



**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**

membros e ex-membros do CGI.br  
(somente os atuais membros têm direito a voto) ➔

# ASSEMBLEIA GERAL

7 membros eleitos pela Assembleia Geral ➔

**CONSELHO DE  
ADMINISTRAÇÃO**

**CONSELHO  
FISCAL**

ADMINISTRAÇÃO  
.....  
JURÍDICO  
.....  
COMUNICAÇÃO  
.....  
ASSESSORIAS:  
CGI.br e PRESIDÊNCIA

**DIRETORIA  
EXECUTIVA**

1 2 3 4 5

**registro.br**

Domínios

**cert.br**

Segurança

**cetic.br**

Indicadores

**ceptro.br**

Redes e Operações

**ceweb.br**

Tecnologias Web

**ix.br**

Troca de Tráfego

**W3C**  
Brasil

Padrões Web

- 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

# Seu provedor mais seguro e eficiente com a ajuda do **NIC.BR**

Gilberto Zorello

Atualiza Telecom 2022 – Encontro Regional de Provedores

28/7/2022

**nic.br**

# Nossa Agenda

- **Sistemas Autônomos**
- **IX.Br – IX.br Salvador - OpenCDN**
- **IPv6**
- **RPKI**
- **NTP + NTS**
- **Boas Práticas**
- **Cidadão na Rede**
- **Programa por uma Internet mais Segura**
- **TOP – Teste os Padrões**

nic.br



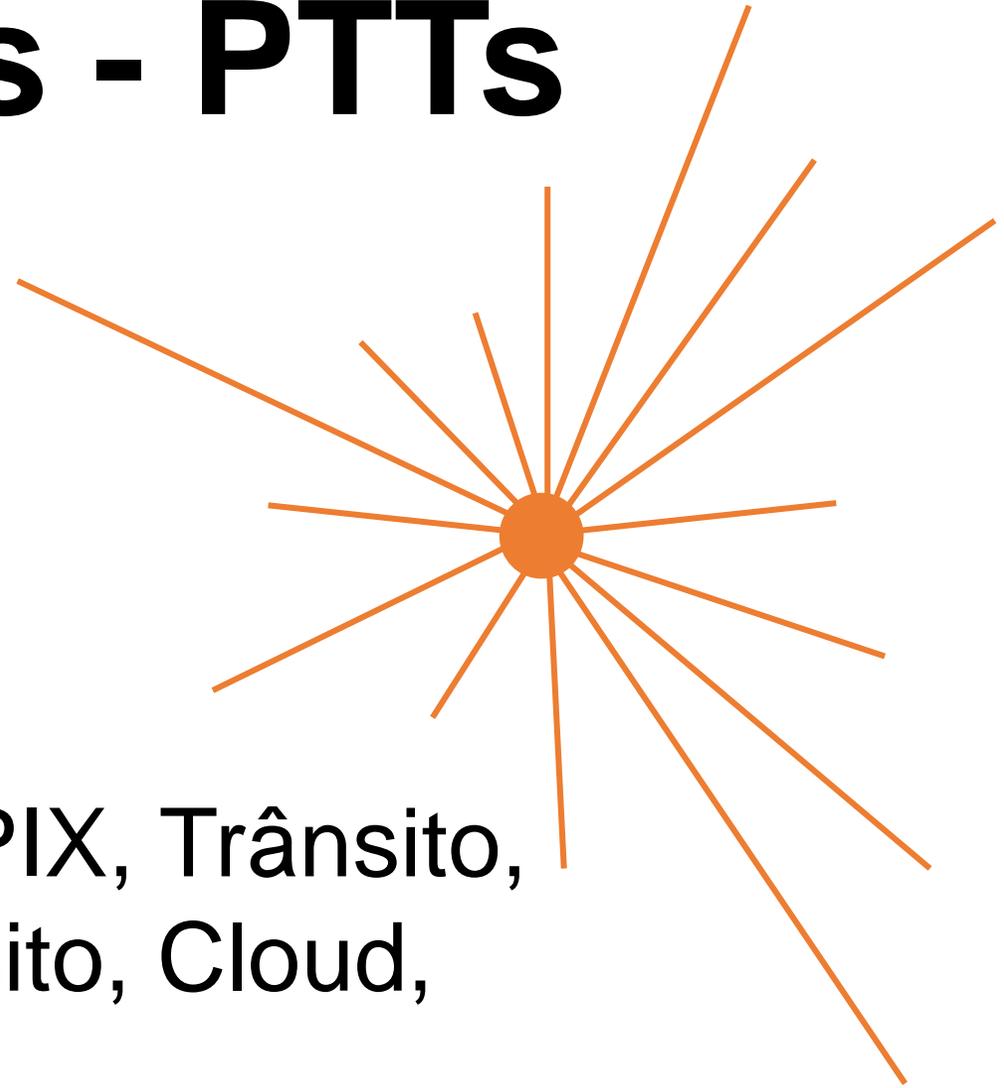
TOP  
TESTE OS PADRÕES

# Sistemas Autônomos

- Recursos próprios: ASN, **IPv6**, IPv4
- **Ainda vale a pena? Sim!**
- Política própria de roteamento
  - Redundância
  - Mais qualidade / Controle / Maturidade da rede
- Peering / Troca de tráfego
- Participação em IX / PTTs

# Internet Exchanges - PTTs

- Qualidade
- Racionalização dos Custos
- Peering / Troca de Tráfego
- Conteúdos Locais e CDNs
- **Negócios em Conjunto:** CIX, PIX, Trânsito, Transporte L2, Backup de Trânsito, Cloud, Mitigação de DDoS





# OpenCDN

- Compartilhamento de infraestrutura
- Datacenter + Transporte/Trânsito
- Custo compartilhado

Disponível em Salvador

# IPv6

- Protocolo atual da Internet
- 35% dos usuários já utilizam
- CPEs, SmartTVs, Games = problemas
- Tira a carga do CGNAT
- Não expanda sua rede sem ele
- Planeje a migração do legado

# RPKI

- Melhora a segurança do BGP, dificultando sequestros de blocos IP
- Certificação de Recursos
- Validação da Origem
- Implante!

# NTP + NTS

- Importante para o funcionamento dos sistemas e para os logs
- Falhas de segurança no NTP
- NTS = Network Time Security
  - Pacotes NTP assinados com criptografia
- **NTP.br**

# Boas Práticas

- Curso **BCOP (On-line e presencial)**
- Curso **IPv6 [Básico (EAD) e Avançado]**
- Semana da Capacitação
- Lives Intra Rede
- IX Fórum Regional
- IX Fórum >> **SP = 26 a 28 de outubro**

# Cidadão na Rede

- Animações de 15 segundos
  - 74 hoje, 1 nova por semana
- Público leigo = **seus usuários / clientes**
- Funcionamento da Internet, como fazer um uso seguro, direitos e deveres, etc.
- Você pode apoiar: animações com seu logotipo: **[cidadanarede.nic.br](http://cidadanarede.nic.br)**



# Programa por uma Internet mais Segura Iniciativa

## Lançado pelo CGI.br e NIC.br

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

## Objetivo - apoio à comunidade técnica para:

- 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 das redes**



PROGRAMA  
**INTERNET  
+SEGURA**



PROGRAMA  
**INTERNET  
+SEGURA**

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



# 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 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 (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



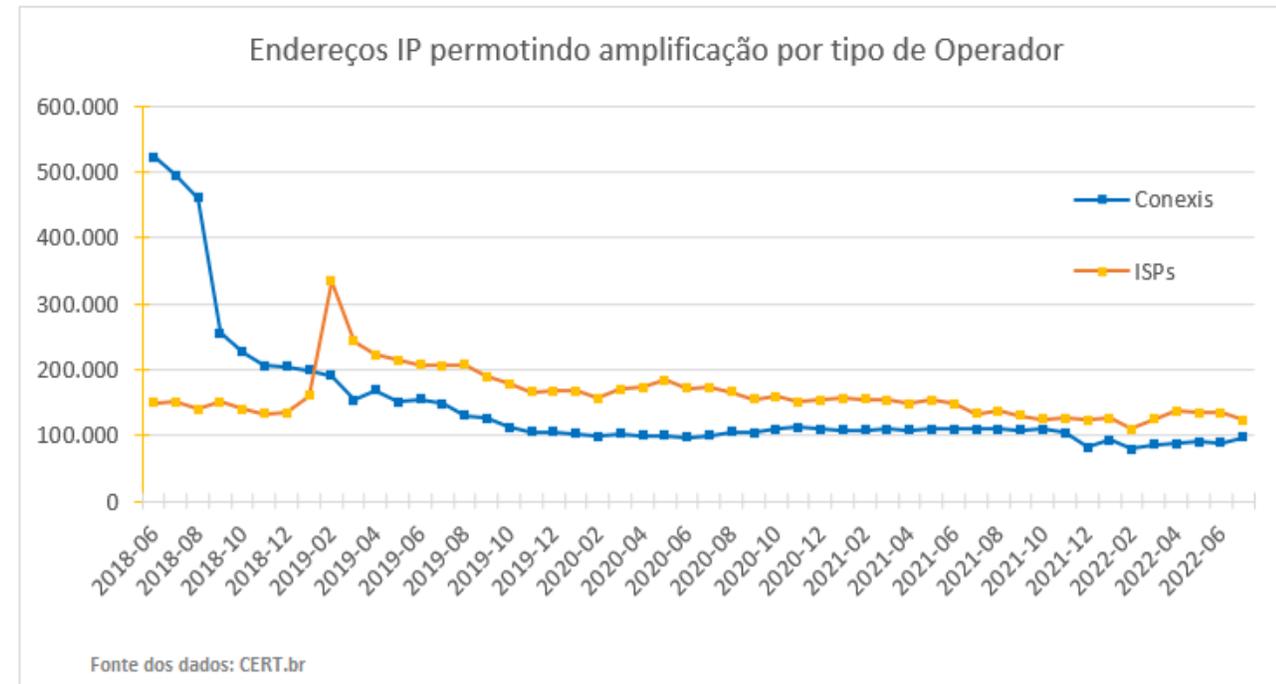
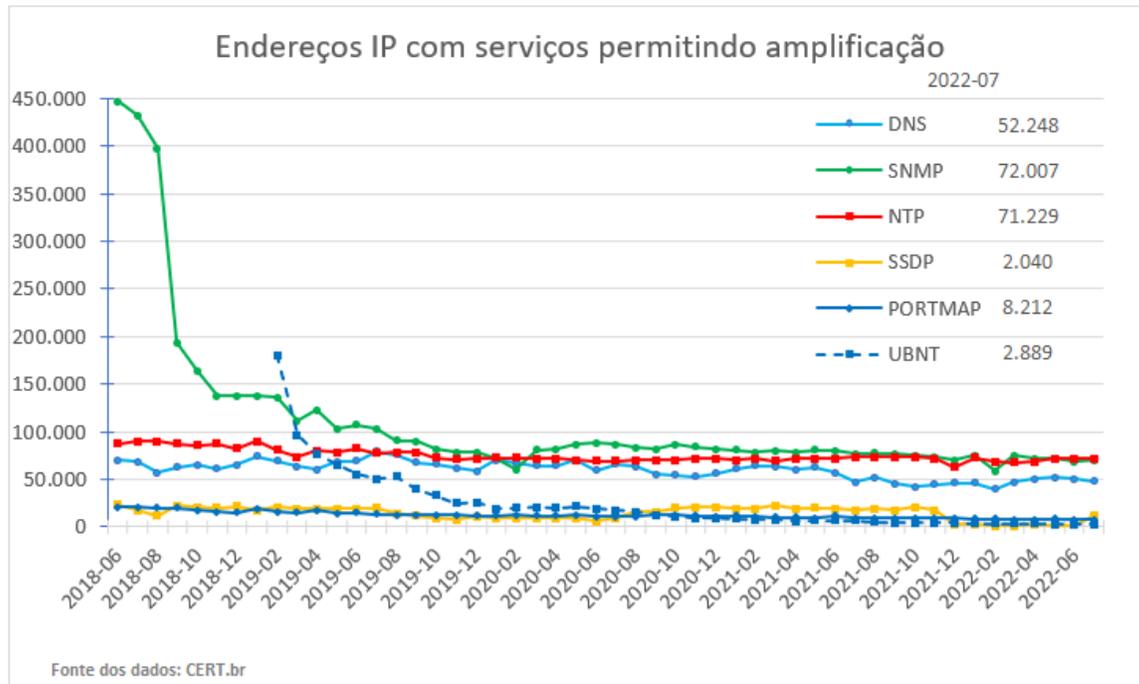
- Reuniões bilaterais bimestrais com as grandes operadoras
- **Reuniões *on-line* com os responsáveis pelos ASes com maior quantidade de endereços IP notificados**
- Encaminhamento de relatório gerencial mensal para o acompanhamento da resolução dos problemas notificados pelo CERT.br
- **Temas tratados nas reuniões bilaterais:**
  - Acompanhamento da correção dos serviços mal configurados notificados
  - 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



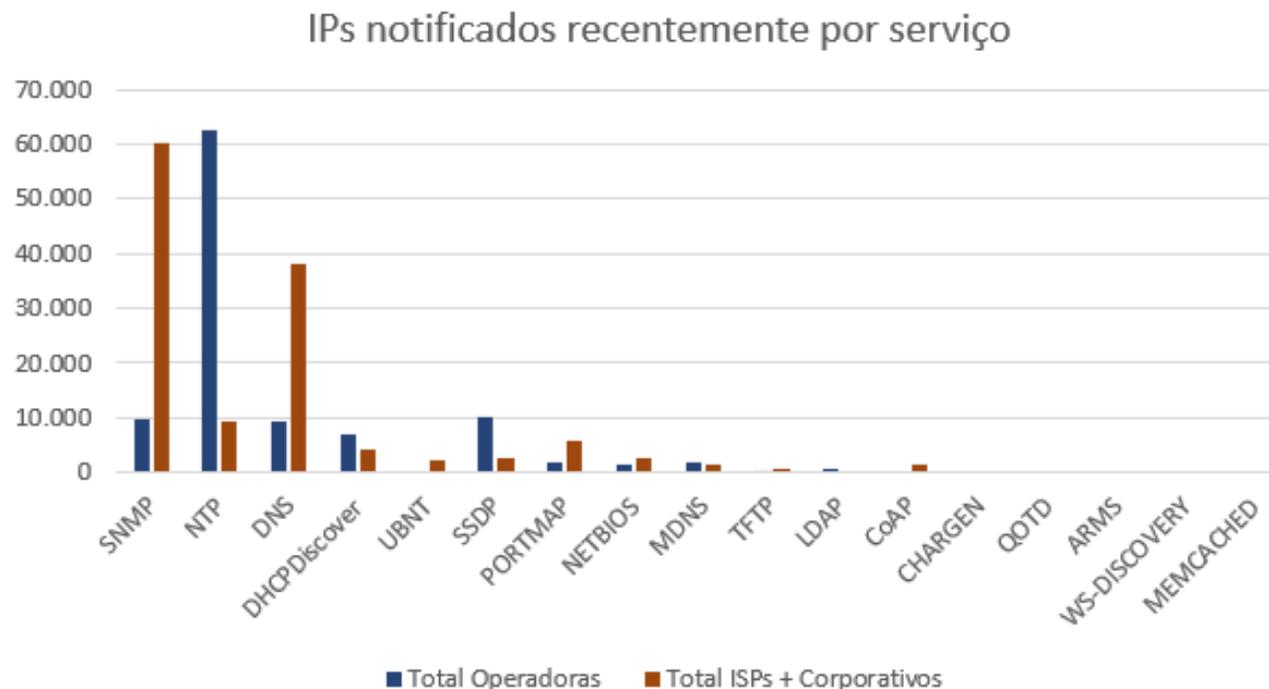
**Redução de 69% dos endereços IP mal configurados desde o início do Programa**

# Programa por uma Internet mais Segura

## Desenvolvimento do Programa



- Endereços IP notificados recentemente por serviço mal configurado



Fonte dos dados: CERT.br

**Principais ofensores: ISPs e ASes corporativos → SNMP e DNS**

**Grandes operadoras → NTP**



# MANRS

## Mutually Agreed Norms for Routing Security

<http://manrs.org>

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

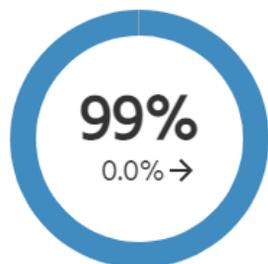
# Programa por uma Internet mais Segura

## MANRS Observatory – Readiness – Jul/22

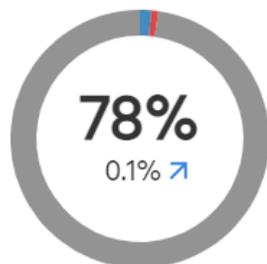
### Conjunto de ASes do Brasil

#### MANRS Readiness <sup>i</sup>

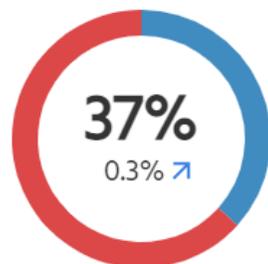
##### Filtering <sup>i</sup>



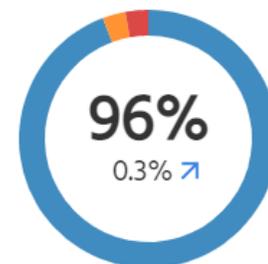
##### Anti-spoofing <sup>i</sup>



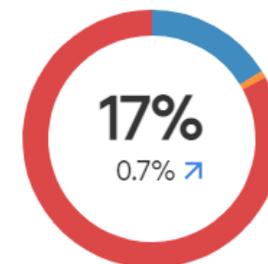
##### Coordination <sup>i</sup>



##### Global Validation IRR <sup>i</sup>



##### Global Validation RPKI <sup>i</sup>



● Ready ● Aspiring ● Lagging ● No Data Available

#### Ação 1

99% (2020)

#### Ação 2

74% (2020)

#### Ação 3

30% (2020)

#### Ação 4

6% (2020)

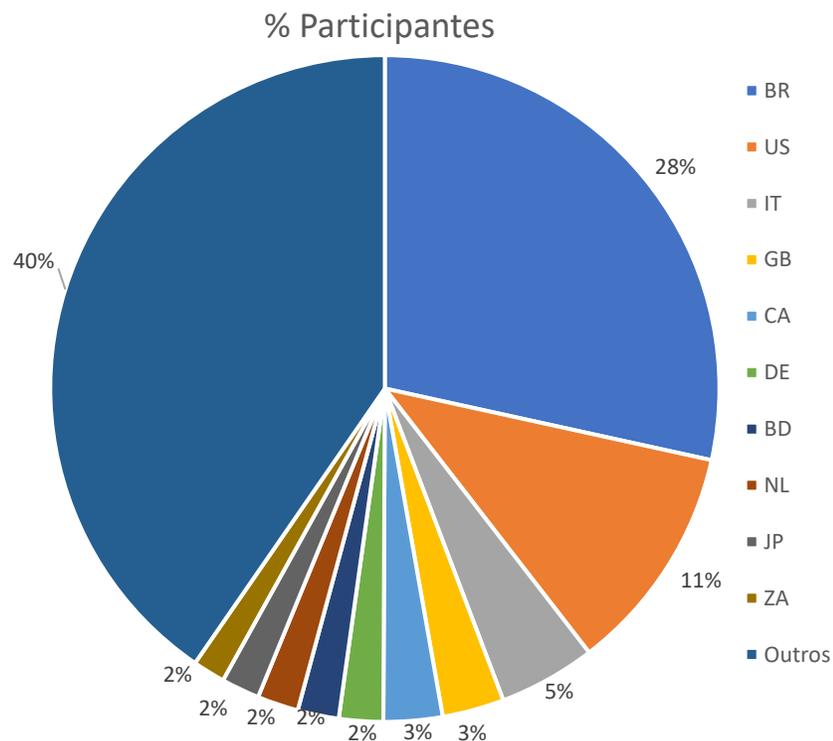
<https://observatory.manrs.org/#/overview> brasil 25/07/22

# Programa por uma Internet mais Segura

## Desenvolvimento do Programa



- Distribuição por país dos participantes da iniciativa MANRS



Total de participantes: 703

Participantes do Brasil: 169 (29%)

140 (2020)

Ref. Jun/22

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



PROGRAMA  
**INTERNET  
+SEGURA**

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



# TOP – Teste os Padrões – Por quê?

A Internet está em constante evolução para poder continuar crescendo e ampliando os serviços oferecidos à sociedade

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

A ferramenta TOP mostra a importância destes novos padrões e como podem ajudar a reduzir as ameaças na Internet e permitir sua expansão



<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 bilhões de usuários utilizando a Internet com informações sensíveis!**

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

Ex.: violação do SMTP para falsificar o endereço do remetente de e-mails

**Devemos começar a usar padrões novos e mais inteligentes para manter a Internet que utilizamos confiável**

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



<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

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

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

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

Outras implementações baseadas no mesmo código de testes:

- Sikkerpånettet.dk ( <https://xn--sikkerpnettet-vfb.dk/> )
- .auCheck ( <https://aucheck.com.au/> )



<https://top.nic.br>

# TOP – Teste os Padrões – Quem deve agir?

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

As **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 pode 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*

- **Teste TOP - Site:** IPv6, DNSSEC, HTTPS e Opções de Segurança
- **Teste TOP - E-mail:** IPv6, DNSSEC, Marcas de Autenticidade e STARTTLS/DANE
- **Teste TOP - IPv6 e DNSSEC da sua rede**

**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 não significa que o serviço seja totalmente seguro**

Os testes baseiam-se nos padrões técnicos especificados em RFCs e em padrões técnicos recomendados por entidades internacionais



<https://top.nic.br>

# TOP – Teste os Padrões – Relatório

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

Os testes principais possuem categorias e estas subtestes

Ex.: Teste TOP - *Site*, possui uma categoria HTTPS, que inclui o subteste HSTS

Um subteste tem três níveis de exigência: **Exigido**, **Recomendado** e **Opcional**

Cada teste resulta em uma pontuação percentual geral

- Cada **categoria pesa** de forma **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**



<https://top.nic.br>

# TOP – Teste os Padrões – Quem é TOP?

## Quem é TOP - Campeões!

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

## Quem é TOP - Site

- Domínios que pontuaram 100% no Teste TOP – Site

## 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 – Site e Teste TOP – E-mail
- Domínios de clientes 2 x 100%
- Registro comercial
- Apenas por solicitação



# Testes Realizados – Teste TOP - Site

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

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	

Cabeçalhos de segurança HTTP	
X-Frame-Options	
X-Content-Type-Options	
Content-Security-Policy (CSP)	
Existência de Referrer-Policy	

Exigido

Recomendado

Opcional

# Testes Realizados – 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
Certificado	Renegociação iniciada pelo cliente
	0-RTT
	Cadeia de confiança do certificado
	Chave pública do certificado
DANE	Assinatura do certificado
	Nome de domínio no certificado
	Existência de DANE
	Validade de DANE
	Esquema de substituição de DANE

Exigido

Recomendado

Opcional

# Testes Realizados – Teste TOP – IPv6 e DNSSEC

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)

Validação de assinatura de domínio (DNSSEC)
Validade de DNSSEC

Exigido

Opcional

# TOP – Teste os Padrões – Resultados - Geral

## Teste TOP - Site

Domínios Únicos	Score 100%	IPv6 100%	DNSSEC 100%	TLS 100%	OPC SEG 100% *	Testes Realizados
7.178	247	1.774	1.520	527	0	17.056
	3%	25%	21%	7%	0%	

## Teste TOP - E-mail

\* Recomendado / Opcional

Domínios Únicos com MX	Score 100%	IPv6 100%	DNSSEC 100%	M. Aut. 100%	STARTTLS DANE 100%	Testes Realizados
2082	30	474	234	421	57	5952
	1%	23%	11%	20%	3%	

Ref.: 24/07/22

# TOP – Teste os Padrões – Resultados - Geral

## Teste TOP – IPv6 e DNSSEC

Cenários IPv6		Qtd / Cenário
I	0%	340
II	20%	395
III	20%	16.438
IV	40%	277
V	60%	8
VI	80%	709
VII	80%	76
VIII	100%	27.373

Cenários DNSSEC		Qtd / Cenário
Válido	100%	26.448
Não válido	0%	19.168

<b>Total de testes realizados</b>	<b>45.616</b>
-----------------------------------	---------------

Cenários IPv6
I - O servidor recursivo não é capaz de acessar o servidor de nomes via IPv6 e o usuário está sem conectividade IPv6 aos computadores da rede via DNS
II - O servidor recursivo não é capaz de acessar o servidor de nomes via IPv6 e o usuário está sem conectividade IPv6 aos computadores da rede via DNS, mas acessa diretamente computadores via IPv6 e as configurações de privacidade para IPv6 estão configuradas
III - O servidor recursivo é capaz de acessar o servidor de nomes via IPv6 mas o usuário está sem conectividade IPv6 aos computadores da rede via DNS
IV - O servidor recursivo é capaz de acessar o servidor de nomes via IPv6, acessa diretamente computadores via IPv6 e as configurações de privacidade para IPv6 estão configuradas, mas o usuário está sem conectividade IPv6 aos computadores da rede via
V - O servidor recursivo não é capaz de acessar o servidor de nomes via IPv6, porém o usuário tem conectividade IPv6 aos computadores da rede via DNS
VI - O servidor recursivo é capaz de acessar o servidor de nomes via IPv6, o usuário está com conectividade IPv6 aos computadores da rede via DNS e as configurações de privacidade para IPv6 estão configuradas, mas não acessa diretamente computadores via
VII - O servidor recursivo não é capaz de acessar o servidor de nomes via IPv6, porém o usuário tem conectividade IPv6 aos computadores da rede via DNS, acessa diretamente computadores via IPv6 e as configurações de privacidade para IPv6 estão configuradas
VIII - O servidor recursivo é capaz de acessar o servidor de nomes via IPv6, o usuário tem conectividade IPv6 aos computadores da rede via DNS, acessa diretamente computadores via IPv6 e as configurações de privacidade para IPv6 estão configuradas

Ref.: 24/07/22

Utilize a ferramenta TOP 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



A CONECTIVIDADE AO SEU ALCANCE



# Obrigado

<https://nic.br/atividades/>

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

<https://top.nic.br>

@ [gzorello@nic.br](mailto:gzorello@nic.br)

28 de julho de 2022

**nic.br egi.br**

www.nic.br | www.cgi.br