nic.br cgi.br | cert.br

3º Correios in Company
11 de junho de 2015
Brasília, DF

Segurança, Estabilidade e Resiliência da Internet

Lucimara Desiderá
lucimara@cert.br

cert.br nic.br cgi.br

Comitê Gestor da Internet no Brasil – CGI.br

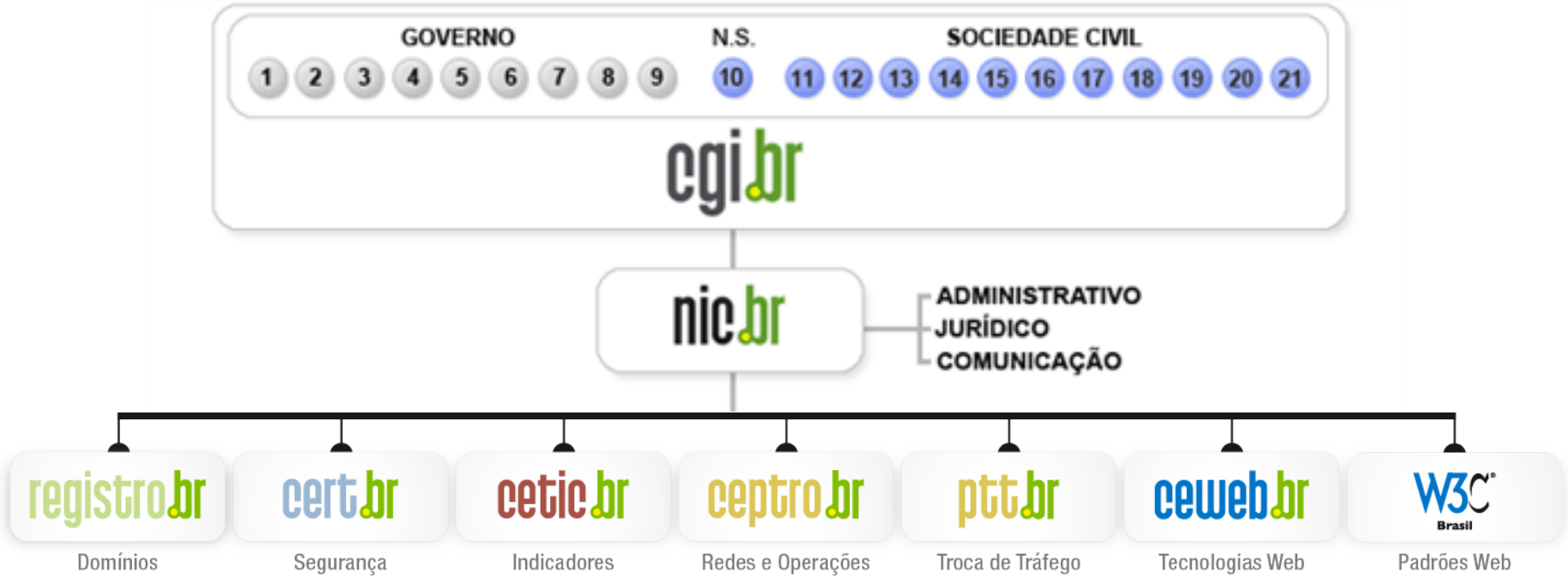
Tem a missão de estabelecer diretrizes estratégicas relacionadas ao uso e desenvolvimento da Internet no Brasil

Dentre as atribuições definidas no Decreto Presidencial nº 4.829, de 03 de setembro de 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;**

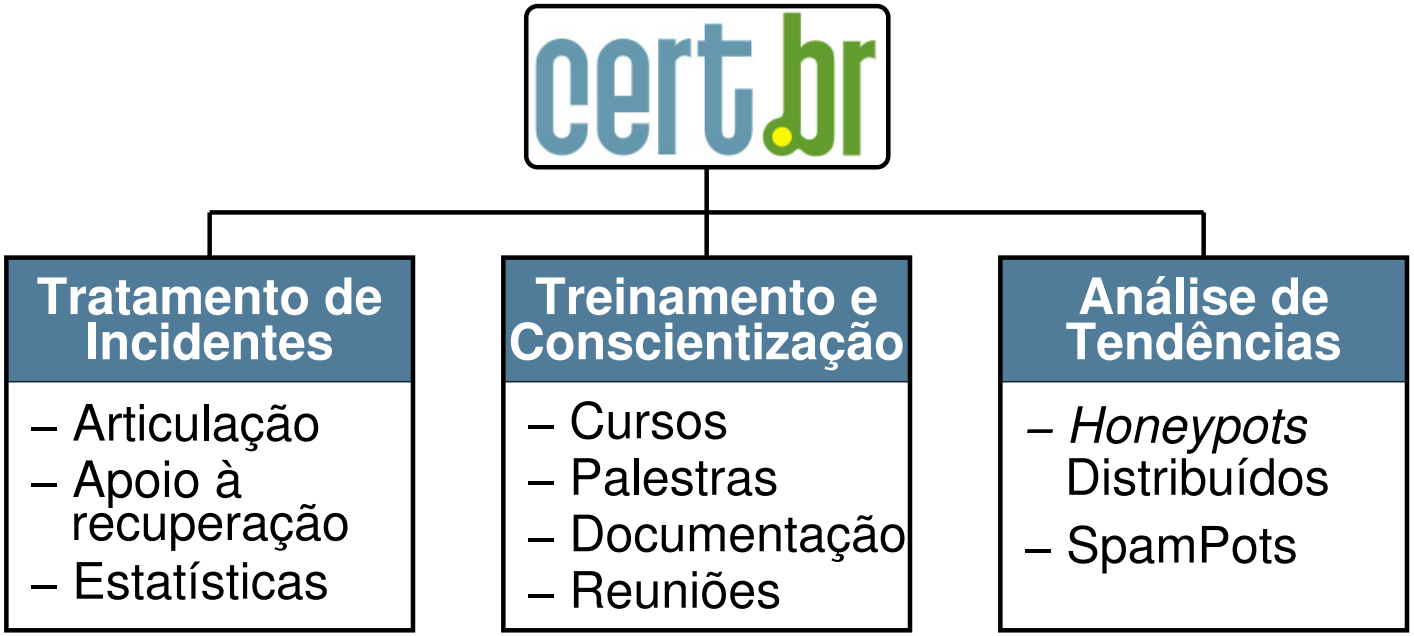
http://www.cgi.br/sobre/

Estrutura do CGI.br e NIC.br



1 – Ministério da Ciência e Tecnologia (Coordenação)
2 – Ministério das Comunicações
3 – Casa Civil da Presidência da República
4 – Ministério da Defesa
5 – Ministério do Desenvolvimento, Indústria e Comércio Exterior
6 – Ministério do Planejamento, Orçamento e Gestão
7 – Agência Nacional de Telecomunicações (Anatel)
8 – Cons. Nacional de Desenvolvimento Científico e Tecnológico
9 – Fórum Nac. de Secretários Estaduais para Assuntos de C&T
10 – Representante de Notório Saber em assuntos de Internet

11 – provedores de acesso e conteúdo
12 – provedores de infra-estrutura de telecomunicações
13 – indústria de bens de informática, telecomunicações e software
14 – segmento das empresas usuárias de Internet
15-18 – representantes do terceiro setor
19-21 – representantes da comunidade científica e tecnológica



SEI Partner
Carnegie Mellon

FIRST
Improving Security Together
MEMBER

APWG
RESEARCH PARTNER
www.antiphishing.org

The Honeynet PROJECT

Criado em 1997 para:

- **Ser um ponto de contato nacional para notificação de incidentes**
- **Prover a facilitação e o apoio necessários no processo de resposta a incidentes**
- **Estabelecer um trabalho colaborativo com outras entidades**
- **Aumentar a conscientização sobre a necessidade de segurança na Internet**
- **Auxiliar novos CSIRTs (Grupos de Tratamento de Incidentes de Segurança) a estabelecerem suas atividades**

Rumo a Criação de uma Coordenadoria de Segurança de Redes na Internet Brasil
http://www.nic.br/grupo/historico-gts.htm | http://www.cert.br/sobre/

Segurança no Contexto de Governança da Internet

cert.br nic.br cgi.br

WSIS:
Declaration of Principles

Document WSIS-03/GENEVA/DOC/4-E

12 December 2003

[...]

B5) Building confidence and security in the use of ICTs

35. Strengthening the trust framework, including information security and network security, authentication, privacy and consumer protection, is a prerequisite for the development of the Information Society and for building confidence among users of ICTs.

[...]

http://www.itu.int/wsis/docs/geneva/official/dop.html

CGI.br:
Princípios para a Governança e Uso da Internet no Brasil

CGI.br/RES/2009/003/P - PRINCÍPIOS PARA A GOVERNANÇA E USO DA INTERNET NO BRASIL

Fevereiro de 2009

[...]

8. Funcionalidade, segurança e estabilidade
A estabilidade, a segurança e a funcionalidade globais da rede devem ser preservadas de forma ativa através de medidas técnicas compatíveis com os padrões internacionais e estímulo ao uso das boas práticas.

[...]

http://www.cgi.br/resolucoes/documento/2009/003

NETmundial:
Internet Governance Principles

NETmundial Multistakeholder Statement

April, 24th 2014, 19:31 BRT

[...]

SECURITY, STABILITY AND RESILIENCE OF THE INTERNET

Security, stability and resilience of the Internet should be a key objective of all stakeholders in Internet governance. As a universal global resource, the Internet should be a secure, stable, resilient, reliable and trustworthy network. Effectiveness in addressing risks and threats to security and stability of the Internet depends on strong cooperation among different stakeholders.

[...]

http://www.netmundial.org/references/

E o que observamos?

cert.br nic.br cgi.br

US restaurant chain P.F. Chang's China Bistro plans to temporarily bring back manual credit card imprinting while it investigates a security breach that allowed hackers to steal customer payment card data from multiple stores.

P.F. Chang's turns to vintage 1970s tech after credit card breach

Restaurant chain goes old school as it investigates theft from multiple stores.

by **Dan Goodin** - June 13 2014, 1:47pm BRT

HACKING INTERNET CRIME 207

Consegue-se Quase Tudo no Mercado Negro

Overall Rank		Item	Percentage		2010 Price Ranges
2010	2009		2010	2009	
1	1	Credit card information	22%	19%	$0.07–$100
2	2	Bank account credentials	16%	19%	$10–$900
3	3	Email accounts	10%	7%	$1–$18
4	13	Attack tools	7%	2%	$5–$650
5	4	Email addresses	5%	7%	$1/MB–$20/MB
6	7	Credit card dumps	5%	5%	$0.50–$120
7	6	Full identities	5%	5%	$0.50–$20
8	14	Scam hosting	4%	2%	$10–$150
9	5	Shell scripts	4%	6%	$2–$7
10	9	Cash-out services	3%	4%	$200–$500 or 50%–70% of total value

Fonte: Underground Economy Servers—Goods and Services Available for Sale
http://www.symantec.com/es/es/threatreport/topic.jsp?id=fraud_activity_trends&aid=underground_economy_servers

Russian Underground – Serviços Disponíveis

- **Pay-per-Install (global mix or specific country): $12–$550**
- **Bulletproof-hosting with DDoS protection: $2000 per month**
- **Styx Sploit Pack rental (affects Java and Adobe Acrobat and Flash Player) $3000/month**
- **Programming: web server hacking $250; browser-in-the-middle $850; trojans $1300**
- **Windows rootkit (for installing malicious drivers): $292**
- **Linux rootkit: $500**
- **Hacking Facebook or Twitter account: $130**
- **Hacking Gmail account: $162**
- **Hacking corporate mailbox: $500**

"Setup of ZeuS: US$100, support for botnet: US$200/month, consulting: US$30."

Offering	Price
Bots (i.e., consistently online 40% of the time)	US$200 for 2,000 bots
DDoS botnet	US$700
DDoS botnet update	US$100 per up

Offering	Price
1-day DDoS service	US$30-70
1-hour DDoS service	US$10
1-week DDoS service	US$150
1-month DDoS service	US$1,200

Fonte: Read Russian Underground 101 - Trend Micro
http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-101.pdf

Incorporando Segurança e Resiliência

cert.br nic.br cgi.br

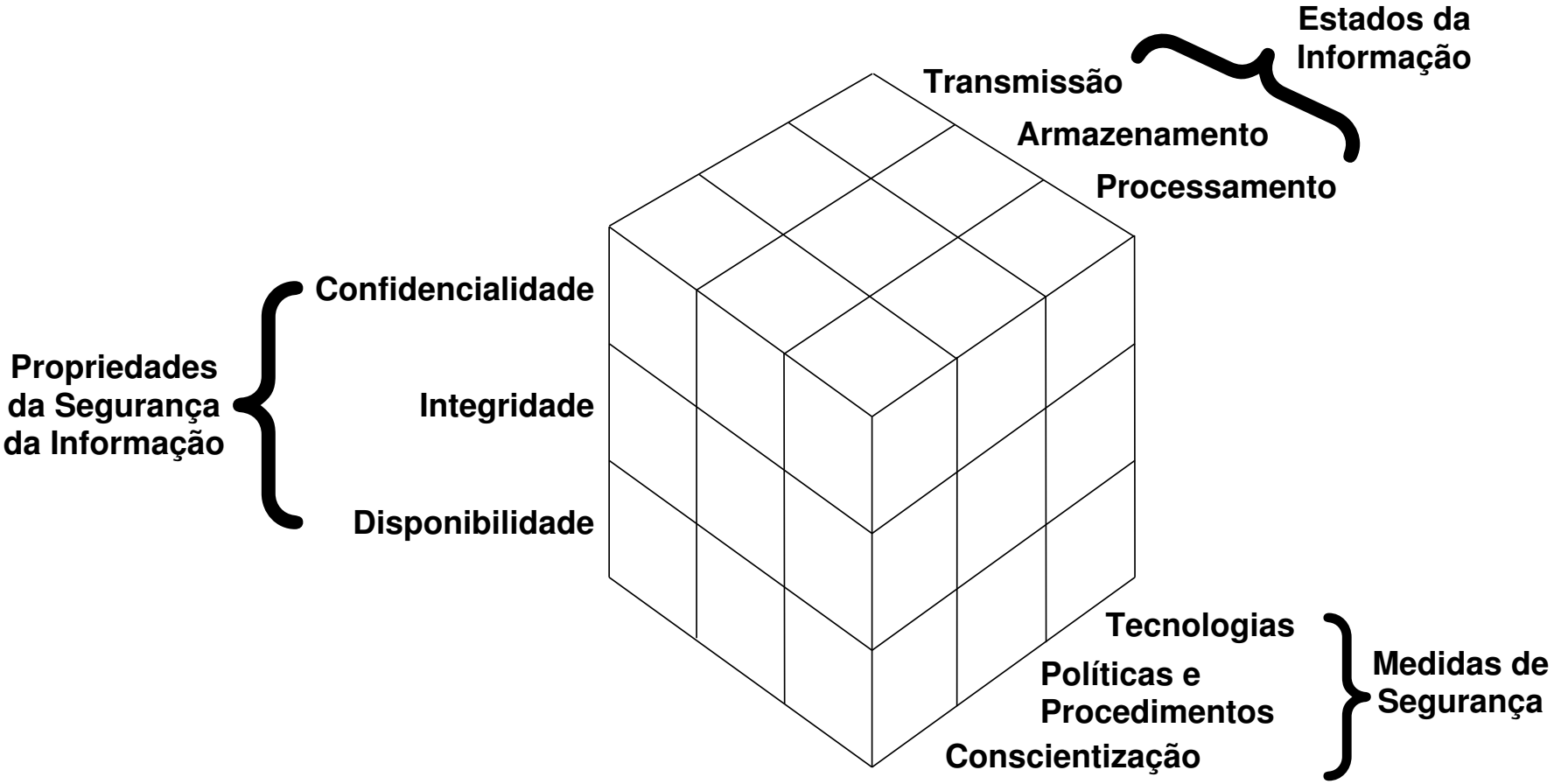
Riscos em Sistemas Conectados à Internet

- indisponibilidade de serviços
- perda de privacidade
- furto de dados
- perdas financeiras
- danos à imagem
- **perda de confiança na tecnologia**

- criminosos
- espionagem industrial
- governos
- vândalos

- defeitos de *software*
- falhas de configuração
- uso inadequado
- fraquezas advindas da complexidade dos sistemas

As informações estão em diversos locais e a segurança depende de múltiplos fatores



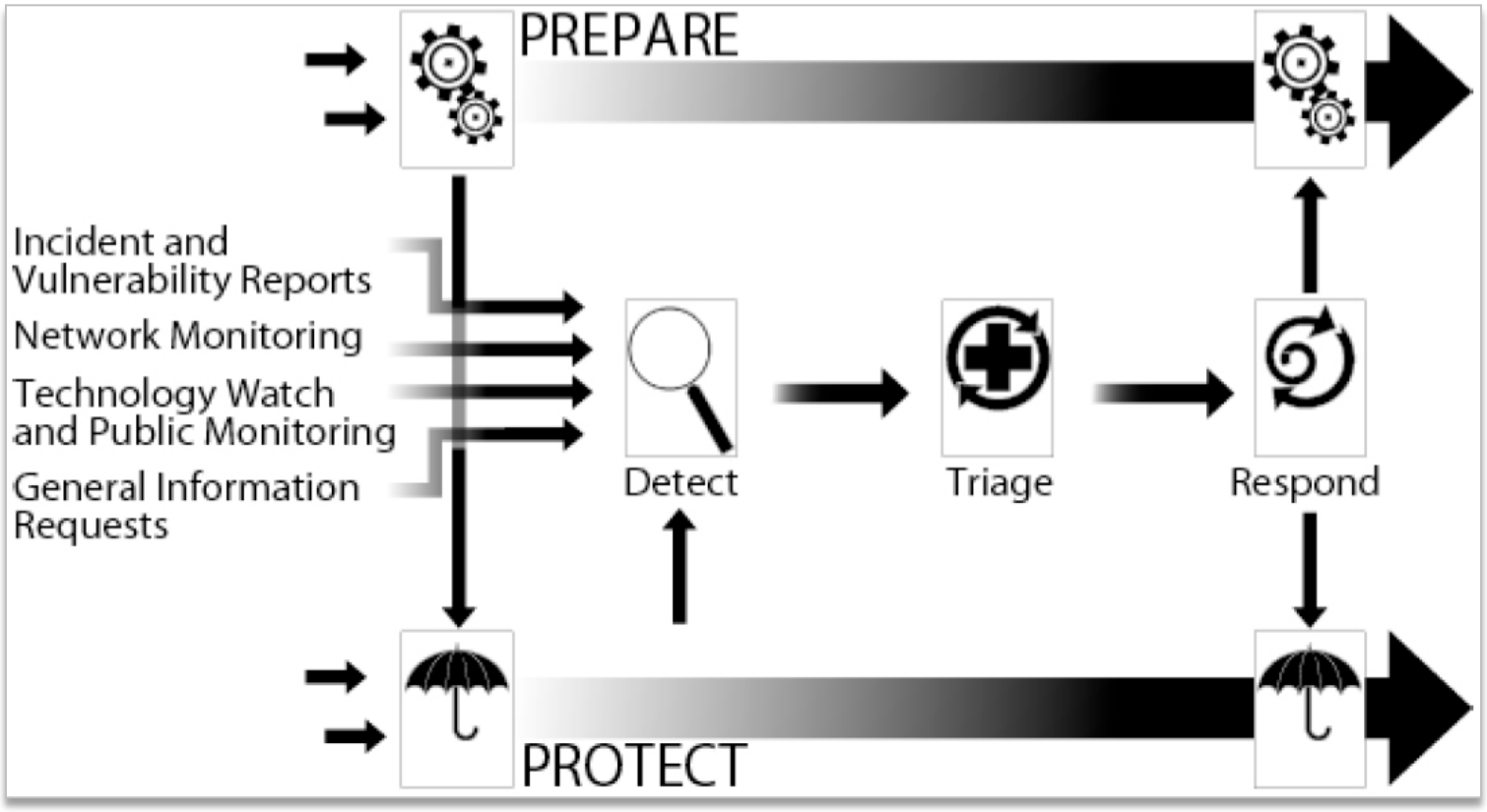
McCumber Information Security Model
http://www.ibm.com/developerworks/security/library/s-confnotes2/

Resiliência

- **Foco deixa de ser em se recuperar de ataques ou incidentes**
- **Foco é continuar operando mesmo na presença de falhas ou ataques**
  - **Não existe segurança 100%**
- **Alcançar um nível aceitável de segurança, busca-se atingir os seguintes objetivos:**
  - **Detectar comprometimentos o mais rápido possível**
  - **Diminuir o impacto**
    - **Conter, mitigar e recuperar de ataques o mais rápido possível**
- **Só é atingida com a integração de diversos processos de TI, Segurança e Continuidade de Negócios, incluindo:**
  - **Gestão de riscos**
  - **Treinamento e conscientização**
  - **Gestão de incidentes de segurança**
    - De acordo com o relatório da Mandiant "M-Trends® 2015: A View from the Frontlines", **69% das instituições vítimas de comprometimento souberam do problema por meio de notificação recebida de entidade externa**.

Gestão, Tratamento e Resposta a Incidentes

Gestão de Incidentes – políticas e processos que permitem a identificação e o tratamento de incidentes de segurança



Fonte: ***Defining Incident Management Processes for CSIRTs: A Work in Progress*****.**
Figura utilizada com permissão do CERT®/CC e do SEI/CMU.

Grupos de Resposta a Incidentes de Segurança - CSIRTs

Organização ou área responsável por receber, analisar e responder a notificações e atividades relacionadas a incidentes de segurança em computadores

Outros acrônimos: IRT, CERT, CIRC, CIRT, SERT, SIRT

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

A redução do impacto de um incidente é conseqüência:

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

O sucesso depende da confiabilidade

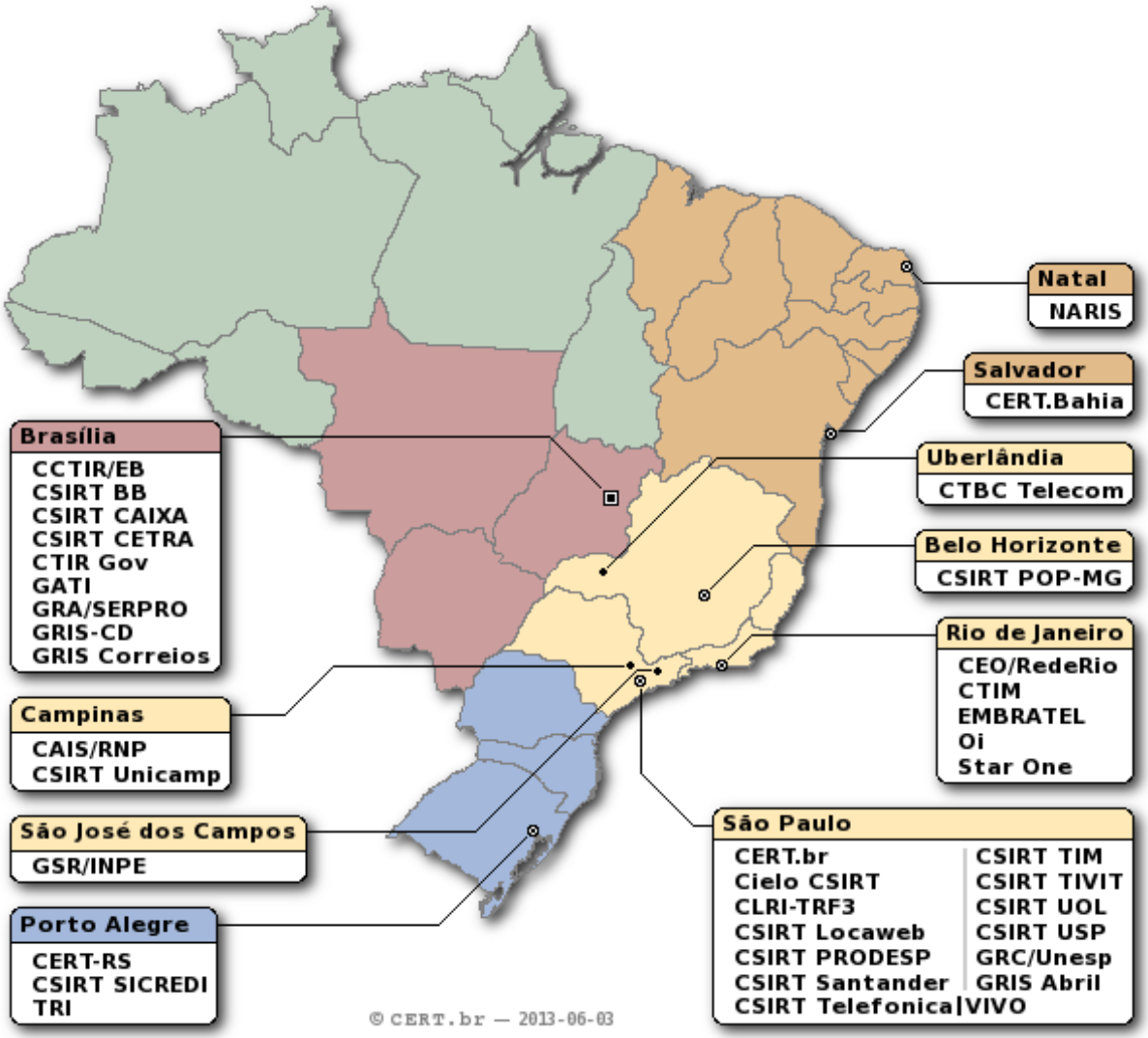
- nunca divulgar dados sensíveis nem expor vítimas, por exemplo

O CSIRT não é um investigador / polícia / juiz

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/

Considerações Finais

Melhorar a Infraestrutura

- **AS próprio, permitindo**
  - seus próprios endereços IP
    - mais facilidade para mudar de operadoras em situações de crise
  - mais de uma saída para Internet e conexão com um PTT (http://ix.br/)
  - mais flexibilidade na definição de rotas
    - mais facilidade para lidar com ataques de Negação de Serviço (DDoS) volumétricos
- **Adoção de IPv6**
  - preparação dos sistemas para IPv6 (firewalls, SIEMs, DBs)
  - chave para a expansão da Internet e dos negócios

Cooperação interna e externa é chave

- nenhum único grupo ou estrutura conseguirá fazer sozinho a segurança ou a resposta a incidentes
- pessoal preparado em todas as redes e áreas

Não faça parte do problema

- Implementar boas práticas

Referências

cert.br nic.br cgi.br

Referências

- **CERT.br**
  http://www.cert.br/
- **Recomendações para Notificações de Incidentes de Segurança**
  http://www.cert.br/docs/whitepapers/notificacoes/
- **Cyber Risk and Resilience Management CERT-RMM**
  http://www.cert.org/resilience/
- **Improving the Security and Resilience of U.S. Postal Service Mail Products and Services Using the CERT® Resilience Management Model**
  http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=77277
- **CERT Resilience Management Model—Mail-Specific Process Areas: International Mail Transportation (Version 1.0)**
  http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=296395
- **CERT® Resilience Management Model (RMM) v1.1: Code of Practice Crosswalk Commercial Version 1.1**
  http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=9849

Educação de Usuários:
Cartilha de Segurança para Internet

Livro (PDF e ePub) e conteúdo no *site* (HTML5)
Dica do dia no site, via *Twitter* e RSS
http://cartilha.cert.br/

Cartilha de Segurança para Internet
Fascículos

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**

Acompanhados de *Slides* de uso livre para:

- **ministrar palestras e treinamentos**
- **complementar conteúdos de aulas**

Obrigada

www.cert.br

lucimara@cert.br @certbr

11 de junho de 2015

nic.br cgi.br

www.nic.br | www.cgi.br