

# NIC.br e CERT.br

## Responsabilidades e Atividades

**Demi Getschko**  
Diretor Presidente, NIC.br  
demi@nic.br

**Frederico Neves**  
Diretor de Serviços e de Tecnologia, NIC.br  
fneves@registro.br

**Cristine Hoepers**  
Gerente, CERT.br/NIC.br  
cristine@cert.br

**Klaus Steding-Jessen**  
Gerente Técnico, CERT.br/NIC.br  
jessen@cert.br

cert.br nic.br egi.br

# Núcleo de Informação e Coordenação do Ponto BR – NIC.br

Pessoa jurídica de direito privado, sem fins lucrativos, criada para implementar as decisões e os projetos do Comitê Gestor da Internet no Brasil - CGI.br.

Dentre suas atribuições estão:

- o registro e manutenção dos nomes de domínios que usam o <.br> , e a distribuição de números de Sistema Autônomo (ASN) e endereços IPv4 e IPv6 no País, por meio do Registro.br;
- atender aos requisitos de segurança e emergências na Internet Brasileira em articulação e cooperação com as entidades e os órgãos responsáveis, atividades do CERT.br;
- projetos que apoiem ou aperfeiçoem a infraestrutura de redes no País, como a interconexão direta entre redes (IX.br) e a distribuição da Hora Legal brasileira (NTP.br). Esses projetos estão a cargo do Ceptro.br;
- promover estudos e recomendar procedimentos, normas e padrões técnicos e operacionais, para a segurança das redes e serviços de Internet, bem assim para a sua crescente e adequada utilização pela sociedade.

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

<https://nic.br/estatuto-nic-br/>

membros e ex-membros do CGI.br  
(somente os atuais membros têm direito a voto) ➔

## ASSEMBLEIA GERAL

7 membros eleitos pela Assembleia Geral ➔

**CONSELHO DE ADMINISTRAÇÃO**

**CONSELHO FISCAL**

ADMINISTRAÇÃO  
.....  
JURÍDICO  
.....  
COMUNICAÇÃO  
.....  
ASSESSORIAS:  
CGI.br e PRESIDÊNCIA

**DIRETORIA EXECUTIVA**

- 1
- 2
- 3
- 4
- 5

- 1 Diretor presidente
- 2 Diretor administrativo e financeiro
- 3 Diretor de serviços e tecnologia
- 4 Diretor de projetos especiais e de desenvolvimento
- 5 Diretor de assessoria às atividades do CGI.br

**registro.br**

Domínios

**cert.br**

Segurança

**cetic.br**

Indicadores

**ceptro.br**

Redes e Operações

**ceweb.br**

Tecnologias Web

**ix.br**

Troca de Tráfego

**W3C**  
Brasil

Padrões Web

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

# Internet no Brasil em Números

## Números de Sistemas Autônomos (ASNs)

**8964** ASNs

- 2º país no mundo (1º EUA)
- 70% dos ASNs da América Latina e Caribe

AS: rede com uma política de roteamento única, com blocos de endereços IP próprios

Fonte:

<https://www.lacnic.net/en/web/lacnic/estadisticas-asignacion>

<https://pulse.internetsociety.org/blog/where-are-the-internet-networks>

## Provedores de Acesso (ISPs)

**12.826** ISPs (estimado)

- 46% possuem ASN

Fonte:

<https://www.cetic.br/pt/pesquisa/provedores/indicadores/>

Dados atualizados em 24 de agosto de 2022

## Domínios sob o ccTLD <.br>

**4.996.262** domínios registrados

- 1.500.681 possuem DNSSEC

Fonte:

<https://registro.br/dominio/estatisticas/>

## Interconexão de Tráfego

IX.br SP é maior *Internet eXchange* do mundo

- **2.349** participantes
- **17.37**Tbps de pico de tráfego
- **9.83**Tbps de média de tráfego

Fonte:

<https://ix.br/trafego/agregado/sp>

# Objetivos do NIC.br:

## Fomentar uma Internet Estável e Resiliente no Brasil

### Robustez e qualidade da Infraestrutura

- Segurança e resiliência dos serviços de DNS
  - possibilidade de DNSSEC desde 2007
  - manutenção de espelhos dos servidores-raiz
- Aumento da eficiência e redução de custos com a manutenção do IX.br e do OpenCDN
  - pontos de interconexão do IX.br em regiões metropolitanas
  - estímulo para mais organizações possuírem AS próprio
  - compartilhamento de infraestrutura no OpenCDN, diminuindo a distância entre o conteúdo e seus usuários

### Métricas relevantes e confiáveis para orientar políticas públicas

- Medição da qualidade da banda larga e de outros serviços, via o Projeto SIMET conduzido pelo Ceptro.br
- Indicadores sobre o uso das TICs e da Internet, atividade do Cetic.br, um Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação, sob os auspícios da UNESCO

### Perenidade e estabilidade dos serviços

- Equipes altamente qualificadas e com pouca rotatividade
  - se reflete na continuidade de projetos e qualidade das entregas
  - viabiliza criação de relações de confiança dentro e fora do País
  - composição: mais de 100 profissionais das áreas de Ciências de Computação e Engenharias, boa parte com Mestrado ou Doutorado

### Parcerias internacionais com instituições correlatas

- Mais de 40 parceiros, entre eles
  - LAC-IX e EURO-IX
  - ICANN, APNIC, LACNIC e RIPE
  - CIRA, DENIC, KRNIC, NETNOD, NIC.AR, NIC.AT, NIC.CL, NIC.CZ e NLNETLabs

### Segurança e tratamento de incidentes

- Contato nacional de último recurso para aqueles que não tenham estrutura própria e fomento para iniciativas de segurança e tratamento de incidentes, atividades do CERT.br

# Histórico:

## Criação do CERT.br

1995: o pleno do CGI.br solicitou a especialistas uma análise sobre a situação nacional de segurança, e uma proposta para uma estrutura de coordenação

Agosto/1996: o relatório “Rumo à Criação de uma Coordenadoria de Segurança de Redes na Internet Brasil” é publicado pelo CGI.br<sup>1</sup>

- Levantamento da situação no País
- Definição de prioridades
- Levantamento do **melhor modelo para agir como facilitador para o tratamento de incidentes de segurança**
  - time autônomo e neutro, para atuar como ponto de contato nacional
  - orientar tecnicamente sobre prevenção e resposta a incidentes
  - fomentar treinamento, atualização e cooperação
  - fomentar a criação de novos CSIRTs (Times de Tratamento de Incidentes de Segurança em Computadores) no País

Junho/1997: o CGI.br cria o CERT.br (à época chamado NBSO – *NIC BR Security Office*), com base nas recomendações do relatório, como um CSIRT de último recurso, com responsabilidade nacional<sup>2</sup>

<sup>1</sup><https://cert.br/sobre/estudo-cgibr-1996.html>

<sup>2</sup><https://nic.br/pagina/gts/157>

## 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



**FIRST:** Membro pleno desde 2002      **TF-CSIRT Trusted Introducer:** *Accredited* desde 2020  
**APWG:** Research partner desde 2004      **SEI/CMU:** Cursos autorizados desde 2003  
**Honeynet Project:** Mantém o capítulo do Brasil desde 2003

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

## 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

## Principais Atividades

- Facilitar a coordenação do tratamento de incidentes entre as partes
  - Ponto de contato nacional de último recurso
  - Trabalho colaborativo com outras entidades
  - Auxílio na análise técnica e compreensão de ataques e ameaças
- Aumentar a detecção, correlação de eventos e determinação de tendências
- Transferir o conhecimento através de cursos, boas práticas e conscientização

Foco do CERT.br nestes 25 anos:

## Aumentar a Capacidade Nacional de Tratamento de Incidentes

**Nenhum time ou estrutura única conseguirá fazer sozinho a segurança ou a resposta a incidentes**

### Comunidade Nacional

- Ações junto a setores chave, para **criação e treinamento de Times** de Tratamento de Incidentes de Segurança (CSIRTs)
- **Auxiliar na análise** técnica e **facilitar** o tratamento de incidentes por outros CSIRTs
- Gerar massa crítica para possibilitar a **cooperação** e melhora na segurança das redes
- Ter uma visão sobre as principais **tendências** de ataques no Brasil

### Comunidade Internacional

- Estabelecer **relações de confiança**
  - facilitar a comunicação em casos de incidentes
  - dar acesso a informações que ajudem a comunidade local
- **Influenciar** os padrões e certificações sendo construídos para CSIRTs
- Levar a **visão nacional** aos fóruns pertinentes

# Fatores de Sucesso no Tratamento de Incidentes: Pessoas e Relações de Confiança Fazem a Diferença

## **Incidentes não acontecem no vácuo**

- envolvem múltiplas organizações, redes e países
- resolução requer análise de informações internas e externas

## **CSIRTs operam em um esquema de governança em rede**

- não há hierarquia
- há a construção de redes de confiança globais e locais

## **Diversas comunidades formadas ao redor do Globo**

- FIRST
- TF-CSIRT
- APCERT
- AfricaCERT
- NatCSIRTs
- EU e-CSIRT Network
- LAC-CSIRTs
- OIC-CERT

## **Maturidade evoluiu para um código de ética e modelos de acreditação e certificação**

- EthicsFIRST
- SIM3 - *Security Incident Management Maturity Model*
- *TF-CSIRT Trusted Introducer*

# Cooperação Internacional: Principais Fóruns com Participação do CERT.br

## FIRST

Fórum Global de CSIRTs, que existe desde 1992

- membro desde 2002

### Destaques da Participação:

- Membro do Conselho Diretor em 2012/2013
- Coordenação de conteúdo do padrão *FIRST CSIRT Services Framework*
- Organização do CTF da Conferência Anual
- Membro do *Membership Committee*
- Participa ativamente dos seguintes SIGs (Grupos de Interesse Especial): *CSIRT Framework Development, DNS Abuse, Ethics, Security Lounge* (do qual é *co-chair*) e TLP
- *Chair* da Conferência 2020
- Viabilização da parceria entre o FIRST e o LACNIC
  - CERT.br é *co-host* dos Simpósios na região

## NatCSIRTs - organizado pelo CERT/CC

CERT.br está presente desde 2006

Reunião anual de CSIRTs de responsabilidade nacional

- participam CERT.br e CTIR Gov

### Maiores parceiros do CERT.br:

CERT/CC	CISA	CERT.at
JPCERT/CC	NISC JP	CERT.LV
CERT.PL	NCSC-NL	NCSC-FI
HKCERT	TWCERT/CC	

## LAC-CSIRTs

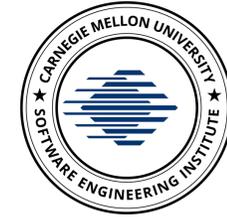
Reunião de Times de Resposta a Incidentes de Segurança (CSIRTs) da região da América Latina e o Caribe – ocorre durante o LACNIC

# Criação de Uma Comunidade Atuante no Brasil: Treinamento e Fomento à Cooperação e Criação de CSIRTs

## Cursos de Gestão de Incidentes

Licencia os cursos do *CERT<sup>®</sup> Division*, do *SEI/Carnegie Mellon*, desde 2003:

- <https://cert.br/cursos/>
- 93 turmas, atingindo 2165 profissionais de diversos setores
  - incluindo por exemplo: ABIN, Anatel, BB, Bradesco, CAIXA, CTIR Gov, Câmara dos Deputados, CDCiber, DASA, Eletrobrás, Eletronuclear, Exército, FINEP, Força Aérea, Furnas, Globo, Intelbras, ITAIPU, Itaú, MJ, Marinha, OEC, Petrobras, Presidência, RNP, Sabesp, SERPRO, STF, STJ, USP, Unicamp, Vale e VIVO.
  - mais de metade dos capacitados são da APF e de outros órgãos de governo
- Turmas especiais e gratuitas para os grandes eventos - 176 profissionais treinados



**SEI**  
Partner  
Network

## Fórum Brasileiro de CSIRTs

- Evento anual para profissionais da área de Tratamento de Incidentes
- *Workshops* sobre assuntos específicos
- <https://cert.br/forum2022/>

## Lista de CSIRTs Brasileiros

- <https://cert.br/csirts/brasil/>

## Fomento à adoção de MISP para compartilhamento de ameaças

- <https://cert.br/misp/>

# Detalhamento das Demais Atividades do CERT.br

cert.br nic.br egi.br

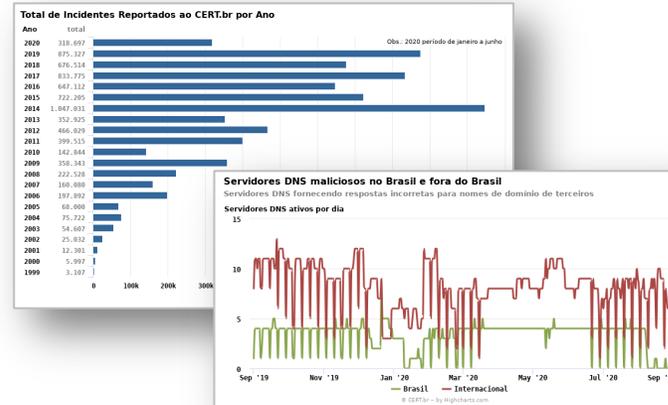
# Gestão de Incidentes e Consciência Situacional

cert.br nic.br egi.br

# Tratamento de Incidentes e Consciência Situacional: Fontes dos Dados, Métricas e Compartilhamento

Notificações voluntárias de incidentes enviadas para: [cert@cert.br](mailto:cert@cert.br)

- Volume em 2021: 1.318.960 e-mails tratados, relativos a 457.270 incidentes notificados ao CERT.br

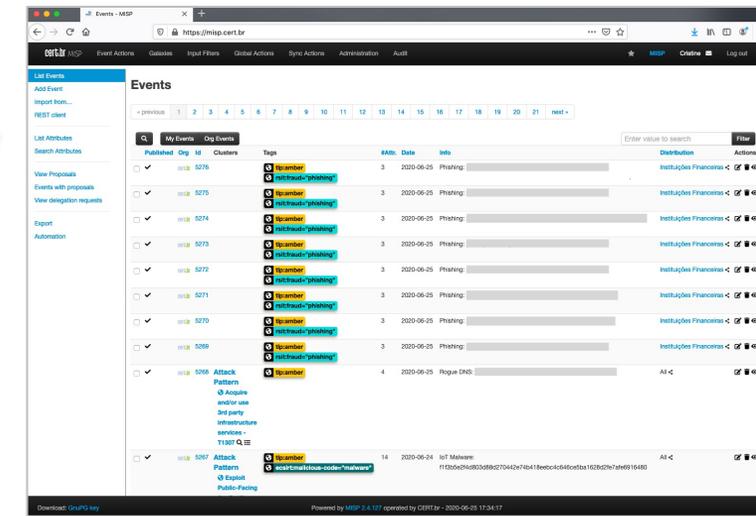
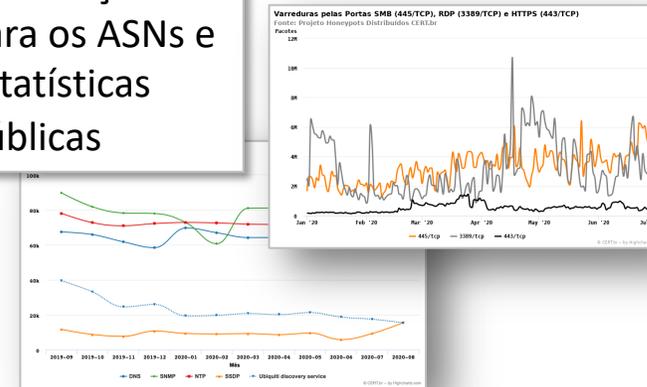


- ### Compartilhamento via MISP
- Indicadores selecionados são compartilhados com parceiros
  - Servidores DNS maliciosos
  - Phishing
  - Binários e Comando e Controle de botnets IoT
  - Amplificadores usados em ataques DDoS

## Threat feeds

- Honeypots Distribuídos do CERT.br
- Team Cymru
- SpamHaus
- ShadowServer
- Shodan
- Operações Anti-Botnet (Microsoft/FBI)

Notificações para os ASNs e estatísticas públicas



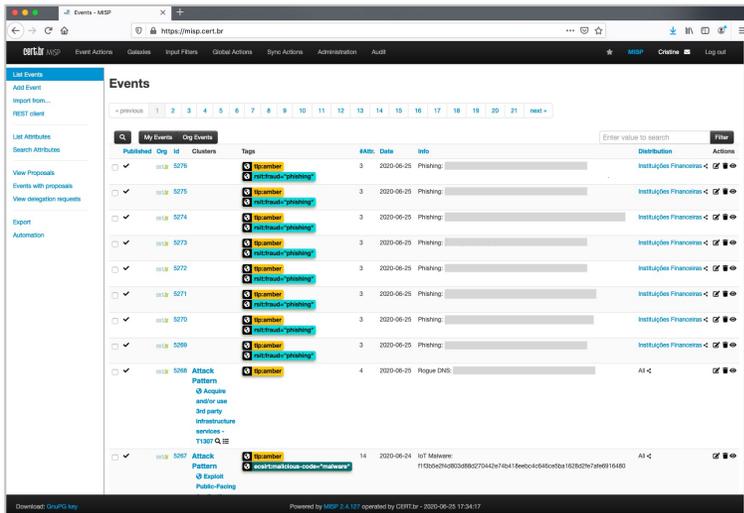
<https://cert.br/stats/>

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

# Tratamento de Incidentes e Consciência Situacional: Compartilhamento de Dados via MISP

## O que é o MISP

- uma plataforma de software livre para compartilhamento de dados de inteligência de ameaças, e
- um conjunto de padrões abertos para compartilhamento destas informações.



## Atividades promovidas pelo CERT.br

- Estímulo do uso por diversos setores
  - financeiro
  - energia
  - acadêmico
  - governo
  - operadores de redes
- Promovendo treinamentos
  - *Workshop* MISP, junto ao Fórum Brasileiro de CSIRTs
  - *Workshop* para o setor financeiro
  - Tutorial *online* disponibilizado na página do CERT.br

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

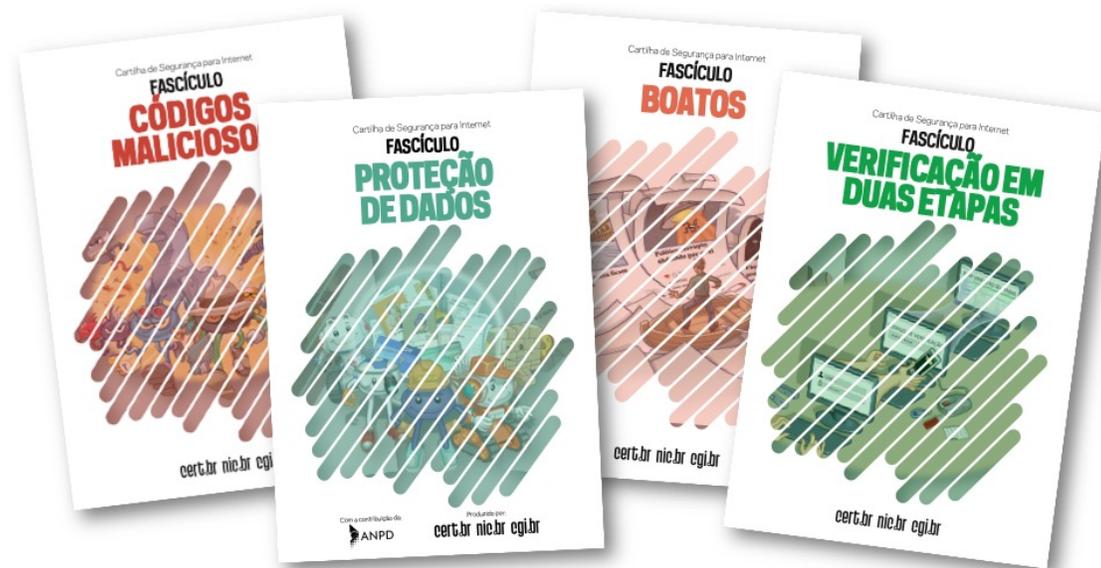
# Boas Práticas e Conscientização

cert.br nic.br egi.br

# Público Geral - 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/>

# Público Infantil: Guia com Dicas e Passatempos + Personagens de Montar

## Guias Internet Segura

- Disponíveis Gratuitamente
- Parcerias de impressão com escolas privadas
- Material de apoio para pais
- Traduzido pelo NCSC-FI



<https://internetsegura.br/criancas/>

# Público Técnico:

## Boas Práticas com Base nos Incidentes mais Prevalentes

Objetivo de fomentar a adoção de boas práticas de segurança por profissionais da área técnica:

- Recomendações para Melhorar o Cenário de Ataques DDoS  
<https://cert.br/docs/whitepapers/ddos/>
- Recomendações para Notificações de Incidentes de Segurança  
<https://cert.br/docs/whitepapers/notificacoes/>
- Recomendações para Evitar o Abuso de Servidores DNS Recursivos Abertos  
<https://cert.br/docs/whitepapers/dns-recursivo-aberto/>
- Práticas de Segurança para Administradores de Redes Internet  
<https://cert.br/docs/seg-adm-redes/>
- *Honeypots e Honeynets*: Definições e Aplicações  
<https://cert.br/docs/whitepapers/honeypots-honeynets/>
- Boas Práticas para Reduzir *Spam*  
<https://antispam.br/admin/>

# Outras Iniciativas por Uma Internet Mais Resiliente

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

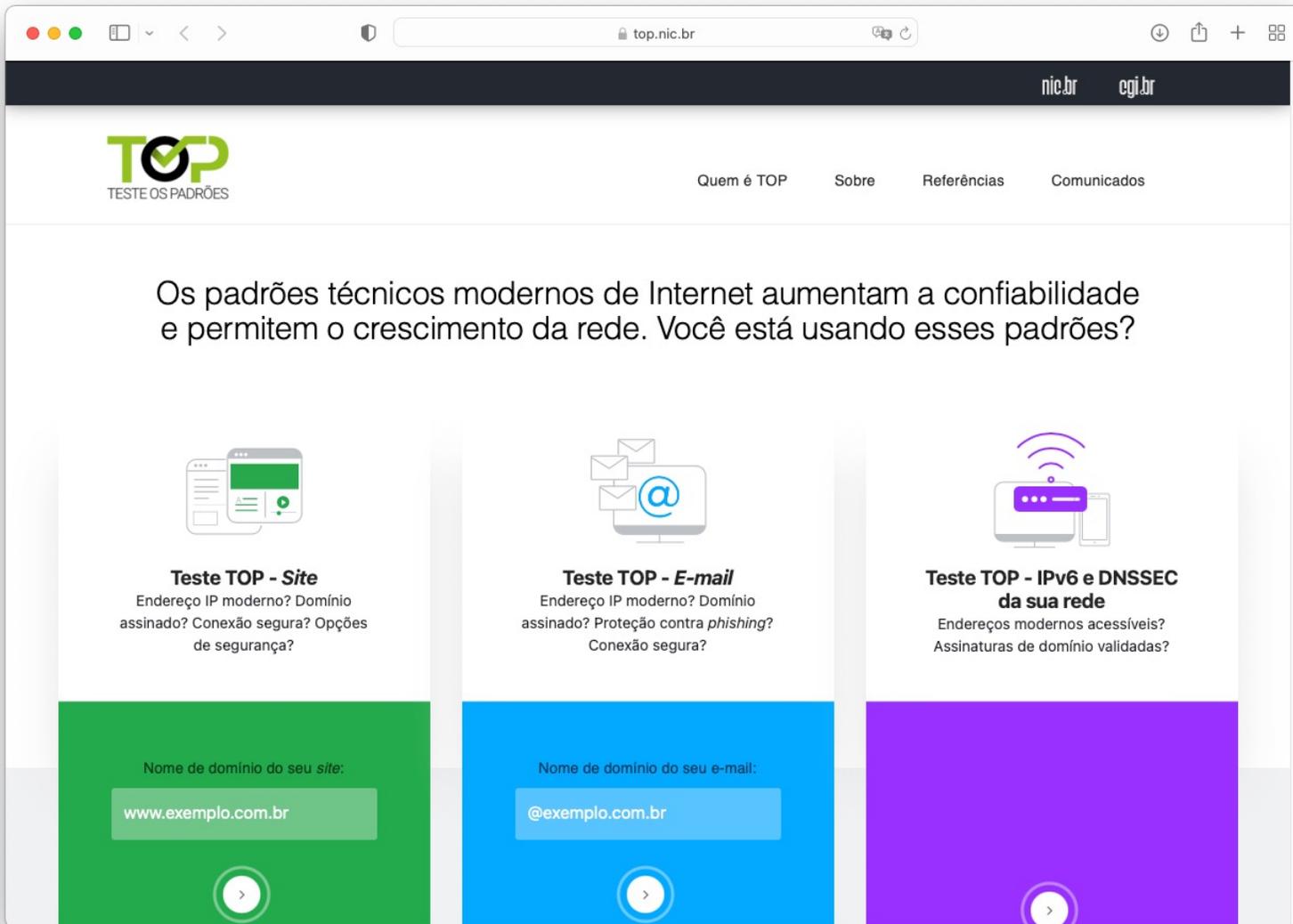
## Iniciativa conjunta:

- ISOC, NIC.br, Abranet, Abrint, Conexis, InternetSul, RedeTelesul e TelComp

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



# 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 sobre os padrões
  - dicas sobre como corrigir possíveis problemas

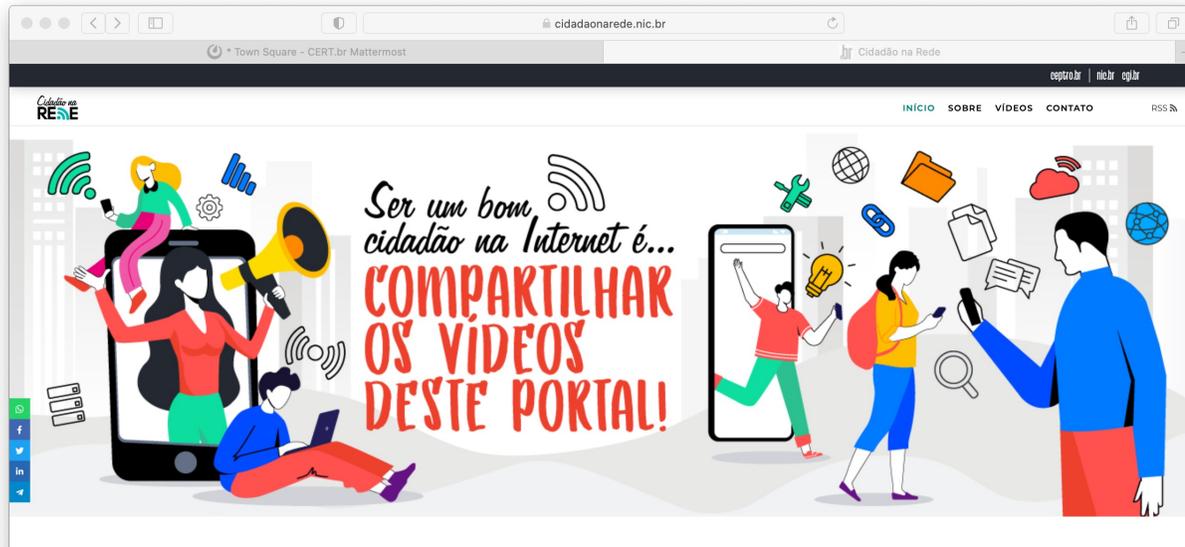
Apoiadores



# 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



### SEGURANÇA

- 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
- 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**  
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**  
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?**  
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.  
Postado em 12/11/2020
- Vídeos consomem muita "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**  
Os repetidores Wi-Fi possuem algumas limitações, uma delas é o alcance do sinal. Existem equipamentos simples para melhorar isso.  
Postado em 12/11/2020
- Sinal Wi-Fi**  
Sabia que existem maneiras simples de melhorar o sinal do seu Wi-Fi 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

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

# Conscientização de Todos é Essencial: Portal InternetSegura.br – materiais gratuitos



The screenshot shows the homepage of the InternetSegura.br portal. At the top left, there are logos for 'nic.br' and 'INTERNET SEGURA BR'. To the right, there are navigation links for 'Sobre' and 'Outras iniciativas', and a button labeled 'Como Pedir Ajuda' with a megaphone icon. The main heading reads 'Internet Segura – Faça sua parte e todos teremos uma Internet mais segura!'. Below this, there are six categories represented by illustrations and text: 'para Crianças' (two children), 'para Adolescentes' (two young adults), 'para Pais e Educadores' (a woman and a man), 'para 60+' (an elderly couple), 'para Técnicos' (a person with a stethoscope), and 'para Interesse Geral' (a diverse group of people).

<https://internetsegura.br/> – Todo o conteúdo disponível *online* gratuitamente sob Licença *Creative Commons*

# LAC-AAWG – Latin American and Caribbean Anti-Abuse Working Group

## CERT.br é co-chair

Iniciativa conjunta do:

- M<sup>3</sup>AAWG - *Messaging, Malware and Mobile Anti-Abuse Working Group*
- LACNOG - *Latin American and Caribbean Network Operators Group*

Principal resultado até o momento:

- *BCOP Minimum Security Requirements for Customer Premises Equipment (CPE) Acquisition*

Disponível em:

- Português, Inglês, Japonês e Coreano

[www.m3aawg.org/CPESecurityBP-Portuguese](http://www.m3aawg.org/CPESecurityBP-Portuguese)

[www.lacnog.net/docs/lac-bcop-1](http://www.lacnog.net/docs/lac-bcop-1)

[www.m3aawg.org/CPESecurityBP](http://www.m3aawg.org/CPESecurityBP)

**LACNOG-M<sup>3</sup>AAWG 공동 작성**  
**고객기밀 (가입자 대내장치) 최소 보안 요구사항에 대한**  
**Best Current Operational Practices**  
LAC-BCOP-1

**Documento conjunto LACNOG-M<sup>3</sup>AAWG:**  
**Melhores Práticas Operacionais Atuais**  
**sobre Requisitos Mínimos de Segurança para**  
**Aquisição de Equipamentos para Conexão de Assinante (CPE)**  
**LAC-BCOP-1**  
Maio 2019

Este documento está disponível no site do LACNOG em [www.lacnog.net/docs/lac-bcop-1](http://www.lacnog.net/docs/lac-bcop-1)  
Este documento está disponível no site do M<sup>3</sup>AAWG em [www.m3aawg.org/CPESecurityBP-Portuguese](http://www.m3aawg.org/CPESecurityBP-Portuguese)  
A versão original em Inglês está disponível no site do M<sup>3</sup>AAWG em [www.m3aawg.org/CPESecurityBP](http://www.m3aawg.org/CPESecurityBP)

Este é um documento conjunto de Melhores Práticas Operacionais Atuais (*Best Current Operational Practices*, BCOP) desenvolvido pelo LACNOG: (Grupo de Operadores de Redes da América Latina e o Caribe) e pelo M<sup>3</sup>AAWG: (Messaging, Malware and Mobile Anti-Abuse Working Group). É o produto das versões originais do LACNOG por seus grupos de trabalho LAC-AAWG<sup>1</sup> (Grupo de Trabalho Antiabuso da América Latina e o Caribe) e Grupo de Trabalho BCOP<sup>2</sup>, em cooperação com membros do M<sup>3</sup>AAWG, Assesores Técnicos Seniores e o Comitê Técnico do M<sup>3</sup>AAWG.

**Índice**

Sumário Executivo .....	2
1. Terminologia .....	2
2. Requisitos Gerais ( <i>General Requirements – GR</i> ) .....	3
3. Requisitos de Segurança de Software ( <i>Software Security Requirements – SSR</i> ) .....	4
4. Requisitos de Atualização e Gerenciamento ( <i>Update and Management Requirements – MR</i> ) .....	4
5. Requisitos Funcionais ( <i>Functional Requirements – FR</i> ) .....	5
6. Requisitos de Configuração Inicial ( <i>Initial Configuration Requirements – IR</i> ) .....	7
7. Requisitos do Fornecedor ( <i>Vendor Requirements – VR</i> ) .....	8
8. Lista de Acrônimos .....	8
9. Agradecimentos .....	9
10. Referências Informativas .....	9
Anexo 1 – Tabela de Requisitos .....	11

**LACNOG**  
Grupo de Operadores de Redes da América Latina e o Caribe  
Departamento de Montevideo, República Oriental do Uruguai  
[www.lacnog.net](http://www.lacnog.net)

**M<sup>3</sup>AAWG**  
Messaging, Malware and Mobile Anti-Abuse Working Group  
781 Beach Street, Suite 302  
San Francisco, California 94109 U.S.A. – [www.m3aawg.org](http://www.m3aawg.org)

**LACNOG-M<sup>3</sup>AAWG Joint Best Current Operational Practices**  
**Minimum Security Requirements**  
**Premises Equipment (CPE) Acquisition**  
**LAC-BCOP-1**  
May 2019

Available on the LACNOG website at [www.lacnog.net/docs/lac-bcop-1](http://www.lacnog.net/docs/lac-bcop-1)  
Available on the M<sup>3</sup>AAWG website at [www.m3aawg.org/CPESecurityBP](http://www.m3aawg.org/CPESecurityBP)

BCOP (Best Current Operational Practices) document developed by LACNOG<sup>1</sup> (Network Operators Group) and M<sup>3</sup>AAWG<sup>2</sup> (Messaging, Malware and Mobile Anti-Abuse Working Group). It is the product of LACNOG's original drafts by its working groups: LAC-AAWG<sup>3</sup> (Latin American and Caribbean Anti-Abuse Working Group) and BCOP Working Group<sup>4</sup> (Best Current Operational Practices Working Group). M<sup>3</sup>AAWG members, Senior Technical Advisors and the M<sup>3</sup>AAWG

Network Operators Group (LACNOG), <http://www.lacnog.net/>  
Messaging, Malware and Mobile Anti-Abuse Working Group (M<sup>3</sup>AAWG), <http://www.m3aawg.org/>  
Latin American and Caribbean Anti-Abuse Working Group (LAC-AAWG), <http://www.lacnog.net/lac-aawg/>  
Best Current Operational Practices Working Group (BCOP), <http://www.lacnog.net/wg-bcop/>

Network Operators Group  
781 Beach Street, Suite 302  
San Francisco, California 94109 U.S.A. – [www.m3aawg.org](http://www.m3aawg.org)

# Campanha #FiqueEsperto

Iniciativa multissetorial em prol do uso seguro da Internet, com o objetivo de disseminar boas práticas

- Site com informações, divulgação via *e-mail*, via redes sociais e via mensagens (SMS) pelas operadoras de celular
- Apoiadores:
  - ABBC
  - Banco Central
  - Febraban
  - Abranet
  - CACB
  - ISOC Brasil
  - Abrint
  - camara-e.net
  - NIC.br
  - Anatel
  - Conexis
  - Telcomp
  - Assoc. Neo
  - CGI.br
  - WhatsApp



<https://fe.seg.br/>

**PROTEJA AS SENHAS. ADOTE UM APLICATIVO DE GESTÃO DE SENHAS, GUARDE EM UM ARQUIVO CRIPTOGRAFADO OU ANOTE NUM PAPEL E GUARDE EM UM LOCAL SEGURO**

**EVITE NOMES DE PESSOAS PRÓXIMAS, DATAS E PRINCIPALMENTE COMBINAÇÕES QUE POSSAM SER FACILMENTE ADIVINHADAS (POR EXEMPLO: ABCD OU 1234)**

**NUNCA FORNEÇA SENHAS OU CÓDIGOS DE SEGURANÇA PELO TELEFONE OU COMO RESPOSTA A MENSAGENS, MESMO QUANDO A FONTE PARECER CONFIÁVEL. EMPRESAS DE TELECOMUNICAÇÕES E BANCOS, POR EXEMPLO, NUNCA SOLICITAM TAIS DADOS DESSA FORMA**

**SEMPRE HABILITE OS MECANISMOS DE DUPLA AUTENTICAÇÃO FORNECIDOS, POR MEIO DE OUTRAS FERRAMENTAS DE AUTENTICAÇÃO OU MESMO VIA SMS, ESPECIALMENTE NOS APLICATIVOS DE MENSAGENS E REDES SOCIAIS. DESSA FORMA, SE ALGUÉM DESCOBRIR SUA SENHA, NÃO CONSEGUIRÁ ACESSAR A CONTA**

**NUNCA USE A MESMA SENHA EM DIFERENTES SERVIÇOS**

# Obrigado

📧 notificações para: cert@cert.br

📧 @certbr

<https://cert.br/>

25 de agosto de 2022

**nic.br** **cgi.br**

[www.nic.br](http://www.nic.br) | [www.cgi.br](http://www.cgi.br)