

nic.br egi.br

cert.br

Workshop CKN

07 de dezembro de 2021

Evento Online

Serviços Prestados à Comunidade

Gestão de Incidentes	Consciência Situacional	Transferência de Conhecimento
<ul style="list-style-type: none"> ▶ Coordenação ▶ Análise Técnica ▶ Suporte à Mitigação e Recuperação 	<ul style="list-style-type: none"> ▶ Aquisição de Dados <ul style="list-style-type: none"> ▶ <i>Honeypots</i> Distribuídos ▶ SpamPots ▶ <i>Threat feeds</i> ▶ Compartilhamento das Informações 	<ul style="list-style-type: none"> ▶ Conscientização <ul style="list-style-type: none"> ▶ Desenvolvimento de Boas Práticas ▶ Cooperação, Eventos e Reuniões (<i>Outreach</i>) ▶ Treinamento ▶ Aconselhamento Técnico e Político

Filiações e Parcerias:



Criação:
Agosto/1996: CGI.br publica o relatório “Rumo à Criação de uma Coordenadoria de Segurança de Redes na Internet Brasil”¹
Junho/1997: CGI.br cria o CERT.br (à época chamado NBSO – *NIC BR Security Office*), com base nas recomendações do relatório²
¹ <https://cert.br/sobre/estudo-cgibr-1996.html> | ² <https://nic.br/pagina/gts/157>

Missão

Aumentar os níveis de segurança e de capacidade de tratamento de incidentes das redes conectadas à Internet no Brasil.

Público Alvo (*Constituency*)

Redes que utilizam recursos administrados pelo NIC.br

- endereços IP ou ASNs alocados ao Brasil
- domínios sob o ccTLD .br

Governança

Mantido pelo **NIC.br** – Núcleo de Informação e Coordenação do .br

- todas as atividades são sustentadas pelo registro de domínios .br

O NIC.br é o **braço executivo do CGI.br** – Comitê Gestor da Internet no Brasil

- entidade multissetorial, coordenada pelo MCTI
- responsável por coordenar e integrar as iniciativas e serviços da Internet no País

<https://cert.br/sobre/>
<https://cert.br/sobre/filiacoes/>
<https://cert.br/about/rfc2350/>

Padrões Modernos para Segurança e Estabilidade dos Serviços

Dra. Cristine Hoepers
Gerente Geral
cristine@cert.br

Dr. Klaus Steding-Jessen
Gerente Técnico
jessen@cert.br

cert.br **nic.br** **egi.br**

Todos Tem um Papel na Segurança: Ecossistema é Complexo e Interdependente



Quase tudo é *software* e está conectado à Internet

Ataques são constantes

- Motivações diversas
- Volume crescente
 - ferramentas facilitam a perpetração por atacantes não especializados

Organizações precisam

- Operar mesmo sob ataque
- Estar preparadas para lidar com estes ataques

Melhora do cenário depende de cada ator fazer sua parte

Precisamos Cuidar da Base Primeiro: Causas Mais Comuns de Invasões e Vazamentos de Dados

Ataques mais reportados e mais observados em sensores do CERT.br:

- Tentativas de fraudes financeiras e de comércio eletrônico
 - via e-mails falsos (phishings)
 - via infecção de roteadores de banda larga (CPEs) para DNS hijacking
 - via infecção de computadores e de celulares
- Invasão por meio de senhas comprometidas, vazadas ou fracas
 - via phishing
 - via força bruta
 - senhas expostas no Github/Pastebin pelos próprios donos/desenvolvedores dos sistemas

Exemplos de serviços afetados:

- e-mails e serviços em nuvem
- acesso remoto (VPN, SSH, RDP, Winbox, etc)
- gestão remota de ativos de rede e servidores

- Exploração de vulnerabilidades para invasão e/ou movimentação lateral
 - falta de aplicação de correções
 - erros de configuração
 - falta / falha de processos

Veja também: Principais Ataques na Internet: Dados do CERT.br

<https://youtu.be/nHh8hHaomFE?t=714>

<https://cert.br/stats/>

Mais de 80% dos incidentes seriam evitados se

- todas as correções (*patches*) fossem aplicadas
- houvesse mais atenção a erros e configurações
- todos os serviços tivessem 2FA / MFA

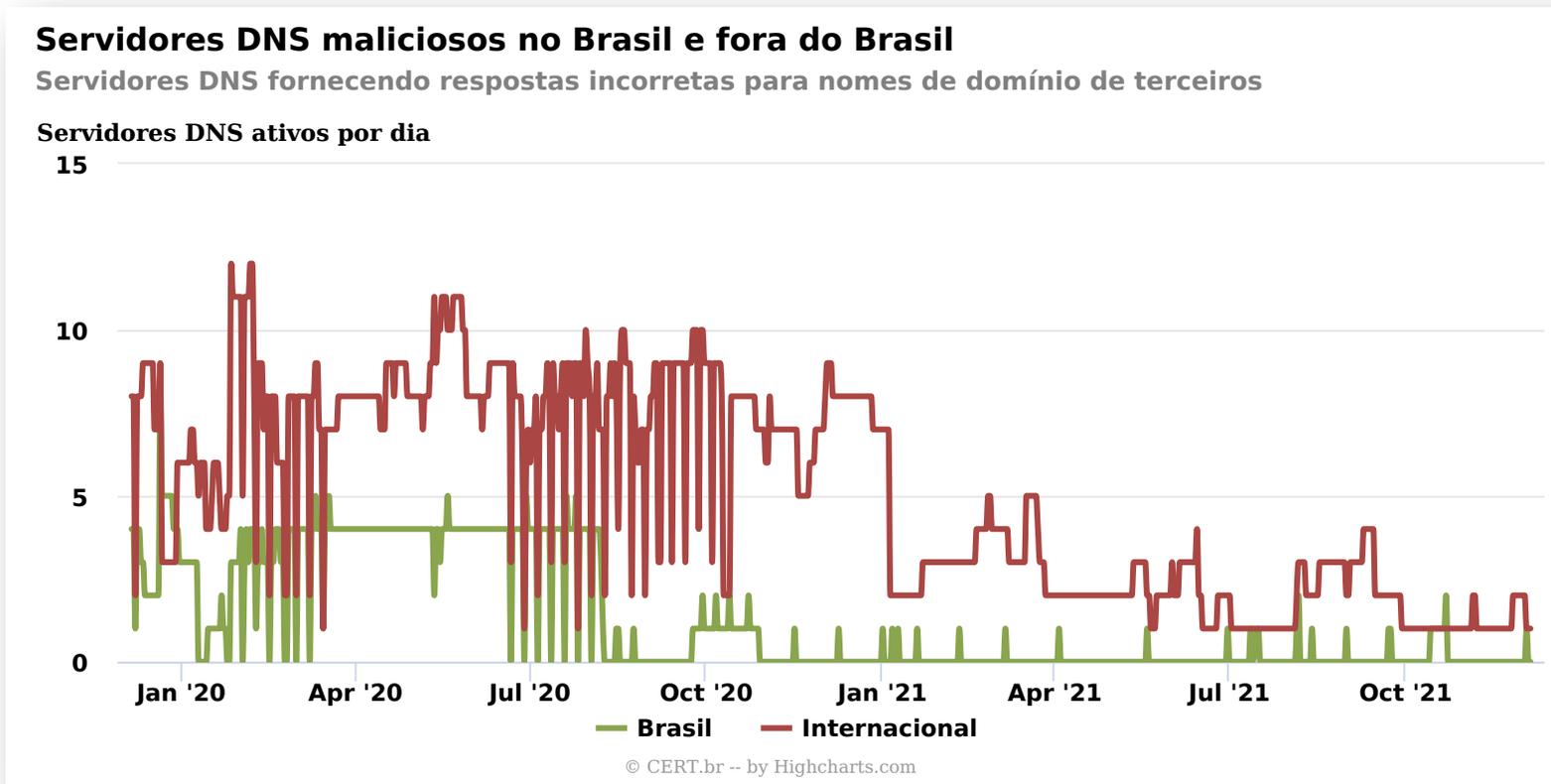
Estudo Setorial Segurança digital: uma análise de gestão de risco em empresas brasileiras

<https://cetic.br/pt/publicacao/seguranca-digital-uma-analise-de-gestao-de-risco-em-empresas-brasileiras/>

Servidores DNS Maliciosos Usados nos CPEs Invadidos: **TLP:WHITE** Fornecem Respostas Autoritativas Erradas

Domínios afetados dos seguintes setores:

- Bancos, Serviços de Pagamento, Serviços de *Streaming*, Mobilidade, Redes Sociais, *Webmail*, Comércio Eletrônico, entre outros



Semântica é importante ao reportar incidentes ou pedir takedown!

- Isto **não é** um DNS invadido
- Isto **não é** envenenamento (*cache poisoning*)
- Isto **não é** sequestro de domínio (*domain hijacking*)

Isto é um **servidor DNS malicioso** (*rogue*) sendo usado para **sequestro de DNS** (*DNS hijacking*)

- autoritativo para os domínios das vítimas
- recursivo aberto respondendo ao restante das consultas

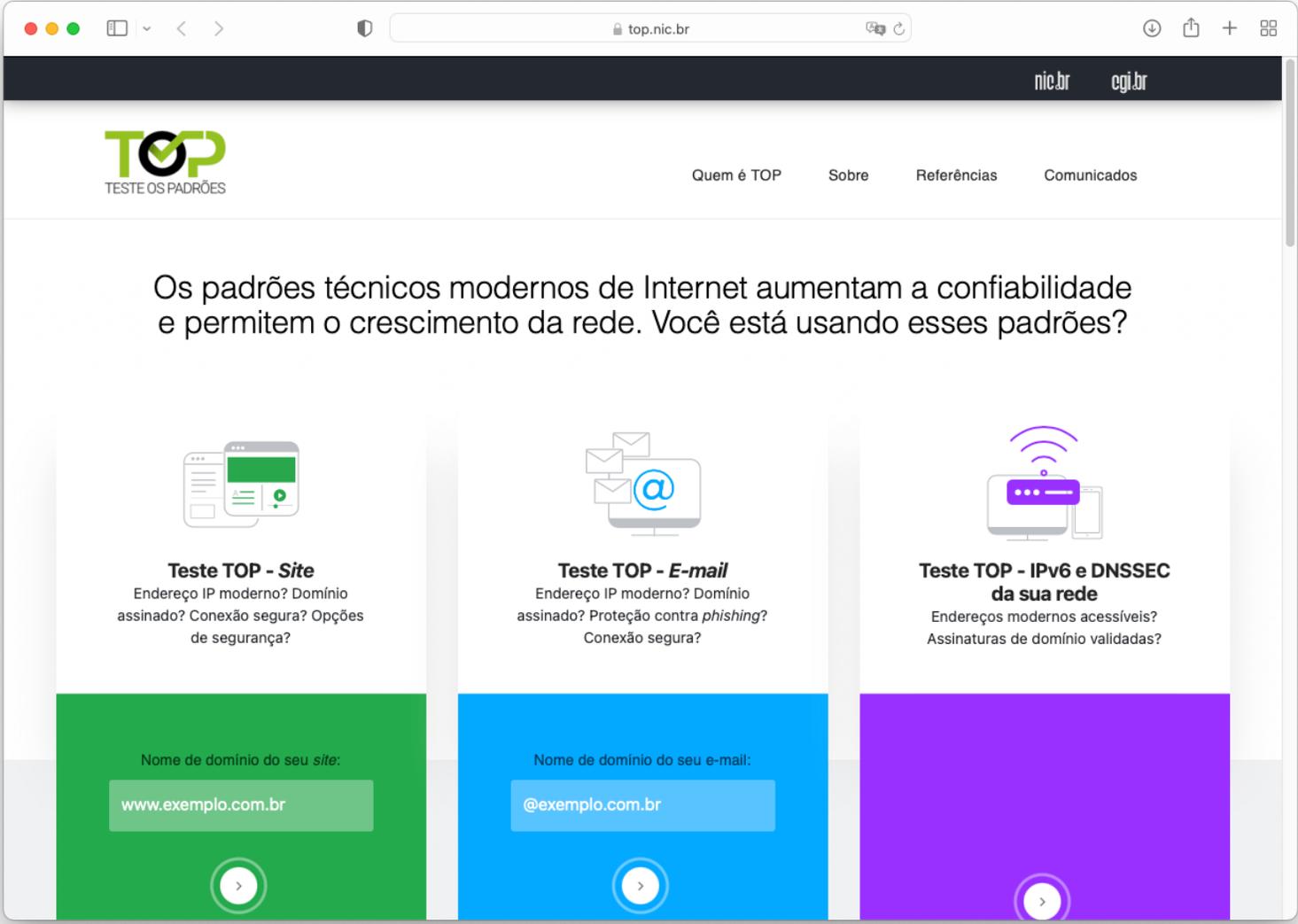
Fonte: <https://cert.br/stats/dns-malicioso/>

Padrões Modernos que Aumentam a Segurança

	Padrões	Vantagens da Adoção
Autenticação com Múltiplos Fatores	Tokens <ul style="list-style-type: none"> • em <i>hardware</i> (FIDO2/U2F) • em <i>software</i> (HOTP/TOTP) 	Impede sucesso de força bruta de senhas Reduz impacto do comprometimento de credenciais
Criptografia forte	HTTPS mandatório e HSTS Versões atuais de TLS <i>Forward Secrecy</i>	Garantia das transações e da proteção de dados Reduz a chance de quebra da criptografia Impede quebra de cripto de tráfego antigo capturado
Segurança de DNS	DNSSEC	Proteção contra envenenamento de <i>cache</i> Habilitar o uso de outras tecnologias como o DANE
Segurança de <i>e-mail</i>	STARTTLS <ul style="list-style-type: none"> • idealmente c/ DANE DMARC, DKIM e SPF	Proteção contra <i>sniffing</i> (“espionagem”) Aumento da reputação da mensagem legítima (ajuda a prevenir <i>phishing</i> da sua marca)
Protocolo IP	IPv6 é o atual IPv4 é legado – e já acabou <ul style="list-style-type: none"> • novas redes só terão IPv6 • redes móveis já tem IPv6 nativo 	Mais estabilidade e menor complexidade <ul style="list-style-type: none"> • Não depender de CGN ou tradução v6 → v4 • Não depender de transição, reduz superfície de ataques Facilita o processo investigativo e de tratamento de incidentes
Segurança de roteamento	RPKI	Certificação de recursos Validação de origem no BGP

	Padrões	Vantagens da Adoção
Autenticação com Múltiplos Fatores	Tokens <ul style="list-style-type: none"> • em <i>hardware</i> (FIDO2/U2F) • em <i>software</i> (HOTP/TOTP) 	Impede sucesso de força bruta de senhas Reduz impacto do comprometimento de credenciais
Criptografia forte	HTTPS mandatório e HSTS Versões atuais de TLS <i>Forward Secrecy</i>	Garantia das transações e da proteção de dados Reduz a chance de quebra da criptografia Impede quebra de cripto de tráfego antigo capturado
Segurança de DNS	DNSSEC	Proteção contra envenenamento de <i>cache</i> Habilitar o uso de outras tecnologias como o DANE
Segurança de <i>e-mail</i>	STARTTLS <ul style="list-style-type: none"> • idealmente c/ DANE DMARC, DKIM e SPF	Proteção contra <i>sniffing</i> (“espionagem”) Aumento da reputação da mensagem legítima (ajuda a prevenir <i>phishing</i> da sua marca)
Protocolo IP	IPv6 é o atual IPv4 é legado – e já acabou <ul style="list-style-type: none"> • novas redes só terão IPv6 • redes móveis já tem IPv6 nativo 	Mais estabilidade e menor complexidade <ul style="list-style-type: none"> • Não depender de CGN ou tradução v6 → v4 • Não depender de transição, reduz superfície de ataques Facilita o processo investigativo e de tratamento de incidentes
Segurança de roteamento	RPKI	Certificação de recursos Validação de origem no BGP

https://top.nic.br/ Testes para *site*, *e-mail* e conectividade



Testes

- verificam a correta implementação dos padrões
- baseiam-se
 - nas especificações das RFCs
 - em padrões técnicos operacionais recomendados por entidades internacionais

Relatório

- detalhamento de todos os resultados
- referências detalhadas dos padrões
- indicações sobre como corrigir possíveis problemas

Apoiadores



Outros *Sites* para Auxiliar nos Testes e Configurações

cert.br nic.br egi.br

SSL Configuration Generator

TLP:WHITE

<https://ssl-config.mozilla.org/>

The screenshot shows the Mozilla SSL Configuration Generator web application. The browser address bar displays "ssl-config.mozilla.org". The page features the Mozilla logo and the title "SSL Configuration Generator". The interface is divided into three main sections: "Server Software", "Mozilla Configuration", and "Environment".

Server Software

- Apache
- AWS ALB
- AWS ELB
- Caddy
- Dovecot
- Exim
- Go
- HAProxy
- Jetty
- lighttpd

Mozilla Configuration

- Modern
Services with clients that support TLS 1.3 and don't need backward compatibility
- Intermediate
General-purpose servers with a variety of clients, recommended for almost all systems
- Old
Compatible with a number of very old clients, and should be used only as a last resort

Environment

Server Version: 2.4.41

OpenSSL Version: 1.1.1k

Miscellaneous

- HTTP Strict Transport Security
This also redirects to HTTPS, if possible
- OCSP Stapling

SSL Server Test

TLP:WHITE

<https://www.ssllabs.com/ssltest/>

Qualys. SSL Labs

Home Projects Qualys Free Trial Contact

You are here: [Home](#) > [Projects](#) > SSL Server Test

SSL Server Test

This free online service performs a deep analysis of the configuration of any SSL web server on the public Internet. **Please note that the information you submit here is used only to provide you the service. We don't use the domain names or the test results, and we never will.**

Hostname:

Do not show the results on the boards

[Recently Seen](#) [Recent Best](#) [Recent Worst](#)

RPKI TEST – A RIPE Labs experiment

TLP:WHITE

<https://sg-pub.ripe.net/jasper/rpki-web-test/>



RPKI TEST

a RIPE Labs **experiment** in collaboration with Job Snijders/NTT

testing valid ROA...
testing invalid ROA (5sec)... [passed]



RPKI TEST

a RIPE Labs **experiment** in collaboration with Job Snijders/NTT

testing valid ROA... [error (what does that mean?)]! [failed]!
testing invalid ROA (5sec)...
The RPKI test could not complete

Referências dos Padrões Citados

Padrões	Referências
Tokens em <i>hardware</i> (FIDO2/U2F)	https://fidoalliance.org/specifications/
Tokens em <i>software</i> (HOTP/TOTP)	https://tools.ietf.org/html/rfc4226 https://tools.ietf.org/html/rfc6238
HTTPS mandatório e HSTS Versões atuais de TLS <i>Forward Secrecy</i>	https://www.ssllabs.com/ssltest/ https://ssl-config.mozilla.org https://observatory.mozilla.org
DNSSEC	https://registro.br/tecnologia/dnssec/dnssec-para-provedores/ https://ftp.registro.br/pub/doc/tutorial-dnssec.pdf https://dnsviz.net
STARTTLS [idealmente c/ DANE] DMARC, DKIM e SPF	https://starttls-everywhere.org https://english.ncsc.nl/publications/factsheets/2019/juni/01/factsheet-secure-the-connections-of-mail-servers https://meca.jrc.ec.europa.eu/en/technical#starttls https://havedane.net https://dmarc.org https://dmarc.globalcyberalliance.org
IPv6	https://ipv6.br https://test-ipv6.com
RPKI	https://bcp.nic.br/rpki https://sg-pub.ripe.net/jasper/rpki-web-test/

Outras Iniciativas para uma Internet mais Segura

cert.br nic.br egi.br

Precisamos um Ecossistema mais Saudável: Programa por uma Internet mais Segura

TLP:WHITE

Objetivo principal:

- Reduzir o número de sistemas que possam ser abusados para gerar ataques DDoS

Incentivo à adoção de boas práticas:

- *Hardening*
- Segurança de roteamento (MANRS)
- *Anti-spoofing* (BCP 38)
- Reduzir serviços abertos que permitam amplificação

Iniciativa conjunta:

- ISOC, NIC.br, SindiTelebrasil, Abranet, Abrint, Abinee



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

Conscientização: Portal InternetSegura.br



The screenshot shows a web browser window with the URL `internetsegura.br`. The page header includes the `nic.br` logo, the `INTERNET SEGURA BR` logo, and navigation links for `Sobre`, `Outras iniciativas`, and `Como Pedir Ajuda`. The main heading reads: **Internet Segura – Faça sua parte e todos teremos uma Internet mais segura!**

Below the heading are six categories, each with an illustration and a label:

- para Crianças**: Illustration of two children, a boy and a girl.
- para Adolescentes**: Illustration of two young adults, a man and a woman.
- para Pais e Educadores**: Illustration of a woman and a man, both holding briefcases.
- para 60+**: Illustration of an elderly couple.
- para Técnicos**: Illustration of a man in a yellow shirt and blue pants, standing next to a server rack.
- para Interesse Geral**: Illustration of a diverse group of people of various ages and ethnicities.

Cartilha de Segurança para Internet: Fascículos e *Slides* para Palestras e Treinamento

Conteúdo disponível *online* gratuitamente sob Licença *Creative Commons*

- **Fascículos** que cobrem assuntos específicos relacionados com segurança na Internet
 - **Slides** sobre cada um dos temas, que podem ser utilizados, por exemplo, para dar aulas ou palestras de conscientização
 - Dica do dia no *site*, via *Twitter* e RSS
 - Impressões em pequena escala enviadas a escolas e centros de inclusão digital
 - Possível gerar versões personalizadas com logo da instituição
- Exemplos de parceiros de impressão e distribuição:
Itaipu, Eletronuclear, ELO, Microsoft, Procergs e Metrô SP

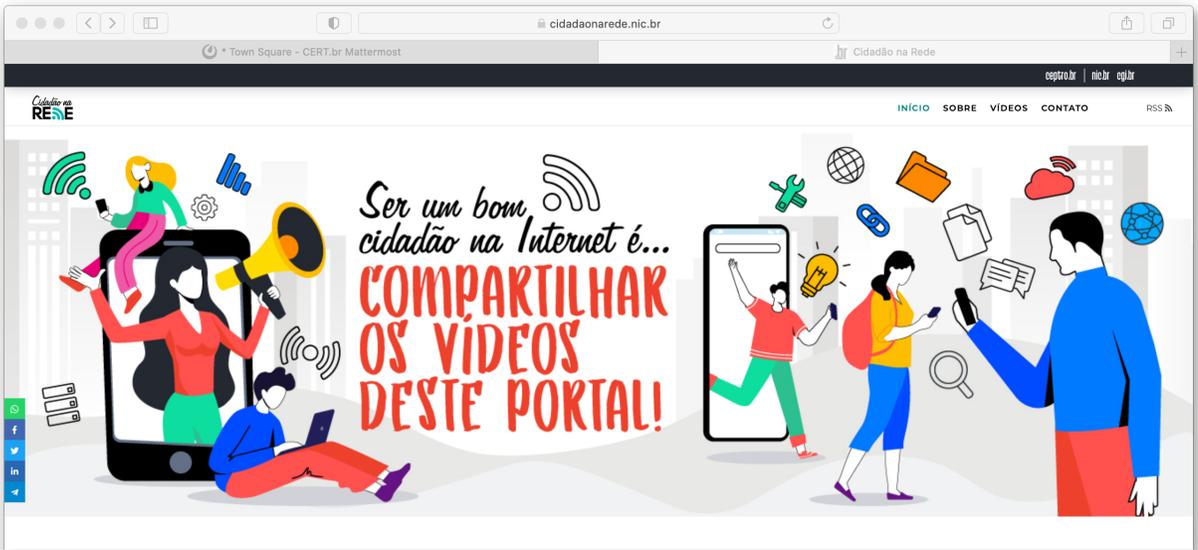


<https://cartilha.cert.br/>

Projeto Cidadão na Rede

“É direito e dever de cada pessoa ser um bom cidadão, e isso também vale para o mundo digital, usando de forma responsável as Tecnologias de Informação e Comunicação, em particular a Internet.”

- Conduzido pelo Ceptro.br
- Vídeos curtos sobre diversos temas:
 - Segurança
 - Infraestrutura da Internet e redes
 - Uso responsável e deveres na Internet



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

SEGURANÇA

Verifique se o site é SEGURO

Navegação segura
Tome cuidado com os sites que acessa! Será que eles são seguros? Entenda como identificar isso e navegar com segurança!

Postado em 22/10/2020

Se você não precisa ter uma SUPER memória!

Gerenciador de senhas
Cada novo cadastro é mais uma senha para decorar! Quantas senhas uma pessoa comum consegue guardar na memória? Gerenciadores de senha estão aí para ajudar a administrar todas as senhas de maneira segura.

Postado em 22/10/2020

Verificação em duas etapas protege ainda + suas contas

Verificação em dois fatores
Usar mais de um fator de segurança pode fazer a diferença na hora em que pessoas mal intencionadas tentarem invadir sua conta. Proteja suas contas!

Postado em 22/10/2020

Não arrisque seus dados

Senhas Variadas
Na hora de criar uma nova senha sempre vem aquela vontade de usar uma das que você já utiliza, não é? Isso pode ser muito perigoso!

Postado em 22/10/2020

VAI CRIAR UMA SENHA?

Senhas Seguras
Existem diversas práticas importantes para criar uma senha mais segura. Este vídeo mostra uma delas. Aprenda a proteger seus dados, criando boas senhas.

Postado em 22/10/2020

INFRAESTRUTURA DA INTERNET E REDES

A sua Internet pode ter CABELO

Minha Internet parou... E agora?
Existem diversos motivos para sua Internet não estar funcionando. Mas, em alguns casos, basta reiniciar o roteador para a conexão voltar. Tente isso antes de ligar para o suporte técnico.

Postado em 12/11/2020

Vídeos consomem muita "Internet"

Vídeos consomem muita banda Internet
Quando várias pessoas usam a Internet na mesma casa, a qualidade da rede para todos pode ficar comprometida. Isso acontece porque a quantidade de banda de Internet contratada pode não ser suficiente para atender a demanda.

Postado em 12/11/2020

Existem repetidores Wi-Fi

Repetidores WiFi
Os roteadores WiFi possuem algumas limitações, uma delas é o alcance do sinal. Existem equipamentos simples para melhorar isso.

Postado em 12/11/2020

SINAL RUIM EM CASA?

Sinal WiFi
Sabia que existem maneiras simples de melhorar o sinal do seu WiFi e com isso também melhorar a qualidade da sua navegação na Internet?

Postado em 12/11/2020

USO RESPONSÁVEL E DEVERES NA INTERNET

Nem tudo é brincadeira

Cyberbullying: e se fosse com você?
Não se deixe enganar, nem toda piada feita às custas de outra pessoa pode soar como uma simples brincadeira. O que pode parecer inocente ou muito engraçado para alguém, pode ter um impacto extremamente negativo no outro. Bullying ou Cyberbullying pode trazer consequências sérias.

Postado em 22/10/2020

A lei protege seus direitos também na Internet

Comprei on-line e me arrependi! O que fazer?
Fez uma compra on-line e se arrependeu, o que fazer? O Código de Defesa do Consumidor garante alguns direitos especiais para compras feitas fora do estabelecimento comercial, por exemplo, via internet.

Postado em 22/10/2020

PODE SER UM ... BOATO

Boatos
A Internet está repleta de notícias, mas será que todas são verdadeiras? Cuidado ao compartilhar! E na dúvida, não compartilhe!

Postado em 22/10/2020

Obrigado

@ cristine@cert.br

@ jessen@cert.br

@ notificações para: cert@cert.br

@ @certbr

<https://cert.br/>

nic.br cgi.br

www.nic.br | www.cgi.br