



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 Norte

Palmas, TO | 31/07/26

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



MANRS

KINDNS



TOP – 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

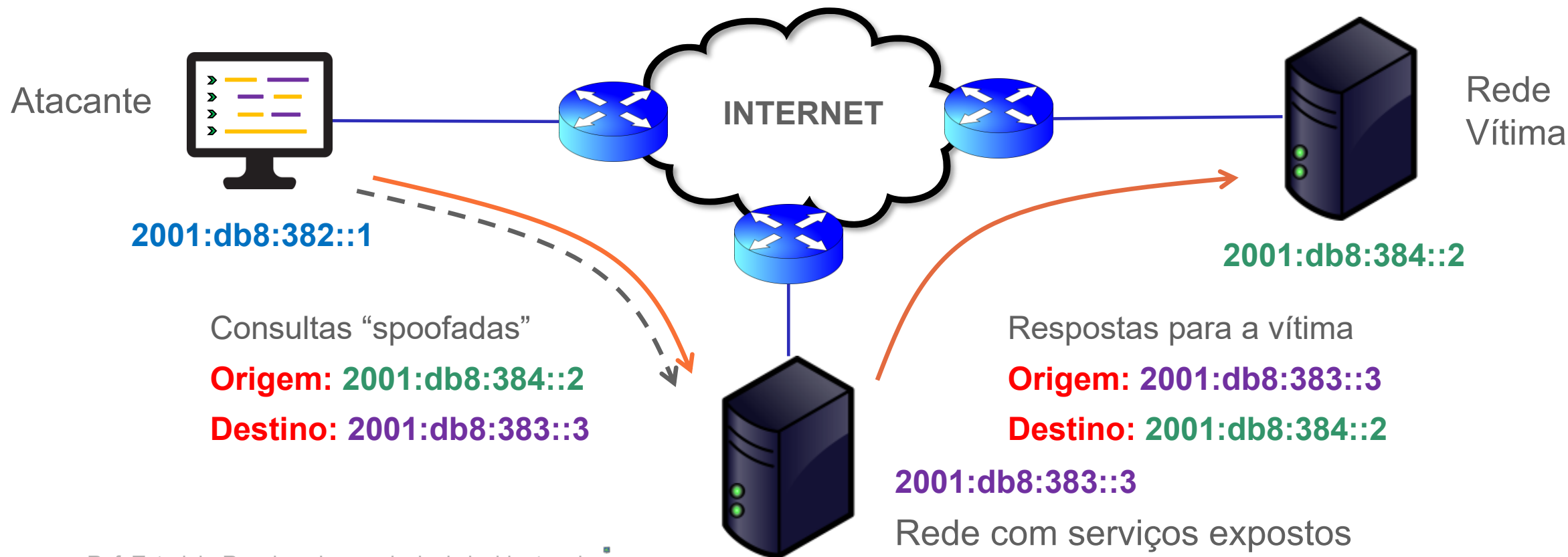
<https://bcp.nic.br/i+seg/acoes/amplificacao/>



Programa por uma Internet mais Segura

Negação de Serviço Reflexivo com Amplificação

Utiliza um terceiro para fazer o ataque



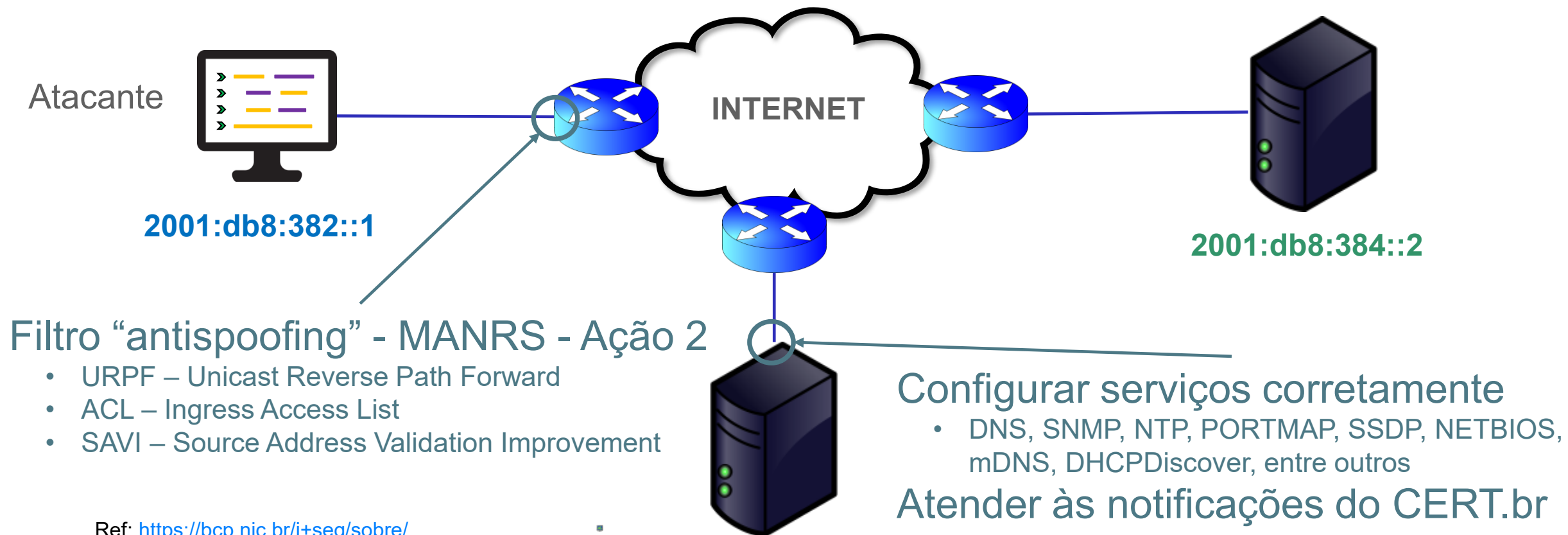
Ref. Tutorial - Resolvendo os principais incidentes de segurança

Programa por uma Internet mais Segura

Negação de Serviço Reflexivo com Amplificação

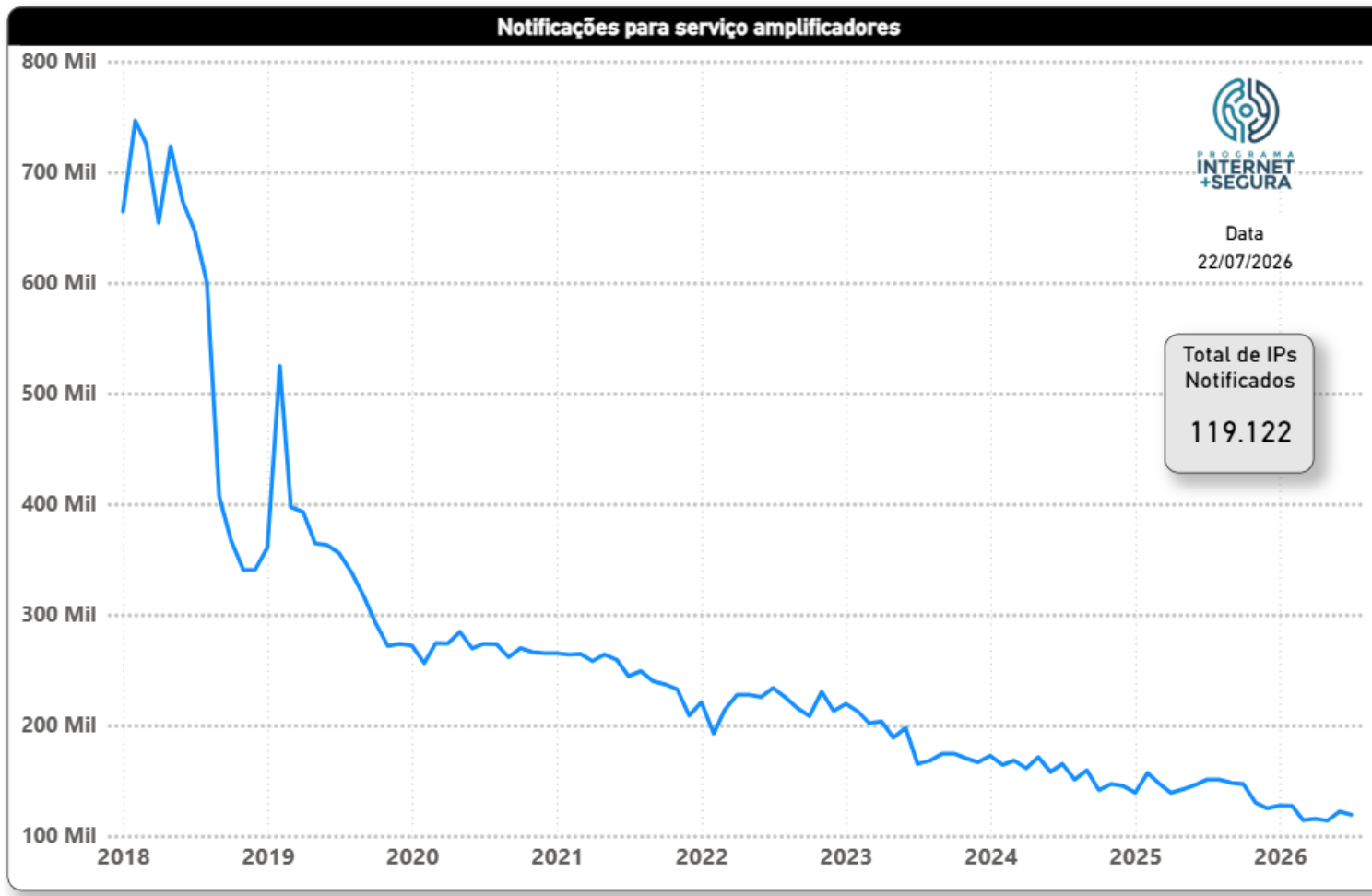


Como resolver o problema



Programa por uma Internet mais Segura

Notificação de amplificadores - evolução

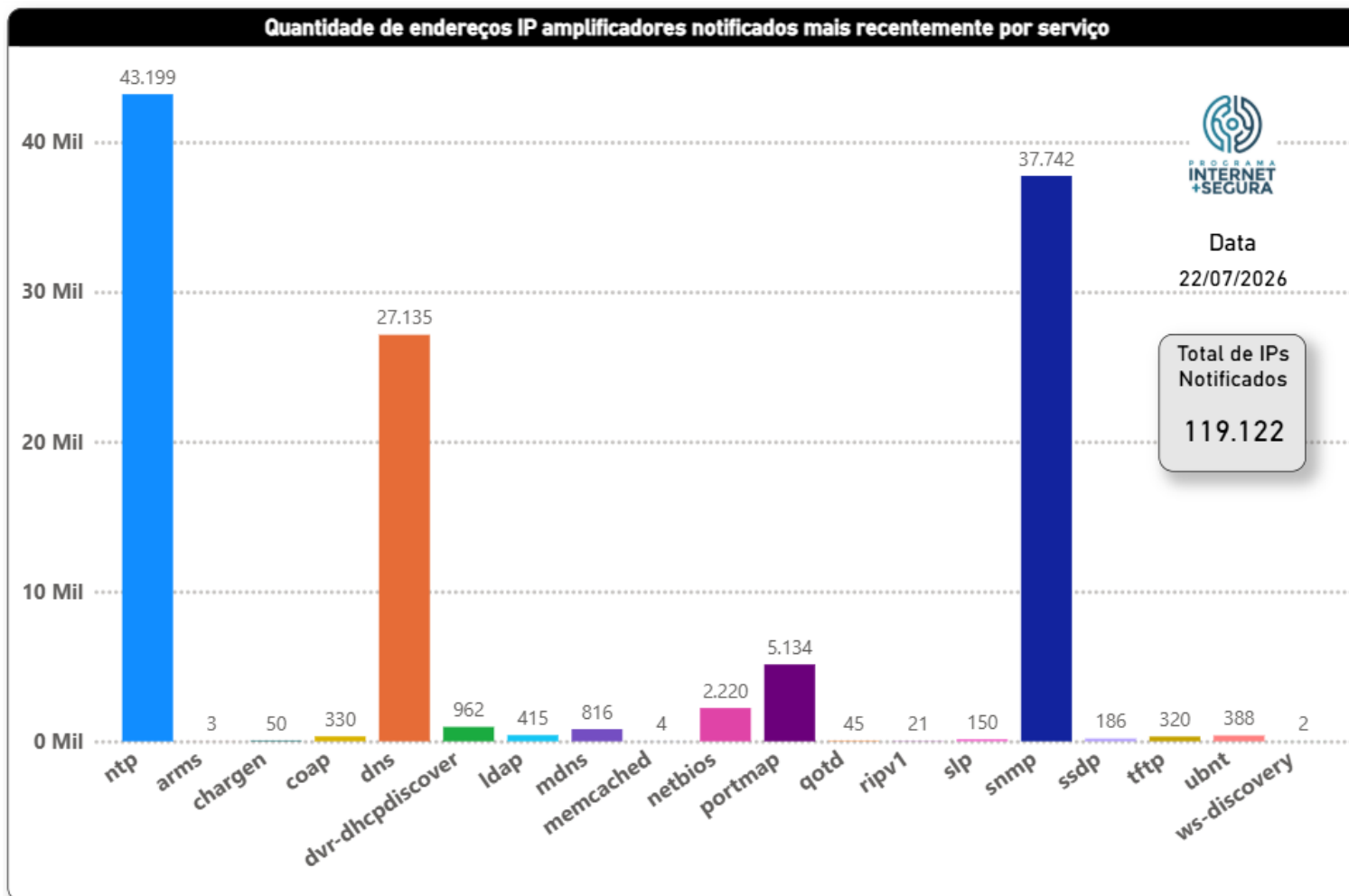


Brasil

- Início (fev/2018)
 - Endereços IP: 746.508
 - Serviços: 5
- Atual:
 - Endereços IP: 119.122
 - Serviços: 19
 - **Redução de 84%**
 - Ref. Jul/26

Programa por uma Internet mais Segura

Notificação de amplificadores - serviços

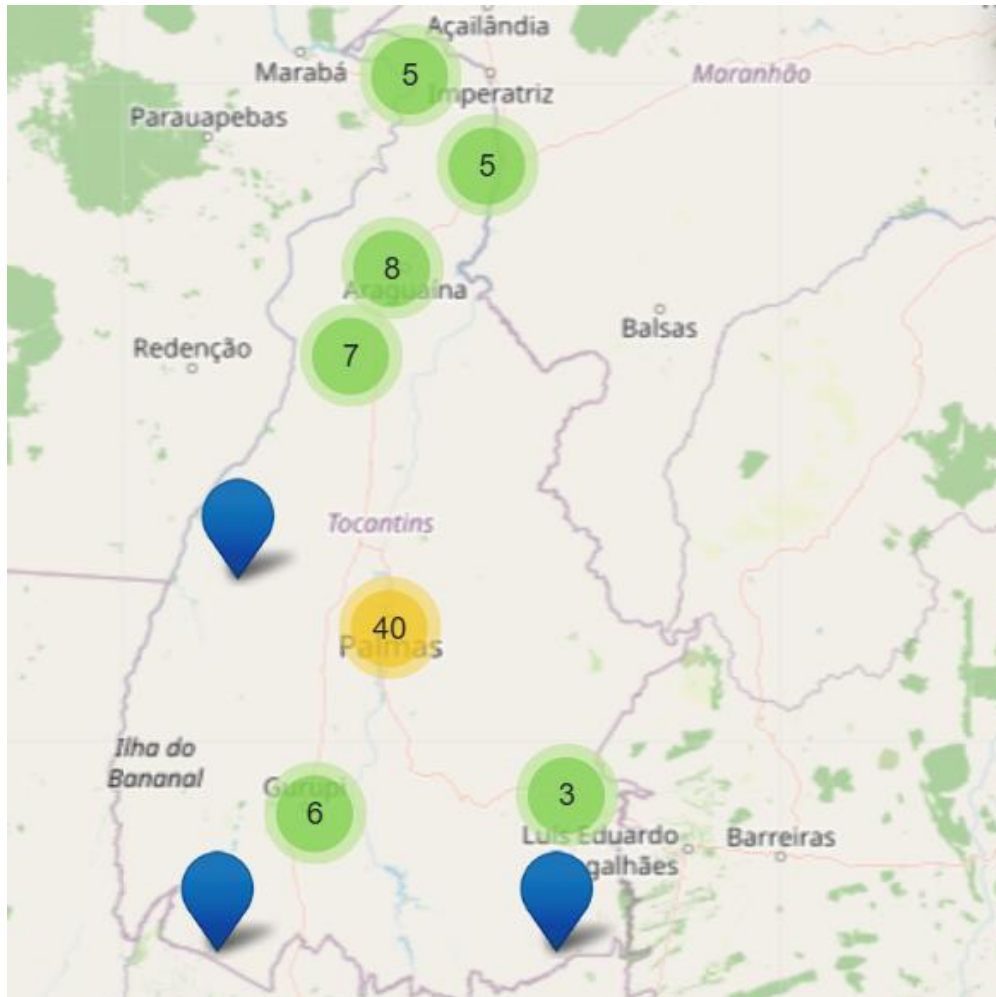


Brasil

- 9.106 AS
- 4.820 AS notificados
- 119.122 endereços IP mal configurados
- **NTP 43.199**
- **SNMP 37.742**
- **DNS 27.135**
- Ref: Jul/26

Programa por uma Internet mais Segura

Notificação de amplificadores - serviços



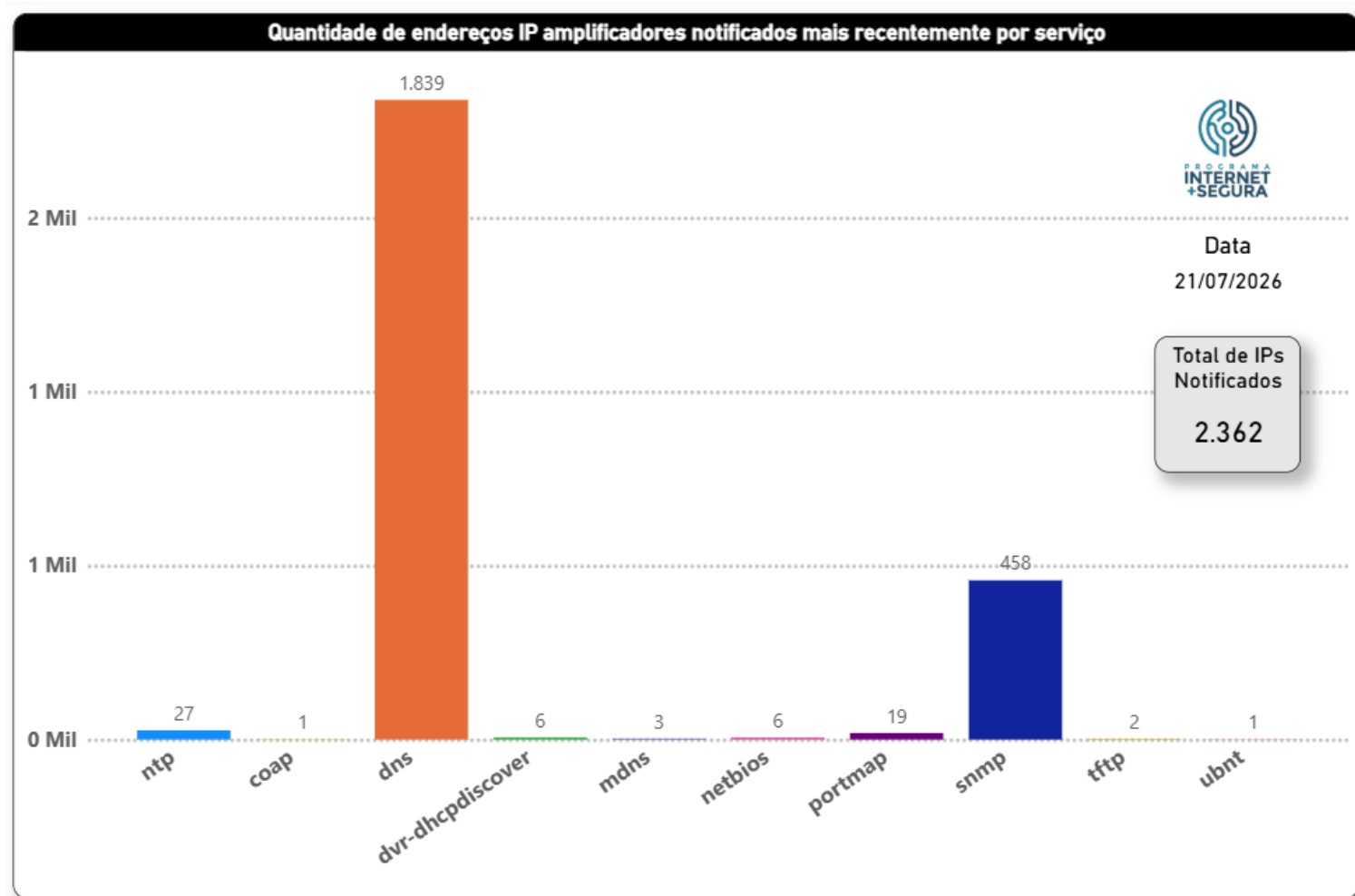
Estado do Tocantins (79)

Palmas	(18)
Araguaína	(9)
Gurupi	(6)
Pedro Afonso	(4)
Porto Nacional	(4)
Araguatins	(3)
Colinas do Tocantins	(3)
Dianópolis	(3)
Paraíso do Tocantins	(3)
Axixá do Tocantins	(2)
Tocantinópolis	(2)
Xambioá	(2)
Aparecida do Rio Negro	(1)
Araguaçu	(1)
Arraias	(1)
Augustinópolis	(1)

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

Programa por uma Internet mais Segura

Notificação de amplificadores - serviços



Estado do Tocantins

- 79 AS em TO
- 36 AS participantes no IX Palmas, 20 do TO
- 52 AS notificados
- 1 AS com mais de 1000 IP notificados (1197)
- 4 AS com mais de 100 IP notificados
- 2362 endereços IP mal configurados
 - DNS 1839
 - SNMP 458



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/>



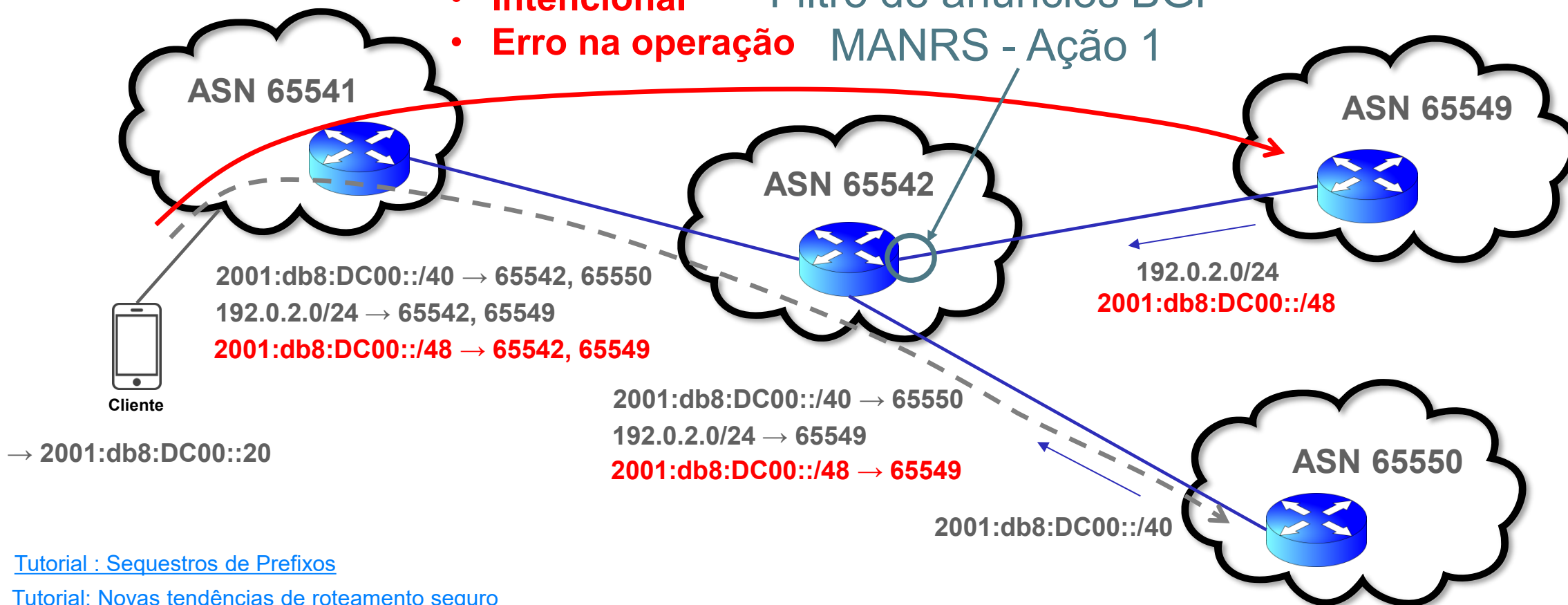
Programa por uma Internet mais Segura

Sequestro de prefixos (Hijacking)

Anúncio de prefixos não autorizados:

- Intencional
- Erro na operação

Filtro de anúncios BGP
MANRS - Ação 1



[Tutorial : Sequestros de Prefixos](#)

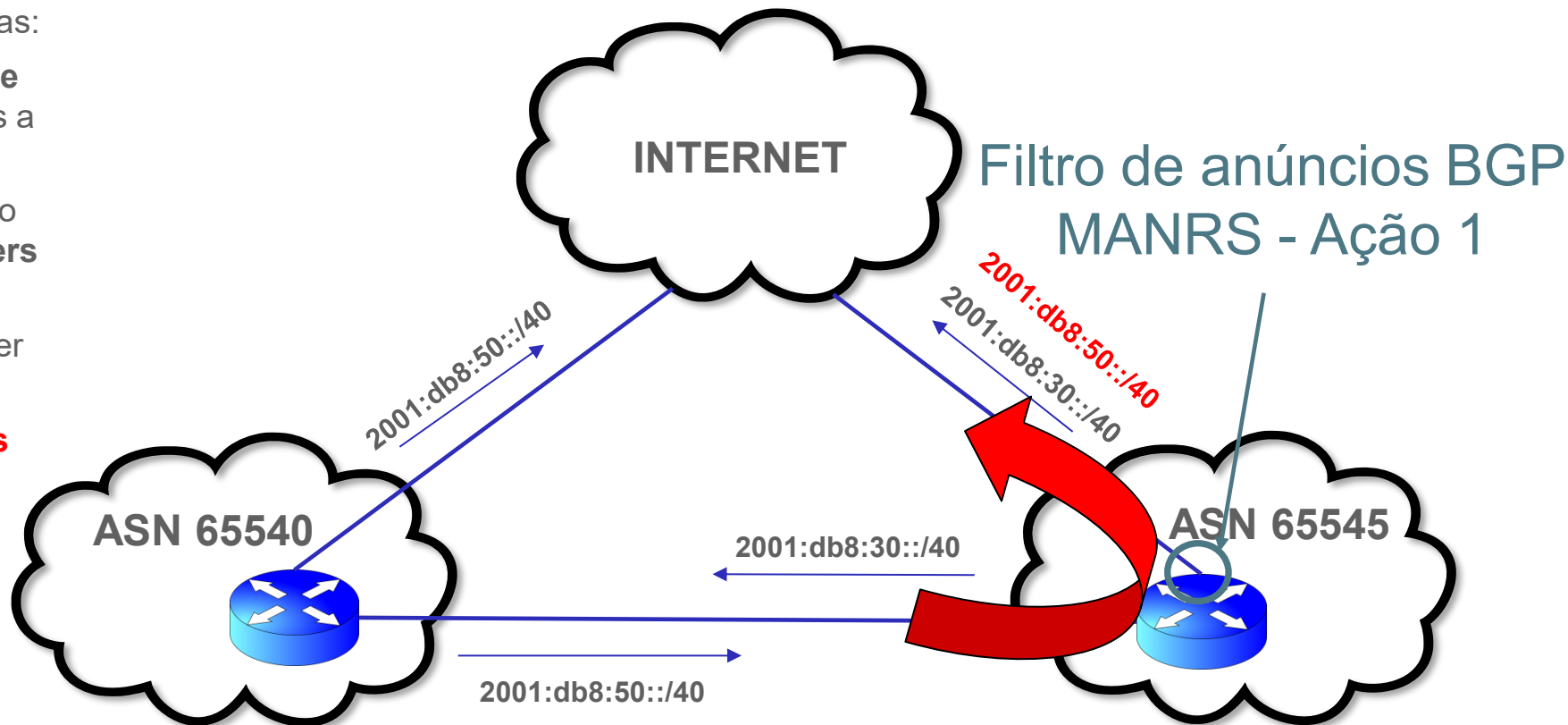
[Tutorial: Novas tendências de roteamento seguro](#)

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



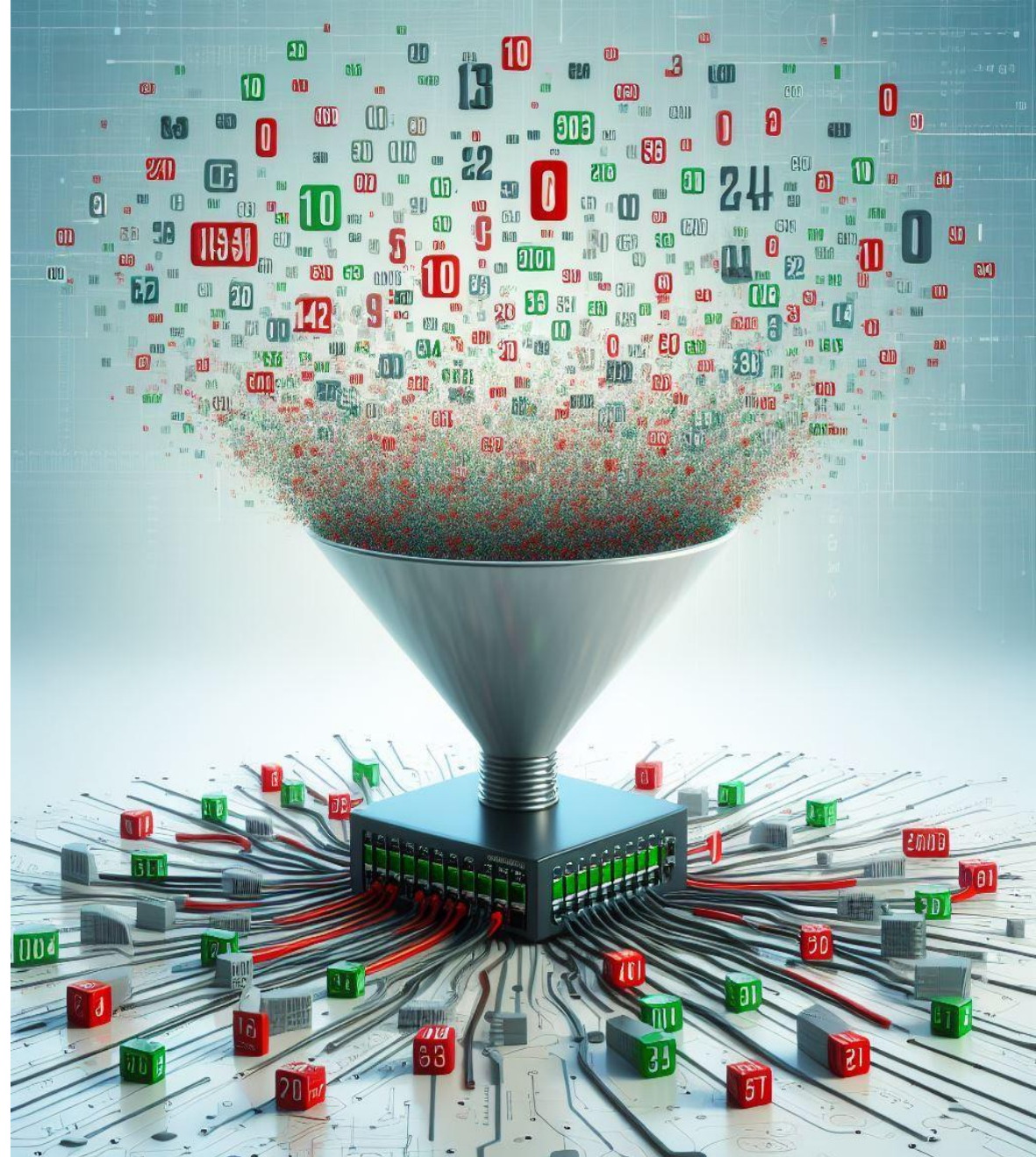
Programa por uma Internet mais Segura



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

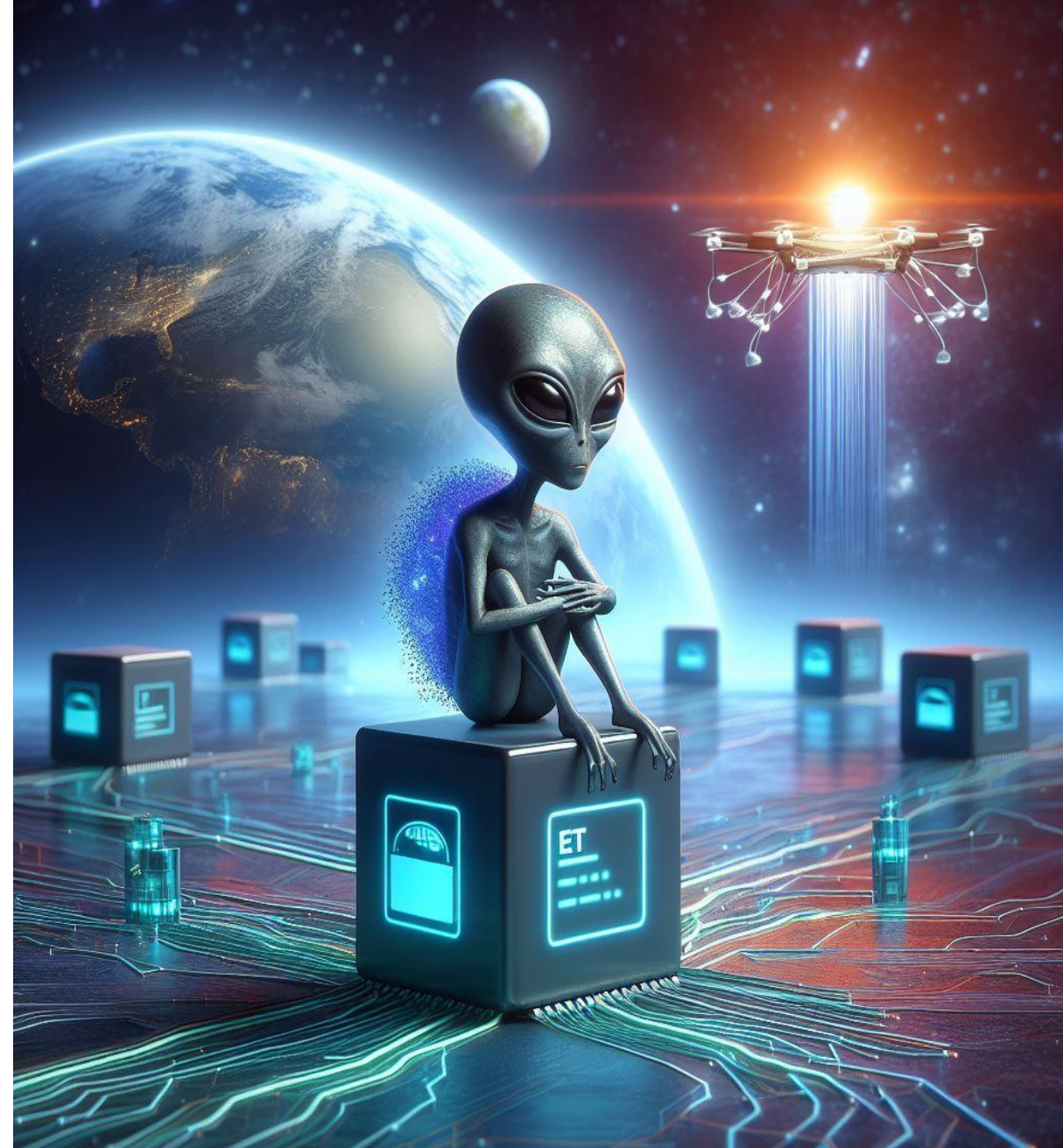


MANRS - Ação 2 - Filtro Anti-spoofing

- 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



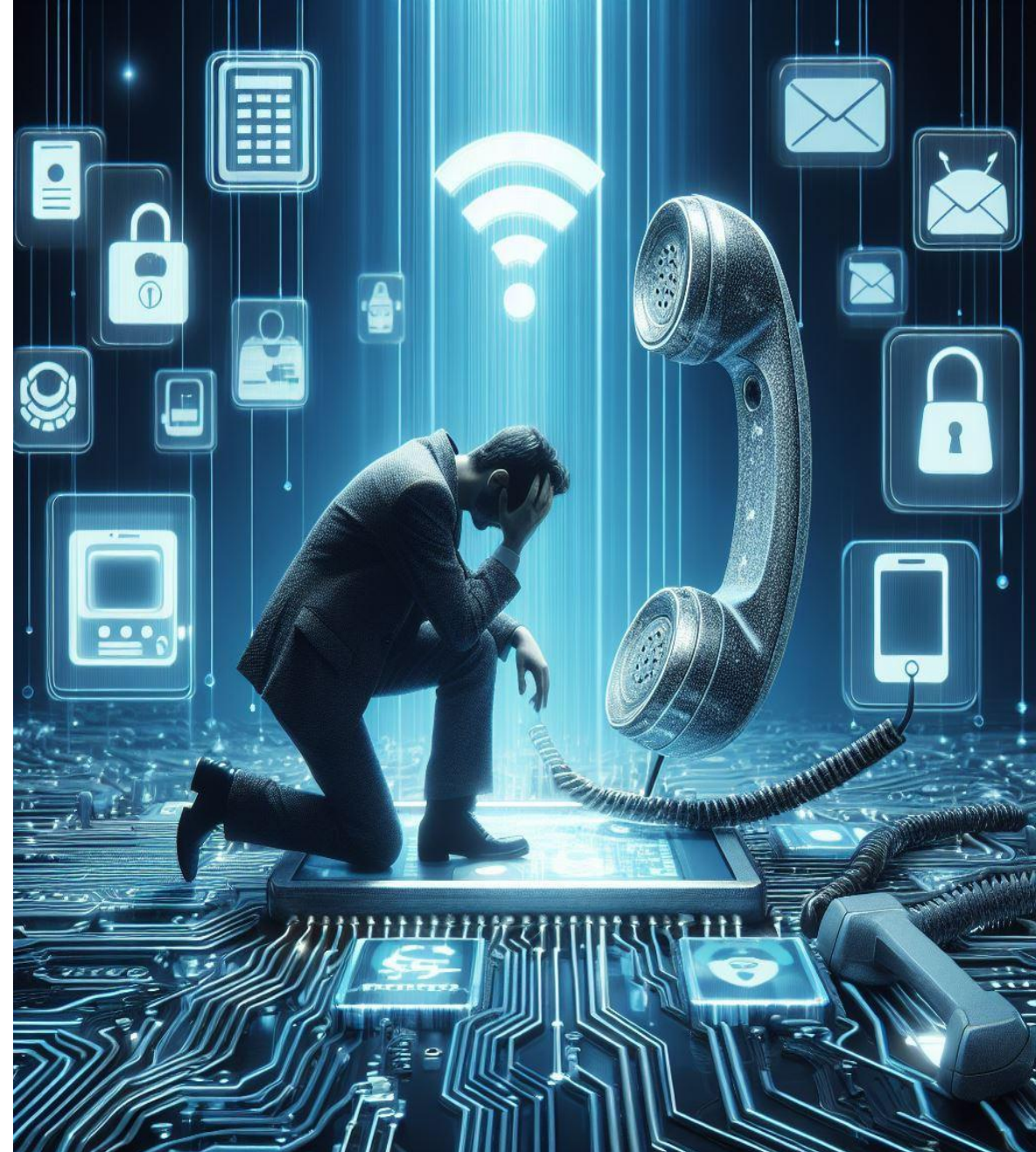
MANRS - Ação 3 - Pontos de Contato

- 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

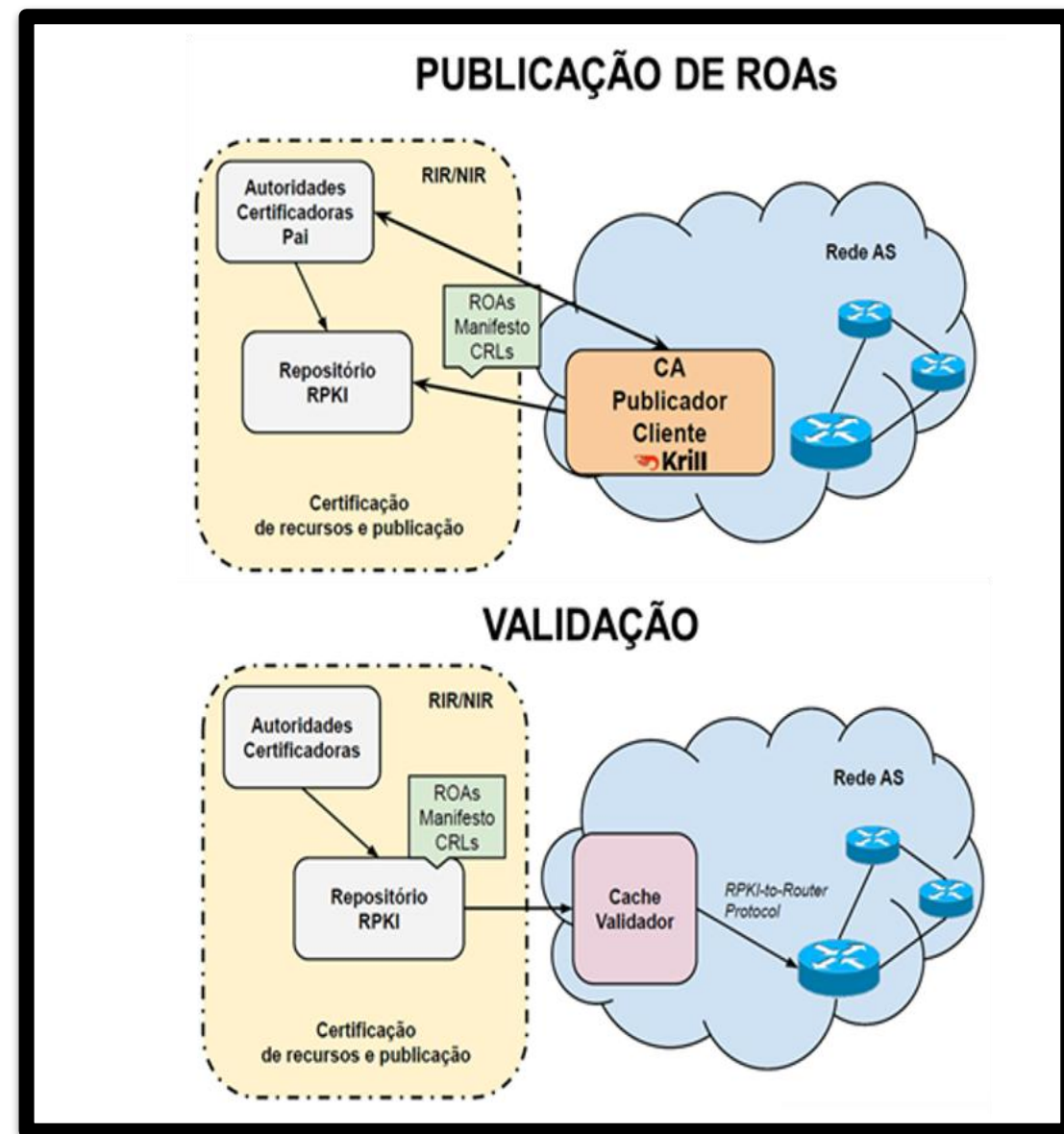
- **IRR** - Internet Routing Registry
 - RADB
 - TC (gratuito)
- **RPKI** - Resource Public Key Infrastructure

<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 - Estado do Tocantins - 79 AS

Resumo

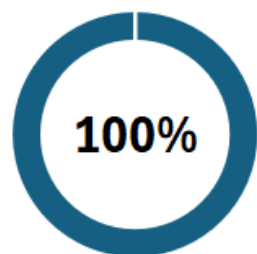
jul-26



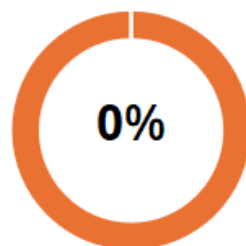
MANRS

MANRS - Prontidão

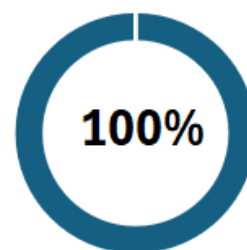
Filtros BGP



Anti-spoofing

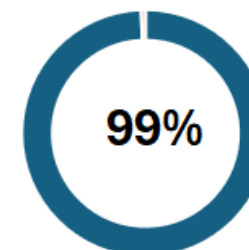


Coordenação

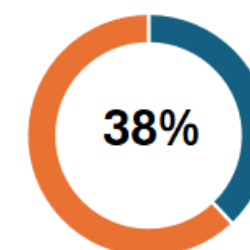


Informação de Roteamento

IRR



RPKI



Fonte: <https://observatory.manrs.org/> - acesso logado em 29/07/26

Programa por uma Internet mais Segura



Participantes por país

- Total: 1.152
- Participantes no Brasil → 324



MANRS

2024 → 292

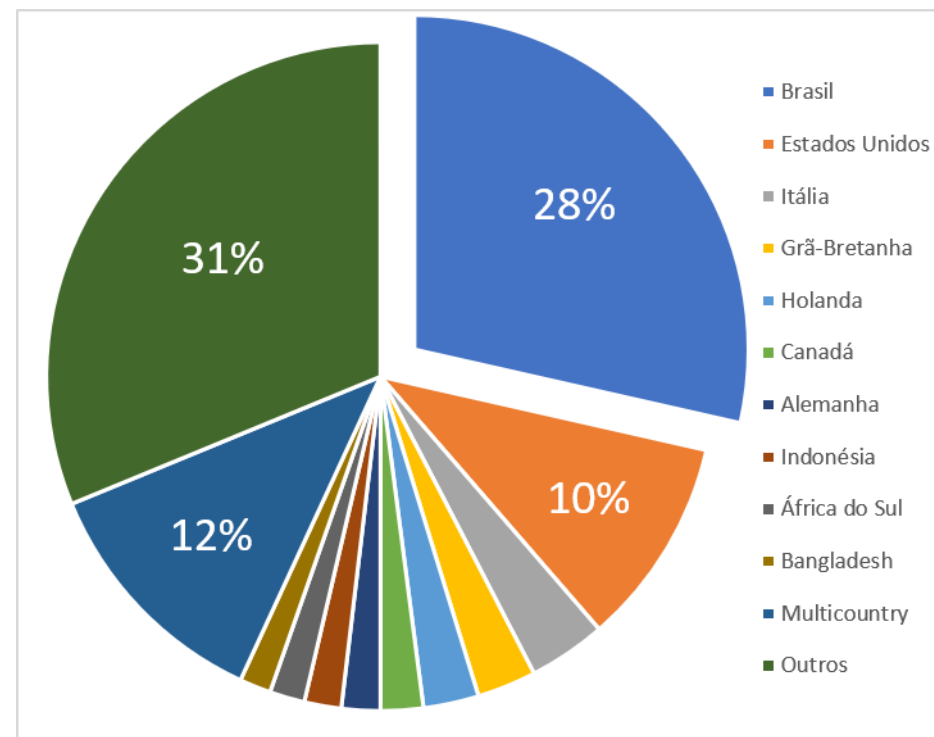
2023 → 258

2022 → 206

2021 → 174

2020 → 140

% de Participantes



Fonte: <https://www.manrs.org/netops/participants/> Acesso 29/07/26

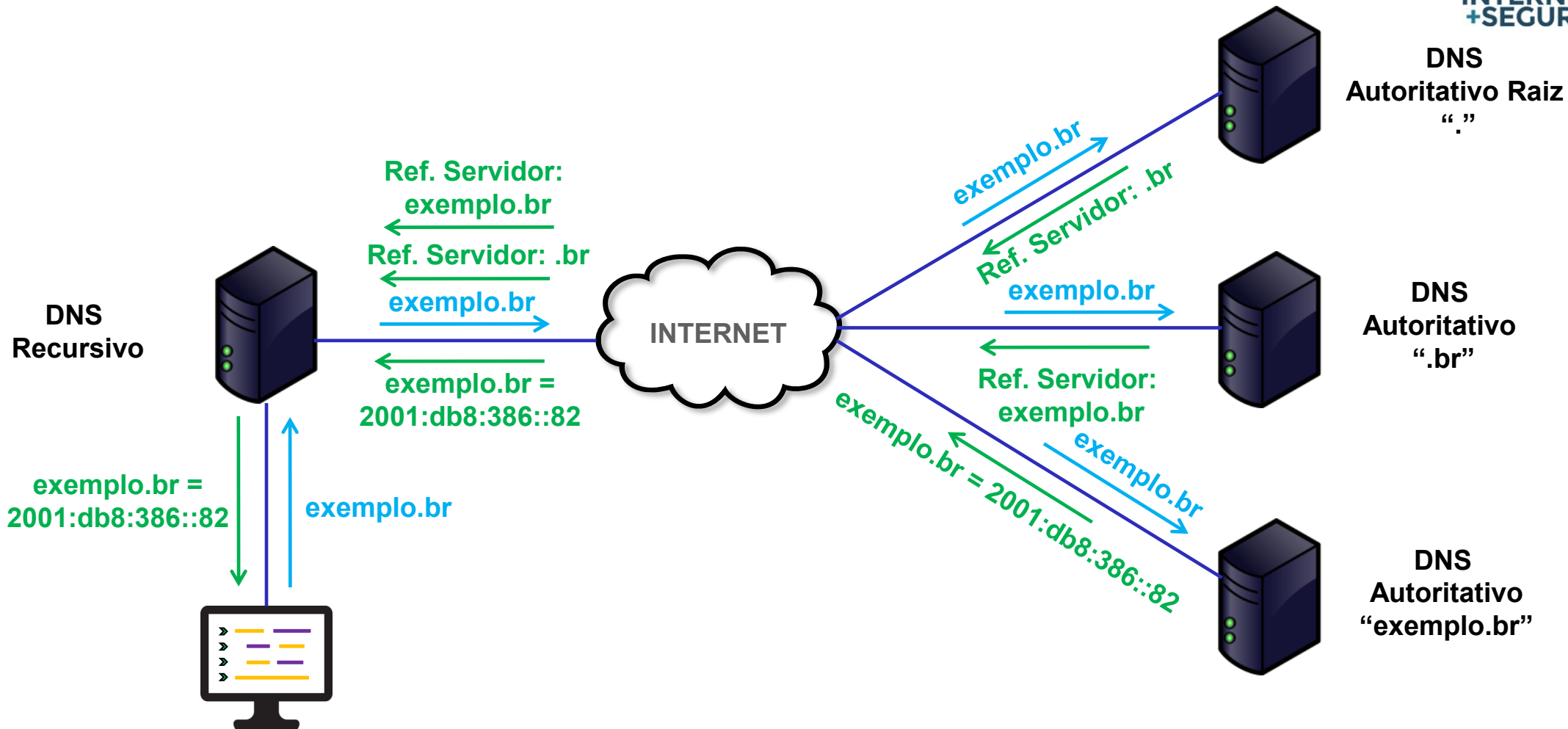


Stands for **K**nowledge-Sharing and
Instantiating **N**orms for **D**NS and **N**aming
Security

<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](#)

Programa por uma Internet mais Segura

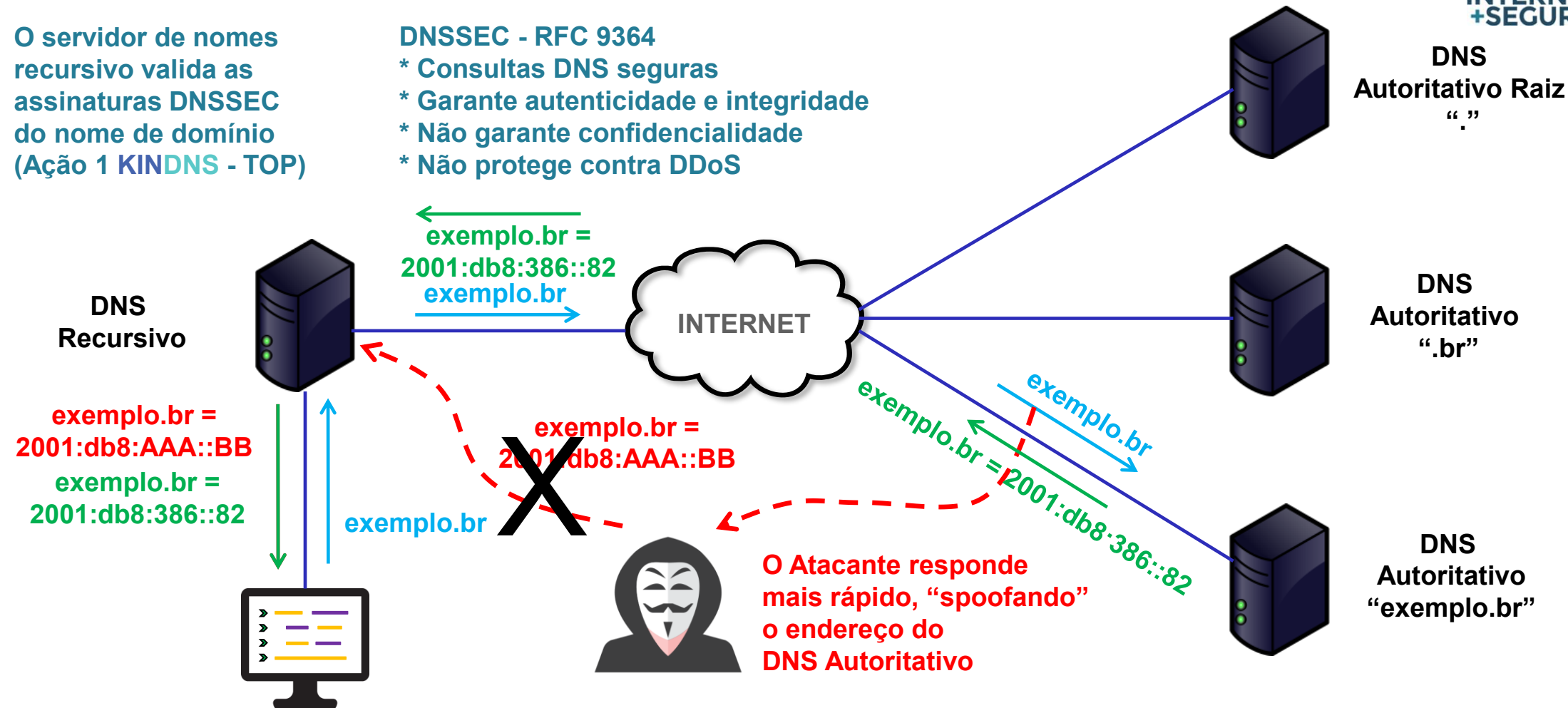
Ataque DNS - Poisoning



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:
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
- Nova versão do software do TOP

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

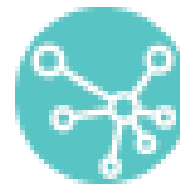
The screenshot shows the TOP website with a header containing the logo and navigation links: "Quem é TOP", "Sobre", "Referências", and "Comunicados". The main content area features a paragraph: "Os padrões técnicos modernos de Internet aumentam a confiabilidade e permitem o crescimento da rede. Você está usando esses padrões?". Below this are three test cards: 1. "Teste TOP - Site" (green) with a checklist: "Endereço IP moderno?", "Domínio assinado? Conexão segura? Opções de segurança?". It includes a text input for "Nome de domínio do seu site:" with the example "www.exemplo.com.br" and a button "Iniciar o teste". 2. "Teste TOP - E-mail" (blue) with a checklist: "Endereço IP moderno?", "Domínio assinado? Proteção contra phishing? Conexão segura?". It includes a text input for "Nome de domínio do seu e-mail:" with the example "@exemplo.com.br" and a button "Iniciar o teste". 3. "Teste TOP - IPv6 e DNSSEC da sua rede" (purple) with a checklist: "Endereços modernos acessíveis? Assinaturas de domínio validadas?". Each card has a right arrow icon and a button "Iniciar o teste". At the bottom, the URL <https://top.nic.br> is displayed.

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%

Panorama Setorial

Ano XII – N. 2 – Internet no Brasil:
robustez, confiança e mais segurança

- Segurança e Tratamento de incidentes de segurança no Brasil
- Segurança da Internet no Brasil: uma trajetória de cooperação
- Cooperação e confiança na gestão de incidentes de cibersegurança de cooperação

Edição Julho/26

<https://cetic.br/pt/panoramas/>

Panorama Setorial
da Internet

Número 2
Julho 2026
Ano 12

Internet no Brasil: robustez, confiança e mais segurança

Construindo confiança no ambiente digital: o papel do NIC.br na promoção de uma Internet mais segura no Brasil¹

A disseminação da Internet e das tecnologias digitais tem impulsionado uma transformação digital cada vez mais acelerada em diversas dimensões da sociedade, nos âmbitos da vida social e econômica, ampliando sua centralidade nas atividades cotidianas de indivíduos, organizações e governos. Se, por um lado, a crescente incorporação dessas tecnologias está associada a importantes benefícios para o desenvolvimento econômico e o bem-estar social, a ampliação de sua presença nas atividades

cotidianas também introduz novos desafios. Entre eles, destacam-se a crescente exposição a riscos digitais e possíveis incidentes de segurança associados ao uso de dispositivos conectados à Internet, o que, em alguma medida, torna seus usuários mais vulneráveis no ambiente digital.

Desde sua concepção, a Internet foi desenvolvida em um contexto caracterizado por relações de confiança entre os participantes que se interligam na rede de computadores, composta inicialmente por um número limitado de instituições acadêmicas, governamentais e de pesquisa, com vínculos ou propósitos em comum. Nesse contexto, os protocolos fundamentais da rede foram projetados com foco na interoperabilidade e na troca de informações, sem incorporar mecanismos robustos de segurança como requisitos centrais de seu desenho. Com a expansão da rede e sua crescente utilização por diferentes segmentos da sociedade, essa premissa original de confiança mostrou-se insuficiente diante dos desafios contemporâneos de segurança digital.

¹ Este artigo foi redigido por Jéssica T. Rodini Maciel, pesquisadora no Centro Nacional de Estudos para o Desenvolvimento de Sociedades de Informação (Cetic.br), Departamento de Estudos de Informação e Comunicação do Fórum de Internet (NIC.br), e parte das pesquisas realizadas de 2014 a 2016 nas pesquisas do NIC.br. Jéssica é autora em colaboração do trabalho e autora em colaboração do livro e da revista de divulgação de informações de Internet de São Paulo (ISP). O artigo contou com a revisão de gestores editoriais dessas instituições.

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

31 de julho de 2026

nic.br **cgi.br**

www.nic.br | www.cgi.br

