

Processo	- TC/010140/2019
Auditada	- São Paulo Transporte S.A.
Objeto	- Auditoria Extraplano – Sistema de Bilhetagem Eletrônica – Verificar o sistema antifraude existente no Sistema de Bilhetagem Eletrônica com a indicação das fraudes detectadas e seus reflexos financeiros

42ª Sessão Ordinária Não Presencial

AUDITORIA EXTRAPLANO. SPTRANS. Verificar o sistema antifraude existente no Sistema de Bilhetagem Eletrônica – SBE, com a indicação das fraudes detectadas e seus reflexos financeiros. 1. A venda de créditos fictícios, possibilitada pela quebra da chave de segurança dos cartões, e a utilização fraudulenta de gratuidades continuam existindo em números expressivos. 2. Registrados boletins de ocorrência indicando que houve indiciados por fraudes. 3. Prejuízo ao erário, decorrentes de condutas criminosas de fraude ao sistema de bilhetagem eletrônica. 4. Constatada ações de gestão para mitigar a ocorrência de fraudes, porém evidenciada que a repressão a essa conduta criminosa não foi totalmente debelada, continuando a existir números expressivos de condutas fraudulentas. CONHECIDA. DETERMINAÇÕES. 1. Desenvolver ferramentas e tabelas de Data Warehouse que permitam a apuração do impacto financeiro das fraudes detectadas de forma continuada e tempestiva. 2. Desenvolver integração entre o SBE e o Sistema Integrado de Monitoramento. 3. Interromper o uso dos cartões smart card dos modelos Classic e Plus com nível de segurança Security Level 1. 4. Elaborar e implantar soluções para os problemas decorrentes da quebra da segurança do cartão inteligente e do módulo Security Access Module do SBE. 5. Disponibilizar internet móvel em todos os pontos onde há equipamentos de leitura do Bilhete Único e realizar a verificação de fraudes em períodos curtos. 6. Adotar medidas de controle no procedimento de alteração da fotografia do cadastro dos estudantes a fim de mitigar o risco de utilizações indevidas. Votação unânime.

ACÓRDÃO

Vistos e relatados estes autos, dos quais é Relator o Conselheiro DOMINGOS DISSEI.

ACORDAM os Conselheiros do Tribunal de Contas do Município de São Paulo, à unanimidade, de conformidade com o relatório e voto do Relator, tendo em conta as inúmeras ações dos gestores para efetivação da segurança do Sistema de Bilhetagem Eletrônica contra condutas fraudulentas e criminosas na sua utilização, em conhecer da auditoria, para fins de registro.

ACORDAM, à unanimidade, em acolher as conclusões do relatório da Auditoria constantes dos itens:

- 4.7 (A existência de cartões fraudados não incluídos na Lista Vermelha, e de cartões inseridos em Lista Vermelha capazes de utilizar o serviço de transporte coletivo, representa falhas graves que requerem medidas imediatas da SPTrans para sua solução);
- 4.8 (O Ciclo de Gestão de Riscos adotado no Sistema de Bilhetagem Eletrônica demonstra-se inapropriado, o que acarreta riscos à continuidade da prestação do serviço de transporte coletivo, em infringência ao art. 22 da Lei Federal 8.078/90 c/c art. 10 da Lei Federal 7.783/89);
- 4.10 (Os cartões smart card dos modelos Classic e Plus com nível de segurança Security Level 1 usados como Bilhete Único são obsoletos) e
- 4.11 (Fragilidade de controle no procedimento de alteração da fotografia do cadastro dos estudantes permitindo utilizações indevidas dos Cartões),

ACORDAM, à unanimidade, em acolher as "**Propostas de Determinações**" constantes dos itens 4.12 a 4.16 e 4.18.

Vencido o Conselheiro ROBERTO BRAGUIM – Revisor, consoante declaração de voto apresentada, quanto à proposta de determinação à SPTrans para que instaure procedimento interno para investigar os prejuízos sofridos pelo erário.

Vencido, também, o Conselheiro MAURÍCIO FARIA, nos termos de sua declaração de voto apresentada, quanto à proposta de determinação à Origem para que apresente um Plano de Ação para o cumprimento das determinações referidas.

ACORDAM, à unanimidade, determinar, cumpridas as formalidades legais, o arquivamento dos autos.

Participaram do julgamento os Conselheiros ROBERTO BRAGUIM – Revisor, MAURÍCIO FARIA e JOÃO ANTONIO.

São Paulo, 19 de abril de 2023.

EDUARDO TUMA – Presidente
DOMINGOS DISSEI – Relator

/smv

TC 010.140/2019

Egrégio Plenário

Em julgamento a Auditoria Extraplano realizada no Sistema de Bilhetagem Eletrônica (SBE) da SPTrans objetivando verificar o sistema antifraude desenvolvido pela empresa e o impacto financeiro das fraudes detectadas.

A Coordenadoria V da Subsecretaria de Fiscalização e Controle teceu considerações sobre as anteriores fiscalizações e apresentou as seguintes justificativas para a realização de uma nova e que lançam luzes e apropriadas informações sobre o tema:

“O Sistema de Bilhetagem Eletrônica (SBE) já foi objeto de auditoria por parte deste Tribunal de Contas. Na Auditoria Programada realizada no ano de 2007 (TC nº 72.000.368.07-09), verificou-se os controles de detecção de fraudes, evidenciando-se que o Poder Público em conjunto com a SPTrans deveriam adotar medidas urgentes visando minimizá-las, pois as irregularidades detectadas oneram os cofres públicos por conta de elevados subsídios para equilíbrio financeiro do Sistema Municipal de Transporte Coletivo, além de penalizar os usuários que efetivamente pagam a tarifa. Os principais tipos de fraudes detectados à época foram: em face de alterações mecânicas (validador, catraca, etc.); uso indevido do Bilhete Único (diversas possibilidades) e comércio irregular de fraudes.

Com base nessa Auditoria foi exarada no Acórdão relativo às contas do Executivo Municipal de 2006 a seguinte Determinação: “Adote medidas visando minimizar as diversas ocorrências de fraudes na utilização do cartão do tipo ‘Comum’ e para evitar o uso indevido de cartões de ‘gratuidades’ ”. Em 2008, uma nova auditoria programada (TC nº 72.001.889.08-28) foi realizada para verificação dos riscos inerentes ao Sistema de Bilhetagem Eletrônica, notadamente quanto: a segurança do Bilhete Único, a gestão de Segurança da Informação, a apreciação da vulnerabilidade específica encontrada, a fiscalização por ferramentas de sistema e detecção de uso irregular e as fraudes identificadas pela fiscalização. Nessa Auditoria, concluiu-se que estava em fase de implementação um Sistema de Gestão da Segurança da Informação, mas o núcleo central desse Sistema, denominado Ciclo de Gestão de Risco, não estava em funcionamento. Além disso, recomendou-se que a SPTrans abordasse imediatamente os riscos de clonagem dos cartões de Bilhete Único. Dessa forma, sugeriu-se à época que a SPTrans empregasse seus próprios efetivos na avaliação dos riscos de

fraude.

No RAF da SPTrans de 2008, foi incluída a seguinte proposta de determinação para a SPTrans (TC nº 72.000.938.09/87 - ainda pendente de julgamento): “Implantar Sistema de Gestão da Segurança da Informação, em face das ocorrências de fraude na utilização do cartão “Bilhete Único”, além de avaliar os riscos envolvidos quanto à possibilidade de clonagem dos cartões”.

Mais recentemente (2017), foi determinada a realização de uma Inspeção (TC nº 72.012.936/17-69) para análise atualizada da forma com que os serviços de bilhetagem eletrônica do Sistema de Transporte Coletivo do Município de São Paulo estão sendo prestados.

O resultado dessa Inspeção pode ser assim sintetizado:

- 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.*
- 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;*
- 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 8.666/93;*
- 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;*
- 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;*
- Os cartões smart card dos modelos Classic e Plus com nível de segurança Security Level 1 usados como Bilhete Único são obsoletos;*
- O protocolo de comunicação Hyper Text Transfer Protocol utilizado pelo Sistema Central de Distribuição para acesso remoto é inseguro.*

Ainda quanto ao assunto, foi noticiado pela imprensa que o Metrô contratou a empresa Ernst & Young (16.04.19) para realizar uma auditoria e verificar porque houve redução na receita em vendas de créditos do Bilhete Único. Uma das suspeitas alegadas é que as fraudes no Sistema de Bilhetagem Eletrônica (SBE) tenham motivado o prejuízo.

Diante desse quadro, propomos a V. Exa. a realização de uma auditoria extraplano com o objetivo de verificar o sistema antifraude existente no Sistema de Bilhetagem Eletrônica (SBE) com a indicação das fraudes detectadas e seus reflexos financeiros. Essa auditoria será composta por integrantes do Grupo de Tecnologia de Informação da SFC e por auditores da Coordenadoria V. O relatório conterá, ao menos, os seguintes pontos:

- 1. a verificação da segurança do banco de dados*
- 2. o mapeamento das fraudes conhecidas;*
- 3. o impacto financeiro das fraudes detectadas;*
- 4. a efetividade dos sistemas antifradude;*
- 5. a sugestão de novos procedimentos;*
- 6. a verificação da compatibilidade do sistema financeiro com o sistema operacional.”*

Autorizada, a nova fiscalização foi realizada e a metodologia utilizada consistiu em planejamento, execução do trabalho, elaboração de relatório e recomendação de ações corretivas.

No Planejamento houve as seguintes fases e atividades: **1ª Fase** – Conhecer todo o Sistema de Bilhetagem Eletrônica (SBE), com o intuito de verificar fragilidades nos procedimentos de emissão de Cartões e Créditos Eletrônicos; comercialização e distribuição; controle do validador e assinaturas dos dados. **2ª fase** – Verificar as medidas antifraude adotadas pela SPTrans no Sistema de Bilhetagem Eletrônica. **3ª Fase** – Impacto financeiro das fraudes detectadas no sistema de remuneração.

Destacou-se que o trabalho buscou discriminar o modo de utilização do sistema de transporte coletivo de ônibus no Município em função do tipo de pagamento, se em dinheiro ou crédito eletrônico (vale comum, vale transporte, entre outros). Tudo isso com vistas a analisar o esforço empregado no combate à corrupção de determinada modalidade de pagamento e sua relevância frente ao sistema.

A Equipe de Fiscalização apresentou, então, a participação de cada modalidade de pagamento no sistema (*gratuidade, integração, temporal, estudante, vale-transporte, comum, dinheiro*) buscando constatar o foco das

medidas de controle por parte da SPTrans quanto às gratuidades uma vez que elas representam dinheiro pago pelo Município em contrapartida a obrigações legais de cunho social. Realçando que esse perfil faturou, no período de janeiro a outubro de 2019, R\$ 511.501.798 (24%).

Do trabalho de auditoria realizado, a Equipe de Fiscalização apresentou aprofundado e pormenorizado relatório em que se objetivou, na **1ª Fase** – Conhecer todo o Sistema de Bilhetagem Eletrônica (SBE), com o intuito de verificar fragilidades nos procedimentos de emissão de Cartões e Créditos Eletrônicos; comercialização e distribuição; controle do validador e assinaturas dos dados; na **2ª fase** – Verificar as medidas antifraude adotadas pela SPTrans no Sistema de Bilhetagem Eletrônica; na **3ª Fase** – Impacto financeiro das fraudes detectadas no sistema de remuneração.

O Sistema de Bibletagem Eletrônica – SBE integra-se com outros, como, por exemplo, o Sistema de Remuneração dos Operadores (SRO), que fornece informações sobre o transporte de passageiros para remuneração dos concessionários, permissionários e prestadores de serviços de transporte do Município de São Paulo e o Sistema Gerenciador de Garagem (SGG), que é um “sistema externo ao SBE, fornecido 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.

Sobre a Gestão do SBE, a Equipe de Auditoria pontou que é gerido pelo Convênio SBE, composto pelos seis partícipes: SPTrans, Metrô, CPTM, Via Quatro, Move São Paulo e Vem ABC. 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).

Quanto a arquitetura, esclareceu que o que o SBE compõe-se de módulos ou subsistemas, que se integram com realização de diferentes tarefas, destacando-se: Sistema Central de Processamento (SCP); Hyper Master (HM) – subsistema de gerenciamento de recarga dos cartões; Sistema de Cadastro e

Atendimento (SCA) – módulo de gestão, cadastro e atendimento dos usuários; Sistema Central de Distribuição (SCD) – subsistema de distribuição de créditos de transporte; Loja Virtual (LV) – subsistema de venda de créditos de transporte.

A Auditoria observou que *“como não há unidade entre os diferentes sistemas, cada um possui sua própria base de dados, o que pode levar à duplicidades e inconsistências dentro do próprio sistema, diminuindo sua confiabilidade. O SBE armazena cerca de 13 milhões de transações diárias dos cartões do tipo Bilhete Único, o que perfaz mais de 300 milhões de transações mensais, e cerca de 4 bilhões de transações anuais (período máximo armazenado na base de dados de usos de cartões atualmente)”*. E que, *“em análise à base de dados do Data Warehouse (DW), não foram identificadas tabelas contendo informações atualizadas que permitam a apuração do impacto financeiro das fraudes detectadas”*.

Destacou que há uma lista de Bilhetes Únicos cancelados, também denominada “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. Essa Lista Vermelha é gerida por meio de outro sistema, sendo recriada diariamente conforme a lista de cartões identificados com fraude”.

A Equipe de Fiscalização assinalou, outrossim, que o SBE não possui integração com 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 permite 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”.

A segurança do Sistema de Bilhetagem Eletrônica foi descrita no TC 1.889/08. A partir desses estudos, a Auditoria fez as seguintes observações:

Devido ao conhecimento de métodos para burlar a segurança dos cartões e permitir sua clonagem ou restauração de estado, já apontados no TC nº 72.001.889/08-28, o modelo MIFARE Classic deixou de ser considerado seguro a partir de 2010, e o mesmo vale para o modelo Plus com nível de segurança Security Level 1 (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 e, portanto, devem ter seu uso como Bilhete Único interrompido. 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 poderia em tese ser atualizada para o nível de segurança necessário, com menor custo e impacto para a Administração e também aos usuários do Bilhete Único.

Nesse sentido, a SPTrans, por meio de sua Superintendência de Atendimento e Comercialização (SAC), informou em requisição desta Auditoria que as seguintes providências estão sendo tomadas para eliminar os cartões Classic (1K) ainda em uso no SBE (peça 8 – fl. 1):

a) Iniciada a troca dos cartões de gratuidade, desde o dia 04/09/2019 os cartões para idosos são emitidos somente no modelo Mifare Plus, reduzindo, paulatinamente, a circulação de cartões de idosos emitidos na tecnologia antiga.

b) As alterações para permitir que os cartões de PcD também passem a ser emitidos na nova tecnologia já está em fase final de desenvolvimento do sistema.

c) O limite de créditos acumulados dos cartões emitidos antes de 2014, na tecnologia Classic, foi reduzido de R\$ 350,00 para apenas R\$ 43,00 na carteira comum. O próximo passo será a gradativa retirada de circulação desses cartões. A intensidade e o volume de cada etapa levará em conta a necessidade de ampla divulgação; o suficiente para que os usuários tenham a compreensão da mudança e façam a troca de seus cartões por novos com o menor transtorno possível.

Após a implantação da nova versão do SBE do Contrato nº 2012/0038-01-00, 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. 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 necessidade da descontinuação dos modelos Classic e Plus SL1.

Por ora, a troca dos validadores visando aumento da segurança do sistema não surtiu o efeito esperado, uma vez que, enquanto os cartões Classic e Plus com nível de segurança SL1 estiverem em uso, 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 (detalhadas no subitem 3.2.3.2). Por ser baseada na confidencialidade da chave privada do algoritmo Advanced Encryption Standard (AES) utilizada pela SPTrans, 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 violação 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 – sem a devida comunicação ao SBE. Outra proposta seria a utilização de ferramentas de inteligência artificial (machine learning) para analisar os cadastros e transações dos cartões em busca de padrões de fraude. Assim, recomendamos que a SPTrans elabore e implante soluções para os problemas decorrentes da quebra da segurança do cartão inteligente e do módulo SAM do sistema (Conclusão 4.15).

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.

Atualmente, 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 Data Center anterior contava somente com ambientes de Desenvolvimento e Produção.

Com relação à gestão de mudanças, ou seja, o gerenciamento de toda e qualquer alteração no banco de dados, verificamos que os funcionários da SPTrans obedecem a um procedimento rígido quando da alteração do banco de dados. Primeiro, via software, é realizada a solicitação de mudanças, depois, após autorização prévia é que a alteração será executada no banco de dados. Ressalta-se que neste processo também se evidencia a segregação de função, uma vez que aquele que autoriza é diferente daquele que solicita”.

Sobre um sistema de gestão de segurança da informação, consoante anotado pela Auditoria, “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 796/04-80, em 16.04.14, paralisada por motivos orçamentários. Esse SGSI foi analisado de forma indireta no TC

1.889/08-28, e o edital de contratação de empresa para continuidade de sua implantação julgado prejudicado no TC 1.305/08-05, em 11.11.15 por perda do objeto”.

As principais fraudes detectadas no Sistema de Bilhetagem Eletrônica, no período de 2008 a 2019, consoante relatou a Auditoria, “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”.¹

Sobre a ação criminoso de “clonagem de cartões”, a Auditoria fez as seguintes observações:

“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 transporte sem remunerá-lo 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”.

E sobre a “recarga falsa”, a Auditoria anotou:

¹ Jornal Metrô News:

“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”. <https://www.metronews.com.br/cidade/fraudes-cancelam-mais-de-370-mil-bilhetes-unicos>

“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 informou³:

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. ³ <https://g1.globo.com/sp/sao-paulo/noticia/vendedores-fraudam-bilhete-unico-e-fazem-venda-irregular-mais-barata-em-esta-coes-da-cptm.ghtml>

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”.

O relatório aborda a mitigação da vulnerabilidade do Sistema de Bilhetagem Eletrônica mediante “processos de conciliação executados sobre os créditos de transporte – 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: 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. 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. 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”. E anotou também “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”.

Sobre a efetividade do sistema antifraude, a Auditoria assinalou que “não foram observados indícios de fraudes relacionadas à questão do cadastro dos cartões do tipo Bilhete Único no SBE”.

Sobre o “reconhecimento facial” fez as seguintes anotações:

“O procedimento de reconhecimento facial é uma ferramenta muito importante no combate à fraude, especificamente no uso indevido de cartões com gratuidade.

O Recon, como é chamado o software de reconhecimento facial, foi implantado em agosto de 2017. Ao longo do ano de 2019, verifica-se que há um aumento significativo de cartões cancelados ou benefícios suspensos de acordo com o quadro a seguir:

Quadro 4 – Quantidade de cartões com gratuidade cancelados por uso indevido

<i>Janeiro</i>	<i>Fevereiro</i>	<i>Março</i>	<i>Abril</i>	<i>Maio</i>	<i>Junho</i>	<i>Julho</i>	<i>Agosto</i>
5.426	9.263	16.965	31.544	34.004	34.189	49.554	29.444

Fonte: Relatório das Análises de Reconhecimento Facial (SPTrans).

Todas as utilizações com cartões de gratuidade são registradas pelos validadores, que são cartões de idosos, PcD e Estudantes com 100% de gratuidade. As fotos registradas são enviadas das garagens das concessionárias à SPTrans e então se inicia o procedimento de reconhecimento facial.

Após a recepção das fotos na SPTrans, elas são submetidas ao processo de

comparação da foto registrada pelo validador no momento do uso com a foto do cadastro do portador do cartão.

Uma vez comparadas as fotos, o Recon determina uma nota, variando de 0 a 100, avaliando a semelhança das fotos. Quanto mais baixa a nota, menor é a semelhança entre as fotos. As fotos com notas baixas são encaminhadas para a área de combate à fraude, onde se confirma que a falta de semelhança apontada pelo software realmente foi usada por uma pessoa que não corresponde ao portador do cartão. Assim, o cartão é cancelado.

O procedimento até agora descrito é eficaz para portadores de cartão de idosos e PcDs, mas não é para estudantes com 100% de gratuidade. Isso porque os dois primeiros, quando desejam trocar suas fotos no cadastro, têm de comparecer a uma unidade da SPTrans.

Os estudantes efetuam a troca de fotos pelo site da SPTrans, sem que haja uma comparação entre a foto anterior e a foto atual. Desta forma, a foto de um estudante pode ser trocada pela foto de alguém que não tenha o benefício. Quando o fraudador usar o cartão indevidamente e sua foto registrada pelo validador for comparada com a nova foto do cadastro, provavelmente a nota da comparação será alta pela semelhança e este registro não será encaminhado para a área de cancelamento (Conclusão 4.11).

Para estimar o risco dessa situação, foram requisitadas à SPTrans a quantidade de estudantes com 100% de gratuidade no mês de maio de 2019, bem como a de estudantes com gratuidade em algum mês de 2019 que trocaram de foto durante o mesmo período. No primeiro caso, havia 658.140 estudantes com o benefício, e no último, foram feitas 94.500 trocas de fotos de cartões. Assim, pode-se observar que o volume de ocorrências associado à situação de risco é bastante significativo.

Outro problema verificado é que as concessionárias não estão enviando as fotos registradas nos validadores em sua totalidade. Tomando como exemplo o mês de setembro de 2019, verificamos que há uma defasagem de 66.377.248 fotos que não foram enviadas (peça 12 – fls. 1/2).

No quadro abaixo, demonstramos alguns pontos de coleta que não enviaram sequer uma foto para a SPTrans:

Quadro 5 – Quantidade de fotos transmitidas

Ponto de Coleta	Quantidade de Utilizações	Quantidade de Fotos Transmitidas
451-Transcooper II – MARRA	4.176.794	0
441-Novo Horizonte	222.6004	0
151-Fenix	669.389	0
352-PAULISTANA – ANTUNES	621.503	0
541-Nova Aliança	482.750	0
251-Fenix	428.368	0
252-Fenix – Agenor	214.275	0
539-TERM. SACOMA -> MERCADO	187.176	0
AR8 – 218 – Gato Preto	120.961	0

Fonte: Relatório de fotos enviadas no mês de setembro de 2019 (SPTrans).

Ressaltamos que uma quantidade significativa de usuários viaja

exclusivamente de Metrô ou CPTM. Nesses dois modais não há o procedimento de registro fotográfico. Os dois concentram uma grande quantidade de passagens do Bilhete Único, sendo que para o mês de setembro de 2019 foram registradas 5.190.718 bilhetagens, exclusivamente para as duas modalidades. Desta forma, o procedimento de reconhecimento facial não é possível de ser executado e o cancelamento do cartão por uso indevido fica prejudicado.

Por fim, há que se ressaltar o resultado do combate antifraude da SPTrans. Com base nos controles acima apresentados, o resultado da produção de cancelamentos do uso indevido de cartões de gratuidade está apresentado no quadro a seguir:

Quadro 6 – Quantidade de cartões com gratuidade cancelados por uso indevido

	<i>Janeiro</i>	<i>Fevereiro</i>	<i>Março</i>	<i>Abril</i>	<i>Mai</i>	<i>Junho</i>	<i>Julho</i>	<i>Agosto</i>
<i>Registros disponibilizados pelo Recon</i>	560.067	1.064.672	1.158.751	1.384.593	1.359.134	1.560.739	1.561.710	1.533.863
<i>Avaliados Manualmente</i>	152.532	179.188	189.803	316.820	414.984	240.600	318.762	422.403
<i>Não Avaliados</i>	407.535	885.484	968.948	1.067.773	944.150	1.320.139	1.242.948	1.111.460

Fonte: Relatório das Análises de Reconhecimento Facial (SPTrans).

No quadro 6, tomando como exemplo o mês de Agosto de 2019, foram analisadas 422.403 fotos de um total de 1.533.863, sendo que 29.444 foram cancelados. Contudo, 1.111.460 fotos não foram analisadas. Verifica-se que o aumento da produtividade, ao longo de 2019, se deve a melhorias implantadas no processo de reconhecimento facial como um todo e no aumento de funcionários exclusivos para esta atividade, contudo a quantidade de funcionários ainda se mostra insuficiente, pois são 11 somente para o sistema Recon.

Embora a SPTrans tenha efetuado esforços no combate à fraude no que tange a gratuidade de cartões, este procedimento pode melhorar em quatro pontos a seguir:

- Aumentar a quantidade de funcionários da área antifraude;*
- Impedir que novas fotos dos estudantes com 100% de gratuidade sejam trocadas por meio do site da SPTrans, ou que haja um procedimento para validar a semelhança das fotos antes de confirmação de troca de foto;*
- Corrigir o problema de defasagem de envio de fotos das concessionárias;*
- Instalar no Metrô e CPTM o registro fotográfico para os usuários de gratuidade.”*

Sobre os arquivos de validadores, a Auditoria verificou que “os dados, do ponto de vista amostral, estão sendo processados de acordo com os dados gerados pelos validadores”.

A Auditoria buscou identificar bilhetagens concentradas em pontos geográficos atípicos ou o uso anormal de cartões em determinadas localidades da cidade de São Paulo, mediante amostragem de algumas bases de dados do Sistema Integrado de Monitoramento (SIM). Relatou, então, a Auditoria, que *“a partir dos registros provenientes exclusivamente das garagens, cruzamos estes dados com a base de dados de bilhetagem das empresas. O objetivo deste cruzamento é verificar se houve bilhetagem nas garagens ou em seus arredores a uma distância de 30 metros. O resultado foi que não houve bilhetagens nas garagens para a amostra selecionada”*.

Com relação aos dois tipos de controles de fraudes, rotinas e vacinas, a Auditoria anotou:

“As vacinas são instaladas nos validadores. No momento do uso do Bilhete Único, elas analisam as características do cartão a fim de identificar se aquele é um cartão falso – isto é, clone do BU fornecido pela SPTrans – ou, no caso de cartões verdadeiros, se contêm evidências de recargas falsas. Em ambos os casos, o cartão fraudado é “queimado”, isto é, marcado como inacessível para que não possa mais ser utilizado.

Já as rotinas são aplicadas pela SPTrans em suas instalações. Elas cruzam diversas informações, buscando evidências de uso indevido do cartão. Caso seja identificado, o cartão é inserido na chamada Lista Vermelha, enviada periodicamente aos validadores. Quando o cartão é novamente utilizado, o validador também o “queima”, nesse caso por conta da inclusão na Lista Vermelha.

Por possuir tamanho limitado, a Lista Vermelha inclui somente os cartões identificados como prioritários pela Gerência de Segurança de Informações da Bilhetagem Eletrônica (GSI). Contudo, como os cartões podem ser clonados, ainda que sejam queimados pela Lista Vermelha, seus clones poderiam continuar sendo apresentados e utilizados normalmente, caso fossem removidos dessa Lista para incluir outros mais prioritários.

Para evitar esse problema, a SPTrans emprega também outra lista chamada Lista Permanente, que possui a mesma funcionalidade que a Lista Vermelha, porém, como o nome indica, possui o rol de todos os cartões já identificados como fraude pelas rotinas da SPTrans. Assim, um mesmo cartão pode estar em ambas as listas ao mesmo tempo, enquanto for considerado prioritário segundo os critérios da GSI. Neste relatório, ambas as listas serão referidas como Lista Vermelha.

A funcionalidade de Lista Vermelha permite a inclusão e a remoção de cartões dessas listas. Portanto, caso um cartão seja inserido indevidamente nessas listas, é possível removê-lo posteriormente. Contudo, caso seja inutilizado por algum validador nesse intervalo, não será possível ao usuário recuperá-lo da mesma forma, sendo necessário levá-lo a um posto da SPTrans para que sejam tomadas as medidas de reativação requeridas.

Não obstante, como é possível clonar os cartões do Bilhete Único, é comum que um único cartão (conforme identificado pelo Sistema de Bilhetagem Eletrônica) apresente diversas ocorrências de “queima” no sistema, uma vez que cada uma delas corresponde a um clone distinto. Isto é, cada vez que um clone é utilizado em um validador, é feita e registrada uma nova “queima” por parte da Lista Vermelha ou mesmo por uma vacina construída para evitá-la”.

Referentemente ao impacto financeiro das fraudes detectadas no Sistema de Bilhetagem Eletrônica, assinalou:

“A venda de créditos fictícios (quebra da chave) ou a utilização indevida de gratuidades oneram os cofres públicos na parcela do Orçamento Municipal destinado à compensação tarifária. A pergunta que esse tópico se propõe a responder é: dos R\$ 2,9 Milhões previstos para compensação tarifária na LOA 2019, quanto se destina a cobrir a fraude do Sistema?

Primeiramente, repisando, os tipos de fraude são: i) venda de créditos fictícios em PDV ilegal para cartões legais/ilegais; ii) venda de acesso individual na porta do ônibus, metrô ou trem; iii) utilização indevida dos cartões de gratuidade; iv) utilização indevida dos cartões de meia gratuidade.

Dessas espécies de fraude verificadas no Município, entendeu-se que a venda de acesso individual é consequência de créditos fictícios de PDV ilegal, bem como a utilização dos cartões de meia gratuidade correspondem a apenas 3% da remuneração do sistema de transporte coletivo.

Assim, o cálculo do impacto financeiro das fraudes focou nas seguintes vertentes: custo dos créditos fictícios que obtiveram acesso à prestação do serviço e custo da utilização indevida de gratuidades cujo somatório delas corresponde ao valor de fraude mensal.”

A Auditoria buscou, então, fazer um cálculo do dano decorrente de fraudes, a partir da seguinte premissa: “o prejuízo ao erário corresponde à diferença negativa entre o valor efetivamente utilizado no sistema de transporte coletivo e o saldo recarregado de forma legítima.

E selecionou, “aleatoriamente, três meses de 2019 (janeiro, maio e setembro) como amostra para calcular a diferença negativa entre o valor efetivamente utilizado no sistema de transporte coletivo e o saldo recarregado de forma legítima. Adotou-se o seguinte método:

- *Seleção das transações de uso dos meses de janeiro, maio e setembro de 2019 referentes a Bilhetes Únicos (excluindo cartões de serviço e bordo);*
- *Utilização das transações de uso com valor unitário maior que R\$ 0;*
- *Comparação do saldo armazenado no cartão (capturado pelo validador no*

- *momento do uso) com o valor dos créditos válidos registrados no SBE;*
- *Caso o saldo armazenado no cartão seja superior ao que ele tinha direito (isto é, havia créditos fictícios), contabilização do valor da transação como perda da SPTrans.*

Quadro 11 – Impacto dos créditos fictícios que obtiveram acesso à prestação do serviço

<i>Mês</i>	<i>Quantidade de cartões com saldo fictício (A)</i>	<i>Média de valor das transações em R\$ (B)</i>	<i>Prejuízo ao erário mínimo em R\$ (C = A x B)</i>
<i>Jan/2019</i>	<i>53.058</i>	<i>36,17</i>	<i>1.918.904,24</i>
<i>Mai/2019</i>	<i>34.072</i>	<i>38,27</i>	<i>1.303.959,53</i>
<i>Set/2019</i>	<i>33.592</i>	<i>29,16</i>	<i>979.686,36</i>

Fonte: Elaboração própria.

Assim, o prejuízo ao erário nos meses de janeiro, maio e setembro de 2019 com a utilização de créditos fictícios foi de pelo menos R\$ 4.202.550,13 (Conclusão 4.1).

O processo também permitiu identificar 79.130 cartões carregados com créditos fictícios que não foram incluídos na Lista Vermelha até 12.12.19 (peça 20 – fl. 1). O valor do prejuízo causado por esses cartões nos meses de janeiro, maio e setembro de 2019 foi de R\$ 2.154.235,33, referentes a 637.236 transações (Conclusão 4.4).

Além desses, 17.947 cartões que estavam inseridos na Lista Vermelha ainda assim foram capazes de utilizar o serviço de transporte coletivo com créditos fictícios nos meses de janeiro, maio e setembro de 2019 (peça 13 – fl. 1). O valor do prejuízo causado por esses cartões no período analisado foi de R\$ 740.930,00, referentes a 185.885 transações (Conclusão 4.5).

Por fim, o processo também apontou 41 cartões sem registro no SBE que realizaram 4.023 transações nos meses de janeiro, maio e setembro de 2019, no valor de R\$ 16.713,40 (peça 19 – fl. 1). Essas transações também apresentam características de uso indevido, uma vez que não deveria ser possível utilizar o serviço de transporte coletivo com cartões com numeração adversa dos cartões oficiais (Conclusão 4.6).

*Os usos desses cartões, portanto, representam irregularidades, uma vez que a fraude não foi evitada pela SPTrans apesar da possibilidade de ser identificada, como demonstrado por esta auditoria. Além disso, a existência de cartões fraudados não incluídos na Lista Vermelha, e de cartões inseridos em Lista Vermelha capazes de utilizar o serviço de transporte coletivo, representa falhas graves que requerem medidas imediatas da SPTrans para sua solução (Conclusão 4.7)”.
Referentemente sobre o impacto financeiro da gratuidade por uso indevido, a Equipe de Auditoria fez as seguintes observações:*

“O perfil gratuidade contempla as modalidades estudante, idoso e pessoa com deficiência (PcD) cujos controles pela SPTrans ocorrem, principalmente, no momento da concessão dos benefícios e durante a utilização. Essa última resultante da comparação da foto capturada pelas câmeras instaladas nos validadores dos ônibus/terminal com aquela

constante na base de dados da SPTrans (biometria facial – Recon).

Por meio da Requisição de Documentos MAC nº 03 (peça 14 – fl. 1), solicitou-se o quantitativo das imagens que foram submetidas ao crivo da biometria facial, bem como a discriminação das imagens que foram consideradas aprovadas/reprovadas após o processo de checagem da foto capturada pelos validadores com a imagem constante no cadastro do usuário e suas respectivas discriminação: estudante, idoso e PcD.

Primeiramente, cumpre registrar uma limitação dessa auditoria em capturar e valorar a totalidade dos usos indevidos de estudante uma vez que a foto constante do seu cadastro e que servirá de parâmetro para comparação pelo Recon pode ser facilmente alterada conforme demonstrado no anexo I.

Ou seja, os estudantes que emprestam seu BU para um terceiro e alteram a imagem do cadastro com o terceiro interessado não são passíveis de captação pela medida de controle. Diferente dos perfis idoso e PcD cuja foto do banco de dados só pode ser alterada pessoalmente em um dos postos da SPTrans. Assim, verifica-se fragilidade nas medidas de controle do procedimento de alteração da fotografia do cadastro dos estudantes, permitindo utilizações indevidas dos Cartões.

Observa-se, ao longo do ano de 2019, que a SPTrans vem aumentando o quantitativo de imagens submetidas a esse procedimento, conforme quadro abaixo:

Quadro 12 – Quantitativo de imagens submetidas ao Recon

<i>Mês</i>	<i>Jan</i>	<i>Fev</i>	<i>Mar</i>	<i>Abr</i>	<i>Mai</i>	<i>Jun</i>	<i>Jul</i>	<i>Ago</i>	<i>Set</i>	<i>Out</i>
<i>Utilizações importadas (em milhares)</i>	4.958	8.518	9.714	9.585	8.749	10.122	10.200	11.522	8.162	8.372

Fonte: SPTrans (peça 15 – fl. 1).

No entanto, uma pergunta se fez imprescindível: o total de imagem geradas e enviadas ao Recon acontece de forma aleatória? Ou seja, existe a mesma probabilidade de uma imagem gerada no extremo da zona leste e uma gerada no terminal na área central da cidade ser selecionada pelo Recon a fim de triagem?

Com o fito de responder a essa questão, elaborou-se a Requisição de Documentos PP nº 02, a qual obteve como resposta do retroquestionamento apenas que:

Atualmente não são todas as garagens que estão enviando as fotos para reconhecimento facial diariamente, porém isto não ocorre devido à falta de infra-estrutura necessária para este procedimento. O motivo identificado deste problema é a falta de atualizações no sistema operacional dos servidores de algumas garagens, que ainda não se adequaram a este procedimento, portanto estão em débito com o envio diário das fotos para análise do Recon. Para a solução deste problema foi acordado com as empresas operadoras do transporte coletivo que até 31/12/2019, todas as empresas deverão estar regularizadas.

Outrossim, restou demonstrado na análise do subitem 3.2.4.2 deste Relatório o quantitativo de imagens que não são enviadas para análise pelo sistema Recon.

Diante de tamanhas fragilidades, ainda assim, buscou-se chegar a um valor monetário do prejuízo mínimo ao erário, de forma que se adotou o seguinte método:

- *Utilização dos dados da SPTrans do total de cartões “cancelados” em virtude de uso indevido para o período de janeiro a outubro de 2019;*
- *Premissa de que cada cartão cancelado foi utilizado apenas uma vez de forma indevida face ao embaraço de saber dos usos anteriores ao momento da flagrante inadequação pelo Recon;*
- *Premissa da adoção do menor valor de Remuneração; e*
- *Determinação do valor mínimo de fraude possível.*

Quadro 13 – Quantidade de cartões com gratuidade cancelados por uso indevido

<i>Quantidade de cartões “cancelados” de Jan a Out de 2019 (A)</i>	<i>Menor valor de remuneração em R\$ (B)</i>	<i>Prejuízo ao erário mínimo em R\$ (C = A x B)</i>
247.907	1,8563	460.189,76

Obs.: Considerou-se o menor valor da Remuneração no ano de 2019, correspondente à Remuneração da Empresa Allibus Transportes Ltda. em janeiro de 2019 (área 4.1 do subsistema local). Fonte: Elaboração própria.

Assim, o prejuízo ao erário no período de janeiro a outubro de 2019 com a utilização indevida de gratuidades foi de pelo menos R\$ 460.189,76 (Conclusão 4.2).”

No item 4 de seu Relatório, concluiu, então, a Equipe de Fiscalização, o quanto segue:

Irregularidades Identificadas

4.1 O prejuízo ao erário nos meses de janeiro, maio e setembro de 2019 com a utilização de créditos fictícios foi de pelo menos R\$4.202.550,13 (subitem 3.2.5.1);

4.2. O prejuízo ao erário no período de janeiro a outubro de 2019 com a utilização indevida de gratuidades foi de pelo menos R\$ 460.189,76 (subitem 3.2.5.2);

4.3. De uma amostra aleatória de 2.500 cartões da Lista Vermelha para os quais se analisou se tiveram uso tarifado após sua identificação pelas rotinas, 258 realizaram no total 2.744 usos após sua inclusão, sumarizando R\$ 9.712,53 de usos indevidos, ou seja, 10,6 usos no valor médio de R\$ 37,52 por cartão (subitem 3.2.4.5);

4.4. Em relação ao mês de setembro de 2019, foram identificados 79.130 cartões carregados com créditos fictícios que não foram incluídos na Lista Vermelha até 12.12.19. O valor do prejuízo causado por esses cartões nos meses de janeiro, maio e setembro de 2019 foi de R\$ 2.154.235,33 (subitem 3.2.5.1);

4.5. Nos meses de janeiro, maio e setembro de 2019, 17.947 cartões que estavam inseridos na Lista Vermelha ainda assim foram capazes de utilizar o serviço de transporte coletivo com créditos fictícios. O valor do prejuízo causado por esses cartões no período analisado foi de R\$ 740.930,00

(subitem 3.2.5.1);

4.6. Há 41 cartões sem registro no SBE que realizaram 4.023 transações nos meses de janeiro, maio e setembro de 2019, no valor de R\$ 16.713,40. Essas transações também apresentam características de uso indevido, uma vez que não deveria ser possível utilizar o serviço de transporte coletivo com cartões com numeração adversa dos cartões oficiais (subitem 3.2.5.1);

4.7. A existência de cartões fraudados não incluídos na Lista Vermelha, e de cartões inseridos em Lista Vermelha capazes de utilizar o serviço de transporte coletivo, representa falhas graves que requerem medidas imediatas da SPTrans para sua solução (subitem 3.2.5.1);

4.8. O Ciclo de Gestão de Riscos adotado no Sistema de Bilhetagem Eletrônica demonstra-se inapropriado, 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 3.2.2.1);

4.9. 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 3.2.1.2);

4.10. Os cartões smart card dos modelos Classic e Plus com nível de segurança Security Level 1 usados como Bilhete Único são obsoletos (subitem 3.2.2);

4.11. Fragilidade de controle no procedimento de alteração da fotografia do cadastro dos estudantes permitindo utilizações indevidas dos Cartões (subitens 3.2.4.2 e 3.2.5.2).”

Propostas de Determinações:

4.12. Desenvolver ferramentas e tabelas de Data Warehouse que permitam a apuração do impacto financeiro das fraudes detectadas de forma continuada e tempestiva (subitem 3.2.1.2).

4.13. Desenvolver integração entre o Sistema de Bilhetagem Eletrônica e o Sistema Integrado de Monitoramento (subitem 3.2.1.3);

4.14. Interromper o uso dos cartões smart card dos modelos Classic e Plus com nível de segurança Security Level 1 (subitem 3.2.2);

4.15. 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 (subitem 3.2.2);

4.16. 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 3.2.3.3);

4.17. Aumentar a quantidade de funcionários da área antifraude (subitem 3.2.4.2);

Corrigir o problema de defasagem de envio de fotos das concessionárias (subitem 3.2.4.2).

Instalar no Metrô e CPTM o registro fotográfico para os usuários de gratuidade (subitem 3.2.4.2).

4.18. Adotar medidas de controle no procedimento de alteração da fotografia

do cadastro dos estudantes a fim de mitigar o risco de utilizações indevidas (subitens 3.2.4.2 e 3.2.5.2).

4.19. Instalar no Metrô e CPTM o registro fotográfico para os usuários de gratuidade (subitem 3.2.4.2).

4.20. Adotar medidas de controle no procedimento de alteração da fotografia do cadastro dos estudantes a fim de mitigar o risco de utilizações indevidas (subitens 3.2.4.2 e 3.2.5.2).

Notificada do resultado da auditoria realizada (peças 22/23, 26 e 28), a São Paulo Transportes S/A encaminhou suas considerações e justificativas (peças 37/38). Afirmou:

Como na época em que o sistema do Bilhete Único foi criado não havia comunicação que permitisse que os validadores pudessem comunicar diretamente à SPTrans quando estivesse em campo, o nosso sistema criou uma lista de validação de cartões totalmente off-line, sendo que essa lista era atualizada nas garagens 1 vez por dia, com limitação de aproximadamente 60.000 cartões cancelados. No ano de 2019, devido à nova tecnologia de comunicação com 3G e 4G, foi possível modificar o validador de modo a enviar as transações realizadas pelos usuários à SPTrans, logo após o uso, e validá-las de modo a incluir em uma nova lista de cartões bloqueadas, com maior abrangência que a anterior, baseada em banco de dados, com os cartões com identificação de fraude. Apesar dessa tecnologia, ter um efeito extremamente positivo no combate a fraude, a mesma ainda possui limitações, visto que em muitos pontos da cidade, existem sombras de comunicação, que prejudicando a atomicidade dessa atualização. Ademais a utilização dos valores de crédito existentes no SBE, em princípio, não está adequada, pois no banco de dados existem registros que foram excluídos devido a backups e expurgos, de modo a manter a capacidade de processamento do ambiente após mais de 17 anos de produção.”

Sobre o Ciclo de Gestão de Riscos adotado no Sistema de Bilhetagem Eletrônica demonstrar-se inapropriado, acarretando riscos à continuidade da prestação do serviço de transporte coletivo, a SPTrans afirmou que “*atualmente está no plano de metas da SPTrans para a área de tecnologia a contratação de consultoria para a retomada dessa atividade. O prazo estipulado para essa contratação está para dez/2020*”.

Relativamente à conclusão da Auditoria de que “*os bancos de dados são separados por binários diferentes e em máquinas distintas devido a evitar que um único motivo possa impactar todos os serviços do Bilhete Único*”, a SPTrans assegurou que “*a afirmativa que o banco de dados mantém dados duplicados é equivocada, pois os bancos de dados mantém em cada sistema os*

objetos a eles pertencentes, sendo acessados por um recurso de interligação dos bancos, chamado de dblink. Esse recurso permite que um sistema através de links entre base de dados possa acessar entidades de outros sistemas, mantendo a integridade das informações”.

No tocante a elaboração de soluções, a SPTrans informou que, “devido à existência de aproximadamente 15.000.000 de cartões em uso no sistema em um ano, não é possível realizar tal interrompimento de maneira abrupta, sem prejudicando o direito constitucional do usuário. E como é de conhecimento, o sistema contratado pela SPTrans para renovar o Bilhete Único, resolvendo os problemas de segurança, foi considerado, em dez/2019, interrompido parcialmente. Nesse momento, frente a esses fatos, estamos construindo um novo sistema de segurança, SAM criptográfico, com equipe interna, que tem como objetivo a absorção e transferência do sistema de segurança realizado pelo antigo fornecedor, a inclusão de novos mecanismos de segurança para os cartões Plus e o incremento do nível de segurança para nível 3 para esses cartões plus. Com esse novo elemento, poderemos realizar a mudança de segurança de forma remota como comentado no relatório. Ainda nesse contexto, após a implantação da nova vacina, foi possível a inibição da criação dos valores de recarga, havendo hoje somente a transação falsa motivada por clones em cartões do tipo 1K. Além do mais, podemos afirmar, em divergência ao que foi dito no relatório, que o algoritmo AES não foi quebrado, mais sim o algoritmo crypto 1 existente nos cartões do tipo 1K. Por último está sendo criado um ambiente novo para a estruturação de BigData e Inteligência artificial para identificação de fraudes”.

A respeito de se “desenvolver integração entre o Sistema de Bilhetagem Eletrônica e o Sistema Integrado de Monitoramento”, a SPTrans informou que está “elaborando um termo de referência para o novo sistema de bilhetagem que irá integrar a Unidade Central de Processamento e o Validador ao mesmo”.

No que concerne à “existência e cartões fraudados não incluídos na Lista Vermelha, e de cartões inseridos em Lista Vermelha capazes de utilizar o serviço de transporte coletivo” e sobre “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”, a SPTrans afirmou que “atualmente está implantado em mais de 10.000 ônibus o Sistema de Lista Permanente que recebe de maneira on-line os dados de utilização registrados no validador. Esses dados são avaliados por rotinas automáticas que ao identificar fraudes, atualizam as listas dos validadores para bloquearem o uso do cartão no próximo uso. Esse sistema substitui de certa forma, a lista vermelha que tem uma limitação de aproximadamente 60.000 cartões. O Sistema de Lista Permanente, além de ser on-line possui uma limitação de mais de 5 milhões de cartões para cancelamento”.

Nas peças 30/31 foram juntados ofício e relatório da Controladoria Geral do Município sobre auditoria realizada por aquele órgão para averiguar eventuais irregularidades na concessão de gratuidade das empresas prestadoras de serviços de transporte coletivo onerando os cofres públicos municipais.

A Equipe de Auditoria, na peça 42, depois de analisar os esclarecimentos oferecidos pela SPTrans, superou o item 4.9 e manteve todos os demais apontamentos referentes às irregularidades identificadas e as propostas de determinação. E anotou que o conteúdo dos documentos encaminhados pela CGM já era de seu conhecimento por ocasião da auditoria extraplano.

A Assessoria Jurídica de Controle Externo (peças 44 e 45) observou que, muito embora haja nuances jurídicas no bojo das conclusões da Auditoria, a aferição do perfeito enquadramento do objeto ao que se destina revestia-se de essencialidade técnica que refugia de sua esfera de competência, daí secundar o entendimento técnico prévio da Auditoria.

Em observância ao princípio da ampla defesa, foram notificados os Srs. Valdemar Gomes de Melo (Presidente da SPTrans), Donizete Santana Costa (Diretor da empresa à época), José Aécio de Souza, Vladimir Martins (Superintendentes da empresa à época) e Paulo César Shingai (Diretor-Presidente à época), consoante peças 50/59 e 67/76. E, às peças 79/81 foi oferecida resposta conjunta da SPTrans com os responsáveis intimados, juntando-se planilha referente aos esforços de combate à fraude, com os Boletins de Ocorrência registrados com auxílio da SPTrans (peça 81).

Sobre as fraudes, os responsáveis fizeram as seguintes considerações:

“A auditoria elencou como responsáveis os Srs.:

• Paulo César Shingai. Diretor-Presidente da SPTrans no período de 21/03/2018 a 19/01/2020; • Donizete Santa Costa. Diretor de Gestão de Receita e Remuneração desde 06/08/2018 (Comunicado da Presidência nº 053/18);

• José Aécio de Souza. Superintendente de Atendimento e Comercialização nos períodos de 15/02/2007 a 20/05/2015, e de 21/05/2017 a 27/11/2019 (Comunicados da Presidência nº 012/07, nº 023/15, nº 025/17, e nº 085/19). A Superintendência de Atendimento e Comercialização não foi responsável pela gestão de contratos de tecnologia da informação relacionada à bilhetagem, seja para o desenvolvimento de sistemas, provimento da infraestrutura, ou outros objetos;

• Vladimir Marns. Superintendente de Tecnologia da Informação no período de 16/09/2019 a 11/12/2019 (Comunicados da Presidência nº 057/19 e nº 096/19). Apenas durante esses três meses o referido senhor esteve à frente da Superintendência, de forma que não seria possível nesse curto período de tempo promover qualquer interferência substancial em relação aos contratos geridos pela Área. Mesmo assim, o referido senhor iniciou a internalização da tecnologia do módulo de segurança e seguiu com as diversas medidas proativas descritas ao longo desta manifestação.

Como exporemos em detalhes, as chamadas fraudes no SBE estão inseridas em um contexto maior que o exercício de 2019 e são decorrentes, em larga medida, de escolhas políticas e de negócio que antecedem, em muito, a atuação dos gestores elencados pela auditoria.

Sobressai o fato de que o Diretor de Gestão de Receita e Remuneração e o Diretor Presidente elencados assumiram os respectivos postos no ano de 2018, sendo virtualmente impossível alterar num curto período de tempo uma situação tecnicamente complexa como a ora discutida. Ademais, o estado de coisas avaliado pela auditoria decorre de escolhas que antecedem a gestão desses Diretores, que, por sua vez, adotaram as providências que estiveram ao seu alcance para preservar o erário.

Desde já, rogamos a este E. Tribunal que observe com o devido cuidado os limites da atuação dos integrantes da SPTrans, levando em conta (i) o período de tempo em que as pessoas mencionadas estiveram à frente de suas equipes; (ii) as esferas de atribuição de cada uma de suas Áreas; e também (iii) as alternativas factíveis à época em que cada uma das pessoas assumiu a respectiva posição de chefia”.

Foram apresentadas, então, considerações, explicações, justificativas e/ou informações sobre o contexto das fraudes no SBE, o histórico e causas da utilização de créditos falsos, observações sobre o uso de gratuidades, o apoio à repressão a fraudadores, inibição de recargas fraudulentas e da clonagem de cartões, prova de vida automática por intermédio do cadastro do Sistema de

Controle de Óbitos mantido pelo INSS (SISOBI), validação de dados pelo cadastro da Receita Federal, tabela informando a quantidade de cartões cancelados por tipo de ocorrência – 2020, considerações sobre o sistema de controle de distribuição de cartões, bloqueio de cartões tipo comum, processo de apuração de infrações, integração com a Secretaria da Educação do Estado de São Paulo, implantação de CadÚnico para concessão de benefícios, informações sobre absorção da tecnologia e do know-how de desenvolvimento e manutenção do SBE visando a reduzir a dependência tecnológica em relação a empresas privadas e para ter cada vez mais autonomia para combater as fraudes.

E buscou responder a cada um dos pontos das conclusões da Equipe de Auditoria, inclusive com apresentação de tabelas com dados sobre o processo de apuração de irregularidades, e afirmando, a final, que a SPTrans “*sempre buscou com afinco e dentro de suas atribuições prevenir e combater todos os tipos de fraudes e abusos*”.

Depois de analisar as informações apresentadas pela empresa, a Equipe de Auditoria considerou superados os itens 4.17 e 4.20, em razão das medidas já adotadas pela empresa, e o item 4.19, por depender de ações que ultrapassam as competências da SPTrans. Ratificou os demais itens, propondo em relação ao item 4.16, nova redação bem como seu endereçamento à SMT (peça 86):

4.16. Determinar à SMT que disponibilize 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.

A Assessoria Jurídica de Controle Externo secundou as conclusões da Auditoria, inclusive quanto à sugestão de oficializar a SMT sobre a proposta 4.16, tendo em vista a nova redação conferida ao apontamento.

Da mesma forma, a Fazenda Municipal acompanhou as manifestações precedentes no sentido de que a SMT fosse intimada para manifestar-se sobre a nova redação da proposta 4.16.

Cientificada da nova redação proposta para o item 4.16, a Origem não se manifestou.

O Órgão Fazendário (peça 107) requereu o conhecimento e registro da auditoria, por entender que seus objetivos foram alcançados, observando que eventuais recomendações deste Tribunal podem ser utilizadas para o incremento da qualidade dos programas executados pela Administração

A Secretaria Geral, acompanhando as conclusões da Auditoria e da Assessoria Jurídica de Controle Externo, entendeu que a Auditoria Extraplano cumpriu os seus objetivos, encontrando-se em condições de ser submetida ao conhecimento e à deliberação.

Apoiado nas conclusões da Auditoria, à SPTrans (peça 111) foi novamente oficiada para se manifestar sobre os questionamentos, e apresentou esclarecimentos.

Às peças 115 e 116 estão relacionadas as respostas oferecidas pela SPTrans, sendo que, do seu teor, foi dado conhecimento ao Órgão Fazendário que, na peça 119, tomando ciência, assinalou que os esclarecimentos da Origem *“mais uma vez comprovam as providências que vêm sendo adotadas no combate às fraudes junto ao sistema de Bilhetagem Eletrônica”*. Reiterando sua anterior manifestação de peça 107, requereu o conhecimento e o registro da presente auditoria.

É o relatório.

VOTO

1 - Trata-se de auditoria extraplano do Sistema de Bilhetagem Eletrônica (SBE) da SPTrans para verificar o sistema antifraude desenvolvido pela empresa e o impacto financeiro das fraudes detectadas, que acabam onerando os cofres públicos na medida em que, para efetivar o equilíbrio financeiro do Sistema de Transporte Coletivo Municipal, são despendidos elevados subsídios.

Constatou-se que, embora haja atuação da SPTrans para a gestão de riscos do Sistema de Bilhetagem Eletrônica, as ações criminosas de “clonagem de cartões” e de “recargas falsas” impactam financeiramente o sistema de bilhetagem do Sistema de Transporte Coletivo do Município de São Paulo, o

qual, consoante registrado no relatório de auditoria, “*armazena cerca de 13 milhões de transações diárias dos cartões do tipo Bilhete Único, o que perfaz mais de 300 milhões de transações mensais, e cerca de 4 bilhões de transações anuais*”.

A venda de créditos fictícios, possibilitada pela quebra da chave de segurança dos cartões, e a utilização fraudulenta de gratuidades continuam existindo em números expressivos.

2 - Há experiências, notadamente internacionais, em que o Sistema de Transporte Coletivo existente em algumas cidades, mitiga o controle da validação do bilhete, dispensando até o uso de catracas, facultando-se ao usuário a incumbência da sua validação por outros meios. Não é o caso do Sistema de Transporte Coletivo da Cidade de São Paulo em que é necessário um bilhete para sua utilização e o correspondente controle ostensivo da validação desse bilhete.

Na efetivação desse controle ostensivo, na peça 81, há planilha com informações sobre Boletins de Ocorrência, registrados com auxílio da SPTrans, entre junho de 2017 e fevereiro de 2021, indicando que houve 1.417 indiciados por fraudes, envolvendo o montante de R\$45.956.177,03. Assim como nas conclusões do relatório da Auditoria, identificadas nos itens 4.1 a 4.6, também se aponta prejuízo ao erário decorrentes de condutas criminosas de fraude ao sistema de bilhetagem eletrônica.

Se, por um lado, constata-se ações de gestão para mitigar a ocorrência de fraudes ao Sistema de Bilhetagem Eletrônica, por outro evidencia-se que a repressão a essa conduta criminosa não foi totalmente debelada, continuando a existir números expressivos de fraudulentas condutas para utilização do transporte coletivo municipal.

3 - Consoante conclusões do relatório da auditoria, que observou o devido processo administrativo em sua instrução, com ampla defesa e contraditório na participação dos responsáveis, há falhas graves no SBE e que requerem medidas imediatas para sua solução, dentre elas, a urgente substituição dos cartões *smart card* dos modelos *Classic* e *Plus* com nível de segurança *Security Level 1* usados como Bilhete Único, pois obsoletos e de segurança comprometida, requerendo bloqueio definitivo.

4 - O procedimento de alteração de fotografia do cadastro dos estudantes é frágil e permite, como ainda infelizmente se constata nas condutas detectadas pelo sistema, indevidas e fraudulentas utilizações dos correspondentes cartões. Deve haver uma efetiva reestruturação da emissão do

bilhete único do estudante, propiciando um controle eficaz sobre a concessão do benefício.

Sobre essa questão, a SPTrans (peça 116), em resposta a indagações deste Relator, registrou:

“Desde o início do ano a emissão do BU Estudante é feita em parceria com entidades estudan0s. A foto e os dados do cadastro do estudante são alterados após análise e aprovação dos documentos (self e documento de iden0ficação). A análise de documentos é realizada por automações sistêmicas e há uma segunda esteira de conferência humana. A análise sistêmica é realizada por robôs que utilizam cruzamento de bases externas, sistema de socre, inteligência artificial, OCR e reconhecimento de imagens. Já os documentos reprovados são submetidos à esteira de conferência humana que valida apenas os itens reprovados pelas automações sistêmicas. São avaliados os seguintes critérios:

- Selfie Foto deve ser de um humano e deve conter apenas um rosto;*
- Deve ser possível identificar dois olhos duas orelhas, nariz e boca;*
- Facematch entre selfie x foto presente no documento de identificação;*
- Facematch entre selfie x banco de celebridades e pessoas famosas;*
- Verificação de conteúdo explícito (violência ou conteúdo de teor sexual);*
- Verificação de posicionamento de face (centralização do rosto, rosto invertido);*
- Verificação se a foto enviada é de um ser humano;*
- Identificação de múltiplos rostos na mesma foto; Identificação de obstáculos que não permitem a identificação do usuário (óculos escuros e acessórios que cubram o rosto)*

Documento de Identificação

- Documento enviado deve ser RG, CNH ou RNE;*
- Se o documento for do 0po RG, deve ser parecido com RG digital ou algum dos 27 modelos existentes no Brasil*
- Se o documento for do tipo CNH, deve ser compatível com o digital ou o físico*
- O nome deve ser o mesmo nome informado no cadastro da escola*
- O nome deve ser o mesmo informado no cadastro da Receita Federal*

-A data de nascimento deve ser a mesma informada no cadastro da escola

-A data de nascimento deve ser a mesma informada no cadastro da Receita Federal

-O número do documento (número do RG ou número do RNE) deve ser o mesmo informado no cadastro da escola.”

5. A Auditoria constatou também que há possibilidade de existir cartões fraudados não serem incluídos na denominada “Lista Vermelha” para consequente inutilização, “queima”; assim como há brecha no sistema de bilhetagem permitindo que, até mesmo alguns cartões inseridos na “Lista Vermelha”, ainda assim possam ser utilizados no serviço de transporte coletivo. Assim, essas possibilidades devem ser erradicadas do SBE.

6. O Ciclo de Gestão de Riscos adotado no Sistema de Bilhetagem Eletrônica demonstra-se inapropriado, podendo até acarretar riscos à própria continuidade da prestação do serviço de transporte coletivo.

Como observou a Auditoria, o Sistema de Gestão de Segurança da Informação (SGSI) diz respeito a uma *“abordagem sistemática para a gestão e proteção das informações de uma organização. Ele 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. Nesse contexto, o Ciclo de Gestão de Riscos é o núcleo do SGSI; ele 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”*.

E, muito embora tenha-se procurado implantá-lo e por motivos orçamentários não tenha sido efetivado, o fato é que, consoante a Superintendência de Tecnologia da Informação (STI), a SPTrans não possui Sistema de Gestão de Segurança da Informação (SGSI) implantado sobre o SBE.

7. Há que se registrar também que, para combater as fraudes perpetradas contra o Sistema de Bilhetagem Eletrônica, a SPTrans, em resposta a indagações deste Relator, relacionou, na peça 116, *“ações já implementadas durante os anos de 2020 e 2021, bem como as que estão sendo implementadas neste exercício de 2022:*

2020 - Implantação da Vacina 4 / Bloqueio definitivo dos cartões;

2020 - Recebimento de novos módulos do SAM;

2020 - Implementação/desenvolvimento da camada de controle nos validadores;

2020 - Preparação do ambiente de gestão da segurança/infraestrutura;

2020/2021 - Validações dos dados de cadastros utilizando consultas da SERPRO para cancelamento/bloqueio de cartões;

2021 - Custódia segura de chaves criptográficas;

2021 - Implantação da camada de controle nos validadores;

2021 - Término da primeira versão de software do SAM;

2021 - Início do desenvolvimento de nova versão do software SAM (v1), para elevação do nível de segurança do cartão;

2021 - Emissão de novos módulos do SAM;

2021 – Distribuição física dos novos módulos/chips SAM para os dispositivos validadores que realizam leituras e gravações do cartão Bilhete Único;

2021 - Descontinuidade dos cartões anônimos (sem cadastro) (1k);

2022 - Realização de prova de conceito (POC) de elevação de nível de segurança, saindo no nível SL1 no MIFARE Plus;

2022 - Homologação de novos equipamentos de segurança (HSMs - Hardware Security Module);

2022 - Criação de novas soluções de HSMs possibilitando maior flexibilidade e rapidez para tomadas de ações e medidas de segurança do Bilhete Único”.

8. Assim, diante do exposto e do que consta dos autos, e tendo em conta as inúmeras ações dos gestores para efetivação da segurança do Sistema de Bilhetagem Eletrônica contra condutas fraudulentas e criminosas na sua utilização, conheço da auditoria, para fins de registro, acolhendo as conclusões do relatório da Auditoria constantes dos itens 4.7 (*A existência de cartões fraudados não incluídos na Lista Vermelha, e de cartões inseridos em Lista Vermelha capazes de utilizar o serviço de transporte coletivo, representa falhas graves que requerem medidas imediatas da SPTrans para sua solução*); 4.8 (*O Ciclo de Gestão de Riscos adotado no Sistema de Bilhetagem Eletrônica demonstra-se inapropriado, 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*); 4.10 (*Os cartões smart card dos modelos Classic e Plus com nível de segurança Security Level 1 usados como Bilhete Único são obsoletos*) e 4.11 (*Fragilidade de controle no procedimento de alteração da fotografia do cadastro dos estudantes permitindo utilizações indevidas dos Cartões*), na forma acima exposta neste voto, bem como as “Propostas de Determinações” constantes dos itens 4.12 (*Desenvolver ferramentas e tabelas de Data Warehouse que permitam a apuração do impacto financeiro das fraudes detectadas de forma continuada e tempestiva*) a 4.16 (*Determinar à SMT que disponibilize 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*) e do item 4.18 (*Adotar medidas de controle no procedimento de alteração da fotografia do cadastro dos estudantes a fim de mitigar o risco de utilizações indevidas*).

9. Cumpridas as formalidades legais, arquivem-se os autos.

É como voto.

DOMINGOS ODONE
DISSEI:81822650887

Assinado de forma digital por
DOMINGOS ODONE DISSEI:81822650887
Dados: 2023.04.03 09:58:22 -03'00'

DOMINGOS DISSEI
Conselheiro TCMSP

AAC/HCMC

42º SONP

E-TCM Nº 10.140/2019

DECLARAÇÃO DE VOTO

Conheço da Auditoria Extraplano para fins de registro, uma vez que ela alcançou satisfatoriamente os resultados almejados.

Não há dúvida que a SPTrans está aperfeiçoando seus sistemas de bilhetagem de modo a mitigar fraudes consoante se apurou ao longo desta instrução. Contudo, como se depreende das irregularidades enumeradas nos itens 4.1 a 4.6, há apontamentos de prejuízos ao Erário, que podem e devem ser dimensionados pela Pasta, apurando-se responsabilidades para fins de ressarcimento, considerando a falha de segurança do Sistema.

Diante do exposto, manifesto minha adesão ao Voto proferido pelo Relator, ao mesmo tempo em que proponho a determinação para que a SPTrans instaure um procedimento interno com o objetivo de investigar os prejuízos efetivamente sofridos pelo Erário, identificando os responsáveis pelas falhas ocorridas no Sistema e as medidas que serão adotadas para fins de ressarcimento. Ademais, determino que esta E. Corte de Contas seja informada, dentro

do prazo máximo de 60 dias, acerca dos resultados alcançados com a referida apuração.

É como voto.

TCM, 17 de abril de 2023.

ROBERTO

TANZI

BRAGUIM:03

999981873

Assinado de forma
digital por ROBERTO
TANZI
BRAGUIM:0399998187
3
Dados: 2023.04.17
10:45:45 -03'00'

ROBERTO BRAGUIM
Conselheiro Vice-Presidente

EMC/RB

Processo: 10.140/2019 (eletrônico)
Origem: São Paulo Transporte S/A – SPTRANS
Objeto: Auditoria Extraplano - Sistema de Bilhetagem Eletrônica - Verificar o sistema antifraude existente no Sistema de Bilhetagem Eletrônica com a indicação das fraudes detectadas e seus reflexos financeiros.

DECLARAÇÃO DE VOTO

Convirjo com o Relator no tocante ao **CONHECIMENTO E REGISTRO DA AUDITORIA EXTRAPLANO**, tendo em vista as constatações trazidas pela Auditoria acerca das salvaguardas instituídas para evitar que o Sistema de Bilhetagem Eletrônica seja atingido por condutas fraudulentas e criminosas na sua utilização. Também acompanho o Relator no sentido de **DETERMINAR** à Origem que:

- (i) Desenvolva ferramentas e tabelas de Data Warehouse que permitam a apuração do impacto financeiro das fraudes detectadas de forma continuada e tempestiva;
- (ii) Disponibilize 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;
- (iii) Adote medidas de controle no procedimento de alteração da fotografia do cadastro dos estudantes a fim de mitigar o risco de utilizações indevidas.

Considerando que tais determinações não podem ser implantadas de imediato, dependendo de várias ações concatenadas ao longo do tempo, da aplicação de recursos financeiro-orçamentários e da realização eventualmente até mesmo de certame licitatório, **PROPONHO** ao Relator que fixe

o prazo de 60 (sessenta) dias para que a Origem apresente um **PLANO DE AÇÃO** para o cumprimento das determinações referidas.

Plenário Cons. **PAULO PLANET BUARQUE,**

MAURÍCIO FARIA
Conselheiro

CRB

Cód. 042 (Versão 05)