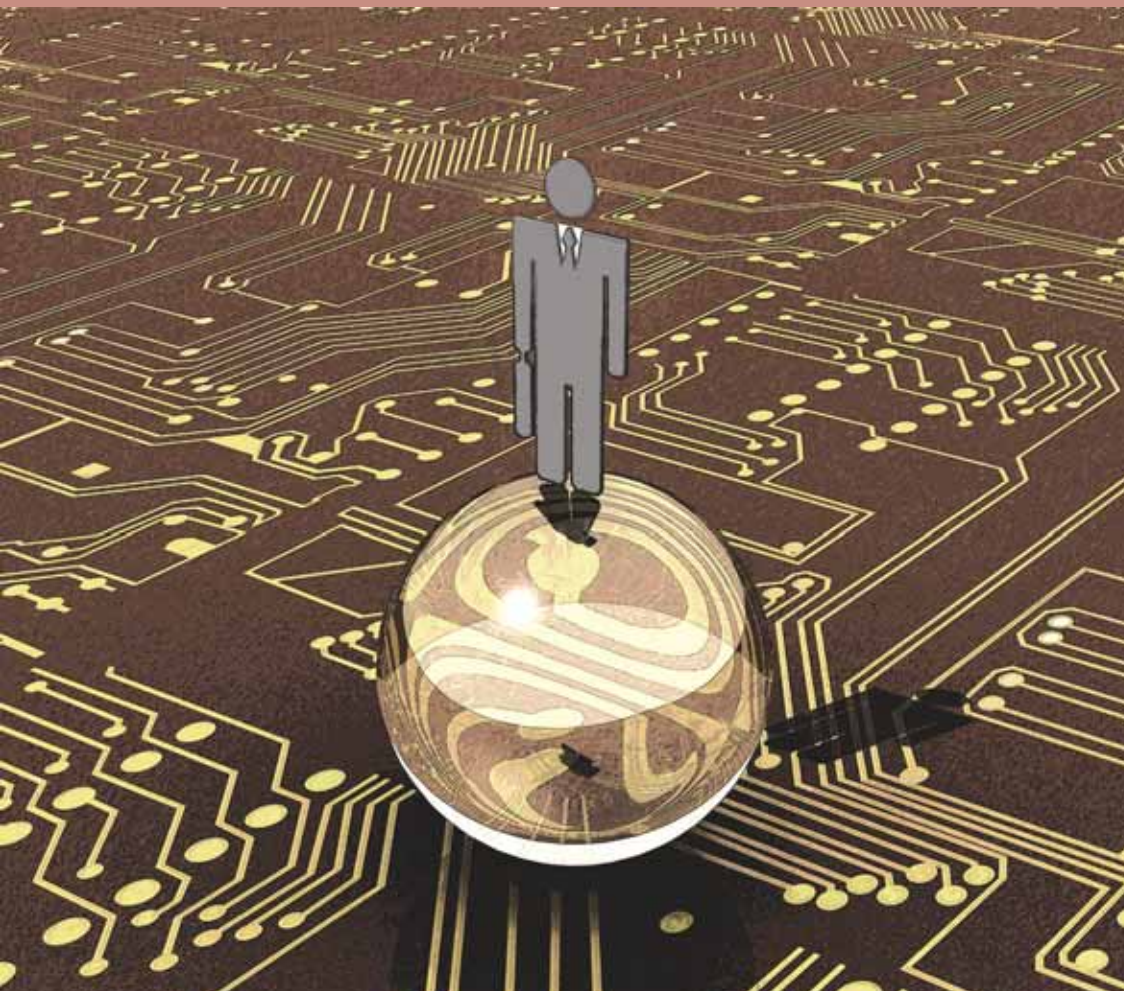
TRIBUNAL DE CONTAS DA UNIÃO

Sumários Executivos

Levantamento acerca da Governança de Tecnologia da Informação na Administração Pública Federal



República Federativa do Brasil

Tribunal de Contas da União

Ministros

Walton Alencar Rodrigues, Presidente
Ubiratan Aguiar, Vice-Presidente
Marcos Vinicios Vilaça
Valmir Campelo
Guilherme Palmeira
Benjamin Zymler
Augusto Nardes
Aroldo Cedraz
Raimundo Carreiro

Auditores

Augusto Sherman Cavalcanti
Marcos Bemquerer Costa
André Luís de Carvalho

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

Levantamento acerca da Governança de Tecnologia da Informação na Administração Pública Federal

Relator
Ministro Guilherme Palmeira

Brasília, Brasil 2008

<www.tcu.gov.br>

Para leitura completa do Relatório, do Voto e do Acórdão nº 1603/2008 - TCU - Plenário, acesse a página do TCU na Internet, no seguinte endereço:

<www.tcu.gov.br/fiscalizacaoti>

Brasil. Tribunal de Contas da União.

Levantamento acerca da Governança de Tecnologia da Informação na Administração Pública Federal/ Tribunal de Contas da União ; Relator Ministro Benjamin Zymler. – Brasília : TCU, Secretaria de Fiscalização de Tecnologia da Informação, 2008.

48 p. : il. color. – (Sumários Executivos)

1. Auditoria – tecnologia da informação. 2. Tráfego aéreo – controle – Brasil. 3. Transporte aéreo – segurança – Brasil. 4. Controlador de vôo – Brasil. I. Título. II. Série.

Catalogação na fonte: Biblioteca Ministro Ruben Rosa

SUMÁRIO

APRESENTAÇÃO

Um dos grandes desafios da Administração Pública Federal na atualidade é a elevação do seu grau de governança. O Tribunal de Contas da União, como órgão de controle externo, tem um papel de destaque no aperfeiçoamento dessa área. Nesse contexto, a governança de tecnologia da informação (TI) é essencial para que se atinja esse objetivo. A TI é o verdadeiro motor das organizações modernas podendo tanto impulsioná-las muito adiante como emperrar o seu progresso.

Devido à complexidade e à dimensão estratégica de que se reveste o tema, a Secretaria de Fiscalização de Tecnologia da Informação (Sefti), criada em 2006, necessitava obter informações acerca da situação da governança de TI na Administração Pública Federal para identificar corretamente o quê e como fiscalizar a gestão e o uso de recursos de TI pelos órgãos e entidades federais. Com esse intuito, decidiu-se pela execução do levantamento ora apresentado.

As informações obtidas neste levantamento serão utilizadas na elaboração do planejamento das fiscalizações a serem realizadas pelo Tribunal com intuito de aumentar a eficiência e eficácia de suas ações. O resultado final esperado é a indução de melhorias na governança de TI na Administração Pública Federal e, conseqüentemente, sua modernização e aperfeiçoamento.

Esta publicação traz o resumo da situação encontrada, à época do levantamento, da governança de TI na Administração Pública Federal. O respectivo processo (TC nº 008.380/2007-1) foi apreciado em sessão do Plenário de 13.08.2008, sob a relatoria do Ministro Guilherme Palmeira, resultando no Acórdão 1.603/2008-TCU-Plenário que autorizou a divulgação dos resultados dele decorrentes

Walton Alencar Rodrigues
Ministro-Presidente

AGRADECIMENTOS

O sucesso deste levantamento está relacionado à parceria que a equipe de auditoria estabeleceu com os gestores de tecnologia da informação (TI) dos órgãos e entidades que responderam ao questionário.

Durante a realização dos trabalhos, a equipe contou com a valiosa colaboração dos Analistas de Controle Externo Antônio Martins Júnior, Rodrigo Machado Benevides e Tibério Cesar Jocundo Loureiro, lotados na Secretaria de Fiscalização de Tecnologia da Informação (Sefti), e Sylvio Xavier Júnior, lotado na Secretaria de Tecnologia da Informação (Setec).

Por fim, agradece-se a colaboração de Rui Nóbrega da Silva Leal, funcionário terceirizado, pelo suporte ao trabalho e atendimento sempre cordial e atencioso.

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, conseqüentemente, sua modernização e aperfeiçoamento. Para tanto, é necessário se obter informações acerca da situação da governança de TI na APF para identificar corretamente o quê e como fiscalizar e aumentar a eficiência e eficácia de suas ações.

Para isso, este levantamento foi autorizado pelo Acórdão nº 435/2007-TCU-Plenário com o objetivo de "coletar informações acerca dos processos de aquisição de bens e serviços de TI, de segurança da informação, de gestão de recursos humanos de TI, e das principais bases de dados e sistemas da Administração Pública Federal." Assim, foram obtidas informações para elaboração de mapa com a situação da governança de TI na Administração Pública Federal e identificados os principais sistemas e bases de dados da APF. Com essa gama de informações, é possível identificar onde a situação da governança de TI está mais crítica e em que áreas o TCU deve atuar. Assim, o planejamento das fiscalizações da Sefti contará com subsídios valiosos para seu aprimoramento.

Foram selecionados, como amostra deste levantamento, 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 a 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).

A partir dos dados coletados, observou-se que a situação da governança de TI na Administração Pública Federal é bastante heterogênea. 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 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. 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.

OBJETIVOS DO LEVANTAMENTO

O objetivo principal deste levantamento foi 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.

Com essa gama de informações será possível verificar onde a situação da governança de TI está mais crítica e identificar as áreas onde o TCU pode, e deve, atuar como indutor do processo de aperfeiçoamento da governança de TI. Além disso, o planejamento das fiscalizações da Sefti contará com subsídios valiosos para seu aprimoramento.

COMO SE DESENVOLVEU O TRABALHO

Durante a fase de planejamento foi elaborada matriz de planejamento com intuito de definir as áreas da governança de TI a serem pesquisadas e organizar a execução do trabalho.

Foram selecionados, como amostra, 333 órgãos/entidades representativos da Administração Pública Federal. Desses órgãos/entidades, 29 responderam em conjunto com outros órgãos/entidades e 14 não se consideram integrantes da Administração Pública Federal, apesar de jurisdicionados ao Tribunal, em especial os que fazem parte do Sistema "S" (Apêndice IV, fl. 42). Outros 25 órgãos/entidades não responderam à pesquisa e 10 não completaram a quantidade mínima estabelecida de respostas (Apêndice III, fl. 41-v). Assim, 255 órgãos/entidades participaram efetivamente do levantamento. Dessa relação constaram ministérios, universidades federais, tribunais federais, agências reguladoras, autarquias, secretarias, departamentos e empresas estatais. Ainda no planejamento, para ser submetido aos órgãos e às entidades da amostra, foi elaborado questionário composto de 39 perguntas baseadas nas normas técnicas brasileiras NBR ISO/IEC 17799:2005, NBR ISO/IEC 15999-1:2007 e no *Control Objectives for Information and related Technology 4.1* (Cobit 4.1).

A norma NBR ISO/IEC 17799:2005 é o código de prática para a gestão da segurança da informação mais adotado em todo o mundo. Essa norma teve sua primeira versão internalizada pela Associação Brasileira de Normas Técnicas (ABNT) em setembro de 2001, e conta com a segunda versão em vigor desde setembro de 2005. Essa norma fornece recomendações em gestão da segurança da informação para uso dos responsáveis pela implementação e manutenção da segurança em suas organizações. Tem como propósito prover uma base comum para o desenvolvimento de normas de segurança organizacional e das práticas efetivas de gestão da segurança, e prover confiança nos relacionamentos entre as organizações.

A norma NBR 15999-1:2007 é o código de prática para a gestão de continuidade de negócios, baseada na norma inglesa BSI 25999:2006 e internalizada no Brasil pela ABNT em outubro de 2007. Seu objetivo é fornecer um sistema baseado nas boas práticas de gestão de continuidade de negócios.

O Cobit, por sua vez, é um modelo de gestão orientado a processos e está dividido em quatro grandes grupos: Planejar e Organizar (*Plan & Organise* – PO), Adquirir e Implementar (*Acquire & Implement* – AI), Entregar e Assistir (*Deliver & Support* – DS) e Monitorar e Avaliar (*Monitor & Evaluate* – ME), cujas iniciais serão utilizadas no decorrer do relatório para fins de referência como critérios de auditoria. O Cobit se encontra disponível no site www.isaca.org. Vale salientar que se trata de modelo já amplamente reconhecido e utilizado, no Brasil e no mundo, no âmbito da tecnologia da informação, tanto por gerentes de informática quanto por auditores de TI.

Na fase de execução do levantamento, os órgãos e entidades selecionados receberam, por meio de correspondência oficial, a identificação e a senha individual para acesso ao questionário e, posteriormente, via mensagem eletrônica, o *link* para o questionário *on-line*. O software *Risk Manager* apoiou o envio, a coleta e a tabulação das informações do questionário.

Durante o preenchimento do questionário, foi solicitado aos gestores de TI dos órgãos e entidades que anexassem documentos eletrônicos para servirem de evidências às respostas apresentadas. Em geral, esses documentos solicitados são atos normativos formais da organização, mas poderiam ser também atas de reunião ou outras publicações internas aceitas e reconhecidas pelo órgão/entidade. Deve-se observar que as informações coletadas foram declaradas pelos gestores e não verificadas pela equipe junto aos órgãos/entidades. Além disso, nesse primeiro momento, não foi avaliada a pertinência e a qualidade dos documentos produzidos e anexados pelos órgãos/entidades.

Ao final da coleta de informações, as respostas apresentadas nos questionários foram tabuladas e as evidências organizadas em pastas eletrônicas para consulta e tratamento posterior.

Como limitação à execução dos trabalhos, deve-se destacar que alguns órgãos/entidades não dispunham de todas as informações solicitadas e fizeram muito esforço para obtê-las. Mesmo assim, alguns órgãos/entidades não conseguiram obter todas as informações e as questões relativas a elas ficaram sem resposta.

LEVANTAMENTO ACERCA DA 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.

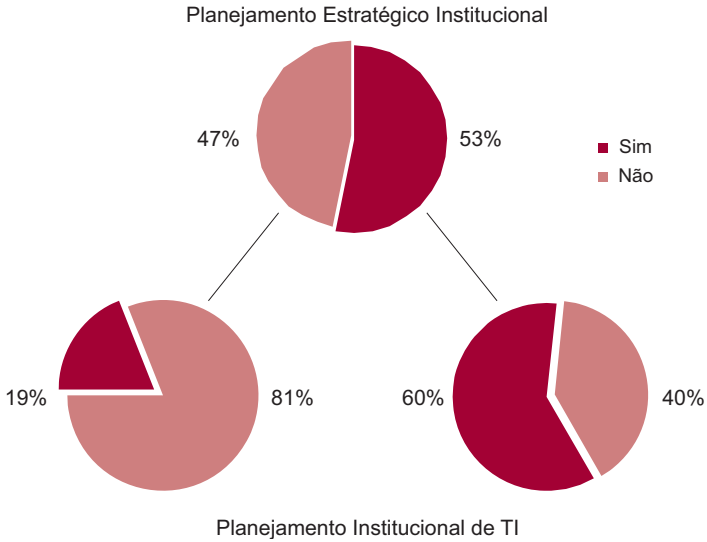
Planejamento estratégico institucional e de TI

Um percentual expressivo dos 255 órgãos/entidades pesquisados (47%) não tem planejamento estratégico institucional em vigor. Esse fato demonstra que quase metade das organizações pesquisadas não possuem a cultura de planejar estrategicamente suas ações e apenas reagem às demandas e às mudanças ocorridas no seu âmbito de atuação. Essa forma de atuação dificulta o planejamento das ações de TI[1].

O confronto desses dados com a informação de que 59% das organizações pesquisadas não fazem planejamento estratégico de TI, permite algumas análises, conforme apresentado no Gráfico 1. Dos 47% dos órgãos/entidades que afirmaram não possuir planejamento estratégico institucional, 81%,

isto é, 97 órgãos/entidades não possuem planejamento estratégico de TI. Por outro lado, o fato de haver planejamento estratégico institucional, por si só, não garante que haverá planejamento estratégico de TI. Em 40% das organizações que dispunham do primeiro, não havia o segundo.

Gráfico 1 – 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.

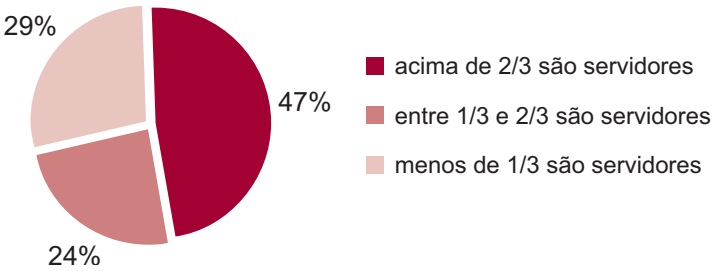
O planejamento estratégico de TI[2] é essencial para que as organizações possam identificar e alocar corretamente os recursos da área de TI de acordo com as prioridades institucionais e com os resultados esperados. O percentual de 59% dos 255 órgãos/entidades pesquisados sem planejamento estratégico 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 conseqüente 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.

A existência de um comitê diretivo de TI (*IT Steering Committee*)[3], que determine as prioridades de investimento e alocação de recursos nos diversos projetos e ações de TI, é de fundamental importância para o alinhamento entre as atividades de TI e o negócio da organização, bem como para a otimização dos recursos disponíveis e a redução do desperdício. 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.

Estrutura de pessoal de TI

Quanto à estrutura de pessoal de TI, a equipe do levantamento identificou que um total de 29% dos 255 órgãos/entidades pesquisados possui menos de 1/3 de seu quadro de TI composto por servidores[4], 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.

Gráfico 2 – Proporção entre servidores e colaboradores externos nos órgãos/entidades pesquisados



Segundo as informações levantadas no questionário, somente 37% dos servidores do quadro das áreas de TI dos órgãos/entidades possuem formação específica em TI[5] (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[6]. 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

Neste tópico, o objetivo é delinear a qualidade do tratamento dado pelos órgãos públicos à segurança das informações sob sua responsabilidade.

A importância do correto tratamento para a confidencialidade, a integridade e a disponibilidade das informações de órgãos públicos é evidente,

sem falar na autenticidade, na responsabilidade pelos dados e na garantia de não-repúdio[7]. A própria prestação do serviço de uma instituição pública aos cidadãos depende da confiabilidade das informações por ela tratadas e ofertadas.

Foram solicitados como evidências os documentos sobre a Política de Segurança da Informação (PSI), o Plano de Continuidade de Negócios (PCN), normas/procedimentos relacionados à classificação de informações e as normas/procedimentos de controle de acesso, que devem orientar o tratamento da segurança das informações.

A política de segurança da informação é o documento que contém as diretrizes da instituição quanto ao tratamento da segurança da informação. De acordo com as orientações da norma NBR ISO/IEC 17799:2005 da ABNT, a política deve declarar explicitamente o comprometimento da direção da instituição com a segurança da informação. Além disso, deve também conter definições dos termos relacionados dentro do escopo da instituição e apontar os objetivos de controle, os controles, as estruturas que implementam esses controles, as responsabilidades e também as políticas e normas que disciplinam e complementam esse documento de diretrizes, incluindo referências à legislação e aos requisitos regulamentares e contratuais[8]. Em geral, esse é o documento da gestão da segurança da informação a partir do qual derivam os documentos específicos para cada meio de armazenamento, transporte, manipulação ou tratamento específico da segurança da informação em TI.

A gestão da continuidade do negócio, por sua vez, é o processo que objetiva minimizar um impacto sobre a organização e recuperar perdas de informações a um nível aceitável, por meio da combinação de ações de prevenção e recuperação. O plano de continuidade de negócios é um documento ou conjunto de documentos que, tipicamente, contém as condições para sua ativação, as responsabilidades individuais, os procedimentos de emergência, os procedimentos operacionais temporários e os procedimentos de recuperação. O plano (ou planos) de continuidade

deve(m) ser periodicamente testado(s) e avaliado(s), para garantir que funcione(m) quando necessário.

A classificação de informações, por sua vez, é o processo que visa garantir que cada informação tenha o tratamento de segurança adequado ao seu valor, aos requisitos legais, à sensibilidade e ao risco de sua perda para a organização. Nesse processo devem existir, pelo menos, dois documentos de referência: o esquema de classificação, que contém as definições dos níveis de proteção considerados, e um conjunto apropriado de procedimentos para rotulação e tratamento da informação segundo esse esquema.[9]

A gestão do controle de acesso, por fim, é o processo que visa garantir que o acesso à informação seja controlado com base nos requisitos de negócio e na adequada segurança da informação. O principal documento relacionado a esse processo é a política de controle de acesso, que contém as regras de controle de acesso e direitos para cada usuário ou grupos de usuários, e relaciona claramente os requisitos de negócio e os controles associados.

Os órgãos foram também questionados sobre algumas estruturas organizacionais para assistir a execução das diretrizes de segurança: área específica para tratamento de segurança, área específica para tratamento de incidentes, evidências de gestão centralizada para mudanças, capacidade e compatibilidade de soluções de TI.

A infra-estrutura para a adequada gestão da segurança da informação na organização é tratada no item 6.1 da NBR ISO/IEC 17799:2005. Cada órgão/entidade deve adotar a estrutura organizacional que mais se adeqüe à cultura e ao tamanho da instituição, assegurando, contudo, que a implementação dos controles de segurança da informação tenha uma coordenação que permeie toda a organização. Assim, as organizações podem até usar um fórum já existente (por exemplo, um conselho de diretores), desde que este assuma também, de forma explícita, as atividades de gestão da segurança da informação. O mais freqüente tem sido o uso de um fórum

específico (por exemplo, um grupo específico para gerenciar a segurança da informação) ou mesmo um gestor individual (que é conhecido no mercado como CSO – *Chief Security Officer*).

O objetivo do processo de gestão de incidentes de segurança é assegurar que seja aplicado tratamento consistente e efetivo para os incidentes, que incluem desde falhas de sistemas até violações intencionais da política de segurança. Para isso, há que se designar claramente as responsabilidades no tratamento de incidentes, bem como os procedimentos a serem adotados, em sintonia com outras diretrizes, como o plano de continuidade de negócio e a classificação das informações. A existência de uma área específica é uma recomendação para a operacionalização desses controles, não só pela NBR ISO/IEC 17799:2005, como também por várias diretrizes para governança de TI.

Outros processos de infra-estrutura relacionados com a segurança são a gestão centralizada de mudanças e a gestão de capacidade e compatibilidade. Na gestão centralizada de mudanças, há controle rígido das mudanças no ambiente operacional para garantir a estabilidade do ambiente e a auditoria das alterações realizadas. O controle inadequado de modificações nos sistemas e nos recursos de processamento da informação é uma causa comum de falhas de segurança ou de sistema.

Já a gestão de capacidade e compatibilidade visa principalmente garantir a disponibilidade das informações, ao verificar continuamente se as soluções de TI suportam adequadamente a demanda por informações sem sobrecarregar os sistemas, gerar descontinuidade de operação e/ou falhas no nível de serviço acordado.

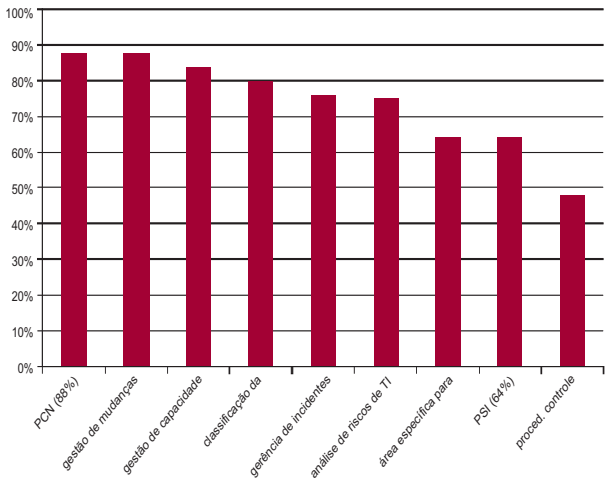
Finalmente, os órgãos/entidades foram instados a apresentar as evidências de que estariam preocupados em realizar o tratamento dos riscos relacionados ao processamento das informações sob sua responsabilidade por meio das soluções de TI. O tratamento dos riscos inclui a identificação, a quantificação e a classificação dos riscos quanto à sua prioridade, com

base em critérios sintonizados com o negócio da organização. Os resultados dessa análise devem orientar as ações de gestão e as prioridades para o gerenciamento dos riscos de segurança da informação e para a implementação dos controles selecionados. Por isso, a análise de risco é estratégica na gestão da segurança e deve ser feita em bases periódicas para garantir a adequação entre gestão e negócio.

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.

Gráfico 3 – Deficiências na segurança da informação



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 infra-estrutura 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 pesquisados 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.

Desenvolvimento de sistemas de informação

Embora haja uma consciência relativamente generalizada de que as áreas de TI nas organizações não são simplesmente produtoras de software[10], o desenvolvimento de sistemas de informação é, sem dúvida, uma de suas principais atividades. A qualidade desse desenvolvimento interfere direta-

mente na qualidade do serviço prestado pela área de TI. A necessidade de conectividade com a Internet e com sistemas em outras organizações faz da segurança da informação um requisito de projeto. Os clientes, cada vez mais exigentes, esperam sistemas rápidos, fáceis de usar, robustos e que realmente atendam às suas necessidades. Além disso, a parceria com o cliente deve ocorrer já no próprio processo de desenvolvimento, que não pode ser mais lento do que a velocidade com que mudam as necessidades, e não pode ser obscuro quanto a prioridades, prazos, qualidade e segurança.

A aplicação de modelos de gestão para qualidade de software vem, exatamente, ao encontro desses requisitos, e o desenvolvimento de sistemas pautado em uma metodologia é um requisito básico de quaisquer desses modelos. A metodologia de desenvolvimento define "como fazer do jeito certo", enquanto a gestão da qualidade se concentra em avaliar e aprimorar o processo de uso dessa metodologia de desenvolvimento na organização.

O uso de metodologia para desenvolvimento de sistemas não é um tema novo e vem, progressivamente, incorporando os conceitos de engenharia de software[11] para tornar o processo de desenvolvimento de sistemas mais controlável, mensurável e eficaz. Com a metodologia, busca-se não só garantir que as várias etapas típicas do desenvolvimento (levantamento, projeto, programação, testes e homologação) sejam executadas de forma sistemática e documentada, mas também permitir a avaliação e melhoria do processo, com vistas à produção de software de qualidade.

O governo brasileiro tem mostrado preocupação com a qualidade do software produzido no Brasil ao instituir programas e ações de incentivo à busca de melhorias. Como exemplo disso, há o Programa Brasileiro de Qualidade e Produtividade do Software (PBQP-Sw)[12] e o Modelo de Melhoria de Processos de Software (MPS.BR)[13]. Nessas orientações, a existência de metodologia é requisito fundamental na construção de software de qualidade.

Além das informações sobre metodologia de desenvolvimento, outra informação solicitada aos órgãos/entidades sobre os seus sistemas foi a existência de serviços transacionais via Internet. Sobre esse assunto, 76% dos pesquisados informaram que prestam serviços pela Internet com troca bidirecional de informações entre o órgão/entidade e seus clientes. Esse percentual expressivo chama atenção para o uso, por órgãos/entidades da Administração Pública, de sistemas *web* na execução da sua missão de prestação de serviços aos cidadãos.

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 conseqüências, 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 que 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 prestação de um bom serviço para os cidadãos é, em última instância, o negócio de toda instituição pública. A definição do que é um "bom serviço", sintonizando as expectativas dos clientes com a oferta, é exatamente o que constitui um acordo de nível de serviço (SLA, sigla do inglês *Service Level Agreement*).

No caso de um acordo de nível de serviço de TI é definida a qualidade dos serviços de TI em função das necessidades da organização, quantificadas e especificadas para cada serviço. Assim, a disponibilidade da infra-estrutura de rede, o desempenho dos sistemas, o tempo de solução de problemas e outros dados semelhantes costumam constituir indicadores dos documentos de acordos de níveis de serviço, e devem ser adequadamente verificados e tratados quando detectadas falhas, de modo a atender às necessidades do negócio. Sem a definição de tais indicadores, fica difícil responder à questão: "os serviços de TI da minha organização estão adequados às necessidades do negócio?". Igualmente, fica difícil priorizar investimentos e ações na área de TI sem saber onde o desempenho está mais próximo ao limite do esperado ou é mais crítico para o negócio.

Um aspecto particularmente importante é a gestão de níveis de serviço também para serviços contratados. A especificação formal de tais indicadores pode ser o principal instrumento dos gestores para garantir o cumprimento dos contratos de TI e possibilitar a aplicação de penalidades em casos de não-atendimento. A necessidade de acordo prévio e de mensuração da qualidade de serviços de TI é citada, inclusive, em trechos de Acórdãos do TCU, como o Acórdão nº 2.172/2005-TCU-Plenário[14] e o Acórdão nº 786/2006-TCU-Plenário[15]. O termo "acordo de nível de serviço" para contratos de TI também já é conhecido do TCU, e foi mencionado no Acórdão nº 1.878/2005-TCU-Plenário[16].

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 conseqüências mais prováveis para tal cenário são clientes insatisfeitos e investimentos inadequados.

Além disso, 74% dos pesquisados informaram que não executam a gestão de níveis de serviço dos serviços contratados, ou seja, mesmo quando o órgão/entidade é cliente e não fornecedor, não há preocupação com a avaliação e o controle dos resultados. Assim, como em última instância um serviço contratado pela área de TI visa atender à necessidade dos seus clientes, a ausência da gestão externa tem as mesmas conseqüências da ausência da gestão interna dos níveis de serviço.

Processo de contratação de bens e serviços de TI

Na contratação de bens e serviços de TI é essencial a adoção de processo de trabalho formalizado, padronizado e judicioso quanto ao custo, à oportunidade e aos benefícios advindos para a organização. Esse processo melhora o relacionamento com os fornecedores e prestadores de serviços, maximiza a utilização dos recursos financeiros alocados à área de TI e contribui decisivamente para que os serviços de TI dêem o necessário suporte às ações da organização no alcance de seus objetivos e metas.

Mesmo que a maioria (54%) dos órgãos/entidades pesquisados tenha informado que adota processo formal de trabalho para contratações de TI, a situação está longe do ideal, já que um percentual expressivo de organizações (46%) não adota processo formal de trabalho para contratações de TI.

Deve-se observar que isso não significa deixar de cumprir a legislação específica. Entretanto, a falta de um processo de trabalho definido, padronizado, documentado e aprovado para realizar as contratações de TI pode

trazer conseqüências danosas à organização. Como não existe um padrão oficial e disseminado pela organização, cada área pode adquirir os recursos de que necessita de uma forma diferente. Dessa maneira, a organização se expõe a riscos desnecessários que poderiam ser evitados com a adoção de um processo de trabalho formalizado.

Devido à complexidade da legislação de licitações vigente, o primeiro risco é de que, eventualmente, não sejam observados todos os dispositivos legais e normativos. Provavelmente, nem todos os responsáveis pelas contratações de TI são especialistas no assunto e, caso não haja um processo formal de trabalho, em algumas aquisições, dispositivos legais podem deixar de ser observados. Além disso, é improvável que todos os responsáveis acompanhem as alterações normativas e estejam atualizados sobre as mudanças na interpretação da legislação e na jurisprudência da área. O mais seguro para a organização é que o processo de contratação esteja padronizado e disponível para todos os responsáveis para minorar a ocorrência de dúvidas e falhas nas aquisições de TI. Deve-se reforçar que muitas falhas no processo de aquisição têm sérias repercussões no processo de gestão dos contratos durante sua vigência e, em alguns casos, mesmo após seu encerramento devido a pendências judiciais.

Outro risco decorrente da não-existência de processo formal é a realização de aquisições desnecessárias, com baixa qualidade ou que não estejam alinhadas às necessidades do negócio a médio e longo prazos. Dessas situações decorre, normalmente, desperdício de recursos. Em alguns casos, inclusive, a ocorrência de fraudes e desvios fica facilitada exatamente pela falta ou dificuldade de controle sobre processos não padronizados.

O item 9.4 do Acórdão nº 786/2006-TCU-Plenário recomendou à Secretaria de Logística e Tecnologia da Informação do Ministério do Planejamento, Orçamento e Gestão (SLTI) que elaborasse "um modelo de licitação e contratação de serviços de informática para a Administração Pública Federal" e promovesse "a implantação dele nos diversos órgãos e entidades sob sua coordenação mediante orientação normativa". Em aten-

dimento a esse acórdão, a SLTI publicou a Instrução Normativa nº 4, de 19 de maio de 2008. A IN-4 da SLTI dispõe sobre o processo de contratação de serviços de TI pela Administração Pública Federal direta, autárquica e fundacional. A norma contempla as fases de planejamento de contratação, seleção do fornecedor e gerenciamento do contrato e entrará em vigor no dia 2 de janeiro de 2009.

Além de processo formal de contratação de bens e serviços de TI, para se obter uma boa gestão é necessária a otimização dos recursos disponíveis. No caso específico da área de TI, essa preocupação se torna essencial tendo em vista as rápidas e constantes mudanças tecnológicas. Assim, é imperativo que qualquer contratação de solução de TI seja precedida de estudo de viabilidade e de análise de custo/benefício. Apesar dessa máxima não ser contestada, apenas pouco mais da metade (53%) dos órgãos/entidades pesquisados realiza essa análise.

É importante notar que toda contratação de TI deve ser anteriormente aprovada levando-se em conta seus aspectos técnicos, sua funcionalidade, sua viabilidade, seu alinhamento com o planejamento estratégico e se os benefícios advindos compensam o seu custo. As contratações de TI, além de referendadas pela área de TI, devem ser aprovadas pelo gestor da área afetada. Em alguns casos, quando envolverem valores elevados, assuntos relevantes ou quando envolverem diversas áreas da organização, as contratações devem ser aprovadas pelo comitê diretivo de TI.

Os artigos 10 a 12 da supracitada IN-4 da SLTI indicam atividades que deverão ser executadas para análise de viabilidade da contratação.

Por outro lado, apesar de seu importante papel na consecução dos objetivos institucionais nas organizações, a tecnologia da informação não pode ser encarada como um fim em si mesma. Todas as ações de TI devem concorrer para que a organização alcance seus objetivos e metas.

O Tribunal, em diversos acórdãos, tem destacado a importância e determinado a necessidade da harmonia entre as contratações de TI e o planejamento estratégico dos órgãos/entidades federais. O item 9.3.11 do Acórdão nº 1.558/2003-TCU-Plenário é taxativo: "ao proceder a licitação de bens e serviços de informática, elabore previamente minucioso planejamento, realizado em harmonia com o planejamento estratégico da unidade e com o seu plano diretor de informática, (...)". Aponta na mesma direção o item 9.1.1 do Acórdão nº 2.094/2004-TCU-Plenário: "todas as aquisições devem ser realizadas em harmonia com o planejamento estratégico da instituição (...)".

Assim, toda contratação de TI deve ter seus benefícios para a organização explicitados, ou seja, deve ser justificada como irá colaborar para a consecução dos objetivos institucionais. Apesar desse entendimento já consolidado, 40% dos órgãos e entidades pesquisados ainda não se preocupam em justificar e destacar os benefícios esperados para a organização. Por outro lado, a letra "c" do inciso V do art. 10 da recém publicada IN-4 da SLTI determina que a justificativa da solução escolhida contenha a "identificação dos benefícios que serão alcançados com a efetivação da contratação em termos de eficácia, eficiência, efetividade e economicidade."

No tocante ao valor, muitas contratações de TI têm seu valor final calculado a partir da soma de valores de diversos componentes. Especialmente na contratação de uma solução de TI, os custos dos componentes podem variar ao longo do tempo de duração do contrato de maneira diferente. Tome-se como exemplo uma solução de TI que envolva recursos humanos, aluguel de equipamentos e recursos de telecomunicação. Pode ser necessário, para se manter o equilíbrio econômico-financeiro do contrato, que haja a repactuação com a assinatura de termo aditivo por questões econômicas, de mercado ou tecnológicas. Se não se souber o quanto cada componente representa na formação do valor final, não se poderá repactuar o contrato de maneira justa e não lesiva aos interesses públicos.

Diante dessa situação, torna-se importante a exigência de que, antes da adjudicação do contrato, seja apresentado o demonstrativo de formação de preço. De acordo com as respostas dos gestores, essa prática somente é observada por metade dos órgãos/entidades participantes do levantamento, apesar da Lei nº 8.666/1993 já recomendá-la, mesmo que implicitamente, em seus artigos 7º e 46.

No que diz respeito ao processo de contratação de bens e serviços de TI, pode-se concluir que 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 sobre a conveniência das contratações de TI.

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

Da mesma forma que é importante que haja processo de trabalho formalizado para contratação de bens e serviços de TI, é essencial que os contratos advindos dessas aquisições sejam bem geridos.

Apesar de a Lei nº 8.666/1993 determinar algumas ações que devem ser obrigatoriamente realizadas, não há indicação do que deve constar de processos de trabalho para gestão dos contratos. Entretanto, para todos os contratos e, especialmente, para os contratos de TI, a boa gestão é essencial para se atingir os objetivos esperados. Para se gerir adequadamente os riscos inerentes às atividades de TI, a adoção de processo formal de trabalho é de suma importância. Esse processo de trabalho deve ser definido, padronizado, documentado, aprovado e divulgado para toda a organização.

A maioria (55%) dos órgãos/entidades participantes do levantamento afirmou que não adota processo formal de trabalho para gestão de contratos de TI. Essa situação merece ser observada com atenção.

A ausência desse processo de trabalho pode causar problemas ao bom funcionamento da área de TI da organização. Se os contratos de TI, que garantem os serviços de infra-estrutura de TI, o desenvolvimento de aplicativos e o atendimento aos usuários, por exemplo, não forem bem geridos, todas as atividades de TI serão afetadas. Além disso, todas as atividades da organização que dependem de serviços de TI poderão sofrer com interrupções ou níveis de serviço abaixo do desejado e comprometer metas e objetivos da instituição.

Caso a organização não consiga exigir dos seus fornecedores uma prestação de serviço adequada à sua necessidade, muitos projetos e atividades correm risco de não serem realizados no prazo necessário, acarretando perdas ou desperdício de recursos. Eventualmente, também, alguma determinação legal poderá deixar de ser cumprida, o que tornará a organização vulnerável em termos jurídicos e na sua prestação de contas.

É interessante notar que 78% das organizações consultadas afirmaram que designam formalmente um gestor para cada contrato de TI. Esse gestor pode, eventualmente, ser a mesma pessoa do "representante da administração" previsto no art. 67 da Lei nº 8.666/1993. Entretanto, observa-se que, apesar de 78% das organizações pesquisadas terem um gestor designado para o contrato, boa parte desses gestores não dispõe de um processo de trabalho formalmente definido. Assim, o bom desempenho da função depende da capacidade e do conhecimento individual do gestor, quando deveria ser uma atividade impessoal que qualquer funcionário habilitado pudesse exercer de acordo com o processo de trabalho padrão. A recém publicada IN-4 da SLTI dedica toda a Seção III ao gerenciamento do contrato.

Outro fato que causa preocupação é que 65% dos órgãos/entidades que participaram do levantamento não realizam reuniões periódicas com os contratados para avaliar o desempenho de cada contrato de TI. Esse procedimento deve fazer parte do processo formal de trabalho para gestão dos contratos de TI.

O art. 67 da Lei nº 8.666/1993 não determina explicitamente a realização de reuniões periódicas com os fornecedores, entretanto, determina que "a execução do contrato deverá ser acompanhada e fiscalizada por um representante da Administração especialmente designado" que "anotará em registro próprio todas as ocorrências relacionadas com a execução do contrato, determinando o que for necessário à regularização das faltas ou defeitos observados".

A forma mais simples e eficiente para o cumprimento desse dispositivo legal é, sem dúvida alguma, a realização de reuniões com a periodicidade adequada para avaliar o andamento do serviço, bem como os problemas enfrentados e as decisões a serem tomadas para solucioná-los. Outra vantagem significativa da realização de reuniões com os contratados é a possibilidade de antevisão de problemas futuros baseada na evolução do desempenho

e outros indicadores que, eventualmente, podem apontar degradação do nível de serviços ou outros riscos iminentes.

Praticamente metade (53%) dos órgãos/entidades que participaram do levantamento afirmou que atesta as faturas apresentadas com base em itens previamente definidos. Por outro lado, 47% das organizações pesquisadas não definem previamente um critério para avaliação se as faturas apresentadas correspondem à realidade e se não contêm erros.

Esse procedimento específico deve constar do processo formal de trabalho para gestão dos contratos de TI. A sua ausência pode dificultar o trabalho do responsável por atestar tecnicamente a realização do serviço. Caso esse responsável tenha que atestar muitas faturas e essas faturas tenham muitos itens a serem verificados, o risco de que sejam aprovados pagamentos indevidos é bastante razoável.

No levantamento, 90% das organizações consultadas disseram que fazem o monitoramento técnico dos contratos de TI. Foram informadas, também, a quantidade de contratos de TI e a quantidade de profissionais que executam essa tarefa. Em 17% dos órgãos/entidades pesquisados cada profissional monitora tecnicamente, em média, mais de cinco contratos de TI. A maior quantidade calculada foi de 14,7 contratos por pessoa e a menor foi de 0,5 contrato por pessoa. Deve-se ter sempre em mente que essas informações devem ser analisadas com cuidado porque esses contratos podem variar do fornecimento de um único item simples de ser controlado ao complexo controle de uma fábrica de software.

Já a monitoração administrativa dos contratos deve ser feita em cumprimento ao disposto no inciso XIII do art. 55 c/c art. 29 da Lei nº 8.666/1993. Tal monitoração envolve a verificação de aspectos trabalhistas (encargos, subordinação direta, desvio de função, não-verificação da impessoalidade, ingerência administrativa), aspectos fiscais (regularidade cadastral),

manutenção das condições de habilitação na licitação, atendimento aos normativos internos do órgão ou entidade e regularidade dos recolhimentos de contribuições sociais.

Nem todos os profissionais de TI estão aptos a realizar a monitoração administrativa, sem uma preparação específica, por ser uma atividade que requer o acompanhamento da legislação e jurisprudência da área de licitações e contratos. Além disso, essa atividade pode tomar um tempo elevado devido à quantidade de documentos e requisitos burocráticos a serem observados. Se a atividade for realizada por pessoa não preparada devidamente ou que não esteja atualizada nessa matéria, o risco de problemas futuros para a organização é considerável. Levando tudo isso em consideração, a monitoração administrativa deve ser realizada por setor especializado que não precisa necessariamente estar ligado à área de TI.

Das organizações consultadas, em menos da metade (45%) a monitoração administrativa é realizada por setor especializado não vinculado à área de TI. Nos outros 55% dos órgãos/entidades pesquisados, uma parte significativa do tempo de profissionais especializados de TI é gasto no desempenho dessa tarefa.

Esse procedimento específico deve constar do processo formal de trabalho para gestão dos contratos de TI e ser realizado por profissionais preparados para tal. Caso contrário, o risco de serem descumpridos dispositivos legais que poderão acarretar pendências judiciais para a organização é significativo. Nesse aspecto, é interessante lembrar o caso recentemente julgado pelo Tribunal, em que órgãos da Administração Pública Federal pagavam 0,5% a mais de FGTS, em contratos de TI, por não terem observado a mudança da alíquota em 1º de janeiro de 2007, conforme a Lei Complementar nº 110/2001 (Acórdão nº 353/2008-TCU-Plenário).

Outra informação que chama a atenção é que menos da metade (43%) dos órgãos/entidades participantes do levantamento informou que exige a transferência de conhecimento nos contratos relativos aos produtos e

serviços de TI terceirizados. O percentual restante, 57%, é significativo, principalmente quando são analisados alguns dos motivos que levam as organizações a terceirizarem serviços de TI: necessidade de acesso a tecnologias mais avançadas e redução de riscos associados a essas tecnologias.

É um contra-senso não exigir a transferência do conhecimento necessário para realização de serviços importantes para a organização, contratados porque não há os recursos necessários para serem realizados internamente. Deve-se observar que a organização paga inclusive pela aquisição do conhecimento por parte do prestador e, em muitos contratos, não assegura, ao seu término, a manutenção do conhecimento na instituição.

Esse procedimento específico deve constar dos processos formais de trabalho para contratação de TI e para gestão dos contratos de TI. No primeiro caso, é necessário que a transferência de conhecimento conste desde o início da contratação, ou seja, no edital da licitação. No segundo caso, deve haver a verificação se a transferência de conhecimento é realizada. Caso contrário, há risco de que os serviços terceirizados, após o final do contrato, não possam ser realizados pelo pessoal da própria instituição.

Em conclusão, o processo formal de trabalho para gestão dos contratos de TI é uma necessidade que menos da metade (45%) das organizações consultadas adota. 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

No Brasil, apesar do processo orçamentário ser regulamentado na área pública, para se prever adequadamente o valor necessário para a área de TI, são necessários dois elementos essenciais: planejamento e controle.

O planejamento estratégico de TI, aliado com os planos de ação e as decisões do comitê diretivo de TI, indica quais gastos deverão ser realizados, a prioridade na execução financeira e como se dará a expansão dos serviços de TI. O controle das atividades de TI, por sua vez, indica as ações que atingem os resultados esperados e aquelas que precisam ser modificadas para alcançar os objetivos determinados. O acompanhamento dos gastos de TI é um dos componentes essenciais para o controle eficiente das ações de TI. A partir da análise das informações obtidas no acompanhamento do planejamento e das atividades de TI, pode-se fazer uma previsão orçamentária apropriada para a área de TI. Entretanto, a falta de conhecimento detalhado dos gastos de TI prejudica tal previsão.

Nesse aspecto, observou-se que uma quantidade razoável de organizações participantes do levantamento teve dificuldade de responder rapidamente o total de gastos com TI e como está distribuído esse gasto. Deve-se ressaltar que, sobre esse assunto, o Tribunal já se manifestou no Acórdão nº 371/2008-TCU-Plenário, com determinações à Secretaria do Tesouro Nacional (STN) do Ministério da Fazenda, ao Departamento de Coordenação e Governança das Empresas Estatais (Dest) e à Secretaria de Orçamento Federal (SOF) do Ministério do Planejamento, Orçamento

e Gestão. Com a finalidade de permitir a identificação clara, objetiva e transparente da previsão e da execução dos gastos em TI, foi determinado que estes elaborassem e encaminhassem ao TCU proposta de alteração do Orçamento Geral da União e do Programa de Dispêndios Globais (PDG). No mesmo Acórdão, o Tribunal propôs a criação de uma ou mais ações que agreguem as despesas relacionadas a TI, de elemento de despesa que identifique execução de despesas com bens e serviços de TI e de rubricas próprias de TI tanto para despesas correntes como para despesas de capital.

Apesar de a maioria (61%) dos órgãos/entidades participantes do levantamento afirmar que, em 2006, foram levadas em consideração as ações previstas para o exercício seguinte na solicitação do orçamento para 2007, um percentual significativo (39%) não utilizou essas informações. A partir desses dados, pode-se supor que 39% das organizações consultadas, quando da solicitação de orçamento para a área de TI em 2007, ou repetiram os valores do ano anterior ou simplesmente aplicaram um percentual de aumento linear sobre as despesas realizadas ou, ainda, acrescentaram um valor ao total do ano anterior sem a utilização de um critério transparente.

Diante disso, verifica-se que a elaboração do orçamento para a área de TI nem sempre utiliza os insumos necessários à obtenção de resultado mais próximo da realidade. Isso causa preocupação, já que o controle sobre os gastos de TI é de suma importância para o melhor aproveitamento dos recursos disponíveis, para a solicitação de recursos financeiros adequados à necessidade da área de TI e para 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

A área de TI foi considerada, por muito tempo, uma "caixa preta", sobre a qual a administração tinha pouco controle e da qual não se sabia ao certo o que esperar como benefício para a organização. Com o aumento da importância estratégica das áreas de TI, essa situação não pôde mais se sustentar. Há uma busca pela aplicação de modelos de governança de TI[17], com o objetivo de tornar a área de TI controlável, com resultados mensuráveis e orientada aos objetivos do negócio da organização.

Nessa perspectiva, a auditoria de TI consiste em verificar um ou vários aspectos da governança de TI de uma organização. Note-se que essa ainda é uma definição ampla e abrange vários tipos e perspectivas para auditorias. Assim, uma auditoria de TI pode, por exemplo, avaliar apenas controles de acesso lógico ao ambiente de TI, por meio de análise de vulnerabilidade. Já se for realizada com um objetivo mais gerencial, a auditoria pode avaliar se os processos de TI ligados ao desenvolvimento de sistemas, por exemplo, estão sendo executados conforme a política da empresa e estão gerando sistemas eficazes. Outra possibilidade é uma auditoria para verificar a integridade e fidedignidade das informações armazenadas nas bases de dados da organização. Ou, ainda, pode-se verificar se a contratação de bens e serviços de TI é feita de acordo com as normas da organização e a legislação vigente.

Em termos gerais, a auditoria de TI é, assim, uma ferramenta para avaliar a conformidade, a qualidade, a eficácia e a efetividade de uma área de TI. Por isso mesmo, há uma tendência em incluir/valorizar atividades de auditoria periódica como instrumento para gestão. Um reflexo dessa tendência é o fato de que uma das principais mudanças quando da atualização do Cobit versão 3.0 para a versão 4.0, em 2005, foi o incremento

e a reorganização do domínio de monitoração, que passou a se chamar "Monitoração e Avaliação", como descrito no Apêndice V do Cobit 4.1, que sinaliza que esse domínio passou a ser visto como parte do processo de melhoria da governança de TI.

Por isso, foram incluídas nesse levantamento questões para verificar se esse tipo de auditoria é realizado nos órgãos/entidades pesquisados da Administração Pública Federal. Alguns dentre os órgãos/entidades pesquisados têm, por força de legislação, a obrigação de executar periodicamente auditorias independentes em várias áreas, inclusive em TI.

Outro objetivo é verificar se os órgãos/entidades possuem a figura do auditor interno de TI. Esse papel é, em muitos aspectos, complementar ao do auditor externo: o auditor interno não apenas verifica a abrangência e efetividade dos controles internos de TI[18] em sua auditoria, como também é agente de melhoria desses controles e, assim, pode ser um agente de melhoria da própria gestão.

Auditorias de TI ainda são pouco freqüentes 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, conseqüentemente, promover a melhoria da sua governança de TI.

Conclusão

O objetivo desse levantamento foi obter informações para elaboração de mapa com a situação da governança de TI na Administração Pública Federal. Ao final do processo, 255 órgãos/entidades representativos da Administração Pública Federal enviaram tais informações ao TCU por meio de questionário eletrônico elaborado pela Sefti. Dessa relação, constaram os ministérios, as universidades federais, os tribunais federais, as agências reguladoras e as principais autarquias, secretarias, departamentos e empresas estatais.

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. 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. O Tribunal já acertou, inclusive, ao editar, em 2003 e 2007, a "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, a integridade e a disponibilidade das informações tratadas pelos órgãos/entidades da Administração Pública Federal.

Assim, existe um campo vasto para atuação desse 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.

BENEFÍCIOS DESTE LEVANTAMENTO

As informações coletadas no presente trabalho possibilitarão à Sefti o planejamento de ações de controle mais efetivas para atingir seu objetivo de aperfeiçoar a governança de TI nos principais órgãos/entidades da Administração Pública Federal. As equipes de futuras fiscalizações na área de TI terão à disposição informações que auxiliarão o planejamento de seus trabalhos. Além disso, a Sefti contará com repositório de contatos dos gestores de TI dos órgãos/entidades participantes do levantamento.

ACÓRDÃO Nº 1603/2008 – TCU – PLENÁRIO

1. Processo: n.º TC - 008.380/2007-1 (com 9 anexos)

2. Grupo I; Classe de Assunto: V - Levantamento de Auditoria

3. Interessado: Congresso Nacional

4. Órgão: Diversos órgãos e entidades da Administração Pública Federal

5. Relator: Ministro Guilherme Palmeira

6. Representante do Ministério Público: não atuou

7. Unidade Técnica: Secretaria de Fiscalização de Tecnologia da Informação – Sefti

8. Advogado constituído nos autos: não há

9. Acórdão:

VISTOS, relatados e discutidos estes autos de Levantamento de Auditoria efetuado pela Secretaria de Fiscalização de Tecnologia da Informação – Sefti, junto a diversos órgãos e entidades da Administração Pública Federal, com vistas a obter informações acerca da situação da gestão e do uso de Tecnologia da Informação – TI.

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

9.1. recomendar ao Conselho Nacional de Justiça - CNJ e ao Conselho Nacional do Ministério Público - CNMP que, nos órgãos integrantes da estrutura do Poder Judiciário Federal e do Ministério Público da União, respectivamente:

9.1.1. promovam ações com o objetivo de disseminar a importância do planejamento estratégico, procedendo, inclusive mediante orientação normativa, ações voltadas à implantação e/ou aperfeiçoamento de planejamento estratégico institucional, planejamento estratégico de TI e comitê diretivo de TI, com vistas a propiciar a alocação dos recursos públicos conforme as necessidades e prioridades da organização;

9.1.2. atentem para a necessidade de dotar a estrutura de pessoal de TI do quantitativo de servidores efetivos necessário ao pleno desempenho das

atribuições do setor, garantindo, outrossim, sua capacitação, como forma de evitar o risco de perda de conhecimento organizacional, pela atuação excessiva de colaboradores externos não comprometidos com a instituição;

9.1.3. orientem sobre a importância do gerenciamento da segurança da informação, promovendo, inclusive mediante normatização, ações que visem estabelecer e/ou aperfeiçoar a gestão da continuidade do negócio, a gestão de mudanças, a gestão de capacidade, a classificação da informação, a gerência de incidentes, a análise de riscos de TI, a área específica para gerenciamento da segurança da informação, a política de segurança da informação e os procedimentos de controle de acesso;

9.1.4. estimulem a adoção de metodologia de desenvolvimento de sistemas, procurando assegurar, nesse sentido, níveis razoáveis de padronização e bom grau de confiabilidade e segurança;

9.1.5. promovam ações voltadas à implantação e/ou aperfeiçoamento de gestão de níveis de serviço de TI, de forma a garantir a qualidade dos serviços prestados internamente, bem como a adequação dos serviços contratados externamente às necessidades da organização;

9.1.6. envidem esforços visando à implementação de processo de trabalho formalizado de contratação de bens e serviços de TI, bem como de gestão de contratos de TI, buscando a uniformização de procedimentos nos moldes recomendados no item 9.4 do Acórdão 786/2006-TCU-Plenário;

9.1.7. adotem providências com vistas a garantir que as propostas orçamentárias para a área de TI sejam elaboradas com base nas atividades que efetivamente pretendam realizar e alinhadas aos objetivos do negócio;

9.1.8. introduzam práticas voltadas à realização de auditorias de TI, que permitam a avaliação regular da conformidade, da qualidade, da eficácia e da efetividade dos serviços prestados;

9.2. recomendar ao Gabinete de Segurança Institucional da Presidência da República - GSI/PR que oriente os órgãos/entidades da Administração Pública Federal sobre a importância do gerenciamento da segurança da informação, promovendo, inclusive mediante orientação normativa, ações que visem estabelecer e/ou aperfeiçoar a gestão da continuidade do negócio, a gestão de mudanças, a gestão de capacidade, a classificação da informação, a gerência de incidentes, a análise de riscos de TI, a área específica para gerenciamento da segurança da informação, a política de segurança da informação e os procedimentos de controle de acesso;

9.3. recomendar à Controladoria-Geral da União - CGU que realize regularmente auditorias de TI e/ou promova ações para estimular a realização dessas auditorias nos órgãos/entidades da Administração Pública Federal;

9.4. recomendar ao Ministério do Planejamento, Orçamento e Gestão - MPOG que, nos órgãos/entidades da Administração Pública Federal:

9.4.1. promova ações com o objetivo de disseminar a importância do planejamento estratégico, procedendo, inclusive mediante orientação normativa, à execução de ações voltadas à implantação e/ou aperfeiçoamento de planejamento estratégico institucional, planejamento estratégico de TI e comitê diretivo de TI, com vistas a propiciar a alocação dos recursos públicos conforme as necessidades e prioridades da organização;

9.4.2. atente para a necessidade de dotar a estrutura de pessoal de TI do quantitativo de servidores efetivos necessário ao pleno desempenho das atribuições do setor, garantindo, outrossim, sua capacitação, como forma de evitar o risco de perda de conhecimento organizacional, pela atuação excessiva de colaboradores externos não comprometidos com a instituição;

9.4.3. estimule a adoção de metodologia de desenvolvimento de sistemas, procurando assegurar, nesse sentido, níveis razoáveis de padronização e bom grau de confiabilidade e segurança;

9.4.4. promova ações voltadas à implantação e/ou aperfeiçoamento de gestão de níveis de serviço de TI, de forma a garantir a qualidade dos serviços prestados internamente, bem como a adequação dos serviços contratados externamente às necessidades da organização;

9.4.5. adote providências com vistas a garantir que as propostas orçamentárias para a área de TI sejam elaboradas com base nas atividades que efetivamente pretendam realizar e alinhadas aos objetivos de negócio;

9.5. recomendar à Diretoria-Geral do Senado Federal e à Diretoria-Geral da Câmara dos Deputados que adotem, no âmbito de suas Casas Legislativas, as providências contidas no item 9.1;

9.6. recomendar à Secretaria-Geral da Presidência - Segepres e à Secretaria-Geral de Administração - Segedam que adotem, no âmbito deste Tribunal, as providências contidas no item 9.1;

9.7. determinar à Secretaria-Geral de Controle Externo - Segecex que oriente suas unidades técnicas para considerarem as informações armazenadas na Secretaria de Fiscalização de Tecnologia da Informação – Sefti quando forem executar ações de controle em governança de TI;

9.8. reiterar diligência aos órgãos/entidades que não responderam ou que não completaram as respostas à pesquisa levada a efeito pela Secretaria de Fiscalização de Tecnologia da Informação - Sefti, fixando prazo de 30 (trinta) dias para que sejam enviados, em meio magnético, conforme orientação daquela Secretaria, as informações necessárias para resposta ao questionário utilizado neste levantamento;

9.9. determinar à Secretaria de Fiscalização de Tecnologia da Informação - Sefti que realize fiscalizações nas áreas consideradas mais críticas da governança de TI nos órgãos/entidades fiscalizados e organize outros levantamentos com o intuito de acompanhar e manter base de

dados atualizada com a situação da governança de TI na Administração Pública Federal;

9.10. remeter cópias do presente Acórdão, acompanhado do Relatório e Voto que o fundamentam, bem como cópia integral do Relatório de Levantamento à Comissão de Ciência, Tecnologia, Inovação, Comunicação e Informática do Senado Federal; à Subcomissão Permanente de Serviços de Informática do Senado Federal; à Diretoria-Geral do Senado Federal; à Secretaria Especial de Informática do Senado Federal - Prodasen; à Comissão de Fiscalização Financeira e Controle da Câmara dos Deputados; à Comissão de Trabalho, de Administração e Serviço Público da Câmara dos Deputados; à Comissão de Ciência e Tecnologia, Comunicação e Informática da Câmara dos Deputados; à Subcomissão Permanente de Ciência e Tecnologia e Informática da Câmara dos Deputados; à Diretoria-Geral da Câmara dos Deputados; ao Centro de Informática da Câmara dos Deputados; ao Conselho Nacional de Justiça; ao Conselho Nacional do Ministério Público; ao Gabinete de Segurança Institucional da Presidência da República; à Controladoria-Geral da União; ao Ministério do Planejamento, Orçamento e Gestão; à Secretaria de Logística Tecnologia da Informação - SLTI do Ministério do Planejamento, Orçamento e Gestão; à Secretaria de Orçamento Federal - SOF do Ministério do Planejamento, Orçamento e Gestão; ao Departamento de Coordenação e Controle das Empresas Estatais - Dest da Secretaria-Executiva do Ministério do Planejamento, Orçamento e Gestão; aos órgãos/entidades que responderam à pesquisa promovida pela Sefti (Apêndice II do Relatório);

9.11. autorizar, a partir da data do acórdão que vier a ser proferido, a divulgação das informações consolidadas constantes deste levantamento em sumários executivos e informativos;

9.12. arquivar os presentes autos na Secretaria de Fiscalização de Tecnologia da Informação - Sefti.

10. Ata nº 32/2008 – Plenário

11. Data da Sessão: 13/8/2008 – Ordinária

12. Código eletrônico para localização na página do TCU na Internet: AC-1603-32/08-P

13. Especificação do quórum:

13.1. Ministros presentes: Walton Alencar Rodrigues (Presidente), Marcos Vinicios Vilaça, Valmir Campelo, Guilherme Palmeira (Relator), Ubiratan Aguiar, Benjamin Zymler, Augusto Nardes, Aroldo Cedraz e Raimundo Carreiro.

13.2. Auditores presentes: Augusto Sherman Cavalcanti, Marcos Bemquerer Costa e André Luís de Carvalho.

WALTON ALENCAR RODRIGUES
Presidente

GUILHERME PALMEIRA
Relator

Fui presente:
PAULO SOARES BUGARIN
Procurador-Geral, em exercício

NOTAS

[1] Cobit 4.1 - PO1.2 *Business-IT Alignment* (Alinhamento de TI com negócio – Estabelecer processos de educação bidirecional e de envolvimento recíproco no planejamento estratégico para obtenção de alinhamento e integração entre o negócio e as ações de TI. As prioridades devem ser acordadas mutuamente a partir da negociação das necessidades do negócio e da área de TI).

[2] Cobit 4.1 - PO1.4 *IT Strategic Plan* (Plano Estratégico de TI – Criar um plano estratégico que defina, em cooperação com os principais interessados, como as metas de TI contribuirão para os objetivos estratégicos da organização e quais os custos e riscos associados. O plano deve incluir os serviços de TI, os ativos de TI e como a área de TI dará suporte aos projetos dependentes de tecnologia da informação. A área de TI deve definir como os objetivos serão alcançados, as métricas a serem usadas e os procedimentos para obter a aprovação formal dos interessados. O plano estratégico de TI deve conter orçamento para investimentos e custeio de TI, fontes de recursos, estratégia de aquisições, e requisitos legais e regulatórios. O plano estratégico deve ser suficientemente detalhado para permitir a definição de planos táticos de TI).

[3] Cobit 4.1 - PO4.3 *IT Steering Committee* (Comitê Diretivo de TI – Criar um comitê diretivo de TI (ou equivalente) composto de gerentes executivos, de negócios e de TI, para: determinar as prioridades de investimento e alocação de recursos nas ações de TI, alinhadas às estratégias e prioridades da organização; acompanhar o estágio de desenvolvimento dos projetos e resolver conflitos relativos a recursos; e monitorar os níveis de serviço de TI e suas melhorias).

[4] Cobit 4.1 - PO7.5 *Dependence Upon Individuals* (Dependência em Indivíduos – Minimizar a ocorrência de dependência crítica em indivíduos chave por meio de aquisição de conhecimento (documentação), compartilhamento de conhecimento, planejamento de sucessão e equipe reserva).

[5] Cobit 4.1 - PO7.2 *Personnel Competencies* (Competências Pessoais – Regularmente verificar que os profissionais de TI têm as competências necessárias para exercer sua função com base em sua formação, treinamento e/ou experiência. Definir as competências de TI básicas e verificar que são mantidas, por meio de programas de qualificação e certificação quando apropriados).

[6] Decreto nº 5.707, de 23 de fevereiro de 2006, art. 3º, incisos VI e VII.

[7] Característica que impede a negação da autoria/execução de uma ação por parte de um agente. Por exemplo: um usuário pode alegar que, dadas as fragilidades à fraude do protocolo padrão de *e-mail*, uma determinada correspondência eletrônica não foi de fato enviada por ele, apesar de aparecer seu nome como remetente, negando sua autoria. Nesse caso, um *e-mail* dotado de não-repúdio deveria possuir uma característica que garantisse que apenas o usuário listado no remetente poderia de fato

ter escrito aquele texto e o enviado. Isso pode ser conseguido, por exemplo, por meio de assinatura digital.

[8] O Decreto nº 3.505, de 13 de junho de 2000, instituiu a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal e tem alcance sobre muitas instituições pesquisadas neste levantamento. Esse documento, porém, é uma norma à qual a PSI específica deve aderir.

[9] O Decreto nº 4.553 de 27 de dezembro de 2002 estabelece um esquema de classificação da informação quanto ao sigilo e tem alcance sobre muitas instituições pesquisadas. Esse documento, porém, é uma norma à qual o esquema de classificação específico deve aderir.

[10] Numa perspectiva mais atual, espera-se que a área de TI seja mais estratégica e não simplesmente "entregue sistemas", mas forneça "soluções de TI" – um conceito mais amplo que engloba serviços, infra-estrutura e sistemas de informação, todos sintonizados com as prioridades da organização.

[11] Área do conhecimento da informática, voltada para a especificação, desenvolvimento e manutenção de sistemas, que aplica tecnologias e práticas de ciência da computação, gerência de projetos e outras disciplinas, objetivando organização, produtividade e qualidade.

[12] Programa que procura estimular a adoção de normas, métodos, técnicas e ferramentas da qualidade e da engenharia de software, bem como promover a melhoria da qualidade dos processos, produtos e serviços de software brasileiros, de modo a tornar as empresas mais capacitadas a competir em um mercado globalizado. Embora voltado para empresas em geral, uma de suas estratégias é fomentar a qualidade de software em empresas e organismos governamentais.

[13] Modelo de qualidade de processo voltado para a realidade do mercado de empresas de desenvolvimento de software no Brasil, compatível com outros padrões internacionais, como a *Capability Maturity Model Integration* (CMMI).

[14] "9.1.11. defina os parâmetros que deverão ser utilizados para balizar a mensuração da disponibilidade da rede corporativa de computadores, incluindo o horário que será considerado na medição da variável, a abrangência da responsabilidade da contratada e a forma de contabilização das paradas para manutenção no percentual de disponibilidade, entre outros pontos que venham a ser considerados cabíveis;"

[15] "9.1.2. faça constar do edital a metodologia de mensuração de serviços e resultados, inclusive os critérios de controle e remuneração dos serviços executados, relativamente ao item 1.2 do objeto, levando em consideração a determinação contida no item 9.1.1 supra e as determinações exaradas nos Acórdãos do Plenário 667/2005, 2.103/2005, 2.171/2005 e 2.172/2005;"

[16] "9.3.22. caso entendam necessário incluir a exigência de "Acordo de Nível de Serviço" no contrato a ser celebrado, especifiquem com precisão, no edital, discriminadamente (...)"

[17] Segundo a definição contida no Cobit 4.1, governança de TI é um conjunto composto de liderança, estruturas organizacionais e processos que garantem que a área de TI da organização apóia e expande os objetivos e estratégias da organização.

[18] Políticas, procedimentos, práticas e estruturas organizacionais desenhadas para garantir o efetivo alinhamento da TI ao seu próprio modelo de governança, e que os desvios sejam prevenidos ou detectados e corrigidos.

Responsabilidade Editorial

Secretaria-Geral de Controle Externo
Secretaria de Fiscalização de Tecnologia da Informação

Equipe de Auditoria
André Luiz Furtado Pacheco (coordenador)
Cláudia Augusto Dias (supervisora)
Luisa Helena Santos Franco
Roberta Ribeiro de Queiroz Martins (supervisora)

Capa e Editoração

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

Impresso pela Sesap/Segedam

TRIBUNAL DE CONTAS DA UNIÃO

Endereço para contato, solicitação de exemplares e consulta na Internet

TRIBUNAL DE CONTAS DA UNIÃO
Secretaria de Fiscalização de
Tecnologia da Informação (Sefti)
SAFS, Quadra 4, Lote 1
Anexo II, 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.