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

IX Fórum Regional - Edição Centro Oeste

Campo Grande, MS | 14/11/25

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

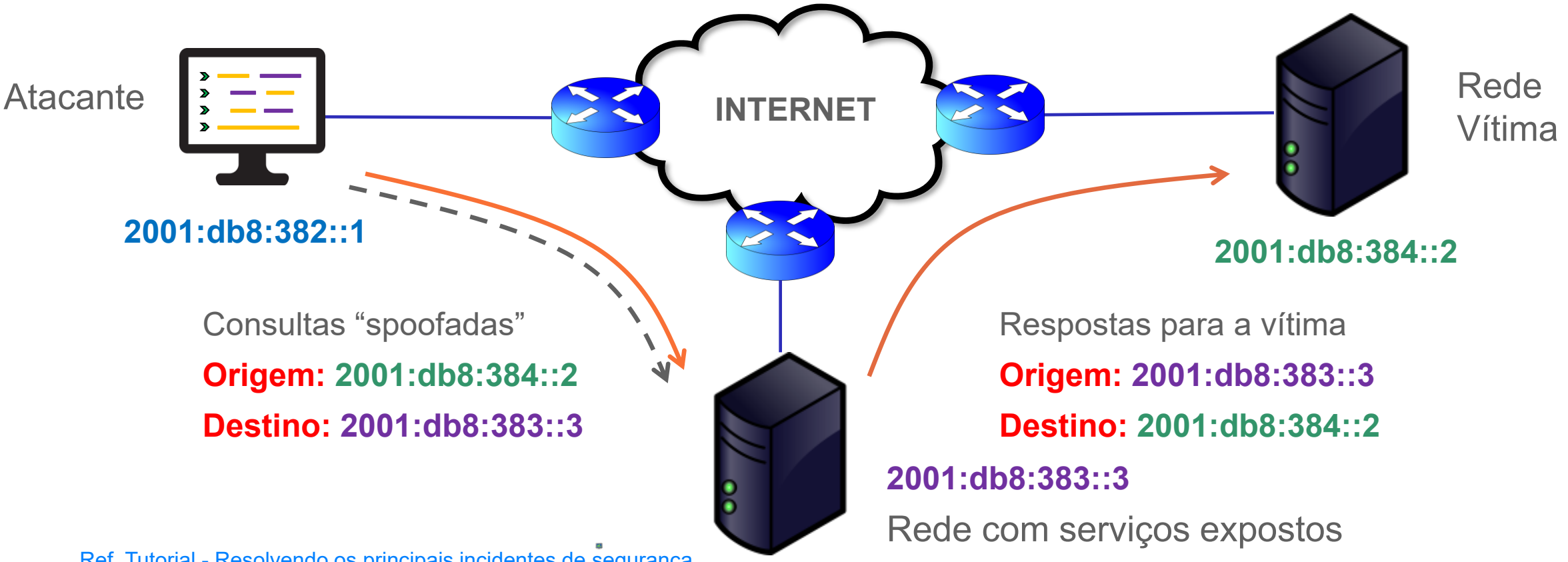
- Usados para amplificação em DDoS
- Portas UDP: DNS (53), SNMP (161), NTP (123), e várias outras!
- Notificações do CERT.br

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

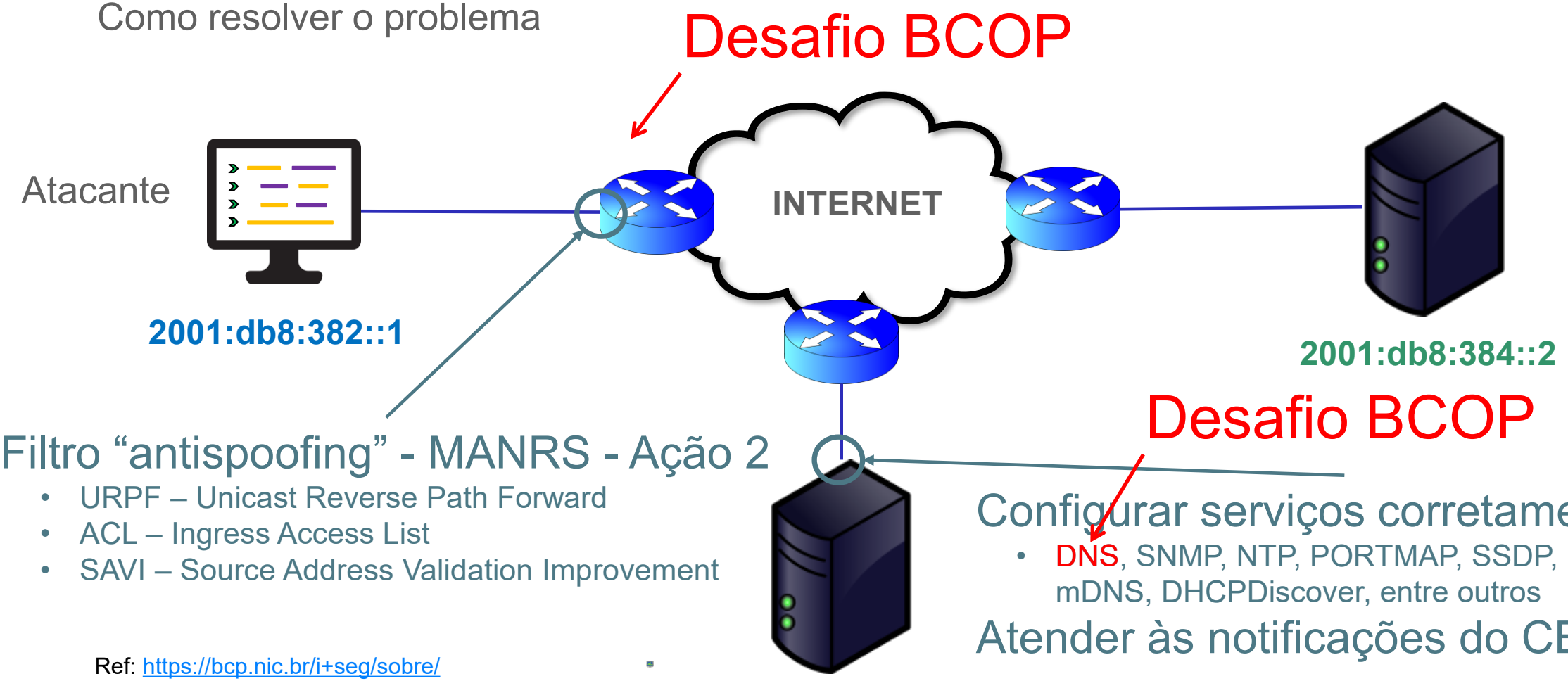


Ref. Tutorial - Resolvendo os principais incidentes de segurança

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

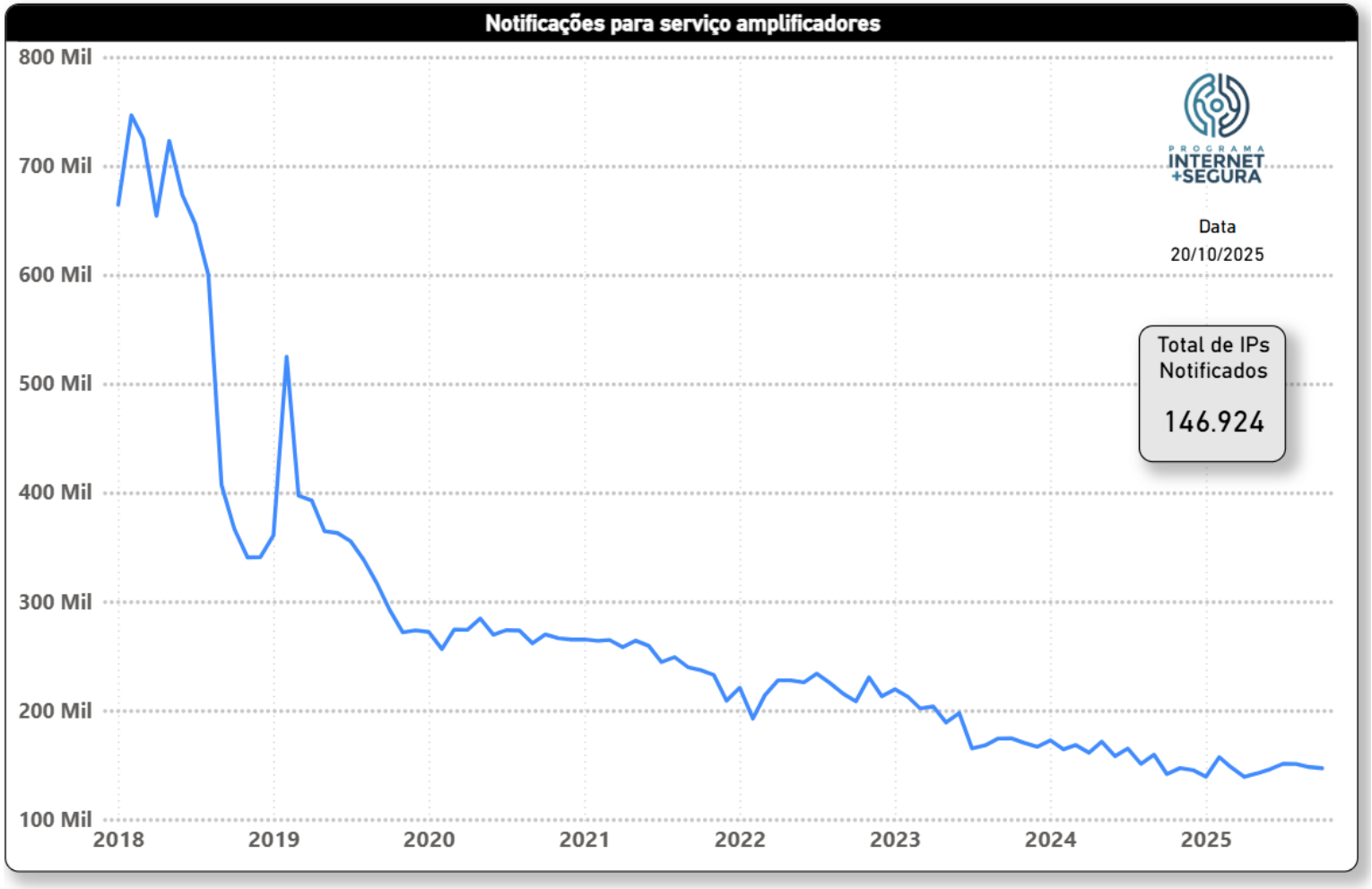
Configurar serviços corretamente

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

Atender às notificações do CERT.br

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

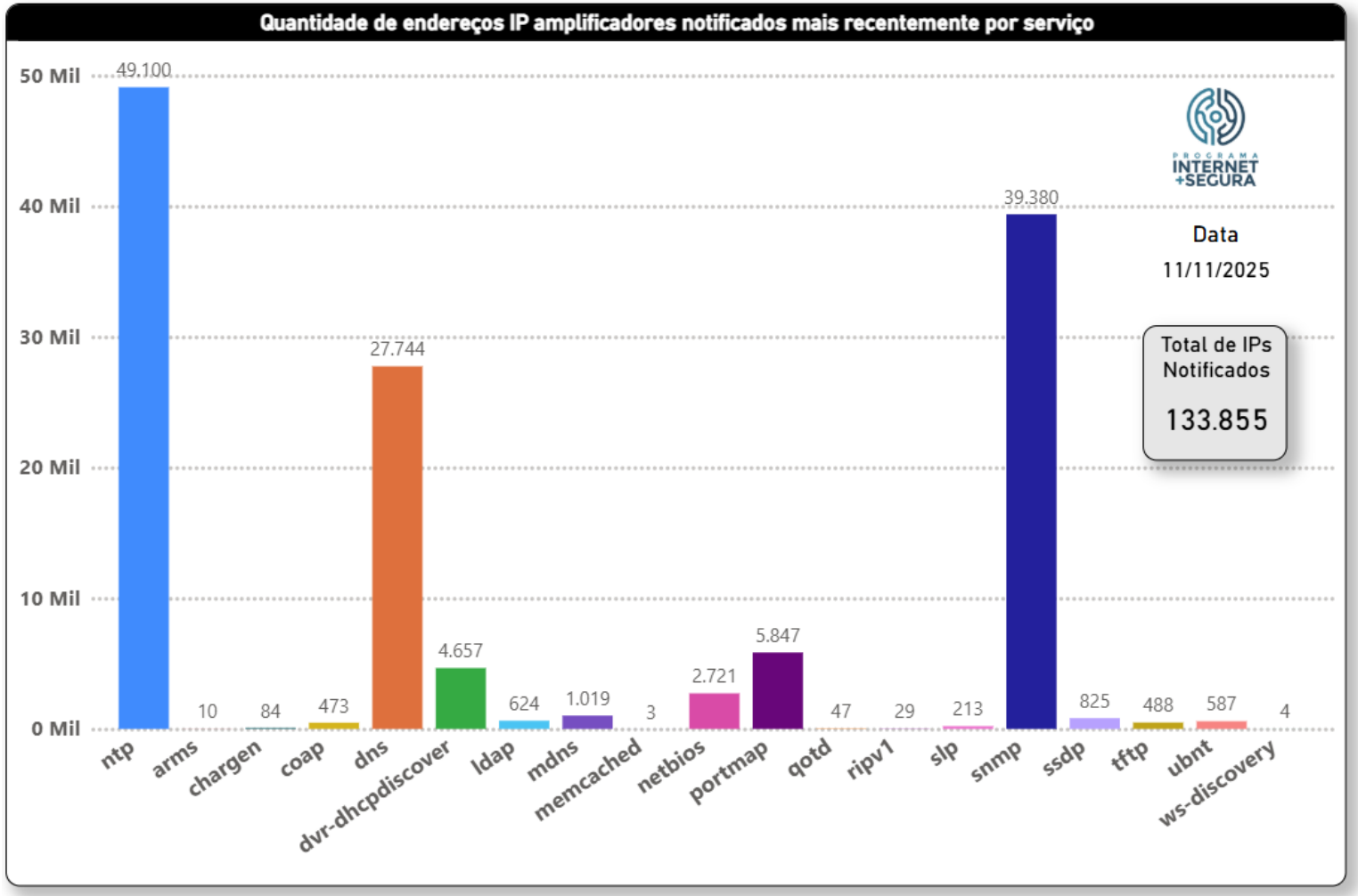
Programa por uma Internet mais Segura
Notificação de amplificadores - evolução



Brasil

- Início (fev/2018)
  - Endereços IP: 746.508
  - Serviços: 5
- Atual:
  - Endereços IP: 146.924
  - Serviços: 19
  - **Redução de 80%**
  - Ref. Out/25

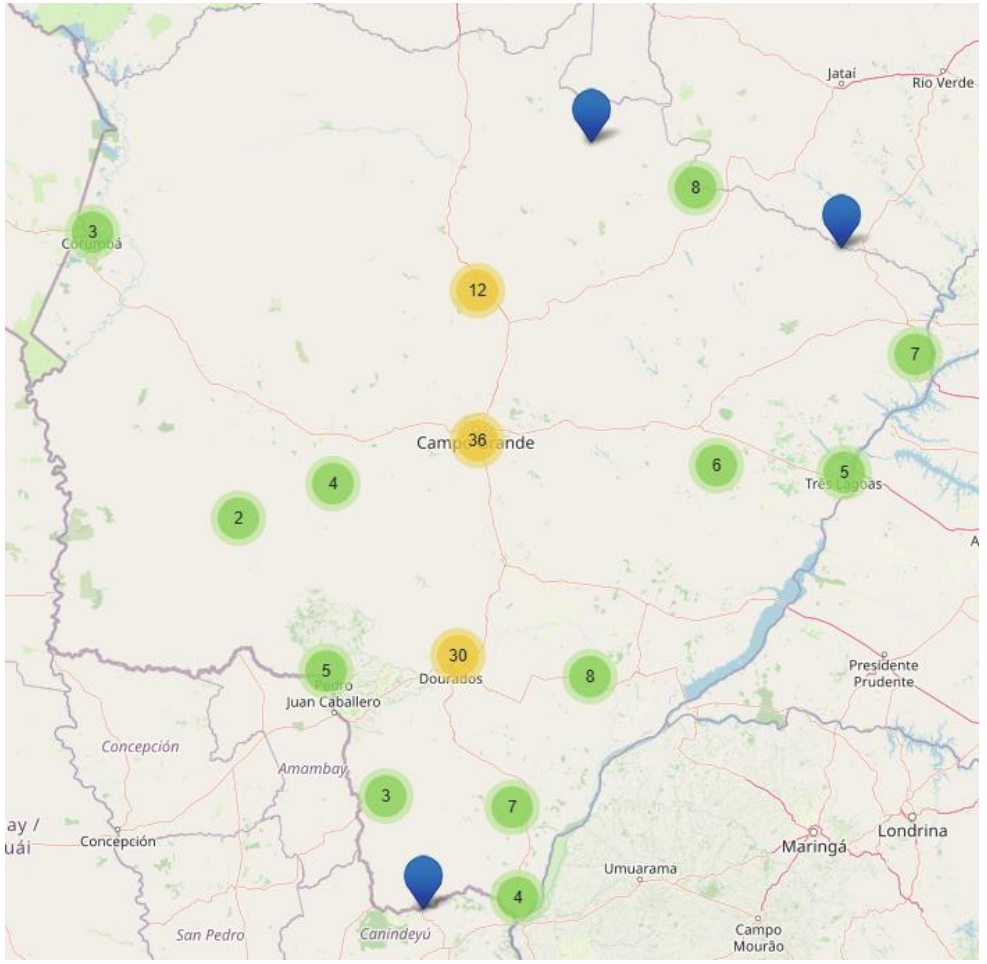
Programa por uma Internet mais Segura
Notificação de amplificadores - serviços



Brasil

- 9.078 AS
- 5.125 AS notificados
- 133.855 endereços IP mal configurados
  - NTP 49.100
  - SNMP 39.380
  - DNS 27.744
  - Ref: 11/11/25

Programa por uma Internet mais Segura
Notificação de amplificadores - serviços

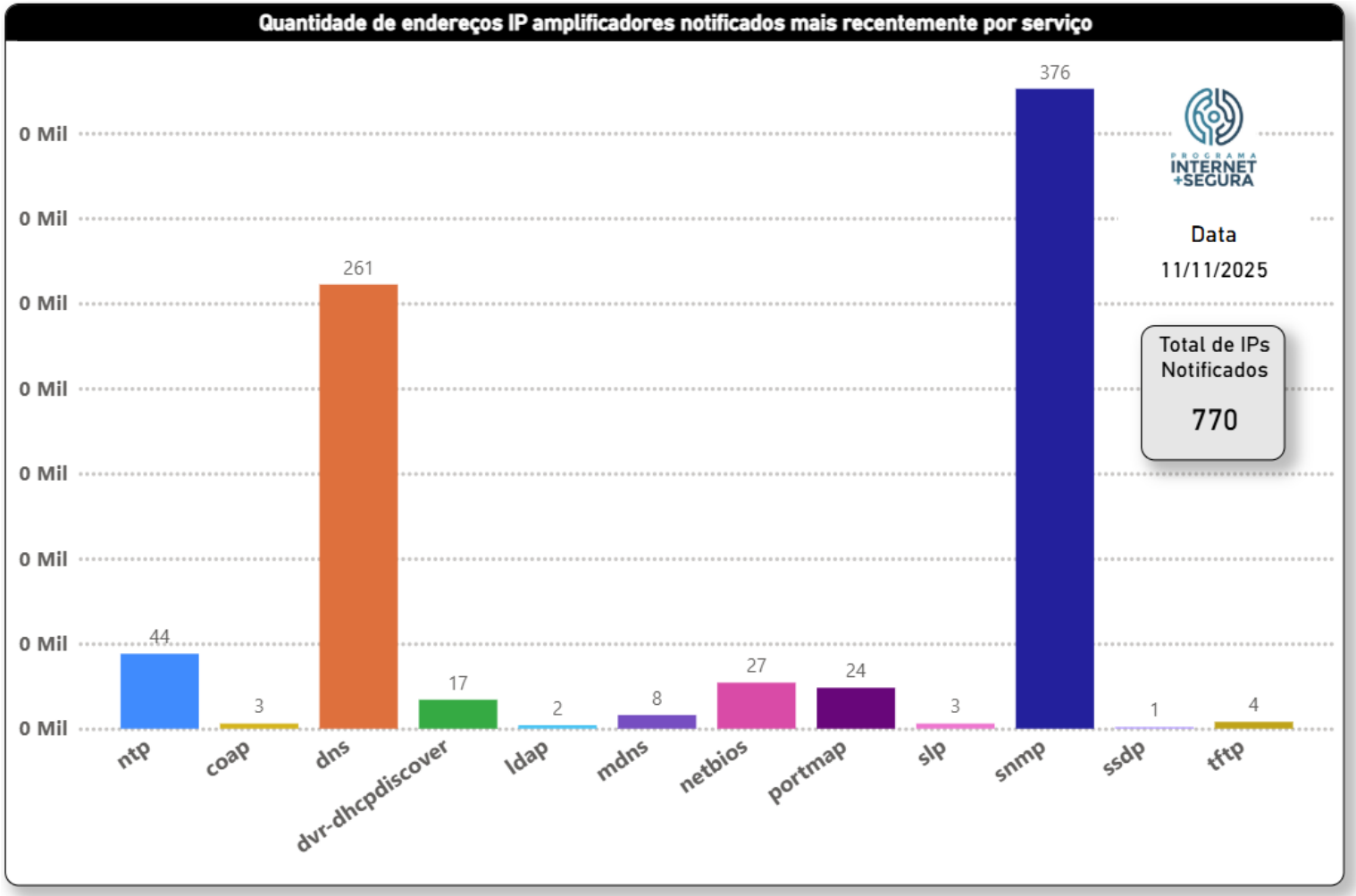


Mato Grosso do Sul (143 AS)

- Campo Grande (31)
- Dourados (15)
- Ivinhema (6)
- Três Lagoas (6)
- Água Clara (4)
- Aparecida do Taboado (4)
- Chapadão do Sul (4)
- Corumbá (4)
- Costa Rica (4)
- Fátima do Sul (4)
- Itaporã (4)
- Naviraí (4)
- Ponta Porã (4)
- Sidrolândia (4)
- Maracaju (3)
- Mundo Novo (3)
- Paranaíba (3)

Ref. https://mapadeas.ceptro.br

Programa por uma Internet mais Segura
Notificação de amplificadores - serviços



Mato Grosso do Sul

- 143 AS
- 41 AS conectados ao IX
- 98 AS notificados
- 1 AS com mais de 57 IP notificados
- 770 endereços IP mal configurados
  - DNS 261
  - SNMP 376
  - Ref: 11/11/25

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

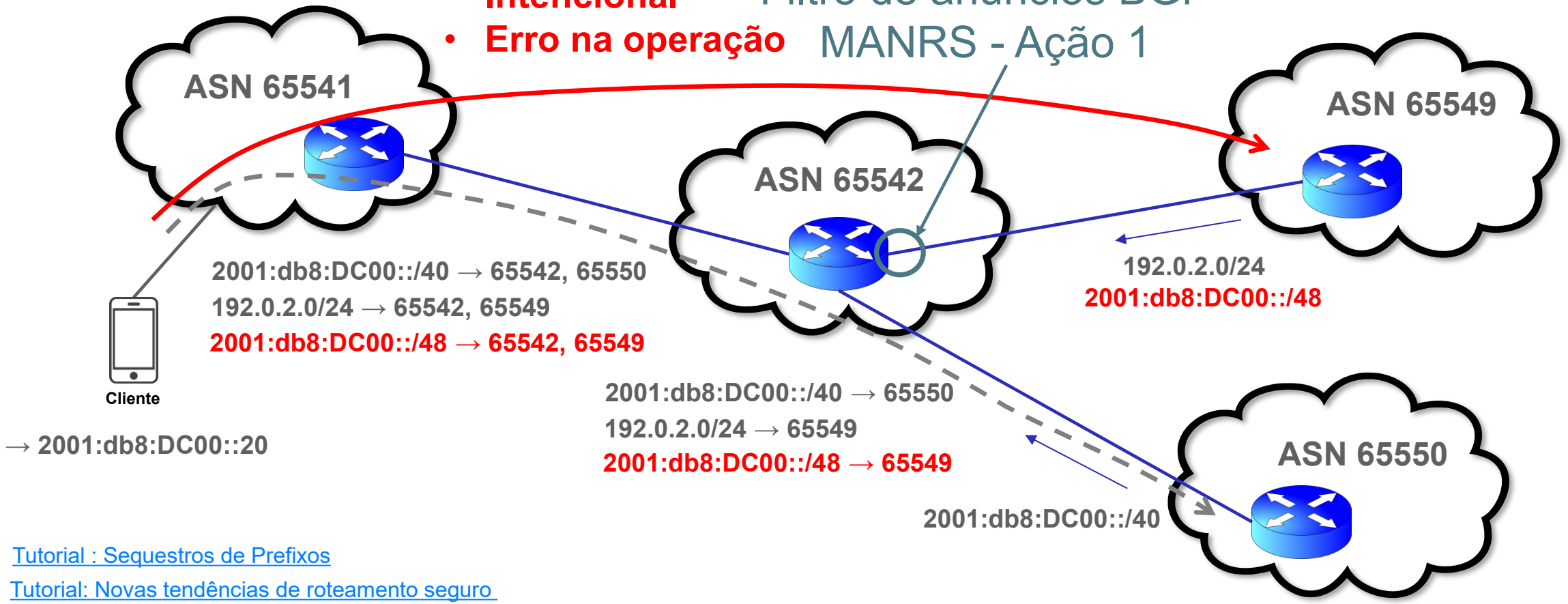
Sequestro de prefixos (Hijacking)

Anúncio de prefixos não autorizados:

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

Filtro de anúncios BGP

MANRS - Ação 1



Tutorial : Sequestros de Prefixos

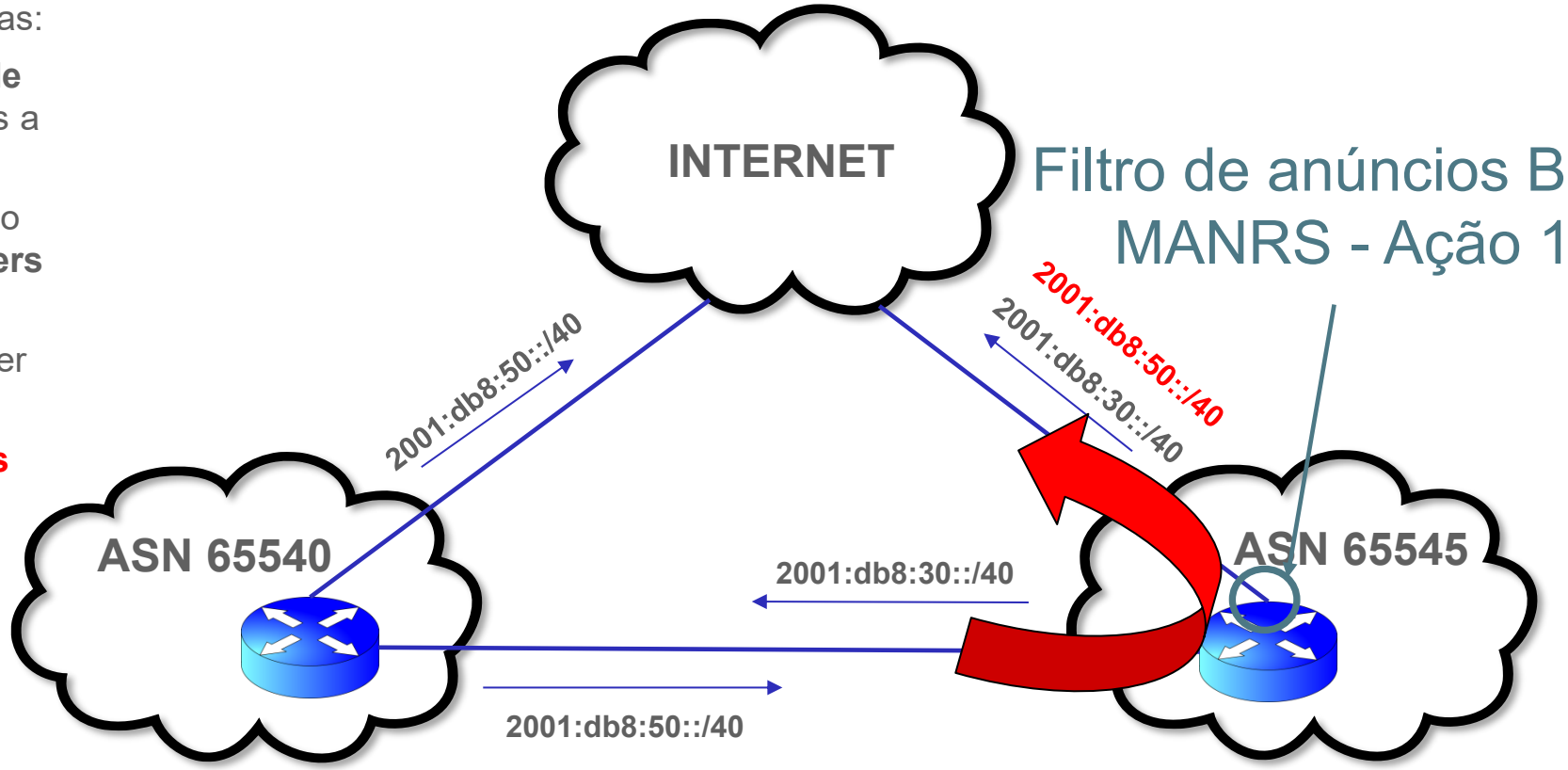
Tutorial: Novas tendências de roteamento seguro

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

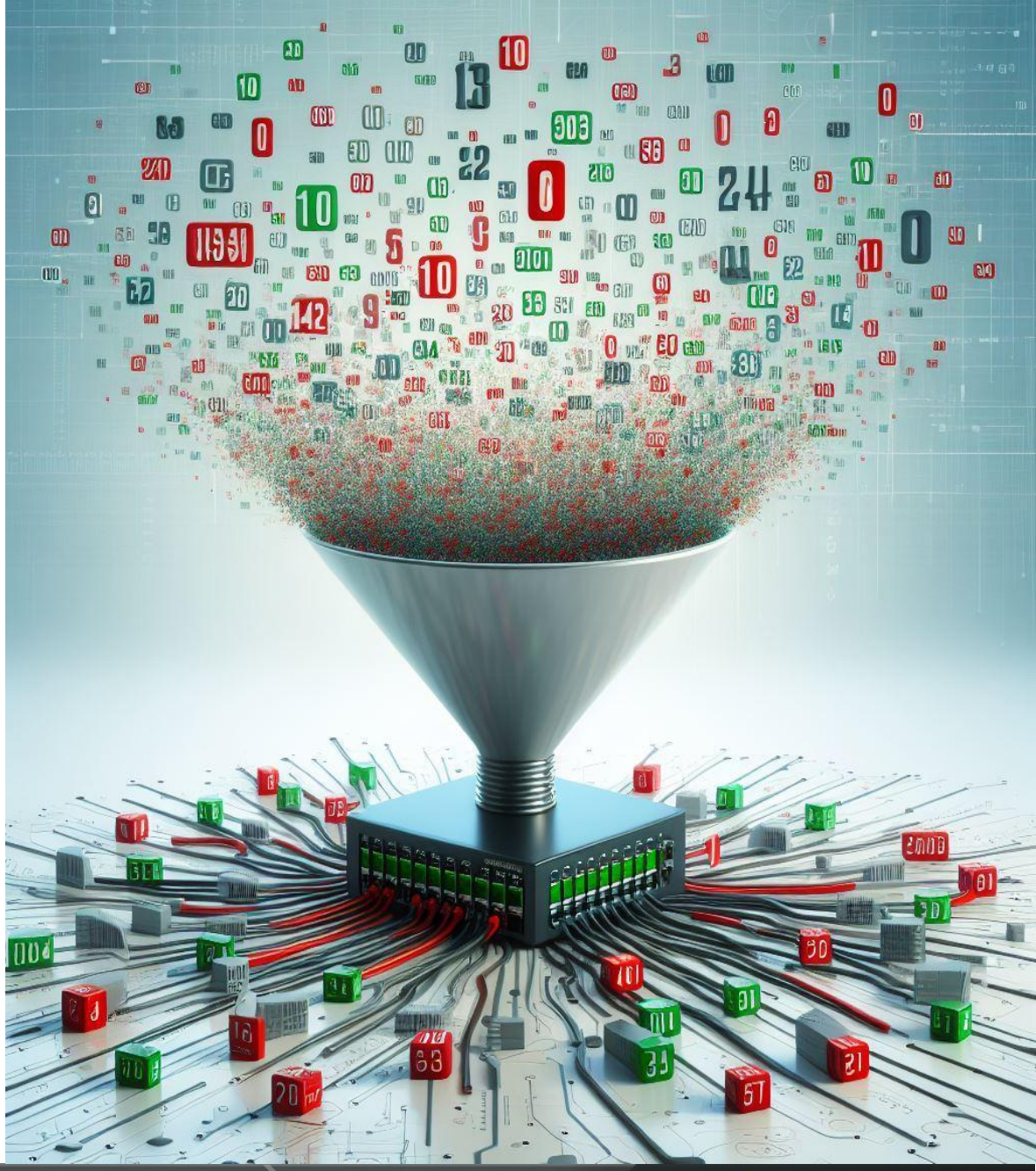
Programa por uma Internet mais Segura

PROGRAMA INTERNET +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

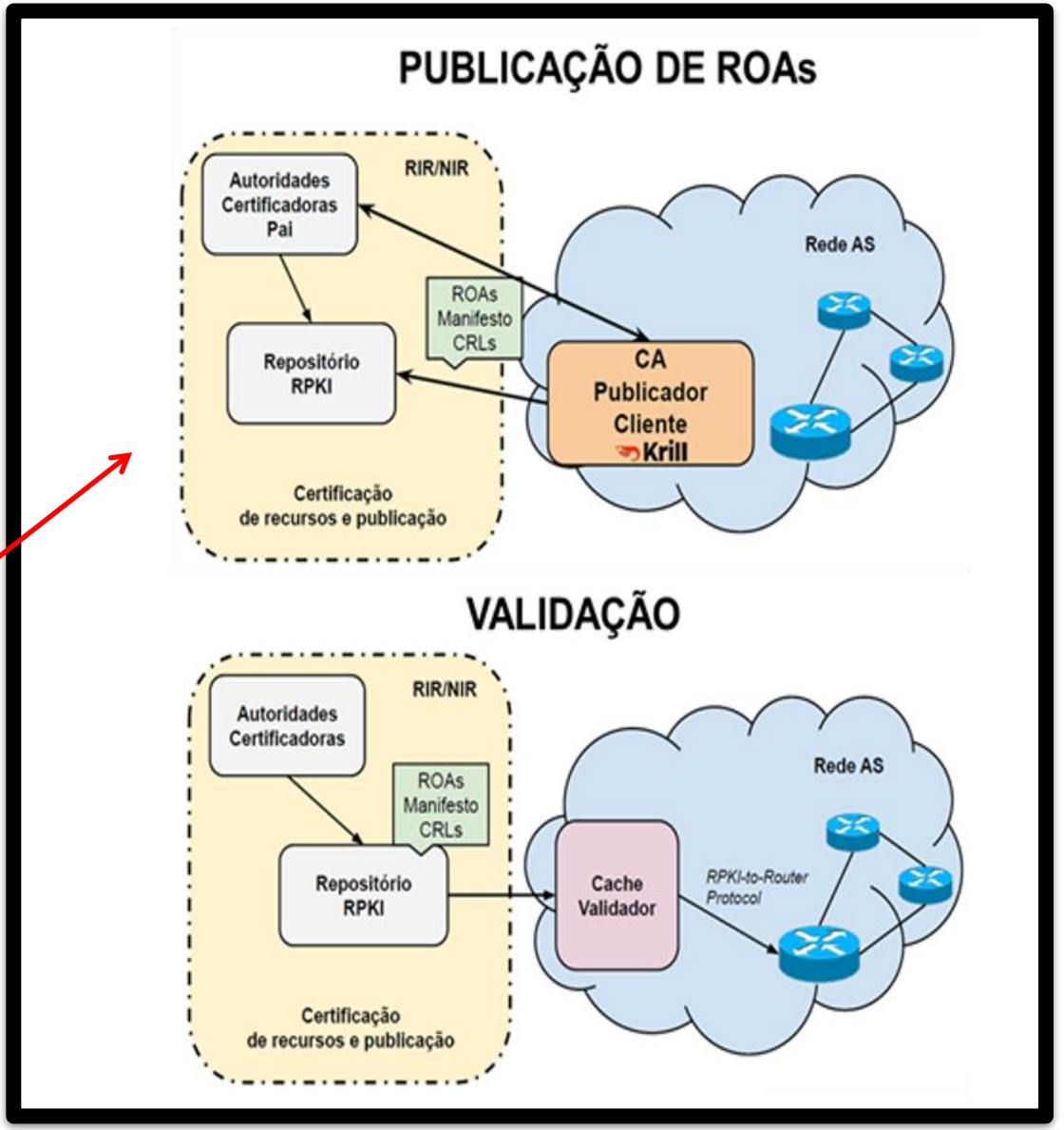
Programa por uma Internet mais Segura

MANRS - Ação 4 - Cadastro da Política de Roteamento

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

- **RPKI** - Resource Public Key Infrastructure

Desafio BCOP



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 - Mato Grasso do Sul - 143 AS

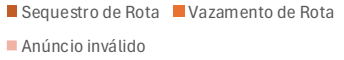
Resumo

31-out-25

MANRS - Status da Segurança de Roteamento

Incidentes

Sequestro de Rota	0
Vazamento de Rota	0
Anúncio inválido	0
Total	0



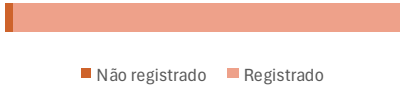
Responsáveis

AS responsáveis	0

Informação de Roteamento

IRR

Não registrado	22	**1,9%**
Registrado	1.118	**98,1%**



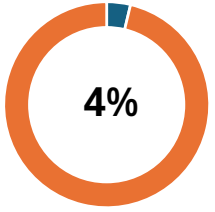
RPKI

Válido	501	**43,9%**
Desconhecido	639	**56,1%**
Inválido	0	**0,0%**

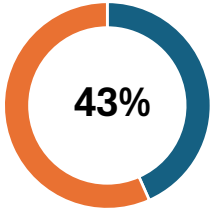
MANRS - Prontidão

Filtros BGP

Anti-spoofing

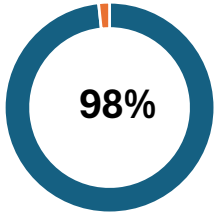


Coordenação

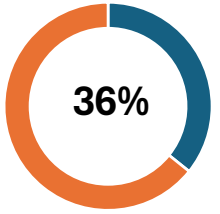


Informação de Roteamento

IRR



RPKI



Programa por uma Internet mais Segura

MANRS Observatory - 143 AS – MS

ASN	Country	RIR Regions	Filtering	Anti-spoofing	Coordination	Routing Information	Routing Information	Participante MANRS	Status abuse-c	Status Notifificações
ASN 10	BR	LACNIC	100%	0%	100%	100%	50%		PEND	
ASN 33	BR	LACNIC	100%	0%	100%	100%	100%		PEND	
ASN 42	BR	LACNIC	100%	0%	100%	100%	0%		PEND	
ASN 52	BR	LACNIC	100%	0%	0%	100%	0%		PEND	
ASN 55	BR	LACNIC	100%	0%	0%	100%	0%		PEND	
ASN 58	BR	LACNIC	100%	0%	100%	100%	0%		PEND	
ASN 59	BR	LACNIC	100%	0%	100%	100%	0%		PEND	
ASN 67	BR	LACNIC	100%	0%	100%	100%	100%		PEND	
ASN 75	BR	LACNIC	100%	0%	0%	100%	100%		PEND	
ASN 85	BR	LACNIC	100%	0%	100%	100%	0%		PEND	
ASN 90	BR	LACNIC	100%	0%	0%	100%	0%		BLOCK	NOK
ASN 92	BR	LACNIC	100%	0%	100%	100%	0%		PEND	
ASN 98	BR	LACNIC	100%	0%	0%	100%	0%		PEND	
ASN 100	BR	LACNIC	100%	0%	0%	100%	0%		BLOCK	
ASN 103	BR	LACNIC	100%	0%	100%	100%	89%		PEND	
ASN 104	BR	LACNIC	100%	0%	0%	100%	0%		BLOCK	
ASN 118	BR	LACNIC	100%	0%	0%	100%	0%		BLOCK	
ASN 126	BR	LACNIC	100%	0%	0%	100%	100%		PEND	

PEND - ASN com status pendente junto ao registro.br

BLOQ - ASN com status bloqueio junto ao registro.br

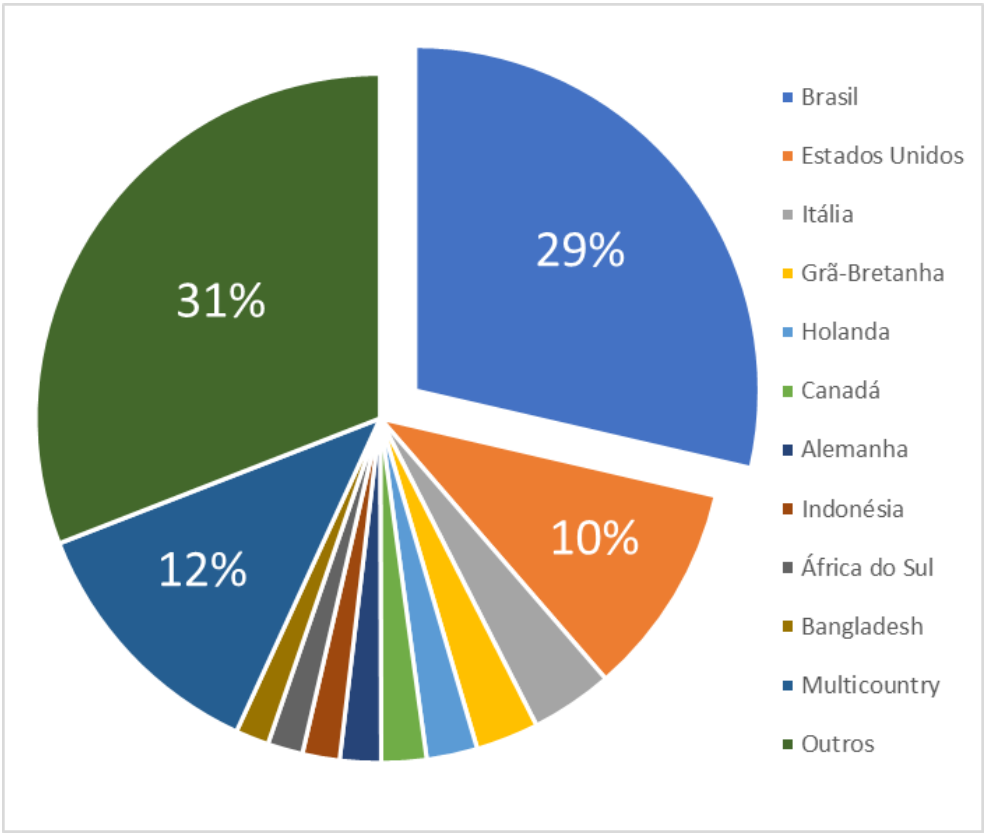
Programa por uma Internet mais Segura

Participantes por país

- Total: 1.095
- Participantes no Brasil → 316

MANRS

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



Fonte: https://www.manrs.org/netops/participants/ Acesso 01/10/25

Programa por uma Internet mais Segura
MANRS Observatory - 143 AS – MS

ASN	Country	RIR Regions	Filtering	Anti-spoofing	Coordination	Routing Information	Routing Information	Participante MANRS
ASN 7	BR	LACNIC	100%	36%	100%	100%	100%	**61588**
ASN 14	BR	LACNIC	100%	0%	100%	100%	0%	**61785**
ASN 30	BR	LACNIC	100%	49%	100%	100%	100%	**263959**
ASN 32	BR	LACNIC	100%	0%	100%	100%	100%	**263968**
ASN 57	BR	LACNIC	100%	0%	100%	100%	0%	**266266**
ASN 105	BR	LACNIC	100%	0%	100%	100%	0%	**269657**
ASN 117	BR	LACNIC	100%	100%	0%	100%	0%	**270812**
ASN 121	BR	LACNIC	100%	0%	100%	100%	0%	**270890**

8 AS da região são participantes do MANRS

PROGRAMA INTERNET +SEGURA

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

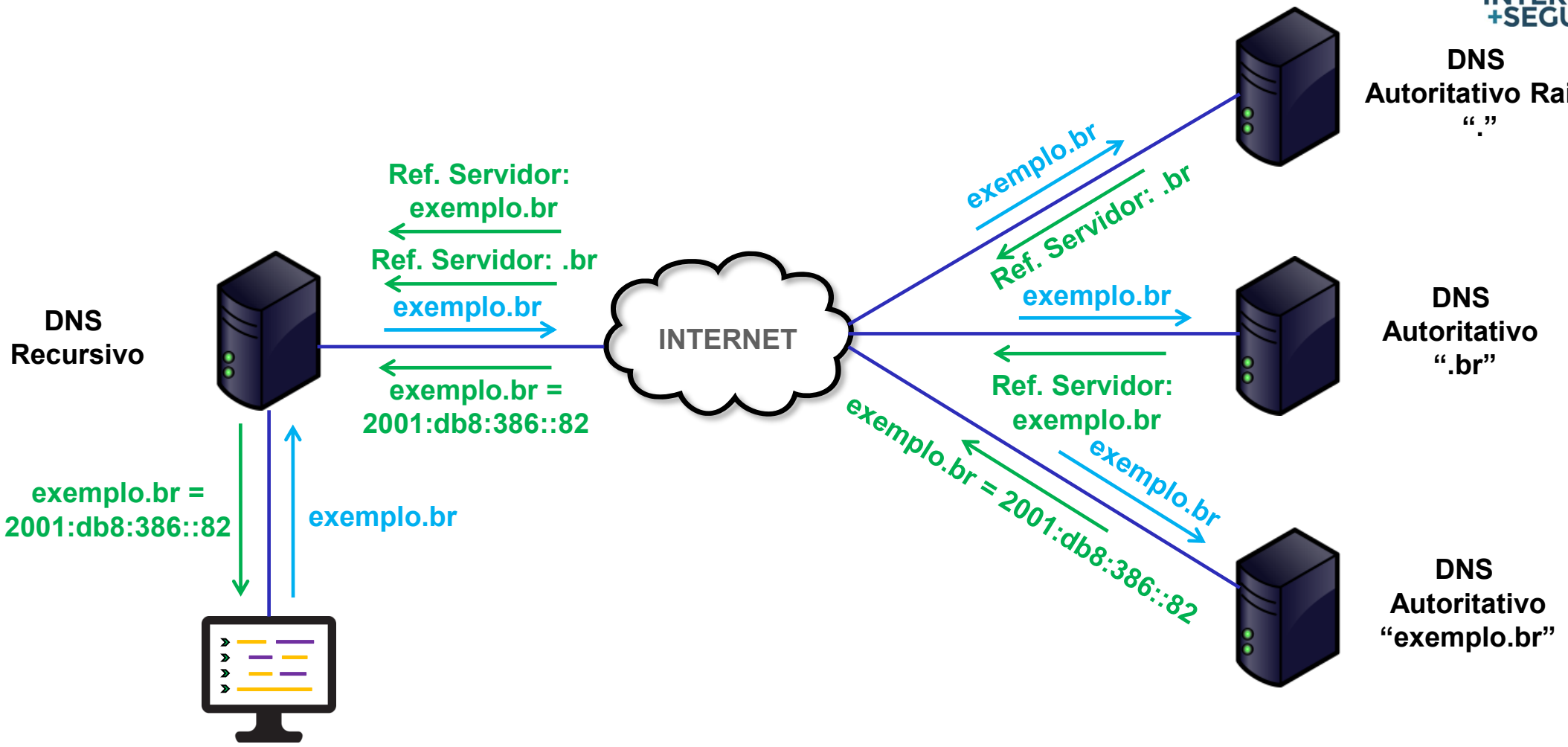
https://kindns.org/

An ICANN Initiative

ICANN

Programa por uma Internet mais Segura

Processo de Recursão DNS



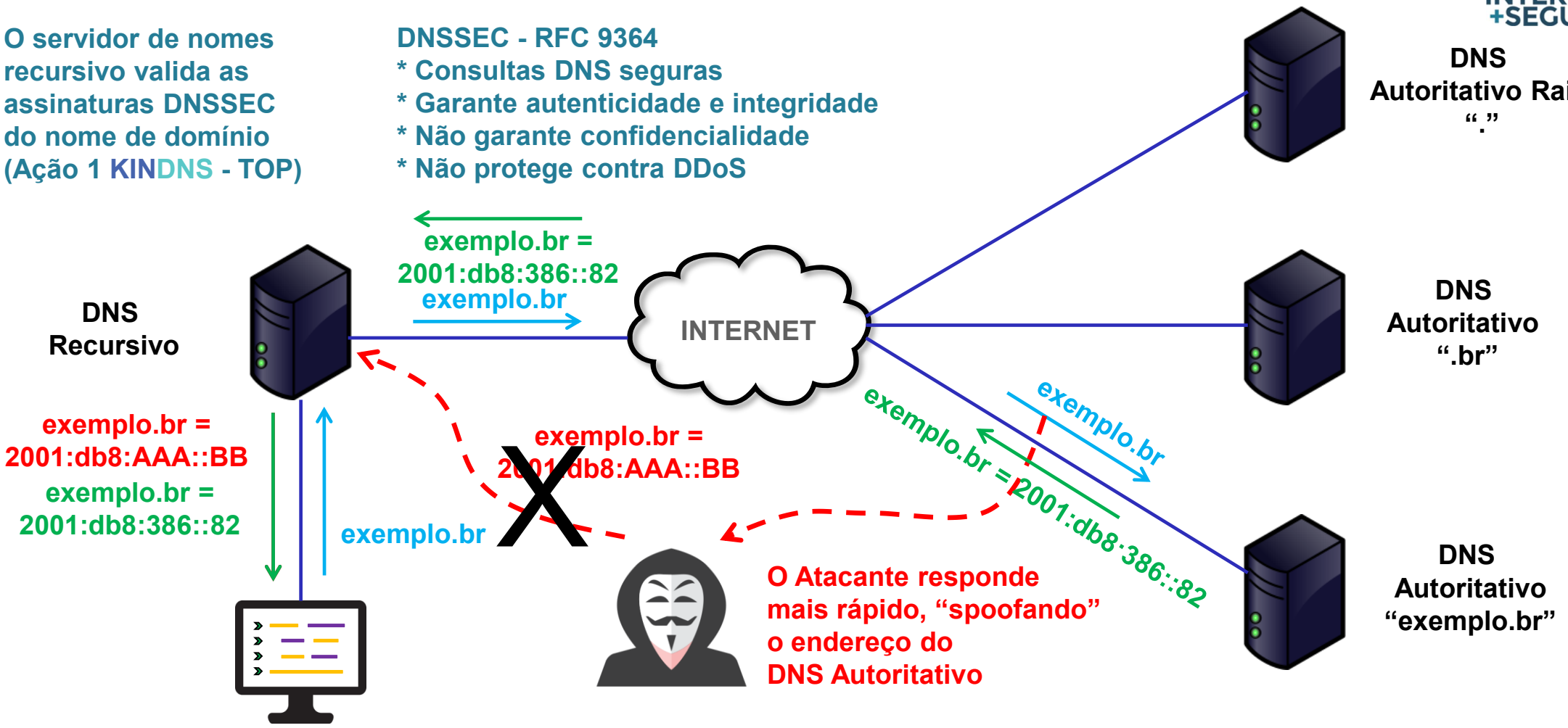
Tutorial: Configurando o seu DNS de forma simples e segura – Ataque DNS Poisoning

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

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/

Tutorial: Configurando o seu DNS de forma simples e segura

KINDNS

PROGRAMA INTERNET +SEGURA

TOP

TESTE OS PADRÕES

https://top.nic.br

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!

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

Desafio BCOP ↑

https://top.nic.br

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

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

14 de novembro de 2025

nic.br cgi.br

www.nic.br | www.cgi.br