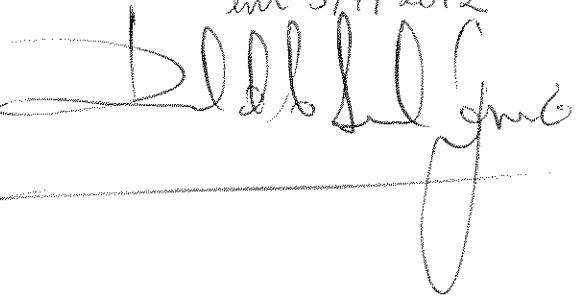


Junta-se ao processado

do AVS nº 29 de 2012

em 5/7/2012



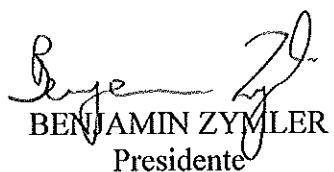
Aviso nº 792 -GP/TCU

Brasília, 29 de junho de 2012.

Senhor Presidente,

Encaminho, em anexo, cópia do Acórdão nº 1.233/2012 (acompanhado dos respectivos Relatório e Voto), para conhecimento, em especial quanto ao item 9.44.5 da referida Deliberação, proferida pelo Plenário do TCU, na Sessão de 23/5/2012, ao apreciar o processo nº TC-011.772/2010-7, que trata de Relatório de Auditoria.

Atenciosamente,

  
BENJAMIN ZYMLER  
Presidente

A Sua Excelência o Senhor  
Senador DELCÍDIO DO AMARAL  
Presidente da Comissão de Assuntos Econômicos do Senado Federal  
Brasília - DF

156

## ACÓRDÃO Nº 1233/2012 – TCU – Plenário

1. Processo nº TC 011.772/2010-7.
2. Grupo I – Classe de Assunto V: Relatório de Auditoria
3. Interessados/Responsáveis:
  - 3.1. Interessada: Secretaria de Fiscalização de Tecnologia da Informação – Sefti.
  4. Órgão: Ministério da Saúde (vinculador).
  5. Relator: Ministro Aroldo Cedraz.
  6. Representante do Ministério Público: Subprocurador-Geral Paulo Soares Bugarin.
  7. Unidade Técnica: Sec. de Fisc. de Tec. da Informação (SEFTI).
  8. Advogado constituído nos autos: não há.
9. Acórdão:

Trata-se de relatório consolidado das ações do TMS 6/2010, cujo objeto foi avaliar se a gestão e o uso da tecnologia da informação estão de acordo com a legislação e aderentes às boas práticas de governança de TI.

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

9.1. recomendar, com fundamento no art. 43, inciso I, da Lei 8.443/1992, c/c o art. 250, inciso III do Regimento Interno do TCU, à Câmara de Políticas de Gestão, Desempenho e Competitividade (CGDC) do Conselho de Governo que:

9.1.1 em atenção Decreto-Lei 200/1967, art. 6º, inciso I, e art. 7º, normatize a obrigatoriedade de que todos os entes sob sua jurisdição estabeleçam processo de planejamento estratégico institucional, observando as boas práticas sobre o tema, a exemplo do critério de avaliação 2 do Gespública, contemplando, pelo menos (subitem II.1):

9.1.1.1. elaboração, com participação de representantes dos diversos setores da organização, de um documento que materialize o plano estratégico institucional de longo prazo, contemplando, pelo menos, objetivos, indicadores e metas para a organização;

9.1.1.2. aprovação, pela mais alta autoridade da organização, do plano estratégico institucional;

9.1.1.3. desdobramento do plano estratégico pelas unidades executoras;

9.1.1.4. divulgação do plano estratégico institucional para conhecimento dos cidadãos brasileiros, exceto nos aspectos formalmente declarados sigilosos ou restritos;

9.1.1.5. acompanhamento periódico do alcance das metas estabelecidas, para correção de desvios;

9.1.1.6. divulgação interna e externa do alcance das metas, ou dos motivos de não as ter alcançado;

9.1.2. em atenção Decreto-Lei 200/1967, art. 6º, inciso I, e art. 7º, normatize a obrigatoriedade de que todos os entes sob sua jurisdição estabeleçam processo de planejamento estratégico de TI, observando as boas práticas sobre o tema, a exemplo do processo “PO1 – Planejamento Estratégico de TI” do Cobit 4.1, contemplando, pelo menos (subitem II.2):

9.1.2.1. elaboração, com participação de representantes dos diversos setores da organização, de um documento que materialize o plano estratégico de TI, contemplando, pelo menos:

9.1.2.1.1. objetivos, indicadores e metas para a TI organizacional, sendo que os objetivos devem estar explicitamente alinhados aos objetivos de negócio constantes do plano estratégico institucional;

9.1.2.1.2. alocação de recursos (financeiros, humanos, materiais etc);

9.1.2.1.3. estratégia de terceirização;

9.1.2.2. aprovação, pela mais alta autoridade da organização, do plano estratégico de TI;

9.1.2.3. desdobramento do plano estratégico de TI pelas unidades executoras;

9.1.2.4. divulgação do plano estratégico de TI para conhecimento dos cidadãos brasileiros, exceto nos aspectos formalmente declarados sigilosos ou restritos;

9.1.2.5. acompanhamento periódico do alcance das metas estabelecidas, para correção de desvios;

9.1.2.6. divulgação interna e externa do alcance das metas, ou os motivos de não as ter alcançado;

9.1.3. em atenção ao Decreto-Lei 200/1967, art. 6º, V, estabeleça, normativamente para todos os entes sob sua jurisdição, a obrigatoriedade de a alta administração implantar uma estrutura de controles internos, mediante a definição de atividades de controle em todos os níveis da organização para mitigar os riscos de suas atividades no processo de planejamento estratégico institucional (subitem II.11);

9.2. recomendar, com fundamento na Lei 8.443/1992, art. 43, inciso I, c/c RITCU, art. 250, inciso III, à Secretaria de Logística e Tecnologia da Informação (SLTI/MP) que:

9.2.1. normatize a obrigatoriedade de que os entes sob sua jurisdição estabeleçam comitês de TI, observando as boas práticas sobre o tema, a exemplo do Cobit 4.1, PO4.2 – comitê estratégico de TI e PO4.3 – comitê diretor de TI (subitem II.3);

9.2.2. oriente os órgãos e entidades sob sua jurisdição a realizar avaliação quantitativa e qualitativa do pessoal do setor de TI, de forma a delimitar as necessidades de recursos humanos necessárias para que estes setores realizem a gestão das atividades de TI da organização (subitem II.3);

9.2.3. elabore um modelo de processo de software para a os entes sob sua jurisdição, observando as boas práticas sobre o tema (e.g., NBR ISO/IEC 12.207 e 15.504, MPS.BR, CMMI; subitem II.5);

9.2.4. estabeleça a obrigatoriedade de que os entes sob sua jurisdição formalizem um processo de software para si, observando as boas práticas sobre o tema (e.g., NBR ISO/IEC 12.207 e 15.504, MPS.BR, CMMI; subitem II.5);

9.2.5. elabore um modelo de estrutura de gerenciamento de projetos para os entes sob sua jurisdição, observando as boas práticas sobre o tema (e.g., PMBoK; subitem II.6);

9.2.6. estabeleça a obrigatoriedade de que os entes sob sua jurisdição formalizem um processo de gerenciamento de projetos para si, observando as boas práticas sobre o tema (e.g., PMBoK; subitem II.6);

9.2.7. elabore um modelo de processo de gestão de serviços para os entes sob sua jurisdição que inclua, pelo menos, gestão de configuração, gestão de incidentes e gestão de mudança, observando as boas práticas sobre o tema (e.g., NBR ISO/IEC 20.000, Itil; subitem II.7);

9.2.8. estabeleça a obrigatoriedade de que os entes sob sua jurisdição formalizem processos de gestão de serviços para si, incluindo, pelo menos, gestão de configuração, gestão de incidentes e gestão de mudança, observando as boas práticas sobre o tema (e.g., NBR ISO/IEC 20.000, Itil; subitem II.7);

9.2.9. em atenção ao Decreto-Lei 200/1967, art. 6º, V, estabeleça, normativamente para todos os entes sob sua jurisdição, a obrigatoriedade de a alta administração implantar uma estrutura de controles internos mediante a definição de atividades de controle em todos os níveis da organização para mitigar os riscos de suas atividades, pelo menos nos seguintes processos (subitem II.11):

9.2.9.1. planejamento estratégico de TI;

9.2.9.2. funcionamento dos comitês de TI;

9.2.9.3. processo orçamentário de TI;

9.2.9.4. processo de software;

9.2.9.5. gerenciamento de projetos;

9.2.9.6. gerenciamento de serviços de TI;

9.2.9.7. segurança da informação;

9.2.9.8. gestão de pessoal de TI;

9.2.9.9. contratação e gestão de soluções de TI;

9.2.9.10. monitoração do desempenho da TI organizacional.

9.3. determinar, com fundamento na Lei 8.443/1992, art. 43, inciso I, c/c RITCU, art. 250, inciso II, à Secretaria de Logística e Tecnologia da Informação (SLTI/MP) que:

9.3.1. em atenção ao previsto no Decreto 7.579/2011, art. 4º, V, oriente os entes sob sua jurisdição sobre a necessidade de vincular seus contratos de serviços de desenvolvimento ou manutenção de software a um processo de software, pois, sem esta vinculação, o objeto do contrato não estará precisamente definido, em desconformidade com o disposto na Lei 8.666/1993, art. 6º, inciso IX (subitem II.5);

9.3.2. em atenção ao disposto no Decreto 1.094/1994, art. 2º, inciso I, oriente os órgãos e entidades sob sua jurisdição para que (subitem III.1):

9.3.2.1. ao realizarem licitação com finalidade de criar ata de registro de preços atentem que:

9.3.2.1.1. devem fundamentar formalmente a criação de ata de registro de preços, e.g., por um dos incisos do art. 2º do Decreto 3.931/2001 (Acórdão 2.401/2006-TCU-Plenário);

9.3.2.1.2. devem praticar todos os atos descritos no Decreto 3.931/2001, art. 3º, § 2º, em especial o previsto no seu inciso I, que consiste em “convidar mediante correspondência eletrônica ou outro meio eficaz, os órgãos e entidades para participarem do registro de preços”;

9.3.2.1.3. o planejamento da contratação é obrigatório, sendo que se o objeto for solução de TI, caso seja integrante do Sisp, deve executar o processo de planejamento previsto na IN – SLTI/MP 4/2010 (IN – SLTI/MP 4/2010, art. 18, inciso III) ou, caso não o seja, deve realizar os devidos estudos técnicos preliminares (Lei 8.666/1993, art. 6º, inciso IX);

9.3.2.1.4. a fixação, no termo de convocação, de quantitativos (máximos) a serem contratados por meio dos contratos derivados da ata de registro de preços, previstos no Decreto 3.931/2001, art. 9º, inciso II, é obrigação e não faculdade do gestor (Acórdão 991/2009-TCU-Plenário, Acórdão 1.100/2007-TCU-Plenário e Acórdão 4.411/2010-TCU-2ª Câmara);

9.3.2.1.5. em atenção ao princípio da vinculação ao instrumento convocatório (Lei 8.666/1993, art. 3º, caput), devem gerenciar a ata de forma que a soma dos quantitativos contratados em todos os contratos derivados da ata não supere o quantitativo máximo previsto no edital;

9.3.3. quando realizarem adesão à ata de registro de preços atentem que:

9.3.3.1. o planejamento da contratação é obrigatório, sendo que se o objeto for solução de TI, caso seja integrante do Sisp, deve executar o processo de planejamento previsto na IN – SLTI/MP 4/2010 (IN – SLTI/MP 4/2010, art. 18, inciso III) ou, caso não o seja, realizar os devidos estudos técnicos preliminares (Lei 8.666/1993, art. 6º, inciso IX);

9.3.3.2. devem demonstrar formalmente a vantajosidade da adesão, nos termos do Decreto 3.931/2001, art. 8º;

9.3.3.3. as regras e condições estabelecidas no certame que originou a ata de registro de preços devem ser conformes as necessidades e condições determinadas na etapa de planejamento da contratação (Lei 8.666/1993, art. 6º, inciso IX, alínea d, c/c o art. 3º, § 1º, inciso I, e Lei 10.520/2002, art. 3º, inciso II);

9.3.4. em atenção ao Decreto 7.579/2011, art. 4º, V, oriente os órgãos e entidades sob sua jurisdição para que, caso possuam contratos com empresas públicas prestadoras de serviços de TI (subitem III.3):

9.3.4.1. analisem a conformidade dos termos do contrato e do projeto básico e verifiquem se:

9.3.4.1.1. foi realizado o adequado planejamento da contratação, consistindo na execução do processo de planejamento previsto na IN – SLTI/MP 4/2010 se for integrante do Sisp (IN – SLTI/MP 4/2010, art. 18, inciso II) ou, caso não o seja, se foram realizados os devidos estudos técnicos preliminares (Lei 8.666/1993, art. 6º, inciso IX);

9.3.4.1.2. as especificações do objeto são precisas e suficientes, em conformidade com a Lei 8.666/1993, art. 6º, IX;

9.3.4.1.3. os critérios de mensuração dos serviços são precisos e suficientes, de acordo com o determinado na Lei 8.666/1993, art. 6º, IX, e (também necessários de acordo com a IN – SLTI 4/2010, art. 14, II, a);

9.3.4.1.4. a metodologia de avaliação da adequação dos produtos é precisa e suficiente, de acordo com o determinado na Lei 8.666/1993, art. 6º, IX, e (também necessária de acordo com a IN – SLTI 4/2010, art. 14, II, c);

9.3.4.1.5. as cláusulas de penalidades contidas na Lei 8.666/1993, art. 87, de acordo com o determinado na Lei 8.666/1993, art. 55, VII e VIII, são detalhadas e atendem aos princípios da razoabilidade, proporcionalidade e prudência (e também o previsto na IN – SLTI 4/2010, art. 15, III, h);

9.3.4.1.6. o modelo de pagamento é vinculado a resultados, obedecendo ao princípio constitucional da eficiência (e também ao previsto no Decreto 2.271/1997, art. 3º, § 1º, e na IN – SLTI 4/2010, art. 15, §§ 2º e 3º);

9.3.4.1.7. a justificativa dos preços contratados é adequadamente fundamentada em arrazoada pesquisa de mercado, de acordo com o determinado na Lei 8.666/1993, art. 26, III, inclusive com a análise da planilha de composição de custos dos serviços, necessária segundo a Lei 8.666/1993, art. 7º, § 2º, II;

9.3.4.2. caso a análise realizada de acordo com orientação acima indique desconformidade, elaborem plano de ação para providenciar as adequações contratuais necessárias, que deverão ser realizadas no prazo de 180 dias;

9.3.4.3. mantenham o resultado da análise de conformidade empreendida em documento formalizado, à disposição dos controles externo e interno;

9.3.4.4. informem seu órgão de assessoramento jurídico e sua unidade de auditoria interna da análise que está sendo empreendida e do resultado obtido;

9.3.5. em atenção ao Decreto 7.579/2011, art. 4º, V, oriente os órgãos e entidades sob sua jurisdição que (subitem III.3):

9.3.5.1. mesmo que a execução de seus serviços de tecnologia da informação seja transferida mediante contrato ou outro acordo a outra organização pública, como as empresas públicas prestadoras de serviços de tecnologia da informação, as atividades de gestão (planejamento, coordenação, supervisão e controle) de TI devem ser acometidas a pessoas integrantes do quadro permanente, ou, excepcionalmente, a detentores de cargo em comissão, da organização contratante, não podendo ser delegadas a pessoas direta ou indiretamente ligadas à contratada;

9.3.5.2. a contratação de empresas públicas prestadoras de serviços de tecnologia da informação não afasta a necessidade de a organização contratante manter estrutura de governança de TI própria, que direcione e controle a gestão desses contratos bem como a gestão de todos os processos de TI da organização;

9.4. recomendar, com fundamento na Lei 8.443/1992, art. 43, inciso I, c/c RITCU, art. 250, inciso III, ao Ministério do Planejamento, Orçamento e Gestão que:

9.4.1. em atenção ao Decreto 5.707/2006, art. 5º, § 2º, c/c o art. 1º, III, discipline a forma de acesso às funções de liderança nos setores de Tecnologia da Informação, considerando as competências multidisciplinares necessárias para estas funções, que incluem, mas não se limitam a conhecimentos em TI (subitem II.3).

9.5. recomendar, com fundamento na Lei 8.443/1992, art. 43, inciso I, c/c RITCU, art. 250, inciso III, à Secretaria de Orçamento Federal (SOF/MP) que:

9.5.1. implante controles para mitigar os riscos de ocorrência de propostas orçamentárias que indevidamente não tenham previsão de despesas com tecnologia da informação (subitem II.4);

9.5.2 com base no disposto na Lei 10.180/2001, art. 8º, II, c/c Decreto 7.063/2010, art. 17, II, normatize a obrigatoriedade de que todos os entes sob sua jurisdição estabeleçam processo de trabalho formal para elaboração e acompanhamento da execução do orçamento, contemplando, pelo menos, a obrigatoriedade de que (subitem II.4):

9.5.2.1. a solicitação do orçamento de TI seja feita com base nas estimativas de custos das atividades que pretendam executar, alinhadas aos objetivos do negócio da organização;

9.5.2.2. haja acompanhamento, ao longo do exercício financeiro, dos gastos efetuados especificamente com TI.

9.6. determinar, com fundamento na Lei 8.443/1992, art. 43, inciso I, c/c RITCU, art. 250, inciso II, à Secretaria de Orçamento Federal (SOF/MP) que, em atenção ao Decreto-Lei 200/1967, art. 75, encaminhe, à Secretaria de Fiscalização de Tecnologia da Informação do Tribunal de Contas da União (Sefti/TCU):

9.6.1. no prazo de quinze dias após o envio do projeto da Lei de Diretrizes Orçamentárias ao Congresso Nacional, as medidas adotadas para permitir a identificação clara, objetiva e transparente da previsão dos gastos em TI no Orçamento Geral da União ou, alternativamente, normatize o processo de trabalho para obtenção de ditas informações, valendo-se da competência prevista no Decreto 7.063/2010, art. 17, II (subitem II.4);

9.6.2. no prazo de quinze dias após o envio do Projeto da Lei Orçamentária Anual (PLOA) ao Congresso Nacional, relação da previsão das despesas com TI que constam do PLOA, em meio magnético, na forma de banco de dados editável ou planilha eletrônica, no maior detalhamento possível, preferencialmente no formato encaminhado por meio do Ofício 06/SECAD/SOF/MP, de 25/2/2010, ou, alternativamente, disponibilize funcionalidade nos seus sistemas informatizados para que a Sefti/TCU possa acessar os dados requeridos para o atendimento da determinação (subitem II.4);

9.6.3. no prazo de quinze dias após a publicação da Lei Orçamentária Anual (LOA), relação da previsão das despesas com TI que constam da LOA, em meio magnético, na forma de banco de dados editável ou planilha eletrônica, no maior detalhamento possível, preferencialmente no formato encaminhado por meio do Ofício 06/SECAD/SOF/MP, de 25/2/2010, ou, alternativamente, disponibilize funcionalidade nos seus sistemas informatizados para que a Sefti/TCU possa acessar os dados requeridos para o atendimento da determinação (subitem II.4).

9.7. determinar, com fundamento na Lei 8.443/1992, art. 43, inciso I, c/c RITCU, art. 250, inciso II, à Departamento de Coordenação e Governança das Estatais (Dest/MP) que: em atenção ao Decreto-Lei 200/1967, art. 75, encaminhe, à Secretaria de Fiscalização de Tecnologia da Informação do Tribunal de Contas da União (Sefti/TCU):

9.7.1. no prazo de quinze dias após o envio do Projeto da Lei Orçamentária Anual (PLOA) ao Congresso Nacional, relação da previsão das despesas com TI que constam do PLOA, em meio magnético, na forma de banco de dados editável ou planilha eletrônica, no maior detalhamento possível, preferencialmente no formato encaminhado por meio do Ofício 163/2010/MP/SE/DEST, de 23/2/2010, ou, alternativamente, disponibilize funcionalidade nos seus sistemas informatizados para que a Sefti/TCU possa acessar os dados requeridos para o atendimento da determinação (subitem II.4);

9.7.2. no prazo de quinze dias após a publicação da Lei Orçamentária Anual (LOA), relação da previsão das despesas com TI que constam da LOA, em meio magnético, na forma de banco de dados editável ou planilha eletrônica, no maior detalhamento possível, preferencialmente no formato encaminhado por meio do Ofício 163/2010/MP/SE/DEST, de 23/2/2010, ou, alternativamente, disponibilize funcionalidade nos seus sistemas informatizados para que a Sefti/TCU possa acessar os dados requeridos para o atendimento da determinação (subitem II.4);

9.7.3. em atenção ao disposto no Decreto 7.063/2010, art. 6º, inciso XII, oriente as entidades sob sua jurisdição para que (subitem III.1):

9.7.3.1. ao realizarem licitação com finalidade de criar ata de registro de preços atentem que:

9.7.3.1.1. devem fundamentar formalmente a criação de ata de registro de preços, e.g., por um dos incisos do art. 2º do Decreto 3.931/2001 (Acórdão 2.401/2006-TCU-Plenário);

9.7.3.1.2. devem praticar todos os atos descritos no Decreto 3.931/2001, art. 3º, § 2º, em especial o previsto no seu inciso I, que consiste em “convidar mediante correspondência eletrônica ou outro meio eficaz, os órgãos e entidades para participarem do registro de preços”;

9.7.3.1.3. o planejamento da contratação é obrigatório, sendo obrigatória a realização dos devidos estudos técnicos preliminares (Lei 8.666/1993, art. 6º, inciso IX);

9.7.3.1.4. a fixação, no termo de convocação, de quantitativos (máximos) a serem contratados por meio dos contratos derivados da ata de registro de preços, previstos no Decreto

3.931/2001, art. 9º, inciso II, é obrigação e não faculdade do gestor (Acórdão 991/2009-TCU-Plenário, Acórdão 1.100/2007-TCU-Plenário e Acórdão 4.411/2010-TCU-2ª Câmara);

9.7.3.1.5. em atenção ao princípio da vinculação ao instrumento convocatório (Lei 8.666/1993, art. 3º, *caput*), devem gerenciar a ata de forma que a soma dos quantitativos contratados em todos os contratos derivados da ata não supere o quantitativo máximo previsto no edital;

9.7.3.2. quando realizarem adesão à ata de registro de preços atentem que:

9.7.3.2.1. o planejamento da contratação é obrigatório, sendo obrigatória a realização dos devidos estudos técnicos preliminares (Lei 8.666/1993, art. 6º, inciso IX);

9.7.3.2.2. devem demonstrar formalmente a vantajosidade da adesão, nos termos do Decreto 3.931/2001, art. 8º;

9.7.3.2.3. as regras e condições estabelecidas no certame que originou a ata de registro de preços devem ser conformes as necessidades e condições determinadas na etapa de planejamento da contratação (Lei 8.666/1993, art. 6º, inciso IX, alínea d, c/c o art. 3º, § 1º, inciso I, e Lei 10.520/2002, art. 3º, inciso II);

9.7.4. em atenção ao disposto no Decreto 7.063/2010, art. 6º, inciso XII, oriente as entidades sob sua jurisdição para que, caso possuam contratos com empresas públicas prestadoras de serviços de TI (subitem III.3):

9.7.4.1. analisem a conformidade dos termos do contrato e do projeto básico e verifiquem se:

9.7.4.1.1. foi realizado o adequado planejamento da contratação, consistindo na execução do processo de planejamento previsto na IN – SLTI/MP 4/2010 se for integrante do Sisp (IN – SLTI/MP 4/2010, art. 18, inciso II) ou, caso não o seja, se foram realizados os devidos estudos técnicos preliminares (Lei 8.666/1993, art. 6º, inciso IX);

9.7.4.1.2. as especificações do objeto são precisas e suficientes, em conformidade com a Lei 8.666/1993, art. 6º, IX;

9.7.4.1.3. os critérios de mensuração dos serviços são precisos e suficientes, de acordo com o determinado na Lei 8.666/1993, art. 6º, IX, e (também necessários de acordo com a IN – SLTI 4/2010, art. 14, II, a);

9.7.4.1.4. a metodologia de avaliação da adequação dos produtos é precisa e suficiente, de acordo com o determinado na Lei 8.666/1993, art. 6º, IX, e (também necessária de acordo com a IN – SLTI 4/2010, art. 14, II, c);

9.7.4.1.5. as cláusulas de penalidades contidas na Lei 8.666/1993, art. 87, de acordo com o determinado na Lei 8.666/1993, art. 55, VII e VIII, são detalhadas e atendem aos princípios da razoabilidade, proporcionalidade e prudência (e também o previsto na IN – SLTI 4/2010, art. 15, III, h);

9.7.4.1.6. o modelo de pagamento é vinculado a resultados, obedecendo ao princípio constitucional da eficiência (e também ao previsto no Decreto 2.271/1997, art. 3º, § 1º, e na IN – SLTI 4/2010, art. 15, §§ 2º e 3º);

9.7.4.1.7. a justificativa dos preços contratados é adequadamente fundamentada em arrazoada pesquisa de mercado, de acordo com o determinado na Lei 8.666/1993, art. 26, III, inclusive com a análise da planilha de composição de custos dos serviços, necessária segundo a Lei 8.666/1993, art. 7º, § 2º, II;

9.7.4.2. caso a análise realizada de acordo com orientação acima indique desconformidade, elaborem plano de ação para providenciar as adequações contratuais necessárias, que deverão ser realizadas no prazo de 180 dias;

9.7.4.3. mantenham o resultado da análise de conformidade empreendida em documento formalizado, à disposição dos controles externo e interno;

9.7.4.4. informem seu órgão de assessoramento jurídico e sua unidade de auditoria interna da análise que está sendo empreendida e do resultado obtido;

9.7.5. em atenção ao disposto no Decreto 7.063/2010, art. 6º, inciso XII, oriente as entidades sob sua jurisdição que (subitem III.3):

9.7.5.1. mesmo que a execução de seus serviços de tecnologia da informação seja transferida mediante contrato ou outro acordo a outra organização pública, como as empresas públicas prestadoras de serviços de tecnologia da informação, as atividades de gestão (planejamento, coordenação, supervisão e controle) de TI devem ser acometidas a pessoas integrantes do quadro permanente, ou, excepcionalmente, a detentores de cargo em comissão, da organização contratante, não podendo ser delegadas a pessoas direta ou indiretamente ligadas à contratada;

9.7.5.2. a contratação de empresas públicas prestadoras de serviços de tecnologia da informação não afasta a necessidade de a organização contratante manter estrutura de governança de TI própria, que direcione e controle a gestão desses contratos bem como a gestão de todos os processos de TI da organização.

9.8. Recomendar, com fundamento na Lei 8.443/1992, art. 43, inciso I, c/c RITCU, art. 250, inciso III, ao Gabinete de Segurança Institucional da Presidência da república (GSI/PR) que:

9.8.1. em atenção à Lei 10.168/2003, art. 6º, IV, articule-se com as escolas de governo, notadamente à Enap, a fim de ampliar a oferta de ações de capacitação em segurança da informação para os entes sob sua jurisdição (subitem II.8);

9.8.2. em atenção a Lei 10.168/2003, art. 6º, IV, oriente os órgãos e entidades sob sua jurisdição que a implantação dos controles gerais de segurança da informação positivados nas normas do GSI/PR não é faculdade, mas obrigação da alta administração, e sua não implantação sem justificativa é passível da sanção prevista na Lei 8.443/1992, art. 58, II (subitem II.8);

9.8.3. reveja a Norma Complementar 4/IN01/DSIC/GSIPR, uma vez que aborda o tema gestão de riscos considerando apenas ativo de informação e não ativo em sentido amplo, como o faz a NBR ISO/IEC 27.002 no item 7.1.1 (subitem II.8).

9.9. Recomendar, com fundamento na Lei 8.443/1992, art. 43, inciso I, c/c RITCU, art. 250, inciso III, ao Comitê Gestor da Política Nacional de Desenvolvimento de Pessoal que, em atenção ao Decreto 5.707/2006, art. 7º, II e IV:

9.9.1. oriente os órgãos e entidades sob sua jurisdição sobre a obrigatoriedade de aprovar o plano anual de capacitação, nos termos do Decreto 5.707/2006, arts. 5º e 2º, c/c Portaria MP 208/2006, art. 2º, I, e art. 4º (subitem II.9);

9.9.2. estabeleça, após consulta à Secretaria de Logística e Tecnologia da Informação, um programa de capacitação em governança e em gestão de tecnologia da informação (subitem II.9).

9.10. Recomendar, com fundamento na Lei 8.443/1992, art. 43, inciso I, c/c RITCU, art. 250, inciso III, à Controladoria-Geral da União (CGU/PR) que:

9.10.1. considere os temas governança de TI, riscos de TI e controles de TI na seleção dos objetos a auditar, consoante o previsto nas boas práticas internacionais para que a atividade de auditoria interna seja mais efetiva (e.g., IPPF 2110.A2, 2120.A1 e 2130.A1; subitem II.11).

9.10.2. oriente as unidades de auditoria interna sob sua orientação normativa a considerar os temas governança de TI, riscos de TI e controles de TI na seleção dos objetos a auditar, consoante o previsto nas boas práticas internacionais para que a atividade de auditoria interna seja mais efetiva (e.g., IPPF 2110.A2, 2120.A1 e 2130.A1; subitem II.11).

9.11. recomendar, com fundamento na Lei 8.443/1992, art. 43, inciso I, c/c RITCU, art. 250, inciso III, à Comissão Interministerial de Governança Corporativa e de Administração de Participações Societárias da União (CGPAR) que:

9.11.1. normalize a obrigatoriedade de que os entes sob sua jurisdição estabeleçam comitês de TI, observando as boas práticas sobre o tema, a exemplo do Cobit 4.1, PO4.2 – comitê estratégico de TI e PO4.3 – comitê diretor de TI (subitem II.3);

9.11.2. oriente os órgãos e entidades sob sua jurisdição a realizar avaliação quantitativa e qualitativa do pessoal do setor de TI, de forma a delimitar as necessidades de recursos humanos necessárias para que estes setores realizem a gestão das atividades de TI da organização (subitem II.3);

9.11.3. discipline a forma de acesso às funções de liderança nos setores de Tecnologia da Informação, considerando as competências multidisciplinares necessárias para estas funções, que incluem, mas não se limitam a conhecimentos em TI (subitem II.3);

160 7

9.11.4. elabore um modelo de processo de software para os entes sob sua jurisdição, observando as boas práticas sobre o tema (e.g., NBR ISO/IEC 12.207 e 15.504, MPS.BR, CMMI; subitem II.5);

9.11.5. estabeleça a obrigatoriedade de que os entes sob sua jurisdição formalizem um processo de software para si, observando as boas práticas sobre o tema (e.g., NBR ISO/IEC 12.207 e 15.504, MPS.BR, CMMI; subitem II.5);

9.11.6. elabore um modelo de estrutura de gerenciamento de projetos para os entes sob sua jurisdição, observando as boas práticas sobre o tema (e.g., PMBoK; subitem II.6);

9.11.7. estabeleça a obrigatoriedade de que os entes sob sua jurisdição formalizem um processo de gerenciamento de projetos para si, observando as boas práticas sobre o tema (e.g., PMBoK; subitem II.6);

9.11.8. estabeleça a obrigatoriedade de que os entes sob sua jurisdição formalizem processos de gestão de serviços para si, incluindo, pelo menos, gestão de configuração, gestão de incidentes e gestão de mudança, observando as boas práticas sobre o tema (e.g., NBR ISO/IEC 20.000, Itil; subitem II.7);

9.11.9. estabeleça a obrigatoriedade de que as entidades sob sua jurisdição aprovem um plano anual de capacitação (subitem II.9);

9.11.10. estabeleça a obrigatoriedade de que as entidades sob sua jurisdição estabeleçam um processo formal para a contratação e gestão de soluções de tecnologia da informação (subitem II.10);

9.11.11. oriente as entidades sob sua jurisdição que o processo a ser formalizado em atenção ao item anterior deve ser elaborado a partir das diretrizes expostas no Acórdão 786/2006-TCU-Plenário, que também estão contidas no modelo implementado pela IN – SLTI/MP 4/2010 (subitem II.10);

9.11.12. em atenção ao Decreto-Lei 200/1967, art. 6º, V, estabeleça, normativamente para todos os entes sob sua jurisdição, a obrigatoriedade de a alta administração implantar uma estrutura de controles internos mediante a definição de atividades de controle em todos os níveis da organização para mitigar os riscos de suas atividades, pelo menos nos seguintes processos (subitem II.11):

9.11.12. 1. planejamento estratégico institucional;

9.11.12.2. planejamento estratégico de TI;

9.11.12.3. funcionamento dos comitês de TI;

9.11.12.4. processo orçamentário de TI;

9.11.12.5. processo de software;

9.11.12.6. gerenciamento de projetos;

9.11.12.7. gerenciamento de serviços de TI;

9.11.12.8. segurança da informação;

9.11.12.9. gestão de pessoal de TI;

9.11.12.10. contratação e gestão de soluções de TI;

9.11.12.11. monitoração do desempenho da TI organizacional.

9.12. Determinar, com fundamento na Lei 8.443/1992, art. 43, inciso I, c/c RITCU, art. 250, inciso II, à Comissão Interministerial de Governança Corporativa e de Administração de Participações Sociedades da União (CGPAR) que, em atenção ao previsto no Decreto 6.021/2007, art. 3º, I, b, oriente os entes sob sua jurisdição sobre necessidade de vincular seus contratos de serviços de desenvolvimento ou manutenção de software a um processo de software, pois, sem essa vinculação, o objeto do contrato não estará precisamente definido, em desconformidade com o disposto na Lei 8.666/1993, art. 6º, inciso IX (subitem II.5).

9.13. Recomendar, com fundamento na Lei 8.443/1992, art. 43, inciso I, c/c RITCU, art. 250, inciso III, ao Conselho Nacional da Justiça (CNJ) que:

9.13.1. oriente os órgãos e entidades sob sua jurisdição a realizar avaliação quantitativa e qualitativa do pessoal do setor de TI, de forma a delimitar as necessidades de recursos humanos necessárias para que estes setores realizem a gestão das atividades de TI da organização (subitem II.3);

9.13.2. discipline a forma de acesso às funções de liderança nos setores de Tecnologia da Informação, considerando as competências multidisciplinares necessárias para estas funções, que incluem, mas não se limitam a conhecimentos em TI (subitem II.3);

9.13.3. elabore um modelo de processo de software para os entes sob sua jurisdição, observando as boas práticas sobre o tema (e.g., NBR ISO/IEC 12.207 e 15.504, MPS.BR, CMMI; subitem II.5);

9.13.4. estabeleça a obrigatoriedade de que os entes sob sua jurisdição formalizem um processo de software para si, observando as boas práticas sobre o tema (e.g., NBR ISO/IEC 12.207 e 15.504, MPS.BR, CMMI; subitem II.5);

9.13.5. elabore um modelo de estrutura de gerenciamento de projetos para os entes sob sua jurisdição, observando as boas práticas sobre o tema (e.g., PMBoK; subitem II.6);

9.13.6. estabeleça a obrigatoriedade de que os entes sob sua jurisdição formalizem um processo de gerenciamento de projetos para si, observando as boas práticas sobre o tema (e.g., PMBoK; subitem II.6);

9.13.7. elabore um modelo de processo de gestão de serviços para os entes sob sua jurisdição que inclua, pelo menos, gestão de configuração, gestão de incidentes e gestão de mudança, observando as boas práticas sobre o tema (e.g., NBR ISO/IEC 20.000, Itil; subitem II.7);

9.13.8. estabeleça a obrigatoriedade de que os entes sob sua jurisdição formalizem processos de gestão de serviços para si, incluindo, pelo menos, gestão de configuração, gestão de incidentes e gestão de mudança, observando as boas práticas sobre o tema (e.g., NBR ISO/IEC 20.000, Itil; subitem II.7);

9.13.9. crie procedimentos para orientar os entes sob sua jurisdição na implementação dos seguintes controles (subitem II.8):

9.13.9.1. nomeação de responsável pela segurança da informação na organização, à semelhança das orientações contidas na NBR ISO/IEC 27.002, item 6.1.3 – Atribuição de responsabilidade para segurança da informação;

9.13.9.2. criação de comitê para coordenar os assuntos de segurança da informação, à semelhança das orientações contidas na NBR ISO/IEC 27.002, item 6.1.2 – Coordenação de segurança da informação;

9.13.9.3. processo de gestão de riscos de segurança da informação, à semelhança das orientações contidas na NBR ISO/IEC 27005 – Gestão de riscos de segurança da informação;

9.13.9.4. estabelecimento de política de segurança da informação, à semelhança das orientações contidas na NBR ISO/IEC 27.002, item 5.1 – Política de segurança da informação;

9.13.9.5. processo de elaboração de inventário de ativos, à semelhança das orientações contidas na NBR ISO/IEC 27.002, item 7.1 – Inventário de ativos;

9.13.9.6. processo de classificação da informação, à semelhança das orientações contidas na NBR ISO/IEC 27.002, item 7.2 – Classificação da informação, processo necessário segundo o Decreto 4.553/2002, art. 6º, § 2º, inciso II, e art. 67;

9.13.10. oriente os órgãos e entidades sob sua jurisdição sobre a obrigatoriedade de aprovar o plano anual de capacitação, nos termos da Resolução – CNJ 90/2009, art. 3º (subitem II.9);

9.13.11. estabeleça um programa de capacitação em governança e em gestão de tecnologia da informação (subitem II.9);

9.13.12. a partir das diretrizes expostas no Acórdão 786/2006-TCU-Plenário, elabore um modelo de processo para contratação e gestão de soluções de tecnologia da informação para o Poder Judiciário ou, alternativamente, adote o modelo contido na IN – SLTI/MP 4/2010 (subitem II.10);

9.13.13. promova a implementação do modelo elaborado em atenção ao item anterior nos órgãos e entidades sob sua jurisdição mediante orientação normativa (subitem II.10);

9.13.14. em atenção ao Decreto-Lei 200/1967, art. 6º, V, estabeleça, normativamente para todos os entes sob sua jurisdição, a obrigatoriedade de a alta administração implantar uma estrutura de controles internos mediante a definição de atividades de controle em todos os níveis da organização para mitigar os riscos de suas atividades, pelo menos nos seguintes processos (subitem II.11):

9.13.14.1. planejamento estratégico institucional;

9.13.14.2. planejamento estratégico de TI;

9.13.14.3. funcionamento dos comitês de TI;

9.13.14.4. processo orçamentário de TI;

9.13.14.5. processo de software;

9.13.14.6. gerenciamento de projetos;

9.13.14.7. gerenciamento de serviços de TI;

9.13.14.8. segurança da informação;

9.13.14.9. gestão de pessoal de TI;

9.13.14.10. contratação e gestão de soluções de TI;

9.13.14.11. monitoração do desempenho da TI organizacional;

9.13.15. oriente as unidades de auditoria interna sob sua orientação normativa a considerar os temas governança de TI, riscos de TI e controles de TI na seleção dos objetos a auditar, consoante o previsto nas boas práticas internacionais para que a atividade de auditoria interna seja mais efetiva (e.g., IPPF 2110.A2, 2120.A1 e 2130.A1; subitem II.11);

9.13.16. em atenção à Constituição Federal, art. 74, c/c o art. 103-B, § 4º, I, estabeleça sistema de controle interno integrado para todo o Poder Judiciário (subitem II.11).

9.14. determinar, com fundamento na Lei 8.443/1992, art. 43, inciso I, c/c RITCU, art. 250, inciso II, ao Conselho Nacional de Justiça (CNJ) que:

9.14.1. em atenção ao previsto na Constituição Federal, art. 103-B, § 4º, II, oriente os entes sob sua jurisdição sobre necessidade de vincular seus contratos de serviços de desenvolvimento ou manutenção de software a um processo de software, pois, sem esta vinculação, o objeto do contrato não estará precisamente definido, em desconformidade com o disposto na Lei 8.666/1993, art. 6º, inciso IX (subitem II.5);

9.14.2. em atenção ao previsto na Constituição Federal, art. 103-B, § 4º, II, oriente os órgãos e entidades sob sua jurisdição para que (subitem III.1):

9.14.2.1. ao realizarem licitação com finalidade de criar ata de registro de preços atentem que:

9.14.2.1.1. devem fundamentar formalmente a criação de ata de registro de preços, e.g., por um dos incisos do art. 2º do Decreto 3.931/2001 (Acórdão 2.401/2006-TCU-Plenário);

9.14.2.1.2. devem praticar todos os atos descritos no Decreto 3.931/2001, art. 3º, § 2º, em especial o previsto no seu inciso I, que consiste em “convidar mediante correspondência eletrônica ou outro meio eficaz, os órgãos e entidades para participarem do registro de preços”;

9.14.2.1.3. o planejamento da contratação é obrigatório, sendo obrigatória a realização dos devidos estudos técnicos preliminares (Lei 8.666/1993, art. 6º, inciso IX);

9.14.2.1.4. a fixação, no termo de convocação, de quantitativos (máximos) a serem contratados por meio dos contratos derivados da ata de registro de preços, previstos no Decreto 3.931/2001, art. 9º, inciso II, é obrigação e não faculdade do gestor (Acórdão 991/2009-TCU-Plenário, Acórdão 1.100/2007-TCU-Plenário e Acórdão 4.411/2010-TCU-2ª Câmara)

9.14.2.1.5. em atenção ao princípio da vinculação ao instrumento convocatório (Lei 8.666/1993, art. 3º, caput), devem gerenciar a ata de forma que a soma dos quantitativos contratados em todos os contratos derivados da ata não supere o quantitativo máximo previsto no edital;

9.14.3. quando realizarem adesão à ata de registro de preços atentem que:

9.14.3.1. o planejamento da contratação é obrigatório, sendo obrigatória a realização dos devidos estudos técnicos preliminares (Lei 8.666/1993, art. 6º, inciso IX);

9.14.3.2. devem demonstrar formalmente a vantajosidade da adesão, nos termos do Decreto 3.931/2001, art. 8º;

9.14.3.3. as regras e condições estabelecidas no certame que originou a ata de registro de preços devem ser conformes as necessidades e condições determinadas na etapa de planejamento da contratação (Lei 8.666/1993, art. 6º, inciso IX, alínea d, c/c o art. 3º, § 1º, inciso I, e Lei 10.520/2002, art. 3º, inciso II);

9.14.4. em atenção ao previsto na Constituição Federal, art. 103-B, § 4º, II, oriente os órgãos e entidades sob sua jurisdição para que, caso possuam contratos com empresas públicas prestadoras de serviços de TI (subitem III.3):

9.14.4.1. analisem a conformidade dos termos do contrato e do projeto básico e verifiquem se:

9.14.4.1.1. foi realizado o adequado planejamento da contratação, consistindo na execução do processo de planejamento previsto na IN – SLTI/MP 4/2010 se for integrante do Sisp (IN – SLTI/MP 4/2010, art. 18, inciso II) ou, caso não o seja, se foram realizados os devidos estudos técnicos preliminares (Lei 8.666/1993, art. 6º, inciso IX);

9.14.4.1.2. as especificações do objeto são precisas e suficientes, em conformidade com a Lei 8.666/1993, art. 6º, IX;

9.14.4.1.3. os critérios de mensuração dos serviços são precisos e suficientes, de acordo com o determinado na Lei 8.666/1993, art. 6º, IX, e (também necessários de acordo com a IN – SLTI 4/2010, art. 14, II, a);

9.14.4.1.4. a metodologia de avaliação da adequação dos produtos é precisa e suficiente, de acordo com o determinado na Lei 8.666/1993, art. 6º, IX, e (também necessária de acordo com a IN – SLTI 4/2010, art. 14, II, c);

9.14.4.1.5. as cláusulas de penalidades contidas na Lei 8.666/1993, art. 87, de acordo com o determinado na Lei 8.666/1993, art. 55, VII e VIII, são detalhadas e atendem aos princípios da razoabilidade, proporcionalidade e prudência (e também o previsto na IN – SLTI 4/2010, art. 15, III, h);

9.14.4.1.6. o modelo de pagamento é vinculado a resultados, obedecendo ao princípio constitucional da eficiência (e também ao previsto no Decreto 2.271/1997, art. 3º, § 1º, e na IN – SLTI 4/2010, art. 15, §§ 2º e 3º);

9.14.4.1.7. a justificativa dos preços contratados é adequadamente fundamentada em arrazoada pesquisa de mercado, de acordo com o determinado na Lei 8.666/1993, art. 26, III, inclusive com a análise da planilha de composição de custos dos serviços, necessária segundo a Lei 8.666/1993, art. 7º, § 2º, II;

9.14.4.2. caso a análise realizada de acordo com orientação acima indique desconformidade, elaborem plano de ação para providenciar as adequações contratuais necessárias, que deverão ser realizadas no prazo de 180 dias;

9.14.4.3. mantenham o resultado da análise de conformidade empreendida em documento formalizado, à disposição dos controles externo e interno;

9.14.4.4. informem seu órgão de assessoramento jurídico e sua unidade de auditoria interna da análise que está sendo empreendida e do resultado obtido;

9.14.5. em atenção ao previsto na Constituição Federal, art. 103-B, § 4º, II, oriente os órgãos e entidades sob sua jurisdição que (subitem III.3):

9.14.5.1. mesmo que a execução de seus serviços de tecnologia da informação seja transferida mediante contrato ou outro acordo a outra organização pública, como as empresas públicas prestadoras de serviços de tecnologia da informação, as atividades de gestão (planejamento, coordenação, supervisão e controle) de TI devem ser acometidas a pessoas integrantes do quadro permanente, ou, excepcionalmente, a detentores de cargo em comissão, da organização contratante, não podendo ser delegadas a pessoas direta ou indiretamente ligadas à contratada;

9.14.5.2. a contratação de empresas públicas prestadoras de serviços de tecnologia da informação não afasta a necessidade de a organização contratante manter estrutura de governança de TI própria, que direcione e controle a gestão desses contratos bem como a gestão de todos os processos de TI da organização;

9.15. recomendar, com fundamento na Lei 8.443/1992, art. 43, inciso I, c/c RITCU, art. 250, inciso III, ao Conselho Nacional do Ministério Públco (CNMP) que:

9.15.1. em atenção ao Decreto-Lei 200/1967, art. 6º, inciso I, e art. 7º, normatize a obrigatoriedade de que todos os entes sob sua jurisdição estabeleçam processo de planejamento

estratégico institucional, observando as boas práticas sobre o tema, a exemplo do critério de avaliação 2 do Gespública, contemplando, pelo menos (subitem II.1):

9.15.1.1. elaboração, com participação de representantes dos diversos setores da organização, de um documento que materialize o plano estratégico institucional de longo prazo, contemplando, pelo menos, objetivos, indicadores e metas para a organização;

9.15.1.2. aprovação, pela mais alta autoridade da organização, do plano estratégico institucional;

9.15.1.3. desdobramento do plano estratégico pelas unidades executoras;

9.15.1.4. divulgação do plano estratégico institucional para conhecimento dos cidadãos brasileiros, exceto nos aspectos formalmente declarados sigilosos ou restritos;

9.15.1.5. acompanhamento periódico do alcance das metas estabelecidas, para correção de desvios;

9.15.1.6. divulgação interna e externa do alcance das metas, ou dos motivos de não ter alcançado;

9.15.2. em atenção ao Decreto-Lei 200/1967, art. 6º, inciso I, e art. 7º, normatize a obrigatoriedade de que todos os entes sob sua jurisdição estabeleçam processo de planejamento estratégico de TI, observando as boas práticas sobre o tema, a exemplo do processo “PO1 – Planejamento Estratégico de TI” do Cobit 4.1, contemplando, pelo menos (subitem II.2):

9.15.2.1. elaboração, com participação de representantes dos diversos setores da organização, de um documento que materialize o plano estratégico de TI, contemplando, pelo menos:

9.15.2.1.1. objetivos, indicadores e metas para a TI organizacional, sendo que os objetivos devem estar explicitamente alinhados aos objetivos de negócio constantes do plano estratégico institucional;

9.15.2.1.2. alocação de recursos (financeiros, humanos, materiais etc);

9.15.2.1.3. estratégia de terceirização;

9.15.2.2. aprovação, pela mais alta autoridade da organização, do plano estratégico de TI;

9.15.2.3. desdobramento do plano estratégico de TI pelas unidades executoras;

9.15.2.4. divulgação do plano estratégico de TI para conhecimento dos cidadãos brasileiros, exceto nos aspectos formalmente declarados sigilosos ou restritos;

9.15.2.5. acompanhamento periódico do alcance das metas estabelecidas, para correção de desvios;

9.15.2.6. divulgação interna e externa do alcance das metas, ou os motivos de não ter alcançado;

9.15.3. normatize a obrigatoriedade de que os entes sob sua jurisdição estabeleçam comitês de TI, observando as boas práticas sobre o tema, a exemplo do Cobit 4.1, PO4.2 – comitê estratégico de TI e PO4.3 – comitê diretor de TI (subitem II.3);

9.15.4. oriente os órgãos e entidades sob sua jurisdição a realizarem avaliação quantitativa e qualitativa do pessoal do setor de TI, de forma a delimitar as necessidades de recursos humanos necessárias para que estes setores realizem a gestão das atividades de TI da organização (subitem II.3);

9.15.5. discipline a forma de acesso às funções de liderança nos setores de Tecnologia da Informação, considerando as competências multidisciplinares necessárias para estas funções, que incluem, mas não se limitam a conhecimentos em TI (subitem II.3);

9.15.6. elabore um modelo de processo de software para os entes sob sua jurisdição, observando as boas práticas sobre o tema (e.g., NBR ISO/IEC 12.207 e 15.504, MPS.BR, CMMI; subitem II.5);

9.15.7. estabeleça a obrigatoriedade de que os entes sob sua jurisdição formalizem um processo de software para si, observando as boas práticas sobre o tema (e.g., NBR ISO/IEC 12.207 e 15.504, MPS.BR, CMMI; subitem II.5);

9.15.8. elabore um modelo de estrutura de gerenciamento de projetos para os entes sob sua jurisdição, observando as boas práticas sobre o tema (e.g., PMBoK; subitem II.6);

9.15.9. estabeleça a obrigatoriedade de que os entes sob sua jurisdição formalizem um processo de gerenciamento de projetos para si, observando as boas práticas sobre o tema (e.g., PMBoK; subitem II.6);

9.15.10. elabore um modelo de processo de gestão de serviços para os entes sob sua jurisdição que inclua, pelo menos, gestão de configuração, gestão de incidentes e gestão de mudança, observando as boas práticas sobre o tema (e.g., NBR ISO/IEC 20.000, Itil; subitem II.7);

9.15.11. estabeleça a obrigatoriedade de que os entes sob sua jurisdição formalizem processos de gestão de serviços para si, incluindo, pelo menos, gestão de configuração, gestão de incidentes e gestão de mudança, observando as boas práticas sobre o tema (e.g., NBR ISO/IEC 20.000, Itil; subitem II.7);

9.15.12. estabeleça a obrigatoriedade de que os entes sob sua jurisdição implementem os seguintes controles gerais de TI relativos à segurança da informação (subitem II.8):

9.15.12.1. nomeação de responsável pela segurança da informação na organização, à semelhança das orientações contidas na NBR ISO/IEC 27.002, item 6.1.3 – Atribuição de responsabilidade para segurança da informação;

9.15.12.2. criação de comitê para coordenar os assuntos de segurança da informação, à semelhança das orientações contidas na NBR ISO/IEC 27.002, item 6.1.2 – Coordenação de segurança da informação;

9.15.12.3. processo de gestão de riscos de segurança da informação, à semelhança das orientações contidas na NBR ISO/IEC 27005 – Gestão de riscos de segurança da informação;

9.15.12.4. estabelecimento de política de segurança da informação, à semelhança das orientações contidas na NBR ISO/IEC 27.002, item 5.1 – Política de segurança da informação;

9.15.12.5. processo de elaboração de inventário de ativos, à semelhança das orientações contidas na NBR ISO/IEC 27.002, item 7.1 – Inventário de ativos;

9.15.12.6. processo de classificação da informação, à semelhança das orientações contidas na NBR ISO/IEC 27.002, item 7.2 – Classificação da informação, processo necessário segundo o Decreto 4.553/2002, art. 6º, § 2º, inciso II e art. 67;

9.15.13. crie procedimentos para orientar os entes sob sua jurisdição na implementação dos controles listados no item acima (subitem II.8);

9.15.14. estabeleça a obrigatoriedade de que os órgãos e entidades sob sua jurisdição aprovem um plano anual de capacitação (subitem II.9);

9.15.15. estabeleça um programa de capacitação em governança e em gestão de tecnologia da informação (subitem II.9);

9.15.16. a partir das diretrizes expostas no Acórdão 786/2006-TCU-Plenário, elabore um modelo de processo para contratação e gestão de soluções de tecnologia da informação para o Ministério Público ou, alternativamente, adote o modelo contido na IN – SLTI/MP 4/2010 (subitem II.10);

9.15.17. promova a implementação do modelo elaborado em atenção ao item anterior nos órgãos e entidades sob sua jurisdição mediante orientação normativa (subitem II.10);

9.15.18. em atenção ao Decreto-Lei 200/1967, art. 6º, V, estabeleça, normativamente para todos os entes sob sua jurisdição, a obrigatoriedade de a alta administração implantar uma estrutura de controles internos mediante a definição de atividades de controle em todos os níveis da organização para mitigar os riscos de suas atividades, pelo menos, nos seguintes processos (subitem II.11):

9.15.18.1. planejamento estratégico institucional/institucional;

9.15.18.2. planejamento estratégico de TI;

9.15.18.3. funcionamento dos comitês de TI;

9.15.18.4. processo orçamentário de TI;

9.15.18.5. processo de software;

9.15.18.6. gerenciamento de projetos;

9.15.18.7. gerenciamento de serviços de TI;

9.15.18.8. segurança da informação;

9.15.18.9. gestão de pessoal de TI;

9.15.18. 10. contratação e gestão de soluções de TI;

9.15.18.11. monitoração do desempenho da TI organizacional.

9.15.19. oriente as unidades de auditoria interna sob sua orientação normativa a considerar os temas governança de TI, riscos de TI e controles de TI na seleção dos objetos a auditar, consoante o previsto nas boas práticas internacionais para que a atividade de auditoria interna seja mais efetiva (e.g., IPPF 2110.A2, 2120.A1 e 2130.A1; subitem II.11);

9.15.20. em atenção à Constituição Federal, art. 74, c/c o art. 103-B, § 4º, I, estabeleça sistema de controle interno integrado para todo o Ministério Público (subitem II.11).

9.16. determinar, com fundamento na Lei 8.443/1992, art. 43, inciso I, c/c RITCU, art. 250, inciso II, ao Conselho Nacional do Ministério Público (CNMP) que:

9.16.1. em atenção ao previsto na Constituição Federal, art. 130-A, § 2º, II, oriente os entes sob sua jurisdição sobre necessidade de vincular seus contratos de serviços de desenvolvimento ou manutenção de software a um processo de software, pois, sem esta vinculação, o objeto do contrato não estará precisamente definido, em desconformidade com o disposto na Lei 8.666/1993, art. 6º, inciso IX (subitem II.5);

9.16.2. em atenção ao previsto na Constituição Federal, art. 130-A, § 2º, II, oriente os órgãos e entidades sob sua jurisdição para que (subitem III.1):

9.16.2.1. ao realizarem licitação com finalidade de criar ata de registro de preços atentem que:

9.16.2.1.1 devem fundamentar formalmente a criação de ata de registro de preços, e.g., por um dos incisos do art. 2º do Decreto 3.931/2001 (Acórdão 2.401/2006-TCU-Plenário);

9.16.2.1.2. devem praticar todos os atos descritos no Decreto 3.931/2001, art. 3º, § 2º, em especial o previsto no seu inciso I, que consiste em “convidar mediante correspondência eletrônica ou outro meio eficaz, os órgãos e entidades para participarem do registro de preços”;

9.16.2.1.3. o planejamento da contratação é obrigatório, sendo obrigatória a realização dos devidos estudos técnicos preliminares (Lei 8.666/1993, art. 6º, inciso IX);

9.16.2.1.4. a fixação, no termo de convocação, de quantitativos (máximos) a serem contratados por meio dos contratos derivados da ata de registro de preços, previstos no Decreto 3.931/2001, art. 9º, inciso II, é obrigação e não faculdade do gestor (Acórdão 991/2009-TCU-Plenário, Acórdão 1.100/2007-TCU-Plenário e Acórdão 4.411/2010-TCU-2ª Câmara);

9.16.2.1.5. em atenção ao princípio da vinculação ao instrumento convocatório (Lei 8.666/1993, art. 3º, caput), devem gerenciar a ata de forma que a soma dos quantitativos contratados em todos os contratos derivados da ata não supere o quantitativo máximo previsto no edital;

9.16.2.2. quando realizarem adesão à ata de registro de preços atentem que:

9.16.2.2.1. o planejamento da contratação é obrigatório, sendo obrigatória a realização dos devidos estudos técnicos preliminares (Lei 8.666/1993, art. 6º, inciso IX);

9.16.2.2.2. devem demonstrar formalmente a vantajosidade da adesão, nos termos do Decreto 3.931/2001, art. 8º;

9.16.2.2.3. as regras e condições estabelecidas no certame que originou a ata de registro de preços devem ser conformes as necessidades e condições determinadas na etapa de planejamento da contratação (Lei 8.666/1993, art. 6º, inciso IX, alínea d, c/c o art. 3º, § 1º, inciso I, e Lei 10.520/2002, art. 3º, inciso II);

9.16.3. em atenção ao previsto na Constituição Federal, art. 130-A, § 2º, II, oriente os órgãos e entidades sob sua jurisdição para que, caso possuam contratos com empresas públicas prestadoras de serviços de TI (subitem III.3):

9.16.3.1. analisem a conformidade dos termos do contrato e do projeto básico e verifiquem se:

9.16.3.1.1. foi realizado o adequado planejamento da contratação, consistindo na execução do processo de planejamento previsto na IN – SLTI/MP 4/2010 se for integrante do Sisp (IN – SLTI/MP 4/2010, art. 18, inciso II) ou, caso não o seja, se foram realizados os devidos estudos técnicos preliminares (Lei 8.666/1993, art. 6º, inciso IX);

9.16.3.1.2. as especificações do objeto são precisas e suficientes, em conformidade com a Lei 8.666/1993, art. 6º, IX;

9.16.3.1.3. os critérios de mensuração dos serviços são precisos e suficientes, de acordo com o determinado na Lei 8.666/1993, art. 6º, IX, e (também necessários de acordo com a IN – SLTI 4/2010, art. 14, II, a);

9.16.3.1.4. a metodologia de avaliação da adequação dos produtos é precisa e suficiente, de acordo com o determinado na Lei 8.666/1993, art. 6º, IX, e (também necessária de acordo com a IN – SLTI 4/2010, art. 14, II, c);

9.16.3.1.5. as cláusulas de penalidades contidas na Lei 8.666/1993, art. 87, de acordo com o determinado na Lei 8.666/1993, art. 55, VII e VIII, são detalhadas e atendem aos princípios da razoabilidade, proporcionalidade e prudência (e também o previsto na IN – SLTI 4/2010, art. 15, III, h);

9.16.3.1.6. o modelo de pagamento é vinculado a resultados, obedecendo ao princípio constitucional da eficiência (e também ao previsto no Decreto 2.271/1997, art. 3º, § 1º, e na IN – SLTI 4/2010, art. 15, §§ 2º e 3º);

9.16.3.1.7. a justificativa dos preços contratados é adequadamente fundamentada em arrazoada pesquisa de mercado, de acordo com o determinado na Lei 8.666/1993, art. 26, III, inclusive com a análise da planilha de composição de custos dos serviços, necessária segundo a Lei 8.666/1993, art. 7º, § 2º, II;

9.16.3.2. caso a análise realizada de acordo com orientação acima indique desconformidade, elaborem plano de ação para providenciar as adequações contratuais necessárias, que deverão ser realizadas no prazo de 180 dias;

9.16.3.3. mantenham o resultado da análise de conformidade empreendida em documento formalizado, à disposição dos controles externo e interno;

9.16.3.4. informem seu órgão de assessoramento jurídico e sua unidade de auditoria interna da análise que está sendo empreendida e do resultado obtido;

9.16.4. em atenção ao previsto na Constituição Federal, art. 130-A, § 2º, II, oriente os órgãos e entidades sob sua jurisdição que (subitem III.3):

9.16.4.1. mesmo que a execução de seus serviços de tecnologia da informação seja transferida mediante contrato ou outro acordo a outra organização pública, como as empresas públicas prestadoras de serviços de tecnologia da informação, as atividades de gestão (planejamento, coordenação, supervisão e controle) de TI devem ser acometidas a pessoas integrantes do quadro permanente, ou, excepcionalmente, a detentores de cargo em comissão, da organização contratante, não podendo ser delegadas a pessoas direta ou indiretamente ligadas à contratada;

9.16.4.2. a contratação de empresas públicas prestadoras de serviços de tecnologia da informação não afasta a necessidade de a organização contratante manter estrutura de governança de TI própria, que direcione e controle a gestão desses contratos bem como a gestão de todos os processos de TI da organização;

9.17. recomendar, com fundamento na Lei 8.443/1992, art. 43, inciso I, c/c RITCU, art. 250, inciso III, ao Tribunal de Contas da União que avalie as orientações contidas no presente acórdão e adote as medidas necessárias a sua implementação;

9.18. recomendar, com fundamento na Lei 8.443/1992, art. 43, inciso I, c/c RITCU, art. 250, inciso III, à Câmara dos Deputados que avalie as orientações contidas no presente acórdão, e adote as medidas necessárias a sua implementação;

9.19. recomendar, com fundamento na Lei 8.443/1992, art. 43, inciso I, c/c RITCU, art. 250, inciso III, ao Senado Federal que avalie as orientações contidas no presente acórdão e adote as medidas necessárias a sua implementação;

9.20. dar ciência à Casa Civil da Presidência da República de que o secretário-executivo não submeteu ao Ministro de Estado o Plano de Ação Global da pasta, o que afronta o Decreto 5.135/2004, art. 23, inciso I;

9.21. dar ciência ao Ministério da Agricultura, Pecuária e Abastecimento de que o secretário-executivo não submeteu ao Ministro de Estado o Plano de Ação Global da pasta, o que afronta o Decreto 7.127/2010, art. 41, inciso I;

9.22. dar ciência ao Ministério da Ciência e Tecnologia de que o secretário-executivo não submeteu ao Ministro de Estado o Plano de Ação Global da pasta, o que afronta o Decreto 5.886/2006, art. 38, inciso I;

9.23. dar ciência ao Ministério da Educação de que o secretário-executivo não submeteu ao Ministro de Estado o Plano de Ação Global da pasta, o que afronta o Decreto 7.480/2011, art. 38, inciso I.

9.24. dar ciência ao Ministério da Fazenda de que o secretário-executivo não submeteu ao Ministro de Estado o Plano de Ação Global da pasta, o que afronta o Decreto 7.482/2011, art. 43, inciso I;

9.25. dar ciência ao Ministério da Integração Nacional de que o secretário-executivo não submeteu ao Ministro de Estado o Plano de Ação Global da pasta, o que afronta o Decreto 7.472/2011, art. 29, inciso IV;

9.26. dar ciência ao Ministério da Justiça de que o secretário-executivo não submeteu ao Ministro de Estado o Plano de Ação Global da pasta, o que afronta o Decreto 6.061/2007, art. 43, inciso I;

9.27. dar ciência ao Ministério da Saúde de que o secretário-executivo não submeteu ao Ministro de Estado o Plano de Ação Global da pasta, o que afronta o Decreto 7.530/2011, art. 49, inciso I;

9.28. dar ciência ao Ministério das Cidades de que o secretário-executivo não submeteu ao Ministro de Estado o Plano de Ação Global da pasta, o que afronta o Decreto 4.665/2003, art. 26, inciso I;

9.29. dar ciência ao Ministério das Minas e Energia de que o secretário-executivo não submeteu ao Ministro de Estado o Plano de Ação Global da pasta, o que afronta o Decreto 5.267/2004, art. 27, inciso I;

9.30. dar ciência ao Ministério do Desenvolvimento Agrário de que o secretário-executivo não submeteu ao Ministro de Estado o Plano de Ação Global da pasta, o que afronta o Decreto 7.255/2010, art. 22, inciso I;

9.31. dar ciência ao Ministério do Desenvolvimento Social e Combate à Fome de que o secretário-executivo não submeteu ao Ministro de Estado o Plano de Ação Global da pasta, o que afronta o Decreto 7.493/2011, art. 36, inciso I;

9.32. dar ciência ao Ministério do Desenvolvimento, Indústria e Comércio Exterior de que o secretário-executivo não submeteu ao Ministro de Estado o Plano de Ação Global da pasta, o que afronta o Decreto 7.096/2010, art. 30, inciso I;

9.33. dar ciência ao Ministério do Esporte de que o secretário-executivo não submeteu ao Ministro de Estado o Plano de Ação Global da pasta, o que afronta o Decreto 7.529/2011, art. 20, inciso I;

9.34. dar ciência ao Ministério do Meio Ambiente de que o secretário-executivo não submeteu ao Ministro de Estado o Plano de Ação Global da pasta, o que afronta o Decreto 6.101/2007, art. 43, inciso I;

9.35. dar ciência ao Ministério do Planejamento, Orçamento e Gestão de que o secretário-executivo não submeteu ao Ministro de Estado o Plano de Ação Global da pasta, o que afronta o Decreto 7.063/2010, art. 49, inciso I;

9.36. dar ciência ao Ministério do Trabalho e Emprego de que o secretário-executivo não submeteu ao Ministro de Estado o Plano de Ação Global da pasta, o que afronta o Decreto 5.063/2004, art. 27, inciso I;

9.37. dar ciência ao Ministério do Turismo de que o secretário-executivo não submeteu ao Ministro de Estado o Plano de Ação Global da pasta, o que afronta o Decreto 6.546/2008, art. 20, inciso I;

9.38. dar ciência ao Ministério dos Transportes de que o secretário-executivo não submeteu ao Ministro de Estado o Plano de Ação Global da pasta, o que afronta o Decreto 4.721/2003, art. 19, inciso I;

9.39. dar ciência à Secretaria de Assuntos Estratégicos da Presidência da República de que o secretário-executivo não submeteu ao Ministro de Estado o Plano de Ação Global da pasta, o que afronta o Decreto 6.517/2008, art. 7º, inciso I;

9.40. dar ciência à Secretaria de Relações Institucionais da Presidência da República de que o secretário-executivo não submeteu ao Ministro de Estado o Plano de Ação Global da pasta, o que afronta o Decreto 6.207/2007, art. 9º, inciso I.

9.41. dar ciência à Secretaria-Geral da Presidência da República de que o secretário-executivo não submeteu ao Ministro de Estado o Plano de Ação Global da pasta, o que afronta o Decreto 6.378/2008, art. 11, inciso I;

9.42. dar ciência à Secretaria de Aviação Civil da Presidência da República de que o secretário-executivo não submeteu ao Ministro de Estado o Plano de Ação Global da pasta, o que afronta o Decreto 7.476/2011, art. 18, inciso I;

9.43. recomendar à Secretaria-Geral de Controle Externo (Segecex) que avalie a oportunidade e conveniência de incluir em futuros planos de fiscalização do TCU Tema de Maior Significância (TMS) com objetivo de avaliar a eficiência e eficácia dos sistemas de controles internos dos poderes da União, em especial como as unidades de auditoria interna atuam na avaliação da eficácia dos processos de gerenciamento de riscos, controle e governança dos órgãos e entidades da Administração Pública Federal, levando em consideração, inclusive, as boas práticas internacionais sobre o tema como o IPPF (International Professional Practices Framework) do Instituto de Auditores Internos;

9.44. determinar à Secretaria de Fiscalização de Tecnologia da Informação do TCU (Sefti/TCU) que:

] 9.44.1. promova a divulgação dos critérios de auditoria contidos no Apêndice VIII.4, a fim de continuar a atividade de orientação que vem desenvolvendo (subitem I.4);

9.44.2. dê publicidade, inclusive por meio do sítio do TCU na internet, às informações acerca de governança de tecnologia da informação que foram solicitadas aos gestores nesta fiscalização (subitem I.6.2);

9.44.3. monitore as deliberações do Acórdão 2.308/2010-TCU-Plenário em conjunto com as proferidas nestes autos (subitem II.11);

9.44.4. divulgue o conteúdo das seis notas técnicas existentes, como forma de informar e orientar a APF e a sociedade sobre a existência do conjunto de normas que regem as aquisições de bens e serviços de tecnologia da informação, bem como sobre a jurisprudência deste Tribunal quanto ao assunto, promovendo, inclusive, a realização de seminários, cursos e palestras, caso entenda conveniente (subitem III.2);

9.44.5. encaminhe o estudo elaborado pelo TCU intitulado “Critérios gerais de controle interno na administração pública” à (item IV):

9.44.5.1. Câmara de Políticas de Gestão, Desempenho e Competitividade do Conselho de Governo, com objetivo de subsidiar possível elaboração de normativo para o poder executivo, com fundamento no Decreto 7.478/2011, art. 2º, II, tratando de gestão de riscos, do controle interno e da governança corporativa;

9.44.5.2. Conselho Nacional de Justiça, com objetivo de subsidiar possível elaboração de normativo para o poder judiciário, com fundamento na Constituição Federal, art. 103-B, § 4º, II, tratando de gestão de riscos, do controle interno e da governança corporativa;

9.44.5.3. Conselho Nacional do Ministério Público, com objetivo de subsidiar possível elaboração de normativo para o ministério público, com fundamento na Constituição Federal, art. 130-A, § 2º, II, tratando de gestão de riscos, do controle interno e da governança corporativa;

9.44.5.4. Comissão de Finanças e Tributação da Câmara dos Deputados, com objetivo subsidiar possível anteprojeto de proposta legislativa para alteração da Lei de Responsabilidade Fiscal;

9.44.5.5. Comissão de Assuntos Econômicos do Senado Federal, com objetivo subsidiar possível anteprojeto de proposta legislativa para alteração da Lei de Responsabilidade Fiscal;

9.44.5.6. promova a divulgação, inclusive por meio de eventos, das recomendações e determinações dirigidas aos órgãos governantes superiores por meio do presente acórdão, como forma de mitigar os riscos da sua implementação;

9.44.5.7. encaminhe cópia deste Acórdão, bem como do relatório e voto que o fundamentam, assim como da íntegra deste relatório, à(ao)(s):

- 9.44.5.7.1. entes a que foram dirigidas as determinações e recomendações da deliberação;
- 9.44.5.7.2. Serviço Federal de Processamento de Dados (Serpro);
- 9.44.5.7.3. Comissão de Ciência e Tecnologia, Comunicação e Informática (CCTCI) da Câmara dos Deputados;
- 9.44.5.7.4. Subcomissão Permanente de Ciência e Tecnologia e Informática da Comissão de Ciência e Tecnologia, Comunicação e Informática (CCTCI) da Câmara dos Deputados;
- 9.44.5.7.5. Comissão de Ciência, Tecnologia, Inovação, Comunicação e Informática (CCT) do Senado Federal;
- 9.44.5.7.6. Subcomissão Permanente de Serviços de Informática (CCTSINF) da Comissão de Ciência, Tecnologia, Inovação, Comunicação e Informática (CCT) do Senado Federal;
- 9.44.5.7.7. Tribunais de Contas dos Estados e dos Municípios, para que adotem as medidas que entenderem pertinentes;
- 9.45. arquivar os presentes autos na Secretaria de Fiscalização de Tecnologia da Informação.

10. Ata nº 19/2012 – Plenário.

11. Data da Sessão: 23/5/2012 – Ordinária.

12. Código eletrônico para localização na página do TCU na Internet: AC-1233-19/12-P.

13. Especificação do quorum:

13.1. Ministros presentes: Benjamin Zymler (Presidente), Valmir Campelo, Walton Alencar Rodrigues, Aroldo Cedraz (Relator), Raimundo Carreiro, José Jorge, José Múcio Monteiro e Ana Arraes.

13.2. Ministro-Substituto convocado: Marcos Bemquerer Costa.

13.3. Ministros-Substitutos presentes: André Luís de Carvalho e Weder de Oliveira.

(Assinado Eletronicamente)  
BENJAMIN ZYMLER  
Presidente

(Assinado Eletronicamente)  
AROLDO CEDRAZ  
Relator

Fui presente:

(Assinado Eletronicamente)  
LUCAS ROCHA FURTADO  
Procurador-Geral

GRUPO I – CLASSE VII – Plenário.

TC 011.772/2010-7

Natureza: Relatório de Auditoria

Interessado: Tribunal de Contas da União.

Unidade: Secretaria de Fiscalização de Tecnologia da Informação  
(Sefiti)

Advogado constituído nos autos: não há.

**Sumário:** TMS 6/20010. GESTÃO E USO DE TECNOLOGIA DA INFORMAÇÃO (TI). RELATÓRIO CONSOLIDADO. 21 TRABALHOS, ABRANGENDO 315 ORGANIZAÇÕES PÚBLICAS FEDERAIS. CONSIDERAÇÕES A RESPEITO DAS CONTRATAÇÕES DE SOLUÇÕES DE TI PELO SISTEMA DE REGISTRO DE PREÇOS (SRP). CONSIDERAÇÕES SOBRE O TEMA “GOVERNANÇA CORPORATIVA E GOVERNANÇA DE TI”. RECOMENDAÇÕES E DETERMINAÇÕES.

## RELATÓRIO

Trata-se de relatório consolidado das ações do TMS 6/2010, cujo objeto foi avaliar se a gestão e o uso da tecnologia da informação estão de acordo com a legislação e aderentes às boas práticas de governança de TI.

2. O objetivo maior dessa fase do trabalho consiste em agregar os resultados de todas as fiscalizações previstas, de modo a sintetizar os achados e conclusões sobre a gestão e uso de TI na Administração Pública Federal (APF).

3. Passo a transcrever, a seguir, o relatório de consolidação das informações obtidas nessas Auditorias, nos moldes apresentados pela equipe coordenadora da Secretaria de Fiscalização de Tecnologia da Informação (Sefit):

### “[...] INTRODUÇÃO

#### Origem do TMS

Por meio de Comunicação da Presidência do TCU de caráter reservado na sessão de 31/3/2010, foi apresentado o plano de fiscalização para 2010/2011, quando foi então aprovado o Tema de Maior Significância (TMS) 6 – Gestão e uso de TI (Tecnologia da Informação), para ser conduzido sob coordenação da Sefiti.

Posteriormente, por meio de diversos despachos do relator, Ministro Aroldo Cedraz (TC 009.329/2010-2), foram autorizadas as 21 fiscalizações que compuseram este TMS.

#### Visão geral

##### Por que TI é importante na APF?

O levantamento de auditoria que resultou no Acórdão 2.308/2010-TCU-Plenário, um dos trabalhos integrantes do presente TMS, solicitou que os entes pesquisados elencassem os sistemas de informação de maior relevância no suporte para cada uma das suas três principais ações finalísticas, solicitando ainda que a informação contemplasse o nível de criticidade do sistema para a consecução da ação (pergunta 5.1, fl. 26, anexo 2).

Os dados apresentados no Quadro 1 (incluindo todas as respostas enviadas no levantamento supra, inclusive as que chegaram após a prolação do acórdão) registram que 74% dos pesquisados declararam que seu negócio é afetado se os seus sistemas de informação pararem de funcionar de forma adequada.

Quadro 1 – Maturidade de governança de TI e existência de sistemas críticos

Criticidade (Se o sistema parar, o negócio...)	Maturidade inicial	Maturidade intermediária	Maturidade aprimorada	Total
... para imediatamente.	82	63	9	154   51%

... para em uma semana.	12	6	3	21	7%
... para em um mês.	5	1	—	6	2%
... é afetado, mas não para.	27	13	3	43	14%
... não é afetado.	50	26	1	77	26%
Total	176	179	16	301	100%

Quando analisamos os dados da previsão orçamentária dos 77 pesquisados que informaram que seu negócio não é afetado pela parada dos seus sistemas de informação (apêndice 0), observamos que 38 deles possuem previsão de gastos em TI acima de R\$ 1 milhão, sugerindo a possibilidade de erro na avaliação empreendida por alguns gestores e a dependência dos sistemas de informação na quase totalidade das organizações da APF pesquisadas.

Esses dados evidenciam a importância da TI na condução das políticas públicas do Governo Federal.

#### Antecedentes da fiscalização

Os seguintes antecedentes fundamentam a estratégia que foi proposta para a condução do TMS 6 – Gestão e uso de TI:

por meio de levantamento em 255 entes da APF realizado no ano de 2007, o relator do processo no TCU registrou que ‘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’ (voto do Acórdão 1.603/2008-TCU-Plenário);

por meio de auditoria integrada, com foco em controles da governança de TI e testes substantivos em processos de contratação de serviços de TI, o TCU identificou inúmeras falhas, algumas delas consideradas graves pelo Relator (relatório e item 10 do voto do Acórdão 2.471/2008-TCU-Plenário);

o Acórdão 2.471/2008-TCU-Plenário expediu diversas medidas que ‘podem contribuir para reduzir de forma significativa as falhas acima relacionadas e para aperfeiçoar a gestão pública’ (item 11 do voto do Acórdão 2.471/2008-TCU-Plenário). No mesmo sentido, o Acórdão 1.603/2008- TCU-Plenário também expediu diversas recomendações estruturantes sobre o tema governança de TI;

por diversas vezes, esta Corte se deparou com constatações graves decorrentes, dentre outros, da falta de implantação de uma estrutura adequada nos entes públicos para lidar com aspectos da governança de TI, em especial na área de segurança da informação. Citamos como exemplos os indícios de fraude no módulo de consignações do sistema Siape (Acórdão 1.505/2007-TCU-Plenário), as falhas de segurança da informação no sistema Infoseg (Acórdão 71/2008-TCU-Plenário), os indícios de fraude na concessão de benefícios gerenciados pelo Cadastro Único (Acórdão 906/2009-TCU-Plenário) e as falhas nos controles e indícios de fraude no sistema do Cadastro Integrado da Dívida Ativa da União – Cida (Acórdão 3.382/2010-TCU-Plenário);

havia determinação, contida no item 9.9 do Acórdão 1.603/2008-TCU-Plenário, para que a Sefti desse continuidade aos trabalhos de acompanhamento da governança de TI, nos seguintes termos:

‘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;’

#### Órgãos Governantes Superiores (OGS)

Conforme descrito no voto condutor do Acórdão 1.145/2011-TCU-Plenário, os OGS são aqueles que ‘têm a responsabilidade por normatizar e fiscalizar o uso e a gestão de TI em seus respectivos segmentos da Administração Pública Federal’. Assim, os OGS serão os destinatários das orientações propostas neste trabalho.

Do relatório daquele decisum, extraímos onze OGS:

Conselho Nacional de Justiça (CNJ);

Conselho Nacional do Ministério Público (CNMP);

Advocacia-Geral da União (AGU/PR);

Controladoria-Geral da União (CGU/PR);

Gabinete de Segurança Institucional (GSI/PR);  
Ministério do Planejamento, Orçamento e Gestão (MP);  
Secretaria de Logística e Tecnologia da Informação (SLTI/MP);  
Secretaria do Orçamento Federal (SOF/MP);  
Departamento de Coordenação e Governança das Estatais (Dest/MP);  
Fundação Escola Nacional de Administração Pública (Enap/MP);  
Secretaria do Tesouro Nacional (STN/MF).

Para os fins deste trabalho, identificamos ainda outros três OGS de interesse:  
Câmara de Políticas de Gestão, Desempenho e Competitividade (CGDC) do Conselho de Governo;

Comitê Gestor da Política Nacional de Desenvolvimento de Pessoal;  
Comissão Interministerial de Governança Corporativa e de Administração de Participações Societárias da União (CGPAR).

A CGDC é OGS de interesse devido ao seguinte dispositivo do Decreto 7.478/2011 (sublinhou-se):

Art. 2º Compete à CGDC:

(...)

II – estabelecer diretrizes estratégicas e planos para formulação e implementação de políticas de melhoria da gestão da administração pública federal;

O Comitê Gestor da Política Nacional de Desenvolvimento de Pessoal é OGS de interesse devido ao seguinte dispositivo do Decreto 5.707/2006:

Art. 7º Fica criado o Comitê Gestor da Política Nacional de Desenvolvimento de Pessoal, com as seguintes competências:

I – avaliar os relatórios anuais dos órgãos e entidades, verificando se foram observadas as diretrizes da Política Nacional de Desenvolvimento de Pessoal;

II – orientar os órgãos e entidades da administração pública federal direta, autárquica e fundacional na definição sobre a alocação de recursos para fins de capacitação de seus servidores;

III – promover a disseminação da Política Nacional de Desenvolvimento de Pessoal entre os dirigentes dos órgãos e das entidades, os titulares das unidades de recursos humanos, os responsáveis pela capacitação, os servidores públicos federais e suas entidades representativas; e

IV – zelar pela observância do disposto neste Decreto.

A CGPAR é OGS de interesse devido ao seguinte dispositivo do Decreto 6.021/2007 (sublinhou-se):

Art. 3º Compete à CGPAR:

(...)

I – aprovar diretrizes e estratégias relacionadas à participação acionária da União nas empresas estatais federais, com vistas à:

(...)

b) promoção da eficiência na gestão, inclusive quanto à adoção das melhores práticas de governança corporativa;

O apêndice 0 contém os normativos que estabelecem os mandatos dos OGS.

Controle interno e auditoria interna

Dentre os trabalhos realizados na condução deste TMS, citam-se catorze auditorias para avaliação de controles gerais de TI (ver item 0 adiante). Considerando que, nas reuniões de encerramento dessas auditorias, por vezes não restava cristalina aos gestores a diferença entre controle interno e auditoria interna, entende-se oportuno trazer à baila as definições a seguir, constantes da IN – TCU 63/2010:

Art. 1º (...)

X. controles internos: conjunto de atividades, planos, métodos, indicadores e procedimentos interligados, utilizado com vistas a assegurar a conformidade dos atos de gestão e a concorrer para que os objetivos e metas estabelecidos para as unidades jurisdicionadas sejam alcançados;

XI. órgãos de controle interno: unidades administrativas, integrantes dos sistemas de controle interno da administração pública federal, incumbidas, entre outras funções, da verificação da consistência e qualidade dos controles internos, bem como do apoio às atividades de controle externo exercidas pelo Tribunal.

A título de complemento, transcrevem-se ainda dois excertos das normas contidas na Estrutura Internacional de Práticas Profissionais (International Professional Practices Framework – IPPF), marco de referência do Instituto de Auditores Internos (The Institute of Internal Auditors – IIA), que contêm orientações para que a atividade de auditoria interna (AI) seja efetiva:

**Definição de Auditoria Interna:** A auditoria interna é uma atividade independente e objetiva que presta serviços de avaliação e de consultoria com o objetivo de adicionar valor e melhorar as operações de uma organização. A auditoria auxilia a organização a alcançar seus objetivos através de uma abordagem sistemática e disciplinada para a avaliação e melhoria da eficácia dos processos de gerenciamento de risco, controle e governança corporativa.

(...)

**IPPF 2120-1:** O gestor e a alta administração são responsáveis pelos processos de gestão de risco e controles da organização.

Pelos excertos transcritos, observa-se que a atividade de controle interno tem por objetivo mitigar os riscos de que a organização não alcance seus objetivos e a responsabilidade pela sua implantação (ou não) é inerente ao gestor responsável pelo processo que recebe o controle.

Por sua vez, a auditoria interna é uma atividade, exercida de forma independente da gestão, que tem como um dos objetivos a avaliação dos controles internos.

**Critérios de auditoria e evolução normativa**

Em 2007, ao conduzir TMS para avaliar a governança de TI (Acórdão 2.471/2008-TCU-Plenário), o TCU praticamente só dispunha de critérios relacionados às boas práticas, como o Cobit (framework da governança de TI) e a NBR 17.799:2005 (atualmente NBR 27.002:2005 – norma de boas práticas em segurança da informação).

Os trabalhos realizados naquele ano deram origem aos Acórdãos 1.603/2008 e 2.471/2008, ambos do Plenário do TCU, que induziram a positivação de diversos critérios de auditoria para a governança de TI no ordenamento jurídico brasileiro.

Tais normas foram então utilizadas como critérios neste TMS, sendo que os resultados sugerem que diversas dessas normas ainda não são de conhecimento dos gestores, em especial as relacionadas à segurança da informação.

Assim, foi composto um quadro sintético com os critérios utilizados em cada tema auditado, e propõe-se determinar à Sefti que promova a divulgação dos critérios de auditoria contidos no Apêndice 0, a fim de continuar a atividade de orientação que vem desenvolvendo (subitem 0).

**Objetivos e questões de auditoria**

**Objetivos**

O objetivo geral da fiscalização foi avaliar se a gestão e o uso da tecnologia da informação estão de acordo com a legislação e aderentes às boas práticas da governança de TI.

Constituem-se objetivos específicos da fiscalização:

elaboração de questionário eletrônico para levantamento da situação da governança de TI na APF (doravante chamado perfil GovTI2010);

atualização da base de dados com o perfil da governança de TI na APF;

elaboração das matrizes de planejamento e possíveis achados para a avaliação de controles gerais de TI;

realização de treinamento para avaliação de controles gerais de TI;

avaliação de controles gerais em catorze jurisdicionados;

validação das respostas dos questionários perfil GovTI2010 (nos catorze jurisdicionados);

avaliação de quatro objetos específicos de TI;

avaliação da atuação dos órgãos governantes superiores (SLTI/MP, GSI/PR, CGU/PR etc);

obtenção da relação de causa-efeito entre maturidade dos controles gerais de TI e desconformidades nos objetos específicos de TI;

obtenção da relação de causa-efeito entre a atuação dos órgãos governantes superiores e a situação da governança de TI na APF;

ratificação ou retificação da situação da governança de TI declarada no perfil GovTI2010, em confronto com a que for evidenciada *in loco*.

Por oportuno, apresentamos o conceito de controles gerais de TI obtido de documento do Instituto de Auditores Internos intitulado GTAG Information Technology Controls Auditing:

Controles gerais de TI – Aplicam-se a todos os componentes do sistema, dos processos, e dos dados de uma organização ou ambiente. Controles gerais incluem, mas não estão limitados às políticas de segurança da informação, de administração, de acesso e de autenticação, de segregação de funções chaves de TI, de gestão de aquisição e implementação de sistemas, de gestão de mudanças, de cópias de segurança e de continuidade do negócio. (tradução livre).

#### Escopo

Fazem parte do escopo das auditorias que compuseram a Fiscalização de Orientação Centralizada (FOC):

controles gerais de TI;

contratos de soluções de TI, nos quais se buscava evidenciar consequências da ausência ou deficiência dos controles gerais de TI.

Uma vez que inexistia contrato de TI em vigor no Dnocs, ente auditado pela Secex/CE, aquela unidade técnica não realizou os testes substantivos nas contratações de TI.

Considerando ainda o cenário obtido por meio do TMS realizado em 2007 (Acórdão 2.471/2008-TCU-Plenário) e os resultados iniciais do levantamento que gerou o Acórdão 2.308/2010-TCU-Plenário, havia expectativa de que os órgãos públicos ainda se encontrassem com pouca maturidade de governança de TI.

Assim, optou-se pela estratégia de desenvolver um método para avaliar a governança de TI em instituições com baixa maturidade, de tal forma que auditores não especialistas em TI, orientados por auditores especialistas, pudessem executar a avaliação pretendida.

O método foi construído por meio de questões e procedimentos de auditoria para que fossem avaliadas duas principais classes de objetos: controles dos processos organizacionais da governança de TI e alguns produtos e artefatos resultantes da execução desses processos. Também foram estabelecidos parâmetros mínimos que garantissem a existência dos produtos ou dos controles avaliados, tudo em função do escopo pretendido (maior amplitude e menor profundidade na avaliação). Os parâmetros foram baseados nos critérios de auditoria positivados na legislação brasileira (ver item 0 – Critérios de auditoria e evolução normativa) e nas boas práticas nacionais e internacionais, como Cobit, normas NBR ISO/IEC 38.500, 27.002, 12.207, 15.504 e 20.000 e PMBoK.

Assim, a inexistência de registro de achado de auditoria na FOC (o que praticamente não ocorreu) não significa que o jurisdicionado encontra-se aderente às boas práticas, mas sim que foram implantados os elementos mínimos verificados no escopo deste trabalho, elementos que podem ser deduzidos a partir das requisições de informações feitas nos trabalhos de campo, que estão contidas no Apêndice 0.

#### Fiscalizações integrantes do TMS

Conforme será detalhado adiante, este TMS foi conduzido por meio de 21 trabalhos: um levantamento de auditoria;

catorze auditorias para avaliação de controles gerais de TI (ACGTI), conduzidas na modalidade Fiscalização de Orientação Centralizada (FOC);

quatro auditorias em objetos específicos de TI (e.g., sistemas, contratos, projetos);

um monitoramento de deliberações com orientações aos OGS;

uma fiscalização consolidadora dos vinte trabalhos anteriores, que se materializa neste relatório.

#### Questões de auditoria

O levantamento perfil GovTI2010 foi realizado por meio de trinta questões, subdivididas em 152 itens, organizadas segundo sete (das oito) dimensões do Gespública: liderança, estratégias e planos, cidadãos, sociedade, informações e conhecimento, pessoas e processos (anexo 2, fls. 25v-26v).

Cada uma das catorze auditorias que integraram a FOC de avaliação de controles gerais de TI foi realizada por meio das doze questões de auditoria a seguir:

O Unidade executa o processo de planejamento estratégico institucional de acordo com as boas práticas?

O Unidade executa o processo de planejamento estratégico de TI de acordo com as boas práticas?

A organização da área de TI é adequada às atividades a que ela deve dar suporte?

O Unidade executa o processo orçamentário de TI segundo a legislação e as boas práticas?

Há processo de software estabelecido no Unidade?

Há processo de gerenciamento de projetos de TI estabelecido no Unidade?

Há processos de gestão de serviços de TI que apoiem o Unidade na administração da qualidade dos serviços de TI?

O Unidade executa os processos corporativos de segurança da informação segundo a legislação e as boas práticas?

Há plano de capacitação de profissionais de TI que auxilie no desenvolvimento das competências necessárias para a boa execução dos trabalhos?

O Unidade realiza monitoração do desempenho da gestão e uso de TI?

O Unidade realiza o processo de contratação de bens e serviços de TI segundo as normas vigentes?

O Unidade realiza o processo de gestão de contratos de bens e serviços de TI segundo as normas vigentes?

Cada uma das quatro auditoras específicas teve suas próprias questões de auditoria, definidas de acordo com o objeto específico auditado.

Questões de auditoria não se aplicam ao monitoramento nos órgãos governantes superiores.

As questões de auditoria da FOC, com seus possíveis achados, encontram-se no Apêndice 0. Registre-se que dos 57 possíveis achados apenas dois não foram evidenciados em qualquer das catorze fiscalizações.

#### Estratégia metodológica

Este trabalho seguiu o roteiro de auditoria de conformidade do TCU, mas não necessariamente guarda conformidade com todo o conteúdo das Normas de Auditoria do TCU (NAT), uma vez que todo o planejamento e boa parte da execução das fiscalizações ocorreram antes da publicação das NAT em 8/12/2010.

#### Diretrizes seguidas no planejamento

Foram seguidas as seguintes diretrizes no planejamento da FOC:

o resultado deve trazer visão sistematizada e sistêmica;

o TMS como um todo deve equilibrar abrangência e profundidade das questões de auditoria, por meio de uma abordagem iterativa e incremental;

a Sefti deve fornecer suporte metodológico, inclusive treinamento, a todos os participantes;

a Sefti deve fornecer apoio durante a execução de todas as fiscalizações, inclusive com um AUFC integrando a equipe em tempo parcial.

#### Estratégia de condução

O trabalho foi dividido em sete fases, a saber:

preparação;

1<sup>a</sup> fase – levantamento do perfil GovTI;

2<sup>a</sup> fase – auditorias-piloto;

3<sup>a</sup> fase – avaliação dos controles gerais de TI;

- 4<sup>a</sup> fase – auditorias específicas;
- 5<sup>a</sup> fase – monitoramentos (órgãos governantes superiores);
- 6<sup>a</sup> fase – consolidação.

#### Preparação

Realizada por meio de levantamento de auditoria (TC 001.484/2010-9; Acórdão 2.196/2010-TCU-1<sup>a</sup> Câmara), teve por objetivo coletar informações que possam subsidiar o planejamento de auditorias relacionadas ao TMS.

#### 1<sup>a</sup> fase – levantamento perfil GovTI2010

Realizado também por meio de levantamento de auditoria (TC 000.390/2010-0; Acórdão 2.308/2010-TCU-Plenário), teve por objetivo acompanhar e manter base de dados atualizada com a situação da governança de TI na Administração Pública Federal.

#### 2<sup>a</sup> fase – auditorias-piloto

Nessa fase foram realizadas duas auditorias-piloto. A auditoria-piloto para avaliação de controles gerais de TI teve o objetivo de validar as matrizes de planejamento e os ofícios de requisição de informações que seriam utilizadas na FOC (3<sup>a</sup> fase), de modo a mitigar futuros riscos de auditorias.

Uma vez validada a matriz, foi elaborado treinamento visando capacitar os auditores das unidades técnicas e da Sefti nas questões e procedimentos de auditoria a serem utilizados nas próximas fases do TMS 2010.

A auditoria-piloto para teste dos papéis de trabalho foi realizada no Departamento Nacional de Infraestrutura de Transportes (Dnit), onde também se realizou a primeira auditoria específica, no Sistema de Acompanhamento de Contratos (Siac) da Autarquia, iniciando o processo de avaliação de causa-efeito pretendido neste trabalho (item 0).

Dentre os papéis de trabalho validados, destacamos o Ofício de Comunicação de Auditoria, cujo modelo encontra-se no apêndice 0, que continha o pedido das informações que os gestores deveriam apresentar às equipes para a avaliação da governança de TI.

Considerando que as informações contidas no ofício supra podem ser orientadoras para os gestores, propõe-se determinar à Sefti que dê publicidade, inclusive por meio do sítio do TCU na internet, às informações acerca da governança de tecnologia da informação que foram solicitadas aos gestores nesta fiscalização (subitem 0).

#### 3<sup>a</sup> fase – avaliação dos controles gerais de TI

Nessa fase foram avaliados os controles gerais de TI nos entes jurisdicionados selecionados. As fiscalizações foram realizadas em três etapas contendo cinco, cinco e três auditorias, respectivamente, num total de treze auditorias, sendo que cada etapa foi executada sequencialmente às demais, de forma a proporcionar o melhor aproveitamento dos recursos humanos disponíveis na unidade coordenadora.

Aproximadamente 25 dias antes do início de cada etapa, foi enviado um ofício de requisição de informações a cada um dos entes jurisdicionados selecionados para aquela etapa. Esse ofício teve como objetivo solicitar antecipadamente alguns documentos e informações necessários à execução dos procedimentos de auditoria, o que em tese reduziria o esforço necessário durante a fase de execução.

Uma vez selecionados os entes jurisdicionados, a Secex, de cuja clientela o ente faz parte, foi convidada a coordenar a auditoria proposta, com o apoio operacional e metodológico da Sefti.

Os entes selecionados foram quatro Ministérios (Saúde, Ciência e Tecnologia, Relações Exteriores e Planejamento), cinco autarquias (Dnit, Susep, Anatel, Dnocs e FNDE), uma fundação (Ibama), dois tribunais (TRT das 2<sup>a</sup> e 4<sup>a</sup> Regiões), uma empresa pública (Finep) e uma sociedade de economia mista (Amazonas Energia).

Catorze equipes participaram da FOC, sendo uma de cada uma das onze unidades técnicas do TCU a seguir – Secex/AM, Secex/CE, Secex/RJ, Secex/RO, Secex/RR, Secex/RS, Secex/SP, Secex/1, Secex/5, Secex/6, Secex/9 – e três equipes da Sefti.

A seleção dos jurisdicionados auditados seguiu o seguinte critério: escolha da instituição com contratos de maior materialidade para prestação de serviços de TI dentro da clientela das unidades

técnicas participantes, com homologação pela Secex que realizaria a auditoria, cabendo eventuais ajustes em função da experiência de cada Secex com seus auditados.

Cabe destacar que a seleção dos jurisdicionados a serem auditados, feita pela coordenação em conjunto com as unidades técnicas do TCU, não é estatisticamente representativa, o que não permite a generalização dos resultados aqui apresentados.

A fase de planejamento dessas auditorias, de duração de duas semanas, foi caracterizada por um treinamento prático, na forma de execução da fiscalização assistida pela Sefti, sobre as questões e procedimentos de auditoria definidos na etapa de preparação e validados na auditoria-piloto de controles gerais (2ª fase). O treinamento previsto para essa fase foi realizado por meio de videoconferência no caso de auditoria sob a responsabilidade de uma ou mais Secex situadas nos estados, e presencialmente para as Secex da sede. Nessa etapa de planejamento, houve um auditor da Sefti alocado em cada equipe em tempo integral.

Durante a fase de execução, prevista para três semanas, o auditor de TI da Sefti integrou a equipe por uma semana, de modo a orientar e auxiliar a execução de alguns procedimentos.

As atividades previstas para a fase de relatório foram de responsabilidade das Secex, estando a Sefti e seus auditores à disposição para o esclarecimento de dúvidas e sugestões sobre o tema. No mesmo período, o auditor de TI da Sefti que participou do trabalho foi alocado em tempo parcial na atividade de acompanhamento da elaboração do relatório final. Importante ressaltar que, embora a Sefti tenha disponibilizado recursos para todas as equipes de auditoria, os processos (TC) foram coordenados e conduzidos pelas Secex, cabendo à Sefti alocar um auditor para participar das equipes, em tempo integral na fase de planejamento e em tempo parcial na fase de execução.

Ao final de cada etapa, um dos entes já avaliados em controles gerais de TI foi selecionado, segundo critérios de relevância estabelecidos pela Sefti, para ter algum aspecto específico de um objeto de TI avaliado detalhadamente (auditoria específica).

#### 4ª fase – auditorias específicas

As auditorias específicas foram realizadas por AUFC da Sefti acerca de alguns aspectos específicos de objetos de TI de jurisdicionados que receberam avaliação de controles gerais de TI, de forma a evidenciar possíveis consequências das fragilidades na governança de TI detectadas à época.

Foram selecionados os seguintes objetos:

contratos de entes da APF com o Serpro, devido à materialidade e aos indícios, obtidos no primeiro grupo de auditorias, de que esses contratos não estavam aderentes ao arcabouço legal (TC 022.241/2010-8);

sistema informatizado que suporta o Sistema Nacional de Transplantes, devido às fragilidades identificadas nos controles gerais relativos à segurança da informação no Datasus durante a ACGTI no Ministério da Saúde, à materialidade do programa (com dotação aproximada de R\$ 1,3 bilhão para 2010) e ao apoio do sistema à política de governo com grande relevância social, uma vez que se interfere em aspectos de manutenção e qualidade da vida humana (TC 029.074/2010-0);

Contrato 02.003.00/2009, firmado entre o Ministério de Ciência e Tecnologia (MCT) e a empresa Módulo Security Solutions S.A. (Módulo), cujo objeto é consultoria em segurança da informação, incluindo suas possíveis implicações na governança de TI do Ministério, devido ao seguinte: identificação de fragilidades nos controles gerais relativos à segurança da informação no MCT durante a ACGTI; materialidade do contrato (R\$ 3.292.151,00); existência de representação de equipe de auditoria registrando indícios de irregularidade na gestão do contrato (TC 022.815/2010-4); possibilidade de multiplicação na APF desse tipo de contrato, devido à edição das Normas Complementares do GSI sobre gestão de segurança da informação (TC 029.120/2010-1).

#### 5ª fase – monitoramento nos OGS

Essa fase teve como objetivo monitorar as determinações e recomendações contidas em diversos acordãos estruturantes (e.g., Acordãos 1.094/2004, 2.471/2008, 1.603/2008, todos do Plenário do TCU). Por essas determinações e recomendações estarem relacionadas ao tema abordado pelo TMS 2010, além do fato de que as ações empreendidas pelos OGS deveriam ter impacto na situação da governança de TI na APF, optou-se por inserir seus monitoramentos no escopo do trabalho.

Falhas e impropriedades eventualmente encontradas nas auditorias das fases anteriores podem ter como uma de suas causas a ausência ou a deficiência de orientações e normativos que fundamentem a atuação dos gestores de TI. Em virtude dessa provável constatação, era necessário realizar monitoramento das ações referentes à promoção da governança de TI conduzidas pelos órgãos com essa competência.

Uma única ação de fiscalização conduzida pela Sefti (TC 028.772/2010-5; Acórdão 1.145/2011-TCU-Plenário) monitorou deliberações contidas em sete acórdãos, dirigidas a onze órgãos governantes superiores.

#### 6ª fase – consolidação

O objetivo dessa fase consiste em agregar os resultados de todas as fiscalizações previstas, de modo a sintetizar os achados e conclusões sobre a gestão e uso de TI na APF, o que se faz por meio deste relatório.

#### Avaliações do trabalho

Como medida para avaliar o trabalho realizado, foram feitas duas avaliações: uma com as equipes participantes e outra com os responsáveis pelos jurisdicionados auditados nas ACGTI.

A avaliação feita pelos analistas do TCU que participaram da FOC (síntese no anexo 4, fl. 34) teve como objetivo avaliar a atuação da Sefti como unidade coordenadora dos trabalhos, bem como buscar oportunidades de melhoria no processo de condução de FOC, uma vez que, como unidade técnica especializada, é razoável imaginar que esse tipo de trabalho (coordenação de FOC) seja uma atividade relativamente comum à Sefti. A coordenação desta Secretaria teve índice de 90% de satisfação e recebeu informações que constituem oportunidades de melhoria.

A avaliação feita com os responsáveis pelos entes auditados (síntese no anexo 4, fl. 1) teve como objetivo verificar a satisfação no relacionamento entre auditor e auditado, além de possibilitar o aperfeiçoamento individual das condutas das diversas equipes em trabalhos futuros. A pesquisa indicou 94% de satisfação dos auditados com as equipes de auditoria e registrou oportunidades de melhoria para a atuação dessas.

#### Limitações

A limitação registrada por algumas equipes diz respeito à demora, por parte do auditados, em responder às solicitações das equipes e em disponibilizar as informações requeridas.

#### Volume de recursos fiscalizados

O volume de recursos fiscalizados foi de cerca de R\$ 47,6 bilhões, conforme consta do apêndice 0. O valor corresponde a soma dos valores dos contratos analisados nas diversas auditorias, mais a soma dos valores dos contratos de obras do Dnit cadastrados no Sistema de Acompanhamento de Contratos – Siac, objeto da auditoria do TC 010.474/2010-2.

#### Benefícios estimados

Devido aos objetivos pretendidos com este TMS, não se obtiveram benefícios quantificáveis.

Os benefícios não quantificáveis se traduzem na indução de melhorias na organização interna (governança e gestão de TI) das catorze unidades auditadas, bem como indução da melhoria da estrutura da governança de TI de toda a APF por meio de orientações aos órgãos governantes superiores.

#### Processos conexos

Os processos conexos a este são os constantes do apêndice 0.

#### RESULTADOS DA AVALIAÇÃO EMPREENDIDA

##### Processo de planejamento estratégico institucional

Considerando que a governança de TI deve prover meios para que as ações de TI estejam alinhadas ao negócio, a primeira questão de auditoria da FOC ('O Unidade executa o processo de planejamento estratégico institucional de acordo com as boas práticas?') buscou evidenciar como os entes auditados organizam suas estratégias de negócio de longo prazo, o que normalmente resulta em um documento chamado Plano Estratégico Institucional (PEI).

O que se esperava, segundo o previsto no critério 2 do Programa Nacional de Gestão Pública e Desburocratização (Gespública), eram documentos resultantes do planejamento de longo prazo do negócio com as seguintes características:

publicados formalmente;

elaborados com a participação de todas as partes envolvidas em sua execução;

elaborados com métodos e técnicas reconhecidos no mercado, o que conduz a planejamentos de melhor qualidade;

desdobrados pelas diversas áreas executoras, em planos de médio e curto prazo;

divulgados;

avaliados periodicamente.

Registre-se que o Gespública, instituído pelo Decreto 5.378/2005, é uma diretriz presidencial focada no cumprimento do princípio da eficiência e, em 2010, teve dotação de R\$ 5,35 milhões (ação 2D330000 – Fomento à Melhoria da Gestão Pública – do Programa 1.088 – Fortalecimento da Capacidade de Gestão Pública, constante do volume II da Lei 12.214/2010 – LOA 2010).

O Quadro 2 apresenta o resultado obtido na avaliação in loco, o qual evidencia que mais da metade dos auditados não possuem planos de negócio para o longo prazo. Além disso, à exceção do Ministério da Saúde, os demais auditados tinham planos incompletos (e.g., falta de metas para os objetivos estratégicos) e apresentavam outras falhas decorrentes da ausência da totalidade das características elencadas no item 0.

Em outra linha de análise, os dados constantes do Apêndice 0 (linha A da tabela) evidenciam que cinco auditados que declararam possuir processo de planejamento estratégico institucional de fato não o possuem, ante a ausência de evidências apresentadas às equipes do TCU, o que sugere que a situação descrita no Acórdão 2.308/2010-TCU-Plenário pode ser pior, ou seja, pode haver mais pesquisados que não executam o processo de planejamento estratégico institucional além dos 21% que declararam não o executar.

Registre-se que, no monitoramento realizado (TC 028.772/2010-5, Acórdão 1.145/2011-TCU-Plenário), foi identificado que o único OGS a orientar seus jurisdicionados quanto ao tema foi o CNJ, o que contribuiu para a suposta melhora da situação, se comparados os dados de 2007 e 2010 (anexo 2, fl. 4, item 42), sendo que, diante do cenário evidenciado, há oportunidade e conveniência para aprimoramento da atuação dos demais OGS.

Quadro 2 – Processo de planejamento estratégico (achados)

Possíveis achados	Dnit	SE/MS	SE/MCT	Ibama	Susep	TRT-SP	Dnocs	SE/MRE	TRT-RS	Anatel	Finep	SE/MP	ADE	FNDE
Inexistência do Plano Estratégico Institucional	X			X				X				X	X	X
Falhas no Plano Estratégico Institucional					X	X			X	X	X			
Falhas no Processo de Planejamento Estratégico Institucional					X	X			X	X	X			

A consequência mais direta da ausência ou deficiência do planejamento institucional é a impossibilidade de os gestores demonstrarem que atendem ao princípio constitucional da eficiência, uma vez que não se pode avaliar sua gestão por meio de parâmetros objetivos de comparação entre o planejado e o executado. É o que se requer, por exemplo, na Decisão Normativa TCU 110/2010, quanto ao primeiro elemento a constar do relatório de auditoria de gestão:

1. Avaliação dos resultados quantitativos e qualitativos da gestão, em especial quanto à eficácia e eficiência no cumprimento dos objetivos e metas (físicas e financeiras) planejados e/ou pactuados para o exercício, identificando as causas de insucessos no desempenho da ação administrativa. (grifamos)

Outra consequência é a impossibilidade de alinhar o uso da TI ao negócio, para que essa contribua para o alcance dos objetivos organizacionais, já que esses objetivos não são explicitados ou mensuráveis objetivamente. A ausência de cultura de planejamento de longo prazo para o negócio consiste em uma lacuna no campo da governança corporativa, lacuna esta que limita a maturidade da governança de TI nas organizações, como relatado no parágrafo 0 adiante.

Por oportuno, transcreve-se a seguir excerto do discurso proferido pelo Sr. Jorge Gerdau, presidente da Câmara de Políticas de Gestão, Desempenho e Competitividade do Conselho de Governo, no evento de lançamento do Plano Estratégico do TCU para o período 2011-2015, que evidencia que aquele dirigente compartilha o entendimento exposto ao longo desta seção: ‘Eu, hoje, estou convicto de que no trabalho que os senhores colocaram, fico extremamente feliz porque eu gostaria que em todos os Ministérios, todas as grandes atividades, tivesse um mapa estratégico como esse (...)’ (sublinhou-se).

Pesquisa na legislação, cujo produto encontra-se nos apêndices 0 e 0, identificou que o normativo que estabelece a estrutura regimental de treze dos 37 órgãos da administração direta do Poder Executivo não se refere a qualquer documento de planejamento institucional.

Para os outros 24 órgãos, o decreto presidencial que define a estrutura regimental estabeleceu como responsabilidade do secretário-executivo da pasta ‘coordenar, consolidar e submeter ao Ministro de Estado o plano de ação global da [pasta]’ (itens 5 a 28 do apêndice 0).

Assim, por meio de diligência (exemplo à fl. 9), solicitaram-se aos 24 secretários-executivos as seguintes informações:

cópia eletrônica do Plano de Ação Global consolidado, conforme previsto no respectivo decreto de regimento interno, identificado no apêndice 0;

o endereço de publicação do Plano de Ação Global na internet, caso esteja ali publicado;

cópia do documento que formaliza a submissão do Plano de Ação Global ao Ministro de Estado, conforme previsto no respectivo decreto de regimento interno, identificado no apêndice 0;

caso exista, cópia do documento de aprovação do Plano de Ação Global pelo Ministro de Estado, conforme previsto no respectivo decreto de regimento interno, identificado no apêndice 0;

caso exista, cópia eletrônica do documento de referência que defina o processo de trabalho utilizado para a elaboração do Plano de Ação Global.

O Quadro 3 resume as respostas encaminhadas em atenção às diligências (fls. 9-306, principal e v.1):

Quadro 3 – Tabulação das respostas sobre a existência do Plano de Ação Global (PAG)

Ofício Sefti	Órgão diligenciado	PAG	Internet	Submissão	Aprovação	Processo
408	Casa Civil da Presidência da República	não	não	não	não	não
409	Ministério da Agricultura, Pecuária e Abastecimento	não	não	não	não	não
410	Ministério da Ciência, Tecnologia e Inovação	SIM	SIM	não	não	não
411	Ministério da Educação	não	não	não	não	não
412	Ministério da Fazenda	não	não	não	não	SIM
413	Ministério da Integração Nacional	não	não	não	não	não
414	Ministério da Justiça	SIM	não	não	não	SIM
415	Ministério da Previdência Social	SIM	não	não	SIM	SIM
416	Ministério da Saúde	SIM	não	não	não	não
417	Ministério das Cidades	não	não	não	não	não
418	Ministério de Minas e Energia	não	não	não	não	não
419	Ministério do Desenvolvimento Agrário	Não respondeu após o prazo de 30 dias.				
420	Ministério do Desenvolvimento, Indústria e Comércio Exterior	SIM	SIM	não	não	não
421	Ministério do Desenvolvimento Social e	SIM	não	não	não	não

	Combate à Fome					
422	Ministério do Esporte					
423	Ministério do Meio Ambiente	não	não	não	não	não
424	Ministério do Planejamento, Orçamento e Gestão	não	não	não	não	não
425	Ministério do Trabalho e Emprego	SIM	não	não	não	SIM
426	Ministério do Turismo	não	não	não	não	não
427	Ministério dos Transportes	não	não	não	não	não
428	Secretaria de Assuntos Estratégicos da Presidência da República	não	não	não	não	não
429	Secretaria de Relações Institucionais da Presidência da República	não	não	não	não	não
430	Secretaria-Geral da Presidência da República	não	não	não	não	não
431	Secretaria de Aviação Civil da Presidência da República	não	não	não	não	não

Legenda: PAG – apresentou evidência de que existe plano de ação global ou outro documento que consolida o planejamento de todo a instituição?; Internet – apresentou evidência de que publica o plano consolidado na Internet?; Submissão – apresentou evidência de que o Secretário-Executivo submeteu o plano consolidado ao Ministro?; Aprovação – apresentou evidência de que o Ministro aprovou o plano consolidado?; Processo – apresentou evidência de que existe um processo formal de planejamento que conduz a um plano consolidado?

A análise da legislação sobre o tema (apêndice 0) juntamente com o Quadro 3 permite chegar às seguintes conclusões:

a ausência de referência a qualquer documento de planejamento institucional no normativo que estabelece a estrutura regimental de treze órgãos constitui lacuna de atribuição de responsabilidade nesses órgãos com respeito ao tema;

não há normativo que estabeleça o que é um Plano de Ação Global (PAG), apesar de haver normativo que obrigue 24 órgãos com status de ministério a ter um;

a maioria dos Ministérios diligenciados (17 de 24, ou seja 71%) não possui PAG;

dos sete órgãos que apresentaram um documento que entendem por PAG, cinco (71%) não dão publicidade do documento na internet;

em nenhum dos 24 Ministérios diligenciados, o secretário-executivo deu cumprimento ao dispositivo regimental de ‘submeter ao Ministro de Estado o plano de ação global’;

somente em um caso há evidência de que o Ministro de Estado aprovou formalmente o documento do PAG;

a maioria dos Ministérios (20 de 24, ou seja 83%) não tem processo de trabalho para elaborar um PAG.

Os dados apresentados sobre o PAG no item 0 corroboram a necessidade de definição, pela Câmara de Políticas de Gestão, Desempenho e Competitividade (CGDC) do Conselho de Governo, de uma orientação sobre como deve ser o processo de planejamento institucional nos órgãos e entidades do Poder Executivo Federal, sem prejuízo de que seja proposto dar ciência aos 23 Ministérios de que os secretários-executivos não submeteram aos Ministros de Estado o Plano de Ação Global da pasta, o que afronta os respectivos decretos que estabelecem sua Estrutura Regimental (considerou-se que a aprovação do PAG pelo Ministro da Previdência Social supriu a não submissão formal pelo secretário-executivo).

Conclui-se que carece de aperfeiçoamento a cultura de planejamento institucional de longo prazo, em especial nos órgãos e entidades do Poder Executivo e do Ministério Público, motivo pelo qual se propõem recomendações para a Câmara de Políticas de Gestão, Desempenho e Competitividade (CGDC) do Conselho de Governo e para o CNMP nos termos a seguir.

Recomendar que, em atenção ao Decreto-Lei 200/1967, art. 6º, inciso I, e art. 7º, normatize a obrigatoriedade de que todos os entes sob sua jurisdição estabeleçam processo de planejamento estratégico institucional, observando as boas práticas sobre o tema, a exemplo do critério de avaliação 2 do Gespública, contemplando, pelo menos (subitem 0):

elaboração, com participação de representantes dos diversos setores da organização, de um documento que materialize o plano estratégico institucional de longo prazo, contemplando, pelo menos, objetivos, indicadores e metas para a organização;

aprovão, pela mais alta autoridade da organização, do plano estratégico institucional; desdobramento do plano estratégico pelas unidades executoras;

divulgação do plano estratégico institucional para conhecimento dos cidadãos brasileiros, exceto nos aspectos formalmente declarados sigilosos ou restritos;

acompanhamento periódico do alcance das metas estabelecidas, para correção de desvios; divulgação interna e externa do alcance das metas, ou dos motivos de não ter alcançado.

#### Processo de planejamento estratégico de TI

A segunda questão de auditoria da FOC ('O Unidade executa o processo de planejamento estratégico de TI de acordo com as boas práticas?') buscou evidenciar como os entes auditados organizam suas estratégias de longo prazo para que a tecnologia da informação apoie o negócio, o que normalmente se faz em um documento chamado Plano Estratégico de TI (PDTI) ou Plano Diretor de TI (PDTI).

O que se esperava, segundo o previsto no processo PO1 – Planejamento Estratégico de TI do Cobit 4.1, eram documentos decorrentes do processo de planejamento de longo prazo da TI com as seguintes características:

publicados formalmente;

elaborados com a participação de todas as partes interessadas (TI e áreas de negócio);

elaborados com métodos e técnicas reconhecidos no mercado, o que conduz a planejamentos de melhor qualidade;

desdobrados pelas diversas áreas executoras, em planos de médio e curto prazo;

divulgados;

avaliados periodicamente;

alinhanados com o plano estratégico institucional.

O Quadro 4 apresenta o resultado obtido na avaliação in loco, no qual se evidencia que nove dos catorze auditados não possuem os planos em questão, enquanto os demais auditados tinham planos incompletos (e.g., falta de metas para os objetivos estratégicos) ou apresentavam outras falhas decorrentes da ausência da totalidade das características elencadas no item 0.

Quadro 4 – Processo de planejamento estratégico de TI (achados)

Possíveis achados	Dnit	SE/MS	SE/MCT	Ibama	Susep	TRT-SP	Dnocs	SE/MRE	TRT-RS	Anatel	Finep	SE/MP	ADE	FNDE
Inexistência do PDTI		X			X	X	X				X			
Falhas no PDTI								X		X		X	X(1)	X(1)
Falhas no Processo de Planejamento de TI	X							X		X				X

(1) Consta do relatório original com o título: Falhas no Plano Diretor de TI (PDTI)

(2) Consta do relatório original com o título: Inexistência de Plano Diretor de Tecnologia da Informação

Em outra linha de análise, os dados constantes do Apêndice 0 (linha B da tabela) evidenciam que houve dois auditados que declararam possuir processo de planejamento estratégico de TI, mas que, ante a ausência de evidências apresentadas às equipes do TCU, de fato não o possuem, o que sugere que a situação descrita no Acórdão 2.308/2010-TCU-Plenário pode ser de fato ainda pior, ou seja,

pode haver mais pesquisados que não executam o processo de planejamento estratégico de TI além dos 61% que declararam não o executar.

Registre-se que, no monitoramento realizado (TC 028.772/2010-5; Acórdão 1.145/2011-TCU-Plenário), foi identificado que o CNJ e a SLTI/MP orientaram seus jurisdicionados quanto ao tema, e, mesmo assim, observa-se que os diversos auditados ainda não tinham dado cumprimento às orientações contidas na Resolução – CNJ 99/2009 e na IN – SLTI 4/2008. Entretanto, orientação contida na IN – SLTI 4/2010 trata apenas da obrigatoriedade de elaboração de PDTI anteriormente às contratações, e não de uma orientação sobre como estabelecer um processo de planejamento estratégico de TI, sendo, diante do cenário evidenciado, oportuna e conveniente a atuação dos OGS.

Assim como ocorre com as deficiências no planejamento estratégico de negócio, uma das consequências da ausência ou deficiência no planejamento de longo prazo para a TI consiste na impossibilidade de evidenciar cumprimento ao princípio constitucional da eficiência. De fato, em todos os processos de contratação analisados nas catorze fiscalizações, não havia demonstração de que a despesa executada consistia na melhor alocação de recursos possível.

Outra consequência da ausência desse tipo de planejamento pode ser evidenciada no caso relatado no Acórdão 2.023/2005-TCU-Plenário, quando, após o término (bem-sucedido) do desenvolvimento de um sistema que suportaria a implementação de uma ação do governo, houve um retardo de dois anos para que o sistema entrasse em produção. A causa do ocorrido foi que, devido à ausência de planejamento da TI como um todo, não foi prevista a substituição da infraestrutura tecnológica (servidores, equipamentos de rede etc) por outra de maior velocidade capaz de suportar o novo sistema.

Sobre o tema, cabe registrar que o plano estratégico de TI tratado nesse item não é um documento do setor de TI da organização, mas um documento da organização, vez que formaliza a alocação de recursos (financeiros, humanos, materiais etc) para que a TI atenda às demandas do negócio. Registre-se que essa ressalva constou de fala do Ministro substituto do TCU Augusto Sherman em evento do Ciclo de Palestras 2011 promovido pelo TCU em 4 de agosto de 2011, cujo público-alvo foi a alta administração dos órgãos do Poder Judiciário.

Conclui-se que carece de aperfeiçoamento a cultura de planejamento de longo prazo de TI, sendo que há necessidade de orientação dos OGS dos órgãos e entidades do Poder Executivo e do Ministério Público nesse sentido, motivo pelo qual se propõem recomendações para a Câmara de Políticas de Gestão, Desempenho e Competitividade (CGDC) do Conselho de Governo e para o CNMP nos termos a seguir.

Recomendar que, em atenção ao Decreto-Lei 200/1967, art. 6º, inciso I, e art. 7º, normatize a obrigatoriedade de que todos os entes sob sua jurisdição estabeleçam processo de planejamento estratégico de TI, observando as boas práticas sobre o tema, a exemplo do processo PO1 – Planejamento Estratégico de TI do Cobit 4.1, contemplando, pelo menos (subitem 0):

elaboração, com participação de representantes dos diversos setores da organização, de um documento que materialize o plano estratégico de TI, contemplando, pelo menos:

objetivos, indicadores e metas para a TI organizacional, sendo que os objetivos devem estar explicitamente alinhados aos objetivos de negócio constantes do plano estratégico institucional;

alocação de recursos (financeiros, humanos, materiais etc);

estratégia de terceirização;

aprovação, pela mais alta autoridade da organização, do plano estratégico de TI;

desdobramento do plano estratégico de TI pelas unidades executoras;

divulgação do plano estratégico de TI para conhecimento dos cidadãos brasileiros, exceto nos aspectos formalmente declarados sigilosos ou restritos;

acompanhamento periódico do alcance das metas estabelecidas, para correção de desvios;

divulgação interna e externa do alcance das metas, ou os motivos de não as ter alcançado.

Estrutura de TI

A terceira questão de auditoria da FOC buscou verificar se a organização da TI organizacional era adequada às atividades a que ela deve dar suporte. Nesse tema foram avaliados:

funcionamento dos comitês de TI;  
definição e ocupação de papéis sensíveis dentro da TI;  
forma de avaliação do quadro de pessoal de TI.

Um comitê estratégico de TI tem como funções básicas assegurar que a governança de TI seja adequadamente tratada, aconselhar a direção estratégica de TI e revisar os grandes investimentos (Cobit 4.1, PO4.2). Já um comitê de direção de TI tem como atribuições típicas priorizar os investimentos de TI em alinhamento com a estratégia e as prioridades do negócio da instituição, acompanhar o status dos projetos e resolver conflitos por recursos e monitorar os níveis de serviço e as melhorias implantadas na organização (Cobit 4.1, PO4.3).

Segundo as boas práticas, espera-se encontrar dentro de um setor de TI uma estrutura formal (Cobit 4.1, PO4.5), com papéis e suas responsabilidades formalmente definidos (Cobit 4.1, PO4.6), em que os papéis sensíveis encontrem-se com responsáveis formalmente designados (Cobit 4.1, PO4.13) e que os responsáveis pela gestão da TI das organizações sejam integrantes do quadro da organização (Decreto-Lei 200/1967, art. 10, § 7º).

O Quadro 5 apresenta o resultado obtido na avaliação in loco, no qual se evidencia que:

em sete auditados o comitê não estava instituído e em outros cinco estava instituído, mas não era atuante. Somente em dois entes identificaram-se comitês atuantes;

ainda há organizações em que as atividades de gestão (planejamento, coordenação, controle e supervisão) são exercidas na prática por não servidores públicos.

A quase totalidade dos auditados não possui uma avaliação das suas necessidades de pessoal no setor de TI, a despeito do recorrente argumento de que falta pessoal nesses setores.

Quadro 5 – Estrutura de TI (achados)

Possíveis achados	Dnit	SE/MS	SE/MCT	Ibama	Susep	TRT-SP	Dnocs	SE/MRE	TRT-RS	Anatel	Finep	SE/MP	ADE	FNDE
Inexistência de comitê de TI				X										
Falhas relativas ao comitê de TI									X		X	X		X
Inexistência de definição formal de papéis e responsabilidades														X
Papéis sensíveis sem responsável														
Papel sensível exercido por não servidor														X
Inexistência de avaliação do quadro de pessoal de TI	X			X	X	X	X	X	X		X	X	X	
Falhas na avaliação do quadro de pessoal de TI										X				
Inadequação do quadro de pessoal de TI			X											

Com respeito aos comitês de TI, os dados constantes do Apêndice 0 (linha C da tabela) evidenciam que houve um auditado que declarou possuir comitê instituído, mas que, ante a ausência de evidências apresentadas à equipe do TCU, de fato não o possui, sugerindo que a situação descrita no Acórdão 2.308/2010-TCU-Plenário de fato pode ser ainda pior, ou seja, pode haver mais pesquisados que não possuem comitês de TI além dos 68% que declararam não o possuir.

Registre-se que, no monitoramento realizado (TC 028.772/2010-5; Acórdão 1.145/2011-TCU-Plenário), foi identificado que o único OGS a orientar seus jurisdicionados quanto à obrigatoriedade de designar formalmente comitês de TI foi o CNJ (a obrigação criada pela SLTI/MP por meio da IN – SLTI 4/2008 foi extinta com a publicação da nova versão da norma, a IN – SLTI 4/2010), e, mesmo assim, observou-se que um auditado do Poder Judiciário ainda não tinha dado cumprimento à orientação da Resolução 90/2009-CNJ, art. 12, sendo, diante do cenário evidenciado, oportuna e conveniente a atuação dos demais OGS.

Registre-se, por oportuno, que há um documento de autoria da SLTI/MP que trata de ‘Diretrizes do Sisp para criação de comitês de TI’ (disponível em [http://www.sisp.gov.br/dotlrn/clubs/gestodetisp/file-storage/index?folder\\_id=13084935](http://www.sisp.gov.br/dotlrn/clubs/gestodetisp/file-storage/index?folder_id=13084935)), que pode ser utilizado como base para atuação dos OGS.

A consequência da ausência de comitês de TI ou comitês instituídos, mas não atuantes, pode ser evidenciada no relatório de auditoria do TC 029.120/2010-1. Naqueles autos foi registrado que a ausência de reuniões do comitê inviabilizou a apreciação de produtos de um contrato, tornando o prosseguimento da execução do contrato parcialmente inviável, visto que a apreciação dos produtos era competência do comitê (anexo 2, fl. 209, itens 398-400). Está em apuração a responsabilidade do presidente do comitê por omissão na convocação das reuniões, assim como possível dano decorrente de tal omissão.

Destarte, propõe-se recomendar à SLTI/MP que normatize a obrigatoriedade de que os entes sob sua jurisdição estabeleçam comitês de TI, observando as boas práticas sobre o tema, a exemplo do Cobit 4.1, PO4.2 – comitê estratégico de TI e PO4.3 – comitê diretor de TI (subitem 0).

Recomendação análoga deve ser proposta ao CNMP e à CGPAR.

Quanto às deficiências do quadro de servidores nos setores de TI, exemplificam-se a seguir dois casos que evidenciam o tipo de risco a que a organização fica exposta em tais situações:

fundamentação de contratação produzida (e assinada) por funcionário de empresa contratada (anexo 2, fl. 38v), isto é, um particular justificando a execução de despesa com recursos públicos;

funcionário de empresa contratada mantendo relação de subordinação direta com servidor público e executando atividade de fiscalização do contrato no qual a empresa contratada é seu próprio empregador (anexo 2, fl. 141).

A mitigação desses riscos passa pelo preenchimento das funções sensíveis dos setores de TI com servidores públicos, o que não prescinde de prévia avaliação formal da adequação (quantitativa e qualitativa) do quadro de pessoal desses setores, de forma que se propõe recomendar ao MP que oriente os órgãos e entidades sob sua jurisdição a realizar avaliação quantitativa e qualitativa do pessoal do setor de TI, de forma a delimitar as necessidades de recursos humanos para que estes setores realizem a gestão das atividades de TI da organização (subitem 0).

Recomendação análoga deve ser proposta ao CNJ, ao CNMP e à CGPAR.

Em outra linha de análise, trazemos excerto do relatório do Acórdão 2.308/2010-TCU-Plenário, que trata da forma de seleção dos dirigentes de TI das organizações pesquisadas (anexo 2, fl. 5):

‘58. Observa-se que 76% das instituições respondentes indicaram que seu dirigente máximo de TI tem experiência em gestão de TI. Portanto, em 24% das instituições respondentes o dirigente máximo supostamente não tem a experiência necessária em gestão de TI, o que é preocupante.

59. Também deve ser ressaltado que, em relação à formação acadêmica dos dirigentes de TI:  
– a frequência de cursos superiores fora da área de TI é maior que na área de TI;  
– a frequência de cursos de pós-graduação (lato ou stricto sensu) fora da área de gestão e governança de TI é menor que a de cursos técnicos de TI ou a de cursos fora da área de TI;

60. Estes números reforçam a impressão de que ainda é muito baixo o investimento das instituições na preparação de gestores de TI para efetivamente gerenciar a TI institucional, especialmente em contextos de alto requerimento de governança corporativa e de TI.’

Considerando a materialidade dos recursos despendidos com TI no Governo Federal (da ordem de R\$ 18,1 bilhões), a condição estratégica da TI nas organizações públicas (ver item 0) e o fato de que as lideranças são fator crítico de sucesso nos processos de governança e gestão (Acórdão 2.308/2011-TCU-Plenário), é recomendável disciplinar o acesso às funções de direção dos setores de TI com base em competências técnicas e gerenciais preestabelecidas.

Nesse sentido, propõe-se recomendar ao MP que, em atenção ao Decreto 5.707/2006, art. 5º, § 2º, c/c o art. 1º, III, discipline a forma de acesso às funções de liderança nos setores de Tecnologia da Informação, considerando as competências multidisciplinares necessárias para estas funções, que incluem, mas não se limitam a conhecimentos em TI (subitem 0).

Recomendação análoga deve ser proposta ao CNJ, ao CNMP e à CGPAR.

A título de contribuição, cita-se o estudo ‘Gestão e Desenvolvimento de Competências Gerenciais Relacionadas à Tecnologia da Informação’, disponível em [http://portal2.tcu.gov.br/portal/page/portal/TCU/comunidades/trabalhos\\_academicos\\_TCU/biblioteca\\_digital/gestao\\_e\\_desenvolvimento\\_de\\_competencias\\_gerenciais\\_rela.pdf](http://portal2.tcu.gov.br/portal/page/portal/TCU/comunidades/trabalhos_academicos_TCU/biblioteca_digital/gestao_e_desenvolvimento_de_competencias_gerenciais_rela.pdf), que pode ser útil no disciplinamento recomendado.

#### Orçamentação de TI

Com relação ao processo orçamentário de TI, espera-se que os entes elaborem suas propostas (planejamento do orçamento) com base nas ações que efetivamente pretendem realizar, alinhadas aos objetivos de negócio (Cobit 4.1, PO5.3), e que mantenham o acompanhamento da sua execução, de forma a saber precisamente quanto foi gasto onde e qual a disponibilidade para gastos futuros (Cobit 4.1, PO5.4).

O Quadro 6 apresenta o resultado obtido na avaliação in loco, no qual se evidencia que em dez dos treze jurisdicionados auditados foram registradas desconformidades (como no Dnocs não havia contrato em vigor, este item não foi avaliado na autarquia).

Quadro 6 – Orçamentação de TI (achados)

Possíveis achados	Dnit	SE/MS	SE/MCT	Ibama	Susep	TRT-SP	Dnocs	SE/MRE	TRT-RS	Anatel	Finep	SE/MP	ADE	ENDE
Inexistência de orçamento de TI na LOA														
Falhas no orçamento de TI constante da LOA	X	X	X	X		X		X						X
Inexistência de controle da execução do orçamento de TI					X						X			
Falhas no controle da execução do orçamento de TI			X			X								

Observa-se no Quadro 6 a existência de ente público sem previsão de orçamento para TI na LOA, o que, no mínimo, é inquietante ante a notória dependência de TI de todas as organizações. Compulsando os dados oferecidos pela SOF/MP no levantamento de auditoria (TC 001.484/2010-9), trabalho da fase preparatória deste TMS, identificaram-se dezenas de órgãos e entidades sem previsão de gastos com TI, o que se pode evidenciar também pela análise do Quadro 17 da LOA 2010 (Lei 12.214/2010). Cite-se, por exemplo, que apenas 22 dos 27 TRT aparecem no mencionado quadro, mas todos os 27 executaram despesas com TI no exercício de 2010.

Considerando o exposto no parágrafo anterior, propõe-se recomendar à SOF/MP que implante controles para mitigar os riscos de ocorrência de propostas orçamentárias que indevidamente não tenham previsão de despesas com tecnologia da informação (subitem 0).

Analizando de outro ponto de vista, os dados constantes do Apêndice 0 (linha D da tabela) evidenciam que houve cinco situações em que as evidências apresentadas às equipes do TCU não corroboram as respostas apresentadas à pergunta ‘A solicitação do orçamento de TI é feita com base nas estimativas de custos das contratações previstas?’, sugerindo que a melhoria identificada no Acórdão 2.308/2010-TCU-Plenário (anexo 2, fl. 7, itens 118 e 119) pode não ser real e que é maior do que 16% o percentual de pesquisados que não elabora sua proposta orçamentária de TI com base nas atividades que pretende executar.

No mesmo sentido, ainda compulsando os dados constantes do Apêndice 0 (linha E da tabela), evidenciou-se que em três situações as evidências apresentadas às equipes do TCU não corroboram as respostas apresentadas à pergunta ‘Ao longo do exercício financeiro há controle dos gastos efetuados especificamente com TI?’, sugerindo que é menor que 88% o percentual de pesquisados que controla os gastos com TI (anexo 2, fl. 7v, item 120).

No monitoramento realizado (TC 028.772/2010-5; Acórdão 1.145/2011-TCU-Plenário), identificou-se que o único OGS a orientar seus jurisdicionados quanto à necessidade de que as propostas orçamentárias para as áreas de TI fossem elaboradas em função das atividades que se pretendessem realizar, alinhadas ao negócio da organização, foi o CNJ (anexo 2, fl. 188v, item II.4.7 e fl. 189v, item II.4.15), e, mesmo assim, observa-se no Quadro 6 que um auditado do Poder Judiciário ainda não tinha

dado cumprimento à orientação da Resolução 99/2009-CNJ, art. 2º, sendo, diante do cenário evidenciado, oportuna e conveniente a atuação dos OGS, em especial da SOF/MP, órgão central do sistema de planejamento e de orçamento federal (Lei 10.180/2001).

Ante o exposto, propõe-se recomendar à SOF/MP que, com base no disposto na Lei 10.180/2001, art. 8º, II, c/c Decreto 7.063/2010, art. 17, II, normatize a obrigatoriedade de que todos os entes sob sua jurisdição estabeleçam processo de trabalho formal para elaboração e acompanhamento da execução do orçamento, contemplando, pelo menos, a obrigatoriedade de que:

a solicitação do orçamento de TI seja feita com base nas estimativas de custos das atividades que pretendam executar, alinhadas aos objetivos do negócio da organização (subitem 0);

haja acompanhamento, ao longo do exercício financeiro, dos gastos efetuados especificamente com TI (subitem 0).

Outro aspecto a ser observado diz respeito à atuação dos OGS, decorrente do Acórdão 371/2008-TCU-Plenário, para a identificação do orçamento de TI dos entes da APF. O monitoramento realizado (TC 028.772/2010-5; Acórdão 1.145/2011-TCU-Plenário) identificou as seguintes vulnerabilidades na solução implantada pela SOF/MP (anexo 2, fl. 187):

a) risco de inconsistência de dados: da forma como implantado, o processo de coleta de informações permite o cadastramento de rubricas inexistentes ou que não sejam específicas de TI. Os dados enviados em 2010 pela SOF, por meio do Ofício 06/SECAD/SOF/MP, de 25/2/2010, permitem identificar diversas ocorrências dessa natureza (peça 29);

b) risco de não coleta da informação: da forma como implantado, a obtenção das informações de previsão de gastos de TI depende de anualmente inserir-se comando específico na LDO que regerá a elaboração do orçamento. No ano em que a SOF por algum motivo não fizer incluir dito comando na LDO, as informações não serão geradas. Tal fato ocorre pelo fato de o processo de trabalho implantado pela SOF não estar documentado (ou seja, não se encontra no nível de maturidade 3 – definido), o que enseja necessidade de implantação de controles para garantir que o processo ocorra todos os anos. Tais fatos deverão ser levados em consideração quando da consolidação do TMS 6 – Gestão e uso de TI.

Em seguida, o monitoramento conclui pela possibilidade de ‘haver necessidade de implantar controles para mitigar o risco de inconsistência e de descontinuidade no envio das informações ao TCU, o que será levado em consideração quando da consolidação do TMS 6 – Gestão e uso de TI’ (anexo 2, fl. 187, item 58).

Considerando as vulnerabilidades supra, propõe-se determinar à SOF/MP que, em atenção ao Decreto-Lei 200/1967, art. 75, encaminhe, à Secretaria de Fiscalização de Tecnologia da Informação do Tribunal de Contas da União (Sefti/TCU):

no prazo de quinze dias após o envio do projeto da Lei de Diretrizes Orçamentárias ao Congresso Nacional, as medidas adotadas para permitir a identificação clara, objetiva e transparente da previsão dos gastos em TI no Orçamento Geral da União ou, alternativamente, normatize o processo de trabalho para obtenção de ditas informações, valendo-se da competência prevista no Decreto 7.063/2010, art. 17, II (subitem 0).

Em outra linha, por meio do item 9.4.3 do Acórdão 2.308/2010-TCU-Plenário, o TCU determinou à Sefti que:

9.4.3. defina e mantenha processo de trabalho permanente e sustentável de acompanhamento da governança de tecnologia da informação na administração pública federal, de modo a subsidiar processos de fiscalização do TCU em TI e processos de planejamento e controle das unidades jurisdicionadas a esta Corte, com definição, se possível, de periodicidade regular para realização de levantamentos gerais como o ora examinado e de mecanismos para coleta de evidências destinadas a aumentar a confiabilidade das informações colhidas mediante questionários;

Um dos mecanismos necessários para coletar evidências consiste na obtenção das informações orçamentárias (dotação e execução orçamentária) dos jurisdicionados.

Por meio do Siafi Gerencial, é possível à Sefti/TCU obter os dados da execução orçamentária da despesa de TI, uma vez que, conforme relatado no monitoramento (anexo 2, fl. 187, item

59), estão estabelecidas contas contábeis para liquidação dessas despesas no MANUAL SIAFI WEB, Seção 021100 ('Outros Procedimentos'), Macrofunção 021130 ('DESPESAS COM TI').

Já para as informações sobre a dotação orçamentária, esta Secretaria tem tido acesso às informações por meio de solicitações sob demanda, como ocorreu com as informações encaminhadas por meio do Ofício 6/Secad/SOF/MP, de 23/2/2010, durante a fase de preparação do TMS (TC 001.484/2010-9). Assim, como forma de sistematizar o recebimento pelo TCU das informações orçamentárias de TI, propõem-se as determinações a seguir.

Determinar à SOF/MP que, em atenção ao Decreto-Lei 200/1967, art. 75, encaminhe, à Secretaria de Fiscalização de Tecnologia da Informação do Tribunal de Contas da União (Sefiti/TCU):

no prazo de quinze dias após o envio do Projeto da Lei Orçamentária Anual (PLOA) ao Congresso Nacional, relação da previsão das despesas com TI que constam do PLOA, em meio magnético, na forma de banco de dados editável ou planilha eletrônica, no maior detalhamento possível, preferencialmente no formato encaminhado por meio do Ofício 06/SECAD/SOF/MP, de 25/2/2010, ou, alternativamente, disponibilize funcionalidade nos seus sistemas informatizados para que a Sefiti/TCU possa acessar os dados requeridos para o atendimento da determinação (subitem 0);

no prazo de quinze dias após a publicação da Lei Orçamentária Anual (LOA), relação da previsão das despesas com TI que constam da LOA, em meio magnético, na forma de banco de dados editável ou planilha eletrônica, no maior detalhamento possível, preferencialmente no formato encaminhado por meio do Ofício 06/SECAD/SOF/MP, de 25/2/2010, ou, alternativamente, disponibilize funcionalidade nos seus sistemas informatizados para que a Sefiti/TCU possa acessar os dados requeridos para o atendimento da determinação (subitem 0);

Determinação análoga deve ser dirigida ao Dest/MP.

Processo de software

Constam da ABNT NBR ISO/IEC 12.207 as seguintes definições:

4.25 processo – conjunto de atividades que se relacionam ou interagem e que transformam entradas em saídas [ABNT NBR ISO 9000:2005].

(...)

4.28 produto – resultado de um processo [ABNT NBR ISO 9000:2005].

(...)

4.42 produto de software – conjunto de programas de computador, procedimentos e possíveis documentação e dados associados.

Um processo de software é, portanto, um conjunto de atividades que transformam requisitos de usuários (entrada do processo) em um produto de software. Por oportuno, chamamos a atenção para o fato de que o produto de software não é composto apenas dos programas de computadores, mas inclui outros itens. Mais ainda, destacamos que os diversos itens que compõem o produto de software são gerados ao longo da execução do processo de software.

Diante dos conceitos apresentados, tem-se que, na contratação de serviços de desenvolvimento ou manutenção de software, é exatamente o processo de software que define o serviço objeto do contrato.

Sendo assim, a definição do processo de software e sua vinculação ao edital e ao contrato é condição necessária para a definição precisa do objeto, nos termos previstos na Lei 8.666/1993, art. 6º, IX. Nessa esteira, há diversos precedentes de julgados do TCU, como, por exemplo:

Acórdão 953/2009-TCU-Plenário:

(...)

1.5. Determinar ao Ministério da Defesa que, nas contratações de serviços de Tecnologia da Informação, em especial no caso de elaboração e publicação de novo edital de licitação em substituição ao Edital da Concorrência nº 03/2008:

(...)

1.5.2. em atenção ao art. 6º, inciso IX, da Lei nº 8.666/93, defina formalmente um processo de desenvolvimento de software, previamente à contratação de serviços de desenvolvimento ou manutenção de software, conforme preconiza o item PO 8.3 do Cobit 4.1 e em consonância com os

Acórdãos 2.023/2005-Plenário, item 9.1.5 e 436/2008-Plenário, item 9.1.5, vinculando o contrato com o processo de desenvolvimento de software, sem o qual o objeto não estará precisamente definido;

Acórdão 71/2007-TCU- Plenário:

(...)

9.2. determinar, com fulcro no art. 43, inciso I, da Lei nº 8.443, de 16 de julho de 1992 c/c o art. 250, inciso II, do Regimento Interno do TCU, à Secretaria Nacional de Segurança Pública do Ministério da Justiça – Senasp/MJ que:

(...)

9.2.9. defina formalmente padrões para desenvolvimento de sistemas no âmbito do Infoseg, à semelhança das orientações contidas no item PO8.3 do COBIT 4.0;

Acórdão 2.023/2005 – Plenário: 9.1. determinar à Secretaria Executiva do Ministério do Trabalho e Emprego que:

(...)

9.1.5. estabeleça e divulgue uma metodologia para desenvolvimento de sistemas (novos e legados), indique seus artefatos e produtos e detalhe seus requisitos mínimos, conforme preconiza o item PO 11.5 do Cobit (item 2.3 do relatório de auditoria); entre outros objetivos, essa metodologia deve regulamentar o desenvolvimento e a manutenção de sistemas pelas outras coordenações e unidades descentralizadas do Ministério, de modo a assegurar níveis mínimos de padronização e segurança dos mesmos (item 2.8 do relatório de auditoria);

Registre-se ainda que um dos processos do ciclo de vida de software descrito na ABNT NBR ISO/IEC 20.207 é o processo de aquisição de software.

Ainda que a organização não contrate serviços dessa natureza, mas sim execute o desenvolvimento e manutenção de software com pessoal próprio (que não é o caso da maioria das organizações públicas), a definição do processo de software utilizado na organização é um controle geral de TI que apoia a qualidade do software produzido, sendo boa prática seu estabelecimento formal.

Para a definição dos processos de software, as organizações podem utilizar-se das normas brasileiras ABNT ISO/IEC 12.207 e 15.504, além de modelos comerciais, como o CMMI e o MPS.BR, este último criado e mantido pela Softex com recursos públicos federais.

Nesse contexto, a quinta questão de auditoria da FOC buscou evidenciar se ‘Há processo de software estabelecido no Unidade?’. O Quadro 7 sumariza os resultados, em que se observa que a totalidade dos auditados avaliados tem problemas, sendo que a maioria deles (dez) não possuíam processo de software.

Os dados constantes do Apêndice 0 (linha F da tabela) evidenciam que, apesar de haver situações em que as evidências apresentadas às equipes do TCU não corroboram as respostas apresentadas à pergunta ‘Há processo de software?’, os resultados discrepantes não sugerem alteração no resultado constante do Acórdão 2.308/2010-TCU-Plenário (anexo 2, fl. 6, item 2.4.2), de que mais da metade das organizações não possuem processo de software, e, consequentemente, quando contratam serviços de desenvolvimento ou manutenção de software, fazem-no de forma ilegal, em virtude de indefinição de objeto.

Quadro 7 – Processo de software (achados)

Possíveis achados	Dnit	SE/MS	SE/MCT	Ibama	Susep	TRT-SP	Dnocs	SE/MRE	TRT-RS	Anatel	Finep	SE/MP	ADE	FNDE
Inexistência de processo de software	X			X	X	X	X		X		X	X	X	(3 )
Falhas no processo de software		X						X		X				

(3) Controle formalizado ao final da fase de execução da auditoria, de forma que não foi avaliado.

No monitoramento realizado (TC 028.772/2010-5; Acórdão 1.145/2011-TCU-Plenário), identificou-se que os OGS não lograram orientar seus jurisdicionados quanto à necessidade de

estabelecimento de processo de software (anexo 2, fl. 188, item II.4.4 e fl. 189v, item II.4.13), sendo, diante do cenário evidenciado, oportuna e conveniente a atuação dos OGS.

As consequências da inexistência de processo de software vinculado ao edital e contrato são diversas, das quais ressaltamos os seguintes dois riscos:

divergência de expectativas entre as partes contratantes, visto que o contratado pode entender que deve executar um processo de software mais simples (e mais barato), gerando, portanto, menos componentes do software (e.g., somente códigos-fonte e executável), enquanto o contratante entende que devem ser gerados mais componentes de software (e.g., documentos de análise e projeto, códigos-fonte e executável, casos de testes, manuais de usuário), o que pode inviabilizar a execução do contrato;

contratação por valor acima do mercado, pois sem a definição do processo de software não há como estimar o preço do serviço de forma aceitável.

O processo de software é controle que mitiga riscos de que o software desenvolvido ou adquirido tenha baixa qualidade, contribuindo para que não ocorram situações como a relatada no TC 010.474/2010-2, em que foi evidenciado que o Sistema de Acompanhamento de Contratos do Dnit (Siac), sistema crítico para a Autarquia, capaz de parar imediatamente o seu negócio (anexo 2, fl. 212, item 9), não possuía dicionário de dados (anexo 2, fl. 221, achado 3.3), a despeito de manipular mais de uma centena de tabelas, com milhares de campos no total. A ausência de dicionário de dados decerto contribuirá de forma negativa no caso de necessidade de manutenções no sistema, quando, não raro, os técnicos necessitam consultar esse artefato para efetuar dita manutenção.

A título exemplificativo, citamos a boa prática identificada por ocasião de auditoria realizada no BNB, apreciada por meio do Acórdão 193/2009-TCU-Plenário, no qual foi registrado que o Banco definiu processo de software, vinculou o contrato de desenvolvimento e manutenção de software ao processo e praticou adequada gestão contratual, utilizando-se dos critérios definidos em seu processo de software para aferir os produtos entregues ao longo da execução contratual.

Outro exemplo de consequência possível ante a ausência desse controle geral de TI foi observado no Ministério da Saúde, o que contribuiu para a existência de software com inconsistências entre as regras utilizadas no sistema informatizado (SIG) que apoia o Sistema Nacional de Transplantes (SNT) e as regras definidas pelos normativos que regem o SNT, nos termos relatados no TC 029.074/2010-0 (anexo 2, fl. 254, item 2.14.5):

225. Embora não tendo acesso à base de dados do sistema conforme requerido pela equipe de auditoria, foi possível identificar, especialmente na ocasião das visitas às CNCDO, algumas inconsistências entre as regras utilizadas pelo SIG e as regras definidas pelo Regulamento Técnico do SNT (Portaria – MS 2.600/2009).

226. As inconsistências identificadas referem-se, em suma, aos seguintes fatos:

- a) não consideração de situações especiais na pontuação atribuída a receptores (em casos bem específicos);
- b) falta de acesso dos receptores a informações de seus prontuários;
- c) permissões indevidas de acesso e alteração de informações do receptor por não membro de equipe especializada;
- d) permissão indevida de inserção de um receptor em situação especial pela equipe especializada;
- e) critério de desempate incorreto para pontuação de potenciais receptores em situação especial.

227. Registre-se que a ausência de um processo de software padronizado no Datasus (Acórdão 757/2011-TCU-Plenário, item 9.2.4) contribui para que as regras de negócio estejam implementadas de forma desconforme com as previsões da Portaria-MS 2.600/2009, pois, por exemplo, a prática da disciplina de gestão de requisitos aliada a um processo de homologação adequado mitigaria os riscos de erros como relatados neste achado.

Para avaliar a gravidade da situação descrita, o TC 029.074/2010-0 registrou ainda que as inconsistências identificadas podem ter como consequência a alteração indevida de posições na lista de

receptores de órgãos para transplantes (anexo 2, fl. 254, item 2.14.3), podendo acarretar, em último caso, a morte indevida de um cidadão.

Diante desse cenário, entende-se necessário que os OGS elaborem modelos de processo de software para seus jurisdicionados, bem como estabeleçam a obrigatoriedade de que os jurisdicionados adotem formalmente um processo de software para si, que pode ser o próprio modelo criado pelo OGS, ou outro, motivo pelo qual se propõe recomendar à SLTI/MP que:

elabore um modelo de processo de software para a os entes sob sua jurisdição, observando as boas práticas sobre o tema (e.g., NBR ISO/IEC 12.207 e 15.504, MPS.BR, CMMI); subitem 0);

estabeleça a obrigatoriedade de que os entes sob sua jurisdição formalizem um processo de software para si, observando as boas práticas sobre o tema (e.g., NBR ISO/IEC 12.207 e 15.504, MPS.BR, CMMI; subitem 0).

Recomendação análoga deve ser proposta ao CNJ, ao CNMP e à CGPAR.

Ademais, propõe-se determinar à SLTI/MP que, em atenção ao previsto no Decreto 7.579/2011, art. 4º, V, oriente os entes sob sua jurisdição sobre necessidade de vincular seus contratos de serviços de desenvolvimento ou manutenção de software a um processo de software, pois, sem esta vinculação, o objeto do contrato não estará precisamente definido, em desconformidade com o disposto na Lei 8.666/1993, art. 6º, inciso IX (subitem 0).

Determinação análoga deve ser proposta ao CNJ, ao CNMP e à CGPAR.

#### Processo de gerenciamento de projetos

A sexta questão de auditoria da FOC buscou avaliar se ‘Há processo de gerenciamento de projetos de TI estabelecido no Unidade?’, e os resultados da avaliação in loco constam do **Error! Reference source not found.** Erro! Fonte de referência não encontrada..

A observação do quadro supra permite identificar que a definição de uma estrutura para gerenciamento de projetos não é prática dos auditados, ainda que seja razoável supor que todos eles conduzem projetos de tecnologia da informação.

Por meio do Acórdão 2.308/2010-TCU-Plenário (anexo 2, fl. 18, questão 7.4), obteve-se a informação de que pelo menos 69% dos pesquisados não adotam um padrão para o gerenciamento de projetos de TI. Analisando os dados constantes do Apêndice 0 (linha G da tabela), foi evidenciado que houve duas situações em que as evidências apresentadas às equipes do TCU não corroboraram as respostas apresentadas à pergunta 7.4 do perfil GovTI2010, sugerindo que o percentual de entes da APF que não possuem estrutura de gerenciamento de projetos de TI pode ser ainda maior.

A consequência da ausência ou da deficiência de uma estrutura de gerenciamento de projetos de TI pode ser observada da leitura do excerto abaixo (TC 029.074/2010-0), que identificou falhas na implantação do SIG, sistema informatizado que dá suporte ao SNT (anexo 2, fl. 254v, item 2.15.6):

239. A Central Nacional de Transplantes (CNT) é a unidade do SNT que possui a atribuição de efetuar a distribuição de órgãos em âmbito nacional, no caso de não utilização no estado onde o órgão foi doado, além de outras atribuições relacionadas à coordenação de logística e à distribuição de órgãos e tecidos no processo de doação/transplante em âmbito nacional.

240. Para que a CNT pudesse atender a tal atribuição e contar com as novas facilidades que o Sistema Informatizado de Gerenciamento (SIG) oferece, seria determinante a utilização do sistema por todas as centrais estaduais de transplantes (CNCDO), e também pela própria Central Nacional.

241. Contudo, em função da implantação paulatina e parcial do SIG nos estados, aliada a não implantação e uso do módulo a ser utilizado pela CNT, houve limitações técnicas para que a Central Nacional pudesse atender plenamente às regras do negócio do SNT, as quais somente serão sanadas com a utilização do novo sistema por todos os estados e pela própria CNT.

242. Registre-se que falhas no processo de gerenciamento de projetos, tais como as identificadas no âmbito da auditoria de controles gerais de TI do Ministério da Saúde (TC 013.718/2010-0, Acórdão 757/2011-TCU-Plenário, item 9.1.4), contribuíram para a ocorrência das falhas relatadas neste achado.

Quadro 8 – Processo de gerenciamento de projetos (achados)

Possíveis achados	Dnit	SE/MS	SE/MCT	Ibama	Susep	TRT-SP	Dnocs	SE/MRE	TRT-RS	Anatel	Finep	SE/MP	ADE	FNDE
Inexistência de processo de gerenciamento de projetos	X													(3)
Falhas no processo de gerenciamento de projetos	X													

(3) Controle formalizado ao final da fase de execução da auditoria

Quanto a esse tema, os acórdãos estruturantes monitorados (TC 028.772/2010-5; Acórdão 1.145/2011-TCU-Plenário) não expediram orientação específica e, diante do cenário evidenciado, entende-se oportuna e conveniente a atuação dos OGS, de forma que se propõe recomendar à SLTI/MP que:

elabore um modelo de estrutura de gerenciamento de projetos para os entes sob sua jurisdição, observando as boas práticas sobre o tema (e.g., PMBoK; subitem 0);

estabeleça a obrigatoriedade de que os entes sob sua jurisdição formalizem um processo de gerenciamento de projetos para si, observando as boas práticas sobre o tema (e.g., PMBoK; subitem 0).

Recomendação análoga deve ser proposta ao CNJ, ao CNMP e à CGPAR.

#### Processos de gestão de serviços

A sétima questão de auditoria da FOC buscou verificar se ‘Há processos de gestão de serviços de TI que apoiam o Unidade na administração da qualidade dos serviços de TI?’. Nesse tema foram avaliados três processos, cujos objetivos, segundo a NBR ISO/IEC 20.000, são:

gestão de configuração – ‘definir e controlar os componentes do serviço e infraestrutura e manter informação precisa da configuração’, processo cuja importância reside em manter uma base de dados de itens de configuração do ambiente de TI, chamada CMDB (Configuration Management DataBase), que é a base para o funcionamento dos demais processos de gestão de serviços;

gestão de incidentes – ‘restaurar o mais rápido possível os serviços acordados com a organização, ou responder às requisições dos serviços’, ou seja, processo cuja importância está ligada ao fato de que é por meio dele que é restaurado diretamente o fornecimento de serviços dos quais dependem os usuários finais;

gestão de mudanças – ‘assegurar que todas as mudanças sejam avaliadas, aprovadas, implementadas e revisadas de maneira controlada’, que é considerado o processo mais crítico no modelo preconizado pelo Cobit 4.1, pois é por meio dele que a consistência dos serviços com continuidade é mantida.

O Quadro 9 apresenta o resultado das avaliações in loco, e, por meio dele, é possível evidenciar que o tema gestão de serviços não encontra prioridade nos auditados.

Quadro 9 – Processos de gestão de serviços (achados)

Possíveis achados	Dnit	SE/MS	SE/MCT	Ibama	Susep	TRT-SP	Dnocs	SE/MRE	TRT-RS	Anatel	Finep	SE/MP	ADE	FNDE
Inexistência do processo de gestão de incidentes	X													
Falhas no processo de gestão de incidentes									X					
Inexistência do processo de gestão de configuração														
Falhas no processo de gestão de configuração														X
Inexistência do processo de gestão de mudanças														
Falhas no processo de gestão de mudanças														

No monitoramento realizado (TC 028.772/2010-5; Acórdão 1.145/2011-TCU-Plenário), identificou-se que os OGS promoveram algum tipo de orientação aos seus jurisdicionados quanto à necessidade de implantar e aperfeiçoar a gestão de níveis de serviço (anexo 2, fl. 188, item II.4.5 e fl.

189v, item II.4.14). Entretanto, o cenário evidenciado sugere que é oportuna e conveniente atuação mais contundente dos OGS, de forma que se propõe recomendar à SLTI/MP que:

elabore um modelo de processo de gestão de serviços para os entes sob sua jurisdição que inclua, pelo menos, gestão de configuração, gestão de incidentes e gestão de mudança, observando as boas práticas sobre o tema (e.g., NBR ISO/IEC 20.000, Itil; subitem 0);

estabeleça a obrigatoriedade de que os entes sob sua jurisdição formalizem processos de gestão de serviços para si, incluindo, pelo menos, gestão de configuração, gestão de incidentes e gestão de mudança, observando as boas práticas sobre o tema (e.g., NBR ISO/IEC 20.000, Itil; subitem 0).

Recomendação análoga deve ser proposta ao CNJ, ao CNMP e à CGPAR.

#### Segurança da informação

No tema segurança da informação, foram feitas avaliações nos seguintes temas:

existência de responsável pela segurança da informação;

funcionamento do comitê de segurança da informação;

política de segurança da informação;

equipe de tratamento e resposta a incidentes em redes computacionais;

inventário de ativos de informação;

classificação da informação;

gestão de riscos de segurança da informação.

Registre-se que esses controles gerais de TI estão positivados em normas complementares do GSI/PR e na IN – GSI/PR 1/2008.

O Quadro 10 resume a situação encontrada na avaliação realizada in loco, cenário esperado ante os resultados constantes do Acórdão 2.308/2010-TCU-Plenário.

Quadro 10 – Segurança da informação (achados)

Possíveis achados	Dnit	SE/MS	SE/MCT	Ibama	Susep	TRT-SP	Dnocs	SE/MRE	TRT-RS	Anatel	Finep	SE/MP	ADE	FNDE
Inexistência de gestor de segurança da informação e comunicações	X	X	X	X	X	X	X	X				X	X	X
Inexistência de comitê de segurança da informação e comunicações	X	X		X	X	X	X	X				X		
Falhas no comitê de segurança da informação e comunicações			X											X
Inexistência de Política de Segurança da Informação e Comunicações (Posic)		X	X	X	X	X	X	X						
Falhas na Política de Segurança da Informação e Comunicações (Posic).								X			X		X	
Inexistência de Equipe de Tratamento e Resposta a Incidentes em redes computacionais (Etri).	X	X	X	X	X	X	X	X	X					
Falhas na Equipe de Tratamento e Resposta a Incidentes em redes computacionais (Etri)											X		X	
Inexistência de classificação da informação	X	X	X	X	X	X	X	X		X	X			
Não classificação de informações conforme níveis de segurança														X
Inexistência de inventário dos ativos de informação	X	X	X	X	X	X	X				X	X	X	X
Falhas no inventário dos ativos de informação								X	X		X			
Inexistência de processo de Gestão de Riscos de Segurança da Informação (GRSIC)	X	X	X	X	X	X	X	X		X	X	X	X	X
Falhas no processo de Gestão de Riscos de Segurança da Informação (GRSIC).														

Os dados coletados por meio do trabalho que culminou no Acórdão 2.308/2010-TCU-Plenário permitiram sinalizar que a situação da segurança da informação na APF era crítica, nos seguintes termos (anexo 2, fl. 5-5v):

64. A Figura 7 apresenta os resultados obtidos em 2010 comparados aos obtidos em 2007. Observe-se que, neste caso, o gráfico apresentado refere-se à ausência das práticas recomendadas, para compatibilizar melhor com a maneira como essa informação foi apresentada em 2007.

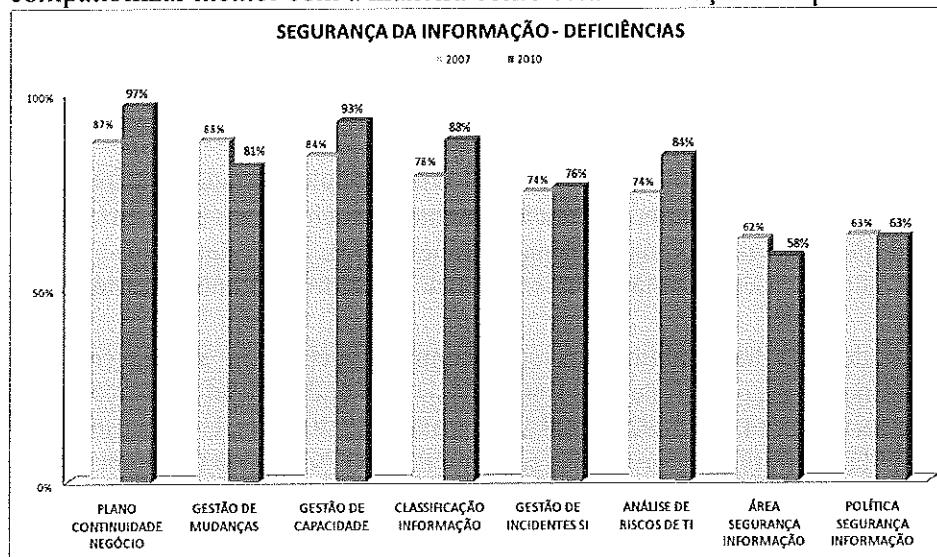


Figura 1 – Indicadores de deficiências em segurança da informação (fonte: Acórdão 2.308/2010-TCU-Plenário)

(...)

69. Percebe-se que, em todos os casos, não houve melhora nos processos que tratam de segurança da informação na APF. Ou seja, se em 2007 a situação já se mostrava preocupante, atualmente é ainda pior, uma vez que o alarme foi soado por meio do Acórdão nº 1.603/2008-TCU-Plenário e, um ano e meio depois, o quadro não apresenta evidências de melhora.

70. Se em 2007 havia o entendimento de que a maior parte das instituições estava exposta a riscos diversos e não mapeados, hoje, além de a Administração estar exposta aos mesmos riscos, não está agindo para saneá-los com a agilidade que o caso requer.

Analizando os dados constantes do Apêndice 0 (linhas K até P da tabela), foi evidenciado que houve doze situações em que as evidências apresentadas às equipes do TCU não corroboraram as respostas apresentadas às perguntas do perfil GovTI2010 no tema segurança da informação, sugerindo que a situação com respeito à segurança da informação, que foi declarada como muito ruim, pode ser de fato ainda pior.

No monitoramento realizado (TC 028.772/2010-5; Acórdão 1.145/2011-TCU-Plenário), identificou-se que o GSI/PR implementou as recomendações propostas pelo TCU (anexo 2, fl. 188v, item II.4.9 e fl. 192v, item II.6.10), publicando a Instrução Normativa – GSI/PR 1/2008 e mais nove normas complementares até 2010, o que consiste em um arcabouço normativo considerável sobre o tema. O mesmo trabalho apontou algumas iniciativas do CNJ nesse tema e nenhuma iniciativa concreta do CNMP (anexo 2, fl. 188, item II.4.3 e fl. 192v, item II.6.10).

A despeito da atuação do GSI/PR e do CNJ, a situação encontrada no conjunto de trabalhos evidencia que a informação na APF continua exposta a riscos de segurança em larga medida, o que justifica proposta de aperfeiçoamento da atuação dos OGS.

Como consequências da ausência dos controles gerais de TI no tema segurança da informação, ou sua implantação de forma desconforme ao preconizado pelas normas e pelas boas práticas, citam-se os seguintes casos:

no Ministério da Saúde, onde não há nenhum dos sete controles gerais de segurança testados, os dados do sistema que suporta o Sistema Nacional de Transplantes (SNT), contendo informações sobre a intimidade de potenciais receptores de órgãos, podem ser alterados e consultados por usuários que, segundo o regulamento do SNT e a Constituição Federal, não deveriam poder fazê-los (anexo 2, fl. 250-250v, itens 119-120 e fl. 252v, item 183);

no Dnit, onde não há seis dos sete controles testados, não há política de controle de acesso nem procedimento para gerenciamento de usuário, o que contribui para a atribuição de perfis de usuários e realização de operações em desconformidade com as regras de segregação de funções e para a atribuição de perfis de usuários e realização de operações em desconformidade com os controles de acessos sensíveis (anexo 2, fl. 221v, item 360), que a seu turno contribuiu para fraudes consistindo no pagamento por serviços não prestados em uma de suas superintendências estaduais (Acórdão 2.766/2009-TCU-Plenário);

no MCT, onde não foram implantados seis dos sete controles testados e a implantação do comitê de segurança não foi seguida de seu efetivo funcionamento, evidenciou-se a terceirização (ilegal) de diversas atividades de gestão de segurança da informação (anexo 2, fl. 208v, item 396) e execução de despesa sem que houvesse efetivo aperfeiçoamento da segurança da informação no Ministério (anexo 2, fl. 209, item 406);

no Ibama, onde não há nenhum dos sete controles gerais de segurança testados, o compartilhamento de senhas no setor contábil da superintendência da Fundação em Goiás contribuiu para desvios praticados por uma servidora (TC 003.921/2008-9, Acórdão 458/2011-TCU-Plenário, item 9.4.3).

Ante oportunidade de atuação, propõe-se recomendar ao CNMP que (subitem 0):

estabeleça a obrigatoriedade de que os entes sob sua jurisdição implementem os seguintes controles gerais de TI relativos à segurança da informação:

nomeação de responsável pela segurança da informação na organização, à semelhança das orientações contidas na NBR ISO/IEC 27.002, item 6.1.3 – Atribuição de responsabilidade para segurança da informação;

criação de comitê para coordenar os assuntos de segurança da informação, à semelhança das orientações contidas na NBR ISO/IEC 27.002, item 6.1.2 – Coordenação de segurança da informação;

processo de gestão de riscos de segurança da informação, à semelhança das orientações contidas na NBR ISO/IEC 27005 – Gestão de riscos de segurança da informação;

estabelecimento de política de segurança da informação, à semelhança das orientações contidas na NBR ISO/IEC 27.002, item 5.1 – Política de segurança da informação;

processo de elaboração de inventário de ativos, à semelhança das orientações contidas na NBR ISO/IEC 27.002, item 7.1 – inventário de ativos;

processo de classificação da informação, à semelhança das orientações contidas na NBR ISO/IEC 27.002, item 7.2 – classificação da informação, processo necessário segundo o Decreto 4.553/2002, art. 6º, § 2º, inciso II e art. 67;

crie procedimentos para orientar os entes sob sua jurisdição na implementação dos controles acima.

Considerando a necessidade de os entes do Poder Judiciário serem orientados sobre como implantar os controles gerais de segurança da informação, propõe-se recomendar ao CNJ que crie procedimentos para orientar os entes sob sua jurisdição na implementação dos seguintes controles (subitem 0):

nomeação de responsável pela segurança da informação na organização, à semelhança das orientações contidas na NBR ISO/IEC 27.002, item 6.1.3 – Atribuição de responsabilidade para segurança da informação;

criação de comitê para coordenar os assuntos de segurança da informação, à semelhança das orientações contidas na NBR ISO/IEC 27.002, item 6.1.2 – Coordenação de segurança da informação;

processo de gestão de riscos de segurança da informação, à semelhança das orientações contidas na NBR ISO/IEC 27005 – Gestão de riscos de segurança da informação;

estabelecimento de política de segurança da informação, à semelhança das orientações contidas na NBR ISO/IEC 27.002, item 5.1 – Política de segurança da informação;

processo de elaboração de inventário de ativos, à semelhança das orientações contidas na NBR ISO/IEC 27.002, item 7.1 – inventário de ativos;

processo de classificação da informação, à semelhança das orientações contidas na NBR ISO/IEC 27.002, item 7.2 – classificação da informação, processo necessário segundo o Decreto 4.553/2002, art. 6º, § 2º, inciso II, e art. 67.

Com respeito à ausência de implantação dos controles positivados pelo GSI/PR por parte dos entes do Poder Executivo, propõe-se recomendar ao GSI/PR que:

em atenção à Lei 10.168/2003, art. 6º, IV, articule-se com as escolas de governo, notadamente com a Enap, a fim de ampliar a oferta de ações de capacitação em segurança da informação para os entes sob sua jurisdição (subitem 0);

em atenção à Lei 10.168/2003, art. 6º, IV, oriente os órgãos e entidades sob sua jurisdição que a implantação dos controles gerais de segurança da informação positivados nas normas do GSI/PR não é faculdade, mas obrigação da alta administração, e sua não implantação sem justificativa é passível da sanção prevista na Lei 8.443/1992, art. 58, II (subitem 0).

Deliberações análogas devem ser propostas ao CNJ e ao CNMP.

Por fim, ainda que a análise das normas expedidas pelos OGS não fizesse parte do escopo dos trabalhos planejados, após análise perfunctória, considera-se oportuno recomendar ao GSI/PR que reveja a Norma Complementar 4/IN01/DSIC/GSIPR, uma vez que aborda o tema considerando apenas ativo de informação e não ativo em sentido amplo, como o faz a NBR ISO/IEC 27.002 no item 7.1.1 (subitem 0).

#### Processo de capacitação em TI

A nona questão de auditoria da FOC ('Q9 – Há plano de capacitação de profissionais de TI que auxilie no desenvolvimento das competências necessárias para a boa execução dos trabalhos?') buscou avaliar se os auditados planejavam capacitação para seu pessoal e se nesse planejamento havia previsão de capacitação em gestão de TI (planejamento, coordenação, supervisão e controle). O resultado da avaliação in loco consta do Quadro 11, em que se observa que apenas um auditado planejou nos termos esperados:

Quadro 11 – Processo de capacitação de profissionais de TI (achados)

Possíveis achados	Dnit	SE/MS	SE/MCT	Ilama	Susep	TRT-SP	Dnocs	SEMRE	TRT-RS	Anatel	Finep	SE/MP	ADE	FNDE
Inexistência de plano anual de capacitação	X	X	X	X			X	X	X		X	X	X	
Plano anual de capacitação não contempla a área de gestão de TI					X	X				X				

Por meio do Acórdão 2.308/2010-TCU-Plenário (anexo 2, fl. 17 questão 6.3), obteve-se a informação de que pelo menos 45% dos pesquisados não têm critério para avaliação e atendimento aos pedidos de capacitação em gestão de TI. Analisando os dados constantes do Apêndice 0 (linha Q da tabela), foi evidenciado que houve seis situações em que as evidências apresentadas às equipes do TCU não corroboraram as respostas apresentadas à pergunta 6.3 do perfil GovTI2010, sugerindo que o percentual de entes da APF que não possuem tais critérios pode ser de fato ainda maior.

A Política e as Diretrizes para o Desenvolvimento de Pessoal da Administração Pública Federal direta, autárquica e fundacional estabelecem como diretriz: 'a capacitação gerencial do servidor e sua qualificação para o exercício de atividades de direção e assessoramento' (Decreto 5.707/2006, art. 3º, III).

Quanto a esse tema, os itens 9.1.2 e 9.4.2 do Acordão 1.603/2008-TCU-Plenário (anexo 2, fls. 187v-188, item II.4.2, e fls. 189-189v, item II.4.12) já haviam recomendado ao CNJ, ao CNMP e ao MP que tomassem providencias para garantir a quantidade e a capacitação adequadas do quadro de servidores em TI. O monitoramento dessas recomendações (TC 028.772/2010-5; Acórdão 1.145/2011-TCU-Plenário) concluiu ter havido atendimento parcial pelos dois primeiros OGS e total pelo último. Entretanto, as ausências e deficiências efetivamente encontradas nas auditorias in loco justificam uma

ação estruturante ainda mais abrangente que as anteriormente recomendadas, pelo que se propõe recomendar ao Comitê Gestor da Política Nacional de Desenvolvimento de Pessoal que, em atenção ao Decreto 5.707/2006, art. 7º, II e IV:

orientar os órgãos e entidades sob sua jurisdição sobre a obrigatoriedade de aprovar o plano anual de capacitação, nos termos do Decreto 5.707/2006, arts. 5º e 2º, c/c Portaria MP 208/2006, art. 2º, I, e art. 4º (subitem 0);

estabeleça, após consulta à Secretaria de Logística e Tecnologia da Informação, um programa de capacitação em governança e em gestão de tecnologia da informação (subitem 0).

Recomendação análoga deve ser proposta ao CNJ, ao CNMP e à CGPAR.

#### Processo de contratação e gestão de soluções de TI

As questões onze e doze das auditorias da FOC trataram dos processos de contratação e gestão contratual de soluções de TI, em que se buscou verificar:

se haviam controles que promovessem o cumprimento do processo de contratação previsto na IN – SLTI 4/2008 (vigente à época) ou outro processo que, no mínimo, promovesse a realização dos obrigatórios estudos técnicos preliminares (Lei 8.666/1993, art. 6º, IX) antes da elaboração do Termo de Referência ou Projeto Básico;

se o processo previsto na referida IN era cumprido, ou se os estudos técnicos preliminares eram realizados;

se havia desconformidade nas contratações;

se havia controles que promovessem a regular gestão contratual;

se havia conformidade na gestão contratual.

Registre-se que, ante a inexistência de contratos em vigor no Dnocs (anexo 2, fl. 109, item 1.5), a Autarquia não foi considerada na consolidação desse tema.

O Quadro 12 e o Quadro 13 sintetizam o resultado das avaliações in loco.

As teses prospectadas e confirmadas foram que:

a ausência de controles na contratação contribui para que o processo da IN – SLTI 4/2008 não seja cumprido ou os estudos técnicos preliminares não sejam realizados;

o descumprimento do processo da IN – SLTI 4/2008 ou a não realização dos estudos técnicos preliminares contribui para desconformidades nas contratações;

a ausência de controles na gestão contratual contribui para a sua desconformidade.

Sobre o tema, merece destaque a IN-SLTI/MP 4/2010 (sucessora da IN-SLTI/MP 4/2008), que instituiu processo de contratação de soluções de TI no âmbito do Sisp e que, se cumprida, tende a mitigar os riscos nas contratações de TI.

No monitoramento realizado (TC 028.772/2010-5; Acórdão 1.145/2011-TCU-Plenário), registrou-se (anexo 2, fl. 188v, item II.4.6) que o CNMP não realizou orientação quanto ao estabelecimento de processo de trabalho formal para contratações de TI e, quanto à atuação do CNJ, que:

116. (...) o fato de ainda não haver processo de trabalho para contratação de TI estabelecido no Poder Judiciário aliado ao fato de que a IN-SLTI/MP 04/2010 vem sendo reconhecida como uma boa prática (e.g., o governo do Distrito Federal formalmente adotou a IN como seu processo de contratação por meio do Decreto 32.218/2010), deve ser levado em consideração quando da consolidação do TMS 6 – Gestão e uso de TI.

Quadro 12 – Processo de contratação de bens e serviços de TI (achados)

Possíveis achados	Dnit	SE/MS	SE/MCT	Ibama	Susep	TRT-SP	SE/MRE	TRT-RS	Anatel	Finep	SE/MP	ADE	FNDE
Inexistência de controles que promovam o cumprimento da IN 4													
Falhas nos controles que promovam o cumprimento da IN 4		X								X			
Inexistência de controles que promovam que o Termo de	(*)					X	X	X	*		X		

Possíveis achados	Dnit	SE/MS	SE/MCT	Ibama	Susep	TRT-SP	SE/MRE	TRT-RS	Anatel	Finep	SE/MP	ADE	FNDE
Referência ou Projeto Básico seja elaborado a partir de estudos técnicos preliminares													
Descumprimento do processo de planejamento de acordo com a IN 4		X	X	X	X								X
Falhas no cumprimento do processo de planejamento de acordo com a IN 4											X		
Inexistência dos estudos técnicos preliminares	X					X		X			X	X	
Falhas nos estudos técnicos preliminares													
Irregularidades na contratação													

(\*) Não havia este achado na auditoria-piloto

Quadro 13 – Processo de gestão de contratos de bens e serviços de TI (achados)

Possíveis achados	Dnit	SE/MS	SE/MCT	Ibama	Susep	TRT-SP	SE/MRE	TRT-RS	Anatel	Finep	SE/MP	ADE	FNDE
Inexistência de controles que promovam a regular gestão contratual	X		X			X	X	X					
Falhas nos controles que promovam a regular gestão contratual				X							X		
Irregularidades na gestão contratual													

No âmbito das empresas estatais, falhas foram identificadas que culminaram na seguinte deliberação (TC 026.347/2009-1; Acórdão 6.677/2010-TCU-1ª Câmara):

1.5. Determinar à Empresa de Tecnologia e Informações da Previdência Social – DATAPREV – que, no prazo de 90 dias:

1.5.1. adeque os termos da norma N/SU/008/02 às exigências da IN/MPOG/SLTI nº 02/2008 e da IN/MPOG/SLTI nº 04/2008, especialmente quanto às orientações acerca de estimativa de preços e à necessidade de consultar os preços praticados em compras similares;

1.5.2. alternativamente à adequação da norma N/SU/008/02 às exigências da IN/MPOG/SLTI nº 04/2008, elabore norma específica para contratação de serviços de tecnologia da informação.

Registre-se que há iniciativa concreta para adotar o modelo da IN-SLTI/MP 04/2010 em entes públicos que não estão jurisdicionados às normas da SLTI/MP, como por exemplo:

a Infraero, conforme Ato Administrativo 2.567/DA/2011 (anexo 3, fl. 38);  
o Governo do Distrito Federal, conforme Decreto (Distrital) 32.218/2010.

Ante o exposto, propõe-se recomendar ao Conselho Nacional de Justiça que:

a partir das diretrizes expostas no Acórdão 786/2006-TCU-Plenário, elabore um modelo de processo para contratação e gestão de soluções de tecnologia da informação para o Poder Judiciário ou, alternativamente, adote o modelo contido na IN SLTI/MP 04/2010 (subitem 0);

promova a implementação do modelo elaborado em atenção ao item anterior nos órgãos e entidades sob sua jurisdição mediante orientação normativa (subitem 0).

Recomendação análoga deve ser proposta à CGPAR e ao CNMP.

Monitoração do desempenho da gestão de TI

180

A décima questão de auditoria buscou avaliar a atuação da alta administração dos auditados na monitoração do desempenho da gestão e uso da TI, bem como se a auditoria interna (AI) apoia esta avaliação.

O que era esperado, segundo as boas práticas, é que a alta administração:

estabelecesse objetivos, indicadores e metas para a gestão de TI, o que já deveria estar no PDTI (Cobit 4.1, ME1.1 – Abordagem de monitoramento e PO1.4 – Plano estratégico de TI);

monitorasse a gestão de TI por meio de relatórios gerenciais (Cobit 4.1, ME1.5 – Relatórios gerenciais);

avaliasse a gestão de TI (Cobit 4.1, ME1.4 – Avaliar o desempenho);

determinasse ações corretivas, se fosse o caso (Cobit 4.1, ME1.6 – Ações corretivas); e

utilizasse a auditoria interna como um dos mecanismos para apoiar a realização das três últimas tarefas acima (Cobit 4.1, ME2.2 – Monitorar e avaliar os controles internos).

Os resultados das avaliações in loco constam do Quadro 14, evidenciando que quase 80% dos auditados não realizam dita avaliação, e os três que a realizam, fazem-no de forma esporádica ou somente a posteriori. Mais ainda, constata-se que a auditoria interna em mais de 70% dos casos não é utilizada como instrumento de apoio na avaliação que a alta administração deve realizar.

Quadro 14 – Monitoração do desempenho da TI (achados)

Possíveis achados	Dnit	SE/MS	SE/MCT	Ibama	Susep	TRT-SP	Dnocs	SE/MRE	TRT-RS	Anatel	Finep	SE/MP	ADE	FNDE
Inexistência de avaliação da gestão de TI	X	X	X	X	X	X	X			X	X			X
Falhas na avaliação da gestão de TI								X	X			X		
Auditoria interna não apoia a avaliação da TI	X	X	X	X	X	X	X		X		X	X		

Sobre o acompanhamento do desempenho da gestão e do uso da TI, o levantamento de auditoria que deu origem ao Acórdão 2.308/2010-TCU-Plenário concluiu nos seguintes termos (anexo 2, fl. 8v):

154. Portanto, a maioria das instituições respondentes não estabelece objetivos de TI, não tem indicadores de desempenho para esses objetivos, não avalia o alcance de objetivos e não toma decisões com base nos benefícios de negócio advindos dos sistemas de informação providos pela TI.

155. Obviamente, as instituições terão muita dificuldade em perseguir objetivos que não estiverem definidos. Além disso, a definição de um objetivo é somente o primeiro passo na sua direção, mas seu alcance geralmente depende de decisões tomadas no esforço de cumpri-lo, de acordo com a análise criteriosa dos indicadores correspondentes.

156. A conquista de um objetivo definido sem o acompanhamento dos indicadores apropriados depende, em geral, mais de fatores fortuitos do que de processos estabelecidos de supervisão e gerência. Nas vezes em que isso ocorre, costuma ser tão difícil repetir esse sucesso quanto aprender com ele.

157. A omissão no cumprimento dessa responsabilidade pela alta administração certamente é causa de ineficiência e inefetividade institucional, que devem ser obstinadamente combatidas.

Analizando os dados constantes do Apêndice 0 (linhas V a Y da tabela), foi evidenciado que houve seis situações em que as evidências apresentadas às equipes do TCU não corroboraram as respostas apresentadas à pergunta 1.2 do perfil GovTI2010, sugerindo que a situação com respeito ao acompanhamento do desempenho da gestão e do uso da TI, que foi declarada como muito ruim (ver excerto transscrito acima), pode ser de fato ainda pior.

Com vistas a sanar essa deficiência, esta Corte já proferiu recomendação por meio do Acórdão 2.308/2010-TCU-Plenário, nos seguintes termos:

9.1. recomendar ao Conselho Nacional de Justiça – CNJ, ao Departamento de Coordenação e Controle das Empresas Estatais – Dest, à Secretaria de Logística e Tecnologia da Informação do Ministério do Planejamento, Orçamento e Gestão – SLTI/MPOG, ao Conselho Nacional do Ministério Público – CNMP, à Secretaria Geral da Presidência do Tribunal de Contas da União – Segepres/TCU, à Diretoria Geral da Câmara dos Deputados e à Diretoria Geral do Senado Federal que, no âmbito de suas respectivas áreas de atuação:

9.1.1. orientem as unidades sob sua jurisdição, supervisão ou estrutura acerca da necessidade de estabelecer formalmente: (i) objetivos institucionais de TI alinhados às estratégias de negócio; (ii) indicadores para cada objetivo definido, preferencialmente em termos de benefícios para o negócio da instituição; (iii) metas para cada indicador definido; (iv) mecanismos para que a alta administração acompanhe o desempenho da TI da instituição;

9.1.2. normatizem a obrigatoriedade de a alta administração de cada instituição sob sua jurisdição, supervisão ou estrutura estabelecer os itens acima;

Neste contexto, resta determinar à Sefti que monitore as deliberações do Acórdão 2.308/2010-TCU-Plenário em conjunto com as que vierem a ser proferidas nestes autos (subitem 0).

Em sede de tema conexo, a ausência de estrutura de governança de TI nos entes da APF foi objeto de análise no levantamento de auditoria que deu origem ao Acórdão 2.308/2010-TCU-Plenário nos seguintes termos:

### 3.2 Estrutura de Governança de TI

138. O quadro abaixo demonstra os resultados obtidos na questão acerca da estrutura de governança de TI provida pela alta administração:

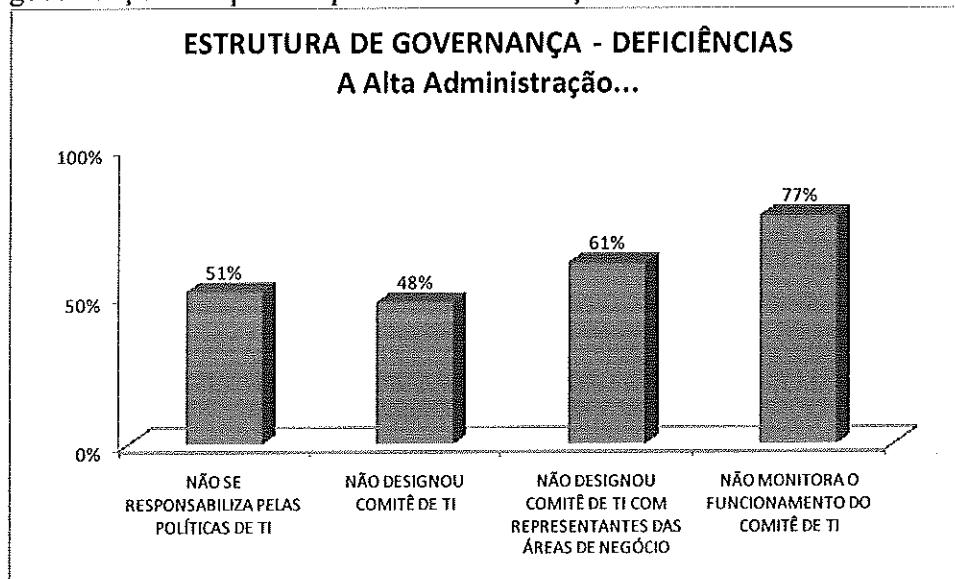


Figura 15. Estrutura de Governança de TI

#### 3.2.1 Análise

139. Considerando que as informações foram obtidas de modo declaratório, e que o questionário foi dirigido especificamente à alta administração, percebe-se, de plano, que a situação não é confortável. Passa da metade – 51% – o número de respondentes que declaram não se responsabilizar pelas políticas corporativas de TI.

140. Ora, são essas políticas que conferem as bases e os limites que norteiam a gestão e o uso de TI na instituição. Não há como se falar em governança de TI se a alta administração não estabelece ou responde pelas diretrizes mais elementares.

141. Dessa forma, é possível supor que a maioria das instituições da APF ainda não se preocupa com governança de TI.

(...)

(omissis)

(...)

### 3.2.2 Conclusão

145. Os dados do levantamento sugerem que o conceito de estrutura de governança de TI ainda é uma novidade para a maior parte das instituições públicas. O fato de que em menos da metade das instituições respondentes a alta administração se enxerga como responsável pelas políticas corporativas de TI, mesmo sendo essa uma área crítica, sugere um motivo pelo qual o amadurecimento da gestão e da governança de TI ainda se mostra tão lento, como demonstrado na análise contida na seção 2.

Lembrando que o estabelecimento de políticas de TI é um tipo de atividade de controle de TI (ver IN – TCU 63/2010, art. 1º, X, transscrito no item 0) a cargo da alta administração, tem-se como corolário que essa alta administração da APF tem pouca cultura no estabelecimento de controles internos de TI.

Analizando os dados constantes do Apêndice 0 (linha U da tabela), foi evidenciado que houve quatro situações em que as evidências apresentadas às equipes do TCU não corroboram as respostas apresentadas à pergunta do perfil GovTI2010 que pesquisou se a alta administração se responsabiliza pelo estabelecimento e pelo cumprimento das políticas de gestão e uso corporativo de TI, sugerindo que o percentual de organizações em que a alta administração não se responsabiliza pelas políticas de TI é ainda maior do que 51%.

Com respeito ao tema da responsabilidade da alta administração quanto ao estabelecimento de controles internos (e.g., políticas e procedimentos internos), o Acórdão 1.732/2009-TCU-Plenário trouxe a seguinte deliberação em processo de fiscalização na Petrobras:

9.15. determinar à Segecex que oriente as unidades técnicas deste Tribunal no sentido de que observem, em fiscalizações realizadas na Petrobras ou em alguma de suas subsidiárias/controladas, a estrutura organizacional da empresa, seus procedimentos internos, a tomada de decisões e outras variáveis que possam influenciar a definição dos responsáveis por irregularidades porventura detectadas, a fim de verificar se a ocorrência origina-se da omissão de dirigentes ocupantes de cargos de alto escalão da companhia, ao deixarem de exigir a elaboração de normativos internos ou a implementação de procedimentos que reflitam o cumprimento das determinações do Tribunal, ou dos próprios gestores no que se refere à sua margem de atuação e poder decisório, segundo suas competências funcionais. (sublinhou-se).

O excerto acima corrobora o entendimento de que a alta administração da APF é responsável pelas atividades de controle de mais alto nível, como o estabelecimento de políticas e definição de atividades de controle que devem ser executadas nos diversos níveis da organização.

Ainda no sentido de que é da alta administração das organizações a responsabilidade pelo estabelecimento de uma estrutura efetiva e consistente de controles internos, traz-se à baila trecho da Resolução – Bacen 2.554/1998, que dispõe sobre a implantação e implementação de sistema de controles internos nas instituições financeiras que operam no Brasil:

Art. 1º Determinar às instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil a implantação e a implementação de controles internos voltados para as atividades por elas desenvolvidas, seus sistemas de informações financeiras, operacionais e gerenciais e o cumprimento das normas legais e regulamentares a elas aplicáveis

Parágrafo 1º Os controles internos, independentemente do porte da instituição, devem ser efetivos e consistentes com a natureza, complexidade e risco das operações por ela realizadas.

Parágrafo 2º São de responsabilidade da diretoria da instituição:

I – a implantação e a implementação de uma estrutura de controles internos efetiva mediante a definição de atividades de controle para todos os níveis de negócios da instituição;

II – o estabelecimento dos objetivos e procedimentos pertinentes aos mesmos;

III – a verificação sistemática da adoção e do cumprimento dos procedimentos definidos em função do disposto no inciso II. (sublinhou-se)

Faz-se necessário, portanto, que a alta administração das organizações públicas estabeleça uma estrutura de controles internos para suas organizações, consistindo em um conjunto de atividades de controle que deve ser executado pelos gestores nos diversos níveis da organização, e que pode ou não

estar acompanhado da criação de uma unidade organizacional (setor dentro da organização) encarregado dessas atividades, o que é conhecido na iniciativa privada por setor de compliance (o termo é originário do verbo, em inglês, to comply, e significa estar em conformidade com regras, normas e procedimentos).

Relevante relembrar que as atividades de controle, conforme já foi mencionado no item 0 deste relatório, são de responsabilidade dos donos dos processos de negócio, não sendo, portanto, atividades da unidade de auditoria interna, a qual tem como um de seus objetivos avaliar a eficácia dos controles internos implantados pelos gestores.

A título de exemplo, o modelo Coso (Committee of Sponsoring Organizations of the Treadway Commission) apresenta as seguintes atividades de controle passíveis de implantação para mitigação de riscos nos processos de negócio: aprovação, autorização, verificação, reconciliação e revisão do desempenho operacional, da segurança dos bens e da segregação de funções.

Ante o exposto e considerando que os gestores dos órgãos e entidades da APF têm pouca (ou quase nenhuma) cultura de implantação de controles internos, conforme evidenciado nos itens 0 a 0 do presente relatório, propõem-se recomendações à CGDC e à SLTI/MP nos termos a seguir.

Recomendar à CGDC que, em atenção ao Decreto-Lei 200/1967, art. 6º, V, estabeleça, normativamente para todos os entes sob sua jurisdição, a obrigatoriedade de a alta administração implantar uma estrutura de controles internos, mediante a definição de atividades de controle em todos os níveis da organização para mitigar os riscos de suas atividades no processo de planejamento estratégico institucional (subitem 0).

Recomendar à SLTI/MP que, em atenção ao Decreto-Lei 200/1967, art. 6º, V, estabeleça, normativamente para todos os entes sob sua jurisdição, a obrigatoriedade de a alta administração implantar uma estrutura de controles internos mediante a definição de atividades de controle em todos os níveis da organização para mitigar os riscos de suas atividades, pelo menos nos seguintes processos (subitem 0):

- planejamento estratégico de TI;
- funcionamento dos comitês de TI;
- processo orçamentário de TI;
- processo de software;
- gerenciamento de projetos;
- gerenciamento de serviços de TI;
- segurança da informação;
- gestão de pessoal de TI;
- contratação e gestão de soluções de TI;
- monitoração do desempenho da TI organizacional.

Recomendação análoga deve ser proposta ao CNJ, ao CNMP e à CGPAR.

A título de exemplo, a alta administração pode instituir uma estrutura de controles internos no processo de planejamento estratégico institucional aprovando um guia de planejamento que descreve o processo (entradas, saídas, tarefas, atores etc) que a organização seguirá para elaborar seu plano estratégico de negócio, e contemplará nesse guia as atividades de controle necessárias para que o processo tenha, pelo menos, as características descritas no item 0 deste relatório.

Em sentido conexo, ainda que a auditoria interna se constitua em importante ator tanto na governança corporativa quanto na governança de TI, os dados do Quadro 14 (item 0 deste relatório) evidenciam que em dez dos catorze auditados a unidade de auditoria interna não realizou auditoria de TI nos últimos três anos.

Analizando os dados constantes do Apêndice 0 (linhas R1 a R6 da tabela), foi evidenciado que houve catorze situações em que as evidências apresentadas às equipes do TCU não corroboram as respostas apresentadas à pergunta do perfil GovTI2010 que trata da realização de auditoria de TI por iniciativa própria, sugerindo que o percentual de organizações em que essas auditorias não são realizadas é ainda maior do que 51%.

No monitoramento realizado (TC 028.772/2010-5; Acórdão 1.145/2011-TCU-Plenário), registrou-se que tanto o CNJ quanto o CNMP não lograram implementar medidas efetivas para o incentivo à auditoria de TI nos seus jurisdicionados (anexo 2, fl. 188v, item II.4.8).

Registre-se, entretanto, iniciativa basilar empreendida pelo CNJ com a edição da Resolução-CNJ 86/2009, determinando a criação de unidades de auditoria interna em todos os entes do Poder Judiciário (anexo 2, fl. 188v, item 129). Essa iniciativa busca suprir uma parte das deficiências estruturais nas unidades de auditoria interna do Poder Judiciário na esfera federal que foram detectadas por meio do levantamento de auditoria que deu origem ao Acórdão 1.074/2009-TCU-Plenário.

Ainda com respeito aos órgãos de controle interno do Poder Judiciário, verifica-se que o controle interno encontra-se na forma de um sistema integrado na Justiça Federal pela Resolução-CJF 85/2009, mas não em todo o Poder Judiciário Federal, como preconiza a Constituição Federal, ensejando recomendar ao CJN que, em atenção à Constituição Federal, art. 74, c/c o art. 103-B, § 4º, I, estabeleça sistema de controle interno integrado para todo o Poder Judiciário (subitem 0).

Recomendação análoga deve ser proposta ao CNMP, uma vez que o controle interno não assume a forma de um sistema integrado no Ministério Público.

No Poder Executivo Federal, o controle interno encontra-se sistematizado pela Lei 10.180/2001, que foi regulamentada pelo Decreto 3.591/2000, que estabelece que a CGU/PR é o órgão central do sistema.

Quanto à atuação do órgão central do sistema de controle interno do Poder Executivo, o monitoramento realizado (TC 028.772/2010-5; Acórdão 1.145/2011-TCU-Plenário) registrou o que segue:

20. Isto posto, conclui-se que a CGU/PR não considera a fiscalização das aquisições de TI como questão estruturante e de maior relevância, fato que deverá ser levado em consideração quando da consolidação do TMS 6 – Gestão e uso de TI.

(...)

30. A atuação de forma pontual, por meio de algumas fiscalizações in loco, consiste em indício de ausência de processos de trabalhos sistêmicos capazes de abranger a multiplicidade de auditados, como, por exemplo, foi feito nos levantamentos de governança de TI (vide Acórdãos 1.603/2008 e 2.308/2010, ambos do Plenário do TCU) e no levantamento sobre a atuação das unidades de auditoria interna (Acórdão 1.074/2009-TCU-Plenário). Além disso, não foi apresentado o critério de seleção para a realização das fiscalizações que teriam sido realizadas. Tais fatos deverão ser levados em consideração quando da consolidação do TMS 6 – Gestão e uso de TI.

(...)

143. Análise: em que pese os resultados apresentados pela CGU, já registramos que as auditorias de TI ainda não são regularmente realizadas pelo órgão (itens 14-22). Ademais, o gestor menciona os trabalhos realizados com foco na avaliação de contratos de terceirização (item 4, peça 18, fl. 3), e não foram apresentadas evidências de que a CGU tem estimulado a realização desse tipo de auditoria nos órgãos e entidades da APF.

144. Novamente, a ausência de evidência de que há uma atuação sistematizada e coordenada pelo órgão central do controle interno do Poder Executivo no tema TI deve ser levada em consideração quando da consolidação dos trabalhos do TMS 6 – Gestão e uso de TI. (sublinhou-se)

Ante as conclusões transcritas acima, visualiza-se oportunidade de melhoria na atuação do órgão central de controle interno do Poder Executivo, ator essencial para a melhoria do péssimo cenário de governança de TI delineado ao longo deste relatório.

O Instituto de Auditores Internos (The Institute of Internal Auditors – IIA) é uma associação mundial de profissionais de auditoria interna. Baseado nas melhores práticas mundiais, o IIA estabeleceu um marco de referência denominado Estrutura Internacional de Práticas Profissionais (International Professional Practices Framework – IPPF) contendo orientações para que a atividade de auditoria interna nas organizações seja efetiva, seja ela privada ou pública.

Do IPPF transcrevem-se abaixo, além da definição de auditoria interna, algumas normas que as unidades de auditorias internas efetivas comumente observam:

Definição de auditoria interna. A auditoria interna é uma atividade independente e objetiva de avaliação (assurance) e de consultoria, desenhada para adicionar valor e melhorar as operações de uma organização. Ela auxilia uma organização a realizar seus objetivos a partir da aplicação de uma abordagem sistemática e disciplinada para avaliar e melhorar a eficácia dos processos de gerenciamento de riscos, controle e governança.

(...)

1210.A3 – Os auditores internos devem possuir conhecimento suficiente sobre os principais riscos e controles de tecnologia da informação e sobre as técnicas de auditoria baseadas em tecnologia disponíveis para a execução dos trabalhos a eles designados. Entretanto, não se espera que todos os auditores internos possuam a especialização de um auditor interno cuja principal responsabilidade seja auditoria de tecnologia da informação.

(...)

2110.A2 – A atividade de auditoria interna deve avaliar se a governança de tecnologia da informação da organização dá suporte às estratégias e objetivos da organização.

(...)

2120.A1 – A atividade de auditoria interna deve avaliar as exposições a riscos relacionadas à governança, às operações e aos sistemas de informação da organização, em relação a:

- Confiabilidade e integridade das informações financeiras e operacionais;
- Eficácia e eficiência das operações e programas;
- Salvaguarda dos ativos; e
- Conformidade com leis, regulamentos, políticas, procedimentos e contratos.

(...)

2130.A1- A atividade de auditoria interna deve avaliar a adequação e a eficácia dos controles em resposta aos riscos, abrangendo a governança, as operações e os sistemas de informação da organização, com relação a:

- Confiabilidade e integridade das informações financeiras e operacionais;
- Eficácia e eficiência das operações e programas;
- Salvaguarda dos ativos; e
- Conformidade com leis, regulamentos, políticas e procedimentos e contratos. (sublinhou-se)

Assim, vê-se que a auditoria interna deve ter foco eminentemente preventivo, por meio da avaliação da eficácia dos processos de gerenciamento de riscos, controle e governança e por meio da contribuição para a melhoria dos mesmos.

Observa-se ainda que as boas práticas recomendam que todos os auditores internos, mesmo os não especialistas em TI, devem ter condições de realizar avaliações com respeito aos principais riscos e controles de TI, o que é conhecido como avaliação limitada. Os trabalhos realizados neste TMS evidenciam que isso é possível, pois onze das catorze auditorias para avaliação de controles gerais de TI foram realizadas por auditores que não são especialistas em TI, após treinamento ministrado por auditores da Sefti.

Considerando a informação contida no item 0, de que tende para a totalidade os entes da APF que dependem de TI para conduzirem as políticas públicas, os temas relacionados à TI devem ser considerados na escolha dos objetos do universo de auditoria, motivo pelo qual propõe-se recomendar à CGU/PR que considere os temas governança de TI, riscos de TI e controles de TI na seleção dos objetos a auditar, consoante o previsto nas boas práticas internacionais para que a atividade de auditoria interna seja mais efetiva (e.g., IPPF 2110.A2, 2120.A1 e 2130.A1).

Propõe-se ainda recomendar à CGU/PR que oriente as unidades de auditoria interna sob sua orientação normativa a considerar os temas governança de TI, riscos de TI e controles de TI na seleção dos objetos a auditar, consoante o previsto nas boas práticas internacionais para que a atividade de auditoria interna seja mais efetiva (e.g., IPPF 2110.A2, 2120.A1 e 2130.A1).

Proposta análoga deve ser feita ao CNJ e ao CNMP.

Ainda com respeito à estruturação e atuação do sistema de controle interno do Poder Executivo, dois pontos foram identificados durante os trabalhos deste TMS.

O primeiro deles, é que, em rápida pesquisa na base de deliberações do TCU, obtiveram-se as seguintes evidências de deficiências nas estruturas das unidades de auditoria interna das entidades vinculadas ao Poder Executivo:

deficiências de pessoal na unidade de auditoria: Infraero (Acórdão 2.882/2009-TCU-Plenário); Agência Nacional do Petróleo (Acórdão 6.210/2010-TCU-1ª Câmara); Fundo Constitucional de Financiamento do Norte (Acórdão 1.352/2011-TCU-Plenário);

ausência da própria unidade de auditoria interna: Instituto Chico Mendes de Conservação da Biodiversidade (Acórdão 6.522/2009-2ª Câmara, item 1.5.2.2.2); Universidade Federal do Mato Grosso do Sul (Acórdão 2.282/2011-TCU-2ª Câmara); Fundação Universidade Federal do Pampa (Acórdão 1.955/2011-TCU-2ª Câmara).

O segundo ponto trata do impedimento, na prática, de que os órgãos da administração direta possuam unidade de auditoria interna em sua estrutura. Isso é consequência da vedação contida na IN-Seges 3/2010, de que o Auditor-Interno (denominado nos ministérios de Assessor Especial de Controle Interno) não pode ter unidades administrativas ou cargos em comissão a ele subordinados, senão vejamos:

Art. 5º – Os cargos em comissão de Gerente de Projeto, Auditor-Interno e Diretor-Adjunto, nível DAS 101.4, de Diretor de Programa e Secretário-Adjunto, nível DAS 101.5, e os cargos de assessoramento não terão unidades administrativas ou cargos em comissão a eles subordinados.

Esses dois pontos, associados à ausência de atuação sistematizada e coordenada pelo órgão central do controle interno do Poder Executivo no tema TI (ver item 0) e ao fato de que falhas em TI podem paralisar a condução das políticas públicas no Governo Federal (ver item 0), sugerem a oportunidade de aperfeiçoamento da atuação do sistema de controle interno do Poder Executivo Federal.

Nesse sentido, registramos trabalho já realizado pelo TCU em 2006, que resultou no Acórdão 412/2007-TCU-Plenário. Entretanto, observa-se pelas perguntas de auditoria formuladas que o foco daquele trabalho foi avaliar a atuação reativa do órgão central (CGU/PR):

1.6. A equipe formulou três questões de auditoria, listadas abaixo, com o intuito de detalhar o objetivo e nortear a execução dos trabalhos.

– Os critérios aplicados pela CGU na seleção das ações de controle levam à alocação de esforços proporcionalmente à materialidade dos recursos envolvidos?

– As ações de auditoria e fiscalização da SFC têm contribuído para identificar irregularidades e desvios nos órgãos do Poder Executivo Federal?

– Quando da identificação de desvios ou danos ao erário, os trabalhos de auditoria têm reunido os elementos necessários para imputação do débito?

Portanto, a atuação preventiva, por meio da avaliação da eficácia dos processos de gerenciamento de riscos, controle e governança e contribuição para a melhoria dos mesmos, não foi objeto daquele trabalho.

No Poder Judiciário também se percebe oportunidade de melhoria na atuação do sistema de controle interno, inclusive ante a ausência de sistematização do mesmo.

Considerando que o referencial estratégico em vigor do TCU contempla como objetivo estratégico ‘Contribuir para a melhoria da gestão e do desempenho da Administração Pública’, o qual tem como um de seus indicadores o ‘índice de governança corporativa dos órgãos da Administração Pública Federal’, considerando também que as unidades de auditoria interna são atores essenciais à boa governança de TI, e considerando ainda as deficiências dos sistemas de controles internos (controles internos dos gestores e atuação das unidades de auditoria interna) conforme evidenciado neste TMS, há espaço para que o TCU contribua para o cumprimento do comando previsto na Constituição Federal, art. 74, mas que somente poderá ocorrer mediante trabalho de avaliação sistematizada dos sistemas de controles internos dos poderes.

## ASPECTOS LEGAIS NAS CONTRATAÇÕES DE SOLUÇÕES DE TI

## Sistema de Registro de Preços (SRP)

O Apêndice 0 contém tabela com os dados declarados pelos jurisdicionados no levantamento GovTI2010 acerca de suas licitações e contratações no ano de 2009 (pergunta 7.9 do questionário), cuja análise fizemos com apoio do mapa mental constante da Figura 4 daquele apêndice.

Do total de 6.442 contratações declaradas, 47% (3.031) foram originadas do SRP por alguma das formas possíveis, indicando tendência de a APF dar cumprimento à Lei 8.666/1993, art. 15, inciso II, que prevê que as aquisições devem dar-se preferencialmente pelo SRP.

Ocorre que das 3.031 contratações por SRP, apenas 7% (199) foram realizadas por meio da prática de planejamento conjunto entre diversos entes, como fundamentado no Decreto 3.931/2001, art. 2º, inciso III:

Art.2º Será adotado, preferencialmente, o SRP nas seguintes hipóteses:

(...)

III – quando for conveniente a aquisição de bens ou a contratação de serviços para atendimento a mais de um órgão ou entidade, ou a programas de governo;

(...)

Parágrafo único. Poderá ser realizado registro de preços para contratação de bens e serviços de informática, obedecida a legislação vigente, desde que devidamente justificada e caracterizada a vantagem econômica.

Observa-se que, das mesmas 3.031 contratações por SRP, 30% (902) foram licitações para criação de atas que não contaram com outras instituições participantes desde o planejamento da contratação, número inquietante se observarmos que bens e serviços de TI dificilmente se enquadrariam nos demais incisos, pelos quais, em princípio, a criação da ata de registro de preços deve ser fundamentada:

Art.2º Será adotado, preferencialmente, o SRP nas seguintes hipóteses:

I – quando, pelas características do bem ou serviço, houver necessidade de contratações freqüentes;

II – quando for mais conveniente aquisição de bens com previsão de entregas parceladas ou contratação de serviços necessários à Administração para o desempenho de suas atribuições;

(...)

IV – quando pela natureza do objeto não for possível definir previamente o quantitativo a ser demandado pela Administração.

Essas atas, criadas sem participantes, podem ter dado origem ao fato mais preocupante desta análise: 64% das contratações por SRP (1.930 das 3.031) foram adesões fundamentadas no art. 8º do Decreto 3.931/2001, prática de adesão tardia ou, como é mais conhecida, ‘carona’.

Mais um dado da análise empreendida consta da **Error! Reference source not found.** Erro! Fonte de referência não encontrada. (no final do Apêndice 0), em que se observa que 11% dos pesquisados repudiam a prática da adesão tardia, mas 63% dos pesquisados o fazem na maioria das suas contratações.

Os números acima evidenciam que, apesar de buscar contratar preferencialmente pelo SRP, o planejamento conjunto para a criação de uma ata, que deveria ser a regra, é exceção. Já a prática de adesão tardia (carona), que deveria ser exceção, tornou-se prática comum.

Registre-se que a problemática envolvendo a adesão tardia a atas de registro de preços é preocupação desta Corte, que já se manifestou contrariamente à sua prática irrestrita por meio do Acórdão 1.487/2007-TCU-Plenário, ora em fase de recurso.

Como exemplo de planejamento conjunto para a geração de ata de registro de preço que atende ao espírito da legislação e, por meio do planejamento, dá cumprimento ao princípio constitucional da eficiência, pode-se citar a ação coordenada pela SLTI/MP para aquisição de mais de 100.000 equipamentos (anexo 3, fl. 37).

Em outro extremo, encontramos uma série de atas de registro de preços, possivelmente criadas sem participantes (ver itens 0 e 0), que se tornam objeto de exploração comercial por parte de empresas privadas (anexo 3, fls. 35-36).

Ocorre que, durante as fiscalizações deste TMS, as quatro contratações analisadas pelas diversas equipes, que foram oriundas de atas de registro de preços, encontravam-se com indícios de graves irregularidades, tanto que foram objetos de representações das equipes (TC 022.804/2010-2, 029.535/2010-7, 030.133/2010-6 e 000.079/2011-1).

Outras contratações de TI por meio de adesão a atas de registro de preços com indícios de graves irregularidades têm sido identificadas no âmbito do TC 017.907/2009-0, por meio do qual a Sefiti realiza acompanhamento de editais e contratos de TI na APF, por exemplo:

Ata de Registro de Preços 14/2010 da Base de Fuzileiros Navais da Ilha das Flores, cujo objeto contém diversos itens de serviços de TI (fato apurado na representação constante do TC 001.280/2011-2, sendo que o Acórdão 1.371/2011-TCU-Plenário prolatado no processo registra que o gestor tornou a ata nula);

Ata de Registro de Preços 25/2010 do Conselho Nacional de Desenvolvimento Científico e Tecnológico, cujo objeto é a manutenção de sistemas de informação, que deu origem às adesões de quatro órgãos (Hospital de Clínicas de Porto Alegre, Instituto Chico Mendes de Conservação da Biodiversidade, Instituto Brasileiro de Geografia e Estatística, Comitê Paraolímpico Brasileiro).

Os problemas recorrentes identificados nas contratações questionadas são:

não declarar a fundamentação legal que sustenta o motivo da criação da ata;

não realizar o planejamento da contratação, tanto na criação da ata quanto na adesão;

não fixar os quantitativos máximos que serão adquiridos por meio da ata;

não demonstrar a vantajosidade em aderir à ata;

aderir à ata de registro de preços oriunda de licitação com critérios e condições aplicáveis ao ente que registrou a ata, porém distintos das necessidades da instituição que realiza a adesão.

Com respeito ao item 0 supra, cite-se, ainda, como exemplo, o caso constante do TC 023.911/2010-7, em que se identificou que o Ministério da Previdência Social aderiu a uma ata da Infraero para a aquisição de solução de storage com valor 22,8% maior do que constava de outra ata com mesmo objeto, a última do Ministério do Desenvolvimento, Indústria e Comércio.

Com respeito ao item 0 supra, citam-se ainda os seguintes casos concretos exemplificativos da situação:

a Universidade Federal da Bahia (UFBA) realizou pregão, registrou ARP e contratou serviços de suporte ao usuário, em que as características mais importantes dos serviços são o ambiente que será suportado (equipamentos e softwares usados pelos usuários) e os níveis mínimos de serviço exigidos. Pelo menos outros cinco órgãos federais aderiram a essa Ata (Ibama, MMA, MCT, Embratur e IBCIT), e há fortes indícios de que essas duas características não são as mesmas em todos estes órgãos. Tal indício, juntamente com os indícios de sobrepreço na contratação efetuada pela UFBA (que potencialmente também ocorreu nos demais contratos, visto que a planilha de custos e formação de preços em princípio é a mesma em todos os contratos) são objetos de apuração em seis representações abertas pela coordenação do TMS (TC 022.804/2010-2, 000.079/2011-1, 021.418/2011-0, 020.503/2011-3, 021.419/2011-6 e 021.874/2011-5), sendo que no processo consta que o gestor do Ibama já iniciou procedimento para glosar cerca de R\$ 750 mil que teriam sido pagos indevidamente (só no contrato do Ibama).

durante o monitoramento das deliberações do Acórdão 1.033/2009-TCU-Plenário (TC 012.953/2011-3), a equipe de auditoria identificou que a Imprensa Nacional (IN) firmou contrato cujo objeto é o suporte ao seu ambiente computacional por meio de adesão à ARP do STJ, sendo que há indícios de que diversos critérios de habilitação contidos no edital do STJ não se aplicam à realidade da IN (e.g., IN não possui servidores com sistema operacional AIX, ao passo que o STJ sim; a IN possui cerca de seiscentos pontos de rede, enquanto o edital pede atestado referente à prestação de suporte em pelo menos 3.000; o edital pede atestado técnico relativo à prestação de serviços de tratamento documental e processamento de imagens de processos ou de documentos, serviço que não será prestado

na IN), de forma que o objeto deveria ter sido licitado com critérios menos rígidos que os do STJ, permitindo potencialmente maior participação de interessados. No mesmo sentido, todas as adesões à ARP da UFBA citadas no parágrafo 0 continham o vício de que houve exigência no edital que originou a ata que não se aplicam à realidade dos demais órgãos aderentes (e.g., a contratada deveria ter escritório em Salvador/BA).

Ante as constatações acima, e a existência de precedentes de julgados para alguns dos assuntos acima tratados nesta Corte, entende-se como oportuno e conveniente que os órgãos governantes superiores orientem seus jurisdicionados para evitar as práticas irregulares acima, e propõe-se determinar à SLTI/MP que

, em atenção ao disposto no Decreto 1.094/1994, art. 2º, inciso I, oriente os órgãos e entidades sob sua jurisdição para que (subitem 0):

ao realizarem licitação com finalidade de criar ata de registro de preços atentem que:

devem fundamentar formalmente a criação de ata de registro de preços, e.g., por um dos incisos do art. 2º do Decreto 3.931/2001 (Acórdão 2.401/2006-TCU-Plenário);

devem praticar todos os atos descritos no Decreto 3.931/2001, art. 3º, § 2º, em especial o previsto no seu inciso I, que consiste em ‘convidar mediante correspondência eletrônica ou outro meio eficaz, os órgãos e entidades para participarem do registro de preços’;

o planejamento da contratação é obrigatório, sendo que se o objeto for solução de TI, caso seja integrante do Sisp, deve executar o processo de planejamento previsto na IN – SLTI/MP 4/2010 (IN – SLTI/MP 4/2010, art. 18, inciso III) ou, caso não o seja, deve realizar os devidos estudos técnicos preliminares (Lei 8.666/1993, art. 6º, inciso IX);

a fixação, no termo de convocação, de quantitativos (máximos) a serem contratados por meio dos contratos derivados da ata de registro de preços, previstos no Decreto 3.931/2001, art. 9º, inciso II, é obrigação e não faculdade do gestor (Acórdão 991/2009-TCU-Plenário, Acórdão 1.100/2007-TCU-Plenário e Acórdão 4.411/2010-TCU-2ª Câmara);

em atenção ao princípio da vinculação ao instrumento convocatório (Lei 8.666/1993, art. 3º, caput), devem gerenciar a ata de forma que a soma dos quantitativos contratados em todos os contratos derivados da ata não supere o quantitativo máximo previsto no edital.

quando realizarem adesão à ata de registro de preços atentem que:

o planejamento da contratação é obrigatório, sendo que se o objeto for solução de TI, caso seja integrante do Sisp, deve executar o processo de planejamento previsto na IN – SLTI/MP 4/2010 (IN – SLTI/MP 4/2010, art. 18, inciso III) ou, caso não o seja, realizar os devidos estudos técnicos preliminares (Lei 8.666/1993, art. 6º, inciso IX);

devem demonstrar formalmente aa vantajosidade da adesão, nos termos do Decreto 3.931/2001, art. 8º;

as regras e condições estabelecidas no certame que originou a ata de registro de preços devem ser conformes as necessidades e condições determinadas na etapa de planejamento da contratação (Lei 8.666/1993, art. 6º, inciso IX, alínea d, c/c o art. 3º, § 1º, inciso I, e Lei 10.520/2002, art. 3º, inciso II).

Determinação análoga deve ser proposta ao Dest, ao CNJ e ao CNMP.

Divulgação de notas técnicas e ações pedagógicas

Com o objetivo de promover ações pedagógicas que divulguem entendimentos sobre assuntos polêmicos no tema contratações de TI, por meio do Acórdão 1.215/2009-TCU-Plenário, o TCU deliberou o que segue:

9.1. recomendar à Secretaria de Fiscalização de Tecnologia da Informação que:

9.1.1. divulgue o conteúdo do Quadro Referencial Normativo e das Notas Técnicas 01 e 02/2008 – Sefti/TCU, como forma de informar e orientar, à Administração Pública e à sociedade, sobre a existência do conjunto de normas que regem as aquisições de bens e serviços de Tecnologia da Informação, bem como jurisprudência deste Tribunal sobre o assunto, promovendo, inclusive, a realização de seminários, cursos e palestras sobre tais assuntos, caso entenda conveniente;

Ocorre que desde então a Sefti revisou as duas notas técnicas mencionadas acima e elaborou outras quatro, de forma que hoje estão disponíveis na rede interna do TCU:

Nota Técnica 1/2008-TCU/Sefti, cujo assunto é ‘Conteúdo mínimo do projeto básico ou termo de referência para contratação de serviços de tecnologia da informação – TI’;

Nota Técnica 2/2008-TCU/Sefti, cujo assunto é ‘Uso do Pregão para aquisição de bens e serviços de Tecnologia de Informação’;

Nota Técnica 3/2009-TCU/Sefti, cujo assunto é ‘Exigência de credenciamento das licitantes pelos fabricantes de produtos de tecnologia da informação, nos certames para aquisição de bens e serviços da área’;

Nota Técnica 4/2009-TCU/Sefti, cujo assunto é ‘Possibilidade de avaliação de amostras na contratação de bens e suprimentos de tecnologia da informação mediante a modalidade Pregão.’

Nota Técnica 5/2010-TCU/Sefti , cujo assunto é ‘Condições em que há possibilidade de exigência da demonstração de qualidade de processo em contratações de serviços de software, a exemplo de CMMI e MPS.BR’;

Nota Técnica 6/2011-TCU/Sefti, cujo assunto é ‘Aplicabilidade da Gestão de Nível de Serviço como mecanismo de pagamento por resultados em contratações de serviços de TI pela Administração Pública Federal’.

Assim, na esteira de continuar informando sobre o tema, e considerando que o Acórdão 1.215/2009-TCU-Plenário já conteve determinação (9.1.1) para a divulgação das notas técnicas 1/2008 e 2/2008, propõe-se determinar à Sefti que divulgue o conteúdo das seis notas técnicas existentes, como forma de informar e orientar a APF e a sociedade sobre a existência do conjunto de normas que regem as aquisições de bens e serviços de tecnologia da informação, bem como sobre a jurisprudência deste Tribunal quanto ao assunto, promovendo, inclusive, a realização de seminários, cursos e palestras, caso entenda conveniente (subitem 0).

#### Contratação do Serpro pela APF

A auditoria-piloto deste TMS (TC 009.982/2010-8; Acórdão 866/2011-TCU-Plenário) identificou, logo no início dos trabalhos, a dependência que alguns entes da APF poderiam ter em relação ao Serviço Federal de Processamento de Dados (Serpro), decorrente da ausência de estruturas de governança de TI adequadas, como exemplificamos no excerto do relatório transcritos a seguir:

A ausência de planejamento estratégico institucional, as falhas no processo de planejamento de TI e a ausência de alguns processos, padrões e políticas de TI, aliada à ampla dependência da Autarquia com relação aos serviços de TI fornecidos pelo Serpro, impõe ao órgão um alto risco quanto à proficiência da TI no âmbito interno. Essa falta de estrutura e a dependência do órgão a uma única contratada pode afetar de maneira negativa o cumprimento dos objetivos de negócio e das obrigações legais da Autarquia.

Essa situação já havia sido detectada em fiscalização realizada por ocasião do TMS 2007 – Terceirização em TI, como se pode depreender dos excertos do relatório transcritos a seguir (TC 026.200/2007-3, Acórdão 1.330/2008-TCU-Plenário):

#### 6.8 Setor de TI – existência de funções sensíveis exercidas por não servidores do ente

a) foram solicitadas informações relativas aos responsáveis pela execução das atividades relacionadas com segurança da informação, administração de banco de dados, administração de rede e outras áreas consideradas críticas, indicando o vínculo com o serviço público. Em atendimento, a SPOA encaminhou os nomes dos responsáveis pelas áreas acima citadas, indicando que todos eles são do SERPRO.

(...)

Segundo os gestores dessa Subsecretaria, a metodologia de desenvolvimento de outros sistemas é de total responsabilidade do SERPRO, não havendo ingerência da SPOA sobre esse processo.

(...)

c) devido a um vírus, houve uma paralização na rede da GRA-SP por mais de duas semanas, o que comprova que o Plano de Contingência do SERPRO, remetido pela SPOA, não tem aplicabilidade efetiva.

(...)

a) foram solicitadas informações relativas à gestão de mudanças. A SPOA remeteu um documento elaborado pelo SERPRO, que trata, no seu item 4.4, da Gestão de Mudanças (fl. 120 do anexo 2). Esse documento é genérico, não detalhando os procedimentos a serem adotados.

(...)

#### 6.19 Plano de Continuidade do Negócio – inexistência/falhas

a) foram solicitadas informações a respeito do Plano de Continuidade de Negócios (PCN). A SPOA remeteu como resposta o documento relativo ao Plano de Contingência (fl. 120 do anexo 2). Esse documento não comprova que o órgão tem um Plano de Continuidade dos Negócios, pois foi elaborado pelo SERPRO e não avalia os recursos críticos de TI.

No âmbito da fiscalização que gerou o Acórdão 1.793/2011-TCU-Plenário, identificou-se que o Serpro recebera mais de R\$ 1 bilhão oriundos de contratos com órgãos e entidades da APF (anexo 2, fl. 224v, item 2.1.2).

O próprio texto da já revogada IN – SLTI 4/2008, a partir de orientações dadas pelo Acórdão 786/2006-TCU-Plenário, trazia no seu art. 5º orientação clara quanto à necessidade de evitar a dependência excessiva de um só fornecedor e de promover o parcelamento das demandas de serviços de TI. Porém, o § 2º dessa IN excepcionava tal orientação nos casos em que a contratada fosse empresa pública de TI. Felizmente, a IN – SLTI 4/2010, que substituiu a citada versão de 2008, eliminou essa excepcionalidade, reforçando o conceito de que as instituições públicas devem exercer pleno governo sobre a tecnologia da informação que utilizam, mesmo quando contratam com empresas públicas de TI.

Assim, pelo risco de os entes da APF ainda entenderem que a contratação do Serpro os exime da responsabilidade de possuir estruturas de governança de TI adequadas e pela alta materialidade dos contratos com aquela empresa, incluiu-se no TMS fiscalização específica para avaliar os ditos contratos.

A fiscalização, conduzida por meio do TC 022.241/2010-8, identificou que, em 2010, o Serpro possuía 236 contratos com a APF, no total de R\$ 5.027.481.735,14, sendo dois deles selecionados para análise: o da Receita Federal do Brasil (RFB) e o do Ministério do Planejamento, Orçamento e Gestão (MP). Em termos de materialidade, a soma do valor desses dois representa mais da metade do valor dos contratos do Serpro (53,5%) e, em termos de abrangência dos serviços, eles contêm praticamente todo o espectro de serviços fornecidos por aquela empresa, além de contemplar serviços que dão suporte a sistemas estratégicos do Governo Federal (anexo 2, fls. 225v-226, item 2.4.7).

Os principais problemas identificados na contratação (em um ou outro dos contratos analisados) são oriundos de deficiências no planejamento da contratação, materializadas pelo seguinte:

descumprimento do processo de planejamento de acordo com a IN – SLTI 4/2008 (vigente à época) ou ausência de elaboração de estudos técnicos preliminares (Lei 8.666/1993, art. 6º, IX) na contratação anterior à vigência da IN – SLTI 4/2008;

especificação imprecisa ou insuficiente do objeto, afrontando a Lei 8.666/1993, art. 6º, IX; falhas nos critérios de mensuração dos serviços, afrontando a Lei 8.666/1993, art. 6º, IX, e (também necessários de acordo com a IN – SLTI 4/2010, art. 14, II, a);

falhas na metodologia de avaliação da adequação dos produtos, afrontando a Lei 8.666/1993, art. 6º, IX, e (também necessária de acordo com a IN – SLTI 4/2010, art. 14, II, c);

falhas nas cláusulas de penalidades ao não detalhar no contrato as penalidades contidas na Lei 8.666/1993, art. 87, afrontando o art. 55, VII e VIII, da mesma lei, e os princípios da razoabilidade e proporcionalidade (e também o previsto na IN – SLTI 4/2010, art. 15, III, h);

modelo de pagamento não vinculado a resultados, afrontando o princípio constitucional da eficiência (e também o Decreto 2.271/1997, art. 3º, § 1º, e a IN – SLTI 4/2010, art. 15, §§ 2º e 3º);

falhas na justificativa de preços, afrontando a Lei 8.666/1993, art. 26, III.

Registre-se que os contratos dos órgãos e entidades da APF com o Serpro não estão excepcionalizados pela legislação para os pontos identificados acima, de forma que devem estar conforme os dispositivos mencionados.

A seu turno, na execução contratual verificaram-se (em um ou outro dos contratos analisados) as seguintes falhas ou improvidades:

- desconformidade na aplicação dos critérios de medição;
- desconformidade na verificação dos critérios de qualidade;
- desconformidade na aplicação dos critérios de pagamento;
- dificuldade de rastrear serviços executados;
- inexecução de serviços previstos no contrato.

Todas as situações acima afrontam o previsto na Lei 8.666/1993, art. 66, que vincula todos os contratos administrativos da Administração Pública, inclusive os feitos com o Serpro.

Ao tempo em que aponta as falhas acima, o relatório do TC 022.241/2010-8 consigna como bom o modelo do contrato da RFB, bem como eficaz a gestão contratual realizada no âmbito daquele órgão, mesmo que o contrato da RFB tenha complexidade acima da média. Esta constatação evidencia que é possível firmar e gerir contratos com o Serpro seguindo os preceitos legais e de acordo com as boas práticas.

Há que se ressaltar que, mesmo sendo a contratada integrante da administração pública, como é o caso do Serpro, ela deve realizar a contratação e gerir o contrato em conformidade com as previsões legais.

Alguns desses problemas detalhados na fiscalização realizada nos contratos com a RFB e o MP também foram identificados no Dnit (Acórdão 866/2011-TCU-Plenário) e na Susep (Acórdão 2.746/2010-TCU-Plenário), que também possuíam contratos com o Serpro.

Considerando que eram 93 contratantes do Serpro à época da auditoria, com 236 contratos em vigor, e que há possibilidade de os problemas identificados nos contratos da RFB, do MP, do Dnit e da Susep serem recorrentes, há oportunidade de atuação dos OGS na orientação de seus jurisdicionados, motivo pelo qual se propõe determinar à SLTI/MP que, em atenção ao Decreto 7.579/2011, art. 4º, V, oriente os órgãos e entidades sob sua jurisdição para que, caso possuam contratos com empresas públicas prestadoras de serviços de TI (subitem 0):

analisem a conformidade dos termos do contrato e do projeto básico e verifiquem se:

foi realizado o adequado planejamento da contratação, consistindo na execução do processo de planejamento previsto na IN – SLTI/MP 4/2010 se for integrante do Sisp (IN – SLTI/MP 4/2010, art. 18, inciso II) ou, caso não o seja, se foram realizados os devidos estudos técnicos preliminares (Lei 8.666/1993, art. 6º, inciso IX);

as especificações do objeto são precisas e suficientes, em conformidade com a Lei 8.666/1993, art. 6º, IX;

os critérios de mensuração dos serviços são precisos e suficientes, de acordo com o determinado na Lei 8.666/1993, art. 6º, IX, e (também necessários de acordo com a IN – SLTI 4/2010, art. 14, II, a);

a metodologia de avaliação da adequação dos produtos é precisa e suficiente, de acordo com o determinado na Lei 8.666/1993, art. 6º, IX, e (também necessária de acordo com a IN – SLTI 4/2010, art. 14, II, c);

as cláusulas de penalidades contidas na Lei 8.666/1993, art. 87, de acordo com o determinado na Lei 8.666/1993, art. 55, VII e VIII, são detalhadas e atendem aos princípios da razoabilidade, proporcionalidade e prudência (e também o previsto na IN – SLTI 4/2010, art. 15, III, h);

o modelo de pagamento é vinculado a resultados, obedecendo ao princípio constitucional da eficiência (e também ao previsto no Decreto 2.271/1997, art. 3º, § 1º, e na IN – SLTI 4/2010, art. 15, §§ 2º e 3º);

a justificativa dos preços contratados é adequadamente fundamentada em arrazoada pesquisa de mercado, de acordo com o determinado na Lei 8.666/1993, art. 26, III, inclusive com a análise da planilha de composição de custos dos serviços, necessária segundo a Lei 8.666/1993, art. 7º, § 2º, II;

caso a análise realizada de acordo com orientação acima indique desconformidade, elaborem plano de ação para providenciar as adequações contratuais necessárias, que deverão ser realizadas no prazo de 180 dias;

mantenham o resultado da análise de conformidade empreendida em documento formalizado, à disposição dos controles externo e interno;

informem seu órgão de assessoramento jurídico e sua unidade de auditoria interna da análise que está sendo empreendida e do resultado obtido;

determinação análoga deve ser feita ao Dest/MP, ao CNJ e ao CNMP.

Na fiscalização realizada, verificaram-se ainda situações em que o serviço prestado pelo Serpro tinha qualidade incompatível com o previsto no contrato, o que foi objeto de medida corretiva por parte da RFB (Anexo 2, fls. 240v-242, item 4.3). Registre-se que, quando o Serpro não atende a um nível mínimo de serviço contratado pela RFB (ou qualquer outro ente público), independentemente da glosa no contrato, há impacto nas atividades do órgão contratante, que utiliza seus sistemas de informação para prestar serviços à sociedade.

No caso do contrato do Dnit com o Serpro, destacou-se abaixo reportagem obtida na mídia que mostra a insatisfação do então dirigente da Autarquia com os serviços prestados pelo Serpro (fonte: [http://www.claudiohumberto.com.br/colunas\\_anteriores/?dataCalendario=2011-07-13](http://www.claudiohumberto.com.br/colunas_anteriores/?dataCalendario=2011-07-13)):

O diretor, que está afastado de suas funções, disse que o grande problema que enfrenta dentro o Dnit é a falta de estrutura e chamou a atenção para o trabalho do Serviço Federal de Processamento de Dados que, segundo ele, chega a demorar dias para resolver um pequeno problema nos sistemas do órgão. ‘Vocês não sabem o que é o Serpro, às vezes demora oito dias para resolver um problema, foram outros dois anos para dar um programa integrado’, disse.

Em outro caso de grande repercussão na mídia, o Ministro Jorge Hage da CGU responsabilizou o Serpro pelo não funcionamento do sistema Siconv, que poderia ter evitado as fraudes praticadas por ONG nos recentes fatos ocorridos dos ministérios do Turismo e dos Esportes:

Folha/UOL: Mas aí eu volto de novo à pergunta anterior. Nove anos de governo, já não era tempo para ter corrigido?

Jorge Hage: Olha, eu lhe digo que muito foi feito para corrigir nesses nove anos. Lá atrás nós tivemos o decreto 6.170 do presidente Lula, por volta de 2007, criando toda uma nova sistemática para a transferência de dinheiro para Prefeituras e para ONGs. A criação do Siconv, que é o sistema de gestão de convênios, aberto na internet, uma boa parte dele aberto ao público, outra parte aberta aos órgãos de controle foi concebida exatamente para resolver esses problemas. Inclusive fazendo com que desde a proposta de convênio vinda da ONG ou da Prefeitura até a prestação de contas fosse feita on-line. Ocorre que, por inúmeras dificuldades materiais de recursos, o Ministério do Planejamento depende, como todos nós, do Serpro [Serviço Federal de Processamento de Dados]. O Serpro não tem condições de atender às demandas de todos os ministérios da Esplanada, essa que é a verdade. Tudo atrasa. Tudo atrasa. Muitos dos módulos do Siconv até hoje não estão implantados. Muitas dessas situações que aconteceram agora não teriam acontecido se o sistema de controle de convênios estivesse totalmente implantado. Então há dificuldades práticas...

Folha/UOL: O que está faltando? Dinheiro? Dinheiro para implantar?

Jorge Hage: Bom, em alguns casos falta dinheiro. No caso do Serpro eu não sei se falta dinheiro ou se é uma mudança que abra a possibilidade de os órgãos públicos usarem outras empresas, que não o Serpro, que não está dando conta de atender as nossas demandas. Nós da CGU, por exemplo, já desistimos de depender do Serpro para uma série de coisas. Estamos tentando desenvolver os nossos sistemas dentro da própria CGU.

Folha/UOL: Mas quem, então, no governo é responsável para fazer com que ande, com que se implante esse sistema de verificação de convênios de maneira mais rápida então?

Jorge Hage: Não. Agora, no momento, o Ministério do Planejamento está cobrando do Serpro a solução dos problemas dos módulos que ainda faltam.

Folha/UOL: Está cobrando com atraso?

Jorge Hage: Não, vem cobrando já há tempo. Se o Serpro vai conseguir atender ou não, eu não tenho condições de te dizer...

Folha/UOL: Mas o Serpro é do governo, não é Ministro?

Jorge Hage: É do governo. É uma empresa do governo.

Folha/UOL: E não cumpre [suas obrigações]?

Jorge Hage: Não tem dado conta.

(fonte:

[http://tools.folha.com.br/print?url=http%3a%2F%2Fwww1.folha.uol.com.br%2Fpoder%2Fpoderepolitica%2Fjorge\\_hage-2.shtml&site=emcimadahora; sublinhamos](http://tools.folha.com.br/print?url=http%3a%2F%2Fwww1.folha.uol.com.br%2Fpoder%2Fpoderepolitica%2Fjorge_hage-2.shtml&site=emcimadahora; sublinhamos).

Registre-se que a qualidade do serviço prestado pelo Serpro será mais bem avaliada em trabalho futuro, a ser realizado por determinação contida no item 9.12 do Acórdão 906/2009-TCU-Plenário.

Em termos de gestão de TI, cabe ressaltar que o Serpro, enquanto prestador do serviço, não integra a estrutura do tomador do serviço, sendo necessário gerir a relação do contratante (ente da APF) com o contratado (Serpro), que deverá executar as atividades contratadas sob planejamento, coordenação, supervisão e controle do primeiro. A gestão dos processos de trabalho do contratante deve ser executada por servidores ou empregados integrantes da sua estrutura organizacional, nos termos preconizados pelo Decreto-Lei 200/1967, art. 10, § 7º, não podendo ser delegada a funcionários contratados de terceiros, mesmo que a contratada seja o Serpro.

Mais ainda, a transferência da execução dos serviços de tecnologia da informação ao Serpro não desobriga a contratante da APF a possuir, além da gestão da execução desses serviços, estruturas de governança de TI na organização, diversamente do que foi evidenciado no MP, como vemos no excerto do relatório da auditoria para avaliação de controles gerais de TI no ministério, que está transscrito a seguir (Acórdão 2.613/2011-TCU-Plenário):

Não foram definidos processos de gestão de mudanças, gestão de configuração e gestão de incidentes, o que pode acarretar falha na entrega e gestão dos serviços de TI. Considerando os diversos sistemas estruturantes geridos pelo Ministério, a ausência de gestão dos serviços de TI eleva o risco de interrupção ou mau funcionamento desses sistemas. Situação como essa pode configurar prejuízo à eficácia e eficiência na execução das ações do MP. No caso, o Ministério entende, equivocadamente, que são do contratado (no caso o Serpro) a responsabilidade por estes processos. Ocorre que o controle e a responsabilidade pelos processos de gestão e governança de TI são dos gestores do MP e não da contratada. A contratada até pode executar boa parte destes processos, mas ainda assim o contratante é quem deve manter seu controle e supervisão, atividades indelegáveis pelo Decreto-Lei 200/1967, art. 10, §7º

Nesse sentido, propõe-se determinar à SLTI/MP que, em atenção ao Decreto 7.579/2011, art. 4º, V, oriente os órgãos e entidades sob sua jurisdição que (subitem 0):

mesmo que a execução de seus serviços de tecnologia da informação seja transferida mediante contrato ou outro acordo a outra organização pública, como as empresas públicas prestadoras de serviços de tecnologia da informação, as atividades de gestão (planejamento, coordenação, supervisão e controle) de TI devem ser acometidas a pessoas integrantes do quadro permanente, ou, excepcionalmente, a detentores de cargo em comissão, da organização contratante, não podendo ser delegadas a pessoas direta ou indiretamente ligadas à contratada;

a contratação de empresas públicas prestadoras de serviços de tecnologia da informação não afasta a necessidade de a organização contratante manter estrutura de governança de TI própria, que direcione e controle a gestão desses contratos bem como a gestão de todos os processos de TI da organização.

Determinação análoga deve ser feita ao Dest/MP, ao CNJ e ao CNMP.

GOVERNANÇA CORPORATIVA COMO LIMITE PARA O AMADURECIMENTO DA GOVERNANÇA DE TI

Nesta seção discorrer-se-á, de forma sucinta, como a doutrina indica que a ausência de maturidade em governança corporativa limita a maturidade em governança de TI (a linha argumentativa foi produzida com base nos documentos listados no apêndice 0).

A norma brasileira de Governança Corporativa de TI (ABNT NBR ISO/IEC 38.500:2008, p. 3-4) está baseada em normas internacionais de governança corporativa e deixa claro que todos os mecanismos de gerenciamento organizacional estão sujeitos à governança corporativa. Na verdade, há fontes que consideram a governança de TI como sendo uma parte integrante da governança corporativa, como encontramos nos documentos citados no item 2 do apêndice 0.

Nesse sentido, a versão 5 do Cobit (com previsão de lançamento oficial no início do próximo ano), um arcabouço de governança de TI tradicionalmente reconhecido no mundo, já procurou garantir o estabelecimento de uma linguagem comum entre as duas governanças e a consistência desse arcabouço com os padrões de governança corporativa (ver item 3 do apêndice 0).

A governança de TI exerce grande influência sobre as definições da governança corporativa em virtude das possibilidades que a tecnologia da informação oferece de suporte e alavancagem do negócio (ver item 4 do apêndice 0).

Por outro lado, a construção de um modelo de governança de TI sofre a influência dos princípios gerais da governança corporativa, em especial dos princípios da transparência e da prestação de contas (ver item 5 do apêndice 0), e a forma como cada organização implementa esses princípios dirige a maneira de construir o modelo de governança de TI (ver item 6 do apêndice 0).

Portanto, embora possa até haver interesse da alta administração de uma instituição pública em alcançar um bom nível de governança de TI, isso não será possível até que essa mesma alta administração lance os fundamentos e construa as estruturas de governança corporativa necessários para governar todos os seus recursos críticos, tais como pessoas, finanças, TI etc.

Registre-se que, no caso do setor privado, já há evidência de que a adoção de boas práticas de governança corporativa está associada com a obtenção de resultados superiores de desempenho, em termos de retorno sobre o ativo (ver item 6 do apêndice 0).

Considerando que é provável que o mesmo efeito seja passível de ocorrer no setor público, é recomendável orientar a alta administração das instituições públicas federais a adotar as boas práticas de governança corporativa e de TI como forma de alcançar a eficiência constitucionalmente exigida.

Registre-se, por oportuno, que o programa Gespública incluiu no seu ciclo 2010 o item de avaliação ‘Governança Pública e governabilidade’ como critério de avaliação (documento disponível em [https://www.gespública.gov.br/folder\\_premio/pasta.2010-04-26.8934490474/Instrumento\\_ciclo\\_2010\\_22mar.pdf](https://www.gespública.gov.br/folder_premio/pasta.2010-04-26.8934490474/Instrumento_ciclo_2010_22mar.pdf)), evidenciando tratar-se de tema de interesse do poder executivo.

No sentido de contribuir com o aperfeiçoamento das organizações públicas no tocante à governança corporativa, esta Corte já produziu estudo intitulado ‘Critérios gerais de controle interno na administração pública’ (anexo 3, fls. 1-34v) que conclui com proposta de anteprojeto de proposta legislativa para alteração da Lei de Responsabilidade Fiscal.

A proposta (anexo 3, fls. 28v-32) consiste em incluir na LRF uma seção tratando ‘Da gestão de riscos, do Controle Interno e da Governança Corporativa’, positivando no ordenamento jurídico brasileiro boas práticas que contribuem para a boa governança corporativa contidas em marcos de referência, como Coso I e II, reconhecidos mundialmente.

Como não se tem notícia de projeto de lei com conteúdo semelhante e considerando que o estudo pode vir a subsidiar proposta legislativa de deputados e senadores que pode contribuir para uma substancial modernização de nossa legislação, com efeitos diretos na melhoria da governança e gestão pública nas três esferas de governo, será proposto encaminhá-lo às comissões temáticas pertinentes das casas legislativas, quais sejam:

Comissão de Finanças e Tributação da Câmara dos Deputados;

Comissão de Assuntos Econômicos do Senado Federal.

O Acórdão 1.145/2011-TCU-Plenário registrou que a esfera federal já possui um arcabouço normativo voltado para o tema governança de TI. Ainda que incipiente, tal arcabouço foi construído por meio de normas infra-legais (Instruções Normativas, Resoluções etc) e o mesmo pode vir a

ocorrer com os temas gestão de riscos, controle interno e governança corporativa, motivo pelo qual se propõe determinar à Sefti/TCU que encaminhe o estudo elaborado pelo TCU intitulado ‘Critérios gerais de controle interno na administração pública’ à Câmara de Políticas de Gestão, Desempenho e Competitividade do Conselho de Governo, com objetivo de subsidiar possível elaboração de normativo para o poder executivo, com fulcro no Decreto 7.478/2011, art. 2º, II, tratando de gestão de riscos, do controle interno e da governança corporativa (item Error! Reference source not found. Erro! Fonte de referência não encontrada.).

No mesmo sentido, a Sefti/TCU deve encaminhar o estudo ao CNJ e ao CNMP, com o propósito análogo.

Esta proposta de encaminhamento alinha-se aos seguintes objetivos estratégicos do TCU:

I – Contribuir para melhoria da gestão e do desempenho da Administração Pública;

V – Intensificar ações que promovam a melhoria da gestão de riscos e controles internos da Administração Pública;

VI – Aprimorar as ações de controle voltadas à melhoria do desempenho da Administração Pública.

#### COMENTÁRIOS DO GESTOR

A maioria das propostas de deliberação contidas neste relatório consiste de recomendações para que os OGS estabeleçam obrigatoriedade de que os jurisdicionados implantem processos e controles de TI.

As propostas de determinação aos jurisdicionados, por sua vez, contemplam solicitações de informações (SOF/MF e Dest/MP) e determinação de orientação de jurisdicionados, de forma que não se tratam de determinações de alta complexidade nem que possam gerar grande impacto às atividades dos jurisdicionados. Por isso, considerando a existência do disposto nos parágrafos 144-146 das ‘Normas de Auditoria do Tribunal de Contas da União’, aprovada pela Portaria – TCU 168/2011, não se proporá o encaminhamento de uma cópia do relatório preliminar desta auditoria aos gestores para comentários sobre as conclusões e as propostas da equipe.

#### CONCLUSÃO

O TMS 6 – Gestão e uso de TI teve como objetivo avaliar se a gestão e o uso da tecnologia da informação estão de acordo com a legislação e aderentes às boas práticas de governança de TI.

Foram realizados 21 trabalhos, sendo um levantamento em 315 organizações públicas federais, catorze auditorias para avaliação de controles gerais de TI, quatro auditorias em objetos específicos (que avaliaram o Sistema de Acompanhamento de Contratos do Dnit, o sistema informatizado que dá suporte ao Sistema Nacional de Transplantes, as contratações da APF com o Serpro e um contrato de consultoria para segurança da informação no MCT), um monitoramento de sete acordos que deliberaram para onze jurisdicionados, e a consolidação de todos os trabalhos neste relatório.

Após a elaboração de questionário eletrônico para levantamento da situação de governança de TI na APF (doravante chamado perfil GovTI2010), a base de dados com o perfil de governança de TI na APF foi atualizada, apresentando um cenário de baixa maturidade em que se destacam (excerto dos votos do Relator nos catorze processos de avaliação de controles gerais de TI):

a) mais de 60% das organizações não possuem planejamento estratégico de TI;

b) algumas organizações continuam a ter sua TI totalmente controlada por pessoas estranhas a seus quadros de pessoal;

c) são graves os problemas de segurança da informação, já que informações críticas não são protegidas adequadamente;

d) metade das organizações não possui método ou processo para desenvolvimento de softwares e para aquisição de bens e serviços de informática, o que gera riscos de irregularidades em contratações;

e) a atuação sistemática da alta administração com respeito à TI ainda é incipiente;

f) mais da metade das organizações está no estágio inicial de governança de TI, e apenas 5% encontram-se em estágio aprimorado.

Com respeito à avaliação de controles gerais de TI, foram elaboradas as matrizes de planejamento e possíveis achados, treinados 28 auditores e realizadas catorze auditorias.

Quadro 15 – iGovTI declarado x avaliado pelo TCU

Sigla	Organização	iGovTI declarado		iGovTI recalculado pelo TCU		Variação
AmE	AMAZONAS DISTRIBUIDORA DE ENERGIA S/A	31,70%	Inicial	24,67%	Inicial	-7,04%
Anatel	AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES	54,04%	Intermediário	22,31%	Inicial	-31,73%
Dnit	DEPARTAMENTO NACIONAL DE INFRAESTRUTURA DE TRANSPORTES	27,26%	Inicial	24,37%	Inicial	-2,89%
Dnocs	DEPARTAMENTO NACIONAL DE OBRAS CONTRA AS SECAS	37,50%	Inicial	24,91%	Inicial	-12,59%
Finep	FINANCIADORA DE ESTUDOS E PROJETOS	39,89%	Inicial	33,97%	Inicial	-5,92%
FNDE	FUNDO NACIONAL DE DESENVOLVIMENTO DA EDUCAÇÃO	59,22%	Intermediário	43,99%	Intermediário	-15,23%
Ibama	INSTITUTO BRASILEIRO DO MEIO AMBIENTE E DOS RECURSOS NATURAIS RENOVÁVEIS	26,46%	Inicial	22,56%	Inicial	-3,90%
MCT	MINISTÉRIO DA CIÊNCIA E TECNOLOGIA	42,61%	Intermediário	21,58%	Inicial	-21,03%
MP	MINISTÉRIO DO PLANEJAMENTO, ORÇAMENTO E GESTÃO	31,71%	Inicial	27,26%	Inicial	-4,45%
MRE	MINISTÉRIO DAS RELAÇÕES EXTERIORES	51,19%	Intermediário	34,33%	Inicial	-16,86%
MS	MINISTÉRIO DA SAÚDE	30,07%	Inicial	23,85%	Inicial	-6,22%
Susep	SUPERINTENDÊNCIA DE SEGUROS PRIVADOS	8,97%	Inicial	9,69%	Inicial	0,71%
TRT-2-SP	TRIBUNAL REGIONAL DO TRABALHO 2 <sup>a</sup> REGIÃO/SP	33,78%	Inicial	26,78%	Inicial	-7,00%
TRT-4-RS	TRIBUNAL REGIONAL DO TRABALHO 4 <sup>a</sup> REGIÃO/RS	62,62%	Aprimorado	45,93%	Intermediário	-16,69%

Essas catorze auditorias evidenciaram que a situação de governança de TI é pior em treze dos catorze auditados, sugerindo que na APF a situação também pode ser pior que a apresentada por meio da tabulação dos dados declarados pelos jurisdicionados no perfil GovTI2010 (Acórdão 2.308/2010-TCU-Plenário). O Quadro 15 apresenta a comparação de pares de valores do iGovTI2010 para os catorze auditados, sendo um dos valores calculado com os dados oferecidos pelos jurisdicionados e outro calculado com base na avaliação realizada pelos auditores do TCU após a solicitação das evidências que suportariam as declarações dos gestores.

A Figura 2 apresenta o gráfico da variação do iGovTI (avaliado pelo TCU menos o declarado) contra o valor do iGovTI2010 declarado, e a análise de regressão linear dos valores sugere que quanto maior é a autoavaliação da instituição, maior é a queda percentual dessa avaliação depois de aplicados os critérios das auditorias do TCU.

Isto sugere que o iGovTI2010 é mais confiável na faixa inicial e menos confiável nas faixas aprimorada e intermediária. Entretanto não é possível calcular um deflator geral a partir da amostra de catorze instituições visto que: a) a amostra não pode ser considerada representativa da população, pois não foi selecionada segundo critérios estatísticos de amostragem; b) não há razões para crer que o grau de otimismo na autoavaliação seja homogêneo ou proporcional à sua autoavaliação.

Em que pese a variação de confiabilidade, típica de dados obtidos por meio declaratório, o iGovTI se mostra útil três razões principais: a) estabelece um arcabouço de boas práticas que deixa mais claro para os gestores o que se espera deles e como a sua gestão será avaliada; b) a maioria das instituições encontra-se na faixa mais confiável do iGovTI (faixa inicial); c) mesmo com a revisão do iGovTI para baixo após as auditorias, as instituições com índices corrigidos mais elevados de fato apresentam algumas práticas de governança implantadas, reconhecimento esse que serve para estimular os respectivos gestores a prosseguirem no esforço de melhorar a sua governança de TI.

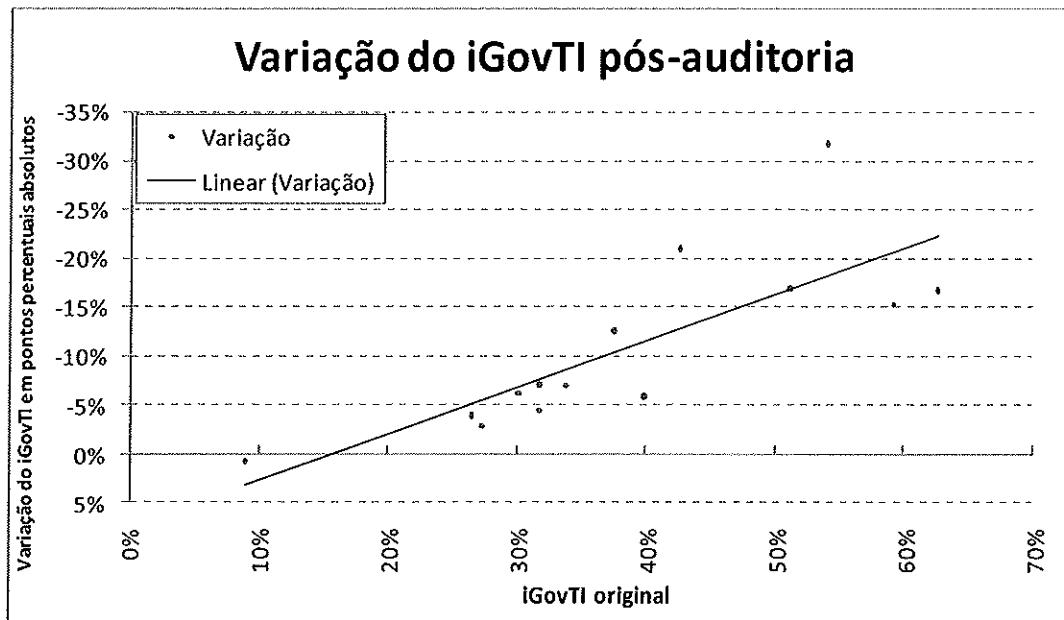


Figura 2 – Variação do iGovTI após a auditoria do TCU

Desta forma, evidenciou-se fragilidade da governança de TI nos catorze auditados por meio da evidenciação da ausência ou deficiência de controles gerais de TI.

Em outra linha de investigação do TMS, a avaliação de quatro objetos específicos de TI permitiu identificar consequências da ausência ou deficiência dos controles gerais de TI. Assim evidenciou-se, por exemplo, que:

a ausência de controles gerais de segurança da informação no Dnit contribui para diversas vulnerabilidades, inclusive já exploradas em sede de fraude no Sistema de Acompanhamento de Contratos da Autarquia, o qual gere R\$ 24 bilhões em contratos ativos, possui (Acórdão 2.831/2011-TCU-Plenário);

a ausência de processo de software no Ministério da Saúde contribui para que o código do sistema que suporta o programa nacional de transplantes não implemente as regras de negócio na forma prevista na legislação, com consequências que podem afetar inclusive a credibilidade do programa (TC 029.074/2010-0);

o não funcionamento do comitê de TI no Ministério da Ciência e Tecnologia impediu a avaliação de produtos de um contrato de consultoria para implantação de controles gerais de segurança da informação, acarretando, além de indícios de pagamento indevido (em apuração), ausência de benefício para o órgão devido a não implantação, até o fim da auditoria, dos controles (TC 029.120/2010-1).

É obrigação dos gestores da alta administração adotarem as medidas necessárias à implantação dos controles gerais de TI que integram uma boa estrutura de governança de TI, evitando consequências como as acima citadas. Esse foi o tom de dois eventos promovidos em 2011 pelo TCU, quando foi convidado o mais alto dirigente em cada instituição da Administração Pública Federal (poderes Executivo, Legislativo e Judiciário, além do Ministério Público) para discutir ‘O papel da Alta Administração na Governança de TI’ (eventos realizados em 16/6/2011 e 4/8/2011, com mais de trezentos participantes em cada um deles).

No monitoramento do cumprimento de determinações e recomendações formuladas por meio de diversos acórdãos prolatados de 2004 a 2009, aos órgãos governantes superiores de TI, realizado no âmbito das ações relativas ao presente TMS, identificou-se oportunidade de melhoria na atuação daqueles órgãos (Acórdão 1.145/2011-TCU-Plenário). Em especial, faz-se necessária maior atuação das auditorias internas, por meio da inclusão dos temas de TI nas suas matrizes de risco.

Ainda que os OGS tenham atuado por meio da implantação de algumas recomendações a eles dirigidas, não se evidenciou melhora substantiva na situação de governança de TI nos entes da APP.

Os próprios gestores públicos confirmaram que suas organizações são dependentes dos sistemas informatizados para a consecução de seus objetivos institucionais, (51% para imediatamente de prestar serviços aos cidadãos se seus sistemas sofrerem interrupção), de forma que a TI deve ser tema prioritário na fiscalização realizada pelas auditorias internas.

Apresenta-se na Figura 3 um gráfico com nova análise dos dados coletados a partir do perfil GovTI2010, em que se posicionaram as organizações públicas pesquisadas por meio do seu iGovTI2010 e do seu orçamento total administrado.

Os valores de orçamento administrado foram obtidos mediante a extração, a partir do sistema Siafi, da receita (29 registros) e da despesa (4.034 registros) totais realizadas em 2010 (procedimento realizado pela Diretoria de Gestão de Informações Estratégicas do TCU), detalhadas por órgão e UG, e pelo pareamento entre as unidades referidas na extração do Siafi e aquelas constantes do levantamento que gerou o perfil GovTI2010.

O conceito de orçamento administrado refere-se ao volume total de recursos (receitas ou despesas) administrado pela unidade. Considera-se que, quanto maior o orçamento administrado por uma dada unidade, maior é a sua importância no cenário nacional e maior a relevância e criticidade da TI que suporta a sua execução.

Com respeito aos aspectos legais das contratações analisadas, verificou-se a forte tendência de contratação por meio do Sistema de Registro de Preços (SRP). O fato seria um bom indicativo se esse sistema não estivesse sendo utilizado de forma distorcida, conforme o TCU já havia detectado (Acórdão 1.487/2007-TCU-Plenário), pois o planejamento conjunto para a criação de uma ata, que deveria ser a regra, é a exceção, enquanto a adesão tardia (carona), que deveria ser a exceção, tornou-se prática comum. Nesse sentido, entende-se que as orientações propostas mitigarão, já no curto prazo, a continuidade de ocorrências de desconformidade.

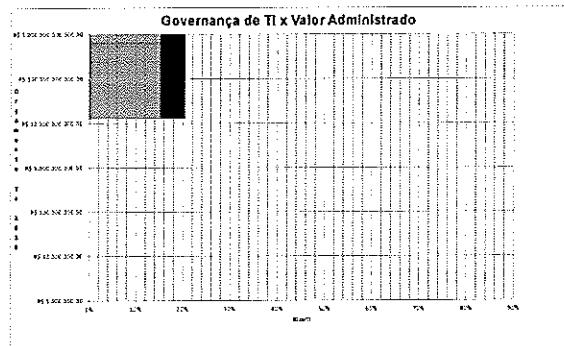


Figura 3 – Avaliação de riscos: iGovTI2010 x Valor Administrado

O mesmo ocorre com as contratações dos entes da APF com empresas públicas prestadoras de serviços de TI. Tais contratações não são excepcionalizadas da legislação, e o conjunto de orientações proposto contribuirá para que a situação esteja conforme os preceitos legais e as boas práticas em contratações.

Outro assunto analisado foi o limite imposto pela governança corporativa para o amadurecimento da governança de TI. Produziu-se argumentação no sentido de que a ausência de maturidade em governança corporativa limita a maturidade em governança de TI, e indicou-se, às comissões temáticas pertinentes das casas legislativas e à CGDC, estudo realizado pelo TCU contendo

proposta de anteprojeto de lei para alteração da LRF por meio da inclusão de dispositivos que visam ao fortalecimento da governança corporativa nos entes públicos.

O conjunto de recomendações propostas aos órgãos governantes superiores, fundamental para o aperfeiçoamento da governança de TI na APF, apresenta-se extenso e complexo, motivo pelo qual se propõe determinar à Sefti/TCU que promova a divulgação, inclusive por meio de eventos, dessas orientações, como forma de mitigar os riscos da sua implementação.

O conjunto de orientações propostas abrange a totalidade dos órgãos e entidades dos poderes executivo e judiciário, além do ministério público, por meio dos comandos dirigidos aos OGS. Entretanto as casas legislativas e o TCU, mesmo não estando na jurisdição de nenhum OGS, também devem primar pelo aperfeiçoamento das governanças de TI e corporativa, motivo pelo qual serão propostas recomendações para que essas três casas avaliem todas as orientações expedidas no acórdão que vier a ser proferido e adotem as medidas necessárias a sua implementação.

As recomendações supra se alinham aos objetivos estratégicos ‘Instituir modelo de governança corporativa e gestão estratégica’ e ‘Promover a melhoria da governança no TCU’ constantes, respectivamente, da agenda estratégica do Senado Federal (síntese disponível em <http://www.senado.gov.br/noticias/veja-a-sintese-da-agenda-estrategica-da-administracao-do-senado-federal.aspx>) e do Plano Estratégico do TCU em vigor (disponível em [http://portal2.tcu.gov.br/portal/page/portal/TCU/planejamento\\_gestao/planejamento2011/pet.pdf](http://portal2.tcu.gov.br/portal/page/portal/TCU/planejamento_gestao/planejamento2011/pet.pdf)).

Por fim, considerando que o referencial estratégico em vigor do TCU contempla como objetivo estratégico ‘Contribuir para o aperfeiçoamento da gestão e do desempenho da Administração Pública’, o qual tem como um de seus indicadores o ‘índice de governança corporativa dos órgãos da Administração Pública Federal’, considerando também que as unidades de auditoria interna são atores essenciais à boa governança de TI, e considerando ainda as deficiências dos sistemas de controles internos (controles internos dos gestores e atuação das unidades de auditoria interna) conforme evidenciado neste TMS, há espaço para que o TCU contribua para o cumprimento do comando previsto na Constituição Federal, art. 74, mas que somente poderá ocorrer mediante trabalho de avaliação sistematizada dos sistemas de controles internos dos poderes.

## PROPOSTA DE ENCAMINHAMENTO

Ante todo o exposto, somos pelo encaminhamento dos autos ao gabinete do Ministro-Relator Aroldo Cedraz, com as propostas a seguir:

Recomendar, com fulcro na Lei 8.443/1992, art. 43, inciso I, c/c RITCU, art. 250, inciso III, à Câmara de Políticas de Gestão, Desempenho e Competitividade (CGDC) do Conselho de Governo que:

em atenção Decreto-Lei 200/1967, art. 6º, inciso I, e art. 7º, normatize a obrigatoriedade de que todos os entes sob sua jurisdição estabeleçam processo de planejamento estratégico institucional, observando as boas práticas sobre o tema, a exemplo do critério de avaliação 2 do Gespública, contemplando, pelo menos (subitem 0):

elaboração, com participação de representantes dos diversos setores da organização, de um documento que materialize o plano estratégico institucional de longo prazo, contemplando, pelo menos, objetivos, indicadores e metas para a organização;

aprovação, pela mais alta autoridade da organização, do plano estratégico institucional; desdobramento do plano estratégico pelas unidades executoras;

divulgação do plano estratégico institucional para conhecimento dos cidadãos brasileiros, exceto nos aspectos formalmente declarados sigilosos ou restritos;;

acompanhamento periódico do alcance das metas estabelecidas, para correção de desvios; divulgação interna e externa do alcance das metas, ou dos motivos de não ter alcançado;

em atenção Decreto-Lei 200/1967, art. 6º, inciso I, e art. 7º, normatize a obrigatoriedade de que todos os entes sob sua jurisdição estabeleçam processo de planejamento estratégico de TI, observando

as boas práticas sobre o tema, a exemplo do processo ‘PO1 – Planejamento Estratégico de TI’ do Cobit 4.1, contemplando, pelo menos (subitem 0):

elaboração, com participação de representantes dos diversos setores da organização, de um documento que materialize o plano estratégico de TI, contemplando, pelo menos:

objetivos, indicadores e metas para a TI organizacional, sendo que os objetivos devem estar explicitamente alinhados aos objetivos de negócio constantes do plano estratégico institucional;

alocação de recursos (financeiros, humanos, materiais etc);

estratégia de terceirização;

aprovação, pela mais alta autoridade da organização, do plano estratégico de TI;

desdobramento do plano estratégico de TI pelas unidades executoras;

divulgação do plano estratégico de TI para conhecimento dos cidadãos brasileiros, exceto nos aspectos formalmente declarados sigilosos ou restritos;

acompanhamento periódico do alcance das metas estabelecidas, para correção de desvios;

divulgação interna e externa do alcance das metas, ou os motivos de não as ter alcançado;

em atenção ao Decreto-Lei 200/1967, art. 6º, V, estabeleça, normativamente para todos os entes sob sua jurisdição, a obrigatoriedade de a alta administração implantar uma estrutura de controles internos, mediante a definição de atividades de controle em todos os níveis da organização para mitigar os riscos de suas atividades no processo de planejamento estratégico institucional (subitem 0).

Recomendar, com fulcro na Lei 8.443/1992, art. 43, inciso I, c/c RITCU, art. 250, inciso III, à Secretaria de Logística e Tecnologia da Informação (SLTI/MP) que:

normatize a obrigatoriedade de que os entes sob sua jurisdição estabeleçam comitês de TI, observando as boas práticas sobre o tema, a exemplo do Cobit 4.1, PO4.2 – comitê estratégico de TI e PO4.3 – comitê diretor de TI (subitem 0);

orienta os órgãos e entidades sob sua jurisdição a realizar avaliação quantitativa e qualitativa do pessoal do setor de TI, de forma a delimitar as necessidades de recursos humanos necessárias para que estes setores realizem a gestão das atividades de TI da organização (subitem 0);

elabore um modelo de processo de software para os entes sob sua jurisdição, observando as boas práticas sobre o tema (e.g., NBR ISO/IEC 12.207 e 15.504, MPS.BR, CMMI; subitem 0);

estabeleça a obrigatoriedade de que os entes sob sua jurisdição formalizem um processo de software para si, observando as boas práticas sobre o tema (e.g., NBR ISO/IEC 12.207 e 15.504, MPS.BR, CMMI; subitem 0);

elabore um modelo de estrutura de gerenciamento de projetos para os entes sob sua jurisdição, observando as boas práticas sobre o tema (e.g., PMBoK; subitem 0);

estabeleça a obrigatoriedade de que os entes sob sua jurisdição formalizem um processo de gerenciamento de projetos para si, observando as boas práticas sobre o tema (e.g., PMBoK; subitem 0);

elabore um modelo de processo de gestão de serviços para os entes sob sua jurisdição que inclua, pelo menos, gestão de configuração, gestão de incidentes e gestão de mudança, observando as boas práticas sobre o tema (e.g., NBR ISO/IEC 20.000, Itil; subitem 0);

estabeleça a obrigatoriedade de que os entes sob sua jurisdição formalizem processos de gestão de serviços para si, incluindo, pelo menos, gestão de configuração, gestão de incidentes e gestão de mudança, observando as boas práticas sobre o tema (e.g., NBR ISO/IEC 20.000, Itil; subitem 0);

em atenção ao Decreto-Lei 200/1967, art. 6º, V, estabeleça, normativamente para todos os entes sob sua jurisdição, a obrigatoriedade de a alta administração implantar uma estrutura de controles internos mediante a definição de atividades de controle em todos os níveis da organização para mitigar os riscos de suas atividades, pelo menos nos seguintes processos (subitem 0):

planejamento estratégico de TI;

funcionamento dos comitês de TI;

processo orçamentário de TI;

processo de software;

gerenciamento de projetos;

gerenciamento de serviços de TI;

segurança da informação;  
gestão de pessoal de TI;  
contratação e gestão de soluções de TI;  
monitóriação do desempenho da TI organizacional.

Determinar, com fulcro na Lei 8.443/1992, art. 43, inciso I, c/c RITCU, art. 250, inciso II, à Secretaria de Logística e Tecnologia da Informação (SLTI/MP) que:

em atenção ao previsto no Decreto 7.579/2011, art. 4º, V, oriente os entes sob sua jurisdição sobre a necessidade de vincular seus contratos de serviços de desenvolvimento ou manutenção de software a um processo de software, pois, sem esta vinculação, o objeto do contrato não estará precisamente definido, em desconformidade com o disposto na Lei 8.666/1993, art. 6º, inciso IX (subitem 0);

em atenção ao disposto no Decreto 1.094/1994, art. 2º, inciso I, oriente os órgãos e entidades sob sua jurisdição para que (subitem 0):

ao realizarem licitação com finalidade de criar ata de registro de preços atentem que:

devem fundamentar formalmente a criação de ata de registro de preços, e.g., por um dos incisos do art. 2º do Decreto 3.931/2001 (Acórdão 2.401/2006-TCU-Plenário);

devem praticar todos os atos descritos no Decreto 3.931/2001, art. 3º, § 2º, em especial o previsto no seu inciso I, que consiste em ‘convidar mediante correspondência eletrônica ou outro meio eficaz, os órgãos e entidades para participarem do registro de preços’;

o planejamento da contratação é obrigatório, sendo que se o objeto for solução de TI, caso seja integrante do Sisp, deve executar o processo de planejamento previsto na IN – SLTI/MP 4/2010 (IN – SLTI/MP 4/2010, art. 18, inciso III) ou, caso não o seja, deve realizar os devidos estudos técnicos preliminares (Lei 8.666/1993, art. 6º, inciso IX);

a fixação, no termo de convocação, de quantitativos (máximos) a serem contratados por meio dos contratos derivados da ata de registro de preços, previstos no Decreto 3.931/2001, art. 9º, inciso II, é obrigação e não faculdade do gestor (Acórdão 991/2009-TCU-Plenário, Acórdão 1.100/2007-TCU-Plenário e Acórdão 4.411/2010-TCU-2ª Câmara);

em atenção ao princípio da vinculação ao instrumento convocatório (Lei 8.666/1993, art. 3º, caput), devem gerenciar a ata de forma que a soma dos quantitativos contratados em todos os contratos derivados da ata não supere o quantitativo máximo previsto no edital;

quando realizarem adesão à ata de registro de preços atentem que:

o planejamento da contratação é obrigatório, sendo que se o objeto for solução de TI, caso seja integrante do Sisp, deve executar o processo de planejamento previsto na IN – SLTI/MP 4/2010 (IN – SLTI/MP 4/2010, art. 18, inciso III) ou, caso não o seja, realizar os devidos estudos técnicos preliminares (Lei 8.666/1993, art. 6º, inciso IX);

devem demonstrar formalmente a vantajosidade da adesão, nos termos do Decreto 3.931/2001, art. 8º;

as regras e condições estabelecidas no certame que originou a ata de registro de preços devem ser conformes as necessidades e condições determinadas na etapa de planejamento da contratação (Lei 8.666/1993, art. 6º, inciso IX, alínea d, c/c o art. 3º, § 1º, inciso I, e Lei 10.520/2002, art. 3º, inciso II);

em atenção ao Decreto 7.579/2011, art. 4º, V, oriente os órgãos e entidades sob sua jurisdição para que, caso possuam contratos com empresas públicas prestadoras de serviços de TI (subitem 0):

analisem a conformidade dos termos do contrato e do projeto básico e verifiquem se:

foi realizado o adequado planejamento da contratação, consistindo na execução do processo de planejamento previsto na IN – SLTI/MP 4/2010 se for integrante do Sisp (IN – SLTI/MP 4/2010, art. 18, inciso II) ou, caso não o seja, se foram realizados os devidos estudos técnicos preliminares (Lei 8.666/1993, art. 6º, inciso IX);

as especificações do objeto são precisas e suficientes, em conformidade com a Lei 8.666/1993, art. 6º, IX;

os critérios de mensuração dos serviços são precisos e suficientes, de acordo com o determinado na Lei 8.666/1993, art. 6º, IX, e (também necessários de acordo com a IN – SLTI 4/2010, art. 14, II, a);

a metodologia de avaliação da adequação dos produtos é precisa e suficiente, de acordo com o determinado na Lei 8.666/1993, art. 6º, IX, e (também necessária de acordo com a IN – SLTI 4/2010, art. 14, II, c);

as cláusulas de penalidades contidas na Lei 8.666/1993, art. 87, de acordo com o determinado na Lei 8.666/1993, art. 55, VII e VIII, são detalhadas e atendem aos princípios da razoabilidade, proporcionalidade e prudência (e também o previsto na IN – SLTI 4/2010, art. 15, III, h);

o modelo de pagamento é vinculado a resultados, obedecendo ao princípio constitucional da eficiência (e também ao previsto no Decreto 2.271/1997, art. 3º, § 1º, e na IN – SLTI 4/2010, art. 15, §§ 2º e 3º);

a justificativa dos preços contratados é adequadamente fundamentada em arrazoada pesquisa de mercado, de acordo com o determinado na Lei 8.666/1993, art. 26, III, inclusive com a análise da planilha de composição de custos dos serviços, necessária segundo a Lei 8.666/1993, art. 7º, § 2º, II;

caso a análise realizada de acordo com orientação acima indique desconformidade, elaborem plano de ação para providenciar as adequações contratuais necessárias, que deverão ser realizadas no prazo de 180 dias;

mantenham o resultado da análise de conformidade empreendida em documento formalizado, à disposição dos controles externo e interno;

informem seu órgão de assessoramento jurídico e sua unidade de auditoria interna da análise que está sendo empreendida e do resultado obtido;

em atenção ao Decreto 7.579/2011, art. 4º, V, oriente os órgãos e entidades sob sua jurisdição que (subitem 0):

mesmo que a execução de seus serviços de tecnologia da informação seja transferida mediante contrato ou outro acordo a outra organização pública, como as empresas públicas prestadoras de serviços de tecnologia da informação, as atividades de gestão (planejamento, coordenação, supervisão e controle) de TI devem ser acometidas a pessoas integrantes do quadro permanente, ou, excepcionalmente, a detentores de cargo em comissão, da organização contratante, não podendo ser delegadas a pessoas direta ou indiretamente ligadas à contratada;

a contratação de empresas públicas prestadoras de serviços de tecnologia da informação não afasta a necessidade de a organização contratante manter estrutura de governança de TI própria, que direcione e controle a gestão desses contratos bem como a gestão de todos os processos de TI da organização.

Recomendar, com fulcro na Lei 8.443/1992, art. 43, inciso I, c/c RITCU, art. 250, inciso III, ao Ministério do Planejamento, Orçamento e Gestão que:

em atenção ao Decreto 5.707/2006, art. 5º, § 2º, c/c o art. 1º, III, discipline a forma de acesso às funções de liderança nos setores de Tecnologia da Informação, considerando as competências multidisciplinares necessárias para estas funções, que incluem, mas não se limitam a conhecimentos em TI (subitem 0).

Recomendar, com fulcro na Lei 8.443/1992, art. 43, inciso I, c/c RITCU, art. 250, inciso III, à Secretaria de Orçamento Federal (SOF/MP) que:

implante controles para mitigar os riscos de ocorrência de propostas orçamentárias que indevidamente não tenham previsão de despesas com tecnologia da informação (subitem 0);

com base no disposto na Lei 10.180/2001, art. 8º, II, c/c Decreto 7.063/2010, art. 17, II, normatize a obrigatoriedade de que todos os entes sob sua jurisdição estabeleçam processo de trabalho formal para elaboração e acompanhamento da execução do orçamento, contemplando, pelo menos, a obrigatoriedade de que (subitem 0):

a solicitação do orçamento de TI seja feita com base nas estimativas de custos das atividades que pretendam executar, alinhadas aos objetivos do negócio da organização;

haja acompanhamento, ao longo do exercício financeiro, dos gastos efetuados especificamente com TI.

Determinar, com fulcro na Lei 8.443/1992, art. 43, inciso I, c/c RITCU, art. 250, inciso II, à Secretaria de Orçamento Federal (SOF/MP) que, em atenção ao Decreto-Lei 200/1967, art. 75, encaminhe, à Secretaria de Fiscalização de Tecnologia da Informação do Tribunal de Contas da União (Sefti/TCU):

no prazo de quinze dias após o envio do projeto da Lei de Diretrizes Orçamentárias ao Congresso Nacional, as medidas adotadas para permitir a identificação clara, objetiva e transparente da previsão dos gastos em TI no Orçamento Geral da União ou, alternativamente, normatize o processo de trabalho para obtenção de ditas informações, valendo-se da competência prevista no Decreto 7.063/2010, art. 17, II (subitem 0);

no prazo de quinze dias após o envio do Projeto da Lei Orçamentária Anual (PLOA) ao Congresso Nacional, relação da previsão das despesas com TI que constam do PLOA, em meio magnético, na forma de banco de dados editável ou planilha eletrônica, no maior detalhamento possível, preferencialmente no formato encaminhado por meio do Ofício 06/SECAD/SOF/MP, de 25/2/2010, ou, alternativamente, disponibilize funcionalidade nos seus sistemas informatizados para que a Sefti/TCU possa acessar os dados requeridos para o atendimento da determinação (subitem 0);

no prazo de quinze dias após a publicação da Lei Orçamentária Anual (LOA), relação da previsão das despesas com TI que constam da LOA, em meio magnético, na forma de banco de dados editável ou planilha eletrônica, no maior detalhamento possível, preferencialmente no formato encaminhado por meio do Ofício 06/SECAD/SOF/MP, de 25/2/2010, ou, alternativamente, disponibilize funcionalidade nos seus sistemas informatizados para que a Sefti/TCU possa acessar os dados requeridos para o atendimento da determinação (subitem 0).

Determinar, com fulcro na Lei 8.443/1992, art. 43, inciso I, c/c RITCU, art. 250, inciso II, à Departamento de Coordenação e Governança das Estatais (Dest/MP) que:

em atenção ao Decreto-Lei 200/1967, art. 75, encaminhe, à Secretaria de Fiscalização de Tecnologia da Informação do Tribunal de Contas da União (Sefti/TCU):

no prazo de quinze dias após o envio do Projeto da Lei Orçamentária Anual (PLOA) ao Congresso Nacional, relação da previsão das despesas com TI que constam do PLOA, em meio magnético, na forma de banco de dados editável ou planilha eletrônica, no maior detalhamento possível, preferencialmente no formato encaminhado por meio do Ofício 163/2010/MP/SE/DEST, de 23/2/2010, ou, alternativamente, disponibilize funcionalidade nos seus sistemas informatizados para que a Sefti/TCU possa acessar os dados requeridos para o atendimento da determinação (subitem 0);

no prazo de quinze dias após a publicação da Lei Orçamentária Anual (LOA), relação da previsão das despesas com TI que constam da LOA, em meio magnético, na forma de banco de dados editável ou planilha eletrônica, no maior detalhamento possível, preferencialmente no formato encaminhado por meio do Ofício 163/2010/MP/SE/DEST, de 23/2/2010, ou, alternativamente, disponibilize funcionalidade nos seus sistemas informatizados para que a Sefti/TCU possa acessar os dados requeridos para o atendimento da determinação (subitem 0);

em atenção ao disposto no Decreto 7.063/2010, art. 6º, inciso XII, oriente as entidades sob sua jurisdição para que (subitem 0):

ao realizarem licitação com finalidade de criar ata de registro de preços atentem que:

devem fundamentar formalmente a criação de ata de registro de preços, e.g., por um dos incisos do art. 2º do Decreto 3.931/2001 (Acórdão 2.401/2006-TCU-Plenário);

devem praticar todos os atos descritos no Decreto 3.931/2001, art. 3º, § 2º, em especial o previsto no seu inciso I, que consiste em ‘convidar mediante correspondência eletrônica ou outro meio eficaz, os órgãos e entidades para participarem do registro de preços’;

o planejamento da contratação é obrigatório, sendo obrigatória a realização dos devidos estudos técnicos preliminares (Lei 8.666/1993, art. 6º, inciso IX);

a fixação, no termo de convocação, de quantitativos (máximos) a serem contratados por meio dos contratos derivados da ata de registro de preços, previstos no Decreto 3.931/2001, art. 9º, inciso

II, é obrigação e não faculdade do gestor (Acórdão 991/2009-TCU-Plenário, Acórdão 1.100/2007-TCU-Plenário e Acórdão 4.411/2010-TCU-2ª Câmara);

em atenção ao princípio da vinculação ao instrumento convocatório (Lei 8.666/1993, art. 3º, caput), devem gerenciar a ata de forma que a soma dos quantitativos contratados em todos os contratos derivados da ata não supere o quantitativo máximo previsto no edital;

quando realizarem adesão à ata de registro de preços atentem que:

o planejamento da contratação é obrigatório, sendo obrigatória a realização dos devidos estudos técnicos preliminares (Lei 8.666/1993, art. 6º, inciso IX);

devem demonstrar formalmente a vantajosidade da adesão, nos termos do Decreto 3.931/2001, art. 8º;

as regras e condições estabelecidas no certame que originou a ata de registro de preços devem ser conformes as necessidades e condições determinadas na etapa de planejamento da contratação (Lei 8.666/1993, art. 6º, inciso IX, alínea d, c/c o art. 3º, § 1º, inciso I, e Lei 10.520/2002, art. 3º, inciso II);

em atenção ao disposto no Decreto 7.063/2010, art. 6º, inciso XII, oriente as entidades sob sua jurisdição para que, caso possuam contratos com empresas públicas prestadoras de serviços de TI (subitem 0):

analisem a conformidade dos termos do contrato e do projeto básico e verifiquem se:

foi realizado o adequado planejamento da contratação, consistindo na execução do processo de planejamento previsto na IN – SLTI/MP 4/2010 se for integrante do Sisp (IN – SLTI/MP 4/2010, art. 18, inciso II) ou, caso não o seja, se foram realizados os devidos estudos técnicos preliminares (Lei 8.666/1993, art. 6º, inciso IX);

as especificações do objeto são precisas e suficientes, em conformidade com a Lei 8.666/1993, art. 6º, IX;

os critérios de mensuração dos serviços são precisos e suficientes, de acordo com o determinado na Lei 8.666/1993, art. 6º, IX, e (também necessários de acordo com a IN – SLTI 4/2010, art. 14, II, a);

a metodologia de avaliação da adequação dos produtos é precisa e suficiente, de acordo com o determinado na Lei 8.666/1993, art. 6º, IX, e (também necessária de acordo com a IN – SLTI 4/2010, art. 14, II, c);

as cláusulas de penalidades contidas na Lei 8.666/1993, art. 87, de acordo com o determinado na Lei 8.666/1993, art. 55, VII e VIII, são detalhadas e atendem aos princípios da razoabilidade, proporcionalidade e prudência (e também o previsto na IN – SLTI 4/2010, art. 15, III, h);

o modelo de pagamento é vinculado a resultados, obedecendo ao princípio constitucional da eficiência (e também ao previsto no Decreto 2.271/1997, art. 3º, § 1º, e na IN – SLTI 4/2010, art. 15, §§ 2º e 3º);

a justificativa dos preços contratados é adequadamente fundamentada em arrazoada pesquisa de mercado, de acordo com o determinado na Lei 8.666/1993, art. 26, III, inclusive com a análise da planilha de composição de custos dos serviços, necessária segundo a Lei 8.666/1993, art. 7º, § 2º, II;

caso a análise realizada de acordo com orientação acima indique desconformidade, elaborem plano de ação para providenciar as adequações contratuais necessárias, que deverão ser realizadas no prazo de 180 dias;

mantenham o resultado da análise de conformidade empreendida em documento formalizado, à disposição dos controles externo e interno;

informem seu órgão de assessoramento jurídico e sua unidade de auditoria interna da análise que está sendo empreendida e do resultado obtido;

em atenção ao disposto no Decreto 7.063/2010, art. 6º, inciso XII, oriente as entidades sob sua jurisdição que (subitem 0):

mesmo que a execução de seus serviços de tecnologia da informação seja transferida mediante contrato ou outro acordo a outra organização pública, como as empresas públicas prestadoras de

serviços de tecnologia da informação, as atividades de gestão (planejamento, coordenação, supervisão e controle) de TI devem ser acometidas a pessoas integrantes do quadro permanente, ou, excepcionalmente, a detentores de cargo em comissão, da organização contratante, não podendo ser delegadas a pessoas direta ou indiretamente ligadas à contratada;

a contratação de empresas públicas prestadoras de serviços de tecnologia da informação não afasta a necessidade de a organização contratante manter estrutura de governança de TI própria, que direcione e controle a gestão desses contratos bem como a gestão de todos os processos de TI da organização.

Recomendar, com fulcro na Lei 8.443/1992, art. 43, inciso I, c/c RITCU, art. 250, inciso III, ao Gabinete de Segurança Institucional da Presidência da república (GSI/PR) que:

em atenção à Lei 10.168/2003, art. 6º, IV, articule-se com as escolas de governo, notadamente à Enap, a fim de ampliar a oferta de ações de capacitação em segurança da informação para os entes sob sua jurisdição (subitem 0);

em atenção a Lei 10.168/2003, art. 6º, IV, oriente os órgãos e entidades sob sua jurisdição que a implantação dos controles gerais de segurança da informação positivados nas normas do GSI/PR não é faculdade, mas obrigação da alta administração, e sua não implantação sem justificativa é passível da sanção prevista na Lei 8.443/1992, art. 58, II (subitem 0);

reveja a Norma Complementar 4/IN01/DSIC/GSIPR, uma vez que aborda o tema gestão de riscos considerando apenas ativo de informação e não ativo em sentido amplo, como o faz a NBR ISO/IEC 27.002 no item 7.1.1 (subitem 0).

Recomendar, com fulcro na Lei 8.443/1992, art. 43, inciso I, c/c RITCU, art. 250, inciso III, ao Comitê Gestor da Política Nacional de Desenvolvimento de Pessoal que, em atenção ao Decreto 5.707/2006, art. 7º, II e IV:

orientie os órgãos e entidades sob sua jurisdição sobre a obrigatoriedade de aprovar o plano anual de capacitação, nos termos do Decreto 5.707/2006, arts. 5º e 2º, c/c Portaria MP 208/2006, art. 2º, I, e art. 4º (subitem 0);

estabeleça, após consulta à Secretaria de Logística e Tecnologia da Informação, um programa de capacitação em governança e em gestão de tecnologia da informação (subitem 0).

Recomendar, com fulcro na Lei 8.443/1992, art. 43, inciso I, c/c RITCU, art. 250, inciso III, à Controladoria-Geral da União (CGU/PR) que:

considere os temas governança de TI, riscos de TI e controles de TI na seleção dos objetos a auditar, consoante o previsto nas boas práticas internacionais para que a atividade de auditoria interna seja mais efetiva (e.g., IPPF 2110.A2, 2120.A1 e 2130.A1; subitem 0).

orientie as unidades de auditoria interna sob sua orientação normativa a considerar os temas governança de TI, riscos de TI e controles de TI na seleção dos objetos a auditar, consoante o previsto nas boas práticas internacionais para que a atividade de auditoria interna seja mais efetiva (e.g., IPPF 2110.A2, 2120.A1 e 2130.A1; subitem 0).

Recomendar, com fulcro na Lei 8.443/1992, art. 43, inciso I, c/c RITCU, art. 250, inciso III, à Comissão Interministerial de Governança Corporativa e de Administração de Participações Societárias da União (CGPAR) que:

normalize a obrigatoriedade de que os entes sob sua jurisdição estabeleçam comitês de TI, observando as boas práticas sobre o tema, a exemplo do Cobit 4.1, PO4.2 – comitê estratégico de TI e PO4.3 – comitê diretor de TI (subitem 0);

orientie os órgãos e entidades sob sua jurisdição a realizar avaliação quantitativa e qualitativa do pessoal do setor de TI, de forma a delimitar as necessidades de recursos humanos necessárias para que estes setores realizem a gestão das atividades de TI da organização (subitem 0);

discipline a forma de acesso às funções de liderança nos setores de Tecnologia da Informação, considerando as competências multidisciplinares necessárias para estas funções, que incluem, mas não se limitam a conhecimentos em TI (subitem 0);

elabore um modelo de processo de software para a os entes sob sua jurisdição, observando as boas práticas sobre o tema (e.g., NBR ISO/IEC 12.207 e 15.504, MPS.BR, CMMI; subitem 0);

estabeleça a obrigatoriedade de que os entes sob sua jurisdição formalizem um processo de software para si, observando as boas práticas sobre o tema (e.g., NBR ISO/IEC 12.207 e 15.504, MPS.BR, CMMI; subitem 0);

elabore um modelo de estrutura de gerenciamento de projetos para os entes sob sua jurisdição, observando as boas práticas sobre o tema (e.g., PMBoK; subitem 0);

estabeleça a obrigatoriedade de que os entes sob sua jurisdição formalizem um processo de gerenciamento de projetos para si, observando as boas práticas sobre o tema (e.g., PMBoK; subitem 0);

estabeleça a obrigatoriedade de que os entes sob sua jurisdição formalizem processos de gestão de serviços para si, incluindo, pelo menos, gestão de configuração, gestão de incidentes e gestão de mudança, observando as boas práticas sobre o tema (e.g., NBR ISO/IEC 20.000, Itil; subitem 0);

estabeleça a obrigatoriedade de que as entidades sob sua jurisdição aprovem um plano anual de capacitação (subitem 0);

estabeleça a obrigatoriedade de que as entidades sob sua jurisdição estabeleçam um processo formal para a contratação e gestão de soluções de tecnologia da informação (subitem 0);

orienta as entidades sob sua jurisdição que o processo a ser formalizado em atenção ao item anterior deve ser elaborado a partir das diretrizes expostas no Acórdão 786/2006-TCU-Plenário, que também estão contidas no modelo implementado pela IN – SLTI/MP 4/2010 (subitem 0);

em atenção ao Decreto-Lei 200/1967, art. 6º, V, estabeleça, normativamente para todos os entes sob sua jurisdição, a obrigatoriedade de a alta administração implantar uma estrutura de controles internos mediante a definição de atividades de controle em todos os níveis da organização para mitigar os riscos de suas atividades, pelo menos nos seguintes processos (subitem 0):

planejamento estratégico institucional;

planejamento estratégico de TI;

funcionamento dos comitês de TI;

processo orçamentário de TI;

processo de software;

gerenciamento de projetos;

gerenciamento de serviços de TI;

segurança da informação;

gestão de pessoal de TI;

contratação e gestão de soluções de TI;

monitoração do desempenho da TI organizacional.

Determinar, com fulcro na Lei 8.443/1992, art. 43, inciso I, c/c RITCU, art. 250, inciso II, à Comissão Interministerial de Governança Corporativa e de Administração de Participações Societárias da União (CGPAR) que, em atenção ao previsto no Decreto 6.021/2007, art. 3º, I, b, oriente os entes sob sua jurisdição sobre necessidade de vincular seus contratos de serviços de desenvolvimento ou manutenção de software a um processo de software, pois, sem essa vinculação, o objeto do contrato não estará precisamente definido, em desconformidade com o disposto na Lei 8.666/1993, art. 6º, inciso IX (subitem 0).

Recomendar, com fulcro na Lei 8.443/1992, art. 43, inciso I, c/c RITCU, art. 250, inciso III, ao Conselho Nacional da Justiça (CNJ) que:

orienta os órgãos e entidades sob sua jurisdição a realizar avaliação quantitativa e qualitativa do pessoal do setor de TI, de forma a delimitar as necessidades de recursos humanos necessárias para que estes setores realizem a gestão das atividades de TI da organização (subitem 0);

disciplina a forma de acesso às funções de liderança nos setores de Tecnologia da Informação, considerando as competências multidisciplinares necessárias para estas funções, que incluem, mas não se limitam a conhecimentos em TI (subitem 0);

elabore um modelo de processo de software para os entes sob sua jurisdição, observando as boas práticas sobre o tema (e.g., NBR ISO/IEC 12.207 e 15.504, MPS.BR, CMMI; subitem 0);

estabeleça a obrigatoriedade de que os entes sob sua jurisdição formalizem um processo de software para si, observando as boas práticas sobre o tema (e.g., NBR ISO/IEC 12.207 e 15.504, MPS.BR, CMMI; subitem 0);

elabore um modelo de estrutura de gerenciamento de projetos para os entes sob sua jurisdição, observando as boas práticas sobre o tema (e.g., PMBoK; subitem 0);

estabeleça a obrigatoriedade de que os entes sob sua jurisdição formalizem um processo de gerenciamento de projetos para si, observando as boas práticas sobre o tema (e.g., PMBoK; subitem 0);

elabore um modelo de processo de gestão de serviços para os entes sob sua jurisdição que inclua, pelo menos, gestão de configuração, gestão de incidentes e gestão de mudança, observando as boas práticas sobre o tema (e.g., NBR ISO/IEC 20.000, Itil; subitem 0);

estabeleça a obrigatoriedade de que os entes sob sua jurisdição formalizem processos de gestão de serviços para si, incluindo, pelo menos, gestão de configuração, gestão de incidentes e gestão de mudança, observando as boas práticas sobre o tema (e.g., NBR ISO/IEC 20.000, Itil; subitem 0);

crie procedimentos para orientar os entes sob sua jurisdição na implementação dos seguintes controles (subitem 0):

nomeação de responsável pela segurança da informação na organização, à semelhança das orientações contidas na NBR ISO/IEC 27.002, item 6.1.3 – Atribuição de responsabilidade para segurança da informação;

criação de comitê para coordenar os assuntos de segurança da informação, à semelhança das orientações contidas na NBR ISO/IEC 27.002, item 6.1.2 – Coordenação de segurança da informação;

processo de gestão de riscos de segurança da informação, à semelhança das orientações contidas na NBR ISO/IEC 27.005 – Gestão de riscos de segurança da informação;

estabelecimento de política de segurança da informação, à semelhança das orientações contidas na NBR ISO/IEC 27.002, item 5.1 – Política de segurança da informação;

processo de elaboração de inventário de ativos, à semelhança das orientações contidas na NBR ISO/IEC 27.002, item 7.1 – Inventário de ativos;

processo de classificação da informação, à semelhança das orientações contidas na NBR ISO/IEC 27.002, item 7.2 – Classificação da informação, processo necessário segundo o Decreto 4.553/2002, art. 6º, § 2º, inciso II, e art. 67;

oriente os órgãos e entidades sob sua jurisdição sobre a obrigatoriedade de aprovar o plano anual de capacitação, nos termos da Resolução – CNJ 90/2009, art. 3º (subitem 0);

estabeleça um programa de capacitação em governança e em gestão de tecnologia da informação (subitem 0);

a partir das diretrizes expostas no Acórdão 786/2006-TCU-Plenário, elabore um modelo de processo para contratação e gestão de soluções de tecnologia da informação para o Poder Judiciário ou, alternativamente, adote o modelo contido na IN – SLTI/MP 4/2010 (subitem 0);

promova a implementação do modelo elaborado em atenção ao item anterior nos órgãos e entidades sob sua jurisdição mediante orientação normativa (subitem 0);

em atenção ao Decreto-Lei 200/1967, art. 6º, V, estabeleça, normativamente para todos os entes sob sua jurisdição, a obrigatoriedade de a alta administração implantar uma estrutura de controles internos mediante a definição de atividades de controle em todos os níveis da organização para mitigar os riscos de suas atividades, pelo menos nos seguintes processos (subitem 0):

planejamento estratégico institucional;

planejamento estratégico de TI;

funcionamento dos comitês de TI;

processo orçamentário de TI;

processo de software;

gerenciamento de projetos;

gerenciamento de serviços de TI;

segurança da informação;

gestão de pessoal de TI;

contratação e gestão de soluções de TI;

monitoração do desempenho da TI organizacional;

orienta as unidades de auditoria interna sob sua orientação normativa a considerar os temas governança de TI, riscos de TI e controles de TI na seleção dos objetos a auditar, consoante o previsto nas boas práticas internacionais para que a atividade de auditoria interna seja mais efetiva (e.g., IPPF 2110.A2, 2120.A1 e 2130.A1; subitem 0);

em atenção à Constituição Federal, art. 74, c/c o art. 103-B, § 4º, I, estabeleça sistema de controle interno integrado para todo o Poder Judiciário (subitem 0).

Determinar, com fulcro na Lei 8.443/1992, art. 43, inciso I, c/c RITCU, art. 250, inciso II, ao Conselho Nacional de Justiça (CNJ) que:

em atenção ao previsto na Constituição Federal, art. 103-B, § 4º, II, oriente os entes sob sua jurisdição sobre necessidade de vincular seus contratos de serviços de desenvolvimento ou manutenção de software a um processo de software, pois, sem esta vinculação, o objeto do contrato não estará precisamente definido, em desconformidade com o disposto na Lei 8.666/1993, art. 6º, inciso IX (subitem 0);

em atenção ao previsto na Constituição Federal, art. 103-B, § 4º, II, oriente os órgãos e entidades sob sua jurisdição para que (subitem 0):

ao realizarem licitação com finalidade de criar ata de registro de preços atentem que:

devem fundamentar formalmente a criação de ata de registro de preços, e.g., por um dos incisos do art. 2º do Decreto 3.931/2001 (Acórdão 2.401/2006-TCU-Plenário);

devem praticar todos os atos descritos no Decreto 3.931/2001, art. 3º, § 2º, em especial o previsto no seu inciso I, que consiste em ‘convidar mediante correspondência eletrônica ou outro meio eficaz, os órgãos e entidades para participarem do registro de preços’;

o planejamento da contratação é obrigatório, sendo obrigatória a realização dos devidos estudos técnicos preliminares (Lei 8.666/1993, art. 6º, inciso IX);

a fixação, no termo de convocação, de quantitativos (máximos) a serem contratados por meio dos contratos derivados da ata de registro de preços, previstos no Decreto 3.931/2001, art. 9º, inciso II, é obrigação e não faculdade do gestor (Acórdão 991/2009-TCU-Plenário, Acórdão 1.100/2007-TCU-Plenário e Acórdão 4.411/2010-TCU-2ª Câmara);

em atenção ao princípio da vinculação ao instrumento convocatório (Lei 8.666/1993, art. 3º, caput), devem gerenciar a ata de forma que a soma dos quantitativos contratados em todos os contratos derivados da ata não supere o quantitativo máximo previsto no edital;

quando realizarem adesão à ata de registro de preços atentem que:

o planejamento da contratação é obrigatório, sendo obrigatória a realização dos devidos estudos técnicos preliminares (Lei 8.666/1993, art. 6º, inciso IX);

devem demonstrar formalmente a vantajosidade da adesão, nos termos do Decreto 3.931/2001, art. 8º;

as regras e condições estabelecidas no certame que originou a ata de registro de preços devem ser conformes as necessidades e condições determinadas na etapa de planejamento da contratação (Lei 8.666/1993, art. 6º, inciso IX, alínea d, c/c o art. 3º, § 1º, inciso I, e Lei 10.520/2002, art. 3º, inciso II);

em atenção ao previsto na Constituição Federal, art. 103-B, § 4º, II, oriente os órgãos e entidades sob sua jurisdição para que, caso possuam contratos com empresas públicas prestadoras de serviços de TI (subitem 0):

analisem a conformidade dos termos do contrato e do projeto básico e verifiquem se:

foi realizado o adequado planejamento da contratação, consistindo na execução do processo de planejamento previsto na IN – SLTI/MP 4/2010 se for integrante do Sisp (IN – SLTI/MP 4/2010, art. 18, inciso II) ou, caso não o seja, se foram realizados os devidos estudos técnicos preliminares (Lei 8.666/1993, art. 6º, inciso IX);

as especificações do objeto são precisas e suficientes, em conformidade com a Lei 8.666/1993, art. 6º, IX;

os critérios de mensuração dos serviços são precisos e suficientes, de acordo com o determinado na Lei 8.666/1993, art. 6º, IX, e (também necessários de acordo com a IN – SLTI 4/2010, art. 14, II, a);

a metodologia de avaliação da adequação dos produtos é precisa e suficiente, de acordo com o determinado na Lei 8.666/1993, art. 6º, IX, e (também necessária de acordo com a IN – SLTI 4/2010, art. 14, II, c);

as cláusulas de penalidades contidas na Lei 8.666/1993, art. 87, de acordo com o determinado na Lei 8.666/1993, art. 55, VII e VIII, são detalhadas e atendem aos princípios da razoabilidade, proporcionalidade e prudência (e também o previsto na IN – SLTI 4/2010, art. 15, III, h);

o modelo de pagamento é vinculado a resultados, obedecendo ao princípio constitucional da eficiência (e também ao previsto no Decreto 2.271/1997, art. 3º, § 1º, e na IN – SLTI 4/2010, art. 15, §§ 2º e 3º);

a justificativa dos preços contratados é adequadamente fundamentada em arrazoada pesquisa de mercado, de acordo com o determinado na Lei 8.666/1993, art. 26, III, inclusive com a análise da planilha de composição de custos dos serviços, necessária segundo a Lei 8.666/1993, art. 7º, § 2º, II;

caso a análise realizada de acordo com orientação acima indique desconformidade, elaborem plano de ação para providenciar as adequações contratuais necessárias, que deverão ser realizadas no prazo de 180 dias;

mantenham o resultado da análise de conformidade empreendida em documento formalizado, à disposição dos controles externo e interno;

informem seu órgão de assessoramento jurídico e sua unidade de auditoria interna da análise que está sendo empreendida e do resultado obtido;

em atenção ao previsto na Constituição Federal, art. 103-B, § 4º, II, oriente os órgãos e entidades sob sua jurisdição que (subitem 0):

mesmo que a execução de seus serviços de tecnologia da informação seja transferida mediante contrato ou outro acordo a outra organização pública, como as empresas públicas prestadoras de serviços de tecnologia da informação, as atividades de gestão (planejamento, coordenação, supervisão e controle) de TI devem ser acometidas a pessoas integrantes do quadro permanente, ou, excepcionalmente, a detentores de cargo em comissão, da organização contratante, não podendo ser delegadas a pessoas direta ou indiretamente ligadas à contratada;

a contratação de empresas públicas prestadoras de serviços de tecnologia da informação não afasta a necessidade de a organização contratante manter estrutura de governança de TI própria, que direcione e controle a gestão desses contratos bem como a gestão de todos os processos de TI da organização.

Recomendar, com fulcro na Lei 8.443/1992, art. 43, inciso I, c/c RITCU, art. 250, inciso III, ao Conselho Nacional do Ministério Público (CNMP) que:

em atenção ao Decreto-Lei 200/1967, art. 6º, inciso I, e art. 7º, normatize a obrigatoriedade de que todos os entes sob sua jurisdição estabeleçam processo de planejamento estratégico institucional, observando as boas práticas sobre o tema, a exemplo do critério de avaliação 2 do Gespública, contemplando, pelo menos (subitem 0):

elaboração, com participação de representantes dos diversos setores da organização, de um documento que materialize o plano estratégico institucional de longo prazo, contemplando, pelo menos, objetivos, indicadores e metas para a organização;

aprovação, pela mais alta autoridade da organização, do plano estratégico institucional; desdobramento do plano estratégico pelas unidades executoras;

divulgação do plano estratégico institucional para conhecimento dos cidadãos brasileiros, exceto nos aspectos formalmente declarados sigilosos ou restritos;;

acompanhamento periódico do alcance das metas estabelecidas, para correção de desvios; divulgação interna e externa do alcance das metas, ou dos motivos de não ter alcançado;

em atenção ao Decreto-Lei 200/1967, art. 6º, inciso I, e art. 7º, normatize a obrigatoriedade de que todos os entes sob sua jurisdição estabeleçam processo de planejamento estratégico de TI, observando as boas práticas sobre o tema, a exemplo do processo ‘POI – Planejamento Estratégico de TI’ do Cobit 4.1, contemplando, pelo menos (subitem 0):

elaboração, com participação de representantes dos diversos setores da organização, de um documento que materialize o plano estratégico de TI, contemplando, pelo menos:

objetivos, indicadores e metas para a TI organizacional, sendo que os objetivos devem estar explicitamente alinhados aos objetivos de negócio constantes do plano estratégico institucional;

alocação de recursos (financeiros, humanos, materiais etc);

estratégia de terceirização;

aprovação, pela mais alta autoridade da organização, do plano estratégico de TI;

desdobramento do plano estratégico de TI pelas unidades executoras;

divulgação do plano estratégico de TI para conhecimento dos cidadãos brasileiros, exceto nos aspectos formalmente declarados sigilosos ou restritos;

acompanhamento periódico do alcance das metas estabelecidas, para correção de desvios;

divulgação interna e externa do alcance das metas, ou os motivos de não as ter alcançado;

normatize a obrigatoriedade de que os entes sob sua jurisdição estabeleçam comitês de TI, observando as boas práticas sobre o tema, a exemplo do Cobit 4.1, PO4.2 – comitê estratégico de TI e PO4.3 – comitê diretor de TI (subitem 0);

orienta os órgãos e entidades sob sua jurisdição a realizarem avaliação quantitativa e qualitativa do pessoal do setor de TI, de forma a delimitar as necessidades de recursos humanos necessárias para que estes setores realizem a gestão das atividades de TI da organização (subitem 0);

discipline a forma de acesso às funções de liderança nos setores de Tecnologia da Informação, considerando as competências multidisciplinares necessárias para estas funções, que incluem, mas não se limitam a conhecimentos em TI (subitem 0);

elabore um modelo de processo de software para os entes sob sua jurisdição, observando as boas práticas sobre o tema (e.g., NBR ISO/IEC 12.207 e 15.504, MPS.BR, CMMI; subitem 0);

estabeleça a obrigatoriedade de que os entes sob sua jurisdição formalizem um processo de software para si, observando as boas práticas sobre o tema (e.g., NBR ISO/IEC 12.207 e 15.504, MPS.BR, CMMI; subitem 0);

elabore um modelo de estrutura de gerenciamento de projetos para os entes sob sua jurisdição, observando as boas práticas sobre o tema (e.g., PMBoK; subitem 0);

estabeleça a obrigatoriedade de que os entes sob sua jurisdição formalizem um processo de gerenciamento de projetos para si, observando as boas práticas sobre o tema (e.g., PMBoK; subitem 0);

elabore um modelo de processo de gestão de serviços para os entes sob sua jurisdição que inclua, pelo menos, gestão de configuração, gestão de incidentes e gestão de mudança, observando as boas práticas sobre o tema (e.g., NBR ISO/IEC 20.000, Itil; subitem 0);

estabeleça a obrigatoriedade de que os entes sob sua jurisdição formalizem processos de gestão de serviços para si, incluindo, pelo menos, gestão de configuração, gestão de incidentes e gestão de mudança, observando as boas práticas sobre o tema (e.g., NBR ISO/IEC 20.000, Itil; subitem 0);

estabeleça a obrigatoriedade de que os entes sob sua jurisdição implementem os seguintes controles gerais de TI relativos à segurança da informação (subitem 0):

nomeação de responsável pela segurança da informação na organização, à semelhança das orientações contidas na NBR ISO/IEC 27.002, item 6.1.3 – Atribuição de responsabilidade para segurança da informação;

criação de comitê para coordenar os assuntos de segurança da informação, à semelhança das orientações contidas na NBR ISO/IEC 27.002, item 6.1.2 – Coordenação de segurança da informação;

processo de gestão de riscos de segurança da informação, à semelhança das orientações contidas na NBR ISO/IEC 27.005 – Gestão de riscos de segurança da informação;

estabelecimento de política de segurança da informação, à semelhança das orientações contidas na NBR ISO/IEC 27.002, item 5.1 – Política de segurança da informação;

processo de elaboração de inventário de ativos, à semelhança das orientações contidas na NBR ISO/IEC 27.002, item 7.1 – Inventário de ativos;

processo de classificação da informação, à semelhança das orientações contidas na NBR ISO/IEC 27.002, item 7.2 – Classificação da informação, processo necessário segundo o Decreto 4.553/2002, art. 6º, § 2º, inciso II e art. 67;

crie procedimentos para orientar os entes sob sua jurisdição na implementação dos controles listados no item acima (subitem 0);

estabeleça a obrigatoriedade de que os órgãos e entidades sob sua jurisdição aprovem um plano anual de capacitação (subitem 0);

estabeleça um programa de capacitação em governança e em gestão de tecnologia da informação (subitem 0);

a partir das diretrizes expostas no Acórdão 786/2006-TCU-Plenário, elabore um modelo de processo para contratação e gestão de soluções de tecnologia da informação para o Ministério Público ou, alternativamente, adote o modelo contido na IN – SLTI/MP 4/2010 (subitem 0);

promova a implementação do modelo elaborado em atenção ao item anterior nos órgãos e entidades sob sua jurisdição mediante orientação normativa (subitem 0);

em atenção ao Decreto-Lei 200/1967, art. 6º, V, estabeleça, normativamente para todos os entes sob sua jurisdição, a obrigatoriedade de a alta administração implantar uma estrutura de controles internos mediante a definição de atividades de controle em todos os níveis da organização para mitigar os riscos de suas atividades, pelo menos, nos seguintes processos (subitem 0):

planejamento estratégico institucional/institucional;

planejamento estratégico de TI;

funcionamento dos comitês de TI;

processo orçamentário de TI;

processo de software;

gerenciamento de projetos;

gerenciamento de serviços de TI;

segurança da informação;

gestão de pessoal de TI;

contratação e gestão de soluções de TI;

monitoração do desempenho da TI organizacional.

oriente as unidades de auditoria interna sob sua orientação normativa a considerar os temas governança de TI, riscos de TI e controles de TI na seleção dos objetos a auditar, consoante o previsto nas boas práticas internacionais para que a atividade de auditoria interna seja mais efetiva (e.g., IPPF 2110.A2, 2120.A1 e 2130.A1; subitem 0);

em atenção à Constituição Federal, art. 74, c/c o art. 103-B, § 4º, I, estabeleça sistema de controle interno integrado para todo o Ministério Público (subitem 0).

Determinar, com fulcro na Lei 8.443/1992, art. 43, inciso I, c/c RITCU, art. 250, inciso II, ao Conselho Nacional do Ministério Público (CNMP) que:

em atenção ao previsto na Constituição Federal, art. 130-A, § 2º, II, oriente os entes sob sua jurisdição sobre necessidade de vincular seus contratos de serviços de desenvolvimento ou manutenção de software a um processo de software, pois, sem esta vinculação, o objeto do contrato não estará precisamente definido, em desconformidade com o disposto na Lei 8.666/1993, art. 6º, inciso IX (subitem 0);

em atenção ao previsto na Constituição Federal, art. 130-A, § 2º, II, oriente os órgãos e entidades sob sua jurisdição para que (subitem 0):

ao realizarem licitação com finalidade de criar ata de registro de preços atentem que:

devem fundamentar formalmente a criação de ata de registro de preços, e.g., por um dos incisos do art. 2º do Decreto 3.931/2001 (Acórdão 2.401/2006-TCU-Plenário);

devem praticar todos os atos descritos no Decreto 3.931/2001, art. 3º, § 2º, em especial o previsto no seu inciso I, que consiste em ‘convidar mediante correspondência eletrônica ou outro meio eficaz, os órgãos e entidades para participarem do registro de preços’;

o planejamento da contratação é obrigatório, sendo obrigatória a realização dos devidos estudos técnicos preliminares (Lei 8.666/1993, art. 6º, inciso IX);

a fixação, no termo de convocação, de quantitativos (máximos) a serem contratados por meio dos contratos derivados da ata de registro de preços, previstos no Decreto 3.931/2001, art. 9º, inciso II, é obrigação e não faculdade do gestor (Acórdão 991/2009-TCU-Plenário, Acórdão 1.100/2007-TCU-Plenário e Acórdão 4.411/2010-TCU-2ª Câmara);

em atenção ao princípio da vinculação ao instrumento convocatório (Lei 8.666/1993, art. 3º, caput), devem gerenciar a ata de forma que a soma dos quantitativos contratados em todos os contratos derivados da ata não supere o quantitativo máximo previsto no edital;

quando realizarem adesão à ata de registro de preços atentem que:

o planejamento da contratação é obrigatório, sendo obrigatória a realização dos devidos estudos técnicos preliminares (Lei 8.666/1993, art. 6º, inciso IX);

devem demonstrar formalmente a vantajosidade da adesão, nos termos do Decreto 3.931/2001, art. 8º;

as regras e condições estabelecidas no certame que originou a ata de registro de preços devem ser conformes as necessidades e condições determinadas na etapa de planejamento da contratação (Lei 8.666/1993, art. 6º, inciso IX, alínea d, c/c o art. 3º, § 1º, inciso I, e Lei 10.520/2002, art. 3º, inciso II);

em atenção ao previsto na Constituição Federal, art. 130-A, § 2º, II, oriente os órgãos e entidades sob sua jurisdição para que, caso possuam contratos com empresas públicas prestadoras de serviços de TI (subitem 0):

analisem a conformidade dos termos do contrato e do projeto básico e verifiquem se:

foi realizado o adequado planejamento da contratação, consistindo na execução do processo de planejamento previsto na IN – SLTI/MP 4/2010 se for integrante do Sisp (IN – SLTI/MP 4/2010, art. 18, inciso II) ou, caso não o seja, se foram realizados os devidos estudos técnicos preliminares (Lei 8.666/1993, art. 6º, inciso IX);

as especificações do objeto são precisas e suficientes, em conformidade com a Lei 8.666/1993, art. 6º, IX;

os critérios de mensuração dos serviços são precisos e suficientes, de acordo com o determinado na Lei 8.666/1993, art. 6º, IX, e (também necessários de acordo com a IN – SLTI 4/2010, art. 14, II, a);

a metodologia de avaliação da adequação dos produtos é precisa e suficiente, de acordo com o determinado na Lei 8.666/1993, art. 6º, IX, e (também necessária de acordo com a IN – SLTI 4/2010, art. 14, II, c);

as cláusulas de penalidades contidas na Lei 8.666/1993, art. 87, de acordo com o determinado na Lei 8.666/1993, art. 55, VII e VIII, são detalhadas e atendem aos princípios da razoabilidade, proporcionalidade e prudência (e também o previsto na IN – SLTI 4/2010, art. 15, III, h);

o modelo de pagamento é vinculado a resultados, obedecendo ao princípio constitucional da eficiência (e também ao previsto no Decreto 2.271/1997, art. 3º, § 1º, e na IN – SLTI 4/2010, art. 15, §§ 2º e 3º);

a justificativa dos preços contratados é adequadamente fundamentada em arrazoada pesquisa de mercado, de acordo com o determinado na Lei 8.666/1993, art. 26, III, inclusive com a análise da planilha de composição de custos dos serviços, necessária segundo a Lei 8.666/1993, art. 7º, § 2º, II;

caso a análise realizada de acordo com orientação acima indique desconformidade, elaborem plano de ação para providenciar as adequações contratuais necessárias, que deverão ser realizadas no prazo de 180 dias;

mantenham o resultado da análise de conformidade empreendida em documento formalizado, à disposição dos controles externo e interno;

informem seu órgão de assessoramento jurídico e sua unidade de auditoria interna da análise que está sendo empreendida e do resultado obtido;

em atenção ao previsto na Constituição Federal, art. 130-A, § 2º, II, oriente os órgãos e entidades sob sua jurisdição que (subitem 0):

mesmo que a execução de seus serviços de tecnologia da informação seja transferida mediante contrato ou outro acordo a outra organização pública, como as empresas públicas prestadoras de serviços de tecnologia da informação, as atividades de gestão (planejamento, coordenação, supervisão e controle) de TI devem ser acometidas a pessoas integrantes do quadro permanente, ou, excepcionalmente, a detentores de cargo em comissão, da organização contratante, não podendo ser delegadas a pessoas direta ou indiretamente ligadas à contratada;

a contratação de empresas públicas prestadoras de serviços de tecnologia da informação não afasta a necessidade de a organização contratante manter estrutura de governança de TI própria, que direcione e controle a gestão desses contratos bem como a gestão de todos os processos de TI da organização.

Recomendar, com fulcro na Lei 8.443/1992, art. 43, inciso I, c/c RITCU, art. 250, inciso III, ao Tribunal de Contas da União que avalie as orientações contidas no acórdão que vier a ser proferido, e adote as medidas necessárias a sua implementação.

Recomendar, com fulcro na Lei 8.443/1992, art. 43, inciso I, c/c RITCU, art. 250, inciso III, à Câmara dos Deputados que avalie as orientações contidas no acórdão que vier a ser proferido, e adote as medidas necessárias a sua implementação.

Recomendar, com fulcro na Lei 8.443/1992, art. 43, inciso I, c/c RITCU, art. 250, inciso III, ao Senado Federal que avalie as orientações contidas no acórdão que vier a ser proferido e adote as medidas necessárias a sua implementação.

Dar ciência à Casa Civil da Presidência da República de que o secretário-executivo não submeteu ao Ministro de Estado o Plano de Ação Global da pasta, o que afronta o Decreto 5.135/2004, art. 23, inciso I.

Dar ciência ao Ministério da Agricultura, Pecuária e Abastecimento de que o secretário-executivo não submeteu ao Ministro de Estado o Plano de Ação Global da pasta, o que afronta o Decreto 7.127/2010, art. 41, inciso I.

Dar ciência ao Ministério da Ciéncia e Tecnologia de que o secretário-executivo não submeteu ao Ministro de Estado o Plano de Ação Global da pasta, o que afronta o Decreto 5.886/2006, art. 38, inciso I.

Dar ciência ao Ministério da Educação de que o secretário-executivo não submeteu ao Ministro de Estado o Plano de Ação Global da pasta, o que afronta o Decreto 7.480/2011, art. 38, inciso I.

Dar ciência ao Ministério da Fazenda de que o secretário-executivo não submeteu ao Ministro de Estado o Plano de Ação Global da pasta, o que afronta o Decreto 7.482/2011, art. 43, inciso I.

Dar ciência ao Ministério da Integração Nacional de que o secretário-executivo não submeteu ao Ministro de Estado o Plano de Ação Global da pasta, o que afronta o Decreto 7.472/2011, art. 29, inciso IV.

Dar ciência ao Ministério da Justiça de que o secretário-executivo não submeteu ao Ministro de Estado o Plano de Ação Global da pasta, o que afronta o Decreto 6.061/2007, art. 43, inciso I.

Dar ciência ao Ministério da Saúde de que o secretário-executivo não submeteu ao Ministro de Estado o Plano de Ação Global da pasta, o que afronta o Decreto 7.530/2011, art. 49, inciso I.

Dar ciência ao Ministério das Cidades de que o secretário-executivo não submeteu ao Ministro de Estado o Plano de Ação Global da pasta, o que afronta o Decreto 4.665/2003, art. 26, inciso I.

Dar ciência ao Ministério das Minas e Energia de que o secretário-executivo não submeteu ao Ministro de Estado o Plano de Ação Global da pasta, o que afronta o Decreto 5.267/2004, art. 27, inciso I.

Dar ciência ao Ministério do Desenvolvimento Agrário de que o secretário-executivo não submeteu ao Ministro de Estado o Plano de Ação Global da pasta, o que afronta o Decreto 7.255/2010, art. 22, inciso I.

Dar ciência ao Ministério do Desenvolvimento Social e Combate à Fome de que o secretário-executivo não submeteu ao Ministro de Estado o Plano de Ação Global da pasta, o que afronta o Decreto 7.493/2011, art. 36, inciso I.

Dar ciência ao Ministério do Desenvolvimento, Indústria e Comércio Exterior de que o secretário-executivo não submeteu ao Ministro de Estado o Plano de Ação Global da pasta, o que afronta o Decreto 7.096/2010, art. 30, inciso I.

Dar ciência ao Ministério do Esporte de que o secretário-executivo não submeteu ao Ministro de Estado o Plano de Ação Global da pasta, o que afronta o Decreto 7.529/2011, art. 20, inciso I.

Dar ciência ao Ministério do Meio Ambiente de que o secretário-executivo não submeteu ao Ministro de Estado o Plano de Ação Global da pasta, o que afronta o Decreto 6.101/2007, art. 43, inciso I.

Dar ciência ao Ministério do Planejamento, Orçamento e Gestão de que o secretário-executivo não submeteu ao Ministro de Estado o Plano de Ação Global da pasta, o que afronta o Decreto 7.063/2010, art. 49, inciso I.

Dar ciência ao Ministério do Trabalho e Emprego de que o secretário-executivo não submeteu ao Ministro de Estado o Plano de Ação Global da pasta, o que afronta o Decreto 5.063/2004, art. 27, inciso I.

Dar ciência ao Ministério do Turismo de que o secretário-executivo não submeteu ao Ministro de Estado o Plano de Ação Global da pasta, o que afronta o Decreto 6.546/2008, art. 20, inciso I.

Dar ciência ao Ministério dos Transportes de que o secretário-executivo não submeteu ao Ministro de Estado o Plano de Ação Global da pasta, o que afronta o Decreto 4.721/2003, art. 19, inciso I.

Dar ciência à Secretaria de Assuntos Estratégicos da Presidência da República de que o secretário-executivo não submeteu ao Ministro de Estado o Plano de Ação Global da pasta, o que afronta o Decreto 6.517/2008, art. 7º, inciso I.

Dar ciência à Secretaria de Relações Institucionais da Presidência da República de que o secretário-executivo não submeteu ao Ministro de Estado o Plano de Ação Global da pasta, o que afronta o Decreto 6.207/2007, art. 9º, inciso I.

Dar ciência à Secretaria-Geral da Presidência da República de que o secretário-executivo não submeteu ao Ministro de Estado o Plano de Ação Global da pasta, o que afronta o Decreto 6.378/2008, art. 11, inciso I.

Dar ciência à Secretaria de Aviação Civil da Presidência da República de que o secretário-executivo não submeteu ao Ministro de Estado o Plano de Ação Global da pasta, o que afronta o Decreto 7.476/2011, art. 18, inciso I.

Determinar à Secretaria de Fiscalização de Tecnologia da Informação do TCU (Sefti/TCU) que:

promova a divulgação dos critérios de auditoria contidos no Apêndice 0, a fim de continuar a atividade de orientação que vem desenvolvendo (subitem 0);

dê publicidade, inclusive por meio do sítio do TCU na internet, às informações acerca de governança de tecnologia da informação que foram solicitadas aos gestores nesta fiscalização (subitem 0);

monitore as deliberações do Acórdão 2.308/2010-TCU-Plenário em conjunto com as que vierem a ser proferidas nestes autos (subitem 0);

divulgue o conteúdo das seis notas técnicas existentes, como forma de informar e orientar a APF e a sociedade sobre a existência do conjunto de normas que regem as aquisições de bens e serviços de tecnologia da informação, bem como sobre a jurisprudência deste Tribunal quanto ao assunto, promovendo, inclusive, a realização de seminários, cursos e palestras, caso entenda conveniente (subitem 0);

encaminhe o estudo elaborado pelo TCU intitulado ‘Critérios gerais de controle interno na administração pública’ à (item Error! Reference source not found. Erro! Fonte de referência não encontrada.):

Câmara de Políticas de Gestão, Desempenho e Competitividade do Conselho de Governo, com objetivo de subsidiar possível elaboração de normativo para o poder executivo, com fulcro no Decreto 7.478/2011, art. 2º, II, tratando de gestão de riscos, do controle interno e da governança corporativa;

Conselho Nacional de Justiça, com objetivo de subsidiar possível elaboração de normativo para o poder judiciário, com fulcro na Constituição Federal, art. 103-B, § 4º, II, tratando de gestão de riscos, do controle interno e da governança corporativa;

Conselho Nacional do Ministério Público, com objetivo de subsidiar possível elaboração de normativo para o ministério público, com fulcro na Constituição Federal, art. 130-A, § 2º, II, tratando de gestão de riscos, do controle interno e da governança corporativa;

Comissão de Finanças e Tributação da Câmara dos Deputados, com objetivo subsidiar possível anteprojeto de proposta legislativa para alteração da Lei de Responsabilidade Fiscal;

Comissão de Assuntos Econômicos do Senado Federal, com objetivo subsidiar possível anteprojeto de proposta legislativa para alteração da Lei de Responsabilidade Fiscal;

promova a divulgação, inclusive por meio de eventos, das recomendações e determinações dirigidas aos órgãos governantes superiores por meio do acórdão que vier a ser proferido, como forma de mitigar os riscos da sua implementação;

encaminhe cópia do acórdão que vier a ser proferido, bem como do relatório e voto que o fundamentarem, assim como da íntegra deste relatório, à(ao)(s):

entes a que foram dirigidas as determinações e recomendações da deliberação;

Serviço Federal de Processamento de Dados (Serpro);

Comissão de Ciência e Tecnologia, Comunicação e Informática (CCTCI) da Câmara dos Deputados;

Subcomissão Permanente de Ciência e Tecnologia e Informática da Comissão de Ciência e Tecnologia, Comunicação e Informática (CCTCI) da Câmara dos Deputados;

Comissão de Ciência, Tecnologia, Inovação, Comunicação e Informática (CCT) do Senado Federal;

Subcomissão Permanente de Serviços de Informática (CCTSINF) da Comissão de Ciência, Tecnologia, Inovação, Comunicação e Informática (CCT) do Senado Federal;

Tribunais de Contas dos Estados e dos Municípios, para que adotem as medidas que entenderem pertinentes.

Arquivar os presentes autos na Secretaria de Fiscalização de Tecnologia da Informação.

[...]"

#### 4. O Relatório acima reproduzido pode ser resumido nos seguintes termos:

“[...] O objetivo do TMS Gestão e Uso de TI foi avaliar se a gestão e o uso da tecnologia da informação estão de acordo com a legislação e aderentes às boas práticas de governança de TI e foi conduzido, entre 2010 e 2011, por meio de 21 trabalhos, abrangendo 315 organizações públicas federais.

Uma pesquisa realizada para levantar a situação da governança de TI na APF identificou, por meio de dados declarados pelos jurisdicionados, que mais de 60% das organizações não possuem planejamento estratégico de TI; que algumas organizações continuam a ter sua TI totalmente controlada por pessoas estranhas a seus quadros de pessoal; que são graves os problemas de segurança da informação, já que informações críticas não são protegidas adequadamente; que metade das organizações não possui método ou processo para desenvolvimento de softwares e para aquisição de bens e serviços de informática, o que gera riscos de irregularidades em contratações; que a atuação sistemática da alta administração em definir diretrizes para o uso de TI na

organização ainda é incipiente. O levantamento concluiu que mais da metade das organizações está no estágio inicial da governança de TI e que apenas 5% encontram-se em estágio aprimorado.

Catorze auditorias in loco evidenciaram situação real da governança de TI pior do que a declarada pelos respectivos auditados, sugerindo que na APF a situação também pode ser pior do que a apresentada por meio da tabulação dos dados declarados pelos jurisdicionados na pesquisa realizada.

Quatro auditorias para avaliação de objetos específicos de TI permitiram identificar consequências da ausência ou da deficiência dos controles gerais de TI, tais como sistemas com falhas de segurança da informação que foram efetivamente exploradas em sede de fraude, sistemas que não implementam as regras do negócio e pagamentos indevidos em contratos de consultoria.

A principal causa do cenário analisado é a falta de envolvimento das lideranças das instituições auditadas, o que aponta para a necessidade de uma nova postura dos administradores públicos do alto escalão, que inclua assumir a responsabilidade pela avaliação, direção e monitoramento da gestão e do uso da TI nessas instituições.

Para implantar tais processos, destaca-se a necessária utilização da auditoria interna das organizações no apoio aos altos dirigentes, de forma que se faz necessário que estas unidades incluam os temas de TI na seleção dos objetos a auditar. Evidenciou-se a elevada dependência das instituições pesquisadas em relação a sistemas informatizados para a consecução dos objetivos de negócio (51% param imediatamente de prestar serviços aos cidadãos se seu sistema mais crítico sofrer interrupção), o que reforça a tese de prioridade para os objetos de TI nas auditorias internas.

Argumentou-se ainda que a pouca maturidade em governança corporativa é fator limitante à maturidade da governança de TI, de forma que foi encaminhado a alguns legitimados estudo realizado pelo TCU contendo anteprojeto de lei para alteração da Lei de Responsabilidade Fiscal, com vistas a aperfeiçoar o arcabouço normativo, contribuindo para o fortalecimento da governança corporativa nos entes públicos.

Aspectos legais nas contratações por meio do sistema de registro de preços e nas contratações de empresas públicas prestadoras de serviços de TI foram endereçados, e orientações para que essas contratações estejam aderentes à legislação e sigam as boas práticas foram formuladas.

Extenso e complexo conjunto de recomendações e determinações para modificar o cenário de baixa maturidade na governança de TI foi expedido aos órgãos governantes superiores, conjunto este que será objeto de discussão em evento a ser promovido pela Secretaria de Fiscalização de Tecnologia da Informação (Sefit) após a apreciação deste trabalho pelo Plenário do TCU. [...].”

5. Como pode ser observado, o título III do relatório trata dos aspectos legais nas contratações de soluções de TI, apresentando informações relevantes acerca de contratações pelo Sistema de Registro de Preços (SRP), destacando a forte tendência de realização de avenças por meio desse sistema, por alguma das formas possíveis.

“[...] Em relação a essa questão, a Secretaria de Fiscalização de Tecnologia da Informação (Sefit) comenta que a utilização do SRP poderia sinalizar tendência de a Administração Pública Federal dar cumprimento ao art. 15, inciso II da Lei 8.666/1993, se não estivesse sendo utilizado de forma distorcida, conforme já detectado por este Tribunal (Acórdão 1.487/2007-TCU-Plenário, ora em fase de recurso).

5. O que foi observado naquela oportunidade, e agora por meio das verificações realizadas pela Sefit, é que o planejamento conjunto para a criação de uma ata, que deveria ser a regra, é exceção, enquanto a adesão tardia (carona), que deveria ser a exceção, tornou-se prática comum.

6. Nesse sentido, a Sefit propõe a realização de determinações à SLTI/MP, com objetivo de mitigar, já no curto prazo, a continuidade de ocorrências de desconformidades, nos termos constantes do item 251 do Relatório (fls. 435 do v. 2).

7. Tendo em vista a natureza e a relevância da matéria em apreciação, com repercussão em toda a administração pública, solicitei a manifestação do Ministério Pùblico junto a este Tribunal, quanto à matéria de direito em relação ao conteúdo e às propostas relacionadas ao título III, subtítulo III.1, do Relatório de Auditoria.

8. Em resposta o Parquet produziu o parecer constante da peça que abaixo reproduzida como parte deste Relatório:

“[...]3. Não obstante observar a tendência de se dar cumprimento ao disposto no art. 15, inciso II, da Lei nº 8.666/93, que estabelece que as compras, sempre que possível, deverão ser processadas por meio do SRP, a Sefti constatou que uma parcela muito pequena delas foi realizada mediante planejamento conjunto, com vistas à aquisição de bens ou a contratação de serviços para atendimento a mais de um órgão ou entidade, ou a programas de governo, hipótese prevista no inciso III do art. 2º do Decreto nº 3.931/2001, que regulamenta o Sistema de Registro de Preços.

4. Além da ausência de planejamento, verificou-se que uma significativa quantidade de atas não contou com outras instituições participantes, dando ensejo ao excessivo número de contratações por meio de adesões realizadas com fundamento no art. 8º da supracitada norma regulamentar, prática esta conhecida como “carona”.

5. A partir desses dados, a Sefti observou que o planejamento conjunto para a criação de uma ata, que deveria ser a regra é exceção, enquanto que a prática da adesão a uma ata, que deveria ser exceção, tornou-se prática comum.

6. Sobre o assunto, a unidade técnica registrou que esta Corte já se posicionou contrária à adesão ilimitada a uma mesma Ata de Registro de Preços, nos termos do Acórdão nº 1.487/2007 – Plenário, atualmente em fase de recurso, tendo em vista a ofensa aos princípios da competição, da igualdade de condições entre os licitantes e da busca da maior vantagem para a Administração Pública.

7. Como exemplo de planejamento conjunto que atende aos objetivos da legislação, a unidade técnica citou a ação coordenada pela Secretaria de Logística e Tecnologia da Informação – SLTI/MP para a aquisição de mais de 100.000 equipamentos.

8. Por outro lado, a Sefti constatou que a prática da adesão possibilita a exploração comercial das Atas de Registro de Preços por empresas privadas.

9. Os problemas recorrentes identificados nas contratações examinadas foram a ausência de fundamentação legal que sustenta o motivo da criação da ata; a ausência de planejamento da contratação, tanto na criação da ata quanto na adesão; a ausência de fixação dos quantitativos máximos que serão adquiridos por meio da ata; a ausência de demonstração da vantajosidade em aderir à ata; assim como a adesão a atas oriundas de licitação com critérios e condições aplicáveis ao ente que a registrou, porém distintos das necessidades da instituição que aderiu.

10. Desse modo, a Sefti concluiu o exame dessa matéria apresentando a seguinte proposta (fl. 435):

“251. Ante as constatações acima, e a existência de precedentes de julgados para alguns dos assuntos acima tratados nesta Corte, entende-se como oportuno e conveniente que os órgãos governantes superiores orientem seus jurisdicionados para evitar as práticas irregulares acima, e propõe-se determinar à SLTI/MP que, em atenção ao disposto no Decreto 1.094/1994, art. 2º, inciso I, oriente os órgãos e entidades sob sua jurisdição

para que (subitem III.1):

251.2. ao realizarem licitação com finalidade de criar ata de registro de preços atentem que:

251.2.1. devem fundamentar formalmente a criação de ata de registro de preços, e.g., por um dos incisos do art. 2º do Decreto 3.931/2001 (Acórdão 2.401/2006-TCU-Plenário);

251.2.2. devem praticar todos os atos descritos no Decreto 3.931/2001, art. 3º, § 2º, em especial o previsto no seu inciso I, que consiste em ‘convidar mediante correspondência eletrônica ou outro meio eficaz, os órgãos e entidades para participarem do registro de preços’;

251.2.3. o planejamento da contratação é obrigatório, sendo que se o objeto for solução de TI, caso seja integrante do Sisp, deve executar o processo de planejamento previsto na IN – SLTI/MP 4/2010 (IN – SLTI/MP 4/2010, art. 18, inciso III) ou, caso não o seja, deve realizar os devidos estudos técnicos preliminares (Lei 8.666/1993, art. 6º, inciso IX);

251.2.4. a fixação, no termo de convocação, de quantitativos (máximos) a serem contratados por meio dos contratos derivados da ata de registro de preços, previstos no Decreto 3.931/2001, art. 9º, inciso II, é obrigação e não faculdade do gestor (Acórdão 991/2009-TCU-Plenário, Acórdão 1.100/2007-TCU-Plenário e Acórdão 4.411/2010-TCU-2ª Câmara);

251.2.5. em atenção ao princípio da vinculação ao instrumento convocatório (Lei 8.666/1993, art. 3º, caput), devem gerenciar a ata de forma que a soma dos quantitativos contratados em todos os contratos derivados da ata não supere o quantitativo máximo previsto no edital.

251.3. quando realizarem adesão à ata de registro de preços atentem que:

251.3.1. o planejamento da contratação é obrigatório, sendo que se o objeto for solução de TI, caso seja integrante do Sisp, deve executar o processo de planejamento previsto na IN – SLTI/MP 4/2010 (IN – SLTI/MP 4/2010, art. 18, inciso III) ou, caso não o seja, realizar os devidos estudos técnicos preliminares (Lei 8.666/1993, art. 6º, inciso IX);

251.3.2. devem demonstrar formalmente a vantajosidade da adesão, nos termos do Decreto 3.931/2001, art. 8º;

251.3.3. as regras e condições estabelecidas no certame que originou a ata de registro de preços devem ser conformes as necessidades e condições determinadas na etapa de planejamento da contratação (Lei 8.666/1993, art. 6º, inciso IX, alínea ‘d’, c/c o art. 3º, § 1º, inciso I, e Lei 10.520/2002, art. 3º, inciso II).”

## II

11. Antes de adentrar no exame da questão propriamente dita, cumpre registrar que o SRP, se utilizado de acordo com as normas legais vigentes, apresenta um potencial fantástico de racionalizar as aquisições de bens e serviços pela Administração Pública, podendo trazer significativa economia aos cofres públicos.

12. Estas vantagens, no entanto, não podem ser obtidas à custa do descumprimento da legislação específica de licitações ou dos princípios constitucionais que regem a matéria.

13. A presente auditoria traz mais uma vez à consideração desta Corte um tema de extrema relevância, que diz respeito ao procedimento de adesão à Ata de Registro de Preços, prevista no Decreto nº 3.931/2001.

14. Com efeito, conforme registrado pela Sefti, o Tribunal apreciou a matéria ao proferir o Acórdão nº 1.487/2007 – Plenário, que culminou com determinação para que fossem reavaliadas as regras previstas na supracitada norma regulamentar, de forma a estabelecer limites para a adesão à Ata de Registro de Preços por outros órgãos e entidades.

15. Sobre o assunto, vale destacar o seguinte trecho do voto condutor da referida deliberação, contra a qual foi interposto recurso, ainda não julgado por esta Corte:

“6. Diferente é a situação da adesão ilimitada a atas por parte de outros órgãos. Quanto a essa possibilidade não regulamentada pelo Decreto nº 3.931/2001, comungo o entendimento da unidade técnica e do Ministério Público que essa fragilidade do sistema afronta os princípios da competição e da igualdade de condições entre os licitantes.

7. Refiro-me à regra inserta no art. 8º, § 3º, do Decreto nº 3.931, de 19 de setembro de 2001, que permite a cada órgão que aderir à Ata, individualmente, contratar até 100% dos quantitativos ali registrados. No caso em concreto sob exame, a 4ª Secex faz um exercício de raciocínio em que demonstra a possibilidade real de a empresa vencedora do citado Pregão 16/2005 ter firmado contratos com os 62 órgãos que aderiram à ata, na ordem de aproximadamente 2 bilhões de reais, sendo que, inicialmente, sagrou-se vencedora de um único certame licitatório para prestação de serviços no valor de R\$ 32,0 milhões. Está claro que essa situação é incompatível com a orientação constitucional que preconiza a competitividade e a observância da isonomia na realização das licitações públicas.

200  
69

8. Para além da temática principiológica que, por si só já reclamaria a adoção de providências corretivas, também não pode deixar de ser considerado que, num cenário desses, a Administração perde na economia de escala, na medida em que, se a licitação fosse destinada inicialmente à contratação de serviços em montante bem superior ao demandado pelo órgão inicial, certamente os licitantes teriam condições de oferecer maiores vantagens de preço em suas propostas.”

16. O exemplo acima mencionado demonstra que a adesão ilimitada às atas representa clara ofensa ao disposto no art. 37, inciso XXI, da Constituição Federal, que exige que compras e serviços sejam contratados mediante processo de licitação pública que assegure igualdade de condições a todos os concorrentes.

17. Com relação à ofensa dessa prática ao princípio da obrigatoriedade da licitação, Marçal Justen Filho, vislumbrando, no dispositivo regulamentar ora questionado, a instituição de competência discricionária para a Administração Pública promover contratação direta, tece as seguintes considerações (Comentários à lei de licitações e contratos administrativos. 12ª ed. São Paulo: Dialética, 2008. p. 196):

“Ora, a ausência de obrigatoriedade de contratar e a não-computação dos quantitativos contratados com entidades não participantes do sistema de registro de preços são duas decorrências jurídicas da inexistência de licitação. Se os objetos das referidas licitações tivessem sido abrangidos numa licitação anterior, existiria a inafastável obrigatoriedade de o particular realizar a contratação quando tal lhe fosse demandado e os quantitativos correspondentes seriam computados para cálculo dos limites previstos na licitação.

Evidencia-se, então, que a figura do ‘carona’ corresponde ao aproveitamento dos efeitos de uma licitação anterior, para que uma entidade administrativa promova contratação sem prévia licitação. Configura-se uma situação similar à da dispensa de licitação, fundada na exclusiva discricionariedade administrativa. Essa solução é incompatível com a regra imposta no art. 37, inc. XXI, da CF/88.

Na verdade, produziu-se a instituição por meio de decreto de mais uma hipótese de dispensa de licitação. O problema imediato reside em que a Constituição estabelece que somente a lei pode criar as hipóteses de dispensa de licitação. No caso concreto, nenhuma lei instituiu o ‘carona’.”

18. Quanto à ofensa ao princípio da isonomia, o nobre autor entende que ela decorre dos seguintes aspectos (ob.cit., pp. 190-191):

“O princípio da isonomia impõe que todos os potenciais interessados tomem ciência da extensão das contratações que a Administração pretende realizar. Não é possível que uma licitação aparentemente irrelevante, que não desperta atenção e competição entre os empresários do setor, seja transformada em uma fonte inegociável de contratações para o licitante que a venceu.”

19. Além desses, a adesão ilimitada também contraria os princípios básicos que norteiam a atividade da Administração Pública, como os da legalidade, da imparcialidade, da economicidade, da vinculação ao instrumento convocatório e da moralidade.

20. Vale observar, em termos práticos, que a sistemática de permitir adesões ilimitadas às Atas de Registro de Preços por intermédio de caronas, ao invés de reduzir a possibilidade de fraude ao procedimento licitatório, tende a ampliar esta possibilidade, como observa Marçal Justen Filho no trecho abaixo transcrito (ob. cit., p. 197):

“A consagração do ‘carona’ favorece a prática da corrupção. Em primeiro lugar, envolve a realização de licitações destinadas ao fornecimento de quantitativos enormes, o que se constitui em incentivo a práticas reprováveis. Isso não significa afirmar que existem desvios éticos apenas nas licitações de grande porte. O que se afirma é que a grande dimensão econômica de uma licitação eleva o risco de corrupção em vista do vulto dos valores envolvidos. Mais grave, consiste na criação de competências amplamente discricionárias. Ao assegurar ao ente administrativo a faculdade de escolher entre utilizar ou não utilizar um registro de preços, abre-se a oportunidade para a corrupção. Não significa que a existência do registro de preços seja um instrumento intrinsecamente propício à corrupção; a figura do ‘carona’ é intrinsecamente propícia à corrupção. E o é porque uma entidade pode ou não se valer de um registro de preços, segundo uma escolha livre e incondicionada.” [Grifei.]

21. Registre-se, ademais, que a Sefti constatou a possibilidade de exploração comercial das Atas de Registro de Preços por empresas privadas, como se observa, por exemplo, no site

www.bidsolutions.com.br, que oferece auxílio nas compras via adesão às atas válidas de órgãos federais, estaduais e municipais, informando a existência, na data do acesso, de 35.610 itens em Atas de Registro de Preços e R\$ 63.347.040,34 em itens, além de apresentar o seguinte anúncio: “Quer vender mais a sua Ata de Registro de Preço? A BID SOLUTIONS TE AJUDA!”.

22. Outro exemplo é o site www2.dlink.com.br, que convida os interessados a aproveitar “as facilidades das atas de registro de preços junto a diversos órgãos federais para adquirir as soluções D-Link com mais agilidade”, além de oferecer um “guia de adesão a atas e preços”.

23. Nota-se, claramente, que a adesão ilimitada à Ata de Registro de Preços representa um desvirtuamento do SRP, que tem como pressuposto principal o planejamento das aquisições pela Administração Pública, na medida em que propicia a contratação de muito mais itens do que a quantidade efetivamente licitada.

24. Por esses motivos, entendo que a possibilidade de adesão à Ata de Registro de Preços deve limitar-se à quantidade remanescente no registro.

### III

25. Como mencionado pela Sefti, um aspecto de fundamental importância para o regular funcionamento do SRP é o devido planejamento que deve ser realizado pelo órgão gerenciador e pelos órgãos participantes.

26. Note-se que o inciso III do art. 2º do Decreto nº 3.931/2001 estabelece que será adotado preferencialmente o SRP, entre outras hipóteses, quando for conveniente a aquisição de bens ou a contratação de serviços para atendimento a mais de um órgão ou entidade, ou programas de governo.

27. Por sua vez, os §§ 2º e 3º do art. 3º da referida norma regulamentar estabelecem uma série de procedimentos que devem ser adotados pelo órgão gerenciador e pelos órgãos participantes, que indicam a necessidade de um amplo planejamento para se estabelecer os produtos e serviços que devem constar da ata, conforme se verifica a seguir:

“§ 2º Caberá ao órgão gerenciador a prática de todos os atos de controle e administração do SRP, e ainda o seguinte:

I – convidar, mediante correspondência eletrônica ou outro meio eficaz, os órgãos e entidades para participarem do registro de preços;

II – consolidar todas as informações relativas à estimativa individual e total de consumo, promovendo a adequação dos respectivos projetos básicos encaminhados para atender aos requisitos de padronização e racionalização;

(...)

V – confirmar junto aos órgãos participantes a sua concordância com o objeto a ser licitado, inclusive quanto aos quantitativos e projeto básico;

(...)

VII – gerenciar a Ata de Registro de Preços, providenciando a indicação, sempre que solicitado, dos fornecedores, para atendimento às necessidades da Administração, obedecendo a ordem de classificação e os quantitativos de contratação definidos pelos participantes da Ata;

(...)

§ 3º O órgão participante do registro de preços será responsável pela manifestação de interesse em participar do registro de preços, providenciando o encaminhamento, ao órgão gerenciador, de sua estimativa de consumo, cronograma de contratação e respectivas especificações ou projeto básico, nos termos da Lei nº 8.666, de 1993, adequado ao registro de preço do qual pretende fazer parte, (...). [Grifei.]

28. As compras devidamente planejadas tendem a apresentar significativo ganho de escala, observando-se, assim, os princípios constitucionais da eficiência e da economicidade.

29. Neste sentido, em adição ao exemplo da SLTI/MP citado no Relatório de Auditoria, cabe registrar a notícia publicada no site do Fundo Nacional de Desenvolvimento da Educação – FNDE em 29/11/2011, de que a sistemática de compras governamentais da referida entidade, baseada em pregões eletrônicos para registro de preços nacional, permitiu uma economia de R\$ 1,39 bilhões aos cofres públicos de estados, municípios e do governo federal no período de 2008 a 2011.

30. Quanto à forma pela qual são efetivadas as compras de grande volume para atender os programas e projetos educacionais do MEC promovidos pela entidade, consta a seguinte informação:

“Com base nas estimativas das necessidades dos estados e municípios, o FNDE realiza licitações e registra os preços que passam a ter validade em todo território nacional. Com isso, os ganhos de escala favorecem o governo federal, estados e municípios, que podem aderir a esses registros de preços, realizando, assim, suas compras com rapidez, transparéncia e economicidade.” [Grifei.]

31. Verifica-se, portanto, que os elementos colhidos na presente auditoria comprovam os problemas que decorrem da adesão ilimitada à Ata de Registro de Preços, causados, basicamente, pela marcante ausência de planejamento dos órgãos e entidades da Administração Pública.

32. Registre-se, mais uma vez, que o instituto do SRP apresenta um grande potencial de proporcionar racionalização administrativa e economia para os cofres públicos.

33. Não obstante, a prática disseminada em todos os entes da federação da adesão ilimitada às Atas de Registro de Preços desvirtua o SRP de sua finalidade principal, fundada no planejamento dos órgãos e entidades da Administração Pública, além de afrontar a Constituição Federal e a Lei nº 8.666/93, trazendo, em seu bojo, uma ampla liberalidade que favorece a prática da fraude, do conluio e da corrupção.

#### IV

34. Ante todo o exposto, este representante do Ministério Público manifesta-se em conformidade com a competente análise realizada no título III, subtítulo III.I, do Relatório de Auditoria, que trata dos aspectos legais nas contratações de soluções de TI por meio do Sistema de Registro de Preços (fls. 433/435), bem como com a proposta formulada pela Sefti no item 251 (fl. 435).

É o Relatório.

## APÊNDICES

### Relatórios consolidados

Item	TC	Tipo de fiscalização	Unidade Técnica	Jurisdicionado	Fls. do Anexo 2
1	000.390/2010-0	Levantamento	Sefti	321 órgãos e entidades	2-27
2	009.982/2010-8	Conformidade (ACGTI)	Sefti	Dnit	28-36
3	013.718/2010-0	Conformidade (ACGTI)	Sefti	SE/MS	37-44
4	013.674/2010-2	Conformidade (ACGTI)	Secex/RR	Ibama	45-58
5	014.088/2010-0	Conformidade (ACGTI)	Secex/9	Susep	59-68
6	013.671/2010-3	Conformidade (ACGTI)	Secex/SP	TRT-2ª Região (SP)	69-81
7	013.761/2010-2	Conformidade (ACGTI)	Secex/RR	SE/MCT	82-97
8	017.791/2010-3	Conformidade (ACGTI)	Secex/1	Anatel	98-107
9	019.052/2010-3	Conformidade (ACGTI)	Secex/CE	Dnocs	108-114
10	018.044/2010-7	Conformidade (ACGTI)	Secex/RJ	Finep	115-125
11	017.903/2010-6	Conformidade (ACGTI)	Secex/RS	TRT-4ª Região (RS)	126-136
12	022.488/2010-3	Conformidade (ACGTI)	Secex/6	FNDE	137-147
13	024.193/2010-0	Conformidade (ACGTI)	Secex/AM	ADE	148-158
14	018.911/2010-2	Conformidade (ACGTI)	Secex/5	SE/MRE	159-167
15	024.956/2010-4	Conformidade (ACGTI)	Sefti	SE/MP	168-184
16	028.772/2010-5	Monitoramento	Sefti	onze órgãos e entidades	185-195
17	010.474/2010-2	Conformidade (AE)	Sefti	Dnit	211-222
18	022.241/2010-8	Conformidade (AE)	Sefti	SRF/MF e SE/MP	223-245
19	029.074/2010-0	Conformidade (AE)	Sefti	SE/MS e SAS/MS	246-256
20	029.120/2010-1	Conformidade (AE)	Sefti	CGTI/MCT	196-210

Orcamento dos pesquisados que declararam que o negócio não é afetado

Cod2010	Criticidade	Maturidade	Orcamento2010	Organização
233	5	3	354.187.397,00	Serviço Federal de Processamento de Dados
195	5	1	118.305.000,00	Ministério Das Cidades
138	5	2	59.728.652,00	Furnas Centrais Elétricas S.A.
65	5	1	51.112.796,00	Companhia Energética de Alagoas
243	5	2	43.826.851,00	Superintendência da Zona Franca de Manaus
50	5	1	43.690.792,00	Casa Civil da Presidência da República
178	5	1	42.585.474,00	Irb-Brasil Resseguros S.A.
183	5	2	40.186.768,00	Ministério da Ciência e Tecnologia
193	5	2	31.725.069,00	Ministério da Previdência Social
250	5	2	19.600.000,00	Tribunal de Contas da União
197	5	1	18.646.542,00	Ministério de Minas e Energia
67	5	1	16.466.905,00	Eletrobras Distribuição Piauí
51	5	2	7.502.352,00	Casa da Moeda do Brasil
152	5	2	6.378.288,00	Instituto Brasileiro de Turismo
7	5	1	5.863.100,00	Companhia Docas do Espírito Santo S.A.
246	5	2	4.790.000,00	Superior Tribunal Militar



Cod2010	Criticidade	Maturidade	Orçamento2010	Organização
306	5	1	4.762.947,00	TRIBUNAL REGIONAL FEDERAL 3ª REGIÃO (SP-MS)
343	5	1	3.986.000,00	Universidade Federal do Abc
11	5	1	3.442.878,00	Companhia Docas do Pará S.A.
331	5	1	3.111.552,00	Universidade Federal do Rio de Janeiro
118	5	1	2.915.811,00	Fundação Universidade do Amazonas
8	5	1	2.755.718,00	Companhia Docas do Estado da Bahia S.A.
315	5	1	2.014.438,00	Universidade Federal de Campina Grande
127	5	2	2.012.940,00	Fundação Universidade Federal de São João Del Rei
116	5	2	1.970.000,00	Fundação Oswaldo Cruz
339	5	2	1.800.000,00	Valec Engenharia, Construções e Ferrovias S.A.
300	5	2	1.579.068,00	Tribunal Regional Eleitoral/Sc
228	5	1	1.565.772,00	Secretaria Especial Dos Direitos Humanos
274	5	1	1.506.924,00	TRIBUNAL REGIONAL DO TRABALHO 7ª REGIÃO/CE
104	5	1	1.410.940,00	Fundação Cultural Palmares
112	5	1	1.400.000,00	Fundação Nacional de Artes
95	5	2	1.388.248,00	Empresa Gestora de Ativos
261	5	2	1.182.505,00	TRIBUNAL REGIONAL DO TRABALHO 18ª REGIÃO/GO
285	5	1	1.121.453,00	Tribunal Regional Eleitoral/Go
17	5	2	1.037.450,00	Superintendência de Desenvolvimento da Amazônia
110	5	1	1.010.000,00	Fundação Joaquim Nabuco
150	5	1	927.147,00	Instituto Benjamín Constant
279	5	2	898.200,00	Tribunal Regional Eleitoral/Am
293	5	1	896.890,00	Tribunal Regional Eleitoral/Pi
131	5	1	890.000,00	Universidade Federal do Acre
120	5	2	792.000,00	Fundação Universidade Federal de Mato Grosso
297	5	2	790.553,00	Tribunal Regional Eleitoral/Ro
303	5	1	723.789,00	Tribunal Regional Eleitoral/To
166	5	1	709.600,00	Instituto Nacional de Educação de Surdos
123	5	1	621.000,00	Fundação Universidade Federal de Pelotas
64	5	1	539.097,00	Companhia Docas do Rio Grande do Norte S.A.
322	5	1	504.000,00	Universidade Federal de Roraima
291	5	2	473.872,00	Tribunal Regional Eleitoral/Pb
288	5	1	457.800,00	Tribunal Regional Eleitoral/Ms
97	5	1	430.000,00	Universidade Federal do Triângulo Mineiro
106	5	1	420.000,00	Fundação Universidade Federal de Ciências Médicas de Porto Alegre
289	5	1	399.488,00	Tribunal Regional Eleitoral/Mt
277	5	2	391.190,00	Tribunal Regional Eleitoral/Ac
124	5	1	379.757,00	Fundação Universidade Federal de Rondônia
102	5	1	302.000,00	Fundação Casa de Rui Barbosa

Cod2010	Criticidade	Maturidade	Orçamento2010	Organização
341	5	1	300.000,00	Universidade Federal da Grande Dourados
260	5	2	200.000,00	TRIBUNAL REGIONAL DO TRABALHO 17 <sup>a</sup> REGIÃO/ES
115	5	1	145.000,00	Fundação Osório
280	5	1	119.000,00	Tribunal Regional Eleitoral/Ap
18	5	1	107.334,00	Superintendência de Desenvolvimento do Nordeste
226	5	1	100.000,00	Secretaria Especial de Políticas de Promoção da Igualdade Racial
10	5	1	61.000,00	Companhia Docas do Maranhão S.A.
336	5	1	50.000,00	Universidade Federal Rural da Amazônia
344	5	1	zero	Universidade Federal do Oeste do Pará
259	5	1	zero	Tribunal Regional do Trabalho 16 <sup>a</sup> Região/Ma
179	5	1	zero	Eletrobrás Participações S.A.
175	5	2	zero	Instituto Nacional do Câncer
170	5	1	zero	Instituto Nacional de Pesquisas da Amazônia
161	5	1	zero	Instituto Evandro Chagas
155	5	1	zero	Instituto de Desenvolvimento Sustentável Mamirauá
141	5	2	zero	Grupo Hospitalar Conceição
132	5	2	zero	Fundaçao Universidade Federal do Amapá
94	5	1	zero	Empresa Gerencial de Projetos Navais
63	5	2	zero	Companhia de Entrepostos e Armazéns Gerais de São Paulo
59	5	1	zero	Companhia Brasileira de Trens Urbanos
35	5	2	zero	Associação Das Pioneiras Sociais
9	5	1	zero	Companhia Docas do Estado de São Paulo S.A.

## OGS e seus mandatos

Conselho Nacional da Justiça (CNJ)	<b>Constituição Federal:</b> Art. 103-B, § 4º) Compete ao Conselho [Nacional de Justiça] o controle da atuação administrativa e financeira do Poder Judiciário e do cumprimento dos deveres funcionais dos juízes, cabendo-lhe, além de outras atribuições que lhe forem conferidas pelo Estatuto da Magistratura: (...) II – zelar pela observância do art. 37 (...)
Conselho Nacional do Ministério Público (CNMP)	<b>Constituição Federal:</b> Art. 130-A, § 2º) Compete ao Conselho Nacional do Ministério Público o controle da atuação administrativa e financeira do Ministério Público e do cumprimento dos deveres funcionais de seus membros, cabendo-lhe: (...) II – zelar pela observância do art. 37 (...)
Advocacia-Geral da União (AGU/PR)	<b>Lei 10.683/2003:</b> Art. 12. Ao Advogado-Geral da União, o mais elevado órgão de assessoramento jurídico do Poder Executivo, incumbe assessorar o Presidente da República em assuntos de natureza jurídica, elaborando pareceres e estudos ou propondo normas, medidas, diretrizes, assistir-lhe no controle interno da legalidade dos atos da Administração Pública Federal, sugerir-lhe medidas de caráter jurídico reclamadas pelo interesse público e apresentar-lhe as informações a ser prestadas ao Poder Judiciário quando impugnado ato

	ou omissão presidencial, dentre outras atribuições fixadas na Lei Complementar nº 73, de 10 de fevereiro de 1993.
Controladoria-Geral da União (CGU/PR)	Lei 10.683/2003: Art. 17. À Controladoria-Geral da União compete assistir direta e imediatamente ao Presidente da República no desempenho de suas atribuições quanto aos assuntos e providências que, no âmbito do Poder Executivo, sejam atinentes à defesa do patrimônio público, ao controle interno, à auditoria pública, à correição, à prevenção e ao combate à corrupção, às atividades de ouvidoria e ao incremento da transparência da gestão no âmbito da administração pública federal.
Gabinete da Segurança Institucional (GSI/PR)	Lei 10.683/2003: Art. 6º Ao Gabinete de Segurança Institucional da Presidência da República compete: (...) IV – coordenar as atividades de inteligência federal e de segurança da informação;
Ministério do Planejamento, Orçamento e Gestão (MP)	Lei 10.683/2003: Art. 27. Os assuntos que constituem áreas de competência de cada Ministério são os seguintes: (...) XVII – Ministério do Planejamento, Orçamento e Gestão: (...) g) coordenação e gestão dos sistemas de planejamento e orçamento federal, de pessoal civil, de organização e modernização administrativa, de administração de recursos da informação e informática e de serviços gerais;
Secretaria de Logística e Tecnologia da Informação (SLTI/MP)	Lei 10.683/2003: Art. 27. Os assuntos que constituem áreas de competência de cada Ministério são os seguintes: (...) XVII – Ministério do Planejamento, Orçamento e Gestão: (...) g) coordenação e gestão dos sistemas de planejamento e orçamento federal, de pessoal civil, de organização e modernização administrativa, de administração de recursos da informação e informática e de serviços gerais. Decreto 7.063/2010: Art. 28. À Secretaria de Logística e Tecnologia da Informação compete planejar, coordenar, supervisionar e orientar normativamente as atividades de administração dos recursos de informação e informática, de serviços gerais e de gestão de convênios e contratos de repasse, bem como propor políticas e diretrizes a elas relativas, no âmbito da administração federal direta, autárquica e fundacional. Decreto 7.579/2011: Art. 4º Compete ao Órgão Central do SISP: I – orientar e administrar os processos de planejamento estratégico, de coordenação geral e de normalização relativos aos recursos de tecnologia da informação abrangidos pelo SISP; II – definir, elaborar, divulgar e implementar, com apoio da Comissão de Coordenação, as políticas, diretrizes e normas gerais relativas à gestão dos recursos do SISP e ao processo de compras do Governo na área de tecnologia da informação; III – promover a elaboração de planos de formação, desenvolvimento e treinamento do pessoal envolvido na área de abrangência do SISP; IV – incentivar ações prospectivas, visando acompanhar as inovações técnicas da área de tecnologia da informação, de forma a atender às necessidades de modernização dos serviços dos órgãos e entidades abrangidos pelo SISP; e V – promover a disseminação das políticas, diretrizes, normas e informações disponíveis, de interesse comum, entre os órgãos e entidades abrangidos pelo SISP.
Secretaria do Orçamento Federal (SOF/MP)	Lei 10.180/2001: Art. 4º Integram o Sistema de Planejamento e de Orçamento Federal: I – o Ministério do Planejamento, Orçamento e Gestão, como órgão central; (...) Art. 8º Compete às unidades responsáveis pelas atividades de orçamento: (...) II – estabelecer normas e procedimentos necessários à elaboração e à implementação dos orçamentos federais, harmonizando-os com o plano plurianual; Lei 10.683/2003:

	<p>Art. 27. Os assuntos que constituem áreas de competência de cada Ministério são os seguintes: (...) <b>XVII – Ministério do Planejamento, Orçamento e Gestão:</b> (...) g) coordenação e gestão dos sistemas de planejamento e orçamento federal, de pessoal civil, de organização e modernização administrativa, de administração de recursos da informação e informática e de serviços gerais; <b>Decreto 7.063/2010:</b> <b>Art. 17.</b> À Secretaria de Orçamento Federal compete: (...) II – estabelecer as normas necessárias à elaboração e à implementação dos orçamentos federais sob sua responsabilidade;</p>
Departamento de Coordenação e Governança das Estatais (Dest/MP)	<p>Lei 10.683/2003: Art. 27. Os assuntos que constituem áreas de competência de cada Ministério são os seguintes: (...) <b>XVII – Ministério do Planejamento, Orçamento e Gestão:</b> (...) h) formulação de diretrizes, coordenação e definição de critérios de governança corporativa das empresas estatais federais; <b>Decreto 7.063/2010:</b> <b>Art. 6º</b> Ao Departamento de Coordenação e Governança das Empresas Estatais compete: (...) <b>XII</b> – contribuir para o aumento da eficiência e transparência das empresas estatais e para o aperfeiçoamento e integração dos sistemas de monitoramento econômico-financeiro, bem como para o aperfeiçoamento da gestão dessas empresas.</p>
Fundação Escola Nacional de Administração Pública (Enap/MP)	<p>Decreto 5.707/2006: Art. 6º Os órgãos e entidades da administração pública federal direta, autárquica e fundacional deverão incluir em seus planos de capacitação ações voltadas à habilitação de seus servidores para o exercício de cargos de direção e assessoramento superiores, as quais terão, na forma do art. 9º da lei 7.834, de 6 de outubro de 1989, prioridade nos programas de desenvolvimento de recursos humanos. Parágrafo único. Caberá à ENAP promover, elaborar e executar ações de capacitação para os fins do disposto no caput, bem assim a coordenação e supervisão dos programas de capacitação gerencial de pessoal civil executados pelas demais escolas de governo da administração pública federal direta, autárquica e fundacional.</p>
Secretaria do Tesouro Nacional (STN/MF)	<p>Lei 10.180/2001: <b>Art. 17.</b> Integram o Sistema de Contabilidade Federal: I – a Secretaria do Tesouro Nacional, como órgão central; (...) <b>Art. 18.</b> Compete às unidades responsáveis pelas atividades do Sistema de Contabilidade Federal: (...) II – estabelecer normas e procedimentos para o adequado registro contábil dos atos e dos fatos da gestão orçamentária, financeira e patrimonial nos órgãos e nas entidades da Administração Pública Federal;</p>
Comitê Gestor da Política Nacional de Desenvolvimento de Pessoal	<p>Decreto 5.707/2006: Art. 7º Fica criado o Comitê Gestor da Política Nacional de Desenvolvimento de Pessoal, com as seguintes competências: I – avaliar os relatórios anuais dos órgãos e entidades, verificando se foram observadas as diretrizes da Política Nacional de Desenvolvimento de Pessoal; II – orientar os órgãos e entidades da administração pública federal direta, autárquica e fundacional na definição sobre a alocação de recursos para fins de capacitação de seus servidores; III – promover a disseminação da Política Nacional de Desenvolvimento de Pessoal entre os dirigentes dos órgãos e das entidades, os titulares das unidades de recursos humanos, os responsáveis pela capacitação, os servidores públicos federais e suas entidades representativas; e IV – zelar pela observância do disposto neste Decreto.</p>

Câmara de Políticas de Gestão, Desempenho e Competitividade (CGDC) do Conselho de Governo	Decreto 7.478/2011: Art. 2º Compete à CGDC: (...) II – estabelecer diretrizes estratégicas e planos para formulação e implementação de políticas de melhoria da gestão da administração pública federal;
Comissão Interministerial de Governança Corporativa e de Administração de Participações Societárias da União (CGPAR)	Decreto 6.021/2007: Art. 3º Compete à CGPAR: (...) I – aprovar diretrizes e estratégias relacionadas à participação acionária da União nas empresas estatais federais, com vistas à: (...) b) promoção da eficiência na gestão, inclusive quanto à adoção das melhores práticas de governança corporativa;

### Possíveis achados e critérios de auditoria

	Achado	Critérios	
1	Inexistência do planejamento estratégico institucional	Decreto-Lei 200/1967, art. 6º, inciso I, e art. 7º; Critério de Avaliação 2 do Gespública.	Decreto-Lei 200/1967, art. 6º, inciso I, art. 7º; Critério de Avaliação 2 do Gespública; Resolução – CNJ 70/2009, art. 2º
2	Falhas no plano estratégico	Decreto-Lei 200/1967, art. 6º, inciso I, e art. 7º; Critério de Avaliação 2 do Gespública.	Decreto-Lei 200/1967, art. 6º, inciso I, e art. 7º; Critério de Avaliação 2 do Gespública; Resolução – CNJ 70/2009, art. 2º
3	Falhas no processo de planejamento estratégico institucional	Decreto-Lei 200/1967, art. 6º, inciso I, e art. 7º; Critério de Avaliação 2 do Gespública.	Decreto-Lei 200/1967, art. 6º, inciso I, e art. 7º; Critério de Avaliação 2 do Gespública; Resolução – CNJ 70/2009, art. 2º
4	Inexistência do PDTI	Instrução Normativa 4/2008 – SLTI/MPOG, art. 3º; Instrução Normativa 4/2008 – SLTI/MPOG, art. 4º, III; Cobit 4.1, processo PO1 – Planejamento Estratégico de TI.	Resolução – CNJ 90/2009, art. 11; Resolução – CNJ 99/2009, art. 2º; Cobit 4.1, processo PO1 – Planejamento Estratégico de TI.
5	Falhas no PDTI	Decreto-Lei 200/1967, art. 6º, inciso I; Instrução Normativa 4/2008 – SLTI/MPOG, art. 3º; Instrução Normativa 4/2008 – SLTI/MPOG, art. 4º, III; Cobit 4.1, processo PO1 – Planejamento Estratégico de TI.	Resolução – CNJ 90/2009; Resolução – CNJ 99/2009; Cobit 4.1, processo PO1 – Planejamento Estratégico de TI.
6	Falhas no processo de planejamento de TI	Decreto-Lei 200/1967, art. 6º, inciso I, e art. 7º; Cobit 4.1, processo PO1 – Planejamento Estratégico de TI.	Resolução – CNJ 90/2009; Resolução – CNJ 99/2009; Cobit 4.1, processo PO1 – Planejamento Estratégico de TI.
7	Inexistência de comitê de TI	Instrução Normativa 4/2008 – SLTI/MPOG, art. 4º, IV; Cobit 4.1, PO4.2 – Comitê Estratégico de TI; Cobit 4.1, PO4.3 – Comitê Diretor de TI.	Resolução – CNJ 90/2009, art. 12; Cobit 4.1, PO4.2 – Comitê Estratégico de TI; Cobit 4.1, PO4.3 – Comitê Diretor de TI.
8	Falhas relativas ao comitê de TI	Cobit 4.1, PO4.2 – Comitê Estratégico de TI; Cobit 4.1, PO4.3 – Comitê Diretor de TI.	Resolução – CNJ 90/2009, art. 12; Cobit 4.1, PO4.2 – Comitê Estratégico de TI; Cobit 4.1, PO4.3 – Comitê Diretor de TI.

9	Inexistência de definição formal de papéis e responsabilidades	Lei 8.112/1990, art. 13; Cobit 4.1, PO4.6 – Estabelecimento de papéis e responsabilidades.	Lei 8.112/1990, art. 13; Resolução – CNJ 90/2009, art. 10; Cobit 4.1, PO4.6 – Estabelecimento de papéis e responsabilidades.
10	Papéis sensíveis sem responsável	Decreto-Lei 200/1967, art. 10, § 7º	Resolução – CNJ 90/2009, art. 2º, § 1º
11	Papel sensível exercido por não servidor	Decreto-Lei 200/1967, art. 10, § 7º	Resolução – CNJ 90/2009, art. 2º, § 1º e § 3º
12	Inexistência de avaliação do quadro de pessoal de TI	Decreto 5.707/2006, art. 1º, inciso III; Cobit 4.1, PO4.12 – Pessoal de TI.	Decreto 5.707/2006, art. 1º, inciso III; Resolução – CNJ 90/2009, art. 2º, § 4º; Cobit 4.1, PO4.12 – Pessoal de TI.
13	Falhas na avaliação do quadro de pessoal de TI	Decreto 5.707/2006, art. 1º, inciso III; Cobit 4.1, PO4.12 – Pessoal de TI.	Decreto 5.707/2006, art. 1º, inciso III; Resolução – CNJ 90/2009, art. 2º, § 4º; Cobit 4.1, PO4.12 – Pessoal de TI.
14	Inadequação do quadro de pessoal de TI	Cobit 4.1, PO 4.12 – Pessoal de TI.	Cobit 4.1, PO4.12 – Pessoal de TI; Resolução – CNJ 90/2009, art. 2º, § 4º
15	Inexistência de orçamento de TI na LOA	Lei 12.017/2009 (LDO 2009/2010), art. 9º, II, c/c Anexo II, XVIII; Cobit 4.1, processo PO5.3 – Orçamentação de TI; Gespública, critério de avaliação 7.3.	Lei 12.017/2009 (LDO 2009/2010), art. 9º, II, c/c Anexo II, XVIII; Cobit 4.1, processo PO5.3 – Orçamentação de TI; Gespública, Critério de Avaliação 7.3.
16	Falhas no orçamento de TI constante da LOA	Lei 12.017/2009 (LDO 2009/2010), art. 9º, II, c/c Anexo II, XVIII; Cobit 4.1, processo PO5.3 Orçamentação de TI; Gespública, Critério de Avaliação 7.3.	Lei 12.017/2009 (LDO 2009/2010), art. 9º, II, c/c Anexo II, XVIII; Cobit 4.1, processo PO5.3 – Orçamentação de TI; Gespública, Critério de Avaliação 7.3.
17	Inexistência de controle da execução do orçamento de TI	Lei 4.320/1964, art. 75, inciso III.	Lei 4.320/1964, art. 75, inciso III.
18	Falhas no controle da execução do orçamento de TI	Lei 4.320/1964, art. 75, inciso III.	Lei 4.320/1964, art. 75, inciso III.
19	Inexistência de processo de software	Lei 8.666/1993, art. 6º, inciso IX; Instrução Normativa 4/2008 – SLTI/MPOG, art. 12, II; Normas NBR ISO/IEC 12.207 e 15.504.	Lei 8.666/1993, art. 6º, inciso IX; Resolução – CNJ 90/2009, art. 10; Normas NBR ISO/IEC 12.207 e 15.504.
20	Falhas no processo de software	Lei 8.666/1993, art. 6º, inciso IX; Instrução Normativa 4/2008 – SLTI/MPOG, art. 12, II; Normas NBR ISO/IEC 12.207 e 15.504.	Lei 8.666/1993, art. 6º, inciso IX; Resolução – CNJ 90/2009, art. 10; Normas NBR ISO/IEC 12.207 e 15.504.
21	Inexistência de processo de gerenciamento de projetos	Cobit 4.1, processo PO10.2 – Estruturas de Gerência de Projetos; PMBOK.	Resolução – CNJ 90/2009, art. 10; Cobit 4.1, processo PO10.2 – Estruturas de Gerência de Projetos; PMBOK.
22	Falhas no processo de gerenciamento de projetos	Cobit 4.1, processo PO10.2 – Estruturas de Gerência de Projetos; PMBOK.	Resolução – CNJ 90/2009, art. 10; Cobit 4.1, processo PO10.2 – Estruturas de Gerência de Projetos; PMBOK.
23	Inexistência do processo de gestão de incidentes	Cobit 4.1, processo DS8 – Gerenciar a central de serviços e incidentes; NBR ISO/IEC 20.000; NBR 27.002.	Resolução – CNJ 90/2009, art. 10; Cobit 4.1, processo DS8 – Gerenciar a central de serviços e incidentes; NBR ISO/IEC 20.000; NBR 27.002.
24	Falhas no processo de gestão de incidentes	Cobit 4.1, processo DS8 – Gerenciar a central de serviços e incidentes; NBR ISO/IEC 20.000; NBR 27.002.	Resolução – CNJ 90/2009, art. 10; Cobit 4.1, processo DS8 – Gerenciar a central de serviços e incidentes; NBR ISO/IEC 20.000; NBR 27.002.
25	Inexistência do processo de gestão de configuração	Cobit 4.1, processo DS9 – Gerenciar configuração; NBR ISO/IEC 20.000.	Resolução – CNJ 90/2009, art. 10; Cobit 4.1, processo DS9 – Gerenciar configuração; NBR ISO/IEC 20.000.

26	Falhas no processo de gestão de configuração	Cobit 4.1, processo DS9 – Gerenciar configuração; NBR ISO/IEC 20.000.	Resolução – CNJ 90/2009, art. 10; Cobit 4.1, processo DS9 – Gerenciar configuração; NBR ISO/IEC 20.000.
27	Inexistência do processo de gestão de mudanças	NBR ISO/IEC 27.002, item 12.5.1; – Cobit 4.1, processo AI6 – Gerenciar mudanças; NBR ISO/IEC 20.000.	Resolução – CNJ 90/2009, art. 10; – Cobit 4.1, processo AI6 – Gerenciar mudanças; NBR ISO/IEC 27.002, item 12.5.1; NBR ISO/IEC 20.000.
28	Falhas no processo de gestão de mudanças	NBR ISO/IEC 27.002, item 12.5.1; – Cobit 4.1, processo AI6 – Gerenciar mudanças; NBR ISO/IEC 20.000.	Resolução – CNJ 90/2009, art. 10; – Cobit 4.1, processo AI6 – Gerenciar mudanças; NBR ISO/IEC 27.002, item 12.5.1; NBR ISO/IEC 20.000.
29	Inexistência de gestor de segurança da informação e comunicações	Instrução Normativa GSI/PR 1/2008, art. 5º, IV e art. 7º; Norma Complementar 3/IN01/DSIC/GSIPR, item 5.3.7.2; NBR ISO/IEC 27.002, item 6.1.3 – Atribuição de responsabilidade para segurança da informação.	Instrução Normativa GSI/PR 1/2008, art. 5º, IV e art. 7º; Norma Complementar 3/IN01/DSIC/GSIPR, item 5.3.7.2; NBR ISO/IEC 27.002, item 6.1.3 – Atribuição de responsabilidade para segurança da informação.
30	Inexistência de comitê de segurança da informação e comunicações	Instrução Normativa GSI/PR 1/2008, art. 5º, VI; Norma Complementar 3/IN01/DSIC/GSIPR, item 5.3.7.3; NBR ISO/IEC 27.002, item 6.1.2 – Coordenação de segurança da informação.	Instrução Normativa GSI/PR 1/2008, art. 5º, VI; Norma Complementar 3/IN01/DSIC/GSIPR, item 5.3.7.3; NBR ISO/IEC 27.002, item 6.1.2 – Coordenação de segurança da informação.
31	Falhas no comitê de segurança da informação e comunicações	Instrução Normativa GSI/PR 1/2008, art. 5º, VI; Norma Complementar 3/IN01/DSIC/GSIPR, item 5.3.7.3; NBR ISO/IEC 27.002, item 6.1.2 – Coordenação de segurança da informação.	Instrução Normativa GSI/PR 1/2008, art. 5º, VI; Norma Complementar 3/IN01/DSIC/GSIPR, item 5.3.7.3; NBR ISO/IEC 27.002, item 6.1.2 – Coordenação de segurança da informação.
32	Inexistência de Política de Segurança da Informação e Comunicações (Posic)	Instrução Normativa – GSI/PR 1/2008, art. 5º, VII; Norma Complementar 3/IN01/DSIC/GSIPR.	Instrução Normativa – GSI/PR 1/2008, art. 5º, inciso VII; Norma Complementar 3/IN01/DSIC/GSIPR; Resolução – CNJ 90/2009, art. 13; NBR – ISO/IEC 27.002, item 5.1 – Política de Segurança da Informação.
33	Falhas na Política de Segurança da Informação e Comunicações (Posic)	Instrução Normativa GSI/PR 1/2008, art. 5º, VII; Norma Complementar 3/IN01/DSIC/GSIPR.	Instrução Normativa – GSI/PR 1/2008, art. 5º, inciso VII; Norma Complementar 3/IN01/DSIC/GSIPR; Resolução – CNJ 90/2009, art. 13; NBR – ISO/IEC 27.002, item 5.1 – Política de Segurança da Informação.
34	Inexistência de Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (Etri)	Instrução Normativa GSI/PR 1/2008, art. 5º, V; Norma Complementar 5/IN01/DSIC/GSIPR.	Instrução Normativa – GSI/PR 1/2008, art. 5º, inciso V; Norma Complementar 5/IN01/DSIC/GSIPR.
35	Falhas na Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (Etri)	Instrução Normativa GSI/PR 1/2008, art. 5º, V; Norma Complementar 5/IN01/DSIC/GSIPR.	Instrução Normativa – GSI/PR 1/2008, art. 5º, inciso V; Norma Complementar 5/IN01/DSIC/GSIPR.
36	Inexistência de classificação da informação	Decreto 4.553/2002, art. 6º, § 2º, inciso II, e art. 67; NBR ISO/IEC 27.002, item 7.2.	Decreto 4.553/2002, art. 6º, § 2º, incisos I e II, art. 67; NBR – ISO/IEC 27.002, item 7.2 – Classificação da informação.

37	Inexistência de inventário dos ativos de informação	Instrução Normativa GSI/PR 1/2008, art. 5º, VII; Norma Complementar 4/IN01/DSIC/GSIPR, item 5.2.1; NBR ISO/IEC 27.002, item 7.1.	Resolução – CNJ 90/2009, art. 9º, § 2º; art. 10; Instrução Normativa GSI/PR 1/2008, art. 5º, VII; Norma Complementar 4/IN01/DSIC/GSIPR, item 5.2.1; NBR ISO/IEC 27.002, item 7.1 – Inventário de ativos.
38	Falhas no inventário dos ativos de informação	Instrução Normativa GSI/PR 1/2008, art. 5º, VII; Norma Complementar 4/IN01/DSIC/GSIPR, item 5.2.1; NBR ISO/IEC 27.002, item 7.1.	Resolução – CNJ 90/2009, art. 9º, § 2º e art. 10; Instrução Normativa GSI/PR 1/2008, art. 5º, VII; Norma Complementar 4/IN01/DSIC/GSIPR, item 5.2.1; NBR ISO/IEC 27.002, item 7.1 – Inventário de ativos.
39	Inexistência de Processo de Gestão de Riscos de Segurança da Informação (GRSIC)	Instrução Normativa GSI/PR 1/2008, art. 5º, VII; Norma Complementar 4/IN01/DSIC/GSIPR.	Resolução – CNJ 90/2009, art. 10; Instrução Normativa GSI/PR 1/2008, art. 5º, VII; Norma Complementar 4/IN01/DSIC/GSIPR; Cobit 4.1, processo PO9 – Avaliar e gerenciar riscos de TI; NBR 27.005 – Gestão de Riscos de Segurança da Informação.
40	Falhas no Processo de Gestão de Riscos de Segurança da Informação (GRSIC)	Instrução Normativa GSI/PR 1/2008, art. 5º, VII; Norma Complementar 4/IN01/DSIC/GSIPR.	Resolução – CNJ 90/2009, art. 10; Instrução Normativa GSI/PR 1/2008, art. 5º, VII; Norma Complementar 4/IN01/DSIC/GSIPR; Cobit 4.1, processo PO9 – Avaliar e gerenciar riscos de TI; NBR 27.005 – Gestão de Riscos de Segurança da Informação.
41	Inexistência de plano anual de capacitação	Decreto 5.707/2006, art. 5º, § 2º; Portaria – MP 208/2006, art. 2º, I, e art. 4º; Cobit 4.1, PO7.2 – Competências Pessoais; Cobit 4.1, PO7.4 – Treinamento do Pessoal.	Resolução – CNJ 90/2009, art. 3º; Cobit 4.1, processo PO7.2 – Competências Pessoais; Cobit 4.1, PO7.4 – Treinamento do Pessoal.
42	Plano anual de capacitação não contempla a área de gestão de TI	Cobit 4.1, processo PO7.2 – Competências Pessoais; Cobit 4.1, PO7.4 – Treinamento do Pessoal.	Resolução – CNJ 90/2009, art. 3º
43	Inexistência de avaliação da gestão de TI	Cobit 4.1, itens ME1.4 – Avaliação de desempenho; ME1.5 – Relatórios gerenciais; ME1.6 – Ações corretivas; ME2 – Monitorar e avaliar os controles internos.	Resolução – CNJ 90/2009, art. 10; Cobit 4.1, itens ME1.4 – Avaliar o desempenho; ME1.5 – Relatórios gerenciais; ME1.6 – Ações corretivas; ME2 – Monitorar e avaliar os controles internos.
44	Falhas na avaliação da gestão de TI	Cobit 4.1, itens ME1.4 – Avaliação de desempenho; ME1.5 – Relatórios gerenciais; ME1.6 – Ações corretivas; ME2 – Monitorar e avaliar os controles internos.	Resolução – CNJ 90/2009, art. 10; Cobit 4.1, itens ME1.4 – Avaliar o desempenho; ME1.5 – Relatórios gerenciais; ME1.6 – Ações corretivas; ME2 – Monitorar e avaliar os controles internos.



45	Auditória interna não apoia avaliação da TI	Cobit 4.1, ME2 – Monitorar.	Resolução – CNJ 90/2009, art. 10; Cobit 4.1, ME2 – Monitorar e avaliar os controles internos.
46	Inexistência de controles que promovam o cumprimento da IN 4	IN 63/2010-TCU, Art.1º, § 1º, X.	Não se aplica.
47	Falhas nos controles que promovam o cumprimento da IN 4	IN 63/2010-TCU, Art.1º, § 1º, X.	Não se aplica.
48	Inexistência de controles que façam com que o termo de referência ou projeto básico seja elaborado a partir de estudos técnicos preliminares	IN 63/2010-TCU, Art.1º, § 1º, X.	IN 63/2010-TCU, Art.1º, § 1º, X.
49	Descumprimento do processo de planejamento de acordo com a IN4	Instrução Normativa 4/2008 - SLTI/MPOG.	Não se aplica.
50	Inexistência dos estudos técnicos preliminares	Lei 8.666/1993, art. 6º, IX.	Lei 8.666/1993, art. 6º, IX.
51	Irregularidades na contratação	Diversos.	Diversos.
52	Inexistência de controles que promovam a regular gestão contratual	IN 63/2010-TCU, Art.1º, § 1º, X.	IN 63/2010-TCU, Art.1º, § 1º, X.
53	Falhas nos controles que promovam a regular gestão contratual	IN 63/2010-TCU, Art.1º, § 1º, X.	IN 63/2010-TCU, Art.1º, § 1º, X.
54	Irregularidades na gestão contratual	Diversos.	Diversos.



Ofício de Comunicação de Auditoria  
OFÍCIO DE COMUNICAÇÃO DE AUDITORIA  
Ofício {n.}/2010-{unidade}

Brasília, {dd} de {mmmm} de 2010.

{Senhor/Senhora} {cargo} {do/da} {órgão auditado},

Comunico a {pron. tratamento} que este Tribunal está iniciando trabalho de fiscalização, ora na fase de planejamento, cujo objetivo é avaliar a gestão e o uso de Tecnologia da Informação (TI) {desse/dessa} {natureza jurídica do órgão auditado}.

Trata-se de trabalho complementar ao realizado no âmbito do TC 000.390/2010-0, no qual foram solicitadas a {pron. tratamento}, por meio do {Aviso/Ofício}, de {data do aviso/ofício}, informações referentes à situação de governança de TI {nesse/nessa} {natureza jurídica do órgão auditado}, pelo preenchimento de questionário em formato PDF.

A equipe de fiscalização apresentar-se-á {nesse/nessa} {natureza jurídica órgão auditado} provavelmente no dia {data início trabalhos}, para início dos trabalhos, os quais se pretende findar no dia {data término trabalhos}.

Desse modo, solicito a {pron. tratamento} as seguintes providências:

a) disponibilização dos documentos e informações constantes do anexo I a este ofício, organizados na ordem em que estão listados, até o dia {data limite anexo I}, em papel e em meio eletrônico, caso disponível;

b) disponibilização dos documentos e informações constantes do anexo II a este ofício, organizados na ordem em que estão listados, até o dia {data limite anexo II}, em papel e em meio eletrônico, caso disponível;

c) designação formal de servidor (nome, matrícula, cargo, telefone e e-mail) para acompanhamento do fornecimento dos documentos referentes a essa e futuras solicitações da equipe de fiscalização, juntamente com o envio das informações do item anterior;

d) disponibilização de local para o trabalho da equipe, com linha telefônica, microcomputador para uso de editor de textos e planilhas, com acesso à internet, e impressora para impressão de documentos com poucas páginas, a partir de {data início disponibilização local};

e) divulgação da realização desse trabalho do TCU junto aos servidores e prestadores de serviços {desse/dessa} {natureza jurídica órgão auditado}, informando o objetivo do trabalho, o período em que a equipe estará nas dependências {do/da} {natureza jurídica órgão auditado} e o telefone (61) 3316-5371 para quaisquer informações ou esclarecimentos sobre o trabalho, de forma a tornar transparente a atuação desta Corte de Contas.

Quando as informações existirem em meio eletrônico, podem ser encaminhadas para o endereço {e-mail da unidade}, permanecendo as versões em papel assinadas no Unidade à disposição da equipe de auditoria. Caso somente existam em papel, devem ser encaminhadas para esta Secretaria no endereço constante da página seguinte.

Em caso de indisponibilidade ou inexistência dos referidos documentos ou informações, favor registrar formalmente tal fato à equipe já na data de sua apresentação.

Cientificamos {pron. tratamento} que a sonegação de processo, documento ou informação ensejará a aplicação de multa nos termos do art. 268, inciso VI, do Regimento Interno do Tribunal de Contas da União e art. 58, inciso VI, da Lei 8.443/1992.

Qualquer dúvida sobre os dados solicitados pode ser esclarecida por telefone ou e-mail junto aos auditores A1 (Tel1, e-mail1); A2 (Tel2, e-mail2), A3(Tel3, e-mail3) ou A4 (Tel4, e-mail4).

Por oportuno, solicito os bons préstimos de {pron. tratamento} no sentido de, ao final dos trabalhos da equipe de auditoria, realizar avaliação da qualidade do trabalho desenvolvido por meio do questionário em anexo, que pode ser encaminhado diretamente à Sefti no seguinte endereço:



Secretaria de Fiscalização de Tecnologia da Informação  
A/C: Cláudio Souza Castello Branco (Secretário)  
SAFS Quadra 4, Lote 1, Anexo 1, sala 304  
CEP: 70042-900 Brasília/DF

Atenciosamente,

{Nome do Secretário}  
Secretário

A {pron. Tratamento} {o/a} {Senhor/Senhora}  
{nome do destinatário}  
{cargo} {do/da} {órgão auditado}

## Anexo I

Os documentos e informações solicitadas neste anexo serão tratados como evidências das respostas do questionário em formato PDF encaminhadas em atenção às solicitações contidas no {Aviso/Ofício} {aviso/ofício}, de {data do aviso/ofício}. As requisições farão referência aos itens do questionário supra.

1. Com relação ao processo de planejamento estratégico institucional do órgão:
  - 1.1. evidências que comprovem a resposta ao item 2.1 do questionário;
  - 1.2. caso exista um plano estratégico institucional (PEI) ou documento equivalente:
    - 1.2.1. cópia do plano com evidência da formalização no âmbito {do/da} {natureza jurídica e órgão auditado} (a formalização envolve a aprovação de um documento pelos responsáveis e a posterior publicação para todos os interessados);
    - 1.2.2. evidências de que houve envolvimento das diversas áreas de negócio no planejamento estratégico institucional;
    - 1.2.3. evidências de que os planos de ação são divulgados para os servidores da instituição;
    - 1.2.4. evidências de que houve desdobramento (planos de ação de curto e médio prazos estabelecidos) pelas unidades executoras e alinhados com as iniciativas estratégicas do PEI;
    - 1.2.5. evidências de que o PEI é avaliado.
  2. Com relação ao planejamento de tecnologia da informação (PO1 – Definir um planejamento estratégico de TI):
    - 2.1. evidências que comprovem a resposta ao item 2.2 do questionário;
    - 2.2. caso exista um plano estratégico de TI, ou documento equivalente:
      - 2.2.1. cópia do plano com evidência da formalização no âmbito {do/da} {natureza jurídica e órgão auditado};
      - 2.2.2. informar as partes envolvidas na elaboração do plano;
      - 2.2.3. apresentar o desdobramento do plano pelas unidades executoras (internas ou externas ao ente), com respectivas evidências de formalização no âmbito {do/da} {natureza jurídica e órgão auditado};
      - 2.2.4. se o plano é divulgado, anexar evidências dessa divulgação;
      - 2.2.5. se o plano é acompanhado, anexar evidências do acompanhamento, incluindo a última avaliação realizada.
    - 2.3. evidências que comprovem a resposta ao item 2.3 do questionário.
  3. Com relação à organização e aos relacionamentos da TI (PO4 – Definir processos, organização e relacionamentos de TI):
    - 3.1. evidências que comprovem a resposta ao item 1.1 do questionário;
    - 3.2. caso exista comitê de TI, suas evidências de deliberações ;
    - 3.3. evidências que comprovem a resposta ao item 2.4 do questionário;
    - 3.4. planilha contendo a quantidade de funcionários da área de TI da Unidade, agrupados por perfil profissional;
    - 3.5. caso exista um documento formal que expresse a definição de papéis e responsabilidades dos profissionais de TI {do/da} {natureza jurídica e órgão auditado}:
      - 3.5.1. cópia do documento com evidência de formalização, no âmbito {do/da} {natureza jurídica e órgão auditado};
      - 3.5.2. apresentar definição de responsabilidades e de atribuições do Coordenador-Geral de gestão de tecnologia da informação, das unidades e dos cargos componentes da CGTI;
    - 3.6. relação de papéis sensíveis da área de TI {do/da} {natureza jurídica e órgão auditado}, indicando se são exercidos por servidores públicos {do/da} {natureza jurídica e órgão auditado}, nomeados a cargos em comissão ou funcionários de empresas prestadoras de serviços, ou ainda se estão vagos. Consideram-se papéis sensíveis as atividades de gestão (planejamento, coordenação, controle e supervisão), conforme previsto no § 7º, do art. 10, do Decreto-Lei 200/1967, e as atividades executivas

consideradas críticas no âmbito de cada ente (e.g., segurança da informação, administração de banco de dados, levantamento de requisitos). As atividades executivas consideradas críticas podem variar de um ente para outro;

3.7. informar se a estrutura de recursos humanos do setor de informática (quantitativo e qualificação dos servidores) é suficiente para o desempenho das atribuições da área e para o atendimento das necessidades do órgão, anexando os estudos que embasem essa informação.

4. Com relação ao processo orçamentário relativo ao setor de TI (PO5 – Gerenciar investimentos de TI):

4.1. evidências que comprovem a resposta ao item 7.15 do questionário;

4.2. caso existam planos estratégicos ou táticos de TI, o Plano de Gastos para 2010 e a vinculação entre os gastos e as ações previstas no(s) plano(s);

4.3. planilha que controle periodicamente a execução dos gastos da área de TI do ano corrente, em função da disponibilidade orçamentária.

5. Com relação ao processo de desenvolvimento de software que apoie a administração da qualidade dos produtos de software (PO8 – Gerenciar a qualidade):

5.1. evidências que comprovem a resposta ao item 7.3 do questionário;

5.2. caso exista um processo de software estabelecido:

5.2.1. descrição dos papéis dos profissionais envolvidos;

5.2.2. lista das atividades previstas no processo;

5.2.3. para um projeto em execução ou finalizado, anexar:

5.2.3.1. documento de requisitos, composto minimamente de uma lista de requisitos e de especificações de casos de uso;

5.2.3.2. registro de aceite dos requisitos;

5.2.3.3. registro de histórico das mudanças nos requisitos;

5.2.3.4. cronograma do projeto, evidenciando o seu acompanhamento.

6. Com relação ao processo de gerenciamento de projetos (PO10 – Gerenciar projetos):

6.1. evidências que comprovem a resposta ao item 7.4 do questionário;

6.2. caso exista um processo de gerenciamento de projetos de TI estabelecido:

6.2.1. descrição dos papéis dos profissionais envolvidos;

6.2.2. lista das atividades previstas no processo;

6.2.3. para um projeto em execução ou finalizado, anexar:

6.2.3.1. definição do escopo;

6.2.3.2. cronograma;

6.2.3.3. orçamento;

6.2.3.4. lista de riscos (com seus respectivos tratamentos previstos);

6.2.3.5. fases do ciclo de vida do projeto;

6.2.3.6. plano para execução do projeto homologado por todos os envolvidos.

7. Com relação ao processo de gestão de serviços de TI (DS1 – Definir e gerenciar níveis de serviços, DS3 – Gerenciar capacidade e desempenho, DS4 – Assegurar a continuidade dos serviços, DS8 – Gerenciar a central de serviço e os incidentes, DS9 – Gerenciar a configuração, DS 10 – Gerenciar os problemas, DS13 – Gerenciar as operações e AI 6 – Gerenciar mudanças):

7.1. evidências que comprovem a resposta ao item 7.6 do questionário;

7.2. caso exista um processo de gestão de mudanças de TI estabelecido:

7.2.1. descrição dos papéis dos profissionais envolvidos;

7.2.2. lista das atividades previstas no processo;

7.2.3. lista de mudanças que contenha:

7.2.3.1. classificação das mudanças (exemplo de classificação: mudanças de infraestrutura, software);

7.2.3.2. priorização das mudanças;

7.2.3.3. avaliação do impacto das mudanças;

7.3. caso exista um processo de gestão de incidentes de TI estabelecido:

- 7.3.1. descrição dos papéis dos profissionais envolvidos;
- 7.3.2. lista das atividades previstas no processo;
- 7.3.3. lista de incidentes ocorridos em 2010 que contenha:
- 7.3.3.1. incidentes classificados por escala de gravidade (exemplo de classificação: urgente, grave, significante etc) e estado (aberto, resolvido etc);
- 7.3.3.2. datas de abertura e fechamento do incidente;
- 7.3.3.3. histórico de ações executadas em virtude do incidente;
- 7.4. caso exista um processo de gestão de configuração de TI estabelecido:
- 7.4.1. descrição dos papéis dos profissionais envolvidos;
- 7.4.2. lista das atividades previstas no processo;
- 7.4.3. artefatos previstos:
- 7.4.3.1. base de dados de gestão da configuração do ambiente computacional (CMDB);
- 7.4.3.2. ferramenta de gestão de configuração implantada de modo a garantir que as informações dos itens de configuração possam ser acessadas no repositório.
8. Com relação ao processo de gestão da segurança da informação (DS5 – Garantir a segurança dos sistemas):
- 8.1. evidências que comprovem a resposta ao item 7.2 do questionário;
- 8.2. caso exista um gestor de Segurança da Informação e Comunicações, designado formalmente, evidências de sua atuação;
- 8.3. caso exista um comitê de segurança da informação e comunicações instituído formalmente, evidências de sua deliberação;
- 8.4. evidências que comprovem a resposta ao item 7.1 do questionário;
- 8.5. caso os ativos de informação sejam inventariados (primeira opção do item 7.1 do questionário):
- 8.5.1. amostra mais recente do inventário dos ativos de informação da Unidade;
- 8.6. caso as informações para o negócio sejam classificadas (segunda opção do item 7.1 do questionário):
- 8.6.1. formalização (aprovação e publicação) de documento corporativo classificando as classes de informação utilizadas pelo Unidade (ex.: restrita, sigilosa etc);
- 8.7. caso exista um processo de gestão de riscos de segurança da informação e comunicações em vigor (terceira opção do item 7.1 do questionário):
- 8.7.1. descrição dos papéis dos profissionais envolvidos (exemplos de papéis: Alta Administração, gestores de Segurança da Informação e Comunicações);
- 8.7.2. lista das atividades previstas no processo;
- 8.7.3. artefatos previstos:
- 8.7.3.1. plano de análise e avaliação de riscos, que contenha:
- 8.7.3.1.1. lista de riscos;
- 8.7.3.1.2. avaliação dos riscos identificados por meio da probabilidade e impacto associado;
- 8.7.3.1.3. relação dos riscos que requeiram tratamento, em ordem de priorização;
- 8.7.3.2. plano de tratamento de riscos, que contenha:
- 8.7.3.2.1. formas de tratamento de riscos (aceitação, mitigação, transferência ou eliminação);
- 8.7.3.2.2. ações a serem tomadas para o tratamento dos riscos.
- 8.8. caso exista uma equipe de tratamento e resposta a incidentes em redes computacionais (Etri), apresentar evidências de sua atuação.
9. Com relação ao processo de capacitação dos profissionais de TI (PO7.2-Competências Pessoais e PO7.4-Treinamento do Pessoal):
- 9.1. evidências que comprovem a resposta ao item 1.3 do questionário;
- 9.2. evidências que comprovem a resposta ao item 6.3 do questionário;
- 9.3. evidências que comprovem a resposta ao item 6.4 do questionário;
- 9.4. plano anual de capacitação de profissionais de TI para o ano de 2010, caso exista.

10. Com relação ao processo de monitoração do desempenho na gestão e uso da TI (ME1 – Monitorar e avaliar o desempenho de TI, ME2 – Monitorar e avaliar os controles internos):
  - 10.1. evidências que comprovem a resposta ao item 1.2 do questionário;
  - 10.2. evidências que comprovem a resposta ao item 1.4 do questionário.
11. Com relação ao processo de contratação de bens e serviços de TI:
  - 11.1. evidências que comprovem a resposta ao item 7.10 do questionário.
  - 11.2. informar se há controles {no/na} {natureza jurídica e órgão auditado} que promovam o cumprimento da IN 4/2008-SLTI, apresentando evidências de que esse controle é utilizado e é monitorado (para o Poder Judiciário substituir por “Informar se há controles {no/na} {natureza jurídica e órgão auditado} que promovam que os termos de referência ou projetos básicos para contratações de TI sejam elaborados a partir de estudos técnicos preliminares e que promovam o cumprimento da IN 4/2008-SLTI, apresentando evidências de que esse controle é utilizado e monitorado”).
12. Com relação ao processo de gestão de contratos de TI:
  - 12.1. Evidências que comprovem a resposta ao item 7.11 do questionário.
  - 12.2. Informar se, no processo de fiscalização da execução dos contratos de TI, há algum tipo de controle (p.ex., utilização de alguma lista de verificação), que permita identificar se todas as obrigações do contratado foram cumpridas (p.e., produtos foram entregues, obrigações previdenciárias e trabalhistas, manutenção das condições de habilitação e pontuação, quando for o caso), apresentando evidências de que esse controle é utilizado e é monitorado.

## Anexo II

1. Apresentar planilha contendo relação de contratos de bens e serviços de TI {do/da} {natureza jurídica e órgão auditado}, com fim de vigência (do último aditivo, se for o caso) posterior a 1º/1/2010, inclusive os que estão em vigor, com as seguintes informações:
  - a) identificador do contrato;
  - b) CNPJ da contratada;
  - c) razão social da contratada;
  - d) objeto da contratação;
  - e) identificador do edital de licitação;
  - f) modalidade e tipo de licitação;
  - g) data da celebração do contrato;
  - h) valor total do contrato (incluindo aditivos);
  - i) elemento e subelemento de despesa onde ocorre a liquidação;
  - j) número de aditivos;
  - k) fim do período de vigência (incluindo aditivos).

Situação dos processos consolidados

Item	TC	Tipo de fiscalização	Unidade Técnica	Jurisdicionado	Acórdão
1	000.390/2010-0	Levantamento	Sefti	321 órgãos e entidades	2.308/2010-TCU-Plenário
2	009.982/2010-8	Conformidade (ACGTI)	Sefti	Dnit	866/2011-TCU-Plenário
3	013.718/2010-0	Conformidade (ACGTI)	Sefti	SE/MS	757/2011-TCU- Plenário
4	013.674/2010-2	Conformidade (ACGTI)	Secex/RR	Ibama	111/2011-TCU-Plenário e 432/2011 – TCU – Plenário
5	014.088/2010-0	Conformidade (ACGTI)	Secex/9	Susep	2.746/2010-TCU-Plenário
6	013.671/2010-3	Conformidade (ACGTI)	Secex/SP	TRT-2ª Região (SP)	2.938/2010-TCU-Plenário
7	013.761/2010-2	Conformidade (ACGTI)	Secex/RR	SE/MCT	380/2011-TCU-Plenário
8	017.791/2010-3	Conformidade (ACGTI)	Secex/1	Anatel	465/2011-TCU- Plenário
9	019.052/2010-3	Conformidade (ACGTI)	Secex/CE	Dnocs	592/2011-TCU-Plenário
10	018.044/2010-7	Conformidade (ACGTI)	Secex/RJ	Finep	7.312/2010-TCU – 2ª Câmara
11	018.911/2010-2	Conformidade (ACGTI)	Secex/5	SE/MRE	758/2011-TCU-Plenário
12	017.903/2010-6	Conformidade (ACGTI)	Secex/RS	TRT-4ª Região (RS)	381/2011-TCU-Plenário
13	022.488/2010-3	Conformidade (ACGTI)	Secex/6	FNDE	594/2011-TCU-Plenário
14	024.193/2010-0	Conformidade (ACGTI)	Secex/AM	ADE	2.612/2011-TCU-Plenário
15	024.956/2010-4	Conformidade (ACGTI)	Sefti	SE/MP	2.613/2011-TCU-Plenário
16	010.474/2010-2	Conformidade (AE)	Sefti	Dnit	2.831/2011-TCU-Plenário
17	022.241/2010-8	Conformidade (AE)	Sefti	SRF/MF e SE/MP	Aguardando comentário do gestor (Sefti)
18	029.074/2010-0	Conformidade (AE)	Sefti	SE/MS e SAS/MS	No gabinete do relator
19	029.120/2010-1	Conformidade (AE)	Sefti	CGTI/MCT	No gabinete do relator
20	028.772/2010-5	Monitoramento	Sefti	onze órgãos e entidades	1.145/2011-TCU-Plenário

Memória de cálculo do volume dos recursos fiscalizados (VRF)

Item	TC	Jurisdicionado	VRF (R\$)
1	000.390/2010-0	321 órgãos e entidades	Não se aplica
2	009.982/2010-8	Dnit	85.721.272,30
3	013.718/2010-0	SE/MS	55.806.530,96

210

4	013.674/2010-2	Ibama	5.916.981,77
5	014.088/2010-0	Susep	8.463.096,88
6	013.671/2010-3	TRT-2ª Região (SP)	563.808,00
7	013.761/2010-2	SE/MCT	10.466.020,00
8	017.791/2010-3	Anatel	7.965.065,65
9	019.052/2010-3	Dnocs	-
10	018.044/2010-7	Finep	95.010.568,74
11	018.911/2010-2	SE/MRE	0,00
12	017.903/2010-6	TRT-4ª Região (RS)	10.188.480,00
13	022.488/2010-3	FNDE	5.495.492,88
14	024.193/2010-0	ADE	8.211.846,75
15	024.956/2010-4	SE/MP	695.317.550,73
16	010.474/2010-2	Dnit	43.804.323.279,26
17	022.241/2010-8	SRF/MF e SE/MP	2.842.224.443,49
18	029.074/2010-0	SE/MS e SAS/MS	Não se aplica
19	029.120/2010-1	CGTI/MCT	3.292.152,00
20	028.772/2010-5	onze órgãos e entidades	Não se aplica
		Total	47.638.966.589,42

Obs.: Os valores referem-se aos valores dos contratos analisados, a menos do TC 010.474/2010-2, cujo VRF corresponde à soma dos valores dos contratos de obras do Dnit cadastrados no Sistema de Acompanhamento de Contratos – Siac, objeto daquela auditoria.

Questões de auditoria e possíveis achados

		Possíveis achados	Dmit	SEMS	SE/MCT	Susep	TRT-SP	SE/MRE	SE/MI	TRT-RS	Anatel	Finemp	SEMP	ADBE	FNDE
1	O Unidade executa o processo de planejamento estratégico institucional de acordo com as boas práticas?	Inexistência do Plano Estratégico Institucional Fallhas no Plano Estratégico Institucional Fallhas no Processo de Planejamento Estratégico Institucional													
2	O Unidade executa o processo de planejamento estratégico de TI de acordo com as boas práticas?	Inexistência do PDTI Fallhas no PDTI Fallhas no Processo de Planejamento de TI												X(1)	X(1)
3	A organização de TI do Unidade é adequada às atividades a que ela deve dar suporte?	Inexistência de comitê de TI Fallhas relativas ao comitê de TI Inexistência de definição formal de papéis e responsabilidades Papéis sensíveis sem responsável Papel sensível exercido por não servidor Inexistência de avaliação do quadro de pessoal de TI Fallhas na avaliação do quadro de pessoal de TI Inadequação do quadro de pessoal de TI													X
4	O Unidade executa o processo orçamentário de TI segundo a legislação e as boas práticas?	Inexistência de orçamento de TI na LOA Fallhas no orçamento de TI constante da LOA Inexistência de controle da execução do orçamento de TI Fallhas no controle da execução do orçamento de TI													X
5	Há processo de software estabelecido no Unidade?	Inexistência de processo de software Fallhas no processo de software													(3)
6	Há processo de gerenciamento de projetos de TI estabelecido no Unidade?	Inexistência de processo de gerenciamento de projetos Fallhas no processo de gerenciamento de projetos													(3)
7	Há processos de gestão de serviços de TI que apoiam o Unidade na administração da qualidade dos serviços de TI?	Inexistência do processo de gestão de incidentes Fallhas no processo de gestão de incidentes Inexistência do processo de configuração Fallhas no processo de configuração Inexistência do processo de gestão de mudanças Fallhas no processo de gestão de mudanças												X	
8	O Unidade executa os processos corporativos de	Inexistência de Gestor de Segurança da Informação e Comunicações Inexistência de comitê de segurança da informação e comunicações													

Questões		Possíveis achados									
segurança da informação segundo a legislação e as boas práticas?		Falhas no comitê de segurança da informação e comunicações									
		Inexistência de política de segurança da informação e comunicações (Posic)	X								
		Falhas na política de segurança da informação e comunicações (Posic).									
		Inexistência de equipe de tratamento e resposta a incidentes em redes computacionais (Etri).									
		Falhas na equipe de tratamento e resposta a incidentes em redes computacionais (Etri).									
		Inexistência de classificação da informação									
		Inexistência de inventário dos ativos de informação									
		Falhas no inventário dos ativos de informação									
		Inexistência de processo de gestão de riscos de segurança da informação (GRSIC)									
		Falhas no processo de gestão de riscos de segurança da informação (GRSIC).									
		Inexistência de plano anual de capacitação									
9	Há plano de capacitação de profissionais de TI que auxile no desenvolvimento das competências necessárias para a boa execução dos trabalhos?										
O Unidade realiza 10 monitoração do desempenho da gestão e uso da TI?		Plano anual de capacitação não contempla a área de gestão de TI									
		Inexistência de avaliação da gestão de TI									
		Falhas na avaliação da gestão de TI									
		Auditória interna não apoia a avaliação da TI									
		Inexistência de controles que promovam o cumprimento da IN4									
		Falhas nos controles que promovam o cumprimento da IN4									
		Inexistência de controles que promovam que o Termo de Referência ou Projeto Básico seja elaborado a partir de estudos técnicos preliminares									
		Descumprimento do processo de planejamento de acordo com a IN4									
11	O Unidade realiza o processo de contratação de bens e serviços de TI segundo as normas vigentes?	Falhas no cumprimento do processo de planejamento de acordo com a IN4									
		Inexistência dos estudos técnicos preliminares									
		Falhas nos estudos técnicos preliminares									
		Irregularidades na contratação									
12	O Unidade realiza o processo	Inexistência de controles que promovam a regular gestão contratual									

Questões	Possíveis achados	Dnit	SE/MCT	SE/MS	SUSEP	SEBAMA	SE/MEP	SE/MP	Antatel	TRT-RS	SEMRSE	Dnocs	TRT-SP	Susep	SE/MEP	SE/MP	Antatel	TRT-RS	SEMRSE	Dnocs	TRT-SP	Susep	SE/MEP	SE/MP	Fnde	TCU
de gestão de contratos de bens e serviços de TI segundo as normas vigentes?	Falhas nos controles que promovam a regular gestão contratual																									
Não decorrente das questões de auditoria	Irregularidades na gestão contratual																									
	TI descentralizada e sem coordenação																									
	Não classificação de informações conforme níveis de segurança																									

- (1) Consta do relatório original com o título: Falhas no Plano Diretor de TI (PDTI)
- (2) Consta do relatório original com o título: Inexistência de Plano Diretor de Tecnologia da Informação
- (3) Controles formalizados ao final da fase de execução da auditoria e não avaliados pela equipe Licitações em 2009

A Figura 4 ilustra o mapa mental utilizado para gerar o Quadro 16 e o gráfico ilustrado na Error! Reference source not found.Erro! Fonte de referência não encontrada., as partir dos dados obtidos das respostas à questão 7.9 do questionário Perfil GovTI2009.

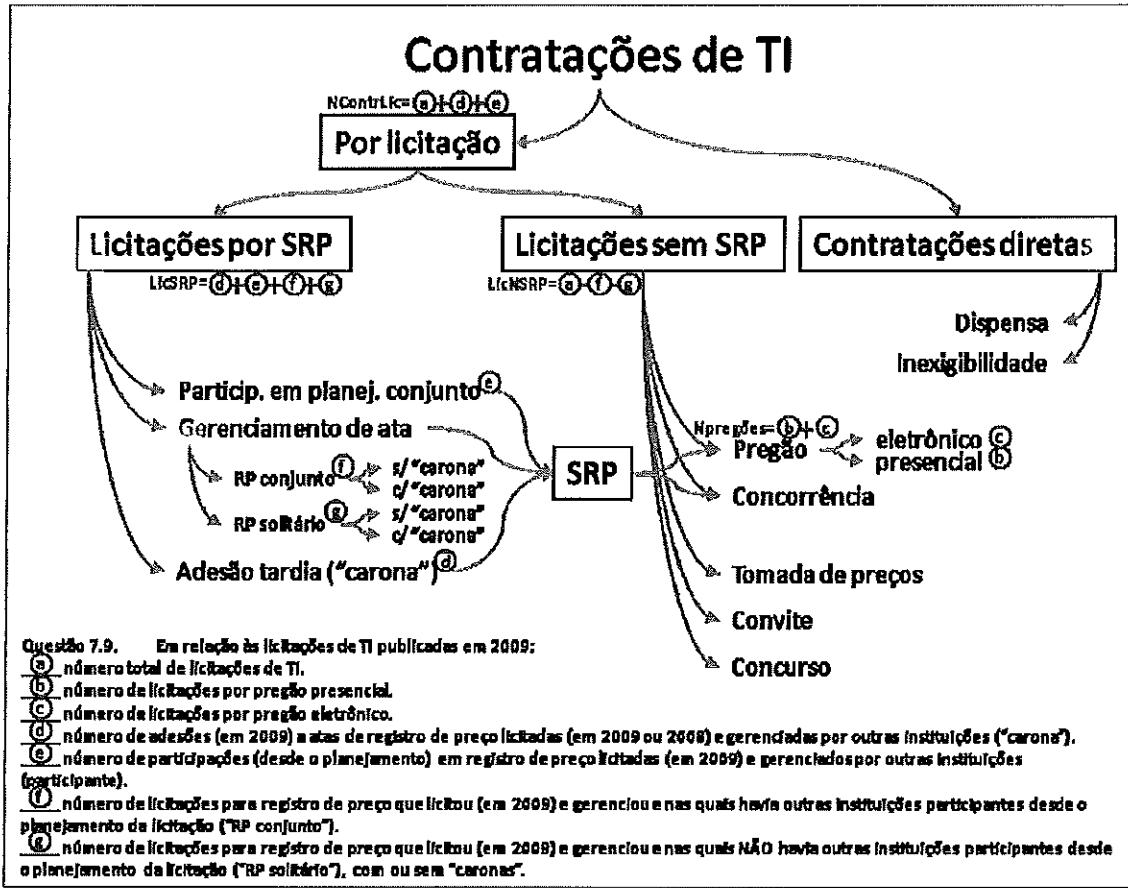


Figura 4 – Mapa mental para análise das licitações de 2009

Quadro 16 – Número de licitações em 2009

Ente nº	a	b	c	d	e	f	e+f	g	NLicProp	NContrLic	LicSRP	LicNSRP	NPregões
250	56	0	18	9	0	1	1	5	56	65	15	50	18
222	13	0	9	3	0	2	2	2	13	16	7	9	9
310	45	11	32	11	0	1	1	23	45	56	35	21	43
78	8	2	6	1	0	0	0	6	8	9	7	2	8
192	4	0	4	1	0	0	0	1	4	5	2	3	4
70	5	5	0	2	0	0	0	2	5	7	4	3	5
81	0	0	0	0	0	0	0	0	0	0	0	0	0
175	33	0	15	9	0	0	0	0	33	42	9	33	15
28	10	0	10	2	0	0	0	0	10	12	2	10	10
130	33	0	33	2	0	0	0	0	33	35	2	33	33
2	2	0	2	0	0	0	0	0	2	2	0	2	2
226	0	0	0	0	0	0	0	0	0	0	0	0	0
36	0	0	0	0	0	0	0	0	0	0	0	0	0
54	21	0	15	1	0	0	0	4	21	22	5	17	15
347	7	0	4	3	0	0	0	0	7	10	3	7	4
113	4	0	4	0	0	0	0	0	4	4	0	4	4
341	9	0	4	5	0	0	0	0	9	14	5	9	4



57	19	0	19	5	0	0	0	0	19	24	5	19	19
22	0	0	0	8	0	0	0	0	0	8	8	0	0
99	10	0	5	5	0	0	0	0	10	15	5	10	5
178	8	0	8	0	0	0	0	0	8	8	0	8	8
150	0	0	0	0	0	0	0	0	0	0	0	0	0
45	24	0	19	2	0	0	0	4	24	26	6	20	19
227	1	0	0	1	0	0	0	0	1	2	1	1	0
163	9	0	9	4	0	0	0	0	9	13	4	9	9
16	15	0	10	2	0	0	0	3	15	17	5	12	10
53	16	0	11	5	0	0	0	0	16	21	5	16	11
298	5	2	2	1	0	0	0	2	5	6	3	3	4
248	14	0	0	0	0	0	0	0	14	14	0	14	0
85	4	4	0	0	0	15	15	4	4	4	19	-15	4
268	7	0	7	7	0	0	0	5	7	14	12	2	7
319	0	0	3	1	0	0	0	0	0	1	1	0	3
102	1	0	1	17	0	0	0	0	1	18	17	1	1
91	11	0	6	3	0	0	0	0	11	14	3	11	6
11	5	0	1	4	0	0	0	0	5	9	4	5	1
96	0	0	1	0	0	0	0	0	0	0	0	0	1
330	3	0	3	1	0	0	0	0	3	4	1	3	3
138	48	0	48	0	0	0	0	0	48	48	0	48	48
13	8	0	8	3	0	0	0	8	8	11	11	0	8
197	11	0	9	2	0	0	0	0	11	13	2	11	9
23	5	0	5	3	0	0	0	1	5	8	4	4	5
41	93	3	73	0	0	0	0	17	93	93	17	76	76
105	7	0	7	5	0	0	0	0	7	12	5	7	7
6	1	1	0	0	0	0	0	0	1	1	0	1	1
174	7	0	7	1	0	0	0	7	7	8	8	0	7
223	0	0	0	2	0	0	0	0	0	2	2	0	0
50	24	0	21	4	0	0	0	3	24	28	7	21	21
48	145	0	145	0	0	0	0	8	145	145	8	137	145
231	23	23	0	0	0	0	0	0	23	23	0	23	23
282	12	0	12	11	1	0	1	4	12	24	16	8	12
32	13	0	13	0	0	0	0	0	13	13	0	13	13
287	26	0	26	0	0	0	0	16	26	26	16	10	26
296	38	0	11	9	0	0	0	9	38	47	18	29	11
263	14	0	14	4	0	0	0	7	14	18	11	7	14
86	26	0	25	0	0	0	0	1	26	26	1	25	25
108	39	0	39	6	0	0	0	21	39	45	27	18	39
115	0	0	0	0	0	0	0	0	0	0	0	0	0
339	0	0	0	18	0	0	0	0	0	18	18	0	0
14	0	0	0	0	0	0	0	0	0	0	0	0	0
322	5	0	5	0	0	0	0	1	5	5	1	4	5
137	0	0	0	4	0	0	0	0	0	4	4	0	0



312	17	0	17	2	0	0	0	17	17	19	19	0	17
273	21	0	11	10	0	0	0	8	21	31	18	13	11
38	280	0	0	0	0	0	0	0	280	280	0	280	0
274	7	0	7	8	0	1	1	6	7	15	15	0	7
243	0	0	0	12	0	0	0	0	0	12	12	0	0
166	1	0	1	0	0	0	0	0	1	1	0	1	1
84	40	5	15	0	0	0	0	0	40	40	0	40	20
149	19	0	19	0	0	0	0	0	19	19	0	19	19
281	6	0	6	8	0	0	0	1	6	14	9	5	6
131	0	0	1	5	0	0	0	0	0	5	5	0	1
277	10	0	10	4	0	0	0	15	10	14	19	-5	10
269	41	0	20	4	0	0	0	4	41	45	8	37	20
55	2	0	2	0	0	0	0	0	2	2	0	2	2
35	2	0	0	0	0	0	0	0	2	2	0	2	0
51	0	1	0	2	0	0	0	0	0	2	2	0	1
293	8	0	8	1	1	0	1	5	8	10	7	3	8
88	133	0	127	50	0	0	0	0	133	183	50	133	127
220	4	0	0	7	0	0	0	0	4	11	7	4	0
284	11	0	11	0	1	0	1	0	11	12	1	11	11
40	30	1	29	0	0	0	0	0	30	30	0	30	30
257	1	0	1	8	0	0	0	0	1	9	8	1	1
343	32	0	32	0	0	0	0	13	32	32	13	19	32
271	19	0	4	12	0	0	0	3	19	31	15	16	4
4	3	1	2	0	0	0	0	0	3	3	0	3	3
10	5	0	5	0	0	0	0	0	5	5	0	5	5
247	38	0	38	5	0	0	0	5	38	43	10	33	38
217	6	0	0	0	0	0	0	0	6	6	0	6	0
346	18	0	18	5	1	0	1	14	18	24	20	4	18
320	6	0	5	0	0	0	0	1	6	6	1	5	5
224	0	0	0	0	0	0	0	0	0	0	0	0	0
69	6	0	6	4	0	0	0	3	6	10	7	3	6
26	12	8	0	2	0	0	0	2	12	14	4	10	8
306	18	0	18	8	0	0	0	10	18	26	18	8	18
350	14	0	14	0	0	0	0	0	14	14	0	14	14
286	24	0	24	4	1	0	1	8	24	29	13	16	24
345	28	0	28	11	0	0	0	0	28	39	11	28	28
112	6	0	3	3	0	0	0	0	6	9	3	6	3
103	15	0	8	3	3	0	3	1	15	21	7	14	8
61	4	0	4	2	0	0	0	1	4	6	3	3	4
67	5	0	5	3	0	0	0	0	5	8	3	5	5
5	12	1	3	8	0	0	0	0	12	20	8	12	4
267	5	0	5	3	2	0	2	3	5	10	8	2	5
122	60	0	33	3	20	0	20	0	60	83	23	60	33
93	7	1	6	1	0	0	0	1	7	8	2	6	7

259	17	0	4	6	3	0	3	4	17	26	13	13	4
266	10	0	10	10	0	0	0	6	10	20	16	4	10
77	59	0	59	8	0	0	0	5	59	67	13	54	59
52	14	2	12	1	0	0	0	0	14	15	1	14	14
18	3	0	3	0	0	0	0	0	3	3	0	3	3
34	12	2	6	1	1	0	1	2	12	14	4	10	8
276	46	0	8	8	0	0	0	0	46	54	8	46	8
280	10	0	10	0	1	0	1	10	10	11	11	0	10
255	53	33	2	5	0	0	0	13	53	58	18	40	35
300	14	0	14	18	1	0	1	4	14	33	23	10	14
265	14	0	14	6	0	0	0	1	14	20	7	13	14
39	18	0	18	4	0	0	0	2	18	22	6	16	18
8	0	0	2	0	1	0	1	0	0	1	1	0	2
304	18	0	18	3	0	0	0	18	18	21	21	0	18
289	5	0	2	2	0	1	1	2	5	7	5	2	2
333	19	0	19	21	0	0	0	0	19	40	21	19	19
292	3	0	1	12	0	0	0	3	3	15	15	0	1
66	31	0	18	11	0	2	2	0	31	42	13	29	18
260	5	0	5	9	1	0	1	0	5	15	10	5	5
294	8	2	6	3	0	0	0	2	8	11	5	6	8
29	7	0	4	1	0	0	0	0	7	8	1	7	4
308	11	3	8	13	0	0	0	7	11	24	20	4	11
326	29	0	25	0	0	0	0	0	29	29	0	29	25
165	19	0	5	14	0	0	0	5	19	33	19	14	5
120	33	0	33	14	0	0	0	12	33	47	26	21	33
27	7	0	7	4	0	0	0	0	7	11	4	7	7
17	13	0	1	12	0	0	0	0	13	25	12	13	1
104	1	0	1	4	0	0	0	0	1	5	4	1	1
142	9	0	9	0	0	0	0	0	9	9	0	9	9
161	6	0	5	1	0	0	0	0	6	7	1	6	5
275	15	0	15	3	4	0	4	7	15	22	14	8	15
152	0	0	0	0	7	0	7	0	0	7	7	0	0
94	5	0	5	0	0	0	0	0	5	5	0	5	5
30	4	0	4	5	0	0	0	0	4	9	5	4	4
173	0	0	1	1	0	0	0	0	0	1	1	0	1
299	11	0	11	0	0	0	0	4	11	11	4	7	11
147	3	0	3	4	0	0	0	0	3	7	4	3	3
225	0	0	2	8	0	0	0	0	0	8	8	0	2
253	17	0	16	4	0	0	0	8	17	21	12	9	16
158	3	0	1	2	0	0	0	0	3	5	2	3	1
349	12	12	0	0	0	0	0	0	12	12	0	12	12
87	19	19	0	0	0	0	0	18	19	19	18	1	19
100	25	0	9	6	0	0	0	0	25	31	6	25	9
128	11	0	11	0	0	0	0	0	11	11	0	11	11



46	31	0	28	1	0	0	0	0	31	32	1	31	28
303	13	6	7	3	0	0	0	6	13	16	9	7	13
302	7	7	0	9	1	0	1	2	7	17	12	5	7
24	20	0	20	8	0	0	0	6	20	28	14	14	20
290	7	0	7	6	0	0	0	3	7	13	9	4	7
301	6	0	6	4	0	0	0	0	6	10	4	6	6
264	13	8	5	8	0	0	0	7	13	21	15	6	13
305	17	0	17	8	0	0	0	0	17	25	8	17	17
272	6	0	6	4	2	0	2	2	6	12	8	4	6
251	12	1	9	6	0	0	0	4	12	18	10	8	10
7	6	0	6	0	0	0	0	0	6	6	0	6	6
211	3	0	3	0	0	0	0	0	3	3	0	3	3
258	10	0	10	7	0	0	0	2	10	17	9	8	10
262	6	1	5	12	0	0	0	5	6	18	17	1	6
82	0	0	0	0	0	0	0	0	0	0	0	0	0
279	4	4	0	3	0	0	0	0	4	7	3	4	4
297	4	0	4	4	1	0	1	3	4	9	8	1	4
295	24	2	22	2	0	0	0	11	24	26	13	13	24
121	24	0	9	8	1	0	1	6	24	33	15	18	9
109	9	0	4	5	0	0	0	0	9	14	5	9	4
307	17	0	17	6	0	0	0	2	17	23	8	15	17
335	13	0	10	3	0	0	0	10	13	16	13	3	10
288	6	0	6	2	0	0	0	3	6	8	5	3	6
133	9	0	9	9	0	0	0	9	9	18	18	0	9
98	1	0	1	3	0	0	0	0	1	4	3	1	1
181	7	0	7	5	0	0	0	0	7	12	5	7	7
261	13	6	7	0	0	2	2	5	13	13	7	6	13
182	4	0	4	10	0	1	1	0	4	14	11	3	4
193	1	0	7	3	1	0	1	0	1	5	4	1	7
160	12	0	10	1	0	0	0	1	12	13	2	11	10
210	5	0	5	44	0	0	0	0	5	49	44	5	5
169	3	0	3	9	0	0	0	0	3	12	9	3	3
325	47	0	47	1	0	0	0	5	47	48	6	42	47
207	12	0	7	5	0	0	0	0	12	17	5	12	7
191	3	0	3	3	0	0	0	0	3	6	3	3	3
183	0	0	1	8	1	0	1	0	0	9	9	0	1
208	36	0	0	3	0	0	0	26	36	39	29	10	0
201	9	0	9	3	0	0	0	6	9	12	9	3	9
187	28	0	28	55	0	21	21	0	28	83	76	7	28
199	2	2	0	0	0	0	0	0	2	2	0	2	2
204	9	0	9	0	0	0	0	0	9	9	0	9	9
195	1	0	0	5	0	0	0	1	1	6	6	0	0
278	15	0	15	4	0	0	0	6	15	19	10	9	15
190	0	0	0	0	0	0	0	0	0	0	0	0	0

321	17	0	3	12	1	0	1	0	17	30	13	17	3
337	23	0	23	32	0	0	0	0	23	55	32	23	23
92	71	0	71	1	0	0	0	6	71	72	7	65	71
189	8	0	7	7	1	4	5	1	8	16	13	3	7
200	5	0	5	2	0	0	0	0	5	7	2	5	5
196	9	0	41	6	0	0	0	3	9	15	9	6	41
143	4	0	1	3	0	0	0	1	4	7	4	3	1
316	42	0	42	0	0	0	0	12	42	42	12	30	42
348	0	0	0	0	0	0	0	0	0	0	0	0	0
58	1	0	1	0	0	0	0	1	1	1	1	0	1
95	4	0	4	4	0	0	0	0	4	8	4	4	4
170	4	0	2	2	0	0	0	0	4	6	2	4	2
221	12	0	0	0	0	0	0	0	12	12	0	12	0
116	117	0	117	4	0	0	0	9	117	121	13	108	117
198	10	0	7	3	0	0	0	0	10	13	3	10	7
202	0	0	0	1	0	0	0	0	0	1	1	0	0
203	15	0	5	10	0	0	0	0	15	25	10	15	5
80	3	0	3	0	0	0	0	1	3	3	1	2	3
118	3	0	3	0	0	0	0	0	3	3	0	3	3
331	2	0	2	5	1	2	3	0	2	8	8	0	2
188	64	0	176	477	74	5	79	59	64	615	615	0	176
136	0	0	0	12	1	0	1	0	0	13	13	0	0
332	4	0	4	0	0	0	0	4	4	4	4	0	4
59	2	0	2	4	0	0	0	0	2	6	4	2	2
9	9	0	5	0	0	0	0	0	9	9	0	9	5
270	12	0	12	5	0	0	0	6	12	17	11	6	12
31	22	0	22	1	0	0	0	0	22	23	1	22	22
194	8	0	8	13	0	0	0	2	8	21	15	6	8
328	3	0	3	10	1	0	1	0	3	14	11	3	3
164	0	0	0	1	0	0	0	0	0	1	1	0	0
72	10	0	10	11	0	0	0	2	10	21	13	8	10
49	40	0	40	3	0	0	0	3	40	43	6	37	40
184	1	0	0	15	1	0	1	0	1	17	16	1	0
71	3	0	2	3	0	0	0	0	3	6	3	3	2
324	17	0	13	4	0	0	0	0	17	21	4	17	13
246	12	0	12	3	0	0	0	1	12	15	4	11	12
309	41	0	41	6	0	0	0	28	41	47	34	13	41
123	0	0	0	0	0	0	0	0	0	0	0	0	0
117	135	0	15	0	0	0	0	120	135	135	120	15	15
63	2	0	2	0	0	0	0	1	2	2	1	1	2
79	1	0	1	1	0	0	0	0	1	2	1	1	1
129	22	0	21	1	0	0	0	20	22	23	21	2	21
186	0	0	0	0	0	0	0	0	0	0	0	0	0
206	9	0	9	4	0	0	0	4	9	13	8	5	9



285	19	0	12	4	0	0	0	3	19	23	7	16	12
148	40	0	4	15	0	0	0	5	40	55	20	35	4
83	14	0	12	1	0	0	0	0	14	15	1	14	12
76	11	0	11	1	0	0	0	4	11	12	5	7	11
351	12	0	12	5	3	1	4	0	12	20	9	11	12
153	6	0	6	3	0	0	0	0	6	9	3	6	6
185	10	0	8	0	0	0	0	2	10	10	2	8	8
213	47	4	43	0	0	0	0	0	47	47	0	47	47
256	12	3	9	10	0	0	0	3	12	22	13	9	12
68	13	0	13	6	0	0	0	2	13	19	8	11	13
124	0	0	0	0	0	0	0	0	0	0	0	0	0
25	9	0	3	2	0	0	0	1	9	11	3	8	3
125	5	0	5	0	0	0	0	1	5	5	1	4	5
64	0	0	0	0	0	0	0	0	0	0	0	0	0
134	4	0	4	1	0	0	0	0	4	5	1	4	4
329	20	0	11	5	0	0	0	4	20	25	9	16	11
135	2	0	2	0	0	0	0	2	2	2	2	0	2
205	3	1	2	9	0	0	0	3	3	12	12	0	3
3	5	0	5	3	0	0	0	1	5	8	4	4	5
141	5	1	4	0	0	0	0	0	5	5	0	5	5
168	12	0	2	3	0	0	0	0	12	15	3	12	2
336	0	0	0	0	0	0	0	0	0	0	0	0	0
101	2	2	0	1	0	0	0	0	2	3	1	2	2
209	102	70	31	298	1	0	1	37	102	401	336	65	101
218	190	0	0	0	0	0	0	0	190	190	0	190	0
244	0	0	0	0	0	0	0	0	0	0	0	0	0
344	0	0	0	0	0	0	0	0	0	0	0	0	0
313	1	0	1	0	0	0	0	0	1	1	0	1	1
242	0	0	0	0	0	0	0	0	0	0	0	0	0
233	44	0	43	8	0	0	0	1	44	52	9	43	43
Total	4.372	260	3.033	1.930	140	59	199	902	4.372	6.442	3.031	3.411	3.293

Comparação das respostas declaradas com a opinião dos auditores do TCU

Questão de Auditoria	Critério Auditoria	de Item quest	Fonte	AmE	ANATEL	DNT	DNOCS	FINEP	FINDE	IBAMA	MCT	MP	MRB	MS	SUSEP	TRT-2-SP	TRT-4-RS
A. A instituição executa um processo de planejamento estratégico institucional?	Q21 >= 3	Q21	origem auditoria	5 1↓	3 1↓	3 1↓	4 1↓	2 4	2 1↓	3 1↓	6 1↓	1 1↓	6 1↓	2 2	2 2	5 4	2 2
B. A instituição executa um processo de planejamento estratégico de TI?	Q22 >= 3	Q22	origem auditoria	3 1↓	3 1↓	2 1	2 1	4 3	3 1	1 3	1 1	1 2	4 2	1 1	1 1	2 1	4 1
C. A alta administração designou formalmente um comitê de TI para auxiliá-la nas decisões relativas à gestão e ao uso corporativos de TI?	Q11b = sim	Q11b	origem não auditoria	não não↓	não não↓	não não↓	não não↓	sim sim↓	sim sim↓	não não↓	sim sim↓	sim sim↓	sim sim↓	não não↓	não não↓	não não↓	não não↓
D. A solicitação de orçamento de TI é feita com base na estimativa dos custos das contratações previstas?	Q715 <sup>a</sup> = sim	Q715 <sup>a</sup>	origem sim auditoria	sim sim↓	sim sim↓	sim sim↓	sim sim↓	não não↓	sim sim↓	sim sim↓	sim sim↓	sim sim↓	sim sim↓	não não↓	sim sim↓	sim sim↓	sim sim↓
E. Ao longo do exercício financeiro, há controle dos gastos efetuados especificamente com TI?	Q715c = sim ou Q715d = sim			↓	S	↓	S	↓	S	↓	S	↓	S	↓	S	↓	S
E1. Ao longo do exercício financeiro, há controle dos gastos efetuados especificamente com TI?	Q715c = sim ou Q715d = sim	Q715c	origem sim auditoria	sim não↓	sim sim↓	não não↓	sim sim↓	não não↓	sim sim↓	sim sim↓							
E2. Ao longo do exercício financeiro, há controle dos gastos efetuados especificamente com TI?	Q715c = sim ou Q715d = sim	Q715d	origem sim auditoria	sim não↓	sim sim↓	não não↓	sim sim↓	não não↓	sim sim↓	não não↓	não não↓	não não↓	não não↓	não não↓	não não↓	sim sim↓	sim sim↓
F. Há processo de software?	Q73 >= 3	Q73	origem auditoria	2 1	3 1	1 1	1 1	4 1	1 1	4 1	1 1	2 1	2 1	3 2	3 2	2 1	2 1
G. Há processo de gerenciamento de projetos?	Q74 >= 3	Q74	origem auditoria	2 1	2 1	2 1	2 1	2 1	2 1	3 1	3 1	2 1	2 1	2 1	2 1	1 1	3 2
H. Há processo de gerenciamento de incidentes?	Q76e = sim	Q76e	origem não auditoria	não não↓													
I. Há processo de configuração?	Q76f = sim	Q76f	origem não auditoria	não não↓													
J. Há processo de gestão de mudanças?	Q76 <sup>a</sup> = sim	Q76 <sup>a</sup>	origem não auditoria	não não↓													
K. Há gestor de segurança da informação?	Q72b = sim	Q72b	origem não auditoria	não não↓													
L. Há Posic em vigor?	Q72 <sup>a</sup> = sim	Q72 <sup>a</sup>	origem não sim	não não↓													

Questão de Auditoria	Critério Auditoria	de Item quest	Fonte	ANATEL	DNIT	DNCS	FNEP	TDE	IBAMA	MCT	ME	SUSEP	MS	TRT-2-SP	TRT-4-RS
M. Gerencia os incidentes de segurança (logo há Etri)?	Q71d = sim		auditoria não	não	sim	não	sim	não	não	não	sim	não	não	não	sim
N. Classifica a informação?	Q71b = sim	Q71d	origem	não	sim	não	sim	não	não	não	sim	sim	não	não	não
O. Faz inventário de ativos?	Q71a = sim	Q71b	auditoria não	não	sim	não	sim	não	não	não	sim	sim	não	não	não
P. Faz gestão de riscos de segurança da informação?	Q71c = sim	Q71c	origem	não	não	não	sim	não	não	não	sim	sim	não	não	não
Q. Plano anual de capacitação contempla área de gestão de TI?	Q63>= 3	Q63	origem	3	3	1	3	3	1	2	3	5	1	1	3
R. Auditoria interna apoia avaliação da gestão da TI?															
R1. Auditoria interna apoia avaliação da gestão da TI? (INV)	Q14a = não	Q14a	origem	não	sim	não	sim	não	sim	sim	não	não	sim	sim	não
R2. Auditoria interna apoia avaliação da gestão da TI?	Q14b = sim	Q14b	origem	não	sim	não	sim	não	sim	sim	não	não	sim	sim	sim
R3. Auditoria interna apoia avaliação da gestão da TI?	Q14c = sim	Q14c	origem	não	sim	não	sim	não	sim	sim	não	não	não	não	não
R4. Auditoria interna apoia avaliação da gestão da TI?	Q14d = sim	Q14d	origem	não	sim	não	sim	não	sim	sim	não	não	não	não	não
R5. Auditoria interna apoia avaliação da gestão da TI?	Q14e = sim	Q14e	origem	não	sim	não	sim	não	sim	sim	não	não	não	não	não
R6. Auditoria interna apoia avaliação da gestão da TI?	Q14f = sim	Q14f	origem	não	sim	não	sim	não	sim	sim	não	não	não	não	não
S. Adota processo de trabalho formal na contratação de bens e serviços Q710 >= 3	Q710	origem	1	2	1	1	3	2	1	2	1	2	1	2	1
T. Adota processo de trabalho formal na gestão de contratos de bens e serviços de TI?	Q711	origem	1	3	1	1	1	1	1	1	2	1	1	1	2
U. A alta administração se responsabiliza pelo estabelecimento e pelo cumprimento das políticas de gestão e uso corporativos de TI?	Q11a = sim	Q11a	origem	não	sim	sim	não	não	sim	não	não	sim	sim	sim	sim



## Governança de TI x Orçamento administrado

Segmento	iGovTI2010	Orçamento de TI (2010)	Faixa Maturidade	Orçamento Administrado (2010)
JUD	0,43767086	1019442	2. Maturidade intermediária	R\$ 104.932.807,24
EXE-Sisp	0,32792748	900000	1. Maturidade inicial	R\$ 74.280.527,15
EXE-Sisp	0,25106895	1400000	1. Maturidade inicial	R\$ 88.497.223,32
EXE-Sisp	0,46275498	25000000	2. Maturidade intermediária	R\$ 946.020.297,30
EXE-Dest	0,34732342	3750000	1. Maturidade inicial	R\$ 473.595.389,30
EXE-Dest	0,31245656	13088000	1. Maturidade inicial	R\$ 276.419.098,29
JUD	0,52585267	1301375	2. Maturidade intermediária	R\$ 137.896.229,18
EXE-Sisp	0,35214866	660359	1. Maturidade inicial	R\$ 205.386.305,82
JUD	0,3514098		1. Maturidade inicial	R\$ 129.649.504,27
JUD	0,22435638	637000	1. Maturidade inicial	R\$ 81.635.331,19
EXE-Sisp	0,39487202	16150000	1. Maturidade inicial	R\$ 2.165.880.361,31
EXE-Sisp	0,27460971	2700000	1. Maturidade inicial	R\$ 691.909.350,66
MPU	0,54233841	6704157	2. Maturidade intermediária	R\$ 373.983.798,42
EXE-Sisp	0,31371335	2915811	1. Maturidade inicial	R\$ 335.523.752,86
EXE-Sisp	0,37652401	3111552	1. Maturidade inicial	R\$ 1.944.131.576,01
JUD	0,54188303	1500000	2. Maturidade intermediária	R\$ 272.257.000,27
EXE-Sisp	0,27766126	420000	1. Maturidade inicial	R\$ 81.026.449,48
EXE-Sisp	0,33804707	107334	1. Maturidade inicial	R\$ 23.841.388,62
JUD	0,3627924	8463828	1. Maturidade inicial	R\$ 558.360.933,97
JUD	0,30248761	119000	1. Maturidade inicial	R\$ 31.908.800,43
JUD	0,52765898	4438000	2. Maturidade intermediária	R\$ 424.636.937,29
JUD	0,42528246	1579068	2. Maturidade intermediária	R\$ 113.349.383,45
JUD	0,51862114	995000	2. Maturidade intermediária	R\$ 170.969.292,44
JUD	0,40632383	512607	2. Maturidade intermediária	R\$ 83.220.232,82
JUD	0,52827974	6592306	2. Maturidade intermediária	R\$ 1.219.939.177,06
EXE-Sisp	0,39531837	189109167	1. Maturidade inicial	R\$ 2.362.416.860,31
EXE-Sisp	0,23341532	145000	1. Maturidade inicial	R\$ 9.502.314,71
EXE-Dest	0,43749423	1800000	2. Maturidade intermediária	R\$ 1.403.087.598,16
EXE-Sisp	0,17850836	504000	1. Maturidade inicial	R\$ 68.614.010,25

Segmento	iGovTI2010	Orçamento de TI (2010)	Faixa Maturidade	Orçamento Administrado (2010)
EXE-Sisp	0,30596807	880000	1. Maturidade inicial	R\$ 57.925.338,10
EXE-Sisp	0,3009215	5908582	1. Maturidade inicial	R\$ 883.874.913,88
EXE-Sisp	0,52916738	109956586	2. Maturidade intermediária	R\$ 2.144.043.092,92
JUD	0,33564123	7246116	1. Maturidade inicial	R\$ 668.082.047,88
JUD	0,39191829	399488	1. Maturidade inicial	R\$ 73.411.052,55
EXE-Sisp	0,294325	1336000	1. Maturidade inicial	R\$ 1.134.701.588,15
JUD	0,38524088	679000	1. Maturidade inicial	R\$ 160.747.944,03
JUD	0,44536667	200000	2. Maturidade intermediária	R\$ 169.391.237,33
EXE-Sisp	0,27005766	302000	1. Maturidade inicial	R\$ 27.112.064,21
EXE-Dest	0,35635512	5086301	1. Maturidade inicial	R\$ 74.333.111,60
JUD	0,64137191	1852309	3. Maturidade aprimorada	R\$ 171.905.694,95
EXE-Sisp	0,43614966	42366000	2. Maturidade intermediária	R\$ 438.243.685,01
JUD	0,38183399	8850000	1. Maturidade inicial	R\$ 1.631.332.652,27
EXE-Sisp	0,33649828	4983915	1. Maturidade inicial	R\$ 878.740.826,80
EXE-Sisp	0,34369369	57250000	1. Maturidade inicial	R\$ 1.678.069.561,26
EXE-Sisp	0,45489871	792000	2. Maturidade intermediária	R\$ 409.769.567,18
EXE-Sisp	0,20995653	5254939	1. Maturidade inicial	R\$ 67.044.050,36
EXE-Sisp	0,45763164	1037450	2. Maturidade intermediária	R\$ 19.884.281,19
EXE-Sisp	0,2817045	1410940	1. Maturidade inicial	R\$ 19.143.048,59
EXE-Sisp	0,72419304	3239348	3. Maturidade aprimorada	R\$ 483.392.975,73
JUD	0,3993776	4243273	1. Maturidade inicial	R\$ 343.307.713,39
EXE-Sisp	0,46793287	6378288	2. Maturidade intermediária	R\$ 132.207.468,12
EXE-Sisp	0,32640335	7060500	1. Maturidade inicial	R\$ 55.759.762,57
EXE-Sisp	0,26611441	2153868	1. Maturidade inicial	R\$ 11.492.405,00
JUD	0,53123559	960500	2. Maturidade intermediária	R\$ 167.115.600,05
JUD	0,44449878	750888	2. Maturidade intermediária	R\$ 465.194.894,36
EXE-Sisp	0,50097661	6670890	2. Maturidade intermediária	R\$ 185.748.622,80
EXE-Sisp	0,26892613	24934837	1. Maturidade inicial	R\$ 110.519.951,14
EXE-Sisp	0,37189295	1672879	1. Maturidade inicial	R\$ 276.502.741,55
JUD	0,34156064	723789	1. Maturidade inicial	R\$ 52.361.848,53

Segmento	iGovTI2010	Orçamento de TI (2010)	Faixa Maturidade	Orçamento Administrado (2010)
JUD	0,40250066	3875516	2. Maturidade intermediária	R\$ 439.605.413,36
EXE-Sisp	0,38654778	25512988	1. Maturidade inicial	R\$ 127.259.673,83
JUD	0,43117777	818000	2. Maturidade intermediária	R\$ 125.198.837,07
EXE-Sisp	0,2846893	3586361	1. Maturidade inicial	R\$ 903.134.949,15
JUD	0,37948378	278081	1. Maturidade inicial	R\$ 54.263.823,25
JUD	0,34929592	1200000	1. Maturidade inicial	R\$ 104.022.030,29
EXE-Sisp	0,32746216	8576068	1. Maturidade inicial	R\$ 122.723.815,10
JUD	0,41334132	7803000	2. Maturidade intermediária	R\$ 301.048.509,93
JUD	0,56131375	1678000	2. Maturidade intermediária	R\$ 652.206.725,26
JUD	0,52652216	17358000	2. Maturidade intermediária	R\$ 1.354.277.238,90
EXE-Dest	0,45186178	1816695	2. Maturidade intermediária	R\$ 211.195.903,04
JUD	0,41415811	3500000	2. Maturidade intermediária	R\$ 884.361.729,31
JUD	0,27875219		1. Maturidade inicial	R\$ 119.034.518,86
JUD	0,40254167	898200	2. Maturidade intermediária	R\$ 74.459.969,84
JUD	0,41258288	790553	2. Maturidade intermediária	R\$ 47.234.393,54
JUD	0,42126302	2230084	2. Maturidade intermediária	R\$ 321.495.533,73
EXE-Sisp	0,32798764	500000	1. Maturidade inicial	R\$ 352.905.922,24
EXE-Sisp	0,42775255	6282300	2. Maturidade intermediária	R\$ 249.791.868,16
JUD	0,52871303	5416293	2. Maturidade intermediária	R\$ 448.720.430,39
EXE-Sisp	0,38049898	3700000	1. Maturidade inicial	R\$ 1.055.583.513,47
JUD	0,16191272	457800	1. Maturidade inicial	R\$ 68.922.149,24
JUD	0,38227629	1772182	1. Maturidade inicial	R\$ 347.672.947,64
EXE-Sisp	0,50257133	665300	2. Maturidade intermediária	R\$ 38.036.011,69
EXE-Sisp	0,2120296	1579200	1. Maturidade inicial	R\$ 443.250.060,15
EXE-Dest	0,39894492	2832000	1. Maturidade inicial	R\$ 1.546.552.556,90
EXE-Sisp	0,26631598	13684742	1. Maturidade inicial	R\$ 548.269.307,59
JUD	0,43832582	1182505	2. Maturidade intermediária	R\$ 216.578.884,75
EXE-Sisp	0,60577573	59748698	3. Maturidade aprimorada	R\$ 4.813.254.130,73
EXE-Sisp	0,46866222	31725069	2. Maturidade intermediária	R\$ 659.935.125,59
EXE-Sisp	0,19848186	6300000	1. Maturidade inicial	R\$ 199.347.339,63

Segmento	iGovTI2010	Orçamento de TI (2010)	Faixa Maturidade	Orçamento Administrado (2010)
MPU	0,38416546	1818082	1. Maturidade inicial	R\$ 126.812.478,47
EXE-Sisp	0,5639113	9242000	2. Maturidade intermediária	R\$ 491.424.486,86
EXE-Sisp	0,26230116	10040000	1. Maturidade inicial	R\$ 2.473.983.189,86
EXE-Sisp	0,42613141	40186768	2. Maturidade intermediária	R\$ 4.379.780.403,97
MPU	0,39783866	23300000	1. Maturidade inicial	R\$ 700.296.534,01
EXE-Sisp	0,42382376	57600630	2. Maturidade intermediária	R\$ 421.161.101,73
EXE-Sisp	0,62913248	19881822	3. Maturidade aprimorada	R\$ 15.429.119.403,80
EXE-Sisp	0,18012687	10600000	1. Maturidade inicial	R\$ 567.329.554,39
EXE-Sisp	0,37299038	138867434	1. Maturidade inicial	R\$ 64.980.675.033,90
EXE-Sisp	0,26232259	118305000	1. Maturidade inicial	R\$ 1.410.585.743,39
JUD	0,38675946	431451	1. Maturidade inicial	R\$ 66.497.446,73
EXE-Sisp	0,47734572	232432490	2. Maturidade intermediária	R\$ 843.534.827.615,37
EXE-Sisp	0,4389361	4861717	2. Maturidade intermediária	R\$ 785.484.109,86
EXE-Sisp	0,21532276	1519000	1. Maturidade inicial	R\$ 245.456.292,28
EXE-Dest	0,59983031	176117534	2. Maturidade intermediária	R\$ 565.561.011,31
EXE-Sisp	0,54972871	14086155	2. Maturidade intermediária	R\$ 24.408.670.981,00
EXE-Sisp	0,44830737	20351380	2. Maturidade intermediária	R\$ 13.064.594.095,99
EXE-Sisp	0,28532343	46470320	1. Maturidade inicial	R\$ 1.203.233.837,12
EXE-Sisp	0,36798603	2110000	1. Maturidade inicial	R\$ 647.316.555,83
EXE-Sisp	0,42815743	1970000	2. Maturidade intermediária	R\$ 1.360.228.308,27
EXE-Sisp	0,51188911	22420000	2. Maturidade intermediária	R\$ 661.966.908,53
EXE-Sisp	0,33679042	28936000	1. Maturidade inicial	R\$ 1.280.944.723,66
EXE-Sisp	0,31714189	112202840	1. Maturidade inicial	R\$ 2.048.948.498,45
EXE-Sisp	0,33651847	7717984	1. Maturidade inicial	R\$ 163.470.320,02
EXE-Sisp	0,46663098	75027945	2. Maturidade intermediária	R\$ 2.056.015.313,51
EXE-Sisp	0,32733934	18646542	1. Maturidade inicial	R\$ 19.394.966.376,09
EXE-Sisp	0,41198682	13950000	2. Maturidade intermediária	R\$ 249.538.904,10
EXE-Sisp	0,30069512	174178890	1. Maturidade inicial	R\$ 48.247.372.713,20
EXE-Sisp	0,37389234		1. Maturidade inicial	R\$ 221.373.420,79
EXE-Sisp	0,47078324	12445000	2. Maturidade intermediária	R\$ 568.354.580,16

Segmento	iGovTI2010	Orçamento de TI (2010)	Faixa Maturidade	Orçamento Administrado (2010)
LEG	0,55102605	49000000	2. Maturidade intermediária	R\$ 2.770.080.022,38
EXE-Sisp	0,45510056	16120476	2. Maturidade intermediária	R\$ 494.766.935,81
EXE-Sisp	0,43343378	16469100	2. Maturidade intermediária	R\$ 1.405.641.519,61
EXE-Sisp	0,46458557	1734889	2. Maturidade intermediária	R\$ 628.497.377,25
JUD	0,46301248	4790000	2. Maturidade intermediária	R\$ 300.974.091,15
JUD	0,61307287	91905122	3. Maturidade aprimorada	R\$ 554.409.886,73
EXE-Sisp	0,2725799	621000	1. Maturidade inicial	R\$ 371.989.518,39
EXE-Sisp	0,47113391	3225000	2. Maturidade intermediária	R\$ 1.045.481.962,53
EXE-Sisp	0,3750482	2045731	1. Maturidade inicial	R\$ 604.259.151,47
EXE-Sisp	0,34578797	5250000	1. Maturidade inicial	R\$ 639.558.071,20
EXE-Sisp	0,27169302	26247391	1. Maturidade inicial	R\$ 10.886.477.872,73
EXE-Sisp	0,52374045	86126209	2. Maturidade intermediária	R\$ 22.556.262.715,14
EXE-Sisp	0,44485254	2477727	2. Maturidade intermediária	R\$ 104.811.289,13
EXE-Sisp	0,33469744		1. Maturidade inicial	R\$ 820.619.131,22
EXE-Dest	0,28156847		1. Maturidade inicial	R\$ 528.644.535,38
JUD	0,3695268	2979654	1. Maturidade inicial	R\$ 1.074.143.100,21
EXE-Sisp	0,41775956	28619156	2. Maturidade intermediária	R\$ 2.343.436.367,20
JUD	0,35125133	1121453	1. Maturidade inicial	R\$ 110.578.183,72
EXE-Dest	0,42667045	1985000	2. Maturidade intermediária	R\$ 128.879.522,99
EXE-Sisp	0,51826156	65600000	2. Maturidade intermediária	R\$ 3.873.687.297,55
EXE-Sisp	0,59219341	318713926	2. Maturidade intermediária	R\$ 19.328.753.176,31
JUD	0,51935103	1325378	2. Maturidade intermediária	R\$ 272.908.950,31
EXE-Sisp	0,38818047	379757	1. Maturidade inicial	R\$ 97.199.312,12
EXE-Sisp	0,23820555		1. Maturidade inicial	R\$ 158.088.630,12
EXE-Sisp	0,2618036	1012000	1. Maturidade inicial	R\$ 338.874.463,08
EXE-Sisp	0,38233152	3289768	1. Maturidade inicial	R\$ 675.792.687,22
EXE-Sisp	0,32203761	10000000	1. Maturidade inicial	R\$ 452.465.893,39
EXE-Sisp	0,3499973	140000	1. Maturidade inicial	R\$ 82.296.631,47
EXE-Sisp	0,2506259	50000	1. Maturidade inicial	R\$ 81.097.864,68
EXE-Sisp	0,30497928	780000	1. Maturidade inicial	R\$ 63.178.029,61

Segmento	iGovTI2010	Orçamento de TI (2010)	Faixa Maturidade	Orçamento Administrado (2010)
MPU	0,38502039	36632031	1. Maturidade inicial	R\$ 165.644.978,11
EXE-Sisp	0,2667851		1. Maturidade inicial	R\$ 7.251.018,78
EXE-Sisp	0,32688149	1140449	1. Maturidade inicial	R\$ 805.816.645,93
EXE-Sisp	0,28245113		1. Maturidade inicial	R\$ 11.636.707,07
EXE-Dest	0,60948305	354187397	3. Maturidade aprimorada	R\$ 1.570.816.048,84
JUD	0,5151329	106874527	2. Maturidade intermediária	R\$ 790.797.007,51
EXE-Sisp	0,39749541	6360000	1. Maturidade inicial	R\$ 822.566.789,43
EXE-Sisp	0,28299865	16076500	1. Maturidade inicial	R\$ 10.405.413,83
EXE-Sisp	0,43803243		2. Maturidade intermediária	R\$ 39.040.257,47
EXE-Sisp	0,38450405	430000	1. Maturidade inicial	R\$ 235.062.490,37
EXE-Sisp	0,30369505	2014438	1. Maturidade inicial	R\$ 318.365.282,80
JUD	0,44466965	473872	2. Maturidade intermediária	R\$ 89.936.042,76
EXE-Sisp	0,18599099	6811867	1. Maturidade inicial	R\$ 346.617.420,57
EXE-Sisp	0,38080793	2556645	1. Maturidade inicial	R\$ 405.410.072,26
JUD	0,30558755	779212	1. Maturidade inicial	R\$ 67.738.326,03
EXE-Sisp	0,45272606	158967472	2. Maturidade intermediária	R\$ 261.897.314.348,75
EXE-Sisp	0,21897252	271500	1. Maturidade inicial	R\$ 67.016.711,03
EXE-Sisp	0,30415184	1010000	1. Maturidade inicial	R\$ 80.494.922,73
EXE-Sisp	0,30078804		1. Maturidade inicial	R\$ 6.024.729,99
EXE-Sisp	0,36823951	23300000	1. Maturidade inicial	R\$ 228.559.108,78
EXE-Sisp	0,49129323	390000	2. Maturidade intermediária	R\$ 257.883.963,39
EXE-Sisp	0,53769647	2012940	2. Maturidade intermediária	R\$ 106.721.486,53
EXE-Sisp	0,3633023	809286	1. Maturidade inicial	R\$ 487.212.848,78
EXE-Sisp	0,34421696	1776749	1. Maturidade inicial	R\$ 408.158.398,00
EXE-Sisp	0,38250991	95000	1. Maturidade inicial	R\$ 76.217.870,20
EXE-Sisp	0,46913123	3112070	2. Maturidade intermediária	R\$ 274.351.036,60
EXE-Sisp	0,40153169	32190000	2. Maturidade intermediária	R\$ 3.078.548.770,64
EXE-Sisp	0,33936156	300000	1. Maturidade inicial	R\$ 97.151.422,70
EXE-Sisp	0,34646059	16081424	1. Maturidade inicial	R\$ 134.871.417,61
EXE-Sisp	0,19346982	24001024	1. Maturidade inicial	R\$ 100.157.698,35

Segmento	iGovTI2010	Orçamento de TI (2010)	Faixa Maturidade	Orçamento Administrado (2010)
EXE-Sisp	0,45681712	200000	2. Maturidade intermediária	R\$ 14.601.009,95
LEG	0,51395677	19600000	2. Maturidade intermediária	R\$ 1.087.803.934,71
EXE-Sisp	0,48190477	1350000000	2. Maturidade intermediária	R\$ 342.655.674.851,46
JUD	0,48747795	529611774	2. Maturidade intermediária	R\$ 612.340.542,84
EXE-Sisp	0,27258468	41000000	1. Maturidade inicial	R\$ 5.033.681.096,45
EXE-Sisp	0,49602801	54846000	2. Maturidade intermediária	R\$ 1.473.351.564,62
JUD	0,37863892		1. Maturidade inicial	R\$ 54.672.250,65
EXE-Sisp	0,64661597	18480707	3. Maturidade aprimorada	R\$ 223.647.881,90
EXE-Sisp	0,49122376	16647164	2. Maturidade intermediária	R\$ 196.023.544,92
JUD	0,41449712	471000	2. Maturidade intermediária	R\$ 31.308.484,94
EXE-Sisp	0,25582835	38436154	1. Maturidade inicial	R\$ 296.375.587,99
EXE-Sisp	0,27044106	2276556	1. Maturidade inicial	R\$ 31.178.466,59
EXE-Sisp	0,38019955	43690792	1. Maturidade inicial	R\$ 1.338.674.988,84
LEG	0,23887413	39239340	1. Maturidade inicial	R\$ 2.498.219.229,11
JUD	0,37437207	574830	1. Maturidade inicial	R\$ 135.712.943,19
JUD	0,38381897	2144094	1. Maturidade inicial	R\$ 335.872.767,65
JUD	0,3407301	1506924	1. Maturidade inicial	R\$ 240.814.548,77
EXE-Sisp	0,49804028	43826851	2. Maturidade intermediária	R\$ 142.666.277,88
EXE-Dest	0,49983307	5112545	2. Maturidade intermediária	R\$ 338.050.612,66
JUD	0,32043481	1560129	1. Maturidade inicial	R\$ 200.049.850,97
EXE-Sisp	0,22689279	890000	1. Maturidade inicial	R\$ 132.556.512,28
JUD	0,5609736	391190	2. Maturidade intermediária	R\$ 31.259.561,06
JUD	0,33775572	12132271	1. Maturidade inicial	R\$ 1.291.316.476,83
EXE-Dest	0,41774324	7502352	2. Maturidade intermediária	R\$ 2.841.867.348,15
JUD	0,36068333	896890	1. Maturidade inicial	R\$ 93.406.376,57
EXE-Dest	0,54207303	18405130	2. Maturidade intermediária	R\$ 1.413.122.169,37
JUD	0,41044617	1059001	2. Maturidade intermediária	R\$ 67.377.650,95
JUD	0,35939009	800000	1. Maturidade inicial	R\$ 338.220.164,77
EXE-Sisp	0,28851457	3986000	1. Maturidade inicial	R\$ 83.997.708,71
JUD	0,62623722	9930000	3. Maturidade aprimorada	R\$ 951.755.912,93

Segmento	iGovTI2010	Orçamento de TI (2010)	Faixa Maturidade	Orçamento Administrado (2010)
JUD	0,46792108	25160188	2. Maturidade intermediária	R\$ 345.382.812,60
EXE-Sisp	0,25942779	2309775	1. Maturidade inicial	R\$ 287.543.707,20
EXE-Sisp	0,26460792	4600000	1. Maturidade inicial	R\$ 883.668.723,60
EXE-Sisp	0,41288345	278187799	2. Maturidade intermediária	R\$ 251.531.526,69
EXE-Sisp	0,2593027	420000	1. Maturidade inicial	R\$ 46.454.955,98
EXE-Sisp	0,27881734	1148744	1. Maturidade inicial	R\$ 74.578.429,47
EXE-Sisp	0,34803627	3005826	1. Maturidade inicial	R\$ 1.186.932.220,16
EXE-Dest	0,35486074	7083440	1. Maturidade inicial	R\$ 1.957.235.462,05
EXE-Sisp	0,54039843	26951145	2. Maturidade intermediária	R\$ 318.651.597,26
JUD	0,41211802	857621	2. Maturidade intermediária	R\$ 134.589.180,02
EXE-Sisp	0,28332201	80000	1. Maturidade inicial	R\$ 134.370.231,72
JUD	0,34104498	4762947	1. Maturidade inicial	R\$ 394.455.370,07

Fundamentação para a assertiva de que a governança corporativa limita a governança de TI

(1) ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS – ABNT. ABNT NBR ISO/IEC 38500:2009 – Governança corporativa de tecnologia da informação.

- p.3 Esta Norma faz referência aos seguintes documentos: Relatório do Comitê sobre Aspectos Financeiros de Governança Corporativa, Sir Adrian Cadbury, Londres, 1992 ISBN 0 85258 913 1 OECD Princípios de Governança Corporativa, OECD, 1999 e 2004

- p.4 1.6.9 Gerenciamento O sistema de controles e processos necessário para alcançar os objetivos estratégicos estabelecidos pela direção da organização. O gerenciamento está sujeito às diretrizes, às políticas e ao monitoramento estabelecidos pela governança corporativa.

(2) BRISEBOIS, Richard; BOYD, Greg; SHADID, Ziad. What is IT Governance? and why is it important for the IS auditor. IntoIT

- p.2 Information technology governance, however, is a subset discipline of Corporate Governance. Although it is sometimes mistaken as a field of study on its own, IT Governance is actually a part of the overall Corporate Governance Strategy of an organisation.

INFORMATION TECHNOLOGY GOVERNANCE INSTITUTE – ITGI. COBIT – Control Objectives for Information and related Technology.

- p.8 A necessidade da avaliação do valor de TI, o gerenciamento dos riscos relacionados à TI e as crescentes necessidades de controle sobre as informações são agora entendidos como elementos-chave da governança corporativa. Valor, risco e controle constituem a essência da governança de TI.

- p.47 PO4.2 Comitê Estratégico de TI Estabelecer um comitê estratégico de TI em nível de Diretoria. Esse comitê assegura que a governança de TI seja devidamente considerada como parte da governança corporativa, aconselha sobre o direcionamento estratégico e analisa os principais investimentos, em nome de toda a Direção.

- p.173 ME4 Prover Governança de TI O estabelecimento de uma efetiva estrutura de governança envolve a definição das estruturas organizacionais, dos processos, da liderança, dos papéis e respectivas responsabilidades para assegurar que os investimentos corporativos em TI estejam alinhados e sejam entregues em conformidade com as estratégias e os objetivos da organização. [...] Controle sobre o

seguinte processo de TI: Prover Governança de TI, que satisfaça aos seguintes requisitos do negócio para a TI: integrar a governança de TI aos objetivos de governança corporativa e ter conformidade com leis, regulamentações e contratos (...) é alcançado por: Estabelecimento de uma estrutura de governança de TI integrada à governança corporativa

• p.176 O gerenciamento do processo de “Prover Governança de TI” que satisfaça ao requisito do negócio para a TI de “integrar a governança de TI com os objetivos de governança corporativa e ter conformidade com as leis e as regulamentações” é: (...) 5 Otimizado quando Há um entendimento avançado, que aponta para o futuro, das questões voltadas à governança de TI e suas soluções. O treinamento e a comunicação são sustentados por conceitos e técnicas mais avançados. Os processos têm sido bem refinados no nível de melhores práticas do seu segmento de indústria a partir dos resultados do aprimoramento contínuo e da modelagem de maturidade com outras organizações. A implementação das políticas de TI permite que a organização, as pessoas e os processos tenham rápida adaptação e completa assimilação dos requisitos de governança de TI. Todos os problemas e desvios têm suas causas-raiz analisadas, e ações eficientes são sistematicamente identificadas e executadas. A TI é utilizada de forma otimizada, integrada e extensiva para automatizar o fluxo de trabalho e disponibilizar ferramentas para melhorar a qualidade e a efetividade. Os riscos e retornos dos processos de TI são definidos, balanceados e comunicados por toda empresa. Especialistas externos são agregados, e benchmarks são utilizados como guias de orientação. O monitoramento, a autoavaliação e a comunicação sobre as expectativas de governança são difundidos na organização, e há uso otimizado de tecnologia para auxiliar na medição, na análise, na comunicação e no treinamento. A governança corporativa e a governança de TI são estrategicamente correlacionadas, alavancando os recursos humanos, tecnológicos e financeiros para aumentar as vantagens competitivas da organização. As atividades da governança de TI são integradas ao processo de governança corporativa.

LEYER, Janeane; QUIGLEY, Katelyn. Small business IT Governance implementation. ISACA Journal Online

• p.1 IT governance is no longer about making specific IT decisions. Businesses that recognize and manage the connection between information technology and economic success are able to realize significant value from their IT investments and enhance their operations. IT governance allows businesses to maximize revenue by utilizing resources only for projects with the highest value. Over a period of time, businesses that successfully govern IT are able to recognize 30 percent higher profits than firms without successful IT governance.2 IT governance can also lead to improved customer satisfaction, as it allows management to fully understand customers' needs and results in more effective and efficient service. By integrating IT governance with corporate governance, businesses are able to improve processes and align resources with business strategy.

• p.2 The connection between IT governance and corporate governance is two-pronged. The information that management relies on to make strategic decisions is often a product of the IT systems. In addition, the vision of the company gaining a competitive advantage is achieved by bridging business and technology.

PARKINSON, Michael J. A.; BAKER, Nicholas J. IT and Enterprise Governance. Information Systems Control Journal

• p.2 Logically, IT governance is a subset of enterprise governance. IT governance covers performance and compliance considerations. Since IT is an enabler to business, perhaps it is fair to say that IT governance exists to help organisations make the most of IT. IT governance...is an integral part of enterprise governance and consists of the leadership and organisational structures and processes that ensure that the organisation's IT sustains and extends the organisation's strategies and objectives.5 Practical Implications This definition implies that IT governance has three components:

- Leadership—Suggesting vision, responsibility and accountability
- Organisation—Suggesting staffing, resourcing and structures
- Processes—Suggesting established standards and procedures

PELANDA, Maurício Luiz. Modelos de governança de tecnologia da informação adotados no Brasil – um estudo de casos múltiplos.

• p.15 De acordo com Guldenopps (2004), a GTI tem como premissa a proteção do valor dos stakeholders<sup>1</sup>; de tornar claro que os riscos de TI sejam quantificados e mitigados; direcionar e

controlar os investimentos de TI. É um processo gerador de oportunidades e benefícios, traz melhor entendimento nas análises de riscos; alinha TI ao negócio enquanto aceita TI como uma entrada crítica para o planejamento estratégico; sustenta as operações, prepara a organização para o futuro e é parte integrante da estrutura global da governança corporativa.

SHORT, Julie; GERRARD, Michael. IT governance must be driven by corporate governance.

• p.3 In 2009, the ITGI adopted the ISO/IEC 38500 IT governance standard, which is based on a pre-existing Australian standard and has been in place since April 2008. It represents an effort to provide guidance in defining IT governance as a component of corporate governance and is intended for all organizations, regardless of size or sector.

### (3) ITGI. COBIT5-Framework-ED-27June2011

• p.18 COBIT 5 provides new capabilities for effective enterprise governance and management of IT: • The starting point of governance and management activities are the stakeholder needs related to enterprise IT. • Creates a more holistic, integrated and complete view of enterprise governance and management of IT that: – Is consistent – Provides an end-to-end view on all IT-related matters – Provides a systemic view • Creates a common language between IT and business for the enterprise governance and management of IT • Is consistent with generally accepted corporate governance standards, and thus helps to meet regulatory requirements • Creates a clear distinction between governance and management of enterprise governance of IT

NOLAN, Richard; MCFARLAN, F. Warren. Information Technology and the Board of Directors. Harvard Business Review

• p.1-2 Because there has been no comparable body of knowledge and best practice, IT governance doesn't exist per se. Indeed, board members frequently lack the fundamental knowledge needed to ask intelligent questions about not only IT risk and expense but also competitive risk. This leaves the CIOs, who manage critical corporate information assets, pretty much on their own. A lack of board oversight for IT activities is dangerous; it puts the firm at risk in the same way that failing to audit its books would.

### (4) ANDREN, E.; FURLONGER, J.; MAGEE F.; MINGAY, S. The five pillars of IS organizational effectiveness. Gartner Group

• p.78 Information technology cannot be used to address the misalignment between the goals of the BUs and the wider goals of the enterprise; only an appropriate governance can achieve this. Unfortunately it is often politically expedient for the misalignment and governance not to be addressed by the business executive team. It is important that the CIO identify root causes, such as this. If the issue cannot be addressed through either a modification in corporate governance, or an agreement on the strategic context and the guiding principles, then it is all the more important that the CIO frame all IS initiatives within his or her view of the strategic context. It is recommended that the CIO clearly articulate his position. In this environment negotiation skills, deal making and being politically aware are critical to the success of the CIO and the perceived alignment of the IS organization.

BARBOSA, Alexandre Fernandes; JUNQUEIRA, Alvaro Ribeiro Botelho; LAIA, Marconi Martins de; FARIA, Fernando Inacio de. Governança de TIC e contratos no setor público. In: CATI – Congresso Anual de Tecnologia da Informação

• p.2 No contexto da gestão pública, governança corporativa está relacionada ao aumento da capacidade que o governo, através da adoção de princípios gerenciais, tem para orientar a ação do estado focada em resultados e ênfase em mecanismos de controle. Pode-se afirmar que a governança no setor público é fruto do movimento de reforma do estado e modernização da gestão pública, tópicos relevantes na agenda política dos governos (BARZELAY, 2000; HEEKS, 2002; PETERS, 1996). Consequentemente, temas como desempenho, eficiência, eficácia, transparéncia, mecanismos de controle, qualidade do gasto público e prestação de contas passaram a ser questões centrais no processo de modernização da gestão pública (BARBOSA et al., 2005; REINHARD e DIAS, 2005), as quais conduzem à idéia de implementação de mecanismos de controle e de boas práticas de governança.

• p.3 A exemplo do setor privado, a adoção e o uso de recursos tecnológicos na gestão pública requerem também a implantação de mecanismos de governança de TIC a fim de garantirem uma gestão eficiente. Assim, a governança dos recursos tecnológicos torna-se um processo vital para a implantação de mecanismos de governança corporativa no setor público. Existem várias estruturas de referência que apresentam boas práticas de governança de TIC, entre elas o COBIT e o ITIL4.

• p.4 Nesse contexto, a governança de TIC se mostra como um dos temas mais relevantes para os altos dirigentes, dado que trata de questões que vão além das fronteiras tecnológicas, sustentando os princípios básicos da governança corporativa.

(5) SHORT, Julie; GERRARD, Michael. IT governance must be driven by corporate governance.

• p.2 Although several principles of corporate governance influence IT governance, there are two where this influence is substantial:

- Disclosure and transparency — This refers to the financial and operational information of the organization and foreseeable risk factors.
- Responsibility of the board of directors — This involves ensuring strategic guidance to the organization, effective monitoring and responsibility to shareholders/stakeholders.

(6) HOLT, Alison. IT Governance Comes of Age. *Information Systems Control Journal*

• p.1 The group also came across a number of IT managers and principal consultants who had failed in an attempt to interest their executive in matters relating to IT governance. The group discovered that however evangelical the IT managers, and however receptive their executives, unless the executives owned the strategic direction of IT governance in the same way they owned the governance of their other key organisational assets, there would be no consistency in the operational management, development or delivery of IT.

SHORT, Julie; GERRARD, Michael. IT governance must be driven by corporate governance.

• p.1 IT governance is driven by good corporate governance. CIOs and other IT leaders need to understand these principles and how to obtain senior business participation in IT governance. Key Findings

- Corporate governance is an important input for defining IT governance.
- IT governance must ensure that IT risks are effectively managed.
- IT governance requires senior business participation, especially at the board level.

• p.3 In speaking with clients, Gartner sees the lines between the business and IT becoming more blurred. We see IT tasks being performed in the business, business taking on IT leadership roles and vice versa. However, when it comes to IT governance, we see that often this is erroneously delegated to the CIO due to several factors:

- A lack of business understanding regarding the role of the board in ensuring that IT assets and resources are managed and measured, and that IT risks are mitigated.
- A perception that anything IT needs should be handled by the CIO.
- Competing factions within IT, all wanting governance over their respective domains. As a result, the term “governance” has become overused and misunderstood. IT leaders should understand that IT governance is effective when it is driven by corporate governance and defined as a cohesive process by using five steps: strategize, plan, implement, manage and monitor (see “Defining IT Governance: Roles and Relationships”).

(7) SILVA, André Luiz Carvalhal da; LEAL, Ricardo Pereira Câmara. Corporate governance index, firm valuation and performance in Brazil. *Revista Brasileira de Finanças*

• Este estudo investiga a relação entre a qualidade das práticas de governança corporativa das empresas e seu valor de mercado e desempenho, através da construção de um índice de governança corporativa para as empresas brasileiras listadas. Os resultados empíricos indicam um alto grau de concentração do controle e propriedade. Pode-se notar também uma diferença significativa entre o capital votante e o capital total dos maiores acionistas, principalmente através da existência de ações sem direito de voto. Os resultados da análise de painel indicam que menos de 4% das firmas brasileiras possuem “boas” práticas de governança corporativa e que as firmas com melhor governança corporativa tem um desempenho (retorno sobre o ativo) significativamente superior. Existe também uma relação positiva entre o Q de Tobin e a qualidade das práticas de governança corporativa, embora os resultados não sejam estatisticamente significativos.

## Plano de Ação Global na estrutura regimental dos ministérios

Nº	Ministério	Decreto	Dispositivo
1.	Advocacia-Geral da União	Decreto 7.392/2010	Não tem
2.	Casa Civil da Presidência da República	Decreto 5.135/2004	Art. 23, inciso I
3.	Controladoria-Geral da União	Decreto 5.683/2006	Não tem
4.	Gabinete de Segurança Institucional da Presidência da República	Decreto 7.411/2010	Não tem
5.	Ministério da Agricultura, Pecuária e Abastecimento	Decreto 7.127/2010	Art. 41, inciso I
6.	Ministério da Ciência e Tecnologia	Decreto 5.886/2006	Art. 38, inciso I
7.	Ministério da Cultura	Decreto 6.835/2009	Não tem
8.	Ministério da Defesa	Decreto 7.364/2010	Não tem
9.	Ministério da Educação	Decreto 7.480/2011	Art. 38, inciso I
10.	Ministério da Fazenda	Decreto 7.482/2011	Art. 43, inciso I
.			
11.	Ministério da Integração Nacional	Decreto 7.472/2011	Art. 29, inciso IV
.			
12.	Ministério da Justiça	Decreto 6.061/2007	Art. 43, inciso I
.			
13.	Ministério da Pesca e Aquicultura	Decreto 6.972/2009	Não tem
.			
14.	Ministério da Previdência Social	Decreto 7.078/2010	Art. 17, inciso I
.			
15.	Ministério da Saúde	Decreto 7.530/2011	Art. 49, inciso I
.			
16.	Ministério das Cidades	Decreto 4.665/2003	Art. 26, inciso I
.			
17.	Ministério das Comunicações	Decreto 7.462/2011	Não tem
.			
18.	Ministério das Relações Exteriores	Decreto 7.304/2010	Não tem
.			
19.	Ministério das Minas e Energia	Decreto 5.267/2004	Art. 27, inciso I
.			
20.	Ministério do Desenvolvimento Agrário	Decreto 7.255/2010	Art. 22, inciso I
.			
21.	Ministério do Desenvolvimento Social e Combate à Fome	Decreto 7.493/2011	Art. 36, inciso I
.			
22.	Ministério do Desenvolvimento, Indústria e Comércio Exterior	Decreto 7.096/2010	Art. 30, inciso I
.			
23.	Ministério do Esporte	Decreto 7.529/2011	Art. 20, inciso I
.			
24.	Ministério do Meio Ambiente	Decreto 6.101/2007	Art. 43, inciso I
.			
25.	Ministério do Planejamento, Orçamento e Gestão	Decreto 7.063/2010	Art. 49, inciso I
.			
26.	Ministério do Trabalho e Emprego	Decreto 5.063/2004	Art. 27, inciso I
.			
27.	Ministério do Turismo	Decreto 6.546/2008	Art. 20, inciso I
.			
28.	Ministério dos Transportes	Decreto 4.721/2003	Art. 19, inciso I
.			

29	Secretaria de Assuntos Estratégicos da Presidência da República	Decreto 6.517/2008	Art. 7º, inciso I
30	Secretaria de Comunicação Social da Presidência da República	Decreto 6.377/2008	Não tem
31	Secretaria de Direitos Humanos da Presidência da República	Decreto 6.980/2009	Não tem
32	Secretaria de Políticas de Promoção da Igualdade Racial da Presidência da República	Decreto 7.261/2010	Não tem
33	Secretaria de Políticas para as Mulheres da Presidência da República	Decreto 7.043/2009	Não tem
34	Secretaria de Portos da Presidência da República	Decreto 7.262/2010	Não tem
35	Secretaria de Relações Institucionais da Presidência da República	Decreto 6.207/2007	Art. 9º, inciso I
36	Secretaria-Geral da Presidência da República	Decreto 6.378/2008	Art. 11, inciso I
37	Secretaria de Aviação Civil da Presidência da República	Decreto 7.476/2011	Art. 18, inciso I

Referencial normativo do Plano de Ação Global

#### ORIGEM DO PLANO DE AÇÃO GLOBAL

1. D99180 [Revogado](1)
2. D99244(2)
3. Recepcionado pela L10180(3)
4. Lei nº 10.683/2003

#### PLANO DE AÇÃO GLOBAL

5. Casa Civil da Presidência da República(5)
6. Ministério da Agricultura, Pecuária e Abastecimento(6)
7. Ministério da Ciência e Tecnologia(7)
8. Ministério da Educação(8)
9. Ministério da Fazenda(9)
10. Ministério da Integração Nacional(10)
11. Ministério da Justiça(11)
12. Ministério da Previdência Social(12)
13. Ministério da Saúde(13)
14. Ministério das Cidades(14)
15. Ministério das Minas e Energia(15)
16. Ministério do Desenvolvimento Agrário(16)
17. Ministério do Desenvolvimento, Indústria e Comércio Exterior(17)
18. Ministério do Desenvolvimento Social e Combate à Fome(18)
19. Ministério do Esporte(19)
20. Ministério do Meio Ambiente(20)
21. Ministério do Planejamento, Orçamento e Gestão(21)
22. Ministério do Trabalho e Emprego(22)
23. Ministério do Turismo(23)
24. Ministério dos Transportes(24)
25. Secretaria de Assuntos Estratégicos da Presidência da República(25)
26. Secretaria de Relações Institucionais da Presidência da República(26)
27. Secretaria-Geral da Presidência da República(27)
28. Secretaria de Aviação Civil da Presidência da República(28)
5. Casa Civil da Presidência da República(5)

6. Ministério da Agricultura, Pecuária e Abastecimento(6)
7. Ministério da Ciência e Tecnologia(7)
8. Ministério da Educação(8)
9. Ministério da Fazenda(9)
10. Ministério da Integração Nacional(10)
11. Ministério da Justiça(11)
12. Ministério da Previdência Social(12)
13. Ministério da Saúde(13)
14. Ministério das Cidades(14)
15. Ministério das Minas e Energia(15)
16. Ministério do Desenvolvimento Agrário(16)
17. Ministério do Desenvolvimento, Indústria e Comércio Exterior(17)
18. Ministério do Desenvolvimento Social e Combate à Fome(18)
19. Ministério do Esporte(19)
20. Ministério do Meio Ambiente(20)
21. Ministério do Planejamento, Orçamento e Gestão(21)
22. Ministério do Trabalho e Emprego(22)
23. Ministério do Turismo(23)
24. Ministério dos Transportes(24)
25. Secretaria de Assuntos Estratégicos da Presidência da República(25)
26. Secretaria de Relações Institucionais da Presidência da República(26)
27. Secretaria-Geral da Presidência da República(27)
28. Secretaria de Aviação Civil da Presidência da República(28)

**NÃO REFEREM A UM DOCUMENTO DE PLANEJAMENTO INSTITUCIONAL**

29. Advocacia-Geral da União(29)
30. Controladoria-Geral da União(30)
31. Gabinete de Segurança Institucional da Presidência da República(31)
32. Ministério da Cultura(32)
33. Ministério da Defesa(33)
34. Ministério da Pesca e Aquicultura(34)
35. Ministério das Comunicações(35)
36. Secretaria de Comunicação Social da Presidência da República(36)
37. Secretaria de Políticas para as Mulheres da Presidência da República(37)
38. Ministério das Relações Exteriores(38)
39. Secretaria de Direitos Humanos da Presidência da República(39)
40. Secretaria de Políticas de Promoção da Igualdade Racial da Presidência da República(40)
41. Secretaria de Portos da Presidência da República(41)

- 
30. Controladoria-Geral da União(30)
  31. Gabinete de Segurança Institucional da Presidência da República(31)
  32. Ministério da Cultura(32)
  33. Ministério da Defesa(33)
  34. Ministério da Pesca e Aquicultura(34)
  35. Ministério das Comunicações(35)
  36. Secretaria de Comunicação Social da Presidência da República(36)
  37. Secretaria de Políticas para as Mulheres da Presidência da República(37)
  38. Ministério das Relações Exteriores(38)
  39. Secretaria de Direitos Humanos da Presidência da República(39)
  40. Secretaria de Políticas de Promoção da Igualdade Racial da Presidência da República(40)
  41. Secretaria de Portos da Presidência da República(41)

30. Controladoria-Geral da União(30)
31. Gabinete de Segurança Institucional da Presidência da República(31)
32. Ministério da Cultura(32)
33. Ministério da Defesa(33)
34. Ministério da Pesca e Aquicultura(34)
35. Ministério das Comunicações(35)
36. Secretaria de Comunicação Social da Presidência da República(36)
37. Secretaria de Políticas para as Mulheres da Presidência da República(37)
38. Ministério das Relações Exteriores(38)
39. Secretaria de Direitos Humanos da Presidência da República(39)
40. Secretaria de Políticas de Promoção da Igualdade Racial da Presidência da República(40)
41. Secretaria de Portos da Presidência da República(41)

---

Fundamentação:

1

BRASIL. Decreto nº 99.180, de 15 de março de 1990.

• Art. 75) Haverá em cada ministério civil um Secretário-Executivo, nomeado pelo Presidente da República, mediante indicação do Ministro de Estado competente.

• Art. 76) Ao Secretário-Executivo incumbe: I – auxiliar o Ministro de Estado na formulação e execução dos assuntos incluídos na área de competência do ministério; II – exercer a coordenação, supervisão e controle das Secretarias do ministério, não subordinadas diretamente ao Ministro de Estado; III – submeter ao Ministro de Estado o planejamento de ação global do ministério, em consonância com as diretrizes de Governo fixadas pelo Presidente da República; IV – supervisionar, coordenar e controlar as atividades de planejamento, orçamento, modernização e reforma administrativa e de programação financeira do ministério; V – coordenar e providenciar o encaminhamento à Presidência da República, de projetos de leis, de medidas provisórias ou de decretos de interesse do ministério; VI – exercer outras atribuições que lhe forem cometidas pelo Ministro de Estado.

---

2

BRASIL. Decreto nº 99.244, de 10 de maio de 1990.

• Art. 75) Haverá em cada Ministério Civil, exceto no Ministério das Relações Exteriores, um Secretário-Executivo, nomeado pelo Presidente da República, mediante indicação do Ministro de Estado competente.

• Art. 76) Ao Secretário-Executivo compete: I – auxiliar o Ministro de Estado na formulação e execução dos assuntos incluídos na área de competência do Ministério; II – exercer a coordenação, supervisão e controle das Secretarias do Ministério não subordinadas diretamente ao Ministro de Estado; III – submeter ao Ministro de Estado o planejamento da ação global do Ministério, em consonância com as diretrizes de Governo fixadas pelo Presidente da República; IV – supervisionar, coordenar e controlar as atividades de planejamento, orçamento, modernização e reforma administrativa e de programação financeira do Ministério; V – coordenar e providenciar o encaminhamento à Presidência da República, de projetos de leis, de medidas provisórias ou de decretos de interesses do Ministério; VI – exercer outras atribuições que lhe forem cometidas pelo Ministro de Estado.

---

3

BRASIL. Lei nº 10.180, de 6 de fevereiro de 2001.

• TÍTULO II. DO SISTEMA DE PLANEJAMENTO E DE ORÇAMENTO FEDERAL.  
CAPÍTULO I. DAS FINALIDADES. Art. 2º O Sistema de Planejamento e de Orçamento Federal tem por finalidade: I – formular o planejamento estratégico nacional; II – formular planos nacionais, setoriais e

regionais de desenvolvimento econômico e social; III – formular o plano plurianual, as diretrizes orçamentárias e os orçamentos anuais; IV – gerenciar o processo de planejamento e orçamento federal; V – promover a articulação com os Estados, o Distrito Federal e os Municípios, visando a compatibilização de normas e tarefas afins aos diversos Sistemas, nos planos federal, estadual, distrital e municipal.

---

4

BRASIL. Lei nº 10.683, de 28 de maio de 2003.

• Art. 27. Os assuntos que constituem áreas de competência de cada Ministério são os seguintes: [...] XVII – Ministério do Planejamento, Orçamento e Gestão: a) participação na formulação do planejamento estratégico nacional; [...] g) coordenação e gestão dos sistemas de planejamento e orçamento federal, de pessoal civil, de organização e modernização administrativa, de administração de recursos da informação e informática e de serviços gerais; [...]

• Art. 28. Haverá, na estrutura básica de cada Ministério: I – Secretaria-Executiva, exceto nos Ministérios da Defesa e das Relações Exteriores; [...] § 2º Caberá ao Secretário Executivo, titular do órgão a que se refere o inciso I, além da supervisão e da coordenação das Secretarias integrantes da estrutura do Ministério, exercer as funções que lhe forem atribuídas pelo Ministro de Estado. § 3º Poderá haver na estrutura básica de cada Ministério, vinculado à Secretaria-Executiva, um órgão responsável pelas atividades de administração de pessoal, de material, patrimonial, de serviços gerais, de orçamento e finanças, de contabilidade e de tecnologia da informação e informática.

---

5

BRASIL. Decreto nº 5.135, de 7 de julho de 2004.

• Art. 23, I) Ao Secretário-Executivo da Casa Civil incumbe: I – coordenar, consolidar e submeter ao Ministro de Estado o plano de ação global da Casa Civil;

---

6

BRASIL. Decreto nº 7.127, de 4 de março de 2010.

• Art. 41, I) Ao Secretário-Executivo incumbe: I – coordenar e promover a consolidação do plano de ação global do Ministério e submetê-lo à aprovação do Ministro de Estado;

---

7

BRASIL. Decreto nº 5.886, de 6 de setembro de 2006.

• Art. 38, I) Ao Secretário-Executivo incumbe: I – coordenar, consolidar e submeter ao Ministro de Estado o plano de ação global do Ministério;

---

8

BRASIL. Decreto nº 7.480, de 16 de maio de 2011.

• Art. 38, I) Ao Secretário-Executivo incumbe: I – coordenar, consolidar e submeter ao Ministro de Estado o plano de ação global do Ministério;

---

9

BRASIL. Decreto nº 7.482, de 16 de maio de 2011.

• Art. 43, I) Ao Secretário-Executivo incumbe: I – coordenar, consolidar e submeter ao Ministro de Estado o plano de ação global do Ministério;

10

BRASIL. Decreto nº 7.472, de 4 de maio de 2011.

• Art. 29, IV) Ao Secretário-Executivo incumbe: [...] IV – coordenar, consolidar e submeter ao Ministro de Estado o plano de ação global do Ministério; e

11

BRASIL. Decreto nº 6.061, de 15 de março de 2007.

• Art. 43, I) Ao Secretário-Executivo incumbe: I – coordenar, consolidar e submeter ao Ministro de Estado o plano de ação global do Ministério;

12

BRASIL. Decreto nº 7.078, de 26 de janeiro de 2010.

• Art. 17, I) Ao Secretário-Executivo incumbe: I – coordenar, consolidar e submeter ao Ministro de Estado o plano de ação global do Ministério;

13

BRASIL. Decreto nº 7.530 de 21 de julho de 2011.

• Art. 49, I) Ao Secretário-Executivo incumbe: I – coordenar, consolidar e submeter ao Ministro de Estado da Saúde o plano de ação global do Ministério;

14

BRASIL. Decreto nº 4.665, de 3 de abril de 2003.

• Art. 26, I) Ao Secretário-Executivo incumbe: I – coordenar, consolidar e submeter ao Ministro de Estado o plano de ação global do Ministério;

15

BRASIL. Decreto nº 5.267 de 9 de novembro de 2004.

• Art. 27, I) Ao Secretário-Executivo incumbe: I – coordenar, consolidar e submeter ao Ministro de Estado o plano de ação global do Ministério;

16

BRASIL. Decreto nº 7.255, de 4 de agosto de 2010.

• Art. 22, I) Ao Secretário-Executivo incumbe: I – coordenar, consolidar e submeter ao Ministro de Estado o plano de ação global do Ministério;

17

BRASIL. Decreto nº 7.096, de 4 de fevereiro de 2010.

• Art. 30, I) Ao Secretário-Executivo incumbe: I – coordenar, consolidar e submeter ao Ministro de Estado o plano de ação global do Ministério, em consonância com as diretrizes do Governo Federal;

18

BRASIL. Decreto nº 7.493, de 2 de junho de 2011.

• Art. 36, I) Ao Secretário-Executivo incumbe: I – coordenar, consolidar e submeter ao Ministro de Estado o plano de ação global do Ministério;

---

19

BRASIL. Decreto nº 7.529 de 21 de julho de 2011.

• Art. 20, I) Ao Secretário-Executivo incumbe: I – coordenar, consolidar e submeter ao Ministro de Estado o plano de ação global do Ministério;

---

20

BRASIL. Decreto nº 6.101, de 26 de abril de 2007.

• Art. 43, I) Ao Secretário-Executivo incumbe: I – coordenar, consolidar e submeter ao Ministro de Estado o plano de ação global do Ministério;

---

21

BRASIL. Decreto nº 7.063, de 13 de janeiro de 2010.

• Art. 49, I) Ao Secretário-Executivo incumbe: I – coordenar, consolidar e submeter ao Ministro de Estado o plano de ação global do Ministério;

---

22

BRASIL. Decreto nº 5.063, de 3 de maio de 2004.

• Art. 27, I) Ao Secretário-Executivo incumbe: I – coordenar, consolidar e submeter ao Ministro de Estado o plano de ação global do Ministério;

---

23

BRASIL. Decreto nº 6.546, de 25 de agosto de 2008.

• Art. 20, I) Ao Secretário-Executivo incumbe: I – coordenar, consolidar e submeter ao Ministro de Estado o planejamento da ação global do Ministério, em consonância com as diretrizes do Governo Federal;

---

24

BRASIL. Decreto nº 4.721, de 5 de junho de 2003.

• Art. 19, I) Ao Secretário-Executivo incumbe: I – coordenar, consolidar e submeter ao Ministro de Estado o plano de ação global do Ministério;

---

25

BRASIL. Decreto nº 6.517, de 28 de julho de 2008.

• Art. 7º, I) Ao Secretário-Executivo da Secretaria de Assuntos Estratégicos incumbe: (Redação dada pelo Decreto nº 7.465, de 20011). I – coordenar, consolidar e submeter ao Ministro de Estado o plano de ação global da Secretaria de Assuntos Estratégicos;

---

26

BRASIL. Decreto nº 6.207, de 18 de setembro de 2007.

• Art. 9º, I) Ao Secretário-Executivo da Secretaria de Relações Institucionais incumbe: (Redação dada pelo Decreto nº 7.465, de 20011). I – coordenar, consolidar e submeter ao Ministro de Estado o plano de ação global da Secretaria;

---

27

BRASIL. Decreto nº 6.378, de 19 de fevereiro de 2008.

• Art. 5º, III) À Secretaria-Executiva compete: [...] III – submeter ao Ministro de Estado o planejamento da ação global da Secretaria-Geral e a proposta orçamentária, bem como a programação financeira anual da Presidência da República; (Redação dada pelo Decreto nº 7.442, de 2011)

---

28

BRASIL. Decreto nº 7.476, de 10 de maio de 2011.

• Art. 18, I) Ao Secretário-Executivo incumbe: I – coordenar, consolidar e submeter ao Ministro de Estado Chefe o plano de ação global da Secretaria de Aviação Civil;

---

29

BRASIL. Decreto nº 6.120, de 29 de maio de 2007. [REVOGADO]

• Art. 2º) Ao substituto do Advogado-Geral da União incumbe: I – coordenar, consolidar e submeter ao Advogado-Geral da União o plano de ação global da Advocacia-Geral da União e de seus órgãos vinculados;

BRASIL. Decreto nº 7.392, de 13 de dezembro de 2010.

• Art. 4º) Ao Departamento de Gestão Estratégica compete: [...] III – coordenar o desenvolvimento das atividades voltadas para o planejamento estratégico, gerencial e de avaliação do desempenho institucional da Advocacia-Geral da União;

• Art. 37) Ao Secretário-Geral de Consultoria compete: [...] IV – auxiliar o Advogado-Geral da União na definição de diretrizes e na implementação das ações da área de competência da Advocacia-Geral da União; e

---

30

BRASIL. Decreto nº 5.683, de 24 de janeiro de 2006.

• Art. 6º) À Secretaria-Executiva compete: [...] III – assistir ao Ministro de Estado na coordenação dos processos de planejamento estratégico, organização e avaliação institucional;

---

31

BRASIL. Decreto nº 7.411, de 29 de dezembro de 2010.

• Art. 4º) À Secretaria-Executiva compete: I – assessorar e assistir o Ministro de Estado no âmbito de sua competência; II – exercer a supervisão e coordenação das atividades dos órgãos integrantes da estrutura do Gabinete de Segurança Institucional; [...] VIII – gerenciar, em articulação com a Secretaria de Administração da Casa Civil da Presidência da República, os assuntos de desenvolvimento organizacional e de administração geral do Gabinete de Segurança Institucional;

• Art. 19) Ao Secretário-Executivo incumbe: I – exercer as atividades de supervisão e coordenação das unidades integrantes da estrutura do Gabinete de Segurança Institucional; II – supervisionar a execução dos projetos e atividades do Gabinete de Segurança Institucional;

• Art. 20) Ao Assessor-Chefe, aos Secretários e aos Diretores incumbe planejar, dirigir, coordenar, orientar, acompanhar e avaliar a execução das atividades das unidades que integram suas respectivas áreas e exercer outras atribuições que lhes forem cometidas.

• Art. 21) Ao Chefe de Gabinete e aos demais dirigentes incumbe planejar, coordenar e orientar a execução das atividades das respectivas unidades e exercer outras atribuições que lhes forem cometidas.

---

**32****BRASIL. Decreto nº 6.835, de 30 de abril de 2009.**

• Art. 4º) À Secretaria-Executiva compete: [...] II – auxiliar o Ministro de Estado na definição das diretrizes e na implementação das ações da área de competência do Ministério;

---

**33****BRASIL. Decreto nº 7.364, de 23 de novembro de 2010.**

• Art. 2º) O Ministério da Defesa tem a seguinte estrutura organizacional: I – órgãos de assistência direta e imediata ao Ministro de Estado da Defesa: a) Gabinete; b) Assessoria de Planejamento Institucional; [...]

• Art. 4º) À Assessoria de Planejamento Institucional compete: [...] II – conduzir e coordenar o processo de elaboração e revisão do planejamento estratégico do Ministério da Defesa, que culmina com as decisões de direcionamento da instituição frente aos riscos, desafios e responsabilidades definidos a partir dos cenários de futuro elaborados; III – elaborar processo contínuo e sistemático de conhecimento do cenário futuro, com o objetivo de alimentar o processo decisório de alto nível do Ministério da Defesa; [...] VI – elaborar o cronograma anual de revisão do planejamento e coordenar a sua execução; e

---

**34****BRASIL. Decreto nº 6.972, de 29 de setembro de 2009.**

• Art. 5º) À Secretaria-Executiva compete: I – assistir o Ministro de Estado na definição de diretrizes e na supervisão e coordenação das atividades das Secretarias integrantes da estrutura do Ministério; [...] III – coordenar, supervisionar, acompanhar e avaliar os planos, programas e ações do Ministério; [...]

• Art. 8º) À Secretaria de Planejamento e Ordenamento da Aquicultura compete: [...] X – subsidiar a Assessoria de Ação Estratégica e Articulação Institucional com informações específicas necessárias para a operacionalização do planejamento estratégico do Ministério; e

---

**35****BRASIL. Decreto nº 7.462, de 19 de abril de 2011.**

• Art. 4º) À Secretaria-Executiva compete: I – assistir ao Ministro de Estado na supervisão e coordenação das atividades das Secretarias integrantes da estrutura do Ministério e das entidades a ele vinculadas; II – supervisionar e coordenar as atividades de organização e modernização administrativa, bem como as relacionadas com os sistemas federais de planejamento e de orçamento, de contabilidade, de administração financeira, de administração dos recursos de informação e informática, de pessoal civil e de serviços gerais, no âmbito do Ministério; III – auxiliar o Ministro de Estado na definição de diretrizes e na implementação das ações da área de competência do Ministério; IV – supervisionar e coordenar as atividades, formular e propor políticas, diretrizes, objetivos e metas relativas às comunicações;

---

**36****BRASIL. Decreto nº 6.377, de 19 de fevereiro de 2008.**

• Art. 4º) À Subchefia-Executiva compete: [...] III – planejar, supervisionar e coordenar das atividades das unidades da Secretaria de Comunicação Social, auxiliando na definição de diretrizes e na implementação das ações da área de sua competência;

• Art. 23) Ao Subchefe-Executivo incumbe: I – planejar, dirigir, orientar, supervisionar, avaliar e controlar a execução dos projetos e atividades das unidades da Subchefia-Executiva; [...]

---

37

BRASIL. Decreto nº 7.043, de 22 de dezembro de 2009.

• Art. 4º) À Subsecretaria de Planejamento e Gestão Interna compete: [...] IX – planejar, acompanhar e executar as atividades orçamentárias e financeiras e a adequada aplicação dos recursos administrados pela Secretaria Especial;

• Art. 8º) Aos Subsecretários incumbe planejar, dirigir, coordenar, orientar, acompanhar e avaliar a execução das atividades de suas unidades e exercer outras atribuições que lhes forem cometidas.

• Art. 9º) Ao Chefe de Gabinete do Secretário Especial e aos demais dirigentes incumbe planejar, coordenar e orientar a execução das atividades das respectivas unidades e exercer outras atribuições que lhes forem cometidas.

---

38

BRASIL. Decreto nº 7.304, de 22 de setembro de 2010.

• Art. 9º) À Secretaria-Geral das Relações Exteriores compete: I – assessorar o Ministro de Estado na direção e execução da política exterior do Brasil, na supervisão dos serviços diplomático e consular e na gestão dos demais negócios afetos ao Ministério; II – orientar, coordenar e supervisionar os órgãos do Ministério no exterior; III – dirigir, orientar, coordenar e supervisionar a atuação das unidades que compõem a Secretaria de Estado das Relações Exteriores, exceto a dos órgãos de assistência direta e imediata ao Ministro de Estado; e IV – realizar outras atividades determinadas pelo Ministro de Estado.

• Art. 65) Ao Secretário-Geral das Relações Exteriores incumbe: I – assistir ao Ministro de Estado na direção e execução da política exterior brasileira; II – supervisionar os serviços diplomático e consular; III – coordenar, supervisionar e avaliar a execução dos projetos e atividades do Ministério;

---

39

BRASIL. Decreto nº 7.256, de 4 de agosto de 2010.

• Art. 23) Ao Secretário-Executivo incumbe supervisionar, coordenar, dirigir, orientar, monitorar, acompanhar e avaliar o planejamento e a execução de todos os órgãos específicos singulares e exercer outras atribuições que lhe forem cometidas.

• Art. 24) Aos Secretários incumbe planejar, dirigir, coordenar, orientar, acompanhar e avaliar a execução das atividades de suas unidades e exercer outras atribuições que lhes forem cometidas.

• Art. 25) Ao Chefe de Gabinete do Ministro de Estado e aos demais dirigentes incumbe planejar, coordenar e orientar a execução das atividades das respectivas unidades e exercer outras atribuições que lhes forem cometidas.

---

40

BRASIL. Decreto nº 7.261, de 12 de agosto de 2010.

• Art. 9º) Ao Secretário-Executivo incumbe supervisionar, coordenar, dirigir, orientar, monitorar, acompanhar e avaliar o planejamento e a execução de todos os órgãos específicos singulares e exercer outras atribuições que lhe forem cometidas.

• Art. 10) Aos Secretários, incumbe planejar, dirigir, coordenar, orientar, acompanhar e avaliar a execução das atividades de suas unidades e exercer outras atribuições que lhes forem cometidas.

• Art. 11) Ao Chefe de Gabinete e aos demais dirigentes incumbe planejar, coordenar e orientar a execução das atividades das respectivas unidades e exercer outras atribuições que lhes forem cometidas.

---

41

BRASIL. Decreto nº 7.262, de 12 de agosto de 2010.

• Art. 15) Ao Secretário-Executivo incumbe supervisionar, coordenar, dirigir, orientar, monitorar, acompanhar e avaliar o planejamento e a execução de todos os órgãos específicos singulares e exercer outras atribuições que lhe forem cometidas.

• Art. 16) Aos Secretários incumbe planejar, dirigir, coordenar, orientar, acompanhar e avaliar a execução das atividades de suas unidades e exercer outras atribuições que lhes forem cometidas.

• Art. 17) Ao Chefe de Gabinete, ao Chefe da Assessoria Jurídica, aos Diretores e aos demais dirigentes incumbe planejar, coordenar e orientar a execução das atividades das respectivas unidades e exercer outras atribuições que lhes forem cometidas.

## VOTO

É com satisfação que trago à apreciação deste Colegiado relatório consolidado das ações do TMS 6/2010, cujo objeto foi avaliar se a gestão e o uso da tecnologia da informação estão de acordo com a legislação e aderentes às boas práticas de governança de TI.

2. O objetivo maior desta fase consiste em agregar os resultados de todas as fiscalizações previstas, de modo a sintetizar os achados e as conclusões sobre a gestão e uso de TI na Administração Pública Federal (APF).

3. O trabalho em questão foi conduzido entre 2010 e 2011, por meio de 21 fiscalizações, abrangendo 315 organizações públicas federais, sendo um levantamento de auditoria; catorze auditorias para avaliação de controles gerais de TI, conduzidas na modalidade “Fiscalização de Orientação Centralizada” (FOC); quatro auditorias em objetos específicos de TI; um monitoramento de deliberações com orientações aos OGS (órgão que têm a responsabilidade por normatizar e fiscalizar o uso e a gestão de TI em seus respectivos segmentos da APF); e uma fiscalização consolidada dos vinte trabalhos anteriores, que se materializaram no relatório ora em apreciação.

4. As questões de auditoria abordaram tanto aspectos operacionais quanto de legalidade, o que fez com que a iniciativa tomasse a forma de uma “auditoria integrada”. O levantamento do perfil foi realizado por meio de trinta questões, subdivididas em 152 itens, organizadas segundo sete (das oito) dimensões do Gespública: liderança, estratégias e planos, cidadãos, sociedade, informações e conhecimento, pessoas e processos (anexo 2, fls. 25v-26v).

5. Cada uma das catorze auditorias que integraram a FOC de avaliação de controles gerais de TI foi realizada por meio das doze questões de auditoria listadas no item 34 e seus subitens da instrução transcrita no Relatório precedente.

6. Neste momento, entendo relevante mencionar que, já em 2007, o TCU realizou duas grandes fiscalizações em TI, uma sobre governança e outra relativa à governança e terceirização. Esses trabalhos deram origem a dois dos mais importantes acórdãos sobre a matéria: o 1.603/2008 e o 2.471/2008, ambos do Plenário.

7. O Acórdão 1.603/2008 constituiu-se no primeiro levantamento para verificar a situação da governança de TI na Administração Pública Federal (APF). A ação foi realizada por meio de uma pesquisa, respondida por 255 unidades jurisdicionadas ao TCU.

8. Os principais resultados da pesquisa mostraram uma situação preocupante da governança de TI federal. Em 2007, entre as organizações que responderam ao levantamento, pelo menos 57% não tinham carreira específica para TI; 59% não tinham planejamento estratégico em vigor; 64% não tinham política de segurança da informação; 75% não tinham análise de risco de TI; 88% não tinham plano de continuidade de negócios. Como se vê, o primeiro trabalho relevante delineou um panorama desolador.

9. A segunda grande iniciativa adotada em 2007, resultou no Acórdão 2.471/2008, já no âmbito do TMS 6, e expediu diversas recomendações estruturantes sobre o tema governança de TI.

10. Cito, também, por significante, o Acórdão 786/2006-TCU-Plenário, que induziu a criação da conhecida e importante Instrução Normativa 4, da Secretaria de Logística e Tecnologia da Informação do Ministério do Planejamento.

11. Das fiscalizações mencionadas no item 3 deste Voto, informo que apresentei a este colegiado o resultado consolidado do levantamento efetuado pela Sefti, em 2010, para avaliar a governança de tecnologia da informação em 315 órgãos e entidades das administrações direta e indireta dos três poderes da União (Acórdão 2.308/2010 – Plenário).

12. Destaquei, naquela oportunidade, a importância da atuação desta Corte com relação à matéria, eis que, a partir da identificação de pontos vulneráveis, seria possível ao Tribunal, em primeiro lugar, atuar como indutor do aperfeiçoamento da governança de TI no setor público e, em segundo lugar, identificar e disseminar entre as unidades jurisdicionadas os bons exemplos e modelos identificados.

13. Apontei, ainda, as conclusões mais significativas do levantamento, que permitiu constatar, em síntese, que:

- a) mais de 60% das organizações não possui planejamento estratégico de TI;

b) algumas organizações continuam a ter sua TI totalmente controlada por pessoas estranhas a seus quadros de pessoal;

c) são graves os problemas de segurança da informação, já que informações críticas não são protegidas adequadamente;

d) metade das organizações não possui método ou processo para desenvolvimento de softwares e para aquisição de bens e serviços de informática, o que gera riscos de irregularidades em contratações;

e) a atuação sistemática da alta administração com respeito à TI ainda é incipiente;

f) mais da metade das organizações está no estágio inicial de governança de TI, e apenas 5% encontram-se em estágio aprimorado.

14. Apresentei, também, ao Plenário, o monitoramento das determinações e recomendações estruturantes, apreciados por meio do Acórdão 1.145/2011-TCU-Plenário, que permitiu constatar, em linhas gerais, que, graças às medidas estruturantes adotadas, os órgãos superiores lograram instituir um arcabouço normativo incipiente para dar sustentação a um modelo de governança de TI na administração pública federal e que o poder Executivo e o poder Judiciário trilharam caminhos distintos: enquanto o primeiro procurou, primordialmente, estabelecer um modelo de contratações de bens e serviços de TI e criar controles gerais relativos à gestão da segurança da informação, o segundo optou por concentrar esforços no aprimoramento da governança na área de planejamento.

15. As 19 auditorias sobre controles gerais, por sua vez, já foram todas apreciadas por este Plenário, entre novembro de 2010 e setembro de 2011. Em todas aquelas fiscalizações foi constatada a fragilidade da governança de TI federal e a existência de falhas e oportunidades de melhoria bastante similares, o que permitiu comprovar a propriedade do levantamento geral há pouco mencionado.

16. Uma das 4 auditorias específicas, realizada no Departamento Nacional de Infraestrutura de Transportes (Dnit), com o objetivo de avaliar o Sistema de Acompanhamento de Contratos (Siasc) daquela autarquia, especialmente no tocante à integralidade e à confiabilidade das bases de dados do sistema e à sua compatibilidade com as regras de negócios da entidade (TC 010.474/2010-2), também já foi apreciada por meio do Acórdão 2831/2011-TCU-Plenário.

17. No mencionado Acórdão, foram expedidas determinações corretivas e recomendações de natureza estruturante ao Dnit, ante a constatação de que o sistema Siasc, que contém informações de grande materialidade, crítico para o funcionamento da autarquia e para a administração da política viária da União, apresenta graves problemas relacionados à segurança da informação e à desconformidade na implementação de importantes regras de negócios, falhas decorrentes da baixa maturidade tanto da governança de TI, quanto da governança corporativa, tema que será abordado com mais profundidade na sequência deste Voto.

18. Ainda estão pendentes de apreciação duas das auditorias específicas realizadas no Serviço Federal de Processamento de Dados – Serpro, SRF/MF e Secretaria Executiva do Ministério do Planejamento, Orçamento e Gestão (SE/MP) (TC 022.241/2010-8) e Ministério da Ciência e Tecnologia CGTI/MCT (029.120/2010-1), que oportunamente trarei à apreciação deste Plenário. No entanto, as informações e os achados dos referidos processos serão consideradas no resultado da consolidação. O processo TC 029.074/2010-0, que se refere à auditoria realizada na Secretaria Executiva do Ministério da Saúde (SE/MS) e Secretaria de Atenção à Saúde (SAS/MS), já foi apreciado por meio do Acórdão 1137/2012-TCU-2ª Câmara.

19. Como resultado da avaliação empreendida, tenho por relevante destacar os principais pontos relativos a cada uma das questões de auditoria:

19.1. processo de planejamento estratégico institucional: foi constatado que mais da metade dos auditados não possuem planos de negócios de longo prazo. À exceção do Ministério da Saúde, os demais auditados tinham planos incompletos e apresentavam outras falhas decorrentes da ausência da totalidade das características da Gespública (item 74 do relatório);

19.2. processo de planejamento estratégico de TI: foi constatado que nove dos catorze auditados não possuem os planos em questão, enquanto os demais auditados tinham planos incompletos ou apresentavam outras falhas decorrentes da ausência da totalidade das características elencadas no item 91

do Relatório. Tal situação pode ser ainda mais crítica, vez que dois dos órgãos que declararam possuir o processo, ante a ausência de evidências apresentadas às equipes, de fato não o possuem;

19.3. estrutura de TI: foi relatado que em sete auditados o comitê não estava instituído e em outros cinco estava instituído, mas não era atuante. Somente em dois entes identificaram-se comitês atuantes. Ainda há organizações em que as atividades de gestão são exercidas, na prática, por não servidores públicos. A quase totalidade dos auditados não possui avaliação das suas necessidades de pessoal no setor de TI, a despeito do recorrente argumento de que falta pessoal nesses setores. Tal situação pode ser ainda mais significativa, pois houve um auditado que declarou possuir comitê instituído, mas que, ante a ausência de evidências apresentadas pela equipe do TCU, de fato não possui;

19.4. orçamento de TI: restou evidenciado que, em dez dos treze jurisdicionados auditados, foram registradas desconformidades no processo orçamentário. Foi observado ente público sem previsão de orçamento para TI na LOA. Compulsando os dados oferecidos pela SOF/MP no levantamento auditoria (TC 001.484/2010-9), identificaram-se dezenas de órgãos e entidades sem previsão de gastos com TI. Tal constatação é inquietante, ante a notória dependência de TI de todas as organizações;

19.5. processo de software: foi observado que a totalidade dos auditados avaliados tem problemas, sendo que a maioria deles (dez) não possuía processo de software. Assim a conclusão é que, quando contratam serviços de desenvolvimento ou manutenção de software, fazem-no de forma ilegal, em virtude da indefinição do objeto;

19.6. processo de gerenciamento de projetos: observou-se que a definição de uma estrutura para gerenciamento de projetos não é prática dos auditados, ainda que seja razoável supor que todos eles conduzem projetos de tecnologia da informação. Por meio do Acórdão 2.308/2010-TCU-Plenário, disponibilizou-se informação de que pelo menos 69% dos pesquisados não adotam um padrão para gerenciamento de projetos de TI;

19.7. processo de gestão de serviços: no monitoramento realizado por meio do TC 028.772/2010-5 (Acórdão 1.145/2011-TCU-Plenário), identificou-se que os OGS promoveram algum tipo de orientação aos seus jurisdicionados quanto à necessidade de implementar e aperfeiçoar a gestão de níveis de serviço. No entanto, o cenário evidenciado sugere que é oportuna e conveniente atuação mais contundente dos OGS;

19.8. segurança da informação: os dados coletados que culminaram no Acórdão 2.308/2010-TCU-Plenário permitiram sinalizar que a situação da segurança da informação na APF era crítica. Em 2007, já havia o entendimento de que a maior parte das instituições estava exposta a riscos diversos e não mapeados. Hoje, além de a Administração estar à mercê dos mesmos riscos, não está agindo para saná-los com a agilidade que o caso requer. Foi evidenciado nos trabalhos que houve doze situações em que as evidências apresentadas às equipes do TCU não corroboraram as respostas apresentadas às perguntas do perfil GovTI2010 no tema segurança da informação, sugerindo que a situação que foi declarada como muito ruim, pode ser de fato pior;

19.9. processo de capacitação em TI: constatou-se que apenas um auditado planejou nos termos esperados. Por meio do Acórdão 2.308/010-TCU-Plenário, obteve-se a informação de que pelo menos 45% dos pesquisados não têm critério para avaliação e atendimento aos pedidos de capacitação em gestão de TI. Entretanto, as informações obtidas pela equipe deste TCU sugerem que o percentual de entes da APF que não possuem tais critérios pode ser de fato maior;

19.10. processo de contratação de soluções de TI: os resultados sintetizados a partir das verificações *in loco* possibilitaram aferir que a ausência de controles no procedimento de contratação contribui para que o processo da IN - SLTI 4/2008 não seja cumprido ou os estudos técnicos preliminares não sejam realizados. Constatou-se, também, que o descumprimento do processo da IN - SLTI 4/2008 ou a não realização dos estudos técnicos preliminares, além da ausência de controles na gestão das avenças, contribui para desconformidades nas contratações. Sobre o tema, a Sefti destaca que a IN-SLTI/MP 4/2010 (sucessora da IN-SLTI/MP 4/2008), que instituiu processo de contratação de soluções de TI no âmbito do Sisp, se cumprida, tende a mitigar os riscos nas aquisições de TI;

19.11. monitoração do desempenho da gestão TI: restou evidenciado que quase 80% dos auditados não realizam dita avaliação e os três que a realizam, fazem-no de forma esporádica ou somente a posteriori.

20. Constatou-se, ainda, que a auditoria interna, em mais de 70% dos casos, não é utilizada como instrumento de apoio na avaliação que a alta administração deve realizar. O acórdão 2.308/2010-TCU-Plenário concluiu que a maioria das instituições respondentes não estabelece objetivos de TI, não tem indicadores de desempenho para esses objetivos, não avalia o alcance de objetivos e não toma decisões com base nos benefícios de negócios advindos dos sistemas de informações providos pela TI e que a omissão no cumprimento dessa responsabilidade pela alta administração é causa de ineficiência e não efetividade institucional, que devem ser combatidos.

21. Quanto à questão tratada no item 19.11, é de se lembrar que o estabelecimento de políticas de TI é um tipo de atividade de controle de TI a cargo da alta administração, tem-se como corolário que essa alta administração da APF tem pouca cultura no estabelecimento de controles de TI.

22. Os dados analisados por equipe desta Casa revelaram que houve quatro situações em que as evidências apresentadas não corroboram as respostas apresentadas à pergunta do perfil GovTI2010, que pesquisou se a alta administração se responsabiliza pelo estabelecimento e pelo cumprimento das políticas de gestão e uso corporativo de TI, inferindo-se que o percentual de organizações em que a alta administração não se responsabiliza pelas políticas de TI é ainda maior do que 51%.

23. Não há dúvida de que a alta administração da APF é responsável pelas atividades de controle de mais alto nível, como o estabelecimento de políticas e definição de atividades de controle, que devem ser executadas nos diversos níveis da organização. Portanto, mais do que adequado cobrar da alta administração a responsabilidade pelo estabelecimento de estruturas efetivas de controles internos para suas organizações, consistentes em atividades de controle que devem ser executadas pelos gestores nos diversos níveis da organização e que podem ou não estarem acompanhadas da criação de uma unidade organizacional, nos moldes propostos no Relatório de consolidação.

24. Destaco a verificação efetivada em relação ao órgão central do sistema de controle interno do Poder Executivo (CGU). O monitoramento realizado no TC 028.772/20105 registrou que a CGU não considera a fiscalização das aquisições de TI como questão estruturante e de maior relevância e que as auditorias de TI ainda não são regularmente realizadas pelo órgão e, ainda, que a CGU não tem estimulando a realização desse tipo de auditoria nos órgãos e nas entidades da APF.

25. Ante essas informações, concordo com a sugestão da Sefti, de que há oportunidade de melhoria na atuação do órgão central de controle interno do Poder Executivo, ator essencial para aprimoramento do cenário de governança de TI delineado ao longo deste trabalho.

## II

26. Tema importantíssimo desenvolvido no relatório diz respeito aos aspectos legais nas contratações de soluções de TI. Os dados declarados pelos jurisdicionados, no levantamento GovTI2010, acerca de suas licitações e contratações no ano de 2009, evidenciam que, das 6.442 contratações declaradas, 47% (3.031) foram originadas do Sistema de Registro de Preços (SRT), por alguma das formas possíveis, indicando tendência de a APF dar cumprimento à Lei 8.666/1993, art. 15, inciso II.

27. A unidade técnica constatou, no entanto, que dessas 3.031 contratações por SRP, apenas 17% (199) foram realizadas por meio da prática de planejamento conjunto entre diversos entes, como fundamentado no Decreto 3.931/2001, art. 2º, inciso III. Registra, como agravante, o fato de que 30% (902) foram licitadas para criação de atas de registro de preços que não contaram com outras instituições participantes desde o planejamento da contratação.

28. Entendo ser particularmente preocupante essa constatação, considerando-se que bens e serviços de TI dificilmente se enquadrariam nos demais incisos do mencionado Decreto 3.931/2001, pelos quais, em princípio, a criação da ata de registro de preços deve ser fundamentada, a saber:

“Art. 2º Será adotado, preferencialmente, o SRP nas seguintes hipóteses:

- I - quando, pelas características do bem ou serviço, houver necessidade de contratações frequentes;
- II – quando for mais conveniente aquisição de bens com previsão de entrega parceladas ou contratação de serviços necessários à administração para o desempenho de suas funções;

(...)

IV – quando pela natureza do objeto não for possível definir previamente o quantitativo a se demandado pela administração.”

29. Mais preocupante, ainda, é a constatação de que 64% das contratações por SRP foram realizadas por meio de adesões fundamentadas nos art. 8º do Decreto 3.931/2001, prática de adesão tardia (por órgão não participante da licitação pelo SRP), mais conhecida como “carona”.

30. O que se abstrai é que, o que deveria ser exceção virou prática comum. O planejamento conjunto para a criação de ata não vem se realizando.

31. Como bem frisou a unidade técnica, a problemática envolvendo a adesão tardia e ilimitada à atas de registro de preços tem sido preocupação constante desta Corte de Contas, que já se manifestou contrariamente a sua prática irrestrita por meio do Acórdão 1.487/2007-TCU-Plenário, ora em fase de recurso.

32. É de se esclarecer que, naquele decisum houve determinação para que fossem reavaliadas as regras previstas na norma regulamentar, de forma a estabelecer limites para a adesão à Ata de Registro de Preços por outros órgãos e outras entidades.

33. De qualquer forma, reconheço que o planejamento conjunto para a geração de ata de registro de preço atende ao espírito da legislação quando realizada seguindo os procedimentos definidos no Decreto já mencionado, especialmente, no que tange à necessidade de que haja planejamento. Nesse aspecto, além de dar cumprimento ao princípio constitucional da eficiência, com certeza atenderá, também, ao princípio da legalidade, tornando-se prática de grande vantajosidade para a administração, conforme pode ser constatado no exemplo apresentados no Relatório de consolidação (item 244).

34. Entretanto, é certo que a situação se torna muito preocupante se forem consideradas as adesões a atas com indícios de graves irregularidades, como os casos também mencionados no Relatório precedente (itens 246/ 250).

35. A possibilidade de fraude é fator que não pode ser afastado nas contratações de grande vulto. Não estou defendendo a presunção de má-fé na conduta do gestor que defende a adesão à ata de registro ou mesmo da empresa contratada. Entretanto, não é adequado ter por razoáveis atitudes como as mencionadas no item 248 do Relatório, a exemplo da não declaração da fundamentação legal que sustenta o motivo da criação da ata; da não realização do planejamento da contratação, tanto na criação da ata quanto na adesão; da não fixação dos quantitativos máximos que serão adquiridos por meio de ata; da não demonstração da vantajosidade em aderir à ata; e da adesão à ata de registro de preços oriunda de licitação com critérios e condições aplicáveis ao ente que registrou a ata.

36. A adesão tardia (carona), que deveria ser exceção, tornou-se prática comum.

37. Nesse sentido, a Sefti propõe a realização de determinações à Secretaria de Logística e Tecnologia da Informação do Ministério do Planejamento, Orçamento e Gestão (SLTI/MP), com objetivo de mitigar, já no curto prazo, a continuidade de ocorrências de desconformidades, nos termos constantes do item 251 do Relatório (fls. 435 do v. 2).

38. Sugeriu, ainda, que determinação análoga deve ser proposta ao Departamento de Coordenação e Governança das Estatais (Dest), ao CNJ e ao CNMP.

39. Tendo em vista a natureza e a relevância da matéria em apreciação, com repercussão em toda a administração pública, solicitei a manifestação do Ministério Público junto a este Tribunal, quanto à matéria de direito em relação ao conteúdo e às propostas relacionadas ao título III, subtítulo III.1, do Relatório de Auditoria.

40. Em resposta, o Parquet elaborou o parecer reproduzido como parte do Relatório precedente, onde, após tecer considerações sobre a matéria, afirma que os elementos colhidos na presente auditoria comprovam os problemas que decorrem da adesão ilimitada à Ata de Registro de Preços, causados, basicamente, pela marcante ausência de planejamento dos órgãos e das entidades da Administração Pública.

41. Defende que o instituto do SRP apresenta grande potencial de proporcionar racionalização administrativa e economia para os cofres públicos, não obstante entender que a prática disseminada em todos os entes da federação, da adesão ilimitada às Atas de Registro de Preços desvirtua o SRP de sua

finalidade principal, fundada no planejamento dos órgãos e entidades da Administração Pública, além de afrontar a Constituição Federal e a Lei 8.666/93, trazendo, em seu bojo, uma ampla liberalidade que favorece a prática da fraude, do conluio e da corrupção.

42. Ante todo o exposto, o representante do Ministério Público manifesta-se em conformidade com a análise realizada no título III, subtítulo III.1, do Relatório de Auditoria, bem como com a proposta formulada pela Sefti no item 251.

43. Como se vê, não há divergência nos entendimentos quanto ao fato de o SRP, se utilizado de acordo com as normas legais vigentes, apresenta potencial fantástico de racionalizar as aquisições de bens e serviços pela Administração Pública, podendo trazer significativa economia aos cofres públicos.

44. Entretanto, conforme defende o **Parquet**, essas vantagens não podem ser obtidas à custa do descumprimento da legislação específica de licitações ou dos princípios constitucionais que regem a matéria. Assim, a adesão ilimitada (ou adesão sem regras claras) às atas, conforme pode ser visto nos pareceres, textos doutrinários e exemplos trazidos aos autos, poderia representar clara ofensa ao disposto no art. 37, inciso XXI, da Constituição Federal, que exige que compras e serviços sejam contratados mediante processo de licitação pública que assegure igualdade de condições a todos os concorrentes.

45. Por ser o Tribunal órgão essencialmente de controle, não pode deixar de avaliar, também, a possibilidade de que a sistemática de permitir adesões ilimitadas às Atas de Registro de Preços, por intermédio de caronas, possa constituir-se em incentivo a práticas reprováveis, como fraude ao procedimento licitatório e prática da corrupção, principalmente em licitações destinadas ao fornecimento de grande vulto.

46. Confesso que fiquei perplexo com a informação constante no parecer do MP/TCU, de que até sites foram criados por empresas privadas com objetivo de oferecer auxílio nas compras via adesão a atas válidas de órgãos federais, estaduais e municipais, configurando verdadeira exploração comercial das Atas de Registro de Preços.

47. Nota-se, claramente, que a adesão ilimitada à Ata de Registro de Preços representa um desvirtuamento do SRP, que tem como pressuposto principal o planejamento das aquisições pela Administração Pública, na medida em que propicia a contratação de muito mais itens do que a quantidade efetivamente licitada. Compreendo, também, que é difícil definir um limite razoável para a adesão. Este, para mim, ainda é um ponto árduo e que merece alguma reflexão.

48. Entretanto, as distorções experimentadas, na prática, em relação ao limite máximo de quantitativo passível de contratação com base no registro de preço, é que me levam a concordar com o entendimento da Sefti e do **Parquet** de que é aspecto de fundamental importância para o regular funcionamento do SRP o devido planejamento que deve ser realizado pelo órgão gerenciador e pelos órgãos participantes. Os elementos colhidos na presente auditoria comprovam os problemas que decorrem da adesão ilimitada à Ata de Registro de Preços, causados, basicamente, pela marcante ausência do indigitado planejamento dos órgãos e das entidades da Administração Pública.

49. Devo observar que interpretação proposta pela unidade técnica comporta todos os dispositivos legais e regulamentares, inclusive a adesão tardia (carona) prevista no Decreto 3.931/2001, art. 8º. Além do que nessa interpretação, o participante passa a ser a regra e o “carona”, a exceção, como deve ser em organizações que atentam ao princípio do planejamento.

50. Ante essas considerações, manifesto-me em conformidade com a proposta formulada pela Sefti no item 251 do Relatório precedente que teve anuência do Ministério Público junto a este Tribunal.

51. Ainda sobre o tema contratação pela APF, devo destacar as avenças firmadas entre os entes da administração e o Serviço Federal de Processamento de Dados (Serpro).

52. Auditoria-piloto deste TMS (TC 009.982/2010-8, Acórdão 866/2011-TCU-Plenário) identificou, logo no início dos trabalhos, a dependência que alguns entes da administração poderiam ter em relação à entidade. Essa situação já havia sido detectada em fiscalização realizada por ocasião do TMS 2007 – Terceirização em TI (TC 026.200/2007-3, Acórdão 1.330/2008-TCU-Plenário).

53. No âmbito da fiscalização que gerou o Acórdão 1.793/2011-TCU-Plenário, identificou-se que o Serpro recebera mais de R\$ 1 bilhão oriundos de contratos com órgãos e entidades da APF. Assim,

pelo risco em razão da dependência e pela alta materialidade dos contratos com aquela empresa, incluiu-se no TMS fiscalização específica para avaliar os ditos contratos.

54. Segundo informações constantes do TC 022.241/2010-8, em 2010, o Serpro possuía 236 contratos com a APF, no total de R\$ 5.027.481.735,14, sendo dois deles selecionados para análise: o da Receita Federal do Brasil (RFB) e o do Ministério do Planejamento, Orçamento e Gestão (MP). Em termos de materialidade, a soma do valor desses dois representa mais da metade do valor dos contratos do Serpro (53,5%) e, em termos de abrangência dos serviços, eles contêm praticamente todo o espectro de serviços fornecidos por aquela empresa, além de contemplar serviços que dão suporte a sistemas estratégicos do Governo Federal.

55. Os principais problemas identificados na contratação são oriundos de deficiências no planejamento e estão descritos no item 261 e subitens do Relatório. Já as falhas ou impropriedades observadas na execução contratual estão descritas no item 263 e subitens. Todas as situações afrontam o previsto na Lei 8.666/1993, art. 66, que vincula todos os contratos administrativos da APF, inclusive os feitos com o Serpro.

56. Ao mesmo tempo, o relatório do TC 022.241/2010-8 consigna como bom o modelo do contrato da RFB, bem como eficaz a gestão contratual realizada no âmbito daquele órgão, mesmo que o contrato da RFB tenha complexidade acima da média. Esta constatação evidencia que é possível firmar e gerir contratos com o Serpro seguindo os preceitos legais e de acordo com as boas práticas.

57. Diante dessas constatações, a Sefti propõe que seja expedido determinar à SLTI/MP para que oriente os órgãos e as entidades sob sua jurisdição para solucionar as ocorrências verificadas.

58. Na fiscalização realizada verificaram-se ainda situações em que o serviço prestado pelo Serpro tinha qualidade incompatível com o previsto no contrato, o que foi objeto de medida corretiva por parte da RFB. Relevante a informação, trazida na instrução, de que, quando o Serpro não atende a um nível mínimo de serviço contratado pela RFB (ou qualquer outro ente público), independentemente da glosa no contrato, há impacto nas atividades do órgão contratante, que utiliza seus sistemas de informação para prestar serviços à sociedade. Exemplos foram colacionados ao Relatório.

59. Em termos de gestão de TI, foi ressaltado que o Serpro não integra a estrutura do tomador do serviço, sendo necessário gerir a relação advinda do contrato, importante também que a gestão dos processos de trabalho do contratante deve ser executada por servidores ou empregados integrantes da sua estrutura organizacional, nos termos preconizados pelo Decreto-Lei 200/1967, art. 10, § 7º, não podendo ser delegada a funcionários contratados de terceiros, mesmo que a contratada seja o Serpro.

60. Da mesma forma, a transferência da execução dos serviços de tecnologia da informação ao Serpro não desobriga a contratante da APF a possuir, além da gestão da execução desses serviços, estruturas de governança de TI na organização, diversamente do que foi evidenciado no MP. Nesse sentido, acolho a proposta de expedição de determinação à SLTI/MP, bem como determinação análoga deve ser feita ao Dest/MP, ao CNJ e ao CNMP.

### III

61. Por fim, na Sessão cujo título é “Governança Corporativa como Limite para o Amadurecimento da Governança de TI”, a unidade técnica discorreu, de forma sucinta, como a doutrina indica que a ausência de maturidade em governança corporativa limita a maturidade em governança de TI.

62. As informações foram extraídas do estudo elaborado pela Secretaria Adjunta de Planejamento e Procedimento, Diretoria de Métodos e Procedimentos de Controle. O estudo em questão foi realizado com o objetivo de subsidiar a discussão, no âmbito do Senado Federal, para a elaboração de anteprojeto de proposta legislativa com a finalidade de estabelecer critérios gerais para controles internos na administração pública brasileira.

63. O Trabalho consistiu em identificar como os países pesquisados tratam controles internos em seus ordenamentos jurídicos. Foram pesquisados materiais disponibilizados pelos seguintes países: Canadá, Estados Unidos da América, Chile, Paraguai, Colômbia, Peru e África do Sul.

64. O estudo demonstrou que a obrigatoriedade de implantar, manter e avaliar controle interno já está incorporada no ordenamento jurídico de diversos países pesquisados e, ainda, que esses países

adotam modelos de controle interno convergentes, calcados em gerenciamento de riscos e em estruturas de governança e que esses modelos têm por base os principais documentos relacionados à gestão de risco e controles internos reconhecidos internacionalmente, como o COSO I/II, o padrão AS/NZS 4360 e as diretrizes para as Normas de controle Interno do Setor Público, da Intosai.

65. O entendimento da Sefti sobre a questão foi, em síntese, o seguinte:

i) a norma brasileira de Governança Corporativa de TI (ABNT NBR ISO/IEC 38.500: 2008, p. 3-4) está baseada em normas internacionais de governança corporativa e deixa claro que todos os mecanismos de gerenciamento organizacional estão sujeitos à governança corporativa. Na verdade, há fontes que consideram a governança de TI como sendo parte integrante da governança corporativa;

ii) versão 5 do Cobit (com previsão de lançamento oficial no início do próximo ano), um arcabouço de governança de TI tradicionalmente reconhecido no mundo, já procurou garantir o estabelecimento de uma linguagem comum entre as duas governanças e a consistência desse arcabouço com os padrões de governança corporativa;

iii) a governança de TI exerce grande influência sobre as definições da governança corporativa em virtude das possibilidades que a tecnologia da informação oferece de suporte e alavancagem do negócio. Por outro lado, a construção de um modelo de governança de TI sofre a influência dos princípios gerais da governança corporativa, em especial dos princípios da transparência e da prestação de contas, e a forma como cada organização implementa esses princípios dirige a maneira de construir o modelo de governança de TI;

iv) embora possa até haver interesse da alta administração de uma instituição pública em alcançar um bom nível de governança de TI, isso não será possível até que essa mesma alta administração lance os fundamentos e construa as estruturas de governança corporativa necessários para governar todos os seus recursos críticos, tais como pessoas, finanças, TI etc.;

v) no caso do setor privado, já há evidência de que a adoção de boas práticas de governança corporativa está associada com a obtenção de resultados superiores de desempenho, em termos de retorno sobre o ativo. Considerando que é provável que o mesmo efeito seja passível de ocorrer no setor público, é recomendável orientar a alta administração das instituições públicas federais a adotar as boas práticas de governança corporativa e de TI como forma de alcançar a eficiência constitucionalmente exigida.

66. Informa, na sequência, que o estudo produzido por este Tribunal, já mencionado neste Voto, foi concluído com sugestão de anteprojeto de proposta legislativa para alteração da Lei de Responsabilidade Fiscal, incluindo uma seção tratando “Da gestão de riscos, do Controle Interno e da Governança Corporativa”, o que contribui para que seja positivado no ordenamento jurídico brasileiro boas práticas para a adequada governança corporativa contidas em marcos de referência, como Coso I e II, reconhecidos mundialmente.

67. Sugere que o estudo e a proposta de anteprojeto sejam encaminhados às comissões temáticas pertinentes das casas legislativas (Comissão de Finanças e Tributação da Câmara dos Deputados e Comissão de Assuntos Econômicos do Senado Federal), visto que podem vir a subsidiar proposta legislativa de deputados e senadores capazes de contribuir para uma substancial modernização de nossa legislação, com efeitos diretos na melhoria da governança e gestão pública nas três esferas de governo.

68. Sugere, também, que este estudo seja encaminhado à Câmara de Políticas de Gestão, Desempenho e Competitividade do Conselho de Governo, como subsídios à possível elaboração de normativo tratando de gestão de riscos, do controle interno e da governança corporativa para o poder executivo, com fundamento no art. 2º, II, do Decreto 7.478/2011, e, no mesmo sentido, sugere o encaminhamento do documento ao CNJ e ao CNMP, com propósito análogo.

69. Relevante destacar a informação trazida pela unidade técnica de que as unidades de auditoria interna são atores essenciais à boa governança de TI, e ainda lembrar as deficiências dos sistemas de controles internos (controles internos dos gestores e atuação das unidades de auditoria interna), conforme evidenciado neste TMS.

70. Em razão desses elementos, a Sefti sugere oportunidade para que o TCU contribua para o cumprimento do comando previsto no art. 74 Constituição Federal, promovendo ações de controle no sentido de verificar a eficiência e eficácia dos sistemas de controles internos dos poderes. Essas ações estariam alinhadas com o referencial estratégico do TCU em vigor, que contempla como objetivo estratégico “Contribuir para a melhoria da gestão e do desempenho da Administração Pública”, o qual tem como um de seus indicadores o “índice de governança corporativa dos órgãos da Administração Pública Federal”.

71. Devo consignar que vejo com bastante otimismo o nível dos trabalhos que vêm sendo desenvolvidos pelas unidades especializadas desta Corte de Contas. O estudo referenciado nos itens supra e os elementos trazidos na consolidação ora em apreciação mostram como esta Corte de Contas é capaz, sim, de contribuir para o aperfeiçoamento do arcabouço legislativo na área de controle. O momento é propício, pois a estrutura administrativa está cada vez mais complexa. Os níveis de investimento público estão se intensificando e, ao mesmo tempo, a sociedade clama por uma gestão pública de melhor desempenho. Assim, as estruturas de controle não podem ficar à margem dessas exigências.

72. Como bem frisou o Ministro emérito Ubiratan Aguiar, na apresentação do estudo “Critérios Gerais de Controle Interno na Administração Pública”, a obrigatoriedade legal de implantar, manter e avaliar estruturas de governança, gestão de risco e controles internos na administração pública é de fundamental importância para prover razoável segurança quanto ao cumprimento de suas missões e ao alcance dos objetivos fixados pelo Poder Público, de modo a restabelecer e manter a reputação das instituições e a confiança da sociedade.

73. Assim, entendo adequadas as propostas formuladas pela Sefti. A iniciativa vem ao encontro das ações que este Tribunal tem desempenhando no sentido de compartilhar informações relevantes, trabalhos realizados e em andamento que podem apoiar e direcionar o esforço de amadurecimento da governança de Tecnologia de Informação e Corporativa na Administração Pública Federal, além de alinhar-se aos objetivos estratégicos “Instituir modelo de governança corporativa e gestão estratégica” e “Promover a melhoria da governança no TCU” constantes, respectivamente, da agenda estratégica do Senado Federal e do Plano Estratégico do TCU. Encaminhe-se, portanto, os documentos conforme sugerido.

74. Quanto à ação de controle proposta, depreendo que esta deve ocorrer mediante trabalho de avaliação sistematizada dos sistemas de controles internos dos poderes, motivo pelo qual proponho determinar a Segecex que analise a oportunidade e conveniência de incluir o tema “avaliação da eficiência e eficácia dos sistemas de controles internos dos poderes” como TMS em futuros planos de fiscalizações do TCU.

75. Por fim, não poderia deixar de parabenizar, nesta oportunidade, o corpo técnico desta Casa pela excelência do trabalho realizado, agradecendo, em particular, a valiosa colaboração dos auditores da Sefti, a quem saúdo na pessoa do secretário Cláudio Souza Castello Branco, pela dedicação à tarefa ora trazida ao Colegiado.

76. Com essas considerações, acolho integralmente o encaminhamento proposto pela unidade técnica especializada, e VOTO por que o Tribunal aprove o Acórdão que ora submeto à consideração deste Plenário.

Sala das Sessões, em 23 de maio de 2012.

AROLDO CEDRAZ  
Relator



9

2009

# Critérios Gerais de Controle Interno na Administração Pública

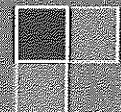
## Um estudo dos modelos e das normas disciplinadoras em diversos países

O estudo explora os modelos de referência em gestão de riscos e controles internos e como os diversos países pesquisados trataram a questão em seus ordenamentos jurídicos. O objetivo é subsidiar discussão, no âmbito do Senado Federal, de anteprojeto de proposta legislativa para definição de critérios gerais de controles internos, gestão de riscos e governança na administração pública brasileira.

Tribunal de Contas da União

Diretoria de Métodos de Procedimentos de Controle

17/07/2009





## SUMÁRIO

I.	APRESENTAÇÃO .....	3
II.	INTRODUÇÃO.....	3
II.1.	METODOLOGIA E LIMITAÇÕES.....	4
III.	CONCEITOS CENTRAIS.....	4
IV.	MODELOS DE REFERÊNCIA PARA CONTROLE INTERNO .....	8
IV.1.	O MODELO DE REFERÊNCIA COSO I.....	8
IV.2.	O MODELO DE REFERÊNCIA COSO II .....	12
IV.2.1.	AMBIENTE INTERNO .....	14
IV.2.2.	FIXAÇÃO DE OBJETIVOS.....	14
IV.2.3.	IDENTIFICAÇÃO DE EVENTOS .....	14
IV.2.4.	AVALIAÇÃO DE RISCOS.....	15
IV.2.5.	RESPOSTA A RISCOS.....	15
IV.2.6.	ATIVIDADES DE CONTROLE .....	16
IV.2.7.	INFORMAÇÃO E COMUNICAÇÃO .....	16
IV.2.8.	MONITORAMENTO.....	17
V.	CONCEITOS DE RISCO E GERENCIAMENTO DE RISCO .....	18
VI.	GOVERNANÇA .....	21
VII.	A REGULAÇÃO DE CONTROLES INTERNOS EM PAÍSES DO MUNDO .....	23
VII.1.	CANADÁ .....	23
VII.2.	ESTADOS UNIDOS DA AMÉRICA .....	24
VII.2.1.	NEW YORK STATE (USA) .....	33
VII.3.	CHILE.....	35
VII.4.	PARAGUAI E COLÔMBIA.....	36
VII.5.	PERU .....	41
VII.6.	ÁFRICA DO SUL .....	42
VIII.	A REGULAÇÃO DE CONTROLES INTERNOS NO BRASIL.....	44
IX.	CONCLUSÃO E PROPOSTA DE ENCAMINHAMENTO.....	53
X.	ANEXO - ANTEPROJETO DE PROPOSTA LEGISLATIVA.....	56
	REFERÊNCIAS .....	64



## CRITÉRIOS GERAIS DE CONTROLES INTERNOS NA ADMINISTRAÇÃO PÚBLICA

### UM ESTUDO DAS NORMAS DISCIPLINADORAS EM DIVERSOS PAÍSES

#### I. APRESENTAÇÃO

O Senador Renato Casagrande, por meio do ofício 166/2008 – GSRENATOC, de 27 de agosto de 2008, solicitou ao Presidente do Tribunal de Contas da União (TCU) que fosse designado técnico dessa Corte para, em conjunto com a Consultoria de Orçamento do Senado Federal, discutirem sobre **anteprojeto de proposta legislativa para definição dos critérios gerais de controles internos na Administração Pública.** (grifos nossos).

O Presidente do Tribunal, por meio do aviso 978-GP/TCU, de 9 de setembro de 2008, atendeu a solicitação do Exmo. Senador, designando o servidor Antonio Alves de Carvalho Neto, titular da atual Diretoria de Métodos e Procedimentos de Controle, para a missão.

#### II. INTRODUÇÃO

O presente estudo tem por objetivo subsidiar a discussão para elaboração de anteprojeto de proposta legislativa com a finalidade de estabelecer critérios gerais para controles internos na administração pública brasileira.

O trabalho consistiu em identificar como os países pesquisados trataram controles internos em seus ordenamentos jurídicos. Foram pesquisados os seguintes países, em função de terem disponibilizado o material correspondente na Internet ou fornecido diretamente:

Continente	País
América do Norte	Canadá
América do Sul	Estados Unidos e neste o estado de Nova York Chile Paraguai Colômbia Peru
África	África do Sul

Procuramos identificar na legislação e demais normas de cada país como o tema *controles internos* foi tratado. Foram analisados os aspectos relativos à obrigatoriedade legal de os órgãos e entidades do setor público implantarem, manterem e avaliarem sistemas de controles internos, a responsabilidade por estas ações e, ainda, a adoção ou não de modelos de referência.



## II.1. METODOLOGIA E LIMITAÇÕES

Procuramos analisar, além da natureza e hierarquia das normas disciplinadoras, se há obrigatoriedade legal e definição de responsabilidades quanto à implantação, manutenção e avaliação de controles internos pelos órgãos e entidades da administração pública, ou se é apenas uma boa prática recomendada pelas EFS. Procurou-se também identificar se tais normas incorporaram ou não, com adaptações ou não, modelos de referência reconhecidos mundialmente.

A pesquisa para a realização do presente trabalho foi efetuada, basicamente, nos sítios da internet das Entidades de Fiscalização Superior (EFS), nas páginas oficiais dos governos e em documentos e modelos disponibilizados pelas EFS da Colômbia, Paraguai e Peru, em função disso alguns países que também são referência no assunto, a exemplo do Reino Unido, deixaram de ser incluídos no estudo por não terem disponibilizado o material em seus sítios.

## III. CONCEITOS CENTRAIS

**Controle**, genericamente falando, é uma ação tomada com o propósito de certificar-se de que algo se cumpra de acordo com o que foi planejado. **Objetivo** é o que se deseja alcançar tal como definido no planejamento. **Risco** é qualquer evento que possa impedir ou dificultar o alcance de um objetivo. Controle, portanto, só tem significado e relevância quando é concebido para garantir o cumprimento de um objetivo definido e só faz sentido se houver riscos de que esse objetivo não venha a ser alcançado.

**Controle interno, controles internos e sistema ou estrutura de controle(s) interno(s)** são expressões sinônimas, utilizadas para referir-se ao processo composto pelas regras de estrutura organizacional e pelo conjunto de políticas e procedimentos adotados por uma organização para a vigilância, fiscalização e verificação, que permite prever, observar, dirigir ou governar os eventos que possam impactar na consecução de seus objetivos. É, pois, um processo organizacional de responsabilidade da própria gestão, adotado com o intuito de assegurar uma razoável margem de garantia de que os objetivos da organização sejam atingidos.

Cabe destacar, aqui, o registro de Wallace (1991, p.51 apud ANTUNES, 1998, p.54) para o fato de o Instituto Americano de Auditores Independentes (*American Institute of Certified Public Accounts - AICPA*), na edição da norma de auditoria SAS 55 – Consideração da Estrutura de Controle Interno nas Auditorias de Demonstrações Financeiras, de 1988, ter introduzido um novo conjunto de terminologias para a área de controle. Dentre outros, os termos substituídos foram:



Terminologia antiga

**Sistema de Controle Interno**

A nova terminologia, segundo Antunes (1998, p.54), amplia o seu conteúdo, porque como “estrutura” a SAS 55 incorpora o *ambiente de controle*, o *sistema de contabilidade* e os *procedimentos de controle*, além de introduzir o conceito de *risco de controle*. Contudo, cumpre-nos assinalar, a literatura técnica sobre o assunto continua a utilizar fartamente a expressão sistema de controle(s) interno(s) ou simplesmente controle(s) interno(s) para se referir à estrutura de controle interno ou ao controle interno aplicado a uma organização. Neste trabalho, essas expressões são usadas como sinônimas.

Alerte-se que o controle interno, da própria entidade, objeto do presente estudo, não deve ser confundido com o sistema de controle interno a que se refere o artigo 74, da Constituição Federal de 1988 (CF/88). Com efeito, as disposições constitucionais trouxeram uma aparente confusão no que diz respeito à terminologia da área de controles, o que tem levado a esforços para estabelecimento de conceitos, inclusive em textos legais, como os citados por Araújo (2006, p.2), a seguir, após admitir que “não obstante tipificar as finalidades do sistema de controle interno, o constituinte não apresentou – e não deveria fazê-lo – o **conceito** dessa importante atividade para a consecução dos resultados de uma gestão.”

No âmbito de algumas unidades do sistema federativo brasileiro ocorreram felizes tentativas de, por meio de legislação ordinária, apresentar conceitos do sistema de controle interno como, por exemplo, o Decreto n.º 14.271, de 21 de agosto de 2003, da Prefeitura Municipal de Porto Alegre:

Art. 3º Para fins deste Decreto considera-se:

I – Controle Interno: conjunto de métodos e processos adotados com a finalidade de comprovar atos e fatos, impedir erros e fraudes e otimizar a eficiência da Administração.

II – Sistema de Controle Interno: conjunto das atividades de controle exercidas pelas diversas unidades técnicas da Administração, organizadas e articuladas a partir de uma unidade central de coordenação.

III – Auditoria: atividade de controle, realizada consoante normas e procedimentos de auditoria, que comprehende o exame detalhado, total, parcial ou pontual, dos atos administrativos e fatos contábeis com a finalidade de verificar se as operações foram realizadas de maneira apropriada e registradas de acordo com o aparato legal.

Nova terminologia

**Estrutura de Controle Interno**



O Tribunal de Contas dos Municípios da Bahia, na Resolução n.º 1.120, que dispõe sobre a criação, implantação e manutenção do sistema de controle interno no âmbito dos poderes municipais do Estado, considerando-o como “peça fundamental para a realização de gestões responsáveis e transparentes”, dispôs que o sistema de controle interno municipal representa:

O conjunto de normas, regras, princípios, planos, métodos e procedimentos que, coordenados entre si, têm por objetivo efetivar a avaliação da gestão pública e o acompanhamento dos programas e políticas públicas, bem como evidenciando sua legalidade e razoabilidade, avaliar os seus resultados no que concerne à economia, eficiência e eficácia da gestão orçamentária, financeira, patrimonial e operacional dos órgãos e entidades municipais.

Vieira (2005, p.2), ao tentar esclarecer a confusão que se faz entre o sistema de controle interno da CF/88 e o controle interno da própria entidade, explica que uma correta compreensão do que seja o “sistema de controle interno” exige o entendimento do que seja *sistema*, assim como do que seja *controle interno*, e a consequência deste controle organizado na forma de sistema pela Constituição Federal de 1988:

**Definição de Sistema:**

Conjunto de partes coordenadas (articuladas entre si) com vistas à consecução de objetivos bem determinados.

**Definição de Controle Interno:**

Conjunto de recursos, métodos e processos, adotados pelas próprias gerências do setor público, com vista a impedir o ERRO, a FRAUDE e a INEFICIÊNCIA.

Com as definições transcritas, Sistema de Controle Interno significa:

Conjunto de unidades técnicas articuladas a partir de um órgão central de coordenação, orientadas para o desempenho das atribuições de controle interno indicados na Constituição e normatizados em cada nível de governo.

Desse modo, convém ter claro que o papel do sistema de controle interno de Poder, previsto no art. 74, da CF/88, não se confunde, e nem substitui, o sistema de controle interno de cada organização pública, em particular. Esse último, como se verá mais adiante, também não é sinônimo de auditoria interna.

A **unidade de controle interno**, quando existente na organização, é parte da gestão e do sistema ou da estrutura de controle interno da própria entidade. Tem o papel de assessorar os



gestores, com seu conhecimento especializado, na definição de estratégias para gerenciamento de riscos, na identificação e avaliação destes e na definição, implantação e no monitoramento de controles internos adequados para mitigá-los.

A **auditoria interna**, que não deve ser confundida com controle interno ou com unidade de ou do controle interno, é um controle da própria gestão que tem por atribuição medir e avaliar a eficiência e eficácia de outros controles. Importa destacar que não cabe à auditoria interna estabelecer estratégias para gerenciamento de riscos ou controles internos para mitigá-los, pois estas são atividades próprias dos gestores. Cabe-lhe avaliar a qualidade desses processos. A auditoria interna de um órgão ou entidade do Poder Executivo Federal integra, por força do que dispõe o decreto 3.591/2000, o sistema de controle interno desse Poder, mas não se confunde, ressalte-se mais uma vez, com o controle interno da própria entidade.

Embora as habilidades dessas duas áreas sejam próximas, suas funções fazem parte de elementos distintos do sistema de controle interno da entidade. Comparando responsabilidades: a auditoria interna não implanta controles, mas a unidade de controle interno pode implantar; a auditoria interna faz trabalhos periódicos com metodologia específica, a unidade de controle interno atua no dia-a-dia, no monitoramento contínuo e na autoavaliação de controles internos; auditoria interna é uma atividade de avaliação independente, voltada para o exame e avaliação da adequação, eficiência e eficácia do sistema de controle interno, é parte desse sistema, mas não integra a estrutura de linha da organização e sim o seu staff; a unidade de controle interno também é parte do sistema de controle interno, mas é um elemento da gestão, faz parte da estrutura de linha da organização, com atribuições ligadas ao gerenciamento de riscos e controles.

O sistema de controle interno da CF/88 é um sistema orgânico, constituído pelas várias unidades técnicas que atuam de forma integrada e sob a orientação normativa e supervisão técnica de um órgão central, sem prejuízo da subordinação ao órgão ou à entidade em cuja estrutura administrativa a unidade esteja integrada. Desse modo, a bem da clareza e de consistência técnica, não é correto se referir à auditoria interna como *unidade de ou do controle interno*, embora ela integre o “sistema de controle interno” do Poder ao qual está vinculada. Também não é correto se referir de tal modo em relação às unidades da Controladoria Geral da União (CGU), principalmente à Secretaria Federal de Controle (SFC). A SFC constitui, por sua posição na estrutura organizacional do Governo Federal, auditoria interna em relação ao Poder Executivo, e externa em relação aos órgãos e entidades por ela auditados dentro desse mesmo Poder.



## IV. MODELOS DE REFERÊNCIA PARA CONTROLE INTERNO

Chamaremos aqui de “modelos de referência” o que também é conhecido mundialmente como padrões, estruturas conceituais ou *frameworks* de controle interno. De início, cumpre-nos destacar que a evolução desses modelos tem encampado fortemente o gerenciamento de riscos como esteio para seus desenvolvimentos. Isso se justifica porque a razão de ser dos controles é mitigar a probabilidade ou o impacto da materialização de um risco em relação a um objetivo fixado. É para mitigar riscos que são estabelecidos controles.

Desse modo, a atenção volta-se primeiramente para identificação dos riscos que possam impactar os objetivos da organização e para avaliação da forma como os gestores atuam para minimizar esses riscos, por meio de controles internos e de outras respostas. Evolui-se, assim, da gestão centrada em controles funcionais para o desenvolvimento de uma cultura de risco, na qual todos os funcionários tornam-se responsáveis pela gestão de risco e adquirem consciência dos objetivos do controle. Essa mudança de paradigma foi adotada, inclusive, pela Organização Internacional de Entidades Fiscalizadoras Superiores (Intosai), ao preconizar, como se verá mais adiante, padrões de estruturas e processos de controle interno calcados no gerenciamento de riscos e em modelos de governança corporativa.

### IV.1. O MODELO DE REFERÊNCIA COSO I

Em 1985, foi criada, nos Estados Unidos, em uma iniciativa independente, a *National Commission on Fraudulent Financial Reporting* (Comissão Nacional sobre Fraudes em Relatórios Financeiros), também conhecida como *Treadway Commission*, composta por representantes das principais associações de classe ligadas à questão, para estudar as causas da ocorrência de fraudes em relatórios financeiros/contábeis e fazer recomendações para a redução de sua incidência. A *Treadway Commission* emitiu seu relatório enfatizando ambiente de controle, códigos de conduta e comitês de auditoria competentes e compromissados, e conclamando as organizações patrocinadoras a integrar os diversos conceitos de controle interno e a desenvolver um referencial comum. Criou-se o *Committee Of Sponsoring Organizations of the Treadway Commission* - COSO (Comitê das Organizações Patrocinadoras).

O COSO publicou critérios práticos, amplamente aceitos, para o estabelecimento de controles internos e para avaliação de sua efetividade. O modelo apresentado em julho de 1992, denominado *Internal Control – Integrated Framework*, atualmente conhecido como **COSO I**,



mudou o conceito tradicional de "controles internos" e chamou a atenção para o fato de que eles tinham de fornecer proteção contra riscos.

O modelo, ao definir **risco como a possibilidade que um evento ocorra e afete de modo adverso o alcance dos objetivos da entidade**, introduziu a noção de que controles internos devem ser ferramentas de gestão e monitoração de riscos em relação ao alcance de objetivos e não mais devem ser dirigidos apenas para riscos de origem financeira ou vinculados a resultados escriturais. O papel do controle interno foi, assim, ampliado e reconhecido como um instrumento de gerenciamento de riscos indispensável à governança corporativa.

Após a publicação do COSO I, vários organizações internacionais revisaram suas normas para incorporar o conceito de controle interno sintetizado pelo modelo, segundo o qual:

Controle Interno é um processo realizado pela diretoria, por todos os níveis de gerência e por outras pessoas da entidade, projetado para fornecer segurança razoável quanto à consecução de objetivos nas seguintes categorias: a) eficácia e eficiência das operações; b) confiabilidade de relatórios financeiros; c) cumprimento de leis e regulamentações aplicáveis. (COSO 1992, p. 1, tradução nossa).

A AICPA emitiu a norma de auditoria SAS 78, substituindo a definição de controle interno da SAS 55 pela definição de controle interno dada pelo COSO e incorporando os componentes e demais conceitos da estrutura de controles internos. Isso fez com que o modelo se tornasse um paradigma no mercado, pois os auditores independentes passaram a utilizá-lo como padrão para revisão do controle interno em seus trabalhos de auditoria.

A Federação Internacional de Contadores (*International Federation of Accountants-IFAC*), que emite as *International Standards on Auditing - ISA* (Normas Internacionais de Auditoria), também incorporou todos os elementos introduzidos pelo COSO na norma denominada *Matter 400 – Risk Assessments and Internal Control* (Avaliações de Risco e Controle Interno). O Instituto Internacional de Auditores Internos (*Institute of Internal Auditors-IIA*), pela definição ampla que vem adotando para controles internos, denota sua adesão aos conceitos introduzidos pelo COSO.

O Comitê de Basileia, em 1998, publicou o documento denominado *Framework for Internal Control Systems in Banking Organizations*, no qual os treze princípios constantes do documento enfatizam os cinco componentes do modelo COSO I.



O modelo COSO I tornou-se referência mundial, pelo fato de:

1. uniformizar definições de controle interno;
2. definir componentes, objetivos e objetos do controle interno em um modelo integrado;
3. delinear papéis e responsabilidades da administração;
4. estabelecer padrões para implementação e validação;
5. criar um meio para monitorar, avaliar e reportar controles internos.

No que diz respeito a entidades ligadas ao setor público, vale ressaltar que o BID, o Banco Mundial e a Intosai também reconheceram a adotaram o modelo COSO. O órgão que auxilia o parlamento norte-americano no exercício do controle externo, *U.S. Government Accountability Office* (GAO), também revisou seus documentos para incorporar o modelo COSO. O Tribunal de Contas da União, como membro da Intosai, também reconhece e utiliza o modelo como base para as suas avaliações de controle interno no setor público.

Segundo Borges (apud DAVIS, BLASCHEK, 2006, p.11) as administrações públicas de países do chamado primeiro mundo, detentores dos níveis mais baixos de fraude e mais altos de pesquisa em gestão pública, seguiram a tendência, desenvolvendo e utilizando seus próprios padrões de estrutura de controles internos com esse papel ampliado. Assim, modelos de controles internos utilizando o gerenciamento de riscos em sua base conceitual, tal qual o COSO, passaram a ser desenvolvidos e utilizados por diversos países, como o *Cadbury* no Reino Unido, o *CoCo* no Canadá, o *Standard AZ/NZS 4360-1999* na Austrália/Nova Zelândia e o *King Report* na África do Sul, e têm sido um enorme marco no progresso da auditoria interna e governança nesses países. (McNAMEE e SELIM, 1999, p.35 apud DAVIS, BLASCHEK, 2006, p.11).

A Intosai vem, nos anos recentes, defendendo padrões de estruturas e processos de controle interno calcados no gerenciamento de riscos e em modelos de governança corporativa. Uma evidência disso foi a atualização, em 2004, de suas Diretrizes para Padrões de Controles internos do Setor Público, adotando o modelo COSO I (INTOSAI, 2004), novamente atualizadas, em 2007, para incorporação do modelo COSO II, tratado a seguir (INTOSAI, 2007). Diamond (2002, p.35, apud DAVIS, BLASCHEK, 2006, p.11) destaca que essa entidade estabeleceu um paradigma mais proativo para os controles internos e o papel das auditorias internas governamentais. A auditoria interna, nesse paradigma, passou a exercer um papel mais voltado para a avaliação mais abrangente dos controles internos, com mais ênfase em controles gerenciais e gerenciamento de riscos, deixando de lado a função de mero avaliador da conformidade legal das despesas públicas.



Além dos modelos já mencionados, há outros específicos para a área de tecnologia da informação (TI), como o *Control Objectives for Information and related Technology* (COBIT), um guia formulado como *framework* pela *Information Systems Audit and Control Association* (ISACA) incluindo sumário executivo, controle de objetivos, mapas de auditoria, ferramentas para a sua implementação e, principalmente, um guia com técnicas de gerenciamento de riscos e governança na área de TI. Na mesma área, há, ainda, o modelo denominado *Information Technology Infrastructure Library* (ITIL), mantido pelo órgão britânico o *Office for Government Commerce* (OGC), um grande aparato de “melhores práticas” utilizadas pelos gestores de TI com o objetivo fazer com que a TI foque no negócio da organização e para que entregue os seus serviços aos seus clientes da melhor maneira possível e a um custo justificável.

Há, ainda, modelos e regulamentações específicas para setores e segmentos do mercado, como os Acordos de Basileia I, de 1988, e II, de 2001, elaborados no âmbito do *Bank for International Settlements* (BIS), cujo objetivo, ao final, é assegurar a solidez e a estabilidade do sistema financeiro por meio de controles de riscos, aliando atuação da supervisão bancária e maior transparência como formas eficientes para evitar o risco sistêmico.

Para o mercado de capitais, cabe mencionar a lei *Sarbanes-Oxley* (SOX), promulgada nos Estados Unidos, em 30/7/2002, na esteira de diversos escândalos corporativos, com o intuito de restabelecer a confiança da sociedade nas empresas de capital aberto. Considerada uma das mais rigorosas regulamentações a tratar de controles internos, elaboração de relatórios financeiros e divulgações. As seções 302 e 404, dessa lei, têm sido o foco das atenções por serem as que mais dizem respeito ao sistema de controles internos e às boas práticas de governança corporativa. A seção 302, “*Corporate Responsibility for Financial Reports*” (Responsabilidade Corporativa por Relatórios Financeiros), também conhecida por “certificações”, exige que o principal executivo e o diretor financeiro assumam a responsabilidade pelas informações divulgadas nos relatórios financeiros, declarando, pessoalmente, que executaram a avaliação do desenho e da eficácia dos controles internos. A seção 404, intitulada “*Management Assessment of Internal Control*” (Avaliação Gerencial do Controle Interno) prescreve que a alta administração da companhia é responsável pela adequação dos controles internos e exige que diretores (executivos e financeiro) avaliem e atestem, periodicamente, a sua eficácia, além de exigir a elaboração, por auditoria independente, de relatório anual sobre sua efetividade. A referência generalizadamente adotada pelas companhias para atendimento às exigências da SOX, em matéria de controles internos, é o modelo COSO.



## IV.2. O MODELO DE REFERÊNCIA COSO II

O prefácio da edição brasileira desse modelo afirma que o COSO I tornou-se referência para ajudar empresas e outras organizações a avaliar e aperfeiçoar seus sistemas de controle interno, sendo que essa estrutura foi incorporada em políticas, normas e regulamentos adotados por milhares de organizações para controlar melhor suas atividades visando ao cumprimento dos objetivos estabelecidos. No entanto, a intensificação da preocupação com riscos – fruto de uma série de escândalos e quebras de negócios de grande repercussão – fez com que o COSO encomendasse o desenvolvimento de uma estratégia de fácil utilização pelas organizações para avaliar e melhorar o próprio gerenciamento de riscos. O resultado foi a publicação, em 2004, do modelo *Enterprise Risk Management – Integrated Framework* (Gerenciamento de Riscos Corporativos – Estrutura Integrada), também conhecida como COSO ERM ou COSO II.

Essa obra amplia o alcance dos controles internos, oferecendo um enfoque mais vigoroso e extensivo ao tema, agregando técnicas de gerenciamento integrado de riscos, sem abandonar, mas incorporando o COSO I. A nova postura é de prever e prevenir os riscos inerentes ao conjunto de processos da organização que possam impedir ou dificultar o alcance de seus objetivos.

A razão de nos atermos à descrição das características desse modelo é a tendência mundial, de adoção de padrões de controles internos fortemente calcados no gerenciamento de riscos e em modelos de governança corporativa, como, inclusive, recomenda a Intosai.

Embora muitos objetivos sejam específicos a uma determinada organização, o modelo definiu quatro **categorias de objetivos**, comuns a praticamente todas as organizações, os quais devem ser previamente fixados para permitir a identificação e análise dos riscos que poderão impactá-los, formando uma base de conhecimento para definir como esses riscos deverão ser gerenciados. Essas categorias de objetivos são:

- **Estratégico:** relacionado à sobrevivência, continuidade e sustentabilidade. Metas de alto-nível, alinhadas e dando suporte à missão da organização.
- **Operacional:** efetividade e eficiência na utilização dos recursos, mediante operações ordenadas, éticas, econômicas e adequada salvaguarda contra perdas, mau uso ou dano.
- **Comunicação:** confiabilidade da informação produzida e sua disponibilidade para a tomada de decisões e para o cumprimento das obrigações de *accountability*.
- **Conformidade:** aderência às leis e regulamentações aplicáveis à entidade, e às normas, políticas, aos planos e procedimentos da própria organização.

O modelo é representado no formato de uma matriz tridimensional, demonstrando a integração dos elementos que o compõem, conhecido como **CUBO COSO II**



A face superior do cubo apresenta os objetivos que devem ser objeto do gerenciamento de risco; a face frontal representa os componentes do gerenciamento de riscos, ou, o que é necessário fazer para atingir os objetivos; a face lateral representa os níveis da organização objetos da gestão de riscos. Observe-se que a visão integrada dos elementos do modelo demonstra o contexto das ações da direção ao gerenciar os riscos da organização. Pode-se, assim, vislumbrar essa gestão tanto ao nível da entidade como um todo, como para cada parte que a compõe:

- objetivos, riscos e controles da organização como um todo;
- objetivos, riscos e controles de uma divisão, unidade de negócio, departamento ou seção da organização;
- objetivos, riscos e controles de um macroprocesso, processo ou de uma atividade.

A seguir, estão descritos, sucintamente, cada um dos oito componentes do modelo.



#### **IV.2.1. AMBIENTE INTERNO**

O ambiente interno é moldado pela história e cultura da organização e, por sua vez, molda, de maneira explícita ou não, a cultura de riscos da organização e a forma como eles são encarados e gerenciados (tom da organização), influenciando a consciência de controle das pessoas. É a base para todos os outros componentes do sistema, provendo disciplina e estrutura.

Os fatores que compõem o ambiente interno incluem integridade, valores éticos e competência das pessoas, maneira pela qual a gestão delega autoridade e responsabilidades, estrutura de governança e organizacional, o “perfil dos superiores” (ou seja, a filosofia da direção e o estilo gerencial), as políticas e práticas de recursos humanos etc.

Organizações com ambientes de controle efetivos fixam um tom (“tom do topo”) positivo, contratam e mantêm pessoas competentes, formalizam e comunicam políticas e procedimentos de modo claro, adotam integridade e consciência de controle, resultando em valores compartilhados e trabalho em equipe para efetivação de objetivos.

#### **IV.2.2. FIXAÇÃO DE OBJETIVOS**

O modelo requer que todos os níveis da organização tenham objetivos fixados e comunicados (estratégicos, operacionais, comunicação e conformidade), ou seja, ao nível da organização como um todo e para todas suas divisões, processos e atividades, e mais, como eles devem e podem ser atingidos e como mensurar o seu nível de atingimento.

Os objetivos devem ser definidos a priori para que seja possível identificar os riscos a eles associados. A explicitação de objetivos, alinhados à missão e à visão da entidade, é necessária para permitir a identificação de eventos que potencialmente impeçam sua consecução. Definir os objetivos é, assim, uma pré-condição para identificação dos eventos de risco e para avaliação e definição de estratégias para gerenciá-los (resposta a riscos).

#### **IV.2.3. IDENTIFICAÇÃO DE EVENTOS**

Todos os processos de uma organização têm algum risco associado, inerente a sua própria natureza. A identificação de eventos consiste em determinar e catalogar esses riscos, nos diversos níveis da organização. Ou seja, mapear a existência de situações que possam impedir o alcance dos objetivos fixados ou a não existência de situações consideradas necessárias para se chegar a tais objetivos ao nível da organização, de suas unidades de negócio, processos e atividades.



O modelo trata do conceito de eventos potenciais, definindo evento como um incidente, ou uma série de incidentes, resultantes de fatores internos ou externos, que possam afetar a implementação da estratégia e o alcance dos objetivos.

O processo de identificação de eventos de risco pode abranger tanto riscos negativos, tidos como ameaças, cujas consequências são perdas, como os riscos positivos, vislumbrados como oportunidades, cujas consequências são ganhos. Aqueles levando a organização a alcançar seus objetivos aquém das expectativas, estes levando a organização a alcançar resultados superiores aos obtidos atualmente ou além das expectativas.

#### **IV.2.4. AVALIAÇÃO DE RISCOS**

Os eventos identificados (componente anterior) devem ser avaliados sob a perspectiva de probabilidade e impacto de sua ocorrência. O objetivo da avaliação é formar uma base para o desenvolvimento de estratégias (resposta a risco) de como os riscos serão administrados, de modo a diminuir a probabilidade de ocorrência e/ou a magnitude do impacto. A avaliação de riscos é feita por meio de análises qualitativas e quantitativas, ou da combinação de ambas.

Os riscos devem ser avaliados quanto a sua condição de inerentes<sup>1</sup> e residuais<sup>2</sup>, e seus impactos devem ser avaliados em uma unidade de medida similar àquela utilizada para mensurar os objetivos de negócio aos quais esses riscos estão relacionados.

Os gestores são responsáveis pela avaliação dos riscos no âmbito das unidades de negócio, de processos e atividades que lhes são afetos. A alta administração deve avaliar os riscos no âmbito da organização, desenvolvendo uma visão de riscos de forma consolidada (portfólio).

#### **IV.2.5. RESPOSTA A RISCOS**

É o processo de desenvolver e determinar estratégias para gerenciar os riscos identificados. O modelo identifica quatro categorias de estratégias: **evitar**, **transferir**, **aceitar** e **tratar**, cuja escolha dependerá do nível de exposição a riscos previamente estabelecido pela organização em confronto com a avaliação que se fez do risco. Isto quer dizer que compete à administração obter uma visão dos riscos em toda organização e desenvolver um conjunto de ações concretas, dentro dessas quatro categorias, para manter o nível de riscos residuais alinhado aos níveis de tolerância e apetite a riscos da organização.

---

<sup>1</sup> Risco inerente é o risco do negócio, do processo ou da atividade, independente dos controles adotados.

<sup>2</sup> Risco residual é o risco que remanesce após a mitigação por controles.



#### **IV.2.6. ATIVIDADES DE CONTROLE**

São as políticas e os procedimentos estabelecidos e executados para mitigar os riscos que a administração opte pela estratégia de tratar. Também denominadas de procedimentos de controle, não devem ser confundidas com o próprio sistema de controle interno, pois este, além de abranger todos os demais componentes do modelo, abrange todas as demais formas de resposta a riscos.

As atividades de controle devem estar distribuídas por toda a organização, em todos os níveis e em todas as funções. Elas incluem uma gama de controles preventivos e detectivos, como procedimentos de autorização e aprovação, segregação de funções (autorização, execução, registro e controle), controles de acesso a recursos e registros, verificações, conciliações, revisões de desempenho, avaliação de operações, de processos e de atividades, supervisão direta etc.

Além de controles preventivos e detectivos, as **ações corretivas** são um complemento necessário às atividades ou aos procedimentos de controle.

#### **IV.2.7. INFORMAÇÃO E COMUNICAÇÃO**

Todos na organização devem receber mensagens claras quanto ao seu papel e ao modo como suas atividades influenciam e se relacionam com o trabalho dos demais na consecução dos objetivos fixados. A importância do controle interno para a gestão das organizações está no seu potencial informativo para suporte ao processo decisório. A habilidade da administração de tomar decisões apropriadas é afetada pela qualidade da informação, que deve ser útil, isto é, apropriada, tempestiva, atual e precisa.

Os sistemas de informação registram, tratam e produzem relatórios contendo informações operacional, financeira/não-financeira e de conformidade, que tornam possíveis a condução e o controle dos negócios. Informações relevantes devem ser identificadas, coletadas e comunicadas a tempo de permitir que as pessoas cumpram suas responsabilidades, não apenas com dados produzidos internamente, mas, também, com informações sobre eventos, atividades e condições externas, que possibilitem o gerenciamento de riscos e a tomada de decisão. A comunicação das informações produzidas deve atingir todos os níveis, por meio de canais claros e abertos que permitam à informação fluir em todos os sentidos.

A informação gerada no curso das operações é usualmente comunicada por meios de canais normais, para quem é responsável e também para um nível superior ao deste. No entanto, canais alternativos de comunicação devem existir para transmitir informação delicada, como atos



ilegais ou incorretos e comunicação de riscos. Além das comunicações internas, a administração deve assegurar que existam meios adequados de se comunicar e de obter informações externas, uma vez que as comunicações externas podem fornecer insumos de impacto significativo na extensão em que a organização alcança seus objetivos. Um plano de comunicação entre os níveis hierárquicos, bem como um plano de comunicação com outras partes interessadas (clientes, fornecedores, acionistas, sociedade etc.) é recomendável.

#### IV.2.8. MONITORAMENTO

Monitorar diz respeito a avaliar, certificar e revisar a estrutura de gestão de riscos e controles internos para saber se estão sendo efetivos ou não. Tem, portanto, o objetivo de avaliar a qualidade da gestão de risco e dos controles internos ao longo do tempo, buscando assegurar que estes funcionam como previsto e que são modificados apropriadamente, de acordo com mudanças nas condições que alterem o nível de exposição a riscos.

O monitoramento pode ser realizado de dois modos, ou por uma combinação de ambos:

- por meio de atividades gerenciais contínuas, isto é, durante o processo, no curso das operações normais;
- por meio de avaliações pontuais, em separado ou específicas.

O primeiro modo é realizado pelo próprio corpo gerencial da entidade e deve distinguir-se claramente da avaliação das operações. Consiste em identificar informações que irão indicar se o processo de gestão de riscos e controles internos está funcionando eficazmente, por meio de análises de variância, comparações de informações provindas de fontes diversas etc., com a devida consideração em relação a mudanças de processos, alterações no volume de transações, dentre outros fatores que necessitam de atenção dado o seu potencial de alterar o nível de exposição a riscos da entidade e de seus processos de negócio. No segundo modo, o monitoramento é realizado mediante autoavaliação, pela própria equipe responsável pelo processo (*process owner* ou *risk owner*<sup>3</sup>) ou por unidade de controle interno, podendo ainda ser executado por auditoria interna ou externa, nesta última incluídas as EFS e as auditorias ou controladorias de Poder.

Todas as deficiências (condição, real ou potencial, que possa afetar o alcance de objetivos) ou oportunidades para fortalecer o controle interno (aumentar as probabilidades de alcance dos objetivos), devem ser comunicadas às pessoas que podem adotar as ações necessárias.

---

<sup>3</sup>“dono do processo” ou “dono do risco”.



## **V. CONCEITOS DE RISCO E GERENCIAMENTO DE RISCO**

O padrão de gestão de risco Australiano-Neozelandês AS/NZS 4360<sup>4</sup> (STANDARDS AUSTRALIA, 1999, p.3) define risco como a possibilidade de algo acontecer e ter um impacto nos objetivos e é medido em termos de consequências e probabilidades. A IFAC (2001) define risco como uma medida de incerteza que engloba fatores que podem facilitar ou impedir a realização dos objetivos organizacionais. O TCU (2003, p.3) define risco como a expressão da probabilidade de ocorrência e do impacto de eventos futuros e incertos que têm potencial para influenciar o alcance dos objetivos de uma organização, e como a suscetibilidade de ocorrência de eventos que afetem negativamente a realização dos objetivos das unidades jurisdicionadas (TCU, 2008, p.2). Essas conceituações trazem embutida a noção de que, para se ter conhecimento dos riscos de uma organização, deve-se primeiro conhecer seus objetivos.

O padrão AS/NZS 4360 (1999) Gerenciamento de Riscos e o Guia para Gerenciar Riscos nos Setores Públicos Australiano e Neozelandês HB143 (1999) são duas importantes publicações que oferecem orientações detalhadas sobre as práticas de gerenciamento de riscos. Constituem um guia para organizações que querem desenvolver estruturas de gerenciamento de risco. Conforme essas publicações, o risco pode surgir de fontes internas ou externas e inclui a exposição a fatos como ganhos ou perdas econômicas ou financeiras, danos materiais, insucessos de projetos, descontentamento de cliente, má reputação, ameaças à segurança das instalações ou falta de segurança, malversação de recursos, inoperância de equipamentos e fraudes.

Os riscos surgem das incertezas e podem se apresentar como problemas ou desafios que necessitam ser encarados como, por exemplo, obstáculos que impedem de cumprir tarefas diárias, desenvolver e implementar projetos ou atingir objetivos e metas da organização ou, então, como oportunidades a serem aproveitadas. Há riscos que influenciam de forma significativa outros, como a inadequada capacitação ou baixa moral do pessoal, que influenciam no risco de se perder clientes importantes. Estas ligações entre riscos são importantes, pois um risco pode não parecer relevante de forma isolada, mas pode ser quando sua relação de causa e efeito é considerada.

Não existe um ambiente completamente seguro, mas muitos riscos podem ser evitados, reduzidos ou eliminados por um bom gerenciamento de riscos, que se baseia em uma estratégia

<sup>4</sup> Esse padrão é a base da futura ISO 31000: *Principles and guidelines for risk management* (Princípios e Diretrizes para o Gerenciamento de Riscos), que visa harmonizar padrões, regulamentações e frameworks publicados anteriormente sobre gerenciamento de riscos.



bem planejada, lógica, abrangente e documentada.

Essa estratégia deve fornecer orientação geral de planos, procedimentos e políticas que podem ser utilizados como parte do trabalho cotidiano da organização para gerenciar riscos. A complexidade e extensão da estratégia devem ser compatíveis com:

- a) o nível de riscos, isto é, a expressão da probabilidade e da consequência de cada risco, ao qual a organização está exposta;
- b) a freqüência e magnitude de riscos.

O padrão AS/NZS 4360 (STANDARDS AUSTRALIA, 1999, p. 4) define **gerenciamento de risco** como a aplicação sistemática de políticas, procedimentos e práticas de gestão, à tarefa de identificar, analisar, avaliar, tratar e monitorar o risco. A classificação dos riscos, segundo esse padrão, é feita, de acordo com as metas, objetivos ou resultados, em:

- a) **Estratégicos** (para a atividade-fim da organização, direção e realização de seus planos)
- b) **Comerciais** (para as relações comerciais, como falhas em contratos)
- c) **Operacionais** (para a atividade operacional da organização, como danos em ativos ou ameaças à segurança física, recursos humanos inadequados etc.)
- d) **Técnicos** (para se administrar ativos, por exemplo, falhas em equipamentos)
- e) **Financeiro e de sistemas** (para controles financeiros e sistemas, por exemplo, fraudes)
- f) **De conformidade** (para cumprir com as obrigações legais).

Para a IFAC (2001), o **gerenciamento de risco** é definido como um processo para:

- a) entender os objetivos organizacionais;
- b) identificar os riscos associados ao alcance desses objetivos, em uma base contínua, de forma a poder reagir a (ou iniciar) mudanças de uma maneira apropriada e oportuna;
- c) estimar os riscos, em termos da probabilidade de algo acontecer e o seu potencial impacto;
- d) estabelecer políticas apropriadas e procedimentos para gerenciá-las, na proporção dos riscos ou oportunidades envolvidos;
- e) monitorar e avaliar os riscos e os programas ou procedimentos utilizados para tratá-los.

Revisar riscos passados e buscar se antecipar aos futuros e monitorar mudanças nos ambientes interno e externo para obter informação que possa sinalizar uma necessidade de se reavaliar os objetivos da entidade ou do controle.

Ainda segundo a IFAC, todos os membros de uma entidade devem identificar e monitorar



os principais riscos e oportunidades e assegurar sistemas apropriados ao seu gerenciamento de riscos como, por exemplo, o de má reputação. **Os dirigentes de entidades do setor público precisam assegurar que sistemas efetivos de gerenciamento de riscos fazem parte de sua estrutura de controle.** (grifos nossos).

Um estudo realizado em conjunto pela KPMG e pelo Governo Federal Canadense, no ano de 1999, identificou as melhores práticas em gerenciamento de riscos desenvolvidas nos setores público e privado e como elas poderiam ser implantadas naquele País. Foram feitas consultas em 228 publicações sobre o tema e entrevistas com dezoito organizações, sendo seis do setor público, de países desenvolvidos, como os do Oeste Europeu, a Austrália, a Nova Zelândia e E.U.A., que relataram terem obtido muitos benefícios, em relação aos objetivos organizacionais e processos de gestão, com a implementação do gerenciamento de riscos. O principal benefício foi o grande auxílio na realização dos objetivos organizacionais. Outros benefícios foram:

- a) o maior foco nas prioridades do negócio, ou seja, não precisaram redirecionar recursos para a resolução de problemas. Ademais, ações tomadas para prevenir e reduzir perdas, ao invés de explicar depois o fato, configuraram uma efetiva estratégia de risco;
- b) a mudança cultural de aceitar a discussão dos riscos e a informação sobre potenciais danos, tolerar erros (mas não erros ocultos) e aprender com eles;
- c) a melhor gestão operacional e financeira, ao garantir que os riscos sejam adequadamente considerados no processo de tomada de decisão, resultando em uma prestação de serviços mais eficiente e efetiva. Por outro lado, ao anteciparem-se aos problemas, gerentes têm maiores oportunidades para reagir e tomar ações;
- d) o fortalecimento do processo de planejamento e o auxílio na identificação de oportunidades; e
- e) no curto prazo, o aumento da *accountability* da gestão, e no longo prazo, o aumento das capacidades gerenciais, de forma geral.

Do exposto é possível concluir que o gerenciamento de risco é um processo necessário, lógico e sistemático para organizações identificarem e avaliarem riscos e oportunidades, visando melhorar a tomada de decisões e a avaliação de desempenhos. Tem uma visão para o futuro, isto é, não apenas evita ou minimiza perdas, mas lida positivamente com oportunidades. Constitui, portanto, uma poderosa ferramenta para os gestores do setor público.



## VI. GOVERNANÇA

Nos últimos tempos, a *governança* tornou-se um conceito-chave, que todos utilizam sem saber exatamente o que é. O que tem a ver governança com riscos e controles? Já que se cunhou até um acrônimo, GRC, para designar e demonstrar a relação Governança, Riscos e Controles. Expressões como *governança corporativa*, *governança organizacional*, *governança institucional* e *governança pública* estão por toda parte.

O uso amplo da expressão exige que se precise o seu significado no contexto em que é aplicado. Para este trabalho, interessa-nos a governança das instituições públicas, portanto, no campo da governança organizacional, em geral, e da governança institucional, em particular.

Controles internos e governança são assuntos inter-relacionados, mas não são sinônimos. A estrutura de controles internos, como já vimos, é estabelecida para governar os acontecimentos dentro de uma organização que possam impactar na consecução de seus objetivos, isto é, os riscos. Portanto, controle interno é a fiscalização das atividades feita pela própria entidade, ou seja, pela sua própria administração e pelo seu corpo funcional.

Mas, e a fiscalização da administração da entidade é feita por quem? Aqui surge o conceito de governança, representado pela adoção de boas práticas, consubstanciadas nos princípios adiante descritos, que assegurem equilíbrio entre os interesses das diferentes partes que, no caso do setor público, inclui a sociedade e os seus representantes, o parlamento, as associações civis, o mercado, os órgãos reguladores e de controle, dentre outros.

A moderna governança surgiu com a necessidade de administrar os chamados conflitos de agência, que

aparecem quando o bem-estar de uma parte (denominada principal) depende das decisões tomadas por outra (denominada agente). Embora o agente deva tomar decisões em benefício do principal, muitas vezes ocorrem situações em que os interesses dos dois são conflitantes, dando margem a um comportamento oportunista por parte do agente (CARVALHO, 2002, p.19 apud SILVA, 2003).

O conceito não é novo, mas só recentemente tomou corpo. Para Peters (2007, p.27)

“ele já existe desde que as empresas passaram a ser administradas por agentes distintos dos proprietários [...] há cerca de 100 anos. Por essa época, começou a ser delineado o conflito de agência, em que o agente recebe uma delegação de recursos [...] e tem, por dever dessa delegação, que gerenciar estes recursos mediante estratégias e ações para

atingir objetivos [...], tudo isto mediante uma obrigação constante de prestação de contas.”

Alguns dos princípios fundamentais da boa governança comuns a diversos autores são:

- **transparéncia (*disclosure*)**: representa o processo de contínua demonstração, pelo agente, de que sua gestão está alinhada às diretrizes estratégicas previamente fixadas pelo principal. Não é só limitar-se à “obrigação de informar” (*accountability*), o agente (a administração) deve cultivar o “desejo de informar”.
- **equidade (*fairness*)**: tratamento justo e igualitário a todas as partes interessadas, sendo totalmente inaceitáveis atitudes ou políticas discriminatórias, sob qualquer pretexto.
- **prestação de contas (*accountability*)**: os agentes da governança devem prestar contas de sua atuação a quem os fez delegação e respondem integralmente por todos os atos que praticarem no exercício desse mandato; e
- **responsabilidade (*responsability*)**: definição de uma política de responsabilidade que assegure a máxima sustentabilidade dos negócios, incorporando considerações de ordem ética, social e ambiental em todos os processos e relacionamentos.

A administração pública brasileira deve obediência a todos esses princípios, espalhados que estão por todo o texto constitucional, e especificamente aos sintetizados no art. 37 da CF/88, que representam os requisitos de sua atuação.

Os agentes da governança institucional de órgãos, entidades, programas e fundos públicos, por subsunção a tais princípios, devem contribuir para aumentar a confiança sobre a forma como são geridos os recursos colocados à sua disposição, reduzindo a incerteza dos membros da sociedade sobre o que acontece no interior da administração pública. Essa contribuição será tanto mais efetiva quanto melhor for a qualidade dos instrumentos e mecanismos de governança institucional arregimentados e mantidos pelos agentes responsáveis pela coisa pública.

Boas estruturas de gestão de riscos e controles internos são pré-requisitos para uma organização bem administrada, e esses três elementos são pré-requisitos para uma boa governança. Desse modo, Governança, Riscos e Controles devem ser geridos de forma integrada, objetivando o estabelecimento de um ambiente que respeite não apenas os valores, interesses e expectativas da instituição e dos agentes que a compõem, mas também de todas as suas partes interessadas, tendo o cidadão e a sociedade como os vetores principais desse processo.



## VII. A REGULAÇÃO DE CONTROLES INTERNOS EM PAÍSES DO MUNDO

Os países pesquisados trataram o tema controles internos em seus ordenamentos jurídicos conforme se descreve a seguir.

### VII.1. CANADÁ

A obrigação de instituir, manter e avaliar controles internos no setor público não é objeto de lei ou norma específica. No entanto, o tema é encontrado em relatórios de auditorias e em estudos sobre métodos e técnicas do *Office of the Auditor General of Canada* (OAG), que tem como jurisdicionados órgãos públicos federais (incluindo as províncias)<sup>5</sup>. Auditorias desse órgão envolvem a avaliação de controles internos, o que pressupõe a necessidade de existência e eficácia desses. Com efeito, a Lei de Administração Financeira do Canadá (*Financial Administration Act*) atribui responsabilidades a ministros e chefes departamentais, perante o Parlamento e as comissões do Senado e da Câmara dos Comuns, pela organização de recursos conforme as políticas e procedimentos governamentais e pela manutenção de eficazes controles internos:

Accountability of accounting officers within framework of ministerial accountability

16.4 (1) Within the framework of the appropriate minister's responsibilities and his or her accountability to Parliament, and subject to the appropriate minister's management and direction of his or her department, the accounting officer of a department named in Part I of Schedule VI is accountable before the appropriate committees of the Senate and the House of Commons for

( a ) the measures taken to organize the resources of the department to deliver departmental programs in compliance with government policies and procedures;

( b ) the measures taken to maintain effective systems of internal control in the department; (grifamos).

O *Advancing Audit Practices Project (AAPP)*, do OAG, desenvolvido em parceira com entidades privadas, como a PricewaterhouseCoopers LLP, inclui os seguintes elementos-chaves para o desenvolvimento de técnicas de auditoria (os grifos são nossos):

<sup>5</sup> *Auditor General Act 6. The Auditor General shall examine the several financial statements required by section 64 of the Financial Administration Act to be included in the Public Accounts, and any other statement that the President of the Treasury Board or the Minister of Finance may present for audit and shall express his opinion as to whether they present fairly information in accordance with stated accounting policies of the federal government and on a basis consistent with that of the preceding year together with any reservations he may have.*



- **Foco no risco do negócio ("Business Risk" Focus);**
- Acúmulo de conhecimento e experiência de auditoria (*Cumulative Audit Knowledge and Experience – CAKE*);
- **Confiança nos controles (Reliance on Controls);**
- Julgamento Profissional (*Professional Judgment*);
- Princípio da melhoria contínua (*The Re-performance Principle*); e
- Trabalho em equipe (*Teamwork*).

A publicação *Federal Government Spending: a priori and a posteriori Control Mechanism*, de 2007, define as seguintes estratégias de controle para o governo canadense:

- *A priori internal control* – controle existente em cada fase do ciclo orçamentário. Visa garantir a sua efetividade;
- *A posteriori internal control* – controle realizado pela Controladoria-Geral, que é a auditoria interna do governo federal (equivalente à nossa CGU);
- *A posteriori external control* – controle externo realizado pelo OAG;
- *A priori parliamentary control* – aprovação do orçamento pelo parlamento (*Senate, House of Commons and theirs committees*), e
- *A posteriori parliamentary control* – acompanhamento da execução orçamentária pelas comissões do parlamento.

## VII.2. ESTADOS UNIDOS DA AMÉRICA

Em 1982, o Congresso dos Estados Unidos, em seção conjunta do Senado e da Câmara dos Representantes, alterou a Lei de Contabilidade e Auditoria de 1950 (*Accounting and Auditing Act of 1950*) com o objetivo de incluir a obrigatoriedade de avaliações contínuas e relatórios sobre a adequação dos sistemas de controle interno contábil e administrativo de cada órgão/entidade, e para outros fins.

A lei alterada passou a denominar-se Lei Federal de Integridade na Gestão Financeira (*Federal Managers Financial Integrity Act of 1982 - FMFIA*), e suas novas disposições obrigam os órgãos públicos federais a estabelecerem controles internos, seguindo padrões prescritos pelo órgão de controle externo daquele país, o GAO.

Section 113 of the Accounting and Auditing Act of 1950 (31 U.S.C.66a) is amended by adding at the end thereof the following new subsection:

(d) (1) (A) To ensure compliance with the requirements of subsection (a)(3) of this section, internal accounting and administrative controls of each executive agency shall be established in accordance with standards prescribed by the Comptroller General, and shall provide reasonable assurances that --



Segundo a Lei Federal de Integridade na Gestão Financeira, esses controles devem prover razoável segurança quanto à conformidade legal de obrigações e custos, à proteção de bens e ativos públicos contra desperdício, perda, utilização não autorizada ou apropriação indevida, e quanto ao apropriado registro e contabilização das receitas e despesas para permitir prestações de contas, relatórios financeiros e estatísticos confiáveis e controle de responsabilidades sobre ativos.

- (i) obligations and costs are in compliance with applicable law
- (ii) funds, property, and other assets are safeguarded against waste, loss, unauthorized use, or misappropriation; and
- (iii) revenues and expenditures applicable to agency operations are properly recorded and accounted for to permit the preparation of accounts and reliable financial and statistical reports and to maintain accountability over the assets.

Os padrões prescritos pelo GAO, segundo determinação da FMFIA, devem incluir normas que assegurem a pronta identificação de todos os achados de auditoria.

(B) The standards prescribed by the Comptroller General under this paragraph shall include standards to ensure the prompt resolution of all audit findings.

A FMFIA também determinou que o diretor do Gabinete de Gestão e Orçamento, em consulta com o Controlador Geral, estabelecesse diretrizes para avaliação, pelos órgãos e entidades, de seus controles internos. Essa autoavaliação, como se verá adiante, é que subsidiará a certificação anual a ser proferida pelo dirigente máximo do órgão ou entidade.

(2) By December 31, 1982 the Director of the Office of Management and Budget, in consultation with the Comptroller General, shall establish guidelines for the evaluation by agencies of their systems of internal accounting and administrative control to determine such systems' compliance with the requirements of paragraph (1) of this subsection. The Director, in consultation with the Comptroller General, may modify such guidelines from time to time as deemed necessary.

Ainda, segundo a FMFIA, o dirigente máximo de cada órgão ou entidade pública federal deve, anualmente, com base em uma avaliação realizada em conformidade com as orientações previstas acima, elaborar uma declaração certificando se os controles internos contábeis e administrativos estão ou não em conformidade com os requisitos estabelecidos.



Caso a certificação do dirigente máximo não seja de conformidade plena, ele deve anexar à sua declaração um relatório reportando cada deficiência material identificada no controle interno, bem como os planos e o cronograma para corrigi-las.

As declarações e os relatórios exigidos pela FMFIA devem ser transmitidos ao Presidente e ao Congresso e também devem ser disponibilizados ao público, exceto, no último caso, se envolver informação proibida por qualquer disposição de direito ou de caráter sigiloso no interesse da defesa nacional ou na condução dos assuntos externos.

(3) By December 31, 1983, and by December 31 of each succeeding year, the head of each executive agency shall, on the basis of an evaluation conducted in accordance with guidelines prescribed under paragraph (2) of this subsection, prepare a statement --

(A) that the agency's systems of internal accounting and administrative control fully comply with the requirements of paragraph (1); or

(B) that such systems do not fully comply with such requirements.

(4) In the event that the head of an agency prepares a statement described in paragraph (3)(B), the head of such agency shall include with such statement a report in which any material weaknesses in the agency's systems of internal accounting and administrative control are identified and the plans and schedule for correcting any such weakness are described.

(5) The statements and reports required by this subsection shall be signed by the head of each executive agency and transmitted to the President and the Congress. Such statements and reports shall also be made available to the public, except that, in the case of any such statement or report containing information which is --

(A) specifically prohibited from disclosure by any provision of law; or

(B) specifically required by Executive order to be kept secret in the interest of national defense or the conduct of foreign affairs, such information shall be deleted prior to the report or statement being made available to the public".



O diretor do Gabinete de Gestão e Orçamento (*Office of Management and Budget - OMB*), órgão vinculado ao Escritório Executivo do Presidente dos Estados Unidos, atendendo a disposição da FMFIA de estabelecer diretrizes para avaliação dos controles internos com vistas à certificação anual a ser proferida pelo dirigente máximo do órgão ou entidade, expediu o documento denominado OMB Circular A-123. A versão atual dessa circular é de 21 de dezembro de 2004, vigente a partir do exercício fiscal de 2006.

As características básicas do documento podem ser abstraídas da sua própria introdução, no texto a seguir, com tradução nossa. Destacam-se os aspectos relativos à responsabilidade fundamental por estabelecer, manter e avaliar o controle interno, que cabe à administração e aos gestores, sem prejuízo da obrigação dos demais empregados de comunicar à instância superior as deficiências identificadas; certificação do controle interno no processo anual de prestação de contas; conceito, objetivos, abrangência do controle interno e alinhamento das ações à missão dos órgãos e entidades. Observe-se, ainda, que a circular menciona que é a FMFIA que estabelece requisitos gerais no que diz respeito ao controle interno.

#### ***Circular n.º A-123 Revisada - Responsabilidade da Administração pelo Controle Interno***

***Fundamentação legal.*** A circular é emitida sob fundamentação da Lei Federal de Integridade da Gestão Financeira, de 1982, como codificada em 31 USC 3512.

#### ***INTRODUÇÃO***

*A administração tem a responsabilidade fundamental de desenvolver e manter controle interno eficaz. A correta gestão dos recursos federais é uma responsabilidade essencial dos gestores e funcionários. Empregados federais devem assegurar que os programas funcionem e os recursos sejam utilizados de forma eficiente e eficaz para alcançar os objetivos desejados. Os programas devem operar e os recursos devem ser utilizados em consistência com a missão dos órgãos, em conformidade com as leis e regulamentos, e com o potencial mínimo de desperdício, fraude e má gestão.*

*A administração é responsável por desenvolver e manter controle interno eficaz. Controle interno eficaz prevê garantia de que deficiências significativas no desenho ou na operação do controle interno, que possam afetar adversamente a capacidade do órgão para cumprir os seus objetivos, serão evitados ou detectados em tempo oportuno.*



**Controle Interno** - organização, políticas e procedimentos - são ferramentas para ajudar gestores financeiros a alcançar resultados e salvaguardar a integridade de seus programas. Esta circular contém orientações sobre a utilização da gama de instrumentos à disposição dos gestores para alcançar os resultados desejados e preencherem os requisitos da Lei Federal de Integridade Financeira (FMFIA) de 1982. A FMFIA engloba controles contábeis e administrativos. Estes controles abrangem programas, operações e áreas administrativas, bem como áreas de contabilidade e gestão financeira.

A importância do controle interno é abordada em muitos estatutos e documentos executivos. A FMFIA estabelece requisitos gerais no que diz respeito ao controle interno. A administração do órgão deve estabelecer controles que razoavelmente garantam que: "(i) as obrigações e os custos estão em conformidade com a lei aplicável, (ii) fundos, bens e outros ativos estão protegidos contra o desperdício, perda, a utilização não autorizada ou utilização abusiva, e (iii) As receitas e despesas aplicáveis às operações do órgão estão devidamente registradas e contabilizadas de modo a permitir a elaboração de prestação de contas, relatórios financeiros e estatísticos confiáveis e de manter a responsabilidade sobre os ativos." Além disso, a administração do órgão deve avaliar anualmente e apresentar um relatório sobre o controle e sistemas financeiros que protegem a integridade dos programas federais (parágrafo 2 e parágrafo 4 da FMFIA respectivamente). Os três objetivos do controle interno são garantir a eficácia e a eficiência das operações, a confiabilidade da informação financeira, bem como a conformidade com as leis e regulamentos aplicáveis. A salvaguarda do patrimônio é um subconjunto de todos estes objetivos.

**Objetivo.** Este Circular fornece orientação aos gestores federais para a melhoria da accountability e da eficácia das operações e dos programas federais, pelo estabelecimento, avaliação, revisão e reporte de controles internos. O anexo à presente Circular define responsabilidades da administração relacionadas ao controle interno e ao processo para avaliar a eficácia do controle interno, juntamente com um resumo das mudanças significativas. A Circular procede a atualização das normas de controle interno e de novos requisitos específicos para a administração conduzir a avaliação da eficácia dos controles internos sobre relatórios financeiros (Anexo A). Esta Circular enfatiza a necessidade de avaliação integrada e coordenada do controle interno sincronizando todas as atividades relacionadas.

**Política.** A administração é responsável por estabelecer e manter controles internos para



*alcançar os objetivos de eficiência e eficácia operacional, confiabilidade dos relatórios financeiros, e conformidade com leis e regulamentos aplicáveis. A administração deve aplicar as normas de controle interno para cumprir cada um dos objetivos de controle interno e para avaliar a sua eficácia. Ao avaliar a eficácia dos controles internos sobre relatórios financeiros e conformidade com leis e regulações financeiras, a administração deve seguir o processo de avaliação contido no apêndice A. Anualmente, a administração deve certificar o controle interno no seu relatório de gestão (desempenho) e de prestação de contas, incluindo uma avaliação em separado dos controles internos sobre relatórios financeiros, juntamente com um relatório sobre fraquezas significativas identificadas e ações corretivas.*

**Ações requeridas.** Órgãos e gestores individuais federais devem tomar medidas proativas e sistemáticas para (i) desenvolver e implementar controle interno adequado, de boa relação custo-eficácia, para gestão orientada a resultados; (ii) avaliar a adequação do controle interno nos programas e operações federais (iii) avaliar separadamente e documentar o controle interno sobre relatórios financeiros conforme processo definido no Anexo A (iv) identificar melhorias necessárias; (v) tomar as ações corretivas correspondentes; e (vi) certificar anualmente o controle interno por meio de declaração da administração.

No que diz respeito ao modelo de referência de controle interno adotado, percebe-se que a OMB Circular A-123 foi revisada com o propósito de incorporar o modelo COSO e os requisitos da Lei Sarbanes-Oxley, de 2002, conforme se depreende dos quadros a seguir transcritos, com tradução nossa, os quais destacam as revisões significativas procedidas, e do seguinte parágrafo inicial da comunicação que envia a referida circular a todos os órgãos federais americanos.

A Circular OMB A-123 define responsabilidades da administração pelo controle interno nos órgãos federais. Um re-exame dos requisitos existentes para controle interno nos órgãos federais foi iniciado à luz dos novos requisitos de controle interno para as companhias abertas contidos na Lei Sarbanes-Oxley<sup>6</sup>, de 2002. A Circular A-123 e o estatuto que a fundamenta, a Lei Federal de Integridade da Gestão Financeira, de 1982, estão no centro das atuais exigências federais para melhorar o controle interno.

---

<sup>6</sup> O Public Company Accounting Oversight Board – PCAOB, o novo órgão regulador criado pela Lei Sarbanes-Oxley para fiscalizar as empresas de auditoria independente, no seu Auditing Standard 2 (AS2) referencia o COSO II como uma boa maneira de definir a eficácia do sistema de controle interno realizado pela gerência da entidade auditada.



*Circular n º. A-123 Revisada - Responsabilidade da Administração pelo Controle Interno*

**ANEXO**  
**Revisões Significativas da Circular OMB A-123**

Seção	Revisão para A-123	Objetivo da Revisão
Mudança de título da Circular	<i>Mudado o título de OMB Circular A-123, <u>Management Accountability and Control</u> para OMB Circular A-123, <u>Management's Responsibility for Internal Control</u></i>	<i>Titulo mudado para alinhar melhor com o foco da circular e a terminologia corrente</i>
Ao longo da Circular	<i>Mudado a terminologia de “controles administrativos” para “controle interno”</i>	<i>Para melhor alinhar com as normas de controle interno aceitas atualmente e a terminologia corrente. Os termos devem ser entendidos como sinônimos.</i>
Seção II. Normas	<i>Realinizada seção sobre as normas de controle interno utilizando as seguintes categorias: ambiente de controle, avaliação de risco, atividades de controle, informação e comunicação, e monitoramento.</i>	<i>Para melhor alinhar com as normas de controle interno aceitas atualmente.</i>
Seção III. Estrutura Integrada de Controle Interno	<i>Disponibilizada uma seção separada sobre a estrutura integrada de controle interno. Disponibilizada uma lista dos critérios a considerar na avaliação do controle interno.</i>	<i>Para destacar as atuais exigências legislativas e regulamentares que devem ser coordenadas e consideradas quando se avalia a eficácia do controlo interno.</i>
Seção IV.B. Identificação de Deficiências	<i>Introduzido condição de reporte como uma categoria de deficiência.</i>	<i>Para melhor alinhar com a terminologia governamental corrente.</i>
Seção VI.A. Declaração Anual de Garantia	<i>Exigir das agências sujeitas à lei de CFO que incluam o relatório anual FMFIA no PAR, sob o título “Certificação da Administração” além de submeter ao OMB 45 dias a contar do final do ano fiscal.</i>	<i>Para consolidar as declarações de certificação em um local dentro do PAR (Seção 2, secção 4, e de controle interno sobre relatórios financeiros). Para antecipar a data de entrega dos relatórios FMFIA para ser coerente com a data de entrega do PAR.</i>



<i>Seção VI.B. Relatórios ao abrigo da Seção 2</i>	<i>Introduzida uma nova declaração de certificação sobre a eficácia do controle interno sobre relatórios financeiros. Esta declaração será um subconjunto do conjunto de declarações de certificação do FMDA.</i>	<i>Para enfatizar a responsabilidade da administração para avaliar e documentar controles internos sobre relatórios financeiros. Para garantir ao Congresso e à opinião pública que o Governo Federal está empenhado em proteger seus bens e prestar informações financeiras confiáveis.</i>
<i>Seção VI. Relatórios sobre Controle Interno</i>	<i>Incluído um resumo gráfico de definições e requisitos para relatórios de deficiência, condição de reporte, fraqueza significativa e não-conformidade.</i>	<i>Para fornecer um resumo conciso de definições para relatórios.</i>
<i>Apêndice A</i>	<i>Para abordar especificamente a avaliação, documentação e comunicação sobre a eficácia dos controles internos sobre relatórios financeiros.</i>	<i>Para garantir ao Congresso e à opinião pública que o Governo Federal está empenhado em proteger seus bens e prestar informações financeiras confiáveis.</i>

***Novos Requisitos do Apêndice A - Controles Internos sobre Relatórios Financeiros***

<i>Nova Seção</i>	<i>Novo Requisito</i>
<i>Transmutação da Circular</i>	<i>Exige que as 24 CFO agências oficiais satisfaçam os requisitos do Apêndice A.</i>
<i>Seção II. Escopo</i>	<i>Define o escopo da avaliação e documentação do controle interno sobre relatórios financeiros para incluir as demonstrações financeiras anuais e outros relatórios financeiros significativos, internos ou externos, e a conformidade com leis e regulamentações que dizem respeito aos relatórios financeiros.</i>
<i>Seção II.C. Materialidade</i>	<i>Define materialidade para efeitos de avaliação e documentação do controle interno sobre relatórios financeiros.</i>
<i>Seção III.A. Estabelece uma Equipe Sênior de Avaliação</i>	<i>Recomenda a criação de uma equipe sênior de avaliação, em termos mínimos, que deve supervisionar o processo de avaliação.</i>
<i>Seção III.B.E. Avaliação de Controle Interno sobre Relatórios Financeiros</i>	<i>Define o processo de avaliação do controle interno sobre relatórios financeiros ao nível da entidade, bem como dos processos, das transações, ou aplicações.</i>
<i>Seção IV. Documentação</i>	<i>Requer que os controles internos sobre relatórios financeiros o processo de avaliação deles sejam documentados.</i>



<i>Seção V. Gestão da avaliação de Controle Interno sobre Relatórios Financeiros</i>	<i>Requer que a declaração de certificação para afirmar a eficácia do controle interno tenha por base “30 de Junho”. O relatório de avaliação e as ações corretivas, se aplicáveis, serão apresentadas no PAR, o mais tardar 45 dias após o final de cada ano fiscal.</i>
<i>Seção V. Gestão da avaliação de Controle Interno sobre Relatórios Financeiros</i>	<i>Fornecer um modelo de declaração de certificação sobre a eficácia do controle interno sobre relatórios financeiros.</i>
<i>Seção V.A. Obtenção da Opinião da Auditoria sobre Controle Interno pelos Órgãos</i>	<i>Agências que escolherem receber uma opinião em separado a respeito do controle interno sobre relatórios financeiros devem ajustar a data base para 30 de junho para alinhar melhor com a data base da opinião da auditoria. Esta circular não exige uma auditoria em separado.</i>
<i>Seção VI. Correção de fraquezas significativas no Controle Interno sobre Relatórios Financeiros</i>	<i>Provê uma cláusula de não-conformidade que permite OMB exigir de um órgão a obtenção de um parecer de auditoria sobre os controles internos sobre relatórios financeiros se os prazos acordados para as ações corretivas são continuamente não cumpridas.</i>

O GAO, por seu turno, conforme determina a Lei Federal de Integridade Financeira, deve prescrever os padrões para estabelecimento de controles internos pelos órgãos e entidades do governo federal. As normas foram inicialmente emitidas pelo GAO em 1983 e se tornaram amplamente conhecidas em todo o governo como o “Livro Verde”. Desde então, mudanças na tecnologia da informação, questões emergentes envolvendo a gestão de capital humano e requisitos de leis recentes sobre gestão financeira motivaram um enfoque renovado no controle interno. Consequentemente, o GAO revisou as normas e as publicou novamente sob o título *Normas de Controle Interno no Governo Federal* (GAO/AIMD-00-21.3.1, novembro de 1999). Essas normas estabelecem o marco geral para a criação e manutenção do controle interno e para a identificação e o tratamento dos principais desafios de desempenho e das áreas mais expostas a riscos de fraude, desperdício, abuso e má gestão na administração pública federal americana.

Em 2001, o GAO emitiu o documento *Internal Control Management and Evaluation Tool*, que é uma ferramenta de gestão e avaliação de controle interno, baseada nas *Normas de Controle Interno no Governo Federal*, para auxiliar órgãos públicos a implementar e manter controles internos efetivos e, quando necessário, ajudá-los a determinar o que, onde e como melhorias podem ser implementadas. Segundo orientação do GAO, essa ferramenta e a Circular A-123 do OMB devem ser usadas concomitantemente.



A ferramenta é apresentada em cinco seções, que correspondem aos cinco componentes do controle interno do COSO I: ambiente de controle, avaliação de riscos, atividades de controle, informação e comunicação, e monitoramento. Cada seção contém uma lista dos principais fatores a serem considerados na revisão do controle interno. Os fatores representam algumas das questões mais relevantes, incluindo itens específicos e suplementares que os usuários devem considerar ao abordar o fator. Os itens específicos e suplementares têm como objetivo auxiliar os usuários a considerarem aspectos que indiquem o grau no qual o controle interno está funcionando e a formar juízo sobre (1) a aplicabilidade do item às circunstâncias; (2) se o órgão foi efetivamente capaz de implementar, cumprir ou aplicar o item; (3) quaisquer fragilidades do controle; e (4) a medida na qual o item afeta a capacidade do órgão para cumprir sua missão e suas metas.

Quanto ao modelo de referência adotado, a própria introdução do documento *Internal Control Management and Evaluation Tool* informa que a ferramenta “foi desenvolvida a partir de diferentes fontes de informações e idéias. A fonte principal foi, obviamente, o documento *Normas de Controle Interno no Governo Federal*, elaborado e publicado pelo GAO. Orientações adicionais foram obtidas na seção “Ferramentas de Avaliação” do documento *Controle Interno – Marco Integrado (Internal Control - Integrated Framework)*, publicado em setembro de 1992 pelo Comitê de Organizações Patrocinadoras da Comissão Treadway (COSO).” (grifamos).

### VII.2.1. NEW YORK STATE (USA)

O Estado de Nova York editou, em 1987, o *New York State Governmental Accountability, Audit and Internal Control Act*, que evidenciou a importância da implantação de bons controles internos. Esse ato foi atualizado em 1999 e estabeleceu a responsabilidade dos controles internos nos vários setores/poderes do governo:

- a) capítulo 18 (*Executive Law*), artigo 45: responsabilidades dos controles internos das agências estatais;
- b) capítulo 32 (*Legislative Law*), artigo 6: responsabilidades dos controles internos do poder legislativo;
- c) capítulo 30 (*Judiciary Law*), artigo 7: responsabilidades dos controles internos do poder judiciário, e
- d) capítulo 43 (*Public Authorities Law*), artigo 9: responsabilidades dos controles internos das autoridades públicas.



O ato é dividido em seções de conteúdos semelhantes em cada capítulo, apenas com adaptações de nomenclatura e outras especificidades de cada poder, por isso serão analisados em conjunto. A lei define responsabilização para que sejam estabelecidas diretrizes de implantação e manutenção de controles internos e, no preâmbulo, diz que deverão ser consideradas as normas profissionais de controle interno e as práticas de organizações públicas e privadas.

**Seções:**

1. Definições
2. Responsabilidades pelo Controle Interno
3. Responsabilidades pela Auditoria Interna
4. Auditores Independentes

Percebe-se que o conceito adotado é, essencialmente, o mesmo do documento *Standards for Internal Control in the Federal Government*, do GAO:

**“Internal Control.** A process that integrate the activities, plans, attitudes, policies, systems, resources and efforts of the people of an organization working together, and that is designed to provide reasonable assurance that the organization will achieve its objectives and mission.”

A norma define que a responsabilidade pelo controle interno é do dirigente máximo de cada órgão e poder (*The head of each state agency, The senate and the assembly, The chief judge, The governing board of each covered authority or its designee*), que deve:

- a) estabelecer e manter diretrizes para o controle interno, e
- b) estabelecer e manter um sistema de controle interno e um programa de revisão de controles internos.

Sobre a auditoria interna, a norma diz que deverá ser implementada levando-se em conta a relação custo-benefício e outros fatores relevantes, com a função de avaliar os controles internos, identificar suas falhas e fazer recomendações para corrigi-las. A norma determina, também, que, pelo menos a cada três anos, uma auditoria independente deverá avaliar os controles internos dos órgãos públicos.

A análise das normas americanas, no âmbito federal e do estado de Nova York, permite concluir que naquele país cada esfera de governo trata de sua própria regulação em matéria de controle interno, e que, nos dois casos estudados, as normas incorporam o que há de mais contemporâneo em relação ao assunto, tanto em termos de responsabilização como no tocante aos conceitos e ao modelo de referência utilizado, que é o modelo COSO.



### VII.3. CHILE

As normas chilenas prescrevem a obrigatoriedade de implantação e avaliação de controles internos nos órgãos e entidades da administração pública. O cumprimento dessa obrigatoriedade é garantido por meio da responsabilização de gestores envolvidos nos processos, em todas as instâncias, além da avaliação realizada pela própria controladoria em auditorias específicas.

Não há, no entanto, ato normativo ou legal específico que institua metodologia ou modelo de controles internos como referência. Os dispositivos estão dispersos em leis, decretos e resoluções. O Estado Chileno é um estado unitário, desse modo, as leis que não tratam de órgãos ou entidades específicos possuem abrangência nacional.

A lei 10.336, de Organização e Atribuições da Controladoria-Geral da República, estabelece a obrigatoriedade de que seus jurisdicionados instituam controles internos, conforme dispositivos a seguir transcritos (tradução e grifos nossos):

Artigo 21º A Controladoria-Geral efetuará auditorias com o objetivo de garantir o cumprimento das normas jurídicas, a proteção do patrimônio público e a probidade administrativa. Por meio dessas auditorias a **Controladoria-Geral avaliará os sistemas de controle interno dos serviços e entidades.**

A responsabilidade pelo estabelecimento e pela manutenção dos controles internos é fixada em normas específicas e, normalmente, é atribuída à autoridade executiva máxima da instituição, conforme os exemplos:

**Lei 18.956/90:** Artigo 6º Funções e faculdades do Ministério da Educação – O subsecretário de educação é o colaborador imediato do ministro, cabendo-lhe a coordenação e o controle interno das unidades integrantes da subsecretaria. [...]

**Decreto 187/98:** Artigo 15. Organização interna e estrutura do Fundo Nacional de Saúde (Fonasa) – O departamento de controladoria interna [...] caberá assessorar ao diretor em matérias de ordem administrativa, patrimonial e financeira [...] para o alcance de uma gestão eficiente de suas operações e no estabelecimento e manutenção de um sistema de controle interno.

**Lei 19.974/2004:** Artigo 34 Administração, recursos humanos e técnicos, uso adequado de fundos e procedimentos da Agencia Nacional de Inteligência (ANI) – O controle interno dos órgãos de inteligência será realizado pelo diretor ou chefe de cada órgão de inteligência que integra o sistema de inteligência do Estado, que será responsável direto pelo cumprimento desta lei. [...]



## **VII.4. PARAGUAI E COLÔMBIA**

Nesses dois países, a obrigatoriedade de controle interno foi estabelecida em leis, sendo que na Colômbia a obrigatoriedade deriva da própria Constituição. Em ambos os casos, as normas relativas à implantação, manutenção e avaliação de sistemas de controle interno ficaram a cargo das Controladorias-Gerais. Ambos desenvolveram modelos próprios de implantação e manutenção de controles internos em suas administrações públicas, tendo como base o modelo COSO. Devido às semelhanças entre eles, serão analisados em conjunto.

No Paraguai, o estabelecimento de controles internos na administração pública é prescrito nas leis 1535/99 (de Administração Financeira do Estado) e 276/94 (Orgânica e Funcional da Controladoria-Geral da República). Como no caso do Chile, o Paraguai também é um estado unitário, portanto essas leis obrigam todos os órgãos e entidades públicos paraguaios instituírem controles internos.

### **Lei 1535/99 de Administração Financeira do Estado.**

[...]

Artigo 60. O controle interno consiste nos instrumentos, mecanismos e técnicas de controle, que serão estabelecidos em regulamentação pertinente. O controle interno compreende o controle prévio a cargo dos responsáveis pela Administração e o controle posterior a cargo da Auditoria Interna Institucional e da Auditoria-Geral do Poder Executivo.

### **Lei 276/94 Orgânica e Funcional da Controladoria-Geral da República.**

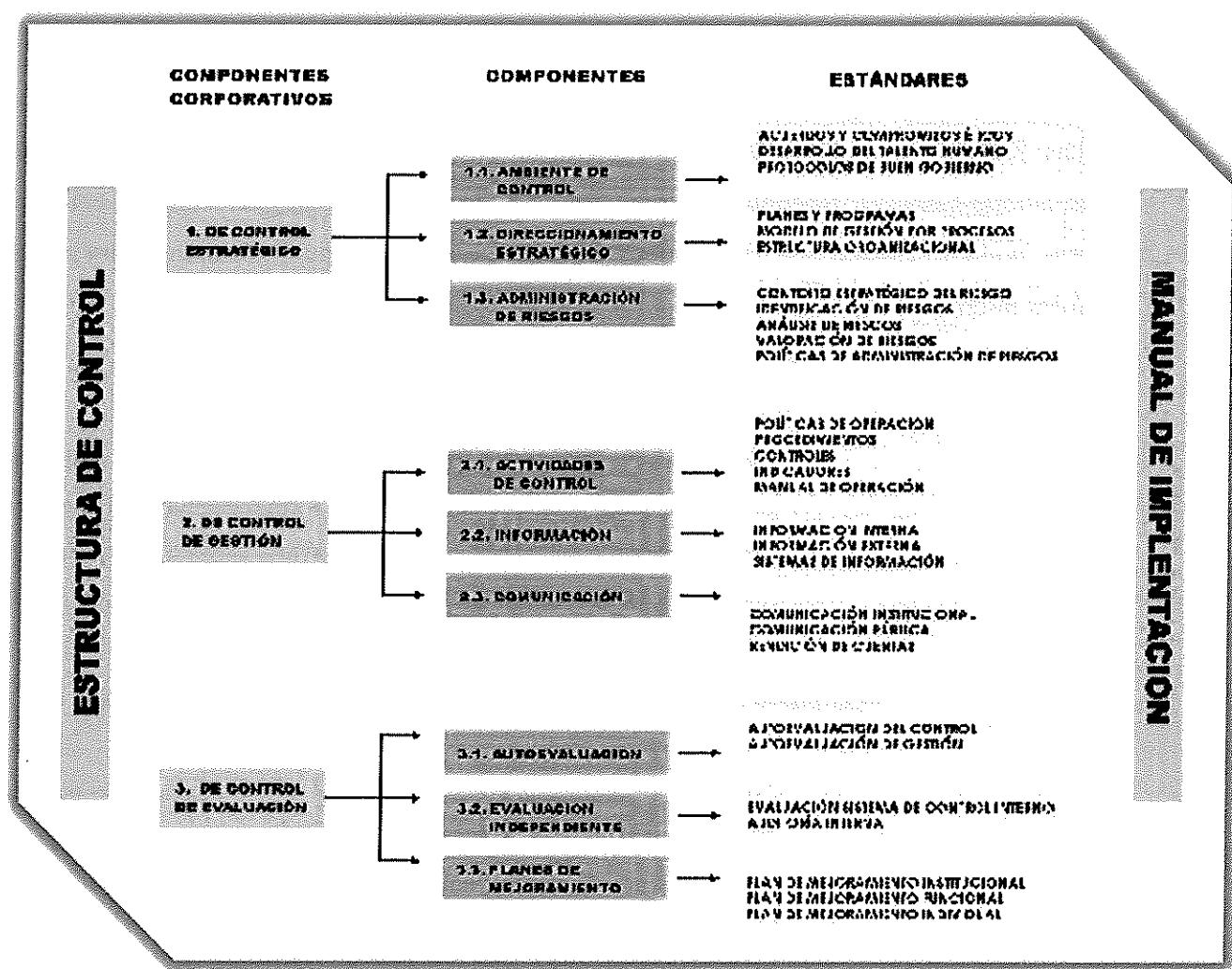
[...]

Artigo 2º A Controladoria-Geral, dentro do marco determinado pelos artigos 281 e 283 da Constituição Nacional, tem por objetivo [...] e recomendar, em geral, as normas de controle interno para as entidades sujeitas à sua supervisão. (grifamos).

Em 2008, conforme estabelecido na lei 276/94, a Controladoria-Geral do Paraguai editou a Resolução 425, estabelecendo um modelo padrão de controle interno para a administração pública, o MECIP (*Modelo Estándar de Control Interno para las Entidades Públicas del Paraguay*). O objetivo do modelo, segundo a resolução, é fornecer uma abordagem sistemática, organizada e estruturada como base para o desenvolvimento e avaliação de controles internos.

O MECIP foi elaborado com auxílio da Agência Americana para o Desenvolvimento Internacional (*The U.S. Agency for International Development – USAID*) e é o padrão utilizado para a fiscalização e avaliação dos sistemas de controle interno das entidades sujeitas à supervisão da Controladoria-Geral do Paraguai.

## O modelo MECIP do Paraguai



Na Colômbia, a previsão de controles internos é constitucional:

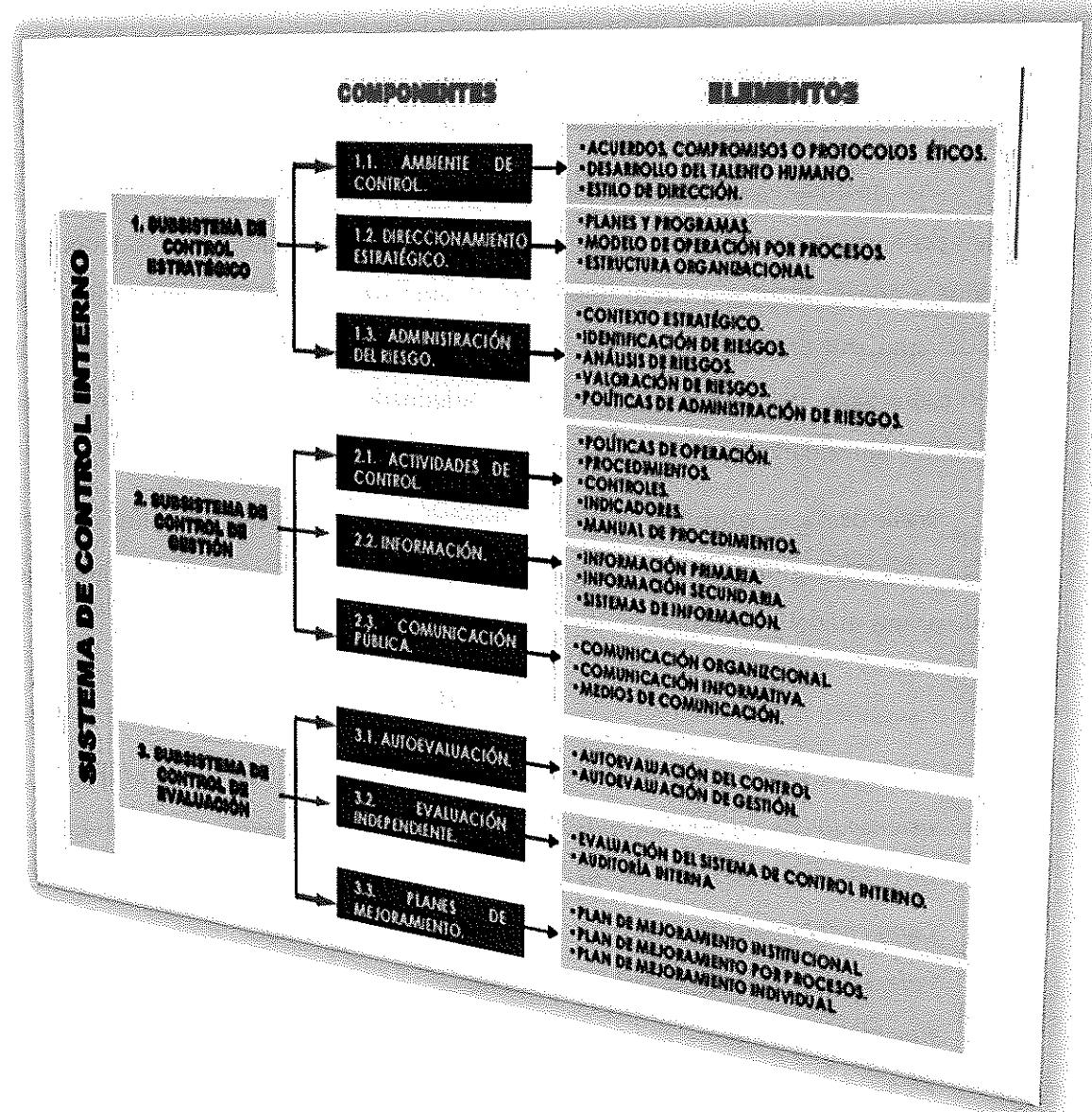
CONSTITUIÇÃO POLÍTICA DA COLOMBIA. ARTIGO 209.

[...]

As autoridades administrativas devem coordenar suas atuações para o adequado cumprimento dos fins do Estado. A administração pública, em todos os seus níveis, terá um controle interno que se exercerá nos termos da lei. (grifamos)

A Colômbia, assim como o Paraguai, elaborou seu modelo de controle com o auxílio da USAID. O modelo foi introduzido por meio de decreto presidencial, regulamentando a Lei 87 de 1993, que fixou normas gerais para o exercício do controle interno nos órgãos e entidades do Estado, uma vez que a Assembléia Nacional Constituinte decidiu eliminar o controle prévio por parte da Controladoria-Geral e, em seu lugar, determinou o estabelecimento de controle interno exercido pelos próprios órgãos e entidades.

## O modelo MECI da Colômbia





Como se pode observar da análise dos componentes dos modelos paraguaio e colombiano, eles foram desenvolvidos a partir do COSO, com pequenas adaptações. Todos os componentes e objetivos do COSO estão presentes em ambos, apenas com outros nomes e agrupamentos. Outra adaptação feita é o detalhamento em nível de elementos ou *estandares*, muito úteis para a aplicação eficiente dos modelos pelos órgãos e entidades públicos.

Em ambos os casos, os modelos são constituídos de três partes, no Paraguai: Componentes Corporativos de Controle (Estratégicos, de Gestão e de Avaliação) que agrupam Componentes de Controle, que por sua vez são detalhados em *Estandares* (fatores que compõem os componentes ou os meios de controle). Na Colômbia: Subsistemas de Controle, Componentes e Elementos de Controle. As partes, nos dois modelos, apesar de pequenas diferenças terminológicas, têm idêntico conteúdo. Nesse sentido é interessante notar que o Paraguai adotou a terminologia *estrutura de controle interno*, enquanto a Colômbia optou por *sistema de controle interno*.

As justificativas dos modelos, nos dois países, apresentam o propósito de melhorar o desempenho institucional dos órgãos e entidades públicos, mediante fortalecimento dos controles prévios e concomitantes a cargo das próprias autoridades administrativas incumbidas da gestão, que deverão, por essa razão, implantar e manter efetivos controles internos. Em ambos os casos, a responsabilidade pela implantação e pelo adequado funcionamento dos controles internos é atribuída à autoridade máxima de cada órgão ou entidade.

Vale destacar aqui um trecho da apresentação do modelo Colombiano (tradução nossa), por nos remeter a situações similares às existentes em nosso país e por enfatizar a importância de se adotar um modelo estrutural único de controle interno.

### *APRESENTAÇÃO*

*[...] ao se propor construir e desenvolver um Modelo Padrão de Controle Interno orientado às entidades do Setor Público Colombiano, com o fim de gerar novas possibilidades de abordagem para a implantação do controle interno no Estado e lograr o cumprimento dos princípios constitucionais de igualdade, moralidade, eficácia, economia, celeridade, imparcialidade e publicidade realizou-se, inicialmente, uma análise de ordem normativa, técnica e aplicativa de controle interno cujo resultado permitiria conhecer os elementos que tem impedido a adequada implementação deste suporte administrativo, fundamental à gestão do Estado.*



*As análises normativa e técnica revelaram que a lei 87 de 1993 estabeleceu os fundamentos básicos do controle interno ordenados pelos artigos 209 e 269 da Constituição, mas não os aspectos estruturais que permitam garantir uniformidade conceitual e técnica na implementação do sistema de controle interno. Apesar disso, a hierarquia jurídica que a Constituição e a lei outorgam ao controle interno lhe dá um valor inestimável ao considerá-lo como de cumprimento obrigatório para todas as entidades do Estado e provê a base constitucional e legal dos aspectos aplicativos do sistema.*

*As normas regulamentadoras da lei 87 de 1993, expedidas até esta data, têm considerado aspectos relacionados com as instâncias de articulação do Sistema, suas responsabilidades, o cumprimento das obrigações de informação, a criação de órgãos consultivos de controle interno, sem definir oficialmente, ainda, um marco de controle padrão que permita implementar e operar de maneira uniforme o Sistema de Controle Interno em todas as entidades do Estado.*

*A falta de uma estrutura única de controle interno, não contemplada na lei 87/93 e não desenvolvida completamente até hoje nos diferentes regulamentos expedidos, tem inibido a possibilidade de se estabelecer e implementar controle interno nas entidades públicas de maneira uniforme, com utilização de uma linguagem comum, padronizando uma estrutura básica de controle que, adaptada às características próprias de cada entidade pública, garanta o cumprimento de seus objetivos e, ao mesmo tempo, unifique critérios de controle do Estado, permita comparabilidade e decisões possíveis para seu melhoramento como um todo.*

*Isto pode ser observado, por exemplo, nos governos locais, onde os níveis de implementação de adequados sistemas de controle interno são baixos, já que a autonomia administrativa que a Constituição lhes confere tem impedido, em boa parte, a observância de diretrizes, guias e instruções expedidas pelo Governo Nacional, ao não existir uma norma superior que obrigue a sua aplicação. Adicionalmente, os poderes legislativo e judiciário, assim como os órgãos de controle externo, têm a competência de expedir suas próprias regulamentações, baseando-se na faculdade outorgada pela lei 87/93, nos conceitos básicos estabelecidos nesta lei, nas normas expedidas pelo Contador-Geral da Nação e nas normas que as regulam.*



*Esta falta de uniformidade, decorrente da inexistência de um marco de controle interno para as entidades do Estado, para se desenvolver e se implementar em cada entidade pública, de acordo com a sua função dentro do Estado e suas próprias características, afeta a falta de consistência conceitual, técnica e metodológica na hora de implementar o controle interno.*

*Se conclui, então, pela necessidade de se modificar a lei 87/93 para unir os conceitos básicos a um marco de controle que o torne aplicável, ou na sua falta, regulamentar uma estrutura de controle única que garanta obrigatoriedade, força vinculante e uniformidade em sua implantação e que, em respeito às características específicas de cada entidade pública, aborde a dispersão conceitual existente e facilite uma função administrativa do Estado com plena coordenação entre suas diferentes instâncias e níveis, uma administração transparente e efetiva no cumprimento de sua função.*

## VII.5. PERU

Em 1998, a Controladoria-Geral do Peru emitiu a resolução 72 (*Normas Técnicas de Control Interno para El Sector Público*), para ser marco de referência em matéria de controle interno. Em decorrência dessa resolução, a implementação dos controles nos órgãos e entidades públicos foi crescente e motivou a expedição de uma lei específica para regular o estabelecimento, funcionamento, manutenção, aperfeiçoamento e avaliação dos sistemas de controle interno das entidades do Estado, o que resultou na lei 28716/2006 (*Ley de Control Interno de las Entidades Del Estado*). Como o Peru é um estado unitário, essa lei tem aplicabilidade nacional.

A lei 28716/2006 estabelece que a Controladoria-Geral deverá editar as normas técnicas de controle para orientar a efetiva implantação e funcionamento do controle interno nas entidades do Estado. O art. 10 da lei determina que, a partir da edição, pela Controladoria, do marco técnico do controle interno, os titulares das entidades públicas estarão obrigados a emitir suas normas específicas, de acordo com a natureza e complexidade da entidade, em consonância com o marco editado pela Controladoria.



O marco técnico exigido pela lei foi aprovado pela resolução 320/2006, da Controladoria-Geral peruana, que optou por adotar, praticamente na íntegra, o modelo COSO. Os componentes do controle interno são definidos separada e detalhadamente nas *Normas Generales de Control Interno*, parte integrante da resolução 320/2006, em: a) ambiente de controle; b) avaliação de riscos; c) atividades de controle; d) informação e comunicação, e, e) supervisão (agrupando as atividades de prevenção e monitoramento).

A responsabilidade pelos controles internos é definida no *Capítulo II - Roles y Responsabilidades do Marco Conceitual da Estrutura de Controle Interno do Peru* e é atribuída aos diversos níveis hierárquicos, sendo o titular e todos os funcionários da entidade responsáveis pela implantação e supervisão dos controles internos, no entanto, é atribuído ao titular dos órgãos diretivos e executivos da entidade o dever de aprovar as disposições e ações necessárias para a implantação:

El titular, funcionarios y todo el personal de la entidad son responsables de la aplicación y supervisión del control interno, así como en mantener una estructura sólida de control interno que promueva el logro de sus objetivos, así como la eficiencia, eficacia y economía de las operaciones.

Para contribuir al fortalecimiento del control interno en las entidades, el titular o funcionario que se designe, debe asumir el compromiso de implementar los criterios que se describen a continuación: ...

## VII.6. ÁFRICA DO SUL

A previsão de implantação e manutenção de controles internos nos órgãos e entidades da administração pública da África do Sul tem origem constitucional e é repercutida em legislações esparsas, que estabelecem critérios e responsabilidades para tal.

Pela análise das normas a que tivemos acesso, percebe-se que os princípios básicos da *accountability* sul-africana são: conformidade, economicidade, desempenho (eficiência e efetividade), publicidade, análise de risco, controles internos, responsabilização e monitoramento (grifamos). Apesar de não consolidados em um único documento, a Auditoria-Geral da África do Sul imprime grande importância a esses princípios, o que pode ser observado pela presença constante nas normas que disciplinam a atuação desse órgão de controle.



As entidades e órgãos públicos sul-africanos, bem como os municípios, são obrigados a manter uma unidade de auditoria interna, que tem, entre outras, a atribuição de gerenciar riscos e avaliar os controles internos. Essa obrigação é encontrada em dispositivos específicos para cada órgão, entidade ou município, e esses regulamentam de forma semelhante a questão. A título de exemplo, citamos o dispositivo referente aos municípios, constante da Lei de Finanças Municipal (*Municipal Finance Management Act.*) (tradução e grifos nossos).

165. (1) Cada municipalidade e cada entidade municipal devem ter uma unidade de auditoria sujeita a esta subseção.

(2) A auditoria interna da municipalidade ou da entidade municipal deve:

(a) preparar um plano de auditoria baseado em risco e um programa de auditoria interna para cada ano fiscal;

(b) Assessorar o secretário de finanças do município e reportar ao comitê de auditoria sobre a implementação do plano de auditoria interna e sobre questões relacionadas a:

(I) auditoria interna;

(II) controles internos;

(III) procedimentos e práticas contábeis;

(IV) risco e gerenciamento de riscos;

(V) gerenciamento de desempenho;

(VI) controle de perdas; e,

(VII) conformidade com esta lei, a lei anual de Repasse de Receitas e qualquer outra legislação aplicável; e

(VIII) desempenhar quaisquer outras funções que lhe forem atribuídas pelo secretário de finanças municipal;

Identificamos que a Auditoria-Geral da África do Sul possui metodologia para avaliação de controles internos, no entanto não nos foi possível identificar manual ou modelo para implantação.

#### Manual do Auditor-Geral

Este aspecto da auditoria de regularidade não deve ser confundido com testes de controle que o auditor realiza para determinar a adequação e confiabilidade da contabilidade de uma entidade e de um sistema de controle interno. No entanto, é aceito que a não-conformidade com leis, normas e regulamentos terá impacto sobre a contabilidade e o sistema de controle interno, e vice-versa.



## **VIII. A REGULAÇÃO DE CONTROLES INTERNOS NO BRASIL**

Como já assinalamos anteriormente, a forma como a Constituição de 1988 dispôs sobre os sistemas de controle interno no setor público tem gerado, ao longo dos anos, certa confusão em relação à terminologia corrente sobre o assunto. Isso porque, nos artigos 31, 70 e 74 da CF/88, o constituinte mais se limitou a tipificar as finalidades e as características orgânicas do sistema de controle interno, e não apresentou – e não deveria fazê-lo – o conceito dessa importante atividade administrativa para a consecução dos resultados de uma gestão.

As normas infraconstitucionais que tratam de controle interno, tais como as leis 4.320/64, 8.666/93 e 10.180/01, a lei complementar 101/00 e o decreto-lei 200/67, também não deixam claro, como seria desejável, que o conjunto de políticas e procedimentos implementados por uma entidade com o intuito de auxiliar no alcance de seus objetivos não se confunde, apesar de homônimos, com o controle interno referente ao poder de autocontrole detido pela administração pública. Essa lacuna, como assinala Araújo (2006, p.2), tem feito com que, no âmbito de algumas unidades do sistema federativo brasileiro, ocorram tentativas de, por meio de legislação ordinária, apresentar conceitos de controle interno como, por exemplo, o decreto 14.271, de 21 de agosto de 2003, da Prefeitura Municipal de Porto Alegre:

Art. 3º Para fins deste Decreto considera-se:

I – **Controle Interno:** conjunto de métodos e processos adotados com a finalidade de comprovar atos e fatos, impedir erros e fraudes e otimizar a eficiência da Administração.

II – **Sistema de Controle Interno:** conjunto das atividades de controle exercidas pelas diversas unidades técnicas da Administração, organizadas e articuladas a partir de uma unidade central de coordenação.

III – **Auditória:** atividade de controle, realizada consoante normas e procedimentos de auditoria, que comprehende o exame detalhado, total, parcial ou pontual, dos atos administrativos e fatos contábeis com a finalidade de verificar se as operações foram realizadas de maneira apropriada e registradas de acordo com o aparato legal.

E mais, ao se tentar acoplar as finalidades do sistema de controle interno dos poderes constituídos ao conceito de controle interno inerente aos processos organizacionais, termina-se criando mais confusão conceitual, como demonstra o exemplo seguinte:



### **Do Conceito e das Garantias**

Art. 2º Entende-se por Sistema de Controle Interno Municipal o conjunto de normas, regras, princípios, planos, métodos e procedimentos que, coordenados entre si, têm por objetivo efetivar a avaliação da gestão pública e o acompanhamento dos programas e políticas públicas bem como, evidenciando sua legalidade e razoabilidade, avaliar os seus resultados no que concerne à economia, eficiência e eficácia da gestão orçamentária, financeira, patrimonial e operacional dos órgãos e entidades municipais.

No que diz respeito a controles internos sob o enfoque contábil, o Conselho Federal de Contabilidade expediu a resolução CFC 1.135/08, aprovando a NBC T 16.8 – Controle Interno, no âmbito das Normas Brasileiras de Contabilidade Aplicadas ao Setor Público. No entanto, em razão de sua origem, a norma restringe-se ao controle interno como suporte do sistema de informação contábil, no sentido de minimizar riscos e dar efetividade às informações da contabilidade.

Sobre o controle interno enfocado neste trabalho, encontramos a seguinte conceituação no Manual do Sistema de Controle Interno do Poder Executivo Federal, aprovado pela Instrução Normativa Nº 01, de 6/4/2001, da Secretaria Federal de Controle Interno (IN-SFC 1/2001):

#### **Seção VIII – Normas relativas aos controles internos administrativos**

[...]

2. Controle interno administrativo é o conjunto de atividades, planos, rotinas, métodos e procedimentos interligados, estabelecidos com vistas a assegurar que os objetivos das unidades e entidades da administração pública sejam alcançados, de forma confiável e concreta, evidenciando eventuais desvios ao longo da gestão, até a consecução dos objetivos fixados pelo Poder Público.  
(SFC 2001, p.67)

Essa conceituação é semelhante à encontrada no glossário do Roteiro de Auditoria de Conformidade do Tribunal de Contas da União:

Controles Internos - Conjunto de atividades, planos, métodos e procedimentos interligados utilizados com vistas a assegurar que os objetivos dos órgãos e entidades da administração pública sejam alcançados, de forma confiável e concreta, evidenciando eventuais desvios ao longo da gestão, até a consecução dos objetivos fixados pelo Poder Público. (TCU 2004, p.20)

Essas definições, apesar de abrangentes e pertinentes, não abarcam o conceito atual de controle interno enquanto sistema. Referem-se mais às atividades ou procedimentos de controle.



A IN-SFC 1/2001 declara que um dos objetivos fundamentais do Sistema de Controle Interno do Poder Executivo Federal é a avaliação desses controles internos administrativos implantados pelas unidades ou entidades sob exame. Todavia, para que isso efetivamente ocorra, é necessário que se estabeleça, normativamente, os padrões que serão utilizados para essa avaliação.

1. Um dos objetivos fundamentais do Sistema de Controle Interno do Poder Executivo Federal é a avaliação dos controles internos administrativos das unidades ou entidades sob exame. Somente com o conhecimento da estruturação, rotinas e funcionamento desses controles, podem os Órgãos/Unidades de Controle Interno do Poder Executivo Federal avaliar, com a devida segurança, a gestão examinada. (SFC 2001, p.67)

A IN-SFC 1/2001 indica, ainda, o objetivo geral e destaca alguns objetivos específicos do controle interno administrativo, enumera seus princípios e **define-o como um processo** no qual **“quanto maior for a adequação dos controles internos administrativos menor será a vulnerabilidade aos riscos inerentes à gestão propriamente dita.”** (destacamos):

#### **Finalidade do controle interno administrativo**

4. O objetivo geral dos controles internos administrativos é evitar a ocorrência de impropriedades e irregularidades, por meio dos princípios e instrumentos próprios, destacando-se entre os objetivos específicos, a serem atingidos, os seguintes:

- I. observar as normas legais, instruções normativas, estatutos e regimentos;
- II. assegurar, nas informações contábeis, financeiras, administrativas e operacionais, sua exatidão, confiabilidade, integridade e oportunidade;
- III. evitar o cometimento de erros, desperdícios, abusos, práticas antieconômicas e fraudes;
- IV. propiciar informações oportunas e confiáveis, inclusive de caráter administrativo/operacional, sobre os resultados e efeitos atingidos;
- V. salvaguardar os ativos financeiros e físicos quanto à sua boa e regular utilização e assegurar a legitimidade do passivo;
- VI. permitir a implementação de programas, projetos, atividades, sistemas e operações, visando à eficácia, eficiência e economicidade na utilização dos recursos; e
- VII. assegurar a aderência das atividades às diretrizes, planos, normas e procedimentos da unidade/entidade.



### **Processo de controle interno administrativo**

5. Os controles internos administrativos implementados em uma organização devem:

- I. prioritariamente, ter caráter preventivo;
- II. permanentemente, estar voltados para a correção de eventuais desvios em relação aos parâmetros estabelecidos;
- III. prevalecer como instrumentos auxiliares de gestão; e
- IV. estar direcionados para o atendimento a todos os níveis hierárquicos da administração.

6. Quanto maior for o grau de adequação dos controles internos administrativos, menor será a vulnerabilidade dos riscos inerentes à gestão propriamente dita.

### **Princípios de controle interno administrativo**

3. Constituem-se no conjunto de regras, diretrizes e sistemas que visam ao atingimento de objetivos específicos, tais como:

- I. relação custo/benefício - consiste na avaliação do custo de um controle em relação aos benefícios que ele possa proporcionar;
- II. qualificação adequada, treinamento e rodízio de funcionários - a eficácia dos controles internos administrativos está diretamente relacionada com a competência, formação profissional e integridade do pessoal. É imprescindível haver uma política de pessoal que contemple:
  - a) seleção e treinamento de forma criteriosa e sistematizada, buscando melhor rendimento e menores custos;
  - b) rodízio de funções, com vistas a reduzir/eliminar possibilidades de fraudes;
  - c) obrigatoriedade de funcionários gozarem férias regularmente, como forma, inclusive, de evitar a dissimulação de irregularidades.
- III. delegação de poderes e definição de responsabilidades - a delegação de competência, conforme previsto em lei, será utilizada como instrumento de descentralização administrativa, com vistas a assegurar maior rapidez e objetividade às decisões. O ato de delegação deverá indicar, com precisão, a autoridade delegante, delegada e o objeto da delegação. Assim sendo, em qualquer unidade/entidade, devem ser observados:



a) existência de regimento/estatuto e organograma adequados, onde a definição de autoridade e consequentes responsabilidades sejam claras e satisfaçam plenamente as necessidades da organização; e

b) manuais de rotinas/procedimentos, claramente determinados, que considerem as funções de todos os setores do órgão/entidade.

IV. segregação de funções - a estrutura das unidades/entidades deve prever a separação entre as funções de autorização/aprovação de operações, execução, controle e contabilização, de tal forma que nenhuma pessoa detenha competências e atribuições em desacordo com este princípio;

V. instruções devidamente formalizadas - para atingir um grau de segurança adequado é indispensável que as ações, procedimentos e instruções sejam disciplinados e formalizados através de instrumentos eficazes e específicos; ou seja, claros e objetivos e emitidos por autoridade competente;

VI. controles sobre as transações - é imprescindível estabelecer o acompanhamento dos fatos contábeis, financeiros e operacionais, objetivando que sejam efetuados mediante atos legítimos, relacionados com a finalidade da unidade/entidade e autorizados por quem de direito; e

VII. aderência a diretrizes e normas legais – o controle interno administrativo deve assegurar observância às diretrizes, planos, normas, leis, regulamentos e procedimentos administrativos, e que os atos e fatos de gestão sejam efetuados mediante atos legítimos, relacionados com a finalidade da unidade/entidade.

Apesar da inegável qualidade desse documento, que é a base conceitual das atividades de auditoria do órgão de controle do poder executivo federal, há que se reconhecer a necessidade de harmonização de conceitos e abordagens às referências mundiais aceitas atualmente, de modo a conceber um modelo lógico que forneça uma abordagem sistemática, organizada e estruturada como base para o desenvolvimento e avaliação de controles internos no setor público.

Ademais, em função da hierarquia da IN-SFC 1/2001 no nosso ordenamento normativo, ela não é norma que vincule todas as esferas e todos os entes da administração pública brasileira.

Contudo, a IN 1/2001 da Secretaria Federal de Controle, juntamente com os demais exemplos citados no decorrer desse trabalho, bem como as regulamentações brasileiras mencionadas a seguir, representam importantes referenciais para a definição de critérios gerais de controle interno, gestão de riscos e governança na administração pública e devem ser considerados na elaboração do anteprojeto de proposta legislativa sobre o assunto.



Embora as normas de controle interno no tocante ao setor público estejam merecendo novo disciplinamento, cumpre ressaltar que órgãos reguladores do governo, como o Banco Central (Bacen), a Comissão de Valores Mobiliários (CVM) e a Superintendência de Seguros Privados (Susep) têm tratada da mesma questão, no âmbito de suas competências regulatórias, em sintonia com o que há de mais atual em termos de referências internacionais.

A resolução 2.554/1998, do Bacen, por exemplo, se tornou um importante instrumento de gerenciamento de riscos e de governança corporativa, garantindo aos bancos brasileiros melhoria significativa em seus ambientes de controles. Ressalte-se que o Bacen antecipou-se em quatro anos ao advento da SOX, regulando o controle interno para as instituições financeiras numa abrangência muito maior, uma vez que alcança todo o ambiente organizacional, independente de ter ou não reflexo contábil, o que é um diferencial positivo em relação à regulação de outros países, fato que pode ter feito toda a diferença na recente crise financeira internacional.

Reproduzimos a seguir as principais disposições da resolução 2.554/98:

**Art. 1. Determinar as instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil a implantação e a implementação de controles internos voltados para as atividades por elas desenvolvidas, seus sistemas de informações financeiras, operacionais e gerenciais e o cumprimento das normas legais e regulamentares a elas aplicáveis.**

**Parágrafo 1. Os controles internos, independentemente do porte da instituição, devem ser efetivos e consistentes com a natureza, complexidade e risco das operações por ela realizadas.**

**Parágrafo 2. São de responsabilidade da diretoria da instituição:**

**I - a implantação e a implementação de uma estrutura de controles internos efetiva mediante a definição de atividades de controle para todos os níveis de negócios da instituição;**

**II - o estabelecimento dos objetivos e procedimentos pertinentes aos mesmos;**

**III - a verificação sistemática da adoção e do cumprimento dos procedimentos definidos em função do disposto no inciso II.**

**Art. 2º Os controles internos, cujas disposições devem ser acessíveis a todos os funcionários da instituição de forma a assegurar sejam conhecidas a respectiva função no processo e as responsabilidades atribuídas aos diversos níveis da organização, devem prever:**



- I - a definição de responsabilidades dentro da instituição;
- II - a segregação das atividades atribuídas aos integrantes da instituição de forma a que seja evitado o conflito de interesses, bem como meios de minimizar e monitorar adequadamente áreas identificadas como de potencial conflito da espécie;
- III - meios de identificar e avaliar fatores internos e externos que possam afetar adversamente a realização dos objetivos da instituição;
- IV - a existência de canais de comunicação que assegurem aos funcionários, segundo o correspondente nível de atuação, o acesso a confiáveis, tempestivas e compreensíveis informações consideradas relevantes para suas tarefas e responsabilidades;
- V - a contínua avaliação dos diversos riscos associados às atividades da instituição;
- VI - o acompanhamento sistemático das atividades desenvolvidas, de forma a que se possa avaliar se os objetivos da instituição estão sendo alcançados, se os limites estabelecidos e as leis e regulamentos aplicáveis estão sendo cumpridos, bem como a assegurar que quaisquer desvios possam ser prontamente corrigidos;
- VII - a existência de testes periódicos de segurança para os sistemas de informações, em especial para os mantidos em meio eletrônico.

Parágrafo 1º Os controles internos devem ser periodicamente revisados e atualizados, de forma a que sejam a eles incorporadas medidas relacionadas a riscos novos ou anteriormente não abordados.

Parágrafo 2º A atividade de auditoria interna deve fazer parte do sistema de controles internos.

Parágrafo 3º A atividade de que trata o parágrafo 2º quando não executada por unidade específica da própria instituição ou de instituição integrante do mesmo conglomerado financeiro, poderá ser exercida:

I - por auditor independente devidamente registrado na Comissão de Valores Mobiliários - CVM, desde que não aquele responsável pela auditoria das demonstrações financeiras;

II - pela auditoria da entidade ou associação de classe ou de órgão central a que filiada a instituição;



III - por auditoria de entidade ou associação de classe de outras instituições autorizadas a funcionar pelo Banco Central, mediante convenio, previamente aprovado por este, firmado entre a entidade a que filiada a instituição e a entidade prestadora do serviço.

Parágrafo 4º. No caso de a atividade de auditoria interna ser exercida por unidade própria, deverá essa estar diretamente subordinada ao conselho de administração ou, na falta desse, a diretoria da instituição.

Parágrafo 5º. No caso de a atividade de auditoria interna ser exercida segundo uma das faculdades estabelecidas no parágrafo 3º, deverá o responsável por sua execução reportar-se diretamente ao conselho de administração ou, na falta desse, a diretoria da instituição.

Parágrafo 6º. As faculdades estabelecidas no parágrafo 3º, incisos II e III, somente poderão ser exercidas por cooperativas de credito e por sociedades corretoras de títulos e valores mobiliários, sociedades corretoras de cambio e sociedades distribuidoras de títulos e valores mobiliários não integrantes de conglomerados financeiros.

Art. 3º. O acompanhamento sistemático das atividades relacionadas com o sistema de controles internos deve ser objeto de relatórios, no mínimo semestrais, contendo:

I - as conclusões dos exames efetuados;

II - as recomendações a respeito de eventuais deficiências, com o estabelecimento de cronograma de saneamento das mesmas, quando for o caso;

III - a manifestação dos responsáveis pelas correspondentes áreas a respeito das deficiências encontradas em verificações anteriores e das medidas efetivamente adotadas para saná-las.

Parágrafo único. As conclusões, recomendações e manifestação referidas nos incisos I, II e III deste artigo devem:

I - ser submetidas ao conselho de administração ou, na falta desse, a diretoria, bem como a auditoria externa da instituição;

II - permanecer a disposição do Banco Central do Brasil pelo prazo de 5 (cinco) anos.

Art. 4º. Incumbe a diretoria da instituição, alem das responsabilidades



enumeradas no art. 1º, parágrafo 2º, a promoção de elevados padrões éticos e de integridade e de uma cultura organizacional que demonstre e enfatize, a todos os funcionários, a importância dos controles internos e o papel de cada um no processo.

A resolução 3.380/2006 dispõe sobre a implementação de estrutura de gerenciamento do risco operacional e faz parte das normas de implantação do Basileia II no Brasil<sup>7</sup>:

Art. 3º A estrutura de gerenciamento do risco operacional deve prever:

- I - identificação, avaliação, monitoramento, controle e mitigação do risco operacional;
- II - documentação e armazenamento de informações referentes às perdas associadas ao risco operacional;
- III - elaboração, com periodicidade mínima anual, de relatórios que permitam a identificação e correção tempestiva das deficiências de controle e de gerenciamento do risco operacional;
- IV - realização, com periodicidade mínima anual, de testes de avaliação dos sistemas de controle de riscos operacionais implementados;
- V - elaboração e disseminação da política de gerenciamento de risco operacional ao pessoal da instituição, em seus diversos níveis, estabelecendo papéis e responsabilidades, bem como as dos prestadores de serviços terceirizados;
- VI - existência de plano de contingência contendo as estratégias a serem adotadas para assegurar condições de continuidade das atividades e para limitar graves perdas decorrentes de risco operacional;
- VII - implementação, manutenção e divulgação de processo estruturado de comunicação e informação.

§ 1º A política de gerenciamento do risco operacional deve ser aprovada e revisada, no mínimo anualmente, pela diretoria das instituições de que trata o art. 1º e pelo conselho de administração, se houver.

Art. 6º A atividade de gerenciamento do risco operacional deve ser executada por unidade específica nas instituições mencionadas no art. 1º.

Parágrafo único. A unidade a que se refere o caput deve ser segregada da unidade executora da atividade de auditoria interna, de que trata o art. 2º da Resolução 2.554, de 24 de setembro de 1998, com a redação dada pela Resolução 3.056, de 19 de dezembro de 2002.

<sup>7</sup> Fonte: <http://www.bcb.gov.br/nor/basileia/BasileiaInaweb.pdf> (acesso em 24/03/2009)



## **IX. CONCLUSÃO E PROPOSTA DE ENCAMINHAMENTO**

O presente estudo demonstrou que a obrigatoriedade de implantar, manter e avaliar controle interno já está incorporada no ordenamento jurídico de diversos países pesquisados, como é o caso dos Estados Unidos da América (e neste o da unidade federada de Nova York), do Chile, Paraguai, Peru, da Colômbia e África do Sul.

O estudo demonstrou, também, que os países pesquisados adotam modelos de controle interno convergentes, calcados em gerenciamento de riscos e em estruturas de governança e que esses modelos têm por base os principais documentos relacionados à gestão de riscos e controles internos reconhecidos internacionalmente, como o COSO I/II, o padrão AS/NZS 4360 (base da ISO 31000 – Princípios e Diretrizes para Gerenciamento de Riscos, com previsão de publicação para outubro de 2009) e as Diretrizes para as Normas de Controle Interno do Setor Público, da Intosai. Esta última, emitida por um organismo autônomo, independente e apolítico que congrega 189 entidades de fiscalização superior de diversos países e atua com status de consultor especial do Conselho Econômico e Social (ECOSOC) das Nações Unidas.

Apesar do consenso atual de que controles internos devem ser ferramentas de gestão e monitoração de riscos em relação ao alcance de objetivos de um modo geral, e não mais dirigidos apenas para riscos de origem financeira ou vinculados a resultados escriturais, o seu regramento jurídico, em alguns países, tem sido agasalhado nas leis que tratam de finanças, orçamentos ou de órgãos públicos de controle como, por exemplo, em leis orgânicas de controladorias-gerais.

Peru e Colômbia editaram leis específicas regulando, de forma exaustiva, a elaboração, aprovação, implantação, funcionamento, aperfeiçoamento e avaliação de controle interno nas entidades do Estado. O primeiro editou a Lei 28716 de 2006 - *Lei de Controle Interno das Entidades do Estado*, regulamentada por resolução de sua Controladoria-Geral. O segundo, a Lei 87 de 1993, que *estabelece normas para o exercício do controle interno nos órgãos e entidades do Estado*, regulamentada por Decretos Nacionais. O Paraguai introduziu controles internos por meio da *Lei Orgânica da Controladoria Geral da República*. O Chile trata do controle interno em diversas normas esparsas e no Canadá o assunto não é objeto de lei específica.

Os demais países analisados adotaram a prática de estabelecer os requisitos gerais em normas de hierarquia superior, deixando para os órgãos superiores de gestão e/ou de controle a competência para estabelecer os padrões de implantação e as diretrizes para avaliação de controles internos, pelos demais órgãos e entidades. Assim fez os Estados Unidos, cujo Congresso optou por



alterar a *Lei de Contabilidade e Auditoria*, de 1950, para nela incluir uma seção obrigando entidades e órgãos públicos a estabelecer controle interno de acordo com padrões prescritos pelo GAO (órgão de controle externo americano) e a realizar avaliações contínuas e relatórios periódicos sobre sua adequação de acordo com as diretrizes estabelecidas pelo OMB (órgão de gestão e orçamento) em consulta com o GAO. A lei, após a inclusão da nova seção, passou a denominar-se oficialmente *Lei Federal de Integridade na Gestão Financeira* (FMFIA).

A solução adotada pelo Congresso americano muito se assemelha à que se estuda para o caso brasileiro, pois aqui também se pensa em tratar do controle interno como um capítulo da Lei 4.320, de 1964, que trata de normas gerais de direito financeiro, contabilidade e orçamento público. No entanto, a nova feição do controle interno, ampliada para integrar responsabilidades quanto à gestão de riscos e suportar estruturas de governança permite-nos vislumbrar como mais apropriado sua incorporação à Lei de Responsabilidade Fiscal (LRF), já que esta foi elaborada para atender às expectativas da sociedade brasileira, na busca pela responsabilidade e pelo bom uso dos recursos públicos na consecução dos objetivos do Estado.

No que diz respeito à adoção de um modelo e sua disposição no ordenamento jurídico, haveremos de considerar a experiência, até agora inconclusa em alguns entes da federação, quanto à implantação de órgãos de controle interno, seja por dificuldades conceituais, técnicas ou de outras naturezas, como, por exemplo, as relacionadas a problemas de autonomia. Desse modo, entendemos que a norma superior deve contemplar bases consistentes para estruturação de um modelo de controle interno, dentre as quais destacamos:

- uniformizar a definição de controle interno, definir seus objetivos e elementos e declarar os princípios relacionados ao processo de gestão de riscos, controles internos e governança institucional;
- estabelecer responsabilidades e papéis de gestores e demais servidores em relação ao desenho, implementação e monitoramento do controle interno, incluindo obrigações de certificação, reporte de deficiências e planos de ação para corrigi-las e disponibilização de informações às partes interessadas da cadeia de governança afeta à instituição; e
- atribuir competência a um comitê para estabelecer ou homologar um modelo nacional de padrões para controle interno, e aos órgãos de controle interno e externo no que diz respeito às diretrizes para avaliação e certificação de sistemas de controle interno.

O estabelecimento de um modelo nacional de padrões para controle interno, conforme



proposição do último item acima, deverá considerar atributos que permitam sua utilização por entidades de qualquer porte, com adaptação às peculiaridades de cada entidade, em consistência com a natureza e complexidade das operações por elas realizadas e com os riscos a elas associados. Deve-se, pois, procurar identificar nos modelos mencionados neste estudo as características mais aderentes à realidade nacional, considerada em seus três níveis de governo, sem perda da perspectiva de um modelo integrado que induza a autogestão de riscos e controles e otimize as ações no sentido de:

- assegurar a consecução de objetivos estratégicos, a continuidade e a sustentabilidade institucional, com a devida consideração aos objetivos correlatos de obediência aos princípios constitucionais da administração pública e ao alcance dos objetivos do sistema de controle interno;
- permitir a identificação, de modo objetivo, de fatores de risco e vulnerabilidades existentes em processos e sistemas organizacionais e no seu ambiente externo;
- melhorar a compreensão de riscos, controles internos e governança institucional, com a devida consideração para planos de ação e seu acompanhamento;
- dimensionar e desenvolver controles internos adequados, na proporção requerida pelos riscos que eles devam mitigar, eliminando controles caros e ineficientes e otimizando a relação custo-benefício; e
- fortalecer a responsabilidade da administração no que diz respeito a implantar, manter e avaliar estruturas de gestão de riscos, controles internos e governança institucional.

Ante o exposto, submetemos o presente estudo à consideração superior, propondo que, inicialmente, ele seja submetido à consulta de especialistas e unidades técnicas deste Tribunal e, após a incorporação de eventuais sugestões recebidas, o seu envio, por intermédio da Presidência da Corte, ao Exmo. Senador Renato Casagrande.

Brasília, 11 de julho de 2009

**ANTONIO ALVES DE CARVALHO NETO**  
Auditor Federal de Controle Externo  
Diretor de Métodos e Procedimentos de Controle

**LIA DE CASTRO SILVA**  
Auditora Federal de Controle Externo  
Matrícula TCU 4777-5



## X. ANEXO - ANTEPROJETO DE PROPOSTA LEGISLATIVA

### PROJETO DE LEI DO SENADO N° , DE 2009

Acrescenta seção à Lei Complementar nº 101, de 4 de maio de 2000, que estabelece normas de finanças públicas voltadas para a responsabilidade na gestão fiscal e dá outras providências, a fim de dispor sobre critérios gerais de gestão de riscos, controle interno e governança na administração pública da União, dos Estados, do Distrito Federal e dos Municípios.

**O PRESIDENTE DA REPÚBLICA** Faço saber que o Congresso Nacional decreta e eu sanciono a seguinte Lei Complementar:

Art. 1º A Lei Complementar nº 101, de 4 de maio de 2000, passa a vigorar com acréscimo da seguinte Seção ao CAPÍTULO IX;

#### CAPÍTULO IX

#### DA TRANSPARÊNCIA, CONTROLE E FISCALIZAÇÃO

[...]

#### Seção VII

##### Da Gestão de Riscos, do Controle Interno e da Governança Institucional

**Art. 59-A.** Os órgãos e entidades da Administração Pública, direta e indireta, de qualquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios deverão implantar, manter, monitorar e revisar controles internos institucionais, tendo por base a identificação, avaliação e gerenciamento de riscos que possam impactar a consecução dos objetivos estabelecidos pelo Poder Público.

§ 1º Controle interno institucional é o processo integrado levado a efeito pela alta administração, por todos os que exerçam cargos executivos de direção e gerência e por todos os demais colaboradores do órgão ou da entidade públicos, estruturado para enfrentar riscos e prover razoável certeza de que, na consecução de suas missões institucionais, os princípios constitucionais da administração pública serão obedecidos e os seguintes objetivos do controle interno serão alcançados:

I – alinhamento das ações aos objetivos estratégicos, dando suporte à missão, à continuidade e à sustentabilidade institucional;

II – eficiência, eficácia e efetividade operacional, mediante execução ordenada, ética e econômica das operações;

III – integridade e confiabilidade da informação produzida e sua disponibilidade para a tomada de decisões e para o cumprimento de obrigações de transparência e prestação de contas;

IV – conformidade com as leis e regulamentos aplicáveis, incluindo normas, políticas, programas, planos e procedimentos de governo e da própria instituição;

V – adequada salvaguarda e proteção de bens, ativos e recursos públicos contra desperdício, perda, mau uso, dano, utilização não autorizada ou apropriação indevida.



§ 2º O controle interno baseia-se no gerenciamento de riscos e integra o processo de gestão; sua estrutura é constituída dos seguintes componentes inter-relacionados:

- I – ambiente institucional
- II – fixação de objetivos
- III – identificação de eventos
- IV – avaliação de riscos
- V – resposta a riscos
- VI – atividades de controle
- VII – informação e comunicação
- VIII – monitoramento

§ 3º Os componentes do controle interno e do gerenciamento de riscos aplicam-se a todos os níveis, unidades e dependências do órgão ou da entidade pública.

§ 4º Os dirigentes máximos dos órgãos e entidades devem assegurar que procedimentos efetivos de gerenciamento de riscos façam parte de seus controles internos.

§ 5º Controle interno institucional adequado é o que tem presente e em funcionamento todos os componentes indicados no § 2º, deve ser integrado ao processo de gestão, dimensionado e desenvolvido na proporção requerida pelos riscos, de acordo com a natureza, complexidade, estrutura e missão do órgão ou da entidade pública.

**Art. 59-B.** Comitê constituído por representantes indicados pelos órgãos superiores de controle interno e externo e de planejamento e gestão das três esferas de governo e Poder, pelos Conselhos Nacionais de Justiça e do Ministério Público, pelo Ministério da Fazenda e pelo Ministério de Planejamento, Orçamento e Gestão, em número máximo de vinte e cinco membros, sob coordenação do último, desenvolverá um Modelo Nacional de Padrões para Controle Interno, que auxilie gestores públicos a conceber, implantar, monitorar e certificar sistemas de controle interno institucionais, de forma ordenada, lógica e prática, contemplando pelo menos:

I – estrutura conceitual: bases conceituais, principiológicas, legais, técnicas e metodológicas para uma correta compreensão da estrutura de controle interno e dos papéis e responsabilidades de todos os envolvidos, incluindo a administração do órgão/entidade, gestores e demais colaboradores, auditoria interna e externa, nesta compreendida os órgãos do sistema de controle interno de Poder e os órgãos de controle externo, conselhos de administração, fiscal e de políticas públicas, comitês de auditoria e de controle interno, dentre outros agentes da governança institucional;

II – estrutura de controle interno: conjunto de componentes, elementos e partes constitutivas do modelo de controle, seus inter-relacionamentos e integrações, conceitos e finalidades; e

III – manual de implementação: recomendações de normas, metodologias, técnicas, ferramentas e orientações necessárias para revisão, desenho, implantação, manutenção e monitoramento de adequados sistemas de controle interno institucionais, consideradas as normas profissionais de controle interno, as práticas de organizações públicas e privadas, as normas nacionais e internacionais e os modelos que representem as melhores práticas em matéria de gestão de riscos, controle interno e governança.

§ 1º O desenvolvimento do modelo integrado a que se refere este artigo observará requisitos que induzam a autogestão de riscos e controles e otimize ações no sentido de:

I – assegurar a consecução de objetivos estratégicos, a continuidade e a sustentabilidade institucional, com a devida consideração aos objetivos correlatos de obediência aos princípios constitucionais da administração pública e ao alcance dos objetivos do sistema de controle interno, conforme estabelecido no § 1º do art. 59-A;



II – permitir a identificação e a avaliação de fatores de risco e vulnerabilidades, de fontes internas e externas, de modo objetivo e tecnicamente consistente;

III – melhorar a compreensão de riscos, controles internos e governança institucional, estimulando a adoção de boas práticas no seu gerenciamento;

IV – dimensionar e desenvolver controles internos adequados, na proporção requerida pelos riscos, eliminando controles caros e ineficientes, maximizando a relação custo-benefício e suprimindo os que se revelarem puramente formais;

V – fortalecer a responsabilidade da administração no que diz respeito a estabelecer, manter e monitorar sistemas de controle interno integrados por procedimentos efetivos de gerenciamento de riscos, com a devida consideração para planos de ação de aperfeiçoamento e correção de deficiências;

§ 2º O Comitê a que se refere o caput terá prazo de até um ano, contado a partir da data de publicação da lei complementar que introduzir os dispositivos dessa seção, para instituir o modelo nele previsto, ficando os órgãos e entidades públicos obrigados à sua adoção em idêntico prazo, contado a partir da data de instituição do modelo.

§ 3º Enquanto não for instituído o modelo previsto no caput, os órgãos e entidades públicos observarão, no mínimo, as disposições constantes do § 1º do art. 59-C.

**Art. 59-C.** A responsabilidade por estabelecer, manter, monitorar e aperfeiçoar o controle interno institucional é do gestor máximo do órgão ou da entidade, sem prejuízo das responsabilidades, em seus respectivos âmbitos de atuação, dos executivos de direção, gestores departamentais, de processos organizacionais e de programas de governo. Aos demais funcionários incumbem-se responsabilidades não apenas quanto à sua observância, mas também quanto à identificação de deficiências e sua comunicação às instâncias superiores.

§ 1º Todo órgão ou entidade pública, sob responsabilidade dos agentes mencionados no caput, deverão implementar, manter e, quando for o caso, documentar pelo menos os seguintes aspectos relativos ao controle interno:

I – estabelecimento de objetivos e metas, tanto gerais como específicos, de planos necessários ao seu alcance, e acompanhamento por indicadores e métodos confiáveis de avaliação de gestão;

II – adoção de estrutura organizacional compatível à execução das atribuições institucionais, livre de arranjos que impliquem conflitos de interesse, com delimitação precisa dos níveis de autoridade e responsabilidade;

III – estabelecimento de políticas e práticas de recursos humanos sedimentadas por valores éticos, sistema de méritos e sanções e por mecanismos de incentivo à capacitação e atualização profissional;

IV – definição de políticas como guia para decisões e ações, e de procedimentos para execução de processos organizacionais finalísticos, gerenciais e de apoio, observados os princípios de simplificação e atualização;

V – edição de normas para proteção e utilização racional de recursos, incluindo disposições contra desperdício, perda, mau uso, dano, utilização não autorizada ou apropriação indevida;

VI – adoção de sistemas adequados de informação e comunicação organizacional que facilitem o processo de gestão e de controle interno, e de mecanismos e instrumentos de comunicação informativa que facilitem o controle social e público da instituição;

VII – implementação, ou justificativa à não implementação, de determinações e/ou recomendações resultantes de auditorias e avaliações de controle procedidas por órgãos de controle interno ou externo ou por unidade do sistema de controle interno institucional;



VIII – monitoramento sistemático, pelo gestor máximo do órgão ou entidade, e acompanhamento contínuo pelos demais responsáveis, dos aspectos mínimos de controle interno referidos nos incisos anteriores, documentando as revisões periódicas efetuadas e as deficiências constatadas.

§ 2º O dirigente máximo de cada órgão ou entidade deve, anualmente, com base em avaliação realizada de acordo com diretrizes estabelecidas pelo Comitê a que se refere o art. 59-B, elaborar declaração certificando se o sistema de controle interno institucional está ou não em conformidade com os requisitos estabelecidos. Caso a certificação não seja de conformidade plena, as deficiências significativas deverão ser reportadas, bem como os planos de ação e cronogramas para corrigi-las.

§ 3º A certificação de que trata o parágrafo anterior deverá integrar as contas anuais e será objeto de pronunciamento por parte do órgão de controle interno de Poder quanto à adequação da avaliação efetuada pela Administração para dar suporte a sua certificação da eficácia dos controles internos.

§ 4º As entidades que fizerem uso de auditorias independentes deverão prever que esta é responsável por certificar a avaliação efetuada pela Administração para suportar a certificação da eficácia dos controles internos.

§ 5º Avaliações em separado ou específicas, quando realizadas no exercício, serão reportadas nas contas anuais com indicação das deficiências significativas identificadas, das determinações e/ou recomendações dos órgãos de controle e respectivos planos de ação e cronogramas para implementá-las.

§ 6º Ações e planos de ação são de responsabilidade do gestor, podendo ser adotadas soluções alternativas às eventualmente recomendadas pelo órgão ou unidade de controle, se mais adequadas, convenientes, oportunas e resultarem mais favoráveis.

**Art. 59-D.** A auditoria interna do órgão ou entidade é parte do seu sistema de controle interno e deverá ser implementada levando-se em conta a relação custo-benefício e outros fatores relevantes, com as atribuições previstas em lei e a função de avaliar os controles internos, identificar suas falhas, fazer recomendações para corrigi-las e acompanhar sua implementação, não lhe cabendo a incumbência de estabelecer estratégias para gerenciamento de riscos ou controles internos para mitigá-los, mas avaliar a qualidade desses processos, que são de responsabilidade dos gestores.

§ 1º A auditoria interna deve reportar-se funcionalmente ao Comitê de Auditoria, ao Conselho de Administração ou ao Conselho Fiscal ou, na falta destes, à autoridade máxima do órgão ou entidade, assegurando-lhe efetiva independência, neutralidade, objetividade e imparcialidade.

§ 2º A avaliação do controle interno institucional pela auditoria interna deve ser devidamente documentada e conter informações suficientes para subsidiar a certificação prevista no § 2º do art. 59-C.

**Art. 59-E.** A unidade de controle interno do órgão ou entidade é parte da própria gestão e do sistema de controle interno e deverá ser implementada levando-se em conta a relação custo-benefício e outros fatores relevantes, com a função de assessorar gestores na identificação e avaliação de riscos, na definição de estratégias para gerenciá-los e no estabelecimento de controles internos adequados para mitigá-los, cabendo-lhe, ainda, monitorar o sistema de controle interno por meio de atividades contínuas e autoavaliações pontuais, em separado ou específicas.

Parágrafo único. Nos órgãos ou entidades que não disponham de auditoria interna, as avaliações realizadas pela unidade de controle interno poderão ser utilizadas para subsidiar a certificação prevista no § 2º do art. 59-C, devendo para isto observar os requisitos previstos no parágrafo único do art. 59-D.

**Art. 59-F.** A governança institucional consiste na adoção de práticas, instrumentos e mecanismos consubstanciados nos princípios da boa gestão pública, que assegurem equilíbrio de interesses e redução de hiatos informacionais entre agentes e partes interessadas, tendo por postulado básico a aferição do adequado exercício da delegação pública outorgada à instituição, da boa e regular aplicação dos recursos disponibilizados para o cumprimento dessa delegação, do cumprimento das atribuições e dos objetivos estabelecidos pelo Poder Público, e inclui:



I – transparéncia, representada pelo processo de contínua demonstração, pelo gestor público, de que sua gestão está alinhada à delegação recebida, não se limitando à obrigação de apenas informar, mas cultivando o desejo de informar;

II – equidade, representada pelo tratamento justo e igualitário de todas as partes interessadas, sendo inaceitáveis atitudes ou políticas discriminatórias, sob qualquer pretexto;

III – responsabilização por parte de todos os agentes e responsabilidade integral por todos os atos praticados no exercício das delegações recebidas em todos os níveis da governança institucional;

IV – responsabilidade institucional, representada pela adoção de políticas que assegurem a máxima sustentabilidade da instituição, incorporando considerações de ordem ética, social e ambiental em todos os processos e relacionamentos.

**Art. 59-G.** As entidades públicas sujeitas à regulação específica sobre sistemas de controle interno, gestão de riscos e governança, observarão as disposições emanadas dos respectivos órgãos reguladores e, no que lhes for aplicável, o disposto na presente seção.

**Art. 59-H.** As entidades privadas que recebam transferências do setor público, a qualquer título, para execução de ações de caráter público, inclusive das entidades da administração indireta, estão sujeitas às disposições desta seção, devendo, aquelas de menor porte, atender, no mínimo, ao disposto no § 1º do art. 59-C.

**Art. 59-I.** O não atendimento do disposto nesta seção sujeita o órgão ou a entidade pública doente à sanção prevista no inciso I do § 3º do art. 23.

Art. 2º Para viabilizar a implementação do disposto nesta Lei Complementar, aplicar-se-á, no que couber, a assistência técnica e cooperação financeira a que se refere o art. 64, da Lei Complementar nº 101, de 4 de maio de 2000.

Art. 3º Esta Lei Complementar entra em vigor na data de sua publicação.

Brasília,

## **JUSTIFICAÇÃO**

Os noticiários nacionais estão cheios de expressões como caos na saúde pública, ensino negligenciado, sistema penitenciário falido, insegurança etc. Não por acaso, ao lado de tais notícias, outras nos dão conta de desvios de verbas públicas, fraudes, conluios, superfaturamento, obras paralisadas, atos de gestão secretos, dentre inumeráveis outras ocorrências, a demonstrar que a gestão pública em nosso país padece de vulnerabilidades e deficiências significativas em seus sistemas de gestão de riscos, controles internos e governança.

A administração pública brasileira tem sido alvo de intensos e renovados questionamentos quanto à sua capacidade de alcançar objetivos de políticas públicas, implantar programas e prover serviços públicos com qualidade, eficiência, eficácia, obtendo resultados efetivos.



Os cidadãos clamam por uma gestão pública de melhor desempenho, dotada de práticas gerenciais modernas, focadas no alcance de objetivos, capazes de gerar melhor retorno aos tributos arrecadados e de agregar, efetivamente, mais valor para a sociedade. E mais, que tudo isso seja feito de tal maneira que se possa acompanhar e aferir o que está ocorrendo no interior da coisa pública.

A pergunta que talvez se deseje fazer nesse ponto é: mas o que tudo isso tem a ver com gestão de riscos, controles internos e governança? – A resposta é: tudo!

Os elevados índices de ineficiência nos serviços públicos e de desvios, fraudes e malversação do patrimônio público é um sinal de que a administração pública brasileira, em todos os níveis, está vulnerável a essas ocorrências, e que sua gestão de riscos e seus controles internos são frágeis, inexistentes ou ineficazes para combatê-las. E quando controles internos no setor público são incapazes de atingir seus objetivos, as consequências atingem toda a sociedade, em especial, as camadas mais carentes que dependem exclusivamente dos serviços oferecidos pelo Estado, revelando a pior face da má gestão pública.

Todavia, controle interno não é panaceia que, por si só, evitará que todos esses problemas sejam resolvidos, até mesmo em função de suas limitações inerentes, já que sistemas de controle interno são estabelecidos para governar os acontecimentos dentro da organização, que tenham o potencial de impactar na consecução de seus objetivos, isto é, os riscos. Em outras palavras, controle interno é a fiscalização das atividades feita pela própria entidade, ou seja, pelo seu corpo funcional e pela sua própria administração. Mas, e a fiscalização da administração da entidade é feita por quem?

A resposta a essa pergunta e a convicção de que boas estruturas de gestão de riscos e de controles internos são pré-requisitos para uma organização bem administrada, mas não suficientes para reduzir a incerteza dos membros da sociedade sobre o que acontece no interior da administração pública, nos levou a contemplar no presente projeto a questão da governança.

Para aumentar a confiança da sociedade sobre a forma como são geridos os recursos colocados à disposição das organizações públicas para dar cumprimento às delegações que lhes são outorgadas, é necessário que, juntamente com a gestão de riscos e controles internos, se plante as bases para uma boa governança pública, de modo a permitir a aferição, por todas as partes interessadas, do bom e regular cumprimento das atribuições e dos objetivos estabelecidos pelo Poder Público.



Assim, entendemos conveniente tratar, de forma integrada a governança, a gestão de riscos e o controle interno, objetivando o estabelecimento de um ambiente que respeite não apenas os valores, interesses e expectativas da instituição e dos agentes que a compõem, mas também de todas as partes que nela tenham interesses, tendo o cidadão e a sociedade como os vetores principais desse processo.

Organizações ao redor do mundo, inclusive do setor público em diversos países, vêm se adaptando ao ambiente de mudanças contínuas, vivenciado nos últimos anos, mediante a adoção de **estruturas de governança** e práticas administrativas fortemente calcadas no **gerenciamento de riscos** que possam impedir ou dificultar a realização de suas missões e o alcance de seus objetivos, estabelecendo estruturas ou **sistemas de controle interno** capazes de responder adequadamente aos riscos identificados e, assim, garantir razoável certeza quanto ao alcance de seus objetivos, à consecução de suas missões e, por conseguinte, à continuidade e sustentabilidade de seus negócios.

A Organização Internacional de Entidades Fiscalizadoras Superiores (Intosai), um organismo autônomo, independente e apolítico que congrega 189 entidades fiscalização superior de diversos países e atua com status de consultor especial do Conselho Econômico e Social (ECOSOC) das Nações Unidas, em documentos publicados nos recentes anos de 2004 e 2007, recomenda a adoção de padrões de controle interno fortemente calcados no gerenciamento de riscos e em modelos de governança corporativa.

Um estudo realizado em conjunto pela KPMG e pelo Governo Federal Canadense, no ano de 1999, abrangendo 228 publicações sobre o tema e entrevistas com dezoito organizações, sendo seis do setor público de países desenvolvidos, como os do Oeste Europeu, a Austrália, a Nova Zelândia e E.U.A., demonstrou que as organizações públicas obtiveram muitos benefícios com a implementação do gerenciamento de riscos, em relação aos seus processos de gestão. O principal deles foi o grande auxílio na realização de objetivos organizacionais. Outros benefícios foram:

- a) maior foco nas prioridades do negócio, ou seja, não precisaram redirecionar recursos para a resolução de problemas. Ademais, ações tomadas para prevenir e reduzir perdas, ao invés de explicar o fato depois - configuraram uma efetiva estratégia de risco;
- b) mudança cultural de aceitar a discussão dos riscos e a informação sobre potenciais danos, tolerar erros (mas não erros ocultos) e aprender com eles;
- c) melhor gestão operacional e financeira, ao garantir que os riscos sejam adequadamente



considerados no processo de tomada de decisão, resultando em uma prestação de serviços mais eficiente e efetiva. Por outro lado, ao anteciparem-se aos problemas, gerentes têm maiores oportunidades para reagir e tomar ações;

- d) fortalecimento do processo de planejamento e o auxílio na identificação de oportunidades; e
- e) no curto prazo, o aumento da *accountability* da gestão, e no longo prazo, o aumento das capacidades gerenciais, de forma geral.

Pelo exposto é possível concluir que o gerenciamento de risco é um processo necessário, lógico e sistemático, para as organizações identificarem e avaliarem riscos e oportunidades, visando melhorar a tomada de decisões e a avaliação de desempenhos. Tem uma visão para o futuro, isto é, não apenas evita ou minimiza perdas, mas lida positivamente com oportunidades. Constitui, portanto, uma poderosa ferramenta para os gestores do setor público.

Ao acoplar à gestão de riscos, os critérios gerais para um bom sistema de controle interno e as bases para o estabelecimento de uma boa governança nas instituições públicas, este projeto fecha o ciclo integrado de um modelo de governança, riscos e controles, cuja implementação poderá trazer benefícios incomensuráveis para o Estado e a sociedade brasileira.

Assim, por acreditar que a presente iniciativa é conveniente, oportuna e indutora de melhorias na gestão e no controle público, inclusive favorecendo a participação do cidadão e da sociedade civil organizada nesses processos, esperamos contar com o valioso apoio dos nobres pares, em favor de sua aprovação nesta Casa.

Sala das Sessões,

**Senador RENATO CASAGRANDE**



## REFERÊNCIAS

- ABNT. Associação Brasileira de Normas Técnicas. Projeto 63.000:01-001 NBR ISO 31000:2009 Gestão de riscos – Princípios e Diretrizes. Brasil, Ago. 2009.
- ANTUNES, Jerônimo. Contribuição ao estudo da avaliação de risco e controles internos na auditoria de demonstrações contábeis no Brasil. Dissertação (Mestrado em Contabilidade e Controladoria). Faculdade de Economia, Administração e Contabilidade da Universidade de São Paulo - USP, São Paulo, 1998.
- ARAÚJO, Inaldo da Paixão Santos. **Controle interno municipal: uma nova visão**. Brasil, 2006. Disponível em <<http://www.consultoriadinamica.com.br/controleinterno.doc>>. Acesso em 21 abr. 2009.
- AUSTRALIA. *AS/NZS 4360 Risk Management*. Standards Australia. Sydney, 1999.  
\_\_\_\_\_. *Guidelines for managing risk in the Australian and New Zealand public sector HB143*. Standards Australia, Sydney, 1999.
- BERNARDINELLI, Mario Luiz; BRACALENTI, Fernando; DINOFRE, Marcelo; PEREIRA, Eduardo Martins. **COSO – The Committee of Sponsoring Organizations of the Treadway Commission**. Disponível em <[www.infosegura.eti.br](http://www.infosegura.eti.br)>. Acesso em 21 abr. 2009.
- BRASIL. BCB - Banco Central do Brasil. Resolução nº 2.554/1998. Disponível em <<http://www.cosif.com.br/mostra.asp?arquivo=r2554>>. Acesso em 19 abr. 2009.
- \_\_\_\_\_. \_\_\_\_\_. Resolução nº 3.380/2006. Disponível em <<https://www3.bcb.gov.br/normativo/detalharNormativo.do?N=106196825&method=detalharNormativo>>. Acesso em 19 abr. 2009.
- \_\_\_\_\_. SFC - Secretaria Federal de Controle Interno. Instrução Normativa nº 01, de 6 de abril de 2001. **Manual do Sistema de Controle Interno do Poder Executivo Federal**. Brasília, 2001. Disponível em: <[http://www.cgu.gov.br/Legislacao/Arquivos/InstrucoesNormativas/IN01\\_06abr2001.pdf](http://www.cgu.gov.br/Legislacao/Arquivos/InstrucoesNormativas/IN01_06abr2001.pdf)>. Acesso em 19 abr. 2009.
- \_\_\_\_\_. TCU - Tribunal de Contas da União. **Roteiro de Aplicação da Metodologia de Análise de Risco para Escolha de Temas de Fiscalização**. Brasília, 2003. Documento não publicado (uso interno do TCU).
- \_\_\_\_\_. \_\_\_\_\_. **Portaria TCU nº 122/2004**. Aprova a primeira revisão do Roteiro de Auditoria de Conformidade. Brasília, 2004. Disponível em: <<https://contas.tcu.gov.br/juris/Web/Juris/ConsultarAtoNormativo/ConsultarAtoNormativo.faces>>. Acesso em 19 abr. 2009.
- \_\_\_\_\_. \_\_\_\_\_. **Instrução Normativa nº 57/2008**. Estabelece normas de organização e apresentação dos relatórios de gestão e dos processos de contas da administração pública federal. Brasília, 2008. Disponível em: <<https://contas.tcu.gov.br/juris/Web/Juris/ConsultarAtoNormativo/ConsultarAtoNormativo.faces>>. Acesso em 19 abr. 2009.



CANADÁ. *Financial Administration Act (Consolidation of this Act)*. Disponível em <<http://www.gov.pe.ca/law/statutes/pdf/f-09.pdf>>. Acesso em 21 abr. 2009.

\_\_\_\_\_. *Federal Government Spending: a priori and a posteriori Control Mechanism*. Parliamentary Information and Research Service, Library of Parliament, Feb. 2006. Disponível em <<http://www.parl.gc.ca/information/library/PRBpubs/prb0550-e.html>>. Acesso em 21 abr. 2009.

\_\_\_\_\_. *OAG. Office of the Auditor General of Canada. The Advancing Audit Practices Project (AAPP)*. Disponível em <[http://www.oag-bvg.gc.ca/internet/English/meth\\_gde\\_e\\_29350.html](http://www.oag-bvg.gc.ca/internet/English/meth_gde_e_29350.html)>. Acesso em 21 abr. 2009.

CHILE. Ley 10.336 de Organización y Atribuciones de la Contraloría General de la República.

<[http://www.contraloria.cl/NewPortal/portal2>ShowProperty/BEA%20Repository/portalCGR/Documentos/Documentos\\_de\\_Interes/DOI\\_01LEY\\_N10336](http://www.contraloria.cl/NewPortal/portal2>ShowProperty/BEA%20Repository/portalCGR/Documentos/Documentos_de_Interes/DOI_01LEY_N10336)>. Acesso em 21 abr. 2009.

\_\_\_\_\_. Ley Nº 18956/1990 de Reestructuración del Ministerio de Educación Pública. Disponível em <<http://www.alfabetizacion.fundacionsantillana.org/paginas/leg.asp?id=4>>. Acesso em 21 abr. 2009.

COBIT – Control Objectives for Information and Related Technology. *Cobit 4.1 – Executive Summary Framework*. United States of America: IT Governance Institute, 2007. Disponível em <<http://www.itgi.org>>. Acesso em 21 abr. 2009.

COCURULLO, Antonio. **Gestão de Riscos Corporativos: riscos alinhados com algumas ferramentas de gestão: um estudo de caso no setor de celulose e papel**. Dissertação (mestrado). Universidade São Francisco - USF, 3. ed. São Paulo, 2004.

COLÔMBIA. **Constitución Política De Colombia**. Disponível em <[http://web.presidencia.gov.co/constitucion/index\\_06102009.pdf](http://web.presidencia.gov.co/constitucion/index_06102009.pdf)>. Acesso em 21 abr. 2009.

\_\_\_\_\_. Ley Nº 87 de 1993, in *Sistema de Control Interno para Entidades del Estado – Marco Conceptual – Versión I*. USAID - The U.S. Agency for International Development/CASALS. Agència de los Estados Unidos para El Desarrollo Internacional. 1. ed. Bogotá, 2004.

COIMBRA, Fábio. **Riscos Operacionais: estrutura para gestão em bancos**. São Paulo: Saint Paul Editora, 2008.

COSO – Committe Of Sponsoring Organizations of the Treadway Commission (Org.). *Internal Control – Integrated Framework*. Executive Summary. United States of America: COSO, 1992. Disponível em <[www.coso.org/IC-IntegratedFramework-summary.htm](http://www.coso.org/IC-IntegratedFramework-summary.htm)>. Acesso em 21 abr. 2009.

\_\_\_\_\_. **Gerenciamento de Riscos Corporativos – Estrutura Integrada**. Sumário Executivo: Estrutura. PriceWatherhouseCoopers – COSO - Audibra. Nov. 2006

\_\_\_\_\_. **Gerenciamento de Riscos Corporativos – Estrutura Integrada**. Técnicas de Aplicação. PriceWatherhouseCoopers – COSO - Audibra. Nov. 2006

DAVIS, Marcelo David; BLASCHEK, José Roberto de Souza. **Deficiências dos sistemas de controle interno governamentais atuais em função da evolução da economia**. In: 6º Congresso USP de Controladoria e Contabilidade. São Paulo: Universidade de São Paulo, 27 e 28 jul. 2006.



Disponível em: <<http://www.congressoeac.locaweb.com.br/artigos62006/1.pdf>>. Acesso em 21 abr. 2009.

DIAMOND, Jack. *The role of Internal Audit in Government Financial Management: An international perspective*. IMF Working Paper, Washington, WP/02/94, 35p, 2002. Disponível em: <<http://www.imf.org/external/pubs/ft/wp/2002/wp0294.pdf>>. Acesso em 24 de jul. 2005.

FEBRABAN – Federação Brasileira dos Bancos; Deloitte Touche Tohmatsu. Metodologia de Auditoria Interna com foco em riscos. São Paulo: IBCB, 2003.

IFAC. *International Federation of Accountants. Governance in the Public Sector: A Governing Body Perspective. International Public Sector Study13*. Aug. 2001. <<http://www.ifac.org>>. Acesso em 19 de abr. 2009.

IIA. *The Institute of Internal Auditors. Práticas para o Exercício Profissional da Auditoria Interna*. Tradução: FREIRE, José Juarez de Paula, CIA, São Paulo: Audibra, 2004

INTOSAI. *Guidelines for Internal Controls Standards for the Public Sector*. 2004. Disponível em: <<http://intosai.connexcc-hosting.net/blueline/upload/1guicspubsece.pdf>>. Acesso em 21 abr. 2009.

INTOSAI. *Guidelines for Internal Controls Standards for the Public Sector. Further Information on Entity Risk Management. PSC Subcommittee on Internal Control Standards*. 2007. Disponível em: <<http://psc.rigsrevisionen.dk/composite-218.htm>>. Acesso em 21 abr. 2009.

LIOTTO, Ari Marcelo. Gerenciamento de Risco. A aderência da metodologia do TCU à metodologia COSO. Monografia (Pós-graduação em Controle Externo - Área Auditoria Governamental). Instituto Serzedello Corrêa - ISC, Brasília, 2004.

MANZI, Vanessa Alessi. **Compliance no Brasil: consolidação e perspectivas**. São Paulo: Saint Paul Editora, 2008.

McNAMEE, David; SELIM, Georges. *The next step in risk management*. The Internal Auditor; Jun; 56, 3; ABI/INFORM Global pg. 35. 1999.

PERU. Ley Nº 28716 *Ley de Control Interno de las entidades del Estado*. Disponível em <[http://www.inen.sld.pe/portal/documentos/pdf/normas\\_legales/leyes\\_y\\_decretos/Ley\\_N\\_28716.pdf](http://www.inen.sld.pe/portal/documentos/pdf/normas_legales/leyes_y_decretos/Ley_N_28716.pdf)>. Acesso em 21 abr. 2009.

\_\_\_\_\_. *Resolución Nº 72 Normas Técnicas de Control Interno para El Sector Público*. Contraloría General de la República. Disponível em <<http://www.contraloria.gob.pe/index.htm>>. Acesso em 21 abr. 2009.

PETERS, Marcos. **Implantando e gerenciando a lei Sarbanes Oxley: Governança corporativa agregando valor aos negócios**. São Paulo, Atlas, 2007.

PARAGUAY. Contraloría General de la República. **Modelo estándar de control interno para las entidades publicas del Paraguay - MECIP**. Asunción, 2008.

\_\_\_\_\_. **Ley nº 1.535/1999 de Administración Financiera del Estado**. Disponível em <[http://www.leyes.com.py/todas\\_disposiciones/1999/leyes/ley\\_1535\\_99.php](http://www.leyes.com.py/todas_disposiciones/1999/leyes/ley_1535_99.php)>. Acesso em 19 abr.2009.



\_\_\_\_\_. Ley nº 276/1994 Orgánica y Funcional de la contraloría General de la República.

Disponível em

<[http://www.cej.org.py/games/Leyes\\_por\\_Materia\\_juridica/ADMINISTRATIVO/LEY%20276.pdf](http://www.cej.org.py/games/Leyes_por_Materia_juridica/ADMINISTRATIVO/LEY%20276.pdf)>. Acesso em 19 abr.2009.

SILVA, W. M. **Composição do Conselho de Administração e suas Implicações para o Desempenho Financeiro**. Prêmio IBGC de Monografias em Governança Corporativa 2003. Disponível em <<http://www.ibgc.org.br/ibConteudo.asp?IDArea=332&IDp=10>>. Acesso em 19 abr.2009.

SOUTH AFRICA. **The Municipal Finance Management Act No. 56 of 2003 (MFMA)**. Disponível em <<http://www.agsa.co.za/Portals/1/ACTS/MFMA.pdf>>. Acesso em 21 abr. 2009.

UNITED STATES. **Federal Managers Financial Integrity Act of 1982. September 8, 1982**. Disponível em <[http://www.whitehouse.gov/omb/financial\\_fmfia1982/](http://www.whitehouse.gov/omb/financial_fmfia1982/)>. Acesso em 19 abr.2009.

\_\_\_\_\_. **GAO. U.S. Government Accountability Office. GAO/AIMD-00-21.3.1 Standards for Internal Control in the Federal Government**. Nov. 1999. Disponível em <<http://www.gao.gov/special.pubs/ai00021p.pdf>>. Acesso em 19 de abr. 2009.

\_\_\_\_\_. **GAO-01-1008G Internal Control Management and Evaluation Tool**. Aug. 2001. Disponível em <<http://www.gao.gov/new.items/d011008g.pdf>>. Acesso em 19 de abr. 2009.

\_\_\_\_\_. **New York State Governmental Accountability. Audit and Internal Control Act**. 1987. Disponível em <[http://www.whitehouse.gov/omb/rewrite/circulars/a123/a123\\_rev.html](http://www.whitehouse.gov/omb/rewrite/circulars/a123/a123_rev.html)>. Acesso em 19 de abr. 2009.

\_\_\_\_\_. **OMB Circular A-123 Management's Responsibility for Internal Control**. Dec 21, 2004. Disponível em <[http://www.whitehouse.gov/omb/rewrite/circulars/a123/a123\\_rev.html](http://www.whitehouse.gov/omb/rewrite/circulars/a123/a123_rev.html)>. Acesso em 19 de abr. 2009.

**USAID-The U.S. Agency for International Development/CASALS. Sistema de Control Interno para Entidades del Estado – Marco Conceptual – Versión I**. 1. ed. Bogotá, 2004.

VIEIRA, Cleiton. **O controle interno nas câmaras municipais, segundo a Lei de Responsabilidade Fiscal**. Disponível em: <[http://www.bnmes.gov.br/clientes/federativo/bf\\_bancos/e0001565.pdf](http://www.bnmes.gov.br/clientes/federativo/bf_bancos/e0001565.pdf)>. Acesso em 19 abr. 2009.

WALLACE, Wanda A. **Handbook of Internal Accounting Controls**. 2. Ed. New Jersey, USA: Prentice-Hall, Inc. Englewood Cliffs, 1991.



**CRITÉRIOS GERAIS DE CONTROLE INTERNO NA ADMINISTRAÇÃO PÚBLICA**  
**UM ESTUDO DOS MODELOS E DAS NORMAS DISCIPLINADORAS EM DIVERSOS PAÍSES**

**DESPACHO**

Considerando que este trabalho foi preliminarmente submetido à consulta e incorpora as sugestões recebidas de especialistas deste Tribunal, conforme proposta à fl.55, encaminhe-se o presente estudo à I. Presidência da Corte, para envio ao Exmo. Senador Renato Casagrande, por intermédio da Assessoria Parlamentar.

Brasília-DF, 10 de agosto de 2009.

**MARCELO LUIZ SOUZA DA EIRA**  
Secretário-Geral de Controle Externo, em substituição