RELATÓRIO DE AUDITORIA DE CONFORMIDADE

Ordem de Serviço	eTCM	Período de abrangência	Período da realização
2023/01730	006545/2023	07.06.23 a 13.07.23	02.06.23 a 17.08.23

Área Auditada

Secretaria Municipal da Saúde (SMS)

Objeto de auditoria

Infraestrutura de TI

Objetivo da auditoria

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

Equipe técnica

Carlos Albuquerque Lemos	20.289
Maurício Kazuhiro Sato	20.117
Renato Sambra Suyama	20.112

LISTA DE SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
BIA	*Business Impact Analysis*
BTU	*British Thermal Unit*
CFTV	Circuito Fechado de Televisão
CMTIC	Conselho Municipal de Tecnologia da Informação e Comunicação
DC	*Data Center*
DTIC	Departamento de Tecnologia da Informação e Comunicação
FTTIC	Fórum Técnico de Tecnologia da Informação e Comunicação
Intosai	*International Organization of Supreme Audit Institutions*
ISO	*International Organization for Standardization*
ISSAI	International Standards of Supreme Audit Institutions
NBASP	Normas Brasileiras de Auditoria do Setor Público
NBR	Normas Brasileiras
PAF	Plano Anual de Fiscalização
PCN	Política de Continuidade do Negócio
PGM	Plano de Gestão de Mudanças
Prodam	Empresa de Tecnologia da Informação e Comunicação do Município
PSAF	Política de Segurança de Acesso Físico
PSI	Política de Segurança da Informação
RASS	Registro de Acessos a Sala Segura
RPO	*Recovery Point Objective*
RTO	*Recovery Time Objective*
SMIT	Secretaria Municipal de Inovação e Tecnologia
SMS	Secretaria Municipal da Saúde
SMTIC	Sistema Municipal de Tecnologia da Informação e Comunicação
SUS	Sistema Único de Saúde
TCMSP	Tribunal de Contas do Município de São Paulo
TI	Tecnologia da Informação
TIC	Tecnologia da Informação e Comunicação
UPS	*Uninterruptible Power Supply*

RESUMO

Trata o presente de auditoria realizada entre 02.06.23 e 17.08.23, com o objetivo de avaliar se o *Data Center* da SMS atende às normas técnicas e às boas práticas de segurança da informação. O trabalho foi previsto no Plano Anual de Fiscalização (PAF) para o exercício de 2023, aprovado pela Resolução nº 32/2022.

A fim de garantir a disponibilização e a segurança das informações, é necessário que o *Data Center* seja provido de uma infraestrutura e processos que permitam aos usuários dos sistemas o acesso de forma adequada, resistente a falhas de *hardware*, *software* e serviços de infraestrutura (energia, comunicações etc.) cujo objetivo é manter os serviços disponibilizados o máximo de tempo possível.

Considerando que em trabalhos anteriores realizados na entidade foi constatado que o *Data Center* da SMS não havia sido submetido a avaliações feitas por entidades certificadoras, optou-se por avaliar o alinhamento do ambiente computacional às orientações da NBR ISO 27002/22 para comprovar se o ambiente do *Data Center* possui características de segurança, resiliência ou sustentabilidade nas operações de TI, isto é, se o *Data Center* da SMS atende às normas técnicas e às boas práticas de segurança da informação.

Considerando os preceitos da NBR ISO 27002/22, o escopo do trabalho abrange controles organizacionais, físicos e tecnológicos possíveis de serem aplicados ao ambiente do *Data Center* da SMS.

Como critério de avaliação da segurança da informação, foram adotados os preceitos recomendados pela NBR ISO 27002/22, que tem como objetivo principalmente fornecer as diretrizes necessárias para programar a segurança da informação nas empresas, visando também mantê-la e melhorá-la ao longo do tempo.

Os procedimentos utilizados para a coleta e análise de dados no presente trabalho baseou-se na coleta de evidências para a avaliação do atendimento de controles especificados na NBR ISO 27002/22, selecionados de acordo com o estudo preliminar realizado sobre os normativos que foram considerados mais aderentes com o entendimento da realidade do ambiente do DC da entidade.

As técnicas e procedimentos utilizados para a coleta e análise de dados permitiram chegar aos seguintes achados de auditoria:

(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 (PSI);

(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;

(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;

(4) Não há procedimento formal para a Política de Continuidade do Negócio e da Segurança da Informação do ambiente do DC;

(5) A ausência de recursos redundantes na infraestrutura do DC da SMS não atende aos padrões necessários de segurança;

(6) Não há procedimento formal para a gestão de capacidade do ambiente do DC;

(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.

Consigna-se que a leitura da íntegra do relatório é recomendável para a compreensão do processo lógico da execução da análise que resultou em cada achado.

O encaminhamento proposto consta do item 7 deste relatório de auditoria.

SUMÁRIO

1. INTRODUÇÃO

Trata o presente de 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* (DC), atende às normas técnicas e às boas práticas de segurança da informação.

O trabalho foi previsto no Plano Anual de Fiscalização (PAF) para o exercício de 2023, aprovado pela Resolução nº 32/2022.

1.1. Destinatário(s) da auditoria

Os seguintes grupos, sem prejuízo de outros, têm especial interesse na obtenção de informações sobre a presente auditoria: Tribunal Pleno do Tribunal de Contas do Município de São Paulo (TCMSP), Câmara de Vereadores do Município de São Paulo, Secretaria Municipal da Saúde (SMS), o Sistema Municipal de Tecnologia da Informação e Comunicação (SMTIC)[1] e eventualmente os usuários do Sistema Único de Saúde (SUS) no município de São Paulo.

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

O objeto do presente trabalho é a infraestrutura de TI da SMS, com o objetivo de avaliar se o *Data Center* da SMS atende às normas técnicas e às boas práticas de segurança da informação.

Denomina-se como *Data Center* um ambiente tecnológico protegido, sala ou edifício, projetado para concentrar os equipamentos dedicados ao processamento e armazenamento de dados, incluindo os equipamentos de infraestrutura e suporte a redes, ativos de telecomunicações e outros. A infraestrutura do *Data Center* tem por objetivo hospedar os equipamentos de processamento e armazenamento de dados, no intuito de preservar os requisitos de segurança

[1] Decreto nº 57.65/17
Art. 5º Integram o Sistema Municipal de Tecnologia da Informação e Comunicação:
I - Conselho Municipal de Tecnologia da Informação e Comunicação – CMTIC [...];
II - Órgão Central: Secretaria Municipal de Inovação e Tecnologia – SMIT [...];
III - Órgãos e Entidades Setoriais [...];
IV - Fórum Técnico de Tecnologia da Informação e Comunicação – FTTIC [...];
V - Integrador Estratégico de soluções de tecnologia da informação e comunicação [...] PRODAM.

necessários para garantir a eficiência e a disponibilidade dos equipamentos e sistemas suportados pela infraestrutura.

A fim de garantir a disponibilização e segurança das informações, é necessário que o *Data Center* seja provido de uma infraestrutura e processos que permitam aos usuários dos sistemas o acesso de forma adequada, resistente a falhas de *hardware*, *software* e serviços de infraestrutura (energia, comunicações etc.), cujo objetivo é manter os serviços disponibilizados o máximo de tempo possível.

Considerando que em trabalhos anteriores realizados na entidade foi constatado que o *Data Center* da SMS não havia sido submetido a avaliações feitas por entidades certificadoras, optou-se por avaliar o alinhamento do ambiente computacional às orientações da NBR ISO 27002/22 para comprovar se o ambiente do *Data Center* possui características de segurança, resiliência ou sustentabilidade nas operações de TI, isto é, se o *Data Center* da SMS atende às normas técnicas e às boas práticas de segurança da informação.

Considerando os preceitos da NBR ISO 27002/22 possíveis de serem aplicados ao ambiente do *Data Center* da SMS, o escopo do trabalho abrange controles organizacionais, físicos e tecnológicos relacionados na NBR ISO 27002/22 concernentes ao ambiente do *Data Center* da SMS.

1.3. Normas de auditoria aplicadas na realização do trabalho

A auditoria, do tipo relatório direto, foi conduzida em conformidade com o Manual de Auditoria Governamental do TCMSP, que é consistente com as Normas Brasileiras de Auditoria do Setor Público (NBASP), desenvolvidas com base nos Princípios Fundamentais de Auditoria (ISSAI 100-199) integrante da Estrutura de Pronunciamentos Profissionais da *International Organization of Supreme Audit Institutions* (Intosai).

2. METODOLOGIA

2.1. Critérios adotados

Como critério de avaliação da segurança da informação, foram adotados os preceitos recomendados pela NBR ISO 27002/22, que tem como objetivo principalmente fornecer as

diretrizes necessárias para programar a segurança da informação nas empresas, visando também mantê-la e melhorá-la ao longo do tempo. Ela apresenta uma série de controles e objetivos de controle para segurança dos ativos de processamento de informações, recursos humanos, ambientes e contratos de maneira que promovam a segurança das informações.

2.2. Métodos de coleta e de análise dos dados

Os procedimentos utilizados para a coleta e análise de dados no presente trabalho foram descritos na matriz de planejamento C8/002/23, e baseou-se na coleta de evidências para a avaliação do atendimento de controles especificados na NBR ISO 27002/22, selecionados de acordo com o estudo preliminar realizado sobre os normativos que foram considerados mais aderentes ao entendimento da realidade do ambiente do DC da entidade.

Como técnica de coleta de dados, foram utilizados a indagação escrita, entrevista, exame documental, inspeção física e observação direta.

2.3. Limitações do trabalho de auditoria

Quanto às limitações para o trabalho, ressalta-se que a infraestrutura atual do *Data Center* está virtualmente em processo de descontinuidade em razão da mudança da sede da SMS e também do *Data Center*, o que restringe eventuais atualizações, aprimoramentos e quaisquer modificações na infraestrutura atual.

3. ACHADOS DE AUDITORIA

3.1. A infraestrutura e utilidades implantadas pela SMS estão alinhadas aos requisitos de segurança da informação para *Data Center* (DC)?

3.1.1. Achado

Não é possível assegurar que a infraestrutura e utilidades implantadas do DC da SMS estão alinhadas às premissas de sua Política de Segurança da Informação.

3.1.2. Situação encontrada

A inspeção física foi realizada com o acompanhamento de representantes da DTIC. A vistoria foi registrada por meio do relatório fotográfico, apêndice I do trabalho. Na inspeção física, foram verificadas as condições gerais da Sala Segura. Em relação às condições das dependências foi constatado:

- O controle de acesso à sala segura é realizado por meio de fechadura eletrônica, controlado por meio de senhas – fotos 1 a 3;

- Não havia extintor de incêndio no interior da sala segura. Havia um extintor localizado na parte externa da sala, ao lado da porta de entrada – foto 4;

- A temperatura do ambiente da sala segura é mantida por meio de dois aparelhos de ar-condicionado, do tipo *Split*, de 22 mil BTUs. Os evaporadores estão dispostos no interior da sala segura. Os condensadores foram instalados na parte externa da edificação. Na data da vistoria, os aparelhos estavam funcionando a uma temperatura de 21ºC – fotos 5 e 7;

- O ambiente interno da sala segura é monitorado por meio de uma câmera de CFTV, posicionada na entrada da sala – foto 6;

- Um equipamento *No Break* no interior da sala segura – foto 8 e 10;

- A sala segura possui uma janela para o exterior do edifício – foto 9;

- A sala segura não possui piso falso para passagem dos cabos – fotos 12, 14/16;

- A organização dos cabos lógicos e de energia elétrica não está de acordo com a norma ABNT NBR 14565 – fotos 11/17;

- A sala possui conduítes para passagem de cabos de/para área externa da sala segura – fotos 15/16;

- Armários no interior da sala (com materiais não relacionados diretamente com a sala segura) – foto 18;

- Cinco *racks* com equipamentos estão instalados no interior da sala segura – fotos 19 a 26;

- Não havia equipamentos de detecção, prevenção ou combate a incêndio no interior da sala.

A fim de subsidiar o exame documental para avaliar a aderência à NBR ISO 27002/22 das premissas adotadas nos normativos e adequação da infraestrutura e utilidades implantadas do DC da SMS aos requisitos de Segurança da Informação, foi feita requisição de documentos e informações direcionada à DTIC, conforme reproduzido (peça 5, fls. 1/2):

> 1. Relação dos equipamentos que compõem o *data center* e croqui simplificado da instalação constando os equipamentos e anexos da instalação (sala de comunicação, suporte etc.)
>
> R: Informação contida no documento Documentação *Datacenter*
>
> 2. Relação dos sistemas e aplicações hospedados, descrevendo o objetivo, se o sistema atende somente a SMS ou se está disponível na internet, disponibilidade (24x7);
>
> R: Informação contida no documento Documentação *Datacenter*
>
> 3. Relação dos contratos de manutenção relacionados com o *data center* (equipamentos e sistemas de infraestrutura, como proteção contra incêndio, refrigeração, UPS etc.), com detalhamento do objeto, prazos e finalidade (incluindo se principal, redundância etc.);
>
> R: Informação contida no documento Relação de Contratos – *Data Center*.
>
> 5. Relação dos ativos de segurança (equipamentos para controle de acesso, câmeras de monitoramento, sistema de refrigeração, sistema de extinção de incêndio, etc.) e demais utilidades instaladas (suprimento de energia, entre outros, assim como suas respectivas contingências) e suas características técnicas;
>
> R: Informação contida no documento Relação de Ativos de Segurança.
>
> 6. Documentos comprobatórios das Certificações de Segurança do ambiente do *data center* (se houver);
>
> R: Estamos em processo de estudo técnico preliminar para contratação de uma empresa de certificação.
>
> 7. Documento da Política de Controle de Acesso Físico ao *data center*;
>
> R: Informação contida nos documentos Política de Segurança de Acesso Físico e no Registro de Acesso a Sala Segura.
>
> 8. Documentações/relatórios com os registros de acesso (entradas e saídas identificadas) realizados ao *data center* no período de mai/23;
>
> R: A fechadura utilizada na sala segura não suporta o registro de histórico de acesso

Em resposta a esta requisição, a SMS encaminhou os seguintes documentos, que compõem a documentação da auditoria:

i. “Documentação *Datacenter*.pdf”

ii. “RELAÇÃO DE CONTRATOS - DATA CENTER.pdf”

iii. “Relação de Ativos de Segurança.pdf”

Uma segunda requisição de documentos e informações foi direcionada à DTIC, cuja resposta segue reproduzida (peça 5, fl. 1):

> 1. Documento Política de Segurança da Informação da SMS;
> Documento em anexo.

Em resposta a esta requisição, a SMS encaminhou o seguinte documento, que compõe a documentação da auditoria:

i. “PSID_001 - Política de Segurança da Informação.pdf”

O documento Documentação *Datacenter* apresenta um croqui com a identificação da disposição dos equipamentos instalados nos *racks* que compõem o DC e o detalhamento dos componentes e sistemas instalados.

O documento RELAÇÃO DE CONTRATOS - DATA CENTER apresenta os contratos relacionados com o ambiente do DC, divididos em contratos de manutenção e contratos de aquisição.

O documento Relação de Ativos de Segurança divididos em 1) Controle de acesso; 2) Câmeras de monitoramento; 3) Sistema de refrigeração e 4) Sistema de energia.

O documento PSID_001 - Política de Segurança da Informação apresenta diretrizes de controles internos, as normas, padrões que tratam da proteção da informação no âmbito da SMS, abrangendo deveres e responsabilidades, gestão da informação, recomendações de segurança, gestão da segurança cibernética e resposta a incidentes de segurança da informação.

3.1.3. Critério

O critério utilizado para avaliar a aderência da infraestrutura e utilidades implantadas pela SMS no ambiente do DC aos requisitos de Segurança da Informação foi baseado nos controles descritos na NBR ISO 27002/22. Nesse quesito, foram avaliados os Controles organizacionais (5.1 - Políticas de segurança da informação) e Controles físicos (7.10 - Mídia de armazenamento; 7.11 - Serviços de infraestrutura; 7.12 - Segurança do cabeamento; 7.13 - Manutenção de equipamentos; 7.14 - Descarte seguro ou reutilização de equipamentos).

O item 5.1 - Políticas de segurança da informação da NBR ISO 27002/22 recomenda que política de segurança da informação e as políticas específicas por tema sejam definidas, aprovadas pela direção, publicadas, comunicadas e reconhecidas pelo pessoal pertinente e partes interessadas pertinentes, e analisadas criticamente em intervalos planejados e se ocorrer mudanças significativas, com o propósito de assegurar a adequação contínua, suficiência, efetividade da direção de gestão e suporte à segurança da informação de acordo com os requisitos comerciais, legais, estatutários, regulamentares e contratuais.

O item 7.10 - Mídia de armazenamento da NBR ISO 27002/22 recomenda que as mídias de armazenamento sejam gerenciadas por seu ciclo de vida de aquisição, uso, transporte e descarte, de acordo com o esquema de classificação e com os requisitos de manuseio da organização, com o propósito de assegurar a divulgação, modificação, remoção ou destruição de informações das mídias de armazenamento apenas de forma autorizada.

O item 7.11 - Serviços de infraestrutura da NBR ISO 27002/22 recomenda que as instalações de tratamento de informações sejam protegidas contra falhas de energia e outras disrupções causadas por falhas nos serviços de infraestrutura, com o propósito de evitar perdas, danos ou comprometimento de informações e outros ativos associados, ou a interrupção das operações da organização devido à falha e disrupção nos serviços de infraestrutura.

O item 7.12 - Segurança do cabeamento da NBR ISO 27002/22 recomenda que os cabos que transportam energia ou dados ou que sustentam serviços de informação sejam protegidos contra interceptação, interferência ou danos, com o propósito de evitar perdas, danos, roubo ou comprometimento de informações e outros ativos associados à interrupção das operações da organização relacionadas ao cabeamento de energia e de comunicação.

O item 7.13 - Manutenção de equipamentos da NBR ISO 27002/22 recomenda que os equipamentos sejam mantidos corretamente para assegurar a disponibilidade, integridade e confidencialidade da informação, com o propósito de evitar perdas, danos, roubos ou comprometimento de informações e outros ativos associados e interrupção das operações da organização causada pela falta de manutenção.

O item 7.14 - Descarte seguro ou reutilização de equipamentos da NBR ISO 27002/22 recomenda que sejam verificados os itens dos equipamentos que contenham mídia de

armazenamento, para assegurar que quaisquer dados confidenciais e *software* licenciado tenham sido removidos ou substituídos com segurança antes do descarte ou reutilização, com o propósito de evitar o vazamento de informações por equipamento que seja descartado ou reutilizado.

3.1.4. Evidências

As constatações da vistoria *in loco* e a documentação apresentada pela SMS foram avaliadas, buscando identificar a aderência da infraestrutura e dos termos dos documentos analisados com as orientações dos itens 5.1 - Políticas de segurança da informação; 7.10 - Mídia de armazenamento; 7.11 - Serviços de infraestrutura; 7.12 - Segurança do cabeamento; 7.13 - Manutenção de equipamentos e 7.14 - Descarte seguro ou reutilização de equipamentos da NBR ISO 27002/22, atendendo o propósito de Segurança da Informação do DC.

3.1.4.1. Políticas de segurança da informação (item 5.1 da NBR ISO 27002/22)

Os procedimentos avaliados não atendem às orientações do item 5.1 - Políticas de segurança da informação da NBR ISO 27002/22, que orienta que a política de segurança da informação e as políticas específicas por tema sejam definidas, aprovadas pela direção, publicadas, comunicadas e reconhecidas pelo pessoal pertinente e partes interessadas pertinentes, e analisadas criticamente em intervalos planejados e se ocorrer mudanças significativas e, portanto, não garantem o propósito de assegurar a adequação contínua, suficiência, efetividade da direção de gestão e suporte à segurança da informação de acordo com os requisitos comerciais, legais, estatutários, regulamentares e contratuais:

i. O item 3 da PSI não explicita a estratégia e requisitos de negócios considerados na PSI ou indicação de quais seriam os “documentos correlatos” considerados;

ii. A PSI não declara ou explicita outras regulamentações, legislação e contratos considerados na PSI, além da referência do item 3;

iii. A PSI não declara ou faz referência aos riscos e ameaças atuais e projetados considerados na PSI.

iv. O documento não declara o tratamento de isenções e exceções.

v. O documento não declara ou faz referência a avaliação de oportunidades de melhoria da política de segurança da informação da organização e das políticas específicas por tema e a gestão da segurança da informação em resposta às mudanças.

vi. O documento não declara ou faz referência à análise crítica da política de segurança da informação e das políticas específicas.

3.1.4.2. Mídia de armazenamento (item 7.10 da NBR ISO 27002/22)

Os procedimentos avaliados não atendem às orientações do item 7.10 - Mídia de armazenamento da NBR ISO 27002/22, que orienta que as mídias de armazenamento sejam gerenciadas por seu ciclo de vida de aquisição, uso, transporte e descarte, de acordo com o esquema de classificação e com os requisitos de manuseio da organização e, portanto, não garantem o propósito de assegurar a divulgação, modificação, remoção ou destruição de informações apenas de forma autorizada sobre as mídias de armazenamento.

i. A PSI não faz referência a mídias de armazenamento removível.

ii. O documento não faz referência a reutilização ou descarte de mídia de armazenamento.

3.1.4.3. Serviços de infraestrutura (item 7.11 da NBR ISO 27002/22)

Os procedimentos avaliados não atendem às orientações do item 7.11 - Serviços de infraestrutura da NBR ISO 27002/22, que orienta que as instalações de tratamento de informações sejam protegidas contra falhas de energia e outras disrupções causadas por falhas nos serviços de infraestrutura e, portanto, não garantem o propósito de evitar perdas, danos ou comprometimento de informações e outros ativos associados, ou a interrupção das operações da organização devido à falha e disrupção nos serviços de infraestrutura.

i. A PSI não faz referência a serviços de infraestrutura.

ii. A PSI não faz referência a iluminação, comunicação ou procedimentos de emergência na sala segura.

3.1.4.4. Segurança do cabeamento (item 7.12 da NBR ISO 27002/22)

Os procedimentos avaliados não atendem às orientações do item 7.12 - Segurança do cabeamento da NBR ISO 27002/22, que orienta que os cabos que transportam energia ou dados ou que sustentam serviços de informação sejam protegidos contra interceptação, interferência ou danos e, portanto, não garantem o propósito de perdas, danos, roubo ou comprometimento de informações e outros ativos associados à interrupção das operações da organização relacionadas ao cabeamento de energia e de comunicação.

A PSI não faz referência à segurança do cabeamento. A sala segura do *Data Center* situa-se onde está alocada fisicamente a DTIC, não dispondo de isolamento e redundância de infraestrutura. O local não dispõe de piso falso para passagem de cabos e apresenta algumas deficiências na proteção e separação de cabeamento lógico e de energia.

3.1.4.5. Manutenção de equipamentos (item 7.13 da NBR ISO 27002/22)

Os procedimentos avaliados não atendem às orientações do item 7.13 - Manutenção de equipamentos, que orienta que os equipamentos sejam mantidos corretamente para assegurar a disponibilidade, integridade e confidencialidade da informação e, portanto, não garantem o propósito de evitar perdas, danos, roubos ou comprometimento de informações e outros ativos associados e interrupção das operações da organização causada pela falta de manutenção.

Não foi informado contrato de manutenção de equipamentos do DC. O contrato de manutenção do ar-condicionado não é específico para o ambiente seguro.

3.1.4.6. Descarte seguro ou reutilização de equipamentos (item 7.14 da NBR ISO 27002/22)

A PSI não prevê o atendimento das diretrizes do item 7.14 - Descarte seguro ou reutilização de equipamentos da NBR ISO 27002/22, que orienta que sejam verificados os itens dos equipamentos que contenham mídia de armazenamento, para assegurar que quaisquer dados confidenciais e *software* licenciado tenham sido removidos ou substituídos com segurança antes do descarte ou reutilização. O PSAF dispõe alguns procedimentos a descarte e reutilização de equipamentos. Ponderando as diversas premissas sugeridas no item 7.14 da NBR, considera-

se que os procedimentos avaliados não garantem o propósito de evitar o vazamento de informações por equipamento que seja descartado ou reutilizado.

i. A PSI não faz referência a descarte ou reutilização de equipamentos.

ii. A PSI não faz referência a procedimento a ser executado sobre mídias de armazenamento que contenham informações confidenciais ou com direitos autorais.

iii. A PSI e a PSAF não fazem referência a procedimentos de remoção de rótulos e marcas que identifiquem a organização ou indiquem a classificação, o proprietário, o sistema ou a rede em caso de descarte ou doação de equipamentos.

3.1.5. Causas

A Política de Segurança da Informação, controles físicos e o ambiente do DC da SMS não se mostram abrangentes o suficiente e carecem de procedimentos alinhados à realidade do DC da SMS.

3.1.6. Efeitos

Exposição a riscos possíveis de serem mitigados por meio de uma política de segurança da informação efetiva.

3.2. O controle do acesso físico e o monitoramento das dependências do DC foram implementados?

3.2.1. Achado

O processo de Segurança de Acesso Físico apresentado no documento Política de Segurança de Acesso Físico não é efetivo e não se mostra 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.

3.2.2. Situação encontrada

A inspeção física foi realizada com o acompanhamento de representantes da DTIC. A vistoria foi registrada por meio do relatório fotográfico, apêndice I do trabalho. Na inspeção física, foram verificadas as condições gerais da Sala Segura. Em relação ao controle do acesso físico e monitoramento das dependências foi constatado:

- O controle de acesso à sala segura é realizado por meio de fechadura eletrônica, controlado por meio de senhas – fotos 1 a 3;

- Não foi constatado extintor no interior da sala segura. Havia um extintor localizado na parte externa da sala, ao lado da porta de entrada – foto 4;

- A temperatura do ambiente da sala segura é mantida por meio de dois aparelhos de ar-condicionado, do tipo *Split*, de 22 mil BTUs. Os evaporadores estão dispostos no interior da sala segura. Os condensadores foram instalados na parte externa da edificação. Na data da vistoria os aparelhos estavam funcionando a uma temperatura de 21ºC – fotos 5 e 7;

- O ambiente interno da sala segura é monitorado por meio de uma câmera de CFTV, posicionada na entrada da sala – foto 6;

- A sala segura possui uma janela para o exterior do edifício – foto 9;

- Armários no interior da sala (com materiais não relacionados diretamente com DC) – foto 18;

- Cinco *racks* com equipamentos estão instalados no interior da sala segura – fotos 19 a 26;

- Não foi constatada a instalação de equipamentos de detecção, prevenção ou combate a incêndio no interior da sala.

A fim de subsidiar o exame documental para avaliar a aderência à NBR ISO 27002/22, das premissas adotadas nos normativos e controles realizados pela SMS no acesso físico e monitoramento do DC, foi feita requisição de documentos e informações direcionada à DTIC, conforme reproduzido (peça 5, fls. 1/2):

> 7. Documento da Política de Controle de Acesso Físico ao *data center*;

R: Informação contida nos documentos Política de Segurança de Acesso Físico e no Registro de Acesso a Sala Segura.

8. Documentações/relatórios com os registros de acesso (entradas e saídas identificadas) realizados ao *data center* no período de mai/23;

R: A fechadura utilizada na sala segura não suporta o registro de histórico de acesso

9. Documento da política de gestão das imagens registradas do ambiente de DC e evidência do armazenamento das imagens de monitoramento do *data center* no período de mai/23;

R: Informações contidas na Política de Segurança de Acesso Físico e na Evidência de Armazenamento de Imagens

Em resposta a esta requisição, a SMS encaminhou os seguintes documentos, que compõem a documentação da auditoria:

i. "Política de Segurança de Acesso Físico.pdf"

ii. "Registro de Acessos a Sala Segura.pdf"

iii. "Evidência do Armazenamento de Imagens.pdf"

A Política de Segurança de Acesso Físico reproduz as orientações da NBR ISO 27002/22 nos subitens dos itens 3 e 4 do documento. O documento apresenta os tópicos na forma de diretrizes, mas não apresenta a contextualização das orientações à realidade do DC da SMS, evidenciando que os procedimentos descritos na Política de Segurança de Acesso Físico são realizados conforme as orientações e boas práticas, resguardando assegurar o acesso autorizado e evitar o acesso não autorizado a informações e outros ativos associados.

O documento Registro de Acessos a Sala Segura apresenta um quadro com relação de pessoal autorizado a acessar o ambiente da sala segura.

O documento Evidência do Armazenamento de Imagens apresenta listagem com arquivos de vídeo, identificando tratar-se de imagens da Câmera 07, dos dias 01.05.23 a 31.05.23.

3.2.3. Critério

O critério utilizado para avaliar a aderência do controle realizado pela SMS no acesso físico ao DC foi baseado nos controles descritos na NBR ISO 27002/22: Controles organizacionais (5.15 - Controle de acesso) e Controles físicos (7.1 - Perímetros de segurança física; 7.2 - Entrada

física; 7.3 - Segurança de escritórios, salas e instalações; 7.4 - Monitoramento de segurança física; 7.5 - Proteção contra ameaças físicas e ambientais e 7.8 - Localização e proteção de equipamentos).

O item 5.15 - Controle de acesso da NBR ISO 27002/22 recomenda que as regras para controlar o acesso físico e lógico às informações e outros ativos associados sejam estabelecidas e implementadas com base nos requisitos de segurança da informação e de negócios, com o propósito de assegurar o acesso autorizado e evitar o acesso não autorizado a informações e outros ativos associados.

O item 7.1 - Perímetros de segurança física da NBR ISO 27002/22 recomenda que perímetros de segurança sejam definidos e usados para proteger áreas que contenham informações e outros ativos associados, com o propósito de evitar acesso físico não autorizado, danos e interferências nas informações da organização e outros ativos associados.

O item 7.2 - Entrada física da NBR ISO 27002/22 recomenda que as áreas seguras sejam protegidas por controles de entrada e pontos de acesso apropriados, com o propósito de assegurar que ocorra apenas acesso físico autorizado às informações da organização e outros ativos associados.

O item 7.3 - Segurança de escritórios, salas e instalações da NBR ISO 27002/22 recomenda que seja projetada e implementada segurança física para escritórios, salas e instalações, com o propósito de evitar acesso físico não autorizado, danos e interferências nas informações da organização e outros ativos associados em escritórios, salas e instalações.

O item 7.4 - Monitoramento de segurança física da NBR ISO 27002/22 recomenda que as instalações sejam monitoradas continuamente para acesso físico não autorizado, com o propósito de detectar e impedir o acesso físico não autorizado.

O item 7.5 - Proteção contra ameaças físicas e ambientais da NBR ISO 27002/22 recomenda que a proteção contra ameaças físicas e ambientais, como desastres naturais e outras ameaças físicas intencionais ou não intencionais à infraestrutura, seja projetada e implementada, com o propósito de prevenir ou reduzir as consequências de eventos originários de ameaças físicas e ambientais.

O item 7.8 - Localização e proteção de equipamentos da NBR ISO 27002/22 recomenda que os equipamentos sejam posicionados com segurança e proteção, com o propósito de reduzir os riscos de ameaças físicas e ambientais, e de acesso não autorizado e danos.

3.2.4. Evidências

As constatações da vistoria *in loco* e a documentação apresentada pela SMS foram avaliadas, buscando identificar a aderência da infraestrutura e dos termos dos documentos analisados com as orientações dos itens 5.15 - Controle de acesso; 7.1 - Perímetros de segurança física; 7.2 - Entrada física; 7.3 - Segurança de escritórios, salas e instalações; 7.4 - Monitoramento de segurança física; 7.5 - Proteção contra ameaças físicas e ambientais e 7.8 - Localização e proteção de equipamentos.

3.2.4.1. Controle de acesso (item 5.15 da NBR ISO 27002/22)

Os procedimentos avaliados não atendem às orientações do item 5.15 - Controle de acesso da NBR ISO 27002/22, que orienta que as regras para controlar o acesso físico e lógico às informações e outros ativos associados sejam estabelecidas e implementadas com base nos requisitos de segurança da informação e de negócios e, portanto, não garantem o propósito de assegurar o acesso autorizado e evitar o acesso não autorizado a informações e outros ativos associados.

i. A PSI e documentos assessórios (PSAF, RASS) não abrangem todas as premissas do item de controle;

ii. Não foi localizada evidência definição dos requisitos de segurança da informação e de negócios relacionados ao controle de acesso no PSAF;

iii. Não há definição de quais entidades requerem qual tipo de acesso ao ambiente seguro e seus recursos;

iv. O RASS não descreve processo formal de solicitações de acesso ao ambiente do DC;

v. A fechadura utilizada na sala segura não suporta o registro de histórico de acesso;

vi. O RASS apresenta a relação de pessoal autorizado a acessar o ambiente do DC, mas não apresenta diferenciação de direitos de acesso e a classificação das informações; diferenciação entre os direitos de acesso e as necessidades e requisitos de segurança do perímetro físico ou diferenciação de direitos e as restrições de acesso a redes e serviços de rede.

3.2.4.2. Perímetros de segurança física (item 7.1 da NBR ISO 27002/22)

Os procedimentos avaliados não atendem às orientações do item 7.1 - Perímetros de segurança física da NBR ISO 27002/22, que orienta que perímetros de segurança sejam definidos e usados para proteger áreas que contenham informações e outros ativos associados e, portanto, não garantem o propósito de evitar acesso físico não autorizado, danos e interferências nas informações da organização e outros ativos associados.

Apesar de o PSAF apresentar diretrizes sobre o controle do perímetro de segurança, ressalva-se que não apresenta a contextualização das orientações à realidade do DC da SMS e, dessa forma, os procedimentos avaliados não garantem o propósito de evitar acesso físico não autorizado, danos e interferências nas informações da organização e outros ativos associados.

3.2.4.3. Entrada física (item 7.2 da NBR ISO 27002/22)

Os procedimentos avaliados não atendem às orientações do item 7.2 - Entrada física da NBR ISO 27002/22, que orienta que as áreas seguras sejam protegidas por controles de entrada e pontos de acesso apropriados e, portanto, não garantem o propósito de assegurar que ocorra apenas acesso físico autorizado às informações da organização e outros ativos associados.

i. O item 3.1.2 do PSAF dispõe que “Todo acesso físico ao ambiente do *Data Center* deve ser registrado, controlado e monitorado”. Entretanto, o procedimento descrito no documento não prevê livro de registro físico nem lógico;

ii. A SMS apresentou a informação de que “a fechadura utilizada na sala segura não suporta o registro de histórico de acesso”;

iii. Na vistoria, não foi solicitado o registro dos visitantes em livro próprio de registro de visitantes da sala segura;

iv. Não é feito um cadastro específico para visitantes acessarem a sala segura;

v. Não fazem parte do procedimento imposto ao visitante, instruções sobre os requisitos de segurança da área e procedimentos de emergência;

vi. Não foi observada área reservada de entrega e carregamento relacionada ao ambiente do DC.

3.2.4.4. Segurança de escritórios, salas e instalações (item 7.3 da NBR ISO 27002/22)

Os procedimentos avaliados estão alinhados com as orientações do item 7.3 - Segurança de escritórios, salas e instalações da NBR ISO 27002/22, que orienta que seja projetada e implementada segurança física para escritórios, salas e instalações, com o propósito de evitar acesso físico não autorizado, danos e interferências nas informações da organização e outros ativos associados em escritórios, salas e instalações.

Não foram identificados apontamentos.

3.2.4.5. Monitoramento de segurança física (item 7.4 da NBR ISO 27002/22)

Os procedimentos avaliados não atendem às orientações do item 7.4 - Monitoramento de segurança física da NBR ISO 27002/22, que orienta que as instalações sejam monitoradas continuamente para acesso físico não autorizado e, portanto, não garantem o propósito de detectar e impedir o acesso físico não autorizado.

i. Ambiente interno da sala segura monitorado por somente uma câmera;

ii. A câmera instalada no interior da sala segura não permite a visualização de todo o ambiente;

iii. Não foi constatado sistema de alarme durante a vistoria.

O PSAF apresenta diretrizes alinhadas às orientações do item 7.4 - Monitoramento de segurança física. Entretanto, falta contextualização com a realidade do ambiente da sala segura da SMS. A vistoria realizada evidenciou impossibilidade de aplicação da política no ambiente atual do DC.

3.2.4.6. Proteção contra ameaças físicas e ambientais (item 7.5 da NBR ISO 27002/22)

Os procedimentos avaliados não atendem plenamente às orientações do item 7.5 - Proteção contra ameaças físicas e ambientais da NBR ISO 27002/22, que orienta que a proteção contra ameaças físicas e ambientais, como desastres naturais e outras ameaças físicas intencionais ou não intencionais à infraestrutura, seja projetada e implementada, e, portanto, não garantem o propósito de prevenir ou reduzir as consequências de eventos originários de ameaças físicas e ambientais.

i. O ambiente do DC possui falhas em sua proteção contra fogo;

ii. Não foram identificadas medidas de proteção adequadas contra inundações, explosivos e armas.

3.2.4.7. Localização e proteção de equipamentos (item 7.8 da NBR ISO 27002/22)

Os procedimentos avaliados não atendem às orientações do item 7.8 - Localização e proteção de equipamentos da NBR ISO 27002/22, que orienta que os equipamentos sejam posicionados com segurança e proteção e, portanto, não garantem o propósito de reduzir os riscos de ameaças físicas e ambientais, e de acesso não autorizado e danos.

iii. Ambiente do DC é isolado fisicamente do ambiente da DTIC por meio de paredes, mas não tem características de sala cofre;

iv. Na inspeção foi observado que está limitado aos aparelhos de ar-condicionado.

O PSAF apresenta diretrizes alinhadas às orientações do item 7.8 - Localização e proteção de equipamentos da NBR ISO 27002/22, mas não apresenta a contextualização das orientações à realidade do DC da SMS, evidenciando de forma prática os procedimentos que devem ser realizados a fim de assegurar segurança e proteção aos equipamentos. A vistoria realizada evidenciou que a aplicação da política no ambiente atual do DC não é efetiva.

3.2.5. Causas

Deficiência na Política de Segurança de Acesso Físico, carecendo de procedimentos alinhados à realidade do DC da SMS.

Procedimentos de controle implantados apresentam deficiências e não atendem à Política de Segurança de Acesso Físico.

3.2.6. Efeitos

As deficiências na Política de Segurança de Acesso Físico e nos procedimentos adotados expõem a riscos possíveis de serem mitigados quanto ao acesso físico ao DC e colocam em risco a segurança da informação do ambiente do DC.

3.3. A política de *Backup* implantada no DC da SMS é efetiva?

3.3.1. Achado

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 atendidas.

3.3.2. Situação encontrada

A fim de subsidiar o exame documental para avaliar a aderência à NBR ISO 27002/22, das premissas adotadas nos normativos e adequação da política de *Backup* implantada no ambiente do DC da SMS, foi feita requisição de documentos e informações direcionada à DTIC, conforme reproduzido (peça 5, fl. 2):

> 10. Documentos da Política de *Backup* vinculando às políticas aos respectivos sistemas e aplicações hospedados;
>
> R: Informação contida no documento Política de *Backup*
>
> 11. Documentos dos Procedimentos Operacionais implantados para suportar o processo de *backup* (e outras políticas de contingência, se houver);
>
> R: Informação contida no documento Política de *Backup*
>
> 12. Documento (ou esclarecimentos, caso necessário) apresentando o embasamento para os períodos de retenção dos *backups* adotados pela SMS;
>
> R: Os períodos de retenção dos *backup*s têm como base a ISO/IEC 27002:2013
>
> 13. Informação sobre os procedimentos relacionados às mídias utilizadas no processo de *backup* (tipos de mídia utilizadas, locais de armazenamento, prazo, política de descarte etc.), apresentando cópia das normas, caso haja;
>
> R: Não temos *backup* em mídia física
>
> 15. Documentação com as evidências da efetiva realização do processo de *backup*, incluindo testes de restauração;
>
> R: Informação contida no documento Evidência de *Backup* e Restauração

Em resposta a esta requisição, a SMS encaminhou os seguintes documentos, que compõem a documentação da auditoria:

i. "Evidência de *Backup* e Restauração.pdf"

ii. "Política de *Backup*.pdf"

3.3.3. Critério

O critério utilizado para avaliar a aderência da política de *backup* implantada no DC da SMS foi baseado nos controles descritos na NBR ISO 27002/22 e Orientação Técnica (OT) nº 07 da Secretaria Municipal de Inovação e Tecnologia (SMIT). Neste quesito foram avaliados controle da NBR ISO 27002/22 (item 8.13 - *Backup* das informações) e Orientação Técnica (OT) SMIT nº 07 (4 - Testes, Retenção e Restauração de *Backup*; 5 - Diretrizes de *Backup* para *Data Center*s Próprios e 6 - Armazenamento de Dados)

O item 8.13 - *Backup* das informações da NBR ISO 27002/22 recomenda que as cópias de *backup* de informações, *software* e sistemas sejam mantidas e testadas regularmente de acordo com a política específica por tema acordada sobre *backup*, com o propósito de permitir a recuperação da perda de dados ou sistemas.

3.3.4. Evidências

Na inspeção física, foram verificadas as condições gerais da Sala Segura. A política de *backup* não fez parte do escopo da inspeção física, uma vez que sua implementação é intangível.

A documentação apresentada pela SMS foi avaliada, buscando identificar a aderência de seus termos com as orientações do item 8.13 - *Backup* das informações da NBR ISO 27002/22 e itens 4, 5 e 6 da Orientação Técnica nº 07 da SMIT.

3.3.4.1. *Backup* das informações (item 8.13 da NBR ISO 27002/22)

Os procedimentos avaliados não atendem às orientações do item 8.13 - *Backup* das informações da NBR ISO 27002/22, que orienta que cópias de *backup* de informações, *software* e sistemas sejam mantidas e testadas regularmente de acordo com a política específica por tema acordada

sobre *backup* e, portanto, não garantem o propósito de permitir a recuperação da perda de dados ou sistemas.

i. Não é possível visualizar a efetividade da realização dos *backups*, na forma definida na Política de *Backup*, que dispõe no item 2.2 - Da frequência e retenção dos dados, assim como efetividade dos testes de restauração, por meio do documento Evidência de *Backup* e Restauração disponibilizado pela SMS;

ii. O documento Política de *Backup* não especifica local das instalações de *backup*;

iii. O documento Política de *Backup* não apresenta planos específicos de *backup*;

iv. O documento Política de *Backup* não apresenta forma de registros das cópias de *backup* e documentação dos procedimentos de restauração de *backup*;

v. O documento Política de *Backup* não estabelece procedimentos operacionais monitorem a execução do *backup* e resolvam falhas dos *backups* programados;

vi. O documento Política de *Backup*, item 2.1 estabelece realização de testes, mas não especifica a sua operacionalização;

vii. O documento Política de *Backup*, item 2.6 não estabelece, em seus procedimentos, tempo de restauração alinhado com o plano de continuidade de negócios;

viii. O documento Política de *Backup* não especifica realização de *backup* em nuvem;

ix. O documento Política de *Backup* não especifica exclusão de informações em mídia de armazenamento usada para *backup*;

O documento apresenta os tópicos na forma de diretrizes, mas não apresenta a contextualização das orientações à realidade do DC da SMS, evidenciando de forma prática os procedimentos que devem ser realizados.

Além das orientações da NBR ISO 27002/22, sugere-se à SMS atentar-se às recomendações da OT nº 07 - *Backup* e armazenamento de dados, especialmente os itens: i) 4 - Testes,

Retenção e Restauração de *Backup*; ii) 5 - Diretrizes de *Backup* para *Data Center*s Próprios e iii) 6 - Armazenamento de Dados.

3.3.5. Causas

Deficiência no documento Política de *Backup*, pela falta de procedimentos alinhados à realidade do DC da SMS e ausência de procedimento operacional padrão para a realização de *backups* e restaurações.

3.3.6. Efeitos

A Política de *Backup* implantada no DC da SMS com pouca efetividade expõe a riscos possíveis de serem mitigados quanto à segurança da informação do ambiente do DC.

3.4. A Política de Continuidade do Negócio (PCN) e da Segurança da Informação foi implementada?

3.4.1. Achado

Não há procedimento formal para a Política de Continuidade do Negócio e da Segurança da Informação do ambiente do DC.

3.4.2. Situação encontrada

A fim de subsidiar o exame documental para avaliar a aderência à NBR ISO 27002/22, das premissas adotadas nos normativos e adequação da Política de Continuidade do Negócio (PCN) e da Segurança da Informação, foi feita requisição de documentos e informações direcionada à DTIC, conforme reproduzido (peça 5, fl. 2):

> 14. Documento da Política de Continuidade do Negócio e da Segurança da Informação (incluindo detalhamento do processo de *backup* no contexto da política);
> R: Documento em fase de elaboração

Conforme a citação acima, foi informado pelo DTIC que o documento estava em fase de elaboração.

Alternativamente, foi realizada a análise da “Política de PSID_001 - Política de Segurança da Informação.pdf”.

3.4.3. Critério

O critério utilizado para avaliar a aderência da Política de Continuidade do Negócio e da Segurança da Informação implantada no DC da SMS foi baseado nos controles descritos na NBR ISO 27002/22. Neste quesito foram avaliados os Controles 5.29 - Segurança da informação durante a disrupção e 5.30 - Prontidão de TIC para continuidade de negócios.

O item 5.29 - Segurança da informação durante a disrupção da NBR ISO 27002/22 recomenda que a organização planeje como manter a segurança da informação em um nível apropriado durante a disrupção, com o propósito de assegurar a disponibilidade das informações da organização e outros ativos associados durante a disrupção.

O item 5.30 - Prontidão de TIC para continuidade de negócios da NBR ISO 27002/22 recomenda que a prontidão da TIC seja planejada, implementada, mantida e testada com base nos objetivos de continuidade de negócios e nos requisitos de continuidade da TIC, com o propósito de proteger as informações e outros ativos associados durante a disrupção.

3.4.4. Evidências

Na inspeção física, foram verificadas as condições gerais da Sala Segura. A política de continuidade de negócio não fez parte do escopo da inspeção física, uma vez que sua implementação é intangível.

A documentação apresentada pela SMS foi avaliada, buscando identificar a aderência de seus termos com as orientações dos itens 5.29 - Segurança da informação durante a disrupção e 5.30 - Prontidão de TIC para continuidade de negócios da NBR ISO 27002/22.

3.4.4.1.1. Segurança da informação durante a disrupção (item 5.29 da NBR ISO 27002/22)

Os procedimentos avaliados não atendem às orientações do item 5.29 - Segurança da informação durante a disrupção da NBR ISO 27002/22, que orienta que a organização planeje como manter a segurança da informação em um nível apropriado durante a disrupção e, portanto,

não garantem o propósito de proteger as informações e outros ativos associados durante a disrupção.

A PSI apresenta diretrizes alinhadas com as orientações do item 5.29 - Segurança da informação durante a disrupção da NBR ISO 27002/22, mas não apresenta a contextualização das orientações à realidade do DC da SMS, materializado em um plano de continuidade de negócios, evidenciando de forma prática os procedimentos que devem ser realizados a fim de garantir a segurança e proteção das informações e outros ativos associados durante a disrupção.

3.4.4.2. Prontidão de TIC para continuidade de negócios (item 5.30 da NBR ISO 27002/22)

Os procedimentos avaliados não atendem às orientações do item 5.30 - Prontidão de TIC para continuidade de negócios da NBR ISO 27002/22, que orienta que a prontidão da TIC seja planejada, implementada, mantida e testada com base nos objetivos de continuidade de negócios e nos requisitos de continuidade da TIC e, portanto, não garantem o propósito de assegurar a disponibilidade das informações da organização e outros ativos associados durante a disrupção.

A PSI apresenta diretrizes alinhadas com as orientações do item 5.30 - Prontidão de TIC para continuidade de negócios da ISO NBR 27002/22, mas não apresenta a contextualização das orientações à realidade do DC da SMS, materializado em um plano de continuidade de negócios, evidenciando de forma prática os procedimentos que devem ser realizados a fim de garantir a disponibilidade das informações da organização e outros ativos associados durante a disrupção.

Os requisitos de continuidade das TIC são o resultado da análise de impacto nos negócios (*Business Impact Analysis* – BIA), essencial para a definição do tempo de recuperação (*Recovery Time Objective* – RTO) e ponto de recuperação (*Recovery Point Objective* – RPO), quesitos essenciais na definição do plano de continuidade de negócios.

3.4.5. Causas

Ausência de procedimento formal para a gestão da Política de Continuidade do Negócio e da Segurança da Informação do ambiente do DC.

3.4.6. Efeitos

Exposição a riscos possíveis de serem mitigados na disponibilidade das informações da organização e outros ativos associados durante a disrupção.

3.5. Existe redundância nos recursos?

3.5.1. Achado

A ausência de redundância de recursos da infraestrutura do DC da SMS não atende aos requisitos de segurança da informação.

3.5.2. Situação encontrada

A inspeção física foi realizada com o acompanhamento de representantes da DTIC. A vistoria foi registrada por meio do relatório fotográfico, apêndice I do trabalho. Na inspeção física, foram verificadas as condições gerais da Sala Segura. Em relação às condições das dependências foi constatado:

- A temperatura do ambiente da sala segura é mantida por meio de dois aparelhos de ar-condicionado, do tipo *Split*, de 22 mil BTUs. Os evaporadores estão dispostos no interior da sala segura. Os condensadores foram instalados na parte externa da edificação. Não foi informado o esquema de funcionamento dos equipamentos (se o funcionamento é concomitante ou se existe algum esquema de funcionamento alternado ou redundante dos equipamentos) – fotos 5 e 7;

- Um equipamento *No Break* no interior da sala segura – fotos 8 e 10.

A fim de subsidiar o exame documental para avaliar a aderência à NBR ISO 27002/22, das premissas adotadas nos normativos e adequação da redundância nos recursos do *Data Center*, foi feita requisição de documentos e informações direcionada à DTIC, conforme reproduzido (peça 5, fl. 1):

> 4. Relação dos *links* de comunicação que suprem o *data center*, relacionando os contratos, prazos e finalidade;
> R: *Link* de 155MB com redundância, anexo documento de adesão e Contratos de *Data Center.*

Em resposta a esta requisição, a SMS encaminhou os documentos:

i. “RELAÇÃO DE CONTRATOS - DATA CENTER.pdf”

ii. “Link MPLS SMS GAB Santa Isabel.pdf”

3.5.3. Critério

O critério utilizado para avaliar a redundância de recursos no DC da SMS foi baseado nos controles descritos na NBR ISO 27002/22. Neste quesito foram avaliados os Controles do item 8.14 - Redundância dos recursos de tratamento de informações.

O item 8.14 - Redundância dos recursos de tratamento de informações da NBR ISO 27002/22 recomenda que os recursos de tratamento de informações sejam implementados com redundância suficiente para atender aos requisitos de disponibilidade, com o propósito de assegurar o funcionamento contínuo dos recursos de tratamento de informações.

3.5.4. Evidências

As constatações da vistoria *in loco* e a documentação apresentada pela SMS foram avaliadas, buscando identificar a aderência da infraestrutura e dos termos dos documentos analisados com as orientações do item 8.14 - Redundância dos recursos de tratamento de informações da NBR ISO 27002/22.

3.5.4.1. Redundância dos recursos de tratamento de informações (item 8.14 da NBR ISO 27002/22)

Os procedimentos avaliados não atendem às orientações do item 8.14 - Redundância dos recursos de tratamento de informações da NBR ISO 27002/22, que orienta que os recursos de tratamento de informações sejam implementados com redundância suficiente para atender aos requisitos de disponibilidade e, portanto, não garantem o propósito de assegurar o funcionamento contínuo dos recursos de tratamento de informações.

i. A PSI não identifica os requisitos para a disponibilidade de serviços de negócios e sistemas de informação;

ii. O único componente redundante disponível no DC é representado por dois *links* redundantes fornecido pela empresa Prodam;

iii. A PSI não aborda componentes redundantes para o caso de falha nos recursos de tratamento de informações;

iv. Foi informado pela SMS que o atual ambiente não possuía redundância em todos os sistemas recomendados na norma;

v. A PSI não aborda procedimentos de testes nos sistemas de informação redundantes;

vi. A PSI não apresenta diretrizes alinhadas com as orientações do item 8.14 - Redundância dos recursos de tratamento de informações da NBR ISO 27002/22.

3.5.5. Causas

Deficiência na PSI e nos processos de redundância de recursos da infraestrutura do DC da SMS, expondo a riscos o funcionamento contínuo dos recursos de tratamento de informações.

3.5.6. Efeitos

A ausência de redundância em alguns dos recursos da infraestrutura do DC da SMS expõe a riscos o funcionamento contínuo dos recursos de tratamento de informações.

3.6. Existe uma gestão da capacidade do DC visando atender aos requisitos dos serviços?

3.6.1. Achado

Não há procedimento formal para a gestão de capacidade do ambiente do DC.

3.6.2. Situação encontrada

A fim de subsidiar o exame documental para avaliar a aderência à NBR ISO 27002/22, das premissas adotadas nos normativos e adequação da gestão da capacidade do DC visando atender aos requisitos dos serviços, foi feita requisição de documentos e informações direcionada à DTIC, conforme reproduzido (peça 5, fl. 2):

> 16. Documento do Plano de Gestão da Capacidade (requisitos e criticidade dos serviços envolvidos e os respectivos controles de identificação dos problemas de capacidade);
> R: Documento em fase de elaboração

Conforme a citação acima, foi informado pelo DTIC que o documento estava em fase de elaboração.

Alternativamente, foi realizada a análise da “Política de PSID_001 - Política de Segurança da Informação.pdf”.

3.6.3. Critério

O critério utilizado para avaliar a gestão da capacidade do DC da SMS foi baseado nos controles descritos na NBR ISO 27002/22. Neste quesito foram avaliados os Controles do item 8.6 - Gestão de capacidade.

O item 8.6 - Gestão de capacidade da NBR ISO 27002/22 recomenda que o uso dos recursos seja monitorado e ajustado de acordo com os requisitos atuais e esperados de capacidade, com propósito de assegurar a capacidade necessária dos recursos de tratamento de informações, recursos humanos, escritórios e outros serviços de infraestrutura.

3.6.4. Evidências

As constatações da vistoria *in loco* e a documentação apresentada pela SMS foram avaliadas, buscando identificar a aderência da infraestrutura e dos termos dos documentos analisados com as orientações do item 8.6 - Gestão de capacidade da NBR ISO 27002/22.

3.6.4.1. Gestão de capacidade (item 8.6 da NBR ISO 27002/22)

Os procedimentos avaliados não atendem às orientações do item 8.6 - Gestão de capacidade da NBR ISO 27002/22, que orienta que o uso dos recursos seja monitorado e ajustado de acordo com os requisitos atuais e esperados de capacidade e, portanto, não garantem o propósito de assegurar a capacidade necessária dos recursos de tratamento de informações, recursos humanos, escritórios e outros serviços de infraestrutura.

i. A PSI não aborda premissas relacionadas a:

    a. Requisitos de capacidade para recursos de tratamento de informações (1.2.2.1.1);

b. Ajuste e monitoramento do sistema para assegurar e melhorar a disponibilidade e a eficiência dos sistemas (1.2.2.1.2);

c. Testes de estresse de sistemas e serviços para confirmar que a capacidade suficiente do sistema (1.2.2.1.3);

d. Controles detectivos e projeções dos requisitos futuros de capacidade. (1.2.2.1.4 e 1.2.2.1.5);

e. Consideração de missão crítica ou documentação do plano de gestão de capacidade. (1.2.2.1.9);

ii. A PSI NÃO apresenta diretrizes alinhadas com as orientações do item 8.6 - Gestão de capacidade da NBR ISO 27002/22.

3.6.5. Causas

Ausência de procedimento formal para a gestão de capacidade do ambiente do DC no contexto da Política de Segurança da Informação da SMS.

3.6.6. Efeitos

Exposição a riscos possíveis de serem mitigados pela falta de planejamento da capacidade necessária dos recursos de tratamento de informações, recursos humanos, escritórios e outros serviços de infraestrutura do ambiente do DC.

3.7. Existe um processo de gestão de mudanças no DC efetivo e suficiente?

3.7.1. Achado

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.

3.7.2. Situação encontrada

A fim de subsidiar o exame documental para avaliar a aderência à NBR ISO 27002/22, das premissas adotadas nos normativos e adequação do processo de gestão de mudanças no DC, foi feita requisição de documentos e informações direcionada à DTIC, conforme reproduzido (peça 5, fl. 2):

> 17. Documento do Plano de Gestão de Mudanças (procedimentos e responsabilidades, identificação, aprovação, recuperação de mudanças).
> R: Informação contida no documento Plano de Gestão de Mudanças

Em resposta a esta requisição, a SMS encaminhou o documento:

i. “Plano de Gestão de Mudanças.pdf”

3.7.3. Critério

O critério utilizado para avaliar a gestão de mudanças no DC da SMS foi baseado nos controles descritos na NBR ISO 27002/22. Neste quesito, foram avaliados os Controles do item 8.32 - Gestão de mudanças.

O item 8.32 - Gestão de mudanças da NBR ISO 27002/22 recomenda que mudanças nos recursos de tratamento de informações e sistemas de informação estejam sujeitas a procedimentos de gestão de mudanças, com o propósito de preservar a segurança da informação ao executar mudanças.

3.7.4. Evidências

Na inspeção física, foram verificadas as condições gerais da Sala Segura. A política de continuidade de negócio não fez parte do escopo da inspeção.

A documentação apresentada pela SMS foi avaliada, buscando identificar a aderência de seus termos com as orientações do item 8.32 - Gestão de mudanças da NBR ISO 27002/22.

3.7.4.1. Gestão de mudanças (item 8.32 da NBR ISO 27002/22)

O Plano de Gestão de Mudanças (PGM) apresenta diretrizes alinhadas com as orientações do item 8.32 - Gestão de mudanças da NBR ISO 27002/22, que orienta que mudanças nos recursos

de tratamento de informações e sistemas de informação estejam sujeitas a procedimentos de gestão de mudanças.

O documento apresenta os tópicos na forma de diretrizes, mas não apresenta a contextualização das orientações à realidade do DC da SMS, evidenciando de forma prática os procedimentos que devem ser realizados a fim de garantir que as mudanças nos recursos de tratamento de informações e sistemas de informação estejam sujeitas aos procedimentos de gestão de mudanças especificados no documento, resguardando o propósito de preservar a segurança da informação ao executar mudanças. Ressalva-se que:

i. O PGM se apresenta sem a identificação completa do documento, indicando tratar-se de minuta que ainda carece de desenvolvimento e a devida formalização, com a aprovação expressa para a sua formalização como um procedimento a ser seguido pelos colaboradores responsáveis pela operação e manutenção do DC da SMS;

ii. A orientação de adoção de que procedimentos de controle de mudanças sejam documentados não foi identificada nas premissas expostas do PGM;

iii. A orientação de que os procedimentos de controle de alteração para infraestrutura e software de TIC sejam integrados não foi identificada nas premissas expostas do PGM.

3.7.5. Causas

Deficiência no Plano de Gestão de Mudanças, sem a devida formalização, controle de versões, aprovação, indicação de responsáveis e responsabilidades, carecendo de procedimentos alinhados à realidade do DC da SMS.

3.7.6. Efeitos

Exposição a riscos possíveis de serem mitigados por meio de um plano e gestão de mudanças à segurança da informação do ambiente do DC.

4. ANÁLISE DOS COMENTÁRIOS DO GESTOR

Não houve comentários do gestor.

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**).

Em 25.03.24

CARLOS ALBUQUERQUE LEMOS
Auditor de Controle Externo

MAURICIO KAZUHIRO SATO
Auditor de Controle Externo

RENATO SAMBRA SUYAMA
Auditor de Controle Externo

ADRIANO GONÇALVES ZAMBON
Supervisor de Controle Externo 17

De acordo em 01.04.24.

HÉLIO RICARDO G. MURCI DE AZEVEDO
Coordenador de Controle Externo VIII

8. APÊNDICES

Relatório Fotográfico – Vistoria *Data Center* SMS

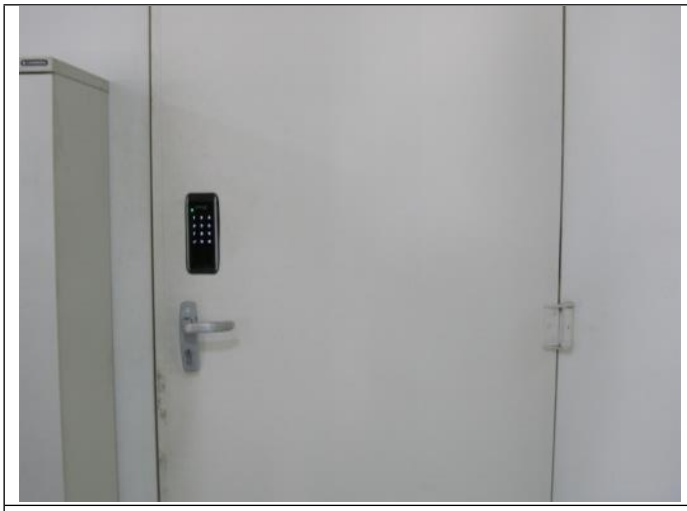

Foto 1 – Porta de entrada única

Foto 2 – Porta vista interna

Foto 3 – Trava eletrônica

Foto 4 – Extintor de incêndio (externo)

Foto 5 – Ar-condicionado um

Foto 6 – Câmera de monitoramento

Foto 7 – Ar-condicionado dois

Foto 8 – Nobreak

Foto 9 – Janela exterior

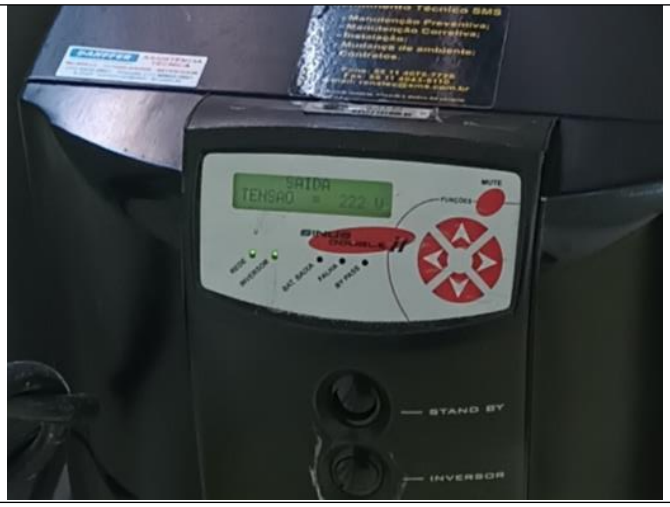

Foto 10 – Detalhe Nobreak

Foto 11 – Vista traseira superior dos *racks*

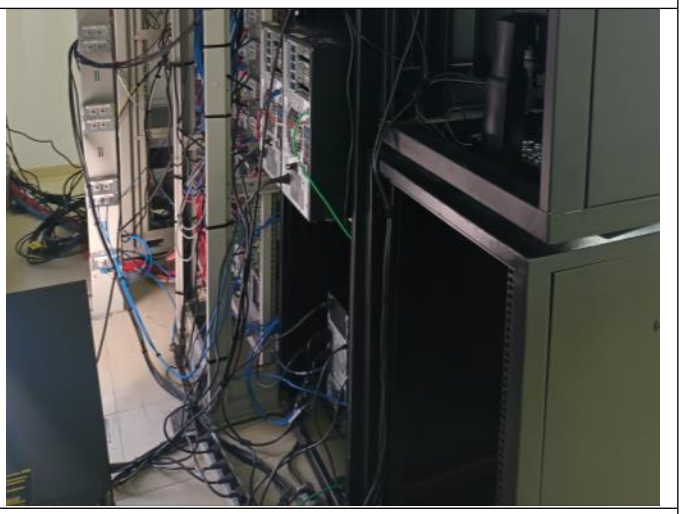

Foto 12 – Vista traseira inferior dos *racks*

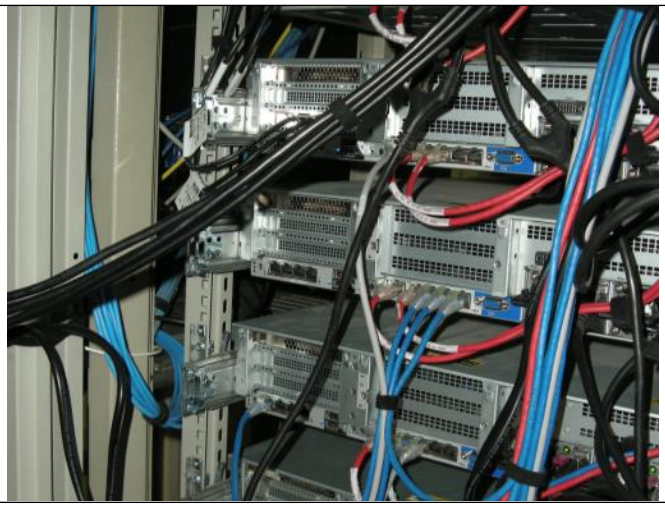

Foto 13 – Cabos

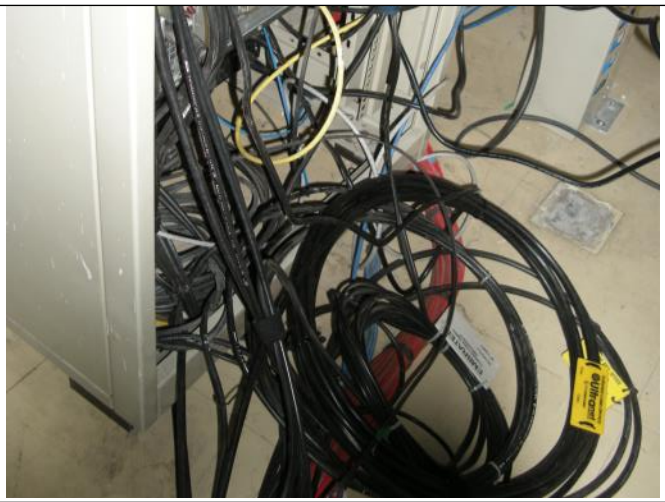

Foto 14 – Cabos

Foto 15 – Cabos

Foto 16 – Cabos

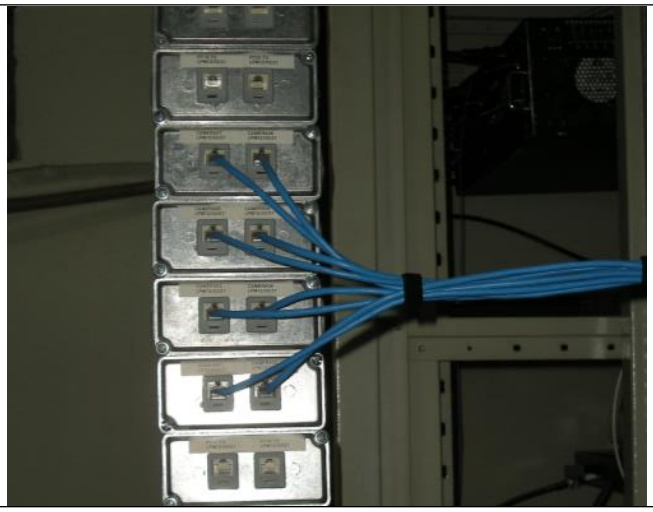

Foto 17 – Cabos

Foto 18 – Armários

Foto 19 – *Rack* 1 e 2

Foto 20 – Rack 3, 4 e 5

Foto 21 – Vista superior *rack* 1

Foto 22 – Vista superior *rack* 3

	
Foto 23 – Vista medial *rack* 3	**Foto 24 – Vista inferior *rack* 3**
	
Foto 25 – Vista superior *rack* 5	**Foto 26 – Vista inferior *rack* 5**