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

TOP – Teste os Padrões

Gilberto Zorello

IX Fórum Sudeste 2022 – Belo Horizonte/MG

26/8/2022

Nossa
Agenda

Programa por uma Internet mais segura

TOP – Teste os Padrões

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

PROGRAMA INTERNET +SEGURA

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

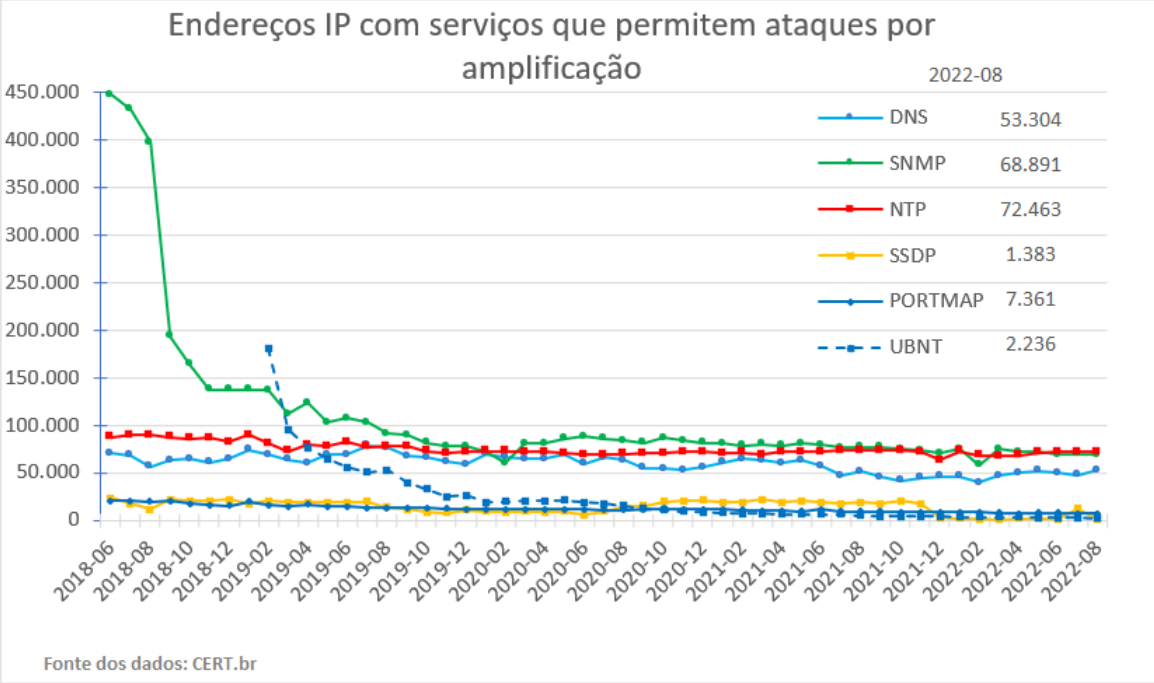
https://bcp.nic.br/i+seg

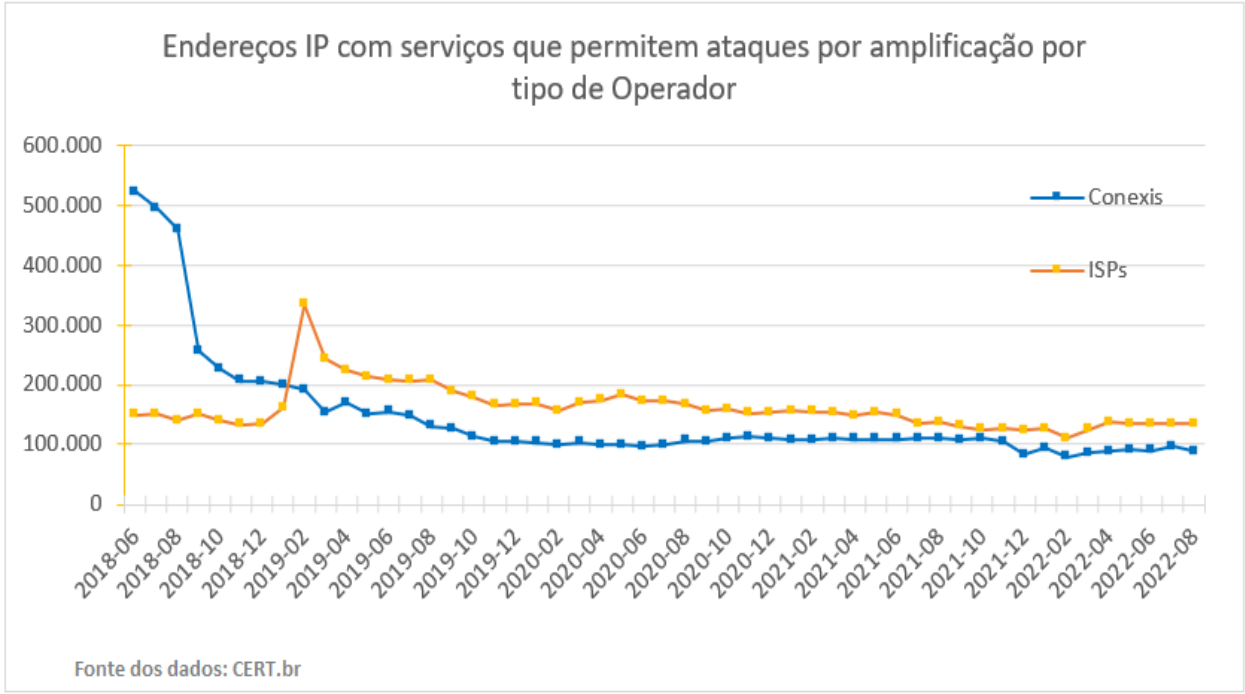
https://bcp.nic.br/i+seg

Programa por uma Internet mais Segura
Notificações contra ataques de amplificação

PROGRAMA INTERNET +SEGURA

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
Notificações contra ataques de amplificação

Quantidade de endereços IP notificados por serviço e por segmento

Programa por uma Internet mais Segura

Configurações de roteamento

MANRS

https://manrs.org

Ações recomendadas

- Prevenir a propagação de informações de roteamento incorretas
  - Filtros BGP
- **Prevenir tráfego com endereço IP de origem falsificado**
  - **Filtros Antispoofing**
- Facilitar comunicação entre os operadores
  - Pontos de contato corretos
- **Divulgar informações de roteamento corretas em escala global**
  - **IRR**
  - **RPKI**

Programa por uma Internet mais Segura

Ferramenta para verificação de configurações

https://top.nic.br

TOP – Teste os Padrões - Motivação

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

Protocolos utilizados na Internet

- Datam das décadas de 70 e 80
- **Desenvolvidos quando o uso da Internet era baixo**
- Não foram desenvolvidos tendo a segurança como pré-requisito
- **Novas versões e protocolos complementares foram desenvolvidos com foco em segurança**

Muitos dos responsáveis pelas configurações os desconhecem e/ou não possuem ferramentas para verificar as configurações

TESTE OS PADRÕES

https://top.nic.br

TOP – Teste os Padrões - Motivação

Os padrões antigos não atendem à escala atual de crescimento da Internet e nem aos requisitos atuais de segurança

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

Devemos utilizar padrões técnicos novos e mais inteligentes para manter a Internet que utilizamos segura e confiável.

A boa notícia é que estes padrões estão disponíveis

TESTE OS PADRÕES

https://top.nic.br

TOP – Teste os Padrões – O que é?

Verifica se os sites, e-mails e conexão à Internet utilizados seguem, os padrões mais modernos e informa o que pode ser feito se não são seguidos.

https://top.nic.br

Foi adaptado pelo NIC.br, tendo como base o código de teste utilizado pelo Internet.nl, que foi desenvolvimento pela holandesa Internet Standards Platform

Outras implementações baseadas no mesmo código de teste:

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

TOP – Teste os Padrões – Quem deve agir?

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

https://top.nic.br

As configurações corretas devem ser implementadas pelos responsáveis pela hospedagem dos serviços **web** e de **e-mail** e pelos **provedores de Internet**

O usuário final também pode executar o teste e solicitar a correção para o seu provedor de serviços!

TOP – Teste os Padrões – Sobre os testes

Testes realizados:

- ***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*

https://top.nic.br

Uma pontuação 100% significa que os serviços estão em conformidade com os padrões modernos de Internet

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

TOP – Teste os Padrões – Relatório

Após o teste ser finalizado é gerado um relatório com os resultados obtidos:

- É fornecida uma nota percentual global
- **Para cada teste é informado:**
  - O que foi verificado
  - **Quais as recomendações e padrões considerados**
  - O resultado dos testes e informações técnicas complementares
  - **O nível de exigência dos testes: Exigido, Recomendado e Opcional**
  - Se o resultado é Bom, Suficiente, Desatualizado ou Insuficiente.

TESTE OS PADRÕES

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 – IPv6

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

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

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)

Exigido **Recomendado** **Opcional**

Testes Realizados – Teste TOP - DNSSEC

Teste TOP - *Site*

Nome de domínio assinado (DNSSEC)
Existência de DNSSEC
Validade de DNSSEC

Teste TOP – *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

Teste TOP – IPv6 e DNSSEC

Validação de assinatura de domínio (DNSSEC)
Validade de DNSSEC

Exigido | Recomendado | Opcional

Testes Realizados – Teste TOP - TLS

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

Teste TOP – *E-mail*

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

Exigido **Recomendado** **Opcional**

Testes Realizados – Teste TOP – Marcas Autenticidade

Teste TOP – *E-mail*

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

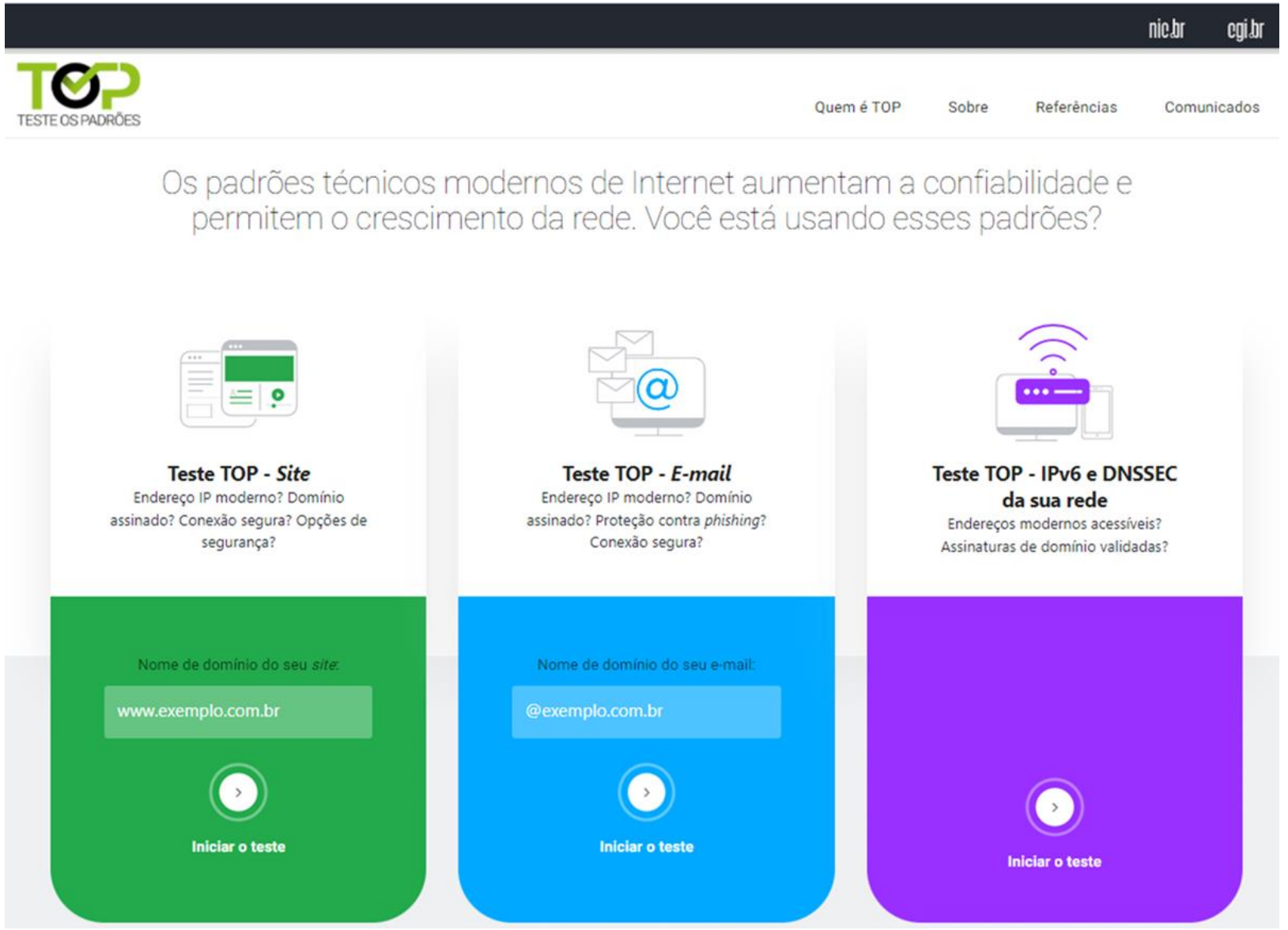
Exigido Recomendado Opcional

Testes Realizados – Teste TOP – Opções de Segurança

Teste TOP - *Site*

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

Exigido | Recomendado | Opcional


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
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
Teste TOP - IPv6 e DNSSEC da sua rede
Endereços modernos acessíveis? Assinaturas de domínio validadas?
Iniciar o teste


nic.br
egi.br
TOP
TESTE OS PADRÕES
Quem é TOP
Sobre
Referências
Comunicados
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)

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)**

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


nic.br
egi.br
TOP
TESTE OS PADRÕES
Quem é TOP
Sobre
Referências
Comunicados
Conectividade IPv6 (direta)
Resultado:
Você é capaz de acessar computadores diretamente em seus endereços IPv6.
Detalhes técnicos:
Endereço IPv6 anonimizado
Nome reverso
Provedor de Internet
2804:14c::
Nenhum(a)
Descrição do teste:
Verificamos se o seu dispositivo, pela sua conexão atual com a Internet, é capaz de conectar-se diretamente, ou seja, sem a tradução de DNS, com nosso servidor web, usando o nosso endereço IPv6 correspondente.
Algumas extensões de navegadores e roteadores oferecem funcionalidade de filtragem de domínio para aumentar a privacidade ou restringir o uso de Internet. Para evitar que esse tipo de filtragem seja contornada, a conexão a endereços IP diretamente muitas vezes é bloqueada, fazendo com que sua conexão à Internet seja reprovada neste subteste.

TOP – Teste os Padrões – Resultados - Geral

Teste TOP - *Site*

Domínios Únicos	Score 100%	IPv6 100%	DNSSEC 100%	TLS 100%	OPC SEG 100% *	Testes Realizados
8.368	261	1.994	1.744	590	0	19.779
	3%	24%	21%	7%	0%	

Teste TOP - *E-mail*

Domínios Únicos com MX	Score 100%	IPv6 100%	DNSSEC 100%	M. Aut. 100%	STARTTLS DANE 100%	Testes Realizados
2470	30	550	273	495	60	6858
	1%	22%	11%	20%	2%	

* Recomendado / Opcional

Ref.: 24/8/22

TOP – Teste os Padrões – Resultados - Geral

Teste TOP – IPv6 e DNSSEC

Cenários IPv6		Qtd / Cenário
I	0%	356
II	20%	414
III	20%	18.657
IV	40%	334
V	60%	9
VI	80%	766
VII	80%	87
VIII	100%	31.691

Cenários DNSSEC		Qtd / Cenário
Válido	100%	30.591
Não válido	0%	21.723

Total de testes realizados	52.314

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.: 22/8/22

Utilize a ferramenta TOP para 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

TOP
TESTE OS PADRÕES

conexis
brasil.digital
A CONECTIVIDADE AO SEU ALCANCE

abranet
Associação Brasileira de Internet

AbraHosting
ASSOCIAÇÃO BRASILEIRA DE EMPRESAS DE INFRAESTRUTURA DE HOSPEDAGEM NA INTERNET

REDETELESUL

abrint

TelComp
Competição para o Futuro Digital

abramulti
Associação brasileira dos operadores de telecomunicações e provedores de internet.

APRONET
Associação Catarinense dos Provedores de Internet

RNP
REDE NACIONAL DE ENSINO E PESQUISA

InternetSul

Obrigado

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

https://top.nic.br

gzorello@nic.br

26 de agosto de 2022

nic.br cgi.br

www.nic.br | www.cgi.br