Workshop em Segurança Cibernética e Crime Cibernético para África Lusófona

22 a 24 de Setembro de 2015

Maputo, Moçambique

Atividades do CERT.br/NIC.br para Segurança e Estabilidade da Internet no Brasil

Lucimara Desiderá
lucimara@cert.br

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

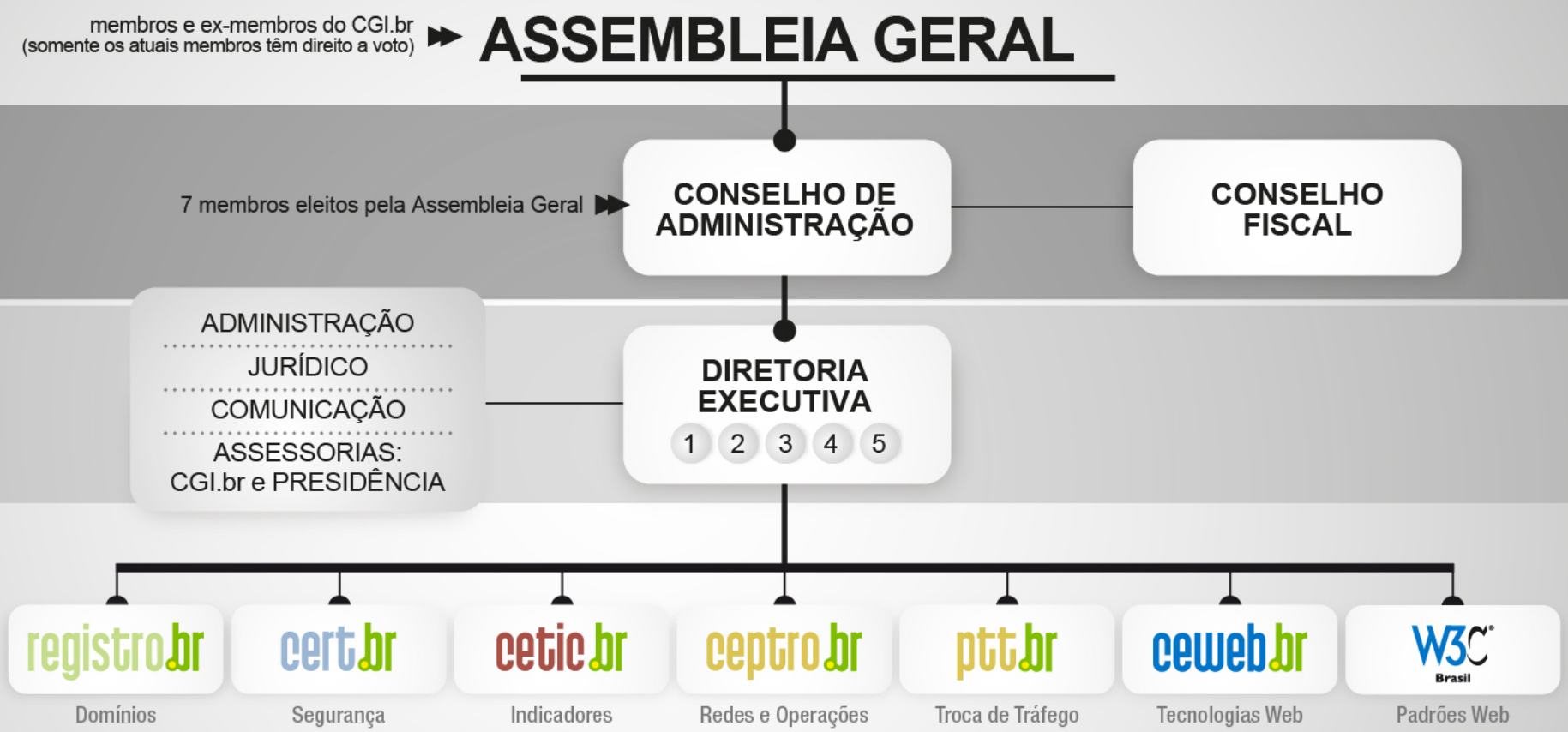
Entidade civil, sem fins lucrativos, criada para implementar as decisões e os projetos do Comitê Gestor da Internet no Brasil - CGI.br.

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;
- 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

Evolução do Tratamento de Incidentes no Brasil

cert.br nic.br cgi.br

Conceitos

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®

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

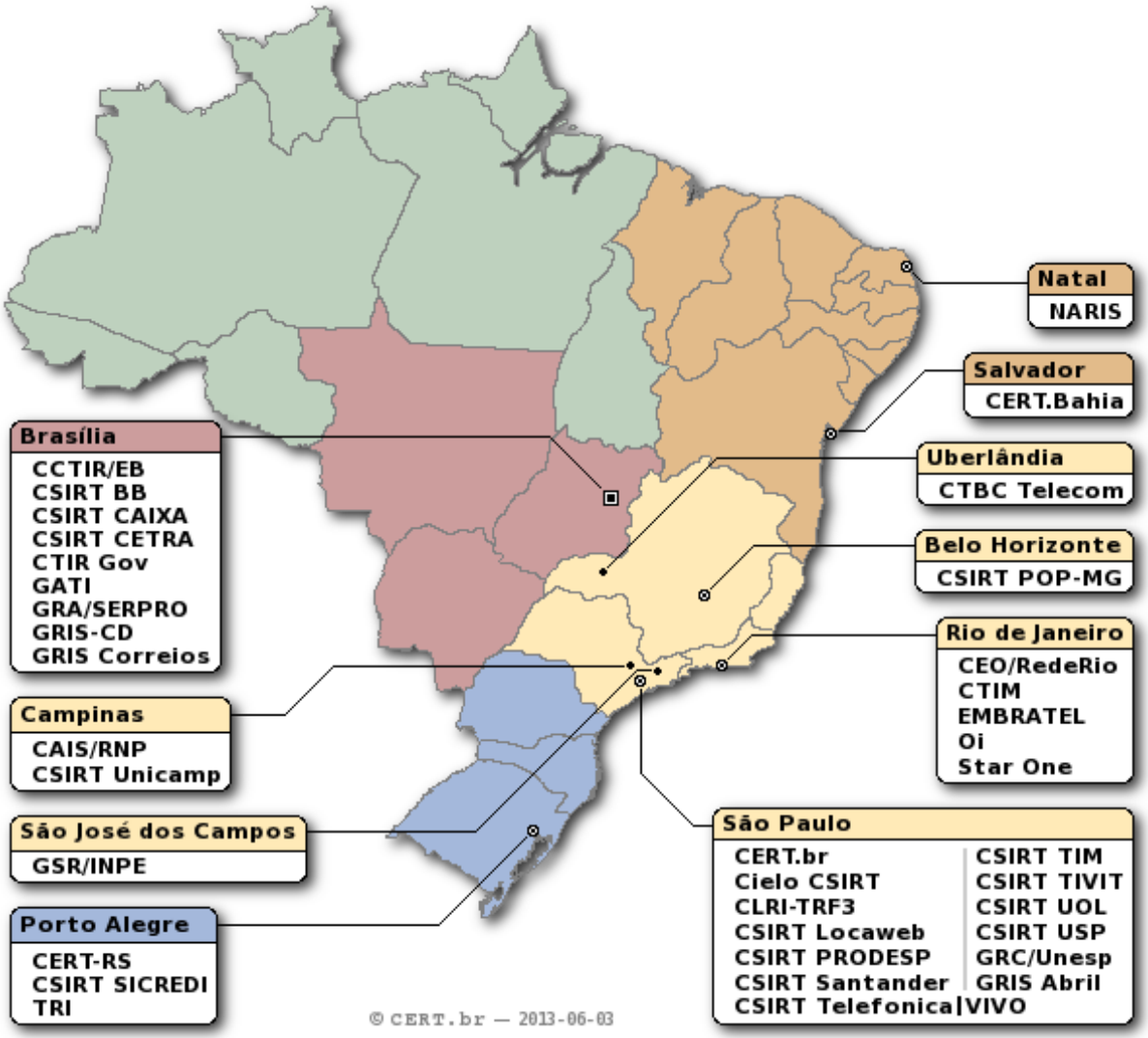
[4] http://www.cert-rs.tche.br/cert-rs.html

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

Grupos de Tratamento de Incidentes Brasileiros

37 times com serviços anunciados ao público

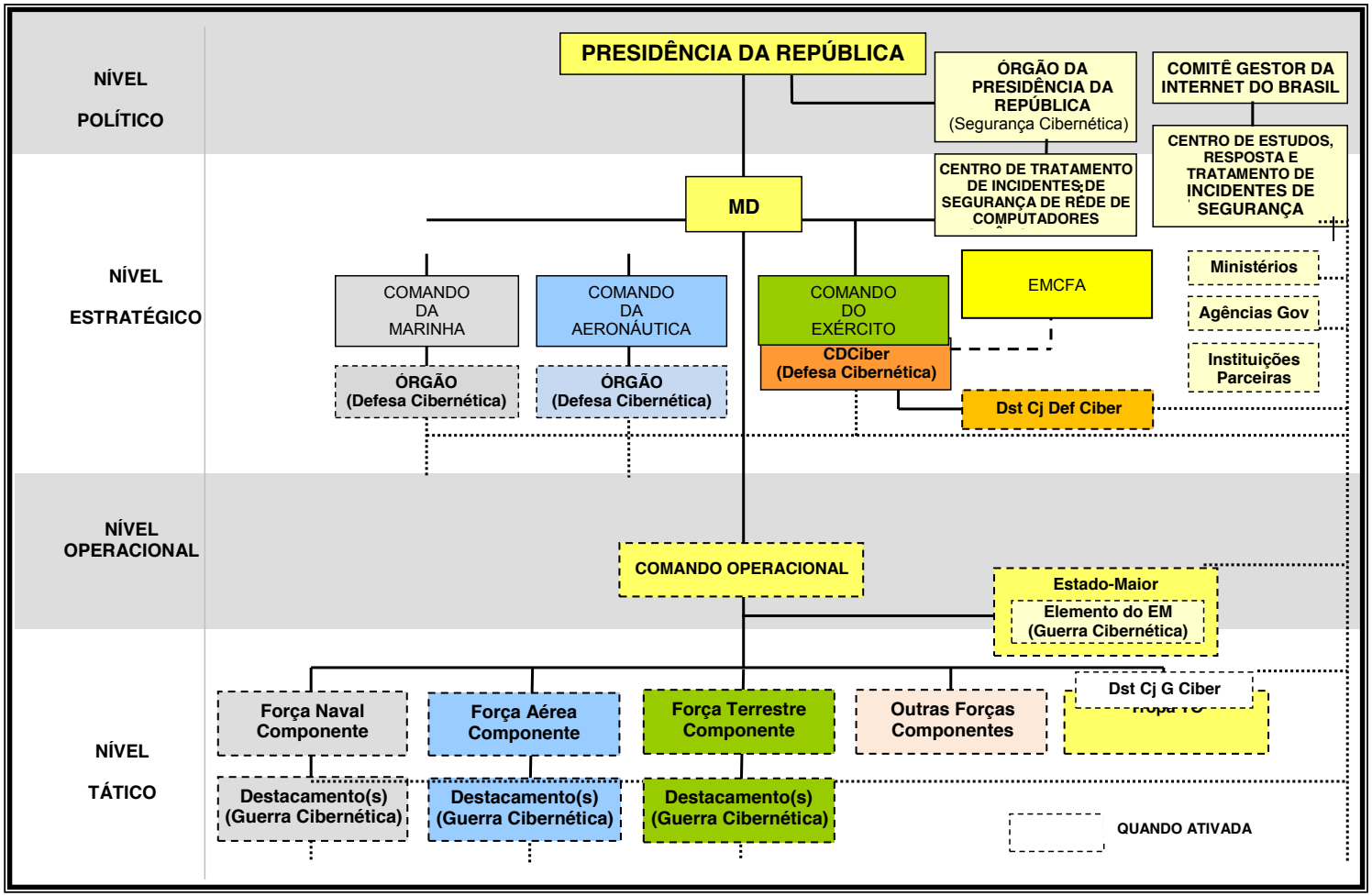
Público Alvo	CSIRTs
Qualquer Rede no País	CERT.br
Governo	CTIR Gov, CCTIR/EB, CLRI-TRF-3, CSIRT PRODESP, GATI, GRA/SERPRO, GRIS-CD, CSIRT CETRA, GRIS Correios
Setor Financeiro	Cielo CSIRT, CSIRT BB, CSIRT CAIXA, CSIRT Sicredi, CSIRT Santander
Telecom/ISP	CTBC Telecom, EMBRATEL, CSIRT Telefonica|VIVO, 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	CSIRT TIVIT, GRIS Abril



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

Agosto/2010: Criação do CDCiber – Proteção no Escopo do Min. da Defesa

APÊNDICE
ESTRUTURAS E ÓRGÃOS NA CONCEPÇÃO DO SISTEMA MILITAR DE DEFESA CIBERNÉTICA
CERT.br



LEGENDA:
SUBORDINAÇÃO
VINCULAÇÃO (SUBORDINAÇÃO OPERACIONAL)
CANAL TÉCNICO (COORDENAÇÃO E INTEGRAÇÃO)

Atuação do CERT.br

cert.br nic.br cgi.br

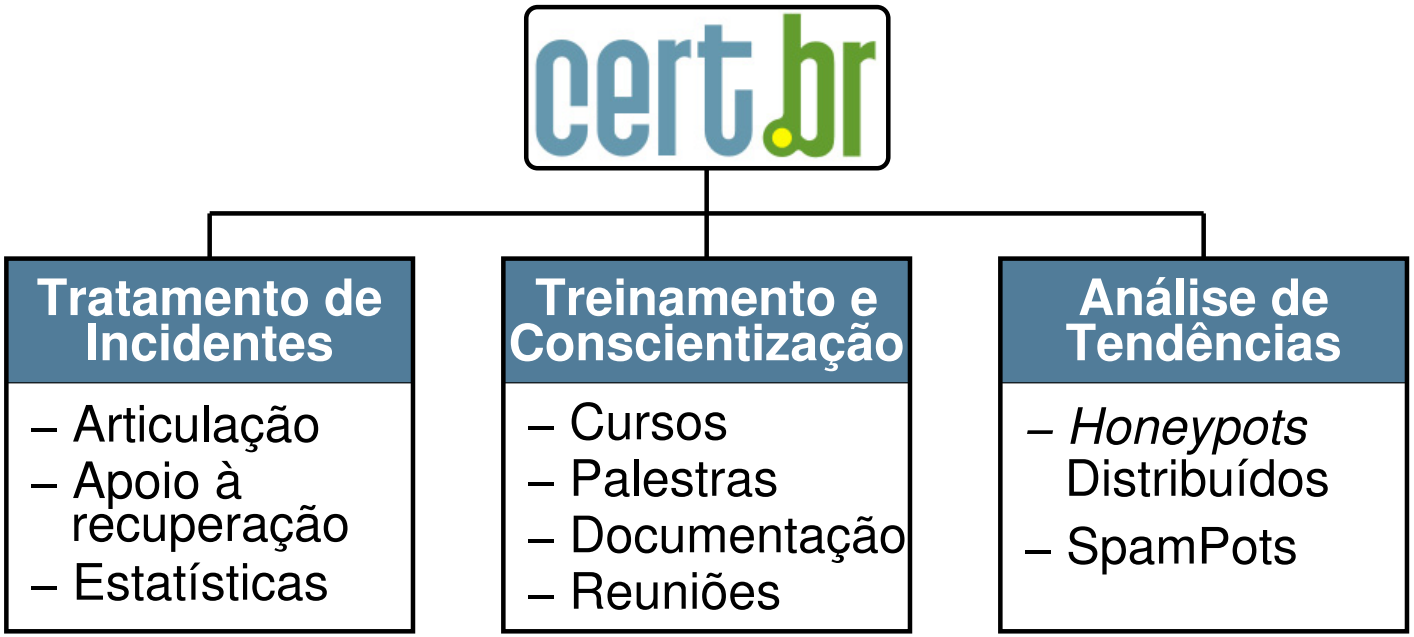
Estratégias para Reduzir os Incidentes e seus Impactos

Primeiro objetivo 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**



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 para diversas audiências**

Atividades de Tratamento de Incidentes

O CERT.br recebe notificações de incidentes de segurança envolvendo redes conectadas à Internet no Brasil

- feitas voluntariamente por administradores de redes e usuários de Internet, sejam eles do Brasil ou do exterior
- ponto de entrada: e-mail cert@cert.br

Modo de atuação:

- provê suporte, dicas e recomendações técnicas para mitigação e recuperação de incidentes, como invasões
- foco na redução no número de vítimas
- agrega dados de organismos internacionais (*data feeds*) e repassa para as redes nacionais, para identificação e erradicação de problemas

APWG RESEARCH PARTNER www.antiphishing.org

FIRST Improving Security Together MEMBER

The Honeynet PROJECT

Treinamento

SEI Partner
Carnegie Mellon®

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

      trata 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.
  - **600+ profissionais treinados em tratamento de incidentes**

Cooperação entre CSIRTs

- **Fórum Brasileiro de CSIRTs**
  - **Evento anual para profissionais da área de Resposta a Incidentes**
- **Reuniões periódicas com diversos setores da Internet no Brasil**
  - **ex: Financeiro, Governo, Telecomunicações**
- **LAC-CSIRTs**
  - **Reunião de Grupos de Resposta a Incidentes de Segurança (CSIRTs) da região da América Latina e o Caribe**
- ***Annual National CSIRTs Meeting***
  - **CERT Division of the SEI/CMU**
- ***FIRST (Forum of Incident Response and Security Teams)***
  - **Desde 1992, promove a formação de uma rede global de CSIRTs**
  - **criar uma rede de confiança**
  - **aumentar a cooperação**
  - **facilitar acesso a uma rede de contatos**
  - **Inclui membros de diversos setores (academia, vendors, ISPs, CSIRTs nacionais)**

Segurança e Estabilidade da Internet: uma Estratégia Integrada

cert.br nic.br cgi.br

Estratégias do NIC.br/CGI.br

Mesmo sendo uma rede distribuída e descentralizada, a Internet possui diversos elementos são críticos para sua contínua operação:

- **Sistemas de registro de nomes de domínio (.br, .com, .de, etc)**
- **Sistemas de Resolução de Nomes (DNS)**
- **Recursos de Numeração**
- **Endereços IP e Sistemas Autônomos (ASNs)**
- **Roteamento**
- **Pontos de Troca de Tráfego**

NIC.br/CGI.br: Estímulo à autonomia das redes no Brasil

- **facilitação para obtenção de um ASN**
- **manutenção gratuita dos Pontos de Troca de Tráfego (IX.br)**
- **aumento da resiliência dos sistemas de resolução de nomes**
- **treinamentos em boas práticas para administração de ASNs, IPv6, DNS**
- **treinamento de especialistas em tratamento de incidentes**

Registro.br:
Segurança e Resiliência de DNS no Brasil

- **Implementação das extensões de segurança do DNS – DNSSEC – em todo o <.br>**
- **Manutenção de cópias (*mirrors*) de servidores DNS raiz (*root servers*) em diversos pontos do Território Nacional**

Presentes em 97 países:

País	servidores
EUA	86
Brasil	19
Alemanha	15
Canadá	13
França	13
Austrália	12
China	10
Itália	10
Japão	09
Inglaterra	08

Fonte: Packet Clearing House – pch.net, em 02/09/2015

IX.br (antigo PTT.br): **Melhora na Disponibilidade e Estabilidade**

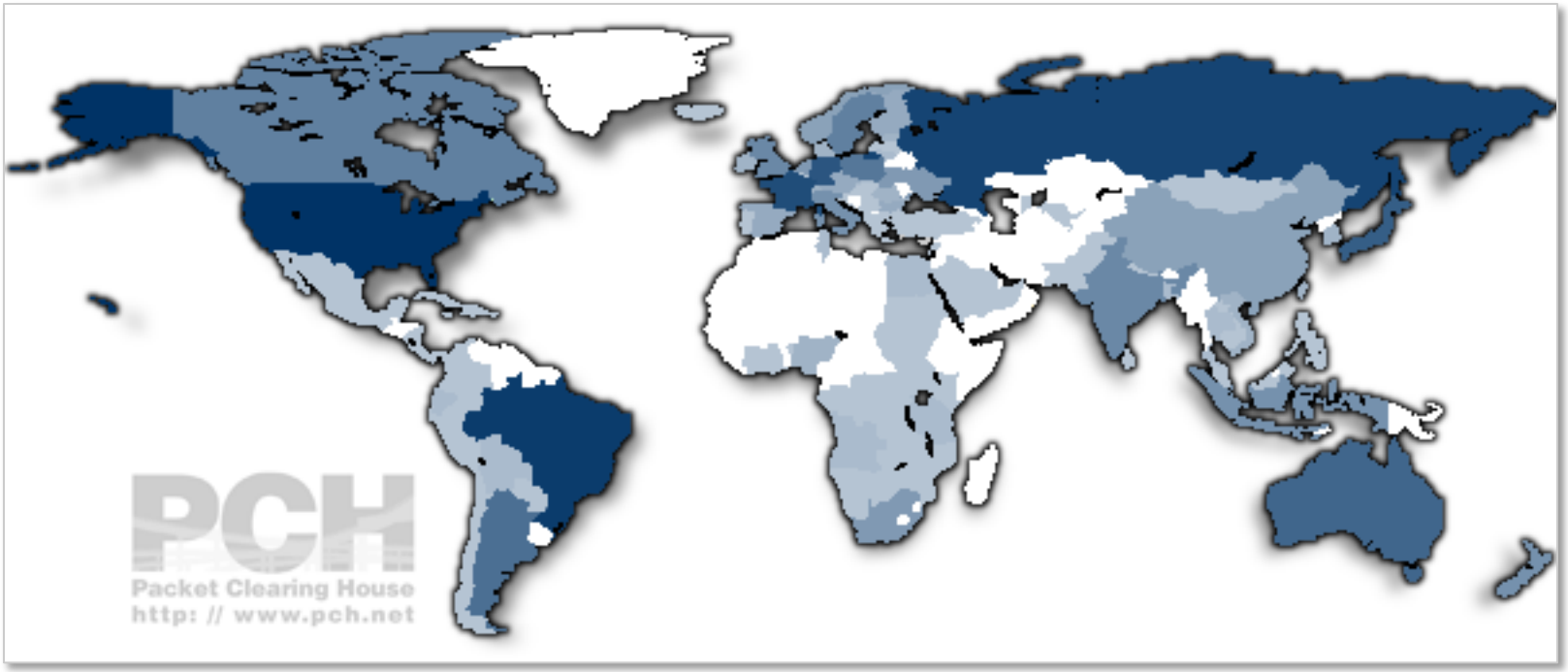
- **Objetivo primário dos Pontos de Troca de Tráfego: melhor conectividade, qualidade e redução de custo.**
- **25 pontos de troca de tráfego mantidos pelo NIC.br (1Tbps):**

  http://ix.br/localidades/atuais

Efeito para disponibilidade e estabilidade:

- **Estimula as redes a terem Sistema Autônomo (AS) próprio:**
  - **seus próprios endereços IP**
  - **mais de uma saída para Internet e possibilidade de conexão com um Ponto de Troca de Tráfego**
  - **mais flexibilidade na definição de rotas**
    - **mais facilidade para lidar com ataques de Negação de Serviço (DDoS) volumétricos**

Países com Mais Pontos de Troca de Tráfego



EUA	84	Japão	16
Brasil	27	Austrália	14
Rússia	21	Argentina	13
França	20	Polônia	10
Alemanha	19	Suécia	09

Fonte: Packet Clearing House – pch.net, em 02/09/2015

Iniciativas de Incentivo a Boas Práticas

- **DNSSEC, para segurança do sistema de nomes (DNS)**
  http://registro.br/tecnologia/dnssec.html?secao=dnssec
- **Cartilha de Segurança para Internet**
  http://cartilha.cert.br
- **Práticas Anti-Spam**
  http://antispam.br/
- **Cursos de IPv6 e de boas práticas em administração de sistemas autônomos**
  http://ipv6.br/calendario/
- **Cursos de Tratamento de Incidentes**
  http://www.cert.br/cursos/
- **Padrões Web**
  http://ceweb.br/publicacoes/indice/

Eventos para Fomentar a Cooperação

Eventos gratuitos organizados pelo NIC.br:

- **Grupo de Trabalho de Engenharia e Operação de Redes (GTER)**
- **Grupo de Trabalho em Segurança de Redes (GTS)**
- **Fórum da Internet no Brasil**
- **Seminário de Proteção à Privacidade e aos Dados Pessoais**
- **Fórum Brasileiro de CSIRTs**
- **Conferência Web W3C Brasil**
- **Semana de Infraestrutura da Internet no Brasil**
  - **PTT Fórum - Encontro dos Sistemas Autônomos da Internet no Brasil**
  - **Fórum IPv6**
  - **GTER/GTS**

http://nic.br/eventos/agenda/organiza/

Obrigada

www.cert.br

lucimara@cert.br @certbr

23 de setembro de 2015

nic.br cgi.br

www.nic.br | www.cgi.br