2º Colóquio CTIR Gov – AGO/2012
"Desafios e Inovações no Tratamento de Incidentes"

Data: 31 de agosto de 2012

Horário: 8h30 às 17h30

Participantes: Órgãos e entidades da APF (Ministérios, Secretarias e Empresas Públicas) e equipes de tratamento de incidentes dos Estados e Distrito Federal (Companhias estaduais de processamento de dados).

Local: Auditório do Anexo I – Palácio do Planalto – Brasília DF

Agenda:

Horário	Evento / Palestra	Órgão	Palestrante / Responsável
8h30 às 9h	Recepção / Credenciamento	CTIR Gov	Integrantes do CTIR Gov / DSIC
9h às 9h20	Abertura do evento (1)	DSIC	Raphael Mandarino Junior
9h20 às 10h10	Tratamento de incidentes de segurança na APF (2)	CTIR Gov	Integrantes do CTIR Gov
10h10 às 10h30	Intervalo – Café	--	--
10h30 às 11h10	Análise de malware – *Ciberis* (3)	CTIR Gov / Laboratório	Vitor Monte Afonso
11h10 às 12h	Desafios no tratamento de incidentes de segurança (4)	CERT.br	Klaus Steding-Jessen
12h às 14h	Intervalo – Almoço	--	--
14h às 14h50	Projeto "Oráculo" (5)	MJ / DPF	Ivo de Carvalho Peixinho
14h50 às 15h40	Os desafios do CSIRT do Governo do Estado de São Paulo (6)	PRODESP	Fábio Raymundo Neves Fernandes
15h40 às 16h	Intervalo – Café	--	--
16h às 16h50	Gestão de Incidentes (7)	CTIR Gov	Integrantes do CTIR Gov
16h50 às 17h30	Debates	Todos os presentes	--

(1) ***Abertura do Evento***: Boas vindas aos órgãos participantes; ações recentes do Departamento de Segurança da Informação e Comunicações na área da segurança da informação e comunicações.

(2) ***Tratamento de Incidentes de Segurança na APF****:* Aperfeiçoamento dos processos de tratamento de incidentes; novos mecanismos de detecção; estudos de caso (*Spamdexing, Phishing e* análise de *malwares*); estatísticas do CTIR Gov; análise de tendências; problemas recorrentes.

(3) ***Análise de malware****:* Apresentação do projeto de análise de *malwares* - *Ciberis (C5B3R15)*.

(4) ***Desafios no tratamento de incidentes***: Apresentação dos desafios no tratamento de incidentes de segurança pelo CERT.br.

(5) ***Projeto "Oráculo"***: Apresentação do Projeto Oráculo, que visa à criação de uma Base Nacional de Segurança Cibernética (BNSC). Através desse projeto será possível coletar informações de incidentes de segurança da APF através das ETIR, informações das bases de dados do DPF, além de informações em fontes abertas, incluindo informações na *deep web.*

(6) **Os desafios do CSIRT-SP**: Histórico e estrutura do CSIRT-SP; ações do Governo de São Paulo para combater a onda de ataques crescente; estatísticas, resumo e exemplos das principais ocorrências; dificuldades e desafios enfrentados no segmento governamental; participação no Consórcio Brasileiro de Honeypots (CERT-BR) e Honeynets (CTI-Campinas); parcerias com outros grupos especiais; ferramentas desenvolvidas internamente para atender ao CSIRT; ferramentas de Forense Digital para apoio na resposta a incidentes.

(7) ***Gestão de Incidentes***: Aperfeiçoamento dos processos de gestão de incidentes do CTIR Gov, baseado na ferramenta *Request Tracker* (RT).