GRUPO I – CLASSE V – Plenário
TC 023.050/2013-6
Natureza: Relatório de Auditoria
Órgãos/Entidades: Empresa Brasileira de Infraestrutura Aeroportuária (Infraero), Eletrobras Eletronuclear, Ministério da Justiça (MJ), Ministério da Educação (MEC), Agência Nacional de Águas (ANA), Instituto Nacional de Colonização e Reforma Agrária (Incra), Hospital de Clínicas de Porto Alegre (HCPA), Tribunal Regional Eleitoral do Rio Grande do Sul (TRE-RS), Companhia de Geração Térmica de Energia Elétrica (CGTEE), Universidade Federal de Pernambuco (UFPE), Tribunal Regional Eleitoral de Pernambuco (TRE-PE), Tribunal Regional Federal da 5ª Região (TRF/5ª), Banco do Nordeste do Brasil S.A. (BNB), Tribunal Regional do Trabalho da 7ª Região (TRT/7ª), Universidade Federal do Ceará (UFC), Companhia Docas do Estado de São Paulo S.A. (Codesp), Instituto Nacional de Pesquisas Espaciais (INPE), Tribunal Regional Eleitoral de São Paulo (TRE-SP), Universidade Federal do Paraná (UFPR), Universidade Tecnológica Federal do Paraná (UTFPR), Tribunal Regional do Trabalho da 9ª Região (TRT/9), Fundação Universidade do Amazonas (UFAM), Superintendência da Zona Franca de Manaus (Suframa), Amazonas Distribuidora de Energia S.A., Banco Central do Brasil (BCB), Companhia Hidroelétrica do São Francisco (Chesf), Petróleo Brasileiro S.A (Petrobras).
Advogado constituído nos autos: Polyanna Ferreira Silva Vilanova (OAB/DF 19.273) e outros, peça 23.

SUMÁRIO: FISCALIZAÇÃO DE ORIENTAÇÃO CENTRALIZADA (FOC). GOVERNANÇA DE TI. RECOMENDAÇÕES. ARQUIVAMENTO.

## Relatório

Trata-se de auditorias realizadas em diversos órgãos e entidades da Administração Pública federal com o objetivo de avaliar a implementação dos controles de TI informados em resposta ao levantamento do perfil de governança de TI de 2012, bem como verificar a implementação de controles e processos de governança e gestão de TI para assegurar a entrega de resultados de TI alinhados aos objetivos de negócio das instituições, gerenciando os riscos de TI existentes.

2. Foram auditados diversos órgãos e entidades das mais diversas áreas de atuação da Administração Pública, sendo que para cada um deles foi exarado um acórdão, em que foram descritos os achados e as recomendações propostas.

3. Transcrevo a seguir excerto do relatório consolidado, que sistematizou os resultados de todo esse trabalho, elaborado pela Sefti (peça 19):

> "1. INTRODUÇÃO
>
> 1.1 Origem da FOC

18. Desde 2007, o Tribunal de Contas da União (TCU) vem coletando informações sobre a situação da governança de tecnologia da informação (TI) junto às organizações que integram a estrutura da Administração Pública Federal (APF). Nesse período, O TCU já realizou três levantamentos dessa natureza (2007, 2010 e 2012) e, após cada um deles, promoveu fiscalizações de orientação centralizada (FOC) com vistas a averiguar, em um subconjunto de organizações públicas federais, se a situação informada pelos gestores corresponde à realidade da instituição avaliada.

19. A primeira FOC, que culminou no Acórdão 2.471/2008-TCU-Plenário, tinha como foco a avaliação de aspectos relacionados à terceirização de TI. O segundo trabalho objetivou avaliar a gestão e o uso da TI, resultando no Acórdão 1.233/2012-TCU-Plenário.

20. Após a realização dessas duas fiscalizações, a Secretaria de Fiscalização de Tecnologia da Informação (Sefti) do TCU, alinhada à atual diretriz desta Corte de Contas que prioriza a melhoria da governança pública no país, entendeu que era preciso avançar na avaliação dos mecanismos de governança e de gestão de TI que suportam a geração de resultados para a APF, bem como da gestão dos riscos de TI envolvidos nesse processo. Ademais, considerou-se que era necessário contribuir para o aprimoramento das perguntas relacionadas a esses dois temas no levantamento de governança de TI, realizado pelo TCU em 2014.

1.2 Visão geral

21. A governança de TI, segundo a ABNT NBR ISO/IEC 38500 (item 1.6.3), é o sistema pelo qual o uso atual e futuro da TI é dirigido e controlado. O IT *Governance Institute* (ITGI) — organismo internacional responsável por pesquisas sobre práticas e percepções globais de governança de TI para a comunidade — estabelece que "a governança de TI é de responsabilidade dos executivos e da Alta Direção, consistindo em aspectos de liderança, estrutura organizacional e processos que garantam que a área de TI da organização suporte e aprimore os objetivos e as estratégias da organização".

22. Esse tema tem sido explorado pelo TCU, de forma mais específica, por meio de levantamentos realizados para avaliar a situação de governança de TI. Além disso, diversas ações têm sido executadas no sentido de disseminar, além dos resultados e boas práticas identificados, os conceitos tratados nesses trabalhos, de forma a destacar a importância da governança de TI para a Administração Pública Federal (APF).

23. O primeiro levantamento, realizado em 2007, contou com a participação de 255 organizações, resultando no Acórdão 1.603/2008-TCU-Plenário. O segundo levantamento, organizado em 2010, avaliou 301 organizações, culminando no Acórdão 2.308/2010-TCU-Plenário. Por fim, o terceiro levantamento, realizado em 2012, avaliou 350 organizações, dando origem ao Acórdão 2.585/2012-TCU-Plenário.

24. De modo geral, as informações obtidas nos levantamentos de governança de TI realizados pelo TCU visam à identificação dos pontos mais vulneráveis da governança de TI na APF, à orientação da atuação do TCU como indutor do processo de aperfeiçoamento da governança de TI, bem como ao auxílio na identificação de bons exemplos e modelos a serem disseminados.

25. O presente trabalho foi dividido em duas fases. Na primeira, foi avaliado, em 24 organizações públicas federais, um subconjunto dos mecanismos questionados no âmbito do levantamento do perfil de governança de TI, bem como a existência de ações e processos voltados à melhoria da governança de TI na organização. A seguir estão discriminadas as organizações auditadas nessa fase.

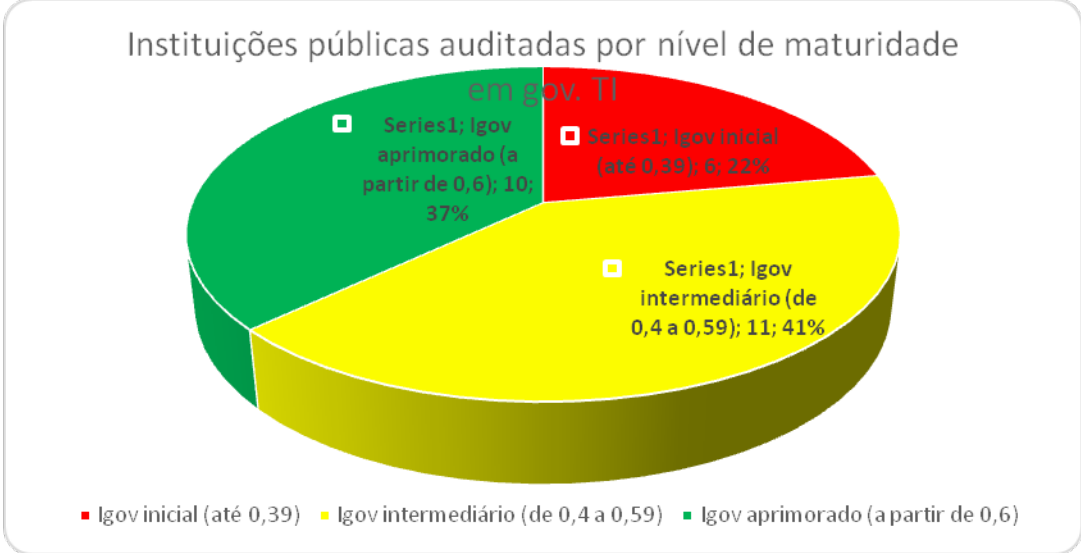
| Secex | Nome | TC |
|---|---|---|
| Sefti | Agência Nacional de Águas | 021.444/2013-7 |

| | | |
|---|---|---|
| Secex-AM | Amazonas Distribuidora de Energia S/A | 021.790/2013-2 |
| Secex-CE | Banco do Nordeste do Brasil S.A. | 015.047/2013-0 |
| Secex-RS | Companhia de Geração Térmica de Energia Elétrica | 021.471/2013-4 |
| Secex-SP | Companhia Docas do Estado de São Paulo S.A. | 020.348/2013-4 |
| Sefti | Eletrobras Termonuclear S.A. | 013.420/2013-5 |
| Sefti | Empresa Brasileira de Infraestrutura Aeroportuária | 032.366/2013-2 |
| Secex-AM | Fundação Universidade Federal do Amazonas | 021.792/2013-5 |
| Secex-RS | Hospital de Clínicas de Porto Alegre | 021.468/2013-3 |
| Sefti | Instituto Nacional de Colonização e Reforma Agrária | 021.445/2013-3 |
| Secex-SP | Instituto Nacional de Pesquisas Espaciais | 020.349/2013-0 |
| Sefti | Ministério da Educação | 014.038/2013-7 |
| Sefti | Ministério da Justiça | 021.447/2013-6 |
| Secex-AM | Superintendência da Zona Franca de Manaus | 021.789/2013-4 |
| Secex-CE | Tribunal Regional do Trabalho 7ª Região/CE | 019.168/2013-6 |
| Secex-PR | Tribunal Regional do Trabalho 9ª Região/PR | 021.899/2013-4 |
| Secex-PE | Tribunal Regional Eleitoral/PE | 015.166/2013-9 |
| Secex-RS | Tribunal Regional Eleitoral/RS | 021.469/2013-0 |
| Secex-SP | Tribunal Regional Eleitoral/SP | 020.346/2013-1 |
| Secex-PE | Tribunal Regional Federal 5ª Região | 022.074/2013-9 |
| Secex-PE | Universidade Federal de Pernambuco | 022.075/2013-5 |
| Secex-CE | Universidade Federal do Ceará | 019.131/2013-5 |
| Secex-PR | Universidade Federal do Paraná | 013.788/2013-2 |
| Secex-PR | Universidade Tecnológica Federal do Paraná | 021.908/2013-3 |

26. Já na segunda fase, procedeu-se à avaliação, em seis organizações públicas (sendo que três foram auditadas também na primeira fase), de temas vinculados à entrega de resultados e à gestão de riscos de TI. A relação de organizações auditadas nessa fase é apresentada a seguir:

| Secex | Nome | TC |
|---|---|---|
| Sefti | Banco Central do Brasil | 023.048/2013-1 |
| Secex-CE | Banco do Nordeste do Brasil S.A. | 025.849/2013-1 |
| Secex-PE | Companhia Hidroelétrica do São Francisco | 025.148/2013-3 |
| Secex-SP | Companhia Docas do Estado de São Paulo S.A. | 025.639/2013-7 |
| Secex-RS | Hospital de Clínicas de Porto Alegre | 025.684/2013-2 |
| Sefti | Petróleo Brasileiro S.A. | 024.827/2013-4 |

27. A figura a seguir apresenta a distribuição das organizações auditadas por nível de maturidade em governança de TI segundo o iGovTI, índice calculado pelo TCU, em 2012:




1.3 Critérios de auditoria

28. O conjunto de critérios que embasaram as auditorias realizadas no âmbito desta FOC incluiu dispositivos constitucionais, legais e infralegais, bem como acórdãos do TCU relacionados aos temas de governança e de gestão de TI. Também foram utilizados como critérios o guia Cobit 5, da *Information Systems Audit and Control Association* (Isaca); as normas NBR ISO/IEC 27002:2005 (NBR 27002), 20000-2:2008 (NBR 20000-2), 38500:2009 (NBR 38500), 31000:2009 (NBR 31000) e 15999-1:2007 (NBR 15999-1); o Código de Melhores Práticas de Governança Corporativa do Instituto Brasileiro de Governança Corporativa (IBGC); e o Guia de Elaboração de Plano Diretor de Tecnologia da Informação (PDTI) do Sistema de Administração dos Recursos de Tecnologia da Informação (Sisp).

1.4 Objetivos

29. Os objetivos da fiscalização podem ser organizados em duas etapas, uma vez que a FOC foi estruturada com base em duas fases distintas.

30. A primeira fase consistiu em um conjunto de 24 auditorias que visavam a avaliar a implementação dos controles de TI informados em resposta ao questionário do perfil de governança de TI em 2012, bem como a verificar a adoção de planos e estratégias para implementação e melhoria da governança de TI.

31. Os objetivos específicos dessa fase consistiram em:

a) aumentar a expectativa de controle em relação ao preenchimento correto e fidedigno de informações por parte das organizações participantes do levantamento do perfil de governança de TI realizado pelo TCU;

b) avaliar e fomentar o estabelecimento de um sistema de governança pelas organizações participantes do perfil GovTI 2012;

c) analisar o nível de implantação dos processos de governança e de gestão de TI que foram informados pelos auditados durante o levantamento do perfil GovTI 2012;

d) identificar oportunidades para aperfeiçoamento do questionário de levantamento de governança de TI.

32. Já a segunda fase consistiu em um novo conjunto de seis fiscalizações que tinham o propósito de avaliar as práticas utilizadas pelas áreas de TI para entregarem resultados alinhados aos objetivos de negócio, considerando os riscos de TI envolvidos.

33. Os objetivos específicos da segunda fase foram:

a) avaliar processos de governança sobre resultados e gestão de TI diretamente ligados à entrega de resultados e gestão de riscos de TI;

b) aprimorar os questionamentos relativos à dimensão de resultados do levantamento do perfil de governança de TI realizado periodicamente pelo TCU;

c) manter a expectativa de controle sobre contratações de bens e serviços de TI.

1.5 Escopo

34. Fazem parte do escopo das auditorias que compuseram a 1ª fase da FOC um subconjunto dos itens do questionário aplicado no levantamento de governança de TI realizado pelo TCU em 2012, agrupados em temas conforme detalhado a seguir:

a) Governança corporativa – gestão da ética, políticas corporativas e comitê de direção estratégica;

b) Governança de TI – processo de aprimoramento da governança de TI, comitê de TI, desempenho da gestão e uso de TI e atuação da auditoria interna na avaliação de temas de TI;

c) Estratégias e planos – planejamento estratégico institucional, planejamento estratégico de TI e planejamento diretor de TI (PDTI);

d) Gestão de pessoal de TI – quadro gerencial de TI, força de trabalho em TI e plano de capacitação em gestão de TI;

e) Processos de TI e segurança da informação (SI) – gestão de nível de serviço de TI, gestão de continuidade dos serviços de TI, gestão de ativos, política de controle de acesso, conscientização e treinamento em SI, política de SI, comitê de SI, gestão de incidentes em SI, gestão de riscos em SI, planejamento e gestão de contratos de TI.

35. Na 2ª fase da FOC, que tinha o foco na avaliação de entrega de resultados mediante adequada gestão dos riscos de TI envolvidos, foram avaliados os seguintes temas: alinhamento entre o setor de TI e o negócio da instituição, gestão de orçamento de TI, gestão de custos de TI, gestão de resultados de TI, retorno sobre investimento em TI, gestão de riscos de TI e contratações de soluções TI orientadas à entrega de resultados.

1.6 Estratégia metodológica

36. Para a realização deste trabalho, foram seguidos os normativos institucionais que tratam das fiscalizações no âmbito do TCU, em especial os documentos intitulados "Manual de Auditoria Operacional", aprovado pela Portaria-Segecex 4, de 26/2/2010; "Orientações para fiscalizações de Orientação Centralizada", aprovado pela Portaria-Adplan 2, de 23/8/2010; e "Normas de Auditoria do TCU" (NAT), aprovada por meio da Portaria-TCU 280, de 8/12/2010, posteriormente alterada pela Portaria-TCU 168, de 30/6/2011.

37. Durante a fase de planejamento da FOC, a unidade técnica orientadora dos trabalhos definiu as questões e os procedimentos de auditoria com base na legislação, na jurisprudência do TCU e em *frameworks* de boas práticas dos temas a serem avaliados. Como resultado dessa etapa, foram geradas matrizes de planejamento padrão para cada uma das fases do trabalho, cujos conteúdos foram transmitidos por meio de *workshops* às equipes de auditoria das unidades executoras da FOC.

38. Cabe ressaltar que, durante a execução da 2ª fase da FOC, foi utilizado o sistema "Pesquisar" do TCU para coletar a percepção dos gestores das principais áreas de negócio das organizações auditadas quanto aos serviços prestados pelo setor de TI. Para cada unidade de negócio pesquisada, solicitou-se, a cada um dos seus respectivos chefes, o preenchimento de questionário eletrônico com o objetivo de se avaliar a contribuição do setor de TI para o seu negócio, em especial em relação à participação da TI no alcance dos seus resultados.

39. Ainda nessa fase, no que diz respeito às contratações de soluções de TI, utilizou-se os seguintes critérios para seleção dos contratos a serem auditados: materialidade dos recursos envolvidos, criticidade do objeto para a instituição e características dos objetos contratados.

Além disso, buscou-se levantar, por meio de questionário com perguntas predominantemente abertas, quais são as principais dificuldades enfrentadas na aplicação do modelo de contratações de soluções de TI que privilegie a entrega de resultados verificáveis em detrimento da alocação de mão de obra, em conformidade com a jurisprudência desta Corte de Contas.

40. Para cada uma das trinta fiscalizações que compuseram a FOC, as unidades executoras encaminharam os relatórios de auditoria preliminares para que os gestores das organizações auditadas apresentassem comentários a respeito dos conteúdos desses relatórios, conforme previsto no parágrafo 185 do Manual de Auditoria Operacional e considerando o disposto nos parágrafos 145 e 146 das Normas de Auditoria do TCU. Esses comentários, apresentados sobre as conclusões e propostas constantes do relatório preliminar, foram incorporados e considerados na versão final do respectivo relatório de auditoria.

41. No que diz respeito à consolidação, é dever ressaltar que os resultados das auditorias na Universidade Federal do Paraná, no Tribunal Regional do Trabalho da 9ª Região e na Universidade Tecnológica Federal do Paraná (TCs 013.788/2013-2, 021.899/2013-4 e 021.908/2013-3) não compõem esta consolidação, tendo em vista que tais fiscalizações não produziram os resultados esperados, conforme registrou o Ministro-Relator nos votos condutores dos acórdãos 1.110/2014, 1.112/2014 e 1.113/2014, todos do Plenário do TCU. Ademais, a fiscalização realizada no âmbito da primeira fase no Hospital das Clínicas de Porto Alegre (TC 021.468/2013-3) também não teve os seus resultados consolidados, já que, durante a execução da consolidação, o processo ainda estava na Secex-RS, unidade técnica responsável pelo trabalho. Ao final da elaboração desse relatório todos os trabalhos integrantes da FOC já haviam sido julgados pelo Plenário do TCU.

1.7 Diretrizes seguidas no planejamento

42. Foram observadas as seguintes diretrizes no planejamento da FOC:

a) o resultado dos trabalhos deveria apresentar visão sistêmica da gestão de resultados de TI feita pelas organizações fiscalizadas considerando os riscos de TI envolvidos nesse processo;

b) a fiscalização deveria balancear abrangência e profundidade das questões de auditoria, por meio de uma abordagem iterativa e incremental;

c) a Sefti forneceria suporte metodológico a todos os participantes.

**Estratégia de condução**

43. O trabalho foi realizado em cinco etapas, a saber:

a) 1ª etapa – Planejamento da FOC;

b) 2ª etapa – Execução de Auditorias Piloto;

c) 3ª etapa – Auditorias da primeira fase da FOC (verificação do perfil de governança de TI);

d) 4ª etapa – Auditorias da segunda fase da FOC (avaliação das práticas de gestão de resultados e de riscos de TI);

e) 5ª etapa – Consolidação.

1 ª etapa – Planejamento da FOC

44. Em síntese, o planejamento da FOC consistiu em quatro etapas: seleção dos processos e controles de TI questionados no levantamento Perfil GovTI 2012 que seriam verificados na primeira fase do trabalho; seleção dos temas ligados à gestão de resultados e riscos de TI que seriam avaliados na segunda fase da FOC; convite às secretarias de controle externo dos estados para participarem da FOC; e seleção das organizações públicas que seriam fiscalizadas.

45. Seis secretarias de controle externo do TCU nos estados atenderam ao convite feito pela Sefti (Secex-AM, Secex-CE, Secex-PE, Secex-PR, Secex-RS, Secex-SP).

46. A fim de alcançar os objetivos delineados nas duas fases da FOC, foram adotados diversos critérios para escolha das organizações públicas auditadas, tais como:

a) divisão proporcional das organizações em função do respectivo setor no Perfil GovTI 2012 (Sistema de Administração dos Recursos de Tecnologia da Informação – Sisp, Departamento de Coordenação e Governança das Empresas Estatais – Dest, Poder Judiciário, entre outros);

b) organizações que apresentassem os maiores índices de governança de TI, mas cuja efetiva situação ainda era desconhecida;

c) organizações de reconhecida governança de TI que poderiam ser objeto das fiscalizações específicas, que abordariam temas relativos à gestão de resultados e riscos, a partir dos quais poderiam ser identificadas boas práticas nesses segmentos;

d) organizações que apresentaram expressivo crescimento no índice de governança de TI de um levantamento a outro;

e) organizações situados nas zonas de maior risco segundo o critério adotado no perfil de governança que realiza um mapeamento de orçamento *versus* índice de governança;

f) evitar a seleção de organizações que foram objeto de recentes fiscalizações sobre o tema ou que terão contas instruídas pela Sefti em 2013;

g) compatibilização da seleção de organizações que atendam aos critérios anteriores com a inclusão de unidades da federação cuja secretaria de controle externo aderiu à FOC;

h) organizações com fiscalizações determinadas ou sugeridas em decisões do Plenário e pendentes de execução pela Sefti.

47. Aplicados esses critérios e considerando as secretarias de controle externo dos estados que atenderam ao convite para participarem da FOC, foi definida uma lista inicial de 38 possíveis organizações públicas federais a serem fiscalizadas, posteriormente reduzida para 27 em função de restrições de cronograma. Ficou estabelecido, ainda, que cada unidade técnica estadual auditaria as organizações que faziam parte da respectiva clientela, enquanto que a Sefti fiscalizaria os jurisdicionados com sede no Distrito Federal e no estado do Rio de Janeiro.

2ª etapa – Execução de Auditorias Pilotos

48. Nessa etapa, a equipe coordenadora da FOC realizou três fiscalizações com o objetivo de validar e testar as matrizes de planejamento e de achados elaboradas durante o planejamento. A sua validação em uma situação prática foi fator mitigador de riscos para as demais auditorias.

49. As matrizes validadas foram documentadas e apresentadas posteriormente nos *workshops* de capacitação da FOC, que tinham por objetivo transferir o conhecimento sobre as questões e os procedimentos de auditoria a todos os auditores que participariam dos trabalhos de fiscalização (Sefti, Secex-AM, Secex-CE, Secex-PE, Secex-PR, Secex-RS e Secex-SP).

50. No âmbito da primeira fase da FOC, as auditorias pilotos foram realizadas na Eletrobras Termonuclear S.A. (Eletronuclear – TC 013.420/2013-5) e na Empresa Brasileira de Infraestrutura Aeroportuária (Infraero – TC 032.366/2013-2), escolhidas segundo os critérios estabelecidos na etapa de planejamento. Na segunda fase da FOC, a auditoria piloto se deu no Banco Central do Brasil (BCB – TC 023.048/2013-1). Esses trabalhos foram realizados pela equipe de coordenação da FOC, composta por três auditores da Sefti.

3ª e 4ª etapas – Auditorias da primeira e segunda fase da FOC

51. Nessas auditorias foram executados os procedimentos constantes das matrizes construídas e revisadas nas auditorias pilotos. As equipes eram compostas por três integrantes,

sendo dois auditores da secretaria de controle externo no Estado à qual a unidade jurisdicionada selecionada estava vinculada e um auditor da Sefti. A participação do auditor da Sefti teve por objetivo propiciar o melhor entendimento das questões e procedimentos de auditoria previstos na matriz de planejamento, além de auxiliar nas discussões dos temas avaliados com os gestores das organizações fiscalizadas.

52. Com a finalidade de agilizar os trabalhos das equipes e uniformizar entendimentos, a unidade orientadora também disponibilizou, para cada fase do trabalho, alguns papéis de trabalho padrão, tais como modelo de ofício de requisição dos documentos que deveriam ser solicitados, modelo de relatório de auditoria, bem como lista de encaminhamentos padrão para cada possível achado contido nas matrizes de planejamento.

5ª etapa – Consolidação

38. Nessa fase, levada a efeito por meio deste relatório, foram agregados os resultados de todas as fiscalizações executadas, de modo a sintetizar os achados e as conclusões sobre os temas avaliados tanto na primeira quanto na segunda fase da FOC.

1.8 Fiscalizações integrantes da FOC

53. Este TMS é composto de 31 trabalhos, formalizados em processos distintos:

a) 24 auditorias operacionais realizadas na primeira fase;

b) 6 auditorias operacionais realizadas na segunda fase;

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

1.9 Questões de auditoria

54. Com o objetivo de avaliar os assuntos que configuravam o objetivo da fiscalização, foram propostos dois conjuntos de questões de auditoria: um para cada fase do trabalho.

55. Para efeito da primeira fase, a fim de avaliar a aderência das organizações às melhores práticas de governança e de gestão de TI, foram elaboradas seis questões de auditoria, agrupadas neste relatório em cinco temas, conforme ilustra a tabela a seguir:

| Temas | Questões de auditoria |
|---|---|
| Governança corporativa | 1.1 Os mecanismos de governança corporativa foram definidos e implementados adequadamente no âmbito da instituição? |
| Governança de TI | 1.2 Há um processo de aprimoramento da governança de TI segundo as boas práticas? |
| | 1.3 Os mecanismos de governança de TI foram definidos e implementados adequadamente no âmbito da instituição? |
| Estratégias e Planos | 1.4 As estratégias e planos corporativos e de TI foram definidos e implementados adequadamente no âmbito da instituição? |
| Gestão de Pessoas de TI | 1.5 Os mecanismos de gestão de pessoal de TI foram definidos e implementados adequadamente no âmbito da instituição? |
| Processos | 1.6 Os processos de TI foram definidos e implementados adequadamente no âmbito da instituição? |

Tabela 1 - Questões de auditoria da primeira fase

56. Já na segunda fase, o principal objetivo das fiscalizações foi avaliar as práticas adotadas pela instituição para assegurar a entrega de resultados de TI, alinhados aos objetivos de negócio da instituição e gerenciando os riscos de TI existentes. Dessa forma, com base no objetivo da fiscalização e a fim de avaliar a aderência das organizações às melhores práticas de governança e de gestão de TI, foram elaboradas cinco questões de auditoria que analisam mais de uma dezena de assuntos ligados a entrega de resultados, gestão de recursos e gestão de riscos de TI (Tabela 2).

57. Há uma ampla interconexão existente entre os assuntos abordados. Contudo, para propiciar maior clareza ao relatório, optou-se por agrupar os assuntos em quatro grupos de achados: mecanismos de governança e de gestão de TI para a entrega de resultados, gestão de riscos de TI, resultados entregues pela TI e contratações de TI. A primeira metade aborda dois

grupos de procedimentos voltados para a análise de processos e métodos de trabalho, enquanto os dois grupos restantes analisam substantivamente os resultados alcançados pela TI e de que forma algumas contratações foram planejadas e têm sido geridas pela instituição.

| Temas | Questões de auditoria |
|---|---|
| Alinhamento entre TI e negócio | 2.1 A instituição adota processos e práticas que garantem alinhamento entre a TI e o negócio? |
| Avaliação de investimentos e priorização, gestão orçamentária e de custos, gestão de serviços, acompanhamento de objetivos e metas. | 2.2 A instituição dispõe de mecanismos adequados para analisar benefícios esperados dos investimentos em TI, gerenciar custos e acompanhar os resultados esperados do setor de TI? |
| Gestão de riscos de TI | 2.3 A entrega de resultados é executada mediante adequada gestão de riscos de TI? |
| Contratações de TI | 2.4 As contratações de TI estão orientadas à entrega de resultados? |
| Resultados alcançados pela TI | 2.5 Os resultados entregues pela TI têm sido satisfatórios? |

Tabela 2 - Questões de auditoria da segunda fase

1.10 Limitações

58. Não houve limitações que pudessem impactar a conclusão dos trabalhos.

1.11 Volume de recursos fiscalizados

59. Tendo em vista que foram avaliados diversos aspectos ligados à gestão e à governança de TI nas organizações questionadas no levantamento de governança de TI realizado pelo TCU em 2012 e que as fiscalizações foram executadas em 2013, será adotado, para efeito de cálculo do volume de recursos fiscalizados (VRF), os orçamentos de TI para o exercício de 2013 informados pelas organizações auditadas no referido levantamento, totalizando o montante de **R$ 3.292.287.906,00**.

1.12 Benefícios estimados

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

## 2. RESULTADOS DA AVALIAÇÃO EMPREENDIDA

61. Os resultados gerais apresentados neste relatório consolidador foram agrupados em torno de temas e subtemas que agrupam questões e objetos de auditoria ligados às duas fases da fiscalização, a saber:

| Tema | Subtema |
|---|---|
| **Perfil Gov TI** | Preenchimento do questionário de governança de TI |
| **Governança** | Governança Corporativa |
| | Governança de TI |
| | Aprimoramento de Governança de TI |
| **Estratégia e Planejamento** | ---------- |
| **Resultados de TI** | Gestão de Serviços |
| | Avaliação de benefício esperado com investimento em soluções de TI |
| | Gestão de Projetos |
| | Acompanhamento dos resultados de TI |
| | Resultados entregues pela TI |
| **Gestão de Riscos** | ---------- |
| **Segurança da Informação** | ---------- |
| **Gestão de Recursos** | Gestão dos recursos humanos em TI |
| | Gestão de Custos de TI |
| | Contratações de TI |

62. Para cada um desses temas e subtemas indicados são apresentadas as questões de auditoria que avaliaram o respectivo objeto em cada fase da fiscalização, bem como a quantificação dos achados ligados àquele objeto.

63. Ao longo de cada capítulo são realizadas avaliações sistêmicas a respeito das constatações acerca do assunto abordado na FOC e, quando possível, são formuladas propostas de encaminhamento destinadas a promover a melhoria da situação observada.

64. Ao final do relatório, um capítulo também foi dedicado a comentar a atuação dos Órgãos Governantes Superiores no que tange aos assuntos abordados em razão de seu papel preponderante no estabelecimento de diretrizes e condições às organizações que lhes são jurisdicionadas.

## 3. PERFIL GOV TI

65. Um dos objetivos dessa FOC era a verificação de eventuais inconsistências entre as evidências de implementação dos controles de TI e as respostas apresentadas pelas organizações no Levantamento do Perfil de Governança de TI de 2012 (Perfil Gov TI). Pretendia-se, com a avaliação, subsidiar o aperfeiçoamento do instrumento de levantamento de governança de TI, além de gerar expectativa de controle por parte dos participantes.

66. Entende-se inconsistência como sendo a divergência existente entre a informação assinalada pelo órgão ao preencher o questionário e a opinião da equipe de fiscalização quanto à pertinência daquela resposta em face da situação observada durante a auditoria. Uma inconsistência pode ser considerada negativa quando o órgão informou adotar um processo ou controle, mas as evidências não foram suficientes para sustentar essa afirmação. Por outro lado, uma inconsistência positiva é registrada quando o órgão não informou que adotava um controle ou processo, mas, de acordo com a avaliação da equipe de fiscalização, a situação encontrada era suficiente para que o órgão registrasse a adoção daquela prática.

67. Ressalte-se que a existência de inconsistências tem causas diversas, tais como: falhas de interpretação do questionário por parte da instituição fiscalizada; falta de clareza de algumas perguntas do questionário; grau de rigor empregado pela instituição na autoavaliação.

68. As inconsistências foram individualmente apuradas pelas equipes em cada trabalho e estão consolidadas em quadros constantes de cada relatório. Foram identificadas ao todo cinco

inconsistências positivas: uma no Ministério da Justiça (021.447/2013-6), uma na Universidade Federal de Pernambuco (022.074/2013-9) e três na Universidade Federal do Ceará (TC 019.131/2013-5). Já as inconsistências negativas, em maior número, estão consolidadas nas tabelas a seguir e organizadas por Órgão Governante Superior (OGS):

Tabela 3 - Inconsistências negativas por órgão – 58 itens avaliados

| DEST | Incons. | SLTI | Incons. | CNJ | Incons. |
|---|---|---|---|---|---|
| Suframa (021.789/2013-4) | 10 | UFPE (022.074/2013-9) | 12 | TRE/RS (021.469/2013-0) | 9 |
| Amazonas Distribuidora (021.790/2013-2) | 5 | MEC (014.038/2013-7) | 9 | TRE/PE (015.166/2013-9) | 4 |
| Codesp (020.348/2013-4) | 5 | CGTEE (021.471/2013-4) | 8 | TRT 7ª (019.168/2013-6) | 3 |
| Infraero (032.366/2013-2) | 3 | MJ (021.447/2013-6) | 6 | TRF 5ª (022.074/2013-9) | 2 |
| BNB (015.047/2013-0) | 2 | Incra (021.445/2013-3) | 6 | TRE/SP (020.346/2013-1) | 2 |
| Eletronuclear (013.420/2013-5) | 1 | Ufam (021.792/2013-5) | 5 | - | |
| - | | Inpe (020.349/2013-0) | 5 | - | |
| - | | ANA (021.444/2013-7) | 3 | - | |
| | | UFCE (019.131/2013-5) | 1 | - | |
| Total | 26 | Total | 55 | Total | 20 |
| Média | 4,33 | Média | 6,11 | Média | 4,00 |

69. Verifica-se que a média de inconsistências apuradas foi maior no âmbito do Sisp, atingindo quase seis inconsistências por órgão. Sob outra ótica, as inconsistências foram também agrupadas por seção temática, de forma a indicar possíveis pontos de atuação na revisão do questionário.

70. Os quantitativos de inconsistências foram maiores na primeira dimensão do questionário (1. Liderança da Alta Administração), o que revela maior dificuldade das organizações em indicar de maneira precisa as práticas adotadas. Entre as possíveis causas estão desde o baixo conhecimento das organizações quanto às práticas, processos e papéis da alta administração no que tange à governança, quanto o fato de que em muitas organizações as respostas ao questionário são elaboradas somente por profissionais das áreas de tecnologia da informação.

71. Muitas vezes os gestores de TI participantes do levantamento alegam que, embora a seção de liderança devesse ser respondida por setores envolvidos com a governança corporativa, ainda há falta de compreensão por parte da administração das organizações de que governança de TI, entre outros assuntos, é responsabilidade da Alta Administração e não é assunto exclusivo da área técnica.

Tabela 4 - Inconsistências negativas por seção do levantamento

| Tema | Inconst. |
|---|---|
| Item 1.1 (Estrutura da governança corporativa) | 11 |
| Item 1.2 (Estrutura de governança de TI) | 16 |
| Item 1.3 (Desempenho institucional da gestão e de uso corporativos de TI) | 15 |
| Item 1.4 (Desenvolvimento interno de gestores de TI) | 1 |
| Item 1.5 (Auditoria formal de TI) | 13 |
| Item 2.1 (Processo de planejamento estratégico institucional) | 5 |
| Item 2.2 (Processo de planejamento estratégico de TI) | 7 |
| Item 2.3 (Plano Diretor de Tecnologia da Informação – PDTI) | 4 |
| Item 4.2 (Quantitativo de pessoas que compõem a força de trabalho de TI) | 1 |

| | |
|---|---|
| Item 4.4 (Plano de capacitação de pessoal para gestão de TI) | 3 |
| Item 5.1 (Implementação de processos de gestão de serviços de TI) | 7 |
| Item 5.2 (Gestão de nível de serviço de TI) | 3 |
| Item 5.3 (Gestão da segurança da informação) | 8 |
| Item 5.8 (Planejamento da contratação em TI) | 4 |
| Item 5.9 (Gestão dos contratos de TI) | 3 |
| Total | 101 |

72. Os questionamentos e dúvidas levantados pelas equipes junto aos jurisdicionados foram encaminhados à equipe responsável pela revisão do instrumento de levantamento. A partir de um detido processo de revisão do questionário que envolveu várias rodadas internas de revisão, consulta a especialistas externos e disponibilização do novo questionário para consulta pública, sugestões e aprimoramentos foram incorporados ao questionário já disponível na 4ª edição do Levantamento de Governança de TI que está sendo realizado em 2014.

73. Apesar das inconsistências apuradas, a avaliação geral é de que o preenchimento das respostas tem sido razoavelmente adequado, pois o percentual médio de inconsistências por instituição auditada frente ao rol de itens avaliados (58) foi de 8,71%. Considerando que foram apenas três edições do questionário e que muitos dos temas ainda são de relativo desconhecimento em algumas organizações, conclui-se que a fidedignidade das respostas é razoavelmente positiva, com poucas exceções.

Propostas de encaminhamento

74. Sem propostas.

## 4. GOVERNANÇA

75. O tema governança nas organizações públicas tem sido alçado ao primeiro plano das ações do Tribunal de Contas da União, tendo suscitado, inclusive, a elaboração por parte do TCU do Referencial Básico de Governança Aplicável a Órgãos e Entidades da Administração Pública.

76. A governança de TI, por sua vez, tem sido objeto de reiteradas ações da Secretaria de Fiscalização de TI do TCU. Desde a primeira edição do levantamento de governança de TI (atualmente na 4ª edição), o Tribunal tem recomendado e indicado a adoção de medidas que propiciem maior governança sobre a gestão e sobre o uso da tecnologia da informação como fator preponderante para garantir melhor entrega de resultados.

77. Dessa forma, sob esse tema foram agrupadas três questões de auditoria (1.1, 1.2 e 1.3) em torno dos seguintes subtemas:

| | |
|---|---|
| Governança corporativa | 1.1 Os mecanismos de governança corporativa foram definidos e implementados adequadamente no âmbito da instituição? |
| Governança de TI | 1.2 Há um processo de aprimoramento da governança de TI segundo as boas práticas? |
| | 1.3 Os mecanismos de governança de TI foram definidos e implementados adequadamente no âmbito da instituição? |

### 4.1 Governança corporativa

78. Desde a primeira edição do levantamento em governança de TI realizado pelo TCU, aspectos de governança corporativa têm sido abordados por serem considerados fundamentais e complementares ao funcionamento da governança de TI. Com efeito, foram avaliados três aspectos extraídos do questionário de 2012: políticas corporativas, direção estratégica e ética institucional.

| Tema | Achado | Total (20 unidades) |
|---|---|---|

| | | |
|---|---|---|
| Políticas corporativas | Atuação insuficiente da alta administração no estabelecimento e monitoramento de políticas corporativas | 12 |
| Comitê de direção estratégica | Inexistência de comitê de direção estratégica para apoio em áreas de competência da alta administração | 4 |
| Ética institucional | Inexistência de Código de Ética | 3 |
| | Falhas na aplicação do código de ética | 6 |
| | Estrutura incompleta do Código de Ética | 0 |

79. De acordo com o Código das Melhores Práticas de Governança Corporativa do Instituto Brasileiro de Governança Corporativa (IBGC), 4ª edição, entre as atribuições do conselho de administração encontra-se a missão de traçar as diretrizes estratégicas para a instituição. Entre os exemplos citados, o documento cita decisões envolvendo: estratégia, perfil de risco, auditoria, práticas de governança corporativa, sistema de controles internos e código de conduta.

80. Nesse sentido, para avaliar a atuação da Alta Administração das organizações auditadas no estabelecimento de diretrizes foi verificado se políticas corporativas haviam sido estabelecidas para os temas: ética, governança de TI e segurança da informação. Em doze organizações, verificou-se que tais políticas não estavam estabelecidas, isto é, não haviam sido formalmente instituídas pela Alta Administração.

81. Em que pese o universo de políticas de caráter corporativo avaliado ter sido baixo, os relatórios apresentam indícios de que a Alta Administração de algumas organizações precisa ser sensibilizada quanto ao seu papel no que tange ao estabelecimento e monitoramento de políticas corporativas em temas que guardam conexão com a TI, sobretudo àquelas ligadas à governança de TI, a fim de que o comportamento desejado na gestão e no uso dos recursos de TI possa ser adequadamente transmitidos por toda a organização.

82. Assim sendo, o Referencial Básico de Governança Aplicável a Órgãos e Entidades da Administração Pública elaborado pelo Tribunal de Contas da União dispõe quanto ao componente L3 – Liderança Organizacional, Prática L3.2, que cabe à liderança organizacional *responsabilizar-se pelo estabelecimento de políticas e diretrizes para a gestão da organização e pelo alcance dos resultados previstos.* Ainda nesse sentido, a prática L3.1 dispõe que o "desempenho da gestão da organização, bem como sua conformidade com normas externas e diretrizes internas, sejam avaliados, direcionados e monitorados pela alta administração".

83. Ainda de acordo com o código do IBGC, o conselho de administração (alta administração) pode estabelecer comitês acessórios para apoiar suas atividades em temas específicos. Nesse sentido, constatou-se que a maioria das organizações já dispõe de alguma sorte de comitê ou comissão que apoia a alta administração na tomada de decisão estratégica e no acompanhamento de planos e da gestão. Apenas quatro das equipes de auditoria que fizeram parte da FOC verificaram a inexistência de tal estrutura. Notadamente, os comitês criados são utilizados no acompanhamento e monitoramento da execução do plano estratégico institucional.

84. Já com relação à questão da ética institucional. Observou-se inexistência de código de ética ou falhas na aplicação do referido código em nove organizações (45%). Número consideravelmente elevado, tendo em vista que o tema está ligado diretamente aos princípios que regem o funcionamento da administração pública insculpidos no art. 37 da Carta Constitucional. Cabe registrar que a ética no âmbito do Poder Executivo Federal é regida por meio dos Decretos 1.171/1994 e 6.029/2007.

85. Das cinco organizações do Poder Judiciário objeto de consolidação, em três delas se detectou a inexistência de um Código de Ética. Foi o caso dos Tribunais Regionais Eleitorais de São Paulo, Pernambuco e do Rio Grande do Sul. Em todas as três organizações, no entanto, a equipe registrou que um código estava em processo de elaboração. No caso, do Tribunal Regional Federal da 5ª Região, observou-se que já há um Código de Conduta aplicável a toda a Justiça Federal.

86. Além disso, em seis organizações verificaram-se falhas na aplicação dos códigos de ética: não realização de campanhas de divulgação (quatro organizações); código de ética não está facilmente acessível (uma entidade); e não há comitê de ética estabelecido (uma organização).

87. Assim, percebe-se que de um lado há uma tendência de definição de códigos de ética ou conduta em âmbito mais geral, como foi o caso do Poder Executivo e do Conselho da Justiça Federal, sujeitando às suas disposições um grande número de organizações. Porém, de outro lado, em algumas dessas organizações constatou-se que as práticas ligadas à gestão de ética não têm sido aplicadas, tais como a divulgação e a instituição de comitês. Finalmente, verificou-se que parte das organizações não submetidas a esses códigos de ética de ampla abrangência não têm logrado sucesso na implantação de seus códigos próprios.

88. As boas práticas de governança corporativa ainda são de relativo desconhecimento por parte dos altos administradores, fomentando, inclusive a elaboração do Referencial Básico de Governança Pública por parte do Tribunal. As avaliações realizadas nesse conjunto de fiscalizações, ainda que parciais, da atuação da governança corporativa indicam que ainda são necessárias ações de sensibilização da alta administração quanto ao tema. O fato de que em doze organizações registrou-se atuação insuficiente da alta administração no estabelecimento ou monitoramento de políticas corporativas sinaliza possível fragilidade em sua atuação. Da mesma forma, as falhas identificadas na gestão de ética desempenhada por diversas organizações reforçam essa percepção.

89. No entanto, mais recentemente, o TCU tem se dedicado ao desenvolvimento de ações fiscalizatórias específicas no âmbito da governança corporativa. Atualmente, está em curso um levantamento de governança pública de âmbito nacional (TC 020.830/2014-9). O trabalho, realizado em parceria com os tribunais de contas estaduais, permitirá a participação de organizações públicas federais, estaduais e municipais e a consolidação de seus resultados fundamentará conclusões e proposição de ações específicas para o aprimoramento da governança pública corporativa nessas organizações.

90. Com efeito, entende-se que, considerando a realização concomitante de trabalho específico sobre governança corporativa pelo TCU, é adequado dispensar a emissão de encaminhamentos nesse sentido em favor daqueles que serão produzidos mediante conclusões obtidas no levantamento nacional.

Propostas de encaminhamento

91. Sem propostas.

4.2 Governança de TI

92. A governança de TI pode ser compreendida como o sistema que direciona e monitora a gestão e o uso da tecnologia da informação em uma organização para assegurar que as necessidades de negócio atuais e futuras sejam atendidas. Ademais, é parte integrante da governança corporativa e compreende os mecanismos de liderança, as estruturas organizacionais, os processos, as políticas, os recursos e outros mecanismos que asseguram o seu funcionamento.

93. É importante relembrar que as falhas no estabelecimento de uma governança efetiva sobre a tecnologia da informação podem ter diversas consequências. A Intosai, ao elencar em seu manual de auditoria de TI o tema governança de TI como um dos capítulos-chave entre as disciplinas de auditoria de TI, apontou os seguintes riscos de uma falta de tratamento adequado da governança de TI (*Handbook on IT Audit for Supreme Audit Institutions*, peça 6, p. 32-34):

a) Sistemas de informação não efetivos, ineficientes ou não amigáveis;

b) TI não servindo às necessidades de negócio institucionais;

c) Restrições ao crescimento do negócio institucional;

d) Gerenciamento ineficiente de recursos;

e) Tomada de decisão inadequada;

f) Fracasso de projetos;

g) Dependência de fornecedores;

h) Falta de transparência e prestação de contas;

i) Exposição a riscos de segurança da informação.

94. Nessa FOC foram avaliados quatro temas no âmbito da governança de TI: o estabelecimento de comitês, os mecanismos para dirigir e avaliar a gestão e uso de TI, a atuação da auditoria interna e a existência de ações ou processo para melhoria da governança da TI na instituição.

| Tema | Achado | Total (20 unidades) |
|---|---|---|
| Comitês de TI | Inexistência de um Comitê de TI | 0 |
| | Falhas na implementação de um Comitê de TI | 6 |
| Desempenho institucional da gestão e do uso corporativos de TI | Falhas nos mecanismos para dirigir e avaliar a gestão e o uso corporativos de TI. | 17 |
| Auditoria interna | Falhas na fiscalização de TI pela auditoria interna ou A auditoria interna não fiscaliza a TI[1] | 9 |
| | Organizações que não dispõem de auditoria interna (administração direta do poder executivo federal) | 3 |
| Processo de melhoria da governança de TI | Inexistência de ações específicas voltadas à melhoria de governança de TI | 3 |
| | Deficiências nas ações de melhoria de governança de TI | 11 |

1. O nome padrão para esse achado sofreu modificações durante a realização do trabalho e houve equipes que registraram o achado com o nome original. Os resultados foram somados.

95. Nenhuma das equipes registrou a inexistência de comitê de TI, o que pode configurar um avanço, pois indicadores presentes nos levantamentos de 2010 e 2012 indicavam inexistência da ordem de 50% e 22% (Relatório do PerfilGovTi2012, peça 3), respectivamente. Ainda que o universo avaliado não seja o mesmo, há uma sinalização no sentido de que a designação de comitês de TI tem sido uma prática de governança de TI cada vez mais adotada no âmbito da APF.

96. Atualmente, cabe destacar a importância do Guia de Comitê de TI do Sisp (peça 4), elaborado pela Secretaria de Logística e Tecnologia da Informação (SLTI) do Ministério do Planejamento, Orçamento e Gestão (MP), que tem por objetivo orientar a estruturação e funcionamento dos comitês.

97. Por outro lado, em seis casos dos vinte avaliados, as equipes identificaram falhas na implementação do Comitê de TI, tais como: falta de atuação, ausência de áreas relevantes em sua composição ou não monitoramento das ações por parte da alta administração. Registre-se que a ausência de comitês atuantes implica em vários riscos, tais como a ausência de priorização adequada de projetos e investimentos ou a alocação de recursos em desconformidade com as prioridades do negócio.

98. Há que se garantir, no entanto, que seja dada divulgação do referido guia às presidências dos comitês de TI de todas as organizações públicas participantes do perfil de governança de TI. Assim como o Guia de Comitê de TI, um número significativo de produtos produzidos, em especial no âmbito do Sisp, é de relativo desconhecimento por parte de organizações vinculadas a outros OGS, como no Judiciário e no Ministério Público. É imprescindível que sejam envidados esforços para viabilizar maior aproveitamento dos esforços realizados pelos OGS por meio do compartilhamento de produtos, guias, orientações e/ou realização de ações conjuntas. Nesse mesmo sentido apontou o Referencial Básico de

Governança Pública do TCU que, no âmbito do Componente E3 - Alinhamento Transorganizacional, assim dispôs:

A obtenção de resultados para a nação exige, cada vez mais, que as organizações públicas trabalhem em conjunto. Do contrário, a fragmentação da missão e a sobreposição de programas tornam-se realidade generalizada no âmbito do governo e muitos programas transversais deixam de ser bem coordenados. Ao trabalharem em conjunto, as organizações públicas podem melhorar e sustentar abordagens colaborativas para atingir as metas nacionais, os objetivos ou os propósitos coletivos.

99. Com efeito, o Referencial assenta, por meio da Prática E3.1, que é necessário "Estabelecer mecanismos de atuação conjunta com vistas a formulação, implementação, monitoramento e avaliação de políticas transversais e descentralizadas". Assim, conclui-se que é necessário propor uma maior interlocução entre os OGS de forma a incentivar o melhor aproveitamento de suas potencialidades.

100. Já em relação aos mecanismos para dirigir e avaliar a gestão e uso de TI, na maioria das organizações (85%) foram identificadas falhas quando aplicados testes para verificação da definição de objetivos de gestão e uso da TI, indicadores, metas, mecanismos de acompanhamento e de avaliação e tratamento dos riscos ao cumprimento desses objetivos.

101. Esse alto índice de organizações que ainda não estabeleceram diretrizes para os vários aspectos concernentes à gestão e ao uso da TI demonstra um aspecto que corriqueiramente é alegado pelos gestores de TI em entrevistas, cursos e seminários realizados pela Sefti: o distanciamento da alta administração em relação a assuntos de TI.

102. Ainda há significativo desconhecimento por parte do corpo dirigente (alta administração) das organizações públicas a respeito das suas responsabilidades no que tange a avaliar, dirigir e monitorar a tecnologia da informação.

103. Atento a essa situação, o TCU promoveu, em 15/6/2011, evento especificamente destinado à sensibilização da alta administração. O evento "Controle Externo em Ação: Papel da Alta Administração na Governança de TI" teve como exemplo de público-alvo secretários-executivos, assessores de ministros, presidentes, diretores-gerais e assessores.

104. No entanto, tal iniciativa parece configurar exceção entre as ações de capacitação em geral na administração pública, consoante testemunhos dos próprios gestores de TI, os quais afirmam que o levantamento de governança de TI tem sido um dos principais meios utilizados por eles para alertar a alta administração a respeito desse assunto.

105. Assim, configura-se necessário que as organizações públicas desenvolvam processos e instrumentos visando orientar o corpo diretivo acerca do tema e de sua responsabilidade perante esse. É necessário fomentar o desenvolvimento de guias, cursos e *workshops* que sejam específicos para esse público, considerando suas peculiaridades, em especial o fato de não serem técnicos no assunto e disporem de agendas de trabalho muito concorridas. Nesse mesmo âmbito, o Referencial de Governança Pública do TCU dispôs, na Prática L1.2 que é recomendável "Assegurar a adequada capacitação dos membros da alta administração".

106. Com relação à atuação da auditoria interna, observa-se que em várias organizações alguns trabalhos de auditoria de TI estão sendo realizados, embora muitas organizações ainda careçam de profissionais capacitados e metodologias para realização de trabalhos na área. Segurança da informação, por exemplo, apesar da criticidade do tema, foi um assunto que, nos dois anos anteriores ao levantamento (2010 e 2011), esteve fora do objeto de avaliação das auditorias internas de seis organizações fiscalizadas.

107. O tema relativo à melhoria da governança de TI é tratado em separado no próximo apontamento por se tratar de um tópico considerado de especial importância.

Propostas de encaminhamento

108. Recomendar aos OGS que, com base no Princípio da Eficiência insculpido no art. 37 da Constituição Federal c/c Prática E3.1 do Referencial Básico de Governança Pública do TCU, estabeleçam mecanismos permanentes de interlocução e compartilhamento de estratégias, ações e produtos no sentido de se maximizar o aproveitamento de soluções elaboradas no âmbito de um OGS, tais como guias, manuais, entre outros, pelos demais OGS, no sentido de se garantir maior eficiência e celeridade na orientação e estruturação das organizações sob suas respectivas jurisdições.

109. Recomendar aos OGS que, com base no Princípio da Eficiência insculpido no art. 37 da Constituição Federal c/c Prática L1.2 do Referencial Básico de Governança Pública do TCU, estabeleçam estratégias e ações de sensibilização da alta administração das organizações sob sua jurisdição quanto ao tema governança de TI, com o objetivo de orientar tais responsáveis acerca de seu papel no sentido de avaliar, dirigir e monitorar a gestão e o uso da tecnologia da informação.

4.3 Aprimoramento da Governança de TI

110. O tema "melhoria de governança de TI" foi selecionado como um tópico de especial importância nas auditorias da 1ª fase da FOC e foi objeto de uma questão de auditoria específica para sua avaliação.

111. Em verdade, a finalidade da questão era identificar de que forma as organizações públicas têm se preparado para conduzir o aprimoramento da governança e da gestão de TI. A partir de contatos e entrevistas com diversos gestores, percebe-se o risco de que os esforços de melhoria sejam dirigidos meramente com objetivo de obter melhores avaliações no Índice de Governança de TI (iGovTI), métrica adotada no levantamento periódico realizado pelo TCU.

112. Embora a melhoria desse indicador possa advir como consequência dos esforços de aprimoramento, ela não é um fim em si mesmo. A implantação ou melhoria de controles e processos deve ser dirigida com vistas à obtenção de melhores resultados em favor do atingimento dos objetivos de negócio, bem como para melhor tratar os riscos existentes e gerir mais eficientemente os recursos disponíveis.

113. O Cobit 5 elenca como primeiro dos processos específicos de governança de TI o EDM01 – Assegurar a definição e manutenção de um *framework* de governança (tradução livre). Esse primeiro processo é responsável pela orientação geral da governança de TI na instituição, por meio da avaliação do sistema de governança atual e pelo estabelecimento da direção desejada. Objetiva-se, assim, viabilizar o funcionamento efetivo das estruturas, princípios, processos e práticas, com definição clara de responsabilidades e mandato na busca da missão, metas e objetivos organizacionais.

114. Associado a esse processo de governança, o processo de gestão APO01 – Gerenciar o sistema de gestão da TI (tradução livre), dispõe de uma atividade especificamente indicada para estabelecer a melhoria contínua de processos. A atividade "APO01.07 – Gerenciar o aprimoramento contínuo de processos" utiliza o *feedback* sobre a efetividade e desempenho da governança, bem como as boas práticas, regulamentos e guias, para desenvolver avaliações de processo e traçar as oportunidades de melhoria guiadas por metas e métricas específicas.

115. Além do aprimoramento contínuo, as demais práticas contidas no processo APO01 – "Gerenciar o sistema de gestão da TI" contribuem para um melhor entendimento do que constituiria um sistema de governança de TI e quais as principais atividades que o compõem (Cobit 5 – Processos viabilizadores, p. 52, tradução livre):

APO01.01 Definir a estrutura organizacional

APO01.02 Estabelecer papéis e responsabilidades

APO01.03 Manter os viabilizadores do sistema de gestão

APO01.04 Comunicar a direção e os objetivos de gestão

APO01.05 Otimizar o posicionamento da função de TI

APO01.06 Definir propriedade de dados e sistemas

APO01.07 Gerenciar o aprimoramento contínuo de processos

APO01.08 Manter conformidade com políticas e procedimentos

116. Dessa forma, constata-se que as boas práticas indicam claramente a importância da avaliação periódica e sistemática da governança da TI para conduzir o seu aprimoramento de forma planejada, medida e controlada.

117. Caso o aprimoramento não seja conduzido por um processo sistemático, orientado por objetivos bem definidos e acompanhado por indicadores e metas, corre-se o risco de que a melhoria almejada pereça no tempo em decorrência das constantes mudanças de gestão e de prioridades, que são próprias da administração pública.

118. A avaliação realizada nas auditorias da FOC, no entanto, indica que a maioria das organizações não têm atuado para estruturar a melhoria de governança por meio de um processo. Em 15% das organizações (três) sequer registrou-se a existência de ações específicas voltadas para a melhoria de governança de TI. Em outras 55% (onze), falhas foram constatadas, tais como: inexistência de processo formal para organização dos esforços e ausência de estrutura organizacional designada para orientar as atividades.

119. Das outras seis organizações (MEC, ANA, INCRA, TRF5, BNB e CGTEE), em apenas uma (BNB) a equipe registrou boas práticas na aplicação do processo de melhoria de governança. Em uma segunda instituição (MEC) há papéis de trabalho (respostas a ofícios) que indicam a existência de ações nesse sentido. Nas outras três não houve menção a esse respeito, embora o achado não tenha sido relatado. Assim, entende-se que, de maneira geral, são raros os exemplos de organizações com práticas amadurecidas voltadas especificamente ao aprimoramento da sua governança de TI.

120. No caso do BNB, frise-se, tratava-se de uma das organizações que também participaram da 2ª fase da fiscalização, ou seja, um grupo de organizações com maior capacidade em processos e práticas de governança e gestão de TI. Ainda assim, a equipe de auditoria relatou (TC 015.047/2013-0, peça 65, p. 10):

não há no BNB um processo instituído formalmente para aprimoramento contínuo da governança de TI. Contudo, constatou-se que muitas das melhorias de governança que estão sendo implementadas foram mapeadas no processo de diagnóstico de melhoria da área de TI, realizado por consultoria externa e foram formalmente incluídas no Plano Estratégico de Tecnologia da Informação 2012-2015 (PETI).

Conforme a Resolução de Diretoria 5449/2013, o BNB dispõe em sua estrutura organizacional do Ambiente de Governança de TI, o qual é subordinado diretamente à Superintendência de Tecnologia da Informação (peça 27, p. 3). Referido ambiente tem a responsabilidade básica de promover, na área de TI, a governança de TI, a gestão das demandas, projetos, processos e serviços, o alinhamento estratégico, a entrega de valor ao negócio, a monitoração do desempenho dos indicadores operacionais e estratégicos, a gestão da conformidade regulamentar e a inovação de soluções tecnológicas (peça 27, p. 8-10).

(...)

No detalhamento dos objetivos estratégicos de TI no PETI evidencia-se a atenção dada à governança de TI, nos objetivos 8 (ampliar o escopo de atuação da Governança de TI) e 9 (Reavaliar e aprimorar a gestão de demandas). Destaca-se aqui o detalhamento das estratégias definidas para o alcance do objetivo estratégico 8 (peça 26, p. 18):

a) mapear processos de TI;

b) medir e divulgar a conformidade dos processos e das metodologias de TI estabelecidos;

c) promover a comunicação entre os ambientes da área de TI;

d) implantar mecanismos de avaliar o desempenho dos processos e indicadores de TI.

121. Esta situação se mostra em acordo com deliberação emitida no Acórdão 2.585/2012-TCU-Plenário, item 9.1.1.3, na qual recomendou-se aos órgãos governantes superiores que orientassem os seus jurisdicionados no sentido de definir e formalizar os objetivos desse processo, nos seguintes termos:

9.1.1.3. definam e formalizem metas de governança, como parte do plano diretor de tecnologia da informação da instituição, baseadas em parâmetros de governança, necessidades de negócio e riscos relevantes, atentando para as metas legais de cumprimento obrigatório e as orientações da ABNT NBR ISO/IEC 31000

122. Assim, em resumo, da análise verificada pela equipe de auditoria no BNB, constataram-se as seguintes boas práticas, as quais podem servir de parâmetro para o desenvolvimento de ações de aprimoramento por outras organizações públicas:

a) elaboração de diagnóstico a partir do qual são realizadas ações de melhoria;

b) estrutura organizacional designada especificamente para governança de TI;

c) alocação de profissionais para atuação nessa estrutura;

d) estabelecimento de objetivos e ações no planejamento da TI ligados ao aprimoramento de governança.

123. Por fim, em razão das dificuldades observadas em campo e relatadas pelos gestores para direcionar os esforços de melhoria de governança, bem como pela reiterada coleta de boas práticas a esse respeito em fiscalizações, entende-se que a emissão de algum tipo de orientação pode colaborar com os gestores nesse processo.

124. Nesse contexto, considerando que é objetivo estratégico do TCU contribuir para a melhoria da gestão e do desempenho da Administração Pública e que a missão da Sefti é assegurar que a TI agregue valor ao negócio da APF em benefício da sociedade, foi elaborada pela Sefti, em paralelo a essa consolidação, uma nota técnica (Apêndice, Seção VII.2) que apresenta uma série de entendimentos que visam apoiar as organizações no processo de amadurecimento de suas práticas de governança de TI.

125. Esse novo instrumento soma-se a outras seis notas técnicas já emitidas pela Sefti, cuja divulgação está prevista no item 9.44.4 do Acórdão 1.233/2012-TCU-Plenário. Dessa forma, propõe-se que também seja autorizado à Sefti promover a divulgação da nova nota técnica.

Propostas de encaminhamento

126. Autorizar a Sefti a promover a divulgação do conteúdo da Nota Técnica Sefti 7/2014 como forma de apoiar as organizações da Administração Pública Federal no processo de amadurecimento de suas práticas de governança de TI, bem como a jurisprudência deste Tribunal quanto ao assunto.

## 5. ESTRATÉGIA E PLANEJAMENTO

127. O desenvolvimento da estratégia e o planejamento das ações institucionais e de TI segue sendo compreendido como um dos pilares de maior importância para a efetiva entrega de resultados. Ainda assim, as fiscalizações seguem identificando organizações onde tal prática não está efetivamente implantada. Nesse sentido, a presente fiscalização estabeleceu uma questão de auditoria em cada fase para avaliação desses aspectos, a saber:

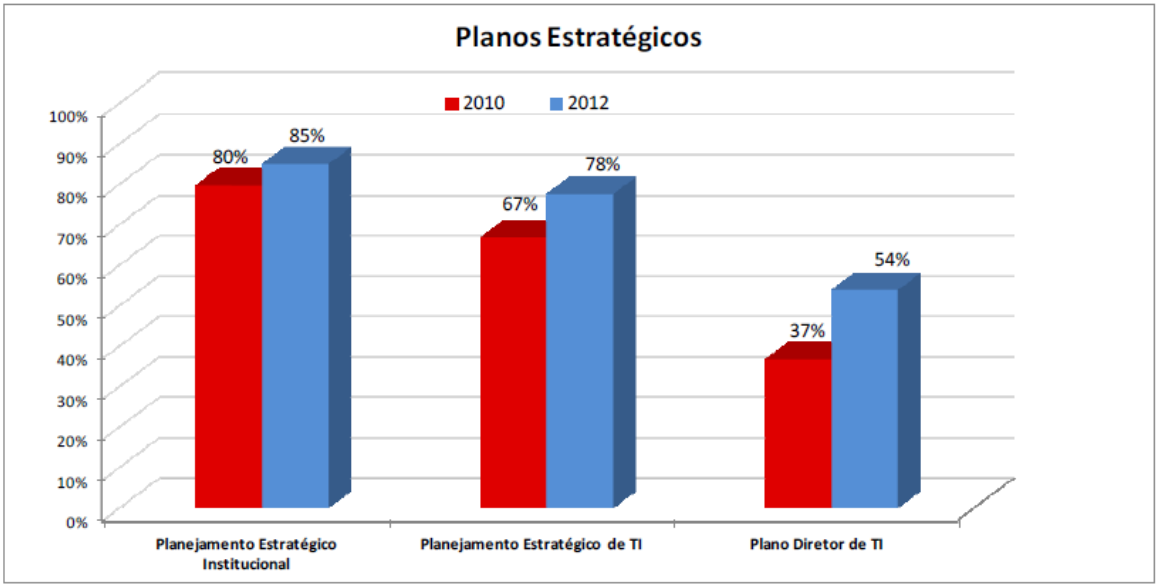
1.4 As estratégias e planos corporativos e de TI foram definidos e implementados adequadamente no âmbito da instituição?

2.1 A instituição adota processos e práticas que garantem alinhamento entre a TI e o negócio?

128. Com efeito, a partir da aplicação de procedimentos foram observados os seguintes achados de auditoria:

| Tema<br>1ª Fase | Achado | Total<br>(20 unidades) |
|---|---|---|
| Planejamento Estratégico Institucional | Inexistência de processo de planejamento estratégico institucional | 5 |
| | Falhas no planejamento estratégico institucional | 0 |
| Planejamento estratégico de TI | Inexistência de Planejamento Estratégico de TI (PETI) | 8 |
| | Falhas no Planejamento Estratégico de TI | 2 |
| Plano Diretor de TI | Inexistência de um PDTI formalizado e publicado pela alta administração | 8 |
| | Falhas no processo de elaboração do PDTI | 4 |
| | Falhas no PDTI | 5 |
| Tema<br>2ª Fase | Achado | Total<br>(5 unidades) |
| Alinhamento de TI com o negócio | Falha no alinhamento da TI com o negócio | 0 |

129. De acordo com o 3º Levantamento de Governança de TI (peça 3, p. 11), a quantidade de organizações que executam ações de planejamento tem se ampliado, conforme destaca a figura abaixo.




130. Por outro lado, de acordo com as fiscalizações efetuadas, em cinco organizações de vinte avaliadas foi detectada a ausência de processo de planejamento estratégico institucional (25%). Em relação ao planejamento estratégico de TI, a inexistência desse processo restou configurada em oito organizações (40%).

131. Inicialmente, parece haver uma contradição entre os números apurados pelo levantamento e aqueles avaliados por meio das fiscalizações em campo, com esses últimos configurando uma possível situação em que menos organizações realizam atividades de planejamento.

132. No entanto, há que se esclarecer mais uma vez que as vinte organizações selecionadas para realização de fiscalizações não configuram uma amostra aleatória, o que inviabiliza comparações com o rol de organizações apurado no levantamento. Além disso, existe uma outra razão ainda mais significativa decorrente da interpretação do questionário. É de conhecimento da unidade técnica, por meio de contatos com gestores em eventos e reuniões

realizadas em diversas ocasiões, que muitos assinalavam as respostas no questionário sem diferenciar completamente as definições dos termos "Plano" e "Processo".

133. De acordo com definição trazida pela norma ISO 9000, "qualquer atividade, ou conjunto de atividades, que usa recursos para transformar insumos (entradas) em produtos (saídas) pode ser considerado como um processo". Com efeito, a especificação de um processo de planejamento deve, no mínimo, defini-lo em termos de um conjunto de atividades, insumos e produtos.

134. Assim, um plano pode ser compreendido como um dos produtos do processo de planejamento, seja ele estratégico ou de TI. O processo, assim entendido, compreende as atividades, responsabilidades e sequência de ações que transformam os insumos utilizados no planejamento em produtos concretos, tais como o plano. A formalização é a transformação da descrição do processo em um normativo ou regulamento interno que estabelece as bases para sua execução (periodicidade, responsabilidades etc) e torna sua aplicação obrigatória no âmbito da organização.

135. Com efeito, muitas organizações, embora não contassem com um processo de planejamento formalizado, assinalavam no questionário que tinham processo de planejamento formal apenas com base na existência de um plano. Diferentemente dessa abordagem, o entendimento da Sefti é de que a existência desse processo só pode ser comprovada com evidências de sua formalização específica.

136. Tendo em vista essa ambiguidade na interpretação da questão. Restou pactuado entre a supervisão da FOC e as equipes de auditoria que, caso a instituição tivesse registrado resposta de que contava com um processo de planejamento com base na existência de um plano, não seria registrada uma inconsistência em sua resposta. Tal dificuldade de entendimento foi indicada à equipe de revisão do questionário de governança de TI e a nova versão do levantamento iniciado em 2014 já contempla seções claramente distintas para itens concernentes ao processo e aqueles concernentes ao plano (peça 5, p. 7):

| **2.1. Com relação ao planejamento estratégico institucional:** |
|---|
| *Processo* |
| a. a organização executa periodicamente **processo** de planejamento estratégico institucional. |
| b. o **processo** de planejamento estratégico institucional prevê a participação das áreas mais relevantes da organização. |
| c. o **processo** de planejamento estratégico institucional prevê a participação da área de TI. |
| d. o **processo** de planejamento estratégico institucional está formalmente instituído, como norma de cumprimento obrigatório. |
| *Plano Vigente* |
| e. a organização possui **plano** estratégico institucional **vigente**, formalmente instituído pelo seu dirigente máximo. |
| f. o **plano** estratégico institucional **vigente** contém pelo menos um indicador de resultado para quantificar o cumprimento de cada objetivo estratégico estabelecido. |

137. Com efeito, espera-se respostas mais fidedignas e menores discrepâncias entre os números apurados no levantamento e aqueles identificados em campo nas próximas fiscalizações.

138. No entanto, o índice de organizações que ainda não dispõem de processo de planejamento chama a atenção, uma vez que esse tema vem sendo objeto de reiteradas deliberações desta Corte, tanto em processos individuais quanto em fiscalizações com caráter sistêmico. O quadro abaixo sintetiza parcialmente a atuação da Corte de Contas e as respectivas mudanças no cenário com relação ao planejamento estratégico institucional e de TI.

| **Processo / Acórdão** | **Evento** |
|---|---|
| TC 008.380/2007-1 - Acórdão 1.603/2008-TCU-Plenário | Recomendações ao CNJ, CNMP e MPOG (itens 9.1.1 e 9.4.1):<br><br>Síntese: promovam ações com o objetivo de disseminar a importância do |

| | |
|---|---|
| - 1º Levantamento de Governança de TI | planejamento estratégico, procedendo, inclusive mediante orientação normativa, ações voltadas à implantação e/ou aperfeiçoamento de planejamento estratégico institucional, planejamento estratégico de TI e comitê diretivo de TI, com vistas a propiciar a alocação dos recursos públicos conforme as necessidades e prioridades da organização |
| TC 000.390/2010-0<br>- Acórdão 2.308/2010-TCU-Plenário<br>- 2º Levantamento de Governança de TI | Recomendações ao CNJ, Dest, SLTI/MPOG, CNMP, Segepres/TCU, DG/CD, DG/SF (itens 9.1.1 e 9.1.2)<br>Síntese:<br>a) 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.<br>b) normatizem a obrigatoriedade de a alta administração de cada instituição sob sua jurisdição, supervisão ou estrutura estabelecer os itens acima. |
| TC 028.772/2010-5<br>- Acórdão 1.145/2011-TCU-Plenário<br>- Monitoramento de deliberações que incluem o Acórdão 1.603/2008-TCU-Plenário | a) considerou atendida a deliberação 9.1.1 do Acórdão 1.603/2008-TCU-Plenário por parte do CNJ tendo em vista a publicação das Resoluções CNJ 70/2009 (planejamento estratégico) e CNJ 90/2009 (planejamento estratégico de TI)<br>b) considerou em implementação a deliberação 9.1.1 do Acórdão 1.603/2008-P por parte do CNMP em face de dificuldades daquele órgão em atuar normativamente e considerando outras ações desempenhadas por aquela instituição que iam ao encontro dos propósitos do encaminhamento;<br>c) considerou as ações por parte do MPOG parcialmente implementadas tendo por base a existência de dispositivo no Art. 4º da IN SLTI/MP 4/2010 que afirma que as contratações de que trata a IN deveriam ser precedidas de planejamento, elaborado em harmonia com o PDTI, alinhado ao planejamento estratégico do órgão ou entidade. |
| TC 011.772/2010-7<br>- Acórdão 1.233/2012-TCU-Plenário<br>- FOC Gestão e uso de TI | Recomendações à Câmara de Políticas de Gestão, Desempenho e Competitividade (CGDC) do Conselho de Governo (itens 9.1.2), CNMP (itens 9.15.1 e 9.15.2)<br>Síntese:<br>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). |
| TC 007.887/2012-4<br>- Acórdão 2.585/2012-TCU-Plenário<br>- 3º Levantamento de Governança de TI | Recomendou ao CNJ, CNMP, SLTI/MP e CGPAR que orientassem as unidades sob sua jurisdição para que (item 9.1.1.1):<br>em atenção ao art. 6º da Lei nº 12.527/2011 e aos princípios da transparência e da prestação de contas, implementem instrumentos de planejamento estratégico institucional e de tecnologia da informação, dando-lhes ampla divulgação, com exceção das informações classificadas como não públicas, nos termos da lei. |

139. Do quadro apresentado, podem ser tecidas algumas considerações. Em primeiro lugar, verifica-se ampla atuação deste Tribunal, em caráter sistêmico, junto aos órgãos governantes superiores, na busca por medidas que busquem aprimorar e incentivar a adoção de mecanismos de planejamento por parte das organizações públicas.

140. Desde o primeiro levantamento, o qual deu origem ao Acórdão 1.603/2008-TCU-Plenário, verifica-se que esta Corte entende que a orientação normativa é o caminho a ser trilhado pelos OGS no encaminhamento desta importante questão. O Acórdão 2.308/2010-TCU-Plenário, por sua vez, é claro ao enfatizar a importância de se normatizar a obrigatoriedade dessa atividade.

141. No entanto, verifica-se que, exceção feita ao CNJ e ao Poder Judiciário, pouco se avançou no quadro normativo referente a esse tema.

142. Embora o monitoramento do Acórdão 1.145/2011-TCU-Plenário tenha considerado parcialmente atendida a disposição emitida ao Ministério do Planejamento no Acórdão 1.603/2008-P no que tange à normatização do tema, há que se considerar que decisões ulteriores, notadamente o Acórdão 1.233/2012-TCU-Plenário, reforçaram a necessidade de o Poder Executivo e o Ministério Público emitirem regulamentos que tornem as ações de planejamento obrigatórias, indicando até mesmo os parâmetros e aspectos que deveriam ser

considerados na elaboração dessas normas (itens 9.1.1, 9.1.2, 9.15.1 e 9.15.2 do Acórdão 1.233/2012-TCU-Plenário).

143. Em referência a essa série de deliberações do TCU, o quadro avaliado durante as fiscalizações de campo apontou os seguintes números:

| Achado | Instituições com o achado / Total (Executivo) | Instituições com o achado / Total (Judiciário) |
|---|---|---|
| Inexistência de processo de planejamento estratégico institucional | 5/15 (33%) | 0/5 (0%) |
| Inexistência de (Processo de) Planejamento Estratégico de TI (PETI) | 7/15 (46%) | 1/5 (20%) |
| Inexistência de um PDTI formalizado e publicado pela alta administração | 7/15 (46%) | 1/5 (20%) |

144. Embora a amostra coletada não tenha sido selecionada com base em parâmetros estatísticos que permitam a extrapolação das conclusões para todo o conjunto de organizações, os números obtidos sugerem que o instrumento de planejamento tem avançado mais no Poder Judiciário. É provável que a força das regulamentações emitidas tenha contribuído sensivelmente nesse sentido. Assim dispôs o Art. 11 da Resolução CNJ 90/2009:

Art. 11. O Tribunal deve elaborar e manter um Planejamento Estratégico de TIC - PETI, alinhado às diretrizes estratégicas institucionais e nacionais.

Parágrafo único. Deverá ser elaborado, com base no PETI, o plano diretor de Tecnologia da Informação e Comunicação (PDTI).

145. Importante relembrar que os efeitos potenciais decorrentes da carência de um sólido planejamento são diversos, sejam diretos ou indiretos, a exemplo de:

a) inviabilidade de se aferir objetivamente o desempenho das organizações e, por conseguinte, assegurar o atendimento ao princípio da eficiência insculpido no caput do art. 37 da Constituição Federal;

b) dificuldade para se realizar o alinhamento entre as ações de TI e o negócio da instituição, pela inexistência de objetivos e metas positivados;

c) impossibilidade de realizar contratações de soluções de TI em conformidade com o art. 4º da IN SLTI/MP 4/2010 para organizações do Poder Executivo ou art. 6º da Resolução CNJ 182/2013 para organizações do Poder Judiciário;

d) outros efeitos potenciais da falta de planejamento, tais como: descontinuidade de projetos, insatisfação de usuários, resultados abaixo do esperado, investimentos que não atingem objetivos.

146. Com efeito, observa-se que, de um lado há riscos relevantes advindos da falta de planejamento, e de outro, constatou-se que ainda existem diversas organizações, notadamente no âmbito do Poder Executivo, que não dispõem de processo de planejamento nem dos planos em si, seja em nível estratégico institucional (PEI), estratégico de TI (PETI) ou tático de TI (PDTI).

147. Uma medida adotada no âmbito do Sisp com vistas a ampliar o número de organizações que adotam o instrumento de planejamento foi a de incluir como indicador e meta na Estratégia Geral de Tecnologia da Informação (EGTI) 2013-2015 o número de órgãos com PDTI publicado e vigente. A EGTI (peça 8) é um instrumento de planejamento periódico de todo o Sisp e estabelece objetivos e metas para todo o setor. Com efeito, embora os resultados da fiscalização sugiram que ela pode não estar sendo plenamente eficaz, tal medida mostra-se bastante salutar no sentido de incentivar a adoção desse instrumento.

148. Ainda, considerando que, como resultado de amplos trabalhos executados pelo Tribunal nesta área, já foram emitidas em diversas ocasiões recomendações em caráter sistêmico para que o Poder Executivo regulamentasse a atividade de planejamento, as quais até

o presente momento não se revelaram plenamente efetivas, entende-se que é necessário, no âmbito de novo monitoramento dos respectivos Acórdãos, avaliar as ações empreendidas pelos gestores nesse sentido e sua efetividade.

149. Interessante notar que na análise ambiental (SWOT) feita para a elaboração da EGTI (peça 8, Anexo 2), a existência da IN – SLTI/MP 4/2010 e a existência de competência formal na definição de políticas e normas de TI foram reconhecidas como pontos fortes. Por outro lado, a mesma análise indica como ponto fraco do ambiente a baixa adoção de padrões tecnológicos do governo. Assim, infere-se que a competência regulatória para instituir ou exigir a adoção de padrões precisa ser ainda mais utilizada pelo órgão gestor do Sisp, a SLTI/MP.

150. Assim, entende-se que, a exemplo do ocorrido no Poder Judiciário, a regulamentação no Poder Executivo poderá viabilizar e orientar as organizações jurisdicionadas na adoção desse processo, seja por meio da declaração expressa de obrigatoriedade, seja pela definição de princípios e aspectos que devem ser observados na realização dessa fundamental atividade.

151. Por fim, entende-se que há possibilidades de fortalecimento do papel da EGTI junto ao setor jurisdicionado. Não se verificou, pela leitura do documento que contém a EGTI ou pelo sítio eletrônico que a hospeda, a existência de uma avaliação e divulgação periódica, do cumprimento dos objetivos e metas dispostos na estratégia. Há apenas menção em seu Anexo 3 (peça 8, p. 37-45) às metas do plano anterior (Plano de Metas 2011-2012). Entende-se que a divulgação dos resultados intermediários atingidos poderia apoiar a contribuição dada pela EGTI para o avanço dos aspectos consignados em seus objetivos e metas. A ampla divulgação de informações de interesse público favorece o controle social, conforme disposto nos incisos II e V, do art. 3º da Lei 12.527/2011 (Lei de Acesso à Informação), e incentiva a adoção das práticas por parte dos jurisdicionados.

Propostas de encaminhamento

152. Recomendar ao Conselho Nacional de Justiça – CNJ e à Secretaria de Logística e Tecnologia da Informação do Ministério do Planejamento, Orçamento e Gestão – SLTI/MP, com base nos incisos II e V da Lei 12.527/2011 c/c inciso I do art. 6º do Decreto-Lei 200/1967, que publiquem periodicamente os resultados das avaliações acerca do alcance dos objetivos e metas dispostos nos respectivos planos estratégicos de TI para o setor jurisdicionado, propiciando ampla transparência aos resultados atingidos.

## 6. RESULTADOS DE TI

153. A NBR 38.500, norma que trata da governança corporativa de TI, define como seu objetivo promover o uso eficaz, eficiente e aceitável da TI. Analisando-se o modelo de governança de TI proposto pela norma (item 2.2, NBR 38.500), centrado nas atividades Avaliar, Dirigir e Monitorar, depreende-se que a governança busca assegurar que o uso da TI atenda aos objetivos de negócio, garantindo o desempenho almejado e em conformidade com as obrigações externas (requisitos de conformidade) e práticas internas de trabalho.

154. Em essência, entende-se que o propósito de concentrar esforços no aprimoramento da governança de TI tem por finalidade propiciar que a TI atinja os resultados que dela são esperados e, por consequência, apoie e suporte a organização no alcance de seus objetivos em benefício dos cidadãos e da sociedade.

155. Nesse sentido, foram avaliados os processos e métodos aplicados para: a) alinhar os objetivos de TI às necessidades das áreas de negócio; b) priorizar planos e projetos; c) avaliar o custo/benefício de investimentos financeiros e não financeiros em TI; d) gerenciar os serviços de TI; e f) acompanhar os objetivos e metas definidos no planejamento.

156. Além de avaliar os processos, controles e práticas adotadas com foco na entrega de resultados, também foram aplicados alguns procedimentos para examinar de maneira substantiva e concreta quais resultados têm sido entregues pela área de TI.

157. Todos esses temas estiveram abordados por procedimentos de três questões de auditoria, uma da primeira fase e duas da segunda fase:

1.6 Os processos de TI foram definidos e implementados adequadamente no âmbito da instituição?

2.2 A instituição dispõe de mecanismos adequados para analisar benefícios esperados dos investimentos em TI, gerenciar custos e acompanhar os resultados esperados do setor de TI?

2.5 Os resultados entregues pela TI têm sido satisfatórios?

158. A tabela a seguir resume os temas abordados nessas questões e os achados a eles vinculados:

| Tema<br>1ª Fase | Achado | Total<br>(20 unidades) |
|---|---|---|
| Gestão de serviços de TI | Falhas na gestão de acordos de nível de serviço | 19/20* |
| Tema<br>2ª Fase | Achado | Total<br>(5 unidades) |
| Gestão de serviços de TI | Inexistência de catálogo formal de serviços de TI | 2 |
| | Falhas na gestão de serviços de TI | 4 |
| Avaliação do benefício esperado com investimentos em ações de TI | Inexistência de procedimentos para avaliação sistemática dos benefícios esperados com os investimentos em ações de TI | 3 |
| | Falhas na avaliação dos benefícios esperados com o investimento em ações de TI | 0 |
| | Ausência de critérios para seleção/priorização de investimentos de TI | 0 |
| Gestão de resultados de TI | Falha no acompanhamento do alcance dos resultados de TI | 2 |
| Resultados entregues pela TI | Baixo cumprimento das metas estabelecidas no planejamento de TI | 0 |
| Satisfação das áreas de negócio | Insatisfação dos clientes quanto aos serviços prestados pela TI | 2 |

*1 – Não houve encaminhamento quanto à gestão de serviços em um dos relatórios, porém a equipe tampouco registrou a sua existência. Outras informações presentes no relatório (TC 021.471/2013-4) sugerem que não há um processo de gestão de nível de serviço instituído.

Tabela 5 – Tabela de Achados quanto a resultados de TI

6.1 Gestão de serviços

159. A gestão de níveis de serviço é um dos instrumentos disponíveis à instituição para comunicar à TI os resultados que dela são esperados e permitir o monitoramento de sua entrega. O Acordo de Nível de Serviço (ANS) ou *Service Level Agreement* (SLA), em inglês, é um acordo estabelecido entre o fornecedor do serviço de TI e o seu cliente. O acordo estabelece os parâmetros sob os quais aquele serviço deverá operar e ser avaliado. Em geral, o ANS é estabelecido entre a unidade de TI da instituição e as unidades de negócio beneficiadas por seus serviços. Quando o ajuste é firmado entre a instituição e um fornecedor ou prestador de serviços contratado, o instrumento é denominado de contrato de nível de serviço.

160. Os números apresentados pelo 3º levantamento de governança em TI indicam que 88% das organizações pesquisadas não monitoram os níveis de serviço (peça 3, p. 22). A situação de baixa implementação indicada por esses números foi corroborada pelas fiscalizações em campo. Na primeira fase do trabalho, os achados indicam que foram detectadas falhas na gestão de nível de serviço em praticamente todas as organizações. A maioria (75%) não dispõe nem mesmo de um catálogo atualizado e formalizado com os serviços de TI disponíveis para uso dos clientes, fase inicial no estabelecimento de um processo de gestão de serviços.

161. Já na segunda etapa, quando foram fiscalizadas organizações de maior nível de capacidade em governança e gestão de TI, falhas foram apuradas em 80% das organizações

(4/5). A ausência de catálogo de serviços, no entanto, diminui para 40% (duas organizações não dispunham de catálogo). Esses números indicam que, mesmo em organizações de maior capacidade e maturidade em governança e gestão de TI, a gestão de serviços de TI ainda não é uma prática amplamente adotada no âmbito da APF.

162. A mensuração dos níveis de serviço prestados por fornecedores é um tema que está muito relacionado à contratação de serviços de TI. Como decorrência da consolidação de sua jurisprudência sobre esse assunto, essa Corte editou a Súmula TCU 269, com o seguinte teor:

Nas contratações para a prestação de serviços de tecnologia da informação, a remuneração deve estar vinculada a resultados ou ao atendimento de níveis de serviço, admitindo-se o pagamento por hora trabalhada ou por posto de serviço somente quando as características do objeto não o permitirem, hipótese em que a excepcionalidade deve estar prévia e adequadamente justificada nos respectivos processos administrativos.

163. Com efeito, observa-se que tal prática vem sendo adotada com maior frequência nos contratos de serviços de TI realizados com terceiros, servindo de instrumento para a avaliação das entregas feitas pelos fornecedores e também para definir sua remuneração. Espera-se que, assim como ocorrido com os contratos junto a terceiros, seja iniciado um processo de amadurecimento da gestão de serviços de TI entre as unidades de TI e o restante das unidades internas clientes de seus serviços.

164. Verifica-se, também, que o tema ainda suscita muitas dúvidas entre os gestores e técnicos das áreas de TI. Não há clareza quanto aos parâmetros pelos quais a gestão de nível de serviço deve operar ou quanto à forma de definição dos sistemas ou dos serviços geridos por meio de níveis de serviço. Ainda, não é claramente compreendido qual o papel das áreas de TI e das áreas de negócio nesse processo.

165. Contudo, já houve disposição a respeito da necessidade de normatização e de elaboração de modelos de processo de gestão de serviços no âmbito do Acórdão 1.233/2012-TCU-Plenário (itens 9.2.7, 9.2.8, 9.11.8, 9.13.7, 9.13.8, 9.15.10 e 9.15.11), portanto não há encaminhamentos a serem propostos nesse sentido em caráter sistêmico.

Propostas de encaminhamento

166. Sem propostas.

6.2 Avaliação de benefício esperado com investimentos em soluções de TI

167. Planejar as ações e avaliar previamente a conveniência de um investimento ou projeto é medida essencial para preservação dos escassos recursos públicos. Como decorrência do princípio constitucional da eficiência, exige-se que o administrador público zele pelos recursos existentes priorizando as ações que propiciem os resultados mais significativos com fundamento no interesse público.

168. Nesse sentido, os processos de governança do Cobit 5 foram estabelecidos em torno do que se denominou "criação de valor", expressão que corresponde a garantir a entrega de benefícios (processo EDM02 – *Ensure Benefits Delivery*), otimizando-se o uso dos recursos disponíveis (processo EDM04 – *Ensure Resource Optimisation*) e a níveis de risco aceitáveis (processo EDM03 – *Ensure Risk Optimisation*).

169. A descrição do processo EDM02 indica que é necessário "otimizar a contribuição para o negócio por parte dos processos de negócio, dos serviços e dos ativos de TI resultantes de investimentos feitos em TI a custos aceitáveis" (tradução livre). Em resumo, espera-se que o retorno advindo dos investimentos feitos em TI seja maximizado. Para tanto, depreende-se que é necessário estabelecer atividades que garantam que os investimentos em TI sejam previamente avaliados de forma a assegurar a priorização daqueles que representem melhor relação entre seu custo e o benefício entregue. Ainda, independentemente de priorização, é necessário garantir que investimentos em projetos ou soluções cujo retorno não atinja patamares mínimos aceitáveis não sejam colocados em prática.

170. Dessa forma, faz-se necessário o estabelecimento de processos, métodos e mecanismos que permitam essa avaliação de forma consistente e estruturada. O TCU também já manifestou-se a esse respeito em encaminhamento sistêmico dirigido ao Departamento de Coordenação e Governança das Empresas Estatais (Dest), no âmbito de auditoria coordenada em sistemas integrados de gestão, por meio do qual recomendou que as organizações jurisdicionadas fossem orientadas a elaborar e estabelecer formalmente:

9.2.3.4. processo de avaliação de custo-benefício para a contratação de novos serviços e produtos relacionados ao sistema integrado de gestão, com indicadores de avaliação dos investimentos alinhados ao cumprimento dos objetivos estratégicos, e monitoramento periódico desses indicadores;

171. Muitos gestores afirmam que não costumam realizar esse tipo de avaliação porque o negócio da administração pública federal, salvo algumas exceções, não está atrelado à obtenção de retorno financeiro. No entanto, é necessário esclarecer que a geração de valor decorrente do uso de TI não está somente relacionada à obtenção de lucro, mas também está ligada à otimização do uso de recursos e à redução de riscos.

172. Evidentemente, não é trivial estabelecer processos que estabeleçam objetivamente o retorno esperado desses investimentos, pois muitos desses visam a atingir ou propiciar benefícios de difícil mensuração, quando não intangíveis ou abstratos, tais como os benefícios decorrentes de uma solução que assegura maior transparência à gestão ou que assegura maior sustentabilidade a determinado processo de trabalho.

173. Muito embora existam dificuldades, não podem ser descartados os estudos que visam assegurar meios mais objetivos de se avaliar essa relação custo-benefício e de selecionar e priorizar projetos, pois possuem importância inegável diante do numeroso histórico de projetos mal sucedidos e que entregam soluções inservíveis e de baixa qualidade.

174. Em três das cinco organizações avaliadas no âmbito da FOC não se identificou a existência desses mecanismos de avaliação sistemática. Observa-se que ações nesse sentido são realizadas de forma *adhoc* e em situações ou projetos específicos. Por outro lado, em todas as organizações auditadas foram identificados mecanismos para priorização objetiva de projetos.

175. Contudo, há que se registrar a experiência de duas organizações que já lograram algum êxito no estabelecimento desse tipo de prática.

176. No caso da Petrobras (TC 024.827/2013-4, peça 94, p. 17-18), a equipe relatou que os investimentos em TIC são validados e priorizados no âmbito da Governança de TIC por gestores de macroprocessos da cadeia de valor da empresa, envolvendo áreas como exploração e produção, abastecimento, financeira, estratégica, entre outras. Os investimentos são avaliados com base nos seguintes parâmetros: escopo da demanda, benefícios esperados, impactos para o negócio, objetivos, estimativa de prazo e custo. Ao setor de Tecnologia da Informação e Comunicações (TIC) da empresa cabe avaliar as soluções técnicas mais adequadas para operacionalizar o investimento.

177. A análise posterior dos investimentos de TIC é realizada sob duas diferentes óticas: uma quanto ao sucesso do projeto e a outra quanto aos benefícios derivados do projeto.

178. Para todos os projetos de TIC que são realizados é feita a análise dos indicadores quanto ao seu desempenho (prazo e custo), ou seja, o projeto é avaliado continuamente pelo Escritório de Projetos. Adicionalmente, após a conclusão dos projetos de TIC, os gestores demandantes da solução realizam sua avaliação por meio de um questionário. Os atributos dessa avaliação são: prazo, custo, atendimento das necessidades e requisitos, atuação da equipe do projeto, satisfação do cliente e benefícios do projeto para a unidade de negócio. A satisfação dos clientes da TIC é, então, calculada por meio do Índice de Satisfação do Projeto (ISP). Esse indicador é monitorado regularmente pelos gestores de TIC, induzindo a acertos e melhorias no desempenho do processo.

179. Pode-se observar que não há processo sistemático de análise do Retorno de Investimento de TIC (ROI). Na análise do sucesso do projeto, a avaliação financeira dos resultados dos projetos é feita sobre o custo do projeto em relação à sua previsão orçamentária, podendo ir além, a depender do tipo de investimento. Os investimentos podem ser examinados, por exemplo, quanto à sua contribuição para a redução de riscos (projetos de Segurança da Informação) ou para a redução de custos.

180. O outro exame dos investimentos de TIC é feito sob a ótica dos benefícios gerados pelo projeto realizado. Esse processo tem o objetivo de auxiliar na condução da avaliação de benefícios (tangíveis e intangíveis) dos projetos e cumpre uma metodologia desenvolvida pela Petrobras em 2012 e que vem sendo aperfeiçoada. Essa metodologia pode ser aplicada a todos os projetos de TIC, embora, no momento, seja aplicada apenas a 50% dos projetos prioritários, ou seja, 2% dos projetos de TIC (TC 024.827/2013-4, peça 78, p. 4).

181. A área de escritório de projetos relata que o quantitativo de avaliações realizadas no âmbito desse processo é bastante reduzido em função de dificuldades encontradas, tais como: tangibilizar os benefícios para obtenção de valores que permitam avaliação; assegurar participação do cliente no levantamento e medição do benefício; "isolar" os benefícios específicos de TIC em um projeto maior do cliente, entre outros (TC 024.827/2013-4, peça 66, p. 2). Segundo o gestor, esse processo ainda não constitui um padrão obrigatório na Petrobras, estando ainda em nível de maturidade inicial. Apesar disso, ele se mostra uma iniciativa concreta e promissora no sentido de medir os resultados alcançados, contribuindo, portanto, para a mensuração do valor gerado pela TIC para a organização.

182. No caso do Banco do Nordeste do Brasil (TC 025.849/2013-1), verificou-se que, para os projetos propostos por outras áreas, a área de TI não realiza análise custo-benefício dos investimentos em TI, pois considera que esse papel deva ser exercido pela área demandante. Dessa forma, a área de TI avalia a viabilidade técnica e orçamentária do projeto, determina a melhor solução aplicável, define os custos das demandas e emite parecer à área proponente.

183. Por outro lado, quando a área de TI é a proponente da ação, deve ela mesma incluir a fundamentação da respectiva proposta e a avaliação do custo-benefício da mesma. Todavia, como as soluções propostas pela TI referem-se a soluções estruturantes e que atendem, em geral, a todas as áreas de negócio da instituição, não há uma análise específica em relação a quesitos de retorno financeiro, mas sim uma avaliação dos benefícios esperados.

184. Ressalta-se que os projetos, tanto da área de TI quando das áreas de negócio, são formalizados à alta administração por meio de Proposta de Ação Administrativa (PAA). A avaliação do custo-benefício dos mesmos é apresentada, via de regra, na seção de contextualização/fundamentação das propostas. Algumas das PAA avaliadas incluíram seções como: análise técnica, custos do projeto, receitas com o produto, cenários (básico, conservador, otimista). A diretoria é o órgão decisório responsável pela apreciação e aprovação das PAA com base em pareceres de unidades interessadas.

185. Em relação às outras demandas encaminhadas à área de TI, não inseridas diretamente em projetos de outras áreas, e que consistem no dia-a-dia da área de TI, o BNB utiliza um modelo de gestão de demandas. A metodologia utilizada contempla análise da demanda referente à gravidade, urgência, tendência e alinhamento estratégico. Esse modelo é usado apenas para soluções que não necessitam contratações, ou seja, soluções que são desenvolvidas internamente. Tal avaliação ocorre em dois momentos distintos:

a. em todas as demandas cujo esforço previsto de TI é maior que 90 horas, há uma análise de alinhamento ao negócio realizada pelo ambiente de planejamento;

b. posteriormente, o grau de alinhamento é utilizado para priorização do projeto/demanda pela área de TI, por meio do cálculo do respectivo índice.

186. Ressalta-se que, no fluxo de gestão de demandas, há uma etapa em que o aprovador da área de negócios valida o esforço e custo fornecido pela área de TI. Dessa forma, verifica-se

que também há uma preocupação com o custo-benefício para os casos de demandas de desenvolvimento interno para a área de TI do BNB.

Propostas de encaminhamento

187. Sem propostas.

6.3 Gestão de projetos

188. No caso do Banco Central do Brasil (BCB, TC 023.048/2013-1), embora a equipe tenha registrado achado diante da inexistência de procedimentos para avaliação sistemática dos benefícios esperados com investimento em TI, há algumas práticas ligadas à gestão de resultados que merecem menção.

189. Além das metas definidas no planejamento da TI, existem metas relacionadas aos projetos de TI que são conduzidos pelo setor de TI. Esses projetos, por seu turno, são alinhados a objetivos estratégicos de TIC definidos no PDTI. O BCB possui indicadores que permitem o acompanhamento periódico dos projetos pelo Departamento de Tecnologia da Informação (Deinf), tais como os projetos com início atrasado, com fim atrasado e com escopo alterado. Também é possível monitorar os projetos por unidade, por fase, quais estão em andamento, entre outros critérios de agrupamento.

190. Ainda em relação ao acompanhamento de projetos de TI, o Deinf realiza o monitoramento do "índice de desempenho de prazo médio dos projetos/TI" por meio de reuniões de acompanhamento gerenciais realizadas mensalmente. Segundo técnicos do BCB, esse índice é apresentado nessas reuniões, destacando-se os projetos que não alcançaram a meta estipulada. Em seguida, são apresentadas as causas e discutidas possíveis formas de correção.

191. Ao final de cada projeto de TI, são realizadas avaliações de qualidade. No que diz respeito à condução do projeto, são analisados critérios quanto à coordenação do projeto pelo gerente, suporte dos patrocinadores do projeto e o produto entregue, relacionamento dos clientes, alterações de escopo, satisfação e envolvimento do cliente no projeto, entre outros aspectos. Em relação ao produto entregue, o cliente avalia se este atendeu os requisitos acordados, se resolveu o problema real ou alcançou os benefícios esperados, se apresentou características inovadoras, se demonstrou praticidade e simplicidade no seu uso, se melhorou a capacidade do solicitante de realizar o seu trabalho e se os resultados do projeto possuem caráter duradouro, justificando, assim, os investimentos realizados.

192. No âmbito da gestão dos projetos corporativos, os quais podem estar vinculados a projetos e ações de TI, existe um índice específico para definição da prioridade dos projetos previsto em metodologia própria padronizada e formalmente instituída. Para tanto, são utilizados critérios como mandatoriedade, alinhamento estratégico, urgência, risco reputacional, impacto na cadeia de valor, entre outros.

193. A priorização dos projetos é feita pela área de planejamento e gestão, por meio da utilização de parâmetros e pesos para produção desse índice. Cabe destacar que a metodologia do BCB não utiliza critérios baseados em retorno financeiro ou diminuições de custos operacionais para priorização de projetos, uma vez que os projetos corporativos têm como principal objetivo o desenvolvimento organizacional da instituição. Cabe ao comitê de gestão de projetos ou à diretoria colegiada decidir quanto à manutenção ou à alteração da ordem de prioridade dos projetos.

194. Projetos e ações de TI que não constituem projetos corporativos são selecionadas e priorizadas por comitê interno da própria área de TI. Isso deverá ser modificado com a criação futura do comitê de priorização de TI, o qual será composto por representantes das áreas de negócio da instituição.

195. Ressalte-se que a participação das áreas de negócio no processo de priorização, controle e resolução de conflitos de recursos de projetos e atividades de TI também é recomendado pelo Cobit 5, Prática de Gestão APO01.01 – *Define the organisational structure*

(Definir a estrutura organizacional – tradução livre), atividade 8. Atualmente, o Deinf utiliza o "Índice de Atratividade" para priorização dos projetos de TI, gerado a partir da alimentação de vinte informações relativas a cada projeto, as quais medem a sua relevância, urgência, mandatoriedade, alcance, abrangência, alinhamento com o PDTI (diretrizes e objetivos estratégicos), se esse propiciará melhorias de processos internos, se compõe um projeto corporativo, entre outros (ex.: TC 023.048/2013-1, peça 32, componentes utilizados para cálculo do projeto "Provisão e Precatórios" – Sistema BCJur II).

196. A partir do preenchimento desses componentes é produzido o referido índice dentro de uma escala de zero até cem. Espera-se que esse índice subsidie as decisões do comitê de priorização, que será composto por representantes das unidades de negócio, quando esse for instituído.

197. O BNB, de forma semelhante, também estabelece critérios para classificação de projetos, tais como: contribuição para o planejamento empresarial (alinhamento); retorno do investimento, inovação, abrangência, risco do projeto, exigência legal ou institucional (TC 028.849/2013-1, peça 36, p. 58).

198. Consolidando-se a análise dessas três fiscalizações, depreendem-se as seguintes considerações:

a) Embora não seja trivial estabelecer processos de análise objetiva de custo/benefício ou de retorno sobre o investimento, este tipo de avaliação é possível em muitas situações;

b) Há organizações que têm empreendido esforços para identificar maneiras de tornar mais objetiva a mensuração de benefícios intangíveis;

c) As avaliações de benefícios esperados ou de retorno sobre o investimento devem ser realizadas de maneira integrada entre as áreas demandantes e a área de TI, pois os impactos positivos que a adoção de uma solução representa só podem ser melhor avaliados pelas áreas de negócio, enquanto os custos, dificuldades e riscos para a implementação precisam de informações tanto das áreas de demandantes quanto da área provedora de soluções de TI.

199. Mecanismos e critérios para seleção e priorização objetiva de projetos costumam ser mais frequentemente aplicados. Entre os parâmetros utilizados encontram-se alinhamento estratégico, benefício financeiro, complexidade (que também pode representar uma medida de risco do projeto), urgência, mandatoriedade, risco de reputação, impacto na cadeia de valor, entre outros.

200. É possível realizar avaliações objetivas do andamento e do sucesso de projetos. Para tais avaliações são adotados parâmetros quanto às várias dimensões de um projeto: prazo, custo, escopo, atuação da equipe de projeto e qualidade do produto. As informações coletadas podem ser de ordem direta, oriundas de cronogramas e sistemas de informação, bem como resultar de avaliações qualitativas decorrentes de questionários aplicados junto a gestores e clientes. A consolidação dessas informações pode resultar na elaboração de índices que permitam o acompanhamento periódico e concomitante dessas variáveis.

201. Verifica-se, no âmbito do Sisp, que a Estratégia Geral de TI 2013-2015 já contempla como indicador e meta do objetivo "4. Alcançar a efetividade na gestão de TI" o quantitativo de órgãos que adotam processos formais de gerenciamento de projetos. É recomendável que, no futuro, como extensão dessa avaliação, seja incluído como indicador a avaliação do número de projetos efetivamente gerenciados por meio de processos formais de gerenciamento de projetos.

202. Além disso, o Acórdão 1.233/2012-TCU-Plenário, por usa vez, já emitiu recomendação aos OGS para que normatizassem a respeito da obrigatoriedade de as organizações jurisdicionadas formalizarem processo de gerenciamento de projetos (itens 9.2.6, 9.11.7, 9.13.6, 9.15.9 do Acórdão 1.233/2012-P). Em razão disso, entende-se que não é cabível nova proposta para tornar obrigatória a adoção de práticas ligadas a gerenciamento de projetos.

Propostas de encaminhamento

203. Recomendar aos OGS, com base no Princípio da Eficiência insculpido no art. 37 da Constituição Federal, que orientem as unidades sob sua jurisdição a avaliar previamente a viabilidade de projetos de TI, incluindo, entre os objetos de análise, a verificação do custo/benefício do projeto, a exemplo do processo EDM02 – Assegurar a Entrega de Benefícios do Cobit 5.

6.4 Acompanhamento dos resultados da TI

204. No âmbito da primeira fase da FOC, como parte da avaliação do achado "Falhas nos mecanismos para dirigir e avaliar a gestão e o uso corporativos de TI", já discutido no âmbito da seção de Governança de TI deste relatório (seção 3.2), foram verificados os mecanismos de controle do cumprimento das metas de gestão e de uso corporativos de TI. Entende-se que o estabelecimento de mecanismos e de responsáveis pelo acompanhamento das metas dispostas nos planos institucionais é um desdobramento direto da aplicação dos princípios fundamentais da administração pública previstos nos incisos I e II do Art. 6º do Decreto-Lei 200/1976: os princípios do Planejamento e da Coordenação.

205. Constatou-se que em quinze organizações (75%) tais mecanismos não estavam definidos. O resultado negativo não chega a surpreender, até mesmo porque em doze organizações (60%) não havia nem metas definidas para serem acompanhadas.

206. Já na 2ª fase, foi constatada a ausência de um processo sistemático de acompanhamento dos indicadores e metas previstos nos planos da TI em duas organizações. Em uma delas as reuniões previstas não foram realizadas e em outra não havia definição da forma de acompanhamento ou designação de responsabilidades. Em outras três, no entanto, boas práticas foram observadas.

207. No caso do Banco Central do Brasil (TC 023.048/2013-1), para o PDTI anteriormente vigente, verificou-se o estabelecimento de ações estratégicas de TI. Para cada uma dessas ações, foram definidos objetivos, benefícios, produtos, público-alvo, indicadores, metas, alinhamento com o objetivo estratégico corporativo e o gerente responsável pela ação. Verificou-se a existência de metas quantitativas (ex.: 100% das estações de trabalho em conformidade com a Política de Segurança) e outras não quantitativas (ex.: reestruturação da intranet oferecendo boa navegabilidade e ferramenta de busca eficiente).

208. Foram designados os cargos responsáveis para cada um dos objetivos e ações estratégicas definidas nesse plano. Para cada objetivo estratégico do PDTI atual, é designado um Gerente de Projetos, responsável pela aferição dos indicadores do respectivo objetivo. A área de planejamento realiza a consolidação desses valores.

209. Os valores dos indicadores (de coleta automatizada ou não) são aferidos e apresentados anualmente a várias instâncias. De forma semelhante há um acompanhamento a cada ciclo (triênio) de vigência do PDTI.

210. Merece especial menção que, além desses instrumentos, há um sistema denominado "Agenda de Trabalho do BC" por meio do qual a alta administração da instituição obtém informações sobre o andamento das ações relacionadas aos objetivos estratégicos de TIC.

211. Na Chesf (TC 025.148/2013-3), a cadeia de responsabilidades quanto ao acompanhamento das metas e indicadores encontra-se definida. São previstas reuniões de acompanhamento dos responsáveis pelos projetos e, em seguida, reuniões com gestores da TI. Todas as informações são registradas ao longo da execução em sistema próprio e podem ser visualizadas por todos os usuários desse sistema, dentre eles os integrantes do comitê de TI, diretores e presidência. O acompanhamento contempla a situação atual das metas, dos indicadores, e fornece visão setorial (de cada diretoria) e da instituição como um todo.

212. Existe um calendário de reuniões de avaliação de desempenho dos departamentos, da área de TI e da diretoria administrativa que antecedem a reunião de avaliação do planejamento institucional envolvendo a presidência. Além disso, o escritório de projetos de TI também acompanha a execução das medidas relacionadas aos objetivos de TI, as quais são representadas

por projetos, com registro de informações relevantes ao gerenciamento (descrição das ações, etapas, atividades, datas, responsáveis, marcos etc.), compondo um conjunto de produtos a serem entregues ao final.

213. A Petrobras também possui mecanismos sofisticados e padronizados para acompanhamento dos objetivos, indicadores e metas estratégicos (TC 024.827/2013-4). A empresa possui um processo definido que estabelece a forma de definição, controle e monitoramento dos indicadores nos níveis estratégico, tático e operacional. Interessante destacar que há um mecanismo que indica as situações em que o indicador deve ser escalado para instâncias superiores, por exemplo, quando os resultados estiverem fora da meta por períodos consecutivos, podem ser escalados para reuniões de gerências de nível superior.

214. Uma boa prática na Petrobras indicada pela equipe de fiscalização é atribuir aos indicadores, além de metas esperadas, metas desafiadoras, também chamadas de desafios. Quando uma meta não é atingida, uma análise da razão é realizada e um plano de ação é elaborado, caso necessário. A reincidência de uma meta descumprida exige que o indicador seja apresentado à instância superior.

215. Chama a atenção o fato de várias organizações estabelecerem mecanismos para conexão entre a gestão de projetos e o planejamento estratégico e tático. Algumas estabelecem inclusive projetos para acompanhamento e persecução dos objetivos dispostos nos planos, conectando de forma indissociável os dois instrumentos.

216. Da análise das práticas adotadas pelas organizações fiscalizadas é possível sintetizar as seguintes boas práticas:

a) estabelecimento formal dos objetivos, metas e indicadores de TI nos respectivos planos;

b) atribuição de responsáveis pelos objetivos estratégicos;

c) definição de responsáveis pela aferição dos indicadores;

d) variados instrumentos de acompanhamento dos objetivos e metas de TI: sistemas, reuniões periódicas, relatórios etc;

e) acompanhamento de objetivos, metas e indicadores de projetos corporativos e de TI;

f) disponibilização dos indicadores estratégicos para acompanhamento por parte da alta administração por meio de relatórios ou sistemas específicos;

g) ações específicas quando do não atendimento de metas (discussão em reuniões, escalamento, planos de tratamento).

217. Entende-se que, tendo em vista o conjunto de práticas identificadas em organizações de alta maturidade e o fato de que muitas organizações ainda não aplicam essas práticas conforme percebido nas fiscalizações da primeira fase, há que se empreender esforços no sentido de divulgar e orientar a APF quanto à importância de serem estabelecidos processos e métodos de monitoramento periódico dos objetivos e metas de TI. A adoção desses mecanismos possibilita maior controle e gestão sobre o uso da TI em âmbito institucional, aumentando, assim, as chances de que a TI possa entregar valor para o negócio da organização.

218. Nesse sentido, cumpre ressaltar que, em outras ocasiões, o Tribunal já se manifestou no sentido de recomendar aos OGS que regulamentassem a obrigatoriedade de realizar acompanhamento efetivo dos planos e ações de TI, a exemplo de:

Acórdão 2.308/2010-TCU-Plenário

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;

Acórdão 1.233/2012-TCU-Plenário

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): (...)

9.1.2.5. **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;

219. Considerando que a emissão reiterada de recomendações por parte do Tribunal para que essas atividades fossem objeto de regulamentação obteve efeito limitado até o momento, com exceção do observado no Poder Judiciário, e que a situação encontrada na presente fiscalização demonstra a baixa adoção desses mecanismos de acompanhamento, entende-se que, por ocasião de futuro monitoramento desses Acórdãos, devem ser avaliadas as ações empreendidas pelos gestores nesse sentido e sua efetividade.

Propostas de encaminhamento

220. Recomendar aos OGS que, com base no art. 6º, inciso I, do Decreto-Lei 200/1967, orientem as organizações sob sua jurisdição a respeito da importância da adoção das seguintes práticas relativas ao planejamento de TI e seu acompanhamento:

1) atribuição de responsáveis pelo alcance dos objetivos e metas de TI;

2) definição de responsáveis pela aferição dos indicadores de TI;

3) disponibilização de indicadores estratégicos para acompanhamento por parte da alta administração por meio de relatórios ou sistemas específicos;

4) estabelecimento de instrumentos de acompanhamento, a exemplo de: sistemas, reuniões periódicas, relatórios;

5) definição de ações específicas para quando as metas de TI não forem alcançadas, a exemplo de: discussão em reuniões, escalamento, elaboração de planos de tratamento;

6) divulgação interna e externa do alcance das metas de TI, ou os motivos de elas não terem sido alcançadas.

6.5 Resultados entregues pela TI

221. Além de avaliar os processos, controles e práticas adotados pela instituição para desenvolver suas atividades com foco na avaliação de resultados, alguns procedimentos de auditoria foram aplicados para avaliar de maneira substantiva e concreta quais resultados têm sido entregues pela área de TI.

222. Para tanto, dois aspectos foram avaliados: o grau de cumprimento dos objetivos e das metas dispostos nos planos de TI e a percepção das áreas de negócio quanto à atuação da TI.

Por um lado, buscou-se avaliar em que medida a TI tem alcançado os objetivos pactuados junto à organização. Complementarmente, e de maneira mais prática, por meio de uma pesquisa junto às unidades de negócio que dependem das soluções de TI, buscou-se identificar de que forma os serviços e produtos entregues pelo setor de TI da instituição são avaliados pelas unidades clientes.

223. Primeiramente, há que se registrar que a avaliação do grau de cumprimento de metas por meio de comparações e consolidações entre organizações é bastante difícil, uma vez que cada instituição possui métodos próprios de definição de indicadores e metas, de acompanhamento e ciclos diferenciados para mensuração e revisão de indicadores.

224. Na fiscalização efetuada na Petrobras (TC 024.827/2013-4) a análise desses indicadores indicou que 53% (dez) apresentaram-se acima da meta, sendo que a maioria cumpriu uma meta denominada de desafiadora (oito). Os indicadores abaixo da meta (oito) representaram 42% do total de indicadores. No caso do BCB (TC 023.048/2013-1), foram avaliadas as metas estabelecidas no PDTI 2009-2011, cuja vigência foi estendida até o fim de 2012. De acordo com a avaliação empreendida (TC 023.048/2013-1, peça 77, p. 33), das 26 metas estabelecidas no PDTI, dezoito foram alcançadas pelo Banco. Além disso, das oito metas não atingidas, sete ficaram a menos de 10% de serem plenamente cumpridas pelo BCB, o que não implica desvio significativo em relação ao que foi definido no plano. Nos casos do HCPA (025.684/2013-2) e da Chesf (025.148/2013-3) não foi possível efetuar tal verificação. Já para o caso do BNB (025.849/2013-1), a equipe registrou informações constantes de um relatório da consultoria KPMG que avaliou o andamento de projetos estratégicos constantes do PETI (2012-2015). De acordo com tal relatório, o sumário geral de andamento dos projetos indica que o "planejado" estaria em 25% e o "realizado" em 36%. Em resumo, equipe entendeu que "o BNB tem atuado adequadamente na condução dos projetos previstos no PETI".

225. De maneira geral, não é possível consolidar essas informações, dada sua disparidade de formato e método de avaliação. No entanto, em nenhuma das fiscalizações ficou registrado baixo nível de atingimento dos objetivos e metas dispostos nos planos de TI. Embora não seja possível registrar com segurança, há hipótese de existência de uma correlação positiva entre o maior nível de capacidade em governança e gestão de TI dessas organizações e o atingimento dos objetivos e metas dispostos nos planos de TI.

226. Além do acompanhamento dos planos e metas, os resultados da pesquisa que avaliou a percepção das unidades de negócio clientes dos serviços de TI também registrou, de maneira geral, percepções positivas, a saber:

| | Inst. A | Inst. B | Inst. C | Inst. D | Média |
|---|---|---|---|---|---|
| Os sistemas contribuem efetivamente para a execução das atribuições da minha unidade. | 100% | 83% | 100% | 96% | 95% |
| Os sistemas raramente apresentam falhas, incorreções ou inconsistências | 89% | 61% | 80% | 71% | 75% |
| O tempo de resposta dos sistemas é adequado para desenvolver as atividades da unidade com eficiência. / a disponibilidade dos sistemas é adequada para desenvolver as atividades da unidade com eficiência. | 96% | 65% | 86% | 71% | 79% |
| A minha unidade está satisfeita com os serviços e soluções fornecidos pela área de TI da instituição. | 96% | 30% | 80% | 67% | 68% |
| Os recursos computacionais (computador; acesso à internet; impressora; correio eletrônico; etc) disponibilizados pela TI atendem satisfatoriamente à minha área de negócio. | 100% | 83% | 86% | 96% | 91% |
| Os serviços e os sistemas disponibilizados pela área de TI da minha instituição contribuem efetivamente para o alcance dos objetivos e metas da minha área de negócio. | 100% | 91% | 100% | 87% | 94% |
| A qualidade do atendimento das demandas de sistema (manutenções; evoluções e correções) é satisfatória. | 81% | 65% | 83% | 75% | 76% |
| O tempo para atendimento das demandas de sistema (manutenções; evoluções e correções) atende satisfatoriamente à minha área de negócio. | 59% | 22% | 51% | 54% | 46% |
| Gestores respondentes | 27 | 23 | 35 | 24 | 27 |

*Valores aproximados

227. As informações apuradas pela pesquisa indicam que há grande dependência das áreas de negócio das várias organizações por soluções de TI. A maioria indica que os serviços e sistemas disponibilizados são, de fato, necessários para o alcance de objetivos e metas das áreas de negócio.

228. De maneira geral, os gestores encontram-se satisfeitos com recursos computacionais disponíveis (91%) e com o tempo de resposta dos sistemas (79%). Com relação à confiabilidade dos sistemas, 75% indicaram que os sistemas raramente apresentam falhas, incorreções ou inconsistências.

229. A satisfação geral das áreas de negócio com os serviços prestados pela área de TI da instituição apresentou certa variabilidade. Na média, 68% alegam estar satisfeitos com os serviços, porém, notadamente uma das organizações conduziu esse índice para baixo, pois nessa entidade apenas 30% dos gestores indicaram satisfação com os serviços prestados. As causas específicas desse baixo índice revelado pela pesquisa precisam ser melhor avaliadas individualmente pela instituição e fogem ao interesse sistêmico dessa consolidação. Se desconsiderada essa instituição, esse mesmo índice sobe para 81% - valor bastante razoável.

230. Por fim, a questão que apresentou os menores índices de satisfação foi claramente a questão que tratava do tempo para atendimento das demandas de sistema. O resultado geral foi de apenas 46% de satisfação. Mesmo em organizações que atingiram alta satisfação das áreas de negócio com a TI (instituição A com 96% de satisfação), a satisfação com o tempo de atendimento para demandas de sistema foi de meros 59%. A instituição precitada que obteve o menor índice nesse quesito atingiu 22%.

231. Esse resultado sugere insatisfação das áreas de negócio para com a capacidade e velocidade da TI em atender suas demandas de sistema. Possivelmente, há demanda reprimida nessas organizações em função da dificuldade de as áreas de TI conseguirem atender tempestivamente às necessidades da instituição.

232. De maneira geral, da pesquisa aplicada a 109 gestores de áreas de negócio de quatro organizações pesquisadas, podem ser extraídas as seguintes inferências:

a) os sistemas de informação dessas organizações contribuem efetivamente para as atividades das áreas de negócio e colaboram de maneira efetiva para o alcance de metas e objetivos revelando grande alinhamento entre TI e negócio;

b) há alta satisfação com a estrutura computacional básica (recursos como estações de trabalho, correio eletrônico, internet e impressoras);

c) o tempo de resposta, a disponibilidade e confiabilidade dos sistemas (ausência de falhas e inconsistências) atingiu patamares positivos;

d) a satisfação geral com os serviços prestados pela área de TI pode ser considerada boa. Na média, caso desconsiderada a instituição que obteve apenas 30% de satisfação, foi de 81%;

e) o elevado índice de descontentamento com o tempo para atendimento das demandas de sistemas é um fator de preocupação para a alta administração das organizações e indica que as unidades desejam maior agilidade na prestação desse serviço.

233. As informações coletadas são limitadas, porém indicam, de um lado, uma possível correlação positiva entre o elevado estágio de capacidade das organizações em governança de TI com a sua capacidade de entregar serviços atendendo as expectativas dos usuários e áreas de negócio. Por outro lado, os resultados indicam que ainda há espaço para amadurecimento e melhora na agilidade e capacidade das áreas de TI de entregarem soluções nos prazos requeridos pelas unidades de negócio.

234. Com efeito, sugere-se, como possível área de atuação deste Tribunal e dos órgãos governantes superiores, a análise da cadeia de produção de software e de atendimento a

demandas de sistemas para avaliar as metodologias, práticas e estratégias empregadas pelas organizações, no sentido de identificar os pontos do processo que podem ser aprimorados com vistas a atender de maneira mais satisfatória as unidades de negócio fazendo o melhor uso dos recursos existentes.

Propostas de encaminhamento

235. Sem propostas.

7. GESTÃO DE RISCOS

236. O TCU julgou, recentemente, amplo trabalho de diagnóstico quanto à gestão de riscos na administração pública (Acórdão 2.467/2013-TCU-Plenário). Assim, discorreu a Ministra-Relatora Ana Arraes no voto que fundamentou o Acórdão (TC 011.745/2012-6, peça 200, p. 1):

a gestão de riscos é uma abordagem que, em qualquer organização, privilegia o alcance de resultados, de forma que sua mitigação, por meio de controles apropriados, tem potencial de garantir maior eficácia da gestão pública. No Brasil, com a inclusão da eficiência no rol dos princípios da administração pública (art. 37, caput, da Constituição), tornou-se "explícita a obrigação dos gestores públicos de direcionarem seus esforços para a consecução de resultados, sendo insuficiente o atendimento aos imperativos legais e normativos.

237. Como afirmou a Ministra-Relatora em seu voto, a depender da situação do setor avaliado, várias medidas podem ser adotadas com o fim de institucionalizar ou melhorar a gestão de riscos, como a implantação de processo de planejamento estratégico, a busca pelo envolvimento ativo da alta administração com a implantação de gestão de riscos e o investimento em ações de capacitação nessa área.

238. Conclui o relatório que "fortalecer a gestão de riscos nas organizações públicas implica aprimorar controles internos, o que, por sua vez, é requisito para uma sólida governança corporativa. Em outras palavras, investir em gestão de riscos é construir importante pilar para a governança".

239. No âmbito da tecnologia da informação, a gestão de riscos é considerada um dos pilares da criação de valor por parte da TI, juntamente com a entrega de benefícios e com a otimização do uso de recursos, de acordo com o Cobit 5. Logo, o processo de gerir e otimizar os riscos existentes necessita ser conduzido conjuntamente com esses dois outros elementos, pois as ações tomadas na gestão de riscos podem influenciar a entrega de benefícios e o uso de recursos.

240. Embora os riscos ligados à segurança da informação contemplem de maneira significativa processos e recursos ligados à TI, e já sejam até mesmo objeto de normatizações específicas – a exemplo da Norma Complementar 4 do Gabinete de Segurança Institucional da Presidência da República (NC 4 GSI/PR) – os riscos de TI ligados à segurança da informação não são a única espécie de risco de TI. Há diversos outros tipos de riscos que podem afetar o cumprimento dos objetivos de TI, tais como: riscos de projetos; riscos específicos de contratações; riscos ligados à disponibilidade de recursos humanos e orçamentários; riscos de mercado, geopolíticos, tecnológicos, regulatórios, entre outros. A título de exemplo, o livro "Cobit 5 for Risk" indica uma lista de riscos genéricos de TI organizados em vinte categorias diferentes.

241. Diante desse quadro, o presente trabalho estabeleceu procedimentos de avaliação da gestão de riscos de TI em questões de auditoria integrantes da 1ª e 2ª fases do trabalho, a saber:

1.6 Os processos de TI foram definidos e implementados adequadamente no âmbito da instituição?

2.3 A entrega de resultados é executada mediante adequada gestão de riscos de TI?

242. No âmbito dessas duas questões foi avaliada a atuação das organizações no que tange à gestão de riscos de TI sob vários aspectos: gestão de riscos de segurança da informação, governança sobre os riscos, estrutura para gestão de riscos, implantação de um processo de gestão de riscos de TI, conteúdo e operacionalização do processo, alinhamento com a gestão de riscos corporativa e com a gestão de riscos de segurança da informação, e a participação da auditoria interna nesse processo. A tabela a seguir apresenta o quadro-resumo de achados identificados:

| Tema<br>1ª Fase | Achado | Total<br>(20 unidades) |
|---|---|---|
| Gestão de Riscos | Inexistência de um processo de gestão de riscos de segurança da informação | 17 |
| Tema<br>2ª Fase | Achado | Total<br>(5 unidades) |
| Gestão de Riscos | Falhas de governança sobre os riscos de TI | 1 |
| | Inexistência de uma política de gestão de riscos corporativa | 0 |
| | Inexistência de um processo de gestão de riscos de TI | 1 |
| | Falhas no processo de gestão de riscos de TI | 0 |
| | Falhas na gestão de riscos de TI | 3 |
| | Falhas na avaliação da gestão de riscos de TI pela auditoria interna | 2 |

243. Na 1ª fase da fiscalização, em 85% das organizações verificou-se a inexistência de um processo para gestão dos riscos de segurança da informação. A ausência desse processo implica dizer que as ações para proteção das informações institucionais não estão respaldadas por análises consistentes, sistemáticas e periódicas para avaliação dos riscos aos quais as organizações estão sujeitas. Sem uma análise de riscos consistente, as ações podem não estar priorizadas de acordo com as principais necessidades de proteção da instituição.

244. Já com relação à 2ª fase, as auditorias lograram identificar atuações mais consistentes no que tange à gestão de riscos de TI. Em geral, os riscos ligados à tecnologia da informação são percebidos como uma espécie dos riscos existentes e aos quais estão sujeitos os processos de negócio em geral das organizações. Em nenhuma das organizações pesquisadas foi registrado o achado de "inexistência de uma política de gestão de riscos corporativa". Esse fato, de início, revela maior maturidade institucional quanto ao tratamento do tema, pois a política de gestão de riscos em caráter corporativo é o instrumento que orienta as ações de gestão de riscos na instituição como um todo.

245. Na maior parte das organizações fiscalizadas nessa 2ª fase também não foram registradas falhas de governança sobre os riscos de TI. Em especial, caso os riscos de TI não fossem regularmente objeto de monitoramento e avaliação de acordo com as diretrizes e parâmetros estabelecidos restaria configurada a falha de governança. No entanto, na maior parte das organizações foram identificadas a alocação de responsáveis e o estabelecimento de práticas com vistas à avaliação dos riscos de TI.

246. A existência de um processo de gestão dos riscos de TI também foi objeto de verificação. O achado não era registrado caso a instituição contasse com um processo específico para gerir os riscos de TI ou com um processo de âmbito corporativo que fosse responsável pela gestão desses riscos. De cinco organizações avaliadas, em apenas uma fiscalização foi registrado tal achado.

247. A situação, no entanto, ainda está longe da ideal, pois foram identificadas falhas na gestão dos riscos de TI (falhas na operacionalização do processo e no alinhamento da gestão de riscos de TI) em três organizações das cinco pesquisadas.

248. Em muitas delas, observa-se ainda que a gestão de riscos de TI tem sido executada de maneira independente da gestão de riscos corporativa. Embora existam políticas corporativas

para o tratamento do assunto, muitas vezes as ações práticas da gestão de riscos são desempenhadas exclusivamente pela TI com fundamento principalmente nos elementos tecnológicos de risco, tais como os riscos que afetam os centros de dados e as comunicações, entre outros. Nesses casos, o foco não está sob o impacto sobre os processos críticos da organização.

249. Conforme dispõe o processo EDM03 (Assegurar a Otimização de Riscos) do Cobit, é fundamental assegurar que os riscos de TI sejam gerenciados. Entende-se que isso deve ser realizado, independentemente se por meio de um processo específico de gestão de riscos de TI, ou por meio de um processo de gestão de riscos corporativo que considere os riscos de TI, desde que abranja, por exemplo, atividades estruturantes como as previstas na NBR ISO/IEC 31.000:2009:

a) entendimento da organização e seu contexto;

b) estabelecimento da política de gestão de riscos;

c) definição das responsabilidades, autoridades e competências envolvidas na gestão de riscos;

d) integração da gestão de riscos aos processos organizacionais;

e) alocação dos recursos apropriados para a gestão de riscos;

f) estabelecimento dos mecanismos de comunicação internos e externos.

250. Quanto à atuação da auditoria interna, de acordo com o item 2120 dos Padrões Internacionais para a Prática Profissional de Auditoria Interna instituída pelo Instituto dos Auditores Internos (IIA), a atividade de auditoria interna deve avaliar a efetividade dos processos de gerenciamento de risco e contribuir para o seu aprimoramento. No entanto, em duas organizações foram constatadas falhas na avaliação da gestão de riscos de TI por parte da unidade de auditoria interna.

251. Por fim, em nível estratégico, verifica-se que ainda não existe uma visão consolidada dos riscos de TI. A identificação e avaliação dos riscos de TI que podem afetar os objetivos e metas definidos para o setor jurisdicionado por meio de instrumentos como a Estratégia Geral de Tecnologia da Informação no âmbito do Sisp (peça 8) e a Estratégia de TIC do Poder Judiciário (peça 9) poderia maximizar o aproveitamento das oportunidades, apoiar a minimização dos riscos e favorecer a consecução dos objetivos e metas definidos.

252. A percepção geral, em especial no âmbito da primeira fase, é de que ainda há baixa adoção da prática de gestão de riscos de TI no âmbito das organizações. Isso se deve, em grande parcela, ao estágio inicial de amadurecimento das organizações no que tange a adoção de práticas consolidadas de governança e de gestão. A regulamentação da obrigatoriedade da prática, bem como a disseminação de instrumentos, guias e realização de capacitações, são algumas das ações que podem ser empreendidas pelos OGS para fomentar sua adoção.

Propostas de encaminhamento

253. Recomendar aos OGS, com base no inciso I no Art. 6º do Decreto-Lei 200/1976 c/c processo EDM03 – Assegurar a Otimização de Riscos do Cobit 5, que normatizem a obrigatoriedade de que todas as organizações sob sua jurisdição gerenciem os riscos de TI a que estão sujeitos por meio de um processo formal.

254. Recomendar aos OGS que, com base no inciso I do Art. 6º do Decreto-Lei 200/1976 e no processo EDM03 – Assegurar a Otimização de Riscos do Cobit 5, promovam ações de sensibilização e capacitação dos gestores das organizações sob sua jurisdição quanto à gestão de riscos de TI, com o objetivo de orientá-los na identificação, análise, tratamento e comunicação dos riscos a que a instituição está sujeita.

## 8. SEGURANÇA DA INFORMAÇÃO

255. Dentre os diversos temas objeto de processos de tecnologia da informação, a segurança das informações institucionais foi tema selecionado para avaliação em razão da percepção de que o cenário identificado nas últimas fiscalizações e levantamentos ainda está longe do desejável, ensejando riscos às organizações e à sociedade.

256. Além disso, os recentes episódios envolvendo ações de espionagem internacional e violação de sigilo das comunicações, inclusive das mais altas autoridades do país, trouxeram novamente o assunto ao primeiro plano das discussões internacionais sendo, inclusive, objeto de discurso da presidente Dilma Roussef na Assembleia Geral da ONU, realizada em setembro de 2013.

257. A esse respeito, por ocasião do 3º levantamento em governança de TI, o relatório da equipe responsável assim dispôs (peça 3, p. 19):

117. Verificou-se evolução de alguns percentuais de segurança da informação, o que sugere tendência de mudança de comportamento dos dirigentes públicos. A redução de outros percentuais não se traduz necessariamente em retrocesso, mas pode ser interpretado como amadurecimento dos gestores de TI no sentido de compreender melhor os conceitos relacionados à segurança da informação. De todo modo, o cenário identificado está longe de ser o desejável, tendo em vista os prejuízos que uma gestão deficiente de segurança da informação pode causar para a instituição e, sobretudo, para a sociedade.

258. Tendo em vista a importância do tema, assuntos ligados à segurança foram objeto de escopo da 1ª fase do trabalho por meio de procedimentos aplicados na seguinte questão:

1.6 Os processos de TI foram definidos e implementados adequadamente no âmbito da instituição?

259. Como resultado da aplicação desses procedimentos, foi possível efetuar a consolidação dos achados no seguinte quadro-resumo:

| Tema 1ª Fase | Achado | Total (20 unidades) |
|---|---|---|
| Gestão de continuidade de negócio | Falhas na gestão de continuidade de negócio | 16 |
| Gestão de ativos | Inexistência de inventário de ativos de informação | 16 |
| Controle de acesso | Inexistência de PCA | 14 |
| Conscientização e treinamento | Inexistência de programas de conscientização e treinamento em segurança da informação | 7 |
| Gestão de Riscos | Inexistência de um processo de gestão de riscos de segurança da informação | 17 |
| Política de Segurança da Informação | Inexistência de uma PCSI/PSI/POSIC | 6 |
| | Falhas na definição da PCSI/PSI/POSIC | 4 |
| Alocação de responsabilidades | Inexistência/Falhas atuação do comitê de segurança da informação | 6 |
| | Ausência de designação de responsável pela segurança da informação | 8 |
| | Falha / Inexistência de equipe de tratamento e resposta a incidentes em redes computacionais | 9 |
| Gestão de incidentes | Falhas na gestão de incidentes de segurança da informação | 15 |

260. Iniciou-se a avaliação da segurança da informação pela verificação da existência de uma Política de Segurança da Informação (PSI) – instrumento basilar de organização da segurança da informação institucional. A existência de uma PSI da instituição é requisito expresso pelo art. 5º, inciso VII, da Instrução Normativa GSI/PR 1/2008 e no art. 13 da Resolução 90/2009 do CNJ, bem como pela ampla jurisprudência do TCU a respeito do tema. Quanto ao estabelecimento e definição de uma PSI, verificou-se problemas em metade das

organizações (dez): em seis foi constatada a inexistência de uma PSI enquanto em outras quatro foram relatadas falhas em sua definição.

261. Ainda, foram objeto de avaliação as estruturas organizacionais requeridas para organizar e conduzir a segurança da informação. Quanto à alocação de responsabilidades, a situação não é muito diferente: 30% (seis) das organizações não contam com um comitê de Segurança da Informação e Comunicações (SIC) ou foram registradas falhas em sua atuação. Em 40% (oito) sequer houve a designação formal de um responsável pela gestão da segurança da informação e em 45% (nove) dos casos foi constatada a inexistência de equipe para tratamento de incidentes em redes computacionais ou falhas em sua designação (equipe não nomeada formalmente).

262. Quanto a outros processos, a situação é ainda mais crítica: em 75% das organizações auditadas na FOC foram identificadas falhas na gestão de incidentes de SIC; 70% não dispõem de uma política de controle de acesso; 80% não dispõem de inventário de ativos de informação.

263. A respeito da gestão de continuidade de negócio (GCN), de acordo com a Norma Complementar 6/GSI/PR, a implantação do processo de GCN busca minimizar os impactos decorrentes de falhas, desastres ou indisponibilidades significativas sobre as atividades do órgão ou entidade, além de recuperar perdas de ativos de informação a um nível aceitável, por intermédio de ações de prevenção, resposta e recuperação. O normativo também expressa que a GCN pode envolver ações mais abrangentes do que as definidas no âmbito da segurança da informação, especialmente devido aos requisitos estratégicos de continuidade relativos às pessoas, à infraestrutura, aos processos e às atividades operacionais.

264. De forma análoga, o CNJ dispôs, na Resolução CNJ 99/2009, como objetivos estratégicos para a tecnologia da informação e comunicações no âmbito do Poder Judiciário: promover a segurança da informação e garantir a disponibilidade de sistemas de TIC essenciais ao judiciário. Complementarmente, o Conselho também dispôs entre as diretrizes para segurança das informações (peça 7, p. 7), a necessidade de viabilizar a "continuidade do negócio, visando reduzir para um nível aceitável a interrupção causada por desastres ou falhas nos ativos que suportam os processos críticos de informação do órgão".

265. Dessa forma, a gestão de continuidade foi analisada sob dois aspectos: gestão de continuidade de negócios (nível corporativo) e gestão de continuidade de TI. A boa prática indica que as ações ligadas à gestão de continuidade de TI formam um subconjunto das ações que visam a garantir a continuidade do negócio como um todo. No entanto, historicamente verifica-se que as áreas de TI costumam adiantar-se no que tange à proteção dos ativos de informação. Analisando-se cumulativamente as duas falhas, verifica-se que 80% das organizações auditadas na FOC possuem falhas ligadas à gestão de continuidade.

266. Nesse sentido, entende-se que, muito embora tenha se avançado de maneira significativa na regulamentação de normativos e processos nesta área. Na prática, muitas organizações não têm empreendido ações nem disposto recursos para garantir a conformidade com as boas práticas requeridas nos normativos aplicáveis.

267. De maneira geral, entende-se que a segurança da informação nas organizações ainda carece de planejamento de suas atividades. O planejamento das ações de segurança da informação constitui uma medida que encontra amparo no Decreto-Lei 200/1967, art. 6º, inciso I, e de maneira específica no item 3.1 da Norma Complementar 02/IN01/DSIC/GSIPR.

268. Ademais, entende-se que seria necessário que os Órgãos Governantes Superiores, no âmbito de suas respectivas jurisdições, elaborassem a estratégia para aprimoramento da segurança da informação no âmbito do setor jurisdicionado, por meio da elaboração de objetivos e definição de metas e de indicadores. Entende-se que os exemplos da Estratégia Geral de Tecnologia da Informação no âmbito do Sisp e da Estratégia de TIC do Poder Judiciário deveriam ser reproduzidos no âmbito da segurança da informação.

269. Nos dois instrumentos, inclusive, já existem objetivos ligados à SIC: "Garantir a Segurança da Informação e Comunicações" e "Promover a segurança da informação", no âmbito do Sisp e Judiciário, respectivamente. Entende-se que essa prática poderia ser aprimorada com a elaboração de uma estratégia específica para a Segurança da Informação, uma vez que o tema segurança da informação ultrapassa os limites decorrentes do uso de tecnologia.

270. Nesse mesmo sentido, em setembro de 2013, um relatório do XIII Encontro Nacional de Estudos Estratégicos (peça 17), promovido pela Secretaria de Assuntos Estratégicos da Presidência da República, discutiu o setor cibernético brasileiro, seu contexto atual e perspectivas. Destaca-se, do texto, as seguintes conclusões, referentes ao Painel 1 (peça 17, p. 20) e ao Painel 2 (peça 17, p. 21), e Apreciação (peça 17, p. 25), respectivamente:

Como resultado é possível identificar que a governança do setor cibernético é relevante, em particular, para a coordenação da atuação do poder público, mas que qualquer iniciativa deve atentar para o que já existe. Melhorias na coordenação dos níveis político, estratégico e tático podem representar oportunidade de avanço em segurança e defesa cibernética. Em resumo, merecem especial atenção: a capacitação de pessoal, o marco legal, o fortalecimento de parcerias e a melhor coordenação do sistema de proteção.

(...)

Sobre a proposta de constituição do comitê gestor, foi ressaltada a necessidade de uma melhor coordenação no âmbito da administração pública federal. Mecanismos devem ser criados de modo a aumentar a interação com o setor privado e eliminar a duplicação de esforços ou sobreposição de tarefas.

(...)

Por tudo analisado, é possível inferir que existe uma lacuna de gestão político-estratégica na área cibernética nacional. Ela se materializa pela baixa articulação e coordenação intragoverno. É preciso definir diretrizes de longo prazo, a fim de orientar a formulação de políticas públicas com a finalidade de suprir necessidades presentes e futuras nas áreas ainda não cobertas pelas estruturas atuais.

Portanto, visualiza-se a possibilidade de formação de um grupo de trabalho legitimado, multissetorial, de modo a dar continuidade não apenas às discussões iniciadas no XIII ENEE, mas também com capacidade de propor uma agenda positiva de melhorias ao sistema de proteção do ambiente cibernético nacional. Esse grupo poderia abrigar as iniciativas já existentes e dar suporte a um eventual comitê multissetorial voltado para a discussão de estratégias de longo prazo para a segurança e defesa cibernética.

271. Registre-se que, em maio desse ano, a Sefti foi convidada a participar de um *workshop* em segurança cibernética, organizado pela Secretaria de Assuntos Estratégicos da Presidência da República (SAE/PR) e com participação do Grupo de Trabalho Interministerial (GTI) do Setor Cibernético. Segundo o convite, a ideia-chave era formular um plano estratégico de fortalecimento do setor cibernético (peça 16), o qual envolvia dimensões diversas como: recursos humanos, normatização, governança, colaboração etc.

272. O GTI foi criado pela Portaria 124/2013 da SAE/PR com o objetivo de elaborar proposta de Plano Estratégico para promover ou subsidiar o aperfeiçoamento das políticas públicas voltadas à segurança e defesa do espaço cibernético nacional. O resultado final, de acordo com a Portaria, deveria ser entregue no prazo de sete meses. O GTI seria extinto com a conclusão dos trabalhos previstos.

273. Em paralelo a esse esforço concentrado de planejamento de fortalecimento do setor cibernético, entende-se que o planejamento periódico de ações de segurança da informação em caráter amplo, a exemplo do que é realizado no âmbito do Sisp, permitiria a coordenação de esforços e o aproveitamento de sinergia entre as organizações. Sinalizaria as diretrizes a serem seguidas e estabeleceria os marcos a serem atingidos. Além disso, permitiria desdobrar a

estratégia em variados temas ligados à SIC, como por exemplo: normatização, capacitação, gestão de riscos, continuidade de negócio, relacionamento com a indústria e academia, inovação. Isso facultaria a definição de objetivos e metas mais detalhados para cada área que for considerada relevante. Atualmente, no âmbito das estratégias gerais de TIC, há um único objetivo e dois indicadores. É uma iniciativa elogiável, mas ainda pequena frente aos desafios dessa área.

274. Não se avaliou, no âmbito desse trabalho, especificamente a governança da segurança da informação e do setor cibernético, suas diferenças, os atores e suas respectivas competências. No entanto, no âmbito do Poder Executivo, especificamente no que concerne a segurança das informações e comunicações, o Gabinete de Segurança Institucional tem desempenhado papel preponderante na regulamentação do setor e na promoção de ações de capacitação. Esse papel decorre do inciso IV, do art. 6º da Lei 10.683/2003, lei que dispõe sobre a organização da Presidência da República e Ministérios, o qual estabelece como competência do Gabinete de Segurança Institucional da Presidência da República a coordenação das atividades de inteligência federal e de segurança da informação. No mesmo sentido, o inciso I, do art. 3º da Instrução Normativa GSI/PR 1/2008 dispõe que compete ao Departamento de Segurança da Informação e Comunicações (DSIC) do GSI "**planejar** e coordenar as atividades de segurança da informação e comunicações na Administração Pública Federal, direta e indireta" (grifou-se). Dessa forma, conclui-se que, no âmbito do Poder Executivo, o papel de promover o desenvolvimento de uma estratégia para melhoria da segurança da informação no âmbito daquele Poder cabe ao GSI, ainda que o faça em articulação com outros órgãos no âmbito das respectivas competências.

275. É evidentemente que, dada a alta interdependência entre os temas de tecnologia e de segurança da informação, as estratégias precisariam ser elaboradas em harmonia e de maneira cooperativa entre as organizações e setores responsáveis.

Propostas de encaminhamento

276. Recomendar ao Gabinete de Segurança Institucional da Presidência da República – GSI que, com base no inciso IV do Art. 6º da Lei 10.683/2003 c/c inciso I do Art. 3º da Instrução Normativa GSI/PR 1/2008, e em articulação com os demais órgãos competentes, elabore e acompanhe periodicamente, a exemplo do realizado na Estratégia Geral de Tecnologia da Informação no Sisp e da Estratégia de TIC no Poder Judiciário, planejamento que contemple a estratégia geral de segurança da informação para o setor sob sua jurisdição, envolvendo não somente a tecnologia da informação, mas também os demais segmentos relacionados à proteção das informações institucionais.

277. Recomendar ao Conselho Nacional de Justiça (CNJ) que, com base no §4 do Art. 103-B da Constituição Federal c/c preâmbulo da Resolução CNJ 70/2009, elabore e acompanhe periodicamente, a exemplo do realizado na Estratégia Geral de Tecnologia da Informação no Sisp e na Estratégia de TIC no Poder Judiciário, planejamento que contemple a estratégia geral de segurança da informação para o setor sob sua jurisdição, envolvendo não somente a tecnologia da informação, mas todos os segmentos relacionados à proteção das informações institucionais.

278. Recomendar ao Conselho Nacional do Ministério Público (CNMP), que com base no §2 do Art. 130-A da Constituição Federal, elabore e acompanhe periodicamente, a exemplo do realizado na Estratégia Geral de Tecnologia da Informação no SISP e da Estratégia de TIC no Poder Judiciário, planejamento que contemple a estratégia geral de segurança da informação para o setor sob sua jurisdição, envolvendo não somente a tecnologia da informação, mas todos os segmentos relacionados à proteção das informações institucionais.

279. Recomendar ao Gabinete de Segurança Institucional da Presidência da República – GSI que, com base no inciso IV, do Art. 6º da Lei 10.683/2003 c/c incisos I e V do Art. 3º da Instrução Normativa GSI/PR 1/2008, alerte as organizações sob sua jurisdição que a elaboração periódica de planejamento das ações de segurança da informação é obrigação expressa prevista

no item 3.1 da Norma Complementar 2/IN01/DSIC/GSIPR, além de ser boa prática prevista na NBR ISO/IEC 27.001/2013, item 6, bem como no Cobit 5, Prática de Gestão APO 13.2.

280. Recomendar ao Conselho Nacional de Justiça (CNJ) que, com base no art. 1º, inciso IV, alínea "g", Objetivo 9, da Resolução 99/2009 do CNJ c/c documento de Diretrizes para a Gestão de Segurança da Informação no âmbito do Poder Judiciário, alerte as organizações sob sua jurisdição que o estabelecimento de um modelo de gestão que contemple, entre outros processos, a elaboração periódica de planejamento estratégico de segurança da informação é diretriz expressa pelo Conselho Nacional de Justiça para a gestão da segurança da informação, além de ser boa prática prevista na NBR ISO/IEC 27.001/2013, item 6, bem como no Cobit 5, Prática de Gestão APO 13.2.

## 9. GESTÃO DE RECURSOS

281. A adequada gestão dos recursos disponíveis às organizações para a consecução de seus objetivos decorre diretamente do princípio da eficiência, expresso no art. 37 da Constituição Federal. Os recursos disponíveis às organizações compreendem tanto os recursos humanos alocados para execução de funções próprias da instituição quanto os recursos financeiros disponíveis para a aquisição de bens ou contratação de serviços.

282. Nesse sentido, a gestão dos recursos humanos, a capacitação, as contratações de TI e a gestão orçamentária e de custos de TI foram objeto de avaliação dessa FOC. Essa avaliação foi levada a efeito por meio de duas questões de auditoria:

1.5 Os mecanismos de gestão de pessoal de TI foram definidos e implementados adequadamente no âmbito da instituição?

2.2 A instituição dispõe de mecanismos adequados para analisar benefícios esperados dos investimentos em TI, gerenciar custos e acompanhar os resultados esperados do setor de TI?

| Tema<br>1ª Fase | Achado | Total<br>(20 unidades) |
|---|---|---|
| Gestão dos recursos humanos em TI | Funções gerenciais de TI ocupadas por pessoal de fora da instituição | 2 |
| | Ausência de avaliação quantitativa e qualitativa da força de trabalho necessária à área de TI | 8 |
| | Insuficiência de recursos humanos de TI frente às necessidades identificadas pela organização | 9 |
| Capacitação | Inexistência / Falhas na implementação de um plano periódico de capacitação | 10 |
| Planejamento e gestão de contratações de TI | Falhas no planejamento das contratações de TI | 9 |
| | Falhas na gestão das contratações de TI | 9 |
| Tema<br>2ª Fase | Achado | Total<br>(5 unidades) |
| Contratações de TI | Falhas na definição dos resultados esperados com a contratação | 2 |
| | Falha no planejamento dos riscos da contratação | 4 |
| | Falhas na avaliação dos serviços prestados | 0 |
| | Falhas no acompanhamento dos resultados esperados pela contratação | 0 |
| Gestão de orçamento e custos de TI | Falhas na gestão de orçamento e de custos de TI | 2 |

### 9.1 Gestão dos recursos humanos em TI

283. Os recursos humanos estão listados entre os elementos viabilizadores da governança e da gestão de TI no Cobit 5 em razão de sua imprescindibilidade para a estruturação e fornecimento de serviços da TI. Esse tema também tem sido objeto de reiterada preocupação desta Corte de Contas, que tem se manifestado a respeito da importância das organizações realizarem avaliações quantitativas e qualitativas do quadro de profissionais de TI disponíveis de forma a fundamentar futuros pleitos de ampliação e preenchimento de vagas (Acórdãos 465/2011, 592/2011, 758/2011, 2.613/2011, todos do Plenário).

284. A carência de recursos humanos nas áreas de TI ganhou tal relevância que foi alçada à condição de destaque no Voto do Ministro-Substituto Augusto Sherman na apreciação das Contas de Governo, Exercício de 2012:

176. destaco, nesta ocasião, a necessidade de a Administração Pública aprimorar a política de pessoal da área de TI. Isto porque, em essência, se a estrutura de pessoal estiver bem cuidada, a tendência natural é a paulatina resolução da maioria das fragilidades atinentes à governança de TI. E sem a incorporação à estrutura de pessoal do Estado brasileiro de bons gerentes de TI, dificilmente alcançaremos as melhorias pretendidas e necessárias, tanto na governança de TI quanto nas contratações públicas de TI.

285. Mais recentemente, o TCU realizou amplo levantamento a respeito da situação da área de pessoal em TI na administração pública federal, resultando no Acórdão 1.200/2014-TCU-Plenário. Em seu voto como Ministro Revisor, o Ministro-Substituto Augusto Sherman Cavalcanti afirmou:

8. Pois bem, o presente levantamento recentemente realizado ao final de 2013, mais abrangente e dedicado em relação aos recursos humanos disponíveis e alocados, revela a persistência de problemas como a falta de cargos estruturados em carreiras, carência de pessoal especializado, ocupação de cargos de gestão por pessoas estranhas ao quadro efetivo, ausência de planejamento para o preenchimento contínuo de vagas de TI, dificuldades de retenção de pessoal contratado devido aos baixos salários comparativamente a outras carreiras e à ausência de perspectivas de progressão profissional, qualificação do pessoal sem planejamento, dentre outros problemas.

286. Nesse mesmo sentido, a verificação realizada no âmbito da 1ª fase da FOC logrou identificar que 40% das organizações não haviam realizado nenhuma espécie de análise objetiva das necessidades de recursos humanos para atuação com tecnologia da informação na instituição. Outros 45%, embora dispusessem do referido diagnóstico, concluíram que os recursos humanos disponíveis atualmente são insuficientes frente às necessidades apontadas pelo estudo. Em outras palavras, os diagnósticos apontaram carência de recursos humanos especializados em TI para atender satisfatoriamente o negócio da instituição.

287. Sob esse aspecto, chamou a atenção o caso da Superintendência da Zona Franca de Manaus (Suframa). De acordo com o relatório de auditoria (021.789/2013-4), a instituição dispõe de apenas três servidores efetivos e 102 empregados terceirizados contratados. De acordo com a equipe, tal situação configura deficiência administrativa que evidencia sua estagnação comparada à evolução de outras organizações públicas.

288. Tal situação possivelmente afronta o arcabouço normativo, uma vez que pode estar em desacordo com a jurisprudência dominante desta Corte, que tem primado pela contratação de serviços por meio da remuneração vinculada a resultados, em detrimento de mera terceirização de postos de trabalho. Assim dispõe a Súmula 269:

Nas contratações para a prestação de serviços de tecnologia da informação, a remuneração deve estar vinculada a resultados ou ao atendimento de níveis de serviço, admitindo-se o pagamento por hora trabalhada ou por posto de serviço somente quando as características do objeto não o permitirem, hipótese em que a excepcionalidade deve estar prévia e adequadamente justificada nos respectivos processos administrativos.

289. Tendo em vista o escopo padronizado da FOC e o reduzido prazo para a execução das três fiscalizações a cargo de cada equipe, a auditoria não aprofundou-se na avaliação desse contrato. No entanto, essa situação foi encaminhada à equipe de coordenação da FOC de contratações de TI (TC 014.815/2014-1), uma vez que a Suframa será uma das organizações auditadas quanto à gestão de contratos de TI no âmbito daquela fiscalização.

290. Ainda a respeito da gestão dos recursos humanos, verificou-se que, sob a ótica da capacitação, ainda há muito a se avançar. Em 50% das organizações registrou-se achado

referente à inexistência de plano de capacitação que envolva aspectos necessários à gestão da TI.

291. Considerando que, recentemente foi prolatado o Acórdão 1.200/2014-TCU-Plenário, que contém encaminhamentos sobre o dimensionamento dos quadros de pessoal de TI, bem como sobre as estratégias de capacitação em TI, entende-se ser mais adequado dispensar a emissão de encaminhamentos aos OGS a respeito desse tema, em favor daqueles já expedidos no Acórdão 1.200/2014-TCU-Plenário.

Propostas de encaminhamento

292. Sem propostas.

9.2 Gestão de custos de TI

293. Um outro importante componente da entrega de valor é o conhecimento e a adequada gestão dos custos de TI existentes. Inicialmente, há que se efetuar uma certa distinção entre gestão orçamentária de TI e gestão de custos de TI, pois embora tais temas sejam altamente interdependentes há algumas nuances que precisam ser exploradas.

294. Historicamente, em sentido estrito, a gestão dos custos da TI não foi um tópico frequentemente abordado pelas fiscalizações de TI realizadas pela Sefti. Na verdade, as organizações públicas, de maneira geral, encontram dificuldades para dimensionar o custo da tecnologia da informação.

295. O conceito de orçamento de TI, ao contrário, em razão dos preceitos e diversos dispositivos legais que orientam a elaboração, execução e monitoramento da execução orçamentária, encontra-se mais amplamente difundido entre as organizações públicas federais. Além disso, há ampla interconexão com as contratações de TI, razão pela qual frequentemente a previsão orçamentária dos gastos e investimentos de TI é objeto de avaliação das fiscalizações.

296. Nesse sentido, o objetivo da FOC foi avaliar de que forma as organizações de maior maturidade estavam tratando a gestão de orçamento e custos de TI. Pretendia-se com essa avaliação, que foi realizada apenas nas organizações que foram auditadas na 2ª fase da FOC, iniciar o desenvolvimento de estratégias de fiscalização e controle sobre esses aspectos, além de coletar boas práticas que pudessem ser disseminadas para organizações públicas que fossem menos desenvolvidas nesses temas.

297. O principal referencial para governança e gestão de TI, o Cobit 5, dispõe esses temas em torno de um processo denominado APO06 – *Manage Budget and Costs* (Gerenciar orçamento e custos, tradução livre), descrito como o ato de gerenciar as atividades financeiras relativas à TI em ambas as funções – negócio e TI – cobrindo orçamento, custo e gerenciamento de benefícios, e priorização de gastos de acordo com a adoção de práticas orçamentárias formais e um sistema de alocação de custos à organização.

298. O objetivo do processo é fomentar a parceria entre o setor de TI e as partes interessadas para habilitar o uso eficiente e eficaz dos recursos de TI, promovendo a transparência e a responsabilidade sobre o custo e valor das soluções e serviços. Em resumo, o objetivo é viabilizar a tomada de decisões bem fundamentadas quanto ao uso de soluções e serviços de TI considerando os custos necessários e orçamento disponível.

299. Esse processo se subdivide em cinco atividades:

1) APO06.01 – Gerenciamento financeiro e contábil
2) APO06.02 – Priorizar alocação de recursos
3) APO06.03 – Criar e manter orçamentos
4) APO06.04 – Modelar e alocar custos
5) APO06.05 – Gerenciar custos

300. De acordo com o Cobit 5, a atividade APO06.4 prevê o estabelecimento e uso de um modelo de custos de TI baseado na definição dos serviços, assegurando que a alocação de custos para os serviços seja identificável, mensurável e previsível para encorajar o uso responsável dos recursos, inclusive aqueles disponibilizados por provedores de serviços. A atividade APO06.05, por sua vez, prevê a implementação de um processo de gerenciamento de custos que compare os custos presentes com os orçamentos de forma que haja monitoramento e reporte, e que, em caso de desvios, esses sejam identificados tempestivamente e seu impacto avaliado.

301. A partir dessa base conceitual, foram definidos procedimentos de auditoria para verificar:

1) presença de um orçamento de TI;

2) existência de um processo de gestão de orçamento e de custos de TI;

3) formalização do processo;

4) completude do processo (se inclui orçamento, custos em geral, custos de recursos humanos, custos indiretos, entre outros);

5) monitoramento dos custos de TI;

6) alocação dos custos de TI aos serviços prestados.

302. Em duas das cinco fiscalizações foi registrado o achado "Falha na gestão de orçamento e custos de TI". Em uma delas em razão da inexistência de um processo de gestão de orçamento e custos de TI e na outra em razão da não formalização e incompletude do processo. Contudo, entende-se que, em função da avaliação dos processos de gestão de custos de TI não se constituir em uma disciplina ainda consolidada no TCU, houve certa variabilidade na classificação das situações encontradas como achados. Assim, os resultados obtidos nessa avaliação possuem maior valor no sentido de descrever as práticas adotadas do que sob o aspecto quantitativo da avaliação.

303. De maneira geral, observou-se que as organizações pesquisadas dispõem de orçamentos de TI. No entanto, os custos indiretos não costumam integrar esse orçamento. Custos como os de recursos humanos ou de infraestrutura (energia elétrica e espaço físico) costumam ser contabilizados por outras unidades, tais como a área administrativa ou de logística.

304. A maioria das organizações também não possui práticas para segregar os custos de TI nos serviços que presta à instituição. Assim, a alocação de custos aos serviços ainda é um objetivo a ser conquistado nessas organizações. Dessa forma, fica prejudicado o rateio desses custos com as áreas demandantes e também a transparência dos custos da TI, pois não é possível identificar com precisão quais serviços demandam mais recursos de TI.

305. Em especial, o fato de o acompanhamento orçamentário e de custos de TI não contemplar os dispêndios com recursos humanos (remuneração, treinamento etc.) torna turva e limitada a visão da evolução dos custos de TI. Por exemplo, uma instituição que decida internalizar serviços anteriormente terceirizados com consequente aumento do quadro de pessoal pode estar sinalizando uma economia de recursos em razão da redução dos gastos diretos com contratos celebrados com fornecedores externos, quando na verdade pode até mesmo estar dispendendo valores superiores em razão das contratações de pessoal para o seu quadro efetivo.

306. A esse respeito, torna-se evidente a conclusão de que muito embora os custos com recursos humanos possam continuar a ser objeto de acompanhamento por outras unidades da instituição, é necessário que existam relatórios e mecanismos de contabilização dos gastos com TI que permitam à instituição uma visão consolidada das despesas com TI, incluindo as despesas com recursos humanos próprios.

307. Por outro lado, em uma das organizações, foi possível observar a adoção de um processo mais consolidado de gestão de custos de TI. Na Petrobras (TC 024.827/2013-4), a equipe relatou:

101. A área de TIC da Petrobras representa um centro de custo da empresa. A apropriação e repasse de custos de TIC está modelada de forma a permitir a identificação e o acompanhamento dos custos de projetos e serviços de TIC para depois repassá-los aos clientes da TIC.

(...)

103. A comunicação às partes interessadas é feita por meio de um demonstrativo dos serviços prestados pela TIC, que nada mais é do que um extrato com todos os serviços prestados, contendo a quantidade, o custo e o valor total. (...)

104. Um dos benefícios desse demonstrativo é criar uma cultura de responsabilidade, por parte dos gestores e usuários da TIC, em relação ao custo dos serviços de TIC prestados, uma vez que cada unidade deduz do seu próprio orçamento os gastos e investimentos com TIC.

308. Como conclusão, observa-se que há estreita correlação entre o aperfeiçoamento da gestão de custos e a gestão de serviços de TI. Para que seja possível efetuar uma alocação dos custos aos diferentes serviços providos é necessário dispor de catálogo de serviços consistente. Entende-se que esse é um caminho a ser trilhado no sentido de se obter maior transparência sobre os gastos de TI ensejando também maior responsabilidade na alocação de investimentos e solicitação de serviços por parte das unidades organizacionais.

Propostas de encaminhamento

309. Recomendar aos OGS, com base no Princípio da Eficiência insculpido no *caput* do art. 37 da Constituição Federal, que orientem as unidades sob sua jurisdição no sentido de aprimorar os respectivos processos de gestão de orçamento e de custos de TI, a exemplo do disposto no processo APO06 – Gerenciar orçamento e custos do Cobit 5, com vistas a permitir a visualização e o acompanhamento da evolução dos custos diretos e indiretos de TI, incluindo, por exemplo, os custos ligados a recursos humanos (remuneração, treinamento etc.) e infraestrutura;

310. Recomendar aos OGS, com base no Princípio da Eficiência insculpido no *caput* do art. 37 da Constituição Federal, que elaborem um modelo de custos de TI para servir de referência para as organizações jurisdicionadas, baseado na definição dos serviços prestados, de forma a tornar a alocação de custos aos serviços de TI identificável, mensurável e previsível, a exemplo do previsto na prática APO06.04 – Modelar e alocar custos do Cobit 5.

9.3 Contratações de TI

311. Para o cumprimento dos objetivos de negócio, as organizações normalmente necessitam realizar contratações de bens e serviços de TI. Com efeito, os processos adotados para planejamento das contratações e gestão dos contratos firmados são um instrumento importante para a padronização dessas atividades na instituição, para a organização dos controles e para a obtenção de melhores resultados com sua execução.

312. Com efeito, no âmbito da primeira fase da FOC foram aplicados testes de auditoria para verificar a adoção por parte das organizações de processos formais de planejamento e de gestão das contratações de TI. A existência de processos permite que as organizações padronizem e organizem as práticas ligadas às contratações de TI, tornando-as perenes mesmo com a mudança dos gestores, algo frequente no âmbito da APF.

313. Cumpre ressaltar que, mesmo no caso de organizações integrantes do Sisp ou jurisdicionadas ao CNJ e sujeitas aos ditames, respectivamente, da IN – SLTI/MP 4/2010 e da Resolução CNJ 182/2013, entende-se que o estabelecimento de processos é desejável. Os referidos normativos estabelecem uma série de atividades e artefatos a serem produzidos, contudo tendo em vista tratarem-se de normas de ampla abrangência, elas não contemplam

aspectos específicos inerentes à organização de cada instituição e poderiam ser complementados por dispositivos específicos no âmbito de cada instituição.

314. É conveniente que cada instituição, considerando a sua estrutura organizacional, recursos e outros regulamentos internos, estabeleça de que forma as suas contratações de TI deverão ser processadas em seu âmbito interno. A esse respeito, o Guia de Boas Práticas em Contratação de Soluções de Tecnologia da Informação do TCU, versão 1.0, assim dispõe:

Para garantir que o processo de trabalho de planejamento da contratação de soluções de TI seja seguido de forma padronizada, torna-se necessária a sua formalização, divulgação e capacitação dos servidores envolvidos. Esse processo de trabalho deve ser publicado após sua aprovação pela alta administração do órgão.

315. Em nove de vinte organizações (45%) avaliadas, constatou-se a inexistência de processos formais para planejamento e gestão das contratações de TI. Os resultados indicam que ainda é possível se avançar, mesmo no âmbito já bastante normatizado como o das contratações, pois muitos gestores ainda não estão conscientizados a respeito da importância do estabelecimento desses processos, confundindo as disposições contidas nos normativos (em especial a IN – SLTI/MP 4/2010) com o conteúdo de um processo dessa natureza.

316. No âmbito da segunda fase da FOC, a avaliação relativa às contratações de TI teve um escopo bem distinto, pois foram objetos de análise os aspectos ligados mais diretamente a riscos e resultados de TI.

317. Primeiramente, foi avaliada a adoção da prática de gestão de riscos nas contratações. Em particular, procurou-se verificar se as organizações analisavam os riscos inerentes às contratações que realizam. Em quatro das cinco organizações avaliadas foram identificadas falhas na análise dos riscos da contratação. Em três registrou-se a inexistência de um processo de avaliação dos riscos da contratação enquanto que na quarta verificou-se que um processo fora adotado, mas não estava padronizado ou formalizado. Na quinta instituição, embora a equipe de auditoria não tenha registrado um achado específico, no relato da situação encontrada de outro achado a equipe registrou (TC 023.048/2013-1, peça 81, p. 27):

a análise de riscos apresentada, que compôs o planejamento da contratação, também foi considerada insuficiente. Ela não relaciona os principais riscos que podem comprometer o sucesso do processo de contratação e de gestão contratual, ou que podem fazer com que a solução de TI pretendida não alcance os resultados que atendam às necessidades da contratação [...]. Ela se limita apenas a identificar o risco da não contratação da solução, [...]

318. Assim, constatou-se que analisar os riscos não é uma prática consolidada e integrante do processo de planejamento das contratações dessas organizações, a despeito de constar como etapa cumprimento obrigatório prevista nos normativos.

319. Sob outro aspecto do planejamento da contratação, tendo em vista a consolidação da prática da remuneração dos fornecedores de serviços de TI vinculadas à entrega objetiva de resultados, procurou-se verificar se as organizações estavam: levantando as necessidades da contratação; definindo os produtos a serem entregues ou o nível de serviço a ser cumprido; indicando o alinhamento da contratação com os objetivos estratégicos de TI; estabelecendo os critérios para avaliação da qualidade dos produtos ou serviços contratados.

320. Em duas das organizações fiscalizadas na segunda fase da FOC foram observadas falhas na aplicação dessas práticas. Entre as falhas apuradas estão: inexistência de Documento de Oficialização da Demanda (DOD), previsto na IN – SLTI/MP 4/2010 (TC 023.048/2013-1, peça 77, p. 30); ausência de definição de níveis de serviço esperados (TC 025.849/2013-1, peça 45, p. 22); falta de demonstração do alinhamento estratégico da contratação (TC 025.849/2013-1, peça 45, p. 22).

321. Como exemplo, conforme apontado pela equipe de auditoria, tais "desconformidades identificadas nesse achado poderiam ter sido evitadas caso os *templates* de contratação de soluções de TI definidos pela entidade tivessem sido utilizados durante o planejamento dessa

contratação" (TC 023.048/2013-1, peça 81, p. 27). Mais uma vez, reforça-se a necessidade do estabelecimento de processos para o planejamento e gestão das contratações de TI, conforme consignado nos parágrafos 314 e 315.

322. De forma semelhante, outra equipe consignou falhas na definição dos níveis de serviço esperados para um contrato de suporte técnico. A equipe assim registrou no relatório (TC 025.849/2013-1, peça 51, p. 17):

Outro ponto evidenciado em relação ao contrato de prestação de serviços de assistência e suporte técnico à plataforma mainframe é que não há no mesmo vinculação da remuneração do fornecedor a resultados ou ao atendimento de níveis de serviço. Ou seja, não há o pagamento mediante a aferição de resultados observáveis, mas sim um desembolso fixo mensal.

323. Assim, conclui-se que, embora os normativos sejam prescritivos quanto a uma série de práticas a serem adotadas, ainda há espaço para aprimoramento. Verifica-se que ainda há baixa conscientização a respeito da importância da implantação de processos institucionais para planejamento e gestão das contratações. Além disso, entende-se que a aplicação prática dos normativos ainda precisa evoluir, pois as falhas de conformidade identificadas nos trabalhos realizados em organizações de maior maturidade demonstram que ainda há situações em que as regras estabelecidas não têm sido aplicadas.

324. Considera-se, no entanto, que, de maneira geral, os OGS têm atuado no aprimoramento dos processos relativos a contratações de TI, tanto pela via normativa, promovendo e revisando os regulamentos, quanto pela via da orientação e capacitação, com a publicação de guias e promoção de capacitações. Exemplos que podem ser citados são a edição de normativo sobre contratações de TI no Poder Judiciário (Resolução CNJ 182/2013), no Ministério Público (Resolução CNMP 102/2013), bem como a publicação de nova edição da IN 4/SLTI/MP, em 11/9/2014. A nova versão da IN, inclusive, já dispõe a respeito da possibilidade de as organizações promoverem, via regulamentos internos, a harmonização de preceitos da IN4 à sua estrutura funcional, conforme dispõe o §3º, do art. 1º da IN. Por essas razões, entende-se que no âmbito dessa consolidação não há propostas de encaminhamento, em caráter sistêmico, a serem emitidas aos OGS.

Propostas de encaminhamento

325. Sem propostas.

9.4 Questionário a respeito de riscos e dificuldades em contratações de TI

326. Por fim, tendo em vista o aspecto operacional da fiscalização empreendida, os gestores de TI de quatro organizações fiscalizadas na segunda fase foram indagados a respeito dos riscos e dificuldades enfrentados na realização de contratações de soluções de TI por suas organizações. Para tanto, foi aplicado um questionário padronizado (peça 13) para coleta de informações. O questionário abordava três temas: modelo de remuneração de serviços contratados e métricas adotadas; local de prestação dos serviços contratados; e preços de mercado.

327. Quanto ao percentual de serviços remunerado por meios objetivos, três organizações informaram que entre 76 e 100% dos seus serviços de TI são remunerados objetivamente.

328. Quanto às métricas adotadas, observa-se desde a adoção de métricas amplamente utilizadas pelo mercado, como a análise de pontos de função, métrica mais citada para medição de tamanho de software, quanto o uso de métricas específicas para a instituição ou para um dado tipo de serviço.

329. Foram também citadas como instrumentos de medição várias outras técnicas/métricas, categorizadas da seguinte forma:

330. Relativas a tamanho: Pontos de caso de uso; Pontos de sustentação; Unidades de serviço técnico; Horas de serviço técnico (HST); páginas impressas; quantidade de usuários

atendidos; quantidade de equipamentos suportados; complexidade de construção (*T-Shirt sizing*); pontos de sustentação; escopo fechado a preço fixo.

331. Nível de serviço: tempo de atendimento; taxa de incidentes; índice de disponibilidade; índice de atendimento; índice de satisfação; índice de reclamações formais; percentual de atualização de softwares em estações; índice de cumprimento de prazos; índice de conformidade de produtos.

332. É visível que as organizações têm empreendido esforços no sentido de estabelecer métricas para a mensuração dos serviços contratados. No entanto, há um risco considerável de que parte dessas métricas não sejam adequadas para a correspondente medição. O amadurecimento de métricas costuma requerer longos estudos e avaliações de organizações e da academia, logo esse risco não pode ser descartado. Além disso, parte significativa do mercado pode desconhecer a métrica aplicada, o que eleva o risco para o contratado e, consequentemente, pode encarecer a contratação.

333. Quanto a eventuais dificuldades na aplicação das métricas, foram colhidas as seguintes impressões dos gestores:

334. dificuldade de utilização em etapas que não seriam diretamente dependentes do tamanho do software, tais como: produção de material de ajuda online, preparação de ambiente, implantação, consultoria, gerência de configuração, produção de *builds*;

335. complexidade na contratação por tamanho de software em projetos de modernização tecnológica ou manutenção (exemplos: conversão do sistema para uma nova linguagem de programação, conversão de repositório de dados, refatoração de projeto, refatoração de código, manutenções adaptativas e perfectivas, *tunning* de aplicação);

336. dificuldade para aplicação de métricas de tamanho de software em soluções híbridas, tais como as que utilizam portais de colaboração, *data warehouse*, migração de dados e páginas HTML;

337. dificuldades para aplicação de medidas sujeitas a nível de serviço, como por exemplo: tempo máximo para início e tempo máximo para término, pois estes indicadores dependem também da disponibilidade da pessoa para qual o suporte será prestado, e eventuais interrupções no atendimento atrapalham a apuração do nível de serviço;

338. dificuldades na mensuração dos serviços prestados em contratos de suporte e manutenção de licenças de pacotes de software de mercado;

339. falta de preparação dos fornecedores e equipes internas no uso das novas métricas.

340. Várias dessas situações já são consideradas pelo Roteiro de Métricas do Sisp, Versão 2.0 (peça 15), que dispõe em seu capítulo 7 as atividades não sujeitas a contagem de pontos de função. No entanto, é possível que muitos gestores ainda desconheçam as minúcias de tal roteiro e, em especial, desconheçam os instrumentos alternativos que estejam ao seu dispor para mensuração e remuneração dessas atividades.

341. Por outro lado, as organizações reconhecem uma melhora na quantificação dos serviços prestados e na respectiva remuneração. Embora uma das organizações alegue elevação significativa dos custos de gestão dos contratos, duas das organizações afirmaram que, apesar das dificuldades, a remuneração por resultados tem contribuído para a eficiência e eficácia no alcance dos objetivos de TIC. Uma cita maior facilidade no gerenciamento dos serviços e maior transparência de custos, com melhor adaptação às flutuações de demandas e de mudanças tecnológicas. Outra instituição alega que, uma vez que os produtos e serviços contratados estejam alinhados aos objetivos de TI e corporativos, a remuneração por resultados cria uma relação convergente entre a remuneração do fornecedor e os objetivos institucionais.

342. Quanto ao local de execução dos serviços, observou-se disparidade nas respostas. Algumas organizações alegam não necessitar da presença contínua de equipe da contratada em suas dependências, enquanto outras enumeram razões para a prestação local dos serviços

contratados. Com efeito, com base nas respostas apresentadas e nas razões enumeradas para necessidade de equipes presenciais, é possível enumerar uma série de possíveis vantagens de cada modelo alegadas por ambos os grupos:

| **Vantagens – Presença contínua** | |
|---|---|
| **Viabiliza a atuação de fornecedores no caso de serviços críticos e complexos por propiciar menor tempo de reação** | Ganho de escala no desenvolvimento |
| **Maior facilidade para comunicação entre áreas de TI e usuários** | Redução de custos com infraestrutura |
| **Facilita o emprego de métodos ágeis** | Divisão clara de responsabilidades entre contratada e contratante |
| **Maior acesso a equipamentos da instituição** | Menor risco de passivos trabalhistas |
| **Menores riscos de segurança** | Maior escalabilidade de serviços |
| **Menor necessidade de reprodução de ambientes** | Ampliação da base de conhecimento |

343. Quanto aos preços praticados, três organizações indicaram já ter vivenciado problemas com os baixos preços oferecidos pelo mercado em alguns contratos, sendo que a quarta instituição, embora não tenha tido problemas com inexecução contratual relacionada a esse fato, afirmou que os preços são reduzidos demasiadamente durante o pregão o que pode gerar dificuldades para viabilização das entregas dos produtos e serviços contratados. Uma das organizações, inclusive, alega que o baixo preço praticado nas licitações estaria abaixo do valor mínimo necessário, não correspondendo à realidade complexa do ambiente de TI da instituição que demanda profissionais com maior expertise e, consequentemente, de maior salário.

344. Em duas fiscalizações, foram citadas ocorrências de contratos encerrados pelo fornecedor alegando prejuízo ou inexequibilidade. Em outro contrato o fornecedor também não manifestou interesse em prorrogar o contrato alegando prejuízos.

345. Em um esforço de mitigação desses riscos, uma das organizações alegou que tem realizado maior investimento nas fases de planejamento e preparação das contratações, resultando em processos aquisitivos mais aderentes ao que o mercado é capaz de oferecer.

346. Não foi objetivo dessa FOC aprofundar a análise das causas ligadas às dificuldades vivenciadas pelas organizações e pelos licitantes na contratação de serviços de TI, mas verificar se a entrega de resultados de TI poderia estar sendo afetada por eventuais dificuldades vivenciadas na aplicação dos modelos e regras previstos na legislação ou por práticas de mercado. Além disso, pretendia-se colher boas práticas aplicadas para mitigação dos riscos e dificuldades enfrentadas.

347. Assim, depreende-se que, por um lado, há dificuldades na aplicação de modelos objetivos de remuneração para alguns tipos de serviços, mas por outro há benefícios claros decorrentes do uso desses modelos. Há várias causas possíveis para as dificuldades enfrentadas, desde o estágio inicial de maturidade do novo modelo e do próprio mercado na sua aplicação, até a dificuldade na identificação de métricas confiáveis para determinados tipos de serviços, cabendo estudos mais aprofundados em cada caso.

348. Quanto ao local de prestação dos serviços (ambiente da contratada versus remotamente), infere-se que a escolha do modelo depende dos requisitos do tipo de serviço sendo contratado, bem como de características e opções de gestão da instituição. Não há um modelo único e definitivo para todos os tipos de serviço.

349. Finalmente, quanto aos preços de mercado, as organizações alegam estar enfrentando dificuldades, as quais têm impactado a entrega de resultados de TI. Com efeito, é necessário a realização de novos estudos e discussões com vistas à identificação de causas e proposição de soluções.

Propostas de encaminhamento

350. Encaminhar cópia integral desse relatório técnico aos OGS de forma a informá-los a respeito das constatações e conclusões obtidas nesse trabalho com o intuito de apoiar e subsidiar suas ações de normatização, estruturação, capacitação e gestão do setor jurisdicionado.

## 10. BOAS PRÁTICAS

351. A Estratégia Geral de TI do Sisp cita como ponto fraco, em sua análise ambiental (peça 8, p. 35), a "Carência de ações e projetos relacionados à gestão do conhecimento e baixa disponibilidade de informações sobre experiências de TI dos órgãos do Sisp". Apesar disso, é de conhecimento que o Sisp tem se empenhado na promoção desse compartilhamento promovendo, inclusive por meio de encontros como o "Gestão em Destaque" o intercâmbio de experiências entre os jurisdicionados.

352. Nessa fiscalização, em especial na 2ª fase da FOC, foi identificada uma série de boas práticas aplicadas pelas organizações fiscalizadas, experiências e conhecimentos que seriam de grande utilidade se compartilhados com o restante da administração pública.

353. No âmbito internacional, a Comissão de Serviços Públicos do governo da Austrália elaborou um relatório denominado Construindo uma Governança Melhor (*Building Better Governance*, peça 14). A partir de consultas efetuadas junto aos diversos departamentos do governo australiano, o estudo agrupou estudos de caso de vários departamentos: serviços humanos, assuntos e comércio exterior, educação, ciência, turismo, entre outros.

354. De acordo com o relatório, as agências consideraram ser particularmente útil o compartilhamento de histórias sobre suas próprias experiências com a adoção de governança para que as demais organizações pudessem ter contato com ideias e estratégias que pudessem vir a implementar.

355. Os estudos de caso (peça 14, p. 27-87) são um verdadeiro repositório de boas práticas de governança e gestão aplicadas pelos diversos departamentos do governo australiano e se constituem na maior e mais significativa parte do relatório. Cada estudo de caso apresenta: uma contextualização do departamento, o desafio enfrentado, o que foi realizado, forma de monitoramento, benefícios e um resumo com os pontos chave do estudo de caso.

356. Entende-se que, de maneira análoga, as organizações públicas federais poderiam se beneficiar do aproveitamento mútuo de suas próprias experiências na adoção de processos e práticas de governança e gestão de TI. Diversas organizações têm reconhecida maturidade na aplicação de determinadas práticas e a divulgação de sua experiência poderia inspirar e alavancar a adoção de boas práticas por outras organizações. Os frequentes encontros técnicos promovidos pela SLTI/MP no âmbito do Sisp, bem como o lançamento do ambiente colaborativo *wikiSISP (*http://sisp.gov.br/wikisisp), constituem bons exemplos de estratégias de disseminação de boas práticas entre os integrantes do sistema, as quais são conduzidas com a participação de diferentes organizações da administração pública federal.

Propostas de encaminhamento

357. Sem propostas.

## 11. COMENTÁRIOS DO GESTOR

358. Em decorrência do procedimento previsto nos parágrafos 144 a 146 das Normas de Auditoria do Tribunal de Contas da União, aprovadas pelas Portarias - TCU 280/2010 e 168/2011, os relatórios preliminares das fiscalizações integrantes dessa FOC foram submetidas aos gestores para avaliação e comentários, a fim de que eles pudessem se pronunciar sobre as conclusões dos trabalhos e, caso fosse necessário, apresentassem comentários sobre as conclusões e as propostas constantes dos trabalhos.

359. Contudo, no caso do presente relatório, as propostas de deliberação consistem em recomendações e orientações para balizar a atuação dos Órgãos Governantes Superiores de TI (OGS) no que tange à promoção da melhoria da governança e da gestão da tecnologia da

informação, em acordo com o disposto no parágrafo 58 do documento Orientações para Fiscalizações de Orientação Centralizada, aprovado pela Portaria-Adplan 2/2010.

360. Desse modo, e 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 consolidador aos gestores para comentários sobre as conclusões e sobre as propostas de encaminhamento.

## 12. CONCLUSÃO

361. A presente Fiscalização de Orientação Centralizada teve por objetivo a avaliação de práticas de governança e de gestão de TI com foco na entrega de resultados e na gestão dos riscos de TI. A fiscalização foi organizada em duas fases. Na primeira, 24 auditorias foram realizadas para avaliar a implementação dos controles que as organizações informaram em resposta ao Levantamento de Governança de TI, conduzido pelo TCU em 2012. Na segunda fase, foram realizadas seis auditorias, cinco delas com a finalidade de avaliar de maneira mais aprofundada processos adotados e identificar boas práticas aplicadas por organizações com índices mais elevados de governança de TI em temas que ainda que são de relativo desconhecimento da maioria das organizações.

362. Com o objetivo de propiciar maior clareza e fluidez na leitura do relatório, os assuntos avaliados foram agrupados por tema, independente de fase. Os temas definidos foram: Perfil de Governança de TI, Governança, Estratégia e Planejamento, Resultados de TI, Gestão de Riscos, Segurança da Informação e Gestão de Recursos.

363. Quanto ao Perfil de Governança de TI, ou seja, a avaliação das respostas apresentadas pelas organizações, concluiu-se que, apesar das inconsistências apuradas, há razoável fidedignidade nas respostas. O percentual médio de inconsistências por instituição auditada frente ao rol de itens avaliados (58) foi de 8,71%, valor considerado razoável considerando que se tratavam de respostas apuradas em levantamento conduzido apenas pela terceira vez e que tem sofrido mudanças ao longo dessas edições. A análise também permitiu a identificação de falhas e dificuldades na interpretação do questionário, o que ensejou mudanças já incorporadas à 4ª edição do levantamento. Entende-se que com o aprimoramento do questionário e o amadurecimento das organizações as inconsistências serão reduzidas.

364. A respeito da governança corporativa (Seção 4 – Governança), diversos aspectos foram avaliados. Destacando-se, no entanto, as práticas ligadas à atuação da alta administração. Como resultado, constata-se necessidade de maior sensibilização da alta administração das organizações para com o tema. É necessário que a alta administração compreenda e assuma o papel de dirigir a melhoria da governança e da gestão das organizações sob seu encargo.

365. Especificamente a respeito da governança de TI (Seção 4.2 – Governança de TI), chama a atenção o fato de que a maioria das organizações avaliadas (85%) ainda falha no estabelecimento de mecanismos para dirigir e avaliar a gestão e o uso de TI. Mecanismos de elevada importância não têm sido implementados, tais como a definição de objetivos, de metas, de indicadores, de mecanismos de acompanhamento e de gestão de riscos do não cumprimento dos objetivos traçados. Uma das possíveis causas é a falta de um processo estruturado para organização da governança de TI. Em razão dessa avaliação e da evolução da jurisprudência a respeito desse assunto, a Sefti considerou necessária a elaboração de uma Nota Técnica com o objetivo de apoiar as organizações públicas na missão de aprimorar a sua governança de tecnologia da informação.

366. A respeito do tema "Estratégias e Planejamento" (Seção 5 – Estratégia e planejamento), concluiu-se que avanços ocorreram no Poder Judiciário. Infere-se que o mesmo avanço não ocorreu no âmbito do Poder Executivo em razão da não regulamentação da obrigatoriedade da prática, ao contrário do ocorrido no Poder Judiciário, a despeito de reiteradas recomendações do TCU à SLTI e ao Dest a esse respeito.

367. Aprofundar o tema "Resultados de TI" (Seção 6 – RESULTADOS DE TI) era uma das principais expectativas que se tinha deste trabalho. Em razão disso, esse foi um tema fortemente abordado na segunda fase da FOC de forma a coletar experiências das organizações de maior maturidade. Há forte correlação desse assunto com processos e práticas tratados em outros temas e seções, por exemplo na seção de Estratégia e Planejamento. No entanto, algumas práticas e processos foram especificamente agrupados nessa seção em razão de abordarem diferentes aspectos do tema. Os assuntos são: gestão de serviços, avaliação de benefício esperado, gestão de resultados, resultados entregues pela TI, satisfação das áreas de negócio.

368. A principal conclusão foi quanto à gestão de serviços de TI (Seção 6.1 – Gestão de serviços), processo que apresentou, na primeira fase, as piores avaliações. Em praticamente todas as organizações fiscalizadas na primeira fase foi relatado o achado "Falhas na gestão de acordos de nível de serviço" e, mesmo em organizações fiscalizadas na segunda fase, falhas foram observadas, permitindo a inferência de que essa prática ainda está pouco disseminada nas organizações públicas.

369. Com relação à avaliação do benefício esperado com investimento em ações de TI (Seção 6.2 – Avaliação de benefício esperado com investimentos em soluções de TI), foram identificadas algumas boas práticas. Contudo, na maioria das organizações analisar o custo/benefício de um projeto de TI antes de investir recursos, financeiros ou humanos, não é uma prática sistematicamente adotada.

370. A prática de gerenciamento de projetos (Seção 6.3 – Gestão de projetos), embora não tenha sido preliminarmente objeto de uma questão de auditoria, surgiu em várias organizações como um instrumento fundamental adotado pelas organizações para viabilizar a entrega de resultados.

371. O acompanhamento dos resultados (objetivos, metas e indicadores), objeto de avaliação na seção governança de TI na primeira fase, também foi avaliado na segunda fase. Pretendia-se colher experiências junto às organizações mais maduras no acompanhamento de seus planos. Verificou-se que o a acompanhamento é realizado de diferentes maneiras pelas organizações (Seção 6.4 – Acompanhamento dos resultados da TI) e várias boas práticas foram identificadas: realização de reuniões periódicas, painéis de indicadores desenvolvidos especificamente para a alta administração, entre outras. Sob esse tema, verifica-se que há necessidade de que as demais organizações sejam instadas a efetuar de maneira sistemática esse acompanhamento, sob pena de não se assegurar o alcance dos objetivos dispostos nos planos diretores e estratégicos de TI. A esse respeito, o TCU também já recomendou, de maneira reiterada, que os OGS normatizassem a respeito da obrigatoriedade dessa prática. Tais recomendações não foram adotadas até o momento, fato que deve ser objeto de atenção no futuro monitoramento dos respectivos Acórdãos, uma vez que os números verificados na primeira fase indicam que a maioria das organizações não estabelece adequadamente esses mecanismos.

372. Ainda, com o fim de avaliar a entrega de resultados de TI (Seção 6.5 – Resultados entregues pela TI), em cinco organizações uma pesquisa foi aplicada junto aos gestores titulares de áreas de negócio. Seus resultados revelaram que há uma percepção de que os sistemas efetivamente contribuem para o atingimento dos resultados organizacionais. Revelou-se alto grau de satisfação com a estrutura computacional básica (estações de trabalho, correio eletrônico, internet e impressoras), mas um elevado índice de descontentamento com o tempo para atendimento de demandas de sistemas (manutenções, evoluções e correções). Esses resultados sugerem que as áreas de negócio reconhecem a contribuição da TI para com sua missão, no entanto requerem maior agilidade no atendimento de suas demandas.

373. As informações coletadas nos procedimentos de auditoria conduzidos sob o tema Gestão de Riscos (Seção 7 – Gestão de riscos) indicam que essa prática ainda precisa amadurecer muito na administração pública. Entre as organizações da primeira fase, a maioria não estabeleceu um processo de gestão para os riscos de segurança da informação, enquanto que, mesmo entre as organizações pesquisadas na segunda fase, a situação está longe da ideal.

Foram identificadas falhas na gestão dos riscos de TI (falhas na operacionalização do processo e no alinhamento da gestão de riscos de TI) em três organizações das cinco pesquisadas.

374. A segurança da informação (Seção 8 – Segurança da informação) segue sendo objeto de preocupação. Há baixa conformidade das organizações para com os normativos e boas práticas aplicáveis. Na maioria das organizações fiscalizadas na primeira fase, falhas foram observadas: falhas na gestão de continuidade de negócio (80%), falhas no controle de acesso (70%), falhas na gestão de incidentes (75%) e falhas na gestão de riscos de segurança da informação (85%). Uma das possíveis causas está ligada a falhas típicas de governança, como a falta de designação de um responsável pela segurança da informação, fato observado em 40% das organizações.

375. Entende-se que há espaço para que sejam definidos, em âmbito estratégico, ações com vistas a impulsionar a melhoria nos processos e práticas de segurança da informação. Ainda não há, por exemplo, um planejamento estratégico do Estado brasileiro que reúna e coordene ações dos diversos atores responsáveis por assuntos ligados a essa área.

376. Na gestão de recursos (Seção 9 – Gestão de recursos) também foram observadas falhas: ausência de diagnóstico da força de trabalho necessária (40%), inexistência ou falhas no plano de capacitação (50%), falhas no planejamento das contratações de TI (45%). Sob o aspecto das contratações, foram levantadas, mediante aplicação de um questionário, as principais dificuldades enfrentadas pelas organizações maduras para consecução de suas contratações de TI. O objetivo era identificar as dificuldades, bem como as práticas adotadas para minimização de riscos e obtenção de melhores resultados com a execução indireta.

377. As propostas de encaminhamento deste relatório consolidador reúnem uma série de determinações e recomendações aos Órgãos Governantes Superiores com o fim de fomentar o aprimoramento da sua atuação e, por consequência, das demais organizações sob sua jurisdição.

378. Foram dirigidas propostas de aprimoramento dos planos estratégicos setoriais de tecnologia da informação conduzidos pelos OGS que já adotam essa prática. Para os que não adotam, foi recomendada sua adoção. A partir dessa experiência, sugeriu-se também a adoção de planejamento estratégico setorial específico para a segurança da informação dada a relevância do tema e o fato de envolver áreas e assuntos que vão além da tecnologia da informação. Também recomendou-se maior interlocução e colaboração entre os OGS de forma a fomentar maior aproveitamento dos produtos e experiências desenvolvidos.

379. Foram registradas, com o fim de apoiar futuros monitoramentos, situações em que a regulamentação da obrigatoriedade de adoção de algumas práticas já foi objeto de manifestação anterior do TCU e que, segundo a avaliação empreendida, seguem sendo objeto de baixa implementação por parte das organizações públicas.

380. Por fim, em paralelo à consolidação desse trabalho, foi elaborada uma nota técnica que consolida, sob a forma de entendimentos, as experiências da unidade em levantamentos, auditorias e ações pedagógicas na área de governança e gestão de TI. Objetiva-se, com a proposição dessa NT, apoiar as organizações na compreensão, avaliação e direcionamento de seus esforços na estruturação de seus respectivos sistemas de governança de TI com o objetivo de favorecer o atendimento das expectativas de suas áreas de negócio e, por consequência, da sociedade.

## 13. PROPOSTAS DE ENCAMINHAMENTO

381. **Recomendar**, com fulcro no art. 43, inciso I, da Lei 8.443/1992 c/c o art. 250, inciso III, do Regimento Interno do TCU, 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/MP, 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:

381.1. com base no Princípio da Eficiência insculpido no art. 37 da Constituição Federal c/c Prática E3.1 do Referencial Básico de Governança Pública do TCU, estabeleçam mecanismos permanentes de interlocução e compartilhamento de estratégias, ações e produtos no sentido de se maximizar o aproveitamento de soluções elaboradas no âmbito de um Órgão Governante Superior (OGS), tais como guias, manuais, entre outros, pelos demais OGS, no sentido de se garantir maior eficiência e celeridade na orientação e estruturação das organizações sob suas respectivas jurisdições;

381.2. com base no Princípio da Eficiência insculpido no art. 37 da Constituição Federal c/c a Prática L1.2 do Referencial Básico de Governança Pública do TCU, estabeleçam estratégias e ações de sensibilização da alta administração das organizações sob sua jurisdição quanto ao tema governança de TI, com o objetivo de orientar tais responsáveis acerca de seu papel no sentido de avaliar, dirigir e monitorar a gestão e o uso da tecnologia da informação;

381.3. com base no Princípio da Eficiência insculpido no art. 37 da Constituição Federal, orientem as unidades sob sua jurisdição a avaliar previamente a viabilidade de projetos de TI, incluindo, entre os objetos de análise, a verificação do custo/benefício do projeto, a exemplo do processo EDM02 – Assegurar a Entrega de Benefícios do Cobit 5;

381.4. com base no art. 6º, inciso I, do Decreto-Lei 200/1967, orientem as organizações sob sua jurisdição a respeito da importância da adoção das seguintes práticas relativas ao planejamento de TI e seu acompanhamento:

381.4.1. atribuição de responsáveis pelo alcance dos objetivos e metas de TI;

381.4.2. definição de responsáveis pela aferição dos indicadores de TI;

381.4.3. disponibilização de indicadores estratégicos para acompanhamento por parte da alta administração por meio de relatórios ou sistemas específicos;

381.4.4. estabelecimento de instrumentos de acompanhamento, a exemplo de: sistemas, reuniões periódicas, relatórios;

381.4.5. definição de ações específicas para quando as metas de TI não forem alcançadas, a exemplo de: discussão em reuniões, escalamento, elaboração de planos de tratamento;

381.4.6. divulgação interna e externa do alcance das metas de TI, ou os motivos de elas não terem sido alcançadas.

381.5. com base no inciso I no Art. 6º do Decreto-Lei 200/1976 c/c processo EDM03 – Assegurar a Otimização de Riscos do Cobit 5, normatizem a obrigatoriedade de que todas as organizações sob sua jurisdição gerenciem os riscos de TI a que estão sujeitos por meio de um processo formal;

381.6. com base no inciso I do Art. 6º do Decreto-Lei 200/1976 c/c processo EDM03 – Assegurar a Otimização de Riscos do Cobit 5, promovam ações de sensibilização e capacitação dos gestores das organizações sob sua jurisdição quanto à gestão de riscos de TI, com o objetivo de orientá-los na identificação, análise, tratamento e comunicação dos riscos a que a instituição está sujeita;

381.7. com base no Princípio da Eficiência insculpido no caput do art. 37 da Constituição Federal, orientem as unidades sob sua jurisdição no sentido de aprimorar os respectivos processos de gestão de orçamento e de custos de TI, a exemplo do disposto no processo APO06 – Gerenciar orçamento e custos do Cobit 5, com vistas a permitir a visualização e o acompanhamento da evolução dos custos diretos e indiretos de TI, incluindo, por exemplo, os custos ligados a recursos humanos (remuneração, treinamento etc.) e infraestrutura;

381.8. com base no Princípio da Eficiência insculpido no *caput* do art. 37 da Constituição Federal, elaborem um modelo de custos de TI para servir de referência para as

organizações jurisdicionadas, baseado na definição dos serviços prestados, de forma a tornar a alocação de custos aos serviços de TI identificável, mensurável e previsível, a exemplo do previsto na prática APO06.04 - Modelar e alocar custos do Cobit 5.

382. **Recomendar**, com fulcro no art. 43, inciso I, da Lei 8.443/1992 c/c o art. 250, inciso III, do Regimento Interno do TCU, ao Conselho Nacional de Justiça – CNJ e à Secretaria de Logística e Tecnologia da Informação do Ministério do Planejamento, Orçamento e Gestão – SLTI/MP que, com base nos incisos II e V da Lei 12.527/2011 c/c inciso I do art. 6º do Decreto-Lei 200/1967, publiquem periodicamente os resultados das avaliações acerca do alcance dos objetivos e metas dispostos nos respectivos planos estratégicos de TI para o setor jurisdicionado, propiciando ampla transparência aos resultados atingidos.

383. **Recomendar**, com fulcro no art. 43, inciso I, da Lei 8.443/1992 c/c o art. 250, inciso III, do Regimento Interno do TCU, ao Gabinete de Segurança Institucional da Presidência da República – GSI que:

383.1. com base no inciso IV do Art. 6º da Lei 10.683/2003 c/c incisos I e V do Art. 3º da Instrução Normativa GSI/PR 1/2008, e em articulação com os demais órgãos competentes, elabore e acompanhe periodicamente, a exemplo do realizado na Estratégia Geral de Tecnologia da Informação no Sisp e da Estratégia de TIC no Poder Judiciário, planejamento que contemple a estratégia geral de segurança da informação para o setor sob sua jurisdição, envolvendo não somente a tecnologia da informação, mas também os demais segmentos relacionados à proteção das informações institucionais;

383.2. com base no inciso IV, do Art. 6º da Lei 10.683/2003 c/c incisos I e V do Art. 3º da Instrução Normativa GSI/PR 1/2008, alerte as organizações sob sua jurisdição que a elaboração periódica de planejamento das ações de segurança da informação é obrigação expressa prevista no item 3.1 da Norma Complementar 2/IN01/DSIC/GSIPR, além de ser boa prática prevista na NBR ISO/IEC 27.001/2013, item 6, bem como no Cobit 5, Prática de Gestão APO 13.2.

384. **Recomendar**, com fulcro no art. 43, inciso I, da Lei 8.443/1992 c/c o art. 250, inciso III, do Regimento Interno do TCU, ao Conselho Nacional de Justiça (CNJ) que:

384.1. com base no §4 do Art. 103-B da Constituição Federal c/c preâmbulo da Resolução CNJ 70/2009, elabore e acompanhe periodicamente, a exemplo do realizado na Estratégia Geral de Tecnologia da Informação no Sisp e na Estratégia de TIC no Poder Judiciário, planejamento que contemple a estratégia geral de segurança da informação para o setor sob sua jurisdição, envolvendo não somente a tecnologia da informação, mas todos os segmentos relacionados à proteção das informações institucionais;

384.2. com base no art. 1º, inciso IV, alínea "g", Objetivo 9, da Resolução 99/2009 do CNJ c/c documento de Diretrizes para a Gestão de Segurança da Informação no âmbito do Poder Judiciário, alerte as organizações sob sua jurisdição que o estabelecimento de um modelo de gestão que contemple, entre outros processos, a elaboração periódica de planejamento estratégico de segurança da informação é diretriz expressa pelo Conselho Nacional de Justiça para a gestão da segurança da informação, além de ser boa prática prevista na NBR ISO/IEC 27.001/2013, item 6, bem como no Cobit 5, Prática de Gestão APO 13.2.

385. **Recomendar**, com fulcro no art. 43, inciso I, da Lei 8.443/1992 c/c o art. 250, inciso III, do Regimento Interno do TCU, ao Conselho Nacional do Ministério Público (CNMP) que:

385.1. com base no §2 do Art. 130-A da Constituição Federal, elabore e acompanhe periodicamente, a exemplo do realizado na Estratégia Geral de Tecnologia da Informação no Sisp e na Estratégia de TIC no Poder Judiciário, planejamento que contemple a estratégia geral de segurança da informação para o setor sob sua jurisdição, envolvendo não somente a tecnologia da informação, mas todos os segmentos relacionados à proteção das informações institucionais;

385.2. com base no §2 do Art. 130-A da Constituição Federal, alerte as organizações sob sua jurisdição que o estabelecimento de um modelo de gestão que contemple, entre outros processos, a elaboração periódica de planejamento estratégico de segurança da informação é boa prática prevista na NBR ISO/IEC 27.001/2013, item 6, bem como no Cobit 5, Prática de Gestão APO 13.2.

386. **Determinar** à Secretaria de Fiscalização de Tecnologia da Informação do TCU (Sefti/TCU) que:

386.1. encaminhe cópia integral deste relatório técnico aos OGS de forma a informá-los a respeito das constatações e conclusões obtidas nesse trabalho com o intuito de apoiar e subsidiar suas ações de normatização, estruturação, capacitação e gestão do setor jurisdicionado;

386.2. 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):

386.2.1. organizações a que foram dirigidas as recomendações da deliberação;

386.2.2. organizações que foram individualmente fiscalizadas no âmbito da FOC;

386.2.3. Comissão de Ciência e Tecnologia, Comunicação e Informática (CCTCI) da Câmara dos Deputados;

386.2.4. Subcomissão Permanente de Ciência e Tecnologia e Informática da Comissão de Ciência e Tecnologia, Comunicação e Informática (CCTCI) da Câmara dos Deputados;

386.2.5. Comissão de Ciência, Tecnologia, Inovação, Comunicação e Informática (CCT) do Senado Federal;

386.2.6. Subcomissão Permanente de Serviços de Informática (CCTSINF) da Comissão de Ciência, Tecnologia, Inovação, Comunicação e Informática (CCT) do Senado Federal;

386.2.7. Tribunais de Contas dos Estados e dos Municípios, para que adotem as medidas que entenderem pertinentes.

386.3. arquive os presentes autos.

387. **Autorizar:**

387.1. a Sefti a promover a divulgação das recomendações dirigidas aos Órgãos Governantes Superiores por meio do Acórdão que vier a ser proferido, como forma de fomentar a melhoria dos processos de governança e gestão das organizações jurisdicionadas;

387.2. a Sefti a promover a divulgação do conteúdo da Nota Técnica Sefti 7/2014 como forma de apoiar as organizações da Administração Pública Federal no processo de amadurecimento de suas práticas de governança de TI, bem como a jurisprudência deste Tribunal quanto ao assunto;

387.3. desde já, a realização de monitoramento do cumprimento das determinações e recomendações contidas neste Acórdão."

É o relatório.

## Voto

Trata-se de auditorias realizadas em diversos órgãos e entidades da Administração Pública federal com o objetivo de avaliar a implementação dos controles de TI informados em resposta ao levantamento do perfil de governança de TI de 2012, bem como verificar a implementação de controles e processos de governança e gestão de TI para assegurar a entrega de resultados de TI alinhados aos objetivos de negócio das instituições e a gestão de riscos.

2. O trabalho foi realizado na forma de fiscalização de orientação centralizada (FOC) e foi dividido em duas fases.

3. A primeira compreendeu 24 auditorias realizadas para avaliar a implementação dos controles informados pelo órgão/entidade em resposta ao levantamento do perfil de governança de TI realizado em 2012, bem como verificar e avaliar a adoção pelo órgão/entidade auditada de planos e estratégias para a implementação e melhoria da governança e da gestão de TI.

4. Nessa fase, foram examinados os seguintes temas:

a) governança corporativa – gestão da ética, políticas corporativas e comitê de direção estratégica;
b) governança de TI – processo de aprimoramento da governança de TI, comitê de TI, desempenho da gestão e uso de TI e atuação da auditoria interna na avaliação de temas de TI;
c) estratégias e planos – planejamento estratégico institucional, planejamento estratégico de TI e planejamento diretor de TI (PDTI);
d) gestão de pessoal de TI – quadro gerencial de TI, força de trabalho em TI e plano de capacitação em gestão de TI;
e) processos de TI e segurança da informação (SI) – gestão de nível de serviço de TI, gestão de continuidade dos serviços de TI, gestão de ativos, política de controle de acesso, conscientização e treinamento em SI, política de SI, comitê de SI, gestão de incidentes em SI, gestão de riscos em SI, planejamento e gestão de contratos de TI.

5. A segunda fase envolveu 6 auditorias, cinco delas realizadas em organizações com índices elevados de governança de TI, conforme levantamentos conduzidos por esta Corte, tendo sido objeto de avaliação os seguintes aspectos: alinhamento entre o setor de TI e o negócio da instituição, gestão de orçamento de TI, gestão de custos de TI, gestão de resultados de TI, retorno sobre investimento em TI, gestão de riscos de TI e contratações de soluções TI orientadas à entrega de resultados.

6. A FOC foi realizada sob a coordenação da Secretaria de Fiscalização de Tecnologia da Informação, com a participação das secretarias de controle externo nos estados do Amazonas, Ceará, Paraná, Pernambuco, Rio Grande do Sul e São Paulo.

7. A escolha dos aspectos examinados, bem como sua avaliação, baseou-se em normativos institucionais que tratam de fiscalização no âmbito deste Tribunal e decisões anteriores sobre a matéria, em especial o acórdão 1233/2012-TCU-Plenário.

8. Como critérios de auditoria, foram adotados os seguintes modelos e normas de boas práticas: Cobit 5, da Information Systems Audit and Control Association (Isaca); NBR ISO/IEC 27002:2005 (NBR: 27002), 20000-2:2008 (NBR 20000-2) e 38500:2009 (NBR 38500); o Código de Melhores Práticas de Governança Corporativa do Instituto Brasileiro de Governança Corporativa (IBGC); e o Guia de Elaboração de Plano Diretor de Tecnologia da Informação (PDTI) do Sistema de Administração dos Recursos de Tecnologia da Informação (Sisp).

**II**

9. A equipe de auditoria agrupou os resultados da seguinte forma:

| TEMA | SUBTEMA |
|---|---|
| **PERFIL GOV TI** | **PREENCHIMENTO DO QUESTIONÁRIO DE GOVERNANÇA DE TI** |
| **GOVERNANÇA** | **GOVERNANÇA CORPORATIVA** |

| | |
|---|---|
| | **GOVERNANÇA DE TI** |
| | **APRIMORAMENTO DE GOVERNANÇA DE TI** |
| **ESTRATÉGIA E PLANEJAMENTO** | **----------** |
| **RESULTADOS DE TI** | **GESTÃO DE SERVIÇOS** |
| | **AVALIAÇÃO DE BENEFÍCIO ESPERADO COM INVESTIMENTO EM SOLUÇÕES DE TI** |
| | **GESTÃO DE PROJETOS** |
| | **ACOMPANHAMENTO DOS RESULTADOS DE TI** |
| | **RESULTADOS ENTREGUES PELA TI** |
| **GESTÃO DE RISCOS** | **----------** |
| **SEGURANÇA DA INFORMAÇÃO** | **----------** |
| **GESTÃO DE RECURSOS** | **GESTÃO DOS RECURSOS HUMANOS EM TI** |
| | **GESTÃO DE CUSTOS DE TI** |
| | **CONTRATAÇÕES DE TI** |

10. No que diz respeito ao perfil de governança de TI (GovTI), um dos objetivos da fiscalização era a saber se havia inconsistências entre as evidências de implementação dos controles de TI e as respostas dadas pelas organizações no levantamento do perfil de GovTI.

11. Segundo a equipe, entende-se como inconsistência a divergência entre a informação assinalada pelo órgão ao preencher o questionário e a opinião da equipe de fiscalização quanto à pertinência daquela resposta em face da situação observada durante a auditoria.

12. Constatou-se que as inconsistências são mais expressivas na primeira dimensão do questionário (1. Liderança da Alta da Administração), o que revela dificuldade das organizações em perceber de maneira clara o papel desempenhado pela alta administração.

13. Dentre as causas apontadas estão o baixo conhecimento das organizações quanto às práticas, processos e papéis da alta administração no que tange à governança, bem como o fato de que em muitas organizações as respostas ao questionário são deixadas a cargo dos profissionais das áreas de tecnologia da informação, evidenciando a falta de compreensão por parte da alta administração de que a governança de TI é responsabilidade sua e não é assunto exclusivo da área técnica.

14. No entanto, a avaliação geral, apesar das inconsistências apuradas, foi de que o preenchimento das respostas tem sido adequado, com razoável fidedignidade das respostas, pois o

percentual médio de inconsistências por instituição auditada em comparação com o rol de itens avaliados (58) foi de 8,71%.

15. Acerca da governança corporativa, em vinte organizações foram avaliados os seguintes aspectos: políticas corporativas, direção estratégica e ética institucional.

16. A principal ocorrência identificada diz respeito a falhas de atuação da alta administração no estabelecimento e no monitoramento de políticas corporativas relacionadas a temas que guardam conexão com TI (60%).

17. Outras ocorrências, relacionadas à ética institucional, referem-se à inexistência de código de ética em 15% das organizações e falhas na sua aplicação em 30% delas: não realização de campanhas de divulgação e conscientização (quatro organizações), dificuldade de acesso ao documento e ausência de comitê de ética (uma organização).

**III**

18. A governança de TI, dentre outras possibilidades, é compreendida como o sistema que direciona e monitora a gestão e o uso da tecnologia da informação em uma organização ara assegurar que as necessidades de negócio atuais e futuras sejam atendidas.

19. A Intosai apontou os seguintes riscos da falta de tratamento adequado da governança de TI: (i) sistemas de informação não efetivos, ineficientes ou não amigáveis; (ii) bens e serviços de TI inadequados às necessidades institucionais; (iii) restrições ao crescimento do negócio institucional; (iv) gerenciamento ineficiente de recursos; (v) tomada de decisão inadequada; (vi) fracasso de projetos; (vii) dependência de fornecedores; (viii) falta de transparência e prestação de contas; (ix) exposição a riscos de segurança da informação.

20. No âmbito da governança de TI foram avaliados quatro temas: (i) estabelecimento de comitês; (ii) mecanismos para dirigir e avaliar a gestão e o uso de TI; (iii) atuação da auditoria interna e (iv) inexistência de ações ou processo para melhoria da governança de TI na instituição.

21. As principais constatações relacionaram-se, notadamente, à falta de definição dos papéis e responsabilidades nas decisões mais relevantes quanto à gestão e ao uso corporativo de TI, à ausência de mecanismos de gestão de riscos relacionados aos objetivos de gestão e usos corporativos, e à inexistência de planos de auditorias internas para avaliar os riscos considerados críticos para o negócio.

22. Além disso, grande parte das instituições não estabelece diretrizes para a avaliação de desempenho dos serviços de TI junto às unidades usuárias em termos de resultado de negócio institucional.

23. Em 85% das instituições, foram observadas falhas nos mecanismos para dirigir e avaliar a gestão e o uso corporativo de TI, atribuídas, usualmente, ao distanciamento da alta administração em relação a assuntos de TI.

24. Todos as instituições auditadas dispunham de comitê de TI, no entanto, em 30% delas foram constatadas falhas na implementação dos comitês, tais como, falta de atuação, ausência de representantes de áreas relevantes em sua composição e não monitoramento das ações por parte da alta administração.

25. Com relação à auditoria interna, foi registrado que 15% das organizações não dispõem de auditoria interna e que, na maior parte delas, a auditoria interna não fiscaliza a área de TI.

26. A avaliação realizada indicou que a maioria das organizações não está atuando para estruturar processos institucionais de aprimoramento constante da governança. Em 15% das organizações detectou-se que não havia nem mesmo ações isoladas de melhoria de governança de TI.

Em 55%, foram constatadas diversas falhas, tais como: inexistência de processo formal para organização dos esforços e ausência de estrutura organizacional designada para orientar as atividades.

**IV**

27. A respeito do tema 'Estratégia e Planejamento', a fiscalização investigou, na primeira fase, se as estratégias e planos corporativos e de TI foram adequadamente definidos e implementados no âmbito da instituição, tendo sido avaliados os seguintes temas: planejamento estratégico institucional, planejamento estratégico de TI e plano diretor de TI.

28. Na segunda fase, por sua vez, buscou-se avaliar se a instituição adota processos e práticas que garantem alinhamento entre a TI e seu negócio.

29. No que tange ao Poder Judiciário, verificou-se que todos as instituições dispunham de processo de planejamento estratégico e apenas 20% não dispunha de planejamento estratégico de TI e de um PDTI formalizado e publicado pela alta administração. Os avanços do Poder Judiciário são atribuídos às regulamentações baixadas pelo CNJ.

30. No Poder Executivo, as fiscalizações apontaram que 33% das instituições auditadas no âmbito do Poder Executivo não dispunham de planejamento estratégico institucional, 46% não dispunham de planejamento estratégico de TI e que em 46% delas não havia um PDTI formalizado e publicado pela alta administração, a despeito de reiteradas recomendações deste Tribunal à SLTI e ao DEST.

31. Dentre os riscos relacionados às deficiências de planejamento destacam-se a dificuldade para se realizar o alinhamento entre as ações de TI e o negócio da instituição, pela inexistência de objetivos e metas positivados.

32. Com a finalidade de verificar se a TI atinge os resultados dela esperados e, por conseguinte, apoia e suporta a organização no alcance de seus objetivos, foi avaliada, na primeira fase, a gestão de serviços, procurando-se identificar se os processos de TI foram definidos e implementados adequadamente no âmbito da instituição.

33. Na segunda fase, além desse tema, foram avaliados os benefícios esperados com investimentos em ações de TI, gestão de resultados, resultados entregues pela TI e satisfação das áreas de negócio. Nessa ocasião, procurou-se verificar se a instituição dispunha de mecanismos adequados para analisar benefícios esperados dos investimentos, gerenciar custos e acompanhar os resultados esperados do setor de TI.

34. Na primeira fase do trabalho, foram apontadas falhas relacionadas à gestão de acordos de nível de serviços, processos de gestão de segurança da informação, gestão de incidentes de segurança da informação, planejamento e gestão das contratações:

- gestão de acordos de nível de serviços: inexistência de catálogo formal de serviços de TI; inexistência de acordos de nível de serviço estabelecidos entre o setor de TI e as áreas internas; e inexistência de processo de gestão de nível de serviço de TI;
- processos de gestão de segurança da informação: inexistência de: processo de gestão da continuidade dos serviços de TI formalmente aprovado e publicado; processo de inventário dos ativos de informação; política de controle de acesso à informação (PCA); programas de conscientização e treinamento em segurança da informação; e processo de gestão de riscos de segurança da informação;
- gestão de incidentes de segurança da informação: ausência de um documento formalmente aprovado e publicado que contemple o processo de gestão dos incidentes de segurança da informação;

- planejamento e gestão das contratações de TI: inexistência de planejamento e gestão: inexistência de processo formal de contratação de bens e serviços de TI.

35. Chama a atenção que os números apresentados pelo 3º levantamento de governança em TI indicam que 88% das organizações pesquisadas não monitoram os níveis de serviço, situação corroborada por fiscalizações em campo.

36. A maioria (75%) sequer dispõe de um catálogo atualizado e formalizado com os serviços de TI disponíveis para uso dos clientes, fase inicial no estabelecimento de um processo de gestão de serviços.

37. Na segunda fase, quando foram fiscalizadas organizações de maior nível de governança, a inexistência de catálogo formal de serviço de TI foi constatada em apenas 40% das instituições.

38. Esses indicadores revelam que, mesmo em organizações de maior capacidade e maturidade em governança e gestão, ainda há bastante espaço para o aprimoramento da gestão de serviços de TI.

39. Com relação à avaliação do benefício esperado com investimento em ações de TI, constatou-se que, na maioria das organizações, a análise do custo/benefício de um projeto de TI antes do aporte de recursos, financeiros ou humanos, não é uma prática adotada sistematicamente.

## V

40. Para a avaliação da gestão de riscos, buscou-se avaliar, na primeira fase, se os processos de TI foram definidos e implementados adequadamente no âmbito da instituição.

41. Constatou-se que, de um modo geral, as organizações não dispõem de processos específicos para gestão dos riscos de segurança da informação, o que implica dizer que as ações para a proteção das informações institucionais não estão respaldadas por análises consistentes e podem não estar merecendo a necessária priorização conforme as necessidades de proteção da instituição.

42. Na segunda fase, por sua vez, procurou-se verificar se a entrega de resultados é executada mediante adequada gestão de riscos de TI.

43. Para tanto, a atuação das organizações foi avaliada sob vários aspectos: gestão de riscos de segurança da informação, governança sobre os riscos, estrutura para gestão de riscos, implantação de um processo de gestão de riscos de TI, conteúdo e operacionalização do processo, alinhamento com a gestão de riscos corporativa e com a gestão de riscos de segurança da informação.

44. Nesse caso, as constatações são no sentido do aumento da maturidade institucional quanto à gestão de riscos de TI, pois, além de não terem sido identificadas organizações sem política de gestão de riscos corporativa, os riscos de TI são percebidos como uma espécie dos riscos existentes e aos quais estão ligados os processos de negócio em geral.

45. Embora existam políticas corporativas para tratamento do assunto, essa fase revelou que muitas vezes as ações práticas são desempenhadas exclusivamente pela TI, à parte da gestão de riscos corporativa, com fundamento principalmente nos elementos tecnológicos de risco.

46. Também foi avaliado se os processos relacionados à segurança de TI foram definidos e implementados adequadamente no âmbito da instituição.

47. De um modo geral, concluiu-se que a segurança da informação ainda não é objeto de planejamento adequado, pois número significativo de organizações não dispunha de política de segurança da informação, além de terem constatados problemas nas estruturas requeridas para organizar e conduzir a questões segurança da informação.

48. Observou-se que, muito embora tenha se avançado de maneira significativa na edição de normativos e regulação de processos relacionados à segurança de TI, diversas organizações não têm empreendido ações nem disponibilizado recursos para garantir a conformidade das ações gerenciais e operacionais com as boas práticas requeridas nos normativos aplicáveis.

**VI**

49. Os recursos humanos são apontados no Cobit 5 como um dos principais elementos viabilizadores da governança e da gestão de TI devido a sua imprescindibilidade para a estruturação e o fornecimento dos serviços de TI, como não poderia deixar de ser.

50. Em vista disso, a gestão de recursos humanos de TI foi objeto de análise nesta fiscalização com o fito de avaliar a adequação dos mecanismos de gestão de pessoal no âmbito da instituição e se haveria ferramentas adequadas para se auferir os benefícios esperados dos investimentos de TI, gerenciar custos e acompanhar os resultados esperados do setor de TI.

51. Como resultado, observou-se que a área de recursos humanos de TI apresenta problemas já identificados em fiscalizações anteriores, dentre os quais, a ausência de avaliações quantitativa e qualitativa da força de trabalho, insuficiência de recursos humanos de TI para atender o negócio da instituição, inexistência ou falhas no planejamento e na gestão das contratações destinadas aos serviços de TI.

52. Com relação à gestão de custos de TI, verificou-se, de maneira geral, que as organizações pesquisadas dispõem de orçamentos específicos de TI, mas, no que tange aos custos indiretos, tais como recursos humanos ou de infraestrutura, ainda não são devidamente apurados e incorporados à avaliação do custo global das ações de TI para a organização.

53. Além disso, a maioria das organizações não tem como prática segregar os custos de TI nos serviços que prestam à instituição, o que prejudica o rateio desses custos com as áreas demandadas, bem como a mensuração da evolução dos custos de TI, incluindo as despesas com pessoal.

54. Muito embora os custos com recursos humanos possam continuar a ser objeto de acompanhamento por outras unidades da instituição, são necessários relatórios e mecanismos de contabilização dos gastos com TI que permitam à instituição ter visão consolidada das despesas com TI, incluindo as despesas com recursos humanos próprios.

**VII**

55. Consolidados os resultados das diversas fiscalizações realizadas com o objetivo de verificar a implementação de controles e processos de governança e gestão de TI para assegurar a entrega de resultados de TI alinhados aos objetivos de negócio das instituições e a gestão de riscos, a Sefti apresenta um painel que permite vislumbrar as deficiências em termos de ações de melhoria de governança e avaliação da gestão de TI na Administração Pública Federal.

56. Nesse sentido, é importante realçar que a inobservância dos padrões de boas práticas importa incorrer em sérios riscos, conforme descrito nos diversos relatórios de fiscalização:

- baixa efetividade de políticas importantes para o incremento da governança corporativa;
- alta exposição a riscos de disseminação de vírus, invasões, furto ou destruição de dados;
- limitações para o alcance da eficácia, eficiência e efetividade da TI para agregar valor ao negócio, com o fornecimento de serviços inadequados e dificuldades na priorização de esforços;
- desalinhamento das ações de TI com os objetivos das áreas de negócio, com aumento do riscos relacionados e da alocação inadequada de recursos financeiros e humanos;

- insuficiência de desempenho de TI, aumento dos riscos associados a TI e dúvidas quanto ao fato de a TI agregar valor ao negócio com riscos e custos aceitáveis;
- aumento da possibilidade de uma determinada ameaça explorar vulnerabilidades de um ativo ou de um conjunto de ativos da entidade;
- descontrole dos riscos a que os ativos de informações críticas para o negócio estão submetidos;
- paralisação de atividades prioritárias do órgão;
- exposição não autorizada de informação sigilosa;
- desconhecimento pelos servidores dos procedimentos a serem adotados quando da ocorrência de incidentes de segurança da informação;
- contratação de soluções não ótimas para os negócios da instituição e aumento de custos nas contratações efetuadas.

Diante do exposto, voto pela aprovação do acórdão que ora submeto à apreciação deste Colegiado.

TCU, Sala das Sessões Ministro Luciano Brandão Alves de Souza, em 5 de novembro de 2014.

**WEDER DE OLIVEIRA**
Relator

ACÓRDÃO Nº 3051/2014 – TCU – Plenário

1. Processo nº TC 023.050/2013-6.
2. Grupo I – Classe V - Assunto: Relatório de Auditoria.
3. Interessados/Responsáveis: não há.
4. Órgão/Entidade Empresa Brasileira de Infraestrutura Aeroportuária (Infraero), Eletrobras Eletronuclear, Ministério da Justiça (MJ), Ministério da Educação (MEC), Agência Nacional de Águas (ANA), Instituto Nacional de Colonização e Reforma Agrária (Incra), Hospital de Clínicas de Porto Alegre (HCPA), Tribunal Regional Eleitoral do Rio Grande do Sul (TRE-RS), Companhia de Geração Térmica de Energia Elétrica (CGTEE), Universidade Federal de Pernambuco (UFPE), Tribunal Regional Eleitoral de Pernambuco (TRE-PE), Tribunal Regional Federal da 5ª Região (TRF/5ª), Banco do Nordeste do Brasil S.A. (BNB), Tribunal Regional do Trabalho da 7ª Região (TRT/7ª), Universidade Federal do Ceará (UFC), Companhia Docas do Estado de São Paulo S.A. (Codesp), Instituto Nacional de Pesquisas Espaciais (INPE), Tribunal Regional Eleitoral de São Paulo (TRE-SP), Universidade Federal do Paraná (UFPR), Universidade Tecnológica Federal do Paraná (UTFPR), Tribunal Regional do Trabalho da 9ª Região (TRT/9), Fundação Universidade do Amazonas (UFAM), Superintendência da Zona Franca de Manaus (Suframa), Amazonas Distribuidora de Energia S.A., Banco Central do Brasil (BCB), Companhia Hidroelétrica do São Francisco (Chesf), Petróleo

Brasileiro S.A (Petrobras).
5. Relator: Ministro-Substituto Weder de Oliveira.
6. Representante do Ministério Público: não atuou.
7. Unidade Técnica: Secretaria de Fiscalização de Tecnologia da Informação (SEFTI).
8. Advogado constituído nos autos: Polyanna Ferreira Silva Vilanova (OAB/DF 19.273) e outros, peça 23.

9. Acórdão:

VISTOS, relatados e discutidos estes autos que tratam da consolidação de auditorias realizadas em diversos órgãos e entidades da Administração Pública Federal com vistas a avaliar a implementação dos controles de TI informados em resposta ao levantamento do perfil de governança de TI de 2012, bem como verificar a adoção de planos e estratégias para implementação e melhoria da governança de TI.

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

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/MP, 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:

9.1.1. estabeleçam mecanismos permanentes de interlocução e compartilhamento de estratégias, ações e produtos no sentido de maximizar o aproveitamento de soluções elaboradas por um órgão governante superior (OGS), tais como guias, manuais, entre outros, pelos demais OGS, com o objetivo de alcançar maior eficiência e celeridade na melhoria dos processos e estruturas das organizações sob sua respectiva jurisdição;

9.1.2. estabeleçam estratégias e ações de sensibilização da alta administração das organizações sob sua jurisdição quanto ao tema governança de TI, com o objetivo de orientar tais responsáveis acerca de seu papel na avaliação, direção e monitoramento da gestão e o uso da tecnologia da informação;

9.1.3. orientem as unidades sob sua jurisdição a avaliar previamente a viabilidade de projetos de TI, incluindo, entre os objetos de análise, a verificação do custo/benefício do projeto, a exemplo do processo EDM02 – Assegurar a Entrega de Benefícios do Cobit 5;

9.1.4. orientem as organizações sob sua jurisdição a respeito da importância da adoção das seguintes práticas relativas ao planejamento de TI e seu acompanhamento:

9.1.4.1. atribuição de responsáveis pelo alcance dos objetivos e metas de TI;

9.1.4.2. definição de responsáveis pela aferição dos indicadores de TI;

9.1.4.3. disponibilização de indicadores estratégicos para acompanhamento por parte da alta administração, mediante relatórios ou sistemas específicos;

9.1.4.4. estabelecimento de instrumentos de acompanhamento, a exemplo de: sistemas, reuniões periódicas, relatórios;

9.1.4.5. definição de ações específicas para quando as metas de TI não forem alcançadas, a exemplo de: discussão em reuniões, escalamento, elaboração de planos de tratamento;

9.1.4.6. divulgação interna e externa do alcance das metas de TI, ou os motivos de elas não terem sido alcançadas.

9.1.5. normatizem a obrigatoriedade de que todas as organizações sob sua jurisdição gerenciem os riscos de TI a que estão sujeitos, por meio de um processo formal;

9.1.6. promovam ações de sensibilização e capacitação dos gestores das organizações sob sua jurisdição quanto à gestão de riscos de TI, com o objetivo de orientá-los sobre a identificação, análise, tratamento e comunicação dos riscos a que a instituição está sujeita;

9.1.7. orientem as unidades sob sua jurisdição no sentido de aprimorar os respectivos processos de gestão de orçamento e de custos de TI, a exemplo do disposto no processo APO06 – Gerenciar orçamento e custos do Cobit 5, com vistas a permitir a visualização e o acompanhamento da evolução dos custos diretos e indiretos de TI, incluindo, por exemplo, os custos ligados a recursos humanos (remuneração, treinamento etc.) e infraestrutura;

9.1.8. elaborem modelo de custos de TI para servir de referência para as organizações jurisdicionadas, baseado na definição dos serviços prestados, de forma a tornar a alocação de custos aos serviços de TI identificável, mensurável e previsível, a exemplo do previsto na prática APO06.04 - Modelar e alocar custos do Cobit 5.

9.2. recomendar ao Conselho Nacional de Justiça – CNJ e à Secretaria de Logística e Tecnologia da Informação do Ministério do Planejamento, Orçamento e Gestão – SLTI/MP que publiquem periodicamente os resultados das avaliações acerca do alcance dos objetivos e metas dispostos nos respectivos planos estratégicos de TI para o setor jurisdicionado, propiciando ampla transparência aos resultados atingidos.

9.3. recomendar ao Gabinete de Segurança Institucional da Presidência da República – GSI que:

9.3.1. elabore e acompanhe periodicamente, a exemplo do realizado na Estratégia Geral de Tecnologia da Informação no Sisp e da Estratégia de TIC no Poder Judiciário, planejamento que abranja a estratégia geral de segurança da informação para o setor sob sua jurisdição, envolvendo não somente a tecnologia da informação, mas também os demais segmentos relacionados à proteção das informações institucionais;

9.3.2. alerte as organizações sob sua jurisdição que a elaboração periódica de planejamento das ações de segurança da informação é obrigação expressa prevista no item 3.1 da Norma Complementar 2/IN01/DSIC/GSIPR, além de ser boa prática prevista na NBR ISO/IEC 27.001/2013, item 6, bem como no Cobit 5, Prática de Gestão APO 13.2.

9.4. recomendar ao Conselho Nacional de Justiça (CNJ) que:

9.4.1. elabore e acompanhe periodicamente, a exemplo do realizado na Estratégia Geral de Tecnologia da Informação no Sisp e na Estratégia de TIC no Poder Judiciário, planejamento que abranja a estratégia geral de segurança da informação para o setor sob sua jurisdição, envolvendo não somente a tecnologia da informação, mas todos os segmentos relacionados à proteção das informações institucionais;

9.4.2. alerte as organizações sob sua jurisdição que o estabelecimento de um modelo de gestão que abranja, entre outros processos, a elaboração periódica de planejamento estratégico de segurança da informação é diretriz expressa pelo Conselho Nacional de Justiça para a gestão da segurança da informação, além de ser boa prática prevista na NBR ISO/IEC 27.001/2013, item 6, bem como no Cobit 5, Prática de Gestão APO 13.2.

9.5. recomendar ao Conselho Nacional do Ministério Público (CNMP) que:

9.5.1. elabore e acompanhe periodicamente, a exemplo do realizado na Estratégia Geral de Tecnologia da Informação no Sisp e na Estratégia de TIC no Poder Judiciário, planejamento que abranja a estratégia geral de segurança da informação para o setor sob sua jurisdição, envolvendo não somente a tecnologia da informação, mas todos os segmentos relacionados à proteção das informações institucionais;

9.5.2. alerte as organizações sob sua jurisdição que o estabelecimento de um modelo de gestão que contemple, entre outros processos, a elaboração periódica de planejamento estratégico de segurança da informação é boa prática prevista na NBR ISO/IEC 27.001/2013, item 6, bem como no Cobit 5, Prática de Gestão APO 13.2.

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

9.6.1. encaminhe cópia integral deste relatório técnico aos OGS de forma a informá-los a respeito das constatações e conclusões obtidas nesse trabalho com o intuito de apoiar e subsidiar suas ações de normatização, estruturação, capacitação e gestão do setor jurisdicionado;

9.6.2. encaminhe cópia desta deliberação:

9.6.2.1. às organizações as quais foram dirigidas as recomendações da deliberação;

9.6.2.2. às organizações que foram individualmente fiscalizadas no âmbito da FOC;

9.6.2.3. à Comissão de Ciência e Tecnologia, Comunicação e Informática (CCTCI) da Câmara dos Deputados;

9.6.2.4. à Subcomissão Permanente de Ciência e Tecnologia e Informática da Comissão de Ciência e Tecnologia, Comunicação e Informática (CCTCI) da Câmara dos Deputados;

9.6.2.5. à Comissão de Ciência, Tecnologia, Inovação, Comunicação e Informática (CCT) do Senado Federal;

9.6.2.6. à Subcomissão Permanente de Serviços de Informática (CCTSINF) da Comissão de Ciência, Tecnologia, Inovação, Comunicação e Informática (CCT) do Senado Federal;

9.6.2.7. aos Tribunais de Contas dos Estados e dos Municípios, para conhecimento e subsídios às suas ações de controle externo pertinentes à área de TI;

9.7. autorizar a Sefti a promover a divulgação da Nota Técnica Sefti 7/2014, como forma de orientar as organizações da Administração Pública Federal no processo de amadurecimento de suas práticas de governança de TI, bem como a jurisprudência deste Tribunal quanto ao assunto.

9.8. encerrar o presente processo e arquivar os autos.

10. Ata n° 44/2014 – Plenário.
11. Data da Sessão: 5/11/2014 – Ordinária.
12. Código eletrônico para localização na página do TCU na Internet: AC-3051-44/14-P.
13. Especificação do quorum:
13.1. Ministros presentes: Aroldo Cedraz (na Presidência), Raimundo Carreiro e José Jorge.

13.2. Ministros-Substitutos convocados: Augusto Sherman Cavalcanti, Marcos Bemquerer Costa e Weder de Oliveira (Relator).

(Assinado Eletronicamente)
AROLDO CEDRAZ
na Presidência

(Assinado Eletronicamente)
WEDER DE OLIVEIRA
Relator

Fui presente:

(Assinado Eletronicamente)
LUCAS ROCHA FURTADO
Procurador-Geral, em exercício