INSTITUTO FEDERAL
Santa Catarina

RELATÓRIO DE AVALIAÇÃO

Área auditada: Governança de TIC

Exercício 2023

8 de novembro de 2023

Instituto Federal de Santa Catarina (IFSC)
Auditoria Interna (Audin)

RELATÓRIO DE AVALIAÇÃO
Unidade Auditada: **Diretoria de Tecnologia da Informação e Comunicação**
Município/UF: Florianópolis/SC
Relatório de Avaliação: 01/2023

Missão

Adicionar valor e melhorar as operações do IFSC, auxiliando-o a realizar seus objetivos, a partir da aplicação de uma abordagem sistemática e disciplinada para avaliar e melhorar a eficácia dos processos de governança, de gerenciamento de riscos e de controles internos, em benefício da sociedade.

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 AUDIN?

Foi realizada ação de auditoria para avaliação da governança de Tecnologia da Informação e Comunicação (TIC) no Instituto Federal de Educação Ciência e Tecnologia de Santa Catariana (IFSC).

O objetivo principal da auditoria foi avaliar se a Instituição está adotando as melhores práticas de governança de TIC com vistas a auxiliar o IFSC no cumprimento de sua missão institucional.

A abordagem adotada pela Audin objetivou responder, dentre outras questões secundárias, as seguintes questões de Auditoria:

Existem políticas e diretrizes definidas para governança e gestão de tecnologia da informação?

Existe acompanhamento, avaliação dos resultados e objetivos de TIC?

As necessidades relacionadas ao desenvolvimento de pessoas e à força de trabalho da área de TI são gerenciadas?

POR QUE A AUDIN REALIZOU ESSE TRABALHO?

A escolha dos temas a serem auditados é realizada durante a construção do Planejamento Anual das Atividades de Auditoria Interna (PAINT), onde é estabelecida uma relação de temas auditáveis que são avaliados por meio da matriz de risco. Tal avaliação tem por base critérios considerados importantes para a auditoria, tais como: relevância, materialidade, criticidade e oportunidade. O tema "Governança de TIC" foi escolhido em virtude dos riscos inerentes aos processos, que foram pontuados no PAINT/2023 considerando os seguintes fatores: a relevância do processo tanto na atividade finalística quanto na atividade-meio do IFSC, a ausência de ações de auditoria no tema nos últimos 10 anos, dentre outros fatores relevantes.

QUAIS AS CONCLUSÕES ALCANÇADAS PELA AUDIN? QUAIS AS RECOMENDAÇÕES QUE DEVERÃO SER ADOTADAS?

Os trabalhos de auditoria revelaram que a Instituição precisa realizar ações imediatas na sua governança de TIC. Isso porque os trabalhos de auditoria evidenciaram que faltam diretrizes claras para avaliação da governança, da gestão e do desempenho dos serviços de TIC, e principalmente, ausência de avaliação e monitoramento dos processos de governança, e resultados dos objetivos estratégicos de TIC.

Diante disso foram emitidas, **dentre outras**, as seguintes recomendações para superação das inconsistências: Aprovar diretrizes para avaliação da governança, da gestão e do desempenho dos serviços de TIC. Elaborar e publicar relatório, pelo menos anual, contendo avaliação dos serviços produzidos pela TIC, monitoramento dos objetivos estratégicos de TIC e demais diretrizes definidas na recomendação 2.

LISTA DE SIGLAS E ABREVIATURAS

APF	Administração Pública Federal
AUDIN	Auditoria Interna do IFSC
CGD/ME	Comitê de Governança Digital/Ministério da Economia
COBIT	Control Objectives for Information and related Technology
GSI	Gabinete de Segurança Institucional
IFSC	Instituto Federal de Educação, Ciência e Tecnologia de Santa Catarina
PAINT	Plano anual das Atividades de Auditoria Interna
PDI	Plano de Desenvolvimento Institucional
PDTIC	Plano Diretor de Tecnologia da Informação e Comunicação
PETIC	Plano Estratégico de Tecnologia da Informação e Comunicação
POSIC	Política de Segurança da Informação e Comunicação
SGD/ME	Secretaria de Governo Digital/Ministério da Economia
SISP	Sistema de Administração dos Recursos de Tecnologia da Informação
TCU	Tribunal de Contas da União
TIC	Tecnologia da Informação e Comunicação

SUMÁRIO

INTRODUÇÃO

A governança de TIC desempenha um papel fundamental em uma instituição governamental, pois garante a eficiência, transparência e prestação de serviços de qualidade aos cidadãos. Uma sólida estrutura de governança de TIC ajuda a gerenciar recursos, mitigar riscos de segurança, promover a inovação e garantir o alinhamento dos sistemas de informação com os objetivos estratégicos institucionais. Além disso, ao estabelecer diretrizes, políticas e processos para a gestão de TIC, as instituições governamentais podem otimizar o uso de recursos públicos, proteger dados sensíveis e, por fim, construir uma administração mais eficaz e responsiva às necessidades da sociedade. Portanto, a governança de TIC não é apenas uma opção, mas uma necessidade imperativa para garantir a prestação de serviços públicos eficazes e a construção de uma administração pública moderna e confiável.

Nos órgãos e entidades do Poder Executivo Federal, a governança de TIC deve ser implementada seguindo as orientações do Guia e Governança de TIC do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP) que foi instituído pelo Decreto nº 7.579, de 11 de outubro de 2011, com o objetivo de organizar a operação, controle, supervisão e coordenação dos recursos de tecnologia da informação da administração direta, autárquica e fundacional do Poder Executivo Federal.

Nesse contexto, e ciente dos benefícios que uma boa governança de TIC é capaz de proporcionar, a Audin realizou esta ação de auditoria que originou-se a partir da aplicação de matriz de riscos que compôs o PAINT/2023, tendo como principais fatores que elevaram o grau de risco: a relevância do processo nas atividades meio e finalística do IFSC, a inexistência de ações de auditoria no tema nos últimos 10 anos.

O objetivo principal da ação foi avaliar o atual estágio da governança de TIC no IFSC e identificar os aspectos que necessitam ser aperfeiçoados. A abordagem adotada pela Audin objetivou responder, dentre outras questões secundárias, as seguintes questões de Auditoria:

- Existem políticas e diretrizes definidas para governança e gestão de tecnologia da informação?
- Existe acompanhamento, e avaliação dos resultados e objetivos de TI?

- As necessidades relacionadas ao desenvolvimento de pessoas e à força de trabalho da área de TI são gerenciadas?
- O processo de planejamento de contratação de TI está sendo executado de acordo com as normas vigentes?

Para alcançar o objetivo proposto nesta ação, a Audin utilizou diversas técnicas de auditoria e realização de testes substantivos tendo como escopo as políticas e diretrizes de TIC vigentes em 2023, contratações de soluções de TIC realizadas em 2022 e o PDI 2020-2024 além do processo de construção do PDI 2025-2029.

As análises se deram com base nas entrevistas, informações e documentos disponibilizados pelos gestores de TIC através de respostas às solicitações de auditoria, sendo que nenhuma restrição foi imposta ao trabalho.

Esta ação de auditoria teve como principal finalidade fornecer uma avaliação imparcial e crítica da maturidade da governança de TIC no IFSC, visando identificar áreas de conformidade, ineficiência, riscos e oportunidades de melhoria. Portanto, ao percorrer o relatório, recomendamos que os leitores estejam atentos aos principais achados, recomendações e conclusões apresentados. É importante considerar que as informações contidas aqui não apenas destacam problemas, mas também apontam caminhos para o aprimoramento das operações e práticas organizacionais.

RESULTADOS DOS EXAMES

1. Ausência de diretrizes formais para construção dos planejamentos de TIC

Ter diretrizes formais para a construção dos planejamentos de TIC são essenciais por proporcionarem estrutura e clareza ao processo, alinhando aos objetivos estratégicos e embasando decisões. Da mesma forma, um planejamento participativo é crucial, ao envolver a equipe ativamente, promovendo comprometimento, diversidade de idéias e coesão, fortalecendo tanto o plano em si quanto a cultura organizacional.

A portaria SGD/ME nº 778/2019, define que os órgãos deverão considerar as práticas definidas no Guia de Governança de TIC do SISP, que na sua prática 06, define uma série de iniciativas para a construção dos planejamentos de TIC, dentre elas:

• Desenvolva e formalize um processo de planejamento de TIC participativo, que envolva a alta administração e os representantes das áreas finalísticas da organização;

• Durante o processo de planejamento de TIC, leve em consideração a complexidade dos serviços públicos providos pelas áreas finalísticas da organização e;

• Comunique a estratégia de TIC.

Contudo, o Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) e o Plano Estratégico de Tecnologia da Informação e Comunicação (PETIC) apresentam sucintamente a metodologia do trabalho de construção mas não define critérios formais de como esses planejamentos foram construídos.

O mapeamento do processo de construção dos planos de TIC, disponível em https://dtic.ifsc.edu.br/processos/processos-de-tic sinaliza que a Coordenadoria de Governança, que é uma unidade administrativa estabelecida dentro do setor de TIC, escolhe a metodologia a ser empregada e elabora a minuta do plano para posterior aprovação.

Em um planejamento não participativo, a falta de envolvimento da equipe pode resultar em falta de comprometimento, resistência às estratégias propostas e falta de diversidade de perspectivas, o que pode, futuramente, gerar dificuldades no atingimento dos objetivos definidos.

Algumas causas podem ser identificadas para a ausência de diretrizes para a construção dos planos de TIC, dentre elas, destacamos:

Insuficiência de conhecimento e experiência sobre a matéria: se a equipe de TIC não possui o conhecimento necessário sobre melhores práticas, *frameworks* e metodologias para o planejamento de TIC, pode ser difícil desenvolver diretrizes eficazes. A falta de experiência também pode levar a abordagens inadequadas ou incompletas.

Falta de comunicação e colaboração: a comunicação inadequada entre os membros da equipe de TIC pode resultar em lacunas de informação e entendimento. A colaboração é essencial para desenvolver diretrizes abrangentes e relevantes.

Aversão à documentação: algumas equipes de TIC podem ter uma cultura ou preferência pela resolução rápida de problemas em vez de investir tempo na documentação de diretrizes formais. Isso pode ser resultado de uma mentalidade mais reativa do que proativa.

A ausência de diretrizes formais para construção de planejamentos de TIC, pode ter diversos efeitos negativos sobre a organização. Alguns desses efeitos incluem: desperdício de recursos, falta de alinhamento estratégico, baixa eficiência e produtividade etc.

Em resumo, a ausência de diretrizes formais para planejamentos de TIC podem ter um efeito cascata que afeta a eficiência operacional, a competitividade, a segurança e a capacidade de inovação da organização. Portanto, é fundamental investir na criação e implementação de diretrizes adequadas para maximizar os benefícios da TIC dentro da Instituição.

2. Ausência de diretrizes para avaliação da governança, da gestão e do desempenho dos serviços de TIC.

Ter diretrizes formais para avaliação da governança, da gestão e do desempenho dos serviços de TIC é de suma importância, pois essas diretrizes fornecem um roteiro claro e objetivo para medir o impacto e eficácia das iniciativas relacionadas à TIC. Elas permitem uma análise criteriosa das metas alcançadas, custo-benefício, eficiência operacional e satisfação dos usuários, garantindo que os investimentos em TIC estejam alinhados com os objetivos estratégicos da Instituição. Além disso, essas diretrizes facilitam a compreensão

dos resultados por parte dos *stakeholders*, permitindo uma comunicação transparente sobre o progresso e as áreas que necessitam de melhorias.

Nesse contexto, a portaria CGD/ME nº 778/2019, em seu artigo 6º, inciso V, dispõe que as organizações tenham 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.

O Decreto 9.203/2017, que dispõe sobre a política de governança da administração pública federal, define como uma das diretrizes, previstas no artigo 4º: monitorar o desempenho e avaliar a concepção, a implementação e os resultados das políticas e das ações prioritárias para assegurar que as diretrizes estratégicas sejam observadas

O Tribunal de Contas da União (TCU), por sua vez, em seu Acórdão nº 1.233/2012, recomendou no item 9.2.9, que as instituições implementassem controles e processos, dentre outros, para o monitoramento do desempenho dos serviços de TIC.

Contudo, em resposta à solicitação de auditoria a gestão informou que não foram definidas diretrizes para a avaliação da governança, da gestão e dos serviços de TIC.

Em virtude dessa ausência, conclui-se que a Instituição pode enfrentar dificuldades na medição efetiva dos benefícios alcançados, podendo levar a uma alocação inadequada de recursos, decisões baseadas em intuição em vez de dados concretos e a incapacidade de identificar e corrigir problemas de forma proativa. A definição de diretrizes robustas de avaliação proporciona não apenas uma base para aprimoramento contínuo, mas também promove a transparência, a *accountability* e a gestão por resultados na Instituição.

A ausência de diretrizes para avaliação da governança, gestão de TIC e desempenho dos serviços de TIC pode ser atribuída a diversas causas, incluindo a falta de compreensão da importância desses aspectos por parte das partes interessadas, como a alta administração e os principais tomadores de decisões, a influência da cultura organizacional que não valoriza a transparência e a responsabilidade relacionadas à TIC, e a falta de incentivos para adotar práticas eficazes de governança e gestão de TIC, o que pode desmotivar a criação de diretrizes formais para a avaliação.

Em conseqüência disso, a ausência de diretrizes pode trazer uma série de efeitos negativos na Instituição, dentre eles: falta de transparência e prestação de contas, baixa

qualidade dos serviços de TIC, riscos de segurança e conformidade, falta de controle orçamentário, dificuldade na tomada de decisões.

Em resumo, a ausência de diretrizes para a avaliação da governança, gestão e desempenho dos serviços de TIC pode comprometer a eficácia organizacional, aumentar os riscos e prejudicar a capacidade da organização de atingir seus objetivos estratégicos. Portanto, é crucial desenvolver e implementar diretrizes robustas para garantir a governança eficaz, a gestão adequada dos recursos de TIC e a entrega de serviços de qualidade.

3. Ausência de diretrizes e gerenciamento das necessidades relacionadas ao desenvolvimento de pessoas da área de TIC

A área de TIC é uma das mais importantes para o sucesso de qualquer organização. É por isso que é fundamental que as instituições tenham diretrizes e processos claros para o desenvolvimento de suas equipes. Essas diretrizes devem ajudar a garantir que os servidores tenham as habilidades e conhecimentos necessários para realizar seu trabalho com eficiência e eficácia.

Nesse contexto, a Portaria SGD/ME nº 778/2019, define em seu art. 6º que o PDTIC deve conter no mínimo, entre outros, um plano de gestão de pessoas de TIC.

O Guia de Governança do SISP sugere que a Instituição implemente práticas organizacionais de gestão de pessoas por competências.

O TCU, por sua vez, orientou através do Acórdão 1233/2012, em seu item 9.2.9, que as Instituições mantenham processo de gerenciamento do pessoal de TIC.

E por fim, o Cobit 4.1, em seu processo PO7 e o Cobit 5 em seu habilitador “Pessoas, habilidades e Competências” trazem uma série de iniciativas para o gerenciamento do pessoal de TIC com vistas a contratar, manter e motivar uma força de trabalho competente para criar e entregar serviços de TIC para o negócio.

Contudo, em resposta a solicitação de auditoria a gestão informou que não existe um plano de gestão de pessoal de TIC que identifique as competências, as necessidades de qualificação, retenção de gestores e técnicos, escolha de gestores, avaliação de desempenho.

Da mesma forma, não existe plano anual de capacitação, alinhado com as competências e necessidade de qualificação para o pessoal de TIC. O PDTIC se limita a informar o quantitativo de pessoal e a formação.

Diante da ausência de plano de gestão de pessoas, plano de capacitação e fluxos processuais de gerenciamento de pessoal constata-se que essa deficiência traz dificuldades no desenvolvimento e retenção de profissionais de tecnologia da informação podendo levar a uma equipe desequilibrada em termos de habilidades e competências, comprometendo a eficiência operacional e a capacidade de inovação. Além disso, a ausência de um plano estruturado pode resultar em lacunas de conhecimento, falta de treinamento adequado e desmotivação entre os membros da equipe de TIC, prejudicando a qualidade dos serviços prestados e aumentando os riscos de não atingimento dos objetivos estratégicos.

O gerenciamento de pessoal é um processo crítico porque as pessoas são ativos importantes e a governança e o ambiente de controle de dados são altamente dependentes da motivação e da competência dessas pessoas. Dentre possíveis causas podemos citar:

Falta de conscientização sobre a importância do gerenciamento de pessoal: algumas instituições podem não reconhecer a importância do gerenciamento de pessoal na área de TIC e podem subestimar o impacto que uma equipe bem gerenciada pode ter nos resultados do negócio.

Falta de recursos: pode haver uma falta de recursos, tanto financeiros quanto humanos, para dedicar a funções de gerenciamento. Isso pode levar a uma sobrecarga dos líderes de equipe de TIC, que podem então não ter tempo suficiente para se concentrar em tarefas de gerenciamento adequado.

Falta de investimento em desenvolvimento pessoal, ausência de *feedback* e avaliação de desempenho, falta de ferramentas e sistemas de suporte e dificuldades em equilibrar tarefas técnicas e de gestão também são possíveis causas para a fragilidade no gerenciamento de pessoal de TIC.

A ausência de gerenciamento de pessoal pode ter um impacto negativo na área de TIC. Isso pode levar a alguns problemas, incluindo:

Baixa produtividade: Equipes mal gerenciadas são frequentemente menos produtivas.

Qualidade inferior do trabalho: Sem supervisão e orientação adequadas, os membros da equipe podem não cumprir os padrões de qualidade esperados.

Desmotivação: A falta de reconhecimento, f*eedback* e oportunidades de desenvolvimento pode levar à desmotivação dos membros da equipe.

4. Participação limitada da área de TIC na construção do Plano Estratégico Institucional (PDI)

A TIC não é uma entidade isolada, ela se interconecta com todas as áreas da Instituição desempenhando um papel crucial em quase todos os processos institucionais, portanto, sua participação no processo de construção do planejamento estratégico é fundamental, garantindo que a visão e os objetivos do negócio tenham suportes tecnológicos tangíveis que apóiem a sua implementação.

Nesse contexto, a Portaria SGD/ME nº 778/2019 estabeleceu que a área de TIC deve ser considerada como um ativo estratégico fundamental, adotando-o como princípio de governança.

O TCU, por sua vez, em seu acórdão 1233/2012 item 9.1.1.1, recomenda que os órgãos elaborem o planejamento estratégico com a participação de representantes dos diversos setores da organização.

Contudo, no IFSC, as portarias de designação das comissões centrais tanto do PDI 2020-2024 quanto do PDI 2025-2029 não constam a participação dos diretores de TIC. A participação destes, se limitam a uma comissão temática para construção de um capítulo específico do documento. Se a área de TIC não estiver envolvida desde o início do processo de planejamento, é possível que as soluções tecnológicas que permitem que a Instituição alcance seus objetivos estratégicos não sejam adequadas às necessidades da organização, levando ao fracasso do atingimento dos objetivos.

Como possível causa podemos indicar a falta de consciência sobre a importância da TI**.** Se a alta administração não reconhece a importância estratégica da TIC, pode não incluir automaticamente a equipe de TIC no processo de planejamento. Isso pode ocorrer quando a TIC é vista apenas como um suporte operacional, em vez de um ativo estratégico capaz de auxiliar a Instituição no atingimento dos objetivos.

Sem sua participação, os objetivos correm riscos de não serem atingidos por falta de suporte tecnológico adequado, e ainda, podem resultar em objetivos estratégicos desalinhados com as capacidades e oportunidades tecnológicas recentes.

5. Fragilidade na execução da Política de Segurança da informação e Comunicação

A Política de Segurança da Informação e Comunicação (POSIC) é um documento essencial para proteger os ativos de informação da Instituição. Ela estabelece os princípios e diretrizes que devem ser seguidos para garantir a disponibilidade, integridade e confidencialidade das informações. Sua efetiva aplicação é fundamental para que a organização possa cumprir seus objetivos e metas. Ela ajuda a proteger as informações contra ameaças e vulnerabilidades, reduzindo o risco de incidentes de segurança.

No IFSC, o Comitê de Governança Digital aprovou a POSIC, por meio da Resolução nº 08/2022, e a Gestão de Segurança da Informação por meio da Resolução nº 06/2022.

O artigo 5º da Resolução nº 06 dispõe que o Comitê de Governança Digital deverá instituir o Comitê de Segurança da Informação ou estrutura equivalente, para deliberar sobre os assuntos relativos à Segurança da Informação no IFSC.

Essas regulamentações internas somam-se ao Decreto nº 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação, a Resolução GSI nº 1, de 11 de setembro de 2019, que aprova o Regimento Interno do Comitê Gestor de Segurança da Informação e demais instruções normativas relacionadas à segurança da informação, publicadas pelo Gabinete de Segurança Institucional da Presidência da República.

O artigo 15, do Decreto 9.637/2018 disciplina que os Órgãos devem promover ações de capacitação e profissionalização dos recursos humanos em temas relacionados à segurança da informação

A Norma Complementar nº 18/IN01/DSIC/GSIPR define diretrizes para as atividades de ensino em Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal, direta e indireta (APF).

Entretanto, em resposta à solicitação de auditoria 1452465 a gestão informou que o comitê não teve atividades em 2022 e os temas de segurança da informação são tratados no Comitê de Governança Digital, no qual o comitê de segurança está vinculado.

Da mesma forma, não foram apresentadas ações de conscientização, educação e treinamento em segurança da informação para os colaboradores, apenas repositório de leis, normas, procedimentos e outros artefatos que colaboram para a manutenção, a divulgação e a auditoria da segurança da informação.

Diante da situação encontrada, pode-se concluir que existem fragilidades na execução da Política de Segurança da informação e Comunicação uma vez que não houve atividades relacionadas a segurança da informação em 2022 e a Instituição não está realizando ações de conscientização, educação e treinamento em segurança da informação para os servidores, o que é essencial para a proteção dos ativos de informação.

Como possíveis causas podemos citar a falta de comprometimento da alta gestão pois ela é responsável por estabelecer a cultura de segurança da informação na organização. Quando ela não está comprometida com a segurança, é difícil que as demais áreas da organização também estejam. Outra possível causa é a falta de conscientização e treinamento, os servidores são a linha de frente da segurança da informação, quando eles não estão conscientes dos riscos e não são treinados para lidar com eles, é mais provável que eles cometam erros que possam comprometer a segurança.

Para superar essas fragilidades, é fundamental uma abordagem proativa, envolvendo a liderança, a conscientização dos servidores, o investimento adequado e a avaliação constante das práticas de segurança.

Uma das consequências mais graves e imediatas da fragilidade na segurança da informação é a possibilidade de ocorrerem violações e perda de dados, onde informações sensíveis, como dados pessoais ou informações financeiras são comprometidas e podem ser acessadas por terceiros não autorizados.

6. Ausência de Avaliação e monitoramento dos processos de governança, e resultados dos objetivos estratégicos de TIC

A avaliação e monitoramento dos processos de governança, resultados e objetivos de Tecnologia da Informação e Comunicação desempenham um papel crucial na eficácia e

sucesso das estratégias tecnológicas da Instituição. Ao implementar uma abordagem contínua de avaliação, a Instituição pode assegurar que seus investimentos em TIC estejam alinhados com os objetivos gerais do negócio.

Através da análise sistemática dos resultados obtidos em relação aos objetivos estabelecidos, a organização pode identificar lacunas, ajustar estratégias e tomar decisões assertivas para otimizar o uso da tecnologia.

Além disso, o monitoramento constante permite a detecção precoce de desafios e problemas, proporcionando a oportunidade de implementar correções antes que impactem negativamente os processos, a segurança dos dados e os resultados operacionais.

Nesse cenário, diversas legislações e manuais orientam sobre a importância da avaliação e monitoramento dos processos, resultados e objetivos de TIC.

A portaria CGD/ME nº 778/2019, em seu artigo 6º, inciso V, disciplina que os órgãos devem ter 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.

O TCU, em seu Acórdão nº 1233/2012, recomendou em seu item 9.2.9, que as instituições implementassem controles e processos, dentre outros, para o monitoramento do desempenho dos serviços de TIC.

O Manual do SISP que define diretrizes para a governança de TIC dos órgãos da Administração Pública Federal estabelece em sua prática 09 um conjunto de orientações relacionadas ao monitoramento e à supervisão do desempenho das ações empreendidas pela TIC, como o atingimento das metas de nível de serviço, resultados de programas e projetos, indicadores de implementação dos planos de TIC, etc.

E por fim, o framework Cobit 5, que auxilia as organizações a desenvolver, organizar e implementar estratégias de gestão de informação e governança traz como um de seus domínios “Avaliar, dirigir e Monitorar” (EDM) onde orienta que todos os processos de TIC precisam ser regularmente avaliados com o passar do tempo para assegurar a qualidade e a aderência aos requisitos de controle. Este domínio aborda o gerenciamento de performance, o monitoramento do controle interno, a aderência regulatória e a governança.

Entretanto, em resposta a solicitação de auditoria, a gestão informou que não existe avaliação e/ou monitoramento formalizado dos processos de governança, resultados dos serviços TIC e avaliação periódica dos objetivos de TIC constante no PETIC.

O PETIC 2020-2024 apresenta 9 objetivos estratégicos, porém, nenhum relatório de monitoramento ou avaliação foi realizado até o momento. Esses relatórios oferecem uma visão clara e transparente do progresso em direção às metas estabelecidas, permitindo que os gestores, demais servidores e órgãos de controle avaliem o desempenho da TIC em relação às expectativas e identifiquem áreas que precisam de melhorias.

Da mesma forma, não foram publicados relatórios de monitoramento dos resultados e da utilização dos serviços produzidos pela TIC no período. Esses relatórios fornecem uma visão detalhada do desempenho dos sistemas, infraestrutura e aplicações de TIC, oferecendo insights sobre a disponibilidade, desempenho, segurança e utilização dos recursos tecnológicos. Ao analisar esses relatórios, as equipes de TIC e os gestores podem identificar padrões, detectar problemas emergentes e tomar decisões informadas para otimizar a eficiência operacional, alocar recursos de maneira mais eficaz e garantir a conformidade com metas e padrões estabelecidos.

Uma série de fatores pode ser a causa para a ausência de avaliação, dentre eles podemos destacar:

Falta de Conscientização e Cultura de Governança: Se a alta administração e os líderes de TIC não compreenderem a importância da governança de TIC e não promoverem uma cultura de responsabilidade e prestação de contas, é provável que não haja um foco suficiente na avaliação e monitoramento dos processos.

Falta de Diretrizes Claras: Objeto da constatação 2 desse relatório, se não houver diretrizes bem definidas para medir o desempenho e os resultados dos objetivos estratégicos de TIC, torna-se difícil avaliar efetivamente o progresso e o impacto das atividades.

Recursos Limitados: A falta de recursos financeiros, humanos e tecnológicos pode dificultar a implementação eficaz de atividades de avaliação e monitoramento.

Para superar essas causas, é importante que a Instituição promova uma cultura de governança, defina métricas claras, aloque recursos adequados e envolva a liderança de TIC

no processo de avaliação e monitoramento contínuo dos resultados dos objetivos estratégicos de TIC.

A ausência de avaliação e monitoramento pode ter diversos impactos negativos para a Instituição, dentre eles, o desalinhamento com objetivos estratégicos institucionais, falta de melhoria contínua, ineficiência operacional, decisões baseadas em dados insuficientes, falta de responsabilização, dentre outros.

Em resumo, a ausência de avaliação e monitoramento adequados pode resultar em perda de eficiência, oportunidades desperdiçadas e riscos não gerenciados, comprometendo a capacidade da Instituição de alcançar seus objetivos estratégicos e se adaptar às demandas em constante evolução do ambiente tecnológico.

7. Fragilidades no mapa de gerenciamento de riscos juntado ao processo de contratação

A análise de riscos desempenha um papel fundamental nos processos licitatórios, uma vez que proporciona uma abordagem estruturada e criteriosa para identificar, avaliar e mitigar potenciais ameaças que podem afetar a realização bem-sucedida de contratações públicas. Ao considerar diversos cenários e possíveis desdobramentos, essa prática permite que as entidades governamentais antecipem desafios, compreendam as vulnerabilidades e adotem medidas preventivas e corretivas adequadas. Além de aumentar a transparência e a eficiência do processo, a análise de riscos capacita os tomadores de decisão a tomar medidas embasadas, promovendo a seleção de fornecedores mais confiáveis e a elaboração de contratos mais robustos, com impactos positivos tanto na qualidade das entregas quanto na otimização dos recursos públicos.

Nesse cenário, a Instrução Normativa SGD/ME nº 01/2019, que dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação, disciplina em seu artigo 38, que a equipe de planejamento da contratação deve produzir o Mapa de Gerenciamento de Riscos e deve ser juntado aos autos do processo administrativo, pelo menos:

I - ao final da elaboração do Termo de Referência ou Projeto Básico;

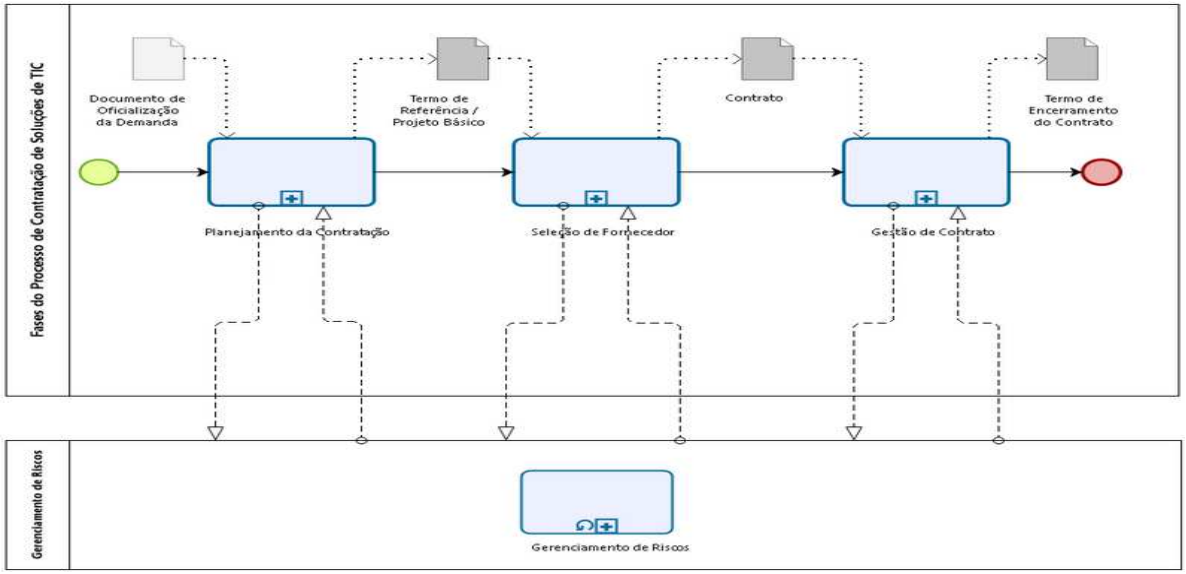
II - ao final da fase de Seleção do Fornecedor;

III - uma vez ao ano, durante a gestão do contrato;

IV - após eventos relevantes.

O TCU, com base nos seus trabalhos de fiscalização, nos quais foram identificados vários problemas na condução das contratações de soluções de TIC pelos órgãos e entidades da Administração Pública Federal, bem como nos respectivos contratos, elaborou o guia de boas práticas em contratações de soluções de TI. No apêndice D desse guia, o TCU sintetiza, pelo menos, 66 riscos identificados nos processos de planejamento das contratações de soluções de TIC, com as respectivas sugestões de controles internos.

De acordo com o Ministério da Gestão e Inovação e Serviços o processo de contratação de soluções de TIC é composto por três fases sequenciais: planejamento da contratação, seleção do fornecedor e a gestão do contrato, e em paralelo a estas fases ocorre o gerenciamento de riscos. Em resumo, o gerenciamento de riscos deve permear todas as fases do processo licitatório conforme fluxograma abaixo disponível em https://www.gov.br/governodigital/pt-br/contratacoes/1-modelo-de-contratacao-de-tic.png



As análises revelaram que a identificação, análise e possíveis ações de tratamento dos riscos foram realizadas **apenas uma vez**, imediatamente após o estudo técnico preliminar e **antes** do Termo de Referência.

Ademais, a matriz de gerenciamento de riscos não identificou riscos recorrentes em licitações, tais como, sobrepreço em licitações baseadas no princípio da padronização (Lei 8.666/1993,art. 15, inciso I), ou, levantamento de mercado deficiente, levando a licitação deserta, entre outros.

Da relação de processos contratação de soluções de TIC realizados em 2022, foram selecionados dois processos finalizados, considerando a materialidade envolvida.

O primeiro processo foi o pregão nº 21005/2022 - Aquisição de softwares prontos e subscrição de licenças SAAS e PAAS, cujo valor estimado era de R$ 4.623.619,87. Neste processo, a matriz de gerenciamento de riscos está apensada na página 296 e identificou apenas 4 riscos: impugnação do edital, cancelamento de itens, recursos administrativos e falta de recursos orçamentários.

O segundo processo selecionado foi o pregão nº 31009/2022 de contratação de bens permanentes de TIC com valor estimado de R$ 8.946.109,90. Neste processo, a matriz de gerenciamento de riscos identificou além dos riscos supracitados, a incompatibilidade entre os objetos adquiridos de diferentes marcas e fornecedores e incompatibilidade da solução com a infraestrutura atual.

Em resumo, embora tenha sido realizada a matriz de gerenciamento de riscos, a mesma não identificou riscos recorrentes em contratações públicas conforme manual de boas práticas do TCU, além de ter sido realizada de maneira estática, durante a fase de planejamento, contrariando a Instrução Normativa SGD/ME nº 01/2019 que considera o gerenciamento de riscos um subprocesso que deve acompanhar a fase de planejamento, seleção do fornecedor e gestão contratual.

A falta de capacitação por parte dos funcionários envolvidos no processo de contratação pode levar a uma compreensão insuficiente dos riscos específicos do setor de tecnologia, resultando em escolhas inadequadas de fornecedores e na subestimação de ameaças potenciais. Além disso, a burocracia excessiva e os processos morosos de aquisições governamentais podem resultar em contratações apressadas, onde a análise de riscos é negligenciada em detrimento de prazos apertados. Isso pode resultar em escolhas inadequadas de fornecedores e escopo de projetos mal definidos, aumentando os riscos de falhas e atrasos.

A fragilidade no gerenciamento de riscos em contratações públicas de soluções de TIC podem resultar em projetos de TIC mal sucedidos, com custos estourando orçamentos e cronogramas estendidos, prejudicando a eficácia da contratação. Além disso, a falta de gestão eficaz de riscos pode abrir espaço para a falhas, e até mesmo fraudes que culminam em desperdício de recursos públicos.

RECOMENDAÇÕES

1 - Definir diretrizes para elaboração dos planos de TIC com aprovação prévia do Comitê de Governança Digital.

Achado nº 1

2 - Aprovar diretrizes para avaliação da governança, da gestão e do desempenho dos serviços de TIC.

Achado nº 2

3 - Elaborar plano de gestão de pessoas utilizando as melhores práticas e que contemple, pelo menos, plano anual de capacitação.

Achado nº 3

4 - Incluir a área de TIC na construção do Plano de Desenvolvimento Institucional.

Achado nº 4

5 - Apresentar, nos próximos 18 meses, os trabalhos desenvolvidos pelo comitê técnico de segurança da informação.

Achado nº 5

6 - Realizar ações de conscientização, educação e treinamento em segurança da informação nos termos da NC 18/IN01/DSIC/GSIPR.

Achado nº 5

7 - Elaborar e publicar relatório, pelo menos anual, contendo avaliação dos serviços produzidos pela TIC, monitoramento dos objetivos estratégicos de TIC e demais diretrizes definidas na recomendação 2.

Achado nº 6

8 - Em futuros processos licitatórios, aprimorar a matriz de gerenciamento de riscos e atualizar durante o processo conforme disciplina o artigo 38 da IN SGD/ME nº 01/2019.

Achado nº 7

CONCLUSÃO

Este trabalho de auditoria proporcionou uma visão abrangente da governança de TIC no IFSC. Identificamos áreas de força que merecem reconhecimento, como a existência de diversas políticas e diretrizes que compõem os pilares da boa governança. No entanto, também identificamos oportunidades de melhoria, especialmente no que diz respeito à avaliação e monitoramento das políticas, planos e entregas de serviços.

Para atender o objetivo da ação, a Audin definiu três questões principais de auditoria que passamos a responder a seguir.

A primeira questão buscou responder se existem políticas e diretrizes definidas para governança e gestão de tecnologia da informação. As análises revelaram que, de forma geral, sim, existem diversas normas, políticas e diretrizes que direcionam a TIC em diferentes dimensões necessárias para o alcance dos objetivos da TIC, contudo, é necessário avançar no pilar de avaliação e monitoramento dos objetivos e resultados de TIC.

A segunda questão procurou verificar se existe acompanhamento, e avaliação dos resultados e objetivos de TI. Aqui, encontramos a maior fragilidade, embora existam políticas e planos que definem os objetivos de TIC, falta acompanhamento periódico e avaliação dos resultados, causado, em partes, pela falta de diretrizes de avaliação levantadas na questão de auditoria acima.

A terceira questão, por sua vez, verificou se as necessidades relacionadas ao desenvolvimento de pessoas e à força de trabalho da área de TIC são gerenciadas. As análises mostraram que é preciso avançar nesse tema, isso porque, não existe um plano de gerenciamento de pessoal de TIC, a gestão informou que já esta trabalhando na construção.

Foram avaliados, ainda, a situação das contratações de soluções TIC, as análises foram realizadas de maneira amostral, e revelaram que, de forma geral, as contratações estão em consonância com o PDTI e demais normas vigentes, necessitando, apenas, realizar uma análise de risco mais robusta e atualizá-la durante o processo licitatório, conforme prevê o artigo 38 da IN SGD/ME nº 01/2019.

Sendo assim, concluímos que, para otimizar a governança de TIC, a instituição precisa avançar no pilar de avaliação e monitoramento dos resultados e objetivos de TIC. É

inevitável manter um compromisso contínuo com a avaliação periódica e consequente transparência, prestação de contas e conformidade regulatória para garantir o uso eficaz e responsável da tecnologia em prol do serviço público e do cidadão.

Esta auditoria ofereceu uma avaliação imparcial em conformidade com as melhores práticas e as normas emanadas pelas entidades reguladoras visando a evolução positiva da governança de TIC na Instituição. O trabalho foi realizado em consonância com nosso compromisso de apoio contínuo à instituição, sendo que nos colocamos à disposição para fornecer esclarecimentos adicionais e colaborar no processo de implementação das recomendações apresentadas.

JOÃO CLOVIS SCHMITZ
Auditor

GREGORY CASTILHO MANCIN
Audito Chefe

ANEXOS

I – MANIFESTAÇÃO DA UNIDADE AUDITADA E ANÁLISE DA EQUIPE DE AUDITORIA

Achado nº 1 - Ausência de diretrizes formais para construção dos planejamentos de TIC

Manifestação da unidade auditada

"Coordenadoria de Governança, que é uma unidade administrativa estranha ao setor de TI" - A coordenação citada não é estranha a unidade administrativa pois como é de conhecimento da Audin a Governança de TIC é parte basilar na construção de uma gestão efetiva e que atenda às diretrizes institucionais. Além disso, cabe também informar, que em função de termos está coordenadoria o índice de governança de TIC do IFSC é bem avaliado quando comparado ao próprio índice do IFSC e demais IFs. Por fim, cabe informar que esta coordenadoria não existe mais desde fevereiro/2023.

O planejamento de TI - PETIC foi construído com a participação de representantes dos câmpus que se dispuseram a auxiliar nesta construção ainda que não citados naquele documento. Cabe ainda ressaltar:

"Este documento foi elaborado pela Coordenadoria de Governança de TIC (CgovTIC) a partir de reuniões de alinhamento com a diretoria de TIC e consultas à Pró-reitoria de Desenvolvimento Institucional." - PETIC, pág. 6

O documento foi apreciado pelo CGTIC, na época composto por representantes das pró-reitorias e diretorias do IFSC e representantes dos diretores gerais dos câmpus do IFSC. Posteriormente foi aprovado pelo Consup.

Desta forma, a DTIC entende que houve a participação dos entes que compõem o IFSC, atendendo assim, as normativas apontadas anteriormente.

Sobre o PDTIC, a parte que envolve os câmpus é retirada do PAT (Plano Anual de Trabalho). Os demais pontos são de gestão da DTIC e estão alinhadas com as normas governamentais conforme exposto na página 10 - Princípios e Diretrizes.

Por fim, cabe informar que o planejamento dos câmpus, inclusive TIC, é realizado através do PAT e não do PDTIC.

Desta forma, esta diretoria de TIC não tem o objetivo inicial de mudar a forma de elaboração do PETIC e PDTIC, visto que a participação dos cÂmpus se dá em seus colegiados para a elaboração do PAT e os demais pontos tanto do PETIC quanto do PDTIC são apreciados e aprovados pelo CGD e seus comitês técnicos.

Análise da equipe de auditoria

Realmente a coordenaria de Governança não é estranha ao setor de TI, ela estava inserida dentro do departamento de TIC e coordenada por um analista de TIC.

O achado, e conseqüentemente a recomendação, não tem como objetivo mudar a forma de elaboração do PETIC e PDTIC, mas sim, propor a definição ou a exposição das diretrizes para a construção desses documentos com o intuito de facilitar a construção de novos documentos por qualquer servidor ou comitê que esteja à frente da elaboração no momento.

Dessa forma, iremos manter a recomendação e monitorar a implementação.

Achado nº 2 - Ausência de diretrizes para avaliação da governança, da gestão e do desempenho dos serviços de TIC.

Manifestação da unidade auditada

A Unidade acatou a recomendação.

Achado nº 3 - Ausência de diretrizes e gerenciamento das necessidades relacionadas ao desenvolvimento de pessoas da área de TIC

Manifestação da unidade auditada

No momento a DTIC está elaborando um plano para tratar do tema. O plano já foi apreciado pelas CTICs, Diretores Gerais, DGP (Capacitação) e estará sendo encaminhado para o CDP antes de ser apreciado e aprovado pelo CGD.

Análise da equipe de auditoria

Conforme a manifestado, já iniciaram os trabalhos para suprir a inconsistência, dessa forma, iremos manter a recomendação e monitorar a implementação.

Achado nº 4 - Ausência de participação da área de TIC na construção do Plano Estratégico Institucional (PDI)

Manifestação da unidade auditada

A DTIC e suas áreas participarão da elaboração conforme portaria abaixo: Portaria do(a) Reitor(a) N° 2714, de 4 de setembro de 2023

Art. 1º Designar os servidores abaixo para comporem a respectiva comissão, com carga horária de 2 horas semanais.

LXXIII. BENONI DE OLIVEIRA PIRES - TITULAR DA DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO E DA COMUNICAÇÃO; LXXIV. GILBERTO JOSÉ DE SOUZA COUTINHO - TITULAR DA CHEFIA DO DEPARTAMENTO DE SISTEMAS DE INFORMAÇÃO;

Análise da equipe de auditoria

A portaria apresentada trata de uma comissão temática criada para construção apenas do capítulo 6 do PDI que trata do planejamento estratégico institucional.

Ao nosso ver, essa designação não atende completamente a recomendação, uma vez que trata apenas da construção de um capítulo específico, e a área de TIC, por ser um ativo estratégico, pode dar relevantes contribuições em todo o documento, por isso deveria compor a comissão central do PDI.

Dessa forma mantemos a recomendação de incluir a área de TIC na comissão central de construção do PDI.

Achado nº 5 - Fragilidade na execução da Política de Segurança da informação e Comunicação

Manifestação da unidade auditada

O comitê já existe e seu funcionamento é regido pelo regimento do CGD. Em agosto de 2023 houve a atualização da portaria dos membros do CTSI: Portaria do(a) Reitor(a) N° 2544 de 17 de agosto de 2023;

Está de acordo com recomendação de realizar ações de conscientização, educação e treinamento em segurança da informação nos termos da NC 18/IN01/DSIC/GSIPR.

Análise da equipe de auditoria

Conforme resposta enviada na solicitação de auditoria inicial, "*o comitê de Segurança da Informação (CSI) não teve atividades em 2022. Temas de segurança foram tratados diretamente pelo CGD. O CSI está subordinado ao CGD conforme regimento deste.*

Não temos um CSI exclusivo, deliberativo ou normativo. Essas são atribuições do CGD. Os membros atuais do comitê não possuem portaria pois estamos aguardando que a solicitação de alteração dos membros seja aprovada no Consup."

Ao nosso ver, embora exista, o comitê não tem atuado de maneira efetiva e se confunde com o CGD, dessa forma, retificamos a recomendação de criar o comitê, para; apresentar, nos próximos 18 meses, os trabalhos desenvolvidos pelo comitê técnico de segurança da informação.

Achado nº 6 - Ausência de Avaliação e monitoramento dos processos de governança, e resultados dos objetivos estratégicos de TIC

Manifestação da unidade auditada

A recomendação foi acatada integramente

Achado nº 7 - Fragilidades no mapa de gerenciamento de riscos juntado ao processo de contratação.

Manifestação da unidade auditada

A recomendação foi acatada integramente.