



nic.br egi.br

cert.br

Brasília, DF

03 de setembro de 2015

Atividades do NIC.br para Segurança e Estabilidade da Internet no Brasil

Cristine Hoepers, D.Sc.
Gerente Geral, CERT.br/NIC.br

cert.br nic.br cgi.br

Comitê Gestor da Internet no Brasil – CGI.br

Entidade multissetorial, criada em 1995, responsável por coordenar e integrar as iniciativas e serviços da Internet no País. Dentre as atribuições definidas no Decreto Presidencial nº 4.829, de 03/09/2003, 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/>



1 2 3 4 5 6 7 8 9

GOVERNO

10 11 12 13 14 15 16 17 18 19 20 21

SOCIEDADE CIVIL

e

Representantes do Governo:

- 1 Ministério da Ciência, Tecnologia e Inovação (coordenador)
- 2 Casa Civil da Presidência da República
- 3 Ministério das Comunicações
- 4 Ministério da Defesa
- 5 Ministério do Desenvolvimento, Indústria e Comércio Exterior
- 6 Ministério do Planejamento, Orçamento e Gestão
- 7 Agência Nacional de Telecomunicações
- 8 Conselho Nacional de Desenvolvimento Científico e Tecnológico
- 9 Conselho Nacional de Secretários Estaduais para Assuntos de Ciência e Tecnologia

Representantes da Sociedade Civil:

- 10 Notório saber em assunto da Internet
- 11 a 14 Representantes do setor empresarial
 - provedores de acesso e conteúdo da Internet
 - provedores de infra-estrutura de telecomunicações
 - indústria de bens de informática, de bens de telecomunicações e de software
 - setor empresarial usuário
- 15 a 18 Representantes do terceiro setor
- 19 a 21 Representantes da comunidade científica e tecnológica

Núcleo de Informação e Coordenação do Ponto BR – NIC.br

Entidade civil, sem fins lucrativos, criada para implementar as decisões e os projetos do Comitê Gestor da Internet no Brasil - CGI.br.

Dentre suas atribuições estão:

- o registro e manutenção dos nomes de domínios que usam o <.br> , e a distribuição de números de Sistema Autônomo (ASN) e endereços IPv4 e IPv6 no País, por meio do Registro.br;
- tratamento e resposta a incidentes de segurança em computadores envolvendo redes conectadas à Internet no Brasil, atividades do CERT.br;
- projetos que apoiem ou aperfeiçoem a infraestrutura de redes no País, como a interconexão direta entre redes (IX.br) e a distribuição da Hora Legal brasileira (NTP.br). Esses projetos estão a cargo do Ceptro.br.
- promover estudos e recomendar procedimentos, normas e padrões técnicos e operacionais, para a segurança das redes e serviços de Internet, bem assim para a sua crescente e adequada utilização pela sociedade.

Estrutura do NIC.br

membros e ex-membros do CGI.br
(somente os atuais membros têm direito a voto)

ASSEMBLEIA GERAL

7 membros eleitos pela Assembleia Geral

CONSELHO DE
ADMINISTRAÇÃO

CONSELHO
FISCAL

ADMINISTRAÇÃO
.....
JURÍDICO
.....
COMUNICAÇÃO
.....
ASSESSORIAS:
CGI.br e PRESIDÊNCIA

DIRETORIA
EXECUTIVA

1 2 3 4 5

registro.br

Domínios

cert.br

Segurança

cetic.br

Indicadores

ceptro.br

Redes e Operações

ptt.br

Troca de Tráfego

ceweb.br

Tecnologias Web

W3C
Brasil

Padrões Web

- 1 Diretor presidente
- 2 Diretor administrativo e financeiro
- 3 Diretor de serviços e de tecnologia
- 4 Diretor de projetos especiais e de desenvolvimento
- 5 Diretor de assessoria às atividades do CGI.br

Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil – CERT.br

Criado em 1997, com base em estudo do CGI.br para o melhor modelo para uma coordenadoria de segurança em redes

Principais atividades:

- **Tratamento de Incidentes**

- Ponto de contato nacional para notificação de incidentes
- Atua facilitando o processo de resposta a incidentes das várias organizações
- Trabalha em colaboração com outras entidades
- Auxíliam novos CSIRTs (Grupos de Tratamento de Incidentes de Segurança) a estabelecerem suas atividades

- **Formação de profissionais para atuar em Tratamento de Incidentes**

- **Produção de boas práticas e material para conscientização sobre a necessidade de segurança na Internet**

<http://www.cert.br/sobre/>

The background of the slide features a dark gray, textured pattern of white circuit board traces and components, including a circular dial-like element on the right side.

Incidentes de Segurança

cert.br nic.br cgi.br

Incidentes de Segurança Reportados ao CERT.br

O CERT.br recebe notificações de incidentes de segurança envolvendo redes conectadas à Internet no País

- feitas voluntariamente por administradores de redes e usuários de Internet, sejam eles do Brasil ou do exterior

Conceitos relacionados:

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

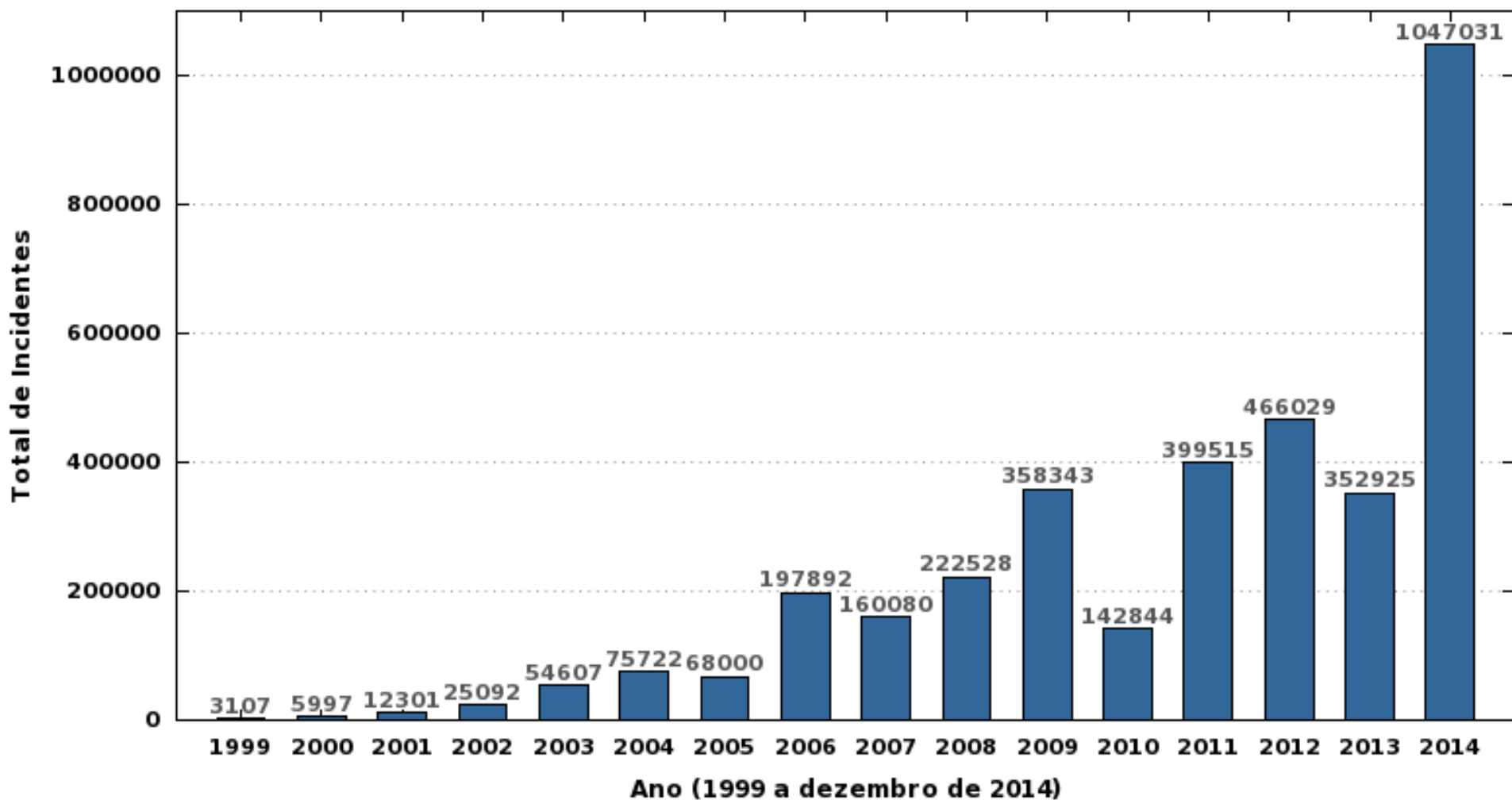
Tratamento de Incidentes – processo de identificar e mitigar os incidentes de segurança; também envolve a prevenção

CSIRT – acrônimo internacional para designar um Grupo de Resposta a Incidentes de Segurança, responsável por tratar incidentes de segurança para um público alvo específico

Outros acrônimos: IRT, CERT, CIRC, CIRT, SERT, SIRT, ETIR, CTIR

Estatísticas CERT.br – 1999-2014

Total de Incidentes Reportados ao CERT.br por Ano



Notificações mais comuns em 2014

44% tentativas de fraude, destas

- 72% notificações de eventuais violações de direitos autorais
- 26% notificações de tentativas de fraude com objetivos financeiros envolvendo o uso de páginas falsas ou códigos maliciosos

29% varreduras em redes de computadores

- amplamente utilizadas por atacantes e códigos maliciosos para identificar potenciais alvos, enumerando vulnerabilidades aos serviços habilitados em um computador

21% ataques de negação de serviço, majoritariamente

- envolvendo servidores mal configurados no Brasil, sendo abusados para amplificar ataques de negação de serviço
- envolvendo computadores, modems e roteadores *wi-fi* infectados ou mal configurados, sendo abusados para participar em ataques de negação de serviço

Como reduzir os incidentes e seus impactos

Primeiro objetivo é um ecossistema saudável

Nenhum único grupo ou estrutura conseguirá fazer sozinho a segurança ou a resposta a incidentes - todos possuem um papel

- **administradores de redes e sistemas**
 - não emanar “sujeira” de suas redes e adotar boas práticas
- **usuários**
 - entender os riscos e seguir as dicas de segurança
 - manter seus dispositivos atualizados e tratar infecções
- **desenvolvedores**
 - precisam pensar em segurança desde o início

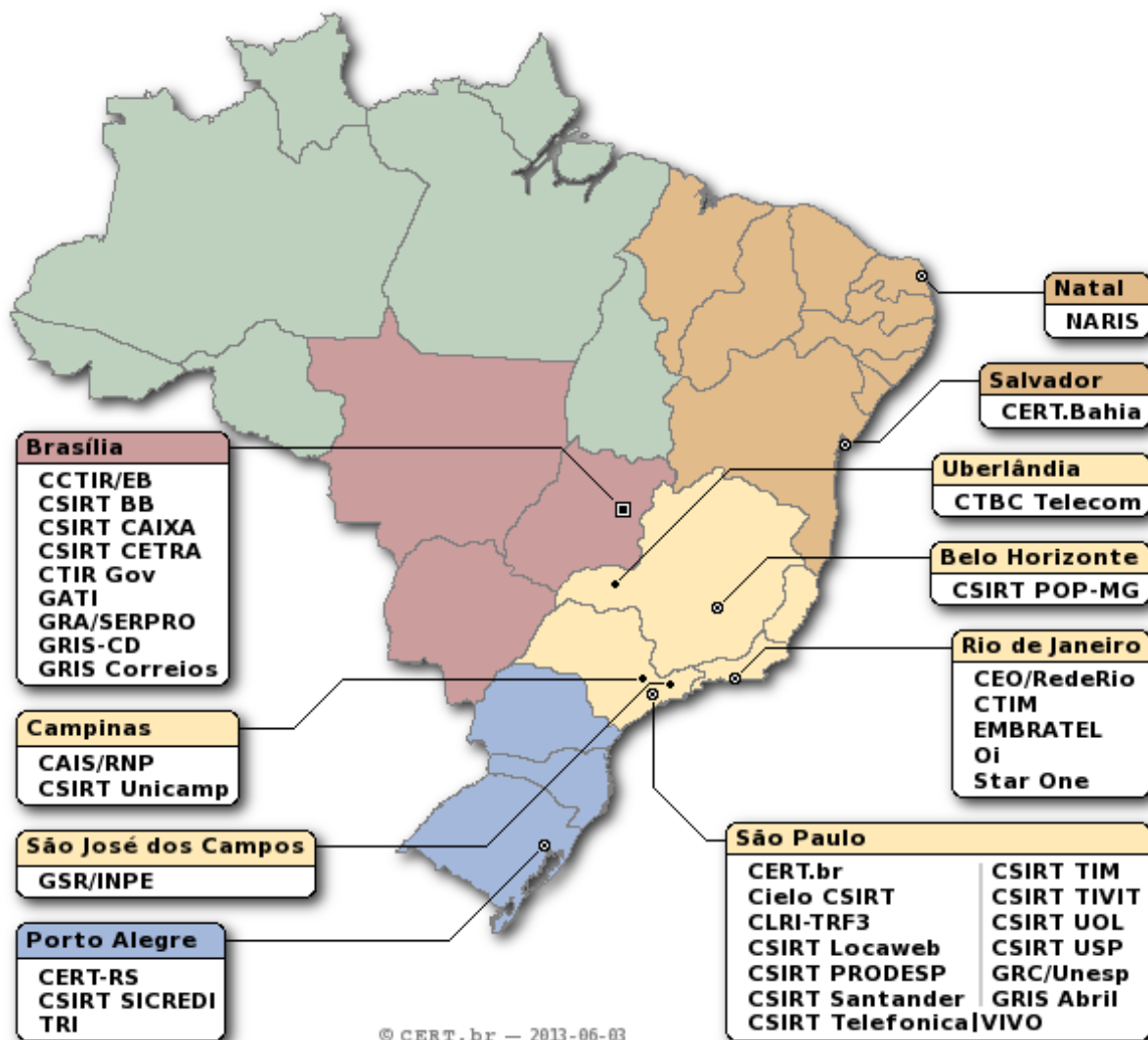
Ainda assim incidentes ocorrerão

- **necessário identificar e mitigar mais rapidamente**
 - redução de impactos é grande se a atuação é rápida
 - necessários profissionais habilitados e CSIRTs estabelecidos
 - cooperação é fundamental – nacional e internacionalmente

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

Conteúdo disponível *online* gratuitamente sob Licença *Creative Commons*

- Livro (PDF e ePub) e conteúdo no *site* (HTML5)
- Dica do dia no *site*, via *Twitter* e RSS
- Impressões em pequena escala enviadas a escolas e centros de inclusão digital
- Uso por instituições para treinar funcionários

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

The image displays a screenshot of the website <http://cartilha.cert.br/> and a physical copy of the booklet. The website interface includes a navigation menu with options like 'Início', 'Livro', 'Fascículos', and 'Sobre'. A main article titled 'Navegar é preciso, arriscar-se não!' is visible, along with a 'Dica do dia' section and a 'Veja também' section. The physical copy of the booklet features a cover illustration of a boat on the ocean with sharks below, and the text 'Cartilha de Segurança para Internet' and logos for cert.br, nic.br, and cgi.br.

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
- Verificação em Duas Etapas
- Redes



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, que possuam material *online*

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

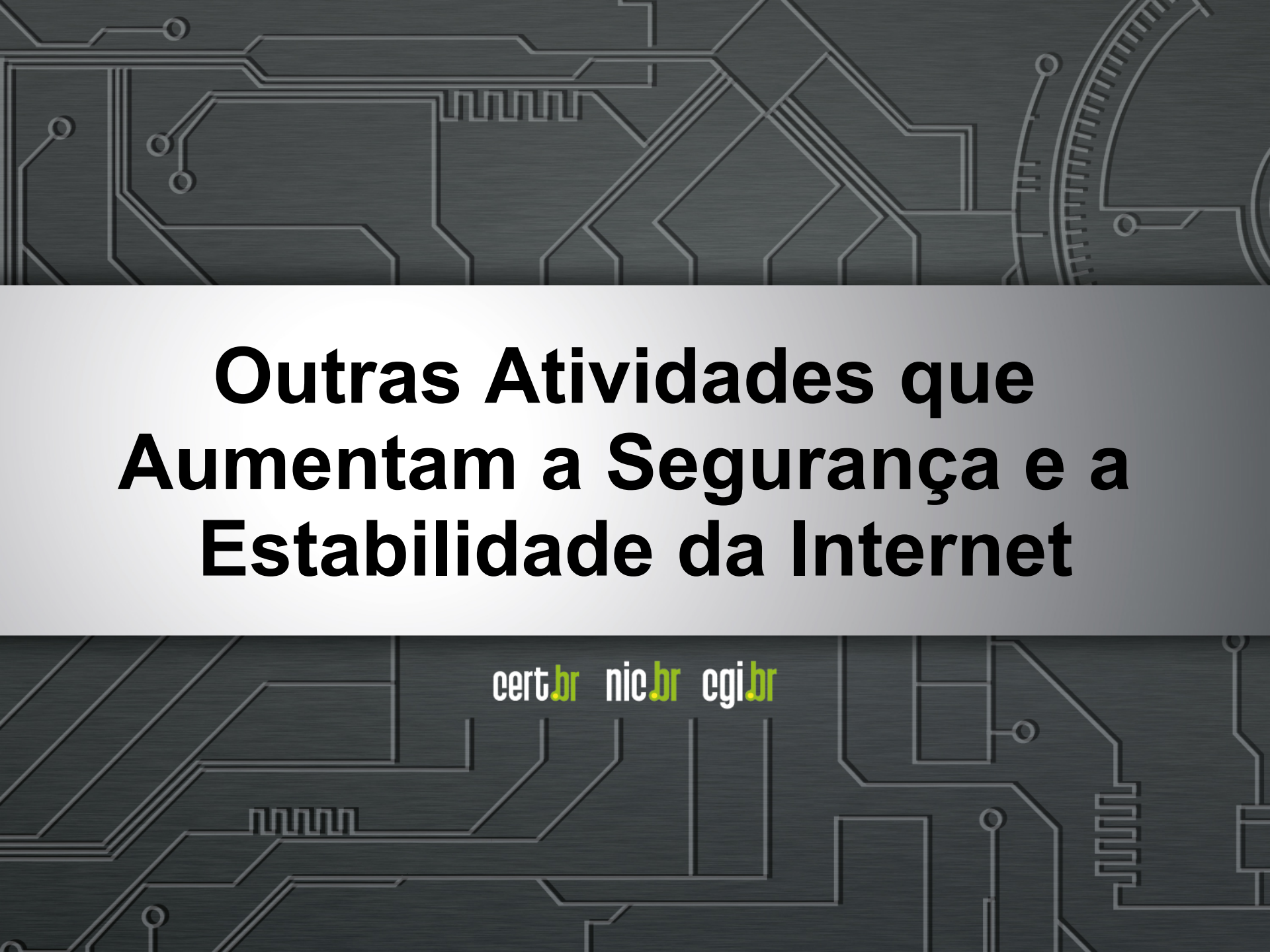


**INTERNET
SEGURA.BR**

Site e vídeos do Antispam.br

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



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.

Outras Atividades que Aumentam a Segurança e a Estabilidade da Internet

cert.br nic.br cgi.br

Recursos Críticos para o Funcionamento da Internet

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

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

“Um nome indica o que procurar. Um endereço aponta aonde encontrar. A rota diz como chegar até lá.”

– John Postel

Estratégias do NIC.br/CGI.br para aumentar a estabilidade e segurança da Internet no Brasil

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 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 ASN**
- manutenção gratuita dos Pontos de Troca de Tráfego (IX.br)**
- aumento da resiliência dos sistemas de resolução de nomes**
- treinamentos em boas práticas para administração de ASNs, IPv6, DNS**
- treinamento de especialistas em tratamento de incidentes**

Registro.br:

Segurança e Resiliência de DNS no Brasil

Implementação das extensões de segurança do DNS – DNSSEC – em todo o <.br>

Manutenção de cópias (*mirrors*) de servidores DNS raiz (*root servers*) em diversos pontos do Território Nacional

- Estes servidores são os ponteiros iniciais para que se possa percorrer a árvore de resolução de nomes

Presentes em 97 países:

País servidores

EUA 86

Brasil 19

Alemanha 15

Canadá 13

França 13

Austrália 12

China 10

Itália 10

Japão 09

Inglaterra 08



Fonte: Packet Clearing House – pch.net

IX.br (antigo PTT.br):

Melhora na Disponibilidade e Estabilidade

Objetivo primário dos Pontos de Troca de Tráfego: melhor conectividade, qualidade e redução de custo.

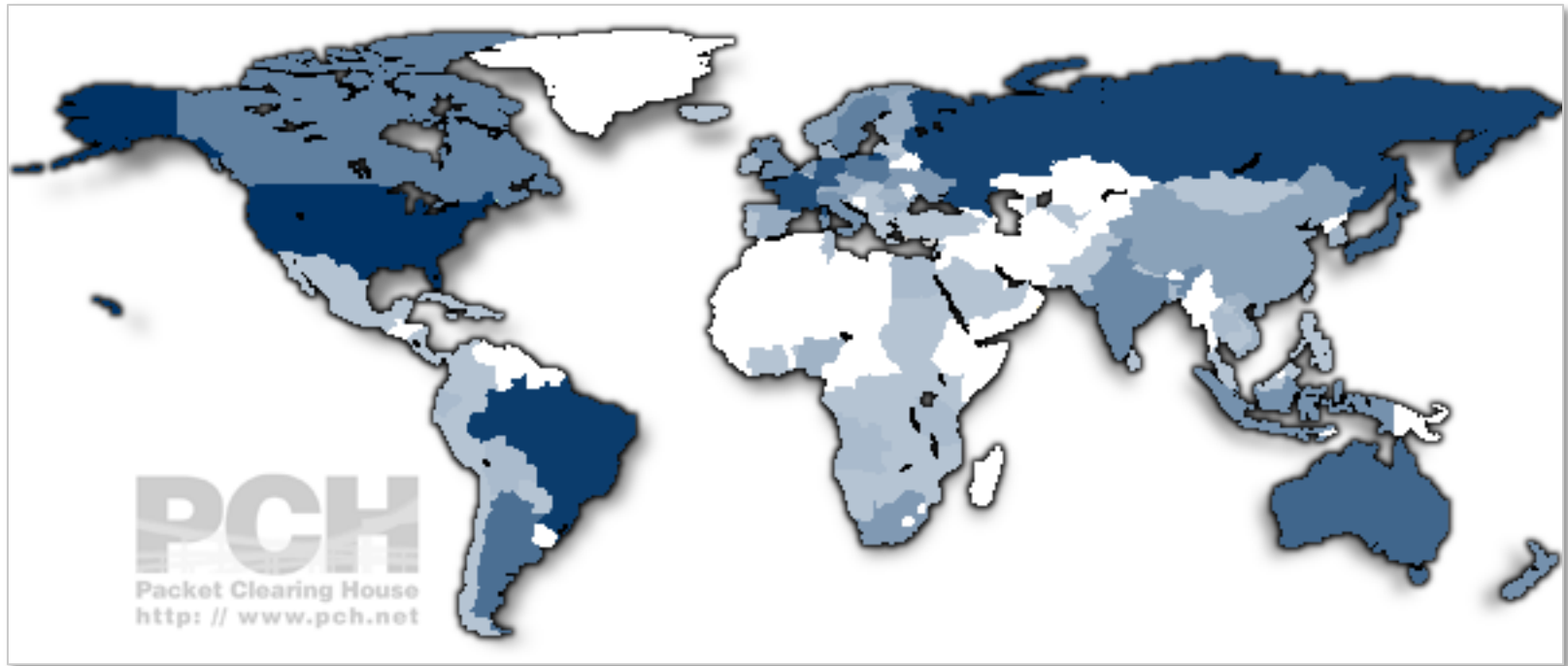
25 pontos de troca de tráfego mantidos pelo NIC.br:

<http://ix.br/localidades/atuais>

Efeito para disponibilidade e estabilidade:

- **Estimula as redes a terem Sistema Autônomo (AS) próprio, permitindo**
 - seus próprios endereços IP
 - mais de uma saída para Internet e possibilidade de conexão com um Ponto de Troca de Tráfego
 - mais flexibilidade na definição de rotas
 - mais facilidade para lidar com ataques de Negação de Serviço (DDoS) volumétricos

Países com Mais Pontos de Troca de Tráfego



EUA	84
<u>Brasil</u>	<u>27</u>
Rússia	21
França	20
Alemanha	19

Japão	16
Austrália	14
Argentina	13
Polônia	10
Suécia	09

Fonte: Packet Clearing House – pch.net

Iniciativas de Incentivo a Boas Práticas

- **DNSSEC, para segurança do sistema de nomes (DNS)**
<http://registro.br/tecnologia/dnssec.html?secao=dnssec>
- **Cartilha de Segurança para Internet**
<http://cartilha.cert.br>
- **Práticas Anti-Spam**
<http://antispam.br/>
- **Cursos de IPv6 e de boas práticas em administração de sistemas autônomos**
<http://ipv6.br/calendario/>
- **Cursos de Tratamento de Incidentes**
<http://www.cert.br/cursos/>
- **Padrões Web**
<http://ceweb.br/publicacoes/indice/>

Eventos para Fomentar a Cooperação

Eventos gratuitos organizados pelo NIC.br:

- Grupo de Trabalho de Engenharia e Operação de Redes (GTER)
- Grupo de Trabalho em Segurança de Redes (GTS)
- Fórum da Internet no Brasil
- Seminário de Proteção à Privacidade e aos Dados Pessoais
- Fórum Brasileiro de CSIRTs
- Conferência Web W3C Brasil
- Semana de Infraestrutura da Internet no Brasil
 - PTT Fórum - Encontro dos Sistemas Autônomos da Internet no Brasil
 - Fórum IPv6
 - GTER/GTS

<http://nic.br/eventos/agenda/organiza/>

Obrigada

www.cert.br

© cristine@cert.br

© @certbr

03 de setembro de 2015

nic.br cgi.br

www.nic.br | www.cgi.br