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

Programa por uma Internet mais segura

Como tornar seu provedor mais seguro

Gilberto Zorello | gzorello@nic.br

IX Fórum Regional - Edição Sul - 2025

Lajeado, RS | 16/05/25

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
- Melhorar a segurança da resolução de nomes
- 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

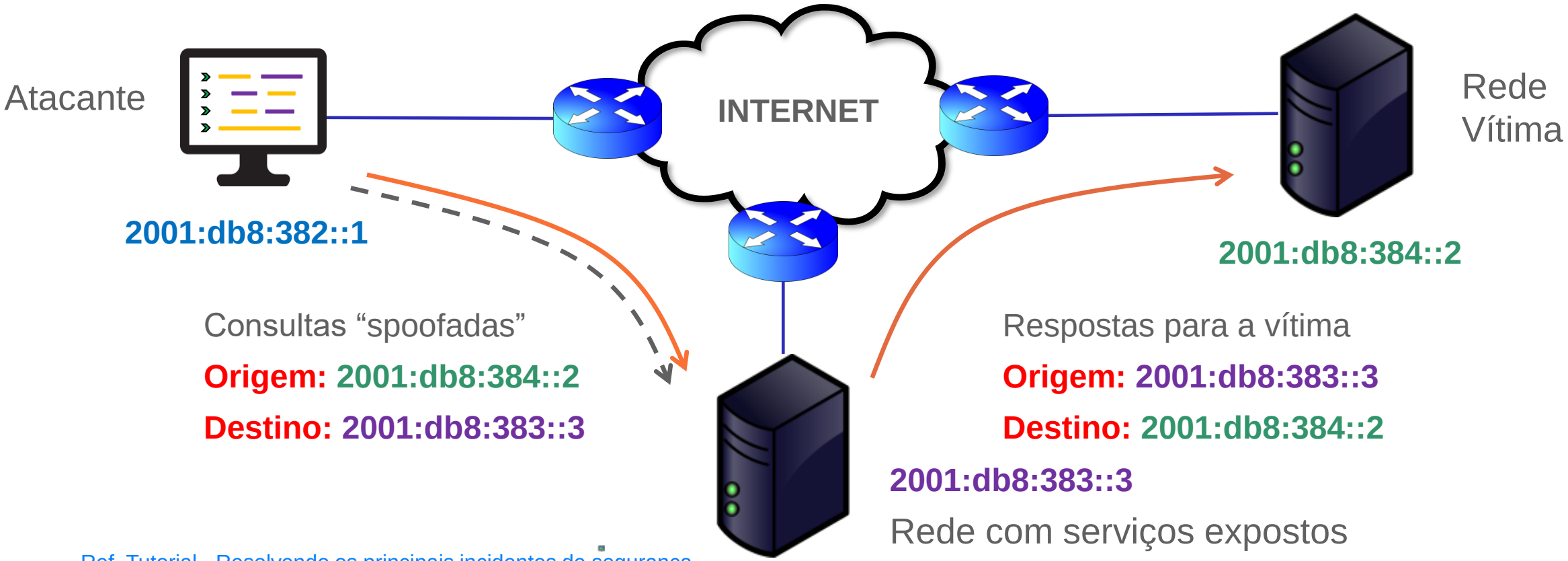
- Usados para amplificação em DDoS
- Portas UDP: DNS (53), SNMP (161), NTP (123), e várias outras!
- Notificações do CERT.br

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

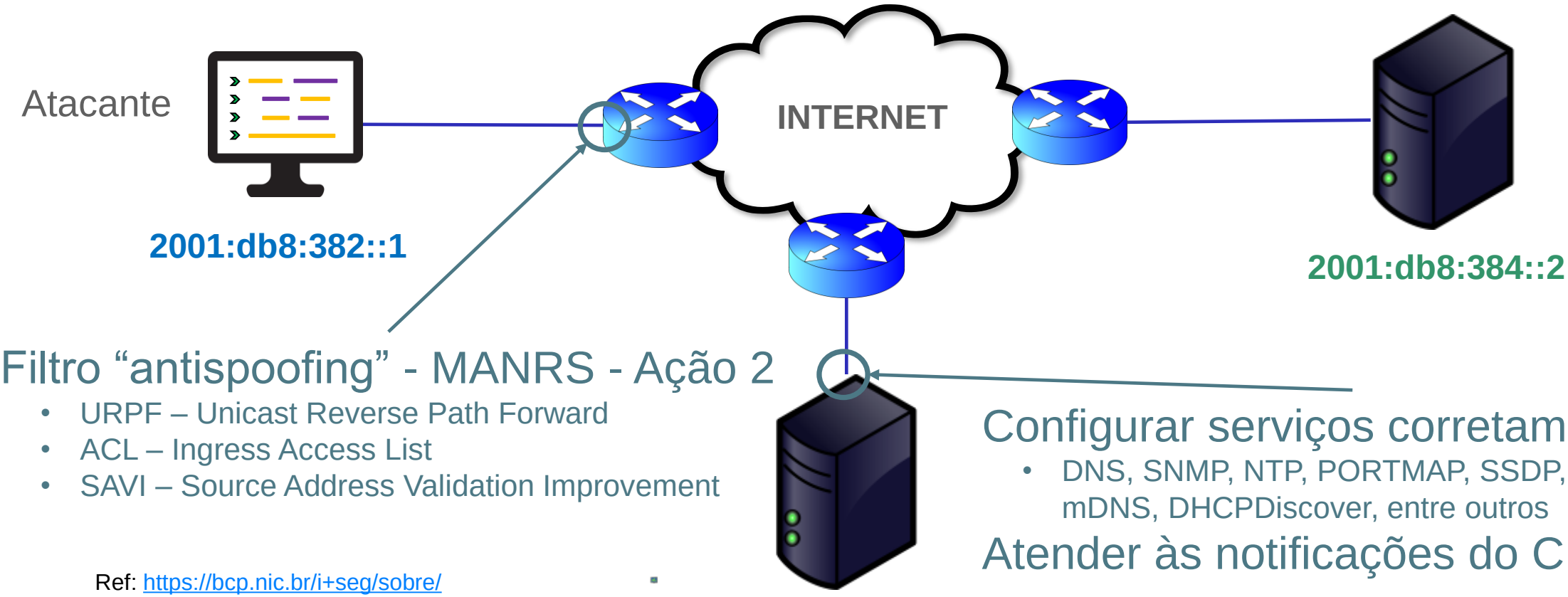


Ref. Tutorial - Resolvendo os principais incidentes de segurança

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

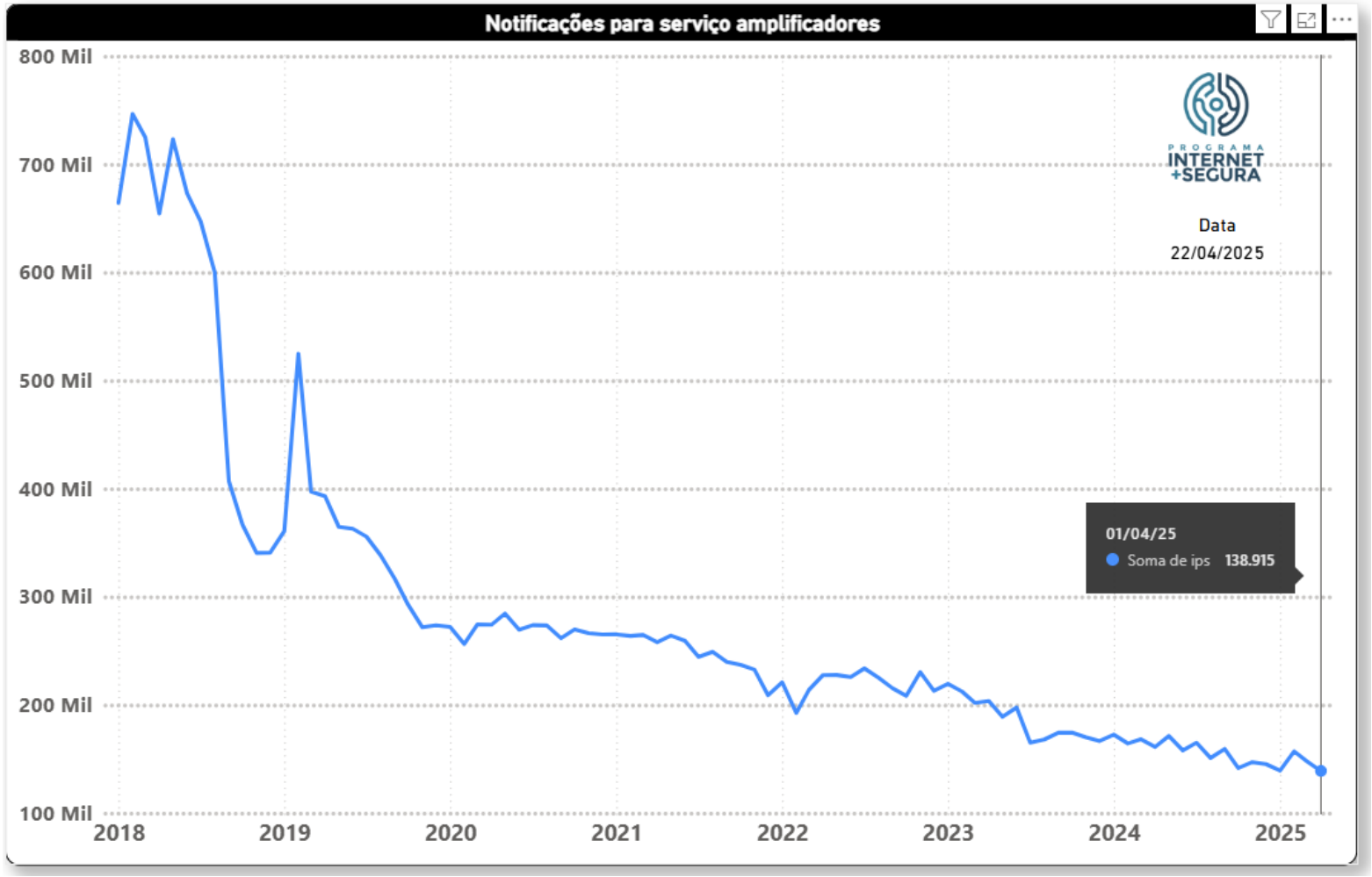
Configurar serviços corretamente

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

Atender às notificações do CERT.br

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

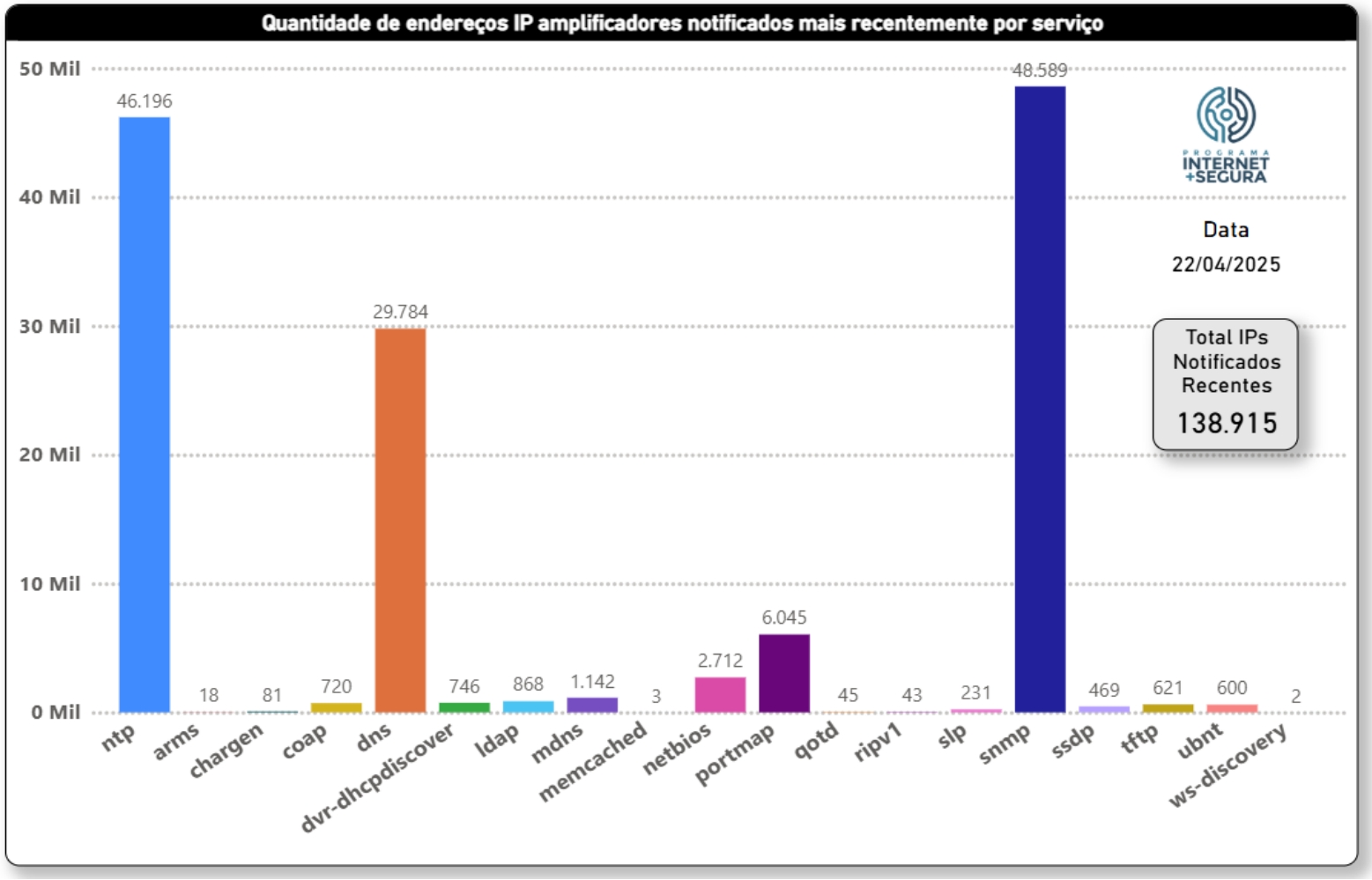
Programa por uma Internet mais Segura
Notificação de amplificadores - evolução



Brasil

- Início (fev/2018)
  - Endereços IP: 746.508
  - Serviços: 6
- Atual:
  - Endereços IP: 138.915
  - Serviços: 19
  - **Redução de 81%**

Programa por uma Internet mais Segura
Notificação de amplificadores - serviços

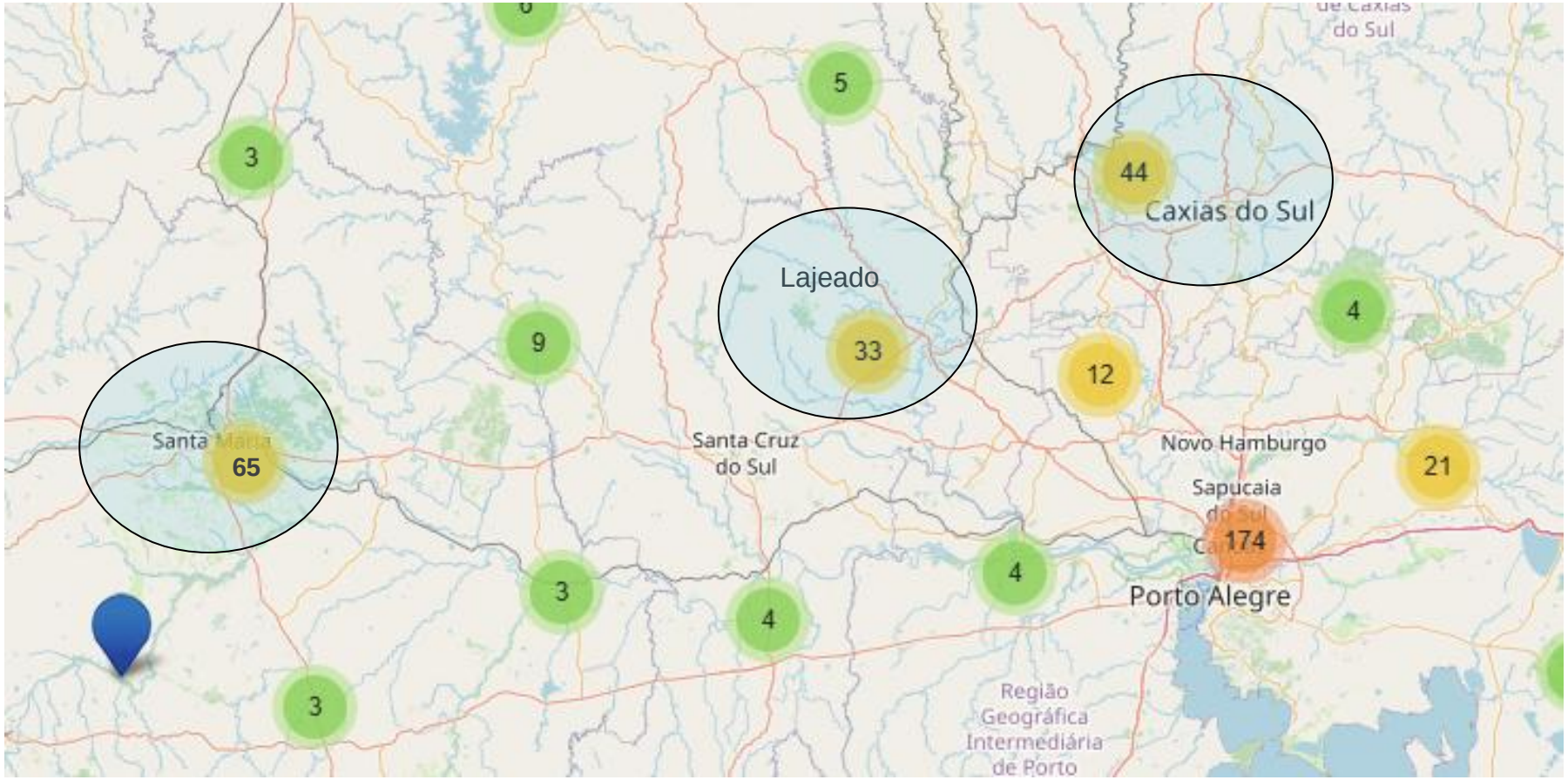


Brasil

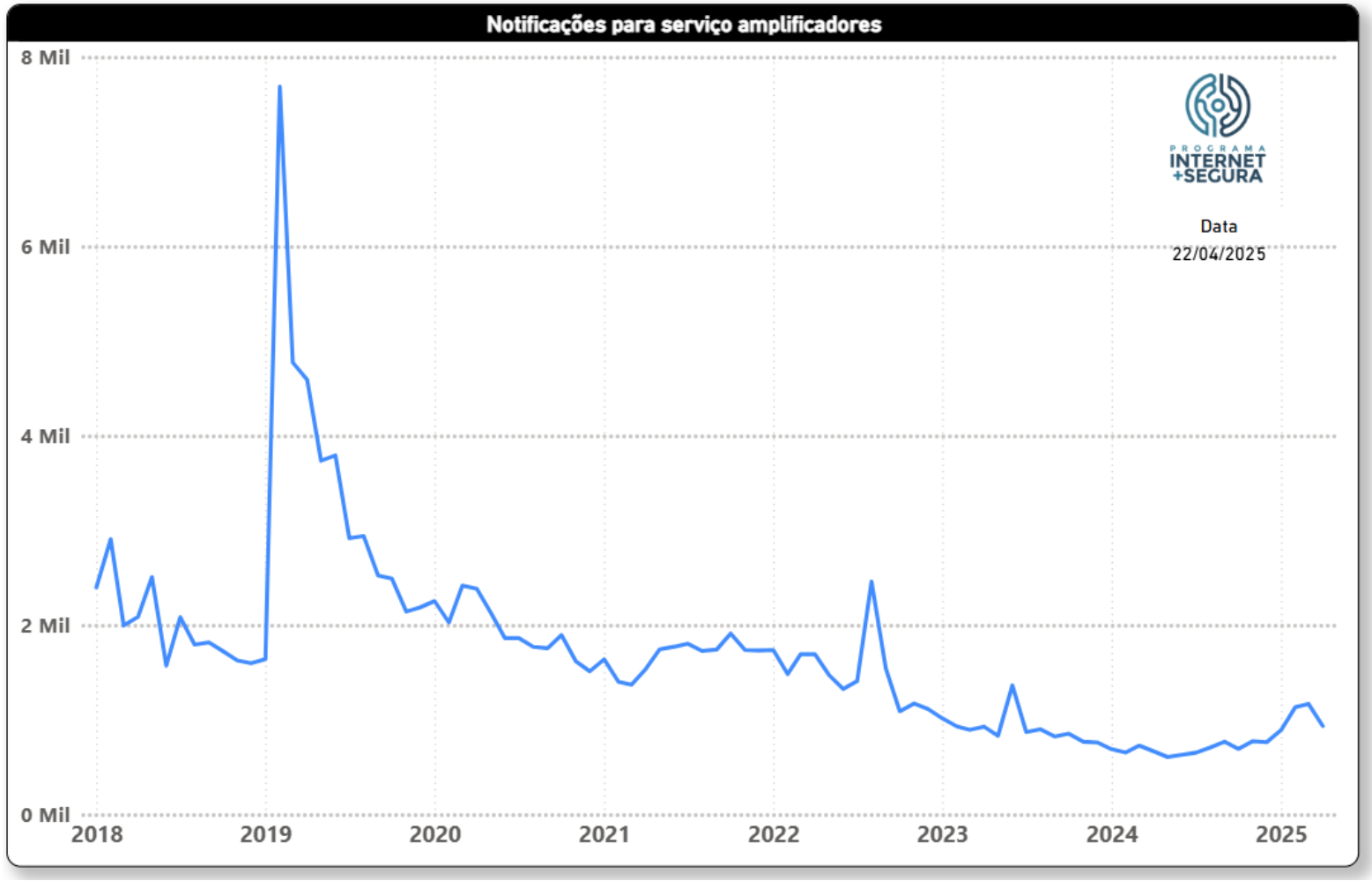
- 5.089 AS notificados
- 138.915 endereços IP mal configurados
  - SNMP 46.196
  - DNS 29.784
  - NTP 48.589

Programa por uma Internet mais Segura

Região dos IX RS – Lajeado, Caxias do Sul e Santa Maria



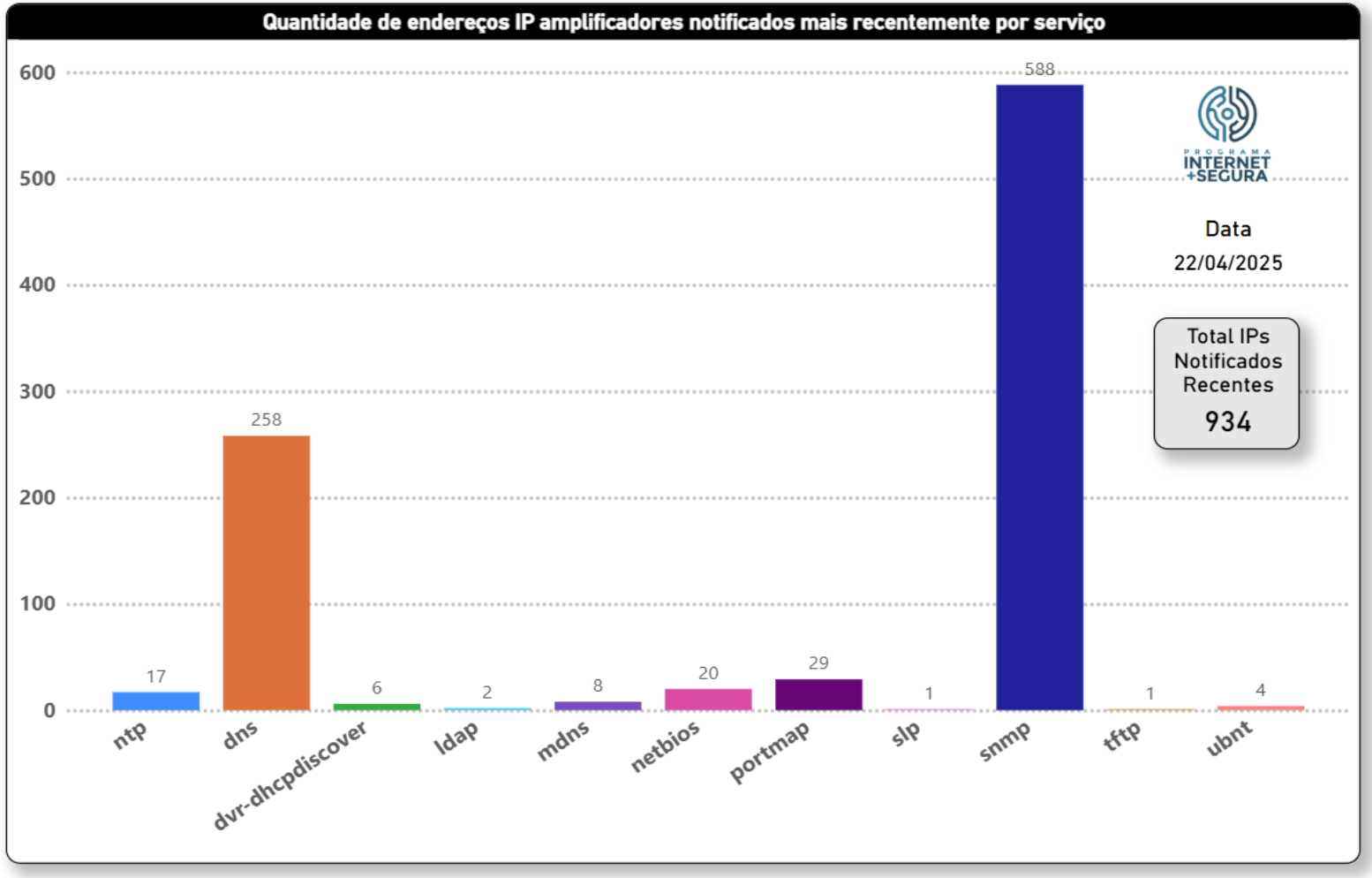
Programa por uma Internet mais Segura
Notificação de amplificadores - evolução



Região LJO CSL SMA

- Início (fev/2018)
  - Endereços IP: 2.908
  - Serviços: 6
- Atual:
  - Endereços IP: 934
  - Serviços: 19
  - **Redução de 68%**

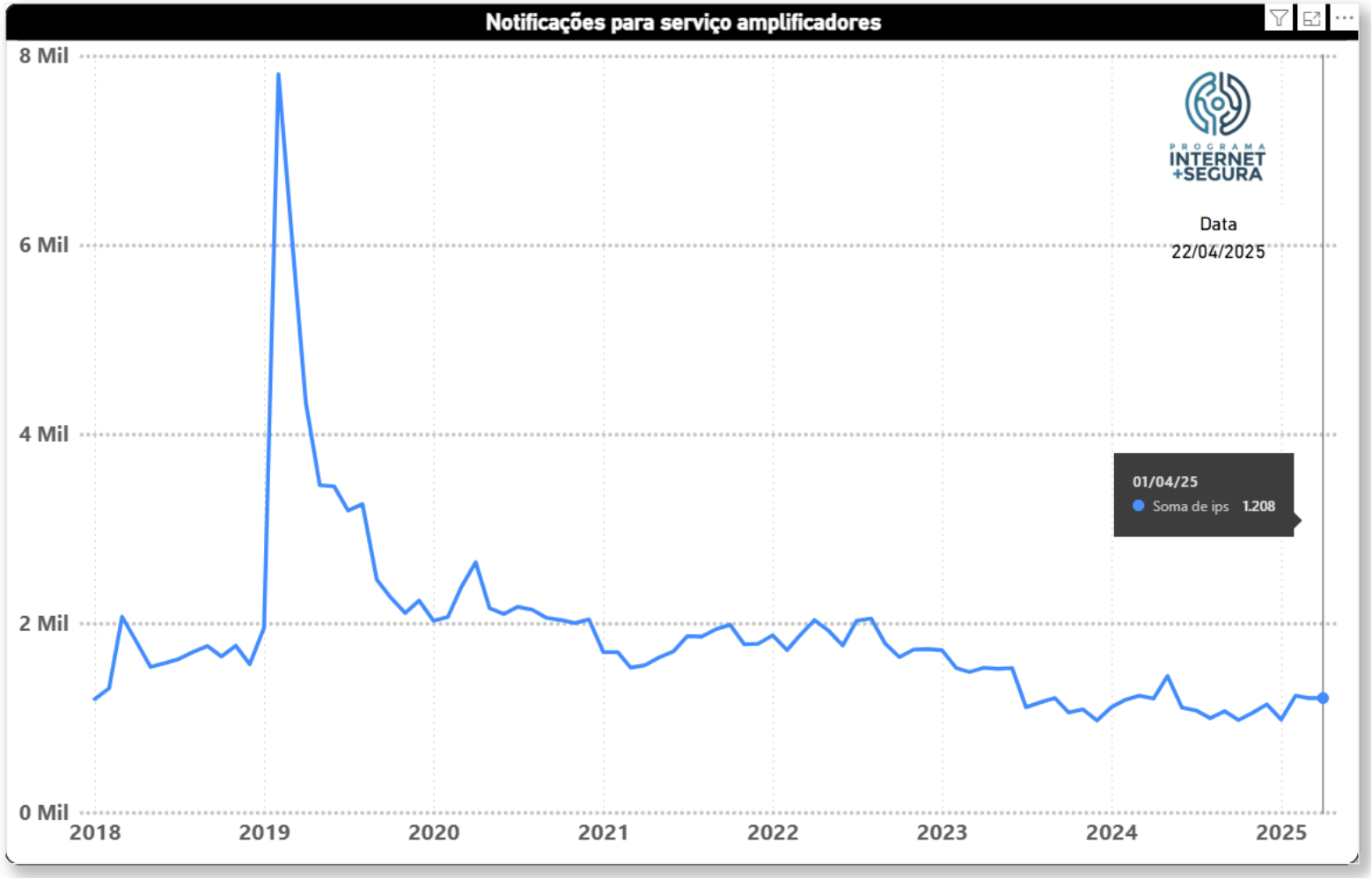
Programa por uma Internet mais Segura
Notificação de amplificadores - serviços



Região LJO CSL SMA

- 70 AS notificados de 126 AS na região
- 934 endereços IP mal configurados
  - SNMP 588
  - DNS 258
  - PORTMAP 29

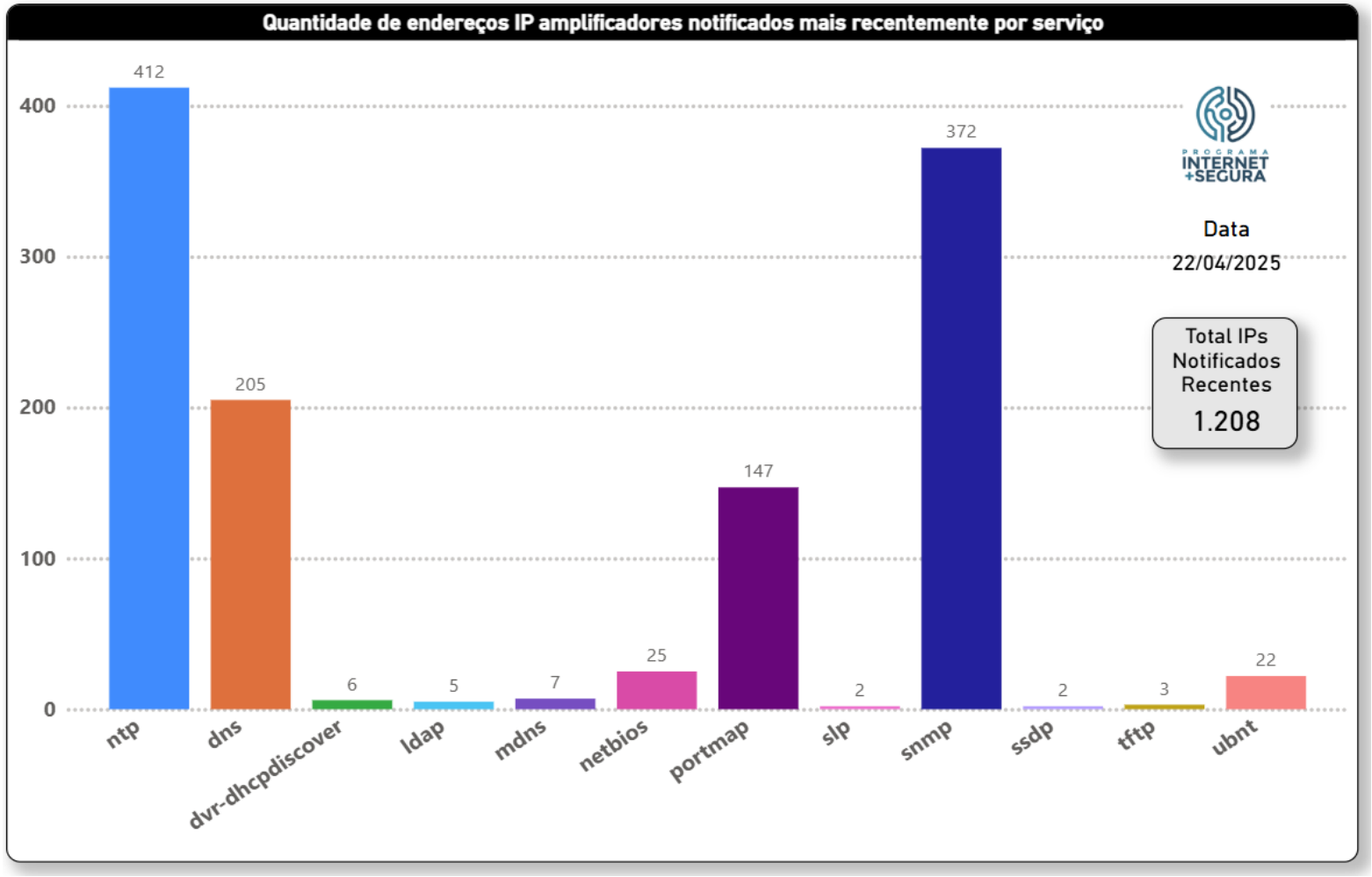
Programa por uma Internet mais Segura
Notificação de amplificadores - evolução



IX Fórum LJO

- Início (fev/2018)
  - Endereços IP: 1.311
  - Serviços: 6
- Atual:
  - Endereços IP: 1.208
  - Serviços: 19
  - **Redução de 8%**

Programa por uma Internet mais Segura
Notificação de amplificadores - serviços



IX Fórum LJO

- 25 AS notificados de 42 AS
- 1.208 endereços IP mal configurados
  - SNMP 372
  - DNS 205
  - NTP 412

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

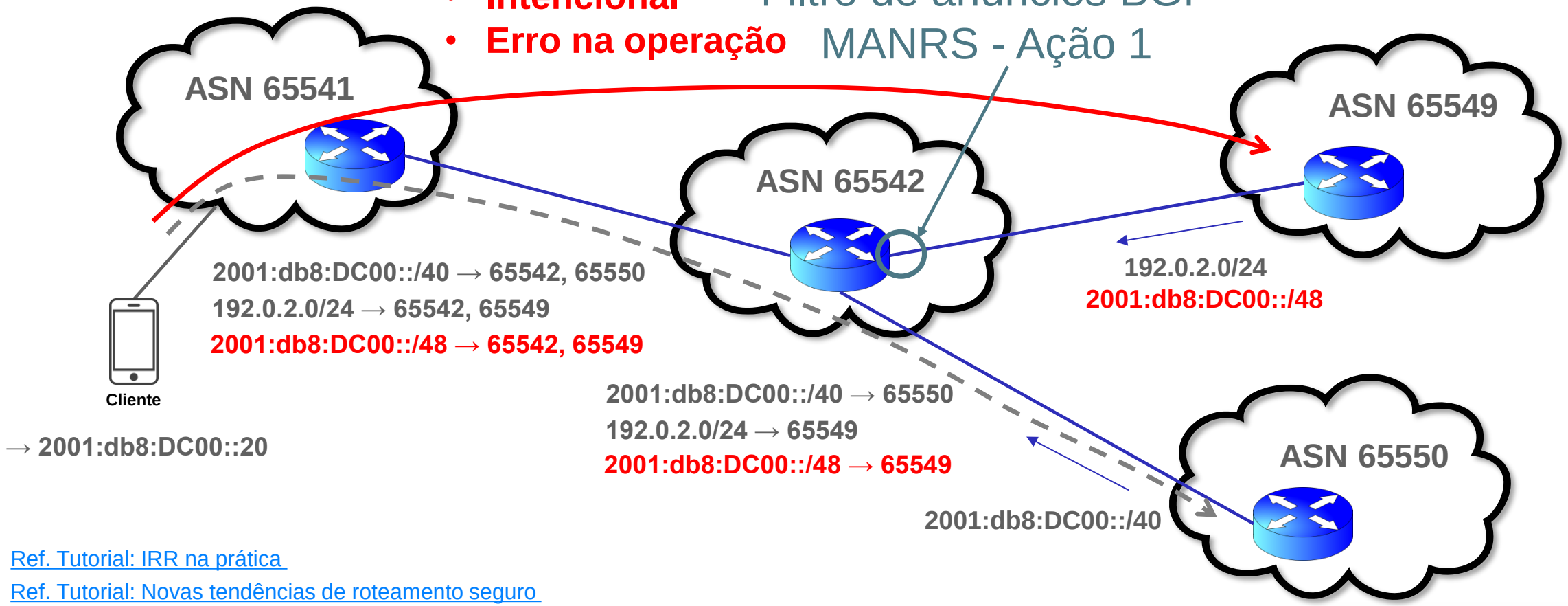
Sequestro de prefixos (Hijacking)

Anúncio de prefixos não autorizados:

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

Filtro de anúncios BGP

MANRS - Ação 1



Ref. Tutorial: IRR na prática

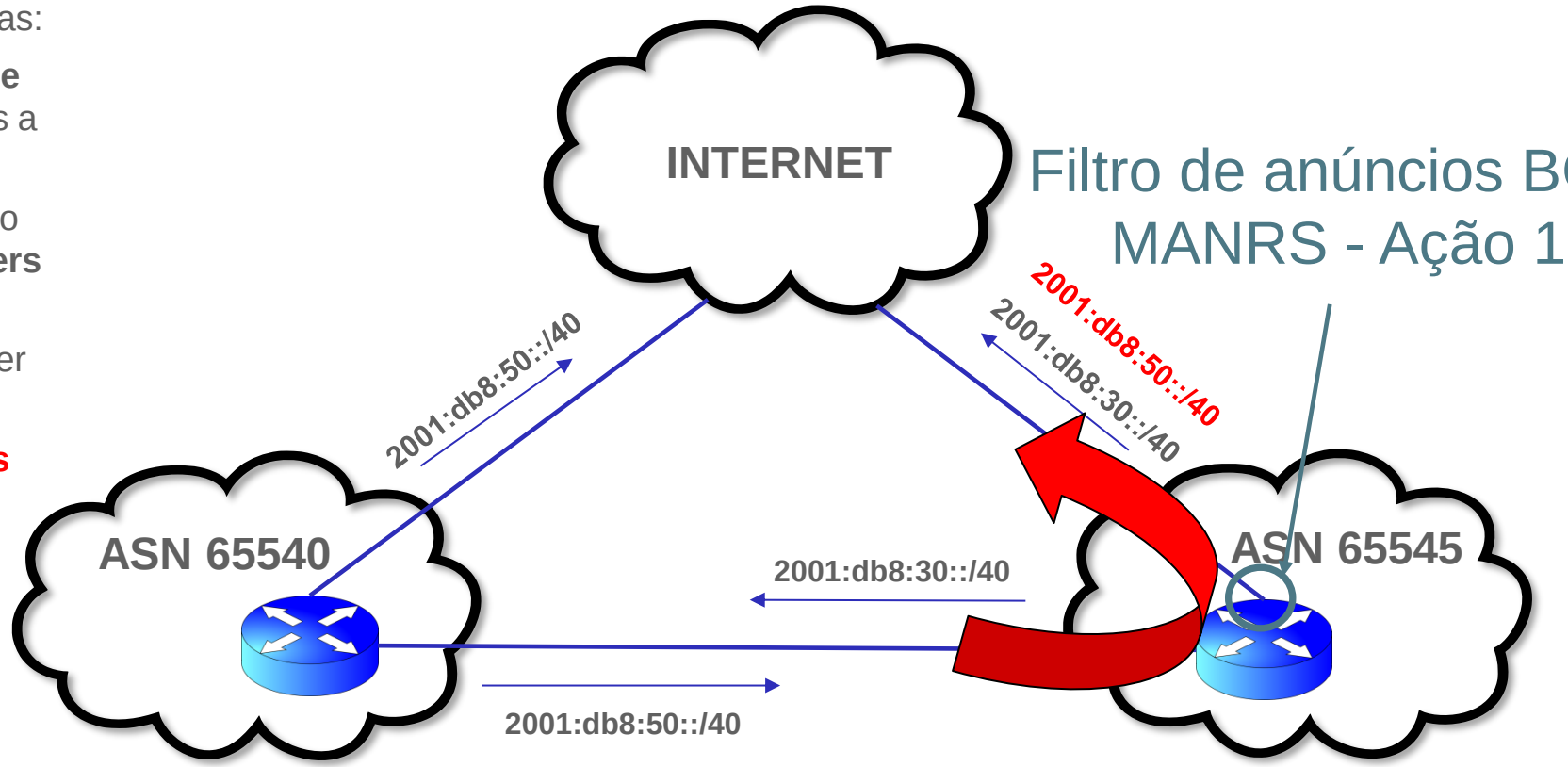
Ref. Tutorial: Novas tendências de roteamento seguro

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



Ref. Tutorial: IRR na prática

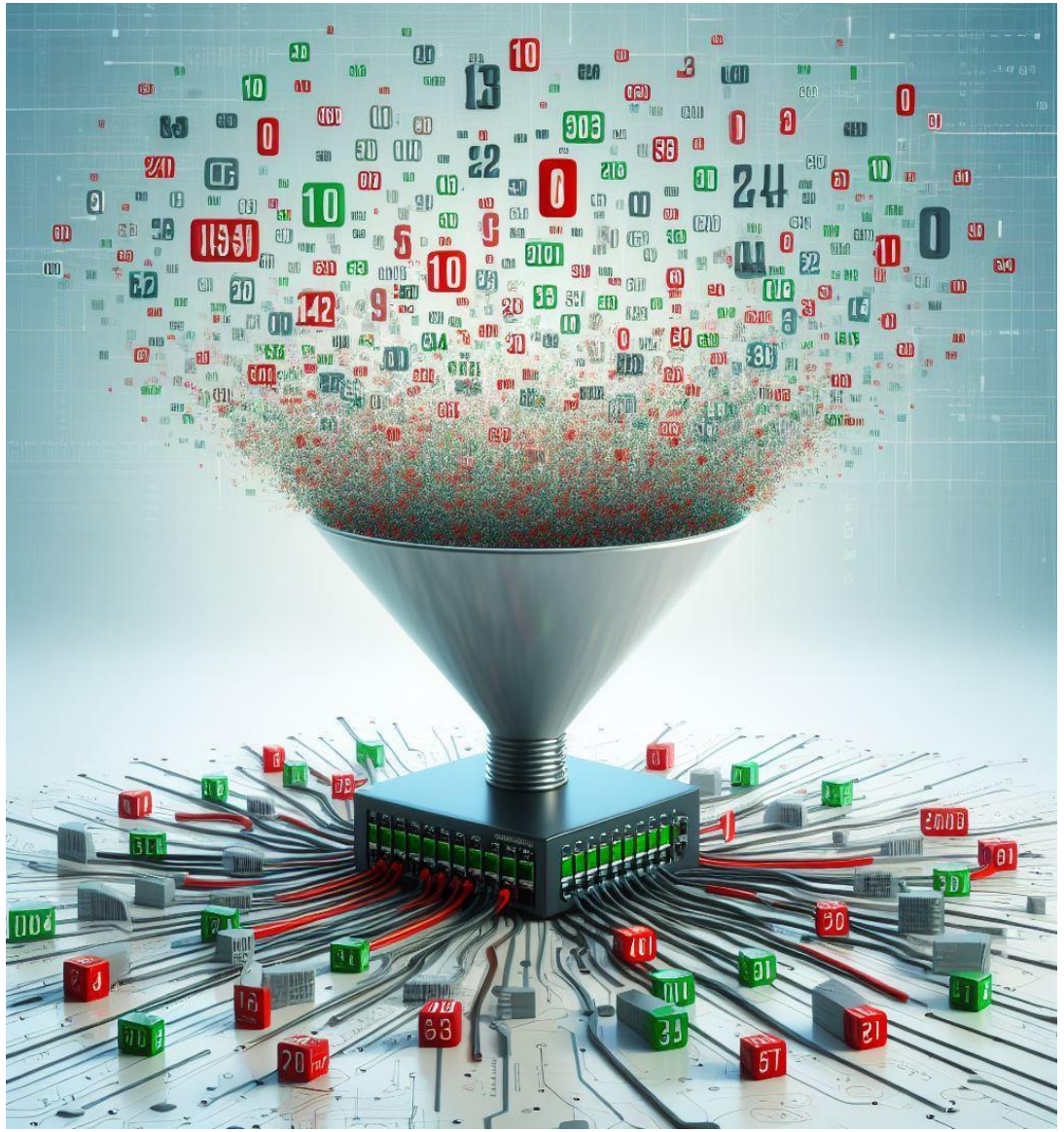
Ref. Tutorial: novas tendências de roteamento seguro

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

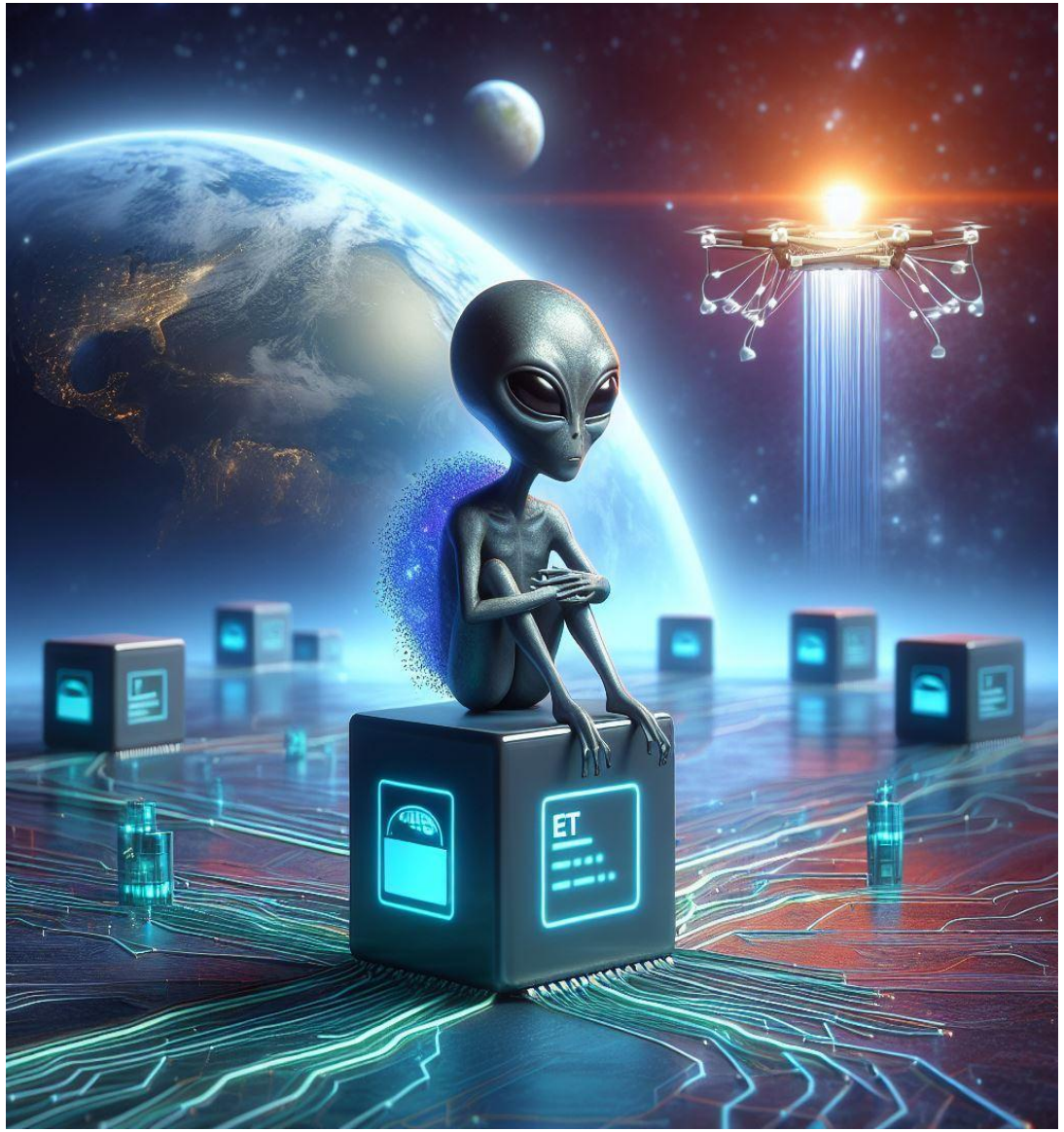
https://bcp.nic.br/i+seg/acoes/manrs/#filtragem-de-rotas



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)!



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 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**

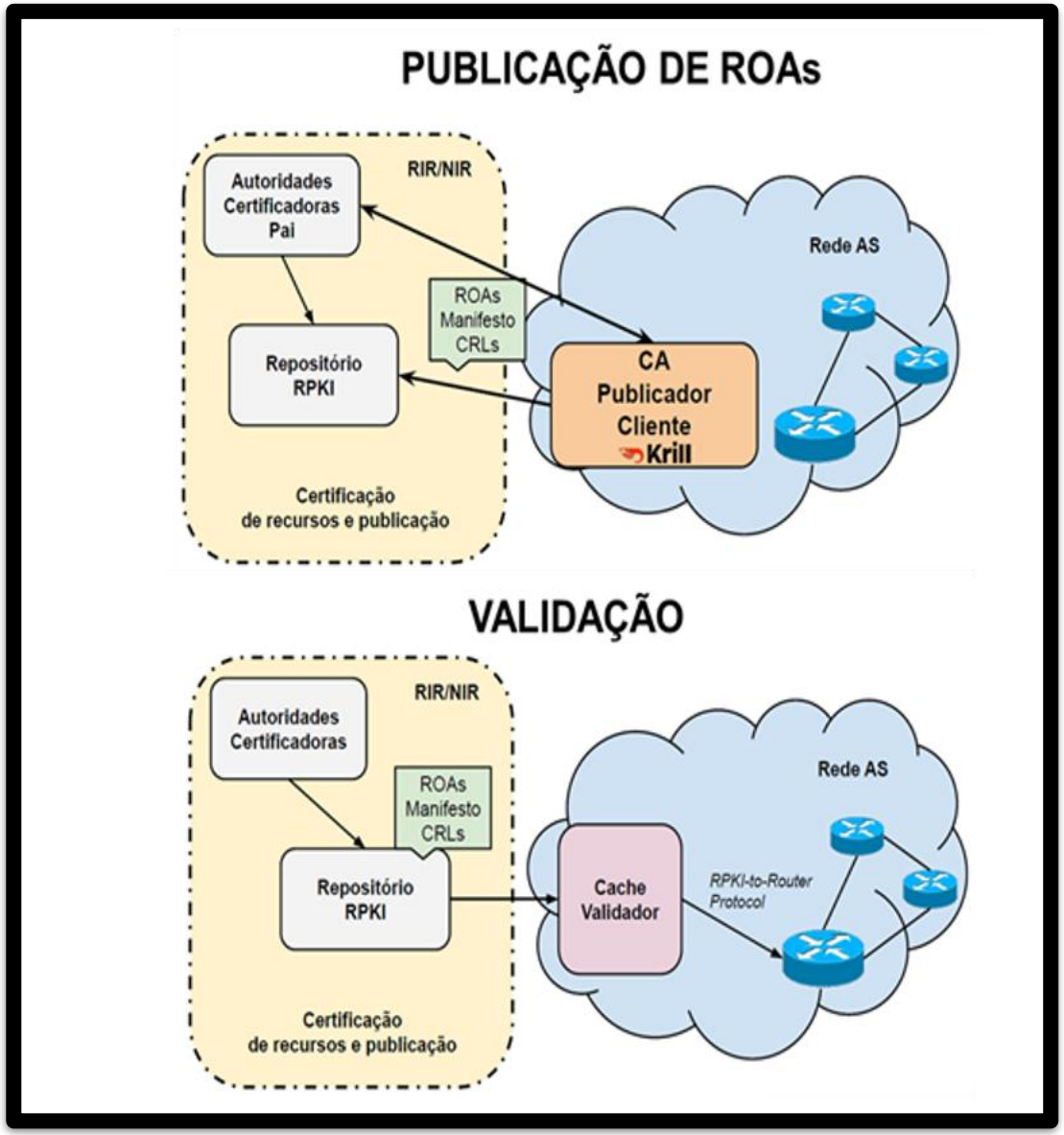
MANRS https://bcp.nic.br/i+seg/acoes/manrs/#coordenacao

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

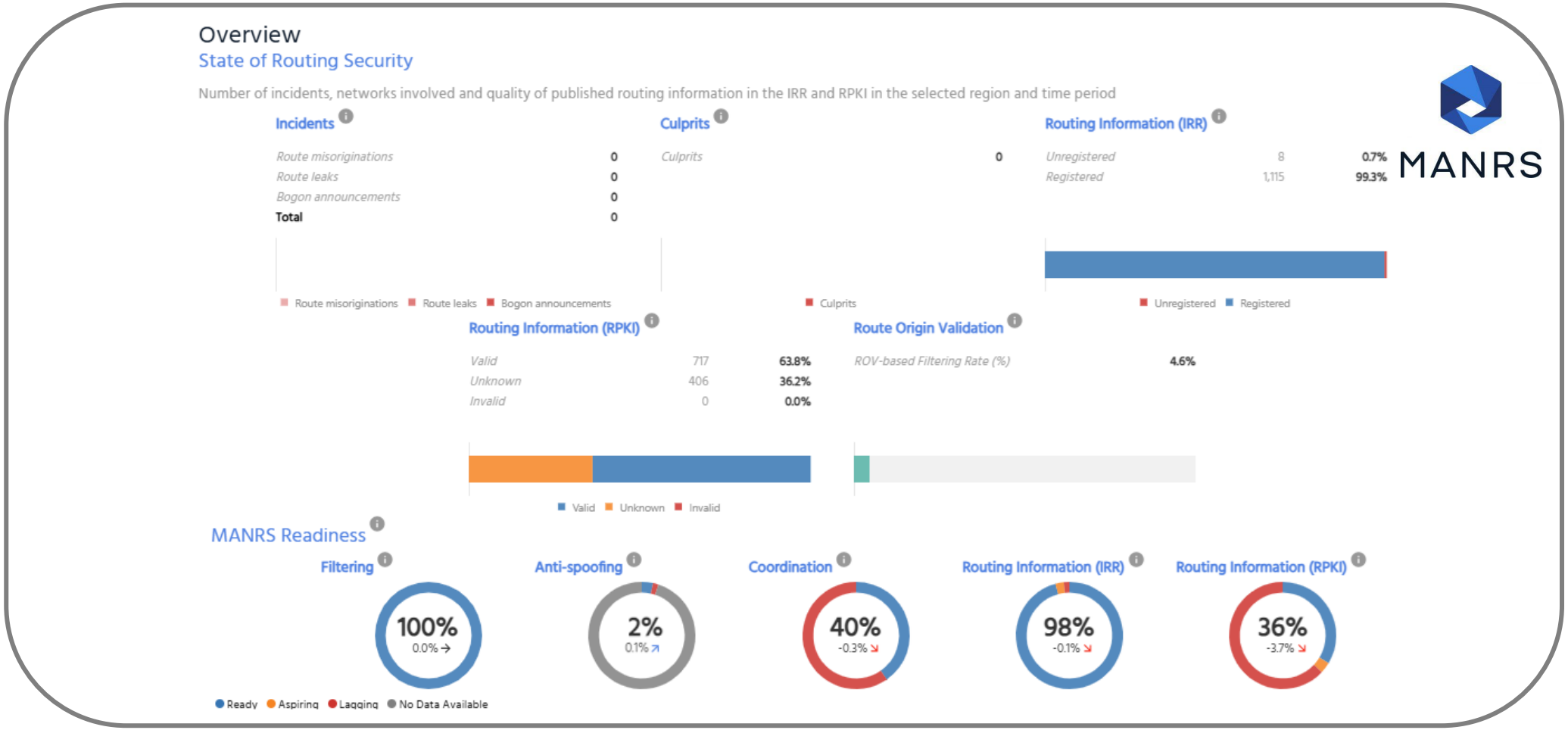


MANRS

https://bcp.nic.br/i+seg/acoes/

Programa por uma Internet mais Segura

MANRS Observatory – 126 AS – LJO SMA CSL

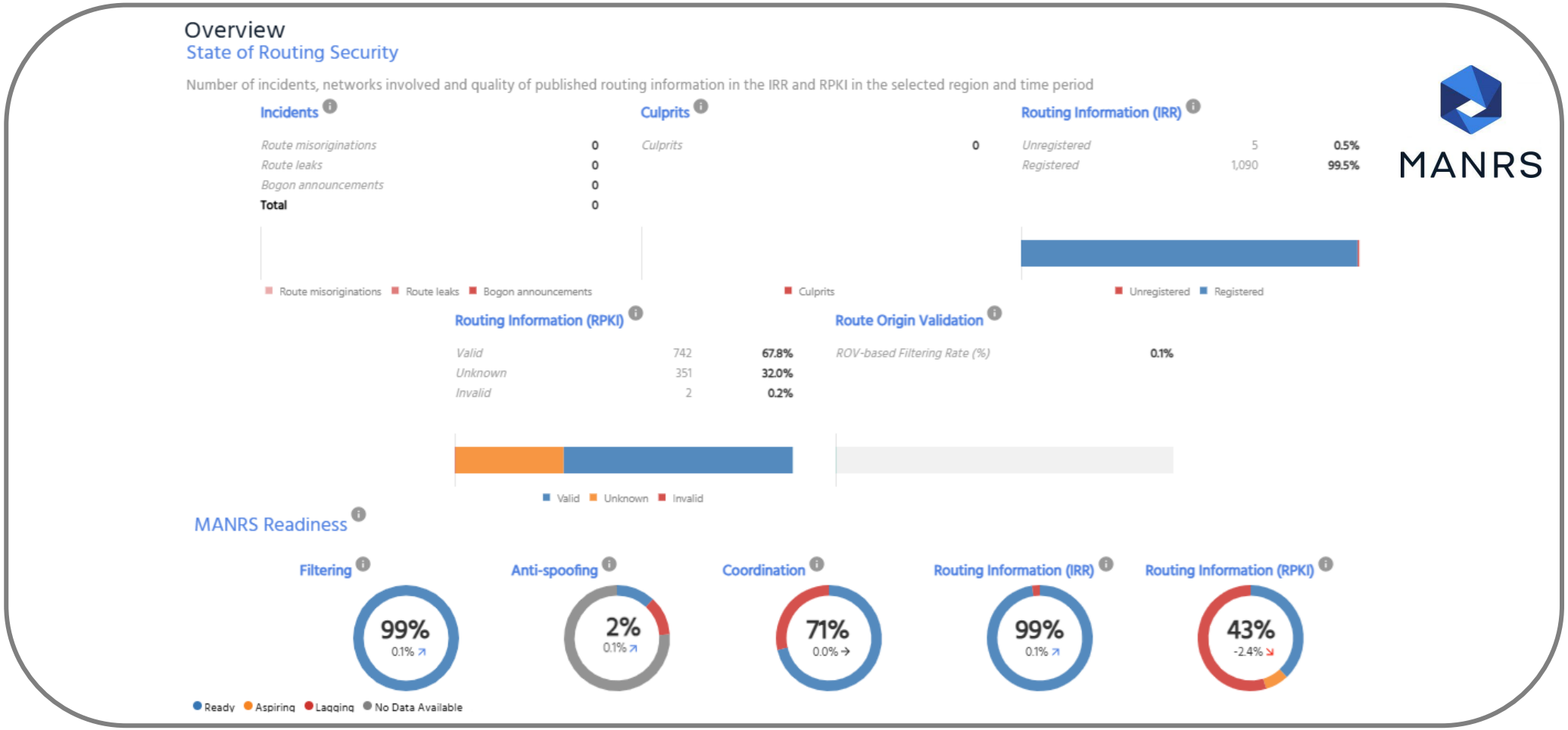


Programa por uma Internet mais Segura

MANRS Observatory – 126 AS – LJO SMA CSL

Programa por uma Internet mais Segura

MANRS Observatory – 42 AS – IX Fórum LJO



Programa por uma Internet mais Segura

MANRS Observatory – 42 AS – IX Fórum LJO

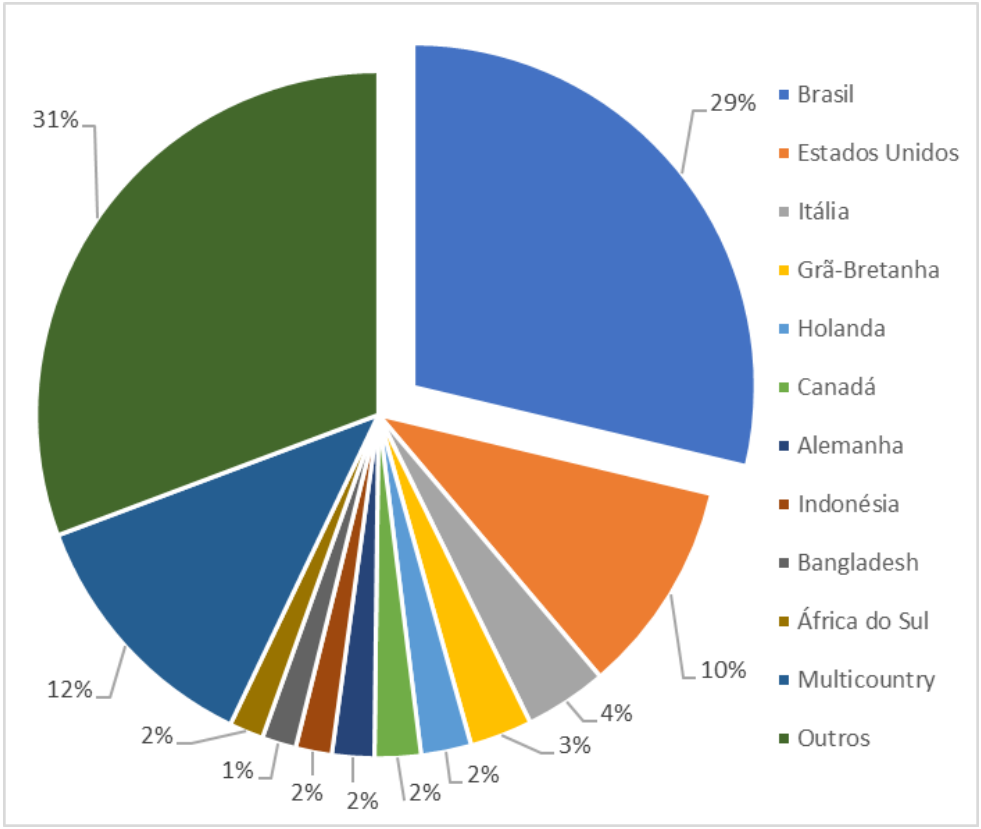
Programa por uma Internet mais Segura

Participantes por país

- Total: 1.052
- Participantes no Brasil → 302

MANRS

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



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

PROGRAMA INTERNET +SEGURA

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

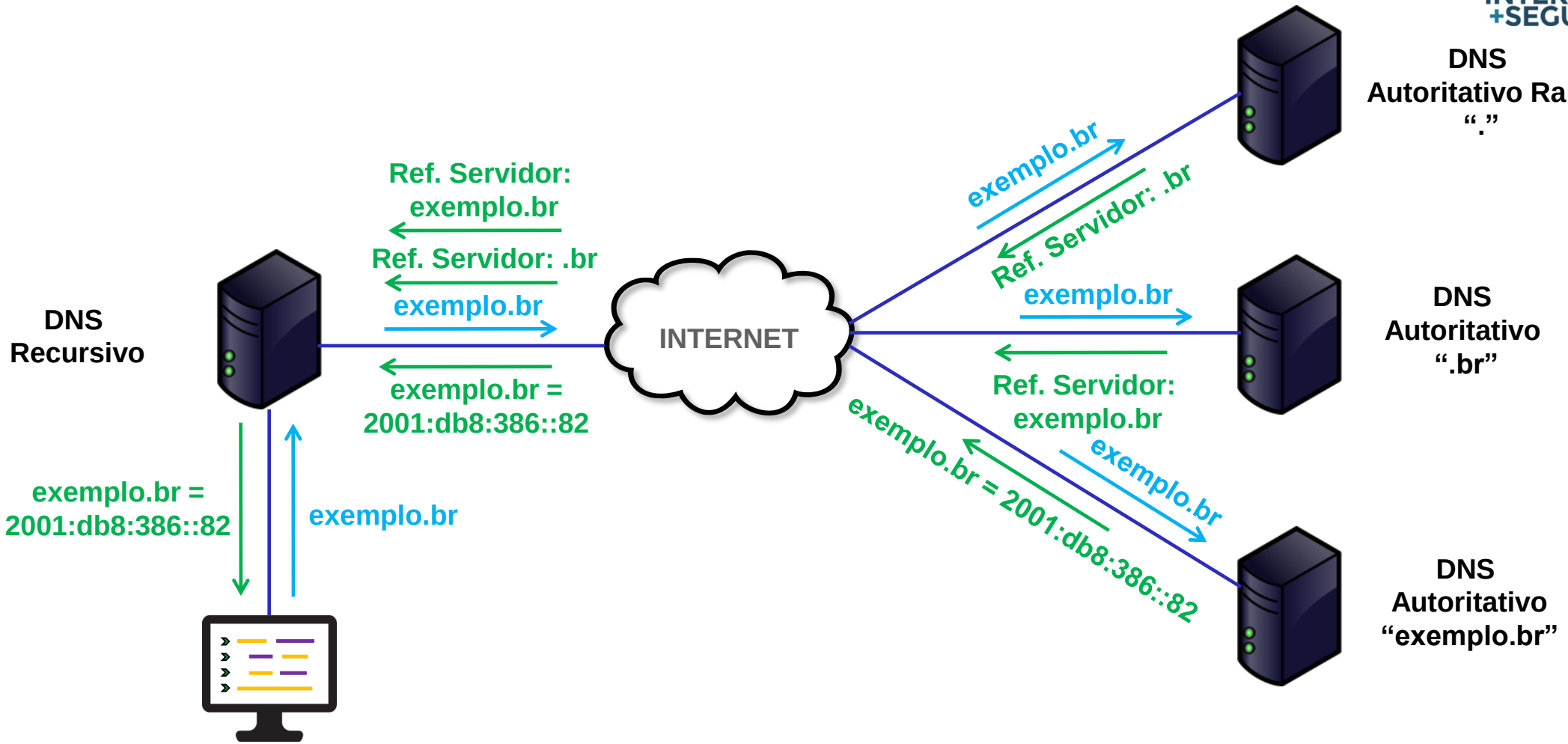
https://kindns.org/

An ICANN Initiative

ICANN

Programa por uma Internet mais Segura

Processo de Recursão DNS



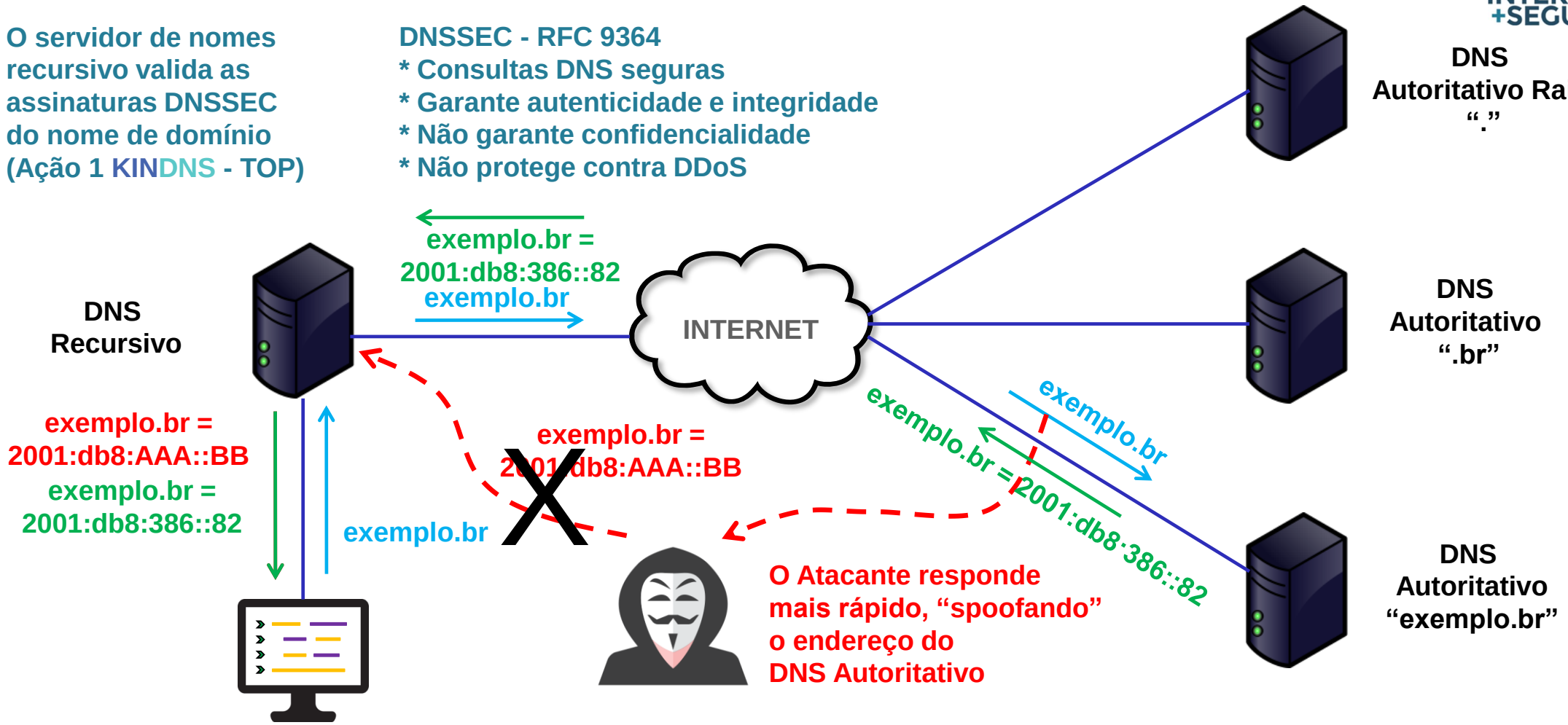
Fonte: [#SemanaCap 7] Curso - Configurando o seu DNS de forma simples e segura – Ataque DNS Poisoning

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



Fonte: [#SemanaCap 7] Curso - 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

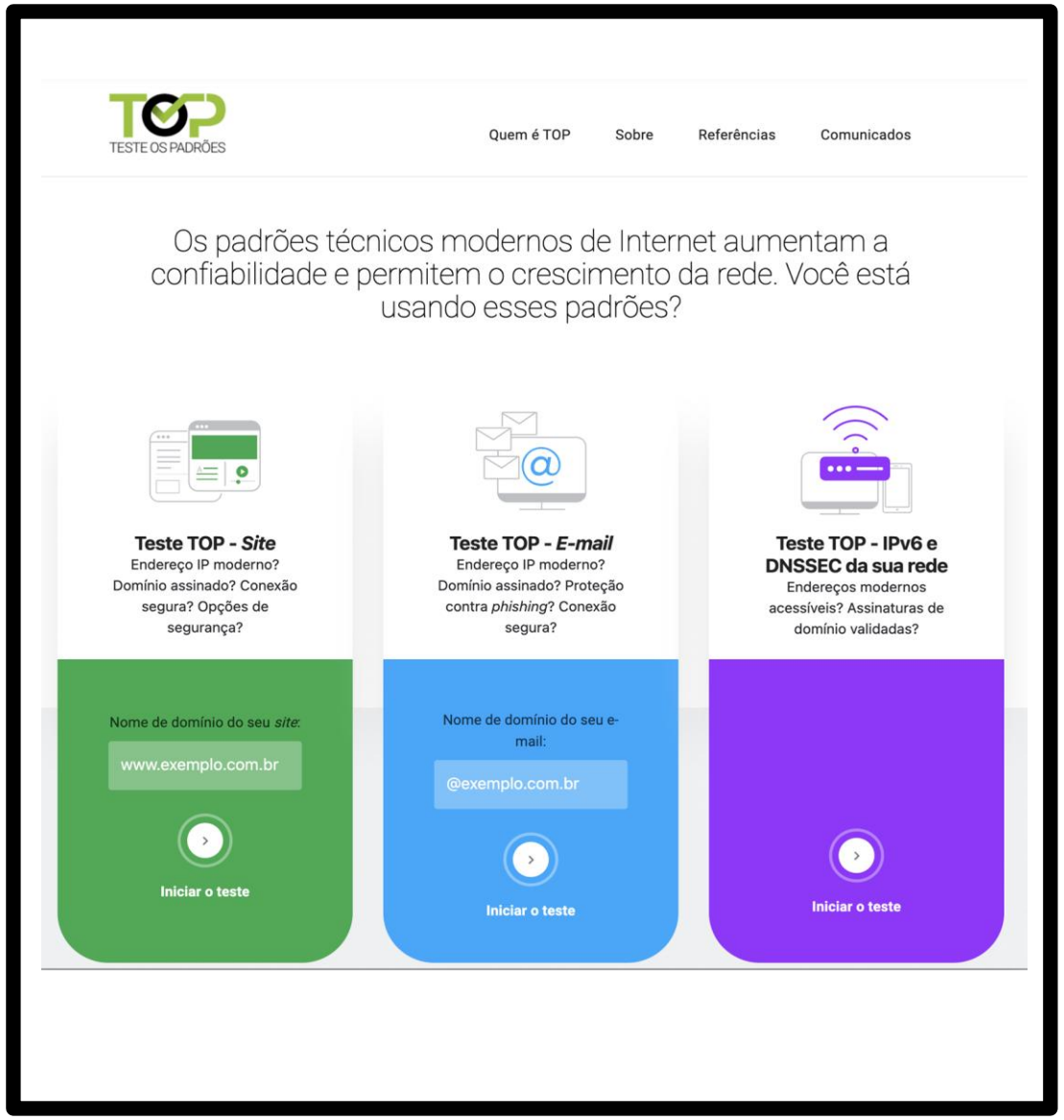
- KinDNS da ICANN (trocadilho em inglês)
- Configuração correta do recursivo somente para seus usuários
- Validação do DNSSEC no recursivo
- Configuração do autoritativo do seu nome de domínio com DNSSEC

https://kindns.org/

KINDNS

PROGRAMA INTERNET +SEGURA

https://top.nic.br



Programa por uma Internet mais Segura

PROGRAMA INTERNET +SEGURA

TOP - 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!

https://top.nic.br

Programa por uma Internet mais Segura

TOP - Teste os padrões – Interface do usuário

- Operação IPv6 no usuário
- Validação DNSSEC pelo servidor DNS recursivo
- Resolução de nomes IPv6

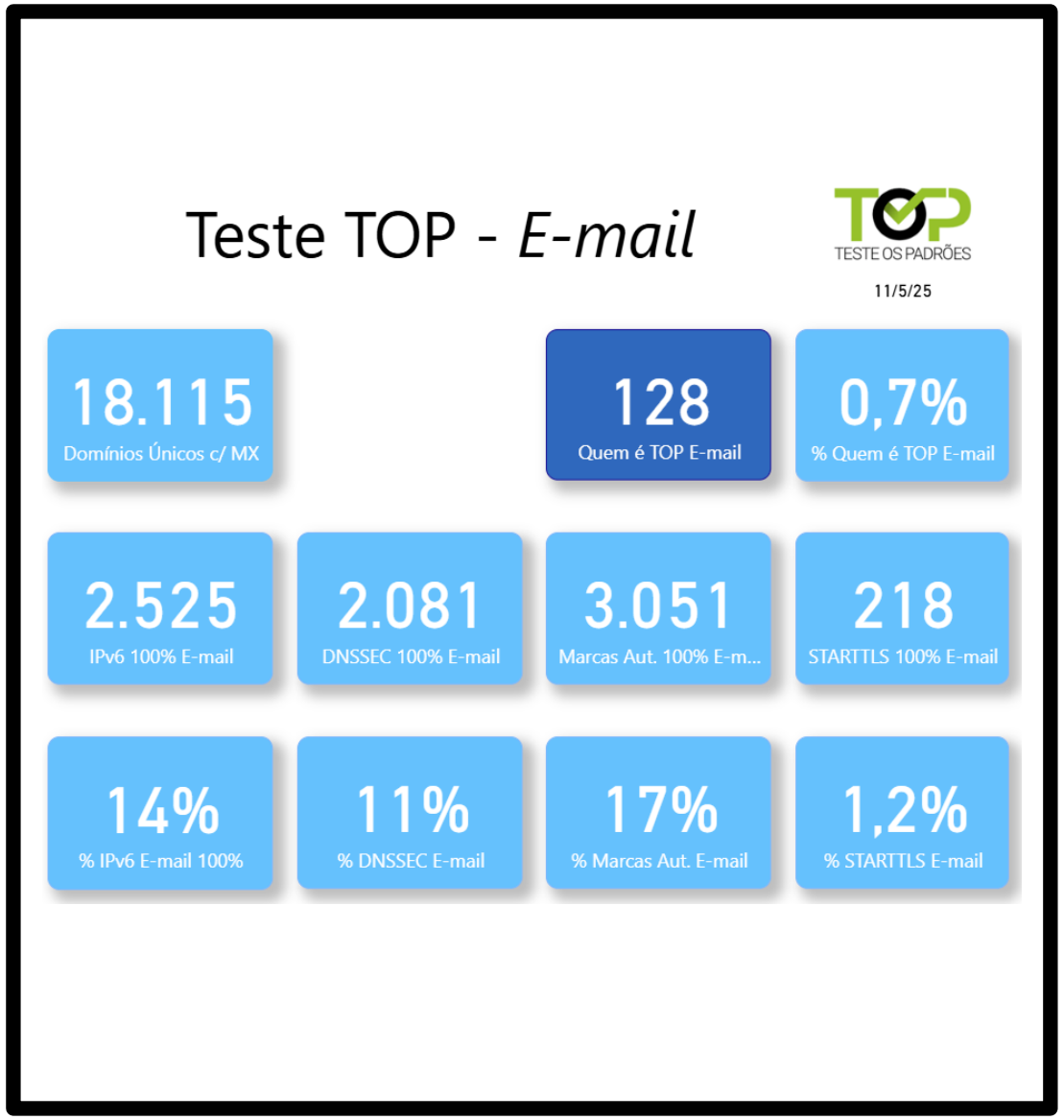
https://top.nic.br

Programa por uma Internet mais Segura

TOP - Teste os padrões - *Site*

- Domínios únicos testados
- Quem é TOP *Site*
- IPv6
- Domínios Assinados
- Implementação HTTPS
- Opções de Segurança
- RPKI

https://top.nic.br



Programa por uma Internet mais Segura

PROGRAMA INTERNET +SEGURA

TOP - Teste os padrões – *E-mail*

- Domínios únicos testados
- Quem é TOP *E-mail*
- IPv6
- Domínios Assinados
- Implementação de STARTTLS
- Marcas Segurança (DMARC, DKIN, SPF)
- RPKI

https://top.nic.br

Programa por uma Internet mais Segura
Implemente as melhores práticas

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

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

16 de maio de 2025

nic.br cgi.br

www.nic.br | www.cgi.br