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

ATUALIZAÇÃO do PROGRAMA / TOP – TESTE OS PADRÕES

Gilberto Zorello | gzorello@nic.br

Evento Nacional ABRINT 2021

São Paulo, SP | 08/12/21

registro.br nic.br cgi.br

Nossa
Agenda

Programa por uma Internet mais Segura

- Iniciativa / Plano de Ação
- Desenvolvimento do Programa

TOP – Teste os Padrões

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

Programa por uma Internet mais Segura
Iniciativa

Lançado pelo CGI.br e NIC.br

- Apoio inicial: Internet Society, Conexis, Abranet e Abrint
- Apoio: RedeTelesul, Abrahosting, InternetSul, Telcomp, 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 INTERNET +SEGURA

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

Programa por uma Internet mais Segura
Plano de Ação

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

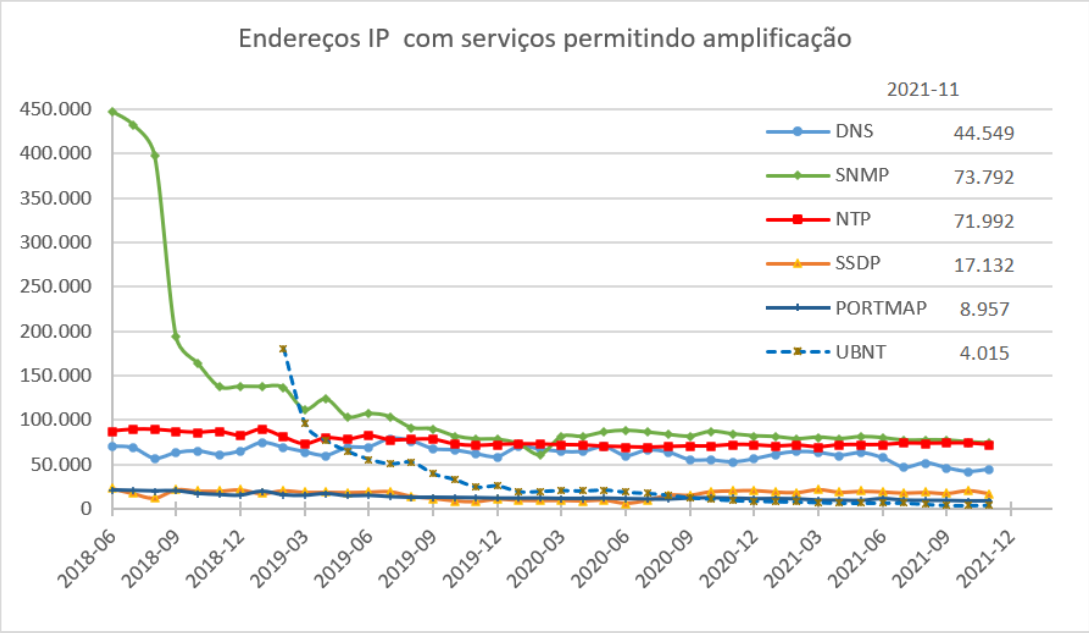
- Transversal no NIC.br: CERT.br, CEPTRO.br, IX.br, Registro.br
- **Conscientização por meio de palestras, cursos e treinamentos**
- Criação de materiais didáticos e boas práticas
- **Interação com Operadores da rede para disseminação da Cultura de Segurança, adoção de Melhores Práticas e Mitigação dos problemas existentes**
- Implementação de filtros de rotas no IX.br, 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

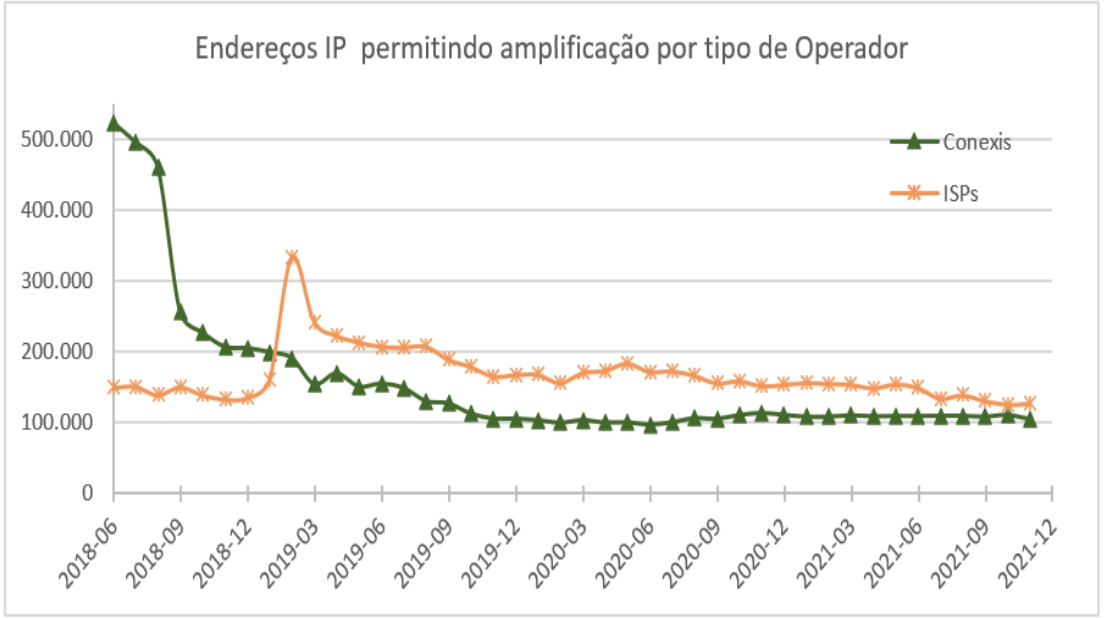
- Reuniões bilaterais bimestrais com as grandes operadoras
- **Em 2021, devido a impossibilidade de participação em eventos presenciais, continuamos com reuniões *on-line* com os responsáveis pelos ASes com maior quantidade de endereços IP notificados**
- Manutenção de contato com os operadores pelo encaminhamento de relatório gerencial mensal para o acompanhamento da resolução dos problemas notificados pelo CERT.br
- **Apoio às grandes operadoras para implantação do RPKI em suas redes**
- 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 Mēris
  - **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

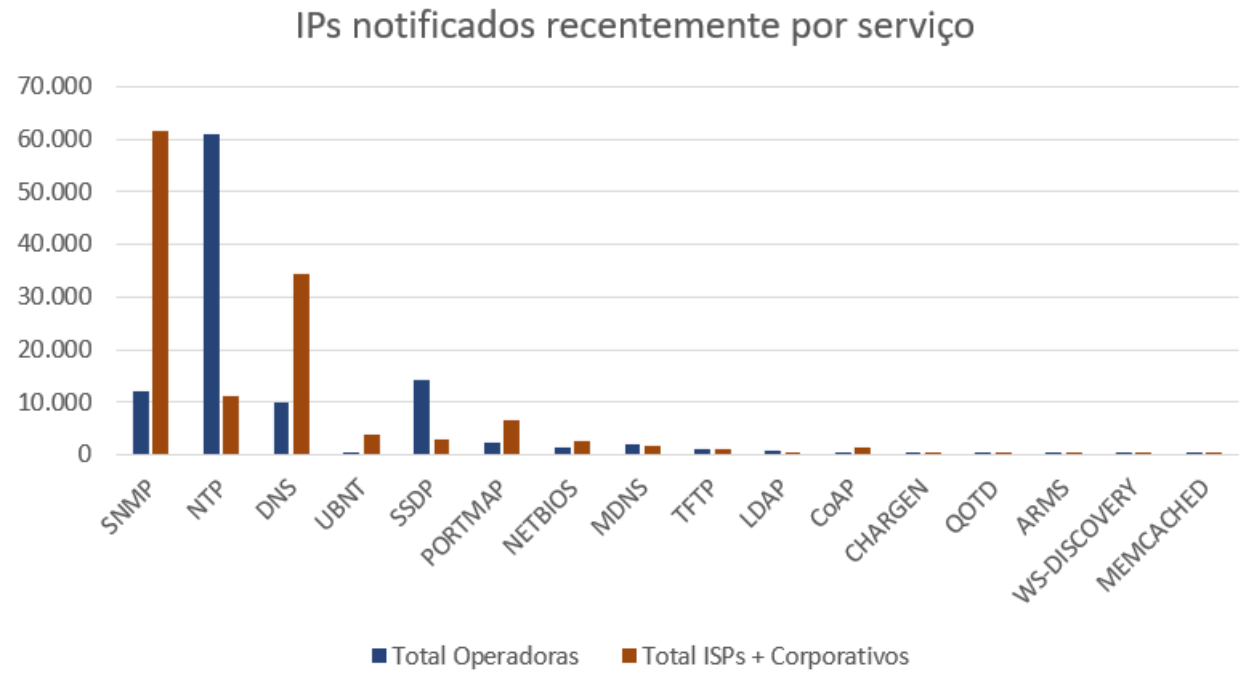


Fonte dos dados: CERT.br

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

MANRS

PROGRAMA INTERNET +SEGURA

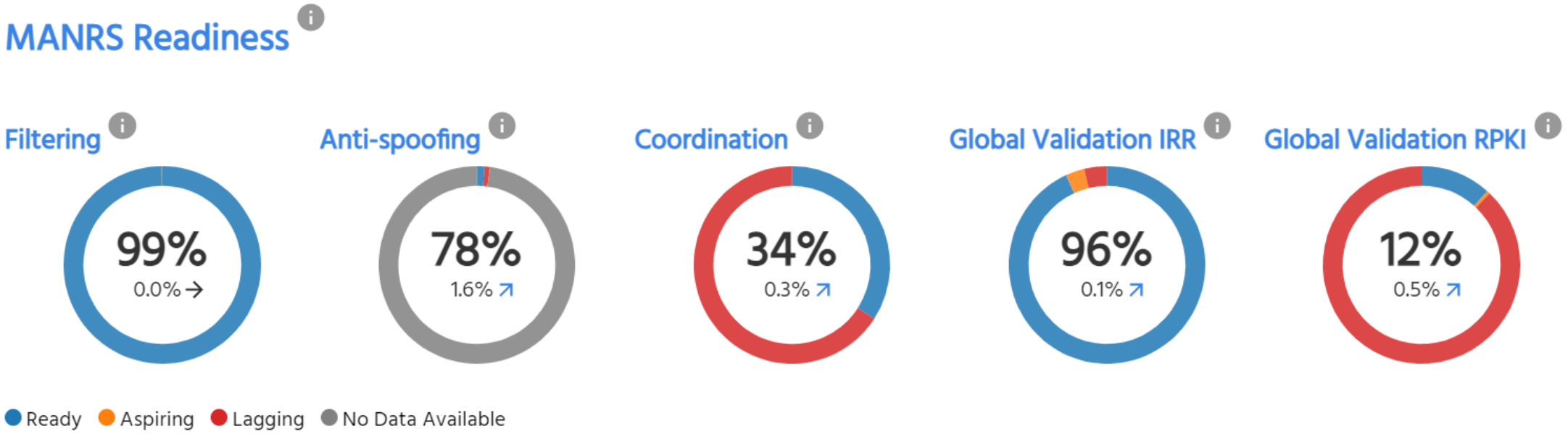
Mutually Agreed Norms for Routing Security

http://manrs.org

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

Programa por uma Internet mais Segura
MANRS Observatory – Readiness – Nov/21

Conjunto de ASes do Brasil

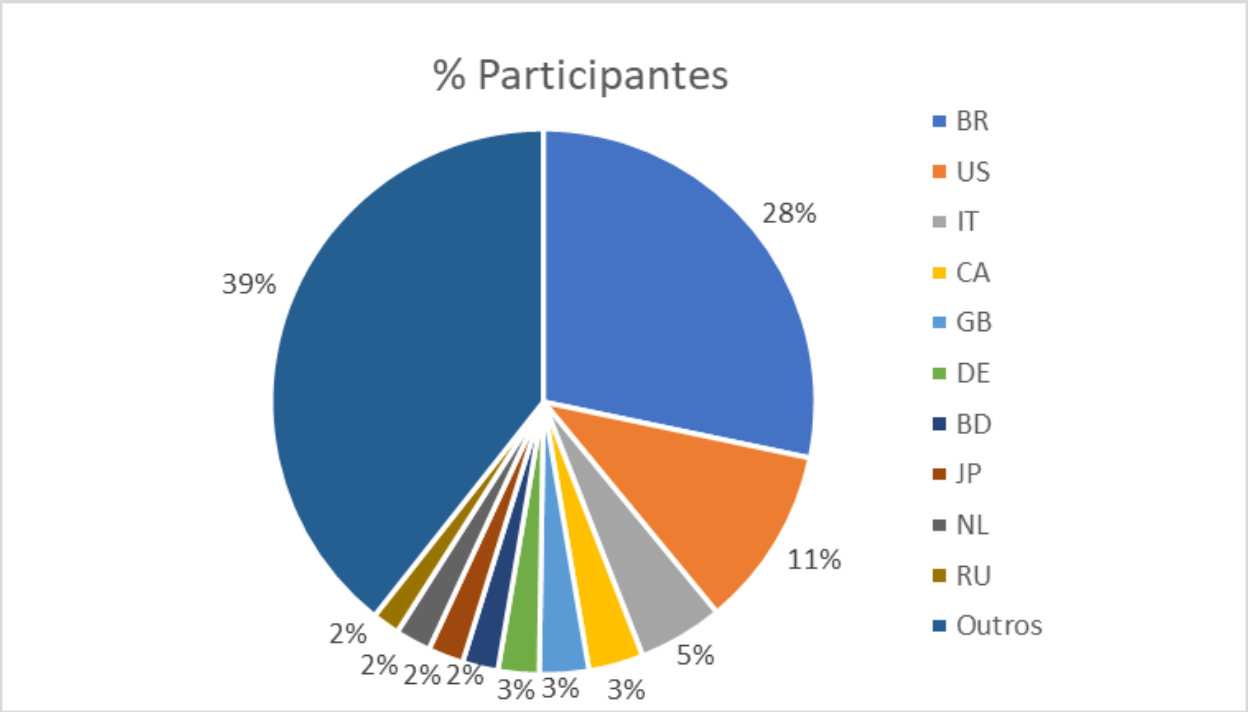


Ação 1	Ação 2	Ação 3	Ação 4	
99% (2020)	74% (2020)	30% (2020)	95% (2020)	6% (2020)

https://observatory.manrs.org/#/overview brazil 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

TOP – Teste os Padrões – Por quê?

A Internet está em constante evolução para poder continuar crescendo e suportando serviços importantes para a sociedade

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 pelos operadores das redes, para reduzir as ameaças 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

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

Adaptado pelo NIC.br tendo 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 para manter nossa Internet confiável

A boa notícia é que estes padrões técnicos modernos 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 se 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 em RFCs de cada categoria de testes e em padrões técnicos operacionais recomendados por entidades internacionais

Referências detalhadas sobre os testes realizados são disponibilizados na ferramenta: 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 a 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, 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

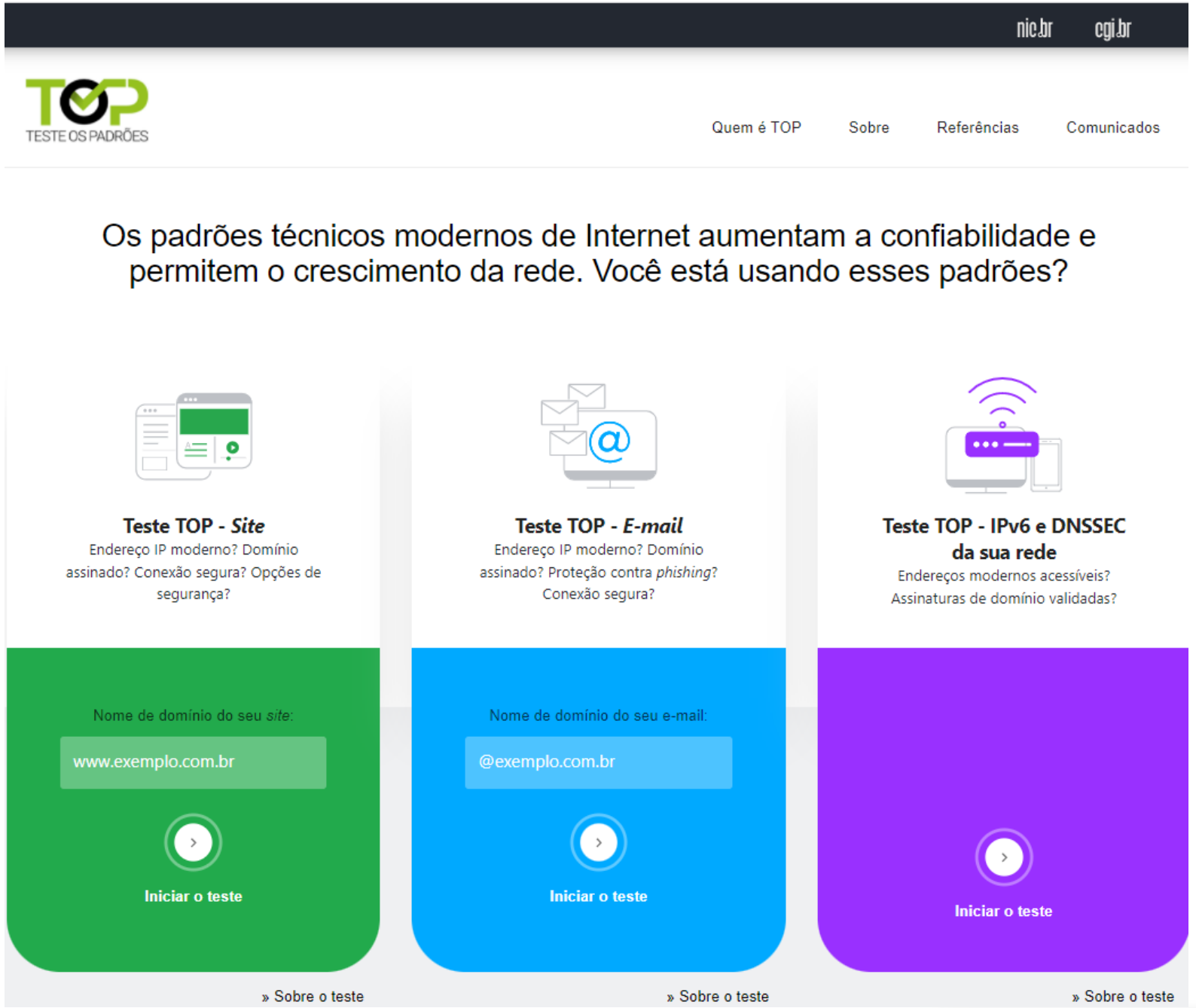
https://top.nic.br

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 hashpara 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


nic.br
cgi.br
TOP
TESTE OS PADRÕES
Quem é TOP
Sobre
Referências
Comunicados
Os padrões técnicos modernos de Internet aumentam a confiabilidade e permitem o crescimento da rede. Você está usando esses padrões?
Teste TOP - Site
Endereço IP moderno? Domínio assinado? Conexão segura? Opções de segurança?
Nome de domínio do seu site:
www.exemplo.com.br
Iniciar o teste
» Sobre o teste
Teste TOP - E-mail
Endereço IP moderno? Domínio assinado? Proteção contra phishing? Conexão segura?
Nome de domínio do seu e-mail:
@exemplo.com.br
Iniciar o teste
» Sobre o teste
Teste TOP - IPv6 e DNSSEC da sua rede
Endereços modernos acessíveis? Assinaturas de domínio validadas?
Iniciar o teste
» Sobre o teste

Teste TOP - *Site*: top.nic.br

TESTE OS PADRÕES

A duração do teste varia entre 5 e 200 segundos.

Você será automaticamente redirecionado para a página de resultados quando todos os testes forem concluídos.

Os itens abaixo estão sendo testados.

Acessível via endereço IP moderno?

Em execução...

Nome de domínio assinado?

Em execução...

Conexão segura?

Em execução...

Opções de segurança de aplicação configuradas?

Em execução...

Teste TOP - *Site*: top.nic.br

TESTE OS PADRÕES

Resultado

Parabéns, seu domínio será adicionado em breve ao **Quem é TOP**!

100%

- **Acessível via endereço IP moderno de Internet (IPv6)**
- **Nome de domínio assinado (DNSSEC)**
- **Conexão suficientemente segura (HTTPS)**
- **Todas as opções de segurança da aplicação estão configuradas (Opções de segurança)**

» **Descrição do relatório de teste**

» ***Link* permanente do resultado do teste (07-12-2021 21:22 -03)**

» **Segundos até a opção de reteste:** 141

Teste TOP - *E-mail*: nic.br

TESTE OS PADRÕES

Resultado

Parabéns, seu domínio será adicionado em breve ao **Quem é TOP**!

100%

- **Acessível via endereço IP moderno de Internet (IPv6)**
- **Todos os nomes de domínio assinados (DNSSEC)**
- **Marcas de autenticidade contra *phishing* por *e-mail* (DMARC, DKIM and SPF)**
- **Conexão de servidor de *e-mail* suficientemente segura (STARTTLS e DANE)**

» **Descrição do relatório de teste**

» ***Link* permanente do resultado do teste (07-12-2021 21:39 -03)**

» **Segundos até a opção de reteste:** 170

Teste TOP - IPv6 e DNSSEC da sua rede

Resultado

50.0%

☺ **Endereços modernos acessíveis (IPv6)**

☹ **Assinaturas de domínio não validadas (DNSSEC)**

» **Descrição do relatório de teste**

Endereços modernos acessíveis (IPv6)

TESTE OS PADRÕES

Muito bem! Seu provedor de Internet lhe fornece um endereço de Internet moderno (**IPv6**), portanto, você pode acessar outros computadores com endereços modernos.

» Mostrar detalhes

- **Conectividade IPv6 do servidor recursivo de DNS**
- **Conectividade IPv6 (via DNS)**
- **Conectividade IPv6 (direta)**
- **Extensões de privacidade para IPv6**
- **Conexão IPv4 (via DNS)**

Endereços modernos acessíveis (IPv6)

Muito bem! Seu provedor de Internet lhe fornece um endereço de Internet moderno (**IPv6**), portanto, você pode acessar outros computadores com endereços modernos.

» Mostrar detalhes

TESTE OS PADRÕES

Conectividade IPv6 do servidor recursivo de DNS

Conectividade IPv6 (via DNS)

Conectividade IPv6 (direta)

Extensões de privacidade para IPv6

Resultado:

Você habilitou as **Extensões de Privacidade para IPv6** ou não está usando SLAAC.

Descrição do teste:

Verificamos se o seu dispositivo usa Extensões de Privacidade IPv6 para SLAAC ou outro processo de configuração IPv6 que não seja SLAAC, a fim de evitar vazamentos do seu endereço MAC potencialmente sensível à privacidade para computadores com os quais se conecta via IPv6.

Conexão IPv4 (via DNS)

TESTE OS PADRÕES

Validação de assinatura de domínio (DNSSEC)

Que pena! As assinaturas de domínio (**DNSSEC**) **não** são validadas para você, portanto, você **não** está protegido contra a tradução manipulada de domínios assinados para endereços IP não autorizados. Solicite a validação do DNSSEC ao seu provedor de Internet e/ou habilite essa validação em seus próprios sistemas.

» Mostrar detalhes

Validação DNSSEC

☹ **Validação DNSSEC**

Resultado:

Você **não** está protegido pela validação da assinatura DNSSEC.

Detalhes técnicos:

Descrição do teste:

Verificamos se os servidores de nomes recursivos que você utiliza validam as assinaturas DNSSEC do nosso nome de domínio. Os servidores são normalmente fornecidos pelo seu provedor de Internet.

Alternativamente, você pode configurar servidores de outro provedor de DNS. Você pode até mesmo usar seu próprio servidor de nome recursivo instalado localmente. Embora a validação seja feita no servidor, a comunicação de volta para o seu dispositivo, denominada como de última milha, poderia ainda ser adulterada por um atacante. Assim, a maneira mais segura é validar perto do dispositivo do usuário final, por exemplo, usando um servidor de nomes recursivo instalado localmente, ou certificar-se de que o canal de comunicação entre o seu servidor e o seu dispositivo de usuário final é seguro/confiável.

Testes IPv6 – Endereçamento moderno?

TESTE OS PADRÕES

Teste TOP – DNSSEC e IPv6 (operadora e provedor de Internet)

- DNS recursivo acessa autoritativo via IPv6, normalmente da operadora / provedor de Internet
- Resolução DNS IPv6
- Acesso direto via IPv6 e IPv4 (opcional)
- Prevenção de vazamento de endereço MAC (**privacidade**)

Teste TOP – *Site* e Teste TOP – *E-mail*

- Dois servidores de nomes IPv6 e se estão acessíveis
- Verifica se os servidores web e *e-mail* tem registro IPv6 nos servidores de nomes e se são acessíveis
- Para servidor web apenas: compara conteúdo web acessível por IPv6 e IPv4

Testes DNSSEC – Resolução DNS Segura?

Teste TOP – DNSSEC e IPv6 (operadora e provedor de Internet)

- Verifica se os servidores recursivos utilizados pelo usuário utilizam assinaturas DNSSEC válidas
- Os servidores recursivos normalmente são disponibilizados pela operadora ou provedor de Internet
- O mais seguro seria utilizar o servidor recursivo localmente ou garantir que o canal deste servidor até o usuário seja seguro

Teste TOP – *Site* e Teste TOP – *E-mail*

- Verifica se o domínio tem assinatura DNSSEC e se é válida
- Assegura o conteúdo do DNS e impede ataques validando os dados e garantindo a origem das informações
- Os remetentes de *e-mail* podem validar a autenticidade das respostas de DNS
- Previne que um atacante redirecione *e-mails* enviados pela manipulação das respostas DNS ou intercepte uma conexão segura com um servidor de *e-mail*

Testes DMARC, DKIM e SPF - Autenticidade?

TESTE OS PADRÕES

Teste TOP – *E-mail*

- **Verifica a existência e a Política de DMARC - Domain-based Message Authentication, Reporting, and Conformance - adotadas para o domínio**
  - Um servidor de recebimento de *e-mail* pode utilizar sua Política de DMARC para tratar *e-mails* que recebe de seu domínio como remetente e que não foram validados pelo **DKIM** e/ou **SPF**
  - Envia relatórios com feedback de autenticação para endereços de *e-mail* especificados na Política de DMARC
  - DMARC requer alinhamento entre os domínios de SPF (MAIL FROM) e de DKIM (d=) com o do corpo do *e-mail* (FROM)
- **Verifica se o domínio suporta registros DKIM - DomainKeys Identified Mail**
  - Um servidor de recebimento de *e-mail* pode usar a chave pública em seu registro DKIM para validar a assinatura de um *e-mail* com um usuário de seu domínio como remetente e determina sua **autenticidade**
- **Verifica se seu domínio tem um registro SPF - Sender Policy Framework**
  - Um servidor de recebimento de *e-mail* pode usar sua relação de servidores de *e-mail* com permissão e a correspondente Política de SPF para determinar a **autenticidade** de um *e-mail* recebido tendo como seu domínio como remetente. Previne abuso de ***phishers*** e ***spammers***.

Testes HTTPS - Confidencialidade/Integridade?

TESTE OS PADRÕES

Teste TOP – *Site*

- **Verifica se o *site* é acessível via HTTPS**
  - O HTTPS garante a **confidencialidade** e **integridade** das informações trocadas e é muito importante para todos *site*
  - Mesmo informações públicas podem ser sensíveis e muito importantes para os usuários
- **Verifica se o servidor web redireciona automaticamente um acesso via HTTP para HTTPS para um mesmo domínio**
- Verifica se o servidor web suporta compressão HTTP, que pode ser utilizado para redução do consumo de banda, porém faz com que uma conexão segura se torne vulnerável a ataques do tipo BREACH - **B**rowser **R**econnaissance & **E**xfiltration via **A**daptive **C**ompression of **H**ypertex (opcional)
- **Verifica se o servidor web suporta HSTS - HTTP Strict Transport Security**
  - O HSTS força um browser se conectar diretamente via HTTPS quando revisita seu *site*. Isto ajuda a evitar ataques MITM - **M**an **I**n **T**he **M**iddle

Testes TLS - Confidencialidade/Integridade?

Teste TOP – *Site* e Teste TOP – *E-mail*

- Verifica se os servidores de recebimento de *e-mail* (MX) oferecem suporte a STARTTLS
- **Verifica a versão de TLS utilizada: Bom: TLS 1.3; Suficiente: TLS 1.2**
- Verifica se os servidores suportam cifras seguras ou suficientemente seguras para: troca de chaves, verificação de certificados, encriptação do conteúdo principal e hashing
- **Verifica se os servidores forçam suas preferências de cifras e se estão de acordo com a ordem preferencial**
- Verifica se os parâmetros públicos usados nas troca de chaves Diffie-Hellman são seguros

Testes TLS - Confidencialidade/Integridade?

TESTE OS PADRÕES

Teste TOP – *Site* e Teste TOP – *E-mail*

- O uso de compressão TLS pode dar ao atacante informações sobre partes secretas da comunicação criptografada, recomenda-se não utilizar compressão TLS
- **Verifica se o seu servidor oferece suporte a Zero Round Trip Time Resumption (0-RTT)**
- Verifica se os servidores suportam funções de hash seguras para criar assinaturas digitais durante a troca de chaves (recomendado)
- **Verifica se o servidor oferece suporte a uma renegociação segura (opcional)**
- Verifica se o servidor web oferece suporte à OCSP stapling (opcional)

Testes Certificados – Autenticidade?

Teste TOP – *Site* e Teste TOP – *E-mail*

- Verifica se é capaz de construir uma cadeia de confiança válida para o certificado do *site* ou servidor de *e-mail* (opcional para *e-mail*)

- **Verifica se a assinatura digital (ECDSA ou RSA) de cada um de seus certificados do *site* ou servidor de *e-mail* utiliza parâmetros seguros**

- Verifica se a assinatura do certificado do *site* foi criada com um algoritmo de hash seguro

- **Verifica se o nome de domínio de seu *site* corresponde ao nome de domínio no certificado.**

Testes Dane – Autenticidade?

Teste TOP – *Site* e Teste TOP – *E-mail*

- Verificamos se os servidores de nomes do domínio do seu *site* ou dos servidores de recebimento de *e-mails* contêm um registro TLSA assinado corretamente para o protocolo DANE (**D**NS-based **A**uthentication of **N**amed **E**ntities)

- **DANE permite que você sejam publicadas informações sobre o certificado de *site* ou servidor de *e-mail* em um registro DNS especial, chamado registro TLSA (TLS Authentication)**

- Clientes, como navegadores web e servidores de envio de *e-mail*, podem verificar a autenticidade do certificado não apenas através da autoridade certificadora, mas também pelo registro TLSA

- **Verificamos se há um esquema ativo com pelo menos dois registros TLSA para DANE para lidar de forma confiável com a substituição de certificados em seus servidores de recebimento de *e-mail* (MX) (opcional para *e-mail*)**

Testes HTTP Security Headers - *Site* Seguro?

TESTE OS PADRÕES

Teste TOP – *Site*

- **Verifica se o servidor web fornece um cabeçalho HTTP para X-Frame-Options que tenha uma política suficientemente segura**
  - Com este cabeçalho HTTP é informado aos navegadores web se deseja permitir que seu *site* seja incluído em frames (framed) ou não. A prevenção de inclusão em frames (framing) defende os visitantes contra ataques como clickjacking (opcional)
- **Verifica se o servidor web fornece um cabeçalho HTTP para X-Content-Type**
  - Com este cabeçalho HTTP é permitido que os navegadores web saibam que eles não devem fazer "MIME type sniffing" e sempre devem seguir o Content-Type conforme declarado pelo seu servidor web (recomendado)

Testes HTTP Security Headers - *Site* Seguro?

TESTE OS PADRÕES

Teste TOP – *Site*

- **Verifica se o servidor web fornece um cabeçalho HTTP para Content-Security-Policy (CSP)**
  - Verifica também várias configurações de CSP (in)seguras, embora não são testadas exaustivamente a eficácia de sua configuração de CSP (recomendado)
- **Verifica se o servidor web fornece um cabeçalho HTTP para Referrer-Policy.**
  - Com este cabeçalho HTTP é informado aos navegadores quais informações de referência, enviadas no cabeçalho Referer, devem fazer parte da solicitação do *site*.
  - O cabeçalho Referer contém o endereço da página anterior, a partir da qual o visitante seguiu um link para a página solicitada (recomendado)

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

Obrigado

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

gzorello@nic.br

08 de dezembro de 2021

nic.br cgi.br

www.nic.br | www.cgi.br