UNIVERSIDADE CATÓLICA DE BRASÍLIA

PRÓ-REITORIA DE PÓS-GRADUAÇÃO E PESQUISA *LATO SENSU* EM MBA GOVERNANÇA EM TECNOLOGIA DA INFORMAÇÃO NO SERVIÇO PÚBLICO

Especialização

PROPOSTA PARA O PROCESSO DE SELEÇÃO E PLANEJAMENTO DE AUDITORIAS DE TI NAS UNIDADES GESTORAS DO PODER EXECUTIVO FEDERAL, BASEADA NA AVALIAÇÃO INTEGRADA DAS ESTRUTURAS DE GOVERNANÇA, GESTÃO DE RISCOS E CONTROLES INTERNOS

Autor: Rodrigo Teodoro Lima
Orientador: Esp. Michel Ivan Osandon Albarran

BRASÍLIA 2013

RODRIGO TEODORO LIMA

PROPOSTA PARA O PROCESSO DE SELEÇÃO E PLANEJAMENTO DE AUDITORIAS DE TI NAS UNIDADES GESTORAS DO PODER EXECUTIVO FEDERAL, BASEADA NA AVALIAÇÃO INTEGRADA DAS ESTRUTURAS DE GOVERNANÇA, GESTÃO DE RISCOS E CONTROLES INTERNOS

Monografia apresentada ao Programa de Pós-Graduação Lato Sensu – MBA em Governança de TI no Serviço Público da Fundação Universa, como requisito parcial para obtenção do certificado de Especialista em Administração Pública e Tecnologia da Informação.

Orientador: Esp. Michel Ivan Osandon Albarran

Brasília
2013

Monografia de autoria de Rodrigo Teodoro Lima, intitulada "PROPOSTA PARA O PROCESSO DE SELEÇÃO E PLANEJAMENTO DE AUDITORIAS DE TI NAS UNIDADES GESTORAS DO PODER EXECUTIVO FEDERAL, BASEADA NA AVALIAÇÃO INTEGRADA DAS ESTRUTURAS DE GOVERNANÇA, GESTÃO DE RISCOS E CONTROLES INTERNOS", apresentada como requisito parcial para obtenção do certificado de Especialista em MBA Governança em Tecnologia da Informação no Serviço Público da Universidade Católica de Brasília / Fundação Universa, em 30 de janeiro de 2013, aprovada por:

_____

Prof. Esp. Michel Ivan Osandon Albarran
Orientador

_____

Prof. Esp. Flávio Roberto Cruz Silva
Coordenador de Trabalho de Conclusão de Curso (TCC)

Brasília
2013

A Jesus, autor e consumador da minha fé, por quem me movo e para quem existo.
À minha bela e querida esposa, Anna Thereza, a quem tanto amo e muito quero bem.
Aos meus pais, Heliomar e Sirlei, que me propiciaram o dom da vida e toda sorte de incentivo e suporte na minha educação e formação.
Aos meus “pais 2”, Itamar e Maria José, que tão bem me acolheram em sua família.
Aos futuros filhos que ainda virão, pela graça de Deus.

AGRADECIMENTO

Ao meu professor e orientador, Michel Osandon, por sua grande parceria nesta empreitada final do curso.

Àqueles professores e colaboradores da Fundação Universa que acrescentaram um pouco de si à minha formação.

Aos colegas da CGU que acreditaram que este curso seria útil não só para mim, mas também para os trabalhos da Casa.

Aos colegas do MBA Eduardo Monnerat e Luiz Wagner, aos quais posso chamar de amigos, por todos os momentos que passamos juntos nestes dois anos de curso.

Ao meu amigo Luís Fernando Duarte, pela disposição em colaborar comigo na revisão do texto da monografia.

A todos familiares e amigos que desejam o melhor pra minha vida e que me amam pelo que sou.

“O saber a gente aprende com os mestres e os livros. A sabedoria se aprende é com a vida e com os humildes.”

Cora Coralina

RESUMO

Referência: LIMA, Rodrigo Teodoro. **Proposta para o processo de seleção e planejamento de auditorias de TI nas unidades gestoras do Poder Executivo Federal, baseada na avaliação integrada das estruturas de governança, gestão de riscos e controles internos.** 72 folhas. MBA em Governança de TI no Serviço Público – Fundação Universa, Brasília, 2013.

Este trabalho tem por objetivo apresentar uma proposta para o processo de seleção e planejamento de auditorias de TI nas unidades gestoras do Poder Executivo Federal, com base na avaliação integrada das estruturas de governança, gestão de riscos e controles internos. Tal avaliação é realizada de modo holístico (vê-se a organização como um todo) bem como de "cima para baixo", ou seja, parte-se da determinação dos objetivos estratégicos da organização e chega-se à identificação dos principais controles de TI que devem ser auditados. Para que isto fosse possível, realizou-se um estudo sistematizado dos principais referenciais teóricos sobre os temas: governança corporativa e planejamento estratégico (institucional e de TI); gestão de riscos; controles internos; *compliance* (conformidade); sistema de controle interno do poder executivo federal; e auditoria operacional.

Palavras-chave: Auditoria. Governança. Tecnologia da Informação. Controles. Planejamento.

ABSTRACT

This work intends to present a proposal for the IT audits selection and planning process on the management units of the Brazilian's Federal Executive Power, based on the integrated evaluation of the governance, risk management and internal controls structures. Such evaluation is done in a holistic and top-down approach, starting from the determination of the strategic objectives and ending on the identification of the key IT controls that have to be audited. In order to make that possible, there was a systematized study of the major theoretical frameworks on the following topics: corporative governance and strategic planning (for the whole organisation and for the IT area); risk management; internal controls; compliance; Federal Executive Power's internal control system; and operational auditing.

Key words: Audit. Governance. Information Technology. Controls. Planning.

LISTA DE FIGURAS

LISTA DE SIGLAS

AAC	Auditoria Anual de Contas
ABBI	Associação Brasileira de Bancos Internacionais
ABNT	Associação Brasileira de Normas Técnicas
AICPA	*American Institute of Certified Public Accountants*
ANVISA	Agência Nacional de Vigilância Sanitária
APF	Administração Pública Federal
APG	Acompanhamento Permanente dos Gastos
APO	*Align, Plan and Organize (COBIT 5)*
AS/NZS	*Australian Standard/New Zealand Standard*
BSC	*Balanced Scorecard*
CEO	*Chief Executive Officer*
CF/88	Constituição Federal de 1988
CGU	Controladoria-Geral da União
CNJ	Conselho Nacional de Justiça
CNMP	Conselho Nacional do Ministério Público
COBIT	*Control Objectives for Information Technology*
COSO	*Committee of Sponsoring Organisations*
DATAPREV	Empresa de Tecnologia e Informações da Previdência Social
DATASUS	Departamento de Informática do SUS
DN	Decisão Normativa
ERM	*Enterprise Risk Management*
FEBRABAN	Federação Brasileira de Bancos
FUNASA	Fundação Nacional de Saúde
GAIT	*Guide to the Assessment of IT*
GAIT-R	*Guide to the Assessment of IT for Business and Risk*
GESPÚBLICA	Programa Nacional de Gestão Pública e Desburocratização
GRC	*Governance, Risk and Compliance*
GTAG	*Global Technology Audit Guide*
IBGC	Instituto Brasileiro de Governança Corporativa
IEC	*International Electrotechnical Comission*
IFAC	*International Federation of Accountants*
IIA	*Institute of Internal Auditors*
IN	Instrução Normativa
INTOSAI	*International Organisation of Supreme Audit Institutions*
IPPF	*International Professional Practices Framework*
ISACA	*Information Systems Audit and Control Association*
ISO	*International Organisation for Standardization*
ITGC	*Information Technology General Control*
ITGI	*IT Governance Institute*
LDO	Lei de Diretrizes Orçamentárias
LOA	Lei Orçamentária Anual
MEGP	Modelo de Excelência em Gestão Pública
MPOG	Ministério do Planejamento, Orçamento e Gestão
NBR	Norma Brasileira
OCDE	Organização para a Cooperação e Desenvolvimento Econômico

OCEG	Open Compliance and Ethics Group
OECD	*Organisation for Economic Co-operation and Development*
OGS	Órgão de Governança Superior
PDTI	Plano Diretor de TI
PEC	Planejamento Estratégico Corporativo
PEE	Planejamento Estratégico Empresarial
PEI	Planejamento Estratégico Institucional
PEN	Planejamento Estratégico do Negócio
PETI	Planejamento Estratégico de TI
PO	*Plan and Organize (COBIT 4.1)*
PPA	Plano Plurianual
PQGF	Prêmio Nacional de Gestão Pública
ROI	*Return on Investment*
SAS	Secretaria de Atenção à Saúde
SAS	*Statement on Audit Standard*
SERPRO	Serviço Federal de Processamento de Dados
SESAI	Secretaria Especial de Saúde Indígena
SFC	Secretaria Federal de Controle Interno
SISP	Sistema de Administração dos Recursos de Informação e Informática
SLTI	Secretaria de Logística e Tecnologia da Informação
TC	Tecnologia da Comunicação
TCE	Tribunal de Contas do Estado
TCU	Tribunal de Contas da União
TI	Tecnologia da Informação
TIC	Tecnologia da Informação e Comunicação
TMS	Tema de Maior Significância
TOGAF	*The Open Group Architecture Framework*
UG	Unidade Gestora

SUMÁRIO

1. INTRODUÇÃO

A governança de tecnologia da informação (TI) é um tema que tem sido colocado em grande evidência na Administração Pública Federal (APF), principalmente após a divulgação do primeiro acórdão do Tribunal de Contas da União (TCU) sobre o assunto, a saber, o Acórdão TCU-Plenário 1.603/2008. Ciente de que a realização periódica de auditorias de TI nos órgãos e entidades da APF é capaz de contribuir significativamente para a melhoria da gestão e da governança de TI no setor público, o TCU tem, desde então, recomendado à Controladoria-Geral da União (CGU), órgão central de controle interno do Poder Executivo Federal, que realize regularmente auditorias de TI, bem como que atue no sentido de estimular a realização dessas auditorias nas unidades sob sua jurisdição.

A partir da Decisão Normativa (DN) TCU nº 117/2011, que inseriu a exigência de avaliação objetiva – nos relatórios de auditoria da gestão elaborados pelos órgãos de controle interno – sobre a gestão de TI das unidades gestoras (UGs) da APF selecionadas para julgamento de suas contas, a CGU passou a ter a obrigação legal de realizar auditorias relacionadas à tecnologia da informação.

É sabido, no entanto, que a avaliação da gestão de TI das UGs realizada dentro da avaliação global de seu processo de prestação de contas não tem sido suficiente para a promoção de uma célere e efetiva evolução da gestão e governança da TI nas unidades avaliadas, em virtude do exíguo tempo e esforço a ela dedicados.

Uma tentativa adicional, por parte da CGU, para a melhoria da avaliação da TI das UGs foi a inserção do tema no processo de acompanhamento permanente dos gastos (APG). Entretanto, por muitas vezes, a avaliação da gestão da TI efetuada dentro do APG tem sido meramente uma simples antecipação da avaliação realizada na auditoria anual de contas (AAC) do exercício seguinte, o que por si só não agrega valor ao processo de avaliação da TI da unidade como um todo.

Corrobora o argumento introduzido o fato de que o TCU ainda julga pouco satisfatórios os resultados até então alcançados pela CGU quanto à realização de auditorias de TI nas UGs por ela avaliadas. Tal inferência pode ser facilmente depreendida a partir da leitura dos excertos a seguir transcritos do Acórdão TCU-Plenário 1.145/2011, referente ao relatório de monitoramento de determinações e recomendações endereçadas aos órgãos de governança superiores (OGS) na APF:

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

> 143. Análise: em que pese os resultados apresentados pela CGU, já registramos que as auditorias de TI ainda não são regularmente realizadas pelo órgão (itens 14-22). Ademais, o gestor menciona os trabalhos realizados com foco na avaliação de contratos de terceirização (item 4, peça 18, fl. 3), e não foram apresentadas evidências de que a CGU tem estimulado a realização desse tipo de auditoria nos órgãos e entidades da APF.
>
> 144. Novamente, a ausência de evidência de que há uma atuação sistematizada e coordenada pelo órgão central do controle interno do Poder Executivo no tema TI deve ser levado em consideração quando da consolidação dos trabalhos do TMS 6 – Gestão e uso de TI.
>
> [...]
>
> 310. Na mesma linha do que já foi relatado em outros itens deste relatório, não há evidências nas diversas deliberações monitoradas de que a CGU atue de maneira sistematizada quando se trata de auditoria de TI. Tais fatos deverão ser levados em consideração quando da consolidação do TMS 6 – Gestão e uso de TI. (ACÓRDÃO TCU-PLENÁRIO 1.145/2011, grifo nosso).

O conteúdo do acórdão supracitado foi posteriormente aproveitado pelo Acórdão TCU-Plenário 1.233/2012, relativo ao relatório consolidado das ações do Tema de Maior Significância (TMS) 6/2010, cujo objetivo foi avaliar se a gestão e o uso da tecnologia da informação estão de acordo com a legislação e aderentes às boas práticas de governança de TI. Deste acórdão são transcritas apenas, a seguir, as recomendações que foram direcionadas à CGU:

> 9.10. Recomendar, com fundamento na Lei 8.443/1992, art. 43, inciso I, c/c RITCU, art. 250, inciso III, à Controladoria-Geral da União (CGU/PR) que:
>
> 9.10.1. considere os temas governança de TI, riscos de TI e controles de TI na seleção dos objetos a auditar, consoante o previsto nas boas práticas internacionais para que a atividade de auditoria interna seja mais efetiva (e.g., IPPF 2110.A2, 2120.A1 e 2130.A1; subitem II.11).
>
> 9.10.2. oriente as unidades de auditoria interna sob sua orientação normativa a considerar os temas governança de TI, riscos de TI e controles de TI na seleção dos objetos a auditar, consoante o previsto nas boas práticas internacionais para que a atividade de auditoria interna seja mais efetiva (e.g., IPPF 2110.A2, 2120.A1 e 2130.A1; subitem II.11).
>
> (ACÓRDÃO TCU-PLENÁRIO 1.233/2012, grifo nosso).

A partir da motivação trazida pela constatação da necessidade de a CGU promover a realização sistemática de trabalhos de auditoria na área de tecnologia da informação, o presente trabalho visa, primariamente, responder à seguinte questão: como planejar auditorias de TI nos órgãos e entidades do Poder Executivo Federal que possam ser capazes de agregar valor à Administração e à sociedade brasileira?

A partir da questão de pesquisa colocada, optou-se pela delimitação de uma abordagem para o processo de seleção e planejamento de auditorias de TI que fosse focada

numa avaliação *top-down*[1] das unidades gestoras, integrando a análise das estruturas de governança, gestão de riscos e controles internos.

Este trabalho tem como objetivo geral apresentar a proposta de um processo que sirva como referência para a elaboração de um plano de auditorias de TI para os órgãos e entidades da Administração Pública Federal, com ênfase naqueles pertencentes ao Poder Executivo, que estão sob o foro de atuação da CGU.

Em se tratando dos objetivos específicos, podemos arrolar os seguintes:

a) analisar e sintetizar os principais referenciais teóricos acerca dos temas: governança, planejamento estratégico, gestão de riscos, controles internos e *compliance*, com uma visão não só da área de TI, mas, holística para a organização, buscando integrá-los e aplicá-los em um guia único de orientações;
b) apresentar uma proposta para o processo de seleção e planejamento de auditorias operacionais de TI (mescladas a avaliações de conformidade) que possa ser utilizada pela CGU nos órgãos e entidades do Poder Executivo Federal.

Esta pesquisa não poderia deixar de comentar sobre o histórico de alguns trabalhos desenvolvidos na CGU com relação ao macrotema "auditoria de TI". Inicialmente cumpre lembrar Hanashiro (2007), dissertação de mestrado referente à "metodologia para desenvolvimento de procedimentos e planejamento de auditorias de TI aplicada à Administração Pública Federal". Esse trabalho, aparentemente pioneiro no assunto no interior da CGU, baseou-se primariamente no *framework Control Objectives for Information Technology* (COBIT), à época em sua versão 4.1, e, secundariamente, em outros modelos de melhores práticas, e.g., ISO[2] 17799:2005, posteriormente atualizada para ISO 27002:2005. A dissertação apresenta, em seu capítulo 4, um modelo geral de planejamento e elaboração de procedimentos e, no capítulo 5, traz um exemplo de aplicação desta metodologia na avaliação dos procedimentos de controle de acesso, dentro da matéria de segurança da informação.

Nesse mesmo diapasão, pode-se resgatar também à memória o trabalho de Silva (2008), dissertação de mestrado que trouxe uma importante contribuição à CGU no que se refere à elaboração de um modelo de diretrizes de auditoria a serem aplicadas quando da avaliação dos processos de contratação de soluções de TI das unidades gestoras da APF.

Numa linha um pouco mais diversa (no que se refere aos objetivos da pesquisa), pode-se citar ainda Hanashiro (2009), monografia de conclusão de curso de especialização

[1] De cima para baixo (iniciando a partir da visão estratégica, passando pela visão tática e chegando à visão operacional da unidade, o que será explicado nos capítulos seguintes do trabalho).
[2] Do inglês, "*International Organisation for Standardization*".

que focou na proposição da criação de uma unidade técnica especializada de auditoria de TI no interior da Secretaria Federal de Controle Interno (SFC), a ser estruturada na forma de um escritório de projetos.

Já saindo do âmbito interno à CGU, impende também ressaltar a grande contribuição trazida à comunidade acadêmica e profissional de auditoria por Monteiro (2008) em seu trabalho direcionado ao estudo das experiências do Tribunal de Contas do Estado do Rio de Janeiro (TCE/RJ) na realização de auditorias operacionais em tecnologia da informação.

Este presente trabalho não pretende ser único, nem o poderia ser. Visa-se aqui apenas adicionar uma modesta contribuição à já ampla bagagem de conhecimento acumulada pela comunidade acadêmica e profissional de governança e auditoria de TI ao longo dos últimos anos. Intenta-se contribuir para o amadurecimento das auditorias de TI realizadas pela CGU nos órgãos e entidades do Poder Executivo Federal, em atendimento às determinações e recomendações expedidas pelo Tribunal de Contas da União, por meio da aplicação das melhores práticas de mercado, devidamente adaptadas, no contexto da Administração Pública Federal.

Com relação ao público alvo da presente monografia, acredita-se que este será composto principalmente pelos servidores da CGU que desejem ou necessitem planejar trabalhos de auditoria na área de tecnologia da informação. O trabalho pretende atender, apesar das dificuldades inerentes a esta abordagem, aos auditores generalistas com pouca ou nenhuma formação na área de TI, bem como àqueles profissionais com razoável ou ampla formação em TI, mas pouca experiência nas matérias de governança, gestão de riscos, controles internos e auditoria interna.

Em resumo, intenta-se dar suporte ao atendimento dos seguintes itens do documento "Normas internacionais para a prática profissional de auditoria interna"[3], do *Institute of Internal Auditors* (IIA):

> 1210.A3 – Os auditores internos devem possuir conhecimento suficiente sobre os principais riscos e controles de tecnologia da informação e sobre as técnicas de auditoria baseadas em tecnologia disponíveis para a execução dos trabalhos a eles designados. Entretanto, não se espera que todos os auditores internos possuam a especialização de um auditor interno cuja principal responsabilidade seja auditoria de tecnologia da informação.
> [...]
> 2110.A2 – A atividade de auditoria interna deve avaliar se a governança de tecnologia da informação da organização dá suporte às estratégias e objetivos da organização.
> [...]

[3] Tradução do documento original na língua inglesa: *International Professional Practices Framework* (IPPF).

> 2120.A1 – A atividade de auditoria interna deve avaliar as exposições a riscos relacionadas à governança, às operações e aos sistemas de informação da organização, em relação a:
>
> - Confiabilidade e integridade das informações financeiras e operacionais;
> - Eficácia e eficiência das operações e programas;
> - Salvaguarda dos ativos;
> - Conformidade com as leis, regulamentos, políticas, procedimentos e contratos;
>
> [...]
>
> 2130.A1 – A atividade de auditoria interna deve avaliar a adequação e a eficácia dos controles em resposta aos riscos, abrangendo a governança, as operações e os sistemas de informação da organização, com relação a:
>
> - Confiabilidade e integridade das informações financeiras e operacionais;
> - Eficácia e eficiência das operações e programas;
> - Salvaguarda dos ativos;
> - Conformidade com as leis, regulamentos, políticas e procedimentos e contratos;
>
> (IIA, 2010, grifo nosso).

No que se refere à metodologia empregada para sua realização, a presente pesquisa pode ser classificada, quanto aos fins, em aplicada, haja vista ter sido motivada pela necessidade de se aprimorar e fomentar a realização de trabalhos de auditoria de TI pelos servidores da CGU. Quanto aos meios, classifica-se em bibliográfica e documental, baseando-se no estudo sistematizado de conteúdo publicado em normas técnicas, *frameworks* de melhores práticas, artigos especializados, documentos acadêmicos, livros, revistas e outros, bem como na consulta e análise dos principais normativos legais e jurisprudência correlata, notadamente a representada pelos acórdãos do TCU.

O trabalho não envolveu pesquisa de campo – cuja necessidade vislumbrou-se, a priori, para a análise e validação da proposta para o processo de seleção e planejamento de auditorias de TI no Poder Executivo Federal – em virtude da limitação de tempo imposta à sua redação e conclusão.

Em termos de organização de seu conteúdo, a monografia está disposta da seguinte forma:

No capítulo 1 – "Introdução" evidenciam-se os antecedentes do problema abordado na pesquisa, a justificativa (também chamada de motivação), a situação problema (ou questão da pesquisa), os objetivos (tanto o geral quanto os específicos), a delimitação do escopo, o público alvo, a metodologia empregada e a estrutura do trabalho.

No capítulo 2 – "Fundamentação teórica" apresenta-se a teoria que suporta a pesquisa. Neste capítulo abordam-se os seguintes temas: governança corporativa, governança de TI, planejamento estratégico institucional e de TI, gestão de riscos, controles internos, controles

de TI, *compliance*, GRC[4], sistema de controle interno do Poder Executivo Federal, auditoria operacional e auditoria de conformidade.

No capítulo 3 – "Proposta": é apresentada e descrita, passo a passo, a proposta relativa ao processo de seleção e planejamento de auditorias de TI no âmbito do Poder Executivo Federal, com base numa avaliação integrada da governança, dos riscos e dos controles internos da unidade gestora examinada.

Por fim, no capítulo 4 – "Conclusão": são apresentadas as conclusões pertinentes ao desfecho da pesquisa empreendida. Evidencia-se o atendimento aos objetivos propostos, comenta-se sobre as principais dificuldades e limitações encontradas e são realizadas sugestões de trabalhos futuros na linha dos temas desenvolvidos.

[4] Esta sigla se refere à abordagem integrada de governança, riscos e conformidade (do inglês, "*governance, risk and compliance*"), a qual é explicada no item 2.5.1 deste trabalho.

2. FUNDAMENTAÇÃO TEÓRICA

Neste capítulo são apresentados e analisados os principais conceitos relacionados ao escopo delimitado pelo trabalho. Por meio destes, pretende-se construir uma linguagem comum aos auditores da CGU quando da realização de trabalhos de auditoria de tecnologia da informação, assim como sustentar a proposta apresentada no capítulo 3 para o processo de seleção e planejamento de auditorias de TI a serem realizadas nos órgãos e entidades do Poder Executivo Federal.

2.1 GOVERNANÇA

2.1.1 Governança corporativa (ou governança institucional)

Segundo o IBGC[5] (2010), "governança corporativa é o sistema pelo qual as organizações são dirigidas, monitoradas e incentivadas, envolvendo os relacionamentos entre proprietários, Conselho de Administração, Diretoria e órgãos de controle". Ainda segundo este instituto, "as boas práticas de governança corporativa convertem princípios em recomendações objetivas, alinhando interesses com a finalidade de preservar e otimizar o valor da organização, facilitando seu acesso a recursos e contribuindo para sua longevidade".

Para o IBGC, os princípios básicos de governança corporativa são: i) a transparência, relativa à disponibilização, para as partes interessadas, das informações que sejam de seu interesse e não apenas aquelas impostas pelas disposições de leis ou regulamentos; ii) a equidade, caracterizada pelo tratamento justo de todos os sócios e demais partes interessadas; iii) a prestação de contas (*accountability*), que diz respeito ao ato, executado pelos agentes de governança, de prestar contas pela sua atuação, assumindo integralmente as consequências de seus atos e omissões; e iv) a responsabilidade corporativa, que diz respeito ao zelo pela sustentabilidade das organizações, visando a sua longevidade.

Para a OCDE[6] (2004), a governança corporativa:

> [...] envolve um conjunto de relacionamentos entre a gerência da organização, seu corpo diretor, seus acionistas e demais partes interessadas. A governança corporativa também provê a estrutura pela qual os objetivos da organização são definidos, assim como determina os meios de alcance destes objetivos e seus respectivos indicadores de desempenho. (OCDE, 2004, tradução livre).

Segundo Matias-Pereira (2010), a governança nas organizações públicas e nas organizações privadas apresenta significativas similitudes, pois, a despeito das

[5] Instituto Brasileiro de Governança Corporativa

[6] Organização para a Cooperação e Desenvolvimento Econômico. Sigla original em inglês: OECD – *Organisation for Economic Co-operation and Development*.

particularidades específicas dos setores público e privado, observa-se que são comuns entre eles as questões que envolvem a separação entre propriedade e gestão (responsáveis pela geração dos problemas de agência), as referentes aos instrumentos definidores de responsabilidades e poder, bem como aquelas que dizem respeito ao acompanhamento e incentivo na execução das políticas e objetivos definidos, entre outros. Enuncia ainda o mesmo autor que "verifica-se, em um sentido amplo, que os princípios básicos que norteiam os rumos dos segmentos dos setores privado e público são idênticos: transparência, equidade, cumprimento das leis, prestação de contas e conduta ética".

De acordo com o IFAC[7] (2001, apud MATIAS-PEREIRA, 2010), os três princípios fundamentais de governança no setor público são:

a. *Openness* (Transparência): é requerido para assegurar que a sociedade possa ter confiança no processo de tomada de decisão executado nas entidades do setor público, assim como na sua gestão e nas pessoas que nelas trabalham;
b. *Integrity* (Integridade): compreende procedimentos honestos e perfeitos. É baseada na honestidade, objetividade, normas de propriedade, probidade na administração dos recursos públicos e na gestão da instituição;
c. *Accountability* (responsabilidade de prestar contas): as entidades do setor público e seus indivíduos são responsáveis por suas decisões e ações, incluindo a administração dos recursos públicos e todos os aspectos de desempenho e, submetendo-se ao escrutínio externo apropriado.

Matias-Pereira, citando o estudo do IFAC, comenta ainda que:

> O IFAC, além dos seus princípios, apresenta as dimensões que as entidades da administração pública devem adotar:
>
> - Padrões de comportamento – como a administração da entidade exercita a liderança e determina os valores e padrões da instituição, como define a cultura da organização e o comportamento de todos os envolvidos.
> - Estruturas e processos organizacionais – como a cúpula da administração é designada e organizada dentro da instituição, como as responsabilidades são definidas e como elas são asseguradas.
> - Controle – a rede de vários controles estabelecidos pela cúpula administrativa da organização no apoio ao alcance dos objetivos da entidade, da efetividade e eficiência das operações, da confiança dos relatórios internos e externos, da complacência com as leis aplicáveis, regulamentações e políticas internas.
> - Relatórios externos – como a cúpula da organização demonstra a prestação de contas da aplicação do dinheiro público e seu desempenho.
>
> (IFAC, 2001, apud MATIAS, 2010).

[7] Do inglês, "*International Federation of Accountants*".

Para Hodger *et al* (1996, apud DE MELLO, 2006), a governança corporativa está preocupada com os procedimentos associados com a tomada de decisão, desempenho e controle, tendo por objetivo providenciar estruturas para dar direção global à organização e satisfazer as expectativas de responsabilidade em prestar contas para seu exterior.

Uma definição simples de governança corporativa e que resume todas estas outras definições anteriormente citadas pode ser encontrada no relatório do comitê dos aspectos financeiros de governança corporativa (CADBURY REPORT, 1992, apud DE MELLO, 2006), que a conceituou como "o sistema pelo qual as organizações são dirigidas e controladas". Essa definição também foi adotada pela norma ABNT/NBR ISO/IEC 38500.

É importante ressaltar que existe uma distinção clara entre os conceitos de governança e gestão. Tal diferenciação conceitual foi muito bem analisada pelo COBIT 5 (2012), sendo um dos cinco princípios fundamentais desse *framework*. Para o COBIT, estas duas disciplinas compreendem diferentes tipos de atividades, requerem estruturas organizacionais distintas e servem a diferentes propósitos, podendo ser definidas como se segue[8]:

- Governança: assegura que as necessidades, condições e opções dos *stakeholders*[9] são avaliadas para se determinar, balancear e acordar os objetivos estratégicos a serem atingidos pela corporação. Tal garantia é alcançada pelo direcionamento dado pela priorização e tomada de decisão, bem como pelo monitoramento do desempenho e da conformidade com a direção acordada e com os objetivos traçados. Na maioria das corporações, a governança é de responsabilidade do corpo de diretores, sob a liderança do presidente.
- Gestão: planeja, define, executa e monitora atividades em alinhamento com a direção definida pelo corpo de governança da organização, de modo a propiciar o alcance dos objetivos estratégicos traçados. Na maioria das organizações, a gestão é de responsabilidade da gerência executiva, sob a liderança do CEO – *Chief Executive Officer*.

A gestão também pode ser alternativamente denominada gerenciamento, de acordo com a linguagem da norma ISO 38500, a qual definiu este termo como sendo "o sistema de controles e processos necessário para alcançar os objetivos estratégicos estabelecidos pela direção da organização, estando sujeito às diretrizes, às políticas e ao monitoramento estabelecidos pela governança corporativa".

[8] Tradução nossa.
[9] Partes interessadas (ou aqueles que detêm uma das "fatias do bolo").

2.1.2 Governança de TI (ou governança corporativa de TI)

Segundo o COBIT 4.1 em português (2007) e o ITGI[10] (2003), 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".

O COBIT 4.1 descreve ainda que:

> [...] a governança de TI integra e institucionaliza boas práticas para garantir que a área de TI da organização suporte os objetivos de negócios. A governança de TI habilita a organização a obter todas as vantagens de sua informação, maximizando os benefícios, capitalizando as oportunidades e ganhando em poder competitivo. Esses resultados requerem um modelo para controle de TI que se adeque e dê suporte ao COSO ("*Committe of Sponsoring Organisations of the Treadway Commission's Internal Control – Integrated Framework*"), um modelo para controles internos amplamente aceito para governança e gerenciamento de riscos empresariais, e outros modelos similares. (COBIT 4.1, 2007, grifo nosso).

Uma definição alternativa interessante é a utilizada pela *Forrester* (2005), a qual define a governança de TI como sendo o "processo pelo qual decisões são tomadas sobre os investimentos em TI, o que envolve: como as decisões são tomadas, quem toma as decisões, quem é responsabilizado e como os resultados são medidos e controlados".

A norma ISO/IEC 38500, por sua vez, preferiu utilizar a denominação "governança corporativa de TI"[11], a qual também passou a ser adotada pelo COBIT 5, definindo-a da seguinte maneira:

> O sistema pelo qual o uso atual e futuro da TI é dirigido e controlado. Governança corporativa de TI significa avaliar e direcionar o uso da TI para dar suporte à organização e monitorar seu uso para realizar os planos. Inclui a estratégia e as políticas de TI dentro da organização. (ABNT NBR ISO/IEC 38500, 2009).

Cumpre informar que o COBIT, após um longo período de amadurecimento por parte de seus autores e colaboradores, constatou, em sua última versão (COBIT 5), como sendo de grande importância visualizar a governança de TI dentro de uma abordagem "ponta-a-ponta" e holística na organização (princípios 2 e 4 do *framework*), situando-a dentro de um contexto de governança corporativa, o que provocou a "evolução" para a denominação "governança corporativa de TI". É importante também notar que, na visão do COBIT 5, a criação de valor pela organização é um objetivo-chave para a governança, sendo que, na definição deste *framework*, criar valor significa realizar benefícios por meio de uma ótima utilização dos recursos e uma ótima gestão dos riscos da organização. Os benefícios podem assumir variadas

[10] Do inglês, "*IT Governance Institute*".
[11] Do inglês, "*corporate governance of IT*".

formas como, por exemplo, financeiros para empresas privadas ou serviços públicos para entes governamentais.

O documento "Normas internacionais para a prática profissional da auditoria interna", do IIA, na mesma linha do já exposto, define a governança da tecnologia da informação como consistindo da liderança, das estruturas organizacionais e dos processos que asseguram que a tecnologia da informação corporativa dá suporte às estratégias e aos objetivos da organização.

Uma descrição um pouco mais detalhada da governança de TI é dada pelo GTAG[12] 17 – *Auditing IT Governance*, também do IIA. Segundo este guia, a governança de TI envolve o gerenciamento das operações e projetos de TI de modo a assegurar o alinhamento destas atividades com as necessidades da organização definidas em seu plano estratégico. Discorre-se ainda que o alinhamento entre a TI e a organização significa que:

a) a direção da organização compreende qual o potencial e quais as limitações de sua área de TI;
b) a área de TI compreende os objetivos e correspondentes necessidades da organização;
c) esta compreensão é aplicada e monitorada por toda a organização por meio de uma estrutura apropriada de governança.

2.2 PLANEJAMENTO ESTRATÉGICO

2.2.1 Planejamento estratégico institucional

Segundo Certo (1993, apud Carmona, 2010), a estratégia "é definida com um curso de ação com vistas a garantir que a organização alcance seus objetivos. Formular estratégia é, então, projetar e selecionar estratégias que levem à realização dos objetivos organizacionais".

De acordo com Christensen e Rocha (1995, apud Barbosa e Brondani, 2005), as origens do termo estratégia encontram-se na teoria militar, de onde foi adotado, significando a utilização do combate para atingir a finalidade da guerra. Já no contexto organizacional, a estratégia, para esses autores, corresponde à capacidade de se trabalhar contínua e sistematicamente o ajustamento da organização às condições ambientais que se encontram em constante mudança, tendo sempre em mente a visão de futuro e a perpetuidade organizacional.

A necessidade de uma nova abordagem para a administração e mensuração de desempenho das organizações, voltada não mais para apenas números financeiros e contábeis, mas, sim, para indicadores de desempenho, se tornou mais forte a partir do final da década de

[12] Do inglês, "*Global Technology Audit Guide*".

1980 e início da década de 1990, quando as organizações migraram de uma competição da era industrial para uma nova competição da era da informação. Nas palavras de Kaplan e Norton (1997), “as empresas não conseguem mais obter vantagens competitivas sustentáveis apenas com a rápida alocação de novas tecnologias e ativos físicos e com a excelência da gestão eficaz dos ativos e passivos financeiros”.

Como bem explicou Eccles (2000, apud Da Silva, 2003), os tradicionais números financeiros retratam apenas o desempenho passado de uma organização. Tal inferência pode ser obtida ao percebermos que o balanço patrimonial, importante instrumento da contabilidade, é, literalmente, um retrato estático das decisões organizacionais, movimentações financeiras e controle dos estoques de ativos físicos compreendidos em um determinado espaço de tempo.

Discorre Da Silva (2003) que o primeiro passo para a gestão de aspectos não financeiros surgiu com o movimento da qualidade ainda na década de 1980, tendo sido assim definidos indicadores de níveis de qualidade, como prazos de resposta, índices de defeitos, compromisso de entrega, entre outros.

Em verdade, apesar de a estruturação do conceito de administração estratégica ter se dado apenas na década de 1990, o conceito de planejamento estratégico foi proposto muito antes disso, ainda em meados dos anos 1960, pelo professor Igor Ansoff, por pesquisadores do *Stanford Research Institute* e por consultores da *McKinsey Consulting*, sendo que Philip Kotler, um dos defensores de sua utilização, propôs o seguinte conceito, complementado por Alday (2000, apud Carmona, 2010):

> O planejamento estratégico é uma metodologia gerencial que permite estabelecer a direção a ser seguida pela organização, visando maior grau de interação com o ambiente. A direção engloba os seguintes itens: âmbito de atuação, macropolíticas, políticas funcionais, filosofia de atuação, macroestratégia, estratégias funcionais, macro-objetivos e objetivos funcionais. (ALDAY, 2000, apud Carmona, 2010).

Apesar de alguns autores tratarem planejamento estratégico e administração estratégica como sinônimos, esta última se apresenta mais ampla, possivelmente compreendendo a primeira, tendo sido definida por Certo como “um processo contínuo e iterativo que visa manter uma organização como um conjunto apropriadamente integrado a seu ambiente”. Ainda na visão deste autor, corroborada pela de Alday, a administração estratégica é composta, basicamente, pelas seguintes etapas: análise do ambiente, estabelecimento da diretriz organizacional, formulação da estratégia, implementação da estratégia organizacional e controle estratégico.

Das definições trazidas, percebe-se que a administração estratégica foi responsável por trazer um novo olhar para a gestão: mais dinâmico, preocupado com as rápidas mudanças ambientais – tanto internas quanto externas – da sociedade do conhecimento, abrigador da avaliação dos ativos organizacionais intangíveis e voltado tanto para o presente quanto para o futuro, na tentativa de garantir a longevidade das organizações.

Como afirmaram Kaplan e Norton (2000, apud Da Silva, 2003), as organizações necessitam, atualmente, de uma linguagem para a comunicação tanto da estratégia como dos processos e sistemas que contribuem para sua implementação e que geram *feedback* sobre ela. Em 1992, estes dois autores, professores da *Harvard Business School*, desenvolveram uma metodologia de gestão estratégica, inicialmente apresentada como um modelo de avaliação de desempenho organizacional, denominada *Balanced Scorecard* (BSC), a qual considerava quatro conjuntos de indicadores, também chamados de perspectivas: financeira, do cliente, dos processos internos e do aprendizado e conhecimento. Estas perspectivas, justificando a própria denominação da metodologia, deveriam estar devidamente balanceadas, ou seja, aplicadas com graus de importância relativa, porém de modo equitativo, com vistas a subsidiar um desenvolvimento real e equilibrado.

Segundo Rocha (2000, apud Balzani, 2006), o BSC é um sistema de medidas que deve traduzir a visão e a estratégia de uma organização em objetivos e metas tangíveis, capazes de representar o equilíbrio entre indicadores externos, voltados para os acionistas e clientes, e internos, focados nos processos críticos, de inovação e de aprendizado e conhecimento.

Nas palavras dos próprios Kaplan e Norton (1997, apud Da Silva, 2003), no BSC a comunicação se dá por meio de sua estrutura lógica, baseada no gerenciamento das metas estabelecidas, possibilitando aos gestores realocar recursos físicos, financeiros e humanos para que possam alcançar os objetivos estratégicos.

O planejamento estratégico das organizações, de maneira geral, tem sido referido pela comunidade acadêmica por meio de variadas denominações e suas correspondentes siglas, dentre as quais podemos citar algumas principais: i) PEI – Planejamento Estratégico Institucional; ii) PEN – Planejamento Estratégico do Negócio; iii) PEE – Planejamento Estratégico Empresarial; e iv) PEC – Planejamento Estratégico Corporativo.

As últimas denominações, planejamento estratégico empresarial – PEE e planejamento estratégico corporativo – PEC, por estarem mais diretamente relacionadas à realidade das corporações da iniciativa privada, não serão utilizadas no âmbito deste trabalho, tendo sido citadas apenas a título de conhecimento. Quanto ao planejamento estratégico do negócio (PEN), importa trazer a conceituação dada por Bhalla (1987, apud Pereira, 2011) para que o

leitor se certifique de que esta guarda estreita afinidade com os conceitos já discutidos. Este autor definiu o PEN como "o processo que favorece a determinação dos principais objetivos de uma organização, do uso e disponibilidade dos recursos para realização dos seus objetivos, das suas políticas e estratégias".

Dentre os quatro termos citados, o que se adotará neste trabalho será o referente ao planejamento estratégico institucional (PEI), haja vista sua maior utilização no contexto da Administração Pública Federal brasileira, possivelmente em razão do fato de ser a denominação preferencialmente adotada pelo Tribunal de Contas da União em seus acórdãos, como se verá a seguir.

Em se tratando da Administração Pública Federal brasileira, a importância dada ao planejamento das ações do Estado vem desde o Decreto-Lei nº 200/1967 – ainda vigente no ordenamento jurídico nacional – o qual definiu o planejamento como um dos cinco princípios fundamentais das atividades da Administração.

O Programa Nacional de Gestão Pública e Desburocratização (GESPÚBLICA), implementado em 2005 pelo Governo Federal, em decorrência da evolução de iniciativas voltadas à missão de contribuir para a melhoria da qualidade dos serviços públicos prestados ao cidadão e o aumento da competitividade do país, tem como uma das vertentes de sua atuação o Prêmio Nacional de Gestão Pública (PQGF). Este prêmio é reconhecido como instância de verificação do nível de gestão das instituições públicas, tendo como principal referência o Modelo de Excelência em Gestão Pública (MEGP), baseado no atendimento aos princípios constitucionais do ser público e em fundamentos contemporâneos de boa gestão.

O MEGP tem como objetivo orientar a adoção de práticas de excelência em gestão nas organizações públicas brasileiras, consistindo na representação de um sistema gerencial constituído por 8 partes integradas, espelhados em 8 critérios utilizados como referenciais de excelência (requisitos), podendo ser dividido em 4 blocos, que se inter-relacionam, de maneira tal que possa subsidiar a implementação de ciclos contínuos de avaliação e melhoria da gestão. A representação gráfica simplificada deste modelo é dada pela figura a seguir:

Figura 1 – Visão sistêmica do MEGP

Fonte: Documento de Referência do Programa Nacional de Gestão Pública e Desburocratização (GESPÚBLICA), Secretaria de Gestão do MPOG, 2009.

O primeiro bloco, representando o planejamento, é composto pelos critérios de 1 a 4, sendo o critério 2 referente a "estratégias e planos". O segundo bloco, representando a execução, é composto pelos critérios "6 – pessoas" e "7 – processos". O terceiro, representando o controle, é composto pelo critério "8 – resultados" e o quarto, referente à inteligência das organizações, é composto pelo critério "5 – informação e conhecimento".

O critério "2 – estratégias e planos", com pontuação máxima de 60 pontos (de um total de 1000) é composto por dois itens, sendo um referente à avaliação da formulação das estratégias da organização pública e o outro referente à implementação destas.

O Tribunal de Contas da União, em seu Acórdão TCU-Plenário 1.603/2008, referente ao levantamento da situação da governança de tecnologia da informação na Administração Pública Federal, teceu as seguintes considerações quanto à importância do planejamento estratégico institucional para os órgãos e entidades da APF:

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

> 18. Dentro desse cenário de instabilidade, o planejamento tem se tornado cada vez mais importante e vital e deve ser construído de maneira flexível, com o engajamento e comprometimento de todos os colaboradores da organização. As organizações que não planejam correm riscos de não alcançarem os objetivos desejados. Com uma visão de futuro estabelecida, as organizações poderão se adaptar às constantes mudanças que ocorrem na sua área de atuação e agilizar seu processo de tomada de decisões.
>
> 19. O planejamento estratégico torna-se uma importante ferramenta para a tomada de decisão e faz com que os gestores estejam aptos a agir com iniciativa, de forma pró-ativa, contra as ameaças e a favor das oportunidades identificadas nas constantes mudanças que ocorrem. (ACÓRDÃO TCU-PLENÁRIO 1.603/2008, grifo nosso).

Por fim, o referido acórdão recomendou ao Conselho Nacional de Justiça (CNJ), ao Conselho Nacional do Ministério Público (CNMP) e ao Ministério do Planejamento, Orçamento e Gestão (MPOG) que, nos órgãos e entidades de suas estruturas, promovessem ações com o objetivo de disseminar a importância do planejamento estratégico, procedendo, inclusive mediante orientação normativa, à execução de ações voltadas à implantação e/ou aperfeiçoamento de planejamento estratégico institucional, planejamento estratégico de TI e comitê diretivo de TI, com vistas a propiciar a alocação dos recursos públicos conforme as necessidades e prioridades da organização.

O CNJ, após o Acórdão 1.603/2008, elaborou e publicou a Resolução nº 70/2009, a qual instituiu o planejamento estratégico no âmbito do Poder Judiciário. O MPOG, apesar de não ter focado na questão da valorização da definição de instrumentos de planejamento estratégico institucional pelos órgãos e entidades do Poder Executivo Federal, instituiu a Instrução Normativa (IN) SLTI[13]/MPOG nº 04/2008, posteriormente atualizada pela IN SLTI/MPOG nº 04/2010, que normatiza o processo de contratação de soluções de tecnologia da informação no âmbito do SISP – Sistema de Administração dos Recursos de Informação e Informática. A única referência a planejamento estratégico institucional existente na IN 04/2010 está em seu artigo quarto, transcrito integralmente a seguir:

> Art. 4º As contratações de que trata esta Instrução Normativa deverão ser precedidas de planejamento, elaborado em harmonia com o PDTI, alinhado ao planejamento estratégico do órgão ou entidade.
>
> Parágrafo único. Inexistindo o planejamento estratégico formalmente documentado, será utilizado o documento existente no órgão ou entidade, a exemplo do Plano Plurianual ou instrumento equivalente, registrando no PDTI a ausência do planejamento estratégico do órgão ou entidade e indicando os documentos utilizados. (IN SLTI/MPOG nº 04, 2010, grifo nosso).

[13] Secretaria de Logística e Tecnologia da Informação.

2.2.1 Planejamento estratégico de TI e plano diretor de TI

Antes de falar sobre o planejamento estratégico da TI, faz-se necessário conhecer, de maneira mais precisa, a própria definição do que é TI. Esta sigla para a tecnologia da informação, segundo a ótima definição da ISO 38500, compreende "os recursos necessários para adquirir, processar, armazenar e disseminar informações". Ainda segundo a norma, este termo também inclui "tecnologia da comunicação – TC" e o termo composto "tecnologia da informação e comunicação – TIC".

De fato, o conceito de tecnologia da informação é bastante amplo, abrangendo, conforme bem resumiu Souza (2008), além de aspectos eminentemente tecnicistas – e.g., *software* (sistemas de informação, programas aplicativos, códigos-fonte, bases de dados, etc.), *hardware* (processadores, dispositivos de memória, periféricos, etc.), redes de computadores e telecomunicações, etc. – outros aspectos de igual ou superior importância, como é o caso das pessoas envolvidas com as tecnologias, dos modelos de gestão e dos contextos organizacionais.

Em verdade, o que é mais importante no termo "tecnologia da informação" não é a palavra "tecnologia", mas, sim, a palavra "informação". As várias tecnologias atualmente existentes só foram criadas, desenvolvidas e aperfeiçoadas em virtude da necessidade de se entregar informação de qualidade às pessoas e organizações, independentemente da finalidade de seu uso.

Em virtude da crescente importância da tecnologia da informação, nas últimas décadas, para o desenvolvimento, prosperidade e sobrevivência das organizações, tornou-se cada vez mais relevante mensurar o retorno sobre o investimento[14] em TI. Como bem afirmaram Henderson e Venkatraman (1993, apud Souza, 2008), a dificuldade das organizações em obter retornos significativos do que é investido em TI se deve, em grande medida, ao não alinhamento entre esta e as estratégias do negócio.

Vê-se então surgir a necessidade de se definir mais um termo, o "alinhamento estratégico". Luftman (2000, apud Souza, 2003) o conceituou como consistindo nas atividades executadas de forma coordenada pela direção da organização, tendo em vista o alcance de seus objetivos estratégicos por meio da coordenação de várias áreas funcionais da organização, tais como: tecnologia da informação, finanças, marketing, recursos humanos, etc.

[14] Do inglês, "*return on investment*" (ROI).

Segundo Henderson e Venkatraman (1993, apud Souza, 2008), o alinhamento estratégico da TI requer uma mudança substancial no pensamento gerencial sobre o papel da TI na organização, assim como um entendimento da estratégia de TI e de sua importância tanto no suporte como no direcionamento das decisões de estratégia de negócios. Na visão destes autores, compartilhada por Luftman, alcançar o alinhamento estratégico de TI é um processo evolucionário e dinâmico, sendo que este alinhamento se refere à aplicação da TI de forma adequada e no momento correto, em harmonia com as estratégias, objetivos e necessidades do negócio. Destarte, este alinhamento compreende, segundo Luftman: de um lado, que a TI deve estar em harmonia com os negócios e, de outro, que os negócios podem ou devem estar alinhados com a TI.

Descreve Souza (2008) que o assunto alinhamento estratégico de TI vem recebendo atenção da área acadêmica desde o final da década de 1970, tendo sido propostos vários modelos de alinhamento estratégico relativos à TI, baseados em conceitos e teorias diversas e complementares, como:

> [...] ajuste estratégico e integração funcional (HENDERSON e VENKATRAMAN, 1993), dimensão intelectual e social (REICH e BENBASAT, 1996), teoria evolucionária e de contingência (TEO e KING, 1997), teoria da gestão do conhecimento (KEARNS e SABHERWAL, 2006), etc. Alguns autores relacionaram o alinhamento estratégico de TI com o desempenho organizacional (CHAN et al., 1997) e a efetividade de TI (CHAN et al., 1997; KEARNS e SABHERWAL, 2006). Outros propuseram formas de se medir a evolução do alinhamento estratégico de TI (TEO e KING, 1997) e seu nível de maturidade (LUFTMAN, 2000).
> (SOUZA, 2008).

Nenhum dos modelos citados acima será discutido neste trabalho, pois isso configuraria um desvio do escopo estabelecido para o mesmo.

Com relação ao planejamento estratégico da tecnologia da informação, conhecido pela sigla PETI, foi este definido por Rezende (2003) como um processo dinâmico e interativo para estruturar estratégica, tática e operacionalmente as informações organizacionais, a TI – composta por todos seus recursos e sistemas de informação e do conhecimento – as pessoas envolvidas e a infraestrutura necessária para o atendimento da totalidade das decisões, ações e respectivos processos da organização.

Basicamente, é no PETI que se identificam quais serão os objetivos e respectivos recursos de TI necessários para suportar a consecução dos objetivos estratégicos de negócio[15] da organização, de modo a garantir o devido alinhamento entre aqueles primeiros e estes últimos.

[15] A palavra "negócio" deve ser entendida como referente ao conjunto de todas as atividades desempenhadas pela organização – em especial aquelas ditas finalísticas, as quais representam a essência de sua existência.

No objetivo de enriquecer e melhor detalhar a definição do plano estratégico de TI, transcreve-se abaixo a descrição do processo PO[16]1.4 do COBIT 4.1, cujo correspondente no COBIT 5 é o APO[17]02.05:

> Criar um plano estratégico que defina, em cooperação com as partes interessadas relevantes, como a TI contribuirá com os objetivos estratégicos da organização (metas) e quais os custos e riscos relacionados. Esse plano estratégico deve contemplar como a TI aplicará os programas de investimentos e como dará sustentação à entrega operacional de serviços. O plano deve definir como os objetivos serão atingidos e medidos e deve ser formalmente liberado para implementação pelas partes interessadas. O plano estratégico de TI deve contemplar o orçamento operacional e de investimento, as fontes de recursos financeiros, a estratégia de fornecimento, a estratégia de aquisição e requisitos legais e regulamentares. O plano estratégico deve ser suficientemente detalhado para possibilitar a definição dos planos táticos de TI. (COBIT 4.1 – PO1.4, 2007).

Muito se fala também do chamado plano diretor de tecnologia da informação (PDTI). Alguns o veem como sinônimo do PETI. Outros acreditam que o PDTI se situa mais nos níveis tático e/ou operacional, sendo um desdobramento da abordagem estratégica do PETI. Os que possuem essa segunda visão por certo poderiam enquadrar o PDTI na definição do COBIT 4.1, processo PO1.5, de um portfólio de planos táticos de TI:

> Criar um portfólio de planos táticos de TI derivados do plano estratégico de TI. Esses planos táticos devem descrever quais são as iniciativas de TI requeridas, quais os recursos necessários e como o uso de recursos e os benefícios alcançados serão monitorados e administrados. Os planos táticos devem ser suficientemente detalhados de forma a permitir o desenvolvimento de planos de projetos. Gerenciar ativamente o conjunto de planos e iniciativas táticas de TI através de análise do portfólio de projetos e serviços. Isso contempla o acompanhamento frequente de requisitos e recursos, comparando-os ao alcance de metas estratégicas e táticas e os benefícios esperados, e tomando-se as ações apropriadas em caso de desvios. (COBIT 4.1 – PO1.5, 2007).

Algumas organizações possuem apenas uma única documentação, referente ao PETI ou ao PDTI. Outras possuem as duas documentações, de modo distinto. Outras tantas preferem considerar o PDTI no interior da documentação do PETI, ou seja, possuem uma única documentação conjunta para as duas abordagens. Entretanto, independentemente da forma como se realiza o planejamento dos objetivos, iniciativas, projetos e ações de TI e de qual nome é dado a este plano, o mais importante e essencial é a sua existência na organização. Além disso, o plano deve existir não apenas no campo formal, mas, sim, consistir em elemento de fundamental importância para o bom funcionamento da organização, sendo constantemente revisitado e atualizado, de acordo com as alterações do contexto onde esta se insere.

---

[16] Do inglês, "*Plan and Organize*".
[17] Do inglês, "*Align, Plan and Organize*".

Por fim, cumpre registrar que, segundo o artigo 2º, inciso XXII da IN 04/2010, o PDTI é o "instrumento de diagnóstico, planejamento e gestão dos recursos e processos de tecnologia da informação que visa atender às necessidades tecnológicas e de informação de um órgão ou entidade para um determinado período". Outrossim, de acordo com o artigo 4º desta mesma instrução normativa, o PDTI deve estar alinhado ao planejamento estratégico do órgão ou entidade ou, no caso da inexistência deste último, ao documento de planejamento disponível, a exemplo da Lei Orçamentária Anual (LOA), da Lei de Diretrizes Orçamentárias (LDO), do Programa Plurianual (PPA) ou de algum outro instrumento equivalente.

2.3 GESTÃO DE RISCOS

O padrão de gestão de riscos australiano-neozelandês AS/NZS 4360 (1999) definiu risco como "a possibilidade de algo acontecer e ter impacto nos objetivos, sendo medido em termos de consequências e probabilidades". Esta definição também foi adotada pelo TCU em sua Instrução Normativa nº 63/2010, a qual estabelece normas de organização e de apresentação dos relatórios de gestão e demais peças complementares dos processos de contas da APF.

O IFAC (2001), por sua vez, define risco como uma "medida de incerteza que engloba fatores que podem facilitar ou impedir a realização dos objetivos organizacionais". O IIA, em seu IPPF (2009), define risco como "a possibilidade de ocorrer um evento que venha a ter impacto no cumprimento dos objetivos, sendo medido em termos de impacto e de probabilidade".

A norma internacional ISO 31000, relativa à "gestão de riscos – princípios e diretrizes", define risco simplesmente como o "efeito da incerteza nos objetivos".[18] Esta sucinta definição é complementada por meio de cinco notas:

1. Um efeito é um desvio do esperado, positivo e/ou negativo.
2. Objetivos podem se referir a diferentes aspectos (e.g., aspecto financeiro, saúde e segurança, meio ambiente, etc.) e podem ser aplicados em diferentes níveis (nível estratégico, extensão da organização, projeto, produto e processo).
3. O risco é normalmente caracterizado pela referência a eventos potenciais e consequências, ou a uma combinação destes.

[18] O autor do trabalho teve acesso apenas ao documento original na língua inglesa (e não ao documento traduzido para a língua portuguesa, da ABNT).

4. O risco é normalmente expresso em termos da combinação das consequências de um evento (incluindo alterações nas circunstâncias) e sua probabilidade de ocorrência associada.
5. Incerteza é o estado, ainda que parcial, de deficiência da informação relacionada ao entendimento ou conhecimento de um evento, à sua consequência ou à sua probabilidade.

É importante notar que todas as conceituações apresentadas expressam, muito claramente, que, para se ter conhecimento dos riscos de uma organização, deve-se primeiro conhecer seus objetivos. Deste modo, fica difícil ou mesmo impossível falar de gestão de riscos em uma organização se essa sequer identificou quais são seus objetivos, o que ressalta mais uma vez a importância do planejamento estratégico e da governança corporativa e demonstra a integração de todos estes elementos.

Uma vez entendido o conceito de risco, faz-se necessário conhecer também o que vem a ser a gestão de riscos, também chamada de gerenciamento de riscos, a depender de qual a tradução adotada para o termo em inglês "*risk management*". A Associação Brasileira de Normas Técnicas – ABNT, ao traduzir a ISO 31000 para o português, optou pelo termo "gestão", enquanto o IIA Brasil, ao traduzir o IPPF do IIA Global, preferiu adotar o termo "gerenciamento". A seguir transcreve-se a definição de gestão (ou gerenciamento) de riscos tanto da ISO 31000 quanto do IPPF:

- Gestão de riscos: conjunto de atividades coordenadas para direcionar e controlar uma organização no que diz respeito aos seus riscos. (ISO 31000, tradução nossa).
- Gerenciamento de riscos: processo para identificar, avaliar, administrar e controlar potenciais eventos ou situações, para fornecer uma razoável certeza em relação ao cumprimento dos objetivos da organização. (IPPF, tradução do IIA Brasil).

Vale lembrar também a definição dada pelo *Comittee of Sponsoring Organisations* (COSO) para o gerenciamento de riscos corporativos, traduzida livremente da original em inglês:

> [...] é o processo – efetuado pela direção da entidade e aplicado no estabelecimento das estratégias – formulado para identificar, por toda a organização, eventos potencialmente capazes de afetá-la, bem como para administrar os riscos de modo a mantê-los compatível com o apetite a risco da organização, com vistas ao provimento de garantia razoável acerca do cumprimento de seus objetivos. (COSO *Enterprise Risk Management*, 2004, tradução nossa).

Nessa mesma linha de raciocínio, faz-se importante conhecer a definição da ISO 31000 para um *framework* de gestão de riscos, qual seja, o conjunto de componentes que

provê as fundações e arranjos organizacionais para o desenho, implementação, monitoramento, revisão e aprimoramento contínuo da gestão de riscos da organização. A seguir relacionamos as notas explicativas da norma para esta definição:

1. As fundações incluem a política, objetivos, mandato e comprometimento para gerenciar riscos.
2. Os arranjos organizacionais incluem planos, relacionamentos, responsabilidades, recursos, processos e atividades.
3. O *framework* de gestão de riscos deve estar embutido na totalidade das políticas e práticas estratégicas e operacionais da organização.

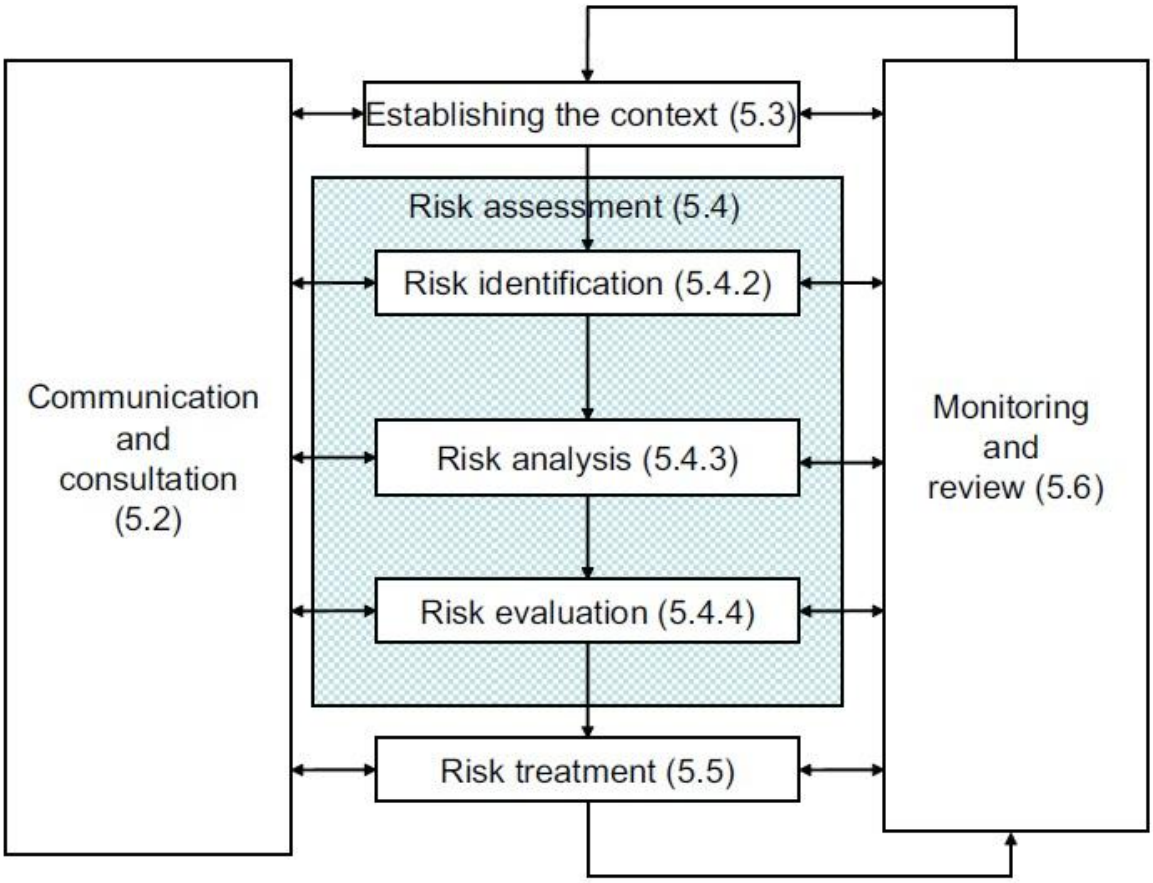
Na visão da ISO 31000, cada organização deveria desenvolver seu próprio *framework* de gestão de riscos a partir da avaliação de suas necessidades, objetivos, contexto, estrutura, operações, processos, funções, projetos, serviços e práticas, tendo por base os princípios e diretrizes trazidos pela norma, a qual não pretende promover uniformidade, mas, sim, por meio de uma abordagem genérica, prover orientação às organizações na implementação de seu processo de gestão de riscos, de modo transparente, confiável e adaptável a qualquer escopo e contexto.

A seguir são relacionados os princípios da ISO 31000 com os quais a gestão de riscos da organização deveria estar em conformidade para ser, de fato, efetiva. A gestão de riscos deve, então:

a) Criar e proteger valor.
b) Ser parte integral de todos os processos da organização.
c) Ser parte da tomada de decisão.
d) Tratar explicitamente a incerteza.
e) Ser sistemática, estruturada e oportuna.
f) Estar alinhada com o contexto interno e externo da organização e com seu perfil de risco.
g) Levar em conta fatores humanos e culturais.
h) Ser transparente e inclusiva.
i) Ser dinâmica, interativa e responsiva a mudanças.
j) Promover a melhoria contínua da organização.

Na figura seguinte é apresentado o processo de gerenciamento de riscos segundo a ISO 31000, cujo modelo é basicamente o mesmo da AS/NZS 4360:

Figura 2 – Visão do processo de gerenciamento de riscos



Fonte: ISO 31000:2009

Vê-se então que o processo de gerenciamento de riscos da norma ISO 31000 inicia-se com a etapa de estabelecimento de contexto, na qual são mapeados os contextos externo e interno da organização, é estabelecido o contexto do processo, bem como se definem os critérios de avaliação da significância dos riscos, os quais devem refletir os objetivos, valores e recursos da organização.

A seguir, vem a etapa de avaliação dos riscos (do inglês, "*assessment*"[19]), a qual é composta pelas subetapas de identificação, análise e avaliação (do inglês, "*evaluation*"[20]) dos riscos.

Na subetapa de identificação dos riscos, procuram-se respostas às seguintes questões: "o que pode acontecer?", "quando e onde?" e "como e por quê?". Na subetapa de análise dos riscos, identificam-se os controles existentes, determinam-se as consequências e probabilidades dos riscos e estima-se o nível de cada risco, de modo coerente aos critérios

[19] A palavra da língua inglesa "*assessment*" não possui tradução direta para a língua portuguesa. Refere-se a uma avaliação ampla, focada na obtenção de melhorias.
[20] "*Evaluation*" se refere a uma avaliação mais estrita dos riscos, focada na comparação com critérios pré-definidos.

anteriormente definidos para avaliação dos riscos. A análise dos riscos pode ser realizada em variados graus de detalhamento (a depender do risco, do propósito da análise e da informação e recursos disponíveis), podendo ser qualitativa, semiquantitativa ou quantitativa, ou mesmo uma combinação destes tipos. Na última subetapa, a de avaliação dos riscos, cada risco é comparado com os critérios definidos na etapa de estabelecimento de contexto, as prioridades são definidas e os riscos são submetidos ou não a tratamento, em conformidade aos critérios de aceitação destes.

Por fim, na etapa de tratamento dos riscos, as opções disponíveis são identificadas e avaliadas, o plano de tratamento é preparado e executado e o risco residual[21] é analisado e avaliado. Algumas possíveis opções para o tratamento dos riscos são:

a) Evitar o risco por meio da supressão da atividade que o ensejou.
b) Aproveitar ou aumentar o risco, quando este se tratar de uma oportunidade.
c) Remover a fonte de risco.
d) Alterar a probabilidade do risco.
e) Alterar as consequências.
f) Compartilhar o risco com terceiros (e.g., contrato com seguradora).
g) Reter o risco por meio de decisão informada.

Quanto à comunicação e consulta das partes interessadas, esta deve ocorrer durante todos os estágios do processo de gerenciamento de riscos. Como as distintas percepções dos *stakeholders* podem ter um significativo impacto nas decisões tomadas, estas devem ser identificadas, anotadas e levadas em consideração no processo de tomada de decisão.

Tendo em vista a completude e o fechamento do ciclo, deve-se realizar um monitoramento contínuo e uma revisão periódica ou *ad hoc* do processo de gerenciamento de riscos, no objetivo de: i) assegurar a efetividade e eficiência dos controles estabelecidos; ii) obter informação adicional com vistas ao aprimoramento da avaliação dos riscos; iii) analisar as lições aprendidas na execução do processo; iv) detectar alterações nos contextos interno e externo, aí incluídas as alterações nos critérios dos riscos, bem como na própria natureza destes, as quais podem demandar revisões nas priorizações e no plano de tratamento; e v) identificar riscos emergentes.

[21] Riscos residuais são os riscos que permanecem após a resposta da administração da organização aos riscos inerentes. Riscos inerentes são os referentes à probabilidade (e impacto associado) natural de ocorrência de determinados eventos, ou seja, são os riscos enfrentados pela organização antes da implementação de qualquer medida/controle.

Cumpre ainda registrar que, de acordo com a ISO 31000, os atributos de uma gestão de riscos aprimorada são: i) melhoria contínua; ii) total responsabilização pelos riscos; iii) aplicação do processo de gerenciamento de riscos em toda tomada de decisão; iv) comunicação contínua; e v) total integração com a estrutura de governança da organização.

Finaliza-se a exposição sobre este assunto com a citação de uma conclusão do IFAC de extrema relevância para a gestão de riscos na Administração Pública Federal brasileira, qual seja: "os dirigentes de entidades do setor público precisam assegurar que sistemas efetivos de gerenciamento de riscos fazem parte de sua estrutura de controle".

2.4 CONTROLES INTERNOS

Após a apresentação das definições de governança, planejamento estratégico e gestão de riscos, faz-se necessário trazer à baila a definição de controles internos. Tal assertiva justifica-se pela existência de um encadeamento lógico e uma integração muito forte entre todos estes conceitos, que será demonstrada a seguir.

Por meio do planejamento estratégico da organização, elaborado num contexto de atuação de sua estrutura de governança corporativa, são determinados os objetivos de sua administração, estreitamente relacionados ao seu conceito particular de geração de valor.

O risco, conforme já visto, é o efeito da incerteza nos objetivos, referindo-se à ocorrência de qualquer evento que possa ter impacto na consecução destes.

Tendo em vista a noção geral de que controle é, basicamente, uma ação tomada com o propósito de certificar-se de que algo se cumpra em acordo ao planejado, torna-se perfeitamente lógico dizer que controle só tem significado e relevância quando concebido para garantir o cumprimento de um objetivo definido e só faz sentido se houver riscos de que esse objetivo não venha a ser alcançado.[22]

Na definição do COSO (1992), traduzida livremente, controle interno é um processo – efetuado pela direção, gerência e demais pessoas da organização – criado para prover razoável garantia acerca do atingimento de objetivos nas seguintes categorias:

- Efetividade e eficiência das operações.
- Confiabilidade dos relatórios financeiros.
- Conformidade com as leis e regulamentos aplicáveis.

Ainda segundo o COSO, tal definição reflete alguns conceitos fundamentais:

[22] Argumentação adaptada de material do TCU (2009).

- Controle interno é um processo. É um meio para um fim, não um fim em si mesmo.
- Controle interno é efetuado por pessoas. Não se refere meramente a formulários e manuais de diretrizes e políticas, mas, sim, às pessoas em todos os níveis da organização.
- Do controle interno só se pode esperar o provimento de garantia razoável, e não total, para a direção da organização.
- Controle interno é focado no atingimento de objetivos em uma ou mais categorias separadas, porém sobrepostas.

Em razão de sua grande relevância, transcreve-se a seguir o detalhamento da explicação do COSO sobre a conceituação de controle interno como um processo:

> Controle interno não é um evento ou circunstância, mas uma série de ações que permeia as atividades de uma organização. Estas ações são penetrantes e inerentes ao modo como a gerência executa o negócio.
>
> Os processos de negócio, conduzidos por todas as unidades ou funções da organização, são gerenciados por meio dos tradicionais processos de planejamento, execução e monitoramento. O controle interno é parte desses processos e está integrado aos mesmos, habilitando seu funcionamento e monitorando sua condução e relevância contínua. É uma ferramenta utilizada pela gestão, não um substituto desta.
>
> Esta conceituação de controle interno é muito diferente da perspectiva de alguns observadores que veem o controle interno como algo adicionado às atividades da organização, ou como uma carga necessária, imposta por reguladores ou pelos ditames de burocratas superzelosos. O sistema de controle interno está entrelaçado com as atividades operacionais da organização e existe por razões fundamentais do negócio. Os controles internos são mais efetivos quando estabelecidos no interior da estrutura organizacional e vistos como parte essencial da corporação. Eles devem ser "estabelecidos no interior" (do inglês, "*built in*") em vez de "estabelecidos sobre" (do inglês, "*built on*"). (COSO, 1992, tradução nossa).

Alerta o COSO que a consecução dos objetivos institucionais classificados na categoria de operações (relativos ao uso eficiente e efetivo dos recursos da entidade) não está sempre sobre o controle da organização. O controle interno não pode prever más decisões ou julgamentos equivocados, nem mesmo a ocorrência de eventos externos que possam comprometer o atingimento das metas do negócio. Para esta categoria de objetivos, o sistema de controle interno pode apenas prover garantia razoável de que a direção da organização, em seu papel supervisor, seja informada, de maneira oportuna, da amplitude na qual a entidade está se movendo na direção do alcance destes objetivos.

Na abordagem do COSO, o controle interno consiste de cinco componentes inter-relacionados: ambiente de controle, avaliação (gestão) dos riscos, atividades de controle, informação e comunicação e monitoramento. Tal inter-relação é sucintamente explicada a seguir:

> O ambiente de controle provê uma atmosfera na qual as pessoas conduzem suas atividades e desempenham suas responsabilidades de controle. Ele serve como fundação para os outros componentes. Dentro deste ambiente, a direção avalia os riscos relacionados ao atingimento de objetivos específicos. As atividades de controle são implementadas com vistas a assegurar que as diretrizes da direção relativas ao tratamento dos riscos são executadas. Entrementes, informação relevante é capturada e comunicada por toda a organização. Todo o processo é monitorado e revisado em acordo às condições impostas. (COSO, 1992, tradução nossa, grifo do autor).

Em 2004 houve o lançamento do COSO ERM (de "*Enterprise Risk Management*"), também conhecido por COSO II, o qual foi traduzido em 2007 para a língua portuguesa. Este novo *framework*, segundo seu próprio prefácio, ampliou seu alcance em controles internos, oferecendo um enfoque mais vigoroso e extensivo no tema mais abrangente de gerenciamento de riscos corporativos, em virtude da crescente importância dada a este assunto desde o lançamento do primeiro *framework* do COSO, período este que foi marcado por uma série de escândalos financeiros e quebras de negócios de grande repercussão. Tal fato corrobora a assertiva inicial deste tópico acerca da intrínseca e indissociável relação da estrutura de controles internos com a gestão dos riscos do negócio da organização.

Os objetivos organizacionais, anteriormente classificados em 3 categorias, passaram a ser classificados em 4:

- Estratégicos: metas gerais (de alto nível), alinhadas e dando suporte à missão da organização.
- Operações: utilização eficaz e eficiente dos recursos.
- Comunicação: confiabilidade de relatórios.
- Conformidade: cumprimento de leis e regulamentos aplicáveis.

Percebe-se, nesta nova classificação, que o aspecto financeiro dos objetivos perdeu importância, deixando de ser explicitamente mencionado na descrição das categorias. Por outro lado, o aspecto estratégico dos objetivos da administração, que entrou em evidência nos anos seguintes à publicação do BSC em 1992, passou a compor uma nova categoria.

A estrutura de gerenciamento de riscos corporativos do COSO ERM é constituída por 8 componentes inter-relacionados, quais sejam:

- Ambiente interno: compreende o tom de uma organização e fornece a base pela qual os riscos são identificados e abordados pelo seu pessoal, inclusive a filosofia de gerenciamento de riscos, o apetite a risco, a integridade e os valores éticos, além do próprio ambiente onde estes operam.
- Fixação de objetivos: os objetivos devem existir antes que a administração possa identificar os eventos em potencial que poderão afetar a sua realização. O

gerenciamento de riscos corporativos assegura que a administração disponha de um processo implementado para estabelecer os objetivos que propiciem suporte e estejam alinhados com a missão da organização e sejam compatíveis com o seu apetite a riscos.

- Identificação de eventos: os eventos internos e externos que influenciam o cumprimento dos objetivos de uma organização devem ser identificados e distinguidos entre riscos e oportunidades.
- Avaliação de riscos: os riscos são analisados, considerando-se a sua probabilidade e o impacto como base para determinar o modo pelo qual deverão ser administrados.
- Resposta a riscos: a administração escolhe as respostas aos riscos – evitando, aceitando, reduzindo ou compartilhando – desenvolvendo uma série de medidas para alinhar os riscos com a tolerância e com o apetite a risco da organização.
- Atividades de controle: políticas e procedimentos são estabelecidos e implementados para assegurar que as respostas aos riscos sejam executadas de modo efetivo.
- Informações e comunicações: as informações relevantes são identificadas, colhidas e comunicadas, de forma e no prazo que permitam às pessoas o cumprimento de suas responsabilidades. A comunicação efetiva também ocorre em um sentido mais amplo, fluindo em todos os níveis da organização.
- Monitoramento: todo o processo de gerenciamento de riscos corporativos é monitorado e revisado quando necessário. O monitoramento é realizado por meio de atividades gerenciais contínuas, avaliações independentes, ou ambos.

A definição da INTOSAI[23] (2007), em seu documento "Diretrizes para as Normas de Controle Interno do Setor Público", para controle interno é quase a mesma estabelecida pelo COSO:

> Controle interno é um processo integrado efetuado pela direção e corpo de funcionários, e é estruturado para enfrentar os riscos e fornecer razoável segurança de que na consecução da missão da entidade os seguintes objetivos gerais serão alcançados:
>
> - execução ordenada, ética, econômica, eficiente e eficaz das operações;
> - cumprimento das obrigações de *accountability*;
> - cumprimento das leis e regulamentos aplicáveis;
> - salvaguarda dos recursos para evitar perdas, mau uso e dano.
>
> (INTOSAI, 2007, grifo nosso).

[23] Do inglês, "*International Organisation of Supreme Audit Institutions*".

Com relação à expressão “segurança razoável”, evidencia-se que esta reconhece que o custo do controle interno não deve exceder os benefícios que dele derivam. O recomendável é que o administrador só implemente determinado controle se considerar que os resultados esperados com a implementação deste superam o seu custo. Tal análise não se restringe ao aspecto financeiro, podendo envolver questões de imagem da organização, valores éticos, dentre outros.

Quanto às categorias de objetivos gerais da INTOSAI, percebe-se que as denominações mais distintas das do COSO são as relativas a *accountability* e salvaguarda de recursos. Uma explicação mais detalhada destas, na visão deste organismo, é apresentada a seguir:

> *Accountability* é o processo através do qual as organizações públicas e os indivíduos que as integram tornam-se responsáveis por suas decisões e ações, incluindo a salvaguarda de recursos públicos, a imparcialidade e todos os aspectos de seu desempenho.
>
> O processo será alcançado mediante o desenvolvimento, manutenção e disponibilização de informações financeiras e não financeiras confiantes e relevantes, e através da apresentação correta dessa informação em relatórios oportunos, destinados tanto ao público interno quanto ao público externo.
>
> [...]
>
> Ainda que o quarto objetivo possa ser visto como uma subcategoria do primeiro (operações ordenadas, éticas, econômicas, eficientes e eficazes), a importância da salvaguarda dos recursos no setor público precisa ser fortalecida. Isso se deve ao fato de que os recursos no setor público geralmente envolvem dinheiro público e sua utilização visa ao interesse coletivo, requerendo, desse modo, cuidado especial. Além disso, a contabilização do orçamento com base na execução financeira, prática que continua sendo muito comum no setor público, não oferece segurança suficiente com relação à aquisição, utilização e disponibilização dos recursos. Como resultado, as organizações no setor público nem sempre têm registros adequados de seus ativos, o que as torna mais vulneráveis. Por isso, devem-se adotar controles internos em cada uma das atividades relacionadas com a administração dos recursos da entidade, desde a aquisição até a sua disponibilização. (INTOSAI, 2007).

Destaca ainda a INTOSAI que:

> “o controle interno nas organizações do setor público deve ser entendido dentro do contexto das características específicas dessas organizações, ou seja, seu enfoque para alcançar os objetivos sociais ou políticos; a utilização dos recursos públicos; a importância do ciclo orçamentário; a complexidade de seu desempenho (a demanda pelo equilíbrio entre os valores tradicionais de legalidade, moralidade e transparência, e os modernos valores gerenciais como eficiência e eficácia) e o amplo escopo decorrente da sua *accountability* pública”. (INTOSAI, 2007).

Em seu “Guia de contratações de soluções de TI”, ressalta o TCU (2012) que:

> [...] com base em uma análise de risco que tenha como fundamento a missão e os objetivos do órgão, os gestores públicos podem estabelecer controles internos para os processos de trabalho, de forma a diminuir a probabilidade ou efeito dos riscos identificados. Portanto, a definição de quais controles internos são mais relevantes para um determinado órgão em um dado momento depende do contexto do órgão naquele momento. (TCU, 2012).

Em se tratando da norma ISO 31000, a definição dada para controle é que este consiste na "medida que está modificando o risco". Explica ainda a norma, por meio de nota, que os controles incluem qualquer processo, política, dispositivo, prática ou outras ações que modificam o risco. Além disso, os controles podem não exercer sempre o efeito modificador esperado ou assumido.

Por último, importa evidenciar a informação trazida por Antunes (1998, apud TCU, 2009) de que o Instituto Americano de Auditores Independentes (*American Institute of Certified Public Accountants* – AICPA), na edição da norma de auditoria SAS[24] 55 – Consideração da Estrutura de Controle Interno nas Auditorias de Demonstrações Financeiras, de 1998, introduziu a substituição da terminologia "sistema de controle interno" por "estrutura de controle interno". Segundo o autor, a nova terminologia amplia o seu conteúdo, porque como "estrutura", a SAS 55 incorpora o ambiente de controle, o sistema de contabilidade e os procedimentos de controle, além de introduzir o conceito de risco de controle. Apesar disto, assinala o TCU que "a literatura técnica sobre o assunto continua a utilizar fartamente a expressão sistema de controle(s) interno(s) ou simplesmente controle(s) interno(s) para se referir à estrutura de controle interno ou ao controle interno aplicado a uma organização".

2.4.1 Controles de TI

De acordo com o IIA (2012), os controles de TI possuem dois elementos significativos: a automação dos controles de negócio, que suportam a gestão e a governança, e o controle do ambiente de TI e das operações, que suportam as aplicações de TI e a infraestrutura.

Para o TOGAF[25] (2009), aplicação é um sistema informatizado que suporta funções e serviços do negócio. As aplicações utilizam os dados do negócio e são suportadas por múltiplos componentes tecnológicos que compõem a infraestrutura, sendo distintas destes.

Para a ISACA[26] (2009), os controles de aplicação são as políticas, procedimentos e atividades designadas para o provimento de garantia razoável de que os objetivos relevantes para uma dada solução automatizada (aplicação) serão atingidos.

A INTOSAI (2007), alinhada às definições do COSO, enuncia que os controles de aplicação são aqueles controles geralmente planejados para prevenir, detectar e corrigir erros e irregularidades enquanto a informação flui através dos sistemas aplicativos. Em outras

[24] Do ingles, "*Statement on Audit Standard*".
[25] Do inglês, "*The Open Group Architecture Framework*".
[26] Do inglês, "*Information Systems Audit and Control Association*".

palavras, são os controles designados ao provimento de garantia razoável acerca da completude e acurácia do processamento, autorização e validação das transações realizadas por uma aplicação.

No "GTAG 8 – *Auditing Application Controls*" (2007), o IIA apresenta uma definição mais detalhada dos objetivos dos controles de aplicação, ressalvando que estes controles pertencem ao escopo individual de processos de negócio ou aplicações, incluindo aí a edição de dados, a separação das funções do negócio, o balanceamento do processamento dos dados, o registro das transações e o relatório de erros. De acordo com o referido guia, os controles de aplicação objetivam assegurar que:

- Os dados de entrada são acurados, completos, autorizados e corretos.
- Os dados são processados de acordo com o planejado e num período de tempo aceitável.
- Os dados são armazenados adequadamente.
- As saídas são acuradas e completas.
- Os registros de entrada, processamento e saída de dados são mantidos.

Ainda de acordo com o GTAG 8, é muito importante a distinção entre controles de aplicação e controles gerais de TI (do inglês, ITGC – *Information Technology General Controls*). Estes últimos são aplicados a todos componentes tecnológicos, processos e dados presentes no ambiente organizacional, fornecendo a base sobre qual operam os sistemas aplicativos e de controle. O objetivo dos ITGCs é assegurar o desenvolvimento e implementação apropriados das aplicações, assim como a integridade dos arquivos de dados e programas e das operações de TI.

Na visão do IIA, os ITGCs incluem (sem se limitar) a governança de TI, a gestão de riscos, a gestão de recursos, as operações de TI, o desenvolvimento e manutenção de aplicações, a segurança lógica, a segurança física, o gerenciamento de mudanças, as políticas de *backup* e restauração de dados e a continuidade do negócio. Alguns controles gerais de TI são diretamente relacionados ao negócio, como é o caso da segregação de funções e dos arranjos de governança; outros são bastante técnicos, caso dos controles de sistemas e softwares de rede específicos, estando relacionados à infraestrutura tecnológica.

Para a ISACA, os controles de aplicação são dependentes da operação confiável da infraestrutura de TI sob a qual a aplicação se situa. Deficiências nos controles gerais de TI podem prejudicar a efetividade dos controles de aplicação, enquanto controles gerais de TI

efetivos podem prover oportunidade para o aumento da confiabilidade dos controles de aplicação.

Com relação a este assunto, conclui o COSO que os controles de aplicação e os controles gerais de TI se inter-relacionam, sendo ambos imprescindíveis ao provimento de garantia razoável acerca da acurácia e completude do processamento da informação gerida pela organização.

2.5 CONFORMIDADE (*COMPLIANCE*)

O termo "*compliance*", que em português pode ser traduzido como "conformidade", origina-se do verbo em inglês "*to comply*", que significa cumprir, executar, satisfazer, realizar o que lhe foi imposto. Segundo Coimbra e Manzi (2010, apud Porta, 2011), "*compliance* é o dever de cumprir, de estar em conformidade e fazer cumprir leis e diretrizes, regulamentos internos e externos, buscando mitigar o risco atrelado à reputação e o risco legal/regulatório".

Para a Associação Brasileira de Bancos Internacionais (ABBI) e a Federação Brasileira de Bancos (FEBRABAN,) a missão de *compliance* é:

> Assegurar, em conjunto com as demais áreas, a adequação, fortalecimento e o funcionamento do sistema de controles internos da instituição, procurando mitigar os riscos de acordo com a complexidade de seus negócios, bem como disseminar a cultura de controles para assegurar o cumprimento de leis e regulamentos existentes, além de atuar na orientação e conscientização à prevenção de atividades e condutas que possam ocasionar riscos à imagem da instituição. (ABBI e FEBRABAN, 2009).

Ainda segundo a ABBI e FEBRABAN:

> "Ser compliance" é conhecer as normas da organização, seguir os procedimentos recomendados, agir em conformidade e sentir quanto é fundamental a ética e a idoneidade em todas as nossas atitudes.
>
> "Estar em compliance" é estar em conformidade com leis e regulamentos internos e externos.
>
> "Ser e estar em compliance" é, acima de tudo, uma obrigação individual de cada colaborador dentro da instituição. (ABBI e FEBRABAN, 2009).

O *compliance* não se confunde com a auditoria interna, explicando Muzilli (2007, apud Porta, 2011) que enquanto esta consiste numa atividade independente que auxilia a organização a alcançar seus objetivos por meio da aplicação de uma abordagem sistemática e disciplinada para a avaliação e melhoria da eficácia dos processos de governança, gestão de riscos e controle, aquela é responsável pela disseminação, por toda a organização, do conceito e do dever de cumprir todos os normativos legais e regulamentares, externos e internos (dentre eles o código de ética/conduta), aos quais a organização está submetida.

Esclarecem a ABBI e FEBRABAN que:

> Enquanto a Auditoria Interna efetua seus trabalhos de forma aleatória e temporal, por meio de amostragens para certificar-se do cumprimento das normas e processos instituídos pela Alta Administração, o Compliance executa tais atividades de forma rotineira e permanente, monitorando-as para assegurar, de maneira corporativa e tempestiva, que as diversas unidades da instituição estejam respeitando as regras aplicáveis a cada negócio, ou seja, cumprindo as normas e processos internos para prevenção e controle dos riscos envolvidos em cada atividade. Compliance é um braço dos órgãos reguladores junto à administração no que se refere à preservação da boa imagem e reputação e às normas e controles na busca da conformidade.
>
> [...]
>
> Compliance faz parte da estrutura de controles, enquanto a auditoria avalia essa estrutura. Assim, a área de Compliance, como as demais, deve ser objeto de avaliação da auditoria interna.
>
> Sendo assim, podemos destacar que auditar compliance constitui oportunidade única para a compreensão de seu processo na instituição, isto é, para a avaliação da cultura de conformidade e do grau de comprometimento dos profissionais. (ABBI e FEBRABAN, 2009, grifo nosso).

É interessante notar a afirmação, no texto anteriormente citado, de que o *compliance* faz parte da estrutura de controles internos, o que guarda coerência com as definições do COSO e COSO ERM acerca da categoria de objetivos de controle relacionada à conformidade, constante de ambas as versões deste *framework*.

Neste ponto, cumpre também destacar a visão do TCU (2009) acerca da distinção entre os conceitos de controle interno e auditoria interna e o posicionamento destes no sistema de controle interno das organizações:

> A auditoria interna não implanta controles, mas a unidade de controle interno pode implantar; a auditoria interna faz trabalhos periódicos com metodologia específica, a unidade de controle interno atua no dia-a-dia, no monitoramento contínuo e na autoavaliação de controles internos; auditoria interna é uma atividade de avaliação independente, voltada para o exame e avaliação da adequação, eficiência e eficácia do sistema de controle interno, é parte desse sistema, mas não integra a estrutura de linha da organização e sim o seu *staff*; a unidade de controle interno também é parte do sistema de controle interno, mas é um elemento da gestão, faz parte da estrutura de linha da organização, com atribuições ligadas ao gerenciamento de riscos e controles. (TCU, 2009, grifo nosso).

Apesar do COSO ter uma visão mais abrangente do conceito de controle interno, vendo este como um processo a ser executado de ponta-a-ponta por todas as unidades estruturais da organização, bem como intermesclado à totalidade das atividades da gestão, várias organizações optam por possuir, dentro de sua estrutura, uma unidade específica para tratar de assuntos relacionados aos controles internos e ao *compliance*.

2.5.1 - GRC

Uma vez introduzido o conceito de conformidade (ou *compliance*), abre-se uma oportunidade para a apresentação de um novo acrônimo que tem sido posto em destaque nas organizações nos últimos anos (em especial, nas instituições financeiras e grandes

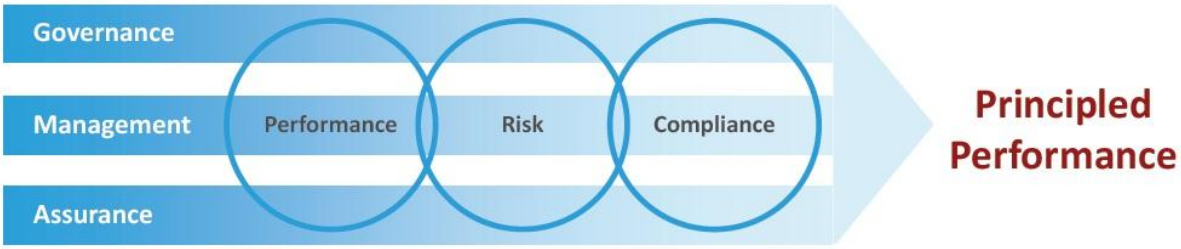
corporações da área de TI), qual seja: o GRC – Governança, Risco e Conformidade (do inglês, *Governance, Risk and Compliance*).

Segundo a ABBI e FEBRABAN, integrar as atividades de governança corporativa, gestão de riscos e conformidade significa entender as exigências das partes interessadas da instituição, em termos de desempenho e conformidade, e alinhá-las na entrega destes objetivos, em retribuição ao apetite e tolerância ao risco.

O OCEG[27] (2012), por sua vez, introduz o conceito de "desempenho orientado a princípios"[28], uma abordagem de negócio que auxilia as organizações a atingirem os objetivos enquanto lidam com a incerteza (tanto com o risco quanto com a recompensa) e a agirem com integridade (honrando os comprometimentos mandatórios e as promessas voluntárias).

O desempenho orientado a princípios, segundo o OCEG, é habilitado por meio da integração e orquestramento de áreas que, em muitas organizações, se encontram fragmentadas e isoladas – tais como governança, gestão de desempenho, gestão de riscos, controle interno, conformidade e auditoria. As atividades nessas áreas são, muitas vezes, gerenciadas em departamentos distintos com pouca ou nenhuma comunicação interfuncional, ou mesmo nem são gerenciadas, sendo mantidas intocadas. A visualização gráfica da integração destas áreas, compondo a abordagem de desempenho orientado a princípios, é dada pela figura a seguir:

Figura 3 – GRC e o desempenho orientado a princípios



Fonte: OCEG *Red Book GRC Capability Model version* 2.1, pág. 15.

Apesar de existirem várias funções que contribuem para o desempenho orientado a princípios, o acrônimo GRC é amplamente utilizado como uma referência sucinta desta coleção de atividades. Como demonstrado pela figura, o atingimento do desempenho orientado a princípios requer, segundo o OCEG, uma visão holística que aborde a governança, a gestão de riscos, a conformidade e a gestão de desempenho.

[27] Do inglês, "*Open Compliance and Ethics Group*"
[28] Do inglês, "*principled performance*".

De acordo com a ABBI e a FEBRABAN, a integração dessas atividades pode resultar em vários benefícios, dentre os quais pode-se citar:

- Melhor entendimento das obrigações que a organização possui para cumprir aquilo que reflete o seu apetite por risco e os seus objetivos de negócio.
- Organização, cultura, processos e tecnologia melhor focados e alinhados.
- Melhor alocação de recursos e eficiência nos processos e na tecnologia que apoia a integração desses conceitos de maneira eficiente em termos de custo.
- Melhor ambiente de controles internos e habilidade contínua da administração em demonstrar que a organização está no controle.
- Ligação entre conformidade e desempenho no estabelecimento do objetivo.
- Maior consciência e responsabilidade em relação aos elementos do GRC.
- Indicadores-chave de desempenho e considerações de riscos identificados e utilizados no auxílio à tomada de decisão.
- Mecanismos de mensuração e apresentação de relatórios desenvolvidos para reduzir o risco de surpresas em resultados operacionais e financeiros.
- Racionalização de processos, com vistas à eliminação de eventuais duplicidades, retrabalhos e atividades improdutivas, bem como oportunidades de automatização.

A estes se acrescentem outros dois benefícios importantes identificados pelo OCEG:

- Otimização do alinhamento dos objetivos de negócio com a missão, visão e valores da organização.
- Responsabilização de cima para baixo (do inglês, "*top to down accountability*") com relação aos objetivos-chave, riscos, requerimentos e iniciativas relacionadas.

2.6 O SISTEMA DE CONTROLE INTERNO DO PODER EXECUTIVO FEDERAL

A Administração Pública Federal é composta pela Administração Direta (órgãos, secretarias e outros) e Indireta (fundações, autarquias, empresas públicas e sociedades de economia mista) dos três poderes da União: Executivo, Legislativo e Judiciário.

Segundo o artigo 70 da Constituição Federal de 1988, a fiscalização contábil, financeira, orçamentária e patrimonial da União e das entidades da administração direta e indireta, quanto à legalidade, legitimidade, economicidade, aplicação das subvenções e renúncia de receitas é exercida pelo Congresso Nacional, mediante controle externo, e pelo sistema de controle interno de cada poder. O controle externo, a cargo do Congresso

Nacional, é exercido com o auxílio do Tribunal de Contas da União – TCU, segundo o artigo 71 da CF/88.

O artigo 74 da CF/88, por sua vez, disciplinou que cada Poder da União deveria manter, de forma integrada, sistema de controle interno com a finalidade de:

> I - avaliar o cumprimento das metas previstas no plano plurianual, a execução dos programas de governo e dos orçamentos da União;
> II - comprovar a legalidade e avaliar os resultados, quanto à eficácia e eficiência, da gestão orçamentária, financeira e patrimonial nos órgãos e entidades da administração federal, bem como da aplicação de recursos públicos por entidades de direito privado;
> III - exercer o controle das operações de crédito, avais e garantias, bem como dos direitos e haveres da União;
> IV - apoiar o controle externo no exercício de sua missão institucional.
> (CF/88, art. 74).

Em se tratando do Poder Executivo Federal, é à Controladoria-Geral da União – CGU, órgão integrante da estrutura da Presidência da República, que compete o papel de Órgão Central de Controle Interno, por meio de sua Secretaria Federal de Controle Interno (SFC). O rol completo de competências da CGU foi descrito pelo artigo 17 da Lei nº 10.683/2003, o qual se transcreve a seguir:

> Art. 17. À Controladoria-Geral da União compete assistir direta e imediatamente ao Presidente da República no desempenho de suas atribuições quanto aos assuntos e providências que, no âmbito do Poder Executivo, sejam atinentes à defesa do patrimônio público, ao controle interno, à auditoria pública, à correição, à prevenção e ao combate à corrupção, às atividades de ouvidoria e ao incremento da transparência da gestão no âmbito da administração pública federal.
> (Lei 10.683, 2003).

A descrição da organização e das competências do Sistema de Controle Interno do Poder Executivo Federal é dada pelos artigos 21 a 24 da Lei nº 10.180/2001:

> Art. 21. O Sistema de Controle Interno do Poder Executivo Federal compreende as atividades de avaliação do cumprimento das metas previstas no plano plurianual, da execução dos programas de governo e dos orçamentos da União e de avaliação da gestão dos administradores públicos federais, utilizando como instrumentos a auditoria e a fiscalização.
> Art. 22. Integram o Sistema de Controle Interno do Poder Executivo Federal:
> I - a Secretaria Federal de Controle Interno, como órgão central;
> II - órgãos setoriais.
> § 1º A área de atuação do órgão central do Sistema abrange todos os órgãos do Poder Executivo Federal, excetuados aqueles indicados no parágrafo seguinte.
> § 2º Os órgãos setoriais são aqueles de controle interno que integram a estrutura do Ministério das Relações Exteriores, do Ministério da Defesa, da Advocacia-Geral da União e da Casa Civil.
> § 3º O órgão de controle interno da Casa Civil tem como área de atuação todos os órgãos integrantes da Presidência da República e da Vice-Presidência da República, além de outros determinados em legislação específica.
> § 4º Os órgãos central e setoriais podem subdividir-se em unidades setoriais e regionais, como segmentos funcionais e espaciais, respectivamente.

> § 5º Os órgãos setoriais ficam sujeitos à orientação normativa e à supervisão técnica do órgão central do Sistema, sem prejuízo da subordinação ao órgão em cuja estrutura administrativa estiverem integrados.
>
> Art. 23. Fica instituída a Comissão de Coordenação de Controle Interno, órgão colegiado de coordenação do Sistema de Controle Interno do Poder Executivo Federal, com o objetivo de promover a integração e homogeneizar entendimentos dos respectivos órgãos e unidades.
>
> Art. 24. Compete aos órgãos e às unidades do Sistema de Controle Interno do Poder Executivo Federal:
>
> I - avaliar o cumprimento das metas estabelecidas no plano plurianual;
>
> II - fiscalizar e avaliar a execução dos programas de governo, inclusive ações descentralizadas realizadas à conta de recursos oriundos dos Orçamentos da União, quanto ao nível de execução das metas e objetivos estabelecidos e à qualidade do gerenciamento;
>
> III - avaliar a execução dos orçamentos da União;
>
> IV - exercer o controle das operações de crédito, avais, garantias, direitos e haveres da União;
>
> V - fornecer informações sobre a situação físico-financeira dos projetos e das atividades constantes dos orçamentos da União;
>
> VI - realizar auditoria sobre a gestão dos recursos públicos federais sob a responsabilidade de órgãos e entidades públicos e privados;
>
> VII - apurar os atos ou fatos inquinados de ilegais ou irregulares, praticados por agentes públicos ou privados, na utilização de recursos públicos federais e, quando for o caso, comunicar à unidade responsável pela contabilidade para as providências cabíveis;
>
> VIII - realizar auditorias nos sistemas contábil, financeiro, orçamentário, de pessoal e demais sistemas administrativos e operacionais;
>
> IX - avaliar o desempenho da auditoria interna das entidades da administração indireta federal;
>
> X - elaborar a Prestação de Contas Anual do Presidente da República a ser encaminhada ao Congresso Nacional, nos termos do art. 84, inciso XXIV, da Constituição Federal;
>
> XI - criar condições para o exercício do controle social sobre os programas contemplados com recursos oriundos dos orçamentos da União.
>
> (Lei 10.180, 2001).

Por fim, cumpre realçar a visão do TCU (2009) de que "a SFC constitui, por sua posição na estrutura organizacional do Governo Federal, auditoria interna em relação ao Poder Executivo, e externa em relação aos órgãos e entidades por ela auditados dentro desse mesmo poder".

2.7 AUDITORIA OPERACIONAL (OU DE DESEMPENHO)

De acordo com a INTOSAI (2001), o escopo total da auditoria governamental compreende as auditorias de regularidade (conformidade) e de desempenho (operacional), do inglês, "*regularity and performance audits*", respectivamente.

Na visão deste organismo internacional, a auditoria de conformidade abrangeria:

a) atestação da *accountability* financeira, envolvendo o exame, avaliação e emissão de opinião acerca de registros financeiros;

b) atestação da *accountability* financeira da administração governamental com um todo;
c) auditoria de sistemas e transações financeiras, incluindo uma análise da conformidade com estatutos e regulações aplicáveis;
d) auditoria do controle interno e das funções da auditoria interna;
e) auditoria da probidade e propriedade das decisões administrativas tomadas na entidade auditada;
f) outras matérias julgadas pertinentes pela Entidade Fiscalizadora Superior.

Por sua vez, a auditoria operacional, sendo concernente à auditoria da economicidade, eficiência e efetividade, abrangeria:

a) auditoria da economicidade das atividades administrativas, em acordo a sólidos princípios e práticas administrativas e políticas de gestão;
b) auditoria da eficiência da utilização de recursos humanos, financeiros e outros, incluindo o exame de sistemas de informação, medidas de desempenho e arranjos de monitoramento, bem como procedimentos seguidos pelas entidades auditadas com vistas ao saneamento das deficiências identificadas;
c) auditoria da efetividade do desempenho em relação ao atingimento dos objetivos da entidade auditada, bem como auditoria do impacto real das atividades, em comparação ao impacto pretendido.

Observa bem a INTOSAI que, na prática, pode haver sobreposição das auditorias de conformidade e de desempenho, sendo que, nestes casos, a classificação de uma auditoria em particular dependerá do propósito primário a ela estabelecido.

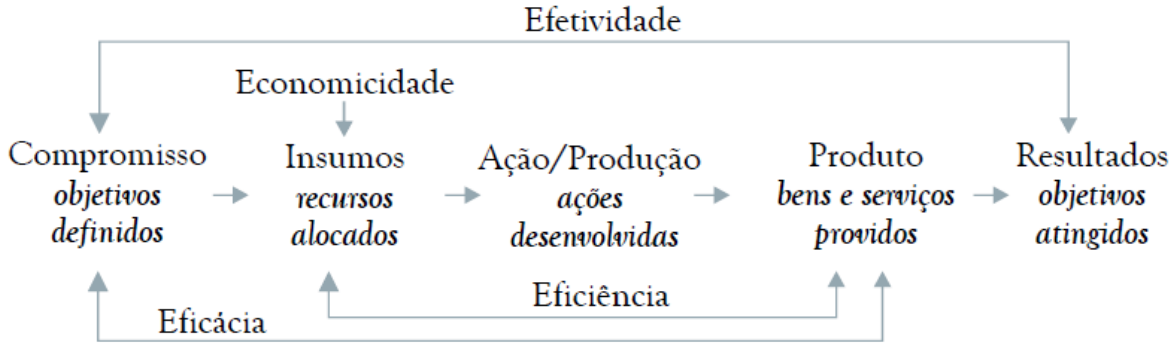
O inciso II do artigo 74 da Constituição Federal de 1988, ao enunciar acerca da finalidade dos sistemas de controle interno dos Poderes da União de "comprovar a legalidade e avaliar os resultados, quanto à eficácia e eficiência, da gestão orçamentária, financeira e patrimonial nos órgãos e entidades da administração federal", também estabelece claramente a distinção entre estes dois tipos básicos de auditoria governamental, sendo a comprovação da legalidade referente à auditoria de conformidade e a avaliação dos resultados da gestão, quanto à eficácia e eficiência, referente à auditoria de desempenho ou operacional. Do exposto, pode-se concluir que a CGU detém um mandato constitucional relativo à realização de auditorias tanto de conformidade quanto operacionais nos órgãos e entidades do Poder Executivo Federal.

O Tribunal de Contas da União, órgão de controle externo brasileiro, ao definir a auditoria operacional, baseou-se na conceituação trazida pela INTOSAI, fazendo-o do seguinte modo:

> Auditoria operacional é o exame independente e objetivo da economicidade, eficiência, eficácia e efetividade de organizações, programas e atividades governamentais, com a finalidade de promover o aperfeiçoamento da gestão pública. (TCU, 2010).

Segundo o TCU, as auditorias operacionais podem examinar, em um mesmo trabalho, uma ou mais das principais dimensões de análise. Tais dimensões e inter-relações são ilustradas pelo diagrama de insumo-produto a seguir:

Figura 4 – Diagrama de insumo-produto das auditorias operacionais



Fonte: Manual de Auditoria Operacional do TCU – 2010

De acordo com a INTOSAI, a auditoria operacional não é tão sujeita a requerimentos e expectativas específicas. Enquanto a auditoria de conformidade normalmente aplica padrões relativamente fixos, a auditoria operacional é mais flexível na escolha dos temas, objetos de auditoria, métodos e opiniões. A auditoria operacional não é uma auditoria regular com opiniões formalizadas nem possui suas raízes na auditoria privada. É, por natureza, de amplo espectro e aberta a julgamentos e interpretações. Ela precisa ter à sua disposição uma ampla seleção de métodos investigativos e avaliativos e operar a partir de uma base completamente distinta da relativa à auditoria tradicional, não sendo, portanto, uma auditoria baseada em *checklists*. Seu escopo pode ser relativo a um ciclo de vários anos, em vez de se limitar a um único exercício financeiro. O caráter especial da auditoria operacional se deve à variedade e complexidade das questões relacionadas ao seu trabalho.

Expostas as peculiaridades da auditoria operacional, conclui a INTOSAI que esta, dentro de seu mandato legal, deve ser livre para examinar todas as atividades governamentais a partir de diferentes perspectivas, observando, porém, que o caráter da auditoria operacional

não deve ser utilizado como argumento para solapar a colaboração entre os dois tipos de auditoria.

A título de enriquecimento do assunto, impende, por fim, destacar quais ideias, segundo a INTOSAI, formam a base da auditoria operacional, assim como quais são as questões básicas a serem respondidas.

Com relação às ideias-chave, estas podem ser resumidas como se segue:

- A *accountability* pública significa que os encarregados de um ministério ou programa governamental são responsáveis pela gestão eficiente e efetiva destes. A auditoria operacional é um meio pelo qual os cidadãos em geral executam controle e obtém conhecimento acerca da execução e do resultado das várias atividades do governo, respondendo a questões do tipo: "estamos alcançando valor por meio do dinheiro gasto ou é possível gastá-lo melhor ou mais sabiamente?". Um dos pressupostos da boa governança é que todos os serviços públicos prestados sejam sujeitos à auditoria.
- É importante que haja uma informação independente e confiável, prestada por auditores que representem o interesse público, que possam pensar e agir de modo independente, com vistas a mostrar e questionar a situação corrente.
- Os auditores devem possuir as competências necessárias para exercerem a habilidade de influenciar e promover melhorias no desempenho das atividades de governo. O aprendizado e conhecimento para mudanças deve ser incentivado, assim como a otimização das condições para tomada de decisão.

Já as questões básicas a serem respondidas são as seguintes:

- As coisas estão sendo feitas da maneira certa?
- As coisas certas estão sendo feitas?

A primeira questão procura conhecer se as decisões políticas são executadas de modo apropriado pelos administradores públicos, estando restrita aos aspectos de economicidade, eficiência e eficácia.

A segunda questão, por sua vez, procura conhecer se as políticas públicas adotadas foram apropriadamente definidas (com relação às necessidades da sociedade) ou se os meios corretos para atingirem certos objetivos foram empregados, referindo-se, portanto ao aspecto de efetividade. Neste ponto, lembra a INTOSAI que o auditor pode considerar uma medida escolhida não efetiva ou inconsistente com os objetivos declarados; entretanto, a partir do momento que o auditor começa a questionar se o compromisso público assumido é factível,

ele necessita ter cuidado para não ir além de seu mandato, ultrapassando temerariamente a fronteira do território das decisões políticas.

3. PROPOSTA

Neste item será apresentada uma proposta para o processo de seleção e planejamento de auditorias de TI em órgãos e entidades do Poder Executivo Federal, com base na avaliação integrada da governança, gestão de riscos e controles internos da unidade gestora a ser examinada.

Apesar de o foco das auditorias a serem selecionadas e planejadas se referir a uma avaliação de natureza predominantemente operacional, também poderão ser abordados aspectos relacionados à conformidade. De fato, é difícil falar em uma auditoria puramente operacional no setor público, haja vista que a necessidade de conformidade legal acaba-se entranhando por todos os assuntos, sendo incomparavelmente maior que a existente no setor privado, ressalvadas, provavelmente, as organizações pertencentes ao setor financeiro. A intersecção dos aspectos operacionais e de conformidade nas auditorias é facilmente identificável na seara dos controles internos, uma vez que a avaliação destes apresenta um caráter híbrido: por vezes, mais próximo da conformidade; por outras, mais sintonizado com o aspecto estratégico do cumprimento dos objetivos da organização.

Este processo se baseia na metodologia GAIT-R (acrônimo para a expressão em inglês "*Guide to the Assessment of IT for Business and Risk*"), do IIA (2008), cujo objetivo é a identificação de todos os controles-chave (do inglês, "*key controls*") que são críticos para o atingimento dos objetivos e metas do negócio. Tal metodologia foi devidamente adaptada para o contexto da Administração Pública Federal, em especial para o Poder Executivo, tendo sido mesclada com outros guias do próprio IIA, da série GTAG – *Global Technology Audit Guide*, e com o *framework* COBIT 5, da ISACA.

Antes de adentrar na descrição pormenorizada de cada passo do processo, faz-se necessário apresentar os princípios fundamentais sobre os quais este se assenta, quais sejam:

1) A falha de uma tecnologia só é um risco que necessita ser avaliado, gerenciado e auditado se representar um risco para o negócio.
2) Os controles-chave devem ser identificados como o resultado de uma avaliação *top-down* dos riscos de negócio, da tolerância aos riscos e dos controles – incluídos os controles manuais e automatizados (e híbridos), os controles de aplicação e os controles gerais de TI – requeridos para o tratamento destes.
3) Os riscos de negócio são mitigados pela combinação de controles manuais, automatizados e híbridos. A avaliação da estrutura de controle interno da

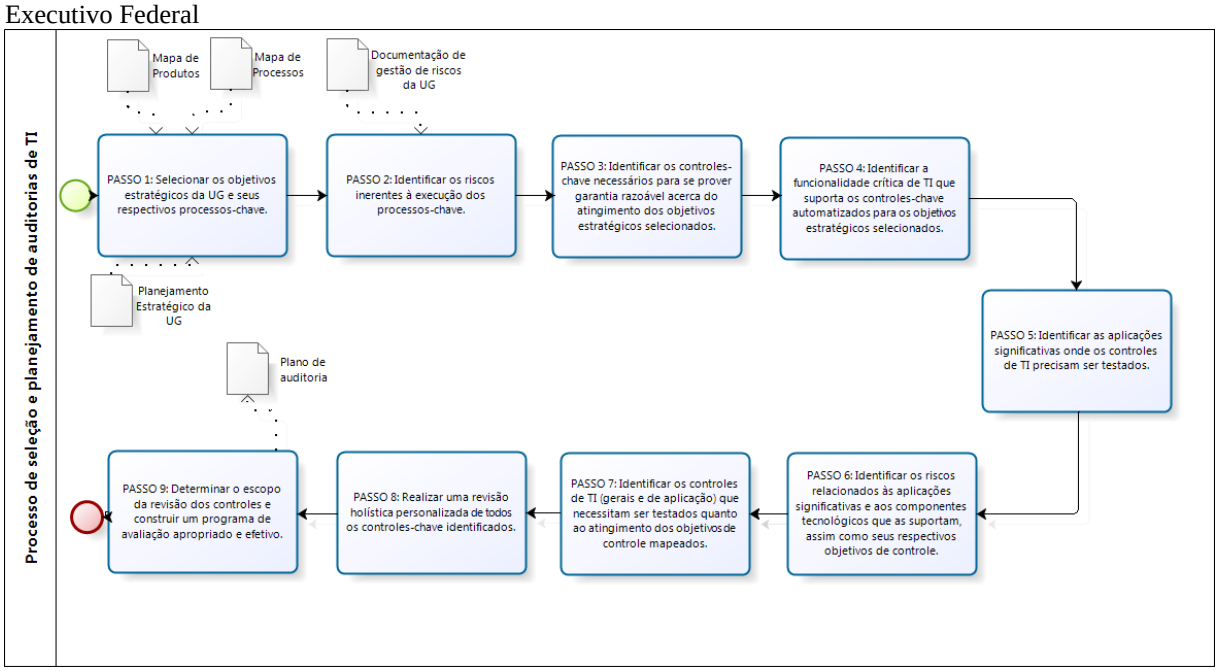
organização se dá por meio da revisão da totalidade de seus controles-chave, independentemente de sua natureza.

4) A operação apropriada e contínua dos controles-chave automatizados pode ser determinada a partir da avaliação dos controles de aplicação e dos controles gerais de TI.
    a. Os controles gerais de TI que necessitam ser identificados e avaliados são apenas aqueles capazes de afetar uma funcionalidade crítica de TI em aplicações significativas para o atingimento dos objetivos de negócio da organização.
    b. Os controles gerais de TI que necessitam ser identificados e avaliados existem em vários processos e camadas do ambiente tecnológico: bases de dados, sistemas operacionais, rede, hardware, etc.
    c. Os riscos nos controles de aplicação e nos controles gerais de TI são mitigados pelo atingimento de objetivos de controle (e não por meio de controles individuais). Isso significa que a definição dos objetivos de controle relevantes para o tratamento dos riscos de negócio identificados deve ser realizada antes da identificação dos controles-chave de TI (sejam estes de aplicação ou gerais). Os controles-chave de TI que devem ser incluídos no escopo da auditoria são apenas aqueles que atendem aos objetivos de controle.

3.1 PASSOS DO PROCESSO

Na figura a seguir é apresentada a visão integral do processo de seleção e planejamento de auditorias de TI para as unidades gestoras do Poder Executivo Federal. Cada um dos nove passos (ou etapas) do processo será descrito detalhadamente nos subtópicos que se seguem. O documento final entregue no último passo do processo é o plano de auditoria de TI para a(s) UG(s) analisada(s). Alguns documentos servem de insumo (entrada) nos passos iniciais do processo, como é o caso do plano estratégico institucional e de TI, dos mapas de produtos e processos e da documentação de gestão de riscos.

Figura 5 – Representação gráfica do processo de seleção e planejamento de auditorias de TI para UGs do Poder Executivo Federal



Fonte: Adaptado do IIA – *GAIT for Business and IT Risk* (2008).

3.1.1 Passo 1: Selecionar os objetivos estratégicos da UG e seus respectivos processos-chave.

De acordo com o primeiro princípio do processo, para que se defina um planejamento efetivo para uma auditoria de TI, é necessário que se tenha em mente que a tecnologia só existe para suportar e promover os objetivos da organização, assim como só representa um risco para esta se a sua falha resultar na incapacidade de se atingir um objetivo de negócio. Por esta razão, é importante entender primeiramente os objetivos da organização, suas estratégias, seu modelo de negócio e sua estrutura de governança, assim como o papel que a tecnologia desempenha neste contexto.

É necessário então que os auditores da equipe de planejamento identifiquem os produtos (bens ou serviços) entregues pela UG. Tal identificação pode ser iniciada por meio da leitura de instrumentos tais como: o PPA, a LDO, a LOA, relatórios de gestão da unidade de anos anteriores, documentação do planejamento estratégico institucional, regimento interno da unidade, relatórios anteriores de auditoria (da CGU, do TCU ou até mesmo da Auditoria Interna, caso a UG em questão se refira a uma entidade da Administração Indireta), dentre outros. Uma das técnicas de auditoria que pode ser empregada para se conhecer os produtos finalísticos entregues pela UG – diretamente à sociedade ou a outros órgãos – é a denominada "mapa de produtos", que é capaz de auxiliar o auditor na representação das relações de

dependência entre os produtos, bem como na identificação dos responsáveis pelos produtos críticos.

Neste ponto, é interessante observar que, em se tratando das unidades gestoras do Poder Executivo Federal, estas podem ser classificadas, quanto ao uso da TI, da seguinte maneira:

- O negócio da UG é a prestação de serviços de TI (e.g., SERPRO, DATASUS, DATAPREV, etc.).
- O negócio da UG não é a prestação de serviços de TI (a grande maioria dos órgãos e entidades da APF).
    - A UG possui área de TI própria (e.g., FUNASA, ANVISA, etc.).
    - A UG não possui área de TI própria, mas, sim, utiliza os serviços de TI entregues por outra UG (e.g., Secretaria de Atenção à Saúde – SAS, Secretaria Especial de Saúde Indígena – SESAI e demais secretarias do Ministério da Saúde, todas utilizando os serviços de TI prestados pelo DATASUS).

O processo de seleção e planejamento de auditorias de TI proposto neste trabalho pode ser aplicado para todos os três tipos de UGs acima. Entretanto, vale ressaltar que, para o último tipo apresentado (UGs cujo negócio não é TI e que dependem da prestação de serviços entregues por outras UGs), o escopo da avaliação dos controles de TI recairá sobre o âmbito de outra unidade, fato este que deverá ser analisado pela equipe de planejamento. Neste caso, pode-se realizar uma auditoria integrada para as UGs envolvidas (finalística e de TI) ou se optar pela realização de auditorias separadas, que serão, posteriormente, consolidadas em um mesmo relatório final.

Após se tornar familiar com os produtos e objetivos estratégicos da UG, o próximo passo da equipe de planejamento da auditoria se refere à identificação dos processos-chave que são críticos para o atingimento dos objetivos. Um processo somente é considerado “chave” se uma falha em sua execução impede a organização de atingir integralmente o objetivo estratégico ao qual este está vinculado. Neste momento, pode-se recorrer à técnica de auditoria denominada “mapa de processos”, que representa importante ferramenta de auxílio ao auditor no conhecimento do funcionamento dos processos de trabalho de uma organização. Após o mapeamento de todos os processos de trabalho da UG, deverão ser identificados aqueles que são “chave” para cada objetivo estratégico.

Uma vez identificados os produtos de ação de governo entregues pela UG, seus objetivos estratégicos de negócio e os respectivos processos-chave vinculados a estes, faz-se

necessário selecionar quais objetivos de negócio serão objeto de exame da(s) auditoria(s) em planejamento.

Definidos os objetivos de negócio da UG e os respectivos processos-chave associados a serem examinados, parte-se, então, para o próximo passo do processo de seleção e planejamento.

3.1.2 Passo 2: Identificar os riscos inerentes[29] à execução dos processos-chave.

Para cada processo-chave, devem-se identificar quais os riscos inerentes à sua execução, ou seja, quais são os eventos suscetíveis de ocorrerem que podem vir a comprometer os resultados (as saídas) do processo. Apesar de ter sido colocado em destaque, o passo 2 poderia ser visto em conjunto com o passo 3, em precedência às atividades arroladas neste. Caso a UG realize gestão de riscos, seja este processo estruturado ou não, é muito importante que a equipe de auditoria verifique quais riscos foram identificados pela unidade, pois é possível que os riscos inerentes aos processos-chave já tenham sido previamente mapeados, ao menos parcialmente. Tal verificação pode auxiliar ou até mesmo poupar os auditores da execução deste passo.

3.1.3 Passo 3: Identificar os controles-chave necessários para se prover garantia razoável acerca do atingimento dos objetivos estratégicos selecionados.

Neste passo, baseado no princípio 3, deve-se identificar os controles-chave necessários ao provimento de garantia razoável acerca do atingimento dos objetivos de negócio selecionados no passo 1. Os controles-chave são aqueles controles responsáveis por tratar os riscos inerentes à execução dos processos-chave, mapeados no passo 2.

Somente os controles-chave precisam ser avaliados, embora o auditor possa incluir outros controles não-chave (e.g., controles redundantes), caso entenda que há valor para o negócio na avaliação destes.

Ressalte-se que uma estrutura de controle interno normalmente é composta por controles manuais e automatizados. Portanto, para determinar se os riscos estão sendo efetivamente gerenciados, ambos os tipos de controles necessitam ser avaliados. Deve-se, inclusive, avaliar se há uma combinação apropriada dos controles, incluídos os relacionados a TI, para o tratamento dos riscos do negócio.

---

[29] Vide definição de riscos inerentes em nota de rodapé do item 2.3 – “Gestão de riscos”.

A identificação dos controles-chave deve incluir os controles no nível da entidade[30] (e.g., o código de ética/conduta) e no nível de atividade/operação (e.g., setor de licitação), assim como outros controles e atividades situados nas diferentes camadas do *framework* COSO.

Os controles-chave identificados neste passo incluem:

- Controles manuais (e.g., execução de um inventário físico).
- Controles completamente automatizados (e.g., instalação periodicamente programada de atualizações das definições do software antivírus corporativo, controle do tipo de dado recebido no preenchimento de um campo de formulário eletrônico).
- Controles parcialmente automatizados (ou híbridos): quando a funcionalidade de uma aplicação é submetida a um controle manual. Exemplo: um controle-chave para a detecção de faturas hospitalares duplicadas pode incluir a revisão humana de um relatório gerado por um sistema. A parte manual do controle não é capaz de garantir que o relatório foi gerado sem erro.

É importante que haja uma revisão e confirmação da classificação de um controle automatizado como "chave", por duas razões:

1) O controle-chave pode ter sido relacionado a partir de uma abordagem *bottom-up*[31] (e.g., *checklist* elaborado por pessoal do nível operacional da UG), a qual pode ter equivocadamente classificado um controle qualquer como "chave".
2) Deve-se avaliar, caso o controle automatizado falhe, se existe uma probabilidade razoável de que haverá a propagação de um erro material não detectado. Isso porque podem existir controles manuais capazes de detectar uma falha em um controle automatizado antes que esta provoque um erro material. Neste caso, o controle manual é que deve ser classificado como chave e não o controle automatizado.

[30] O COSO descreve que os controles existem no "nível de entidade" (do inglês, "*entity-level*") e no nível de atividade do processo ("*activity-level*"). Os riscos no nível de entidade normalmente são de natureza mais penetrante, uma vez que podem afetar toda a organização e a efetividade dos múltiplos controles no nível de atividade. Os controles em nível de atividade estão relacionados aos objetivos estabelecidos para as várias atividades da organização, as quais podem estar separadas em áreas funcionais distintas (área administrativa, de contabilidade, jurídica, etc.) ou apenas compreendendo os vários processos do negócio, numa organização puramente orientada a processos (o que, normalmente, não é o caso das organizações públicas).

[31] Não se pretende aqui desqualificar a abordagem *bottom-up* ("de baixo para cima") de identificação dos controles de uma organização, porém apenas ressaltar que este tipo de abordagem pode estar desconectada dos objetivos estratégicos estabelecidos pela Alta Administração.

Por último, cumpre anotar que, se na auditoria dos riscos de negócio, são abordados alguns controles responsáveis pelo tratamento dos riscos, porém não todos (e.g., apenas os controles relacionados à segurança de TI, mas não os relacionados à segurança física), tal limitação no escopo deve ser claramente comunicada no relatório de auditoria.

3.1.4 Passo 4: Identificar a funcionalidade crítica de TI que suporta os controles-chave automatizados para os objetivos estratégicos selecionados.

A funcionalidade crítica de TI que suporta os processos-chave inclui os controles completa ou parcialmente automatizados (identificados no passo 3), podendo compreender também outras funcionalidades de TI não necessariamente vinculadas aos controles automatizados. Como exemplo deste último componente da funcionalidade crítica de TI, pode-se citar o fato de que muitas aplicações executam vários procedimentos que suportam a entrega de um ou mais produtos da organização. Estes procedimentos, tecnicamente, não são controles. Entretanto, se a funcionalidade provida apresenta alguma falha, pode ocorrer a introdução de erros que não serão detectados pelos controles manuais ou automatizados. Se estes erros não detectados resultarem no comprometimento de algum objetivo selecionado, então as aplicações em questão deverão ser consideradas uma funcionalidade crítica de TI.

3.1.5 Passo 5: Identificar as aplicações significativas onde os controles de TI precisam ser testados.

Uma vez identificada e confirmada a funcionalidade crítica de TI, devem-se identificar as aplicações significativas, sendo assim classificadas aquelas aplicações que compreendem uma funcionalidade crítica de TI, onde há um risco potencial em um controle de aplicação ou em um controle geral de TI[32].

As aplicações significativas podem ser identificadas da seguinte maneira:

a) Deve-se ordenar a funcionalidade crítica de TI por aplicação. A lista resultante da ordenação é uma lista de aplicações significativas cujos riscos relacionados aos controles de TI deverão ser avaliados e que deverão ser submetidas apenas ao próximo passo do processo.
b) Para as aplicações que não foram consideradas significativas (com base no critério da presença de funcionalidade crítica de TI), há um teste adicional: deve-se avaliar

[32] Os controles de aplicação e os controles gerais de TI são explicados e diferenciados no item 2.4.1 deste trabalho.

se uma alteração não autorizada nos dados da aplicação poderia resultar numa falha não detectada do atingimento do objetivo de negócio. Se houver essa possibilidade, a aplicação deve ser classificada como significativa[33].

O processo deve continuar apenas para as aplicações significativas.

3.1.6 Passo 6: Identificar os riscos relacionados às aplicações significativas e aos componentes tecnológicos que as suportam, assim como seus respectivos objetivos de controle.

Uma vez identificadas e listadas as aplicações significativas, faz-se necessário elaborar uma matriz "TxP", onde T se refere às tecnologias e P aos processos. O número de linhas (tamanho de T) e de colunas (tamanho de P) dependerá da complexidade técnica do ambiente de TI e do grau de detalhamento (tanto tecnológico quanto de processos) desejado (ou necessário) para a(s) auditoria(s) em planejamento. Uma matriz inicial simples seria uma de dimensão 2x3, ilustrada a seguir:

Tabela 1 – Matriz simples para o planejamento de auditorias de TI

	PROCESSOS			
	P x T	Aquisição	Operação	Monitoramento
TECNOLOGIAS	Aplicações			
	Infraestrutura			

Fonte: IIA – *GAIT for Business and IT Risk* (adaptado)

A primeira linha da matriz, referente a aplicações, é constante. A segunda linha, que se refere à infraestrutura tecnológica (sobre a qual residem os controles gerais de TI), pode ser desmembrada em quantas linhas forem desejadas pela equipe de planejamento da auditoria (e.g., bases de dados, sistemas operacionais, rede, hardware).

Quanto aos processos, os três listados se referem aos mais comuns e mais básicos. Entretanto, inúmeros outros processos podem ser mapeados e analisados, tanto a partir do desmembramento de algum destes quanto pela adição de algum outro. O processo relativo à

[33] Ocasionalmente, algumas funcionalidades de uma aplicação podem fazer uso de dados criados em outra aplicação. Quando uma alteração nestes dados puder resultar em um erro não detectado, o risco pode recair não apenas na aplicação que utiliza os dados, mas também em outras aplicações (como é o caso da aplicação onde os dados foram criados e de quaisquer outras aplicações onde estes dados foram armazenados). Neste caso, todas estas aplicações poderão ser classificadas como significativas, se a alteração nos dados não puder ser detectada por elas mesmas ou por algum outro controle.

operação, por exemplo, poderia ser subdividido em: gestão de níveis de serviço, gestão da capacidade, gestão da segurança, gerenciamento de configuração, etc. Para este tipo de detalhamento dos processos, recomenda-se recorrer ao guia viabilizador "COBIT 5 – *Enabling Processes*", disponível, até o fechamento deste trabalho, apenas na versão original em língua inglesa.

Para cada célula da matriz, deve-se responder à seguinte questão:

- "Existe uma probabilidade razoável de que a ocorrência de um evento relacionado ao processo e à tecnologia em questão poderá afetar a funcionalidade crítica de TI mapeada, de modo a comprometer o atingimento do objetivo de negócio ao qual esta funcionalidade se vincula? Se sim, identificar os riscos existentes, mensurados em termos de probabilidade e impacto, e os objetivos de controle relacionados."

Os objetivos de controle a serem identificados são aqueles que atendem à seguinte questão: "o que deve ser feito para que os riscos referentes a esta tecnologia e processo sejam adequadamente tratados pela organização?".

3.1.7 Passo 7: Identificar os controles de TI (gerais e de aplicação) que necessitam ser testados quanto ao atingimento dos objetivos de controle mapeados.

Uma vez que todos os riscos e objetivos de controle de TI relevantes foram identificados, os controles-chave de TI específicos (tanto de aplicação quanto gerais), necessários ao tratamento dos riscos, devem ser determinados. O COBIT 5 pode, novamente, ser significativamente útil para a consecução de tal tarefa.

Cada controle-chave de TI deve ser especificamente relacionado aos objetivos de controle identificados durante o passo 6 e, então, à operação apropriada da funcionalidade crítica de TI submetida a risco.

3.1.8 Passo 8: Realizar uma revisão holística personalizada de todos os controles-chave identificados.

Neste passo, a equipe de auditoria deve rever os controles identificados e se assegurar acerca do provimento do nível de garantia requerido. Também deve-se examinar se existem controles duplicados ou redundantes, com vistas à eliminação daqueles controles cujas falhas possam ser detectadas e compensadas por outros controles.

3.1.9 Passo 9: Determinar o escopo da revisão dos controles e construir um programa de avaliação apropriado e efetivo.

Como já visto, o processo de planejamento de auditorias proposto identifica os controles-chave necessários ao provimento de razoável garantia acerca do cumprimento dos objetivos do negócio da UG selecionada. A equipe de auditoria pode então decidir que tipo de revisão ou auditoria executará:

- Uma auditoria completa do negócio da UG (auditoria integrada de todos os riscos e respectivos controles).
  - Pode-se realizar a auditoria em um único projeto ou dividi-la em múltiplos projetos, a serem executados em momentos distintos.
  - Se a avaliação for dividida em múltiplos projetos, a equipe de auditoria deve determinar como será realizada e reportada a avaliação consolidada (totalizadora) e como serão avaliados e comunicados os resultados dos projetos individuais.
- Uma auditoria cujo escopo está limitado a apenas alguns controles selecionados.
  - O escopo limitado deve ser claramente identificado e comunicado antes do início dos trabalhos, bem como deve ser ressaltado no relatório de auditoria.
  - A equipe de auditoria deve estar ciente de que a avaliação de apenas algumas deficiências de controle pode ser bem mais difícil sem o entendimento da efetividade dos controles relacionados e da possibilidade de mitigação das deficiências por outros controles-chave não avaliados.

3.2 PERFIL DESEJADO PARA A EQUIPE DE AUDITORIA

Conforme muito bem observado pelo IIA (2007) em sua metodologia GAIT, a experiência mostra que auditores generalistas de negócio normalmente não compreendem completamente as funcionalidades da TI que suportam os objetivos do negócio, assim como os auditores especialistas em TI nem sempre compreendem completamente os processos de negócio suportados pela tecnologia.

Deste modo, para que se atenda à norma de atributo 1210[34] do IPPF, é recomendável

[34] NA 1210 – Proficiência: "Os auditores internos devem possuir o conhecimento, as habilidades e outras competências necessárias ao desempenho de suas responsabilidades individuais. A atividade de auditoria interna deve possuir, ou obter, coletivamente o conhecimento, as habilidades e outras competências necessárias ao desempenho de suas responsabilidades."

que a equipe envolvida no planejamento da auditoria (e, posteriormente, em sua execução) seja composta tanto por pessoas com um bom entendimento das atividades finalísticas de negócio da UG a ser examinada (e.g., passos 1 a 3 do processo proposto) quanto por pessoas com experiência profissional ou acadêmica na área de tecnologia da informação (e.g., passos 5 a 7), de modo que os conhecimentos de ambos os perfis profissionais desejados possam se integrar sinergicamente na composição do rol de competências necessárias ao bom desempenho das atividades de auditoria.

4. CONCLUSÃO

Tendo em vista a necessidade, apontada pelo TCU, de se fortalecer e de se sistematizar a realização de auditorias de TI por parte da CGU, assim como de se orientar e incentivar as unidades de Auditoria Interna da Administração Indireta a também realizá-las, este trabalho se propôs a apresentar um processo de seleção e planejamento de auditorias de TI no âmbito das unidades gestoras do Poder Executivo Federal, com base em uma avaliação integrada das estruturas de governança, riscos e controles internos.

A proposta apresentada se baseia em uma abordagem *top-down*, iniciada a partir da identificação dos objetivos estratégicos estabelecidos pela organização e de seus principais produtos (bens ou serviços) entregues à sociedade. No final do processo, são identificados os controles-chave de TI que devem ser objeto de auditoria, haja vista o fato de estarem associados a riscos capazes de comprometer o alcance dos objetivos de negócio da unidade.

Este tipo de abordagem possui uma alta probabilidade de entrega de valor à Administração e à sociedade, uma vez que os objetos de TI a serem auditados são selecionados com base em uma visão holística da organização, tendo como foco o suporte à consecução plena de seus objetivos finalísticos.

A proposta foi devidamente suportada por um arcabouço teórico que também tenciona orientar, do ponto de vista conceitual, os auditores com pouca experiência nos temas abordados.

Em vista do exposto, considera-se que o trabalho conseguiu atingir os objetivos específicos propostos em sua introdução, assim como seu objetivo geral.

Com relação às dificuldades e limitações encontradas na execução desta pesquisa, podem-se apontar as seguintes:

- Pouco tempo disponível para sua realização, em razão: da necessidade de se concluir, concomitantemente, as disciplinas finais do curso e da ocorrência de interrupções relacionadas a período de recesso de final de ano e remoção do autor para outra Unidade da Federação.
- Impossibilidade de se discutir e validar a proposta com os colegas de trabalho, em virtude da dificuldade anterior.

Finalmente, no objetivo de se dar continuidade ao presente trabalho, sugerem-se os seguintes trabalhos futuros:

- Complementação da abordagem *top-down* de planejamento de auditorias de TI com uma abordagem *bottom-up* (de baixo para cima, originária do nível

operacional), de modo a identificar controles mais operacionais/técnicos que, embora possam não estar diretamente relacionados à consecução dos objetivos estratégicos do negócio, sejam capazes de representar um risco razoável para a unidade, ainda que de maneira indireta.

- Elaboração de propostas que sirvam como modelos de referência para a execução e apresentação de trabalhos de auditoria de TI na CGU, com base nas diretrizes e boas práticas de mercados já existentes, em especial as do IIA e da ISACA.
- Promoção de pesquisa interna na CGU com vistas à identificação das principais necessidades de capacitação dos servidores, no que se refere à realização sistemática de trabalhos de auditoria de TI, e criação de um banco de talentos de TI que possa ser aproveitado para a execução de trabalhos em conjunto, seminários, palestras, oficinas técnicas, intercâmbio, dentre outras atividades.
- Promoção de pesquisa nas unidades de Auditoria Interna da Administração Indireta com vistas à identificação das principais dificuldades, desafios e casos de sucesso com relação à realização de trabalhos de auditoria de TI.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE BANCOS INTERNACIONAIS (ABBI); FEDERAÇÃO BRASILEIRA DE BANCOS (FEBRABAN). **Função de Compliance.** Julho 2009. Disponível em: <http://www.abbi.com.br/download/funcaodecompliance_09.pdf>. Acessado em: 30 dez. 2012.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **NBR ISO/IEC 38500:2009: Governança corporativa de tecnologia da informação.** 2009.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **NBR ISO/IEC 27002:2005: Tecnologia da Informação – Técnicas de Segurança – Código de prática para a gestão da segurança da informação.** 2005.

AUSTRALIAN STANDARD – AS/NZS 4360:1999. **Risk Management.** 1999

BALZANI, Haylla Souza. **Balanced Scorecard – BSC: uma ferramenta de gestão.** 2006. Disponível em <http://www.administradores.com.br/informe-se/artigos/balanced-scorecard-bsc-uma-ferramenta-de-gestao/12951/>. Acessado em: 29 dez. 2012.

BARBOSA, Emerson Rodrigues; BRONDANI, Gilberto. **Planejamento estratégico organizacional.** Revista Eletrônica de Contabilidade v. 1, n. 2, dez./2004 – fev./2005, Universidade Federal de Santa Maria, Santa Maria, 2004.

BRASIL. Conselho Nacional de Justiça. **Resolução – CNJ 70, de 18 de março de 2009.** Dispõe sobre o Planejamento e a Gestão Estratégica no âmbito do Poder Judiciário e dá outras providências. 2009. Disponível em:<http://www.cnj.jus.br/gestao-e-planejamento/gestao-e-planejamento-do-judiciario/resolucao-n-70>. Acessado em: 30 dez. 2012.

BRASIL. **Constituição da República Federativa do Brasil, de 5 de outubro de 1988.** 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm>. Acessado em: 30 dez. 2012.

BRASIL. **Decreto-Lei 200, de 25 de fevereiro de 1967**. Dispõe sobre a organização da Administração Federal, estabelece diretrizes para a Reforma Administrativa e dá outras providências. 1967. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del0200.htm>. Acessado em: 30 dez. 2012.

BRASIL. **Lei 10.180, de 06 de fevereiro de 2001.** Organiza e disciplina os Sistemas de Planejamento e de Orçamento Federal, de Administração Financeira Federal, de Contabilidade Federal e de Controle Interno do Poder Executivo Federal, e dá outras providências. 2001. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/LEIS_2001/L10180.htm>. Acessado em: 30 dez. 2012.

BRASIL. **Lei 10.683, de 28 de maio de 2003.** Dispõe sobre a organização da Presidência da República e dos Ministérios, e dá outras providências. 2003. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/2003/L10.683.htm>. Acessado em: 30 dez. 2012.

BRASIL. Secretaria de Gestão do Ministério do Planejamento, Orçamento e Gestão. **Programa Nacional de Gestão Pública e Desburocratização – GesPública – Documento de Referência 2008/2009**. 2009.1 CD-ROM.

BRASIL. Secretaria de Logística e TI do Ministério do Planejamento, Orçamento e Gestão. **Instrução Normativa SLTI/MPOG 04, de 12 de novembro de 2010.** Dispõe sobre o processo de contratação de Soluções de Tecnologia da Informação pelos órgãos integrantes do Sistema de Administração dos Recursos de Informação e Informática (SISP) do Poder Executivo Federal. 2010. Disponível em: < http://www.governoeletronico.gov.br/biblioteca/arquivos/instrucao-normativa-no-04-de-12-de-novembro-de-2010>. Acessado em: 30 dez. 2012.

BRASIL. Tribunal de Contas da União. **Acórdão 1.145/2011-TCU-Plenário.** 2011. Disponível em: <http://www.tcu.gov.br/Consultas/Juris/Docs/judoc/Acord/20110512/AC_1145_15_11_P.doc>. Acessado em: 30 dez. 2012.

BRASIL. Tribunal de Contas da União. **Acórdão 1.233/2012-TCU-Plenário.** 2012. Disponível em: <http://www.tcu.gov.br/Consultas/Juris/Docs/judoc/Acord/20120528/AC_1233_19_12_P.doc>. Acessado em: 30 dez. 2012.

BRASIL. Tribunal de Contas da União. **Acórdão 1.603/2008-TCU-Plenário.** 2008. Disponível em: <http://www.tcu.gov.br/Consultas/Juris/Docs/judoc%5CAcord%5C20080814%5C008-380-2007-1-GP.doc>. Acessado em: 30 dez. 2012.

BRASIL. Tribunal de Contas da União. **Critérios Gerais de Controle Interno na Administração Pública**: um estudo dos modelos e das normas disciplinadoras em diversos países. Brasília, 2009. Disponível em: <http://portal2.tcu.gov.br/portal/pls/portal/docs/2056688.PDF>. Acessado em: 30 dez. 2012.

BRASIL. Tribunal de Contas da União. **Decisão Normativa – TCU 117, de 19 de outubro de 2011.** Dispõe sobre a elaboração e o envio ao TCU das peças complementares ao relatório de gestão, para a constituição de processos de contas de 2011. Disponível em: <http://www.tcu.gov.br/Consultas/Juris/Docs/judoc/DN/20111025/DNT2011-117.doc>. Acessado em: 30 dez. 2012.

BRASIL. Tribunal de Contas da União. **Guia de boas práticas em contratação de soluções de tecnologia da informação**: riscos e controles para o planejamento da contratação. Versão 1.0, Brasília, 2012. Disponível em: <http://portal2.tcu.gov.br/portal/page/portal/TCU/imprensa/noticias/noticias_arquivos/Guia%20de%20contrata%C3%A7%C3%A3o%20de%20solu%C3%A7%C3%B5es%20de%20TI_Vers%C3%A3o%20Eletr.pdf>. Acesso em: 30 dez. 2012.

BRASIL. Tribunal de Contas da União. **Manual de auditoria operacional.** Brasília, 2010. Disponível em: <portal2.tcu.gov.br/portal/pls/portal/docs/2058980.PDF>. Acessado em: 30 dez. 2012.

CARMONA, Rafael Selau. **Administração estratégica no Poder Judiciário: o planejamento estratégico do Conselho Nacional de Justiça.** 2010. Disponível em: <http://www2.trf4.jus.br/trf4/upload/editor/apg_RafaelSelauCarmona.pdf>. Acessado em: 30 dez. 2012.

COMMITTEE OF SPONSORING ORGANISATIONS OF THE TREADWAY COMISSION (COSO). **Internal Control – Integrated Framework.** September 1992.

COMMITTEE OF SPONSORING ORGANISATIONS OF THE TREADWAY COMISSION (COSO). **COSO Enterprise Risk Management (ERM) – Integrated Framework.** 2004.

COMMITTEE OF SPONSORING ORGANISATIONS OF THE TREADWAY COMISSION (COSO). **COSO Gerenciamento de Riscos Corporativos – Estrutura Integrada.** 2007.

DA SILVA, Leandro Costa. **O Balanced Scorecard e o processo estratégico.** Caderno de Pesquisas em Administração, São Paulo, v.10, n. 4, p. 61-73, 2003.

DE MELLO, Gilmar Ribeiro. **Governança corporativa no setor público federal brasileiro.** Dissertação de Mestrado em Ciências Contábeis, Departamento de Contabilidade, Faculdade de Economia, Administração e Contabilidade, Universidade de São Paulo, São Paulo, 2006.

DE SOUZA, José Geraldo Andrade. **Alinhamento estratégico de TI: avaliando as percepções de executivos de negócio e TI.** Dissertação de Mestrado em Gestão Empresarial, Escola Brasileira de Administração Pública e de Empresas, Fundação Getúlio Vargas, Rio de Janeiro, 2008.

FERREIRA, André Ribeiro. **Modelo de excelência em gestão pública**. Revista Eixo n. 1, v. 1, p. 31-43, Instituto Federal de Educação, Ciência e Tecnologia de Brasília, Brasília, 2012.

FORRESTER RESEARCH. **IT Governance Framework.** 2005.

GIBBS, Nelson et al. **A new auditor's guide to planning, performing and presenting IT audits.** The Institute of Internal Auditors Research Foundation (IIARF): Florida, USA, 2010.

HANASHIRO, Maíra. **Metodologia para desenvolvimento de procedimentos e planejamento de auditorias de TI aplicada à administração pública federal.** Dissertação de Mestrado em Engenharia Elétrica, Departamento de Engenharia Elétrica, Faculdade de Tecnologia, Universidade de Brasília, Brasília, 2007.

HANASHIRO, Maíra. **Proposta de modelo de implementação de auditoria de tecnologia da informação no âmbito da Controladoria-Geral da União**. Monografia de especialização em Auditoria Interna e Controle Governamental, Instituto Serzedelo Corrêa, Tribunal de Contas da União, Brasília, 2009.

INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION (ISACA). **COBIT 5 Framework.** 2012.

INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION (ISACA). **COBIT 5 Enabling Processes.** 2012.

INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION (ISACA). **COBIT and application controls: a management guide**. 2009.

INSTITUTE OF INTERNAL AUDITORS (IIA). **Global Technology Audit Guide (GTAG) 17 – Auditing IT Governance.** July 2012.

INSTITUTE OF INTERNAL AUDITORS (IIA). **Global Technology Audit Guide (GTAG) 1 – Information Technology Risk and Controls.** 2nd edition, March 2012.

INSTITUTE OF INTERNAL AUDITORS (IIA). **Global Technology Audit Guide (GTAG) 8 – Auditing Application Controls.** July 2007.

INSTITUTE OF INTERNAL AUDITORS (IIA). **Global Technology Audit Guide (GTAG) 11 – Developing the IT Audit Plan.** July 2008.

INSTITUTE OF INTERNAL AUDITORS (IIA). **GAIT for Business and IT Risk (GAIT-R).** March 2008.

INSTITUTE OF INTERNAL AUDITORS (IIA). **GAIT Methodology: a risk based approach to assessing the scope of IT general controls.** August 2007.

INSTITUTE OF INTERNAL AUDITORS (IIA). **Normas Internacionais para a Prática Profissional da Auditoria Interna.** 2010.

INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA (IBGC). **Código das Melhores Práticas de Governança Corporativa.**1ª reimpressão da 4ª edição, 2010.

INTERNATIONAL FEDERATION OF ACCOUNTANTS (IFAC). **Governance in the Public Sector: a governing body perspective.** New York, August 2001. Disponível em: <http://www.ifac.org/sites/default/files/publications/files/study-13-governance-in-th.pdf>. Acessado em: 30 dez. 2012.

INTERNATIONAL ORGANISATION OF SUPREME AUDIT INSTITUTIONS (INTOSAI). **Diretrizes para as normas de controle interno do setor público.** Tribunal de Contas do Estado da Bahia, série Traduções, n. 13, Bahia, Brasil, 2007. Disponível em: <http://www.tce.ba.gov.br/images/intosai_diretrizes_p_controle_interno.pdf>. Acessado em: 30 dez. 2012.

INTERNATIONAL ORGANISATION OF SUPREME AUDIT INSTITUTIONS (INTOSAI). **Performance Audit Guidelines: ISSAI 3000 – 3100.** Vienna, Austria, 2001.

INTERNATIONAL STANDARD – ISO 31000:2009. **Risk Management – Principles and Guidelines.** 2009

IT GOVERNANCE INSTITUTE (ITGI). **Board Briefing on IT Governance.** 2nd edition, 2003.

IT GOVERNANCE INSTITUTE (ITGI). **COBIT 4.1 Portuguese.** 2007

MATIAS-PEREIRA, José. **A governança corporativa aplicada no setor público brasileiro.** APGS, Viçosa, v. 2, n. 1, p. 110-135, jan./mar. 2010.

MOELLER, Robert R. **IT audit, control, and security.** John Wiley & Sons: New Jersey, 2010

MONTEIRO, Gustavo Bastos. **Auditoria de tecnologia da informação no âmbito dos municípios do Estado do Rio de Janeiro.** Dissertação de Mestrado em Administração Pública, Escola Brasileira de Administração Pública e de Empresas, Fundação Getúlio Vargas, Rio de Janeiro, 2008.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OCDE). **Principles of Corporate Governance.** 2004.

PEREIRA, Carlos Diego Cavalcanti. **A estratégia de tecnologia da informação: uma análise sobre modelos de interação com o negócio.** Universidade Federal de Pernambuco, Recife, 2011. Disponível em: <http://www.valcann.com/A_estrategia_de_Tecnologia_da_Informacao_Rev_03_12_07_2011.pdf>. Acessado em: 29 dez. 2012.

PORTA, Flaviano Carvalho Dalla. **As diferenças entre auditoria interna e compliance.** Dissertação de Mestrado em Economia, Faculdade de Ciências Econômicas, Universidade Federal do Rio Grande do Sul, Porto Alegre, 2011.

REZENDE, Denis Alcides. **Planejamento de sistemas de informação e informática.** São Paulo: Atlas, 2003.

SILVA, Carlos Alberto dos Santos. **Diretrizes para auditoria do processo de contratação de tecnologia da informação na administração pública federal.** Dissertação de Mestrado em Gestão do Conhecimento e da Tecnologia da Informação, Universidade Católica de Brasília, Brasília, 2008.

THE OPEN COMPLIANCE AND ETHICS GROUP (OCEG). **OCEG Red Book GRC Capability Model version 2.1**: achieving principled performance by integrating the governance, assurance and management of performance, risk and compliance. 2012.

THE OPEN GROUP. **The Open Group Architecture Framework (TOGAF) version 9.** 2009.