TRT-7ª REGIÃO
Secretaria de Auditoria Interna

ADRIENNE GARCIA XEREZ SILVA
ANA PAULA BORGES DE ARAUJO ZAUPA
SONILDES DANTAS DE LACERDA
ANISIO DE SOUSA MENESES FILHO

RELATÓRIO DE MONITORAMENTO DE PROVIDÊNCIAS
AÇÃO DE CONTROLE EXTERNO

I. IDENTIFICAÇÃO	
Nº do Processo	Proad 784/2018
Decisão	Acórdão TCU 750/2014 - Plenário
Unidade Auditada	TRT7
Seção Responsável pela Auditoria	Secretaria de Fiscalização de TI (SEFTI) do TCU
Objeto da Auditoria	Segundo Monitoramento - 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 pendentes de cumprimento do Acórdão TCU 750/2014 - Plenário e se faz referência aos conteúdos dos itens a seguir referidos:

- Manifestação e documentos (Doc. 20) acostados pela Secretaria de Tecnologia da Informação em ação de monitoramento, 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, realizada em 17/6/2020;
- Fatos e documentos constatados e informações obtidas pela SAUDI em ação de monitoramento.

II. DETERMINAÇÕES

ITEM[1]	CONTEÚDO
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:
9.1.3.5. mecanismos de gestão dos riscos relacionados aos objetivos de gestão e de uso corporativos de TI;	
Providências adotadas: *"FORMALIZAÇÃO DO PROCESSO DE GESTÃO DE RISCOS DE TIC (ATO N. 106/2018);* *https://www.trt7.jus.br/files/institucional/governanca_ti/seguranca_de_ti/BD_ATO_PRESI_106-2018.pdf*	

[1] Subitem do Acórdão TCU 750/2014 - Plenário.

-ANÁLISE DE RISCOS DOS SISTEMAS ESSENCIAIS (https://drive.google.com/drive/u/0/folders/1SLjKcloiKMpgL1f9bsfeF8CTtjZiRzXP)

-MONITORAMENTO DAS AÇÕES DE TRATAMENTO (https://docs.google.com/document/d/1rB08W25ARjUHnn90VXk99x-PRipMtxtM-Sux5CW2ajw/edit)
-ANÁLISE DE RISCOS DO PLANO DE CONTRATAÇÕES DE TIC (2020)

https://docs.google.com/spreadsheets/d/1fMblyOH0OuiqigbAe2A8rvPt5RRdutjFxlri26Zavek/edit?usp=sharing

Foi publicada no repositório de documentação das contratações o plano de contratação e o mapa de riscos:(acesso interno ou pela VPN)

https://confluence.trt7.jus.br/confluence/pages/viewpage.action?pageId=5050540

O plano de tratamento dos riscos das contratações será individual em cada novo processo de contratação, como parte dos Estudos Técnicos Preliminares."

Análise de auditoria:

Em que pese a implementação do processo gestão de risco de TIC, verificou-se que as ações realizadas contemplaram apenas o tema segurança da informação e os serviços considerados essenciais, sendo ainda necessário mapear os riscos corporativos de TIC, a exemplo de pessoas, recursos e capacitação.

Ademais, constata-se que o mapeamento realizado no Processo de Contratação de TIC, embora elaborado, não foi implementado nas novas contratações. Segundo a SETIC, o plano de tratamento de risco será individualizado em cada nova contratação, em consonância com o mapeamento de riscos do Processo Contratação. A SETIC, contudo, não explicitou, em sua manifestação, um prazo para essa implementação.

Determinação 9.1.3.5 em atendimento.

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:

"A SETIC ELABOROU E ENCAMINHOU AO TRIBUNAL PROPOSTA DE ANTEPROJETO DE LEI PARA CRIAÇÃO DE CARGOS. O TRIBUNAL PLENO APROVOU (RESOLUÇÃO ADMINISTRATIVA Nº 412/2016), ENCAMINHANDO-O AO CSJT. PORÉM TAL PROPOSTA FOI ARQUIVADA PELO CSJT.

Para minimizar o risco de incidentes na área de banco de dados foi autorizado pelo Comitê de Governança (Ata do dia 06/05/2020, doc. 59 do Proad 6057/2017) a inclusão no planejamento orçamentário de TIC para 2021 a contratação de serviços de operação de banco de dados, para

minimamente dotar a área de banco de dados com força de trabalho compatível com a demanda."	
Análise de auditoria: As ações adotadas pela Administração não foram suficiente para o atendimento da Determinação. Determinação 9.1.5 em atendimento.	
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: **"***FOI EDITADO O ATO TRT7 N. 102/2017, QUE DISPÕE SOBRE OS REQUISITOS PARA O PLANO DE CONTINUIDADE DOS SERVIÇOS ESSENCIAIS DE TIC.* *POR DELIBERAÇÃO DO COMITÊ DE GOVERNANÇA DE TIC, EM 29/08/2018, O TRT MANTERÁ PLANO DE CONTINUIDADE DE TIC APENAS PARA PARA O SISTEMA PJE.* *https://proad.trt7.jus.br/proad/pages/exibirarquivo/DOCUMENTO%20-%20Ata%20do%20CGTIC%20de%2029-08-2018.pdf?idArquivo=348900&* *O PLANO FOI CONSTRUÍDO E TESTADO EM 06 E 07/04/2019. OS DOCUMENTOS QUE DETALHAM A EXECUÇÃO DO TESTE DO PLANO E O PLANO EM SI MESMO PODEM SER VISUALIZADOS EM* *https://drive.google.com/drive/folders/1HFuAgZiah_mufnCk4XV6tjeS5OOlwyDe* *CONVÉM DESTACAR QUE O ESCOPO DO PLANO MENCIONADO É CONTINUIDADE DE TIC. NÃO FOI ELABORADO PLANO DE CONTINUIDADE DE NEGÓCIO"*	
Análise de auditoria: Conforme manifestação da unidade auditada não foi elaborado o plano de continuidade do negócio. 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: *"PAINEL DE GESTÃO DE ATIVOS DE TIC.* *https://drive.google.com/file/d/1w-Xqjru6fB0_DXLfLBw_-3OHOr6On88F/view?usp=sharing* *PÁGINA DE CONHECIMENTO PARA MANUTENÇÃO DO INVENTÁRIO ATUALIZADO DOS ATIVOS DE TIC QUE MANTÉM OS SERVIÇOS ESSENCIAIS*	

https://drive.google.com/file/d/1hvN9bdLHo8-dH_KKlU-Mz0v1i0yQ2Cy3/view?usp=sharing"	
Análise de auditoria: As providências atendem parcialmente à determinação, haja vista a necessidade de revisão do ato normativo vigente, bem como a complementação do inventário. 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: *"NOTÍCIA ORIENTANDO OS USUÁRIOS SOBRE O QUE É UM INCIDENTE DE SEGURANÇA DA INFORMAÇÃO E QUAL O PROCEDIMENTO PARA REGISTRÁ-LO (VEICULADA NA INTRANET DO TRIBUNAL NOS DIAS 26/04/2019 E 16/09/2019).* *https://extranet.trt7.jus.br/index.php?option=com_content&view=article&id=3782:sti-explica-como-identificar-e-prevenir-incidente-de-seguranca-da-informacao* *CRIAÇÃO E PUBLICAÇÃO NA INTRANET/EXTRANET DO TRIBUNAL DE CINCO CARTILHAS DE SEGURANÇA DA INFORMAÇÃO:* • *Cartilha 1: SPAM - Mensagens de E-mail Indesejadas* • *Cartilha 2: Conceitos Gerais sobre Segurança da Informação* • *Cartilha 3: Utilização do E-mail Institucional* • *Cartilha 4: Engenharia Social* • *Cartilha 5: Contas de Usuários e Senhas* *PUBLICAÇÃO DE VÍDEO NA INTRANET, NO EMAIL E NOS GRUPOS DE WHATSAPP DO TRIBUNAL INFORMANDO AOS USUÁRIOS A IMPORTÂNCIA LER AS CARTILHAS DE SEGURANÇA DA INFORMAÇÃO* *https://extranet.trt7.jus.br/index.php?option=com_content&view=article&id=4152:seguranca-da-informacao-conheca-dicas-importantes-para-proteger-seus-dados-e-nao-cair-em-golpes-virtuais&catid=8&Itemid=117"*	
Análise de auditoria: Determinação 9.1.10 Atendida	
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: "*O Processo de gestão de riscos de de segurança da informação foi elaborado conforme pode-se evidenciar no PROAD 1431/2020.*	

A implementação foi efetivada, tendo sido executada uma primeira análise de riscos para os sistema críticos definidos para alta administração do TRT7, conforme projeto NGTICP-7 (proad 6616/2019) que produziu

a)documentos de contexto;

b)análise de riscos e

c)plano de tratamento.

https://drive.google.com/drive/u/0/folders/1SLjKcloiKMpgL1f9bsfeF8CTtjZiRzXP

Referidos artefatos foram submetidos à avaliação e aprovados pelo Comitê Gestor de Segurança da Informação."

Análise de auditoria:

As providências adotadas confirmam o atendimento da Determinação.

Determinação 9.1.11 Atendida

CONCLUSÃO:

O presente monitoramento foi feito para subsidiar a Administração no atendimento da determinação constante do item 9.2[2] do Acórdão TCU 750/2014 - Plenário.

Após a realização do primeiro monitoramento (Doc.09), constatou-se que, das (16) dezesseis determinações dirigidas ao TRT7, 10 (dez) haviam sido atendidas e seis permaneciam em atendimento.

Nesta segunda ação de monitoramento, verificou-se que, das (6) seis determinações pendentes de atendimento, 2 (duas) foram atendidas e 4 (quatro) ainda se encontram em atendimento.

Dessa forma, até o momento, as providências adotadas resultaram no cumprimento de 75% das Determinações iniciais.

Responsável pela Elaboração:

Adrienne Ramos Garcia
Coordenadora de Serviço da SCGAP

[2] 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.

Anísio de Sousa Meneses Filho Analista Judiciário – Esp. Eng. Civil
Data: 22/6/2020

Responsável pela Revisão: **Ana Paula Borges de Araújo Zaupa** Assistente-Secretária	**Supervisão e Aprovação:** **Sonildes Dantas de Lacerda** Secretária de Auditoria Interna
Data: 23/6/2020	**Data: 23/6/2020**