Tribunal de Contas
DO MUNICÍPIO DE SÃO PAULO

**II – ACÓRDÃO**

| | | |
|---|---|---|
| Processo | - | TC/002933/2019 |
| Interessada | - | Secretaria Municipal de Educação |
| Objeto | - | Auditoria Extraplano – Inspecionar e avaliar a efetividade dos controles de segurança implementados na infraestrutura física e lógica instalados no Data Center da Secretaria |

3.194ª Sessão Ordinária

AUDITORIA EXTRAPLANO. SME. Inspeção e avaliação da efetividade dos controles de segurança implementados na infraestrutura física e lógica instalados no Data Center da Secretaria. 1. Riscos de adulteração ou vazamentos de dados. O banco de dados com informações pessoais dos educandos deve ser protegido. Lei 13.709/18. 2. Risco para a prestação dos serviços de educação. Os sistemas armazenados no Data Center são utilizados para atividades escolares cotidianas, como registro de frequência, diário de classe, avaliações, ou para atividades administrativas, por sistemas como o Escola Online e o Sistema de Gestão Pedagógica. CONHECIDA. DETERMINAÇÃO. 1. Apresente Plano de Ação para solução dos apontamentos do Relatório de Auditoria, ou comprove medidas já iniciadas. Votação unânime.

**A C Ó R D Ã O**

Vistos, relatados e discutidos estes autos, dos quais é Relator o Conselheiro MAURICIO FARIA.

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

**ACORDAM**, à unanimidade, em determinar que a Secretaria Municipal de Educação apresente, **no prazo de 30 (trinta dias)**, um plano de ação para solução dos apontamentos constantes nos itens 4.1 a 4.15 do Relatório de Auditoria, ou comprove eventuais medidas já iniciadas a respeito.

**ACORDAM**, à unanimidade, em determinar a intimação da Origem, na pessoa do Secretário, bem como da Controladoria Geral do Município, encaminhando-lhes cópia eletrônica integral dos autos, do relatório e voto do Relator e deste Acórdão.

Participaram do julgamento os Conselheiros DOMINGOS DISSEI – Revisor, ROBERTO BRAGUIM e EDUARDO TUMA.

Presente o Procurador-Chefe da Fazenda ROBINSON SAKIYAMA BARREIRINHAS.

Plenário Conselheiro Paulo Planet Buarque, 15 de dezembro de 2021.

JOÃO ANTONIO – Presidente
MAURICIO FARIA – Relator

/cv

Tribunal de Contas
DO MUNICÍPIO DE SÃO PAULO

**I – RELATÓRIO E VOTO DO CONSELHEIRO MAURICIO FARIA – RELATOR**

**Processo:** **TC/002933/2019**
**Origem:** Secretaria Municipal da Educação – SME
**Objeto:** Auditoria Extraplano que tem como objetivo avaliar a efetividade dos controles de segurança implementados na infraestrutura física e lógica instalados no *Data Center* da Secretaria Municipal de Educação – SME

**AUDITORIA EXTRAPLANO. *DATA CENTER* DA SECRETARIA MUNICIPAL DE EDUCAÇÃO. FALHAS E VULNERABILIDADES CONSTADAS. RISCOS QUANTO AOS SISTEMAS E AOS DADOS ARMAZENADOS. APRESENTAÇÃO DE PLANO DE AÇÃO EM 30 DIAS.**

Egrégio Plenário,

Trago a julgamento o TC/002933/2019 que consiste em Auditoria Extraplano, prevista no Regimento Interno deste Tribunal, que tem como objetivo avaliar a efetividade dos controles de segurança implementados na infraestrutura física e lógica instalados no *Data Center* da Secretaria Municipal de Educação – SME.

A Auditoria apresentou as seguintes constatações preliminares no Relatório, cuja estrutura original é reproduzida:

4.1. A inexistência de um contrato de manutenção vigente representa um risco à continuidade dos sistemas, serviços e processos de negócios hospedados sob a infraestrutura do *Data Center* SME, situação que poderá resultar em perdas irreparáveis para os dados hospedados no ambiente tecnológico;

4.2. As vulnerabilidades encontradas no sistema de fornecimento e contingenciamento de energia elétrica instalado no *Data Center* SME representam uma não conformidade em relação ao projeto original do ambiente, abrindo possibilidade de que o Centro de Dados perca as certificações alcançadas e coloque em risco as informações nele hospedadas;

4.3. As vulnerabilidades encontradas no sistema de climatização instalado no *Data Center* SME representam uma não conformidade em relação ao projeto original do ambiente, abrindo possibilidade de que o Centro de Dados perca as certificações alcançadas e coloque em risco as informações nele hospedadas;

4.4. A inexistência de evidências da realização de ensaios de funcionamento do Sistema de Proteção Contra Incêndio instalado no *Data Center* SME abre possibilidade de que o Centro de Dados perca as certificações alcançadas e coloque em risco as informações nele hospedadas;

4.5. A infraestrutura de telecomunicações implantada no *Data Center* SME é parcialmente adequada, pois a solução de redundância existente não está alinhada às orientações da norma ABNT ISO/IEC 27.002:2013;

4.6. A inexistência de um Plano de Continuidade de Negócios – PCN formalizado e aprovado pela instituição contribui para o aumento das chances de perdas irreparáveis das informações, serviços e processos de negócios providos pelo Órgão;

4.7. A inexistência de um Site Backup constitui uma fragilidade para salvaguarda da segurança das informações e para continuidade dos serviços e processos de negócios providos;

4.8. A inexistência de uma Política de Segurança da Informação - PSI formalizada e aprovada pela instituição contribui para o aumento das chances de fraudes ou de perdas irreparáveis das informações custodiadas pelo Órgão;

4.9. A inexistência de uma Política de Controle de Acesso e de uma Política de Segurança da Informação - PSI formalizadas e aprovadas pela instituição contribui para o aumento das chances de fraudes ou de perdas irreparáveis das informações custodiadas pelo Órgão;

4.10. O processo de Controle de Acesso ao *Data Center* implementado pela SME não está alinhado às recomendações da norma ABNT ISO/IEC 27.002:2013;

4.11. A inexistência de uma Política de Cópias de Segurança ou Backup e de uma Política de Segurança da Informação - PSI formalizadas e aprovadas pela instituição constitui uma não conformidade em relação à norma ISO e Orientações Técnicas da SMIT, assim como contribui para o aumento das chances de fraudes ou de perdas irreparáveis das informações custodiadas pelo Órgão;

4.12. A inexistência de embasamento para determinação dos períodos de retenção dos backups implementadas e o armazenamento inadequado das mídias envolvidas no processo constituem uma não conformidade em relação à norma ABNT ISO/IEC 27.002:2013 e contribuem para o aumento das chances de fraudes ou de perdas irreparáveis das informações custodiadas pelo Órgão;

4.13. A inexistência de um procedimento formalizado para realização de testes de integridade e recuperação no processo de backup implementado constitui uma não conformidade em relação à norma ABNT ISO/IEC 27.002:2013 e às Orientações Técnicas da SMIT, contribuindo para o aumento das chances de fraudes ou de perdas irreparáveis das informações custodiadas pelo Órgão;

4.14. A inexistência de um processo formalizado, aprovado e operacionalizado pela SME para o controle da vida útil e do descarte das mídias utilizadas no processo de backup constitui uma não conformidade em relação à norma ABNT ISO/IEC 27.002:2013 e às Orientações Técnicas da SMIT, contribuindo para o aumento das chances de fraudes ou de perdas irreparáveis das informações custodiadas pelo Órgão;

4.15. É necessário que seja feito um redimensionamento do quantitativo de profissionais de TI da Cotic-SME, levando-se em consideração as demandas da SME. Adicionalmente, recomendamos que seja aumentada a proporção de profissionais com formação em TI.

Ouvida a Assessoria Jurídica de Controle Externo, esta opinou que as constatações preliminares obtidas pela Especializada não apresentavam questões jurídicas a serem esclarecidas. Não obstante, observou que a Resolução TCM 14/2019, então recém-expedida, que disciplina as Auditorias Operacionais, poderia ser aplicada de imediato à presente fiscalização.

Esta Relatoria divergiu do entendimento da Especializada, considerando que os apontamentos constantes do relatório inicial da Auditoria, composto em sua maioria por constatações fáticas sobre as fragilidades apresentadas pela estrutura do *Data Center* da Secretaria Municipal de Educação, não se amoldavam à finalidade precípua da Auditoria Operacional, prevista na Resolução TCM 14/2019, de avaliar a gestão das políticas públicas ou de programas governamentais. Nessa toada, manteve o processamento da presente fiscalização como Auditoria Extraplano, aplicando o Regimento Interno desta Corte de Contas, determinando a oitiva da Origem.

A Secretaria Municipal de Educação prestou esclarecimentos informando ter ciência sobre o prazo de validade da certificação da Sala Cofre e que até a data de encerramento do último contrato de manutenção, as características necessárias para manter a certificação seguiram conservadas, dado que os contratos firmados para manter a manutenção da Sala Cofre, desde sua inauguração e durante o período de sustentação foram celebrados com empresas que possuíam autorização do fabricante e da unidade certificadora para manter a sua operação, de forma a preservar as características da Sala Cofre.

Tornados os autos à Subsecretaria de Fiscalização e Controle, o Grupo Auditor examinou as informações encaminhadas pela Origem, considerou que a resposta apresentada abrangeu apenas os itens 4.2 a 4.4, e, ainda assim, de forma insuficiente, e, por consequência manteve todos os apontamentos (itens 4.1 a 4.15) referentes às irregularidades e inconsistências identificadas no Relatório Inicial.

A Assessoria Jurídica de Controle Externo, em sua manifestação derradeira, não identificou a presença de questões jurídicas de alta indagação, de modo que o exame dos autos permitiu inferir que a Auditoria Extraplano cumpriu plenamente a sua finalidade, que é a de inspecionar e avaliar a efetividade dos controles de segurança implementados na infraestrutura física e lógica do *Data Center* da Secretaria Municipal de Educação, eis que identificou fragilidades capazes de ocasionar sérios problemas ao órgão.

Ouvida a Procuradoria da Fazenda Municipal, esta afirmou que não obstante haja a necessidade de aperfeiçoar alguns procedimentos, restou demonstrado que a Origem está ciente dos problemas existentes no *Data Center* e que está trabalhando para implementar as ações necessárias. Concluiu aduzindo que a Auditoria Extraplano prescinde de análise de mérito e que possui natureza instrumental, razão pela qual pugna pelo conhecimento e

registro do processado, com eventuais determinações que forem consideradas cabíveis pelo Órgão Julgador.

Encerrando a instrução processual, a Secretaria-Geral entendeu que a Auditoria Extraplano cumpriu os objetivos propostos, reunindo condições de ser submetida à apreciação do Conselheiro Relator, para conhecimento dos resultados alcançados, sem prejuízo das recomendações e determinações que forem consideradas pertinentes, observando-se que a Auditoria revelou a existência de fragilidades e vulnerabilidades que podem colocar em risco a salvaguarda das informações custodiadas pela SME, o que evidencia a necessidade de aprimoramento dos controles internos e das operações pertinentes ao *Data Center*.

É o relatório.

## V O T O

O objetivo principal da presente Auditoria Extraplano era avaliar a efetividade dos controles de segurança existentes na infraestrutura física e lógica do *Data Center* da Secretaria Municipal de Educação, que, por definição, consiste em uma estrutura física que abriga os recursos necessários para o armazenamento e gerenciamento de servidores, rede e telecomunicação.

É neste ambiente tecnologicamente protegido que as informações de uma organização – seja ela pública ou privada –, são processadas, sendo função do *Data Center* disponibilizar os equipamentos para que os sistemas essenciais funcionem adequadamente e permitam que, no caso em tela, a Secretaria Municipal de Educação possa executar suas atividades cotidianas.

Ou seja, na atualidade, os *Data Centers* são indispensáveis para a consecução de um enorme contingente de atividades humanas e, portanto, falhas ocorridas nesses centros de informação podem ter consequências desastrosas, como a perda irreparável de dados ou informações, a paralisação de atividades de uma organização ou mesmo o vazamento de informações pessoais protegidas.

Por esta razão, há diversas normas técnicas, procedimentos e equipamentos que devem compor a construção e a manutenção de *Data Centers,* para mitigar os riscos existentes. A Auditoria selecionou alguns desses itens de segurança, por critério de relevância e criticidade, e verificou sua implementação na Secretaria Municipal da Educação.

Assim, o Relatório de Auditoria abrangeu os sistemas de controle de segurança física no acesso à Sala-Cofre, os processos de provisionamento (gerenciamento de acesso aos dados e recursos), a manutenção de centro de contingência (sistema *back-up*), a manutenção de uma equipe de monitoramento em tempo integral, o sistema de climatização que serve para manutenção de umidade e temperatura constantemente em padrões adequados, o sistema que garante o fornecimento contínuo de energia elétrica (gerador), o sistema de combate e prevenção a incêndios e a política de segurança da informação.

Ao examinar tais itens, a Auditoria constatou várias falhas, extremamente relevantes, que se colocam como sérios riscos às atividades da Secretaria Municipal de Educação, que na instrução processual limitou-se a informar sobre ciência sobre a certificação da Sala-Cofre, mas não tratou de questões fundamentais que demandam atuação imediata.

As infringências e irregularidades podem ser sintetizadas como: (i) inexistência de um contrato de manutenção dos equipamentos do *Data Center;* (ii) falhas no sistema de fornecimento e contingenciamento de energia elétrica, no sistema de climatização e no sistema de proteção contra incêndios, o que ameaça a integridade física dos equipamentos e dos dados armazenados, já que não há uma política de *back-up*; (iii) inexistência de Política de Controle de Acessos, de Plano de Continuidade de Negócios, de Política de Segurança da Informação, de procedimentos de testes de integridade e de controle da vida útil das mídias utilizadas, o que aumenta as chances de fraudes ou perdas irreparáveis dos dados da Secretaria Municipal de Educação; (iv) insuficiência do quadro de profissionais com formação específica e adequada para atuar na Coordenadoria responsável pela área de tecnologia da informação na Pasta.

Tais apontamentos merecem atenção, pois constituem riscos de adulteração de dados ou mesmo de vazamentos de dados, já que a Secretaria Municipal de Educação possui um expressivo banco de dados com informações pessoais dos educandos que devem ser protegidas nos termos da Lei Geral de Proteção de Dados (Lei Federal n.º 13.709/2018). Além disso, há também risco para a prestação dos serviços de educação, pois os sistemas armazenados no *Data Center* são utilizados para atividades escolares cotidianas, como registro de frequência, diário de classe, avaliações, ou para atividades administrativas, por sistemas como o Escola Online – EOL e o Sistema de Gestão Pedagógica – SGP.

Assim, as inconsistências e vulnerabilidades constatadas pelo Relatório de Auditoria precisam ser enfrentadas de imediato pela Secretaria Municipal de Educação, a fim de eliminar ou mitigar os riscos constatados.

Diante do exposto, **CONHEÇO** da Auditoria Extraplano para fins de **REGISTRO.**

**DETERMINO** que a Secretaria Municipal de Educação apresente, no prazo de 30 (trinta dias), um **PLANO DE AÇÃO** para solução dos apontamentos constantes dos itens 4.1 a 4.15 do Relatório de Auditoria, ou comprove eventuais medidas já encetadas a respeito.

**INTIME-SE** a Origem, na pessoa do Secretário Municipal de Educação, bem como a Controladoria Geral do Município, encaminhando-se cópia eletrônica integral dos autos, deste voto e do acórdão que vir a ser prolatado pelo E. Pleno desta Corte de Contas.

Plenário Conselheiro **PAULO PLANET BUARQUE, 15 de dezembro de 2021.**

***MAURICIO FARIA***
*Conselheiro*