



Tribunal de Contas
Mato Grosso

TRIBUNAL DO CIDADÃO

Relatório de Auditoria Operacional

Governança de Tecnologia da Informação da Secretaria de Estado de Fazenda

de Mato Grosso – 2017



PubliContas

Editora do Tribunal de Contas
do Estado de Mato Grosso



Tribunal de Contas
Mato Grosso

TRIBUNAL DO CIDADÃO

Identidade Organizacional

NEGÓCIO

Controle da gestão dos recursos públicos.

MISSÃO

Controlar a gestão dos recursos públicos do Estado e dos municípios de Mato Grosso, mediante orientação, avaliação de desempenho, fiscalização e julgamento, contribuindo para a qualidade e a efetividade dos serviços, no interesse da sociedade.

VISÃO

Ser reconhecido como instituição essencial ao regime democrático, atuando pela melhoria da qualidade da gestão pública e no combate à corrupção e ao desperdício.

VALORES

Justiça: Pautar-se estritamente por princípios de justiça, pela verdade e pela lei, com integridade, equidade, coerência, impessoalidade e imparcialidade.

Qualidade: Atuar com inovação e de forma ágil, tempestiva, efetiva, eficiente e eficaz, com base em padrões de excelência de gestão e de controle.

Profissionalismo: Atuar com base nos princípios e valores éticos e de forma independente, técnica, responsável, proativa, leal e comprometida com a identidade institucional e com o interesse público.

Transparência: Disponibilizar e comunicar tempestivamente, em linguagem clara e de fácil acesso, as ações, decisões e atos de gestão do TCE-MT, bem como as informações dos fiscalizados sob sua guarda, no interesse da sociedade.

Consciência Cidadã: Estimular o exercício da cidadania e do controle social da gestão pública.

Corpo Deliberativo

TRIBUNAL PLENO

Presidente

Conselheiro Gonçalo Domingos de Campos Neto

Vice-Presidente

Conselheiro Interino Luiz Henrique Moraes de Lima

Corregedor-Geral

Conselheiro Interino Isaías Lopes da Cunha

Ouvidor-Geral

Conselheiro Interino Luiz Carlos Azevedo Costa Pereira

Integrantes

Conselheira Interina Jaqueline Maria Jacobsen Marques

Conselheiro Interino Moises Maciel

Conselheiro Interino João Batista de Camargo Junior

1ª CÂMARA

Presidente

Conselheira Interina Jaqueline Maria Jacobsen Marques

Integrantes

Conselheiro Interino Luiz Henrique Moraes de Lima

Conselheiro Interino Luiz Carlos Azevedo Costa Pereira

2ª CÂMARA

Presidente

Conselheiro Interino Moises Maciel

Integrantes

Conselheiro Interino Isaías Lopes da Cunha

Conselheiro Interino João Batista de Camargo Junior

CONSELHEIROS

Conselheiro Antonio Joaquim Moraes Rodrigues Neto

Conselheiro José Carlos Novelli

Conselheiro Valter Albano da Silva

Conselheiro Waldir Júlio Teis

Conselheiro Sérgio Ricardo de Almeida

CONSELHEIRO SUBSTITUTO JUNTO À PRESIDÊNCIA

Ronaldo Ribeiro de Oliveira

MINISTÉRIO PÚBLICO DE CONTAS

Procurador-Geral

Getúlio Velasco Moreira Filho

Procurador-Geral Substituto

Alisson Carvalho de Alencar

Procuradores de Contas

Gustavo Coelho Deschamps

William de Almeida Brito Júnior

Corpo Técnico

Secretaria-Geral do Tribunal Pleno

Ligia Maria Gahyva Daoud Abdallah

Secretaria da Primeira Câmara

Elizabet Teixeira Sant'anna

Secretaria da Segunda Câmara

Renata Arruda Rosas

Núcleo de Certificação e Controle de Sanções

Ana Karina Pena Endo

Secretaria-Geral de Controle Externo (Segecex)

Volmar Bucco Júnior

Secretaria-Geral Adjunta de Controle Externo

Daniel Poletto Chu

Secretaria de Métodos e Desenvolvimento do Controle Externo

Mônica Cristina dos Anjos Acendino

Secretaria de Gerenciamento de Sistemas Técnicos

Lisandra Ishizuka Hardy Barros

Secretaria de Informações Estratégicas

Victor Augusto Godoy

Consultoria Técnica

Gabriel Liberato Lopes

Secretaria de Controle Externo de Administração Estadual

Carlos Eduardo Amorim França

Secretaria de Controle Externo de Administração Municipal

Francisney Liberato Batista Siqueira

Secretaria de Controle Externo de Atos de Pessoal

Osiel Mendes de Oliveira

Secretaria de Controle Externo de Contratações Públicas

Francis Bortoluzzi

Secretaria de Controle Externo de Educação e Segurança

Patrícia Leite Lozich

Secretaria de Controle Externo de Obras e Infraestrutura

Emerson Augusto de Campos

Secretaria de Controle Externo de Previdência

Eduardo Benjaino Ferraz

Secretaria de Controle Externo de Receita e Governo

Joel Bino do Nascimento Júnior

Secretaria de Controle Externo de Saúde e Meio Ambiente

Lidiane Anjos Bortoluzzi

Corpo de Gestão

Chefe de Gabinete da Presidência

Glauber Silva Tocantins

Secretaria do Sistema de Controle Interno

Élia Maria Antoniêto Siqueira

Secretaria de Articulação Institucional e

Desenvolvimento da Cidadania

Cassyrá Lúcia Corrêa Barros Vuolo

Secretaria de Apoio às Unidades Gestoras

Naíse Godoy de Campos Silva Freire

Consultoria Jurídica-Geral

Patrícia Maria Paes de Barros

Secretaria-Geral da Presidência

Risodalva Beata de Castro

Secretaria Executiva da Corregedoria-Geral

Cristiane Laura de Souza

Secretaria Executiva da Ouvidoria-Geral

Marco Aurélio Queiroz de Souza

Secretaria de Planejamento, Integração e Coordenação

Augustinho Moro

Subsecretaria de Planejamento

Julinil Fernandes de Almeida

Subsecretaria de Integração e Coordenação

Narda Consuelo Vitório Neiva Silva

Secretaria de Comunicação Social

Américo Santos Corrêa

Escola Superior de Contas

Marina Bressane Spinelli Maia de Andrade

Secretaria Executiva de Orçamento, Finanças e Contabilidade

Maurício Marques Júnior

Secretaria Executiva de Tecnologia da Informação

Gilson Gregório

Secretaria Executiva de Gestão de Pessoas

Eneias Viegas da Silva

Núcleo de Qualidade de Vida no Trabalho

Estela Rosa Biancardi

Secretaria Executiva de Administração

Carla Cristiny Esteves de Oliveira

Núcleo de Gestão de Contratos, Convênios e Parcerias

João Norberto de Barros Mayer

Núcleo de Patrimônio

Marcelo Catalano Corrêa

Núcleo de Expediente

Luciano Macaúbas Leite de Campos

Núcleo de Cerimonial

Tânia de Cássia Melo Bosaipo



Tribunal de Contas
Mato Grosso

TRIBUNAL DO CIDADÃO

Relatório de Auditoria Operacional

Governança de Tecnologia da Informação da Secretaria de Estado de Fazenda

de Mato Grosso – 2017



PubliContas
Editora do Tribunal de Contas
do Estado de Mato Grosso

Copyright © Tribunal de Contas de Mato Grosso, 2018.

É permitida a reprodução total ou parcial dos textos dessa obra, desde que citada a fonte.

O conteúdo desta obra está disponível no Portal do TCE-MT para download (www.tce.mt.gov.br).

Dados Internacionais para Catalogação na Publicação (CIP)

M433r

Mato Grosso. Tribunal de Contas do Estado

Relatório de auditoria operacional: governança de Tecnologia da Informação da Secretaria de Estado de Fazenda de Mato Grosso - 2017 / Tribunal de Contas do Estado. – Cuiabá : PubliContas, 2018.

32p. ; 21x29,7 cm ; il.

ISBN 978-85-98587-98-1

1. Planejamento de TI. 2. Profissionais de TI.
3. Gestão de risco de TI. 4. Gerenciamento dos projetos de TI.
- I- Título.

CDU 658.011.56(817.2)

Jânia Gomes
CRB1 2215

EQUIPE TÉCNICA DE AUDITORIA

SECRETARIA DE CONTROLE EXTERNO DE AUDITORIAS OPERACIONAIS

Lidiane Anjos Bortoluzzi *Secretária de Controle Externo de Auditorias Operacionais*

EQUIPE DE AUDITORIA:

Supervisão Patrícia Leite Lozich *Auditadora Pública Externa (coordenadora)*
Equipe de Auditoria Bruno Alberto Zys *Auditor Público Externo*
Marlos Siqueira Alves *Auditor Público Externo*

PRODUÇÃO EDITORIAL

SECRETARIA DE COMUNICAÇÃO

SUPERVISÃO Américo Correa..... *Secretário de Comunicação Social*
EDIÇÃO E PROJETO Doriane Miloch *Assessora Técnica de Publicações da PubliContas*
CAPA Boanerges Capistrano..... *Publicitário*
ILUSTRAÇÕES iStock by Getty Images <<https://www.istockphoto.com/br>>
REVISÃO ORTOGRÁFICA Andhressa Sawaris Barboza



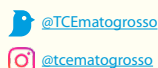
Rua Conselheiro Benjamin Duarte Monteiro, nº 1
Centro Político e Administrativo – CEP: 78049-915 – Cuiabá-MT
+55 65 3613-7561 – publicontas@tce.mt.gov.br – www.tce.mt.gov.br

CARTA DE SERVIÇOS AO CIDADÃO

<http://www.tce.mt.gov.br/uploads/flipbook/CartadeServicos2013/index.html>

Horário de atendimento: 8h às 18h, de segunda a sexta-feira.

Siga:



Resumo

No intuito de colaborar com a Administração Pública, de forma a identificar oportunidades de aperfeiçoamento na Fazenda Pública, esta auditoria avaliou se a Secretaria de Estado de Fazenda (Sefaz-MT) adota práticas de governança para avaliar, gerenciar e monitorar o uso da Tecnologia da Informação no âmbito da instituição.

A avaliação foi realizada com base em normas e boas práticas relacionadas ao tema e executada por meio de pesquisa eletrônica e análise documental. Também foram realizadas reuniões com a Coordenação de Tecnologia da Informação (Coti) no intuito de alinhar entendimentos.

Constatou-se que as práticas de governança corporativa não foram plenamente definidas e implementadas no âmbito da instituição, o que impactou diretamente a implementação das práticas de governança de TI.

Foram identificados:

- a. insuficiência de diretrizes com o objetivo de dirigir a atuação da TI com foco na entrega de resultados para a instituição;
- b. ausência de plano estratégico de TI;
- c. inexistência de estudo de dimensionamento da força de trabalho necessária para o setor de tecnologia da informação, bem como ausência de plano de capacitação de profissionais de TI;
- d. falhas na gestão de riscos de TI, nos processos de segurança da informação, na execução de processos de gestão de serviços de TI e no gerenciamento de projetos de TI.

Por que realizar a auditoria?

A informação é um recurso primordial para todas as instituições, de modo que a Tecnologia da Informação (TI) se tornou uma ferramenta fundamental de negócio.

As despesas com TI podem representar uma proporção significativa dos gastos de recursos financeiros e humanos de uma organização, no entanto, o retorno desse investimento pode não ocorrer devido ao uso da TI desalinhado ao contexto geral do negócio.


Atingir excelência operacional por meio da aplicação eficiente e confiável da tecnologia, manter os riscos a um nível aceitável e otimizar os custos dos serviços são alvos da governança de TI que devem ser perseguidos para o bom aproveitamento dos recursos públicos.



A reduzida maturidade da governança de TI da Secretaria de Fazenda nos tópicos analisados expõe a instituição a riscos. Em especial, aos riscos de priorização de investimentos em TI que não estejam alinhados às necessidades do negócio, ao desperdício de recursos fi-

nanceiros, ao gerenciamento ineficiente de recursos de TI, a restrições ao crescimento do negócio institucional, à indisponibilidade de serviços públicos providos com uso de TI e a falhas de segurança da informação.

Diante de tais achados, **recomendou-se à Sefaz-MT que:**



| | |
|----------|--|
| 1 | institua políticas corporativas de gestão de riscos e de continuidade de negócios; |
| 2 | defina e comunique formalmente os papéis e responsabilidades mais relevantes para a governança de TI; |
| 3 | normatize a obrigatoriedade da Sefaz-MT executar periodicamente processo de planejamento estratégico institucional e de TI; |
| 4 | realize estudo quantitativo e qualitativo de dimensionamento da força de trabalho necessário ao setor de TI e elabore plano anual de capacitação para esses servidores; |
| 5 | institua política de gestão de riscos de TI; e |
| 6 | estabeleça comitê de segurança da informação, processos de gestão de serviços e gerenciamento de projetos de TI. |

Essas recomendações visam possibilitar a identificação e o gerenciamento das ameaças atuais e futuras para o negócio; o alinhamento da TI com as necessidades do negócio; a melhoria no desempenho dos servidores e dos gestores da área de TI; a otimização dos investimentos em TI e a redução dos riscos de perda de informações sensíveis ou o furto/alterações de informações fiscais.

Sumário

| | |
|--|----|
| Resumo | 7 |
| 1. Introdução | 10 |
| 1.1 Contextualização | 10 |
| 1.2 Critérios | 10 |
| 1.3 Objetivo e escopo de auditoria | 10 |
| 2. Liderança da Alta Administração | 12 |
| 2.1 Práticas de governança corporativa não foram plenamente definidas e implementadas no âmbito da instituição | 12 |
| 2.2 Práticas de governança de TI não foram plenamente definidas e implementadas no âmbito da instituição | 13 |
| 2.3 Insuficiência de diretrizes com o objetivo de dirigir a atuação da TI com foco na entrega de resultados para a instituição | 14 |
| 2.4 Não avaliação da governança de TI pelo controle interno da Sefaz-MT | 15 |
| 3. Estratégias e Planos | 16 |
| 3.1 Deficiências no processo e no plano estratégico institucional | 16 |
| 3.2 Não formalização do processo de planejamento de TI e inexistência de plano de TI vigente | 17 |
| 4. Pessoal | 19 |
| 4.1 Ausência de diretrizes para garantir o desenvolvimento de competências e a retenção de gestores e do pessoal técnico de TI | 19 |
| 4.2 Ausência de plano de capacitação de profissionais de TI que auxilie no desenvolvimento de competências necessárias para a boa execução dos trabalhos | 20 |
| 4.3 Inexistência de avaliação do quadro de pessoal de TI | 21 |
| 5. Processos | 22 |
| 5.1 Falhas na gestão de riscos de TI | 22 |
| 5.2 Deficiências nos processos de segurança da informação | 23 |
| 5.3 Deficiências na execução de processos de gestão de serviços de TI | 24 |
| 5.4 Deficiência no gerenciamento dos projetos de TI | 26 |
| 6. Conclusão | 27 |
| 7. Proposta de Encaminhamento | 28 |

1. Introdução

1.1 Contextualização

Na modalidade operacional, a auditoria é voltada ao desempenho da instituição avaliada, com a finalidade de promover o aperfeiçoamento de suas ações governamentais. No tema governança de TI, o objetivo é avaliar a implantação dos mecanismos de governança nas atividades de tecnologia da informação de acordo com as boas práticas existentes.

A Auditoria Operacional em Governança de TI visa dar cumprimento ao Objetivo Estratégico nº 4 do Planejamento Estratégico 2016-2021 do Tribunal de Contas de Mato Grosso (TCE-MT): “contribuir para a melhoria do desempenho da Administração Pública”.

1.2 Critérios

1.2.1 Relevância

A informação é um recurso primordial para todas as instituições, sejam elas públicas ou privadas, de modo que a TI tornou-se uma ferramenta fundamental de negócio. Dessa forma, atingir excelência operacional por meio da aplicação eficiente e confiável da tecnologia, manter os riscos a um nível aceitável e otimizar os custos dos serviços de TI são alvos de governança que devem ser perseguidos para o bom aproveitamento dos investimentos em tecnologia da informação.

No âmbito da Secretaria de Fazenda, esta área deve ser tratada com especial atenção pelo fato de ser a responsável pela guarda e armazenamento de dados sensíveis dos contribuintes e por impactar diretamente nas atividades de fiscalização e arrecadação tributárias, bem como nos controles financeiros e contábeis do Estado.

1.2.2 Materialidade

A Secretaria de Fazenda tem orçamento de R\$ 562,5 milhões¹ previsto para o exercício de 2017. Desse total, R\$ 11 milhões são destinados às ações de tecnologia da informação.

Dado o volume de recursos destinado à Tecnologia da Informação, bem como a importância das atividades desenvolvidas por tal área, é de vital importância a existência de uma boa governança no sentido de otimizar os custos, entregar bons resultados e agregar valor ao negócio.

1.2.3 Risco

A Secretaria de Fazenda tem como missão institucional “garantir a realização da receita pública e o controle da aplicação do gasto público”². Grande parte dos documentos fiscais são emitidos eletronicamente e as declarações e escriturações feitas pelos contribuintes são entregues à Sefaz por meio eletrônico.

Desse modo, é essencial que a Secretaria de Fazenda mantenha uma boa governança de tecnologia da informação de forma a diminuir os riscos do negócio a um nível aceitável pela instituição.

1.3 Objetivo e escopo de auditoria

Com o intuito de avaliar o desempenho da Sefaz-MT na governança de TI, a auditoria operacional verificou a efetiva implementação de controles e processos de governança de TI, a qual deve assegurar a entrega de resultados alinhados aos objetivos e agregar valor ao negócio da instituição, de modo a gerenciar os riscos existentes.

¹ Lei Estadual nº 10.515/2017 – Lei Orçamentária Anual – LOA.

² Decreto nº 292/2015 – Regimento Interno da Sefaz-MT.

1.3.1 Questões de auditoria

A questão de auditoria, segundo o Manual de Auditoria Operacional do TCE-MT, é o elemento central na determinação do direcionamento dos trabalhos, das metodologias a adotar e dos resultados que se pretende atingir.

Nessa diretriz, a questão respondida neste trabalho foi:

A Sefaz-MT adota práticas de governança de TI de forma a auxiliar a organização na alocação de recursos (materiais, humanos e financeiros), na proteção de informações críticas e no alcance dos seus objetivos institucionais?



A fim de responder a referida questão, elaborou-se sub-questões de auditoria, as quais foram formuladas segregando o trabalho em eixos, organizados segundo o tema analisado.

O trabalho está dividido em quatro eixos. O primeiro eixo avaliado é relativo à liderança da alta administração. O segundo eixo refere-se às estratégias e planos da Sefaz-MT. O terceiro eixo é relativo à política de pessoal de TI. Por fim, o quarto eixo do trabalho refere-se aos processos de TI.

1.3.2 Critérios de auditoria

Critério de auditoria “é o padrão de desempenho usado para medir se há economicidade, eficiência, eficácia e efetividade. Serve para determinar se o objeto auditado atinge, excede ou está aquém do desempenho esperado”³.

Os critérios que embasaram a auditoria incluem dispositivos constitucionais, legais e infralegais, bem como Acórdãos do Tribunal de Contas da União (TCU) relacionados ao tema de governança e de gestão de TI.

Também foram utilizados como critérios o guia Cobit 5⁴, da *Information Systems Audit and Control Association*

(Isaca); as normas ABNT⁵ NBR ISO/IEC 12207:2009, 22301:2013, 27002:2013, 27005:2011, 31000:2009 e 38500:2009; o Referencial Básico de Governança, do TCU (versão 2.0)⁶; a Nota Técnica 7/2017, do TCU⁷; o Código das Melhores Práticas de Governança Corporativa, do Instituto Brasileiro de Governança Corporativa (IBGC)⁸; e a Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal 2015-2018⁹.

1.3.3 Metodologia

A metodologia utilizada no planejamento do trabalho consistiu no uso dos procedimentos previstos no Manual de Auditoria Operacional do TCE-MT.

1.3.4 Universo analisado

A auditoria teve por objetivo verificar a implementação e execução de controles e processos de governança de TI no âmbito da Secretaria de Estado de Fazenda. O trabalho avaliou primordialmente a atuação da alta administração e da Coordenadoria de Tecnologia da Informação (Coti).

1.3.5 Limitações

A inexistência de normatização, em um único documento ou manual, em âmbito estadual acerca da governança de TI, exceto algumas normas esparsas, constituiu limitação de auditoria. Assim, adotou-se as normas federais sobre o tema, a exemplo do Referencial Básico de Governança do TCU e da Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal 2015-2018.

3 Definição do Manual de Auditoria Operacional do TCE-MT

4 COBIT - *Control Objectives for Information and related Technology* - Um framework para governança e controle de TI, reconhecido internacionalmente.

5 Associação Brasileira de Normas Técnicas (ABNT).

6 Brasil. Tribunal de Contas da União. Referencial básico de governança aplicável a órgãos e entidades da administração pública / Tribunal de Contas da União. Versão 2 - Brasília: TCU, Secretaria de Planejamento, Governança e Gestão, 2014. 80 p.

7 Organização do sistema de governança de tecnologia da informação (TI): Nota Técnica 7/2014 Sefti/TCU / Tribunal de Contas da União. – Brasília: TCU, Secretaria de Fiscalização de Tecnologia da Informação, 2015.

8 Instituto Brasileiro de Governança Corporativa. Código das melhores práticas de governança corporativa. 5.ed. / Instituto Brasileiro de Governança Corporativa. - São Paulo, SP: IBGC, 2015. 108p.

9 Brasil. Presidência da República. Gabinete de Segurança Institucional. Estratégia de segurança da informação e comunicações e de segurança cibernética da Administração Pública federal 2015 - 2018: versão 1.0 / Gabinete de Segurança Institucional, Secretaria-Executiva, Departamento de Segurança da Informação e Comunicações. Brasília: Presidência da República, 2015. 82 p.: il.

2. Liderança da Alta Administração

2.1 Práticas de governança corporativa não foram plenamente definidas e implementadas no âmbito da instituição

Em decorrência da inércia da alta administração, da baixa sensibilização e compreensão sobre a importância da governança corporativa para os resultados organizacionais e da alta rotatividade de secretários, as práticas de governança corporativa não foram plenamente definidas e implementadas no âmbito da instituição, resultando no risco da estrutura estabelecida ser ineficaz; com falhas na avaliação, direcionamento e monitoramento da atuação da gestão, principalmente no que diz respeito ao gerenciamento de riscos estratégicos e ameaças atuais e futuras para a continuidade do negócio.

De acordo com o Código das Melhores Práticas de Governança Corporativa, do Instituto Brasileiro de Governança Corporativa (IBGC)¹⁰:

Governança corporativa é o sistema pelo qual as empresas e demais organizações são dirigidas, monitoradas e incentivadas, envolvendo os relacionamentos entre sócios, conselho de administração, diretoria, órgãos de fiscalização e controle e demais partes interessadas.

Sob essas perspectivas, em avaliação à estrutura de governança corporativa da Sefaz-MT, identificou-se que:

- a. a organização define e comunica formalmente papéis e responsabilidades para a governança corporativa, contudo não a avalia.
- b. não há políticas de gestão de riscos e de gestão de continuidade do negócio formalmente instituídas.

Foi detectado que essas deficiências de governança corporativa são decorrentes da inércia da alta administração em responsabilizar-se e tomar a iniciativa de estabelecer as práticas acima identificadas, da baixa sensibilização e compreensão da alta administração sobre a importância da governança corporativa para os resultados organizacionais e da alta rotatividade de secretários.

Esse cenário expõe a Sefaz-MT ao risco de manter uma estrutura de governança corporativa ineficaz (formal, porém inoperante); com falhas na avaliação, direcionamento e monitoramento da atuação da gestão, principalmente no que diz respeito ao gerenciamento de riscos estratégicos e ameaças atuais e futuras para a continuidade do negócio.

¹⁰ Instituto Brasileiro de Governança Corporativa. Código das melhores práticas de governança corporativa. 5.ed. / Instituto Brasileiro de Governança Corporativa. - São Paulo, SP: IBGC, 2015. 108p. (Pág.20)

2.2 Práticas de governança de TI não foram plenamente definidas e implementadas no âmbito da instituição

Em decorrência da inércia da alta administração, da baixa sensibilização e compreensão sobre a importância da governança de TI para os resultados organizacionais e da alta rotatividade de secretários, as práticas de governança de tecnologia da informação não foram plenamente definidas e implementadas no âmbito da instituição, resultando no risco da estrutura de TI não servir às necessidades do negócio institucional, ocasionando restrições ao crescimento do negócio e gerenciamento ineficiente de recursos.

De acordo com a norma ABNT NBR ISO 38500:2009¹¹, governança de TI é:

O sistema pelo qual o uso atual e futuro da TI é dirigido e controlado. Significa avaliar e direcionar o uso da TI para dar suporte à organização e monitorar seu uso para realizar os planos. Inclui a estratégia e as políticas de uso da TI dentro da organização.

Neste tópico, foi avaliado o nível de implantação das práticas de governança de TI pela Sefaz-MT. Nesse contexto, foi identificado que:

- a. a organização não define e nem comunica formalmente papéis e responsabilidades mais relevantes para a governança de TI;
- b. a organização não dispõe de um comitê de TI formalmente instituído, composto por representantes de áreas relevantes da organização;
- c. há deficiências na priorização das ações de TI com apoio do comitê de TI (ou colegiado equivalente).

Como causas para essas deficiências de governança de TI, foram identificadas a inércia da alta administração em responsabilizar-se e tomar a iniciativa de estabelecer as práticas acima identificadas; a alta rotatividade de secretários; e a baixa sensibilização e compreensão da alta administração sobre a importância da governança de TI para os resultados organizacionais.

É importante destacar, conforme apontado pelo TCU no Acórdão 3.051/2014-TCU-Plenário, que possíveis consequências da falha de governança de TI são:

- a. sistemas de informação não efetivos, ineficientes ou não amigáveis;
- b. TI não servindo às necessidades de negócio institucionais;
- c. restrições ao crescimento do negócio institucional;
- d. gerenciamento ineficiente de recursos;
- e. tomada de decisão inadequada;
- f. fracasso de projetos;
- g. dependência de fornecedores;
- h. falta de transparência e prestação de contas;
- i. exposição a riscos de segurança da informação.

11 Associação Brasileira de Normas Técnicas. ABNT NBR ISO 38500:2009.

2.3 Insuficiência de diretrizes com o objetivo de dirigir a atuação da TI com foco na entrega de resultados para a instituição

Em decorrência da inércia da alta administração em estabelecer as práticas de sua responsabilidade e da baixa sensibilização e compreensão sobre a importância da governança de TI para os resultados organizacionais, não há diretrizes formalizadas suficientes com o objetivo de dirigir a atuação da TI com foco na entrega de resultados para a instituição, acarretando, dessa forma, nos riscos de: não cumprimento das obrigações legais, regulamentares e éticas com relação ao uso da TI; não alinhamento da TI com os objetivos do negócio; e não alcance dos benefícios esperados dos investimentos em TI.

Neste tópico foi avaliado se a organização define formalmente diretrizes para:

- a. o planejamento de TI;
- b. a gestão do portfólio de projetos e serviços de TI;
- c. a contratação de bens e serviços de TI;
- d. a avaliação de desempenho dos serviços de TI; e
- e. a comunicação com as partes interessadas.

Das diretrizes avaliadas, a organização possui somente a diretriz para a contratação de bens e serviços de TI, evidenciada pelo documento “Sistemática para as aquisições de bens e serviços de tecnologia da informação e comunicação no âmbito do Poder Executivo do Estado de Mato Grosso”.

Com relação as demais diretrizes os documentos apresentados não atendem o solicitado, visto que o Plano Setorial de Tecnologia da Informação (PSTI) não pode ser considerado como um planejamento estratégico de TI ou planejamento diretor de TI, pois não contempla os requisitos necessários.

Sobre a definição formal de diretrizes para gestão do portfólio de projetos e serviços de TI, inclusive para definição de critérios de priorização e de alocação orçamentária, em questionário eletrônico a Sefaz-MT informou que “adota parcialmente” a prática e apresentou as Portarias 33/2014¹² e 75/2007¹³ para comprová-la.

Em análise às normas apresentadas, verificou-se que

elas não atendem a questão, visto que não são específicas ao tema e não contemplam todos os requisitos necessários para direcionar a gestão do portfólio de projetos e serviços de TI, contemplando a matéria de forma parcial (superficial).

Quanto à definição formal de diretrizes para avaliação do desempenho dos serviços de TI, a Sefaz-MT informou em questionário eletrônico que “iniciou plano para adotar” a prática, contudo, posteriormente retificou a informação informando não possuir documento que comprovasse a prática. Corroborando nesse sentido, o Parecer CGE 003/2016¹⁴ informou que a Sefaz-MT não possui essas diretrizes.

No que se refere à definição formal de diretrizes para comunicação com as partes interessadas (público interno e externo) sobre os resultados da gestão e do uso de TI, contemplando o meio de divulgação, o conteúdo, a frequência e o formato das comunicações, a Sefaz-MT informou em questionário eletrônico que “não adota” a prática.

Percebe-se que essa inércia da alta administração em formalizar diretrizes com o objetivo de dirigir a atuação da TI com foco na entrega de resultados, aliada à baixa sensibilização e compreensão sobre a importância da governança de TI para os resultados organizacionais, expõe a instituição a riscos. Em especial, tem-se os riscos de não cumprimento das obrigações legais, regulamentares e éticas com relação ao uso da TI; de não alinhamento da TI com os objetivos do negócio; e de não alcance dos benefícios esperados dos investimentos em TI.

¹² Portaria nº 033/2014 – SEFAZ. Institui os critérios relativos à política de informatização de negócios setoriais fazendários e dá outras providências.

¹³ Portaria nº 075/2007 – SARP/SEFAZ. Dispõe sobre política de fiscalização, cruzamento de dados, indução ao cumprimento voluntário, recuperação de débitos, simplificação, planos especiais e dá outras providências.

¹⁴ Mato Grosso. Controladoria Geral do Estado. Parecer Técnico Conclusivo do Controle Interno nº 003/2016. Prestação de Contas Anual: Secretaria de Estado de Fazenda – Exercício 2015.

2.4 Não avaliação da governança de TI pelo controle interno da Sefaz-MT

Em decorrência da falta de pessoal capacitado para realizar avaliações em governança de TI, da não previsão dessas avaliações no plano anual de acompanhamento e controles internos e da baixa sensibilização da alta administração acerca da importância dessa atividade, não são realizadas avaliações na governança de TI pelo controle interno da Sefaz-MT, ocasionando riscos de não conhecimento dos processos de governança de TI na instituição, de não aderência da governança de TI aos planos estratégicos existentes e de não contribuição do controle interno para a melhoria do desempenho organizacional.

Os controles internos devem ser implantados com a finalidade de diminuir os riscos existentes a um nível aceitável pela organização, levando-se em consideração a relevância do processo a ser controlado e os custos dos controles.

No âmbito da Sefaz-MT, existe uma Unidade Setorial de Controle Interno (Uniseci) que possui dentre suas atribuições regimentais¹⁵ “elaborar o plano anual de acompanhamento e controles internos” e “verificar a conformidade dos procedimentos relativos aos processos dos subsistemas planejamento e orçamento, financeiro, contábil, patrimônio e serviços, aquisições, gestão de pessoas, arquivo, protocolo e outros relativos a atividades de apoio e serviços comuns a todos os órgãos e entidades da Administração”.

Entretanto, foi identificado que não são realizadas avaliações na governança de TI da Sefaz-MT. Tal constatação é evidenciada pela resposta da Sefaz-MT ao questionário eletrônico aplicado, afirmando não adotar a prática.

Com relação à avaliação dos riscos considerados críticos para o negócio e da eficácia dos respectivos controles, inicialmente a Sefaz-MT respondeu no questionário que havia iniciado plano para adotar a prática. No entanto, no e-mail encaminhado em 20/07/17 houve retificação da resposta para “não adota” a prática.

Como causas para a não realização de avaliações na governança de TI

da Sefaz-MT, pode-se apontar a ausência de pessoal capacitado para realizar avaliações em governança de TI, a não previsão no plano de auditoria interna de avaliação da governança de TI e a baixa sensibilização e compreensão da alta administração acerca da importância da realização de avaliações na governança de TI.

Tais fatos expõem a Sefaz-MT a riscos, tais como, a não contribuição do controle interno para a melhoria do desempenho organizacional, o risco de não aderência da governança de TI aos planos existentes, o não conhecimento da maturidade dos processos de governança de TI na instituição, o risco de inadequação dos processos de TI em relação às políticas da instituição e o risco de imaturidade da governança na área de TI, sem controles e indicadores que possam apontar os problemas e oportunidades de negócio para a organização.



15 Regimento Interno da Sefaz, art. 21, I e II.

3. Estratégias e Planos

3.1 Deficiências no processo e no plano estratégico institucional

Em decorrência de falhas na governança corporativa, há deficiências no processo e no plano estratégico institucional. Essas deficiências resultam na impossibilidade dos gestores demonstrarem que atendem ao princípio constitucional da eficiência; na impossibilidade de se alinhar o uso da TI ao negócio; na inaptidão da organização para agir com iniciativa, de forma proativa, contra as ameaças e a favor das oportunidades identificadas nas constantes mudanças que ocorrem no ambiente que atua; e na dificuldade no estabelecimento de diretrizes para a área de TI.

Sob esta análise restou evidenciado que:

- **Quanto ao processo:** o processo de planejamento estratégico institucional não está formalmente instituído como norma de cumprimento obrigatório.
- **Quanto ao produto:** O plano estratégico institucional vigente não contém metas associadas aos indicadores de resultado, bem como não estabelece as ações (atividades e projetos) consideradas necessárias para o alcance das metas fixadas. Cabe ressaltar, ainda, que a execução do plano estratégico institucional vigente não é acompanhada periodicamente quanto ao alcance das metas estabelecidas, para correção de desvios.

Com relação à instituição formal do processo de planejamento estratégico como norma de cumprimento obrigatório, foi respondido em questionário eletrônico que a Sefaz-MT “iniciou plano para adotar” a prática. Entretanto, quando solicitado documentos que evidenciassem a atividade, foi apresentada a Portaria nº 219/GSF/SEFAZ/2014 que homologa o Plano Estratégico da Sefaz/MT para o período de 2015 a 2030, não atendendo à questão.

Sobre a existência de metas associadas aos indicadores de resultado do plano vigente e de ações (atividades e

projetos) consideradas necessárias para o alcance das metas fixadas, foi identificado que o Plano Estratégico da Sefaz-MT para o período de 2015 a 2030 não contém esse desdobramento. No Parecer nº 003/2016, a CGE¹⁶ evidencia essa deficiência. Em questionário eletrônico a Sefaz-MT respondeu que “iniciou plano para a adotar” a prática e apresentou a publicação no Diário Oficial de Manifestação de Interesse para seleção e contratação de serviços de consultoria para implantar modelo de gestão por resultado na Sefaz-MT.

Com relação ao acompanhamento periódico da execução do plano estratégico institucional quanto ao alcance das metas estabelecidas, para correção de desvios, a Sefaz-MT informou em questionário eletrônico que “não adota” a prática.

Essas falhas de governança corporativa no tocante a não formalização do processo de planejamento estratégico institucional e à ausência de iniciativa para desdobramento do plano, resultam na impossibilidade de os gestores demonstrarem que atendem ao princípio cons-

16 Mato Grosso. Controladoria Geral do Estado. Parecer Técnico Conclusivo do Controle Interno nº 003/2016. Prestação de Contas Anual: Secretaria de Estado de Fazenda – Exercício 2015

titucional da eficiência, uma vez que não se pode avaliar sua gestão por meio de parâmetros objetivos de comparação entre o planejado e o executado.

De igual modo, há a impossibilidade de se alinhar o uso da TI ao negócio, para que esta contribua para o alcance dos objetivos organizacionais, já que esses objeti-

vos não são explicitados ou mensuráveis objetivamente; na inaptidão da organização para agir com iniciativa, de forma proativa, contra as ameaças e a favor das oportunidades identificadas nas constantes mudanças que ocorrem no ambiente que atua; e na dificuldade no estabelecimento de diretrizes para a área de TI.

3.2 Não formalização do processo de planejamento de TI e inexistência de plano de TI vigente

Devido a falhas na governança de Tecnologia da Informação, o processo de planejamento de TI não está formalmente instituído como norma de cumprimento obrigatório na Sefaz-MT e não há plano de TI vigente formalmente instituído pelo dirigente máximo da organização. Esse cenário expõe o órgão a riscos de suporte ineficaz da área de TI na consecução da missão da organização; alocação indevida e desperdício de recursos; decisões dos gestores de TI incompatíveis com as necessidades da organização; enfraquecimento das ações de TI; descontinuidade de projetos; insatisfação de usuários e servidores; e resultados da área de TI abaixo do esperado.

Este tópico avaliou como a Sefaz-MT organiza suas estratégias de longo prazo para que a tecnologia da informação apoie o negócio.

Conforme destaca o livro “Implantando a governança de TI: da estratégia à gestão dos processos e serviços”¹⁷:

O processo de alinhamento estratégico revelará requisitos do negócio para TI, os quais vão alimentar o estudo da demanda por serviços, recursos e infraestrutura, sendo transformados em objetivos de desempenho e acordos de níveis de serviço para clientes externos e internos, em necessidades de novas soluções, de infraestrutura de TI e de outros recursos e serviços de TI.

O Plano de TI é o principal produto dessa fase de alinhamento estratégico e, para este trabalho, considerou-se apto tanto o Plano Estratégico de TI (Peti) quanto o Plano Diretor de TI (PDTI).

Cabe registrar que o plano estratégico de TI tratado nesse item não é um documento do setor de TI da orga-

nização, mas um documento da organização, dado que formaliza a alocação de recursos (financeiros, humanos e materiais) para que a TI atenda às demandas do negócio.

Sob essa perspectiva foi analisado e detectado que:

- **Quanto ao processo:** o processo de planejamento de TI não está formalmente instituído como norma de cumprimento obrigatório e a organização não o executa periodicamente.
- **Quanto ao produto:** a organização não possui plano de TI vigente, formalmente instituído pelo seu dirigente máximo.

Sobre o processo de planejamento de TI estar formalmente instituído como norma de cumprimento obrigatório, a Sefaz-MT respondeu inicialmente em questionário eletrônico que “adota parcialmente” a prática. É importante destacar que neste caso não há como se adotar parcialmente a prática, visto que ou existe a norma formalmente instituída ou não. Para este tópico foi apresentado como documentação o Decreto nº 1.751/2013¹⁸, que estabelece normas

¹⁷ Fernandes, A. A.; Abreu, V. F. Implantando a Governança de TI - 4ª Ed.: Da estratégia à Gestão de Processos e Serviços. Brasport, 2014. Rio de Janeiro - RJ.

¹⁸ Decreto 1.751, de 29 de abril de 2013. Estabelece normas e procedimentos a serem observados para as aquisições de produtos e contratações de serviços de Tecnologia da Informação e Comunicação (TIC) no âmbito do Poder Executivo Estadual.

e procedimentos a serem observados para as aquisições de produtos e contratações de serviços de tecnologia da informação e comunicação no âmbito do Poder Executivo Estadual, portanto não atende a questão.

Quanto à execução periódica de processo de planejamento de TI, a Sefaz-MT informou inicialmente em questionário eletrônico que “adota parcialmente a prática”, porém na análise documental foi identificado que ela “iniciou plano para adotar” a prática, visto que foi apresentado o Termo de Referência nº 75/2017, que define os critérios e parâmetros que servirão de base e referência para a contratação de Empresa Especializada em Serviços de Consultoria para a elaboração, planejamento de implantação e avaliação do seu Plano Diretor de Tecnologia da Informação.

Em relação à organização possuir plano de TI vigente formalmente instituído pelo seu dirigente máximo, a Sefaz-MT informou por meio do questionário eletrônico não adotar a prática.

Identifica-se como causa dessas deficiências de planejamento de TI a falha de governança de TI em estabelecer

normas que dirijam a atuação da gestão. Essa falha implica em riscos de:

- a. suporte ineficaz da área de TI na consecução da missão da organização;
- b. decisões dos gestores de TI incompatíveis com as necessidades da organização;
- c. alocação indevida de recursos de TI por falta de entendimento sobre as prioridades da organização;
- d. desperdício de recursos devido a decisões erradas acerca da alocação de recursos de TI;
- e. enfraquecimento das ações de TI;
- f. descontinuidade dos projetos de TI;
- g. insatisfação dos usuários;
- h. insatisfação da equipe de TI por não haver clareza quanto às metas e objetivos da organização;
- i. visão negativa da área de TI;
- j. resultados da área de TI abaixo do esperado; e
- k. dificuldade de obtenção de recursos para a área de TI.



4. Pessoal

4.1 Ausência de diretrizes para garantir o desenvolvimento de competências e a retenção de gestores e do pessoal técnico de TI

Em decorrência da inércia da alta administração em estabelecer plenamente mecanismos de governança corporativa, da baixa sensibilização e compreensão acerca da importância do desenvolvimento de competências e da não identificação das competências necessárias para o pessoal de TI, não há definição formal de diretrizes para garantir o desenvolvimento de competências e a retenção de gestores e do pessoal técnico de TI, ocasionando prejuízos à atuação da Sefaz-MT nessa atribuição, de modo a trazer dificuldades para a retenção dos gestores.

No âmbito da Secretaria de Fazenda, cabe ao titular da Sefaz-MT regulamentar internamente a política de desenvolvimento de competências para os servidores da instituição.

Sob essa perspectiva, identificou-se uma atuação deficiente da alta administração da Sefaz-MT quanto à direção do desenvolvimento de competências do pessoal de TI.

Quanto à definição formal de diretrizes para garantir o desenvolvimento de competências e a retenção de gestores e do pessoal técnico de TI, a Sefaz-MT informou, em resposta ao questionário eletrônico, respectivamente, que “adota parcialmente” a prática (quanto aos gestores de TI) e que “iniciou plano para adotar” (quanto ao pessoal técnico de TI).

Quando solicitada documentação que comprovasse as respostas, a Sefaz-MT enviou um contrato de prestação de serviços de consultoria especializada¹⁹ para “implantar um modelo de gestão de pessoas com foco em competências para o órgão, com fornecimento de *software* e banco de dados, que possibilite o gerenciamento e operacionalização das respectivas rotinas, com desenvolvimento e implantação de um Modelo de Planejamento

e Dimensionamento da Força de Trabalho” e a Portaria nº 218/2015-Sefaz²⁰, que constituiu a Comissão Técnica de Coordenação e Implementação do Plano de Trabalho decorrente do contrato citado.

A consultoria contratada teve como abrangência as unidades priorizadas da Secretaria Adjunta da Receita Pública (Sarp) e, posteriormente, o modelo desenvolvido seria replicado para as demais unidades da Sefaz-MT pela Comissão instituída pela Portaria nº 218/2015-Sefaz.

Diante disso, não obstante ter respondido adotar parcialmente o quesito quanto à definição formal de diretrizes para garantir o desenvolvimento de competências de gestores de TI, verificou-se que a Sefaz-MT ainda está em fase inicial de implantação de um modelo de gestão por competências, seja de gestores, seja do pessoal técnico. Dessa forma, demonstra-se que a documentação enviada é insuficiente para comprovar a adoção parcial do quesito.

¹⁹ Contrato nº 003/2015/SAAF/SEFAZ/PROFISCO.

²⁰ Portaria nº 0218/2015-SEFAZ, que constitui, no âmbito da Secretaria de Estado de Fazenda, a Comissão Técnica de Coordenação e Implementação do Plano de Trabalho decorrente do contrato para prestação de serviços de consultoria para implementar um Modelo de Gestão de Pessoas com foco em Competências, com desenvolvimento e implantação de um Modelo de Planejamento e Dimensionamento da Força de Trabalho, nas condições que especifica, conforme produto constante do Profisco-MT.

Como causas para essa atuação deficiente da Sefaz-MT, pode-se apontar a inércia da alta administração em estabelecer plenamente os mecanismos de governança corporativa e a baixa sensibilização e compreensão acerca da

importância do desenvolvimento de competências.

Tal cenário expõe a Sefaz-MT ao risco de prejuízos ao desenvolvimento de competência e a dificuldade na retenção dos gestores e do pessoal técnico de TI.

4.2 Ausência de plano de capacitação de profissionais de TI que auxilie no desenvolvimento de competências necessárias para a boa execução dos trabalhos.

Em decorrência da inércia da gestão em elaborar plano de capacitação para os servidores de TI, não há formalização de tal documento que auxilie no desenvolvimento das competências necessárias para a boa execução dos trabalhos, inviabilizando a obtenção de recursos para a execução de capacitações, dificultando a atualização dos servidores e desmotivando-os.

Uma vez que o incentivo e a promoção de oportunidades para a capacitação profissional dos servidores são incumbência dos órgãos e entidades estaduais, há que se elaborar um planejamento para as capacitações necessárias.

Nesse diapasão, buscou-se avaliar, no tocante à gestão de pessoal de TI da Sefaz-MT, a definição das competências necessárias ao pessoal de TI, bem como a execução de plano de capacitação dos servidores.

Quanto à definição de competências, conforme tratado no tópico 4.1, a Sefaz-MT contratou uma consultoria especializada para elaborar um modelo de gestão de pessoas com foco em competências, o qual abrangerá o desenvolvimento e implantação de um modelo de planejamento e dimensionamento da força de trabalho. Esse modelo, após desenvolvido, seria replicado aos demais setores da Sefaz-MT, incluindo a Coordenação de Tecnologia da Informação (Coti).

Quanto à capacitação dos servidores, em resposta ao questionário eletrônico, a Sefaz-MT informou que “adota parcialmente”:

- a definição de critérios para avaliação e atendimento aos pedidos de capacitação;
- a elaboração periódica de plano de capacitação para suprir as necessidades de desenvolvimento de competências de TI;
- a avaliação da execução do plano de capacitação e a verificação quanto ao alcance dos objetivos e resultados esperados.

Quanto ao item relativo ao acompanhamento da execução do plano de capacitação, com identificação e correção de desvios, a Sefaz-MT respondeu ter iniciado plano para adotar.

No entanto, quando solicitado documento que evidenciasse a adoção parcial ou o início de plano para adotar as práticas acima identificadas, a Sefaz-MT retificou sua resposta, informando que não possui tais documentos.

Como causas para a ausência do plano de capacitação para os profissionais de TI, identificou-se a inércia da gestão em elaborar o plano e a ausência de definição das competências necessárias ao pessoal de TI, para, com isso, identificar as capacitações efetivamente necessárias.

Tal cenário expõe a Coordenação de Tecnologia da Informação aos riscos de não obtenção dos recursos para execução das capacitações, de dificuldade na atualização dos servidores quanto às boas práticas na execução dos trabalhos e sua desmotivação.



4.3 Inexistência de avaliação do quadro de pessoal de TI

Em decorrência da inércia da alta administração em determinar a realização de dimensionamento da força de trabalho necessária para a área de Tecnologia da Informação, inexistente uma avaliação do quadro de pessoal de TI da Sefaz-MT, o que resulta na impossibilidade de dimensionamento do quantitativo ideal da força de trabalho e nos riscos de alocação inadequada de servidores de TI, de contratação de terceirizados em quantidade inadequada e de comprometimento da produtividade dos servidores de TI.

A gestão de pessoas é atividade essencial em qualquer organização para o alcance dos objetivos institucionais. A falta de dimensionamento da necessidade de pessoal influencia na qualidade da prestação dos compromissos assumidos e na eficiência dos gastos públicos, tanto na subestimação quanto na superestimação do quantitativo necessário.

A Sefaz-MT, em resposta ao questionário eletrônico aplicado, informou não haver estudo de dimensionamento de pessoal de TI, bem como estar o modelo de alocação de

pessoal sob revisão. Como causa dessa situação, aponta-se a inércia da alta administração em providenciar a realização de tal estudo, seja diretamente ou via contratação de consultoria especializada.

Tal situação expõe a Sefaz-MT a riscos como:

- a. alocação inadequada dos servidores de TI;
- b. contratação de terceirizados de TI em quantitativo inadequado; e
- c. comprometimento da produtividade dos servidores.



5. Processos

5.1 Falhas na gestão de riscos de TI

Diante da ausência de política de gestão de riscos corporativos, da não sensibilização da alta administração acerca da importância do tema para a organização e da inércia da alta administração em dirigir a gestão de riscos de TI, foram evidenciadas falhas na gestão de riscos de TI na Sefaz-MT. Essa deficiência pode impactar em prejuízos aos ativos de informação da organização; em interrupção dos serviços e prejuízos à avaliação e à resposta aos riscos de TI; e no desalinhamento da gestão de riscos de TI com a gestão de riscos da organização.

O TCU²¹ esclarece que, de acordo com o Cobit 5,

a gestão de riscos, no âmbito da tecnologia da informação, é considerada um dos pilares da criação de valor por parte da TI, juntamente com a entrega de benefícios e com a otimização do uso de recursos.

Em resposta ao questionário eletrônico, a Sefaz-MT informou que “iniciou plano para adotar” a definição formal das diretrizes e de papéis e responsabilidades para a gestão de riscos de TI, a execução de processo de gestão de riscos de TI e a formalização como norma de cumprimento obrigatório do processo de gestão de riscos de TI.

No entanto, quando solicitado documento que evidenciasse essas afirmações, foi informado, no caso da definição formal das diretrizes, que inexistia tal documento e, no caso da definição de papéis e responsabilidades, que a Sefaz-MT não adota a prática.

Já quanto aos questionamentos sobre a execução do processo de gestão de riscos de TI e se o processo está formalmente instituído como norma de cumprimento obrigatório, o documento apresentado²² não traz nenhu-

ma referência ao início de formalização nem da prática de execução de processo de gestão de riscos nos processos críticos. No documento há somente um processo com seus riscos avaliados. Pelo exposto, concluiu-se que a Sefaz-MT não adota tais práticas.

Pelas mesmas razões, concluiu-se que não são adotadas as práticas de identificação, avaliação e tratamento aos riscos de TI dos processos críticos de negócio, as quais constam no questionário como “adotada parcialmente”.

No tocante à definição dos níveis de risco de TI aceitáveis pela organização na consecução dos seus objetivos e a tomada de decisões estratégicas considerando os níveis de risco de TI definidos, a Sefaz-MT respondeu “não adotar” as práticas.

A falta de política estabelecendo diretrizes para a gestão de riscos corporativos acaba por inviabilizar o estabelecimento de política de gestão de riscos de TI, tendo em vista que não há sequer como conceber quais são os níveis de riscos aceitáveis pela organização (apetite ao risco).

Essa falta de definição do apetite ao risco da organização impacta negativamente no planejamento, eleva a possibilidade de respostas ineficazes aos riscos e pode gerar prejuízos aos ativos de informação da organização.

²¹ Acórdão 3.051/2014-TCU-Plenário, pág. 36.

²² Relatório de Análise de Risco - Acessos a informações fazendárias. Versão 1.0.

5.2 Deficiências nos processos de segurança da informação

Diante da não sensibilização da alta administração acerca da importância do tema para a organização, de falhas de governança de TI na implementação de processos específicos de segurança da informação e da ausência de responsáveis, formalmente instituídos, por esses processos, constatou-se que há deficiências nos processos de segurança da informação na Sefaz-MT. Tais falhas podem ocasionar problemas na avaliação das políticas de segurança da informação e no risco de acesso indevido, alteração ou perda de informações fiscais.

A informação é um ativo primordial para qualquer organização. A Sefaz-MT tem como dever funcional a guarda de informações fiscais resguardadas por sigilo. Alterações ou perdas dessas informações podem causar prejuízos na arrecadação, gerando obstáculos à implementação de políticas públicas.

Quanto à existência de uma política de segurança da informação formalmente instituída como norma de cumprimento obrigatório e de uma política de controle de acesso à informação, a Sefaz-MT afirmou, em questionário eletrônico, que “adota integralmente” as práticas.

Entretanto, após analisar os documentos solicitados por *e-mail* para comprovar as respostas ao questionário (resposta por *e-mail* datado de 28/07/2017), observou-se que as políticas apresentadas eram normas gerais estaduais (Resoluções 03/2010, 08/2010, 09/2011 e 011/2011 do Conselho Superior do Sistema Estadual de Informação e Tecnologia da Informação).

A única norma elaborada pela Sefaz-MT foi a Portaria nº 128/2005 que estabelece normas de segurança a serem observadas para liberação de acesso aos sistemas informatizados. No entanto, é específica para a Secretaria Adjunta da Receita Pública (Sarp), não alcançando todos os setores da organização. Pelo exposto, concluiu-se que a Sefaz-MT “não adota” os tópicos analisados.

Quanto às outras perguntas do questionário eletrônico, a Sefaz-MT respondeu que “não adota” Comitê de Segurança da Informação, não há gestor de segurança da informação formalmente instituído e inexistente política de cópias de segurança (*backup*).

O Comitê de Segurança da Informação e Comunicações constitui-se de um grupo de pessoas com a responsabilidade de assessorar a implementação das ações de segurança da informação e comunicações no âmbito do órgão ou entidade²³. Tem o papel de auxiliar na implementação das ações de segurança da informação e comunicações além de propor soluções específicas e normas internas.

Por sua vez, o Gestor de Segurança da Informação e Comunicações é responsável pelas ações de segurança da informação e comunicações no âmbito do órgão ou entidade²⁴. Dentre suas responsabilidades estão: promoção da cultura de segurança da informação e comunicações, acompanhamento das investigações e das avaliações dos danos

23 Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. Gestão de Continuidade de Negócios em Segurança da Informação e Comunicações. Norma Complementar 06/IN01/DSIC/GSI/PR, pág. 2.

24 Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. Gestão de Continuidade de Negócios em Segurança da Informação e Comunicações. Norma Complementar 06/IN01/DSIC/GSI/PR, pág. 2.

decorrentes de quebras de segurança e a proposição dos recursos necessários às ações de segurança da informação e comunicações.

A falta dessas figuras pode ocasionar problemas na avaliação e execução das políticas de segurança da informação, além de não haver responsável por exigir a execução conforme a política estabelecida pela organização.

A falta de política de *backup* traz aumento do risco de perda de informação sensível ao negócio da organização. Segundo informações repassadas por meio do questionário eletrônico, ratificadas no Parecer nº 003/2016 da CGE-MT²⁵, a Sefaz-MT não possui política de *backup*. Pois, só há replicação do ambiente de banco de dados na estrutura do Cepromat, atual Empresa Mato-Grossense de Tecnologia da Informação (MTI).



5.3 Deficiências na execução de processos de gestão de serviços de TI

Devido a não formalização da política de gestão de continuidade de negócio; da não sensibilização da alta administração acerca da importância para a organização da gestão de continuidade de serviços de TI e de falhas na governança de TI na implementação de processos específicos para gestão de serviços de TI, constatou-se que há deficiências na execução de processos de gestão de serviços de TI na Sefaz-MT, especificamente na gestão de continuidade, de mudança e de incidentes. Tais deficiências podem ocasionar perda de informação fiscais e interrupção dos serviços prestados pela Sefaz-MT.

Os processos de gestão de serviços de TI estão diretamente relacionados à gestão de riscos e aos processos de segurança da informação, influenciando na manutenção das atividades da organização. O uso das melhores práticas de governança de TI direciona os esforços para o alinhamento dos processos com a necessidade da organização, gerando valor.

Em relação ao processo de gerenciamento da continuidade dos serviços de TI, a Sefaz-MT afirmou, por meio de questionário eletrônico, que este não está formalmente instituído como norma de cumprimento obrigatório. Afir-
mou, ainda, que “iniciou plano para adotar” a prática de gerenciamento de continuidade de serviços de TI em seus processos.

O gerenciamento de continuidade dos serviços de TI é consequência do gerenciamento da continuidade do negócio (conforme já analisado no tópico 2.1) e tem como objetivo recuperar os serviços de TI dentro de um tempo determinado²⁶.

Em análise aos documentos encaminhados²⁷ para comprovar as respostas ao questionário, verificou-se que inexistiu iniciativa de implantação (prazos, criação de comissão ou outra iniciativa que demonstre que está em curso a implementação do processo de continuidade dos serviços de TI). Pelo exposto, concluiu-se que não é adotado o processo em análise.

²⁵ Parecer Técnico Conclusivo do Controle Interno nº 0003/2016 – Prestação de Contas Anual: Secretaria de Estado de Fazenda, Exercício 2015 – Fev/2016.

²⁶ Definição retirada do livro Implantando a Governança de TI: da Estratégia à Gestão dos Processos e Serviços, 4ª ed. 2014.

²⁷ Reestruturação do projeto GT-Serviços e GTT Serviços – Apresentação.

É importante destacar que o gerenciamento de continuidade é de extrema importância para uma organização como a Sefaz-MT, pois reduz o risco de que haja interrupção dos serviços prestados à população acima do período acordado com os responsáveis pela manutenção dos serviços de TI. Serviços importantes, como emissão de certidão negativa débitos e emissão de documentos de arrecadação podem ficar inacessíveis, gerando queda de arrecadação para o Estado e prejuízos à população.

Outra falha evidenciada neste tópico foi relativa ao gerenciamento de mudanças. No questionário eletrônico, as respostas dadas foram de que a Sefaz-MT “iniciou plano para adotar” a formalização da norma pertinente e a execução do processo de gerenciamento de mudanças. Contudo, após análise dos documentos enviados e pelas mesmas razões apontadas no tópico sobre a continuidade dos serviços de TI, concluiu-se que não é adotada a execução do processo e que nem mesmo foi iniciado o processo de formalização da norma.

O Gerenciamento de Mudanças visa assegurar o tratamento sistemático e padronizado de todas as mudanças ocorridas no ambiente operacional, minimizando assim os impactos decorrentes de incidentes/problemas relacionados. Como consequência, promove melhorias na rotina operacional da organização²⁸.

Esse processo é necessário a todo tipo de organização que utiliza sistemas informatizados, seja por questões de aperfeiçoamento ou por necessidade de mudança do *software* utilizado em que algum momento será necessário realizar algum tipo de transição.

Dados fiscais como os de responsabilidade da Sefaz-MT precisam de um tratamento baseado nas melhores práticas, a fim de evitar perdas de informações que possam gerar prejuízos ao erário. No intuito de demonstrar a importância do gerenciamento de mudanças, destaca-se a falha na migração dos dados do sistema Conta Corrente (versão 2.6) para a versão 3.0, conforme identificado no Relatório de Levantamento da Receita Pública Estadual (2013 a 2016) de junho de 2016.

Alguns débitos não foram encontrados na nova versão e a Sefaz também informou, à época, que não realizava controle desses valores, visto que não havia, até então, informação da área de tecnologia da informa-



ção acerca da falta de dados na nova plataforma. Os processos de governança de TI relativos ao gerenciamento de mudanças poderiam ter mitigado os riscos de ter ocorrido tal perda de informação.

Por fim, há falha quanto ao processo de gerenciamento de incidentes. No questionário eletrônico, a Sefaz-MT informou que “adota integralmente” a execução do processo gestão de incidentes. Com relação à formalização do processo como norma de cumprimento obrigatório, relatou que “adota parcialmente” a prática.

O Gerenciamento de Incidentes visa restaurar a operação normal de um serviço no menor tempo possível, de forma a minimizar os impactos adversos para o negócio, garantindo que os níveis de qualidade e disponibilidade sejam mantidos dentro dos padrões acordados²⁹. Nesse ponto, o foco é no efeito e não na causa.

Em análise aos documentos solicitados por *e-mail*³⁰ para comprovar as respostas ao questionário, observa-se que há documentos que comprovam que há processo de gerenciamento de incidentes na Sefaz-MT, com política, mapa e modelo. No entanto, são políticas adstritas ao setor da Coordenação de Tecnologia da Informação (Coti).

Não há nenhuma regulamentação publicada (portaria, resolução ou outro instrumento), de modo que não estão chanceladas pela alta administração. Assim, evidenciou-se que, embora seja executado o processo de gerenciamento de incidentes, este não está formalmente instituído como norma de cumprimento obrigatório.

28 Definição retirada do livro Implantando a Governança de TI: da Estratégia à Gestão dos Processos e Serviços, 4ª ed. 2014.

29 Definição retirada do livro Implantando a Governança de TI: da Estratégia à Gestão dos Processos e Serviços, 4ª ed. 2014.

30 E-mail 23/05/2017.

5.4 Deficiência no gerenciamento dos projetos de TI

Diante da não sensibilização da alta administração acerca da importância da gestão de portfólio de projetos de TI, consubstanciado na falta de diretriz para a atividade, constatou-se que há deficiências no gerenciamento de projetos de TI da Sefaz-MT. Tais falhas podem ocasionar má alocação de recursos e problemas na priorização dos projetos de tecnologia da informação.

O Gerenciamento de Projetos é a aplicação de conhecimentos, habilidades e técnicas para a execução de projetos de forma efetiva e eficaz. Trata-se de uma competência estratégica para organizações.³¹

No questionário eletrônico, a Sefaz-MT informou que “adota parcialmente” o gerenciamento de projetos de TI e que “iniciou plano para adotar” o portfólio de projetos de TI.

Em análise aos documentos solicitados para comprovar as respostas ao questionário eletrônico sobre o gerenciamento de projetos de TI, concluiu-se que há gerenciamento parcial de projetos de TI, pois nos documentos constam cronograma, projeto e situação em que se encontram, apesar de nem todos os documentos estarem atualizados.

Contudo, está adstrito a poucos projetos. Segundo informações, em função do tamanho da equipe, a designação de gerentes de projetos é feita apenas para os projetos mais críticos. De uma média de 30 a 40 projetos em execução, cerca de cinco são acompanhados por gerentes de projeto.

Além disso, a classificação de projetos críticos é feita pela percepção da equipe ou quando há determinação expressa da direção estratégica. Não há (ainda) um critério objetivo para a sua classificação e priorização.

Esse último ponto, falta de critério objetivo, coaduna com o achado de portfólio de projetos de TI. Quando da análise dos documentos solicitados para comprovar as respostas ao questionário eletrônico sobre o tema, foi enviado arquivo³² que traz os projetos de TI categorizados pela ordem de prioridade a partir de notas atribuídas a um elenco de critérios.

O portfólio de TI é uma metodologia para a priorização dos investimentos de TI com base no retorno de projetos e ativos para a organização e no seu alinhamento com os objetivos estratégicos do negócio. O portfólio de projetos torna claras as regras de priorização de projetos e ativos e faz com que a administração saiba onde deve investir³³.

Apesar de conter uma lista de projetos categorizados por ordem de prioridade, trata-se de um documento interno da Coordenadoria de Tecnologia da Informação (Coti). Ou seja, não é algo ratificado pela alta administração, por isso acaba não sendo utilizado no momento da tomada de decisão. É importante destacar que, conforme abordado no tópico 2.2, não há efetiva priorização das ações de TI pela alta administração.

Ainda, não há nenhuma referência sobre data de início da política, comissão formada responsável, ou outro documento que permita inferir que foi iniciado o plano para que o portfólio de TI passe a ser implementado como política a ser seguida no desenvolvimento dos projetos de TI. Por isso, concluiu-se que a Sefaz-MT não adota este processo.



31 Definição do site do *Project Management Institute* – PMI, disponível em <<https://brasil.pmi.org/brazil/AboutUs/WhatIsProjectManagement.aspx>>.

32 Projetos de TI – Atualizado dia 3-5.

33 Definição retirada do livro *Implantando a Governança de TI: da Estratégia à Gestão dos Processos e Serviços*, 4ª ed. 2014.

6. Conclusão

A auditoria buscou verificar a implementação dos controles e processos de governança de tecnologia da informação para assegurar a entrega de resultados alinhados aos objetivos de negócio da instituição, gerenciando os riscos existentes.

Nessa seara, o trabalho buscou responder à seguinte questão de auditoria:

A Secretaria de Fazenda de Mato Grosso, adota práticas de governança de TI de forma a auxiliar a organização na alocação de recursos (materiais, humanos e financeiros), na proteção de informações críticas e no alcance dos seus objetivos institucionais?



Para responder a essa questão foram analisados quatro eixos de auditoria: liderança da alta administração, estratégia e planos, pessoal e processos.

No eixo liderança da alta administração, constatou-se que as práticas de governança corporativa e de governança de TI não foram plenamente definidas e implementadas no âmbito da instituição, e, ainda, que há insuficiência de diretrizes com o objetivo de dirigir a atuação da TI com foco na entrega de resultados para a instituição.

No eixo estratégia e planos, observou-se deficiências no processo e no plano estratégico institucional. Além disso, verificou-se a não formalização do processo de planejamento de TI e a inexistência de plano de TI vigente.

No eixo de pessoal, foram apontados como achados a ausência de plano de capacitação de profissionais de TI que auxilie no desenvolvimento das competências necessárias para a boa execução dos trabalhos e a inexistência de estudo de dimensionamento da força de trabalho necessária

para o setor de tecnologia da informação.

Por último, quanto aos processos, foram identificadas falhas na gestão de riscos de TI, deficiências na execução de processos de gestão de serviços, nos processos de segurança da informação e no gerenciamento dos projetos de TI.

As causas mais importantes identificadas para estes achados relacionam-se à inércia da alta administração em definir políticas e estabelecer diretrizes para a governança de TI e a baixa sensibilização e compreensão da alta administração acerca da importância da governança de TI para os resultados organizacionais.

Como consequências, têm-se os riscos de se ter uma estrutura de governança corporativa e de TI ineficiente; de que a TI não atenda às necessidades de negócio institucionais; de gerenciamento ineficiente de recursos; de tomada de decisão inadequada; de não alinhamento da TI com os objetivos do negócio; e de descontinuidade dos projetos de TI.

Pelo exposto, resta evidenciado que a Sefaz-MT ainda carece de práticas efetivas de governança de TI que estejam alinhadas às estratégias e ao negócio da instituição e que auxiliem na alocação de recursos materiais, humanos e financeiros, na proteção de informações críticas e no alcance dos objetivos institucionais.

Em decorrência do panorama relatado, foi proposto aos gestores da Secretaria de Fazenda a adoção de medidas com o objetivo de solucionar as fragilidades evidenciadas, conforme demonstra a proposta de encaminhamento.

Os benefícios esperados são a identificação e o gerenciamento das ameaças atuais e futuras para o negócio; o alinhamento da TI com as necessidades do negócio; a melhoria no desempenho dos servidores e dos gestores da área de TI; a otimização dos investimentos em TI e a redução dos riscos de perda de informações sensíveis ou furto/alterações de informações fiscais.

7. Proposta de Encaminhamento

Diante do exposto, com a finalidade de contribuir para a melhoria da governança de tecnologia da informação da Secretaria de Estado de Fazenda, encaminha-se o relatório conclusivo de auditoria, com a seguinte proposta de encaminhamento:

- a. apreciação pelo Tribunal Pleno, nos termos do art. 189 do Regimento Interno do TCE-MT (Resolução nº 14/2007);
- b. estabelecimento de prazo, não superior a 90 dias, para apresentação de plano de ação pela Sefaz-MT para implementação das recomendações e determinações prolatadas pelo TCE-MT, com a designação dos responsáveis pela execução das medidas;

- c. realização de monitoramento pela equipe técnica dos resultados alcançados decorrentes da adoção das deliberações do TCE-MT, no prazo de 24 a 36 meses após sua publicação;
- d. envio de cópia deste relatório aos seguintes interessados:
 - Secretaria de Estado de Fazenda (Sefaz-MT);
 - Empresa Mato-Grossense de Tecnologia da Informação (MTI);
 - Controladoria Geral do Estado (CGE-MT).

Por fim, apresenta-se, em síntese, as propostas de recomendações.

Recomenda-se ao **Secretário de Estado de Fazenda** que:

1

institua, no âmbito da Sefaz-MT, como normas de cumprimento obrigatório, políticas corporativas de gestão de riscos e de continuidade de negócios;

2

determine que seja realizada avaliação dos papéis e responsabilidades organizacionais relativos à governança corporativa no âmbito da Sefaz-MT;

3

defina e comunique formalmente os papéis e responsabilidades mais relevantes para a governança de TI no âmbito da Sefaz-MT;

4

institua formalmente um comitê de TI, composto por representantes de áreas relevantes da organização, de forma que se possibilite a priorização das ações de TI no âmbito da instituição;

5

defina formalmente diretrizes para:

- a) o planejamento de TI;
- b) a gestão do portfólio de projetos e serviços de TI, inclusive para definição de critérios de priorização e de alocação orçamentária;
- c) a avaliação do desempenho dos serviços de TI; e
- d) a comunicação com as partes interessadas (público interno e externo) sobre os resultados da gestão e do uso da TI, contemplando o meio de divulgação, o conteúdo, a frequência e o formato das comunicações.

| | |
|----|---|
| 6 | providencie servidor capacitado para atuar em auditoria de governança de TI; |
| 7 | normatize a obrigatoriedade de a Sefaz-MT executar periodicamente processo de planejamento estratégico institucional, observando as boas práticas sobre o tema; |
| 8 | determine a realização do desdobramento de cada objetivo do Plano Estratégico 2015-2030 em metas quantificáveis e ações; |
| 9 | normatize a obrigatoriedade de a Sefaz-MT executar periodicamente processo de planejamento estratégico de TI, observando as boas práticas sobre o tema; |
| 10 | institua, no âmbito da Sefaz-MT, como norma de cumprimento obrigatório, diretrizes para garantir o desenvolvimento de competências multidisciplinares dos gestores de TI, com conteúdo abrangendo temas específicos de TI e temas relacionados à gestão; |
| 11 | institua, no âmbito da Sefaz-MT, como norma de cumprimento obrigatório, diretrizes para garantir o desenvolvimento do pessoal técnico de TI; |
| 12 | realize estudo quantitativo e qualitativo de dimensionamento da força de trabalho necessário no setor de TI, de forma a delimitar as necessidades de recursos humanos da Coti; |
| 13 | institua, no âmbito da Sefaz-MT, como norma de cumprimento obrigatório, política de gestão de riscos de TI; |
| 14 | formalize o processo de gestão de riscos de TI a fim de adequar os riscos de TI aos níveis aceitáveis pela organização, executando a avaliação dos riscos periodicamente, conforme estabelecem as melhores práticas; |
| 15 | promova ações de sensibilização e capacitação dos gestores quanto à gestão de riscos de TI, com o objetivo de orientá-los na identificação, análise, tratamento e comunicação dos riscos de TI a que a instituição está sujeita; |
| 16 | estabeleça comitê de segurança da informação, ou institucionalize as competências em colegiado equivalente, assim como designe responsável pela segurança da informação a fim de deixar clara a responsabilidade global pelo controle dos processos de segurança da informação; |
| 17 | estabeleça política de cópia de segurança a fim de evitar a perda de informações sensíveis às atividades do órgão; |
| 18 | estabeleça o processo de gerenciamento de continuidade de serviços de TI, a fim de tornar a norma obrigatória e passível de avaliação pelos órgãos de controle, alinhando com as diretrizes de continuidade de negócio da organização; |
| 19 | estabeleça o processo de gerenciamento de mudanças a fim de tornar a norma obrigatória e passível de avaliação pelos órgãos de controle; |

20

formalize o processo de gerenciamento de incidentes a fim de tornar a norma obrigatória a todos envolvidos com o processo na organização, além de possibilitar a avaliação pelos órgãos de controle;

21

estabeleça processo de gerenciamento projetos, incluindo regras de priorização e todos os processos críticos de negócio, a fim de utilizar melhor os recursos organizacionais e deixar clara a taxa de retorno dos projetos para a organização.

Recomenda-se à **Coordenação de Tecnologia da Informação** que:

1

realize estudo acerca das competências necessárias ao pessoal de TI;

2

elabore plano anual de capacitação alinhado às necessidades da área de TI;

3

acompanhe a execução do plano de capacitação, com a finalidade de identificar e corrigir desvios e avaliar se os resultados esperados foram alcançados.

Recomenda-se ao responsável pelo **Controle Interno** da Sefaz-MT que:

1

inclua nos planos de auditoria interna futuros, a avaliação da governança de tecnologia da informação.

Inteiro Teor

Para ler o Relatório de Auditoria na íntegra basta acessar <<http://www.tce.mt.gov.br/conteudo/download/id/86004>>.

Ou se você quiser ver o trâmite completo do Processo nº 57339/2017, acesse <<http://www.tce.mt.gov.br/protocolo/detalhe/num/151203/ano/2017>>.



Tribunal de Contas
Mato Grosso

TRIBUNAL DO CIDADÃO



PubliContas

Editora do Tribunal de Contas
do Estado de Mato Grosso

ISBN 978-85-98587-98-1



9 788598 587981