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 Regional Edição Sudeste

Belo Horizonte, MG | 22/09/23

registro.br nic.br cgi.br

Nossa Agenda

Programa por uma Internet mais Segura

- **Objetivo / Plano de Ação**
- Interação com Provedores e Operadoras
- **Ações do Programa**
  - MANRS
  - Notificação de Amplificadores
  - TOP – Teste os Padrões

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
- **Divulgar melhores práticas que devem ser utilizadas nas redes**
- **Incentivo ao crescimento de uma cultura de segurança entre os operadores das redes**

PROGRAMA INTERNET +SEGURA

Programa por uma Internet mais Segura
Plano de Ação

Ações executadas pelo NIC.br

- Transversal no NIC.br: CERT.br, CEPTRO.br, IX.br, Registro.br, Sistemas, Comunicação
- **Criação de materiais didáticos e boas práticas**
- Conscientização por meio de palestras, cursos e treinamentos
- **Interação com operadores das redes**
- Implementação de filtros de rotas no IX.br
- **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 Provedores e Operadoras

- Reuniões bilaterais on-line com **os responsáveis pelos ASes com maior quantidade de endereços IP notificados**

- Ações do Programa tratados nas reuniões bilaterais:
  - **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**)
  - **Verificação da adoção de melhores práticas de configuração**
  - Apresentação de medições, por AS, sobre o status da adoção das boas práticas recomendadas

Programa por uma Internet mais Segura

Ações do Programa – Notificação de Amplificadores

- Estatísticas das notificações encaminhadas pelo CERT.br
- **Relatório gerencial encaminhado mensalmente**

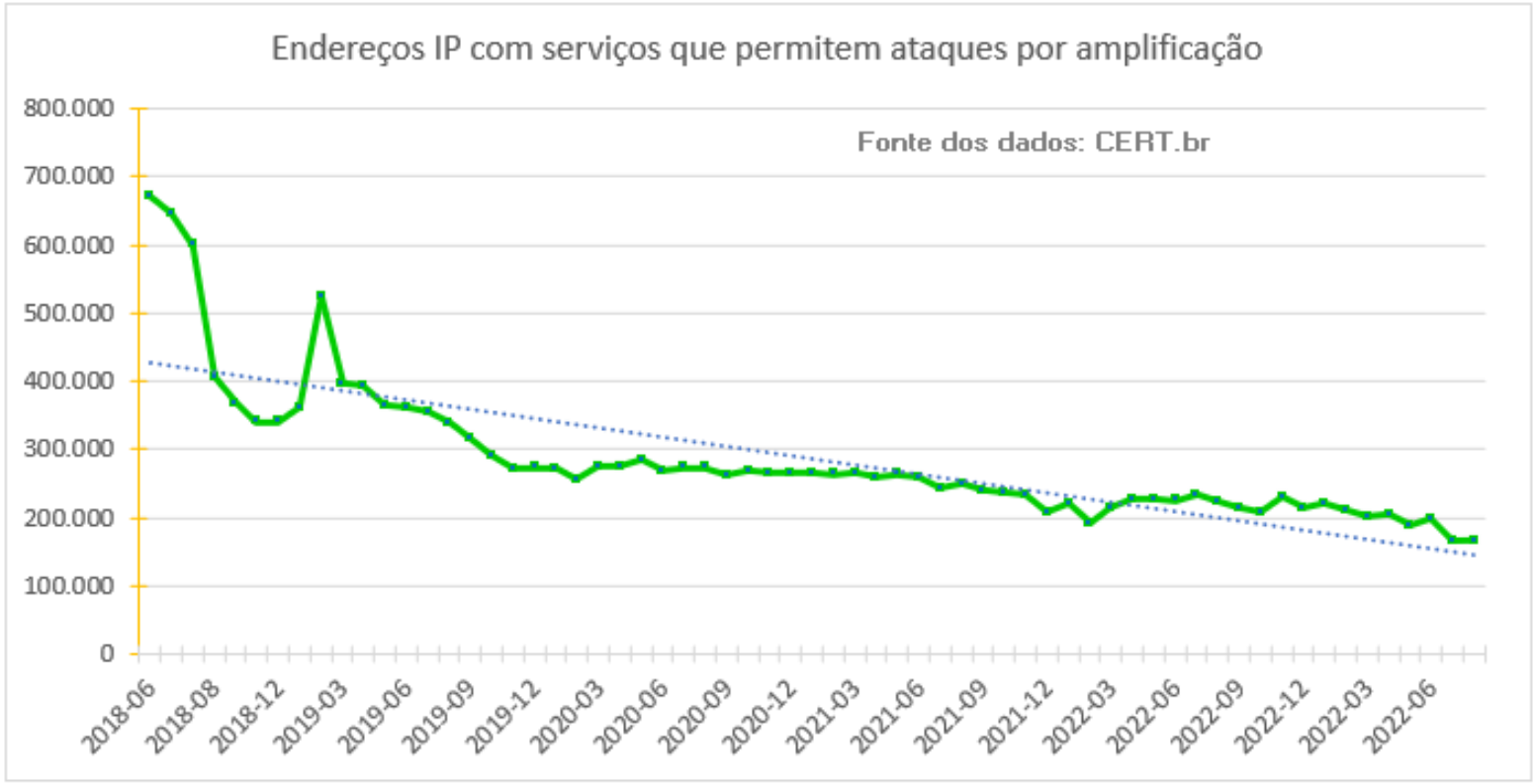
ASN	DNS	SNMP	NTP	SSDP	PORTMAP	MEMCACHED	NETBIOS	QOTD	CHARGEN	LDAP	MDNS	UBNT	WS-DICOVERY	TFTP	CoAP	ARMS	DHCPDiscover	2023-05	2023-06	2023-07	2023-08	MT4145	MT5678
ASN1	17	116	42	1	18	0	4	0	0	1	2	0	0	3	0	1	0	204	215	211	205	0	0
ASN2	72	34	4	1	8	0	10	0	0	3	2	0	0	0	0	0	2	89	93	90	136	0	1
Total	38%	32%	9%	4%	-30%		17%	-100%	-100%	50%	-9%			-63%		9%	-50%	**293**	**308**	**301**	**341**		20%

ASN	SNMP																			
	2022-01	2022-02	2022-03	2022-04	2022-05	2022-06	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
																				#
22381	80	67	73	83	82	84	64	55	57	66	83	84	87	87	81	85	109	110	115	116
28330	26	21	28	26	26	26	23	22	27	27	30	30	30	29	30	30	28	30	28	34
Total								77	84	93	113	114	117	116	111	115	137	140	143	

Programa por uma Internet mais Segura

Ações do Programa – Notificação de Amplificadores

- Quantidade de endereços IP notificados com serviços mal configurados

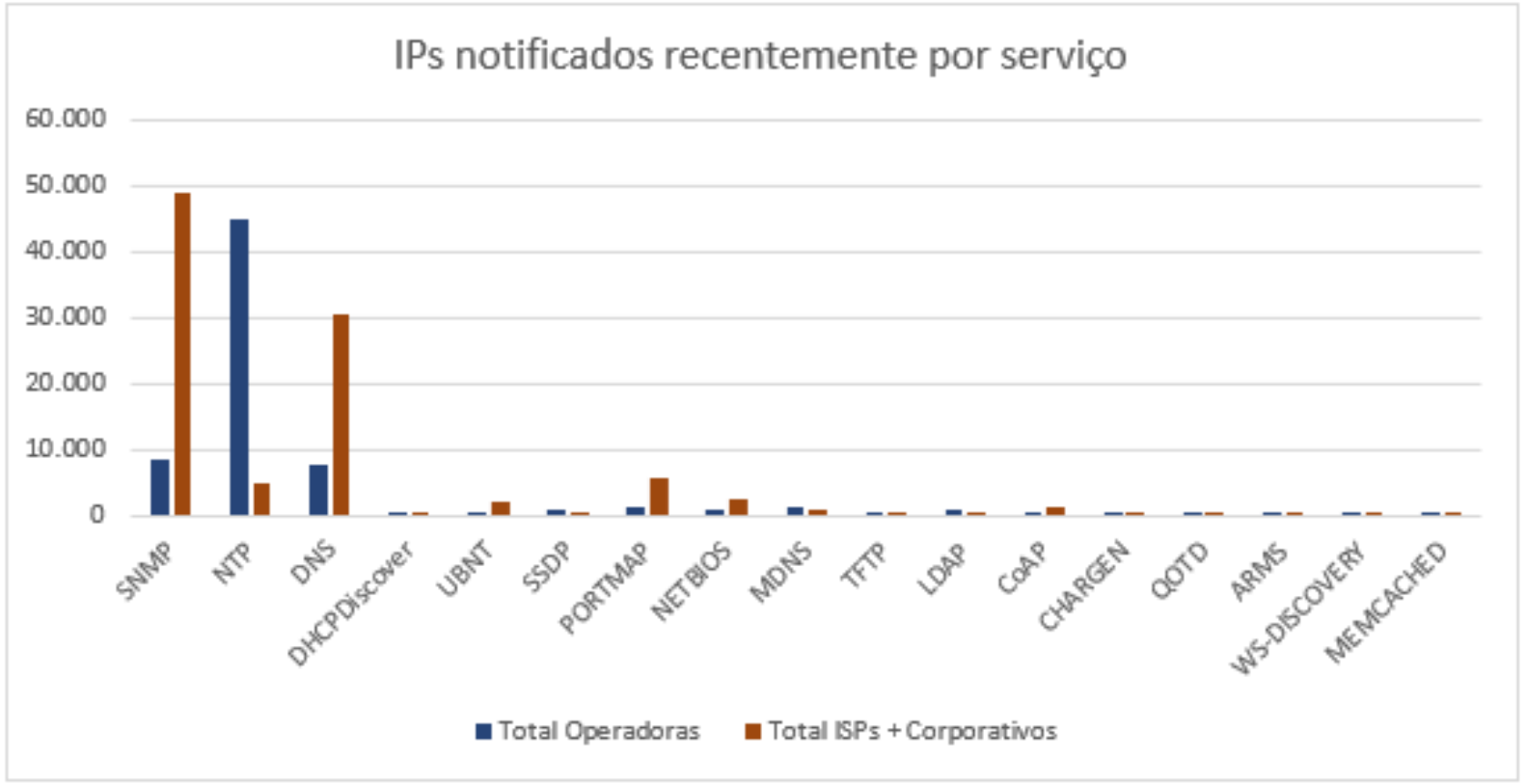


Redução de 77% dos endereços IP mal configurados desde o início do Programa

Programa por uma Internet mais Segura

Ações do Programa – Notificação de Amplificadores

- Quantidade de endereços IP notificados por tipo de serviço



Ago/23

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

Grandes operadoras → NTP mal configurado

Programa por uma Internet mais Segura

Ações do Programa – MANRS

MANRS

Mutually Agreed Norms for Routing Security

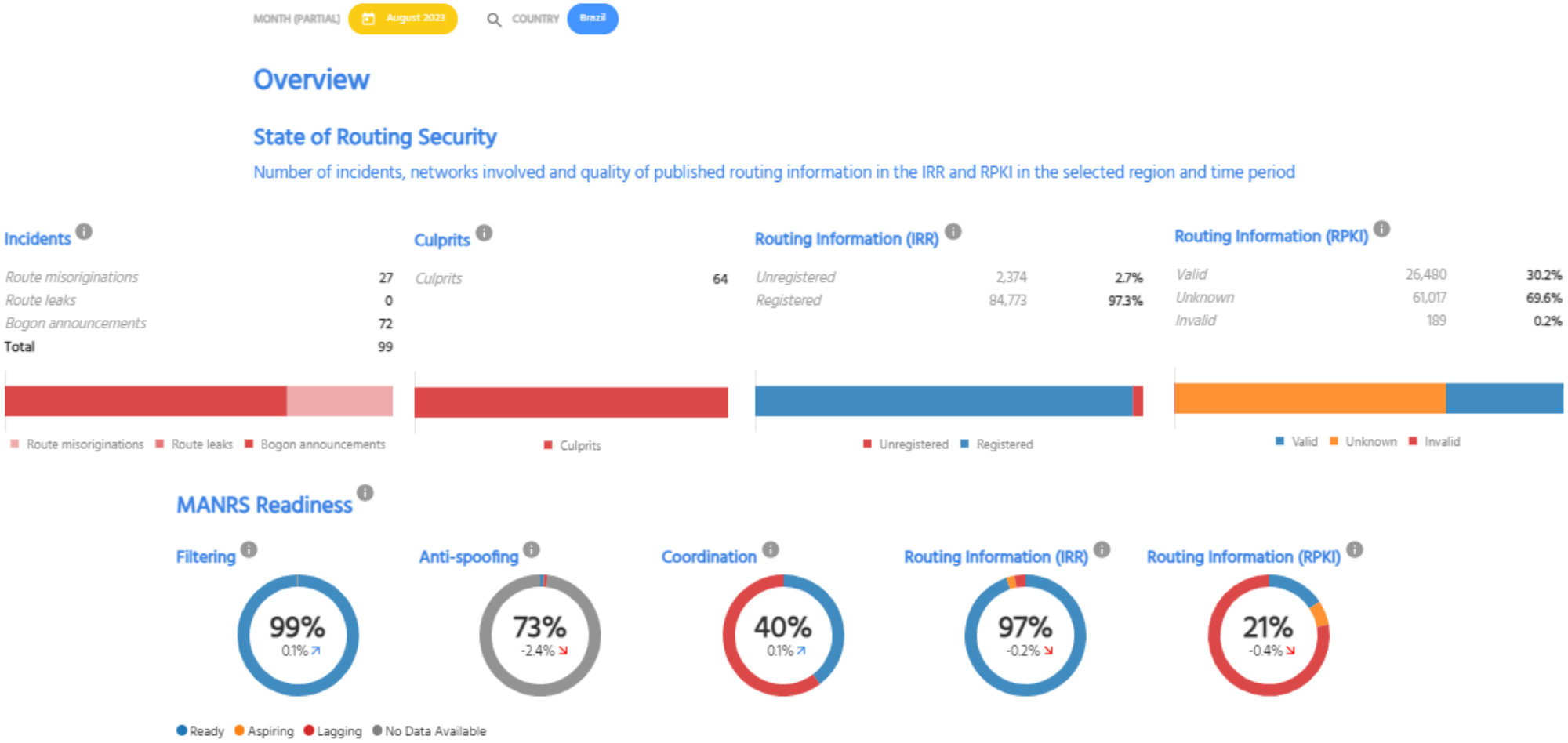
http://manrs.org

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

https://www.manrs.org/netops/participants/

Programa por uma Internet mais Segura

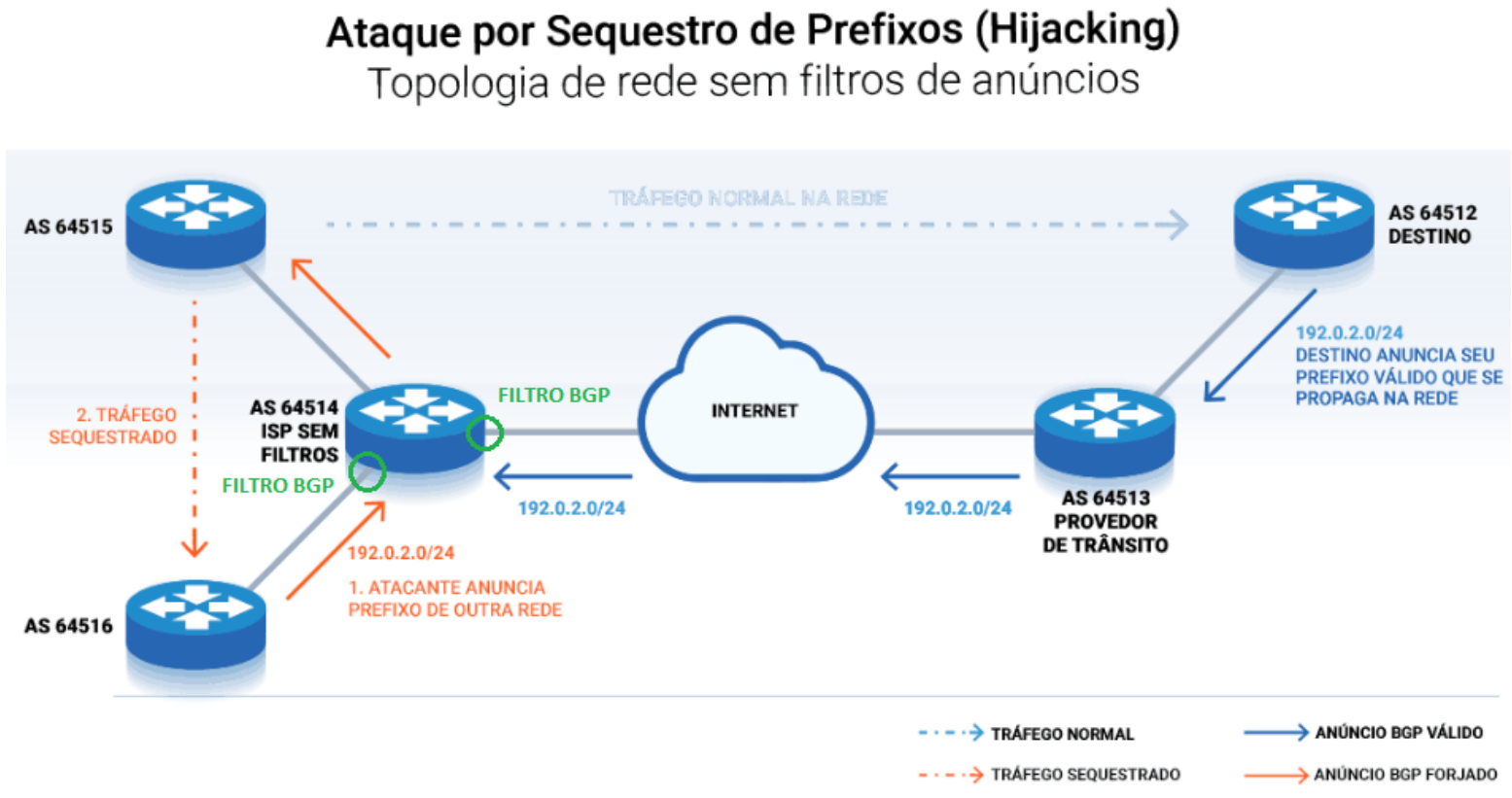
MANRS Observatory Readiness - Brasil



Fonte: https://observatory.manrs.org/#/overview

Programa por uma Internet mais Segura

Ação 1 - Implementação de Filtros de Anúncios BGP



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

O provedor deve garantir a correção dos próprios anúncios e de seus clientes

BGP Stream recebe alertas de:

- Hijacking (sequestro de prefixos)
- Leak (vazamento de rotas)
- Outages
- Últimos 180 dias de eventos
- Monitoramento se seus anúncios BGP

https://bgpstream.crosswork.cisco.com/

MANRS Observatory analisa 8 métricas:

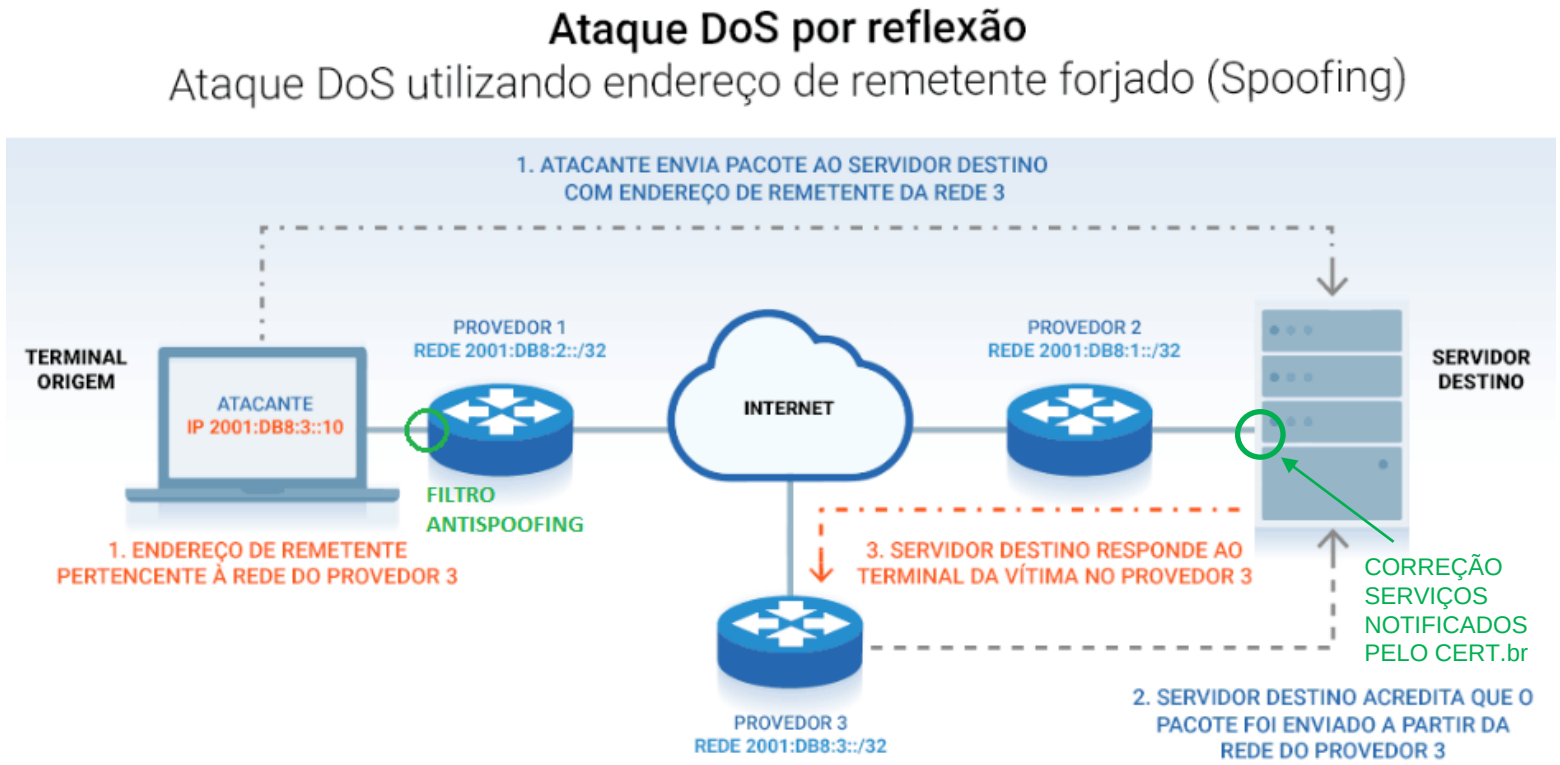
- Hijacking
- Leak
- Bogon - prefixos
- Bogon - ASNs

Gerado pelo AS ou por seu cliente Direto

https://observatory.manrs.org/#/about

Programa por uma Internet mais Segura

Ação 2 - Implementação de Filtros Antispoofing



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

Implementação de filtro antispoofing o mais próximo do cliente

uRPF (Unicast Reverse Path Forwarding)

- Strict Mode
- Loose Mode
- VRF Mode

Testes contra o CAIDA Spoofer

https://www.caida.org/projects/spoofer/

MANRS Observatory analisa a base de dados do CAIDA Spoofer

Programa por uma Internet mais Segura

Ação 3 - Coordenação entre Operadores

Facilitar a comunicação operacional global e a coordenação entre os operadores de rede

Endereços de *e-mail* indicados no Whois:

nic.br | registro.br

https://registro.br/tecnologia/ferramentas/whois/

Titular

Roteamento

Abuse

Endereços de *e-mail* indicados no PeeringDB:

PeeringDB

https://www.peeringdb.com/

NOC

Abuse

Outros

- **As notificações de segurança do CERT.br são encaminhadas para o *e-mail* do campo Abuse**
- Utilize grupos de *e-mails* ao invés de *e-mails* pessoais
- **Manter compatibilidade dos pontos de contatos em relação a cadastros em outras bases (Whois, PeeringDB, IRR)**
- Manter pontos de contatos atualizados após mudanças internas e incorporação de outros ASes
- O MANRS Observatory analisa os pontos de contato técnicos do PeeringDB

Verificar se estão recebendo notificações do CERT.br: há endereços de *e-mail* que não recebem mensagens de cert@cert.br: SPAM, caixa cheia, host/domínio not found, inválido (~40 tipos de erros)

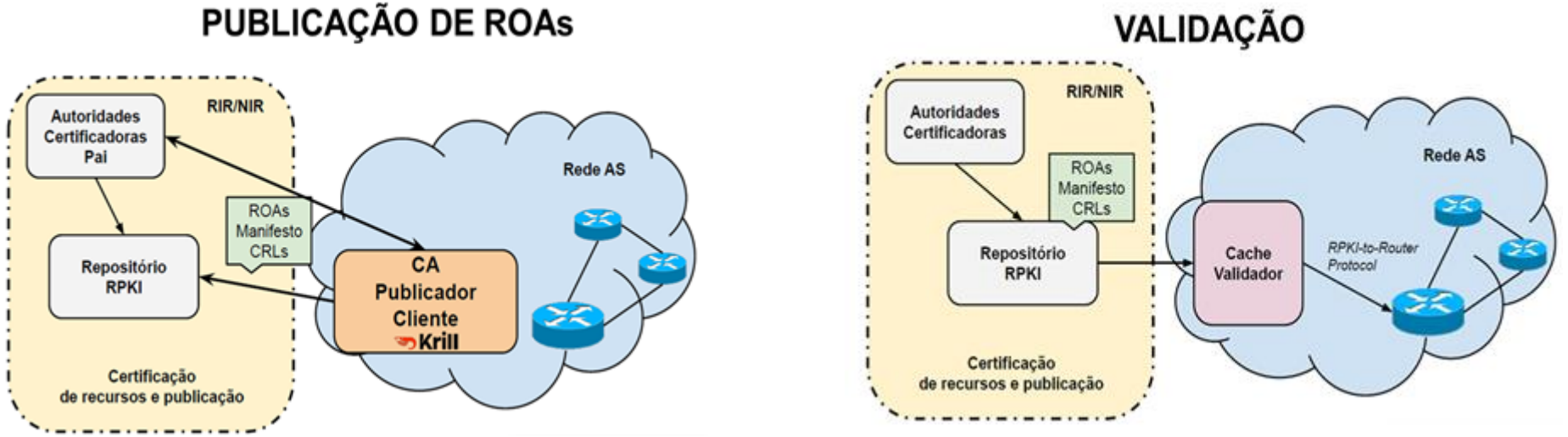
O Registro.br faz validação dos pontos de contato de Abuse: se não foi validado, é enviado um aviso e se não responde em seis meses a administração dos recursos é bloqueada no sistema

Programa por uma Internet mais Segura
Ação 4 - Cadastro da Política de Roteamento

IRR - Internet Routing Registry

- Cadastro da política da política de Roteamento no IRR (RADB) ou no TC
- MANRS Observatory analisa a base de dados do RIPEStat (https://stat.ripe.net/ui2013/)

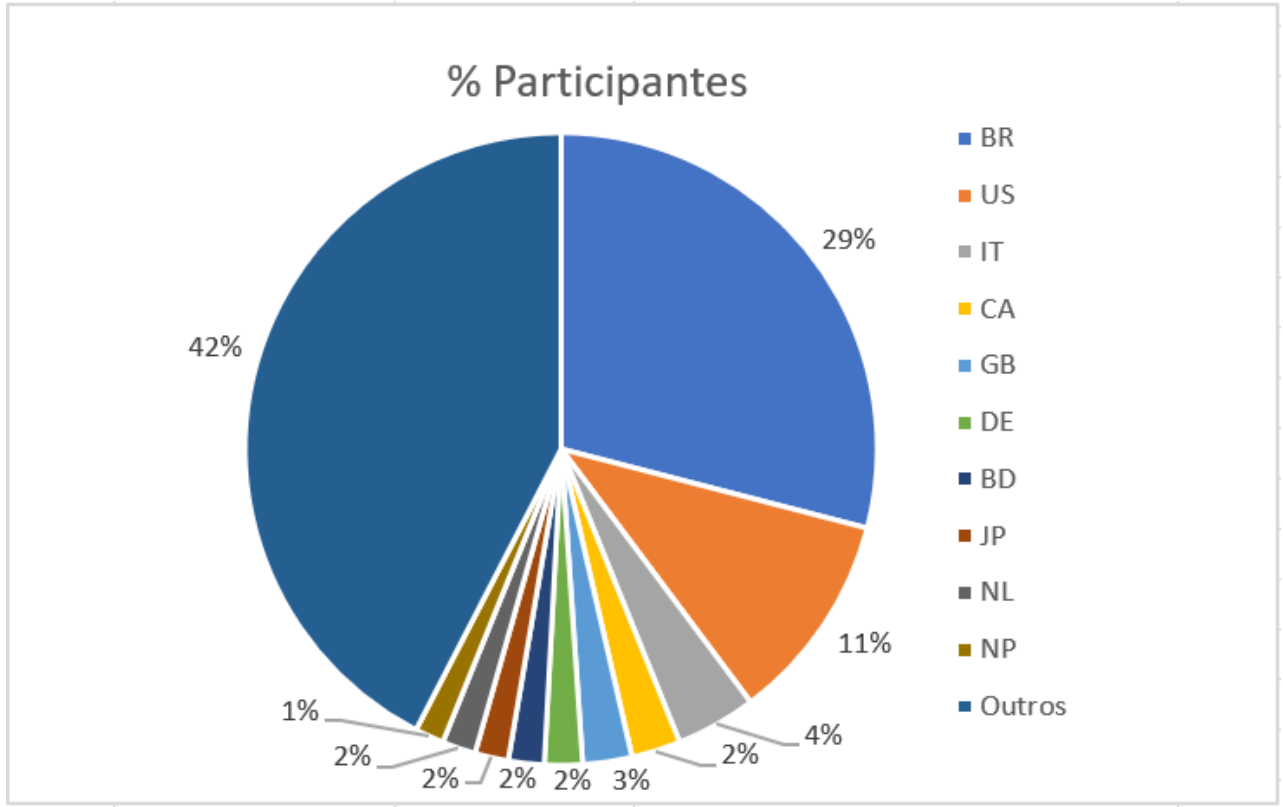
RPKI - Resource Public Key Infrastructure



- MANRS Observatory analisa os ROAS publicados com um Validador RPKI próprio

Programa por uma Internet mais Segura
Participantes do MANRS

- Distribuição por país dos Provedores participantes da iniciativa MANRS



Total de participantes: 875

Participantes do Brasil: 254 (Ago/23)

206 (2022)

174 (2021)

140 (2020)

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

Programa por uma Internet mais Segura

Ações do Programa – TOP – Teste os Padrões

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 - 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

TOP – Teste os Padrões – Desenvolvimento

Teste TOP - IPv6 e DNSSEC da rede do usuário

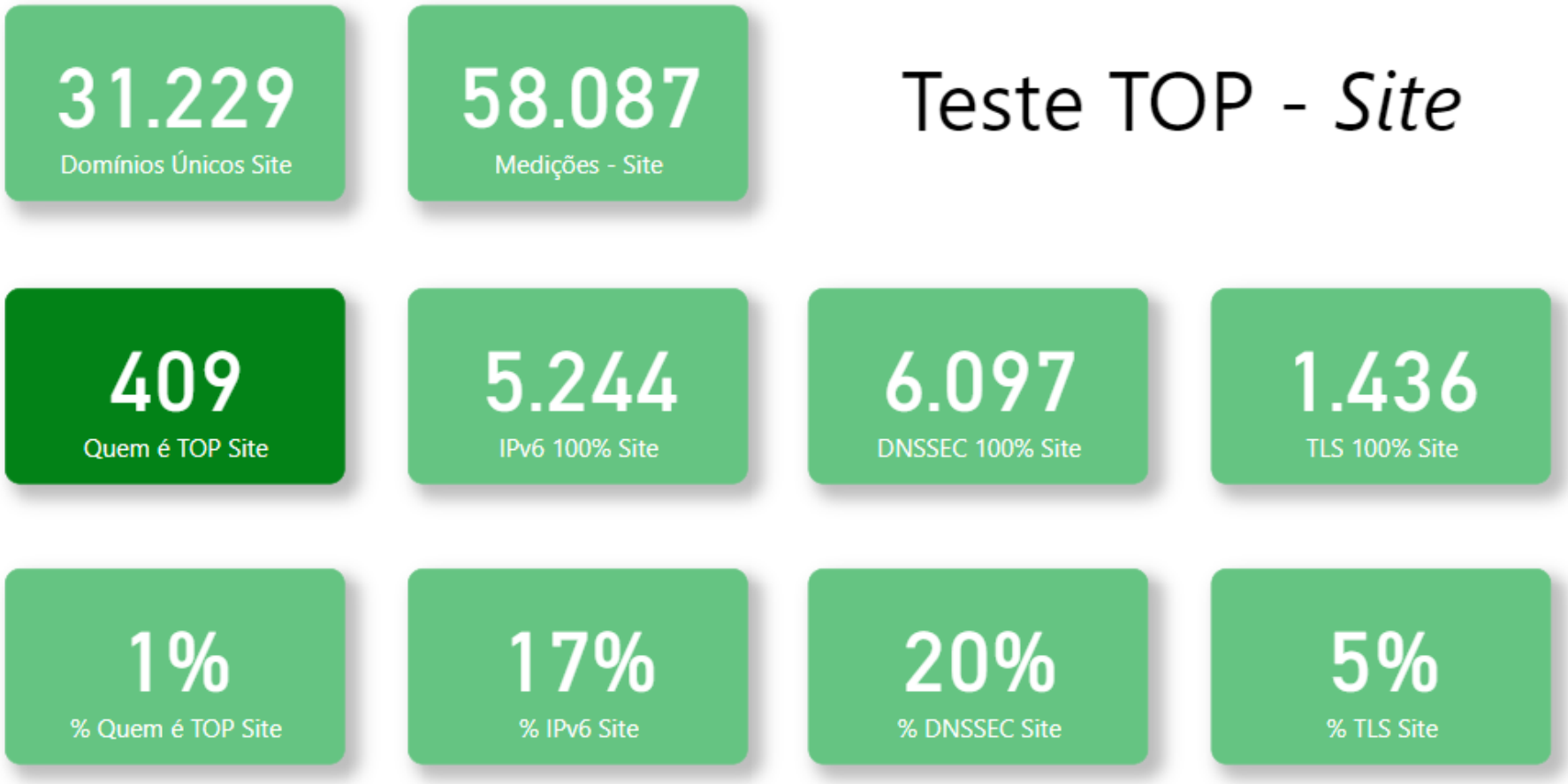
146.597 Med. - IPv6 DNSSEC Final.	**94.333** Recursivo c/ DNSSEC Validado	**64%** % Recursivo c/ DNSSEC Validado
5.795 AS Únicos Testados	**92.092** Usuários com IPv6	**63%** % Usuários IPv6 100%

Medições totais IPv6 100%

TESTE OS PADRÕES

18/9/23

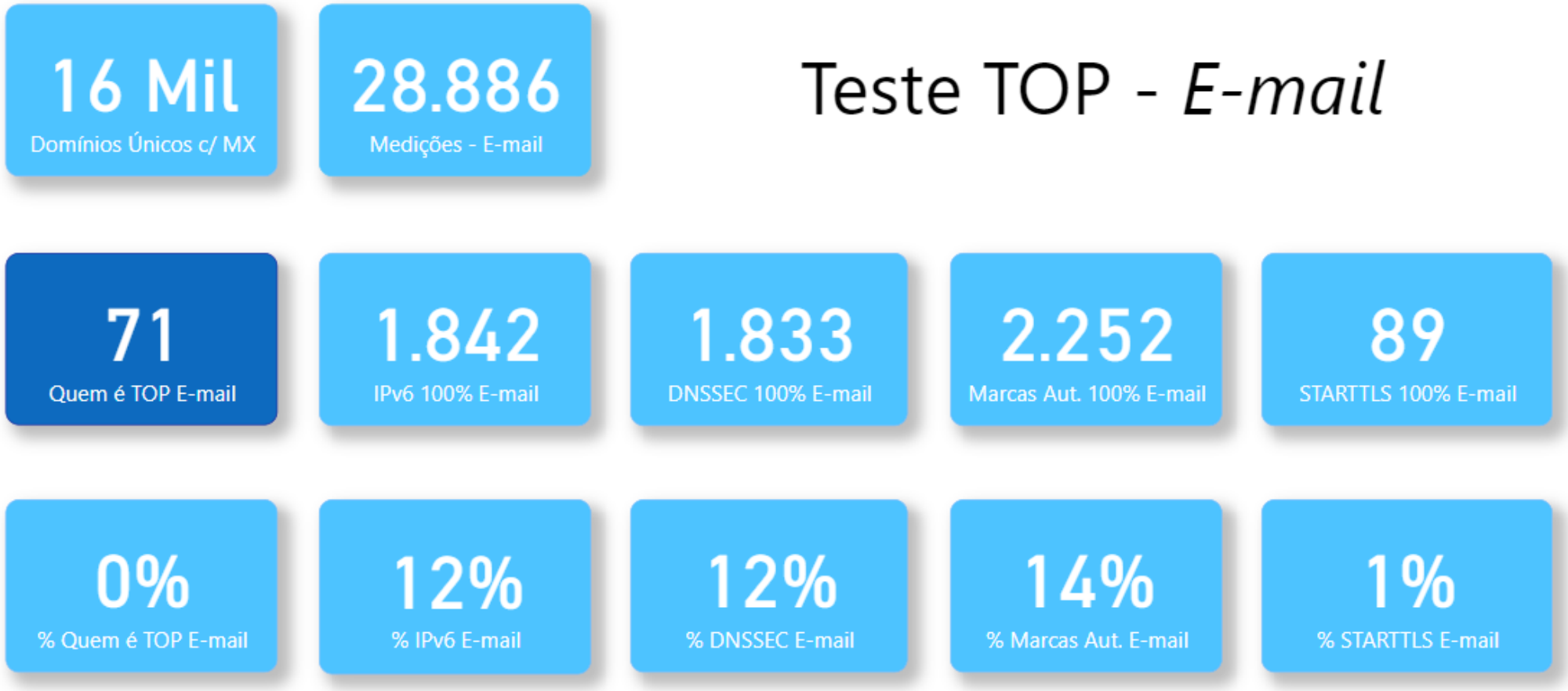
TOP – Teste os Padrões – Desenvolvimento



TESTE OS PADRÕES

18/9/23

TOP – Teste os Padrões – Desenvolvimento



TOP
TESTE OS PADRÕES

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

Obrigado

Gilberto Zorello

gzorello@nic.br

22 de setembro de 2023

nic.br cgi.br

www.nic.br | www.cgi.br