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

Semana de Infraestrutura da Internet do Brasil – IX Fórum 16

São Paulo, SP | 27/10/22

registro.br nic.br cgi.br

Nossa
Agenda

Programa por uma Internet mais Segura

- Objetivo / Plano de Ação
- Desenvolvimento do Programa

TOP – Teste os Padrões

- Desenvolvimento da ação

Programa por uma Internet mais Segura

Objetivo

Atuar em apoio à comunidade técnica da Internet:

- Redução dos ataques de Negação de Serviço
- **Melhora da Segurança de Roteamento na rede**
- Redução das vulnerabilidades e falhas de configuração
- **Incentivar o crescimento de uma cultura de segurança entre os operadores da rede**

PROGRAMA INTERNET +SEGURA

Programa por uma Internet mais Segura
Plano de Ação

Ações executadas pelo NIC.br com os operadores dos ASes:

- Transversal no NIC.br: CERT.br, CEPTRO.br, IX.br, Registro.br, Sistemas
- **Conscientização por meio de palestras, cursos e treinamentos**
- Criação de materiais didáticos e boas práticas
- Interação com Operadores da rede para disseminação da **cultura de segurança**, **adoção de melhores práticas** e **mitigação dos problemas existentes**
- Implementação de filtros de rotas no IX.br, que contribui para a melhora do cenário geral
- **Estabelecimento de métricas e acompanhamento da efetividade das ações**

PROGRAMA INTERNET +SEGURA

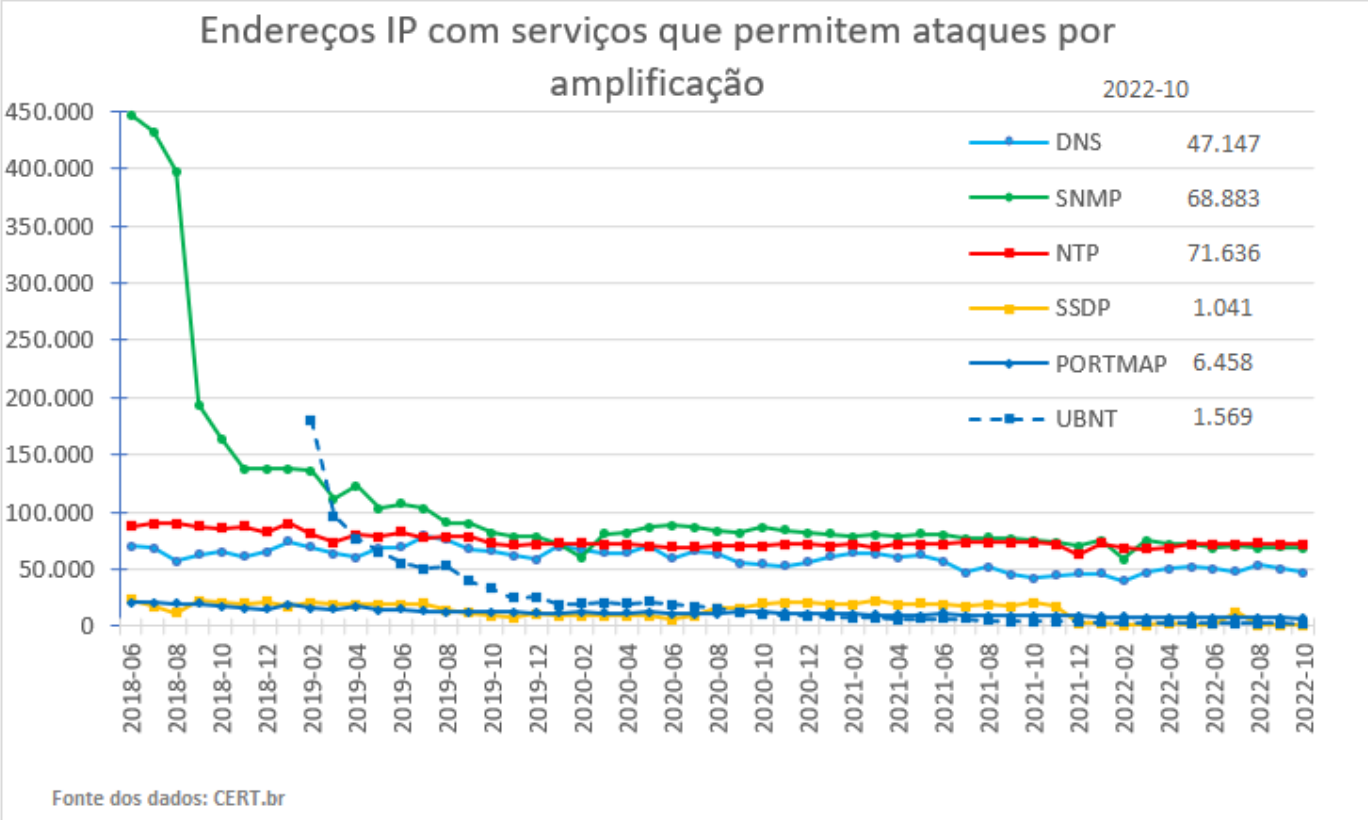
https://bcp.nic.br/i+seg

Programa por uma Internet mais Segura
Interação com Operadores

- Reuniões bilaterais periódicas com as grandes operadoras
- **Reuniões *on-line* com os responsáveis pelos ASes com maior quantidade de endereços IP notificados**
- Envio de relatório gerencial mensal para o acompanhamento da resolução dos problemas notificados pelo CERT.br
- **Apoio às grandes operadoras para implantação do RPKI em suas redes**
- Temas tratados nas reuniões bilaterais:
  - **Acompanhamento da correção dos serviços mal configurados notificados pelo CERT.br, que podem ser abusados para fazer parte de ataques DDoS**
  - Adoção de Boas Práticas de roteamento (MANRS)
  - **TOP – Teste os Padrões**

Programa por uma Internet mais Segura
Desenvolvimento do Programa

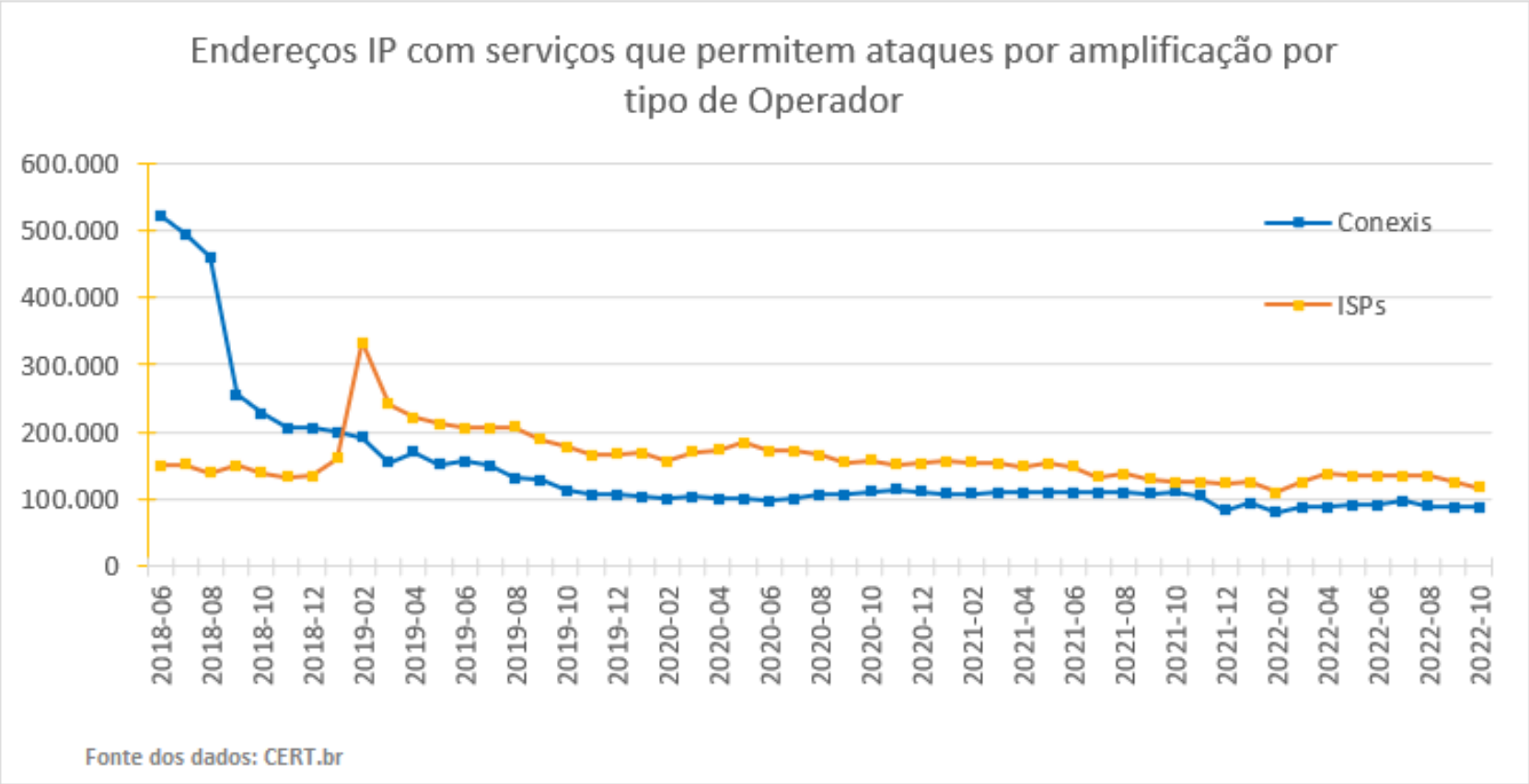
- Quantidade de endereços IP notificados com serviços mal configurados



Redução de 71% dos endereços IP mal configurados desde o início do Programa

Programa por uma Internet mais Segura
Desenvolvimento do Programa

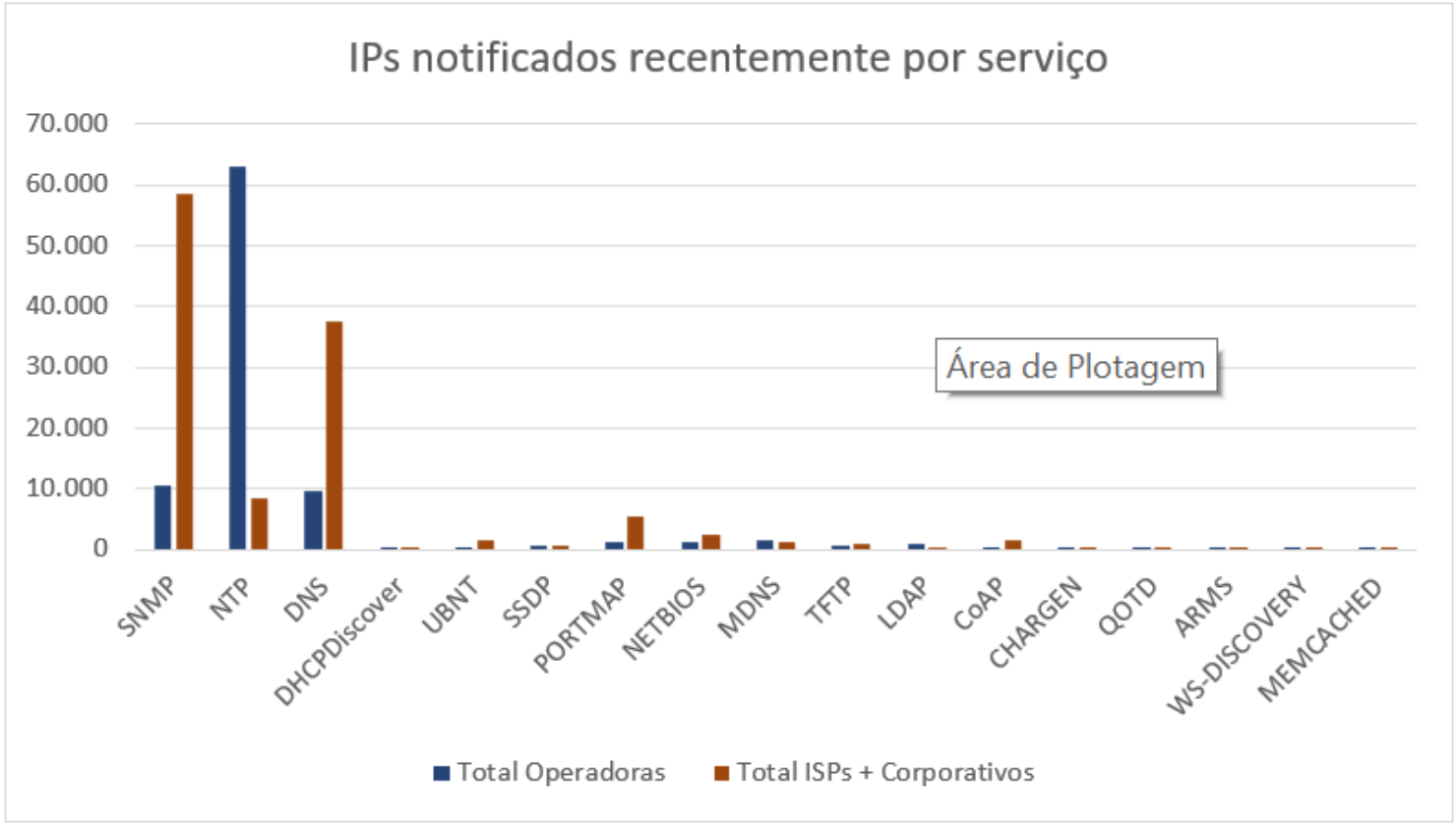
- Quantidade de endereços IP notificados por tipo de operador



A quantidade de endereços IP notificados para grandes operadoras e ISPs é da mesma ordem de grandeza

Programa por uma Internet mais Segura
Desenvolvimento do Programa

- Quantidade de endereços IP notificados por tipo de serviço



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

Grandes operadoras → NTP mal configurado

MANRS

PROGRAMA INTERNET +SEGURA

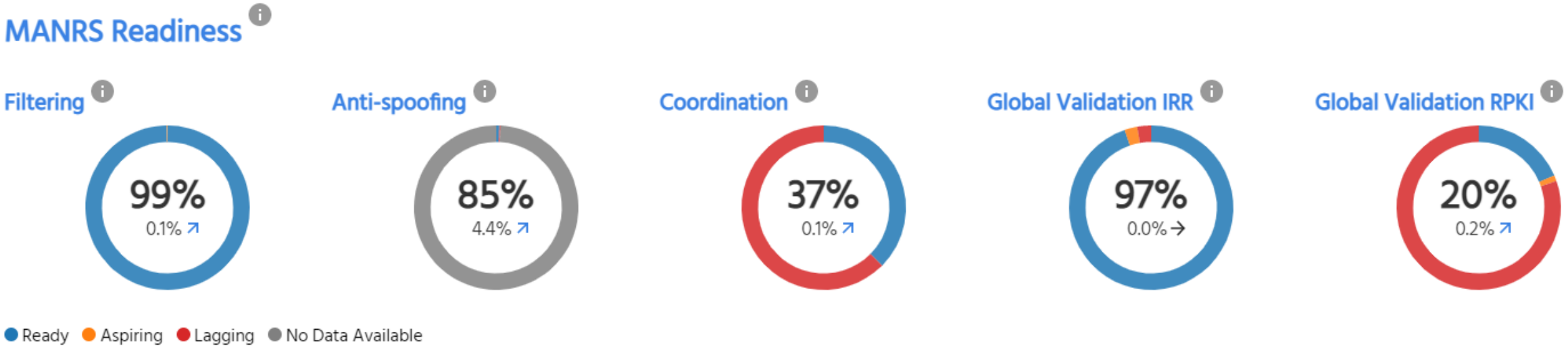
Mutually Agreed Norms for Routing Security

http://manrs.org

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

Programa por uma Internet mais Segura
MANRS Observatory – Readiness – Out/22

Conjunto de ASes do Brasil



Ação 1

Ação 2

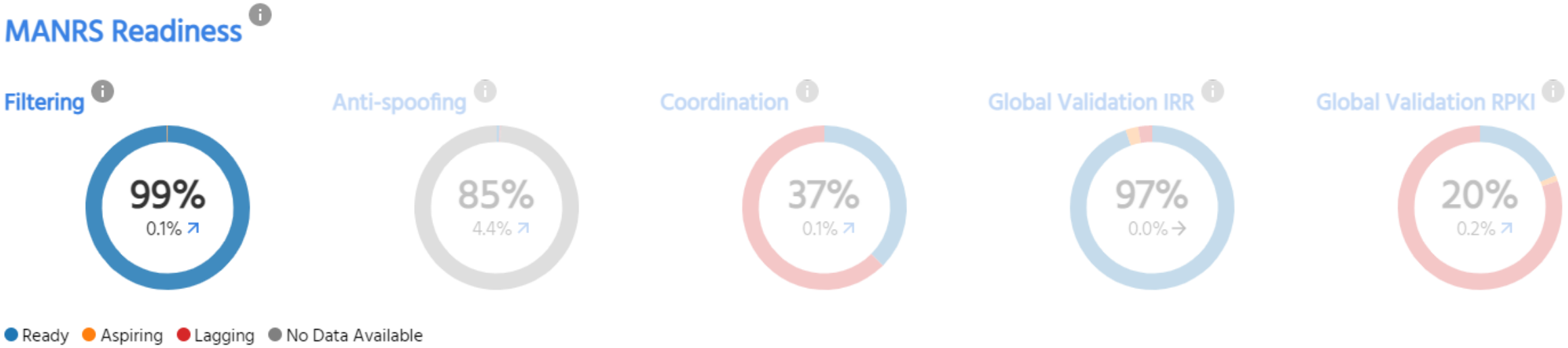
Ação 3

Ação 4

Fonte: https://observatory.manrs.org/#/overview acesso 17/10/22

Programa por uma Internet mais Segura
MANRS Observatory – Readiness – Out/22 – Ação 1

Conjunto de ASes do Brasil



Meses com incidentes *

- 9 - 12 → 40 ASes → Análise dos últimos 12 meses
- 5 - 8 → 46 ASes → 8 métricas para análise de Hijacking e Leak
- 1 - 4 → 758 ASes

Incidents (out/22) #

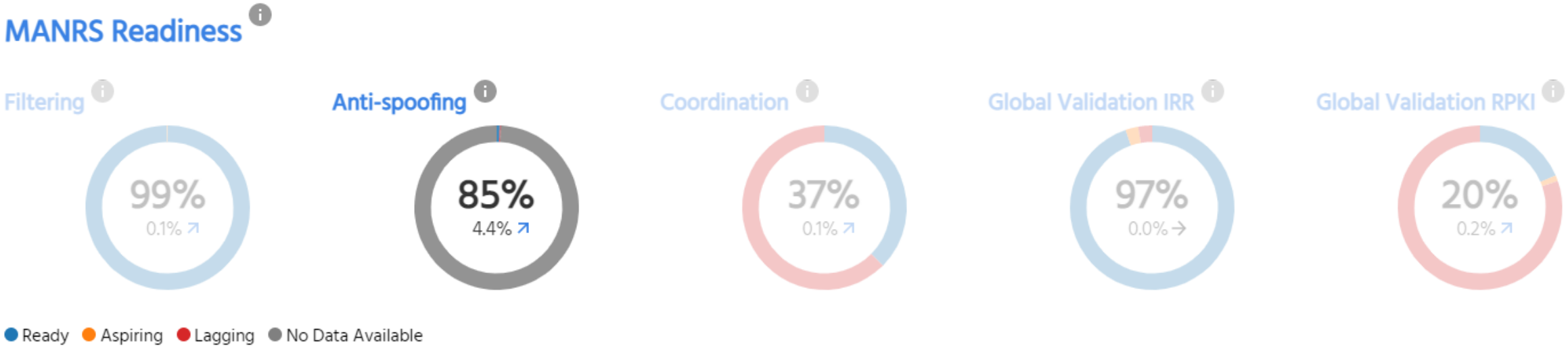
- Route misoriginations → 35
- Route Leaks → 1
- Bogon announcements → 57
- Networks that caused incidentes → 66

* Fonte: MANRS Observatory, acesso logado em 17/10/22

Fonte: https://observatory.manrs.org/#/overview acesso em 18/10/22

Programa por uma Internet mais Segura
MANRS Observatory – Readiness – Out/22 – Ação 2

Conjunto de ASes do Brasil



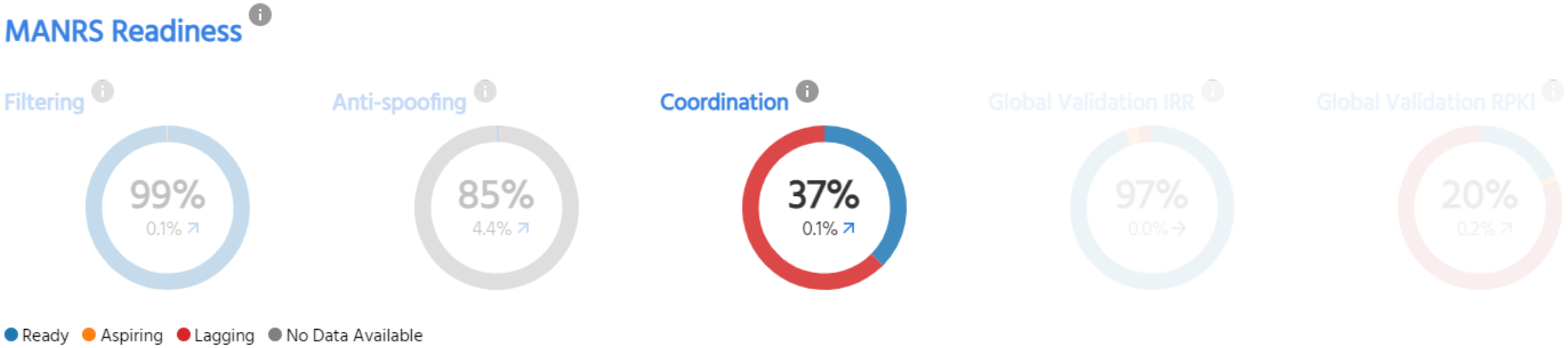
- Medição no CAIDA Spoofer
- Depende de testes realizados pelos usuários
- Poucos testes realizados (477 Ases) #
- 196 ASes com blocos IP que permitem tráfego spoofado #

Fonte: https://observatory.manrs.org/#/overview acesso 17/10/22

Fonte: https://spoofer.caida.org/as_stats.php acesso em 18/10/22

Programa por uma Internet mais Segura
MANRS Observatory – Readiness – Out/22 – Ação 3

Conjunto de ASes do Brasil

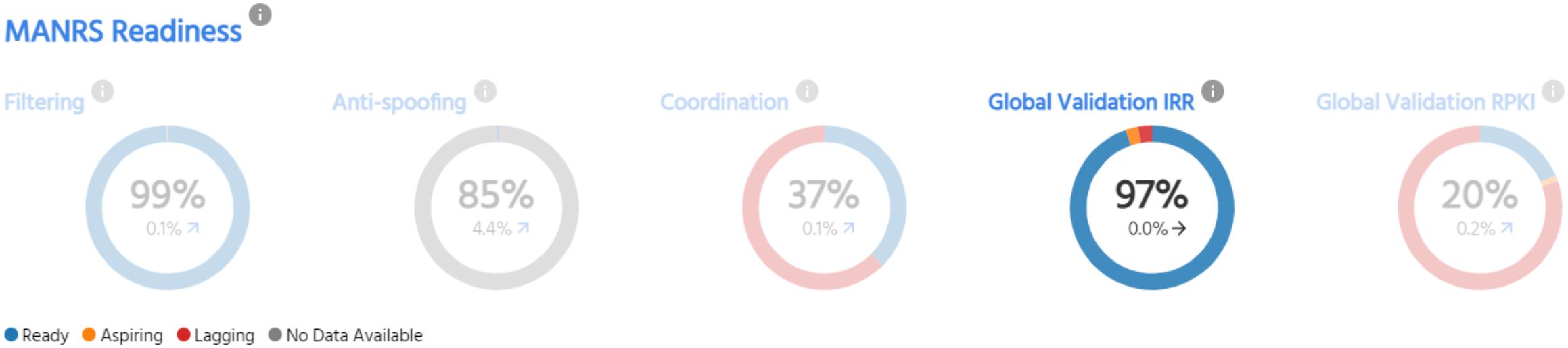


% de cadastros de ponto de contato técnico no PeeringDB

Fonte: https://observatory.manrs.org/#/overview acesso 17/10/22

Programa por uma Internet mais Segura
MANRS Observatory – Readiness – Out/22 – Ação 4 (IRR)

Conjunto de ASes do Brasil



Registros (Ases) *
- Sem → 124
- Incompletos → 323

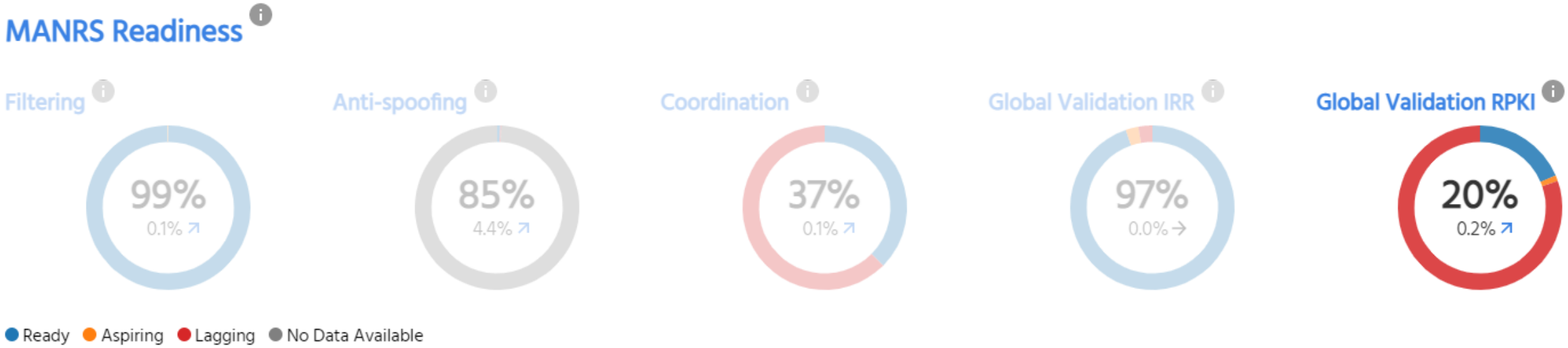
Routing completeness (IRR) #
- Unregistered → 4.108 4,9%
- Registered → 80.067 95,1%

* Fonte: MANRS Observatory, acesso logado em 17/10/22

Fonte: https://observatory.manrs.org/#/overview acesso 18/10/22

Programa por uma Internet mais Segura
MANRS Observatory – Readiness – Out/22 – Ação 4 (RPKI)

Conjunto de ASes do Brasil



ROAs (Ases) *
- Válidos → 1534
- Inválidos → 159

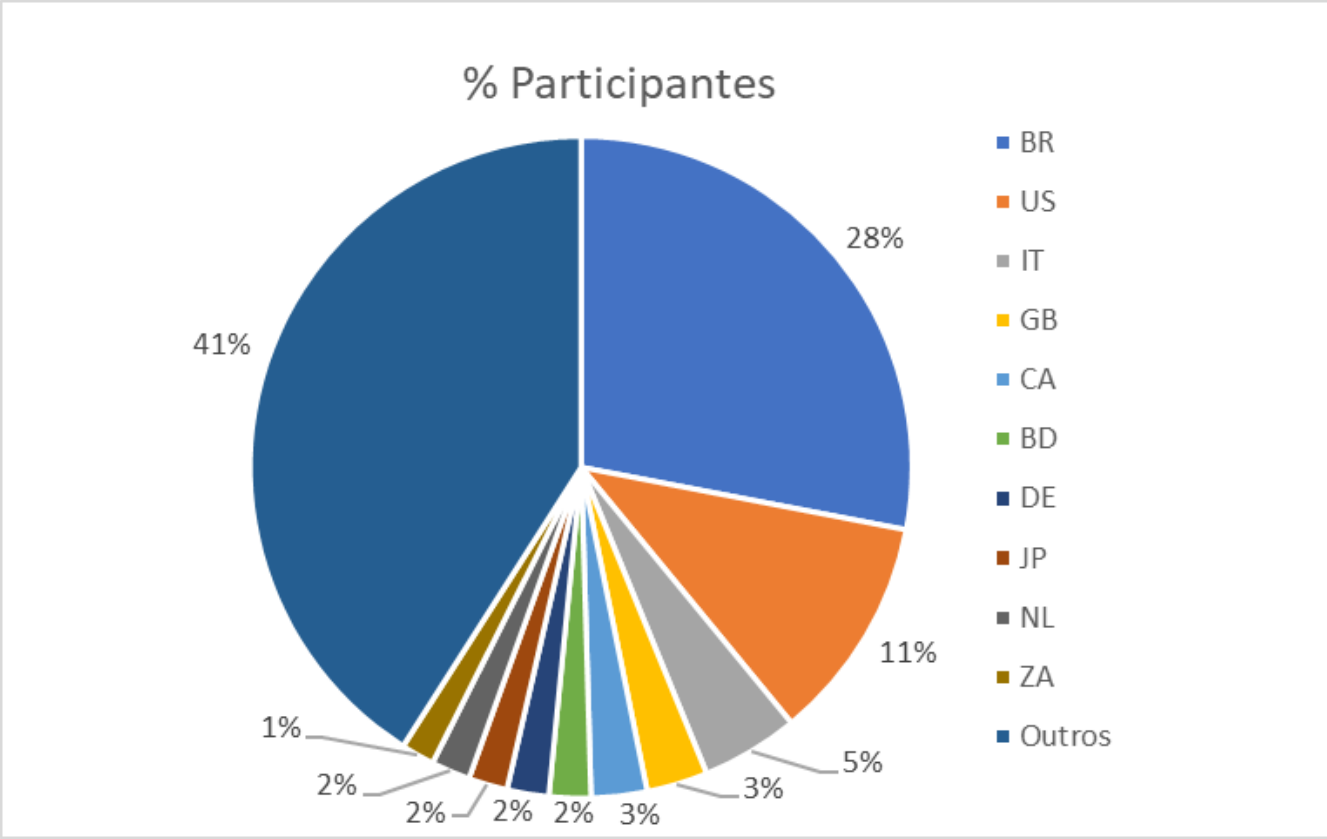
Routing completeness (RPKI) #
- Valid → 22.798 27,1%
- Unkown → 61.174 72,7%
- Invalid → 203 0,2%

* Fonte: MANRS Observatory, acesso logado em 17/10/22

Fonte: https://observatory.manrs.org/#/overview acesso 18/10/22

Programa por uma Internet mais Segura
Desenvolvimento do Programa

- Distribuição por país dos participantes da iniciativa MANRS



Total de participantes: 735

Participantes do Brasil: 206

140 (2020)

174 (2021)

Fonte: https://www.manrs.org/netops/participants/ Acesso 17/10/22

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

https://top.nic.br

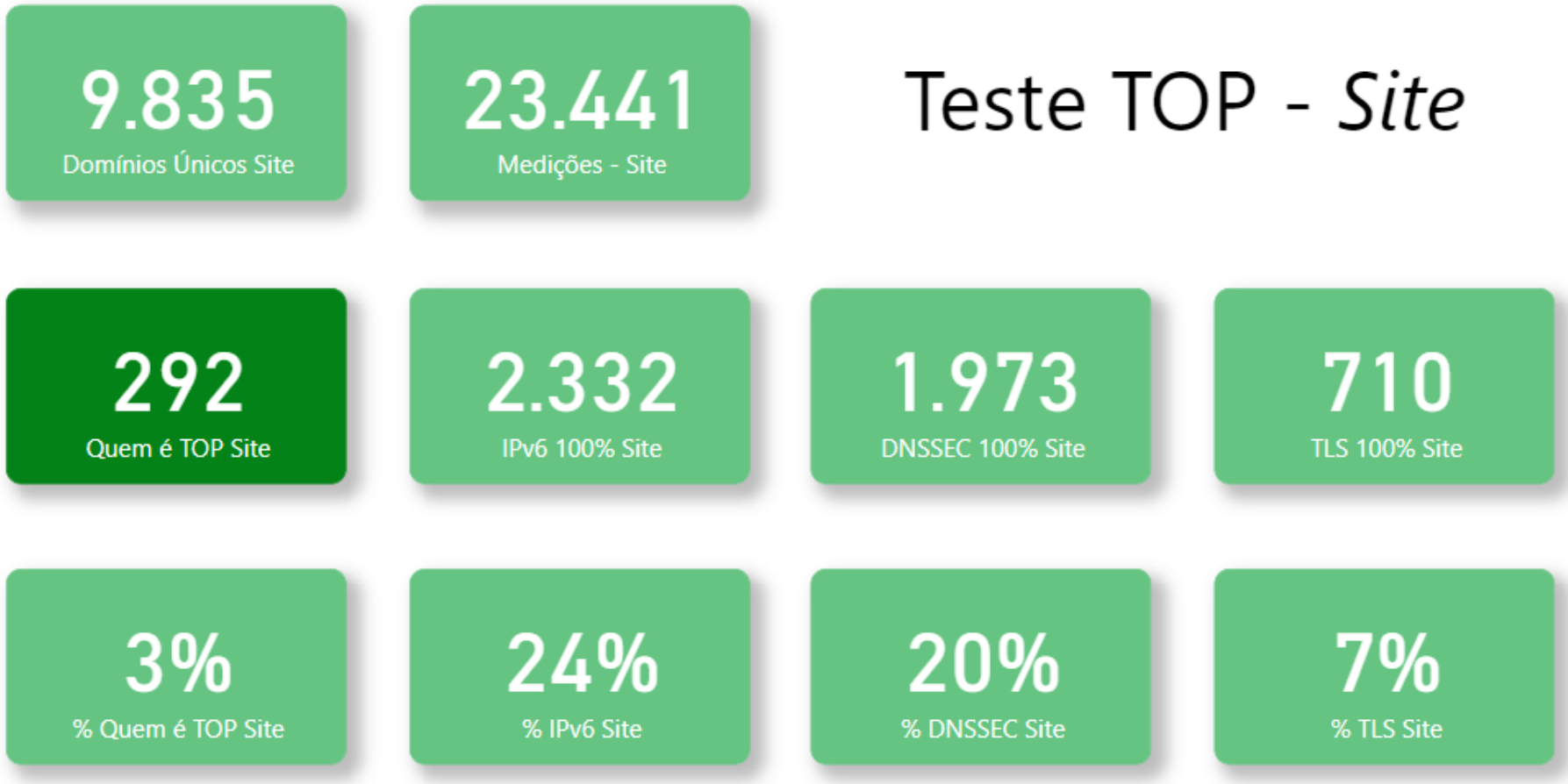
TOP – Teste os Padrões – O que é?

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

- Teste TOP – *Site*
- Teste TOP – *E-mail*
- Teste TOP - IPv6 e DNSSEC da rede do usuário

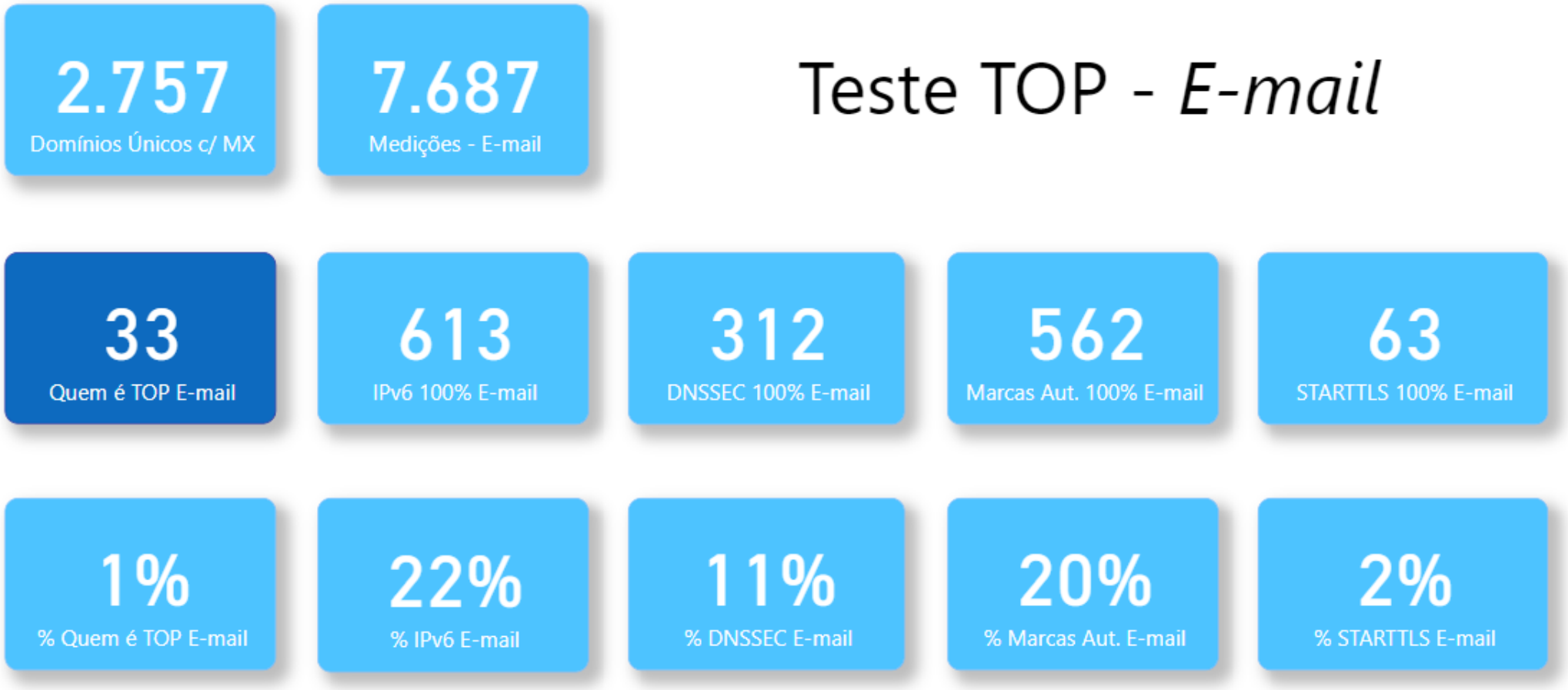
Acesso: https://top.nic.br

TOP – Teste os Padrões – Desenvolvimento



TESTE OS PADRÕES

TOP – Teste os Padrões – Desenvolvimento



26/10/22

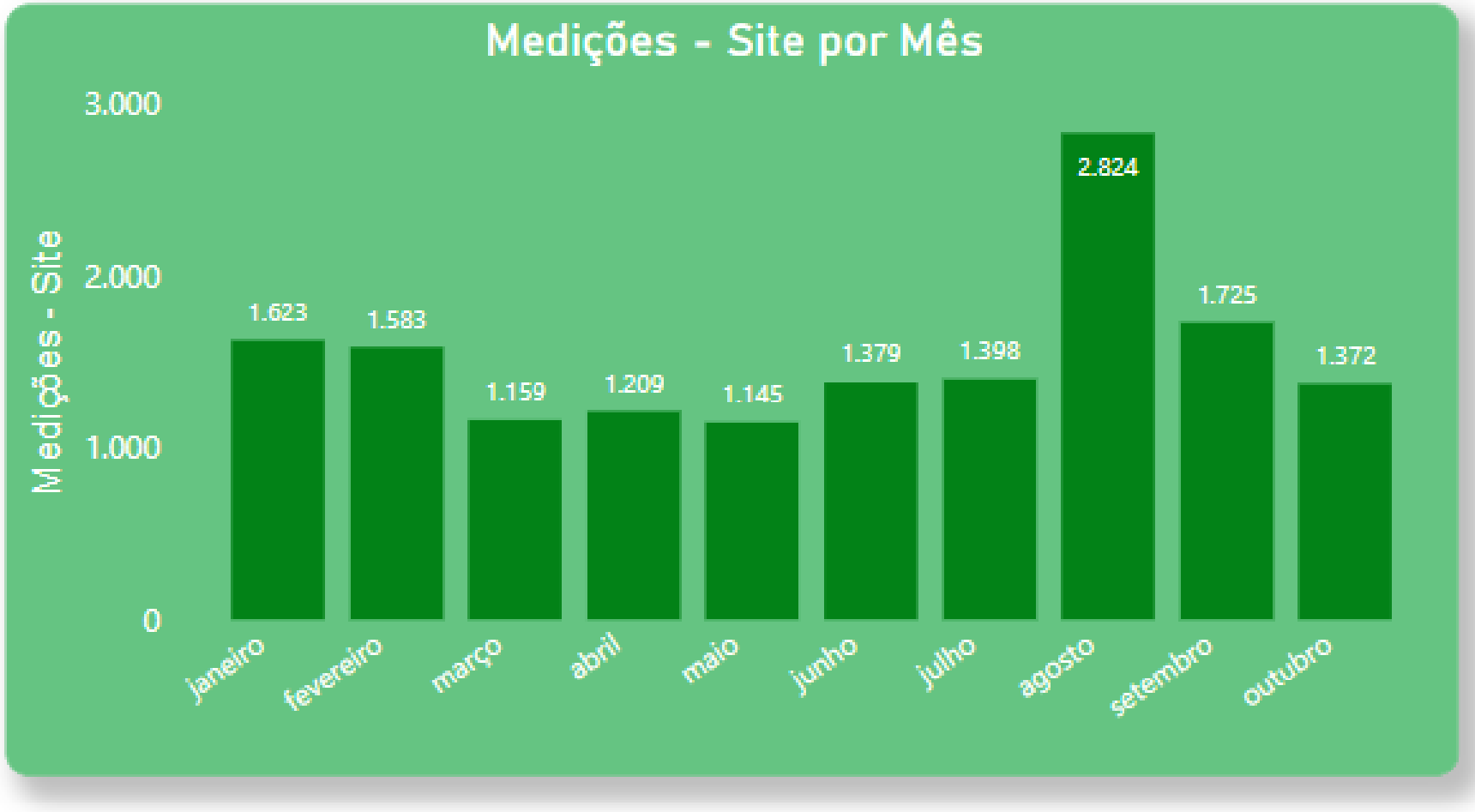
TOP – Teste os Padrões – Desenvolvimento

Teste TOP - IPv6 e DNSSEC da rede do usuário

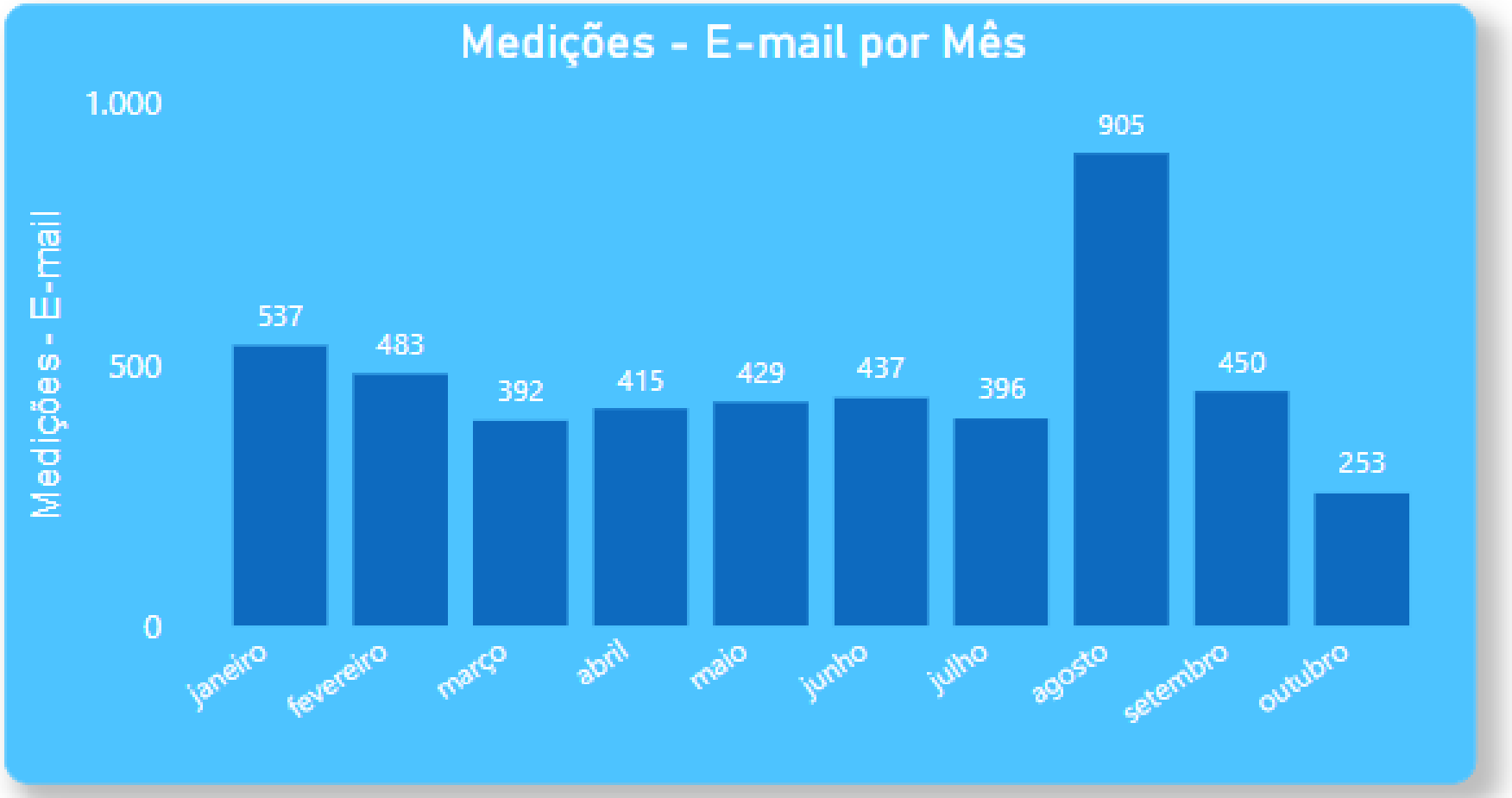
65.247 Medições - IPv6 DNSSEC	38.967 Recursivo c/ DNSSEC Validado	60% % Recursivo c/ DNSSEC Validado
4243 AS Únicos Testados	39.829 IPv6 100% (Cenário VIII)	61% % IPv6 100%

TESTE OS PADRÕES

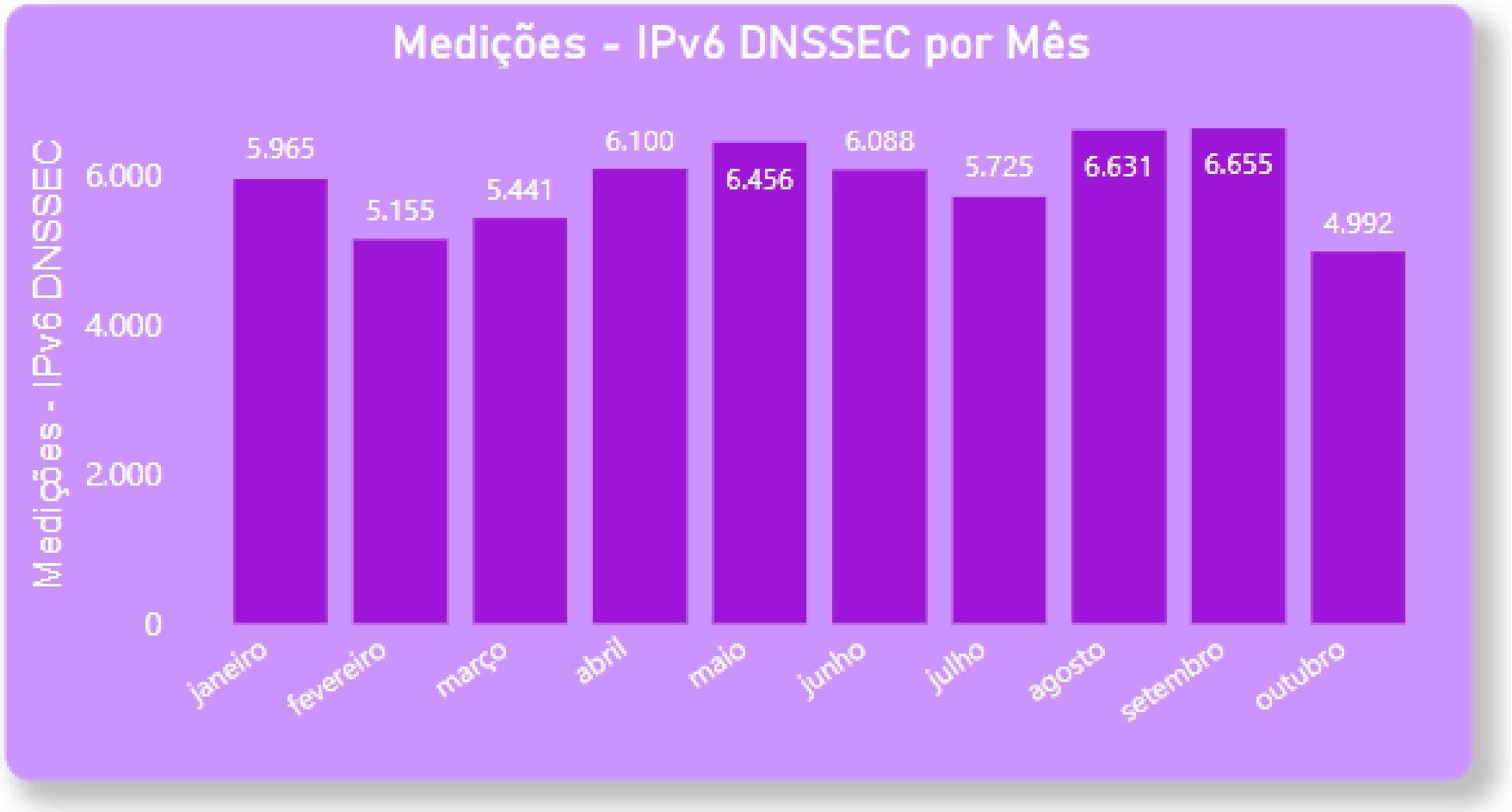
TOP – Teste os Padrões – Desenvolvimento



TOP – Teste os Padrões – Desenvolvimento



TOP – Teste os Padrões – Desenvolvimento



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

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

gzorello@nic.br

27 de outubro de 2022

nic.br cgi.br

www.nic.br | www.cgi.br