
egi
Escola de Governança
da Internet no Brasil

Fundamentos de Segurança da Informação

Cristine Hoepers, D.Sc.
Klaus Steding-Jessen, D.Sc.

19/07/2016 – 18:30 às 19:30h

Objetivos

Discutir os conceitos técnicos relacionados com segurança, privacidade e resiliência de sistemas conectados à Internet

- De forma não exaustiva

Subsidiar os participantes para as crescentes discussões sobre privacidade, segurança, estabilidade e resiliência nos fóruns nacionais e internacionais de governança da Internet

- Embasamento técnico para identificar e questionar falácias, mitos e artigos não embasados

Segurança e Governança da Internet

egi

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/

Segurança da Informação

egi

Propriedades da Segurança da Informação

Confidencialidade – é a necessidade de garantir que as informações sejam divulgadas somente para aqueles que possuem autorização para vê-las.

Ex. de quebra: alguém obtém acesso não autorizado ao seu computador e lê todas as informações contidas na sua declaração de Imposto de Renda

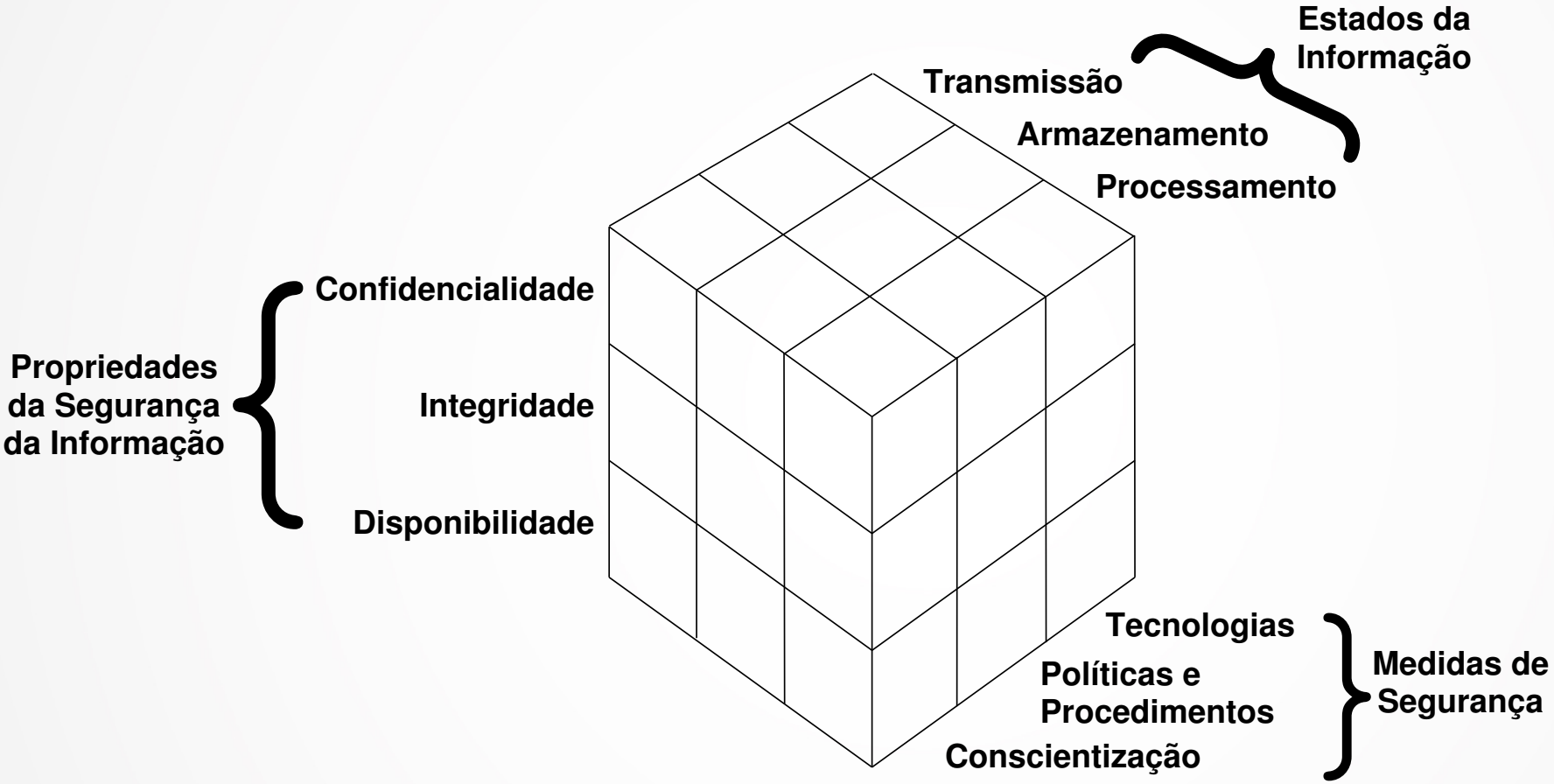
Integridade – é a necessidade de garantir que as informações não tenham sido alteradas acidentalmente ou deliberadamente, e que elas estejam corretas e completas.

Ex. de quebra: alguém obtém acesso não autorizado ao seu computador e altera informações da sua declaração de Imposto de Renda, momentos antes de você enviá-la à Receita Federal.

Disponibilidade – é a necessidade de garantir que os propósitos de um sistema possam ser atingidos e que ele esteja acessível àqueles que dele precisam.

Ex. de quebra: o seu provedor sofre uma grande sobrecarga de dados ou um ataque de negação de serviço e por este motivo você fica impossibilitado de enviar sua declaração de Imposto de Renda à Receita Federal.

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/

Privacidade vs. Confidencialidade

Do ponto de vista de Segurança da Informação:

Privacidade – habilidade e/ou direito de proteger suas informações pessoais, extende-se à habilidade e/ou direito de prevenir invasões do seu espaço pessoal.

Confidencialidade – envolve a obrigação de proteger os segredos de outras pessoas ou organizações, se você souber deles.

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**

Sistemas na Internet

Riscos

Atacantes

- criminosos
- espionagem industrial
- governos
- vândalos

Vulnerabilidades

- projeto sem levar em conta segurança
- defeitos de *software*
- falhas de configuração
- uso inadequado
- fraquezas advindas da complexidade dos sistemas

Importância da Criptografia

Criptografia

- ciência e a arte de escrever mensagens em forma cifrada ou em código
- é um dos principais mecanismos de segurança

É a base para o funcionamento de:

- certificados e assinaturas digitais
- mecanismos de autenticação
- conexão segura na Web (HTTPS)
- conexão segura para outras aplicações na Internet (SSL/TLS, IPSec)
- proteção de dados armazenados em disco, em mídias removíveis e dispositivos móveis
- integridade de consultas DNS (DNSSEC)

Cartilha de Segurança para a Internet, Capítulo 9
ISBN: 978-85-60062-54-6 **–** http://cartilha.cert.br/livro/

Registros de Eventos (*Logs*)

São os registros de atividades gerados por programas e serviços de:

- computadores (servidores e clientes);
- elementos de rede;
- dispositivos.

Formatos

- são definidos pelos desenvolvedores dos sistemas e aplicações
- cada serviço tem necessidades diferentes

Qualidade dos *logs*

- horário sincronizado (NTP – http://ntp.br/)
- data completa, incluindo ano e fuso horário

A partir da análise destas informações é possível:

- registrar as atividades normais;
- detectar problemas de *hardware* ou nos programas e serviços instalados no computador;
- detectar um ataque ou o uso indevido do sistema.

Cartilha de Segurança para a Internet, Seção 7.6
ISBN: 978-85-60062-54-6 **–** http://cartilha.cert.br/livro/

Exemplo de Registros de Eventos: *Logs* de funcionamento de sistema

Jul 4 10:47:01 localhost UserEventAgent[11]: CaptiveNetworkSupport:CreateInterfaceWatchList:2788 **WiFi Devices Found. :)**

Jul 4 10:47:02 localhost configd[14]: **network configuration changed.**

Jul 28 15:07:21 notebook **Software Update[443]: Can't instantiate distribution from** http://swcdn.apple.com/content/downloads/11/05/041-0925/g27esO4pw9re5ggrfp3suf8ew6t53asfz8/041-0925.English.dist: **Error** Domain=NSXMLParserErrorDomain Code=4 "zero length data" UserInfo=0x7fed3da20e50 {NSLocalizedDescription=zero length data}

Exemplo de Registros de Eventos: *Logs* de *firewall* pessoal

#Software: Microsoft Windows Firewall

2005-04-11 08:05:57 DROP UDP 123.45.678.90 123.456.78.255 137 137 78 - - - - - - - - RECEIVE

#Software: MacOS X Firewall

Jul 18 16:40:11 notebook Firewall[65]: Stealth Mode **connection attempt to TCP 192.0.2.209:80 from 118.244.186.157:53031**

Jul 18 16:46:22 notebook Firewall[65]: Stealth Mode **connection attempt to TCP 192.0.2.209:8080 from 118.244.186.157:53031**

Jul 18 16:49:30 notebook Firewall[65]: Stealth Mode **connection attempt to TCP 192.0.2.209:3128 from 118.244.186.157:53031**

Jul 18 16:59:09 notebook Firewall[65]: Stealth Mode **connection attempt to TCP 192.0.2.209:22 from 116.10.191.176:6000**

Jul 18 17:40:20 notebook Firewall[65]: Stealth Mode **connection attempt to UDP 192.0.2.209:5060 from 199.19.109.76:5079**

Exemplo de Registros de Eventos: ***Logs* de autenticação em uma conta de um sistema**

```
Mar 29 13:36:52 computador sshd[2540]: Accepted
keyboard-interactive/pam for usuario from 192.0.2.68
port 16608 ssh2
Mar 29 13:36:53 computador sshd: usuario [priv][2540]:
USER_PROCESS: 2548 ttys001


Mar 29 13:42:14 computador sshd[2556]: Accepted
keyboard-interactive/pam for usuario from
2001:db8:0:2001::68 port 29580 ssh2
Mar 29 13:42:14 computador sshd: usuario [priv][2556]:
USER_PROCESS: 2559 ttys001
```

Detecção de Atividades Maliciosas na Rede

Existem inúmeras maneiras de detectar atividades maliciosas

As mais comuns são:

Logs* de *firewall

IDS (*Intrusion Detection System*) – programa, ou um conjunto de programas, cuja função é detectar atividades maliciosas ou anômalas

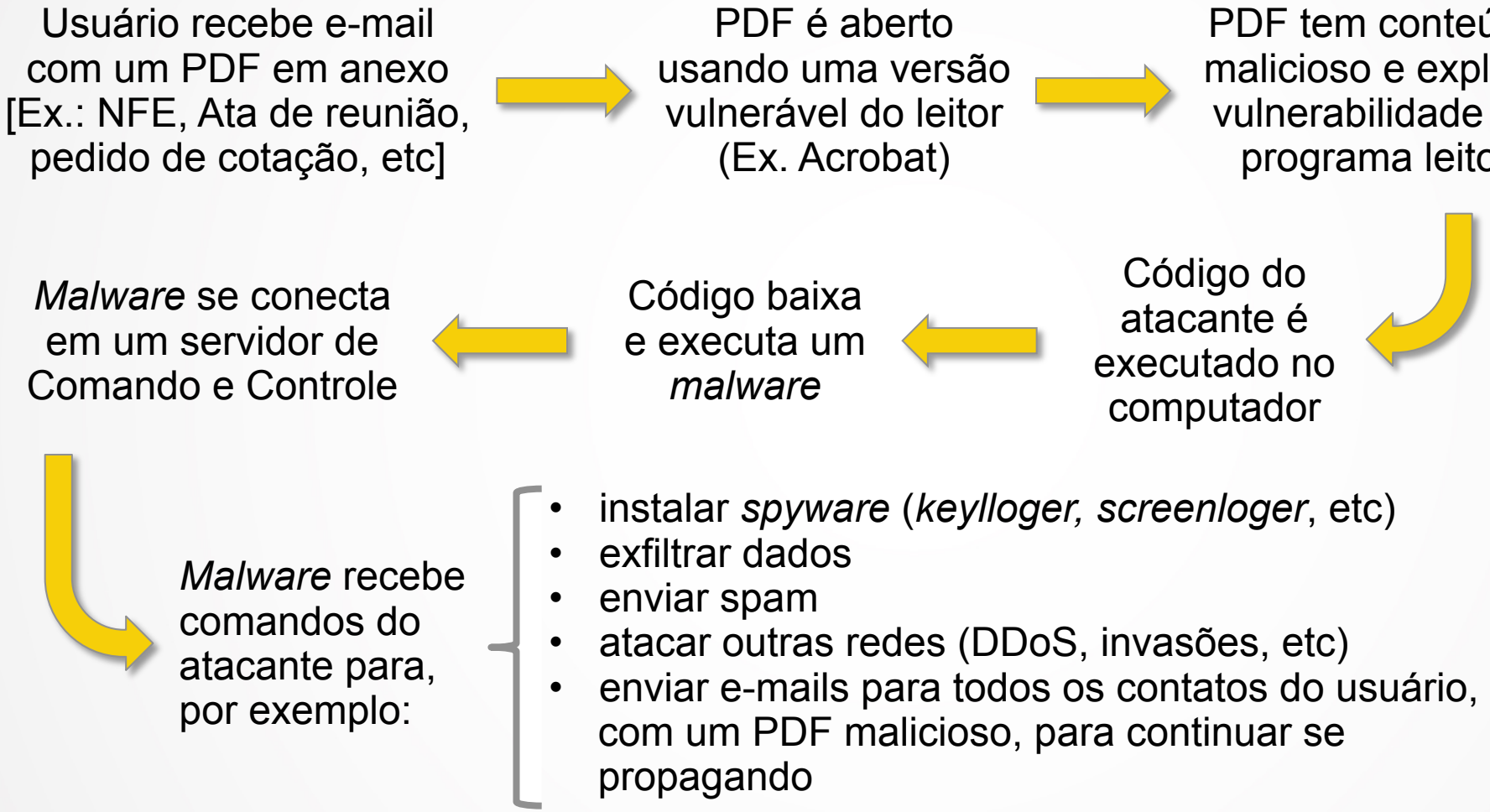
- geralmente implementado com base na análise de *logs* ou de tráfego de rede, em busca de padrões de ataque pré-definidos.

Fluxos de rede (*Netflows*) – sumarização de tráfego de rede

- armazena IPs, portas, bytes e pacotes trafegados
- permite identificar anomalias na rede
- em segurança usado para identificar:
  - ataques de negação de serviço
  - identificar computadores comprometidos

Cenários Comuns de Ataques

Cenário:
Ataque Contra Usuários de Internet



Cenário:
Ataque Contra Servidores Web

Atacante instala ferramentas em um *site* já comprometido

Varre a Internet em busca de *sites* com sistemas CMS (Wordpress, Joomla, etc)

Constrói uma lista de *sites* a serem atacados

Em cada *site* realiza um ataque de força bruta de *logins* e senhas

Ao conseguir acesso ao *site* pode, entre outras coisas:

- alterar o seu conteúdo (*defacement*)
- desferir ataques contra outros sistemas ou redes (como DDoS, enviar *spam*, tentar invadir outros sistemas, etc)
- levantar páginas de *phishing*
- inserir *scripts* maliciosos, que são executados pelos navegadores dos visitantes (para infectar os usuários, alterar configurações do modem/wi-fi, etc)
- instalar suas ferramentas e iniciar a busca por outros *sites* com CMS para reiniciar o ciclo do ataque

Resiliência

Resiliência

Um sistema 100% seguro é muito difícil de atingir

Novo paradigma: Resiliência

Continuar funcionando mesmo na presença de falhas ou ataques

- Identificar o que é crítico e precisa ser mais protegido
- Definir políticas (de uso aceitável, acesso, segurança, etc)
- Treinar profissionais para implementar as estratégias e políticas de segurança
- Treinar e conscientizar os usuários sobre os riscos e medidas de segurança necessários
- Implantar medidas de segurança que implementem as políticas e estratégias de segurança
  - como: aplicar correções ou instalar ferramentas de segurança
- Formular estratégias para gestão de incidentes de segurança e formalizar grupos de tratamento de incidentes

Gestão de Incidentes e Correlatos

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

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

CSIRT – acrônimo internacional para designar um Grupo de Resposta a Incidentes de Segurança, uma organização 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

Inserção nas discussões de Governança:

IGF Best Practices Forums

- Establishing and supporting CSIRTs for Internet security
- Regulation and mitigation of unsolicited communications (*spam*)

2015: http://www.intgovforum.org/cms/best-practice-forums/2015-best-practice-forum-outputs

2014: http://www.intgovforum.org/cms/best-practice-forums/igf-2014-best-practices-forums

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 um investigador

Evolução histórica:
Tratamento de Incidentes no Brasil

Agosto/1996: o relatório "Rumo à Criação de uma Coordenadoria de Seguraça de Redes na Internet Brasil" é publicado pelo CGI.br[1]

Junho/1997: o CGI.br cria o CERT.br (naquele tempo chamado NBSO – *NIC BR Security Office*), com base nas recomendações do relatório, como um grupo com responsabilidade nacional[2]

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

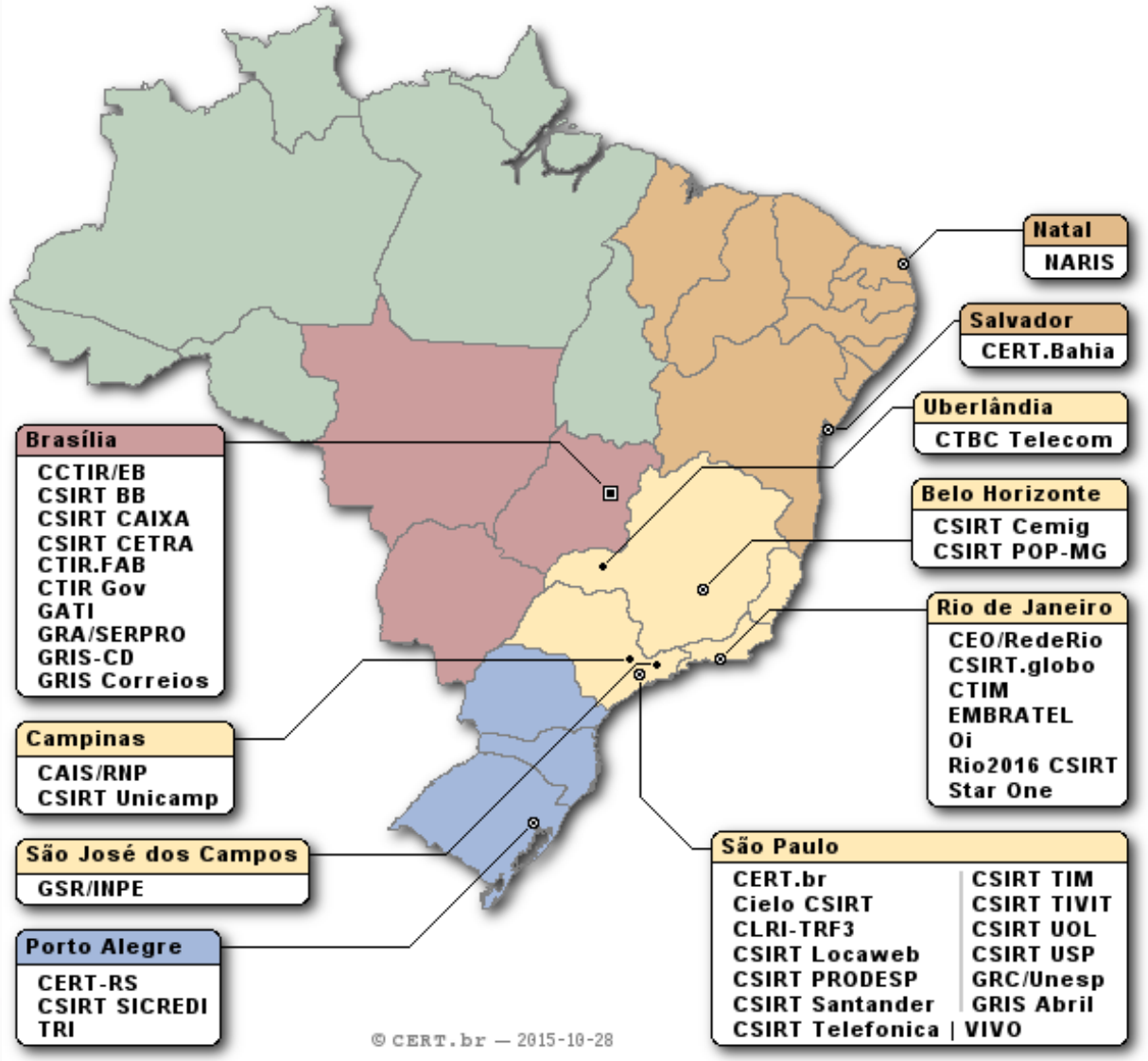
2002–2004 : grupos de trabalho para definição da estrutura de um CSIRT para a Administração Pública Federal

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

[1] http://www.nic.br/pagina/grupos-de-trabalho-documento-gt-s/169
[2] http://www.nic.br/pagina/gts/157
[3] http://memoria.rnp.br/_arquivo/documentos/rel-rnp98.pdf
[4] http://www.cert-rs.tche.br/index.php/missao
[5] http://www.ctir.gov.br/sobre-CTIR-gov.html

Grupos de Tratamento de Incidentes Brasileiros:
41 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, 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/

Fóruns Internacionais de Segurança

FIRST – *Forum of Incident Response and Security Teams*

- **Criação:** 1990
- **Membros:** 326 CSIRTs, de mais de 70 países, participantes de todos os setores;

APWG – (originalmente *AntiPhishing Working Group*)

- **Criação:** 2003
- **Membros:** 2000 organizações, participantes de todos os setores, incluindo organizações internacionais;

M³AAWG – *Messaging, Mobile, Malware Anti-Abuse Working Group*

- **Criação:** 2004
- **Membros:** Indústria – "*Internet Service Providers (ISPs), telecomm companies, Email Service Providers (ESP), social networking companies, leading hardware and software vendors, major brands, major antivirus vendors and numerous security vendors*"

Referências:
Fontes dos Conceitos Apresentados

Cartilha de Segurança para a Internet
http://cartilha.cert.br/

Security Engineering, 2nd Edition, 2008, Ross Anderson
http://www.cl.cam.ac.uk/~rja14/book.html

Glossary of Security Terms,* SANS *Institute
http://www.sans.org/security-resources/glossary-of-terms/

RFC 2196: Site Security Handbook
http://tools.ietf.org/html/rfc2196

Cyber Risk and Resilience Management, CERT/CC
http://www.cert.org/resilience/

Obrigado

Cristine Hoepers, D.Sc.
cristine@cert.br

Klaus Steding-Jessen, D.Sc.
jessen@cert.br

nic.br cgi.br

www.nic.br | www.cgi.br