nic.br cgi.br | cert.br

Workshop Lições Aprendidas Jogos Rio2016

17 de abril de 2017

Brasília, DF

Atuação do CERT.br e Lições Aprendidas no Tratamento de Incidentes na Rio 2016

Cristine Hoepers, D.Sc.
Gerente Geral
cristine@cert.br

cert.br nic.br cgi.br

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/

cgi.br

1 2 3 4 5 6 7 8 9 — GOVERNO e 10 11 12 13 14 15 16 17 18 19 20 21 — SOCIEDADE CIVIL

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

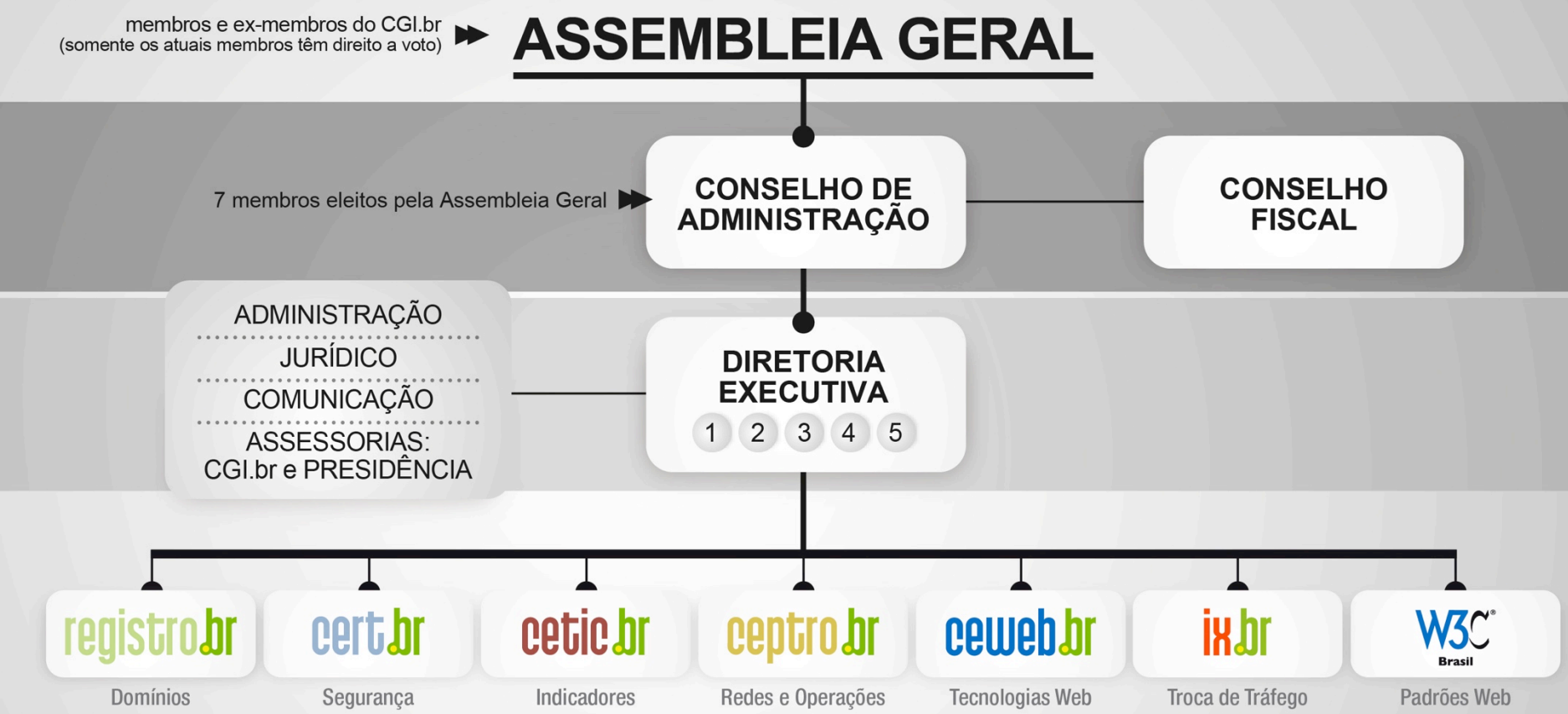
Entidade civil, sem fins lucrativos, criada para implementar as decisões e os projetos do Comitê Gestor da Internet no Brasil - CGI.br.

Dentre suas atribuições estão:

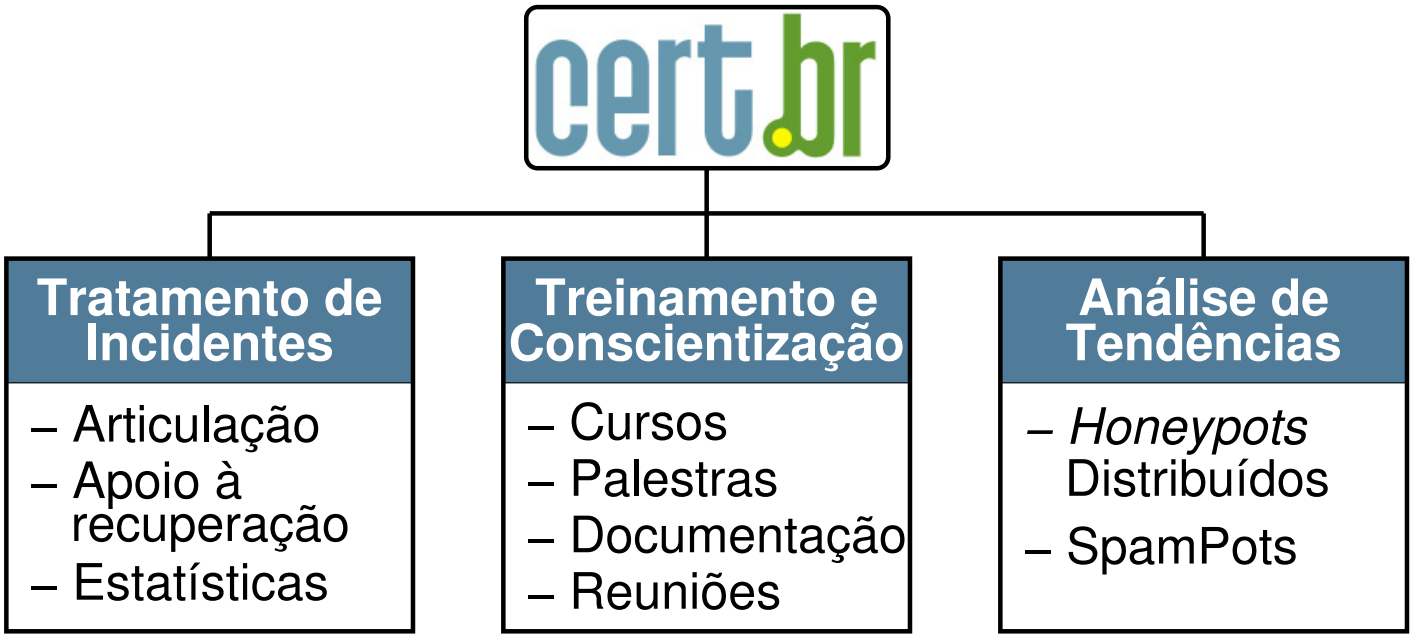
- o registro e manutenção dos nomes de domínios que usam o <.br> , e a distribuição de números de Sistema Autônomo (ASN) e endereços IPv4 e IPv6 no País, por meio do Registro.br;
- **tratamento e resposta a incidentes de segurança em computadores envolvendo redes conectadas à Internet no Brasil, atividades 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.**

http://www.nic.br/sobre/

Estrutura do NIC.br



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



SEI Partner
Carnegie Mellon

FIRST
Improving Security Together
MEMBER

APWG
RESEARCH PARTNER
www.antiphishing.org

The Honeynet PROJECT

Atuação nacional desde junho de 1997:

- **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
  - Auxilia 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 para diversas audiências**

Atuação do CERT.br nos Jogos Rio2016

cert.br nic.br cgi.br

Cooperação Entre
Rio 2016, CERT.br, CTIR Gov e CDCiber

Planejamento similar ao da Copa 2014

Adição do Rio2016 CSIRT como parceiro

Divisão de tarefas

- **Rio2016 CSIRT : time 24x7 para as redes dos jogos**
- **CDCiber: atuação presencial nos Centros de Comando e Controle e foco em redes do interesse do MD e infraestruturas críticas**
- **CTIR Gov: foco nos ataques às redes do Governo**
- **CERT.br: facilitar a comunicação e coordenação com outros atores e auxiliar no acompanhamento de ameaças**

Atuação CERT.br:
Período Preparatório

Participação nas atividades parte do "*Rio2016 Cyber Security Core Team*" – 2014-2016

- **identificação possíveis ameaças e cenários de ataques**
- **levantamento das necessidades de infraestrutura**
- **definição do modelo e dos processos de tratamento de incidentes**

Treinamentos Especiais em Tratamento de Incidentes

- **2015: SOC e CSIRT Rio2016**
- **2016: Destacamentos de Defesa Cibernética**

Rede iNOC-DBA mantida pelo NIC.br

- **Alocação de aparelhos para comunicação rápida entre CSIRTs (Grupos de Resposta a Incidentes) e Operadores de Redes**

Atividades para facilitar a cooperação antes e durante os Jogos

- **reunião e grupo de cooperação com operadoras e empresas de *hosting***
- **divulgação do planejamento nacional para parceiros internacionais**
  - LAC-CSIRTs Bogotá, setembro/2015
  - FIRST TC Praga / TF-CSIRTs Meeting, Janeiro/2016

Mensagem ao FIRST

```
Date: Mon, 4 Jul 2016 21:22:58 -0300
From: Cristine Hoepers <cristine@cert.br>
To: first-teams@first.org
Subject: Rio 2016 Olympic Games - Incident Handling Contacts

Dear FIRST Teams,
[...]
As part of the coordinated efforts to prevent and respond to incidents
related to the games we'll have 4 teams working in cooperation:

- Rio2016 CSIRT <csirt@rio2016.com> - 24/7 team, onsite at the games,
  that will handle incidents related to the games infrastructure (they
  are also handling all cases involving phishing of the Games' Oficial
  sites and sites selling fake tickets).

- CERT.br <cert@cert.br> - will coordinate and facilitate
  communication with external parties, situational awareness and
  network monitoring.  You can copy CERT.br in any notification, this
  will help situational awareness and will allow us to pull in anyone
  else needed for coordination.

- CTIR Gov <ctir@ctir.gov.br> - will handle all incidents targetted to
  .gov.br networks.

- CDCiber <abuse@cdciber.eb.mil.br> - 24/7 personnel at the Games'
  Security Command and Control Centers, with special focus on national
  critical infrastructure.
[...]
```

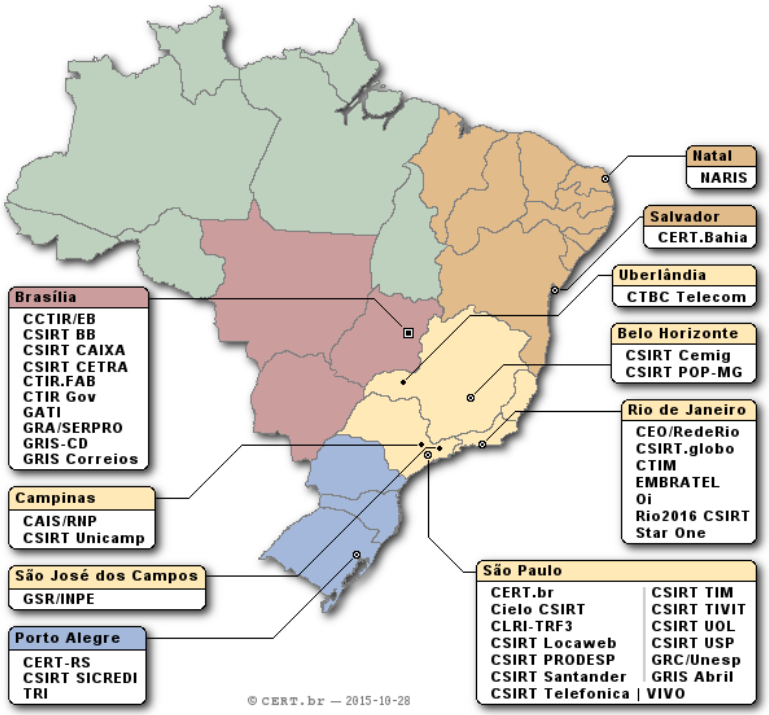
Atuação CERT.br:
Durante os Jogos

Monitoramento extra de incidentes e fontes de dados sobre ataques

- notificações de incidentes
- *feeds* de dados (*Honeypots* Distribuídos do CERT.br, Team Cymru, ShadowServer, Operações Anti-Botnet)
- fontes públicas de informação (Twitter, Facebook, IRC, C&C, *defacements*)

Comunicação e coordenação com outros atores

- via a rede de contatos já estabelecida, principalmente CSIRTs
  - https://www.cert.br/csirts/brasil/
  - https://first.org/members
  - https://www.cert.org/incident-management/national-csirts/national-csirts.cfm



Incidentes Observados e Lições Aprendidas

cert.br nic.br cgi.br

Categorias de Incidentes Observados

- **Tentativas de fraudes financeiras usando o nome dos Jogos como atrativo para infectar vítimas**
- ***Sites* com vendas não autorizadas de ingressos**
- **Desfiguração de *sites* com mensagens de protesto contra os Jogos**
  - **em menor número que na Copa 2014**
- **Supostos vazamentos de dados de *sites* de governo e de entidades envolvidas com os jogos**
  - **alguns dados eram públicos**
  - **outros dados não foi possível verificar se eram confidenciais ou se foram forjados**
- **Ataques Distribuídos de Negação de Serviço (DDoS) contra *sites* de governo e contra patrocinadores**

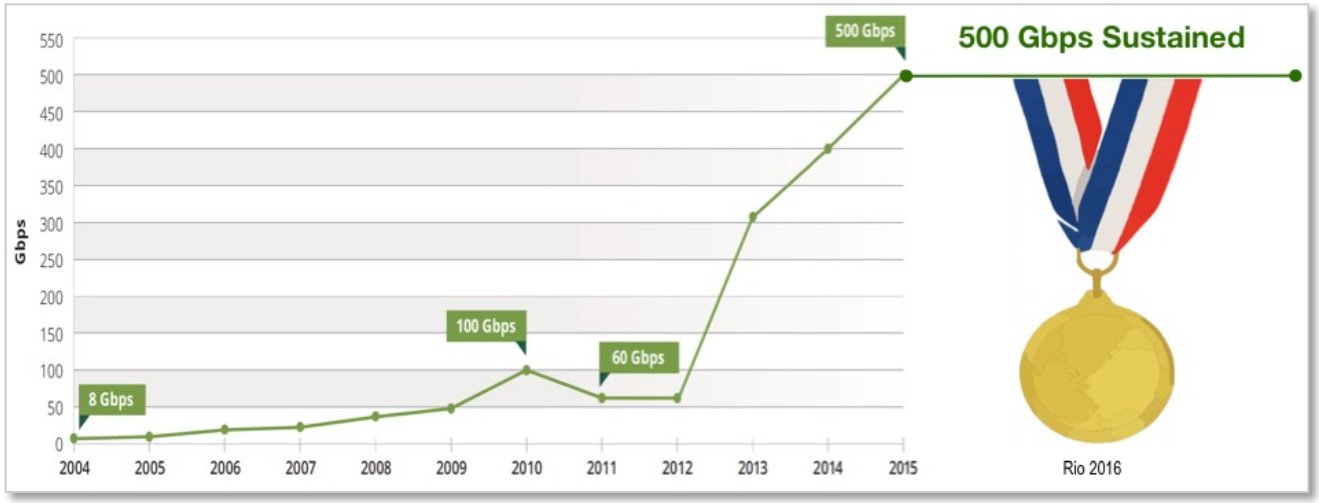
Sobre fatos divulgados na mídia

Vazamento de dados da Agência Mundial Antidoping (WADA)

- confirmado publicamente pela agência[1], apontando a causa como uma mensagem direcionada de *phishing* que levou ao comprometimento de credenciais
- infraestrutura da WADA era independente dos Jogos Rio2016

Ataques DDoS de 540Gbps, segundo Arbor ASERT

- Publicou o artigo entitulado "*Rio Olympics Take the Gold for 540gb/sec Sustained DDoS Attacks!*"[2], que continha este gráfico:



[1] https://www.wada-ama.org/en/media/news/2016-09/wada-confirms-attack-by-russian-cyber-espionage-group
[2] https://www.arbornetworks.com/blog/asert/rio-olympics-take-gold-540gbsec-sustained-ddos-attacks/

Copa 2014 vs. Rio 2016:
Principais Diferenças

Copa 2014

- **Processo quase não envolveu a FIFA ou Comitê local de organização**
- **Sem ponto de contato para notificar incidentes envolvendo a infraestrutura dos jogos**
- **Manifestações de rua e *hacktivismo* intensos e com grande impacto**
- **Pico de DDoS reportado: 4Gbps**

Rio 2016

- **Comprometimento e envolvimento total do Comitê Organizador local**
- **Rio2016 CSIRT como ponto focal, com funcionamento 24x7**
- **Manifestações reduzidas, *hacktivismo* presente, mas sem tanto impacto**
- **Pico de DDoS: entre 300Gbps e 500Gbps**

Os Jogos Rio2016 foram os primeiros em um cenário tão hostil do ponto de vista de ataques DDoS

Destaques

- **A existência do CSIRT Rio2016 foi essencial**
  - **Parte da comissão organizadora**
  - **Conhecimento profundo da infraestrutura e das pessoas**
- **Vários CSIRTs cooperando foi mais efetivo que um único time**
  - **A Internet é uma rede de redes**
  - **A segurança depende de cada organização implementar sua parte**
- **Pontos que fizeram diferença**
  - **Haver uma rede de cooperação já existente no país**
  - **Relação de confiança entre os profissionais foi essencial**
    - habilitou compartilhamento intenso de informações, mesmo sem uso de plataformas específicas
  - **Pessoal qualificado fez a diferença**
    - ferramentas são irrelevantes sem pessoal altamente qualificado

Obrigada

www.cert.br

cristine@cert.br @certbr

17 de abril de 2017

nic.br cgi.br

www.nic.br | www.cgi.br