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 Centro-Oeste

Goiânia, GO | 12/07/24

registro.br nic.br cgi.br

Nossa Agenda

Programa por uma Internet mais Segura

- **Objetivos / Plano de Ação**
- Interação com Provedores e Operadoras
- **Ações do Programa**
  - MANRS
  - Notificação de Amplificadores
  - 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

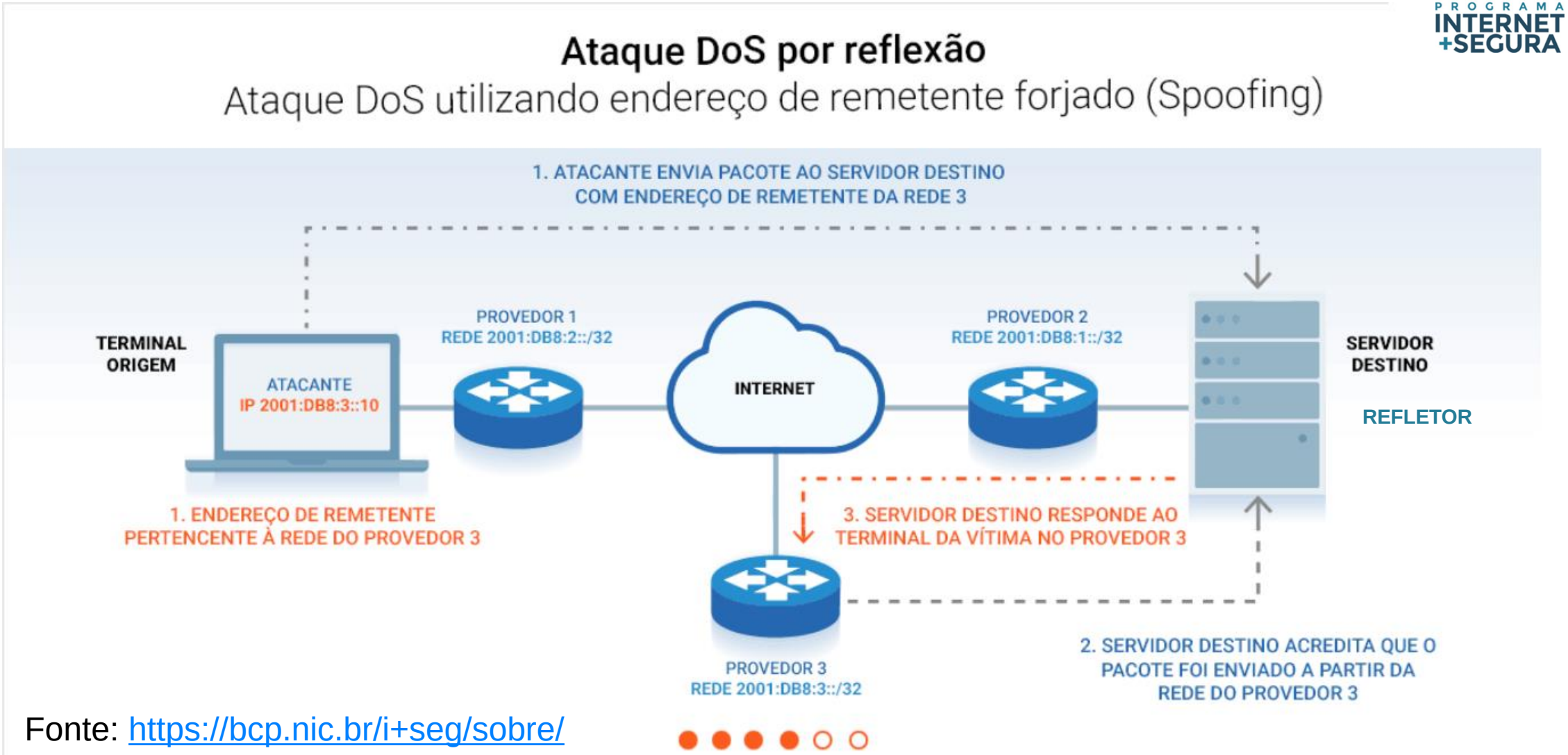
https://bcp.nic.br/i+seg

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



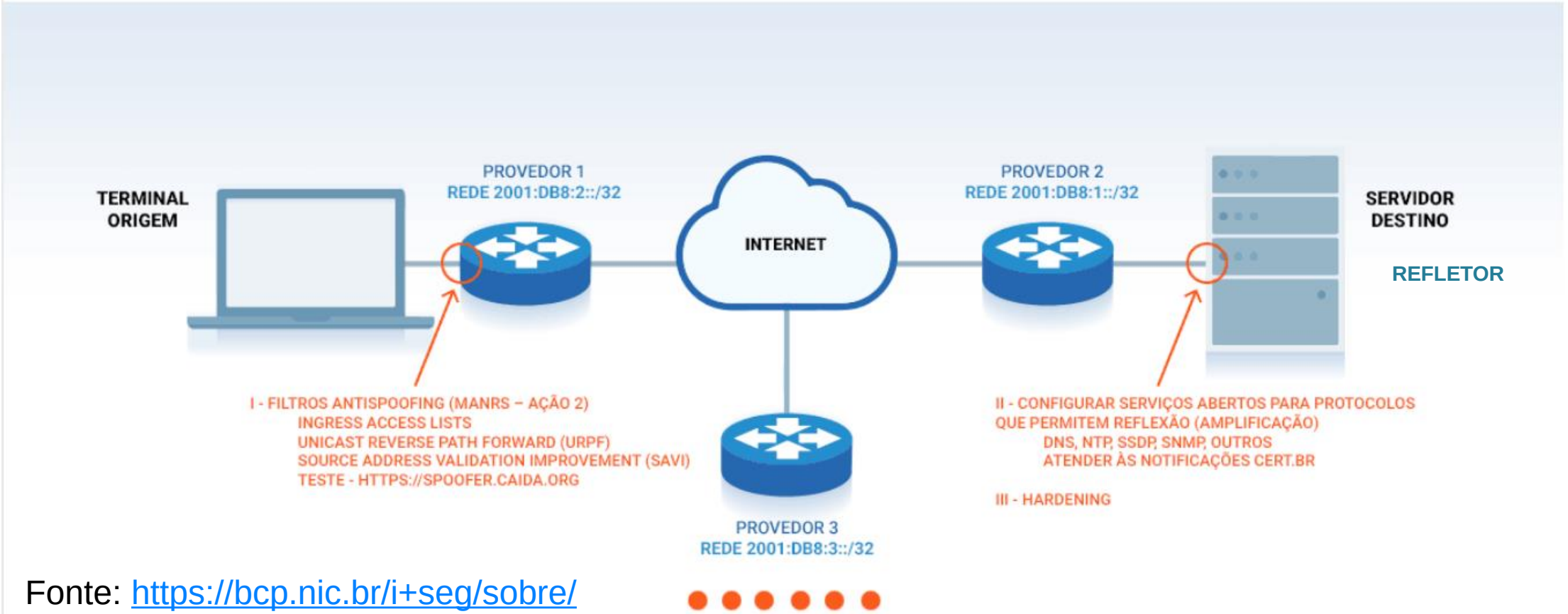
Fonte: https://bcp.nic.br/i+seg/sobre/

Programa por uma Internet mais Segura

PROGRAMA INTERNET +SEGURA

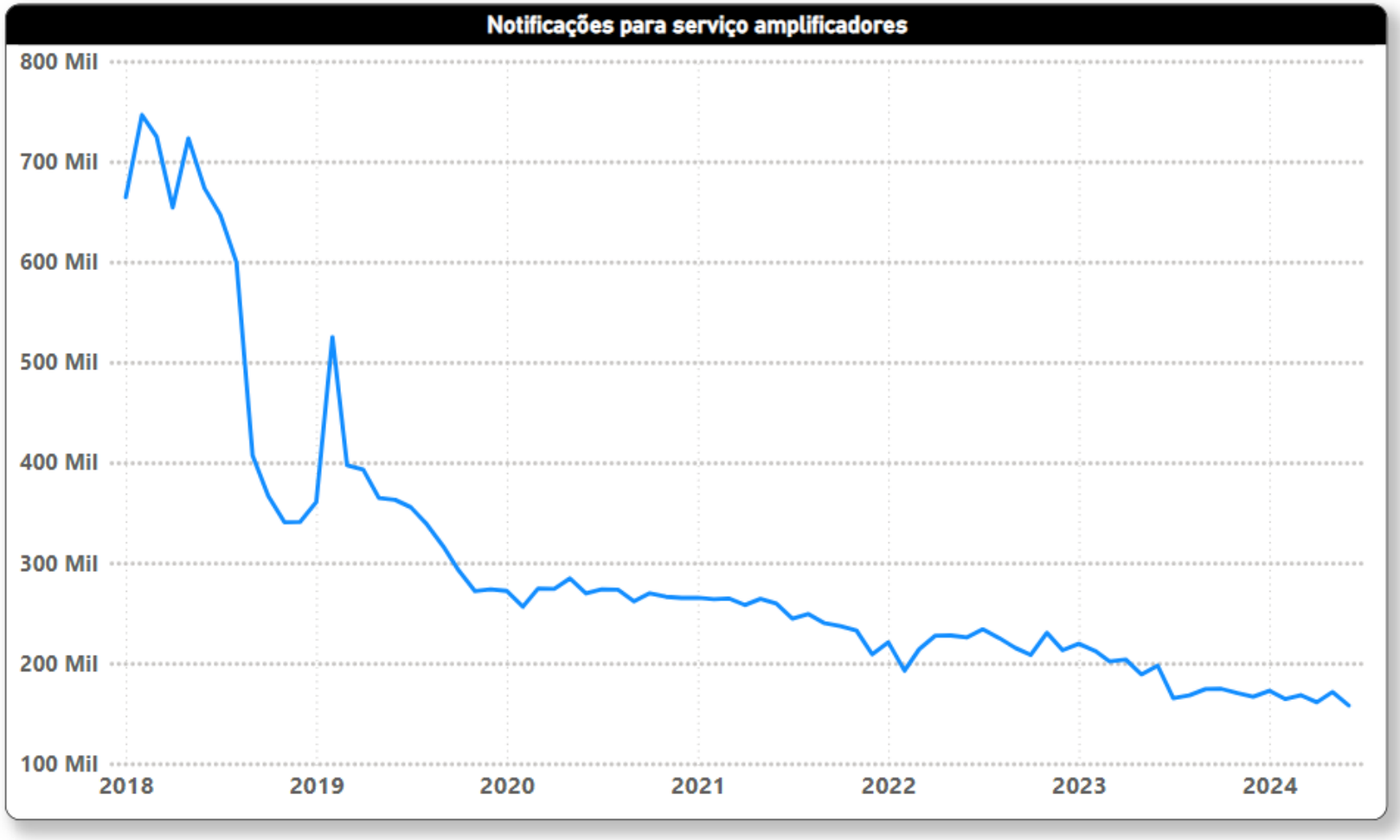
Ataque DoS por reflexão

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



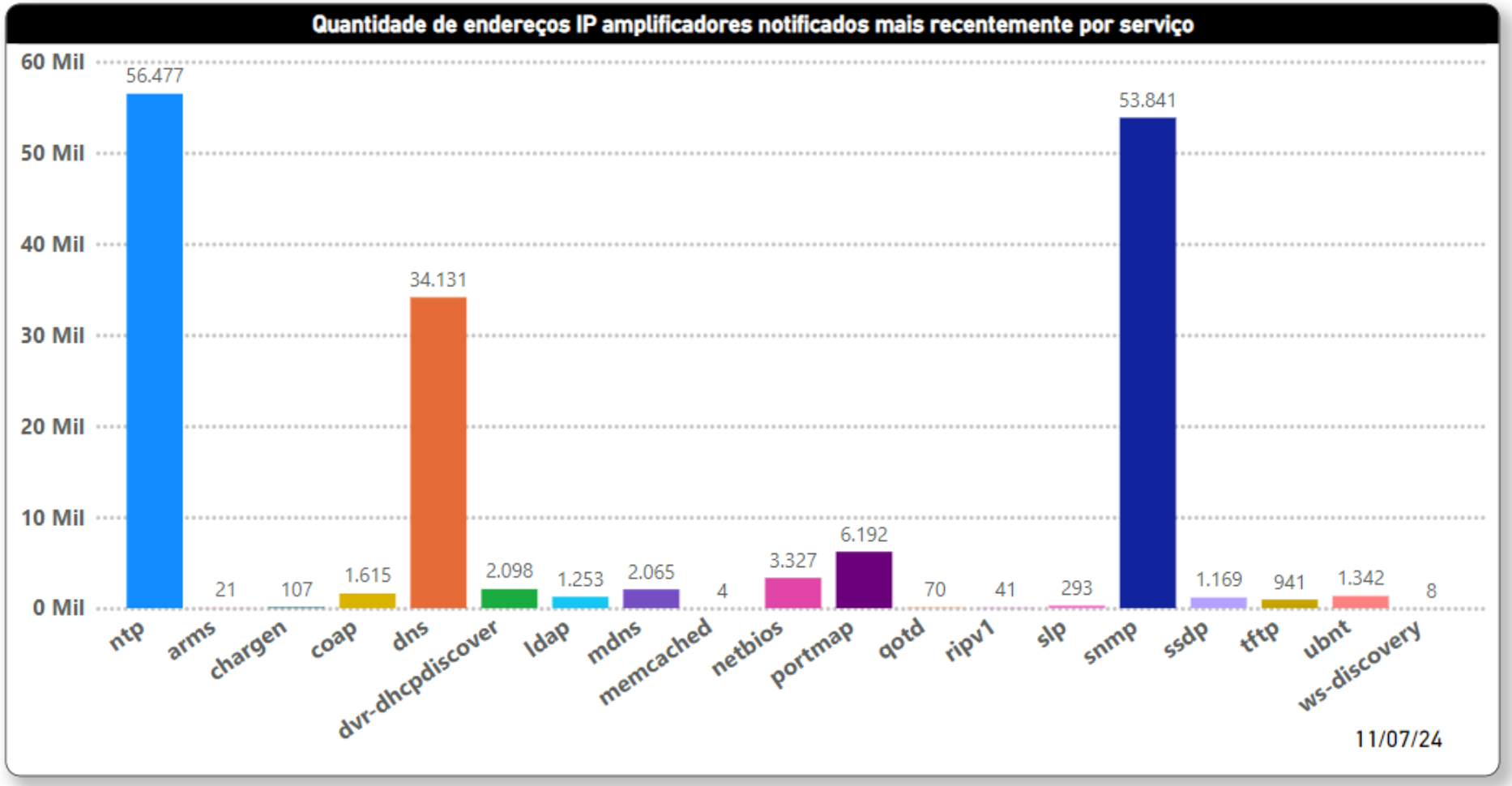
Fonte: https://bcp.nic.br/i+seg/sobre/

Notificação de Amplificadores - Evolução

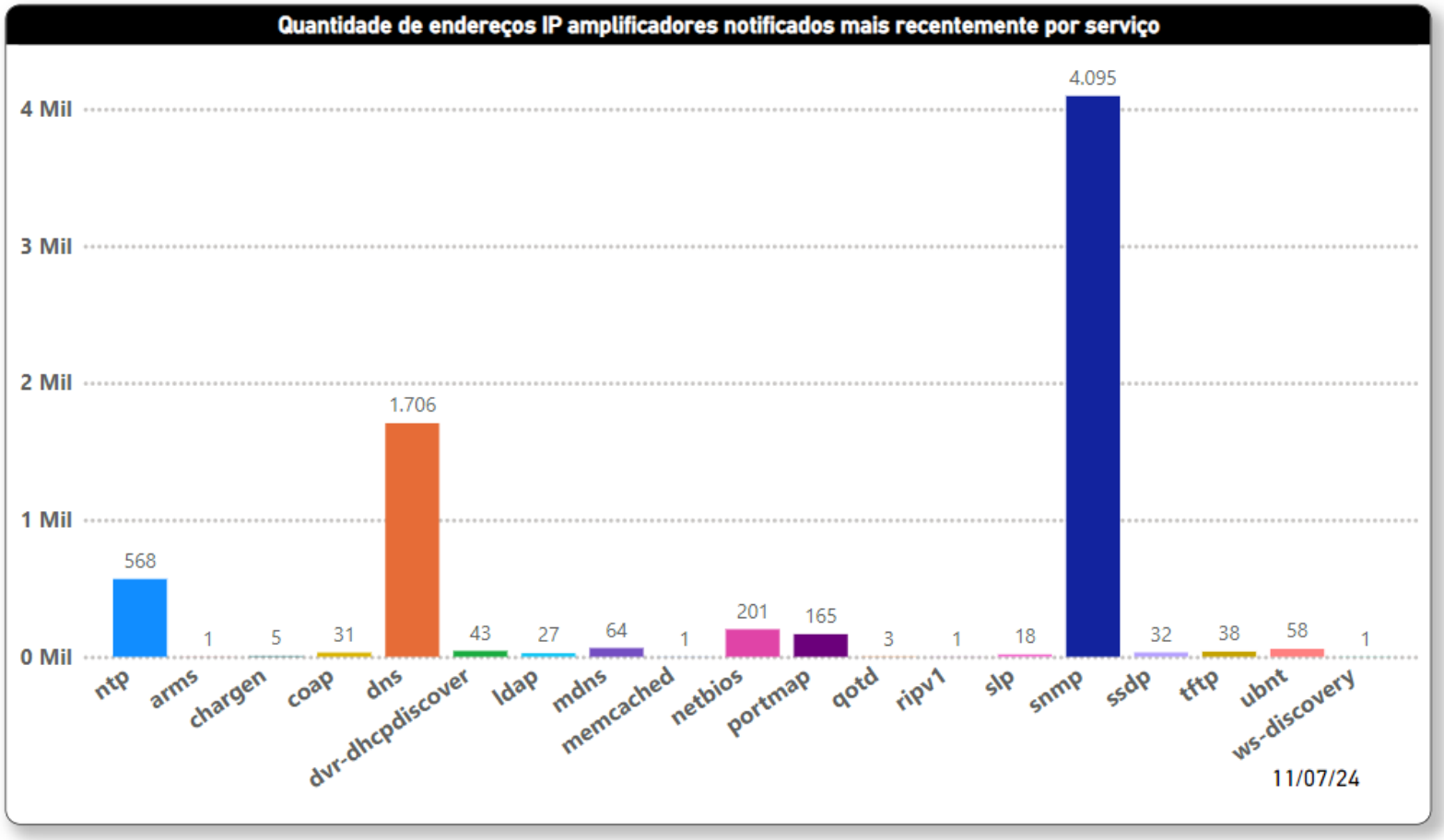


78% de redução de serviços mal configurados desde o início do Programa

Programa por uma Internet mais Segura
Notificação de amplificadores



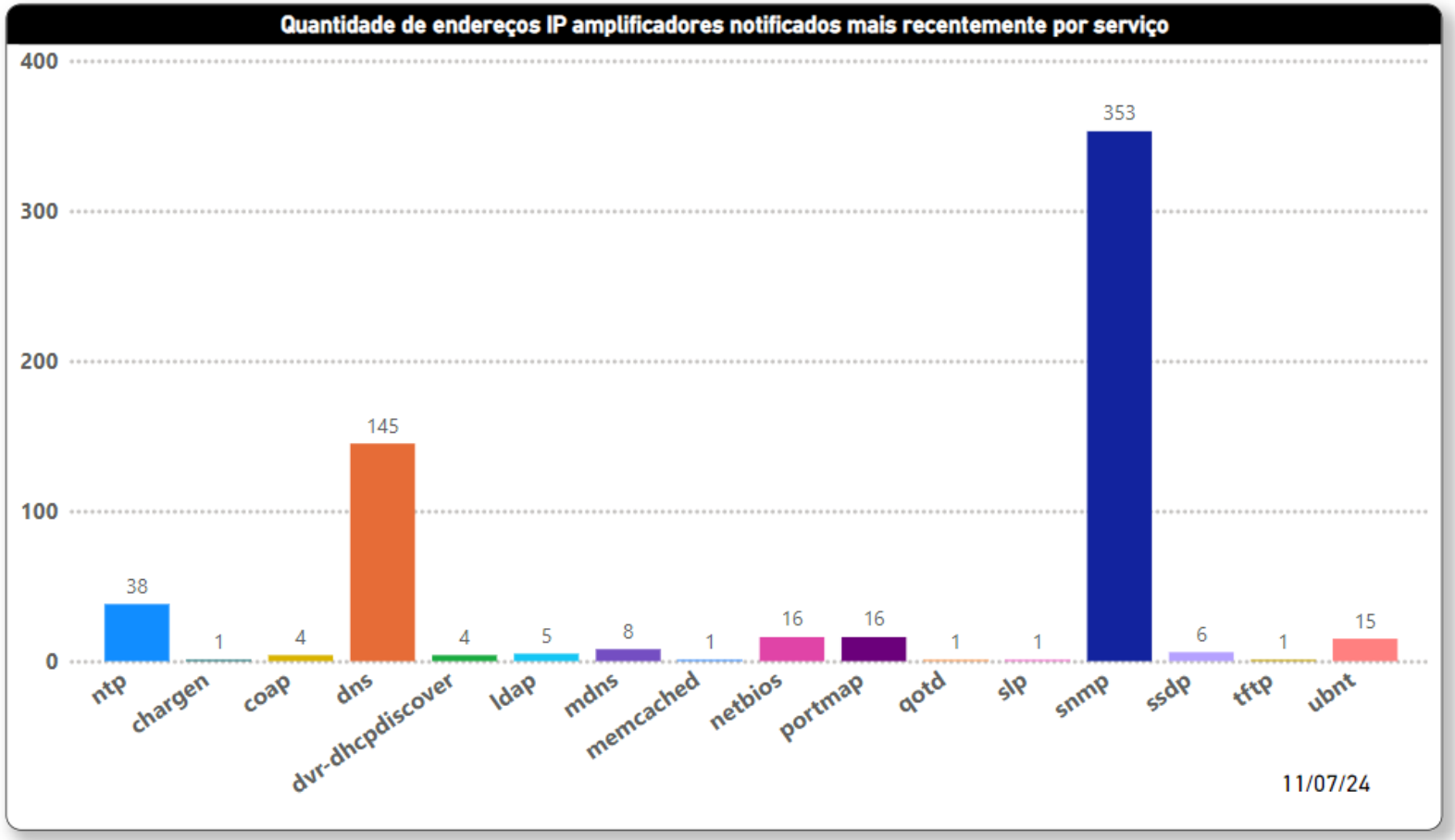
Programa por uma Internet mais Segura
Notificação de amplificadores



Região Centro-Oeste

- 844 ASN
- **6905 endereços IP mal configurados**
  - SNMP 4095
  - DNS 1706
  - NTP 568

Programa por uma Internet mais Segura
Notificação de amplificadores



Participantes do IX

Fórum Centro-Oeste

- 52 ASN cadastrados
- **576 endereços IP mal configurados**
  - SNMP 353
  - DNS 145
  - NTP 38

Programa por uma Internet mais Segura
MANRS

PROGRAMA INTERNET +SEGURA

MANRS

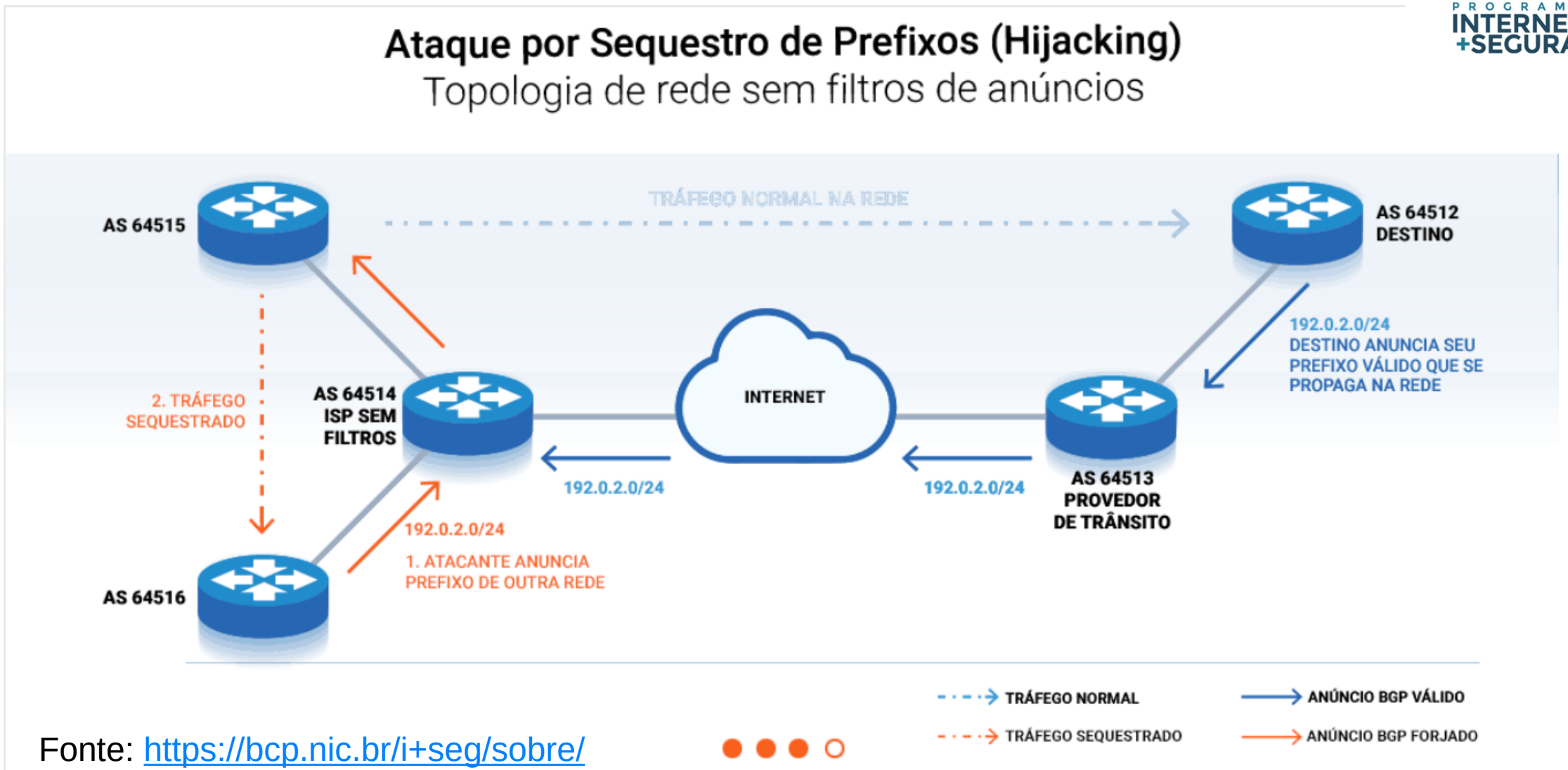
Mutually Agreed Norms for Routing Security

http://manrs.org

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

Programa por uma Internet mais Segura

PROGRAMA INTERNET +SEGURA



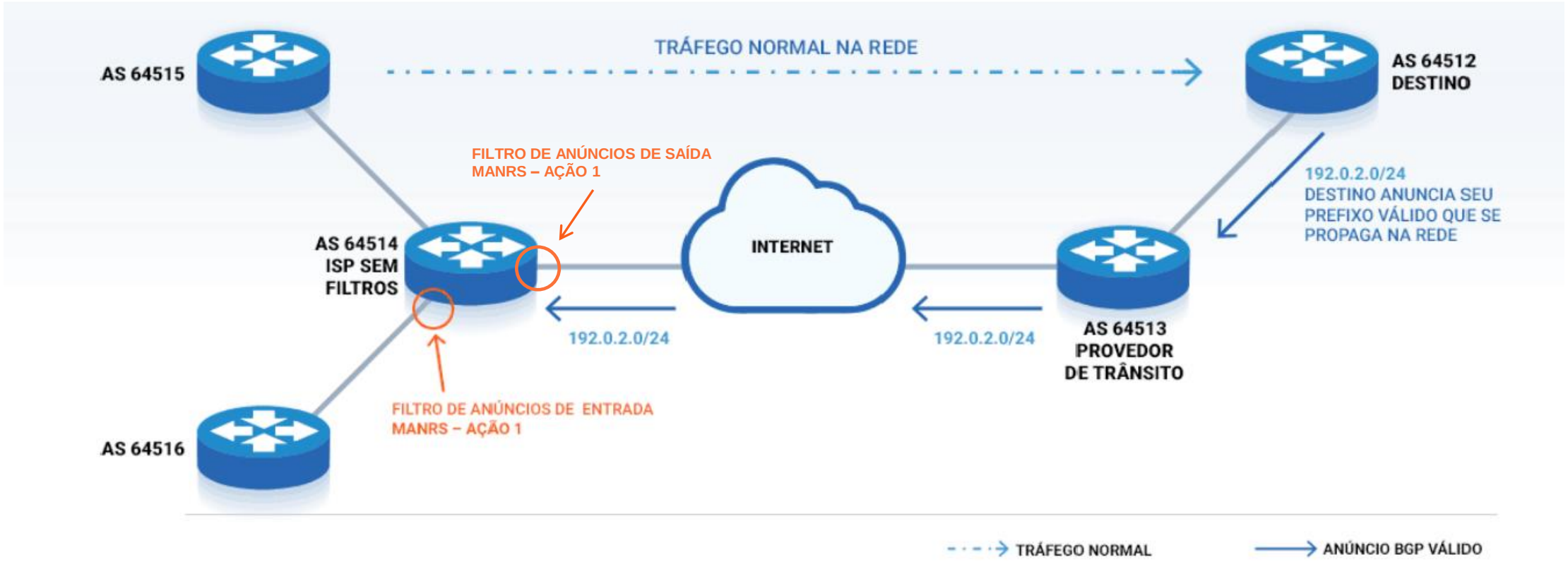
Fonte: https://bcp.nic.br/i+seg/sobre/

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/

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

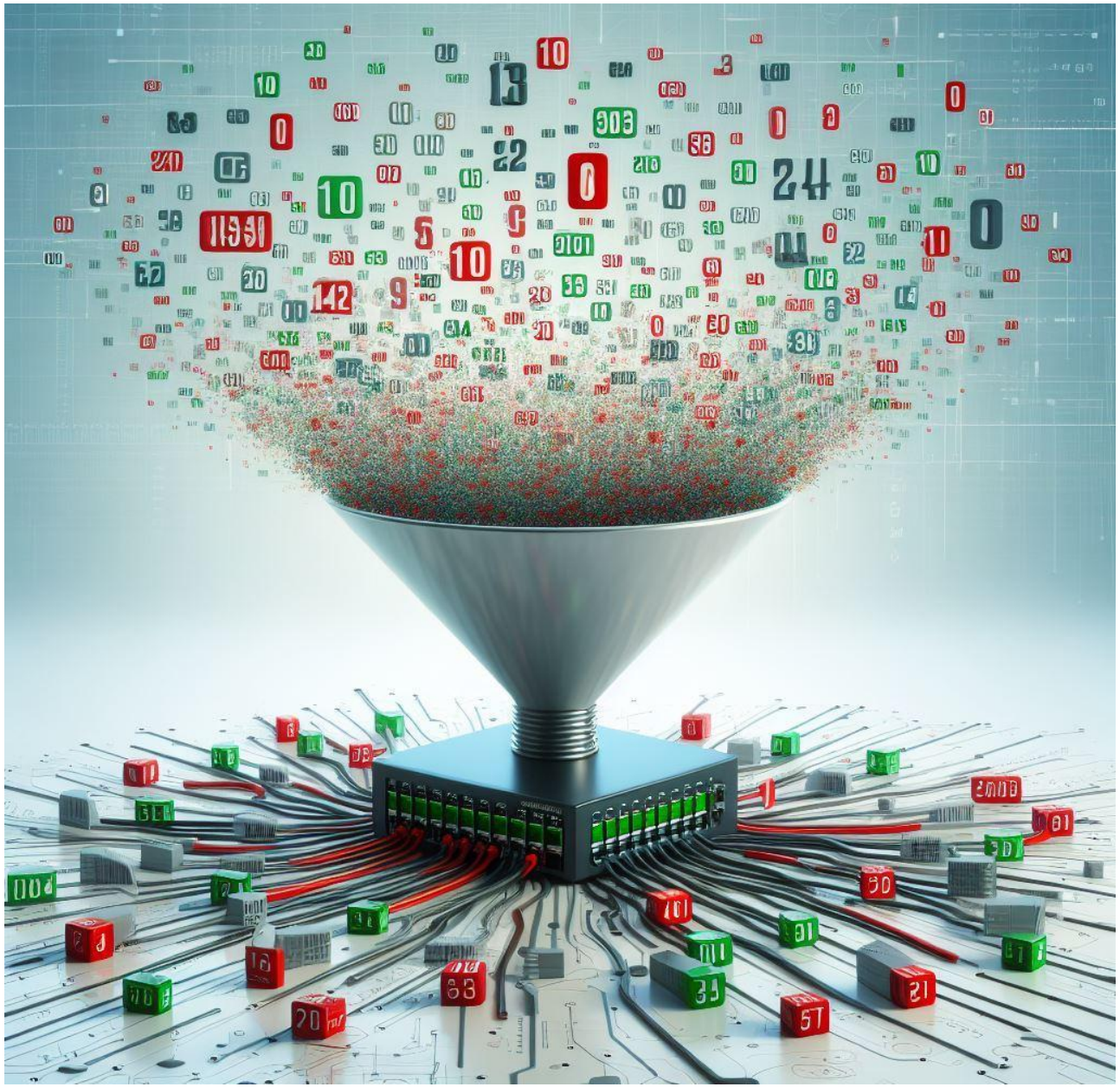
https://bcp.nic.br/i+seg/acoes/manrs/

MANRS

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/



MANRS

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/

MANRS

MANRS - Ação 3 - Pontos de Contato

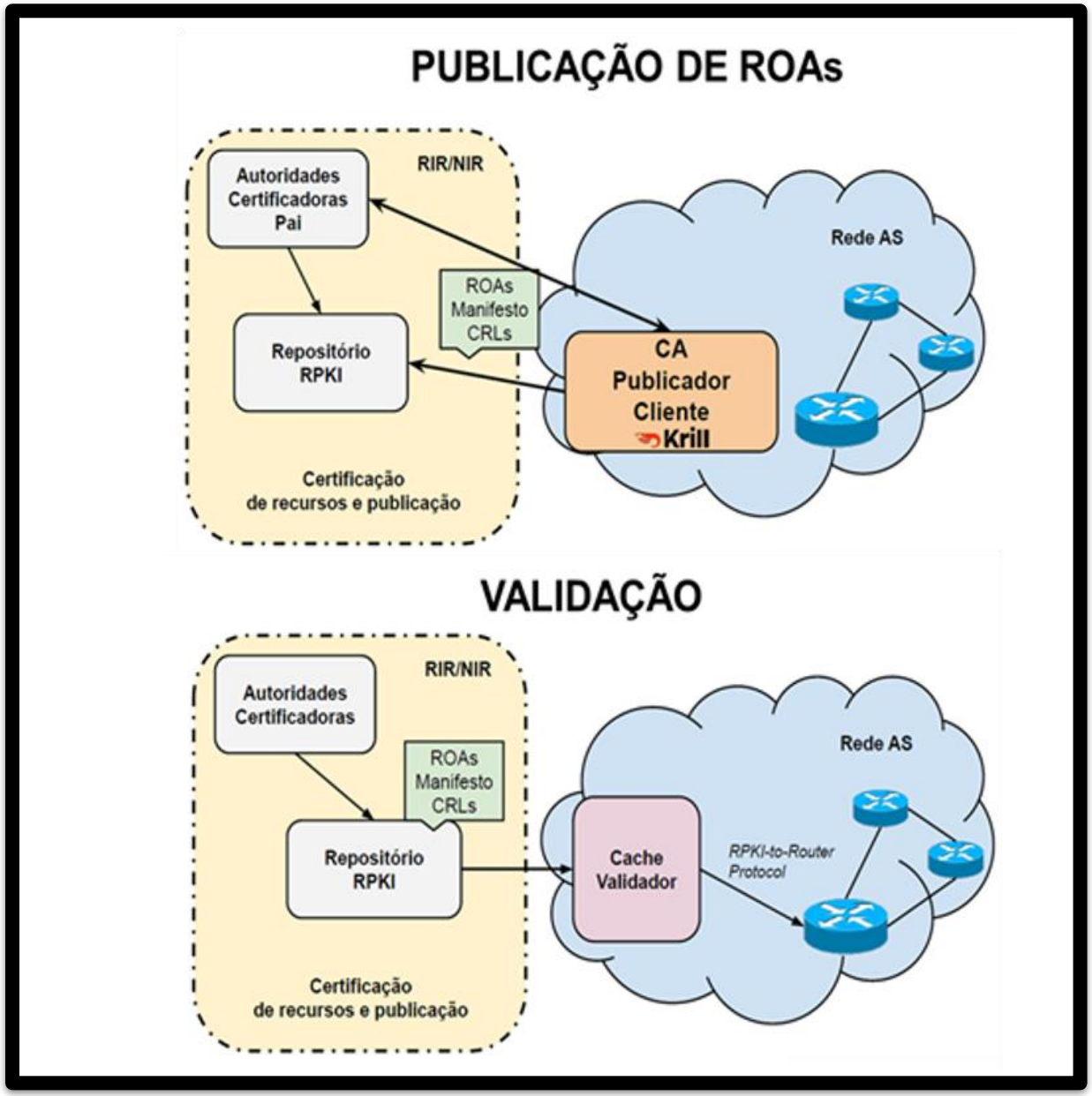
- **Contatos de roteamento e abuse no Registro.br** devem estar atualizados e serem de grupos de pessoas. Ex.: noc@seuprovedor.com.br
    - Registro.br está validando os e-mails de abuse e a não resposta pode causar a recuperação (perda) dos endereços IP
    - Mensagens do CERT.br estão indo para o SPAM em alguns casos!
- Atualizar contatos no **PeeringDB**
- Atualizar contatos no **IRR**

MANRS

MANRS - Ação 4 - Cadastro da Política de Roteamento

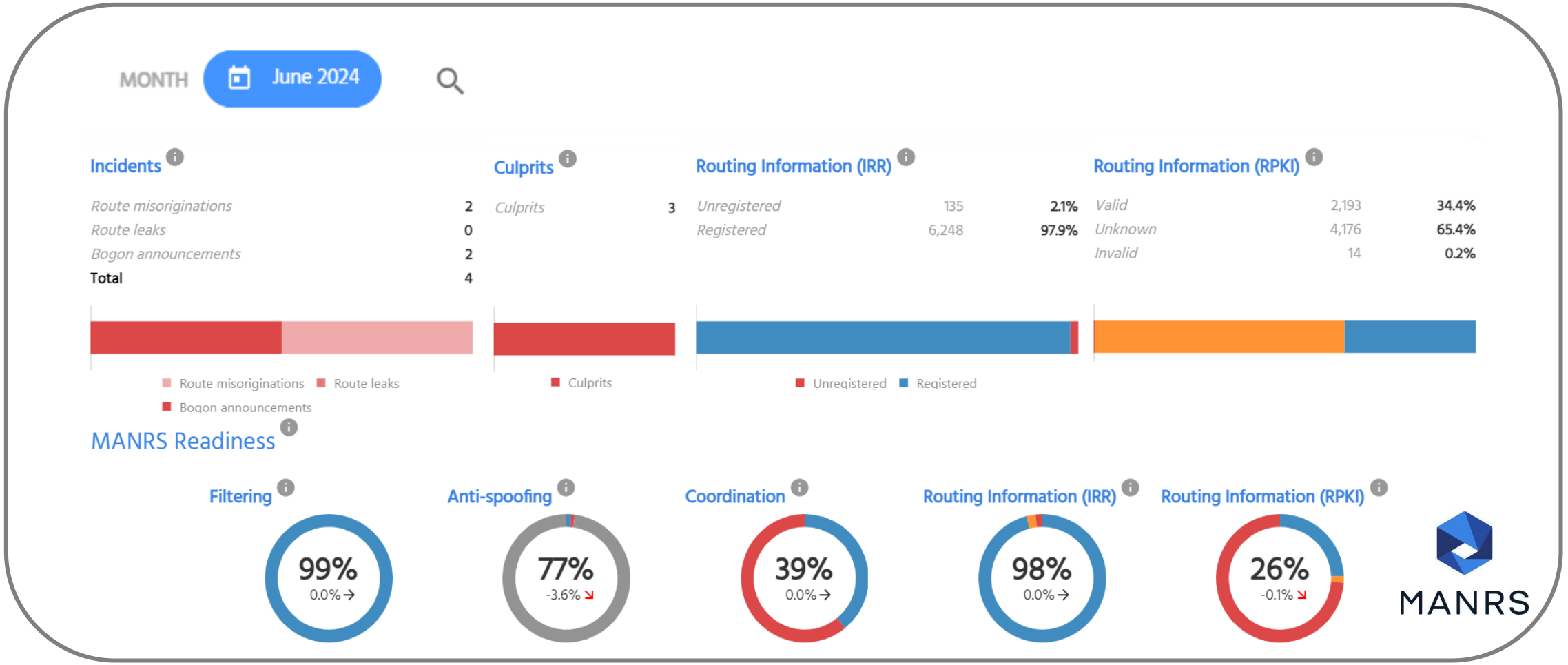
- **IRR** - Internet Routing Registry
  - RADB
  - TC (gratuito)

- **RPKI** - Resource Public Key Infrastructure

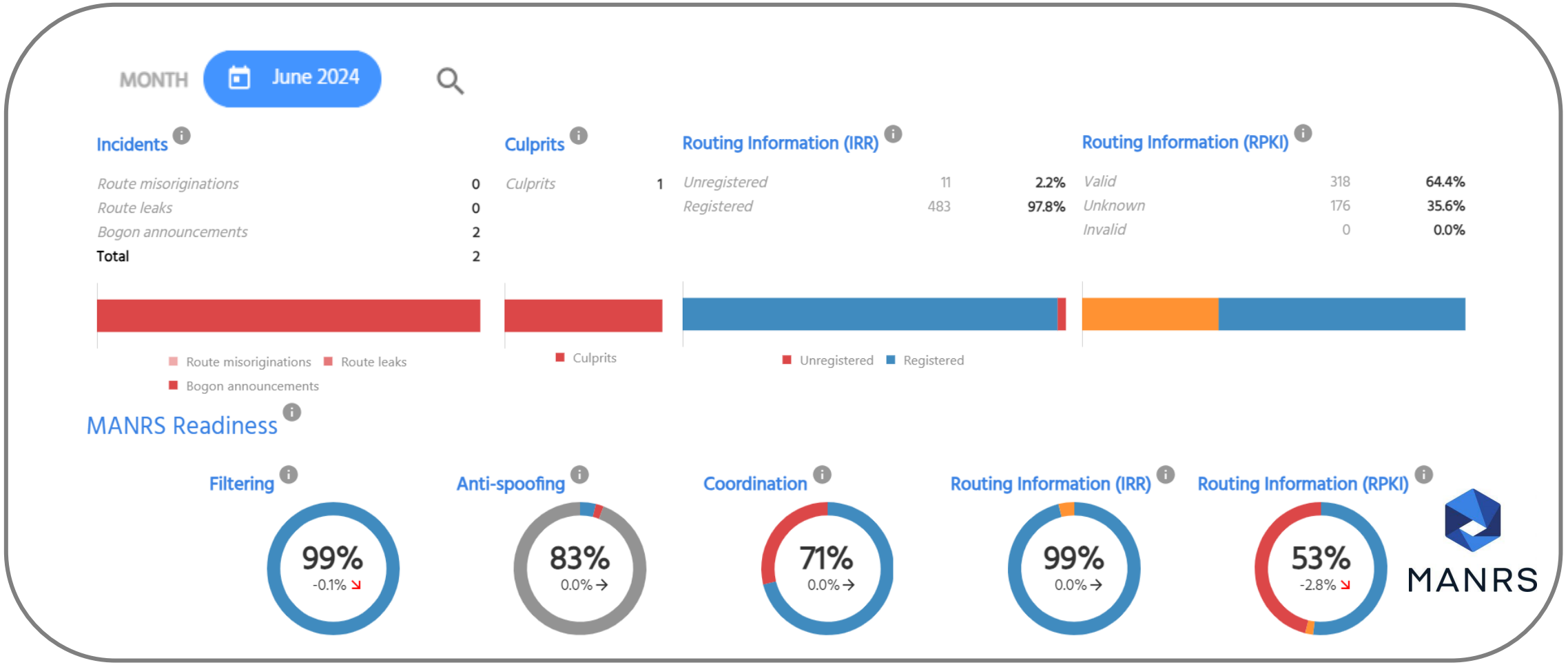


Programa por uma Internet mais Segura

MANRS Observatory - 844 AS - CO

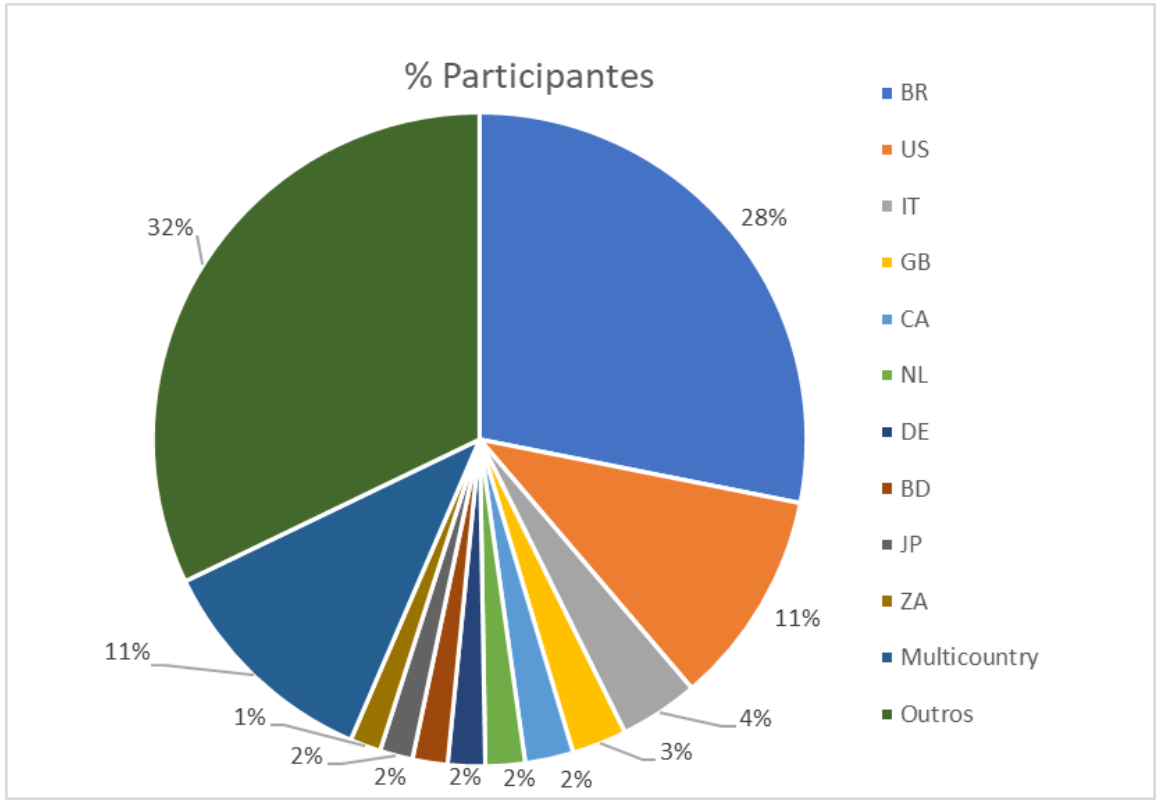


Programa por uma Internet mais Segura
MANRS Observatory - 52 AS – Part. IX CO



Programa por uma Internet mais Segura

Participantes do MANRS por país



Total de participantes do MANRS: 942

Participantes no Brasil: 265 (Jun/24)

258 (2023)

206 (2022)

174 (2021)

140 (2020)

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

Programa por uma Internet mais Segura
KINDNS

PROGRAMA INTERNET +SEGURA

Stands for **K**nowledge-Sharing and **I**nstantiating
Norms for **DNS** and **N**aming **S**ecurity

An ICANN Initiative

ICANN

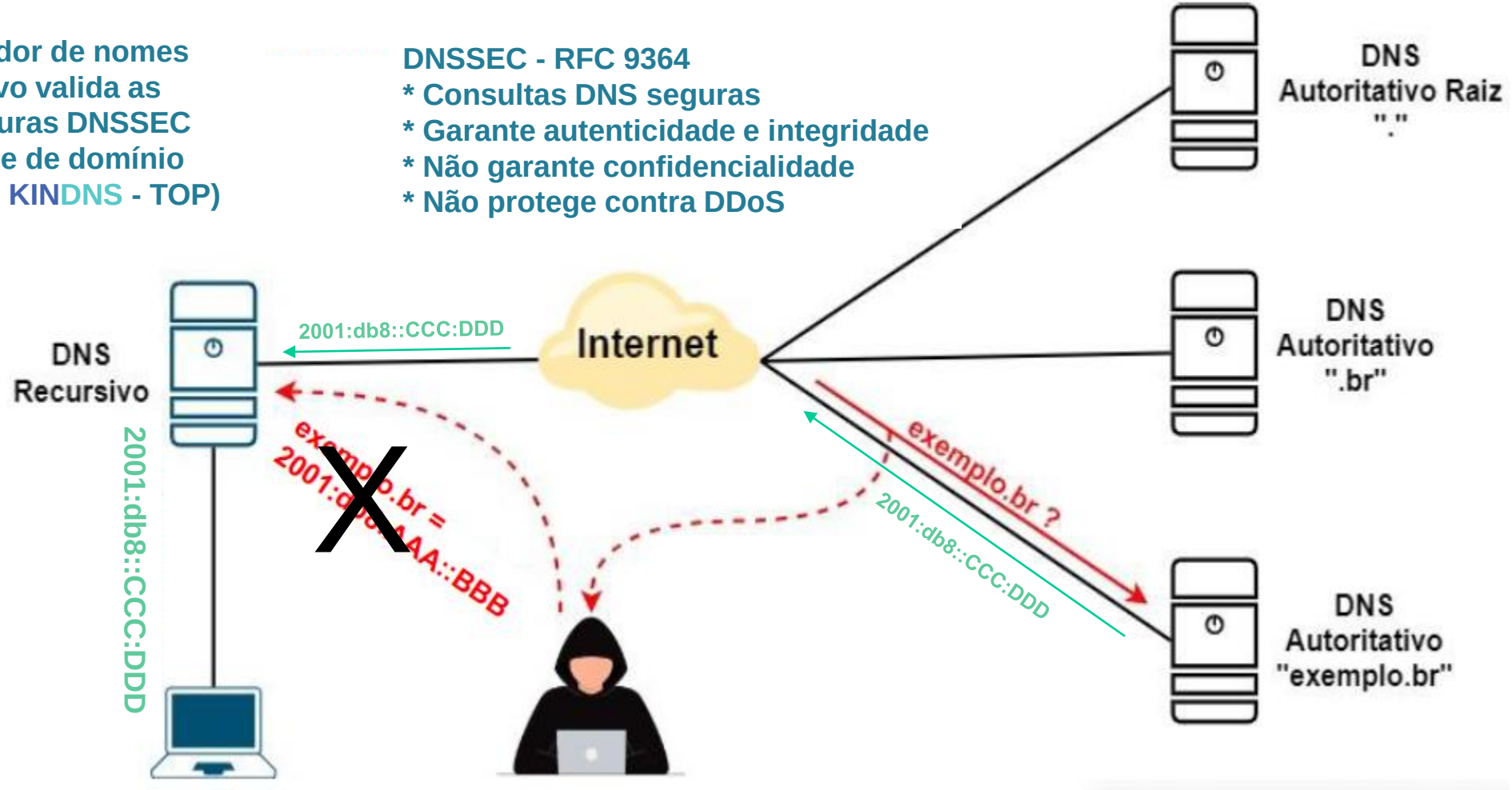
https://kindns.org/

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

Boas práticas para DNS

- KIN**DNS** 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
- Torne-se um participante

https://kindns.org/

KINDNS

Programa por uma Internet mais Segura

PROGRAMA INTERNET +SEGURA

TOP TESTE OS PADRÕES

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 orienta como corrigir!

https://top.nic.br

TESTE OS PADRÕES

Programa por uma Internet mais Segura
Selos de segurança

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

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

12 de julho de 2024

www.nic.br | www.cgi.br