



nic.br

Núcleo de Informação
e Coordenação do
Ponto BR

egi.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

Antonio M. Moreiras e Gilberto Zorello

Apronet 2025 – Florianópolis, SC, 30/05/2025

nie.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



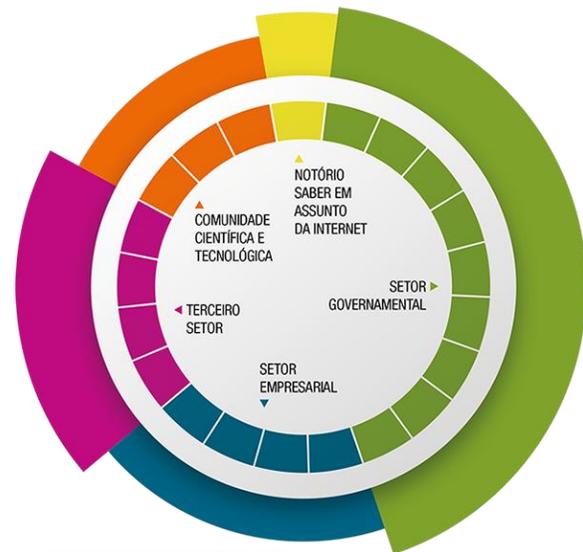


NIC.br e CGI.br

- 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



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

Domínios

cert.br

Segurança

cetic.br

Indicadores

ceptro.br

Redes e Operações

ceweb.br

Tecnologias Web

ix.br

Troca de Tráfego

W3C
CHAPTER
São Paulo

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/>



Boas práticas e padrões na Infraestrutura

ceptro.br

ix.br

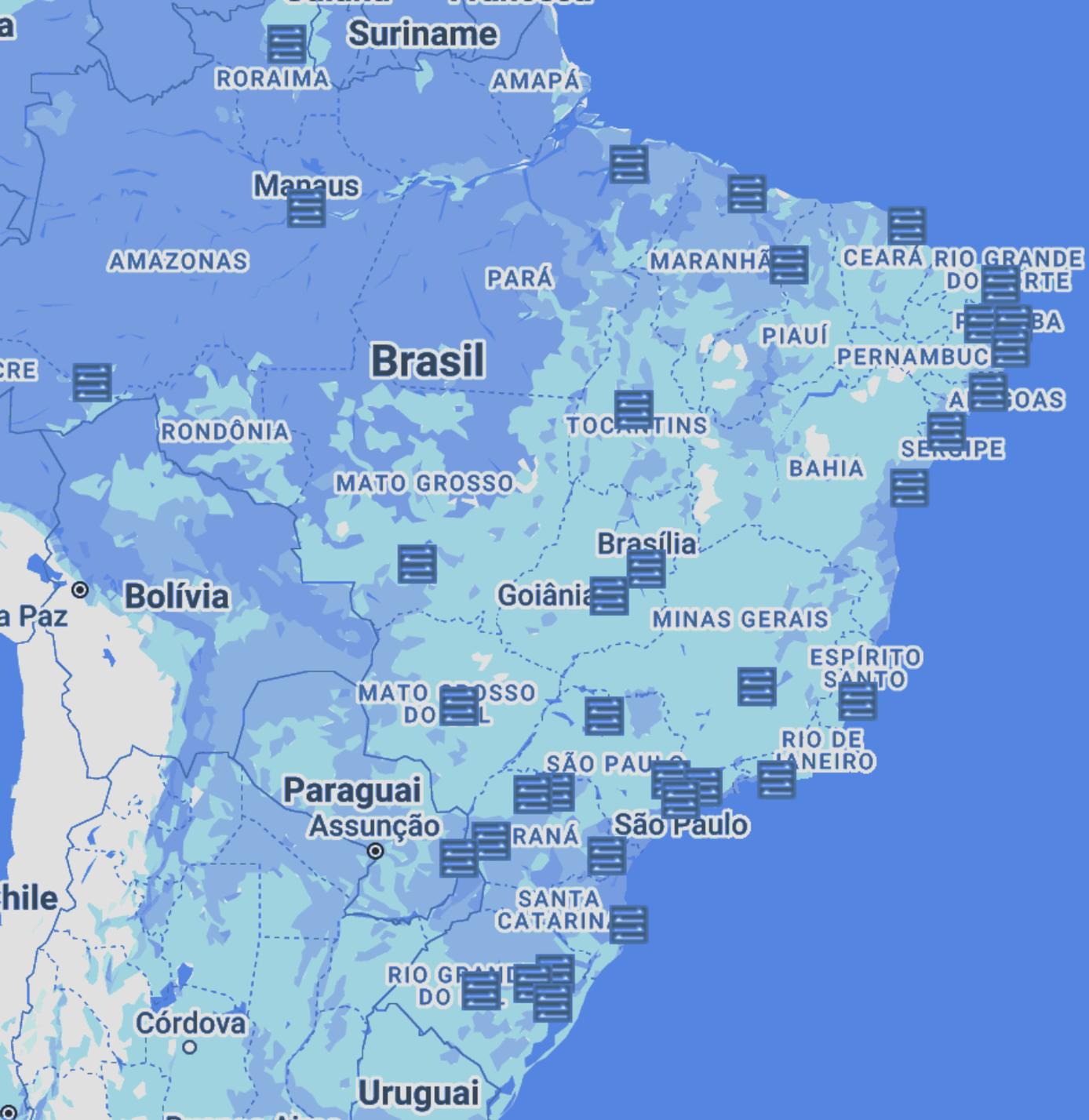
IPv6

- Esgotamento do IPv4
- 50% de adoção no Brasil
- Diminui a carga do CGNAT
- Menos propenso a ataques DDoS hoje
- Melhor experiência do usuário

<https://ipv6.br/>

IPv6.br





Internet Exchanges

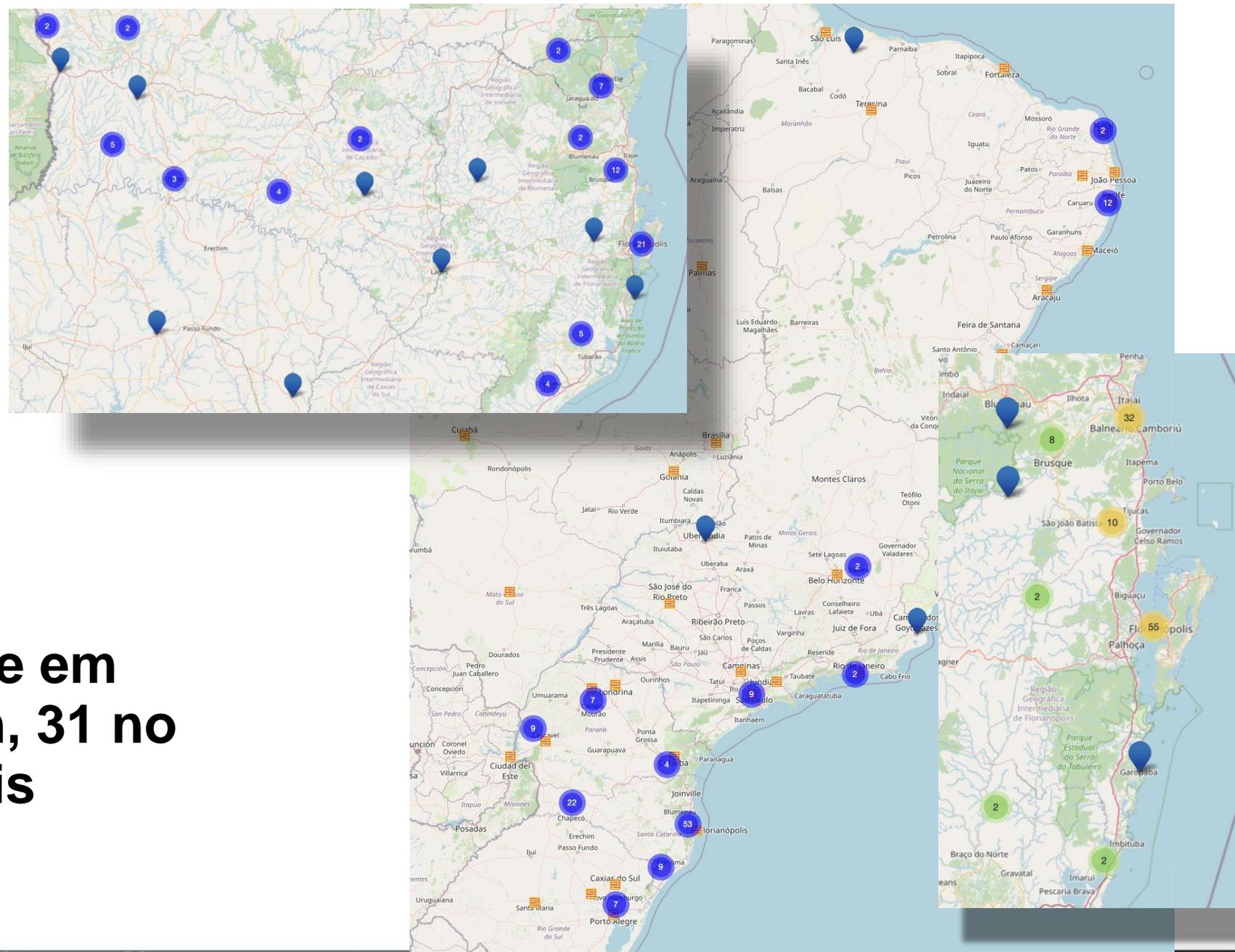
- IX.br - 38 PTTs
- Troca de tráfego local
- Acesso a conteúdos locais
- CDNs
- Mais resiliência
- Melhor experiência do usuário
- Mais qualidade



<https://ix.br/>

IX.br de Florianópolis

- 108 participantes diretos
- 5914 AS visíveis na tabela de rotas do Route Server
- **107 AS com sede em um raio de 80km, 31 no PTT Florianópolis apenas**



Medição de qualidade

- SIMET
- Medidor de qualidade neutro, do NIC.br
- É possível ter um servidor na sua rede
- Servidores nos PTTs
- PAS = Portal do AS
- Acesso aos dados de suas medições

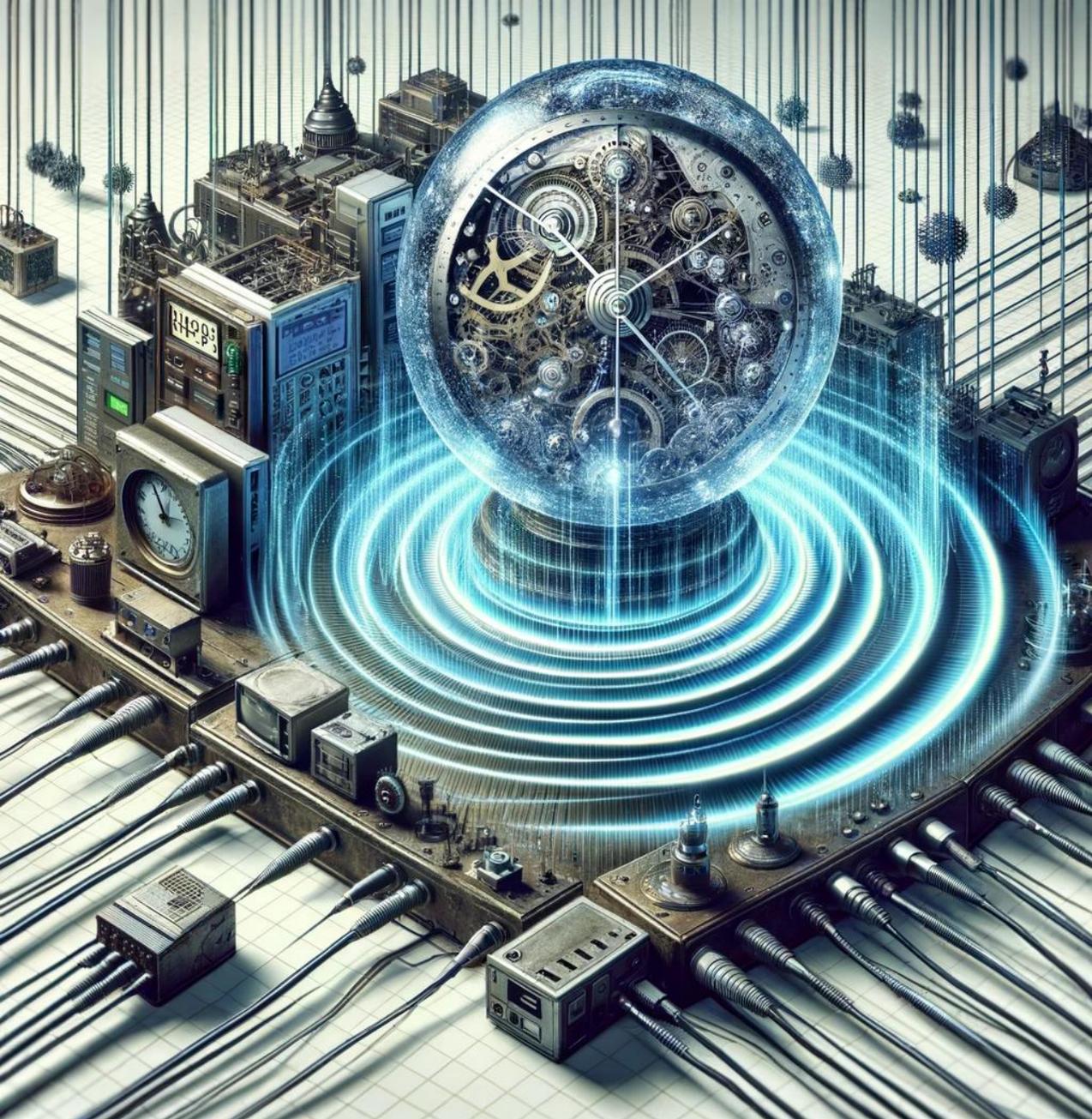


<https://medicoes.nic.br/>

<https://simet.nic.br/>

<https://pas.nic.br/>





Sincronismo de tempo

- NTP.br
- Relógios de Césio do Observatório Nacional
- Independência em relação a GPS / GNSS
- Logs com registro de tempo correto
- Importante para o bom funcionamento e segurança dos sistemas

ntp.br <https://ntp.br/>

nic.br cgi.br

Capacitação técnica

- Cursos, eventos, lives, presenciais e a distância, podcast, gratuitos!
- <https://nic.br/>
- <https://ceptro.br/cursos-eventos/>
- <https://cursoseventos.nic.br/>

Nos siga nas redes sociais:

- No Twitter, somos @comunicbr
- No Facebook, LinkedIn, Instagram e Telegram, nós somos @NICbr!



Boas práticas e padrões de Segurança



PROGRAMA
**INTERNET
+SEGURA**

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



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**

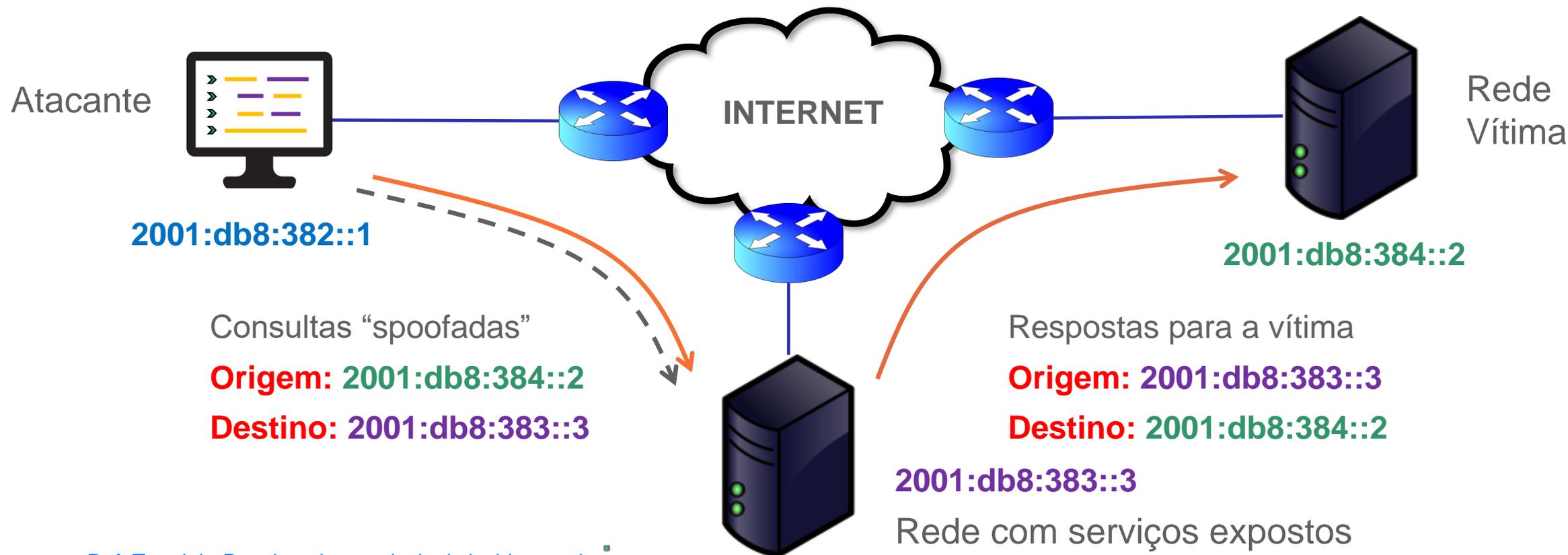
<https://bcp.nic.br/i+seg>



Programa por uma Internet mais Segura

Negação de Serviço Reflexivo com Amplificação

Utiliza um terceiro para fazer o ataque

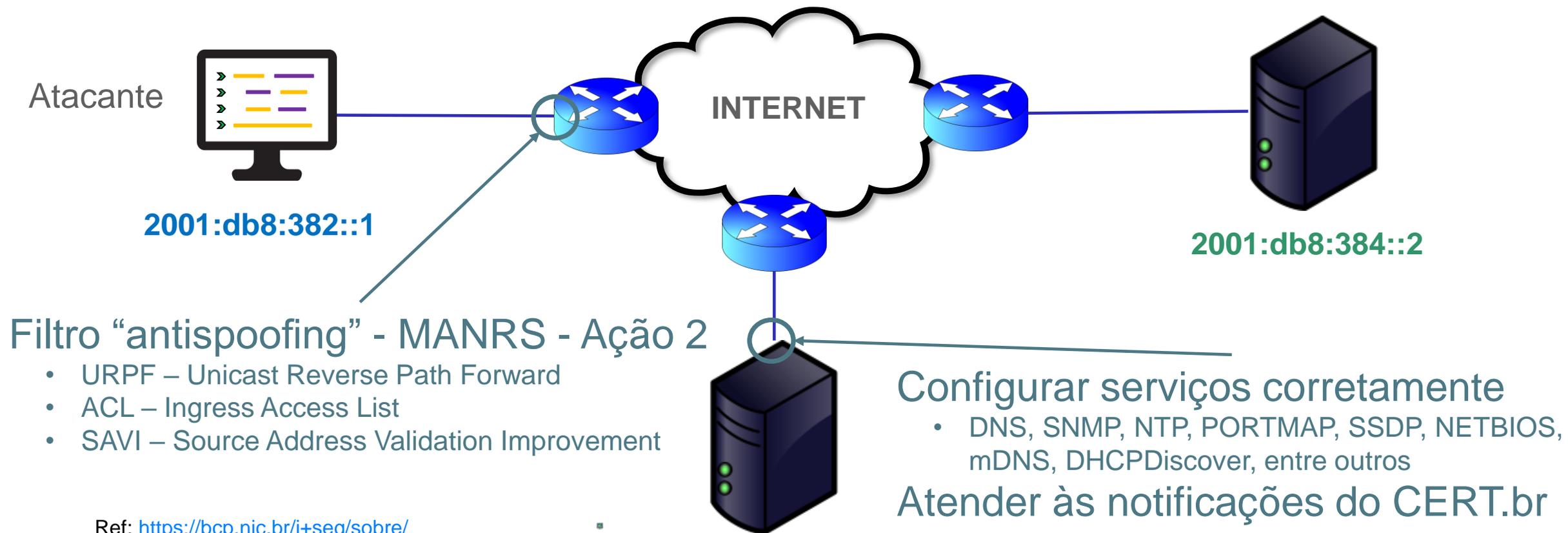


[Ref. Tutorial - Resolvendo os principais incidentes de segurança](#)

Programa por uma Internet mais Segura

Negação de Serviço Reflexivo com Amplificação

Como resolver o problema



Configuração de serviços expostos na Internet

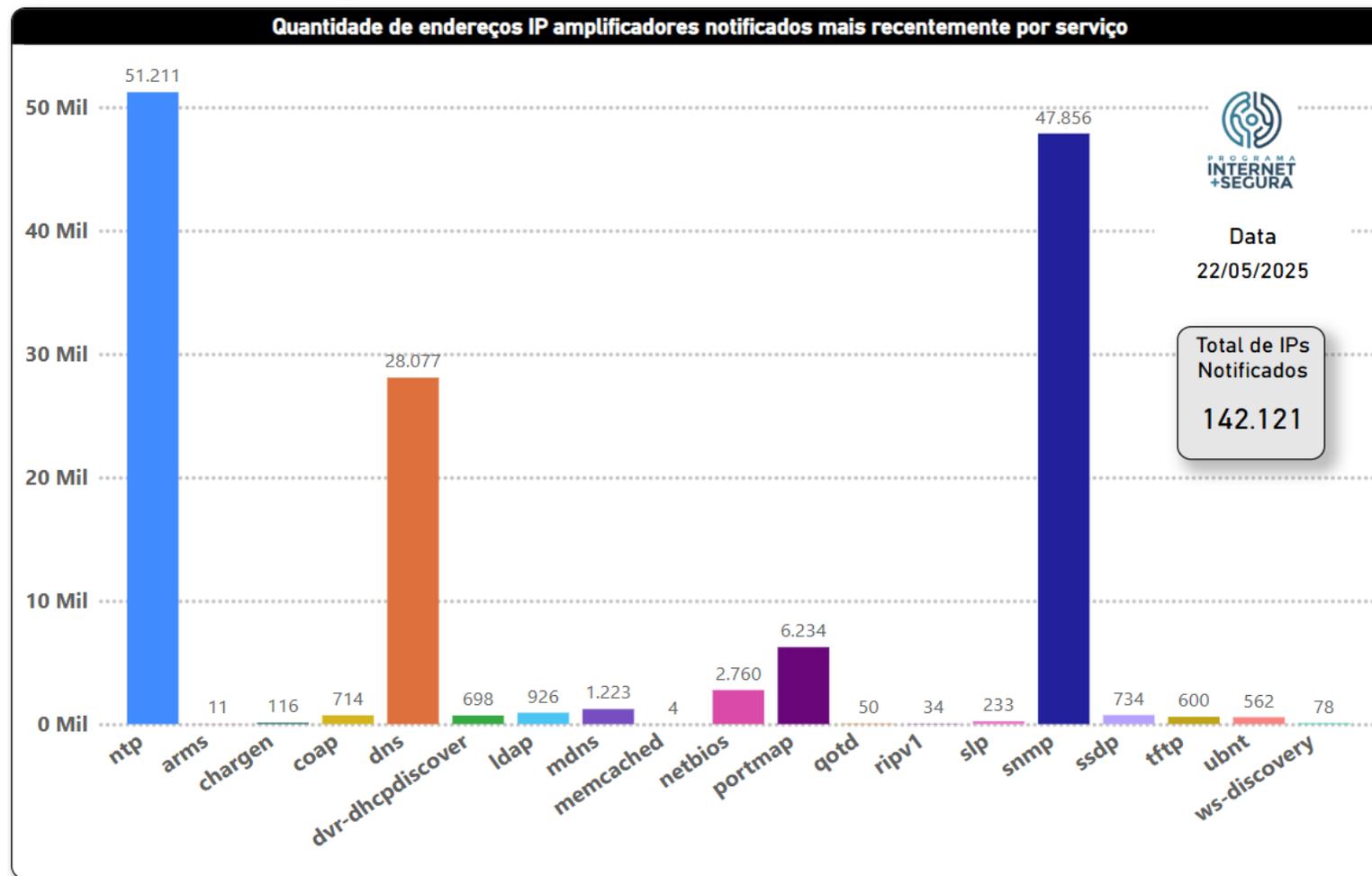
- Usados para amplificação em DDoS
- Portas UDP: DNS (53), SNMP (161), NTP (123), e várias outras!
- Notificações do CERT.br

<https://bcp.nic.br/i+seg/acoes/amplificacao/>



Programa por uma Internet mais Segura

Notificação de amplificadores - serviços

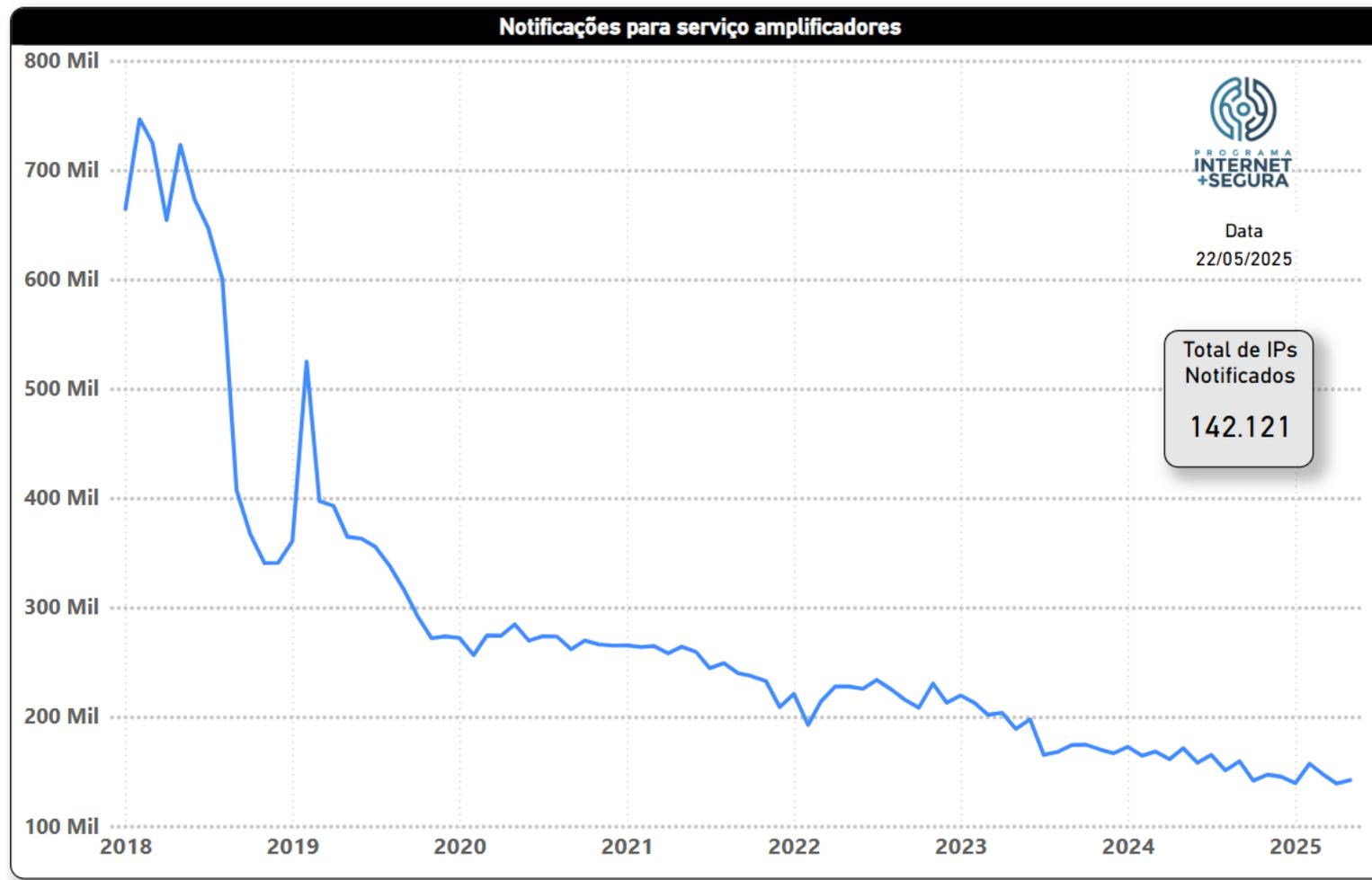


Brasil

- 5.077 AS notificados
- 142.121 endereços IP mal configurados
- **SNMP 47.856**
- **NTP 51.211**
- **DNS 28.077**

Programa por uma Internet mais Segura

Notificação de amplificadores - evolução



Brasil

- Início (fev/2018)
 - Endereços IP: 746.508
 - Serviços: 5
- Atual:
 - Endereços IP: 142.121
 - Serviços: 19
 - **Redução de 80%**
 - Operadoras: 41%
 - ISP: 59%

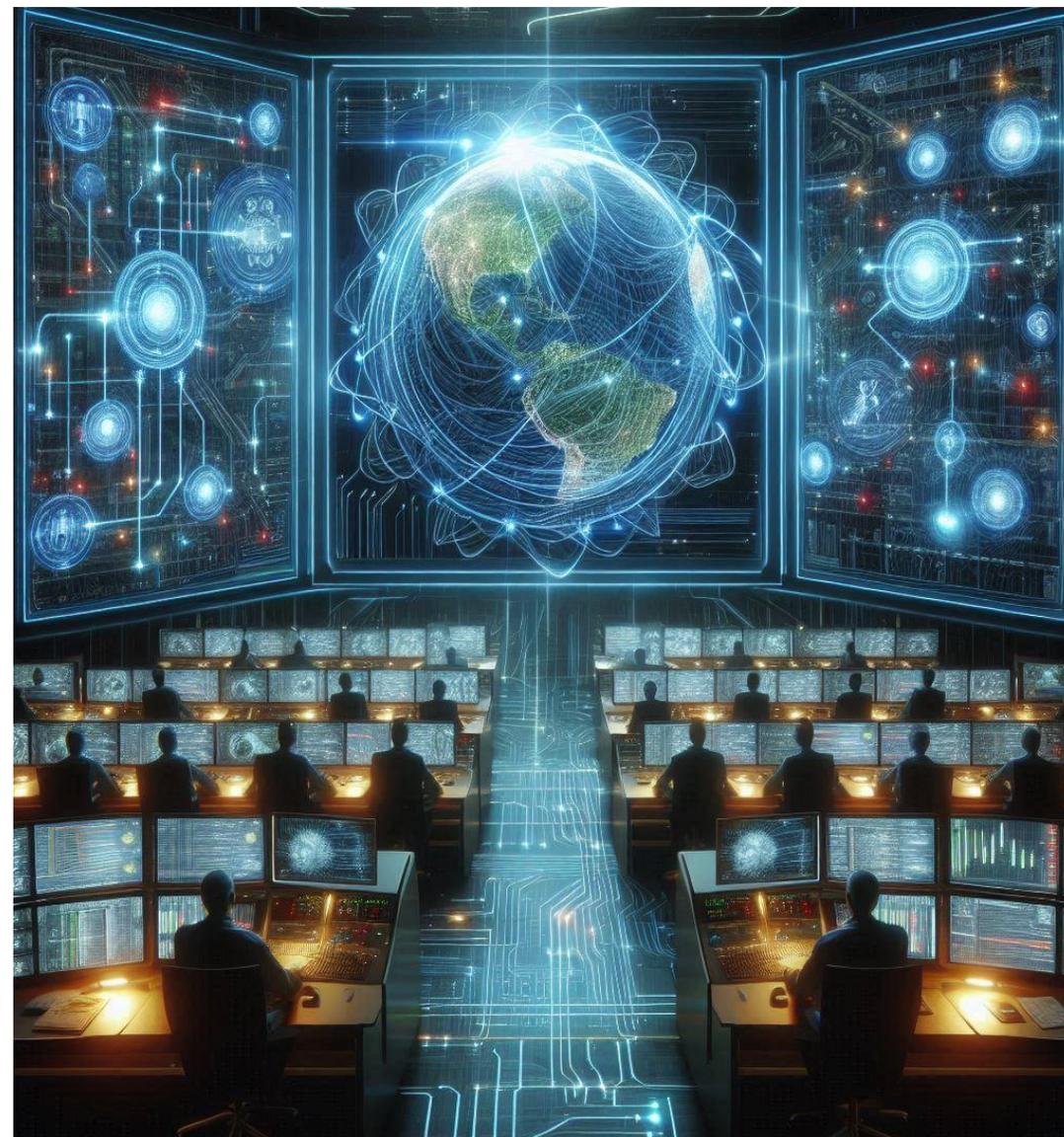
Programa por uma Internet mais Segura



Boas práticas de gerenciamento

- **Autenticação:** senhas, duplo fator
- **Acesso:** protocolos seguros
- **Monitorar:** interfaces entrada e saída
- **Sistema:** hardening e sistemas atualizados
- **Registros:** gerar e armazenar logs
- **Configurações:** backup e scripts atualizados
- **Autorização:** permissão de usuários
- **Auditoria:** registrar e classificar usuários

Ref: [Melhores Práticas de Hardening](#)
[Uso de Netflows para Segurança](#)





MANRS

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/>



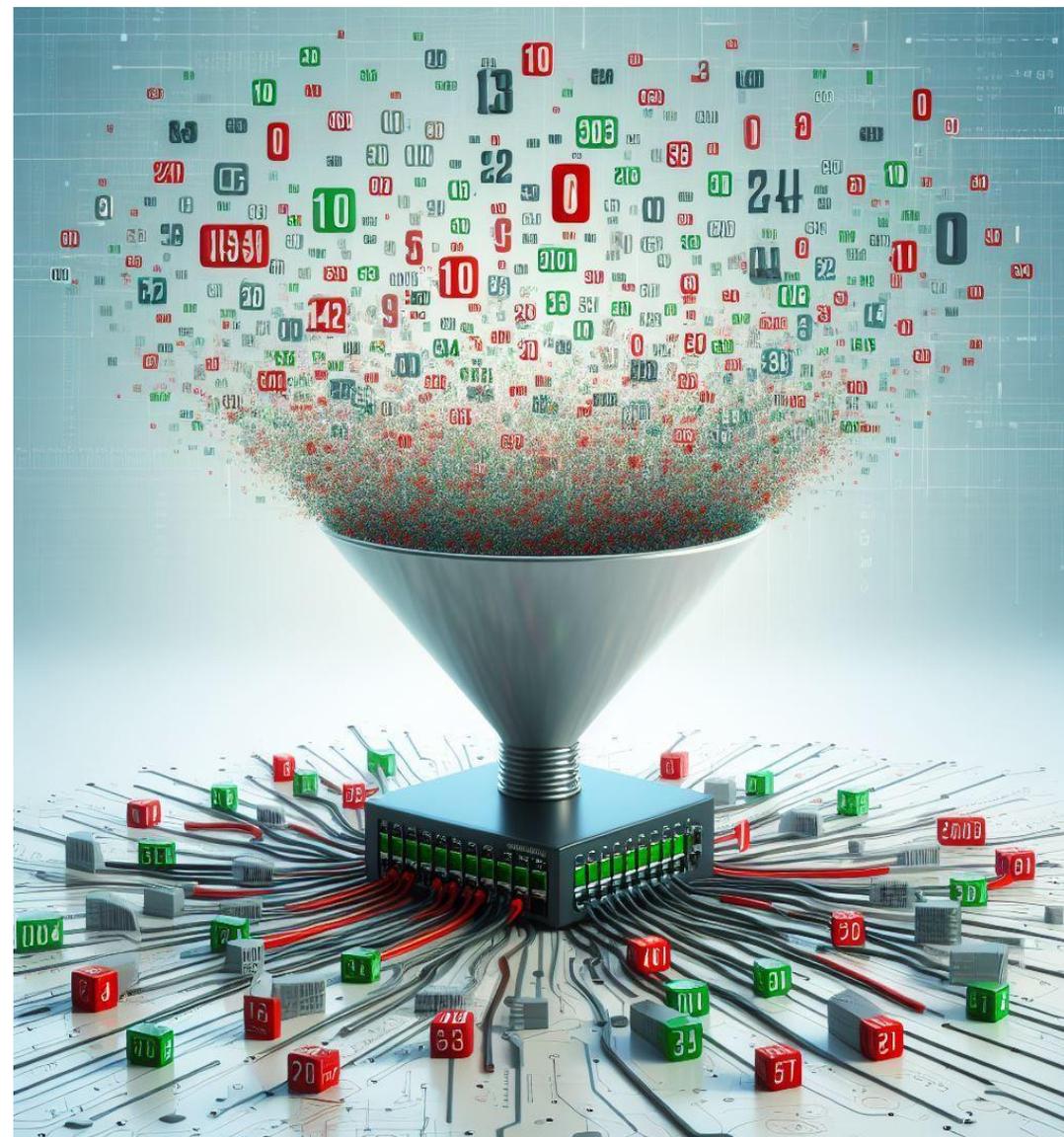
Programa por uma Internet mais Segura



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

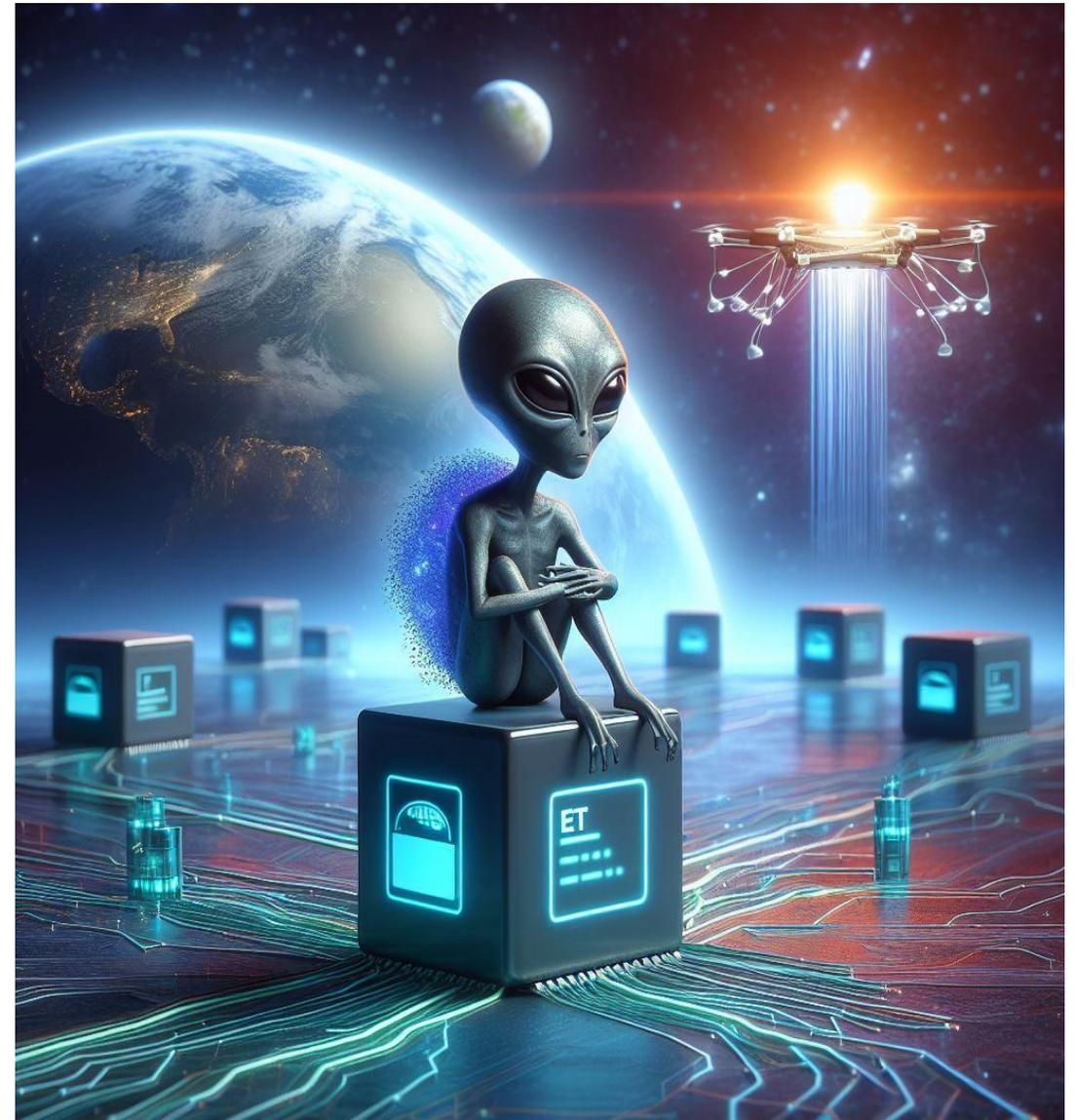


MANRS - Ação 2 - Filtro Anti Spoofing

- 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)!



<https://bcp.nic.br/antispoofing/>

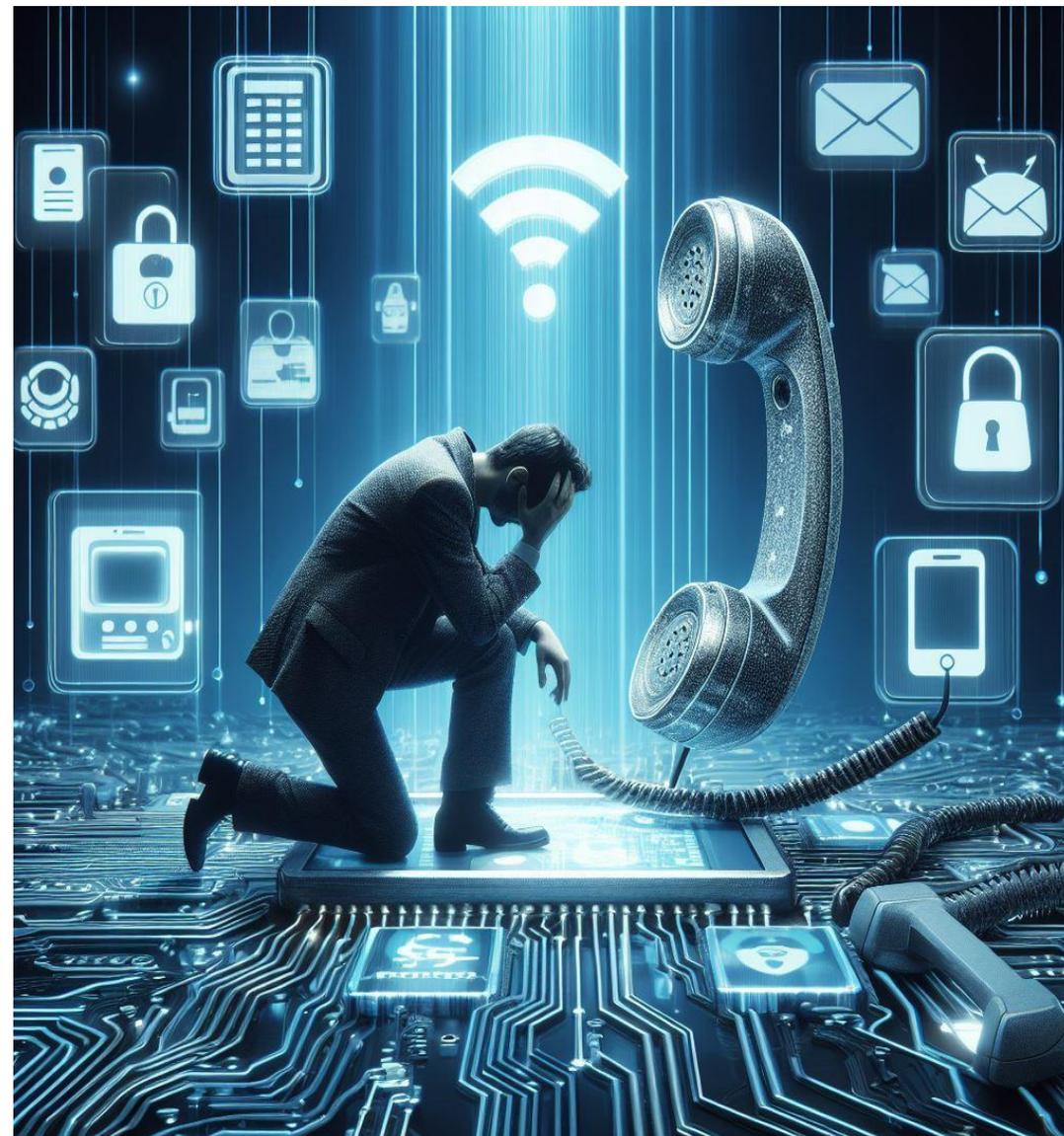


Programa por uma Internet mais Segura



MANRS - Ação 3 - Pontos de Contato

- Contatos de roteamento e abuse no **Registro.br** devem estar atualizados e serem de grupos de pessoas (RFC2142). 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



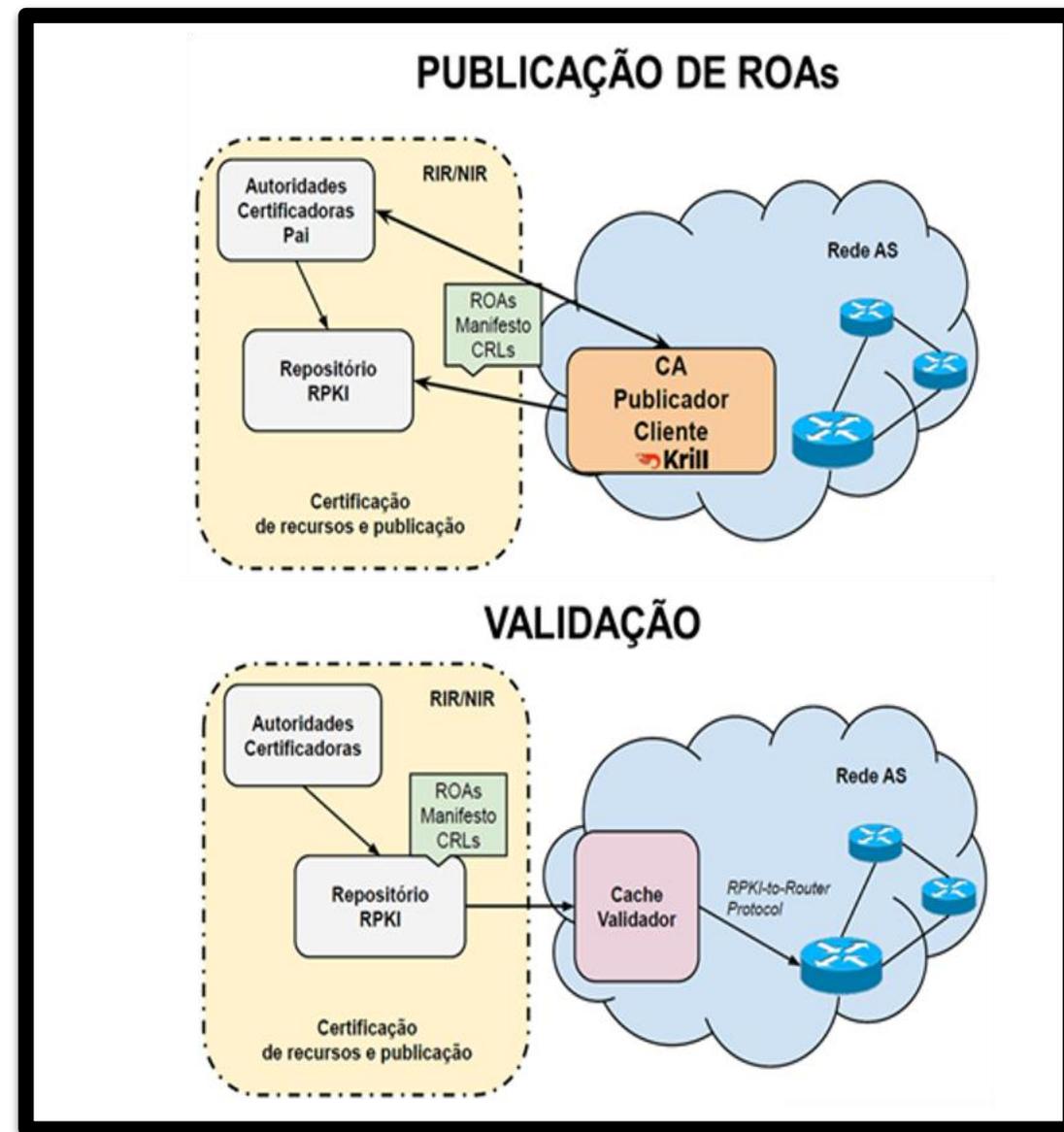
MANRS - Ação 4 - Cadastro da Política de Roteamento

- IRR - Internet Routing Registry
 - RADB
 - TC (gratuito)
- RPKI - Resource Public Key Infrastructure

Artigo: [War story: RPKI is working as intended](#)



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



Programa por uma Internet mais Segura

MANRS Observatory - Brasil - 8647 AS

Resumo

27-mai-25



MANRS

MANRS - Status da Segurança de Roteamento

Incidentes

Sequestro de Rota	39
Vazamento de Rota	0
Anúncio inválido	16
Total	55



Responsáveis

AS responsáveis 44



Informação de Roteamento

IRR

Não registrado 4.022 4,4%
Registrado 88.070 95,6%



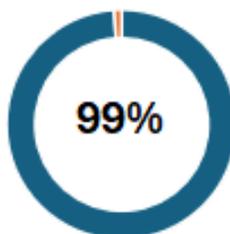
RPKI

Válido 43.896 47,7%
Desconhecido 48.018 52,1%
Inválido 178 0,2%

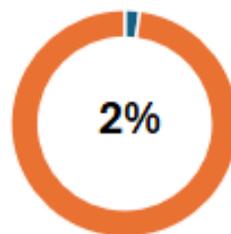


MANRS - Prontidão

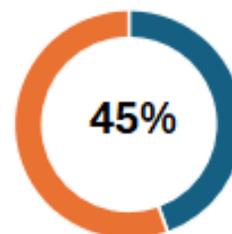
Filtros BGP



Anti-spoofing

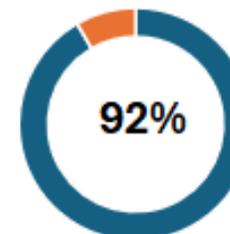


Coordenação

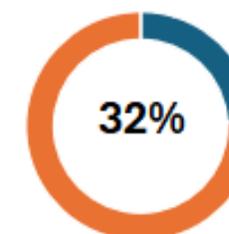


Informação de Roteamento

IRR



RPKI



Programa por uma Internet mais Segura



Participantes por país

- Total: 1195
- Participantes no Brasil → 302



MANRS

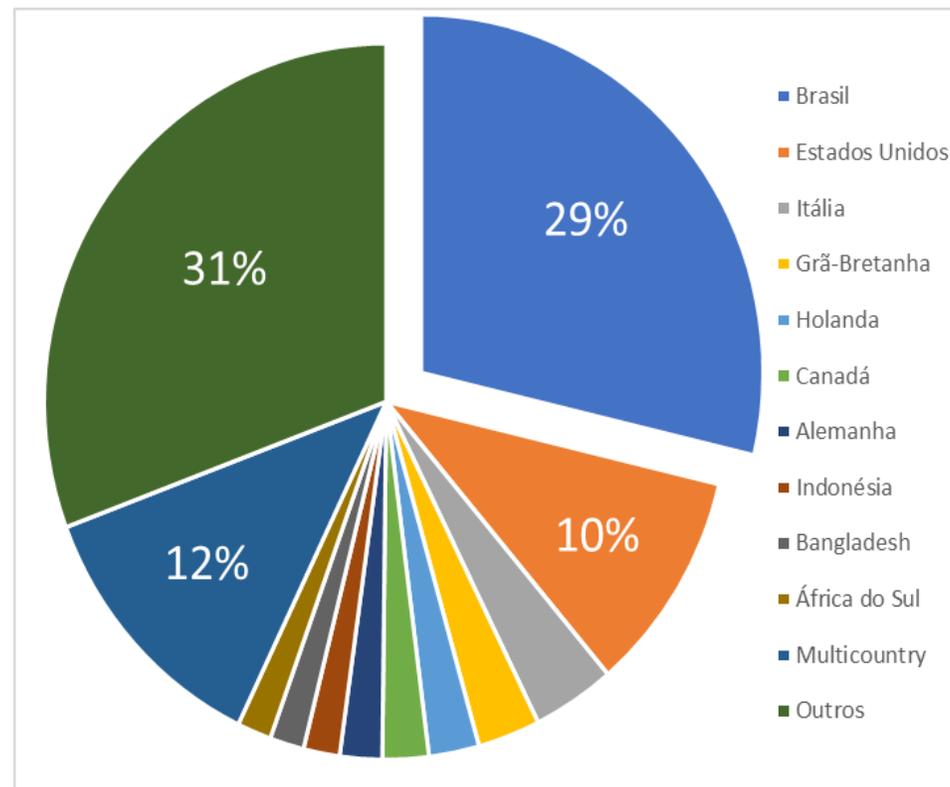
2023 → 258

2022 → 206

2021 → 174

2020 → 140

% de Participantes



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



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

<https://kindns.org/>



Programa por uma Internet mais 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

BCP: [Recomendações para Evitar o Abuso de Servidores DNS Recursivos Abertos](#)

<https://kindns.org/>  **KINDNS**

TOP

TESTE OS PADRÕES

<https://top.nic.br>

TOP
TESTE OS PADRÕES

Quem é TOP Sobre Referências Comunicados

Os padrões técnicos modernos de Internet aumentam a confiabilidade e permitem o crescimento da rede. Você está usando esses padrões?

Teste TOP - Site
Endereço IP moderno?
Domínio assinado? Conexão segura? Opções de segurança?

Nome de domínio do seu site:
www.exemplo.com.br

Iniciar o teste

Teste TOP - E-mail
Endereço IP moderno?
Domínio assinado? Proteção contra phishing? Conexão segura?

Nome de domínio do seu e-mail:
@exemplo.com.br

Iniciar o teste

Teste TOP - IPv6 e DNSSEC da sua rede
Endereços modernos acessíveis? Assinaturas de domínio validadas?

Iniciar o teste

Programa por uma Internet mais 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

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>



CAMADA 8
(nic.br)

**INTERNET
MAIS SEGURA**

COM GILBERTO ZORELLO,
COORDENADOR DE PROJETOS NO NIC.BR

Programa por uma Internet mais Segura

APOIO



A CONECTIVIDADE AO SEU ALCANCE



Obrigado

Gilberto Zorello

@ gzorello@nic.br



Antonio M Moreiras

@ moreiras@nic.br



30 de maio de 2025

nic.br cgi.br

www.nic.br | www.cgi.br