



nic.br egi.br

cert.br

**CPBR8**

**São Paulo, SP**

**05 de fevereiro de 2015**

# Pergunte ao CERT.br

Equipe CERT.br  
cert@cert.br

cert.br nic.br cgi.br

# Evolução da Internet no Brasil

<b>1989</b>	<b>Criação e delegação do código de país (ccTLD) “.br” à FAPESP</b>
<b>1991</b>	<b>Primeira conexão TCP/IP brasileira, realizada entre a FAPESP e o Energy Sciences Network (ESNet) por meio do Fermilab (<i>Fermi National Accelerator Laboratory</i>)</b>
<b>1995</b>	<b>Criação do CGI.br (Portaria Interministerial MC/MCT nº 147, de 31 de maio) com a missão de coordenar e integrar todas as iniciativas de serviços Internet no país, promovendo a qualidade técnica, a inovação e a disseminação dos serviços ofertados</b>
<b>1995</b>	<b>Criação do Registro.br</b>
<b>1997</b>	<b>Criação do CERT.br (à época NBSO)</b>
<b>2005</b>	<b>Criação do NIC.br, entidade sem fins lucrativos para executar as diretrizes do CGI.br e prestar serviços para a estabilidade e segurança da Internet no Brasil</b>

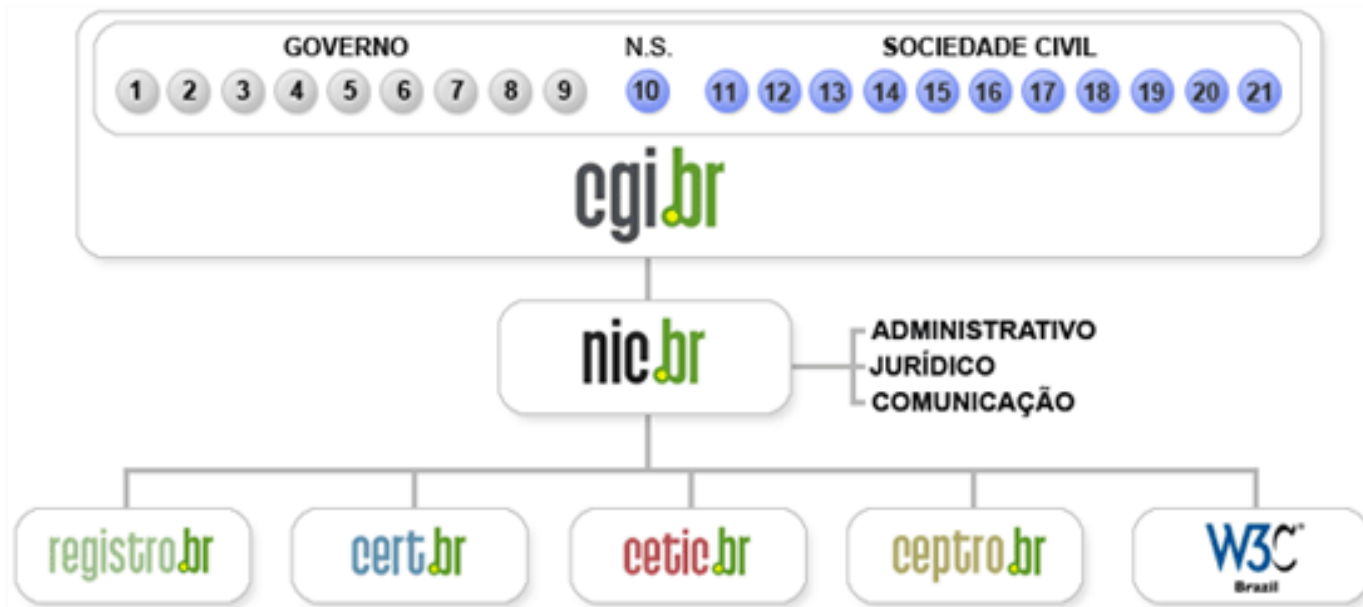
<http://www.nic.br/imprensa/releases/2010/rl-2010-12.htm>

# 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;

# 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



### Tratamento de Incidentes

- Articulação
- Apoio à recuperação
- Estatísticas

### Treinamento e Conscientização

- Cursos
- Palestras
- Documentação
- Reuniões

### Análise de Tendências

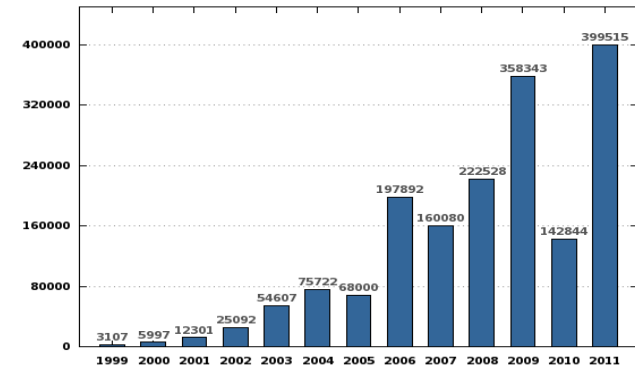
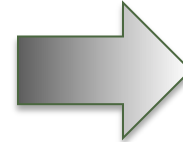
- *Honeypots* Distribuídos
- SpamPots

# Tratamento de Incidentes

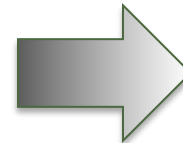
- Notificações voluntárias de incidentes de segurança na Internet - são a fonte de dados das estatísticas

Ponto de entrada: email [cert@cert.br](mailto:cert@cert.br)

- 2011: 1.245.478 e-mails
- 2012: 3.044.502 e-mails
- 2013: 1.675.205 e-mails
- 2014: 2.611.920 e-mails



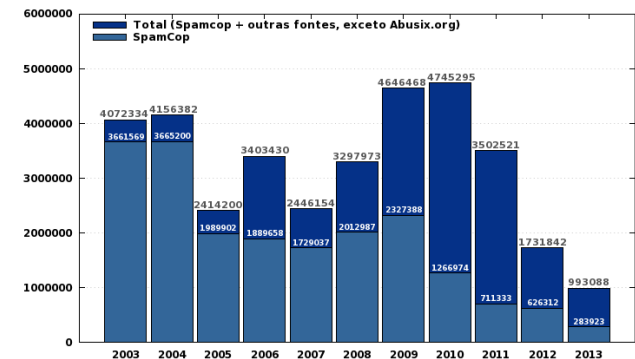
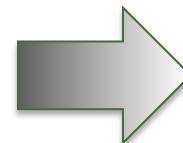
- Feeds de ataques partindo de redes brasileiras (Honeypots Distribuídos, Arbor Atlas, ShadowServer, Operações anti-botnets, etc)



**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
- 2012: 1.731.842 reclamações
- 2013: 993.088 reclamações
- 2014: 735.262 reclamações





### Tratamento de Incidentes

- Articulação
- Apoio à recuperação
- Estatísticas

### Treinamento e Conscientização

- Cursos
- Palestras
- Documentação
- Reuniões

### Análise de Tendências

- *Honeypots* Distribuídos
- SpamPots



# Treinamento

## Objetivos:

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

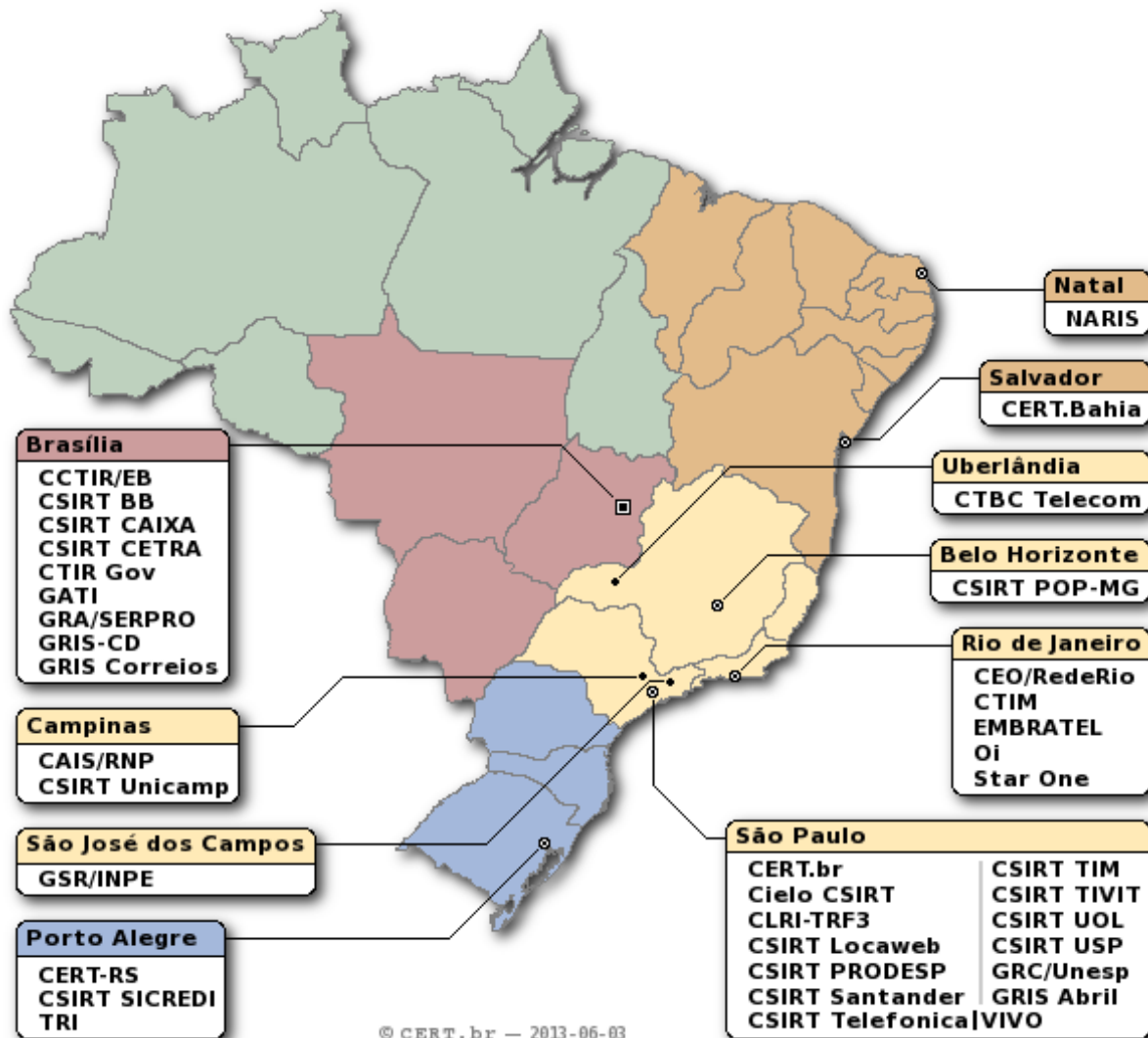
***SEI/Carnegie Mellon Partner*** desde 2004, licenciado para ministrar cursos do ***CERT® Program*** no Brasil:

- <http://www.cert.br/cursos/>
  - *Overview of Creating and Managing CSIRTs*
  - *Fundamentals of Incident Handling*
  - *Advanced Incident Handling for Technical Staff*
- 600+ profissionais treinados em tratamento de incidentes

# 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



© CERT.br - 2013-06-03

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

# 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/>

The screenshot shows a web browser window with the address bar displaying 'http://cartilha.cert.br/'. The page header includes the logo for 'cert.br' (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil) and 'nic.br cgi.br' (Ir para o conteúdo). A navigation menu contains 'Início', 'Livro', 'Fascículos', and 'Sobre'. A search bar is labeled 'Buscar'. The main content area features a large illustration of a boat on the water with sharks below, and a text box with the heading 'Navegar é preciso, arriscar-se não!' and a paragraph of text. A sidebar on the right contains a 'Dica do dia' section with a tip about backing up passwords and a 'Veja também' section with links to 'INTERNETSEGURA.BR', 'antispam.br', and 'Teste a qualidade de sua conexão'.



# Fascículos da Cartilha de Segurança para Internet

Organizados de forma a facilitar a difusão de conteúdos específicos:

- Redes Sociais
- Senhas
- Comércio Eletrônico
- Privacidade
- Dispositivos Móveis
- Internet Banking
- Computadores
- Códigos Maliciosos



Acompanhados de *Slides* de uso livre para:

- ministrar palestras e treinamentos
- complementar conteúdos de aulas

# Outros Materiais para Usuários Finais

## Portal Internet Segura

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

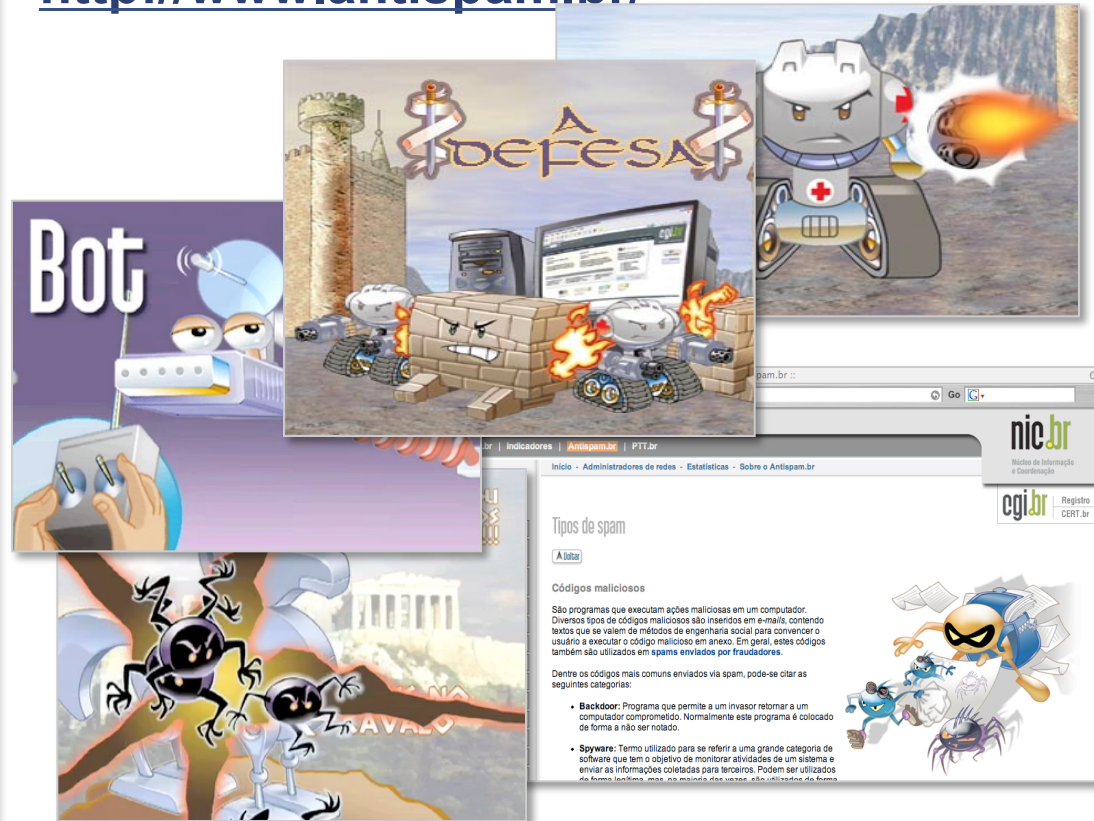
<http://www.internetsegura.br/>



**INTERNET  
SEGURA.BR**

## Site e vídeos do Antispam.br

<http://www.antispam.br/>





### Tratamento de Incidentes

- Articulação
- Apoio à recuperação
- Estatísticas

### Treinamento e Conscientização

- Cursos
- Palestras
- Documentação
- Reuniões

### Análise de Tendências

- *Honeypots* Distribuídos
- SpamPots

# Análise de Tendências



## 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

*The HoneyNet Project*

*honeyTARG Chapter*

<http://honeytarg.cert.br/>

The screenshot shows a web browser window displaying the honeyTARG HoneyNet Project website. The browser's address bar shows 'honeytarg.cert.br'. The website header includes the CERT.br logo and the text 'Computer Emergency Response Team Brazil'. Below the header, the main heading is 'honeypots for Threats and Abuse passive Reconnaissance and information Gathering' followed by 'honeyTARG HoneyNet Project' and a small illustration of a pig. The main content area is divided into two columns. The left column contains a paragraph about the project, a list of current projects (Spampots Project and Distributed Honeypots for Attack Trend Analysis), and a section for the SpamPots Project with its goals. The right column contains a section for Distributed Honeypots, a paragraph about the project's objective, a list of data produced, and a section for Flows with a small line graph. At the bottom right, there is a section for TCP/UDP Port Summary with another small line graph. The footer of the website includes the CERT.br, NIC.br, and CGI.br logos.

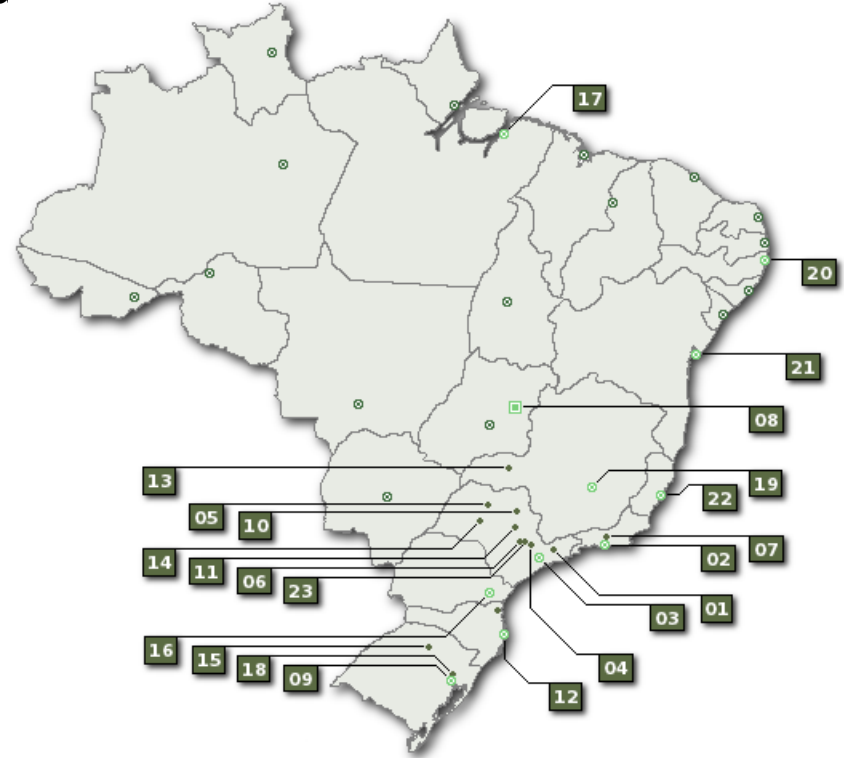
# Honeypots Distribuídos

## Mapeamento das atividades maliciosas na Internet no Brasil

- 55 sensores em 43 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
- Parceria com o Laboratório eSpeed/DCC/UFMG para mineração de dados
  - Aprox. 10 milhões de spams coletados por dia
- Sensores em 12 países, em parceria com: CSIRT UNLP (Argentina), AusCERT (Austrália), CERT.at (Áustria), CSIRT USP (Brasil), CLCERT (Chile), CSIRT CEDIA (Equador), University of Alabama at Birmingham (Estados Unidos), SurfCERT (Holanda), HKCERT (Hong Kong), ShadowServer Foundation (Noruega e EUA), TWCERT/CC (Taiwan) e CSIRT ANTEL (Uruguai)
- Envio de dados para países originadores de abuso
  - Japão: JPCERT/CC, JADAC, IIJ e Min. das Comunicações
  - Taiwan: TWCERT/CC e NCC/TW

The background of the slide features a dark gray, textured pattern of white circuit board traces. The traces form various geometric shapes, including rectangles, lines, and circular paths, creating a complex, technical aesthetic. The pattern is consistent across the top and bottom sections of the slide, framing the central white area.

# Outras atividades


cert.br nic.br cgi.br

# Outras Atividades

- **Fórum Brasileiro de CSIRTs**
  - evento dedicado à discussão de assuntos relacionados com tratamento de incidentes de segurança
- **Participação na CT-Spam do CGI.br**
  - Grupo de Trabalho para Adoção de Gerência de Porta 25 no Brasil
- **Reuniões periódicas com diversos setores da Internet no Brasil**
  - Sistema Financeiro
  - Anatel, Provedores e Operadoras de Telecomunicações e suas Associações
  - Ministérios Públicos e Associações de Defesa do Consumidor

# Outras Atividades

- **Campus Party**
  - **Brasil**
  - **Recife**
  
- **Articulação para trazer ao Brasil eventos com assuntos relevantes ao cenário nacional, proporcionando treinamento e integração com boas práticas mundiais**
  - **2010: APWG Counter e-Crime Operations Summit, evento de combate a *phishing* e a outras fraudes**
  - **2012: 1º FIRST Symposium na América Latina, São Paulo**

The background of the slide is a dark gray circuit board pattern with white lines representing traces and components. The top and bottom sections of the slide feature this pattern, while the middle section is a solid light gray gradient.

# Aproveite e tire suas dúvidas

[cert.br](http://cert.br) [nic.br](http://nic.br) [cgi.br](http://cgi.br)

# Obrigado

[www.cert.br](http://www.cert.br)

✉ [cert@cert.br](mailto:cert@cert.br)

📧 [@certbr](https://twitter.com/certbr)

05 de fevereiro de 2015

nic.br cgi.br

[www.nic.br](http://www.nic.br) | [www.cgi.br](http://www.cgi.br)