FABIANO REGO DE SOUSA

GRUPO I – CLASSE V – Plenário
TC 019.168/2013-6
Natureza: Relatório de Auditoria
Órgão: Tribunal Regional do Trabalho da 7ª Região/CE
Advogado constituído nos autos: não há.

SUMÁRIO: AUDITORIA OPERACIONAL. TRIBUNAL REGIONAL DO TRABALHO DA 7ª REGIÃO. FISCALIZAÇÃO INTEGRANTE DA PRIMEIRA FASE DO TRABALHO DE FISCALIZAÇÃO DE GOVERNANÇA DE TECNOLOGIA DA INFORMAÇÃO (TI) COM FOCO NA AVALIAÇÃO DA ENTREGA DE RESULTADOS E NA GESTÃO DE RISCOS, REALIZADO NA SISTEMÁTICA DE FISCALIZAÇÃO DE ORIENTAÇÃO CENTRALIZADA (FOC). DETERMINAÇÕES. RECOMENDAÇÕES.

Relatório

Trata-se de auditoria integrante do conjunto de auditorias da primeira fase do trabalho de fiscalização de governança de tecnologia da informação (TI) com foco na avaliação da entrega de resultados e na gestão de riscos, realizado na sistemática de Fiscalização de Orientação Centralizada (FOC).

2. O objetivo da auditoria foi avaliar a implementação dos controles informados pelo Tribunal Regional do Trabalho da 7ª Região em resposta ao levantamento do perfil de governança de TI realizado em 2012, bem como verificar e avaliar a adoção pela entidade auditada de planos e estratégias para implementação e melhoria da governança e da gestão de TI.

3. Transcrevo a seguir excerto do relatório de auditoria elaborado pela equipe da Secex-CE responsável pelos trabalhos (peça 48):

> " 1. Introdução
>
> 1.1. Antecedentes (Deliberação)
>
> No item 9.4.3 do Acórdão 2.308/2010-TCU-Plenário (2º Levantamento de Governança de TI), o TCU determinou à Sefti que mantenha processo de trabalho permanente e sustentável de acompanhamento da governança de TI na Administração Pública Federal de modo a subsidiar processos de fiscalização do TCU em TI e processos de planejamento e controle das unidades jurisdicionadas, com a definição, se possível, da realização periódica de levantamentos gerais e de mecanismos para a coleta de evidências destinadas a aumentar a confiabilidade das informações colhidas mediante questionários.
>
> Com efeito, a presente fiscalização foi autorizada mediante Despacho do Ministro-Relator Weder de Oliveira (peça 4), proferido no âmbito do TC 012.164/2013-5. No referido despacho, foi aprovada a sistemática de FOC em duas fases, sendo que este trabalho integra o conjunto de auditorias da primeira fase.
>
> 1.2. Objetivos e Questões de Auditoria
>
> O principal objetivo desta fiscalização foi avaliar a implementação dos controles de TI informados em resposta ao levantamento do perfil de governança de TI realizado pelo TCU em 2012, bem como verificar a adoção de planos e estratégias para implementação e melhoria da governança de TI.

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade, informando o código 50952303.

Dessa forma, com base no objetivo da fiscalização e a fim de avaliar a aderência do TRT7 às melhores práticas de governança e de gestão de TI, foram elaboradas seis questões de auditoria, agrupadas neste relatório em cinco temas, conforme ilustra a tabela a seguir:

Temas	Questões de auditoria
Governança corporativa	Os mecanismos de governança corporativa foram definidos e implementados adequadamente no âmbito da instituição?
Governança de TI	Há um processo de aprimoramento da governança de TI segundo as boas práticas?
	Os mecanismos de governança de TI foram definidos e implementados adequadamente no âmbito da instituição?
Estratégias e Planos	As estratégias e planos corporativos e de TI foram definidos e implementados adequadamente no âmbito da instituição?
Gestão de Pessoas de TI	Os mecanismos de gestão de pessoal de TI foram definidos e implementados adequadamente no âmbito da instituição?
Processos	Os processos de TI foram definidos e implementados adequadamente no âmbito da instituição?

1.3. Visão Geral

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.

Esse tema tem sido explorado pelo TCU, de forma mais específica, por meio de levantamentos realizados para avaliar a situação de governança de TI, bem como mediante diversas ações no sentido de disseminar, além dos resultados e boas práticas identificados, os conceitos tratados nesses trabalhos, buscando sempre destacar a importância da governança de TI para a Administração Pública Federal (APF).

O primeiro levantamento, realizado em 2007, contou com a participação de 255 instituições, resultando no Acórdão 1.603/2008-TCU-Plenário. O segundo levantamento, organizado em 2010, avaliou 301 instituições, culminando no Acórdão 2.308/2010-TCU-Plenário, que apresentou, pela primeira vez, a evolução da situação de governança de TI na APF. Por fim, o terceiro levantamento, realizado em 2012, avaliou 350 instituições, dando origem ao Acórdão 2.585/2012 TCU-Plenário.

De modo geral, as informações obtidas nos levantamentos de governança de TI realizados pelo TCU visam à identificação dos pontos mais vulneráveis da governança de TI na APF, à orientação da atuação do TCU como indutor do processo de aperfeiçoamento da governança de TI, bem como ao auxílio na identificação de bons exemplos e modelos a serem disseminados.

Nesse contexto, definiu-se como objeto desta auditoria um subconjunto dos mecanismos avaliados no âmbito do levantamento do perfil de governança de TI realizado pelo TCU em 2012, bem como o processo de aprimoramento da governança de TI no TRT7. Em síntese,

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade, informando o código 50952303.

foram avaliados aspectos ligados à governança corporativa, à governança de TI, às estratégias e planos do TRT7, à gestão de pessoas e à gestão de processos de TI.

1.4. Critérios e Metodologia

Para a realização deste trabalho, foram seguidos os normativos institucionais que tratam das fiscalizações no âmbito do TCU, em especial os documentos intitulados "Manual de Auditoria Operacional", aprovado pela Portaria-Segecex 4, de 26/2/2010; "Orientações para fiscalizações de Orientação Centralizada", aprovado pela Portaria-Adplan 2, de 23/8/2010; e "Normas de Auditoria do TCU" (NAT), aprovada por meio da Portaria-TCU 280, de 8/12/2010, posteriormente alterada pela Portaria-TCU 168, de 30/6/2011.

Durante a fase de planejamento da FOC, a unidade técnica orientadora dos trabalhos definiu as questões e os procedimentos de auditoria com base nos itens do questionário utilizado no levantamento do perfil de governança de TI de 2012. Como resultado dessa fase, foi gerada a matriz de planejamento da auditoria, cujo conteúdo foi transmitido durante workshop realizado em Brasília com membros das equipes de fiscalização das unidades executoras da FOC.

Ressalte-se que a equipe desta auditoria recebeu, durante uma semana na fase de planejamento, apoio técnico de auditor da equipe de coordenação da FOC com o objetivo de auxiliar na aplicação dos procedimentos de auditoria contidos na matriz de planejamento, de fornecer esclarecimentos sobre conceitos ligados à gestão e à governança de TI, além de participar de reuniões técnicas com gestores do TRT7.

Além de dispositivos constitucionais, legais e infralegais, foram utilizadas como critérios decisões do TCU relacionadas à governança e à gestão de TI, em especial o Acórdão 1.233/2012-TCU-Plenário. Também foram utilizados como critérios o guia Cobit 5, da Information Systems Audit and Control Association (Isaca); as normas NBR ISO/IEC 27002:2005 (NBR 27002), 20000-2:2008 (NBR 20000-2) e 38500:2009 (NBR 38500); o Código de Melhores Práticas de Governança Corporativa do Instituto Brasileiro de Governança Corporativa (IBGC); e o Guia de Elaboração de Plano Diretor de Tecnologia da Informação (PDTI) do Sistema de Administração dos Recursos de Tecnologia da Informação (Sisp).

O Cobit 5 consiste em um modelo de boas práticas para governança e gestão de tecnologia da informação organizado em cinco grandes domínios: Evaluate, Direct and Monitor (EDM), Align, Plan and Organize (APO), Build, Acquire and Implement (BAI), Deliver, Service and Support (DSS) e Monitor, Evaluate and Assess (MEA), cujas siglas serão utilizadas no decorrer do relatório para fins de referência ao critério de auditoria.

A NBR 27002 consiste em um código de boas práticas para a gestão da segurança da informação amplamente adotado no mundo e tem como propósito prover uma base comum para o desenvolvimento de normas de segurança organizacional e das práticas efetivas de gestão da segurança, além de prover confiança nos relacionamentos entre as organizações, fornecendo aos seus usuários recomendações para a boa gestão da segurança da informação.

Por sua vez, a NBR 20000-2 estabelece um código de prática que descreve as melhores práticas para processos de gerenciamento de serviços dentro do escopo da ABNT NBR ISO/IEC 20000 1. Essa norma faz parte da série ABNT NBR ISO/IEC 20000, que habilita provedores de serviços a entender como melhorar a qualidade dos serviços entregues aos seus clientes, tanto internos como externos.

Já a NBR ISO/IEC 38500 – norma de governança corporativa em tecnologia da informação – tem por objetivo fornecer uma estrutura de princípios para os dirigentes usarem na avaliação, no gerenciamento e no monitoramento do uso da tecnologia da informação em suas organizações. Essa norma oferece uma estrutura (contendo definições, princípios e um modelo) para a governança eficaz de TI que ajuda a alta administração das organizações a entender e cumprir suas obrigações legais, regulamentares e éticas com relação ao uso da TI em suas organizações.

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade, informando o código 50952303.

O Código de Melhores Práticas de Governança Corporativa do IBGC propõe a adoção de princípios e boas práticas de governança corporativa, com vistas a reduzir eventuais fragilidades no sistema de governança das organizações, que se aplicam a qualquer tipo de organização, independente do porte, natureza jurídica ou tipo de controle. O código é adotado como referência para alguns controles e práticas que ajudam a orientar a organização como um todo e, por consequência, sua atuação na governança da TI.

Por fim, o Guia de Elaboração de PDTI do Sisp provê informações que ajudam as organizações a planejarem melhor as ações relacionadas a TI. Cabe ressaltar que, apesar do referido guia ser destinado às instituições que fazem parte do Sistema de Administração dos Recursos de Tecnologia da Informação (Sisp), considerou-se que as informações ali contidas são boas práticas que poderiam ser aplicadas para as demais instituições fiscalizadas neste trabalho.

1.5. Limitações ocorridas

Não houve limitações à execução do trabalho em vista do escopo e aplicação dos procedimentos planejados.

2. Governança Corporativa

Governança Corporativa é o sistema pelo qual as organizações são dirigidas, monitoradas e incentivadas, envolvendo os relacionamentos entre proprietários, Conselho de Administração, Diretoria e órgãos de controle. As boas práticas de Governança Corporativa convertem princípios em recomendações objetivas, alinhando interesses com a finalidade de preservar e otimizar o valor da organização, facilitando seu acesso a recursos e contribuindo para sua longevidade. Os princípios básicos de governança corporativa são a transparência, a equidade, a prestação de contas e a responsabilidade corporativa.

A governança da área de TI não está isolada no ambiente corporativo, mas sim conectada ao ambiente geral da organização. A atuação da área de TI é diretamente influenciada pela direção e pela organização da instituição, logo há uma dependência entre a governança de TI e a governança institucional.

Neste trabalho, os seguintes aspectos relacionados à governança corporativa, parte integrante do levantamento de governança de TI, foram avaliados:

a) atuação da alta administração quanto ao estabelecimento e monitoramento de políticas corporativas (liderança);

b) comitê de direção estratégica;

c) ética institucional.

A análise da documentação encaminhada pelo TRT7, bem como as entrevistas realizadas na fase de execução da auditoria evidenciaram a criação do Núcleo de Gestão Estratégica por meio da Resolução 283/2008 (peça 10), que tem entre suas atribuições a formulação do planejamento institucional do órgão. Nesse contexto, verificou-se que o TRT7 elaborou e formalizou o Plano Estratégico Corporativo 2010-2014 (PEC), o Planejamento Estratégico de Tecnologia da Informação e Comunicação 2010-2014 (PETI) e os Planos Diretores de Tecnologia da Informação para os anos de 2012 e 2013 (PDTI) (Peças 21, 22, 23 e 24).

Todavia, verificou-se que há deficiências na utilização de instrumentos de governança corporativa, como por exemplo, o Código de Ética e a Política Institucional de Segurança da Informação, uma vez que, apesar de instituídos, não foram implementados de fato.

Frente ao exposto, evidenciou-se que há inconsistência entre a situação encontrada e a resposta apresentada pelo TRT7 ao item 1.1 do questionário Perfil GovTI 2013, uma vez que a alta administração, apesar de estabelecer políticas corporativas, não monitora o cumprimento das mesmas.

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade, informando o código 50952303.

2.1. Achado 1: Atuação insuficiente da alta administração no monitoramento de políticas corporativas.

Critérios

a) Código das Melhores Práticas de Governança Corporativa do IBGC - Item 2.3 – Atribuições do Conselho de Administração.

Análise das evidências

A seção 2.3 do Código das Melhores Práticas de Governança Corporativa do Instituto Brasileiro de Governança Corporativa (IBGC) recomenda que a alta administração deva prevenir e administrar situações de conflitos de interesses e administrar divergências de opiniões. Também nesse sentido, a norma ABNT ISO/IEC 38.500 recomenda que a alta administração deve exercer a governança de TI por meio de três tarefas principais: a) avaliar o uso atual e futuro da TI; b) orientar a preparação e a implementação de planos e políticas para assegurar que o uso da TI atenda aos objetivos do negócio e c) monitorar o cumprimento das políticas e o desempenho em relação aos planos.

A fim de evitar essas situações de conflitos, a alta administração deve discutir, aprovar e monitorar as decisões envolvendo, dentre outras:

a) Estratégia;

b) Praticas de Governança Corporativa;

c) Relacionamento com partes interessadas;

d) Sistema de controles internos (incluindo políticas e limites de alçada);

e) Política de gestão de pessoas;

f) Código de Conduta.

Em sua resposta ao questionário do levantamento do perfil de governança de TI de 2012, o TRT7 informou que, em relação à estrutura de governança corporativa, a alta administração do órgão se responsabiliza pelo estabelecimento e pelo cumprimento das políticas corporativas.

A fim de avaliar essa informação, o item 1.8 do anexo I do Ofício 785/2013-TCU/Secex-Ce solicitou que o TRT7 encaminhasse evidências de que a alta administração se responsabiliza pelas políticas corporativas, tais como o código de ética, a política de segurança da informação e comunicações, a política de governança de TI, entre outras (peça 2).

Em sua resposta, o TRT7 apresentou como evidências o Ato 195/2011 que instituiu a Norma de Segurança dos Recursos de Tecnologia da Informação - NSRTI (peça 6), a Resolução 75/2009, que instituiu o Estatuto de Ética Profissional do Servidor do TRT da 7ª Região (peça 7), a Portaria 800/2012, que nomeia os componentes da Comissão Permanente de Informática (peça 8) e a Resolução 313/2010, que instituiu a Política de Segurança Institucional do TRT7 (peça 9).

Os documentos apresentados, apesar de estabelecerem políticas corporativas, não evidenciaram que a alta administração monitora o cumprimento das políticas por ela estabelecidas. Em entrevista com representantes do TRT7 foi verificado que, tanto em relação ao Estatuto de Ética quanto em relação à Política de Segurança Institucional não há um acompanhamento formal pela alta administração do cumprimento dos controles estabelecidos nos normativos apresentados.

Causas

a) Governança corporativa em fase incipiente de maturação.

Efeitos e riscos decorrentes da manutenção da situação encontrada

a) Baixa efetividade das políticas corporativas estabelecidas.

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade, informando o código 50952303.

Conclusão

Frente ao exposto, conclui-se que a alta administração do TRT7 não exerce de forma adequada o papel de estabelecer e monitorar o cumprimento das políticas corporativas definidas.

Propostas de encaminhamento

Recomendar ao Tribunal Regional do Trabalho da 7ª Região que, com base nas boas práticas contidas na seção 1.6 do Código das Melhores Práticas de Governança Corporativa do IBGC, sensibilize os membros da alta administração acerca de sua responsabilidade em estabelecer e monitorar as políticas corporativas do órgão, a exemplo do código de ética, da política de segurança da informação e das demais políticas relativas à governança de tecnologia da informação.

2.2. Achado 2: Falhas na aplicação do Código de Ética

Critérios

a) Art. 7º, inciso II, alínea "d" c/c art. 8º, inciso I do Decreto 6.029/2007;

b) Art. 8º, inciso I do Decreto 6.029/2007;

c) Decreto 1.171/1994, art. 2º (plena vigência do código) c/c Decreto 6.029/2007, art. 15 (compromisso de acatamento).

Análise das evidências

Em resposta ao item 1.1 do questionário Perfil GovTI 2012 (peça 12), o TRT7 informou que adotou e publicou um código de ética, e encaminhou como evidência à equipe de auditoria a Resolução 75/2009, a qual instituiu o Estatuto de Ética Profissional do servidor do TRT 7ª Região (peça 11). Na mesma resposta ao questionário, informou ainda que nos exercícios de 2010 e 2011 não houve divulgação do mesmo nem o seu cumprimento foi monitorado.

Em entrevista realizada com os servidores ligados à Comissão de Ética do TRT7, foi informado à equipe de auditoria que nos exercícios de 2010 e 2011 houve cerca de 10 processos nos quais o referido comitê atuou. Contudo, à época desta auditoria, verificou-se que desde a mudança da gestão do TRT7, ocorrida em julho de 2012, houve por força normativa destituição automática dos membros da comissão de ética sem que houvesse a eleição de novos membros. Ou seja, apesar de instituída formalmente, não há membros designados para a comissão desde julho de 2012. Segundo informado pelo Secretário de Gestão de Pessoas, uma nova eleição para membros do comitê de ética está prevista para agosto de 2013.

Também foi relatado pelos ex-membros da comissão destituída que a alta administração do TRT7 não disponibilizou as condições necessárias para o pleno funcionamento da comissão, uma vez que à época da presente auditoria não havia local definido para a execução dos trabalhos da comissão e nem para arquivamento dos documentos utilizados e produzidos. Confirmou-se também na entrevista que não foram desenvolvidas ações de divulgação do Estatuto de Ética Profissional para os servidores da instituição.

Causas

a) Governança corporativa em fase incipiente de maturação.

Efeitos e riscos decorrentes da manutenção da situação encontrada

a) Baixa efetividade das políticas corporativas estabelecidas;

b) Subjetividade das interpretações pessoais sobre os princípios e normas éticos inerentes às atividades dos servidores do TRT7, em razão do desconhecimento do código de ética;

Conclusão

Frente ao exposto, conclui-se que há falhas na aplicação do código de ética no Ministério da Educação, principalmente no que se refere à falta de campanha interna de divulgação do código de ética, conforme prevê o art. 7º, inciso II, alínea "d" do Decreto 6.029/2007 e

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade, informando o código 50952303.

verificação do cumprimento do código de ética, de acordo com o previsto no art. 8º, inciso I, c/c o art. 15 do Decreto 6.029/2007.

Propostas de encaminhamento

Recomendar ao Tribunal Regional do Trabalho 7ª Região que, à semelhança das disposições contidas no art. 7º, inciso II, alínea "d", c/c o art. 8º, inciso I, c/c o art. 15 do Decreto 6.029/2007, defina mecanismos que possibilitem o adequado comprometimento dos servidores com o código de ética institucional, bem como as formas de apuração e de encaminhamento no caso de eventuais desvios de conduta.

3. Governança de TI

A governança de TI compreende a análise do ambiente corporativo, implantando e provendo sustentação a estruturas organizacionais, princípios, processos e práticas, com divisão clara de responsabilidades e delegação de autoridade, no sentido de se atingir a missão, as metas e os objetivos organizacionais, e, ao mesmo, tempo gerenciando os riscos existentes.

A governança de TI objetiva, assim, prover uma abordagem consistente e integrada à governança corporativa para assegurar que as decisões de TI estejam de acordo com as estratégias e objetivos organizacionais. Espera-se, dessa forma, que seja possível assegurar que os processos de TI sejam monitorados e utilizem os recursos disponíveis de forma eficiente e em conformidade com os requisitos legais e regulatórios.

Nesse sentido, a presente avaliação compreendeu diversos aspectos que formam o arcabouço de governança de TI que tem sido objeto de avaliação nos levantamentos de governança conduzidos pelo TCU, a saber:

a) políticas de governança, gestão e uso de TI;

b) processo de melhoria do próprio sistema de governança de TI;

c) mecanismo decisório e de priorização das demandas da TI;

d) organização das responsabilidades quanto à governança, gestão e uso de TI;

e) diretrizes formuladas pela alta administração;

f) mecanismos adotados para o monitoramento das diretrizes, das políticas e dos princípios estabelecidos.

No que tange à responsabilidade pelas políticas corporativas de TI, o Acórdão 2.308/2010-TCU-Plenário, em seu item 9.1 e respectivos subitens, recomendou aos órgãos governantes superiores (OGS) que orientassem as instituições sob sua jurisdição sobre a necessidade de a alta administração responsabilizar-se formalmente pelas políticas de TI, com o estabelecimento de objetivos, indicadores e metas de TI, bem como com mecanismos para avaliação do desempenho de TI.

Para a organização ter condições de avaliar seu desempenho na gestão e no uso de TI, é necessário estabelecer objetivos institucionais de TI, indicadores de desempenhos para cada objetivo, metas para cada indicador e monitorar regularmente esses indicadores, conforme recomendado no item 9.1 do Acórdão 2.308/2010-TCU-Plenário.

O TRT7, por meio do Ato 249/2010 (peça 13), criou a Comissão Permanente de Informática, que, conforme disposto no art. 2º do normativo, tem a competência para governar a execução do portfólio de projetos e das ações estratégicas constantes no PETI, e acompanhar o andamento dos trabalhos autorizados pelo PETI ou pela própria comissão.

Apesar do Ato 249/2010 não estabelecer quais áreas do TRT7 devem compor a Comissão Permanente de Informática, verificou-se que os representantes atualmente nomeados pela presidente do TRT7 representam as áreas necessárias à execução das atividades previstas (peça14). Ressalta-se ainda que a presidência da Comissão Permanente de Informática é

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade, informando o código 50952303.

exercida pela Presidente da Corte, o que assegura que a alta administração participa das discussões envolvidas.

Também foram evidenciados vários exemplos de reuniões da Comissão Permanente de Informática nos exercícios de 2010 e 2011, nas quais se vislumbram as atividades de acompanhamento da execução de ações previstas nos PETI e PDTI, bem como decisões em relação a priorizações do portfólio de projetos (peça 15).

No que se refere às diretrizes para contratação de bens e serviços de TI, evidenciou-se, conforme disposto na Portaria DG 375/201 (peça 19), que o TRT7 adotou o modelo prescrito na Instrução Normativa 4/2010-SLTI-MP como referência para a contratação de bens e serviços de TI (peça 20).

Já em relação à avaliação e priorização de demandas de negócio recebidas pela área de TI, o TRT7 implementou por meio da Resolução 229/2011 o Escritório de Projetos, o qual é gerenciado pela Secretaria de Gestão Estratégica e pela Secretaria de gestão de TI e que tem como missão ser a estrutura de suporte para a gestão do portfólio de programas e projetos estratégicos, garantindo a aderência estratégica, implantando as melhores práticas e difundindo a cultura de gerenciamento de projetos na Instituição (peça 16). No âmbito de suas competências, o Escritório de Projetos desenvolveu processo específico para gestão do portfólio de projetos, conforme evidenciado às peças 17 e 18.

O estabelecimento de objetivos de gestão e uso corporativos de TI, bem como os indicadores e metas de desempenho da gestão e uso corporativos de TI são definidos nos instrumentos de planejamento já citados (PEC, PETI e PDTI). Verificou-se ainda que há o efetivo acompanhamento da execução dos planos, conforme descrito no item 5.

Em entrevista com representantes da auditoria interna, constatou-se que não houve trabalhos específicos em TI nos exercícios de 2011 e 2012. Todavia, conforme evidenciado no Plano Anual de Ações de Controle para o exercício de 2013, houve previsão para realização de auditorias sobre a gestão de contratações e gestão de serviços de TI, constatando-se dessa forma evolução neste tema (peça 21, p. 36, item 2.1-c).

Em relação às respostas do TRT7 aos itens 1.2, 1.3, 1.5 e 1.6 do questionário Perfil GovTI 2012, verificou-se inconsistência apenas em relação à ausência de aprovação e publicação de diretrizes de avaliação de desempenho dos serviços de TI junto às unidades usuárias em termos de resultado de negócio institucional, ao contrário do informado na resposta ao item 1.2.

3.1. Achado 3: Deficiências nas ações de melhoria de governança de TI

Critério:

a) Cobit 5 - Framework, Capítulo 7 - Guia de Implementação;

b) Cobit 5 - Implementação, Guia de Referência - Capítulo 3 - Adotando os primeiros passos em direção à governança de TI;

c) Acórdão 2.585/2012-TCU-Plenário.

Análise das Evidências:

Por meio de análise dos documentos encaminhados pelo TRT7 e da realização de entrevistas, verificou-se que, em decorrência do estágio inicial de maturidade da instituição no que se refere às práticas de governança de TI, não há um processo instituído formalmente nem uma política de Governança de TI para aprimoramento contínuo da governança de TI na instituição.

Constatou-se ainda que não há uma área na estrutura organizacional específica que tenha a atribuição de conduzir o processo de Governança de TI. Conforme informado em entrevista, atualmente há dois servidores lotados na Secretaria de TI que atuam na área de governança nas áreas de planejamento e segurança da informação.

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade, informando o código 50952303.

Apesar disso há mecanismos e instâncias na instituição que implementam procedimentos e controles referentes à governança de TI, como, por exemplo, a Comissão Permanente de Informática (peça 15).

Causas:

a) Governança de TI em fase incipiente de maturação.

Efeitos e Riscos:

a) Desalinhamento das ações de TI com os objetivos das áreas de negócio.

b) Limitações para o alcance da máxima eficácia, eficiência e efetividade da TI para agregar valor ao negócio com riscos controlados.

c) Indisponibilidade de mecanismos adequados para que os gestores se antecipem aos problemas e os resolvam antes que gerem impactos negativos nas áreas de negócio do órgão.

Conclusão:

Apesar de dispor de alguns instrumentos voltados para a governança de TI, o TRT7 não adota um processo formal voltado para a melhoria da governança de TI na instituição.

Proposta de Encaminhamento:

Recomendar ao TRT7 que elabore e aprove formalmente um 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 pelo menos o seguinte:

a) definição de papéis e responsabilidades voltadas especificamente para a melhoria da governança de TI;

b) realização de diagnósticos ou autoavaliações de governança e de gestão de TI;

c) 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.

3.2. Achado 4: Falha na formulação de diretrizes de governança de TI por parte da alta administração.

Critérios

a) Itens 2 e 3 da NBR ISO/IEC 38.500/2009 - Governança Corporativa de TI c/c Item 2.2 Modelo para governança corporativa de TI da Norma NBR ISO/IEC 38.500

Análise das evidências

O item 2.1 da norma NBR ISO/IEC 38.500/2009 estabelece seis princípios de boa governança de TI, elencando entre eles o princípio da Responsabilidade, assim definido:

Os indivíduos e grupos dentro da organização compreendem e aceitam suas responsabilidades com respeito ao fornecimento e demanda de TI. Aqueles responsáveis pelas ações também tem autoridade para desempenhar tais ações.

Em relação ao esse princípio, os trabalhos de auditoria evidenciaram que não há documento aprovado e publicado que defina a distribuição de papéis e responsabilidades nas decisões mais relevantes quanto à gestão e o uso corporativo de TI. Algumas atribuições são verificadas no documento que institui a Comissão Permanente de Informática (peça 13), a qual é encarregada governar a execução do portfólio de projetos e ações estratégicas constantes no planejamento estratégico de TI. Todavia não há o estabelecimento de um processo que contemple o fluxo de decisões e responsabilidades quanto à gestão dos recursos de TI.

Já em relação ao princípio de desempenho citado no item 2.1 da norma NBR ISO/IEC 38.500/2009, também foi verificado que o TRT7 não estabeleceu diretrizes para avaliação de desempenho dos serviços de TI junto às unidades usuárias em termos de resultado de negócio

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade, informando o código 50952303.

institucional. Observa-se, contudo que foram realizadas pesquisas de satisfação com os usuários e, nos instrumentos de planejamento, foram incluídos indicadores para medir a satisfação do cliente, conforme se evidencia no Objetivo Estratégico 8 do PETIC: Assegurar a satisfação dos usuários, melhorando assim a imagem de TIC do TRT da 7ª.

A equipe de auditoria confirmou ainda que, de acordo com o respondido ao questionário Perfil GovTI 2012, a alta administração do TRT7 ainda não instituiu documentos formais relacionados a diretrizes para: formulação sistemática de planos para gestão e uso corporativos de TI, com foco na obtenção de resultados de negócio institucional; gestão dos riscos aos quais o negócio está exposto, como, por exemplo, a política de gestão de riscos da organização; e para a obtenção, desenvolvimento e retenção de competências de pessoal.

Causas

a) Governança corporativa em fase incipiente de maturação.

Efeitos e riscos decorrentes da manutenção da situação encontrada

a) A falta de diretrizes estabelecidas pela alta administração pode dificultar o amadurecimento dos processos de gestão de TI.

Conclusão

Conforme explicitado, constatou-se que a alta administração do TRT7 não estabeleceu algumas diretrizes recomendáveis para possibilitar evolução na governança de TI da instituição.

Propostas de encaminhamento

Recomendar ao TRT7 que, à luz do itens 2 e 3 da NBR ISO/IEC 38.500/2009 - Governança Corporativa de TI c/c Item 2.2 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.

3.3. Achado 5: Falhas nos mecanismos para dirigir e avaliar a gestão e o uso corporativos de TI.

Critérios

a) Item 9.1.1 do Acórdão 2.308/2010-P c/c Item 3.3 da NBR ISO/IEC 38.500/2009 - Governança Corporativa de TI

Análise das evidências

A fim de avaliar os mecanismos para dirigir e avaliar a gestão e o uso corporativos de TI foram solicitados ao TRT7 os seguintes documentos:

a) Plano Estratégico Institucional (PEI);

b) Plano Estratégico de TI (PETI);

c) Plano Diretor de Tecnologia da Informação (PDTI).

d) Processo e/ou Plano de gestão de riscos de TI;

e) Documento ou Relatório de avaliação periódica do cumprimento de metas de TI da organização;

f) Planos de auditoria(s) interna(s) aprovados para os anos de 2010 e/ou 2011 para avaliar os riscos considerados críticos para o negócio e a eficácia dos respectivos controles.

Os documentos encaminhados evidenciaram que o TRT7 elaborou o Plano Estratégico Corporativo 2010-2014 (PEC) (peça 21), o Planejamento Estratégico de Tecnologia da

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade, informando o código 50952303.

Informação e Comunicação 2010-2014 (PETI) (peça 22) e os Planos Diretores de Tecnologia da Informação para os anos de 2012 e 2013 (PDTI) (peças 23 e 24). Tais documentos foram devidamente aprovados pela alta administração, conforme evidenciado à peça 25.

A análise dos documentos mostrou que os objetivos estratégicos do PETI 2010-2014 estão devidamente alinhados aos objetivos do PEC 2010-2014. Além disso, os indicadores de desempenho para cada objetivo estratégico e suas respectivas metas estão discriminados no PETI 2010-2014 (peça 22, p. 25-39). Também se constatou que o PETI foi revisado em 2012 (peças 26 e 27).

No que tange ao acompanhamento dos objetivos estratégicos definidos no PEC, no PETI e no PDTI, verificou-se a realização de reuniões periódicas nos exercícios de 2010, 2011 e 2012, com a participação da alta administração, nas quais são apresentados os resultados mensurados por meio dos indicadores definidos (peças 28 e 29).

Apesar do exposto, foi verificado que a alta administração não estabeleceu mecanismos de gestão de riscos relacionados aos objetivos de gestão e uso corporativos de TI nem aprovou, para 2010 ou 2011, planos de auditorias internas para avaliar os riscos considerados críticos para o negócio e a eficácia dos respectivos controles.

Causas

a) Governança corporativa em fase incipiente de maturação.

Efeitos e riscos decorrentes da manutenção da situação encontrada

a) Falta instrumento de gestão para assegurar que a TI agregue valor ao negócio com riscos e custos aceitáveis.

Conclusão

Conforme explicitado, constatou-se que, apesar de apresentar instrumentos que permitem um adequado planejamento e gestão de TI, a alta administração do TRT7 ainda não implementou mecanismos que permitam gerenciar os riscos considerados críticos ao negócio, e seus impactos na TI.

Proposta de Encaminhamento:

Recomendar ao Tribunal regional do trabalho da 7ª região que, em consonância com o disposto no item 9.1.1 do Acórdão 2.308/2010-TCU-Plenário e com base nas boas práticas contidas na seção 3.3 da ABNT NBR ISO/IEC 38500:2009:

a) Estabeleça formalmente mecanismos de gestão dos riscos relacionados aos objetivos de gestão e de uso corporativos de TI;

b) inclua no plano anual de auditoria interna, entre outras atividades, ações com o objetivo de avaliar os riscos para o negócio e a eficácia dos respectivos controles em relação à gestão e ao uso da TI corporativa.

4. Estratégias e Planos.

Conforme dispõe o Guia de Elaboração de PDTI do Sisp (seção 3.2, p. 12), traduzindo a definição de planejamento para o conceito organizacional:

[...] pode-se dizer que planejar é determinar os objetivos ou metas da organização e coordenar os meios e recursos para atingi-los. E para atingir esses objetivos satisfatoriamente, as instituições devem ter a capacidade de percepção e de organização de suas experiências e perspectivas futuras. Para isso, é necessário integrar conhecimento e conteúdo, priorizando questões relevantes com ações associadas a objetivos definidos

Com efeito, para melhor conduzir a instituição na busca dos seus objetivos é mandatório planejar. Porém, conforme o item 83 do relatório que fundamenta o Acórdão 2.585/2012-TCU-

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade, informando o código 50952303.

Plenário, ainda preocupa o fato de que muitas instituições não executam um processo de planejamento estratégico (15% do universo pesquisado declararam não realizar planejamento estratégico). De acordo com o mesmo relatório, as contratações de TI devem estar planejadas em harmonia com instrumentos que derivam do planejamento estratégico, conforme estabelece a jurisprudência do TCU (Acórdãos 1.521/2003, 1.558/2003, 2.094/2004, 786/2006 e 1.603/2008, todos do Plenário) e a Instrução Normativa 4, de 12/11/2010, da Secretaria de Logística e Tecnologia da Informação (IN – SLTI/MP 4/2010).

Contudo, não somente as contratações de TI derivam desse processo, mas, sobretudo o conjunto de ações da instituição, que deve estar pautado pelos objetivos e metas estabelecidos na estratégia organizacional. Nesse sentido, o TCU recomendou aos OGS, por meio do item 9.1.1 do Acórdão 1.233/2012-TCU-Plenário, que estabelecessem a obrigatoriedade de que todos os entes sob sua jurisdição estabeleçam processo de planejamento estratégico institucional, em atenção ao princípio do planejamento expresso no art. 6º, inciso I, e no art. 7º do Decreto-Lei 200/1967.

Avançando-se no nível de especialização do planejamento, no âmbito do Poder Judiciário, o Conselho Nacional de Justiça, por meio da Resolução 90/2009, também estabeleceu a obrigatoriedade dos órgãos sob sua jurisdição de elaborarem o Plano Estratégico de Tecnologia da Informação (PETI) e o Plano Diretor de TI (PDTI). O TCU possui jurisprudência pacífica a respeito da importância do PDTI (Acórdãos 380/2011, 465/2011, 592/2011, 2612/2011, 1.233/2012, entre outros, todos do Plenário). No âmbito do Sisp, desenvolveu-se, inclusive, o Guia de Elaboração de PDTI do Sisp, que apresenta uma série de considerações a respeito desse importante instrumento.

Nesse aspecto, os documentos encaminhados evidenciaram que o TRT7 elaborou o Plano Estratégico Corporativo 2010-2014 (PEC) (peça 21), o Planejamento Estratégico de Tecnologia da Informação e Comunicação 2010-2014 (PETI) (peça 22) e os Planos Diretores de Tecnologia da Informação para os anos de 2012 e 2013 (PDTI) (peças 23 e 24). Tais documentos foram elaborados sob a condução do Núcleo de Gestão Estratégica e da Secretaria de tecnologia da Informação e devidamente aprovados pela alta administração, conforme evidenciado à peça 25. Não existe um processo formalizado para elaboração dos referidos planos. Na resposta aos itens 2.1, 2.2 e 2.3 do questionário Perfil GovTI o TRT7 referiu-se às metodologias de elaboração descritas nos próprios planos.

No processo de elaboração do PEC foi conduzido pelo Núcleo de Gestão Estratégica e contou com metodologia própria, a qual permitiu a participação de todas as áreas da instituição, e inclusive da sociedade (peça 30, p. 13-16). O documento formalmente aprovado apresenta os objetivos estratégicos da instituição, bem como seus respectivos indicadores e metas estabelecidas para cada indicador nos exercícios de 2010 a 2014 (peça 30, p. 27-44).

Ressalta-se que todas as informações referentes à execução do PEC são disponibilizadas em nível nacional por meio do sistema SIGEST, desenvolvido e gerido pelo Conselho Nacional de Justiça. No âmbito do TRT7, há a designação formal de um magistrado para exercer as atribuições de Gestor de Metas do Conselho Nacional de Justiça, assessorado pelo Núcleo de Ação Estratégica (peça 31). O PEC é ainda devidamente publicado na internet no endereço eletrônico www.trt7.jus.br/pe.

O PETI também contempla os indicadores e metas estabelecidos em seu processo de elaboração (peça 22, p. 25-57). O acompanhamento da sua execução é realizado por meio de reuniões de acompanhamento estratégico na Comissão Permanente de Informática, conforme evidenciado à peça 29. O TRT7 efetua ainda revisões periódicas do PETI (peças 26 e 27).

Em relação ao PDTI, verificou-se que o TRT7 encontra-se em um estágio inicial de maturidade com relação ao processo de elaboração do mesmo, tendo produzido os documentos referentes aos exercícios 2012 e 2013.

Finalmente, esclarece-se que não foram encontradas inconsistências nas respostas fornecidas pelo TRT7 aos itens 2.1, 2.2 e 2.3 do questionário perfil GovTI. Nesse caso,

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade, informando o código 50952303.

considerou-se que parte dos subitens do item 2.3 referentes ao detalhamento do PDTI é implementada pelo TRT7 no PETI.

4.1. Achado 6: Falhas no planejamento de TI

Critérios

a) Guia SISP de elaboração do PDTI c/c art. 3º da IN 04/2010

Análise das evidências

Conforme abordado no item 4 do Guia SISP de elaboração do PDTI, é recomendado que o processo de elaboração do PDTI envolva os seguintes papéis: a autoridade máxima da instituição, o Comitê de TI e a equipe de elaboração do PDTI, sendo que é recomendado que componham a esta última tanto representantes da área de TI como das áreas de negócio.

No caso do TRT7, em decorrência do mesmo estabelecer no PETI, e não no PDTI, os objetivos estratégicos, indicadores e metas com seus respectivos alinhamentos ao PEC, entende-se que não necessariamente as áreas de negócio deveriam estar diretamente envolvidas.

Contudo, verificou-se que o PDTI, é integralmente elaborado pela Secretaria de Tecnologia da Informação a qual, depois de finalizada a elaboração, deveria submeter o documento para aprovação da Comissão Permanente de Informática, conforme determina o item 3.3 da metodologia de elaboração dos PDTI 2012 e 2013 (peças 23, p. 5 e 24, p.5). Constatou-se que, nos dois exercícios, o PDTI foi aprovado pela alta administração (peça 32) ad referendum da Comissão Permanente de Informática. Ocorre que, em nenhum dos exercícios foi evidenciada a aprovação pela Comissão Permanente de Informática.

Causas

a) Governança corporativa em fase incipiente de maturação.

Efeitos e riscos decorrentes da manutenção da situação encontrada

a) Falta garantia de que as ações priorizadas no PDTI para execução no exercício estejam alinhadas às necessidades do negócio.

Conclusão

Conforme explicitado, constatou-se que a alta administração do TRT7 aprovou os PDTI de 2012 e 2013 sem o devido aval da Comissão Permanente de Informática.

Propostas de encaminhamento

Recomendar ao Tribunal Regional do Trabalho da 7ª Região que, em consonância com o art. 6º, inciso 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.

5. Gestão de Pessoas de TI

Entre os elementos viabilizadores da governança e da gestão de TI apresentados no Cobit encontram-se as pessoas, em razão de sua elevada importância para a estruturação da TI. O tema tem sido objeto de reiterada preocupação desta Corte de Contas, que tem se manifestado a respeito da importância das instituições realizarem avaliações quantitativas e qualitativas do quadro de profissionais de TI disponíveis de forma a fundamentar futuros pleitos de ampliação e preenchimento de vagas (Acórdãos 465/2011, 592/2011, 758/2011, 2.613/2011).

A carência de recursos humanos nas áreas de TI ganhou tal relevância que foi alçada a condição de destaque no Voto do Ministro-Substituto Augusto Sherman na apreciação das Contas de Governo, Exercício de 2012:

destaco, nesta ocasião, a necessidade de a Administração Pública aprimorar a política de pessoal da área de TI. Isto porque, em essência, se a estrutura de pessoal estiver bem cuidada, a

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade, informando o código 50952303.

tendência natural é a paulatina resolução da maioria das fragilidades atinentes à governança de TI. E sem a incorporação à estrutura de pessoal do Estado brasileiro de bons gerentes de TI, dificilmente alcançaremos as melhorias pretendidas e necessárias, tanto na governança de TI quanto nas contratações públicas de TI.

No mesmo sentido, a Estratégia-Geral de TI do Sisp definiu como uma das duas prioridades estratégicas para 2013: "Aprimorar a gestão de pessoas de TI", reforçando a importância do assunto. Objetiva-se, em última instância, que as áreas de TI sejam providas dos profissionais necessários para que a TI desempenhe adequadamente sua missão institucional.

No TRT7, à época da resposta ao questionário perfil GovTI 2012, todas as funções gerenciais de TI eram ocupadas por servidores do quadro permanente da instituição (peças 33, 34 e 35), situação essa que continua vigente. Todavia, não há um processo de seleção formalizado que considere o preenchimento de vagas gerenciais com base na competência dos candidatos.

O quantitativo de pessoas existente e ideal que compõem a força de trabalho de TI informado pelo TRT7 na resposta ao item 4.2 do questionário foi identificado com base em levantamento realizado em 2012 pela Secretaria de tecnologia da Informação. Tal estudo teve como base os direcionadores contidos no art. 2º da Resolução CNJ 90/2009 e a Resolução CSJT 69/2010 (peça 36).

Esclarece-se ainda que não foram encontradas inconsistências nas respostas fornecidas pelo TRT7 aos itens 1.4, 4.1, 4.2 e 4.4 do questionário perfil GovTI 2012.

5.1. Achado 7: Falhas na gestão de recursos humanos de TI

Critérios

a) Item 9.2.2, 9.11.2, 9.13.1, 9.15.4, 9.2.2, Acórdão 1233/2012-P;

b) APO 07.01 - Manter equipe adequada e apropriada - Cobit 5 - APO 07 - Gerenciar Recursos Humanos.

Análise das evidências

Conforme estudo efetuado pela área de TI do TRT7 em fevereiro de 2012 (peça 36), seriam necessários 28 servidores lotados na área de TI, contra um quadro real de 41 servidores. A equipe de auditoria verificou que a demanda de pessoal ainda não foi provida.

Tal fato adquire maior relevância tendo em vista que a Justiça do Trabalho vem, nos últimos anos, investido fortemente na prestação de serviços eletrônicos aos clientes externos, com a implementação do processo eletrônico, o que tem gerado considerável aumento na demanda dos serviços prestados pela Secretaria de tecnologia da Informação.

Causas

a) Governança corporativa em fase incipiente de maturação;

b) Restrições orçamentárias e dependência de anuência do Conselho Superior da Justiça do Trabalho;

Efeitos e riscos decorrentes da manutenção da situação encontrada

a) Insuficiência de desempenho de TI;

b) Aumento dos riscos do negócio associados a TI;

c) Dificuldades em melhorar a governança de TI.

Conclusão

Os recursos humanos são fundamentais para o bom desempenho da área de TI. As recomendações contidas no Cobit 5 com vistas a manter pessoal adequado e apropriado para desempenhar as funções de TI respaldam a importância do tema.

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade, informando o código 50952303.

Propostas de encaminhamento

Recomendar ao Tribunal Regional do Trabalho da 7ª Região que avalie a adequação do estudo efetuado pela Secretaria de Tecnologia da Informação em relação às necessidades quantitativas e qualitativas de pessoal para a área de TI, e envide esforços no sentido de dotar esse setor com o quantitativo de pessoal necessário para suprir as necessidades de trabalho em TI, à semelhança das orientações contidas no Cobit 5, Prática de Gestão APO07.01 – Maintain adequate and appropriate staffing (Manter pessoal adequado e apropriado – tradução livre).

5.2. Achado 8: Inexistência de um plano periódico de capacitação

Critérios

a) item 9.9.1, 9.11.9, 9.13.10, 9.15.14 Acórdão 1233/2012-P;

Análise das evidências

Em resposta ao item 4.4 do questionário Perfil GovTI 2012 o TRT7 informou que não há critério definido para avaliação e atendimento aos pedidos de capacitação em gestão de TI. A equipe de auditoria verificou, por meio de entrevista, que a situação permanece a situação informada.

Causas

a) Governança de TI ainda em incipiente de maturação.

Efeitos e riscos decorrentes da manutenção da situação encontrada

a) Insuficiência de desempenho da TI;

b) Aumento dos riscos do negócio associados a TI;

c) Dificuldades em melhorar a governança de TI.

Conclusão

Frente ao exposto, confirmou-se a inexistência de um plano de capacitação em TI pelo TRT7.

Propostas de encaminhamento

Recomendar ao Tribunal Regional do Trabalho da 7ª Região que, em consonância com o item 9.9.1 do Acórdão 1.233/2012-TCU-Plenário, elabore, aprove e acompanhe a execução de um 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, à semelhança das orientações contidas no Cobit 5, Prática de Gestão APO07.03 – Maintain the skills and competencies of personnel (Manter as habilidades e as competências de pessoal – tradução livre), atividades 4 e 5.

6. Processos

A dimensão de processos do perfil de governança de TI compreende uma série de atividades sobre as quais estrutura-se a gestão da TI. Nesse contexto, foram avaliados os processos ligados à gestão dos serviços de TI oferecidos, da segurança da informação, incluindo a garantia de continuidade dos serviços de TI e gestão sobre os incidentes de segurança, ao planejamento e à gestão das contratações.

A gestão de serviços de TI objetiva garantir que os serviços sejam prestados em conformidade com as expectativas e necessidades da organização. Os processos de gestão de serviços, conforme definidos na NBR ISO/IEC 20000-2, compreendem diversos aspectos relacionados ao fornecimento dos serviços, tais como a organização de um catálogo de serviços de TI, o estabelecimento de acordos de níveis de serviço com as áreas de negócio, os mecanismos de monitoramento dos serviços e dos acordos pactuados.

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade, informando o código 50952303.

Os processos de gestão da segurança da informação foram destacados em razão dos resultados apresentados nos três levantamentos de governança de TI, que ainda sinalizam, de forma geral, deficiências na forma como a APF gerencia a segurança de suas informações.

Inicia-se a avaliação da segurança da informação pela verificação da existência de uma Política de Segurança da Informação (PSI) – instrumento basilar de organização da segurança da informação institucional. A existência de uma PSI da instituição é requisito expresso pelo art. 5º, inciso VII, da Instrução Normativa GSI/PR 1/2008 e no art. 13 da Resolução 90/2009 do CNJ, bem como pela ampla jurisprudência do TCU a respeito do tema.

Ainda, foram objeto de avaliação as estruturas organizacionais requeridas para organizar e conduzir a segurança da informação, além de uma série de outros aspectos abordados no perfil de governança, tais como gestão de continuidade, gestão de ativos, política de controle de acesso, ações de conscientização e treinamento, gestão de riscos e gestão de incidentes, todos no âmbito da segurança da informação.

Para a execução dos objetivos de negócio, às instituições normalmente necessitam realizar contratações de TI. Com efeito, os processos adotados para planejamento das contratações e gestão dos contratos firmados são um instrumento importante para a padronização dessas atividades na instituição, a organização de controles e a obtenção de melhores resultados com sua execução.

Em resposta ao item 5.1 do questionário Perfil GovTI 2012, o TRT7 informou que, dentre os processos de gestão de serviços de TI, o TRT7 implementou apenas o processo de gestão de incidentes. Contudo, a auditoria evidenciou evolução na implementação em outros processos, em especial com relação à normatização. A alta administração aprovou em 2013 os seguintes normativos:

a) Ato 233/2013 - Institui a Política de Gerenciamento de Serviços de Tecnologia da Informação (TI) no âmbito do Tribunal Regional do Trabalho da 7ª Região;

b) Ato 232/2013 - Aprova a Norma Complementar de Procedimentos para Inventariar Ativos de Tecnologia da Informação;

c) Ato 231/2013 - Aprova a Norma Complementar de Controles de Acesso Relativos à Segurança da Informação e Comunicações;

d) Ato 230/2013 - Aprova a Norma Complementar de Gestão de Riscos de Segurança da Informação e Comunicações;

e) Ato 229/2013 - Aprova a Norma Complementar de Criação da Equipe de Tratamento e Resposta a Incidentes na Rede de Computadores do Tribunal Regional do Trabalho da 7ª Região;

f) Ato 228/2013 - Aprova a Norma Complementar de Utilização dos Recursos de Tecnologia da Informação;

g) Ato 227/2013 - Aprova a Norma Complementar de Cópia de Segurança e de Restauração de Sistemas, Aplicativos, Dados e de Documentos no âmbito do Tribunal Regional do Trabalho da 7ª Região;

h) Ato 195/2011 - Institui a Norma de Segurança dos Recursos de Tecnologia da Informação - NSRTI, do Tribunal Regional do Trabalho da 7ª Região.

Todavia, por meio de entrevistas verificou-se que houve apenas a normatização dos temas, contudo o TRT7 ainda carece dos recursos de pessoal para implementação dos mesmos.

Apesar de ter informado em resposta às questões 5.3 do questionário Perfil GovTI 2012 que não formalizou uma política corporativa de segurança da informação, o TRT7 já dispunha da Política de Segurança Institucional publicada em 19/11/2010 por meio da Resolução 313/2010 (peça 37). A referida norma instituiu o Comitê de Segurança Institucional, o qual teve seus membros nomeados por meio da Portaria 803/2012 (peça 38).

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade, informando o código 50952303.

Conforme já informado, ressalta-se que o TRT7 instituiu formalmente um processo de tratamento de incidentes em segurança da informação por meio do Ato 229/2013.

Apesar de não ser alcançado pela Instrução Normativa 04/2009/SLTI, o TRT7 adotou a norma como referência obrigatória para suas contratações de TI por meio da publicação da Portaria DG 375/2011 (peça 39), além de ter formalizado o processo de contratação (peças 40 e 41).

6.1. Achado 9: Falhas na gestão de acordos de nível de serviços

Critérios

a) Itens 6.1.1 e 6.1.3 da NBR ISO/IEC 20.000-2 c/c APO09 - Manage Service Agreements, Cobit 5

Análise das evidências

Em resposta à questão 5.1 e 5.2 do questionário Perfil GovTI 2012, o TRT7 informou que não implementou o processo de gestão de nível de serviços, mas que há um catálogo formal e atualizado dos serviços de TI oferecidos aos clientes.

Por meio do Ato 233/2013, publicado em 3/6/2013 (peça 42), o TRT7 instituiu a Política de Gerenciamento de Serviços de Tecnologia da Informação, a qual contempla a implementação de um catálogo de serviços (art. 5º) e de acordos de nível de serviços (art. 6º).

Em relação ao catálogo de serviços de TI, foi apresentada à equipe de auditoria página na intranet que elenca todos os serviços prestados pela TI, a qual também serve de entrada para a solicitação de atendimento a chamados técnicos. Todavia não contempla informações detalhadas sobre os serviços, tais como responsável pelo serviço, prazos para atendimento, horários de serviços, à luz do recomendado no item 6.1.1 da NBR ISO/IEC 20.000-2.

O TRT7 também não havia formalizado ainda, à época da auditoria, implementado o processo de gerenciamento de serviços e acordos de nível de serviços com as áreas clientes. Verificou-se, conforme informado na peça 43, que a Secretaria de Tecnologia da Informação criou unilateralmente níveis de serviços para alguns itens do catálogo, sendo que tais níveis podem ser negociados posteriormente sob demanda das áreas.

Causas

a) Governança corporativa em fase incipiente de maturação.

Efeitos e riscos decorrentes da manutenção da situação encontrada

a) Fornecimento de serviços inadequados aos clientes, acarretando o não atendimento às necessidades do negócio;

b) Dificuldades na priorização de esforços de pessoal e tecnológicos.

Conclusão

Verificou-se que, apesar de normatizado, o processo de gestão de acordos de serviços de TI não foi implementado adequadamente.

Propostas de encaminhamento

a) Recomendar ao Tribunal Regional do Trabalho da 7ª Região que avalie a conveniência e a oportunidade de implementar 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, à semelhança das orientações contidas na seção 6.1.3 da ABNT NBR ISO/IEC 20000-2:2008;

b) Recomendar ao Tribunal Regional do Trabalho da 7ª Região que elabore, publique e mantenha atualizado catálogo de serviços de TI do órgão, à semelhança das orientações contidas na seção 6.1.1 da ABNT NBR ISO/IEC 20000-2:2008 e no Cobit 5, Prática de Gestão

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade, informando o código 50952303.

APO09.02 – Catalogue IT-enabled services (Catalogar serviços de tecnologia da informação habilitados – tradução livre).

6.2. Achado 10: Falhas em processos de gestão de segurança da informação

Critérios

a) Acórdão 436/2008, 1609/2012, 2523/2012 c/c itens 8.7.2 da NBR ISO 15.999, 14.1.3 da NBR ISO 27.002:2005 c/c art. 1º, inc. IV, alínea g da Resolução 99/2009 do CNJ c/c Diretrizes para a Gestão de SI no âmbito do Poder Judiciário;

b) NC 10/IN01/DSIC/GSIPR c/c art. 13 da Resolução CNJ 90/2009 c/c documento de "Diretrizes para a Gestão de Segurança da Informação no âmbito do Poder Judiciário" publicado pelo CNJ c/c item 11.1.1 da NBR 27.002/2005 c/c Acórdãos 1609/2012 e 2523/2012;

c) Art. 13 da Resolução CNJ 90/2009 c/c documento de "Diretrizes para a Gestão de Segurança da Informação no âmbito do Poder Judiciário" publicado pelo CNJ c/c item 11.1.1 da NBR 27.002/2005 c/c Acórdãos 1609/2012 e 2523/2012;

e) Acórdão 2938/2010, 380/2011 c/c art. 13 da Resolução CNJ 90/2009 c/c documento de "Diretrizes para a Gestão de Segurança da Informação no âmbito do Poder Judiciário" publicado pelo CNJ.

Análise das evidências

Em resposta às questões 5.1 e 5.3 do questionário Perfil GovTI 2012, o TRT7 informou que não implementou os processos corporativos de gestão de continuidade dos serviços de TI, de inventário de ativos de informação, de análise de riscos aos quais a informação crítica ao negócio está submetida e de gestão de incidentes de segurança da informação. Informou ainda que não formalizou uma política de controle de acesso e que não realizou ações de conscientização em segurança da informação.

Os trabalhos de auditoria constataram a publicação dos seguintes documentos, todos no exercício de 2013:

a) Ato 232/2013 - Aprova a Norma Complementar de Procedimentos para Inventariar Ativos de Tecnologia da Informação (peça 44, p. 1-5);

b) Ato 230/2013 - Aprova a Norma Complementar de Gestão de Riscos de Segurança da Informação e Comunicações (peça 44, p. 6-9);

c) Ato 229/2013 - Aprova a Norma Complementar de Criação da Equipe de Tratamento e Resposta a Incidentes na Rede de Computadores do Tribunal Regional do Trabalho da 7ª Região (peça 44, p. 10-15);

d) Ato 231/2013 - Aprova a Norma Complementar de Controles de Acesso Relativos à Segurança da Informação e Comunicações (peça 44, p. 16-20).

A equipe de auditoria verificou que as referidas normas, apesar de formalizadas e publicadas, ainda estão em fase de planejamento de implementação. Conforme informou a Secretaria de Tecnologia da Informação, a implementação dos processos ainda depende do aumento do efetivo da equipe de TI do TRT7.

Em relação a ações de divulgação de segurança da informação, foram apresentadas evidências de publicação na intranet do TRT7 de notícias e artigos de segurança da informação, além de cartilhas elaboradas pelo Cert.BR (peça 45).

Causas

a) Governança corporativa em fase incipiente de maturação.

Efeitos e riscos decorrentes da manutenção da situação encontrada

a) Desconhecimento dos riscos a que os ativos de informação críticos para o negócio estão submetidos;

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade, informando o código 50952303.

b) Interrupção nos serviços prestados pelo TRT7 à população;

c) Exposição não autorizada de informação sigilosa;

d) Desconhecimento pelos servidores dos procedimentos a serem adotados quando da ocorrência de incidentes de segurança da informação.

Conclusão

Verificou-se que, apesar de ter normatizados alguns dos processos de gestão de segurança da informação, não ocorreu a implantação dos mesmos.

Propostas de encaminhamento

a) Recomendar ao Tribunal Regional do Trabalho da 7ª Região que elabore e execute processo de gestão de continuidade dos serviços de TI, à semelhança das orientações contidas no Cobit 5, DSS04.3 – Develop and implement a business continuity response (Desenvolver e implementar resposta à continuidade do negócio – tradução livre);

b) Recomendar ao Tribunal Regional do Trabalho da 7ª Região que, em atenção às Diretrizes para a Gestão de Segurança da informação no âmbito do Poder Judiciário, estabelecidas pelo CNJ e em consonância com o item 9.1.3 do Acórdão 1.603/2008-TCU-Plenário, elabore, execute e teste periodicamente o plano de gestão de continuidade do negócio da instituição, de forma a minimizar os impactos decorrentes de falhas, desastres ou indisponibilidades significativas sobre as atividades do órgão, à semelhança das 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 (Desenvolver e implementar resposta à continuidade do negócio – tradução livre);

c) Recomendar ao Tribunal Regional do Trabalho da 7ª Região que, em atenção às Diretrizes para a Gestão de Segurança da informação no âmbito do Poder Judiciário, estabelecidas pelo CNJ, elabore e execute processo de gestão de ativos de informação do órgão, à semelhança das orientações contidas na seção 7.1 da ABNT NBR ISO/IEC 27002:2005 e no Cobit 5, Processo BAI09 – Manage assets (Gerenciar ativos – tradução livre);

d) Recomendar ao Tribunal Regional do Trabalho da 7ª Região que, em atenção às Diretrizes para a Gestão de Segurança da informação no âmbito do Poder Judiciário, estabelecidas pelo CNJ, implante programas de conscientização e treinamento em segurança da informação no âmbito do órgão, à semelhança das orientações contidas na seção 8.2.2 da ABNT NBR ISO/IEC 27002:2005;

e) Recomendar ao Tribunal Regional do Trabalho da 7ª Região que, em atenção às Diretrizes para a Gestão de Segurança da informação no âmbito do Poder Judiciário, estabelecidas pelo CNJ, elabore e implemente processo de gestão de riscos de segurança da informação, à semelhança das orientações contidas na seção 4 da ABNT NBR ISO/IEC 27002:2005.

7. Comentários do gestor

Solicitado a manifestar-se em relação aos achados contidos no presente relatório, o gestor informou estar de acordo com as conclusões apresentadas pela equipe de auditoria (peça 47).

8. Conclusão

Os trabalhos de auditoria realizados no TRT7 constataram que a instituição apresenta vários elementos que impulsionam a evolução da Governança de Corporativa e de TI, como o estabelecimento do Plano de Estratégia Corporativo, do Plano Estratégico de TI e do Plano Diretor de TI. Verificou-se que há um amadurecimento constante do TRT7 em relação ao estabelecimento de objetivos estratégicos de TI, definição de indicadores e metas, sempre com a preocupação de alinhar as atividades da TI às necessidades do negócio. Também foram verificados instrumentos de monitoramento da execução dos referidos planos.

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade, informando o código 50952303.

Por outro lado, até por estar em um estágio inicial de governança de TI, ainda há áreas que necessitam ser aperfeiçoadas para que a TI consiga efetivamente cumprir o seu papel, como o processo de gestão dos serviços de TI que, apesar dos normativos recentes publicados pela alta administração, ainda não tiveram a sua implementação de fato realizada.

Verificaram-se também deficiências em relação à gestão da Segurança da Informação, tema este relevante e que deve ser mais bem avaliado e acompanhado tanto pela alta administração como pela área de TI do Tribunal.

Um dos objetivos secundários da fiscalização em tela era a verificação de eventuais inconsistências entre as evidências de implementação dos controles de TI e as respostas apresentadas pelos órgãos e entidades no levantamento do perfil de governança de TI de 2012. Pretende-se, assim, subsidiar o aperfeiçoamento do instrumento de levantamento e de avaliação de governança de TI.

Ressalte-se que a existência de inconsistências tem causas diversas, tais como: falhas de interpretação do questionário por parte do órgão/ente fiscalizado; falta de clareza de algumas perguntas do questionário; grau de rigor empregado pela instituição na autoavaliação. As inconsistências relatadas ao longo da exposição dos achados de auditoria estão resumidas no quadro a seguir:

Seção Resposta apresentada no Perfil GovTI2012 Situação encontrada (referência aos parágrafos)

1.1 A Alta Administração da instituição se responsabiliza pelo estabelecimento e pelo cumprimento das políticas corporativas Apesar de estabelecer as políticas corporativas, a Alta Administração não monitora o cumprimento das mesmas (item 3.1)

1.2 A Alta Administração aprovou e publicou as diretrizes de avaliação de desempenho dos serviços de TI junto às unidades usuárias em termos de resultado do negócio institucional Não foi aprovado documento algum nesse sentido (item 4.2)

5.2 Há um catálogo formal e atualizado de serviços dos serviços de TI oferecido aos clientes. O catálogo apresentado não é formalizado e não dispõe de todas as informações recomendadas (item 7.1)

Dentre os questionamentos apresentados, constatou-se junto aos gestores entrevistados que duas das inconsistências apresentadas acima decorreram de evidentes dificuldades no entendimento das questões, enquanto uma inconsistência constitui situação em que as evidências apresentadas não foram consideradas suficientes pela equipe de auditoria para respaldar a resposta apresentada.

9. Proposta de Encaminhamento

I) Recomendar, com fulcro no art. 43, inciso II, da Lei 8.443/1992 c/c o art. 250, inciso III, do Regimento Interno do TCU, ao Tribunal Regional do Trabalho da 7ª Região que:

a) com base nas boas práticas contidas na seção 1.6 do Código das Melhores Práticas de Governança Corporativa do IBGC, sensibilize os membros da alta administração acerca de sua responsabilidade em estabelecer e monitorar as políticas corporativas do órgão, a exemplo do código de ética, da política de segurança da informação e das demais políticas relativas à governança de tecnologia da informação;

b) à semelhança das disposições contidas no art. 7º, inciso II, alínea "d", c/c o art. 8º, inciso I, c/c o art. 15 do Decreto 6.029/2007, defina mecanismos que possibilitem o adequado comprometimento dos servidores com o código de ética institucional, bem como as formas de apuração e de encaminhamento no caso de eventuais desvios de conduta;

c) elabore e aprove formalmente um processo de aprimoramento contínuo da governança de TI, a exemplo das boas práticas contidas no capítulo 3 do guia de referência da

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade, informando o código 50952303.

implementação do Cobit 5, que contemple pelo menos a definição de papéis e responsabilidades voltadas especificamente para a melhoria da governança de TI, a realização de diagnósticos ou autoavaliações de governança e de gestão de TI e a 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;

d) à luz dos itens 2 e 3 da NBR ISO/IEC 38.500/2009 - Governança Corporativa de TI c/c Item 2.2 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;

v) em consonância com o disposto no item 9.1.1 do Acórdão 2.308/2010-TCU-Plenário e com base nas boas práticas contidas na seção 3.3 da ABNT NBR ISO/IEC 38500:2009 e estabeleça formalmente mecanismos de gestão dos riscos relacionados aos objetivos de gestão e de uso corporativos de TI e inclua no plano anual de auditoria interna, entre outras atividades, ações com o objetivo de avaliar os riscos para o negócio e a eficácia dos respectivos controles em relação à gestão e ao uso da TI corporativa;

vi) em consonância com o art. 6º, inciso 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;

vii) tendo em vista o resultado da avaliação do pessoal da área de TI da entidade, envide esforços no sentido de dotar esse setor com o quantitativo de pessoal identificado como necessário para suprir as necessidades de trabalho em TI, à semelhança das orientações contidas no Cobit 5, Prática de Gestão APO07.01 – Maintain adequate and appropriate staffing (Manter pessoal adequado e apropriado – tradução livre);

viii) em consonância com o item 9.9.1 do Acórdão 1.233/2012-TCU-Plenário, elabore, aprove e acompanhe a execução de um 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, à semelhança das orientações contidas no Cobit 5, Prática de Gestão APO07.03 – Maintain the skills and competencies of personnel (Manter as habilidades e as competências de pessoal – tradução livre), atividades 4 e 5;

ix) avalie a conveniência e a oportunidade de implementar 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, à semelhança das orientações contidas na seção 6.1.3 da ABNT NBR ISO/IEC 20000-2:2008;

x) elabore, publique e mantenha atualizado catálogo de serviços de TI do órgão, à semelhança das orientações contidas na seção 6.1.1 da ABNT NBR ISO/IEC 20000-2:2008 e no Cobit 5, Prática de Gestão APO09.02 – Catalogue IT-enabled services (Catalogar serviços de tecnologia da informação habilitados – tradução livre);

xi) elabore e execute processo de gestão de continuidade dos serviços de TI, à semelhança das orientações contidas no Cobit 5, DSS04.3 – Develop and implement a business continuity response (Desenvolver e implementar resposta à continuidade do negócio – tradução livre);

xii) em atenção às Diretrizes para a Gestão de Segurança da informação no âmbito do Poder Judiciário, estabelecidas pelo CNJ e em consonância com o item 9.1.3 do Acórdão 1.603/2008-TCU-Plenário, elabore, execute e teste periodicamente o plano de gestão de continuidade do negócio da instituição, de forma a minimizar os impactos decorrentes de falhas, desastres ou indisponibilidades significativas sobre as atividades do órgão, à semelhança das

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade, informando o código 50952303.

orientações contidas na seção 14 da ABNT NBR ISO/IEC 27002:2005, nas seções 8.5 e 8.7 da ABNT NBR 15999-1:2007 e no Cobit 5, DSS04.3 – Develop and implement a business continuity response (Desenvolver e implementar resposta à continuidade do negócio – tradução livre);

e) em atenção às Diretrizes para a Gestão de Segurança da informação no âmbito do Poder Judiciário, estabelecidas pelo CNJ, elabore e execute processo de gestão de ativos de informação do órgão, à semelhança das orientações contidas na seção 7.1 da ABNT NBR ISO/IEC 27002:2005 e no Cobit 5, Processo BAI09 – Manage assets (Gerenciar ativos – tradução livre);

f) em atenção às Diretrizes para a Gestão de Segurança da informação no âmbito do Poder Judiciário, estabelecidas pelo CNJ, implante programas de conscientização e treinamento em segurança da informação no âmbito do órgão, à semelhança das orientações contidas na seção 8.2.2 da ABNT NBR ISO/IEC 27002:2005;

g) em atenção às Diretrizes para a Gestão de Segurança da informação no âmbito do Poder Judiciário, estabelecidas pelo CNJ, elabore e implemente processo de gestão de riscos de segurança da informação, à semelhança das orientações contidas na seção 4 da ABNT NBR ISO/IEC 27002:2005.

II) Determinar ao Tribunal Regional do Trabalho da 7ª Região que, no prazo de 60 (sessenta) dias a contar da ciência do acórdão que vier a ser proferido, encaminhe a esta Corte de Contas plano de ação para a implementação das medidas contidas no decisum, contendo:

a) para cada recomendação, cuja implementação seja considerada conveniente e oportuna, o prazo e o responsável (nome, cargo e CPF) pelo desenvolvimento das ações;

b) para cada recomendação cuja implementação não seja considerada conveniente ou oportuna, justificativa da decisão.

III) Determinar ao Tribunal Regional do Trabalho da 7ª Região que, até que o plano de ação proposto no item II seja plenamente implementado, inclua nos relatórios de gestão dos exercícios vindouros informações específicas que permitam o acompanhamento pelos órgãos de controle das ações realizadas."

4. A Sefti, em seu parecer técnico, ao analisar os encaminhamentos propostos, ressalvou, de maneira unânime (peças 51, 52 e 53):

"2. Inicialmente, cabe salientar que a coordenação central da FOC está a cargo da Secretaria de Fiscalização de Tecnologia da Informação (Sefti). Diante disso e considerando que o relatório de fiscalização produzido pela Secex-CE (peça 48) foi objeto de revisão preliminar realizada por auditores da Sefti para verificação da adequação do relatório aos padrões técnicos e metodológicos propostos no âmbito da FOC, e cujas adaptações foram previamente sugeridas à Secex-CE para realização de ajustes, entende-se que, nesse momento, há somente duas novas considerações a serem apresentadas, conforme explicitado a seguir.

3. A primeira se refere à proposta de encaminhamento "I) d)" feita pela Secex-CE, referente ao achado quatro do relatório de auditoria. Entendemos que o estabelecimento de determinadas diretrizes de governança e de gestão de TI, conforme consta da proposta, será melhor abordado em um contexto de um sistema de governança de TI, que pretendemos trabalhar no âmbito do processo consolidador da FOC (TC 023.050/2013-6). Diante disso, entendemos que, neste momento, é desnecessária a referida proposta de recomendação.

4. A segunda consideração está relacionada à proposta de encaminhamento "I) vii)" referente ao achado sete do relatório de auditoria. Nesse caso, entendemos que a instituição, a partir da avaliação quantitativa e qualitativa do pessoal do setor de TI da universidade, deve envidar esforços para dotar a instituição com o quantitativo de pessoal que ela julgar ser adequado frente às necessidades, não devendo, necessariamente, acatar o quantitativo que o setor de TI considera como necessário para suprir as necessidades de TI da UFC. Dessa forma,

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade, informando o código 50952303.

sugerimos a substituição da redação da recomendação pela seguinte: "Recomendar ao Tribunal Regional do Trabalho da 7ª Região que avalie a adequação do estudo efetuado pela Secretaria de Tecnologia da Informação em relação às necessidades quantitativas e qualitativas de pessoal para a área de TI e envide esforços no sentido de dotar esse setor com o quantitativo de pessoal adequado para suprir as necessidades de trabalho em TI, à semelhança das orientações contidas no Cobit 5, Prática de Gestão APO07.01 – Maintain adequate and appropriate staffing (Manter pessoal adequado e apropriado – tradução livre)."

É o relatório.

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade, informando o código 50952303.

Proposta de Deliberação

Tratam os autos de auditoria integrante do conjunto de auditorias da primeira fase do trabalho de fiscalização de governança de tecnologia da informação (TI) com foco na avaliação da entrega de resultados e na gestão de riscos, realizado na sistemática de fiscalização de orientação centralizada (FOC).

2. Para responder às questões de auditoria formuladas com o fito de aferir a aderência do órgão/entidade às melhores práticas de governança e de gestão de TI, foi avaliada pela equipe de auditoria, no tocante à governança corporativa, a atuação da alta administração e do comitê de direção estratégica quanto ao estabelecimento e ao monitoramento de políticas corporativas, bem como aspectos relacionados à existência, à aplicação e à disseminação do código de ética.

3. No que diz respeito à governança de TI, foi verificado se: (i) foram definidas políticas e diretrizes de governança, gestão e uso de TI aptas a propiciar aprimoramento contínuo da governança de TI na instituição; (ii) foram definidos papéis e responsabilidades quanto à gestão e ao uso corporativo de TI, no sentido de se atingir os objetivos organizacionais; (iii) foram estabelecidas diretrizes para avaliar a gestão, o uso corporativo e o desempenho dos serviços de TI com foco no negócio institucional.

4. A equipe de auditoria examinou, ainda, se as estratégias e planos de TI são traçados em harmonia com o planejamento estratégico do órgão, a jurisprudência deste Tribunal e a IN SLTI 4/2010.

5. Quanto à gestão de pessoal de TI, procurou-se verificar se o órgão realiza avaliações quantitativas e qualitativas de seu quadro de profissionais alocados a essa área de forma a fundamentar futuros pleitos de ampliação e preenchimento de vagas, bem como se dispõe de plano periódico de capacitação.

6. A escolha dos aspectos examinados, bem como sua avaliação, baseou-se em normativos institucionais que tratam de fiscalização no âmbito deste Tribunal e decisões anteriores sobre a matéria, em especial o acórdão 1233/2012-TCU-Plenário.

7. Como critérios de auditoria, foram adotadas os seguintes modelos e normas de boas práticas: Cobit 5, da *Information Systems Audit and Control Association* (Isaca); NBR ISO/IEC 27002:2005 (NBR: 27002), 20000-2:2008 (NBR 20000-2) e 38500:2009 (NBR 38500); o Código de Melhores Práticas de Governança Corporativa do Instituto Brasileiro de Governança Corporativa (IBGC); e o Guia de Elaboração de Plano Diretor de Tecnologia da Informação (PDTI) do Sistema de Administração dos Recursos de Tecnologia da Informação (Sisp), assim definidos pela unidade técnica (grifos nossos):

> "O Cobit 5 consiste em um modelo de boas práticas para governança e gestão de tecnologia da informação organizado em cinco grandes domínios: *Evaluate, Direct and Monitor* (EDM), *Align, Plan and Organize* (APO), *Build, Acquire and Implement* (BAI), *Deliver, Service and Support* (DSS) e *Monitor, Evaluate and Assess* (MEA), cujas siglas serão utilizadas no decorrer do relatório para fins de referência ao critério de auditoria.
>
> A NBR 27002 consiste em um código de boas práticas para a gestão da segurança da informação amplamente adotado no mundo e tem como propósito prover uma base comum para o desenvolvimento de normas de segurança organizacional e das práticas efetivas de gestão da segurança, além de prover confiança nos relacionamentos entre as organizações, fornecendo aos seus usuários recomendações para a boa gestão da segurança da informação.
>
> Por sua vez, a NBR 20000-2 estabelece um código de prática que descreve as melhores práticas para processos de gerenciamento de serviços dentro do escopo da ABNT NBR ISO/IEC 20000-1. Essa norma faz parte da série ABNT NBR ISO/IEC 20000, que habilita provedores de

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade, informando o código 50952304.

serviços a entender como melhorar a qualidade dos serviços entregues aos seus clientes, tanto internos como externos.

Já a NBR ISO/IEC 38500 – norma de governança corporativa em tecnologia da informação – tem por objetivo fornecer uma estrutura de princípios para os dirigentes usarem na avaliação, no gerenciamento e no monitoramento do uso da tecnologia da informação em suas organizações. Essa norma oferece uma estrutura (contendo definições, princípios e um modelo) para a governança eficaz de TI que ajuda a alta administração das organizações a entender e cumprir suas obrigações legais, regulamentares e éticas com relação ao uso da TI em suas organizações.

O Código de Melhores Práticas de Governança Corporativa do IBGC propõe a adoção de princípios e boas práticas de governança corporativa, com vistas a reduzir eventuais fragilidades no sistema de governança das organizações, que se aplicam a qualquer tipo de organização, independente do porte, natureza jurídica ou tipo de controle. O código é adotado como referência para alguns controles e práticas que ajudam a orientar a organização como um todo e, por consequência, sua atuação na governança da TI.

Por fim, o Guia de Elaboração de PDTI do Sisp provê informações que ajudam as organizações a planejarem melhor as ações relacionadas a TI. Cabe ressaltar que, apesar do referido guia ser destinado às instituições que fazem parte do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP), considerou-se que as informações ali contidas são boas práticas que poderiam ser aplicadas para as demais instituições fiscalizadas neste trabalho."

II

8. Realizados os exames e ouvidos os servidores e administradores vinculados aos achados, a equipe de auditoria firmou diversas conclusões, relacionadas, principalmente, a deficiências em termos de ações de melhoria de governança e de falhas nos mecanismos de direção e avaliação da gestão de TI no órgão auditado.

9. Acerca da **governança corporativa**, dois aspectos foram considerados responsáveis para a qualificação "inadequada" que a equipe atribuiu à implementação dos mecanismos de governança corporativa no âmbito do TRT7: atuação deficiente da alta administração no monitoramento das políticas corporativas e falhas na aplicação do código de ética.

10. Constatou-se que, apesar da definição de políticas corporativas, tais como a Norma de Segurança dos Recursos de Tecnologia da informação, Estatuto de Ética Profissional e Política de Segurança Institucional do TRT7, não haveria evidências de que a alta administração exerça de forma adequada a definição e o monitoramento dessas políticas.

11. O segundo aspecto refere-se ao código de ética. O tribunal não realizou ações com o fito de divulgar o código de ética para seus servidores, bem como não haveria condições adequadas para o pleno funcionamento da comissão de ética, devido à ausência de local definido para execução de suas atribuições e para o arquivamento dos documentos utilizados e produzidos.

12. No que diz respeito especificamente à **governança de TI**, foram verificadas deficiências nas ações de melhoria de governança de TI, na formulação de diretrizes de governança por parte da alta administração e nos mecanismos para direção e avaliação da gestão e do uso corporativo de TI.

13. A equipe de auditoria constatou que, apesar de possuir procedimentos e controles voltados para a governança de TI, como, por exemplo, Comissão Permanente de Informática, o órgão judiciário não adota um processo formal voltado para a melhoria da governança de TI.

14. A equipe de auditoria qualificou como achados, notadamente, a falta de definição dos papéis e responsabilidades nas decisões mais relevantes quanto à gestão e ao uso corporativo de TI, e a

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade, informando o código 50952304.

ausência de mecanismos de gestão de riscos relacionados aos objetivos de gestão e usos corporativos e de planos de auditorias internas para avaliar os riscos considerados críticos para o negócio.

15. No que concerne ao item **'estratégias e planos'**, foram detectadas deficiências no planejamento de TI, por ter sido o PDTI aprovado nos exercícios de 2012 e 2013 sem o devido aval da Comissão Permanente de Informática.

16. Identificaram-se também falhas na **gestão de recursos humanos de TI**. Estudo realizado pela área de TI do TRT7 revelou a necessidade de acréscimo de 28 cargos especializados de analista judiciário - especialidade tecnologia da informação, que ainda não foram criados. Além disso, constatou que não há plano periódico de capacitação em gestão de TI.

17. No que diz respeito à **gestão de processos**, foram apontadas falhas relacionadas à gestão de acordos de nível de serviços, processos de gestão de segurança da informação, gestão de incidentes de segurança da informação, planejamento e gestão das contratações:

- gestão de acordos de nível de serviços: catálogo formal de serviços de TI que não contém informações detalhadas sobre os serviços, tais como responsáveis, prazos e horários de atendimento; inexistência de acordos de nível de serviço estabelecidos entre o setor de TI e as áreas internas;
- processos de gestão de segurança da informação: inexistência de: processo de gestão da continuidade dos serviços de TI formalmente aprovado e publicado; processo de inventário dos ativos de informação; política de controle de acesso à informação (PCA); programas de conscientização e treinamento em segurança da informação; e processo de gestão de riscos de segurança da informação.

18. Dados os achados mencionados e os critérios de avaliação utilizados pela equipe de auditoria, as conclusões implícitas em seu relatório, quanto às questões de auditoria indicam implementação parcial dos mecanismos de gestão e governança.

III

19. Concomitantemente com o exame das questões de auditoria, avaliou-se a ocorrência de possíveis inconsistências entre as evidências de implementação dos controles de TI pesquisadas na auditoria e as respostas apresentadas pelos órgãos e entidades quando do levantamento do perfil de governança de TI de 2012 (GovTI2012). Foram detectadas inconsistências.

20. A equipe de auditoria considerou que as inconsistências encontradas decorrem de causas diversas, tais como: falhas de interpretação do questionário por parte do órgão/ente fiscalizado; falta de clareza de algumas perguntas do questionário; grau de rigor empregado pela instituição na autoavaliação.

21. As principais inconsistências relatadas estão resumidas no quadro a seguir:

Seção	Resposta apresentada no Perfil GovTI2012	Situação encontrada (referência aos parágrafos)
1.1. Em relação à estrutura de governança corporativa, a Alta Administração da instituição:	A Alta Administração da instituição se responsabiliza pelo estabelecimento e pelo cumprimento das políticas corporativas	Apesar de estabelecer as políticas corporativas, a Alta Administração não monitora o cumprimento das mesmas (item 3.1)
1.2. Em relação à estrutura de governança de TI, a Alta Administração da instituição	A Alta Administração aprovou e publicou as diretrizes de avaliação de desempenho dos serviços de TI junto às unidades usuárias em termos de resultado do negócio institucional	Não foi aprovado documento algum nesse sentido (item 4.2)
5.2. Em relação à gestão de nível de serviço de TI:	Há um catálogo formal e atualizado de serviços dos serviços de TI oferecido aos clientes.	O catálogo apresentado não é formalizado e não dispõe de todas as

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade, informando o código 50952304.

		informações recomendadas (item 7.1)

22. Tal verificação possibilita subsidiar o aperfeiçoamento consistente do instrumento de levantamento e de avaliação de governança de TI.

IV

23. Considerados os parâmetros de avaliação utilizados e as conclusões reportadas pela equipe, as recomendações e determinações propostas são, na essência, adequadas, de forma que as acolho, com ajustes de forma e de tipo, e com exclusão daquelas cuja relação de pertinência não estava suficientemente demonstrada.

24. Por fim, é de capital importância realçar que a inobservância dos padrões de boas práticas mencionados anteriormente importa incorrer em sérios riscos, como bem apontou a equipe de auditoria:

- baixa efetividade de políticas importantes para o incremento da governança corporativa;
- limitações para o alcance da eficácia, eficiência e efetividade da TI para agregar valor ao negócio, com o fornecimento de serviços inadequados e dificuldades na priorização de esforços;
- desalinhamento das ações de TI com os objetivos das áreas de negócio, com aumento do riscos relacionados e da alocação inadequada de recursos financeiros e humanos;
- insuficiência de desempenho de TI, aumento dos riscos associados a TI e dúvidas quanto ao fato de a TI agregar valor ao negócio com riscos e custos aceitáveis;
- aumento da possibilidade de uma determinada ameaça explorar vulnerabilidades de um ativo ou de um conjunto de ativos da entidade;
- descontrole dos riscos a que os ativos de informações críticas para o negócio estão submetidos;
- paralisação de atividades prioritárias do órgão;
- exposição não autorizada de informação sigilosa;
- desconhecimento pelos servidores dos procedimentos a serem adotados quando da ocorrência de incidentes de segurança da informação.

25. Logo a alta administração do Tribunal Regional do Trabalho da 7ª Região deve ser alertada sobre os riscos atinentes à contratação de bens e serviços de TI a que está exposta ao não adotar adequadamente as boas práticas utilizadas como parâmetro de avaliação, bem como as recomendações exaradas nos acórdãos de referência.

Diante do exposto, manifesto-me pela aprovação do acórdão que ora submeto à apreciação deste Colegiado.

TCU, Sala das Sessões Ministro Luciano Brandão Alves de Souza, em 26 de março de 2014.

WEDER DE OLIVEIRA
Relator

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade, informando o código 50952304.

ACÓRDÃO Nº 750/2014 – TCU – Plenário

1. Processo nº TC 019.168/2013-6.
2. Grupo I – Classe V - Assunto: Relatório de Auditoria.
3. Interessados/Responsáveis: não há.
4. Órgão: Tribunal Regional do Trabalho da 7ª Região/CE.
5. Relator: Ministro-Substituto Weder de Oliveira.
6. Representante do Ministério Público: não atuou.
7. Unidade Técnica: Secretaria de Controle Externo no Ceará (Secex-CE).
8. Advogado constituído nos autos: não há.

9. Acórdão:

VISTOS, relatados e discutidos estes autos que tratam de auditoria realizada para avaliar processos e práticas de governança e de gestão de tecnologia da informação, com foco na avaliação da entrega de resultados e na gestão de riscos, adotados pelo Tribunal Regional do Trabalho da 7ª Região/CE.

ACORDAM os Ministros do Tribunal de Contas da União, reunidos em Sessão do Plenário, ante as razões expostas pelo Relator, em:

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;

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;

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;

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade, informando o código 50952307.

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;

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;

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;

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;

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;

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*;

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;

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;

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;

9.3. alertar a administração do Tribunal Regional do Trabalho da 7ª Região sobre os riscos atinentes à contratação de bens e serviços de TI, elencados no item 24 da proposta de deliberação, a que está exposta ao não adotar adequadamente as boas práticas utilizadas como parâmetro de avaliação, bem como as recomendações exaradas nos acórdãos de referência;

9.4. encerrar o presente processo e arquivar os autos.

10. Ata nº 9/2014 – Plenário.
11. Data da Sessão: 26/3/2014 – Ordinária.
12. Código eletrônico para localização na página do TCU na Internet: AC-0750-09/14-P.
13. Especificação do quorum:

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade, informando o código 50952307.

13.1. Ministros presentes: Aroldo Cedraz (na Presidência), Valmir Campelo, Walton Alencar Rodrigues, Benjamin Zymler, Raimundo Carreiro, José Múcio Monteiro e Ana Arraes.
13.2. Ministros-Substitutos presentes: Augusto Sherman Cavalcanti, Marcos Bemquerer Costa e Weder de Oliveira (Relator).

(Assinado Eletronicamente)
AROLDO CEDRAZ
na Presidência

(Assinado Eletronicamente)
WEDER DE OLIVEIRA
Relator

Fui presente:

(Assinado Eletronicamente)
PAULO SOARES BUGARIN
Procurador-Geral

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade, informando o código 50952307.