



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

IX Fórum Regional Edição Nordeste

Natal, RN | 12/09/25

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**

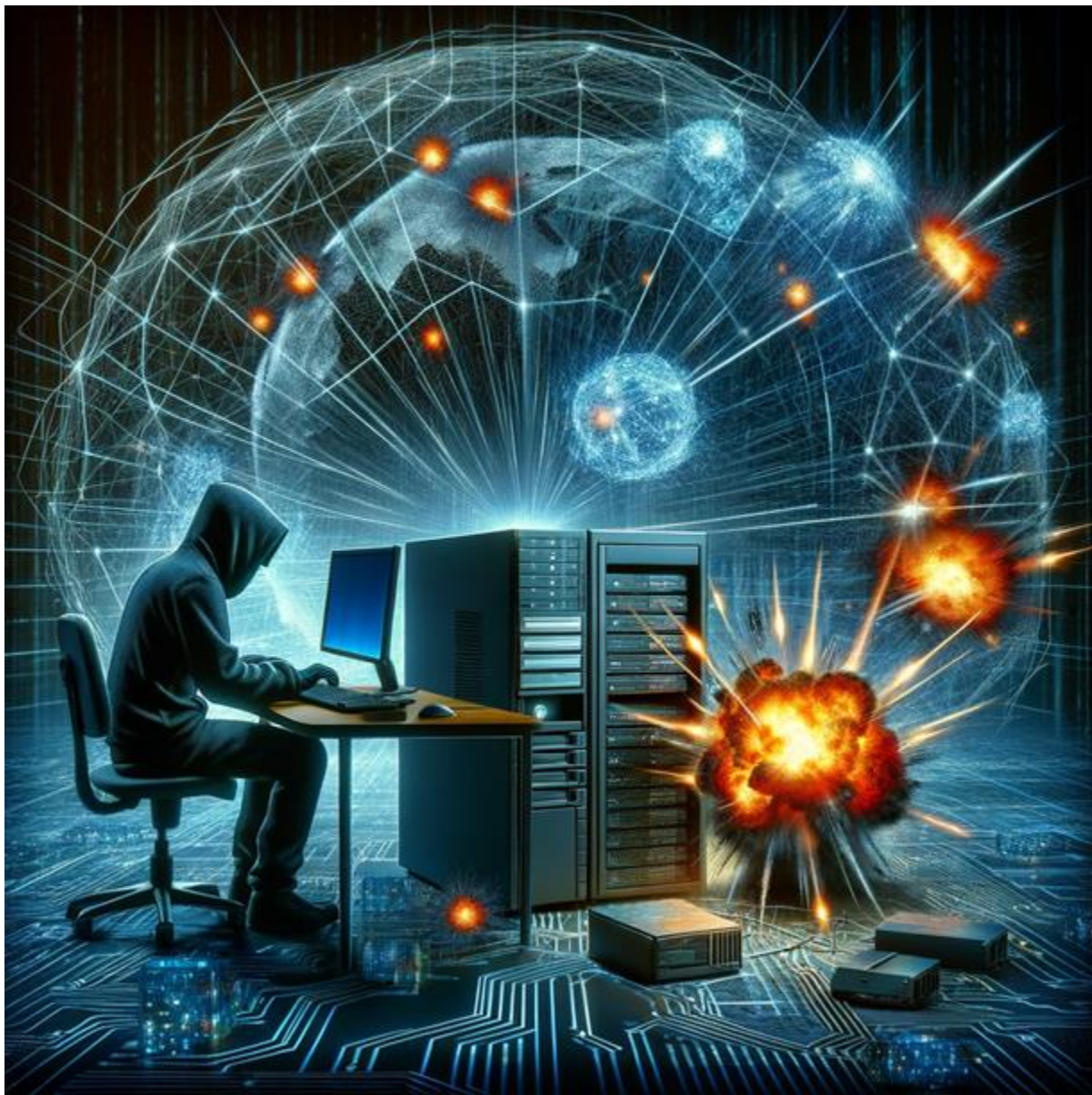
<https://bcp.nic.br/i+seg>



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

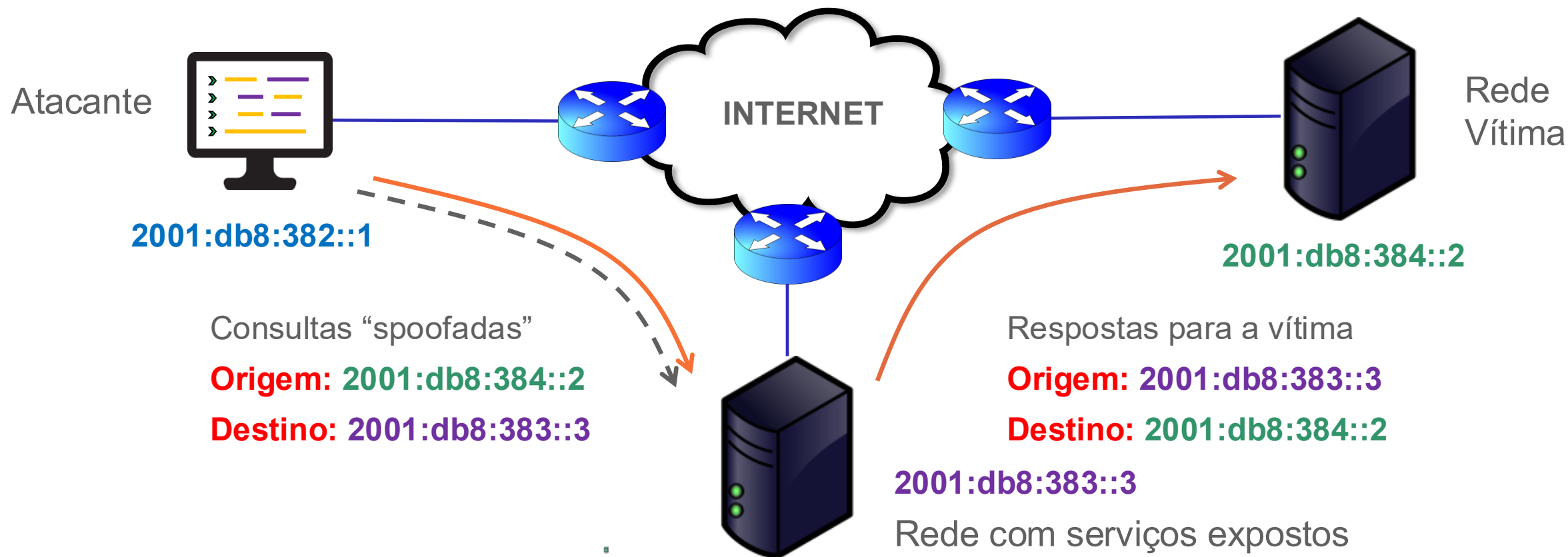
<https://bcp.nic.br/i+seg/acoes/amplificacao/>



Programa por uma Internet mais Segura

Negação de Serviço Reflexivo com Amplificação

Utiliza um terceiro para fazer o ataque



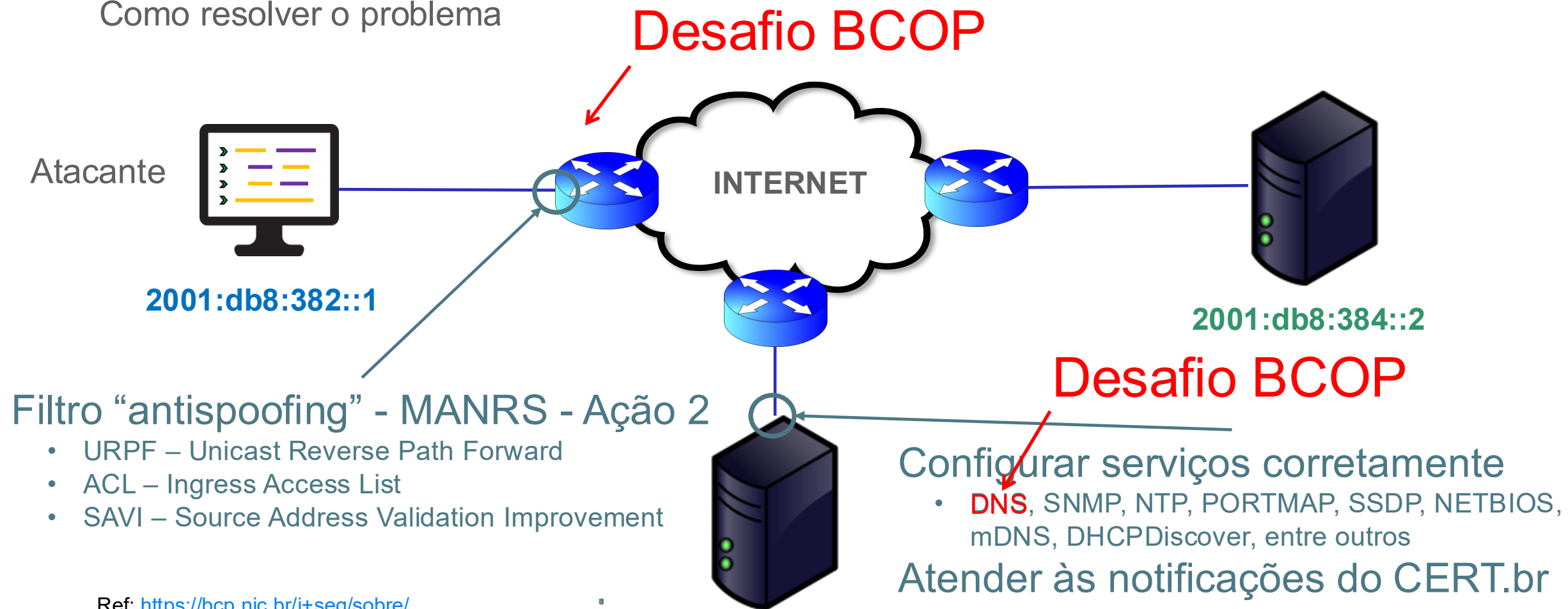
[Ref. Tutorial - Resolvendo os principais incidentes de segurança](#)

Programa por uma Internet mais Segura

Negação de Serviço Reflexivo com Amplificação



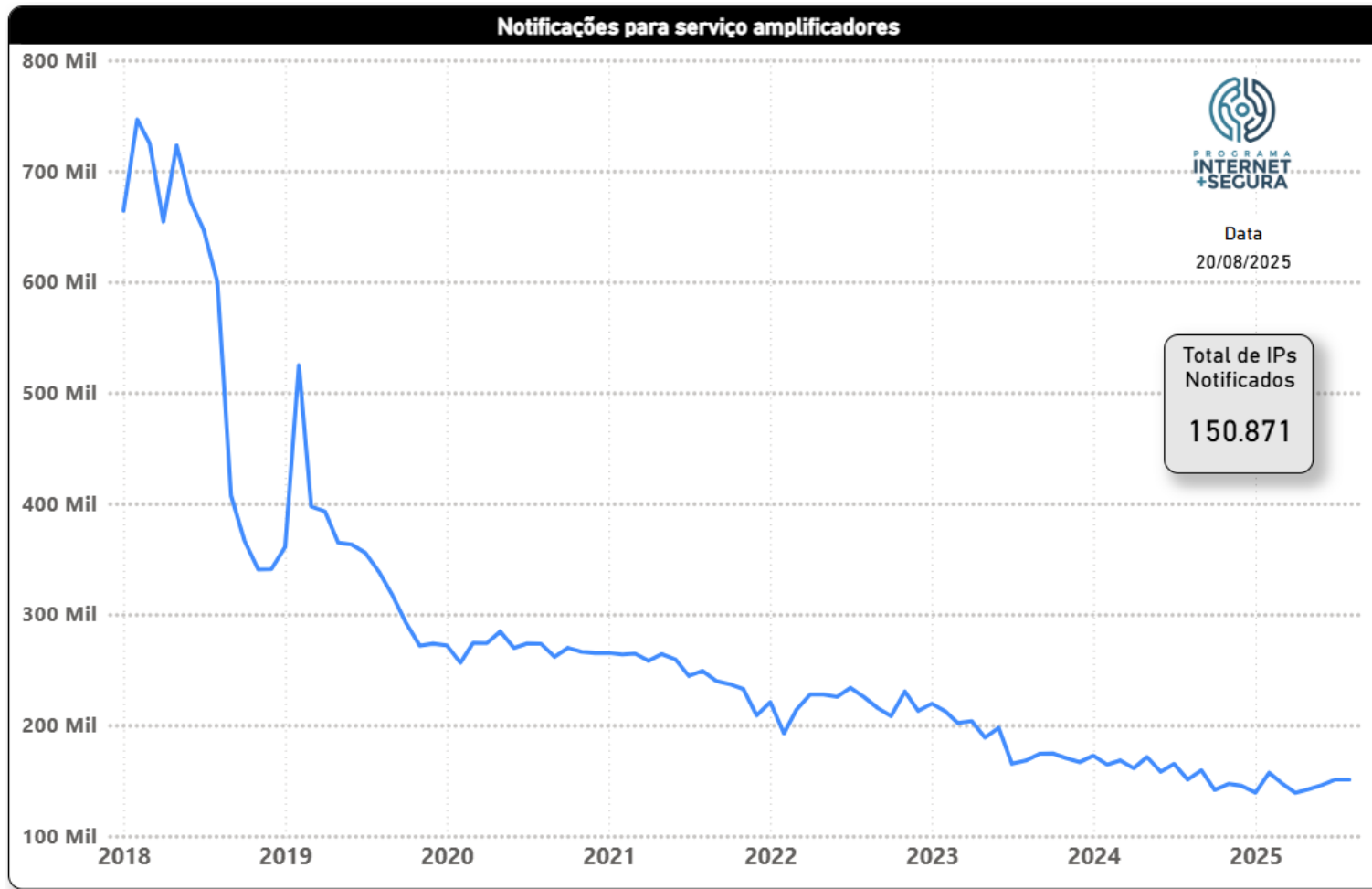
Como resolver o problema



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

Programa por uma Internet mais Segura

Notificação de amplificadores - evolução

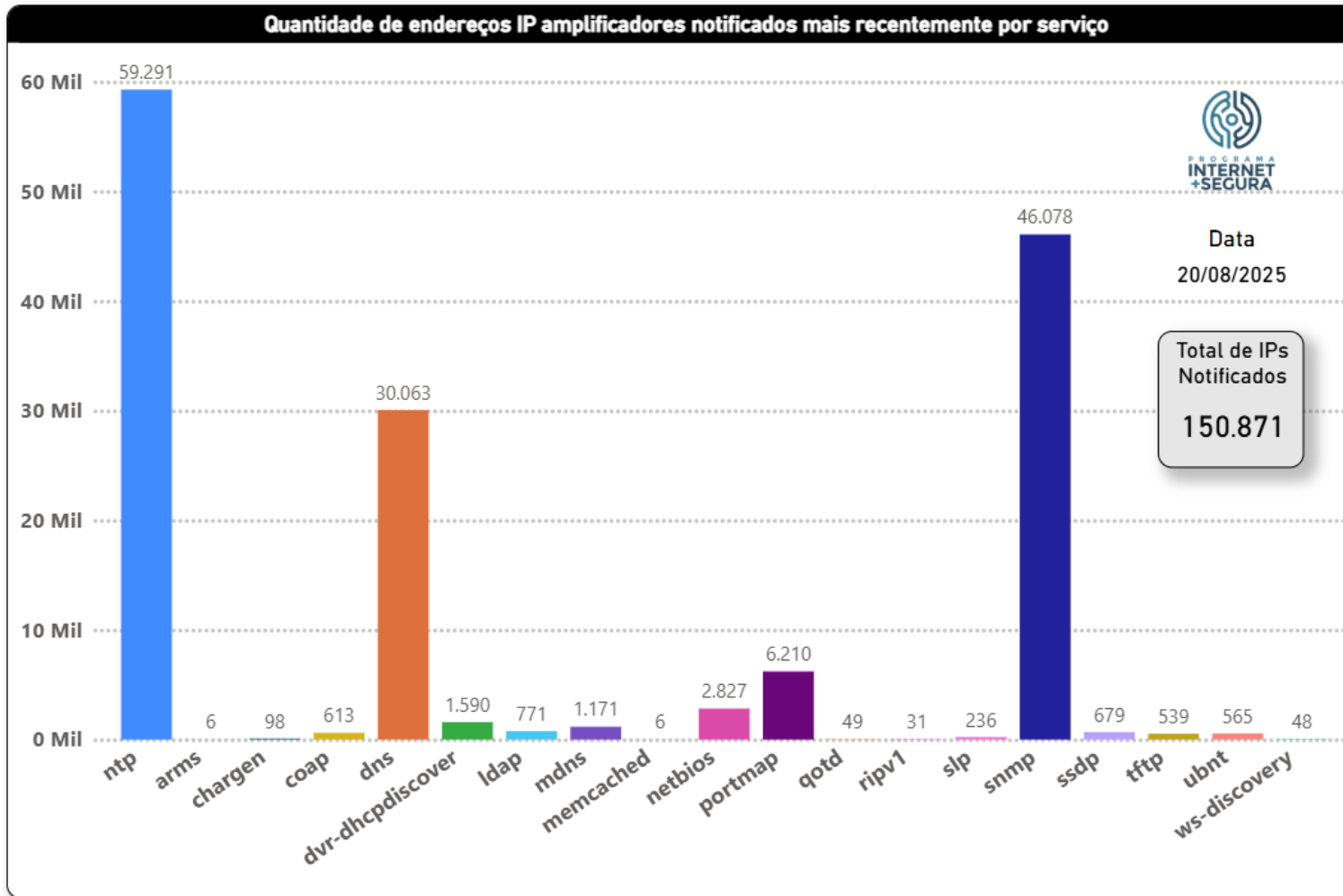


Brasil

- Início (fev/2018)
 - Endereços IP: 746.508
 - Serviços: 5
- Atual:
 - Endereços IP: 150.871
 - Serviços: 19
 - **Redução de 79%**

Programa por uma Internet mais Segura

Notificação de amplificadores - serviços

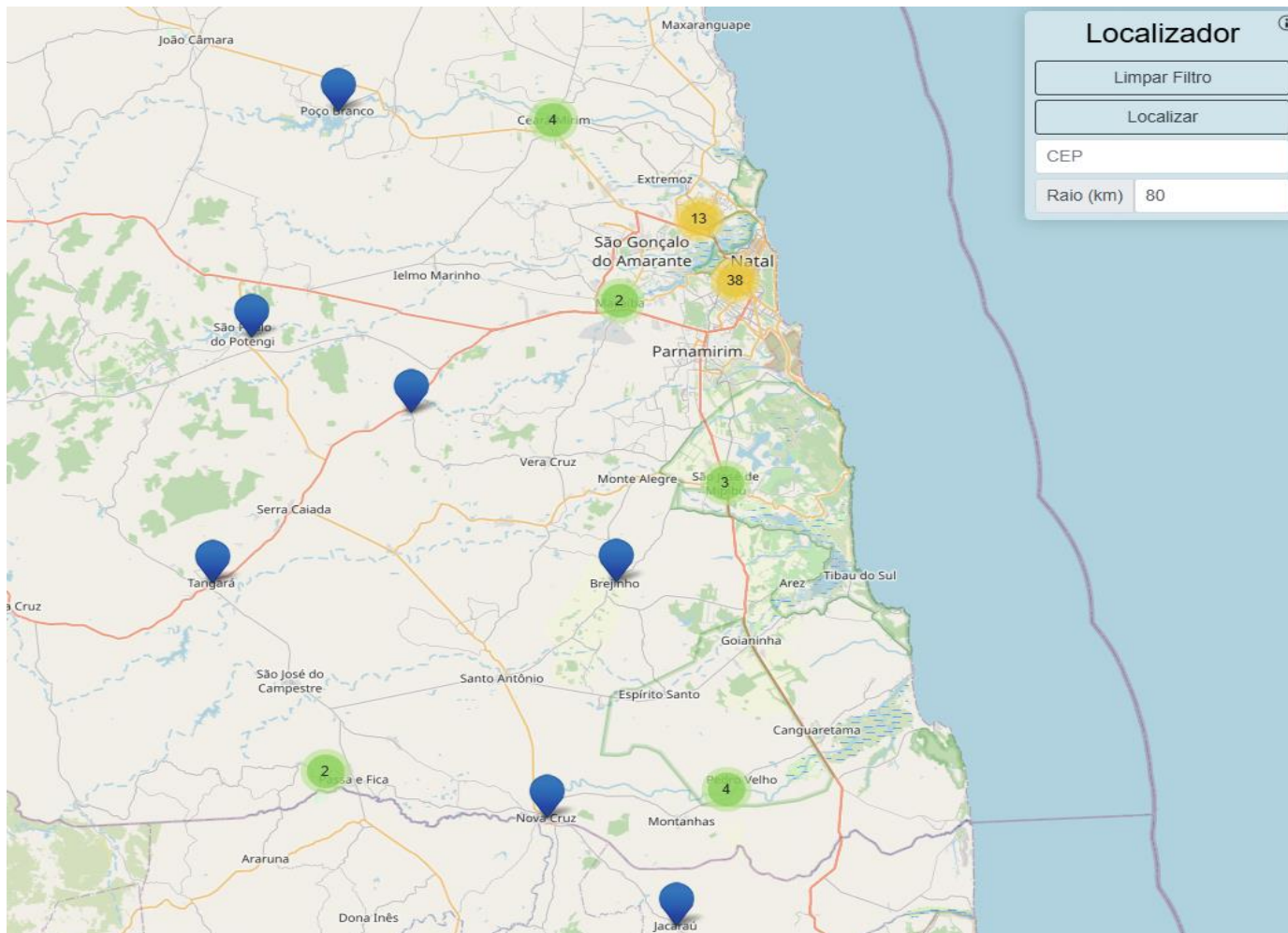


Brasil

- 9.030 AS
- 5.178 AS notificados
- 150.871 endereços IP mal configurados
- **NTP 59.291**
- **SNMP 46.078**
- **DNS 30.063**

Programa por uma Internet mais Segura

Notificação de amplificadores - serviços



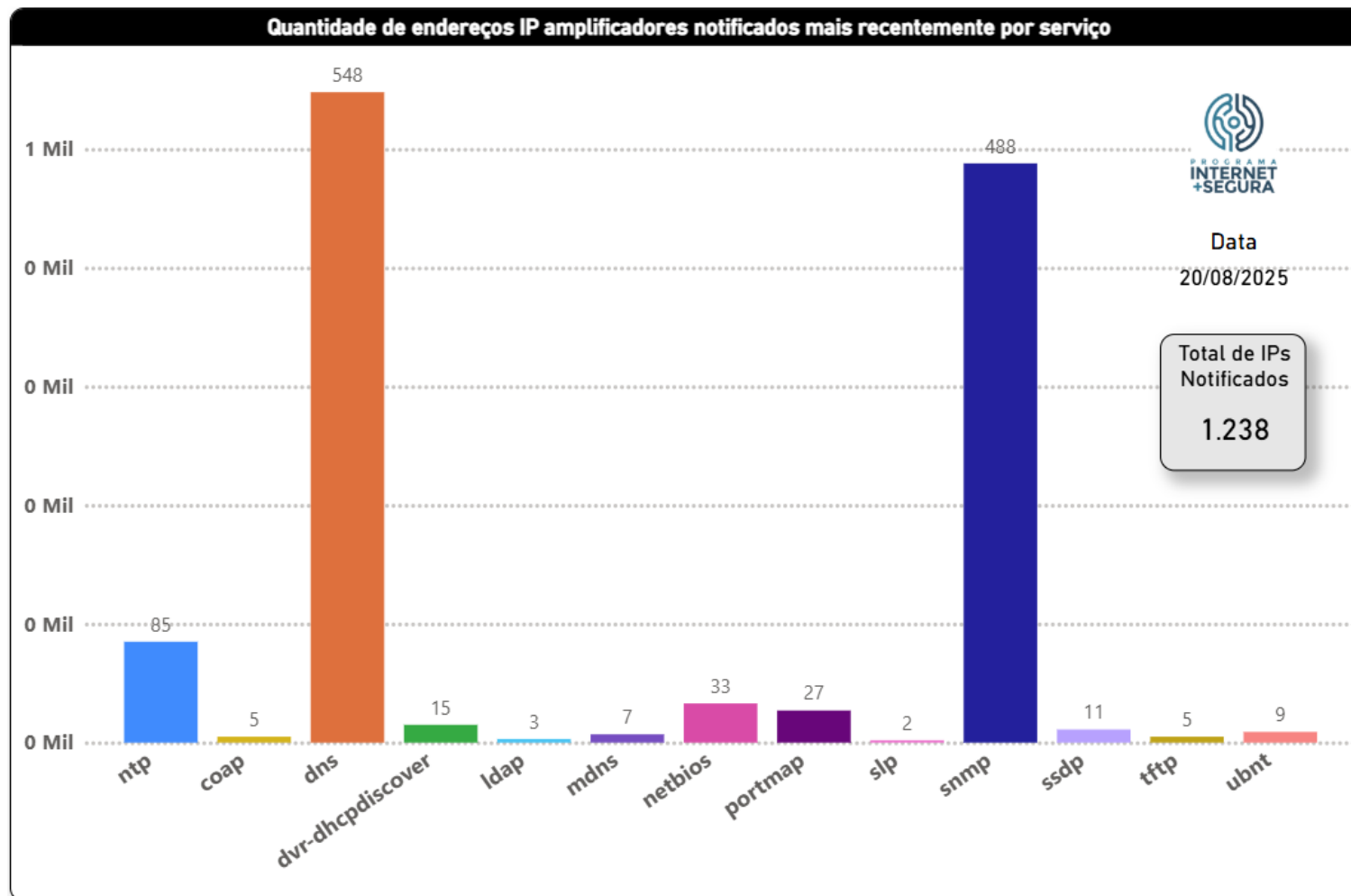
Natal – 80 Km (73 AS)

- Natal (42)
- Ceará-Mirim (4)
- Parnamirim (4)
- São Gonçalo do Amarante (4)
- Macaíba (3)
- Pedro Velho (3)
- São José de Mipibu (3)
- Bom Jesus (1)
- Brejinho (1)
- Caiçara do Rio do Vento (1)
- Montanhas (1)
- Nova Cruz (1)
- Passa e Fica (1)
- Poço Branco (1)
- São Miguel do Gostoso (1)
- São Paulo do Potengi (1)
- Tangará (1)

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

Programa por uma Internet mais Segura

Notificação de amplificadores - serviços



Natal – 80 Km

- 73 AS
- 37 AS conectados ao IX
- 42 AS notificados
- **2 AS com mais de 400 IP notificados**
- 1.238 endereços IP mal configurados
 - **DNS 548**
 - **SNMP 488**
 - **NTP 85**



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)

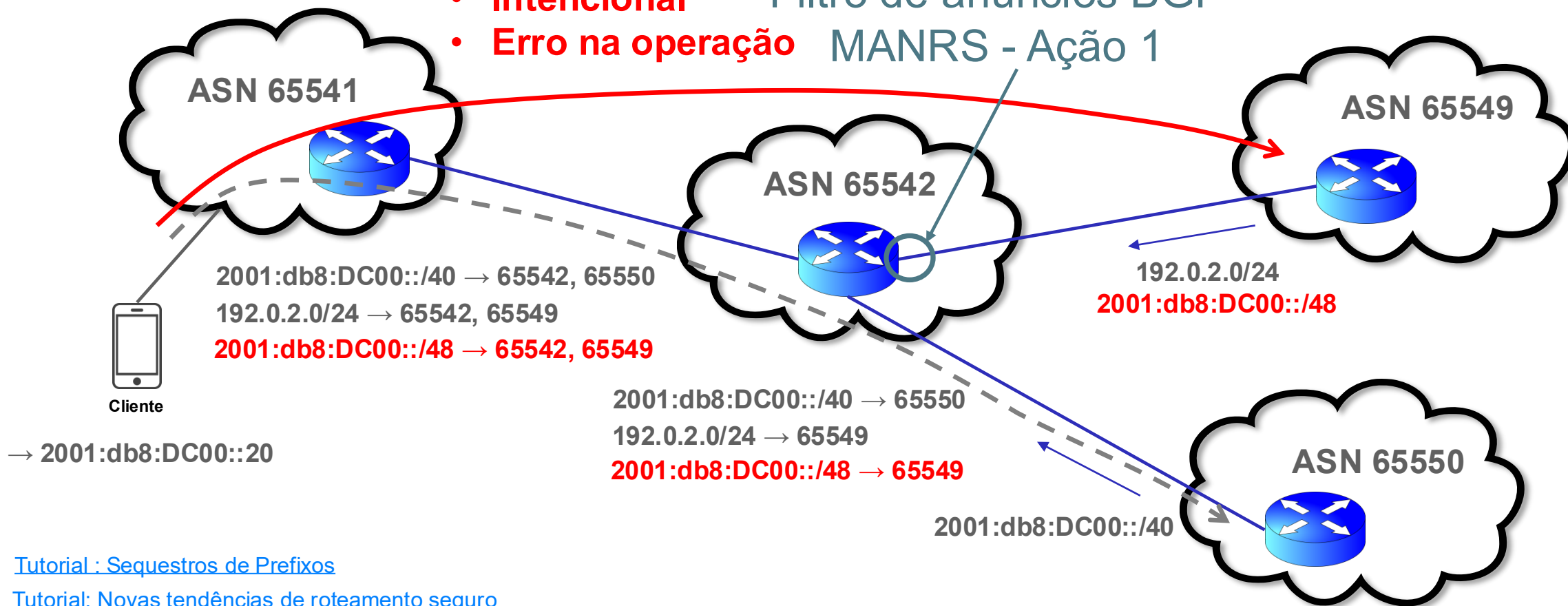
Anúncio de prefixos não autorizados:

- Intencional

Filtro de anúncios BGP

- Erro na operação

MANRS - Ação 1



[Tutorial: Sequestros de Prefixos](#)

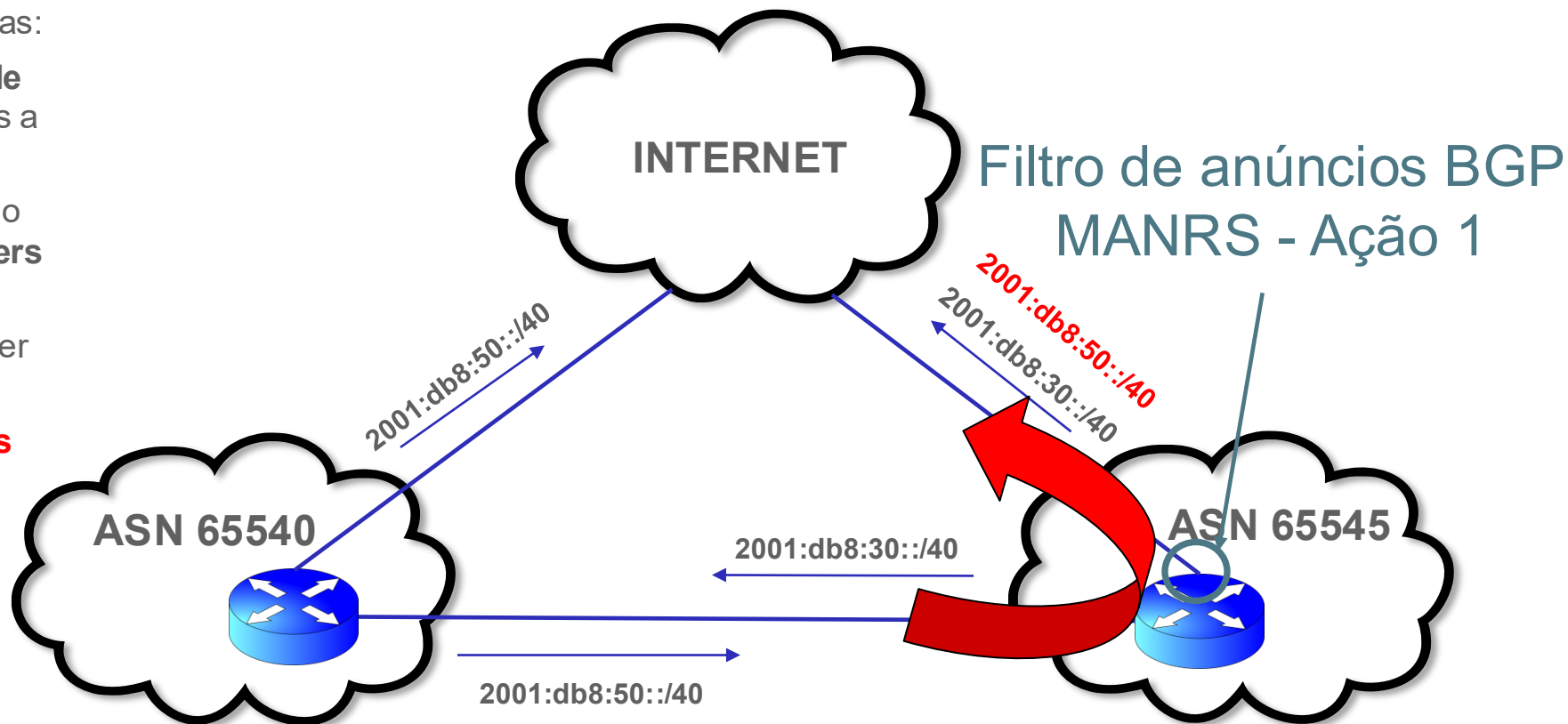
[Tutorial: Novas tendências de roteamento seguro](#)

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



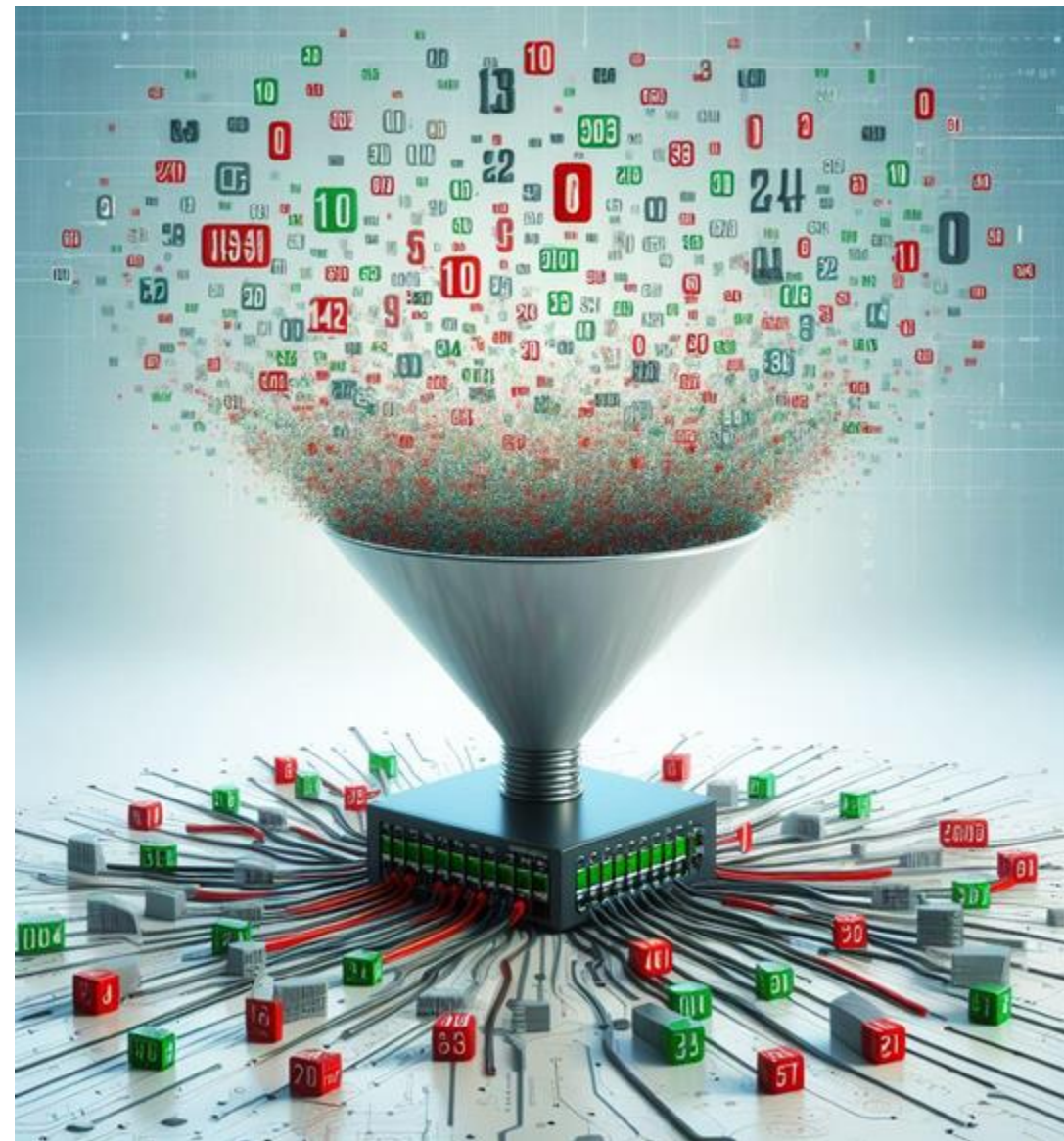
Programa por uma Internet mais Segura



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**



<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

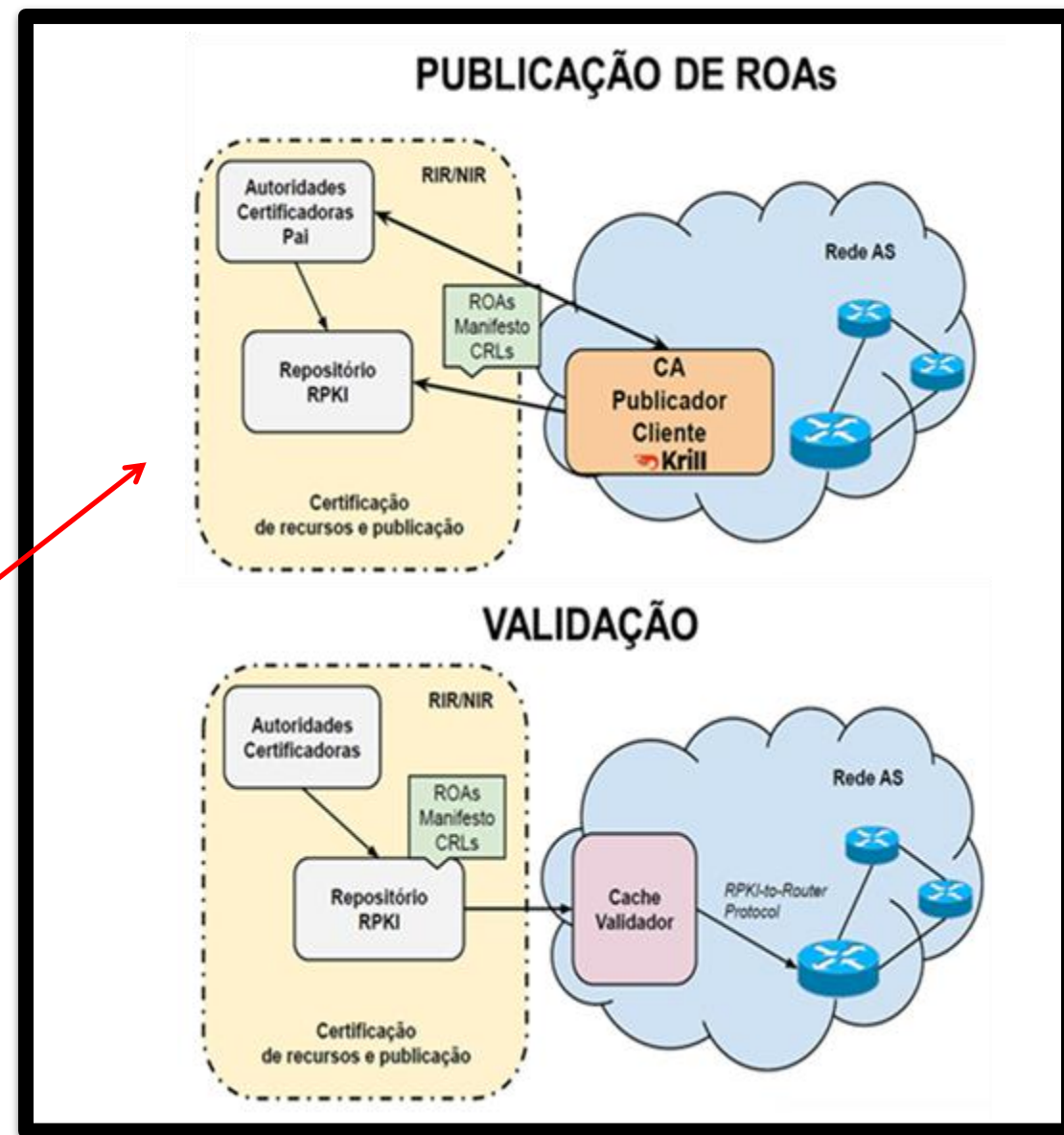
- RPKI - Resource Public Key Infrastructure

<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 - Natal 80 Km - 72 AS



MANRS

Resumo

31-ago-25

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

Não registrado	8	1,4%
Registrado	580	98,6%



■ Não registrado ■ Registrado

RPKI

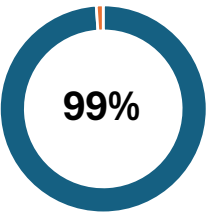
Válido	373	64,1%
Desconhecido	205	35,2%
Inválido	4	0,7%



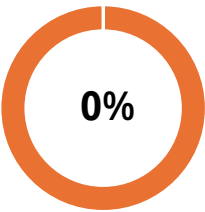
■ Válido ■ Desconhecido ■ Inválido

MANRS - Prontidão

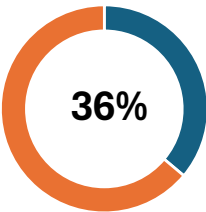
Filtros BGP



Anti-spoofing

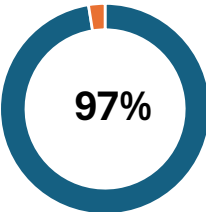


Coordenação

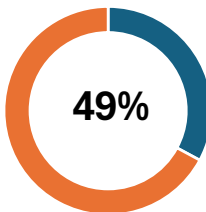


Informação de Roteamento

IRR



RPKI



Programa por uma Internet mais Segura

MANRS Observatory - 72 AS – Natal 80Km



ASN	Holder	Country	UN Regions	UN Sub-Regions	RIR Regions	Filtering	Anti-spoofing	Coordination	Routing Information	Routing Information	Participante MANRS	Status abuse-c
ASN 2	---	BR	Americas	Latin America and the Caribbean	LACNIC	100%	0%	100%	100%	100%	28184	OK
ASN 3	---	BR	Americas	Latin America and the Caribbean	LACNIC	94%	0%	100%	98%	100%		OK
ASN 9	---	BR	Americas	Latin America and the Caribbean	LACNIC	100%	0%	0%	100%	95%		OK
ASN 18	---	BR	Americas	Latin America and the Caribbean	LACNIC	100%	0%	100%	100%	100%		PEND
ASN 22	---	BR	Americas	Latin America and the Caribbean	LACNIC	100%	0%	100%	100%	93%		OK
ASN 25	---	BR	Americas	Latin America and the Caribbean	LACNIC	100%	0%	100%	100%	80%		OK
ASN 26	---	BR	Americas	Latin America and the Caribbean	LACNIC	100%	0%	100%	100%	0%		PEND
ASN 28	---	BR	Americas	Latin America and the Caribbean	LACNIC	100%	0%	0%	100%	0%		PEND
ASN 31	---	BR	Americas	Latin America and the Caribbean	LACNIC	100%	0%	100%	100%	100%	266388	OK
ASN 36	---	BR	Americas	Latin America and the Caribbean	LACNIC	100%	0%	100%	100%	57%		OK
ASN 44	---	BR	Americas	Latin America and the Caribbean	LACNIC	100%	0%	0%	100%	100%		PEND
ASN 57	---	BR	Americas	Latin America and the Caribbean	LACNIC	100%	0%	0%	100%	0%		PEND
ASN 63	---	BR	Americas	Latin America and the Caribbean	LACNIC	100%	0%	0%	20%	0%		OK
ASN 70	---	BR	Americas	Latin America and the Caribbean	LACNIC	100%	0%	0%	50%	0%		OK
ASN 71	---	BR	Americas	Latin America and the Caribbean	LACNIC	100%	0%	0%	50%	100%		OK

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: 1.087
- Participantes no Brasil → 311

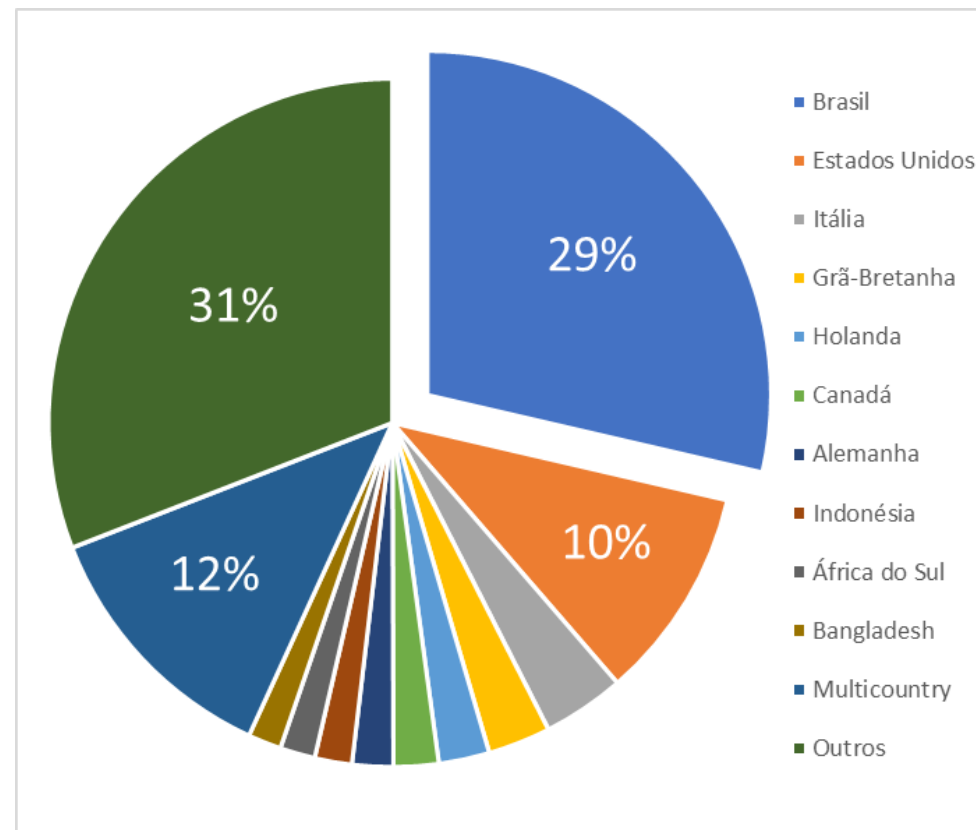


MANRS

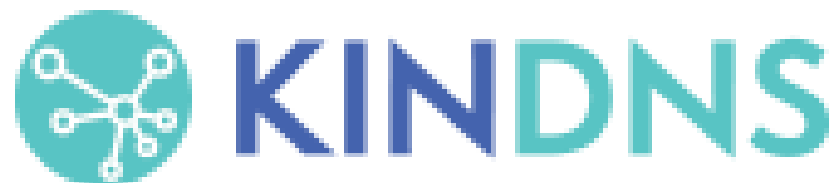
2024 → 292
2023 → 258
2022 → 206
2021 → 174
2020 → 140

- Participante de Natal 80 km:
AS28184 e AS266388

% de Participantes



Fonte: <https://www.manrs.org/netops/participants/> Acesso 01/09/25

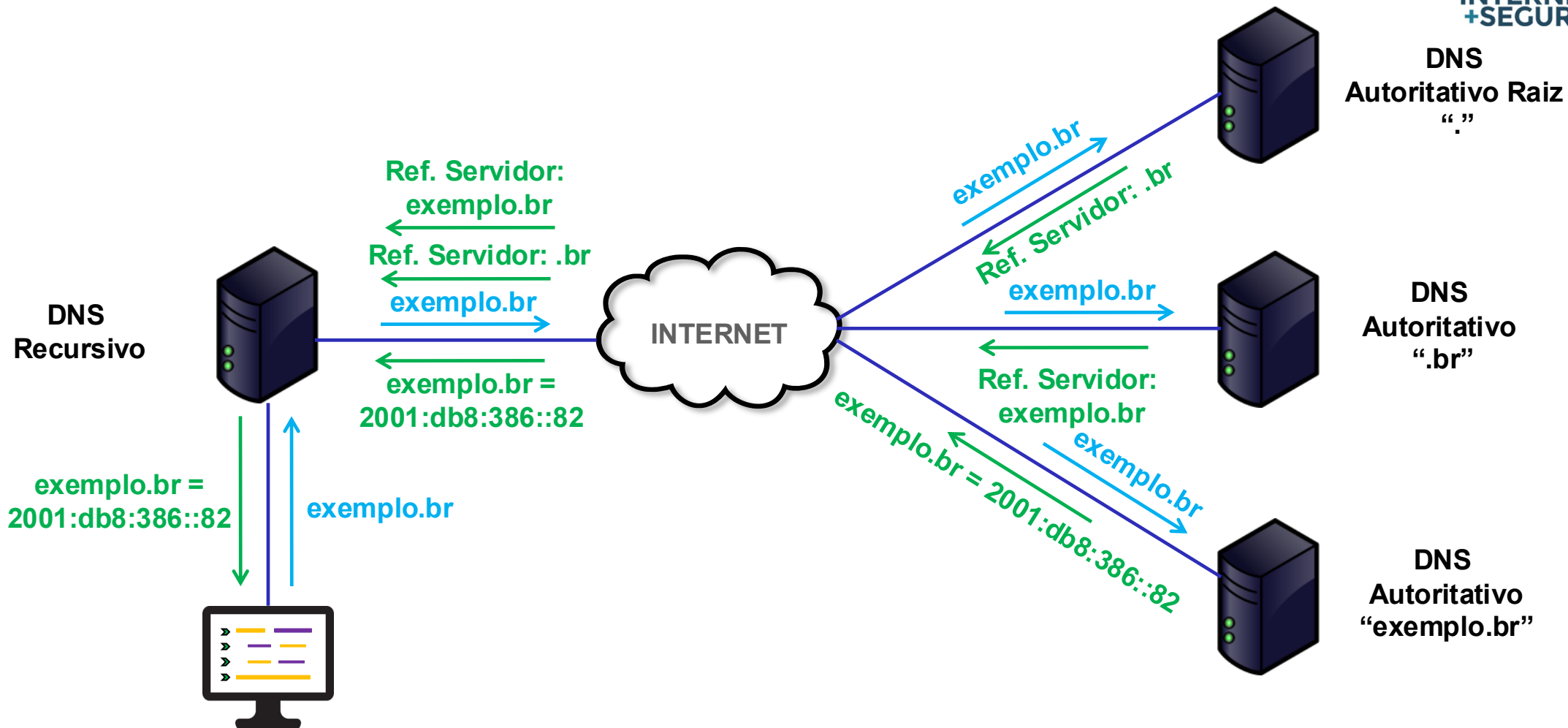


Stands for **K**nowledge-Sharing and
Intantiating **N**orms for **D**NS and **N**aming
Security

<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

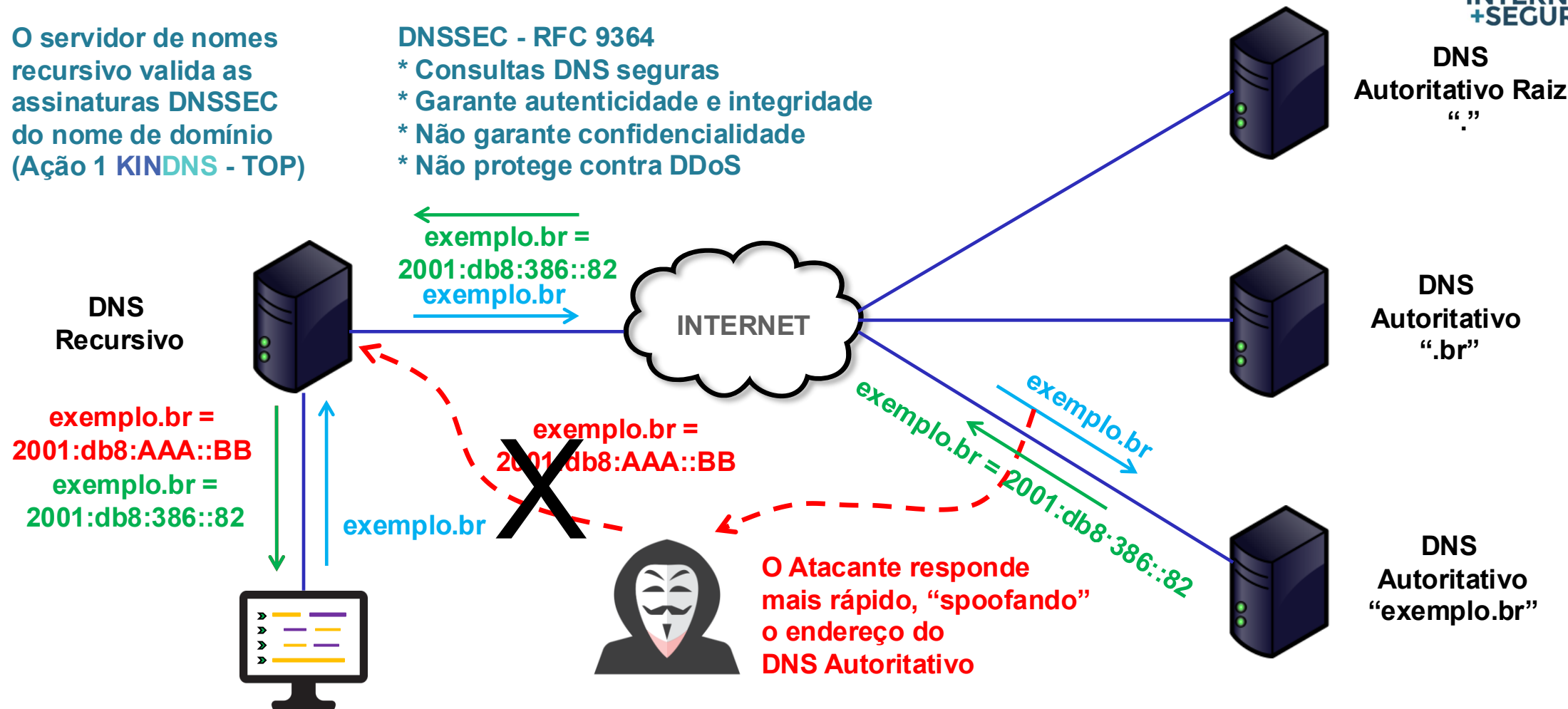
Ataque DNS - Poisoning



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>

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 ← **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](#)

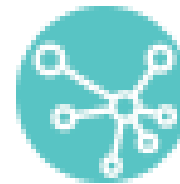


Programa por uma Internet mais Segura

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

01 de agosto de 2025

nic.br **cgi.br**

www.nic.br | www.cgi.br

