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
UPDATE

Gilberto Zorello | gzorello@nic.br

Semana de Infraestrutura da Internet do Brasil – IX Fórum 14

São Paulo, SP | 02/12/20

registro.br nic.br cgi.br

Nossa
Agenda

Programa por uma Internet mais Segura

- Iniciativa
- Plano de Ação
- Interação com Operadores
- MANRS Observatory
- Desenvolvimento do Programa
- Página web do Programa
- Próximos passos

Programa por uma Internet mais Segura

Iniciativa

Lançado pelo CGI.br e NIC.br

- Apoio inicial: Internet Society, Conexis, Abranet e Abrint
- Apoio: RedeTelesul, InternetSul, Telcomp, Abrahosting, Apronet, Abramulti

PROGRAMA INTERNET +SEGURA

Objetivo - atuar em apoio à comunidade técnica da Internet para:

- Redução dos ataques de Negação de Serviço
- **Melhora da Segurança de Roteamento na rede**
- Redução das vulnerabilidades e falhas de configuração

- **Incentivo ao crescimento de uma cultura de segurança entre os operadores da rede**

Programa por uma Internet mais Segura
Plano de Ação

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

- Conscientização por meio de palestras, cursos e treinamentos
- **Criação de materiais didáticos e boas práticas**
- Interação com Operadores, com apoio das Associações, 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 por uma Internet mais Segura
Interação com Operadores

- Reuniões bilaterais bimestrais com as grandes operadoras

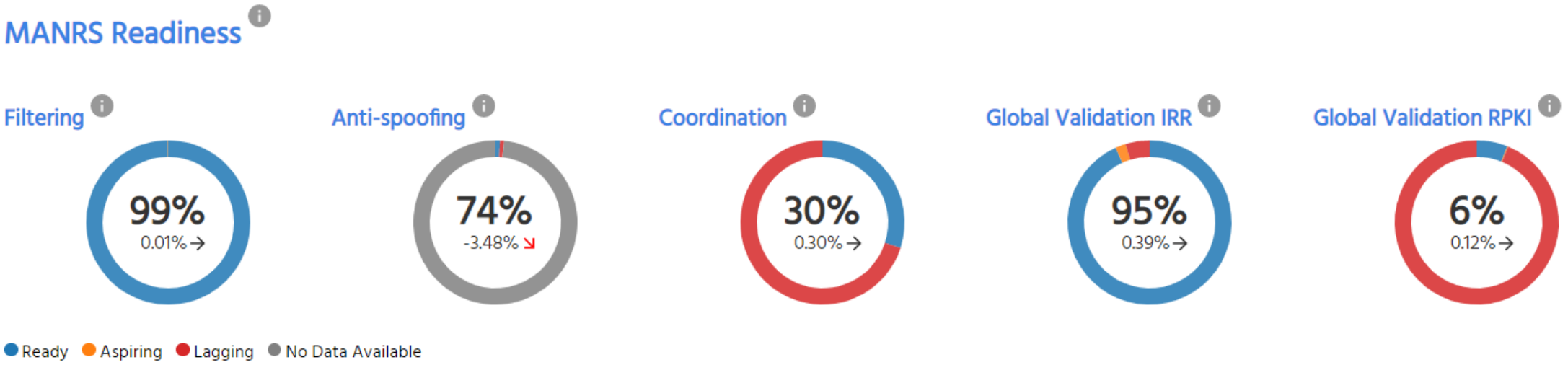
- **Em 2020, devido a impossibilidade de participação em eventos presenciais, passamos a realizar reuniões on-line com os responsáveis pelos ASes com maior quantidade de endereços IP notificados**

- Manutenção do contato com os operadores pelo encaminhamento de relatório gerencial mensal para o acompanhamento da resolução dos problemas notificados

- **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)

Programa por uma Internet mais Segura
MANRS Observatory - Readiness

Conjunto de ASes do Brasil



Ação 1

Ação 2

Ação 3

Ação 4

Programa por uma Internet mais Segura
MANRS Observatory - Métricas

Ação	Métrica	Descrição	Fonte de dados
Filtros BGP	M1	Route leak causado pelo AS	bgpstream
	M2	Hijacking causado pelo AS	
	M1C	Route leak causado por cliente conectado diretamente ao AS	
	M2C	Hijacking causado por clienteconectado diretamente ao AS	
	M3	Prefixos Bogon anunciados pelo AS	CIDR report
	M3C	Prefixos Bogon propagados pelo AS	
	M4	ASNs Bogon anunciados pelo AS	
	M4C	ASNs Bogon propagados pelo AS	
Filtro Anti-spoofing	M5	Possibilidade de IP Spoofing pelo AS	CAIDA Spoofer
Coordenação	M8	Registro de ponto de contato no PeeringDB	PeeringDB
Facilitar Validação Global	M7IRR	Rotas não registradas	RIPEstat
	M7RPKI	ROAs não registrados	RPKI Validator
	M7RPKIN	Rotas inválidas	

Programa por uma Internet mais Segura
Desenvolvimento do Programa

- **Cursos de Boas Práticas Operacionais p/ Sistemas Autônomos – BCOP – ministrado pelo CEPTRO.br no formato on-line**

- **Palestras sobre o Programa com ênfase nas recomendações do CERT.br e do MANRS:**
  - ABRINT na Estrada – Porto Velho, RO (jan/20) – Campo Grande, MS (mar/20)
  - **Congresso APRONET de Provedores – Florianópolis, SC (fev/20)**
  - Apresentação do Programa no Curso BCOP – São José do Rio Preto, SP (fev/20)
  - **IX Fórum Regional Edição Especial On-line (mar/20)**
  - Abrahosting – Evento Fechado – On-line (set/20)

Programa por uma Internet mais Segura
Desenvolvimento do Programa

- ***Lives* com Associações de Provedores**
  - **InternetSul** – Segurança na Internet – c/ participação do CEPTRO e do CERT.br (jun/20)
  - **RedeTelesul** - Segurança, Troca de Tráfego, Recursos de Numeração e OpenCDN – c/ participação do IX e do Registro (jul/20)
  - **Abranet** - Como você pode ter sua Internet mais segura conhecendo as melhores práticas em infraestrutura para ISP e TIC? - c/ participação do CERT.br (set/20)

- Curso **Implantação de RPKI para operadoras** – ministrado pelo CEPTRO.br no formato on-line: Vivo, Oi e Claro

- **Reuniões Bilaterais on-line com operadores**
  - Grandes operadoras: reuniões bimestrais
  - ISPs + ASes Corporativos: reuniões on-line com os responsáveis dos ASes com maior quantidade de notificações (75)
  - Relatórios gerenciais encaminhados mensalmente: 94, cobrindo mais de 200 ASes

Programa por uma Internet mais Segura
Endereços IP e ASNs notificados pelo CERT.br

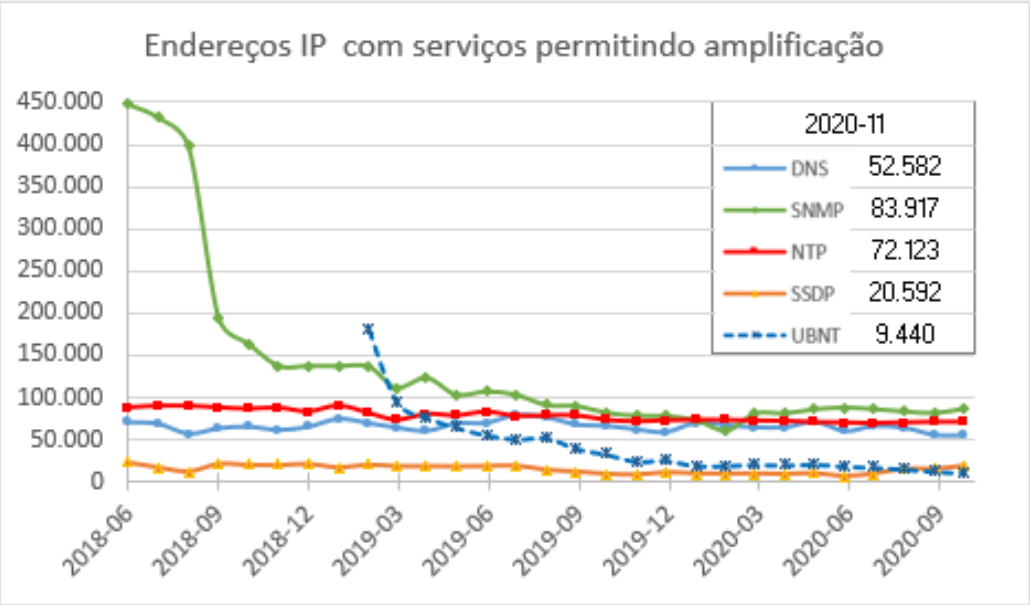
Brasil	DNS		SNMP		NTP		SSDP		Ubiquit	
mês	ASNs	IPs	ASNs	IPs	ASNs	IPs	ASNs	IPs	ASNs	IPs
2019-12	2.962	58.453	2.900	77.952	1.003	72.235	736	10.791	1.374	25.964
2020-01	3.144	69.680	2.881	72.806	1.013	72.862	705	9.386	1.251	19.407
2020-02	3.086	66.958	2.545	60.678	1.013	72.591	680	9.134	1.315	19.726
2020-03	3.143	64.219	3.021	81.009	1.015	71.864	721	9.326	1.305	20.780
2020-04	3.051	64.224	3.044	81.169	1.050	71.528	720	8.703	1.290	20.134
2020-05	3.217	69.588	3.121	86.097	1.080	70.097	749	9.624	1.475	21.312
2020-06	3.248	59.613	3.119	87.996	1.063	69.523	705	5.859	1.388	18.746
2020-07	3.270	65.856	3.201	86.097	1.120	69.026	699	9.380	1.339	17.531
2020-08	3.261	63.398	3.191	83.327	1.131	69.764	770	15.579	1.274	15.503
2020-09	3.193	54.958	3.172	81.526	1.143	70.447	720	15.395	1.208	12.596
2020-10	3.247	54.648	3.253	86.907	1.128	70.329	818	19.746	1.147	10.771
2020-11	3.268	52.582	3.231	83.917	1.161	72.123	803	20.592	1.104	9.440

O Brasil está em **quarto** lugar entre os endereços IPs com serviços SNMP mal configurados

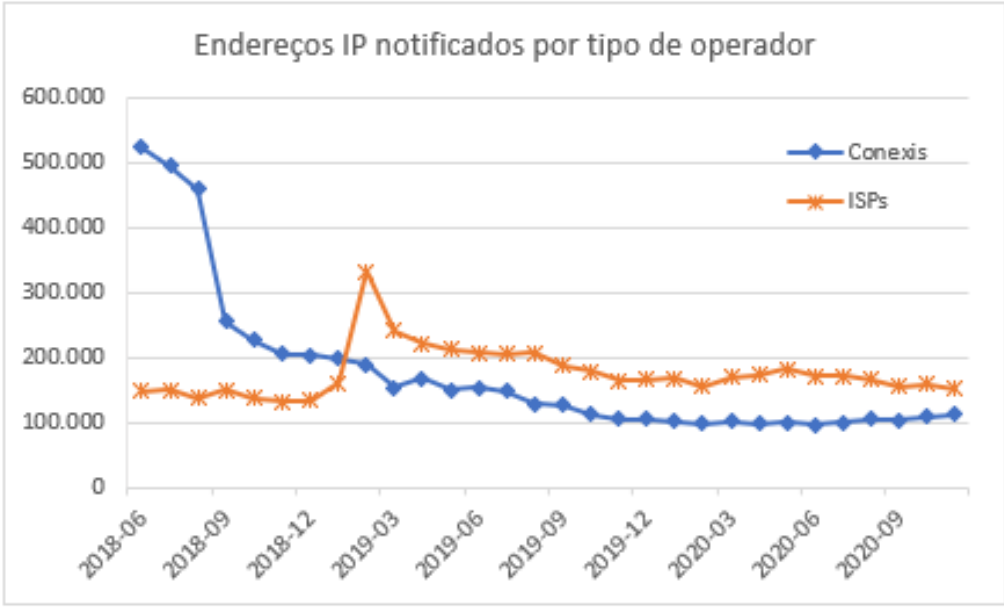
Fonte: https://snmpscan.shadowserver.org/

Programa por uma Internet mais Segura
Desenvolvimento do Programa

- Quantidade de endereços IP notificados com serviços mal configurados



Fonte dos dados: CERT.br

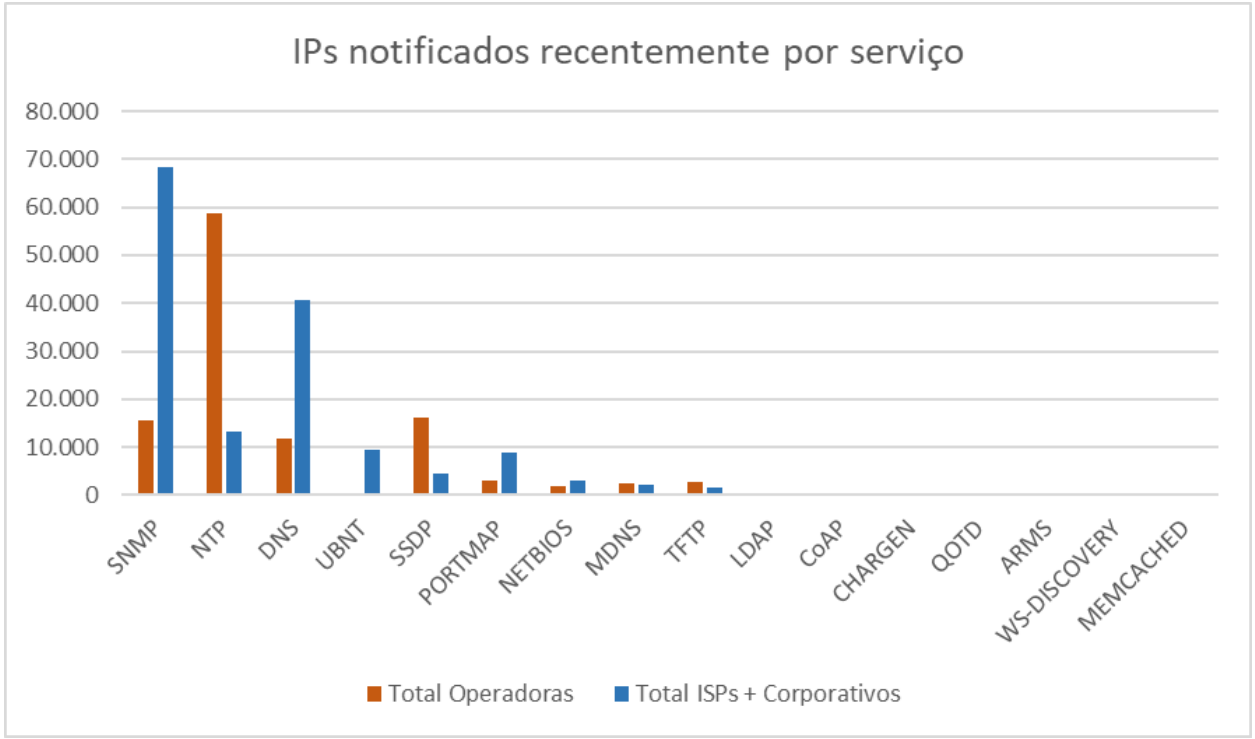


Fonte dos dados: CERT.br

Redução de 62% dos endereços IP mal configurados desde o início do Programa

Programa por uma Internet mais Segura
Desenvolvimento do Programa

- Endereços IP notificados recentemente por serviço mal configurado

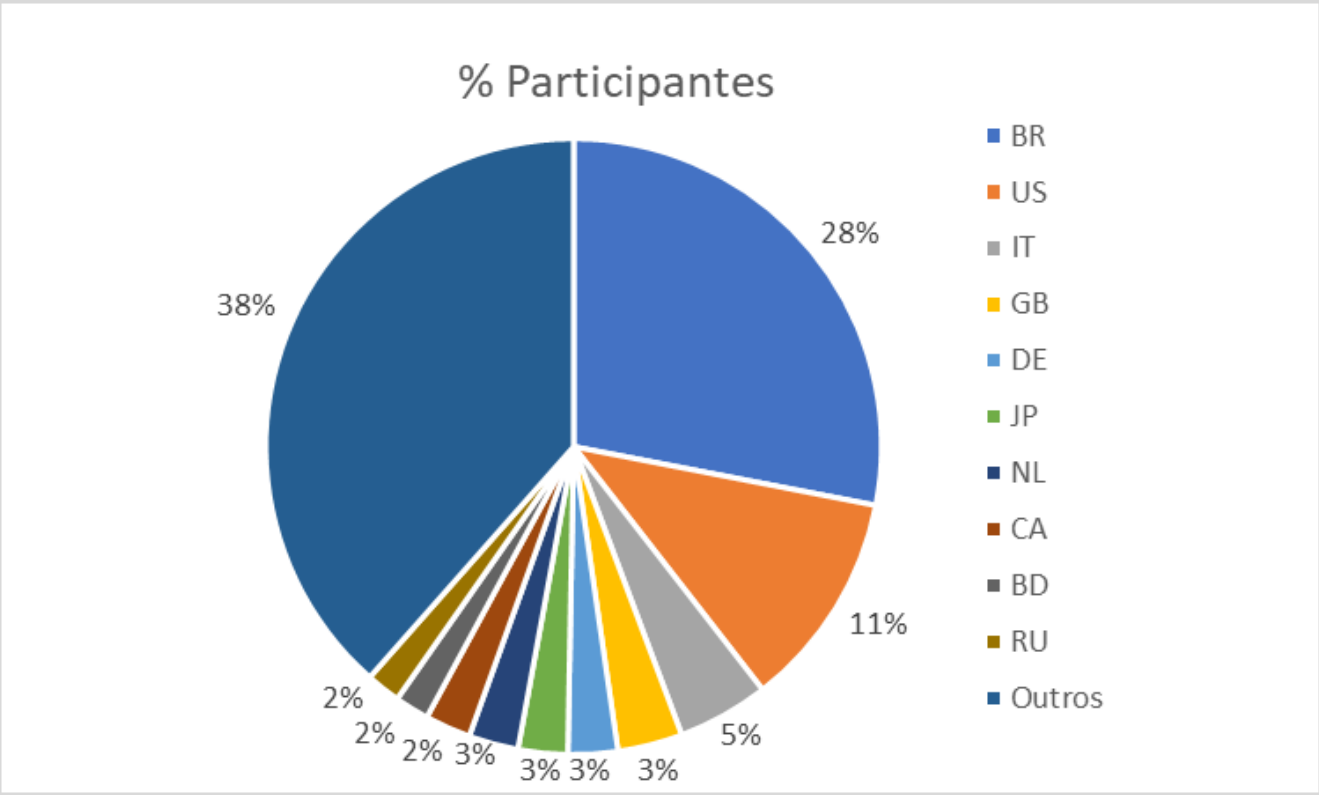


Principais ofensores: **ISPs e ASes corporativos → SNMP, DNS, NTP, UBNT e PORTMAP**

Grandes operadoras → NTP, SSDP, SNMP e DNS

Programa por uma Internet mais Segura
Desenvolvimento do Programa

- Distribuição por país dos participantes da iniciativa MANRS



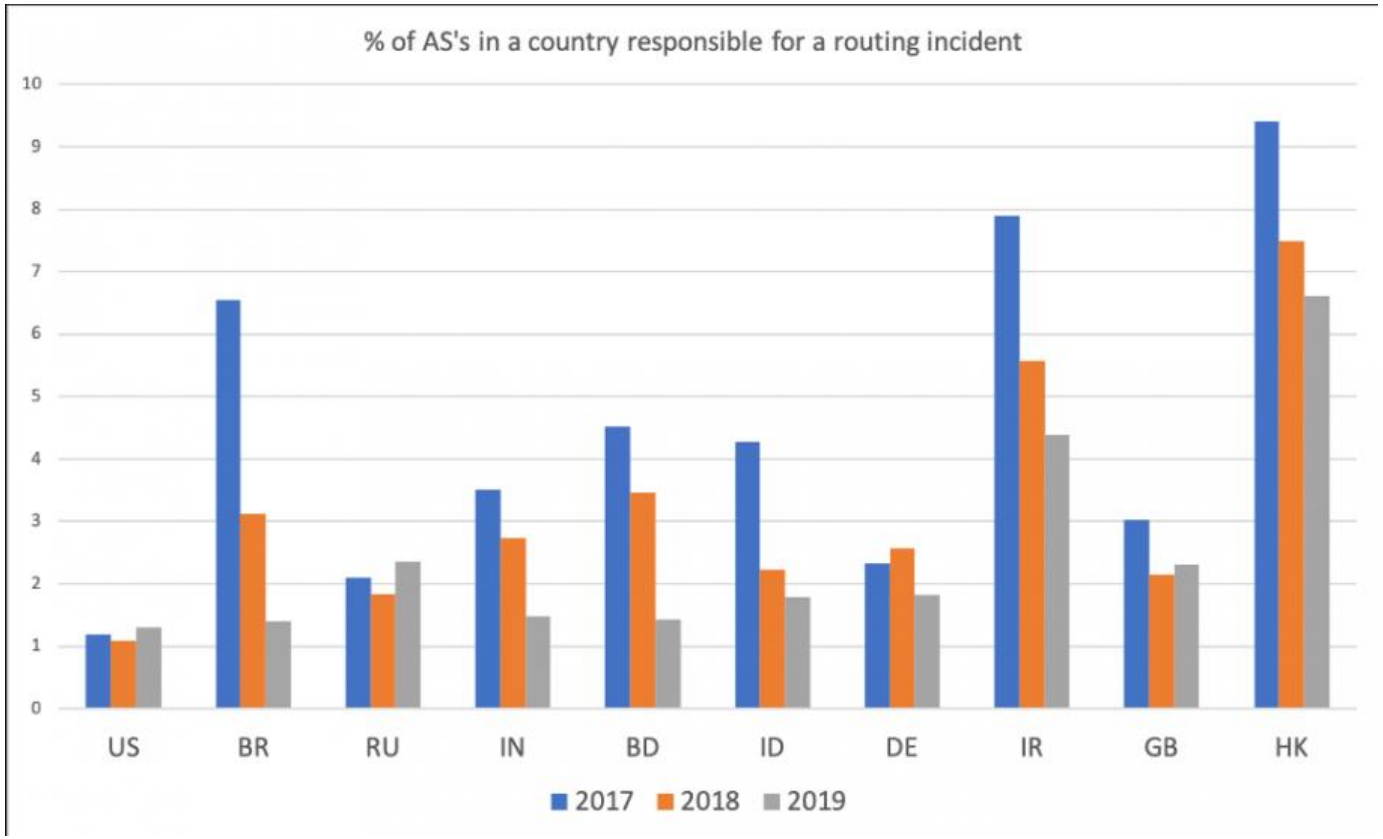
Fonte: https://www.manrs.org/isps/participants//

Total de participantes: 499

Participantes do Brasil: 140

Programa por uma Internet mais Segura
Desenvolvimento do Programa

- Porcentual de incidentes de roteamento ao longo do tempo



Fonte: https://www.manrs.org/2020/06/making-the-most-of-our-manrs-partnerships-nic-br-and-brazil-lead-the-manrs-pack/

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

Programa por uma Internet mais Segura
Próximos Passos

- Continuidade das ações com as grandes operadoras com reuniões bilaterais e acompanhamento das ações

- **Reuniões bilaterais com provedores e ASes corporativos, selecionados em função dos indicadores**

- Continuidade da realização de cursos, treinamento e tutoriais pelo CEPTRO

- **Retorno da realização de palestras nos IX Fóruns Regionais e Eventos de Associações de Provedores, assim que possível**

Obrigado

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

gzorello@nic.br

2 de dezembro de 2020

nic.br cgi.br

www.nic.br | www.cgi.br