JUSTIÇA ELEITORAL
TRIBUNAL REGIONAL ELEITORAL DE MATO GROSSO DO SUL
COORDENADORIA DE CONTROLE INTERNO E AUDITORIA
SEÇÃO DE CONTROLE DA ATIVIDADE ADMINISTRATIVA

RELATÓRIO DE AUDITORIA 5/2018

Normas referentes: IPPF/IIA (2400 e 2420); ISSAI/INTOSAI (300 e 400)

PREÂMBULO

PROCESSO: 0001483-55.2018.6.12.8000.

ATO ORIGINÁRIO: Plano Anual de Auditoria (PAA), relativo ao exercício de 2018, aprovado pela Decisão n. 6 / 2017 - TRE/PRE/GABPRE, no processo SEI n. 0009610-16.2017.6.12.8000.

OBJETIVO: Avaliar os conteúdos estabelecidos para a governança e gestão de TI, considerando projetos, processos, riscos e resultados de TI em comparação com padrões internacionalmente aceitos, como COBIT, PMBOK, ITIL, CMMI, ISO 17799, ISO 27001, as Resoluções CNJ n. 91/2009, n. 182/2013, n. 198/2014 e n. 211/2015 e o perfil de governança de TI traçado pelo TCU.

ATO DE DESIGNAÇÃO: Portaria Presidência N. 44/2018 TRE/PRE/GABPRE, publicada no DJE/MS n. 1909, de 27 de fevereiro de 2018, página 02.

PERÍODO ABRANGIDO PELA AUDITORIA: últimos 36 (trinta e seis) meses.

PERÍODO DE REALIZAÇÃO DA AUDITORIA: fevereiro a junho de 2018.

UNIDADE AUDITADA: Secretaria de Tecnologia da Informação.

ÁREA A SER AUDITADA: Sistema de Governança de Tecnologia da Informação – Secretaria de Tecnologia da Informação do Tribunal Regional Eleitoral de Mato Grosso do Sul.

RESUMO

A presente auditoria é parte integrante do conjunto de auditorias realizado simultaneamente em todo o Poder Judiciário do país, na sistemática de Ações Coordenadas de Auditoria, centralizada pela Secretaria de Controle Interno do Conselho Nacional de Justiça (CNJ).

As Ações Coordenadas de Auditoria estão previstas na Resolução CNJ n. 171/2013 e objetivam a gestão concomitante, tempestiva e padronizada sobre questões de relevância e criticidade para o Poder Judiciário, bem como o atendimento aos princípios de eficiência, eficácia, economicidade e efetividade. A auditoria foi prevista no Plano Anual de Auditoria (PAA), para o exercício de 2018, aprovado pela Decisão n. 6 / 2017 - TRE/PRE/GABPRE, no processo SEI n. 0009610-16.2017.6.12.8000.

O objetivo desta auditoria foi avaliar os conteúdos estabelecidos para a governança e gestão de TI, considerando projetos, processos, riscos e resultados de TI em comparação com padrões internacionalmente aceitos, como COBIT, PMBOK, ITIL, CMMI, ISO 17799, ISO 27001, as Resoluções CNJ n. 91/2009, n. 182/2013, n. 198/2014 e n. 211/2015 e o perfil de governança de TI traçado pelo TCU.

Dessa forma, com base no objetivo das Ações Coordenadas de Auditoria e a fim de avaliar a aderência dos Tribunais, entre eles o Tribunal Regional Eleitoral de Mato Grosso do Sul, às melhores práticas de governança e gestão de TI, o CNJ elaborou sete questões de auditoria que nortearam este trabalho: 1ª) Existem políticas e diretrizes definidas para governança e gestão de tecnologia da informação? 2ª) Os planos estratégicos institucional e de TI fornecem suporte apropriado à governança e à gestão de TI? 3ª) As necessidades relacionadas ao desenvolvimento de pessoas e à força de trabalho da área de TI são gerenciadas? 4ª) Os processos de gestão de TI são gerenciados? 5ª) O processo de planejamento de contratação de TI está sendo executado de acordo com o disposto na Resolução CNJ n. 182/2013? 6ª) Os resultados apresentados pela TI são dimensionados? 7ª) A Unidade de Auditoria Interna (UAI) realiza exames de auditoria na área de TIC para aferir o estágio de governança e gestão de TI?

As sete questões de auditoria foram detalhadas em cinquenta e duas perguntas elaboradas pelo CNJ no modelo de questionário previamente definido. O resultado do trabalho de avaliação foi enviado ao CNJ no formato de respostas a tal questionário, acompanhadas de evidências quando as respostas eram positivas. O preenchimento do questionário exigiu a execução de um conjunto de procedimentos que permitissem concluir, com nível razoável de segurança, quanto ao grau de efetividade do sistema de governança e gestão de TIC do TRE/MS.

As técnicas utilizadas para responder as questões de auditoria foram a aplicação de questionário, exame documental e reuniões. Da aplicação dos testes, houve trinta e três achados de auditoria, posteriormente reduzidos a trinta achados, em razão do atendimento de algumas recomendações após a fase de testes e antes da conclusão deste relatório. Os achados revelaram que o órgão, de maneira geral, apresenta baixa maturidade de governança de TI, vez que não foram estabelecidos vários dos processos e políticas recomendados para uma boa governança corporativa de TI.

Desta forma, foram propostas recomendações para que o Tribunal estabeleça políticas e processos de governança de TI, entre as quais: diretrizes formais para planejamento de TI, gestão do portfólio de projetos e de serviços de TI, contratação de bens e serviços de TI, avaliação do desempenho dos serviços de TI; políticas de gestão de riscos de TI; de controle de acesso aos recursos de TI e de cópia de segurança (backup); ausência de plano diretor de tecnologia de informação e comunicação (PDTIC), de processos de gestão de serviços, de plano de continuidade de serviços essenciais de TI, de processo de software, de plano de contratações de TI, de medição dos resultados dos objetivos estratégicos, de medição do grau de alcance dos objetivos e benefícios esperados nos projetos de TI, dentre outros.

LISTA DE SIGLAS

ABR	Auditoria Baseada em Riscos
CMMI	*Capability Maturity Model Integration* (Modelo Integrado de Maturidade em Capacitação)
CNJ	Conselho Nacional de Justiça
COBIT	*Control Objectives for Information and Related Technologies* (Modelo Corporativo para Governança e Gestão de TI da Organização)
DG	Direção-Geral
DJE/MS	Diário da Justiça Eleitoral de Mato Grosso do Sul
DSIC	Departamento de Segurança da Informação e Comunicações
ETIR	Equipe de Resposta a Incidentes de Segurança em Redes Computacionais
GSIPR	Gabinete de Segurança Institucional da Presidência da República
IIA Brasil	Instituto dos Auditores Internos do Brasil
INTOSAI	Organização Internacional de Entidades Fiscalizadoras Superiores
IPPF	*International Professional Practices Framework* (Normas Internacionais para a Prática Profissional de Auditoria Interna)
IN	Instrução Normativa
ISO	*International Organization for Standardization* (Organização Internacional de Normalização)
ISSAI	Normas Internacionais das Entidades Fiscalizadoras Superiores
ITIL	*Information Technology Infrastructure Library* (Biblioteca de Infraestrutura de Tecnologia da Informação)
NBR	Norma Brasileira ABNT
NC	Norma Complementar.
PAA	Plano Anual de Auditoria
PDTIC	Plano Diretor de Tecnologia da Informação e Comunicação
PETIC	Planejamento Estratégico de Tecnologia da Informação e Comunicação
PMBOK	*Project Management Body of Knowledge* (Guia do Conhecimento em Gerenciamento de Projetos)
PSI	Política de Segurança da Informação
SEI	Sistema Eletrônico de Informações

STI	Secretaria de Tecnologia da Informação
TCU	Tribunal de Contas da União
TI	Tecnologia da Informação
TIC	Tecnologia da Informação e Comunicação
TRE/MS	Tribunal Regional Eleitoral de Mato Grosso do Sul
TSE	Tribunal Superior Eleitoral

SUMÁRIO

I. INTRODUÇÃO

Em Sessão Virtual, o Plenário do CNJ aprovou o Parecer n. 7/2014 – SCI/Presi/CNJ – para realização de três Ações Coordenadas de Auditoria, conforme previsto no artigo 13 da Resolução CNJ n. 171/2013.

Este trabalho consiste na primeira Ação Coordenada de Auditoria que teve por objeto a área de tecnologia da informação, com escopo na avaliação de conteúdos estabelecidos para governança, gestão, riscos e controle de TI e TIC, considerando projetos, processos, riscos e resultados de TI em comparação com padrões internacionalmente aceitos como COBIT, PMBOK, ITIL, CMMI, ISSO 17799 e ISSO 27001, bem como com as Resoluções CNJ n. 91/2009, n. 182/2013 e n. 211/2015. Além disso, essa Ação levou em consideração o perfil de governança de tecnologia da informação e comunicação traçado pelo Tribunal de Contas da União.

Em cumprimento ao prazo definido pelo Conselho Nacional de Justiça, foi encaminhado à Secretaria de Tecnologia da Informação deste Regional o questionário elaborado pela Secretaria de Controle Interno do Conselho Nacional de Justiça para a Ação Coordenada de Auditoria com o tema Governança e Gestão de Tecnologia da Informação (0002188-53.2018.6.12.8000).

Para fins do questionário e deste relatório, considerou-se:

Glossário	
Alta administração	São considerados como alta administração a Diretoria-Geral e a Secretaria-Geral ou equivalente.
Partes interessadas	No setor público abrange: agentes políticos, servidores públicos, usuários de serviços, fornecedores, a mídia e os cidadãos em geral, cada qual com interesse legítimo na organização pública, mas não necessariamente com direitos de propriedade (IFAC, 2001).
Força de trabalho	Quadro permanente com servidores que exercerão atividades voltadas exclusivamente para a área de Tecnologia da Informação e Comunicação, conforme art. 13 da Resolução CNJ n. 211/2015.
Agentes públicos	Todo aquele que exerce, ainda que transitoriamente ou sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função nos órgãos e entidades da Administração Pública, direta e indireta.
Plano de contratações	É o documento no qual a organização define o planejamento das aquisições para o período mínimo de um ano.

Foram realizadas reuniões de abertura e encerramento dos trabalhos entre a equipe de auditoria e a Secretária de Tecnologia da Informação e o Assessor de Governança de TI, gestores responsáveis pela área

auditada. Na reunião de abertura, foram apresentados os membros da equipe de auditoria, os objetivos do trabalho, o escopo e as questões de auditoria. Na reunião de encerramento, foi apresentado relatório preliminar com os achados resultantes dos testes aplicados. Na ocasião, foi possibilitada aos gestores manifestação sobre os achados. As respostas foram consideradas e incluídas neste relatório final.

II. VISÃO GERAL DO OBJETO AUDITADO

A governança de TI, segundo a ABNT NBR ISO/IEC 38500 (item 1.6.3), é o sistema pelo qual o uso atual e futuro da TI é dirigido e controlado. O IT *Governance Institute* (ITGI) – organismo internacional responsável por pesquisas sobre práticas e percepções globais de governança de TI para a comunidade – estabelece que "a governança de TI é de responsabilidade dos executivos e da alta direção, consistindo em aspectos de liderança, estrutura organizacional e processos que garantam que a área de TI da organização suporte e aprimore os objetivos e as estratégias da organização". Pode-se afirmar que a governança de TI é uma parte da governança corporativa que, em suma, consiste no estabelecimento de um conjunto de mecanismos com o objetivo de assegurar que o uso da TI agregue valor ao negócio com riscos aceitáveis, sendo responsabilidade dos executivos e da alta administração da organização prover a estrutura e garantir uma boa governança de TI.[1]

As organizações dependem fundamentalmente de recursos para funcionar. Recursos humanos, financeiros, materiais e imateriais. A informação é um recurso essencial para todas as organizações e a velocidade e volume com que informações são geradas cresce diariamente. Dessa forma, do momento em que as informações são geradas até o ponto em que elas devem ser descartadas, a tecnologia utilizada para armazenar, processar e transferir essas informações tem papel destacado. A tecnologia da informação evolui com rapidez e tem se difundido para a totalidade das atividades executadas, tanto nos ambientes domésticos quanto nos corporativos.

O cenário resultante é a busca constante das instituições e seus dirigentes para:

- Manter informações tempestivas e relevantes, ou seja, de alta qualidade e que suportem a tomada de decisões estratégicas e táticas;
- Planejar e executar investimentos em tecnologia da informação que resultem em benefícios valiosos para a organização. Por exemplo, utilizar a tecnologia da informação

[1] Tribunal de Contas da União: Relatório de Fiscalização TC 021.792/2013-5, Fiscalis 578/2013, Ministro-Relator: Weder de Oliveira, disponível em www.tcu.gov.br.

de forma efetiva e inovadora para transformar o ambiente organizacional, obtendo maior produtividade, maior qualidade e redução de custos;

- Conseguir a otimização dos seus processos operacionais por meio da aplicação de tecnologia da informação de forma confiável e eficiente;
- Manter os riscos relacionados com a aplicação de tecnologia da informação em níveis aceitáveis;
- Otimizar os custos envolvidos com o uso de tecnologia da informação;
- Manter a conformidade com a normatização relacionada ao tema, tais como, leis, jurisprudência, regulamentos, acordos contratuais e políticas diversas, entre outras.

Ao longo da última década a governança foi alçada a um nível elevado dentro das organizações, passando a ser o foco dos principais dirigentes. As instituições que têm obtido sucesso em seu desenvolvimento e aprimoramento necessariamente entenderam que os diretores e gestores devem se envolver com a governança de TIC tanto quanto se envolvem com outros temas estratégicos. Ou seja, a governança de TIC passou a ser assunto estratégico, estando sempre presente entre as preocupações dos dirigentes máximos das organizações.

Assim, os dirigentes máximos e os executivos da área de tecnologia da informação devem trabalhar de forma colaborativa para que a tecnologia seja inserida nas abordagens institucionais de governança e gestão. Além disso, os órgãos de controle demonstram que estão atentos para essa necessidade de sinergia entre a alta administração dos órgãos e suas áreas de tecnologia ao publicar normativos que exigem a interação entre a governança e a gestão dos órgãos públicos. As boas práticas mais atualizadas fazem clara distinção entre a governança e a gestão de TIC. De acordo com essas práticas, tais disciplinas envolvem atividades diferentes, exigem estruturas organizacionais diferentes e seus propósitos também são diversos.

A governança procura assegurar que as necessidades das diversas partes interessadas, as condições e as opções sejam avaliadas para definir objetivos organizacionais equilibrados e consensuais. Ainda no escopo da governança, está o estabelecimento da direção a ser seguida, que deve ser feito por meio da tomada de decisão e da priorização na aplicação de recursos. Todo o esforço desprendido para avaliar e direcionar deve ser monitorado para garantir que as decisões e priorizações sejam seguidas e que os resultados de tais decisões entreguem os benefícios idealizados no momento em que foram tomadas.

Nos Tribunais, a governança é responsabilidade da Presidência, que deve ter o apoio de instâncias internas de governança como o Comitê de Governança de TIC (CGTIC). A gestão de TIC deve planejar, construir, executar e controlar atividades alinhadas com a direção estabelecida pela Presidência e CGTIC, para

impulsionar o Tribunal na busca dos objetivos organizacionais. A gestão de TIC é de responsabilidade da Diretoria-Geral do Tribunal, apoiada pela Secretaria de Tecnologia da Informação.

As definições de governança e gestão deixam claro que cada uma das disciplinas é composta de tipos de atividades diferentes, com responsabilidades diversas para os atores envolvidos na execução de cada uma delas. Todavia, a responsabilidade de avaliar, dirigir e monitorar o uso da tecnologia da informação pelo Tribunal, atribuída à governança, exige uma interação constante entre as instâncias de governança e o corpo gestor, para que o sistema de governança seja efetivo.[2]

Na figura abaixo está disposto um diagrama que ilustra a distinção entre os domínios da governança e da gestão e o conjunto das interações necessárias entre eles.

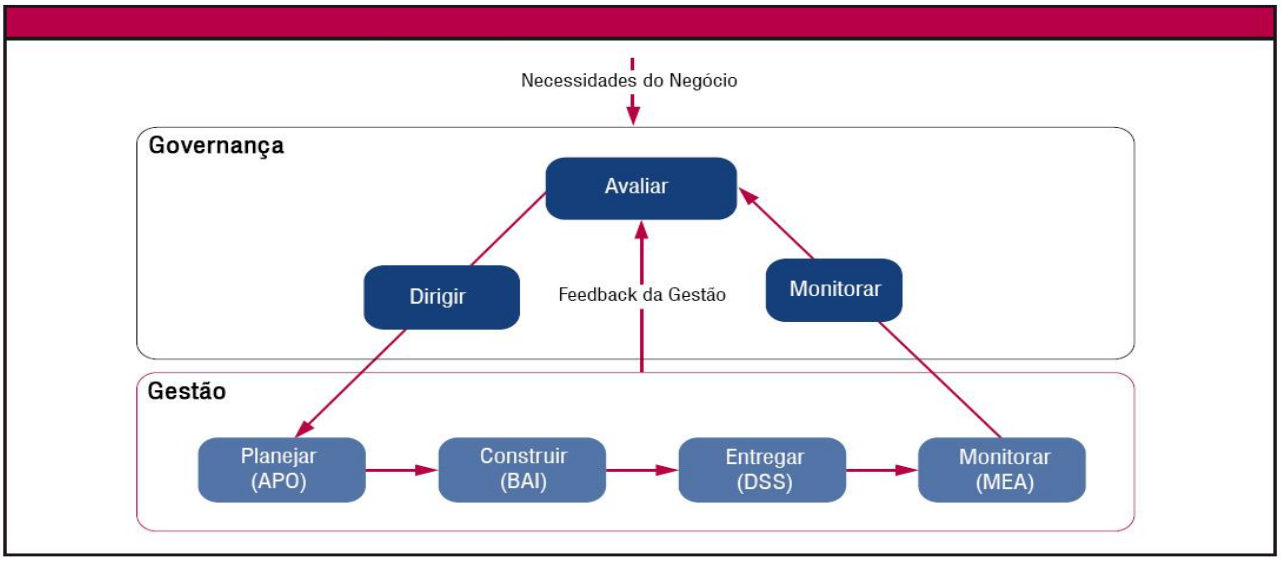

Figura 1: Domínios da governança e da gestão e as interações entre eles (fonte: COBIT 5).

III. OBJETIVO DA AUDITORIA

Este trabalho de auditoria visou avaliar os conteúdos estabelecidos para a governança e gestão de TIC, considerando projetos, processos, riscos e resultados de TI em comparação com padrões internacionalmente aceitos, como COBIT, PMBOK, ITIL, CMMI, ISO 17799, ISO 27001, as Resoluções CNJ n. 91/2009, n. 182/2013, n. 198/2014 e n. 211/2015 e o perfil de governança de TI traçado pelo TCU.

[2] Tribunal Regional do Trabalho da 9ª Região – Paraná, Secretaria de Auditoria Interna, Relatório de Auditoria AUDINT n. 09/2018.

IV. ESCOPO

A realização da auditoria compreendeu o período entre fevereiro a junho de 2018 e analisou, sob os aspectos da governança e gestão no âmbito da tecnologia da informação e comunicação, processos administrativos no Tribunal Regional Eleitoral de Mato Grosso do Sul, a partir de critérios definidos pelo Conselho Nacional de Justiça. Foram avaliados os seguintes aspectos: políticas e diretrizes, planos de TI, pessoal, gestão dos processos, planejamento das contratações de TI, resultados e atuação da unidade de auditoria interna.

V. CRITÉRIOS

Os critérios utilizados como parâmetros para a elaboração do questionário pela Secretaria de Controle Interno do Conselho Nacional de Justiça (SCI/ CNJ) para a Ação Coordenada de Auditoria com o tema Governança e Gestão de Tecnologia da Informação (0426433) foram os seguintes:

1) Referencial Básico de Governança do TCU;
2) Guia de boas práticas em contratação de soluções de tecnologia da informação do TCU;
3) ABNT NBR ISO 31000:2009 – Gestão de riscos – princípios e diretrizes;
4) ABNT NBR ISO 22313:2015 – Sistemas de gestão de continuidade de negócios;
5) ABNT NBR ISO 38500:2009 – Governança corporativa de tecnologia da informação;
6) ABNT NBR ISO 12207:2009 – Engenharia de sistemas e software – Processos de ciclo de vida de software;
7) ABNT NBR ISO 20000-2:2013 – Tecnologia da Informação – Gerenciamento de serviços – Parte 2: Guia de aplicação do sistema de gestão de serviços
8) ABNT NBR ISO 27001:2013 – Tecnologia da Informação – Sistemas de gestão da segurança da informação – Requisitos
9) ABNT NBR ISO 27002:2013 – Tecnologia da Informação – Técnicas de Segurança – Código de prática para controles de segurança da informação;
10) ABNT NBR ISO 27005:2011 – Tecnologia da Informação – Técnicas de Segurança – Gestão de riscos de segurança da informação;
11) COBIT 5 – *Control Objectives for Information and related Technology*;
12) ITIL 3.0 – *Information Technology Infrastructure Library*;

13) PMBoK – *A Guide to the Project Management Body of Knowledge*;
14) Acórdão TCU n. 1.603/2008 – Plenário;
15) Acórdão TCU n. 2.308/2010 – Plenário;
16) Acórdão TCU n. 1.233/2012 – Plenário;
17) Acórdão TCU n. 2.585/2012 – Plenário;
18) Resolução CNJ n. 171/2013;
19) Resolução CNJ n. 182/2013;
20) Resolução CNJ n. 198/2014;
21) Resolução CNJ n. 211/2015;
22) Decreto-Lei n. 200, de 25 de fevereiro de 1967;
23) Lei n. 12.527/2011 – Lei de Acesso a Informações (LAI);
24) Decreto n. 5.707/2006;
25) Medida Provisória n. 2.200-2, de 24 de agosto de 2001 (ICP-Brasil);
26) Norma Complementar n. 03/IN01/DSIC/GSIPR – Diretrizes para Elaboração de Política de Segurança da Informação e Comunicações nos Órgãos e Entidades da Administração Pública Federal;
27) Norma Complementar n. 04/IN01/DSIC/GSIPR – Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC;
28) Norma Complementar n. 05/IN01/DSIC/GSIPR – Criação de Equipes de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR;
29) Norma Complementar n. 07/IN01/DSIC/GSIPR – Diretrizes para Implementação de Controles de Acesso Relativos à Segurança da Informação e Comunicações;
30) Norma Complementar n. 08/IN01/DSIC/GSIPR – Gestão de ETIR: Diretrizes para Gerenciamento de Incidentes em Redes Computacionais nos Órgãos e Entidades da Administração Pública Federal;
31) Norma Complementar 10/IN01/DSIC/GSIPR – Inventário e Mapeamento de Ativos de Informação nos Aspectos Relativos à Segurança da Informação e Comunicações nos Órgãos e Entidades da Administração Pública Federal;
32) Norma Complementar 17/IN01/DSIC/GSIPR – Atuação e Adequações para Profissionais da Área de Segurança da Informação e Comunicações nos Órgãos e Entidades da Administração Pública Federal;

33) Norma Complementar 18/IN01/DSIC/GSIPR – Diretrizes para as Atividades de Ensino em Segurança da Informação e Comunicações nos Órgãos e Entidades da Administração Pública Federal.

VI. ACHADOS DE AUDITORIA

Os achados representam o resultado dos testes de auditoria aplicados e das informações coletadas nas reuniões de trabalho, guardando relação com o Programa de Auditoria (0423994). O programa para esta auditoria foi desenvolvido pelo CNJ, assim como o questionário de levantamento inicial.

Como ponto positivo, ressalta-se que três achados apontados no relatório preliminar (0498015) foram descaracterizados até a conclusão deste relatório final de auditoria, tendo em vista que as propostas de encaminhamento foram implementadas. Trata-se dos achados A18, A19 e A21. O achado A18 apontava a ausência de Comitê Gestor de Segurança da Informação, o qual foi constituído neste Regional pela Portaria Presidência n. 170/2018, publicada no DJE/MS n. 2002, de 18.7.2018, pág. 2/3. O Gestor de Segurança da Informação no TRE/MS foi designado pela Portaria Presidência n. 178/2018, publicada na mesma edição do DJE/MS, pág. 3.

Por sua vez, o achado A19 assinalava a ausência de Política de Segurança da Informação (PSI) formalmente instituída para o TRE/MS, que foi formalizada pela adoção da PSI do TSE pela Resolução TRE/MS n. 616/2018, publicada no DJE/MS n. 1958, de 11.5.2018, pág. 12.

Por fim, o achado A21 indicava a ausência de Equipe de Resposta a Incidentes de Segurança em Redes Computacionais (ETIR), a qual foi criada pela Portaria Presidência n. 206/2018, publicada no DJE/MS n. 2021, de 14.8.2018, pág. 3/6.

A seguir, apresentam-se as atividades auditadas com os riscos identificados, o resultado dos testes de auditoria, as questões gerais avaliadas, o comentário da unidade auditada e a conclusão da equipe de auditoria.

A1 – AUSÊNCIA DE DIRETRIZES FORMAIS PARA PLANEJAMENTO DE TI, GESTÃO DO PORTFÓLIO DE PROJETOS E DE SERVIÇOS DE TI, CONTRATAÇÃO DE BENS E SERVIÇOS DE TI E AVALIAÇÃO DO DESEMPENHO DOS SERVIÇOS DE TI.

Situação encontrada: Não existe política formal instituída para planejamento de TI; gestão do portfólio de projetos e de serviços de TI; contratação de bens e serviços de TI; avaliação do desempenho dos

serviços de TI.

Evidência: Informação N. 4622 - TRE/PRE/DG/STI/GABSTI (0443192).

Critérios: ISO 38500 e Acórdão TCU n. 1.603/2008 - Plenário.

Manifestação do Auditado: *Solicitamos mais esclarecimentos para o mesmo porque possuímos normativo para o item CONTRATAÇÕES DE BENS E SERVIÇOS DE TI (0506247).*

Conclusão da Equipe de Auditoria: Achado mantido. Esclareceu-se na Informação N. 10999 - TRE/PRE/CCIA/SCAA (0506619) que o achado teve por base as respostas prestadas no Questionário de Levantamento de Informações para Auditoria CNJ nas questões n. 4, 5, 6 e 7. Foi solicitada a remessa do normativo sobre Contratação de Bens e Serviços de TI para avaliação, porém a unidade auditada não o enviou.

Proposta de Encaminhamento: Instituir política formal para as seguintes áreas:

a) Planejamento de TI;
b) Gestão do portfólio de projetos e de serviços de TI;
c) Contratação de bens e serviços de TI;
d) Avaliação do desempenho dos serviços de TI.

A2 – AUSÊNCIA DE POLÍTICA DE GESTÃO DE RISCOS DE TI.

Situação encontrada: Inexistência de política de gestão de riscos de TI definida para o TRE/MS.

Evidência: Informação N. 4622 - TRE/PRE/DG/STI/GABSTI (0443192).

Critérios: ISO 31000 e COBIT 5.

Manifestação do Auditado: *Sem considerações (0506247).*

Conclusão da Equipe de Auditoria: Achado mantido.

Proposta de Encaminhamento: Instituir política de gestão de riscos de TI que contemple a definição de papéis e responsabilidades e sua comunicação formal; níveis de risco aceitáveis; e que as tomadas de decisões estratégicas considerem os níveis de risco de TI definidos.

A3 – AUSÊNCIA DE INCENTIVOS PARA DESENVOLVIMENTO E RETENÇÃO DE PESSOAL DE TI.

Situação encontrada: Inexistência de política formal para a gestão de pessoal de TI, para a avaliação e incentivo ao desempenho de gestores e técnicos de TI e para a escolha dos líderes de TI.

Evidência: Informação N. 4622 - TRE/PRE/DG/STI/GABSTI (0443192).

Critérios: Resolução CNJ n. 211/2015, Acórdão TCU n. 1.233/2012 – Plenário, ISO 38500 e COBIT 5.

Manifestação do Auditado: *Sem considerações (0506247).*

Conclusão da Equipe de Auditoria: Achado mantido.

Proposta de Encaminhamento: Instituir políticas formais para:

a) Gestão de pessoas, de forma a promover o desenvolvimento de competências e a retenção de gestores e técnicos de TI.

b) Avaliação e incentivo ao desempenho de gestores e técnicos de TI.

c) Escolha dos líderes da área de TI, ocupantes de cargos de chefia e de assessoramento.

A4 – AUSÊNCIA DE COMUNICAÇÃO COM PARTES INTERESSADAS SOBRE OS RESULTADOS DE TI.

Situação encontrada: Inexistência de diretrizes formais para comunicação dos resultados da gestão e do uso de TI para as partes interessadas (públicos interno e externo).

Evidência: Informação N. 4622 - TRE/PRE/DG/STI/GABSTI (0443192).

Critérios: ISO 38500, COBIT 5 e Acórdão TCU n. 2.585/2012 – Plenário.

Manifestação do Auditado: *Sem considerações (0506247).*

Conclusão da Equipe de Auditoria: Achado mantido.

Proposta de Encaminhamento: Instituir diretrizes formais para comunicação com as partes interessadas, considerando os públicos interno e externo, sobre os resultados da gestão e do uso de TI que contemple: a) Divulgação; b) Conteúdo; c) Frequência; e d) Formato das comunicações.

A5 – AUSÊNCIA DE AVALIAÇÃO DA GOVERNANÇA E/OU GESTÃO DE TI.

Situação encontrada: Inexistência de diretrizes para avaliação da governança e da gestão de TI.

Evidência: Informação N. 4622 - TRE/PRE/DG/STI/GABSTI (0443192).

Critérios: ISO 38500 e COBIT 5.

Manifestação do Auditado: *Sem considerações (0506247).*

Conclusão da Equipe de Auditoria: Achado mantido.

Proposta de Encaminhamento: Instituir diretrizes para avaliação da governança e da gestão de TI, com realização de avaliações periódicas de:

a) Governança e gestão de TI;

b) Sistemas de informação;

c) Segurança da informação; e

d) Contratos de TI.

A6 – AUSÊNCIA DE POLÍTICAS DE CONTROLE DE ACESSO AOS RECURSOS DE TI.

Situação encontrada: Inexistência de política formal para o controle de acesso à informação e aos recursos e serviços de TI.

Evidência: Informação N. 4622 - TRE/PRE/DG/STI/GABSTI (0443192).

Critério: ISO 27002:05.

Manifestação do Auditado: *Sem considerações (0506247).*

Conclusão da Equipe de Auditoria: Achado mantido.

Proposta de Encaminhamento: Instituir política formal de controle de acesso à informação, aos recursos e serviços de TI.

A7 – AUSÊNCIA DE POLÍTICAS DE CÓPIA DE SEGURANÇA (BACKUP).

Situação encontrada: Inexistência de política formal para a realização de cópias de segurança (backup).

Evidência: Informação N. 4622 - TRE/PRE/DG/STI/GABSTI (0443192).

Critério: ISO 27002:05.

Manifestação do Auditado: *Sem considerações (0506247).*

Conclusão da Equipe de Auditoria: Achado mantido.

Proposta de Encaminhamento: Instituir política formal para a realização de cópias de segurança (backup).

A8 – AUSÊNCIA DE ACOMPANHAMENTO E REVISÃO DO PLANO ESTRATÉGICO DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO (PETIC).

Situação encontrada: Embora exista PETIC vigente, ele não é acompanhado e revisado periodicamente e a proposta orçamentária de TI não é feita com base nos objetivos estratégicos nele definidos.

Evidência: Informação N. 4622 - TRE/PRE/DG/STI/GABSTI (0443192).

Critérios: Resolução CNJ n. 211/2015, Acórdão TCU n. 1.603/2008 – Plenário, Acórdão TCU n. 2.308/2010 – Plenário, Acórdão TCU n. 1.233/2012 – Plenário, Acórdão TCU n. 2.585/2012 – Plenário, COBIT 5 e Resolução TRE/MS n. 557/2016.

Manifestação do Auditado: *Gostaríamos de sugerir que a recomendação fosse alterada para "...exercício 2020 e seguintes.", uma vez que a proposta orçamentária de 2019 foi encerrada em Março/2018 e não temos mais como alterá-la. (0506247).*

Conclusão da Equipe de Auditoria: Achado mantido. Foi acolhida a sugestão para constar na proposta de encaminhamento os exercícios 2020 e seguintes.

Proposta de Encaminhamento: Efetuar o efetivo acompanhamento da execução do PETIC, conforme determinado no artigo 2º, da Resolução TRE/MS n. 557/2016; promover sua revisão periódica e considerar o PETIC para fundamentar as propostas orçamentárias de TI para os exercícios 2020 e seguintes.

A9 – AUSÊNCIA DE PLANO DIRETOR DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO (PDTIC).

Situação encontrada: O Plano Diretor de Tecnologia da Informação do TRE/MS (0109348) está vencido e não há previsão de elaboração do próximo.

Evidência: Informação N. 6346 - TRE/PRE/CCIA/SCAA (0458292).

Critérios: Resolução CNJ n. 211/2015, Acórdão TCU n. 1.603/2008 – Plenário, Acórdão TCU n. 2.308/2010 – Plenário, Acórdão TCU n. 1.233/2012 – Plenário, Acórdão TCU n. 2.585/2012 – Plenário e COBIT 5.

Manifestação do Auditado: *Sem considerações (0506247).*

Conclusão da Equipe de Auditoria: Achado mantido.

Proposta de Encaminhamento: Instituir formalmente Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) que:

a) Contemple as ações a serem desenvolvidas com vinculação às estratégias institucional e nacional do Poder Judiciário;
b) Vincule as ações e projetos a indicadores e metas de negócio;
c) Cuja execução seja periodicamente acompanhada; e
d) Haja revisão periódica.

A10 – AUSÊNCIA DE DEFINIÇÃO DAS COMPETÊNCIAS NECESSÁRIAS PARA O PESSOAL DE TI.

Situação encontrada: Não há definição de quais são as competências necessárias para o pessoal de TI.

Evidência: Informação N. 4622 - TRE/PRE/DG/STI/GABSTI (0443192).

Critérios: Resolução CNJ n. 211/2015 e Acórdão TCU n. 1.603/2008 – Plenário.

Manifestação do Auditado: *Sem considerações (0506247).*

Conclusão da Equipe de Auditoria: Achado mantido.

Proposta de Encaminhamento: Definir as competências necessárias para o pessoal de TI executar suas atividades e apresentar relação à Secretaria de Gestão de Pessoas (SGP), para que tal definição seja considerada no projeto de Gestão por Competências.

A11 – AUSÊNCIA DE PLANO ANUAL DE CAPACITAÇÃO PARA O PESSOAL DE TI (PAC-TI) E DE ACOMPANHAMENTO DOS RESULTADOS DO PAC-TI.

Situação encontrada: Inexistência de Plano Anual de Capacitação para o pessoal de TI vigente e com revisão periódica.

Evidência: Informação N. 4622 - TRE/PRE/DG/STI/GABSTI (0443192).

Critérios: Resolução CNJ n. 211/2015 e Acórdão TCU n. 1.233/2012 – Plenário.

Manifestação do Auditado: *Sem considerações (0506247).*

Conclusão da Equipe de Auditoria: Achado mantido.

Proposta de Encaminhamento: Apresentar minuta de Plano Anual de Capacitação para o pessoal de TI à SGP que contemple:

a) Previsão para sua revisão periódica;
b) Diretrizes para avaliação e atendimento aos pedidos de capacitação em TI;
c) Desenvolvimento de competências em governança e gestão de TI;
d) Desenvolvimento de competências em contratação de bens e serviços de TI e em gestão de contratos de TI;
e) Previsão para acompanhamento da execução do Plano, inclusive dos objetivos e resultados esperados.

A12 – AUSÊNCIA DE ACOMPANHAMENTO DO DESEMPENHO DO PESSOAL DE TI.

Situação encontrada: Inexistência de avaliação de desempenho específica para o pessoal de TI.

Evidência: Informação N. 4622 - TRE/PRE/DG/STI/GABSTI (0443192).

Critérios: Resolução CNJ n. 211/2015, COBIT 5 (APO 07.04).

Manifestação do Auditado: *Sem considerações (0506247).*

Conclusão da Equipe de Auditoria: Achado mantido.

Proposta de Encaminhamento: Estabelecer metas de desempenho para o pessoal de TI e acompanhá-las periodicamente.

A13 – AUSÊNCIA DE PREVISÃO DOS QUANTITATIVOS IDEAIS DA FORÇA DE TRABALHO DE TI.

Situação encontrada: Não há previsão do quantitativo ideal da força de trabalho de TI.

Evidência: Informação N. 4622 - TRE/PRE/DG/STI/GABSTI (0443192).

Critérios: Resolução CNJ n. 211/2015, Acórdão TCU n. 1.603/2008 – Plenário, Acórdão TCU n. 1.233/2012 – Plenário e COBIT 5 (APO 07.01).

Manifestação do Auditado: *Sem considerações (0506247).*

Conclusão da Equipe de Auditoria: Achado mantido.

Proposta de Encaminhamento: Apresentar à SGP os quantitativos ideais de força de trabalho de TI, estimados com base:

a) Em estudo técnico que indique o número de usuários internos e externos de recursos de TI; e

b) No anexo da Resolução CNJ n. 211/2015.

A14 – AUSÊNCIA DE PROCESSOS DE GESTÃO DE SERVIÇOS FORMALMENTE INSTITUÍDOS.

Situação encontrada: Não há processos de gerenciamento formalmente instituídos no âmbito do TRE/MS.

Evidência: Informação N. 4622 - TRE/PRE/DG/STI/GABSTI (0443192).

Critérios: Resolução CNJ n. 211/2015, Acórdão TCU n. 1.233/2012 – Plenário, ITIL 3 (*Service Strategy*, *Service Design*, *Service Transition*, *Service Operation*).

Manifestação do Auditado: *Sem considerações (0506247).*

Conclusão da Equipe de Auditoria: Achado mantido.

Proposta de Encaminhamento: Instituir processos de gerenciamento de:

a) Portfólio de serviços;

b) Catálogo de serviços;

c) Continuidade dos serviços de TI;

d) Mudanças;

e) Configuração e de ativos;

f) Liberação e implantação;

g) Incidentes;

h) Eventos;

i) Problemas; e

j) Acesso.

A15 – AUSÊNCIA DE PLANO DE CONTINUIDADE DE SERVIÇOS ESSENCIAIS DE TI.

Situação encontrada: Inexistência de Plano de Continuidade de Serviços Essenciais de TI.

Evidência: Informação N. 4622 - TRE/PRE/DG/STI/GABSTI (0443192).

Critérios: Resolução CNJ n. 211/2015, Acórdão TCU n. 1.233/2012 – Plenário e ITIL 3.

Manifestação do Auditado: *Sem considerações (0506247).*

Conclusão da Equipe de Auditoria: Achado mantido.

Proposta de Encaminhamento: Instituir e aplicar Plano de Continuidade de Serviços Essenciais de TI.

A16 – AUSÊNCIA DE ACORDOS DE NÍVEIS DE SERVIÇO (ANS) E DE GERENCIAMENTO DOS NÍVEIS DE SERVIÇO.

Situação encontrada: Inexistência de catálogo de serviços e TI, com níveis de serviço entre a área de TI e as áreas clientes.

Evidência: Informação N. 4622 - TRE/PRE/DG/STI/GABSTI (0443192).

Critérios: Resolução CNJ n. 211/2015, Acórdão TCU n. 1.603/2008 – Plenário, ISO 20000:08 e ITIL 3 (Service Design).

Manifestação do Auditado: *Sem considerações (0506247).*

Conclusão da Equipe de Auditoria: Achado mantido.

Proposta de Encaminhamento: Instituir catálogo de serviços de TI com os níveis de serviço entre a área de TI e as áreas clientes formalmente definidos (Acordo de Nível de Serviço – ANS) e que:

a) Os ANS incluam indicador de grau de satisfação dos usuários;

b) Os níveis de serviço definidos sejam monitorados;

c) Previsão de ações corretivas para as situações de não alcance dos níveis definidos;

d) Comunicação periódica às áreas clientes dos resultados do monitoramento.

A17 – AUSÊNCIA DE PROCESSOS DE GESTÃO DE RISCOS DE TI.

Situação encontrada: Inexistência de processo formalmente instituído de gestão de riscos de TI.

Evidência: Informação N. 4622 - TRE/PRE/DG/STI/GABSTI (0443192).

Critérios: Resolução CNJ n. 211/2015, ISO 38500:09, ISO 31000:09, COBIT 5 (APO 12).

Manifestação do Auditado: *Sem considerações (0506247).*

Conclusão da Equipe de Auditoria: Achado mantido.

Proposta de Encaminhamento: Instituir processo de gestão de riscos de TI, em que os riscos de TI dos processos críticos de negócio sejam: a) Identificados; b) Avaliados; e c) Tratados com base em plano de tratamento de riscos.

A18 – AUSÊNCIA DE COMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO.

Situação encontrada: Inexistência de Comitê Gestor de Segurança da Informação formalmente instituído no TRE/MS.

Evidência: Informação N. 4622 - TRE/PRE/DG/STI/GABSTI (0443192).

Critérios: Resolução CNJ n. 211/2015, Acórdão TCU n. 1.233/2012 – Plenário, ISO 27002:05, ISO 27005:08 e NC 03/IN01/DSIC/GSIPR.

Manifestação do Auditado: *A Comissão de Segurança da Informação foi nomeada, conforme Portaria PRE n. 170/2018 (0506247).*

Conclusão da Equipe de Auditoria: Achado atendido.

A19 – AUSÊNCIA DE POLÍTICA DE SEGURANÇA DA INFORMAÇÃO.

Situação encontrada: Inexistência de Política de Segurança da Informação formalmente instituída para o TRE/MS.

Evidência: Informação N. 4622 - TRE/PRE/DG/STI/GABSTI (0443192).

Critérios: Resolução CNJ n. 211/2015, Acórdão TCU n. 1.233/2012 – Plenário, ISO 27002:05, ISO 27005:08 e NC 03/IN01/DSIC/GSIPR.

Manifestação do Auditado: *A política de segurança da informação foi aprovada no TRE-MS, conforme Resolução TRE-MS n. 616/2018 (0506247).*

Conclusão da Equipe de Auditoria: Achado atendido.

A20 – AUSÊNCIA DE PROCESSOS DE GESTÃO DA SEGURANÇA DA INFORMAÇÃO.

Situação encontrada: Inexistência de processos de gestão da segurança da informação formalmente instituídos.

Evidência: Informação N. 4622 - TRE/PRE/DG/STI/GABSTI (0443192).

Critérios: Resolução CNJ n. 211/2015, Acórdão TCU n. 1.233/2012 – Plenário, ISO 27002:05, ISO 27005:08 e NC 03/IN01/DSIC/GSIPR.

Manifestação do Auditado: *Sem considerações (0506247).*

Conclusão da Equipe de Auditoria: Achado mantido.

Proposta de Encaminhamento: Instituir processos de gestão da segurança da informação que englobem:

a) Classificação e tratamento de informações, com controles que garantam a proteção adequada ao grau de confidencialidade de cada classe de informação;
b) Riscos;
c) Vulnerabilidades técnicas de TI;
d) Monitoramento do uso dos recursos de TI; e
e) Incidentes de segurança da informação.

A21 – AUSÊNCIA DE EQUIPE DE RESPOSTA A INCIDENTES DE SEGURANÇA EM REDES COMPUTACIONAIS (ETIR).

Situação encontrada: Inexistência de ETIR instituída no TRE/MS.

Evidência: Informação N. 4622 - TRE/PRE/DG/STI/GABSTI (0443192).

Critérios: NC 05/IN01/DSIC/GSIPR.

Manifestação do Auditado: *Sem considerações (0506247).*

Conclusão da Equipe de Auditoria: Embora não tenha havido manifestação do auditado sobre o achado, foi identificada no DJE/MS n. 2021, de 14.8.2018, pág. 3/6, a publicação da Portaria Presidência n. 206/2018, que instituiu a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR) no âmbito do TRE/MS. Portanto, o achado foi atendido.

A22 – AUSÊNCIA DE AÇÕES DE CONSCIENTIZAÇÃO DOS COLABORADORES QUANTO À SEGURANÇA DA INFORMAÇÃO.

Situação encontrada: Não são realizadas ações de sensibilização, conscientização e capacitação em segurança da informação para os agentes públicos do TRE/MS.

Evidência: Informação N. 4622 - TRE/PRE/DG/STI/GABSTI (0443192).

Critérios: NC 18/IN01/DSIC/GSIPR.

Manifestação do Auditado: *Sem considerações (0506247).*

Conclusão da Equipe de Auditoria: Achado mantido.

Proposta de Encaminhamento: Realizar, periodicamente, ações de conscientização, educação (capacitação) e treinamento em segurança da informação para os agentes públicos do TRE/MS. Para tal fim, entende-se como agente público, "todo aquele que exerce, ainda que transitoriamente ou sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função no TRE/MS."

A23 – AUSÊNCIA DE PROCESSO DE SOFTWARE INSTITUÍDO.

Situação encontrada: Inexistência de processo de software formalmente instituído.

Evidência: Informação N. 4622 - TRE/PRE/DG/STI/GABSTI (0443192).

Critérios: Resolução CNJ n. 211/2015, Acórdão TCU n. 1.233/2012 – Plenário e ISO 12207/09.

Manifestação do Auditado: *Sugestão de acréscimo da palavra "DESENVOLVIMENTO" e retirada da palavra "INSTITUÍDO", ou seja, "AUSÊNCIA DE PROCESSO DE DESENVOLVIMENTO DE SOFTWARE" (0506247).*

Conclusão da Equipe de Auditoria: Achado mantido. Foi esclarecido, na Informação Nº 10999 - TRE/PRE/CCIA/SCAA (0506619) que o verbete "instituído" no título do achado possui o significado de "formalmente definido". Quanto à expressão "processo de software", ressalta-se que é a linguagem utilizada tanto pelo Conselho Nacional de Justiça, na Resolução CNJ n. 211/2015, quanto pelo Tribunal de Contas da União, no Acórdão n. 1233/2012 - Plenário. Neste, esclarece o TCU:

> Processo de software
>
> Constam da ABNT NBR ISO/IEC 12.207 as seguintes definições:
>
> 4.25 processo – conjunto de atividades que se relacionam ou interagem e que transformam entradas em saídas [ABNT NBR ISO 9000:2005].
>
> (...)
>
> 4.28 produto – resultado de um processo [ABNT NBR ISO 9000:2005].
>
> (...)
>
> 4.42 produto de software – conjunto de programas de computador, procedimentos e possíveis documentação e dados associados.
>
> Um processo de software é, portanto, um conjunto de atividades que transformam requisitos de usuários (entrada do processo) em um produto de software. Por oportuno, chamamos a atenção para o fato de que o produto de software não é composto apenas dos programas de computadores, mas inclui outros itens. Mais

ainda, destacamos que os diversos itens que compõem o produto de software são gerados ao longo da execução do processo de software.

Portanto, acrescentar a palavra "desenvolvimento" antes da palavra "software" poderia restringir o alcance da expressão, o que não foi o intento do CNJ na condução da referida Ação Coordenada de Auditoria.

Proposta de Encaminhamento: Instituir processo de software que seja: a) Acompanhado por meio de mensurações, com indicadores quantitativos e metas; b) Periodicamente revisado; e c) Gerenciado por pessoal próprio e capacitado.

A24 – AUSÊNCIA DE GERENCIAMENTO DO PORTFÓLIO DE PROJETOS DE TI.

Situação encontrada: Inexistência de processo de gerenciamento do portfólio de projetos de TI.

Evidência: Informação N. 4622 - TRE/PRE/DG/STI/GABSTI (0443192).

Critérios: Resolução CNJ n. 211/2015 e PMBOK 5ª Edição.

Manifestação do Auditado: *Sem considerações (0506247).*

Conclusão da Equipe de Auditoria: Achado mantido.

Proposta de Encaminhamento: Instituir formalmente processo de gerenciamento de portfólio de projetos de TI.

A25 – AUSÊNCIA DE ACOMPANHAMENTO NO PROCESSO DE GERENCIAMENTO DE PROJETOS DE TI.

Situação encontrada: Não há acompanhamento no gerenciamento de projetos de TI.

Evidência: Informação N. 4622 - TRE/PRE/DG/STI/GABSTI (0443192).

Critérios: Resolução CNJ n. 211/2015, Acórdão TCU n. 1.233/2012 – Plenário, PMBOK 5ª Edição e COBIT 5.

Manifestação do Auditado: *Sem considerações (0506247).*

Conclusão da Equipe de Auditoria: Achado mantido.

Proposta de Encaminhamento: Acompanhar, por meio de mensurações, o gerenciamento de projetos de TI e revisá-lo periodicamente.

A26 – AUSÊNCIA DE PLANO DE CONTRATAÇÕES DE TI.

Situação encontrada: Inexistência de plano de contratações de soluções de tecnologia da informação e comunicação formalmente instituído.

Evidência: Informação N. 4622 - TRE/PRE/DG/STI/GABSTI (0443192).

Critérios: Resolução CNJ n. 182/2013 e Guia Boas Práticas TCU.

Manifestação do Auditado: *Sem considerações (0506247).*

Conclusão da Equipe de Auditoria: Achado mantido.

Proposta de Encaminhamento: Instituir plano de contratações de soluções de tecnologia da informação e comunicação que:

a) Inclua as contratações necessárias ao alcance dos objetivos estabelecidos nos planejamentos estratégicos e institucional de TI.
b) Seja revisado periodicamente para incluir novas contratações pretendidas; e
c) Contenha prazos de entrega dos Estudos Preliminares e dos Projetos Básicos ou Termos de Referência.

A27 – AUSÊNCIA DE MEDIÇÃO DOS RESULTADOS DOS OBJETIVOS ESTRATÉGICOS.

Situação encontrada: Inexistência de monitoramento, com medições periódicas e revisões, nos objetivos estratégicos e táticos de TI.

Evidência: Informação N. 4622 - TRE/PRE/DG/STI/GABSTI (0443192).

Critérios: Resolução Acórdão TCU n. 2.308/2010, ISO 38500:09 e COBIT 5 (EDM2 e 4, MEA1).

Manifestação do Auditado: *Sem considerações (0506247).*

Conclusão da Equipe de Auditoria: Achado mantido.

Proposta de Encaminhamento: Monitorar, com medições periódicas e revisões, os objetivos estratégicos e táticos de TI que constam no PETIC e no PDTIC.

A28 – AUSÊNCIA DE DIVULGAÇÃO DOS RESULTADOS DOS OBJETIVOS, DAS AÇÕES E DOS PROJETOS DE TI.

Situação encontrada: Os resultados dos objetivos, das ações e dos projetos de TI não são divulgados.

Evidência: Informação N. 4622 - TRE/PRE/DG/STI/GABSTI (0443192).

Critérios: Acórdão TCU n. 2.585/2012 – Plenário, Acórdão TCU n. 1.233/2012 – Plenário e COBIT 5.

Manifestação do Auditado: *Sem considerações (0506247).*

Conclusão da Equipe de Auditoria: Achado mantido.

Proposta de Encaminhamento: Divulgar informações sobre os resultados dos objetivos de TI e o acompanhamento das ações e projetos de TI que constam no PETIC e PDTIC.

A29 – AUSÊNCIA DE MEDIÇÃO DO GRAU DE ALCANCE DOS OBJETIVOS E BENEFÍCIOS ESPERADOS NOS PROJETOS DE TI.

Situação encontrada: Não há medição do grau de alcance dos objetivos e benefícios que justificaram a abertura de projetos de TI.

Evidência: Informação N. 4622 - TRE/PRE/DG/STI/GABSTI (0443192).

Critérios: COBIT 5 (EDM02, BAI01) e PMBOK 5ª Edição.

Manifestação do Auditado: *Sem considerações (0506247).*

Conclusão da Equipe de Auditoria: Achado mantido.

Proposta de Encaminhamento: Implementar medição do grau de alcance dos objetivos e benefícios que justificam a abertura de projetos de TI e verificar se os resultados são satisfatórios.

A30 – AUSÊNCIA DE ESTIMATIVA ORÇAMENTÁRIA NOS PROJETOS DE TI.

Situação encontrada: Os projetos de TI não possuem orçamento estimado.

Evidência: Informação N. 4622 - TRE/PRE/DG/STI/GABSTI (0443192).

Critérios: PMBOK 5ª Edição.

Manifestação do Auditado: *Sem considerações (0506247).*

Conclusão da Equipe de Auditoria: Achado mantido.

Proposta de Encaminhamento: Estimar o orçamento dos projetos de TI no início e acompanhá-lo durante a sua execução, verificando se há diferenças significativas entre a estimativa inicial e o valor real obtido ao final e levantar os motivos para as eventuais diferenças significativas encontradas.

A31 – AUSÊNCIA DE AVALIAÇÃO PERIÓDICA DA EFETIVA UTILIZAÇÃO DOS SISTEMAS INFORMATIZADOS QUE SUPORTAM O NEGÓCIO.

Situação encontrada: Não existe levantamento dos processos críticos que dependam de sistemas de TI.

Evidência: Informação N. 4622 - TRE/PRE/DG/STI/GABSTI (0443192).

Critérios: Acórdão TCU n. 2.585/2012 – Plenário e COBIT 5 (APO 01.06).

Manifestação do Auditado: *Sem considerações (0506247).*

Conclusão da Equipe de Auditoria: Achado mantido.

Proposta de Encaminhamento:

a) Implementar verificação se os processos críticos de negócio são suportados por sistemas informatizados;

b) Designar formalmente os responsáveis da área de negócio para a gestão dos respectivos sistemas informatizados;

c) Implementar avaliação periódica da efetiva utilização dos sistemas informatizados que suportam o negócio.

A32 – IMPLANTAÇÃO INCOMPLETA DAS AÇÕES PREVISTAS PARA OS GRUPOS 1 E 2 DO PLANO DE TRABALHO A QUE SE REFERE O ART. 29 DA RESOLUÇÃO CNJ N. 211/2015.

Situação encontrada: Não foram implementadas todas as iniciativas programadas no Plano de Trabalho previsto no art. 29 da Resolução CNJ n. 211/2015.

Evidência: Plano de Trabalho 0456374.

Critérios: Resolução CNJ n. 211/2015.

Manifestação do Auditado: *Sem considerações (0506247).*

Conclusão da Equipe de Auditoria: Achado mantido.

Proposta de Encaminhamento: Implementar todas as ações programadas e constantes do Plano de Trabalho 0456374 em relação aos Grupos 1 e 2, conforme especificado no § 1º do art. 29 da Resolução CNJ n. 211/2015.

A33 – FALHAS NA ATUAÇÃO DA UNIDADE DE AUDITORIA INTERNA.

Situação encontrada: Ausência de exames de auditoria para aferir o estágio de Governança e de Gestão de TIC no TRE/MS.

Evidência: Durante a auditoria não foram encontradas evidências de atuação da Unidade de Auditoria Interna do TRE/MS, durante os anos de 2015, 2016 e 2017, na realização de exames de auditoria com avaliações detalhadas sobre o estágio da Governança e da Gestão de TIC, inclusive nos aspectos relativos aos riscos afetos à segurança da informação, dos serviços judiciais e aos demais ativos de TIC críticos do órgão. Foram encontradas evidências de avaliações no ano de 2014, relativas às contratações de soluções de TIC, porém os objetivos de tais avaliações ficaram restritos aos aspectos de conformidade legal com a legislação correlata aos procedimentos licitatórios. Não foram avaliados os aspectos de riscos relacionados com a

importância estratégica e os benefícios a serem obtidos com as referidas contratações. Também não se localizou evidência da execução de exames de auditoria para verificar a implementação das diretrizes formuladas pelo CNJ na Resolução CNJ n. 211/2015, que instituiu a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD), nem avaliação ou acompanhamento da implementação do Plano de Trabalho previsto no artigo 29 da mesma Resolução.

Critérios: Acórdão TCU n. 1.233/2012 – Plenário, Acórdão TCU n. 1.273/2015 – Plenário, Acórdão TCU n. 2.622/2015 – Plenário, Resolução CNJ n. 211/2015.

Manifestação do Auditado: Não houve manifestação do auditado acerca do achado e da situação encontrada.

Conclusão da Equipe de Auditoria: A atuação da unidade de Auditoria Interna em relação aos processos de TIC tem se mostrado aquém da ideal. A demanda por avaliações de auditoria em tal área é crescente, a exemplo do Acórdão TCU n. 1.233/2012 – Plenário, das Resoluções CNJ n. 182/2013 e n. 211/2015, dos questionários anuais de avaliação de TIC enviados pelo CNJ, da Resolução TSE n. 23.501/2016 e da Resolução TRE/MS n. 616/2018. A especialização da equipe de auditores nas áreas auditadas é uma necessidade que urge, principalmente em TIC, em que não há nenhum servidor com especialidade na área dentre os lotados na CCIA.

Desse modo, conclui-se que a unidade de Auditoria Interna deixou de apoiar as instâncias de governança e gestão de TIC do órgão, por não fornecer avaliações imparciais dos controles internos de TIC que permitam concluir, com nível razoável de segurança, que tais controles são efetivos na resposta aos riscos relacionados ao uso de tecnologia da informação. Em consequência, os gestores deixaram de obter informações de qualidade, ou seja, informações relevantes e oportunas para tomada de decisão e eventuais correções de desvios.

A falta de atuação da Unidade de Auditoria Interna nas avaliações descritas expõe o órgão ao risco de manter controles internos de TIC ineficazes e até mesmo de não implementação de tais controles. Consequentemente, não há a redução da probabilidade, nem do impacto, relacionados aos investimentos que não entregam os benefícios esperados, não otimizam a alocação de recursos e não mantém o adequado nível de segurança da informação.

Proposta de Encaminhamento: Recomenda-se à Administração do TRE/MS que lote ao menos um servidor da área de TIC na Auditoria Interna, a fim de viabilizar que a unidade elabore o Plano Anual de Auditoria considerando os diversos riscos de TIC aos quais o Regional está exposto e insira a execução de exames de auditoria nos controles de governança e gestão de TIC. Dessa maneira, a unidade de Auditoria

Interna atuará de forma a gerar valor para os tomadores de decisão, com a emissão de recomendações assertivas que assegurem a redução dos riscos relacionados com TIC, bem como a obtenção dos resultados e benefícios almejados com tais investimentos. É imperioso destacar que a área de TIC é a que o TCU e o CNJ mais têm cobrado ações de controle e atividades de auditoria interna. A relevância da tecnologia da informação e a criticidade dos processos a ela relacionados recomendam inserir nas prioridades institucionais a disponibilização de um servidor da área de TIC para estar em exercício na unidade de auditoria interna.

VII. CONCLUSÃO

A principal conclusão deste trabalho diz respeito à baixa maturidade da governança de TI no Tribunal Regional Eleitoral de Mato Grosso do Sul, vez que a instituição não estabeleceu alguns dos processos e políticas recomendados para uma boa governança corporativa de TI.

Sobre o panorama da governança de TI no TRE/MS, cabe destacar, inicialmente, que o órgão não dispõe de normas que definam diretrizes para as seguintes questões de governança de TI: gestão dos riscos aos quais o negócio está exposto; planejamento de TI; gestão do portfólio de projetos e serviços de TI; contratação de bens e serviços de TI; avaliação do desempenho dos serviços de TI junto às unidades usuárias em termos de resultado de negócio institucional, inclusive para definição de critérios de sua priorização, inclusão, exclusão, manutenção e suprimento orçamentário; controle de acesso aos recursos de TI; cópia de segurança (backup).

Também não há Plano Diretor de Tecnologia da Informação e Comunicação; acompanhamento e revisão do Plano Estratégico de Tecnologia da Informação e Comunicação; definição das competências necessárias para o pessoal de TI; incentivos para o desenvolvimento e retenção de pessoal de TI; plano anual de capacitação para o pessoal de TI; acompanhamento do desempenho do pessoal de TI; previsão dos quantitativos ideais da força de trabalho de TI.

Verificou-se, ainda, ausência de processos de gestão de serviços; plano de continuidade de serviços essenciais de TI; de acordos de níveis de serviço (ANS) e gerenciamento dos níveis de serviço; ações de conscientização dos colaboradores quanto à segurança da informação; processo de software; divulgação dos resultados dos objetivos, das ações e dos projetos de TI; de medição do grau de alcance dos objetivos e benefícios esperados nos projetos de TI; de estimativa orçamentária nos projetos de TI, de avaliação periódica da efetiva utilização dos sistemas informatizados que suportam o negócio e da implantação das ações previstas para os Grupos 1 e 2 do Plano de Trabalho a que se refere o artigo 29 da Resolução CNJ n. 211/2015.

Constatou-se, pelas informações prestadas pela unidade auditada, que o TRE/MS não dispõe de um processo de avaliação da governança e da gestão de TI, tampouco um aprimoramento contínuo da governança de TI. Não foram identificadas ações com intuito de diagnosticar o nível de maturidade em governança de TI, e nem a definição de metas de governança para os próximos exercícios, embora o órgão possua estrutura de pessoal formalmente alocada para a melhoria de governança de TI.

Ante todas as análises realizadas, pode-se deduzir que o efeito potencial e os riscos decorrentes da manutenção da situação encontrada são ausência de governança de TI em nível adequado e comprometimento da evolução do nível de maturidade da governança de TI, o que pode acarretar, em última análise, prejuízo ao alcance dos objetivos de TI do tribunal.

VIII. PROPOSTA DE ENCAMINHAMENTO

Ante o exposto submete-se o presente relatório à Presidência e à Diretoria-Geral do TRE/MS para apreciação e ciência dos seus termos e das propostas de encaminhamento abaixo:

À Secretaria de Tecnologia da Informação – STI:

Descrição	Item
Instituir política formal para as seguintes áreas: a) Planejamento de TI; b) Gestão do portfólio de projetos e de serviços de TI; c) Contratação de bens e serviços de TI; d) Avaliação do desempenho dos serviços de TI.	A1
Instituir política de gestão de riscos de TI que contemple a definição de papéis e responsabilidades e sua comunicação formal; níveis de risco aceitáveis; e que as tomadas de decisões estratégicas considerem os níveis de risco de TI definidos.	A2
Instituir políticas formais para: a) Gestão de pessoas, de forma a promover o desenvolvimento de competências e a retenção de gestores e técnicos de TI. b) Avaliação e incentivo ao desempenho de gestores e técnicos de TI. c) Escolha dos líderes da área de TI, ocupantes de cargos de chefia e de assessoramento.	A3

Instituir diretrizes formais para comunicação com as partes interessadas, considerando os públicos interno e externo, sobre os resultados da gestão e do uso de TI que contemple: a) Divulgação; b) Conteúdo; c) Frequência; e d) Formato das comunicações.	A4
Instituir diretrizes para avaliação da governança e da gestão de TI, com realização de avaliações periódicas de: a) Governança e gestão de TI; b) Sistemas de informação; c) Segurança da informação; e d) Contratos de TI.	A5
Instituir política formal de controle de acesso à informação, aos recursos e serviços de TI.	A6
Instituir política formal para a realização de cópias de segurança (backup).	A7
Efetuar o efetivo acompanhamento da execução do PETIC, conforme determinado no artigo 2º, da Resolução TRE/MS n. 557/2016; promover sua revisão periódica e considerar o PETIC para fundamentar as propostas orçamentárias de TI para os exercícios 2020 e seguintes.	A8
Instituir formalmente Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) que: a) Contemple as ações a serem desenvolvidas com vinculação às estratégias institucional e nacional do Poder Judiciário; b) Vincule as ações e projetos a indicadores e metas de negócio; c) Cuja execução seja periodicamente acompanhada; e d) Haja revisão periódica.	A9
Definir as competências necessárias para o pessoal de TI executar suas atividades e apresentar relação à Secretaria de Gestão de Pessoas (SGP), para que tal definição seja considerada no projeto de Gestão por Competências.	A10
Apresentar minuta de Plano Anual de Capacitação para o pessoal de TI à SGP que contemple: a) Previsão para sua revisão periódica; b) Diretrizes para avaliação e atendimento aos pedidos de capacitação em TI; c) Desenvolvimento de competências em governança e gestão de TI; d) Desenvolvimento de competências em contratação de bens e serviços de TI e em gestão de contratos de TI;	A11

e) Previsão para acompanhamento da execução do Plano, inclusive dos objetivos e resultados esperados.	
Estabelecer metas de desempenho para o pessoal de TI e acompanhá-las periodicamente.	A12
Apresentar à SGP os quantitativos ideais de força de trabalho de TI, estimados com base: a) Em estudo técnico que indique o número de usuários internos e externos de recursos de TI; e b) No anexo da Resolução CNJ n. 211/2015.	A13
Instituir processos de gerenciamento de: a) Portfólio de serviços; b) Catálogo de serviços; c) Continuidade dos serviços de TI; d) Mudanças; e) Configuração e de ativos; f) Liberação e implantação; g) Incidentes; h) Eventos; i) Problemas; e j) Acesso.	A14
Instituir Plano de Continuidade de Serviços Essenciais de TI e aplicá-lo.	A15
Instituir catálogo de serviços de TI com os níveis de serviço entre a área de TI e as áreas clientes formalmente definidos (Acordo de Nível de Serviço – ANS) e que: a) Os ANS incluam indicador de grau de satisfação dos usuários; b) Os níveis de serviço definidos sejam monitorados; c) Previsão de ações corretivas para as situações de não alcance dos níveis definidos; d) Comunicação periódica às áreas clientes dos resultados do monitoramento.	A16
Instituir processo de gestão de riscos de TI, em que os riscos de TI dos processos críticos de negócio sejam: a) Identificados; b) Avaliados; e c) Tratados com base em plano de tratamento de riscos.	A17
Instituir processos de gestão da segurança da informação que englobem: a) Classificação e tratamento de informações, com controles que garantam a proteção adequada ao grau de confidencialidade de cada classe de informação;	A20

b) Riscos; c) Vulnerabilidades técnicas de TI; d) Monitoramento do uso dos recursos de TI; e e) Incidentes de segurança da informação.	
Realizar, periodicamente, ações de conscientização, educação (capacitação) e treinamento em segurança da informação para os agentes públicos do TRE/MS. Para tal fim, entende-se como agente público, "todo aquele que exerce, ainda que transitoriamente ou sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função no TRE/MS."	A22
Instituir processo de software que seja: a) Acompanhado por meio de mensurações, com indicadores quantitativos e metas; b) Periodicamente revisado; e c) Gerenciado por pessoal próprio e capacitado.	A23
Instituir formalmente processo de gerenciamento de portfólio de projetos de TI.	A24
Acompanhar, por meio de mensurações, o gerenciamento de projetos de TI e revisá-lo periodicamente.	A25
Instituir plano de contratações de soluções de tecnologia da informação e comunicação que: a) Inclua as contratações necessárias ao alcance dos objetivos estabelecidos nos planejamentos estratégicos e institucional de TI. b) Seja revisado periodicamente para incluir novas contratações pretendidas; e c) Contenha prazos de entrega dos Estudos Preliminares e dos Projetos Básicos ou Termos de Referência.	A26
Monitorar, com medições periódicas e revisões, os objetivos estratégicos e táticos de TI que constam no PETIC e no PDTIC.	A27
Divulgar informações sobre os resultados dos objetivos de TI e o acompanhamento das ações e projetos de TI que constam no PETIC e PDTIC.	A28
Implementar medição do grau de alcance dos objetivos e benefícios que justificam a abertura de projetos de TI e verificar se os resultados são satisfatórios.	A29

Estimar o orçamento dos projetos de TI no início e acompanhá-lo durante a sua execução, verificando se há diferenças significativas entre a estimativa inicial e o valor real obtido ao final e levantar os motivos para as eventuais diferenças significativas encontradas.	A30
a) Implementar verificação se os processos críticos de negócio são suportados por sistemas informatizados; b) Designar formalmente os responsáveis da área de negócio para a gestão dos respectivos sistemas informatizados; c) Implementar avaliação periódica da efetiva utilização dos sistemas informatizados que suportam o negócio.	A31
Implementar todas as ações programadas e constantes do Plano de Trabalho 0456374 em relação aos Grupos 1 e 2, conforme especificado no § 1º do art. 29 da Resolução CNJ n. 211/2015.	A32

À Presidência e à Diretoria-Geral:

Descrição	**Item**
Recomenda-se a lotação de ao menos um servidor da área de TIC na Auditoria Interna, a fim de viabilizar que a unidade elabore o Plano Anual de Auditoria considerando os diversos riscos de TIC aos quais o Regional está exposto, inserindo a execução de exames de auditoria nos controles de governança e gestão de TIC. Dessa maneira, a unidade de Auditoria Interna atuará de forma a gerar valor para os tomadores de decisão, com a emissão de recomendações assertivas que assegurem a redução dos riscos relacionados com TIC, bem como a obtenção dos resultados e benefícios almejados com tais investimentos. É imperioso destacar que a área de TIC é a que o TCU e o CNJ mais têm cobrado ações de controle e atividades de auditoria interna. A relevância da tecnologia da informação e a criticidade dos processos a ela relacionados recomendam inserir nas prioridades institucionais a disponibilização de um servidor da área de TIC para estar em exercício na unidade de auditoria interna.	A33

Recomenda-se a notificação da Secretaria de Tecnologia da Informação, unidade auditada, para que apresente Plano de Ação no prazo fixado por V. Exa., especificando as medidas a serem adotadas em relação às propostas de encaminhamento acima que a unidade decidiu implementar, os respectivos prazos para

atendê-las e os responsáveis por cada tarefa, bem como justificativa técnica a respeito das recomendações que, eventualmente, decidiu não adotar. Após, solicita-se o retorno do processo a esta unidade de auditoria interna.

Numa fase seguinte, a Coordenadoria de Controle Interno e Auditoria irá monitorar o cumprimento das medidas, bem como sua efetividade, com o objetivo de contribuir para a melhoria no processo de governança e de gestão de TIC.

Campo Grande/MS, 21 de agosto de 2018.

Elaborado por: Adriana Morales Alencar (Líder de equipe).

Revisado por: Nivaldo Azevedo dos Santos (Supervisor da Auditoria).