



nic.br

Núcleo de Informação
e Coordenação do
Ponto BR

egi.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

Gilberto Zorello | gzorello@nic.br

Semana de Infraestrutura da Internet do Brasil – GTER 50

São Paulo, SP | 30/11/21

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



Programa por uma Internet mais Segura Iniciativa

Lançado pelo CGI.br e NIC.br

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

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



PROGRAMA
**INTERNET
+SEGURA**

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

- Transversal no NIC.br: CERT.br, CEPTRO.br, IX.br, Registro.br
- 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



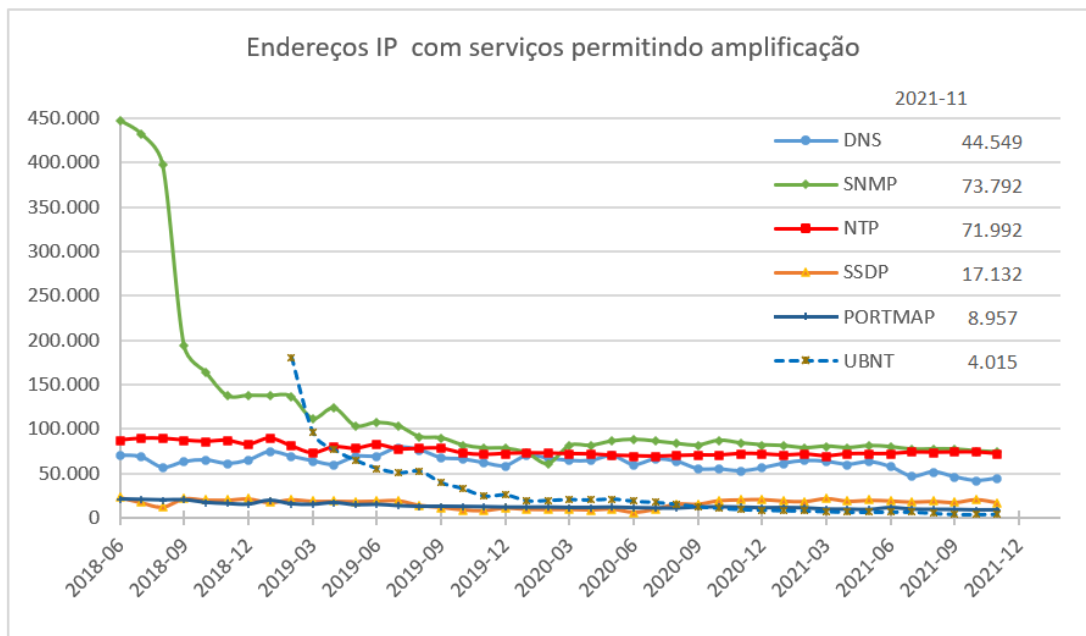
- Reuniões bilaterais bimestrais com as grandes operadoras
- **Em 2021, devido a impossibilidade de participação em eventos presenciais, continuamos com reuniões on-line com os responsáveis pelos ASes com maior quantidade de endereços IP notificados**
- Manutenção do contato com os operadores pelo encaminhamento de relatório gerencial mensal para o acompanhamento da resolução dos problemas notificados
- **Apoio à implantação do RPKI com as grandes operadoras**
- 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**
 - Nova notificação: Serviço SOCKS4 habilitado na porta 5678/TCP, provável infecção com a botnet Mëris
 - **Adoção de Boas Práticas de roteamento (MANRS)**

Programa por uma Internet mais Segura

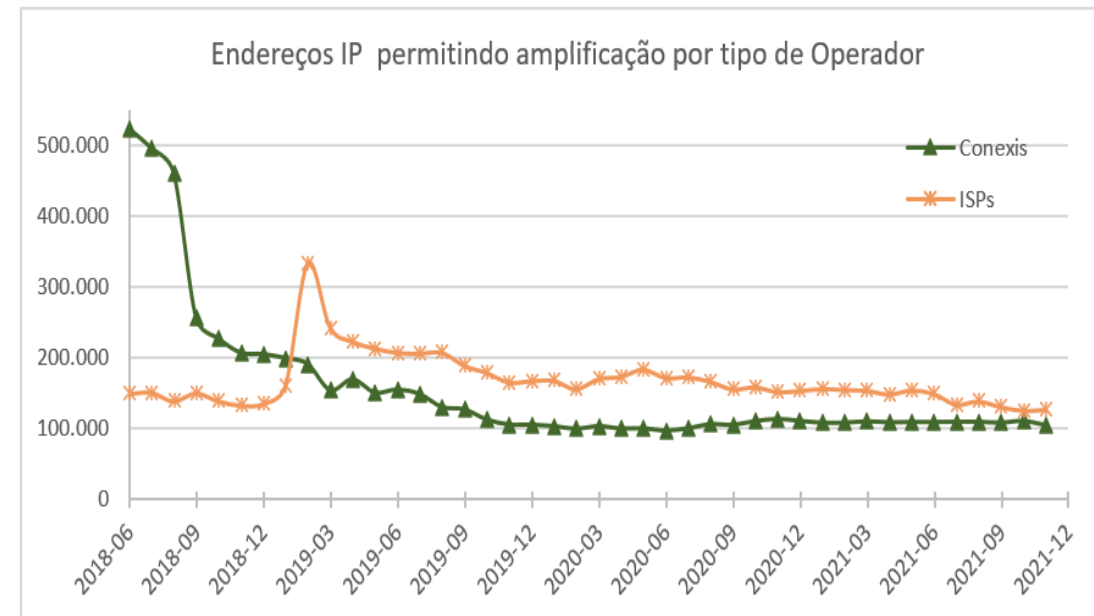
Desenvolvimento do Programa



- Quantidade de endereços IP notificados com serviços mal configurados



Fonte dos dados: CERT.br



Fonte dos dados: CERT.br

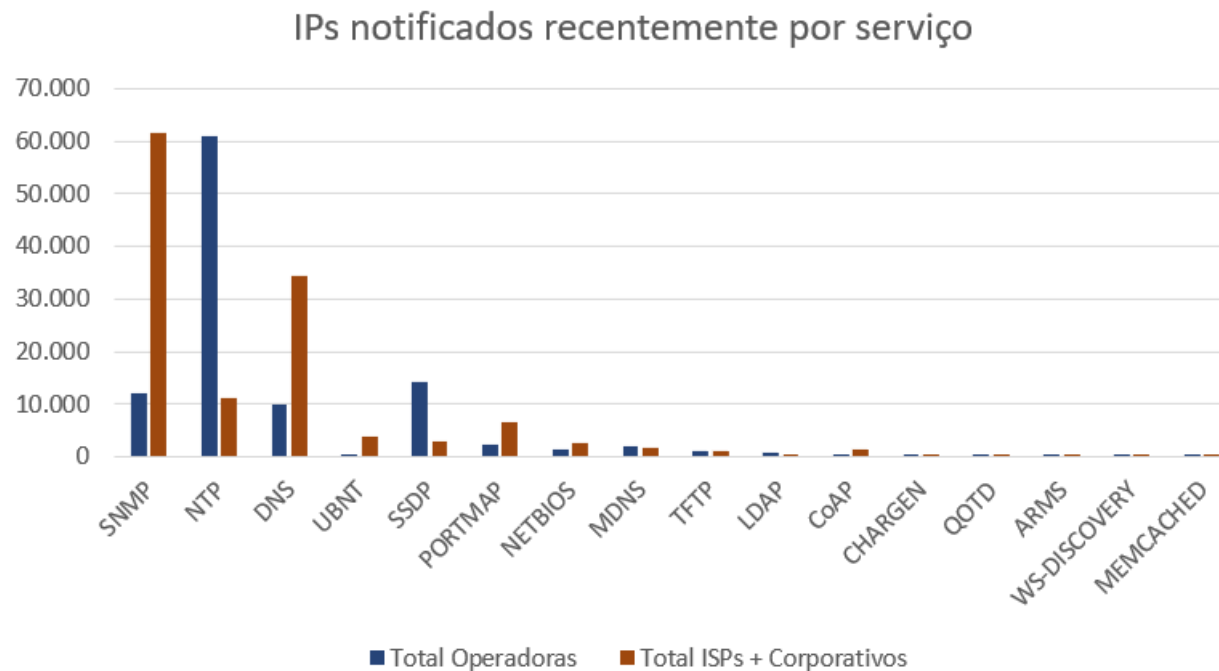
Redução de 68% dos endereços IP mal configurados desde o início do Programa

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 e PORTMAP**

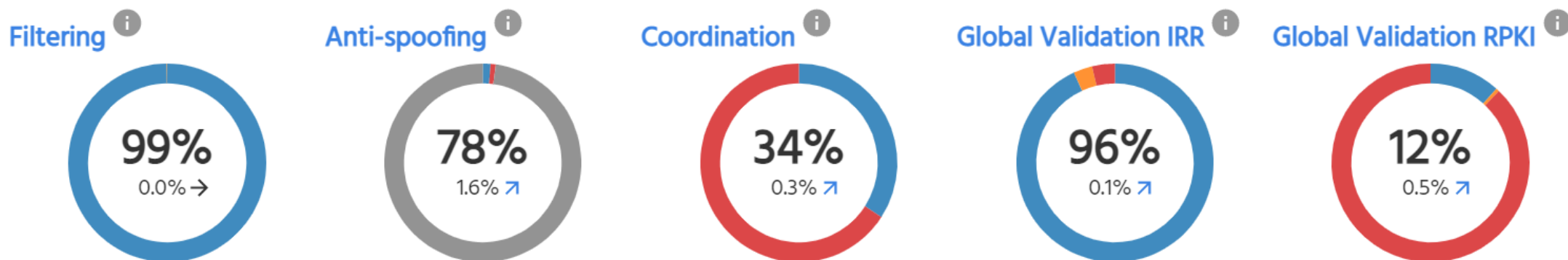
Grandes operadoras → **NTP, SSDP, SNMP e DNS**

Programa por uma Internet mais Segura

MANRS Observatory – Readiness – Nov/21

Conjunto de ASes do Brasil

MANRS Readiness ⁱ



● Ready ● Aspiring ● Lagging ● No Data Available

Ação 1

99% (2020)

Ação 2

74% (2020)

Ação 3

30% (2020)

Ação 4

95% (2020)

6% (2020)

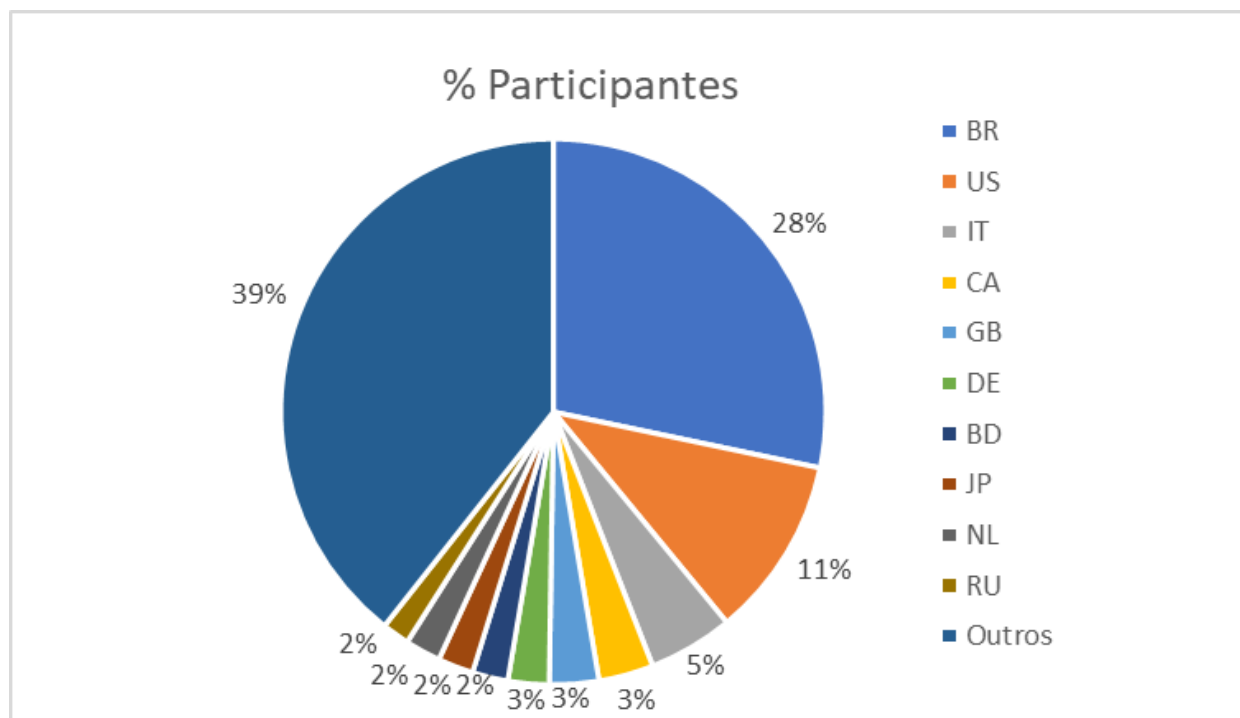
<https://observatory.manrs.org/#/overview> brasil 26/11/21

Programa por uma Internet mais Segura

Desenvolvimento do Programa



- Distribuição por país dos participantes da iniciativa **MANRS**



Total de participantes: 615

Participantes do Brasil: 174

140 (2020)

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



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



TOP – Teste os Padrões – Por quê?



A Internet está em constante evolução para poder continuar crescendo e suportando os serviços

Os protocolos padronizados utilizados na Internet tem suas novas versões e muitos as desconhecem

A ferramenta TOP procura mostrar a importância destes novos padrões e da sua adoção para reduzir as ameaças na Internet e permitir a expansão da Internet

TOP – Teste os Padrões – O que é?



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

Informa se o *site*, *e-mail* ou conexão à Internet utilizada segue os padrões técnicos mais modernos e confiáveis de Internet

Informa o que pode ser feito se os padrões não são seguidos

Adaptado pelo NIC.br que utiliza como base o Internet.nl, iniciativa da holandesa Internet Standards Platform

Acessível por <https://top.nic.br>

TOP – Teste os Padrões - Motivação



Os padrões técnicos originais de Internet datam das décadas de 70 e 80, quando o número de usuários de Internet era pequeno

Atualmente, existem mais de três bilhões de usuários em todo o mundo!

A Internet é cada vez mais utilizada para transações com informações sensíveis e muitas vezes envolvendo altos valores

Os padrões antigos não conseguem atender à escala atual de crescimento e nem aos modernos requisitos de segurança

Exemplo: violação do padrão SMTP para falsificar o endereço do remetente de *e-mails*

Temos que começar a usar padrões novos e mais inteligentes que mantenham nossa Internet confiável

A boa notícia é que estes padrões técnicos modernos de Internet estão disponíveis

<https://top.nic.br>

TOP – Teste os Padrões – Quem deve agir?



O Brasil é um país de uso intensivo de Internet e infelizmente utilizamos muitos padrões técnicos ultrapassados

Não utilizar os padrões técnicos modernos é um risco não só para o usuário individual, mas para a economia do país e do mundo

Faça sua parte e ajude a melhorar a Internet tendo a certeza de utilizar os padrões técnicos modernos!

Nossas operadoras, provedores de acesso, de hospedagem de *sites* e de *e-mail* devem se encarregar da implementação dos padrões técnicos modernos de Internet e configurá-los corretamente

Se os resultados dos testes mostrarem alguma deficiência, o usuário deve enviar uma mensagem a respeito à sua operadora ou provedor de serviço!

<https://top.nic.br>

TOP – Teste os Padrões – Sobre os testes



O TOP verifica a correta implementação dos padrões técnicos modernos de Internet que melhoram a confiabilidade e qualidade dos serviços *on-line*

Uma pontuação de 100% significa que um *site*, *e-mail* ou conexão à Internet foi testado e está em conformidade com os padrões modernos de Internet

Porém o resultado 100% não significa que um serviço *on-line* seja totalmente seguro

Os testes baseiam-se nos padrões técnicos especificados nas RFC de cada categoria de testes e em padrões técnicos operacionais recomendados por entidades internacionais

Referências detalhadas sobre os testes realizados são disponibilizados: padrões utilizados em cada teste, categoria de teste e subtestes

Após o teste ser finalizado é disponibilizado um relatório com os resultados dos testes

<https://top.nic.br>

TOP – Teste os Padrões – Relatório



Há três testes principais: *sites*, serviços de *e-mail* e IPv6 e DNSSEC da rede

Os testes principais são constituídos de categorias de testes que incluem subtestes

Exemplo: teste de *site*, contém uma categoria de teste HTTPS, que inclui um subteste HSTS

Um subteste tem três níveis de exigência: Exigido (*must*), Recomendado (*should*) e Opcional (*may*)

Cada teste resulta em uma pontuação percentual geral

- Cada categoria pesa de forma mais ou menos uniforme no percentual geral
- Somente os subtestes com nível de exigência **Exigido** contribuem para a pontuação geral
- *Sites* e serviços de *e-mail* com pontuação de 100% são incluídos no **Quem é TOP**
- As pontuações são transparentes e individualizadas

Os resultados para cada categoria de teste e subteste podem ser: Bom, Ruim, Aviso, Informação, Não testado, Erro

<https://top.nic.br>

TOP – Teste os Padrões – Quem é TOP?



Quem é TOP - Campeões!

- Domínios que pontuaram 100% no **Teste TOP – Sites** e **Teste TOP – E-mail**

Quem é TOP - Sites

- Domínios que pontuaram 100% no Teste TOP – Sites

Quem é TOP – E-mail

- Domínios que pontuaram 100% no Teste TOP – E-mail



Quem é TOP – Hospedagem

- Domínios que pontuaram 2 x 100% no Teste TOP – Sites e Teste TOP – E-mail
- Domínios de clientes 2 x 100%
- Registro comercial
- Apenas por solicitação



<https://top.nic.br>

Testes IPv6 – Testes Realizados

Teste TOP - Site	
Endereço IP moderno (IPv6)	
Servidores de nomes	Endereços IPv6 para servidores de nomes Acessibilidade IPv6 dos servidores de nomes
Servidor web	Endereços IPv6 para servidor web Acessibilidade IPv6 do servidor web Mesmo site com endereços IPv6 e IPv4
Nome de domínio assinado (DNSSEC)	
Existência de DNSSEC Validade de DNSSEC	
Conexão segura (HTTPS)	
HTTP	HTTPS disponível Redirecionamento para HTTPS Compressão HTTP HSTS
TLS	Versão de TLS Cifras (Seleções de algoritmos) Ordem das cifras Parâmetros de troca de chaves Função hash para troca de chaves Compressão TLS Renegociação segura Renegociação iniciada pelo cliente 0-RTT OCSP stapling
Certificado	Cadeia de confiança do certificado Chave pública do certificado Assinatura do certificado Nome de domínio no certificado
DANE	Existência de DANE Validade de DANE
Opções de segurança	
Cabeçalhos de segurança HTTP X-Frame-Options X-Content-Type-Options Content-Security-Policy (CSP) Existência de Referrer-Policy	

Teste TOP - E-mail	
Endereço IP moderno (IPv6)	
Servidores de nomes	Endereços IPv6 para servidores de nomes Acessibilidade IPv6 dos servidores de nomes
Servidor(es) de e-mail	Endereços IPv6 para servidor(es) de e-mail Acessibilidade IPv6 do(s) servidor(es) de e-mail
Nomes de domínio assinados (DNSSEC)	
Domínio do endereço de e-mail Existência de DNSSEC Validade de DNSSEC	
Domínio(s) do(s) servidor(es) de e-mail Existência de DNSSEC Validade de DNSSEC	
Marcas de autenticidade contra phishing (DMARC, DKIM and SPF)	
DMARC	Existência de DMARC Política de DMARC
DKIM	Existência de DKIM
SPF	Existência de SPF Política de SPF
Conexão segura com servidor de e-mail (STARTTLS e DANE)	
TLS	STARTTLS disponível Versão de TLS Cifras (Seleções de algoritmos) Ordem das cifras Parâmetros de troca de chaves Função hash para troca de chaves Compressão TLS Renegociação segura Renegociação iniciada pelo cliente 0-RTT
Certificado	Cadeia de confiança do certificado Chave pública do certificado Assinatura do certificado Nome de domínio no certificado
DANE	Existência de DANE Validade de DANE Esquema de substituição de DANE

Teste TOP - IPv6 e DNSSEC da sua rede
Endereços modernos acessíveis (IPv6)
Conectividade IPv6 do servidor recursivo de DNS Conectividade IPv6 (via DNS) Conectividade IPv6 (direta) Extensões de privacidade para IPv6 Conexão IPv4 (via DNS) Assinaturas de domínio não validadas (DNSSEC)
Validação DNSSEC

Utilize o TOP como ferramenta para ajudar a corrigir as configurações dos serviços prestados e ajude a melhorar a segurança da infraestrutura da Internet

<https://top.nic.br>



TOP – Teste os Padrões - Apoio





<https://top.nic.br>

Dúvidas

?

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

Obrigado

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

@ gzorello@nic.br

30 NOV 21

nic.br **cgi.br**

www.nic.br | www.cgi.br