



**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**

# **TOP – TESTE OS PADRÕES**

Gilberto Zorello

IX Fórum Regional – Centro-Oeste – Brasília/DF – 29 de abril de 2022

**nic.br**

# Nossa Agenda

## Programa por uma Internet mais Segura

- Iniciativa / Plano de Ação
- Ações recentes

## TOP – Teste os Padrões

- Motivação / O que é?
- Quem deve agir?
- Testes realizados
- Quem é TOP?
- Apoio



# Programa por uma Internet mais Segura

## Iniciativa

**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
- **Incentivar o crescimento de uma cultura de segurança entre os operadores da rede**





PROGRAMA  
**INTERNET  
+SEGURA**

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



# Programa por uma Internet mais Segura

## Novas ações

### Novo serviço notificado pelo CERT.br a partir de Abr/22

- Serviço DHCPDiscover habilitado (37810/udp)
- **Equipamentos de vídeo podem ser abusados em ataques DDoS**
- Consome recursos da rede e impacta terceiros
- **Pode ter o serviço interrompido se for abusado em ataque DDoS**
- Informações sensíveis armazenadas nos equipamentos podem ser reveladas
- **Deve ser acessível somente a usuários e redes autorizadas que utilizem o serviço**
- Caso seja desnecessário, recomenda-se que seja desativado ou ter acesso limitado
- <https://www.netscout.com/blog/asert/dhcpdiscover-reflectionamplification-ddos-attack-mitigation>
- <https://nsfocusglobal.com/dhdiscover-reflection-attacks-can-magnify-nearly-200-times-of-the-attack-1/>



# Programa por uma Internet mais Segura

## Ação do Registro.br

### Validação do contato de abuso de ASN

- Confirmar que o responsável conhece os procedimentos e políticas do Registro.br/NIC.br e LACNIC sobre administração de recursos
- **Confirmar que o e-mail é monitorado regularmente e são tomadas medidas para atender às reclamações**
- Contribui com a segurança da rede → **Ação 3 do MANRS - Coordenação**
- **Requer que o contato de Abuso dos ASNs sejam validados (responder um e-mail)**
- Passados mais de seis meses sem validação começa ter impacto
- **O titular do ASN fica impedido de administrar recursos no sistema do Registro.br**
- A não validação é uma **violação da política** e pode implicar na inclusão do ASN e blocos IP associados em um processo de recuperação
- <https://registro.br/tecnologia/numeracao/contato-abuso-asn/>





# 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

# 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, que 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/>)

# 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

**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*

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

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

# 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 se serviço!**

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

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

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

# TOP – Teste os Padrões – Relatório



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

Exemplo: Teste TOP *site*, contém uma categoria de teste 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 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**

# 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 – 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



# TOP – Teste os Padrões – Resultados



## Teste TOP - Site

Domínios Únicos	Score 100%	IPv6 100%	DNSSEC 100%	TLS 100%	OPC SEG 100% *	Testes Realizados	Score Null
5.679	208	1.395	1.201	433	0	13.491	8
	4%	25%	21%	8%	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
1679	26	410	206	346	54	4782
	2%	24%	12%	21%	3%	

## Teste TOP - IPv6 e DNSSEC

ASes com medições 100% - IPv6	1.316	Testes Realizados
ASes com medições 100% - DNSSEC	1.040	
ASes com medições 100% - IPv6 + DNSSEC	1.036	
Total de ASes únicos testados	2.790	
		28.289

Ref.: 28/4/22



<https://top.nic.br>

# TOP – Teste os Padrões - Apoio



A CONECTIVIDADE AO SEU ALCANCE



# Obrigado

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

<https://top.nic.br>

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

29 de abril de 2022

**nic.br egi.br**

www.nic.br | www.cgi.br