Análise Técnica de Laudo Pericial

Laudo 106/2009-SETEC/SR/DPF/TO

Referente ao exame de urnas eletrônicas
usadas no município de Monte do Carmo, TO,
na eleição municipal de 2008.

0. Introdução

O laudo sob análise foi datado no dia 01 de abril de 2009 e assinado por três peritos da Polícia Federal de Tocantins, que analisaram 24 urnas eletrônicas usadas nas eleições de 2008 no município de Monte do Carmo, TO, para responder a 5 quesitos sobre a confiabilidade destes equipamentos, em atendimento a ordem judicial.

O laudo contém 9 páginas. Os 5 quesitos que se propõe a responder são apresentados logo na introdução na primeira página. A seguir o laudo contém os seguintes itens ou capítulos:

1. Avaliação do Laudo

O laudo se desenvolve com superficialidade de detalhamento e com lacunas essenciais.

Tais superficialidade e lacunas, em nosso entender, conforme abaixo fundamentado, comprometem definitivamente sua conclusividade, presumida no item V, em referência a um possível valor probante alusivo a seu caráter técnico.

Conforme descrito no item IV-EXAMES (pág.4 do laudo) foram feitos os seguintes exames periciais *apenas*:

a) verificação de um dos lacres das urnas;

b) verificação de conteúdo digital nos cartões de memória pelo cálculo das resumos SHA1 dos arquivos encontrados nas flash cards internas (FI) das urnas;

c) verificação, sem detalhamento, do conteúdo dos arquivos de log das urnas recebidos do

TRE.

Quanto às lacunas, uma leitura do laudo constata que:

1- não foram verificados nem analisados:

a) Se os processos de carga e lacração das urnas analisadas atenderam às especificações de procedimentos de segurança previstos por legislação vigente, ou se contém, nas atas e demais documentos comprobatórios, algum indício de irregularidade procedimental ou impropriedade técnica, em relação aos ditos procedimentos de segurança previstos por legislação vigente.

b) Se os dados das Tabelas de Correspondências Esperadas e Efetivadas correspondem exatamente aos respectivos dados encontráveis nas urnas.

c) Se os arquivos de dados de auditoria (BU, RDV e LOG) recepcionados pelo sistema de totalização produzem resumos digitais iguais aos resumos encontrados na tabela correspondente, ou ainda, se os dados neles contidos coincidem com os das cópias destes arquivos que deveriam ser encontrados nas flash cards internas e externas, nas urnas usadas na votação ou numa amostra destas.

d) Se os Boletins de Urna (BU) impressos contém dados coincidentes com os dos BU digitais, nas urnas usadas na votação ou numa amostra destas.

e) se os totais de votos registrados nos três tipos de arquivos de auditoria (BU, RDV e LOG), onde acessíveis, coincidem entre si, em cada urna usada na votação ou numa amostra destas.

f) se os conteúdos das flash externas (de votação) e das flash internas de cada urna coincidem, onde cabível.

g) Se as áreas livres dos flash cards nas urnas continham ou não partes de arquivos porventura apagados, em algum momento entre a carga da urna e a varredura das flashes. Arquivos apagados por comandos regulares do sistema operacional deixam vestígios, inclusive, com certos *filesystems* na tabela de alocação de arquivos (ver e.

2- Não foram completos nem conducentes a respostas conclusivas:

a) A análise dos logs: superficial e nenhum detalhamento foi apresentado. Dos detalhes omitidos, alguns são essenciais para qualquer resposta conclusiva ao segundo quesito respondido.

b) A análise dos lacres: verificado apenas um dos lacres. Os lacres cuja verificação foi omitida são essenciais para qualquer resposta conclusiva do segundo, quarto e quinto quesitos respondidos.

c) A consideração de interesses: não consta do laudo que a parte demandante estivesse representada, através de um assistente de perícia durante a mesma, ou que esta tivesse sido notificada do horário e local em que tal perícia seria conduzida, para lá fazer-se representar.

Assim, pode-se afirmar que os dados colhidos pela perícia omitem informações pertinentes e essenciais à fundamentação das respostas oferecidas aos quesitos levantados, afirmação que pode

ser melhor insculpida com alguns fatos e exemplos de melhores práticas, a seguir.

2. Subsídios à Avaliação do Laudo

Fato 1 - Dos atos de fiscalização

Os peritos consideraram como etapas de fiscalização algo que é só uma descrição sucinta e incompleta do que deveriam ser as mesmas, obtida em página do TSE na Internet, e apresentaram-nas no laudo como tal, através da Tabela 2, ignorando a legislação vigente que define estas etapas e os documentos eleitorais que teriam registrado o seu fiel cumprimento no caso por eles analisado.

Como exemplo, a etapa referente à assinatura e lacração dos sistemas, citada na pág. 4 do laudo: tal etapa é regida pelos § 2º e 4º do Art. 66 da Lei 9.504/97, que determina a preparação final e a lacração dos sistemas, até 20 dias antes das eleições, quando os dados constituintes desses sistemas são gravados em CD e assinados pelos fiscais presentes á cerimônia, a serem considerados os válidos para efeito de fiscalização. Enquanto no laudo não há indício de terem sido esses dados, mas outros, contra os quais a perícia teria comparado o conteúdo das urnas analisadas.

Os atos de preparação, carga e lacração das urnas são regidos pela Resolução TSE 22.712/08, em especial nos art. 22 a 34. O acesso dos peritos aos Registros Digitais dos Votos (RDV) são regulamentados pela Resolução TSE 22.770/08. A análise dos RDV foi ignorada pelos peritos embora tais arquivos deveriam conter dados que se presumem de auditoria, conforme descrito na página "Como realizar auditoria" do próprio TSE, em:

`http://www.tse.gov.br/internet/eleicoes/votoeletronico/como_audit.htm`

> "É possível ser realizada auditoria do processo sob diversos aspectos, a saber:
> - Recontagem dos votos por meio do Registro Digital do Voto (RDV);
> - Comparação da recontagem do RDV com o boletim de urna."

Ao adotar uma fonte incompleta como roteiro para condução da perícia, seus autores descuidaram de considerar, por exemplo, que entre as cerimônias oficiais necessárias à confiabilidade dos sistemas envolvidos, consta que a Conferência Visual dos Dados de Carga, após a lacração das urnas, deveria ser feita somente mediante comunicação aos agentes fiscais, como regula o Art. 28 da supracitada resolução.

> "Res. TSE 22.712/08 - Art. 28. Após a lacração das urnas a que se refere o art. 25, ficará facultado aos tribunais regionais eleitorais determinar a conferência visual dos dados de carga constantes das urnas, mediante a ligação dos equipamentos, notificados o Ministério Público, a Ordem dos Advogados do Brasil, os partidos políticos e as coligações."

Estas conferências deveriam ser feitas, por orientação do TRE, na véspera do dia da eleição, antes da remessa das urnas aos respectivos locais de votação. Portanto, se foram feitas, devem estar

registradas nos arquivos de log de cada urna analisada, e conseqüentemente, deve existir o edital de convocação e a respectiva ata da cerimônia entre os documentos eleitorais oficialmente arquivados junto à Justiça Eleitoral.

Ao se pautarem por fontes incompletas sobre os atos preparatórios e fiscalizatórios do processo eleitoral, cujas possíveis desconformidades, no caso em tela, poderiam estar indicadas por dados extraíveis das urnas analisadas, as quais poderiam estar indicando possíveis violações, subsidiando respostas aos quesitos segundo e quinto (como exemplificado acima), a perícia simplesmente descuidou-se desses atos e de suas respectivas conformidades em seu conjunto, atos cuja eficácia técnica só pode ser presumida da *totalidade* desse conjunto.

Não foram buscados e analisados os editais e as respectivas atas das cerimônias oficiais de geração, preparação e conferência das urnas, para atestar se os ritos necessários à validade do processo foram cumpridos com eficácia, em conformidade à norma. Não foi sequer verificado se, na Cerimônia de Carga das Urnas, a análise dos resumos digitais dos programas das urnas foi feita como previsto na Tabela 2 do *próprio* laudo.

Fato 2 - Da integridade dos lacres

A verificação dos lacres, descrita pelos peritos na pág. 5 do laudo, apenas conferiu a integridade do lacre do gabinete, que fica localizado na parte lateral das urnas. Este lacre, se rompido, permite acesso a placa-mãe das urnas onde se localiza, em soquetes, os dois cartões de memória das urnas denominados Flash Interno (FI) e Flash de Votação (FV).

Nada consta, porém, no laudo sobre a verificação dos demais quatro lacres, que ficam na parte traseira do gabinete, os quais, se rompidos, permitem acesso ao mesmo cartão FV e a outras portas lógicas de entrada de dados. A simples existência destes cinco lacres, demandados pela Resolução TSE 22.830/08, indica que o acesso indevido a qualquer destas portas pode comprometer a integridade dos programas gravados nas urnas antes das eleições, e estes, contaminados, comprometer a integridade dos dados de votação de maneira quase indetectável.

Em especial, o acesso ao FV pelo soquete externo (traseiro) é muito perigoso pelo fato da arquitetura e configuração das urnas permitirem a sua inicialização (boot) por meio de um flash externo devidamente programado para este fim. Para se confirmar que é possivel inicializar as urnas por flash colocado no soquete externo das mesmas, e com isso ser possível inserir programas maliciosos na FI *depois* da carga oficial das urnas, basta verificar o procedimento de carga oficial das urnas, sobre como ele é feito: por meio da um cartão denominado "flash de carga".

O flash de carga funciona colocado *no soquete externo* das urnas. Tanto para carregá-la com os programas oficiais, quanto para atualizar a tabela de candidados entre o primeiro e segundo turnos, por exemplo. Mesmo uma urna já carregada pode ser recarregada com cartões deste tipo, o que indica ser perfeitamente viável a contaminação dos programas em urnas já carregadas. Esta observação é pertinente porque, até mesmo entre supostos *experts* nessas urnas, circula a desinformação de que tal boot seria impossível. Seria pelo FV, mas este pode ser substituído mediante acesso ao soquete externo. Certamente os signatários do laudo em análise têm capacidade para verificar se os

flash de carga são capazes de "dar boot" externo nas urnas, mas, também nisso, foram omissos.

Pelo ângulo da plausibilidade, muita vez inferido para se descuidar de detalhes em análises desse tipo, um agente infiltrado poderia adulterar os programas gravados nas FI duma urna em menos de um minuto, usando um cartão previamente preparado para esta finalidade, colocando-o no soquete externo, ligando a urna para efetuar o "boot", desligando a urna e recolocando o FV original de volta em seu lugar. E se o lacre for de má qualidade, colocando de volta ele também.

Por se tratar de um calcanhar de aquiles na arquitetura dessas urnas, para tentar atenuá-lo o administrador eleitoral estabeleceu a necessidade do lacre sobre a porta externa posterior do soquete da FV, cuja integridade não foi mencionada no laudo em análise. E mesmo que tivesse sido, se esses lacres estivessem íntegros isto somente poderia atestar que os mesmos não foram rompidos depois de colocados, se forem de boa qualidade; mas isto não pode assegurar que o que já estava dentro das urnas, no momento da lacração, era o que de fato deveria estar lá.

A simples lacração das urnas não pode garantir a integridade dos programas nelas gravados se os atos preparatórios não tiverem sido executados conforme as práticas recomendadas. Lacres intactos também não podem assegurar, por si só, que o que se encontra gravado no flash depois da eleição é exatamente aquilo que estava gravado, ou que executou, no dia da eleição, uma vez que é possível a um programa fraudulento apagar-se a si mesmo, logo após executar sua lógica sorrateira, à maneira dos vírus digitais. No caso, antes do encerramento da eleição, para alterar os totais a serem gravados no BU, e portanto, antes dos lacres serem rompidos para auditoria ou para perícia.

Neste caso um tal programa poderia ser inserido em série, com um flash adequadamente preparado, por quem tiver acesso ao soquete externo na traseira de urnas enfileiradas, ao aguardo da distribuição para sessões eleitorais no dia da eleição. Assim, como não foi feita a verificação de integridade de todos os lacres, nem análise de sua qualidade, nem análise alguma para determinar se foram cumpridos os ritos e práticas recomendadas para a carga oficial das urnas (que culminam na lacração das mesmas), nem tampouco se os setores livres dos flashes continham vestígios de arquivos inesperadamente apagados, vestígios que programas auto-apagáveis podem deixar, podemos reafirmar, pelo que foi analisado no laudo em tela, que dele nada se pode concluir acerca da integridade dos programas nas urnas *no dia da eleição*.

Fato 3 - Verificação dos conteúdos dos cartões de memória

Os peritos alegam, na página 5 do laudo, que

> "realizaram o cálculo dos resumos digitais de todos os arquivos presentes nos cartões... Os resultados foram comparados com os códigos divulgados pelo TSE na Internet... Não foram encontrados quaisquer divergências entre os hashs calculados a partir dos cartões das urnas e aqueles divulgados no sítio do TSE".

A primeira irregularidade a ser destacada nesta metodologia se refere aos tais "códigos divul-

gados pelo TSE na Internet". Na tabela 2 do laudo, na referência à Cerimônia de Assinatura Digital e Lacração dos Sistemas, exigida pelo Art. 66 da Lei 9.504/97 e realizada até 20 dias antes da eleição (dia 15 de setembro de 2008, segundo o calendário oficial das eleições contido na Resolução TSE 22.579/07), é dito que:

> "Os resumos digitais (hashes) dos programas são gerados, distribuidos aos representantes e publicados na Internet. Os sistemas (fontes e executáveis) são assinados digitalmente pelo TSE, gravados em mídia não regravável, lacrados e armazenados no cofre."

Esta cerimônia oficial, obrigatória por lei, foi efetivamente realizada no dia 15 de setembro de 2008 perante os fiscais de partidos, da OAB e do Ministério Público, e os resumos digitais nela produzidos foram publicados no endereço:

`http://www.tse.gov.br/internet/eleicoes/resumos_digitais.htm`

Em Monte do Carmo, segundo o laudo, foram usadas urnas modelos 2000 e 2004, sendo as urnas de contingência, não usadas, de modelo 2002. As tabelas oficiais dos hashes destas urnas então respectivamente nos endereços:

```
www.tse.gov.br/internet/eleicoes/resumos_digitais/2008/991ue00.pdf
www.tse.gov.br/internet/eleicoes/resumos_digitais/2008/991ue04.pdf
www.tse.gov.br/internet/eleicoes/resumos_digitais/2008/991PART.pdf
www.tse.gov.br/internet/eleicoes/resumos_digitais/2008/chaves_ue.pdf
```

Analisando os conteúdos destes arquivos pode-se verificar que os três primeiros foram efetivamente criados em 15 de setembro de 2008 (acessando o metadado “data de criação”, anotada como 09/15/08, em formato MM/DD/AA conforme configuração do programa de gravação).

Porém, o quarto arquivo, referente justamente às chaves de verificação de resumos digitais, fundamentais para a verificabilidade da integridade do sistema, foi criado no dia 25 de setembro de 2008 (anotada como 09/25/08), portanto, após e fora da cerimônia oficial exigida por lei para este fim, ao arrepio e fora das vistas dos fiscais de partidos, da OAB e do Ministério Público.

Nesta tabela constam os seguintes resumos digitais relativos ao Estado de Tocantins:

Localização e nome do arquivo	Resumo Digital SHA1-Radix64
`/uenux/app/chave/avusrchave.vmt`	`vCAhr2dCCBdJExlmpluWtVqBTKI=`
`/uenux/app/chave/bu.pk1`	`n82NqjOg2FHJ8pRTfFqjdbGwtqk=`
`/uenux/app/chave/ue.pri`	`jv2xkDflPeWbvD2GpwZhybEqNA8=`
`/uenux/app/chave/ue.pub`	`DmauAeRYAT6a+qjRbEsXYKDPs2k=`
`/uenux/app/chave/vd.pk1`	`6y/wfxqjzwQrDevoetvK0FK0wac=`

O laudo omite o fato de que os resumos digitais usados para “auditar” os arquivos examinados carecem de confiabilidade ou validade segundo a própria legislação eleitoral vigente, por terem sido criados em desconformidade às normas de segurança, transparência e fiscalização determinados por lei.

Outro omissão, ou inconsistência no laudo, está no fato de que havia, ou deveria haver, na pasta "/lib" dos flashes analisados (área de arquivos fixos da FI) ao menos oito ponteiros de arquivos não descritos nos respectivas tabelas oficiais de resumos digitais, e portanto, sem resumo digital

para ser conferido:

```
> /lib/
> ld-linux.so
> libc.so
> libdl.so
> libgcc_s.so
> libm.so
> libpthread.so
> librt.so
> libstdc++.so
```

Outra omissão grave no laudo analisado é a ausência de verificação dos resumos digitais dos arquivos contendo os resultados da votação e os arquivos de auditoria (BU, RDV e LOG), cujos valores-resumo estavam, ou deveriam estar, disponíveis nos próprios cartões analisados.

Os programas que são executados nas urnas eletrônicas no dia da eleição geram uma série de arquivos de dados que, ao final da votação, são gravados na FI, na FV e no disquete destinado à totalização. O formato dos nomes dos arquivos de dados produzidos em cada urna eletrônica obedece ao seguinte sintaxe:

```
MMMMMZZZZSSSS.O1x
```

onde `MMMMM` é o número da cidade; `ZZZZ` é o número da Zona Eleitoral; `SSSS` é o número da Seção Eleitoral do respectivo arquivo; `01` se refere ao primeiro turno; e `x` indica o tipo do arquivo conforme a seguinte tabela:

x	Extensão	Tipo	Conteúdo
K	O1K	HASH	Resumos Digitais
L	O1L	LOG	Relação de Eventos
A	O1A	RDV	Registro Digital do Voto
B	O1B	BU	Boletim de Urna
F	O1F	-	Eleitores Faltosos
S	O1S	-	Justificativas

Assim, dever-se-ia verificar se os resumos digitais contidos nos arquivos de extensão `O1K` resultam iguais aos calculados sobre os respectivos arquivos, o que foi omitido no laudo analisado.

Outro falha grave nos procedimentos de verificação do conteúdo dos cartões de memória foi a omissão da varredura das áreas livres, em busca de indícios de arquivos inesperadamente apagados. Numa perícia desta natureza, com quesitos tais como os quatro últimos levantados, não se deve ignorar a possibilidade de programas maliciosos, porventura presentes nas urnas no dia da eleição, apagarem-se a si mesmos, antes do final do votação e após a execução de sua lógica sorrateira, para eliminar vestígios de sua presença, de forma que uma análise superficial posterior, como a que foi feita neste caso, não os encontre. No entanto, se o auto-apagamento for feito de forma descuidada,

restarão vestígios destes arquivos nas áreas do flash que normalmente aparacem como áreas livres, disponíveis para novas gravações.

Como exemplo de auditoria sobre sistema eleitoral que seguiu boas práticas podemos citar, por ter sido amplamente divulgada e poder servir de referência, aquela contratada a professores da Unicamp para o caso conhecido como "Painel do Senado". Naquela perícia, coordenada pelo Prof. Dr. Álvaro Crósta, os setores livres do disco rígido (que correspondem aos flashes no caso em tela) foram varridos, e lá encontrados vestígios e partes de arquivos inesperadamente apagados, os quais indicavam violação, conforme o seguinte trecho do Sumário Executivo do respectivo laudo, publicado pela folha on-line em

http://www1.folha.uol.com.br/folha/brasil/ult96u17682.shtml

"Há alguma evidência de violação do sigilo?

... é importante destacar que, durante a busca de arquivos apagados realizada nos discos rígidos, foram encontrados fragmentos de arquivos com nomes como "?enador.doc", "?enh_sen.doc" e "?adeiras.xls", cujas datas de criação coincidem com ou são próximas às de votações secretas. Os atributos recuperáveis desses arquivos poderiam ser usados como indícios para investigações de outra natureza."

Este caso ilustra, também, como a boa prática pericial considera, para erguer-se acima de fundadas suspeições, os interesses envolvidos de maneira equilibrada, dando acesso, para acompanhamento das atividades periciais, às partes diretamente interessadas e não a apenas uma delas (presente na perícia estava um funcionário de empresa Procomp, contratada pelo TSE para manutenção das urnas, ambas propagadoras do mito da inviolabilidade das urnas em análise). Como se pode ver pela leitura completa da referida matéria.

Fato 4 - Verificação do conteúdo dos arquivos de log das urnas

Os peritos teriam obtido os arquivos de log das urnas junto ao TRE, supostamente para análise, mas não os compararam com seus respectivos originais, gravados nos próprios flashes analisados. Como também não conferiram os resumos digitais dos arquivos de logs analisados com os resumos contidos nos flashes. Assim não se pode, a princípio, afirmar a integridade dos dados analisados. A análise apresentada foi demais sucinta, reduzindo-se a uma única frase:

"A análise dos arquivos (de log) não reportaram anormalidades na operação da urnas eletrônicas utilizadas na votação".

Como nada mais foi reportado, tal situação indica que:

- Não foi feita a conferência das datas de carga das urnas comparando-as com a Ata da Cerimônia de Carga;
- Não foi feita a verificação se existiam registros dos procedimentos de conferência visual da

carga na véspera da eleição e o respectivo edital de convocação previsto pelo art. 28 da Res. TSE 22.712/08;

- não foi verificado o uso de programas que possibilitem a alteração do relógio ou calendário para confirmar se existiam as respectivas atas prevista pelo art. 29 da Res. TSE 22.712/08;

- não foi verificado se foi realizado o teste obrigatório de simulação de votação ou conferência por amostragem, regulamentado pelo §1º do art. 31 da Res. TSE 22.712/08;

- Não foi feita nenhuma conferência do total de votos computados, segundo o LOG, com os totais de votos registrados nos arquivos de Registro Digital do Voto (RDV) e do Boletim de Urna (BU), o que parece inacreditável em face do quesito cinco;

A respeito da omissão na conferência dos totais de votos de cada urna, que deveria ser feita cruzando-se os dados dos três arquivos de auditoria (BU, RDV e LOG) presentes, ou que deveriam estar presentes, nos flashes analisados, os peritos nem mesmo notaram, ou se notaram não reportaram no laudo, que os arquivos de RDV nos flashes estavam criptografados, impossibilitando uma auditoria – no sentido ou aspecto técnico do termo – do resultado eleitoral, por impossibilitar resposta conclusiva ao terceiro quesito, em contradição com o descrito na própria página do TSE:

`http://www.tse.gov.br/internet/eleicoes/votoeletronico/como_audit.htm`

"É possível ser realizada auditoria do processo sob diversos aspectos, a saber:

- Recontagem dos votos por meio do Registro Digital do Voto (RDV);
- Comparação da recontagem do RDV com o boletim de urna."

3. Conclusão

Diante do grau de superficialidade e parcialidade, e da natureza essencial de lacunas técnicas encontradas na perícia cujo laudo aqui se analisa, consubstanciamos nosso entendimento, expresso no início da seção 1 acima, de que resta definitivamente comprometida a conclusividade da referida perícia, presumida nas respostas por ela oferecidas aos quesitos levantados. E de que, portanto, resta afastado um possível valor probante alusivo a seu caráter técnico.

Brasília, 7 de Maio de 2009

Pedro Antonio Dourado de Rezende
Ex-membro do Comitê Gestor da Infra-estrutura de Chaves Públicas brasileira
Professor de Criptografia e Segurança na Informática
Departamento de Ciência da Computação
Universidade de Brasília