Gestão de Incidentes e Resiliência das Infraestruturas Críticas de Internet

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

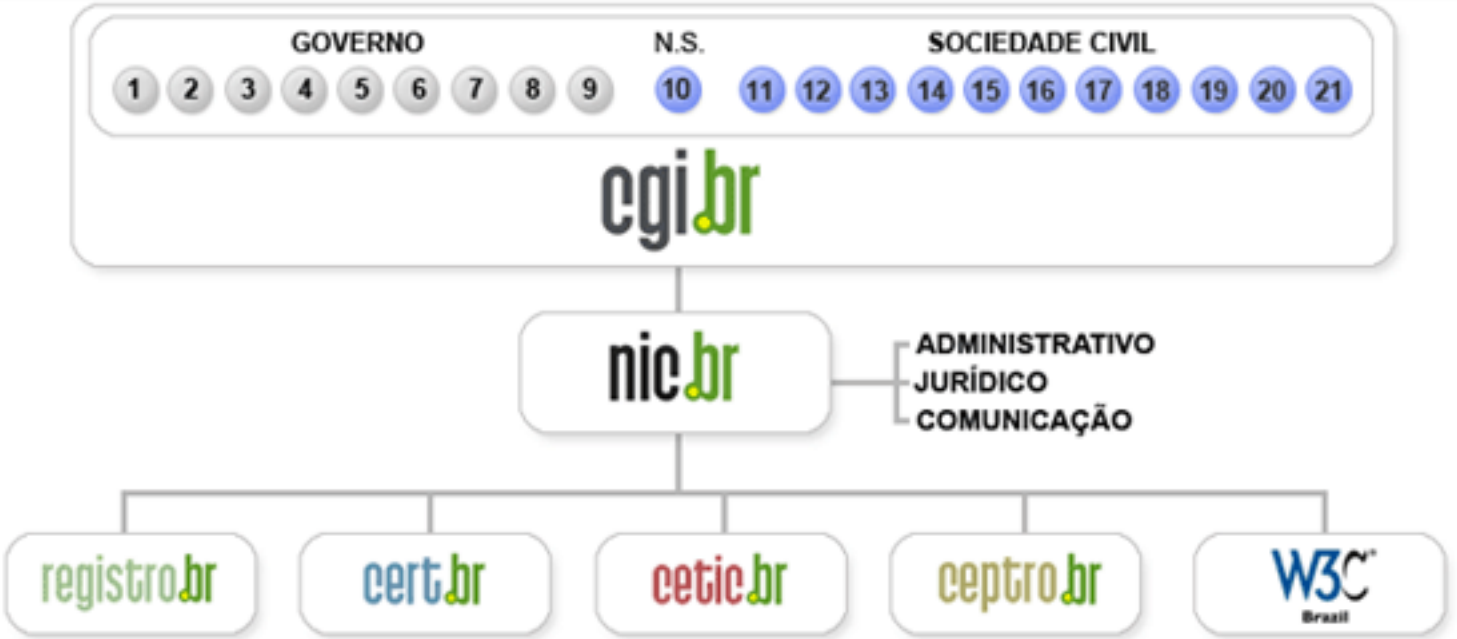
Comitê Gestor da Internet no Brasil – CGI.br

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



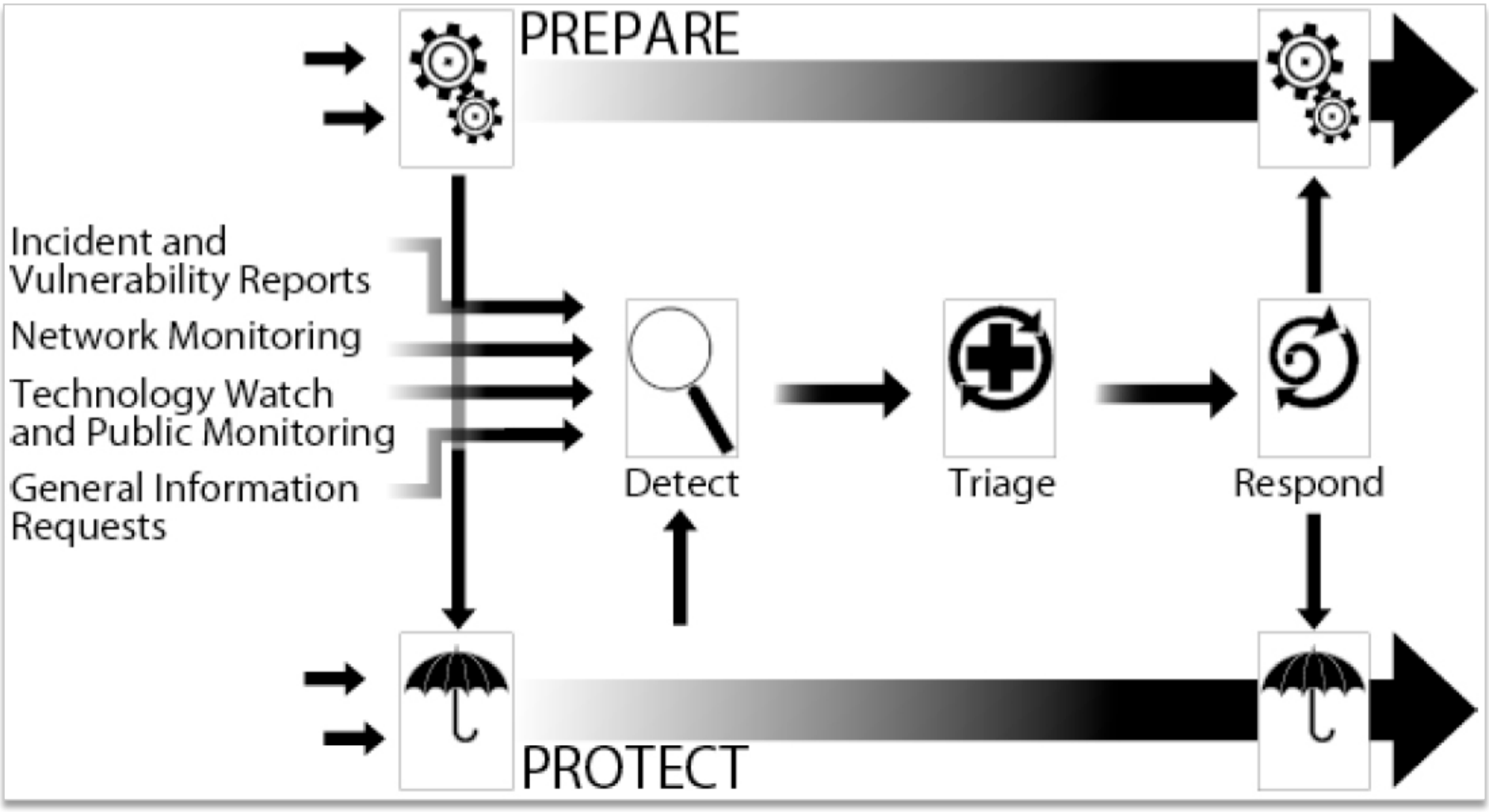
1 – Ministério da Ciência e Tecnologia (Coordenação)
2 – Ministério das Comunicações
3 – Casa Civil da Presidência da República
4 – Ministério da Defesa
5 – Ministério do Desenvolvimento, Indústria e Comércio Exterior
6 – Ministério do Planejamento, Orçamento e Gestão
7 – Agência Nacional de Telecomunicações (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

Resiliência

- **Foco deixa de ser em se recuperar de ataques ou incidentes**
- **Foco é continuar a operação mesmo sob a presença de ataques ou incidentes**
- **Só é atingida com a integração de diversos processos de TI, Segurança e Continuidade de Negócios, incluindo:**
  - **Análise de riscos**
  - **Treinamento e conscientização**
  - **Gestão de incidentes**

Gestão, Tratamento e Resposta a 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

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 com a missão de:

- **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/

Histórico do Tratamento de Incidentes no Brasil

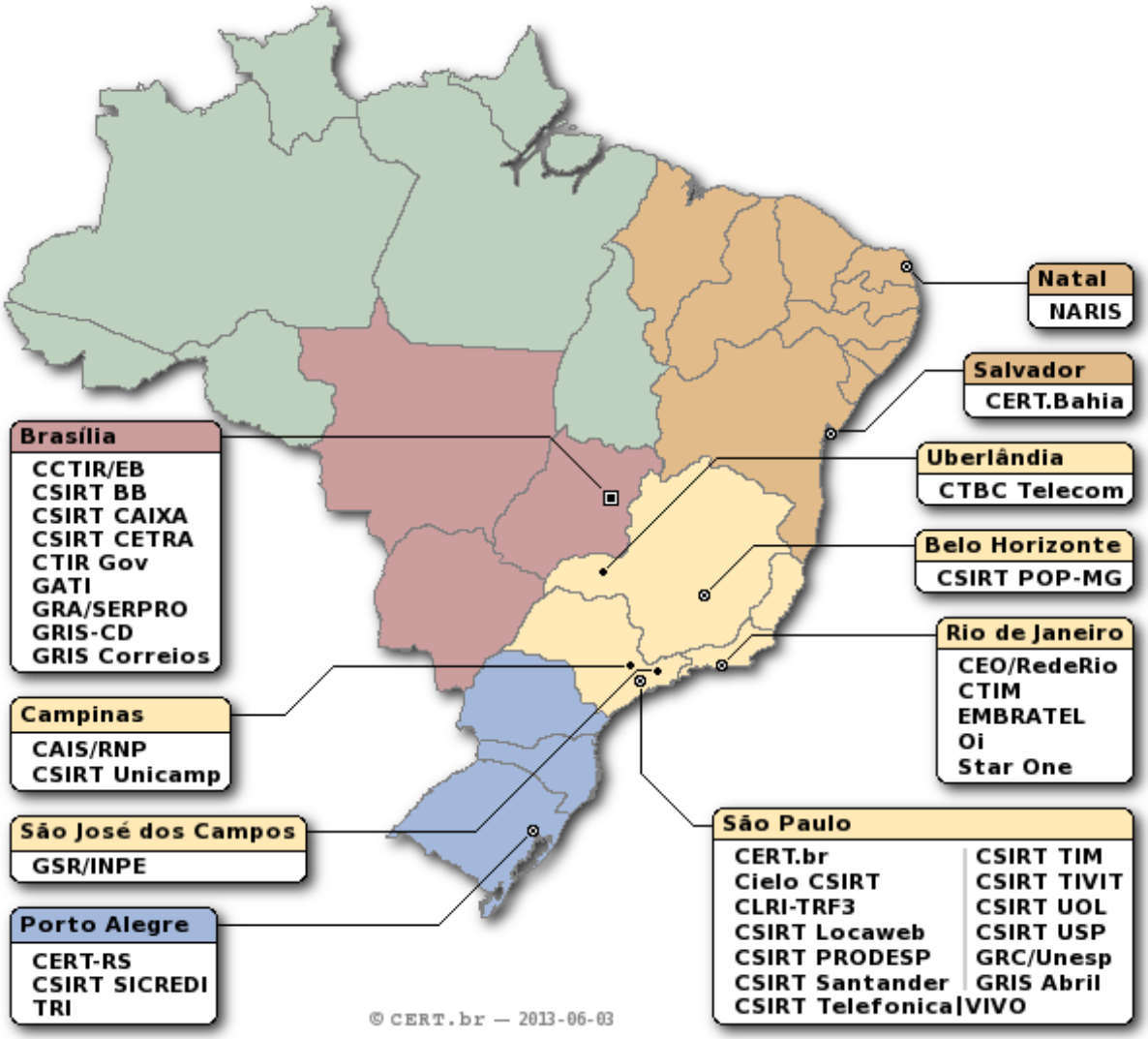
- Agosto/1996: o relatório "Rumo à Criação de uma Coordenadoria de Seguraça de Redes na Internet Brasil" é publicado pelo CGI.br[1]
- Junho/1997: o CGI.br cria o CERT.br (à época chamado NBSO – *NIC BR Security Office*), com base nas recomendações do relatório, como um grupo com responsabilidade nacional[2]
- 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

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/

Infraestruturas Críticas da Internet

Mesmo sendo uma rede distribuída e descentralizada, diversos elementos são críticos para sua contínua operação:

- **Recursos de Numeração**
  - **Endereços IP e Sistemas Autônomos (ASNs)**
- **Roteamento**
- **Sistemas de registro de nomes de domínio (.br, .com, .de, etc)**
- **Sistemas de Resolução de Nomes (DNS)**
- **Pontos de Troca de Tráfego**
- **Infraestrutura física**

Mas nada disso opera sem pessoal capacitado

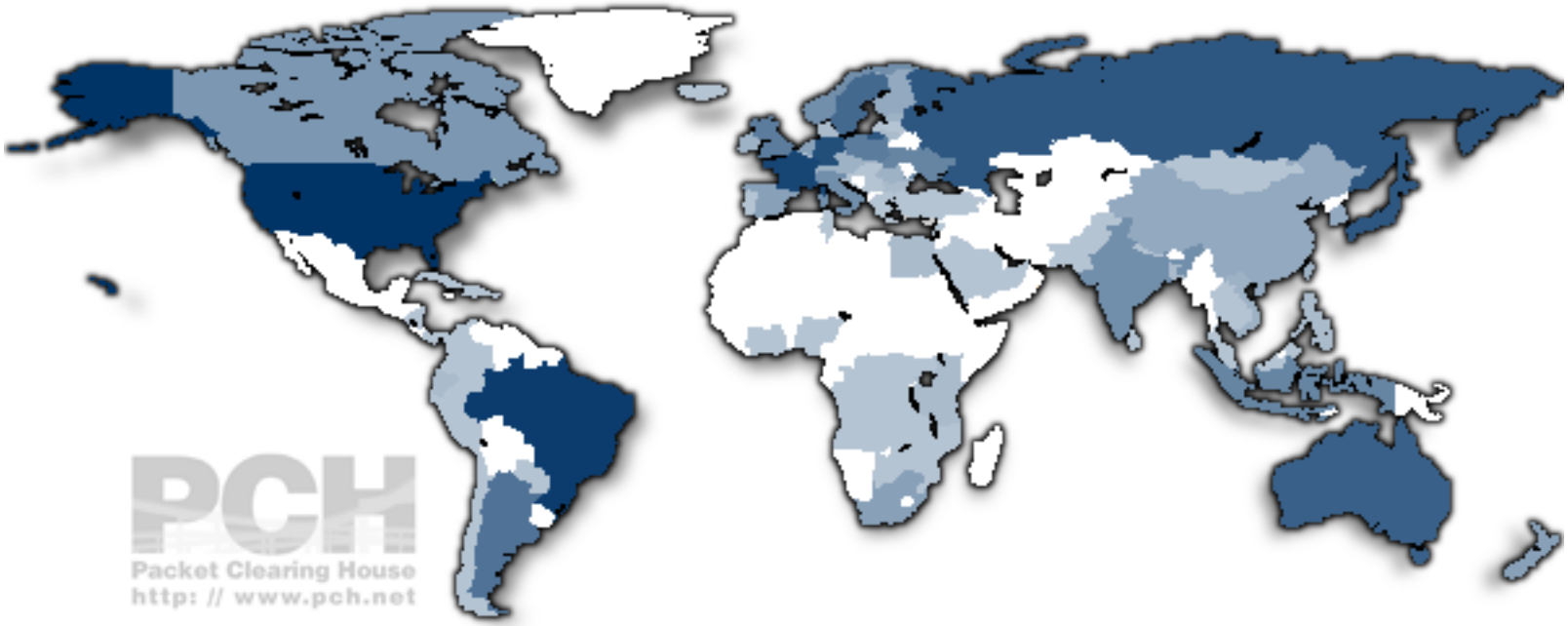
- **redes (IPv4 e IPv6) e administração de sistemas**
- **segurança**
- **tratamento de incidentes**

Estratégias do NIC.br/CGI.br na Última Década

- **Dar autonomia ao Brasil e à América Latina na área de recursos de nomes e endereços:**
  - **Registro.br: Nomes, IPs e ASNs para o Brasil**
  - **LACNIC: participação estratégica na criação do órgão e na definição das políticas para a região**
  - **Articulação com outros administradores de recursos globais (ICANN, IANA, APNIC, AfriNIC, ARIN, RIPE, LACTLD)**

- **Estímulo à autonomia das redes no Brasil**
  - **facilitação para obtenção de um AS**
  - **manutenção gratuita dos Pontos de Troga de Tráfego (PTTs)**
  - **aumento da resiliência dos sistemas DNS no Brasil**
  - **treinamentos em administração de ASNs, IPv6, DNS**
  - **treinamento de especialistas em tratamento de incidentes**

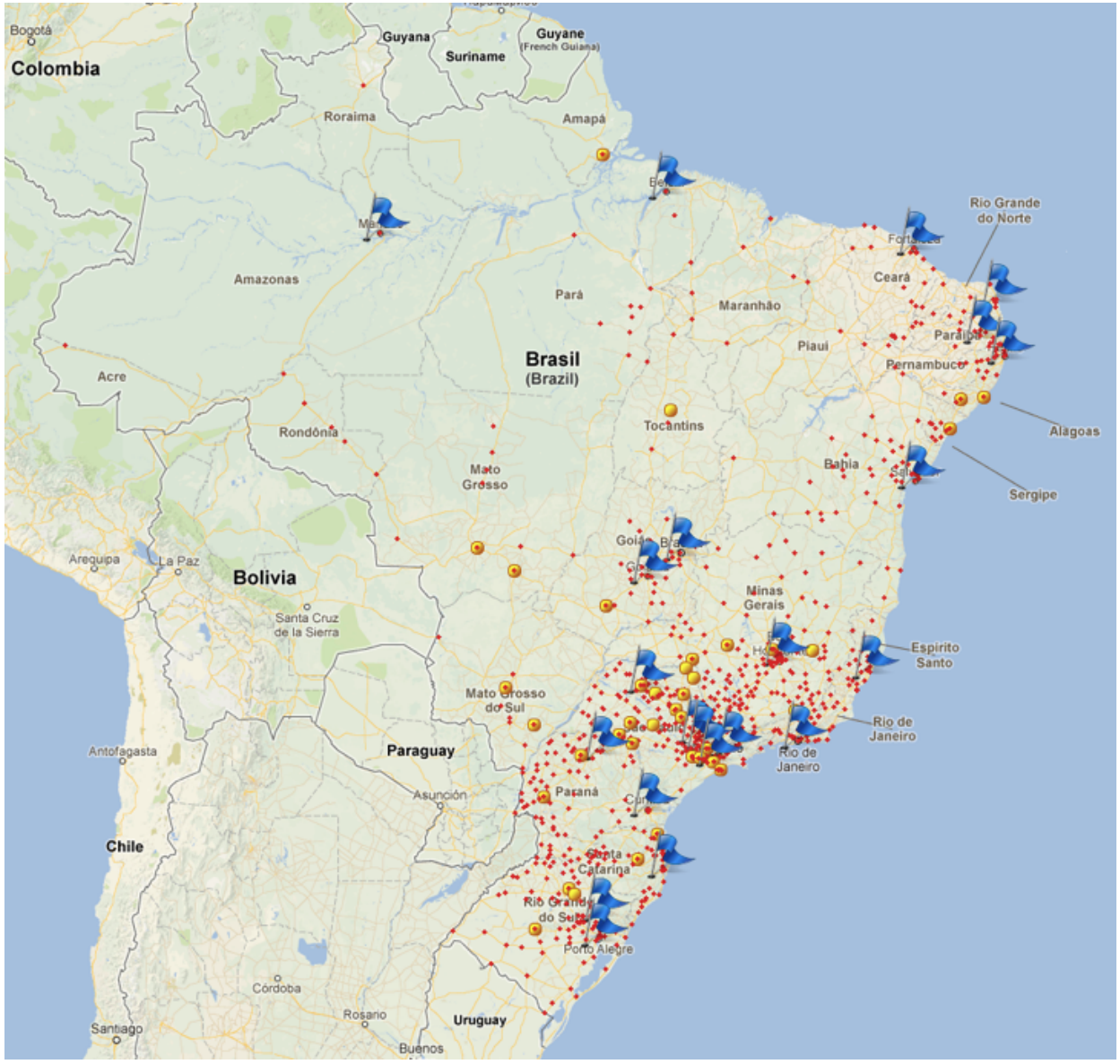
Países com Mais Pontos de Troca de Tráfego



Estados Unidos	87	Rússia	16
Brazil	23	Austrália	14
França	21	Suécia	12
Alemanha	17	Argentina	10
Japão	16	Reino Unido	09

Fonte: Packet Clearing House – pch.net

Localização dos PTTs do NIC.br/CGI.br no Brasil



Projeto iniciado em 2004 pelo CGI.br

Atualmente tem média de 200 Gbps de tráfego agregado: http://ptt.br

Países com Mais Servidores Raiz de DNS

Estados Unidos	78	França	10
Alemanha	14	Itália	10
Brazil	13	China	09
Austrália	12	Japão	08
Canadá	10	Nova Zelândia	08

Fonte: Packet Clearing House – pch.net

Como aumentar a resiliência das redes de governo e de infraestruturas críticas

- **Ter AS próprio, permitindo**
  - **seus próprios endereços IP**
  - **mais de uma saída para Internet**
  - **controle sobre configuração de roteadores, autonomia na definição de rotas**
  - **conectar-se a um PTT**
  - **mais facilidade para lidar com ataques de Negação de Serviço (DDoS)**
  - **mais facilidade para mudar de operadoras em situações de crise (apagões, fibras rompidas, etc)**

- **Haver mais operadoras por região, para permitir saídas múltiplas para a Internet, permitindo mais disponibilidade**

Alguns Desafios para o Futuro

- Qualificação profissional
  - redes, administracao de sistemas, desenvolvimento de *software* seguro
- Resistir a DDoS
  - em alguns casos a migração para CDNs é a única solução
- Migrar para o Protocolo IPv6
  - os endereços IPv4 na América Latina estão previstos para acabar em cerca de 240 dias
- Adoção de DNSSEC
  - Novos protocolos, como DANE, em estudo
- Alternativas ou melhorias ao sistema atual de certificados digitais
- Segurança na infraestrutura de roteamento
  - Roteamento fuciona por confiança nos anúncios
  - Em discussão na comunidade o uso de RPKI e S-BGP
    - Em resumo: tabelas de rotas passam a ser assinadas

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