TC nº 72-001.889.08-28

AUDITORIA. SMT. Avalição dos resultados alcançados. Programa de Governo Mobilidade e Acessibilidade. Bilhete Único. Sistema de Bilhetagem Eletrônica. Recomendações atendidas. CONHECIDA. DETERMINAÇÃO. Votação unânime.

TC citado 72-000.854.09-99.

2.896ª Sessão Ordinária

Trânsito em julgado: 26/05/2017

A C Ó R D Ã O

Vistos, relatados e discutidos estes autos, dos quais é Relator o Conselheiro JOÃO ANTONIO.

ACORDAM os Conselheiros do Tribunal de Contas do Município de São Paulo, à unanimidade, de conformidade com o relatório e voto do Relator, em conhecer da auditoria para fins de registro.

ACORDAM, ademais, à unanimidade, em determinar à São Paulo Transporte S.A. – SPTrans, que mantenha constante aprimoramento do Sistema de Bilhetagem Eletrônica, como diretiva de preservação do interesse coletivo, vislumbrando a mitigação dos riscos envolvidos, a fim de preservar o sistema contra possíveis e eventuais fraudes.

ACORDAM, afinal, à unanimidade, em determinar, após as demais comunicações de praxe, o arquivamento dos autos.

Participaram do julgamento os Conselheiros EDSON SIMÕES – Revisor, MAURÍCIO FARIA e DOMINGOS DISSEI.

Presente o Procurador Chefe da Fazenda CARLOS JOSÉ GALVÃO.

Plenário Conselheiro Paulo Planet Buarque, 26 de outubro de 2016.

ROBERTO BRAGUIM
Presidente

JOÃO ANTONIO
Relator

RELATÓRIO

Trata o presente de auditoria programada efetuada em 2008 com o fito de avaliar os resultados alcançados na execução do programa "Mobilidade e Acessibilidade – Bilhete Único", enfatizando a segurança do Sistema de Bilhetagem Eletrônica – SBE da SPTrans, tendo como interessado a Secretaria Municipal de Transporte.

A Subsecretaria de Fiscalização e Controle, às fls. 19/60, concluíram o seguinte:

> ***"4.1 – Segurança do Sistema de Bilhetagem Eletrônica***
>
> *O Sistema de Bilhetagem Eletrônica (SBE) é hoje um sistema maduro, aparentando boa estabilidade. Apesar de não ter sido objetivo específico desta auditoria avaliar se o Sistema atende às regras de negócio conforme estabelecidas ou detectar a existência de erros (bugs), nenhum evento desabonador foi constatado ao longo da auditoria.*
>
> *Quanto à segurança do SBE, esta sim objeto de avaliações na auditoria, observamos a existência de oportunidades de melhoria.*
>
> *A Superintendência de Sistemas de Receita e Remuneração (DG/SSR) está em fase de implementação de um Sistema de Gestão da Segurança da Informação - SGSI, o que auxilia na organização de documentos e procedimentos.*
>
> *O núcleo central de um SGSI, o Ciclo de Gestão de Risco, porém, ainda não está em funcionamento. Assim não existe uma investigação sistemática visando à detecção de riscos e avaliação dos procedimentos utilizados nessa detecção, bem como usados no tratamento de riscos. Consideramos recomendável que se enfoque a implementação do Ciclo de Gestão de Risco e seus procedimentos de gestão.*
>
> *Consideramos recomendável ainda que a SPTrans, com seu corpo de efetivos, aborde imediatamente os riscos de* ***clonagem*** *dos cartões de Bilhete Único – BU, bem como de* ***restauração de estado*** *comentados no item 3.5. Ainda que a técnica represente uma barreira àqueles que criminosamente pretendam clonar o BU, restaurar seu estado ou praticar outro tipo de fraude, ainda não detectado, o risco é importante, com uma probabilidade considerável de ocorrer e de impacto razoável.*

Recomendamos, no entanto, que a SPTrans empregue seus próprios efetivos na avaliação dos riscos de fraude, com possível auxílio de especialistas independentes. Consideramos que o apoio da Digicon certamente trará contribuições importantes, porém nos parece pouco efetivo transferir tal responsabilidade à Digicon, isto porque:

1. Quem sofrerá o impacto de eventos de segurança é a Municipalidade e a SPTrans e não a Digicon, portanto o interesse primordial não é desta;

2. A Digicon já demonstrou ou estar mal informada ou pouco afeita a informar à SPTrans quanto ao surgimento de novos riscos relacionados ao BU, como visto no subitem 3.5.7;

3. Como se mostrou no item 3.6, ainda que detentora de alta tecnologia na área de segurança da informação, a Digicon também tem suas dificuldades em relação à segurança;

4. Enquanto desenvolvedora da segurança do SBE e parceira internacional da NXP, a Digicon tem tendência de ser mais complacente em relação aos seus produtos e ao Mifare Classic.

Por fim, recomendamos que providências sejam adotadas no sentido de se eliminar a vulnerabilidade detectada no ponto de acesso por conexão sem fio (wireless) e evidenciada no item 3.6.

4.2 – Fiscalização do Uso do Bilhete Único

Concluiu-se que não há uma metodologia que permita a medição direta dos resultados das ações de combate às fraudes. Ainda sim, há boas ferramentas de prevenção e combate às fraudes dentre as quais a SPTrans vem fazendo uso de políticas de tarifação e remuneração específicas, fiscalização em campo e detecção de anomalias por meio dos registros eletrônicos das transações.

Em relação a políticas de tarifação, tem-se adotado medidas que efetivamente dificultam diversos tipos de fraudes, seja diminuindo a quantidade de dinheiro em espécie circulando pelo sistema, seja por medidas que tornem menos rentável a fraude. Medidas como a vedação da validação do cartão sem crédito direto na catraca.

A fiscalização vem ganhando uma configuração mais adequada, pois passou a ser feita principalmente por agentes concursados da SPTrans e não mais por empregados de empresas contratadas. Assim, a SPTrans vem corrigindo essa irregularidade, já há muito apontada por essa E. Corte.

Poucos são, ainda, as análises efetuadas sobre os bancos de dados oriundos dos registros das transações no Sistema de Bilhetagem Eletrônica. Assim, há um terreno a ser explorado nessa área da fiscalização eletrônica. Como a detecção das possíveis fraudes de clonagem e restauração de estado não podem ser detectadas por fiscalização de campo ou mesmo pelo cobrador, a fiscalização eletrônica será a principal ferramenta de combate nesses casos.

4.3 – Plano Plurianual 2006/2009

As metas do PPA 2006/2009 de custeio de gratuidades no Sistema de Bilhetagem Eletrônica foram atendidas. Observamos, porém, que tais metas não são realistas."

O Núcleo de Tecnologia da Informação, às fls. 62/63, manifestou-se acompanhando o entendimento da área técnica, evidenciou os itens 3.5 (Cartão inteligente do SBE) e 3.6 (Vulnerabilidade na Rede de Desenvolvimento Operada pelo Digicon).

Enfatizaram a importância das *"ações referentes ao gerenciamento de risco inerente à operação indevida dos cartões"* e a necessidade da adoção de *"ações corretivas no sentido de garantir segurança à rede operada pela Digicon, alterando-se o protocolo utilizado atualmente*".

A Origem foi devidamente oficiada, tendo trazido aos autos suas justificativas (fls. 74/81) sobre as conclusões alcançadas pelos técnicos.

Manifestou-se, novamente a Auditoria sobre as justificativas apresentadas relatou que as recomendações feitas por esta Corte foram atendidas pela SPTRANS. Assim, o objetivo desta Auditoria restou atendido. Informou que os resultados alcançados foram consolidados no Relatório Anual de Fiscalização de 2008 – TC nº 72-000.854.09-99 e, por derradeiro, sugeriu que seja dada ciência à Origem de eventuais possibilidades de clonagem do Bilhete Único.

A Procuradoria da Fazenda Municipal, às fls. 91/96, opinou pelo conhecimento e registro da auditoria realizada, por entender que do ponto de vista técnico os objetivos foram atendidos.

A Secretaria Geral, às fls. 98/102, concluiu que "*a auditoria realizada cumpriu adequadamente o determinado e, ainda, suas conclusões promoveram os esclarecimentos suficientes, não remanescendo questionamentos jurídicos*."

Entende ainda que a presente auditoria encontra-se em condições de ser submetida à apreciação, para conhecimento, registro e atendimento do disposto na Resolução nº 06/00.

A Origem foi oficiada para conhecimento da sugestão feita no item C, do relatório de fls. 85/89 de autoria da Área Técnica.

A SFC, às fls. 114/115, trouxe aos autos a notícia de que "*"pesquisadores" de uma empresa brasileira da área de Segurança da Informação teriam "descoberto" uma forma de recarregar o Bilhete Único, sem o correspondente pagamento.*"

Na opinião da referida Área Técnica nada de novo foi criado, além do já esperado e suscitado por ela, por fim "*sugere que seja determinado à SPTrans a elaboração, no prazo de 15 dias, de um plano de ação voltado à mitigação dos riscos envolvidos, informando este Tribunal quanto ao plano de ação elaborado.*"

A Assessoria Jurídica, às fls. 118/123, acompanha o entendimento formulado pela SFC, assim, o "constante aprimoramento do sistema, entendo pertinente, como diretiva de preservação do interesse coletivo, a sugestão da Subsecretaria de Fiscalização e Controle de que a SPTrans elabore um plano de ação voltado à mitigação dos riscos envolvidos, a fim de preservar o sistema contra possíveis e eventuais fraudes."

Novamente a Secretaria Geral se pronuncia, "*Diante de todo o quadro traçado pelas equipes técnicas da SFC e da AJCE, reitero a manifestação às fls. 98/102, opino pelo conhecimento e registro da auditoria programada, restando, entretanto, afastado o exame do mérito, à vista de sua natureza documental.*"

É o Relatório.

VOTO

Em julgamento a auditoria programada efetuada em 2008 com o fito de avaliar os resultados alcançados na execução do programa "Mobilidade e Acessibilidade – Bilhete Único", enfatizando a segurança do Sistema de Bilhetagem Eletrônica – SBE da SPTrans, tendo como interessada a Secretaria Municipal de Transporte.

A dialética processual demonstrou que as recomendações feitas por esta Corte foram atendidas pela SPTrans, assim o objetivo desta Auditoria restou atendido.

E, mais, os resultados alcançados foram consolidados no Relatório Anual de Fiscalização de 2008, no TC nº 72-000.854.09-99.

Contudo, remanesce uma grande preocupação com relação a possibilidade de novas clonagens do sistema de bilhete único, de tal sorte que faço determinação ao final do meu voto.

Diante do exposto, **CONHEÇO** da presente auditoria para fins de **REGISTRO,** com **DETERMINAÇÃO à** SPTrans para que mantenha constante aprimoramento do Sistema de Bilhetagem Eletrônica, como diretiva de preservação do interesse coletivo, vislumbrando a mitigação dos riscos envolvidos, a fim de preservar o sistema contra possíveis e eventuais fraudes.

Após as demais comunicações de praxe, **ARQUIVEM-SE** os autos.