Incidentes de Segurança em Redes de Governo
Cenário Atual e Desafios Futuros

2º Fórum Brasileiro de CSIRTs

São Paulo, 17/09/2013

Objetivo

Apresentar o atual cenário de incidentes de segurança em redes governamentais, destacando como o CTIR Gov trabalha para cumprir sua missão institucional e quais são os principais desafios para o futuro.

Agenda

- ✓ Ambientação
- ✓ Evolução histórica
- ✓ Cenário atual de incidentes de segurança
- ✓ Desafios para o futuro
- ✓ Conclusões

CTIR Gov

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

Ambientação

Coordenação-Geral de Tratamento de Incidentes de Redes

✓ Missão (Art.39 Port. nº 13, de agosto/2006)

- *(...) operar e manter o Centro de Tratamento de Incidentes de Redes de Computadores da Administração Pública Federal;*
- ***apoiar** órgãos e entidades da Administração Pública Federal nas atividades de tratamento de Incidentes de Segurança de Redes de computadores;*
- ***monitorar e analisar** tecnicamente os incidentes de segurança nas redes de computadores da administração pública federal; (...)*

✓ Centro de Coordenação Nacional

O CTIR Gov age como **centro de coordenação de responsabilidade nacional**, na ligação entre os envolvidos e no acompanhamento das ações de tratamento e resposta aos incidentes de segurança ocorridos na APF.

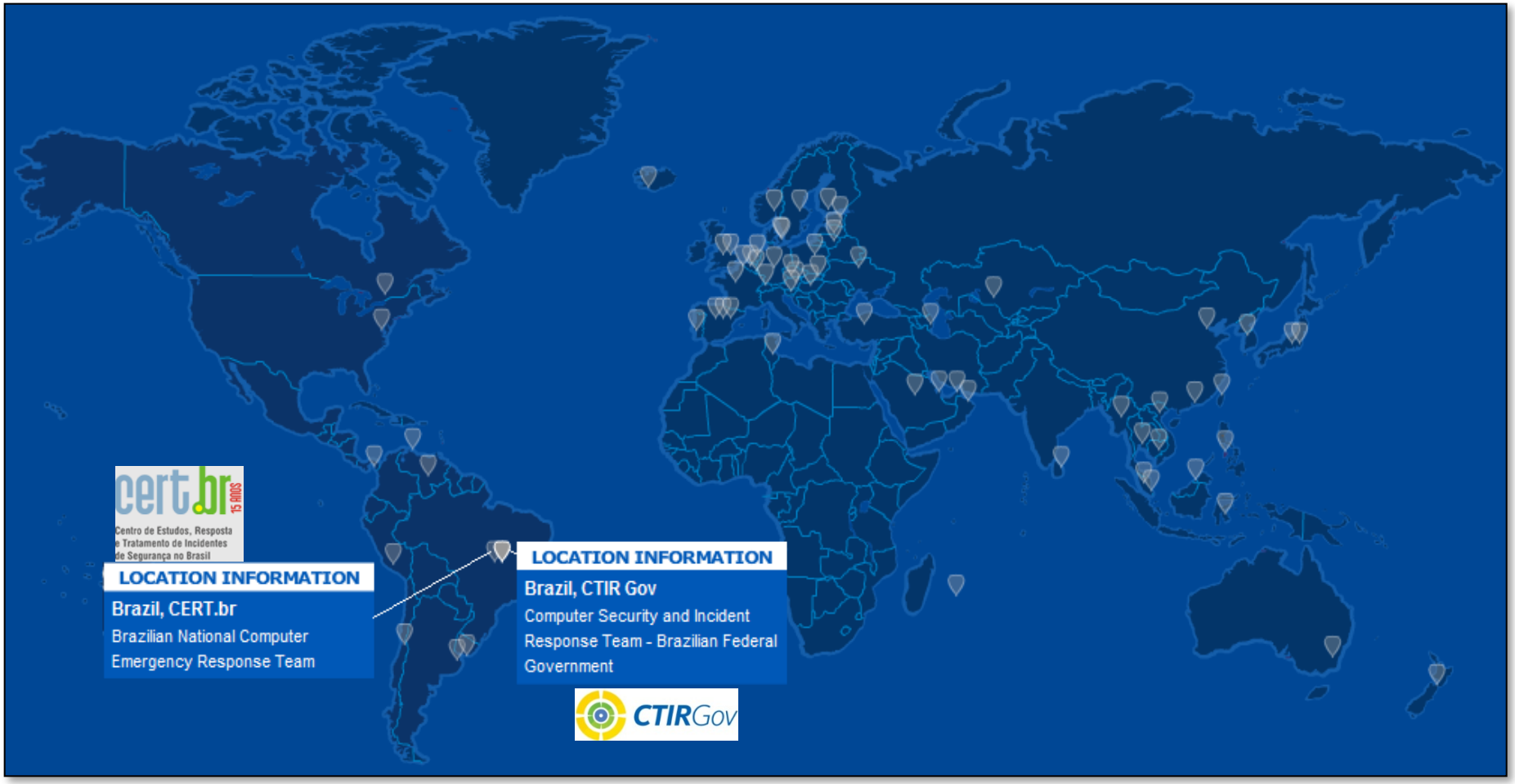
✓ Comunidade de Tratamento de Incidentes do CTIR Gov

Composta por todos os órgãos e entidades da APF direta e indireta. Em caráter excepcional e de forma colaborativa os órgãos dos Estados e Municípios, pertencentes aos domínios **“gov.br”, “jus.br”, “leg.br”, “mil.br”, “mp.br”** e outros.

CTIR Gov

Ambientação

Centros de tratamento com responsabilidade nacional



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

CTIRGov

Evolução da Abordagem

2014/15	Aumento na quantidade e complexidade dos serviços demandados.
2012/13	Ampliação do número de serviços oferecidos pelo CTIR Gov à APF e intensificação de trocas de informação com parceiros; Referência no Acórdão 1233/2012 – Tribunal de Contas da União
2010/11	Implantação e consolidação do RT (*Request Tracker*) como ferramenta para suportar o modelo de negócios do CTIR Gov
2008/09	Criação e amadurecimento do "Modelo de melhoria de qualidade baseado em processos para tratamento de incidentes de rede na APF"
2006/07	Definição das competências da CGTIR publicadas em Portaria Ministerial.
2004/05	Criação e consolidação do CTIR Gov no âmbito do GSIPR.

Cenário atual de incidentes

Incidentes por mês de criação e *status*

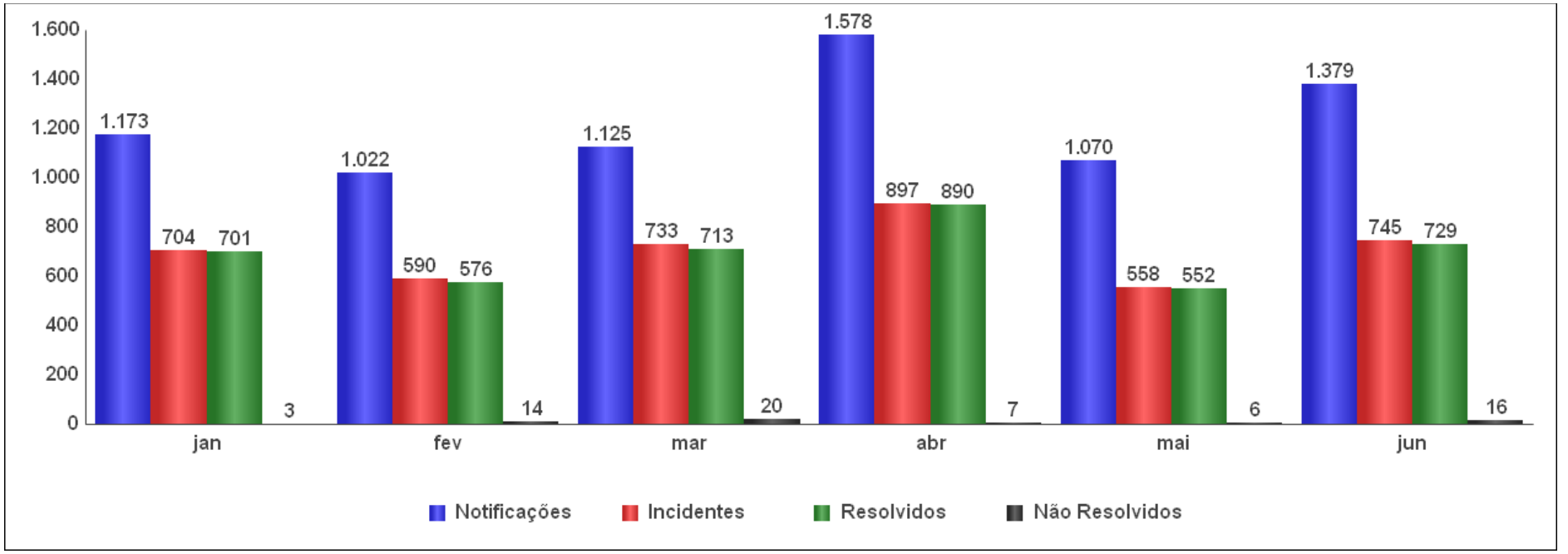


Gráfico 1 – Distribuição de notificações por *status* e mês de criação – 1S13

Cenário atual de incidentes

Incidentes por mês de criação e *status*

Mês	1º Semestre 2012	1º Semestre 2013	Variação (%)
jan	626	704	12,46
fev	550	590	7,27
mar	488	733	50,20
abr	485	897	84,95
mai	425	558	31,29
jun	477	745	56,18
Total	**3.051**	**4.227**	**38,54**

Tabela 1 – Variação no número de incidentes tratados nos primeiros semestres de 2012 e 2013

Cenário atual de incidentes

Incidentes por categoria

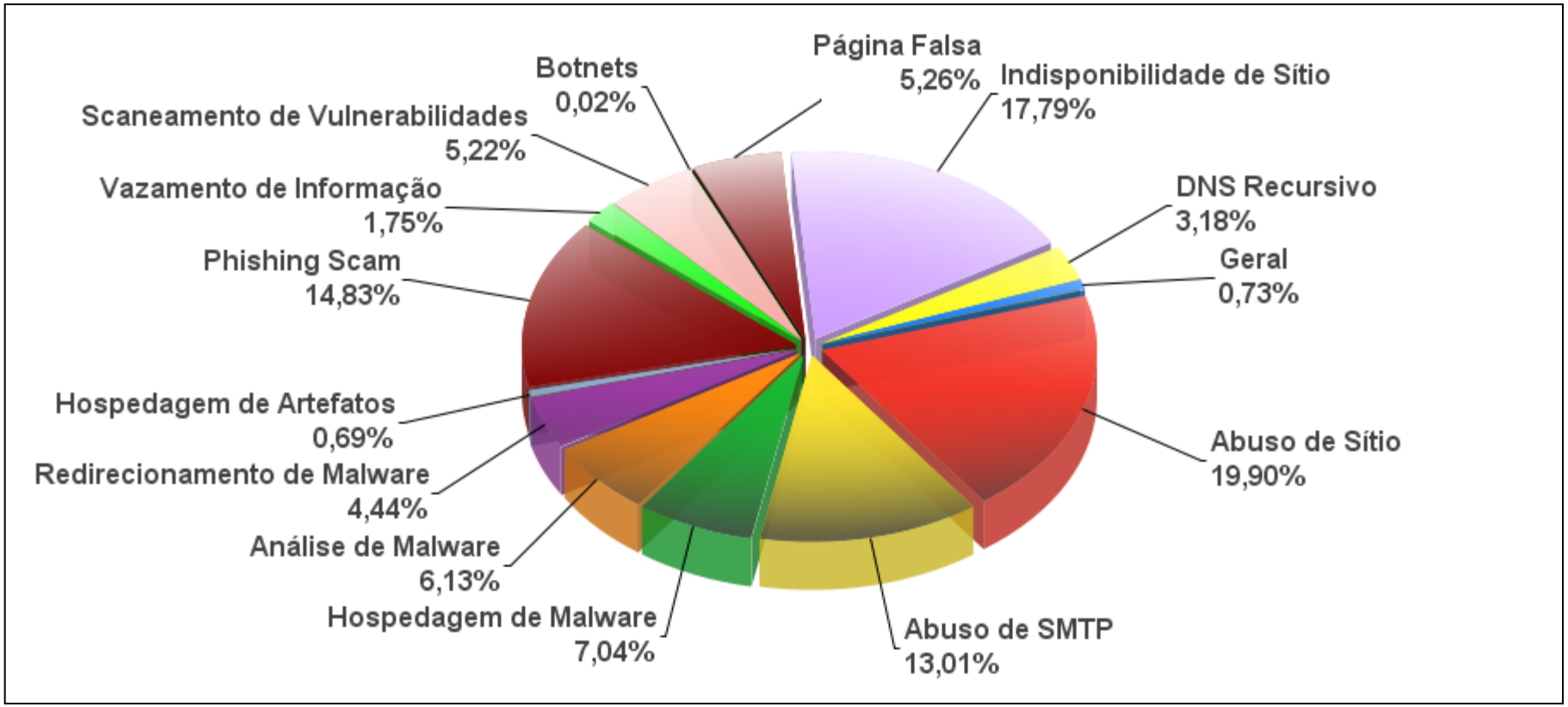


Gráfico 2 – Distribuição de incidentes por categoria – 1S13

Cenário atual de incidentes

Incidentes por categoria

Categoria	2S12	1S13	Variação (%)
Abuso de Sítio	676	896	32,54
Abuso de SMTP	428	586	36,92
Análise de Malware	236	276	16,95
Botnets	46	1	-97,83
DNS Recursivo	0	143	-
Não categorizados (Geral)	335	33	-90,15
Hospedagem de Artefatos	185	31	-83,24
Hospedagem de Malware	229	317	38,43
Indisponibilidade de Sítio	453	801	76,82
Página Falsa	383	237	-38,12
Phishing Scam	465	668	43,66
Redirecionamento de Malware	132	200	51,52
Scaneamento de Vulnerabilidades	1.111	235	-78,85
Vazamento de Informação	59	79	33,90

Tabela 2 – Variação do número de incidentes por categoria (2S12 e 1S13)

Cenário atual de incidentes

Abuso de sítios por Estado *(top 10)*

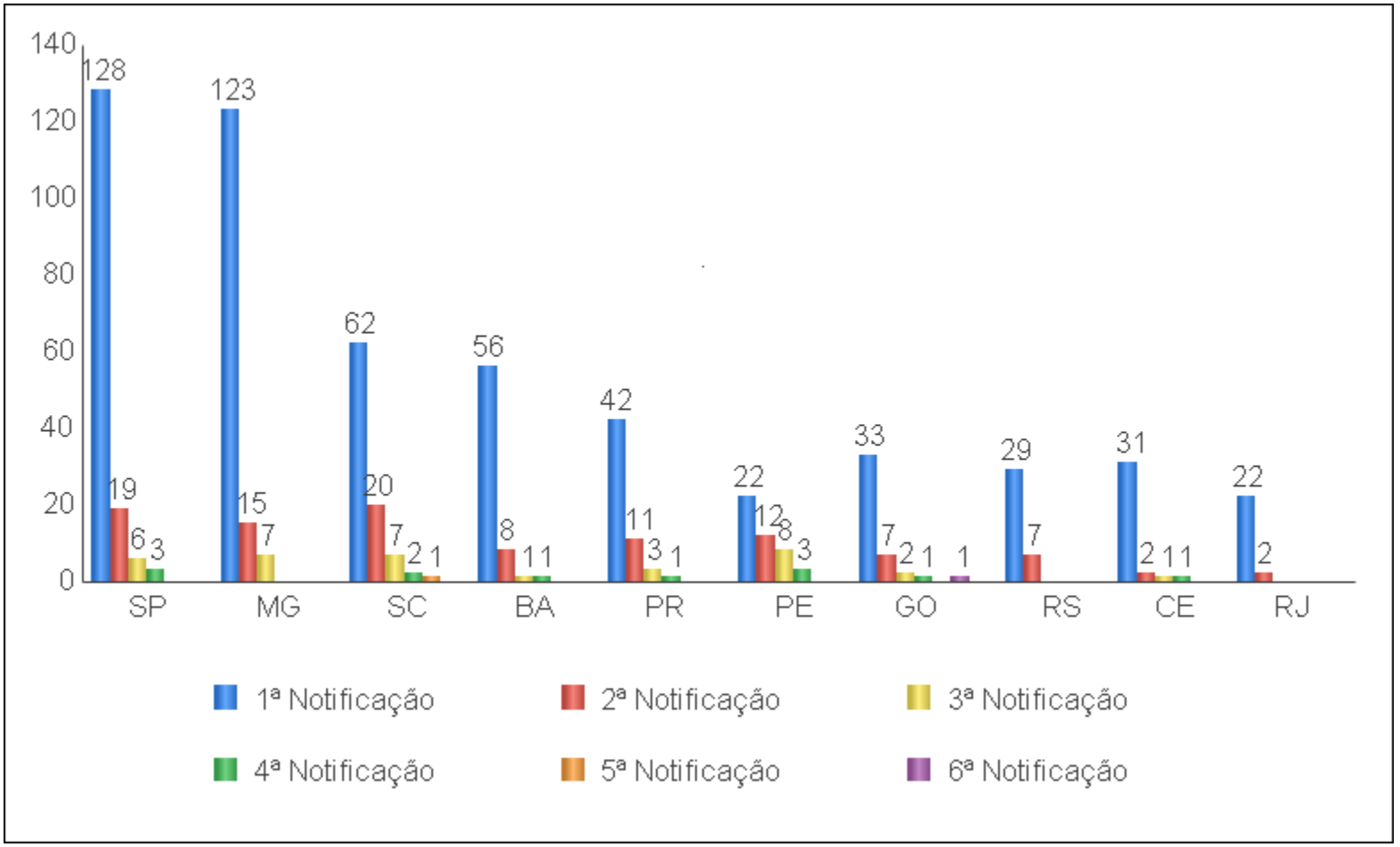


Gráfico 5 – Número de notificações de Abuso de Sítio por Estado

Cenário atual de incidentes

Tempo médio de resolução de incidentes

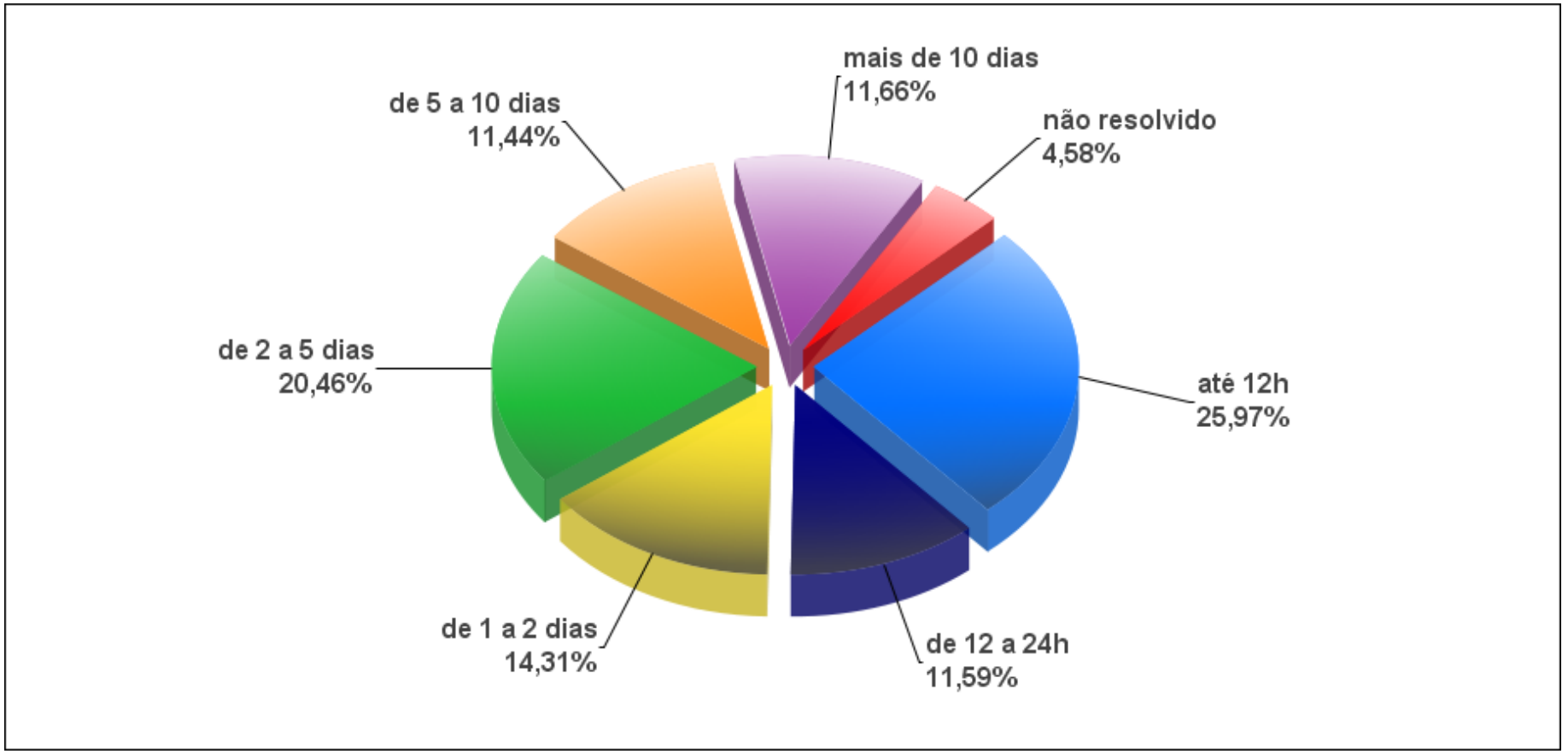


Gráfico 6 – Tempo de resolução de incidentes – 1S13

Cenário atual de incidentes

Tempo médio de resolução de incidentes

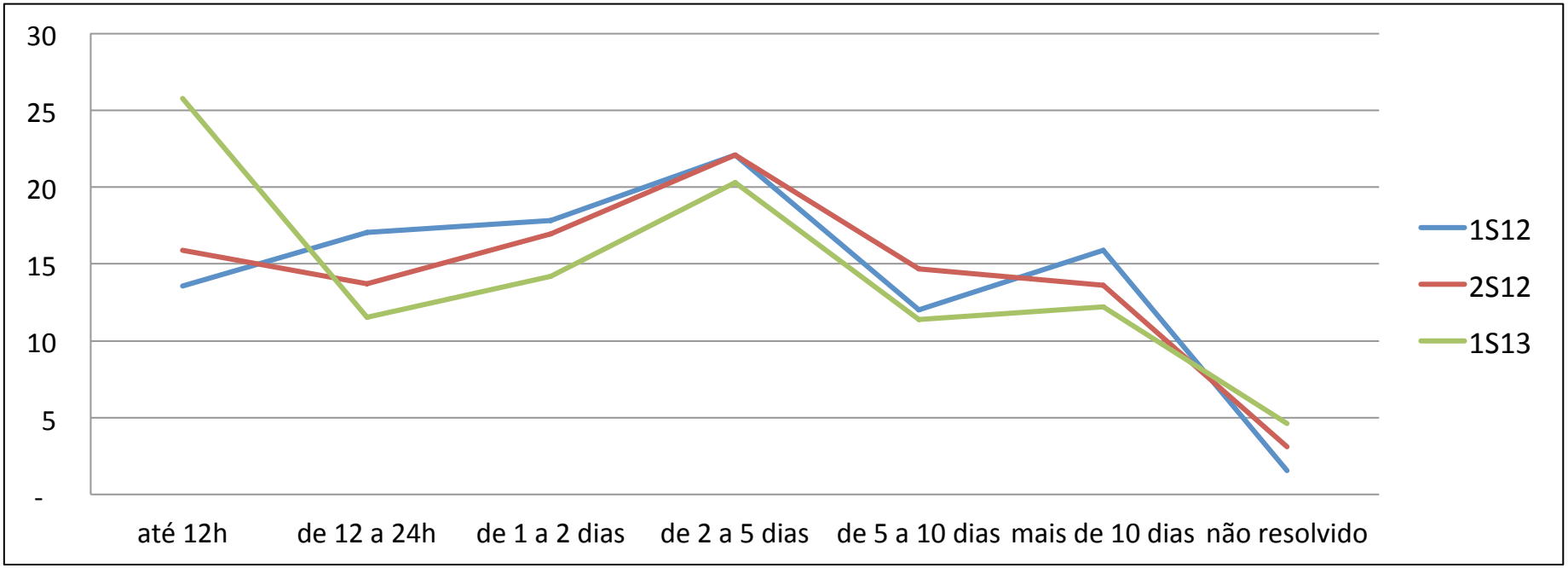


Gráfico 7 - Evolução percentual do tempo de resolução de incidentes por semestre

Desafios para o futuro

Pessoas

“If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology.”

Bruce Schneier

Desafios para o futuro

Pessoas

✓ Segurança não é produto, é processo. Quem cria, define, aperfeiçoa e segue tais processos são as **PESSOAS!**

✓ Com isso, surgem alguns desafios:

- ✓ Grande parte do trabalho de uma ETIR envolve questões **não-técnicas**. Estar atento às condições ambientais é fator crítico para o sucesso da equipe;
- ✓ A ETIR depende mais de boas **atitudes pessoais** do que de boas **ferramentas**;
- ✓ A formação de um profissional de tratamento de incidentes de rede é complexa e pode levar muito tempo. Por isso, retenha seus talentos a qualquer custo;
- ✓ O profissional completo é um mito. Possuir perfis complementares no time é de fundamental importância;
- ✓Além do conhecimento técnico, é preciso estabelecer um **código de conduta** e certificar-se de que todos os integrantes o seguem rigorosamente;
- ✓ A **reputação** de uma ETIR é o seu bem mais precioso. Ela é construída ao longo de anos, mas pode ser destruída em poucos segundos.

Desafios para o futuro

Gerenciamento dos Recursos

Carga de trabalho 

Equipe 

Produtividade 

CTIRGov

Desafios para o futuro

Ataques com características “novas”

- ✓ APT & Targetted Attacks
  - ✓Aumento na complexidade dos ataques;
  - ✓Rápida reação à contramedidas de segurança;
  - ✓Aumento de ameaças *“tailor made”* .
- ✓ Hacktivismo
  - ✓ As mudanças sociais ocorrem cada vez mais rápido;
  - ✓ “Se algo não está acontecendo, é porque você não está fazendo.” (*Thomas Friedman*, em “O mundo é plano”.)
  - ✓ Conturbações sociais resultam em aumento no número de incidentes de segurança em redes de governo.

Desafios para o futuro

Trato com a imprensa

- ✓Trato com a imprensa
  - ✓Assuntos técnicos são temas árido para a maioria dos leitores e dos profissionais de comunicação social;
  - ✓ Pequenos incidentes técnicos podem virar grandes incidentes políticos;
  - ✓ “Nada a declarar” é uma postura que contraria a transparência.

Desafios para o futuro

Métricas

“Não se gerencia o que não se mede. Não se mede o que não se define, não se define o que não se entende, ou seja, não há sucesso no que não se gerencia.”

Adaptado de *W. Edwards Deming*

CTIR Gov

Desafios para o futuro

Métricas

- ✓ De quais indicadores preciso?
- ✓ Como avaliar o desempenho de um CSIRT?
- ✓ Como definir metas para a equipe?
- ✓ Medição quantitativa oferece informação de qualidade?
- ✓ Qual impacto minhas publicações possuem na minha *constituency*?
- ✓ Minha metodologia está clara e alinhada com as melhores práticas?

Conclusões

Pontos principais

✓ O papel exercido por Centros de Coordenação Nacional de Tratamento de Incidentes não é estático. Flexibilidade e dinamismo são essenciais na condução do time;

✓ Um CSIRT é tão bom quanto suas pessoas, e não quanto suas ferramentas;

✓ Prospectar profissionais que atendam aos requisitos técnicos e comportamentais é tarefa complexa e demanda tempo; e

✓ O cenário futuro indica maior quantidade e complexidade dos incidentes de segurança. Como existem restrições ao aumento do efetivo de CSIRTs, o desafio é trabalhar com mais inteligência e automatização, sem perder jamais o foco na qualidade do serviço.

OBRIGADO!

http://www.ctir.gov.br

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

cgtir@planalto.gov.br (assuntos diversos)

INOC-DBA: **10954*810**

CGTIR: **(61) 3411-4383**