

nic.br cgi.br

20 anos
cert.br

Conselho do CGI.br
São Paulo – SP
23 de novembro de 2018

CERT.br

Atividades

Cristine Hoepers, D.Sc.
Gerente Geral
cristine@cert.br

Klaus Steding-Jessen, D.Sc.
Gerente Técnico
jessen@cert.br

20cert.br nic.br egi.br

Histórico:

Criação e Missão do CERT.br

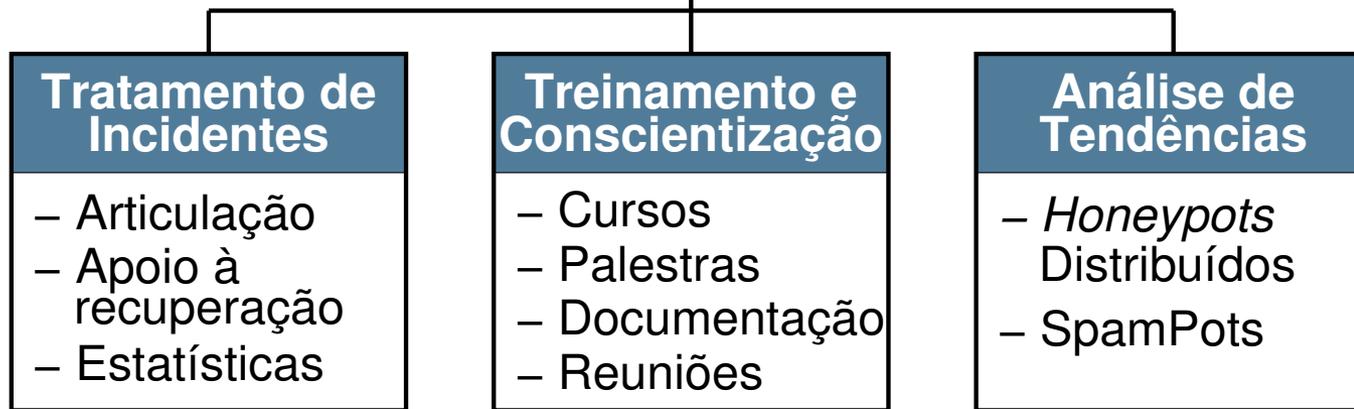
Agosto/1996: o relatório “Rumo à Criação de uma Coordenadoria de Segurança de Redes na Internet Brasil” é publicado pelo **CGI.br**¹

- Levantamento da situação no País
- Definição de prioridades
- Levantamento do melhor modelo para agir como facilitador para o tratamento de incidentes de segurança
 - grupo 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 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 grupo com responsabilidade nacional²

¹<https://www.nic.br/grupo/historico-gts.htm>

²<https://www.nic.br/pagina/gts/157>



Principais atividades:

Tratamento de Incidentes

- Ponto de contato nacional para notificação de incidentes
- Atua facilitando o processo de resposta a incidentes das várias organizações
- Trabalha em colaboração com outras entidades
- Auxilia novos CSIRTs (Grupos de Tratamento de Incidentes de Segurança) a estabelecerem suas atividades

Formação de profissionais para atuar em Tratamento de Incidentes

Produção de boas práticas e material para conscientização sobre a necessidade de segurança na Internet

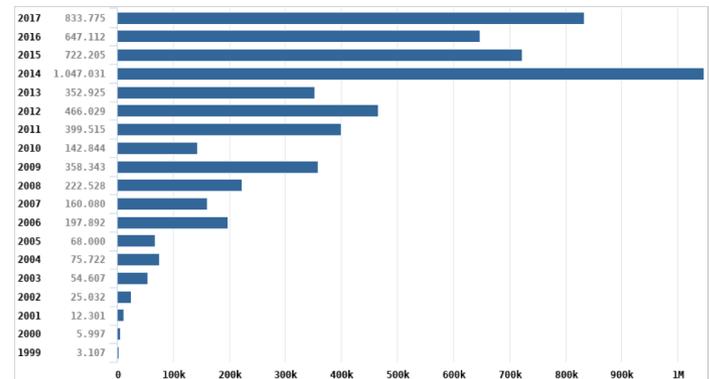
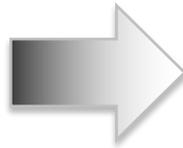
<https://www.cert.br/sobre/>

Tratamento de Incidentes e Abusos: Fontes dos Dados e Ações/Métricas

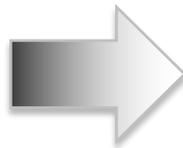
Notificações voluntárias de incidentes

enviadas para: `cert@cert.br` –
jan-out/2018: **2.112.865 e-mails** tratados

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



Data feeds (Honeypots Distribuídos do CERT.br, Team Cymru, SpamHaus, ShadowServer, Shodan, Operações Anti-Botnet)

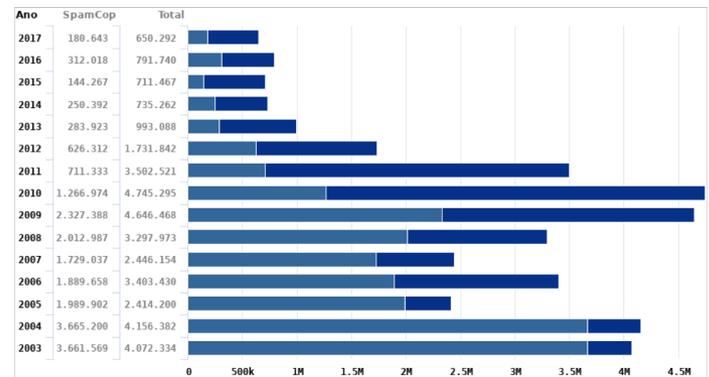
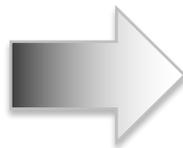


Responsáveis pelos ASNs são notificados, com dicas sobre como identificar os ataques e se recuperar

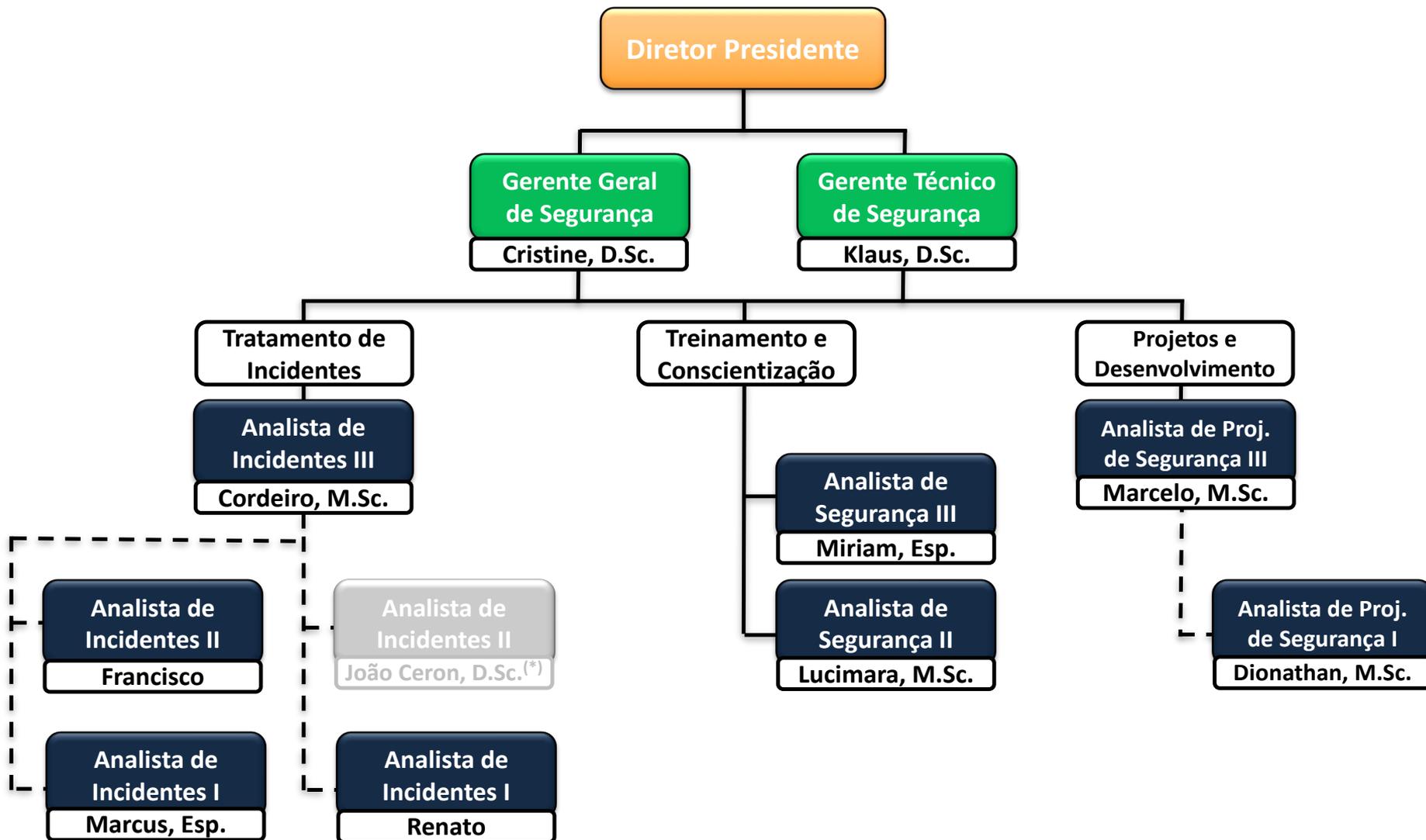
Reclamações de *spams* originados nas redes brasileiras

tratados de forma automatizada –
foco em identificar redes com problemas e reduzir abusos: **382.456 reclamações** tratadas

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



CERT.br: Equipe de 10 Analistas



(*) Saiu em fevereiro/2018 para fazer Post-doc

Foco do CERT.br nestes 21 anos: **Aumentar a Capacidade Nacional de Tratamento de Incidentes**

Premissa

- Nenhum grupo ou estrutura única conseguirá fazer sozinha a segurança ou a resposta a incidentes

Comunidade Nacional

- auxiliar e facilitar o tratamento de incidentes por outros CSIRTs
- ações junto a setores chave, para criação e treinamento de Grupos de Tratamento de Incidentes de Segurança (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

Objetivos

- Ter um “termômetro” das atividades maliciosas na Internet
- Entender o abuso da infraestrutura da Internet por atacantes, spammers e fraudadores
- Propor técnicas para proteger os usuários e coibir o abuso

Projetos

- *Honeypots* Distribuídos
- *SpamPots*

The Honeynet Project

honeyTARG Chapter

<https://honeytarg.cert.br>

CERT.br -- honeyTARG Honeynet Project

honeytarg.cert.br

cert.br Computer Emergency Response Team Brazil

egibr nicbr

honeypots for Threats and Abuse passive Reconnaissance and information Gathering

honeyTARG Honeynet Project

The honeyTARG Honeynet Project, led by CERT.br, is a Chapter of the Global Honeynet Project focused on using low-interaction honeypots to gather information about the Internet infrastructure's abuse by attackers and spammers.

Currently we have the following projects:

- Spampots Project
- Distributed Honeypots for Attack Trend Analysis

SpamPots Project

The [Spampots Project](#) uses low-interaction honeypots to gather data related to the abuse of the Internet infrastructure by spammers. The main goals are:

- measure the problem from a different point of view: abuse of infrastructure X spams received at the destination
- help develop the spam characterization research
- measure the abuse of network infrastructure to send spam
- develop better ways to
 - identify phishing and malware
 - identify botnets via the abuse of open proxies

Distributed Honeypots

CERT.br maintains the [Distributed Honeypots Project](#), whose objective is to increase the capacity of incident detection, event correlation and trend analysis in the Brazilian Internet space.

The data produced by the project include

- Daily summaries to project partners, with detailed information about the traffic observed in each honeypot;
- A system to notify CSIRTs of networks that generate attacks against the honeypots;
- The following public statistics:

Flows
Daily statistics for the network flow data directed to honeypots from the Distributed Honeypots Project

TCP/UDP Port Summary
Port summary statistics for TCP/UDP traffic data directed to honeypots from the

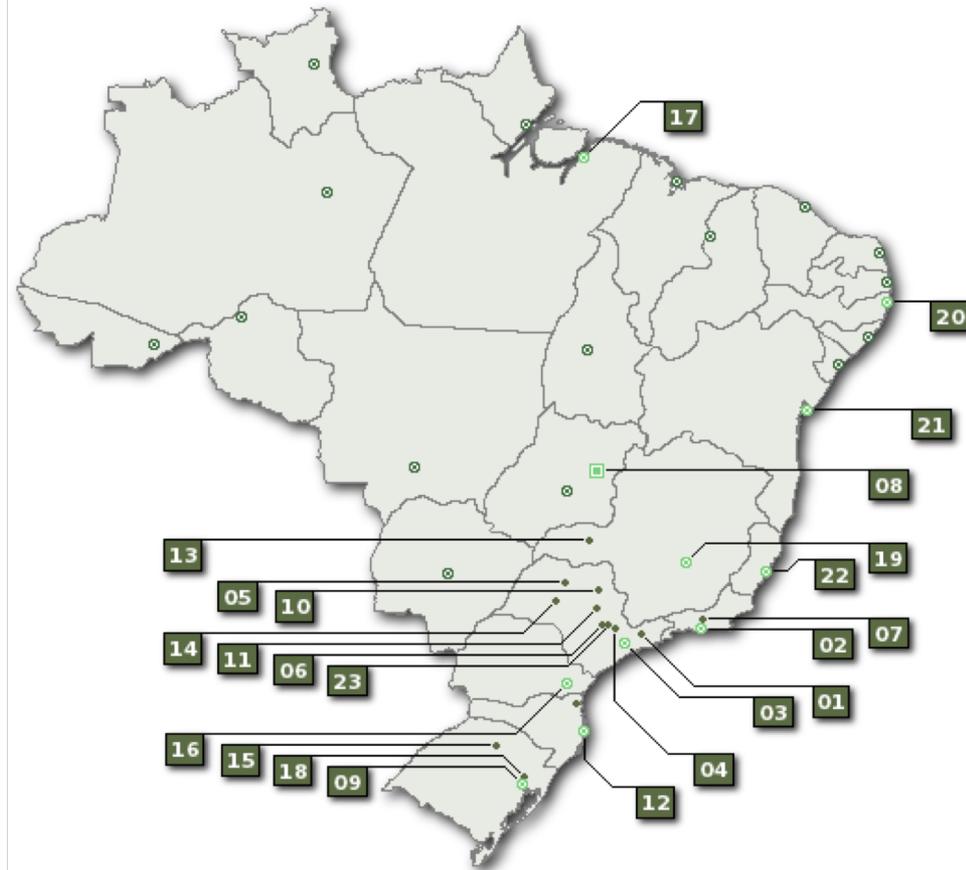
Honeypots Distribuídos – Início em 2003

Mapeamento das atividades maliciosas na Internet no Brasil

- 59 sensores em 47 organizações
 - (universidades, governo, provedores, operadoras e empresas)

Uso dos dados:

- Gerar estatísticas públicas sobre tendências
- Notificar sites brasileiros com problemas
- Enviar dados anonimizados
 - para CERTs Nacionais, para auxiliar esforços de combate a botnets
 - para grandes redes brasileiras
 - entidades de combate a abusos: Team Cymru e ShadowServer



Projeto SpamPots – Início em 2006

- Entender o abuso da infra-estrutura da Internet por spammers e fraudadores
- Propor técnicas para proteger os usuários e coibir o abuso
- Parceria com o Laboratório eSpeed/DCC/UFMG para mineração de dados
 - Mais de 2 milhões de spams coletados por dia
- Sensores em 12 países, em parceria com: CSIRT UNLP (Argentina), AusCERT (Austrália), CERT.at (Áustria), CSIRT USP (Brasil), CLCERT (Chile), CSIRT CEDIA (Equador), HKCERT (Hong Kong), IIJ - Internet Initiative Japan (Japão), SurfCERT (Holanda), Team Cymru (Holanda), Shadowserver Foundation (EUA), TWCERT (Taiwan) e CSIRT ANTEL (Uruguai).
- Envio de dados para países originadores de abuso
 - Japão: JPCERT/CC, JADAC, IIJ e Min. das Comunicações
 - Taiwan: TWCERT/CC e NCC/TW

Cooperação Internacional: Principais Fóruns

FIRST

Fórum existe desde 1992

- membro desde 2002

É uma Rede Global de CSIRTs

- fomenta a cooperação
- acesso a times e especialistas do mundo todo

Destaques da Participação:

- *Co-chair* do *Membership Committee*
- *Chair* da Conferência 2020
- Parte do grupo de Especialistas do *Education Initiative*
 - atualizando a lista de serviços
 - formalizando a lista de competências
- **Viabilizamos a parceria entre o FIRST e o LACNIC**
 - CERT.br é *co-host* dos TCs e Simpósios na região

Rede de CSIRTs Nacionais

Existe desde 2006

Fórum para discussão de assuntos específicos para grupos de responsabilidade nacional

- CERT.br e CTIR Gov são membros

Maiores parceiros do CERT.br:

CERT/CC	CERT.at
NCSC-NL	NCSC-FI
US-CERT	HKCERT
JPCERT/CC	TWCERT/CC

LAC-CSIRTs

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

Cooperação Nacional: Iniciativas de Destaque

Fórum Brasileiro de CSIRTs

- evento anual para profissionais da área de Resposta a Incidentes

Febraban (GTI) - Instituições associadas à Febraban, CERT.br e CTIR Gov

- Reuniões periódicas desde 2005
- CERT.br hospeda o fórum online de discussão deste grupo

Guardião Cibernético – promovido por GSI/PR e ComDCiber

- Exercício de segurança cibernética
 - 2018: setores nuclear e financeiro
 - 2019: setores nuclear, financeiro, energia e telecomunicações
- CERT.br faz parte dos grupo de órgãos parceiros
 - juntamente com DPF, ABIN, SERPRO e CAIS/RNP

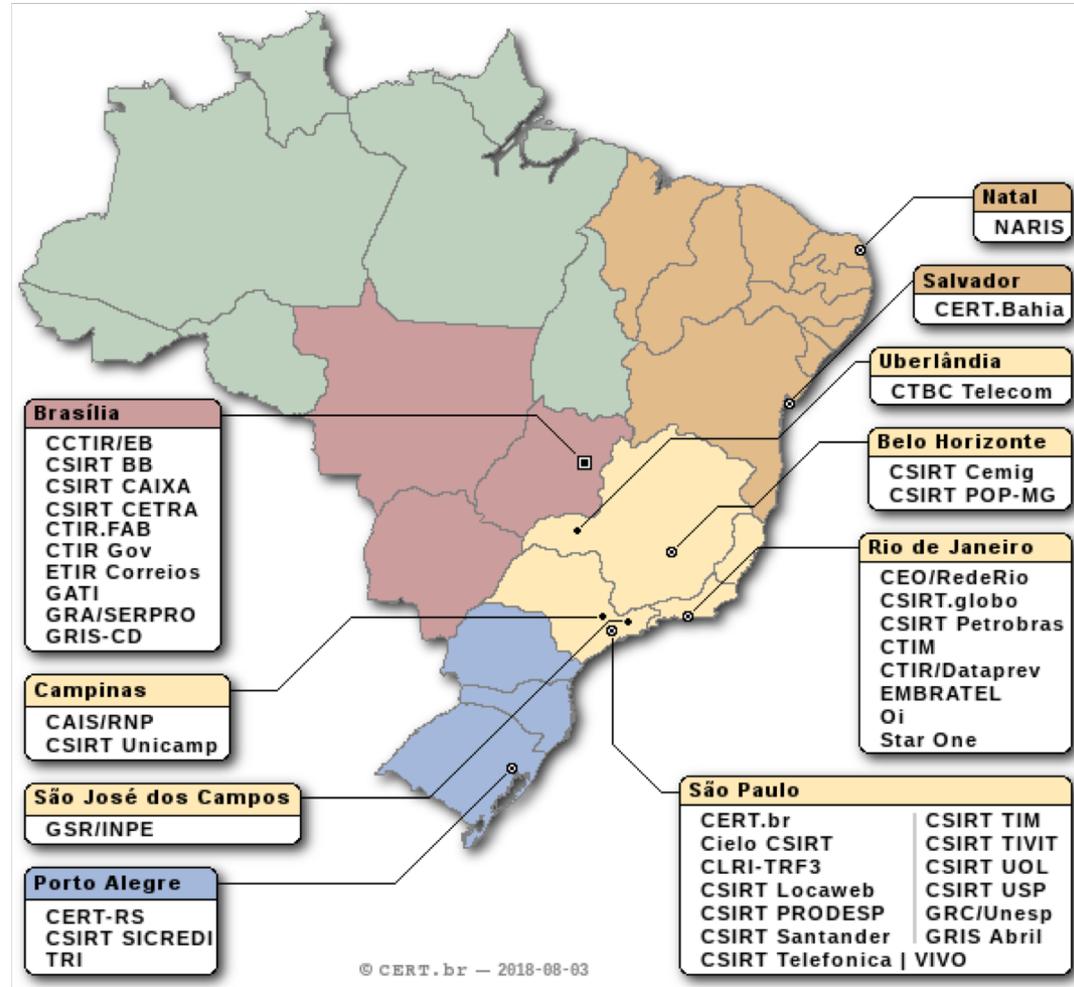
Atuação nos Grandes Eventos

(Rio+20, Copa das Confederações, Copa 2014, Jogos Olímpicos Rio2016)

- Treinou todos os profissionais que atuaram em tratamento de incidentes
- Guiou a criação do CSIRT Rio2016
- Atuou na comunicação e coordenação com outros atores e no auxílio ao acompanhamento de ameaças

Grupos de Tratamento de Incidentes Brasileiros: 42 times com serviços anunciados ao público

Setor	CSIRTs
Nacional – domínios .br, ASNs ou IPs alocados ao Brasil.	CERT.br
Nacional – Administração Pública Federal	CTIR Gov
Governo	CCTIR/EB, CLRI-TRF-3, CSIRT CETRA, CSIRT PRODESP, CTIM, CTIR.FAB, CTIR/Dataprev, ETIR Correios, GATI, GRA/SERPRO, GRIS-CD
Energia	CSIRT Cemig, CSIRT Petrobras
Sistema Financeiro	Cielo CSIRT, CSIRT BB, CSIRT CAIXA, CSIRT Santander, CSIRT Sicredi
Provedores Operadoras Hospedagem	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
Outros	CSIRT.globo, GRIS Abril



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

Objetivos:

- Criar/aproximar CSIRTs (Grupos de Tratamento de Incidentes de Segurança) no Brasil
- Possuir profissionais preparados para resolver os problemas de segurança no país

SEI/Carnegie Mellon Partner desde 2004, licenciado para ministrar cursos do CERT[®] Program no Brasil:

- <https://www.cert.br/cursos/>
 - *Overview of Creating and Managing CSIRTs*
 - *Fundamentals of Incident Handling*
 - *Advanced Incident Handling for Technical Staff*
- 800+ profissionais treinados em tratamento de incidentes

Cartilha de Segurança para Internet

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

- Livro (PDF e ePub) e conteúdo no *site* (HTML5)
- Dica do dia no *site*, via *Twitter* e RSS
- Impressões em pequena escala enviadas a escolas e centros de inclusão digital
- Uso por instituições para treinar funcionários
- Nova versão será lançada em 2019

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

The image displays a screenshot of the website <http://cartilha.cert.br/> in a browser window. The browser's address bar shows the URL and search engines like Reader and Google. The website header includes the logo for 'cert.br' (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil) and 'nic.br cgi.br' (Ir para o conteúdo). The main navigation menu has links for 'Início', 'Livro', 'Fascículos', and 'Sobre'. A search bar is also present.

The main content area features a prominent article titled 'Navegar é preciso, arriscar-se não!' with a sub-headline '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!'. To the right, there is a 'Dica do dia' section with the text 'Faça backup de seu arquivo de senhas, caso opte por mantê-las gravadas localmente. Saiba mais...'. Below this, a 'Veja também' section highlights 'INTERNETSEGURABR' and 'antispam.br'.

On the left side of the screenshot, a book cover for 'Cartilha de Segurança para Internet' is shown. The cover features a cartoon illustration of a boat on the water with a shark below it, and the website URL 'http://cartilha.cert.br/' and logos for 'nic.br' and 'cgi.br' at the bottom.

Fascículos da Cartilha de Segurança para Internet

Organizados de forma a facilitar a difusão de conteúdos específicos:

- Redes Sociais
- Senhas
- Comércio Eletrônico
- Privacidade
- Dispositivos Móveis
- *Internet Banking*
- Computadores
- Códigos Maliciosos
- Verificação em Duas Etapas
- Redes
- Backup
- Boatos



Acompanhados de *slides* de uso livre para:

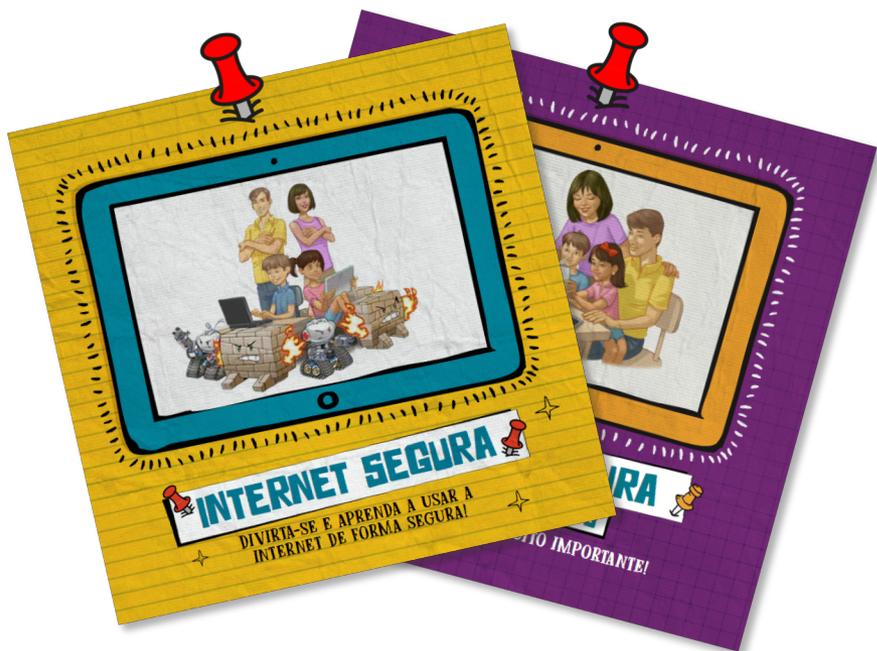
- ministrar palestras e treinamentos
- complementar conteúdos de aulas

Materiais para Crianças

Guias Internet Segura

- Dicas e brincadeiras para crianças
- Material de apoio para pais

<http://internetsegura.br/>



Boas Práticas para a Área Técnica

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

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

Programa por uma Internet mais Segura: Atuação do CERT.br

Lançado por NIC.br, CGI.br, SindiTelebrasil, Abranet e ISOC¹

Tem o objetivo de promover a redução de tráfego malicioso na Internet no Brasil e melhorar a segurança de dispositivos de rede.

Atuação do CERT.br dentro da iniciativa:

- Desenvolvimento de documentos de boas práticas
- Desenvolvimento e visualização de métricas para acompanhar a evolução das atividades maliciosas ao longo da implementação
 - serviços que permitem amplificação (ASNs e IPs)
 - dados do Brasil no projeto Spoofer CAIDA

https://spoofer.caida.org/recent_tests.php?country_include=bra

1. <http://www.nic.br/noticia/releases/programa-do-cgi-br-incentiva-adocao-de-boas-praticas-de-seguranca-entre-sistemas-autonomos/>

Obrigado

www.cert.br

© cristine@cert.br

© jessen@cert.br

© @certbr

23 de novembro de 2018

nic.br cgi.br

www.nic.br | www.cgi.br