CTIR Gov

CENTRO DE TRATAMENTO DE INCIDENTES DE SEGURANÇA DE REDES DE COMPUTADORES DA ADMINISTRAÇÃO PÚBLICA FEDERAL

http://www.ctir.gov.br

Antônio Magno
Coordenador-Geral

3º Fórum Brasileiro de CSIRTs – São Paulo/SP – 16/09/2014

Objetivo

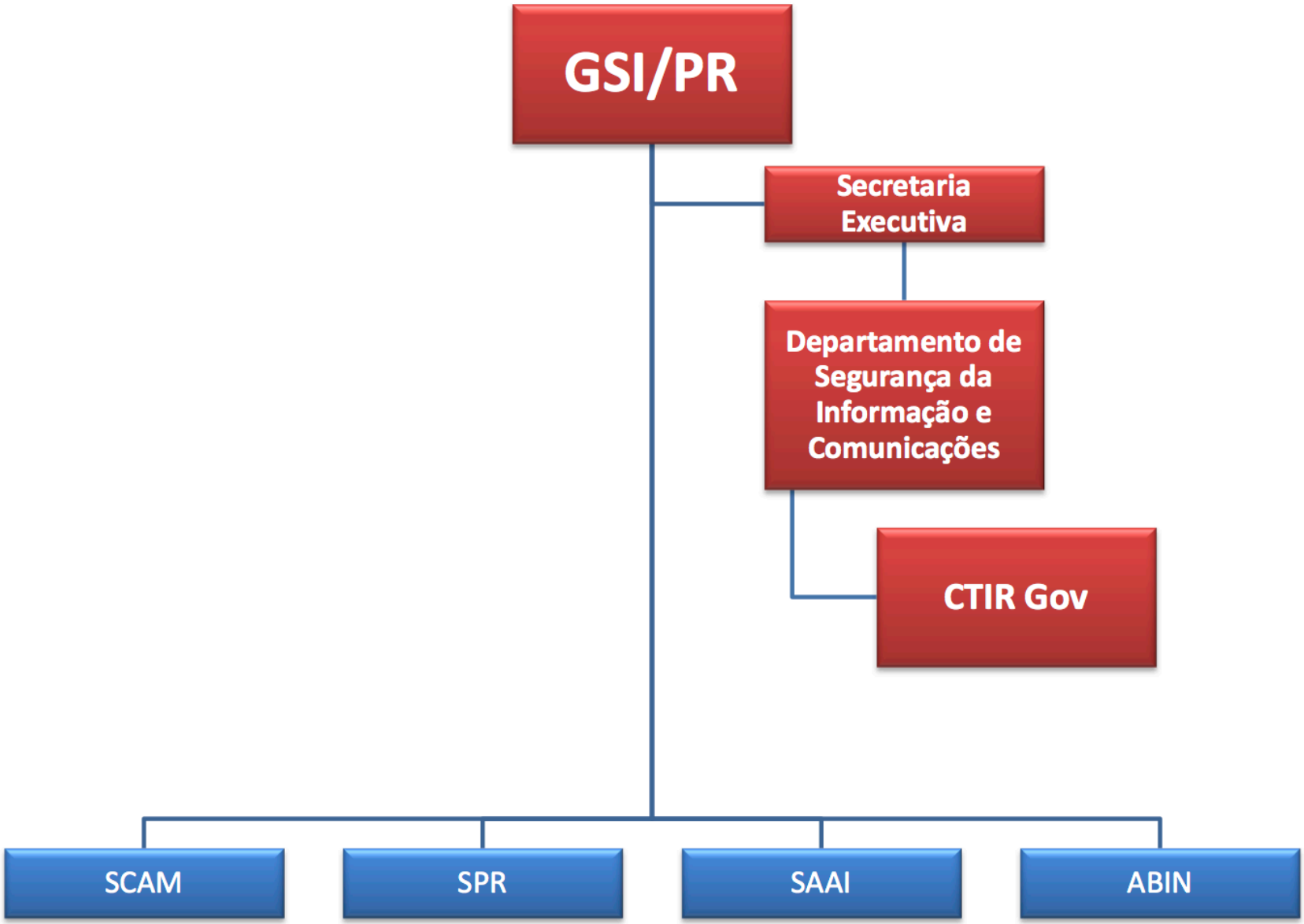
Atuação do CTIR Gov na coordernação das atividades de tratamento de incidentes na APF durante os Grandes Eventos.

Sumário

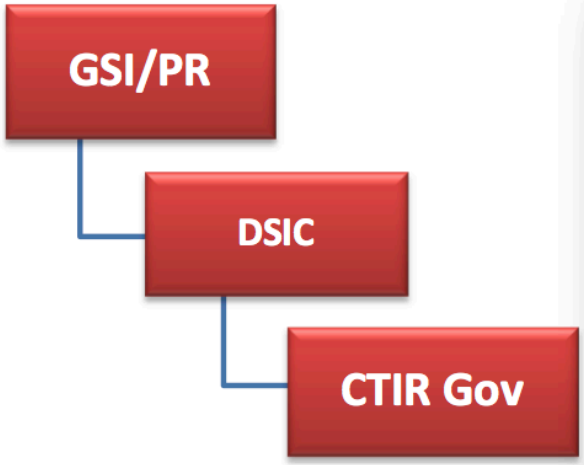
Agenda

- ✓ Ambientação
- ✓ Grandes Eventos
- ✓ Conclusões

Ambientação



Ambientação



LEI Nº 10.683, DE 28 DE MAIO DE 2003.

CAPÍTULO I
DA PRESIDÊNCIA DA REPÚBLICA
Seção I
Da Estrutura

Art. 1º A Presidência da República é constituída, essencialmente:

VI - pelo Gabinete de Segurança Institucional;

Art. 6º Ao Gabinete de Segurança Institucional da Presidência da República compete:

IV - coordenar as atividades de inteligência federal e de segurança da informação;

DECRETO Nº 5.772, DE 8 DE MAIO DE 2006. (revogado)
DECRETO Nº 6.931, DE 11 DE AGOSTO DE 2009. (revogado)
DECRETO Nº 7.411, DE 29 DE DEZEMBRO DE 2010. (revogado)

DECRETO Nº 8.100, DE 4 DE SETEMBRO DE 2013

Aprova a Estrutura Regimental
Cargos e Funções

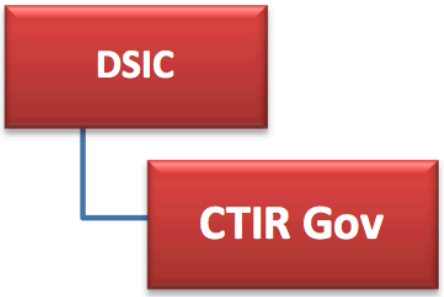
CAPÍTULO III
DAS COMPETÊNCIAS DOS ÓRGÃOS
Seção I

Art. 6º Ao Departamento de Segurança da Informação e Comunicações compete:

III - operacionalizar e manter centro de tratamento e resposta a incidentes ocorridos nas redes de computadores da administração pública federal;

CTIRGov

Ambientação



GABINETE DE SEGURANÇA INSTITUCIONAL

PORTARIA Nº 56, DE 5 DE NOVEMBRO DE 2009

Art. 1º Aprovar o Regimento Interno do Gabinete de Segurança Institucional da Presidência da República, na forma do anexo a esta Portaria.

Art. 39. À Coordenação-Geral de Tratamento de Incidentes de Redes compete:

I - operar e manter o Centro de Tratamento de Incidentes de Segurança de Redes de Computadores da Administração Pública Federal (CTIR Gov);

II - promover o intercâmbio científico-tecnológico relacionado a incidentes de segurança em redes de computadores junto a outros centros;

III - apoiar órgãos e entidades da administração pública federal nas atividades de tratamento de incidentes de segurança em redes de computadores;

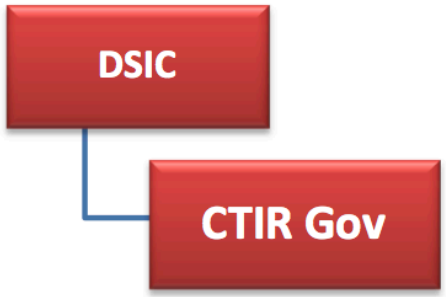
IV - monitorar e analisar tecnicamente os incidentes de segurança nas redes de computadores da administração pública federal;

V - implementar mecanismos que permitam a avaliação dos danos ocasionados por incidentes de segurança nas redes de computadores da administração pública federal; e

VI - apoiar, incentivar e contribuir no âmbito da administração pública federal para a capacitação no tratamento de incidentes de segurança em redes de computadores.

CTIRGov

Ambientação



- ✓ **Centro de Coordenação Nacional**
- ✓ **Comunidade de Tratamento de Incidentes do CTIR Gov**
  - APF direta e indireta
  - excepcionalmente, Estados e Municípios
  - "gov.br", "jus.br", "leg.br", "mil.br", "mp.br" e outros.

GABINETE DE SEGURANÇA INSTITUCIONAL

PORTARIA Nº 56, DE 5 DE NOVEMBRO DE 2009

Art. 1º Aprovar o Regimento Interno do Gabinete de Segurança Institucional da Presidência da República, na forma do anexo a esta Portaria.

Art. 39. À Coordenação-Geral de Tratamento de Incidentes de Redes compete:

I - operar e manter o Centro de Tratamento de Incidentes de Segurança de Redes de Computadores da Administração Pública Federal (CTIR Gov);

II - promover o intercâmbio científico-tecnológico relacionado a incidentes de segurança em redes de computadores junto a outros centros;

III - apoiar órgãos e entidades da administração pública federal nas atividades de tratamento de incidentes de segurança em redes de computadores;

IV - monitorar e analisar tecnicamente os incidentes de segurança nas redes de computadores da administração pública federal;

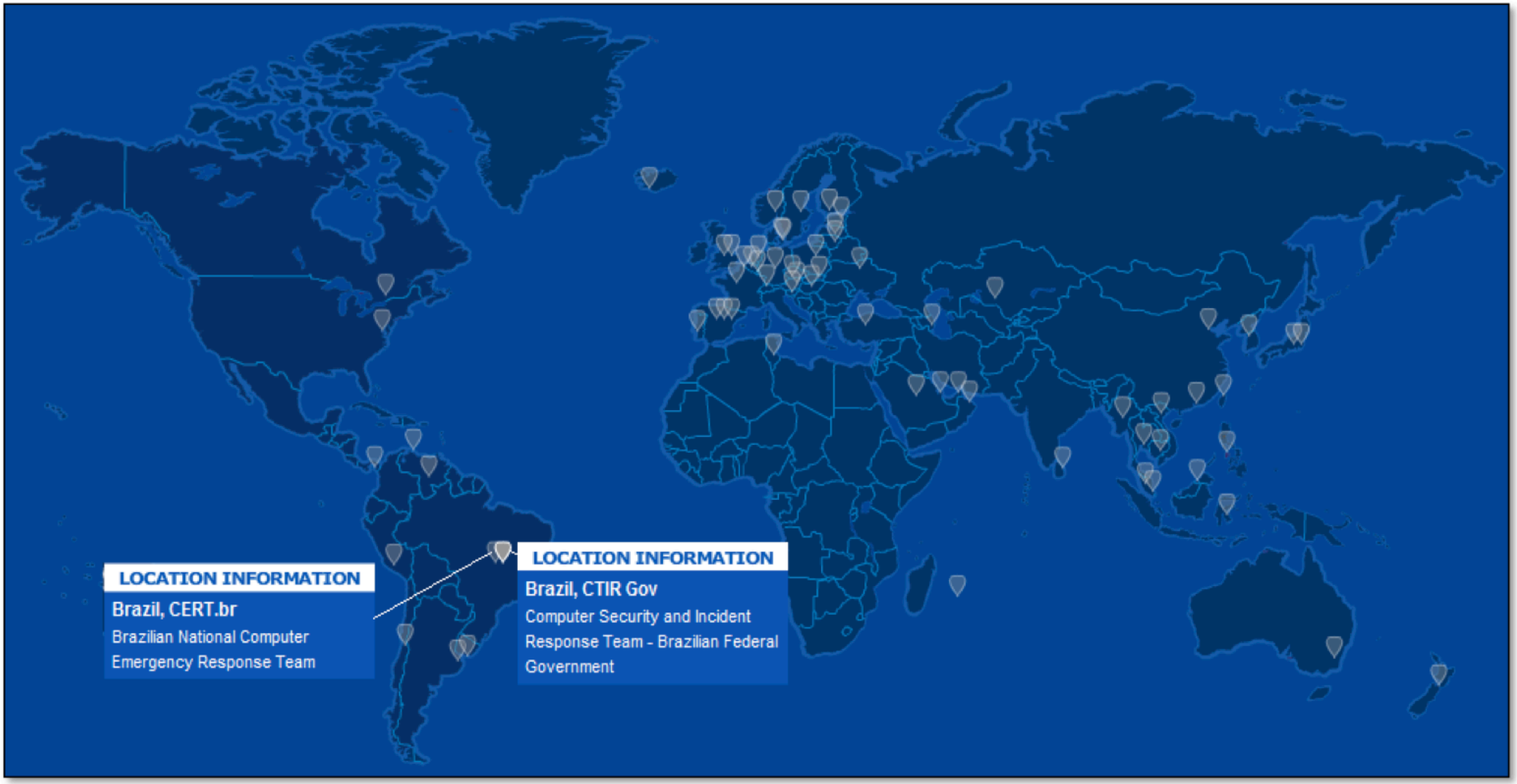
V - implementar mecanismos que permitam a avaliação dos danos ocasionados por incidentes de segurança nas redes de computadores da administração pública federal; e

VI - apoiar, incentivar e contribuir no âmbito da administração pública federal para a capacitação no tratamento de incidentes de segurança em redes de computadores.

CTIRGov

Ambientação

Centros de tratamento com responsabilidade nacional



Fonte: http://www.cert.org/csirts/national/

CTIR Gov

Tratamento de Incidentes de Rede

Legislação de SIC

- **Instrução Normativa GSI Nº 1** , de 13 de junho de 2008. Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências. (Publicada no DOU Nº 115, de 18 Jun 2008- Seção 1)

  - **Norma Complementar nº 05/IN01/DSIC/GSIPR** , e seu **Anexo**, Disciplina a criação de Equipes de Tratamento e Respostas a Incidentes em Redes Computacionais - ETIR nos órgãos e entidades da Administração Pública Federal. (Publicada no DOU Nº 156, de 17 Ago 2009 - Seção 1)

  - **Norma Complementar nº 08/IN01/DSIC/GSIPR** , Estabelece as Diretrizes para Gerenciamento de Incidentes em Redes Computacionais nos órgãos e entidades da Administração Pública Federal. (Publicada no DOU Nº 162, de 24 Ago 2010 - Seção 1)

*** Para mais informações sobre Legislação de SIC, acesse o sítio do DSIC em http://dsic.planalto.gov.br/legislacaodsic**

CTIR Gov

Tratamento de Incidentes de Rede

Serviços oferecidos pelo CTIR Gov

- ✓ Notificação de incidentes de segurança
- ✓ Análise de incidentes de segurança
- ✓ Suporte à recuperação de incidentes
- ✓ Coordenação na resposta a incidentes
- ✓ Distribuição de alertas, recomendações e estatísticas
- ✓ Cooperação com outras equipes de tratamento de incidentes

CTIR Gov

Sumário

Agenda

- ✓ Ambientação
- ✓ **Grandes Eventos**
- ✓ Conclusões

CTIR Gov

Coordenação prévia

Preparação

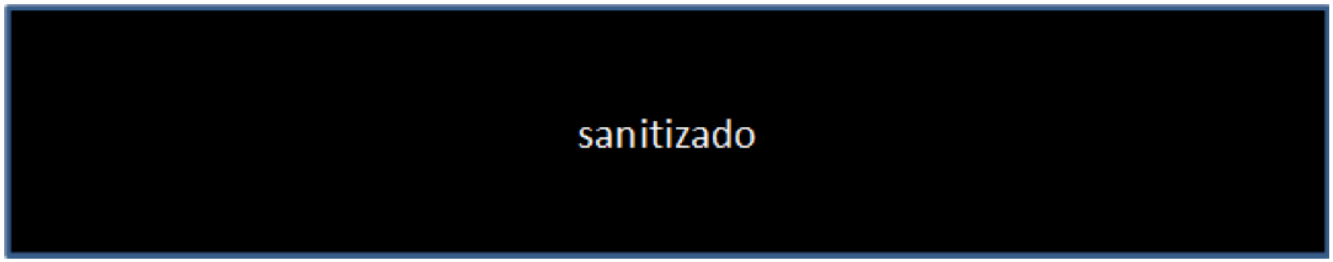
- ✓Reuniões em diversos níveis
  - ✓Coordenação geral
  - ✓Aspectos técnicos
- ✓ Definição de tarefas
  - ✓ CDCiber -> Coordenar e Integrar
  - ✓ CERT.br -> Botnets, IRC e desfigurações
  - ✓ CTIR Gov -> Indisponibilidade de sítios, GSS e análise de *malware*
- ✓ Matriz de comunicação
  - ✓ Sobreaviso
  - ✓ INOC-DBA
  - ✓ Telefones fixos

CTIR Gov

Rio+20 (Junho 2012)

Principais eventos:

1. Indisponibilidade de sítios:
   - "Agenda Total", www.dilma13.com.br, sanitizado
   - Anúncio de utilização da ferramenta T50.
2. Vazamento de dados:



3. Desfiguração de sítios:
   - Diversos sítios;
   - Anúncio de utilização de *Zero Day* em Joomla.
4. Acesso não autorizado a servidor FTP do STF:
   - Possibilitava escrita a usuários não autorizados;
   - Foram identificados arquivos e diretórios suspeitos.

CTIR Gov

Copa das Confederações (Junho 2013)

Linha do Tempo x Principais Incidentes

15/06 – Sáb	16/06 – Dom	17/06 – Seg	18/06 – Ter	19/06 – Qua	20/06 - Qui
• Início das operações	• Alerta CDCiber sobre sítios possivelmente vulneráveis • Notificações do CERT.br para os sítios "Gov"	• Dificuldades de correlacionamento dos incidentes (triagem)	• Deface "Blog da Dilma" • Outras desfigurações mencionando "fora Dilma" e "OpPasseLivre"	• Migração de copa2014.gov.br para BlockDos.com	• Ataques DDoS sanitizado
21/06 – Sex	**22/06 – Sáb**	**24/06 – Seg**	**25/06 – Ter**	**30/06 – Dom**	**01/07 - Seg**
• Alerta do DSIC na Reu do Por do Sol • Aviso Interministerial	• Vazamento no sanitizado cientificado	• Notícia Estadão • Dezenas de sanitizado ra	• DDoS em múltiplos sítios • Supostos Vazamentos • Notícias na Imprensa sanitizado • Tutorial DDoS em Gov.br	• Final da Copa	• Desmobilização das equipes

CTIRGov

Jornada Mundial da Juventude - JMJ (Julho 2013)

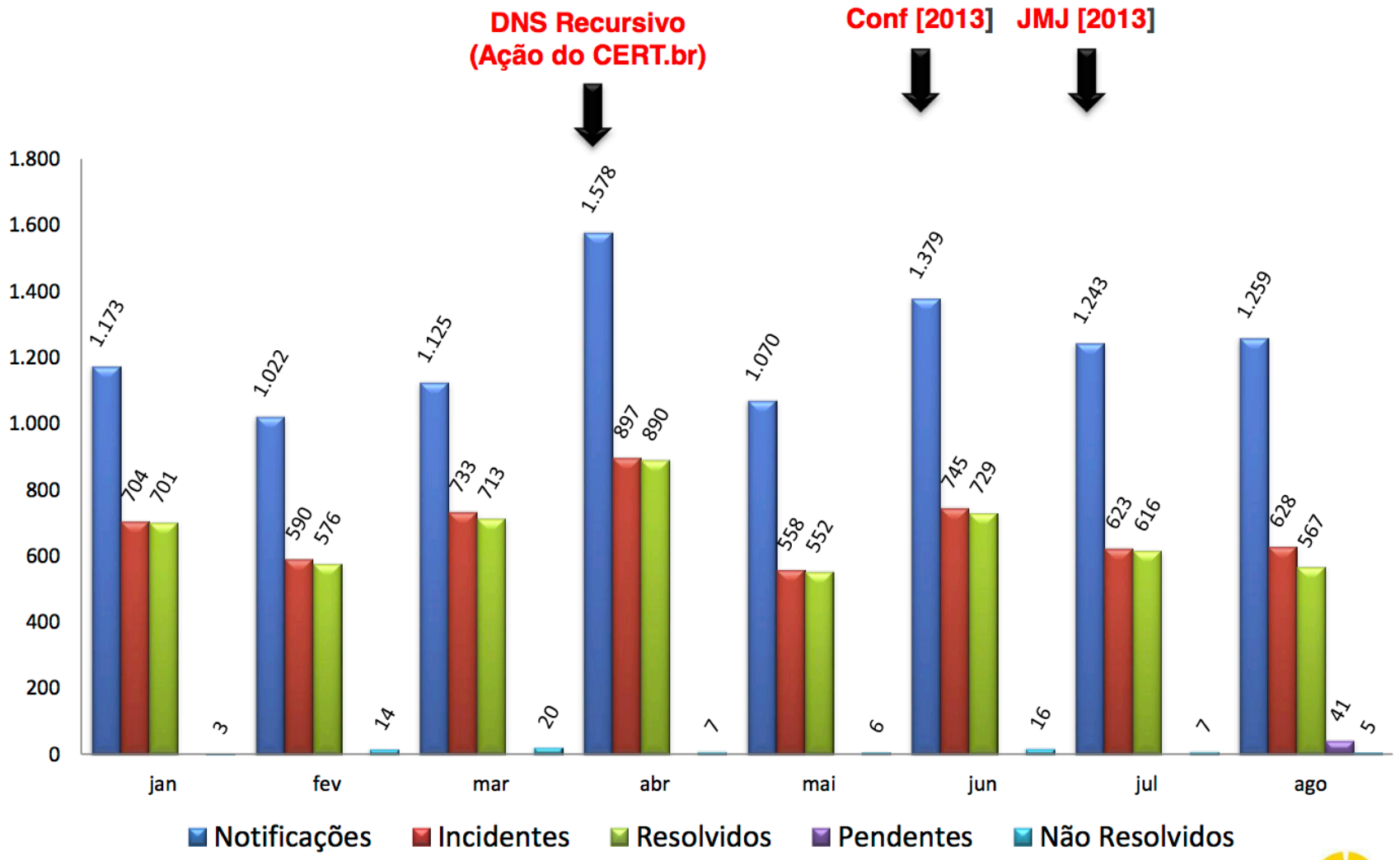
- Possível Vazamento de Dados [sanitizado]
- Interceptação em Mídias Sociais Abertas de possível utilização de servidor da [sanitizado] [sanitizado]s;
- Indisponibilid
- Possível Vazamento de Dados [sanitizado]
- Possível Vazamento de Dados
- Possível Vazamento de Dados
- Interceptação em Mídias Sociais Abertas de articulação de ataque aos sítios das PC de SP e RJ;
- Possível Vazamento de Dados [sanitizado]
- Possível Vazamento de usuário e senha diversos gov.br;
- Interceptação em Mídias Sociais Abertas de articulação de ataque aos sítios das [sanitizado]
- Possível "Phishing Message" - Falso cadastro associado à participação na JMJ (mudança de sede de Guaratiba para Copacabana) – Atuação do CDCIBER-CERT.br e CTIR Gov;
- Possível Vazamento de Dados [sanitizado]

Obs: Diversas desfigurações sem referência sobre a JMJ, apenas mensagens sobre "OperacaoSeteSetembro" e questões políticas em outros países.

CTIRGov

Copa das Confederações e JMJ

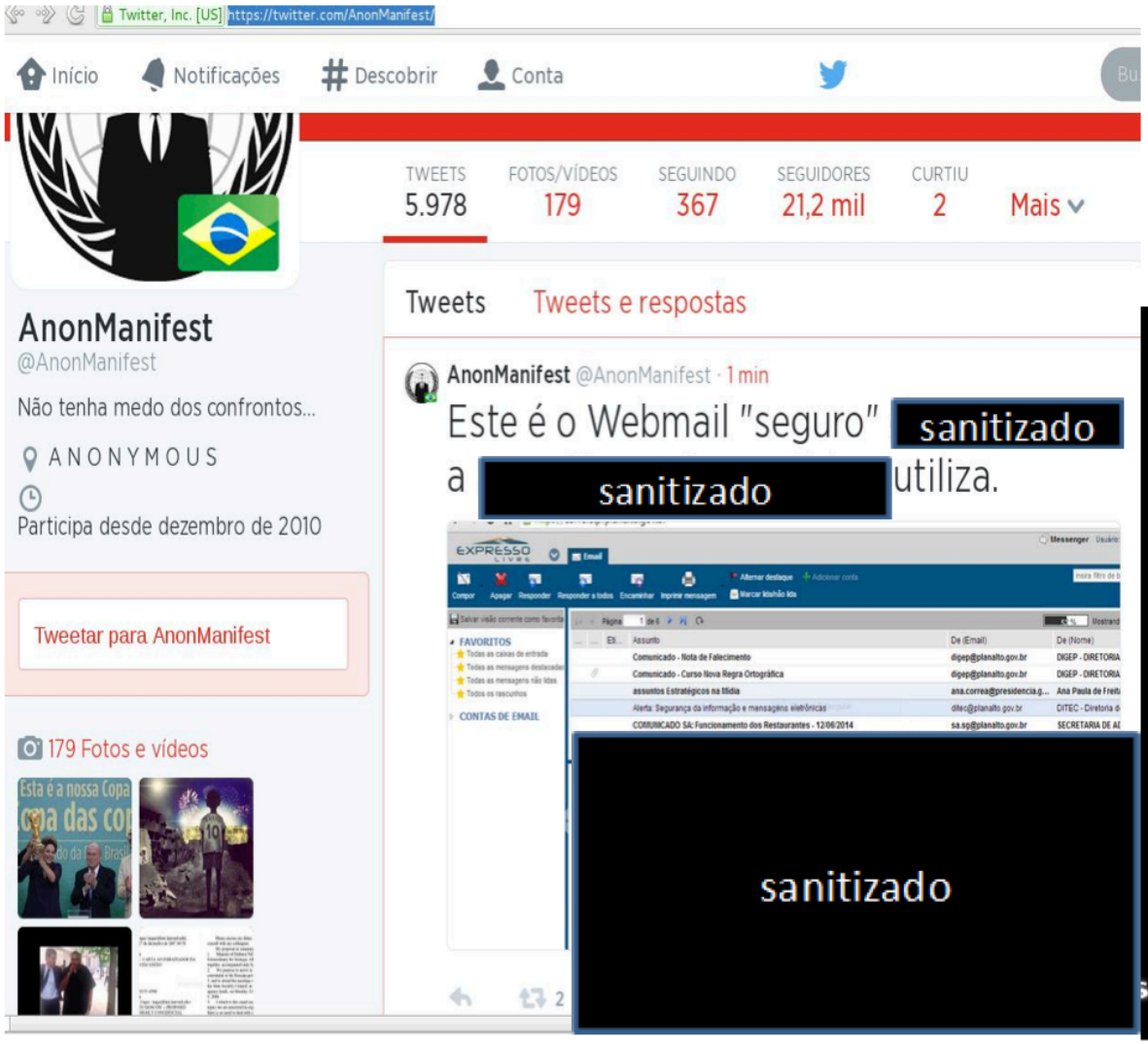
Estatísticas



CTIRGov

Copa do Mundo (Junho/Julho 2014)

INCIDENTES DE MAIOR RELEVÂNCIA

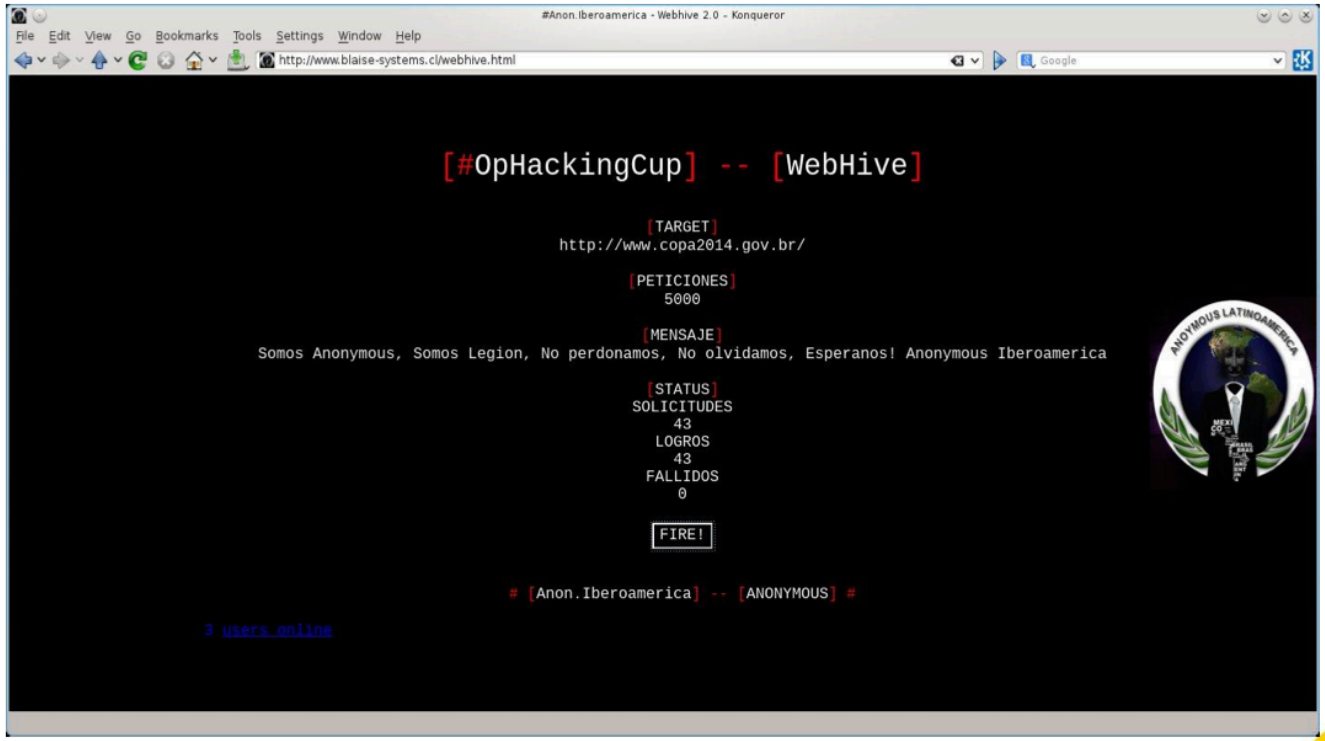


Copa do Mundo (Junho e Julho 2014)

INCIDENTES DE SEGURANÇA DE MAIOR RELEVÂNCIA

1. Ataques de Negação de Serviço:

1.1 Os ataques de negação de serviço foram, em sua maior parte, detectados por meio de acompanhamento de canais de comunicação IRC (*Internet Relay Chat*), o que permitiu identificar a hospedagem de diversas ferramentas para ataques de negação de serviço (DoS/DDoS*)* do tipo "LOIC" (*Low Orbit Ion Canon*).



sítio comprometido hospedando LOIC contra o sítio copa2014.gov.br

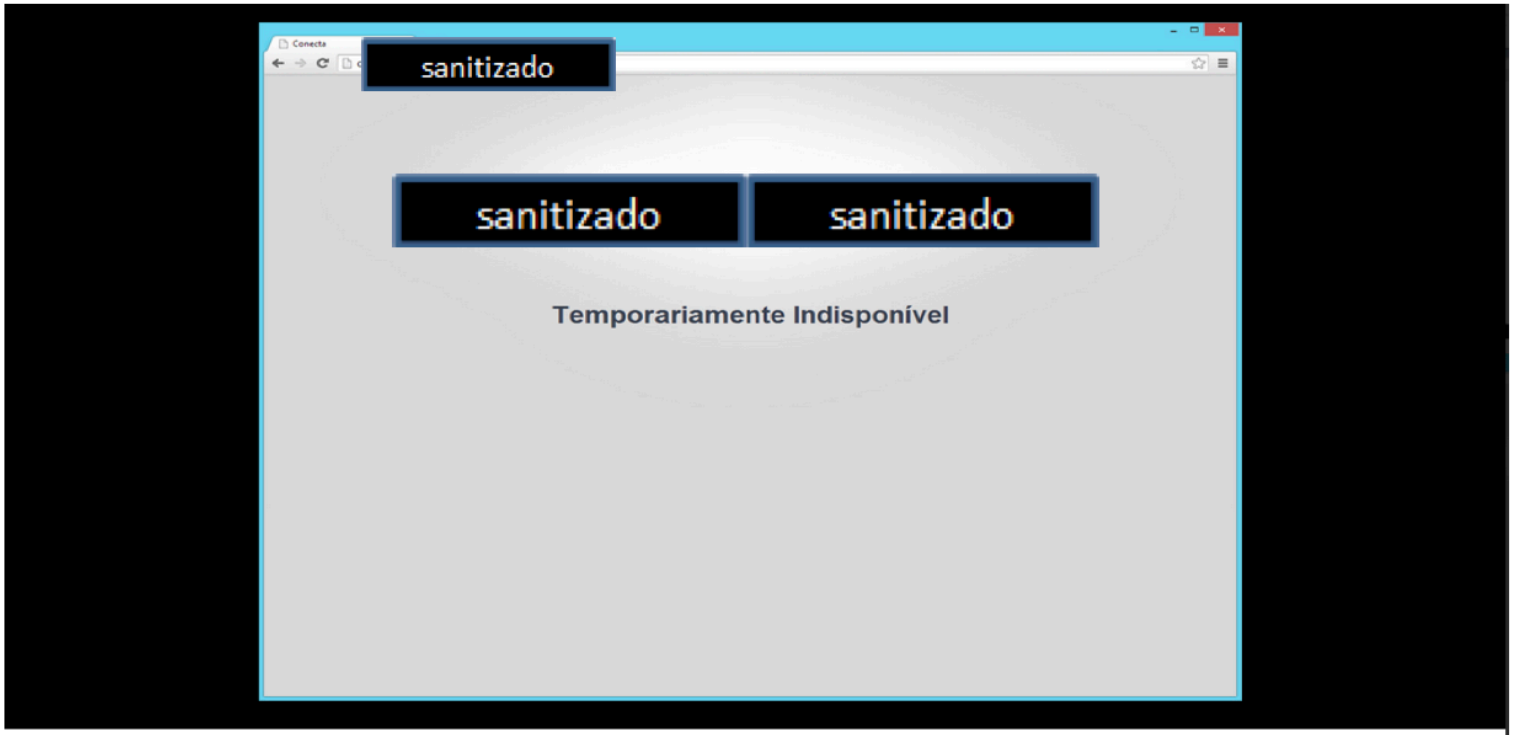
CTIR Gov

Copa do Mundo (Junho e Julho 2014)

INCIDENTES DE SEGURANÇA DE MAIOR RELEVÂNCIA

2. Indisponibilidade de Sítios:

Como consequência do ataques de negação de serviço destacamos também os eventos de Indisponibilidade de Sítio, com algumas ocorrências relacionadas aos domínios do Governo, FIFA e patrocinadores do evento.



CTIR Gov

Copa do Mundo (Junho e Julho 2014)

INCIDENTES DE SEGURANÇA DE MAIOR RELEVÂNCIA

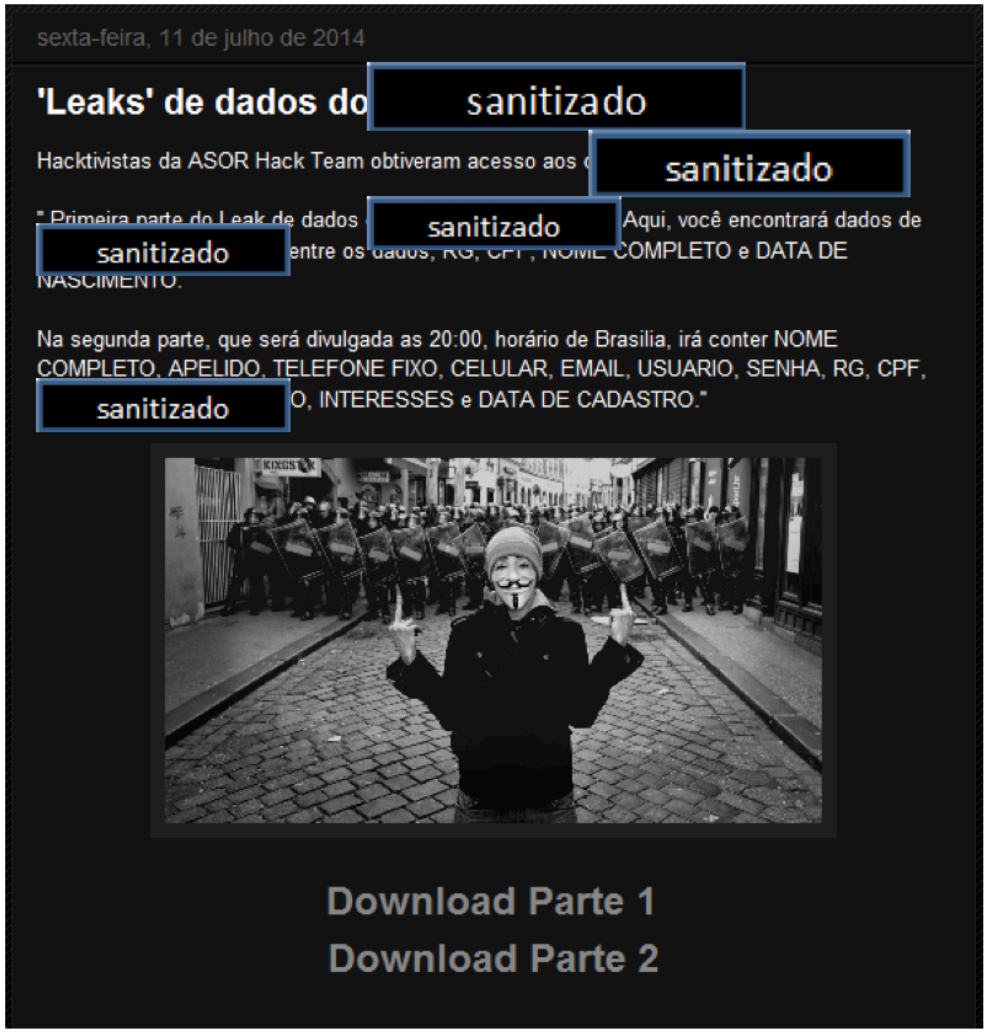
3.Ataques de Engenharia Social (Spear Phishing):

O CTIR Gov recebeu notificações de Instituições governamentais que foram vítimas de ataques de engenharia social (*Phishing Message*), enviados com o objetivo de obter credenciais de usuários daquelas redes.

Copa do Mundo (Junho e Julho 2014)

INCIDENTES DE SEGURANÇA DE MAIOR RELEVÂNCIA

4. Exposição de informações sensíveis (LEAKS):

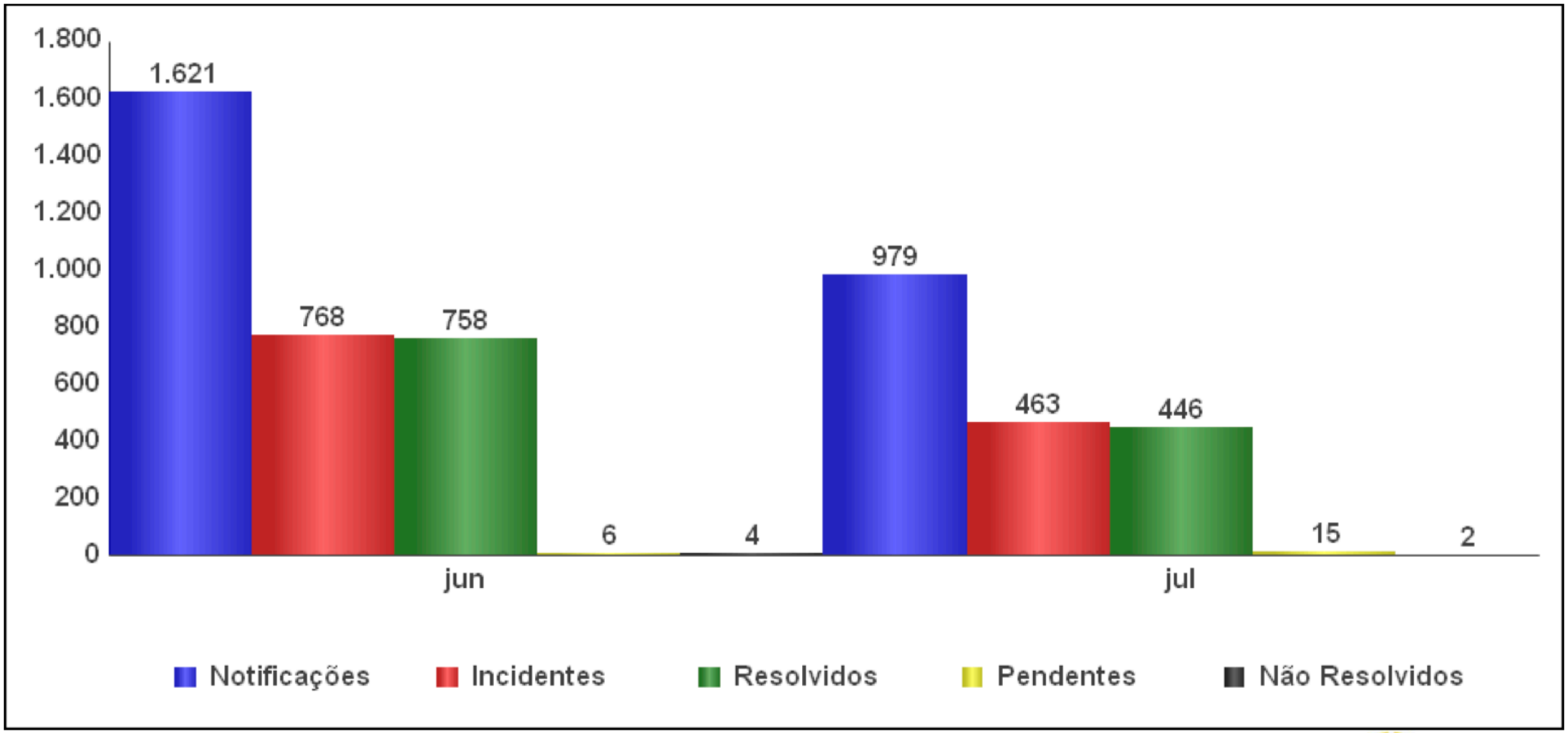


O CTIR Gov categoriza como “LEAKS”, os incidentes com ocorrência de exposição na Internet, de informações sensíveis ou privadas ou que afetem a imagem de Instituições da Administração Pública.

Total de 182 notificações de Exposição/Vazamento de Informação de dados sensíveis expostos nos domínios: http://pastebin.com, http://siph0n.net, http://justpaste.it, além de outros.

Copa do Mundo (Junho e Julho 2014)

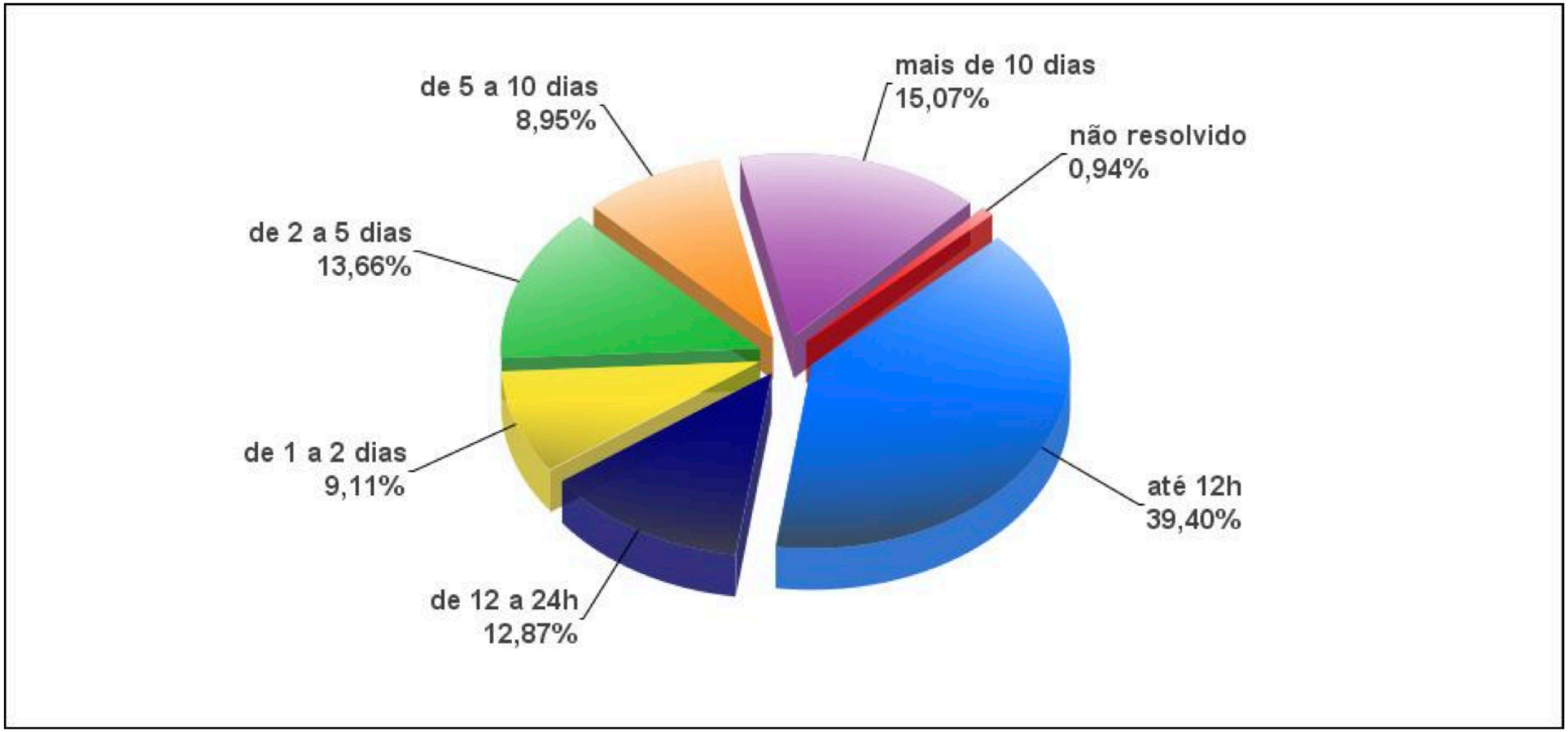
	Notificações	Incidentes	Resolvidos	Pendentes	Não Resolvidos
Ano Mes					
jun	1.621	768	758	6	4
jul	979	463	446	15	2
Total	**2.600**	**1.231**	**1.204**	**21**	**6**



CTIRGov

Copa do Mundo (Junho e Julho 2014)

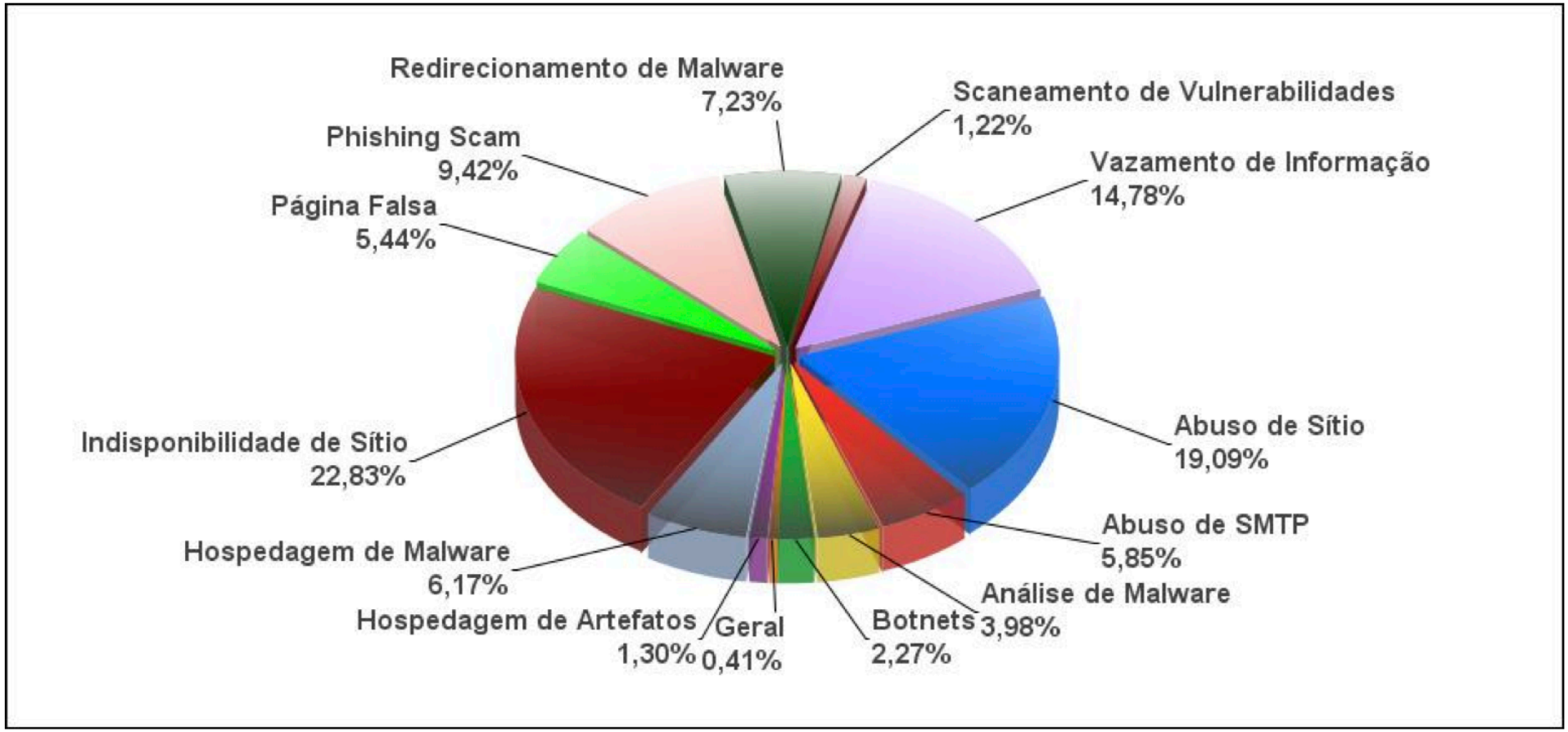
Tempo de resolução de incidentes



CTIRGov

Copa do Mundo (Junho e Julho 2014)

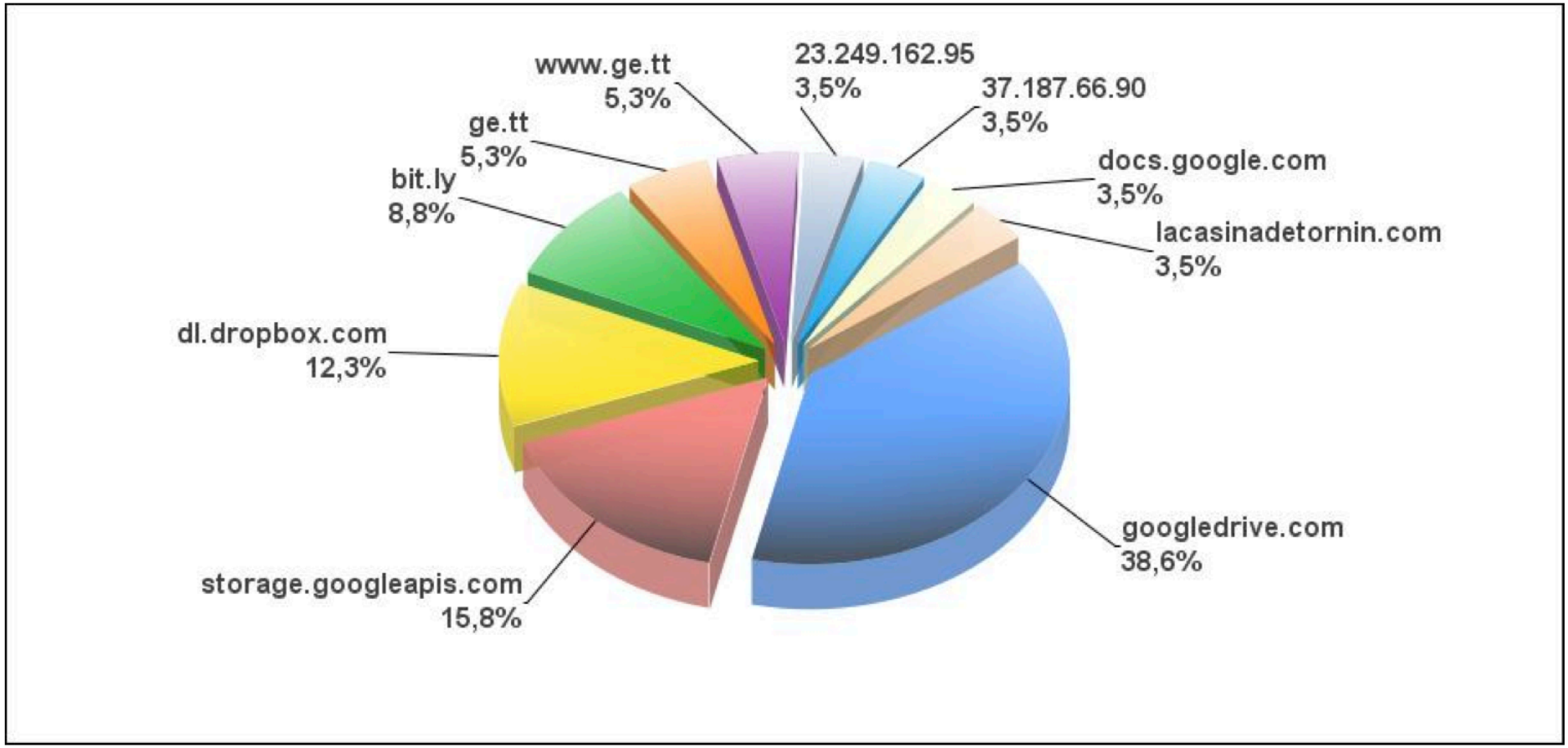
Incidentes por categoria



CTIRGov

Copa do Mundo (Junho e Julho 2014)

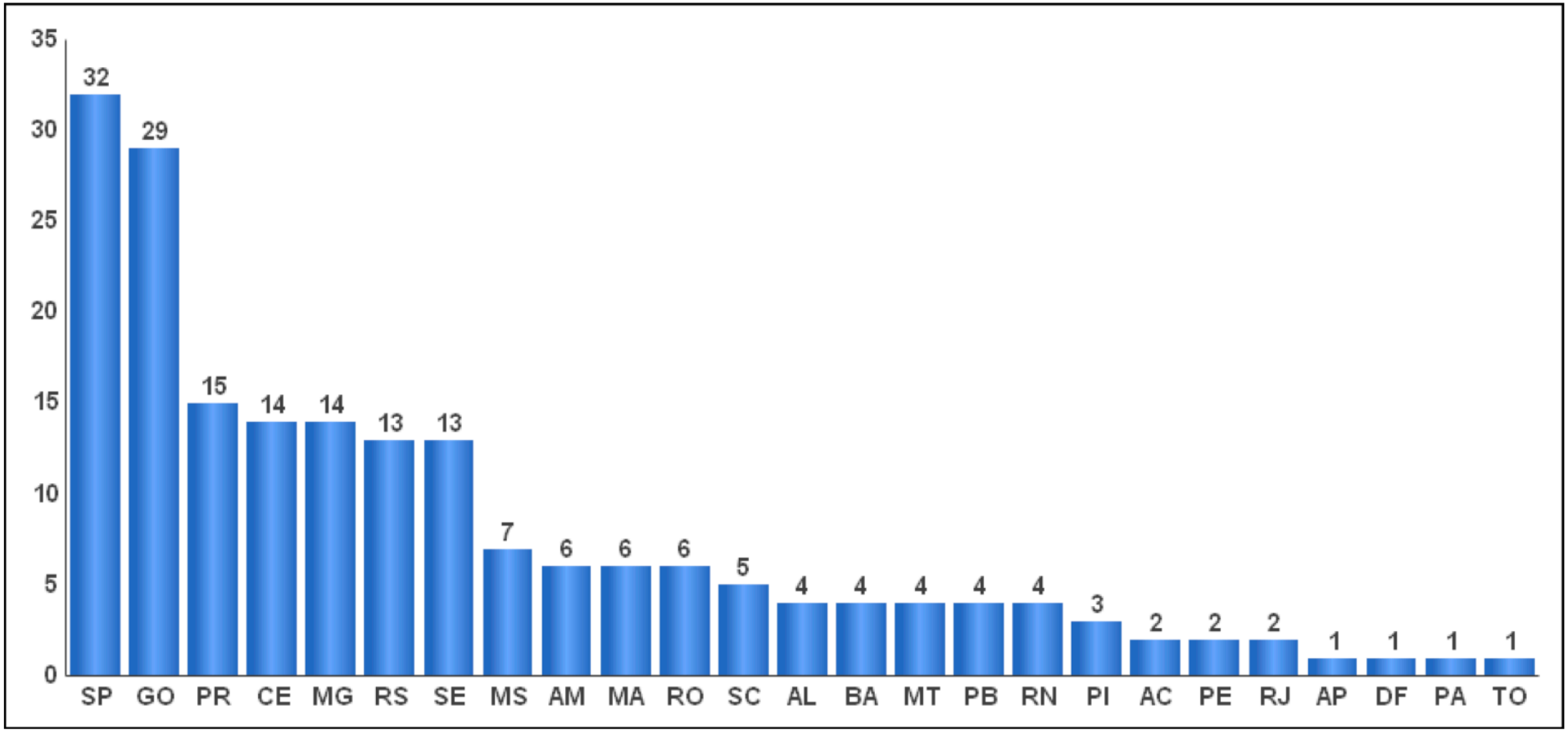
Domínios hospedando malwares



CTIRGov

Copa do Mundo (Junho e Julho 2014)

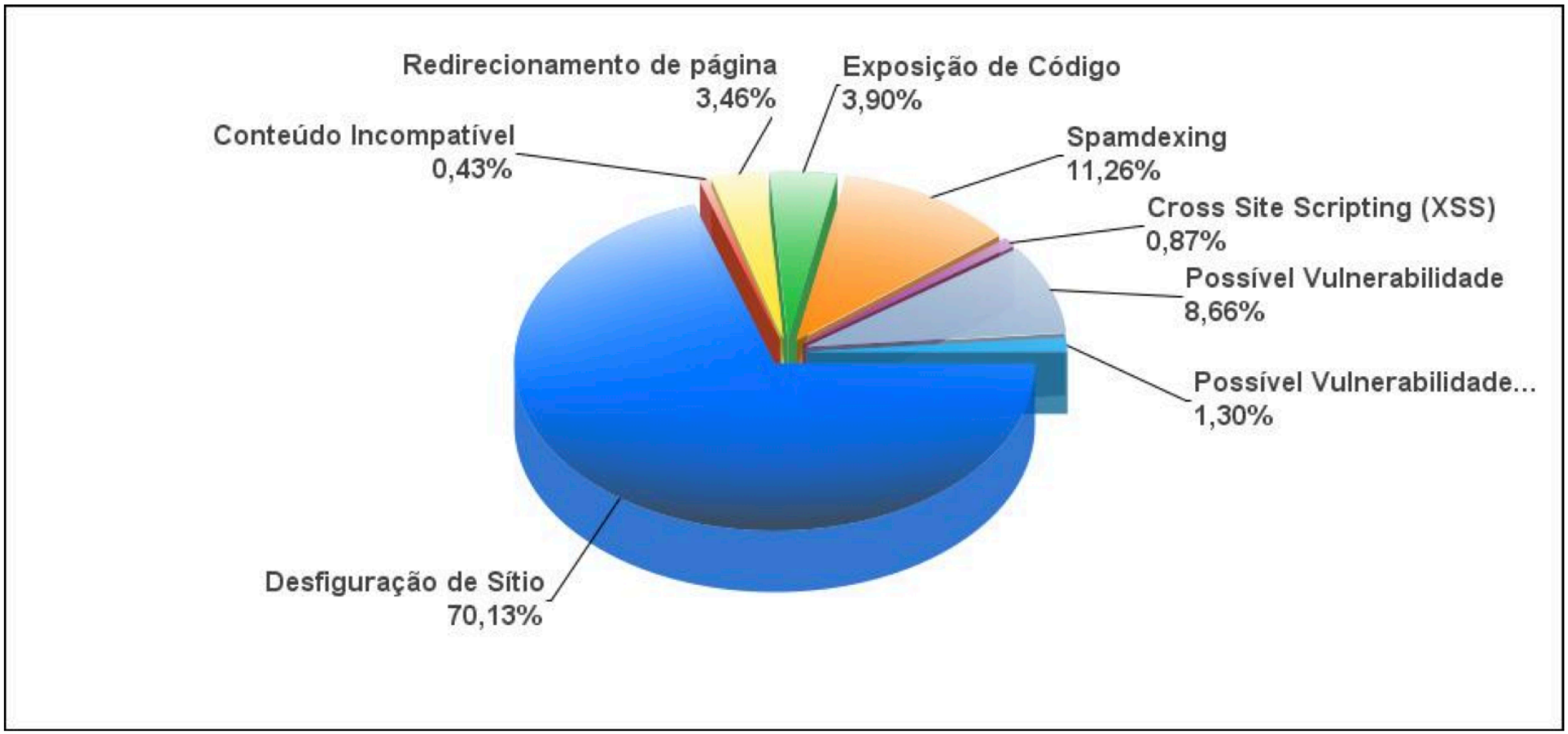
Incidentes Abuso de Sítio por Estado



CTIRGov

Copa do Mundo (Junho e Julho 2014)

Tipos de Abuso de Sítio



CTIRGov

Percepções do CTIR Gov

Aspectos Positivos

- ✓ Integração das equipes
  - ✓ Instituições e pessoas estão bem integradas;
  - ✓ Percepção das potencialidades de cada time.
- ✓ Preparação técnica
  - ✓ Conhecimentos nivelados;
  - ✓ Metodologias semelhantes.
- ✓ Pró-atividade
  - ✓ Todas as equipes foram além dos trabalhos inicialmente previstos;
  - ✓ Em algumas ocasiões, uma equipe antecipou-se à outra com o objetivo de resolver o problema.

Conclusões

Pontos principais

✓ O acompanhamento de canais de "Mídias Sociais" realizado pelas diversas instituições, tais como CDCIBER e CERT.br e empresas parceiras, repassadas a este Centro, reduziu, de forma significativa, o tempo de resposta aos incidentes de redes ocorridos nas organizações da Administração Pública;

✓Necessidade de aprimorar o acompanhamento das redes sociais, como forma de ampliação do escopo de atuação do CTIR Gov;

✓Necessidade de ações proativas e resposta imediata: "destacamos as ações imediatas, tomadas pelas equipes de segurança dos respectivos Órgãos vítimas de "Spear Phishing".

CTIR Gov

CTIR Gov

OBRIGADO!

http://www.ctir.gov.br

ctir@ctir.gov.br (notificação de incidentes)

cgtir@planalto.gov.br (assuntos diversos)

INOC-DBA: **10954*810**