**Identificação**

Acórdão 1603/2008 - Plenário

**Número Interno do Documento**

AC-1603-32/08-P

**Grupo/Classe/Colegiado**

GRUPO I / CLASSE V / Plenário

**Processo**

008.380/2007-1

**Natureza**

Levantamento de Auditoria

**Entidade**

Órgão: Diversos órgãos e entidades da Administração Pública Federal

**Interessados**

Interessado: Congresso Nacional

**Sumário**

LEVANTAMENTO DE AUDITORIA. SITUAÇÃO DA GOVERNANÇA DE TECNOLOGIA DA INFORMAÇÃO - TI NA ADMINISTRAÇÃO PÚBLICA FEDERAL. AUSÊNCIA DE PLANEJAMENTO ESTRATÉGICO INSTITUCIONAL. DEFICIÊNCIA NA ESTRUTURA DE PESSOAL. TRATAMENTO INADEQUADO À CONFIDENCIALIDADE, INTEGRIDADE E DISPONIBILIDADE DAS INFORMAÇÕES. RECOMENDAÇÕES

**Assunto**

Levantamento de Auditoria

**Ministro Relator**

Guilherme Palmeira

**Representante do Ministério Público**

não atuou

**Unidade Técnica**

Secretaria de Fiscalização de Tecnologia da Informação - Sefti

**Advogado Constituído nos Autos**

não há

**Dados Materiais**

(com 9 anexos)

**Relatório do Ministro Relator**

Reproduzo, no essencial, o Relatório da equipe da Secretaria de Fiscalização de Tecnologia da Informação - Sefti encarregada dos trabalhos, com cujas conclusões manifestaram-se de acordo a Diretora e o Secretário:

"2. Introdução

1. Este levantamento foi autorizado pelo Acórdão 435/2007 - 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".

Visão geral

2. O objetivo da governança de TI é assegurar que as ações de TI estejam alinhadas com o negócio da organização, agregando-lhe valor. O desempenho da área de TI deve ser medido, os recursos propriamente alocados e os riscos inerentes, mitigados. Assim, é possível gerenciar e controlar as iniciativas de TI nas organizações para garantir o retorno de investimentos e a adoção de melhorias nos processos organizacionais.

3. A governança adequada da área de tecnologia da informação na Administração Pública Federal promove a proteção a informações críticas e contribui para que essas organizações atinjam seus objetivos institucionais. Além disso, garantir a correta aplicação dos recursos empregados em tecnologia da informação se torna cada vez mais importante, tendo em vista que somente na Administração Federal o gasto em TI ultrapassa seis bilhões de reais por ano, segundo dados do Sistema Integrado de Administração Financeira (Siafi) e do Departamento de Coordenação e Governança das Empresas Estatais (Dest), obtidos pela Sefti em levantamento realizado em 2007 (TC-007.972/2007-8).

Objetivos e questões de Auditoria

4. 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.

5. Durante a fase de planejamento, a equipe do levantamento realizou diversas reuniões com a equipe de analistas da Sefti e formulou as seguintes questões de Auditoria:

Q1. É feito planejamento estratégico institucional e de TI nos órgãos/entidades?

Q2. Qual o perfil dos recursos humanos da área de TI quanto à formação, vínculo com a organização e pré-requisitos para ocupação de funções comissionadas?

Q3. São efetuadas ações e procedimentos que contribuam para a minimização dos riscos e o aumento no nível de segurança das informações dos órgãos/entidades?

Q4. O desenvolvimento de sistemas segue alguma metodologia? Os órgãos/entidades mantêm inventário dos principais sistemas e bases de dados?

Q5. Os órgãos/entidades gerenciam os acordos de níveis de serviço tanto quando prestam internamente como quando contratam externamente serviços de TI?

Q6. O processo de contratação de bens e serviços de TI é formalizado, padronizado e judicioso quanto ao custo, à oportunidade e aos benefícios advindos das contratações de TI?

Q7. O processo de gestão dos contratos de TI é formalizado, padronizado e executado?

Q8. Os órgãos/entidades solicitam o orçamento de TI com base no planejamento da área e controlam os gastos com TI ao longo do exercício financeiro?

Q9. Os órgãos/entidades realizam Auditorias de TI nas suas organizações?

Estratégia metodológica e limitações

6. 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.

7. 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)".

8. 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.

9. 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.

10. 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.

11. 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.

12. 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.

13. 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.

14. 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.

Volume de recursos fiscalizados

15. Conforme a Portaria n.º 222, de 10 de novembro de 2003, a mensuração do volume de recursos fiscalizados não se aplica a este instrumento de fiscalização.

Benefícios estimados

16. Os benefícios estimados do presente trabalho são a possibilidade da Sefti planejar ações a serem realizadas com intuito de aperfeiçoar a governança de TI nos principais órgãos/entidades da APF e a disponibilidade de informações importantes nessa área às equipes de futuras fiscalizações. Além disso, a Sefti contará com um repositório com os contatos dos gestores de TI dos órgãos/entidades participantes do levantamento.

3. Planejamento estratégico institucional e de TI

17. O contexto atual de intensas mudanças faz com que as organizações tenham que se adaptar rapidamente às alterações do ambiente em que atuam. No entanto, há organizações que ainda atuam de maneira reativa, apenas respondendo às demandas geradas por essas mudanças. Há gestores que ainda acreditam ser impossível definir estratégias de ação devido à rapidez e à constância dessas mudanças.

18. Dentro desse cenário de instabilidade, o planejamento tem se tornado cada vez mais importante e vital e deve ser construído de maneira flexível, com o engajamento e comprometimento de todos os colaboradores da organização. As organizações que não planejam correm riscos de não alcançarem os objetivos desejados. Com uma visão de futuro estabelecida, as organizações poderão se adaptar às constantes mudanças que ocorrem na sua área de atuação e agilizar seu processo de tomada de decisões.

19. O planejamento estratégico torna-se uma importante ferramenta para a tomada de decisão e faz com que os gestores estejam aptos a agir com iniciativa, de forma pró-ativa, contra as ameaças e a favor das oportunidades identificadas nas constantes mudanças que ocorrem.

20. O alinhamento de todos os planos, recursos e unidades organizacionais é um fator fundamental para que a estratégia delineada no planejamento possa ser implementada. Assim, o planejamento estratégico de TI tem que estar alinhado com os planos de negócio da organização para o estabelecimento das prioridades e das ações a serem realizadas na área de TI.

Achado I. Ausência de planejamento estratégico institucional em vigor

21. 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.

22. O confronto desses dados com a informação de que 59% das organizações pesquisadas não fazem planejamento estratégico de TI (Achado II), permite algumas análises. Dos 47% dos órgãos/entidades que afirmaram não possuir planejamento estratégico institucional, 81%, isto é, 97 órgãos/entidades não possuem planejamento estratégico de TI (Gráfico 1).

23. 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).

24. Deve-se destacar, mais uma vez, a importância do planejamento estratégico institucional para a governança de TI. Para que o planejamento estratégico de TI seja efetivo e proporcione os resultados esperados, ele deve estar alinhado ao planejamento estratégico institucional. A falta deste impede o alinhamento desejado e ainda dificulta o estabelecimento de diretrizes para a área de TI.

Planejamento Estratégico de TI

Gráfico 1 - Planejamento estratégico

Critérios

a) 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);

b) Acórdão 1.558/2003-TCU-Plenário, item 9.3.9.

Evidências

a) Apêndice I, planilha de resultados, pergunta: 1. Há planejamento institucional em vigor? (fl. 37).

Efeitos potenciais

a) Suporte ineficaz da área de TI na consecução da missão da organização;

b) Decisões dos gestores de TI incompatíveis com as necessidades da organização;

c) Alocação indevida de recursos de TI por falta de entendimento sobre as prioridades da organização;

d) Desperdício de recursos devido a decisões erradas acerca da alocação de recursos de TI.

Achado II. Ausência de planejamento estratégico de TI em vigor

25. Por sua magnitude, o percentual de órgãos/entidades que não dispõem de planejamento estratégico de TI em vigor, 59 %, chama a atenção. Evidentemente, não se deve confundir o fato de não possuir planejamento estratégico com o fato de não possuir planejamento algum. Os órgãos/entidades podem possuir algum tipo de planejamento, normalmente um plano de ação anual. Apesar de necessários, os planos de ação anuais são insuficientes porque não conseguem indicar caminhos e estratégias, apenas prevêem como serão alocados os recursos disponíveis naquele ano. Além disso, esses planos não são bons instrumentos para acompanhar e apoiar os projetos de média e longa durações, comuns na área de TI. Outro problema normalmente observado quando da ausência de planejamento estratégico é a descontinuidade desses projetos e o conseqüente desperdício de recursos.

26. O planejamento estratégico de TI deve indicar os projetos e serviços de TI que receberão recursos, os custos, as fontes de recursos e as metas a serem alcançadas. Deve ser uma atividade regular e os documentos resultantes devem ser aprovados pela alta administração.

27. Além disso, ao analisar superficialmente algumas das evidências apresentadas como planos estratégicos de TI por órgãos/entidades participantes do levantamento, a equipe observou que vários desses documentos eram cartas de intenção internas da área de TI e/ou projetos de planos, e não propriamente planos estratégicos de TI.

Critérios

a) 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);

b) Acórdão 1.558/2003-TCU-Plenário, item 9.3.9.

Evidências

a) Apêndice I, planilha de resultados, pergunta: 2. Há planejamento estratégico para a área de TI em vigor? (fl. 37).

Efeitos potenciais

a) Suporte ineficaz da área de TI na consecução da missão da organização;

b) Planos de TI não alinhados às necessidades do negócio;

c) Inexistência de consultas regulares entre gerente de TI e demais gerentes acerca dos projetos e serviços de TI;

d) Enfraquecimento das ações de TI;

e) Descontinuidade dos projetos de TI;

f) Insatisfação dos usuários;

g) Visão negativa da área de TI;

h) Resultados da área de TI abaixo do esperado;

i) Dificuldade de obtenção de recursos para a área de TI;

j) Investimentos desnecessários em TI;

k) Desperdício de recursos.

Achado III. Ausência de comitê diretivo sobre ações e investimentos em TI

28. A existência de um comitê diretivo de TI (IT Steering Committee), 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 desse comitê ser composto por dirigentes de TI e de outras áreas da organização possibilita que as decisões de investimentos sejam obtidas a partir de uma visão mais abrangente, o que reduz os riscos de erro.

29. Menos de um terço (32 %) dos órgãos/entidades pesquisados declararam possuir um comitê diretivo de TI ou algo equivalente. Por não haver um fórum competente para discussão, as decisões sobre investimentos em TI correm maior risco de serem equivocadas e levarem ao desperdício de recursos, e ainda de não estarem alinhadas aos objetivos da organização.

Critérios

a) 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).

Evidências

a) Apêndice I, planilha de resultados, pergunta: 3. Há comitê que decida sobre a priorização das ações e investimentos de TI? (fl. 37).

Efeitos potenciais

a) Estratégia de TI não alinhada com a estratégia da organização;

b) Apoio inexistente ou insuficiente dos projetos baseados em TI aos objetivos institucionais;

c) Apoio e envolvimento insuficientes da administração nas decisões essenciais da área de TI.

Conclusão

30. Tendo em vista os dados apresentados, pode-se inferir que a falta de planejamento estratégico institucional inibe e/ou prejudica o planejamento das ações de TI. Desse fato podem decorrer ações de TI equivocadas que levam a desperdício de recursos. 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.

31. 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% de 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.

32. 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.

Proposta de encaminhamento

33. Recomendar à Secretaria de Logística e Tecnologia da Informação (SLTI) do Ministério do Planejamento, Orçamento e Gestão, ao Conselho Nacional de Justiça e ao Conselho Nacional do Ministério Público que promovam ações com objetivo de disseminar a importância do planejamento estratégico e induzir, mediante orientação normativa, os órgãos/entidades da Administração Pública Federal a realizarem ações para implantação e/ou aperfeiçoamento de planejamento estratégico institucional, planejamento estratégico de TI e comitê diretivo de TI.

4. Estrutura de pessoal de TI

34. Em qualquer área de atuação técnica da organização é crítica a adequação da estrutura de pessoal - e não é diferente quando nos referimos à tecnologia da informação. O TCU tem observado esse requisito na administração pública brasileira a fim de fornecer orientações adequadas com base em observações feitas em Auditorias relacionadas à TI (exemplos: Acórdão 667/2005-TCU-Plenário ; Acórdão 2.023/2005-TCU-Plenário ; e Acórdão 786/2006-TCU-Plenário ).

35. Um marco importante é o Acórdão 140/2005-TCU-Plenário, no qual o Relator expressa sua preocupação com os recursos humanos da área de TI de toda a administração pública:

I -

II -

III - "Existe, pois, um núcleo de atividades de informática que são estratégicas: ou porque lidam com informações privilegiadas, ou porque tratam da fiscalização dos contratos, ou porque delas depende o funcionamento do próprio setor e das demais unidades que utilizam seus serviços, ou porque envolvem a tomada de decisão sobre a realização de despesas de vulto na aquisição de bens e contratação de serviços. Quando essas atividades não são regularmente executadas, as chances de serem causados prejuízos à Administração aumentam consideravelmente. Portanto, não é razoável que esses encargos sejam exercidos por servidores sem qualificação ou, dado o conflito de interesses, sejam "delegados" a pessoal terceirizado em razão das deficiências no quadro do órgão público.

IV - Não me parece que a situação constatada no Ministério da Agricultura seja um caso isolado, visto que a carência de recursos humanos na Administração Pública Federal é fato notório".

V -

VI -

36. Uma das determinações desse Acórdão foi a realização de Auditoria para avaliar a adequação da estrutura de pessoal de TI , que motivou a inclusão, no presente trabalho, de questões sobre aspectos de recursos humanos apontados no Acórdão.

37. A necessidade de haver uma quantidade mínima de servidores da área de TI do órgão/entidade, em relação à quantidade daqueles que atuam na área mas não são servidores efetivos, foi uma das preocupações do Acórdão para evitar que ações críticas ou estratégicas de TI sejam delegadas a pessoal terceirizado em função da ausência de quadro mínimo. Para avaliar essa situação na Administração Pública Federal, os gestores participantes deste levantamento foram questionados quanto à composição do seu quadro de TI, no que diz respeito ao vínculo com a administração, considerando os profissionais que trabalham nas dependências do órgão (servidores, comissionados e terceirizados). É importante ressaltar que não foram computados aqui os profissionais que trabalham na execução de serviços para projetos específicos, executados primordialmente no ambiente da contratada.

38. Outro aspecto importante é a qualificação dos profissionais em relação às atividades que deve desempenhar a área de TI dos órgãos/entidades. Nesse caso, há duas preocupações: qualificação gerencial e qualificação técnica em TI. Quanto à qualidade dos gerentes, a estratégia utilizada foi levantar, no presente questionário, se há critérios para concessão das funções comissionadas de TI nos órgãos/entidades. Já a qualificação técnica foi examinada a partir do nível de formação dos profissionais em TI, desde a graduação - que não é obrigatória para a investidura em cargo de TI, por não haver regulamentação da profissão - até pós-graduações formais. Optou-se, nesse primeiro momento, por não levantar treinamentos técnicos específicos (certificações, cursos de atualização, congressos) que, apesar de extremamente necessários para a área, não permitiriam uma tabulação em função da diversidade. Finalmente, foi verificado também se os órgãos/entidades possuem carreira específica para a área de TI.

39. Vale ressaltar que as verificações realizadas quanto à quantidade dos profissionais e sua qualificação não são exaustivas para traçar o perfil do corpo técnico de TI dos órgãos/entidades, mas apenas um ponto de partida para fornecer subsídios ao direcionamento de ações de Auditoria específicas. Além disso, outros indicadores de qualidade, como o nível de rotatividade do pessoal, porcentagem de certificações técnicas, existência de planos de treinamento regulares, aderência do corpo técnico a esses planos, nível de satisfação dos clientes com a qualidade do corpo técnico e outros, apontados pelo Cobit na gestão de pessoal, foram deixados para próximas edições deste levantamento.

Achado IV. Quantidade reduzida de servidores na área de TI

40. Uma quantidade expressiva de órgãos/entidades (95%) informou que possui algum servidor do seu quadro atuando na área de TI. Contudo, ao verificar-se a proporção entre servidores do quadro e colaboradores externos a ele, é possível observar ainda a ocorrência de muitos colaboradores externos em alguns órgãos/entidades. O Gráfico 2 mostra três grupos de órgãos/entidades: aqueles com mais de 2/3 do seu quadro composto por servidores, aqueles nos quais esse valor está entre 1/3 e 2/3, e aqueles onde os servidores constituem menos de 1/3 do quadro.

Gráfico 2 - Servidores/terceirizados na área de TI

41. É importante ressaltar que não há uma resposta definitiva, nem na literatura especializada, nem em estatísticas, para a questão: "o quanto podemos terceirizar?". Uma grande quantidade de terceirizados e de outros colaboradores externos representa um aumento do risco organizacional, especialmente se associado a controles fracos, terceirização da "inteligência" da organização ou de atividades estratégicas. Sozinha, entretanto, é apenas um indício de que pode haver dificuldade na gestão desses colaboradores e um alerta para o Auditor sobre a necessidade de considerar crítica a inexistência de controles sobre eles.

42. Seguindo esse raciocínio, verificou-se que dentre os 70 órgãos pesquisados (29%) com área de TI composta de menos de 1/3 de servidores do quadro, 63% também não têm planejamento estratégico de TI (Gráfico 2). Ao mesmo tempo em que aumenta o risco de ausência de controles, a ausência de planejamento aponta uma potencial dificuldade de alocação de recursos humanos necessários à realização das ações de TI.

43. Finalmente, a maior quantidade de colaboradores externos ao quadro dos órgãos/entidades pesquisados aumenta o risco de perda de conhecimento organizacional, na medida em que esse conhecimento esteja depositado em indivíduos sem vínculo e menos compromissados com a organização. Quanto menor o quadro de servidores, maior a probabilidade de que algum conhecimento fique somente entre os colaboradores externos e, portanto, maior o risco de que esse conhecimento se perca.

Critérios

a) Acórdão 140/2005-TCU-Plenário;

b) 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).

Evidências

a) Apêndice I, planilha de resultados, pergunta: 4. Há servidores/empregados do quadro que atuam na área de TI desse órgão/entidade? (fl. 37)

Efeitos potenciais

a) Dependência do órgão/entidade de servidores/empregados alheios ao quadro para execução de atividades críticas para o negócio;

b) Aumento de custo para a Administração em contratos onde o contratado não pode ser facilmente substituído sem perda de continuidade de serviços de TI;

c) Inobservância da política de segurança da informação da empresa em função da necessidade de manipulação de informações sigilosas por terceirizados;

d) Conflito de interesses na fiscalização de contratos, quando feita por outros terceirizados.

Achado V. Ausência de formação específica em TI

44. Segundo as informações levantadas no questionário, somente 37% dos servidores que atuam nas áreas de TI dos órgãos/entidades pesquisados possuem formação específica em TI (incluindo aqui doutorado, mestrado, pós-graduação lato sensu e nível superior). A falta de especialização preocupa em função do aumento da importância estratégica da TI para as organizações, pois um quadro menos especializado tende a produzir resultados de mais baixa qualidade.

45. Outra preocupação é que tal perfil leve a organização a buscar no mercado a competência pessoal que lhe falta em seu quadro, seja por meio de terceirizados, seja por meio de requisições/comissões. De acordo com as informações coletadas, entre os colaboradores requisitados há um percentual maior (48%) com formação específica em TI. Não foram coletadas informações sobre a formação de terceirizados.

46. De todo modo, apenas buscar a formação na seleção de colaboradores externos não resolve o problema, pois a equipe interna continua com dificuldades na execução de ações estratégicas e tarefas de fiscalização de contratos terceirizados.

47. Finalmente, há que se considerar que a profissão de analista de sistemas não é regulamentada e, portanto, não há restrição legal para a atuação em TI. Além disso, pode haver dificuldade em especificar nos editais de concurso qual o universo de cursos superiores da área de TI que são aceitáveis para o perfil profissional desejado.

Critérios

a) Acórdão 140/2005-Plenário;

b) 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).

Evidências

a) Apêndice I, planilha de resultados, pergunta: 6. Esse órgão/entidade conhece o grau de formação das pessoas que atuam na área de TI? (fl. 37)

Efeitos potenciais

a) Baixa qualidade dos serviços de TI em função da baixa qualificação da equipe de TI;

b) Órgão/entidade dependente de prestadora de serviços de TI.

Achado VI. Inobservância das competências necessárias para funções comissionadas

48. Um total de 60% dos pesquisados declarou que não considera as competências gerenciais, técnicas e resultados produzidos anteriormente na seleção de pessoas para funções comissionadas na área de TI. O risco nesse caso é uma baixa qualificação do corpo gerencial de TI e o comprometimento dos resultados da área, desde a falta de alinhamento com os negócios até a perda de produtividade da equipe por má gestão.

Critérios

a) Decreto no 5.707, de 23 de fevereiro de 2006, art. 3o, incisos VI e VII.

Evidências

a) Apêndice I, planilha de resultados, pergunta: 8. São consideradas as competências gerenciais, técnicas e resultados produzidos anteriormente na seleção de pessoas para funções comissionadas na área de TI? (fl. 37).

Efeitos potenciais

a) Baixa produtividade da equipe de TI em função da baixa qualidade do corpo gerencial;

b) Falta de alinhamento da TI com o negócio da organização.

Achado VII. Ausência de carreira específica para a área de TI

49. Um total de 57% dos pesquisados informou que não possui carreira específica para a área de TI. Segundo os dados do questionário, os 43% dos órgãos/entidades que têm carreira de TI possuem 2/3 do total de pessoal alocado para TI entre os pesquisados. Em valores absolutos, também há mais profissionais com formação em TI (incluindo doutorado, mestrado, pós-graduação lato sensu e nível superior) nas organizações com carreira específica: 58% dos profissionais com formação em TI estão nessas organizações. Contudo, há que se registrar que, em valores proporcionais, não há diferença significativa entre a formação em TI dos servidores em órgãos com e sem carreira específica (37% e 38% respectivamente - Gráfico 3). Ou seja, mesmo nos órgãos com carreira específica, ainda há muitos servidores sem formação superior em TI ou com formação em nível médio.

Gráfico 3 - Formação dos profissionais de TI

Critérios

a) Cobit 4.1 PO7.1 Personnel Recruitment and Retention (Recrutamento e Retenção de Pessoal - Manter processos de recrutamento de pessoal de TI em linha com as políticas e os procedimentos de pessoal gerais da organização, isto é, contratação, ambiente positivo para o trabalho, orientação. Implementar processos que garantam que a organização tenha força de trabalho de TI apropriadamente preparada com as habilidades necessárias para atingir os objetivos organizacionais).

Evidências

a) Apêndice I, planilha de resultados, pergunta: 4. Há servidores/empregados do quadro que atuam na área de TI desse órgão/entidade? (fl. 37)

b) Apêndice I, planilha de resultados, pergunta: 6. Esse órgão/entidade conhece o grau de formação das pessoas que atuam na área de TI? (fl. 37)

c) Apêndice I, planilha de resultados, pergunta: 7. Há carreiras específicas para a área de TI no plano de cargos do órgão/entidade? (fl. 37)

Efeitos potenciais

a) Insuficiência de servidores para atuar na área de TI.

Conclusão

50. Conforme o Gráfico 2, um total de 29% dos pesquisados possui menos de 1/3 de sua área de TI composta 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.

51. Segundo as informações levantadas no questionário, somente 37% dos servidores que atuam na área 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.

52. 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 nos órgãos/entidades participantes é objetiva e baseada no mérito.

Proposta de encaminhamento

53. Enviar as conclusões acerca de estrutura de pessoal de TI ao Ministério do Planejamento, Orçamento e Gestão, ao Conselho Nacional de Justiça e ao Conselho Nacional do Ministério Público para ciência e promoção das ações cabíveis.

5. Segurança da informação

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

55. 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 . A própria prestação do serviço de uma instituição pública aos cidadãos depende da confiabilidade das informações por ela tratadas e ofertadas.

56. 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.

57. 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 . 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.

58. 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.

59. 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.

60. 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.

61. 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.

62. 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).

63. 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.

64. 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.

65. 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.

66. 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.

Achado VIII. Ausência de política de segurança da informação em vigor

67. A ausência de política de segurança da informação (PSI) formalmente definida na organização foi declarada por 64% dos órgãos/entidades pesquisados. Como esse documento de diretrizes é um dos primeiros passos na construção de uma gestão da segurança da informação, tal achado é um indício preocupante de que essa gestão é inexistente ou incipiente na maioria das organizações da Administração Pública Federal.

68. É possível que haja ações em segurança da informação nesses órgãos. Porém, a ausência da política central indica que tais ações não são motivadas por diretrizes institucionais e, portanto, podem ser conflitantes e/ou incompletas.

Critérios

a) NBR ISO/IEC 17799:2005, item 5.1 - Política de segurança da informação: convém que a direção estabeleça uma política clara, alinhada com os objetivos do negócio e demonstre apoio e comprometimento com a segurança da informação por meio da publicação e manutenção de uma política de segurança da informação para toda a organização;

b) Cobit 4.1 DS5.2 IT Security Plan (Plano de Segurança de TI - Traduzir requisitos de negócio, risco e conformidade num plano geral de segurança de TI, levando em consideração a infra-estrutura de TI e a cultura de segurança. Garantir que o plano seja implementado dentro das políticas e dos procedimentos de segurança em conjunto com investimentos apropriados em serviços, pessoal, software e hardware. Comunicar as políticas e procedimentos de segurança aos interessados e usuários).

Evidências

a) Apêndice I, planilha de resultados, pergunta: 11. Existe política de segurança da informação (PSI) em vigor? (fl. 37).

Efeitos potenciais

a) Enfraquecimento das ações de segurança, por não serem respaldadas por uma política institucional;

b) Descompasso entre a gestão da segurança da informação e os objetivos de negócio;

c) Percepção pelos usuários e clientes de falta de comprometimento da alta administração da organização com a segurança da informação.

Achado IX. Ausência de plano de continuidade de negócios em vigor

69. A cultura de segurança da informação predominante nas organizações brasileiras, inclusive na área governamental, ainda não está madura o suficiente no que diz respeito à preocupação com desastres e interrupção nos serviços. É o que pode ser inferido da ausência de plano de continuidade de negócios (PCN) em cerca de 88% dos pesquisados. A situação se agrava quando, adicionalmente, observa-se que, dentre os que possuem PCN em vigor, apenas 30% declararam tê-lo revisado em período inferior a um ano.

70. A ausência de PCN na organização é um indício de falta de conscientização em nível estratégico com os riscos de interrupção dos serviços da organização. Sem planejamento dessa natureza, a organização fica vulnerável quando da ocorrência de desastres (naturais ou por sabotagem) e interrupções de serviços. Eventos que poderiam ser resolvidos sem grande perda, acabam por comprometer toda a base atual e histórica de informações da organização. Pode ser até que o PCN nunca precise ser acionado mas, se houver a necessidade e ele não existir, isso pode significar risco à continuidade da existência da organização.

71. Ao considerar os efeitos da perda de informações como as relacionadas à vida, à saúde, à segurança e à história dos cidadãos brasileiros, não é aceitável correr riscos elevados que possam comprometer a própria finalidade das instituições governamentais.

Critérios

a) NBR 15999-1:2007, item 8.6 - Planos de Continuidade de Negócios: o propósito de um plano de continuidade de negócios (PCN) é permitir que uma organização recupere ou mantenha suas atividades em caso de uma interrupção das operações normais de negócios.

b) Cobit 4.1 DS4 Ensure Continuous Service (Garantir a Continuidade do Serviço - A necessidade de prover serviços contínuos de TI requer desenvolvimento, manutenção e teste de planos de continuidade de TI, armazenamento de cópias de segurança em local alternativo e treinamento periódico de planejamento de continuidade).

c) NBR ISO/IEC 17799:2005, item 14.1.3 - Desenvolvimento e implementação de planos de continuidade relativos à segurança da informação: convém que os planos sejam desenvolvidos e implementados para a manutenção ou recuperação das operações e para assegurar a disponibilidade da informação no nível requerido e na escala de tempo requerida, após a ocorrência de interrupções ou falhas dos processos críticos do negócio.

Evidências

a) Apêndice I, planilha de resultados, pergunta: 10. Existe plano de continuidade de negócios em vigor? (fl. 37).

Efeitos reais e potenciais

a) Vulnerabilidade das organizações à ocorrência de desastres e interrupção de serviços;

b) Perda de dados, inclusive históricos, de difícil recuperação;

c) Dificuldade no restabelecimento das operações normais quando da ocorrência de interrupção de serviços;

d) Vulnerabilidade a fraudes e erros durante a interrupção de serviços;

e) Paralisação de funções essenciais de governo e/ou de Estado.

Achado X. Ausência de classificação das informações

72. Um total de 80% dos órgãos/entidades declararam não classificar as informações. Esse é um processo caro e trabalhoso, que envolve muitas áreas da organização, e essa é uma possível causa para um percentual tão expressivo.

73. A classificação das informações, porém, de forma semelhante à PSI, é um dos pilares da segurança da informação numa organização. A sua ausência indica que o tratamento da segurança sobre as informações não é feito de forma consistente, variando em função da maior ou menor maturidade das áreas que as armazenam, transportam ou alteram. Assim, pode ser, por exemplo, que uma informação em papel seja tratada com um nível maior de sigilo, mas ao ser passada para um sistema informatizado, receba o tratamento comum dado a outras informações não-sigilosas, inadequado para suas especificidades. Como não existe um rótulo de segurança único para aquela informação, o qual deveria apontar para procedimentos próprios em cada meio de armazenamento, o tratamento da segurança daquela informação torna-se ineficaz como um todo, já que

é uma máxima da segurança da informação que a segurança de um conjunto é igual à segurança do elo mais fraco.

74. Além disso, é difícil responsabilizar alguém por um tratamento indevido sem uma classificação da informação. A declaração expressa de que um dado ativo de informação deve ser tratado com um determinado nível de proteção (e é nisso que consiste a atribuição dos rótulos de segurança às informações) é o subsídio de que dispõe o gestor para avaliar se uma dada ação foi ou não adequada ao nível de proteção da informação e, caso não tenha sido, propor a responsabilização, bem como a correção da situação.

Critérios

a) Cobit 4.1 PO2.3 Data Classification Scheme (Esquema de Classificação da Informação - Estabelecer um esquema de classificação aplicável em toda organização baseado na criticidade e na sensibilidade - isto é, pública, reservada ou sigilosa - das informações institucionais. Esse esquema deve incluir detalhes sobre propriedade da informação; definição de níveis de segurança e controles de proteção adequados; e uma breve descrição dos requisitos de retenção e destruição de dados, criticidade e sensibilidade. Deve ser usado como a base para a aplicação de controles tais como controles de acesso, armazenamento ou encriptação);

b) NBR ISO/IEC 17799:2005, item 7.2 - Classificação da informação: convém que a informação seja classificada para indicar a necessidade, prioridades e o nível esperado de proteção quando do tratamento da informação.

Evidências

a) Apêndice I, planilha de resultados, pergunta 12. É feita classificação de informações? (fl. 37).

Efeitos potenciais

a) Informações tratadas com nível inadequado de proteção, suscetíveis à perda de integridade, confiabilidade e disponibilidade;

b) Tratamento da segurança das informações de maneira inconsistente e dependente do meio em que transitam ou são armazenadas;

c) Falta de amparo para responsabilização por acesso indevido a informações;

d) Falta de sintonia entre a proteção das informações e o negócio da organização.

Achado XI. Ausência de procedimentos de controle de acesso em vigor

75. De acordo com as respostas fornecidas, procedimentos para disciplinar o controle de acesso a recursos computacionais existem em 52% dos pesquisados. É provável que esse resultado seja uma conseqüência da necessidade de controle de acesso lógico em sistemas de informação e sistemas operacionais em geral, que induz a necessidade de definição de normativos de identificação e de senhas, bem como de direitos de acesso para cada usuário ou grupo de usuários. Isso faz com que a situação dos 48% restantes seja crítica.

76. A definição de normativos para controle de acesso é fundamental para sincronizar o controle de acesso às informações com as reais necessidades de acesso dos usuários, garantir o acesso mínimo e necessário a cada informação, isto é, que só tenha acesso a uma informação quem realmente precisa dela, e que toda informação realmente necessária esteja disponível para acesso. A ausência da formalização de normativos é um indício de que o acesso não está definido de forma criteriosa.

77. A ausência de procedimentos é também um indício de que o processo de concessão/manutenção/revogação do acesso conforme definido não é devidamente controlado. O risco dessa ausência de controle é a ocorrência de concessão/manutenção/revogação de acesso a recursos em desconformidade com as reais necessidades de acesso.

Critérios

a) Cobit 4.1 DS5.3 Identity Management (Gerência de Identidade - Garantir que todos usuários (internos, externos e temporários) e sua atividade em sistemas de TI (aplicações do negócio, sistema operacional,

desenvolvimento e manutenção) devem ser unicamente identificáveis. Direitos de acesso do usuário a sistemas e dados devem estar alinhados com as necessidades do negócio e requisitos do cargo definidos e documentados. Direitos de acesso do usuário são requisitados pelo gerente do usuário, aprovados pelo proprietário do sistema e implementados pelo responsável pela segurança. Identidades e direitos de acesso do usuário são mantidos num repositório central. Medidas técnicas e procedimentais são alocadas e mantidas correntes para estabelecer identificação do usuário, implementar autenticação e conceder os direitos de acesso);

b) Cobit 4.1 DS5.4 User Account Management (Gerência de Contas de Usuários - Garantir que requisitar, estabelecer, entregar, suspender, modificar e fechar contas de usuários e respectivos privilégios de usuário é realizado pela gerência de contas de usuário. Deve ser incluído um procedimento de aprovação pelo proprietário do sistema ou dado delineando a concessão de privilégios de acesso. Esses procedimentos devem ser aplicados para todos usuários, incluindo administradores (usuários privilegiados), usuários internos e externos, em uso normal ou em casos de emergência. Direitos e obrigações relativos a acessos a sistemas e dados corporativos são contratualmente ajustados para todos os tipos de usuários. Executar revisão regular gerencial de todas as contas e respectivos privilégios.

c) Cobit 4.1 DS12.2 Physical Security Measures (Medidas de Segurança Física - Definir e implementar medidas de segurança física alinhadas com os requisitos do negócio para assegurar o local e os ativos físicos. Medidas de segurança física devem ser capazes de eficientemente prevenir, detectar e mitigar riscos relativos a roubos, temperatura, incêndio, fumaça, água, tremor de terra, terrorismo, vandalismo, interrupções de energia, produtos químicos ou explosivos);

d) Cobit 4.1 DS12.3 Physical Access (Acesso Físico - Definir e implementar procedimentos para permitir, limitar e revogar acesso aos terrenos, edifícios e áreas de acordo com as necessidades do negócio, inclusive emergências. Acesso aos terrenos, edifícios e áreas deve ser justificado, autorizado, registrado e monitorado. Isso deve ser aplicado a todas as pessoas que entrem na propriedade, incluindo funcionários, temporários, clientes, vendedores, visitantes ou qualquer outro terceiro);

e) NBR ISO/IEC 17799:2005, item 11.1.1 - Política de controle de acesso: convém que a política de controle de acesso seja estabelecida, documentada e analisada criticamente, tomando-se como base os requisitos de acesso dos negócios e segurança da informação.

Evidências

a) Apêndice I, planilha de resultados, pergunta 14. Existem procedimentos definidos que disciplinem o controle de acesso (lógico e físico) a recursos computacionais? (fl. 37).

Efeitos potenciais

a) Perfil de acesso a informações excessivamente permissivo para determinados usuários ou grupos de usuários;

b) Concessão ou alteração do acesso a recurso para pessoas não autorizadas, visando fraudes;

c) Divulgação não autorizada de informação reservada ou sigilosa.

Achado XII. Ausência de área específica para lidar com segurança da informação

78. Um total de 64% dos órgãos/entidades informaram que não possuem área específica, com responsabilidades definidas, para lidar estrategicamente com segurança da informação. Sem tal estrutura, há grande probabilidade de que as questões de segurança não sejam tratadas de maneira consistente. Além disso, torna-se difícil para a organização avaliar se estão sendo endereçados de modo adequado os recursos humanos e de logística para a implementação dos controles de segurança da informação, ou se tais controles estão sintonizados com o negócio da organização. A ausência de fórum adequado, de nível estratégico e com representantes de diversas áreas da organização, também é um indício de ausência de um fator considerado

crítico no sucesso da gestão da segurança: a preocupação da direção da organização com a segurança da informação.

Critérios

a) Cobit 4.1 DS5.1 Management of IT Security (Gerência da Segurança de TI - Gerenciar a segurança de TI no nível organizacional apropriado mais alto de maneira que a gerência de ações de segurança esteja alinhada com os requisitos do negócio);

b) NBR ISO/IEC 17799:2005, item 6.1 - Infra-estrutura da segurança da informação: convém que uma estrutura de gerenciamento seja estabelecida para iniciar e controlar a implementação da segurança da informação dentro da organização.

Evidências

a) Apêndice I, planilha de resultados, pergunta: 9. Existe uma área específica, com responsabilidades definidas, para lidar estrategicamente com segurança da informação? (fl. 37).

Efeitos potenciais

a) Ausência ou atuação deficiente em segurança da informação na organização;

c) Ações de segurança da informação da organização incoerentes e ineficazes;

d) Desperdício de recursos em ações não-prioritárias.

Achado XIII. Ausência de área específica para gerência de incidentes

79. Apesar da gerência centralizada de incidentes ser um dos pontos-chave apontados pela norma NBR ISO/IEC 17799:2005 para resolução rápida de incidentes em TI, não existe área específica para gerência de incidentes em 76% dos órgãos/entidades pesquisados, segundo declarações dos gestores. Tal resultado representa um risco de que eventuais incidentes envolvendo a disponibilidade, a integridade ou o sigilo das informações não tenham tratamento adequado e consistente.

80. Adicionalmente, em outra questão verificou-se que, coincidentemente, apesar de não serem as mesmas instituições, também 76% das organizações pesquisadas oferecem serviços transacionais pela Internet, o que aumenta a sua exposição a tentativas de acesso indevido e à indisponibilidade da informação. Ao cruzar esses dados, verificou-se que 54% dos pesquisados possuem serviços transacionais pela Internet e não possuem área própria para gerência de incidentes. Nesses casos, o risco associado à ausência do controle aumenta.

81. Outro aspecto a considerar é a possibilidade de um incidente em serviços da Internet afetar mais de uma instituição. Nesse caso, a ausência dessa área tem efeito multiplicador e pode, inclusive, comprometer o trabalho dos órgãos que a possuem. Existem grupos articuladores de tratamento de incidentes na Internet, como o Grupo de Resposta a Incidentes de Segurança para a Internet brasileira (CERT.br) e outros grupos localizados, como o Grupo de Incidentes da Rede Nacional de Pesquisa (RNP) e de outros provedores de rede. Sem um contato nos órgãos da administração pública, fica comprometida a atuação de tais entidades na ocorrência de incidentes que afetam várias instituições, inclusive quanto à possibilidade de articulação específica para tratamento de incidentes de órgãos governamentais.

Critérios

a) Cobit 4.1 DS5.5 Security Testing, Surveillance and Monitoring (Teste, Vigilância e Monitoramento de Segurança - Testar e monitorar a implementação da segurança de TI de uma forma pró-ativa. A segurança de TI deve ser formalmente aprovada de uma maneira tempestiva para assegurar a manutenção do padrão estabelecido de segurança da informação da organização. A função de registro e monitoramento permitirá a prevenção e/ou rápida detecção e o subseqüente informe tempestivo de atividades não usuais e/ou anormais que necessitem de tratamento);

b) Cobit 4.1 DS5.6 Security Incident Definition (Definição de Incidente de Segurança - Definir e comunicar claramente as características de potenciais incidentes de segurança para que possam ser corretamente classificados e tratados pelo processo de gestão de problemas e incidentes);

c) NBR ISO/IEC 17799:2005, item 13.2 - Gestão de incidentes de segurança da informação e melhorias: convém que responsabilidades e procedimentos estejam definidos para o manuseio efetivo de eventos de segurança da informação e fragilidades, uma vez que estes tenham sido notificados. Convém que um processo de melhoria contínua seja aplicado às respostas, monitoramento, avaliação e gestão total de incidentes de segurança da informação.

Evidências

a) Apêndice I, planilha de resultados, pergunta 15. Existe uma área específica para gerência de incidentes de segurança? (fl. 37);

b) Apêndice I, planilha de resultados, pergunta: 16. O Órgão/Entidade oferece serviços transacionais via Internet, ou seja, prestação de serviço que pode ser executado do início ao fim pela Internet com troca bidirecional de informações entre o Órgão/Entidade e o cliente? (fl. 37-v).

Efeitos potenciais

a) Tratamento de incidentes inexistente, inadequado ou inconsistente;

b) Inexistência de registro histórico de incidentes, o que dificulta o aprendizado e o tratamento das causas;

c) Maior risco de que indisponibilidades, perdas de integridade ou acessos indevidos tenham maior impacto sobre as informações e, conseqüentemente, sobre o negócio da organização.

Achado XIV. Ausência de gestão de mudanças

82. No escopo da governança de TI, a gestão de mudanças costuma ser um processo de difícil implementação, pois requer a colaboração de quase todas as áreas de TI, desde o desenvolvimento de sistemas até o suporte e a produção. Não é surpresa, então, que 88% dos pesquisados tenham declarado não gerenciar mudanças.

83. A realização de mudanças no ambiente de TI sem o devido controle é causa comum de instabilidade e falhas de segurança. Isso porque há mudanças freqüentes e necessárias no ambiente de TI que oferecem risco à disponibilidade das informações: a atualização de versões de produtos de software, a oferta de novos sistemas ou módulos de sistemas, a atualização de sistemas operacionais e a atualização de aplicativos, dentre outros. Caso um novo produto não adequadamente testado seja disponibilizado no ambiente, há um risco de comprometer o funcionamento de outras soluções de TI. Além disso, as

mudanças devem ser registradas tanto para possibilitar Auditoria quanto para restaurar situações anteriores a uma mudança inadequada.

Critérios

a) Cobit 4.1 AI6 Manage Changes (Gestão de Mudanças - Todas as mudanças, incluindo manutenção e correções de emergência, relativas a infra-estrutura e aplicativos do ambiente de produção, devem ser formalmente geridas de maneira controlada);

b) NBR ISO/IEC 17799:2005, item 10.1.2 - Gestão de mudanças: convém que modificações nos recursos de processamento da informação e sistemas sejam controladas;

c) NBR ISO/IEC 17799:2005, item 12.5.1 - Procedimentos para controle de mudanças: convém que a implementação de mudanças seja controlada utilizando procedimentos formais de controle de mudanças.

Evidências

a) Apêndice I, planilha de resultados, pergunta 17. É feita a gestão de mudanças? (fl. 37-v).

Efeitos potenciais

a) Comprometimento da disponibilidade das informações nos sistemas e da estabilidade do ambiente de TI devido à realização de mudanças não-criteriosas;

b) Impossibilidade de restaurar uma situação anterior a uma mudança malsucedida, pela falta de cuidado com a preservação do estado anterior e de registro preciso dos passos executados;

c) Alteração do nível de proteção de uma ou várias informações de forma não avaliada, não prevista ou não aprovada pelo gestor da informação como efeito de mudança em um recurso de TI.

Achado XV. Ausência de gestão de capacidade e compatibilidade das soluções de TI

84. De acordo com as respostas recebidas, a gestão de capacidade e compatibilidade não é feita em 84% dos órgãos/entidades pesquisados. Tal processo está ligado ao monitoramento do ambiente de TI e sua ausência indica que esse monitoramento não é executado adequadamente. A principal conseqüência é o aumento do risco de descontinuidade na prestação dos serviços de TI, o que afeta diretamente a disponibilidade das informações.

85. Adicionalmente, a ausência desse processo priva os gerentes de uma importante ferramenta para direcionar os investimentos necessários na manutenção da qualidade da infra-estrutura de TI, de acordo com os requisitos do negócio.

Critérios

a) Cobit 4.1 PO3.4 Technology Standards (Padrões Tecnológicos - Para prover soluções tecnológicas consistentes, efetivas e seguras para toda a organização, estabelecer um fórum de tecnologia para prover diretrizes tecnológicas, pareceres e indicação sobre produtos de infra-estrutura e seleção de tecnologias, e verificar a conformidade com esses padrões e diretrizes. Esse fórum deve direcionar as práticas e padrões tecnológicos com base na relevância para o negócio, riscos e conformidade com requisitos externos);

b) Cobit 4.1 DS3 Manage Performance and Capacity (Gestão de Capacidade e Desempenho - A necessidade de gerir a capacidade e o desempenho dos recursos de TI requer um processo de avaliação periódica do desempenho atual e da capacidade desses recursos. Esse processo inclui prever futuras necessidades com base na carga de trabalho e nos requisitos de armazenamento e de contingência. Esse processo garante que as fontes de informação que suportam os requisitos de negócio estejam continuamente disponíveis);

c) NBR ISO/IEC 17799:2005, item 10.3.1 - Gestão de capacidade: convém que a utilização dos recursos seja monitorada e sincronizada e as projeções feitas para necessidades de capacidade futura, para garantir o desempenho requerido do sistema.

Evidências

a) Apêndice I, planilha de resultados, pergunta: 18. É efetuada a gestão de capacidade e compatibilidade das soluções de TI do órgão/entidade? (fl. 37-v).

Efeitos potenciais

a) Interrupções nos sistemas de informação por sobrecarga no processamento e indisponibilidade das informações;

b) Inadequação de investimentos em infra-estrutura de TI, por desconhecimento da real capacidade do ambiente e das necessidades de ampliação/atualização;

c) Desperdício provocado pela aquisição de produtos de TI incompatíveis com o ambiente existente.

Achado XVI. Ausência de análise de riscos na área de TI

86. A ausência da análise de riscos na área de TI, informada por 75% dos órgãos/entidades pesquisados, é um indício de que as ações de segurança não são executadas de maneira sintonizada com as necessidades do negócio dessas organizações. Isto porque, sem análise de riscos, não há como o gestor priorizar ações e investimentos com base em critérios claros e relacionados com o negócio da organização. O resultado pode ser desperdício, uso ineficaz de recursos, carência de ações prioritárias.

87. Além disso, o desconhecimento dos riscos na área de TI aumenta a exposição às ameaças de acesso indevido, indisponibilidade e perda de integridade (intencional, como no caso das fraudes, ou por falhas) das informações sob responsabilidade dessas organizações.

Critérios

a) Cobit 4.1 PO9.4 Risk Assessment (Análise de Riscos - Avaliar periodicamente a probabilidade e o impacto de todos os riscos identificados, usando métodos qualitativos e quantitativos. A probabilidade e o impacto associados com o risco inerente e residual devem ser determinados individualmente por categoria);

b) NBR ISO/IEC 17799:2005, item 4.1 - Analisando/avaliando os riscos de segurança da informação: convém que as análises/avaliações de riscos identifiquem, quantifiquem e priorizem os riscos com base em critérios relevantes para a organização, e que os resultados orientem e determinem as ações de gestão apropriadas e as prioridades para o gerenciamento dos riscos de segurança da informação, e para a implementação dos controles selecionados, de maneira a proteger contra estes riscos.

Evidências

a) Apêndice I, planilha de resultados, pergunta 13. É efetuada análise de riscos na área de TI? (fl. 37).

Efeitos potenciais

a) Estabelecimento inadequado de prioridades para ações de segurança;

b) Desperdício de recursos em ações não-prioritárias, enquanto outras mais críticas deixam de ser realizadas.

Conclusão

87.1. As respostas fornecidas pelos 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. O Gráfico 4 resume as deficiências encontradas no tratamento de segurança da informação, indicando para cada questão qual o percentual de órgãos/entidades que informaram não executar o controle associado. O resultado preocupa, pois a própria prestação do serviço de uma instituição pública aos cidadãos depende da confiabilidade das informações por ela tratadas e ofertadas.

87.2. 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 4 - Deficiências na segurança da informação

87.3. A seu turno, a ausência de uma gestão de mudanças em 88% dos pesquisados declarada pelos próprios 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.

87.4. 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.

87.5. 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.

87.6. 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.

87.7. 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.

87.8. 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.

87.9. 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.

87.10. 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.

87.11. 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.

Proposta de encaminhamento

88. Recomendar ao Gabinete de Segurança Institucional da Presidência da República, ao Conselho Nacional de Justiça e ao Conselho Nacional do Ministério Público que promovam ações com objetivo de disseminar a importância do gerenciamento da segurança da informação e induzir, mediante orientação normativa, os órgãos/entidades da Administração Pública Federal a realizarem ações para implantação e/ou aperfeiçoamento da gestão da continuidade do negócio, da gestão de mudanças, da gestão de capacidade, da classificação da informação, da gerência de incidentes, da análise de riscos de TI, da área específica para gerenciamento da segurança da informação, da política de segurança da informação e dos procedimentos de controle de acesso.

6. Desenvolvimento de sistemas de informação

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

90. 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.

91. O uso de metodologia para desenvolvimento de sistemas não é um tema novo e vem, progressivamente, incorporando os conceitos de engenharia de software 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.

92. 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) e o Modelo de Melhoria de Processos de Software (MPS.BR) . Nessas orientações, a existência de metodologia é requisito fundamental na construção de software de qualidade.

92.1. 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 (pergunta 16 do questionário). 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.

92.2. Finalmente, foi solicitado aos órgãos/entidades que participaram do levantamento o envio de dados acerca dos principais sistemas utilizados e suas bases de dados associadas (pergunta 20 do questionário). Ao final, 205 organizações enviaram informações sobre 9.494 sistemas. Essa base de dados ficará organizada e disponível na Sefti para utilização em futuras fiscalizações e levantamentos.

Achado XVII. Não-adoção de metodologia de desenvolvimento de sistemas

92.3. Segundo as declarações fornecidas, é adotada uma metodologia de desenvolvimento de sistemas em quase metade dos pesquisados (49%). É um resultado ainda modesto, se considerarmos a tendência de sistemas cada vez mais complexos e interligados, requerendo sempre mais qualidade dos sistemas aplicativos produzidos.

92.4. A ausência de metodologia em 51% dos pesquisados aumenta o risco de construir sistemas pouco robustos, suscetíveis a falhas, sem testes adequados e com documentação deficiente, ou seja, aumenta o risco de que etapas mal conduzidas do processo produzam resultados inadequados para a organização. Um levantamento malfeito, por exemplo, gera um produto que não é o esperado pelo cliente; um sistema mal documentado ou cuja documentação não segue um padrão ou, ainda, cuja documentação não é atualizada corretamente, fica dependente da manutenção pelo(s) desenvolvedor(es); um teste mal realizado permite que programas não adequadamente homologados pelo cliente sejam dados como concluídos.

92.5. Além disso, o risco para a organização é ainda maior quando se verifica que, dentre os 130 pesquisados que declararam não ter metodologia, 68% informaram que oferecem serviço transacional pela Internet e, portanto, possuem sistemas expostos a ações indevidas, intencionais ou não. Tal exposição é significativa pois, na Internet brasileira, os ataques a servidores web no primeiro trimestre de 2008 aumentaram 34% em relação ao trimestre anterior, e 519% em relação ao mesmo período de 2007 .

92.6. Outro aspecto importante a considerar é a terceirização do serviço de desenvolvimento: sem uma metodologia, não é possível terceirizar todo o processo ou mesmo parte dele sem que isso represente um risco para a organização. Como o processo em si não é bem definido, não há como medir o serviço prestado ou garantir que não haverá perda de conhecimento ou ainda que o resultado seja o adequado para a organização.

92.7. Finalmente, a falta de metodologia dificulta a Auditoria do processo de desenvolvimento em si tanto quanto dos seus produtos, ou seja, aumenta o risco de Auditoria. Em última instância, esse aumento do risco de Auditoria representa aumento de risco para a proteção de informações e dificulta a melhoria do processo. Nesse contexto, o Auditor de TI pode funcionar como indutor da adoção de metodologia por meio das recomendações de Auditoria. Para isso, é necessária a capacitação constante desse Auditor em metodologias de gestão e qualidade em desenvolvimento de sistemas, tais como CMMI, Rational Unified Process (RUP) e MPS.BR.

Critérios

a) Cobit 4.1 AI2.7 Development of Application Software (Desenvolvimento de Software Aplicativo - Assegurar que os aplicativos sejam desenvolvidos de acordo com as especificações de projeto, padrões de desenvolvimento e documentação, requisitos de qualidade e padrões de aprovação. Assegurar que todos os aspectos legais e contratuais estejam identificados e tratados para software aplicativo desenvolvido por terceiros).

Evidências

a) Apêndice I, planilha de resultados, pergunta: 16. O órgão/entidade oferece serviços transacionais via Internet, ou seja, prestação de serviço que pode ser executado do início ao fim pela Internet com troca bidirecional de informações entre o órgão/entidade e o cliente? (fl. 37-v);

b) Apêndice I, planilha de resultados, pergunta: 19. O desenvolvimento de sistemas segue alguma metodologia? (fl. 37-v);

c) Apêndice I, planilha de resultados, pergunta: 20. O órgão/entidade possui e mantém inventário dos principais sistemas informatizados e suas bases de dados? (fl. 37-v).

Efeitos potenciais

a) Processo de desenvolvimento de sistemas lento e sistemas de informação ineficazes;

b) Perda de informações por causa de sistemas pouco robustos, sujeitos a falhas de segurança, seja por fraude, seja por uso incorreto;

c) Execução de contratos de prestação de serviços de desenvolvimento sem métricas adequadas nem etapas claras com produtos para cada etapa;

d) Sistemas de difícil manutenção, sem documentação, em que apenas quem desenvolveu detém o conhecimento. Esse caso pode ser ainda mais sério se o desenvolvedor for contratado externamente.

Conclusão

93. 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 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, representa risco de má gestão dos recursos dos órgãos/entidades da Administração Pública Federal.

93.1. 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.

Propostas de encaminhamento

94. Recomendar à Secretaria de Logística e Tecnologia da Informação (SLTI) do Ministério do Planejamento, Orçamento e Gestão, ao Conselho Nacional de Justiça e ao Conselho Nacional do Ministério Público que promovam ações com objetivo de disseminar a importância da adoção de metodologia de desenvolvimento de sistemas e induzir os órgãos/entidades da Administração Pública Federal a realizarem ações para implantação e/ou aperfeiçoamento dessa metodologia.

7. Gestão de acordos de níveis de serviço

95. 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).

96. No caso de um acordo de nível de serviço de TI, então, é definida a qualidade dos serviços de TI em função das necessidades da organização, quantificada e especificada 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 no limite do esperado ou é mais crítico para o negócio.

97. 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 mensuração da qualidade de serviços de TI é citada, inclusive, em trechos de Acórdãos do TCU, como o Acórdão 2.172/2005-TCU-Plenário e o Acórdão 786/2006-TCU-Plenário . O termo "acordo de nível de serviço" para contratos de TI também já é conhecido do TCU, e foi mencionado no Acórdão 1.878/2005-TCU-Plenário .

Achado XVIII. Ausência de gestão de acordos de níveis de serviços prestados internamente

98. A gestão de níveis de serviços foi a questão com mais alto percentual de resposta negativa: 89% dos pesquisados informaram não executar a gestão de níveis de serviço de TI ofertados aos seus clientes. Essa resposta é coerente com o resultado obtido na verificação de alguns dos processos de trabalho que apóiam a gestão de níveis de serviço: o plano de continuidade de negócios (Achado IX - 88% de respostas negativas), a gestão de mudanças (Achado XIV - 88% de respostas negativas) e a gestão de capacidade e compatibilidade (Achado XV - 84% de respostas negativas).

99. A ausência da gestão de acordo de níveis de serviço em percentual tão expressivo indica que grande parte dos pesquisados não realiza a negociação da qualidade dos serviços de TI com os seus clientes. A conseqüência disso é uma dificuldade em ajustar expectativas: as áreas de TI não sabem se estão atendendo às necessidades de qualidade de serviço dos seus clientes, nem tampouco os clientes sabem, ao pedir um serviço de

TI, qual o nível de qualidade que podem esperar. Os resultados podem ser áreas de TI cujos esforços e investimentos não estão sintonizados com as necessidades e expectativas dos seus clientes.

Critérios

a) Cobit 4.1 DS1 Define and Manage Service Levels (Definir e Gerenciar Níveis de Serviço - A comunicação efetiva entre gerente de TI e usuários sobre requisitos de serviço é possível por meio de acordo definido e documentado acerca dos serviços de TI e níveis de serviço. Esse processo também inclui monitoramento e divulgação tempestiva aos interessados do cumprimento dos níveis de serviço. Esse processo permite um alinhamento entre os serviços de TI e os requisitos de negócio relacionados).

Evidências

a) Apêndice I, planilha de resultados, pergunta: 21. É efetuada a gestão de acordos de níveis de serviço das soluções de TI do órgão/entidade oferecidas a seus clientes? (fl. 37).

Efeitos potenciais

a) Insatisfação dos clientes com a qualidade e desempenho das soluções ofertadas por sua área de TI;

b) Ausência de informações para os gerentes de TI sobre as reais expectativas dos seus clientes;

c) Inadequação da distribuição dos investimentos em TI em relação às necessidades dos clientes.

Achado XIX. Ausência de gestão de acordos de níveis de serviços contratados externamente

100. Um total de 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.

101. Na verdade, a administração precisa, por força da lei, monitorar os seus contratos de TI. De fato, as questões 31 (sobre verificação de itens predefinidos para atestação das faturas, com 56% de resposta positiva) e 33 (sobre monitoração técnica dos contratos, com 90% de resposta positiva) obtiveram resultados melhores do que a questão sobre níveis de serviço. Uma possível explicação para esses resultados é que talvez exista algum monitoramento dos serviços contratados, mas ele nem sempre se dê em função de um indicador de desempenho. Ou, ainda, quando há tal indicador, ele não é estratégico e sintonizado com o negócio, como é o caso do acordo de nível de serviço.

102. Assim, por exemplo, exige-se no contrato que a provedora de link para Internet forneça serviço à velocidade de 4MB/s, em regime 24x7, com 99% de qualidade do serviço (isto é, é tolerado 1% de falha no fornecimento). Em alguns casos, a falha consiste em não verificar relatórios comprobatórios do índice de qualidade para atestação de fatura. Porém, mesmo quando tal índice é verificado, isso não é garantia de que o usuário final foi atendido em suas necessidades, pois não houve verificação nem acordo prévio de que tais velocidade e qualidade seriam suficientes para o negócio da organização. Nesse caso, as organizações se arriscam a manter contratos de serviços que não são efetivos para o seu negócio, mesmo quando cumprem metas contratuais.

103. Adicionalmente, 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 sua ausência da gestão interna dos níveis de serviço.

104. É necessário destacar que o art. 14 da recém publicada IN-4 da Secretaria de Logística Tecnologia da Informação (SLTI) do Ministério do Planejamento, Orçamento e Gestão indica o mínimo que deve constar nos contratos com objetivo de estabelecer níveis de serviço.

Critérios

a) Cobit 4.1 DS1 Define and Manage Service Levels (Definir e Gerenciar Níveis de Serviço - A comunicação efetiva entre gerente de TI e usuários sobre requisitos de serviço é possível por meio de acordo

definido e documentado acerca dos serviços de TI e níveis de serviço. Esse processo também inclui monitoramento e divulgação tempestiva aos interessados do cumprimento dos níveis de serviço. Esse processo permite um alinhamento entre os serviços de TI e os requisitos de negócio relacionados).

Evidências

a) Apêndice I, planilha de resultados, pergunta: 22. É efetuada a gestão dos níveis de serviço acordados para os serviços de TI prestados ao órgão/entidade? (fl. 37-v).

Efeitos potenciais

a) Insatisfação dos clientes com a qualidade e desempenho das soluções de TI contratadas;

b) Realização e manutenção de contratos de qualidade inadequada e pouco efetivos para o negócio da organização;

c) Inadequação da distribuição dos investimentos em TI em relação às necessidades da organização;

d) Não-aplicação de multas contratuais e pagamento de valores indevidos aos fornecedores.

Conclusão

105. 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.

106. 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 sua ausência da gestão interna dos níveis de serviço.

Proposta de encaminhamento

107. Recomendar à Secretaria de Logística e Tecnologia da Informação (SLTI) do Ministério do Planejamento, Orçamento e Gestão, ao Conselho Nacional de Justiça e ao Conselho Nacional do Ministério Público que promovam ações com objetivo de disseminar a importância de gestão de níveis de serviço e induzir os órgãos/entidades da Administração Pública Federal a realizarem ações para implantação e/ou aperfeiçoamento de acordos de níveis de serviço.

8. Processo de contratação de bens e serviços de TI

108. 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 suas metas.

Achado XX. Ausência de processo formal de trabalho para contratações de TI

109. 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.

110. 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 e que poderiam ser evitados com a adoção de um processo de trabalho formalizado.

111. 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.

112. 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 decorrem, 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.

113. O item 9.4 do Acórdão 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 atendimento a esse acórdão, durante o processo de revisão deste relatório, a SLTI publicou a Instrução Normativa n.º 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 da contratação, seleção do fornecedor e gerenciamento do contrato e entrará em vigor no dia 2 de janeiro de 2009.

Critérios

a) Cobit 4.1 AI5.1 Procurement Control (Controle sobre aquisições - Desenvolver e seguir um conjunto de procedimentos e padrões consistente com o processo de licitação e a estratégia de aquisição gerais da organização para adquirir infra-estrutura, instalações, hardware, software e serviços de TI necessários ao negócio).

Evidências

a) Apêndice I, planilha de resultados, pergunta: 23. O órgão/entidade adota processo formal de trabalho na contratação de bens e serviços de TI? (fl. 37-v).

Efeitos potenciais

a) Aquisições de TI não alinhadas às necessidades de médio e longo prazos da organização;

b) Contratação de bens e serviços de TI que não atendem à qualidade necessária ao bom desenvolvimento do negócio do órgão/entidade;

c) Descumprimento de leis e normas relativas às licitações de TI;

d) Problemas na gestão dos contratos decorrentes de aquisições de TI por falta de requisitos previamente estabelecidos na licitação;

e) Desperdício de recursos.

Achado XXI. Ausência de análise de custo/benefício da solução de TI contratada

114. 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.

115. É importante notar que toda contratação de TI deve ser anteriormente aprovada levando-se em conta os 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, a contratação deve ser aprovada pelo comitê diretivo de TI (Achado III).

116. Os artigos 10 a 12 da recém publicada IN-4 da SLTI (item 113) indicam atividades que deverão ser executadas para análise de viabilidade da contratação.

Critérios

a) Cobit 4.1 AI1.3 Feasibility Study and Formulation of Alternative Courses of Action (Estudo de viabilidade e formulação de soluções alternativas - Desenvolver um estudo de viabilidade que examine a possibilidade da implementação dos requisitos. A gerência do negócio, apoiada pela gerência de TI, deve avaliar a viabilidade e as soluções alternativas e fazer uma recomendação ao patrocinador da ação);

b) Cobit 4.1 AI1.4 Requirements and Feasibility Decision and Approval (Decisão e aprovação dos requisitos e da viabilidade - Verificar se o processo requer que o patrocinador da ação formalize sua aprovação dos requisitos funcionais e técnicos e dos relatórios de estudo de viabilidade em etapas chave predeterminadas. O patrocinador da ação deve tomar a decisão final no que diz respeito à escolha da solução e da forma de sua aquisição).

Evidências

a) Apêndice I, planilha de resultados, pergunta: 24. Na elaboração do projeto básico das contratações de TI é feita análise de custo/benefício da solução a ser contratada ? (fl. 37-v).

Efeitos potenciais

a) Contratação de bens e serviços de TI com custos acima do necessário;

b) Soluções alternativas satisfatórias e a um custo mais baixo não identificadas;

c) Desperdício de recursos.

Achado XXII. Ausência de explicitação dos benefícios nas contratações de TI

117. 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.

118. 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 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, (...)". Na mesma direção é o item 9.1.1 do Acórdão 2.094/2004-TCU-Plenário: "todas as aquisições devem ser realizadas em harmonia com o planejamento estratégico da instituição (...)".

119. Assim, toda contratação de TI deve ter seus benefícios para a organização explicitados, ou seja, deve ser justificada em que medida 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 (item 113) 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".

Critérios

a) Cobit 4.1 AI1.3 Feasibility Study and Formulation of Alternative Courses of Action (Estudo de viabilidade e formulação de soluções alternativas - Desenvolver um estudo de viabilidade que examine a possibilidade da implementação dos requisitos. A gerência do negócio, apoiada pela gerência de TI, deve avaliar a viabilidade e as soluções alternativas e fazer uma recomendação ao patrocinador da ação);

b) Cobit 4.1 AI1.4 Requirements and Feasibility Decision and Approval (Decisão e aprovação dos requisitos e da viabilidade - Verificar se o processo requer que o patrocinador da ação formalize sua aprovação dos requisitos funcionais e técnicos e dos relatórios de estudo de viabilidade em etapas chave predeterminadas. O patrocinador da ação deve tomar a decisão final no que diz respeito à escolha da solução e da forma de sua aquisição);

c) Acórdão 1.558/2003-TCU-Plenário, item 9.3.11;

d) Acórdão 2.094/2004-TCU-Plenário, item 9.1.1.

Evidências

a) Apêndice I, planilha de resultados, pergunta: 25. Na elaboração do projeto básico das contratações de TI são explicitados os benefícios da contratação em termos de negócio do órgão/entidade e não somente em termos de TI? (fl. 37-v).

Efeitos potenciais

a) Aquisições de TI não alinhadas às necessidades de médio e longo prazos da organização;

b) Contratação de bens e serviços de TI com desempenho abaixo do esperado e/ou requerido;

c) Contratação de bens e serviços de TI não integrados à infra-estrutura de TI existente;

d) Desperdício de recursos.

Achado XXIII. Não-exigência de demonstrativo de formação de preço antes da adjudicação

120. O valor de muitas contratações de TI é resultado 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.

121. 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 n.º 8.666/1993 já recomendá-la, mesmo que implicitamente, em seus artigos 7º e 46.

Critérios

a) Lei n.º 8.666/1993, art. 7º, § 2º, inciso II, e art. 46, § 1º, inciso II.

Evidências

a) Apêndice I, planilha de resultados, pergunta: 27. É exigido o demonstrativo de formação de preço antes da adjudicação? (fl. 37-v).

Efeitos potenciais

a) Problemas na gestão dos contratos decorrentes de aquisições de TI por falta de parâmetros para renegociação de valores, caso seja necessário;

b) Dificuldade de se identificar a prática de "jogo de planilhas" .

Conclusão

122. 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. Em atendimento ao item 9.4 do Acórdão 786/2006-TCU-Plenário, a SLTI editou a IN-4, que entrará em vigor em janeiro de 2009 e pode ser considerada um bom começo para mudança do quadro atual.

123. 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 47% do universo pesquisado não 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.

124. 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 XXIV e XXV, mostra que muito ainda precisa ser feito para que haja controle efetivo de que as contratações de TI são convenientes para a organização.

125. 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.

Proposta de encaminhamento

126. Recomendar ao Conselho Nacional de Justiça e ao Conselho Nacional do Ministério Público que promovam ações com objetivo de disseminar a importância de processo de trabalho formalizado de contratação de bens e serviços de TI e induzir, mediante orientação normativa nos moldes recomendados pelo item 9.4 do Acórdão 786/2006-TCU-Plenário, os órgãos do Poder Judiciário e do Ministério Público a realizarem ações para implantação e/ou aperfeiçoamento do processo de contratação de TI.

9. Processo de gestão de contratos de TI

127. 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.

128. Apesar da Lei n.º 8.666/1993 determinar algumas ações que devem ser obrigatoriamente realizadas, não há a indicação do que deve constar de processo de trabalho para gestão dos contratos. Entretanto, para todos os contratos e, especialmente, para os contratos de TI, a sua 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.

Achado XXIV. Ausência de processo formal de trabalho para gestão de contratos de TI

129. 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.

130. 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.

131. 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 prestação de contas.

132. 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 n.º 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 conhecimento individual do gestor, quando deveria ser uma atividade impessoal que qualquer funcionário habilitado pudesse exercer de acordo com o processo de trabalho padrão.

133. A recém publicada IN-4 da SLTI dedica toda a Seção III ao gerenciamento do contrato (item 113).

Critérios

a) Lei n.º 8.666/1993, Capítulo III - Dos Contratos;

b) Cobit 4.1 AI5.1 Procurement Control (Controle sobre aquisições - Desenvolver e seguir um conjunto de procedimentos e padrões consistente com o processo de licitação e a estratégia de aquisição gerais da organização para adquirir infra-estrutura, instalações, hardware, software e serviços de TI necessários ao negócio).

Evidências

a) Apêndice I, planilha de resultados, pergunta: 28. O órgão/entidade adota processo formal de trabalho na gestão de contratos de bens e serviços de TI? (fl. 37-v);

b) Apêndice I, planilha de resultados, pergunta: 29. Há designação formal do gestor de cada contrato relativo a bens e serviços de TI? (fl. 37-v).

Efeitos potenciais

a) Descumprimento de leis e normas relativas à gestão de contratos de TI;

b) Problemas na gestão dos contratos de TI;

c) Baixa qualidade dos serviços prestados;

d) Não-aplicação de multas previstas nos contratos;

e) Interrupções na execução de contratos de TI;

f) Interrupção de processos que sustentam o negócio da organização;

g) Não-conclusão de projetos importantes para se atingir as metas da organização;

h) Desperdício de recursos.

Achado XXV. Não-realização de reuniões periódicas para avaliar o andamento dos contratos de TI

134. Causa preocupação o fato de 65% dos órgãos/entidades que participaram do levantamento não realizarem 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.

135. O art. 67 da Lei n.º 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".

136. 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.

Critérios

a) Art. 67 da Lei n.º 8.666/1993;

b) Cobit 4.1 AI5.2 Supplier Contract Management (Gerenciamento de Contratos de Fornecedores - Definir um procedimento para estabelecimento, modificação e conclusão de contratos com todos os fornecedores. O procedimento deve cobrir, no mínimo, responsabilidades, obrigações e penalidades legais, financeiras, organizacionais, documentais, de desempenho, de segurança, de propriedade intelectual e de conclusão. Todos os contratos e aditivos devem ser revisados por consultores jurídicos);

c) Cobit 4.1 DS2.2 Supplier Relationship Management (Gerenciamento de Relacionamento com Fornecedores - Formalizar o processo de gerenciamento e relacionamento com cada fornecedor. O contato com o fornecedor deve tratar dos assuntos relativos a clientes e fornecedores e garantir a qualidade do relacionamento baseado na confiança e transparência, isto é, por meio de acordos de nível de serviço (SLA));

d) Cobit 4.1 DS2.3 Supplier Risk Management (Gerenciamento de Riscos com Fornecedores - Identificar e mitigar riscos relacionados à capacidade dos fornecedores de continuarem efetivamente a entregar os produtos de uma maneira segura, eficiente e contínua. Garantir que os contratos estejam de acordo com os padrões gerais do negócio e requisitos legais e regulatórios. O gerenciamento de riscos deve considerar antecipadamente acordos de não-divulgação de informações, contratos de garantia, viabilidade de continuidade do fornecedor, conformidade com requisitos de segurança, fornecedores alternativos, penalidades, recompensas etc.);

e) Cobit 4.1 DS2.4 Supplier Performance Monitoring (Monitoramento de Desempenho de Fornecedores - Estabelecer um processo para monitorar a entrega dos serviços de forma a garantir que o fornecedor esteja cumprindo os requisitos do negócio e continue seguindo os termos acordados no contrato e no SLA. Esse processo deve garantir, também, que o desempenho do fornecedor seja compatível com o de fornecedores alternativos e com as condições do mercado);

Evidências

a) Apêndice I, planilha de resultados, pergunta: 30. Há realização de reunião periódica com o contratado para avaliar o andamento de cada contrato relativo a bens e serviços de TI? (fl. 37-v).

Efeitos potenciais

a) Descumprimento de leis e normas relativas à gestão de contratos de TI;

b) Problemas na gestão dos contratos de TI;

c) Baixa qualidade dos serviços prestados;

d) Não-aplicação de multas previstas nos contratos;

e) Interrupções na execução de contratos de TI;

f) Interrupção de processos que sustentam o negócio da organização;

g) Não-conclusão de projetos importantes para se atingir as metas da organização;

h) Desperdício de recursos.

Achado XXVI. Não-definição prévia de itens para atestação técnica das faturas de contratos de TI

137. 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.

138. 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.

139. 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.

Critérios

a) Cobit 4.1 DS2.4 Supplier Performance Monitoring (Monitoramento de Desempenho de Fornecedores - Estabelecer um processo para monitorar a entrega dos serviços de forma a garantir que o fornecedor esteja cumprindo os requisitos do negócio e continue seguindo os termos acordados no contrato e no SLA. Esse processo deve garantir, também, que o desempenho do fornecedor seja compatível com o de fornecedores alternativos e com as condições do mercado).

Evidências

a) Apêndice I, planilha de resultados, pergunta: 31. Há verificação de itens predefinidos que embasem a atestação técnica dos bens e serviços de TI contratados referentes a cada fatura apresentada? (fl. 37-v);

b) Apêndice I, planilha de resultados, pergunta: 33. É feita monitoração técnica dos contratos relativos a bens e serviços de TI? Quantos funcionários realizam esta atividade? Quantos contratos relativos a bens e serviços de TI estão em vigor? (fl. 38).

Efeitos potenciais

a) Descumprimento de leis e normas relativas à gestão de contratos de TI;

b) Pagamentos indevidos;

c) Não-aplicação de multas previstas nos contratos;

d) Desperdício de recursos.

Achado XXVII. Monitoração administrativa dos contratos de TI feita pela área de TI

140. A monitoração administrativa dos contratos deve ser feita em cumprimento ao disposto no inciso XIII do art. 55, c/c o art. 29, da Lei n.º 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.

141. 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.

142. 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.

142.1. 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 n.º 110/2001 (Acórdão 353/2008-TCU-Plenário).

Critérios

a) Art. 29 e inciso XIII do art. 55 da Lei n.º 8.666/1993;

b) Cobit 4.1 DS2.2 Supplier Relationship Management (Gerenciamento de Relacionamento com Fornecedores - Formalizar o processo de gerenciamento e relacionamento com cada fornecedor. O contato com o fornecedor deve tratar dos assuntos relativos a clientes e fornecedores e garantir a qualidade do relacionamento baseado na confiança e transparência, isto é, por meio de SLA).

Evidências

a) Apêndice I, planilha de resultados, pergunta: 32. A monitoração administrativa dos contratos relativos a bens e serviços de TI é feita pela área de TI? (fl. 38).

Efeitos potenciais

a) Descumprimento de leis e normas relativas à gestão de contratos de TI;

b) Pendências judiciais relativas a encargos trabalhistas e previdenciários;

c) Não-aplicação de multas previstas nos contratos.

Achado XXVIII. Não-transferência de conhecimento relativo aos produtos e serviços terceirizados para os servidores dos órgãos/entidades

143. 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, ainda mais 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.

144. É um contra-senso a contratação de serviços importantes para a organização mas para os quais não há os recursos necessários para serem realizados internamente, ou serviços que usem novas tecnologias e não ser exigida a transferência do conhecimento para sua realização. 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.

145. 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.

Critérios

a) Cobit 4.1 AI4.4 Knowledge Transfer to Operations and Support Staff (Transferência de Conhecimentos para Equipes de Operação e Suporte - Transferir conhecimento e habilidades para permitir que

equipes de operação e suporte técnico possam executar, dar suporte e manter efetiva e eficientemente o sistema e a infra-estrutura associada).

Evidências

a) Apêndice I, planilha de resultados, pergunta: 34. Há transferência de conhecimento para servidores do órgão/entidade referente a produtos e serviços de TI terceirizados?

(fl. 38).

Efeitos potenciais

a) Problemas com a continuidade do serviço de TI após o fim do contrato;

b) Documentação insuficiente dos produtos advindos do contrato;

c) Serviço de ajuda (help-desk) sobrecarregado;

d) Perda de conhecimento importante para a organização;

e) Desperdício de recursos.

Conclusão

146. 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.

147. 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 .

148. 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.

Proposta de encaminhamento

149. Recomendar ao Conselho Nacional de Justiça e ao Conselho Nacional do Ministério Público que promovam ações com objetivo de disseminar a importância de processo de trabalho formalizado de gestão de contratos de TI e induzir, mediante orientação normativa nos moldes recomendados pelo item 9.4 do Acórdão 786/2006-TCU-Plenário, os órgãos do Poder Judiciário e do Ministério Público a realizarem ações para implantação e/ou aperfeiçoamento desse processo de gestão.

10. Processo orçamentário de TI

150. 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.

151. O planejamento estratégico de TI (Achado II), aliado com os planos de ação e as decisões do comitê diretivo de TI (Achado III), 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 do conhecimento detalhado dos gastos de TI prejudica tal previsão.

152. 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 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 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.

Achado XXIX. Não-consideração das ações planejadas para o próximo ano quando da solicitação de orçamento para a área de TI

153. Apesar da 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.

154. 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.

155. 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.

Critérios

a) Cobit 4.1 PO5.3 IT Budgeting (Orçamento de TI - Estabelecer e implementar práticas para elaborar um orçamento que reflita as prioridades estabelecidas na lista de projetos de TI e inclua os custos atuais de operação e manutenção da infra-estrutura existente. As práticas devem dar suporte ao desenvolvimento de um orçamento geral para TI, assim como o desenvolvimento de orçamentos específicos para os projetos com ênfase específica nos componentes de TI. As práticas devem permitir revisão do andamento, refinamento das informações e aprovação do orçamento geral para TI e dos orçamentos específicos dos projetos).

Evidências

a) Apêndice I, planilha de resultados, pergunta: 35. A solicitação do orçamento para a área de TI, encaminhada em 2006, foi feita com base nas ações da área de TI planejadas para 2007? (fl. 38).

Efeitos potenciais

a) Recursos insuficientes para a área de TI;

b) Interrupção de serviços de TI por falta de recursos necessários;

c) Não-alcance de metas estabelecidas para a organização por falta de suporte da área de TI.

Achado XXX. Não-alocação dos recursos previstos no orçamento às ações constantes do planejamento de TI no início do ano

156. Apesar de 82% dos órgãos/entidades consultados afirmarem que controlam os gastos de TI, um percentual considerável (21%) não enviou informações sobre o total de gastos com TI e uma parcela significativa, mesmo enviando os dados, informou que teve dificuldade em obter esses valores.

157. Além disso, pouco menos da metade (49%) das organizações consultadas disse que no 1º trimestre de 2007 fez a alocação orçamentária às ações constantes do planejamento de TI. Esse quadro é um indício de que 51% dos pesquisados não exerce o controle sobre os gastos de TI a partir do orçamento aprovado

e das ações planejadas. Provavelmente, essas organizações apenas atendem o que a legislação determina e não realizam um controle eficiente sobre os gastos de TI.

Critérios

a) Cobit 4.1 PO5.3 IT Budgeting (Orçamento de TI - Estabelecer e implementar práticas para elaborar um orçamento que reflita as prioridades estabelecidas na lista de projetos de TI e inclua os custos atuais de operação e manutenção da infra-estrutura existente. As práticas devem dar suporte ao desenvolvimento de um orçamento geral para TI, assim como o desenvolvimento de orçamentos específicos para os projetos com ênfase específica nos componentes de TI. As práticas devem permitir revisão do andamento, refinamento das informações e aprovação do orçamento geral para TI e dos orçamentos específicos dos projetos).

Evidências

a) Apêndice I, planilha de resultados, pergunta: 36. No 1º trimestre de 2007 foi feita a alocação orçamentária às ações constantes do planejamento? (fl. 38);

b) Apêndice I, planilha de resultados, pergunta: 37. Ao longo do exercício financeiro há controle dos gastos e da disponibilidade orçamentária? (fl. 38).

Efeitos potenciais

a) Recursos insuficientes para a área de TI;

b) Interrupção de serviços de TI por falta de recursos necessários;

c) Não-alcance de metas estabelecidas para a organização por falta de suporte da área de TI.

Conclusão

158. 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.

159. 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. Assim, espera-se que os órgãos/entidades elaborem suas propostas orçamentárias para a área de TI com base nas ações que efetivamente pretendam realizar e alinhadas aos objetivos de negócio. Além disso, os órgãos/entidades devem manter acompanhamento da execução dos gastos de TI para que saibam, precisamente, quanto foi gasto, em que ações e qual a disponibilidade para gastos futuros.

Proposta de encaminhamento

160. Recomendar à Secretaria de Logística e Tecnologia da Informação (SLTI) do Ministério do Planejamento, Orçamento e Gestão, ao Conselho Nacional de Justiça e ao Conselho Nacional do Ministério Público que promovam ações com objetivo de garantir que as propostas orçamentárias para a área de TI dos órgãos/entidades da Administração Pública Federal sejam elaboradas com base nas atividades que efetivamente pretendam realizar e alinhadas aos objetivos de negócio.

11. Auditoria de tecnologia da informação

161. 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 , com o objetivo de tornar as áreas de TI controláveis, com resultados mensuráveis e orientadas aos objetivos do negócio da organização.

162. 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.

163. 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 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.

164. 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.

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

Anexo XXXI. Inexecução de Auditoria de TI pelos órgãos/entidades

166. Somente 40% dos pesquisados declarou ter realizado Auditoria de TI nos últimos cinco anos no seu órgão/entidade. O Gráfico 5 estratifica a quantidade de Auditorias de TI realizadas nessas 101 organizações.

Gráfico 5 - Quantidade de Auditorias de TI realizadas nos últimos cinco anos

167. Dentre os órgãos/entidades que realizaram alguma Auditoria de TI nos últimos cinco anos, observa-se que 68% deles declararam ter feito somente até cinco Auditorias de TI nesse período. Além disso, 55% desses órgãos (38 instituições) declararam que, dentre essas Auditorias de TI realizadas, pelo menos uma foi executada por órgão de controle externo (TCU) ou interno (Secretaria Federal de Controle ou Controladoria Geral da União). Isso é um indício de que nessas instituições a Auditoria de TI ainda não é realizada em bases periódicas.

168. A conseqüência disso é que as organizações correm o risco de ter processos de TI com controles inadequados e, assim, de tais processos serem executados em desacordo com as políticas de TI da própria organização e com a legislação vigente, sem que haja conhecimento do ocorrido pela administração da organização. Além disso, os gestores de TI deixam de ter em mãos uma importante ferramenta para a melhoria dos processos de TI.

Critérios

a) Cobit 4.1 ME2 Monitor and Evaluate Internal Control (Monitorar e Avaliar os Controles Internos - Estabelecer um programa efetivo de controle interno de TI requer um processo bem definido de monitoramento. Esse processo inclui o monitoramento e o relato das exceções de controle, resultados de auto-avaliações e revisão de terceiros. Um benefício chave do monitoramento dos controles internos é prover segurança com vistas a operações efetivas e eficientes e conformidade com leis e regulações);

b) NBR ISO/IEC 17799:2005, item 15.2 - Conformidade com normas e políticas de segurança da informação e conformidade técnica: convém que a segurança dos sistemas de informação seja analisada criticamente a intervalos regulares;

c) NBR ISO/IEC 17799:2005, item 6.1.8 - Análise crítica independente de segurança da informação: convém que o enfoque da organização para gerenciar a segurança da informação e a sua implementação (...) seja analisado criticamente, de forma independente, a intervalos planejados, ou quando ocorrerem mudanças significativas relativas à implementação da segurança da informação.

Evidências

a) Apêndice I, planilha de resultados, pergunta: 39. Foi realizada alguma Auditoria de TI nos últimos cinco anos no órgão/entidade? (fl. 38).

Efeitos potenciais

a) Inobservância da política de segurança da informação da organização quando da implementação dos controles de acesso lógico nos sistemas de informação;

b) Existência de informações não confiáveis na base de dados da organização, o que compromete não só a efetividade dos seus sistemas de informação como a de sistemas de outras organizações que utilizam essa mesma base de dados;

c) Área de TI com governança imatura, sem controles e indicadores que possam apontar os problemas e oportunidades de negócio para a organização.

Achado XXXII. Inexistência de equipe própria para realizar Auditoria de TI

169. Somente 19% dos pesquisados declararam ter equipe interna para Auditoria de TI. Assim, para uma quantidade expressiva de órgãos/entidades, a Auditoria de TI somente é realizada por Auditores/consultores independentes, ou por organizações reguladoras, como TCU e CGU. Por esses dados, infere-se que tais organizações ainda não foram afetadas pela tendência de incorporar atividades de Auditoria nos seus próprios processos de trabalho. Com isso, tais organizações perdem a oportunidade de ter, no seu Auditor interno, um parceiro no processo de melhoria dos seus controles de TI. Além disso, expõem-se ao risco inerente de Auditorias realizadas por terceiros: o risco de uso malicioso de ferramentas de Auditoria e das informações acessadas durante os trabalhos de Auditoria.

170. Vale ressaltar, por outro lado, que ao serem contabilizadas todas as Auditorias declaradas pelos órgãos/entidades dos últimos cinco anos, 73% delas foram realizadas por equipe de Auditoria interna. Assim, pode-se inferir que, entre os órgãos que declararam fazer tal tipo de Auditoria com maior regularidade, o fazem com equipe interna. De fato, ao observar o Achado XXXI, considerando os 22% que declararam ter realizado mais de 10 Auditorias nos últimos cinco anos, 91% deles têm equipe interna de Auditoria.

171. Observa-se, também, que dentre as Auditorias realizadas, a maior quantidade delas (32%) está focada na aquisição de bens e serviços de TI, seguida das Auditorias com foco em segurança da informação (20%). Uma possível explicação é que as organizações que executam tais Auditorias o fazem em função de exigências legais de agências reguladoras, mais do que por necessidades de gestão.

Critérios

a) Cobit 4.1 ME2 Monitor and Evaluate Internal Control (Monitorar e Avaliar os Controles Internos - Estabelecer um programa efetivo de controle interno de TI requer um processo bem definido de monitoramento. Esse processo inclui o monitoramento e o relato das exceções de controle, resultados de auto-avaliações e revisão de terceiros. Um benefício chave do monitoramento dos controles internos é prover segurança com vistas a operações efetivas e eficientes e conformidade com leis e regulações);

b) NBR ISO/IEC 17799:2005, item 15.2 - Conformidade com normas e políticas de segurança da informação e conformidade técnica: convém que a segurança dos sistemas de informação seja analisada criticamente a intervalos regulares.

Evidências

a) Apêndice I, planilha de resultados, pergunta: 38. O órgão/entidade possui equipe própria para realizar Auditorias de TI? (fl. 38).

Efeitos potenciais

a) Ausência de Auditores internos que poderiam auxiliar em Auditorias de processos de gestão.

Conclusão

172. 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.

172.1. 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.

Proposta de encaminhamento

173. Recomendar à Controladoria-Geral da União que realize regularmente Auditorias de TI nos órgãos/entidades da Administração Pública Federal.

174. Recomendar à Controladoria-Geral da União, ao Conselho Nacional de Justiça e ao Conselho Nacional do Ministério Público que promovam ações para estimular a realização de Auditorias de TI nos órgãos/entidades da Administração Pública Federal.

12. Conclusão

175. O objetivo deste 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.

As respostas recebidas foram agrupadas em nove conjuntos, apresentados nos itens 3 a 11 do presente relatório, em função das questões de Auditoria e das áreas de foco da governança de TI. Os grupos foram: 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; Auditoria de tecnologia da informação.

176. Sobre planejamento estratégico, observou-se que 59% das organizações declararam não realizar o planejamento estratégico de TI, e mais de dois terços não têm comitê diretivo de TI, do qual participam vários setores da organização que decidem sobre as estratégias de TI. A partir desses dados pode-se inferir que a falta de planejamento estratégico institucional pode inibir e/ou prejudicar o planejamento das ações de TI. Assim, o estímulo à elaboração de planejamento estratégico institucional acompanhado da elaboração do planejamento estratégico de TI, em consonância com o primeiro, é uma ação para a melhoria da governança de TI.

177. No que diz respeito à estrutura de pessoal de TI, observou-se que 29% dos pesquisados possuem menos de 1/3 da sua área de TI composta 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. Do ponto de vista da governança de TI, ainda há que se coletar informações que correlacionem a qualidade das áreas de TI e a sua estrutura de pessoal, para avaliar a adequação entre estruturas e as necessidades dos órgãos/entidades.

178. Já no grupo de questões sobre segurança da informação, observou-se o pior desempenho. Dentre as nove questões sobre o assunto, apenas em uma delas um pouco mais da metade dos pesquisados afirmou executar o controle correspondente, enquanto nas outras questões, a maioria dos órgãos/entidades declarou não fazê-lo (Gráfico 4). O maior quantitativo de respostas negativas ocorreu nas questões sobre plano de continuidade de negócios (88%) e gestão de mudança (88%), ambos relacionados diretamente com a manutenção da disponibilidade dos serviços de TI. As questões tiveram por base recomendações de boas práticas da norma de segurança NBR ISO/IEC 17799:2005 e incluíram diversos controles que visam garantir a confidencialidade, a integridade e a disponibilidade das informações tratadas por órgãos/entidades públicas. O resultado preocupa pois a própria prestação do serviço de uma instituição pública aos cidadãos depende da confiabilidade das informações por ela tratadas e ofertadas. O Auditor de TI pode ter papel fundamental no aperfeiçoamento da gestão 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.

179. Quanto ao desenvolvimento de sistemas de informação, observou-se que 51% dos pesquisados declararam não possuir metodologia de desenvolvimento de sistemas. Esse resultado representa um risco de produção de software de baixa qualidade, bem como maior dificuldade no gerenciamento do processo de desenvolvimento, o que representa risco de má gestão dos recursos. Além disso, identificou-se o uso de sistemas transacionais com acesso via Internet para as atividades de prestação de serviço ao cidadão por 76% das organizações. Essas informações indicam que é relevante que o Auditor de TI esteja preparado para recomendar controles relacionados às boas práticas dos modelos de desenvolvimento de sistemas e, também, avaliar os controles especificamente relacionados às tecnologias de sistemas transacionais via Internet.

180. Sobre gestão de níveis de serviço, 89% dos pesquisados declararam não realizá-la para os serviços prestados internamente, e 74% não o fazem para os serviços contratados. Essa gestão é o principal instrumento de negociação de qualidade de serviço entre as gerências de TI e os seus clientes, e sua ausência em quantidade tão expressiva de organizações preocupa pelo risco tanto de clientes insatisfeitos quanto de investimentos inadequados.

181. Quanto à existência de processo formal de contratação de TI, 46% dos órgãos/entidades consultados informaram não adotá-lo. Essa informação, associada ao fato de que 47% dos pesquisados não realizam análise de custo/benefício das contratações de TI e 40% das organizações consultadas não explicitam os benefícios para a obtenção dos resultados institucionais esperados com cada contratação de TI, sugere que há muito trabalho a ser feito para a melhoria das aquisições de bens e serviços de TI nos órgãos/entidades da Administração Pública Federal.

182. Na gestão dos contratos de TI, a situação não é confortável já que mais da metade (55%) das organizações consultadas não adotam processo formal de trabalho para essa atividade. Além disso, um percentual expressivo (65%) das organizações consultadas não realiza periodicamente reuniões com os contratados para avaliação da execução de cada contrato de TI e, 57% não exigem, em contrato, que o conhecimento seja transferido pelos prestadores de serviço aos servidores do órgão/entidade. Assim, 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 e baixa qualidade de serviços contratados.

183. Sobre Auditorias de TI, 60% dos pesquisados declararam não ter realizado Auditorias de TI nos últimos cinco anos. Dentre os órgãos/entidades que realizam esses trabalhos, a maioria (68%) executou de uma a

cinco Auditorias nos últimos cinco anos. Tal resultado indica que a realização de Auditorias de TI em bases periódicas não é uma realidade entre os pesquisados e, portanto, esse recurso não é utilizado de maneira contínua para melhoria da governança de TI.

184. Em paralelo aos itens relacionados à governança, foram identificados os principais sistemas utilizados pelos órgãos/entidades da Administração Pública Federal pesquisados e as bases de dados associadas. Com essas informações, o planejamento das fiscalizações da Sefti contará com subsídios valiosos para seu aprimoramento.

185. Diante do quadro apresentado, 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.

186. 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.

187. 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.

13. Proposta de encaminhamento

188. Ante o exposto, submetemos os autos à consideração superior, com fulcro no art. 43, inciso I, da Lei n.º 8.443/1992, c/c o art. 250, incisos II e III, do Regimento Interno do TCU, com as seguintes propostas:

I - recomendar ao Conselho Nacional de Justiça que:

a) promova ações com o objetivo de disseminar a importância do planejamento estratégico e induzir, mediante orientação normativa, os órgãos do Poder Judiciário a realizarem ações para implantação e/ou aperfeiçoamento de planejamento estratégico institucional, planejamento estratégico de TI e comitê diretivo de TI (parágrafos 17 a 32);

b) promova as ações cabíveis quanto à estrutura de pessoal de TI nos órgãos do Poder Judiciário (parágrafos 34 a 52);

c) promova ações com objetivo de disseminar a importância do gerenciamento da segurança da informação e induzir, mediante orientação normativa, os órgãos do Poder Judiciário a realizarem ações para implantação e/ou aperfeiçoamento da gestão da continuidade do negócio, da gestão de mudanças, da gestão de capacidade, da classificação da informação, da gerência de incidentes, da análise de riscos de TI, da área específica para gerenciamento da segurança da informação, da política de segurança da informação e dos procedimentos de controle de acesso (parágrafos 54 a 87.11);

d) promova ações com objetivo de disseminar a importância da adoção de metodologia de desenvolvimento de sistemas e induzir os órgãos do Poder Judiciário a realizarem ações para implantação e/ou aperfeiçoamento dessa metodologia (parágrafos 89 a 93.1);

e) promova ações com objetivo de disseminar a importância de gestão de níveis de serviço e induzir os órgãos do Poder Judiciário a realizarem ações para implantação e/ou aperfeiçoamento de acordos de níveis de serviço (parágrafos 95 a 106);

f) promova ações com objetivo de disseminar a importância de processo de trabalho formalizado de contratação de bens e serviços de TI e induzir, mediante orientação normativa nos moldes recomendados pelo item 9.4 do Acórdão 786/2006-TCU-Plenário, os órgãos do Poder Judiciário a realizarem ações para implantação e/ou aperfeiçoamento do processo de contratação de TI (parágrafos 108 a 125);

g) promova ações com objetivo de disseminar a importância de processo de trabalho formalizado de gestão de contratos de TI e induzir, mediante orientação normativa nos moldes recomendados pelo item 9.4 do Acórdão 786/2006-TCU-Plenário, os órgãos do Poder Judiciário a realizarem ações para implantação e/ou aperfeiçoamento desse processo de gestão (parágrafos 127 a 148);

h) promova ações com objetivo de garantir que as propostas orçamentárias para a área de TI dos órgãos do Poder Judiciário sejam elaboradas com base nas atividades que efetivamente pretendam realizar e alinhadas aos objetivos de negócio (parágrafos 150 a 159);

i) promova ações para estimular a realização de Auditorias de TI nos órgãos do Poder Judiciário (parágrafos 161 a 172.1);

II - recomendar ao Conselho Nacional do Ministério Público que:

a) promova ações com objetivo de disseminar a importância do planejamento estratégico e induzir, mediante orientação normativa, os órgãos do Ministério Público a realizarem ações para implantação e/ou aperfeiçoamento de planejamento estratégico institucional, planejamento estratégico de TI e comitê diretivo de TI (parágrafos 17 a 32);

b) promova as ações cabíveis quanto à estrutura de pessoal de TI nos órgãos do Ministério Público (parágrafos 34 a 52);

c) promova ações com objetivo de disseminar a importância do gerenciamento da segurança da informação e induzir, mediante orientação normativa, os órgãos do Ministério Público a realizarem ações para implantação e/ou aperfeiçoamento da gestão da continuidade do negócio, da gestão de mudanças, da gestão de capacidade, da classificação da informação, da gerência de incidentes, da análise de riscos de TI, da área específica para gerenciamento da segurança da informação, da política de segurança da informação e dos procedimentos de controle de acesso (parágrafos 54 a 87.11);

d) promova ações com objetivo de disseminar a importância da adoção de metodologia de desenvolvimento de sistemas e induzir os órgãos do Ministério Público a realizarem ações para implantação e/ou aperfeiçoamento dessa metodologia (parágrafos 89 a 93.1);

e) promova ações com objetivo de disseminar a importância de gestão de níveis de serviço e induzir os órgãos do Ministério Público a realizarem ações para implantação e/ou aperfeiçoamento de acordos de níveis de serviço (parágrafos 95 a 106);

f) promova ações com objetivo de disseminar a importância de processo de trabalho formalizado de contratação de bens e serviços de TI e induzir, mediante orientação normativa nos moldes recomendados pelo item 9.4 do Acórdão 786/2006-TCU-Plenário, os órgãos do Ministério Público a realizarem ações para implantação e/ou aperfeiçoamento do processo de contratação de TI (parágrafos 108 a 125);

g) promova ações com objetivo de disseminar a importância de processo de trabalho formalizado de gestão de contratos de TI e induzir, mediante orientação normativa nos moldes recomendados pelo item 9.4 do Acórdão 786/2006-TCU-Plenário, os órgãos do Ministério Público a realizarem ações para implantação e/ou aperfeiçoamento desse processo de gestão (parágrafos 127 a 148);

h) promova ações com objetivo de garantir que as propostas orçamentárias para a área de TI dos órgãos do Ministério Público sejam elaboradas com base nas atividades que efetivamente pretendam realizar e alinhadas aos objetivos de negócio (parágrafos 150 a 159);

i) promova ações para estimular a realização de Auditorias de TI nos órgãos do Ministério Público (parágrafos 161 a 172.1);

III - recomendar ao Gabinete de Segurança Institucional da Presidência da República que promova ações com objetivo de disseminar a importância do gerenciamento da segurança da informação e induzir, mediante orientação normativa, os órgãos/entidades da Administração Pública Federal a realizarem ações para implantação e/ou aperfeiçoamento da gestão da continuidade do negócio, da gestão de mudanças, da gestão de capacidade, da classificação da informação, da gerência de incidentes, da análise de riscos de TI, da área específica para gerenciamento da segurança da informação, da política de segurança da informação e dos procedimentos de controle de acesso (parágrafos 54 a 87.11);

IV - recomendar à Controladoria-Geral da União que realize regularmente Auditorias de TI e/ou promova ações para estimular a realização dessas Auditorias nos órgãos/entidades da Administração Pública Federal (parágrafos 161 a 172.1);

V - recomendar ao Ministério do Planejamento, Orçamento e Gestão que promova as ações cabíveis quanto à estrutura de pessoal de TI nos órgãos/entidades da Administração Pública Federal (parágrafos 34 a 52);

VI - recomendar à Secretaria de Logística e Tecnologia da Informação (SLTI) do Ministério do Planejamento, Orçamento e Gestão que:

a) promova ações com objetivo de disseminar a importância do planejamento estratégico e induzir, mediante orientação normativa, os órgãos/entidades da Administração Pública Federal a realizarem ações para implantação e/ou aperfeiçoamento de planejamento estratégico institucional, planejamento estratégico de TI e comitê diretivo de TI (parágrafos 17 a 32);

b) promova ações com o objetivo de disseminar a importância da adoção de metodologia de desenvolvimento de sistemas e induzir os órgãos/entidades da Administração Pública Federal a realizarem ações para implantação e/ou aperfeiçoamento dessa metodologia (parágrafos 89 a 93.1);

c) promova ações com o objetivo de disseminar a importância de gestão de níveis de serviço e induzir os órgãos/entidades da Administração Pública Federal a realizarem ações para implantação e/ou aperfeiçoamento de acordos de níveis de serviço (parágrafos 95 a 106);

d) promova ações com objetivo de garantir que as propostas orçamentárias para a área de TI dos órgãos/entidades da Administração Pública Federal sejam elaboradas com base nas atividades que efetivamente pretendam realizar e alinhadas aos objetivos de negócio (parágrafos 150 a 159);

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

VIII - recomendar à Secretaria-Geral da Presidência (Segepres) e à Secretaria-Geral de Administração (Segedam) que adotem as providências contidas no item I no âmbito deste Tribunal;

IX - determinar à Secretaria-Geral de Controle Externo (Segecex) que oriente suas unidades técnicas para considerarem as informações armazenadas na Sefti quando forem executar ações de controle em governança de TI (parágrafos 12, 13, 16, 92.2 e 179.3);

X - assinar prazo de 30 dias, com fulcro no § 1º do art. 42 da Lei n.º 8.443/1992, para que os integrantes da lista disponível no Apêndice III deste relatório enviem, em meio magnético, conforme orientação da Sefti, as informações necessárias para resposta ao questionário utilizado neste levantamento;

XI - remeter cópias do Acórdão que vier a ser adotado nestes autos, acompanhado dos respectivos Relatório e Voto, e deste Relatório de Levantamento:

a) à Comissão de Ciência, Tecnologia, Inovação, Comunicação e Informática do Senado Federal;

b) à Subcomissão Permanente de Serviços de Informática do Senado Federal;

c) à Diretoria-Geral do Senado Federal;

d) à Secretaria Especial de Informática do Senado Federal (Prodasen);

e) à Comissão de Fiscalização Financeira e Controle da Câmara dos Deputados;

f) à Comissão de Trabalho, de Administração e Serviço Público da Câmara dos Deputados;

g) à Comissão de Ciência e Tecnologia, Comunicação e Informática da Câmara dos Deputados;

h) à Subcomissão Permanente de Ciência e Tecnologia e Informática da Câmara dos Deputados;

i) à Diretoria-Geral da Câmara dos Deputados;

j) ao Centro de Informática da Câmara dos Deputados;

k) ao Conselho Nacional de Justiça;

l) ao Conselho Nacional do Ministério Público;

m) ao Gabinete de Segurança Institucional da Presidência da República;

n) à Controladoria-Geral da União;

o) ao Ministério do Planejamento, Orçamento e Gestão;

p) à Secretaria de Logística Tecnologia da Informação (SLTI) do Ministério do Planejamento, Orçamento e Gestão;

q) à Secretaria de Orçamento Federal (SOF) do Ministério do Planejamento, Orçamento e Gestão;

r) ao Departamento de Coordenação e Controle das Empresas Estatais (Dest) da Secretaria-Executiva do Ministério do Planejamento, Orçamento e Gestão;

s) aos integrantes da lista disponível no Apêndice II deste relatório;

XII - remeter relatório individualizado contendo a posição de cada órgão/entidade e do seu segmento de atuação aos integrantes da lista disponível no Apêndice II deste relatório;

XIII - 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;

XIV - arquivar os presentes autos na Secretaria de Fiscalização de Tecnologia da Informação (Sefti)".

É o Relatório.

**Voto do Ministro Relator**

Os presentes autos referem-se a 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 governança de Tecnologia da Informação - TI, identificando as áreas onde o TCU deve, preferencialmente, atuar como indutor do processo de aperfeiçoamento do setor.

Dos achados de Auditoria discriminados pela equipe encarregada dos trabalhos, gostaria de destacar aqueles que considerei mais relevantes.

O primeiro diz respeito à constatação da ausência, em 64% dos órgãos/entidades pesquisados, de uma Política de Segurança da Informação formalmente definida na organização, motivada por diretriz institucional. Consoante destacado, é a partir dessa política que derivam os documentos específicos para cada meio de armazenamento, transporte, manipulação ou tratamento específico da segurança da informação em TI.

Verificou-se também a ausência de Plano de Continuidade de Negócios, em cerca de 88% dos pesquisados. Tal plano, nos termos consignados no Relatório, deve abarcar o conjunto de documentos que contém a definição das responsabilidades individuais, dos procedimentos de emergência, dos procedimentos operacionais temporários e dos procedimentos de recuperação.

Essas constatações preocupam-me porque revelam certo descompasso entre a gestão da segurança da informação e os objetivos intrínsecos da instituição, podendo boa parte da administração pública estar vulnerável à ocorrência de interrupção de serviços, perda de dados, fraudes e paralisação de funções essenciais.

Outro ponto que vale ser ressaltado refere-se ao fato de que 47% dos órgãos/entidades pesquisados não tem planejamento estratégico institucional em vigor e 59% não fazem planejamento estratégico de TI. A ausência de planejamento afeta diretamente a eficácia e a efetividade das propostas orçamentárias e das contratações de bens e serviços de informática.

Realmente, a partir dos dados obtidos, deduziu-se 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".

Da mesma forma, no tocante à contratação de bens e serviços de TI, apurou-se que percentual expressivo de entes (46%) não adota processo de trabalho formalizado e padronizado, que demonstre o custo, a oportunidade e os benefícios a serem obtidos pela organização.

Tal cenário remete inevitavelmente à alocação indevida de recursos de TI por desarmonia com as prioridades da organização.

Constatou-se também que mais da metade dos entes pesquisados não adota processo formal de trabalho para gestão de contratos de tecnologia da informação, o que pode acarretar baixa qualidade dos serviços prestados, interrupção na execução de contratos e, em última instância, o desperdício de recursos.

Quanto à estrutura de pessoal de TI, além de quantitativo deficiente de servidores efetivos, com significativo percentual de colaboradores externos nos órgãos/entidades pesquisados, foi identificado ainda percentual elevado de funcionários sem formação específica no setor. Como bem assinalado pela unidade técnica, tal circunstância aumenta o risco de perda de conhecimento organizacional, porquanto apreendido por trabalhadores não compromissados com a instituição.

Merece registro, ainda, os percentuais elevados dos órgãos/entidades pesquisados que não executam seja gestão de acordos de níveis de serviços prestados internamente (89%), seja gestão de acordos de níveis de serviços contratados externamente (74%). Conforme salientado, é a partir desses ajustes que se estabelece a qualidade dos serviços de TI em função das necessidades da organização, devendo neles integrar como indicadores, entre outros, a disponibilidade da infra-estrutura de rede, o desempenho dos sistemas e o tempo de solução de problemas.

Não se pode ignorar que os fatos evidenciados neste Levantamento de Auditoria preocupam, pois sugerem um quadro inquietante da governança de TI na Administração Pública Federal.

Contudo, há que vê-los com cautela, já que a própria equipe de fiscalização registrou que "as informações coletadas foram declaradas pelos gestores e não verificadas pela equipe junto aos órgãos/entidades", não tendo sido também, nesse primeiro momento, avaliada a pertinência e a qualidade dos documentos produzidos e anexados pelos órgãos/entidades. Ainda que reconheça o caráter preliminar dos trabalhos, penso que maior solidez dos resultados adviria com uma correspondente confirmação dos fatos em algumas entidades selecionadas por amostragem estatística.

Nada obstante, diante das informações coligidas e da relevância da gestão e do uso de Tecnologia da Informação - TI para que os diversos órgãos e entidades da Administração Pública Federal consigam cumprir suas missões, considero imprescindível a realização de fiscalizações com o objetivo de verificar in loco a situação das áreas consideradas mais críticas. Faz-se necessária, ademais, a atualização regular das informações coletadas neste levantamento de modo a permitir que o Tribunal tenha condições de acompanhar a evolução da situação então encontrada. Nesse sentido, acrescentei determinação à Sefti a respeito.

Ante o exposto, VOTO por que seja adotada a deliberação que ora submeto à apreciação deste Plenário.

Sala das Sessões Ministro Luciano Brandão Alves de Souza, em 13 de agosto de 2008.

GUILHERME PALMEIRA

Ministro-Relator

**Declaração de Voto**

Considerando a relevância do tema, louvo a iniciativa deste tribunal em determinar a realização de levantamento 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".

O Relatório produzido pela Sefti teve como principal objetivo obter informações para elaboração de mapa com a situação da governança de TI na Administração Pública Federal.

No percurso do alcance desse objetivo, o Tribunal identificou as seguintes lacunas:

a) ausência de planejamento estratégico institucional

b) quantidade reduzida e deficiência de qualificação de servidores na área de TI

c) ausência de carreira específica para a área;

d) ausência de política de segurança da informação, dentre outras.

O resultado alcançado pelo presente processo justifica, assim, a atuação deste Tribunal como instrumento de aperfeiçoamento da gestão publica. Some-se a isso a significância dos recursos empregados pela Administração Federal na área de tecnologia da informação, que, segundo dados do Siafi de 2007, ultrapassam a soma de seis bilhões de reais por ano.

Vejo, portanto, com satisfação, o conjunto de recomendações sugerido pelo relator da matéria, o qual, certamente, se devidamente implementado, trará grande contribuição para o alcance da governança adequada de TI no setor público federal.

Com esse breve comentário, manifesto minha concordância com o voto proferido pelo relator, ao tempo em que parabenizo a equipe técnica que atuou no processo.

AROLDO CEDRAZ

Ministro-Relator

**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

**Quorum**

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

**Publicação**

Ata 32/2008 - Plenário

Sessão 13/08/2008