Relatório de Auditora nº. 04/2014 - AUDIN

À
Diretoria de Gestão de Tecnologia da Informação

O presente relatório visa demonstrar resultados dos exames na gestão de Tecnologia da Informação, dando-se cumprimento ao Plano Anual de Atividades de Auditoria Interna (6.12.01 – Gestão de TI), o qual foi apreciado pela Controladoria Regional da União no Estado do Paraná e aprovado pelo Conselho Universitário da UTFPR.

1) Introdução

Os exames foram realizados entre os meses de abril a agosto de 2014, em documentos e *web site* da UTFPR, por meio da expedição da Solicitação de Auditoria nº. 25/2014.

Salienta-se que os exames são complementares ao Ofício GABIR nº 188/2013, de 9 de agosto de 2013; do "Levantamento de pessoal de TI 2013", pelo TCU, de 30 de agosto de 2013; do Processo TC 021.908/2013-3, de 20 de novembro de 2013; do TC 023.414/2013-8, de 05/09/2013; bem como de auditorias da CGU-PR.

As técnicas de auditoria utilizadas foram, em especial, a análise documental, indagação oral e escrita, e correlação dos dados obtidos.

A auditoria atentou-se aos seguintes escopos:

a) Avaliação em governança de TI da UTFPR de acordo com determinações do TCU e estudos recentes da CGU;
b) Averiguação da implantação de documentos e procedimentos de planejamento da gestão de TI;
c) Realização de pesquisa acerca do perfil de recursos humanos na gestão de TI;
d) Mapeamento dos procedimentos para contratação e gestão de bens e serviços de TI;
e) Verificação das ações da DIRGTI quanto aos documentos e procedimentos em segurança da informação;
f) Averiguação da capacidade de desenvolvimento e produção de sistemas pela DIRGTI;
g) Indagação sobre questões de sustentabilidade ambiental.

2) Resultado dos exames

A inclusão do assunto de gestão de TI nas atividades da Auditoria Interna foi uma solicitação da Controladoria-Regional da União no Estado do Paraná com o propósito de o órgão de controle interno acompanhar as ações do setor responsável na implementação de políticas e procedimentos relacionados à Governança de TI. Por esta feita, houve colaboração da Diretoria de Gestão de TI da UTFPR para a efetivação das atividades de auditoria, com o fim de acompanhamento das implementações das ações da gestão de TI.

Portanto, tendo em vista as exigências do TCU e da CGU, especialmente quanto às práticas do *Cobit*, normas da ABNT e Acórdãos, a Auditoria Interna realizou um questionário, bem como mapeou as providências que já foram tomadas e as que ainda faltam implementar pela UTFPR.

2.1 Do questionário acerca da Governança de TI

Quadro 1 – Governança de TI

N.	Avaliação de governança de TI	Sim	Não	Informações adicionais, previsão de implementação ou justificativas
I DO PLANEJAMENTO DA GESTÃO DE TI				
1.	Há formalização de processo de aprimoramento contínuo da governança de TI (conforme Cobit 5, capítulo 3)?		X	
2.	Há implementação do Comitê de Tecnologia de Informação designado por meio de Portaria (conforme Cobit 5, prática de gestão APO01.01, atividades 7 e 8, em atenção à iniciativa estratégica 3.1 da Estratégia Geral de TI de 2013-2015 do SISP)?	X		
3.	Há versão atualizada do Planejamento Estratégico de TI (PETI) devidamente aprovado e publicado (contemplando as boas-práticas dos itens 9.1.2.1 a 9.1.2.6 do Acórdão TCU 1.233/2012-PL)?	X		
4.	Há versão atualizada do Plano Diretor de Tecnologia da Informação (PDTI) devidamente aprovado e publicado (em consonância com o Art. 6º, I, do Decreto-Lei 200/67 e Guia SISP de elaboração do PDTI)?	X		
5.	Há estabelecimento formal de objetivos, indicadores de desempenho para os objetivos da Gestão de TI e as respectivas metas para cada indicador?		X	
II PERFIL DOS RECURSOS HUMANOS				
6.	Há avaliação quantitativa e qualitativa de pessoal do setor de TI, de forma a delimitar as necessidades de recursos humanos necessárias para a gestão e operação das atividades de TI da Instituição (semelhante ao Cobit 5, Prática de Gestão APO07.01, atividade 1, em consonância com o item 9.2.2 do Acórdão TCU 1.233/2012-PL)?	X		Foi realizado um dimensionamento do quadro ideal de servidores ocupantes de cargos de TI, o qual encontra-se no PETI.
7.	Há formalização de um plano anual de capacitação de pessoal para prover e aprimorar o conhecimento necessário para a gestão de TI (semelhante ao Cobit 5, Prática de Gestão APO07.03, atividades 4 e 5, em consonância com o item 9.9.1 do Acórdão TCU 1.233/2012-TCU-PL)?		X	Não existe um plano formal de capacitação, porém os servidores desta DIRGTI realizam treinamentos internos e externos.
8.	Há instituição formal de equipe de tratamento e resposta a incidentes em redes computacionais (semelhante à seção 13 da ABNT NBR ISSO/IEC 27002:2005, em atenção ao Art. 5º, V, da NC – GSI/PR 1/2008 e às disposições contidas na NC-DSIC/GSI/PR 5/IN01, de 14/08/2009)?		X	A partir da aprovação da POSIC, que determina o modelo a ser usado na instituição da equipe de tratamento de incidentes de redes de computadores – ETIR, a DIRGTI solicitou emissão de portaria para designação desta equipe, via memorando nº 036/2014 de 26 de setembro de 2014.
9.	Os servidores lotados na gestão de TI da UTFPR são continuamente capacitados para planejar, gerir e controlar os serviços e as demandas relacionados à gestão de TI?	X		A gestão de TI é realizada pelas chefias formalmente designadas, que participam de capacitações de forma esporádica.
III PROCEDIMENTOS PARA CONTRATAÇÃO E GESTÃO DE BENS E SERVIÇOS DE TI				
10.	Há elaboração, publicação e constante atualização de catálogo de serviços de TI da Instituição (semelhante ao Cobit 5, Prática de Gestão APO09.02)?		X	
11.	Há formalização de acordos de nível de serviço entre o setor de TI e as áreas internas da Instituição (semelhante às orientações da seção 6.1.2 da ABNT NBR ISSO/IEC 20000-2:2008)?		X	
12.	Há implementação de processo de gestão de nível de serviço de TI, de forma a assegurar que níveis adequados de serviço sejam entregues para os clientes internos de TI, de acordo com as prioridades do negócio e dentro do orçamento estabelecido (semelhante à seção 6.1.3 da ABNT NBR ISSO/IEC 20000-2:2008)?		X	
13.	Há elaboração e execução de processo de gestão de ativos de informação da entidade (semelhante à seção 7.1 da ABNT NBR ISO/IEC 27002:2005; e Cobit 5, processo BAI09, em atenção à NC DISC/GSI/PR 10/IN01, de 30/01/12)?		X	Em fase inicial de implantação.
14.	Há implantação formal de processo de contratação de soluções de TI, adequando o processo definido na IN-SLTI/MP 4/2010 ao contexto da UTFPR, de acordo com o item 9.2.9.9 do Acórdão TCU 1.233/2012-PL?	X		Há um processo formal de contratações e será instituído um grupo de trabalho para revisar e fazer as possíveis adequações à IN 04/2010,

Quadro 1 – Governança de TI				
N.	**Avaliação de governança de TI**	**Sim**	**Não**	Informações adicionais, previsão de implementação ou justificativas
				solicitado via Memorando 038/2014 de 02 de outubro de 2014.
15.	Há implantação formal de processo de gestão de contratos de soluções de TI, adequando o processo definido na IN SLTI/MP 4/2010 ao contexto da UTFPR, em consonância ao item 9.2.9.9 do Acórdão TCU 1.233/2012-PL?	X		
IV SEGURANÇA DA INFORMAÇÃO				
16.	Há elaboração e execução de processo de gestão de continuidade dos serviços de TI (conf. Cobit 5, DSS4.3)?		X	Em fase de elaboração, foi especificado um Termo de Referência para contratação de empresa para executar este projeto, porem o Pregão 09/2014 foi cancelado, devemos reeditar no próximo ano, com valores adequados ao projeto.
17.	Há elaboração e aprovação formal de política de controle de acesso a informações e recursos de TI, de acordo com requisitos de negócio e de segurança da informação da entidade (semelhante à seção 11.1.1 da ABNT NBR ISO/IEC 27002:2005, em atenção à NC – DSIC/GSI/PR 7/IN01, de 06/05/10)?	X		http://www.utfpr.edu.br/estrutura-universitaria/diretorias-de-gestao/dirgti/documentos/REGULAMENTODEGESTEDEUTILIZ.DEREC.deTIAprovado.pdf
18.	Há implantação de programas de conscientização e treinamento em segurança da informação na Instituição (semelhante à seção 8.2.2 da ABNT NBR ISSO/IEC 27002:2005, em atenção à seção 3.2.5 da NC – DSIC/GSI/PR 2/IN01, de 13/10/08)?		X	Foi designada comissão pela Portaria 64/14 para a elaboração do programa. Em fase de aprovação.
19.	Há elaboração e implementação de processo de gestão de riscos de segurança da informação (semelhante à seção 4 da ABNT NBR ISSO/IEC 27002:2005, em atenção à NC – DSIC/GSI/PR 4/IN01, de 15/02/13)?		X	O processo de gestão de riscos integra o Plano de Continuidade de Negócios, que se encontra em elaboração.
20.	Há elaboração e aprovação formal de Política de Segurança da Informação e Comunicações da UTFPR (constando ao menos o que estabelece o item 5.3 da NC – DSIC/GSI/PR 3/IN01, de 30/06/2009, e seção 5.1.1 da ABNT NBR ISO/IEC 27002:2005, em atenção ao Art. 5º, VII, da NC – GSI/PR 1/2008)? (PPP/14, OCI, ordem 5)	X		A Politica de Segurança da Informação foi aprovada no COUNI em reunião realizada em 06/06/2014. http://www.utfpr.edu.br/estrutura-universitaria/couni/portarias/Deliberao09_2014c.POSIC.pdf
21.	Há designação formal de área ou pessoa responsável pela segurança da informação e comunicações da instituição (semelhante ao item 6.1.3 da ABNT NBR ISSO/IEC 27002:2005, em atenção ao Art. 5º, IV, da NC – GSI/PR 1/2008 c/c item 5.3.7.2 da NC – DSIC/GSI/PR 3/IN01, de 30/06/2009)?	X		O Regimento Interno da UTFPR atribui esta responsabilidade ao DEINFRA, porém agora com a aprovação da Politica de Segurança da Informação terá de ser designado um Comitê de Segurança da Informação.
22.	Há elaboração e execução de processo de gestão de incidentes de segurança da informação, bem como instituição formal de equipe específica para tratar de incidentes dessa natureza (semelhante à seção 13 da ABNT NBR ISSO/IEC 27002:2005, em atenção ao item 3.2.7 da NC-DSIC/GSI/PR 2/IN01, de 13/10/08)?	X		O processo de gestão de incidentes de segurança da informação e tratamento estão definidos na Política de Segurança da Informação, Art. 31 a 37.
23.	Há instituição de Comitê Gestor de Segurança da Informação e Comunicações da UTFPR (semelhante ao item 6.1.2 da ABNT NBR ISSO/IEC 27002:2005, em atenção ao Art. 5º, VI, da NC-GSI/PR 1/2008 c/c item 5.3.7.3 da NC DSIC/GSI/PR 3/IN01, de 30/06/2009)?		X	Em fase de aprovação.
V DA CAPACIDADE DE DESENVOLVIMENTO E PRODUÇÃO DE SISTEMAS				
24.	Os servidores lotados na gestão de TI foram capacitados para desenvolver			

Quadro 1 – Governança de TI				
N.	**Avaliação de governança de TI**	**Sim**	**Não**	Informações adicionais, previsão de implementação ou justificativas
	e aprimorar sistemas informatizados?	X		
25.	Existem indicadores de desempenho dos servidores (individual e coletivo) para o desenvolvimento e produção de sistemas?		X	
26.	Há contato com outros órgãos para troca de experiências ou transferência de tecnologias entre instituições (*softwares* livres, códigos abertos)?	X		
27.	A gestão de TI procura integrar os sistemas da Instituição para melhor eficiência das informações?	X		
28.	Há envolvimento de alunos para o desenvolvimento e produção de sistemas (ex.: bolsistas, projetos de pesquisa e extensão), como forma de fortalecimento de discussões acadêmicas?		X	
VI SUSTENTABILIDADE AMBIENTAL				
29.	A versão atualizada do Plano Estratégico de TI (PETI) vai abordar questões de sustentabilidade ambiental? Caso positivo, por favor, aponte alguns aspectos a serem inseridos. (Ref. Item 3)	X		O PETI, embora desatualizado quanto ao PDI, já aborda questões de sustentabilidade e estas deverão ser mantidas (item 6.2, Quadro 1, Dimensão universitária do PETI).
30.	A versão atualizada do Plano Diretor de Tecnologia da Informação (PDTI) vai abordar questões de sustentabilidade ambiental? Caso positivo, por favor, aponte alguns aspectos a serem inseridos. (Ref. Item 4)	X		A versão atual do PDTI e PETI já contemplam esta questão no Item 5 (alinhamento da TI com os objetivos estratégicos) e item 6.2 (dimensão universitária).
31.	A elaboração e execução de processo de gestão de ativos de informação da UTFPR vão contemplar aspectos de sustentabilidade ambiental? (Ref. Item 13)	X		Toda aquisição de equipamentos segue as orientações quanto à TI Verde exigidas pela legislação.

Fonte: Audin e DIRGTI.

2.2 Dos prazos para implementação de políticas de TI

No intuito de acompanhar as ações da Diretoria de Gestão de Tecnologia da Informação (DIRGTI) da UTFPR, foi solicitado o cronograma de execução de políticas e procedimentos de assuntos relacionados à TI da UTFPR, de acordo com o preconizado no Ofício Gabir nº 36/2014.

Data limite	Descrição da atividade
28/02/2014	**Aprovação Plano Diretor de TI** Portaria Nº 0354/2014 de 11 de março de 2014: http://www.utfpr.edu.br/estrutura-universitaria/diretorias-de-gestao/dirgti/documentos/0354.2014_Plano_Diretor_Tecnologia_Informacao_PDTI.pdf
30/04/2014	**Política de Segurança da Informação** Aprovada em 06/06/2014 pelo COUNI, deliberação 09/2014: http://www.utfpr.edu.br/estrutura-universitaria/couni/portarias/Deliberao09_2014c.POSIC.pdf
31/05/2014	**Instituição do Comitê de Segurança da Informação** Está sendo constituído: foi enviado memorando às áreas para indicação dos nomes para sua composição.
30/06/2014	**Programa de conscientização e treinamento em segurança da informação** Foi designado grupo de trabalho por meio da Portaria 647/2014 e 1174/2014 (prorrogação de prazo) para tratar do assunto. Trabalho em andamento. Previsão de término: 10/10/2014 http://www.utfpr.edu.br/estrutura-universitaria/diretorias-de-gestao/diretoria-de-gestao-de-pessoas/portarias-do-reitor/portarias-2014/portaria-1174_2014-prorroga-a-vigencia-da-portaria-ndeg-647-de-14-04-2014-seguranca-da-informacao/view
31/08/2014	**Implementação do processo de contratação de soluções de TI** Em estudo
30/06/2015	**Plano de Gestão de Continuidade do Negócio** Em estudo
30/06/2015	**Gestão de Riscos de Segurança da Informação** Em estudo

31/08/2015	**Alteração do Plano Diretor de TI**, conforme recomendado no item 9, alínea b2 do Relatório de Fiscalização, estabelecendo-se indicadores de desempenho para os objetivos de gestão e de uso corporativo de TI. Esta ação não foi iniciada.

Fonte: DIRGTI

3) Recomendações

Diante dos resultados decorrentes dos exames de auditoria, e a critério da autoridade administrativa, colacionamos as seguintes recomendações à DIRGTI, com a participação das COGETIs, quando possível:

a) Que avaliem a possibilidade em estabelecer formalmente um processo de aprimoramento contínuo da governança de TI, similar ao que consta no guia Cobit 5, capítulo 3;
b) Que avaliem a possibilidade de formalizar plano anual de capacitação de pessoal, com o propósito de prover e aprimorar o conhecimento necessário para a gestão de TI;
c) Que elaborem, publiquem e mantenham atualizado o catálogo de serviços de TI da Instituição;
d) Que realizem a formalização de acordos de nível de serviço entre o setor de TI e as áreas internas da Instituição;
e) Que implementem processo de gestão de nível de serviço de TI, visando assegurar que níveis adequados de serviço sejam entregues para clientes internos de TI, conforme as prioridades do negócio e dentro do orçamento estabelecido;
f) Que elaborem e executem processo de gestão de ativos de informação da entidade;
g) Que o processo de contratação de Soluções de Tecnologia da Informação seja adaptado e atenda os requisitos da IN SLTI nº 04, de 11 de setembro de 2014 (vigência a partir de 02.01.2015);
h) Que elaborem e executem o processo de gestão de continuidade dos serviços de TI;
i) Que implantem programas de conscientização e treinamento em segurança da informação, na Instituição;
j) Que elaborem e implantem o processo de gestão de riscos de segurança da informação;
k) Que instituam o Comitê Gestor de Segurança da Informação e Comunicações;
l) Que avaliem a possibilidade de elaboração de indicadores de desempenho dos servidores (individual e coletivo) para o desenvolvimento e produção de sistemas;
m) Que avaliem a possibilidade de cooperação entre o meio acadêmico para com o desenvolvimento e produção de sistemas, especialmente por meio de bolsistas;
n) Que atualizem o Plano Estratégico de TI (PETI), a fim de alinhá-lo ao PDI, recentemente aprovado.

4) Conclusão

Considerando a importância da boa Governança de TI desta Instituição, constatou-se a necessidade de acompanhamento, implementação e fortalecimento de políticas e procedimentos que garantam o melhor funcionamento de sistemas e recursos de TI, a segurança das informações, e a boa prestação de serviços e aquisições de bens de TI. Salientam-se os avanços ocorridos no âmbito da DIRGTI e os esforços para o atendimento das demandas dos órgãos de controle, contudo as recomendações prolatadas no presente relatório, além de serem inseridas no Plano de Providências Permanentes (PPP), também visam estabelecer prazos e acompanhamentos para suas implementações, conforme determinações do TCU, bem como recomendações da CGU e Auditoria Interna.

Curitiba, 12 de novembro de 2014.

Tiago Hideki Niwa
Auditor

De acordo

Sadi Daronch
Chefe da Auditoria Interna