Atuação do CERT.br

Cristine Hoepers
cristine@cert.br

Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
Núcleo de Informação e Coordenação do Ponto BR
Comitê Gestor da Internet no Brasil

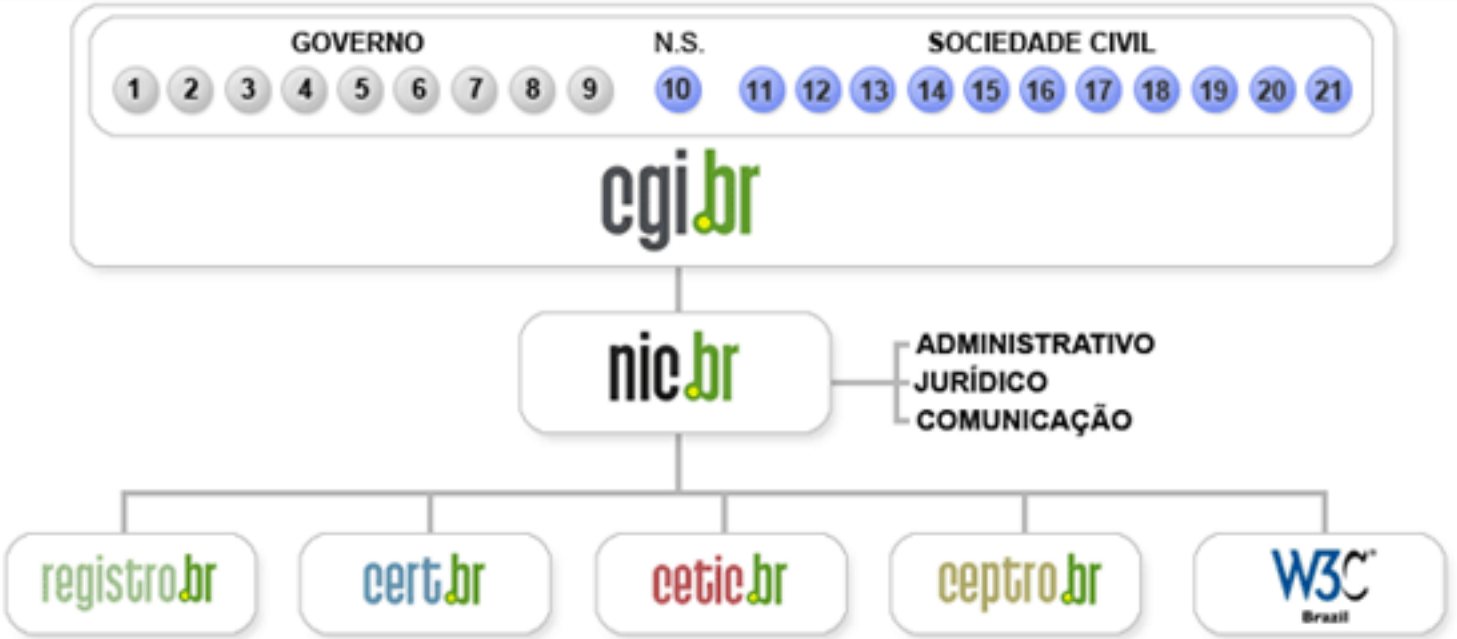
Comitê Gestor da Internet no Brasil – CGI.br

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-cg/

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

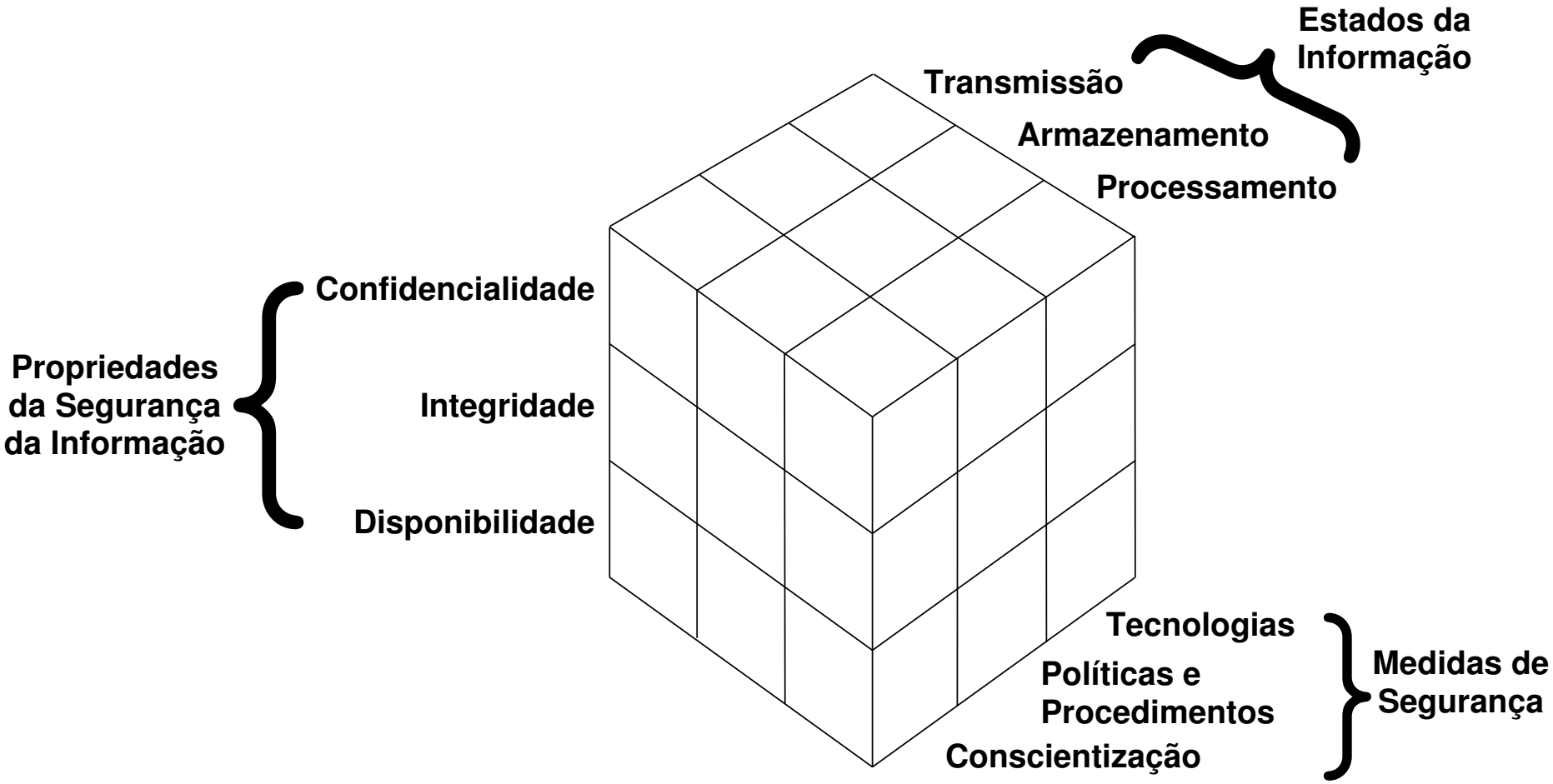
11 – provedores de acesso e conteúdo
12 – provedores de infra-estrutura de telecomunicações
13 – indústria de bens de informática, telecomunicações e software
14 – segmento das empresas usuárias de Internet
15-18 – representantes do terceiro setor
19-21 – representantes da comunidade científica e tecnológica

Agenda

- **Tratamento de Incidentes**
  - **Conceitos**
  - **Cenário Brasileiro**
- **Serviços do CERT.br para a Comunidade**
  - **Tratamento de Incidentes**
  - **Treinamento e Conscientização**
  - **Análise de Tendências**
- **Tratamento de Incidentes de Segurança em Computadores em Grandes Eventos**

Alguns Conceitos

Relembrando o Modelo Clássico de Segurança da Informação



As Informações Estão em Diversos Locais e a Segurança Depende de Múltiplos Fatores

Incidente de Segurança

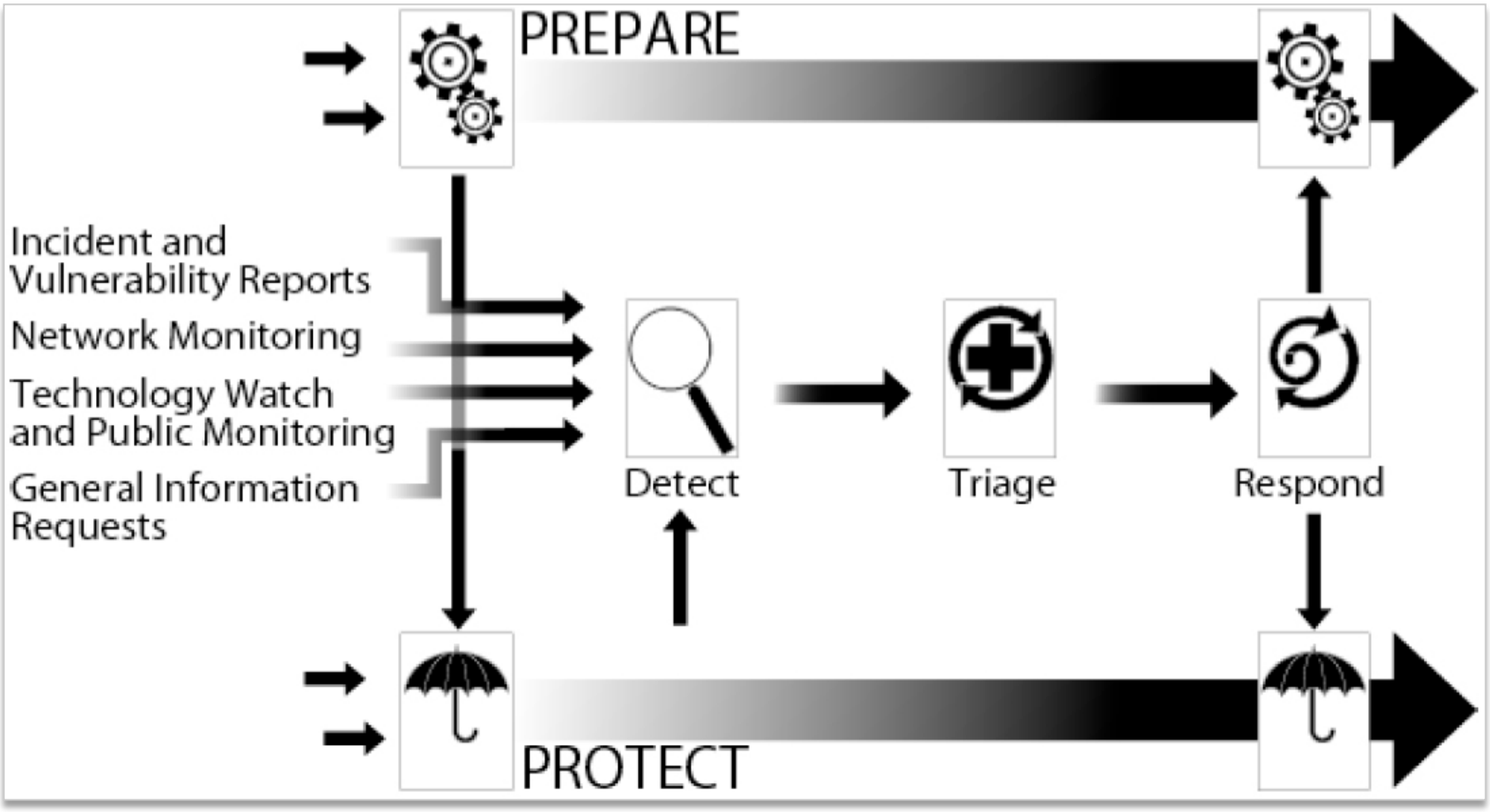
Qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores.

-ou-

O ato de violar uma política de segurança, explícita ou implícita.

http://www.cert.br/certcc/csirts/csirt_faq-br.html

Gestão e Tratamento de Incidentes



Fonte: ***Defining Incident Management Processes for CSIRTs: A Work in Progress*.**
Figura utilizada com permissão do CERT®/CC e do SEI/CMU.
http://www.cert.org/archive/pdf/04tr015.pdf

Grupos ou Times de Tratamento a Incidentes

"Um CSIRT provê serviços de suporte para prevenção, tratamento e resposta a incidentes de segurança em computadores."

– *CERT® Program CSIRT Development Team*

CSIRT – *Computer Security Incident Response Team*

- **Acrônimo global para denotar todos os times que fazem tratamento de incidentes**
  - **em qualquer país sabe-se o que é um "CSIRT"**
  - **identificar-se como um "*incident response team*" já identifica ao interlocutor os serviços e a atuação do time**
  - **o nome também procura denotar o público alvo**
- **Outros acrônimos internacionais: IRT, IRC, SIRT, CIRT, CIRC, CERT**

Exemplos:

- **Siemens CERT, NASIRC, CERT-VW, GovCERT.UK, CERT.AT, TWNCERT, CNCERT/CC, MSIRT, CERTuy, CoICERT, ECUCERT**

Papel dos CSIRTs na Mitigação e Recuperação

- O papel do CSIRT (*Computer Security Incident Response Team*) é:
  - auxiliar a proteção da infra-estrutura e das informações
  - prevenir incidentes e conscientizar sobre os problemas
  - atuar de maneira estruturada e rápida na recuperação de incidentes
- A redução do impacto é conseqüência da:
  - agilidade de resposta
  - 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
- A pessoa que responde um incidente é a primeira a entrar em contato com as evidências de um possível crime
  - seguir as políticas
  - preservar as evidências
  - recuperar do incidente – retornar o ambiente ao estado de produção

Evolução do Tratamento de Incidentes no Brasil

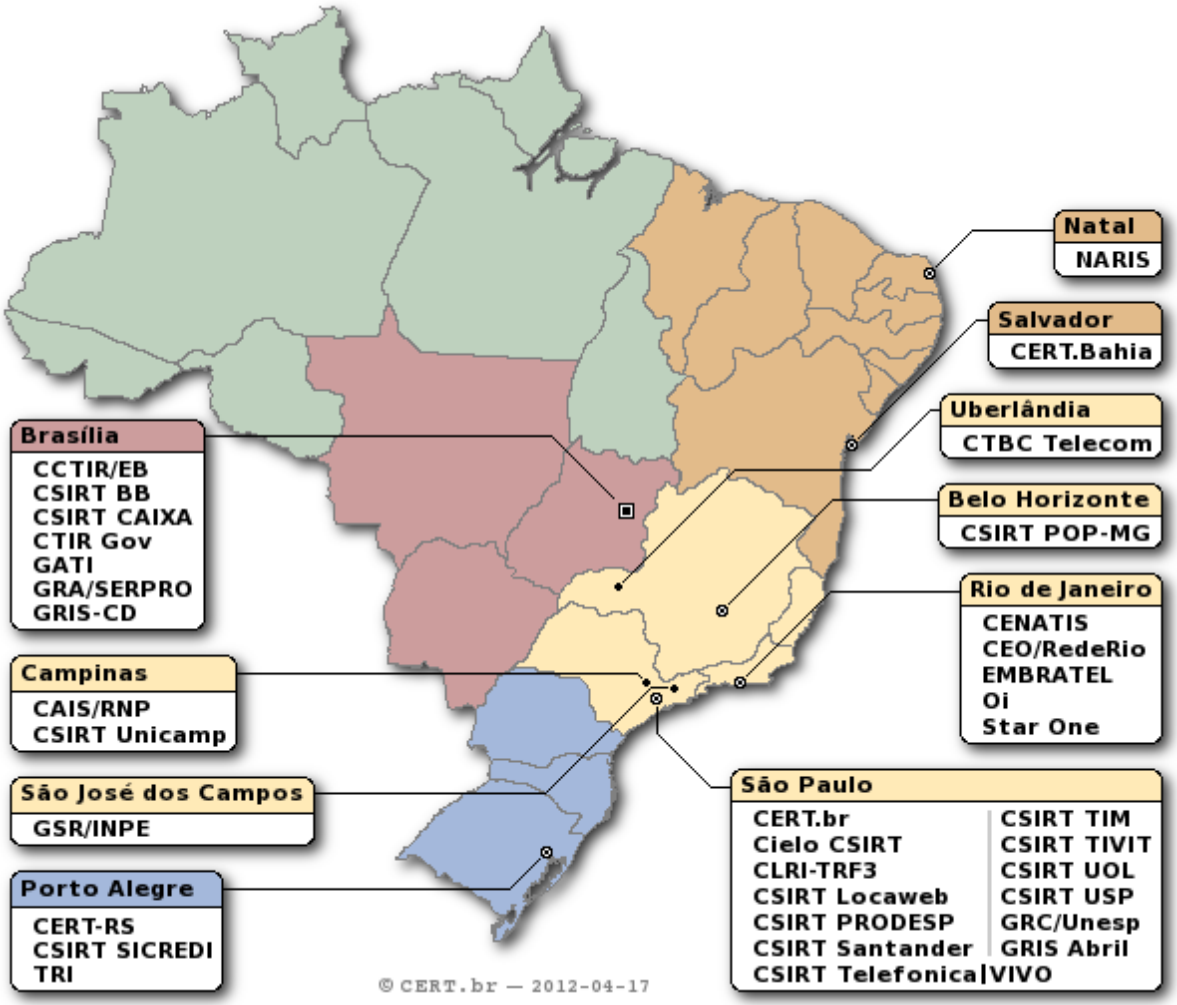
- Agosto/1996: o relatório "Rumo à Criação de uma Coordenadoria de Seguraça de Redes na Internet Brasil" é publicado pelo CGI.br[1]
- Junho/1997: o CGI.br cria o CERT.br (à época chamado NBSO – *NIC BR Security Office*), com base nas recomendações do relatório, como um grupo com responsabilidade nacional[2]
- 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
- 2003/2004 : grupo de trabalho no MP 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/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

CSIRTs Brasileiros

34 times com serviços anunciados ao público

Público Alvo	CSIRTs
Qualquer Rede no País	CERT.br
Governo	CCTIR/EB, CLRI-TRF-3, CSIRT Prodesp, CTIR Gov, GATI, GRA/SERPRO, GRIS-CD
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, CENATIS, CEO/RedeRio, CERT-Bahia, CSIRT USP, GRC/UNESP, TRI
Outros	CSIRT TIVIT, GRIS Abril



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

CERT.br

SEI Partner
Carnegie Mellon

FIRST
Improving Security Together
MEMBER

APWG
RESEARCH PARTNER
www.antiphishing.org

The Honeynet PROJECT

Tratamento de Incidentes

- Articulação
- Apoio à recuperação
- Estatísticas

Treinamento e Conscientização

- Cursos
- Palestras
- Documentação
- Reuniões

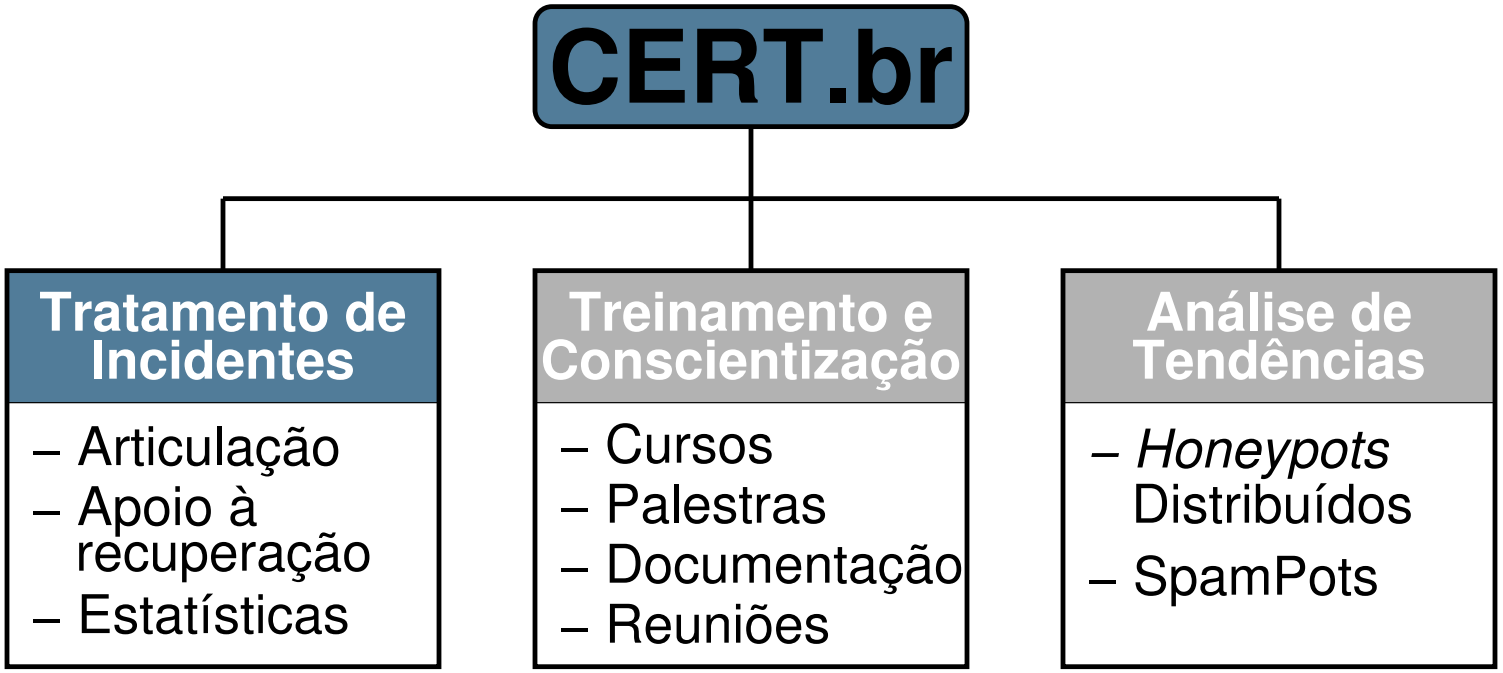
Análise de Tendências

- *Honeypots* Distribuídos
- SpamPots

Criado em 1997 para:

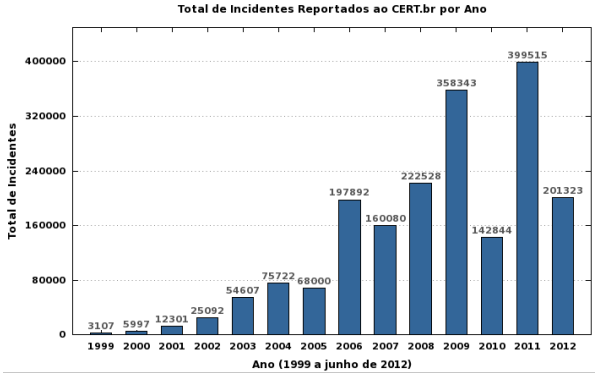
- **Ser um ponto de contato nacional para notificação de incidentes**
- **Prover a facilitação e o apoio necessários no processo de resposta a incidentes, através de um trabalho colaborativo com outras entidades**
- **Aumentar a conscientização sobre a necessidade de segurança na Internet**
- **Auxiliar 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/


CERT.br
Tratamento de Incidentes
– Articulação
– Apoio à recuperação
– Estatísticas
Treinamento e Conscientização
– Cursos
– Palestras
– Documentação
– Reuniões
Análise de Tendências
– *Honeypots* Distribuídos
– SpamPots

Dados Usados para Tratamento de Incidentes

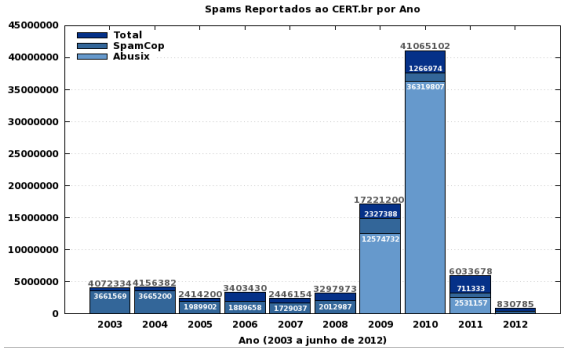
- **Notificações voluntárias de incidentes de segurança na Internet - são a fonte de dados das estatísticas trimestrais**
  Ponto de entrada: email cert@cert.br
  - **2010: 885.731 *e-mails***
  - **2011: 1.245.478 *e-mails***



- ***Feeds* de ataques partindo de redes brasileiras (Honeypots Distribuídos do CERT.br, Team Cymru, Arbor Atlas, ShadowServer, Operações Anti-*Botnets*)**

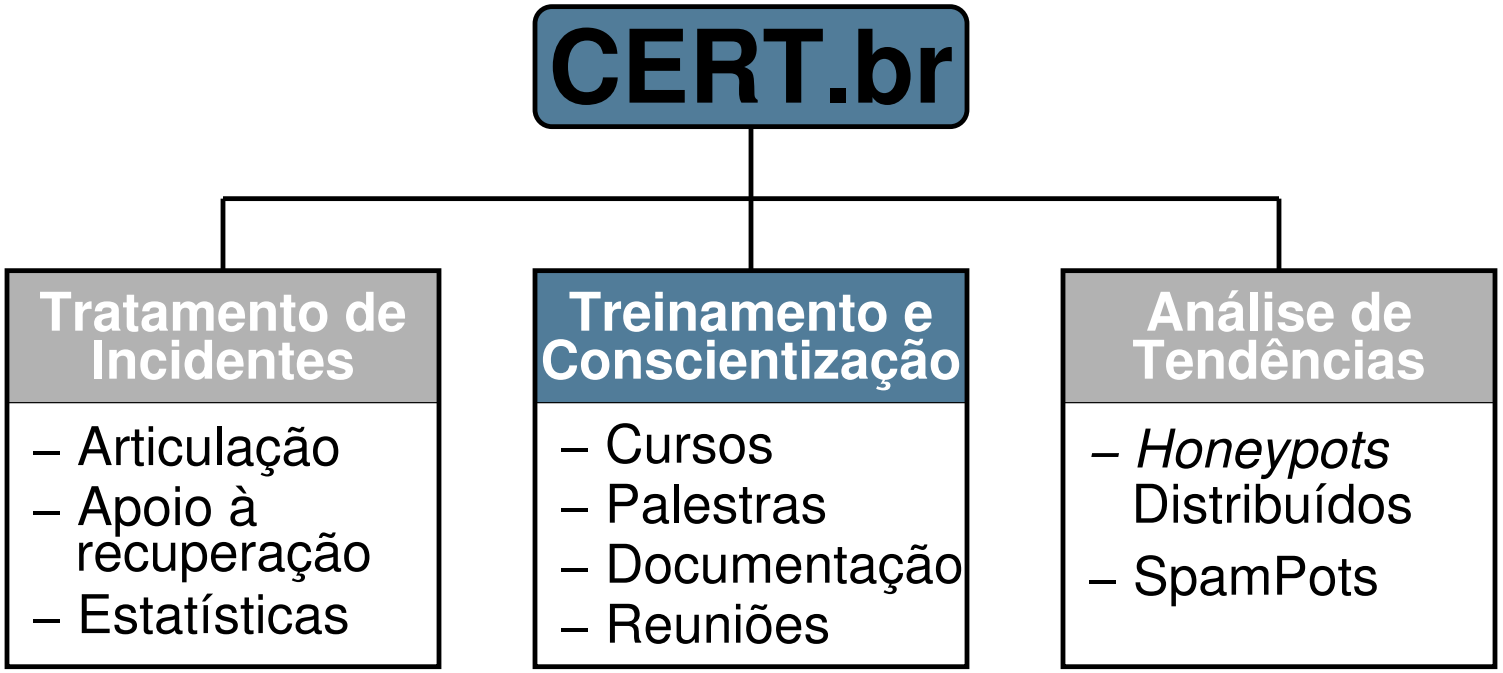
Agrupados e enviados aos donos das redes, com dicas para identificação e recuperação

- **Reclamações de *Spams* que saem das redes Brasileiras - são a fonte das estatísticas de *spam* no Brasil**
  - **2011: 6.033.678 reclamações**



- **Monitoração de**
  - **Canais de IRC, twitter**
  - **Desfiguração de *sites***

Identificação de novas atividades e de ataques a redes de alto valor


CERT.br
Tratamento de Incidentes
– Articulação
– Apoio à recuperação
– Estatísticas
Treinamento e Conscientização
– Cursos
– Palestras
– Documentação
– Reuniões
Análise de Tendências
– *Honeypots* Distribuídos
– SpamPots

Treinamento

SEI Partner
Carnegie Mellon

Objetivos:

- Criar/aproximar CSIRTs (Grupos de Tratamento de Incidentes de Segurança) no Brasil
- Possuir profissionais preparados para resolver incidentes de segurança no país

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***
  - ***Fundamentals of Incident Handling***
  - ***Advanced Incident Handling for Technical Staff***
- **500+ profissionais treinados em tratamento de incidentes**
  - **máximo de 25 participantes por turma**

Educação e Conscientização de Usuários – 1

Cartilha de Segurança para Internet
Site e Livro em PDF e ePub
http://cartilha.cert.br/

- **Fascículos organizados e diagramados de forma a facilitar a difusão de conteúdos específicos**

Primeiro Fascículo: Redes Sociais

***Slides* de uso livre para:**

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

Educação e Conscientização de Usuários – 2

Portal Internet Segura

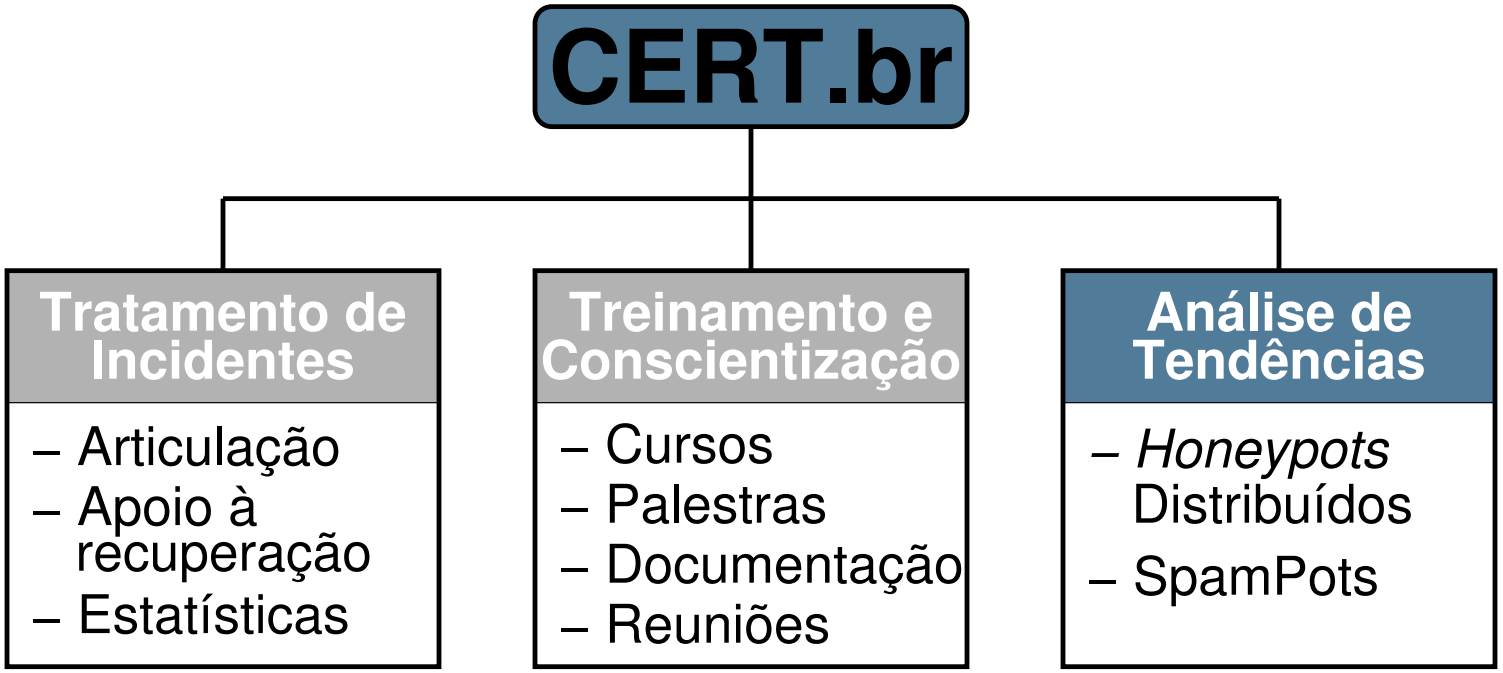
- Reúne todas as iniciativas conhecidas de educação de usuários no Brasil

http://www.internetsegura.br/

INTERNET SEGURA.BR

Site e vídeos do Antispam.br

http://www.antispam.br/

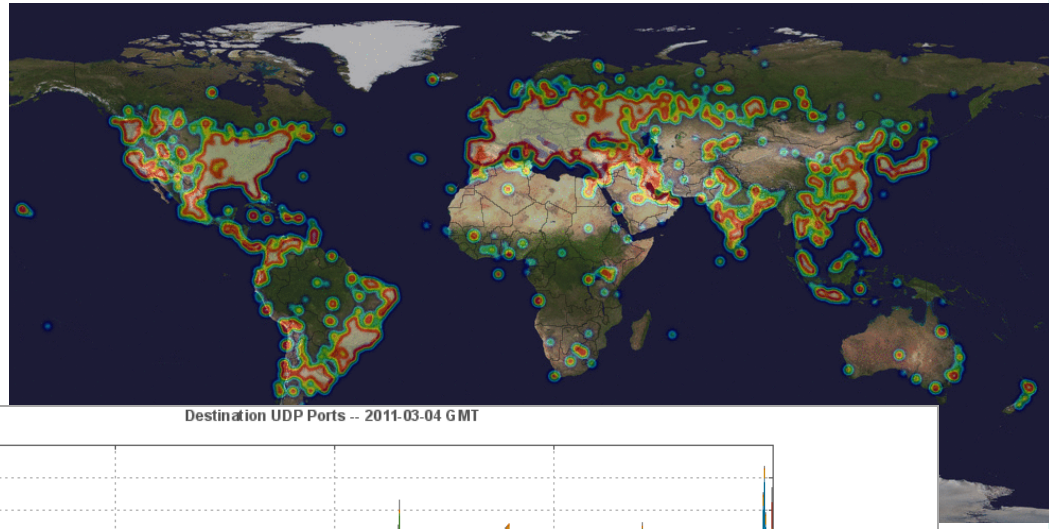

CERT.br
Tratamento de Incidentes
– Articulação
– Apoio à recuperação
– Estatísticas
Treinamento e Conscientização
– Cursos
– Palestras
– Documentação
– Reuniões
Análise de Tendências
– *Honeypots* Distribuídos
– SpamPots

Análise de Tendências

The Honeynet PROJECT

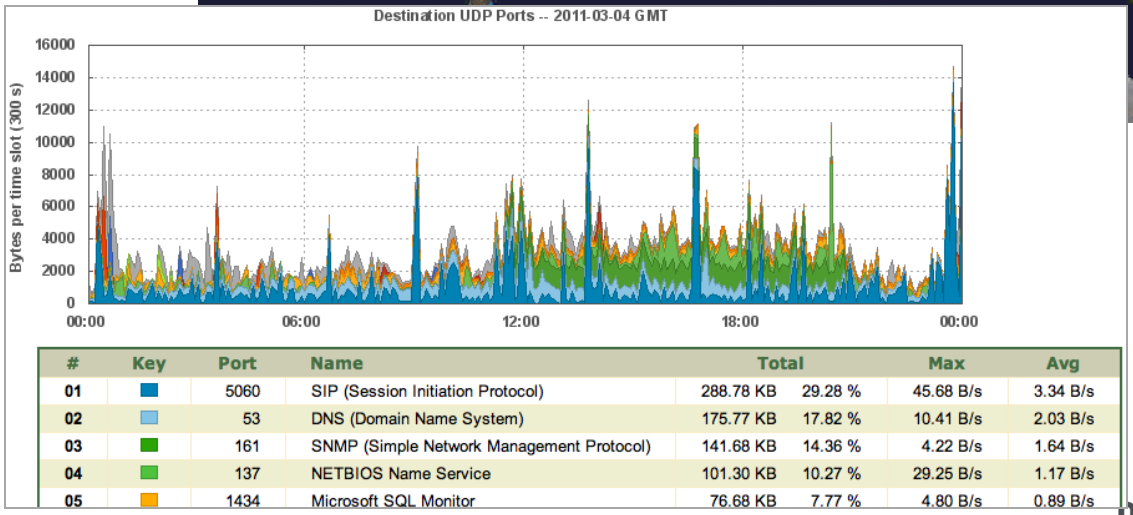
Objetivos

- Ter um "termômetro" das atividades maliciosas na Internet
- Entender o abuso da infra-estrutura da Internet por atacantes, *spammers* e fraudadores
- Propor técnicas para proteger os usuários e coibir o abuso



Projetos

- Honeypots Distribuídos
- SpamPots



#	Key	Port	Name	Total		Max	Avg
01		5060	SIP (Session Initiation Protocol)	288.78 KB	29.28 %	45.68 B/s	3.34 B/s
02		53	DNS (Domain Name System)	175.77 KB	17.82 %	10.41 B/s	2.03 B/s
03		161	SNMP (Simple Network Management Protocol)	141.68 KB	14.36 %	4.22 B/s	1.64 B/s
04		137	NETBIOS Name Service	101.30 KB	10.27 %	29.25 B/s	1.17 B/s
05		1434	Microsoft SQL Monitor	76.68 KB	7.77 %	4.80 B/s	0.89 B/s

The Honeynet Project

honeyTARG Chapter

http://honeytarg.cert.br/

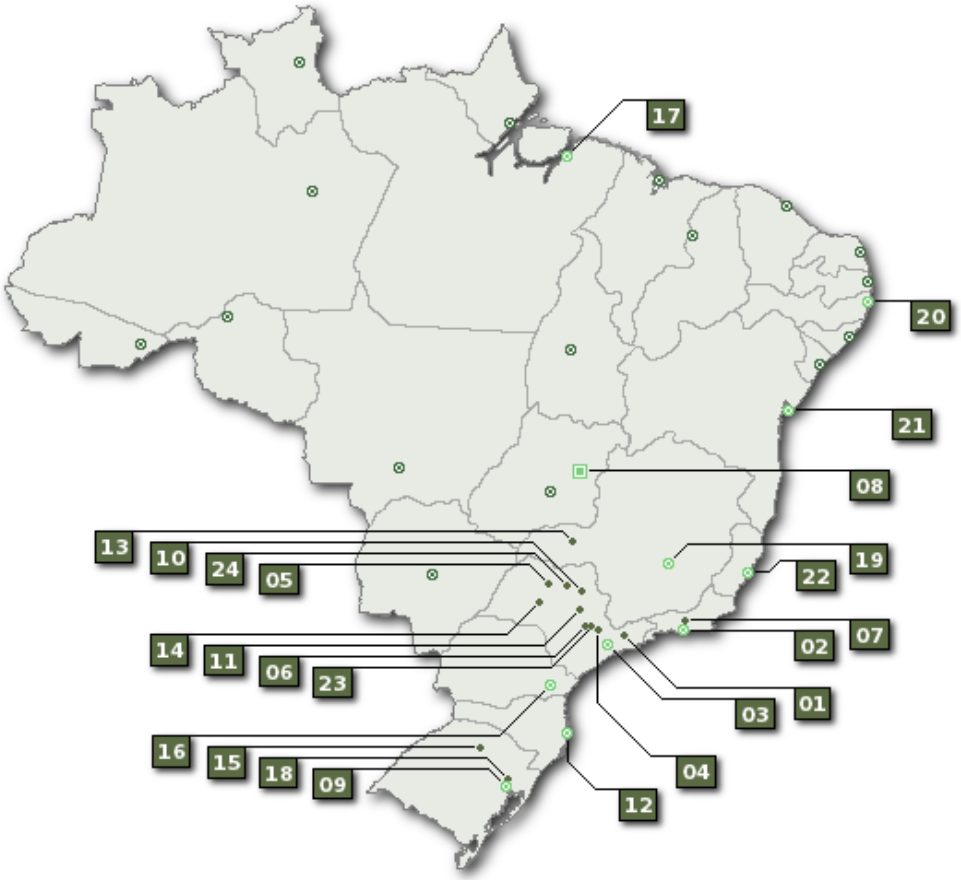
Honeypots Distribuídos

Mapeamento das atividades maliciosas na Internet no Brasil

- **51 sensores em 41 redes (universidades, governo, provedores, operadoras e empresas)**

Uso dos dados:

- **Gerar estatísticas públicas sobre tendências**
- **Notificar *sites* brasileiros com problemas**
- **Enviar dados anonimizados**
  - **para CERTs Nacionais, para auxiliar esforços de combate a *botnets*: Austrália, Polônia, Uruguai, Argentina, Colômbia, Qatar**
  - **entidades de combate a *botnets*: Arbor Atlas, Team Cymru, ShadowServer**



Projeto SpamPots

- Entender o abuso da infra-estrutura da Internet por *spammers* e fraudadores
- Propor técnicas para proteger os usuários e coibir o abuso
  - Exemplo: Acordo de Cooperação para Implementação de Gerência de Porta 25, assinado por Anatel, NIC.br, CGI.br, ABTA, SindiTelebrasil e Associações de Provedores de Acesso e Serviços.
- Parceria com o Laboratório eSpeed/DCC/UFMG para mineração de dados
  - Aprox. 11 milhões de spams coletados por dia
- Sensores em 8 países, em parceria com CERTs locais: AusCERT (Austrália), CERT.at (Áustria), CLCERT (Chile), CSIRT ANTEL (Uruguai). CSIRT USP (Brasil), CSIRT UTPL (Equador), SurfCERT (Holanda) e TWCERT/CC (Taiwan)
- Envio de dados para países originadores de abuso
  - Japão: JPCERT/CC, JADAC, IIJ e Min. das Comunicações
  - Taiwan: TWCERT/CC e NCC/TW

Tratamento de Incidentes em Grandes Eventos

Diferenças com outros Incidentes

Um único evento que:

- Atrai mais atenção por parte do mundo
  - e dos atacantes
- Os momentos críticos tem data e hora marcados com antecedência
- Os incidentes tem impacto na imagem do país
- A Internet é infra-estrutura crítica, entre outros, para:
  - trasmissão dos jogos
  - comunicação dos jornalistas
  - comunicação da própria organização do evento

Pontos Chave para o Sucesso

- A rede que estiver provendo conectividade precisa
  - ter um time atuante e experiente
  - compartilhar informações
- Cooperação
  - nenhum único grupo ou estrutura conseguirá fazer sozinho a segurança ou a resposta a incidentes
  - pessoal preparado em todas as redes e áreas
  - cooperação direta entre os diversos atores
- Os times serão os mesmos de sempre, mas é necessário ter mais troca de informações e cooperação entre
  - os grupos organizadores
  - o pessoal tecnico das operadores
  - e todos os CSIRTs formados no Brasil
- Acões necessitam iniciar já

Ações do NIC.br/CGI.br para Resiliência e Estabilidade das Infraestruturas Críticas de Internet

- PTT.br – Pontos de Troca de Tráfego nas grandes áreas metropolitanas
  - "uma única saída é o mesmo que nenhuma"
- Estabilidade da Infraestrutura de DNS (Registro.br)
  - Diversos mirrors no Brasil dos Servidores DNS Raíz
  - Mirrors do `.br` hospedados em outros países
  - Suporte a DNSSEC no ccTLD `.br`
    - Segundo país no mundo a ter DNSSEC disponível na raiz
- Capacitação de profissionais
  - IPv6 e gerência de redes (CEPTRO.br)
  - Tratamento de incidentes (CERT.br)
- Rede iNOC-DBA
  - mas as operadoras precisam usá-lo
- Análise de tendências e tratamento de incidentes (CERT.br)

O que pode ser feito pelo CERT.br

Ajudar na identificação de

- possíveis ameaças e cenários de ataques
- necessidades de infraestrutura (como redundância de conectividade)

Monitoramento extra de incidentes e fontes de dados sobre ataques

- notificações de incidentes
- feeds de dados (Honeypots Distribruídos do CERT.br, Team Cymru, Arbor Atlas, ShadowServer, Operações Anti-Botnet)
- fontes públicas de informação (Twitter, IRC, *defacements*)

Facilitação e suporte no tratamento de incidentes

- via a rede de contatos já estabelecida

Perguntas?

Cristine Hoepers

cristine@cert.br

- **CGI.br - Comitê Gestor da Internet no Brasil**
  http://www.cgi.br/
- **NIC.br - Núcleo de Informação e Coordenação do .br**
  http://www.nic.br/
- **CERT.br -Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil**
  http://www.cert.br/