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

ATUALIZAÇÃO do PROGRAMA / MANRS / TOP

Gilberto Zorello | gzorello@nic.br

13ª Semana de Infraestrutura da Internet do Brasil – IX Fórum 17

São Paulo, SP | 6/12/23

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

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

Programa por uma Internet mais Segura

Objetivo

Atuar em apoio à comunidade técnica

Reduzir os ataques de Negação de Serviço

Melhorar a Segurança de Roteamento da rede

Reduzir as vulnerabilidades e falhas de configuração

Divulgar boas práticas que devem ser utilizadas

Incentivar a cultura de segurança entre os operadores

PROGRAMA INTERNET +SEGURA

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

Transversal no NIC.br: CERT.br, CEPTRO.br, IX.br, Registro.br, Sistemas, Comunicação

Programa por uma Internet mais Segura

Interação com provedores e operadoras

Reuniões bilaterais on-line com os responsáveis pelos ASes mais notificados e com operadoras

Ações tratadas nas reuniões bilaterais:

- **Correção dos serviços mal configurados notificados pelo CERT.br, que podem ser abusados em ataques DDoS**
- Adoção de Boas Práticas de roteamento (**MANRS**)
- **Adoção das práticas recomendadas e testadas pelo TOP**
- Apresentação de medições, por AS
- Envio de relatório gerencial mensal s/ serviços mal configurados

Programa por uma Internet mais Segura

Notificação de amplificadores

Estatísticas das notificações encaminhadas pelo CERT.br

ASN	SNMP	NTP	SSDP	PORTMAP	MEMCACHED	NETBIOS	QOTD	CHARGEN	LDAP	MDNS	UBNT	WS-DICOVERY	TFTP	CoAP	ARMS	SLP	DHCPDiscover	2023-08	2023-09	2023-10	Mais Recente	MT4145	MT5678
ASN1	103	42	0	23	0	3	0	0	1	2	0	0	3	0	1	3	0	205	204	209	199	0	0
ASN2	40	5	2	10	0	7	0	0	3	2	0	0	0	0	0	0	0	136	142	114	125	0	1
Total	11%	6%	26%	-5%		-20%			37%	-6%			-54%		9%		-100%	**341**	**346**	**323**	**321**		9%

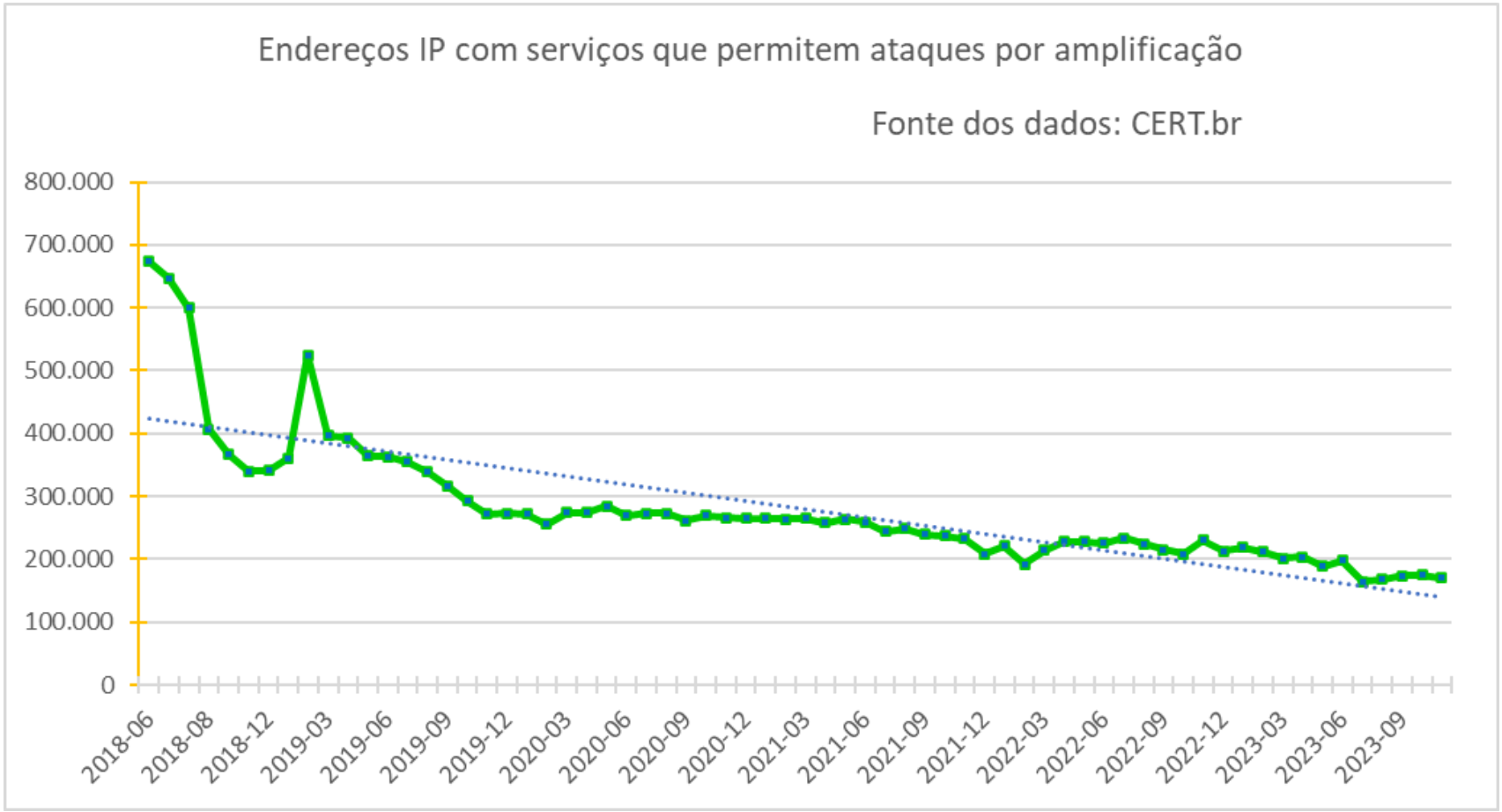
ASN	SNMP																	SNMP
	2022-07	2022-08	2022-09	2022-10	2022-11	2022-12	2023-01	2023-02	2023-03	2023-04	2023-05	2023-06	2023-07	2023-08	2023-09	2023-10	2023-11	
ASN1	64	55	57	66	83	84	87	87	81	85	109	110	115	116	104	111	103	103
ASN2	23	22	27	27	30	30	30	29	30	30	28	30	28	34	38	31	40	40
Total					113	114	117	116	111	115	137	140	143	150	142	142		11%

Novo: o serviço SLP (Service Location Protocol) passou a ser notificado em **nov/23** pelo CERT.br

236 ASNs - 354 IPs

Programa por uma Internet mais Segura

Notificação de amplificadores

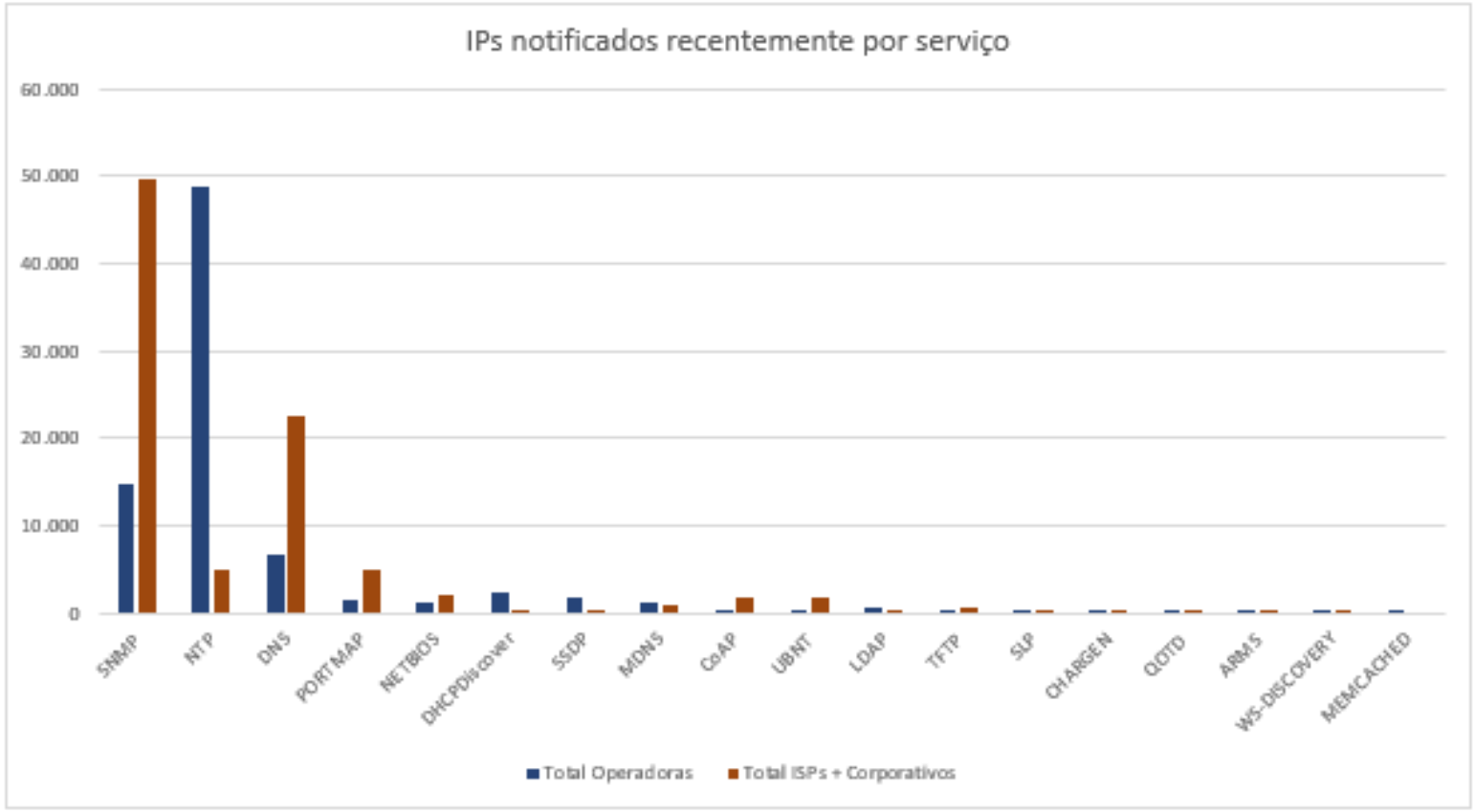


46% Operadoras
54% ISPs

Redução de 76% dos endereços IP mal configurados desde o início do Programa

Programa por uma Internet mais Segura

Notificação de amplificadores



Nov/23

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

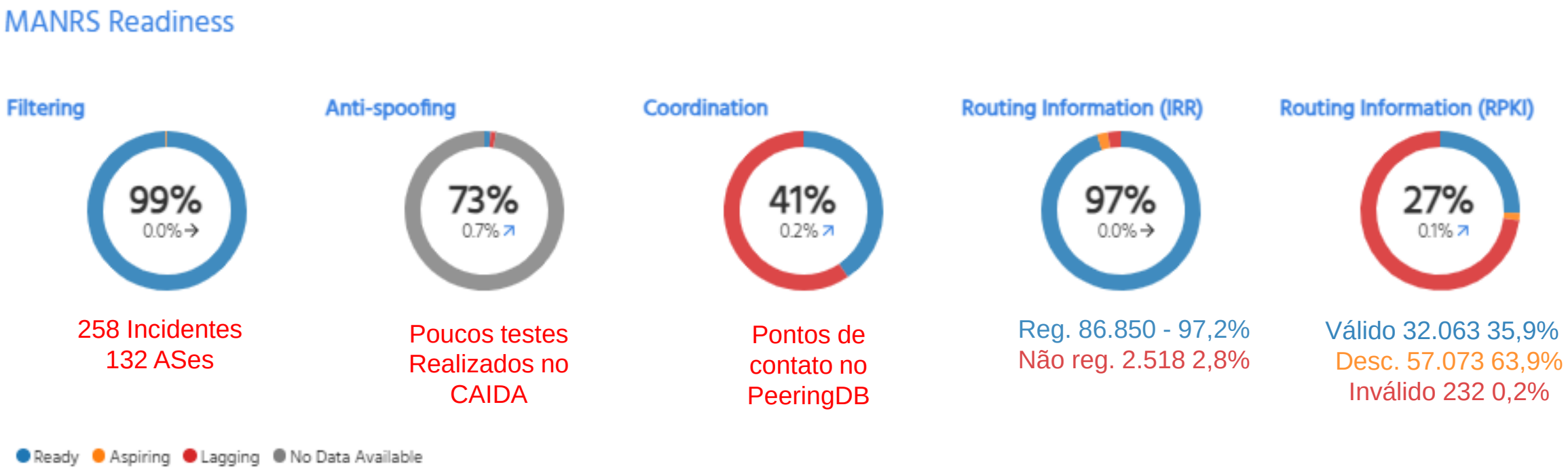
http://manrs.org

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

Programa por uma Internet mais Segura

MANRS Observatory – Readiness – Nov/23

Conjunto de ASes do Brasil



258 Incidentes
132 ASes

Poucos testes
Realizados no
CAIDA

Pontos de
contato no
PeeringDB

Reg. 86.850 - 97,2%
Não reg. 2.518 2,8%

Válido 32.063 35,9%
Desc. 57.073 63,9%
Inválido 232 0,2%

Ação 1

Ação 2

Ação 3

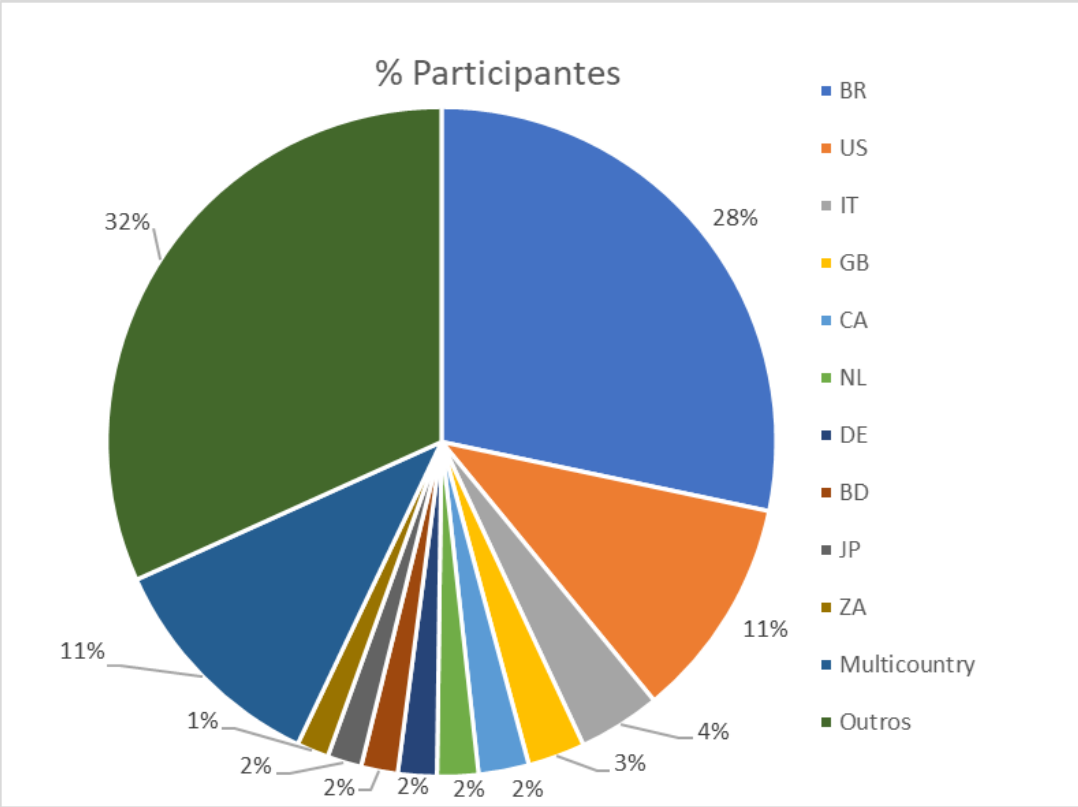
Ação 4

Fonte: https://observatory.manrs.org/#/overview acesso 30/11/23

Programa por uma Internet mais Segura

MANRS - Participantes

Distribuição por país dos participantes da iniciativa MANRS



Fonte: https://www.manrs.org/netops/participants/ Acesso nov/23

Total de participantes: 904

Participantes do Brasil: 256

206 (2022)

174 (2021)

140 (2020)

A Global Cyber Alliance assumiu a Gestão operacional do MANRS (nov/23)

An ICANN Initiative

ICANN

PROGRAMA INTERNET +SEGURA

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

https://kindns.org /

Programa por uma Internet mais Segura
KINDNS

Promove boas práticas de segurança de DNS

Programa de participantes do **KINDNS** - https://kindns.org/support-engage/)

5 categorias:

- **TLD & Zonas Críticas** — **Autoritativos**
- **Zonas SLD** — **Autoritativos**
- **Privado** — **Recursivos**
- **Privado Compartilhado** — **Recursivos**
- **Público** — **Recursivos**

Fonte: https://kindns.org/

Programa por uma Internet mais Segura
KINDNS – Privado Compartilhado

1. **A validação DNSSEC DEVE ser habilitada para servidores recursivos (TOP)**
2. ACLs DEVEM ser usadas para restringir quem pode enviar consultas recursivas aos seus servidores/validadores DNS
3. **A minimização QNAME DEVE ser habilitada para mitigar o vazamento de nomes de domínio (Privacidade)**
4. Os serviços DNS autoritativos e recursivos NÃO DEVEM coexistir no mesmo servidor DNS
5. **Seus serviços de recursão DEVEM ter resiliência usando pelo menos dois servidores distintos que levem em consideração a diversidade (Programas, Redes e Geográfica)**
6. DEVE ser implementado o monitoramento dos serviços, servidores e equipamentos de rede que compõem sua infraestrutura DNS
7. **Adicionalmente recomenda-se que DoT (DNS-sobre-TLS) ou DoH (DNS-sobre-HTTPS) DEVAM estar habilitados (Privacidade)**

Fonte: https://kindns.org/

https://top.nic.br

Programa por uma Internet mais Segura
TOP – Teste os Padrões – O que é?

Ajuda a verificar se a Internet que utiliza está seguindo os padrões abertos mais recentes de Internet

Teste TOP - IPv6 e DNSSEC (Conexão do usuário)

Teste TOP – *Site* (IPv6, DNSSEC, TLS, Opções de Segurança)

Teste TOP – *E-mail* (IPv6, DNSSEC, STARTTLS, DMARC)

Acesso: https://top.nic.br

Programa por uma Internet mais Segura

Teste TOP - IPv6 e DNSSEC da rede do usuário

KINDNS **Action 1 – Shared Private Resolver**

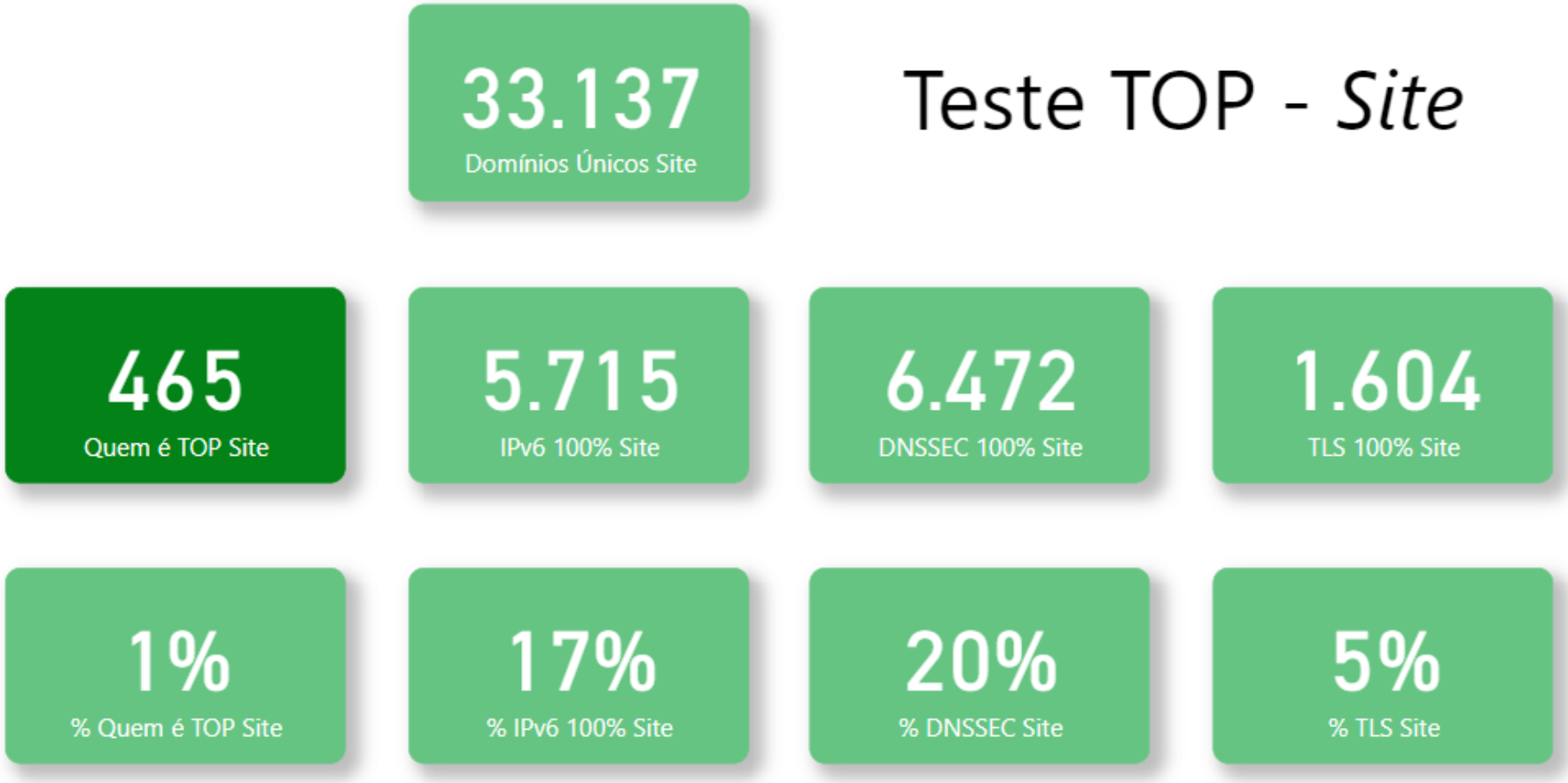
161.851 Med. - IPv6 DNSSEC Final.	105.116 DNS Rec com DNSSEC Validado	65% % DNS Rec c/ DNSSEC Validado
5.963 AS Únicos Testados	101.793 Usuários com IPv6 100%	63% % Usuários IPv6 100%

Medições totais IPv6 100%

TOP TESTE OS PADRÕES

1/12/23

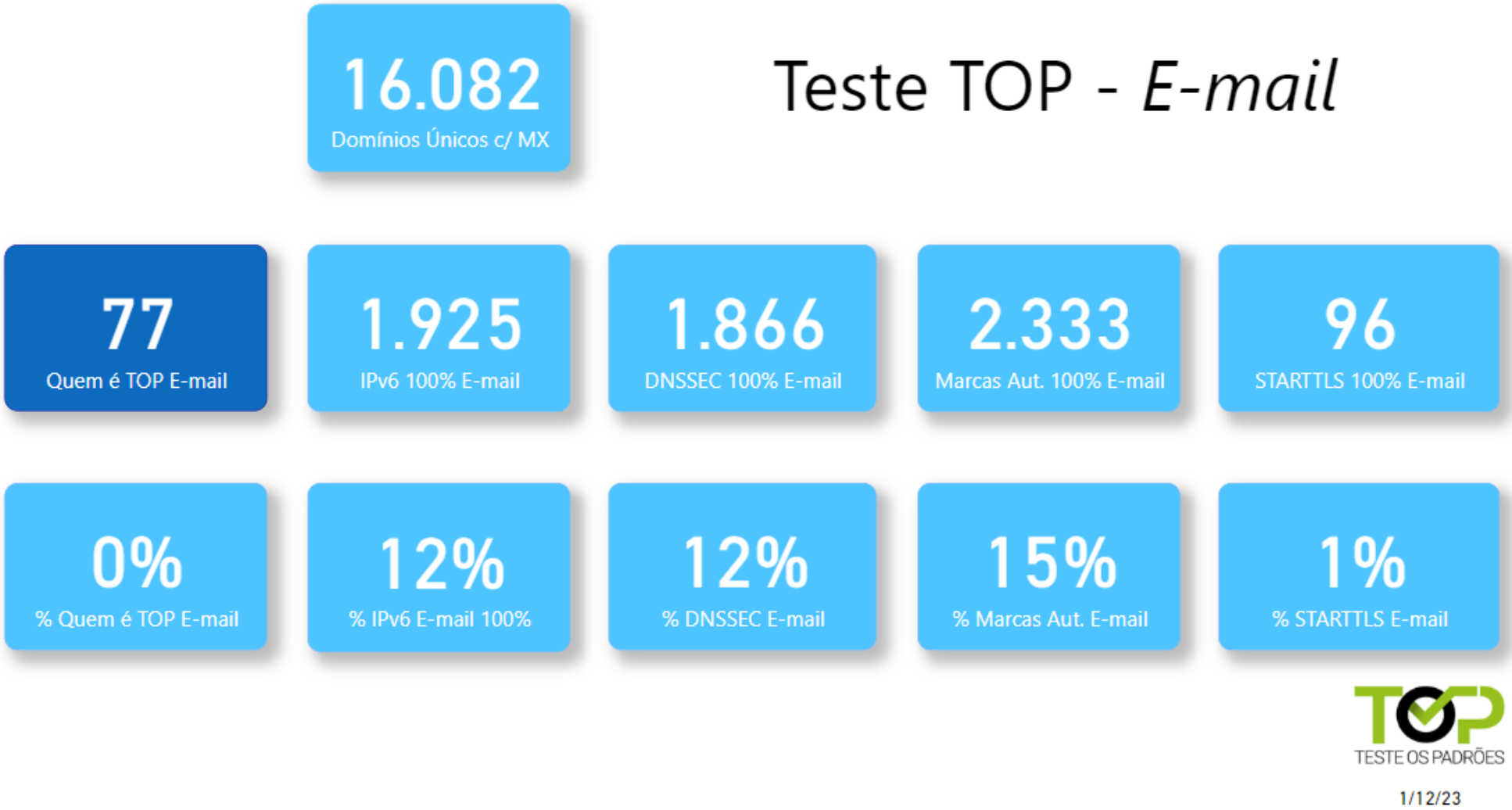
Programa por uma Internet mais Segura



TESTE OS PADRÕES

1/12/23

Programa por uma Internet mais Segura



TOP – Teste os Padrões - Apoio

TESTE OS PADRÕES

https://top.nic.br

conexis brasil.digital
A CONECTIVIDADE AO SEU ALCANCE

abranet
Associação Brasileira de Internet

AbraHosting
ASSOCIAÇÃO BRASILEIRA DE EMPRESAS DE INFRAESTRUTURA DE HOSPEDAGEM NA INTERNET

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

Dúvidas

?

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

https://top.nic.br

Obrigado

Gilberto Zorello

gzorello@nic.br

6 de dezembro de 2023

nic.br cgi.br

www.nic.br | www.cgi.br