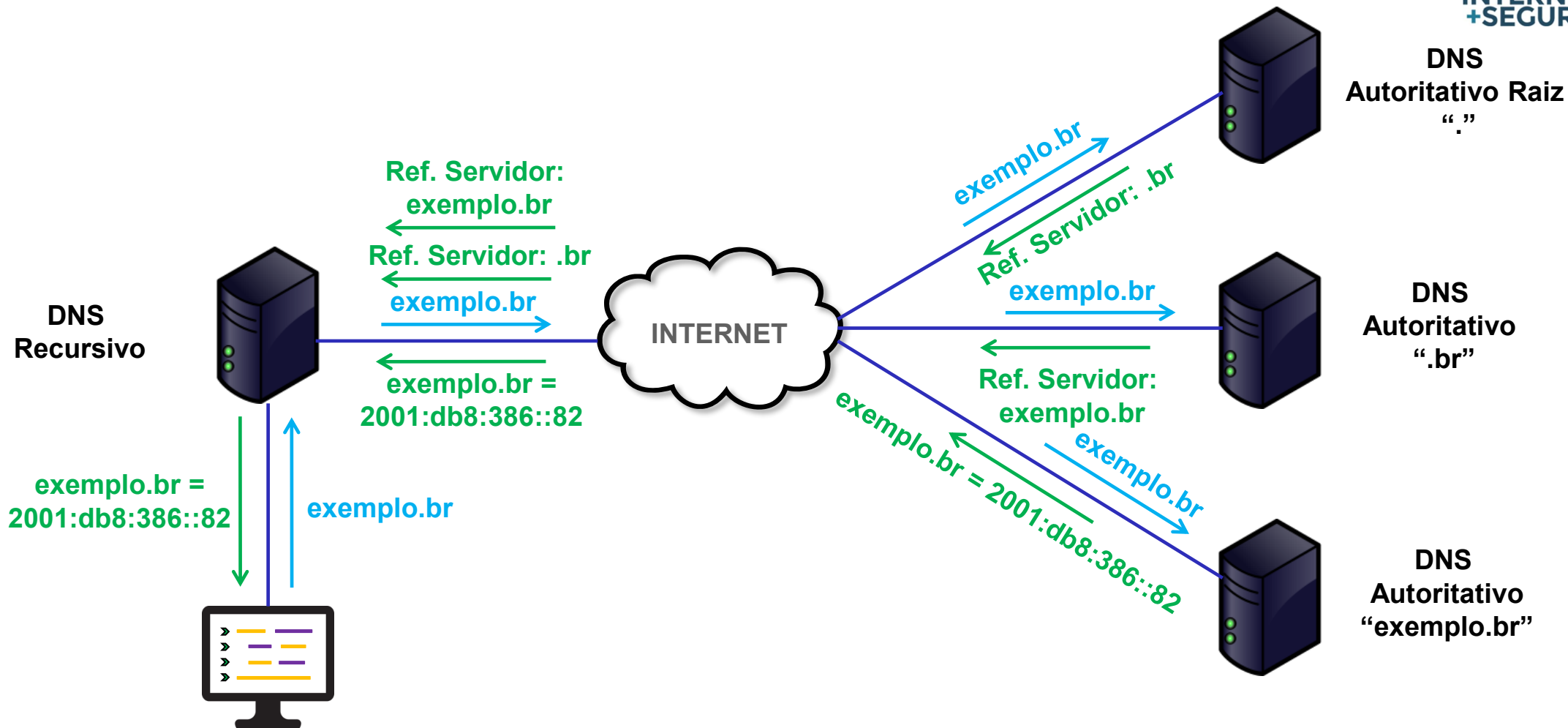


Stands for **K**nowledge-Sharing and
Intantiating **N**orms for **DNS** and **N**aming
Security

<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

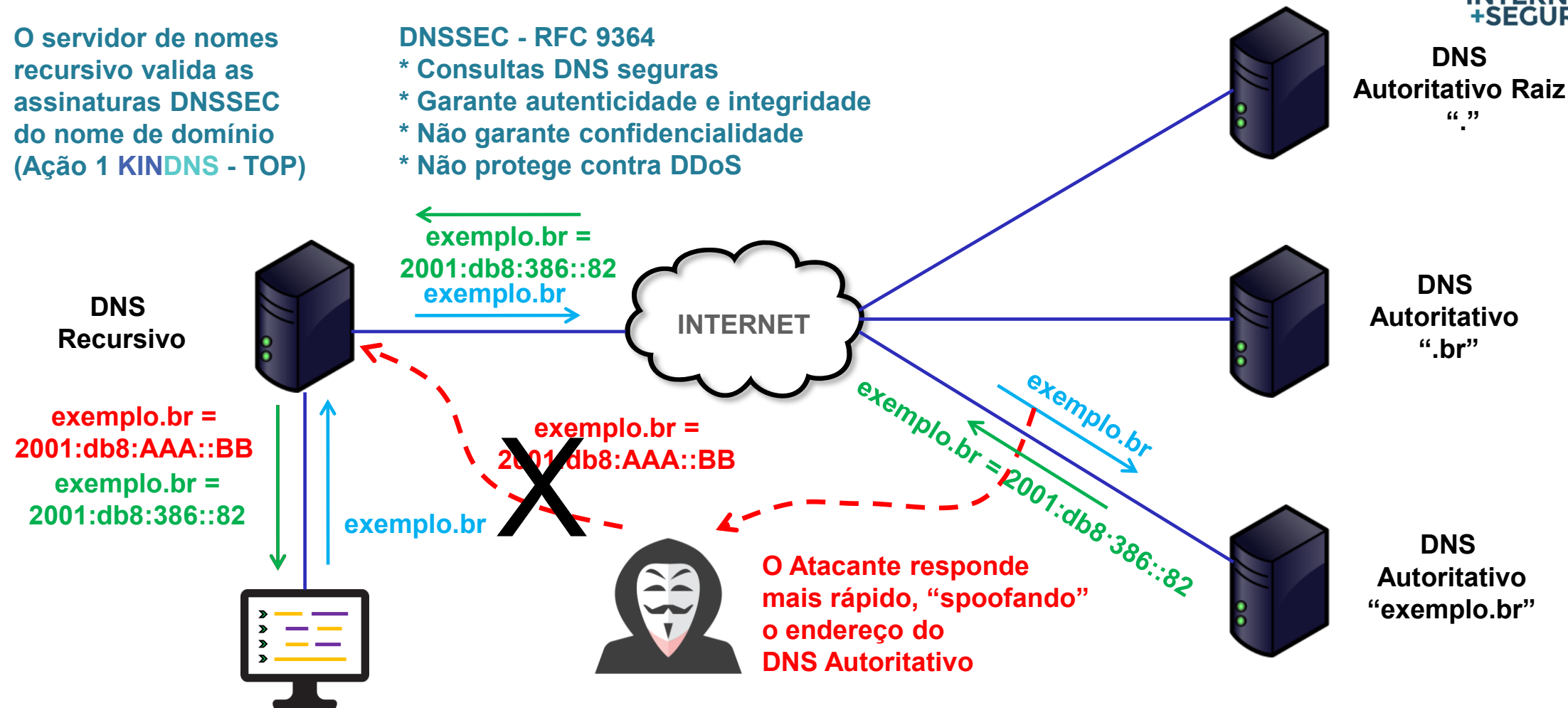
Ataque DNS - Poisoning



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>



Quem é TOPSobreReferênciasComunicados

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

* Novos testes

Desafio BCOP

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

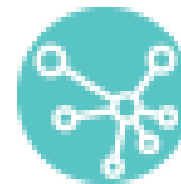


Programa por uma Internet mais Segura

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>



Programa por uma Internet mais Segura

APOIO



A CONECTIVIDADE AO SEU ALCANCE



Obrigado

Gilberto Zorello

@ gzorello@nic.br

11 de julho de 2025

nic.br **cgi.br**

www.nic.br | www.cgi.br

