# Roteiro

**1 - IRREGULARIDADES NAS ELEIÇOES 2012**

**2 - BREVE RELATO SOBRE A PREPARAÇÃO DAS URNAS 2012 – SMARTMATIC**

**3 - IRREGULARIDADES ENCONTRADAS NA ETAPA DE DESENVOLVIMENTO E COMPILAÇÃO DOS PROGRAMAS 2014**

**4 - EMPRESA RESPONSAVEL PELA PREPARAÇÃO DO PLEITO EM 2014**

# Excertos do Processo 163.24.2012.6.160157

## RESUMO

Uma versão adulterada do programa *hotswap* teve testes iniciados na 157ª Zona Eleitoral de Londrina em 27/08/2012, conforme dados do arquivo de fiscalização (log) do sistema GEDAI gerados no respectivo cartório:

**27/08/2012 13:31:51** info Abertura do GEDAI-UE
**27/08/2012 13:31:51** info Usuario: 091874830612 | Perfil: 0 | UF: PR
**27/08/2012 13:31:51** info Verificação de Assinatura | Envelope: M:/Aplic/Ele2012/GEDAIUE/gedai-ue.vst
**27/08/2012 13:31:51** info Arquivo de URIs atualizado a partir de 'http://uri-ele.tse.jus.br:80/URLs/producao/uris-sistemas-eleitorais-pr-oficial.properties'.
**27/08/2012 13:31:53** info Verificação de Assinatura | Envelope: M:/Aplic/Ele2012/GEDAIUE/app.ini.vsc .....
**27/08/2012 13:31:53** info Início da verificação do serviço HotSwapFlash
**27/08/2012 13:31:53** info Serviço HotSwapFlash, versão 1.9.9.0, em execução
**27/08/2012 13:31:53** alerta Versão incompatível do HotSwapFlash. Executando [1.9.9.0], mas GEDAI-UE requer [1.9.9.3].
**27/08/2012 13:32:17** info Fechamento do GEDAI-UE
**28/08/2012 14:47:29** info Abertura do GEDAI-EU

# Excertos do Processo 163.24.2012.6.160157

**RESUMO**

No dia 28/08/2012, no mesmo computador do cartório eleitoral da 157ª Zona, nova tentativa de inserção do programa adulterado – como se fosse uma versão oficial – foi tentada. Novamente sem êxito:

**28/08/2012 14:47:31** info Verificação de Assinatura | Envelope: M:/Aplic/Ele2012/GEDAIUE/uenux/avpart.vst
**28/08/2012 14:47:31** info Início da verificação do serviço HotSwapFlash
**28/08/2012 14:47:31** info ServiçoHotSwapFlash, versão 1.9.9.0, em execução.
**28/08/2012 14:47:31** alerta Versão incompatível do HotSwapFlash. Executando [1.9.9.0], mas GEDAI-UE requer [1.9.9.3].
**28/08/2012 14:47:36** info Fechamento do GEDAI-UE
**28/08/2012 14:47:57** info Abertura do GEDAI-EU

# Excertos do Processo 163.24.2012.6.160157

**RESUMO**

Já no dia 21/09/2012, o programa adulterado estava funcionalmente adaptado ao sistema oficial das eleições. Embora ainda gerando alertas sobre a adulteração, conseguiu, enfim, ser verificado como um programa oficial, ...

**21/09/2012 15:15:02** info Início da verificação do serviço HotSwapFlash
**21/09/2012 15:15:02** info Serviço HotSwapFlash, versão 1.9.9.0, em execução.
**21/09/2012 15:15:02** alerta Versão incompatível do HotSwapFlash. Executando [1.9.9.0], mas GEDAI-UE requer [1.9.9.3].
**21/09/2012 15:15:53** info Processo eleitoral registrado: 00001 - Eleições Municipais 2012
**21/09/2012 15:15:53** info Pacote 'o00001pr-cp.jez' (versão '201208271452') importado.

# Excertos do Processo 163.24.2012.6.160157

**RESUMO**

Na cerimonia de Geração de Midias o programa rodou normalmente, como se fosse oficial, mas o alerta de irregularidade permaneceu

*24/09/2012 08:51:20 info Início da verificação do serviço HotSwapFlash*

*24/09/2012 08:51:20 info Serviço HotSwapFlash, versão 1.9.9.0, em execução.*

***24/09/2012 08:51:20 alerta Versão incompatível do HotSwapFlash. Executando [1.9.9.0], mas GEDAI-UE requer [1.9.9.3].***

*24/09/2012 08:54:03 info Pacote 'o00047pr76678-ca.jez' (versão '201209211536') importado.*

**SMARTIMATIC INTERNATIONAL CORPORATION**
INTEGRANTE CONSORCIO ESF – FORMADO 13/07/2012
NIRE 3550070232-1 **REGISTRO JUCESP DE 25/10/2012** – art. 278/ 279 Lei 6.404/76

**1 -** LICITAÇÃO 42/2012 – CONTRATO 80/2012 **assinado em 17/07/2015** Objeto - contratação de serviços de exercitação das urnas eletrônicas que incluía recepção de mídias e transmissão de boletins de urna, via sistema de apuração do TSE. Vencedor: SMARTMATIC Brasil Ltda ENGETEC Tecnologia S.A. e FIXTI Soluções em Tecnologia da Informação Ltda

**1.1. – Primeiro Termo Aditivo 17/09/2012**

Nesse aditivo foi incluída no contrato 80/2012, a empresa **SMARTMATIC INTERNATIONAL CORPORATION,** embora, conforme documentação disponibilizada nos sites de transparência do TSE, ela não tenha participado do processo de licitação.
Ela permaneceu no contrato até o ultimo termo aditivo

# Votação no Brasil: fases do processo

## 1. Desenvolvimento

**TSE** Programação

ABIN, STI, Módulo, etc:
*UEnix, GEDAI, SIS,...*

Apresentação dos programas
180 dias antes da eleição

Cerimônia de Compilação,
Assinatura e Lacração
80.000 progs, 26/08 a 4/09

## 2. Preparação: Geração de Mídias

**TREs** Distribuição e Instalações iniciais


Instalação de programas em equipamentos da JE

Gera Mídias: a)Carga b)Votação c)Resultados d)ADH

## 3. Carga: Inseminação das Urnas

**TREs e Cartórios Eleitorais** Instalações finalis e Configurações

Instalação de mídias e programas em Urnas

Lacração física e elaboração de Ata

## 4. Votação e Apuração


## 5. Totalização




## 6. Divulgação

**Tribunais**


Linha divisória
obscuridade | transparência

**Fiscalização:**

Lisura do pleito depende *totalmente* da honestidade dos programas e das empresas envolvidas na operacionalização dos processos.

## ELEIÇÕES 2014 - PROGRAMA *INSERATOR CPP*

Na analise do codigo fonte dos programas das eleições 2014 foi encontrado no projeto SIS, o programa de nome “programaInserator.cpp” , isolado do resto do SIS (não é chamado por nenhum outro componente do sistema) que é executado a partir da digitação de um comando por um operador que conheça sua função. Seu código-fonte, simples, descrevia apenas uma função de inserir (dai o nome) uma par chaves criptográficas ofuscadas por uma senha simples e constante, em qualquer base de dados que o computador tiver acesso, por ex.: no banco de chaves criptográficas válidas. O risco que se apresenta, é que além de proteger de forma fraca as chaves "ofuscadas", o comando invisível pode incluir no sistema, chaves de assinatura digital que passarão a ser aceitas pelos demais sistemas de verificação

**JUSTIFICATIVA TSE:** *Essa Classe MiniCA era utilizada para criação de uma Mini Certification Autority, utilizada até as eleições de 2004 como geradora de certificados para o TSE. Em 2006 já começou a utilização de certificados ICP. A referida classe apesar de estar em desuso desde 2004 se encontra ainda na sala de lacração pela necessidade de utilização dos leitores binários em diversos outros projetos. Não é mais utilizada para manipulação de certificados.*

1 – O PROGRAMA NÃO ESTAVA NA SALA DE APRESENTAÇÃO E SIM NO CODIGO FONTE, JUNTO COM OS DEMAIS PROGRAMAS DAS ELEIÇOES 2014

2 – NÃO CONSTA NA TABELA DE RESUMOS CRIPTOGRAFICOS (HASH)

3 – NÃO SE TRATA DE MERA BIBLIOTECA É UM PROGRAMA EXECUTAVEL QUE PODE SER ACESSADO POR COMANDO EM TECLADO

4 – OS LEITORES BINARIOS NÃO FAZIAM USO DE FUNCIONALIDADES DA CLASSE DE PROGRAMAS ONDE ESTAVA O INSERATOR CUJO ÚNICO METODO CONTIDO NA CLASSE É *obterChaveSimetricaCA()*.

**INTERNET ACESSIVEL DURANTE PROCEDIMENTO DE GERAÇÃO DE MIDIAS**

Representante de partido solicitou que fossem realizados procedimentos de geração de midias em computador conetado e nao conetactado a internet

TSE confirma o teste: *Em 2/9/2014, foi realizada a apresentação do GEDAI-UE e software da urna. No GEDAI-UE houve geração de mídias (flashes e MRs) com e sem conexão com a Internet, visualização dos candidatos e visualização do log*.

RESULTADO: Não existe nenhuma trava do sistema para evitar que o procedimento de geração de midias seja protegido em computadores conectados a rede mundial de computadores.

# Vulnerabilidades encontradas

Fonte: www.....

PARTIDO DEMOCRÁTICO TRABALHISTA
PDT – DIRETÓRIO NACIONAL

COPIA

EXCELENTÍSSIMO SENHOR MINISTRO DIAS TOFFOLI – RELATOR DAS ELEIÇÕES DE 2014 NO COLENDO TRIBUNAL SUPERIOR ELEITORAL

Tribunal Superior Eleitoral
PROTOCOLO JUDICIARIO
23.891/2014 Cópia.
04/09/2014-16:16

**PARTIDO DEMOCRÁTICO TRABALHISTA – PDT** – por sua advogada e representante credenciada para analisar os códigos-fonte e participar da Cerimonia de Homologação e Lacração dos programas a serem usados nas eleições 2014 vem, com todo respeito e acato, informar que:

Nos exames de código fonte dos programas apresentados para auditoria do sistema de votação informatizada no TSE, realizado conforme preve a Resolução TSE nº 23.397, artigo 1º, fatos relevantes foram encontrados a seguir articulados.

**I – VULNERABILIDADES**

1 - Vulnerabilidade no gerador de mídias de ajuste de data e hora:

No projeto GEDAI, o programa geradoradh.cpp tem sua inicialização feita com uma chamada de função srand(time(null)), fato que constitui vulnerabilidade, por redução drástica de entropia ao efeito protetor pretendido pelo desenho deste programa, que seria o de impedir a geração indiscriminada de mídias de ajuste de data e hora para as Urnas Eletrônicas.

Exatamente a mesma vulnerabilidade encontrada pela equipe vencedora nos Testes Públicos de segurança de 2012 com respeito ao embaralhamento do RDV, permanece, portanto, também para a geração de mídias de ajuste de data e hora.

# Vulnerabilidades encontradas

2- Vulnerabilidade no driver de partições minix no kernel Linux das Urnas Eletrônicas.

No projeto UEnux, no arquivo ueminixkey.h, há um vetor de ofuscamento e uma chave criptográfica às claras, fixas e acessíveis por leitura direta. Tal chave se destina a cifrar partições minix, conforme invocada a partir do código em ueminix.c, como por exemplo nas mídias capazes de inicializar as Urnas Eletrônicas de modelo 2009 ou posterior, tais como os flashes de carga oficiais.

Tal arquitetura para inicialização criptográfica torna inócuos os mecanismos de controle e proteção a esses novos modelos, pois, mediante simples acesso a uma mídia de inicialização oficial, será possível gerar outras de diferente teor.

3 - Vulnerabilidade na classe MiniCA.cpp.

Essa classe do projeto SIS foi desenvolvida contendo um - único método – obterChaveSimetricaCA() – cuja única funcionalidade é retornar uma chave criptográfica simétrica ofuscada, porém fixa e embutida, o que anula qualquer efeito pretendível com o ofuscamento.

O programa programaInserator.cpp é o único local do código do projeto SIS que invoca tal classe, de forma tal que sua existência não revela propósito claro, pois não é literalmente chamado por nenhum outro programa desse projeto.

Trata-se de um programa independente e separado, que só pode ser diretamente invocado através de digitação no teclado – linha de comando – por um operador do SIS que conheça sua existência, seja no TSE ou nos TREs. Ele gera um script SQL (executável por banco de dados) capaz de inserir chaves de assinatura e verificação digitais em bancos de dados indeterminados.

Consultados por volta das 15h do dia 3 de setembro, representantes do fornecedor do sistema SIS, presentes à cerimônia de apresentação no TSE, não souberam explicar nem a origem do programa nem a finalidade da classe programaInserator – cujo formato e contexto significam que só pode ser acionado pelo operador no teclado –, de potencial impacto na higidez da verificação automática de programas.

# Vulnerabilidades encontradas

II – Conexão Internet

1 - Noutro ponto, a signatária solicitou que fossem demonstrados os procedimentos de geração de midias, usando um computador conectado à Internet. A demonstração foi realizada na sala de apresentação dos programas em 02.09.2014. Foram realizados todos os atos dos procedimentos, desde a geração de mídias até o final da votação.

Constatou-se, nessa oportunidade, que o computador que gera mídias para eleições oficiais pode estar conectado à rede mundial Internet. Essa conexão não é bloqueada, nem o sistema emite qualquer aviso da conseqüente exposição a riscos, o que a torna imperceptível a potencialização agravada por acesso externo das vulnerabilidades descritas nos itens 1 e 3 acima, com possibilidade de instalação, validação e uso de programas não oficiais.

Por todo o exposto, tem a presente o objetivo de noticiar a essa Colenda Corte as vulnerabilidades encontradas, para as providencias que o caso requer.

Brasília, 05 de setembro de 2014.

Pp

MARIA APARECIDA ROCHA CORTIZ
ADVOGADA OAB.SP 147.214

Praça Joao Mendes, 42 – Conjunto 155
Centro – SP – CEP 01501-000

Fonte: www.....


Nenhum partido que estava participando da cerimonia assinou digitalmente os programas das eleiçoes 2014

# Empresa Smartmatic

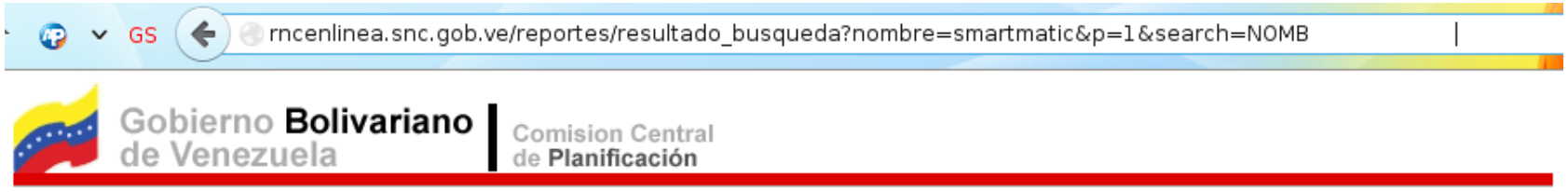
## CONCEITO INTERNACIONAL

### INTERDIÇÕES

- A empresa Smartmatic foi constituída na Venezuela, onde atuou na eleição de 2006, mas naquele pais suas ramificações encontram-se atualmente suspensas das atividades eleitorais por prática de irregularidades, conforme dados do portal oficial de informações empresariais do governo da Venezuela (imagem seguinte)
- Segundo outras informações midiáticas, disponíveis na internet, o mesmo ocorre nas Filipinas (imagem adiante).
- Estando suspensa como esta na Venezuela e nas Filipinas por irregularidades em contratos com objeto similar, a empresa Smartimatic, pelo principio da isonomia, estaria proibida de licitar no Brasil.

# Empresa Smartmatic

## III - CONCEITO INTERNACIONAL




### Resultado de la Busqueda de Empresas

| RIF. | Nombre o Razón Social | Status Actual en el RNC | Nivel FEC | Persona Contacto Directo | Telefonos |
|---|---|---|---|---|---|
| J296556873 | SMARTMATIC DEPLOYMENT CORPORATION | **EXTRANJERA, SIN DOMICILIO NI FILIAL EN VENEZUELA** ( exceptuada de la CALIFICACIÓN por el Registro Nacional de Contratistas de conformidad con el Articulo 49, numerales 6 y 7.) | | Argishaiel Briceño | 0212-7062500 |
| J298274093 | SMARTMATIC INTERNATIONAL CORPORATION | **EXTRANJERA, SIN DOMICILIO NI FILIAL EN VENEZUELA** ( exceptuada de la CALIFICACIÓN por el Registro Nacional de Contratistas de conformidad con el Articulo 49, numerales 6 y 7.) | | Argishaiel Briceño | 0212-02127062500 |
| J304879970 | SMARTMATIC LABS, C.A. | **EN PROCESO DE DESCAPITALIZACION** ( INHABILITADA para contratar con el Estado por encontrarse en proceso de DESCAPITALIZACION según el Artículo 264 del Código de Comercio Venezolano.) | NIVEL VIII | Milagros Alfonzo | 02127626360 Ext. 104 |
| J298794550 | SMARTMATIC LATAM CORPORATION | **EXTRANJERA, SIN DOMICILIO NI FILIAL EN VENEZUELA** ( exceptuada de la CALIFICACIÓN por el Registro Nacional de Contratistas de conformidad con el Articulo 49, numerales 6 y 7.) | | Argishaiel Briceño | 0424-136-78-37 |
| J304116128 | TECNOLOGÍA SMARTMATIC DE VENEZUELA, C.A. | **REGISTRADA NO ACTUALIZADA** ( INHABILITADA para contratar con el Estado de conformidad con el Articulo 50 LCP) | NIVEL XXVII | Chandler Molina | (0212) 706-2500 Ext: 5143 |

# Empresa Smartmatic

## III - CONCEITO INTERNACIONAL

www.manilatimes.net/smartmatic-faces-total-ban-in-ph-election-watchdog/166551/

The Manila Times

Home | News | Opinion | Regions | World | Sports | Business | Special Reports

Fast Times | Tech Times | Life & Times | Show Times | Expats & Diplomats | Hi! Society

Fri, Mar 13, 2015, 1:18 AM PHT

Curtir 211.982 pessoas curtiram isso. Cadastre-se para ver

Loadi

**Smartmatic faces total ban in PH – election watchdog**

*March 1, 2015 10:23 pm*

***by WILLIAM B. DEPASUPIL***

Curtir 21 Share Tweet

CONTROVERSIAL voting machine supplier Smartmatic Corp. will be banned from doing business with the Commission on Elections (Comelec) when the Supreme Court (SC) accepts the evidence showing it lied to the court to bag the Precinct Count Optical Scan (PCOS) machine supply contract, the poll watchdog said.

**AUSENCIA DE AUTORIZAÇÃO PARA ATUAR NO BRASIL**

artigo 1134 CC *A sociedade estrangeira, qualquer que seja o seu objeto, não pode, sem autorização do Poder Executivo, funcionar no País, ainda que por estabelecimentos subordinados, (...)*

artigo 28 V da Lei 8666/93 *V - decreto de autorização, em se tratando de empresa ou sociedade estrangeira em funcionamento no País, e ato de registro ou autorização para funcionamento expedido pelo órgão competente, quando a atividade assim o exigir*

**OFENSA A SOBERANIA NACIONAL**

Conforme jurisprudência do TSE trata-se de atividade vedada a estrangeiros (processo nº 185520.2014.6000.0000 Relatada pelo Exmo Sr Ministro Dias Tofolli (...)
*Entretanto os sistemas e programas utilizados nas urnas, de propriedade da Justiça Eleitoral, não podem ter seu acesso franqueado a pessoas fisicas ou juridicas estrangeiras ou vinculadas a paises ou entidades internacionais Tal providencia implicaria ofensa á soberania nacional um dos fundamentos da Republica Federativa do Brasil (...)*

# Legislação Brasileira

## SISTEMA ELEITORAL BRASILEIRO

- **CONCENTRAÇÃO PODERES** – gerou processo inauditável, obscuro, ultrapassado, caro e pior impossível de ser fiscalizado.

- **IMPOSSIBILIDADE DE CONFERENCIA** – nao há como garantir que a vitoria é legitima ou a derrota é oficial.

- **7 FASES IMPOSSIVEIS DE SEREM FISCALIZADAS** (analise codigo fonte, geração de midias, carga das urnas, votação, apuração, totalização e divulgação resultados)