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

Segurança de Redes

Programa por uma Internet mais segura

Gilberto Zorello | gzorello@nic.br

IX Fórum Edição Norte

Manaus, AM | 23/08/24

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
- Divulgar melhores práticas de segurança
- Aumentar a cultura de segurança

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

PROGRAMA INTERNET +SEGURA

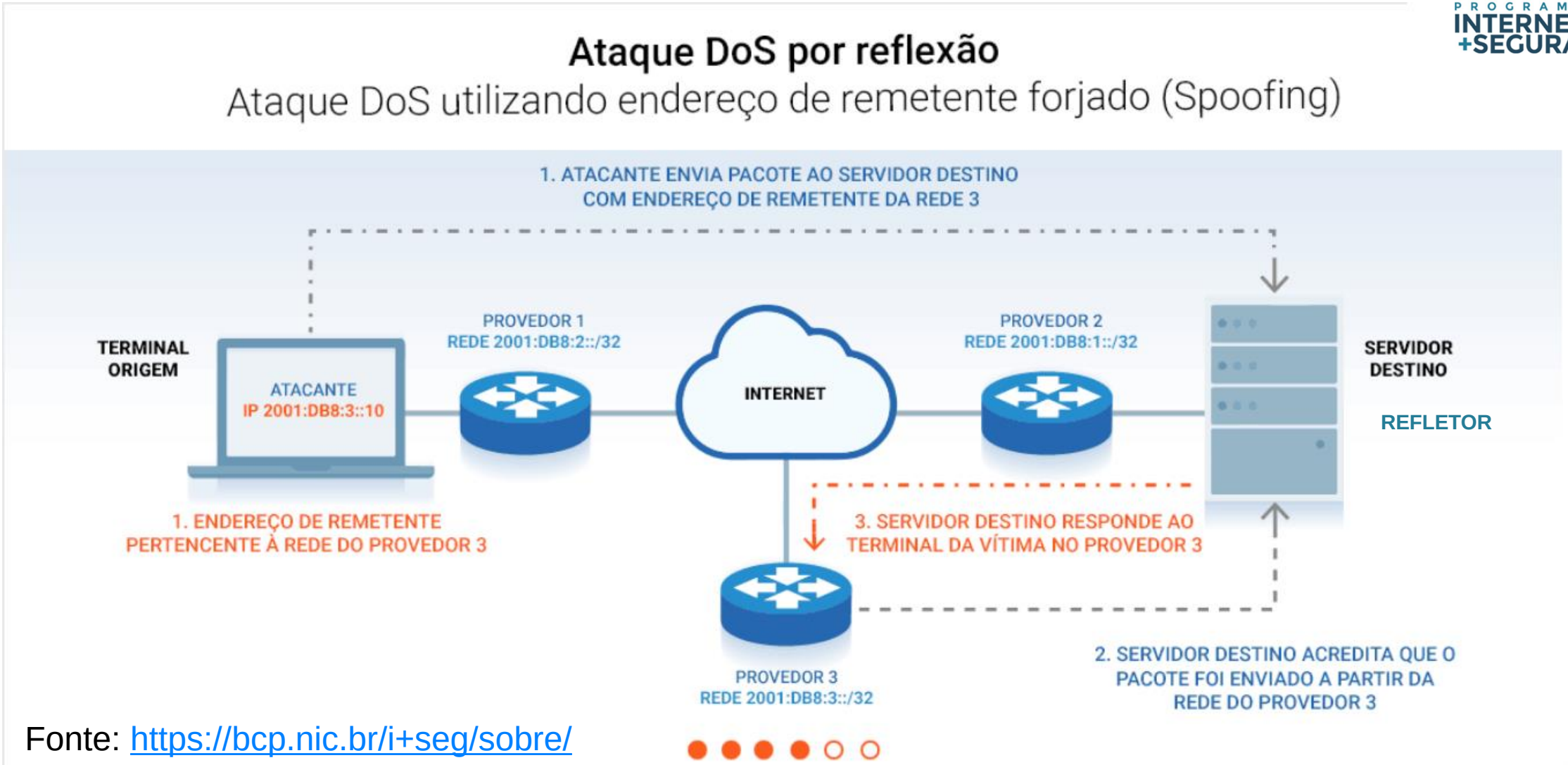
https://bcp.nic.br/i+seg

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



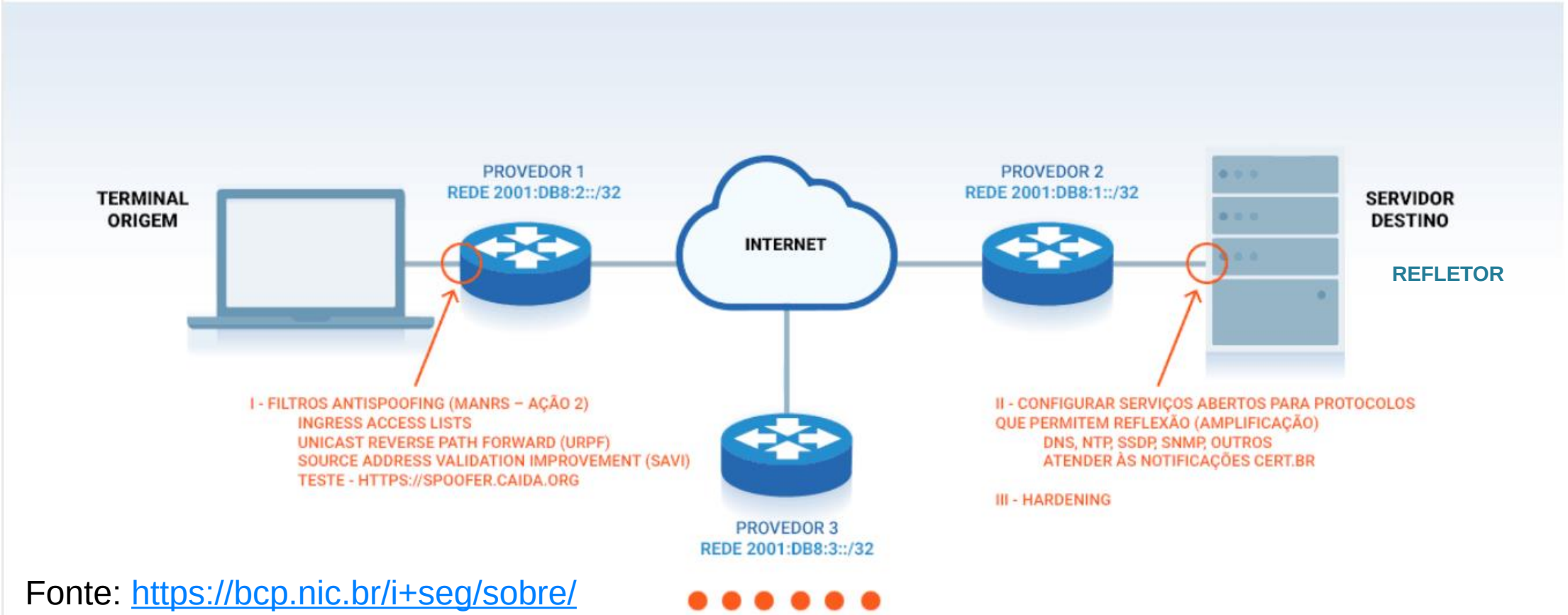
Fonte: https://bcp.nic.br/i+seg/sobre/

Programa por uma Internet mais Segura

PROGRAMA INTERNET +SEGURA

Ataque DoS por reflexão

Solução: Aplicação de filtros antispoofing, configuração de serviços e Hardening

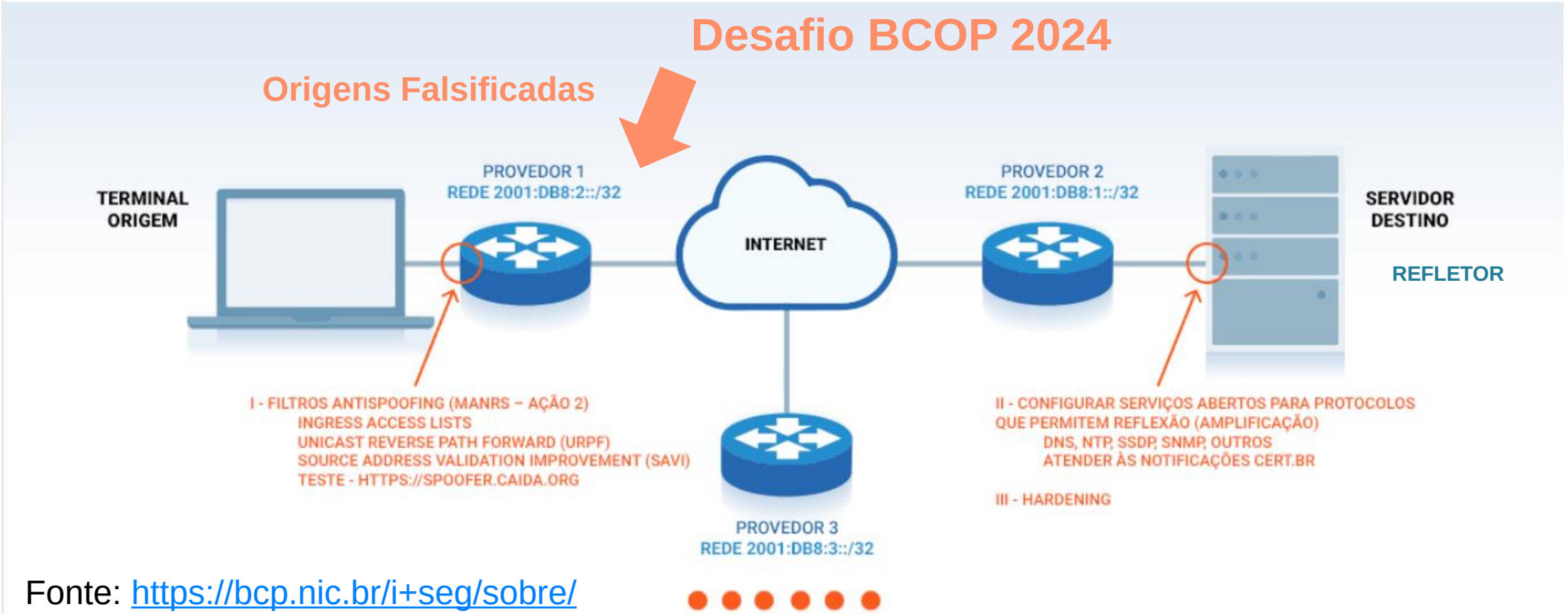


Fonte: https://bcp.nic.br/i+seg/sobre/

Programa por uma Internet mais Segura

Ataque DoS por reflexão

Solução: Aplicação de filtros antispoofing, configuração de serviços e Hardening

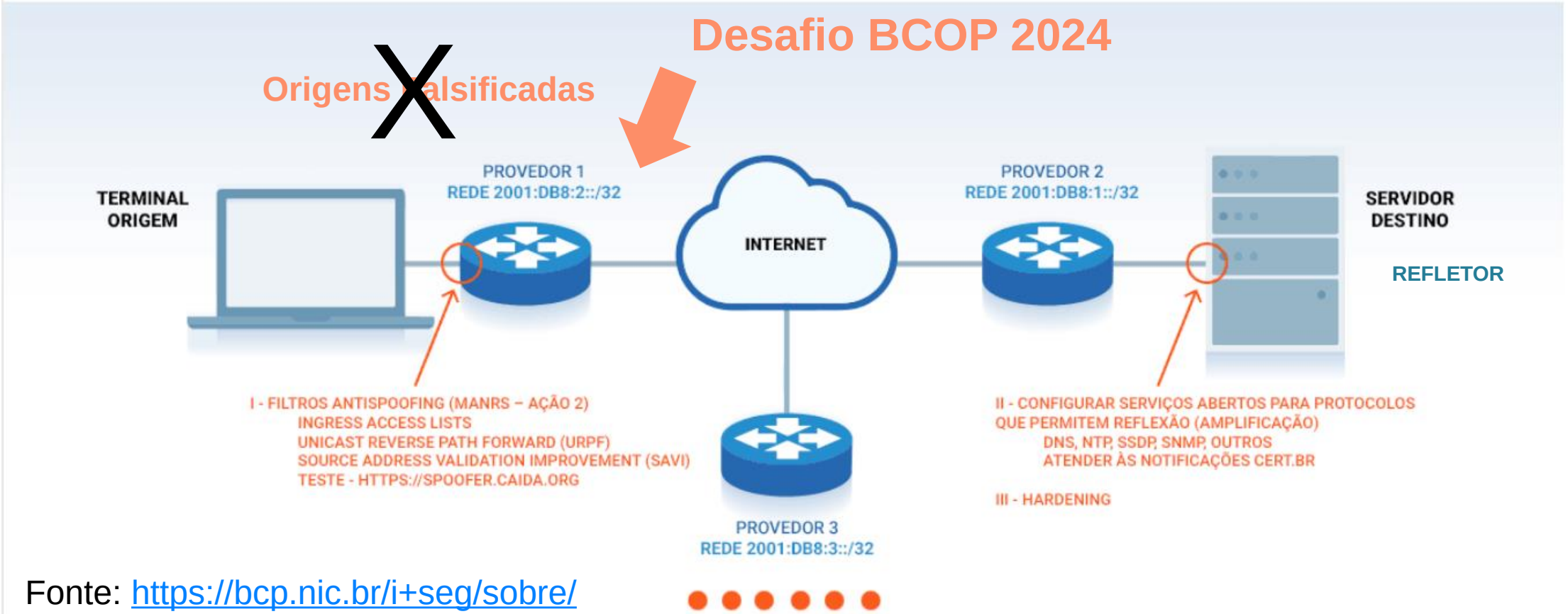


Fonte: https://bcp.nic.br/i+seg/sobre/

Programa por uma Internet mais Segura

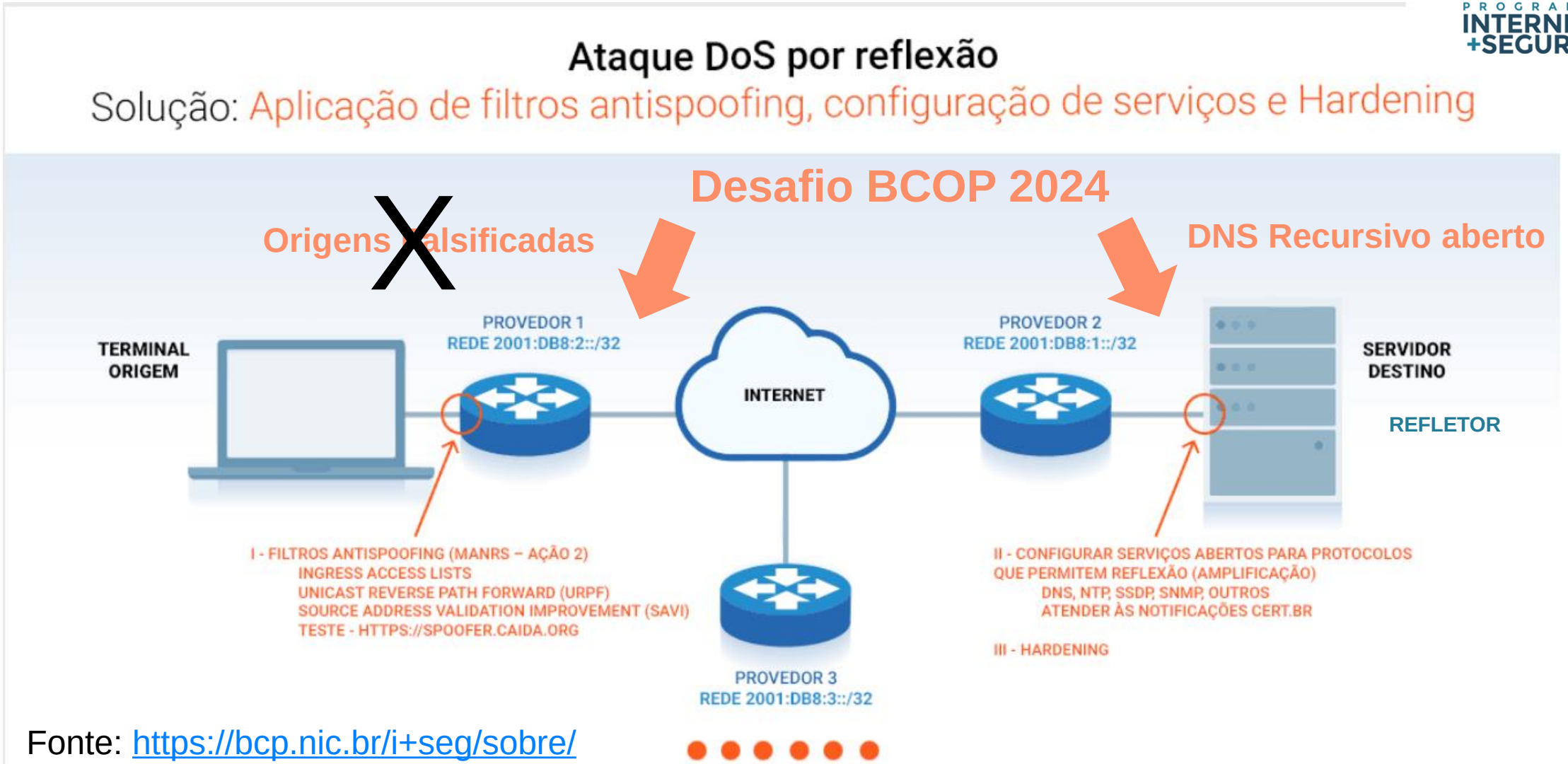
Ataque DoS por reflexão

Solução: Aplicação de filtros antispoofing, configuração de serviços e Hardening



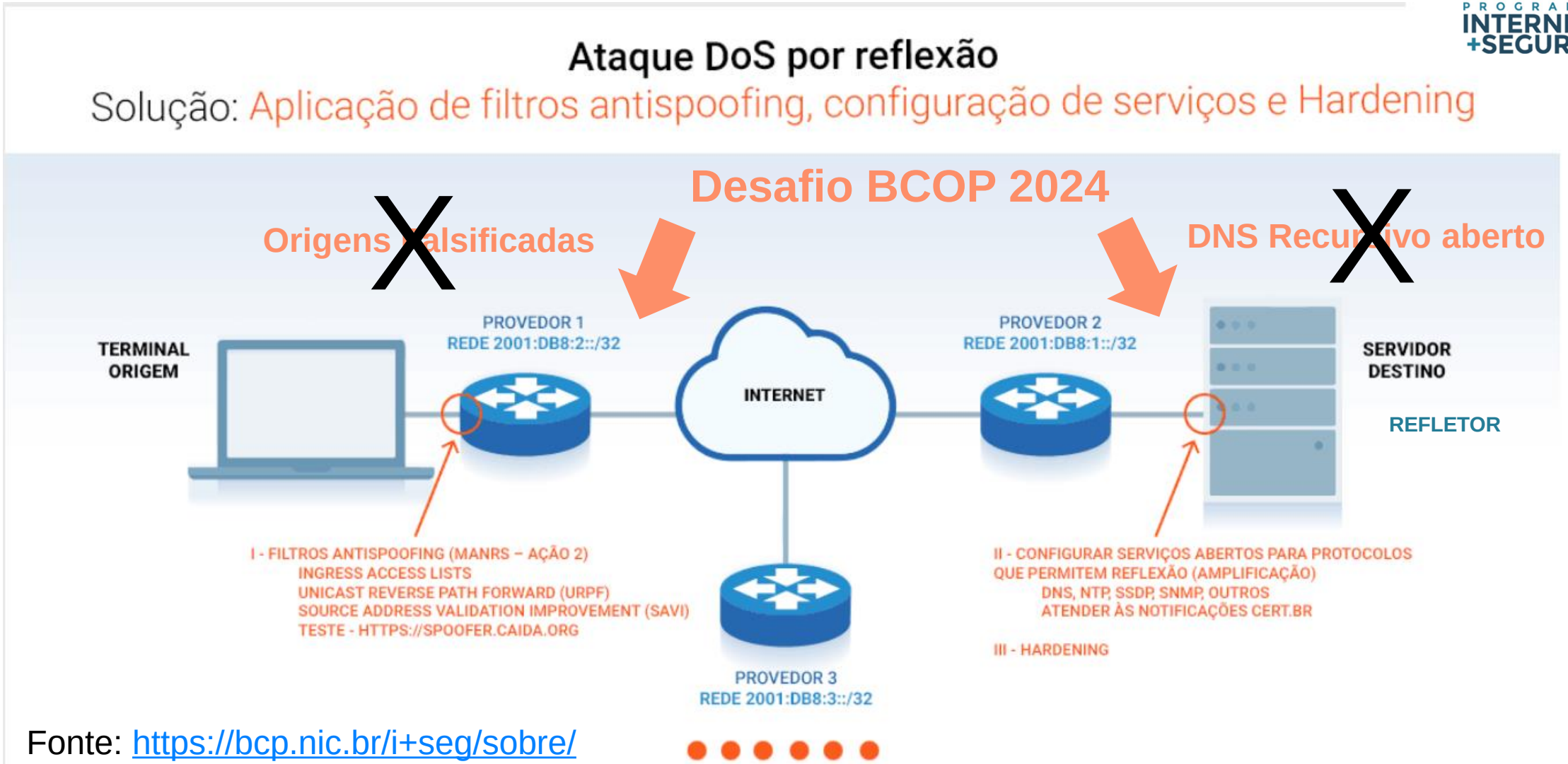
Fonte: https://bcp.nic.br/i+seg/sobre/

Programa por uma Internet mais Segura



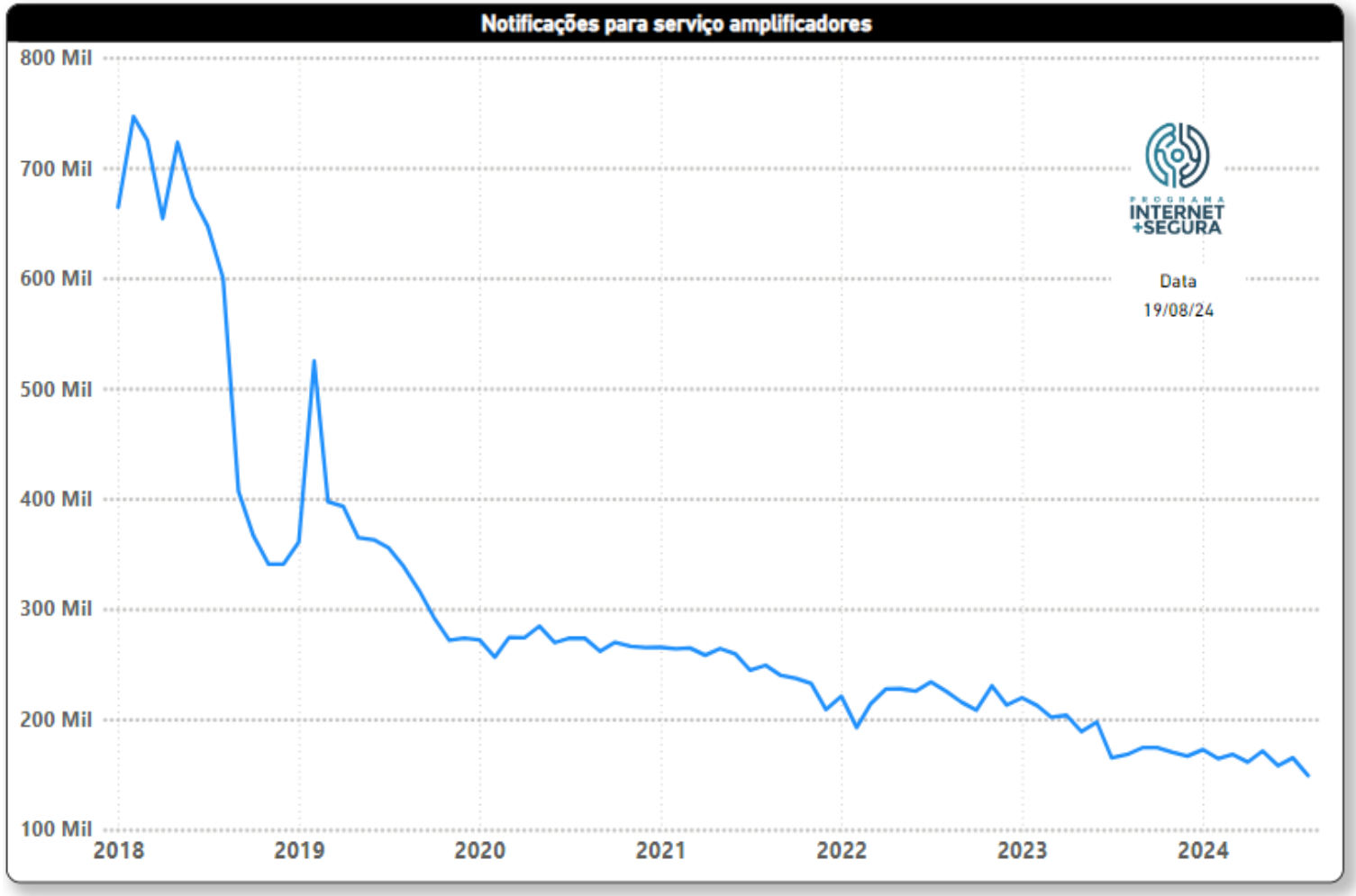
Fonte: https://bcp.nic.br/i+seg/sobre/

Programa por uma Internet mais Segura



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

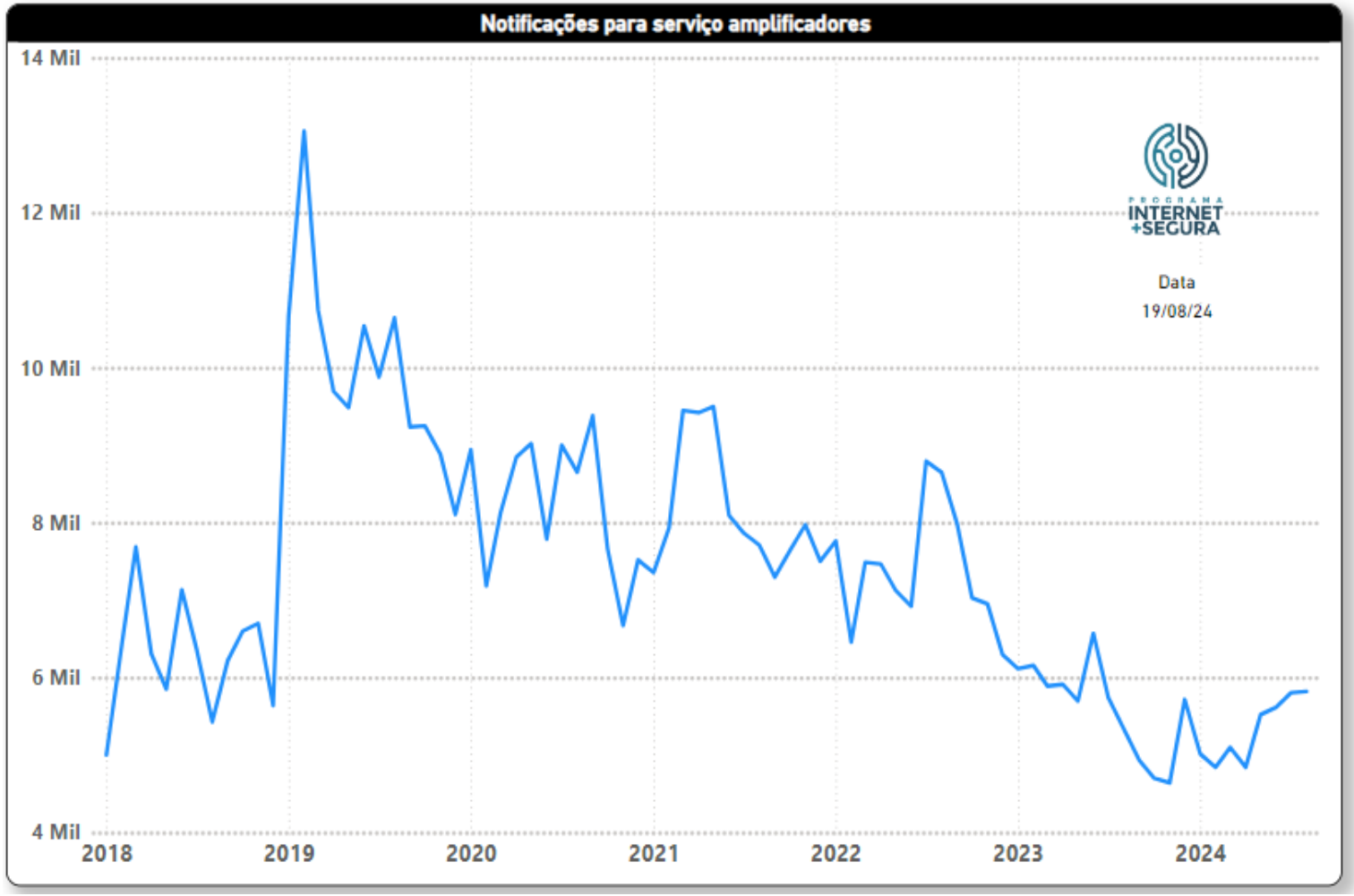
Programa por uma Internet mais Segura
Notificação de amplificadores - evolução



Brasil

- Início (fev/2018)
  - Endereços IP: 746.508
  - Serviços: 5
- Atual:
  - Endereços IP: 150.670
  - Serviços: 19
  - **Redução de 80%**

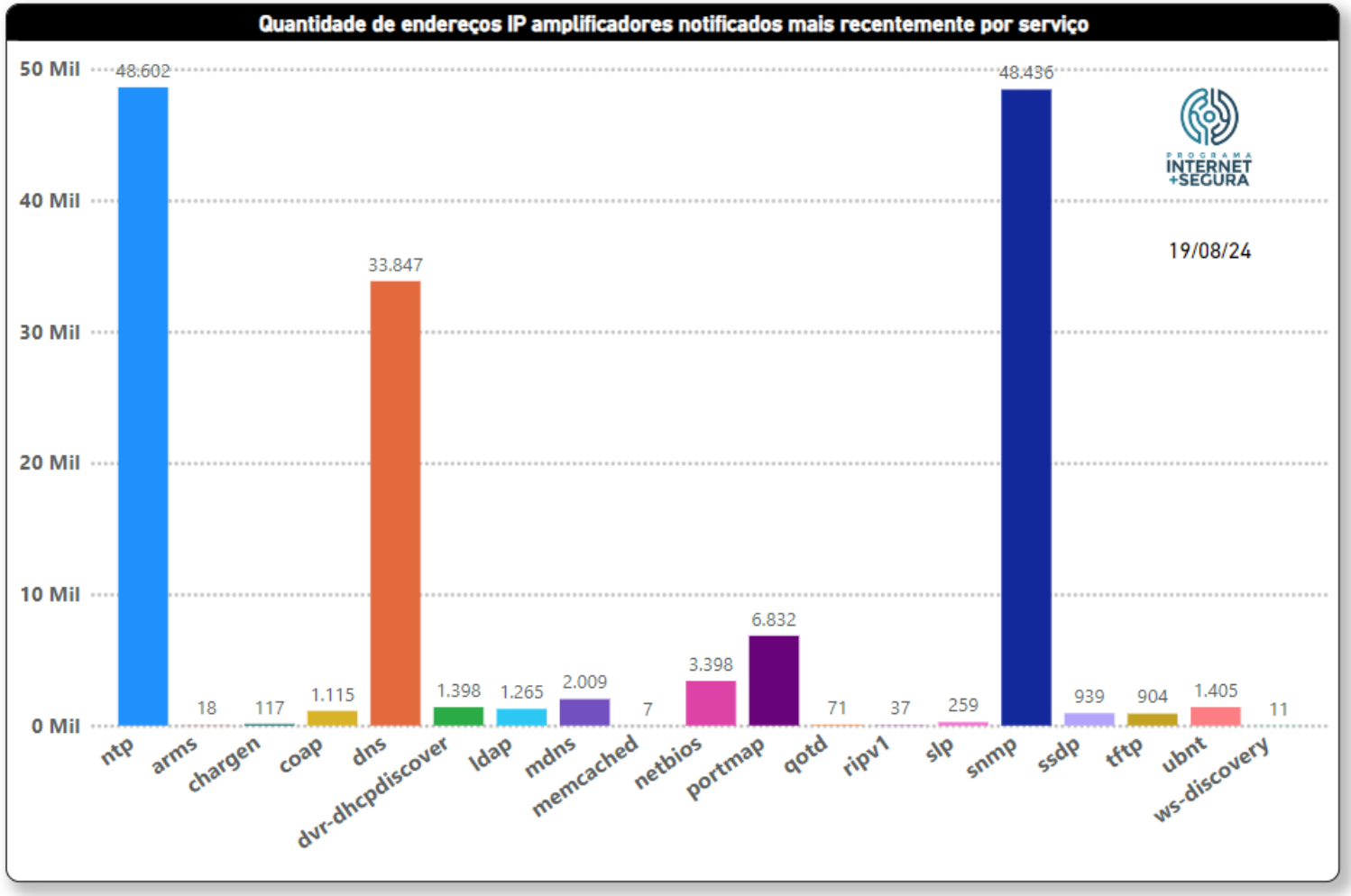
Programa por uma Internet mais Segura
Notificação de amplificadores - evolução



Região Norte

- Pico (fev/2019)
  - Endereços IP: 13.053
  - Serviços: 12
- Atual:
  - Endereços IP: 5.842
  - Serviços: 16

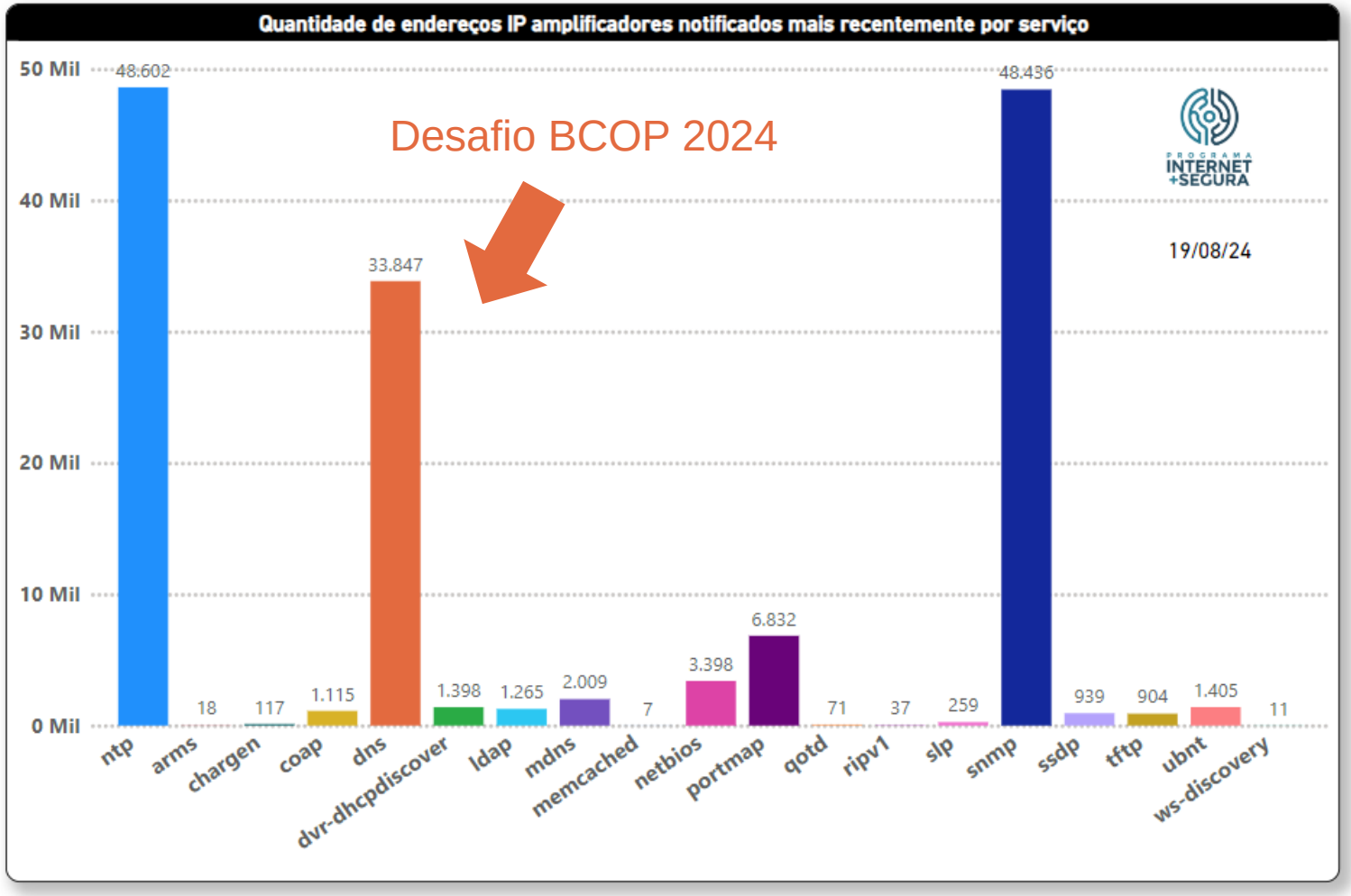
Programa por uma Internet mais Segura
Notificação de amplificadores - serviços



Brasil

- 5241 AS notificados
- 150670 endereços IP mal configurados
  - SNMP 48436
  - DNS 33847
  - NTP 48602

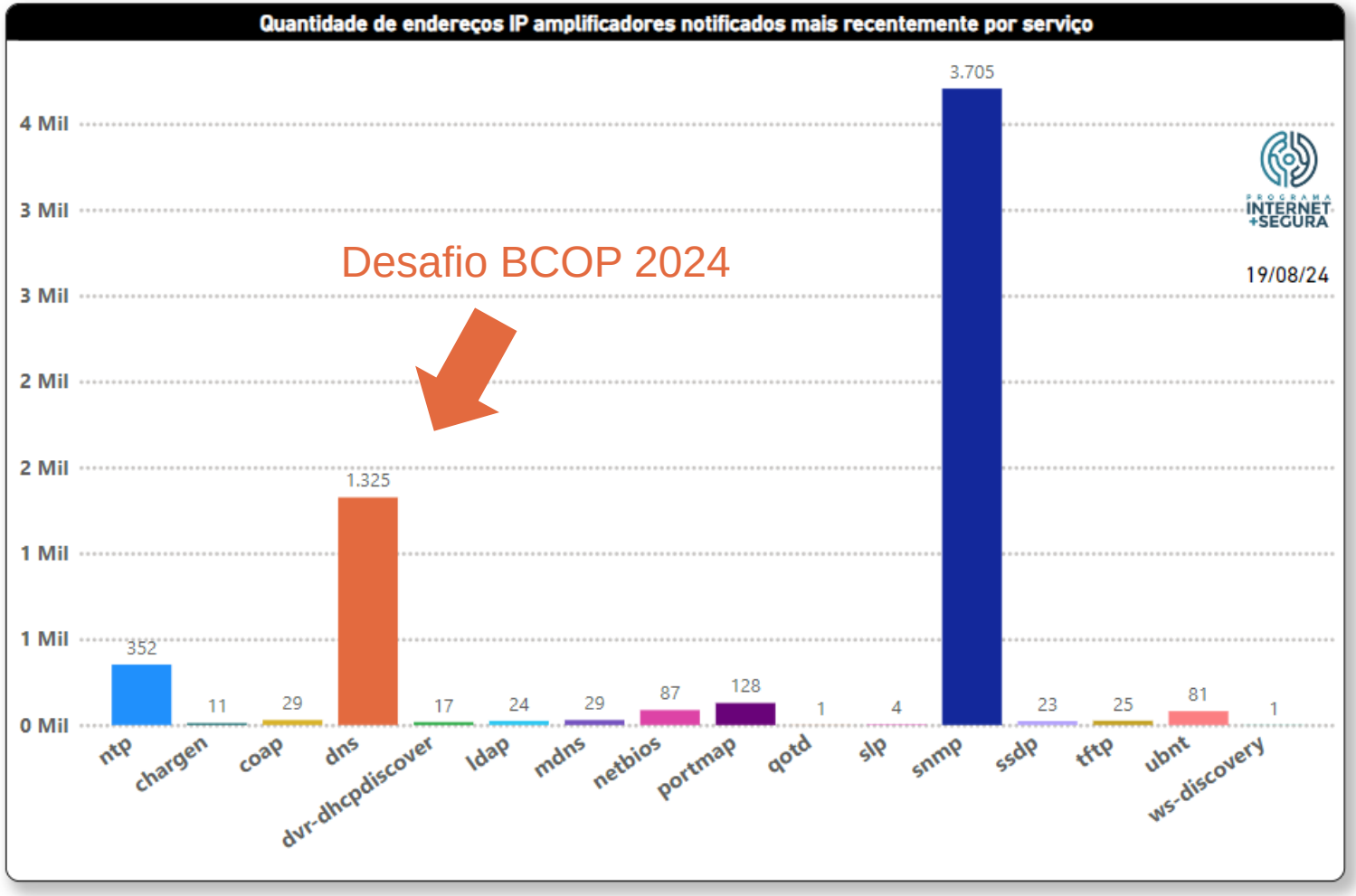
Programa por uma Internet mais Segura
Notificação de amplificadores - serviços



Brasil

- 5241 AS notificados
- 150670 endereços IP mal configurados
  - SNMP 48436
  - DNS 33847
  - NTP 48602

Programa por uma Internet mais Segura
Notificação de amplificadores - serviços



Região Norte

- 342 AS notificados
- 5842 endereços IP mal configurados
  - SNMP 3705
  - DNS 1325
  - NTP 352

MANRS

PROGRAMA INTERNET +SEGURA

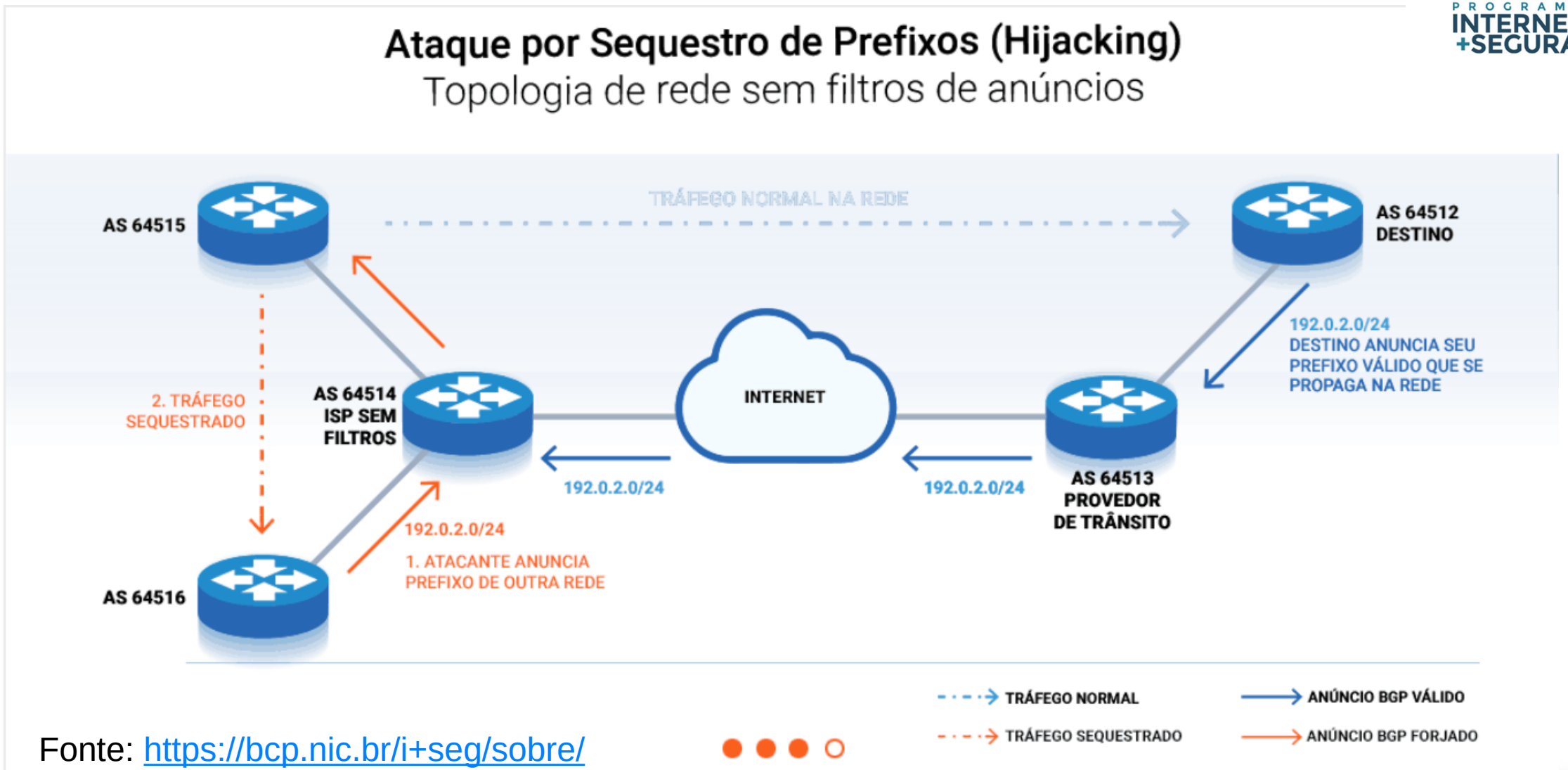
Mutually Agreed Norms for Routing Security

http://manrs.org

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

Programa por uma Internet mais Segura

PROGRAMA INTERNET +SEGURA



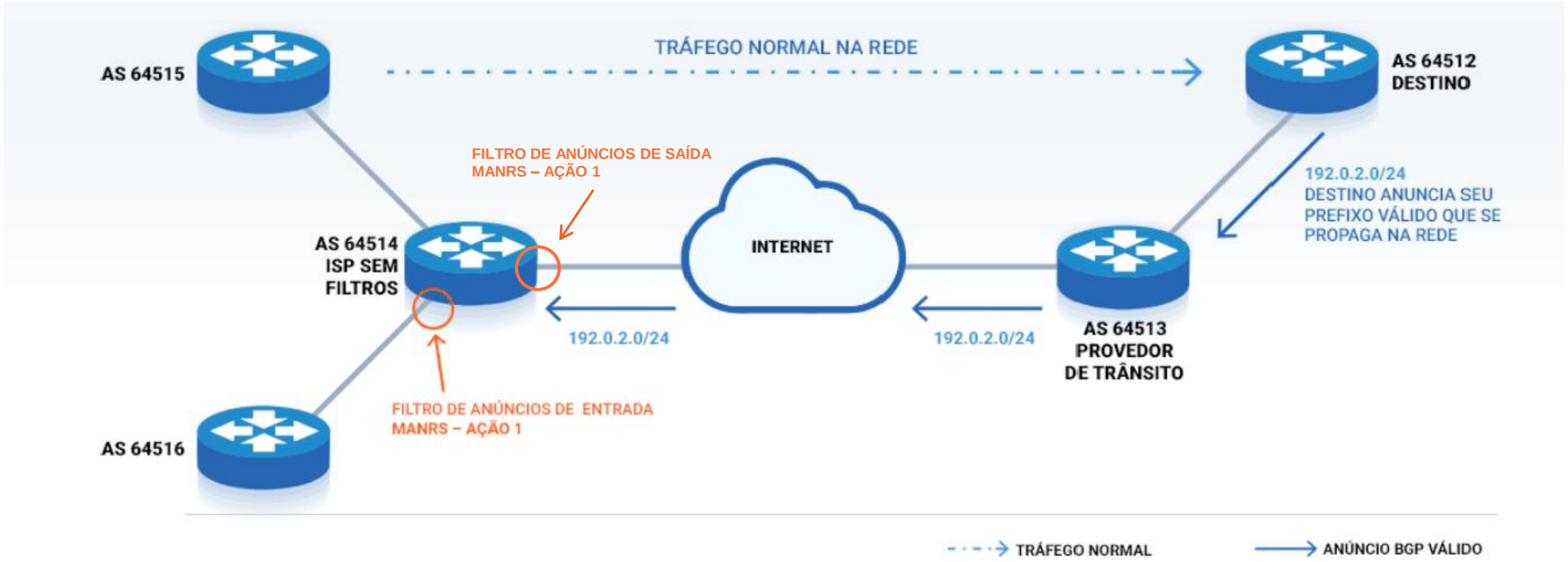
Fonte: https://bcp.nic.br/i+seg/sobre/

Programa por uma Internet mais Segura

PROGRAMA INTERNET +SEGURA

Ataque por Sequestro de Prefixos (Hijacking)

Solução: Filtro de anúncios de entrada (clientes) – MANRS - Ação 1



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

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

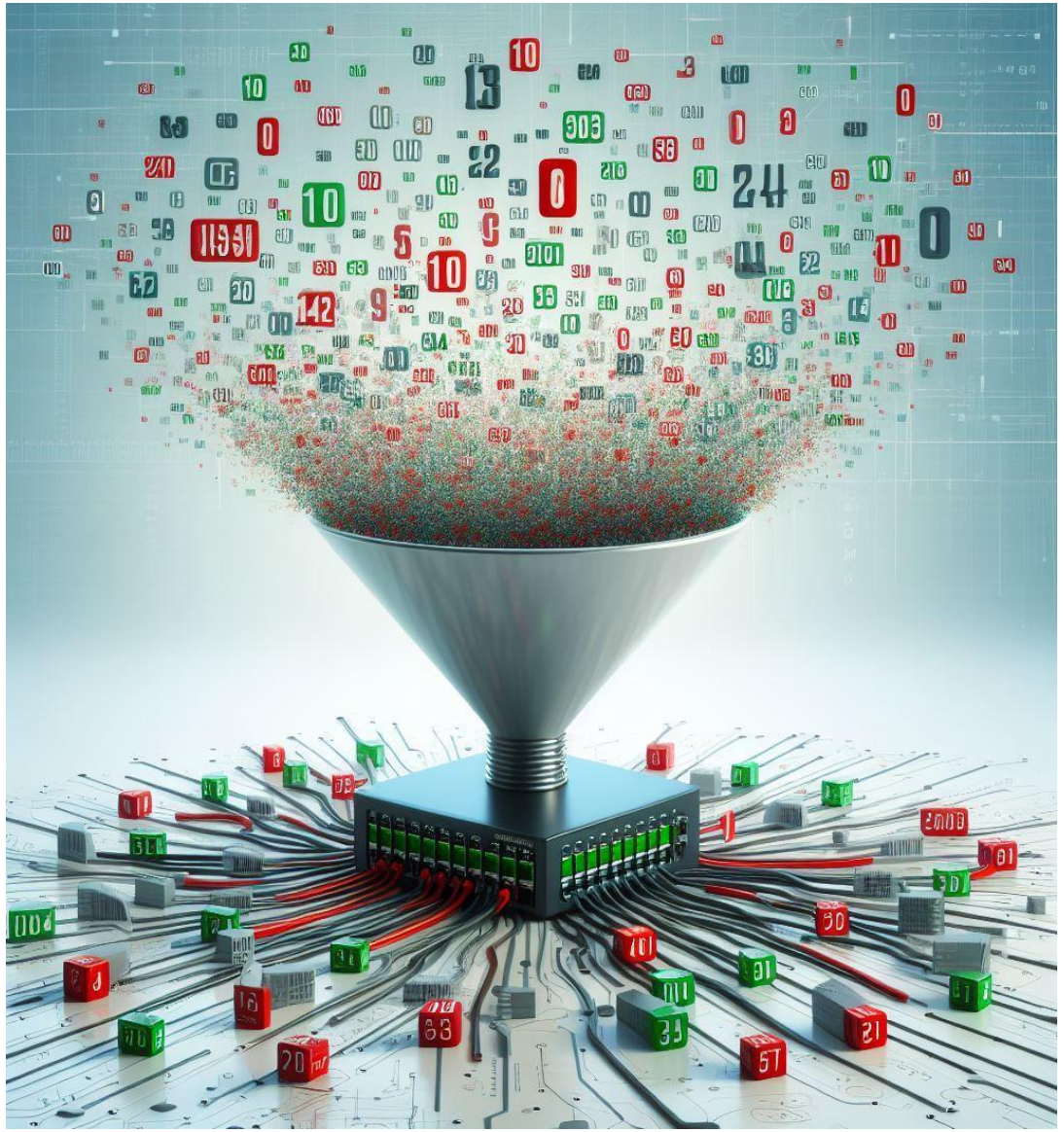
MANRS https://bcp.nic.br/i+seg/acoes/manrs/

Programa por uma Internet mais Segura

MANRS - Ação 1 - Impedir a propagação de informações incorretas no BGP

- Implemente filtros no BGP para os seus prefixos e dos seus clientes

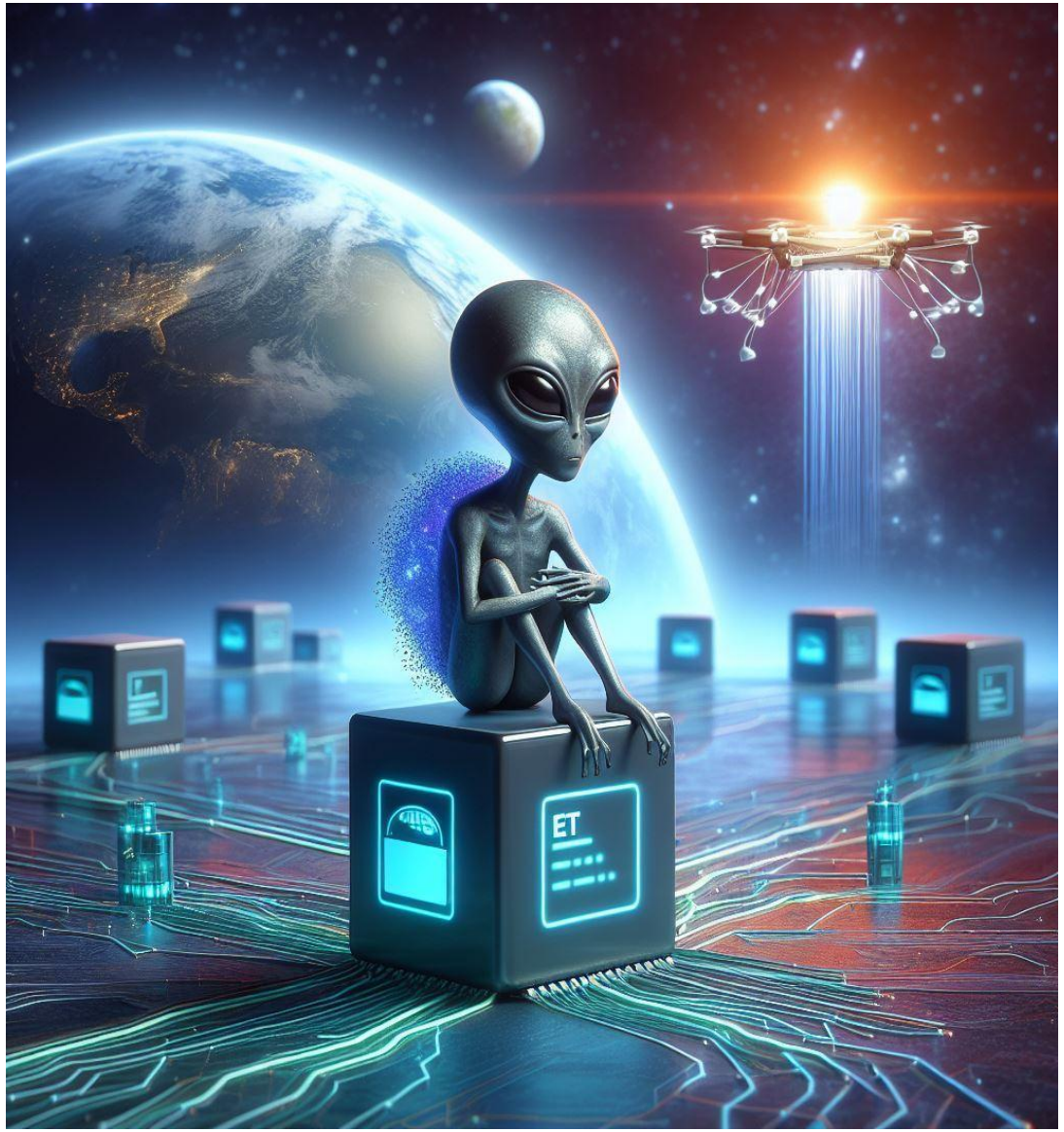
https://bcp.nic.br/i+seg/acoes/manrs/#filtragem-de-rotas



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

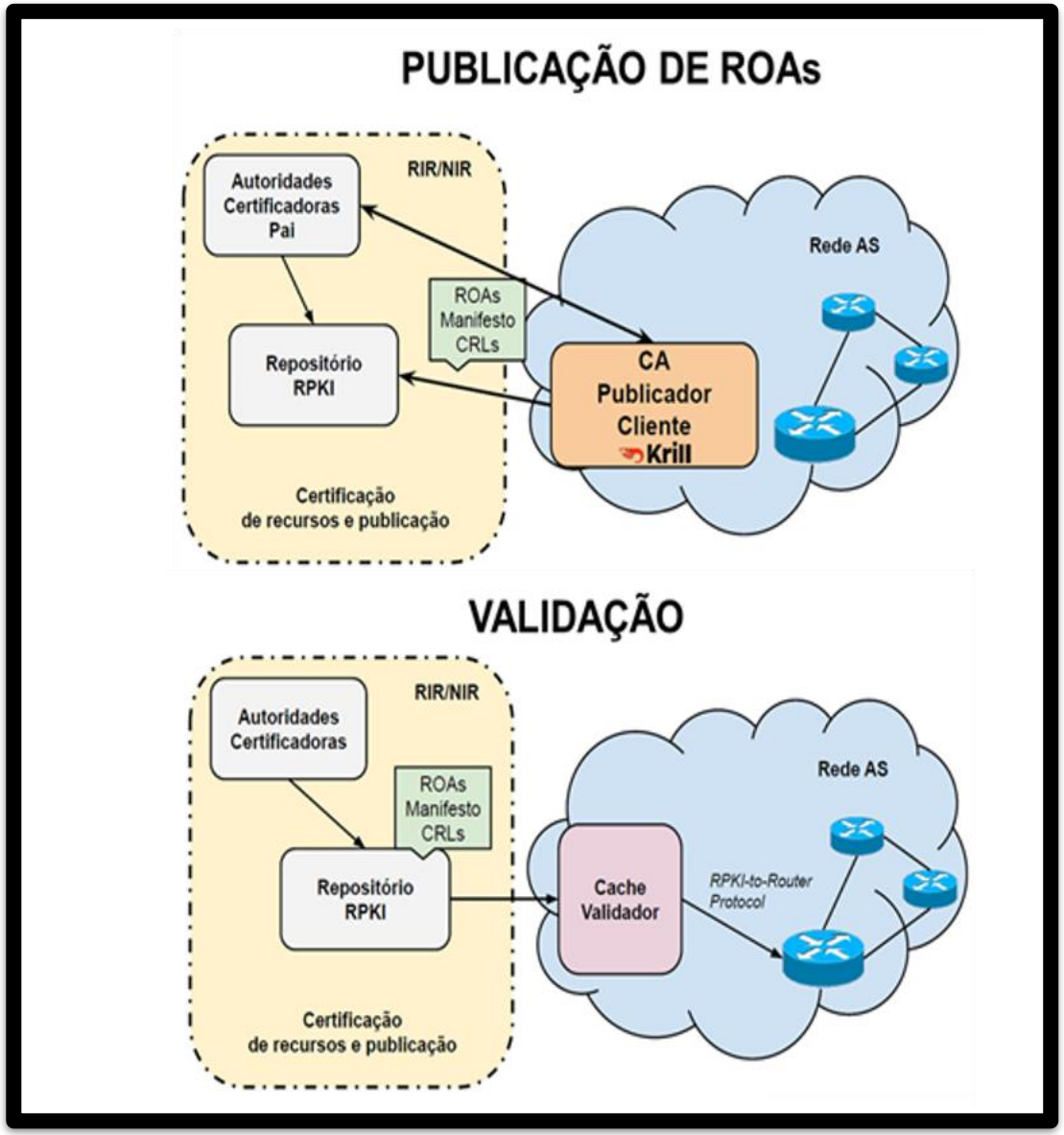
MANRS - Ação 4 - Cadastro da Política de Roteamento

- **IRR** - Internet Routing Registry
  - RADB
  - TC (gratuito)

- **RPKI** - Resource Public Key Infrastructure

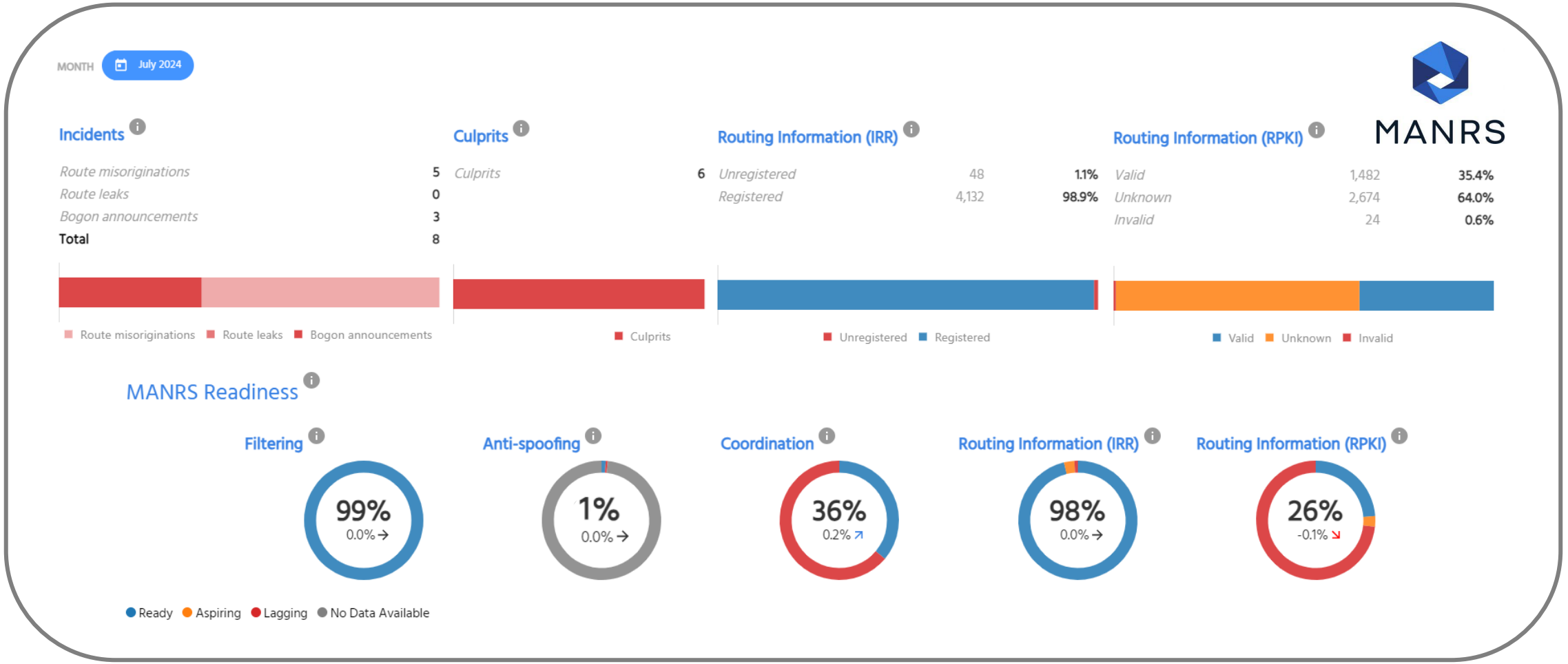
MANRS

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



Programa por uma Internet mais Segura

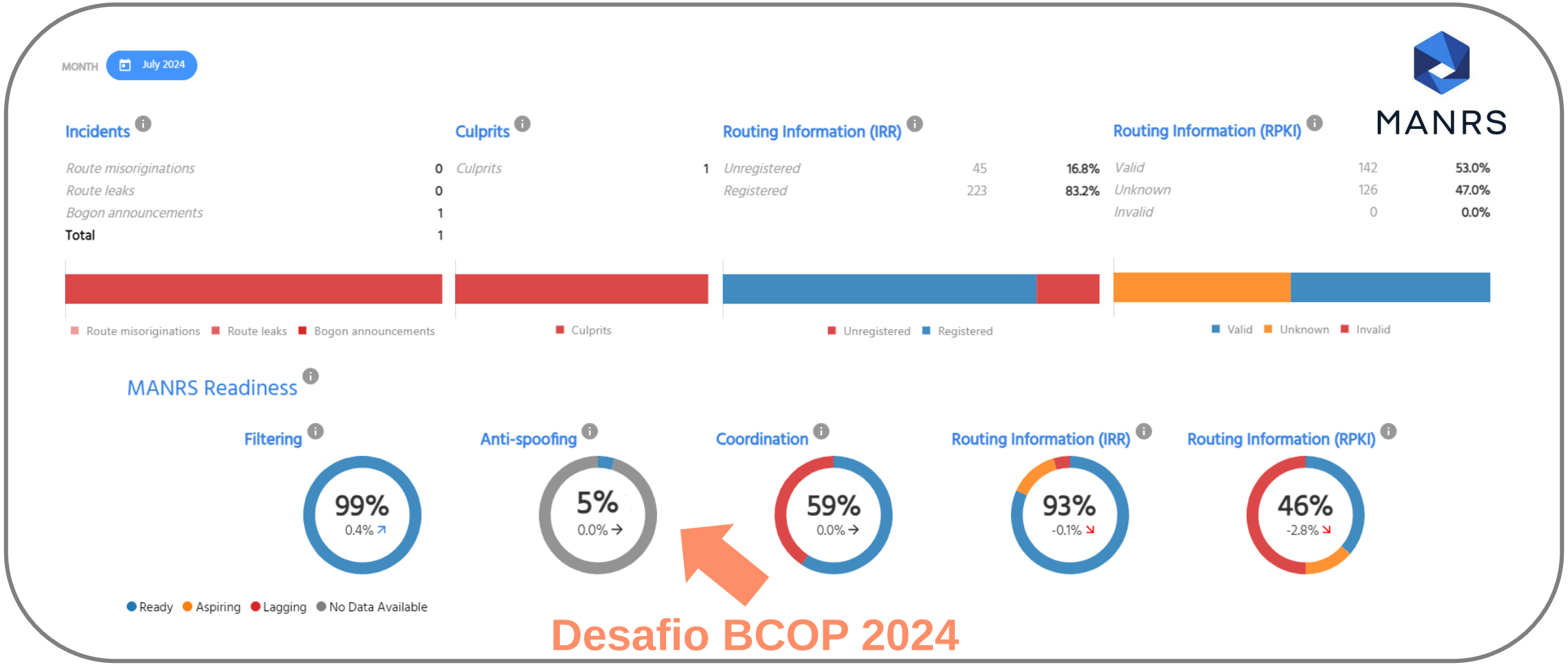
MANRS Observatory - 545 AS - NO



Programa por uma Internet mais Segura

MANRS Observatory - 545 AS - NO

Programa por uma Internet mais Segura
MANRS Observatory - 23 AS – Part. IX NO



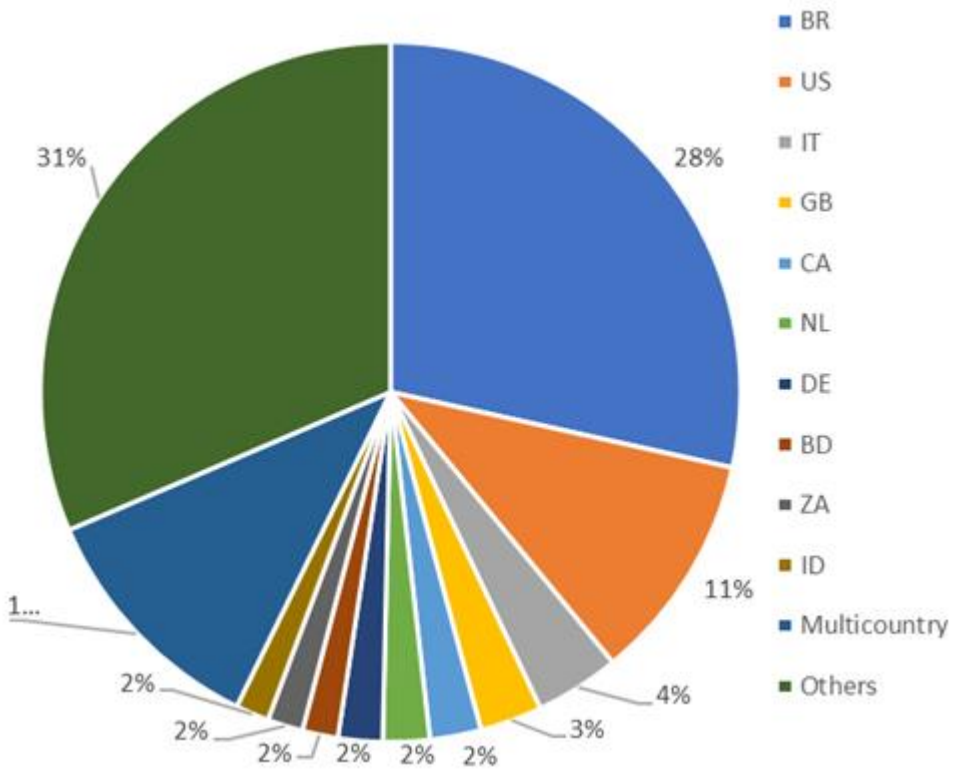
Programa por uma Internet mais Segura

Participantes por país

- Total: 973
- Participantes no Brasil → 277 (ago/24)

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

MANRS



Fonte: https://www.manrs.org/netops/participants/ Acesso ago/24

PROGRAMA INTERNET +SEGURA

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

https://kindns.org/

An ICANN Initiative

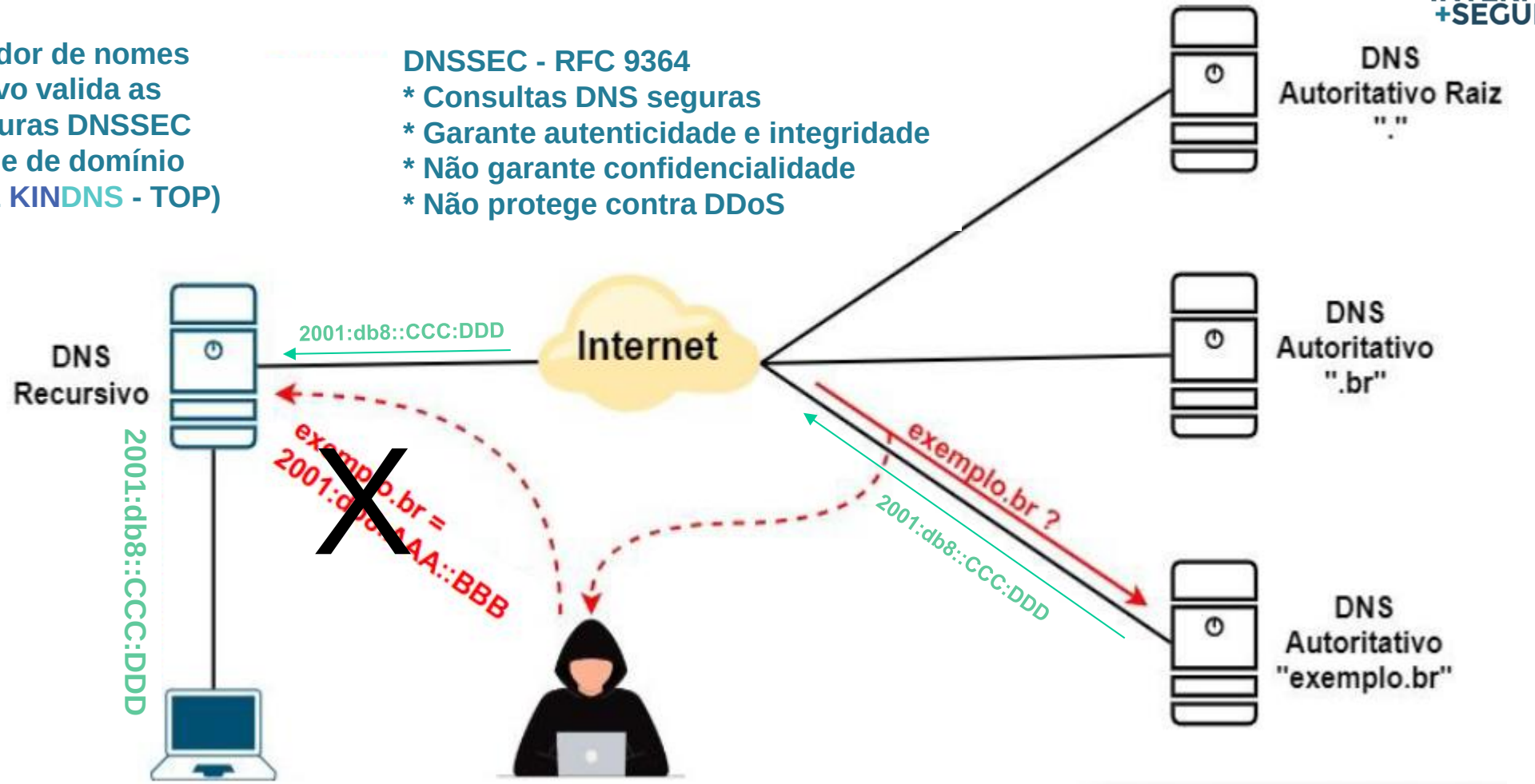
ICANN

Programa por uma Internet mais Segura

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



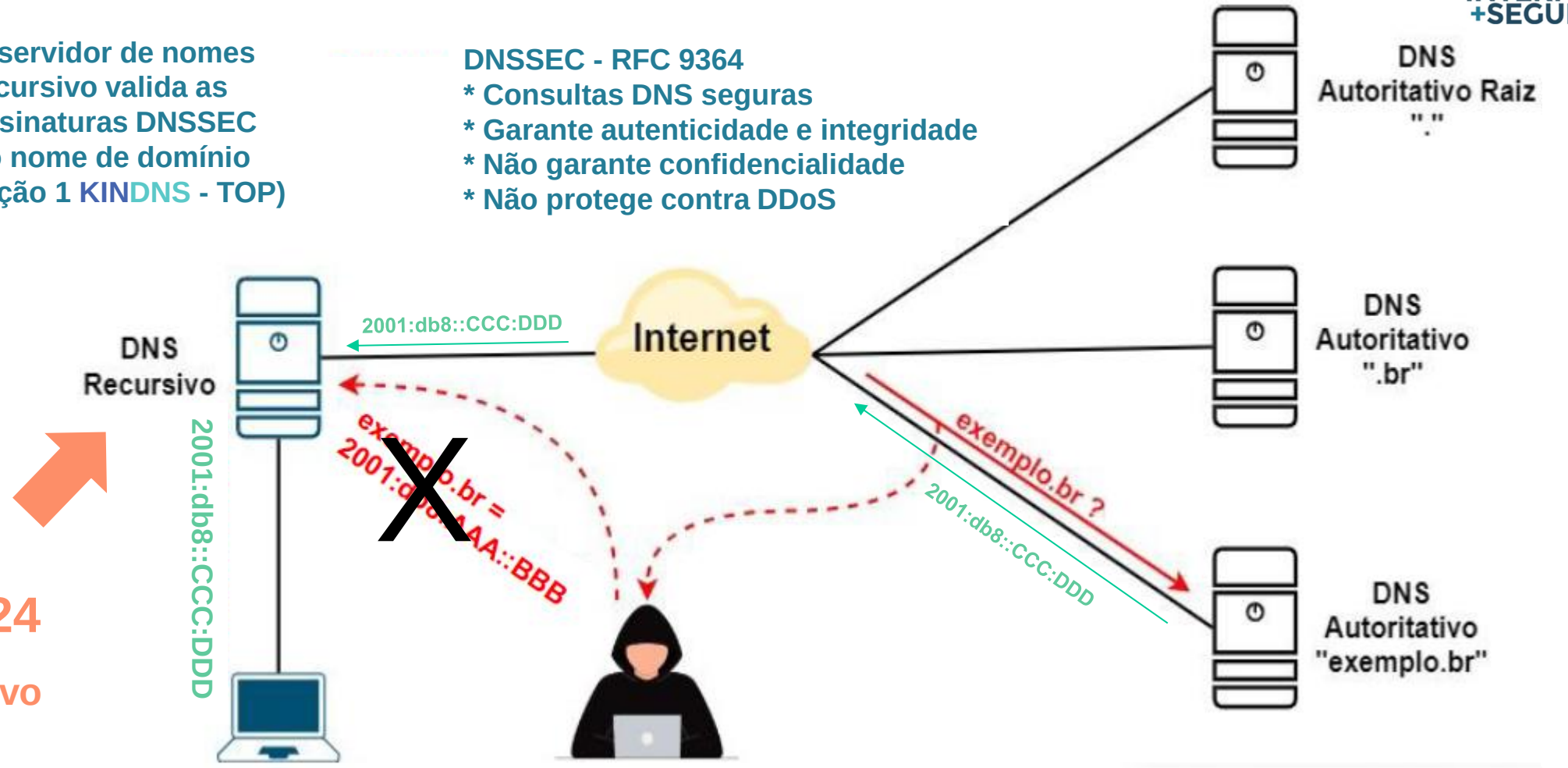
Fonte: [#SemanaCap 7] Curso - Configurando o seu DNS de forma simples e segura – Ataque DNS Poisoning

Programa por uma Internet mais Segura

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



Desafio BCOP 2024

DNS Recursivo próprio

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/

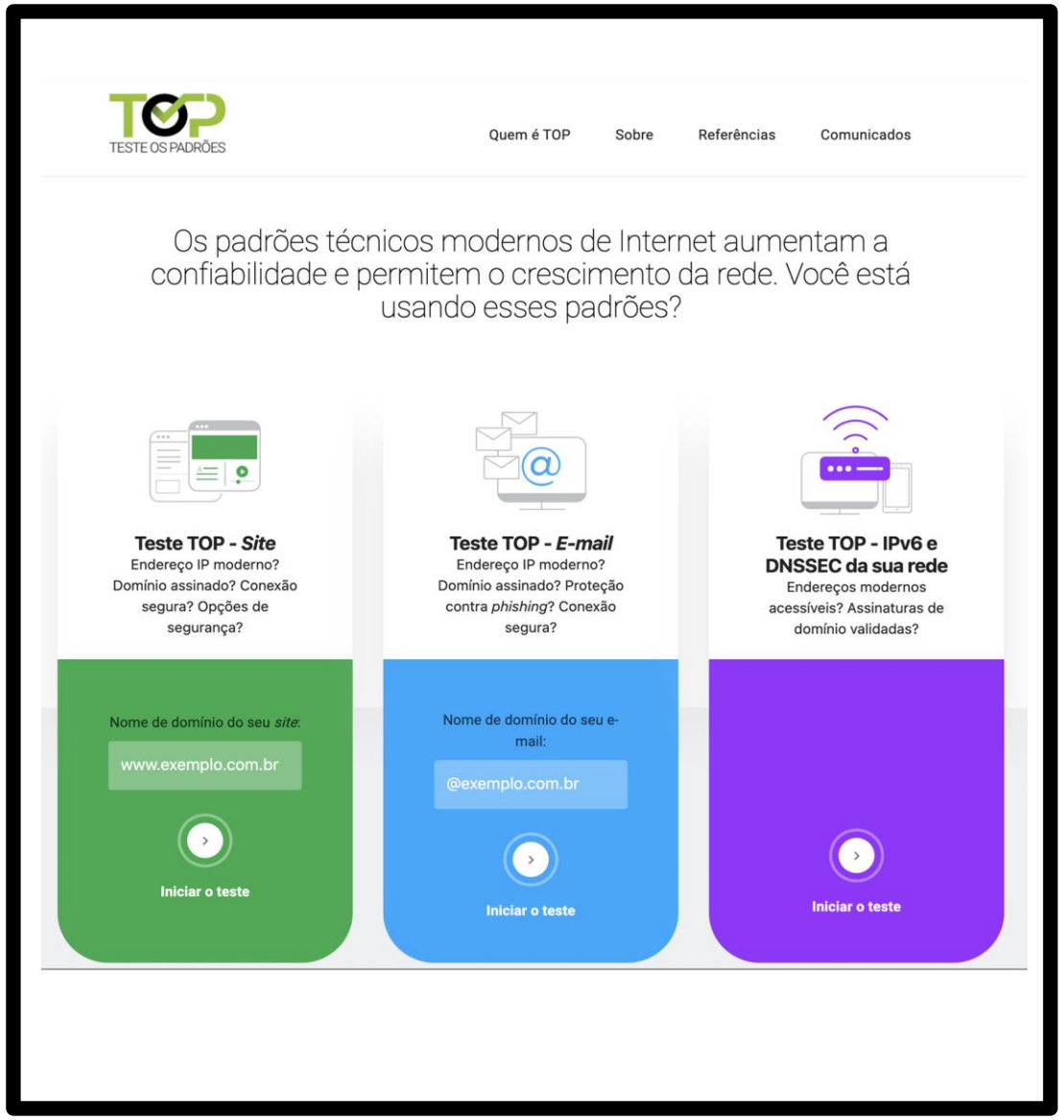
KINDNS

PROGRAMA INTERNET +SEGURA

TOP

TESTE OS PADRÕES

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!

https://top.nic.br

Programa por uma Internet mais Segura
Implemente as melhores práticas

MANRS

BCP
Portal de boas práticas para a Internet no Brasil

KINDNS

Desafio BCOP 2024

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

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

23 de agosto de 2024

nic.br cgi.br

www.nic.br | www.cgi.br