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

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

Gilberto Zorello | gzorello@nic.br

Abramulti Comics 2016 – Plenária NIC.br

Belo Horizonte, MG | 08/04/26

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
- 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

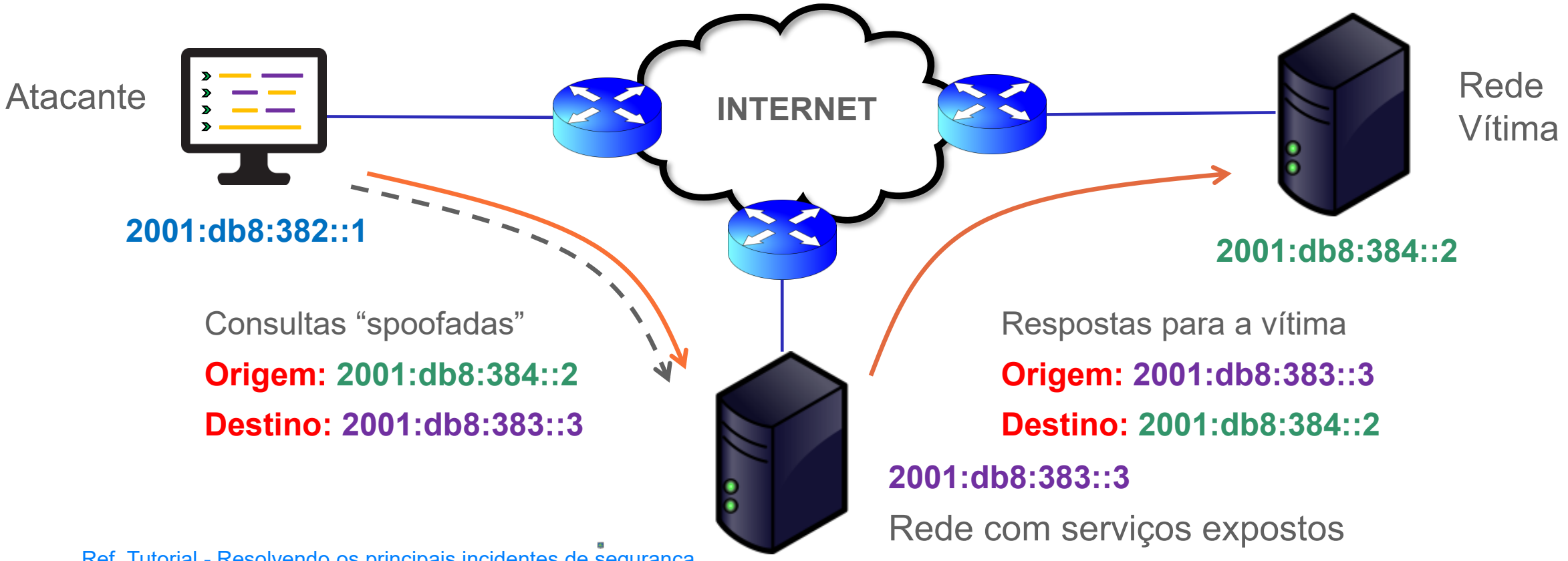
- Usados para amplificação em DDoS
- Portas UDP: DNS (53), SNMP (161), NTP (123), e várias outras!
- Notificações do CERT.br

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

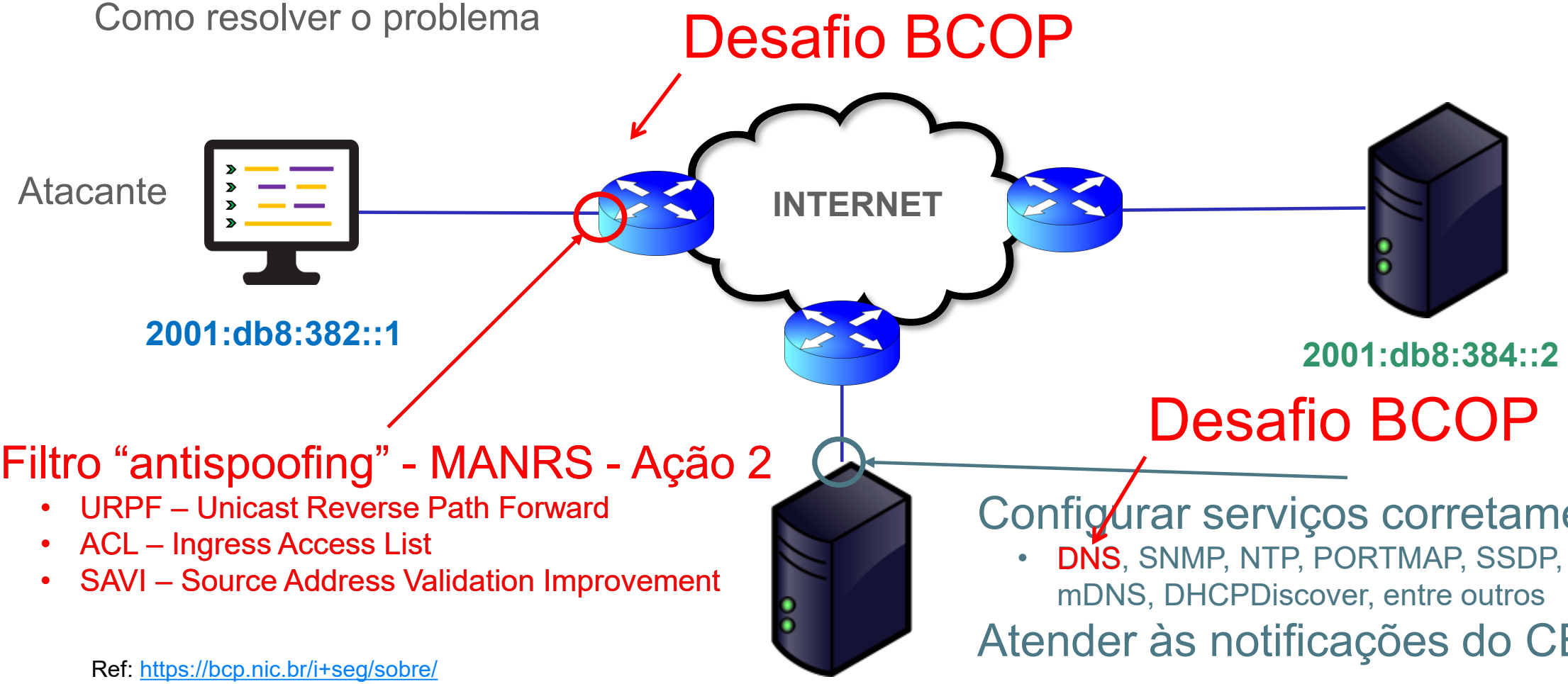


Ref. Tutorial - Resolvendo os principais incidentes de segurança

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

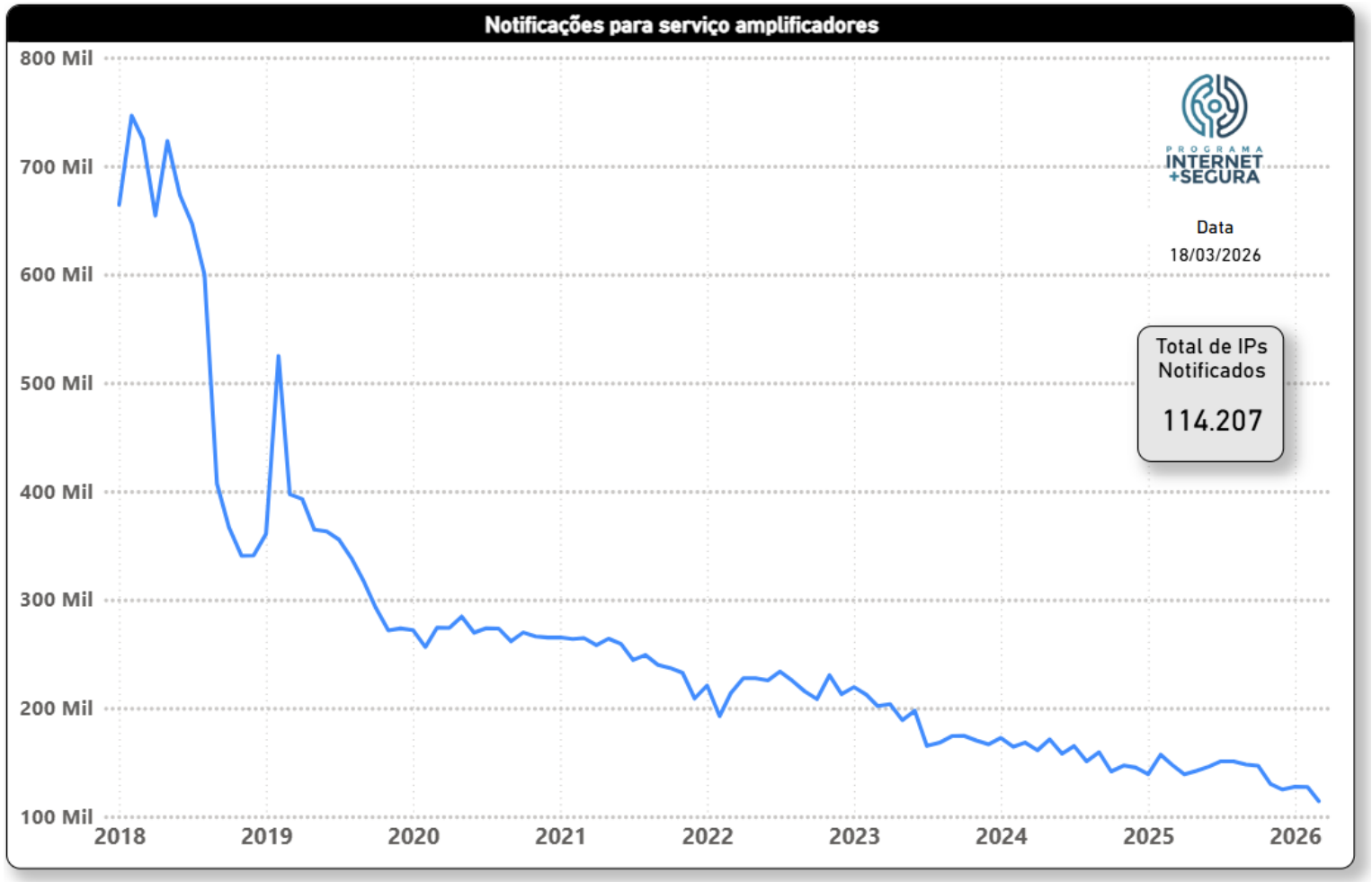
Configurar serviços corretamente

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

Atender às notificações do CERT.br

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

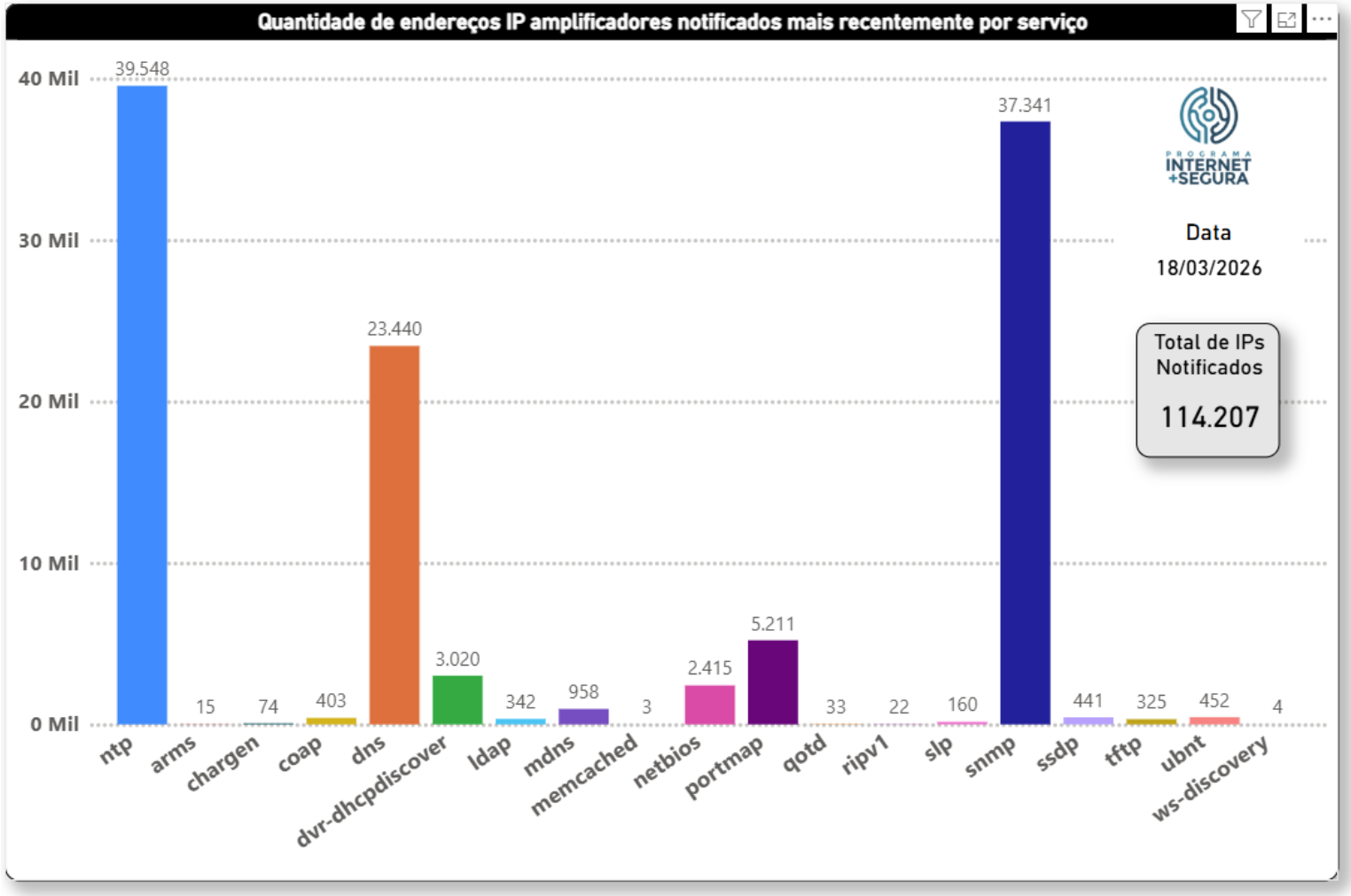
Programa por uma Internet mais Segura
Notificação de amplificadores - evolução



Brasil

- Início (fev/2018)
  - Endereços IP: 746.508
  - Serviços: 5
- Atual:
  - Endereços IP: 114.207
  - Serviços: 19
  - **Redução de 84%**
  - Ref. Mar/26

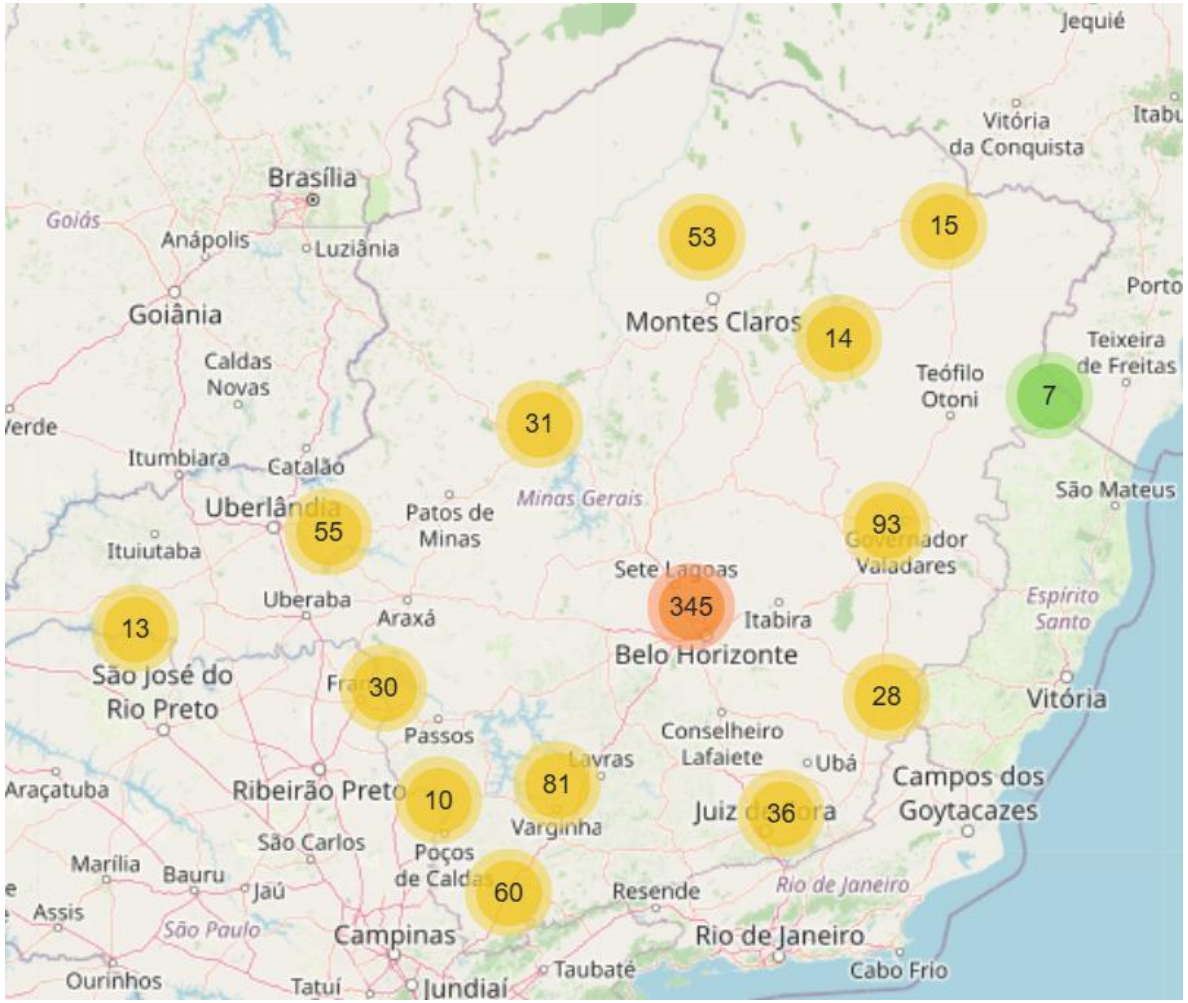
Programa por uma Internet mais Segura
Notificação de amplificadores - serviços



Brasil

- 9.112 AS
- 4.966 AS notificados
- 114.207 endereços IP mal configurados
  - NTP 39.548
  - SNMP 37.341
  - DNS 23.440
  - Ref: Mar/26

Programa por uma Internet mais Segura
Notificação de amplificadores - serviços

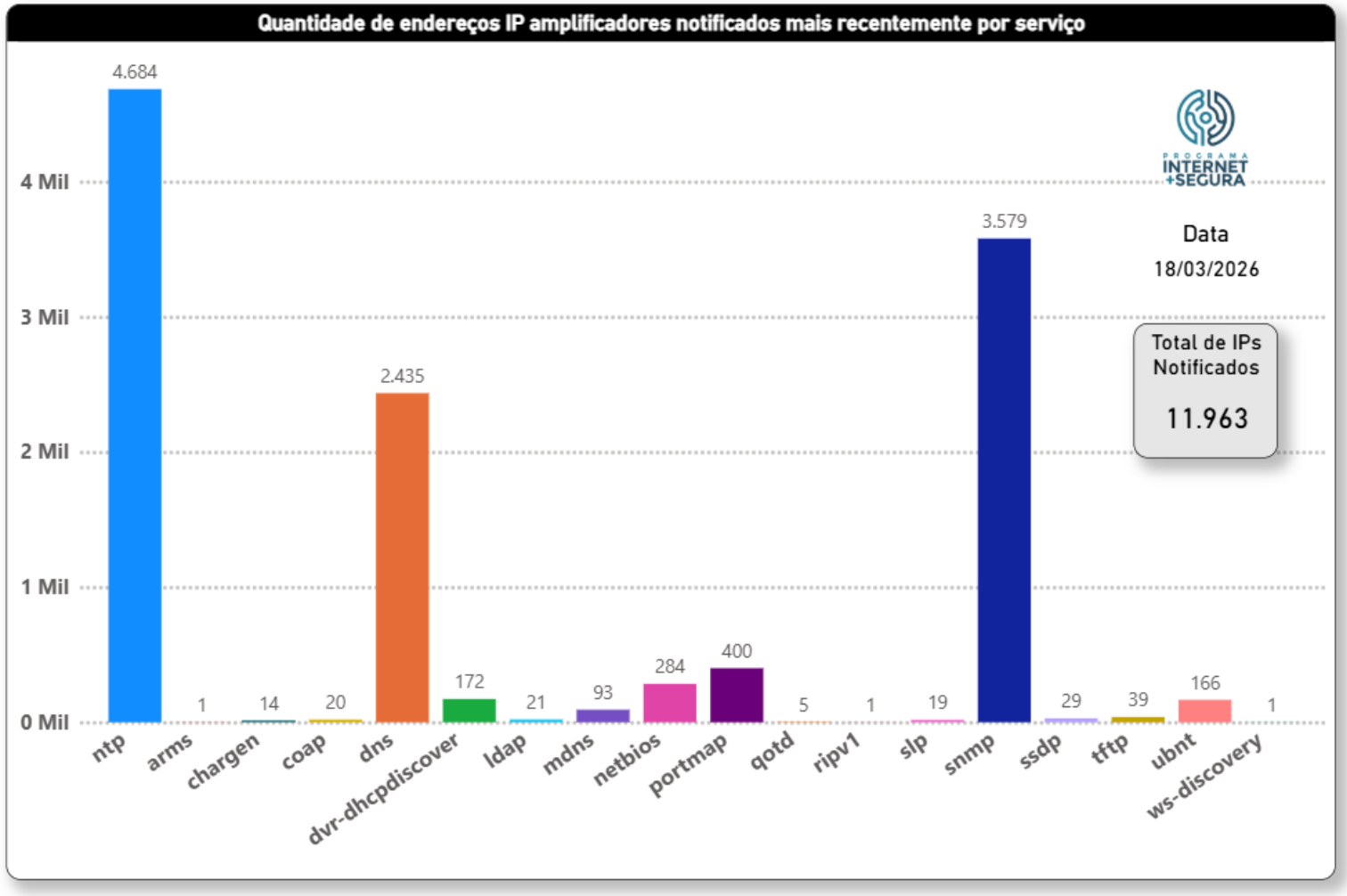


Estado de Minas Gerais (864 AS)

- Belo Horizonte (110)
- Montes Claros (21)
- Uberlândia (20)
- Betim (18)
- Contagem (18)
- Pouso Alegre (15)
- Governador Valadares (13)
- Juiz de Fora (10)
- Varginha (10)
- Ipatinga (9)
- Sete Lagoas (9)
- Divinópolis (8)
- Passos (8)
- Teófilo Otoni (8)
- Ibirité (7)
- Itaúna (7)
- Viçosa (7)

Ref. https://mapadeas.ceptro.br

Programa por uma Internet mais Segura
Notificação de amplificadores - serviços



Estado de Minas Gerais

- 864 AS
- 108 AS participantes do IX de Belo Horizonte
- 505 AS notificados
- 13 AS com mais de 100 IP notificados
- 11.963 endereços IP mal configurados
  - SNMP 3.579
  - DNS 2.435
  - NTP 4.684

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

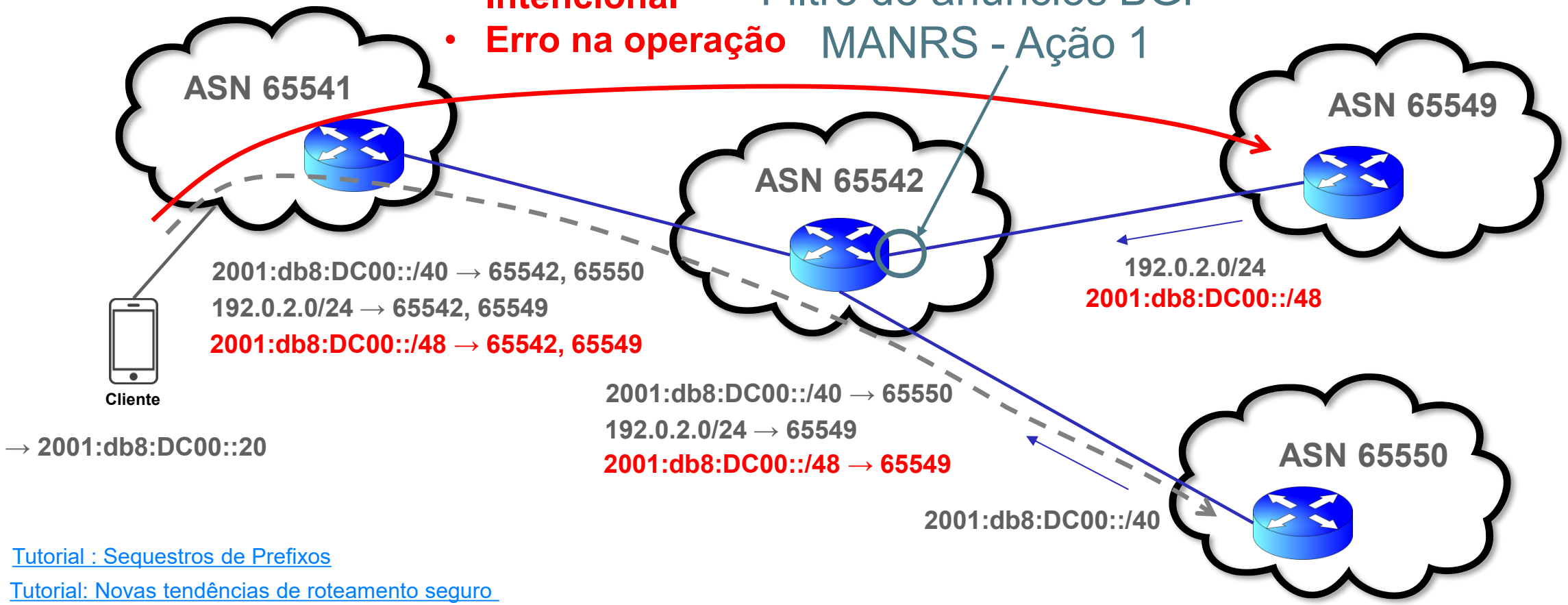
Sequestro de prefixos (Hijacking)

Anúncio de prefixos não autorizados:

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

Filtro de anúncios BGP

MANRS - Ação 1



Tutorial : Sequestros de Prefixos

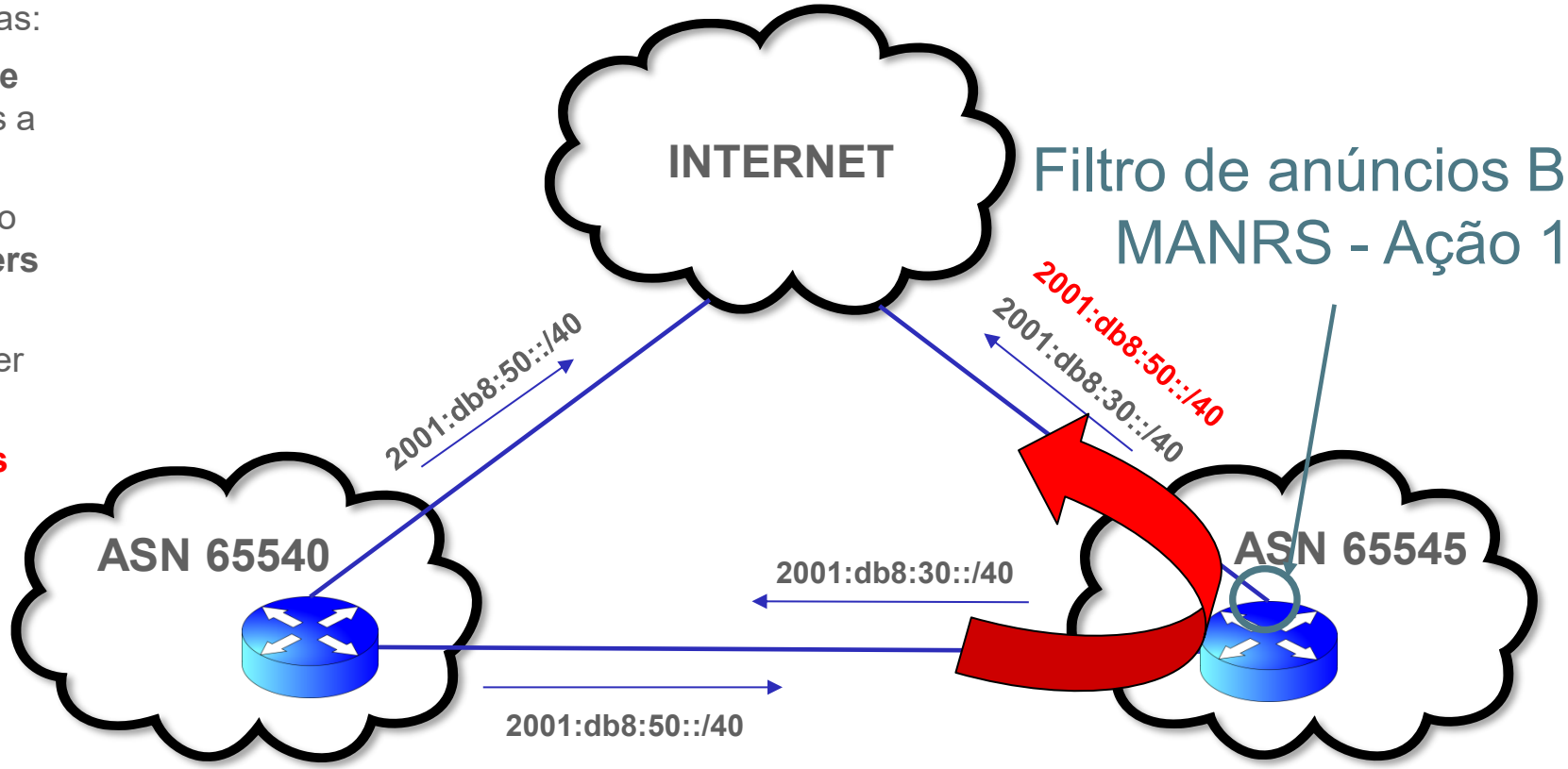
Tutorial: Novas tendências de roteamento seguro

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

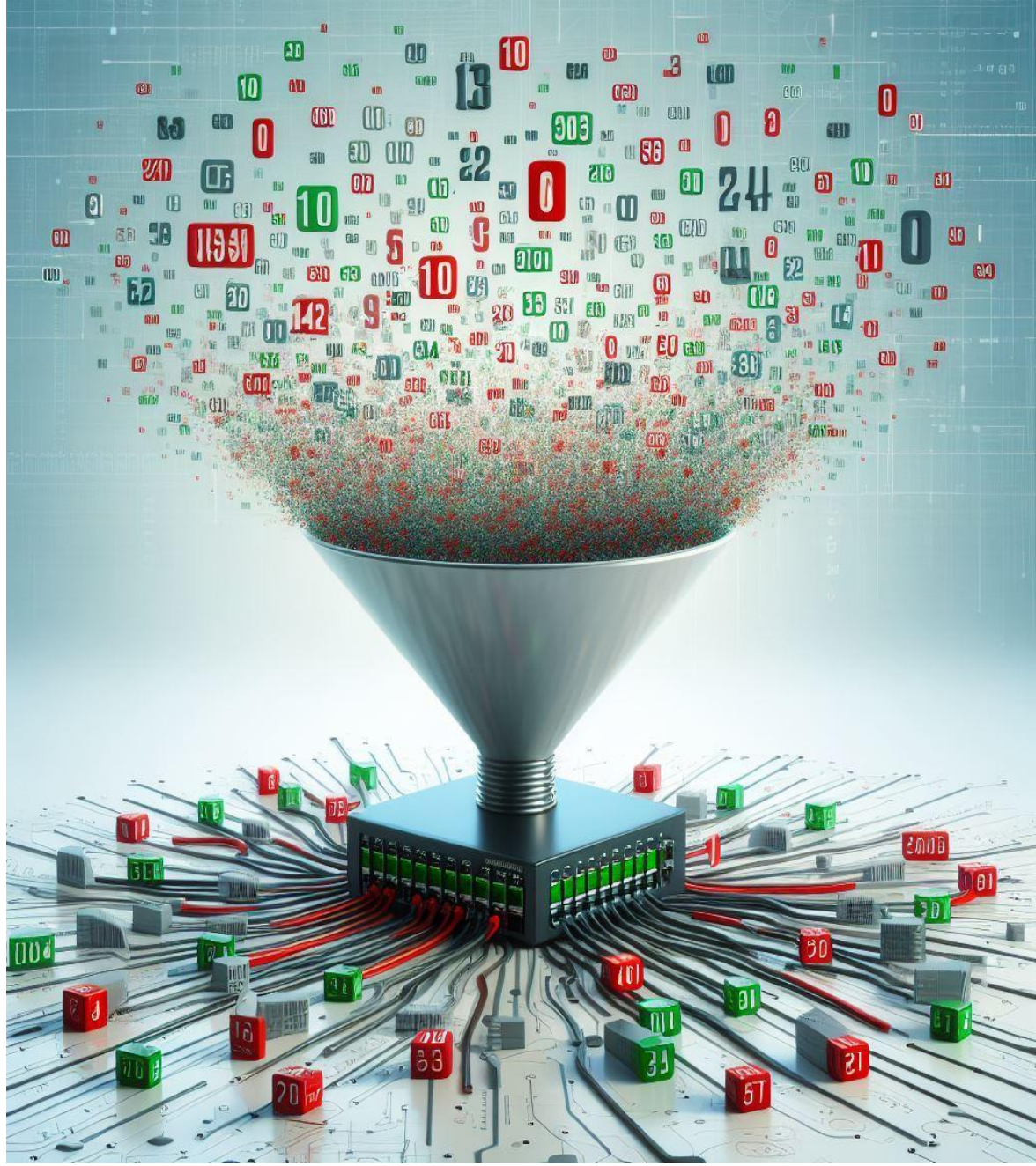
PROGRAMA INTERNET +SEGURA

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
Atenção em relação ao e-mail de abuse-c

Status	Qtd
AS em Minas Gerais	864
Status de **PENDÊNCIA** com o Registro.br	49
Status de **BLOQUEIO** com o Registro.br	21
Não recebe notificações do **CERT.br**	53

PENDÊNCIA: Não responde mensagens de **abuse-c** do Registro.br.
BLOQUEIO: Por não responder mensagens do Registro.br perde a gerência dos blocos IP e entra em processo de recuperação de blocos IP.

CERT.br recebe mensagem de erro ao encaminhar mensagens de notificação para o e-mail **abuse-c**

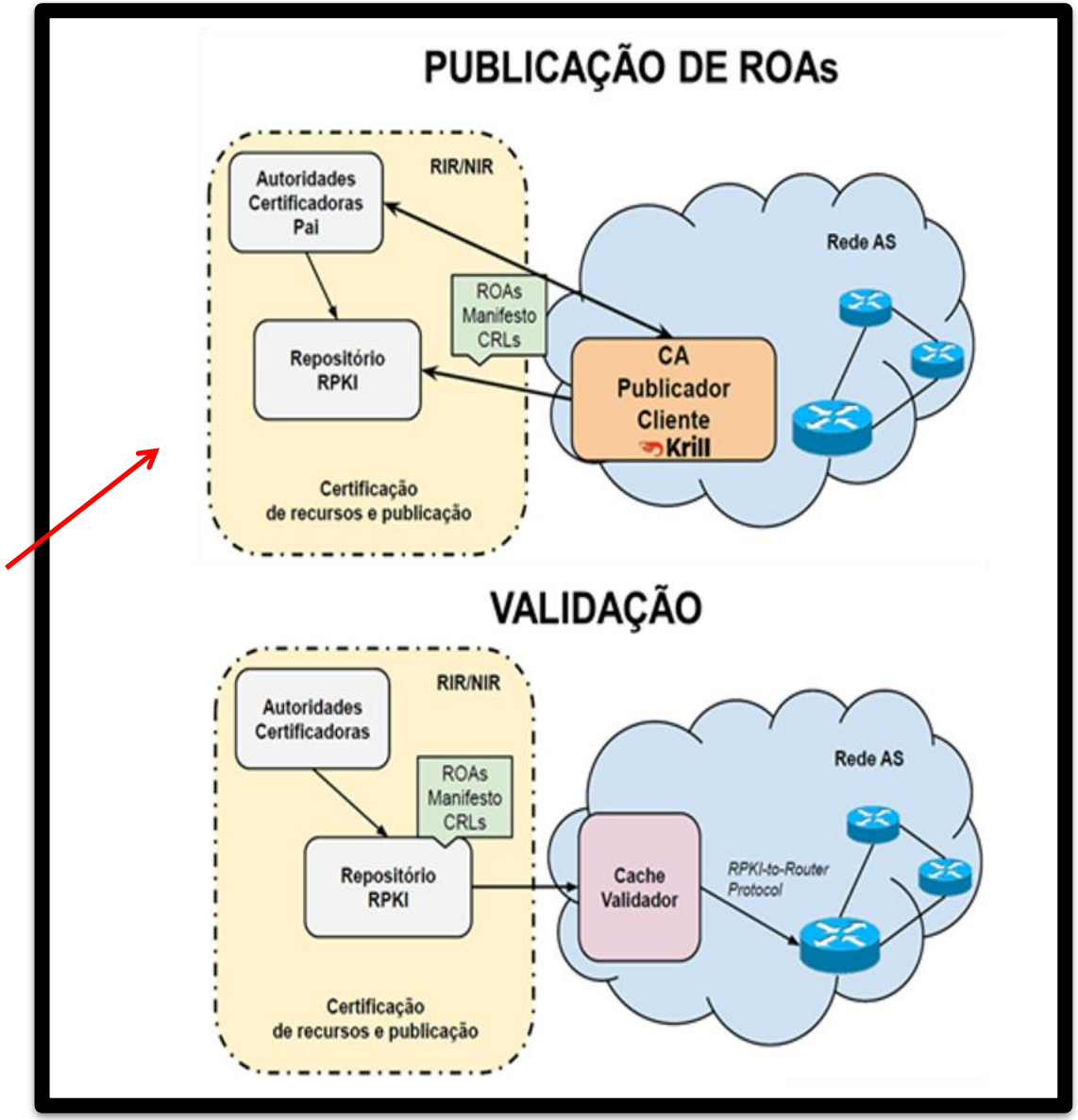
Programa por uma Internet mais Segura

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 - Minas Gerais - 828 AS

Resumo 31-mar-26

MANRS - Status da Segurança de Roteamento

Incidentes

Sequestro de Rota	1
Vazamento de Rota	0
Anúncio inválido	2
Total	3

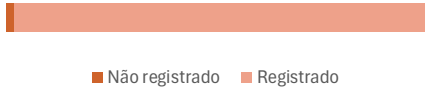
Responsáveis

AS responsáveis	3

Informação de Roteamento

IRR

Não registrado	170	**1,7%**
Registrado	9.966	**98,3%**

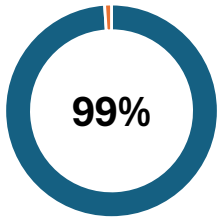


RPKI

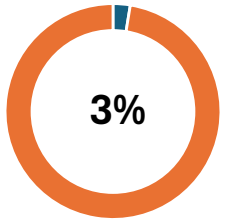
Válido	6.015	**59,3%**
Desconhecido	4.054	**40,0%**
Inválido	67	**0,7%**

MANRS - Prontidão

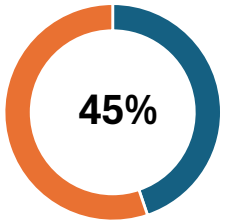
Filtros BGP



Anti-spoofing

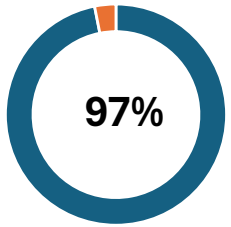


Coordenação

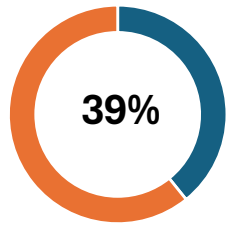


Informação de Roteamento

IRR



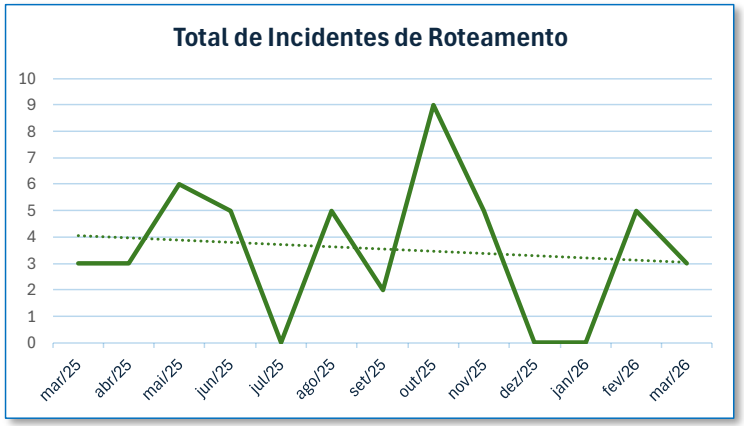
RPKI

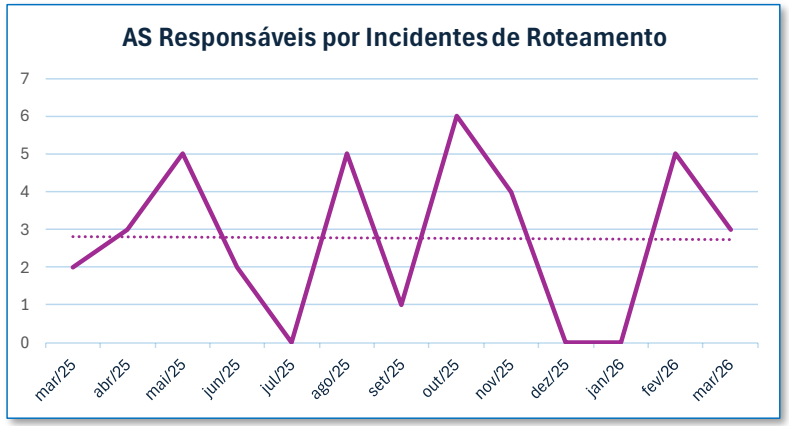


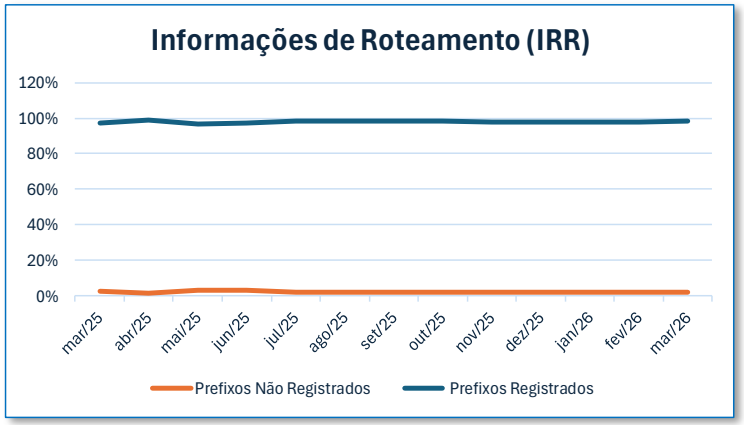
Fonte: https://observatory.manrs.org/ - acesso logado em 28/02/26

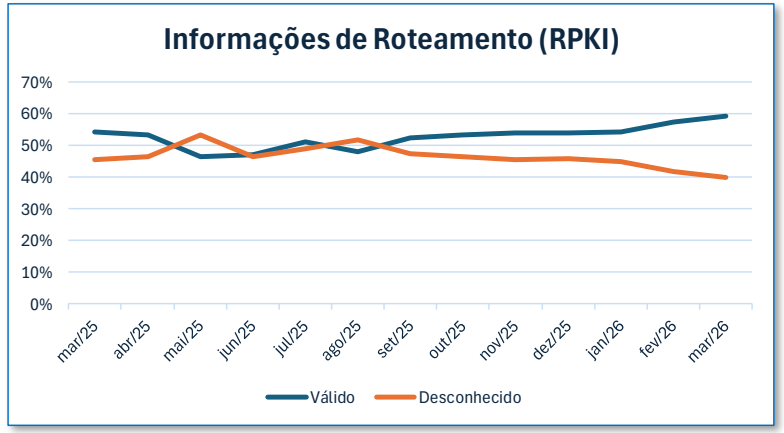
Programa por uma Internet mais Segura

MANRS Observatory Histórico - Minas Gerais 828 AS









Fonte: https://observatory.manrs.org/ - acesso logado em 31/03/26

Programa por uma Internet mais Segura

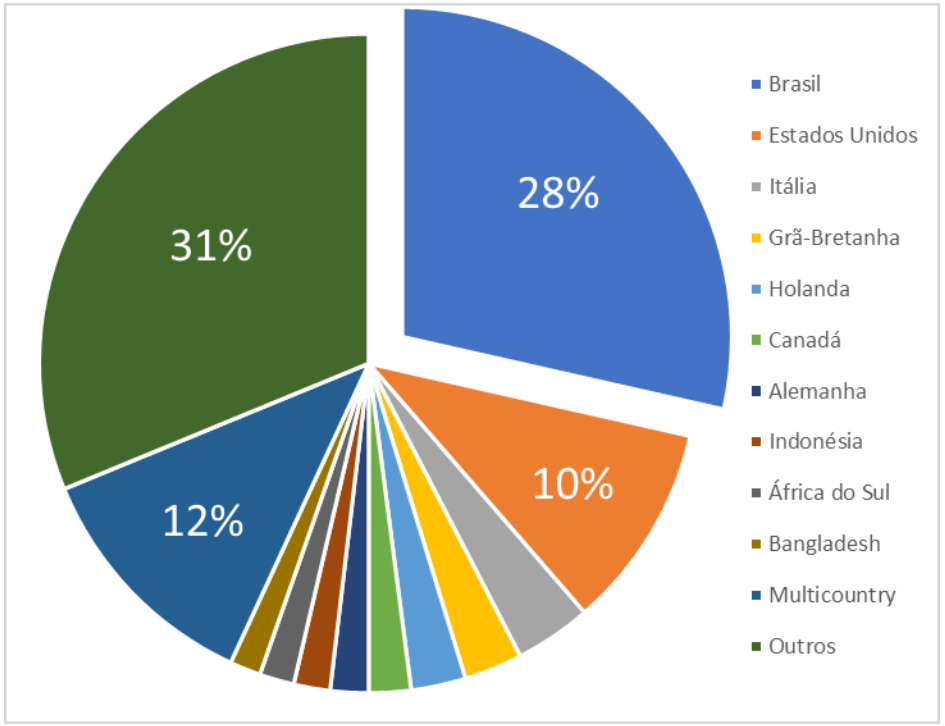
Participantes por país

- Total: 1.095
- Participantes no Brasil → 319

MANRS

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

Participantes em Minas Gerais: 22



Fonte: https://www.manrs.org/netops/participants/ Acesso 25/02/26

PROGRAMA INTERNET +SEGURA

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

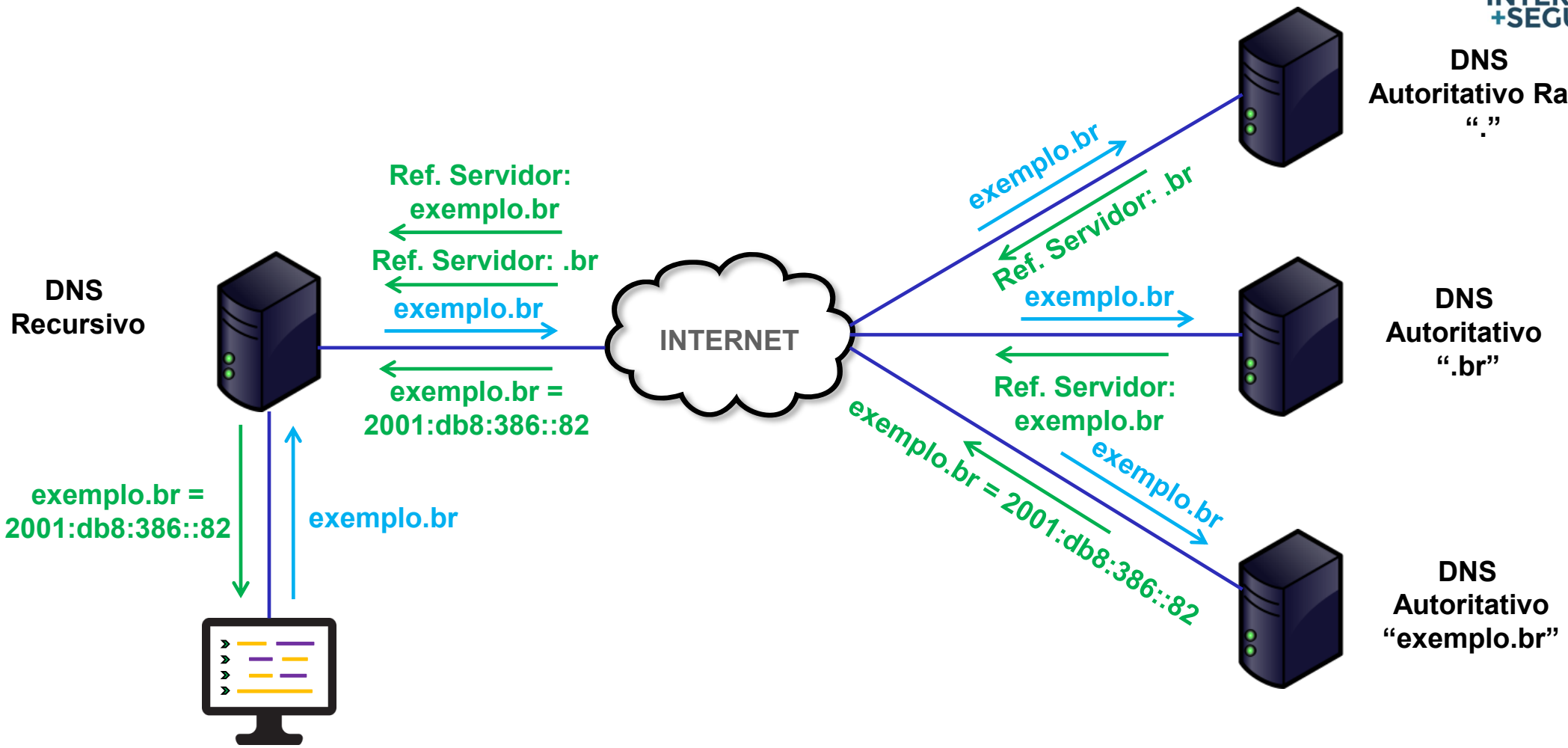
https://kindns.org/

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

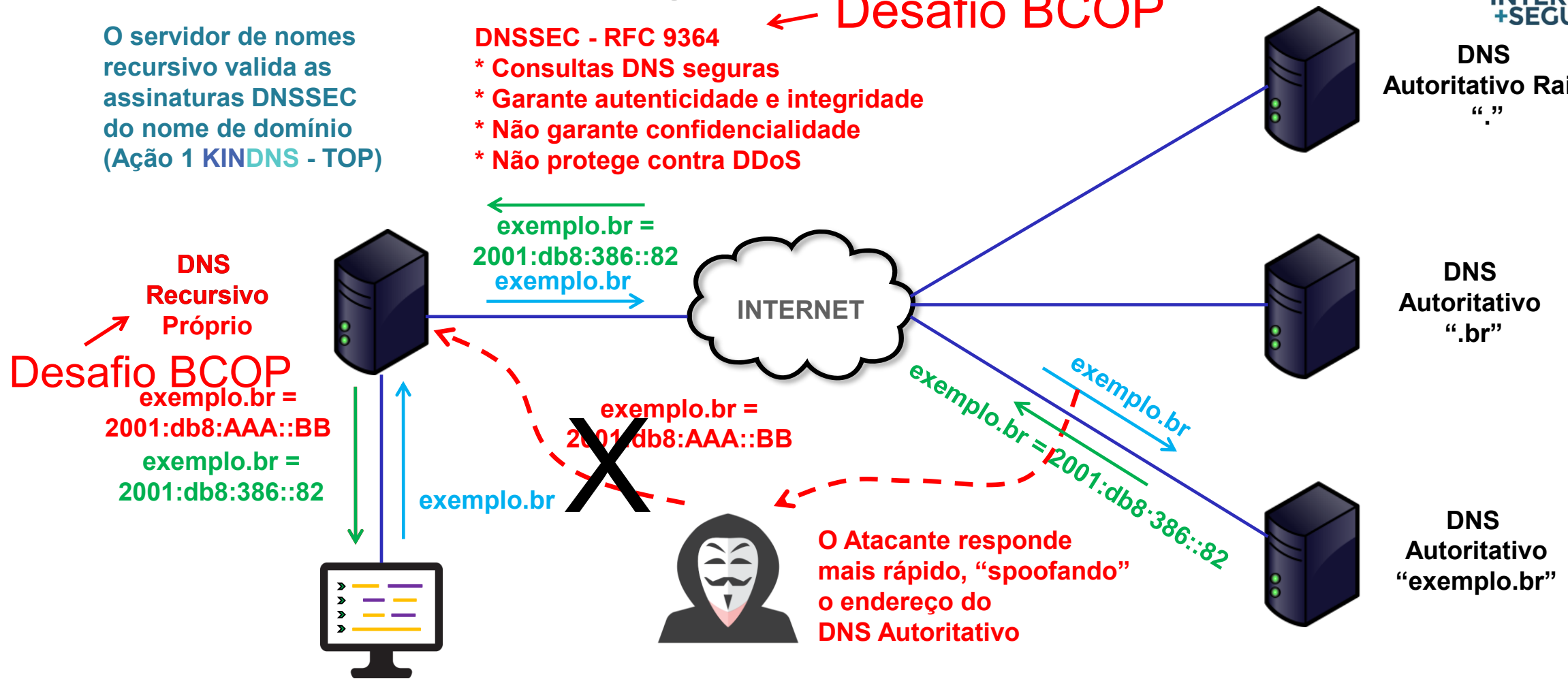
Ataque DNS - Poisoning

PROGRAMA INTERNET +SEGURA

O servidor de nomes recursivo valida as assinaturas DNSSEC do nome de domínio (Ação 1 KINDNS - TOP)

Desafio BCOP

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

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

https://top.nic.br

Programa por uma Internet mais Segura

Nota média de validação DNSSEC por recursivos – Minas Gerais

Nota Média de Validação de DNSSEC por AS por Ano					
Nota média por AS	2022	2023	2024	2025	2026
0% a 20%	10%	8%	3%	2%	4%
20% a 50%	22%	18%	17%	7%	14%
50% a 80%	19%	20%	11%	9%	10%
80% a 100%	49%	54%	69%	81%	72%

Total de Sistemas Autônomos que fizeram medições	333	383	398	413	232

Total de Sistemas Autônomos na Região em mar/26	**864**

Total de Sistemas Autônomos que já fizeram medições	**611**

Programa por uma Internet mais Segura
Implemente as melhores práticas - Selos

MANRS

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-DICOVERY	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%

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

08 de abril de 2026

nic.br cgi.br

www.nic.br | www.cgi.br