

nic.br egi.br

cert.br

WTRio 2022 - Workshop de Tecnologias de Redes POP-RJ/RNP

22 de setembro de 2022

Rio de Janeiro - RJ

Serviços Prestados à Comunidade

Gestão de Incidentes

- ▶ Coordenação
- ▶ Análise Técnica
- ▶ Suporte à Mitigação e Recuperação

Consciência Situacional

- ▶ Aquisição de Dados
 - ▶ *Honeypots* Distribuídos
 - ▶ SpamPots
 - ▶ *Threat feeds*
- ▶ Compartilhamento das Informações

Transferência de Conhecimento

- ▶ Conscientização
 - ▶ Desenvolvimento de Boas Práticas
 - ▶ Cooperação, Eventos e Reuniões (*Outreach*)
- ▶ Treinamento
- ▶ Aconselhamento Técnico e de Políticas

Filiações e Parcerias:



SEI
Partner
Network



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

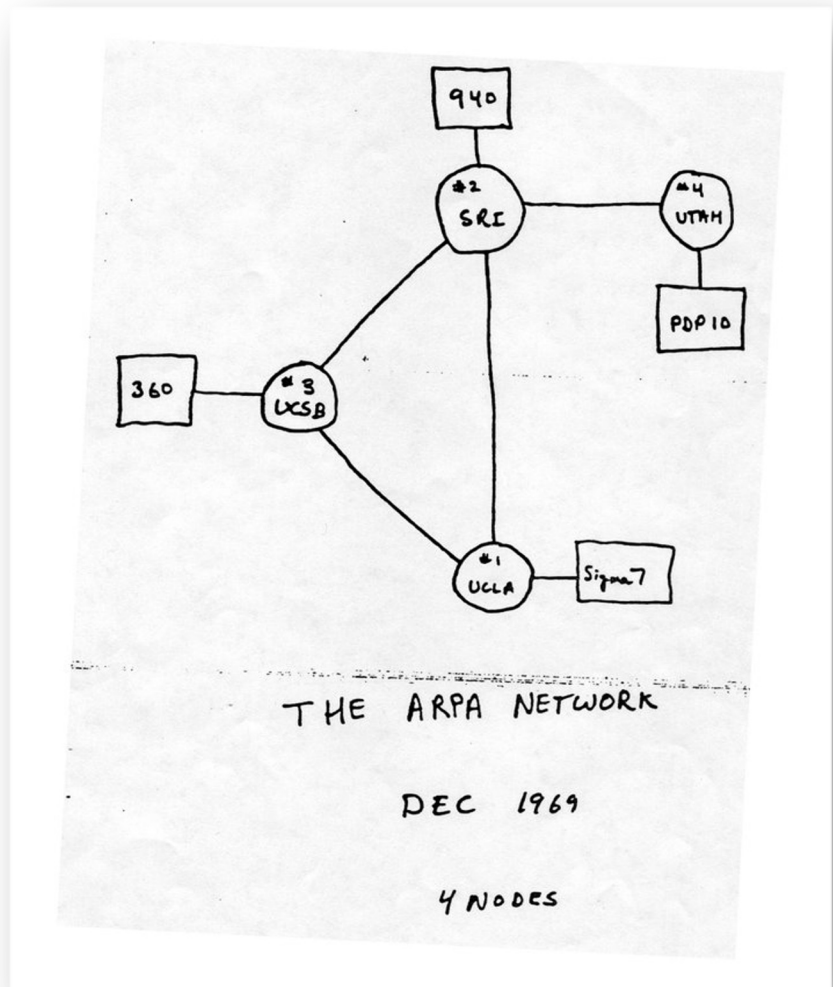
<https://cert.br/sobre/>
<https://cert.br/sobre/filiacoes/>
<https://cert.br/about/rfc2350/>

Importância de Padrões Modernos para a Segurança e Proteção de Dados

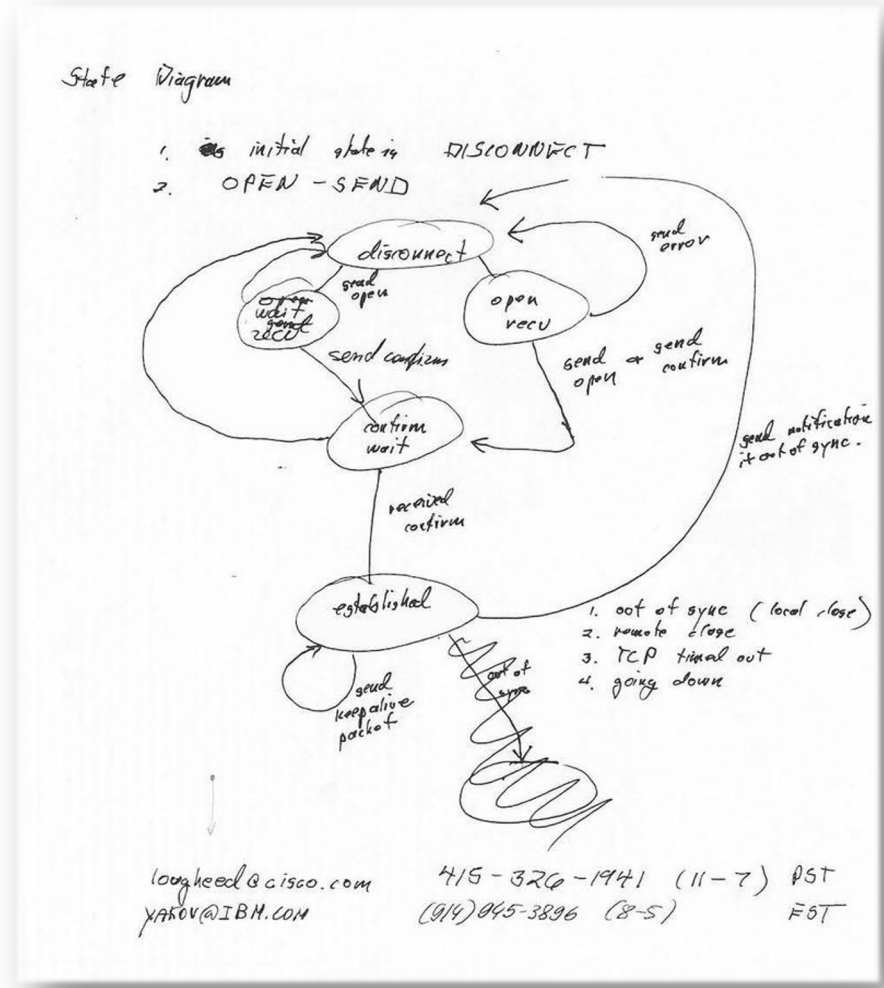
Dra. Cristine Hoepers
Gerente CERT.br/NIC.br
cristine@cert.br

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

Segurança Não Era Parte do Projeto



<https://twitter.com/darpa/status/1013047020326739969>



<https://computerhistory.org/blog/the-two-napkin-protocol/>

olhardigital.com.br

MENU **OLHAR DIGITAL** 🔍

STJ se restabelece após ransomware; PF investiga cópia de dados

Renato Santino | 13/11/2020 21h45, atualizada em 13/11/2020 21h50

infomoney.com.br

InfoMoney 🔍

O "lado B" da digitalização

Fleury é o mais recente episódio de ransomware; veja como os ataques cibernéticos têm afetado os mercados

Vistos como algumas das maiores ameaças da era atual, sequestros de dados, ou ransomware, viram novo risco a ser monitorado no mercado

www1.folha.uol.com.br

JBS pagou US\$ 11 mi em resposta a ataque ransomware em operações na América do Norte

Empresa cancelou turnos em fábricas nos EUA e Canadá na semana passada, após ser afetada por ciberataque

9.jun.2021 às 21h26

REUTERS A JBS USA, subsidiária da brasileira JBS nos Estados Unidos, confirmou em comunicado divulgado nesta quarta-feira (9) que pagou o equivalente a US\$ 11 milhões (R\$ 55,5 milhões) em resposta [a um ataque hacker](#) contra suas operações

poder360.com.br

PODER 360 Diretor Fernando Rodrigues 🔍

Renner diz não ter pago resgate de dados depois de ataque hacker

A varejista sofreu uma invasão na última 5ª feira (19.ago.2021), mas informou que principais bancos de dados estão preservados

Compartilhe



Divulgação/Renner



Photographer: Samuel Corum/Bloomberg

Cybersecurity

Hackers Breached Colonial Pipeline Using Compromised Password

By [William Turton](#) and [Kartikay Mehrotra](#)
June 4, 2021, 4:58 PM GMT-3

- ▶ Investigators suspect hackers got password from dark web leak
- ▶ Colonial CEO hopes U.S. goes after criminal hackers abroad

<https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password>

SolarWinds – Ataque atribuído à Rússia pelos EUA

Causas: senha vazada + exploração de vulnerabilidades

SolarWinds FTP credentials were leaking on GitHub

in November 2019 Featured

3 Shares Share Tweet 3

By Sam Varghese

More details are emerging about poor security at SolarWinds, following the compromise of its Orion network management software that was then used to effect attacks on many companies in a number of regions around the globe.

A researcher from India had advised SolarWinds in November 2019 that he had found a public GitHub repository which was leaking the company's FTP credentials.

Downloads Url: <http://downloads.solarwinds.com>
FTP Url: <ftp://solarwinds.upload.akamai.com>
Username:
Password:
POC: <http://downloads.solarwinds.com/test.txt>

I was able to upload a test POC.
Via this any hacker could upload malicious exe and update it with release SolarWinds product.

bounty hunter, said in a tweet: "Was bragging SolarWinds. Hmmm, how that d was *****123 Rolling on the floor

- <https://www.itwire.com/security/solarwinds-ftp-credentials-were-leaking-on-github-in-november-2019.html>
- <https://threatpost.com/solarwinds-default-password-access-sales/162327/>
- <https://us-cert.cisa.gov/remediating-apt-compromised-networks>

Alert (AA22-117A)

[More Alerts](#)

2021 Top Routinely Exploited Vulnerabilities

Original release date: April 27, 2022

[Print](#)
[Tweet](#)
[Send](#)
[Share](#)

Summary

This joint Cybersecurity Advisory (CSA) was coauthored by cybersec Canada, New Zealand, and the United Kingdom: the Cybersecurity and Security Agency (NSA), Federal Bureau of Investigation (FBI), Australian Centre for Cyber Security (CCCS), New Zealand National Cyber Security Centre (NCSC-NZ), and the United Kingdom National Cyber Security Centre (NCSC-UK). This advisory provides details on Exposures (CVEs) routinely exploited by malicious cyber actors in 2021.

Table 1: Top 15 Routinely Exploited Vulnerabilities in 2021

CVE	Vulnerability Name	Vendor and Product	Type
CVE-2021-44228	Log4Shell	Apache Log4j	Remote code execution (RCE)
CVE-2021-40539		Zoho ManageEngine AD SelfService Plus	RCE
CVE-2021-34523	ProxyShell	Microsoft Exchange Server	Elevation of privilege
CVE-2021-34473	ProxyShell	Microsoft Exchange Server	RCE
CVE-2021-31207	ProxyShell	Microsoft Exchange Server	Security feature bypass
CVE-2021-27065	ProxyLogon	Microsoft Exchange Server	RCE
CVE-2021-26858	ProxyLogon	Microsoft Exchange Server	RCE
CVE-2021-26857	ProxyLogon	Microsoft Exchange Server	RCE
CVE-2021-26855	ProxyLogon	Microsoft Exchange Server	RCE
CVE-2021-26084		Atlassian Confluence Server and Data Center	Arbitrary code execution
CVE-2021-21972		VMware vSphere Client	RCE
CVE-2020-1472	ZeroLogon	Microsoft Netlogon Remote Protocol (MS-NRPC)	Elevation of privilege
CVE-2020-0688		Microsoft Exchange Server	RCE
CVE-2019-11510		Pulse Secure Pulse Connect Secure	Arbitrary file reading
CVE-2018-13379		Fortinet FortiOS and FortiProxy	Path traversal

<https://www.cisa.gov/uscert/ncas/alerts/aa22-117a>

Infraestruturas Críticas e Órgãos Governamentais Alvos de Ataques

DigiNotar Certificate Authority Breach Crashes e-Government in the Netherlands

> A taste of what is to routinely come?

BY ROBERT N. CHARETTE | 09 SEP 2011 | 7 MIN READ |

Inside 'Operation Black Tulip': DigiNotar hack analysed

CA systems falsely told Iranians they were secure

John Leyden

Tue 6 Sep 2011

28



The Google webmail of as many as 300,000 Iranians may have been intercepted using fraudulently issued security certificates made after a hack against Dutch certificate authority outfit DigiNotar, according to the preliminary findings of an official report into the megahack.

Fox-IT, the security consultancy hired to examine the breach against DigiNotar, reveals that DigiNotar was hacked on or around 6 June – a month before hackers begun publishing rogue certificates.

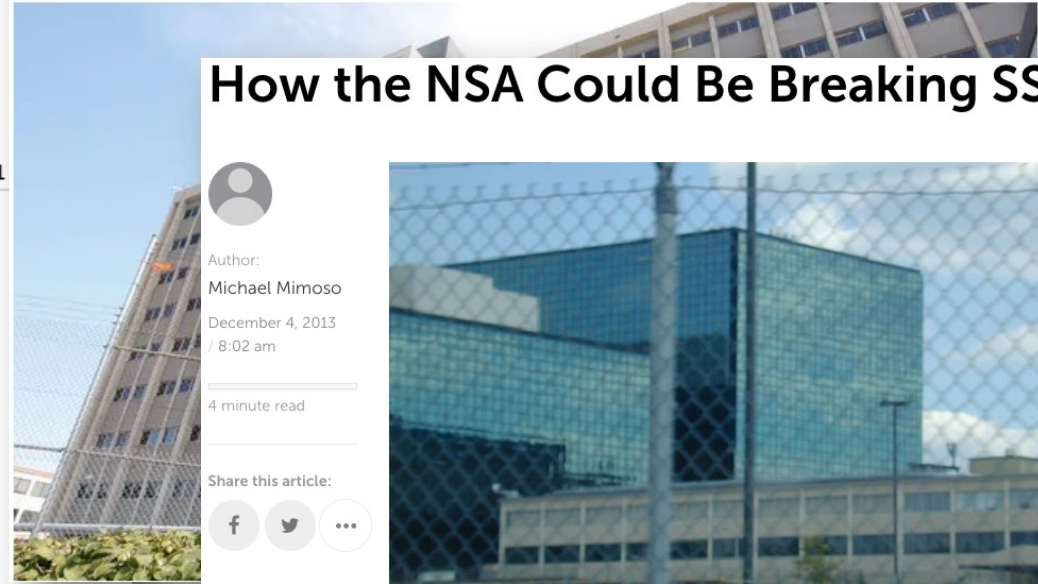
Between 10 July and 20 July hackers used compromised access to DigiNotar's systems to issue rogue 531 SSL certificate for Google and other domains, including Skype, Mozilla add-ons, Microsoft update and others. DigiNotar only began revoking

- <https://spectrum.ieee.org/diginotar-certificate-authority-breach-crashes-egovernment-in-the-netherlands>
- https://www.theregister.com/2011/09/06/diginotar_audit_damning_fail/
- <https://www.usatoday.com/story/news/world/2013/07/07/brazil-concern-nsa-spying-snowden/2497161/>
- <https://threatpost.com/how-the-nsa-could-be-breaking-ssl/103091/>

Brazil expresses concern at report of NSA spying

AP

Published 5:17 p.m. ET July 7, 2013 | Updated 7:19 p.m. ET July 7, 2013



How the NSA Could Be Breaking SSL



Author: Michael Mimoso

December 4, 2013 8:02 am

4 minute read

Share this article:



How is the NSA beating or breaking SSL? Cryptographer Matthew Green lays out a number of possibilities.

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

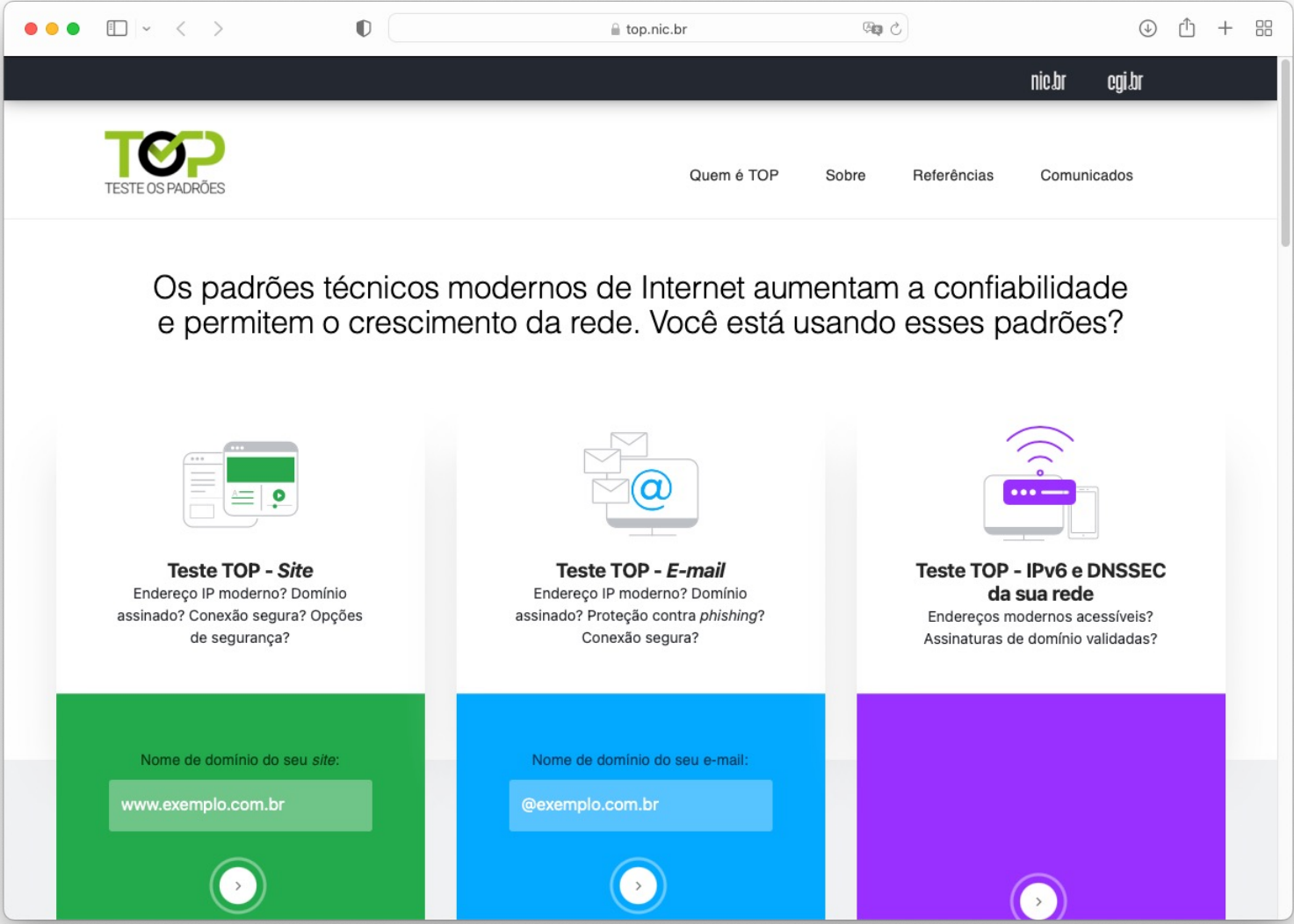
<https://cetic.br/pt/publicacao/seguranca-digital-uma-analise-de-gestao-de-risco-em-empresas-brasileiras/>

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 e-mail	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

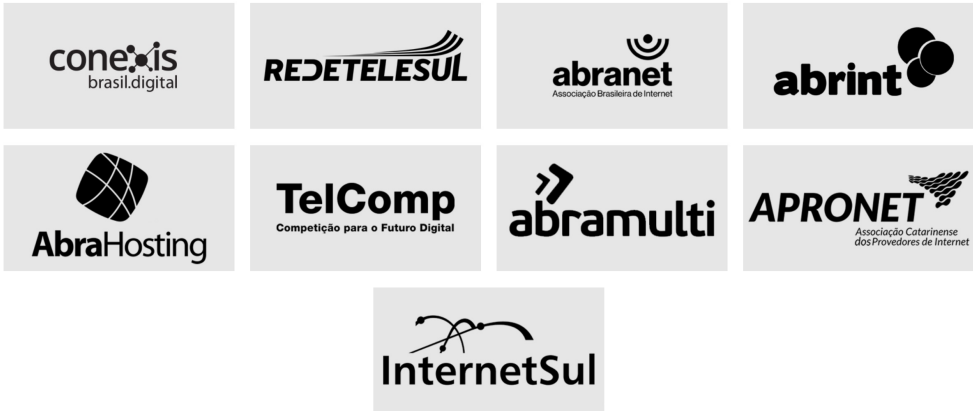


Testes

- 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



Outros *Sites* para Auxiliar nos Testes e Configurações

cert.br nic.br egi.br

SSL Configuration Generator

TLP:CLEAR

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

The screenshot shows the Mozilla SSL Configuration Generator interface. At the top left is the Mozilla logo. The main heading is "SSL Configuration Generator". Below this, there are three main sections: "Server Software", "Mozilla Configuration", and "Environment".

Server Software

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

MySQL

nginx

Oracle HTTP

Postfix

PostgreSQL

ProFTPD

Redis

Tomcat

Traefik

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

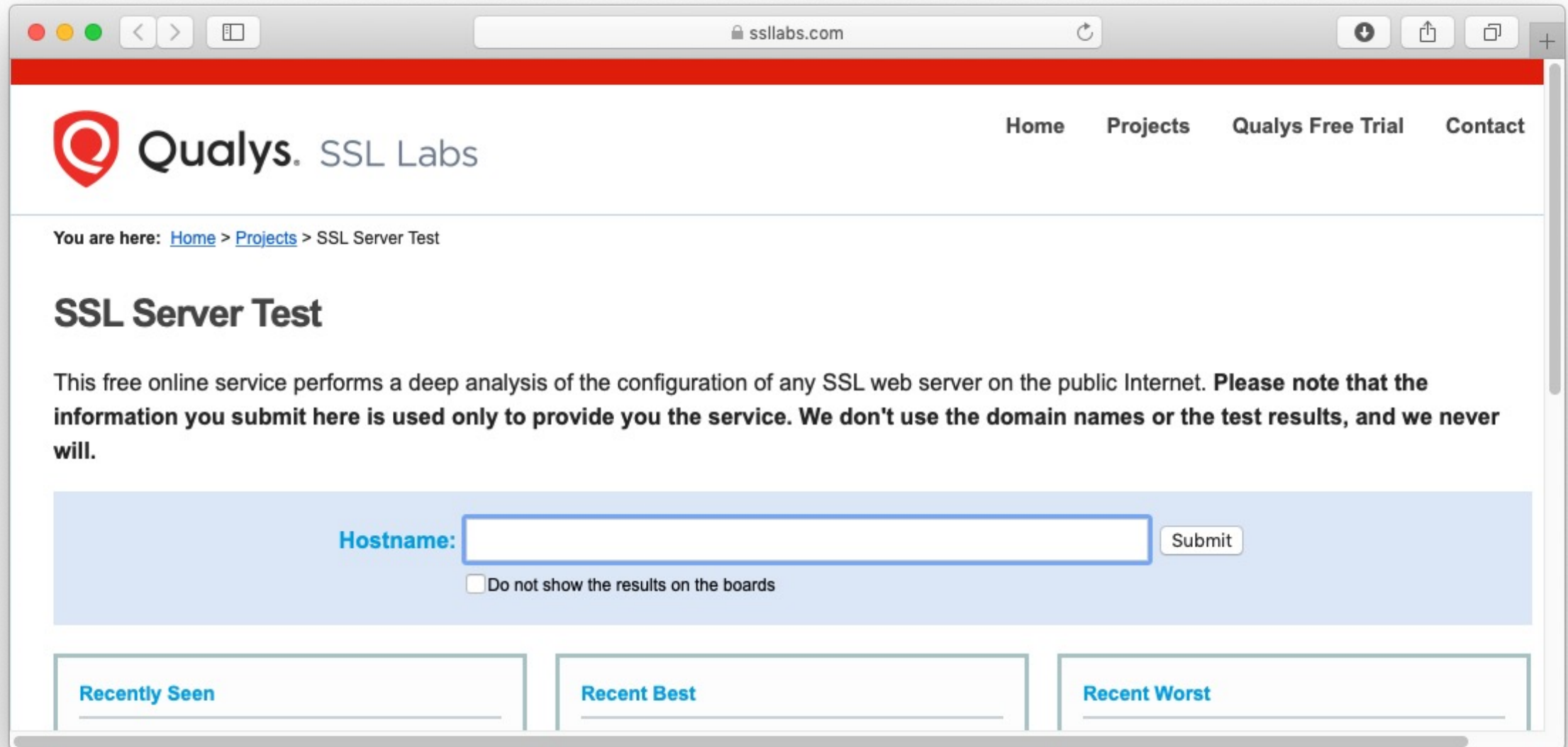
Miscellaneous

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

SSL Server Test

TLP:CLEAR

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



The screenshot shows a web browser window with the URL [ssllabs.com](https://www.ssllabs.com). The page features the Qualys SSL Labs logo and navigation links for Home, Projects, Qualys Free Trial, and Contact. A breadcrumb trail indicates the current location: Home > Projects > SSL Server Test. The main heading is "SSL Server Test". Below this, a paragraph explains the service: "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." The form area has a light blue background and contains a "Hostname:" label, a text input field, and a "Submit" button. Below the input field is a checkbox labeled "Do not show the results on the boards". At the bottom of the form area, there are three tabs: "Recently Seen", "Recent Best", and "Recent Worst".

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](#)

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



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, Conexis, Abranet, Abrint, InternetSul, RedeTelesul, Telcomp

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



Conscientização: Portal InternetSegura.br

TLP:CLEAR



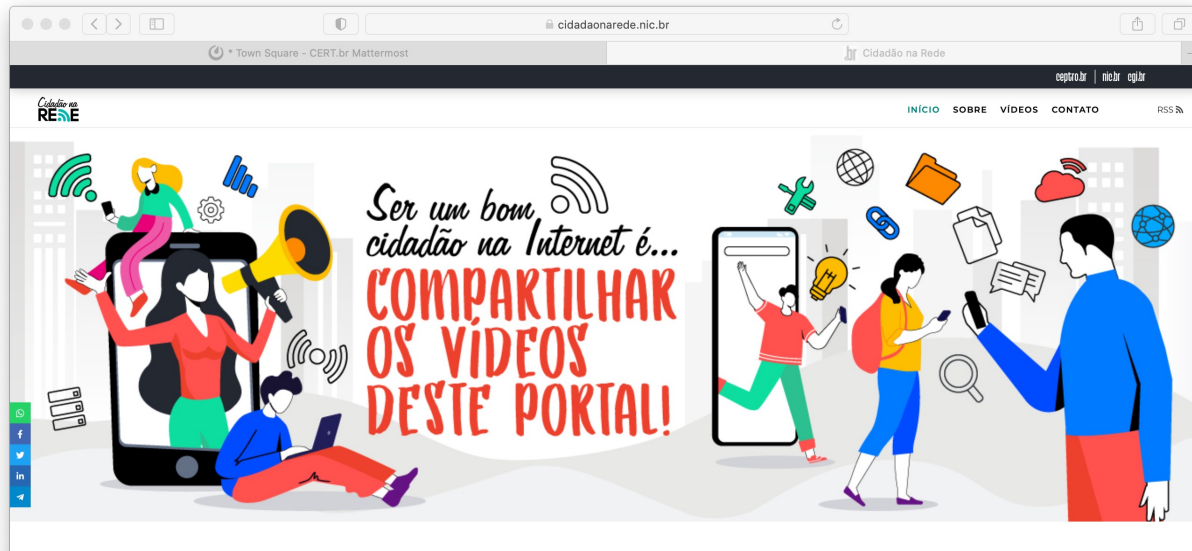
The screenshot shows a web browser window with the URL `internetsegura.br`. The page header includes the `nic.br` logo, the `INTERNET SEGURA BR` logo, and navigation links for `Sobre`, `Outras iniciativas`, and `Como Pedir Ajuda`. The main heading reads: `Internet Segura – Faça sua parte e todos teremos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

Below the heading, there are six categories represented by illustrations and text:

- `para Crianças`: Illustration of two children.
- `para Adolescentes`: Illustration of two young adults.
- `para Pais e Educadores`: Illustration of a woman and a man.
- `para 60+`: Illustration of an elderly couple.
- `para Técnicos`: Illustration of a person in a lab coat next to server racks.
- `para Interesse Geral`: Illustration of a diverse group of people.

Projeto Cidadão na Rede

- Vídeos curtos sobre diversos temas:
 - Segurança
 - Infraestrutura da Internet e redes
 - Uso responsável e deveres na Internet
- Seja um apoiador
 - Tenha os vídeos com seu logo
 - Todo o processo via o portal



<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 cabo

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 do provedor.

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 ser insuficiente 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

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/>

Novo Material: Furto de Celular

SEU CELULAR É SUA CARTEIRA: CUIDE DA SUA VIDA DIGITAL



Toda praticidade que o celular traz pode rapidamente se tornar um pesadelo se ele cair nas mãos erradas.

O **Fascículo Furto de Celular** mostra como se preparar para reduzir os danos e traz dicas sobre o que fazer se um furto ocorrer.

<https://cartilha.cert.br/fasciculos/#furto-de-celular>

Obrigada

✉ cristine@cert.br

✉ notificações para: cert@cert.br

📧 @certbr

<https://cert.br/>

nic.br cgi.br

www.nic.br | www.cgi.br