TC/006545/2023

**Objeto:** Infraestrutura de TI - Avaliação de Data Center

**Interessados:** Secretaria Municipal da Saúde (*)

**Relator:** Ricardo Torres

**Competência:** PLENO

**SENHORA SECRETÁRIA-GERAL**

Trata-se de *Auditoria de Conformidade*[1] realizada no âmbito da Secretaria Municipal da Saúde (SMS) com o objetivo abaixo transcrito:

> *Avaliar se o Data Center da SMS atende as normas técnicas e as boas práticas de segurança da informação.*

Com base na análise da documentação de suporte, evidências coletadas em diligências à SMS e vistoria *in loco* no Data Center da SMS, a Auditoria elaborou o relatório encartado na Peça 06, concluindo o quanto segue:

> ***5. CONCLUSÃO***
>
> *A partir das análises realizadas no presente trabalho, concluiu-se que:*
>
> ***5.1.*** *Não é possível assegurar que a infraestrutura e utilidades implantadas do DC da SMS estão alinhadas com as premissas de sua Política de Segurança da Informação (item 3.1);*
>
> ***5.2.*** *Não é possível assegurar que o processo de Segurança de Acesso Físico seja efetivo e suficiente para assegurar o acesso autorizado e evitar o acesso não autorizado, danos e interferências nas informações da organização e outros ativos associados, e prevenir ou reduzir as consequências de eventos originários de ameaças físicas e ambientais (item 3.2);*
>
> ***5.3.*** *Não é possível assegurar que a Política de Backup implantada no DC da SMS seja efetiva, em razão de diversas recomendações apresentadas*

[1] O período de abrangência da auditoria foi de 07.06.2023 a 13.07.2023 e o período de realização, de 02.06.2023 a 17.08.2023 (Peça 06).

*na NBR ISO 27002/22 não serem possíveis de serem asseguradas ou desatendidas (item 3.3);*

***5.4.*** *Não há procedimento formal para a Política de Continuidade do Negócio e da Segurança da Informação do ambiente do DC (item 3.4);*

***5.5.*** *A ausência de redundância de recursos da infraestrutura do DC da SMS não atende aos requisitos de segurança (item 3.5);*

***5.6.*** *Não há procedimento formal para a gestão de capacidade do ambiente do DC (item 3.6);*

***5.7.*** *O processo de gestão de mudanças apresentado no documento no Plano de Gestão de Mudanças não é efetivo e não se mostra suficiente para preservar a segurança da informação ao executar mudanças (item 3.7).*

## *6. ELEMENTOS DE RESPONSABILIZAÇÃO*

*Não foram constatados, neste trabalho, achados que denotem irregularidades, tampouco a ocorrência de danos ao erário, não havendo pressupostos de responsabilização no presente caso.*

## *7. PROPOSTA DE ENCAMINHAMENTO*

***7.1.*** *Propostas de recomendações*
***7.1.1.*** *Aprimorar a Política de Segurança da Informação e procedimentos de controle voltados a preservar a segurança da informação no ambiente do Data Center, contextualizado aos requisitos de negócio da Secretaria Municipal da Saúde (item 3.1.1);*

***7.1.2.*** *Aprimorar a Política de Segurança de Acesso Físico, definindo procedimentos voltados a assegurar o acesso autorizado e evitar o acesso não autorizado, danos e interferências nas informações da organização e outros ativos associados, e prevenir ou reduzir as consequências de eventos originários de ameaças físicas e ambientais (item 3.2.1);*

***7.1.3.*** *Aprimorar a Política de Backup, definindo responsabilidades e procedimentos voltados à segurança da informação ao executar o backup e a restauração das informações armazenadas no Data Center, elaborando acessoriamente procedimento operacional padrão para a realização de backups e restaurações, contextualizado à realidade e adequado às necessidades da Secretaria Municipal da Saúde. Sugere-se ainda alinhar a política de backup à OT nº 07 - Backup e armazenamento de dados (item 3.3.1);*

> ***7.1.4.*** *Elaborar a Política de Continuidade do Negócio para o ambiente do Data Center, contextualizado à realidade e às diretrizes traçadas pela Secretaria Municipal da Saúde (item 3.4.1);*
>
> ***7.1.5.*** *Aprimorar a Política de Segurança da Informação, identificando os requisitos para a disponibilidade de serviços de negócios e sistemas de informação, incorporando o planejamento de eventual arquitetura de sistemas com redundância de recursos de infraestrutura do Data Center adequada para atender aos requisitos de negócio da Secretaria Municipal da Saúde para o funcionamento contínuo do tratamento de informações (item 3.5.1);*
>
> ***7.1.6.*** *Elaborar o Plano de Gestão da Capacidade para o ambiente do Data Center, contextualizado à realidade e às diretrizes traçadas pela Secretaria Municipal da Saúde (item 3.6.1);*
>
> ***7.1.7.*** *Elaborar o Plano de Gestão de Mudanças, definindo responsabilidades e procedimentos voltados a preservar a segurança da informação ao executar mudanças no ambiente do Data Center, contextualizado à realidade e às diretrizes traçadas pela Secretaria Municipal da Saúde (item 3.7.1).*

Intimada para manifestação quanto ao concluído pela Auditoria, a SMS informou, em síntese, que se encontrava em processo de mudança de sede e em fase de aprovação de políticas e procedimentos elaborados para garantir a Segurança da Informação. Com relação à mudança da sede, asseverou que tal fato teria ocasionado melhorias *alinhadas com as pontuações estipuladas* no Relatório de Auditoria de Conformidade – *controle de acesso ao Data Center; implementação de câmeras de segurança; melhorias no sistema de ar condicionado; garantia da presença de extintores de incêndio (detector de fumaça e prevenção e combate); adequações no layout da sala; revisão e aprimoramento do procedimento de backup; verificação e manutenção dos links de comunicação.* Quanto às novas políticas, informou que estava *em processo de adequação juntamente com os procedimentos, conforme estabelecido no Plano de Adequação e Mapeamento de Dados iniciado em 03/01/2024* (Peças 22/23).

Na sequência, os autos foram encaminhados para a Auditoria, que, após análise dos esclarecimentos trazidos pela SMS, considerou *a conclusão e os achados do Relatório de Auditoria de Conformidade* ***prejudicados em razão da consecução de um novo Data Center*** e, nesse contexto**, sugeriu *a realização de uma nova auditoria no novo* local *em momento oportuno*** (Peça 27).

Por fim, a Procuradoria da Fazenda Municipal requereu o conhecimento e o registro da Auditoria (Peça 30).

De minha parte, acompanho o entendimento da Auditoria no sentido de que, de fato, os achados do Relatório de Auditoria de Conformidade restaram prejudicados, pois as conclusões alcançadas se referem à infraestrutura do antigo local do Data Center.

Nesse contexto, entendo que a presente auditoria reúne condições de ser submetida à apreciação do Nobre Conselheiro Relator, para conhecimento e deliberação, conforme disposto no parágrafo único do art. 11 da Resolução nº 06/00[2] (redação conferida pelo art. 1º da Resolução nº 02/02).

É o meu parecer que submeto à consideração de Vossa Senhoria.

São Paulo, 17 de setembro de 2024.

**DANIELA SHIMIZU**
**Auditora de Controle Externo**
**OAB/SP 208.355**

[2] Art. 11, parágrafo único, da Resolução nº 06/00 (redação conferida pelo art. 1º da Resolução nº 02/02):
*O Relator, ao apreciar o relatório de auditoria, deliberará sobre a conveniência e oportunidade de submetê-lo à apreciação do Plenário ou sobre a sua remessa ao processo das contas anuais, para subsidiar seu julgamento, podendo expedir determinações ou recomendações tendentes ao aperfeiçoamento dos órgãos, atividades ou serviços auditados para, se for o caso, posterior confronto.*