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

cert.br nic.br cgi.br

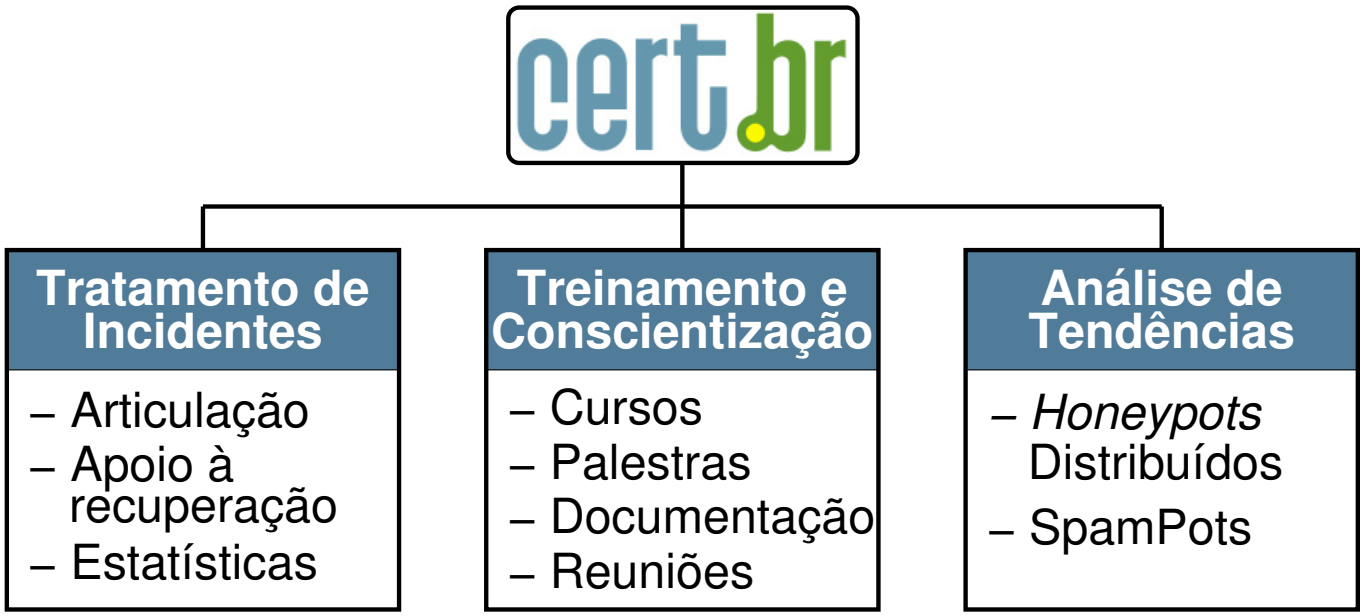
Histórico:
Criação e Missão do CERT.br

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 nacional[2]

[1] https://www.nic.br/grupo/historico-gts.htm
[2] https://www.nic.br/pagina/gts/157



SEI Partner
Carnegie Mellon

FIRST
Improving Security Together
MEMBER

APWG
RESEARCH PARTNER
www.antiphishing.org

The Honeynet PROJECT

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

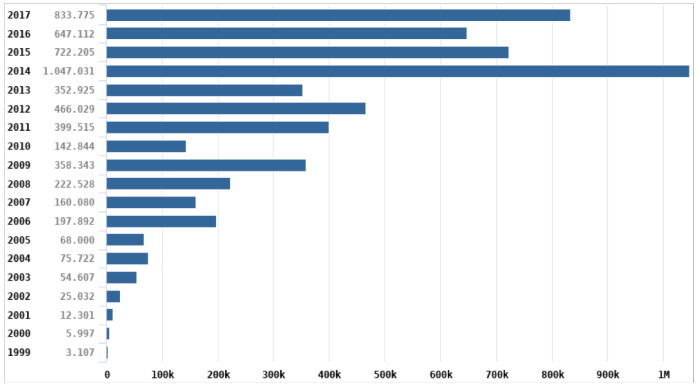
https://www.cert.br/sobre/

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/

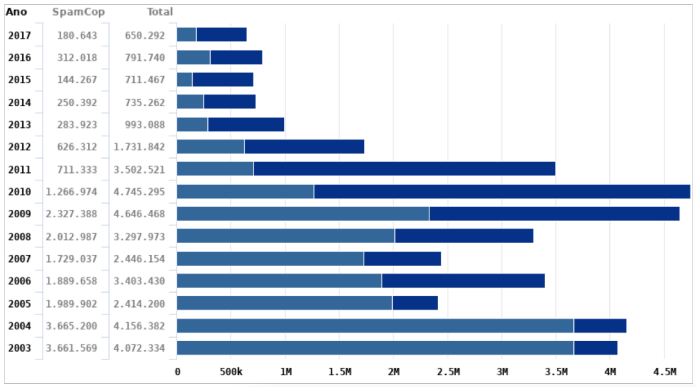


Data feeds (Honeypots Distribuídos do CERT.br, Team Cymru, SpamHaus, ShadowServer, Shodan, Operações Anti-Botnet)

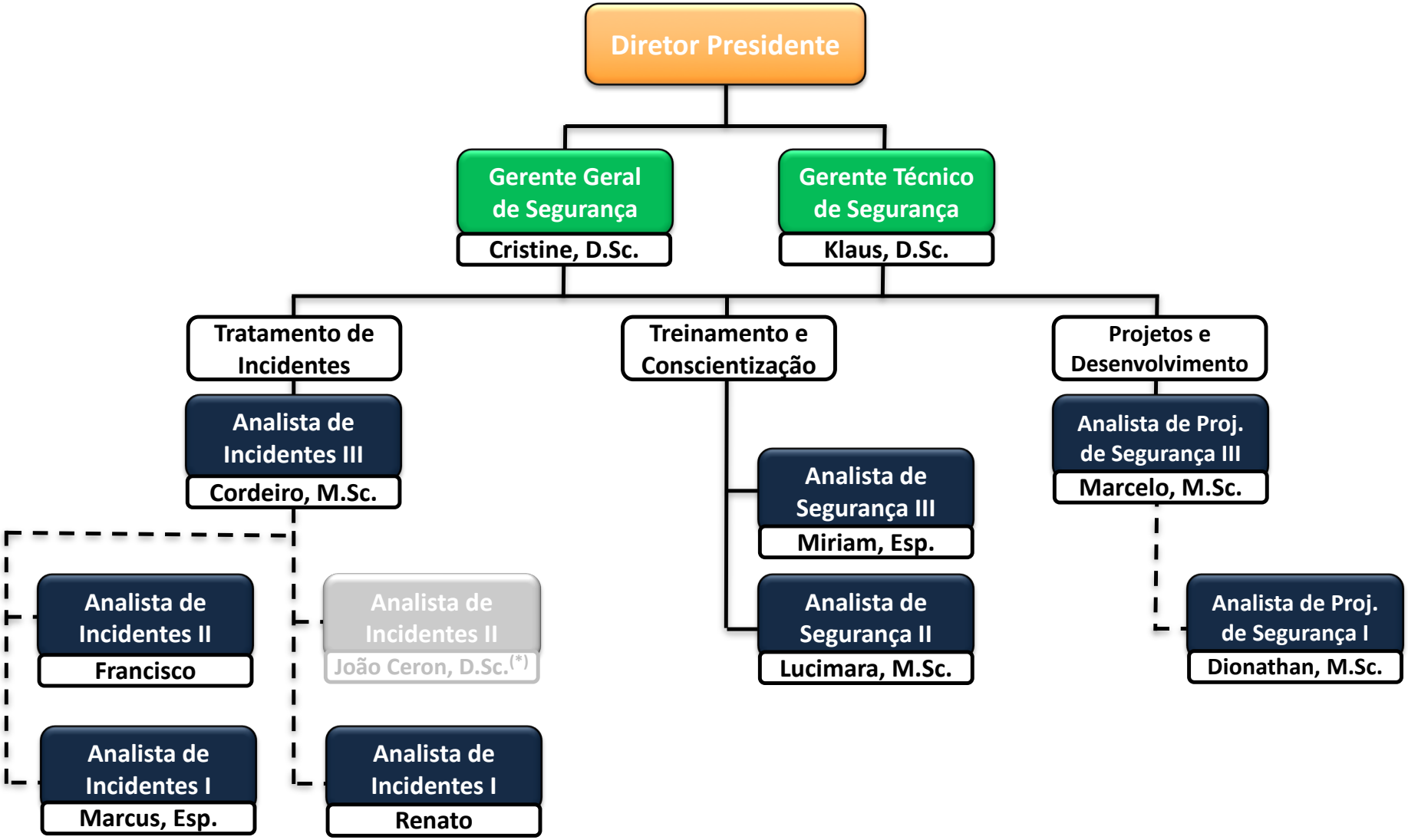
Responsáveis pelos ASNs são notificados, com dicas sobre como identificar os ataques e se recuperar

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

Análise de Tendências

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

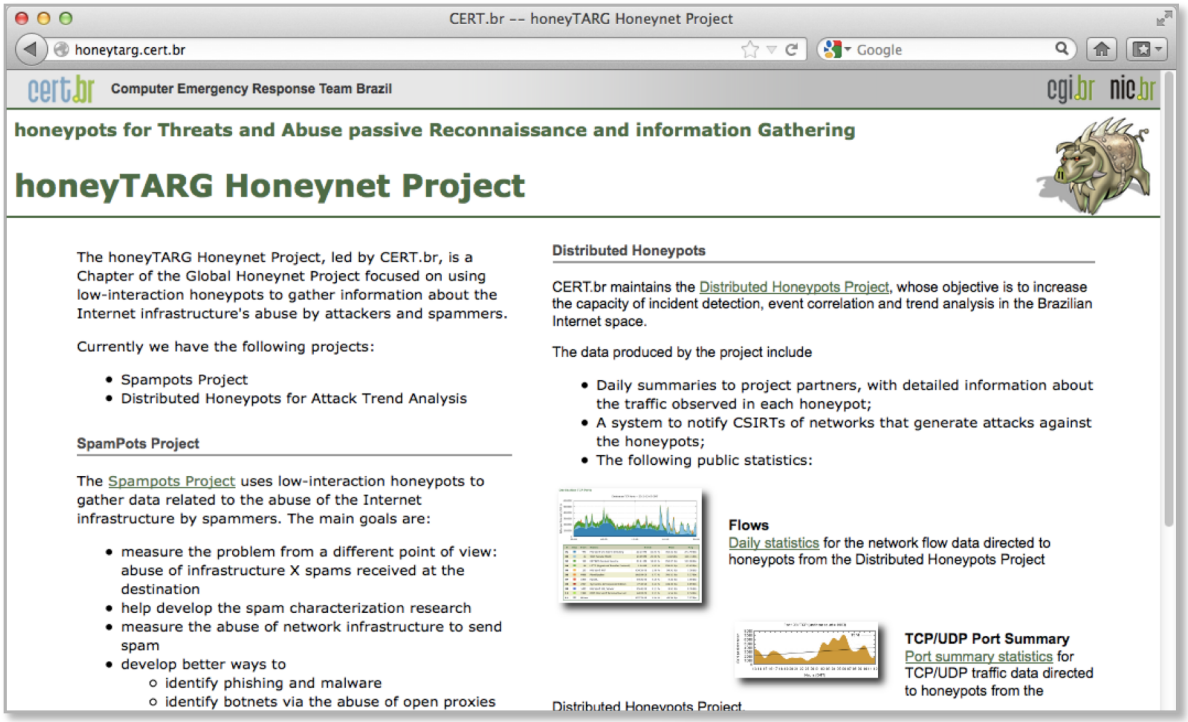
Projetos

- *Honeypots* Distribuídos
- *SpamPots*

The Honeynet Project

honeyTARG Chapter

https://honeytarg.cert.br



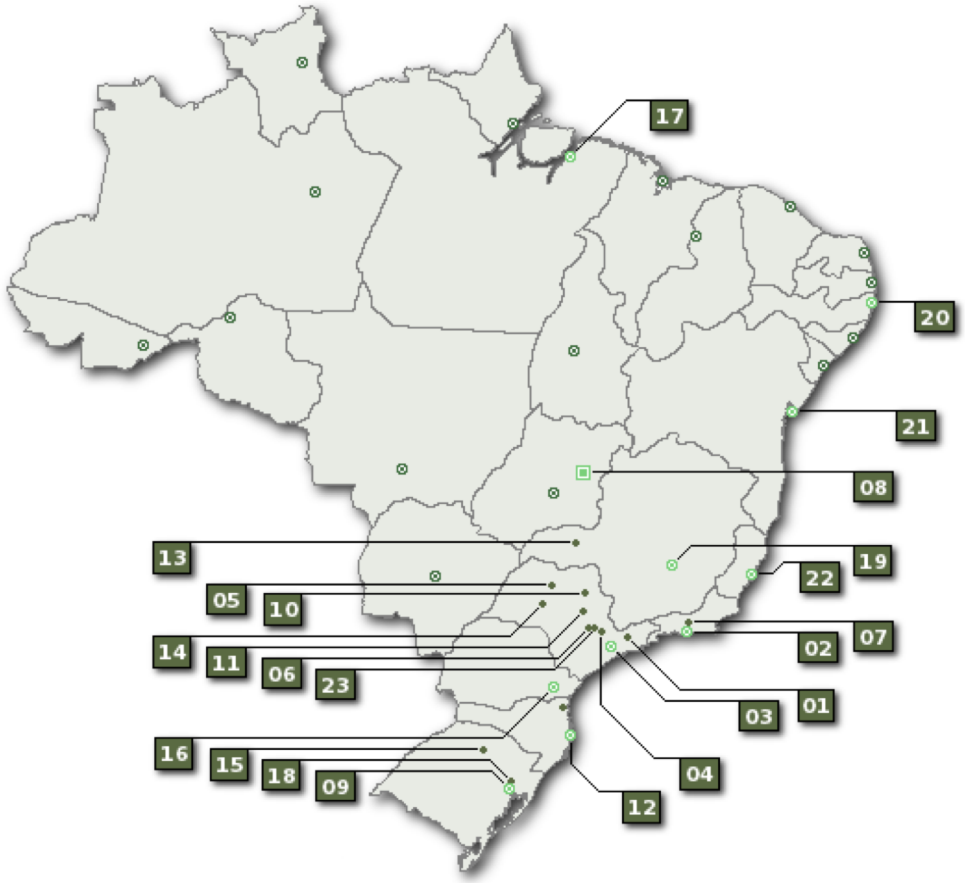
Honeypots Distribuídos – Início em 2003

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

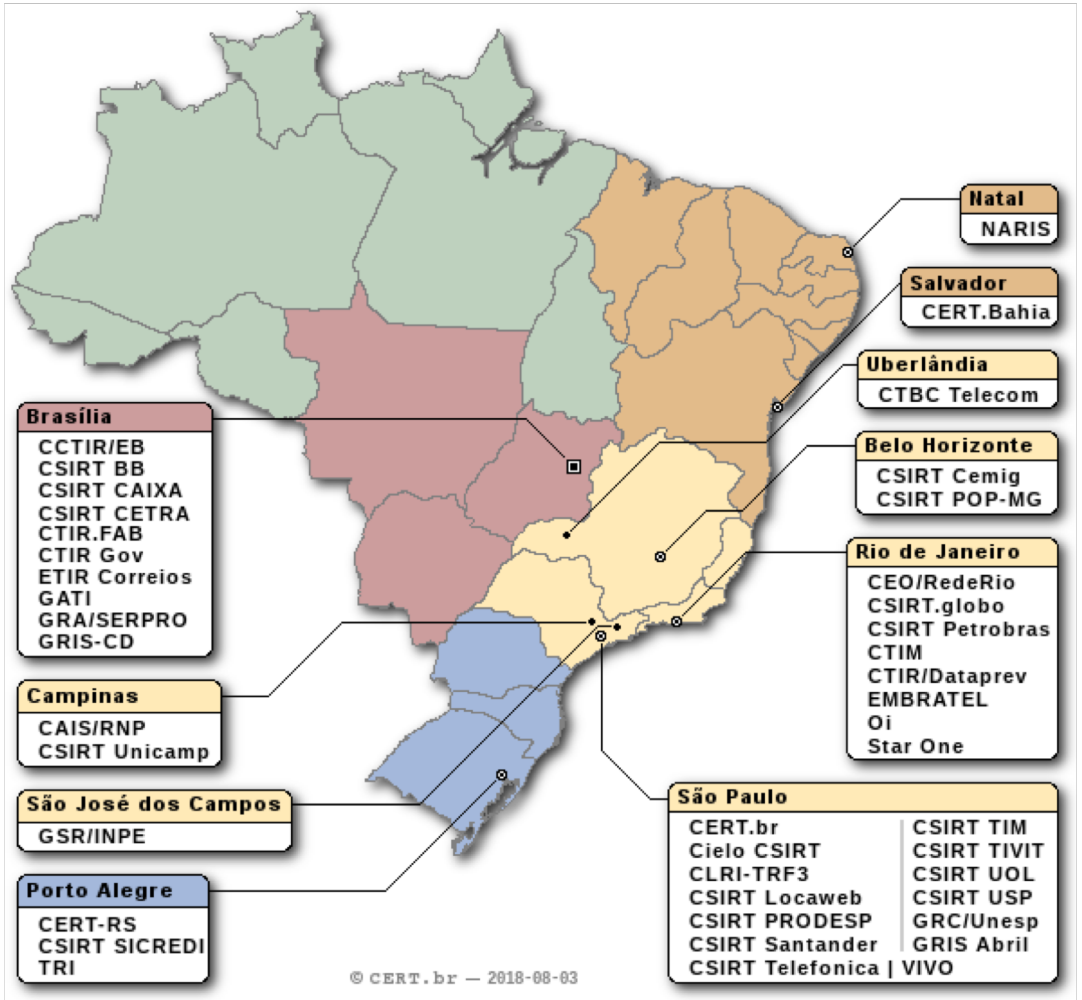
- Exercício de segurança cibernética
  - 2018: setores nuclear e financeiro
  - 2019: setores nuclear, financeiro, energia e telecomunicações
- CERT.br faz parte dos grupo de órgãos parceiros
  - juntamente com DPF, ABIN, SERPRO e CAIS/RNP

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/

Treinamento

SEI Partner
Carnegie Mellon

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/

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 ISOC[1]

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