nic.br

Núcleo de Informação e Coordenação do Ponto BR

cgi.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 MACAPÁ

Macapá, AP | 14/03/25

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

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

PROGRAMA INTERNET +SEGURA

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

Configuração de serviços expostos na Internet

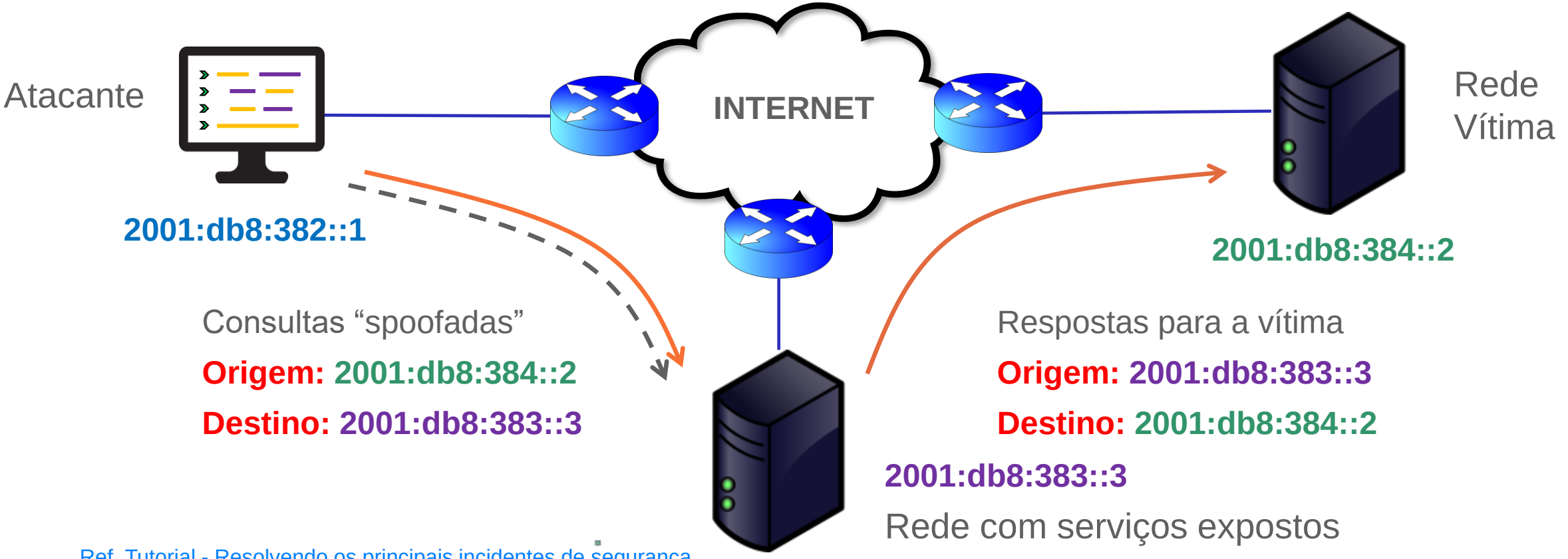
- Usados para amplificação em DDoS
- Portas UDP: DNS (53), SNMP (161), NTP (123), e várias outras!
- Notificações do CERT.br

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

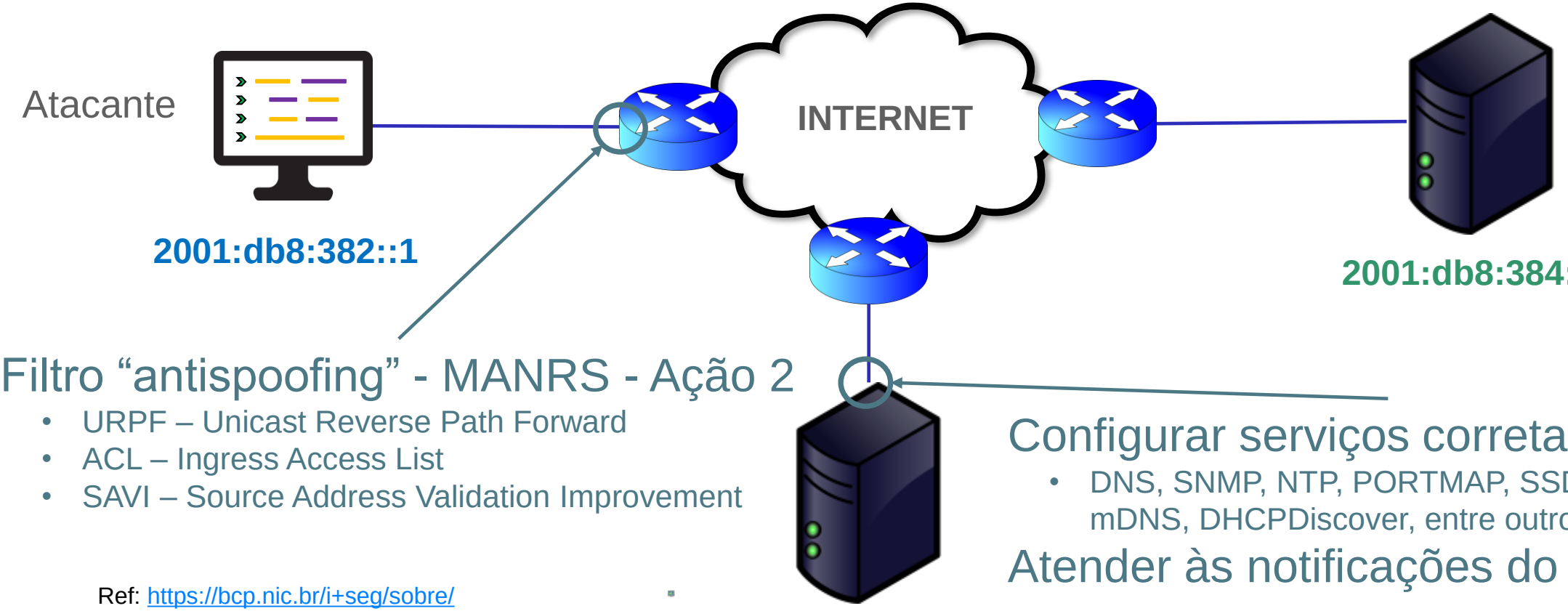


Ref. Tutorial - Resolvendo os principais incidentes de segurança

Programa por uma Internet mais Segura

Negação de Serviço Reflexivo com Amplificação

Como resolver o problema



Filtro “antispoofing” - MANRS - Ação 2

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

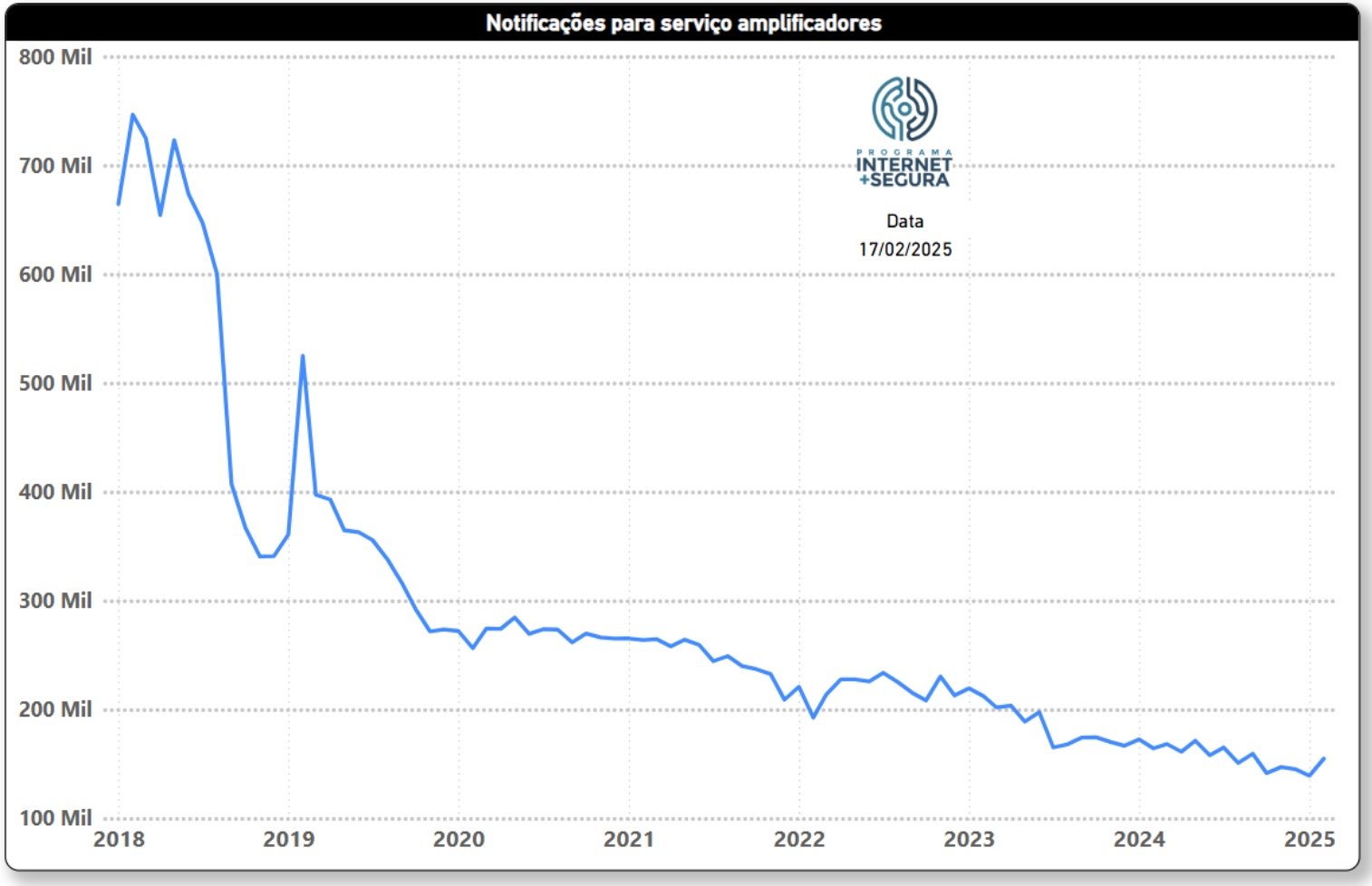
Configurar serviços corretamente

- 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

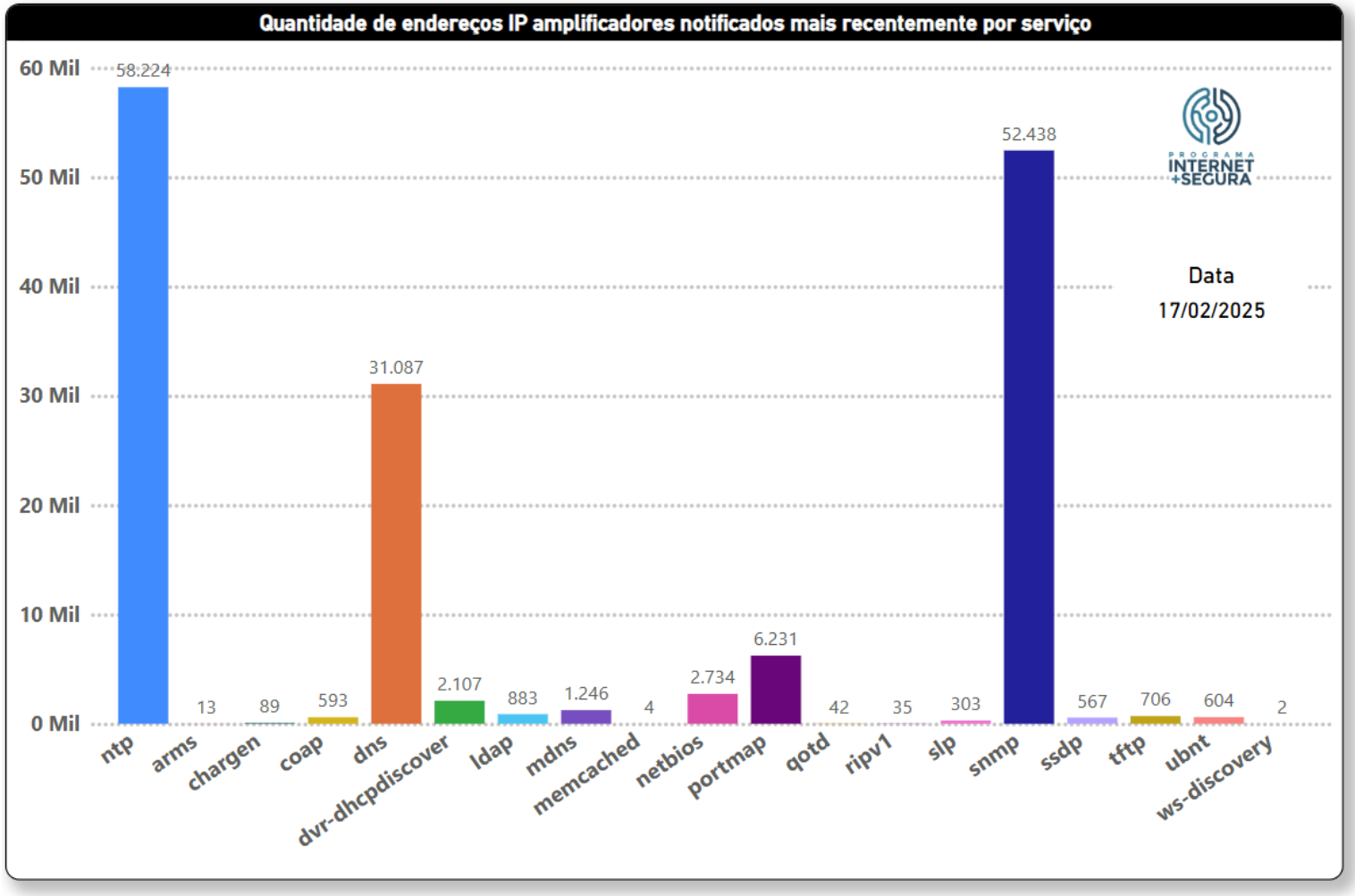


Brasil

- Início (fev/2018)
  - Endereços IP: 746.508
  - Serviços: 5
- Atual:
  - Endereços IP: 157.908
  - Serviços: 19
  - **Redução de 79%**

Fev/25

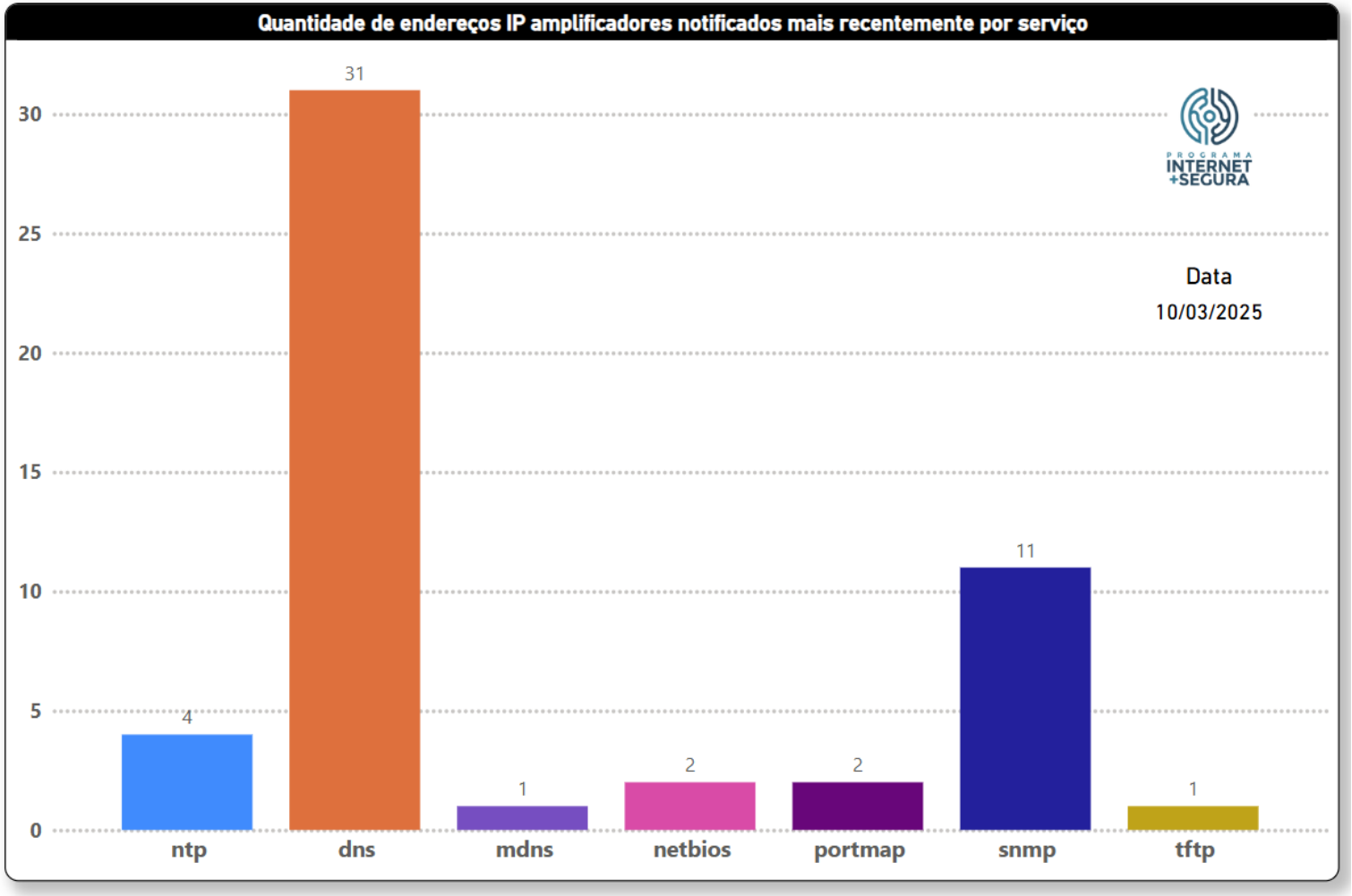
Programa por uma Internet mais Segura
Notificação de amplificadores - serviços



Brasil

- 9.038 AS
- 5.179 AS notificados
- 157.908 endereços IP mal configurados
  - NTP 58.224
  - SNMP 52.438
  - DNS 31.087

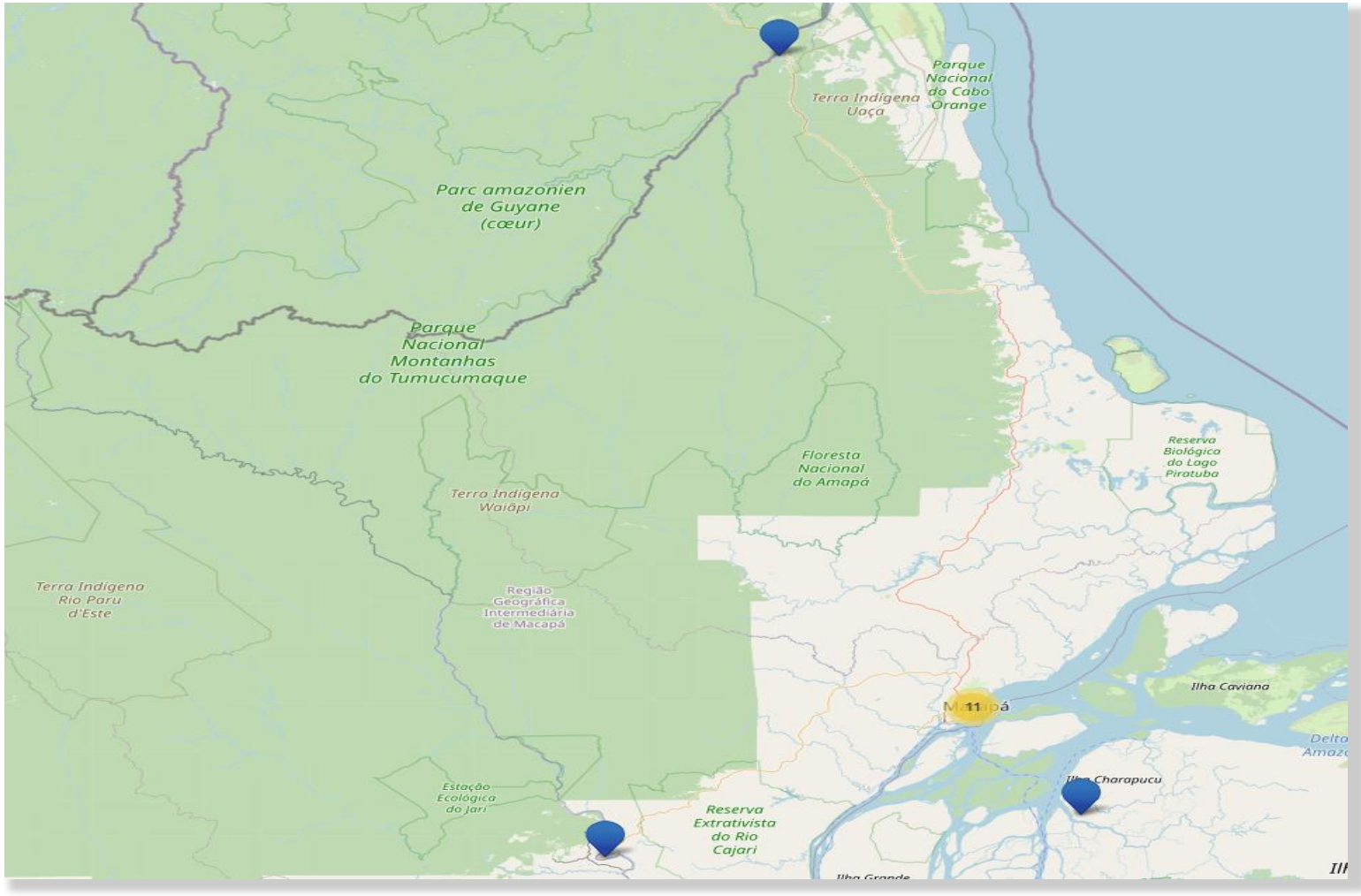
Programa por uma Internet mais Segura
Notificação de amplificadores - serviços



Amapá

- 14 AS
- 5 AS notificados
- 52 endereços IP mal configurados
  - DNS 31
  - SNMP 11
  - NTP 4

Programa por uma Internet mais Segura
Notificação de amplificadores - serviços



Amapá

- Macapá (11)
- Santana (1)
- Oiapoque (1)
- Laranjal do Jari (1)

MANRS

PROGRAMA INTERNET +SEGURA

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

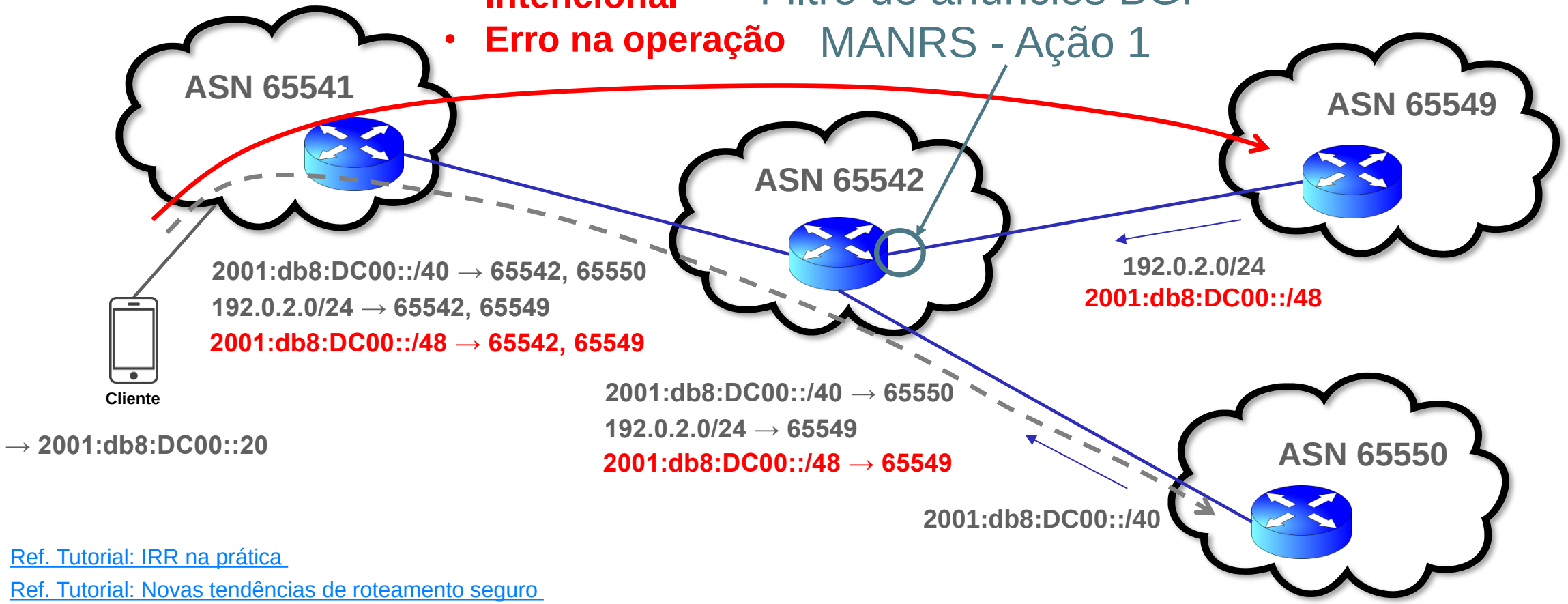
Sequestro de prefixos (Hijacking)

Anúncio de prefixos não autorizados:

- **Intencional**
- **Erro na operação**

Filtro de anúncios BGP

MANRS - Ação 1



Ref. Tutorial: IRR na prática

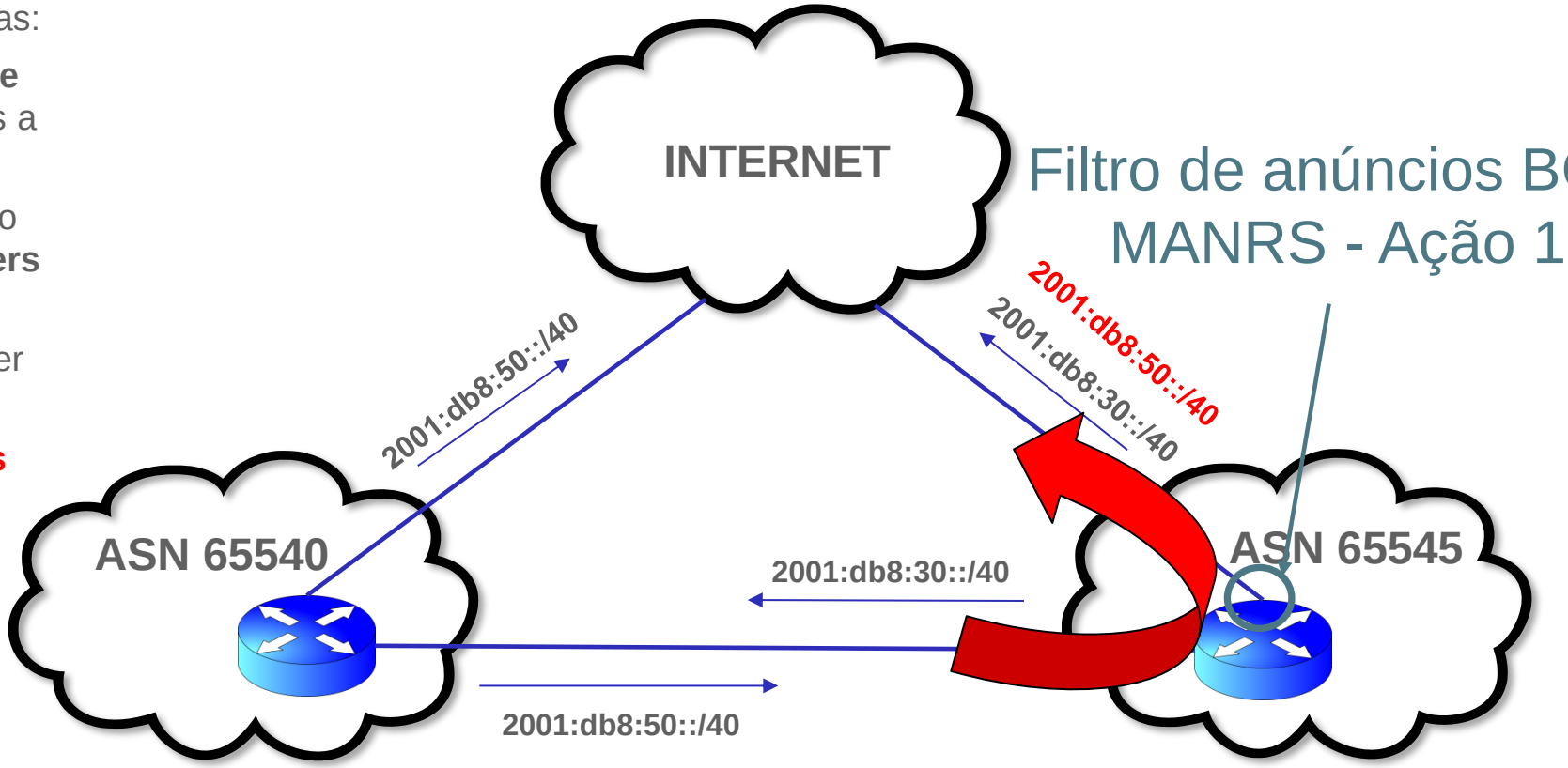
Ref. Tutorial: Novas tendências de roteamento seguro

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

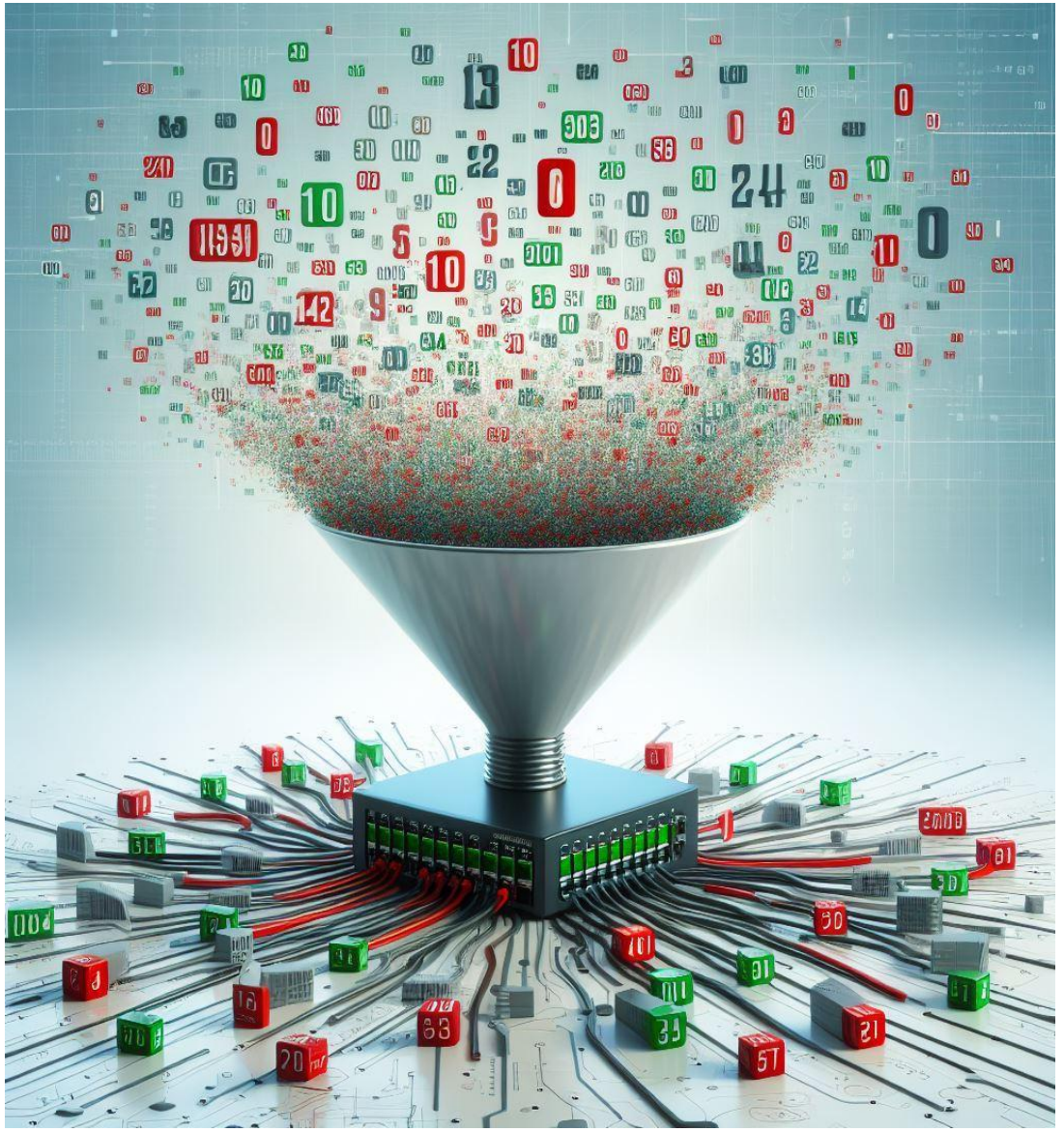
Ref. Tutorial: novas tendências de roteamento seguro

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

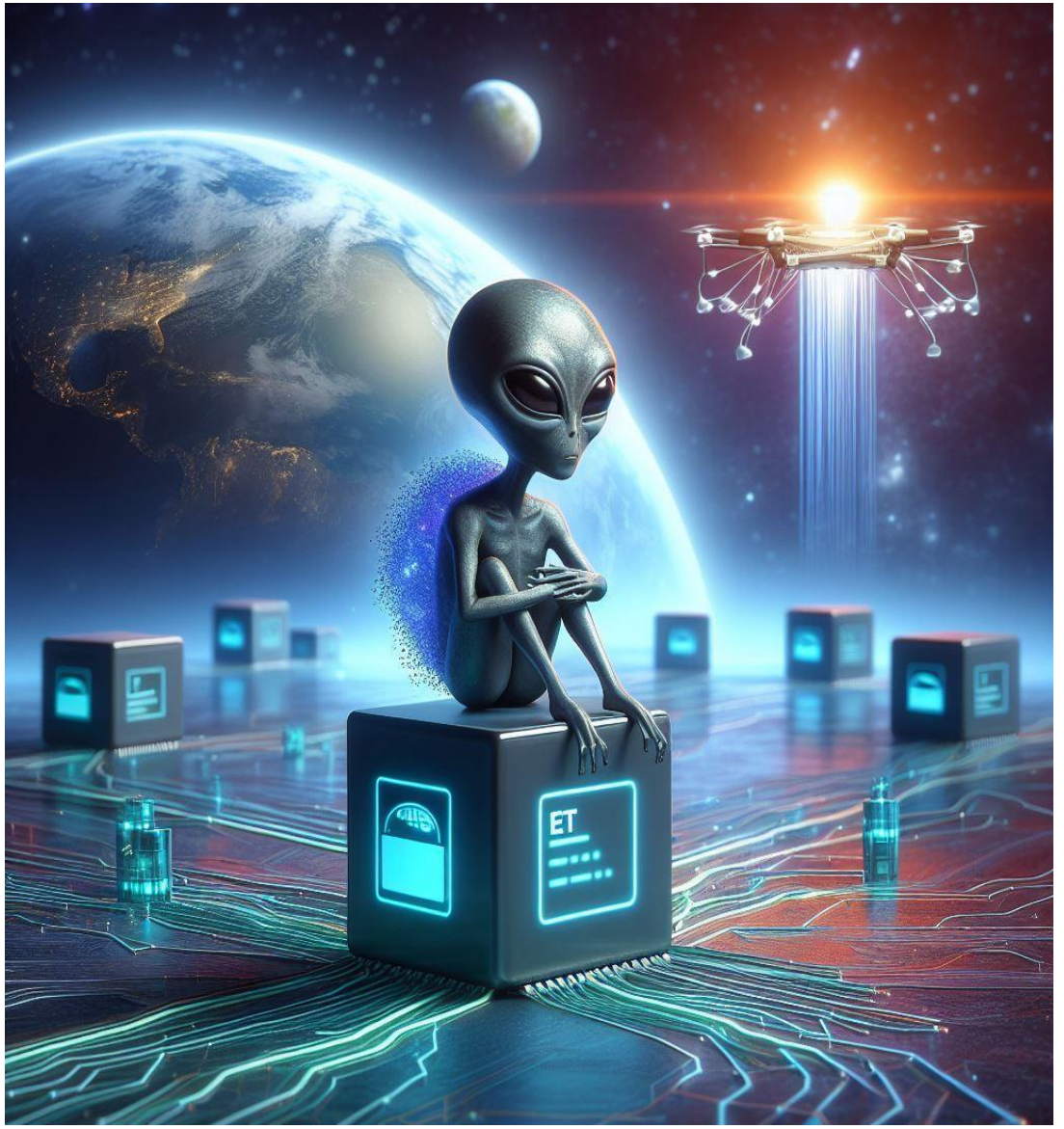


MANRS

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)!



MANRS

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

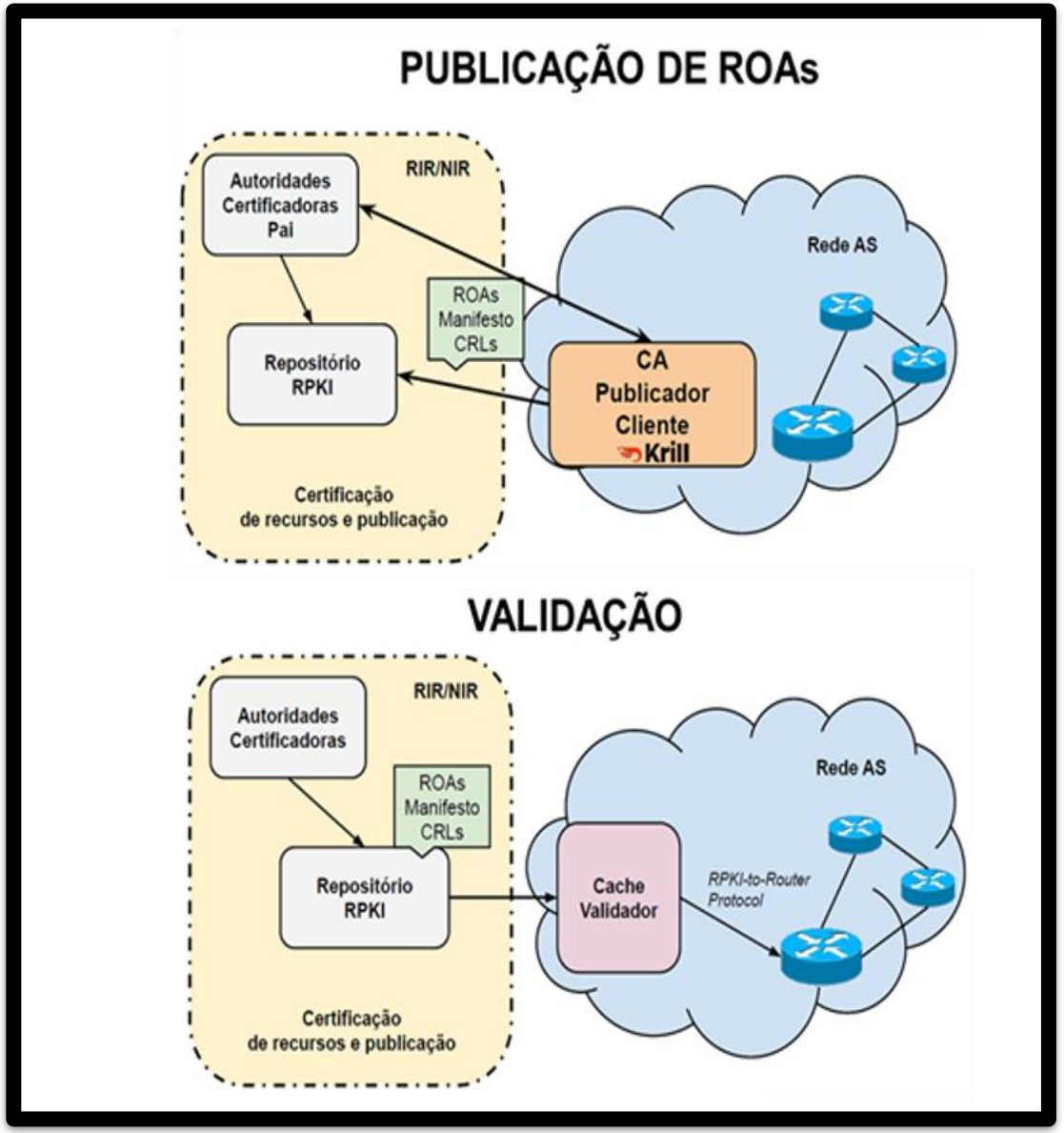
MANRS - Ação 4 - Cadastro da Política de Roteamento

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

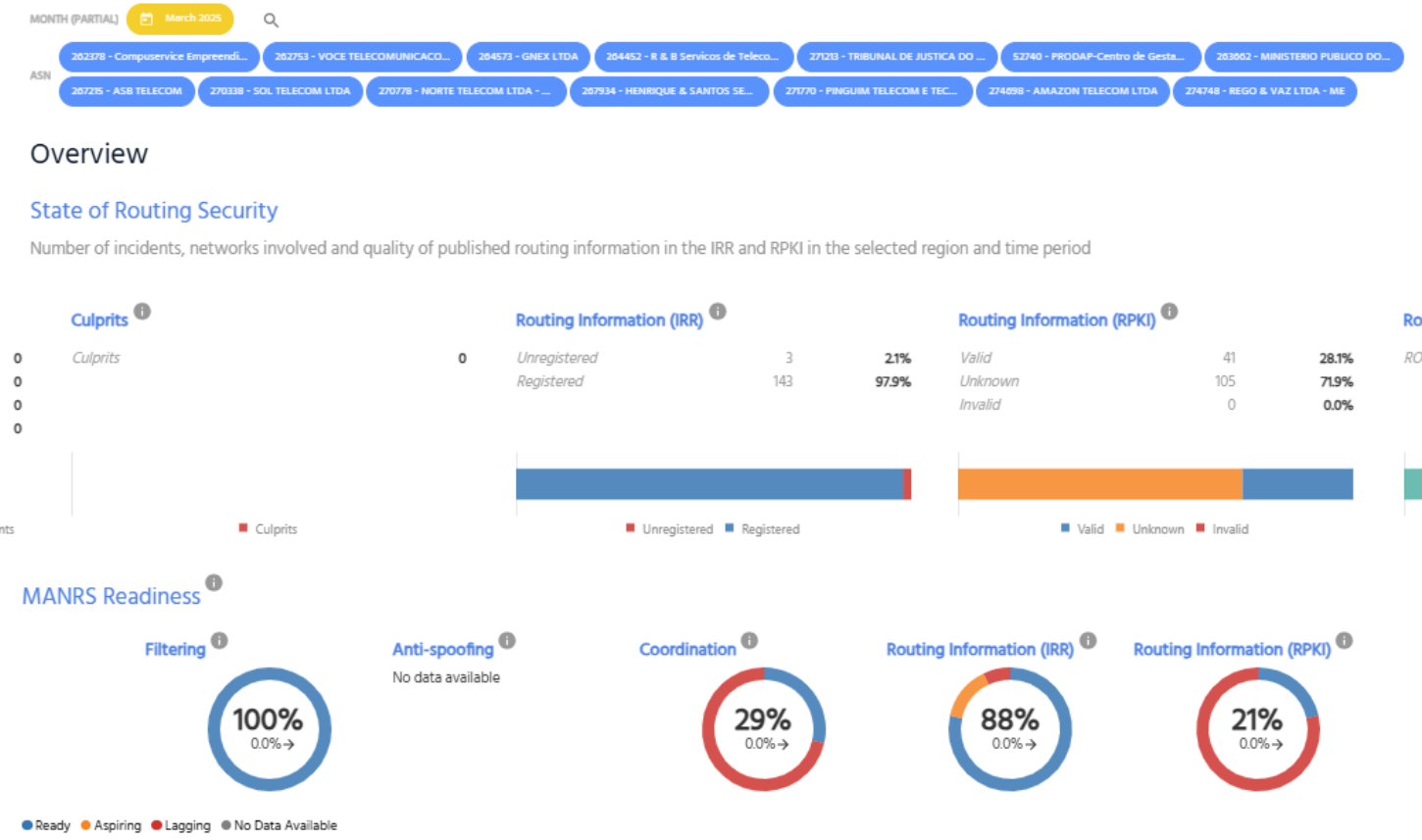
- **RPKI** - Resource Public Key Infrastructure

MANRS

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



Programa por uma Internet mais Segura
MANRS Observatory - 14 AS – AP



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%	não tst	0%	100%	0%
ASN 2	---	BR	Americas	Latin America and the Caribbean	LACNIC	100%	não tst	100%	100%	100%
ASN 3	---	BR	Americas	Latin America and the Caribbean	LACNIC	100%	não tst	100%	100%	0%
ASN 4	---	BR	Americas	Latin America and the Caribbean	LACNIC	100%	não tst	0%	100%	0%
ASN 5	---	BR	Americas	Latin America and the Caribbean	LACNIC	100%	não tst	0%	100%	0%
ASN 6	---	BR	Americas	Latin America and the Caribbean	LACNIC	100%	não tst	100%	100%	100%
ASN 7	---	BR	Americas	Latin America and the Caribbean	LACNIC	100%	não tst	0%	100%	0%
ASN 8	---	BR	Americas	Latin America and the Caribbean	LACNIC	100%	não tst	100%	100%	0%
ASN 9	---	BR	Americas	Latin America and the Caribbean	LACNIC	100%	não tst	0%	100%	0%
ASN 10	---	BR	Americas	Latin America and the Caribbean	LACNIC	100%	não tst	0%	80%	0%
ASN 11	---	BR	Americas	Latin America and the Caribbean	LACNIC	100%	não tst	0%	100%	0%
ASN 12	---	BR	Americas	Latin America and the Caribbean	LACNIC	100%	não tst	0%	100%	100%
ASN 13	---	BR	Americas	Latin America and the Caribbean	LACNIC	100%	não tst	0% *	50%	0%
ASN 14	---	BR	Americas	Latin America and the Caribbean	LACNIC	100%	não tst	0%	0%	0%

* - ASN com status pendente junto ao registro.br

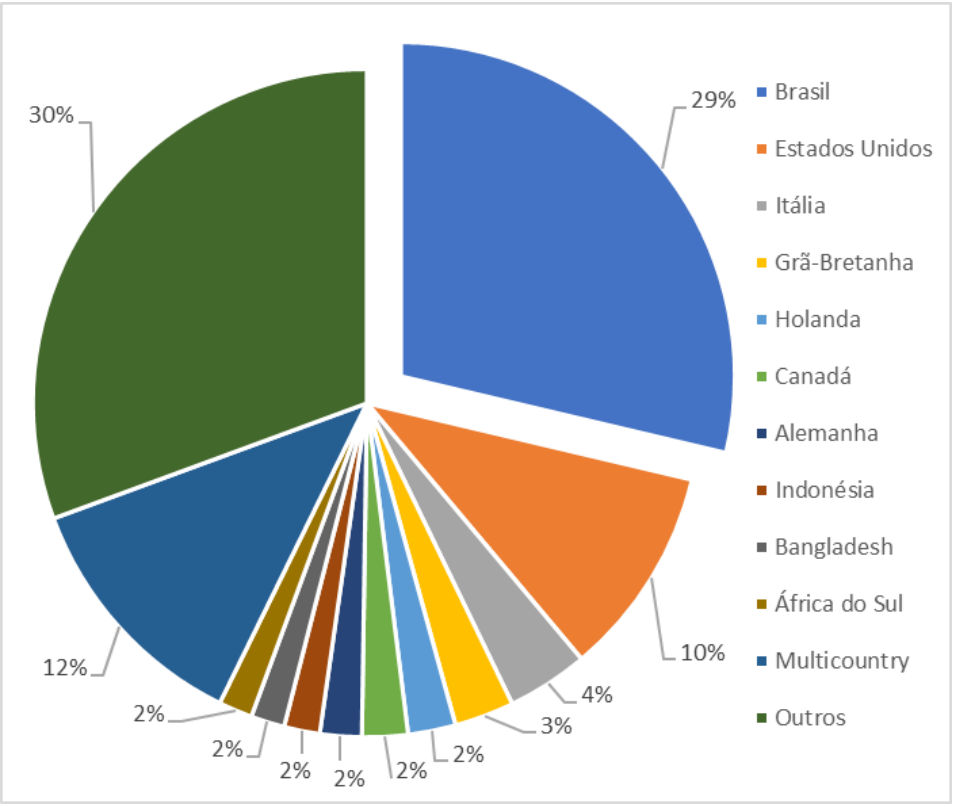
Programa por uma Internet mais Segura

Participantes por país

- Total: 1.039
- Participantes no Brasil → 298 (fev/25)

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

MANRS



Fonte: https://www.manrs.org/netops/participants/ Acesso fev/25

PROGRAMA INTERNET +SEGURA

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

https://kindns.org/

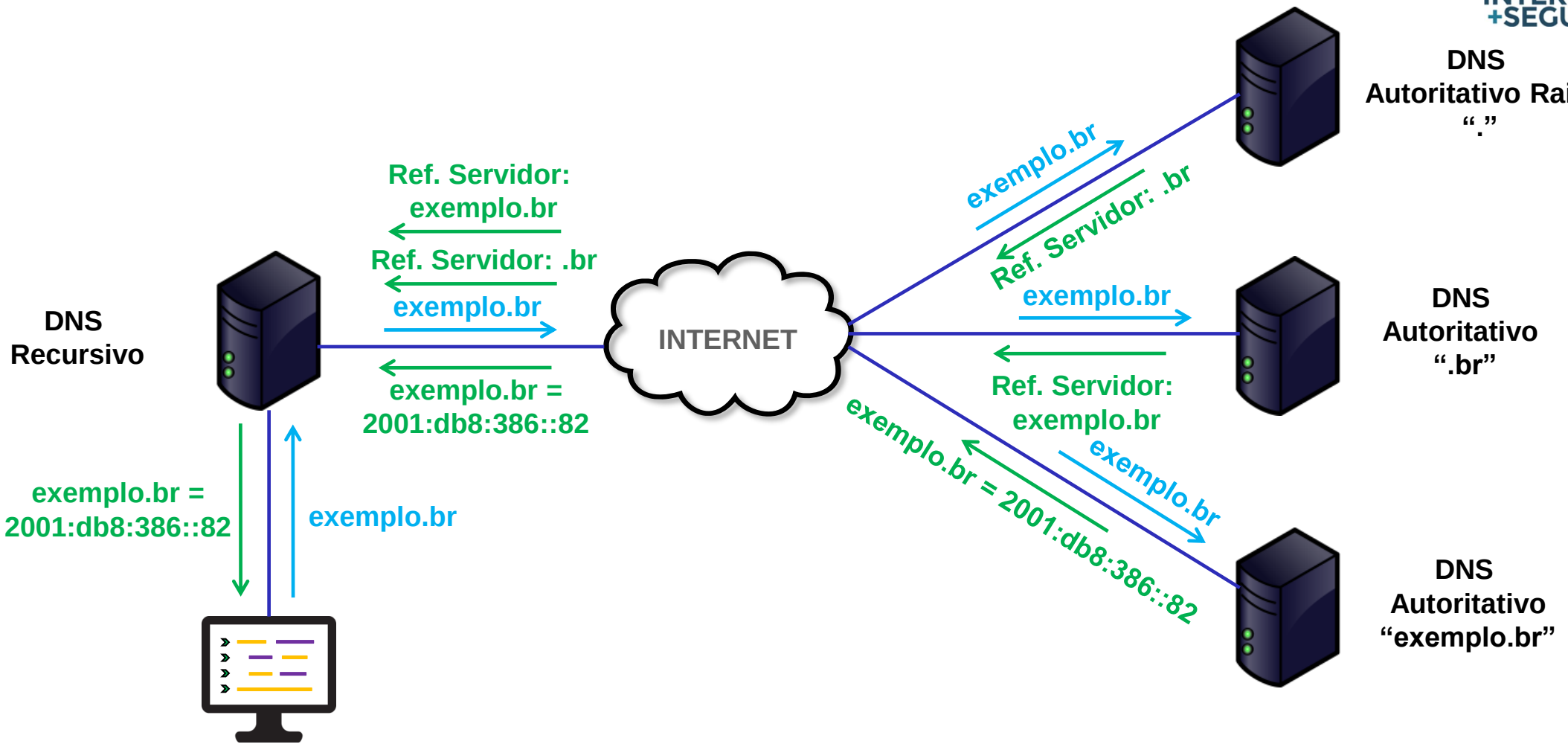
An ICANN Initiative

ICANN

nic.br cgi.br

Programa por uma Internet mais Segura

Processo de Recursão DNS



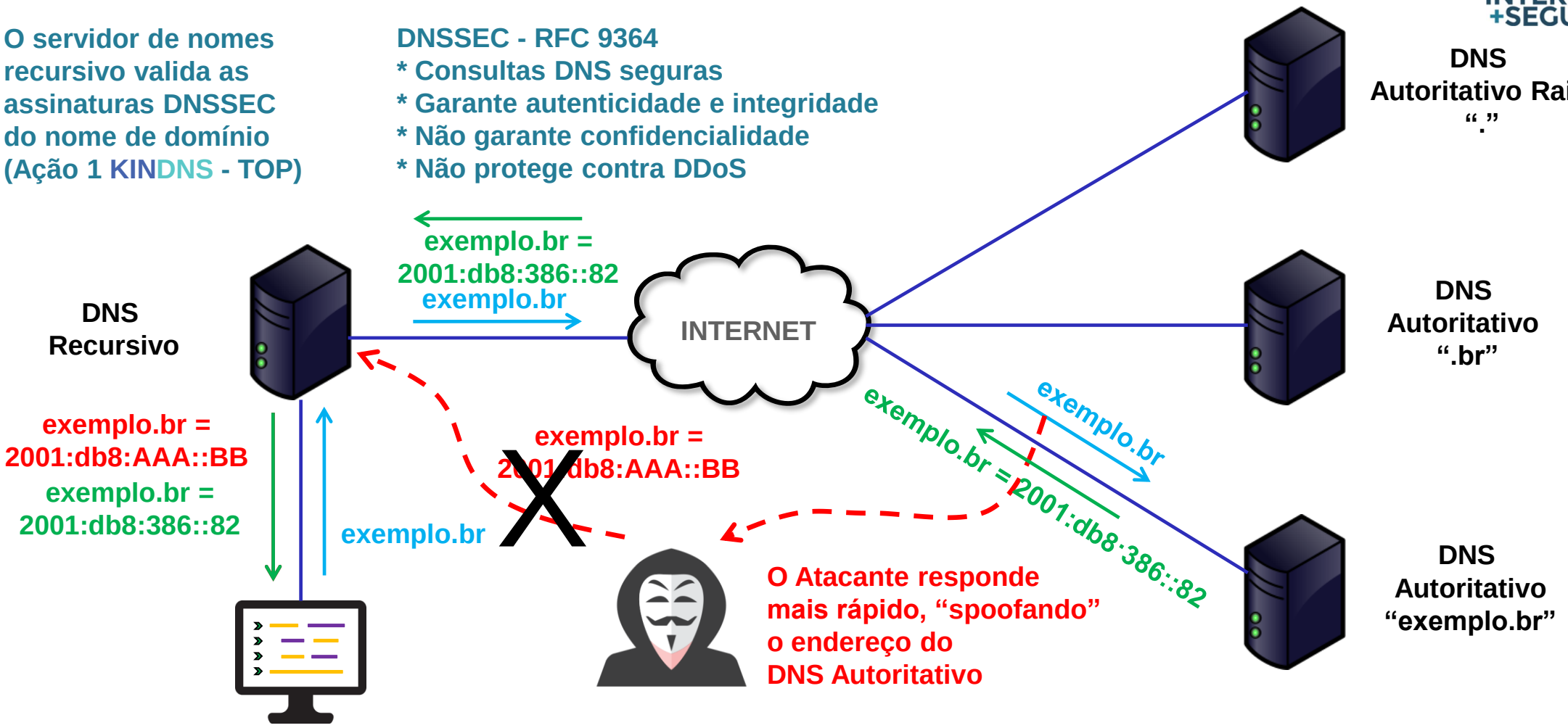
Fonte: [#SemanaCap 7] Curso - Configurando o seu DNS de forma simples e segura – Ataque DNS Poisoning

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

Programa por uma Internet mais Segura

PROGRAMA INTERNET +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/

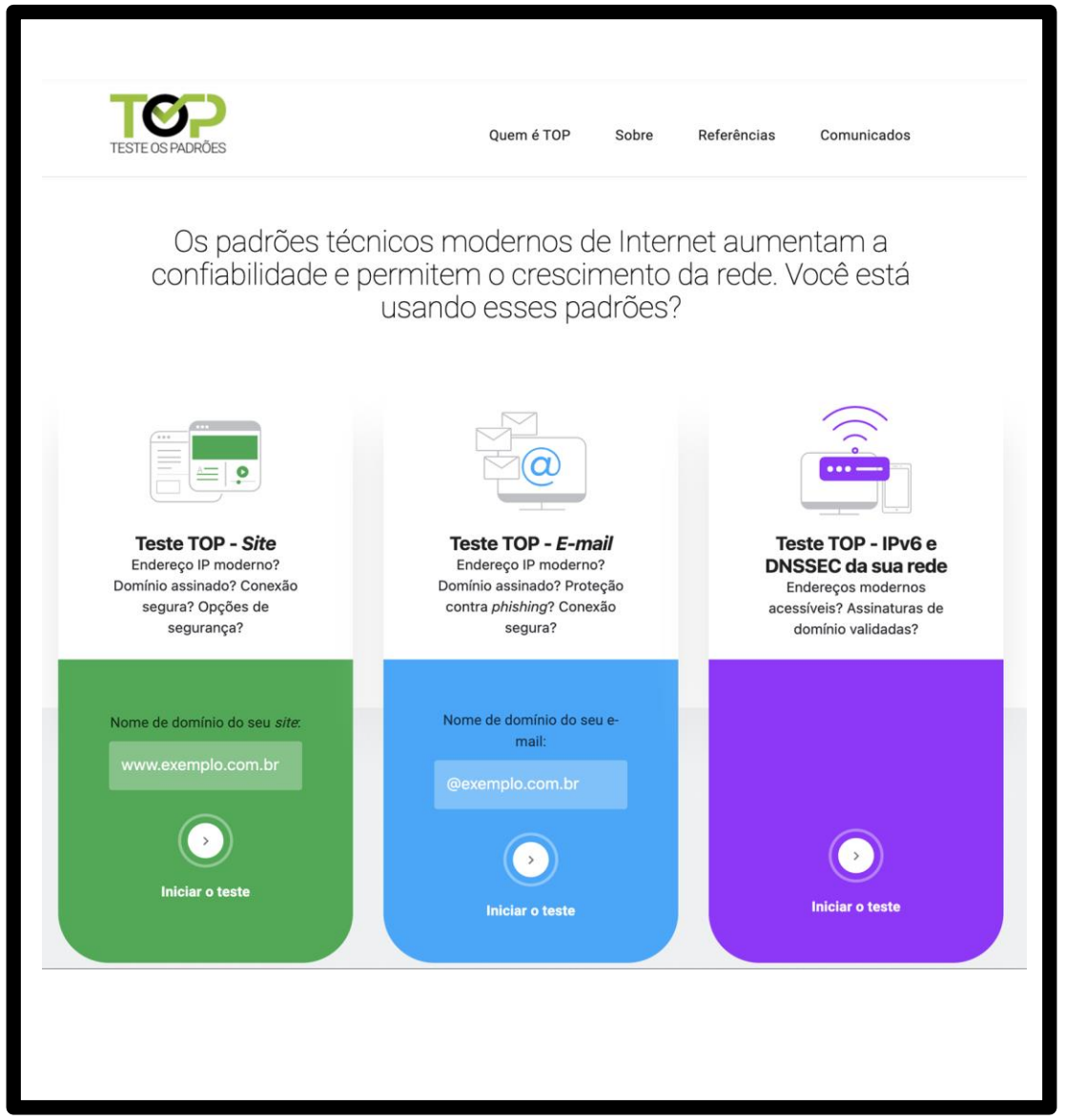
KINDNS

PROGRAMA INTERNET +SEGURA

TOP

TESTE OS PADRÕES

https://top.nic.br



Programa por uma Internet mais Segura

PROGRAMA INTERNET +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!

Acesso: https://top.nic.br

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

* Novos testes

Acesso: 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

Programa por uma Internet mais Segura

APOIO

conexis brasil.digital

A CONECTIVIDADE AO SEU ALCANCE

abranet
Associação Brasileira de Internet

AbraCloud

REDETELESUL

abrint

TelComp
Competição para o Futuro Digital

abramulti
Associação brasileira dos operadores de telecomunicações e provedores de internet.

APRONET
Associação Catarinense dos Provedores de Internet

RNP
REDE NACIONAL DE ENSINO E PESQUISA

InternetSul

Obrigado

Gilberto Zorello

gzorello@nic.br

13 de março de 2025

www.nic.br | www.cgi.br