Grupos de Resposta a Incidentes de Segurança em Computadores (CSIRTs):

Cenário Brasileiro e Internacional

Cristine Hoepers
cristine@nic.br

NIC BR Security Office – NBSO
Brazilian Computer Emergency Response Team
http://www.nbso.nic.br/

Comitê Gestor da Internet no Brasil
http://www.cg.org.br/

Roteiro

- CSIRTs no Brasil:
  - NBSO / CGI.br
  - Outros CSIRTs
- CSIRTs no Exterior
- Iniciativas Regionais
- Considerações Finais

Histórico e Atuação do NBSO

Comitê Gestor da Internet no Brasil – CGI.br

- Criado por portaria interministerial MCT/MC 147, de 31 de maio de 1995.
  - recomendar padrões e procedimentos técnicos e operacionais para a Internet no Brasil;
  - coordenar a atribuição de endereços Internet, o registro de nomes de domínios, e a interconexão de *backbones*;
  - coletar, organizar e disseminar informações sobre os serviços Internet.

http://www.cg.org.br/sobre-cg/historia.htm

CGI.br (cont.)

Decreto Nº 4.829, de 3 de setembro de 2003:

- Dispõe sobre a criação do Comitê Gestor da Internet no Brasil - CGIbr, sobre o modelo de governança da Internet no Brasil, e dá outras providências.
- Composição: 21 membros – MCT, Casa Civil, MC, Defesa, MDIC, MP, Anatel, representantes da comunidade acadêmica e empresarial, entre outros.

http://www.cg.org.br/regulamentacao/

Criação do NBSO

Agosto/1996, documento: “Rumo à Criação de uma Coordenadoria de Segurança de Redes na Internet Brasil”, apontando a necessidade de:

- Um ponto central de contato
- Manutenção de estatísticas sobre incidentes na Internet Brasileira
- Neutralidade para coordenar ações entre redes envolvidas em incidentes
- Representação junto a órgãos internacionais de segurança

Junho/1997: criado o NBSO

http://www.cg.org.br/grupo/historico-gts.htm

Missão do NBSO

CSIRT responsável por receber, analisar e responder a incidentes de segurança em computadores envolvendo redes conectadas à Internet Brasileira. Atua:

- no trabalho de conscientização sobre os problemas de segurança
- no auxílio ao estabelecimento de novos CSIRTs no Brasil
- no desenvolvimento de documentação
- na coordenação do tratamento de incidentes

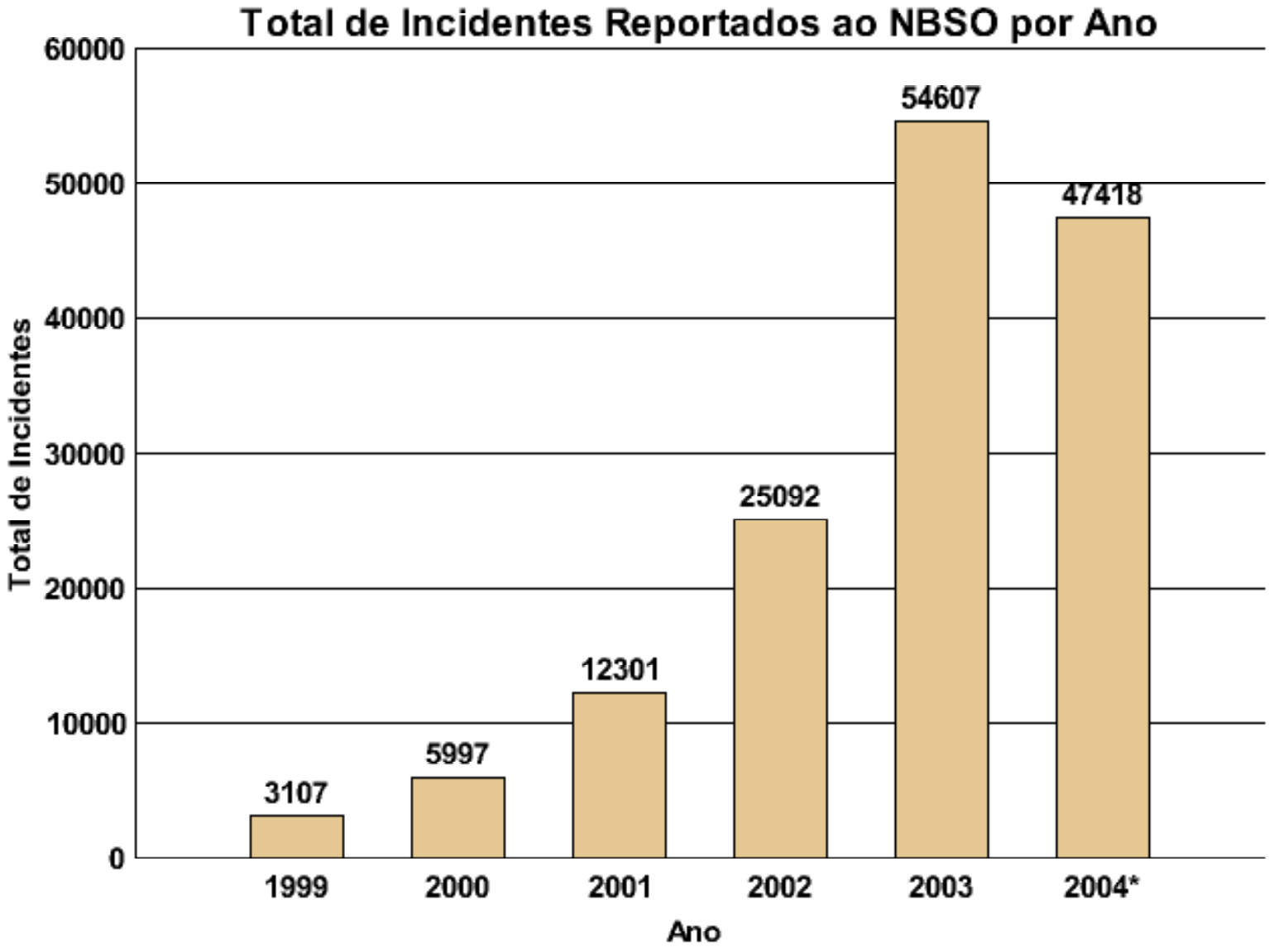
http://www.nbso.nic.br/missao.html

Serviços Prestados para Todas as Redes Conectadas à Internet no Brasil

Coordenação do Tratamento de Incidentes

- Ponto central de contato para a Internet no Brasil
- Facilitação de ações entre redes envolvidas em incidentes
  - colocar as partes em contato
  - prover apoio necessário para recuperação e análise de sistemas comprometidos
- Trabalho colaborativo com outras entidades, como as polícias, provedores, *backbones* e setor financeiro

Incidentes Reportados ao NBSO



http://www.nbso.nic.br/stats/incidentes/

Notificações

Identificação de IPs brasileiros e envio de notificações para os responsáveis das redes, com base em:

- Consultas regulares em bases mundiais de abuso
- Ataques identificados na rede de Honeypots distribuídos
  http://www.honeypots-alliance.org.br/

Controle e Acompanhamento de Notificações de Spam Recebidas via SpamCop

- Perfil do spam no Brasil: tipo mais comum e origem
- Ajudar redes brasileiras a direcionar esforços
  http://www.nbso.nic.br/stats/spam/

Documentos em Português

Produção de Documentos

- Cartilha de Segurança para Internet
  - I: Conceitos de Segurança
  - II: Riscos Envolvidos no Uso da Internet e Métodos de Prevenção
  - III: Privacidade
  - IV: Fraudes na Internet
  - V: Redes de Banda Larga e Redes Sem Fio (Wireless)
  - VI: Spam
  - VII: Incidentes de Segurança e Uso Abusivo da Rede
  - Checklist
  - Glossário

http://www.nbso.nic.br/docs/cartilha/

Documentos em Português (cont.)

Produção de Documentos

- Práticas de Segurança para Administradores de Redes

  http://www.nbso.nic.br/docs/seg-adm-redes/

- Tradução de Documentos do CERT/CC
  - Advisories

    http://www.nbso.nic.br/certcc/advisories/
  - Documentos sobre CSIRTs

    http://www.nbso.nic.br/csirts/

Formação e Capacitação de CSIRTs

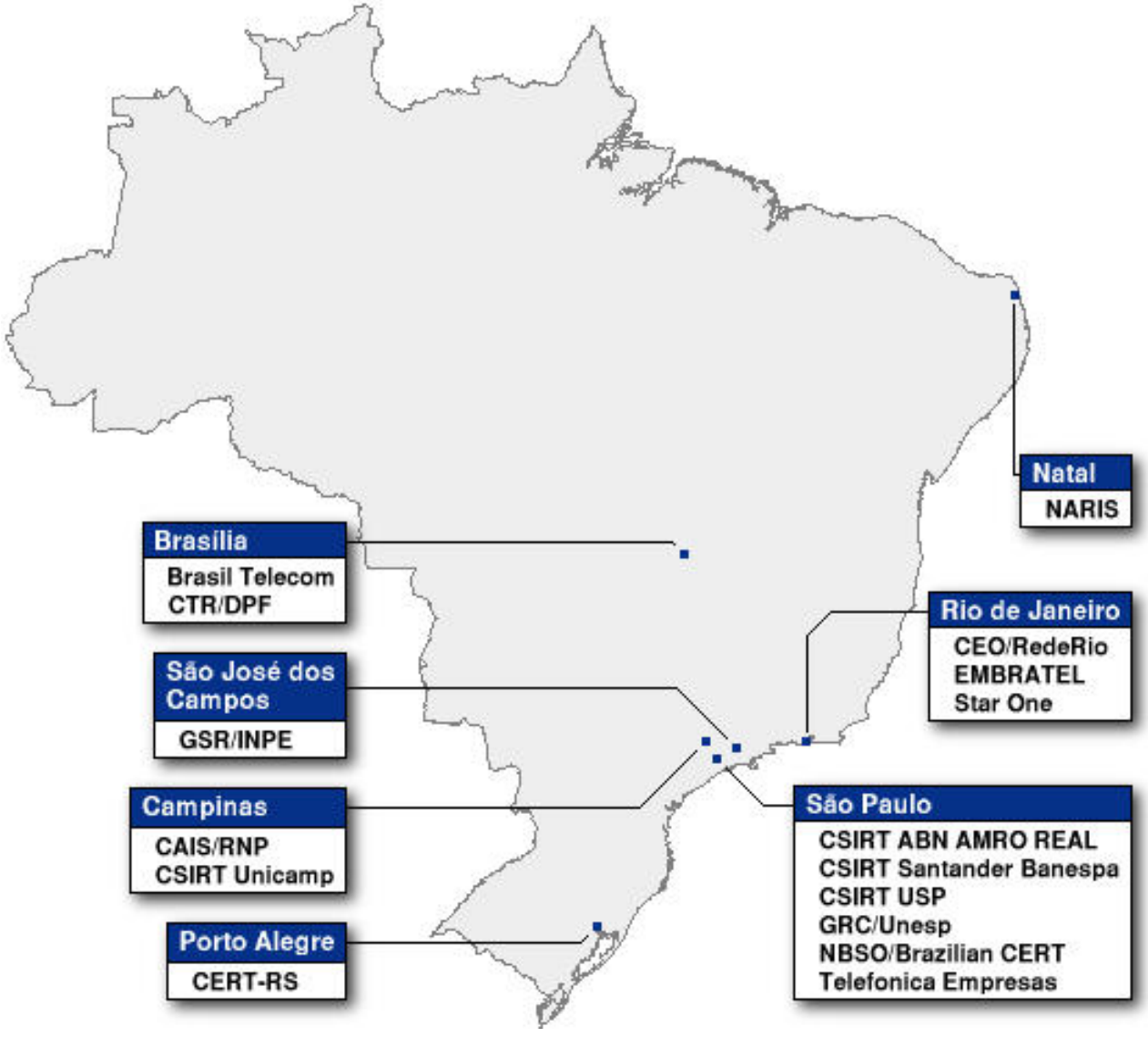
Enfoque no aumento da capacidade nacional de resposta a incidentes de segurança

- Carnegie Mellon Software Engineering Institute Partner
- Cursos do CERT Coordination Center:
  - Fundamentals of Incident Handling
  - Advanced Incident Handling for Technical Staff
  - Creating a CSIRT (a partir de 2005)
  - Managing CSIRTs (a partir de 2005)

http://www.nbso.nic.br/cursos/

CSIRTs em Atividade no Brasil

CSIRTs Brasileiros



http://www.nbso.nic.br/contato-br.html

CSIRTs Brasileiros (cont.)

Grupos não listados na página do NBSO:

- CSIRT Banco do Brasil
- CSIRT Bradesco
- Citibank
- GRA Caixa Econômica Federal
- GRA SERPRO
- Itaú
- Telemar

CSIRTs Brasileiros (cont.)

Projeto INOC-DBA* BR

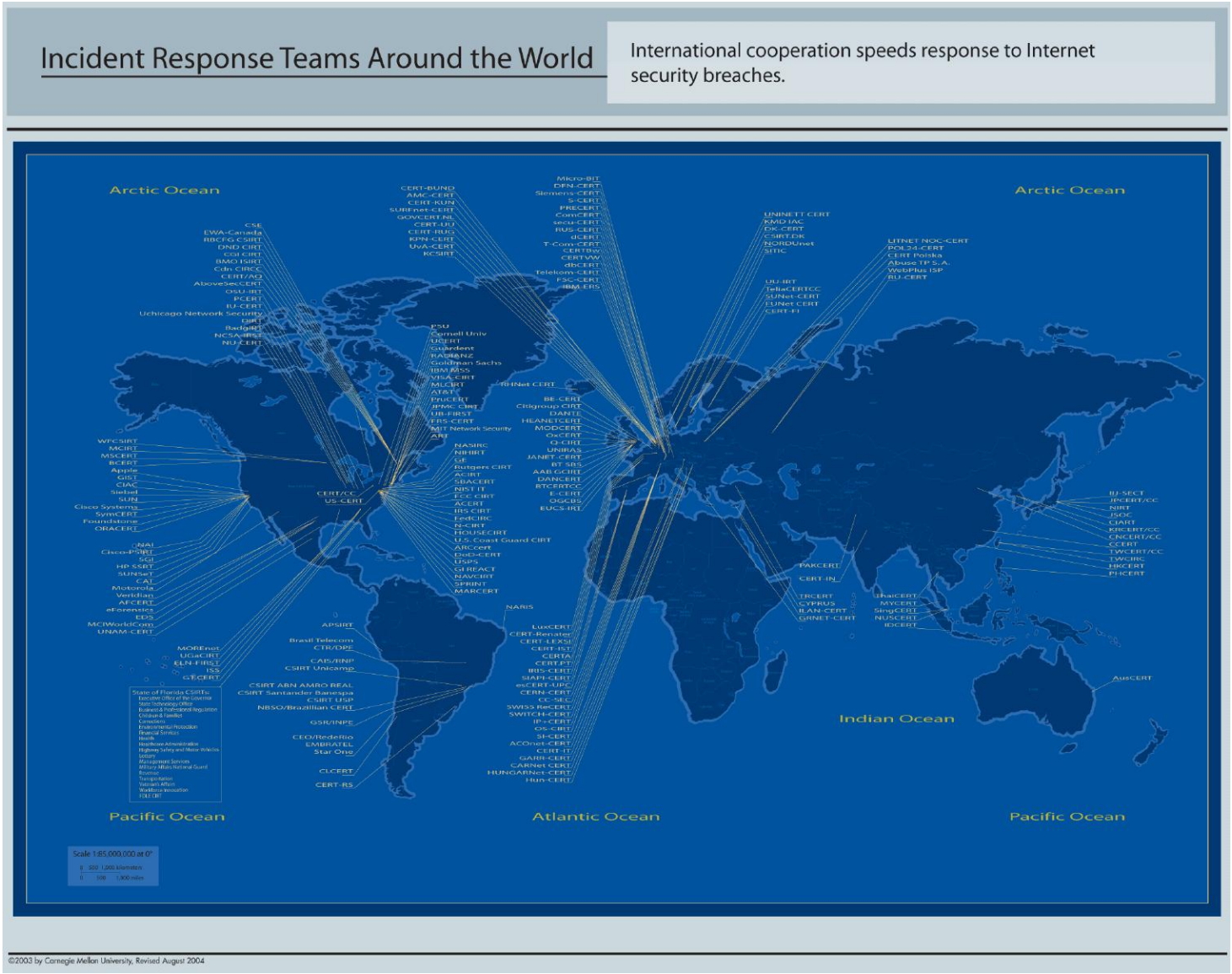
Sistema de comunicação imediata entre operadores de redes e CSIRTs, baseado em telefonia IP.

- 120 telefones IP distribuídos pelo CGI.br para:
  - 100 maiores AS (*Autonomous Systems*) do Brasil
  - 20 CSIRTs (nomeados pelo NBSO)

* INOC-DBA (Internet Network Operation Centers – Dial By AS Number) Hotline Phone System – http://www.pch.net/inoc-dba/

Cenário Internacional

CSIRTs no Mundo



Fonte: CERT Coordination Center

FIRST

Forum of Incident Response and Security Teams

- "*brings together a variety of computer security incident response teams from government, commercial, and academic organizations*"
- "*FIRST aims to foster cooperation and coordination in incident prevention, to prompt rapid reaction to incidents, and to promote information sharing among members and the community at large.*"

Fonte: http://www.first.org/

APCERT

Asia Pacific Computer Emergency Response Team

- "*It is a coalition of CSIRTs, from 12 economies across the Asia Pacific region.*"
- "*Any CSIRT from Asia Pacific Region, who is interested to furthering the objectives of APCERT, will be allowed to join as APCERT members after meeting all member accreditation requirements.*"

Fonte: http://www.apcert.org/

TF-CSIRT

Collaboration of Security Incident Response Teams

- "*Task Force established under the auspices of the TERENA Technical Programme to promote the collaboration between CSIRTs in Europe.*"
- "*activities of TF-CSIRT are focused on Europe and neighbouring countries*"
- "*Services for CSIRTs: Trusted Introducer for CSIRTs in Europe*"

Fonte: http://www.terena.nl/tech/task-forces/tf-csirt/index.html

Trusted Introducer for CSIRTs in Europe

- "*TI provides European CSIRTs with a public repository that lists all known European CSIRTs*"
- "*An important pre-requisite for mutual trust is shared and accurate operational knowledge about one another.*"
- "*The TI accreditation service is meant to do just that: facilitate trust by formally accrediting CSIRTs that are ready to take that step.*"

Fonte: http://www.ti.terena.nl/

EGC

European Government CSIRTs group

- "*EGC is an informal group of governmental CSIRTs that is developing effective co-operation on incident response matters between its members, building upon the similarity in constituencies and problem sets between governmental CSIRTs in Europe.*"
- "*Current members: CERTA (France), CERT-Bund (Germany), CERT-FI (Finland), GOVCERT.NL (The Netherlands), SITIC (Sweden), UNIRAS (United Kingdom)*"

Fonte: http://www.bsi.de/certbund/EGC/index_en.htm

Iniciativa da OEA

Inter-American CSIRT Watch and Warning Network

- "*Objective: To create a hemisphere-wide network (...) to be made up of national contact points among Computer Security Incident Response Teams (CSIRTs) in Member States of the OAS*"
- "*These teams could begin simply as official points of contact located in each State and charged with receiving computer security information, to be transformed into CSIRTs in the future.*"

Fontes: http://www.cicte.oas.org/cybersecurity_Ottawa.htm
http://www.cicte.oas.org/Docs/Informe/Informe%20final%2016%20(ingles).doc

Considerações Finais

Fatores de Sucesso

- Apoio por parte dos superiores
- Perfil e motivação dos profissionais
- Treinamento e atualização da equipe
- Reconhecimento por parte da comunidade a que atende, facilitado através:
  - da capacidade técnica
  - da qualidade das informações providas
  - do relacionamento com esta comunidade

Fatores de Sucesso (cont.)

- Grau de confiança adquirido
  - é construído a partir dos fatores anteriores
  - depende da ética dos profissionais
- Relacionamento com outros CSIRTs
  - essencial para o desempenho das funções
  - depende da confiança adquirida e do reconhecimento por parte da comunidade a que atende

Relatórios Internacionais

- CERT/CC: *"State of the Practice of Computer Security Incident Response Teams"*
  http://www.cert.org/archive/pdf/03tr001.pdf
- ITU (International Telecommunication Union): *"The Case of Brazil"*
  http://www.itu.int/osg/spu/ni/security/docs/cni.06.pdf
- Electronic Commerce Branch, Industry Canada: *"Approaches to Critical Network Infrastructure Protection"*
  http://www.cicte.oas.org/ciberseguridad.htm
- The World Bank: *"Electronic Safety and Soundness: Securing Finance in a New Age"*
  http://www.worldbank.org/

Referências

- NBSO - NIC BR Security Office
  Brazilian Computer Emergency Response Team
  http://www.nbso.nic.br/
- Comitê Gestor da Internet no Brasil
  http://www.cg.org.br/
- Material de Apoio para CSIRTs
  http://www.nbso.nic.br/csirts/
- Cursos do CERT/CC ministrados pelo NBSO
  http://www.nbso.nic.br/cursos/
- Staffing Your Computer Security Incident Response Team – What Basic Skills Are Needed?
  http://www.cert.org/csirts/csirt-staffing.html