PODER JUDICIÁRIO - JUSTIÇA DO TRABALHO
TRIBUNAL REGIONAL DO TRABALHO DA 7ª REGIÃO
SECRETARIA DE CONTROLE INTERNO – SCI

ANA PAULA BORGES DE ARAUJO ZAUPA

RELATÓRIO DE MONITORAMENTO DE PROVIDÊNCIAS

AÇÃO DE CONTROLE EXTERNO

I. IDENTIFICAÇÃO	
Nº do Processo	Proad 784/2018
Decisão	Acórdão TCU 750/2015 - Plenário
Unidade Auditada	TRT7
Seção Responsável pela Auditoria	Secretaria de Fiscalização de TI (SEFTI) do TCU
Objeto da Auditoria	Fiscalização de Orientação Centralizada (FOC) - Fiscalização de Governança de Tecnologia da Informação (TI) com foco na Avaliação da entrega de resultados e na Gestão de Riscos
Tipo de Auditoria	Operacional

Adiante detalham-se as determinações do Acórdão TCU 750/2014 - Plenário e se faz referência aos conteúdos dos itens a seguir referidos:

- Manifestação e documentos acostados pela Secretaria de Tecnologia da Informação em ação de monitoramento anterior, nos autos do Proad 784/2018, e em entrevista do Coordenador do Núcleo de Apoio à Gestão de Tecnologia da Informação e Comunicação e Segurança da Informação;
- Fatos e documentos constatados e informações obtidas pela SCI em ação de monitoramento.

II. DETERMINAÇÕES

ITEM[1]	CONTEÚDO
9.1	recomendar ao Tribunal Regional do Trabalho da 7ª Região que:
9.1.1.	elabore e aprove formalmente processo de aprimoramento contínuo da governança de TI, a exemplo das boas práticas contidas no capítulo 3 do guia de referência da implementação do Cobit 5, que contemple, ao menos: definição de papéis e responsabilidades voltadas especificamente para a melhoria da governança de TI; realização de diagnósticos ou autoavaliações de governança e de gestão de TI; e definição e acompanhamento de metas de governança de TI e das ações necessárias para alcançá-las, com base em parâmetros de governança, necessidades de negócio e riscos relevantes;

Providências adotadas:

A Presidência do Tribunal editou:

- **Ato 100/2017**: Define diretrizes para o planejamento, para a gestão do portfólio e para a avaliação de desempenho e para comunicação sobre o resultado da gestão e do uso de Tecnologia da Informação

[1] Subitem do Acórdão TCU 2750/2015 - Plenário.

- **Ato n. 131/2017 -** Dispõe sobre a Política de Governança de Tecnologia da Informação e Comunicação do Tribunal Regional do Trabalho da 7ª Região (PGTIC).

Análise de auditoria:

Determinação 9.1.1 atendida.

9.1.2.	com base nos itens 2 e 3 da NBR ISO/IEC 38.500/2009 - Governança Corporativa de TI c/c o item 2.2 do modelo para governança corporativa de TI da Norma NBR ISO/IEC 38.500, estabeleça diretrizes para a formulação sistemática de planos para gestão e uso corporativos de TI, com foco na obtenção de resultados de negócio institucional, em especial quanto à gestão dos riscos aos quais o negócio está exposto, à avaliação do desempenho dos serviços de TI junto às unidades usuárias em termos de resultado de negócio institucional, e, ainda, diretrizes para a obtenção, desenvolvimento e retenção de competências de pessoal;

Providências adotadas:

A Presidência do Tribunal editou:

- **Ato 100/2017**: Define diretrizes para o planejamento, para a gestão do portfólio e para a avaliação de desempenho e para comunicação sobre o resultado da gestão e do uso de Tecnologia da Informação
- **Ato 106/2018** - Estabelece as diretrizes da Gestão de Riscos relacionada ao ambiente tecnológico no âmbito do TRT7 e define o Processo de Gestão de Riscos de Segurança da Informação do TRT7

O Pleno do TRT7 aprovou:

- **Proposta de criação de novos cargos de TIC** - Foi apresentado, ao CSJT, projeto com vistas a provocar a definição e instituição da política em âmbito nacional, acompanhado de criação de cargos e gratificação especifica para a atividade de TI.
- **Plano Estratégico de Tecnologia da Informação (PETI) 2015-2020** contém valor, objetivo, diretriz e indicadores pertinentes à força de trabalho de TIC

O Conselho Superior da Justiça do Trabalho editou:

- A **Recomendação CJST 23/2018**, com fundamento nas Resoluções CNJ 211/2015 e nas Resoluções CSJT 193/2008 e 208/2017 dispôs sobre a fixação dos servidores de cargo efetivo de TIC na área respectiva e atuação na execução dos macroprocessos e processos típicos de TIC elencados na Res. CNJ 211/2015.

Análise de auditoria:

Determinação 9.1.2 atendida.

9.1.3.	estabeleça, formalmente, em consonância com o disposto no item 9.1.1 do acórdão 2308/2010-TCU-Plenário e com base nas boas práticas contidas na seção 3.3 da ABNT NBR ISO/IEC 38500:2009:

9.1.3.1. objetivos de gestão e de uso corporativos de TI alinhados às estratégias de negócio;

9.1.3.2. indicadores de desempenho para os objetivos de gestão definidos;

9.1.3.3. metas de desempenho da gestão e do uso corporativos de TI para cada indicador definido;

9.1.3.4. mecanismos para que a alta administração acompanhe o desempenho da TI da instituição; e

9.1.3.5. mecanismos de gestão dos riscos relacionados aos objetivos de gestão e de uso corporativos de TI;

Providências adotadas:

O Pleno do Tribunal aprovou:

- O Plano Estratégico de TI para o período de 2015-2020, o qual estabelece objetivos, metas e indicadores para acompanhamento.

A Presidência do Tribunal editou:

- **Ato 100/2017**: Define diretrizes para o planejamento, para a gestão do portfólio e para a avaliação de desempenho e para comunicação sobre o resultado da gestão e do uso de Tecnologia da Informação
- **Ato TRT7 61/2018** - Dispõe sobre a Política de Gestão de Riscos do Tribunal Regional do Trabalho da 7ª Região
- **Ato TRT7. 106/2018** - Estabelece as diretrizes da Gestão de Riscos relacionada ao ambiente tecnológico no âmbito do TRT7 e define o Processo de Gestão de Riscos de Segurança da Informação do TRT7

Deliberação Comitê de Governança de TIC (Reunião de 29/8/2018):

- Definiu as soluções nacionais críticas de TIC para mapeamento de riscos (PJE, AUD, PROAD e SIGEP)
- Procedeu a ajustes na classificação dos serviços, para definição de SLA, Mapeamento de Riscos e Mensuração de indisponibilidade e Plano de Continuidade

O processo de gestão de risco de TIC foi formalmente instituído pelo ATO TRT7 106/2018 e descrito em seus anexos. Atualmente, está sendo estabelecido o contexto de cada um dos sistemas nacionais: PROAD, Sistema de RH/Folha (SIGEP), PJe e AUD. As atividades estão sendo conduzidas pelo servidor Alexandre Barbosa e registradas no projeto "Implantar a Gestão de Riscos de TIC" do PDTIC 2018/2020, identificado no Jira pelo código NGTICP-7.

Cabe destacar que o documento chamado de "contexto" é um dos artefatos previstos no referido processo estabelecido pelo Ato 106/2018.

Análise de auditoria:

Determinações 9.1.3.1, 9.1.3.2, 9.1.3.3 e 9.1.3.4 atendidas.

Determinação 9.1.3.5 em atendimento.

9.1.4.	em consonância com o art. 6º, I, do Decreto-Lei 200/1967 e com o art.11, parágrafo único, da Resolução – CNJ 90/2009, ao elaborar o plano diretor de TI, utilize as práticas contidas na seção 5 do Guia de Elaboração de PDTI do Sisp, em especial no que se refere ao envolvimento das áreas de negócio no processo de elaboração;

Providências adotadas:

Elaborado Plano Diretor de Tecnologia da Informação conforme Guia de Elaboração do PDTI do SISP e conforme processo definido pelo Tribunal Regional do Trabalho da 7ª Região.

Análise de auditoria:

Determinação 9.1.4 atendida.

9.1.5.	adote providências no sentido de dotar a área de TI com o quantitativo de pessoal adequado para suprir as necessidades de trabalho em TI, com fundamento nas orientações contidas no Cobit 5, Prática de Gestão APO07.01 – *Maintain adequate and appropriate staffing*, levando em consideração as necessidades de pessoal das demais áreas do órgão;

Providências adotadas:

O Pleno do TRT7 aprovou:

- **Proposta de criação de novos cargos de TIC** - Foi apresentado, ao CSJT, projeto com vistas a provocar a definição e instituição da política em âmbito nacional, acompanhado de criação de cargos e gratificação específica para a atividade de TI.

Entretanto, em contrapartida à pretensão de dotação de pessoal, a SETIC, nos últimos dois anos, perdeu seis servidores, dos quais três por razões alheias à vontade da Administração do TRT7.

Análise de auditoria:

Determinação 9.1.5 em atendimento.

9.1.6.	elabore, aprove e acompanhe a execução de plano anual de capacitação do pessoal do setor de TI da entidade, de forma a prover e aprimorar o conhecimento necessário para a gestão e operação de TI, com fundamento nas orientações contidas no Cobit 5, Prática de Gestão APO07.03 – Maintain the skills and competencies of personnel, atividades 4 e 5, e em consonância com o item 9.9.1 do acórdão 1233/2012-TCU-Plenário;

Providências adotadas:

Elaborado Plano de Capacitação para TI em 2016 e mas não aprovado formalmente.
Elaborados Planos para os exercícios de 2017, 2018 e 2019, os quais foram aprovados formalmente.

Análise de auditoria:

Determinação 9.1.6 atendida.

9.1.7.	implemente processo de gestão de nível de serviço de TI, de forma a assegurar que níveis adequados de serviço sejam entregues para os clientes internos de TI de acordo com as prioridades do negócio e dentro do orçamento estabelecido, com fundamento nas orientações contidas na seção 6.1 da ABNT NBR ISO/IEC 20000-2:2008 c/c APO09 - Manage Service Agreements, Cobit 5;

Providências adotadas:

O processo foi mapeado pela consultoria (CPQD) e implantado na ferramenta de gerenciamento adquirida pelo TRT7 (Axios Assyst).

Deliberação Comitê Gestor de TIC (Reuniões 12 , 16 e 19/05):
Constituída Comissão Específica – reunião 03 e 04 de agosto/2017
Foram acordados os níveis de serviços para os principais serviços de TI ofertados, conforme ata da reunião de 3 e 4/8/2017

Deliberação Comitê de Governança de TIC (Reunião de 29/8/2018)
Foram feitos ajustes na classificação dos serviços, para definição de SLA, Mapeamento de Riscos e Mensuração de indisponibilidade e Plano de Continuidade.

Análise de auditoria: Determinação 9.1.7 atendida.	
9.1.8.	elabore, execute e teste periodicamente o plano de gestão de continuidade do negócio da instituição com fundamento nas orientações contidas na seção 14 da ABNT NBR ISO/IEC 27002:2005, nas seções 8.6 e 8.7 da ABNT NBR 15999-1:2007 e no Cobit 5, DSS04.3 – Develop and implement a business continuity response, em consonância com o item 9.1.3 do acórdão 1603/2008-TCU-Plenário;
Providências adotadas: Deliberação Comitê Gestor (Reuniões 12 , 16 e 19/05/2018): 8.3. Implantação adotando as seguintes fases: Fase 1: Designar grupo de trabalho Fase 2: Treinamento Conceitual Fase3: Planejamento (refinamento e cronograma) Fase 4: Inventário de ativos (não se trata do processo de gestão de ativos, mas tão somente um inventário de bens e serviços de TI). Fase 5: Escrever PRD Fase 6: Escrever PCO Fase 7: Treinamento Prático Fase 8: Simulação Fase 9: Ajustes Fase 10 (contínuo): Testes periódicos e ajustes. Estão sendo desenvolvidos os planos de contingência operacional de TIC para os sistemas considerados essenciais (definidos pelo Comitê de Governança de TIC), com base na política para o plano de continuidade instituída pelo Ato TRT7 2/2017. O plano de continuidade relativo ao PJe foi elaborado e testado com sucesso.	
Análise de auditoria: Determinação 9.1.8 em atendimento.	
9.1.9.	elabore e execute processo de gestão de ativos de informação da entidade, com fundamento nas orientações contidas na seção 7.1 da ABNT NBR ISO/IEC 27002:2005 e no Cobit 5, Processo BAI09 – *Manage assets*;
Providências adotadas: O processo foi mapeado pela consultoria (CPQD) e implantado na ferramenta de gerenciamento adquirida pelo TRT7 (Axios Assyst). A solução já foi homologada. O gerente do processo e seu substituto foram escolhidos e participaram da validação do processo. Na fase atual o processo está sendo aprimorado e adaptado as peculiaridades de cada área da STI. Serão nomeados gerentes separados para as atividades de cada divisão, após o período de experiência, a gerência será unificada novamente. Os registros de gestão de ativos de serviço são inseridos manualmente no Sistema de Controle de Material e Patrimônio SCMP. No momento, está sendo aprimorado o inventário de ativos (equipamentos e *softwares*).	

Análise de auditoria: Determinação 9.1.9 em atendimento.	
9.1.10.	implante programas de conscientização e treinamento em segurança da informação no âmbito da entidade, com fundamento nas orientações contidas na seção 8.2.2 da ABNT NBR ISO/IEC 27002:2005;
Providências adotadas: Consta do Plano de ação do Escritório de Segurança – item 5.15. Inicialmente foram criadas 4 cartilhas para orientação em segurança da informação (assuntos gerais, email, engenharia social, senhas) as quais foram encaminhadas, em dezembro de 2017, ao Setor de Comunicação Social do TRT7 para avaliação/sugestão da estratégia de divulgação. Em 25/4/2019 foi divulgada notícia na intranet explicando como identificar e prevenir incidente de Segurança da Informação.	
Análise de auditoria: Determinação 9.1.10 em atendimento.	
9.1.11.	elabore e implemente processo de gestão de riscos de segurança da informação, com fundamento nas orientações contidas na seção 4 da ABNT NBR ISO/IEC 27002:2005;
Providências adotadas: Consta do Plano de ação do Escritório de Segurança – item 5.9. O **Ato TRT7. 106/2018** - Estabelece as diretrizes da Gestão de Riscos relacionada ao ambiente tecnológico no âmbito do TRT7 e define o Processo de Gestão de Riscos de Segurança da Informação do TRT7. Foi concluída a definição de contexto de riscos e respectivos artefatos; atualmente está em andamento a fase de identificação dos riscos.	
Análise de auditoria: Determinação 9.1.11 em atendimento.	

ITEM	CONTEÚDO
9.2.	determinar ao Tribunal Regional do Trabalho da 7ª Região que inclua nos relatórios de gestão dos exercícios vindouros informações específicas que permitam o acompanhamento pelos órgãos de controle das ações afetas à governança de TI, conforme orientações contidas no item 7 e seus subitens do Anexo Único da Portaria-TCU 175/2013
Providências adotadas: Informações sobre as providências para cumprimento das determinações do Acórdão têm sido inseridas nos Relatórios de Gestão do TRT7.	
Análise de auditoria: Determinação 9.2 cumprida.	

CONCLUSÃO:

O presente monitoramento foi feito para subsidiar a Administração no atendimento da determinação constante do item 9.2 do Acórdão TCU 750/2014 - Plenário.

Das dezesseis determinações dirigidas ao TRT7, 10 (dez) foram atendidas e seis se encontram em atendimento.

Responsável pela Elaboração:

assinado eletronicamente
Ana Paula Borges de Araújo Zaupa
Secretária de Controle Interno

Data: 25/4/2019