RELATÓRIO DE INSPEÇÃO

1. ORDEM DE SERVIÇO

Nº 2017.10400.10

2. IDENTIFICAÇÃO

2.1. Objeto

Sistema de Bilhetagem Eletrônica (SBE)

2.2. Objetivo

Cumprir determinação do Conselheiro Relator no TC nº 72.002.495/08-88, contendo: análise atualizada da forma com que os serviços de bilhetagem eletrônica do Sistema de Transporte Coletivo do Município de São Paulo estão sendo prestados, tendo por base o julgamento proferido no TC nº 72.000.481/06-30 – cuja determinação de acompanhamento do Contrato 2008/0359-01-00 foi executada nos autos dos TCs 72.002.208/08-94 (análise formal) e 72.002.485/08-24 (execução contratual).

2.3. Unidade Fiscalizada

São Paulo Transporte S/A (SPTrans)

2.4. Período de Realização

17.11.17 a 16.03.18

2.5. Período de Abrangência

05.10.01 a 07.03.18

2.6. Equipe Técnica

Adriano Gonçalves Zambon RF nº 20.309

2.7. Procedimentos

- Análise e verificação das funcionalidades do Sistema de Bilhetagem Eletrônica (SBE);
- Entrevista com os responsáveis da SPTrans pelo gerenciamento das bases de dados e rotinas do SBE.

2.8. Quadro de Siglas e Abreviaturas

ABNT	Associação Brasileira de Normas Técnicas
AES	*Advanced Encryption Standard*
ASP	*Active Server Pages*
AVL	*Automatic Vehicle Location*
BI	*Business Intelligence*
BU	Bilhete Único
CMBD	Catálogo Municipal de Bases de Dados
CPTM	Companhia Paulista de Trens Metropolitanos
DG	Diretoria de Gestão da Receita e Remuneração
DP	Diretoria da Presidência
GAT	Gerência de Atendimento
GESP	Governo do Estado de São Paulo
GOS	Gerência de Operação e Segurança
GPS	*Global Positioning System*
HM	*Hyper Master*
HSM	*Hardware Security Module*
HTTP	*Hyper Text Transfer Protocol*
HTTPS	*Hyper Text Transfer Protocol Secure*
IEC	*International Electrotechnical Commission*
IP	*Internet Protocol*
ISO	*International Organization for Standardization*
LV	Loja Virtual
NBR	Norma Brasileira
PALC	Processo Administrativo de Licitações e Contratos
PcD	Pessoa com Deficiência
PDV	Ponto de Venda
PIC	*Programmable Interface Controller*
PMD	Plano Municipal de Desestatização
PMSP	Prefeitura do Município de São Paulo
SA	Sistema de Atendimento
SAC	Superintendência de Atendimento e Comercialização
SAM	*Security Access Module*
SBE	Sistema de Bilhetagem Eletrônica
SCA	Sistema de Cadastro e Atendimento
SCD	Sistema Central de Distribuição
SCP	Sistema Central de Processamento
SGG	Sistema Gerenciador de Garagem
SGSI	Sistema de Gestão de Segurança da Informação
SIM (1)	Sistema Integrado de Monitoramento
SIM (2)	*Subscriber Identity Module*
SL1	*Security Level* 1
SL3	*Security Level* 3
SMDP	Secretaria Municipal de Desestatização e Parcerias
SMT	Secretaria Municipal de Mobilidade e Transportes
SPTrans	São Paulo Transporte S/A
SSL	*Secure Sockets Layer*
STI	Superintendência de Tecnologia da Informação
SUAC	Sistema Único de Arrecadação Centralizada
TCP	*Transmission Control Protocol*
TLS	*Transport Layer Security*

3. RESULTADO

3.1. Introdução

O Sistema de Bilhetagem Eletrônica (SBE) é um sistema de gestão financeira das receitas do Sistema de Transporte Coletivo Urbano de Passageiros do Município de São Paulo, implantado em 2004 pela SPTrans – contratada pela Secretaria Municipal de Mobilidade e Transportes (SMT) para efetuar a venda e utilização dos créditos eletrônicos no serviço de transporte sobre pneus do município. Sua utilização decorre do artigo 31 c/c artigo 39 da Lei Municipal nº 13.241/01, que atribui à SPTrans a competência de gerenciar, planejar, fiscalizar e controlar a receita tarifária do Serviço de Transporte Coletivo Público de Passageiros.

Inicialmente, seu uso ficou restrito a algumas linhas de ônibus como forma de testes, sendo em 17.05.04 estendido a toda a frota da cidade. Em 06.10.05, foi firmado o Convênio SBE entre Governo do Estado de São Paulo (GESP), Companhia do Metropolitano de São Paulo (Metrô), Companhia Paulista de Trens Metropolitanos (CPTM), Prefeitura do Município de São Paulo (PMSP) e SPTrans, estabelecendo condições para integração operacional e tarifária nas esferas municipal e estadual de transporte.

A partir dele, o SBE foi expandido para o serviço de transporte sobre trilhos em 2006. Posteriormente, por meio de termos aditivos, ingressaram no Convênio as concessionárias do Metrô de São Paulo para as linhas 4 (empresa “ViaQuatro”, integrada ao SBE em 2008), 6 (empresa “Move São Paulo”), e monotrilho da linha 18 (empresa “Vem ABC”) – as duas últimas, até o momento, não efetivaram sua integração ao sistema.

A proposta deste trabalho é avaliar a estrutura e modelo de contratação do sistema informatizado de bilhetagem eletrônica adotado pela São Paulo Transporte S/A (SPTrans), assim como de suas atualizações; verificar se os contratos relacionados preveem a independência da Administração Pública Municipal sobre seus fornecedores, bem como a eficácia e efetividade dos controles de acesso, inclusão e alteração de créditos de transporte no sistema.

3.2. Análise

3.2.1. Descrição do SBE

O SBE funciona por meio da aquisição e consumo de créditos de transporte pelos usuários dos serviços de transporte sobre pneus (municipal) e sobre trilhos (estadual). Esses créditos são armazenados em cartões inteligentes (*smart cards*) denominados Bilhete Único (BU), lidos por equipamentos de recarga de créditos e validadores que controlam o acesso às modalidades de transporte. Mais de 13,7 milhões de BUs realizaram algum tipo de transação (recarga ou utilização) entre dezembro de 2016 e dezembro de 2017, sendo dessa forma considerados ativos (fls. 24/25).

O modelo de cartão inteligente utilizado é o MIFARE, fabricado pela holandesa NXP Semiconductors. O MIFARE possui alguns modelos distintos, dentre os quais estão em uso no SBE o Classic e o Plus (nas versões X e EV1). O modelo Classic utiliza criptografia fraca de algoritmo Crypto-1 – considerada insegura, conforme TC nº 72.001.889/08-28, que cuida dos resultados alcançados na execução do programa Bilhete Único, enfatizando a segurança do SBE – e possui 1 kB de capacidade de memória. Ele é considerado ultrapassado e inadequado para novas aplicações.

Por sua vez, o modelo Plus suporta criptografia forte de 128 bits *Advanced Encryption Standard* (AES) versão 2008, além de capacidades de memória (4 kB), processamento e segurança melhoradas em relação ao Classic, o que permitiu a implantação de políticas de tarifação nas modalidades mensal, semanal e diária, assim como a concentração de todas as modalidades de cartões de passageiros pagantes no mesmo cartão.

Entre 2013 e 2015, a SPTrans, visando melhorar a segurança e funcionalidade do SBE, procedeu à troca dos validadores de cartões no serviço de transportes, substituindo os equipamentos então utilizados – que só suportavam cartões MIFARE Classic – por outros que suportam também o modelo Plus. Assim, os novos validadores podem atender tanto aos novos cartões quanto aos antigos, permitindo sua troca gradativa – desde 2015, apenas cartões MIFARE Plus são comercializados.

Esses equipamentos permitem a utilização de até 4 módulos *Security Access Module* (SAM), presentes nos validadores e terminais de recarga e que assinam digitalmente as transações realizadas, garantindo sua autenticidade. Atualmente, são utilizados microcontroladores *Programmable Interface Controller* (PIC) projetados pela própria SPTrans como módulos SAM.

Hoje, cerca de 60% da base de cartões em uso ainda são do tipo Classic (fl. 24/25), isto é, do tipo de menor capacidade. Por conta disso, não é possível trocar os módulos SAM por outros que utilizem criptografia forte na comunicação com os cartões, e só a criptografia fraca de algoritmo Crypto-1 – utilizada pelo cartão Classic e considerada insegura, consoante TC nº 72.001.889/08-28 – é usada hoje. Por conta disso, os cartões Plus distribuídos possuem nível de segurança *Security Level 1* (SL1), que emula um cartão Classic.

A utilização de um novo SAM para criptografia forte em paralelo com os atuais está prevista para a nova versão do SBE em construção a partir do Contrato nº 2012/0038-01-00 e seu Termo Aditivo nº 01. O novo SAM, desenvolvido pela Montreal, é um chip *Subscriber Identity Module* (SIM), mais moderno e elaborado para suportar a criptografia forte oferecida pelos cartões MIFARE Plus.

O SBE realiza diversas funções de gestão da tarifação e faturamento de créditos de transporte, dentre as quais abordaremos a venda de créditos e a tarifação de serviços de transporte.

3.2.1.1. Venda de créditos

Denominam-se créditos de transporte os valores armazenados no Bilhete Único destinados ao pagamento de tarifas no transporte público de passageiros nos ônibus ou nas catracas do Metrô e CPTM. Tais créditos são comercializados de duas formas:

- Venda direta;
- Venda por lista.

Na venda direta, o portador do BU deve dirigir-se a um dos pontos de vendas (PDV) de créditos, onde pagará o valor correspondente à quantidade de tarifas que deseja

carregar. O operador do PDV, então, executará a operação de carregamento dos créditos no cartão utilizando o equipamento de recarga.

Na chamada venda por lista, pagamento e recarga são realizados em momentos distintos. O comprador – por exemplo, um empregador que ofereça vales-transporte a seus empregados – acessa a loja virtual da SPTrans ou uma credenciada, informa quais beneficiários deverão ter seus cartões carregados e com quanto, solicita a emissão de boleto e efetua o pagamento no sistema bancário. Após o SBE constatar o pagamento, o usuário do cartão passa em um dos pontos de recarga automatizados e o carrega com os créditos adquiridos.

Em ambos os casos, a carga dos créditos ocorre de forma *online* no SBE, uma vez que os pontos de recarga estão conectados a ele – apesar de utilizarem sistemas proprietários, de mais de 10 empresas diferentes – e o utilizam para validar e persistir a recarga realizada. Uma exceção a isso, conforme será visto no item 3.2.5.2, ocorre em alguns casos de fraude detectados pela SPTrans.

A receita bruta arrecadada com a venda de créditos de transporte foi de cerca de R$ 6,2 bilhões em 2017 (fl. 29), uma média de mais de R$ 500 milhões por mês.

3.2.1.2. Tarifação

A tarifação trata da cobrança de tarifas pela prestação de serviços de transporte aos usuários do sistema de transportes integrado pelo SBE. Essa cobrança se dá nas catracas dos ônibus ou de entrada nas estações do Metrô ou da CPTM. Para tanto, basta o usuário do cartão aproximá-lo a uma distância de até 13 cm do painel de leitura do validador, que verificará a necessidade de se cobrar ou não tarifa e a existência de crédito suficiente para cobri-la, e efetuará o débito no cartão. O validador registra ainda no cartão os detalhes da transação, o que permitirá que os validadores de viagens posteriores concedam o benefício da integração gratuita. Hoje, o SBE processa cerca de 13 milhões de transações por dia referentes à tarifação, divididas entre 10 milhões nos ônibus e mais 3 milhões nos trilhos (Metrô/CPTM) (fl. 23).

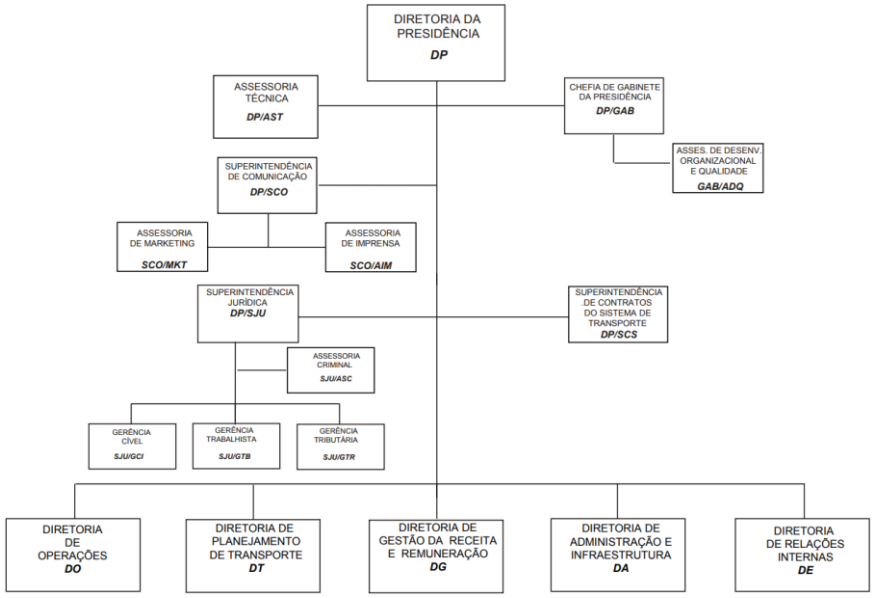
Ao contrário da venda de créditos, a tarifação ocorre de maneira *offline*. Como os validadores se encontram em locais sem acesso a rede como a maioria dos ônibus,

e/ou com grande fluxo de pessoas como estações do Metrô ou da CPTM (onde o acesso à rede poderia gerar lentidão no processamento das transações de pagamento), essa atividade utiliza as informações armazenadas nos próprios equipamentos e cartões, registrando a cobrança nestes e sincronizando-a posteriormente no SBE. A demora entre a tarifação e sua contabilização representa uma das maiores fragilidades do sistema, como será visto no item 3.2.5.2.

3.2.2. Gestão do SBE

O Sistema de Bilhetagem Eletrônica é gerido pelo Convênio SBE, composto pelas entidades retrocitadas. Dentro da SPTrans, o sistema é de responsabilidade da Diretoria de Gestão da Receita e Remuneração (DG), que está subordinada à Diretoria da Presidência (DP) da maneira a seguir:

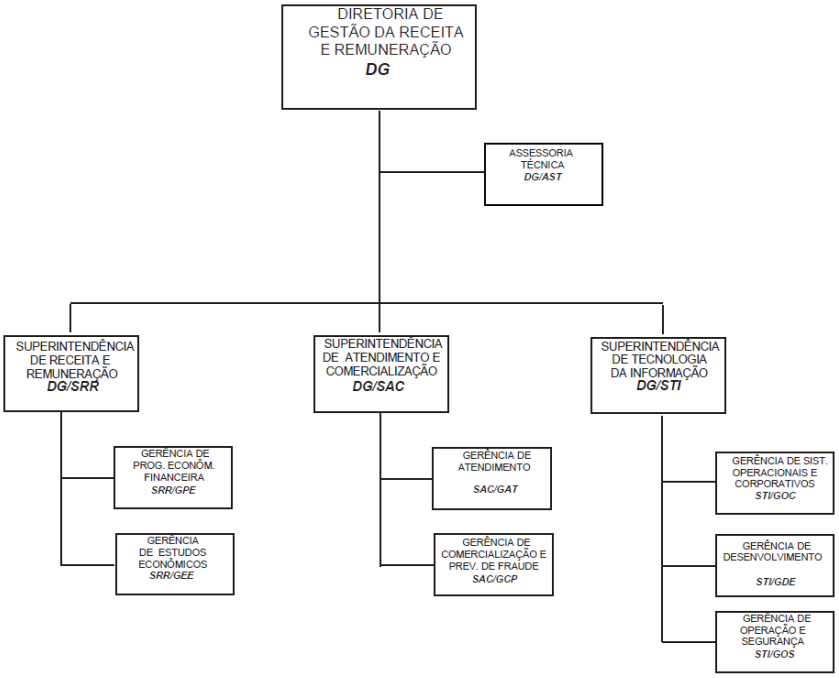
Figura 1 – Organograma geral SPTrans.



Fonte: SPTrans.

Ao longo do relatório far-se-á referência às seguintes superintendências e gerências da Diretoria de Gestão da Receita e Remuneração:

Figura 2 – Organograma DG SPTrans.

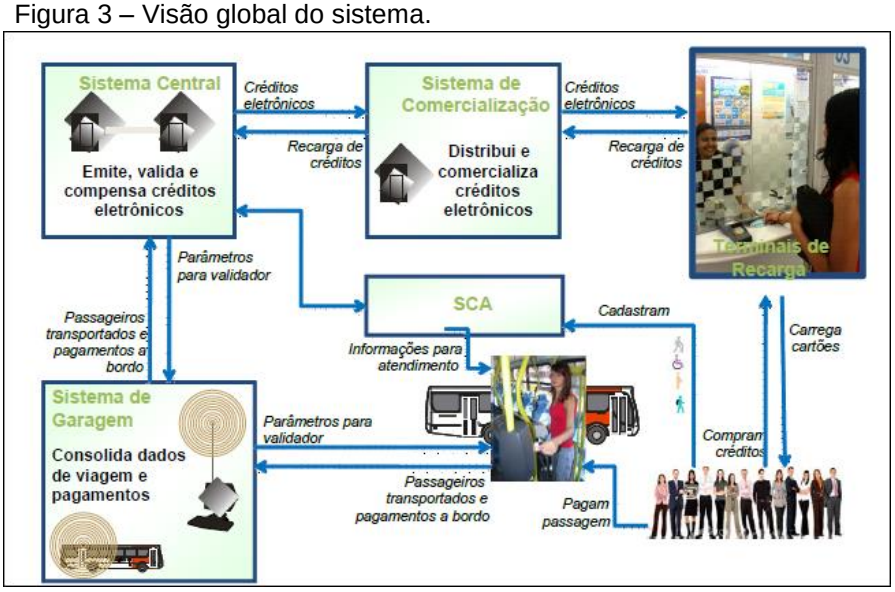


Fonte: SPTrans.

3.2.3. Solução informatizada SBE

A solução informatizada SBE foi construída em etapas, atendendo às necessidades que surgiam na bilhetagem eletrônica. Destarte, foram criados “sistemas” (na realidade, subsistemas ou módulos) que eram integrados aos preexistentes. Sua constituição iniciou-se pelo Sistema Central; seguiu para o Sistema de Cadastro e Atendimento; depois ao Sistema de Distribuição; e por fim à Loja Virtual, chegando à estrutura apresentada no diagrama abaixo, que exemplifica o relacionamento entre componentes e o fluxo de dados atual:

Figura 3 – Visão global do sistema.



Fonte: SPTrans.

O Sistema de Garagem trata-se de sistema externo ao SBE, utilizado pelas operadoras de transporte. De acordo com o Catálogo Municipal de Bases de Dados (CMBD), os seguintes sistemas e bases de dados integram a bilhetagem na SPTrans:

Quadro 1 – Bilhetagem segundo CMBD

Órgão ou Entidade	Seção Responsável	Título da Base	Resumo
São Paulo Transporte S.A.	Bilhetagem/Usuário de Bilhete Único	Sistema Central de Atendimento (SCA)	Sistema de Gerenciamento, Cadastro e Atendimento de todos os usuários do Bilhete Único
São Paulo Transporte S.A.	Bilhetagem/Credenciadas de VT	Sistema Central de Distribuição (SCD)	Sistema Central de Distribuição que controla todas as vendas de VT e produtos adquiridos pela WEB
São Paulo Transporte S.A.	Bilhetagem/Garagens	Sistema Central de Processamento (SCP)	Sistema Central de Processamento dos dados de passageiros do Bilhete Único
São Paulo Transporte S.A.	Bilhetagem/Empregador VT/Credenciados VT	Loja Virtual (LV)	Sistema WEB de venda de Vale Transporte para empregadores com aquisição direta na SPTrans
São Paulo Transporte S.A.	Bilhetagem	Data Warehouse (DW)	Sistema de manutenção de dados históricos para gestão e tomada de decisões referentes à bilhetagem eletrônica.
São Paulo Transporte S.A.	Bilhetagem	Idoso (Cadastro Idoso)	Sistema de cadastro de Beneficio para o cartão do Idoso
São Paulo Transporte S.A.	Bilhetagem	Defic (Cadastro Deficiente)	Sistema de cadastro de beneficio para cartão do Deficiente
São Paulo Transporte S.A.	Bilhetagem/Redes de Recarga	*Hyper Master* (HM)	Sistema de gerenciamento de recarga do bilhete único.

Fonte: CMBD.

Entendemos junto à Superintendência de Tecnologia da Informação (STI) que as bases de dados DW, Idoso e Defic não podem ser consideradas sistemas propriamente ditos, mas somente ferramentas de cadastro – ainda que, do ponto de vista do CMBD (cujo

foco é nas bases de dados e não nos sistemas que as suportam), possam ser consideradas bases de dados apartadas.

A questão sobre o que compõe ou não o SBE decorre de ele não ter sido concebido como sistema unificado, integrando módulos de características e arquiteturas diferentes, bem como do próprio conceito de sistema. Segundo Maria Esmeralda Ballestero Alvarez, em seu livro “Organização, sistemas e métodos” (vol. 1, São Paulo: McGraw-Hill, 1990),

> Sistema pode ser definido como um conjunto de elementos interdependentes que interagem com objetivos comuns formando um todo, e onde cada um dos elementos componentes comporta-se, por sua vez, como um sistema cujo resultado é maior do que o resultado que as unidades poderiam ter se funcionassem independentemente. Qualquer conjunto de partes unidas entre si pode ser considerado um sistema, desde que as relações entre as partes e o comportamento do todo sejam o foco de atenção.

Portanto, a definição dos elementos da solução SBE e daquilo que a constitui é baseada na visão desta Auditoria a esse respeito, não instituindo assim acepção categórica sobre o assunto. Os critérios utilizados foram a classificação indicada pela STI e refletida no CMBD, e a participação do elemento na realização do objetivo precípuo do SBE, qual seja, a gestão da venda e tarifação de créditos de transporte.

3.2.3.1. Contratos

Em resposta a questionamento desta Auditoria, a STI apresentou (fls. 07/22) os seguintes contratos e valores como relativos ao desenvolvimento, manutenção e atualização do SBE, totalizando o valor de R$ 129.604.197,90 investidos no sistema:

Quadro 2 – Relação de contratos

Contrato	Detalhes
2001/0060-01-00 (julgado irregular no TC 72.000.399/02-28 em 04.09.13)	Fornecedor: Digicon S/A Controle Eletrônico para Mecânica Objeto: A prestação, na forma de regime de execução por empreitada por preço global e de prestação continuada, de serviços técnicos especializados de planejamento, desenvolvimento e implantação de sistema informatizado para o processamento dos dados do sistema de cobrança automática do transporte público coletivo de passageiros. Responsável: José Aécio de Sousa Valor: R$ 4.310.382,24 Vigência: 05.10.01 a 04.10.04
2003/0067-01-00 (julgado irregular no TC 72.003.611/04-99 em 10.08.16)	Fornecedor: Digicon S/A Controle Eletrônico para Mecânica Objeto: Prestação de serviços técnicos especializados de desenvolvimento e implantação de software para processamento de dados do Sistema Central de Distribuição de créditos eletrônicos do Sistema de Bilhetagem Eletrônica – Projeto Bilhete Único – do transporte coletivo de passageiros do Município de São Paulo. Responsável: Não informado Valor: R$ 4.536.812,00 Vigência: 11.04.03 a 10.06.06
2004/0001-01-00 (julgado irregular no TC 72.003.611/04-99 em 28.06.11)	Fornecedor: Digicon S/A Controle Eletrônico para Mecânica Objeto: Prestação de serviços técnicos especializados de desenvolvimento e implantação do software de segurança do Sistema de Bilhetagem Eletrônica, aplicado às transações de recarga de créditos eletrônicos em redes online. Responsável: Não informado Valor: R$ 1.060.800,00 Vigência: 19.12.03 a 31.03.05
2005/0029-01-00 (julgado irregular no TC 72.000.481/06-30 em 05.04.17)	Fornecedor: Digicon S/A Controle Eletrônico para Mecânica Objeto: Prestação de serviços técnicos especializados de suporte técnico, operação assistida e manutenção evolutiva para o Sistema de Bilhetagem Eletrônica, com a finalidade de integrar o Bilhete Único, adotado pelo Sistema de Transporte Coletivo de Passageiros do Município de São Paulo. Responsável: Fernando Antônio Farias Valor: R$ 4.084.450,00 Vigência: 14.10.05 a 13.04.07
2006/0042-01-00 (analisado no TC 72.002.205/08-04 e acompanhado no TC 72.002.486/08-97, ambos não julgados)	Fornecedor: Digicon S/A Controle Eletrônico para Mecânica Objeto: Prestação de serviços técnicos especializados para atualização tecnológica dos componentes de segurança do Sistema de Bilhetagem Eletrônica e manutenção dos softwares aplicativos de todos os seus subsistemas incluindo fornecimento de equipamentos. Responsável: Fernando Antônio Farias Valor: R$ 3.105.142,28 Vigência: 21.11.06 a 20.11.09
2008/0359-01-00 (analisado no TC 72.002.208/08-94 e acompanhado no TC 72.002.485/08-24, ambos não julgados)	Fornecedor: Digicon S/A Controle Eletrônico para Mecânica Objeto: Prestação de serviços técnicos especializados de monitoramento e otimização do desempenho, evolução tecnológica e desenvolvimento de novas funcionalidades do sistema de recarga de créditos eletrônicos online e subsistemas interligados que constituem o Sistema de Bilhetagem Eletrônica do transporte público coletivo de passageiros do Município de São Paulo, integrado ao transporte metropolitano sobre trilhos – Metrô e CPTM. Responsável: Pedro José Pezzuto Gimene Valor: R$ 10.917.260,00 Vigência: 01.07.08 a 01.07.14
2012/0038-01-00 (edital julgado regular no TC 72.000.827/12-11 em 10.05.17; analisado no TC 72.012.943/17-24, não julgado)	Fornecedor: Consórcio Bilhete São Paulo (Tivit Terceirização de Processos, Serviços e Tecnologia S.A. / PC Service Tecnologia Ltda.) Objeto: Prestação de serviços técnicos integrados de processamento, armazenamento e comunicação de dados em ambiente de alta disponibilidade (Data Center), monitoramento da operação do sistema em regime ininterrupto, atualização tecnológica e manutenção dos softwares aplicativos, objetivando uma única solução integrada de Tecnologia da Informação do Sistema de Bilhetagem Eletrônica (Bilhete Único), atualmente implantado no sistema de transporte público coletivo de passageiros do Município de São Paulo, no Metrô e na CPTM. Responsável: Sergio Krichanã Rodrigues Valor: R$ 94.377.777,77 Vigência: 20.05.14 a 27.06.19

Fonte: SPTrans.

Além dos acima, identificamos também o seguinte contrato, cujos detalhes foram retirados do sistema Átomo/Radar:

Quadro 3 – Contrato adicional

Contrato	Detalhes
2014/0219-01-00	Fornecedor: Digicon S/A Controle Eletrônico para Mecânica Objeto: Prestação de serviços técnicos especializados de manutenção preventiva, corretiva e evolutiva dos softwares aplicativos que constituem o Sistema de Bilhetagem Eletrônica (Bilhete Único) do sistema de transporte público coletivo de passageiros do Município de São Paulo, integrado ao transporte metropolitano sobre trilhos – Metrô e CPTM. Responsável: Não informado Valor: R$ 7.211.573,64 Vigência: 01.07.14 a 30.06.18

Fonte: Átomo/Radar-TCM.

Conforme demonstra a listagem dos contratos, a atual versão do SBE foi quase integralmente desenvolvida pela Digicon, com o apoio da equipe da SPTrans. No tocante aos contratos vigentes, cumpre informar que o nº 2014/0219-01-00 envolve o suporte e manutenção preventiva, corretiva e evolutiva da versão atual do SBE, enquanto o 2012/0038-01-00 desenvolve-se em duas fases, englobando:

- Fase um: prestação de serviços de *Data Center* para o sistema informatizado;
- Fase dois: desenvolvimento de solução integrada de Tecnologia da Informação para o Sistema de Bilhetagem Eletrônica, ainda em testes.

Destacamos os seguintes problemas na relação de contratos acima:

1) Como foi desenvolvido em etapas, nas quais havia diferentes contratos relacionados, não é possível identificar o(s) contrato(s) responsável(is) por módulo do SBE, nem quais módulos foram modificados sob cada contrato. Mesmo depois de reiteradas requisições desta equipe, a STI também não foi capaz de informar os contratos que alteraram cada subsistema. Um agravante é que, em alguns períodos, havia mais de um contrato ativo para o SBE, ou seja, poderia haver contratos diferentes alterando o mesmo módulo ao mesmo tempo.

   Dessa forma, avaliamos que a SPTrans não possui controle adequado sobre os objetos entregues sob cada contrato relacionado ao Sistema de Bilhetagem Eletrônica, dificultando a estimativa dos valores investidos no mesmo, em infringência ao art. 67, *caput* e § 1º, da Lei Federal nº 8.666/93, que determinam o

acompanhamento e fiscalização da execução do contrato e o registro próprio de todas as ocorrências relacionadas (**Conclusão 4.2**).

2) A listagem identifica um responsável por contrato (em certos casos, nem isso), mas a Auditoria tomou conhecimento de que alguns tiveram mais de um gestor – inclusive, diferentes do apontado na relação fornecida. Por exemplo, o Processo Administrativo de Licitações e Contratos (PALC) do Contrato 2012/0038-01-00 indica que ele teve os seguintes gestores (fls. 26/28):

   - 06.14 a 01.17 – Pedro José Pezzuto Gimene
   - 01.17 a 07.17 – Selma Strublic
   - 07.17 em diante – Fernando Antônio Farias

   Assim, verificamos que a SPTrans também não possui controle adequado sobre os responsáveis pela gestão dos contratos relativos aos SBE no período em que este está em uso, em infringência ao art. 67, *caput* e § 1º, da Lei Federal nº 8.666/93, que determinam o acompanhamento e fiscalização da execução do contrato por representante da Administração especialmente designado (**Conclusão 4.3**).

Devido aos problemas anteriormente descritos na relação entre contratos e módulos, somente pudemos verificar que o contrato nº 2014/0219-01-00 prevê a propriedade e transferência do conhecimento para a SPTrans sobre a solução informatizada SBE decorrente dele. No entanto, observamos que, na prática, a propriedade dos sistemas é garantida à SPTrans independentemente de previsão editalícia, uma vez que ela possui os códigos-fonte, dados e demais elementos integrantes e/ou resultantes da solução informatizada SBE.

Avaliamos que também a transferência de conhecimento sobre o sistema está sendo efetivada independentemente de previsão contratual, vez que a equipe de Tecnologia da Informação da própria SPTrans é capacitada a operar e dar suporte aos diferentes módulos (ainda que a equipe da fornecedora seja necessária para isso, inclusive em razão da demanda). Assim, entendemos que a situação atual permite a independência da Administração Pública Municipal sobre seus fornecedores em relação ao SBE, ainda que essa independência não seja absoluta. Isso exige a manutenção de contrato com a

Digicon – que desenvolveu a versão atual do sistema – para suporte à SPTrans, o que onera ao erário municipal para a gestão do sistema.

Além disso, a escolha de agentes privados como fornecedores de um sistema crítico enseja cuidados adicionais por parte da Administração, preconizados na norma da Associação Brasileira de Normas Técnicas (ABNT) NBR ISO/IEC 27.005/2013, que aduz nas Diretrizes para implementação do item 15.1.3, “Cadeia de suprimento na tecnologia da informação e comunicação”:

> e) implementação de um processo para identificação dos componentes do serviço ou produto que são críticos para manter a funcionalidade e, portanto, requerem uma maior atenção e verificação quando construídos fora da organização, especialmente se o fornecedor principal terceirizar partes dos componentes do serviço ou produto com outros fornecedores;
>
> f) obtenção de garantia de que os componentes críticos e as suas origens podem ser rastreados ao longo de toda a cadeia de suprimento;
>
> [...]
>
> h) definição de regras para compartilhamento da informação com relação à cadeia de suprimento e quaisquer questões potenciais e compromissos assumidos entre a organização e os fornecedores;

Assim, a manutenção de tal contrato representa um risco aumentado para o Poder Público, uma vez que o SBE possui informações essenciais para a prestação do Serviço de Transporte Coletivo Público de Passageiros, e a ausência de controles adequados sobre o mesmo por parte da SPTrans permitiu o comprometimento da segurança dessas informações, conforme será visto no item 3.2.4.

É importante notar que, no momento, o SBE é objeto de um Edital Conjunto de Chamamento Público (nº 01/2017), lançado pela Secretaria Municipal de Desestatização e Parcerias (SMDP) em conjunto com o Governo do Estado de São Paulo (GESP), que visa obter estudos sobre o potencial de exploração de receitas acessórias ao mesmo, com vistas à concessão de sua gestão, operação e manutenção por eventual parceiro privado. Tal procedimento é parte do projeto denominado Sistema Único de Arrecadação Centralizada (SUAC), previsto na Lei Municipal nº 16.703/17 que “disciplina as concessões e permissões de serviços, obras e bens públicos que serão realizadas no âmbito do Plano Municipal de Desestatização (PMD)”.

3.2.3.2. Arquitetura

Atualmente, os subsistemas do SBE utilizam bancos de dados Oracle 10, executados em plataforma IBM AIX, e servidores de arquitetura Intel. Contudo, como não há unidade entre os diferentes sistemas, cada um possui sua própria base de dados, o que pode levar a duplicidades e inconsistências dentro do próprio sistema, diminuindo sua confiabilidade (**Conclusão 4.4**). A nova versão do SBE será fundamentada em uma visão holística, onde os módulos serão integrados e utilizarão uma base de dados única baseada em Oracle 12, o que pode mitigar este problema.

Além das distintas bases de dados e de ter sido construída em etapas, a versão atual do SBE foi desenvolvida em diferentes linguagens de programação – Java, C, *Active Server Pages* (ASP), o que contribui para a dificuldade de integrar seus módulos, uma vez que novas funcionalidades precisam ser pensadas de forma diferente para cada linguagem, além das possíveis limitações técnicas referentes à comunicação entre elas (ou da necessidade de criar interfaces para essa comunicação).

Segundo a STI, atuam hoje de forma direta na gestão da solução informatizada SBE 17 analistas do quadro de pessoal da SPTrans, além de 5 analistas da Digicon que trabalham junto à equipe própria (fl. 23). Detalhamos a seguir os módulos ou subsistemas que compõe a solução informatizada SBE:

Sistema Central de Processamento (SCP)

O Sistema Central de Processamento (SCP) é o módulo central do SBE, e tem a função de manter contas correntes que permitem o controle dos créditos efetuados nos cartões dos usuários e a sua utilização nos validadores eletrônicos instalados nos ônibus que compõem o Sistema de Transporte Coletivo Municipal e nas estações que integram o sistema sobre trilhos.

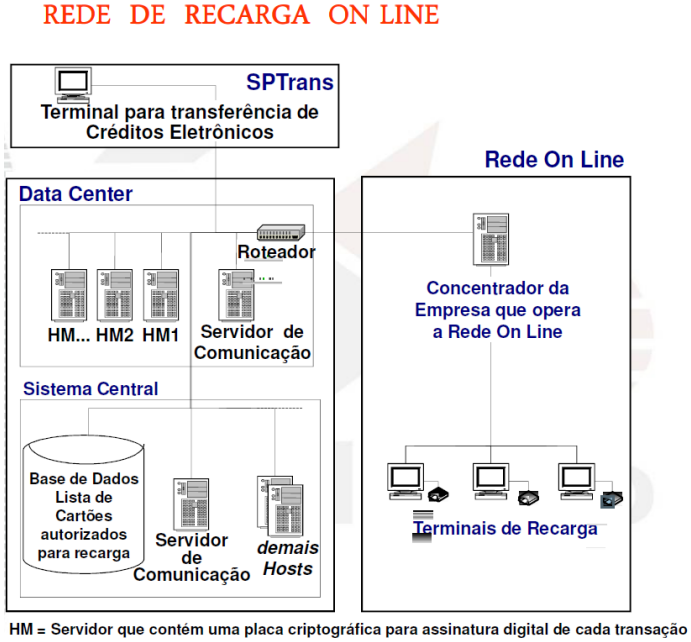
Também é responsável por ativar os cartões eletrônicos; disponibilizar informações para a câmara de compensação (*Clearing*), que servem de base para a remuneração dos operadores do Sistema de Transporte Coletivo de Passageiros; e, gerar todos os relatórios operacionais e gerenciais do SBE.

O SCP é um módulo *back-end*[1], composto por diversos processos que realizam os objetivos do subsistema. Esses processos são executados sob demanda, isto é, conforme uma programação predefinida ou pela necessidade eventual de seus usuários, e ele não possui telas para geração de consultas ou relatórios, não oferecendo opção de interação humana. O SCP foi desenvolvido nas linguagens Java e ASP.

Hyper Master **(HM)**

O *Hyper Master* (HM) – sistema de gerenciamento de recarga do BU – funciona como um "cartão-mestre" para o SBE, disponibilizando os créditos a serem distribuídos para os terminais de recarga responsáveis por comercializá-los. Para isso, utiliza placas criptográficas *Hardware Security Module* (HSM) da IBM – estão em uso 20 delas – para gerar esses créditos e também conferir a assinatura das requisições de recarga, gerada pelo SAM. Sua estrutura pode ser mais bem observada no diagrama abaixo:

Figura 4 – Arquitetura HM.



Fonte: SPTrans.

A cada solicitação de recarga, os terminais conectam-se ao HM diretamente ou através dos concentradores das redes de recarga a fim de obter créditos de transporte. O módulo SAM do terminal assina digitalmente as transações, cuja assinatura deve ser

[1] Parte do sistema responsável pela aplicação das regras de negócios.

verificada pelo HSM. Essa comunicação oferece um nível extra de segurança, garantindo que cada recarga seja validada e registrada no SBE. O HM processa 500 a 600 mil transações de recarga por dia nos dias úteis, passando de 1 milhão nos dias de pico, segundo a STI (fl. 23).

O HM é um módulo *back-end* e, devido a seu perfil de confidencialidade e segurança, não é acessível senão por outros subsistemas do SBE. Sua interface humana é através de um aplicativo de consulta que se conecta via *Transmission Control Protocol/Internet Protocol* (TCP/IP[2]) em determinada porta por meio da qual o HM recebe as solicitações, as executa e consulta/atualiza o banco de dados do sistema. Os relatórios do HM são gerados a partir do Discovery – sistema de apoio de *Business Intelligence* (BI) que acumula dados sumarizados e históricos – para não afetar a produção. O HM foi escrito em linguagem C.

Sistema de Cadastro e Atendimento (SCA)

É o componente de gerenciamento, cadastro e atendimento de todos os usuários do BU. Esse componente proporciona as funcionalidades relacionadas ao atendimento, registro de ocorrências, bloqueio de cartões, cadastramento de usuários, restituição de créditos, restauração de dados em cartões, etc.

O sistema consiste de dois módulos *Web* distintos, ambos escritos em linguagem Java e que utilizam a mesma base de dados – as bases de dados referentes a usuários Idosos e Pessoas com Deficiência (PcDs) são também carregadas nessa base para acesso direto – mas cada um com uma parcela das funcionalidades acima. São eles:

- SCA: é o *front-end*[3] original do sistema, que realiza tanto a gestão de processos e parâmetros do sistema, quanto a administração de usuários e perfis de acesso. Operacionaliza também alguns aspectos relacionados ao BU, tais como a gestão do cadastro de estudantes.
- Sistema de Atendimento (SA): é o *front-end* mais moderno, responsável pela maior parte das capacidades do sistema. É o único que continua sendo atualizado conforme as necessidades da SPTrans. Executa a gestão de boletos, interface com

[2] Conjunto de protocolos de comunicação entre computadores em rede.
[3] Parte do sistema responsável pela entrada de dados pelos usuários.

o Sistema de Controle de Óbitos (SisObi), consulta e gestão do cadastro de Idosos/PcDs, ocorrências de reconhecimento facial, e demais atividades de atendimento.

Além desses, existe uma aplicação *Web* desenvolvida em Java e C#, específica para tratamento das fraudes de uso indevido, relacionadas à funcionalidade de reconhecimento facial. Ela foi desenvolvida pelo Consórcio Bilhete São Paulo dentro do escopo do Contrato 2012/0038-01-00 como parte da nova versão do SBE, mas já está em utilização para suprir as necessidades correntes. A aplicação utiliza as imagens capturadas pelas câmeras instaladas na área do validador nos ônibus e as compara à registrada para o dono do Bilhete Único Especial usado; se ambas não corresponderem, o caso será apontado a um analista, que poderá confirmar a fraude e suspender o BU usado. Essas ocorrências são posteriormente gerenciadas no SA.

Sistema Central de Distribuição (SCD)

É o subsistema que gerencia a distribuição de créditos de transporte no SBE. Por exemplo, verifica se o tipo de recarga solicitada é possível no cartão em questão, se o cartão está válido, autoriza a liberação de créditos para prosseguir com a recarga e mantém a lista dos créditos já pagos e ainda não carregados nos BUs, além de controlar todas as vendas de vales-transporte e produtos adquiridos na Loja Virtual.

As empresas integrantes da rede de comercialização de vales-transporte (voltada a pessoas jurídicas), assim como a Loja Virtual da SPTrans (voltada a pessoas físicas) e os aplicativos de compras de créditos Comum e Estudante, captam os pedidos de compras de forma *online*. Esses pedidos ficam aguardando sua liquidação financeira, quando são então confirmados no SCD e seu crédito efetivado nos BUs através do HM. O pico de liquidações financeiras ocorre por volta do dia 30 de cada mês, enquanto o de efetivações no HM, entre os dias 1 e 5.

Quando a recarga é feita por meio de aplicativos de celular – que utilizam *Web services* disponibilizados pela Loja Virtual – ou postos de atendimento da própria SPTrans, o SCD também participa na liquidação das transações, contudo os créditos são efetivados no Bilhete Único através do HM.

O SCD possui um *front-end* para gerenciamento dos processos financeiros do sistema, como as ocorrências relacionadas à aquisição de créditos não refletidos no Bilhete Único, que são realizados com apoio da equipe do serviço 156 da Prefeitura de São Paulo. Porém, em sua maioria, é considerado um módulo *back*-end. Ele foi desenvolvido em linguagem ASP.

Loja Virtual (LV)

Esse sistema possibilita às empresas e pessoas físicas que têm empregados adquirirem vales-transporte na forma de créditos eletrônicos ou cotas temporais da SPTrans, bem como a aquisição de créditos e/ou cotas temporais para cartões dos tipos Comum e Estudante pelos demais usuários. É um instrumento de distribuição do VT, por atender e dar suporte a todas as empresas credenciadas, e acompanhar as vendas por elas realizadas.

A Loja Virtual compreende dois subsistemas para vendas, que são:

- LV: é o *front-end* responsável pela comercialização de vales-transporte.
- VCW (Venda *Web*): é o *front-end* encarregado da venda de créditos dos tipos Comum e Estudante.

A Loja Virtual, assim como os *Web services* disponibilizados por ela, foi desenvolvida em linguagem Java.

3.2.3.3. Integração com Outros Sistemas

Além desses, o SBE também interage com sistemas relacionados como o Sistema de Remuneração dos Operadores (SRO), fornecendo informações sobre o transporte de passageiros para remuneração dos concessionários, permissionários e prestadores de serviços de transporte do Município de São Paulo; Sistema Gerenciador de Garagem (SGG); dentre outros.

Em relação ao SGG, cabe informar que se trata não de um único sistema, mas de vários sistemas construídos por diferentes desenvolvedores – Prodata, Digicon, Empresa 1, Itacon e Transdata – segundo as especificações de funcionalidade e segurança da SPTrans para o SBE. Assim, cada operadora de transporte sobre pneus

adquiriu um deles para realizar as funções de garagem relacionadas à bilhetagem, como interface com validador para recebimento dos arquivos contendo registros de transações efetuadas ao longo do dia. O SGG também se integra ao SCP para envio das informações da garagem, assim como recebimento de atualizações de política tarifária e BUs cancelados – para essa integração, é utilizada criptografia forte AES.

A lista de BUs cancelados é também chamada Lista Vermelha, e é armazenada nos validadores pelo SGG quando o ônibus está recolhido à sua respectiva garagem. Caso seja apresentado um cartão ao validador que esteja nessa lista, não só ele será recusado, como o validador configurará todos os seus setores como inacessíveis – no jargão, "queimá-lo" – para que nunca mais possa ser utilizado. A Lista Vermelha é gerida por meio de outro sistema, sendo recriada diariamente, e um BU só não é reinserido nela a cada dia após ser "queimado". Outra forma de incluir BUs nessa lista é apresentada no subitem 3.7.2 - "Detecção de Anomalias por meio de logs (registros no Sistema)", do relatório do TC nº 72.001.889/08-28, que cuida dos resultados alcançados na execução do programa Bilhete Único, enfatizando a segurança do SBE.

Cumpre citar também o Sistema Integrado de Monitoramento (SIM), responsável pelo georreferenciamento de veículos da cidade de São Paulo, utilizado para controle, planejamento e operação da frota. O SIM foi criado com o intuito de automatizar a fiscalização da frota, planejar a operação em tempo real, entre outras demandas, permitindo a localização dos ônibus durante 24 horas do dia usando informações de *Global Positioning System* (GPS), registradas pelos módulos de localização *Automatic Vehicle Location* (AVL) presentes nos veículos.

Contudo, note-se que o SBE, a despeito da importância do papel que desempenha, não possui integração com o SIM. Isso ocasiona severas consequências, desde diferenças entre as informações registradas, como viagens registradas em horários e/ou sentido diferente em cada sistema, até a possibilidade de as empresas de transporte desconstituírem autuações por descumprimento de viagens usando dados do SBE, ainda que tais informações estejam em desconformidade com o SIM, que é a base para essas autuações; tal situação é analisada em detalhes no TC nº 72.012.310/17-06, que cuida da aplicação de multas aos operadores do Sistema Municipal de Transporte Público de Passageiros. Assim, recomenda-se o

desenvolvimento de integração entre os sistemas SBE e SIM, registrando no momento da utilização do validador as informações de localização correntes para posterior comparação (**Conclusão 4.7**).

3.2.4. Segurança do SBE

Existem três níveis de segurança quanto aos créditos de transporte no sistema informatizado SBE:

1) Cartão inteligente;

2) Módulos SAM;

3) *Data Center*.

Devido ao conhecimento de métodos para burlar a segurança dos cartões e permitir sua clonagem ou restauração de estado, conforme já apontado no TC nº 72.001.889/08-28, desde 2010 o modelo MIFARE Classic não pode ser considerado seguro, e o mesmo vale para o modelo Plus com nível de segurança SL1, isto é, que mantém compatibilidade com o algoritmo criptográfico do Classic.

Assim, concluímos que os cartões *smart card* dos modelos Classic e Plus com nível de segurança *Security Level* 1, são obsoletos (**Conclusão 4.5**) e, portanto, devem ter seu uso como Bilhete Único interrompido (**Conclusão 4.8**). O *upgrade* da versão Plus X – a ser realizado de modo presencial – ou a interrupção de seu suporte devem ser analisados em termos de custo/benefício. Por permitir configuração remota, a versão Plus EV1 pode em tese ser atualizada para o nível de segurança necessário dessa maneira, com menor custo e impacto para a Administração e também aos usuários do BU. Contudo, caso não seja possível atualizar o modelo Plus presencial ou remotamente, o suporte às unidades com nível de segurança SL1 também deverá ser interrompido.

Faz-se mister informar que, após a implantação da nova versão, a continuidade do suporte aos modelos Classic e Plus SL1 obrigará a SPTrans a manter em funcionamento a versão corrente do SBE, uma vez que a nova versão não está apta a atender a esses modelos (fl. 23). Assim, haverá duplo convívio entre as versões do

SBE enquanto o suporte a esses cartões se fizer necessário, onerando ao erário municipal pela manutenção de contrato exclusivo para esse fim. Esses fatores corroboram a brevidade da descontinuação dos modelos acima.

Por ora, a troca dos validadores visando aumento da segurança do sistema não surtiu o efeito esperado, uma vez que, enquanto as providências acima não forem tomadas em relação aos cartões compatíveis com o Classic, as vulnerabilidades decorrentes do algoritmo Crypto-1 continuarão existindo.

A partir de 2015/16, a SPTrans detectou que a segurança do SAM também havia sido comprometida, por meio da existência de recargas falsas (a serem detalhadas no item 3.2.5.2). Por ser baseada na confidencialidade da chave privada do algoritmo AES, o nível de fraudes por recarga falsa sugere que seu sigilo foi comprometido. Com isso, torna-se possível ativar módulos SAM falsos, capazes de atuar como terminais de recarga não oficiais.

Essa falha permite a “criação” de créditos no sistema sem comunicação com o SBE, alterando o estado do cartão e incluindo créditos sem solicitá-los ao HM – um risco mais extenso que o de clonagem ou restauração de estado, uma vez que atua sobre cartões válidos do sistema, o que dificulta sua detecção e impede a criação de bloqueios preventivos.

Uma possível forma de prevenir o problema seria impedir certas alterações de estado do cartão – como a recarga de créditos – de modo *offline*, sem devida comunicação ao SBE. Contudo, a SPTrans é responsável por elaborar e implantar soluções definitivas para os problemas decorrentes da quebra da segurança do cartão inteligente e do módulo SAM do sistema, além da identificação das suas causas (**Conclusão 4.9**).

É preciso notar que tal brecha não decorre da antiguidade do sistema ou do atraso da SPTrans em substituí-lo pela nova versão. A segurança do SAM deveria manter-se íntegra durante todo o ciclo de vida do sistema, e assim como seria possível (e desejável) que isso acontecesse, também o seria que ela fosse quebrada ainda que o sistema fosse novo (dada a ocorrência de condições para tal). É obrigação da SPTrans

e de suas contratadas oferecer as garantias necessárias de segurança e integridade para o Sistema de Bilhetagem Eletrônica a qualquer momento.

A segurança do *Data Center* refere-se às garantias que o sistema SBE oferece para que não seja possível alterar os créditos de transporte no sistema sem anuência da SPTrans, tais como controle de acesso, criptografia e segurança física. O *Data Center* onde o sistema opera foi inicialmente provido pela empresa Cobra Tecnologia, que subcontratou a Diveo para hospedagem das máquinas do parque tecnológico – um dos gestores do SBE durante o período abrangido, Sr. Pedro José Pezzuto Gimene, foi funcionário da Diveo antes de transferir-se à SPTrans. O contrato com a Cobra foi julgado irregular no TC nº 72.003.609/04-47 em 01.06.11, e sua execução acompanhada no TC nº 72.000.798/04-05, ainda não julgado.

Hoje, toda a estrutura é fornecida pela Tivit através do Contrato nº 2012/0038-01-00, que implantou, além da tecnologia necessária para execução e proteção do SBE, ferramentas de acompanhamento da operação do sistema para uso pela SPTrans, e melhorou a segregação de funções com ambientes separados para Produção, Desenvolvimento/Testes, Homologação e Garantia da Qualidade – o antigo contava somente com ambientes de Desenvolvimento e Produção. A segurança do *Data Center* pode ser considerada atualmente íntegra.

3.2.4.1. Sistema de Gestão de Segurança da Informação

O Sistema de Gestão de Segurança da Informação (SGSI) é uma abordagem sistemática para a gestão e proteção das informações de uma organização. O SGSI representa um conjunto de políticas, procedimentos e vários outros controles que definem as regras de segurança da informação em uma organização, e inclui estratégias, planos, políticas, medidas, controles, e diversos instrumentos usados para estabelecer, implantar, operar, monitorar, analisar criticamente, manter e melhorar a segurança da informação.

Segundo a STI, a SPTrans não possui SGSI implantado sobre o SBE, sendo que entre 2006 e 2008 iniciaram sua implantação com uma consultoria contratada (Fundação Aplicações de Tecnologias Críticas – Atech, cujo contrato foi julgado regular

no TC nº 72.000.796/04-80 em 16.04.14), que depois foi paralisada por motivos orçamentários. Esse SGSI foi analisado de forma indireta no TC 72.001.889/08-28, e o edital de contratação de empresa para continuidade de sua implantação julgado prejudicado no TC nº 72.001.305/08-05 em 11.11.15 por perda do objeto. No entanto, segundo eles próprios, procuram seguir as melhores práticas do mercado e seus parceiros tecnológicos (Digicon e Consórcio Bilhete São Paulo) seguem todas as normas pertinentes (fl. 23). Verificamos como alguns tópicos principais de um SGSI – a gestão de riscos e a gestão de mudanças – foram adotados pela empresa.

A gestão de riscos de segurança da informação é um dos processos do Sistema de Gestão da Segurança da Informação; ela ajuda a identificar os riscos que possam comprometer a confidencialidade, a integridade, a disponibilidade ou a autenticidade da informação, priorizando seu tratamento com base em critérios compatíveis com os objetivos institucionais. Esse tratamento pode compreender: aceitar, evitar, transferir, mitigar ou explorar os riscos, conforme a avaliação e a tolerância da instituição a eles.

Por sua vez, a gestão de mudanças busca garantir que os métodos e procedimentos mais adequados serão usados para o manuseio de todas as alterações no ambiente de Tecnologia da Informação. O objetivo é manter o controle sobre esse ambiente, a fim de minimizar o impacto de eventuais incidentes. As mudanças podem surgir de forma reativa em resposta a problemas ou exigências impostas externamente, como alterações legislativas, mas também podem ser uma ação proativa de busca da maior eficiência e eficácia na organização.

A STI informou que promove reuniões semanais com o Consórcio Bilhete São Paulo para avaliar os riscos da entrada em produção de alterações (fl. 23). Contudo, não identificamos um processo definido e dedicado de gestão de riscos dentro do SBE. A gestão de riscos hoje é feita como parte da gestão de mudanças; sempre que é necessária alguma alteração, ela segue um processo formal de mudança, porém a avaliação de seus riscos é feita pelos próprios solicitantes e aprovadores, que devem ser experientes na área de atuação a fim de estimá-los corretamente. Da mesma forma, os responsáveis pela área os são também pela avaliação e tratamento dos riscos inerentes a esta.

O exposto, considerando a norma ABNT NBR ISO/IEC 27.005/2013 e o grande volume de recursos financeiros envolvidos no SBE, demonstra a aplicação de uma política de gestão de riscos inapropriada, o que acarreta riscos à continuidade da prestação do serviço de transporte coletivo, em infringência ao art. 22 da Lei Federal nº 8.078/90 c/c art. 10 da Lei Federal nº 7.783/89 (**Conclusão 4.1**).

3.2.4.2. Administração de Usuários e Perfis de Acesso

O processo de administração de usuários e perfis de acesso do SBE inicia-se por meio de solicitações enviadas pelos gestores, em nome de seus usuários, ao responsável pela gestão de acesso dentro da Gerência de Operação e Segurança (GOS) da STI. A solicitação é operacionalizada pela GOS por meio do sistema SCD, e os dados para acesso são enviados manualmente aos solicitantes.

O SCD possui um módulo de controle de acesso que centraliza os usuários para os sistemas do SBE. Ao usuário é atribuído um *login* nominal. Posteriormente, quando acessa cada um dos subsistemas, esse se reporta ao SCD para verificar o perfil de acesso atribuído ao usuário e o recria em sua própria base de dados de acesso.

A exceção à regra é o Sistema de Cadastro e Atendimento. Como ele possui uma lista maior de usuários – por tratar-se de um sistema voltado ao gerenciamento do usuário final do serviço de transportes – e de perfis de acesso, sua gestão de acesso é feita pela área usuária, isto é, a Gerência de Atendimento (GAT) da Superintendência de Atendimento e Comercialização (SAC). Essa então operacionaliza a criação do *login* e perfil de acesso do usuário dentro do SCA.

Essa situação é prejudicial ao controle de acesso ao SBE, pois, devido à replicação de informações em diferentes sistemas, a base de usuários é inflada com registros e permissões duplicadas, que podem ser conflitantes entre si. A norma técnica ABNT NBR ISO/IEC 27.002, em sua edição 2013, preconiza inclusive nas Diretrizes para implementação do item 9.2.2, “Provisionamento para acesso de usuário”, a “manutenção de um registro central de direitos de acesso concedido ao ID de usuário para acessar serviços e sistemas de informação”.

Assim, recomenda-se que a administração de usuários e perfis de acesso seja revista para as versões posteriores do sistema, sobretudo a desenvolvida em razão do Contrato nº 2012/0038-01-00. A implantação da nova versão da solução informatizada SBE deve ser priorizada e patrocinada pela alta administração da SPTrans, uma vez que pode solucionar esse e outros problemas funcionais relacionados à versão corrente (**Conclusão 4.10**).

Além dos usuários e perfis de acesso aos subsistemas do SBE, existe também a gestão de acessos à estrutura de tecnologia desse sistema; isto é, é preciso controlar também os acessos aos servidores e bancos de dados onde tais subsistemas estão hospedados. Hoje, o gerenciamento desses acessos é feito pela Tivit, que cria todos os acessos de infraestrutura conforme as solicitações do responsável da GOS. Neste caso, os usuários da própria SPTrans recebem acesso em modo consulta aos servidores e bancos de dados de que necessitam. Por tratar-se de estrutura baseada em *softwares* considerados padrão de mercado e utilizados em diversos ambientes de alta criticidade, consideramos a aplicação desse modelo adequada para as necessidades do SBE.

3.2.4.3. Regras de Formação de Senhas

Segundo a STI, existe uma política rigorosa de permissão de acesso ao Sistema de Bilhetagem Eletrônica (fl. 23). Contudo, em nossas análises não identificamos uma política organizacional para a definição de senhas que abarque todos os subsistemas do SBE. Assim como cada subsistema tem sua própria base de usuários, também as regras de formação de senha variam entre eles, não existindo uma regra unificada para a criação de senhas no SBE. O exposto, considerando a norma técnica ABNT NBR ISO/IEC 27.002/2013, demonstra a aplicação de uma política de formação de senhas inapropriada.

Foram realizados testes de segurança no SCA, buscando identificar a possibilidade de acesso mediante *login* padrão (“*admin*”, “*user*”, etc.) e/ou sem senha ou com senhas fracas (“12345”, senha igual ao *login*, etc.). Nesses testes, não foram identificadas as situações acima. Contudo, tais testes não podem ser considerados exaustivos nem extensíveis para os demais subsistemas do SBE, uma vez que, como informado acima,

não existe uma política global para as senhas. Assim, a SPTrans deve definir e implantar uma política de formação de senhas unificada para todos os módulos do sistema SBE (**Conclusão 4.11**).

No caso dos acessos à estrutura de tecnologia do SBE, gerenciados pela Tivit, existe uma política de padronização de senhas definida pela própria contratada. Apesar de não termos analisado essa política, entendemos que sua existência atende ao menos parcialmente à necessidade de regras de formação de senhas, o que diminui o risco de acessos indevidos à aplicação.

3.2.4.4. Consistência de **Dados**

Outro ponto observado em relação ao SBE foi a existência de inconsistências entre os dados desse sistema e do Sistema Integrado de Monitoramento, como exarado no TC nº 72.012.310/17-06, que cuida da aplicação de multas aos operadores do Sistema Municipal de Transporte Público de Passageiros. Essas falhas permitem verificar que o SBE nem sempre reflete a realidade no que diz respeito às viagens realizadas pelo serviço de transporte sobre pneus. Apesar disso ser objetivo precípuo do SIM, o SBE também deve prezar pela veracidade de suas informações, até porque conforme TC supracitado tais elementos podem ser utilizados como contraprova quanto ao descumprimento de viagens não registradas pelo SIM.

Essas inconsistências decorrem, dentre outros motivos, dos procedimentos manuais realizados na operação do SBE. O sentido de cada viagem, bem como seu início e fim, são determinados por meio do chamado cartão de serviço, que é um cartão inteligente similar a um Bilhete Único, mas utilizado pelas prestadoras de serviços de transporte para definir essas características. Por tratar-se de operação manual e, portanto, sujeita a falhas, esse procedimento representa uma fragilidade com possíveis consequências severas do SBE. Recomenda-se a utilização dos dados do módulo de localização dos veículos (AVL) para preenchimento do sentido de cada viagem e de sua hora de início e fim no SBE, reduzindo o risco de falhas nessas informações (**Conclusão 4.12**).

3.2.4.5. Acesso Remoto

Conforme informado anteriormente, o SBE possui 5 *front-end* que oferecem a possibilidade de acesso tanto através de dispositivos conectados à rede interna da SPTrans (intranet), quanto externamente (internet). No caso dos acessos externos, é usado o seguinte endereço de acesso para cada uma das aplicações:

- SA: https://scapub.sbe.sptrans.com.br/sa/login.jsp
- SCA: https://scapub.sbe.sptrans.com.br/sca/operador/login.jsp
- LV: https://lv.sbe.sptrans.com.br/
- VCW: https://lv.sbe.sptrans.com.br/vcw/login.action
- SCD: http://scd.sbe.sptrans.com.br/scd_web/

Os sistemas SA, SCA, LV e VCW apresentam conexões seguras, o que significa que as informações enviadas ou recebidas por meio deles são privadas. Isso se deve ao fato de que tais módulos utilizam o protocolo de comunicação *Hyper Text Transfer Protocol Secure* (HTTPS), que funciona sobre uma camada adicional de segurança baseada no protocolo *Transport Layer Security* (TLS) versão 1.2, o que permite que seus dados sejam transmitidos por uma conexão criptografada e que se verifique a autenticidade do servidor e, opcionalmente, do cliente por meio de certificados digitais fornecidos por uma autoridade certificadora. Ainda que tal versão do TLS não seja imune a ataques, a segurança oferecida por ela é considerada satisfatória.

O SCD, por sua vez, apresenta uma situação de insegurança grave. Isso se deve a que esse subsistema utiliza o protocolo de comunicação *Hyper Text Transfer Protocol* (HTTP), que não oferece nenhum nível de criptografia ou autenticação e é, portanto, inseguro (**Conclusão 4.6**). Essa situação pode permitir que alguém não autorizado tenha acesso a quaisquer informações desse sistema durante seu tráfego, o que representa um risco significativo. Por tratar de informações financeiras e pessoais, o sigilo dos dados armazenados e trafegados por esse sistema é de grande importância, assim a SPTrans deve substituir o protocolo de comunicação utilizado no módulo SCD pelo HTTPS e bloquear o acesso via internet a esse sistema até que a troca seja feita (**Conclusão 4.13**).

3.2.5. Fraudes Detectadas

As principais fraudes detectadas no SBE resultam de questões de origem tecnológica – decorrentes da defasagem na solução informatizada SBE – e dividem-se nas categorias "clonagem de cartão" e "recarga falsa". Outros tipos incluem o uso indevido de Bilhete Único Especial – tratado pela aplicação desenvolvida pelo Consórcio Bilhete São Paulo – e o uso de múltiplas integrações de um único Bilhete por várias pessoas.

Recentemente, o jornal Metrô News publicou reportagem[4] sobre as fraudes no Bilhete Único. Conforme a reportagem:

> De acordo com os dados da SPTrans, a maior causa dos cancelamentos ocorre por conta de recargas falsas. Dos 374 mil cancelamentos, 254 mil ocorreram por conta deste tipo de crime. Os outros 120 mil são referentes à gratuidade utilizada por estudantes, idosos e deficientes. Segundo a SPTrans, não existe a mesma informação associada aos bilhetes de 2016. Também não foi informada a perda de arrecadação com estas ilegalidades.

Sobre o mesmo tema, O Estado de S. Paulo apresentou matéria[5] no ano passado, informando:

> Dados obtidos pelo Estado, por meio da Lei de Acesso à Informação (LAI), apontam que no ano passado houve 78.202 cartões apreendidos ou cancelados pelo sistema interno da São Paulo Transporte (SPTrans) por irregularidades e fraudes. Em 2015, 8,5 mil cartões haviam sido cancelados ante 3,8 mil em 2014 e 3,4 mil em 2013.

O aumento no número de fraudes detectadas denota a melhora na sua detecção pela SPTrans, mas também pode ser indicativa de crescimento desse tipo de ocorrência. Isto indica o potencial lesivo desse problema ao erário municipal e a importância de combatê-lo adequadamente pela SPTrans.

3.2.5.1. Clonagem de cartão

Este tipo consiste na utilização de cartões falsos, clones do BU fornecido pela SPTrans, compatíveis com o SBE mas que não realizam repasse de recursos para a inclusão de créditos de transporte. Assim, seu usuário pode utilizar o sistema de

[4] https://www.metronews.com.br/cidade/fraudes-cancelam-mais-de-370-mil-bilhetes-unicos
[5] http://sao-paulo.estadao.com.br/noticias/geral,fraude-no-bilhete-unico-aumenta-820-com-esquema-tipico-do-crime-organizado,70001725502

transporte sem remunerá-la por isso. Essa fraude é decorrente da quebra do algoritmo criptográfico Crypto-1, possível desde 2010.

Atualmente, são usados três modelos de cartão nesse tipo de fraude, todos vindos da China. Os modelos I e II já foram tratados no SBE, sendo bloqueados na primeira tentativa de uso – esse tipo de tratamento é chamado pela SPTrans de vacina. O modelo III, mais recente, continua em uso, e seu bloqueio está sendo providenciado pela SPTrans. Todavia, enquanto as vulnerabilidades decorrentes do Crypto-1 não forem extraídas do sistema, podem surgir novos modelos de clones.

No caso dos modelos não tratados, a garantia consiste nos controles de *back-office*. Por meio deles, o Bilhete Único – tanto original quanto clones – é bloqueado e seu usuário precisa comparecer à SPTrans para desbloqueá-lo, o que pode permitir a denúncia e identificação da origem dos clones. Contudo, muitas vezes o portador do cartão clonado sabe da fraude e não faz esse procedimento, deixando de usar o BU assim que bloqueado.

3.2.5.2. Recarga falsa

Na categoria acima, incluem-se as realizadas por máquinas capazes de alterar o conteúdo do Bilhete Único para incluir créditos de transporte, mas que não fazem repasse de recursos para o SBE. Neste caso, os cartões são originais, porém os créditos carregados não se refletem em arrecadação. O usuário dessas recargas também pode utilizar livremente o sistema de transporte, porém, como o cartão que utiliza é original, só pode ser bloqueado quando a SPTrans detecta que o consumo de créditos por esse BU é maior que a soma das recargas realizadas.

No caso desse cenário, o portador do cartão também reconhece muitas vezes que está incorrendo em fraude, uma vez que o valor da recarga é menor do que o oficial praticado pela municipalidade. Não obstante, o Bilhete Único utilizado nela normalmente é o anônimo, que não permite a identificação do usuário. Quando se trata

de bilhete personalizado, o usuário evita incorrer nessa fraude pelo risco de ser identificado e penalizado. Ainda sobre o assunto, o *site* G1[6] informou:

> Nas estações da Companhia Paulista de Trens Metropolitanos (CPTM), vendedores irregulares são flagrados vendendo passagens mais baratas perto das catracas. Após o usuário efetuar o pagamento, eles acompanham a pessoa até a catraca, e passam o bilhete único.

O SBE conta com os controles de *back-office* para verificar e suspender os cartões na condição retrocitada. Contudo, isso abre brecha para o uso de grande quantidade de créditos não remunerados até o efetivo bloqueio. Esse problema decorre da quebra da confidencialidade do SAM em 2015/16, tendo seu risco aumentado pelo fato de que não é feita verificação de fraudes nos créditos de transporte em períodos curtos.

3.2.5.3. Políticas de prevenção

As vulnerabilidades do SBE são parcialmente mitigadas pelos processos de conciliação executados sobre os créditos de transporte – referimo-nos a esses como controles de *back-office*. Eles comparam os créditos utilizados por Bilhete Único com os valores recebidos por eles via HM. Caso haja divergência, o cartão é suspenso, exigindo que o usuário compareça a um posto de atendimento para sanar o problema. Os controles de *back-office* também podem ser ativados por situações normais, tais como recargas realizadas com sucesso, mas canceladas indevidamente no HM – nesse caso, o tratamento é confirmar o montante carregado no HM. Existem duas limitações em relação a essa abordagem:

1) A detecção de fraude *a posteriori* – isto é, por seus efeitos – faz com que o prejuízo decorrente não possa ser totalmente evitado. Alguns equipamentos de leitura, tais como validadores embarcados em ônibus, informam ao SBE sobre os usos uma vez ao dia quando o veículo retorna à garagem, majorando o impacto do problema.

2) Caso o cartão já esteja carregado com uma quantia quando receber a recarga falsa, continuará sendo usado normalmente, e a fraude só será detectada quando o valor consumido ultrapassar o recebido, dificultando ainda mais a investigação de sua origem.

[6] https://g1.globo.com/sp/sao-paulo/noticia/vendedores-fraudam-bilhete-unico-e-fazem-venda-irregular-mais-barata-em-estacoes-da-cptm.ghtml

Uma possível melhoria na prevenção a fraudes seria a disponibilização de internet móvel em todos os pontos onde há equipamentos de leitura do Bilhete Único, e a verificação de fraudes em períodos curtos (por exemplo, a cada 15 minutos) a partir desses dados como já acontece nas estações do Metrô e da CPTM, o que diminui o risco dessas acontecerem, assim como seu impacto (**Conclusão 4.14**).

Outras abordagens adotadas pela SPTrans para mitigar o impacto de problemas relacionados à segurança do SBE são restrições à venda de Bilhete Único, permitindo a compra de um só por usuário; a identificação do usuário de cada BU; e a definição de políticas mais restritivas de tarifação para cartões sem identificação.

Ademais, como determinado no TC nº 72.012.310/17-06, recomenda-se que a SPTrans proceda à auditoria do SBE e também do sistema correlato SIM, a fim de aumentar a credibilidade desses sistemas e evitar o desperdício de recursos humanos e materiais, já que uma vez auditados, a possibilidade de fraudes decorrentes dos mesmos tende a diminuir consideravelmente (**Conclusão 4.15**).

3.2.6. Responsáveis

Nome	Cargo
José Carlos Nunes Martinelli	Diretor-Presidente – SPTrans (anterior) – até 20.03.18
Sergio Krichanã Rodrigues	Diretor de Gestão da Receita e Remuneração – SPTrans (durante período abrangido)
Sandro Augusto Cuoghi	Diretor de Gestão da Receita e Remuneração – SPTrans
José Aécio de Souza	Superintendente de Atendimento e Comercialização – SPTrans
Pedro José Pezzuto Gimene	Superintendente de Tecnologia da Informação – SPTrans (durante período abrangido)
Fernando Antônio Farias	Superintendente de Tecnologia da Informação – SPTrans
Paulo Cézar Shingai	Diretor-Presidente – SPTrans – a partir de 21.03.18

4. CONCLUSÃO

O Sistema de Bilhetagem Eletrônica é um sistema maduro e estável, até por estar em uso há vários anos. Apesar de não ter sido objetivo desta auditoria avaliar se o sistema atende a regras de negócio específicas ou detectar a existência de erros (*bugs*), nenhum evento desabonador foi constatado ao longo do trabalho. Contudo, o sistema se ressente das deficiências do modelo de integração utilizado e da antiguidade do projeto, que não permitem sua evolução para atender às necessidades funcionais e de segurança atuais.

Considerando o volume monetário envolvido na gestão financeira do Sistema de Transporte Coletivo Urbano de Passageiros do Município de São Paulo e a quantidade de fraudes detectadas no serviço, a materialidade do risco dessas fraudes é bastante significativa, podendo impactar a eficiência e continuidade de um serviço essencial à população, além do erário municipal. Por serem decorrentes principalmente da obsolescência do Sistema de Bilhetagem Eletrônica e dos modelos de Bilhete Único ainda em uso, esses problemas demandam atuação urgente da Administração Pública Municipal (na figura da SPTrans) para corrigi-los.

Diante dos exames efetuados com a finalidade de verificar o Sistema de Bilhetagem Eletrônica, tanto acerca de sua integridade quanto em relação às funcionalidades, destacamos:

Irregularidades Identificadas

4.1. A política de gestão de riscos adotada no Sistema de Bilhetagem Eletrônica demonstra-se inapropriada, o que acarreta riscos à continuidade da prestação do serviço de transporte coletivo, em infringência ao art. 22 da Lei Federal nº 8.078/90 c/c art. 10 da Lei Federal nº 7.783/89 (subitem **3.2.4.1**);

4.2. A SPTrans não possui um controle adequado sobre os objetos entregues sob cada contrato relacionado ao Sistema de Bilhetagem Eletrônica, em infringência ao art. 67, *caput* e § 1º da Lei Federal nº 8.666/93 (subitem **3.2.3.1**);

4.3. A SPTrans também não possui um controle adequado sobre os responsáveis pela gestão dos contratos relativos ao Sistema de Bilhetagem Eletrônica, em infringência ao art. 67, *caput* e § 1º da Lei Federal nº 8.666/93 (subitem **3.2.3.1**);

4.4. Os módulos do Sistema de Bilhetagem Eletrônica possuem bases de dados distintas, o que pode levar a duplicidades e inconsistências dentro do próprio sistema, diminuindo sua confiabilidade (subitem **3.2.3.2**);

4.5. Os cartões *smart card* dos modelos Classic e Plus com nível de segurança *Security Level* 1 usados como Bilhete Único são obsoletos (subitem **3.2.4**);

4.6. O protocolo de comunicação *Hyper Text Transfer Protocol* utilizado pelo Sistema Central de Distribuição para acesso remoto é inseguro (subitem **3.2.4.5**);

Propostas de Determinações

4.7. Desenvolver integração entre o Sistema de Bilhetagem Eletrônica e o Sistema Integrado de Monitoramento, registrando no momento da utilização do validador as informações de localização correntes para posterior comparação (subitem **3.2.3.3**)**;**

4.8. Interromper o uso dos cartões *smart card* dos modelos Classic e Plus com nível de segurança *Security Level* 1 (subitem **3.2.4**);

4.9. Elaborar e implantar soluções para os problemas decorrentes da quebra da segurança do cartão inteligente e do módulo *Security Access Module* do Sistema de Bilhetagem Eletrônica, além da identificação das suas causas (subitem **3.2.4**);

4.10. Priorizar e patrocinar pela alta administração da SPTrans a implantação da nova versão do Sistema de Bilhetagem Eletrônica, que pode solucionar diversos problemas relacionados à versão corrente (subitem **3.2.4.2**);

4.11. Definir e implantar uma política de formação de senhas unificada para todos os módulos do Sistema de Bilhetagem Eletrônica (subitem **3.2.4.3**);

4.12. Utilizar os dados do módulo de localização dos veículos para preenchimento do sentido de cada viagem e de sua hora de início e fim no sistema, reduzindo o risco de falhas nessas informações (subitem **3.2.4.4**);

4.13. Substituir o protocolo de comunicação utilizado pelo Sistema Central de Distribuição pelo *Hyper Text Transfer Protocol Secure* e bloquear o acesso via internet a esse sistema até que a troca seja feita (subitem **3.2.4.5**);

4.14. Disponibilizar internet móvel em todos os pontos onde há equipamentos de leitura do Bilhete Único e realizar a verificação de fraudes em períodos curtos (por exemplo, a cada 15 minutos) a partir desses dados (subitem **3.2.5.3**);

4.15. Auditar o Sistema de Bilhetagem Eletrônica e o Sistema Integrado de Monitoramento e, se possível, certificá-los a fim de conceder maior credibilidade a e evitar o desperdício de recursos humanos e materiais (subitem **3.2.5.3**).

Em 16.04.18

ADRIANO ZAMBON
Agente de Fiscalização