nic.br cgi.br | cert.br

Desafios da Segurança Cibernética no Brasil
Belo Horizonte, MG
11 de março de 2016

Tratamento de Incidentes no Brasil

Cristine Hoepers, D.Sc.
Gerente Geral

cert.br nic.br cgi.br

Comitê Gestor da Internet no Brasil – CGI.br

Entidade multissetorial, criada em 1995, responsável por coordenar e integrar as iniciativas e serviços da Internet no País. Dentre as atribuições definidas no Decreto Presidencial nº 4.829, de 03/09/2003, destacam-se:

a proposição de normas e procedimentos relativos à regulamentação das atividades na internet;

a recomendação de padrões e procedimentos técnicos operacionais para a internet no Brasil;

o estabelecimento de diretrizes estratégicas relacionadas ao uso e desenvolvimento da internet no Brasil;

a promoção de estudos e padrões técnicos para a segurança das redes e serviços no país;

a coordenação da atribuição de endereços internet (IPs) e do registro de nomes de domínios usando <.br>;

a coleta, organização e disseminação de informações sobre os serviços internet, incluindo indicadores e estatísticas.

ser representado nos fóruns técnicos nacionais e internacionais relativos à Internet;

http://www.cgi.br/sobre/

cgi.br

1 2 3 4 5 6 7 8 9 — GOVERNO e 10 11 12 13 14 15 16 17 18 19 20 21 — SOCIEDADE CIVIL

Representantes do Governo:

1 Ministério da Ciência, Tecnologia e Inovação (coordenador)
2 Casa Civil da Presidência da República
3 Ministério das Comunicações
4 Ministério da Defesa
5 Ministério do Desenvolvimento, Indústria e Comércio Exterior
6 Ministério do Planejamento, Orçamento e Gestão
7 Agência Nacional de Telecomunicações
8 Conselho Nacional de Desenvolvimento Científico e Tecnológico
9 Conselho Nacional de Secretários Estaduais para Assuntos de Ciência e Tecnologia

Representantes da Sociedade Civil:

10 Notório saber em assunto da Internet
11 a 14 Representantes do setor empresarial
- provedores de acesso e conteúdo da Internet
- provedores de infra-estrutura de telecomunicações
- indústria de bens de informática, de bens de telecomunicações e de software
- setor empresarial usuário

15 a 18 Representantes do terceiro setor
19 a 21 Representantes da comunidade científica e tecnológica

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

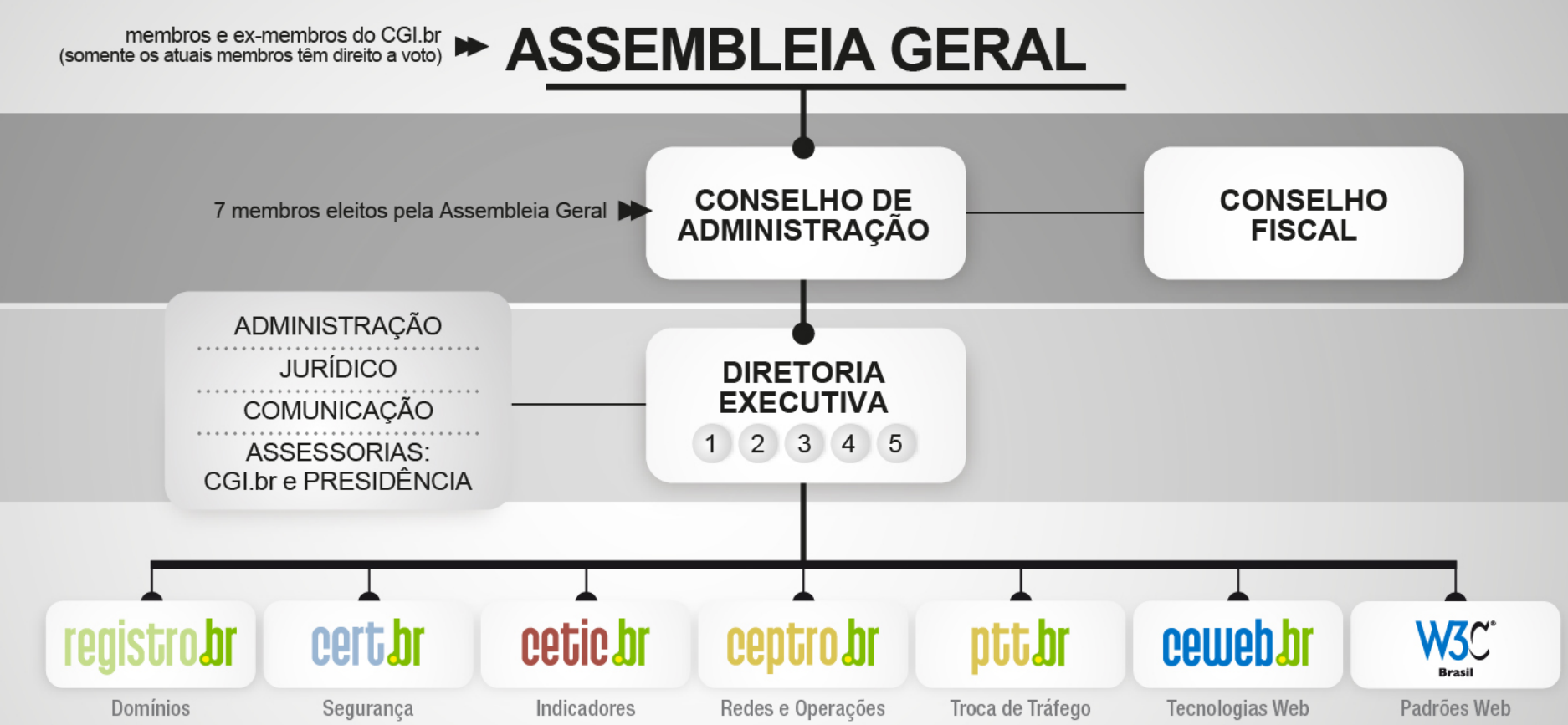
Entidade civil, sem fins lucrativos, que implementa as decisões e os projetos do Comitê Gestor da Internet no Brasil – CGI.br.

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;
- tratamento e resposta a incidentes de segurança em computadores envolvendo redes conectadas à Internet no Brasil, 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.

http://www.nic.br/sobre/

Estrutura do NIC.br



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

Tratamento de Incidentes

cert.br nic.br cgi.br

Tratamento de Incidentes e Conceitos Relacionados

Incidente de Segurança em Computadores – qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores

Tratamento de Incidentes – processo de identificar e mitigar os incidentes de segurança; também envolve a prevenção

CSIRT – acrônimo internacional para designar um Grupo de Resposta a Incidentes de Segurança, responsável por tratar incidentes de segurança para um público alvo específico

Outros acrônimos: IRT, CIRC, CIRT, SERT, SIRT, CERT®, CTIR, ETIR

Papel dos CSIRTs

A redução do impacto de um incidente é conseqüência:

- da agilidade de resposta
- da redução no número de vítimas

O papel do CSIRT é:

- auxiliar a proteção da infraestrutura e das informações
- prevenir incidentes e conscientizar sobre os problemas
- auxiliar a detecção de incidentes de segurança
- responder incidentes – retornar o ambiente ao estado de produção

O sucesso depende da confiabilidade

- nunca divulgar dados sensíveis nem expor vítimas, por exemplo

O CSIRT não é "investigador"

- foco é entender "o que" o que aconteceu, não "quem" originou a ação
  - ferramentas muitas vezes são as mesmas da investigação e da perícia
- naturalmente pode identificar possíveis crimes e então:
  - atuar na preservação de evidências
  - auxiliar investigações posteriores, dependendo de sua missão

Tipos Mais Comuns de CSIRTs

Internos a uma organização

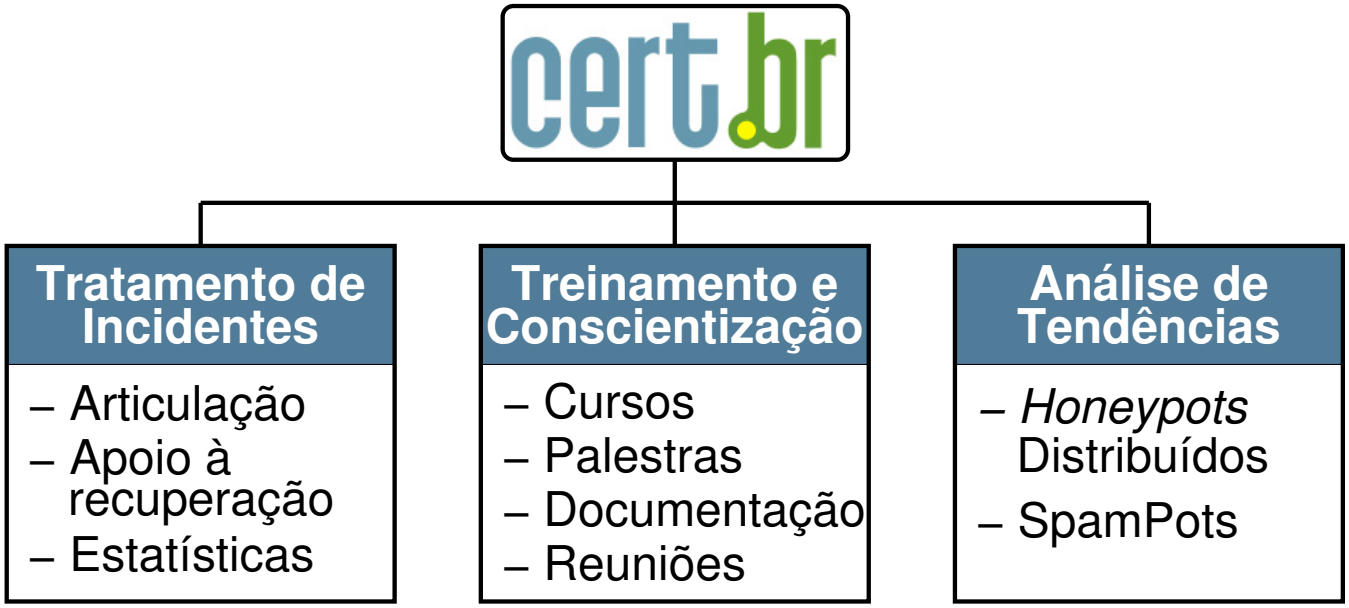
- Ex: CSIRT BB, CSIRT Cemig, CSIRT POP-MG, CSIRT.globo

Internos de Coordenação

- Ex: CAIS/RNP, CCTIR/EB

De Responsabilidade Nacional (ou também chamados de Nacionais)

- Ex: CERT.br, CTIR Gov



SEI Partner
Carnegie Mellon

FIRST
Improving Security Together
MEMBER

APWG
RESEARCH PARTNER
www.antiphishing.org

The Honeynet
PROJECT

Principais atividades:

- **Tratamento de Incidentes**
  - CERT de responsabilidade nacional
  - 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 para diversas audiências**

http://www.cert.br/sobre/

Evolução do Tratamento de Incidentes no Brasil e Cenário Atual

cert.br nic.br cgi.br

Criação do CERT.br

Agosto/1996: o relatório "Rumo à Criação de uma Coordenadoria de Seguraça 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, que atue como ponto de contato nacional
  - que possa orientar tecnicamente sobre prevenção e resposta a incidentes
  - que fomente treinamento, atualização e cooperação
  - que fomente 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] http://www.nic.br/grupo/historico-gts.htm

[2] http://www.nic.br/grupo/gts.htm

Criação de Outros Grupos no País

Agosto/1997: a RNP cria seu próprio CSIRT (CAIS)[3], seguida pela rede acadêmica do Rio grande do Sul (CERT-RS)[4]

1999: outras instituições, incluindo Universidades e Operadoras de Telecomunicações, iniciaram a formação de seus CSIRTs

2003/2004: grupo de trabalho no Ministério do Planejamento para definição da estrutura de um CSIRT para a Administração Pública Federal

2004: o CTIR Gov foi criado, também com responsabilidade nacional, com a Administração Pública Federal como seu público alvo[5]

[1] http://www.nic.br/grupo/historico-gts.htm

[2] http://www.nic.br/grupo/gts.htm

[3] http://www.rnp.br/_arquivo/documentos/rel-rnp98.pdf

[4] http://www.cert-rs.tche.br/cert-rs.html

[5] http://www.ctir.gov.br

Investimento Estratégico no Aumento da Capacidade Nacional de Tratamento de Incidentes

Objetivos:

- formar/aproximar CSIRTs (Grupos de Tratamento de Incidentes de Segurança) no Brasil
- preparar profissionais para o Tratamento de Incidentes de Segurança no Brasil

CERT.br/NIC.br é um *SEI/Carnegie Mellon Partner* desde 2004, licenciado para ministrar cursos do *CERT® Program* no Brasil

- http://www.cert.br/cursos/
  - ***Overview of Creating and Managing CSIRTs***

    discute boas práticas de planejamento, implementação, operação e avaliação de um CSIRT.
  - ***Fundamentals of Incident Handling***

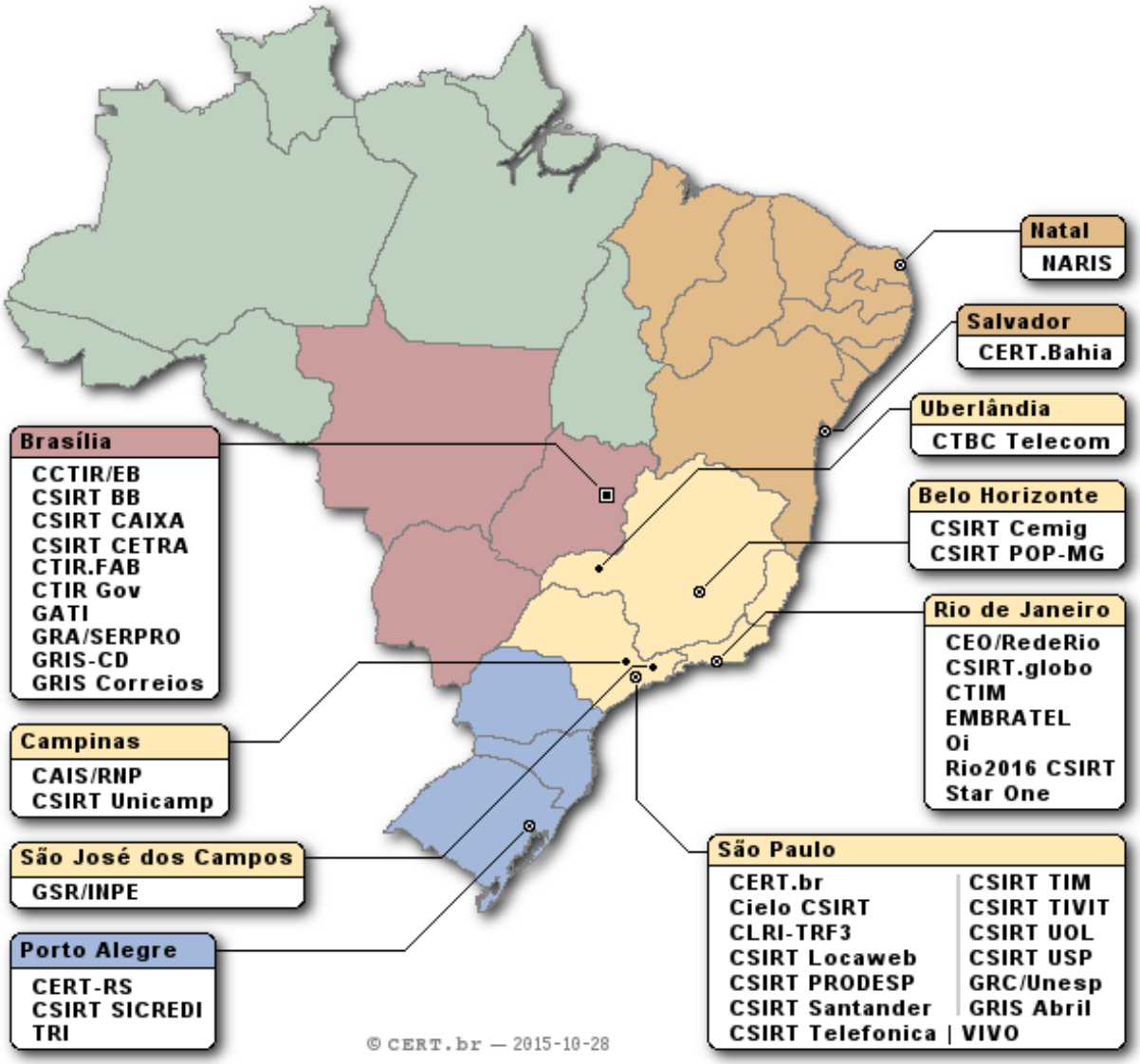
    visa definir e esclarecer a natureza do trabalho que um *incident handler* realiza, incluindo os serviços prestados pelo CSIRT, as ameaças dos invasores e a natureza das atividades de resposta a incidentes.
  - ***Advanced Incident Handling for Technical Staff***

    trata cenários avançados de tratamento de incidentes, incluindo análise de artefatos, desenvolvimento de *advisories*, alertas e interação com administração superior.
- **700+ profissionais treinados em tratamento de incidentes**

Grupos de Tratamento de Incidentes Brasileiros

40 times formalizados e com serviços anunciados ao público

Público Alvo	CSIRTs
Qualquer Rede no País	CERT.br
Governo	CTIR Gov, CCTIR/EB, CLRI-TRF-3, CSIRT PRODESP, GATI, CTIM, GRA/SERPRO, CTIR.FAB, GRIS-CD, CSIRT CETRA, GRIS Correios
Setor Financeiro	Cielo CSIRT, CSIRT BB, CSIRT CAIXA, CSIRT Sicredi, CSIRT Santander
Telecom/ISP	CTBC Telecom, EMBRATEL, CSIRT Telefonica|VIVO, CSIRT Locaweb, CSIRT TIM, CSIRT UOL, StarOne, Oi,
Academia	GSR/INPE, CAIS/RNP, CSIRT Unicamp, CERT-RS, NARIS, CSIRT POP-MG, CEO/RedeRio, CERT.Bahia, CSIRT USP, GRC/UNESP, TRI
Outros	Rio2016 CSIRT, CSIRT TIVIT, GRIS Abril, CSIRT Globo, CSIRT Cemig



http://www.cert.br/csirts/brasil/

Considerações Finais

Objetivo maior é um ecossistema saudável

- **Nenhum grupo ou estrutura única conseguirá fazer sozinha a segurança ou a resposta a incidentes - todos tem um papel**
  - administradores de redes e sistemas
    - não emanar “sujeira” de suas redes e adotar boas práticas
  - usuários
    - entender os riscos e seguir as dicas de segurança
    - manter seus dispositivos atualizados e tratar infecções
  - desenvolvedores
    - precisam pensar em segurança desde as etapas iniciais de desenvolvimento

Ainda assim incidentes ocorrerão

- **necessário identificar e mitigar mais rapidamente**
  - redução de impactos é proporcional à agilidade na resposta
  - é necessário ter CSIRTs estabelecidos e profissionais preparados
    - equipe multidisciplinar é um fundamental
      - conhecimentos técnicos profundos (redes, sistemas, desenvolvimento)
      - habilidades de comunicação e negociação
  - cooperação é primordial – nacional e internacional

Obrigada

www.cert.br

cristine@cert.br

@certbr

11 de março de 2016

nic.br cgi.br

www.nic.br | www.cgi.br