MINISTÉRIO DA EDUCAÇÃO
Secretaria de Educação Profissional e Tecnológica
Instituto Federal de Educação, Ciência e Tecnologia de Mato Grosso do Sul
Unidade de Auditoria Interna Governamental

RELATÓRIO DE AVALIAÇÃO

GOVERNANÇA E GESTÃO DE TECNOLOGIA DA INFORMAÇÃO

Unidade Auditada: Diretoria de Gestão de Tecnologia da Informação- DIRTI

Exercício 2023

Dezembro 2023

Unidade de Auditoria Interna Governamental do Instituto Federal de Mato Grosso do Sul (AUDIT/IFMS)

RELATÓRIO DE AVALIAÇÃO

Órgão: **Instituto Federal de Mato Grosso do Sul**

Unidade Auditada: **Diretoria de Gestão de Tecnologia da Informação**

Município/UF: **Campo Grande/MS**

Relatório de Avaliação: **01/2023**

Missão

Contribuir para a realização dos objetivos institucionais, por meio de uma abordagem sistemática e disciplinada para avaliar e melhorar a eficácia dos processos de controles internos, governança e gerenciamento de riscos.

Avaliação

O trabalho de avaliação, como parte da atividade de auditoria interna, consiste na obtenção e na análise de evidências com o objetivo de fornecer opiniões ou conclusões independentes sobre um objeto de auditoria. Objetiva também avaliar a eficácia dos processos de governança, de gerenciamento de riscos e de controles internos relativos ao objeto e à Unidade Auditada, e contribuir para o seu aprimoramento.

QUAL FOI O TRABALHO REALIZADO PELA AUDIT?

O trabalho realizado consistiu na avaliação da maturidade da estrutura de governança e os mecanismos utilizados para desempenhar as funções de avaliar, dirigir e monitorar a governança e gestão de TI do IFMS.

POR QUE A AUDIT REALIZOU ESSE TRABALHO?

Ação prevista no Plano Anual de Auditoria Interna – PAINT 2023, aprovado pela Resolução/COSUP nº 09 de 09 de dezembro de 2022.

QUAIS AS CONCLUSÕES ALCANÇADAS PELA AUDIT?

QUAIS AS RECOMENDAÇÕES QUE DEVERÃO SER ADOTADAS?

Haja vista a relevância e materialidade da governança, foram identificadas oportunidades de melhorias quanto à estruturação de um sistema de governança, controles internos, gerenciamento de riscos e segurança da informação.

Foram propostas recomendações de caráter essencialmente preventivo aos pontos de melhoria identificados para viabilização a função direcionadora com a formalização dos alicerces para uma boa governança, promoção de uma gestão focada em resultados, definição de um processo formal de aprimoramento contínuo da governança de modo a assegurar que os responsáveis pela tomada de decisão tenham acesso tempestivo quanto aos riscos que a instituição está exposta.

LISTA DE SIGLAS E ABREVIATURAS

ABNT - Associação Brasileira de Normas Técnicas

APF – Administração Pública Federal

AUDIT – Auditoria Interna

CGD - Comitê de Governança Digital

COBIT - *Control Objectives for Information and Related Technology*

COSO - *Committee of Sponsoring Organizations of the Treadway Commission*

COSUP – Conselho Superior

CSTIC - Comitê de Segurança da Informação

DIRTI - Diretoria de Gestão de Tecnologia da Informação

ETIR - Equipe de Tratamento e Resposta a Incidentes Cibernéticos

GRSI - Gestão de Riscos de Segurança da Informação

GSI - Gabinete de Segurança Institucional

IIA - *Institute of Internal Auditors*

IEC - *International Electrotechnical Commission*

IFMS - Instituto Federal de Educação, Ciência e Tecnologia de Mato Grosso do Sul

IGG - Índice Integrado de Governança e Gestão Públicas

IN - Instrução Normativa

ISO - *International Organization for Standardization*

ME – Ministério da Economia

MP – Ministério Público

NBR - Norma Brasileira

PAA - Plano de Ação Anual

PAINT - Plano Anual de Auditoria Interna

PCA - Plano de Contratações Anual

PDI - Plano de Desenvolvimento Institucional

PDTIC - Plano Diretor de Tecnologia da Informação e Comunicação

PNSI - Política Nacional de Segurança da Informação

POSIC - Política de Segurança da Informação e Comunicação

PR – Presidência da República

SA – Solicitação de Auditoria

SEFTI - Secretaria de Fiscalização de Tecnologia da Informação

SGD - Secretaria de Governo Digital

SI - Segurança da Informação

SISP - Sistema de Administração dos Recursos de Tecnologia da Informação

SUAP - Sistema Unificado de Administração Pública

TCU – Tribunal de Contas da União

TI - Tecnologia da Informação

TIC - Tecnologia da Informação e Comunicação

SUMÁRIO

1. INTRODUÇÃO

Em cumprimento à Ordem de Serviço nº 001/2023 – AUDIT, item nº 3 do Plano Anual de Atividades da Auditoria Interna – PAINT 2023 do IFMS, referente à realização de auditoria de governança de TI, apresentamos os resultados dos exames realizados no período de 05 de abril a 31 de outubro de 2023.

O objetivo geral da ação de auditoria foi avaliar a maturidade dos mecanismos utilizados para desempenhar as funções de avaliar, dirigir e monitorar a governança e gestão de Tecnologia da Informação do IFMS.

A ação foi realizada em estrita observância às normas de auditoria aplicáveis ao Serviço Público.

Nenhuma restrição foi imposta à realização do trabalho.

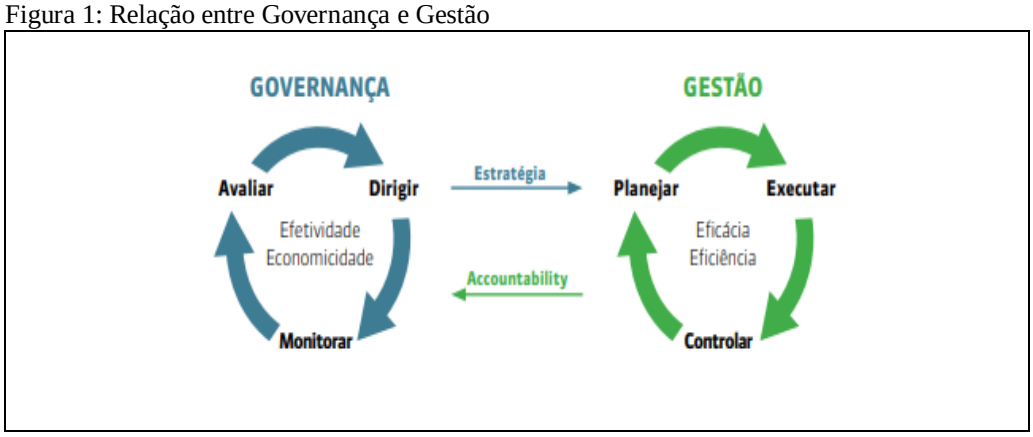
1.1. Visão Geral do Objeto

O Decreto nº 9.203 de 22 de novembro de 2017, que trata sobre a política de governança da administração pública federal dispõe no art. 2º:

> *I - Governança pública - conjunto de mecanismos de liderança, estratégia e controle postos em prática para avaliar, direcionar e monitorar a gestão, com vistas à condução de políticas públicas e à prestação de serviços de interesse da sociedade.*

A governança não se confunde com gestão. A governança direciona enquanto a gestão realiza, tem papel de planejar, executar e controlar as atividades em consonância com a direção definida pela governança com objetivo de atingir os objetivos institucionais.

Figura 1: Relação entre Governança e Gestão



Fonte: Referencial Básico de Governança Organizacional (TCU, 2020)

Nesse sentido, a Portaria de implantação da Governança de TIC SGD/ME nº 778, de 4 de abril de 2019, reitera a diferenciação entre a Governança e Gestão de TI. Segundo a supracitada portaria, a Governança é o sistema pelo qual o uso atual e futuro de TIC é dirigido e controlado, mediante avaliação e direcionamento, para atender às necessidades prioritárias e estratégicas da organização e monitorar sua efetividade por meio de planos, incluída a estratégia e as políticas de uso de TIC no âmbito da organização. Já a Gestão é o conjunto de ações relacionadas ao planejamento, desenvolvimento, execução e monitoramento das atividades de TIC, em linha com a direção definida pela função de governança, a fim de atingir os objetivos institucionais.

A Nota Técnica nº 07/2014 Sefti/TCU também apresenta uma série de entendimento da Sefti sobre a organização do sistema de governança de TI, propõe alguns viabilizadores da governança de TI, tais como, princípios, políticas, *frameworks;* estruturas organizacionais; processos, cultura, ética e comportamento; pessoas, habilidades e competências.

A Governança de Tecnologia da Informação possui um papel importante para Governança Corporativa em âmbito das decisões estratégicas da instituição. O TCU entende que a Governança de TI consiste no estabelecimento de mecanismos para assegurar que o uso da TI agregue valor ao negócio das organizações, com riscos aceitáveis. Esses mecanismos incluem a definição de políticas, estruturas organizacionais, processos, controles, entre outros componentes que possibilitam que os recursos investidos em tecnologia da informação atendam às necessidades não só do negócio da instituição, mas também das diversas partes interessadas que podem ser afetadas pelas decisões relacionadas à TI.

O Ministro Aroldo Cedraz por meio do Acórdão 2.308/2010 – Plenário, define Governança de TI como sendo um conjunto estruturado de políticas, normas, métodos e procedimentos destinados a permitir à alta administração e aos executivos o planejamento, a direção e o controle

da utilização atual e futura de tecnologia da informação, de modo a assegurar, a um nível aceitável de risco, eficiente utilização de recursos, apoio aos processos da organização e alinhamento estratégico com objetivos desta última. Seu objetivo, pois, é garantir que o uso da TI agregue valor ao negócio da organização.

Considerando o exposto, denota-se que a governança de TI não se refere ao departamento de TI, mas, sobretudo, do seu uso em toda a instituição, assim dizendo, uma **visão estratégica** voltada para a efetividade e os seus resultados que se darão perante a sociedade e está diretamente ligada ao papel da mais alta administração de internalizar essa cultura e alinhar as políticas e estratégias da área de TI com as necessidades das demais áreas. O Acórdão 2471/2008 TCU-Plenário deliberou sobre esse assunto: "*a governança de TI **deve ser responsabilidade da alta administração**[1]. Logo, a criação do arcabouço de governança de TI a ser utilizado nos entes da Administração Pública Federal (APF) também deve ser de responsabilidade da alta administração*".

O IFMS, conforme previsão regimental, é organizado em estrutura multi*campi*, sendo sua administração exercida pela Reitoria de forma sistêmica. A Diretoria de Gestão Tecnologia de Informação é o órgão sistêmico responsável por propor, planejar, coordenar, executar e avaliar os projetos, as ações e as atividades relacionadas à Tecnologia da Informação.

A instituição ainda conta com a previsão regimental de dois comitês relacionados à TI: Comitê de Governança Digital (CGD) e Comitê de Segurança da Informação (CSTIC), com atribuições e competências relacionadas à Governança Digital e à segurança da informação, respectivamente.

2. PLANEJAMENTO

2.1. Questões de Auditoria

Para consecução dos objetivos foram elaboradas as seguintes questões de auditoria:

a) A estrutura de Governança e Gestão de TI está formalmente definida em efetivo funcionamento?

b) Qual o nível de maturidade do IFMS em relação à Governança e Gestão de TI?

[1] Entende-se por Alta Administração - gestores que integram o nível executivo mais elevado da organização com poderes para estabelecer as políticas, os objetivos e conduzir a implementação da estratégia para realizar os objetivos da organização.

c) Existem mecanismos de controles internos que garantam a execução dos processos relacionado à Tecnologia da Informação de forma íntegra e livre de fraudes e erros?

2.2. Escopo

Instrumentos de Governança e Gestão de TI do IFMS - normativos, planos/políticas de tecnologia da informação, gestão de riscos e dos controles de governança.

2.3. Metodologia

Os procedimentos de auditoria adotados foram Testes de Observância, que têm por finalidade atestar a segurança dos controles internos estabelecidos quanto ao seu efetivo funcionamento e aderência às normas em vigor, e Testes Substantivos, que objetivam comprovar a suficiência, exatidão e validade das informações produzidas.

A execução foi planejada levando-se em consideração a utilização das seguintes técnicas de auditoria:

✓ Indagação Escrita (Solicitações de Auditoria e interlocuções);

✓ Reaplicação do questionário de autoavaliação IGG (Índice Integrado de Governança e Gestão Públicas) – Ciclo 2021 (Tema 4200. Gestão de Tecnologia e Gestão de Tecnologia da Informação e da segurança da Informação);

✓ Análise da adequação aos normativos pertinentes;

✓ Análise de adequação às boas práticas;

✓ Avaliação de Controles Internos (metodologia *COSO*) com base na percepção da Auditoria Interna.

3. EXECUÇÃO DOS TRABALHOS

Com objetivo de obter as respostas às questões de auditoria, foram emitidas Solicitações de Auditoria destinadas à DIRTI, com o intutito de coletar informações suficientes para o entendimento do contexto geral (análise preliminar), apresentação de informações e aplicação de questionário.

3.1. Respostas às Questões de Auditoria

a) A estrutura de Governança e Gestão de TI está formalmente definida e em

efetivo funcionamento?

Para fins de resposta à primeira questão de auditoria, buscou-se evidenciar se (i) a estrutura de Governança e Gestão de TI está formalmente definida e se (ii) existem evidências da efetiva e regular utilização dessa estrutura na tomada de decisão e na supervisão dos processos institucionais.

Mediante as análises realizadas as respostas às solicitações de auditoria, ao questionário de autoavaliação, e evidenciou-se a inexistência de um sistema de governança formalmente instituído e completo, com definição das diretrizes, papéis e responsabilidades, estrutura, mecanismos para as funções de avaliar, dirigir e monitorar, e as interfaces entre funções de governança e gestão de TI.

O IFMS possui em sua estrutura organizacional dois comitês permanentes da área de tecnologia, Comitê de Governança Digital (CGD) e Comitê de Segurança da Informação (CSTIC).

O CSTIC foi instituído/reformulado por meio da Portaria nº 1387 de 09 de outubro de 2018, por meio da Portaria nº 1387 de 09 de outubro de 2018. Todavia, foram encontradas inconsistências na composição dos membros, tendo em vista que designa somente servidores lotados na DIRTI, bem como, ausência do gestor de Segurança da Informação, em desacordo com art. 21 da Portaria GSI nº 01 de 27 de maio 2020:

> *O Comitê de Segurança da Informação disposto terá a seguinte composição:*
>
> *I - o gestor de segurança da informação do órgão ou da entidade, que o coordenará;*
>
> *II - um representante da Secretaria-Executiva ou da unidade equivalente do órgão ou da entidade;*
>
> *III - um representante de cada unidade finalística do órgão ou da entidade; e*
>
> *IV - o titular da unidade de tecnologia da informação do órgão ou da entidade.*

No que se refere ao CGD, com previsão no Regimento Geral do IFMS, em seu art. 174:

> *O Comitê de Governança Digital tem a finalidade de deliberar sobre os assuntos relativos à Governança Digital, a fim de gerar benefícios para a sociedade mediante o uso da informação e dos recursos de tecnologia da informação e comunicação na prestação de serviços públicos, bem como assegurar a obtenção de informações pela sociedade, observadas as restrições legalmente previstas, conforme disposto no Decreto n° 8.638, de 15 de janeiro de 2016, cujas* ***competências, composição e funcionamento são definidos em regimento próprio*** *(grifo nosso).*

O CGD foi instituído por meio da portaria nº 874 de 27 de julho de 2021, até o período que ocorreram as análises de auditoria não houve sua regulamentação. Embora não haja essa regulamentação, o regimento geral do IFMS define os comitês em sua estrutura organizacional como **órgãos colegiados de instância consultiva**.

> *TÍTULO II*
> *DOS ÓRGÃOS COLEGIADOS*
> *(...)*
> *Art. 5º Os órgãos colegiados do IFMS são organizados em:*
> *(...)*
> *III - **Consultivos**:*
> *(...)*
> *d) Comissões e **Comitês Permanentes**. (grifo nosso)*

Diante da legislação em vigor que dispõe aos comitês a responsabilidades de natureza deliberativa, entende-se que o CGD do IFMS deva ser estruturado com natureza **consultiva e deliberativa**.

Nesse contexto, o Decreto nº 10.332/2020 que institui a estratégia de governo digital, determina que os órgãos e entidades instituam seus respectivos comitês para **deliberar** sobre assuntos relativos à implementação das ações de governo digital e ao uso de recursos de tecnologia da informação e comunicação. Também prevê que deverão ser elaborados instrumentos de planejamento (Plano de Transformação Digital, Plano Diretor de Tecnologia da Informação e Comunicação e o Plano de Dados Aberto) pela unidade competente da instituição e aprovados pelo respectivo Comitê de Governança Digital.

Assim como a Portaria nº 778/2019 alterada pela Portaria n° 18.152, de 4 de agosto de 2020 art. 4º III- *"é papel do Comitê de Governança Digital exercer a governança de TIC nos órgãos e entidades do SISP, conduzindo os processos de direção, monitoramento e avaliação do desempenho de TIC."*

Enquanto o art. 5º define que os assuntos relacionados à Governança de TIC serão deliberados pelo Comitê de Governança Digital, instituído pelo Decreto nº 10.332, de 28 de abril de 2020, ou estrutura equivalente. O Parágrafo Único da mesma portaria *"o Comitê é responsável pelo estabelecimento e alcance dos objetivos e das metas de TIC, bem como pela orientação das iniciativas e dos investimentos em TIC"*.

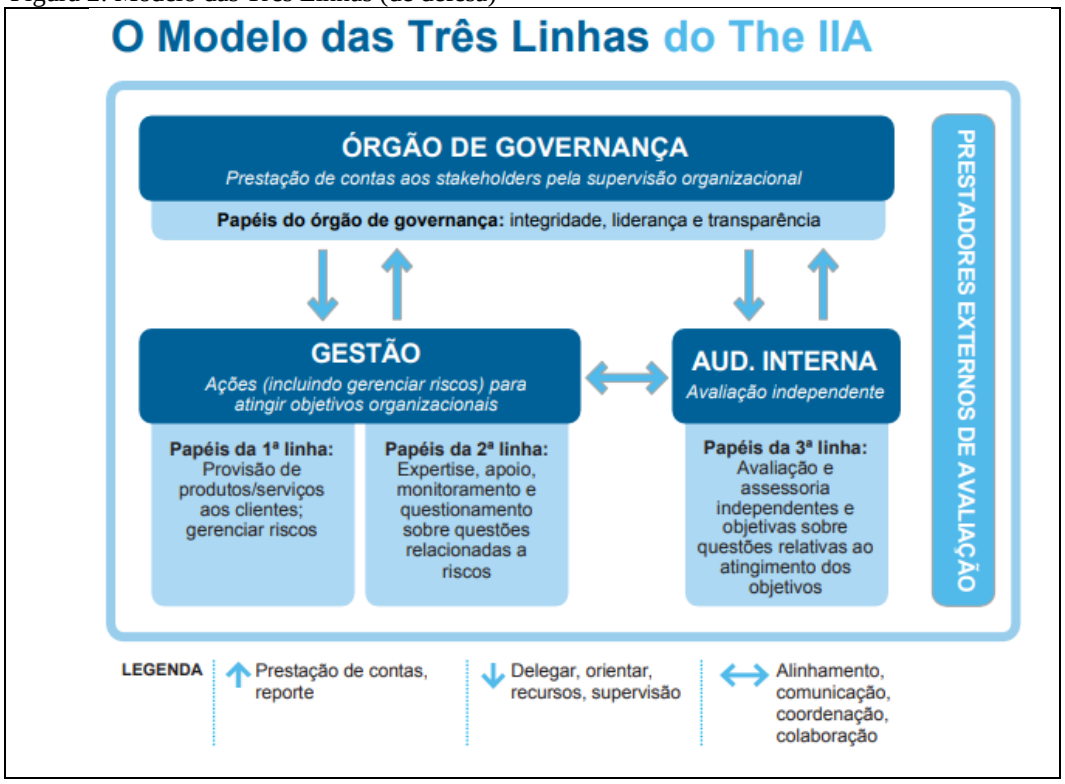
Como consequência das incompletudes da estrutura de governança, evidenciou-se fragilidades na Gestão de TI, como a ausência de alinhamento entre o PDTIC e a estratégia institucional, ausência de revisão tempestiva e atualização dos normativos institucionais e ausência de ações voltadas à valorização e retenção de recursos humanos.

Em relação à Gestão de TI, evidenciou-se a ausência de monitoramento e mensuração de seus resultados e do acompanhamento das metas e indicadores do PDTIC e PDI.

Considerando o modelo das três linhas de defesa do *Institute of Internal Auditors* (IIA 2020), embora a governança e a alta administração não estejam consideradas entre as três linhas de defesa, esse modelo serve como exemplo para melhorias na comunicação e conscientização sobre os papéis e as responsabilidades.

Utilizando-se como referência o modelo das Três Linhas (de defesa) do Instituto dos Auditores Internos (IIA), que objetiva esclarecer os papéis e responsabilidades a serem desempenhados nas organizações pelos atores envolvidos na governança, gestão e auditoria interna, é possível verificar a existência, na teoria, das 3 linhas no processo de TI do IFMS.

Figura 2: Modelo das Três Linhas (de defesa)

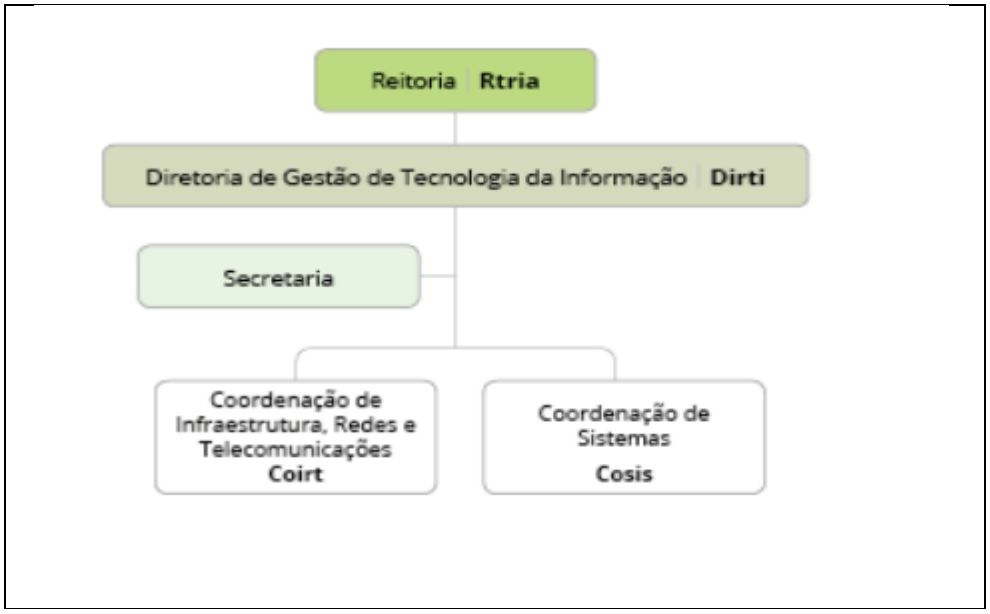


Fonte:. Adaptado IIA (2020)

No âmbito do IFMS, considerando o organograma da Dirti, na primeira linha posicionam-se as coordenações e na segunda linha, a Diretoria de Tecnologia da Informação e Comunicação

e; na terceira linha, a Auditoria Interna; e enquanto a governança sob a responsabilidade primária da Alta Gestão – Reitoria, com o suporte dos comitês relacionados ao tema.

Figura 3: Organograma DIRTI/IFMS



Fonte: *Site* do IFMS (2023)

Em que pese a existência formal da estrutura de governança e gestão, não foi possível evidenciar a sua efetiva utilização na tomada de decisão, na supervisão dos processos institucionais (de maneira sistêmica) e no apoio à alocação de recursos (principalmente humanos) relacionados à TI no IFMS.

Resposta à questão de auditoria:

Conclui-se que a estrutura de Governança e Gestão de TI não está formalmente instituída em sua completude, possuindo lacunas relacionadas à definição das diretrizes, papéis e responsabilidades; valores, processos e estruturas necessárias para que as atividades de governança **avaliar, dirigir e monitorar**, bem como as interfaces entre as funções de governança e gestão de TI sejam desempenhadas de forma eficaz, de modo a possibilitar que a instituição alinhe seus objetivos ao interesse público, gerencie seus riscos e entregue o valor esperado de forma íntegra, transparente e responsável.

b) Qual o nível de maturidade do IFMS em relação à Governança e Gestão de TI?

Segundo TCU para que a TI seja bem governada, as seguintes condições devem ser satisfeitas, sem exceção: (i) ter uma forte estrutura de liderança que estabeleça os objetivos e a direção a seguir, sendo capaz de corrigir os possíveis desvios de rumo; (ii) estabelecer estratégias e planos que materializem a direção estabelecida, de forma a contribuir com o alcance dos objetivos da organização; (iii) dispor de informações tempestivas para subsidiar a tomada de decisão, bem como dar transparência das ações às partes interessadas; (iv) definir e estabelecer processos para implementar as políticas e entregar os resultados esperados, bem como para garantir a continuidade da ações; (v) dispor de pessoas capazes de fazer funcionar essa engrenagem organizacional de forma eficiente e efetiva.

A maturidade da governança é construída por meio de macanismos viabilizadores que proporcionam assegurar que o processo agregue valor ao negócio com riscos aceitáveis. Esses mecanismos são as politicas, diretrizes, normas, estruturas organizacionais, processos e definição clara dos papéis.

Nesse sentido, o TCU, por meio do levantamento do Perfil Integrado de Governança Organizacional e Gestão Pública (IGG), tem avaliado as organizações públicas quanto à maturidade da governança e gestão em diferentes áreas, dentre elas a de TI.

O IFMS compõe o rol de organizações respondentes e obteve no último levantamento (ciclo 2021) índices que variaram de iniciantes a intermediários nos diferentes quesitos de avaliação. Para fins de mensuração do atual estágio, passados 2 anos da aplicação, a equipe de auditoria reaplicou o questionário junto à DIRTI, identificando estagnação institucional desde o último ciclo de 2021, tenha-se em vista que não foram implementadas soluções voltadas para a melhoria do desempenho institucional.

Resposta à questão de auditoria:

Evidenciou-se a manutenção de um nível intermediário de Governança e iniciante de Gestão de TI, considerando a autoavaliação reaplicada do IGG 2021.

c) Existem mecanismos de controles internos que garantam a execução dos processos relacionados à Tecnologia da Informação de forma íntegra e livre de fraudes e erros?

A Instrução Normativa/CGU nº 3/2017, estabelece que a avaliação dos controles internos da gestão deve considerar os seguintes componentes: ambiente de controle, avaliação de riscos, atividades de controle, informação e comunicação e atividades de monitoramento. Os

componentes descritos na supracitada IN alinham-se às melhores práticas corporativas emitidas pelo Relatório do *Committee of Sponsoring Organizations of the Treadway Commission* (COSO).

Ambiente de controle

O ambiente de controle é a base que sustenta todo o Sistema de Controle Interno. Os fatores que compõem o ambiente de controle são determinados pela alta administração (*top down*), incluem integridade e valores éticos, competência das pessoas, maneira pela qual a gestão delega autoridade e responsabilidades, estrutura de governança, plano organizacional, regulamentos e manuais de procedimentos, políticas e práticas de recursos humanos.

Ainda que existam algumas iniciativas como PDTIC, POSIC, instituição do comitê de governança digital, a alta gestão não estabeleceu um sistema de governança com diretrizes definidas, políticas e estratégias para exercer a governança que promova uma função direcionadora, que defina claramente os papeis e responsabilidades necessárias para desempenhar as funções de avaliar, dirigir e monitorar.

Avaliação de riscos

Os riscos são enfrentados por todos os órgãos, independentemente do seu tamanho, da sua estrutura ou da sua natureza. Deve-se ter consciência dos riscos relevantes que envolvam as atividades desenvolvidas através dos macroprocessos e de como se deve gerenciar esses riscos a fim de alcançar os objetivos.

No âmbito da área de tecnologia da informação, não há definição de políticas e diretrizes para o tratamento de riscos e no que se refere ao gerenciamento da segurança da informação. Em que pese exista a POSIC aprovada, constatou-se uma baixa efetividade de sua execução tendo em vista que não foram identificadas ações suficientes que produzam seus efeitos na prática, apresentando contornos de mera formalidade.

Atividades de controle

As atividades de controle são geralmente expressas em políticas e procedimentos que tendem a assegurar que sejam cumpridas as instruções emanadas da alta direção no ambiente de controle orientadas primordialmente à prevenção e à neutralização dos riscos, os quais devem contribuir na determinação dos processos a serem priorizados que forneçam segurança razoável de que os objetivos serão alcançados, as diretrizes sejam cumpridas e que as ações de tratamento dos riscos

sejam implementadas.

Constatou-se que as atividades de controle ocorrem em nível informal e dependente de características pessoais dos servidores envolvidos, visto a ausência de um processo formalizado para o processo de planejamento estratégico de TIC, desenvolvimento, execução e monitoramento do mesmo.

O Comitê de Governança Digital não tem sua regulamentação interna, a definição formal dos papéis e competências dos envolvidos na tomada de decisão é de fundamental importância para o sucesso fornecendo os mecanismos necessários para que a alta gestão possa monitorar e direcionar a TI.

Assim como foi constatada a inexistência mapeamento de macroprocessos finalísticos e de apoio à governança que permita identificar as etapas, responsáveis, controles existentes, oportunidades de melhoria, gargalos e possíveis riscos ao atingimento dos objetivos.

A segurança da informação é um ponto crítico, tendo em vista a baixa efetividade da POSIC, não há qualquer procedimento formalizado para administração de contingências frente a impactos decorrentes de falhas, ameaças, desastres ou indisponibilidades significativas. Ausência de controles que forneçam segurança razoável que a direção estabelecida seja cumprida e que os ajustes sejam realizados para evitar que os riscos impeçam ou prejudiquem a consecução dos objetivos.

Informação e comunicação

Contemplam as informações e os sistemas de comunicação que permitem garantir a identificação, o armazenamento e a comunicação de todas as informações relevantes, com o intuito de permitir a realização dos procedimentos estabelecidos e outras responsabilidades, orientando a tomada de decisões, permitindo o monitoramento de ações e contribuindo para a realização de todos os objetivos de controle interno.

Evidenciou-se a ausência de fluxos, diretrizes formais para informação, comunicação e prestação de contas dos resultados da gestão e do uso de TI para as partes interessadas (públicos interno e externo), não sendo possível afirmar a existência de mecanismos de comunicação e prestação de contas de TIC que forneçam informações apropriadas para o monitoramento das ações e resultados da TIC.

Atividades de monitoramento

As atividades de monitoramento avaliam a qualidade do desempenho dos controles internos ao longo do tempo. Nesse processo estão envolvidas atividades como a verificação de inconsistências dos processos ou implicações relevantes, bem como a tomada de ações corretivas.

As atividades de monitoramento apresentadas durante a execução do trabalho se mostraram insuficientes e carentes de papéis e responsabilidades estabelecidos (característicos de um sistema de governança).

Resposta à questão de auditoria:

Não foi possível evidenciar a existência de procedimentos de controles estruturados que sejam capazes de fornecer segurança razoável de que os processos relacionados à governança e gestão de Tecnologia da Informação e Comunicação estejam pautados em ambiente íntegro e confiável que promova a eficiência, efetividade e eficácia para atingimento dos objetivos institucionais.

4. RESULTADOS DOS EXAMES

4.1 Constatações

1. Incompletude do arcabouço de Governança de TI

Critérios:

- Lei 14.129/2021.
- ABNT NBR ISO 38500:2009 – Governança corporativa de tecnologia da informação.
- Nota Técnica 07/2014 Sefti/TCU de 30 de setembro de 2014.
- Decreto nº 9.203/2017.
- Acórdão 1684/2014 TCU- Plenário.
- Acórdão 2471/2008 TCU-Plenário.

- ABNT NBR ISO/IEC 38500/2009.
- COBIT 5.
- Constituição Federal, art. 37, caput (princípio da eficiência).
- Instrução Normativa nº 01 de 27 de maio de 2020.
- Decreto nº 10.332/2020.
- Portaria nº778/2019 alterado pela Portaria n° 18.152, de 4 de agosto de 2020.
- Acórdão nº 1233/2012 TCU-Plenário, item 9.2.9.
- Instrução Normativa GSI nº 01/2020.
- Lei nº 12.527/2011

Causas:

- Comprometimento da gestão insuficiente.
- Fragilidade na estruturação dos comitês relacionados a TI.
- Ausência de controle/monitoramento estratégico (sistêmico).
- Ausência de cultura de planejamento institucional focada em resultados.
- Ações adotadas insuficientes para a efetiva implementação do Planejamento de Desenvolvimento Institucional.

Consequências:

- Baixa maturidade de governança.
- Insuficiência em atender os objetivos institucionais.

Fato:

Mediante as análises realizadas, as respostas às solicitações de auditoria e ao questionário de autoavaliação, evidenciou-se a inexistência de um sistema de governança completo e formalmente instituído, com definição das diretrizes, papéis e responsabilidades, estrutura,

mecanismos para as funções de avaliar, dirigir e monitorar, e as interfaces entre funções de governança e gestão de TI.

Em uma de suas manifestações, a DIRTI reconhece a insuficiência dos arranjos institucionais para adequado tratamento da governança na área:

> *"a parte de objetivos, riscos e controles associados a Governança e Gestão não estão documentados, inclusive em nosso PDTIC 2021-2023 foi identificada a* ***necessidade da criação de uma Coordenação de Governança em Tecnologia da Informação****, que possa trabalhar no sentido de aprimorar os processos de planejamento, manutenção, continuidade e otimização de recursos referentes a TI, ou seja, Gestão e Governança de TI". (grifo nosso)*

O IFMS possui em sua estrutura organizacional dois comitês permanentes da área de tecnologia da informação: Comitê de Governança Digital (CGD) e Comitê de Segurança da Informação (CSTIC). Em que pese possuírem atribuições inerentes à governança, evidenciou-se fragilidades na regulamentação, composição e, principalmente, na natureza dos comitês.

No que se refere a responsabilidade pela implementação da governança, o Acórdão 2471/2008 TCU-Plenário dispôs que a governança de TI deve ser responsabilidade da alta administração:

> *Logo, a criação do arcabouço de governança de TI a ser utilizado nos entes da Administração Pública Federal (APF) também* ***deve ser de responsabilidade da alta administração****". (grifo nosso)*

Por fim, não foi possível evidenciar a existência e efetivação de mecanismos adequados relacionados ao acompanhamento do funcionamento dos comitês por parte da alta administração. o Acórdão nº1.684/2014 TCU –Plenário recomenda que a alta administração defina mecanismos que possibilitem monitorar o funcionamento dos comitês de TI, à semelhança das orientações da ABNT NBR ISO/IEC 38500:2009.

Manifestação do Gestor: O relatório preliminar foi encaminhado à unidade auditada e a mesma não se manifestou até o fechamento do presente relatório.

Análise da Auditoria Interna: Diante da ausência de manifestação, deduz-se a concordância tácita por parte do gestor.

Recomendação 1: Implementar sistema formalizado e sistêmico de governança de TI (políticas e diretrizes de governança, estrutura e conjunto de mecanismos viabilizadores necessários para avaliar, dirigir e monitorar a gestão da TI no IFMS).

Recomendação 2: Definir as competências, composição e funcionamento do Comitê de Governança Digital (CGD) em regimento próprio.

Recomendação 3: Reformular a composição do CSTIC, em atendimento ao art. 21 da Instrução Normativa GSI nº 01/2020.

Recomendação 4: Promover a transparência da área de TI, por meio da concentração das informações na página da Dirti, tais como o PDTIC, informações relativas aos comitês, normativos, agenda e atas das reuniões.

Benefícios Esperados:

- Promoção da função direcionadora.
- Fixação dos parâmetros básicos de governança.
- Engajamento da alta administração.
- Promover o alinhamento estratégico.
- Definição clara dos papéis e responsabilidades necessários para desempenhar as funções de avaliar, dirigir e monitorar.

2. PDTIC desatualizado/intempestivo

Critérios:

- Constituição Federal, art. 37, caput (princípio da eficiência).
- Guia de PDTIC do SISP.
- Portaria nº 778 de 4 de abril de 2019 alterada pela portaria nº 18.152 de 4 de agosto de 2020.
- Nota Técnica Sefti/TCU nº 07 de 30 de setembro de 2014.
- Acórdão nº 2.308/2010 TCU – Plenário.

- Acórdão nº 2.135/2017 TCU-Plenário.
- Portaria SGD/ME nº 18.152/2020.
- Portaria nº 778/2019.
- Lei 14.129/2021.

Evidências:

- Resolução COSUP nº 44 de 10 de outubro de 2019.
- Resolução COSUP nº 09 de 10 de fevereiro de 2022.
- Plano Diretor de Tecnologia da Informação e Comunicação 2021-2023.
- Plano Diretor de Tecnologia da Informação e Comunicação 2019-2020.
- Solicitações de Auditoria.
- Regimento Geral do IFMS.
- Plano de Desenvolvimento Institucional.
- Plano Anual Específico.

Causas:

- Insuficiência de ações efetivas para implantação das melhores práticas de governança.
- Aprovação do PDTIC em atraso.
- Ausência de cultura organizacional com foco na gestão por resultados.
- Baixo envolvimento da Alta Administração em processos de governança de TIC.

Consequências:

- Não atendimento das metas de desempenho de gestão.
- Potencial Ineficiência da área de TI.
- Potencial desvinculação dos objetivos da TI em relação aos objetivos estratégicos institucionais.
- Ineficiência da instituição no alcance dos seus objetivos institucionais.

Fato:

No tocante à Tecnologia da Informação, o Plano Diretor de TIC (PDTIC) é o instrumento de alinhamento entre as estratégias e os planos de TIC e as estratégias organizacionais. Assim como orienta o Guia de PDTIC do SISP:

> "*é cada vez mais impraticável que o PDTIC não esteja alinhado a estratégia institucional, pois assim o planejamento de TI complementa o*

planejamento estratégico da instituição. A área de TI deve possuir estratégias que promovam ações estruturantes para suportar as metas e objetivos definidos no Planejamento Estratégico do Órgão".

Com vigência mínima de dois anos (com revisão anual) e o dever de estar alinhado à Estratégia de Governo Digital e ao Plano Estratégico Institucional, o Plano Diretor é um instrumento de gestão utilizado para direcionar a execução das ações de TI da instituição, possibilitando justificar os recursos aplicados, minimizar o desperdício, garantir o controle adequado, e aplicar os recursos naquilo que é considerado mais relevante, promovendo a eficiência do gasto público e do serviço público prestado ao cidadão.

Isto posto, verificou-se que o PDTIC 2021-2023 que deveria estar em plena vigência para o início do exercício 2021 foi aprovado somente em 10 de fevereiro de 2022, assim como os planos referentes aos biênios 2017-2018 e 2019-2020 foram aprovados em 29 de junho de 2017 e 10 de outubro de 2019, respectivamente, demonstrando um *delay* entre a elaboração do documento e o período a que se refere.

O PDTIC 2021-2023 tem vigência até 31/12/2023 e até o momento do fechamento deste trabalho de auditoria não foram encontradas no SUAP movimentações processuais, atas de reuniões ou grupos de trabalho referentes a elaboração e aprovação do próximo plano que iniciará em 01/01/2024.

Além de obviamente apresentar inconformidade legal, a situação sugere a adoção do plano de maneira pró-forma, uma vez que as decisões tomadas nos períodos de lacunas não se basearam em um PDTIC atual/tempestivo.

Ademais, a Instrução Normativa nº 01/2019 SGD/ME, estabelece a necessidade de que as contratações de soluções de Tecnologia da Informação e Comunicação estejam em conformidade com o Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) vigente. Portanto, é possível afirmar que as contratação de soluções de tecnologia nos períodos em que não havia plano diretor vigente ocorreram com inconformidades normativas e estratégicas.

Manifestação do Gestor: O relatório preliminar foi encaminhado à unidade auditada e a mesma não se manifestou até o fechamento do presente relatório.

Análise da Auditoria Interna: Diante da ausência de manifestação, deduz-se a concordância tácita por parte do gestor.

Recomendação 5: Definir rotina formalizada de elaboração do PDTIC (contendo, no mínimo, prazos, responsáveis e instâncias de aprovação e revisão).

Benefício Esperado: Prover a instituição de um Plano Diretor de TIC atualizado e tempestivo.

3. Acompanhamento dos resultados de TI insuficiente.

Critérios:

- Constituição Federal, art. 37, caput (princípio da eficiência).
- Guia de PDTIC do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP), dezembro de 2021.
- Nota Técnica Sefti/TCU nº 07 de 30 de setembro de 2014.
- Acórdão nº 2.308/2010 TCU – Plenário.
- Acórdão nº2.135/2017 TCU-Plenário.
- Portaria SGD/ME nº 18.152/2020.
- Portaria nº 778/2019.

Evidências:

- Resolução COSUP nº 44 de 10 de outubro de 2019.
- Resolução COSUP nº 09 de 10 de fevereiro de2022.
- Plano Diretor de Tecnologia da Informação e Comunicação 2021-2023.
- Plano Diretor de Tecnologia da Informação e Comunicação 2019-2020.
- Solicitações de Auditoria.
- Regimento Geral do IFMS.

Causas:

- Dissonância entre o PDTIC e a estratégia institucional
- Falta de ações efetivas para implantação das melhores práticas de governança corporativa.

- Aprovação do PDTIC em atraso.
- Ausência de cultura organizacional com foco na gestão por resultados.
- Baixo envolvimento da Alta Administração em processos de governança de TI.

Consequências:

- Não atendimento das metas de desempenho de gestão.
- Potencial Ineficiência da área de TI.
- Potencial desvinculação dos objetivos da TI em relação aos objetivos estratégicos institucionais.
- Ineficiência da organização no alcance dos seus objetivos institucionais

Fato:

A equipe de auditoria cruzou informações referentes aos principais instrumentos de planejamento da instituição com o intuito de verificar a coerência e o grau de suporte entre os diferentes instrumentos nos diversos níveis de atuação (estratégico, tático e operacional), uma vez que para que as políticas e planos de TI tenham sucesso no alcance dos objetivos institucionais, é necessário que os instrumentos de planejamento e gestão estejam alinhados.

O plano estratégico é representado pelo Plano de Desenvolvimento Institucional (PDI), cujo plano vigente é referente ao quinquênio 2019 – 2023. Compõem o PDI o Mapa Estratégico e Plano de Metas, que servem de base para o desenvolvimento do Plano de Ação Anual (PAA) que tem sido o instrumento utilizado para desdobrar a missão institucional em objetivos estratégicos, iniciativas, indicadores e metas (tático e operacional).

No tocante à Tecnologia da Informação, o Plano Diretor de TIC (PDTIC) é o instrumento de gestão norteador das ações de TIC. Conforme já explicitado no presente relatório, **possui o dever de estar alinhado à Estratégia de Governo Digital e ao Plano Estratégico Institucional.**

Embora o PDTIC vigente indique o macro objetivo nº 4 do PDI como base, evidenciou-se que há uma baixa correlação entre as metas estratégicas constantes no PAE referentes aos três exercícios (2021, 2022 e 2023) e o PDTIC.

Tabela 3: Comparativo Metas PDTIC 2021-2023 X Metas Estratégicas PAE 2021-2023

METAS PDTIC	METAS ESTRATÉGICAS PAE 2023	METAS ESTRATÉGICAS PAE 2022	METAS ESTRATÉGICAS PAE 2021
M01 - Manter atualizado o parque de equipamentos e softwares de tecnologia da informação do IFMS.	4.2.6 Elaborar a Política de Integração dos Sistemas Computacionais do IFMS até 2021.	4.2.6 Elaborar a Política de Integração dos Sistemas Computacionais do IFMS até 2021.	4.2.6 Elaborar a Política de Integração dos Sistemas Computacionais do IFMS até 2021.
M02 - Implementar as ações previstas no Plano de Transformação Digital (PTD).	4.6.1 Criar portal de participação social para melhoria de políticas e serviços públicos, até 2023	4.6.1 Criar portal de participação social para melhoria de políticas e serviços públicos, até 2023	4.6.1 Criar portal de participação social para melhoria de políticas e serviços públicos, até 2023
M03 - Desenvolver competências em gestão de serviços de TIC.	4.6.3 Implementar um serviço digital por ano, a fim de estimular o uso e o acesso a serviços digitais.	4.6.3 Implementar um serviço digital por ano, a fim de estimular o uso e o acesso a serviços digitais.	4.6.3 Implementar um serviço digital por ano, a fim de estimular o uso e o acesso a serviços digitais.
M04 - Alcançar a quantidade máxima dentro do quadro necessário de servidores (conforme previsto nas tabelas 12 e 13).	4.6.4 Implantar 100% dos conjuntos de Dados Abertos, a partir de 2021, até 2022, contido no Plano de Dados Abertos do IFMS atualizado em 2020.	4.6.4 Implantar 100% dos conjuntos de Dados Abertos, a partir de 2021, até 2022, contido no Plano de Dados Abertos do IFMS atualizado em 2020.	4.6.4 Implantar 100% dos conjuntos de Dados Abertos, a partir de 2021, até 2022, contido no Plano de Dados Abertos do IFMS atualizado em 2020.
M05 - Desenvolver uma área de Governança de TI.			
M06 - Implantar funcionalidades específicas de cada área, de modo a atender suas demandas por meio de sistema.	4.6.5 Criar, até 2023, com o uso da Tecnologia da Informação e Comunicação (TIC), mecanismos para integração de sistemas visando promover a transparência e dar publicidade à aplicação de recursos públicos.	4.6.5 Criar, até 2023, com o uso da Tecnologia da Informação e Comunicação (TIC), mecanismos para integração de sistemas visando promover a transparência e dar publicidade à aplicação de recursos públicos.	4.6.5 Criar, até 2023, com o uso da Tecnologia da Informação e Comunicação (TIC), mecanismos para integração de sistemas visando promover a transparência e dar publicidade à aplicação de recursos públicos.
M07 - Alinhar as estratégias institucionais a Estratégia do Governo Digital (EGD).			

Fonte: Audit/IFMS

Por meio de Solicitações de Auditoria, a DIRTI foi questionada quanto a (i) metodologia de monitoramento do PDTIC; (ii) periodicidade de apuração das metas e indicadores; e (ii) nos casos de não atingimento, quais as providências tomadas e meios de reporte à alta administração. Em resposta a Dirti se manifestou nos seguintes termos:

> "*Em termos de metas e indicadores, é feita uma avaliação durante a elaboração do próximo PDTIC. No PDTIC atual, em seu capítulo 9, está anotado que 50% das metas do PDTIC anterior não foram totalmente atingidas. A cada ano, durante a elaboração do Plano Anual Específico (PAE) da DIRTI, são consideradas as metas e indicadores constantes no PDTIC. E a cada elaboração do Plano de Contratações Anual (PCA) institucional ou nova solicitação de compra/contratação de TIC, o PDTIC é consultado e, se preciso, revisado.*
> *Em caso de não atingimento de meta isso é relatado no novo texto do próximo PDTIC que vai via processo para consulta do CGD e por fim, deliberação do COSUP".*

Considerando a manifestação apresentada e os autos/informações disponíveis, constatou-se a **ausência de um processo formalizado e periódico de acompanhamento** dos resultados com finalidade de monitorar e avaliar a implementação das ações. Além disso, evidenciou-se que eventuais avaliações são feitas somente à época de elaboração do próximo PDTIC.

A metodologia utilizada não permite realizar avaliações concomitantes à execução para verificar o progresso das ações que possibilitem a identificação de possíveis desvios e subsidiem a tomada de decisão quanto à correção ou reavaliações dessas metas.

Outra fragilidade encontrada é a ausência de ações voltadas para avaliação e monitoramento contínuo da efetividade e desempenho da área de TIC com finalidade de verificar se os mecanismos implementados (estrutura, políticas, processos, etc.) estão sendo efetivos.

A Portaria SGD/ME nº 18.152/2020 dispõe que o PDTIC deve conter *"um processo de **acompanhamento formalizado** para monitorar e avaliar a implementação das ações, o uso dos recursos e a entrega dos serviços, com o objetivo de atender às estratégias e aos objetivos institucionais e, primordialmente, verificar o alcance das metas estabelecidas e, se necessário, estabelecer ações para corrigir possíveis desvios".*

Manifestação do Gestor: O relatório preliminar foi encaminhado à unidade auditada e a mesma não se manifestou até o fechamento do presente relatório.

Análise da Auditoria Interna: Diante da ausência de manifestação, deduz-se a concordância tácita por parte do gestor.

Recomendação 6: Instituir processo de acompanhamento formalizado para monitorar e avaliar a implementação das ações e verificar o alcance das metas previstas no PDTIC.

Benefício Esperado: Atender às estratégias e aos objetivos institucionais e, primordialmente, verificar o alcance das metas estabelecidas e, se necessário, estabelecer ações para corrigir possíveis desvios.

5. Estagnação institucional na capacidade e maturidade da governança de TI

Critérios:

- ABNT NBR ISO 38500:2009 – Governança corporativa de tecnologia da informação.
- Nota técnica nº 07/2014 Sefti/TCU de 30 de setembro de 2014.
- Decreto nº 9.203/2017.
- Acórdão nº 1684/2014 TCU- Plenário.
- Acórdão nº 2471/2008 TCU-Plenário.
- Portaria nº 778/2019.
- Acórdão nº 2.585/2012 TCU-Plenário

Evidências:

- Respostas às solicitações de auditoria.
- Resultado da reaplicação do questionário do IGG – Ciclo 2021 (autoavaliação).

Causas:

- Ausência de um sistema de governança de TI que coordene e oriente os esforços em nível adequado para o alcance dos objetivos.
- Baixo envolvimento da Alta Gestão no processo de planejamento de TI.
- Modelo da estratégia da organização não estabelecido.

Consequências:

- Estagnação institucional na capacidade e maturidade da governança de TI.
- Desalinhamento entre os objetivos da área de TI e os objetivos institucionais.
- Dificuldade na definição de diretrizes, objetivos, planos e ações, de critérios de priorização e alinhamento entre instituição e partes interessadas, para que os serviços alcancem o resultado pretendido.
- Tomada de decisão sem o suporte adequado.

Fato:

A maturidade da governança é aferida por meio da existência de mecanismos viabilizadores que proporcionam assegurar que a TI agregue valor ao negócio dentro de riscos aceitáveis. Esses mecanismos são as políticas, diretrizes, normas, estruturas organizacionais, processos e definição clara dos papéis.

Segundo o TCU, para que a TI seja bem governada, as seguintes condições devem ser satisfeitas, **sem exceção**: (i) ter uma forte estrutura de liderança que estabeleça os objetivos e a direção a seguir, sendo capaz de corrigir os possíveis desvios de rumo; (ii) estabelecer estratégias e planos que materializem a direção estabelecida, de forma a contribuir com o alcance dos objetivos da organização; (iii) dispor de informações tempestivas para subsidiar a tomada de decisão, bem como dar transparência das ações às partes interessadas; (iv) definir e estabelecer processos para implementar as políticas e entregar os resultados esperados, bem como para garantir a continuidade da ações; (v) dispor de pessoas capazes de fazer funcionar essa engrenagem organizacional de forma eficiente e efetiva.

Em seu instrumento de avaliação da Governança e Gestão Públicas (IGG), o TCU dispõe 20 itens para a governança e gestão de TIC, onde aborda práticas voltadas ao tema baseadas na legislação pertinente e boas práticas nacionais e internacionais.

O IFMS faz parte do rol de entidades participantes do IGG, tendo no último ciclo atingido estágio intermediário em Governança de TI e inicial em Gestão de TI.

Cumpre informar que o levantamento trata-se de uma autoavaliação com o intuito orientativo e pedagógico, sem avaliação *in loco* posterior por parte do TCU.

Após a aplicação do Ciclo 2021, esta Auditoria Interna do IFMS emitiu recomendações à gestão do IFMS com o objetivo de gerar maior aderência e incorporação das práticas pervistas no levantamento.

Com o intuito de verificar o atual estágio em relação à Governança e Gestão de TI, fora reaplicado o questionário do IGG – Ciclo 2021. Avaliou-se apenas as respostas apresentadas, não

sendo possível aferir os índices, uma vez que são formados por vários agregadores que para a correta aferição seria necessário aplicar o questionário completo.

Figura 4: Comparativo Reaplicação 2023 x Resultado do IGG 2021

4200. Gestão de Tecnologia da Informação e da Segurança da Informação			
Item	**Reaplicação IGG 2021 em 2023**	**Resultado do IGG 2021**	**Variação**
4210. Realizar Planejamento de Tecnologia da Informação			
4211.A organização executa processo de planejamento de tecnologia da informação	Adota em maior parte ou totalmente	Adota em maior parte ou totalmente	Estagnação
4212. A organização possui plano de tecnologia da informação vigente	Adota parcialmente	Adota parcialmente	Estagnação
4220. Gerir serviços de tecnologia da Informação			
4221. A organização elabora um catálogo de serviços de tecnologia da informação	Adota em maior parte ou totalmente	Adota em maior parte ou totalmente	Estagnação
4222. A organização executa processo de gestão de mudanças	Adota em menor parte	Adota parcialmente	Involução
4223. A organização executa processo de gestão de configuração e ativos (de serviços de tecnologia da informação)	Adota parcialmente	Adota em menor parte	Evolução
4224. A organização executa processo de gestão de incidentes de serviços de tecnologia da informação	Adota em menor parte	Adota em menor parte	Estagnação
4230. Gerir nível de serviço de tecnologia da informação			
4231. A área de gestão de tecnologia da informação acorda os níveis de serviço com as demais áreas de negócio internas à organização (Acordo de Nível de Serviço - ANS)	Não adota	Não adota	Estagnação
4240. Gerir riscos de tecnologia da informação			
4241. A organização executa processo de gestão dos riscos de tecnologia da informação relativos a processos de negócio	Adota em menor parte	Não adota	Evolução
4242. A organização executa processo de gestão de continuidade de serviços de tecnologia da informação	Não adota	Não adota	Estagnação
4250. Definir políticas de responsabilidades para a gestão da segurança da informação			
4251. A organização dispõe de uma política de segurança da informação	Adota em maior parte ou totalmente	Adota em maior parte ou totalmente	Estagnação
4252. A organização dispõe de comitê de segurança da informação	Adota em maior parte ou totalmente	Adota em maior parte ou totalmente	Estagnação
4253. A organização possui um gestor institucional de segurança da informação	Adota parcialmente	Adota parcialmente	Estagnação
4260. Estabelecer processo e atividades para a gestão da segurança da informação			
4261. A organização executa processo de gestão de riscos de segurança da informação	Adota em menor parte	Adota em menor parte	Estagnação
4262 - A organização executa processo de controle de acesso à informação e aos ativos associados à informação.	Adota em menor parte	Adota parcialmente	Involução

4263. A organização executa processo de gestão de ativos associados à informação	Adota em menor parte	Adota em menor parte	Estagnação
4264. A organização executa processo para classificação e tratamento de informações	Adota em menor parte	Adota em menor parte	Estagnação
4265. A organização executa processo de gestão de incidentes de segurança da informação	Adota em menor parte	Adota em menor parte	Estagnação
4266. A organização executa atividades de gestão da segurança dos recursos de processamento da informação, inclusive dos recursos de computação em nuvem	Adota em maior parte ou totalmente	Adota parcialmente	Evolução
4270. Executar processos de software			
4271. A organização executa um processo de software	Adota em menor parte	Adota parcialmente	Involução
4280. Gerir projetos de tecnologia da informação			
4281. A organização executa processo de gestão de projetos de tecnologia da informação	Adota em menor parte	Adota em menor parte	Estagnação

Fonte: Audit/IFMS

O resultado da reaplicação do questionário demonstra que houve estagnação ou involução em 85% dos itens, o que demonstra pouca ou nenhuma priorização à internalização das práticas preconizadas pelo TCU.

Quanto aos itens que apresentaram evolução, não foi possível evidenciar ações efetivas que representem a melhoria indicada, principalmente em relação à "gestão dos riscos de tecnologia da informação relativos a processos de negócio".

Manifestação do Gestor: O relatório preliminar foi encaminhado à unidade auditada e a mesma não se manifestou até o fechamento do presente relatório.

Análise da Auditoria Interna: Diante da ausência de manifestação, deduz-se a concordância tácita por parte do gestor.

Recomendação 7: Elaborar Plano de Ação para plena implementação das práticas preconizadas no questionário do IGG/TCU.

Benefício Esperado: Alinhamento às melhores práticas identificadas pelo Órgão de Controle Externo, visando o aumento da capacidade e maturidade da Governaça e Gestão de TIC.

6. Controles internos informais

Critérios:

- Boas práticas administrativas - Acórdão nº 1162/2013 – TCU Plenário, item 2.4.11: *"Em auditorias de avaliação de controles internos, os critérios são tipicamente baseados em bom senso e boas práticas administrativas".*
- Metodologia COSO (*Committee of Sponsoring Organizations of the Treadway Commission*) de avaliação dos controles internos e gerenciamento de riscos. Instrução Normativa/CGU nº 3/2017 (revogada parcialmente): "82. A avaliação dos controles internos da gestão deve considerar os seguintes componentes: ambiente de controle, avaliação de riscos, atividades de controle, informação e comunicação e atividades de monitoramento."
- Instrução Normativa Conjunta MP/CGU nº 01/2016.
- Decreto nº 9.203/2017.
- Decreto-Lei nº 200/1967.
- Instrução Normativa GSI/PR nº 3 de 28 de maio de 2021.
- Instrução Normativa GSI/PR nº 01/2020.
- Acórdão nº 1.603/2008 TCU-Plenário.
- ABNT NBR ISO 31.000:2009 –Gestão de Riscos – Princípios e diretrizes.
- Norma Complementar 04/IN01/DSIC/GSI/PR.
- Lei nº 14.129/2021.
-

Evidências:

- Respostas às Solicitações de Auditoria.
- Página institucional
- Resultado da avaliação da Auditoria Interna - Metodologia COSO

Causas:

- Ausência de cultura organizacional
- Ausência de mapeamento de macroprocessos finalísticos e de apoio à governança
- Ausência de Gestão de Riscos
- Fragilidade da Gestão da Segurança da Informação
- Ausência de fluxos, manuais ou instruções formalizadas
- Posic como mera formalidade (não implementação de itens relevantes que estão previstos na Posic).

- Descontinuidade do CSTIC.
- Ausência de definição das competências do Gestor de segurança da informação.
- Ausência de arcabouço de Governança de TI.
- Fragilidades na 1ª e 2ª linhas de defesa.
-

Consequências:

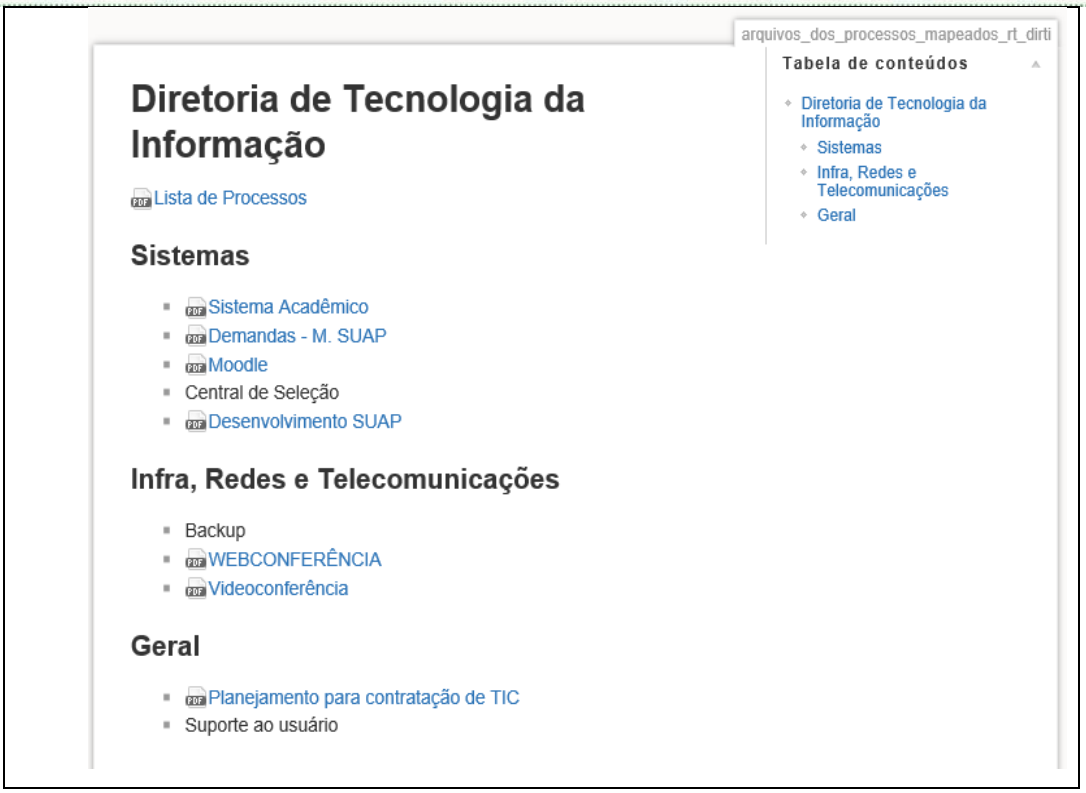
- Desconhecimento sobre os esforços necessários para alcançar os resultados almejados, esforços desnecessários ou ineficientes.
- Ausência de critérios objetivos para definição de indicadores e metas.
- Dificuldade em obter visão integrada de todas as atividades do processo, com objetivo de identificar as informações, os fluxos e as partes envolvidas.
- Não tratamento à exposição aos riscos

Fato:

No âmbito dos controles internos, verificou-se a ausência de controles formais e padronizados voltados à area de TI e, principalmente, à segurança de TI. Não existem processos mapeados suficientes tampouco mapeamento dos riscos. Verificou-se a centralização de funções em poucos servidores, o que aumenta o risco de eventuais erros e fraudes.

Quanto aos processos, segundo consta na página da Diretoria de Planejamento e Gestão do Conhecimento (Dipla/Prodi), estão disponibilizados 7 processos mapeados, sendo 6 de sistemas operacionais e 1 de planejamento de contratação. Não foi identificado mapeamento do macroprocesso de governança e de gestão de TI, de modo a ter uma visão estratégica do ciclo da governança - avaliar, direcionar e monitorar, e do ciclo da função de gestão - planejar, executar, controlar e agir. Assim como verificou-se a ausência dos mapeamentos dos processos de apoio, tais como, mapeamento do processo do PDTIC, de riscos, de segurança da informação (plano de contingência/continuidade, cópias de segurança, gestão de mudanças, gestão de incidentes, classificação e tratamento de informações e de gestão da segurança dos recursos de processamento da informação).

Figura 5: Mapeamento dos processos Dirti



Fonte: Mapeamento processos- Dipla/IFMS

Em relação aos riscos, questionou-se a Dirti sobre (i) a existência de politica de gestão de riscos, (ii) as práticas adotadas para a sistematização relacionadas a gestão de riscos, (iii) os principais riscos que a área de TI está exposta e (iv) os controles internos associados a estes riscos. Em resposta, foi informado que:

> *"Hoje não temos uma Política de Gestão de Riscos de TI ou da DIRTI. O que temos é um capítulo no PDTIC 2021-2023, o capítulo "14. Plano de Gestão de Riscos", no qual tratamos deste assunto de uma forma breve.*
> *(...)*
> *No capítulo "14. Plano de Gestão de Riscos" do PDTIC 2021-2023 temos a tabela 18 onde foram identificados os principais riscos da não execução do PDTIC, ou seja, da não execução/adoção de um planejamento de TI institucional".*

A resposta apresentada corrobora apontamentos constantes desta Unidade de Auditoria Interna Governamental em seus relatórios e pareceres quanto à inexistência do Gerenciamento de Riscos institucional. Destacamos ainda que **a gestão de riscos da área de TIC <u>não se confunde</u> com os riscos de execução do PDTIC**, tendo em vista que, em uma visão geral, a gestão de riscos envolve identificação, análise, avaliação, tratamento e monitoramento destes riscos que possam

impactar os objetivos institucionais, em consonância com o disposto no art. 48 da lei nº 14.129/2021:

> "*Os órgãos e as entidades deverão estabelecer, manter, monitorar e aprimorar sistema de gestão de riscos e de controle interno com vistas à identificação, à avaliação, ao tratamento, ao monitoramento e à análise crítica de riscos da prestação digital de serviços públicos que possam impactar a consecução dos objetivos da organização no cumprimento de sua missão institucional e na proteção dos usuários*".

Quanto à Segurança da Informação (SI), considerando as respostas ao questionário de autoavaliação do IGG, embora no quesito "definir políticas de responsabilidades para a gestão da segurança da informação" o IFMS encontre-se em nível "**aprimorado**" (benefício decorrente de atendimento às recomendações do Relatório de Auditoria nº 11/2017 AUDIT/IFMS, quando foi atualizada a Política de Segurança da Informação e designado o Gestor de Segurança da Informação e Comunicações do IFMS), a prática "estabelecer processo e atividades para a gestão da segurança da informação" recebeu classificação "**iniciando"**, o que demonstra dissonância entre a teoria e a prática, resultando em características pró forma das políticas institucionais.

Nesse sentido, apesar de terem sido constatada a existência de iniciativas para implementação da Segurança da Informação, verificou-se a ausência de mecanismos com enfoque na **execução,** devendo ser priorizada a sua implementação com ações capazes de produzir seus efeitos na prática que garantam em níveis aceitáveis que a instituição irá cumprir seus objetivos mesmo em face de sinistros.

Evidenciou-se, ainda, falhas nos processos de (i) gestão de riscos de Segurança da Informação, (ii) de controle de acesso, (iii) de gestão de ativos, (iv) classificação e tratamento de informações, (v) gestão de incidentes de segurança da informação, (vi) atividades de gestão da segurança dos recursos de processamento da informação, conforme destacados abaixo os itens do questionário:

Item	**Resposta**
A organização executa processo de gestão de riscos de segurança da informação	Adota em menor parte
Avaliação da Auditoria Interna	
A unidade não apresentou evidências das ações de controles que realiza, estando em desacordo com o que determina o decreto nº 9.637/2018 (*"V - **estabelecer diretrizes para o processo de gestão de riscos de segurança da informação**; VII implementar **controles internos** fundamentados na gestão de riscos da segurança da informação; VIII instituir um **sistema de gestão de segurança da informação**"),* bem como determina a Instrução Normativa GSI/PR nº 03/2021 art. 3º *("A gestão de segurança da informação será constituída pelos seguintes*	

processos de ***realização obrigatória pelos órgãos e pelas entidades da administração pública federal****; II- gestão de riscos de segurança da informação"*).

A Instrução Normativa determina que o processo de gestão de riscos de SI deverá fornecer:

1. *Plano de gestão de riscos de segurança da informação;*
2. *Relatório de identificação, análise e avaliação dos riscos de segurança da informação; e*
3. *Relatório de tratamento de riscos de segurança da informação.*

É importante pontuar que é de competência da alta administração a governança de segurança da informação e estabelecer as diretrizes para o processo de GRSI, cabendo ao Gestor de SI coordenar conforme determina art. 16 que cabe ao gestor de segurança da informação de cada órgão ou entidade:

I - Coordenar a gestão de riscos de segurança da informação;
II - Designar o agente responsável pela gestão de riscos de segurança da informação, dentre os servidores efetivos do órgão;
III - Aprovar o plano de gestão de riscos de segurança da informação;
IV - Aprovar o relatório de identificação, análise e avaliação dos riscos de segurança da informação e encaminhá-lo à alta administração;
V - Aprovar o relatório de tratamento de riscos de segurança da informação; e
VI - Propor medidas preventivas à alta administração.

Item	**Resposta**
A organização executa processo de controle de acesso à informação e aos ativos associados à informação	Adota em menor parte
Avaliação da Auditoria Interna	
O Acórdão 2831/2011 TCU - Plenário recomendou que as organizações definam uma política de controle de acesso a informações e recursos de TI, com base nos requisitos de negócio e de segurança da informação da entidade.	
Item	**Resposta**
A organização executa processo de gestão de ativos associados à informação	Adota em menor parte
Avaliação da Auditoria Interna	

Quanto a esse aspecto, a Dirti informou que mantém um inventário dos ativos associados à informação, contudo não apresentou evidências. O que se observou é a ausência de formalização de gestão de ativos, orientações quanto à execução do processo, definição das responsabilidades, avaliações periódicas de desempenho e conformidade de gestão dos ativos. Conforme estabelece a IN GSI/PR nº 03/2021 a gestão da SI é de realização obrigatória pelos órgãos e entidades da APF:

I - mapeamento de ativos de informação;
II - gestão de riscos de segurança da informação;

III - gestão de continuidade de negócios em segurança da informação;
IV - gestão de mudanças nos aspectos de segurança da informação; e
V - avaliação de conformidade de segurança da informação.

A Instrução Normativa supracitada dispõe que o mapeamento de ativos e informação tem como objetivo de estruturar e manter um registro de ativos de informação, destinado a subsidiar os processos de gestão de riscos, de gestão de continuidade e de gestão de mudanças e **cabe ao Gestor de SI coordenar o processo de mapeamento de ativos de informação**, bem como designar um agente responsável pela gestão de ativos de informação, dentre os servidores efetivos.

A NBR ISO/IEC 17799/2005 estabelece que convém que todos os ativos sejam inventariados e tenham um proprietário responsável. Que os proprietários dos ativos sejam identificados e a eles seja atribuída a responsabilidade pela manutenção apropriada dos controles. A implementação de controles específicos pode ser delegada pelo proprietário, conforme apropriado, porém o proprietário permanece responsável pela proteção adequada dos ativos.

Item	Resposta
A organização executa processo para classificação e tratamento de informações	Adota em menor parte

Avaliação da Auditoria Interna

Nesse tópico também não foram apresentadas evidências. O Acórdão 1.603/2008 preceitua que a classificação de informações, por sua vez, é um dos pilares da segurança da informação numa organização, sendo o processo que visa garantir que cada informação tenha o tratamento de segurança adequado ao seu valor, aos requisitos legais, à sensibilidade e aos riscos de sua perda para a organização. Nesse processo devem existir, pelo menos, dois documentos de referência: o esquema de classificação, que contém as definições dos níveis de proteção considerados, e um conjunto apropriado de procedimentos para rotulação e tratamento da informação segundo esse esquema. A sua ausência indica que o tratamento da segurança sobre as informações não é feito de forma consistente.

A IN nº 01/2020 também determina as diretrizes mínimas que a PoSIC das entidades deve conter no art. 12:

"IV- Diretrizes gerais: estabelece diretrizes sobre a implementação, no mínimo, dos seguintes temas:
a) Tratamento da Informação;
b) Segurança Física e do Ambiente;
c) Gestão de Incidentes em Segurança da Informação;
d) Gestão de Ativos;
e) Gestão do Uso dos Recursos Operacionais e de Comunicações, como: e-mail, acesso à internet, mídias sociais, computação em nuvem, dentre outros;
f) Controles de Acesso;
g) Gestão de Riscos;
h) Gestão de Continuidade; e

i) Auditoria e Conformidade".

Item	Resposta
A organização executa processo de gestão de incidentes de segurança da informação	Adota em menor parte

Avaliação da Auditoria Interna

A unidade auditada não apresentou as evidências, cabe frisar que esse tema "Segurança da Informação" já foi objeto de trabalho de auditoria realizado em 2017 e foi apontada a seguinte fragilidade: **Ausência da instituição de equipe de tratamento e resposta a incidentes em redes computacionais**, e até o momento do fechamento destes achados de auditoria não foi atendida a recomendação que se encontra expirada desde 04/06/2021. Estando em desacordo com o que determina o Decreto nº 9.637/2018 o qual dispõe como um dos princípios da Política Nacional de Segurança da Informação (PNSI) "prevenção e tratamento de incidentes de segurança da informação" e determina à alta administração " instituir um sistema de gestão de segurança da informação e **implantar mecanismo de comunicação imediata sobre a existência de vulnerabilidades ou incidentes de segurança que impactem ou possam impactar os serviços** prestados ou contratados pelos órgãos da administração pública federal". (grifo nosso)

Assim como a Instrução Normativa nº 01/2020 PR/GSI que estabelece que os órgãos da Administração Pública Federal devem "instituir e implementar Equipe de Tratamento e Resposta a Incidentes Cibernéticos - ETIR, que constituirá a rede de equipes, integrada pelos órgãos e pelas entidades da administração pública federal, coordenada pelo Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo do Gabinete de Segurança Institucional da Presidência da República", e que a estrutura para a gestão da segurança da informação deverá designar ou instituir, ao menos, uma Equipe de Tratamento e Resposta a Incidentes Cibernéticos (ETIR) ou estrutura equivalente.

Ainda sobre a equipe de tratamento e respostas a incidentes cibernéticos a IN n° 01/2020 no art. 22 preceitua:

> "*Todos os órgãos e entidades que possuem a competência de administrar a infraestrutura de rede de sua organização deverão criar uma Equipe de Tratamento e Resposta a Incidentes Cibernéticos".*

Item	Resposta
A organização executa processo de gestão de continuidade de serviços de tecnologia da informação	Não adota

Avaliação da Auditoria Interna

Em resposta à Solicitação de Auditoria nº 01/2023 a unidade auditada informou que não dispunha de um plano de continuidade instituído, em desconformidade com a Instrução Normativa GSI/PR nº 03/2021 "O processo de gestão de continuidade de negócios em segurança da informação **deve ser baseado nas estratégias de continuidade para as atividades críticas, na avaliação dos riscos levantados no processo de gestão de riscos** em diretrizes institucionais sobre gestão de continuidade de negócio".

A POSIC por determinação legal prevê a gestão da continuidade e que cabe ao CSTIC, com a participação

da Dirti, manter um Programa de Gestão da Continuidade de Negócios.

A IN 03/2021 art. 25 "O gestor de segurança da informação coordenará o processo de gestão de continuidade de negócios em segurança da informação nos seus respectivos órgãos ou entidades, bem como designará um agente responsável pela referida gestão, dentre os servidores efetivos do órgão".

A Instrução normativa nº 01 de 27 de maio de 2020 também trata desse assunto determina as diretrizes mínimas que a POSIC das entidades deve possuir incluindo a **gestão de continuidade**.

Por fim, o Acórdão nº 1.603/2008 TCU-Plenário prevê que "*O plano (ou planos) de continuidade deve (m) ser periodicamente testado (s) e avaliado(s), para garantir que funcione(m) quando necessário".*

Item	Resposta
A organização executa atividades de gestão da segurança dos recursos de processamento da informação, inclusive dos recursos de computação em nuvem	Adota em maior parte ou totalmente

Avaliação da Auditoria Interna

A DIRTI em resposta ao questionário informou *"inventariamos ativos conectados à rede e softwares presentes neles, conforme prints do sistema sd.ifms.edu.br. Também mantemos, monitoramos e analisamos (se preciso), logs de ativos e de rede (firewall - panorama). Com a recente atualização do firewall temos uma defesa de perímetro de rede atualizada, controlamos e limitamos portas, protocolos e serviços de rede. E também com a solução de backup adquirida, temos cópias de segurança dos principais serviços e sistemas institucionais*". Ressaltamos que não foram apresentadas evidências das práticas adotadas.

O Acórdão nº 3.369/2015 TCU - Plenário deliberou sobre esse tema "*É recomendável a elaboração, e atualização, de um documento que defina diretrizes e procedimentos de rotina para gerar cópias de segurança dos dados que possibilitem sua recuperação em tempo aceitável em caso de perda, conforme recomenda o item 10.5.1 da NBR ISO/IEC 27002:2005*".

Ademais, como supramencionadas as diretrizes mínimas, uma delas "Gestão do uso dos recursos operacionais e de comunicações, como: e-mail, acesso à internet, mídias sociais, computação em nuvem, dentre outros".

Isto posto, acrescentamos ainda, no contexto da governança da segurança da informação, as competências da alta administração expressas pelo art. 17 do Decreto nº 9.637/2018, destacamos especialmente sobre a necessidade de "monitorar o desempenho e avaliar a concepção, a implementação e os resultados da sua política de segurança da informação e das normas internas de segurança da informação".

Outra fragilidade encontrada refere-se ao gestor de Segurança da Informação, tendo em vista a insuficiência das atribuições estando em desacordo com a determinação legal, assim como a ausência de definição dos meios de comunicação e a quem o gestor se reporta internamente.

Por fim, a inexistência de formalização de geração de cópias de segurança (*backup*) por meio de política ou instrumento congênere de forma a proporcionar a padronização em relação ao escopo dos dados, requisitos alinhados aos objetivos institucionais, definições das janelas, periodicidade, revisão, testes, dentre outros.

Manifestação do Gestor: O relatório preliminar foi encaminhado à unidade auditada e a mesma não se manifestou até o fechamento do presente relatório.

Análise da Auditoria Interna: Diante da ausência de manifestação, deduz-se a concordância tácita por parte do gestor.

Recomendação 8: Mapear macroprocesso de governança de TIC (ciclo avaliar, direcionar e monitorar).

Recomendação 9: Mapear os processos de gestão de TIC (função planejar, executar e controlar).

Recomendação 10: Mapear os processos do PDTIC (elaboração e acompanhamento).

Recomendação 11: Mapear o processo de gestão de riscos relativos a TIC e de SI.

Recomendação 12: Mapear o macroprocesso de segurança da informação (contendo, no mínimo: gerenciamento de ativos associados à informação, gerenciamento de incidentes, gestão de riscos, cópias de segurança, gestão da continuidade, gestão de mudanças, controles de acesso, classificação e tratamento de informações, segurança de serviços de nuvem).

Benefícios Esperados: Apoiar a identificação das etapas, dos responsáveis, das atribuições, dos controles existentes, das oportunidades de melhoria, das lacunas, dos gargalos e dos possíveis riscos ao atingimento dos objetivos, inclusive riscos de fraude e riscos relacionados à TI. Mapear possibilidades de redefinições de fluxos que podem aumentar a eficiência e a segurança de um processo de trabalho. Possibilitar a identificação de fragilidades e potenciais riscos, contribuindo ainda para a adoção de medidas para mitigá-los. Identificar todas as etapas, fluxos e objetivos de um determinado processo da organização. Apoiar a tomada de decisão e a elaboração do planejamento estratégico. Direcionar e controlar o risco de SI e adequá-los aos níveis aceitáveis para a instituição. Assegurar que os responsáveis pela tomada de decisão tenham acesso tempestivo quanto aos riscos aos quais está exposta. Aumentar a probabilidade de alcançar os objetivos. Direcionar e controlar o risco de SI e adequá-los aos níveis aceitáveis para a intuição. Agregar valor à instituição.

Recomendação 13: Realizar o processo de mapeamento/levantamento de ativos da informação.

Benefícios Esperados: Saber quais dados são essenciais para a instituição. A gestão adequada de

ativos ajudará a identificar os ativos institucionais que mantêm ou gerenciam esses dados críticos para que as medidas de segurança apropriadas possam ser aplicadas. Subsidiar os processos de gestão de riscos, de gestão de continuidade e gestão de mudanças relativos à SI.

Recomendação 14: Elaborar um plano de gestão de continuidade/contingência em SI.

Benefícios Esperados: Identificar proativamente impactos de uma interrupção operacional. Minimizar os impactos decorrentes de falhas, desastres ou indisponibilidades significativas. Recuperar perda de ativos de informação em nível aceitável. Administrar a contingência quando houver interrupção de atividades.

Recomendação 15: Promover o processo gestão de mudanças de Segurança da Informação.

Benefícios Esperados: Preparar e adaptar a instituição para mudanças decorrentes da evolução de processos e de tecnologias.

Recomendação 16: Instituir e gerir equipe de Tratamento e Resposta a Incidentes Cibernéticos (ETIR) ou estrutura equivalente.

Benefícios Esperados: Identificar ameaças na instituição, responder a elas antes que possam se espalhar e remediá-las antes que possam causar danos.

Recomendação 17: Elaborar periodicamente relatório de identificação, análise e avaliação dos riscos de SI e relatório de tratamento de riscos de Segurança da Informação.

Benefícios Esperados: Manter as instâncias informadas para que as respostas aos riscos sejam apropriadas.

Recomendação 18: Monitorar o desempenho e avaliar a concepção, a implementação e os resultados da sua política de segurança da informação.

Benefícios Esperados: Garantir que a direção estabelecida seja cumprida e que os ajustes de percurso sejam realizados para evitar que os riscos impeçam ou prejudiquem a consecução dos objetivos. Gerar insumos para avaliação.

Recomendação 19: Reformular normativo interno de atribuições do gestor de Segurança da Informação para atendimento art. 10, 19, 21 da IN GSI/PR nº 01/2020 art. 8, 14, 16, 25, 35, 41 e

42 da IN GSI/PR nº 03/2021 além das já previstas na portaria de designação do gestor.

Benefícios Esperados: Promover as ações de segurança da informação.

Recomendação 20: Instituir processo de avaliação de conformidade nos aspectos de segurança da informação.

Benefícios Esperados: Proporcionar adequado grau de confiança mediante atendimento dos requisitos definidos na legislação vigente.

Recomendação 21: Normatizar plano de gestão para cópias de segurança (backups).

Benefícios Esperados: Promover a implantação de mecanismos que possibilitem a continuidade do negócio contra interrupções e falhas.

Recomendação 22: Formalizar e promover a gestão de tratamento e classificação da informação em consonância com a Lei nº 12.527/2011.

Benefícios Esperados: Assegurar que a informação receba nível adequado de proteção.

5. RECOMENDAÇÕES CONSOLIDADAS

Número da Recomendação	Recomendação	Setor responsável
1 Prazo: **30.05.2024**	Implementar sistema formalizado e sistêmico de governança de TI (políticas e diretrizes de governança, estrutura e conjunto de mecanismos viabilizadores necessários para avaliar, dirigir e monitorar a gestão da TI no IFMS).	IFMS
2 Prazo: **30.05.2024**	Definir as competências, composição e funcionamento do Comitê de Governança Digital (CGD) em regimento próprio.	IFMS
3 Prazo: **30.05.2024**	Reformular a composição do CSTIC, em atendimento ao art. 21 da Instrução Normativa GSI nº 01/2020.	IFMS
4 Prazo: **30.05.2024**	Promover a transparência da área de TI, por meio da concentração das informações na página da Dirti, tais como o PDTIC, informações relativas aos comitês, normativos, agenda e atas das reuniões.	DIRTI
5 Prazo: **30.05.2024**	Definir rotina formalizada de elaboração do PDTIC (contendo, no mínimo, prazos, responsáveis e instâncias de aprovação e revisão).	DIRTI

6 Prazo: **30.05.2024**	Instituir processo de acompanhamento formalizado para monitorar e avaliar a implementação das ações e verificar o alcance das metas previstas no PDTIC.	DIRTI
7 Prazo: **30.05.2024**	Elaborar Plano de Ação para plena implementação das práticas preconizadas no questionário do IGG/TCU.	DIRTI
8 Prazo: **30.05.2024**	Mapear macroprocesso de governança de TIC (ciclo avaliar, direcionar e monitorar).	DIRTI
9 Prazo: **30.05.2024**	Mapear os processos de gestão de TIC (função planejar, executar e controlar).	DIRTI
10 Prazo: **30.05.2024**	Mapear os processos do PDTIC (elaboração e acompanhamento).	DIRTI
11 Prazo: **30.05.2024**	Mapear o processo de gestão de riscos relativos a TIC e de SI.	DIRTI
12 Prazo: **30.05.2024**	Mapear o macroprocesso de segurança da informação (contendo, no mínimo: gerenciamento de ativos associados à informação, gerenciamento de incidentes, gestão de riscos, cópias de segurança, gestão da continuidade, gestão de mudanças, controles de acesso, classificação e tratamento de informações, segurança de serviços de nuvem).	DIRTI

13 Prazo: **30.05.2024**	Realizar o processo de mapeamento/levantamento de ativos da informação.	DIRTI
14 Prazo: **30.05.2024**	Elaborar um plano de gestão de continuidade/contingência em SI.	DIRTI
15 Prazo: **30.05.2024**	Promover o processo gestão de mudanças de Segurança da Informação.	DIRTI
16 Prazo: **30.05.2024**	Instituir e gerir equipe de Tratamento e Resposta a Incidentes Cibernéticos (ETIR) ou estrutura equivalente.	DIRTI
17 Prazo: **30.05.2024**	Elaborar periodicamente relatório de identificação, análise e avaliação dos riscos de SI e relatório de tratamento de riscos de Segurança da Informação.	DIRTI
18 Prazo: **30.05.2024**	Monitorar o desempenho e avaliar a concepção, a implementação e os resultados da sua política de segurança da informação.	DIRTI
19 Prazo: **30.05.2024**	Reformular normativo interno de atribuições do gestor de Segurança da Informação (para atendimento art. 10, 19, 21 da IN GSI/PR nº 01/2020 art. 8, 14, 16, 25, 35, 41 e 42 da IN GSI/PR nº 03/2021, além das já previstas na portaria de designação do gestor).	DIRTI

20 Prazo: **30.05.2024**	Instituir processo de avaliação de conformidade nos aspectos de segurança da informação.	DIRTI
21 Prazo: **30.05.2024**	Normatizar plano de gestão para cópias de segurança (backups).	DIRTI
22 Prazo: **30.05.2024**	Formalizar e promover a gestão de tratamento e classificação da informação em consonância com a Lei nº 12.527/2011.	DIRTI

6. CONCLUSÃO DA EQUIPE DE AUDITORIA

Considerando o trabalho desenvolvido, desde a etapa de planejamento até a fase de elaboração do relatório, conclui-se que os objetivos delineados para esta ação foram alcançados. Obteve-se resposta para todas as questões de auditoria propostas, com participação ativa do setor envolvido, subsidiando a análise da equipe de auditoria.

O objetivo geral da ação foi avaliar a maturidade da governança e gestão de TI do IFMS. Para tanto, buscou-se informações e evidências da (i) existência dormal de estrutura de Governança e Gestão de TI, para assim (ii) avaliar-se o nível de maturidade da mesma. Por fim, avaliou-se os (iii) mecanismos de controles internos existentes nos processos.

Em relação à primeira questão de auditoria, concluiu-se que a estrutura de Governança e Gestão de TI não está formalmente instituída em sua completude, possuindo lacunas relacionadas à definição das diretrizes, papéis e responsabilidades; valores, processos e estruturas necessárias para que as atividades de governança **avaliar, dirigir e monitorar**, bem como as interfaces entre as funções de governança e gestão de TI sejam desempenhadas de forma eficaz, de modo a possibilitar que a instituição alinhe seus objetivos ao interesse público, gerencie seus riscos e entregue o valor esperado de forma íntegra, transparente e responsável.

Quanto ao nível de maturidade, por meio da reaplicação do questionário de autoavaliação do IGG – Ciclo 2021, verificou-se estagnação ou involução em 85% das práticas preconizadas para a Governança e Gestão de TI, sendo que nos itens que houve evolução não foi possível evidenciá-la na prática.

Por fim, em relação aos controles internos, não foi possível evidenciar a existência de procedimentos de controles estruturados que sejam capazes de fornecer segurança razoável de que os processos relacionados à governança e gestão de Tecnologia da Informação e Comunicação estejam pautados em ambiente íntegro e confiável que promova a eficiência, efetividade e eficácia para atingimento dos objetivos institucionais.

Também foram identificadas vulnerabilidades na gestão de riscos diante da ausência de uma política de gestão de riscos e de diretrizes para efetivação do processo de gestão de riscos e de

segurança da informação de maneira formal de modo a manter a Alta Gestão informada dos riscos relevantes que podem impactar a instituição e que as respostas aos riscos sejam apropriadas.

Alertamos para fragilidades na segurança da informação, diante da ausência de equipe de tratamento e resposta a incidentes cibernéticos (ETIR), ausência de plano de contingência/continuidade de forma a identificar proativamente impactos de uma interrupção operacional, minimizar os impactos decorrentes de falhas, desastres ou indisponibilidades significativas, bem como recuperar perda de ativos de informação em nível aceitável.

Em que pese o setor auditado não ter mencionado os recursos humanos nas respostas às Solicitações de Auditoria, esta equipe de auditoria entende que a recomposição e planejamento de fortalecimento e valorização da equipe de TI deve ser priorizada pela Alta Gestão do IFMS.

Desta forma, foram emitidas recomendações no intuito de contribuir para a estruturação da governança da tecnologia da informação. As referidas recomendações serão cadastradas no sistema de gestão da Atividade de Auditoria Interna Governamental (e-Aud) e terão as suas implementações acompanhadas mediante monitoramento no próprio sistema.

Ressaltamos que esta ação não tem a intenção de esgotar as possibilidades de inconsistências que possam ser observadas, mas sim, servir como orientação para as boas práticas da Administração Pública. As ações da Auditoria Interna devem ser entendidas como de caráter essencialmente preventivo, destinadas a agregar valor e a melhorar as operações da entidade, assistindo-a na consecução de seus objetivos mediante uma abordagem sistemática e disciplinada, fortalecendo a gestão e racionalizando as ações de Controle Interno.

Campo Grande, 22 de janeiro de 2024

Unidade de Auditoria Interna Governamental
AUDIT/IFMS