Tratamento de Incidentes de Segurança em Grandes Eventos

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

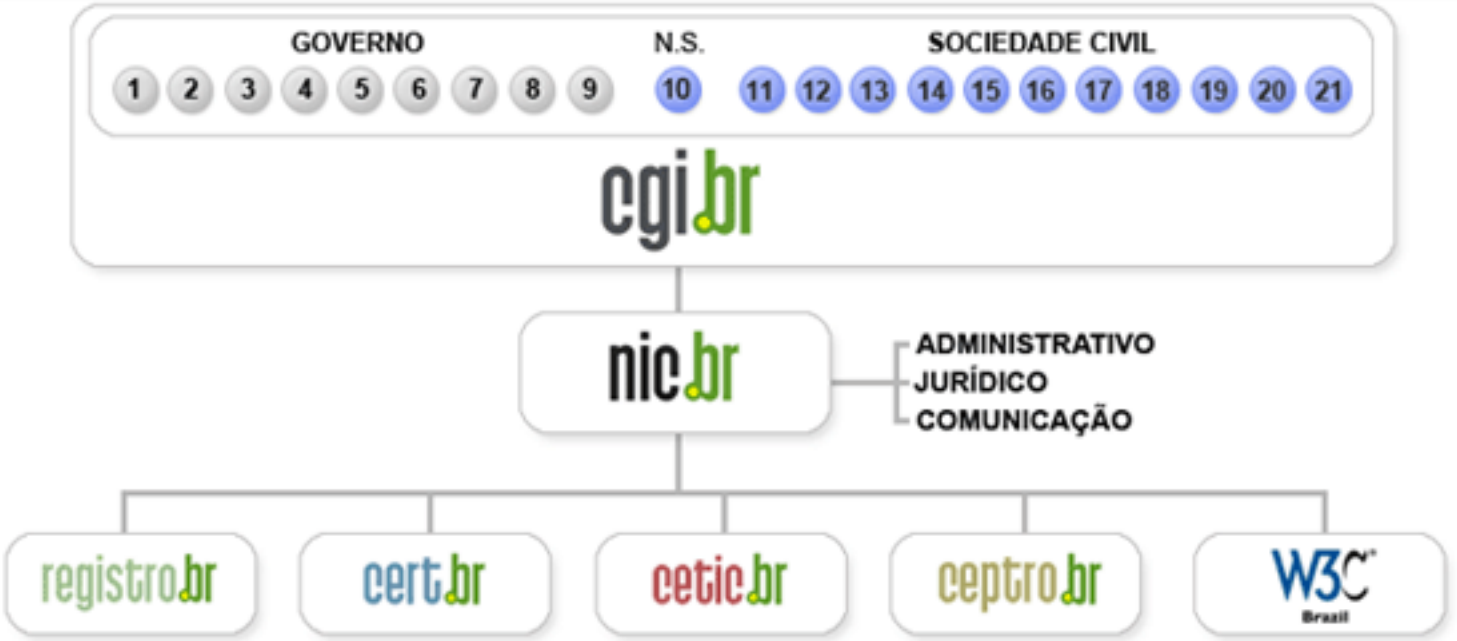
Comitê Gestor da Internet no Brasil – CGI.br

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 infraestrutura 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

cert.br

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

SEI Partner
Carnegie Mellon

FIRST
Improving Security Together
MEMBER

APWG
RESEARCH PARTNER
www.antiphishing.org

The Honeynet PROJECT

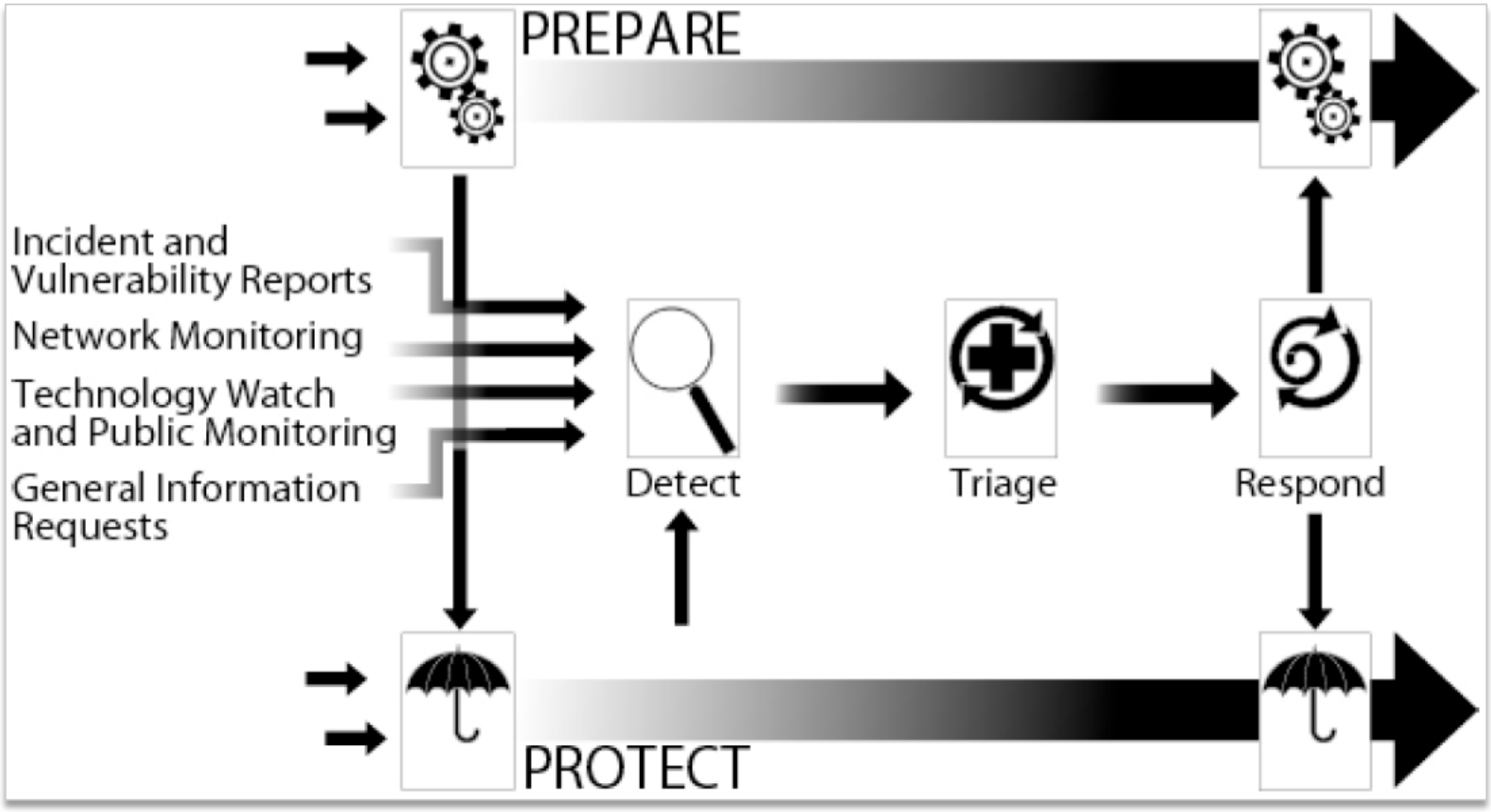
Criado em 1997 para:

- **Ser um ponto de contato nacional para notificação de incidentes**
- **Prover a facilitação e o apoio necessários no processo de resposta a incidentes, 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/

Características do Tratamento de Incidentes

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

Papel dos CSIRTs na Mitigação e Recuperação

- O papel do CSIRT (*Computer Security Incident Response Team*) é:
  - auxiliar a proteção da infraestrutura 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
- Mas quem responde um incidente é o primeiro 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

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 infraestrutura crítica, entre outros, para:
  - transmissão dos jogos
  - comunicação dos jornalistas
  - comunicação da própria organização do evento
- A rede do evento pode ser usada como base para ataques

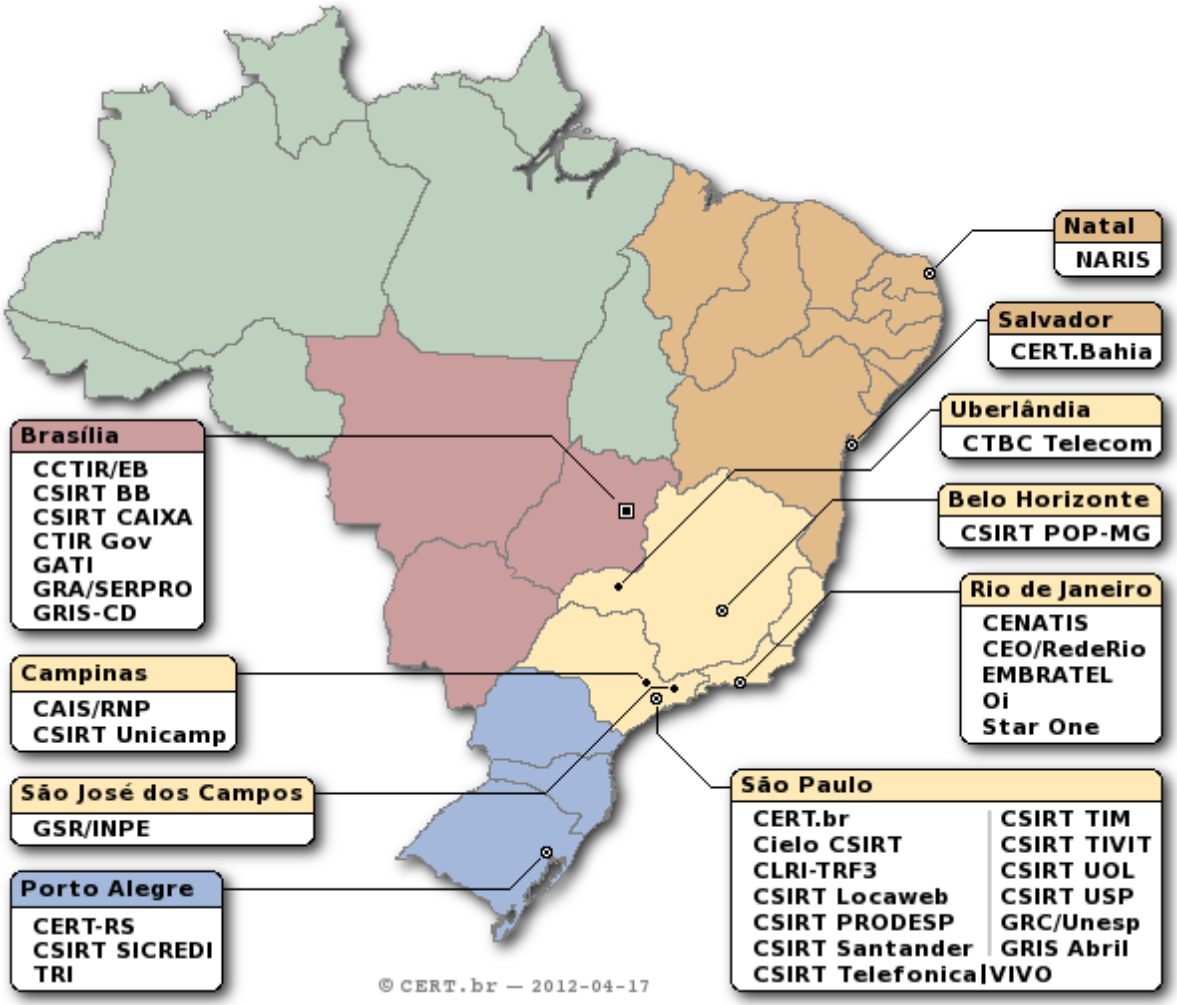
Pontos Chave para o Sucesso

- A rede que estiver provendo conectividade precisa
  - ter um time atuante e experiente
  - compartilhar informações com parceiros
- 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 eles
- Acões necessitam iniciar já
  - principalmente a construção das relações de confiança e o treinamento de pessoal

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/

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 Raiz
  - *Mirrors* do `.br` hospedados em outros países
  - Suporte a DNSSEC no ccTLD `.br`
- Capacitação de profissionais
  - IPv6 e gerência de redes (CEPTRO.br)
  - Tratamento de incidentes (CERT.br)
- Rede iNOC-DBA
- Análise de tendências e tratamento de incidentes (CERT.br)

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/