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 cgi.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/

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/

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

Dados atualizados em 24 de agosto de 2022

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[1]

- 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[2]

[1] https://cert.br/sobre/estudo-cgibr-1996.html
[2] https://nic.br/pagina/gts/157

cert.br

Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

CERT Nacional de Último Recurso

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:

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

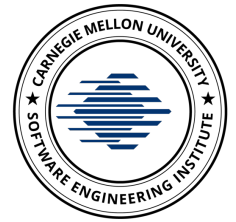
Maiores parceiros do CERT.br:

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



SEI Partner Network

Cursos de Gestão de Incidentes

Licencia os cursos do *CERT® 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

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 cgi.br

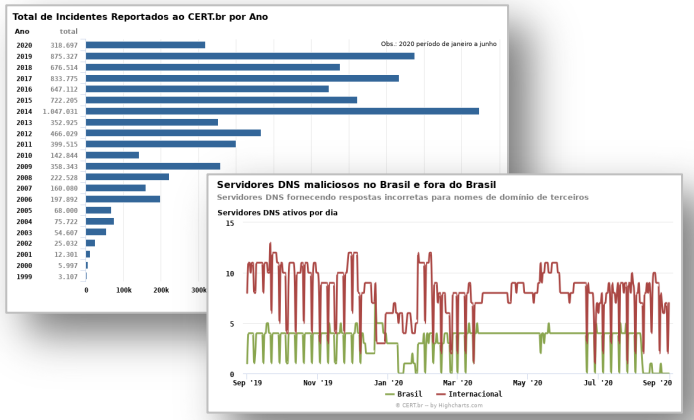
Gestão de Incidentes e Consciência Situacional

cert.br nic.br cgi.br

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

Notificações voluntárias de incidentes enviadas para: cert@cert.br

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



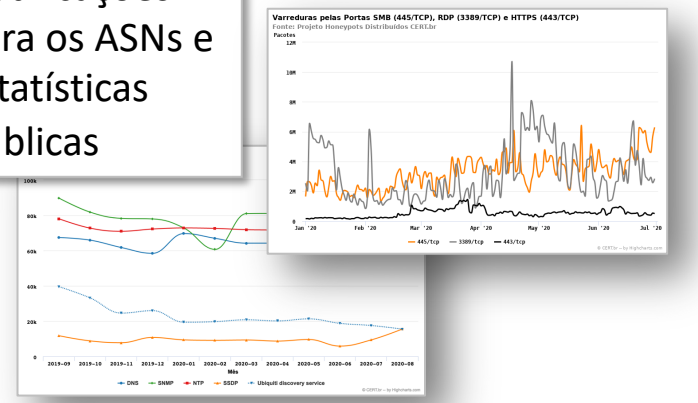
Compartilhamento via MISP

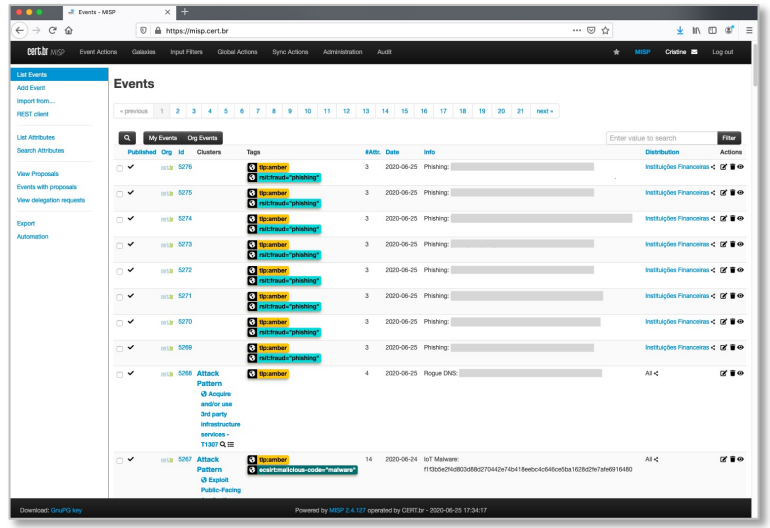
- Indicadores selecionados são compartilhados com parceiros
  - Servidores DNS maliciosos
  - *Phishing*
  - Binários e Comando e Controle de *botnets* IoT
  - Amplificadores usados em ataques DDoS

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/

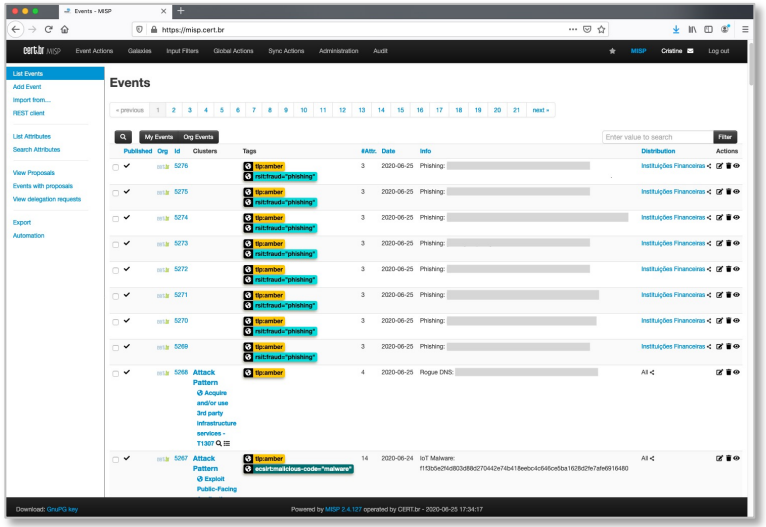
https://cert.br/misp/

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 cgi.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:

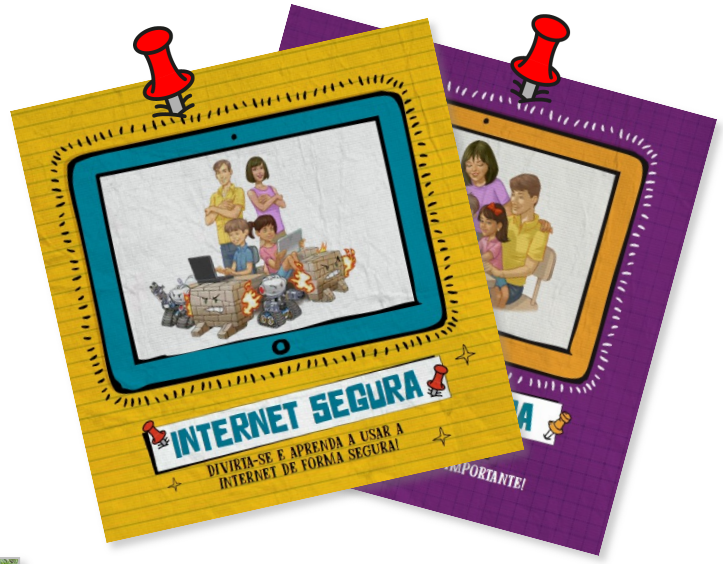
    Itaipu, Eletronuclear, ELO, Microsoft, Procergs e Metrô SP

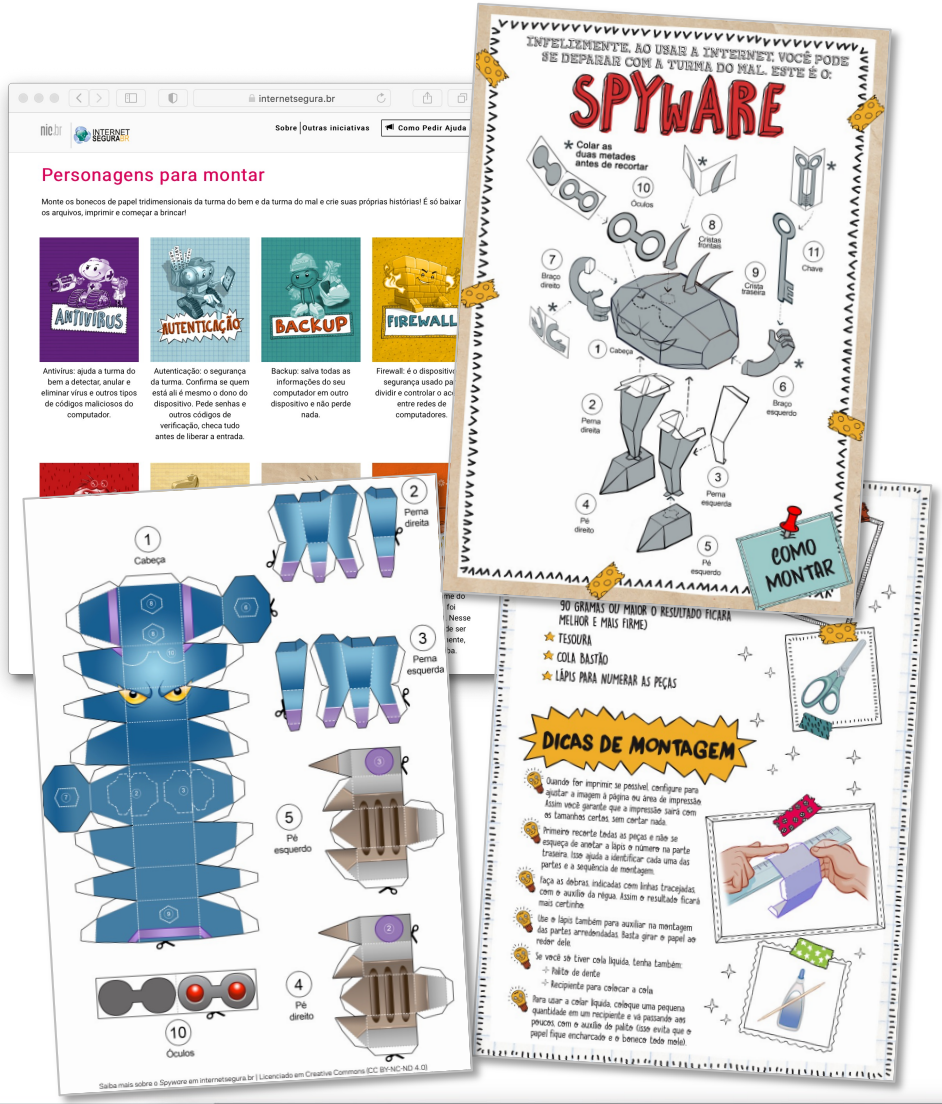
https://cartilha.cert.br/

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 cgi.br

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

PROGRAMA INTERNET +SEGURA

Objetivo principal:

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

Incentivo à adoção de boas práticas:

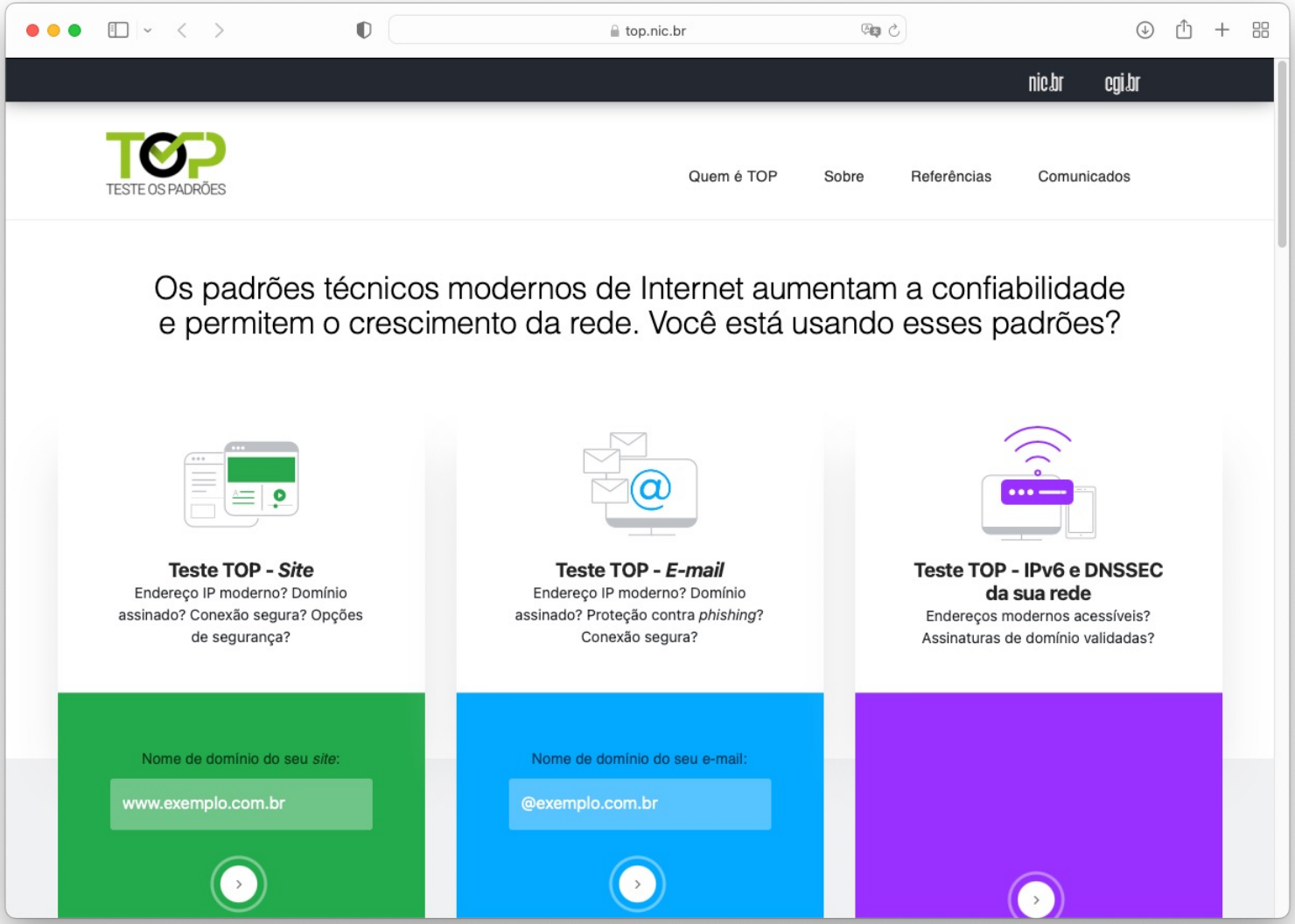
- *Hardening*
- Segurança de roteamento (MANRS)
- *Anti-spoofing* (BCP 38)
- Reduzir serviços abertos que permitam amplificação

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

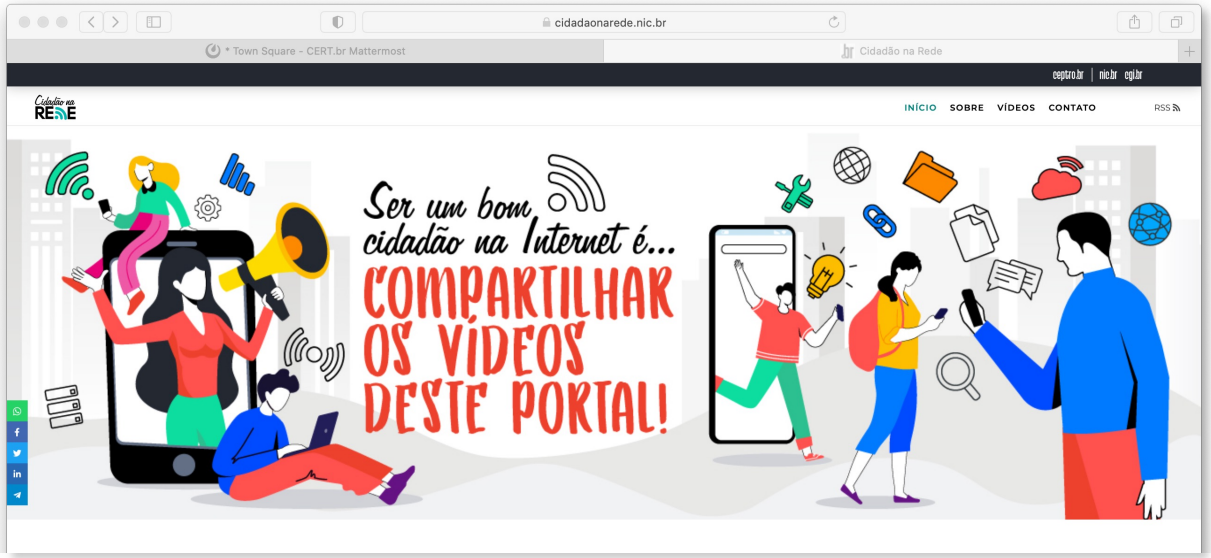
- detalhamento de todos os resultados
  - referências sobre os padrões
  - dicas sobre como corrigir possíveis problemas

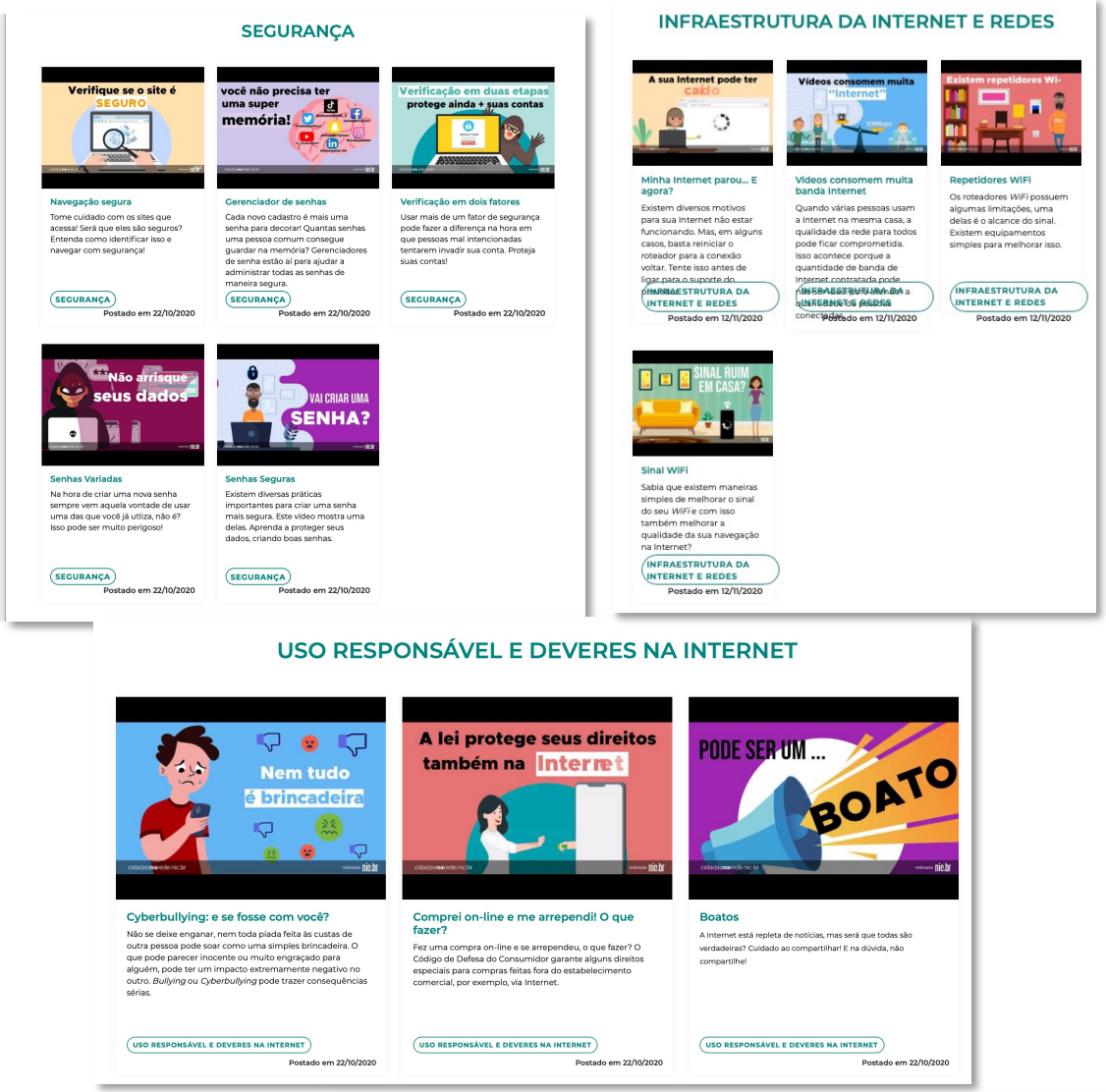
Apoiadores

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





https://cidadaonarede.nic.br/

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

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:

- M³AAWG - *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

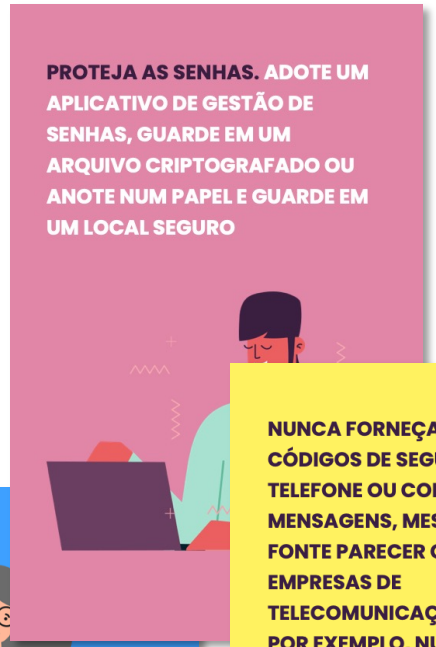
www.m3aawg.org/CPESecurityBP-Portuguese
www.lacnog.net/docs/lac-bcop-1
www.m3aawg.org/CPESecurityBP

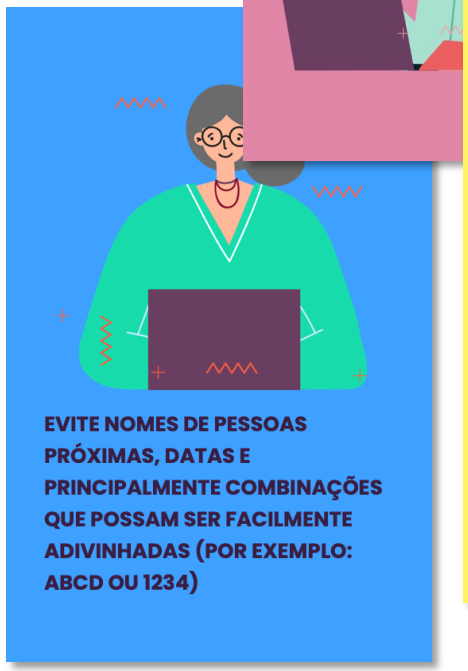
Campanha #FiqueEsperto

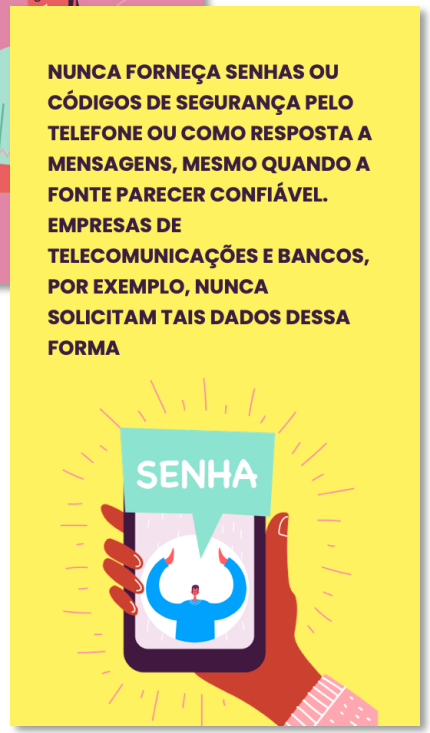
Iniciativa multissetorial em prol do uso seguro da Internet, com o objetivo de disseminar boas práticas

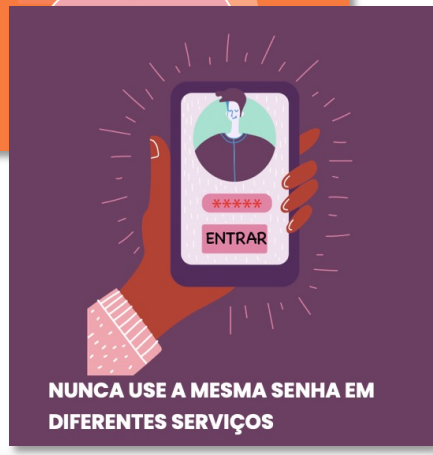
– *Site* com informações, divulgação via *e-mail*, via redes sociais e via mensagens (SMS) pelas operadoras de celular

– Apoiadores:
- ABBC
- Abranet
- Abrint
- Anatel
- Assoc. Neo
- Banco Central
- CACB
- camara-e.net
- Conexis
- CGI.br
- Febraban
- ISOC Brasil
- NIC.br
- Telcomp
- WhatsApp









https://fe.seg.br/

Obrigado

notificações para: cert@cert.br

@certbr

https://cert.br/

25 de agosto de 2022

nic.br cgi.br

www.nic.br | www.cgi.br