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

Atualizações sobre a iniciativa i+Seg

Gilberto Zorello | gzorello@nic.br

IX Fórum - Fortaleza

Fortaleza, CE | 08/08/24

registro.br nic.br cgi.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

Programa por uma Internet mais Segura

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

Programa por uma Internet mais Segura

Notificação de amplificadores

PROGRAMA INTERNET +SEGURA

Estatísticas das notificações encaminhadas pelo CERT.br

ASN	DNS	SNMP	NTP	SSDP	PORTMAP	MEMCACHED	NETBIOS	QOTD	CHARGEN	LDAP	MDNS	UBNT	WS-DICOVERY	TFTP	CoAP	ARMS	SLP	RIPv1	DHCPdiscover	2024-04	2024-05	2024-06	Mais Recente	MT4145	MT5678
ASN1	45	137	67	0	0	0	3	0	0	1	1	0	0	0	0	0	0	0	1	266	252	244	255	1	0
ASN2	12	21	259	0	0	0	5	0	0	0	0	1	0	0	0	0	0	0	0	314	288	302	298	0	0
Total	-30%	-4%	128%		-100%		0%			-45%	-33%	-59%		-100%	-100%				-8%	**580**	**540**	**546**	**553**	0%	

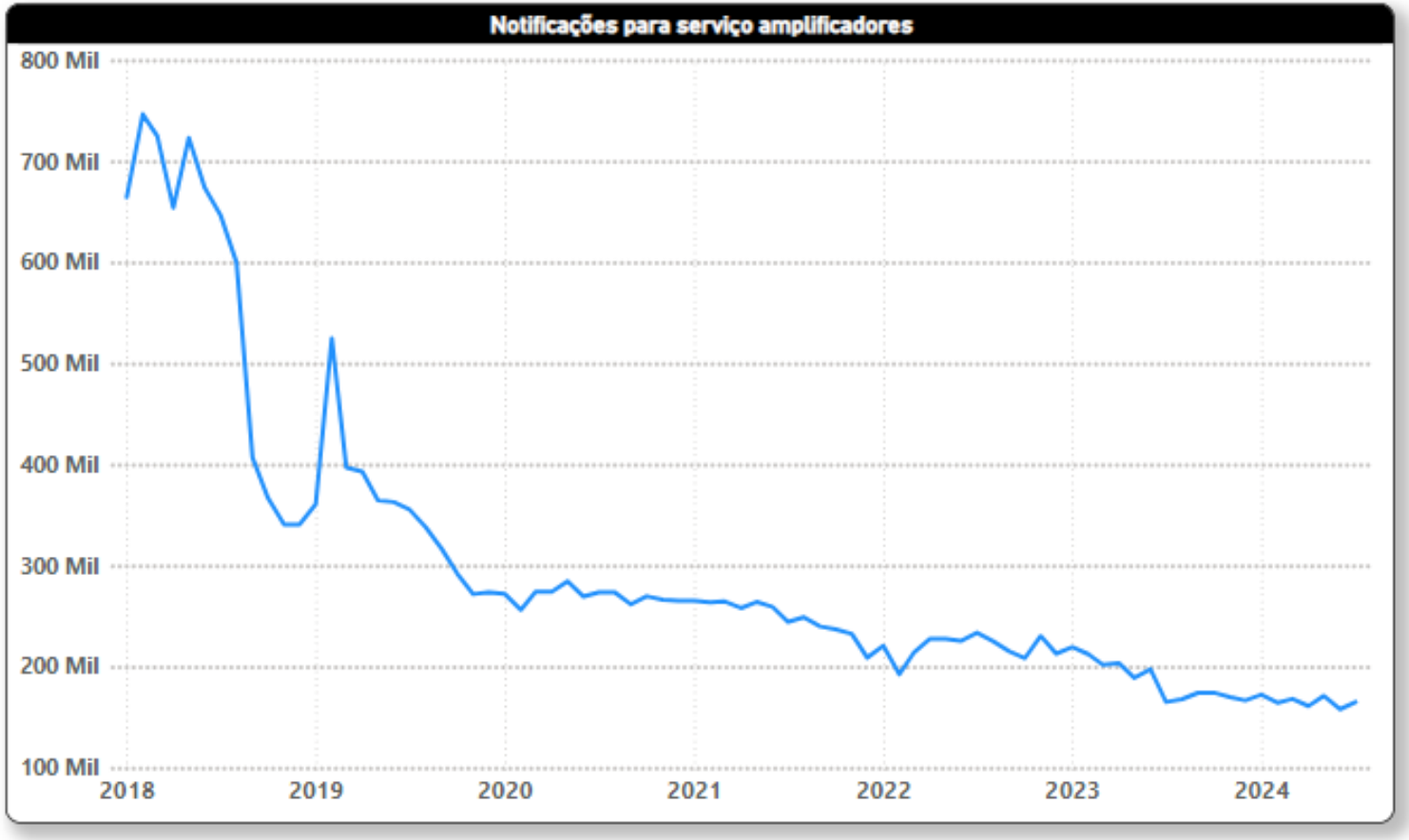
ASN	NTP																			NTP
	2023-01	2023-02	2023-03	2023-04	2023-05	2023-06	2023-07	2023-08	2023-09	2023-10	2023-11	2023-12	2024-01	2024-02	2024-03	2024-04	2024-05	2024-06	2024-07	
ASN1	248	248	246	248	247	249	3	2	2	3	3	4	11	71	68	73	71	65	67	67
ASN2	106	112	110	112	96	88	7	1	1	0	0	0	0	287	274	258	252	261	259	259
Total							10	3	3	3	3	4	11	358	342	331	323	326		128%

O serviço RIPv1 (Routing Information Protocol versão 1 passou a ser notificado em fev/24 pelo CERT.br

O serviço SLP (Service Location Protocol passou a ser notificado em nov/23 pelo CERT.br

Programa por uma Internet mais Segura

Notificação de amplificadores



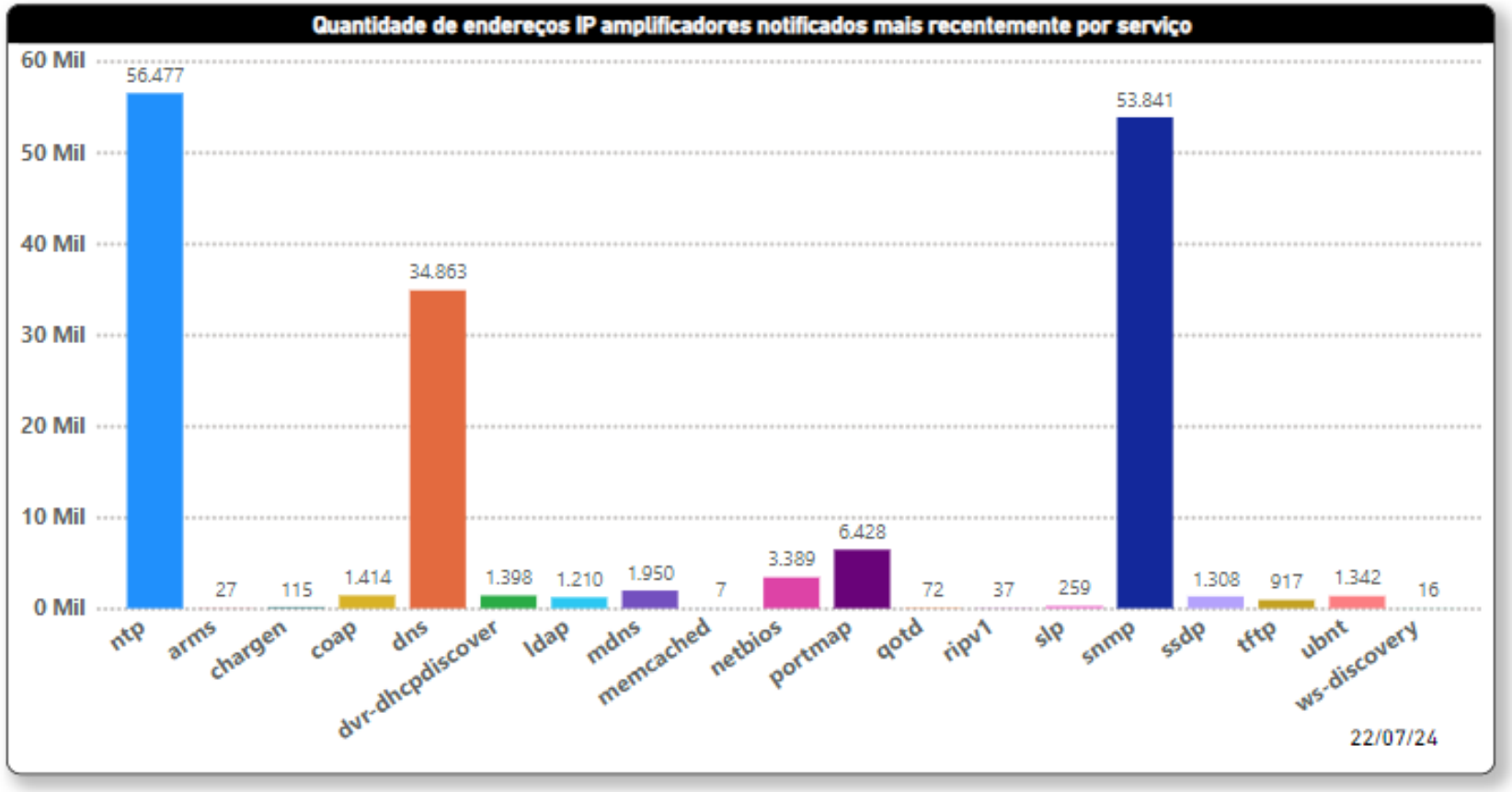
Total jul/24
165.070

43% Operadoras
57% ISPs/Corp

Redução de 77% dos endereços IP mal configurados desde o início do Programa

Programa por uma Internet mais Segura

Notificação de amplificadores



Principais ofensores: ISPs e ASes corporativos → SNMP habilitado e DNS recursivo aberto

Grandes operadoras → NTP mal configurado

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

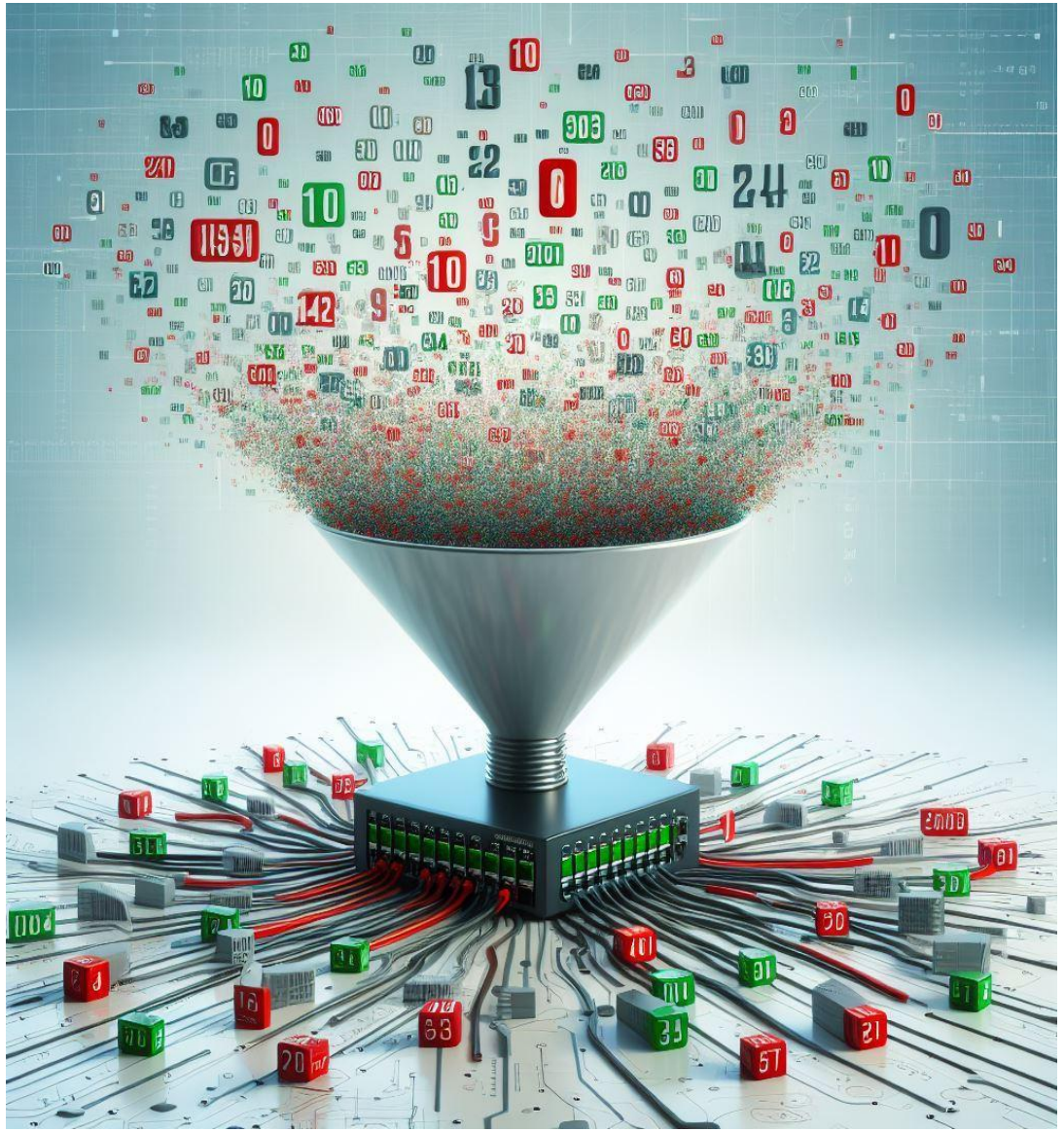
MANRS https://bcp.nic.br/i+seg/acoes/manrs/

Programa por uma Internet mais Segura

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

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

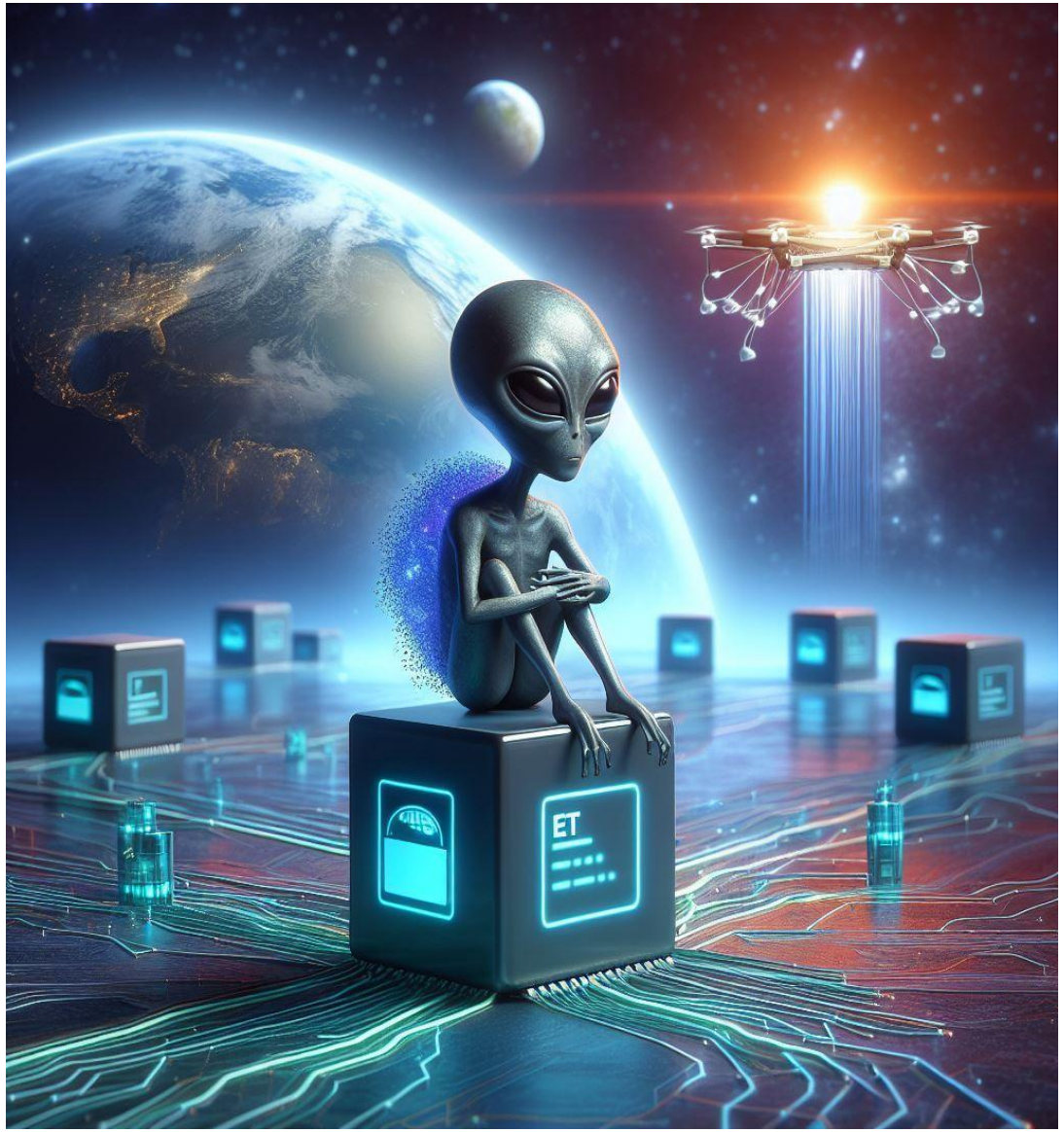
https://bcp.nic.br/i+seg/acoes/manrs/#filtragem-de-rotas



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

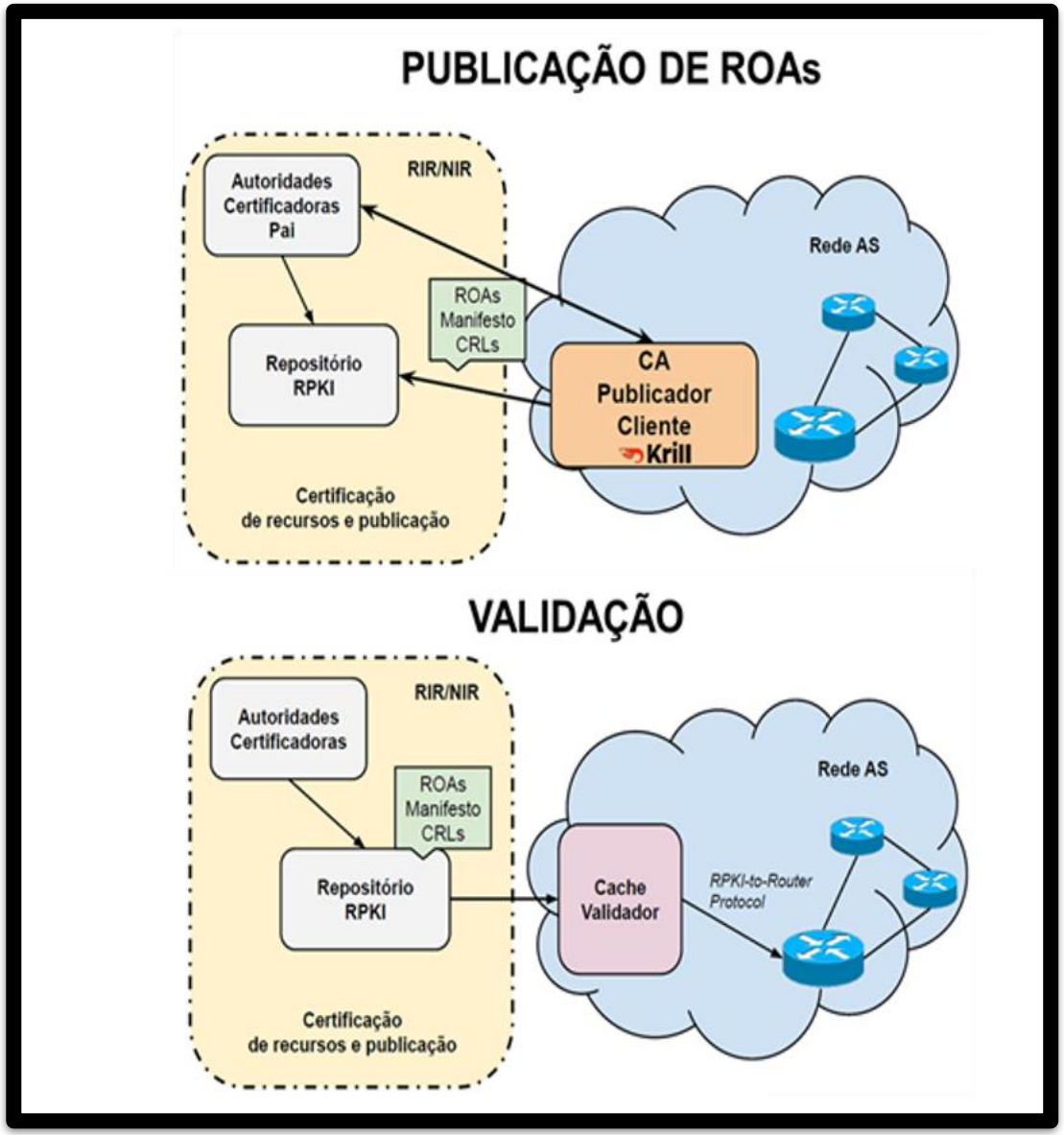
MANRS - Ação 4 - Cadastro da Política de Roteamento

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

- **RPKI** - Resource Public Key Infrastructure

MANRS

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



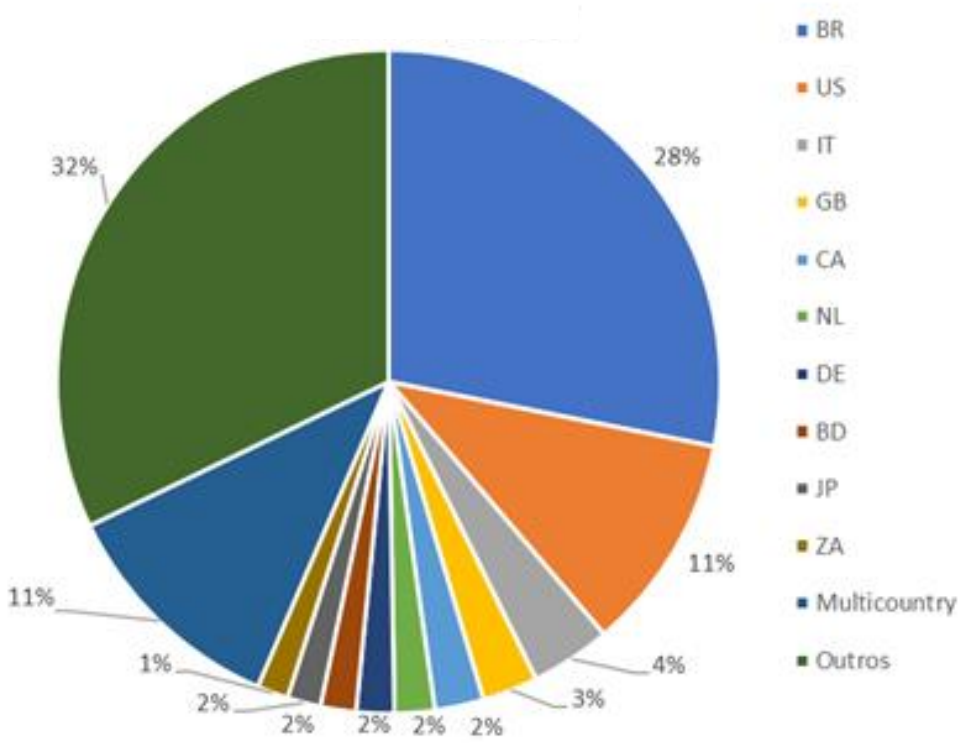
Programa por uma Internet mais Segura

Participantes por país

- Total: 942
- Participantes no Brasil → 265 (Jun/24)

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

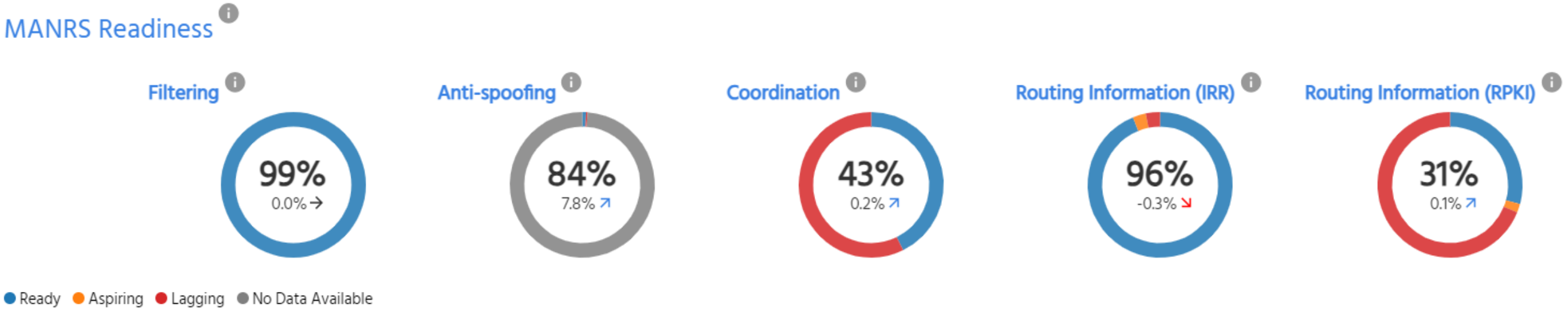
MANRS



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

Programa por uma Internet mais Segura
MANRS Observatory – Readiness – Ago/24

Conjunto de ASes do Brasil



Ação 1

Ação 2

Ação 3

Ação 4

Fonte: https://observatory.manrs.org/#/overview acesso 05/08/24

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

PROGRAMA INTERNET +SEGURA

Boas práticas para DNS

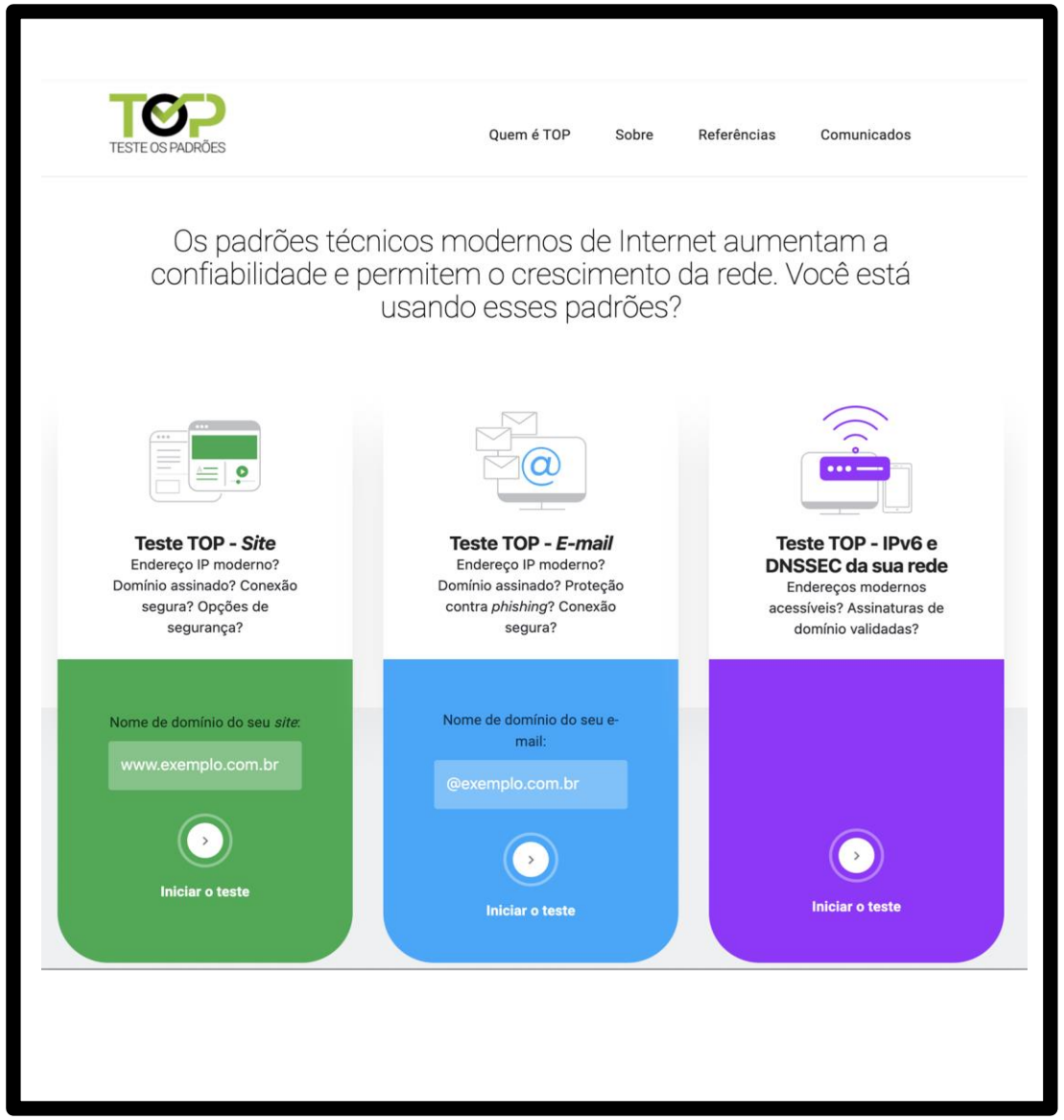
- KinDNS da ICANN (trocadilho em inglês)
- Configuração correta do recursivo somente para seus usuários
- Validação do DNSSEC no recursivo
- Configuração do autoritativo do seu nome de domínio com DNSSEC

https://kindns.org/

KINDNS

PROGRAMA INTERNET +SEGURA

https://top.nic.br



Programa por uma Internet mais Segura

PROGRAMA INTERNET +SEGURA

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

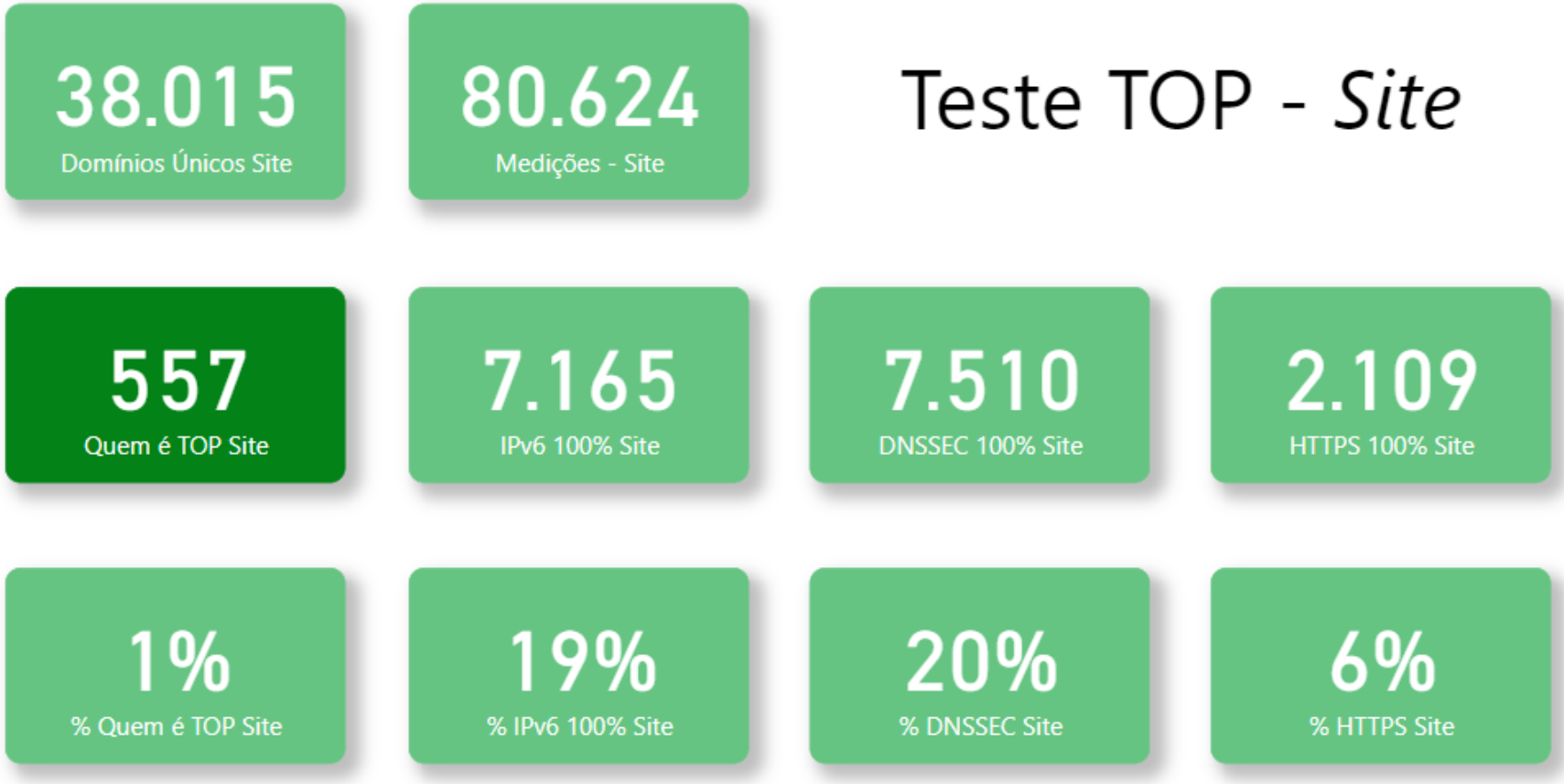
TOP – Teste os Padrões – Desenvolvimento

Teste TOP - IPv6 e DNSSEC da rede do usuário

TESTE OS PADRÕES

4/8/24

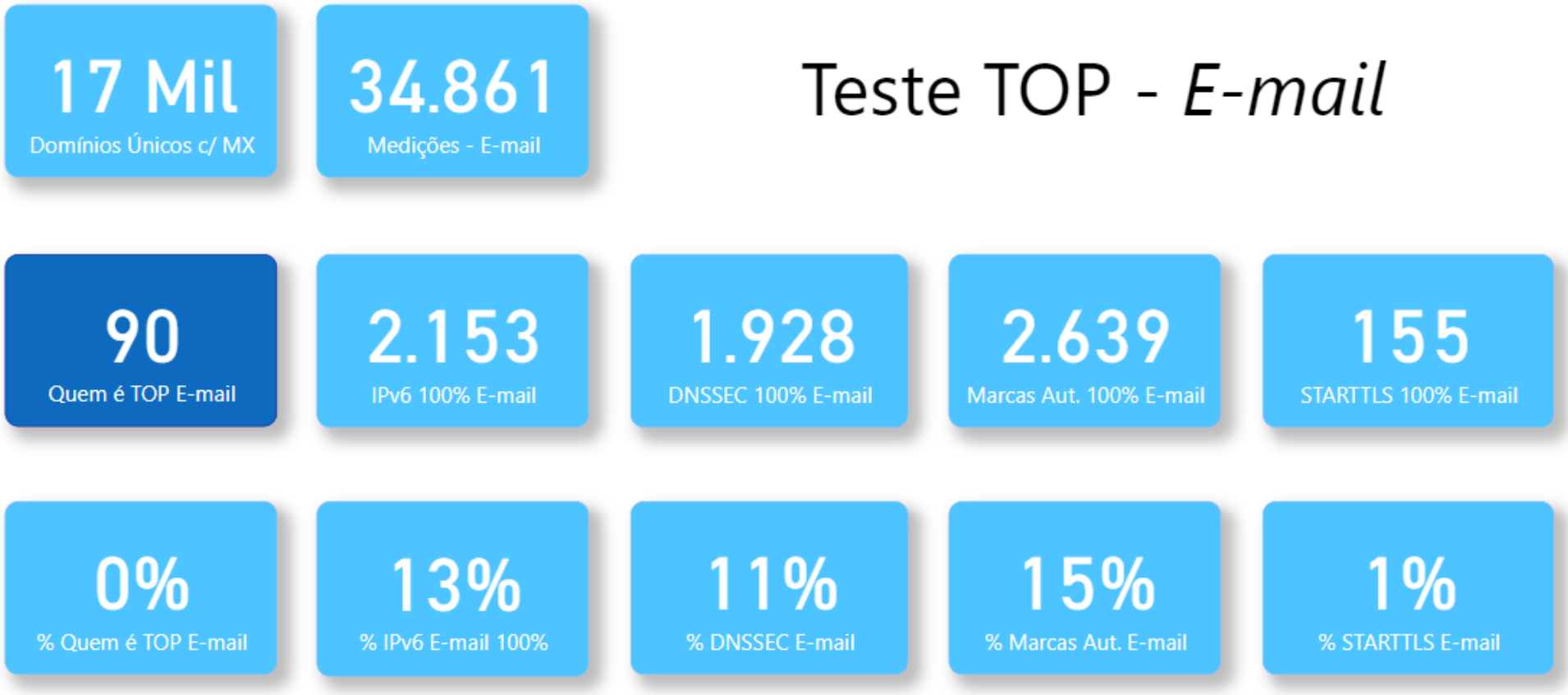
TOP – Teste os Padrões – Desenvolvimento



TESTE OS PADRÕES

4/8/24

TOP – Teste os Padrões – Desenvolvimento



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

Dúvidas ?

https://bcp.nic.br/i+seg (Programa)

https://top.nic.br

Obrigado

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

gzorello@nic.br

8 de agosto de 2024

nic.br cgi.br

www.nic.br | www.cgi.br