

Processo - TC/006545/2023
Auditada - Secretaria Municipal da Saúde
Objeto - Auditoria Programada – Avaliar se o Data Center da Secretaria atende às normas técnicas e as boas práticas de segurança da informação

73ª Sessão Ordinária Não Presencial

AUDITORIA. SMS. AVALIAR. DATA CENTER. NORMAS TÉCNICAS E AS BOAS PRÁTICAS DE SEGURANÇA DA INFORMAÇÃO. 1. A superveniente alteração das condições fáticas que fundamentaram auditoria de conformidade, notadamente a mudança de sede e a modificação substancial da infraestrutura avaliada, prejudica a análise anteriormente realizada, por ausência de aderência entre o objeto auditado e a realidade atual. 2. A implementação superveniente de políticas, procedimentos e controles de segurança da informação, bem como a instalação de novo ambiente físico (Data Center), impõe a realização de nova auditoria após a estabilização da infraestrutura, a fim de assegurar avaliação atual, adequada e fidedigna às normas técnicas e às boas práticas aplicáveis. NBR ISO/IEC 27002:2022. 3. Perda de objeto. PREJUDICADA. Votação unânime.

ACÓRDÃO

Vistos e relatados estes autos, dos quais é Relator o Conselheiro RICARDO TORRES.

ACORDAM os Conselheiros do Tribunal de Contas do Município de São Paulo, à unanimidade, de conformidade com o relatório e voto do Relator, em declarar prejudicada a presente auditoria programada, na forma do quanto opinado pelas Áreas Técnicas desta Corte, tendo em vista a mudança de sede do Data Center, e da implementação das políticas, procedimentos e controles de segurança da informação.

ACORDAM, à unanimidade, em determinar à **Secretaria de Controle Externo** a realização de nova auditoria no Data Center, em momento oportuno, após a efetiva estabilização da mudança definitiva de sede, conforme requerido pela SMS (Peça 23) e de acordo com as manifestações das Áreas Técnicas deste Tribunal, acostadas às Peças 27, 32 e 33.

ACORDAM, à unanimidade, em determinar o envio de cópia do relatório e voto do Relator e deste Acórdão ao Secretário Municipal da Saúde e às demais partes interessadas no feito, para ciência.

ACORDAM, afinal, à unanimidade, em determinar, após o trânsito em julgado com as cautelas de praxe, o arquivamento dos autos.

Participaram do julgamento os Conselheiros ROBERTO BRAGUIM – Revisor, JOÃO ANTONIO e EDUARDO TUMA.

São Paulo, 17 de dezembro de 2025.

DOMINGOS DISSEI – Presidente
RICARDO TORRES – Relator

/affo

Processo: TC/006545/2023
Origem: Secretaria Municipal da Saúde
Objeto: Infraestrutura de TI - Avaliação de Data Center

AUDITORIA DE CONFORMIDADE.
SEGURANÇA DA INFORMAÇÃO. DATA
CENTER DA SECRETARIA MUNICIPAL DA
SAÚDE

1. Alteração substancial da realidade fática, consubstanciada na mudança física de sede, na implementação de melhorias estruturais e na revisão das políticas e controles de segurança da informação, circunstâncias que descaracterizaram o ambiente originalmente auditado. 2. Manifestação das Áreas Técnicas reconhecendo a ausência de aderência entre o objeto auditado e o ambiente atual.

PERDA SUPERVENIENTE DO OBJETO –
PREJUDICIALIDADE.

RELATÓRIO

Egrégio Plenário,

Trago a julgamento auditoria de conformidade com o objetivo de avaliar, do ponto de vista da Segurança da Informação, se a infraestrutura de Tecnologia da Informação (TI), representada pelo *data center* da Secretaria Municipal da Saúde, atende às normas técnicas e as boas práticas de segurança da informação.

A equipe de auditoria elaborou relatório acostado à Peça 6 tendo constatado uma série de achados de auditoria e emitido diversas propostas de recomendação:

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 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).

Ocorre que o DTIC da SMS, à Peça 23, informou que houve mudança física do local de instalação e funcionamento Data Center. Em sua visão, o novo local dispõe de algumas melhorias nas instalações, o que tornaria o relatório anterior *desatualizado*:

Considerando o relatório de auditoria de conformidade destinado a avaliar se o Data Center da SMS está em conformidade com as normas técnicas e as melhores práticas de segurança da informação, gostaríamos de ressaltar a sugestão de uma nova inspeção em nosso Data Center. Isso se deve à recente mudança física de local, pois agora estamos situados na Rua Dr. Siqueira de Campos, 176, 9º andar, Bairro Liberdade, São Paulo/SP. Esta mudança resultou em algumas melhorias em nossas instalações, tornando assim o relatório anterior desatualizado.

Acrescenta que, atualmente, encontram-se em processo de mudança de sede e em fase de aprovação de políticas e procedimentos elaborados para garantir a Segurança da Informação. Com a mudança para um novo prédio, argumenta que as melhorias no Data Center estariam alinhadas com as pontuações estipuladas no Relatório de Auditoria de Conformidade, incluindo:

- (i) Controle de acesso ao Data Center;
- (ii) Implementação de câmeras de segurança;
- (iii) Melhorias no sistema de ar-condicionado;
- (iv) Garantia da presença de extintores de incêndio (detector de fumaça e prevenção e combate);
- (v) Adequações no layout da sala;
- (vi) Revisão e aprimoramento do procedimento de backup;
- (vii) Verificação e manutenção dos links de comunicação.

Finaliza a manifestação informando que em relação às políticas, estavam em processo de adequação juntamente com os procedimentos, conforme estabelecido no Plano de Adequação e Mapeamento de Dados iniciado em 03/01/2024.

A Auditoria, em Manifestação acostada à Peça 27, entende que, considerando os esclarecimentos apresentados pelo DTIC da SMS, de fato, os achados do Relatório de Auditoria de Conformidade tornam-se *prejudicados*, pois as conclusões foram alcançadas considerando a infraestrutura encontrada no Data Center vistoriado à época.

Em sua visão, a realização de uma simples inspeção para a avaliação do novo Data Center em relação aos achados do Relatório de Auditoria de Conformidade não seria adequada, pois se trata de um Data Center completamente novo, o que demandaria uma nova avaliação para o atingimento dos objetivos de avaliar se o Data Center da SMS atende às normas técnicas e às boas práticas de segurança da informação.

Nesses termos, considerou as conclusões do relatório *prejudicadas*, e sugeriu a realização de uma nova auditoria, em um período oportuno, para avaliar se o Data Center da SMS atende às

normas técnicas e às boas práticas de segurança da informação, considerando as informações de que o DTIC da SMS se encontra em “processo de mudança de sede e em fase de aprovação de políticas e procedimentos elaborados para garantir a Segurança da Informação”.

Em seguida, a Procuradoria da Fazenda Municipal (Peça 30) manifestou-se no seguinte sentido:

Em face do exposto, considerando a natureza adjetiva e instrumental deste processado, o qual prescinde de análise de mérito, a Fazenda requer seja a presente Auditoria conhecida e registrada, sem embargo da realização de novas diligências, à critério do Nobre Conselheiro Relator.

Por fim, a Secretaria Geral (Peças 32 e 33) acompanhou o entendimento da Área Técnica deste Tribunal no sentido de que o relatório de auditoria de conformidade restou *prejudicado*, pois se refere à infraestrutura do antigo local do data center do órgão fiscalizado. Ao final, opinou no sentido de que os trabalhos realizados nestes autos de auditoria de conformidade merecem ser submetidos ao conhecimento e deliberação superior

É o Relatório.

VOTO

É o caso de julgar PREJUDICADA a presente auditoria de conformidade, determinando-se a realização de nova auditoria no novo Data Center em momento oportuno, após a efetiva estabilização da mudança definitiva de sede, conforme requerido pela SMS e opinado pelas áreas técnicas.

1. Trago a julgamento auditoria de conformidade com o objetivo de avaliar, do ponto de vista da Segurança da Informação, se a infraestrutura de Tecnologia da Informação (TI), representada pelo *data center* da Secretaria Municipal da Saúde, atende às normas técnicas e as boas práticas de segurança da informação.

2. Após a realização de diligências à SMS e vistoria *in loco* ao Data Center da SMS, foi elaborado o Relatório de Auditoria de conformidade (peça 6), tendo sido considerados os preceitos da NBR ISO 27002/22 possíveis de serem aplicados ao ambiente do Data Center da SMS, abrangendo controles organizacionais, físicos e tecnológicos relacionados na NBR ISO 27002/22, concernentes ao ambiente do Data Center da SMS.

3. No entanto, o Departamento de Tecnologia da Informação e Comunicação da Secretaria Municipal da Saúde (DTIC/SMS), por meio da Peça 23, informou que houve mudança física do local de instalação e funcionamento Data Center. Em sua visão, o novo local dispõe de algumas melhorias nas instalações, o que tornaria o relatório anterior *desatualizado*.

4. Com a mudança para um novo prédio e com a implementação de políticas e procedimentos elaborados para garantir a Segurança da Informação, a SMS entende que as melhorias no Data

Center estariam alinhadas com as pontuações estipuladas no Relatório de Auditoria de Conformidade, quanto a temas como (i) controle de acesso ao Data Center, (ii) implementação de câmeras de segurança, (iii) presença de extintores de incêndio e detectores de fumaça e etc., propondo a realização de nova avaliação para análise do Data Center atualmente em implantação.

5. A Auditoria, em manifestação acostada à Peça 27, acolheu os esclarecimentos do DTIC/SMS, reconhecendo que os achados restaram *prejudicados* por ausência de aderência entre o objeto auditado e a infraestrutura atual do órgão. Recomendou, assim, que eventual nova auditoria somente seja realizada em momento oportuno, após estabilização do novo ambiente, dada a mudança substancial das condições técnicas que embasaram o relatório original.

5. Dessa forma, acompanho o entendimento das Áreas Técnicas, reconhecendo que as conclusões constantes do Relatório de Auditoria (Peça 6) tornaram-se prejudicadas em razão da superveniente mudança de sede e da implementação das políticas, procedimentos e controles de segurança da informação. Tais circunstâncias inviabilizam a utilização daquele relatório para avaliar, no presente momento, a conformidade do Data Center da Secretaria Municipal da Saúde às normas técnicas e às boas práticas de segurança da informação.

Diante do exposto, julgo no sentido de tornar **PREJUDICADA** a presente auditoria de conformidade, na forma do quanto opinado pelas Áreas Técnicas desta Corte, cujas manifestações encontram-se acostadas às Peças 27, 32 e 33.

DETERMINO a realização de nova auditoria no novo Data Center em momento oportuno, após a efetiva estabilização da mudança definitiva de sede, conforme requerido pela SMS (Peça 23) e

de acordo com as manifestações das Áreas Técnicas desta Corte (Peças 27, 32 e 33).

INTIME-SE a Origem, na pessoa do Sr. Secretário de Saúde, bem como as demais partes interessadas no feito, para ciência do presente voto e do acórdão resultante.

Após o trânsito em julgado, e cumpridas as cautelas de praxe, arquivem-se os autos.

É como Voto.

Plenário Cons. **PAULO PLANET BUARQUE,**

Ricardo Torres
Conselheiro