TRIBUNAL DE CONTAS DA UNIÃO

Sumários Executivos

Levantamentos de informações para estruturação da Sefti

República Federativa do Brasil

Tribunal de Contas da União

Ministros

Ubiratan Aguiar, Presidente
Benjamin Zymler, Vice-Presidente
Valmir Campelo
Walton Alencar Rodrigues
Augusto Nardes
Aroldo Cedraz
Raimundo Carreiro
José Jorge
José Múcio

Auditores

Augusto Sherman Cavalcanti
Marcos Bemquerer Costa
André Luís de Carvalho
Weder de Oliveira

Ministério Público

Lucas Rocha Furtado, Procurador-Geral
Paulo Soares Bugarin, Subprocurador-Geral
Maria Alzira Ferreira, Subprocuradora-Geral
Marinus Eduardo de Vries Marsico, Procurador
Cristina Machado da Costa e Silva, Procuradora
Júlio Marcelo de Oliveira, Procurador
Sérgio Ricardo Costa Caribé, Procurador

Negócio

Controle Externo da Administração Pública
e da gestão dos recursos públicos federais

Missão

Assegurar a efetiva e regular gestão dos
recursos públicos em benefício da sociedade

Visão

Ser instituição de excelência no controle e contribuir
para o aperfeiçoamento da Administração Pública

TRIBUNAL DE CONTAS DA UNIÃO

Sumários Executivos

Levantamentos de informações para estruturação da Sefti

Relatores
Ministro Benjamin Zymler
Ministro Guilherme Palmeira

Brasília, 2009

<www.tcu.gov.br>

Para leitura completa dos Relatórios, dos Votos e dos Acórdãos
acesse a página do TCU na
Internet, no seguinte endereço:

<www.tcu.gov.br/fiscalizacaoti>

Brasil. Tribunal de Contas da União.
Levantamentos de informações para estruturação da Sefti / Relatores Benjamin Zymler, Guilherme Palmeira – Brasília : TCU, 2009.
37 p. – (Sumários Executivos)

1.Tecnologia da informação. 2. Governança. 3. Auditoria. I. Secretaria de Fiscalização de Tecnologia da Informação (Sefti). II. Título.

Catalogação na fonte: Biblioteca Ministro Ruben Rosa

SUMÁRIO

APRESENTAÇÃO

Os sumários executivos da Secretaria de Fiscalização de Tecnologia da Informação (Sefti), editados pelo Tribunal de Contas da União, têm por objetivo divulgar os principais resultados dos trabalhos realizados pela Sefti. As publicações contêm, de forma resumida, aspectos importantes verificados durante auditorias e levantamentos, recomendações e determinações para melhorar a governança de tecnologia da informação na Administração Pública Federal, e boas práticas identificadas.

O foco das fiscalizações de Tecnologia da Informação (TI) realizadas pela Sefti é a verificação da conformidade e do desempenho das ações governamentais nessa área, a partir de análises sistemáticas de informações sobre aspectos de governança, segurança e aquisições de bens e serviços de TI, utilizando critérios fundamentados. O principal objetivo dessas fiscalizações é contribuir para o aperfeiçoamento da gestão pública, para assegurar que a tecnologia da informação agregue valor ao negócio da Administração Pública Federal em benefício da sociedade.

Pretende-se, com a divulgação desses trabalhos, oferecer aos parlamentares, à mídia, aos órgãos governamentais, à sociedade civil e às organizações não-governamentais informações suficientes e fidedignas para que possam exercer o controle das ações de governo.

Este número, em especial, traz os principais resultados dos quatro levantamentos de informações realizados por equipes da Sefti: referencial estratégico e possíveis formas de atuação da Sefti; legislação, jurisprudência, normas e estudos na área de TI; gastos e referência de preços em TI; e governança de TI na Administração Pública Federal. Os processos relacionados com tais levantamentos foram apreciados de agosto de 2007 a agosto de 2008, sob a relatoria dos Ministros Benjamin Zymler e Guilherme Palmeira.

Ubiratan Aguiar
Ministro-Presidente

RESUMO

A dimensão estratégica da tecnologia da informação (TI), a complexidade de sua gestão, o aumento dos gastos públicos com TI na administração pública e a quantidade crescente de denúncias e representações sobre aquisições nessa área levaram, no final de 2006, à criação da Secretaria de Fiscalização de TI (Sefti). A Sefti tem por finalidade fiscalizar a gestão e o uso de recursos de TI pela Administração Pública Federal (APF) e induzir melhorias na governança de TI e, consequentemente, sua modernização e aperfeiçoamento.

Para que seja possível alcançar, com efetividade, tal finalidade, essa secretaria especializada concluiu que, em seu processo de estruturação, haveria necessidade de levantar informações para criação do seu referencial estratégico, identificar formas de atuação de outras entidades fiscalizadoras de TI, sistematizar legislação, jurisprudência, padrões, estudos e pesquisas na área de TI, e conhecer a situação da TI na APF, para melhor direcionar suas atividades de fiscalização. O presente trabalho resume os resultados alcançados por quatro levantamentos, realizados por meio de pesquisa e análise documental, entrevistas e questionários autoaplicáveis. Devido à natureza do instrumento de fiscalização levantamento, não há registro de volume de recursos fiscalizados nos quatro levantamentos aqui resumidos.

Em essência, a forma com que a Sefti atua está bem alinhada com a forma de atuação das outras entidades de fiscalização pesquisadas. Com a incorporação em sua rotina das boas práticas identificadas no levantamento para a construção do seu referencial estratégico, a Sefti tem como metas aumentar a eficiência e a eficácia de suas auditorias, tornar-se unidade de referência em fiscalização de tecnologia da informação e disseminar métodos e técnicas para outras equipes de auditoria da Administração Pública Federal.

Os produtos gerados pelo levantamento sobre normas, por sua vez, foram: base de referências sobre tecnologia da informação (nos assuntos selecionados), base de colaboradores externos, plano de atualização per-

manente da base de dados obtida e insumos para a fiscalização de tema de maior significância - terceirização em TI (TMS 2007).

Em relação ao levantamento sobre gastos em TI na APF, pode-se dizer que os dados coletados irão auxiliar no direcionamento das ações de controle do TCU nessa área. Registre-se, também, como fruto desse levantamento, o aprimoramento da gestão dos recursos destinados à TI, uma vez que se identificaram boas práticas utilizadas por gestores da área que poderão ser estendidas a toda APF.

Por fim, a partir dos dados coletados no levantamento sobre governança de TI, observou-se que a área mais crítica na Administração Pública Federal é o tratamento da segurança da informação. Conclui-se que essa é uma área em que o TCU pode, e deve, atuar como indutor do processo de aperfeiçoamento da governança de TI.

Assim, existe um campo vasto para atuação deste Tribunal na área de governança de TI na Administração Pública Federal. Se essa atuação for realizada de forma consistente e constante, os resultados serão promissores tendo em vista que poderá haver melhoria generalizada em todos os aspectos da governança de TI. Esse fato repercutirá na gestão pública como um todo e trará benefícios para o País e os cidadãos.

INTRODUÇÃO

A Secretaria de Fiscalização de Tecnologia da Informação (Sefti), criada em agosto de 2006, pela Resolução n.º 193/2006, tem como finalidade fiscalizar a gestão e o uso de recursos de Tecnologia da Informação (TI) pela Administração Pública Federal (APF). Para que seja possível alcançar, com efetividade, tal finalidade, essa secretaria especializada concluiu que, em seu processo de estruturação, haveria necessidade de levantar informações para criação do seu referencial estratégico, identificar formas de atuação de outras entidades fiscalizadoras de TI, sistematizar legislação, jurisprudência, acórdãos, normas, padrões, estudos e pesquisas na área

de TI, e conhecer a situação da TI na APF, para melhor direcionar suas atividades de fiscalização.

O presente trabalho originou-se, então, de determinação do Ex.mo Sr. Ministro Presidente Walton Alencar Rodrigues à Secretaria Geral de Controle Externo (Segecex), para que a Sefti priorizasse, no primeiro semestre do ano de 2007, a realização de quatro levantamentos para a construção do seu referencial estratégico. Essa determinação foi comunicada durante a Sessão Plenária de 7 de fevereiro de 2007.

OBJETIVOS DOS LEVANTAMENTOS

No levantamento de auditoria para criação do referencial estratégico da Sefti e identificação de formas de atuação de entidades fiscalizadoras de TI, foram definidas questões de auditoria que tivessem como resposta informações para criação de base de dados sobre fiscalização de TI, possíveis formas de atuação da Sefti, plano de divulgação de suas atividades, consolidação do conteúdo e da estrutura de sua página na *intranet*, plano de desenvolvimento profissional para seus servidores, plano interno e externo de ação conjunta, conteúdo programático para concursos específicos para a Sefti, modelos de instrução, relatório e controle de qualidade, lista de ferramentas e de critérios aplicáveis a fiscalizações de TI.

No levantamento de normas na área de TI, por sua vez, o objetivo foi obter e sistematizar informações sobre legislação, jurisprudência, acórdãos, normas, padrões, estudos e pesquisas em quatro áreas: contratação de serviços de TI, gestão da segurança da informação, política nacional de informática e governo eletrônico.

Dois levantamentos trataram sobre a situação da TI na APF: um sobre gastos e outro sobre governança de TI. O levantamento sobre gastos teve como objetivo mensurar o total de recursos gastos em TI pela Administração Pública Federal nos últimos cinco anos. Tal levantamento detalhou de que forma esses recursos são aplicados com intuito de municiar a Secretaria de

dados representativos que orientem suas ações. Fizeram parte do escopo desse trabalho questões relacionadas à execução desses gastos, como por exemplo, análise do processo de formação de preço para contratações, fontes de informação para estimativa de preços e identificação de mecanismos de gestão do orçamento de TI.

Já o levantamento sobre governança de TI, teve como objetivo principal obter informações para elaboração de mapa com a situação da governança de TI na Administração Pública Federal. Em paralelo, foram identificados os principais sistemas e bases de dados da Administração Pública Federal.

POR QUE FORAM REALIZADOS

Devido à complexidade e dimensão estratégica do tema Tecnologia da Informação, à difusão do uso da TI e ao aumento dos gastos públicos com TI na Administração Pública Federal, foi oportuna a criação da Sefti pelo Tribunal de Contas da União (TCU). Para identificar bem o quê e como fiscalizar, com o objetivo de aumentar a eficiência e a eficácia de suas ações, a Secretaria necessitava obter informações acerca da situação da gestão e do uso de TI na APF. O conhecimento de boas práticas de fiscalização, utilizadas por seus pares internos e externos, também foi considerado fundamental para a formulação do referencial estratégico da Secretaria.

Assim, definiu-se que a obtenção dessas informações dar-se-ia por intermédio de levantamentos de auditoria, como os aqui resumidos. As informações desses levantamentos serão utilizadas na elaboração de indicadores da Secretaria, na definição do seu referencial estratégico, na identificação, mapeamento e modelagem dos seus processos de trabalho, e na sistematização de normas na área de TI, com vistas a dar a segurança necessária à atuação da nova Secretaria, em especial quanto ao efeito multiplicador de seus entendimentos.

A consolidação das informações coletadas nos levantamentos sobre governança e gastos em TI pela Administração Pública Federal, estimados

em seis bilhões de reais por ano, possibilitará também a construção de diagnóstico preliminar da situação de TI na APF. Tal diagnóstico subsidiará a identificação de instituições governamentais e sistemas informatizados prioritários para fiscalização por equipes de servidores da Sefti e de outras unidades técnicas do Tribunal. Com essa gama de informações será possível verificar onde a situação da governança de TI está mais crítica e identificar as áreas em que o TCU pode, e deve, atuar como indutor do processo de aperfeiçoamento da governança de TI.

COMO SE DESENVOLVERAM OS TRABALHOS

No levantamento de auditoria para criação do referencial estratégico da Sefti e identificação de formas de atuação de entidades fiscalizadoras de TI, foram entrevistados representantes de 24 entidades externas e 46 unidades técnicas do TCU, e enviados questionários a 25 entidades internacionais de fiscalização superior e 13 Tribunais de Contas Estaduais e Municipais.

Nas entrevistas e reuniões, as informações levantadas foram registradas em formulários preenchidos pelos membros da equipe de auditoria. Foram, ainda, encaminhados questionários a serem preenchidos pelos próprios pesquisados e solicitadas informações complementares por meio de ofícios de requisição.

O levantamento sobre normas, por sua vez, foi realizado em três etapas: pesquisa efetuada pela equipe para identificação e coleta de normas, jurisprudência e estudos de interesse; complementação da base obtida na primeira etapa com dados fornecidos por órgãos normativos das quatro áreas de conhecimento escolhidas (contratação de serviços de TI, gestão da segurança da informação, política nacional de informática e governo eletrônico); e classificação e sistematização dos documentos relativos aos assuntos contratação de serviços de TI e segurança da informação.

Foram identificados e visitados quatro entes normativos: Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional (GSI); Secretaria de Política de Informática do Ministério

da Ciência e Tecnologia (MCT); Secretaria de Tecnologia Industrial do Ministério do Desenvolvimento, Indústria e Comércio Exterior (MDIC); e Secretaria de Logística e Tecnologia da Informação do Ministério do Planejamento, Orçamento e Gestão (MP).

No levantamento sobre gastos de TI pela APF, foi analisado o Orçamento Geral da União, em conjunto com as leis orçamentárias, sobre previsão e execução do orçamento de TI. Foram identificados quais entes da Administração são os principais investidores em TI, quais programas de governo demandam mais recursos de TI, o que a Administração tem adquirido em Tecnologia da Informação, quais os principais instrumentos envolvidos nesse processo, entre outras informações.

Foram entrevistados gestores públicos de cinco instituições, inclusive de empresas estatais, para se conhecer o processo de elaboração e execução do orçamento de TI em órgãos e entidades da APF. As entrevistas abordaram não só aspectos relativos ao processo de estimativa de preços para bens e serviços de TI, mas também as bases de informação utilizadas. Realizaram-se também pesquisas na Internet, exame documental de processos licitatórios do TCU e consultas no Sistema de Inteligência e Suporte ao Controle Externo (Síntese), Sistema Integrado de Administração Financeira do Governo Federal (Siafi) e Sistema Integrado de Administração de Serviços Gerais (Siasg).

Em reuniões com a equipe de auditoria, representantes do Departamento de Coordenação e Governança das Empresas Estatais (Dest), da Secretaria do Tesouro Nacional (STN), da Secretaria de Orçamento Federal (SOF) e da Secretaria de Logística e Tecnologia da Informação (SLTI) tiveram oportunidade de se manifestar acerca das limitações identificadas ao longo do estudo sobre gastos de TI. A restrita quantidade de órgãos selecionados nesse levantamento sobre gastos deveu-se à limitação de tempo e de recursos humanos para sua execução. Os critérios de seleção dos órgãos foram facilidade de acesso às informações e materialidade. Quanto às empresas públicas escolhidas, prevaleceu o critério de materialidade.

Já no levantamento sobre governança de TI, foram selecionados, como amostra, 255 órgãos/entidades representativos da Administração Pública Federal. Dessa relação, constaram os ministérios, as universidades federais, os tribunais federais, as agências reguladoras e as principais autarquias, secretarias, departamentos e empresas estatais. Os órgãos e entidades incluídos na amostra responderam ao questionário composto de 39 perguntas baseadas nas normas técnicas brasileiras sobre segurança da informação e gestão de continuidade de negócios, e no *Control Objectives for Information and related Technology 4.1* (Cobit 4.1).

RECURSOS FEDERAIS ALOCADOS

Devido à natureza do instrumento de fiscalização levantamento, não há registro de volume de recursos fiscalizados nos quatro levantamentos aqui resumidos. Todavia, considerando que o total dos gastos em bens e serviços de TI na Administração Pública Federal no exercício de 2006 superou R$ 6 bilhões, os levantamentos sobre gastos e governança de TI assumem relevância ao trazer o mapeamento das despesas e das fragilidades gerenciais na área de TI de entes da APF como fonte de informação estratégica para que a Sefti direcione e oriente suas fiscalizações.

A inexistência, na estrutura do orçamento público federal, de elemento capaz de identificar a totalidade dos gastos de TI foi uma limitação significativa para o cálculo do montante dos gastos em TI. Por um lado, o orçamento carece de ações específicas que agreguem os gastos em tecnologia da informação despendidos em atividades de suporte a programas de diversas áreas finalísticas. Por outro, a estrutura da programação financeira não contém classificações específicas para todos os tipos de bens e serviços de TI.

PRODUTOS E RESULTADOS

Neste item, serão apresentados os produtos dos quatro levantamentos e os resultados alcançados.

Levantamento para elaboração do referencial estratégico da Sefti

As informações coletadas nesse levantamento subsidiaram a criação de base de dados sobre fiscalização de TI e a definição de outros produtos relevantes para a Secretaria, tais como possíveis formas de atuação, plano de divulgação de suas atividades, plano de desenvolvimento profissional para seus servidores, conteúdo programático para concursos específicos para a Sefti, plano interno e externo de ação conjunta, práticas, técnicas de fiscalização e modelos de controle de qualidade, e consolidação do conteúdo e da estrutura da página da Sefti no portal corporativo do TCU.

Base de dados sobre fiscalização de TI

O repositório de informações sobre áreas de atuação, normas, ferramentas, métodos e boas práticas utilizadas será a base de conhecimentos que subsidiará a Sefti em futuros trabalhos de fiscalização, na elaboração de manuais de auditoria e na tomada de decisão sobre seu referencial estratégico.

As áreas de atuação mais citadas pelos representantes das entidades fiscalizadoras entrevistadas foram segurança da informação, análise de dados, governança de TI e verificação de conformidade, enquanto as normas mais citadas foram a NBR ISO/IEC 17799[1] em fiscalizações de segurança da informação, e o *Control Objectives for Information and Related Technology*[2] (Cobit) em trabalhos sobre governança de TI.

As ferramentas mais citadas pelas mesmas entidades foram o programa *Audit Command Language*[3] (ACL) para análise de dados e ferramentas desenvolvidas pelas próprias entidades para suportar suas auditorias. Foram recebidos manuais de fiscalização de TI de algumas entidades, os quais serão analisados à época da revisão do manual de auditoria de sistemas, produzido em 1998, citado como referência por órgãos da APF, que aguardam sua atualização.

Nos entes entrevistados, à exceção da Controladoria-Geral da União (CGU) e do Departamento de Polícia Federal (DPF), não foram identificadas práticas para divulgação externa dos resultados alcançados de fiscalização de TI. Também não foram identificadas entidades que mantivessem descrições das competências profissionais de auditores de TI. Apesar disso, há preocupação com treinamento e capacitação desses profissionais. Algumas entidades possuem previsão de orçamento próprio para treinamento, e estimulam a participação em eventos e a obtenção de certificações profissionais na área de TI.

Em relação às boas práticas, destaca-se a busca das unidades de auditoria pela compreensão do negócio a ser auditado para que a área de auditoria agregue valor ao negócio da entidade. Além disso, ressaltam-se o mapeamento e a gestão de riscos de TI, a produção de *releases*[4], a aplicação de questionários de satisfação de usuários, o acompanhamento *in loco* de testes de contingência, a busca de certificações, o incentivo à pós-graduação e a realização de auditoria contínua, com o uso de rotinas automatizadas de verificação de dados que possibilitam análise concomitante das transações de negócio.

Proposta de formas de atuação da Sefti

De modo geral, os representantes das secretarias e gabinetes do TCU entrevistados não desejam que haja qualquer tipo de reserva de mercado ou regras rígidas para proposição, participação e execução de futuros trabalhos de fiscalização de TI. Entendem que a Sefti tem o objetivo de aperfeiçoar a atuação do TCU em fiscalizações de TI, além de auxiliar as demais unidades do Tribunal. As unidades entrevistadas concordam com a necessidade de especialização dos analistas para execução de trabalhos sobre TI e acreditam que serão capazes de lidar com situações menos complexas em processos e fiscalizações.

No que concerne à execução de auditorias de TI, devido à maior dificuldade de disseminar procedimentos às outras unidades, entenderam que a Sefti deve trabalhar em um modelo misto, com participação direta ou indireta da Secretaria na execução das fiscalizações, conforme o caso.

Quanto ao relacionamento da Sefti com as unidades técnicas do TCU na área de fiscalização de aquisições e contratos, aprovam a criação de filtros que evitem que a Sefti venha a tratar de assuntos não relacionados à TI. Para isso, na opinião dos entrevistados, a Secretaria deve priorizar a criação de produtos e ferramentas, além de roteiros e formulários para a elaboração de quesitos. Contudo, não devem existir regras rígidas quanto ao encaminhamento de processos, principalmente os complexos e/ou urgentes. Acreditam que essa forma de atuação permitirá o controle das demandas de análise em contratos pontuais e liberará a Sefti para a análise de questões e problemas de TI na APF mais significativos.

Por consequência, consideram prioritária a execução de ações que capacitem as secretarias, por meio de treinamentos de rápida aplicabilidade, trabalhos conjuntos de fiscalização e oferta de produtos e ferramentas desenvolvidos pela Sefti, tais como manuais e procedimentos de fiscalização de TI, base de dados para consulta/comparação de preços de produtos e serviços de TI, índice consolidado sobre jurisprudência de TI e base de dados para consulta de matrizes de planejamento, de procedimentos e de achados em fiscalizações de TI.

Quanto às áreas ou temas de fiscalização de TI, foram identificadas, junto a 43 unidades, 70 sugestões de trabalhos para a Sefti, desde auditoria em sistemas específicos de arrecadação de multas e controles de benefícios, até assuntos mais amplos, como avaliação da situação e gerenciamento da área de informática em determinados órgãos e autarquias.

Plano de divulgação permanente da Sefti

Durante o levantamento de novas formas de divulgação das atividades da Sefti, foram criados dois roteiros de divulgação, para os públicos interno e externo do TCU, com passos a serem cumpridos para encaminhamento de matérias à Assessoria de Comunicação Social (Ascom). Também, identificaram-se 20 periódicos e jornais relativos à TI, discriminados por

público-alvo, que poderão ser utilizados para divulgação externa, tais como a Revista Tema, publicada pelo Serviço Federal de Processamento de Dados (Serpro), e o periódico *Into IT – The Intosai IT Journal,* distribuído pela *International Organization of Supreme Audit Institutions* (Intosai) a mais de 300 entidades fiscalizadoras.

Foram identificados também sete eventos nacionais e internacionais nos quais as ações da Sefti podem ser divulgadas. Destacam-se, no âmbito nacional, o Congresso Nacional de Auditoria de Sistemas, Segurança da Informação e Governança (Cnasi), promovido pelo IDETI (Eventos em Tecnologia da Informação), e, na esfera internacional, o *Latin America Conference in Computer Audit, Control and Security* (Latin Cacs), promovido pela *Information Systems Audit and Control Association* (Isaca), entidade referência internacional em auditoria de sistemas.

Em reunião com representantes da Ascom, constatou-se que a Assessoria está desenvolvendo ação interna, em parceria com a Secretaria de Planejamento e Gestão (Seplan), para elaboração de um plano de comunicação para o TCU, com escopo nos públicos interno e externo. Dessa forma, entendeu-se que a Sefti deverá esperar pelo resultado dessa ação, que será referência para todas as unidades do Tribunal.

Plano de desenvolvimento profissional e proposta de seleção em concurso público específico

Em relação ao plano de desenvolvimento profissional, a equipe avaliou quais habilidades e competências são necessárias para que os servidores lotados na Sefti possam desenvolver seus trabalhos na área de fiscalização de TI. Identificaram-se certificações e cursos correlatos à área, tais como as certificações Certified Information Systems Auditor5 (Cisa), Certified Information Systems Security Professional6 (Cissp), e treinamentos sobre análise de dados com o programa ACL, Control Objectives for Information and related Technology[7] (Cobit) e Information Technology Infrastructure Library[8] (ITIL).

Entende-se que a Sefti deva atuar junto ao Instituto Serzedello Corrêa (ISC) para propor alteração da Resolução nº 165/2003, a fim de obter patrocínio do TCU para os processos de certificação profissional mais relevantes às atividades da Sefti; e elaborar guia de desenvolvimento técnico para seus servidores, com um conjunto mínimo de certificações e cursos identificados.

De forma complementar, apresentou-se proposta de conteúdo programático de futuros processos seletivos do TCU para seleção de analistas da Sefti, abrangendo desde temas genéricos de TI até itens específicos de auditoria e fiscalização de contratos de TI. Tal proposta foi utilizada pelo ISC na elaboração do edital do concurso de 2007 para Analista de Controle Externo – orientação Auditoria de Tecnologia da Informação.

Planos interno e externo de atuação conjunta

Quanto aos planos interno e externo de ação conjunta, foram identificadas três possíveis formas de parceria da Sefti com entidades externas: atuação conjunta com equipes de auditoria interna em trabalhos a serem executados na própria entidade auditada; atuação conjunta com outras entidades fiscalizadoras na realização de auditoria em uma terceira entidade; e intercâmbio de informações sobre métodos, procedimentos e técnicas de auditoria com entidades públicas e privadas. A conveniência de execução e formalização dessas parcerias deverá ser analisada, caso a caso, pela Sefti, à época da elaboração de futuras propostas de fiscalização.

Práticas, técnicas de fiscalização e modelos de controle de qualidade

Constatou-se a existência de práticas e técnicas de outras unidades do Tribunal que poderiam também ser utilizadas em fiscalizações de TI, como por exemplo, o modelo genérico da Secretaria de Fiscalização de Desestatização (Sefid), e as técnicas de auditoria de natureza operacional

desenvolvidas pela Secretaria de Fiscalização e Avaliação de Programas de Governo (Seprog). Identificaram-se, ainda, ferramentas de apoio a fiscalizações, além da legislação e normas aplicáveis, utilizadas por unidades técnicas do Tribunal e entidades externas entrevistadas, em auxílio à execução de fiscalizações de TI. Dentre as ferramentas em uso no TCU, destacam-se os programas ACL e Síntese, disponíveis aos analistas do Tribunal, e o Fiscalis Execução, em fase de implantação.

No âmbito interno, constatou-se a existência de modelos de controle de qualidade também aplicáveis a fiscalizações de TI, como o Roteiro de Garantia de Qualidade (RGQ), o *Check-list* de controle de qualidade da Sefid e os roteiros utilizados em auditorias de natureza operacional e de conformidade, que poderão subsidiar a Sefti no processo de elaboração de modelo de controle de qualidade próprio para a execução de seus trabalhos.

Junto aos entes externos entrevistados, entretanto, não foram identificados procedimentos específicos de controle de qualidade aplicados às auditorias de TI. Pelo contrário, identificou-se a utilização de controles de auditoria de caráter geral.

Consolidação do conteúdo e estrutura da página da Sefti

Quanto à consolidação de conteúdo para a página da Sefti no portal do TCU, criou-se uma proposta de organização de produtos e informações, destacando as possíveis áreas responsáveis por cada conteúdo e as limitações para a utilização do portal. Nessa proposta, a qual subsidiará a Secretaria no processo de elaboração e publicação de sua página *web*, os produtos e informações foram agrupados em "Conheça a Sefti", "Processos e relatórios", "Normas e jurisprudência", "Pesquisa de preços", "Base de informações de governança da APF", "Cursos, treinamentos, certificações e eventos recomendados para auditores de TI", "Comunicação" e "Procedimentos e manuais de fiscalização de TI".

Referencial estratégico da Sefti

Tomando como subsídios algumas das informações coletadas nesse levantamento, a Sefti, sob orientação da Seplan, definiu sua missão, negócio e visão (Quadro 1).

Quadro 1 - Referencial estratégico da Sefti	
Negócio	Controle externo da governança de tecnologia da informação na Administração Pública Federal
Missão	Assegurar que a tecnologia da informação agregue valor ao negócio da Administração Pública Federal em benefício da sociedade
Visão	Ser unidade de excelência no controle e no aperfeiçoamento da governança de tecnologia da informação

Levantamento sobre normas na área de TI

Esse levantamento de auditoria gerou, como produtos, bases de referências sobre tecnologia da informação, base de colaboradores externos, plano de atualização permanente dessas bases e ainda insumos para a fiscalização de Tema de Maior Significância (TMS) Terceirização em TI.

Bases de referências sobre tecnologia da informação

Para os assuntos de interesse (contratação de serviços de TI, gestão da segurança da informação, política de informática e governo eletrônico) foram classificados e estruturados, em CD-ROM, mais de 400 documentos de diversos tipos, desde livros e artigos científicos até acórdãos e decretos, referenciados no seu local de origem (URL[9] na Internet) por meio de *link*, quando existente.

Base de colaboradores externos

A partir da lista de interessados constante do relatório de auditoria de natureza operacional realizada pelo TCU em ações do Programa Governo

Eletrônico (Acórdão nº 1.386/2006 – TCU – Plenário) e das informações obtidas nas visitas aos quatro entes normativos e demais atividades desenvolvidas ao longo desse levantamento, foram relacionados possíveis colaboradores nos assuntos de interesse. O TCU poderá eventualmente recorrer a tais especialistas para a formação de painéis de referência no planejamento de auditorias ou para o esclarecimento de dúvidas pontuais.

Plano de atualização permanente das bases

O plano de atualização permanente das bases de referências sobre tecnologia da informação, fundado em proposta da Secretaria das Sessões (Seses), prevê estreito relacionamento entre Sefti, Seses e Secretaria de Tecnologia da Informação (Setec), também interessada no tema. A Seses forneceria à Sefti e à Setec a lista de acórdãos que tratam de assuntos na área de TI à medida que são publicados, enquanto que os especialistas da Sefti e da Setec gerariam entendimentos para acórdãos paradigmáticos na área de TI e revisariam entendimentos gerados regularmente pela Seses.

Insumos para a fiscalização de Tema de Maior Significância

Na revisão da sistematização da base de documentos sobre contratação de serviços de TI, foram identificados pontos de maior incidência de irregularidades nos processos que tramitaram pela Sefti em 2006 e 2007, o que resultou na elaboração da versão preliminar da matriz de planejamento referencial para a Fiscalização de Orientação Centralizada (FOC) para atender ao TMS "Terceirização em TI".

Levantamento sobre gastos em TI

Como produtos desse levantamento, foram identificadas fontes de informação para referência de preços em contratações de TI, além de métodos de formação de preços e de identificação dos gastos em TI. Foram ainda feitas considerações acerca da estimativa do valor das contratações e dos mecanismos

de gestão do orçamento de TI pelos órgãos/entidades da amostra, e levantadas informações quantitativas relativas ao gasto em TI de 2002 a 2006.

Fontes de informação para referência de preços em contratações de TI

Embora se tenha identificado um rol significativo de fontes de referência de preços na Internet, em geral, os portais não provêem mecanismos que sejam ao mesmo tempo eficazes e eficientes para que o gestor encontre preços praticados em contratações de produtos e serviços semelhantes aos que deseja adquirir. Entre os instrumentos para aferição de preço, sem dúvida, os mais amplos são as próprias bases de preços praticados em compras da Administração Pública.

Métodos de formação de preços em contratações de TI

Os mecanismos de composição de estimativa de preços identificados, desde cotação específica com fornecedores e avaliação de contratos recentes ou vigentes até pesquisa em bases de sistemas de compras, ofertas de registros de preço e composição de bases de preço próprias, têm aplicação combinada ou isolada, de acordo com o porte da contratação, a estrutura da organização contratante para gerir suas compras e a complexidade do objeto, dentro dos ditames da legislação vigente. Para contratações vultosas, é essencial a combinação de métodos de estimativa do valor da contratação para alcançar o real preço de mercado e promover a economicidade da aplicação dos recursos públicos.

Considerações acerca da estimativa do valor das contratações de TI

Entre as práticas identificadas para estimar valores de contratações de TI, as mais comuns são a cotação de preços com fornecedores e a consulta a contratos recentes ou vigentes no próprio órgão ou entidade. Apesar de permitir crítica prévia às especificações, a cotação de preços com fornecedores é

pouco precisa devido ao comportamento dos próprios fornecedores em relação a cotações públicas: ora não têm interesse em cotar seus produtos e serviços para essa finalidade, ora optam por apresentar valores que não comprometam antecipadamente sua real condição de participação no futuro certame.

Já na consulta a contratos vigentes ou recentes, há dificuldade em identificar objeto suficientemente semelhante para ser considerado na estimativa de preços. Isso ocorre devido à inexistência de repositório de contratações único e prático que permita consultas eficazes e eficientes a aquisições semelhantes, com base em descrições pormenorizadas das especificações de produtos já adquiridos pela Administração.

A partir dos mecanismos identificados para estimativa de preços e das falhas recorrentes expostas pelo Tribunal em seus acórdãos, percebe-se que a Administração Pública Federal carece de orientações sobre os mecanismos disponíveis para estimativa de preços. Constata-se a necessidade de aprimoramento dos sistemas de compras governamentais e mecanismos de consultas a compras realizadas no âmbito da APF, apesar de já existirem ações, por parte da SLTI/MP, para padronização de especificações técnicas de referência.

Método de identificação dos gastos em TI

O método definido para identificação dos gastos em Tecnologia da Informação no Orçamento Geral da União (OGU) consiste na soma das despesas realizadas na subfunção Tecnologia da Informação (126), gastos efetuados em subelementos específicos de TI e gastos das Estatais, identificados no Orçamento de Investimento por meio da mesma subfunção (126) e no Programa de Dispêndios Globais (PDG) por meio de rubricas próprias de TI.

Considerações acerca dos mecanismos de gestão do orçamento de TI

Embora definido o método para identificação dos gastos de TI, a estrutura do Orçamento Geral da União não permite a identificação cabal dos

gastos realizados pela Administração Pública Federal em Tecnologia da Informação por dois motivos: o OGU não contém classificações orçamentárias específicas para todos os tipos de bens e serviços ligados ao domínio da Tecnologia da Informação; e os dispêndios em TI estão dispersos, sem identificação, nas ações finalísticas e de apoio de cada órgão ou entidade.

Para permitir a identificação precisa dos gastos de TI, faz-se necessária não só a criação de ação que agregue as despesas relacionadas à Tecnologia da Informação, sob a ótica meio, como apoio ao desenvolvimento e execução de programas, a exemplo da Ação 2003 – Ações de Informática, existente em anos anteriores, mas também a criação de elemento de despesa específico para a área, capaz de abarcar todos os tipos de bens e serviços de TI. Quanto aos gastos das Estatais, constata-se a necessidade de definição de rubricas específicas para a área de Tecnologia da Informação, prezando-se pela simetria entre os Programas de Dispêndios Globais das Instituições Financeiras e do Setor Produtivo Estatal.

Ressaltada a importância do planejamento orçamentário na área de TI, há necessidade de instrumentos que permitam o controle da gestão orçamentária de TI, haja vista a insuficiência dos instrumentos existentes, tanto por parte do Governo (Siafi, Siasg e Contas Públicas), como por parte dos órgãos e entidades, que não possuem ferramentas que possibilitem a obtenção das informações acerca desse orçamento e de sua execução. As unidades de TI, por realizarem a gestão ativa dos gastos e orçamentos de TI de sua organização, parecem ser a fonte de informação mais fidedigna sobre esse assunto.

Dessa forma, o Tribunal de Contas da União deve definir mecanismos sistematizados para obter informações precisas dos gastos em TI realizados por órgãos e entidades da APF e determinar-lhes que informem, anualmente, sua previsão orçamentária discriminada para acompanhamento e apoio ao planejamento das ações de fiscalização do TCU na área de Tecnologia da Informação.

Informações quantitativas relativas ao gasto em TI de 2002 a 2006

Os gastos identificáveis em Tecnologia da Informação executados pela APF cresceram de 4,2 a 6,5 bilhões de reais, de 2002 a 2006. Tais valores restringem-se aos gastos liquidados em classificações específicas de TI no Orçamento Geral da União e no PDG, as quais não comportam todos os serviços e bens da área.

Da análise dos dados apresentados, notou-se predominância dos gastos de TI em serviços e, dentre os programas de TI identificados no Plano Plurianual 2004/2007, o programa de maior materialidade em 2006 foi o programa 0751 – Serviços de Tecnologia da Informação, com despesa total em torno de 1,3 bilhão de reais, programa exclusivo do Serpro, que abrange toda sua despesa.

Vale ressaltar que os gastos associados aos programas de TI não são exclusivamente relativos a aquisições de bens e serviços de tecnologia. Neles se inserem todos os insumos necessários à realização dos programas na área tais como diárias, passagens, material de expediente, combustível, material para manutenção e também recursos de TI, os quais não necessariamente figuram como parcela significativa dos gastos totais.

Foram verificadas ainda limitações no âmbito da programação orçamentária quanto à utilização de subelementos genéricos para classificação de despesas de TI, tais como despesas com consultorias de TI, locação de mão-de-obra, serviço de apoio administrativo, técnico e operacional, serviço de seleção e treinamento, manutenção e conservação de equipamentos, apoio administrativo e operacional. Os valores encontrados nesse grupo não são considerados no total dos gastos de TI pela inviabilidade de se isolar, de forma sistemática, gastos específicos de TI no montante dos gastos contabilizados nos subelementos.

Diante dessas restrições e do valor levantado de 710 milhões de reais, referente aos gastos de TI liquidados em 2006 em subelementos genéricos, ou seja, subelementos não específicos de TI, conclui-se que o montante dos gastos em TI supera significativamente o valor mensurado de 6,5 bilhões de reais em 2006.

Levantamento sobre governança de TI

Nesse levantamento, foram identificados os principais problemas de governança de tecnologia da informação na Administração Pública Federal nas seguintes áreas: planejamento estratégico institucional e de TI; estrutura de pessoal de TI; segurança da informação; desenvolvimento de sistemas de informação; gestão de acordos de níveis de serviço; processo de contratação de bens e serviços de TI; processo de gestão de contratos de TI; processo orçamentário de TI; e auditoria de tecnologia da informação.

Planejamento estratégico institucional e de TI

A partir dos dados coletados, pôde-se inferir que a falta de planejamento estratégico institucional inibe e/ou prejudica o planejamento das ações de TI. O estímulo à elaboração de planejamento estratégico institucional deve ser a primeira ação para a melhoria da governança de TI. O segundo passo deve ser o estímulo a que, em consonância com o planejamento estratégico institucional, seja elaborado o planejamento estratégico de TI.

O planejamento estratégico de TI é essencial para que as organizações possam identificar e alocar corretamente os recursos da área de TI de acordo com as prioridades institucionais e com os resultados esperados. O percentual de 59% dos 255 órgãos/entidades pesquisados sem planejamento estratégico de TI é preocupante porque a ausência de planejamento estratégico leva ao enfraquecimento das ações e da própria área de TI devido à descontinuidade dos projetos e consequente insatisfação dos usuários e resultados abaixo do esperado. Isso pode comprometer toda a área de

TI e influenciar negativamente o desempenho do órgão/entidade na sua missão institucional, já que a TI representa importante ferramenta para o desenvolvimento das ações previstas.

O fato de menos de um terço dos órgãos/entidades pesquisados terem um comitê diretivo de TI funcionando demonstra a pouca importância dada à participação de todos os setores da organização nas decisões estratégicas de TI. A existência do comitê diretivo de TI, aliada aos planejamentos estratégicos institucionais e de TI, constitui instrumento valioso no direcionamento dos investimentos de TI e no combate ao desperdício de recursos.

Estrutura de pessoal de TI

Quanto à estrutura de pessoal de TI, a equipe do levantamento identificou que um total de 29% dos 255 pesquisados possui menos de 1/3 de seu quadro de TI composto por servidores, o que pode acarretar risco de dependência de indivíduos sem vínculo com o órgão/entidade para a execução de atividades críticas ao negócio, além de perda do conhecimento organizacional.

Segundo as informações levantadas no questionário, somente 37% dos servidores do quadro das áreas de TI dos órgãos/entidades possuem formação específica em TI (incluindo aqui doutorado, mestrado, pós-graduação *lato sensu* e nível superior). Além disso, 43% dos órgãos/entidades possuem carreira específica para a área. Esse resultado preocupa em função do aumento da importância estratégica da TI para as organizações, que correm o risco de não terem pessoal qualificado suficiente nem para executar as atividades básicas nem para fiscalizar eventuais contratados.

De acordo com as respostas ao questionário, 60% dos pesquisados não consideram competências gerenciais, técnicas e resultados produzidos anteriormente na seleção de gerentes de TI. Com esse resultado, não se pôde verificar se a escolha de chefias no órgãos/entidades participantes é objetiva e baseada no mérito.

Segurança da informação

As respostas fornecidas pelos 255 órgãos/entidades pesquisados às questões sobre o tratamento dado à segurança das informações sob sua responsabilidade indicam que é preciso mais atenção ao tema. Dentre as nove questões sobre esse assunto, apenas uma obteve mais de 50% de resposta positiva.

A ausência de plano de continuidade de negócios (PCN) em 88% dos órgãos/entidades pesquisados aponta para a falta de cultura acerca de continuidade de negócios. Isso constitui um alto risco para a segurança das informações tratadas por essas instituições governamentais, ao deixá-las vulneráveis à perda ou ao comprometimento de informações em caso de interrupção de serviços por causas naturais ou intencionais.

A seu turno, a ausência de uma gestão de mudanças em 88% dos pesquisados declarada pelos pesquisados indica que a maior parte desses órgãos/entidades corre risco de instabilidade e falhas de segurança no tratamento das informações no seu ambiente de TI quando da ocorrência de mudanças. Além disso, há o risco de enfrentar dificuldades quando for realizar auditoria ou investigação por ocasião de problemas ocorridos em mudanças no ambiente de TI.

Sobre a gestão de capacidade e compatibilidade do ambiente de TI, vale ressaltar que sua ausência em 84% dos pesquisados expõe o risco de indisponibilidade em quantidade significativa dessas organizações da Administração Pública Federal. Além disso, é um indício de que os gerentes de TI dessas entidades não dispõem de instrumentos adequados para embasar as necessidades de investimento em infraestrutura de TI.

A classificação das informações, por sua vez, é um dos pilares da gestão da segurança da informação numa organização. A declaração de sua ausência por um percentual tão expressivo de pesquisados (80%) é indício de que o tratamento da segurança sobre as informações não é feito de forma

consistente e independente do meio que as armazenam nesses órgãos/entidades da Administração Pública Federal. Além disso, essa ausência aumenta o risco de que a proteção das informações não esteja adequada às necessidades do negócio.

A existência de área específica para gerência de incidentes não garante que um incidente não ocorra, mas promove o melhor tratamento possível aos incidentes. Assim, o fato de que 76% dos pesquisados declararam não possuir tal área acarreta risco para o negócio dessas organizações. Além disso, a ausência dessa área inviabiliza a articulação do governo para o tratamento de incidentes que envolvam vários órgãos e dificulta o trabalho de grupos de resposta a incidentes existentes. Dessa forma, essa falha pode prejudicar, inclusive, aqueles que possuem grupo constituído.

A análise de riscos de TI é outra importante ferramenta de gestão da segurança da informação. Sua ausência em 75% dos órgãos/entidades pesquisados indica falha significativa que pode resultar em desperdício, ações ineficazes e lacunas no tratamento da segurança.

Apenas 36% dos pesquisados declararam ter área específica para lidar estrategicamente com segurança da informação. A inexistência dessa área representa um risco de ausência de ações de segurança da informação ou ocorrência de ações ineficazes, descoordenadas e sem alinhamento com o negócio.

Já a política de segurança da informação (PSI) foi declarada inexistente nas organizações de 64% dos pesquisados. Como a definição dessa política é um dos primeiros passos para o reconhecimento da importância da segurança da informação na organização e seu tratamento, isso é um indício de que a gestão de segurança da informação é inexistente ou incipiente na maior parte desses órgãos/entidades da administração pública.

Finalmente, dentre os itens relacionados diretamente com a segurança da informação, a existência de procedimentos de controle de acesso apresentou o resultado mais positivo, pois 52% dos órgãos/entidades pesquisa-

dos declararam possuir tais procedimentos. Entretanto, 48% ainda é um percentual preocupante de ausência, pois a falta desses procedimentos é um indício de que, nessas organizações, o controle de acesso implementado não está adequado ao nível de proteção necessário para a informação.

Esses resultados delineiam um cenário no qual o auditor de TI tem papel fundamental no incentivo à governança da segurança de informação por meio da indicação de controles para apoiar estruturas e processos organizacionais com vistas à proteção das informações, tendo como referência modelos apropriados. Para tanto, há necessidade do aperfeiçoamento constante das competências do auditor de TI nos principais modelos de gestão e controle na área de TI, tais como a *Information Technology Infrastructure Library* (ITIL) e modelos de análise de riscos.

Desenvolvimento de sistemas de informação

O uso de metodologia de desenvolvimento de sistemas é um requisito fundamental para a produção de *software* de qualidade. A sua ausência declarada por 51% dos 255 pesquisados preocupa pelo risco que representam, para a segurança da informação, produtos de *software* de baixa qualidade. Além disso, outras consequências, como maior dificuldade no gerenciamento do processo de desenvolvimento, seja ele interno ou terceirizado, representam risco de má gestão dos recursos dos órgãos/entidades da Administração Pública Federal.

Adicionalmente, há de se considerar o perfil delineado por 76% das organizações que declararam possuir sistemas transacionais via Internet. Tais sistemas apresentam um risco inerente relacionado à maior exposição a ações indevidas que podem afetar a integridade, a disponibilidade e a confidencialidade das informações por eles tratadas. Esse risco é aumentado na presença de controles fracos que afetem diretamente esses sistemas, como é o caso da ausência de metodologia para desenvolvimento de sistemas ou deficiências nos controles de segurança da informação, ambos identificados

no presente levantamento. Nesse cenário, a atuação da auditoria de TI pode colaborar diretamente por meio da recomendação de controles, inclusive aqueles específicos para sistemas transacionais via Internet. Para tanto, é imperativo que o auditor esteja familiarizado com tais tecnologias, seus riscos e as boas práticas e ferramentas que auxiliam a mitigação desses riscos.

Gestão de acordos de níveis de serviço

A gestão de acordos de níveis de serviço é o principal instrumento de negociação de qualidade de serviço entre as gerências de TI e os seus clientes. A sua ausência em 89% dos pesquisados é um indício de que as áreas de TI desses órgãos/entidades ainda estão distantes dos seus usuários e não negociam adequadamente com eles sobre a qualidade dos seus serviços. As consequências mais prováveis para tal cenário são clientes insatisfeitos e investimentos inadequados.

Processo de contratação de bens e serviços de TI

Uma quantidade expressiva (46%), pouco menos que a metade dos órgãos/entidades pesquisados, não dispõe de processo formal de trabalho. Essa é uma situação que merece atenção especial dos órgãos/entidades no sentido da implantação de processo formal de contratação de TI, para evitar falhas, fraudes e desperdícios de recursos.

A despeito das dificuldades enfrentadas, como falta de recursos humanos e outras condições fundamentais para o bom funcionamento das áreas de TI, o fato de apenas 53% do universo pesquisado realizarem análise de custo/benefício das contratações de TI demonstra que a melhor utilização dos recursos públicos ainda não é uma preocupação para boa parte dos gestores de TI.

Apesar da maioria dos órgãos/entidades pesquisados explicitarem os benefícios para a obtenção dos resultados institucionais esperados com cada contratação de TI, um percentual ainda muito expressivo não adota tal

prática (40%). Essa situação, em conjunto com os achados sobre o processo de gestão de contratos de TI, mostra que muito ainda precisa ser feito para que haja controle efetivo de que as contratações de TI são convenientes para a organização.

O fato de metade dos órgãos/entidades pesquisados não exigir o demonstrativo de formação de preço antes da adjudicação indica que uma quantidade significativa de gestores não está atenta para os problemas que poderá enfrentar na gestão dos contratos decorrentes das aquisições de bens e serviços TI. Essa visão imediatista poderá trazer riscos à conclusão do contrato e/ou prejuízos à organização.

Processo de gestão de contratos de TI

A adoção de processo formal de trabalho para gestão dos contratos de TI é uma necessidade que menos da metade (45%) das 255 organizações consultadas executa. Mesmo a maioria (90%) realizando a monitoração técnica, apenas 78% designam formalmente um gestor para cada contrato e somente 53% definem previamente os itens a serem verificados para atestar as faturas apresentadas. A monitoração administrativa é ainda realizada pela área de TI em 55% das organizações pesquisadas.

Um percentual pequeno (35%) das organizações consultadas realiza periodicamente reuniões com os contratados para avaliação da execução de cada contrato de TI. Somente 43% exigem, em contrato, que o conhecimento seja transferido pelos prestadores de serviço aos servidores do órgão/entidade.

Os órgãos/entidades da Administração Pública Federal devem ser encorajados a adotar processo formal de trabalho para gestão dos contratos de TI para minimizar os riscos de descumprimento da legislação, desperdício de recursos, interrupção de serviços de TI, baixa qualidade de serviços contratados, entre outros.

Processo orçamentário de TI

O controle sobre os gastos de TI é de suma importância para o melhor aproveitamento dos recursos disponíveis, a solicitação de recursos financeiros adequados à necessidade da área de TI e o atendimento das ações consideradas prioritárias. Esse processo de trabalho está ligado aos processos de planejamento e contratação de bens e serviços de TI.

Apesar de 82% dos órgãos/entidades pesquisados afirmarem que realizam essa atividade, foi observado que, em muitos casos, as informações sobre gastos de TI foram de difícil obtenção. Esse fato denota a necessidade de melhoria no controle de gastos de TI.

Auditoria de tecnologia da informação

Auditorias de TI ainda são pouco frequentes entre os pesquisados: apenas 40% declararam ter realizado alguma auditoria de TI nos últimos cinco anos. Mesmo entre os 101 órgãos/entidades que a realizaram, 68% executaram no máximo uma auditoria de TI por ano. Além disso, apenas 19% dos pesquisados declararam possuir equipe interna de auditoria de TI.

Tal resultado indica que a realização de auditorias de TI em bases periódicas não é uma realidade entre os pesquisados. Com isso, esses órgãos/entidades estão perdendo a oportunidade de usar essas auditorias para aperfeiçoar os seus controles internos de TI e, consequentemente, promover a melhoria da sua governança de TI.

Diante do quadro apresentado nos itens anteriores, observa-se que a situação da governança de TI na Administração Pública Federal é bastante heterogênea do ponto de vista dos seus diversos aspectos. Os aspectos que de alguma forma são regulados por leis e normas (processo orçamentário e contratação e gestão de bens e serviços de TI), somados a planejamento

estratégico, desenvolvimento de sistemas, gestão de níveis de serviço e auditoria de TI, apresentam algum desenvolvimento, apesar de estarem longe do ideal. A questão de estrutura de pessoal de TI é bastante diversa e está atrelada à natureza jurídica da organização. O aspecto em que a situação da governança de TI está mais crítica é no que diz respeito ao tratamento da segurança da informação.

Boas práticas identificadas

Durante as entrevistas com a Câmara Interbancária de Pagamentos (CIP), a CGU, o DPF e outras 18 unidades fiscalizadoras, no levantamento para elaboração do referencial estratégico da Sefti, foram identificadas boas práticas sobre fiscalizações de TI, dentre as quais, destaca-se a busca das unidades de auditoria pela compreensão do negócio a ser auditado, para permitir que a auditoria agregue valor ao negócio da entidade. Além disso, ressaltam-se o mapeamento e a gestão de riscos de TI, a produção de *releases*[10], a aplicação de questionários de satisfação de usuários, o acompanhamento *in loco* de testes de contingência, a busca de certificações, o incentivo à pós-graduação e a realização de auditoria contínua, com o uso de rotinas automatizadas de verificação de dados que possibilitam análise concomitante das transações de negócio. Tais boas práticas constam da base de dados sobre fiscalização de TI, produto desse levantamento.

No levantamento sobre gastos de TI, também foram identificadas boas práticas, como por exemplo, modelagem formal do processo de aquisição de bens e serviços de TI, estimativa de preços considerando equivalência de competitividade e manuais de licitação elaborados em colaboração pela Internet.

BENEFÍCIOS DOS LEVANTAMENTOS

Os principais benefícios dos levantamentos aqui resumidos são a obtenção e a geração de conhecimento para definir a forma de atuação da Sefti e

identificar o quê e como fiscalizar, condições essenciais para que desempenhe sua missão de assegurar que a tecnologia da informação agregue valor ao negócio da Administração Pública Federal em benefício da sociedade.

O levantamento sobre normas na área de TI trará, como benefício, a melhoria da Administração Pública Federal em duas frentes: aprimoramento da atuação do TCU na fiscalização da gestão e uso de TI, atribuição acometida à Sefti; e aprimoramento da gestão de TI na APF, pois os gestores poderão contar com base normativa que até então não se encontrava disponível, de forma sistematizada, ao público em geral.

Os dados obtidos acerca da governança e gastos em Tecnologia da Informação na APF e a identificação de seus principais sistemas e bases de dados irão auxiliar no direcionamento das ações de controle do Tribunal. O TCU pode, e deve, atuar como indutor do processo de aperfeiçoamento da governança de TI, em especial no tratamento da segurança da informação, identificada no levantamento sobre governança como a área mais crítica.

O Tribunal já acertou, inclusive, ao editar duas edições, em 2003 e 2007, da **Cartilha de Segurança da Informação** para servir como orientação sobre o tema. Outra maneira de induzir a melhoria no tratamento da segurança é a realização de auditorias de TI com foco em segurança da informação, que poderão fornecer subsídios valiosos para os gestores sobre os principais controles que devem ser implementados visando garantir a confiabilidade das informações tratadas pelos órgãos/entidades da Administração Pública Federal.

Assim, existe um campo vasto para atuação deste Tribunal na área de governança de TI na Administração Pública Federal. Se essa atuação for realizada de forma consistente e constante, os resultados serão promissores tendo em vista que poderá haver melhoria generalizada em todos os aspectos da governança de TI. Esse fato repercutirá na gestão pública como um todo e trará benefícios para o País e os cidadãos.

REFERÊNCIAS

TC 007.263/2007-0 – Acórdão nº 1.499/2007-TCU-Plenário – Relação nº 30/2007-Benjamin Zymler - Plenário – Levantamento de informações para elaboração do referencial estratégico da Sefti e prospecção das formas de atuação de entidades fiscalizadoras de TI.

TC 007.973/2007-5 – Acórdão nº 1.934/2007-TCU-Plenário – Levantamento de auditoria para obter informações sobre legislação, jurisprudência, normas e estudos na área de TI.

TC 007.972/2007-8 - Acórdão nº 371/2008-TCU-Plenário – Relação nº 14/2008-Guilherme Palmeira - Plenário – Levantamento de auditoria para obter informações acerca dos gastos em TI na Administração Pública Federal e de bases para consultas a referências de preços nas aquisições de bens e serviços de TI.

TC 008.380/2007-1 - Acórdão nº 1.603-TCU-Plenário – Levantamento de auditoria para coletar informações acerca da governança de TI e das principais bases de dados e sistemas da Administração Pública Federal.

NOTAS

[1] Norma técnica da Associação Brasileira de Normas Técnicas sobre boas práticas de segurança da informação.

[2] Guia para a gestão de TI que inclui sumário executivo, framework, objetivos de controle, mapas de auditoria, conjunto de ferramentas de implementação e guia com técnicas de gerenciamento.

[3] Programa de computador que auxilia auditores na realização de testes em arquivos de dados.

[4] Notícias distribuídas à imprensa, ao rádio, à TV, para serem divulgadas gratuitamente.

[5] Certificação para auditores de sistemas de informação.

[6] Certificação para profissional em segurança de sistemas de informação.

[7] Objetivos de controle para informação e tecnologias relacionadas.

[8] Biblioteca de infraestrutura de tecnologia da informação.

[9] URL – Uniform Resource Locator

[10] Notícias distribuídas à imprensa, ao rádio, à TV, para serem divulgadas gratuitamente.

Responsabilidade pelo Conteúdo
Secretaria-Geral de Controle Externo
Secretaria de Fiscalização de Tecnologia da Informação

Equipe de Auditoria - Levantamento para elaboração do referencial estratégico da Sefti:
Cláudia Augusto Dias (supervisora)
Harley Alves Ferreira
Rodrigo Machado Benevides (coordenador)
Tibério Cesar Jocundo Loureiro

Equipe de auditoria - Levantamento sobre normas na área de TI:
Carlos Alberto Mamede Hernandes
Carlos Renato Araujo Braga (coordenador)
Cláudio da Silva Cruz
Cláudio Souza Castello Branco (supervisor)

Equipe de auditoria - Levantamento sobre gastos de TI:
Carlos Renato Araujo Braga (supervisor)
Edward Lúcio Vieira Borba
Marcelo Meireles de Sousa
Mônica Cotrim Chaves (coordenadora)

Equipe de auditoria - Levantamento sobre governança de TI:
André Furtado Pacheco (coordenador)
Antônio Martins Júnior
Cláudia Augusto Dias (supervisora)
Luísa Helena Santos Franco
Roberta Ribeiro de Queiroz Martins (supervisora)

Responsabilidade Editorial
Secretaria-Geral da Presidência
Instituto Serzedello Corrêa
Centro de Documentação
Editora do TCU

Capa
Daniel Akira Hirozawa
Diagramação
Bianca
Fotos
Tiffany Szerpicki, Sanja Gjenero, Piotr Lewandowski, Michal Zacharzewski, Ivan Vicencio, Gokhan Okur

TRIBUNAL DE CONTAS DA UNIÃO

Endereço para contato e consulta na Internet

TRIBUNAL DE CONTAS DA UNIÃO
Secretaria de Fiscalização de
Tecnologia da Informação (Sefti)
SAFS, Quadra 4, Lote 1
Anexo I, sala 311
70042-900 Brasília - DF
Fone: (61) 3316-5371/7396
Fax: (61) 3316-5372
http://www.tcu.gov.br/fiscalizacaoti
sefti@tcu.gov.br

Secretaria de Fiscalização de Tecnologia da Informação

Negócio

Controle externo da governança de tecnologia da informação na Administração Pública Federal.

Missão

Assegurar que a tecnologia da informação agregue valor ao negócio da Administração Pública Federal em benefício da sociedade.

Visão

Ser unidade de excelência no controle e no aperfeiçoamento da governança de tecnologia da informação.