RELATÓRIO DE INSPEÇÃO

Ordem de Serviço	e-TCM	Período de abrangência	Período da realização
2023/01477	003981/2023	Não se aplica	06.02.23 a 14.07.23

Área auditada

Secretaria Municipal de Educação (SME)

Objeto de auditoria

Monitoramento - Infraestrutura e controles de segurança do *Data Center* da SME.

Valor do objeto de auditoria (em R$)	Montante fiscalizado (em R$)
Não se aplica	Não se aplica

Objetivo da auditoria

Avaliar o cumprimento das determinações exaradas no Acórdão.

Equipe técnica

Maurício Kazuhiro Sato – Auditor de Controle Externo	RF 20.117

LISTA DE QUADROS

Quadro 1 – Processos de contratações desmembradas.....11

LISTA DE SIGLAS

ABNT	–	Associação Brasileira de Normas Técnicas
Cotic	–	Coordenação de Tecnologia da Informação e Comunicação
DC	–	*Data Center*
DRE	–	Diretoria Regional de Educação
IEC	–	*International Electrotechnical Commission*
ISO	–	*International Organization for Standardization*
LGPD	–	Lei Geral de Proteção de Dados
NBR	–	Norma Técnica Brasileira
PCN	–	Plano de Continuidade de Negócios
PMSP	–	Prefeitura do Município de São Paulo
PSI	–	Política de Segurança da Informação
SME	–	Secretaria Municipal de Educação
Smit	–	Secretaria Municipal de Inovação e Tecnologia
SSG	–	Subsecretária-Geral
UPS	–	*Uninterruptible Power Supply*

RESUMO

O presente relatório refere-se à inspeção realizada, por ordem do Conselheiro Relator (peça 8 – peça 52 do TC nº 002933/2019), com o objetivo de obter informações e dados para verificar a eficácia das medidas já implementadas ou em andamento na Secretaria Municipal de Educação (SME) no intuito de sanear as inconformidades destacadas no Relatório de Auditoria Extraplano (peça 5 – cópia da peça 24 do TC nº 002933/2019) que teve como objetivo avaliar a efetividade dos controles de segurança implementados na infraestrutura física e lógica instalados no *Data Center* (DC) dessa Secretaria.

Posteriormente, tais inconformidades foram novamente analisadas e, em sua integralidade, mantidas em sede de manifestação (peça 6 – cópia da peça 37 do TC nº 002933/2019) e do Acórdão exarado (peça 2 – cópia da peça 52 do TC nº 002933/2019), que determinou à SME que apresentasse um plano de ação para solução dos apontamentos constantes dos itens 4.1 a 4.15 do Relatório de Auditoria, ou comprovasse eventuais medidas já encetadas a respeito –o que foi atendido com a manifestação da SME (peça 7 – cópia da peça 61 do TC nº 002933/2019).

Entre os apontamentos do Relatório de Auditoria Extraplano (peça 5) e mantidos integralmente (peça 6), analisados no presente trabalho, destacam-se:

- 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 (apontamento 4.11 – peça 5, fl. 43);

- 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 a 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 (apontamento 4.12 – peça 5, fl. 43);

- 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 (apontamento 4.14 – peça 5, fl. 43);

- 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 (apontamento 4.15 – peça 5, fl. 43).

SUMÁRIO

1. INTRODUÇÃO 9

1.1. Destinatários da Auditoria 9

1.2. Visão geral do objeto, objetivos e escopo da auditoria 9

1.3. Normas de auditoria aplicadas na realização do trabalho 9

2. METODOLOGIA 9

2.1. Critérios adotados 9

2.2. Métodos de coleta e de análise de dados 10

2.3. Limitações do trabalho de auditoria 10

3. ACHADOS 10

3.1. 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 (apontamento 4.1) 10

3.2. 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 (apontamento 4.2) 13

3.3. 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 (apontamento 4.3) 14

3.4. 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 (apontamento 4.4).....15

3.5. 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 (apontamento 4.5) 16

3.6. A inexistência de um Plano de Continuidade de Negócios – PCN formalizada e aprovada pela instituição contribui para o aumento das chances de perdas irreparáveis das informações, serviços e processos de negócios providos pelo Órgão (apontamento 4.6) 17

3.7. 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 (apontamento 4.7).....18

3.8. 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 (apontamento 4.8) 19

3.9. 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 (apontamento 4.9) 19

3.10. 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 (apontamento 4.10) 21

3.11. 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 (apontamento 4.11) 22

3.12. 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 a 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 (apontamento 4.12).....24

3.13. 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 (apontamento 4.13).....25

3.14. 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 (apontamento 4.14) 26

3.15. 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 (apontamento 4.15) 27

4. CONCLUSÃO 28

5. ANÁLISE DOS ELEMENTOS DE RESPONSABILIZAÇÃO.....28

6. PROPOSTAS DE ENCAMINHAMENTOS 28

6.1. Propostas de Recomendação.....29

1. INTRODUÇÃO

A inspeção foi instaurada em atenção ao encaminhado pela SCE (peças 9 e 10), para atendimento do determinado pelo Conselheiro Relator (peça 8 – peça 52 do TC nº 002933/2019), em razão dos resultados do Relatório de Auditoria Extraplano (peça 5 – cópia da peça 24 do TC nº 002933/2019), manifestação (peça 6 – cópia da peça 37 do TC nº 002933/2019) e do acórdão exarado (peça 2 – cópia da peça 52 do TC nº 002933/2019), que teve como objetivo avaliar a efetividade dos controles de segurança implementados na infraestrutura física e lógica instalados no *Data Center* (DC) da Secretaria Municipal de Educação (SME), considerando a manifestação da SME (peça 7 – cópia da peça 61 do TC nº 002933/2019).

1.1. Destinatários da Auditoria

O órgão jurisdicionado ao qual se vincula o objeto da fiscalização é a Secretaria Municipal de Educação (SME).

1.2. Visão geral do objeto, objetivos e escopo da auditoria

Este trabalho tem por objetivo avaliar a efetividade dos controles de segurança implementados na infraestrutura física e lógica instalados no *Data Center* (DC) da Secretaria Municipal de Educação (SME), considerando a manifestação da SME (peça 7 – cópia da peça 61 do TC nº 002933/2019).

1.3. Normas de auditoria aplicadas na realização do trabalho

A auditoria foi conduzida, no que foi cabível, em conformidade com o Manual de Auditoria Governamental (MAG) e o Manual de Segurança da Informação, ambos elaborados e aplicados pelo Corpo de Auditores do TCMSP, em concordância com as Normas Brasileiras de Auditoria do Setor Público (NBASP).

2. METODOLOGIA

2.1. Critérios adotados

Entre os principais critérios aplicáveis ao objeto examinado destacam-se:

- Manual de Segurança da Informação;
- Normas NBR ISSO 27.000.

2.2. Métodos de coleta e de análise de dados

Foram realizados os seguintes procedimentos de auditoria:

- Obtenção de documentação e vistoria *in-loco*;
- Análise das correções propostas pela SME;
- Verificação da aderência às normas que regulamentam o objeto;
- Elaboração do Relatório de Inspeção reportando as condições de funcionamento verificadas.

2.3. Limitações do trabalho de auditoria

Não houve limitações ao trabalho de auditoria.

3. ACHADOS

Considerando a manifestação da SME (peça 7), a fim de avaliar a adoção dos procedimentos informados, foram solicitadas esclarecimentos e informações complementares e atualizadas quanto as providências adotadas (peças 11 e 12), e vistoria *in loco* realizada em 27.04.23.

A verificação das providências propostas e situação atualizada foi realizada conforme a sequência dos apontamentos que constaram da conclusão do Relatório de Auditoria Extraplano (peça 5, fls. 41/43).

3.1. 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 (apontamento 4.1)

Manifestação da SME (peça 7)

Conforme manifestação em resposta à comunicação do Acórdão exarado (peça 7), a SME informou que foi instaurado o processo SEI nº 6016.2021/0109523-9 visando a contratação de empresa especializada para prestação de serviços de manutenção preventiva, corretiva e evolutiva com suporte técnico e fornecimento e substituição de peças, para o *Data Center*, ressaltando que a contratação pretendida estaria em conformidade com as Orientações Técnicas da Smit, esclarecendo que o contrato anterior firmado entre SME e Green 4T não foi prorrogado, citando o documento SEI nº 029708146, encerrado em 09.06.20 por determinação do gabinete da SME à época, que direcionou a realização de novas contratações desmembrando os itens, resultando nos processos conforme o Quadro 1:

Quadro 1 – Processos de contratações desmembradas

Processo	Objeto
6016.2020/0068985-0	Contratação de empresa especializada para prestação de serviços de manutenção preventiva, corretiva e evolutiva com suporte técnico e fornecimento e substituição de peças, pelo período de 12 meses dos equipamentos do Sistema de Climatização de *Datacenter*
Resultado: Contrato nº 04/SME/2021 (assinado em 29.01.21), firmado com a empresa Gtermica Comercio Soluções Eireli. Valor Mensal: R$ 2.000,00 – Valor Total (12 meses): R$ 24.000,00	
6016.2020/0069131- 6	Contratação de Empresa especializada para prestação de serviços de manutenção preventiva, corretiva e evolutiva com suporte técnico e fornecimento e substituição de peças, pelo período de 12 meses dos componentes do Grupo Gerador
Resultado: Contrato nº 03/SME/2021 (assinado em 29.01.21), firmado com a empresa G2R Manutenção e Serviços Ltda. ME. Valor Mensal: R$ 533,34 – Valor Total (12 meses): R$ 6.400,08	
6016.2020/0069740-3	Contratação de Empresas especializadas para prestação de serviços de manutenção preventiva, corretiva e evolutiva com suporte técnico, fornecimento e substituição de peças, pelo período de 12 meses dos equipamentos UPS (*Uninterruptible Power Supply*) *Nobreak*
Resultado: Não houve contratação em virtude das dezenove respostas negativas fornecidas durante a realização da pesquisa de mercado - documento SEI nº 038623198. Valor Referência Mensal: R$ 46.330,67 – Valor Ref. (12 meses): R$ 555.968,04	
6016.2020/0069997-0	Contratação de Empresa especializada para prestação de serviços de manutenção preventiva, corretiva e evolutiva com suporte técnico e fornecimento e substituição de peças, exceto para os itens de climatização, UPS e gerador, pelo período de 12 (doze) meses da Sala Cofre
Resultado: Não houve contratação em virtude das dezesseis respostas negativas fornecidas durante a realização da pesquisa de mercado - documento SEI nº 038625955. Valor Referência Mensal: R$ 38.847,50 – Valor de Referência (12 meses): R$ 466.170,00	

Fonte: Elaborado com base no quadro do item (i) da manifestação da SME (peça 7, fls. 4/6).

Argumenta que com o fracionamento do objeto, foram contratadas por dispensa de licitação duas empresas, a GTermica e a G2R para prestarem serviços de manutenção de geradores e climatização, respectivamente, e que nos outros dois processos (UPS e manutenção do DC), em razão do número de respostas negativas recebidas na elaboração de pesquisa de mercado

e o alto valor de referência, não prosseguiu, ressaltando que a soma dos valores (contratados e valores referencias) resultariam no valor mensal de R$ 87.711,51, valor este superior ao contratado anteriormente que era de R$ 50.500,00.

Diante do exposto e para mitigar os riscos existentes, informou ter instaurado processo licitatório visando a contratação da empresa especializada para manutenção e a recertificação do DC (peça 7, fl. 6).

Resposta da SME à requisição de informações (peça 11)

Em resposta à requisição de informações (peça 11, fls. 2/6), a SME complementou as informações prestadas na manifestação (peça 7), esclarecendo que o procedimento licitatório informado teve como vencedora a empresa Green4T Soluções TI Ltda., que teve sua proposta aceita no valor de R$ 1.294.000,00 para o período de 24 meses, R$ 53.916,67 mensais. Em razão de questão superveniente ao seu início relacionada à exigência da norma ABNT NBR nº 15247, houve a revogação do procedimento licitatório (Ofício SSG nº 13290/2022 – TC nº 004885/2022 – Processo Eletrônico SEI nº 6016.2022/0027920-6).

Após a revogação do processo licitatório, um novo processo foi realizado por meio do processo SEI nº 6016.2022/0046498-4, visando a contratação de empresa especializada para prestação de serviços de manutenção preventiva, corretiva e evolutiva com suporte técnico e fornecimento e substituição de peças, pelo período de 24 meses dos seguintes itens: Sistema de Climatização, Grupo Gerador, Sistema de *Nobreak* (UPS) e Sala Cofre, que teve a empresa GLS Engenharia e Consultoria declarada vencedora, resultando no Contrato nº 377/SME/2022, conforme cópia encaminhada (peça 11, fls. 304/330).

Situação encontrada

Foi constatada na vistoria que a empresa contratada GLS Engenharia estava prestando os serviços contratados, corroborando os esclarecimentos apresentados pela SME. Foi verificada a presença de técnicos da contratada no local, além das evidências documentais apresentadas na manifestação (peça 11, fls. 744/765). Foi constata significativa evolução nas condições gerais do ambiente do DC, indicando a efetividade da contratação.

Análise e conclusão

Considerando os esclarecimentos apresentados e as constatações da vistoria *in loco*, conclui-se que a SME tem adotado providências para a solução do problema apontado.

3.2. 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 (apontamento 4.2)

Manifestação da SME (peça 7)

Conforme a manifestação (peça 7) em resposta à comunicação do Acórdão exarado, a SME informou que não houve contratação para prestação de serviços de manutenção dos equipamentos *Uninterruptible Power Supply* (UPS) *Nobreak* em razão das 19 respostas negativas fornecidas durante a realização da pesquisa de mercado, citando o documento SEI nº 038623198 (vide Quadro 1 do item 3.1), argumentando que estaria em curso uma nova contratação de empresa especializada na manutenção do DC, com objetivo mitigar as falhas no sistema de fornecimento e contingenciamento de energia elétrica, no sistema de climatização e no sistema de proteção contra incêndios, preservando a integridade física dos equipamentos e dos dados armazenados (peça 7, fl. 6).

Resposta da SME à requisição de informações (peça 11)

Conforme esclarecimento apresentado pela SME (peça 11, fl. 6), a contratação da empresa GLS Engenharia e Consultoria Ltda. (Contrato nº 377/SME/2022 – peça 11, fls. 304/330) engloba a prestação de serviços no Grupo Gerador e Sistema de *Nobreak* (UPS).

Situação encontrada

Foi constatada na vistoria que as condições gerais do ambiente do DC sofreram significativa evolução, com a manutenção dos sistemas gerados / UPS.

Análise e conclusão

Considerando os esclarecimentos apresentados e as constatações da vistoria *in loco*, conclui-se que a SME tem adotado providências para a solução do problema apontado.

3.3. 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 (apontamento 4.3)

Manifestação da SME (peça 7)

Conforme constou das informações apresentadas no quadro do item (i) da manifestação da SME (peça 7, fl. 4), a contratação de empresa especializada para prestação de serviços de manutenção dos equipamentos do Sistema de Climatização do DC foi realizada por meio do processo SEI nº 6016.2020/0068985-0, que teve como resultado o Contrato nº 04/SME/2021, assinado em 29.01.21, firmado com a empresa Gtermica Comercio Soluções Eireli, no valor mensal: R$ 2.000,00.

Argumenta ainda que estaria em curso uma nova contratação de empresa especializada na manutenção do DC, que teria como objetivo mitigar as falhas no sistema de fornecimento e contingenciamento de energia elétrica, no sistema de climatização e no sistema de proteção contra incêndios, preservando a integridade física dos equipamentos e dos dados armazenados (peça 7, fl. 6).

Resposta da SME à requisição de informações (peça 11)

Conforme esclarecimento apresentado pela SME (peça 11, fl. 6), a contratação da empresa GLS Engenharia e Consultoria Ltda. (Contrato nº 377/SME/2022 – peça 11, fls. 304/330) engloba a prestação de serviços de manutenção preventiva, corretiva e evolutiva com suporte técnico e fornecimento e substituição de peças dos seguintes itens: Sistema de Climatização, Grupo Gerador, Sistema de *Nobreak* (UPS) e Sala Cofre.

Situação encontrada

Foi constatada na vistoria que as condições gerais do ambiente do DC sofreram significativa evolução, com a manutenção dos sistemas climatização e monitoramento da temperatura do ambiente do DC.

Análise e conclusão

Considerando os esclarecimentos apresentados e as constatações da vistoria *in loco*, conclui-se que a SME tem adotado providências para a solução do problema apontado.

3.4. 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 (apontamento 4.4)

Manifestação da SME (peça 7)

Em sua manifestação, a SME informou ter instaurado processo licitatório visando a contratação da empresa especializada para manutenção e a recertificação do DC (peça 7, fl. 6).

Resposta da SME à requisição de informações (peça 11)

Conforme esclarecimento apresentado pela SME (peça 11, fl. 7), a contratação da empresa GLS Engenharia e Consultoria Ltda. (Contrato nº 377/SME/2022 – peça 11, fls. 304/330) foi resultado da decisão de não limitar o certame licitatório de Manutenção da Sala Cofre a empresas que possuíssem certificação, ressalvando que por esse motivo não teriam como garantir que a Sala manteria todos os requisitos técnicos exigidos para qualquer procedimento de revalidação das certificações.

Resposta da SME à requisição de informações (peça 12)

Conforme esclarecimento apresentado pela SME (peça 12, fl. 1), os ensaios são feitos nas manutenções preventivas trimestralmente conforme o cronograma desde o início do contrato, apresentando as ordens de serviços com ensaios realizados (peça 12, fls. 6/33).

Situação encontrada

Foi constatada na vistoria que as condições gerais do ambiente do DC sofreram significativa evolução, com a manutenção do sistema de prevenção de incêndios do ambiente do DC.

Análise e conclusão

Considerando os esclarecimentos apresentados e as constatações da vistoria *in loco*, conclui-se que a SME tem realizado ensaios de funcionamento do Sistema de Proteção Contra Incêndio.

3.5. 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 (apontamento 4.5)

Manifestação da SME (peça 7)

Conforme constou do item (iii) da manifestação da SME (peça 7, fl. 7), a SME argumentou estar ciente da necessidade de aperfeiçoar alguns procedimentos e que estariam trabalhando na implementação de ações necessárias para suprir as fragilidades existentes, informando ter firmado contrato de expansão da solução de segurança e otimização do enlace de dados, com a Empresa Compwire Informática S/A, por meio do processo SEI nº 6016.2019/0040177-4, para permitir somente a transmissão e a recepção de dados autorizados, e que não seriam permitidas "atividades que comprometam a segurança das informações" e a "utilização de softwares maliciosos para sequestrar de forma criptografada os dados trafegados e sigilosos" na rede da SME.

Resposta da SME à requisição de informações (peça 12)

Conforme esclarecimento apresentado pela SME (peça 12, fls. 1/2), o documento "Dados da infraestrutura de *datacenter*", na guia "*Network Topology*" (peça 12, fl. 34), apresenta a topologia e uma breve descrição da forma como os equipamentos que compõem a solução de telecomunicações estão interligados em redundância, destacando que alguns equipamentos como o Firewall central foram atualizados, porém a lógica da topologia se mantém.

Situação encontrada

Na vistoria realizada, foi informado que a solução de redundância das linhas de comunicação adotada foi a utilização de linhas de comunicação com entradas distintas na edificação, o que garantiria a utilização de circuitos diferentes, mitigando os riscos de interrupção simultânea das linhas, mesmo utilizando a mesma operadora para o fornecimento.

Análise e conclusão

Considerando os esclarecimentos apresentados e as informações prestadas na vistoria *in loco*, conclui-se que a SME tem adotado providências para a solução do problema apontado.

3.6. A inexistência de um Plano de Continuidade de Negócios – PCN formalizada e aprovada pela instituição contribui para o aumento das chances de perdas irreparáveis das informações, serviços e processos de negócios providos pelo Órgão (apontamento 4.6)

Manifestação da SME (peça 7)

A manifestação da SME (peça 7) não apresentou esclarecimento sobre as ações pertinentes à elaboração de um Plano de Continuidade de Negócios ou justificativas para a sua não realização.

Resposta da SME à requisição de informações (peça 11)

Conforme esclarecimento apresentado pela SME (peça 11, fl. 8), o documento que concentra as informações sobre os processos previstos para o restabelecimento dos ambientes e continuidade dos serviços alocados no *Data Center* de SME foi apresentado no anexo 12 (peça 11, fls. 300/303), e a infraestrutura de segurança estava citada no documento do anexo 08, no documento Plano de Gerenciamento da Capacidade – Funcionamento Tecnológico (peça 11, fls. 251/288).

Situação encontrada

A questão não foi abordada na vistoria, considerando que se trata de um apontamento de cunho procedimental que não afeta o ambiente físico do DC.

Análise e conclusão

Considerando os esclarecimentos apresentados, conclui-se que a SME tem adotado providências para a solução do problema apontado.

3.7. 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 (apontamento 4.7)

Manifestação da SME (peça 7)

A manifestação da SME (peça 7) não apresentou esclarecimento sobre as ações pertinentes a planos relacionados a obtenção de um *Site Backup* ou justificativas para a sua não realização.

Resposta da SME à requisição de informações (peça 12)

Conforme esclarecimento apresentado pela SME (peça 12, fl. 2), a SME tem o objetivo de atuar com a virtualização de seu ambiente de *backup*, bem como garantir a disponibilidade dos recursos computacionais, ponderando não identificaram a necessidade de espelhar integralmente a estrutura em uma solução de *Site Backup*, mas que para garantir uma alternativa de segurança das informações e dados, uma opção seria criar um ambiente com equivalência a *Disaster Recover* em Nuvem, destacando que as melhorias dependem também de viabilidade de recursos humanos, tempo hábil de execução e disponibilidade orçamentaria.

Situação encontrada

A questão não foi abordada na vistoria, considerando que se trata de um apontamento de cunho procedimental que não afeta o ambiente físico do DC.

Análise e conclusão

Considerando os esclarecimentos apresentados, conclui-se que a SME tem adotado providências para a mitigação dos riscos e a opção da não adoção do *Site Backup* faz parte do contexto do plano de contingências da SME.

3.8. 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 (apontamento 4.8)

Manifestação da SME (peça 7)

A manifestação da SME (peça 7) não apresentou esclarecimento sobre as ações pertinentes à elaboração de uma Política de Segurança da Informação (PSI) ou justificativas para a sua não realização.

Resposta da SME à requisição de informações (peça 12)

Conforme esclarecimento apresentado pela SME (peça 12, fl. 2), a SME não possui PSI devidamente redigida e publicada, mas que existem ações, aplicações, fluxos deliberados entre SME/COTIC, SME/GAB ou outras coordenadorias envolvidas, quais as equipes de gestão e operação tomam como padrão no cotidiano da operação de TIC, porém que não possuem publicação ou o mesmo peso de uma normativa de PSI na instituição.

Situação encontrada

A questão não foi abordada na vistoria, considerando que se trata de um apontamento de cunho procedimental que não afeta o ambiente físico do DC.

Análise e conclusão

Considerando os esclarecimentos apresentados, conclui-se que a SME ainda necessita aprimorar seus procedimentos, elaborando e adotando uma Política de Segurança da Informação.

3.9. 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 (apontamento 4.9)

Manifestação da SME (peça 7)

A manifestação da SME (peça 7) não apresentou esclarecimento sobre as ações pertinentes à elaboração de uma Política de Controle de Acesso ou justificativas para a sua não realização.

Resposta da SME à requisição de informações (peça 11)

Conforme esclarecimento apresentado pela SME (peça 11, fl. 7), a SME esclareceu que ainda não contam com uma política completa publicada da forma acesso ao DC, ressalvando que o Plano de Gerenciamento de Capacidade (peça 11, fls. 251/288) identificou o processo como necessário para uma efetiva gestão do nosso ambiente tecnológico, esclarecendo que o acesso físico ao nosso DC é permitido apenas à equipe de redes de Cotic, equipe terceirizada de manutenção da Sala Cofre (empresa GLS), e a supervisores e técnicos atuantes no nível 3 de atendimento a chamados (empresa Central IT), e que o acesso e permanência de visitantes e técnicos é validado pessoalmente pela equipe de infraestrutura, sendo permitida a permanência de outros técnicos, apenas com o acompanhamento de um servidor da equipe de redes da Cotic ou ainda com o acompanhamento de técnico ou supervisor de N3 da Central IT.

Acrescenta que a execução de serviços de terceiros no local deve ser previamente validada pela equipe de Cotic, sendo solicitado aos técnicos ao término do serviço, documento comprovando as ações e interferências que foram realizadas no ambiente e que em casos de saída dos colaboradores das empresas atuantes ou de SME, os acessos devem ser removidos, e que o ambiente do DC possui três leitores biométricos que operam de forma independente, sendo respectivamente, Sala Cofre, Sala UPS e Sala de Monitoramento NOC.

Apresenta documento (peça 11, fls. 14/17) que trata dos procedimentos técnicos necessários para a realização de cadastro/permissionamento de um novo técnico ou membro da equipe gestora do ambiente aos acessos biométricos que compõem o ambiente de *Data Center* de SME.

Situação encontrada

Na vistoria constatou-se que o procedimento adotado para visitantes ocorre em conformidade com os esclarecimentos apresentados. O procedimento pode ser aprimorado, com o registro no livro de visitas das pessoas que acessaram o ambiente seguro do DC.

Análise e conclusão

Considerando os esclarecimentos apresentados e as constatações da vistoria *in loco*, conclui-se que a SME tem adotado providências para a solução do problema apontado, mas ainda dispõe de pontos a serem aprimorados.

3.10. 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 (apontamento 4.10)

Manifestação da SME (peça 7)

A manifestação da SME (peça 7) não apresentou esclarecimento sobre as ações pertinentes à elaboração de uma Política de Controle de Acesso ou justificativas para a sua não realização.

Resposta da SME à requisição de informações (peça 11)

O esclarecimento apresentado pela SME (peça 11, fl. 7) consta do item 3.9.

Situação encontrada

Na vistoria constatou-se que o procedimento adotado para registro no livro de visitas dos visitantes ocorre em conformidade com os esclarecimentos apresentados, mas com práticas que podem ser aprimoradas buscando maior alinhamento às recomendações da norma ABNT ISO/IEC 27.002:2013.

Análise e conclusão

Na vistoria constatou-se que o procedimento adotado para registro dos visitantes ocorre em conformidade com os esclarecimentos apresentados, mas com práticas que podem ser aprimoradas.

3.11. 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 (apontamento 4.11)

Manifestação da SME (peça 7)

Conforme constou do item (ii) da manifestação (peça 7, fl. 6), a SME ressalta que apesar do ambiente tecnológico da SME contar com *backup* local, o processo de recuperação de dados em caso de eventual desastre ou grave impacto dos recursos contidos no DC seria mais complexo, que poderiam inviabilizar a recuperação de dados.

Argumenta que para a garantia da segurança de dados, além do *backup* local seria fundamental que os arquivos armazenados dentro do DC fossem replicados e armazenado em outros ambientes externos, a partir do qual os dados podem ser recuperados no caso de uma infraestrutura danificada ou problema de serviço, que seria procedente que o armazenamento desses arquivos em ambiente de nuvem, diminuindo o risco de instabilidade nos sistemas e evitando a paralisação de serviços essenciais para as rotinas administrativas e pedagógicas.

Diante dos fatos, informa que a SME estaria contratando a Cia de Processamento de Dados do Estado de São Paulo (Prodesp), por dispensa de licitação, para prestação de serviços de *backup* e *restore* em nuvem pública, por meio do processo SEI nº 6016.2021/0113748-9, conforme publicação no Diário Oficial da Cidade de São Paulo (DOC), de 30.12.21, pág. 133.

Entretanto, a manifestação da SME (peça 7) não apresentou esclarecimento sobre as ações pertinentes à elaboração de uma Política de Cópias de Segurança ou *Backup* ou justificativas para a sua não realização.

Resposta da SME à requisição de informações (peça 11)

Conforme esclarecimento apresentado pela SME (peça 11, fl. 8), as rotinas de *backup* executadas nos servidores seriam conforme as rotinas divididas em: DRE's; Incremental Diário;

Full Mensal 1ª Semana; *Full* Mensal 2ª Semana; *Full* Mensal 3ª Semana; *Full* Mensal 4ª Semana; *Custom Backup*; *Full* Semanal (peça 11, fls. 18/43).

As rotinas dos servidores descentralizados (Diretorias Regionais) e as rotinas de *backup* dos demais equipamentos são segmentados por periodicidade e *hosts*, de acordo com periodicidades por tipo. Esclarece que os equipamentos de SME responsáveis pelo *backup*, bem como os servidores de armazenamento de arquivos, estão em seus limites e vida útil ou capacidade, de forma que se faz necessário garantir a contratação em andamento de equipamentos para garantir a disponibilidade dos recursos desta secretaria.

Apresenta documentos que especificam os procedimentos básicos para iniciar as ações de *backup* (peça 11, fls. 293/297) e restauração dos servidores (peça 11, fls. 298/299), abrangendo desde o acesso as máquinas até os comandos necessários utilizando a ferramenta atual de *backup* de SME.

Situação encontrada

A questão não foi abordada na vistoria, considerando que se trata de um apontamento de cunho procedimental que não afeta o ambiente físico do DC.

Análise e conclusão

Considerando os esclarecimentos apresentados, conclui-se que a SME tem adotado providências para a solução do problema apontado.

Ressalva-se, entretanto, que os parâmetros adotados nos procedimentos relacionados às cópias de segurança de dados e sistemas devem estar ancorados nas reais necessidades da unidade, estruturadas de forma ordenada e consolidada na forma de um documento de Política de Cópias de Segurança ou *Backup*, componente da Política de Segurança da Informação da unidade. O item 8.13 da norma NBR ISO 27002/2022 (ou item 12.3.1 da NBR ISO 27002/2013) ilustra os pontos a serem considerados na parametrização da política de *backup*.

Assim, sugere-se recomendar à unidade a elaboração de uma Política de Cópias de Segurança ou *Backup*, considerando as práticas sugeridas na norma NBR ISO 27002/2022, especialmente as disposições de seu item 8.13.

3.12. 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 a 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 (apontamento 4.12)

Manifestação da SME (peça 7)

A manifestação da SME (peça 7) não apresentou esclarecimento sobre as ações pertinentes à realização de estudos para determinação dos períodos de retenção dos *backups* implementada e a solução quanto ao armazenamento das mídias ou justificativas para a sua não realização.

Resposta da SME à requisição de informações (peça 12)

Conforme esclarecimento apresentado pela SME (peça 12, fl. 2), o período de retenção atual é determinado relacionando o tamanho da capacidade dos discos que fazem parte do conjunto da ferramenta de *backup* para suportar o volume de dados diários utilizados e uma estimativa de tempo qual se considera ser segura para o armazenamento dos dados e necessidade de recuperação. Os *backups* adotados pela SME atuam com retenção: Completo Mensal 60 dias, Completo Bimestral 90 dias, Completo Trimestral 120 dias, Incremental (Seg a Sex) 14 dias, de forma que seria possível cobrir boa parte das possíveis catástrofes ao ambiente.

Situação encontrada

A questão não foi abordada na vistoria, considerando que se trata de um apontamento de cunho procedimental que não afeta o ambiente físico do DC.

Análise e conclusão

Considerando os esclarecimentos apresentados, conclui-se que a SME tem adotado providências para a solução do problema apontado. Entretanto, ressalva-se que os parâmetros adotados de frequência, períodos de retenção dos *backups*, o armazenamento etc. devem estar ancorados nas reais necessidades da unidade, e não nas “limitações” de sua infraestrutura. O item 8.13 da norma NBR ISO 27002/2022 (ou item 12.3.1 da NBR ISO 27002/2013) ilustra os pontos a serem considerados na parametrização da política de *backup*.

Assim, sugere-se recomendar à unidade a adoção das orientações sugeridas no item 8.13 da norma NBR ISO 27002/2022, especialmente quanto ao período de retenção de informações essenciais do negócio, para que seja determinado levando em conta qualquer exigência de retenção de cópias de arquivo, documentando os parâmetros utilizados.

3.13. 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 (apontamento 4.13)

Manifestação da SME (peça 7)

A manifestação da SME (peça 7) não apresentou esclarecimento sobre as ações pertinentes à formalização de procedimento para realização de testes de integridade e recuperação no processo de *backup* ou justificativas para a sua não realização.

Resposta da SME à requisição de informações (peça 11)

O esclarecimento apresentado pela SME (peça 11, fl. 8) dispõe os documentos que especificam os procedimentos básicos para iniciar as ações de *backup* (peça 11, fls. 293/297) e restauração dos servidores (peça 11, fls. 298/299), abrangendo desde o acesso às máquinas até os comandos necessários utilizando a ferramenta atual de *backup* de SME.

A documentação com as evidências da efetiva realização do processo de *backup*, incluindo testes de restauração, foi apresentada (peça 11, fls. 44/250), extraída da ferramenta de *backup* após operações do dia a dia, como peça de evidência da execução da rotina de *backup*.

Acrescenta que está prevista a renovação da estrutura de *backup*, que devido à idade da solução atual e ausência de garantia dos recursos atuais, estava em andamento nova aquisição (SEI nº 6016.2022/0111790-0).

Situação encontrada

A questão não foi abordada na vistoria, considerando que se trata de um apontamento de cunho procedimental que não afeta o ambiente físico do DC.

Análise e conclusão

Considerando os esclarecimentos apresentados, conclui-se que a SME tem adotado providências para a solução do problema apontado.

3.14. 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 (apontamento 4.14)

Manifestação da SME (peça 7)

A manifestação da SME (peça 7) não apresentou esclarecimento sobre as ações pertinentes à formalização de procedimento para controle da vida útil e do descarte das mídias utilizadas no processo de *backup* ou justificativas para a sua não realização.

Resposta da SME à requisição de informações (peça 11)

A questão não foi abordada na manifestação.

Situação encontrada

A questão não foi abordada na vistoria, considerando que se trata de um apontamento de cunho procedimental que não afeta o ambiente físico do DC.

Análise e conclusão

A ausência de manifestações sugere que a SME não dispensa a devida atenção ao tratamento das mídias utilizadas no armazenamento dos dados da Unidade. O item 7.10 da norma NBR

ISO 27002/2022 (ou itens 8.3.1, 8.3.2, 8.3.3, 11.2.5 da NBR ISO 27002/2013) ilustram os pontos a serem considerados na parametrização da política de mídias de armazenamento.

Assim, sugere-se recomendar à unidade a consideração em sua Política de Cópias de Segurança ou *Backup*, das práticas sugeridas no item 7.10 da norma NBR ISO 27002/2022, no especificando os parâmetros de utilização e tratamento das mídias de armazenamento de dados utilizados pela unidade.

3.15. 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 (apontamento 4.15)

Manifestação da SME (peça 7)

Conforme constou do item (iv) da manifestação da SME (peça 7, fl. 7), foi informado que “Diante das inúmeras demandas dessa Coordenadoria, informamos que estamos pleiteando junto ao gabinete atendimento a essa recomendação”.

Resposta da SME à requisição de informações (peça 11)

Conforme esclarecimento apresentado pela SME (peça 11, fl. 9), a SME/COTIC é composta por 31 servidores distribuídos em divisões técnicas, porém ainda há carência de profissionais formados ou especialistas em TI, ressaltando que a coordenadoria deveria iniciar com uma reestruturação formal de suas divisões, de forma que adequar sua estrutura. Esclarece que houve alguns levantamentos realizados pela Fundação Getúlio Vargas, e pela Secretaria Municipal de Gestão, onde foram expostos diversos pontos, sob a expectativa de viabilidade de reestruturação e possível ampliação do quadro, porém nenhuma das consultas gerou resultados e que não há ações factuais em andamento para prover a ampliação do quadro de técnicos da unidade.

Situação encontrada

A questão não foi abordada na vistoria, considerando que se trata de um apontamento de cunho procedimental que não afeta o ambiente físico do DC.

Análise e conclusão

Considerando os esclarecimentos apresentados, conclui-se que a SME não adotou providências em relação ao apontamento.

Sugere-se recomendar à unidade, a atualização formal da estrutura da unidade de forma a prover capacidade de manutenção e desenvolvimento das atividades relacionadas à estrutura de TI da unidade, considerando ainda a necessidade de adequação do corpo técnico para fazer frente aos desafios impostos à área.

4. CONCLUSÃO

À vista das análises efetuadas para acompanhamento da implementação das correções propostas por SME para as inconformidades destacadas no Relatório da Auditoria Extraplano (peça 5 – cópia da peça 24 do TC nº 002933/2019), conclui-se a SME tem adotado providências para a solução dos problemas apontados (apontamentos 3.1, 3.2, 3.3, 3.4, 3.5, 3.6, 3.7, 3.8, 3.9, 3.10 e 3.13), ressalvando a necessidade de aprimoramento de alguns procedimentos às boas práticas do mercado, materializados pelas orientações da norma NBR ISO 27002/2022 (apontamentos 3.11, 3.12 e 3.14), além da necessidade e adequação da estrutura da unidade responsável pela infraestrutura de TI e seu corpo técnico (apontamento 3.15).

5. ANÁLISE DOS ELEMENTOS DE RESPONSABILIZAÇÃO

Considerando-se que os referidos achados não representam irregularidades, não há que se falar em análise dos elementos de responsabilização no presente caso. A proposta de encaminhamento relativo aos achados consta do item 6 deste relatório, para promoção de ajustes e melhorias nas situações encontradas.

6. PROPOSTAS DE ENCAMINHAMENTOS

À vista das análises efetuadas para acompanhamento da implementação das correções propostas por SME, ressalva-se a necessidade de aprimoramento de alguns procedimentos às boas práticas do mercado, materializados pelas orientações da norma NBR ISO 27002/2022 (apontamentos 3.11, 3.12 e 3.14), além da necessidade e adequação da estrutura da unidade responsável pela infraestrutura de TI e seu corpo técnico (apontamento 3.15).

6.1. Propostas de Recomendação

Nestes termos, sugere-se recomendar à unidade que:

- Elabore uma Política de Cópias de Segurança ou *Backup*, considerando as práticas sugeridas na norma NBR ISO 27002/2022, especialmente as disposições de seu item 8.13 (apontamento 3.11);

- Adote as orientações sugeridas no item 8.13 da norma NBR ISO 27002/2022, especialmente quanto ao período de retenção de informações essenciais do negócio, para que seja determinado levando em conta qualquer exigência de retenção de cópias de arquivo, documentando os parâmetros utilizados (apontamento 3.12);

- Considere em sua Política de Cópias de Segurança ou *Backup*, as práticas sugeridas no item 7.10 da norma NBR ISO 27002/2022, especificando os parâmetros de utilização e tratamento das mídias de armazenamento de dados utilizados pela unidade (apontamento 3.14);

- Atualize formalmente a estrutura da unidade de forma a prover capacidade de manutenção e desenvolvimento das atividades relacionadas à estrutura de TI da unidade, considerando ainda a necessidade de adequação do corpo técnico para fazer frente aos desafios impostos à área (apontamento 3.15).

Em 25.11.23

MAURICIO KAZUHIRO SATO
Auditor de Controle Externo

ADRIANO GONÇALVES ZAMBON
Supervisor de Controle Externo 18

De acordo.

HELIO RICARDO GUIMARÃES MURCI DE AZEVEDO
Coordenador de Controle Externo - VIII