GRUPO I – CLASSE V – Plenário
TC 021.908/2013-3
Natureza: Relatório de Auditoria
Entidade: Universidade Tecnológica Federal do Paraná (UTFPR)
Advogado constituído nos autos: não há

SUMÁRIO: AUDITORIA OPERACIONAL. UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ. 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). TRABALHO REALIZADO EM DESACORDO COM AS ORIENTAÇÕES DIFUNDIDAS DURANTE A FOC. DETERMINAÇÃO. RECOMENDAÇÕES. ARQUIVAMENTO.

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 de TI informados pela Universidade Tecnológica Federal do Paraná (UTFPR) 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 o relatório de auditoria elaborado pela equipe da Secex-PR responsável pelos trabalhos (peça 17):

> "**1 Apresentação**
>
> 2 Em 27/3/2013, por meio da Ata 9 do Plenário do Tribunal de Contas da União (TCU), foi autorizado o Plano de Controle Externo de 2013/2014, contemplando 49 linhas de ação que impactam diretamente dez objetivos estratégicos do Plano Estratégico do Tribunal (PET-TCU) para o quadriênio 2011-2015 relacionados aos processos finalísticos do exercício do controle externo.
>
> 3 Entre os objetivos estratégicos estabelecidos no plano, destacam-se aqueles ligados à intensificação de ações que promovam a melhoria da gestão de riscos e de controles internos da Administração Pública (Objetivo Estratégico V) e ao aprimoramento de ações de controle voltadas à melhoria do desempenho da Administração Pública (Objetivo Estratégico VI).
>
> 4 A presente fiscalização, que tem por objetivo avaliar a implementação dos controles de TI informados em resposta ao levantamento do perfil de governança de TI de 2012, bem como verificar a adoção de planos e estratégias para implementação e melhoria da governança de TI, está alinhada a linhas de ação do Tribunal ligadas ao aperfeiçoamento do sistema de controle interno e da governança da Administração Pública.
>
> 5 Este trabalho foi realizado no âmbito 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 sob a forma de Fiscalização de Orientação Centralizada (FOC). Nesse contexto, a Secretaria de Fiscalização de Tecnologia da

Informação (Sefti), unidade orientadora dos trabalhos, é responsável pela preparação centralizada e pela consolidação dos resultados das auditorias, enquanto a execução das fiscalizações ficou a cargo de seis secretarias de controle externo dos estados, além da própria Sefti.

6 As instituições fiscalizadas no âmbito da FOC foram selecionadas com base em critérios de relevância, materialidade, risco e oportunidade, procurando-se, também, incluir nesse rol os órgãos e entidades para os quais já havia alguma fiscalização na área de TI previamente determinada por deliberação do TCU.

7 O presente relatório trata, em linhas gerais, de avaliação na Universidade Tecnológica Federal do Paraná - UTFPR de aspectos ligados à governança corporativa, à governança de TI, à formulação e implantação de estratégias e planos, à gestão de pessoas e à gestão de processos.

2 Introdução

2.1 Deliberação

8 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.

9 Com efeito, a presente fiscalização foi autorizada mediante Despacho do Ministro-Relator Weder de Oliveira 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.

2.2 Objetivos e Questões de Auditoria

10 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.

11 Para a realização deste trabalho, foram observados 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.

12 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.

13 Dessa forma, com base no objetivo da fiscalização e a fim de avaliar a aderência da Entidade 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?

Temas	Questões de auditoria
	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?

2.3 Visão Geral

14 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'.

15 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.

16 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).

17 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.

18 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.

19. 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 na Entidade. Em síntese, foram avaliados aspectos ligados à governança corporativa, à governança de TI, às estratégias e planos, à gestão de pessoas e à gestão de processos de TI.

2.4 Critérios e Metodologia

20 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.

21 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.

22 Ressalte-se que a equipe desta auditoria recebeu, durante uma semana na fase de planejamento/execução, 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 da entidade.

23 Além de dispositivos constitucionais, legais e infralegais, foram utilizados 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).

24 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.

25 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.

26 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.

27 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.

28 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.

29 Por fim, o Guia de Elaboração de PDTI do Sisp provê informações que ajudam as organizações a planejarem melhor as ações relacionadas à 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.

3 Governança Corporativa

30 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.

31 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.

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

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

comitê de direção estratégica;

ética institucional.

33 Achado 1 – Inexistência de comitê de direção estratégica para apoio em áreas de competência da alta administração.

Critério: seção 2.28 do Código das Melhores Práticas de Governança Corporativa do IBGC.

Análise das evidências: A Universidade não designou um comitê de direção estratégica, a Instituição não logrou comprovar a existência desse comitê.

Causas: deficiências dos controles internos

Efeitos e riscos decorrentes da manutenção da situação encontrada: planejamento estratégico deficiente

Esclarecimentos dos Responsáveis: A UTFPR informou que não possui um comitê de direção estratégica, porém alegou que as decisões e o estabelecimento de diretrizes estratégicas e as políticas e acompanhamento da gestão institucional são exercidas pela reitoria e suas assessorias de desenvolvimento institucional e de desenvolvimento acadêmico.

Conclusão da Equipe: Os esclarecimentos apresentados pela UTFPR confirmam a inexistência de um comitê de direção estratégica, porém a Instituição demonstrou a adoção de outra forma de tomada de decisão que cumpre a função desse comitê, razão pelo qual entendo que os esclarecimentos podem ser aceitos.

Propostas de encaminhamento: acatar os esclarecimentos apresentados pela Instituição.

33.1 Achado 2: falhas no planejamento estratégico institucional

Situação: inexistência de um processo de planejamento estratégico institucional formalmente aprovado

Critério: art. 6º, inciso I, do Decreto-Lei 200/1967.

Análise das evidências: embora a Instituição tenha informado no questionário que existe um processo de planejamento estratégico institucional formalmente aprovado e que esse processo é acompanhado e aperfeiçoado continuamente com base na análise de seus indicadores

ou metas estabelecidos, a Universidade não logrou comprovar a existência do processo. Constatou-se que o plano estratégico foi elaborado sem a definição de metas e indicadores.

Causas: deficiências dos controles internos

Efeitos e riscos decorrentes da manutenção da situação encontrada: deficiência do planejamento estratégico institucional

Esclarecimentos dos Responsáveis: informou que a elaboração do plano de desenvolvimento institucional segue a estruturação estabelecida no Artigo 16 do Decreto 5.773/2006, que trata da instrução para elaboração de plano de desenvolvimento institucional e o acompanhamento e prestação de contas deste planejamento são realizados anualmente e apresentadas no relatório de gestão, onde são detectadas as necessidades de aperfeiçoamento.

Conclusão da Equipe: Embora o artigo 16 do Decreto 5773/2006 se restrinja a definir o que deve integrar o plano de desenvolvimento institucional, pelos esclarecimentos apresentados, podemos considerar que a Instituição possui um plano de desenvolvimento institucional, razão pela qual os esclarecimentos podem ser aceitos.

Propostas de encaminhamento: acatar os esclarecimentos apresentados pela Instituição.

4 Governança de TI

34 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.

35 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.

36 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:

36.1 políticas de governança, gestão e uso de TI;

36.2 processo de melhoria do próprio sistema de governança de TI;

36.3 mecanismo decisório e de priorização das demandas da TI;

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

36.5 diretrizes formuladas pela alta administração;

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

37 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.

38 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.

39 Achado 3: Falhas nos mecanismos para dirigir e avaliar a gestão e o uso corporativos de TI.

Situação: ausência de indicadores de desempenho para cada objetivo de gestão e de uso corporativos de TI

Critério: item 9.1.1 do Acórdão 2.308/2010-TCU-Plenário e seção 3.3 da ABNT NBR ISO/IEC 38500:2009.

Análise das evidências: A UTFPR não aprovou documentos que estabeleçam indicadores de desempenho para cada objetivo de gestão e de uso corporativos de TI, embora tenha informado no item 1.3 do questionário que foram estabelecidas metas de desempenho de gestão e de uso corporativos de TI, bem como mecanismos de controle do cumprimento dessas metas.

Causas: deficiências dos controles internos.

Efeitos e riscos decorrentes da manutenção da situação encontrada: deficiências na direção e avaliação da gestão e o uso corporativos de TI.

Esclarecimentos dos Responsáveis: a UTFPR informou que as metas de gestão e de uso corporativo de TI, bem como os mecanismos de controle do cumprimento destas metas estão documentadas no relatório de gestão do exercício de 2012, que é o instrumento oficial das instituições para prestarem contas de suas atividades.

Conclusão da Equipe: o documento apresentado pela Entidade apresenta metas a serem alcançadas no período, mas não define indicadores para seu acompanhamento e tampouco apresentou mecanismos de controle do cumprimento dessas metas. Dessa forma, os esclarecimentos apresentados pela UTFPR não foram capazes de afastar a ocorrência do achado.

Propostas de encaminhamento: recomendar à Instituição a adoção de medidas corretivas.

5 Estratégias e Planos

40 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

41 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-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).

42 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.

43 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.

44 Achado 4 - Falhas no planejamento de TI.

Situação 1 – Não aprovação do PDTI pela alta administração.

Critério: art. 6º, inciso I, do Decreto-Lei 200/1967.

Análise das evidências: A UTFPR não apresentou documento que comprovasse a aprovação do PDTI pela alta administração.

Causas: deficiências dos controles internos.

Efeitos e riscos decorrentes da manutenção da situação encontrada: deficiências no planejamento de TI.

Esclarecimentos dos Responsáveis: informou que o PDTI foi enviado ao Reitor por intermédio Memorando n. 09/2012, pois comitê de TI não estava formalmente instituído. Em 30/10/2012, na primeira reunião do comitê, não houve tempo suficiente para análise do PDTI, ficando estabelecido em ata que seria enviado eletronicamente aos membros e que esta matéria seria apreciada na próxima reunião.

Conclusão da Equipe: os esclarecimentos apresentados pela UTFPR não foram capazes de afastar a ocorrência do achado.

Propostas de encaminhamento: efetuar determinação à Instituição.

6 Gestão de Pessoas de TI

45 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).

46 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 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.’

47 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.

48 Achado 5: Inexistência de um plano periódico de capacitação.

Critério: item 9.9.1 do Acórdão 1.233/2012-TCU-Plenário.

48 Análise das evidências: a Universidade informou no questionário Perfil GovTI 2012 que elaborou e executou um plano de capacitação para atender as necessidades na gestão de TI, mas não apresentou documentos que comprovem a existência e a execução desse plano.

Causas: deficiências dos controles internos

Efeitos e riscos decorrentes da manutenção da situação encontrada: deficiências na capacitação de pessoal

Esclarecimentos dos Responsáveis: embora o plano de capacitação dos servidores de TI não esteja definido em um documento específico, ele está previsto no item 9.1 do PDTI.

Conclusão da Equipe: Embora o PDTI não tenha sido aprovado pela Administração, as ações de capacitação do período constam naquele plano, razão pelo qual as justificativas apresentadas podem ser aceitas.

Propostas de encaminhamento: acatar os esclarecimentos apresentados pela Instituição.

7 Processos

49 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.

50 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.

51 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.

52 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.

53 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.

54 Para a execução dos objetivos de negócio, as 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.

55 Achado 6: Falhas em processos de gestão de segurança da informação.

Situação 1: inexistência de processo de gestão de continuidade de serviços de TI.

Critério: Cobit 5, DSS04.3 – Develop and implement a business continuity response.

Análise das evidências: a UTFPR não comprovou que possui um processo de gestão da continuidade dos serviços de TI formalmente aprovado e publicado, apesar de informar essa situação no questionário Perfil GovTI 2012.

Causas: deficiências dos controles internos

Efeitos e riscos decorrentes da manutenção da situação encontrada: deficiências na segurança das informações

Esclarecimentos dos Responsáveis: a UTFPR reconheceu que não possuí um plano formal de gestão da continuidade dos serviços de TI, porém informou a existência de ações instituídas para preservar os dados institucionais, como procedimento de backup e redundância em outro local físico.

Conclusão da Equipe: os esclarecimentos apresentados pela UTFPR não foram capazes de afastar a ocorrência do achado.

Propostas de encaminhamento: recomendar à Instituição a adoção de medidas corretivas.

Situação 2 – Ausência de processo de análise dos riscos.

Critério: NC – DSIC/GSI/PR 4/IN01

Análise das evidências: apesar de informado no questionário Perfil GovTI 2012, a Universidade não comprovou possuir um processo aprovado e publicado de análise dos riscos, aos quais as informações críticas para o negócio estão submetidas. O plano de gestão de riscos incluído no PDTI trata o processo de forma superficial e não foi comprovada a sua aprovação pela alta administração.

Causas: deficiências dos controles internos

Efeitos e riscos decorrentes da manutenção da situação encontrada: deficiências na segurança das informações

Esclarecimentos dos Responsáveis: a UTFPR informou que o plano de gestão de riscos está inserido no PDTI.

Conclusão da Equipe: os esclarecimentos apresentados pela UTFPR não foram capazes de afastar a ocorrência do achado, pois o plano de gestão de riscos incluído no PDTI trata o processo de forma superficial.

Propostas de encaminhamento: recomendar à Instituição a adoção de medidas corretivas.

55.1 Achado 7: Inexistência de Política de Segurança da Informação e Comunicações

Critério: art. 5º, inciso VII, Instrução Normativa GSI/PR n. 1, de 13 de junho de 2008.

Análise das evidências: apesar de informado no questionário Perfil GovTI 2012, a UTFPR não possui norma que defina uma política de segurança de informação e de controle de acesso. A Universidade apresentou apenas uma proposta de regulamento de gestão e de utilização de recursos de tecnologia da informação da UTFPR.

Causas: deficiências dos controles internos

Efeitos e riscos decorrentes da manutenção da situação encontrada: deficiências na segurança das informações

Esclarecimentos dos Responsáveis: a UTFPR informou que foi designada uma comissão para elaborar a Política de Segurança da Informação.

Conclusão da Equipe: os esclarecimentos apresentados pela UTFPR não foram capazes de afastar a ocorrência do achado.

Propostas de encaminhamento: determinar à Instituição a adoção de medidas corretivas.

55.2 Achado 8: Falhas na alocação de responsabilidades pela segurança da informação

Critério: art. 5º, inciso VI, Instrução Normativa GSI/PR n. 1, de 13 de junho de 2008.

Análise das evidências: a Universidade não designou formalmente um comitê de segurança, um gestor de segurança da informação, uma equipe de gestão de incidentes de segurança da informação e uma equipe de tratamento e resposta de incidentes em redes computacionais.

Causas: deficiências dos controles internos

Efeitos e riscos decorrentes da manutenção da situação encontrada: deficiências na segurança das informações

Esclarecimentos dos Responsáveis: a UTFPR informou que até a designação formal de um comitê de segurança da informação e comunicação estas responsabilidades ficam a cargo dos servidores do Departamento de Infraestrutura de TI, atribuição expressa no Regimento Geral.

Conclusão da Equipe: os esclarecimentos apresentados pela UTFPR não foram capazes de afastar a ocorrência do achado.

Propostas de encaminhamento: determinar à Instituição a adoção de medidas corretivas.

55.3 Achado 9: Falhas na gestão das contratações de TI.

Critério: item 9.2.9.9 do Acórdão 1.233/2012-TCU-Plenário.

Análise das evidências: apesar de informado no questionário Perfil GovTI 2012, a Universidade não logrou comprovar que existem procedimentos internos que auxiliam na padronização do processo de planejamento das contratações.

Causas: deficiências dos controles internos

Efeitos e riscos decorrentes da manutenção da situação encontrada: falta de padronização, compras antieconômicas, diminuição da qualidade, etc.

Esclarecimentos dos Responsáveis: a Universidade informou que as contratações de TI baseiam-se no PDTI, visando atender aos itens 10.1, 'Ações/projetos Estruturantes' e 11.2 'Investimentos' do PDTI.

Conclusão da Equipe: os esclarecimentos apresentados pela UTFPR não foram capazes de afastar a ocorrência do achado, pois o PDTI não foi aprovado pela Administração.

Propostas de encaminhamento: recomendar à Instituição a adoção de medidas corretivas.

8 Conclusão

56 Um dos objetivos 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.

57 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 abaixo:

Seção	Resposta apresentada no Perfil GovTI2012	Situação encontrada
1.3	Estabeleceu metas de desempenho da gestão e do uso corporativos de TI, para 2012.	Inexistência de indicadores para acompanhamento das metas e de mecanismos de controle do cumprimento dessas metas (Achado 3).
2.3	A instituição aprovou e publicou PDTI interna ou externamente.	Inexistência de PDTI aprovado pela alta administração (Achado 4, Situação 1).
5.1	Implementou os processos de gestão da continuidade dos serviços de TI.	Inexistência de um processo de gestão da continuidade dos serviços de TI formalmente aprovado e publicado (Achado 6, Situação 1).
5.3	implementou formalmente processo de análise dos	Inexistência de processo de análise dos riscos (Achado 6,

Seção	Resposta apresentada no Perfil GovTI2012	Situação encontrada
	riscos aos quais a informação crítica para o negócio está submetida.	Situação 2).
5.3	designou formalmente pessoas ou unidade para gerenciar a segurança de informação e comunicações.	Inexistência de um comitê ou gestor de segurança da informação (Achado 8).
5.8	Além dos procedimentos legais, há procedimentos internos que auxiliam na padronização do processo de planejamento das contratações.	Inexistência de procedimentos internos que auxiliam na padronização do processo de planejamento das contratações (Achado 9).

58 A quantidade de achados decorrentes das divergências entre as respostas apresentadas no questionário Perfil GovTI 2012 e as situações reais colhidas na ocasião da auditoria na UTFPR demonstra que não se tratou de falta de clareza do questionário ou interpretação equivocada das questões, mas do baixo grau de rigor empregado pela Instituição na autoavaliação, que deve ser motivo de recomendação para que essa situação seja evitada nos próximos levantamentos do perfil de governança de TI.

9 Encaminhamento

59 Diante do exposto, propõe-se o encaminhamento ao Gabinete do Ministro-Relator com a seguinte proposta de decisão:

a) determinar à Universidade Tecnológica Federal do Paraná que, no prazo de 90 (noventa) dias, adote as seguintes providências:

a1) elabore e aprove formalmente a Política de Segurança da Informação, que deve contemplar, em especial, os elementos estabelecidos no item 5.3 da NC – DSIC/GSI/PR 3/IN01, 30 de junho de 2009, e na seção 5.1.1 da ABNT NBR ISO/IEC 27002:2005, em atenção ao art. 5º, inciso VII, da IN – GSI/PR 1/2008;

a2) institua Comitê Gestor de Segurança da Informação e Comunicações à semelhança das orientações contidas no item 6.1.2 da ABNT NBR ISO/IEC 27002:2005 em atenção ao art. 5º, inciso VI, da IN – GSI/PR 1/2008 c/c o item 5.3.7.3 da NC – DSIC/GSI/PR 3/IN01, de 30 de junho de 2009;

a3) institua formalmente o plano diretor de TI, que deve ser aprovado pelo dirigente máximo da instituição em atenção ao art. 6º, inciso I, do Decreto-Lei 200/1967;

a4) 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, 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,* em atenção às disposições contidas na NC – DSIC/GSI/PR 6/IN01, de 11 de novembro de 2009, e em consonância com o item 9.2 do Acórdão 1.603/2008-TCU-Plenário;

a5) implante programas de conscientização e treinamento em segurança da informação, à semelhança das orientações contidas na seção 8.2.2 da ABNT NBR ISO/IEC 27002:2005, em atenção ao disposto na seção 3.2.5 da NC – DSIC/GSI/PR 2/IN01, 13 de outubro de 2008;

a6) 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, em atenção ao disposto na NC – DSIC/GSI/PR 4/IN01, de 15 de fevereiro de 2013;

b) recomendar à Universidade Tecnológica Federal do Paraná – UTFPR, com fulcro no art. 43, inciso II, da Lei 8.443/1992 c/c o art. 250, inciso III, do Regimento Interno do TCU, que:

b1) aumente o rigor das informações a serem prestadas nos próximos levantamentos do perfil de governança de TI de modo a refletir a real situação da Instituição e aumentar a confiabilidade dos questionários;

b2) faça constar do plano diretor de TI pelo menos os seguintes elementos, em consonância com o art. 6º, inciso I, do Decreto-Lei 200/1967:

- desdobramento das diretrizes estabelecidas em planos estratégicos, a exemplo do plano;
- estratégico institucional e do plano estratégico de TI;
- vinculação das ações de TI (atividades e projetos) a indicadores e metas de negócio;
- vinculação das ações de TI a indicadores e metas de serviços ao cidadão;
- vinculação entre as ações de TI priorizadas ao orçamento de TI;
- quantitativo necessário (ideal) para a força de trabalho em TI;

b3) em consonância com o disposto no item 9.1.1 do Acórdão 2.308/2010-TCU-Plenário e com base nas boas práticas abaixo, contidas na seção 3.3 da ABNT NBR ISO/IEC 38500:2009, estabeleça formalmente:

- objetivos de gestão e de uso corporativos de TI alinhados às estratégias de negócio;
- indicadores de desempenho para os objetivos de gestão definidos;
- metas de desempenho da gestão e do uso corporativos de TI para cada indicador definido;
- mecanismos para que a alta administração acompanhe o desempenho da TI da instituição;
- mecanismos de gestão dos riscos relacionados aos objetivos de gestão e de uso corporativos de TI. (usar subitem 'a' se não houver objetivo estratégico definido; usar subitem 'b' se não houver indicador de desempenho definido e assim sucessivamente);

b4) implante formalmente processo de contratação de soluções de TI, adequando o processo definido na IN – SLTI/MP 4/2010, em consonância com o item 9.2.9.9 do Acórdão 1.233/2012-TCU-Plenário;

c) determinar à Secex-PR que monitore o cumprimento das determinações contidas no subitem 'a' desta deliberação;

d) arquivar o presente processo."

4. Por meio do despacho à peça 22, encaminhei os autos à Secretaria de Fiscalização de Tecnologia da Informação (Sefti), para que aquela unidade técnica, coordenadora da FOC, examinasse a proposta apresentada pela Secex-PR.

5. Em seguida, o auditor da Sefti emitiu o parecer à peça 23, nos seguintes termos:

"Trata-se de auditoria operacional executada e coordenada pela Secretaria de Controle Externo no Estado do Paraná (Secex-PR) na Universidade Tecnológica Federal do Paraná (UFPR), no âmbito da primeira fase da Fiscalização de Orientação Centralizada (FOC), na área de governança de Tecnologia da Informação (TI), com foco na avaliação da entrega de resultados e na gestão de riscos.

HISTÓRICO

Inicialmente, cabe salientar que a coordenação central da FOC está a cargo da Secretaria de Fiscalização de Tecnologia da Informação (Sefti), que orientou e acompanhou a equipe de auditoria da Secex-PR durante toda a fiscalização. Após a conclusão da versão preliminar do relatório de fiscalização pela unidade executora, auditores da Sefti realizaram revisão do documento para verificação de sua adequação aos padrões técnicos e metodológicos propostos no âmbito da FOC.

Ressalte-se que, uma vez que a fiscalização na UTFPR foi realizada e supervisionada pela Secex-PR, a Sefti encaminhou sugestões de melhoria à equipe de auditoria, para que fizesse as adaptações que entendesse pertinentes ao relatório.

Posteriormente, por meio do Ofício 3112/2013-GAB-SECEX/PR (peça 4), a Secex-PR encaminhou à entidade documento contendo o resumo dos treze achados identificados durante auditoria para que os gestores da UTFPR pudessem se manifestar a respeito. Dessa forma, os gestores não tiveram contato com o relatório preliminar de auditoria à época, portanto também não teriam tomado conhecimento das propostas de encaminhamento formuladas pela equipe de fiscalização, aparentemente divergindo do preconizado pelo parágrafo 185 do 'Manual de Auditoria Operacional', aprovado pela Portaria-Segecex 4, de 26/2/2010.

Em resposta ao citado ofício, a UTFPR apresentou comentários aos achados de auditoria por meio do Ofício 188 – GABIR (peça 5). Após a análise do pronunciamento da entidade, a Secex-PR manteve todos os achados de auditoria identificados preliminarmente, encaminhando o relatório (peça 10) ao Gabinete do Relator para fins de julgamento do processo. No entanto, mediante Despacho (peça 12), o Ministro-Relator submeteu os autos à Sefti para emissão de parecer técnico sobre a fiscalização.

Concluída a avaliação do relatório de fiscalização produzido pela Secex-PR, a Sefti propôs a devolução dos autos àquela Secretaria para realização de ajustes com o intuito de padronizar a nomenclatura e a organização dos achados de auditoria, informando que já havia realizado tratativas com representantes da Secex-PR no sentido de se efetuar as mudanças necessárias (peça 13). Mediante despacho, essa proposta foi acolhida pelo Ministro-Relator, que restituiu os autos à referida unidade técnica (peça 16).

Assim, a Secex-PR produziu uma nova versão do relatório (peça 17), reduzindo a sua quantidade de achados de treze para nove, sendo que os achados, 1, 2 e 5 foram descaracterizados em decorrência do acatamento dos comentários dos gestores pela equipe de auditoria. Além disso, foram incorporadas diversas sugestões de mudanças apresentadas por esta Secretaria.

Contudo, após o encaminhamento dessa nova versão ao Relator do processo, o relatório foi novamente submetido à análise da Sefti, com o intuito de alcançar harmonização de entendimentos e uniformidade de encaminhamentos (peça 22). O parecer em tela tem como objetivo atender a esse comando do Ministro-Relator.

EXAME TÉCNICO

Inicialmente, cabe destacar que não foram identificadas na versão final do relatório de auditoria (peça 17) descrições que remetessem à situação atual de diversos dos processos e práticas de governança e gestão de TI existentes na instituição, fato que se mostrou em desacordo com as orientações difundidas pela equipe de coordenação da FOC.

Na verdade, a equipe de auditoria limitou-se a registrar as situações que geraram achados e/ou inconsistências entre as evidências de implementação dos controles de TI e as respostas apresentadas pela UTFPR no levantamento do perfil de governança de TI de 2012 (GovTI 2012). Dessa forma, não é possível identificar, pela leitura do aludido relatório, se existiriam situações que remetessem a boas práticas de governança e de gestão da entidade.

No que diz respeito aos achados de auditoria, será feita análise individual de cada um deles.

Em relação ao Achado 1 (peça 17, p. 7, 'Inexistência de comitê de direção estratégica para apoio em áreas de competência da alta administração'), verificou-se que a equipe de auditoria não apresentou proposta de encaminhamento, acatando as justificativas da entidade. A equipe entendeu que, embora a instituição não tenha um comitê de direção estratégica, existe outra forma de tomada de decisão que cumpriria a função do referido comitê.

Considerando que, a partir dos esclarecimentos dos responsáveis, as decisões relacionadas às diretrizes estratégicas e às políticas de acompanhamento da gestão institucional

são exercidas pela reitoria e suas assessorias, entende-se que esse grupo de tomadores de decisão constitui, ainda que informalmente, o comitê de direção estratégica da universidade, razão pela qual concorda-se com o acatamento dos esclarecimentos dos gestores quanto a esse ponto, descaracterizando-se, assim, o referido achado. Nesse contexto, inexiste motivo para que o Achado 1 permaneça, motivo pelo qual sugere-se sua supressão.

No que tange ao Achado 2 (peça 17, p. 7, 'Falhas no planejamento estratégico institucional'), constatou-se que a equipe de auditoria também acatou as justificativas da entidade, abstendo-se de apresentar propostas de encaminhamento. A equipe da Secex-PR entendeu que, embora o art. 16 do Decreto 5.773/2006 se restrinja a definir o que deve integrar o plano de desenvolvimento institucional (PDI), poderia se considerar que a universidade possui um PDI, razão pela qual os esclarecimentos poderiam ser aceitos.

Analisando-se os presentes autos, não foi possível confirmar o entendimento da Secex-PR de que a universidade possui, de fato, um PDI, tendo em vista que tal documento não consta como peça do processo. Além disso, o procedimento de auditoria que deu origem a esse achado previa verificar, além da aderência ao GovTI 2012, se a entidade possui processo (formal ou informal) de planejamento estratégico institucional, e não somente o resultado desse processo, que seria o plano estratégico institucional.

De acordo com definição trazida pela norma ISO 9.000, 'qualquer atividade, ou conjunto de atividades, que usa recursos para transformar insumos (entradas) em produtos (saídas) pode ser considerado como um processo'. Com efeito, a especificação de um processo de planejamento deve, no mínimo, defini-lo em termos de um conjunto de atividades, insumos e produtos.

O art. 16 do Decreto 5.773/2006 estabelece os elementos que devem constar do PDI, tais como missão, objetivos e metas da instituição, projeto pedagógico, cronograma de implantação e desenvolvimento da instituição e de cada um de seus cursos, entre outro. No entanto, tal normativo não define as etapas e as atividades que compõem a elaboração desse plano, nem as pessoas (papéis) envolvidas. Nesse sentido, conclui-se que o PDI não se confunde com o processo de planejamento estratégico institucional.

Assim sendo, entende-se que o achado deveria ser mantido, o que implicaria na seguinte proposta de encaminhamento: 'Determinar à UTFPR que, em atenção ao art. 6º, inciso I, do Decreto-Lei 200/1967, estabeleça processo de planejamento estratégico institucional que contemple, pelo menos, as práticas descritas nos itens 9.1.1.1 a 9.1.1.6 do Acórdão 1.233/2012-TCU-Plenário'.

Registre-se que, à época da resposta ao GovTI 2012, a entidade informou possuir um processo formal (aprovado e publicado) de planejamento estratégico institucional, algo que não restou demonstrado. Vale ressaltar que a identificação de inconsistências quanto às respostas ao GovTI 2012 não geram, necessariamente, achados de auditoria, devido a causas variadas, tais como falhas de interpretação do questionário por parte do órgão/ente fiscalizado e falta de clareza em algumas perguntas do questionário.

Quanto à resposta ao item em particular, constatou-se, durante a execução das demais auditorias, que era comum aos gestores confundir 'plano estratégico formalmente aprovado' com 'processo formal de planejamento estratégico institucional'. Erro que, aparentemente, a UTFPR também incorreu e, portanto, deveria ter sido relatado na conclusão do relatório da Secex-PR, mais especificamente no quadro de inconsistências de respostas do questionário do perfil GovTI 2012, conforme explicitado a seguir:

Seção	Resposta apresentada no Perfil GovTI 2012	Situação encontrada
2.1	O processo de planejamento estratégico institucional formal é aperfeiçoado continuamente com base na análise de seus indicadores.	Inexistência de processo de planejamento estratégico institucional (Achado 2).

Por fim, tendo em vista que esse achado faz parte da questão 4 de auditoria ('As estratégias e planos corporativos e de TI foram definidos e implementados adequadamente no âmbito da Instituição?') e que essa questão está associada ao tema 'Estratégias e Planos' (peça 17, p. 4), o Achado 2 deveria ter sido incluído no capítulo relativo a esse tema, ao invés de ter sido relatado no capítulo de 'Governança Corporativa'.

Relativamente ao Achado 3 (peça 17, p. 8, 'Falhas nos mecanismos para dirigir e avaliar a gestão e o uso corporativos de TI'), a equipe de auditoria entendeu que o documento apresentado pela entidade estabelece metas a serem alcançadas no período, mas não define indicadores para seu acompanhamento, tampouco define mecanismos de controle do cumprimento dessas metas, o que acarretou na manutenção do achado.

Analisando-se o documento 'Relatório de Gestão do Exercício de 2012', p. 49 e 52-55, consultado em 28/3/2014 no link 'http://www.utfpr.edu.br/estrutura-universitaria/diretorias-de-gestao/diretoria-de-gestao-da-avaliacao-institucional/relatorios-de-gestao/relatorio_gestao_2012_20130510.pdf', verifica-se que foram estabelecidos dois objetivos estratégicos relacionado à TI, a saber: objetivo 1.1 – consolidar a UTFPR como referência das instituições tecnológicas brasileiras, bem como o objetivo 1.3 – aprimorar os mecanismos de gestão de tecnologia de informação.

Para cada objetivo, é possível constatar que foram definidas metas, além das etapas necessárias para atingi-las. Entretanto, não é possível identificar claramente os indicadores que permitem avaliar o alcance dos referidos objetivos estratégicos. Além disso, não foi constatada a existência de mecanismos que permitam supervisionar a progressão e o cumprimento das metas de TI, tais como reuniões periódicas de acompanhamento ou relatórios contendo essas informações. Também não há evidências nos autos de que a entidade adota mecanismos de gestão dos riscos relacionados aos objetivos de gestão e de uso corporativos de TI. Diante disso, entende-se que o achado deve ser mantido.

Verificou-se, no entanto, que a proposta de encaminhamento 'b3' da seção '9. Encaminhamento' do relatório elaborado pela Secex-PR (peça 17, p. 15) recomendou o estabelecimento de elementos para dirigir e avaliar o uso da TI que já haviam sido definidos pela universidade, em especial os objetivos de gestão e de uso corporativos de TI e as metas de desempenho da gestão e do uso corporativos de TI.

Dessa forma, sugere-se que a proposta de encaminhamento 'b3' do relatório tenha a seguinte redação:

> 'em consonância com o disposto no item 9.1.1 do Acórdão 2.308/2010-TCU-Plenário e com base nas boas práticas abaixo, contidas na seção 3.3 da ABNT NBR ISO/IEC 38500:2009, estabeleça formalmente: indicadores de desempenho para os objetivos de gestão definidos; mecanismos para que a alta administração acompanhe o desempenho da TI da instituição; mecanismos de gestão dos riscos relacionados aos objetivos de gestão e de uso corporativos de TI.'

Ademais, a inconsistência relatada pela equipe da Secex-PR relativa à seção 1.3 do questionário do perfil GovTI 2012 está equivocada. Na verdade, a inconsistência que deveria ter sido lançada está relacionada à resposta 'estabeleceu os mecanismos de controle do cumprimento das metas de gestão e de uso corporativos de TI' e não à resposta 'estabeleceu metas de desempenho da gestão do uso corporativos de TI, para 2012', pois tais metas, a exemplo dos objetivos estratégicos, foram, de fato, estabelecidas.

Por sua vez, os indicadores não foram definidos, todavia a entidade informou no questionário do perfil GovTI 2012 que não os havia instituído, razão pela qual não existe inconsistência nesse caso. Diante disso, sugere-se que seja lançada a seguinte inconsistência:

Seção	Resposta apresentada no Perfil GovTI 2012	Situação encontrada
1.3	Estabeleceu os mecanismos de controle do	Inexistência de mecanismos que permitam supervisionar a

Seção	Resposta apresentada no Perfil GovTI 2012	Situação encontrada
	cumprimento das metas de gestão	progressão e o cumprimento das metas de TI, tais como reuniões periódicas de acompanhamento ou relatórios contendo essas informações (Achado 3)

Quanto ao Achado 4 (peça 17, p. 9-10, 'Falhas no planejamento de TI'), a equipe de auditoria da Secex-PR entendeu que os esclarecimentos dos responsáveis não foram capazes de afastar a ocorrência do achado de que a alta administração não teria aprovado o Plano Diretor de Tecnologia da Informação (PDTI) da entidade.

Avaliando-se os comentários dos gestores a esse respeito (peça 5, p. 3) entende-se que, embora a universidade tenha afirmado que o tema será submetido à discussão na próxima reunião do comitê de TI, o PDTI, de fato, ainda não foi aprovado pela alta direção da instituição, razão pela qual tanto o achado quanto as respectivas propostas de encaminhamento devem ser mantidos. Além disso, persiste a inconsistência entre a resposta informada à seção 2.3 do questionário perfil GovTI 2012 e a situação fática encontrada na entidade (peça 17, p. 13)

No que concerne ao Achado 5 (peça 17, p. 10, 'Inexistência de um plano periódico de capacitação'), constatou-se que a equipe de auditoria acatou as justificativas da entidade, abstendo-se de apresentar propostas de encaminhamento. A equipe de auditoria da Secex-PR entendeu que, apesar de o PDTI não ter sido aprovado pela Administração da entidade, as ações de capacitação do período constam naquele plano, razão pela qual as justificativas apresentadas poderiam ser aceitas.

Ao analisar o item 9.1 da minuta do Plano Diretor de Tecnologia da Informação, p. 23, consultado em 28/3/2014 no link 'http://www.utfpr.edu.br/estrutura-universitaria/diretorias-de-gestao/dirgti/documentos/PDTI2011Versofinal.pdf', verifica-se apenas a existência de um quadro informando a participação do setor de TI da universidade em cursos e eventos em 2011, ano anterior à minuta do plano, não estando presentes os seguintes elementos: treinamentos que se pretendia realizar nos próximos anos; eventos que se pretendia participar; competências que se pretendia desenvolver com as ações de capacitação.

Tais elementos, que são típicos de um instrumento que traduz o planejamento das ações de capacitação, não constam do item 9.1 da minuta de PDTI da UTFPR, razão pela qual essa seção do documento não deve ser considerada como plano de capacitação da universidade.

Sendo assim, discorda-se do entendimento da Secex-PR e considera-se que o achado deveria ter sido mantido, acompanhado da seguinte proposta de encaminhamento: 'Recomendar à UTFPR 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'.

Além disso, sugere-se que fique registrada a inconsistência da resposta apresentada à seção 4.4 do questionário do perfil GovTI 2012, pois não restou comprovado que 'a instituição elabora e executa um plano de capacitação para atender às necessidades de capacitação em gestão de TI', conforme assinalado pela entidade (peça 1, p. 5). Nesse caso, a inconsistência poderia ser lançada da seguinte forma:

Seção	Resposta apresentada no Perfil GovTI 2012	Situação encontrada
4.4	A instituição elabora e executa um plano de capacitação para atender às necessidades de capacitação em gestão de TI.	Inexistência de plano de capacitação para atneder às necessidades em gestão de TI (Achado 5)

Quanto ao Achado 6 (Peça 17, p. 11-12, 'Falhas em processos de gestão de segurança da informação'), a equipe de auditoria da Secex-PR entendeu que os esclarecimentos dos responsáveis não foram capazes de afastar a ocorrência do achado, pois, segundo a equipe, a entidade não dispõe de um processo de gestão de continuidade de serviços de TI e o plano de gestão de riscos incluído no PDTI trata o processo de forma superficial.

Analisando-se os comentários dos gestores quanto aos problemas relatados nesse achado (peça 5, p. 3-4), verifica-se que a entidade adota ações com a finalidade de preservar os dados institucionais, como procedimento de *backup* e redundância em outro local físico, porém reconhece que não dispõe de processo formal para gestão da continuidade dos seus serviços de TI. Diante disso, as justificativas apresentadas pelos gestores não são capazes de descaracterizar essa parte do achado de auditoria. Em relação ao processo de gestão de riscos de segurança da informação, entende-se que o plano de gestão de riscos, constante da seção 10.2 da minuta de PDTI, não deve ser confundido com um processo destinado a gerenciar esses riscos, conforme já explicado no parágrafo deste parecer.

Ante o exposto, entende-se que o achado deve ser mantido. No entanto, há uma ressalva a se fazer na proposta de recomendação referente à inexistência de processo de gestão de continuidade dos serviços de TI, pois a Secex-PR lançou a proposta relativa a inexistência de plano de continuidade de negócio, situação que não foi objeto de avaliação do relatório de fiscalização. Assim, sugere-se a substituição da proposta 'a4' da seção '9. Encaminhamento' (peça 17, p. 14) pela seguinte proposta: 'Recomendar à UTFPR 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 implemente a business continuity response* (Desenvolver e implementar resposta à continuidade do negócio – tradução livre)'.

No que diz respeito ao Achado 7 (Peça 17, p. 12, 'Inexistência de Política de Segurança da Informação e Comunicações' – PSI), a equipe de auditoria da Secex-PR entendeu que os esclarecimentos dos responsáveis também não foram capazes de afastar a ocorrência do achado.

De fato, os comentários dos gestores quanto a esse achado (peça 5, p. 4) demonstram que foi designada uma comissão para elaborar a PSI, conforme consta do link http://utfpr.edu.br/estrutura-universitaria/diretorias-de-gestao/dirgti/seguranca (acessado em 28/3/2014). Nessa página, fica claro que tal política ainda está em fase de elaboração. Diante disso, o achado e a respectiva proposta de encaminhamento devem ser mantidos.

Em relação ao Achado 8 (peça 17, p. 12-13, 'Falhas na alocação de responsabilidades pela segurança da informação'), a equipe de auditoria da Secex-PR registrou que a universidade não havia designado formalmente um comitê de segurança da informação (CSI), um gestor de segurança da informação (SI), uma equipe de gestão de incidentes de SI e uma equipe de tratamento e resposta a incidentes em redes computacionais (Etir). A equipe concluiu que o achado deveria ser mantido, apesar das justificativas apresentadas pelos responsáveis.

Avaliando-se os comentários apresentados (peça 5, p.4), verificou-se que os gestores da entidade se manifestaram apenas a respeito da ausência de CSI, não se posicionando sobre a inexistência das outras responsabilidades em segurança da informação apontadas pela equipe de auditoria. A UTFPR informou que, até que seja designado formalmente um comitê de SI, as responsabilidades relativas à segurança da informação ficam a cargo dos servidores do Departamento de infraestrutura de TI, conforme atribuição expressa no art. 143 do Regimento Geral.

Em que pese as competências previstas no art. 143 do aludido regimento, elas não suprem as responsabilidades definidas no item 5.3.7.3 da NC – DSIC/GSI/PR 3/IN01, de 30 de junho de 2009, razão pela qual o achado e a respectiva proposta de encaminhamento devem ser mantidos. Além disso, como a universidade não se manifestou sobre a possível inexistência das demais responsabilidades apontadas pela equipe da Secex-PR, considera-se que as demais propostas de encaminhamento também devem permanecer.

No que tange ao Achado 9 (peça 17, p. 13, 'Falhas na gestão das contratações de TI), mais uma vez a equipe entendeu que os esclarecimentos dos responsáveis não descaracterizam a situação previamente identificada.

Sobre esse achado, os gestores informaram que as contratações de TI baseiam-se no PDTI, visando atender aos itens 10.1, 'Ações/projetos Estruturantes' e 11.2 'Investimentos'. De fato, da leitura dos referidos itens da minuta do PDTI (http://www.utfpr.edu.br/estrutura-universitaria/diretorias-de-gestao/dirgti/documentos/PDTI2011Versofinal.pdf, p. 25-27 e 30-31), verifica-se apenas uma descrição sucinta de como é feito o planejamento da área de TI da universidade, além dos investimentos e dos projetos prioritários da área de TI para os anos de 2012 a 2015.

No entanto, essa descrição não se confunde com um processo de gestão das contratações de soluções de TI, que trata dos responsáveis, atividades e artefatos relacionados à gestão dos contratos de TI da entidade. Além disso, não constam dos autos evidências de que eventuais procedimentos reconhecidos como boas práticas em gestão de contratações de TI são internamente disseminados e praticados na instituição. Por essas razões, entende-se que o achado e a respectiva proposta de encaminhamento devem ser mantidos.

Quanto à inconsistência lançada pela equipe da Secex-PR relativa a esse achado (peça 17, p. 14), verificou-se que houve um equívoco, pois o procedimento correto seria lançar a inconsistência relativa à seção 5.9 do questionário do perfil GovTI 2012, ao invés da seção 5.8, que trata do processo de planejamento das contratações de TI, de modo que se propõe o ajuste conforme explicitado a seguir:

Seção	Resposta apresentada no Perfil GovTI 2012	Situação encontrada
5.9	As diretrizes legais são observadas e os procedimentos reconhecidos como boas práticas são disseminados internamente e praticados.	Inexistência de processo de gestão de contratação de soluções de TI formalmente instituído. Ausência de evidências que indiquem que boas práticas no tema são internamente disseminadas e praticadas na entidade (Achado 9).

De modo geral, com as ressalvas explicitadas ao longo deste parecer, as propostas de encaminhamento da equipe Secex-PR seguiram as orientações da coordenação da FOC. Entretanto, no que diz respeito às propostas de determinação efetuadas (peça 17, p. 14, item 'a' da seção '9. Encaminhamento'), entende-se que o prazo de noventa dias pode ser insuficiente para que a entidade cumpra todas as determinações propostas. Diante disso, sugere-se que a própria universidade informe, no plano de ação que deverá encaminhar a este Tribunal, o prazo necessário para adotar cada uma das medidas necessárias ao atendimento do acórdão que será prolatado.

As demais propostas de encaminhamento da equipe de auditoria não afetam o prosseguimento da FOC (peça 17, p. 15, itens 'c' e 'd'), pois se tratam de formalismos adotados pela própria Secex-PR quanto a tratativas pós-auditoria. Contudo, identificaram-se alguns pontos de melhoria e aperfeiçoamento relativos à sua proposta de monitoramento (peça 17, p. 15, item 'c').

Inicialmente, entende-se que a proposta registrada não está aderente à Portaria Segecex 27, de 19/10/2009, que aprovou os Padrões de Monitoramento do TCU, pois essa proposta prevê apenas o monitoramento das determinações que venham a ser proferidas, contrariando o §1º do art. 2º da referida norma, *in verbis*:

Art. 2º Denomina-se monitoramento a ação de verificação do cumprimento de determinações e recomendações expedidas pelo Tribunal e dos resultados delas advindos.

§ 1º Serão monitoráveis as determinações de adoção de providências corretivas previstas no inciso II do Art. 250 do Regimento Interno e as recomendações de implementação de providências de que trata o inciso III do mesmo artigo. (grifos nossos)

Também nesse sentido, esta Corte tem firmado entendimento de que recomendações também devem ser monitoradas, conforme Voto do Ex.mo. Ministro-Substituto Augusto Sherman Cavalcanti, proferido no Acórdão 73/2014-TCU- Plenário:

A recomendação emanada do Tribunal de Contas da União não representa mera sugestão, cuja implementação é deixada ao alvedrio do gestor destinatário da medida, pois tem como objetivo buscar o aprimoramento da gestão pública. Contudo, admite-se certa flexibilidade na sua implementação. Pode o administrador público atendê-la por meios diferentes daqueles recomendados, desde que demonstre o atingimento dos mesmos objetivos, ou, até mesmo, deixar de cumpri-la em razão de circunstâncias específicas devidamente motivadas. A regra, entretanto, é a implementação da recomendação, razão por que deve ser monitorada. (grifo nosso)

Por fim, convém fixar um prazo para a remessa do plano de ação da entidade que explicite as medidas a serem tomadas para fins de cumprimento das deliberações e/ou para solucionar os problemas apontados. Essa medida é prevista no parágrafo 4.2 dos Padrões de Monitoramento do TCU. Ademais, conforme previsto no parágrafo 5 do referido documento, o plano de ação deve conter, no mínimo, por deliberação: as ações a serem tomadas; os responsáveis pelas ações; e os prazos para implementação.

Assim sendo, sugere-se que o item 'c' da seção '9. Encaminhamento' seja substituído pelas seguintes propostas:

'**Determinar**, com fulcro no art. 43, inciso I, da Lei 8.443/1992 c/c o art. 250, inciso II, do Regimento interno do TCU, à Universidade Federal do Paraná que, no prazo de sessenta dias a contar da ciência do acórdão que vier a ser proferido, encaminhe a esta Corte de Contas plano de ação contemplando cronograma para a implementação das determinações e recomendações proferidas no *decisum*, contendo:

a unidade responsável pelo desenvolvimento das ações, para cada determinação em que foi fixado prazo específico por este Tribunal;

o prazo e a unidade responsável pelo desenvolvimento das ações, para cada recomendação cuja implementação seja considerada conveniente e oportuna;

justificativa da decisão e medidas alternativas que serão adotadas, para cada recomendação cuja implementação não seja considerada conveniente ou oportuna.

Determinar à Secex-PR a realização de monitoramento referente ao cumprimento das determinações e recomendações expedidas neste Acórdão'.

CONCLUSÃO

Por todo o exposto, considera-se que as sugestões e propostas destacadas ao longo deste parecer devem ser implementadas para que haja, de fato, harmonização de entendimentos e uniformidade dos encaminhamentos propostos pela Secex-PR com os padrões definidos no âmbito da primeira fase da FOC na área de governança de TI com foco na avaliação da entrega de resultados e na gestão de riscos.

PROPOSTA DE ENCAMINHAMENTO

Propõe-se que o Relator considere, em suas razões de decidir:

desconsiderar o Achado 1 do relatório de auditoria, tendo em vista o acatamento dos esclarecimentos dos gestores quanto a esse ponto, o que o descaracteriza;

rejeitar as justificativas dos gestores para o Achado 2 do relatório de auditoria, tendo em vista que o plano de desenvolvimento institucional não se confunde com o processo de planejamento estratégico institucional;

considerar o Achado 2 do relatório de auditoria como parte do capítulo 'Estratégias e Planos', pois esse achado faz parte da questão 4 de auditoria ('As estratégias e planos

corporativos e de TI foram definidos e implementados adequadamente no âmbito da Instituição?');

substituir a proposta de encaminhamento 'b3' da seção '9. Encaminhamento' (peça 17, p. 15) pela seguinte proposta: '**Recomendar** à Universidade Tecnológica Federal do Paraná que, em consonância com o disposto no item 9.1.1 do Acórdão 2.308/2010-TCU-Plenário e com base nas boas práticas abaixo, contidas na seção 3.3 da ABNT NBR ISO/IEC 38500:2009, estabeleça formalmente: indicadores de desempenho para os objetivos de gestão definidos; mecanismos para que a alta administração acompanhe o desempenho da TI da instituição; mecanismos de gestão dos riscos relacionados aos objetivos de gestão e de uso corporativos de TI.'.

rejeitar as justificativas dos gestores para o Achado 5, pois o item 9.1 da minuta do Plano Diretor de Tecnologia da Informação da entidade apresenta apenas eventos realizados antes da elaboração da minuta do referido plano, além de não conter os elementos necessários para se caracterizar um plano de capacitação de TI;

substituir a proposta 'a4' da seção '9. Encaminhamento' (peça 17, p. 14) pela seguinte proposta: '**Recomendar** à UTFPR 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 implemente a business continuity response* (Desenvolver e implementar resposta à continuidade do negócio – tradução livre)'.

considerar como inconsistências de respostas ao questionário do perfil GovTI 2012 o quadro a seguir:

Seção	Resposta apresentada no Perfil GovTI 2012	Situação encontrada
2.1	O processo de planejamento estratégico institucional formal é aperfeiçoado continuamente com base na análise de seus indicadores.	Inexistência de processo de planejamento estratégico institucional (Achado 2).
1.3	Estabeleceu os mecanismos de controle do cumprimento das metas de gestão.	Inexistência de mecanismos que permitam supervisionar a progressão e o cumprimento das metas de TI, tais como reuniões periódicas de acompanhamento ou relatórios contendo essas informações (Achado 3).
2.3	A instituição aprovou e publicou PDTI interna ou externamente.	Inexistência de PDTI aprovado pela alta administração (Achado 4, situação 1).
4.4	A instituição elabora e executa um plano de capacitação para atender às necessidades de capacitação em gestão de TI.	Inexistência de plano de capacitação para atneder às necessidades em gestão de TI (Achado 5).
5.1	Implementou os processos de gestão da continuidade dos serviços de TI.	Inexistência de um processo de gestão da continuidade dos serviços de TI formalmente aprovado e publicado (Achado 6, situação 1).
5.3	Implementou formalmente processo de análise dos riscos aos quais a informação crítica para o negócio está submetida.	Inexistência de processo de análise dos riscos (Achado 6, situação 2).
5.3	Designou formalmente pessoas ou unidade para gerenciar a segurança da informação e comunicações.	Ausência de designação formal de gestor de segurança da informação (Achado 8).
5.9	As diretrizes legais são observadas e os procedimentos reconhecidos como boas práticas são disseminados internamente e praticados.	Inexistência de processo de gestão de contratação de soluções de TI formalmente instituído. Ausência de evidências que indiquem que boas práticas no tema são internamente disseminadas e praticadas na entidade (Achado 9).

acrescentar as seguintes propostas:

determinar à Universidade Federal Tecnológica do Paraná que, em atenção ao art. 6º, inciso I, do Decreto-Lei 200/1967, estabeleça processo de planejamento estratégico institucional

que contemple, pelo menos, as práticas descritas nos itens 9.1.1.1 a 9.1.1.6 do Acórdão 1.233/2012-TCU-**Plenário**;

recomendar à UTFPR 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';

determinar, com fulcro no art. 43, inciso I, da Lei 8.443/1992 c/c o art. 250, inciso II, do Regimento interno do TCU, à Universidade Federal Tecnológica do Paraná que, no prazo de sessenta dias a contar da ciência do acórdão que vier a ser proferido, encaminhe a esta Corte de Contas plano de ação contemplando cronograma para a implementação das determinações e recomendações proferidas no *decisum*, contendo:

a unidade responsável pelo desenvolvimento das ações, para cada determinação em que foi fixado prazo específico por este Tribunal;

o prazo e a unidade responsável pelo desenvolvimento das ações, para cada recomendação cuja implementação seja considerada conveniente e oportuna;

justificativa da decisão e medidas alternativas que serão adotadas, para cada recomendação cuja implementação não seja considerada conveniente ou oportuna.

determinar à Secex-PR a realização de monitoramento referente ao cumprimento das determinações e recomendações expedidas neste Acórdão."

6. O Secretário da Sefti reencaminhou os autos a este Relator, manifestando sua concordância com a proposta formulada pelo auditor, ressaltando que (peça 24):

"a manifestação da Sefti nestes autos deu-se em prol da harmonização das propostas da Fiscalização de Orientação Centralizada, a pedido do Relator. Louve-se o trabalho desenvolvido pela Secex-PR, que, assim como as demais unidades técnicas participantes da FOC, conduziu a auditoria com profissionalismo e zelo."

É o relatório.

Voto

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).

7. O objetivo dos trabalhos foi avaliar a implementação dos controles informados em resposta ao levantamento do perfil de governança de TI de 2012, bem como verificar a adoção de planos e estratégias para implementação e melhoria da governança e da gestão de TI na Universidade Tecnológica Federal do Paraná (UTFPR).

8. Para responder às questões de auditoria formuladas com o fito de aferir a aderência do órgão às melhores práticas de governança e de gestão de TI, a equipe de auditoria avaliou aspectos relacionados à governança corporativa, governança de TI, estratégias e planos de TI, gestão de pessoal e processos de TI.

9. 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.

10. 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):

> "23. 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.
>
> 24. 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.
>
> 25. 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.
>
> 26. 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.
>
> 27. 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.
>
> 28. 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

11. Realizados os exames e ouvidos os servidores e administradores vinculados aos achados, a equipe de auditoria produziu nova versão do relatório de auditoria, no qual incorporou diversos ajustes sugeridos pela Sefti, relacionados à padronização de nomenclatura e à organização de achados, e acatou os comentários apresentados pelos gestores, descaracterizando três dos nove achados de auditoria.

12. Acerca da **governança corporativa**, foram apontados, inicialmente, dois achados, a saber: inexistência de comitê de direção estratégica para apoio em áreas de competência da alta administração e falhas no planejamento estratégico institucional.

13. Quanto ao primeiro achado, a equipe de auditoria acatou as justificativas apresentadas pela entidade argumentando que, embora a instituição não possua um comitê de direção estratégica, dispõe de outra forma de tomada de decisão cumprindo a função do comitê. A Sefti concordou com essa análise e sugeriu a supressão do achado.

14. De fato, a UTFPR confirmou que não possui comitê de direção estratégica. Contudo, informou que as decisões e o estabelecimento de diretrizes estratégicas e as políticas de acompanhamento da gestão institucional são exercidas pela reitoria e pelas respectivas assessorias de desenvolvimento institucional e de desenvolvimento acadêmico, motivo pelo qual assinto às análises empreendidas pela Secex-PR e pela Sefti.

15. O achado relativo a falhas no planejamento estratégico institucional será tratado no item "estratégias e planos" por estar a ele associado, conforme acertada observação da Sefti.

16. No que diz respeito à **governança de TI**, foram identificadas falhas nos mecanismos para dirigir e avaliar a gestão e o uso corporativos de TI. A equipe de auditoria concluiu que os esclarecimentos oferecidos pela entidade não foram capazes de afastar as falhas apontadas. A Sefti aduziu que, embora a instituição tenha definido metas para cada objetivo estratégico de TI, não foram estabelecidos indicadores para avaliar o alcance desses objetivos, tampouco mecanismos que permitam acompanhar a evolução e o cumprimento das metas de TI.

17. No que tange ao item **'estratégias e planos'**, foram verificadas falhas no planejamento estratégico institucional, bem como falhas no planejamento de TI.

18. A equipe de auditoria concluiu que os esclarecimentos apresentados pela universidade quanto às falhas no planejamento estratégico institucional podem ser aceitas, dado que a instituição segue a estruturação estabelecida no art. 16 do Decreto 5.773/2006 para a elaboração do plano de desenvolvimento institucional (PDI), embora tal artigo se restrinja a definir o que deve integrar o referido plano.

19. No entanto, acompanho o entendimento da Sefti, exposto nos seguintes termos (peça 23):

> "O art. 16 do Decreto 5.773/2006 estabelece os elementos que devem constar do PDI, tais como missão, objetivos e metas da instituição, projeto pedagógico, cronograma de implantação e desenvolvimento da instituição e de cada um de seus cursos, entre outro. No entanto, tal normativo não define as etapas e as atividades que compõem a elaboração desse plano, nem as pessoas (papéis) envolvidas. Nesse sentido, conclui-se que o PDI não se confunde com o processo de planejamento estratégico institucional."

20. Relativamente às falhas no planejamento de TI, a equipe de auditoria da Secex-PR e a Sefti concordam que os comentários dos gestores não foram capazes de afastar a ocorrência do achado, dado que a alta administração da entidade não apresentou documento que comprove a aprovação do plano diretor de tecnologia da informação (PDTI) da instituição.

21. No que concerne à **gestão de pessoas de TI**, foi apontado como achado de auditoria a inexistência de um plano periódico de capacitação dos servidores de TI da entidade. Contudo, a equipe da Secex-PR acatou os esclarecimentos apresentados pelos gestores da universidade concluindo que, embora o PDTI não tenha sido aprovado pela alta administração da entidade, as ações de capacitação dos servidores da área de TI estão previstas no item 9.1 do plano.

22. A Sefti discordou desse posicionamento ao analisar o item 9.1 do PDTI da entidade. Aduziu que não estão presentes no documento elementos típicos de um instrumento de planejamento das ações de capacitação, razão pela qual não deve ser considerado como plano de capacitação dos servidores de TI da entidade, entendimento ao qual me alinho.

23. No que diz respeito à **gestão de processos**, foram apontadas falhas nos processos de gestão de segurança da informação, na alocação de responsabilidades pela segurança da informação, e na

gestão das contratações de TI, bem como inexistência de política de segurança da informação e comunicações:

- processos de gestão de segurança da informação: inexistência de processo de gestão da continuidade dos serviços de TI formalmente aprovado e publicado;
- alocação de responsabilidades pela segurança da informação – inexistência de: comitê de segurança da informação (CSI), equipe de gestão de incidentes de segurança da informação, equipe de tratamento e resposta a incidentes em redes computacionais (Etir);
- gestão de contratações de TI: inexistência de processo de planejamento e contratação de bens e serviços de TI formalmente aprovado e publicado;
- inexistência de política de segurança da informação e comunicações: a entidade não dispõe de normativos internos que definam a política de segurança da informação e de controle de acesso (PCA).

III

24. Concomitantemente com o exame das questões de auditoria, verificou-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).

25. 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.

26. As principais inconsistências relatadas pela equipe de auditoria da Secex-PR, com as alterações propostas pela Sefti, estão resumidas no quadro a seguir:

Seção	Resposta apresentada no Perfil GovTI 2012	Situação encontrada
1.3. Em relação ao desempenho institucional da gestão e de uso corporativos de TI, a alta administração da instituição:	Estabeleceu os mecanismos de controle do cumprimento das metas de gestão.	Inexistência de mecanismos que permitam supervisionar a progressão e o cumprimento das metas de TI, tais como reuniões periódicas de acompanhamento ou relatórios contendo essas informações.
2.1. Em relação ao processo de planejamento estratégico institucional, marque a opção que melhor descreve a sua instituição:	O processo de planejamento estratégico institucional formal é aperfeiçoado continuamente com base na análise de seus indicadores.	Inexistência de processo de planejamento estratégico institucional.
2.3. Em relação ao PDTI (Plano Diretor de Tecnologia da Informação e Comunicação:	A instituição aprovou e publicou PDTI interna ou externamente.	Inexistência de PDTI aprovado pela alta administração.
4.4. Em relação ao plano de capacitação de pessoal para gestão de TI, assinale a opção que melhor descreve sua instituição:	A instituição elabora e executa um plano de capacitação para atender às necessidades de capacitação em gestão de TI.	Inexistência de plano de capacitação para atender às necessidades em gestão de TI.
5.1. A instituição implementou os processos de gestão de serviços de TI abaixo relacionados?	Implementou os processos de gestão da continuidade dos serviços de TI.	Inexistência de um processo de gestão da continuidade dos serviços de TI formalmente aprovado e publicado.
5.3. Em relação à gestão da segurança da informação, a instituição:	Implementou formalmente processo de análise dos riscos aos quais a informação crítica para o negócio está submetida.	Inexistência de processo de análise dos riscos.
5.3. Em relação à gestão da segurança da informação, a instituição:	Designou formalmente pessoas ou unidade para gerenciar a segurança da informação e comunicações.	Ausência de designação formal de gestor de segurança da informação.

Seção	Resposta apresentada no Perfil GovTI 2012	Situação encontrada
5.9. Em relação à fase de gestão dos contratos de TI, em qual das descrições abaixo a instituição se encaixa melhor?	As diretrizes legais são observadas e os procedimentos reconhecidos como boas práticas são disseminados internamente e praticados.	Inexistência de processo de gestão de contratação de soluções de TI formalmente instituído. Ausência de evidências que indiquem que boas práticas no tema são internamente disseminadas e praticadas na entidade.

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

IV

28. Conforme registrou a Sefti em seu parecer, a equipe de auditoria da Secex-PR consignou em seu relatório, ao final dos trabalhos de auditoria, apenas as situações que geraram achados e/ou inconsistências entre as evidências de implementação dos controles de TI e as respostas apresentadas pela instituição no levantamento do perfil de governança de TI de 2012 (GovTI2012).

29. A equipe de auditoria não firmou conclusões sobre a situação atual dos processos e práticas de governança e gestão de TI existentes na instituição, tampouco sobre situações que remetessem a boas práticas de governança e gestão da entidade. Portanto, o trabalho foi realizado, segundo o auditor da Sefti, em desacordo com as orientações difundidas durante a FOC.

Nesse contexto, e observando que o presente trabalho não produziu os resultados esperados acerca da avaliação da adoção de planos e estratégias da UTFPR para implementação e melhoria de sua governança e de sua gestão de TI, voto pela aprovação do acórdão que ora submeto à apreciação deste Colegiado.

TCU, Sala das Sessões Ministro Luciano Brandão Alves de Souza, em 30 de abril de 2014.

WEDER DE OLIVEIRA
Relator

ACÓRDÃO Nº 1113/2014 – TCU – Plenário

1. Processo TC 021.908/2013-3.
2. Grupo I – Classe V – Assunto: Relatório de Auditoria.
3. Interessados/Responsáveis: não há.
4. Entidade: Universidade Tecnológica Federal do Paraná.
5. Relator: Ministro-Substituto Weder de Oliveira.
6. Representante do Ministério Público: não atuou.
7. Unidade Técnica: Secretaria de Controle Externo no Paraná (Secex-PR).
8. Advogado constituído nos autos: não há.

9. Acórdão:

VISTOS, relatados e discutidos estes autos que tratam de auditoria realizada na Universidade Tecnológica Federal do Paraná (UTFPR) com vistas a avaliar a implementação dos controles de TI informados em resposta ao levantamento do perfil de governança de TI de 2012, bem como verificar a adoção de planos e estratégias para implementação e melhoria da governança de TI.

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

9.1. recomendar à Universidade Tecnológica Federal do Paraná que:

9.1.1. elabore e aprove formalmente a Política de Segurança da Informação e Comunicações da entidade, com fundamento no art. 5º, VII, da IN GSI/PR 1/2008, devendo contemplar, em especial, os elementos estabelecidos no item 5.3 da NC – DSIC/GSI/PR 3/IN01, de 30/6/2009, e na seção 5.1.1 da ABNT NBR ISO/IEC 27002:2005;

9.1.2. institua Comitê Gestor de Segurança da Informação e Comunicações da entidade, com fundamento nas orientações contidas no item 6.1.2 da ABNT NBR ISO/IEC 27002:2005, em atenção ao art. 5º, VI, da NC – GSI/PR 1/2008 c/c o item 5.3.7.3 da NC – DSIC/GSI/PR 3/IN01, de 30 de junho de 2009;

9.1.3. institua formalmente o plano diretor de TI da entidade (PDTI), que deve ser aprovado pelo dirigente máximo da instituição, em atenção ao art. 6º, I, do Decreto-Lei 200/1967;

9.1.4. elabore e execute processo de gestão de continuidade dos serviços de TI, com fundamento nas orientações contidas no Cobit 5, DSS04.3 – *Develop and implement a business continuity response*;

9.1.5. 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, em atenção ao disposto na seção 3.2.5 da NC – DSIC/GSI/PR 2/IN01, de 13 de outubro de 2008;

9.1.6. 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, em atenção ao disposto na NC – DSIC/GSI/PR 4/IN01, de 15 de fevereiro de 2013;

9.1.7. faça constar do plano diretor de TI, em consonância com o art. 6º, I, do Decreto-Lei 200/1967, pelo menos os seguintes elementos:

9.1.7.1. desdobramento das diretrizes estabelecidas em planos estratégicos, a exemplo do plano estratégico institucional e do plano estratégico de TI;

9.1.7.2. vinculação das ações de TI (atividades e projetos) a indicadores e metas de negócio;

9.1.7.3. vinculação das ações de TI a indicadores e metas de serviços ao cidadão;

9.1.7.4. vinculação entre as ações de TI priorizadas ao orçamento de TI;

9.1.7.5. quantitativo necessário (ideal) para a força de trabalho em TI;

9.1.8. 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:

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

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

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

9.1.9. implante formalmente processo de contratação de soluções de TI, adequando o processo definido na IN SLTI/MP 4/2010 ao contexto da entidade, em consonância com o item 9.2.9.9 do acórdão 1233/2012-TCU-Plenário;

9.1.10. estabeleça processo de planejamento estratégico institucional, com fundamento no art. 6º, I, do Decreto-Lei 200/1967, contemplando, pelo menos, as práticas descritas nos itens 9.1.1.1 a 9.1.1.6 do acórdão 1233/2012-TCU-Plenário;

9.1.11. 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;

9.2. determinar à Universidade Tecnológica Federal do Paraná 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. encerrar o processo e arquivar os autos.

10. Ata n° 14/2014 – Plenário.
11. Data da Sessão: 30/4/2014 – Ordinária.
12. Código eletrônico para localização na página do TCU na Internet: AC-1113-14/14-P.
13. Especificação do quorum:
13.1. Ministros presentes: Augusto Nardes (Presidente), Benjamin Zymler e Raimundo Carreiro.
13.2. Ministros-Substitutos convocados: Marcos Bemquerer Costa, André Luís de Carvalho e Weder de Oliveira (Relator).

(Assinado Eletronicamente)
JOÃO AUGUSTO RIBEIRO NARDES
Presidente

(Assinado Eletronicamente)
WEDER DE OLIVEIRA
Relator

Fui presente:

(Assinado Eletronicamente)
PAULO SOARES BUGARIN
Procurador-Geral