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

ABRINT Nordeste 2025

Fortaleza, CE | 27/11/25

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

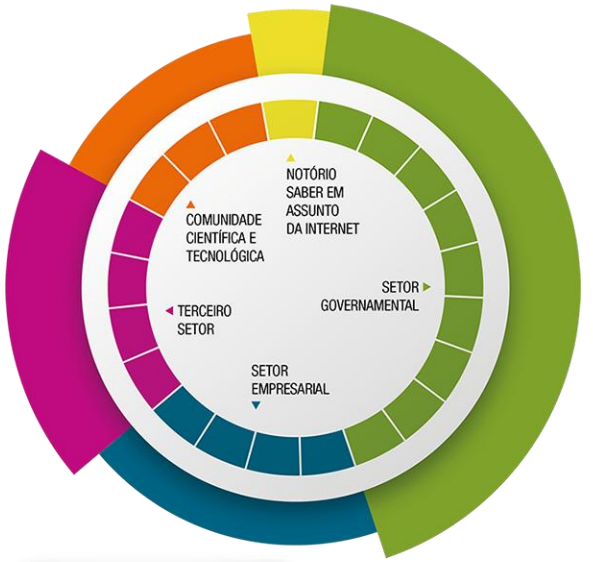
NIC.br e CGI.br

- 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://cgi.br/
https://nic.br/

NIC.br e CGI.br

cgi.br



nic.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	cert.br	cetic.br	ceptro.br	ceweb.br	ix.br	W3C CHAPTER São Paulo
Domínios	Segurança	Indicadores	Redes e Operações	Tecnologias Web	Troca de Tráfego	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

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

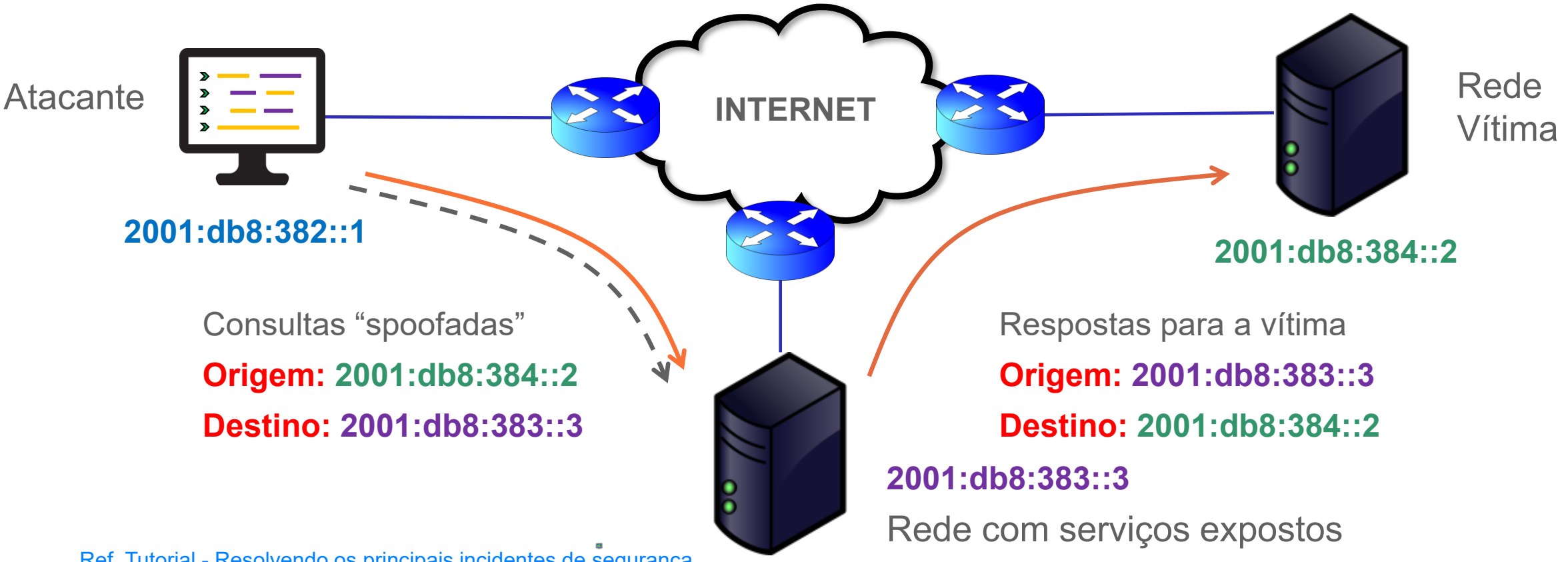
- Usados para amplificação em DDoS
- Portas UDP: DNS (53), SNMP (161), NTP (123), e várias outras!
- Notificações do CERT.br

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

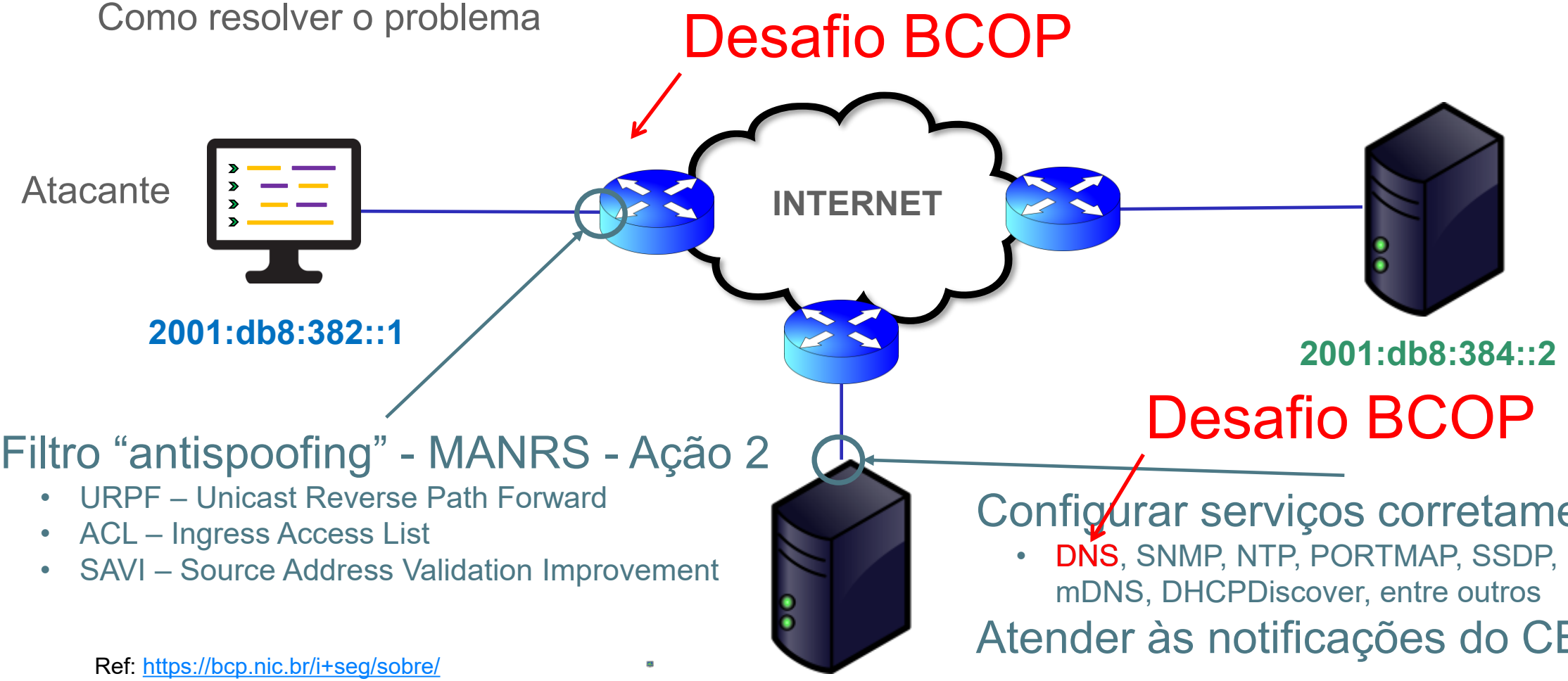


Ref. Tutorial - Resolvendo os principais incidentes de segurança

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

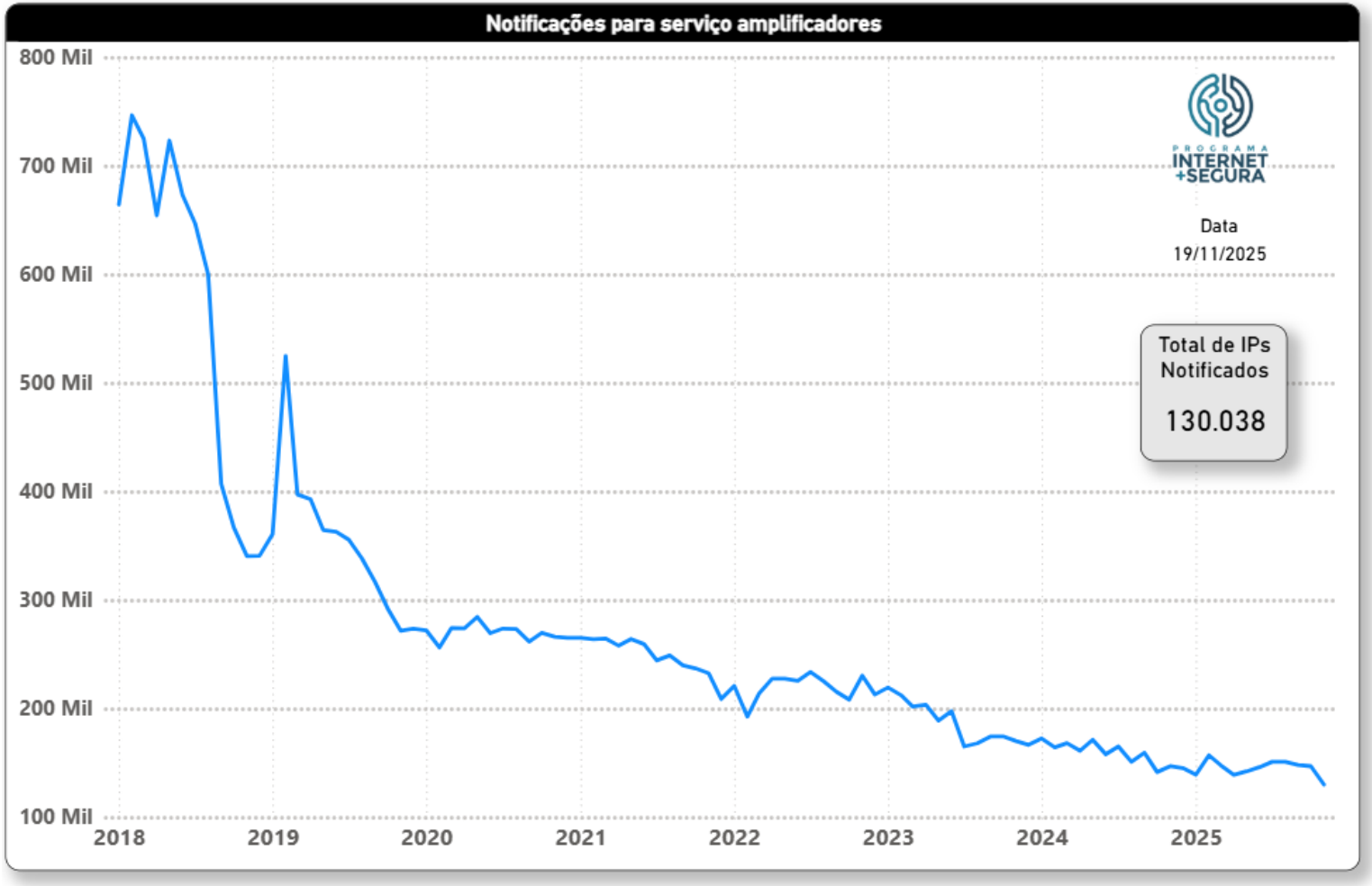
Configurar serviços corretamente

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

Atender às notificações do CERT.br

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

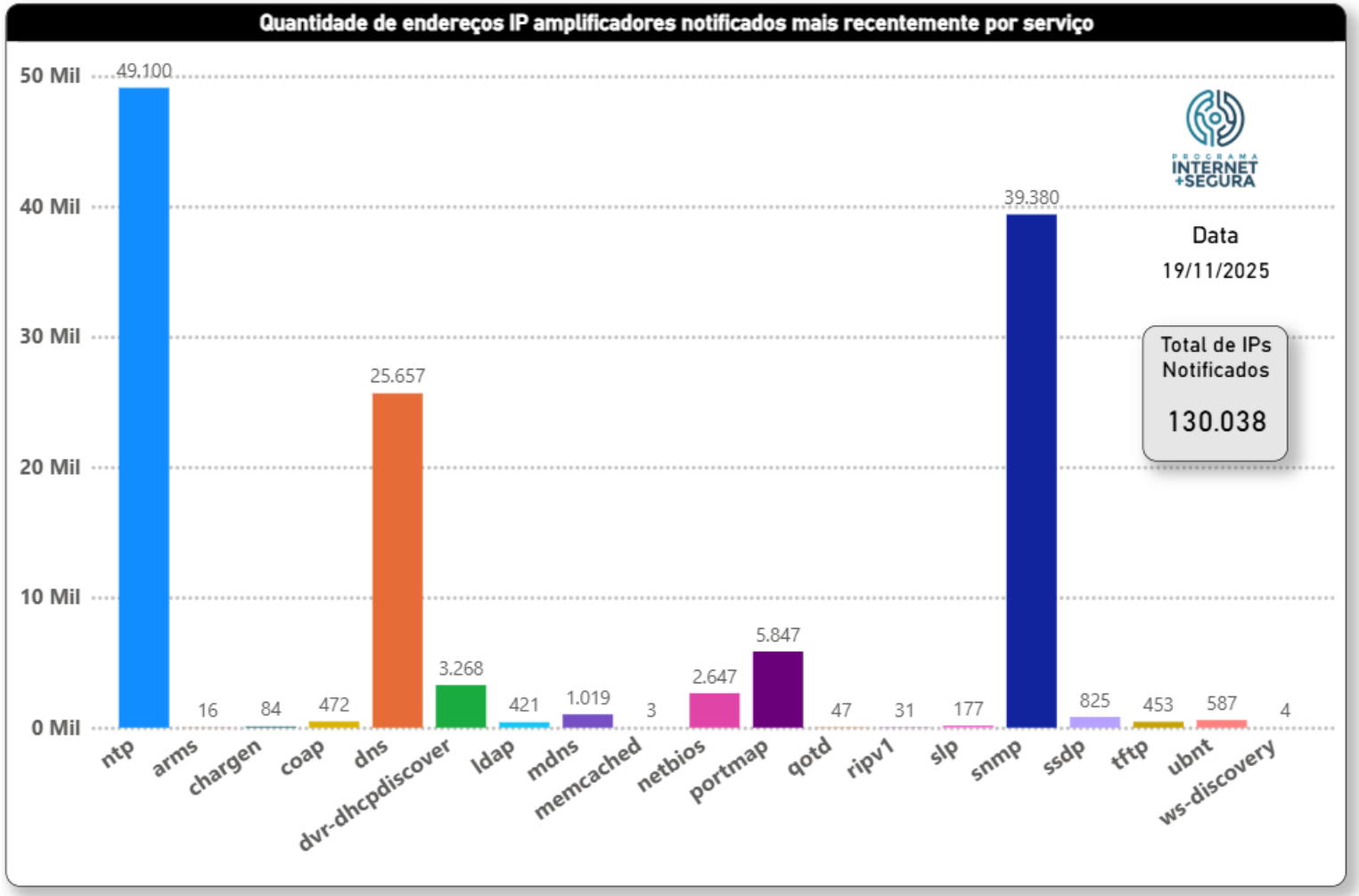
Programa por uma Internet mais Segura
Notificação de amplificadores - evolução



Brasil

- Início (fev/2018)
  - Endereços IP: 746.508
  - Serviços: 5
- Atual:
  - Endereços IP: 130.038
  - Serviços: 19
  - **Redução de 82%**

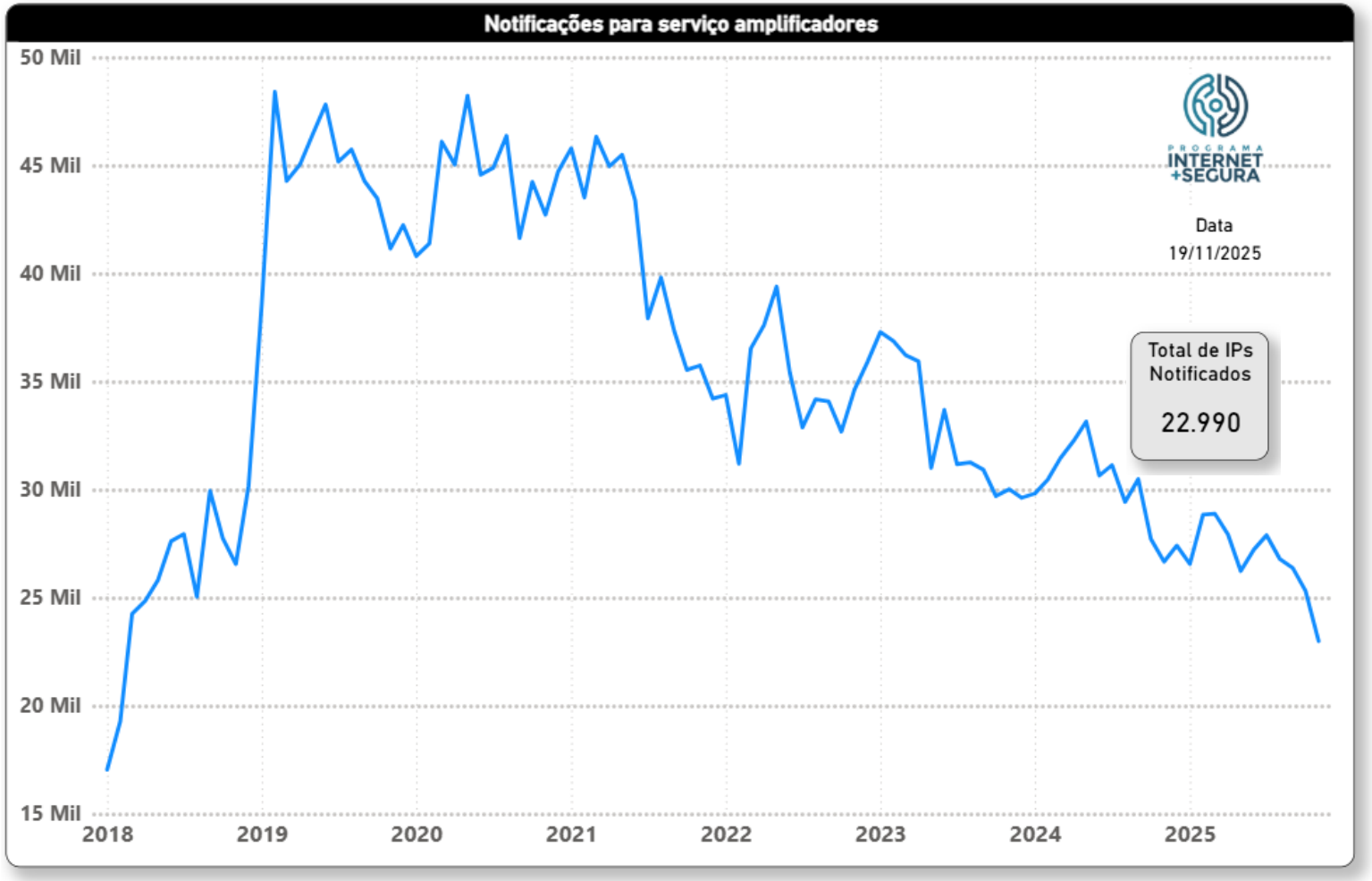
Programa por uma Internet mais Segura
Notificação de amplificadores - serviços



Brasil

- 9.048 AS
- 5.099 AS notificados
- 130.038 endereços IP mal configurados
  - NTP 49.100
  - SNMP 39.380
  - DNS 25.657

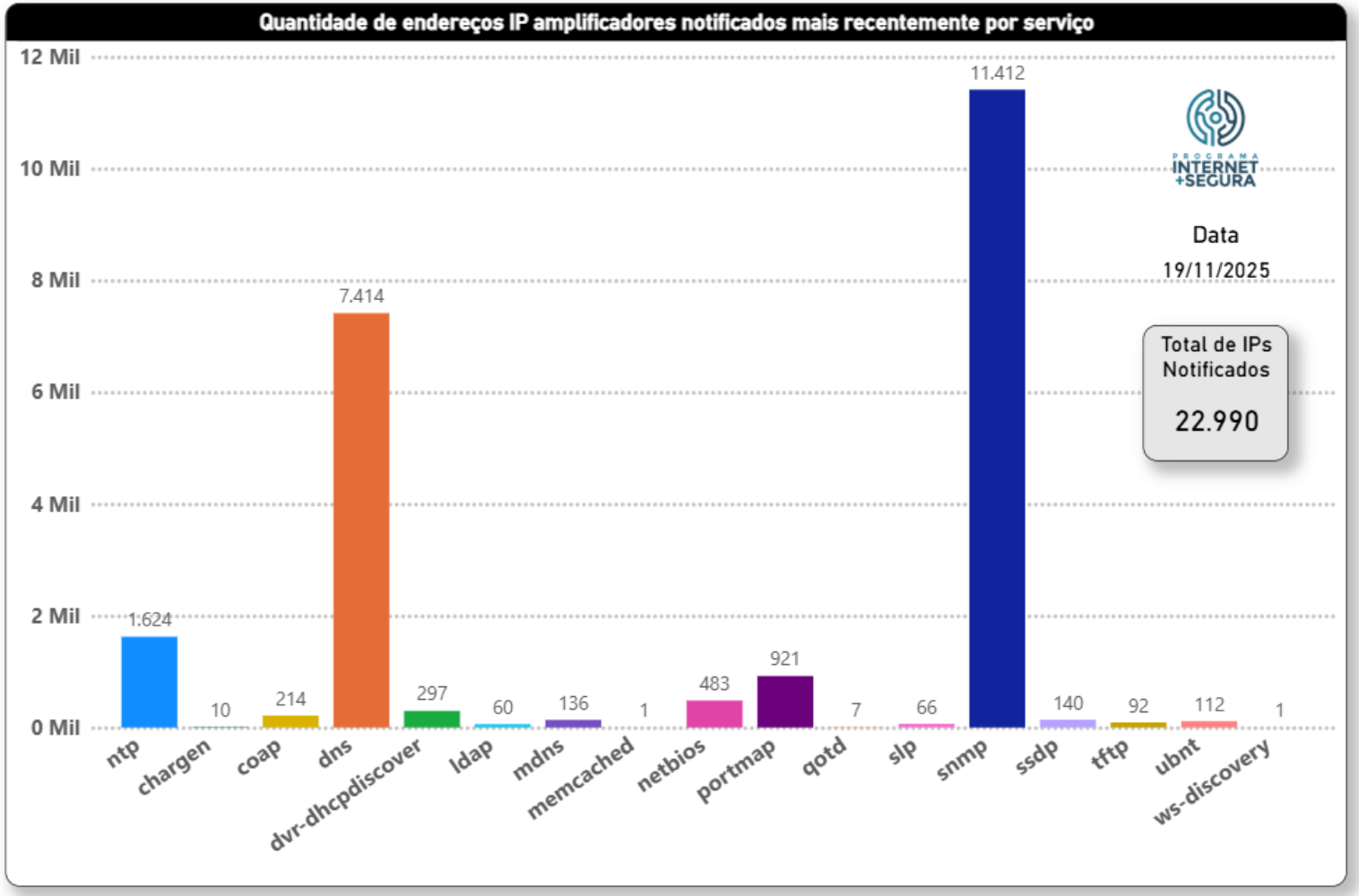
Programa por uma Internet mais Segura
Notificação de amplificadores - evolução



Região Nordeste

- Início (fev/2018)
  - Endereços IP: 17.048
  - Serviços: 5
- Atual:
  - Endereços IP: 22.990
  - Serviços: 19
  - **Aumento de 35%**

Programa por uma Internet mais Segura
Notificação de amplificadores - serviços



Região Nordeste

- 2.385 AS na região
- 2.373 AS notificados
- 17 AS com mais de 200 IP notificados (2 > 500)
- 22990 endereços IP mal configurados
  - SNMP 11.412
  - DNS 7.414
  - NTP 1.624

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

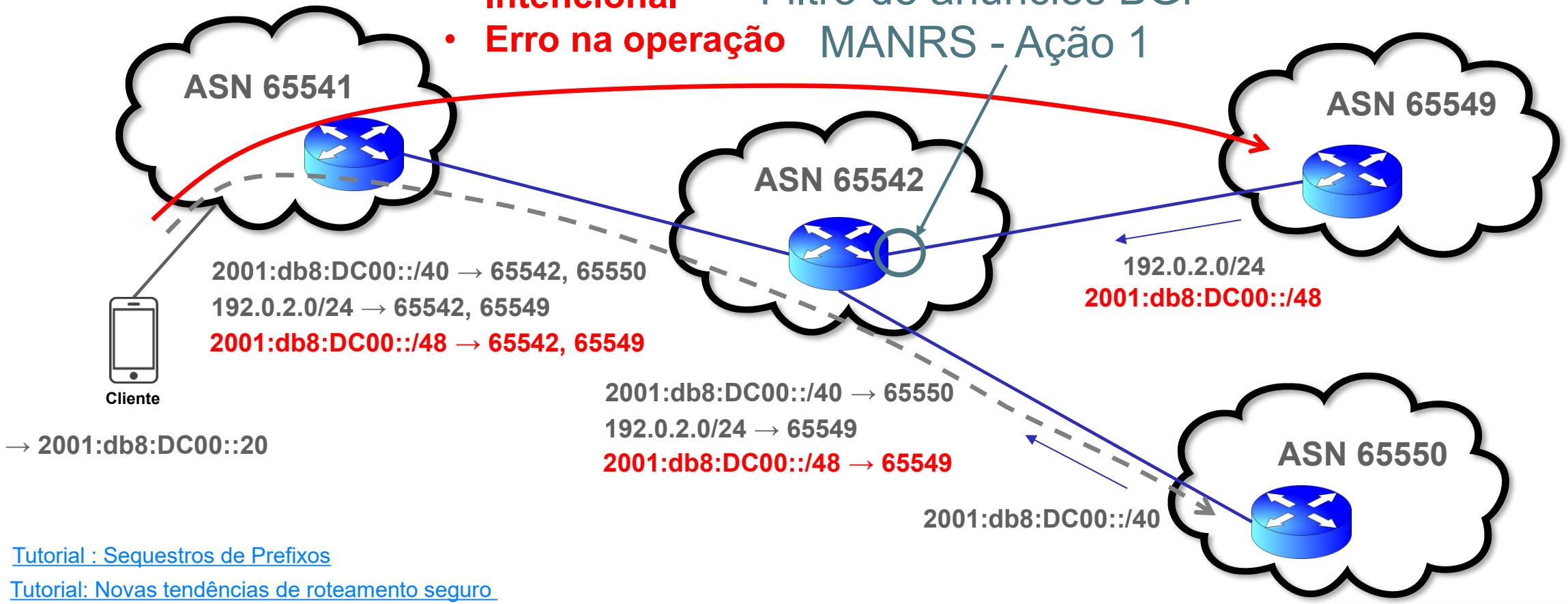
Sequestro de prefixos (Hijacking)

Anúncio de prefixos não autorizados:

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

Filtro de anúncios BGP

MANRS - Ação 1



Tutorial : Sequestros de Prefixos

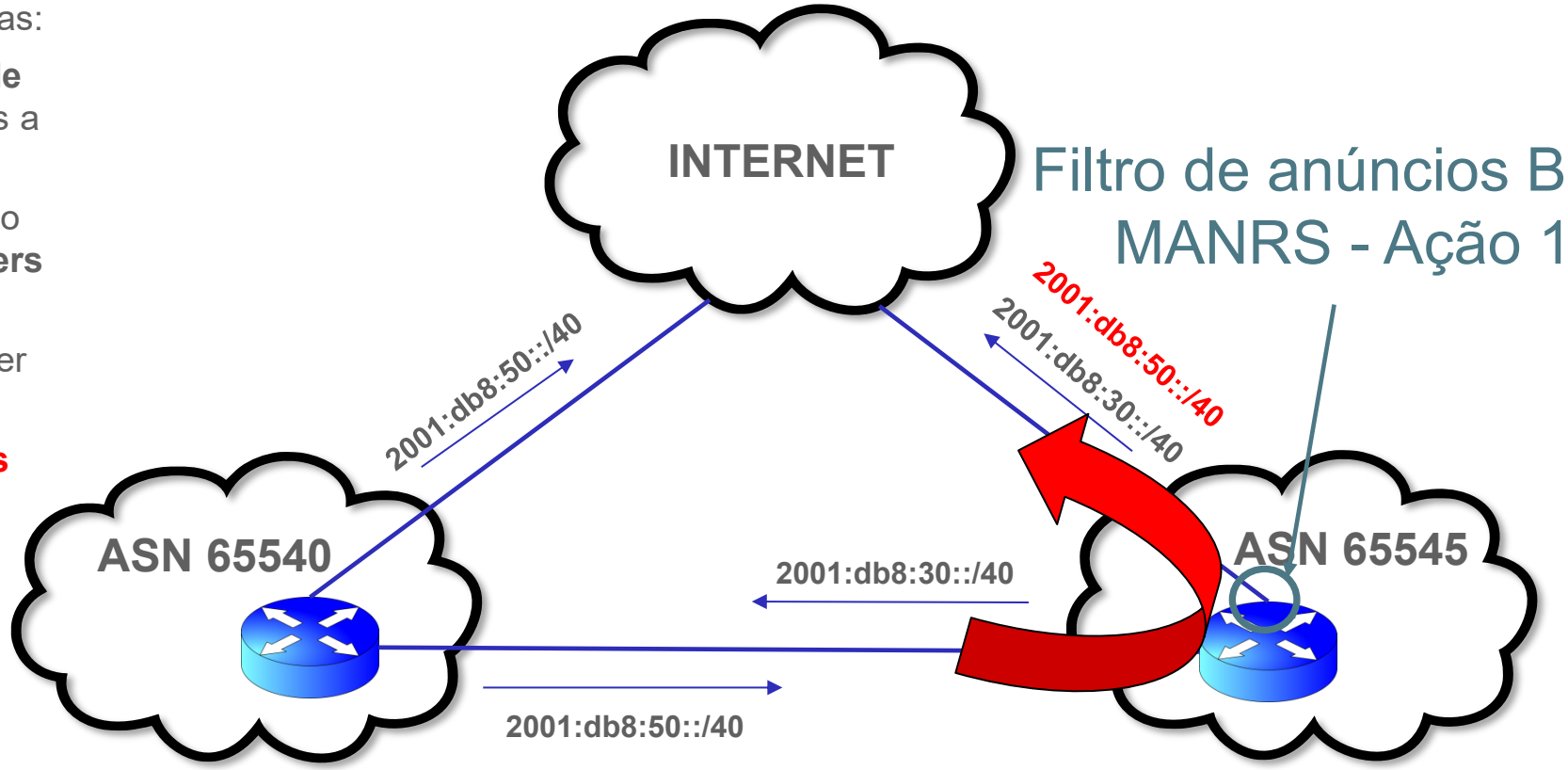
Tutorial: Novas tendências de roteamento seguro

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

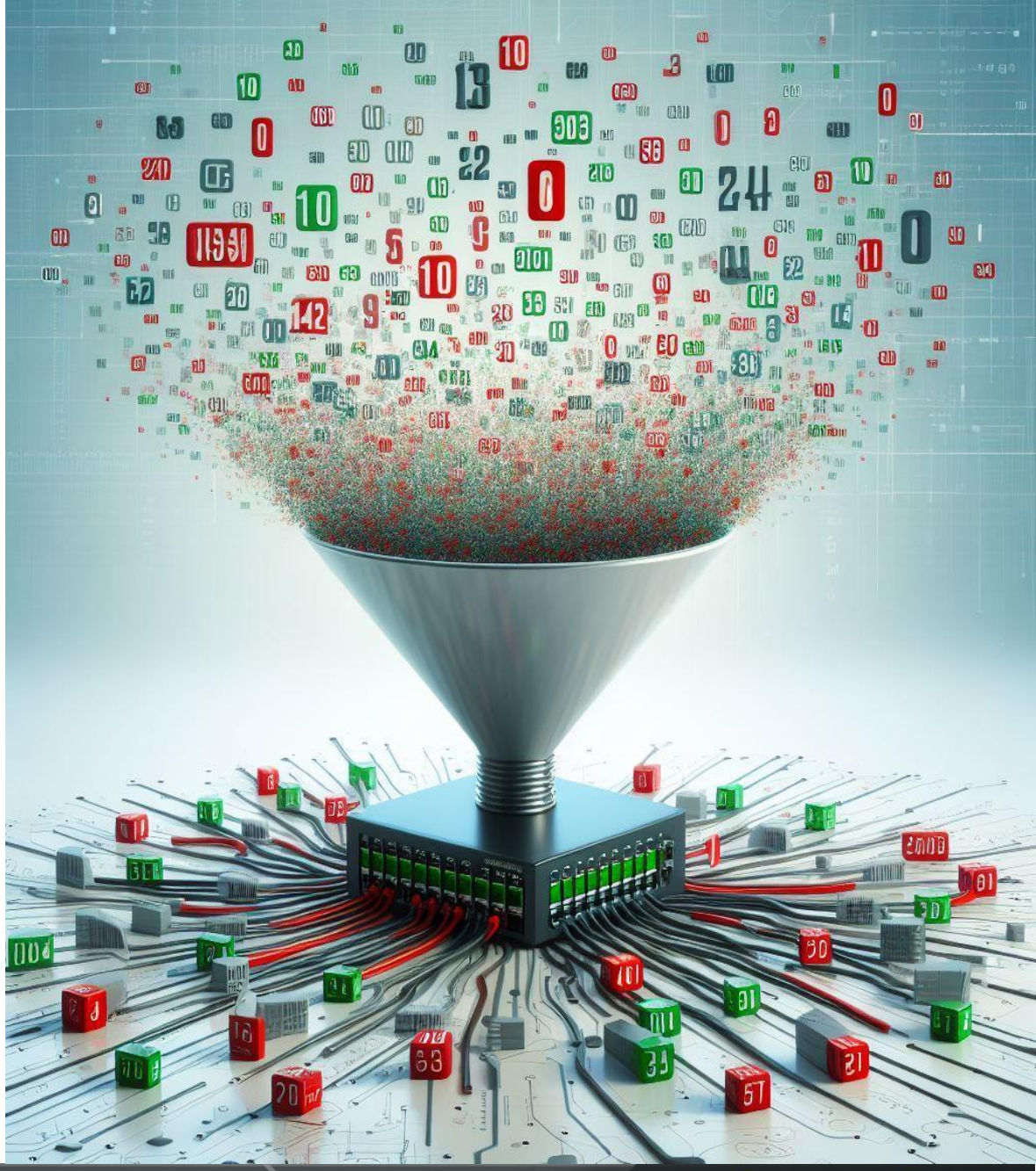
Programa por uma Internet mais Segura

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 Observatory - 2385 AS – Nordeste

Verificação de recebimento de mensagens de abuse

- **241** AS não respondem a mensagens quinzenais de validação de e-mail de abuse do **Registro.br** – **PENDÊNCIA**
- Até 12 tentativas de contato
- Risco de entrar em processo de bloqueio

- **76** AS não responderam mensagens de validação de e-mail de abuse do **Registro.br** – **BLOQUEIO**
- Impedido de designar blocos e delegar DNS
- Inicia processo de recuperação de blocos IP

Recebimento de notificações

- **28** AS não receberam mensagens de notificação de amplificadores por erro no recebimento de mensagens enviadas pelo **CERT.br** (bounce)

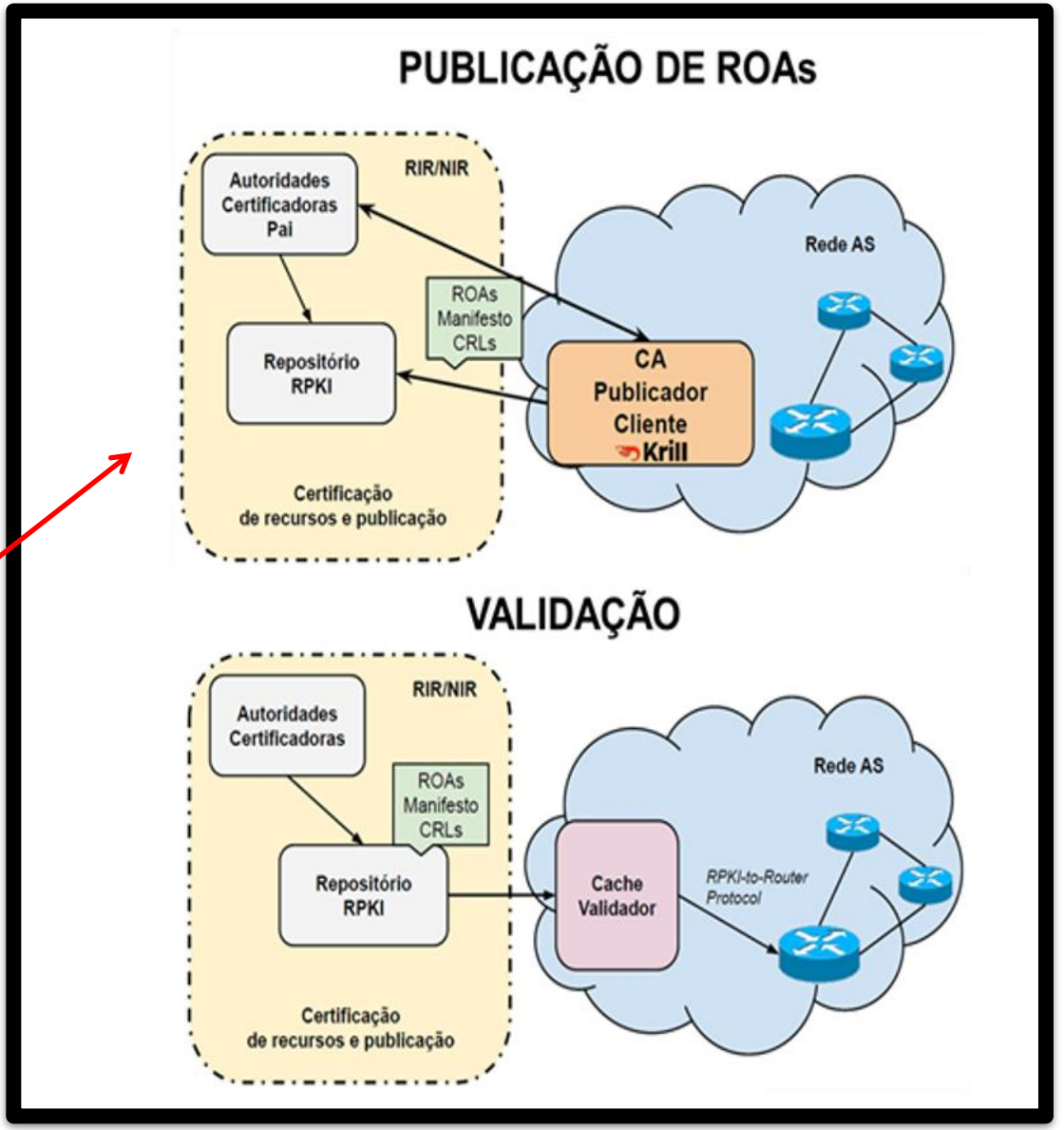
Programa por uma Internet mais Segura

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 - Região Nordeste - 2327 AS

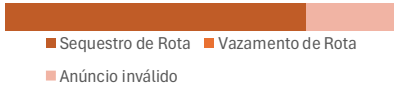
Resumo

25-nov-25

MANRS - Status da Segurança de Roteamento

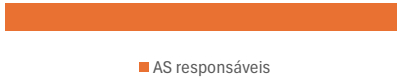
Incidentes

Sequestro de Rota	7
Vazamento de Rota	0
Anúncio inválido	2
Total	9



Responsáveis

AS responsáveis	9



Informação de Roteamento

IRR

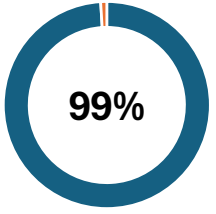
Não registrado	246	**1,2%**
Registrado	20.481	**98,8%**

RPKI

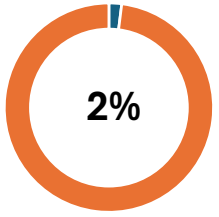
Válido	10.625	**51,3%**
Desconhecido	10.060	**48,5%**
Inválido	42	**0,2%**

MANRS - Prontidão

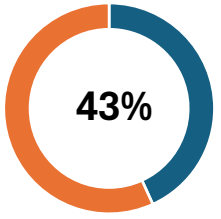
Filtros BGP



Anti-spoofing

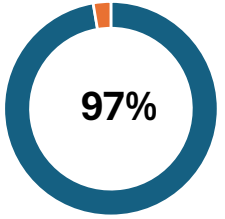


Coordenação

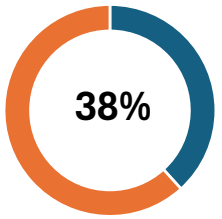


Informação de Roteamento

IRR



RPKI



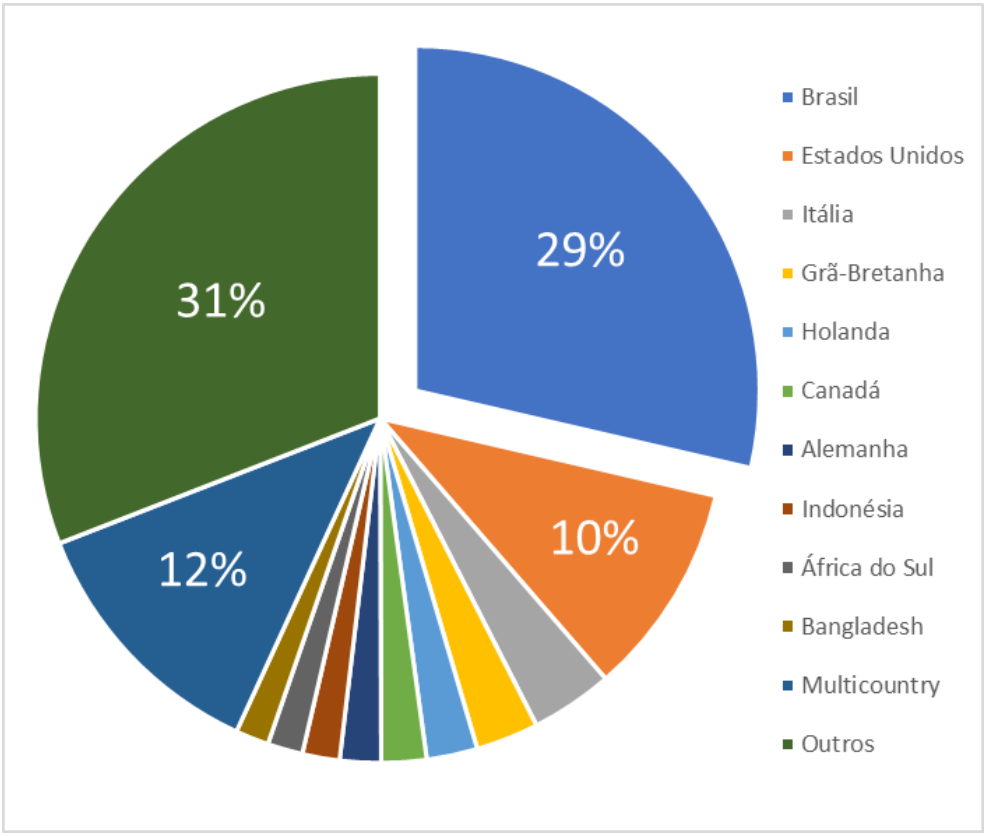
Programa por uma Internet mais Segura

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
Participantes do MANRS - 66 AS - Nordeste

PROGRAMA INTERNET +SEGURA

Sistemas Autônomos Participantes

28126	53005	263338	266039	267271	269292
28184	53045	263861	266129	267361	269424
28186	53236	263903	266136	267390	269433
28264	61618	263929	266152	267408	269497
28300	61888	264201	266289	267440	270370
52592	262293	264293	266303	268101	270928
52871	262300	264300	266309	268349	271175
52872	262393	264359	266388	268674	271383
52873	262494	264479	266551	268887	271566
52913	263086	265019	266979	269159	273316
52999	263327	265397	267086	269194	273517

MANRS

PROGRAMA INTERNET +SEGURA

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

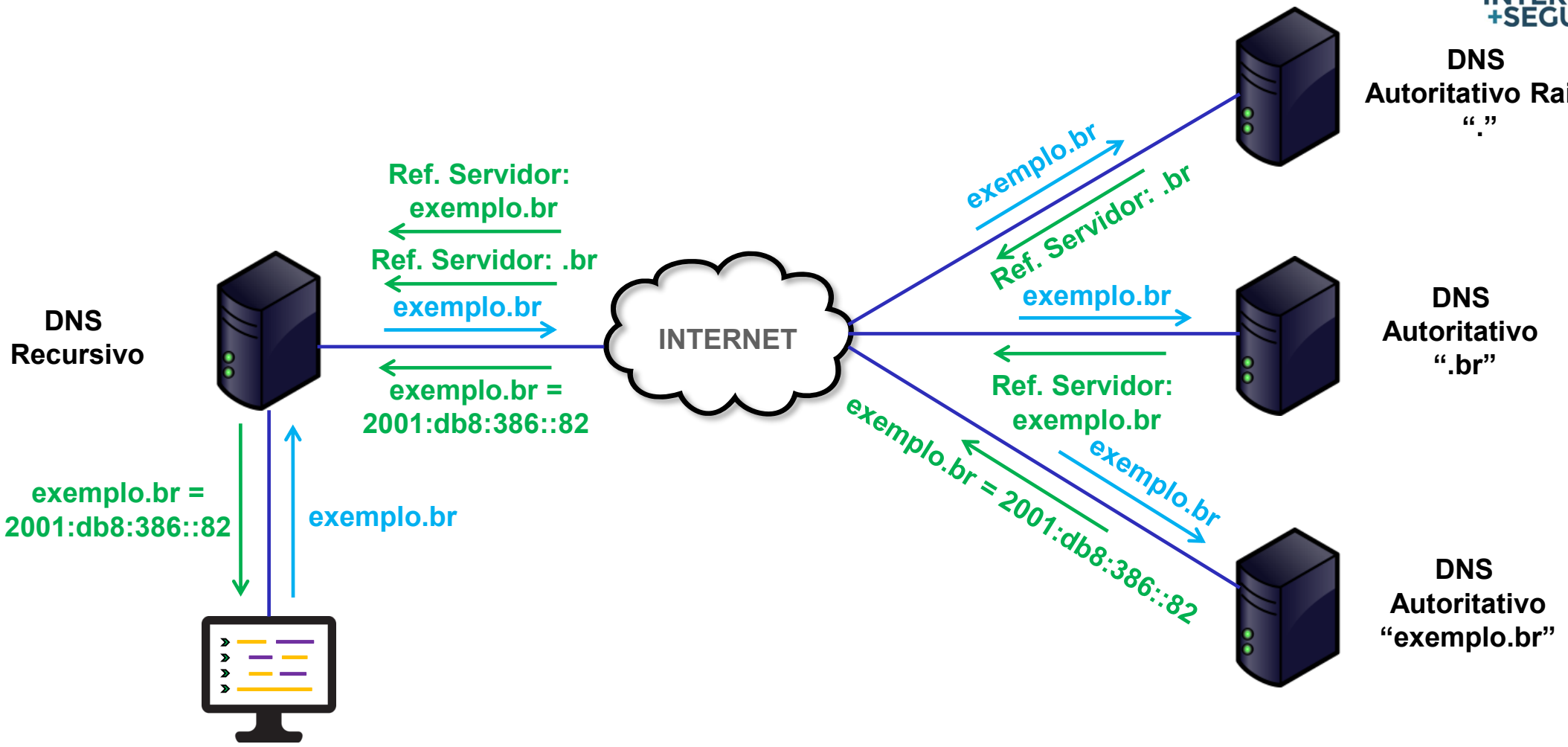
https://kindns.org/

An ICANN Initiative

ICANN

Programa por uma Internet mais Segura

Processo de Recursão DNS



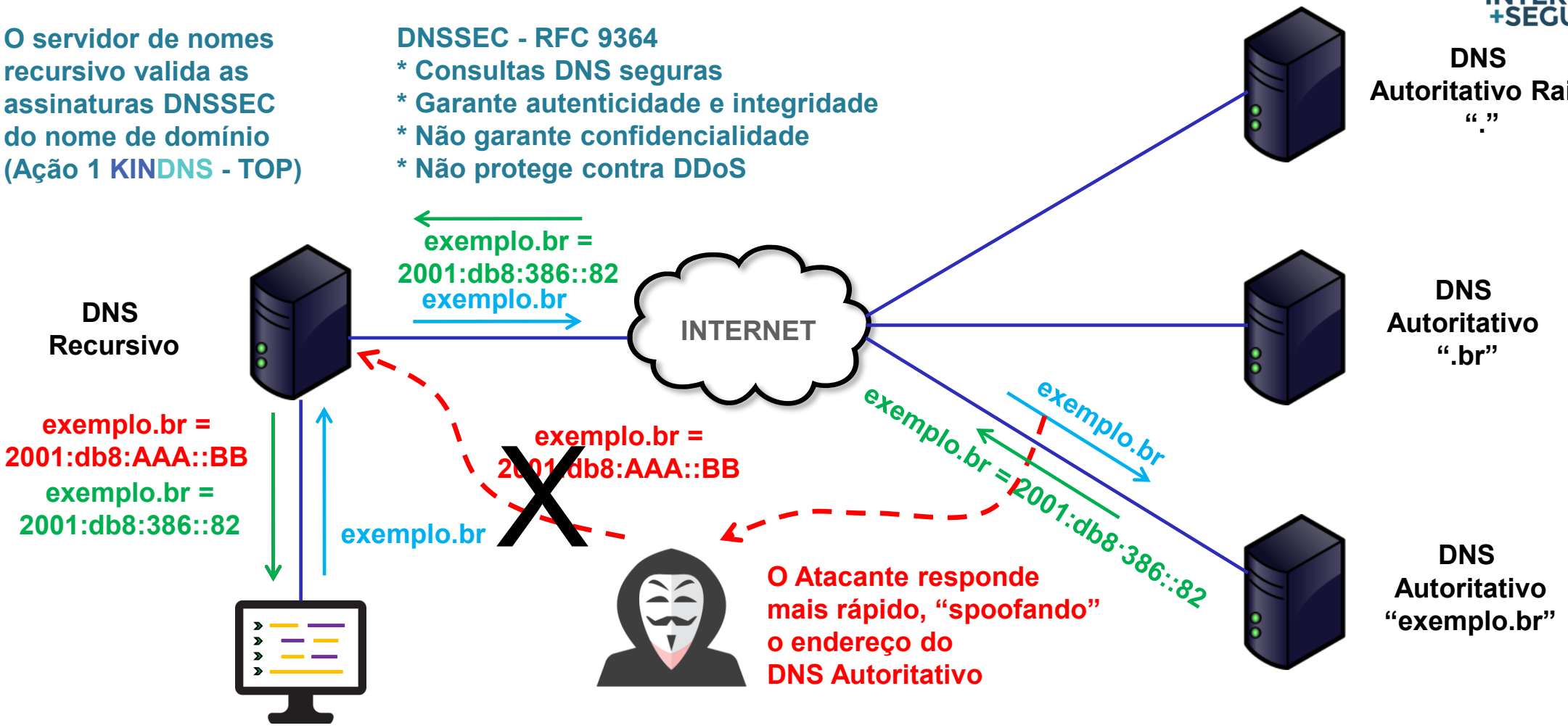
Tutorial: Configurando o seu DNS de forma simples e segura – Ataque DNS Poisoning

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

Obrigado

Gilberto Zorello

gzorello@nic.br

27 de novembro de 2025

nic.br cgi.br

www.nic.br | www.cgi.br