nic.br cgi.br

20 years cert.br

Regional Meeting of CSIRTs of the Americas

Brasília, DF, Brazil

May 16, 2018

Evolution of the Scenario of Incidents in Brazil

Dr. Cristine Hoepers
General Manager
cristine@cert.br

cert.br nic.br cgi.br

Internet Governance in Brazil:
The *Brazilian Internet Steering Committee* – CGI.br

CGI.br is a multi-stakeholder organization created in **1995** by the Ministries of Communications and Science and Technology to **coordinate all Internet related activities in Brazil.**

According to the General Telecommunications Law **Internet is a unregulated value added service**, that should not be confused with telecommunications.

Among the diverse responsibilities reinforced by the Presidential Decree 4.829, it has as the main attributions:

- **to propose policies and procedures related to the regulation of Internet activities**
- **to recommend standards for technical and operational procedures**
- to establish strategic directives related to the use and development of Internet in Brazil
- **to promote studies and technical standards for the network and services' security in the country**
- to coordinate the allocation of Internet addresses (IP) and the registration of domain names using <.br>
- to collect, organize and disseminate information on Internet services, including indicators and statistics

http://www.cgi.br/about/

cgi.br

1 2 3 4 5 6 7 8 9

GOVERNMENT (Appointed) *and*

10 11 12 13 14 15 16 17 18 19 20 21

CIVIL SOCIETY (Elected)

Government Representatives:

1 Ministry of Science and Technology (Coordination)

2 Presidential Cabinet

3 Ministry of Communications

4 Ministry of Defense

5 Ministry of Development, Industry and Foreign Trade

6 Ministry of Planning, Budget and Management

7 National Telecommunications Agency

8 National Council of Scientific and Technological Development

9 National Forum of Estate Science and Technology Secretaries

Civil Society Representatives:

10 Internet Expert

11 General Business Sector Users

12 Internet Service Providers

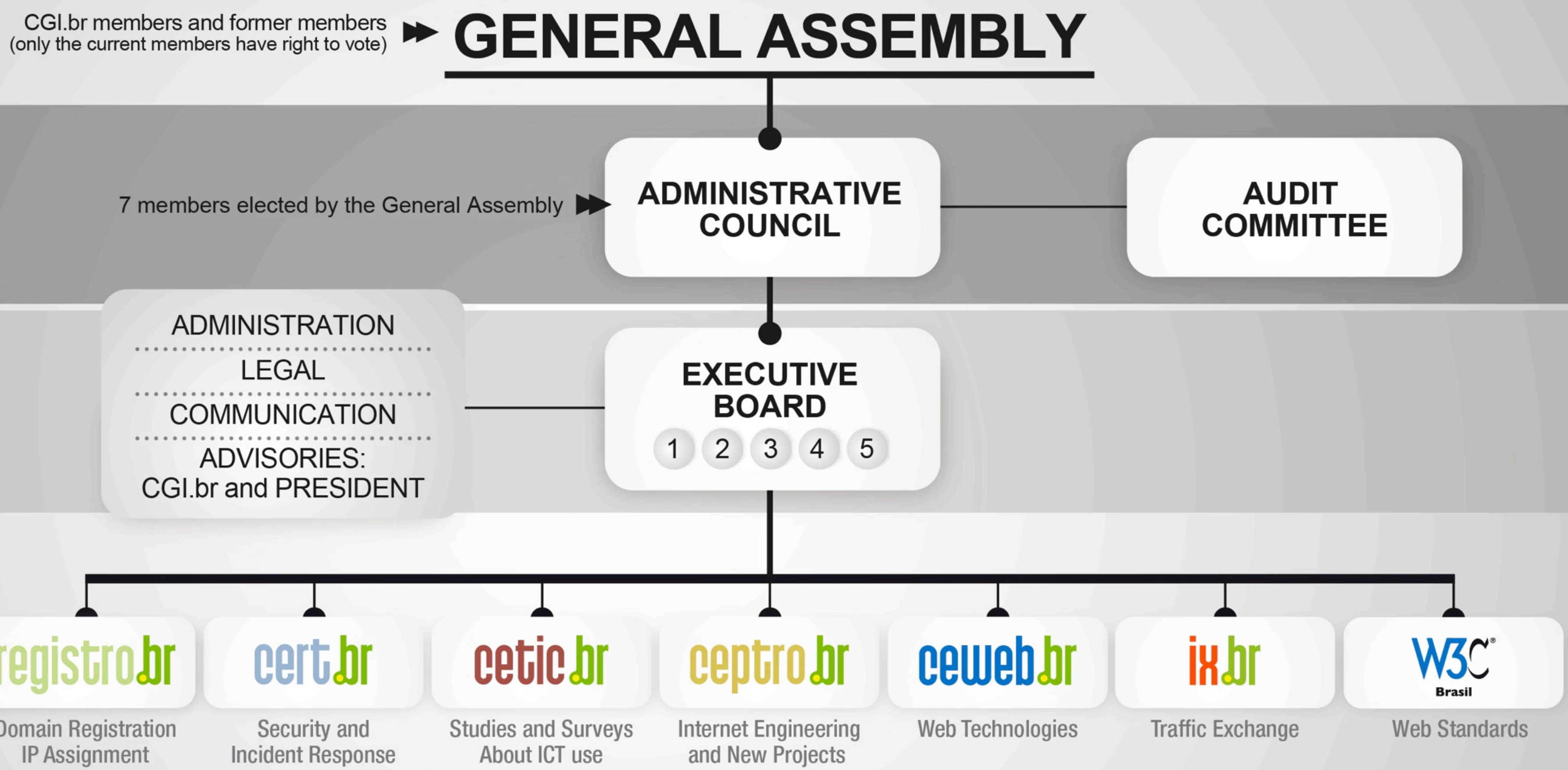
13 Telecommunication Infrastructure Providers

14 Hardware and Software Industries

15 a 18 Non-governmental Entity

19 a 21 Academia

NIC.br – Not for profit organization that implements all services and decisions of CGI.br



CGI.br members and former members
(only the current members have right to vote)

GENERAL ASSEMBLY

7 members elected by the General Assembly

ADMINISTRATIVE COUNCIL

AUDIT COMMITTEE

ADMINISTRATION

LEGAL

COMMUNICATION

ADVISORIES:
CGI.br and PRESIDENT

EXECUTIVE BOARD

1 2 3 4 5

registro.br
Domain Registration
IP Assignment

cert.br
Security and
Incident Response

cetic.br
Studies and Surveys
About ICT use

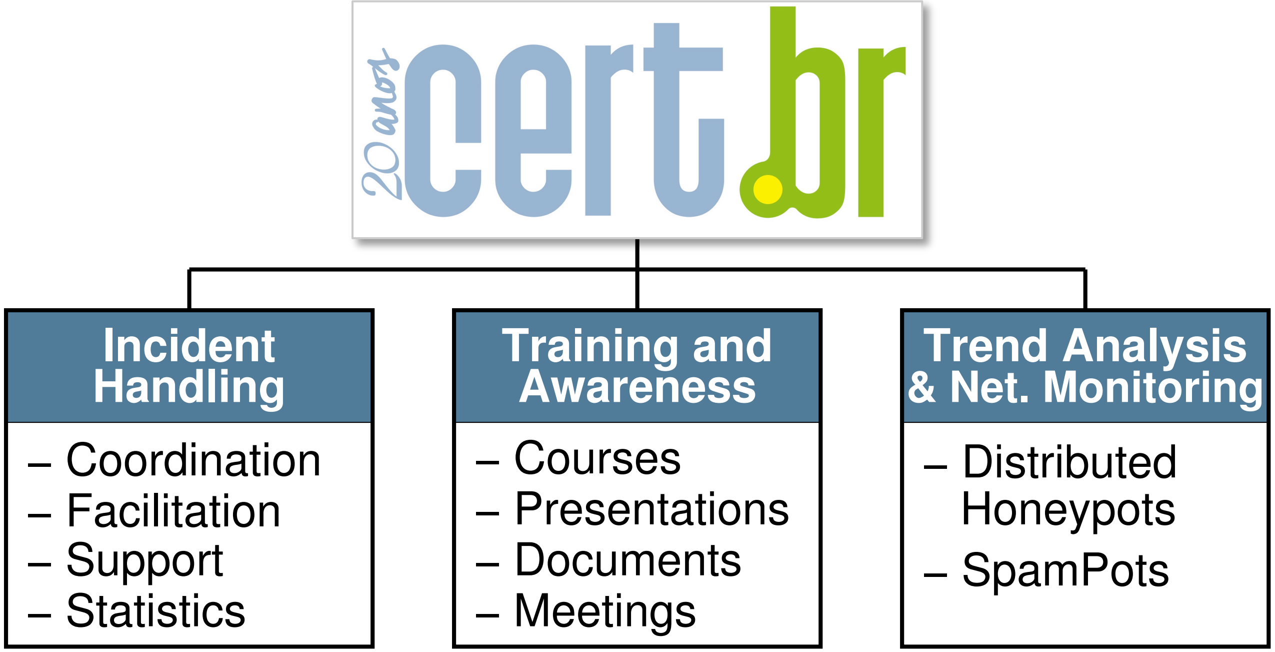
ceptro.br
Internet Engineering
and New Projects

ceweb.br
Web Technologies

ix.br
Traffic Exchange

W3C Brasil
Web Standards

1 Chief Executive Officer
2 Administrative and Financial Director
3 IT and Services Director
4 Director of Special Projects and Development
5 Consulting Director for CGI.br activities



20 anos cert.br

Incident Handling

- Coordination
- Facilitation
- Support
- Statistics

Training and Awareness

- Courses
- Presentations
- Documents
- Meetings

Trend Analysis & Net. Monitoring

- Distributed Honeypots
- SpamPots

Created in 1997 to handle computer security incident reports and activities related to networks connected to the Internet in Brazil

- National focal point for reporting security incidents
- Collect and disseminate information about threats and attack trends
- Increase the country’s security awareness and incident handling capacity
- Develop collaborative relationships with other entities
- Help new CSIRTs to establish their activities

1996 Study that defined the needs and mission of CERT.br:
http://www.nic.br/pagina/grupos-de-trabalho-documento-gt-s/169
https://www.cert.br/about/

What are we seeing in Brazil

Size of the Internet in Brazil:
Cetic.br National Households Survey

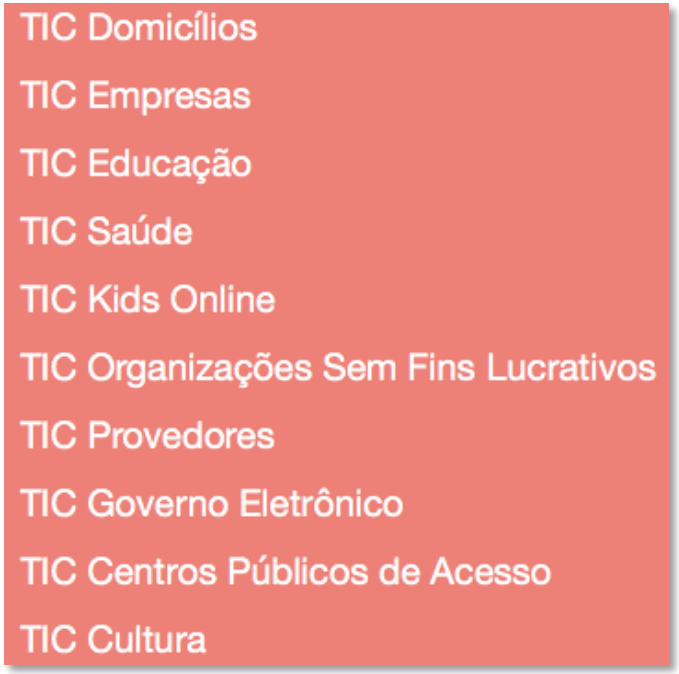
- 54% of households have Internet access
- 69% of the citizens have used Internet at least once
- 61% of the citizens have used the Internet in the last 3 months

UNESCO

Organização
das Nações Unidas
para a Educação,
a Ciência e a Cultura

cetic.br

Centro Regional de Estudos
para o Desenvolvimento da
Sociedade da Informação
sob os auspícios da UNESCO



TIC Domicílios

TIC Empresas

TIC Educação

TIC Saúde

TIC Kids Online

TIC Organizações Sem Fins Lucrativos

TIC Provedores

TIC Governo Eletrônico

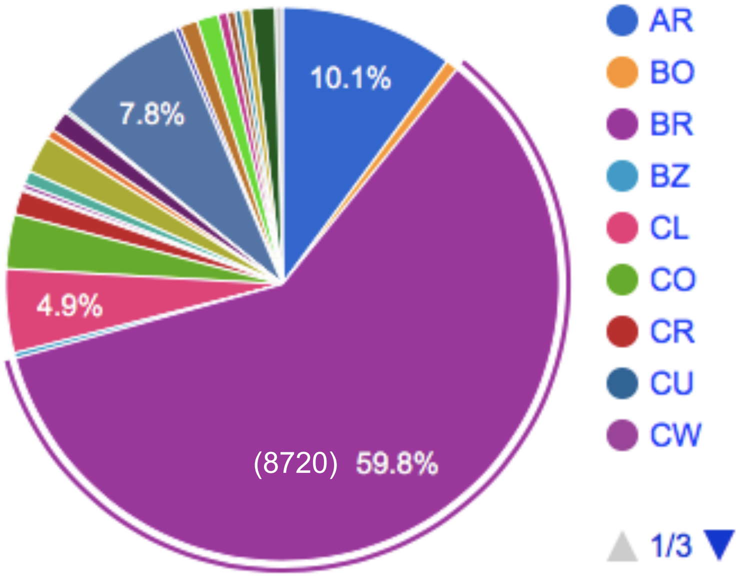
TIC Centros Públicos de Acesso

TIC Cultura

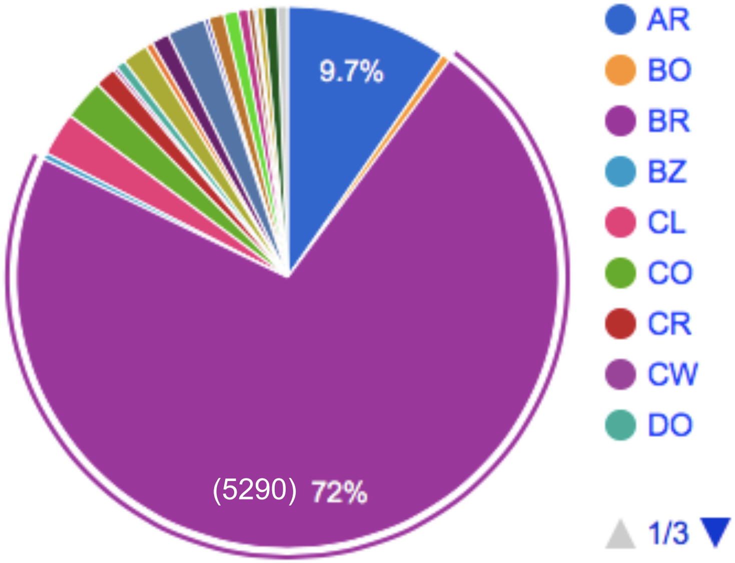
Cetic.br is UNESCO's first center of studies on the information society.
Cetic.br's surveys are based on international reference models, such as the UN's Partnership on Measuring ICT for Development, Eurostat documents, OECD and UNCTAD.
http://cetic.br/about/

Size of the Internet in Brazil: **Data from LACNIC**

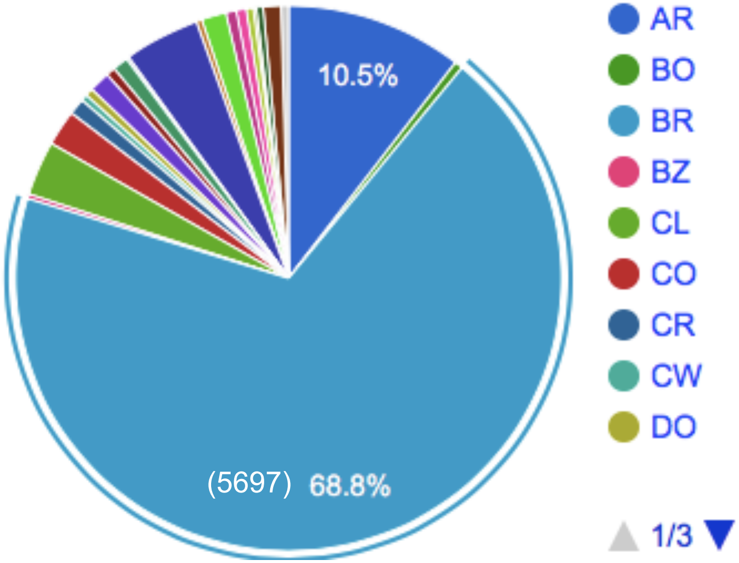
Distribution of IPv4 blocks per country



Distribution of IPv6 blocks per country



Distribution of ASN per country

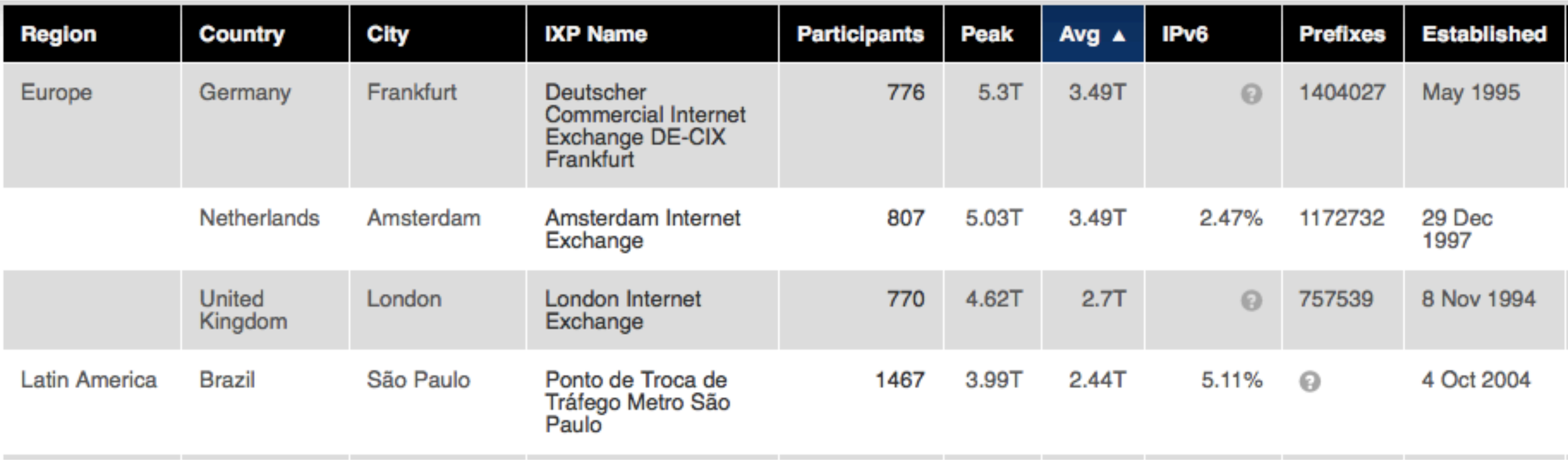


http://www.lacnic.net/en/web/lacnic/estadisticas-asignacion

Size of the Internet in Brazil:
Internet eXchange Points

IX.br SP in the world

- #1 in participants
- #4 in traffic (both average and peak)
- #3 in IPv6 traffic



Region	Country	City	IXP Name	Participants	Peak	Avg ▲	IPv6	Prefixes	Established
Europe	Germany	Frankfurt	Deutscher Commercial Internet Exchange DE-CIX Frankfurt	776	5.3T	3.49T	?	1404027	May 1995
	Netherlands	Amsterdam	Amsterdam Internet Exchange	807	5.03T	3.49T	2.47%	1172732	29 Dec 1997
	United Kingdom	London	London Internet Exchange	770	4.62T	2.7T	?	757539	8 Nov 1994
Latin America	Brazil	São Paulo	Ponto de Troca de Tráfego Metro São Paulo	1467	3.99T	2.44T	5.11%	?	4 Oct 2004

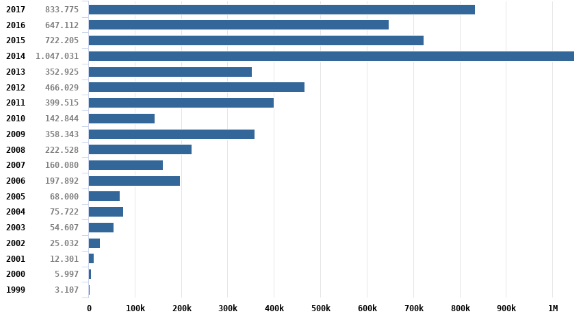
https://www.pch.net/ixp/dir

CERT.br Data Sources

Voluntary Incident Notification

Entry point: e-mail cert@cert.br

- https://www.cert.br/stats/incidentes/

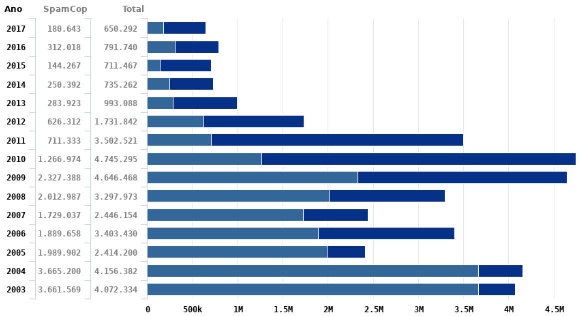


Attack data feeds (CERT.br Distributed Honeypots, Team Cymru, Arbor Atlas, SpamHaus, ShadowServer, Shodan, Anti-Botnet Operations)

Generate incident notification with tips on how to identify the attacks and recover

Complaints of spam originating from Brazilian networks

- https://www.cert.br/stats/spam/

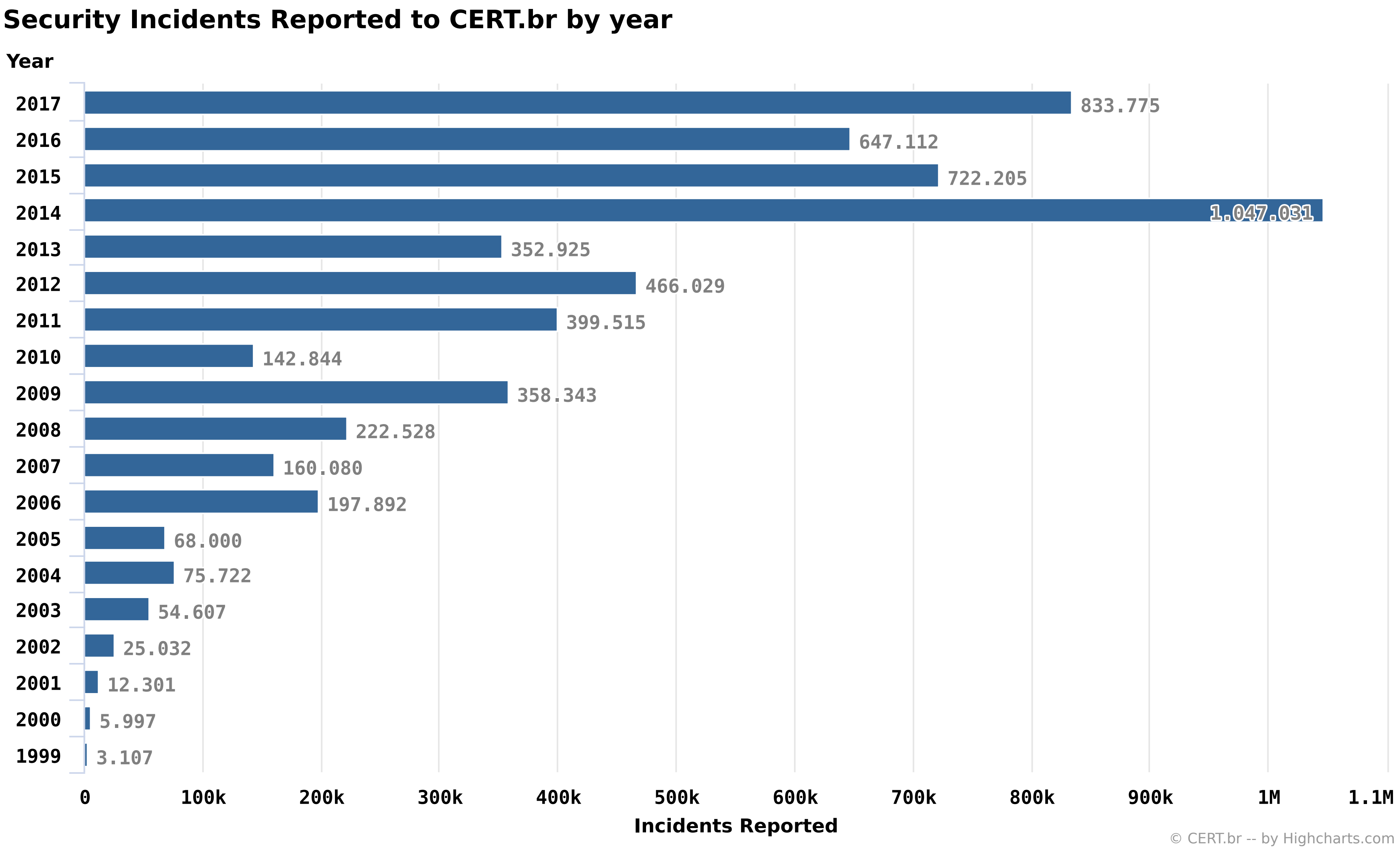


Monitoring of

- IRC Channels, twitter, etc
- Web defacements

Identify new trends and attacks to high value networks

CERT.br Incident Notification Statistics: **1999 to 2017**



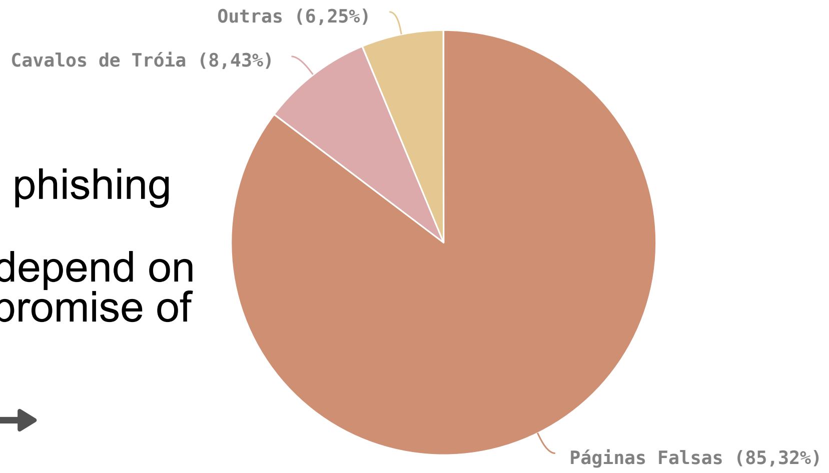
2017 Statistics Highlights

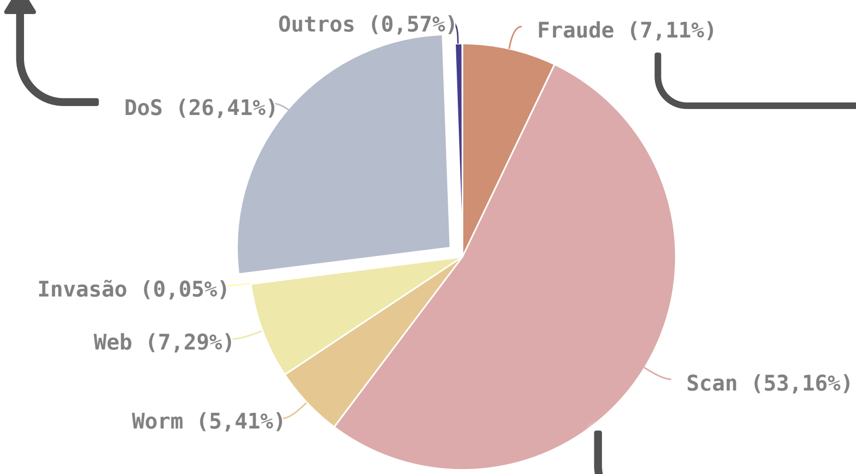
DDoS – increased 3.6 times

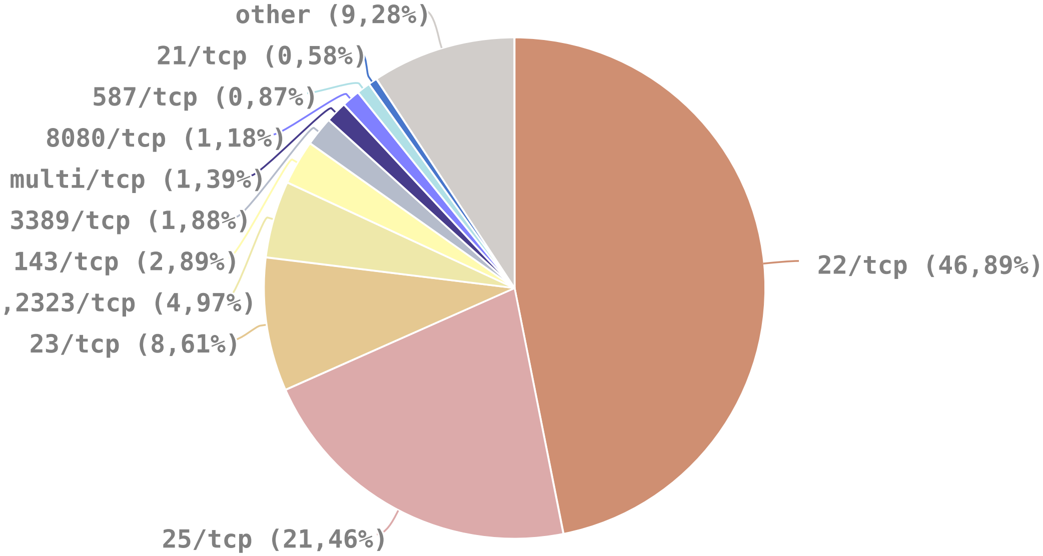
- 300Gbps is the new “normal”
- Up to 1Tbps against some targets
- Most reported DDoS types
  - . IoT botnets
  - . amplification

Fraud

- 85% are phishing pages
- Attacks depend on the compromise of CPEs







Scan

- Ports 22 & 23: servers & IoT passwords brute force attacks
- Port 25: e-mail brute force attacks

Activities on our Distributed Honeypots: **Most Attacked Services**

Password brute force (used by IoT malware and to compromise Unix servers):

- Telnet (23/TCP)
- SSH (22/TCP)
- RDP (3389/TCP)
- Other TCP (2323, 23231, 2222)

Protocols abused by Mirai, in its variant for CPEs (*Customer Premises Equipments*)

- TCP: 7547, 5555, 37777, 6789, 81

Search for protocols that can be abused for amplification attacks

- UDP: DNS, NTP, SSDP, SNMP, Chargen, Netbios, Quotd, mDNS, LDAP

https://honeytarg.cert.br/honeypots/

Devices/Services that Allow Amplification:
Brazilian ASNs and IPs Notified by CERT.br

	DNS		SNMP		NTP		SSDP	
2017	**ASNs**	**IPs**	**ASNs**	**IPs**	**ASNs**	**IPs**	**ASNs**	**IPs**
January	2.133	87.953	–	–	981	97.423	–	–
February	2.066	67.159	1.681	573.373	–	–	805	37.459
March	–	–	1.805	604.805	915	104.665	–	–
April	2.191	72.124	–	–	861	92.120	812	27.233
May	2.280	69.957	1.869	573.400	–	–	839	40.814
June	2.183	64.179	1.948	596.348	860	91.257	812	33.805
July	–	–	1.963	551.953	841	107.097	–	–
August	2.347	72.677	2.018	554.457	872	108.168	891	27.209
September	2.307	62.283	1.791	406.015	800	89.603	–	–
October	2.328	67.066	1.886	343.674	845	108.605	902	32.056
November	2.279	61.281	–	–	–	–	863	26.999
December	2.436	62.758	2.001	460.519	–	–	845	27.828
2018	**ASNs**	**IPs**	**ASNs**	**IPs**	**ASNs**	**IPs**	**ASNs**	**IPs**
January	2.412	61.875	2.130	479.247	823	97.075	888	25.982
February	2.438	72.185	2.324	559.784	849	93.801	778	20.210
March	2.476	63.811	2.278	515.345	844	84.483	544	11.431

Legend: "–" means there was no notification of this category in a given month.

CPEs Compromised by Criminals: **to Change the DNS Resolver Information**

Compromised

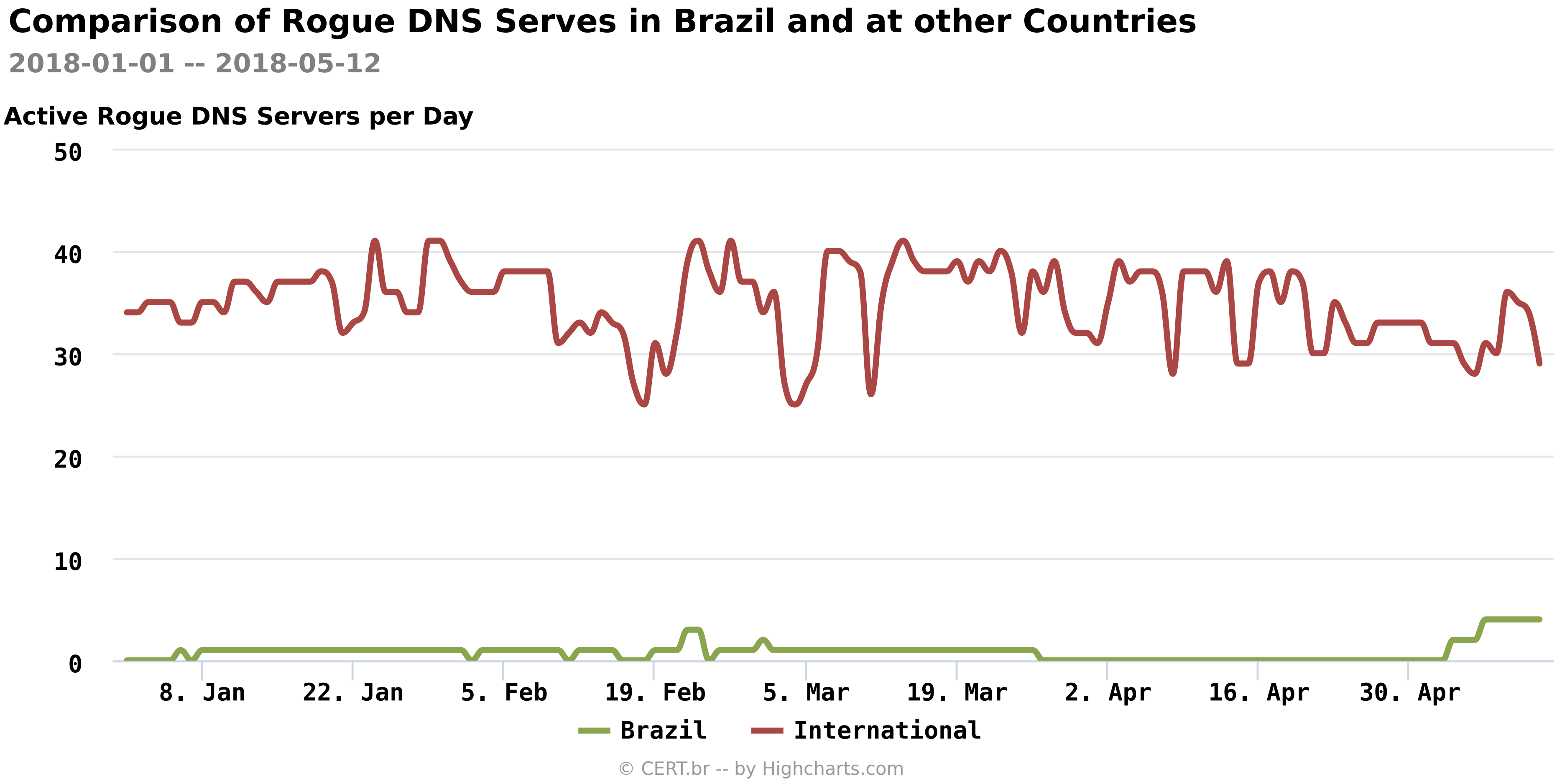
- via password brute force (usually via telnet)
  - could be either through the network or via a malware on the victims' computer
- exploiting vulnerabilities
- via CSRF attacks, using iFrames with malicious JavaScripts
  - These are left in legitimate servers compromised by the intruders

Attacks' Objectives

- **change the CPE's DNS configuration, so the DNS resolver is set to a server set up by the criminals**
- the criminals' DNS servers are hosted at hosting/cloud providers
  - some cases with more than 30 domains from social networks, e-mail providers, search engines, e-commerce, credit card companies, banks, etc

Note: CPE stands for "Consumer Premises Equipment", that is home routers/modems

Rogue DNS Servers online, daily statistics



Attacks Involving BGP (Route) Hijacking: **Objective is Financial Fraud**

Anatomy of the Attacks

- Attackers compromise small ISPs border routers
- Announce a more specific network prefix from the target’s organization address space (usually a /24)
  - the compromised ISP’s “peers” learn the new route affecting some prefixes of the targeted organization
  - clients of all ASNs that learned the new route are now redirected to a server under the attacker’s control
- These attacks started in March 2017 and are still ongoing

Strategies for Increasing Cybersecurity Readiness and Awareness in Brazil

Strategies to Increase Incident Handling Capacity: **CSIRTs, Capacity Building and Awareness**

CSIRTs

- support the creation of CSIRTs in all sectors
- create an environment for teams to
  - build trust
  - cooperate
- encourage a bottom-up approach to cooperation

Capacity Building

- champion the need for CSIRTs among C-Level Managers and VPs
- provide formal training on incident handling
  - focus on processes
- provide training to other professionals
  - best practices
  - focus on preventing incidents

Awareness

- technically sound material, but with simple language
- license is Creative Commons
  - anyone can use it
- current campaigns for
  - general public
  - children
  - youth
  - 60+

Establishment of new CSIRTs

Help new Computer Security Incident Response Teams (CSIRTs) to establish their activities

- meetings, training and presentations at conferences

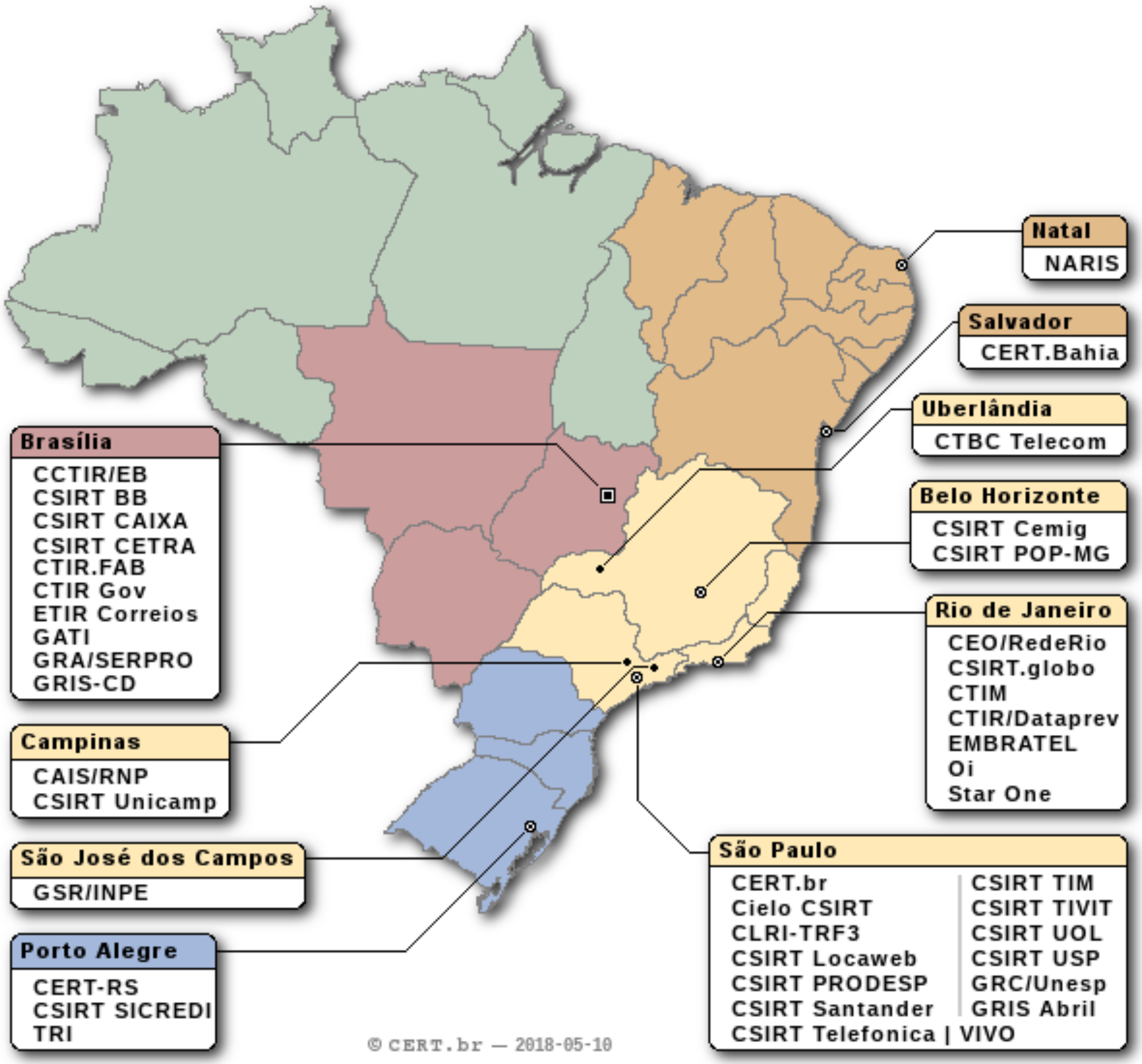
SEI/CMU Partner **since 2004, delivers in Brazil the following CERT® Program courses:**

- https://www.cert.br/courses/
  - *Overview of Creating and Managing CSIRTs*
  - *Fundamentals of Incident Handling*
  - *Advanced Incident Handling for Technical Staff*
- 800+ security professionals trained in Brazil
- *Overview of Creating and Managing CSIRTs* workshop delivered at 2008, 2009 and 2010 LACNIC Conferences, with permission
- Special training for the personnel that worked at the World Cup, Olympics and other Major Events

Brazilian CSIRTs - https://www.cert.br/csirts/brazil

List with 41 teams with services announced to the public

Sector	CSIRTs
National - Any Brazilian Network	CERT.br
National – Federal Public Administration	CTIR Gov
Government	CCTIR/EB, CLRI-TRF-3, CSIRT CETRA, CSIRT PRODESP, CTIM, CTIR.FAB, CTIR/Dataprev, ETIR Correios, GATI, GRA/SERPRO, GRIS-CD
Energy	CSIRT Cemig
Financial	Cielo CSIRT, CSIRT BB, CSIRT CAIXA, CSIRT Santander, CSIRT Sicredi
Telecom ISP Hosting	CSIRT Locaweb, CSIRT TIM, CSIRT TIVIT, CSIRT UOL, CSIRT Telefonica|VIVO, CTBC Telecom, EMBRATEL, StarOne, Oi
Academia	CAIS/RNP, CEO/RedeRio, CERT-RS, CERT.Bahia, CSIRT POP-MG, CSIRT Unicamp, CSIRT USP, GSR/INPE, GRC/UNESP, NARIS, TRI
Others	CSIRT.globo, GRIS Abril



Brasília
CCTIR/EB
CSIRT BB
CSIRT CAIXA
CSIRT CETRA
CTIR.FAB
CTIR Gov
ETIR Correios
GATI
GRA/SERPRO
GRIS-CD

Campinas
CAIS/RNP
CSIRT Unicamp

São José dos Campos
GSR/INPE

Porto Alegre
CERT-RS
CSIRT SICREDI
TRI

Natal
NARIS

Salvador
CERT.Bahia

Uberlândia
CTBC Telecom

Belo Horizonte
CSIRT Cemig
CSIRT POP-MG

Rio de Janeiro
CEO/RedeRio
CSIRT.globo
CTIM
CTIR/Dataprev
EMBRATEL
Oi
Star One

São Paulo
CERT.br
Cielo CSIRT
CLRI-TRF3
CSIRT Locaweb
CSIRT PRODESP
CSIRT Santander
CSIRT Telefonica | VIVO
CSIRT TIM
CSIRT TIVIT
CSIRT UOL
CSIRT USP
GRC/Unesp
GRIS Abril

© CERT.br — 2018-05-10

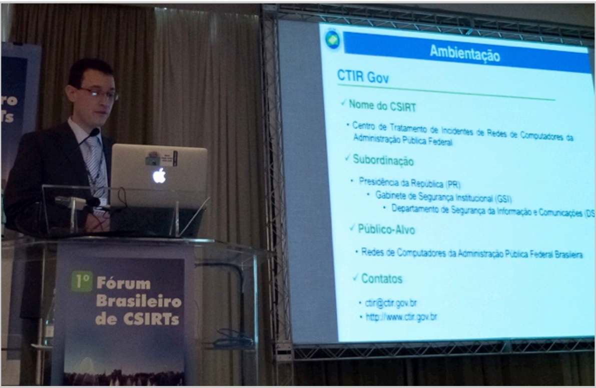
Brazilian CSIRTs Forum

Annual Conference (Free)

- 2012: 1st Event, co-located with the FIRST Regional Symposium
- 2017: celebrated CERT.br's 20 years
- 2018: call for presentations open
  https://cert.br/forum2018/cfp/

Focus on

- Best Practices
  - national and international
- Case Studies
- Cooperation
  - plenty of networking opportunities!



Best Current Practices Portal and Training
https://bcp.nic.br/

Audience: Network Operators

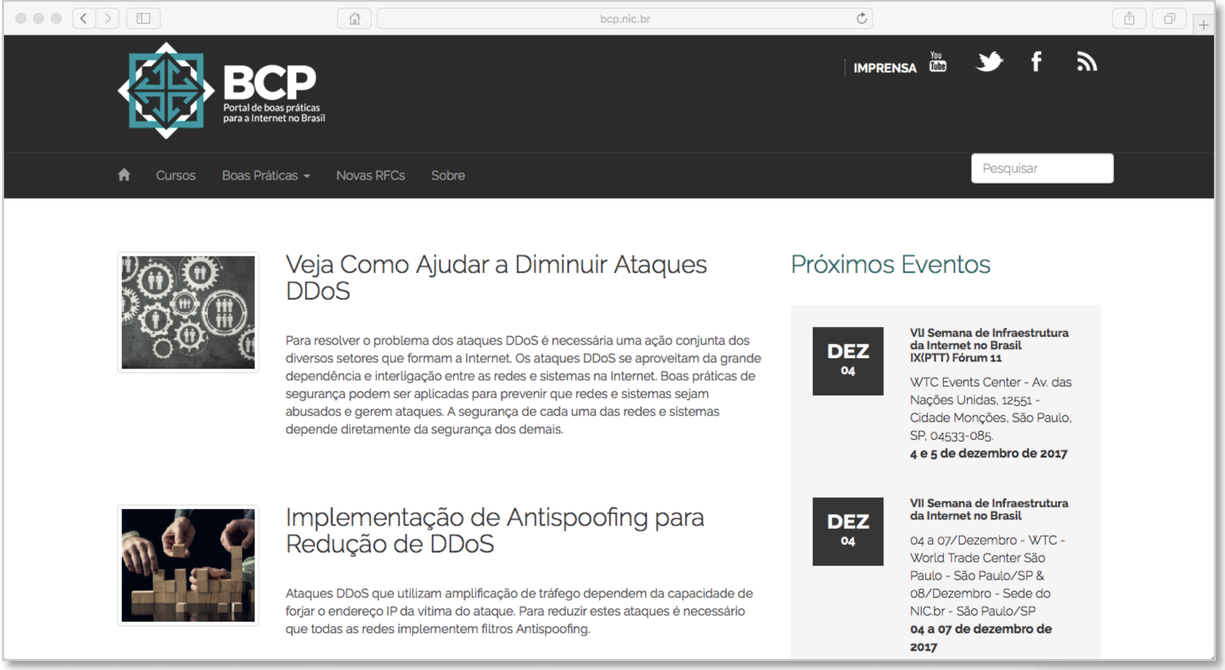
Objective is improve the Internet resilience:

- Routing and BGP
- Antispoofing and CPE management
- DDoS reduction and mitigation

Part of the Initiative "*Por uma Internet mais Segura*", which involves ISPs and Telcos

International Partners:

- ISOC – MANRS.org
- IETF – BCP 38 (antispoofing)
- M^{3}AAWG, LAC-AAWG, LACNOG and LACNIC: BCOP for CPE's acquisition requirements



Veja Como Ajudar a Diminuir Ataques DDoS

Para resolver o problema dos ataques DDoS é necessária uma ação conjunta dos diversos setores que formam a Internet. Os ataques DDoS se aproveitam da grande dependência e interligação entre as redes e sistemas na Internet. Boas práticas de segurança podem ser aplicadas para prevenir que redes e sistemas sejam abusados e gerem ataques. A segurança de cada uma das redes e sistemas depende diretamente da segurança dos demais.

Implementação de Antispoofing para Redução de DDoS

Ataques DDoS que utilizam amplificação de tráfego dependem da capacidade de forjar o endereço IP da vítima do ataque. Para reduzir estes ataques é necessário que todas as redes implementem filtros Antispoofing.

Próximos Eventos

DEZ 04

VII Semana de Infraestrutura da Internet no Brasil IX(PTT) Fórum 11

WTC Events Center - Av. das Nações Unidas, 12551 - Cidade Monções, São Paulo, SP, 04533-085.
4 e 5 de dezembro de 2017

DEZ 04

VII Semana de Infraestrutura da Internet no Brasil

04 a 07/Dezembro - WTC - World Trade Center São Paulo - São Paulo/SP & 08/Dezembro - Sede do NIC.br - São Paulo/SP
04 a 07 de dezembro de 2017

Security is inherently multistakeholder: **Cooperation for a Healthy Internet Ecosystem**

No single group or body will be able to achieve better security or incident response on its own – all stakeholders have a role

Universities

- need to include security considerations in all disciplines

Developers / vendors

- need to think about security in all phases of development, including its initial design

Managers / C-level executives

- need to consider security as an investment and allocate adequate resources

System and network administrators, and security professionals

- should strive to stop emanating “polution” from their networks
- must adopt best practices

End users

- need to understand the risks and follow security tips
- need to update their devices and recover from infections

Yet, attacks and security incidents will occur

- https://cert.br/csirts/brazil/   https://www.first.org/members/

Antispam Multistakeholder Success Case: **Port 25 Management Adoption in Brazil**

Port 25 Management in Brazil depended on a coordinated effort:

- 1st: ISPs offering Message Submission services and changing at least 90% of their clients' configuration
- 2nd:Telcos blocking outbound port 25 traffic – residential networks only

A formal implementation agreement was signed

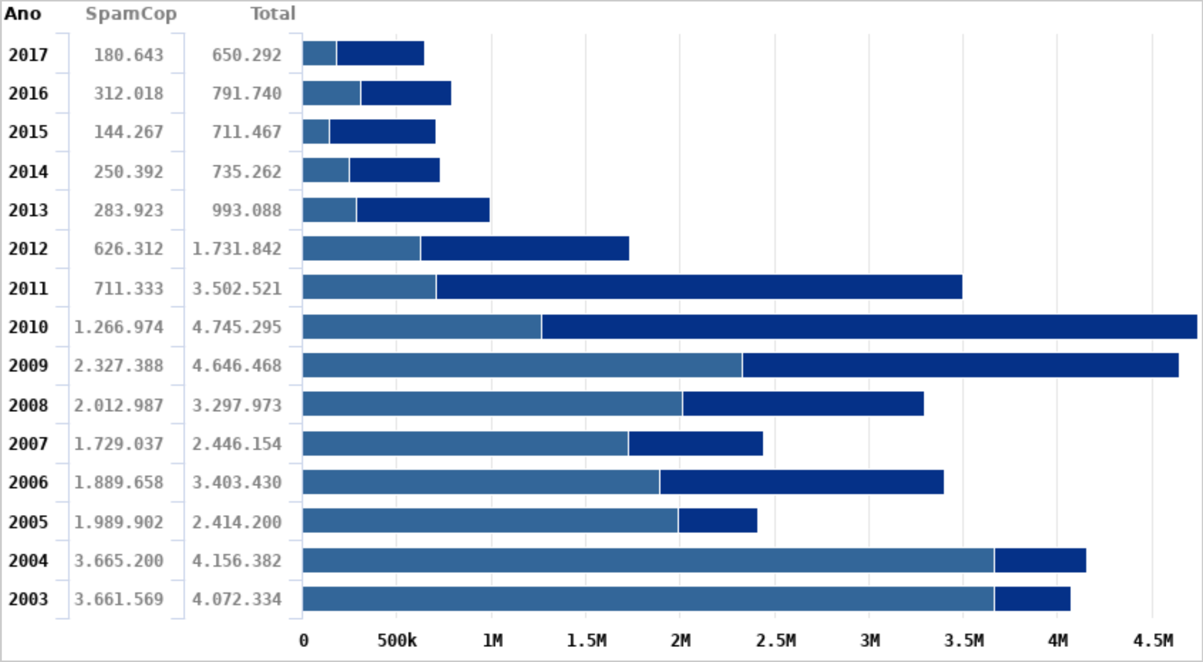
- CGI.br, NIC.br, Anatel, Telcos and ISP's Associations
- The consumer protection associations supported formally the agreement

Once the agreement was signed, NIC.br/CERT.br started a national awareness campaign about

- the importance of these measures
- the impact on the consumers
- part of the already existing Antispam.br Awareness Campaign

Antispam Multistakeholder Success Case: **Results of the Efforts**

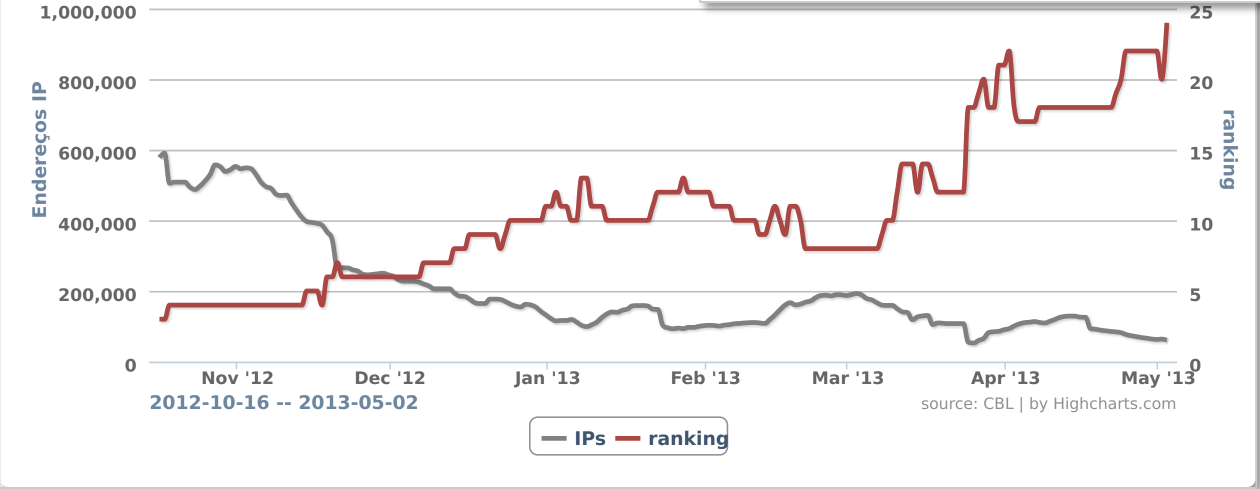
- **Spam complaints reduced in 2013 and remain low since then**



Ano	SpamCop	Total
2017	180.643	650.292
2016	312.018	791.740
2015	144.267	711.467
2014	250.392	735.262
2013	283.923	993.088
2012	626.312	1.731.842
2011	711.333	3.502.521
2010	1.266.974	4.745.295
2009	2.327.388	4.646.468
2008	2.012.987	3.297.973
2007	1.729.037	2.446.154
2006	1.889.658	3.403.430
2005	1.989.902	2.414.200
2004	3.665.200	4.156.382
2003	3.661.569	4.072.334

Brasil (BR) na

IPs listados e evolução r



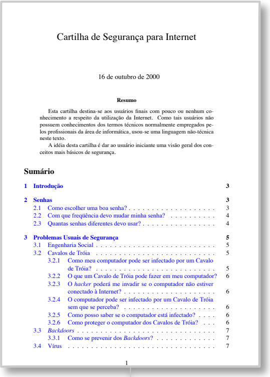
2012-10-16 -- 2013-05-02

source: CBL | by Highcharts.com

- **From CBL number 1 in 2009 to 25 in 2013**
  - The deadline for the implementation was March 2013

General Public Awareness Materials and Campaign:
Internet Security Booklet – Evolution

1.0



Cartilha de Segurança para Internet

16 de outubro de 2000

Resumo

Esta cartilha destina-se aos usuários finais com pouco ou nenhum conhecimento a respeito da utilização da Internet. Como tais usuários não possuem conhecimentos dos termos técnicos normalmente empregados pelos profissionais da área de informática, usou-se uma linguagem não-técnica neste texto.

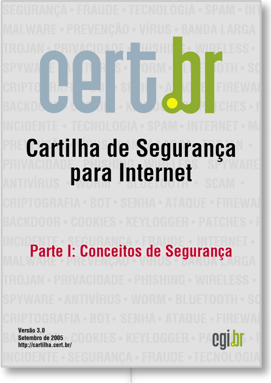
A idéia desta cartilha é dar ao usuário iniciante uma visão geral dos conceitos mais básicos de segurança.

Sumário

1

- **20 pages**
- **basic concepts**
- **FAQ format**

3.0



cert.br

Cartilha de Segurança para Internet

Parte I: Conceitos de Segurança

Versão 3.0
Setembro de 2005
http://cartilha.cert.br/

cgi.br

- **included a dedicated malware section**
- **folder with tips**

- **illustrated**
- **eBook (ePub)**
- **new topics: social networks and mobile**

4.0

Cartilha de Segurança para Internet

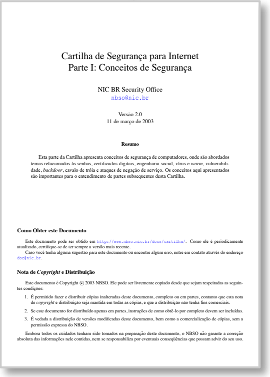
Publicação cert.br

http://cartilha.cert.br/

nic.br cgi.br

2000 2003 2005 2006 2012

- **became a set of documents**
- **Internet Fraud topic added**



Cartilha de Segurança para Internet
Parte I: Conceitos de Segurança

NIC BR Security Office
nbso@nic.br

Versão 2.0
11 de março de 2003

Resumo

Esta parte da Cartilha apresenta conceitos de segurança de computadores, onde são abordados temas relacionados às senhas, certificados digitais, engenharia social, vírus e *worm*, vulnerabilidade, *backdoor*, cavalo de tróia e ataques de negação de serviço. Os conceitos aqui apresentados são importantes para o entendimento de partes subseqüentes desta Cartilha.

Como Obter este Documento

Este documento pode ser obtido em http://www.nbso.nic.br/docs/cartilha/. Como ele é periodicamente atualizado, certifique-se de ter sempre a versão mais recente.

Caso você tenha alguma sugestão para este documento ou encontre algum erro, entre em contato através do endereço doc@nic.br.

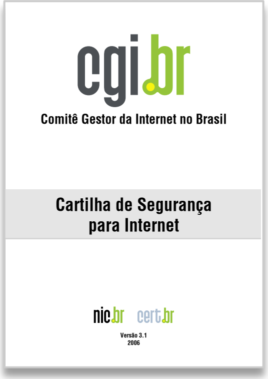
Nota de *Copyright* e Distribuição

Este documento é Copyright © 2003 NBSO. Ele pode ser livremente copiado desde que sejam respeitadas as seguintes condições:

1. É permitido fazer e distribuir cópias inalteradas deste documento, completo ou em partes, contanto que esta nota de *copyright* e distribuição seja mantida em todas as cópias, e que a distribuição não tenha fins comerciais.
2. Se este documento for distribuído apenas em partes, instruções de como obtê-lo por completo devem ser incluídas.
3. É vedada a distribuição de versões modificadas deste documento, bem como a comercialização de cópias, sem a permissão expressa do NBSO.

Embora todos os cuidados tenham sido tomados na preparação deste documento, o NBSO não garante a correção absoluta das informações nele contidas, nem se responsabiliza por eventuais conseqüências que possam advir do seu uso.

2.0



cgi.br

Comitê Gestor da Internet no Brasil

Cartilha de Segurança para Internet

nic.br cert.br

Versão 3.1
2006

3.1

- **released for the first time as a book with ISBN**

Segurança em redes sociais

Cartilha de Segurança para Internet

Fascículo Redes Sociais

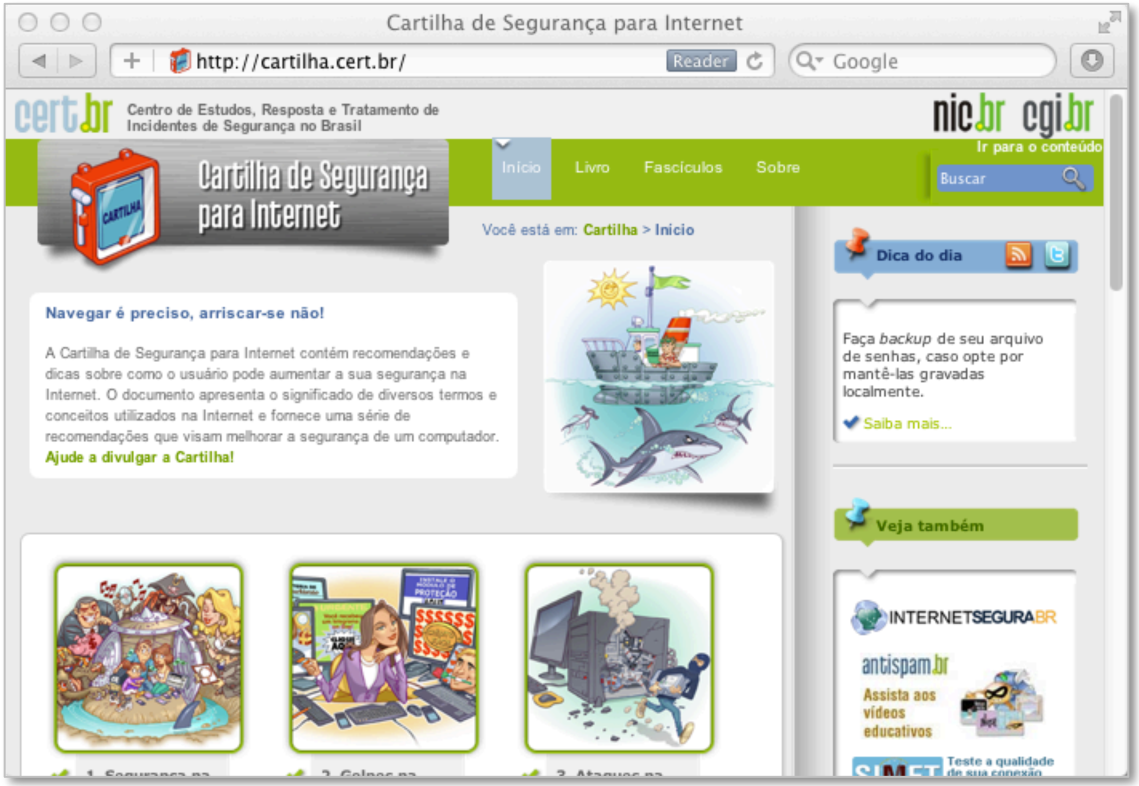
nic.br cgi.br

- **slides & fascicles**

Book and Website

All material online (Creative Commons License)
https://cartilha.cert.br/

➔ **Spanish Version sponsored by ISOC**
https://cartilla.cert.br/



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

Você está em: Cartilha > Início

Navegar é preciso, arriscar-se não!

A Cartilha de Segurança para Internet contém recomendações e dicas sobre como o usuário pode aumentar a sua segurança na Internet. O documento apresenta o significado de diversos termos e conceitos utilizados na Internet e fornece uma série de recomendações que visam melhorar a segurança de um computador.
Ajude a divulgar a Cartilha!

Dica do dia

Faça *backup* de seu arquivo de senhas, caso opte por mantê-las gravadas localmente.

✓ Saiba mais...

Veja também

INTERNETSEGURA.BR

antispam.br
Assista aos vídeos educativos

SIMET Teste a qualidade de sua conexão

Used as reference in

- Law schools
- Test study material for public servants’ tests

Partnerships for printing and distribution

- Microsoft DCU
- Itaipu Binacional
- ELO
- PROCERGS

Support Material for Trainers and Teachers

Shorter versions focused on:

- Social Networks
- Passwords
- e-Commerce
- Privacy
- Mobile Devices
- Internet Banking
- Computers
- Malicious Code
- Two-factor Authentication
- Networks
- Backup
- Hoaxes and Fake News

Companion *slides* for:

- presentations and training
- complementing classes

2016/2017: Ransomware and Backup

- **New character: ransomware**
  - **Slogan: Do you have backup?**
- **Updated the Malicious Code material**
- **Created a leaflet specially for SMEs**
- **New character: backup**

BACKUP
CERT.br/NIC
Cartilha de Segurança para Internet
Fascículo Backup
BACKUP
cert.br
https://cartilha.cert.br/
nic.br
cgi.br
Cartilha de Segurança para Internet
Fascículo Códigos Maliciosos
cert.br
nic.br
cgi.br

RANSOMWARE

Você tem BACKUP?

Quando você copiou seus arquivos pela última vez?
Proteja-se de *ransomware* e preserve seus dados!

Você sabe o que é *ransomware*?

Ransomware é um tipo de código malicioso que torna inacessíveis os dados armazenados em um equipamento, geralmente usando criptografia, e que exige pagamento de resgate (*ransom*) para restabelecer o acesso ao usuário.

Como devo me proteger de *ransomware*?

Para se proteger de *ransomware* você deve tomar os mesmos cuidados que toma para evitar os outros códigos maliciosos, como ter um antivírus instalado e ser cuidadoso ao clicar em *links* ou abrir arquivos.

Fazer *backups* regularmente também é essencial para proteger os seus dados pois, se seu equipamento for infectado, a única garantia de que você conseguirá acessá-los novamente é possuir *backups* atualizados. O pagamento do resgate não garante que você conseguirá restabelecer o acesso aos dados.

Onde encontro mais informações?

Para saber mais sobre *ransomware* acesse: **cartilha.cert.br/ransomware**

May/2018: Hoaxes and Fake News

- **New character**
  - **Fake News**
- **Focus on how to identify false narratives, scams and hoaxes**

CC CERT.br/NIC.br

Cartilha de Segurança para Internet

Fascículo Boatos

Publicação cert.br

Terra Pl
Canais de Veneza ficam congelados
Político corrupto abduzido por ovni
Fim do mundo no próximo final de semana
Brasileiro inventa carro movido a suco de laranja
Alien Marte

https://cartilha.cert.br/

nic.br cgi.br

Completely New Focus and Language: **Kids and Parents**

INTERNET SEGURA
DIVIRTA-SE E APRENDA A USAR A INTERNET DE FORMA SEGURA!
INTERNET SEGURA
PARA SEUS FILHOS
UA PARTICIPAÇÃO É MUITO IMPORTANTE!

INTERNET SEGURA.BR

http://internetsegura.br/

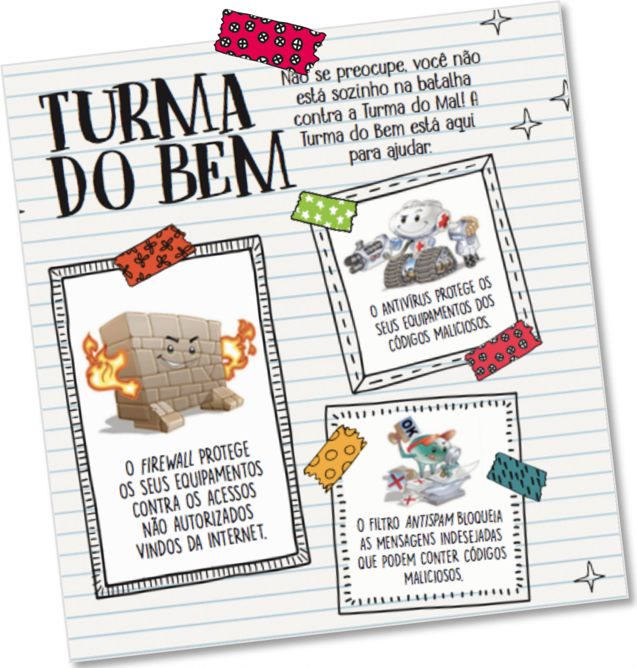
CUIDADO COM PESSOAS ESTRANHAS OU QUE VOCÊ CONHECE APENAS PELA INTERNET

Você já deve ter escutado dos seus pais e de outros adultos para não falar com estranhos. Na Internet é a mesma coisa, você deve falar com quem você realmente conhece.

Se algum estranho tentar falar com você na Internet ou lhe adicionar em alguma rede social, chame seus pais. Infelizmente nem todo mundo é legal e diz a verdade – seus pais podem lhe ajudar a lidar com isso.

SEJA VOCÊ MESMO!
VOCÊ GOSTARIA DE DESCOBRIR QUE AQUELE AMIGO QUE VOCÊ CONHECEU NA INTERNET NÃO É QUEM ELE DIZIA SER? PROVAVELMENTE NÃO. ENTÃO NÃO FAÇA ISSO COM AS OUTRAS PESSOAS. NÃO CRIE PERFIS FALSOS (*FAKES*) E NEM TENTE SE PASSAR POR QUEM VOCÊ NÃO É. ISSO É ERRADO E PODE TRAZER PROBLEMAS AOS SEUS PAIS.

CUIDADO COM O QUE VOCÊ COMPARTILHA



TURMA DO BEM

Não se preocupe, você não está sozinho na batalha contra a Turma do Mal! A Turma do Bem está aqui para ajudar.

O ANTIVÍRUS PROTEGE OS SEUS EQUIPAMENTOS DOS CÓDIGOS MALICIOSOS.
O *FIREWALL* PROTEGE OS SEUS EQUIPAMENTOS CONTRA OS ACESSOS NÃO AUTORIZADOS VINDOS DA INTERNET.
O FILTRO *ANTISPAM* BLOQUEIA AS MENSAGENS INDESEJADAS QUE PODEM CONTER CÓDIGOS MALICIOSOS.

PROTEJA OS SEUS EQUIPAMENTOS

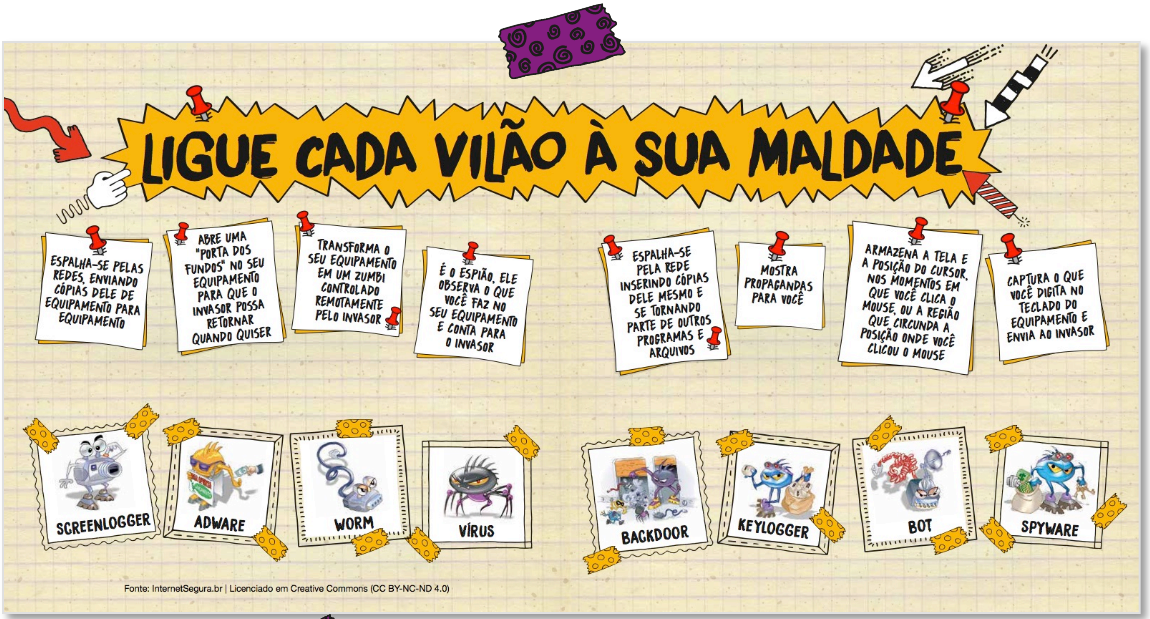
INFELIZMENTE, AO USAR A INTERNET, VOCÊ PODE SE DEPARAR COM A TURMA DO MAL.

A TURMA DO MAL É FORMADA POR VILÕES QUE CRIAM ARMADILHAS PARA TENTAR INFECTAR OS SEUS EQUIPAMENTOS E ACESSAR AS SUAS INFORMAÇÕES.

Esses vilões, também chamados de códigos maliciosos (*malware*), são programas feitos para executar ações danosas e maliciosas nos seus equipamentos.

Seus equipamentos podem cair nas armadilhas deixadas pela Turma do Mal se estiverem com os aplicativos desatualizados, se você abrir arquivos infectados, ou ainda, se ficar acessando *sites* inseguros.

PARA COLORIR



LIGUE CADA VILÃO À SUA MALDADE

ESPALHA-SE PELAS REDES, ENVIANDO CÓPIAS DELE DE EQUIPAMENTO PARA EQUIPAMENTO

ABRE UMA "PORTA DOS FUNDOS" NO SEU EQUIPAMENTO PARA QUE O INVASOR POSSA RETORNAR QUANDO QUISER

TRANSFORMA O SEU EQUIPAMENTO EM UM ZUMBI CONTROLADO REMOTAMENTE PELO INVASOR

É O ESPIÃO, ELE OBSERVA O QUE VOCÊ FAZ NO SEU EQUIPAMENTO E CONTA PARA O INVASOR

ESPALHA-SE PELA REDE INSERINDO CÓPIAS DELE MESMO E SE TORNANDO PARTE DE OUTROS PROGRAMAS E ARQUIVOS

MOSTRA PROPAGANDAS PARA VOCÊ

ARMAZENA A TELA E A POSIÇÃO DO CURSOR, NOS MOMENTOS EM QUE VOCÊ CLICA O MOUSE, OU A REGIÃO QUE CIRCUNDA A POSIÇÃO ONDE VOCÊ CLICOU O MOUSE

CAPTURA O QUE VOCÊ DIGITA NO TECLADO DO EQUIPAMENTO E ENVIA AO INVASOR

Fonte: InternetSegura.br | Licenciado em Creative Commons (CC BY-NC-ND 4.0)

CAÇA-PALAVRAS

AJUDE A "CAÇAR" A GALERA DO MAL:

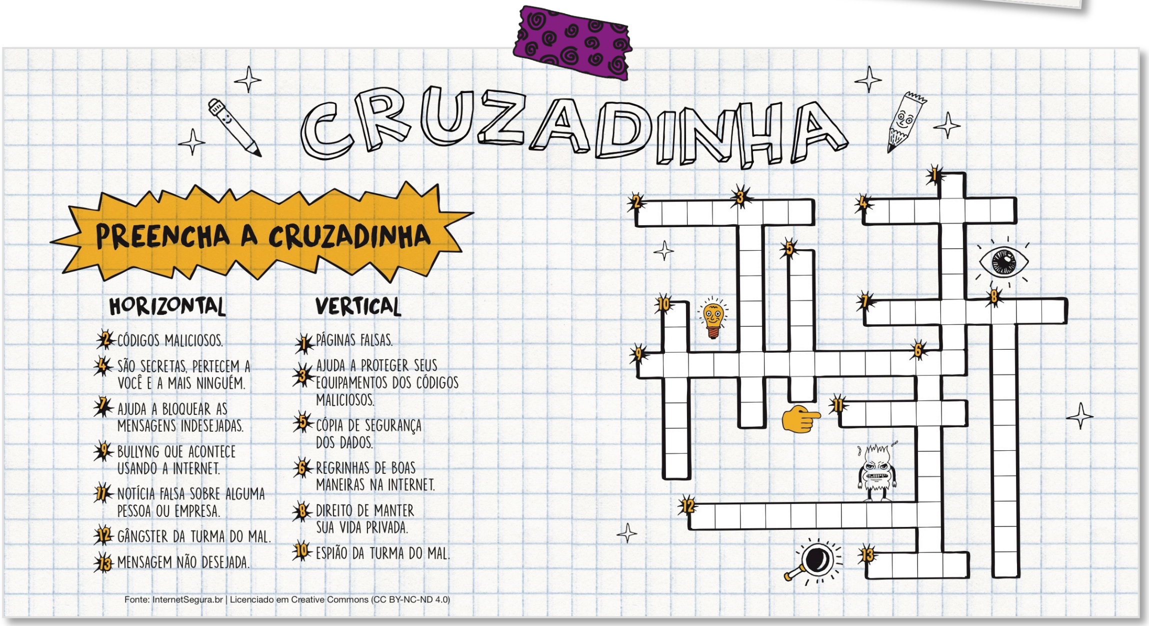
VÍRUS ▪ WORM ▪ BOT ▪ SPYWARE ▪ KEYLOGGER ▪ SCREENLOGGER
ADWARE ▪ BACKDOOR ▪ TROJAN ▪ ROOTKIT ▪ RANSOMWARE

T	P	I	Y	J	L	A	D	W	A	R	E	Q	P	E
F	T	V	A	C	J	Y	Q	V	Í	R	U	S	E	G
S	S	B	T	R	O	J	A	N	N	A	D	D	W	L
P	C	V	L	W	H	E	D	B	S	N	P	R	O	K
Y	R	R	O	O	T	K	I	T	U	S	O	J	Z	B
W	E	Z	N	R	O	R	Y	F	Q	O	K	J	Z	O
A	E	K	D	M	H	X	N	M	D	M	E	J	V	T
R	N	M	W	K	J	I	V	K	Z	W	Y	I	Z	M
E	L	E	T	A	D	A	C	V	I	A	L	E	F	H
G	O	B	A	Z	V	A	M	G	H	R	O	C	P	E
U	G	Z	A	E	B	Z	T	O	U	E	G	D	X	S
C	G	T	R	N	A	J	U	U	S	Q	G	B	D	E
A	E	E	T	H	Q	P	T	I	E	R	E	O	T	H
J	R	Z	I	X	X	K	T	Z	Y	V	R	U	X	P

Fonte: InternetSegura.br | Licenciado em Creative Commons (CC BY-NC-ND 4.0)

JOGO DOS 7 ERROS

Fonte: InternetSegura.br | Licenciado em Creative Commons (CC BY-NC-ND 4.0)



CRUZADINHA

PREENCHA A CRUZADINHA

HORIZONTAL

2 CÓDIGOS MALICIOSOS.

4 SÃO SECRETAS, PERTECEM A VOCÊ E A MAIS NINGUÉM.

7 AJUDA A BLOQUEAR AS MENSAGENS INDESEJADAS.

9 BULLYNG QUE ACONTECE USANDO A INTERNET.

11 NOTÍCIA FALSA SOBRE ALGUMA PESSOA OU EMPRESA.

12 GÂNGSTER DA TURMA DO MAL.

13 MENSAGEM NÃO DESEJADA.

VERTICAL

1 PÁGINAS FALSAS.

3 AJUDA A PROTEGER SEUS EQUIPAMENTOS DOS CÓDIGOS MALICIOSOS.

5 CÓPIA DE SEGURANÇA DOS DADOS.

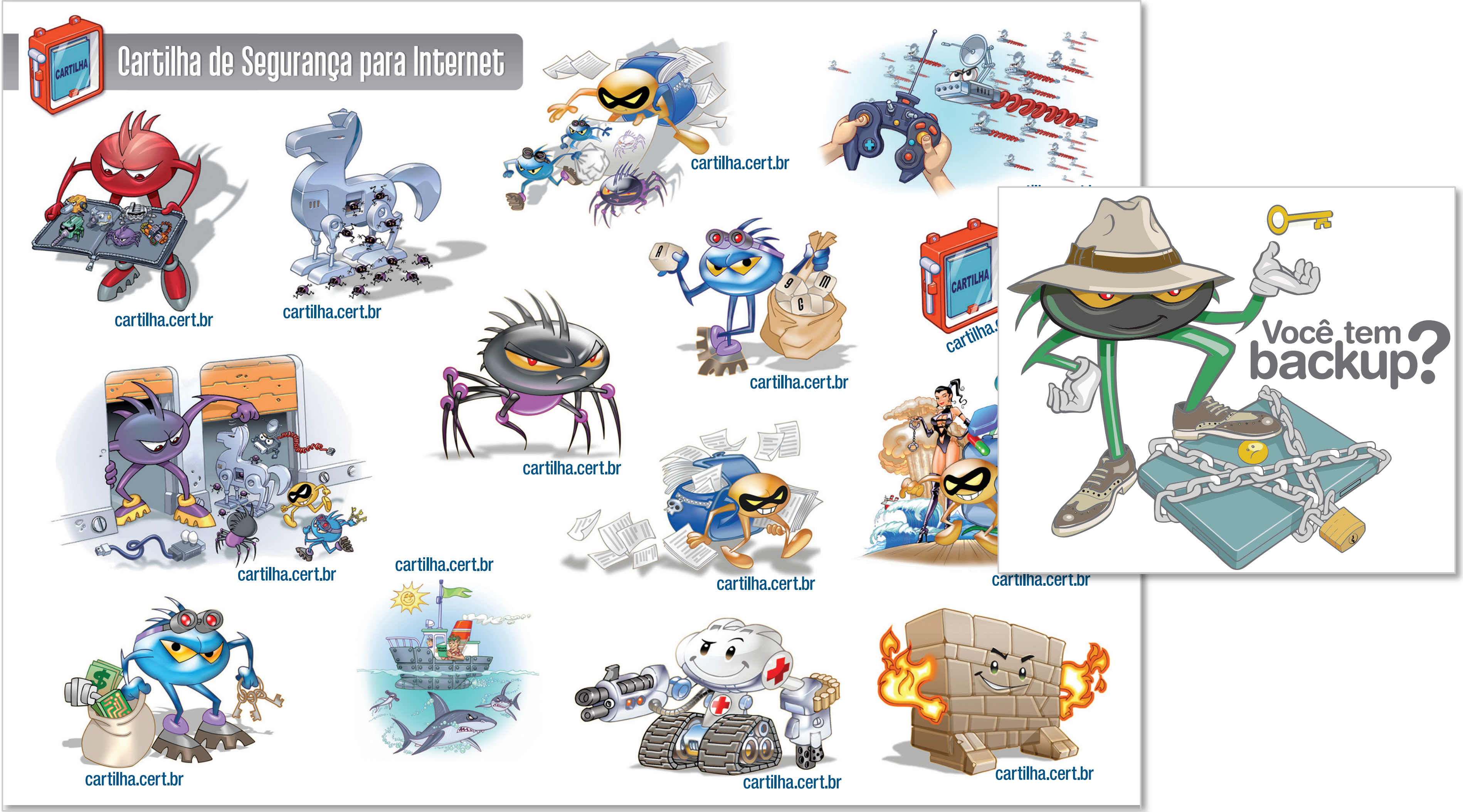
6 REGRINHAS DE BOAS MANEIRAS NA INTERNET.

8 DIREITO DE MANTER SUA VIDA PRIVADA.

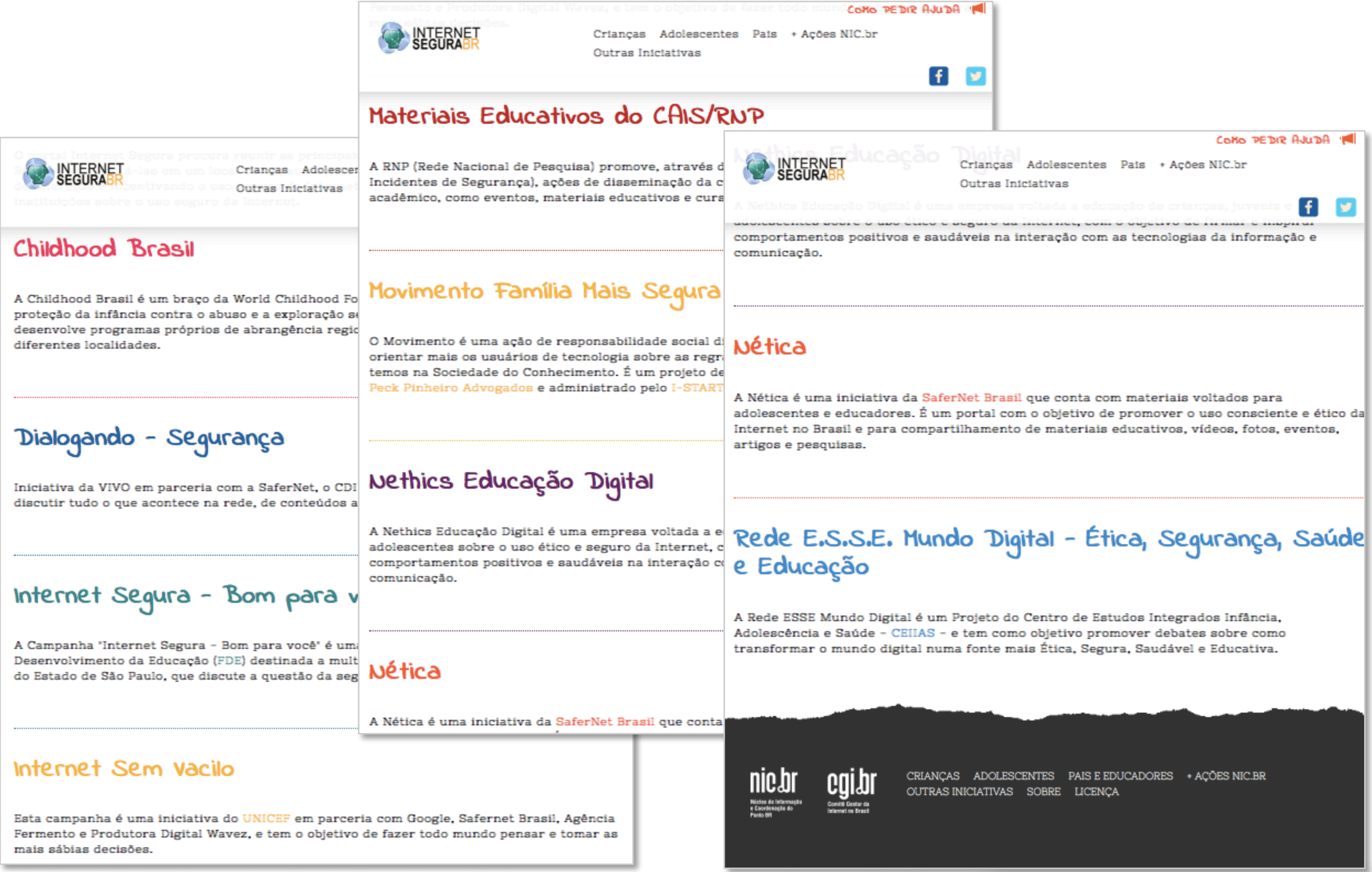
10 ESPIÃO DA TURMA DO MAL.

Fonte: InternetSegura.br | Licenciado em Creative Commons (CC BY-NC-ND 4.0)

Stickers with the main characters



http://internetsegura.br/ – Other Brazilian Initiatives



Childhood Brasil

A Childhood Brasil é um braço da World Childhood Fo
proteção da infância contra o abuso e a exploração se
desenvolve programas próprios de abrangência regio
diferentes localidades.

Dialogando - Segurança

Iniciativa da VIVO em parceria com a SaferNet, o CDI
discutir tudo o que acontece na rede, de conteúdos a

Internet Segura - Bom para v

A Campanha "Internet Segura - Bom para você" é uma
Desenvolvimento da Educação (FDE) destinada a mult
do Estado de São Paulo, que discute a questão da seg

Internet Sem Vacilo

Esta campanha é uma iniciativa do UNICEF em parceria com Google, Safernet Brasil, Agência Fermento e Produtora Digital Wavez, e tem o objetivo de fazer todo mundo pensar e tomar as mais sábias decisões.

Materiais Educativos do CAIS/RNP

A RNP (Rede Nacional de Pesquisa) promove, através d
Incidentes de Segurança), ações de disseminação da c
acadêmico, como eventos, materiais educativos e curs

Movimento Família Mais Segura

O Movimento é uma ação de responsabilidade social d
orientar mais os usuários de tecnologia sobre as regr
temos na Sociedade do Conhecimento. É um projeto de
Peck Pinheiro Advogados e administrado pelo I-START

Nethics Educação Digital

A Nethics Educação Digital é uma empresa voltada a e
adolescentes sobre o uso ético e seguro da Internet, c
comportamentos positivos e saudáveis na interação c
comunicação.

Nética

A Nética é uma iniciativa da SaferNet Brasil que conta

comportamentos positivos e saudáveis na interação com as tecnologias da informação e comunicação.

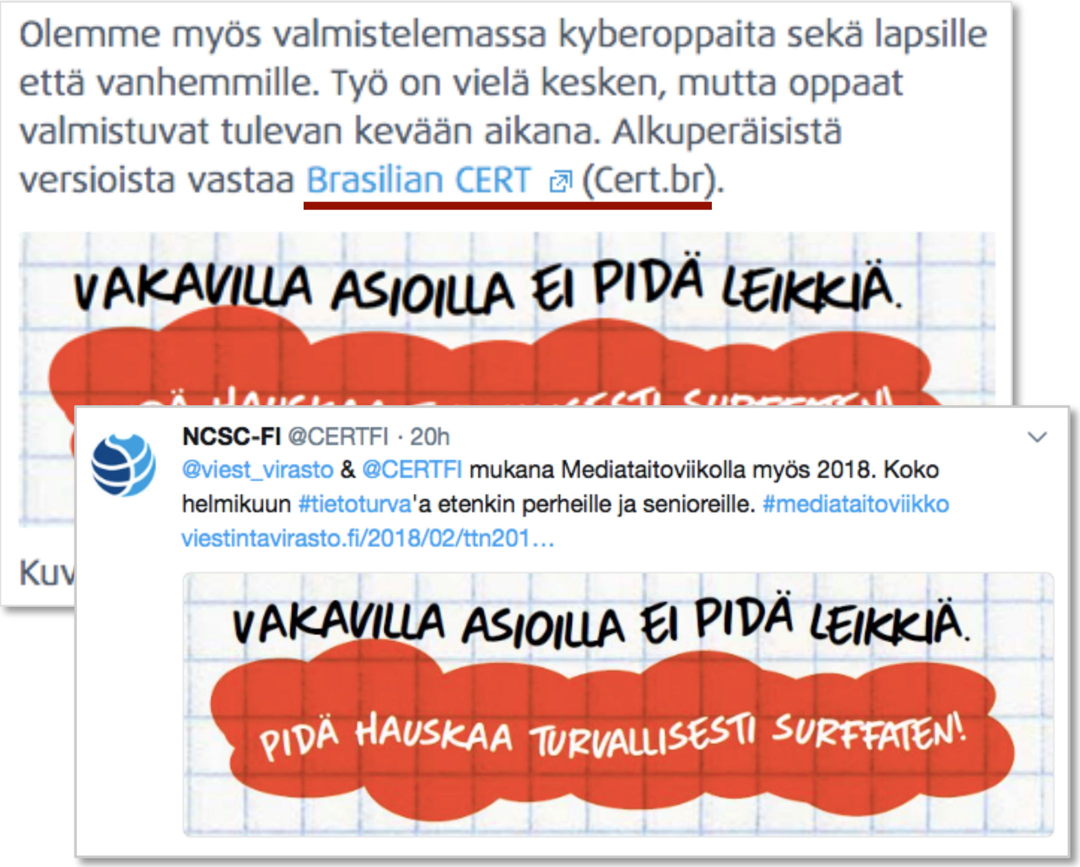
Nética

A Nética é uma iniciativa da SaferNet Brasil que conta com materiais voltados para adolescentes e educadores. É um portal com o objetivo de promover o uso consciente e ético da Internet no Brasil e para compartilhamento de materiais educativos, vídeos, fotos, eventos, artigos e pesquisas.

Rede E.S.S.E. Mundo Digital - Ética, Segurança, Saúde e Educação

A Rede ESSE Mundo Digital é um Projeto do Centro de Estudos Integrados Infância, Adolescência e Saúde - CEIIAS - e tem como objetivo promover debates sobre como transformar o mundo digital numa fonte mais Ética, Segura, Saudável e Educativa.

Partnership with Finland CERT (NCSC-FI):
Children material will be used in Finland



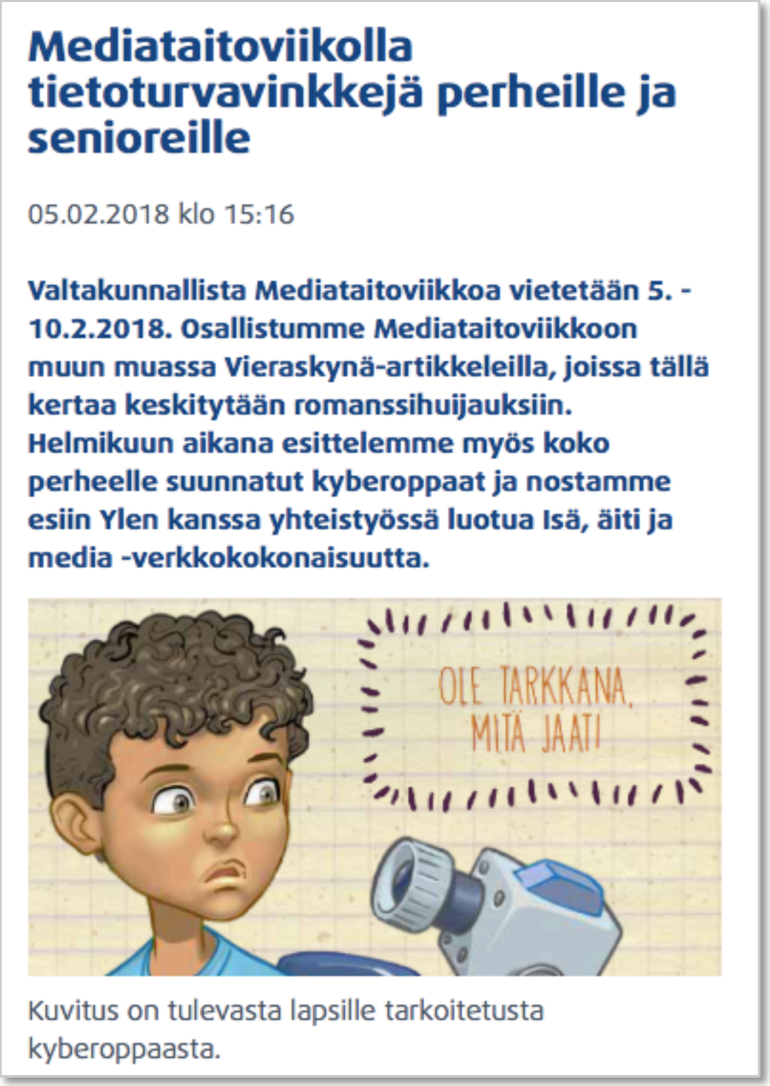
Olemme myös valmistelemassa kyberoppaita sekä lapsille että vanhemmille. Työ on vielä kesken, mutta oppaat valmistuvat tulevan kevään aikana. Alkuperäisistä versioista vastaa Brasilian CERT (Cert.br).

Kuv

NCSC-FI @CERTFI · 20h

@viest_virasto & @CERTFI mukana Mediataitoviikolla myös 2018. Koko helmikuun #tietoturva'a etenkin perheille ja senioreille. #mediataitoviikko viestintavirasto.fi/2018/02/ttn201…

VAKAVILLA ASIOILLA EI PIDÄ LEIKKIÄ.
PIDÄ HAUSKAA TURVALLISESTI SURFFATEN!



Mediataitoviikolla tietoturvavinkkejä perheille ja senioreille

05.02.2018 klo 15:16

Valtakunnallista Mediataitoviikkoa vietetään 5. - 10.2.2018. Osallistumme Mediataitoviikkoon muun muassa Vieraskynä-artikkeleilla, joissa tällä kertaa keskitytään romanssihuijauksiin. Helmikuun aikana esittelemme myös koko perheelle suunnatut kyberoppaat ja nostamme esiin Ylen kanssa yhteistyössä luotua Isä, äiti ja media -verkkokokonaisuutta.

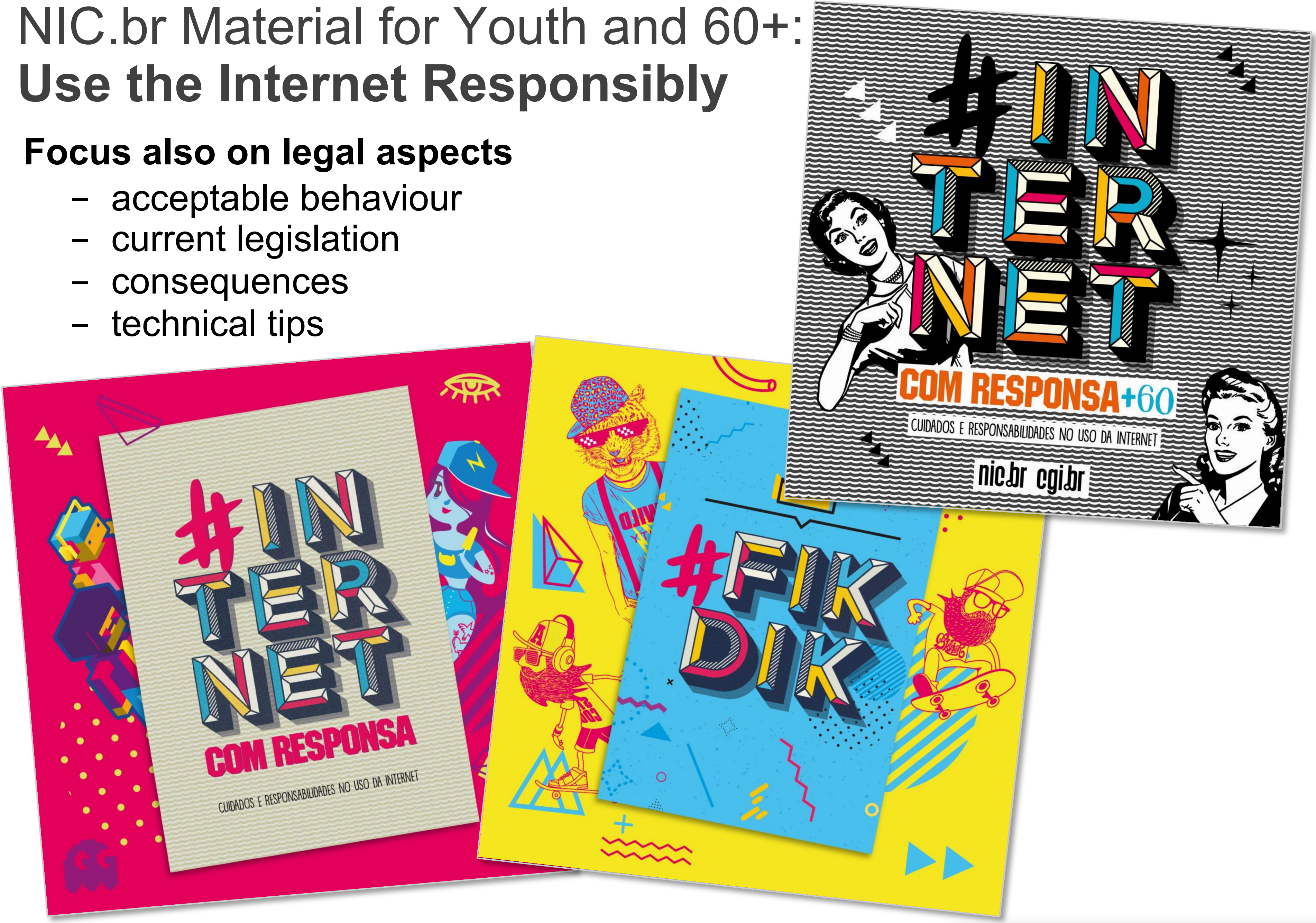
Kuvitus on tulevasta lapsille tarkoitetusta kyberoppaasta.

https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2018/02/ttn201802051516.html

NIC.br Material for Youth and 60+: **Use the Internet Responsibly**

Focus also on legal aspects

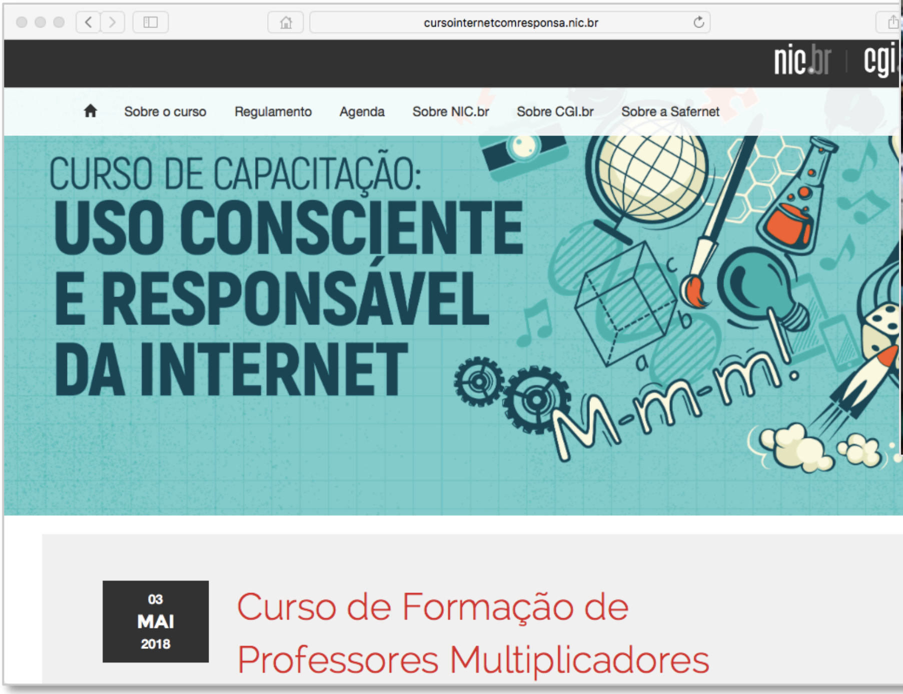
- acceptable behaviour
- current legislation
- consequences
- technical tips


#INTERNET
COM RESPONSA
CUIDADOS E RESPONSABILIDADES NO USO DA INTERNET
#FIKDIK
#INTERNET
COM RESPONSA+60
CUIDADOS E RESPONSABILIDADES NO USO DA INTERNET
nic.br cgi.br

NIC.br Training for K12 Teachers

Free training for teachers

- technical aspects
- legal aspects
- how to use our materials
- where to find more information



cursointernetcomresponsa.nic.br

CURSO DE CAPACITAÇÃO:
USO CONSCIENTE
E RESPONSÁVEL
DA INTERNET

03
MAI
2018

Curso de Formação de Professores Multiplicadores

http://www.cursointernetcomresponsa.nic.br

Thank You

www.cert.br

cristine@cert.br

@certbr

May 16, 2018

20 anos cert.br

nic.br cgi.br

www.nic.br | www.cgi.br