



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

Programa por uma Internet mais segura

Como tornar seu provedor mais seguro

Gilberto Zorello | gzorello@nic.br

IX Fórum Regional – Edição Sudeste

Ribeirão Preto, SP | 27/02/26

registro.br nic.br cgi.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
- Divulgar melhores práticas de segurança
- **Aumentar a cultura de segurança**

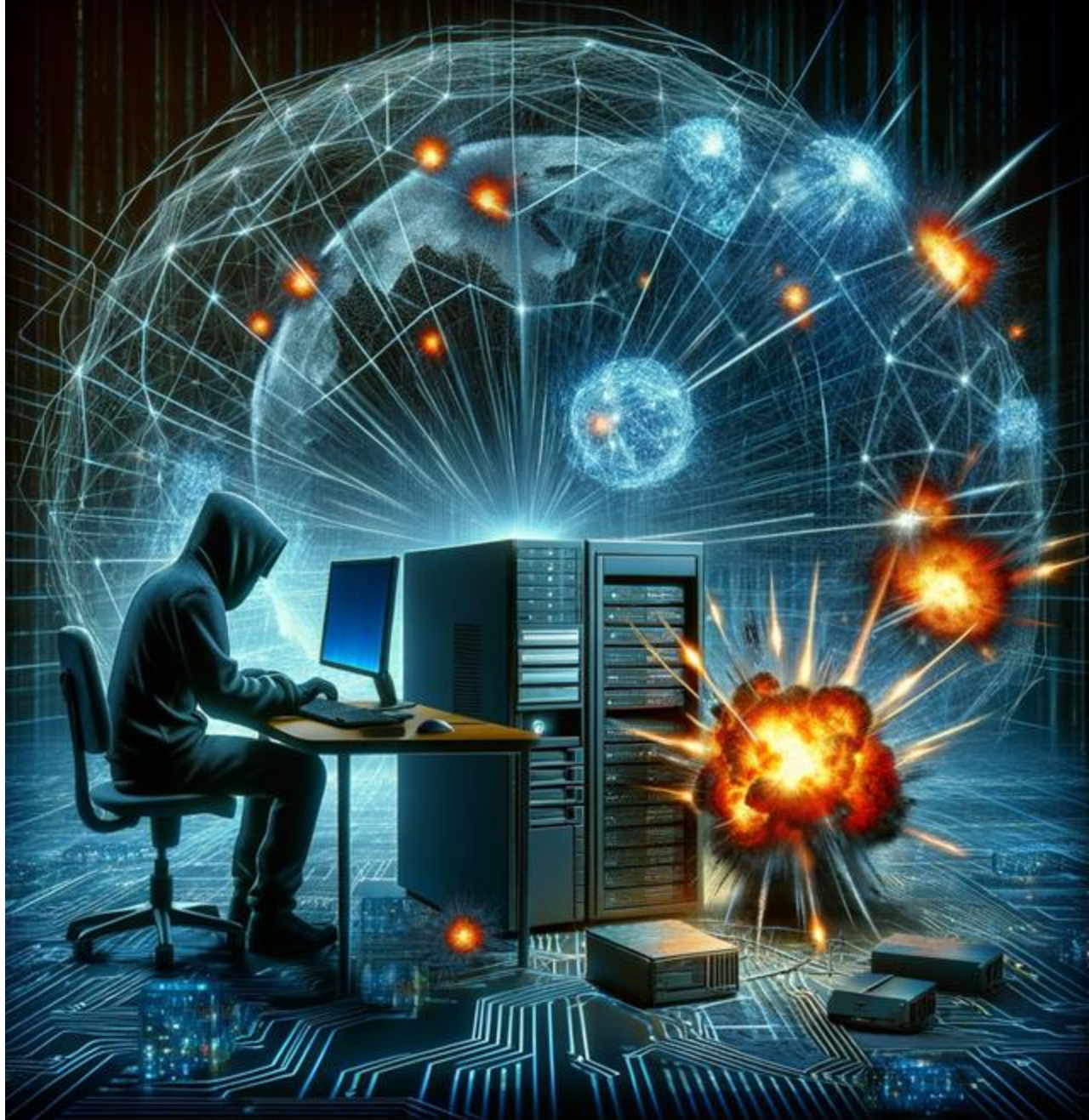
<https://bcp.nic.br/i+seg>



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

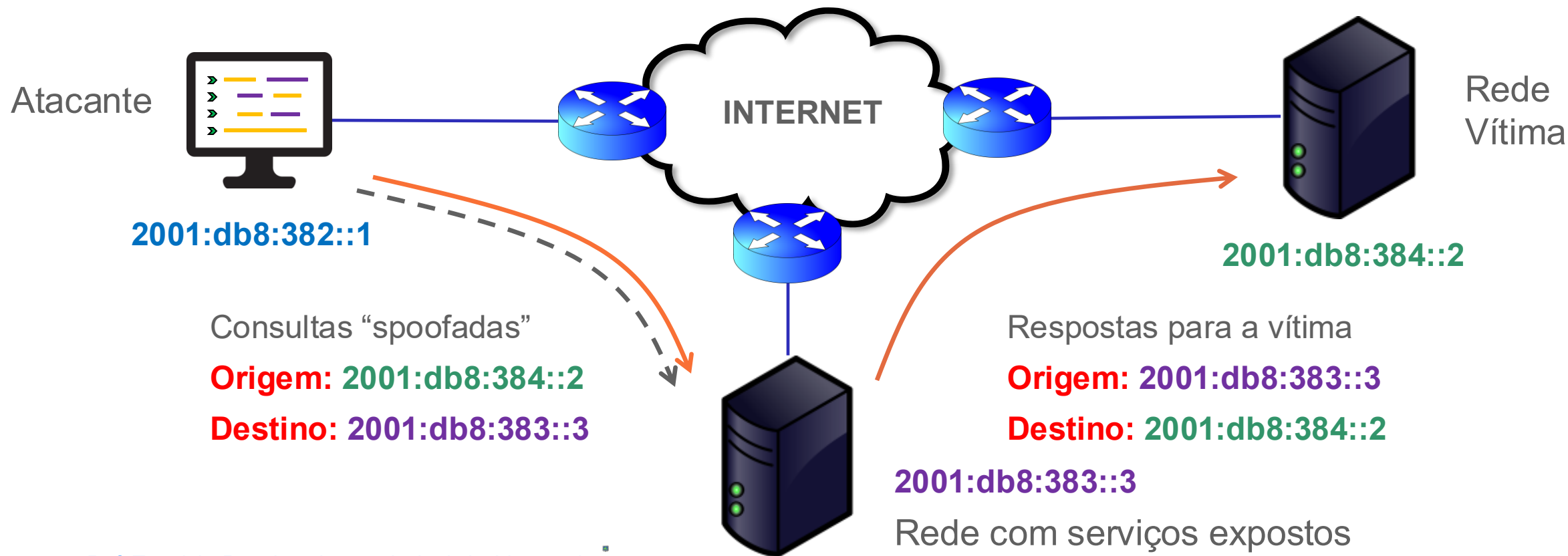
<https://bcp.nic.br/i+seg/acoes/amplificacao/>



Programa por uma Internet mais Segura

Negação de Serviço Reflexivo com Amplificação

Utiliza um terceiro para fazer o ataque



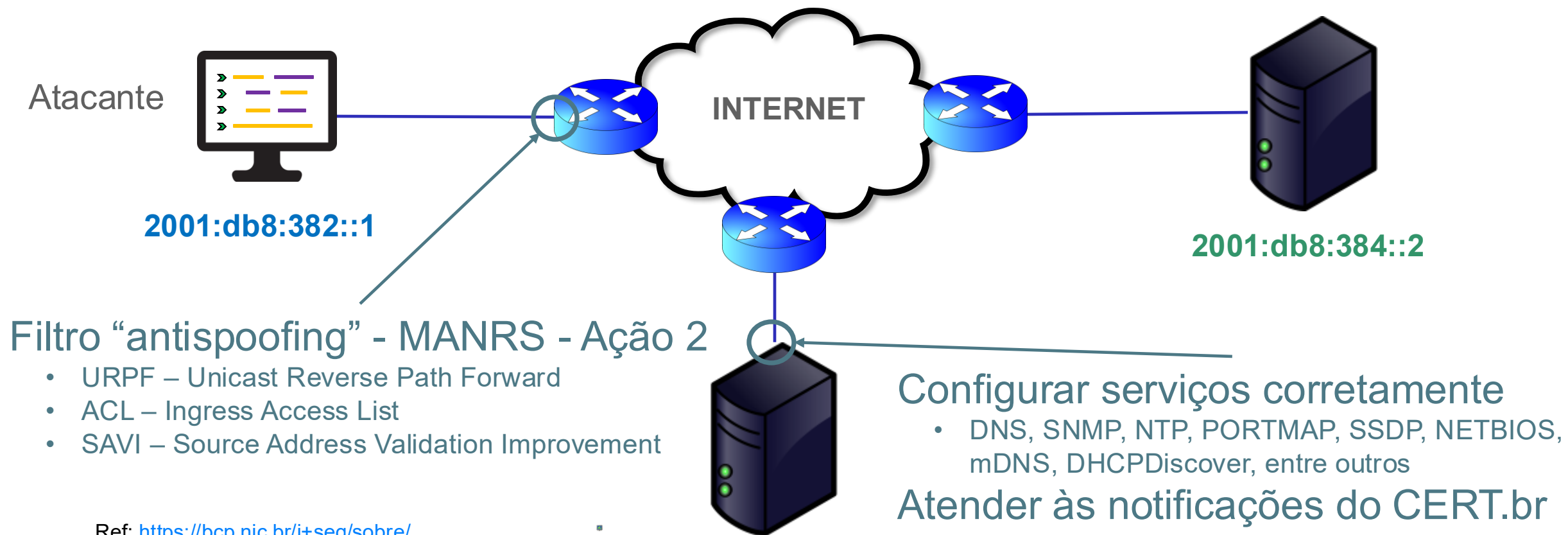
[Ref. Tutorial - Resolvendo os principais incidentes de segurança](#)

Programa por uma Internet mais Segura

Negação de Serviço Reflexivo com Amplificação



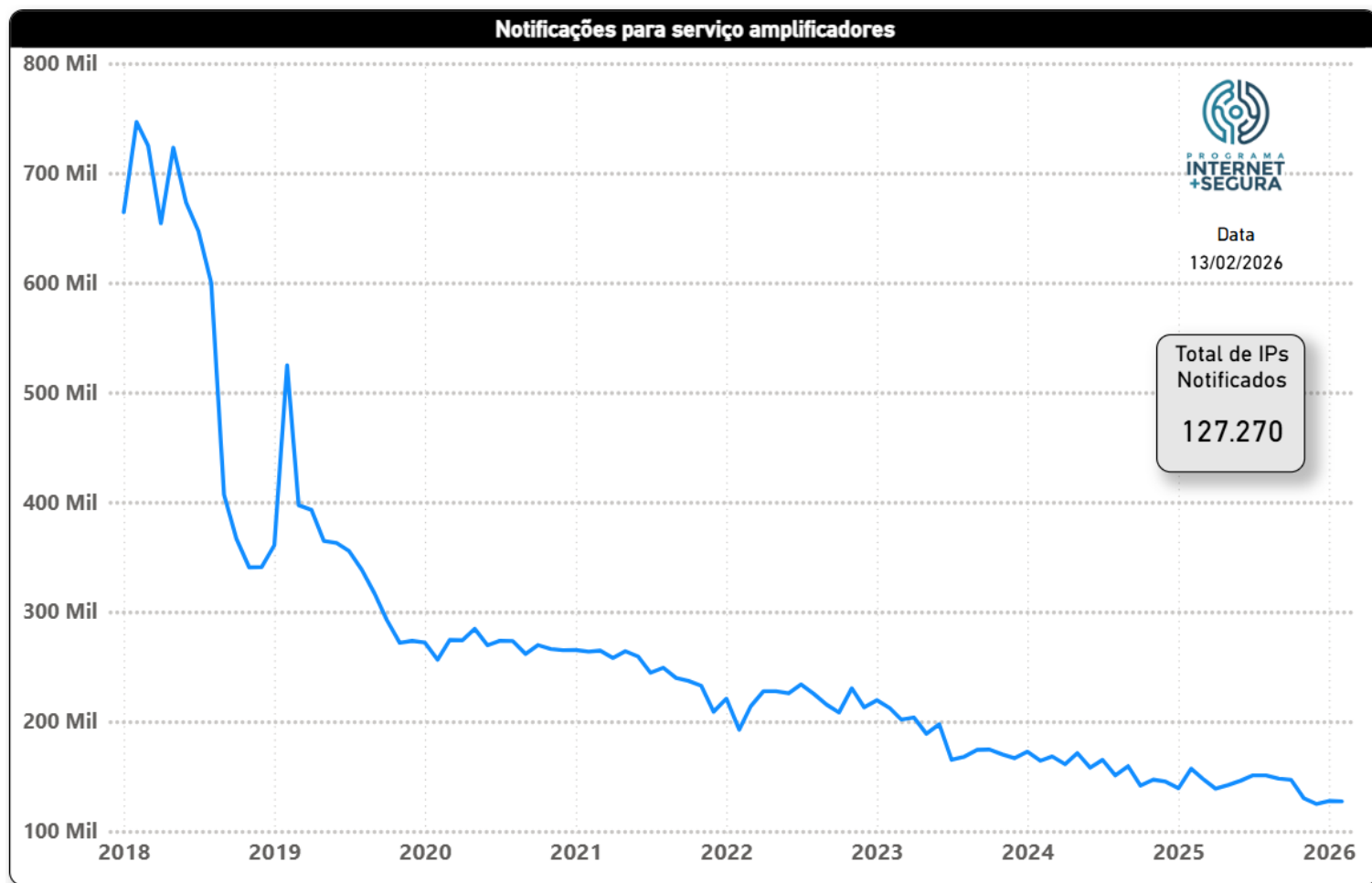
Como resolver o problema



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

Programa por uma Internet mais Segura

Notificação de amplificadores - evolução

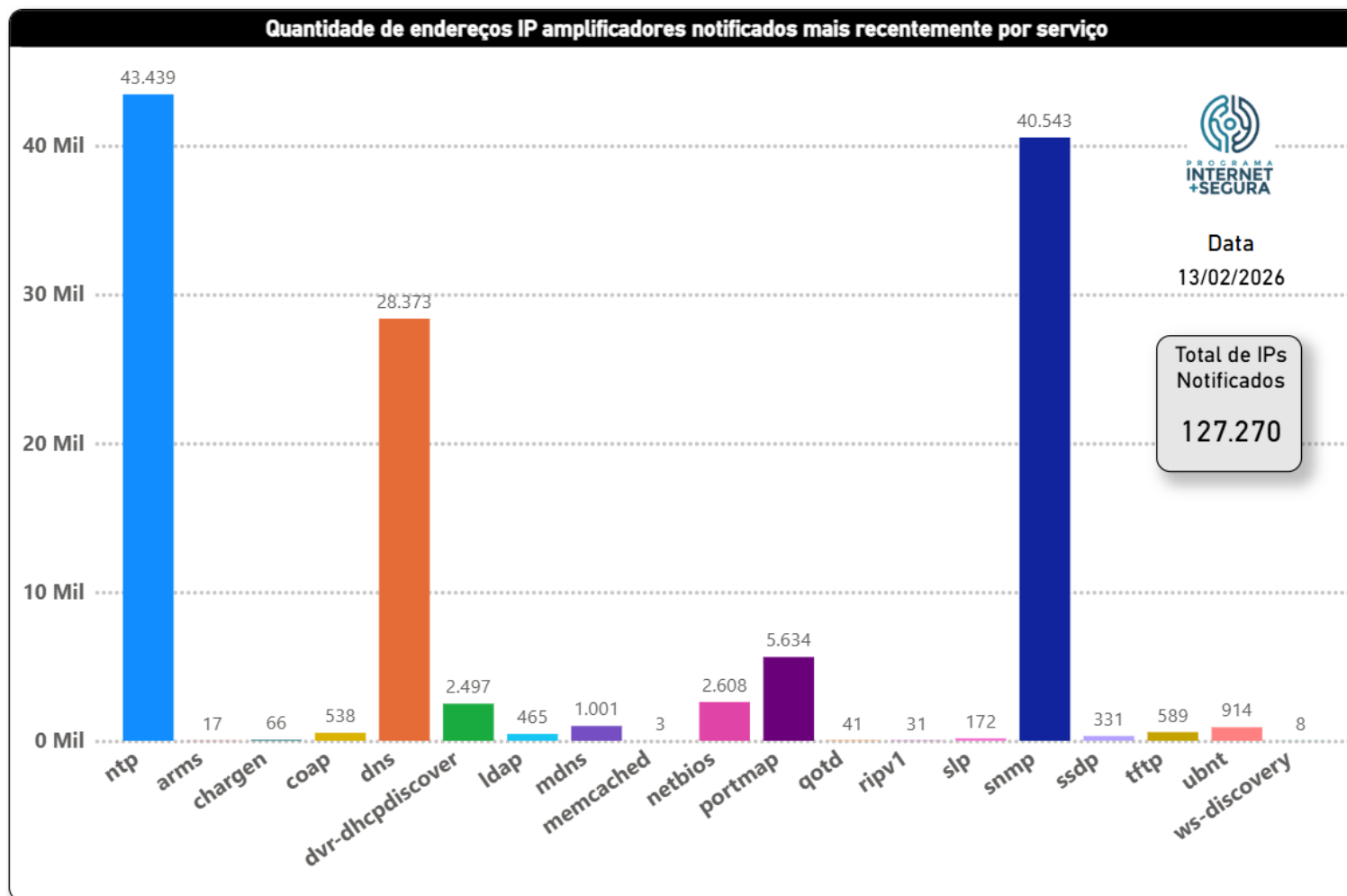


Brasil

- Início (fev/2018)
 - Endereços IP: 746.508
 - Serviços: 5
- Atual:
 - Endereços IP: 127.270
 - Serviços: 19
 - **Redução de 82%**
 - Ref. Fev/26

Programa por uma Internet mais Segura

Notificação de amplificadores - serviços

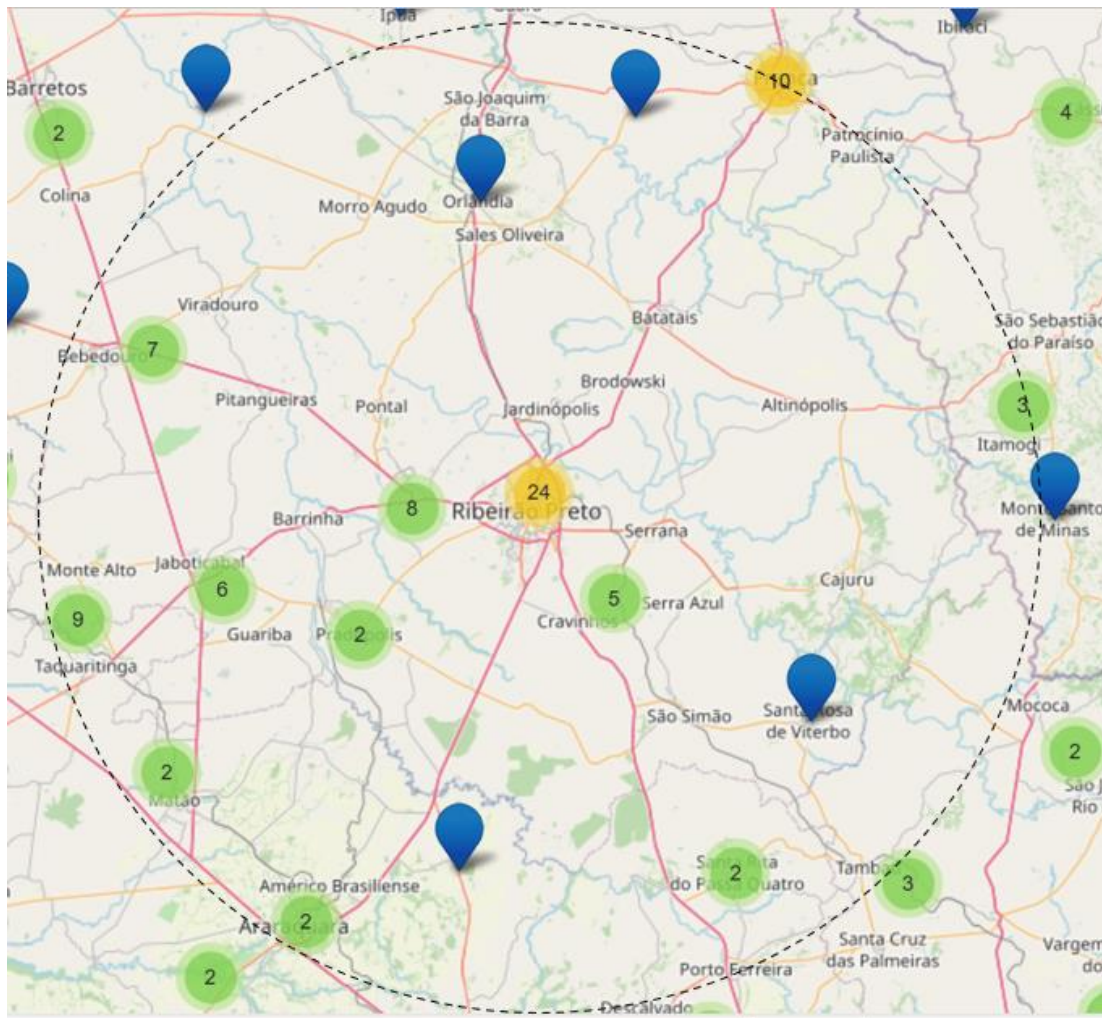


Brasil

- 9.100 AS
- 5.128 AS notificados
- 127.270 endereços IP mal configurados
- **NTP 43.439**
- **SNMP 40.543**
- **DNS 28.373**
- Ref: Fev/26

Programa por uma Internet mais Segura

Notificação de amplificadores - serviços



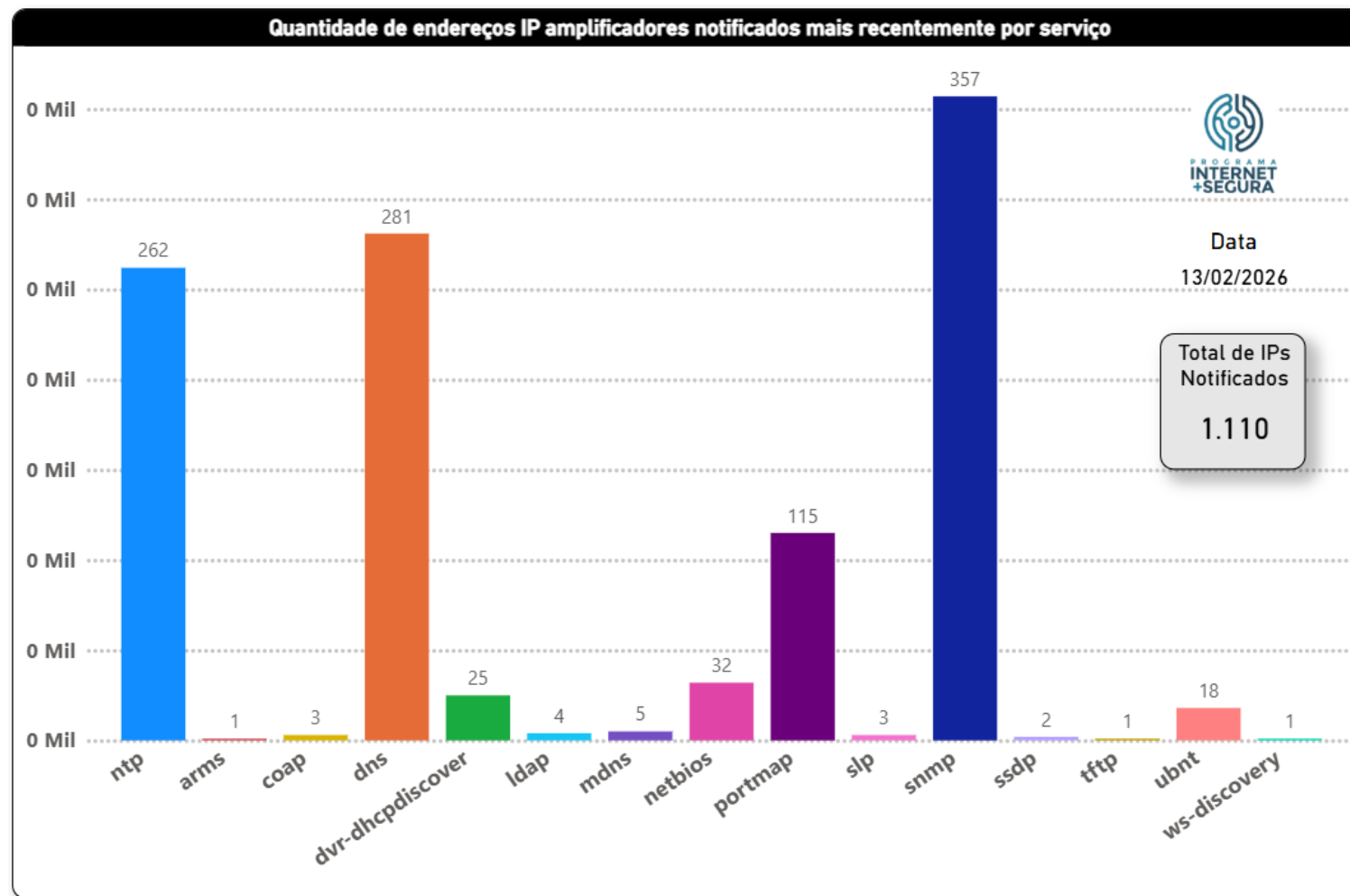
Ribeirão Preto e Região (99 AS)

- Ribeirão Preto (24)
- Franca (10)
- Bebedouro (7)
- Monte Alto (5)
- Araraquara (4)
- Jaboticabal (4)
- Taquaritinga (4)
- Barretos (3)
- Cravinhos (3)
- Sertãozinho (3)
- Altinópolis (2)
- Brodowski (2)
- Guariba (2)
- Itamogi (2)
- Jardinópolis (2)
- Pontal (2)
- Pradópolis (2)

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

Programa por uma Internet mais Segura

Notificação de amplificadores - serviços



Ribeirão Preto e Região

- 99 AS
- 11 AS conectados ao IX RPO
- 63 AS notificados
- 2 AS com mais de 100 IP notificados
- 1.110 endereços IP mal configurados
 - SNMP 357
 - DNS 281
 - NTP 262



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)

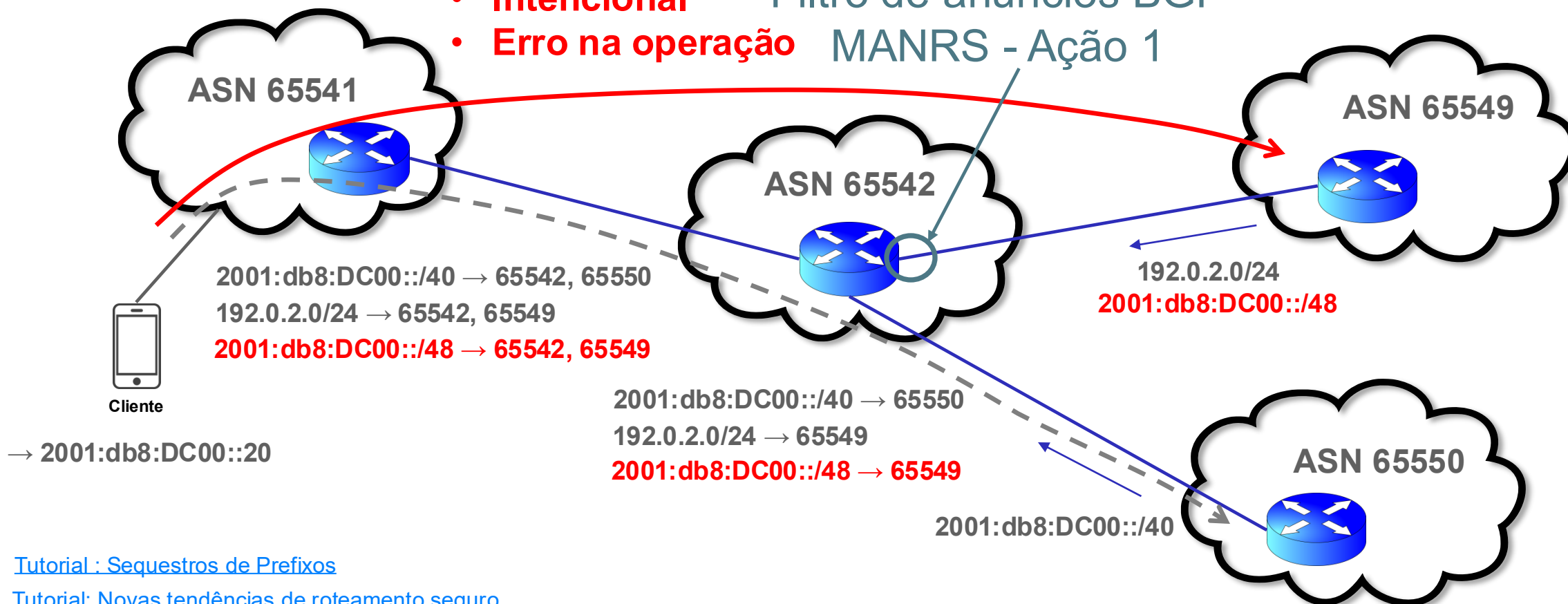
Anúncio de prefixos não autorizados:

- Intencional

Filtro de anúncios BGP

- Erro na operação

MANRS - Ação 1



[Tutorial: Sequestros de Prefixos](#)

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

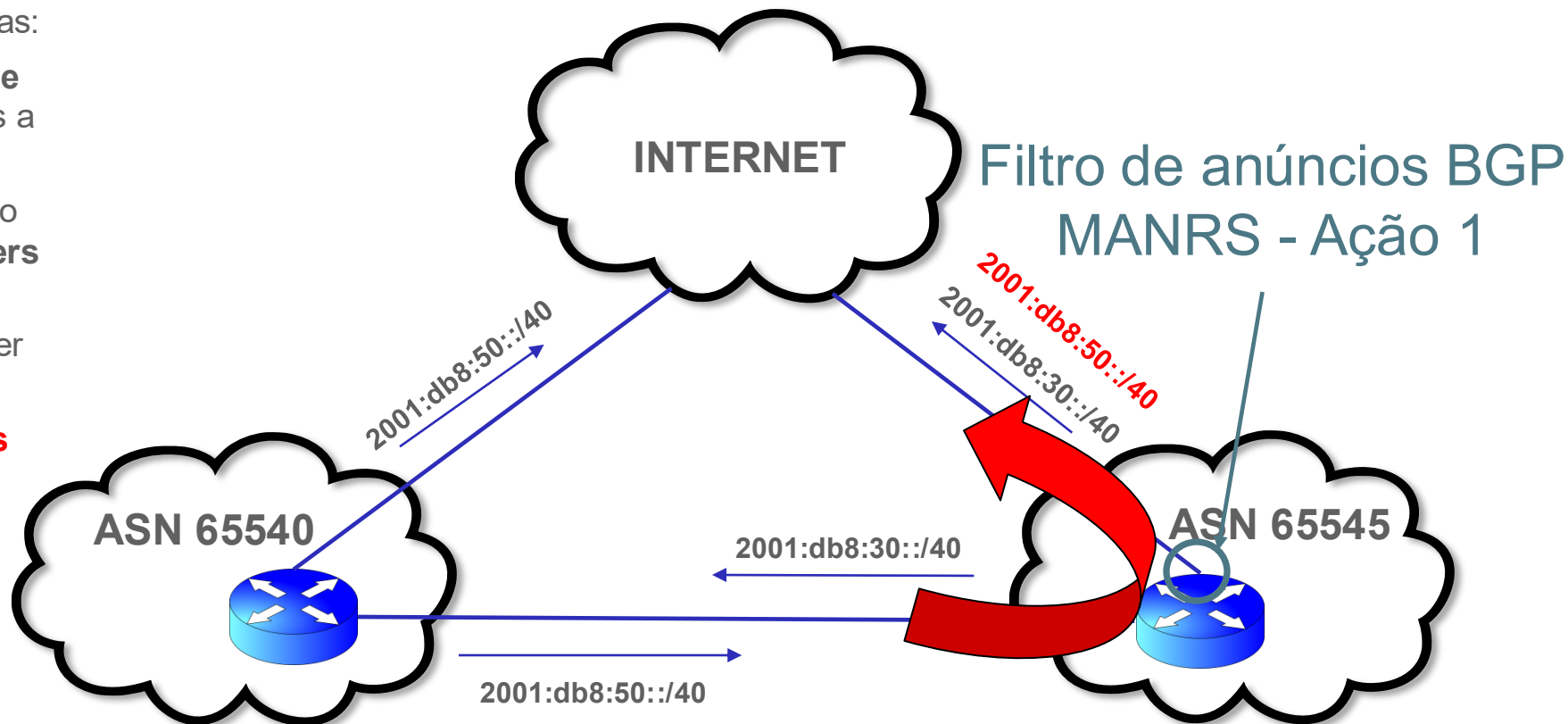
Programa por uma Internet mais Segura



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



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

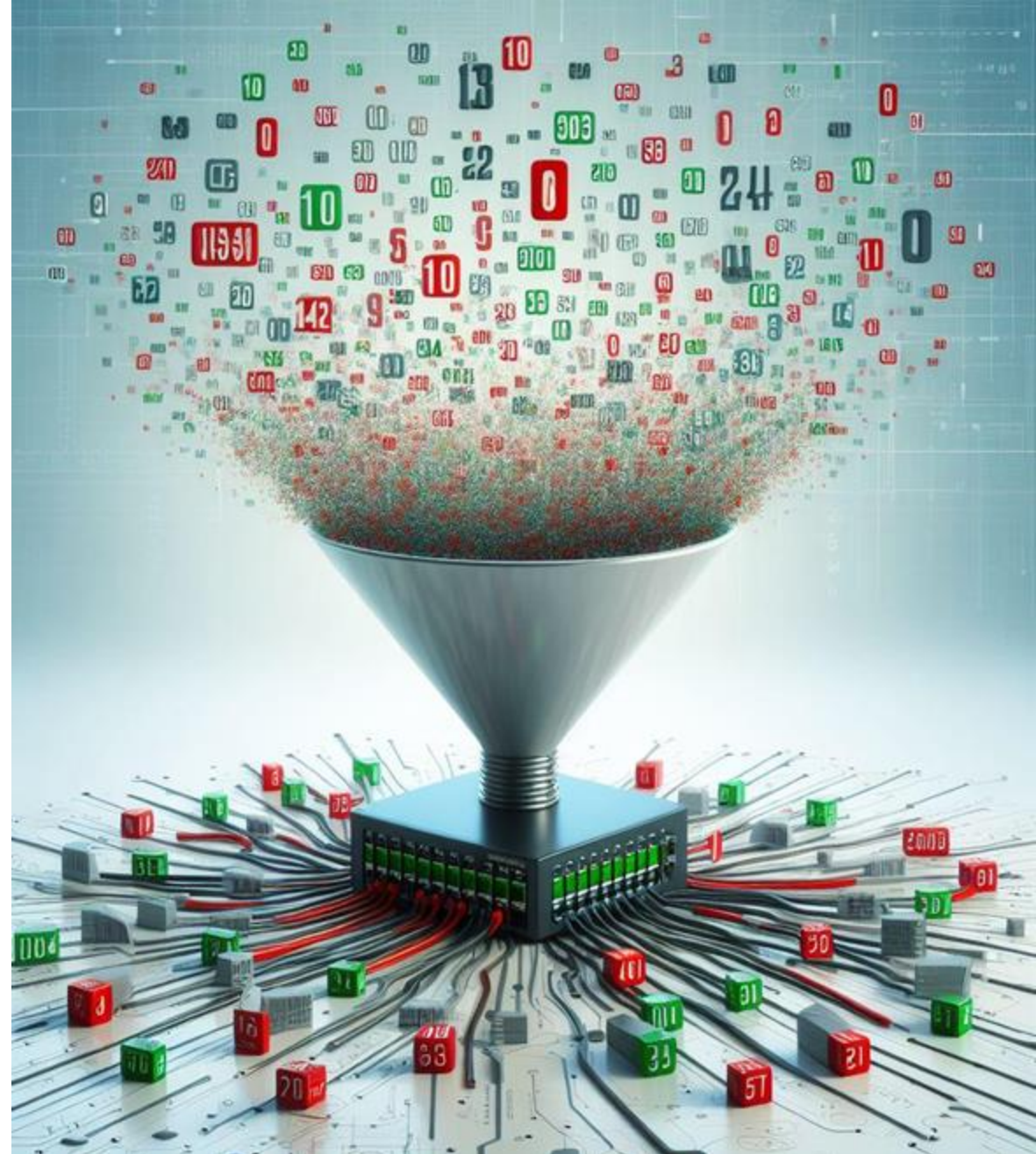
Programa por uma Internet mais Segura



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
- 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

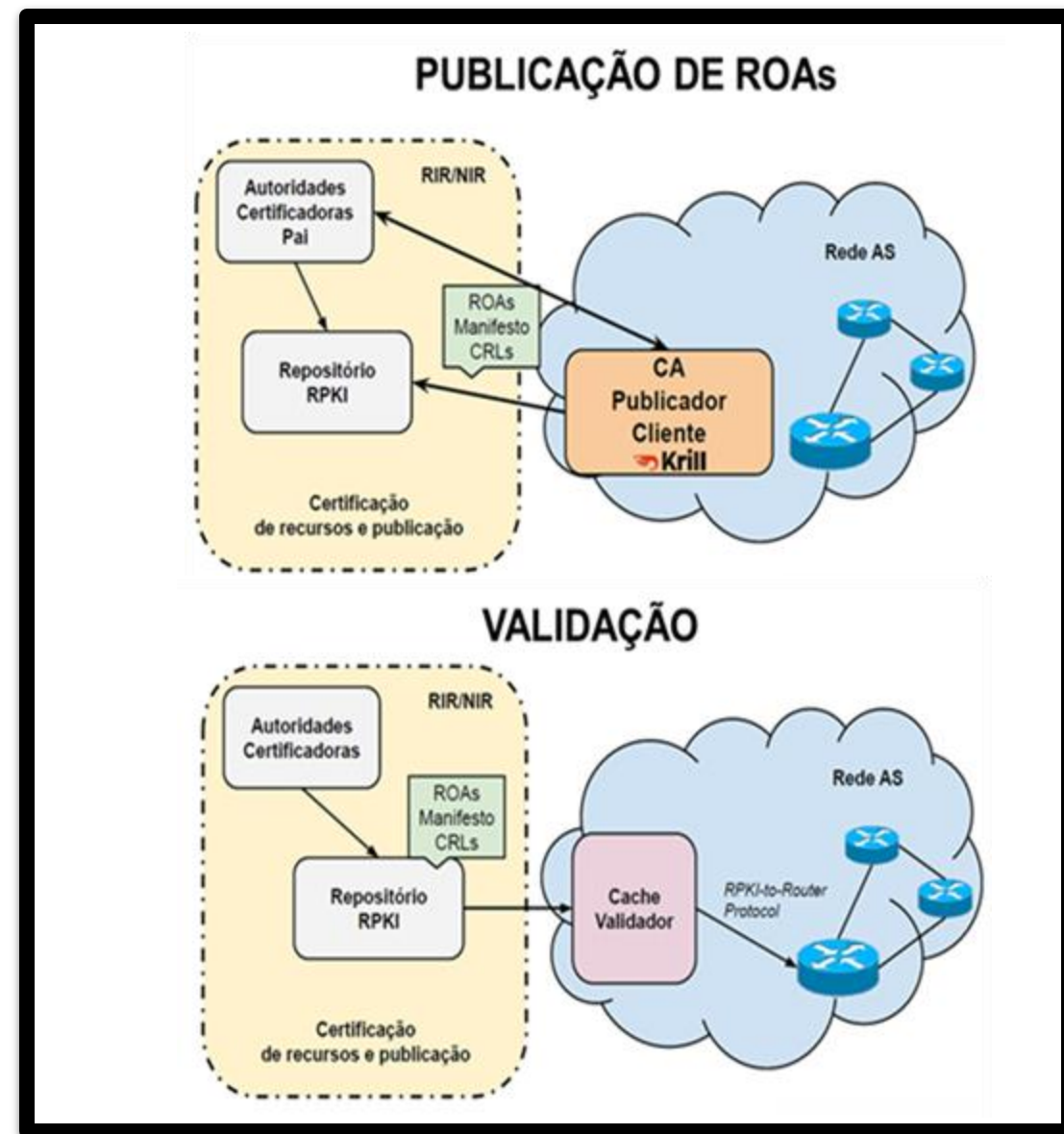
- IRR - Internet Routing Registry
 - RADB
 - TC (gratuito)
- RPKI - Resource Public Key Infrastructure

<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 - Ribeirão Preto - 98 AS

Resumo

25-fev-26



MANRS

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

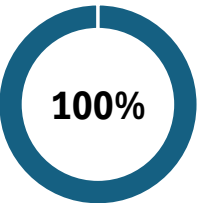
IRR			RPKI		
Não registrado	23	1,8%	Válido	475	37,7%
Registrado	1.236	98,2%	Desconhecido	781	62,0%
			Inválido	3	0,2%

■ Não registrado ■ Registrado

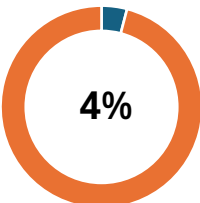
■ Válido ■ Desconhecido ■ Inválido

MANRS - Prontidão

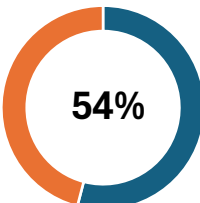
Filtros BGP



Anti-spoofing

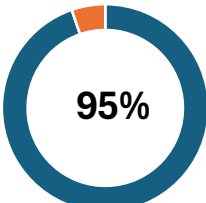


Coordenação

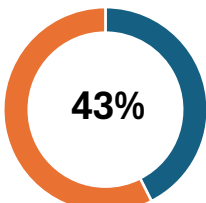


Informação de Roteamento

IRR



RPKI



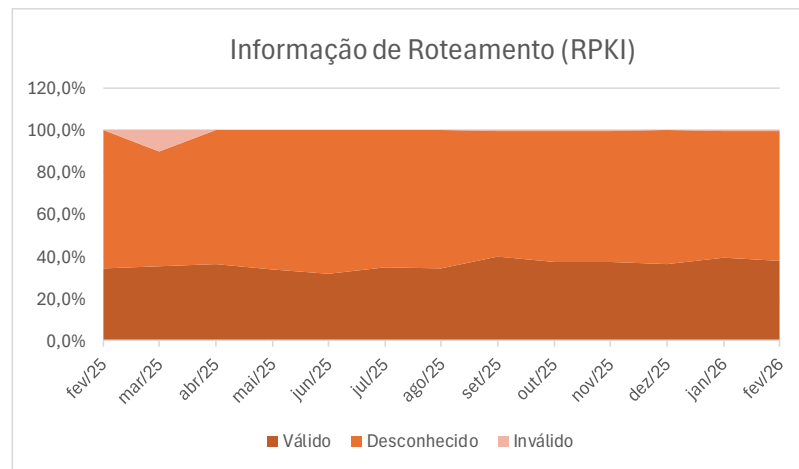
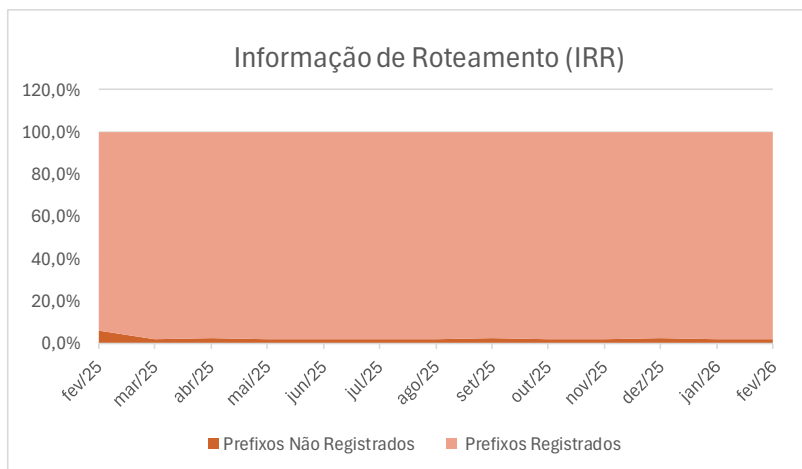
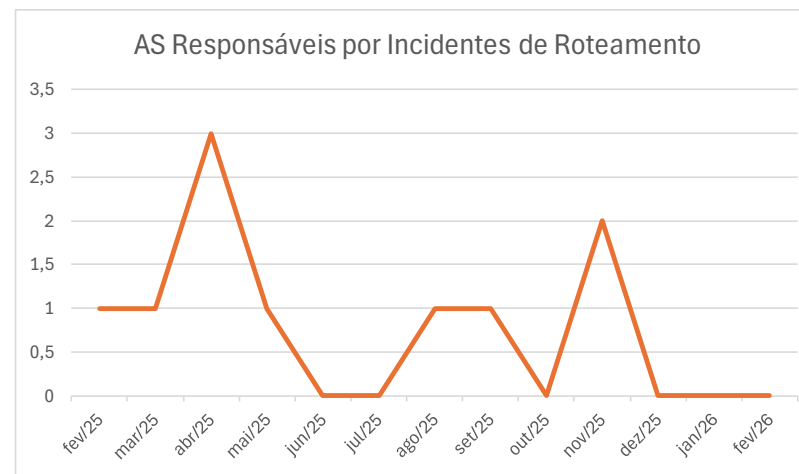
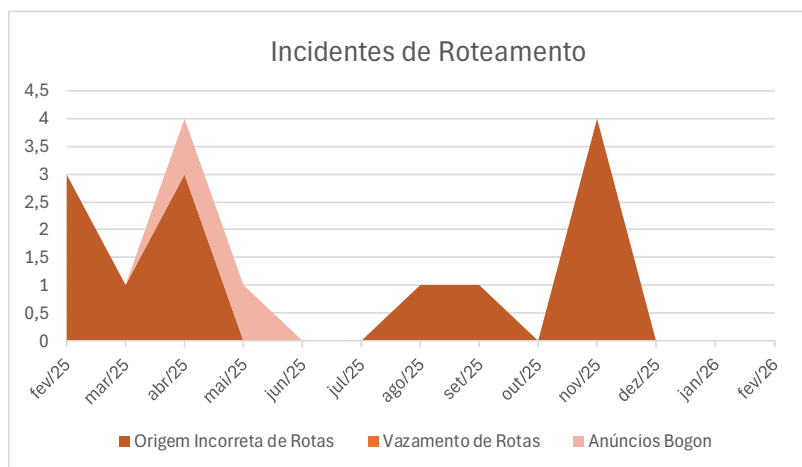
Fonte: <https://observatory.manrs.org/> - acesso logado em 25/02/26

Programa por uma Internet mais Segura

MANRS Observatory - Ribeirão Preto -

98 AS

Histórico



Fonte: <https://observatory.manrs.org/> - acesso logado em 25/02/26

Programa por uma Internet mais Segura

MANRS Observatory - 98 AS – RPO



ASN	Country	Filtering	Anti-spoofing	Coordination	Routing Information (IRR)	Routing Information (RPKI)	Status abuse-c	Status Notificações CERT.br	MANRS Participante
ASN1	BR	100%		100%	100%	100%	PEND		
ASN2	BR	100%		100%	100%	0%	PEND		
ASN3	BR	100%		0%	100%	38%	PEND		
ASN4	BR	100%		100%	100%	0%	PEND		
ASN5	BR	100%		0%	100%	0%	PEND		
ASN6	BR	100%		0%	100%	0%	OK	NOK	
ASN7	BR	100%	49%	100%	100%	100%	OK		28352
ASN8	BR	100%		100%	100%	100%	OK		53152
ASN9	BR	100%		100%	100%	100%	OK		61595
ASN10	BR	100%		100%	100%	100%	OK		263142
ASN11	BR	100%	100%	100%	100%	100%	OK		264426
ASN12	BR	100%		100%	100%	71%	OK		266044
ASN13	BR	100%		100%	90%	0%	OK		266525
ASN14	BR	100%	100%	100%	100%	100%	OK		266984
ASN89	BR	100%	100%	100%	100%	100%			273514

PEND: Status de pendência junto ao Registro.br
NOK: CERT.br não consegue entregar notificações

9 AS da região são participantes do MANRS

Programa por uma Internet mais Segura



Participantes por país

- Total: 1.095
- Participantes no Brasil → 319



MANRS

2024 → 292

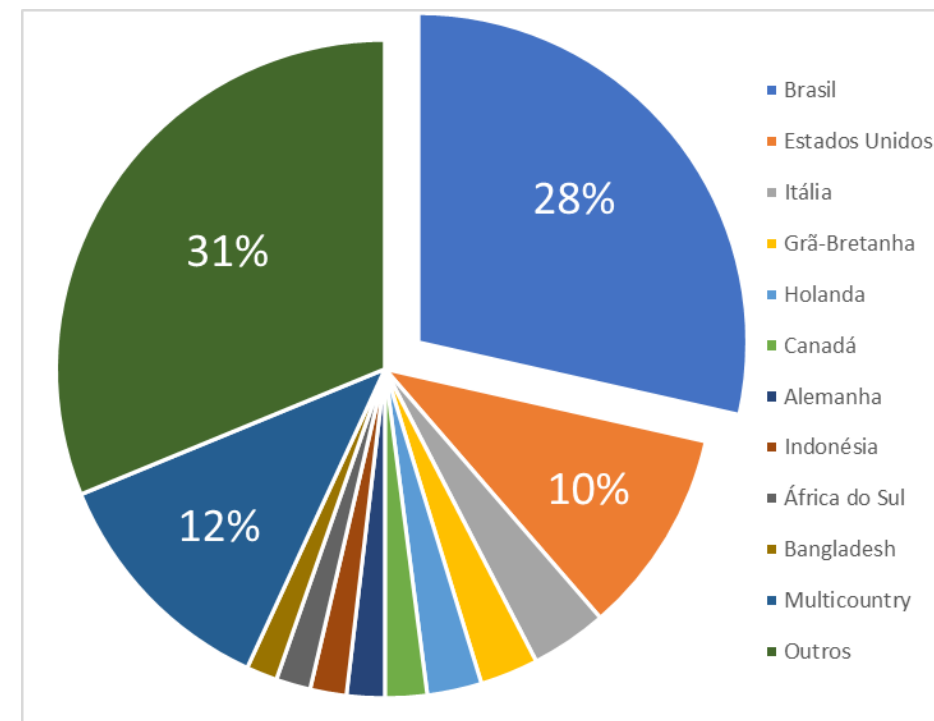
2023 → 258

2022 → 206

2021 → 174

2020 → 140

% de Participantes



Fonte: <https://www.manrs.org/netops/participants/> Acesso 25/02/26

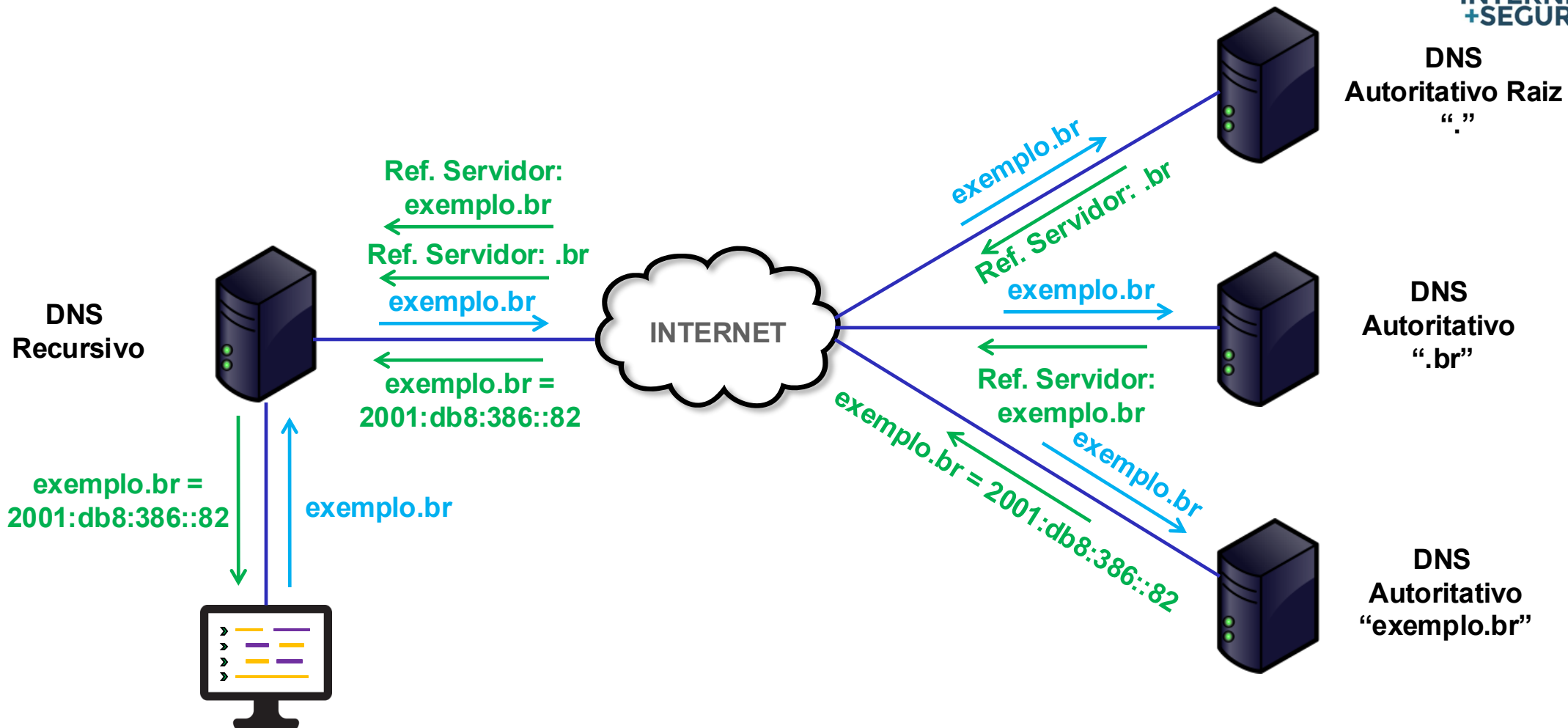


Stands for **K**nowledge-Sharing and
Instantiating **N**orms for **D**NS and **N**aming
Security

<https://kindns.org/>

Programa por uma Internet mais Segura

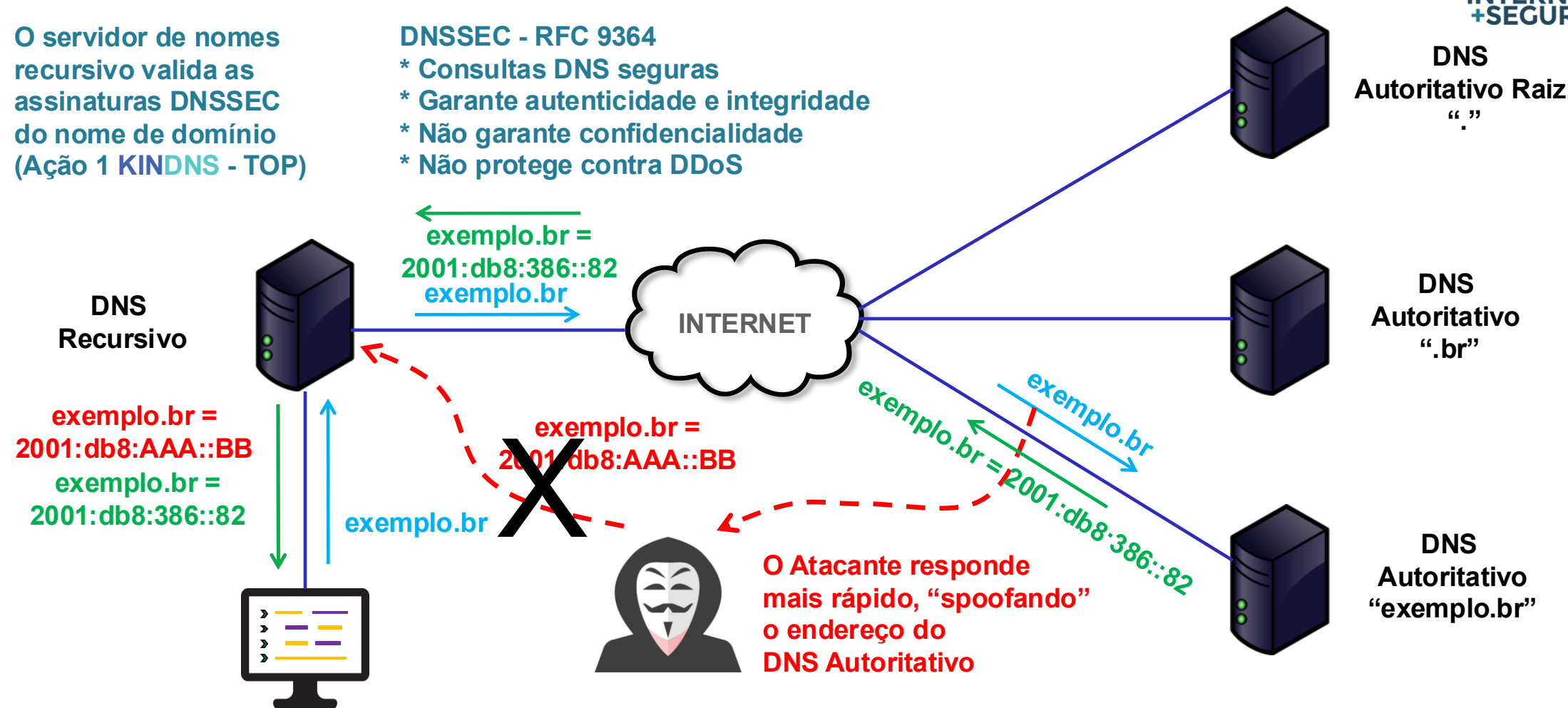
Processo de Recursão DNS



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

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>

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

<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
 - 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

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

The screenshot shows the TOP website with a header containing the logo and navigation links: Quem é TOP, Sobre, Referências, and Comunicados. The main heading asks if the user is using modern Internet standards. Below this are three test cards: 1. 'Teste TOP - Site' (green) for website security checks, 2. 'Teste TOP - E-mail' (blue) for email security checks, and 3. 'Teste TOP - IPv6 e DNSSEC da sua rede' (purple) for network-level checks. Each card includes a list of checks, a text input field for domain information, and a button to start the test. At the bottom, the URL <https://top.nic.br> is displayed.

Programa por uma Internet mais Segura



Nota média de validação DNSSEC por recursivos – Região Rib. Preto

Nota Média de Validação de DNSSEC por AS por Ano					
Nota média por AS	2022	2023	2024	2025	2026
0% a 20%	6%	7%	1%	2%	12%
20% a 50%	14%	6%	17%	4%	0%
50% a 80%	36%	27%	2%	32%	24%
80% a 100%	44%	61%	80%	62%	64%

Total de Sistemas Autônomos na Região	99
---------------------------------------	----

Total de Sistemas Autônomos que fizeram medições	74
--	----

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



Programa por uma Internet mais Segura



Acompanhamento gerencial das notificações de amplificadores notificados pelo CERT.br

ASN	DNS	SNMP	NTP	SSDP	PORTMAP	MEMCACHED	NETBIOS	QOTD	CHARGEN	LDAP	MDNS	UBNT	WS-DISCOVERY	TFTP	CoAP	ARMS	SLP	RIPv1 (novo)	DHCPdiscover	2025-11	2025-12	2026-01	2026-02	MT4145	MT5678
ASN1	28	52	13	0	8	0	5	0	0	0	3	2	0	0	0	0	0	0	1	124	122	124	112	0	0
ASN2	24	100	32	0	23	0	6	0	0	1	2	0	0	0	0	0	0	0	1	196	161	183	189	0	0
ASN3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
ASN4	57	37	5	0	14	0	8	0	0	1	1	0	0	0	0	0	0	0	1	127	129	132	124	0	1
Total	-19%	-1%	-4%	-100%	10%		18%			-38%	-3%	-25%		-100%		-100%			64%	447	412	439	425	-100%	0%

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

27 de fevereiro de 2026

nic.br **cgi.br**

www.nic.br | www.cgi.br

