



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

Tecnologias e boas práticas para garantir a segurança e qualidade do seu provedor

Gilberto Zorello | gzorello@nic.br

Provedor em Foco - ABRINT - Edição Cascavel

Cascavel, PR | 05/11/25

nic.br

**Quem são o NIC.br e o CGI.br
e por que padrões técnicos,
boas práticas e colaboração
são importantes para a Internet?**

Como a Internet começou?

- Projeto da DARPA
- Redes resilientes
- Chegou ao Brasil na década de 1990
- Eco 92
- Abertura comercial
- CGI.br e NIC.br

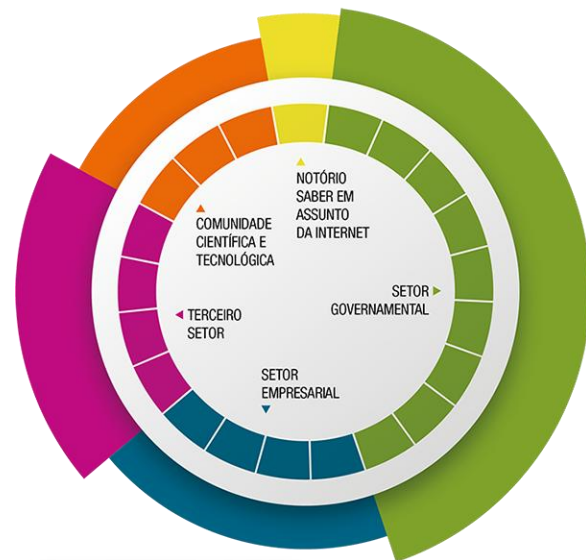




- CGI.br: criado em 1995
- Decreto em 2003
- Diretrizes para o desenvolvimento da Internet no Brasil
- NIC.br: organização privada sem finalidade de lucro
- Braço executivo do CGI.br

<https://nic.br/>

NIC.br e CGI.br



membros e ex-membros do CGI.br
(somente os atuais membros têm direito a voto)

ASSEMBLEIA GERAL

7 membros eleitos pela Assembleia Geral

CONSELHO DE
ADMINISTRAÇÃO

CONSELHO
FISCAL

ADMINISTRAÇÃO
JURÍDICO
COMUNICAÇÃO
ASSESSORIAS:
CGI.br e PRESIDÊNCIA

DIRETORIA
EXECUTIVA

1 2 3 4 5

registro.br

Domínios

cert.br

Segurança

cetic.br

Indicadores

ceptro.br

Redes e Operações

ceweb.br

Tecnologias Web

ix.br

Troca de Tráfego

W3C
CHAPTER
São Paulo

Padrões Web

- 1 Diretor presidente
- 2 Diretor administrativo e financeiro
- 3 Diretor de serviços e de tecnologia
- 4 Diretor de projetos especiais e de desenvolvimento
- 5 Diretor de assessoria às atividades do CGI.br



Padrões técnicos e colaboração

- RFCs
- IETF
- Padrões Abertos
- ~ 75 mil redes na Internet
- ~ 8,5 mil no Brasil
- Colaboração

<https://ietf.org/>
<https://bgp.potaroo.net/>
<https://mapadeas.ceptro.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

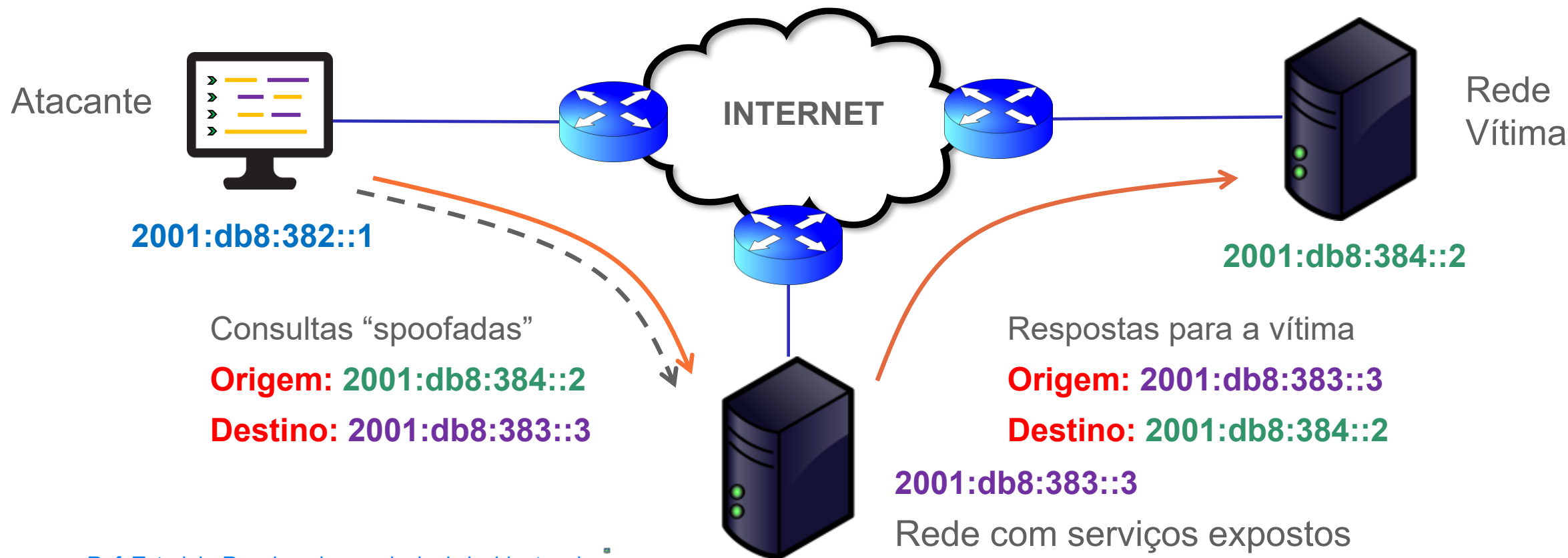
<https://bcp.nic.br/i+seg/acoes/amplificacao/>



Programa por uma Internet mais Segura

Negação de Serviço Reflexivo com Amplificação

Utiliza um terceiro para fazer o ataque



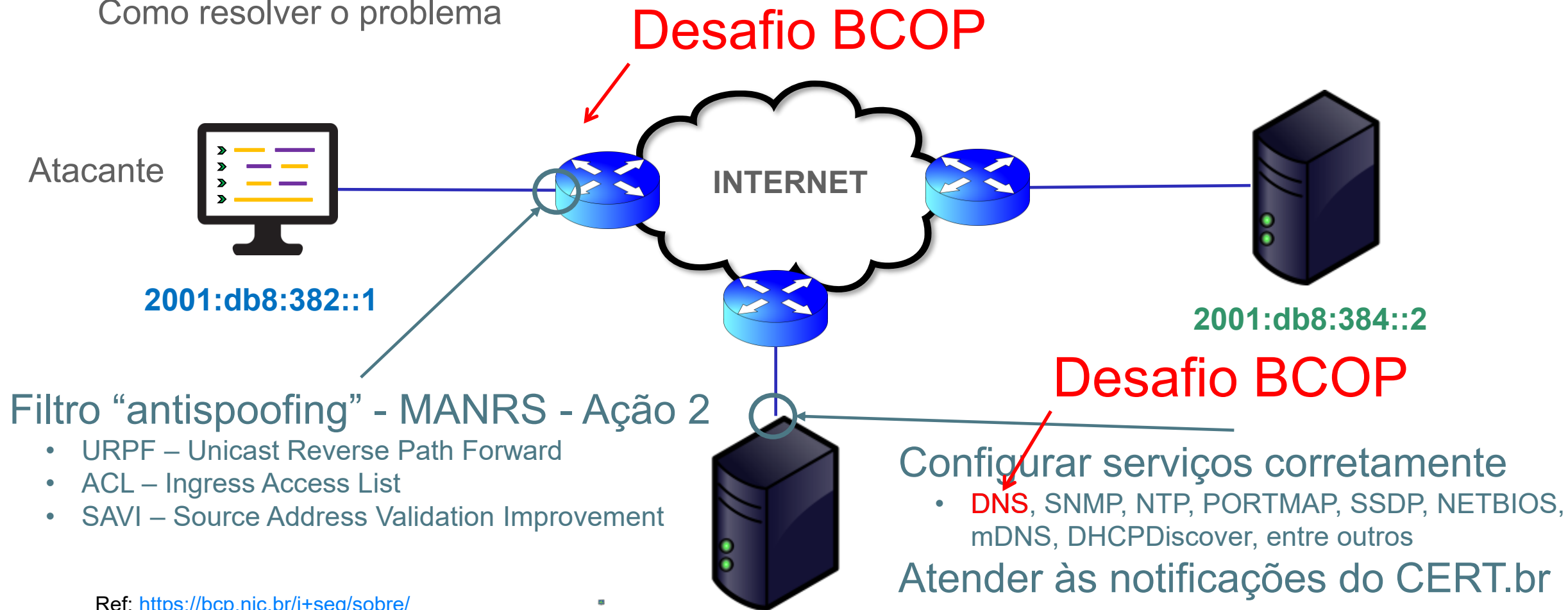
[Ref. Tutorial - Resolvendo os principais incidentes de segurança](#)

Programa por uma Internet mais Segura

Negação de Serviço Reflexivo com Amplificação



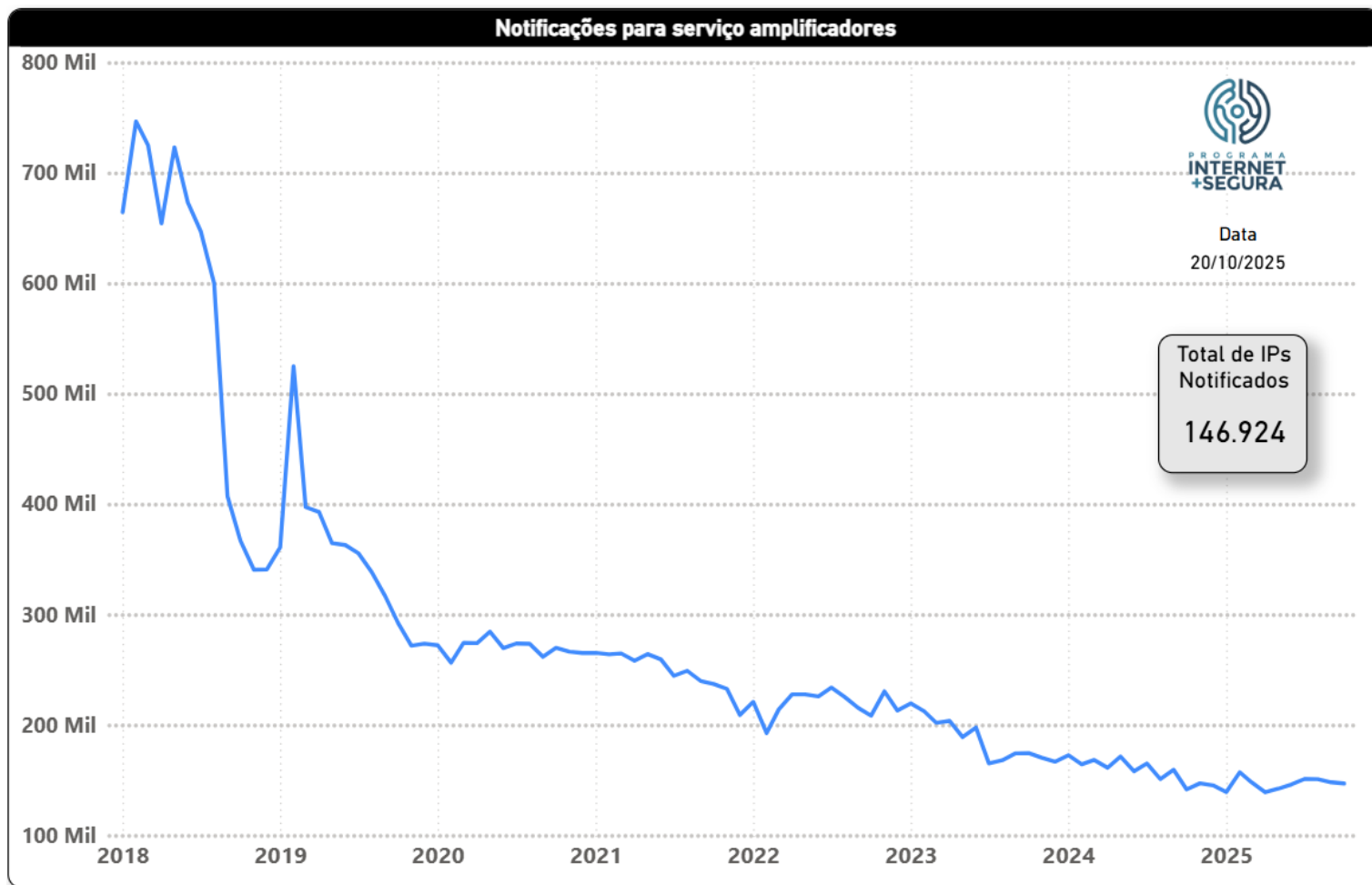
Como resolver o problema



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

Programa por uma Internet mais Segura

Notificação de amplificadores - evolução

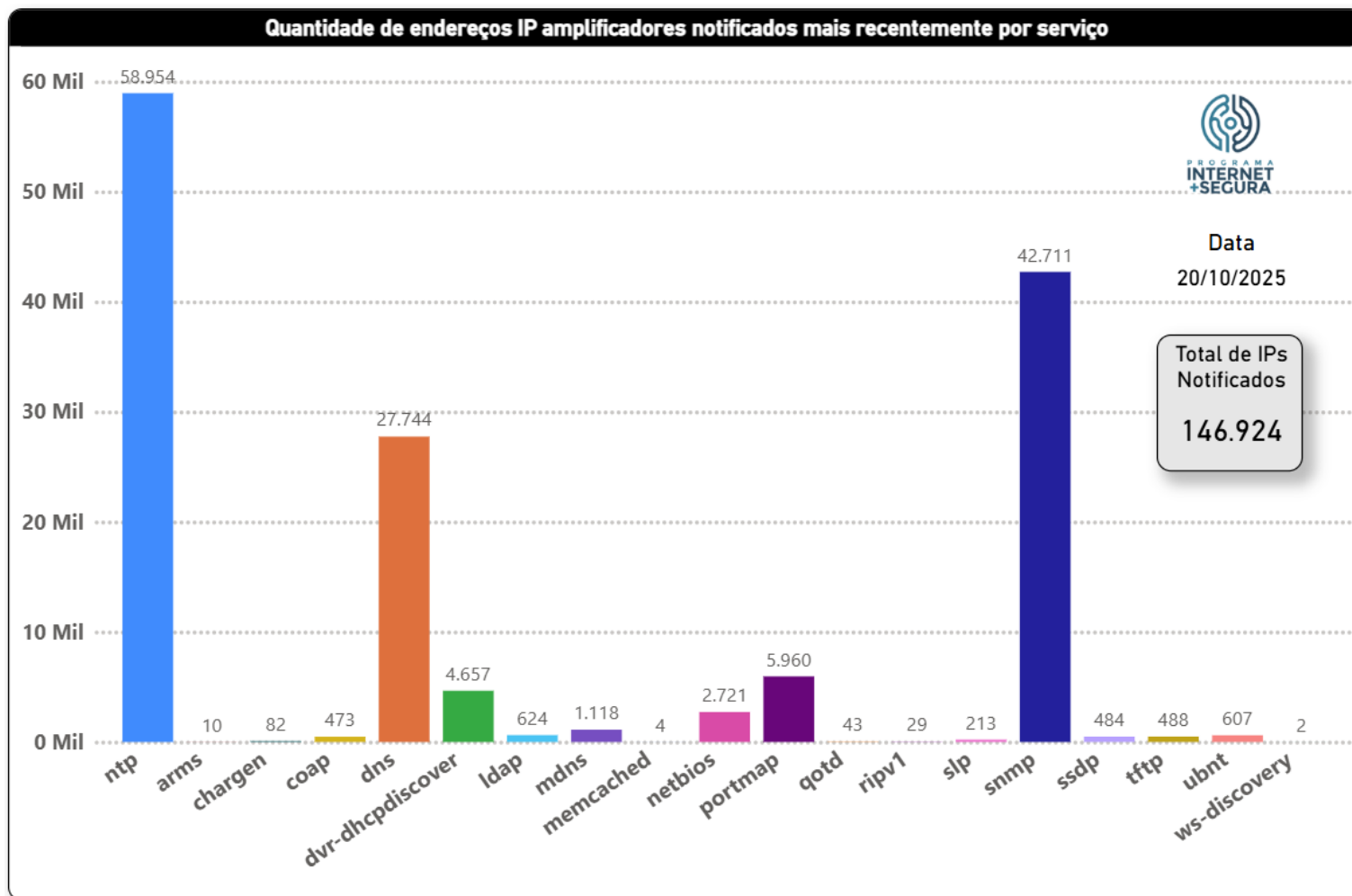


Brasil

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

Programa por uma Internet mais Segura

Notificação de amplificadores - serviços

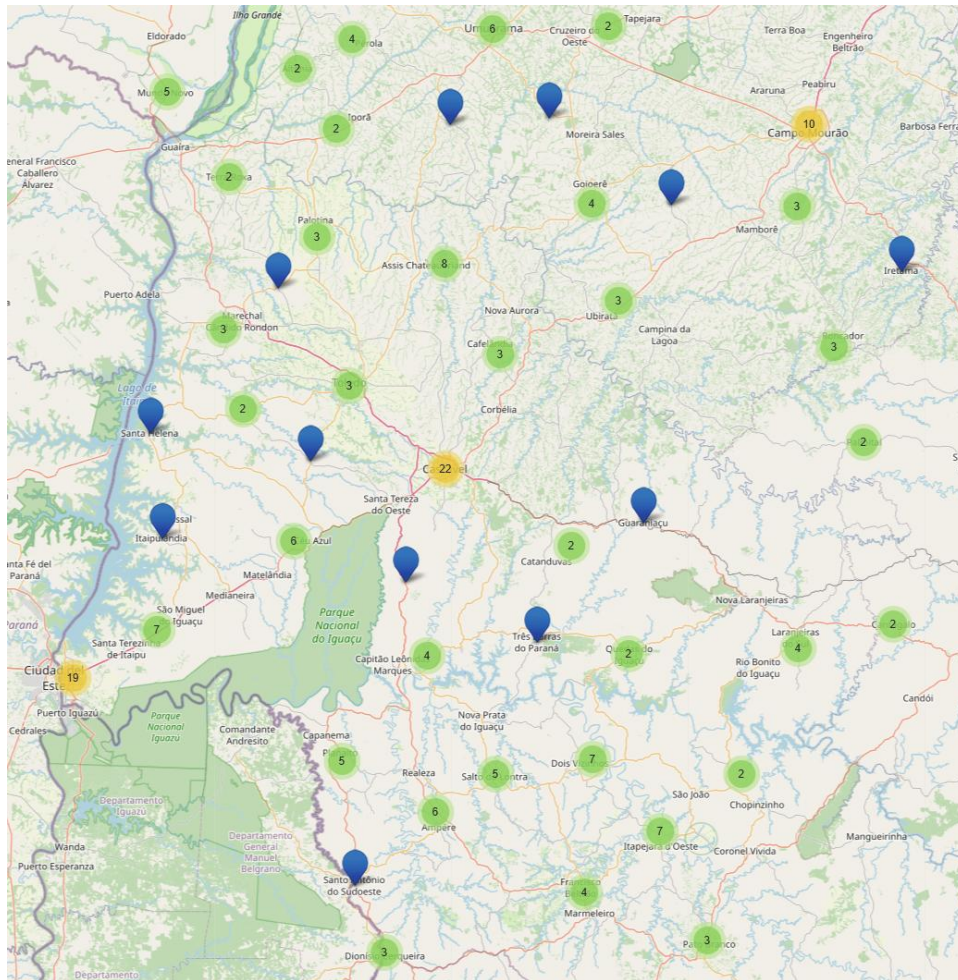


Brasil

- 9.070 AS
- 5.129 AS notificados
- 146.924 endereços IP mal configurados
- **NTP 58.954**
- **SNMP 42.711**
- **DNS 27.744**

Programa por uma Internet mais Segura

Notificação de amplificadores - serviços



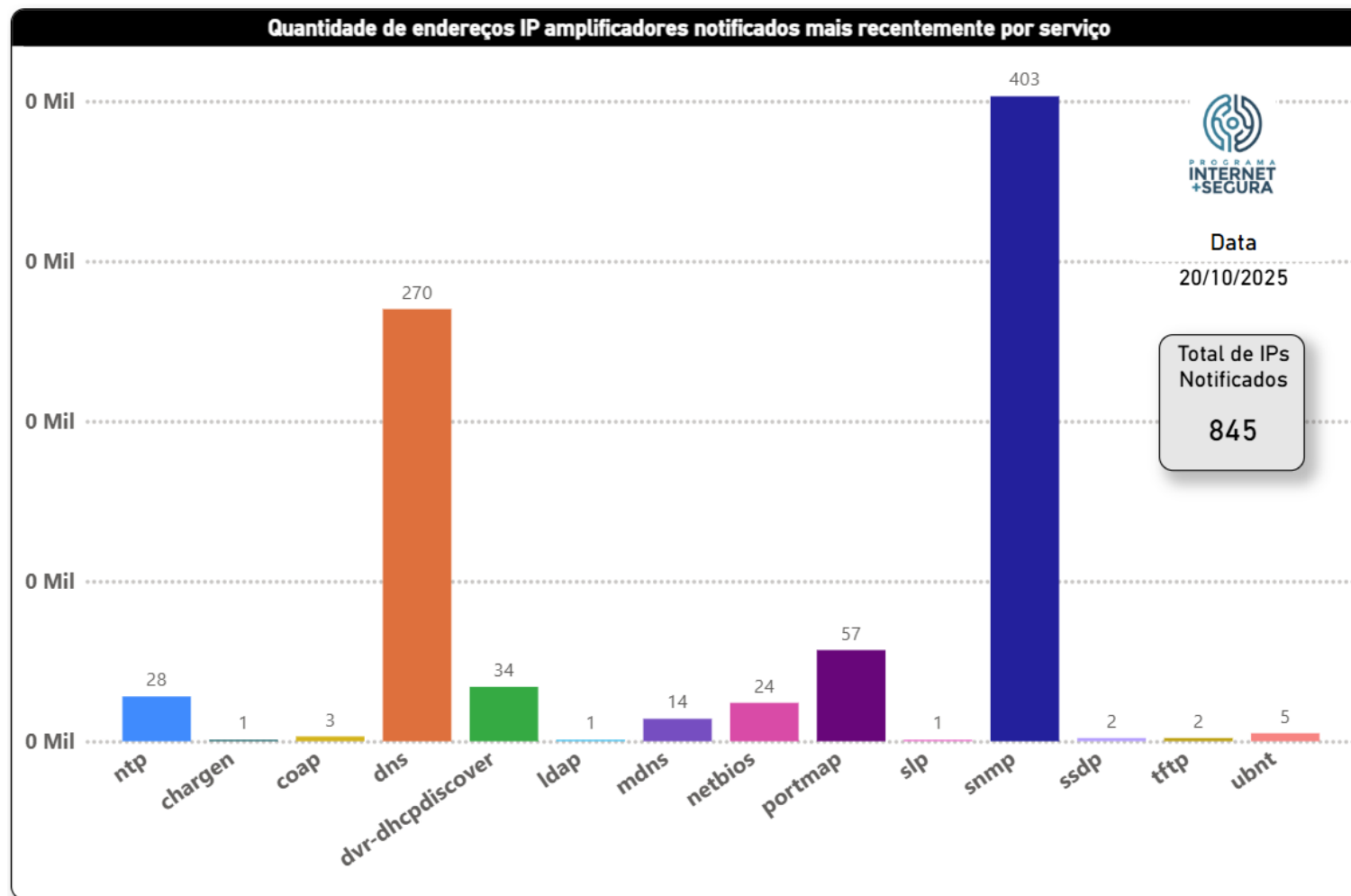
Cascavel 197 AS)

- Cascavel (21)
- Foz do Iguaçu (19)
- Campo Mourão (12)
- Assis Chateaubriand (5)
- Dois Vizinhos (5)
- Marechal Cândido Rondon (5)
- Umuarama (5)
- Ampére (4)
- Francisco Beltrão (4)
- Itapejara d'Oeste (4)
- Planalto (4)
- São Miguel do Iguaçu (4)
- Barracão (3)
- Laranjeiras do Sul (3)
- Mundo Novo (3)
- Palotina (3)
- Pato Branco (3)

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

Programa por uma Internet mais Segura

Notificação de amplificadores - serviços



Cascavel (raio 150 km)

- 197 AS
- 44 AS conectados ao IX
- 121 AS notificados
- 1 AS com mais de 130 IP notificados
- 845 endereços IP mal configurados
 - DNS 270
 - SNMP 403
 - Portmap 57



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/>

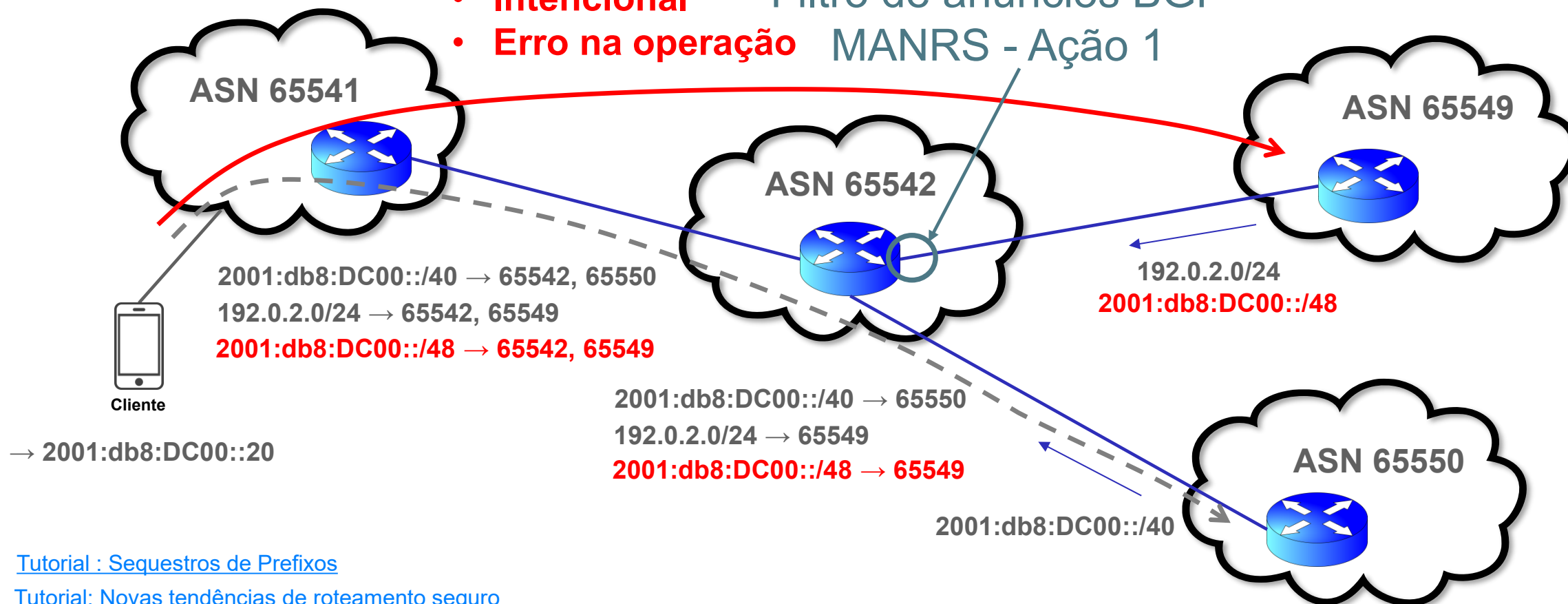


Programa por uma Internet mais Segura

Sequestro de prefixos (Hijacking)

Anúncio de prefixos não autorizados:

- Intencional Filtro de anúncios BGP
- Erro na operação MANRS - Ação 1



[Tutorial : Sequestros de Prefixos](#)

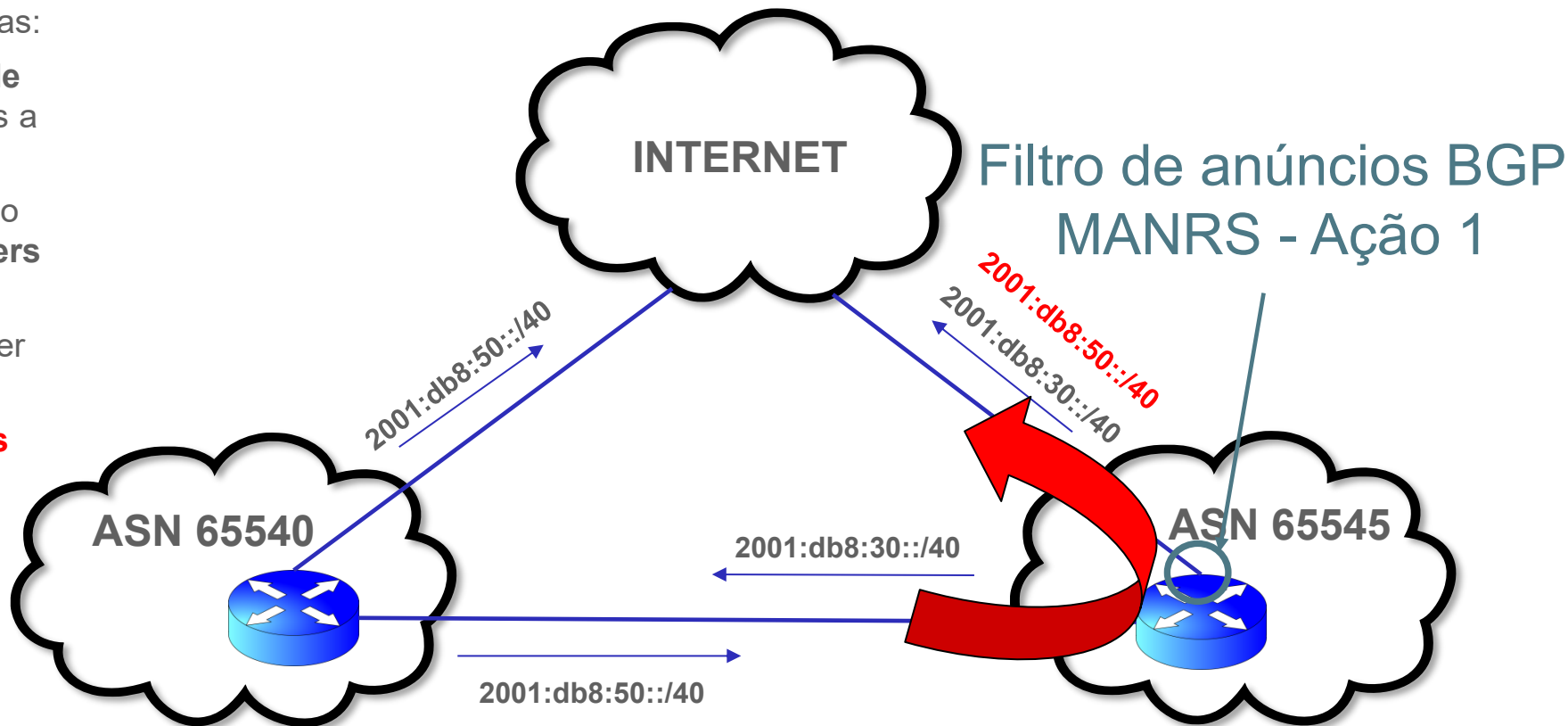
[Tutorial: Novas tendências de roteamento seguro](#)

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



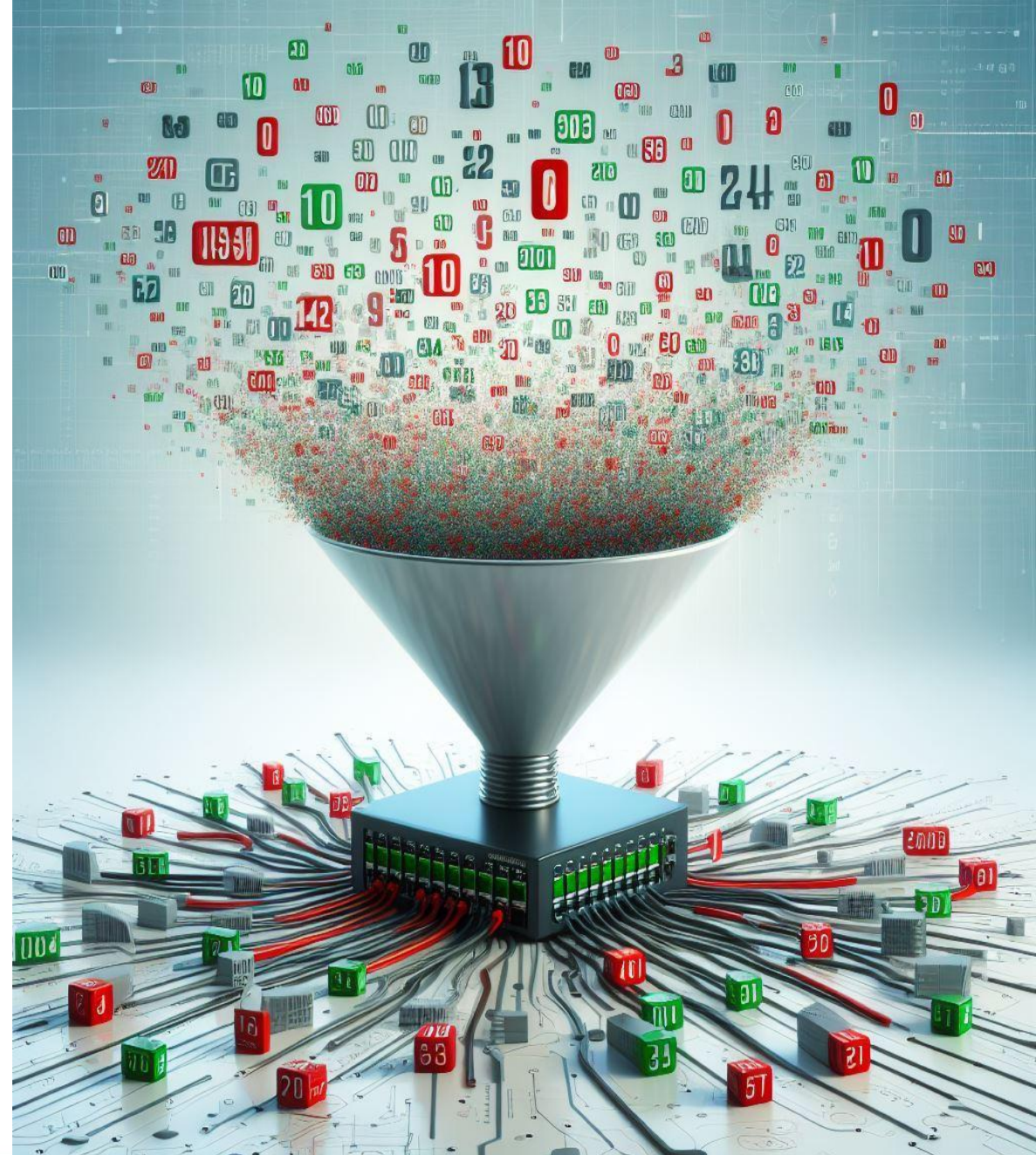
Programa por uma Internet mais Segura



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

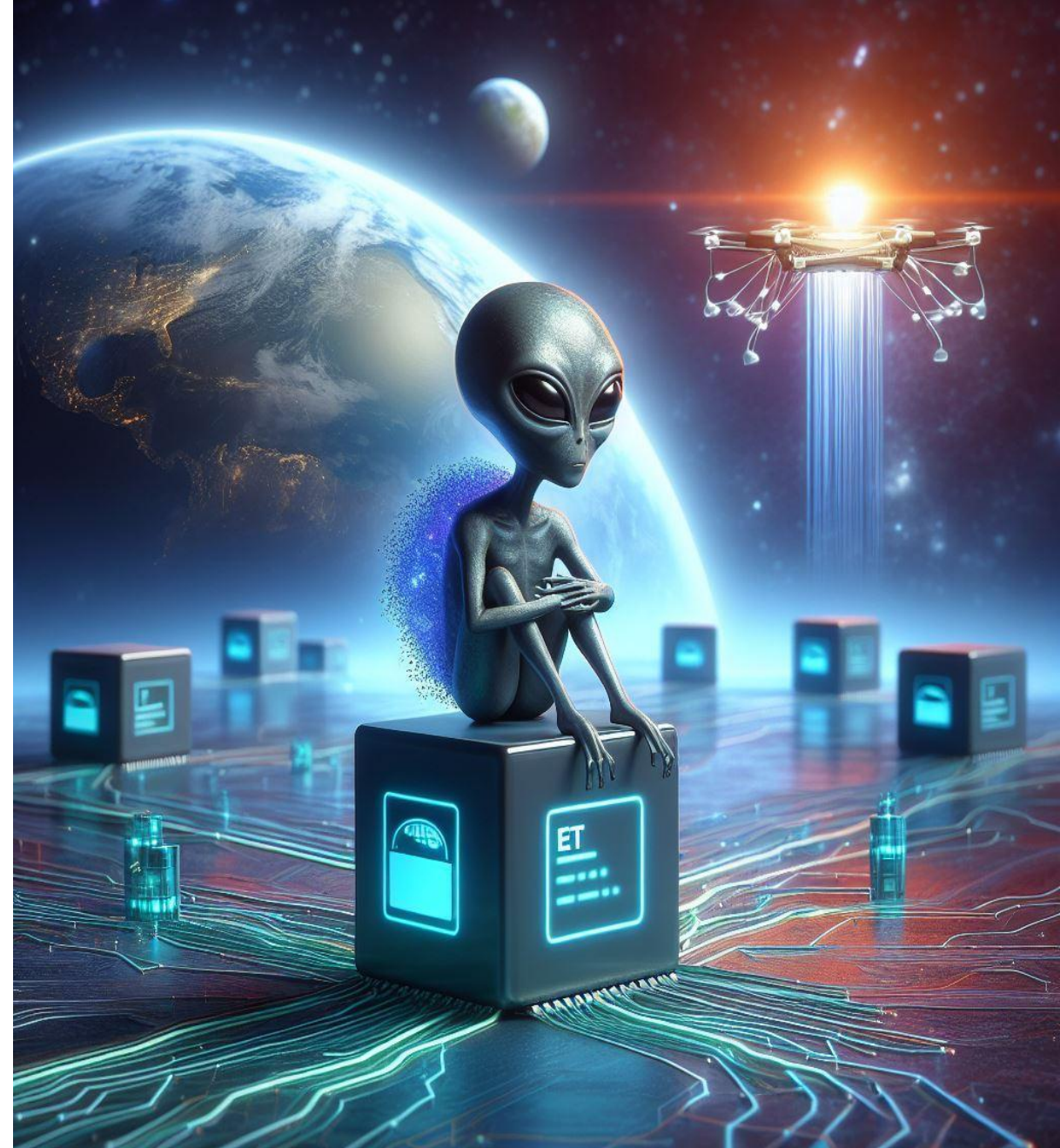


MANRS - Ação 2 - Filtro Anti-spoofing

- 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**



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)

Desafio BCOP

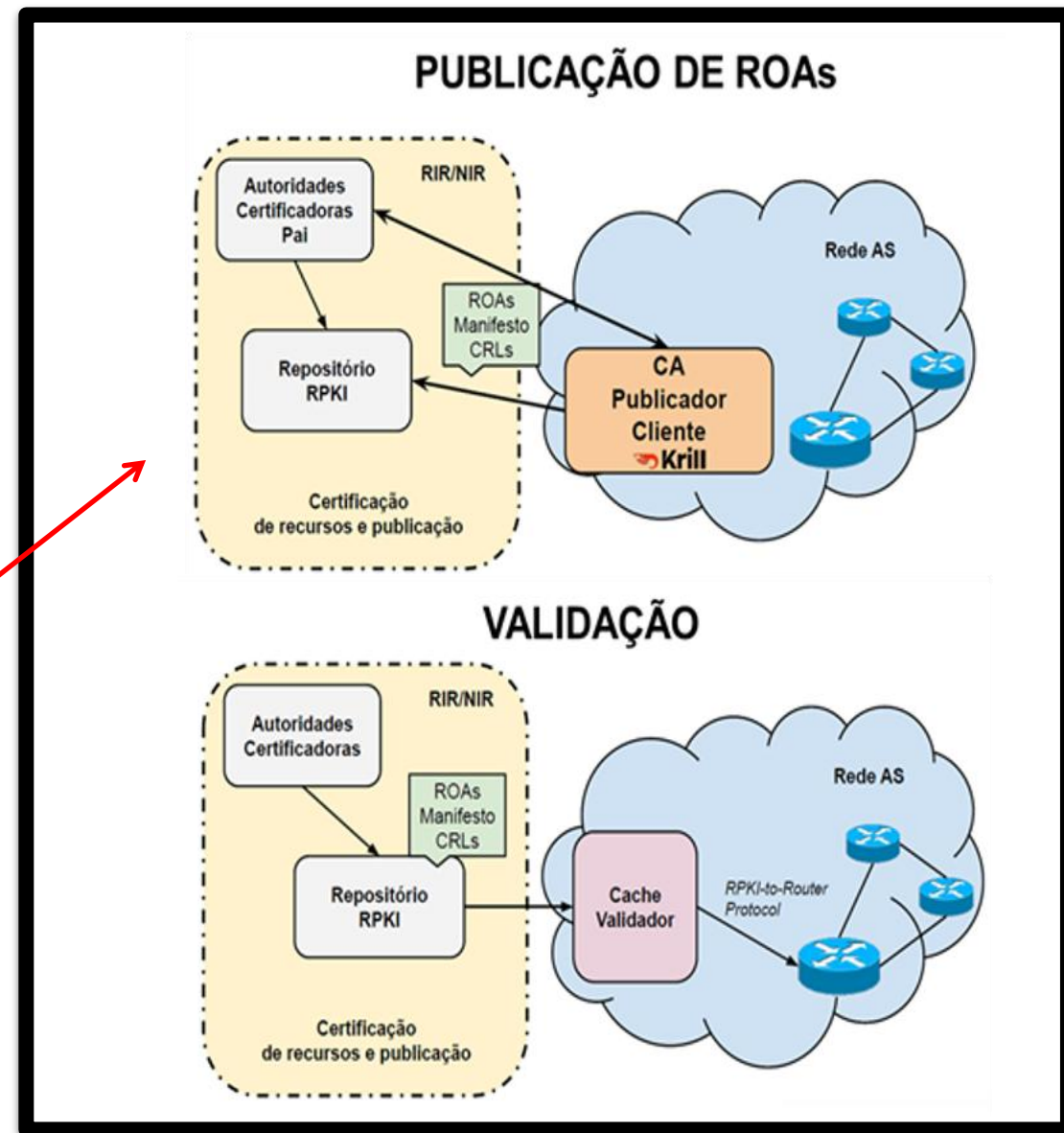
- RPKI - Resource Public Key Infrastructure

<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 - Cascavel - 150 Km - 192 AS



MANRS

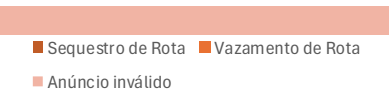
Resumo

31-out-25

MANRS - Status da Segurança de Roteamento

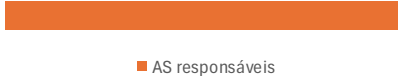
Incidentes

Sequestro de Rota	0
Vazamento de Rota	0
Anúncio inválido	1
Total	1



Responsáveis

AS responsáveis	1
-----------------	---



Informação de Roteamento

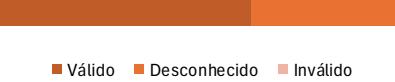
IRR

Não registrado	19	1,1%
Registrado	1.746	98,9%



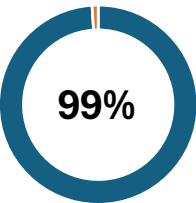
RPKI

Válido	1.121	63,5%
Desconhecido	644	36,5%
Inválido	0	0,0%

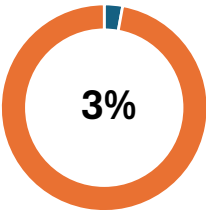


MANRS - Prontidão

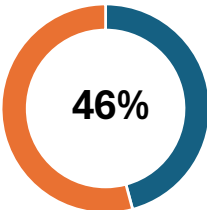
Filtros BGP



Anti-spoofing

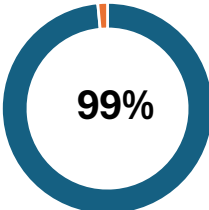


Coordenação

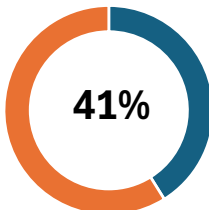


Informação de Roteamento

IRR



RPKI



Programa por uma Internet mais Segura

MANRS Observatory - 192 AS – Cascavel



ASN	Holder	Country	UN Regions	UN Sub-Regions	RIR Regions	Filtering	Anti-spoofing	Coordination	Routing Information	Routing Information	Participante MANRS	Status abuse
ASN 20	---	BR	Americas	Latin America and the Caribbean	LACNIC	100%	0%	100%	80%	0%		PEND
ASN 38	---	BR	Americas	Latin America and the Caribbean	LACNIC	100%	0%	0%	100%	0%		PEND
ASN 55	---	BR	Americas	Latin America and the Caribbean	LACNIC	100%	0%	0%	100%	0%		PEND
ASN 61	---	BR	Americas	Latin America and the Caribbean	LACNIC	0.87	100%	100%	100%	100%		PEND
ASN 68	---	BR	Americas	Latin America and the Caribbean	LACNIC	100%	0%	0%	100%	0%		PEND
ASN 72	---	BR	Americas	Latin America and the Caribbean	LACNIC	100%	0%	100%	100%	100%		PEND
ASN 94	---	BR	Americas	Latin America and the Caribbean	LACNIC	100%	0%	0%	100%	0%		PEND
ASN 113	---	BR	Americas	Latin America and the Caribbean	LACNIC	100%	0%	100%	100%	0%		PEND
ASN 127	---	BR	Americas	Latin America and the Caribbean	LACNIC	100%	0%	100%	100%	0%		PEND
ASN 132	---	BR	Americas	Latin America and the Caribbean	LACNIC	100%	0%	0%	100%	100%		PEND
ASN 133	---	BR	Americas	Latin America and the Caribbean	LACNIC	100%	0%	100%	100%	0%		PEND
ASN 146	---	BR	Americas	Latin America and the Caribbean	LACNIC	100%	0%	0%	100%	0%		PEND
ASN 153	---	BR	Americas	Latin America and the Caribbean	LACNIC	100%	0%	0%	100%	0%		PEND
ASN 157	---	BR	Americas	Latin America and the Caribbean	LACNIC	100%	0%	100%	100%	100%	269347	PEND
ASN 160	---	BR	Americas	Latin America and the Caribbean	LACNIC	100%	0%	0%	100%	0%		PEND
ASN 172	---	BR	Americas	Latin America and the Caribbean	LACNIC	100%	0%	0%	100%	0%		PEND
ASN 178	---	BR	Americas	Latin America and the Caribbean	LACNIC	100%	0%	100%	100%	0%		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

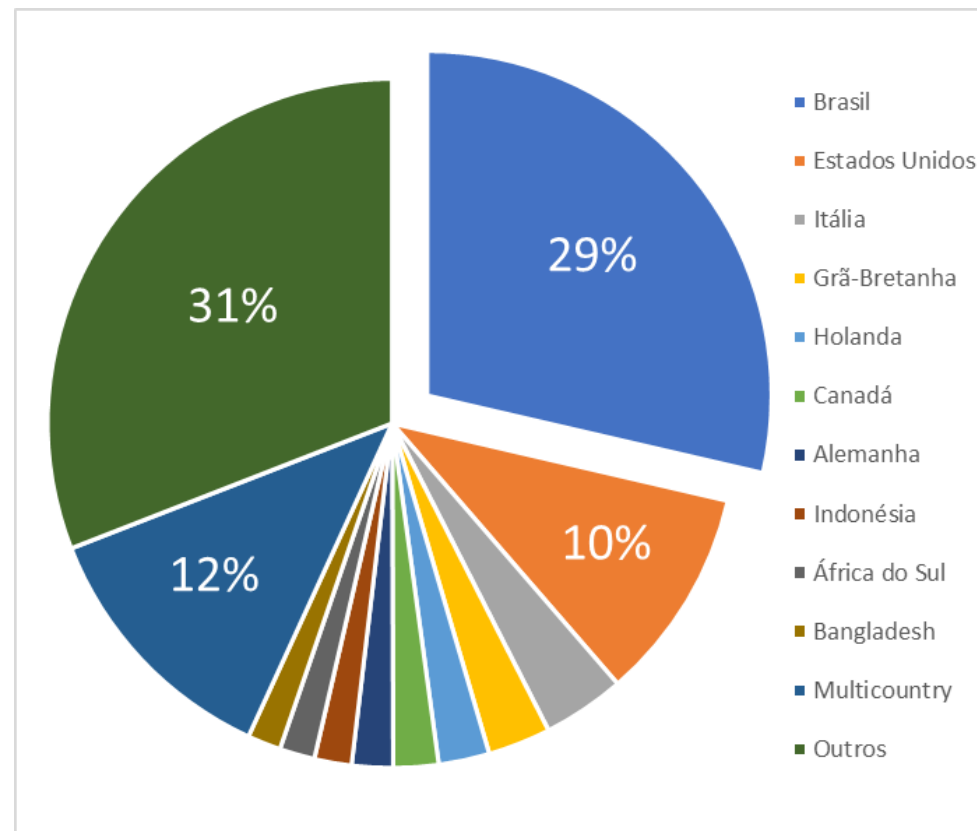
2023 → 258

2022 → 206

2021 → 174

2020 → 140

% de Participantes



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

Programa por uma Internet mais Segura

MANRS Observatory - 192 AS – Cascavel



ASN	Holder	Country	UN Regions	UN Sub-Regions	RIR Regions	Filtering	Anti-spoofing	Coordination	Routing Information	Routing Information	Participante MANRS	Status abuse
ASN 2	---	BR	Americas	Latin America and the Caribbean	LACNIC	100%	0%	100%	100%	100%	28130	OK
ASN 4	---	BR	Americas	Latin America and the Caribbean	LACNIC	100%	0%	100%	100%	100%	28145	OK
ASN 6	---	BR	Americas	Latin America and the Caribbean	LACNIC	100%	100%	100%	100%	100%	28223	OK
ASN 23	---	BR	Americas	Latin America and the Caribbean	LACNIC	100%	0%	100%	100%	100%	53049	OK
ASN 35	---	BR	Americas	Latin America and the Caribbean	LACNIC	100%	0%	100%	100%	0%	61895	OK
ASN 37	---	BR	Americas	Latin America and the Caribbean	LACNIC	100%	0%	100%	100%	43%	262328	OK
ASN 52	---	BR	Americas	Latin America and the Caribbean	LACNIC	100%	0%	100%	100%	100%	262657	OK
ASN 60	---	BR	Americas	Latin America and the Caribbean	LACNIC	100%	100%	100%	100%	0%	262968	OK
ASN 73	---	BR	Americas	Latin America and the Caribbean	LACNIC	100%	0%	100%	100%	100%	263495	OK
ASN 76	---	BR	Americas	Latin America and the Caribbean	LACNIC	100%	36%	100%	100%	100%	263616	OK
ASN 114	---	BR	Americas	Latin America and the Caribbean	LACNIC	100%	0%	100%	100%	0%	266287	OK
ASN 141	---	BR	Americas	Latin America and the Caribbean	LACNIC	100%	0%	100%	100%	0%	268352	OK
ASN 157	---	BR	Americas	Latin America and the Caribbean	LACNIC	100%	0%	100%	100%	100%	269347	PEND
ASN 179	---	BR	Americas	Latin America and the Caribbean	LACNIC	100%	0%	0%	100%	0%	271310	OK

14 AS as região são participantes do MANRS

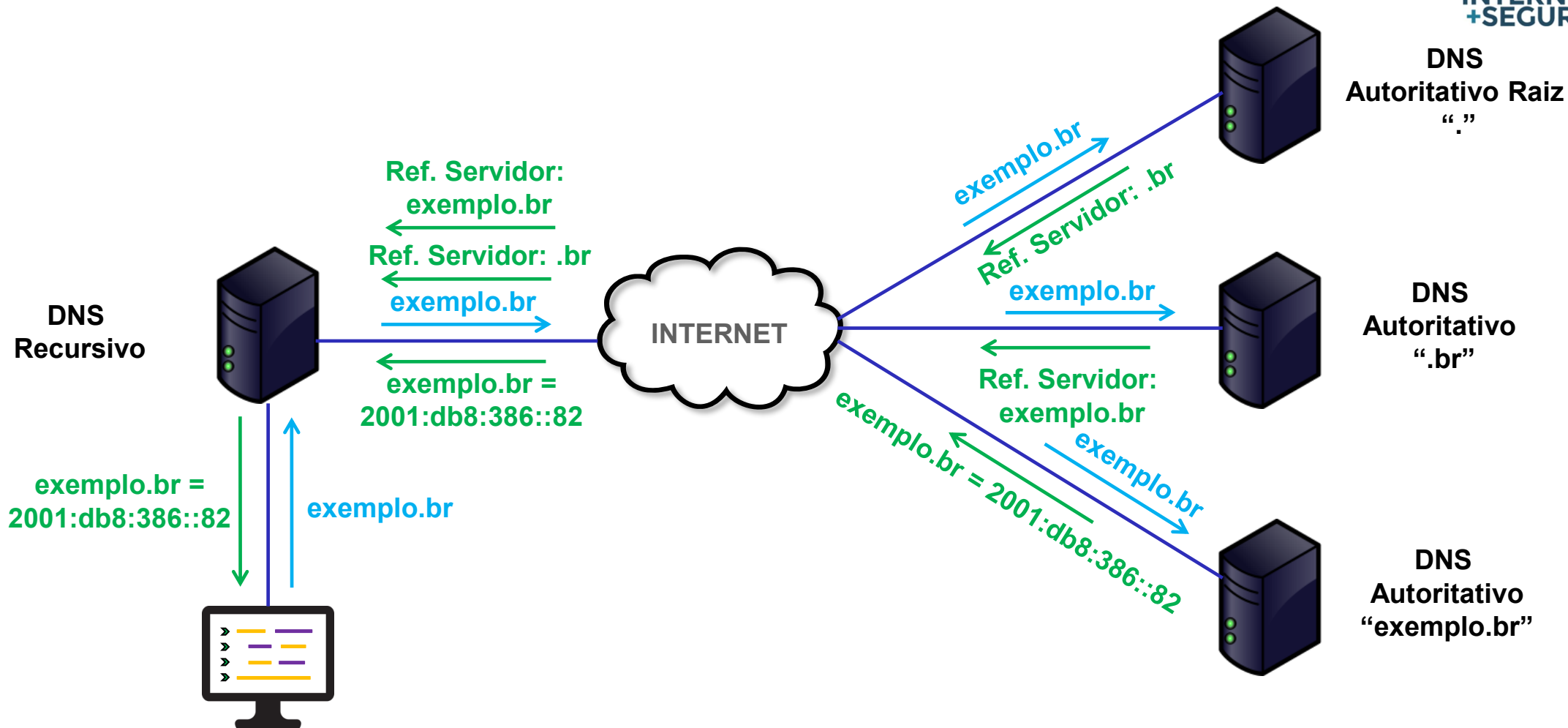


Stands for **K**nowledge-Sharing and
Intantiating **N**orms for **D**NS and **N**aming
Security

<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

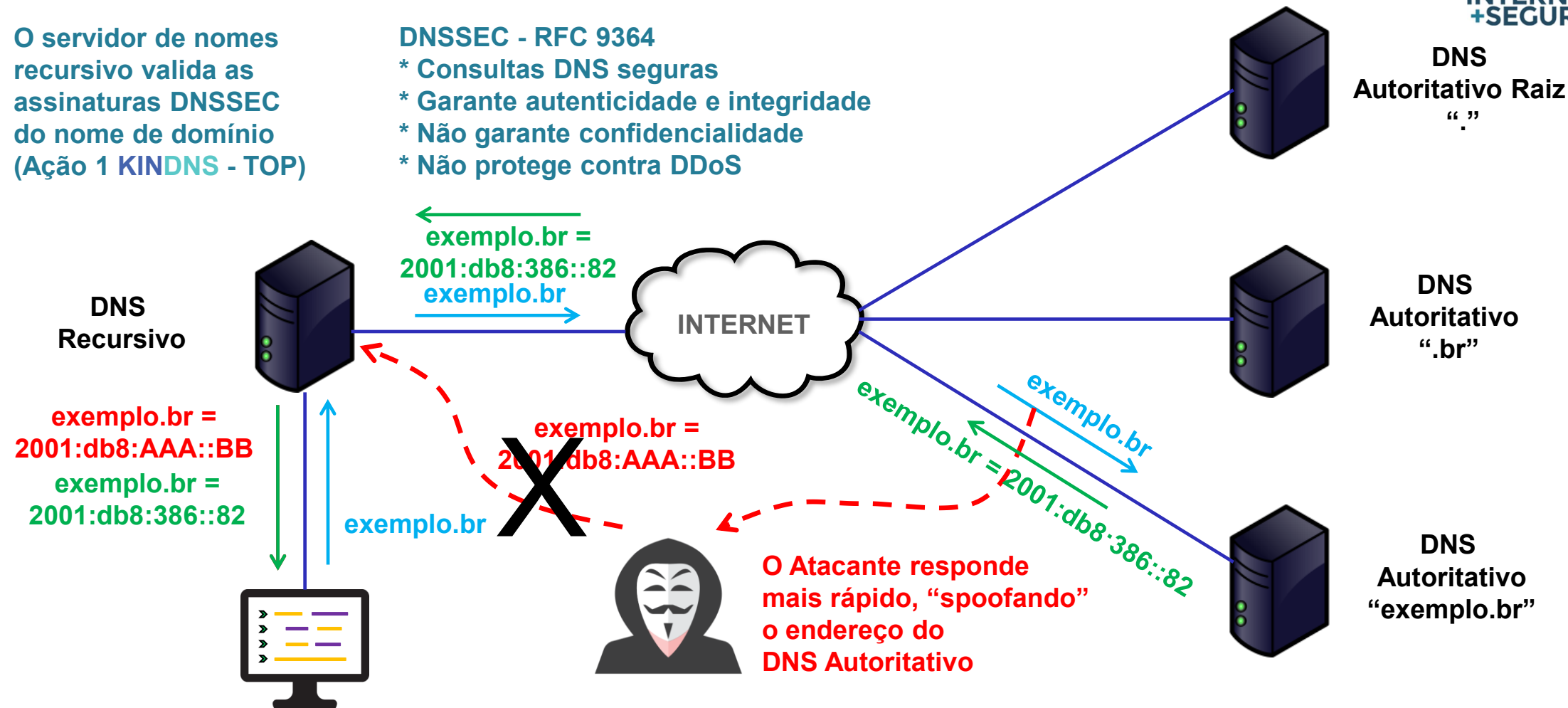
Ataque DNS - Poisoning



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>

The screenshot shows the TOP website with a header containing the logo and navigation links. The main content area features a introductory text and three test cards: 'Teste TOP - Site' (green), 'Teste TOP - E-mail' (blue), and 'Teste TOP - IPv6 e DNSSEC da sua rede' (purple). Each card includes a list of checks, a text input field with an example, and a button to start the test. The URL <https://top.nic.br> is displayed at the bottom.

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:

Iniciar o teste

Teste TOP - E-mail
Endereço IP moderno?
Domínio assinado? Proteção contra phishing? Conexão segura?

Nome de domínio do seu e-mail:

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

↖
Desafio BCOP

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



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](#)

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

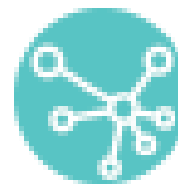
<https://top.nic.br>

Programa por uma Internet mais Segura

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>



The image is a promotional graphic for a podcast. It features a man, Gilberto Zorello, with grey hair, wearing a dark blue blazer over a light blue shirt, standing with his arms crossed. He is positioned in the center-right of the frame. The background is a stylized, isometric illustration in shades of blue and teal, depicting a network infrastructure with server racks, data flows, and people working. In the top left corner, the text 'CAMADA 8' is written in a large, white, sans-serif font, with '« nic.br »' in a smaller font below it. In the bottom right corner, the text 'INTERNET MAIS SEGURA' is written in a large, white, sans-serif font, with 'COM GILBERTO ZORELLO, COORDENADOR DE PROJETOS NO NIC.BR' in a smaller font below it. At the very bottom right, the logos 'nic.br' and 'cgi.br' are displayed in a green and white color scheme.

CAMADA 8
« nic.br »

INTERNET
MAIS SEGURA

COM GILBERTO ZORELLO,
COORDENADOR DE PROJETOS NO NIC.BR

nic.br cgi.br

Programa por uma Internet mais Segura

APOIO



A CONECTIVIDADE AO SEU ALCANCE



Obrigado

Gilberto Zorello

@ gzorello@nic.br



05 de novembro de 2025

nic.br **cgi.br**

www.nic.br | www.cgi.br