
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

Melhores práticas para a segurança de seu provedor

Uma abordagem para os gestores

Gilberto Zorello

Encontro Nacional ABRINT 2024 – São Paulo, SP | 12/06/24

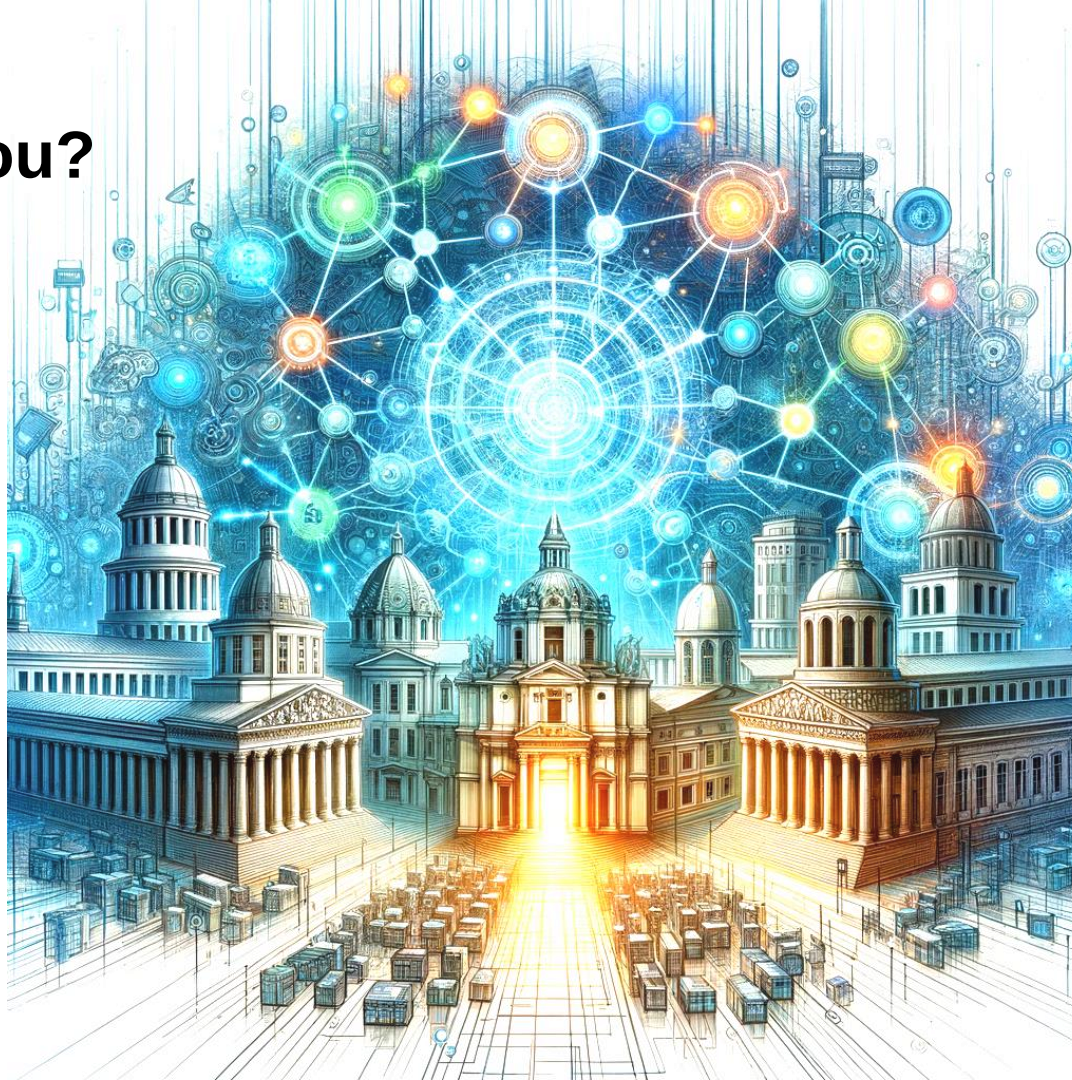
registro.br nic.br cgi.br

Por que os padrões técnicos, boas práticas e colaboração são importantes para a Internet?

registro.br nic.br cgi.br

Como a Internet começou?

- Projeto da DARPA
- Redes resilientes
- Chegou ao Brasil na década de 1990
- Eco 92
- Abertura comercial
- CGI.br e NIC.br



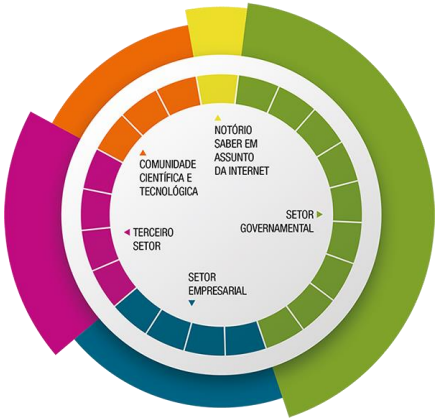
NIC.br e CGI.br

- CGI.br: criado em 1995
- Decreto em 2003
- Diretrizes para o desenvolvimento da Internet no Brasil
- NIC.br: organização privada sem finalidade de lucro
- Braço executivo do CGI.br

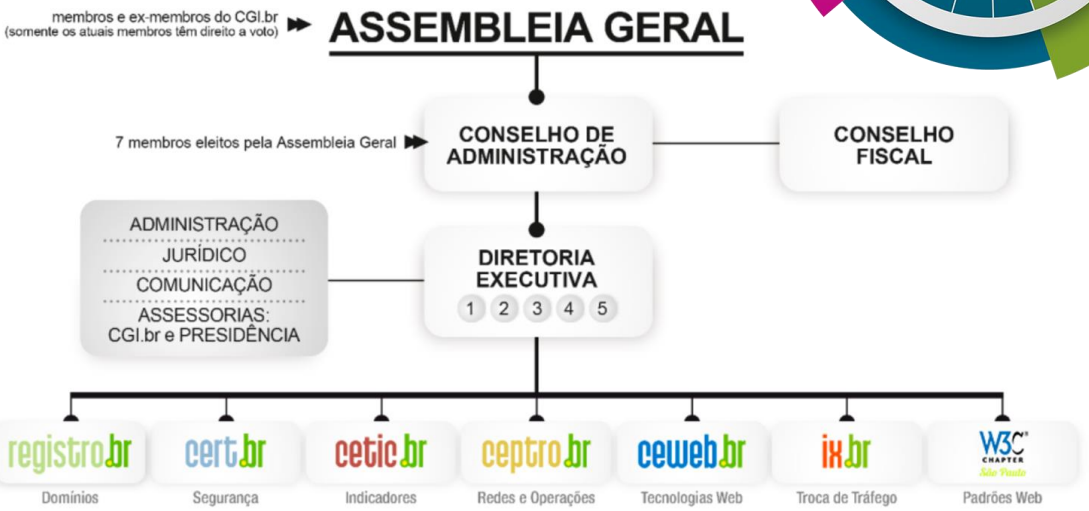
https://cgi.br/
https://nic.br/

NIC.br e CGI.br

cgi.br



nic.br



1 Diretor presidente
2 Diretor administrativo e financeiro
3 Diretor de serviços e de tecnologia
4 Diretor de projetos especiais e de desenvolvimento
5 Diretor de assessoria às atividades do CGI.br

Padrões técnicos e colaboração

- RFCs
- IETF
- Padrões Abertos
- ~ 75 mil redes na Internet
- ~ 9 mil no Brasil
- Colaboração

https://ietf.org/
https://bgp.potaroo.net/
https://mapadeas.ceptro.br/

Boas práticas e padrões na Infraestrutura

Boas práticas e padrões de Segurança

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

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

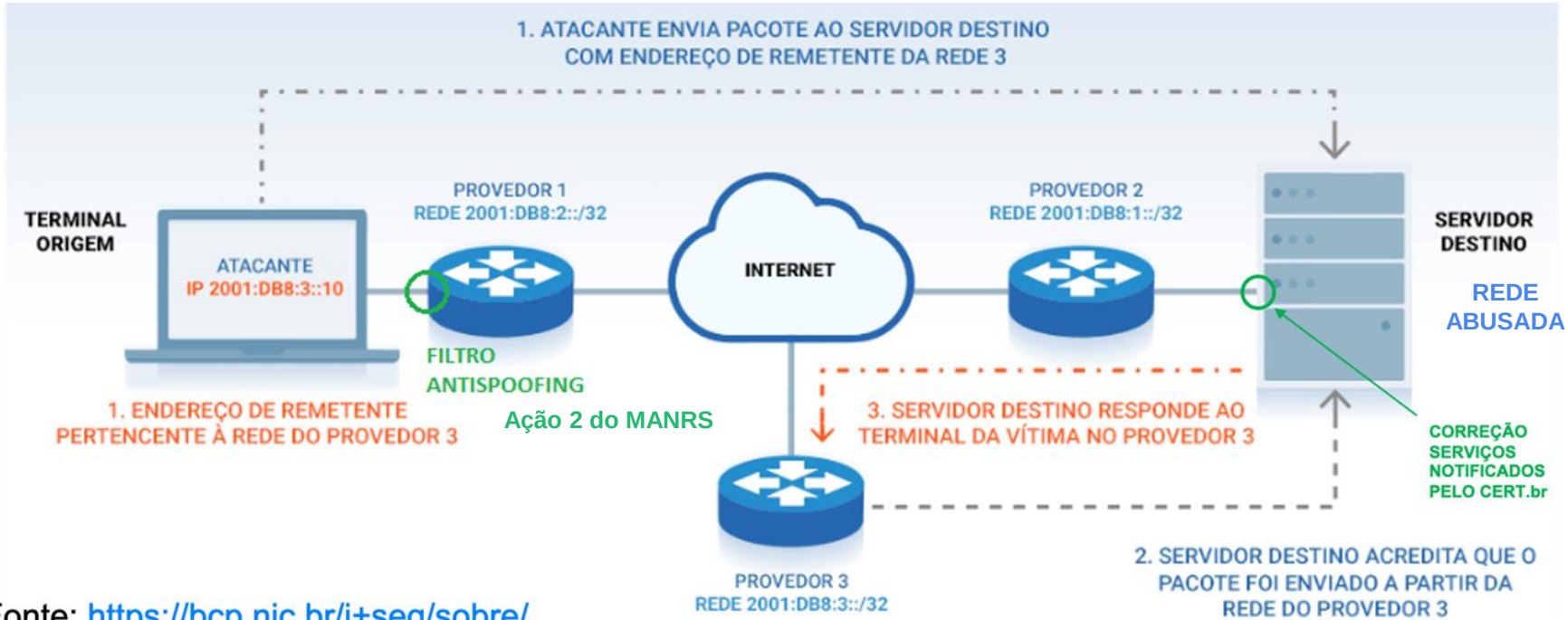
https://bcp.nic.br/i+seg

Programa por uma Internet mais Segura

Plano de Ação

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

Ataque DoS utilizando endereço de remetente forjado (Spoofing)



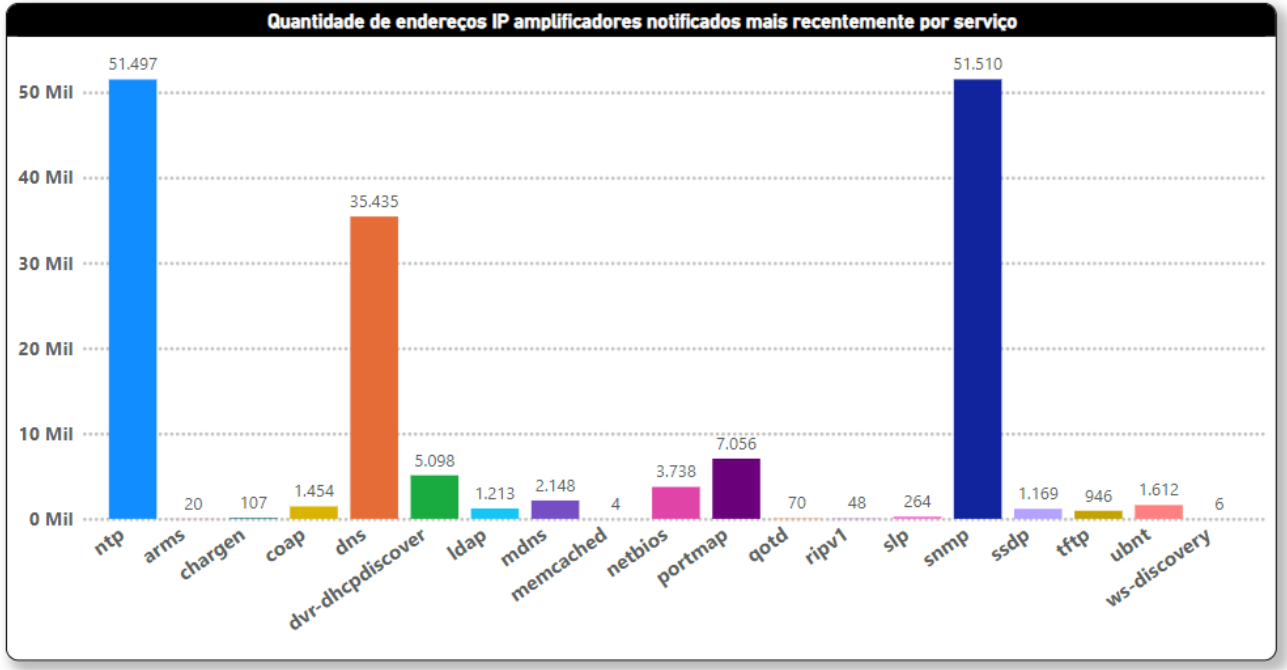
Fonte: https://bcp.nic.br/i+seg/sobre/

Configuração de serviços expostos na Internet

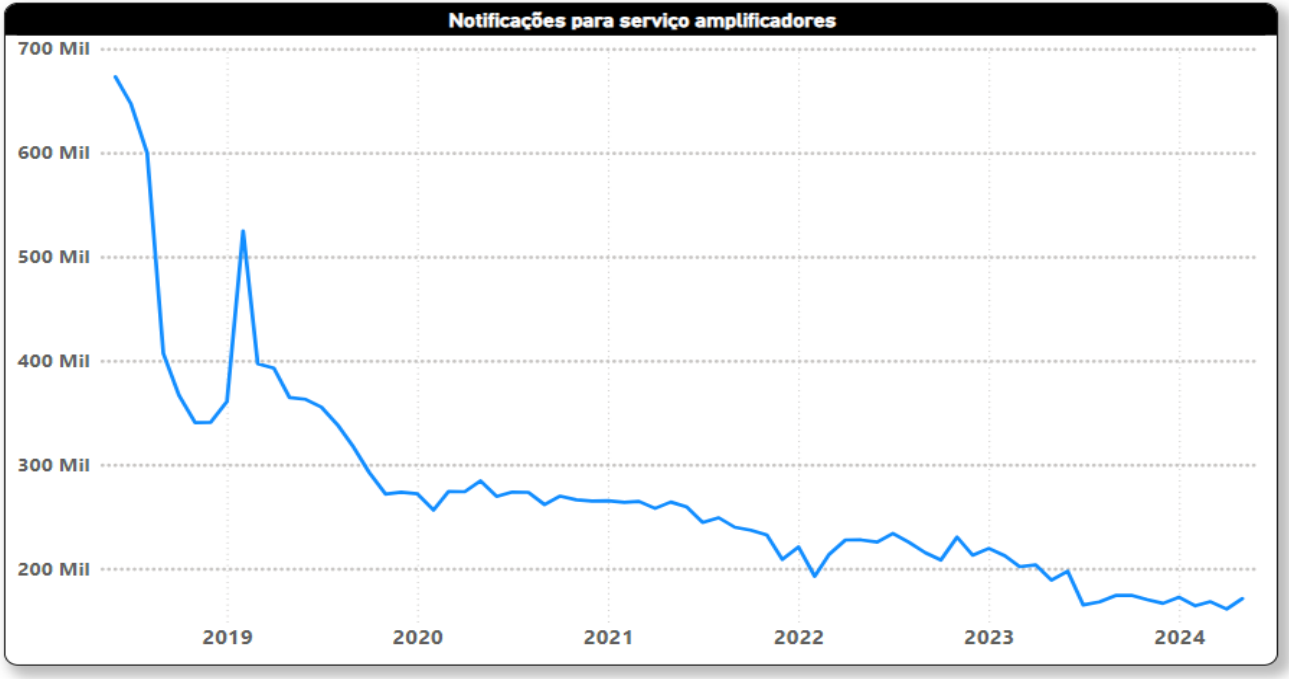
- Usados para amplificação em DDoS
- Portas UDP: DNS (53), SNMP (161), NTP (123), e várias outras!
- Notificações do CERT.br

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

Notificação de Amplificadores - Serviços



Notificação de Amplificadores - Evolução



76% de redução de serviços mal configurados desde o início do Programa

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

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

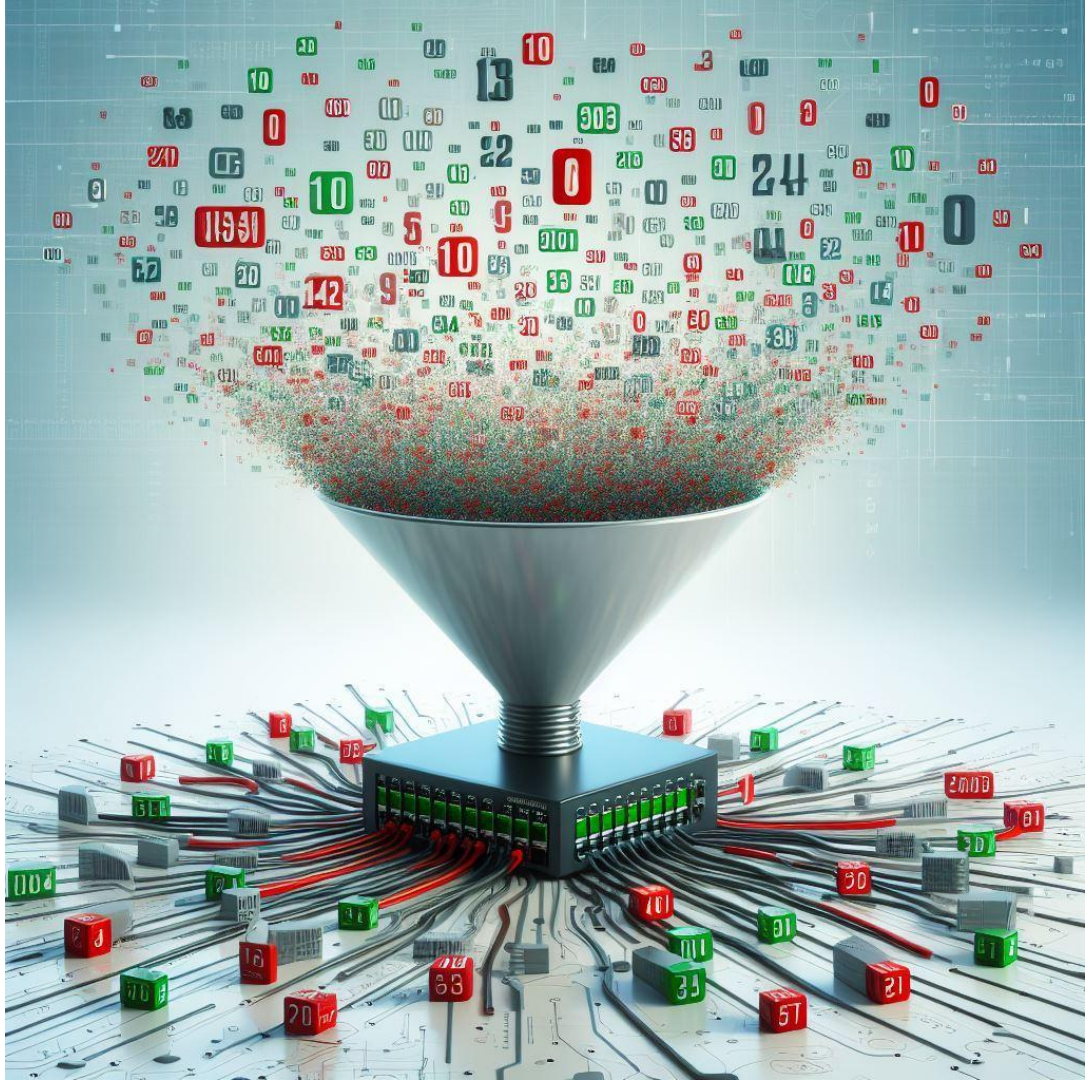
nic.br cgi.br

MANRS

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/



nic.br cgi.br

MANRS

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)!

https://bcp.nic.br/antispoofing/

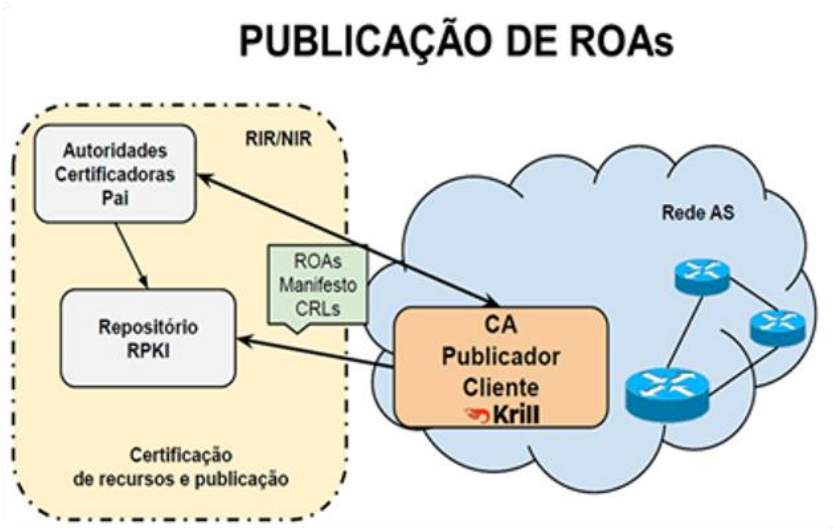
MANRS - Ação 3 - Pontos de Contato

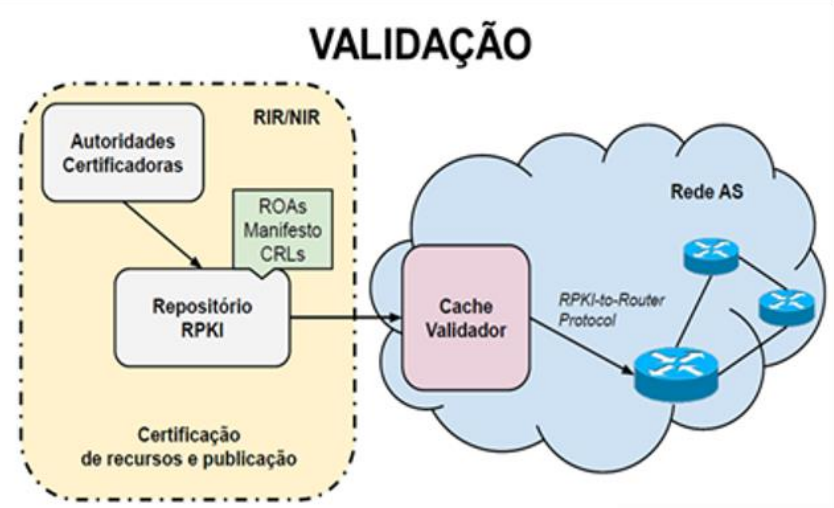
- **Contatos de roteamento e abuse no Registro.br** devem estar atualizados e serem de grupos de pessoas. Ex.: noc@seuprovedor.com.br
  - Registro.br está validando os e-mails de abuse e a não resposta pode causar a recuperação (perda) dos endereços IP
  - Mensagens do CERT.br estão indo para o SPAM em alguns casos!
- Atualizar contatos no **PeeringDB**
- Atualizar contatos no **IRR**

MANRS - Ação 4 - Cadastro da Política de Roteamento

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

- **RPKI** - Resource Public Key Infrastructure



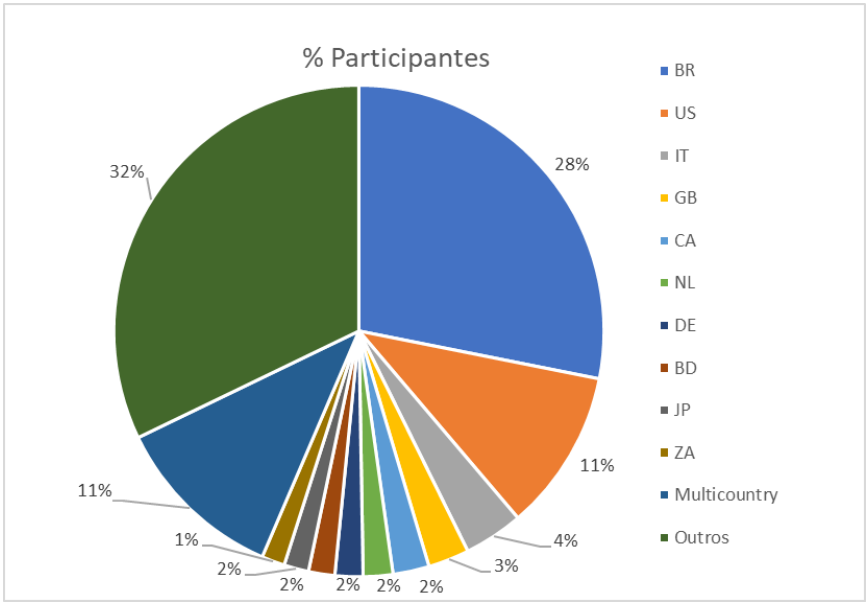


nic.br cgi.br

MANRS

Programa por uma Internet mais Segura

Participantes do MANRS por país



Total de participantes do MANRS: 942

Participantes no Brasil: 264 (Mai/24)

258 (2023)

206 (2022)

174 (2021)

140 (2020)

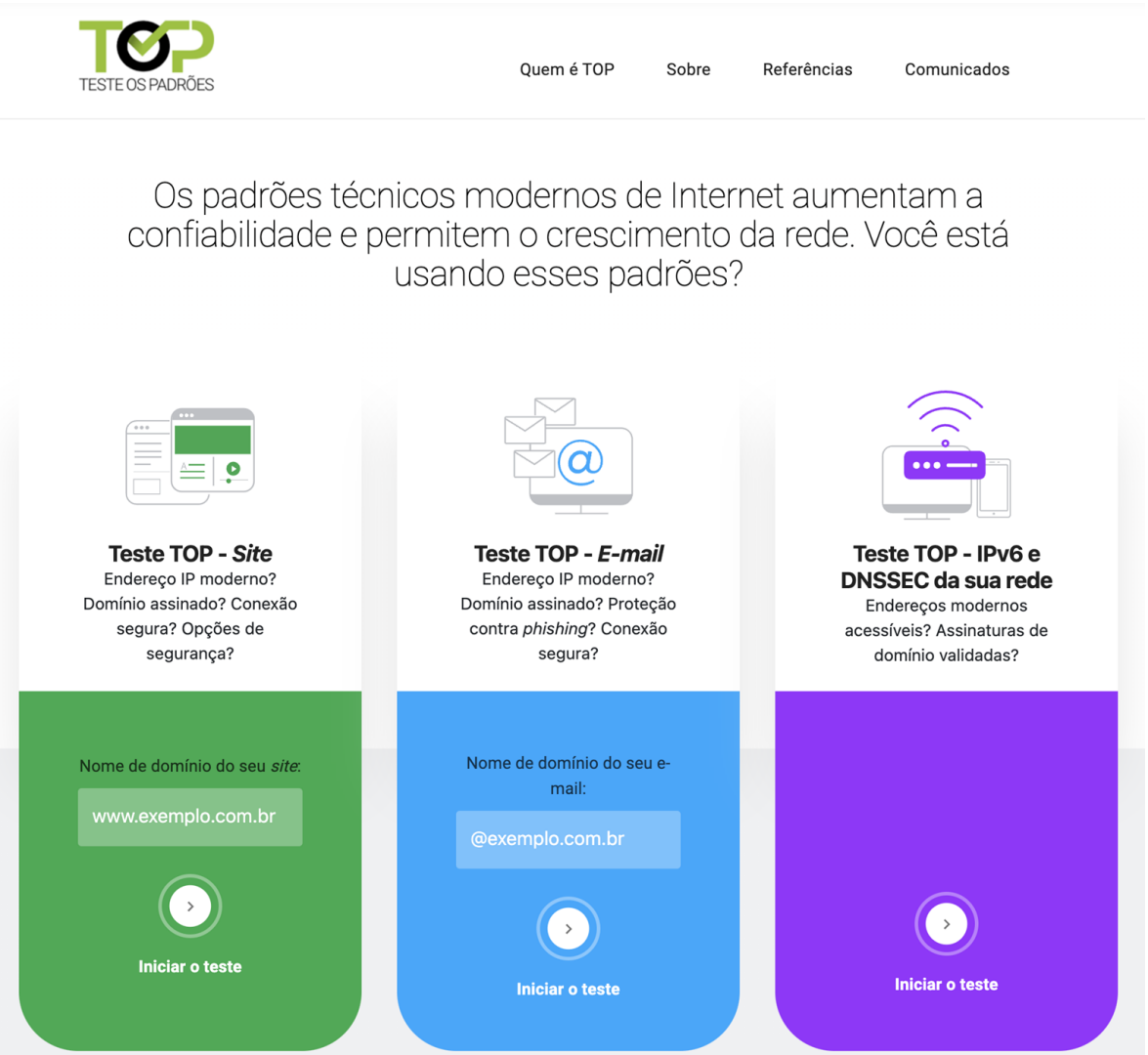
Fonte: https://www.manrs.org/netops/participants/ Acesso mai/24

Boas práticas para DNS

- KIN**DNS** 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



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

TESTE OS PADRÕES

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

Programa por uma Internet mais Segura

Apoio

Obrigado!

Venha conversar com a gente
no stand aqui no Encontro Nacional
ABRINT 2024!

Giberto Zorello
gzorello@nic.br
https://www.linkedin.com/in/gzorello

nic.br cgi.br