Controle Externo da governança de Tecnologia da Informação

Raimir Holanda Filho
Doutor em Ciência da Computação pela Universitat Politècnica de Catalunya
Certificado de Auditor Líder em Sistema de Gestão de Segurança da Informação ISO/IEC 27001
Professor do Programa de Mestrado e Doutorado em Informática da Universidade de Fortaleza (UNIFOR)
Analista de Controle Externo e Diretor da 13a Inspetoria de Controle Externo do Tribunal de Contas do Estado do Ceará (TCE)

José Auriço Oliveira
Mestre em Informática Aplicada pela Universidade de Fortaleza
Certificado *Project Management Professional (PMP)*
Certified Information Systems Auditor (CISA) pela ISACA
Certificado de Auditor Líder em Sistema de Gestão de Segurança da Informação ISO/IEC 27001
Professor Universitário na área de Tecnologia da Informação
Analista de Controle Externo e SubDiretor da 13a Inspetoria de Controle Externo do Tribunal de Contas do Estado do Ceará (TCE)

Resumo: O crescente processo de informatização da Administração Pública brasileira contribui para uma maior agilidade e qualidade nos serviços públicos prestados para a sociedade e um consequente aumento na transparência das ações governamentais. Por outro lado, os gastos nos investimentos e na manutenção dos recursos de Tecnologia da Informação (TI) vêm aumentando consideravelmente, bem como tem-se verificado uma forte dependência das instituições com relação aos sistemas informatizados e à segurança das suas bases de dados. Com o aumento da importância estratégica da área de TI, houve uma busca pela aplicação de modelos de governança, com o objetivo de tornar a área controlável, com resultados mensuráveis e orientada aos objetivos do negócio da

instituição. A auditoria de TI tem como função principal avaliar o processo de gestão, no que se refere aos seus diversos aspectos, tais como a governança corporativa, gestão de riscos de TI e procedimentos de aderência às normas regulatórias, apontando eventuais desvios e vulnerabilidades, como também oferecendo alternativas de soluções para esses diversos problemas. No âmbito do controle externo, os Tribunais de Contas começam a reconhecer a necessidade de implantar áreas especializadas na realização de Auditoria de TI. Neste contexto, o presente trabalho pretende apresentar quais as abordagens utilizadas nesta área de fiscalização, destacando a importância da Governança de TI como importante instrumento na atuação do controle externo na fiscalização da gestão e do uso da Tecnologia da Informação na Administração Pública.

Palavras-chaves: auditoria de TI; governança de TI e gestão de riscos.

Introdução

O crescente processo de informatização da Administração Pública brasileira contribui para uma maior agilidade e qualidade nos serviços públicos prestados para a sociedade e um consequente aumento na transparência das ações governamentais. Por outro lado, os gastos nos investimentos e na manutenção dos recursos de Tecnologia da Informação vêm aumentando consideravelmente, bem como tem-se verificado uma forte dependência das instituições com relação aos sistemas informatizados e à segurança das suas bases de dados.

Recentemente, tem-se observado que os países com maiores níveis de transparência são aqueles que se encontram nas melhores posições no ranking corrupção. Logo, existe uma relação direta entre o controle social e a qualidade/quantidade da informação que os entes governamentais disponibilizam aos seus cidadãos, sendo exatamente esta combinação a principal responsável pela melhora nos processos de gestão e pela redução nos níveis de corrupção.

Vê-se, portanto, que não basta simplesmente disponibilizar a informação, necessita-se que esta informação apresente um conjunto de requisitos para que ela efetivamente possa ser utilizada como ferramenta de controle. Dentre estes requisitos, podemos citar a necessidade de que a informação represente de forma

fiel todos os atos ocorridos no âmbito da administração pública, a garantia da completude dos documentos associados a estes dados bem como a tempestividade das informações.

Neste âmbito, auditorias especializadas em Tecnologia da Informação são realizadas com o propósito de garantir que os requisitos acima elencados estejam presentes.

Dada a importância estratégica da área de tecnologia da informação, a expressiva materialidade tanto das aquisições relacionadas à tecnologia da informação quanto dos recursos geridos por meio de sistemas informatizados no governo estadual, e o uso cada vez mais crescente da tecnologia da informação para manipulação e armazenamento de dados da Administração Pública estadual, introduzindo novos riscos e aumentando a fragilidade de algumas atividades, o Tribunal de Contas do Estado do Ceará conta com a 13a Inspetoria de Controle Externo como unidade especializada na área de Auditoria de Tecnologia da Informação.

Neste trabalho, apresenta-se, segundo alguns autores, os diferentes tipos de abordagens possíveis de serem utilizados nos trabalhos de fiscalização na área de Auditoria de Tecnologia da Informação. Será demonstrado no âmbito de controle externo tanto federal como estadual como os órgãos fiscalizadores estão organizando e agrupando as áreas de atuação em Auditoria de TI. Será destacada a área de Governança de TI, em virtude de a mesma agrupar todas as demais áreas de atuação em Auditoria de TI, apresentando alguns conceitos e como os trabalhos podem ser conduzidos pelos órgãos de controle na execução de uma fiscalização nesta área.

1. Auditoria em Tecnologia da Informação

Segundo Schmidt (SCHMIDT, 2006), a Auditoria de TI deve ser utilizada para promover adequação, revisão, avaliação e recomendações para o aprimoramento dos controles internos nos sistemas de informações da empresa, bem como avaliar a utilização dos recursos humanos, materiais e tecnológicos envolvidos no processamento dos mesmos.

Existe uma diversidade de trabalhos relacionados à área de auditoria de TI, podendo estes trabalhos serem executados em qualquer nível estratégico de uma

organização, abrangendo desde a alta administração até o nível operacional.

Para agrupar as auditorias de TI por tipos ou por abordagens, existem alguns trabalhos na literatura técnica que apresentam diversas formas de classificação. De acordo com (LYRA, 2008, pag. 108), os tipos de auditorias possuem as seguintes modalidades:

"AUDITORIA DURANTE O DESENVOLVIMENTO DE SISTEMAS

Compreende auditar todo o processo de construção de sistemas de informação, da fase de requisitos até a sua implementação.

AUDITORIA DE SISTEMAS EM PRODUÇÃO

Preocupa-se com os procedimentos e resultados dos sistemas já implantados, com relação à segurança, corretude e tolerância a falhas.

AUDITORIA NO AMBIENTE TECNOLÓGICO

Compreende a análise do ambiente de informática em termos de estrutura organizacional, contratos, normas, técnicas, custos, nível de utilização de equipamentos e planos de segurança e de contingência.

AUDITORIA EM EVENTOS ESPECÍFICOS

Compreende a análise das causas, consequências e ações corretivas cabíveis em eventos não cobertos pelas auditorias anteriores."

Segundo Dias (DIAS, 2008), a Auditoria da Tecnologia da Informação é um tipo de auditoria operacional, que analisa a gestão de recursos, enfocando os aspectos de eficiência, eficácia, economia e efetividade. Pode abranger: o ambiente de informática como um todo; a organização do departamento de informática; controles sobre BD´s; redes e diversos aplicativos."

Para Dias (DIAS, 2008), existem 3 subáreas de auditoria em ambientes informatizados:

"AUDITORIA DA SEGURANÇA DE INFORMAÇÕES

Determina a postura da organização com relação à segurança das suas informações. Faz parte da auditoria de TI.

Escopo:

• Avaliação da política de segurança;

• Controles de acesso lógico;

• Controles de acesso físico;

• Controles ambientais;

• Planos de contingências e continuidade dos serviços.

AUDITORIA DA TECNOLOGIA DA INFORMAÇÃO

Abrange todos os aspectos relacionados com a auditoria da segurança das informações, além de outros controles que podem influenciar a segurança de informações e o bom funcionamento dos sistemas da organização.

Controles:

• Organizacionais;

• De mudanças;

• De operação dos sistemas;

• Sobre bancos de dados;

• Sobre microcomputadores;

• Sobre ambientes cliente-servidor.

AUDITORIA DE APLICATIVOS

Voltada para a segurança e o controle de aplicativos específicos.

Controles:

• Desenvolvimento de sistemas aplicativos;

• Entrada, processamento e saída de dados;

• Sobre conteúdo e funcionamento do aplicativo, com relação a área por ele atendida. ″

O Isaca (ISACA, 2012), em seu manual de revisão 2012, para a obtenção da Certificação CISA, divide os Domínios necessários para os Auditores de TI da seguinte forma: Governança e Gerenciamento de TI; Aquisição, desenvolvimento e implementação de sistemas de informação; Operação, Manutenção e Suporte de Sistemas de Informação; e, proteção de ativos de informação.

No ambiente de Controle Externo, verificamos que na esfera federal o Tribunal de Contas da União-TCU, através da Secretaria de Fiscalização de Tecnologia da Informação – Sefti, utiliza as seguintes abordagens na área de Auditoria de TI, seja na Fiscalização operacional e/ou de conformidade: Governança; Programas e Políticas; Segurança; Sistemas ; Dados; Infraestrutura e Contratações de TI.

Na esfera estadual, o Tribunal de Contas do Estado do Ceará, através da 13a Inspetoria de Controle Externo, definiu 6 (seis) áreas de atuação para a realização dos trabalhos de fiscalização operacional e/ou de conformidade: Auditoria de Governança de TI; Auditoria de Infraestrutura de TI; Auditoria de Sistemas de Informação; Auditoria de Aquisições de TI; Avaliação de Programas de TI e Auditoria de Segurança da Informação. Os objetivos e os parâmetros utilizados em cada área serão descritos a seguir:

Auditoria de Governança de TI

Aferir as práticas de Governança de TI nos órgãos/entidades do Governo do Estado do Ceará sob sua jurisdição. As bases de referência utilizadas para essas verificações são a Norma ABNT NBR ISO/IEC 38500:2009 (ABNT, 2009) e o *Control Objectives for Information and related Technology* (COBIT) 4.1.

Auditoria de Infraestrutura de TI

Aplicar as verificações mínimas que devem ser efetuadas pelos auditores nos componentes aplicáveis da infraestrutura de TI de um órgão/entidade do Governo do Estado do Ceará sob sua jurisdição. A base de referência utilizada para essas verificações é a norma ABNT NBR ISO/IEC 20000-2:2008 – Tecnologia da Informação – Gerenciamento de Serviços – Código de Prática (ABNT, 2008).

Auditoria de Sistemas de Informação

Aplicar as verificações mínimas que devem ser efetuadas pelos auditores para aferir características dos Sistemas da Informação utilizados pelos órgãos/entidades do Governo do Estado do Ceará sob sua jurisdição.

A auditoria de Sistemas de Informação compreende:

1) Auditoria no processo de desenvolvimento do sistema;

A auditoria no processo de Desenvolvimento do Sistema visa a avaliar a adequação das metodologias e procedimentos de levantamento de necessidades, projeto, desenvolvimento e implementação do sistema produzido.

A base de referência utilizada para essas verificações é o domínio AI – Aquisição e Implementação do *Control Objectives for Information and related Technology* (COBIT) 4.1.

2) Auditoria dos sistemas em produção;

A atividade de Produção refere-se a todas as atividades relacionadas a um sistema depois que ele é implementado. Incluem-se aí atividades tais como a correção de software que não funcione adequadamente, a adição de novos recursos aos sistemas em resposta às novas demandas dos usuários, entre outros. Por isso, essa atividade serve como realimentação para o ciclo de desenvolvimento.

A Auditoria de Sistemas em Produção tem por objetivo verificar sua disponibilidade e robustez contra erros, acidentes e fraudes. As bases de referência utilizadas para essas verificações são as normas ISO/IEC 15408 - *Information technology — Security techniques — Evaluation criteria for IT security* e ABNT NBR ISO/IEC 27002:2005 – Tecnologia da Informação – Técnicas de Segurança – Código de prática para a gestão da segurança da informação (ABNT, 2005).

3) Auditoria dos bancos de dados;

A Auditoria de Bancos de Dados visa a avaliar aspectos de confidencialidade, integridade e disponibilidade dos bancos de dados onde as informações manipuladas pelos sistemas de informação estão armazenadas. A base de referência utilizada para essas verificações é a Norma ABNT NBR ISO/IEC 27002:2005 – Tecnologia da Informação – Técnicas de Segurança – Código de prática para a gestão da segurança da informação (ABNT, 2005).

4) Auditoria do processo de *backup* de informações.

A Auditoria do Processo de *Backup* de informações busca obter evidências de que os procedimentos de *backup* são executados satisfatoriamente, assegurando que os controles de *backup* estão efetivos e aumentando a garantia de que perdas acidentais de informações não trarão impacto para o órgão/entidade. A base de referência utilizada para essas verificações é a Norma ABNT NBR ISO/IEC 27002:2005 – Tecnologia da Informação – Técnicas de Segurança – Código de prática para a gestão da segurança da informação.

Auditoria de Aquisições de TI

Aplicar as verificações mínimas que devem ser efetuadas pelos auditores no processo de aquisições de TI efetuadas pelos órgãos/entidades do Governo do Estado do Ceará sob sua jurisdição. As bases de referência utilizadas para essas verificações são:

Instrução Normativa 04/2010, publicada pela Secretaria de Logística e Tecnologia da Informação – SLTI do Ministério do Planejamento, Orçamento e Gestão (BRASIL, 2010b);

Guia de Boas Práticas em Contratação de Soluções de Tecnologia da Informação, versão 1.0 de 2011, do Ministério do Planejamento, Orçamento e Gestão;

Decreto Nº 29.227/2008 - Política de Segurança da Informação do Governo do Estado do Ceará (CEARÁ, 2012b);

Decreto Nº 29.644/2009 - Instituição das diretrizes da Política de aquisições de serviços de Tecnologia da Informação e Comunicação (TIC) do Governo do Estado do Ceará (CEARÁ, 2012c);

Instrução Normativa Nº 001/2009 - Dispõe sobre as aquisições de serviços de Tecnologia da Informação e Comunicação (TIC) pela Administração Pública Estadual do Governo do Estado do Ceará (CEARÁ, 2012d);

Instrução Normativa Nº 003/2009 - Dispõe sobre procedimentos para liberação de recursos financeiros orçamentários referentes à Tecnologia da Informação e Comunicação (TIC) e procedimentos aplicáveis aos processos administrativos de aquisição de bens e contratação de serviços de TIC no âmbito da Administração Pública Estadual, sujeitos à deliberação da Secretaria de

Planejamento e Gestão – SEPLAG do Governo do Estado do Ceará;

Resolução Nº 1/2008 do Conselho Superior de Tecnologia da Informação e Comunicação - CSTIC do Estado do Ceará.

Avaliação de Programas de TI

Aplicar as verificações mínimas que devem ser efetuadas pelos auditores da 13ª ICE nos Programas de TI de um órgão/entidade do Governo do Estado do Ceará sob sua jurisdição. A base de referência utilizada para essas verificações é a publicação *The Standard for Program Management* – 2006, editada pelo *Project Management Institute* (PMI).

Auditoria de Segurança da Informação.

Aplicar as verificações mínimas que podem ser efetuadas pelos auditores para aferir características de Segurança da Informação nos órgãos/entidades do Governo do Estado do Ceará sob sua jurisdição. A base de referência utilizada para essas verificações é a Norma ABNT NBR ISO/IEC 27002:2005 (ABNT, 2005).

2. Governança em Tecnologia da Informação

A Governança Corporativa é definida como um sistema pelo qual as instituições são dirigidas e monitoradas. As boas práticas de governança corporativa têm a finalidade de aumentar a confiabilidade nas instituições, através da criação de um conjunto eficiente de mecanismos, a fim de assegurar que o comportamento de seus dirigentes esteja sempre alinhado com os interesses institucionais. Segundo Weill (Weill, 2006), uma maior atenção ao tema da governança se deu a partir do início do milênio, como explica: "a governança corporativa tornou-se um tema dominante nos negócios por ocasião da safra de escândalos corporativos em meados de 2002 – Enron, Worldcom e Tyco". Tais escândalos abalaram profundamente as bolsas de valores, pois demonstrou que não se podia confiar nos relatórios financeiros como base para análises de investimentos no mercado de capitais, tendo em vista as manipulações que ocorreram. Isso acarretou a criação de alguns marcos

regulatórios, dentre eles o *Sarbanes-Oxley Act* de 2002 e o Acordo de Basiléia, que buscaram recuperar a confiança dos investidores nas bolsas de ações, depois das vertiginosas quedas que ocorreram.

Para Fernandes (Fernandes, 2006), a fundamentação do *Sarbanes-Oxley Act* de 2002 é justamente para amenizar e restaurar a confiança dos investidores depois dos escândalos financeiros que ocorreram nos Estados Unidos com companhias de capital aberto, visando a proteger os investidores que aplicam no mercado de capitais de fraudes na contabilidade e mascaramento financeiro, através de uma maior transparência e controles internos e externos sobre relatórios contábeis. A lei *Sarbanes-Oxley*, em seu artigos, destaca alguns requisitos que contribuem para a redução dos riscos e inibem a ocorrência de fraudes, como o controle sobre a criação, edição e versionamento de documentos conforme os padrões ISO. Especifica, também, que esses documentos devem estar disponíveis em vários sites, devendo ser armazenados em formato digital e impresso, entre outras exigências.

Já o Acordo de Basiléia, trata de instituições financeiras, estabelecendo requisitos mínimos de capital que as operadoras de crédito devem ter para atuar em operações de risco de crédito. Isso visa a garantir a liquidez dos investimentos.

De acordo, ainda, com as pesquisas realizadas por Weill, as instituições em geral têm maior atenção dedicada para os ativos financeiros e físicos, negligenciando os ativos de informação. Essa forma de tratar a TI, no entanto, tem se mostrado bastante ineficiente. As instituições que conseguem desenvolver uma metodologia comum para gerenciar os vários ativos, sem deixar nenhuma área desfavorecida, tendem a ter melhor desempenho.

Porém, a área de TI, em especial, tem merecido atenção reforçada e se constituído em um ativo extremamente estratégico para qualquer instituição, com custos e investimentos elevados, tendo papel importante nas tomadas de decisões e posicionamento das corporações no mercado. Este papel estratégico se dá através da dependência crescente das instituições com a tecnologia, tendo em vista que grande parte de seus processos atualmente ocorre através da rede.

A governança de TI surge, então, com o propósito de atender a uma crescente demanda por aplicações e para prover conformidade com marcos regulatórios, proporcionando uma gestão baseada em resultados, um alinhamento com o planejamento estratégico e um retorno sobre o investimento.

A definição de Governança de TI para Weill (Weill, 20006), é: "a especificação dos direitos decisórios e do framework de responsabilidades para estimular comportamentos desejáveis na utilização da TI". O *IT Governance Institute* define o termo da seguinte forma:

"A governança de TI é de responsabilidade da alta administração (incluindo diretores e executivos), na liderança, nas estruturas organizacionais e nos processos que garantem que a TI da empresa sustente e estenda as estratégias e objetivos da organização".

A partir destas duas definições, Fernandes (Fernandes, 2006) conclui que a Governança de TI deve:

•Garantir o alinhamento da TI ao negócio (suas estratégias e objetivos), tanto no que diz respeito a aplicações como à infraestrutura de serviços de TI;

•Garantir a continuidade do negócio contra interrupções e falhas (manter e gerir as aplicações e a infraestrutura de serviços);

•Garantir o alinhamento da TI a marcos de regulação externos como a Sarbanes-Oxley, Baliléia II e outras normas e resoluções.

Atualmente, percebe-se o quão importante é ter uma gestão eficiente dos recursos de TI, com papéis bem definidos e decisões compartilhadas, para que todos possam colaborar com o sucesso da instituição. Esse comprometimento de toda gestão é bem definido por Weill (Weill, 2006), quando ele explica:

"A alta gerência não tem a capacidade de atender a todas as requisições de investimento em Tecnologia da Informação que ocorrem numa grande empresa, quanto mais para envolver-se nas muitas outras decisões relativas à TI. Se os altos executivos tentarem tomar decisões demais, tornar-se-ão um gargalo. Entretanto, decisões tomadas em quaisquer áreas da empresa devem ser consistentes com a direção que a alta gerência escolheu para a organização. Uma Governança de TI cuidadosamente planejada proporciona um processo decisório claro e transparente, que resulta num comportamento consistente com a visão da alta gerência e ao mesmo tempo estimula a criatividade geral".

Fernandes (Fernandes, 2006), entretanto, propõe ir além dessas definições formais, apresentando uma visão da TI através do "Ciclo da Governança de TI", ciclo este subdividido em quatro grupos: alinhamento estratégico e *compliance*,

decisão, estrutura e processos, e medição de desempenho da TI.

O primeiro grupo, referente ao alinhamento estratégico e *compliance,* está relacionado à necessidade de desenvolver um planejamento estratégico para a TI, sempre alinhado com a estratégia geral da instituição, de forma a suportar seus produtos, serviços e segmentos de atuação. Quanto ao *compliance,* a TI deve estar de acordo com os marcos regulatórios externos.

O segundo grupo, que se desdobra em decisão, compromisso, priorização e alocação de recursos, está relacionado às decisões de TI no que se refere à arquitetura, infraestrutura, investimento e necessidades de aplicações. Busca também, o comprometimento dos principais gestores da instituição, na determinação das prioridades dos projetos e serviços, além de almejar distribuir da melhor forma os recursos destinados à TI dentre o seu *portfolio*.

O grupo seguinte, formado por estrutura, processos, operações e gestão, está relacionado à estrutura organizacional e funcional da TI, alinhando-a com a estratégia e operação da instituição. Neste grupo, são definidas e revistas as operações de sistemas, infraestrutura, suporte técnico e segurança da informação.

O último grupo, medição de desempenho, refere-se à determinação, coleta e geração de indicadores de resultados dos processos, produtos e serviços de TI e à sua contribuição para as estratégias e objetivos do negócio.

Esse ciclo de Governança de TI vem atender o principal objetivo da Governança de TI, que Fernandes (Fernandes, 2006) define como: "alinhar a TI aos requisitos do negócio". Esse alinhamento tem como base a continuidade do negócio, o atendimento às estratégias do negócio e o atendimento a marcos de regulação externos.

2.1. Controle Externo da Governança de TI na Administração Pública Federal

O Tribunal de Contas da União – TCU –, através do Acórdão no 1.603/2008-TCU-Plenário, determinou à Secretaria de Fiscalização de Tecnologia da Informação (Sefti) do TCU a realização periódica de levantamentos com o objetivo de acompanhar e manter base de dados atualizada com a situação da governança de TI na Administração Pública Federal, em razão da grave

situação da governança e gestão de TI exposta no levantamento realizado no ano de 2007. Apesar de um novo levantamento ter sido realizado em 2010, constatou-se que inúmeros problemas ainda persistiam.

A situação da governança de TI foi avaliada a partir da coleta de informações em questionário disponibilizado a instituições representativas de diversos segmentos da Administração Pública Federal. A definição dos tópicos avaliados e os critérios utilizados fundamentaram-se em: legislação, normas técnicas da ABNT (ABNT NBR ISO/IEC 27002:2005 – segurança da informação e ABNT NBR ISO/IEC 38500:2009) e modelos de boas práticas reconhecidos internacionalmente, em especial o Cobit 4.1 (*Control Objectives for Information and Related Technology*).

A área de segurança da informação, por exemplo, chamou a atenção pelos altos índices de não-conformidade, sugerindo que, de forma geral, as organizações públicas, além de não tratarem os riscos aos quais estão expostas, os desconhecem.

Verificou-se, ainda, através do levantamento do ano de 2010, que os conceitos de governança de TI ainda são pouco difundidos na maioria da instituições públicas federais e que, de forma geral, a alta administração não se considera responsável pelas políticas corporativas de TI e nem por prover a estrutura básica para que a sua governança seja efetiva.

No Acórdão no 1.603/2008-TCU-Plenário, foram produzidas recomendações estruturantes nos seguintes temas: planejamento estratégico institucional e de TI; estrutura de pessoal de TI; segurança da informação; desenvolvimento de software; gestão de níveis de serviço; processos de contratação e gestão de contratos de TI; processo orçamentário de TI; e auditoria de TI.

Relacionado ao primeiro tema, o TCU recomendou que as instituições da administração pública federal promovessem ações com o objetivo de disseminar a importância do planejamento estratégico, procedendo, inclusive, mediante orientação normativa, ações voltadas à implantação e/ou aperfeiçoamento de planejamento estratégico de TI e comitê diretivo de TI, com vistas a propiciar a alocação dos recursos públicos conforme as necessidades e prioridades da organização.

As recomendações com relação à estrutura de pessoal de TI foram para que

as instituições atentem para a necessidade de dotar uma estrutura com quantitativo de servidores efetivos necessário ao pleno desempenho das atribuições de setor, garantindo, outrossim, sua capacitação, como forma de evitar o risco de perda de conhecimento organizacional, pela atuação excessiva de colaboradores externos não comprometidos com a instituição.

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

Uma seguinte recomendação estimula a adoção de metodologia de desenvolvimento de sistemas, procurando assegurar níveis razoáveis de padronização e bom grau de confiabilidade e segurança.

A gestão de níveis de serviço foi um outro tema abordado, ao recomendar a promoção de ações voltadas à implantação e/ou aperfeiçoamento de gestão de níveis de serviço de TI, de forma a garantir a qualidade dos serviços prestados internamente, bem como a adequação dos serviços contratados externamente às necessidades da organização.

Com relação aos processos de contratação e gestão de contratos de TI, o TCU recomenda que sejam envidados esforços visando à implementação de processo de trabalho formalizado de contratação de bens e serviços de TI, bem como de gestão de contratos de TI, buscando a uniformização de procedimentos.

O tema relacionado ao processo orçamentário de TI foi abordado através da recomendação de que sejam adotadas providências com vistas a garantir que as propostas orçamentárias para a área de TI sejam elaboradas com base nas atividades que efetivamente pretendem realizar e alinhadas aos objetivos dos negócio.

Finalmente, o tema de auditoria de TI teve recomendação para que se fossem introduzidas práticas voltadas à realização de auditorias de TI, que permitam a avaliação regular da conformidade, da qualidade, da eficácia e da efetividade dos serviços prestados.

2.2. Controle Externo da Governança de TI na Administração Pública do Estado do Ceará

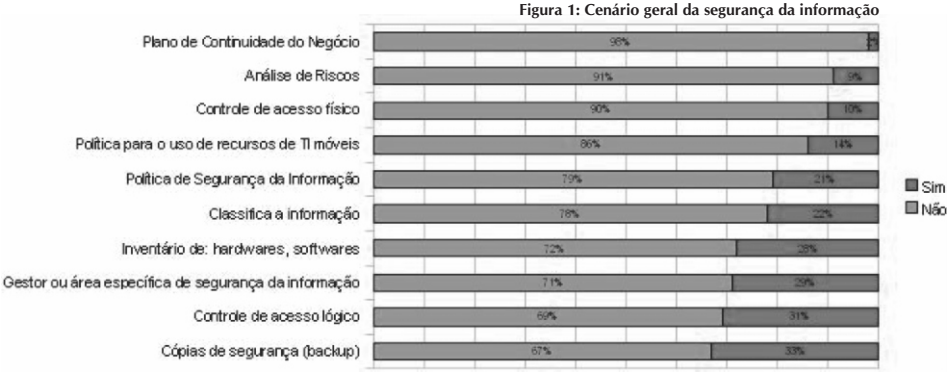
Levantamento semelhante foi realizado no âmbito da administração pública do estado do Ceará através da 13a Inspetoria de Controle Externo do Tribunal de Contas do Estado do Ceará em dezembro de 2009 (CEARÁ, 2011). O objetivo principal deste levantamento foi coletar informações relevantes sobre a Governança de TI no estado do Ceará para subsidiar os trabalhos futuros da Comissão Especial de Auditoria de Tecnologia da Informação (atual 13a Inspetoria de Controle Externo), constituída no âmbito desta Corte de Contas, nas atividades de fiscalização da gestão e do uso de recursos de Tecnologia da Informação e Comunicação (TIC) pela Administração Pública Estadual.

Para a realização deste trabalho, foram selecionados para o levantamento todos os jurisdicionados do TCE-CE, totalizando 58 órgãos/entidades que compõem a Administração Pública estadual. Dessa relação, constaram as secretarias, órgãos auxiliares de assessoramento, autarquias, fundações, empresas públicas e empresas de economia mista, que compõem o Poder Executivo, o Tribunal de Contas dos Municípios (TCM), o Tribunal de Justiça do Ceará (TJCE), a Assembleia Legislativa do Ceará (AL), a Procuradoria Geral de Justiça do Ceará (PGJ) e o Tribunal de Contas do Estado do Ceará (TCE-CE). Os órgãos/entidades responderam a um questionário eletrônico, disponível em plataforma Web via Internet, composto de 37 perguntas objetivas, baseadas nas normas técnicas brasileiras sobre segurança da informação (NBR ISO/IEC 27002:2005) e gestão de continuidade de negócios (ABNT, 2007), no *Control Objectives for Information and related Technology* 4.1 (COBIT 4.1), no *Project Management Body Of Knowledge* (PMBOK), e na norma técnica brasileira sobre gerenciamento de serviços (ABNT, 2008), dentre outros processos relacionados a TI.

Nesse levantamento, foram identificados os principais problemas de Governança de Tecnologia da Informação na Administração Pública Estadual nas seguintes áreas: Planejamento Estratégico Institucional e de TI; Segurança da Informação; Processo de Desenvolvimento de Software; Estrutura de Pessoal de TI; Auditoria de TI; Gerência de Projetos; Gerenciamento de Serviços; Processo de Gestão de Contratos de TI e Processo Orçamentário de TI.

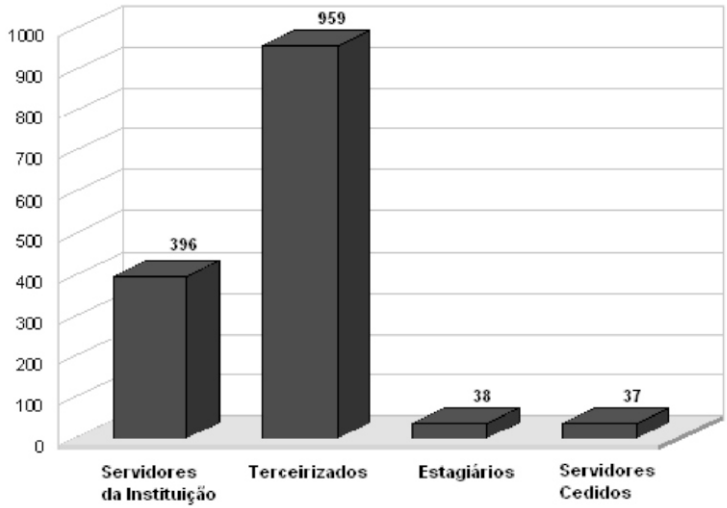
A segurança da informação, por exemplo, como foi demonstrado na pesquisa, encontra-se crítica nos órgão/entidades da Administração Pública estadual. A falta de planejamento e de cultura organizacional no tema contribuem para a existência desse cenário. Vários foram os problemas encontrados, tais como a falta de um controle de acesso físico e lógico, a não existência de procedimentos para a classificação das informações, a falta de uma política de segurança, até a não implementação de cópia de segurança das informações. Vale destacar a falta de um plano de continuidade em praticamente todos os pesquisados e a falta de uma análise de risco dos serviços de TI. A Figura 1, a seguir, mostra o cenário geral da situação da segurança da informação nos órgãos/entidades pesquisados, com temas (questões) ordenados de forma decrescente pelo nível de criticidade em que se encontram.

Figura 1: Cenário geral da segurança da informação



Os dados demonstraram ainda que a grande maioria (67%) dos colaboradores que trabalha na área de TI são terceirizados, totalizando 959. Com uma quantidade bem menos expressiva (396), os servidores próprios da instituição representam 27% do total apurado, enquanto os estagiários, num total de 38, representam 3%. Finalmente, em número de 37, os servidores públicos cedidos de outras instituições, totalizaram 3% dos colaboradores que trabalham na área de TI. A Figura 2 apresenta a relação existente entre esses diferentes vínculos.

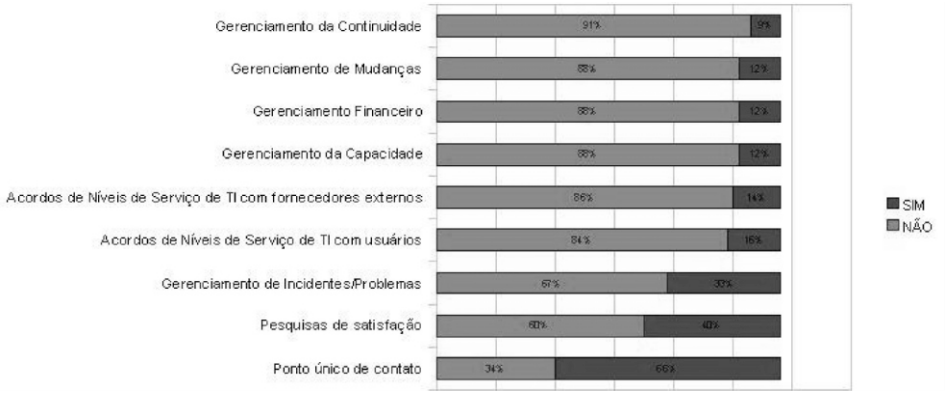
Figura 2: Distribuição dos colaboradores de TI por tipo de vínculo



Quanto ao processo de Gerenciamento de Serviços, a maioria dos pesquisados (86%) informou que não realiza formalmente a gestão de níveis de serviço dos serviços contratados, ou seja, mesmo quando a área de TI da instituição é cliente e não fornecedor, não há preocupação com a avaliação e o controle dos resultados. Considerando que um serviço contratado pela área de TI visa a atender às necessidades dos seus usuários, a ausência da gestão dos fornecedores externos resulta em usuários insatisfeitos, baixa qualidade dos serviços e investimentos inadequados.

A Figura 3, a seguir, mostra a situação geral do Gerenciamento de Serviços de TI na Administração Pública estadual, com temas (questões) ordenados de forma decrescente pelo nível de criticidade em que se encontram.

Figura 3: Situação geral do Gerenciamento de Serviços de TI na Administração Pública Estadual



O levantamento completo e detalhado pode ser encontrado na síntese de auditoria; "Levantamento acerca da situação da Governança de Tecnologia da Informação na Administração Pública Estadual" [referência], tendo sido um conjunto de recomendações e determinações produzidas através da Resolução No 3550/2010 TCE-CE (CEARÁ, 2012a). O teor da resolução permitirá aos gestores de TI priorizar as ações necessárias para melhorar a Governança de TI nos órgãos/entidades jurisdicionados, adequar-se às normas vigentes na Administração Pública estadual e às melhores práticas da área, além de servir de instrumento acessório nas negociações junto à alta administração por recursos orçamentários para a área.

Conclusões

A Governança de TI pode ser vista como um conjunto de iniciativas que fornecem a base para o gerenciamento estratégico da tecnologia da informação dentro das instituições, elevando o nível de maturidade dos processos e garantindo o suporte tecnológico necessário para que a instituição atinja seus objetivos estratégicos.

Através do alinhamento entre os processos de TI e os objetivos estratégicos da instituição, é possível gerar um ambiente favorável à criação de valor. A TI passa, então, a contribuir de forma estratégica, ajudando a agregar valor aos

produtos e serviços ofertados.

Em face desse perfil estratégico que a TI vem assumindo, faz-se necessário avaliar a correta utilização da Tecnologia da Informação através da realização periódica de auditorias independentes. Nesse sentido, no âmbito das administrações públicas, os Tribunais de Contas têm se estruturado no sentido de dotar suas Cortes de pessoal qualificado para atuar nesse segmento.

Levantamentos realizados, entretanto, no âmbito da esfera federal, através do TCU, e do Estado do Ceará, através do TCE-CE, têm apontado para inúmeras deficiências na área de Governança de TI, possibilitando, portanto, grandes oportunidades de melhorias na gestão e no uso de recursos de Tecnologia da Informação por parte das instituições públicas.

Referências

ABNT. NBR ISO/IEC 15999-1:2007 - Gestão de Continuidade de Negócios.

ABNT. NBR ISO/IEC 20000-2:2008 - Tecnologia da Informação – Gerenciamento de Serviços – Código de Prática.

ABNT. NBR ISO/IEC 27002:2005 - Tecnologia da Informação – Técnicas de Segurança – Código de prática para a gestão da segurança da informação.

ABNT. NBR ISO/IEC 38500:2009 - Governança Corporativa de TI.

BRASIL, Tribunal de Contas da União. Levantamento de Governança de TI 2010 / Relator Ministro Aroldo Cedraz - Brasília : TCU, 2010a.

BRASIL, Ministério do Planejamento, Orçamento e Gestão / Secretaria de Logística e Tecnologia e Informação - SLTI. Instrução Normativa 04, 2010b.

CEARÁ, Tribunal de Contas. Levantamento acerca da situação da Governança de Tecnologia da Informação da Administração Pública Estadual / Tribunal de Contas do Estado do Ceará. Fortaleza: TCE, 2011.

CEARÁ, Tribunal de Contas. Resolução No 3550/2010 TCE-CE. Disponível em

< http://www.tce.ce.gov.br/sitetce/Sessao.resolucaoATI.tce >. Acessado em: 22 ago. 2012a.

CEARÁ. Decreto Nº 29.227/2008. Institui a Política de Segurança da Informação Governo do Estado do Ceará. Disponível em < http://www.seplag.ce.gov.br /images/stories/Gestao/Tecnologia-da-Informacao-e-Comunicacao/Politicas/ Decreto%2029%20227%2013%20marco%202008%20Politica%20seguranca .pdf >. Acessado em: 23 ago 2012b.

CEARÁ. Decreto Nº 29.644/2009. Instituição das diretrizes da Política de aquisições de serviços de Tecnologia da Informação e Comunicação (TIC) do Governo do Estado do Ceará. Disponível em < http://www.seplag.ce.gov.br/ images/stories/Gestao/Tecnologia-da-Informacao-e-Comunicacao/Aquisicao-de-TIC/decreto29644%20politica%20aquisicoesdetic.pdf >. Acessado em: 23 ago 2012c.

CEARÁ. Instrução Normativa Nº 001/2009. Dispõe sobre as aquisições de serviços de Tecnologia da Informação e Comunicação (TIC) pela Administração Pública Estadual do Governo do Estado do Ceará. Disponível em < http://www.seplag.ce.gov.br/images/stories/Gestao/Tecnologia-da-Informacao-e-Comunicacao/Aquisicao-de-TIC/Instrucao-normativa-012009de12%2003%2009%20aquisicoes%20servicos%20tic.pdf >. Acessado em: 23 ago 2012d.

DIAS, C. **Segurança e Auditoria da Tecnologia da Informação**. 1ª Edição, AXCEL BOOKS, 2000.

FERNANDES, A.A.; ABREU, V.F. **Implantando a governança de TI**: da estratégia à gestão dos processos e serviços. Rio de Janeiro: Brasport, 2006.

ISACA. CISA **Review Manual** 2012. ISACA, USA, 2012.

LYRA, M. R. **Segurança e Auditoria de Sistemas de Informação**. Rio de Janeiro, Editora Ciência Moderna LTDA , 2008.

SCHMIDT, P.; SANTOS, J. L.; ARIMA, C. H. **Fundamentos de Auditoria de Sistemas**. São Paulo, Atlas , 2006. (Coleção resumos de contabilidade, v.9).

WEILL, Peter; ROSS, Jeanne. **Governança de TI, Tecnologia da Informação**. M.Books do Brasil, São Paulo, 2006.