Auditoria de Tecnologia da Informação – A Experiência do TCE-CE

Paulo Alcântara Saraiva Leão
Mestre em Ciências em Engenharia de Sistemas e Computação pela COPPE/UFRJ. MBA em Gestão Empresarial pela FGV. Analista de Gestão da TI da Empresa de Tecnologia da Informação do Ceará – ETICE. Secretário Executivo do Instituto Escola Superior de Contas e Gestão Pública Ministro Plácido Castelo. Coordenador da Comissão Especial de Auditoria de Tecnologia da Informação do Tribunal de Contas do Estado do Ceará, no período de julho de 2009 a agosto de 2011.

Resumo: O presente artigo tem como propósito apresentar a experiência de implantação da área de auditoria de Tecnologia da Informação no Tribunal de Contas do Estado do Ceará (TCE-CE). O controle externo sobre a governança e o uso dos recursos de Tecnologia da Informação (TI), bem como os processos de aquisição dos mesmos no âmbito da Administração Pública estadual, é de extrema importância, uma vez tratar-se de área estratégica, de alto teor técnico, de grande dinamicidade e que envolve recursos financeiros significativos dentro dos orçamentos públicos.

O objetivo maior com a implantação de uma área de auditoria de TI no TCE-CE foi buscar garantir que os recursos destinados a essa área, dentro da Administração Pública, sejam corretamente aplicados. Teve também o intuito de contribuir para a boa governança da TI na Administração Pública estadual, em benefício da sociedade. Neste contexto, o TCE-CE espera introduzir uma visão de auditoria de TI não limitada apenas ao regramento legal, mas também com ênfase na verificação da efetividade dos resultados dos programas, projetos, processos e atividades de TI, que dão suporte à aplicação de políticas públicas.

Neste artigo, são apresentadas as motivações que justificaram a criação desta nova área, sua estrutura organizacional, ações realizadas, competências, atribuições, processo de trabalho; e finalmente os resultados e benefícios alcançados com sua atuação.

Palavras-chave: auditoria; auditoria governamental; tecnologia da informação; TI; Tribunal de Contas do Estado do Ceará, TCE-CE; administração pública.

Introdução

A crescente utilização das novas tecnologias tem provocado uma forte dependência das organizações atuais com os sistemas informatizados. Essa dependência é consequência da quantidade e complexidade dos sistemas computacionais que controlam os mais variados tipos de operações e o próprio fluxo de informações das organizações. O TCE-CE e os órgãos e entidades sob sua jurisdição não são uma exceção neste cenário, uma vez que utilizam intensamente a Tecnologia da Informação para automatizar seus processos, além de gerar e manter informações.

O processo de modernização pelo qual vem atravessando a Administração Pública do Estado do Ceará, ao longo dos últimos anos, tem estado intrinsecamente relacionado ao uso da Tecnologia da Informação, o que vem provocando sensíveis alterações no funcionamento do Estado, sob diferentes aspectos, principalmente nos processos organizacionais; armazenamento, tratamento e disseminação de informações; capacitação profissional; e no relacionamento entre o governo e a sociedade e entre os órgãos públicos. Verifica-se ainda uma maior aplicação do governo eletrônico e um crescente aumento da utilização de redes sociais como forma de interação com a sociedade. No caso específico do Estado do Ceará, iniciativas do governo estadual, tais como o Cinturão Digital, Sistema de Gestão Governamental por Resultados - S2GPR, sistema de compras pela Internet, virtualização de processos, entre outras, fortalecem a certeza de que essa tendência tende a se acentuar.

A informatização crescente reclama, portanto, especial atenção das organizações, uma vez que a utilização da Tecnologia da Informação para manipulação e armazenamento de dados tem adquirido um caráter crítico na medida em que são introduzidos novos riscos e aumenta-se a fragilidade de algumas atividades. Assim, torna-se essencial a atenção dos gestores públicos para as questões relacionadas à segurança da informação, qualidade de software e disponibilização de sistemas informatizados ao público.

A TI desempenha, portanto, um papel cada vez mais importante no suporte aos processos e no apoio à tomada de decisões nas organizações. No setor público, típico prestador de serviços à sociedade, a TI é especialmente relevante

porque suporta decisões relativas a políticas públicas e à aplicação de recursos públicos. São portanto decisões que afetam diretamente a vida de muitas pessoas, ou mesmo de toda a sociedade. Nesse sentido, podemos dizer que o uso da TI é estratégico para os governos.

Nesse sentido, o TCE-CE tomou a decisão estratégica de implantar uma área de auditoria de TI, com o objetivo de buscar garantir que os recursos destinados a programas, projetos, processos e atividades baseados em TI, dentro da Administração Pública estadual, sejam bem aplicados. Igualmente importante é buscar garantir que a TI seja corretamente administrada, com uma boa governança, buscando sempre aprimorar os resultados alcançados a partir de sua utilização, sempre em benefício da gestão pública e, em última análise, da população. Neste contexto, o TCE-CE busca introduzir uma visão de auditoria de TI que, além do aspecto puramente contábil e legal, também tivesse foco nos resultados efetivamente alcançados pelas ações de TI, que dão suporte à aplicação de políticas públicas.

Obviamente mantendo o aspecto fiscalizatório dos trabalhos, no primeiro momento, o TCE-CE decidiu, quando cabível e legalmente respaldado, adotar uma abordagem mais orientativa que punitiva, considerando o ineditismo do tema para os jurisdicionados e entendendo que investimentos em TI muitas vezes demandam tempo para serem concretizados. No que concerne à governança de TI, por exemplo, optou-se algumas vezes por dar prazos ou exigir planos e cronogramas, para que o jurisdicionado se adequasse (obtivesse conformidade) aos padrões desejáveis e recomendados, antes de aplicar penalidades. Durante e após os prazos dados, o TCE-CE realiza acompanhamentos periódicos para avaliar a implementação das recomendações e determinações proferidas pelo Tribunal.

Espera-se com isso que os gestores públicos, ao implementarem projetos baseados em TI, não só apliquem corretamente os recursos, mas também contribuam com a efetiva melhoria de qualidade da prestação dos serviços públicos, com o aperfeiçoamento dos processos intra e intersetoriais, e com o aumento da transparência dos atos governamentais.

Porque auditar TI

Dentro desse contexto, a importância de se fiscalizar a gestão e o uso da TI

nas administrações públicas deve-se basicamente a três motivos principais: a importância estratégica da TI dentro das organizações governamentais, considerando a relevância da informação para a gestão pública e o processo de tomada de decisão; a complexidade da TI, devido ao seu alto grau de tecnicidade e dinamicidade de atualização; e os valores financeiros gastos com aquisições de bens e serviços de TI, que são significativos dentro dos orçamentos públicos de investimento e custeio.

Informação é estratégica

A TI é estratégica para as organizações, pois é através de sua utilização que são criadas, gerenciadas e recuperadas as informações utilizadas nas atividades diárias e no planejamento de ações futuras. Como informação é um fator cada vez mais estratégico para uma correta tomada de decisão, a TI deve ser tratada com esse enfoque. Hoje em dia, é praticamente impossível pensar em dados e informações que não estejam armazenados em documentos digitais e bancos de dados, e sejam manipulados através de programas e sistemas computadorizados. Por esse motivo, entendemos que a auditoria de TI deve ser considerada estratégica, pois pode ajudar a prevenir problemas de má gestão pública, uma vez que as decisões são tomadas com base nas informações existentes nos órgãos e entidades governamentais. Tais informações precisam ser íntegras e confiáveis.

Complexidade da TI

A área de TI, devido a sua tecnicidade elevada, torna-se relativamente complexa para os procedimentos de auditoria administrativos, contábeis e financeiros tradicionais, e para o público leigo. De forma geral, um auditor governamental padrão não possui o nível de especialização necessário para auditar essa área. Nesse sentido, para um bom resultado dos trabalhos de controle externo nessa área, os auditores precisam ser especializados, visando a atender às competências necessárias ao desempenho das funções, através de um processo permanente de capacitação.

Aquisições de TI podem às vezes suscitar uma avaliação subjetiva e de mensuração não trivial. A própria avaliação dos resultados de projetos também

não é simples, pois muitos dos resultados obtidos com o uso da tecnologia são intangíveis, sendo, portanto, de difícil mensuração. Melhoria da qualidade de um serviço e agilização de um determinado processo são exemplos de resultados que podem ser alcançados com a implantação de um novo sistema de informação, por parte de um órgão público, e que às vezes são difíceis de mensurar. No entanto, mesmo nesses casos, há técnicas para a avaliação dos resultados e até mesmo cálculo do retorno dos investimentos realizados. A área de auditoria de TI do TCE-CE deverá não apenas fiscalizar se o processo de aquisição foi feito de forma regular, seguindo os princípios da Administração Pública (legalidade, impessoalidade, moralidade, publicidade, economicidade, isonomia, eficiência, etc), mas, sim, também avaliar se aquela ação teve retorno para o governo e se gerou resultados efetivos para a população.

Diante do exposto, faz-se necessário, portanto, que as aquisições que envolvam bens e serviços de TI sejam auditadas de forma especial, por equipe especializada, possuindo competências muitas vezes bastante específicas.

Valores significativos

Em muitos casos, os valores gastos pela Administração Pública com TI são significativos dentro do conjunto das despesas públicas. Aquisições de tecnologia podem, algumas vezes, requerer recursos financeiros elevados, quando proporcionam alto valor agregado às atividades do governo. Para que efetivamente proporcione estes benefícios, a TI precisa ser bem utilizada, tendo seu uso otimizado ao máximo, evitando desperdício ou subutilização. Além disso, a avaliação do custo correto para um projeto de TI pode não ser uma tarefa fácil de ser feita, devido à complexidade e tecnicidade envolvidas.

Diante do exposto, faz-se necessário, portanto, que as aquisições que envolvam bens e serviços de TI sejam auditadas de forma ampla, considerando não só os valores empregados, mas também a qualidade dos bens e serviços adquiridos, o nível de qualidade dos produtos gerados, a garantia da segurança da informação, os prazos e condições impostos pela gestão pública e o alcance dos benefícios obtidos.

Fase inicial : a Comissão

Ciente da necessidade de se fiscalizar o uso e gestão da TI na Administração Pública, o TCE-CE decidiu, então, iniciar uma atuação nessa área. Em agosto de 2008, foi criada a orientação de Auditoria de TI para a especialidade "Auditoria, Fiscalização e Avaliação da Gestão Pública", na área "Controle Externo" do cargo de Analista de Controle Externo do TCE-CE, através de Resolução Administrativa TCE Nº 005/2008.

Para dar início efetivo às atividades, foi criada em fevereiro de 2009, por meio da Resolução Administrativa TCE Nº 001/2009, a Comissão Especial de Auditoria de Tecnologia da Informação, no âmbito da Secretaria de Controle Externo, destinada a realizar auditorias de TI, com a finalidade de fiscalizar a gestão e o uso de recursos da TI pela Administração Pública estadual. A área de auditoria de TI teve, portanto, sua atuação delimitada dentro do conjunto de jurisdicionados do TCE-CE.

Após realização de concurso público, tomaram posse em junho de 2009 os novos analistas de controle externo na área de auditoria de TI, sendo os mesmos incorporados à Comissão Especial de Auditoria de TI, conforme Ato da Presidência do TCE-CE Nº 18/2009, de 2 de julho de 2009. A Comissão ficou, então, composta de 5 (cinco) integrantes, sendo ampliada posteriormente para 6 (seis), todos servidores efetivos da casa, mais um coordenador (o autor que vos fala), detentor de cargo comissionado do Tribunal.

A estruturação da área por meio de uma comissão foi a opção adotada pelo TCE-CE na fase inicial de implantação da área, por ser de mais fácil e rápida implementação. No entanto, acreditávamos que, em um futuro breve, a partir do volume e relevância dos trabalhos desempenhados, seria plenamente justificável a estruturação da área de auditoria de TI nos moldes de uma Inspetoria de Controle Externo (ICE). Como uma ICE, a área estaria mais bem estruturada organicamente dentro do padrão dos setores executivos do controle externo do TCE-CE. De fato, em 2011 foi criada uma ICE específica para auditar TI.

No caso do Tribunal de Contas da União (TCU), por exemplo, a área de auditoria de TI daquela Corte de Contas, teve início como um grupo de trabalho. Com os resultados obtidos, a área foi gradativamente crescendo de importância, ocupando níveis cada vez mais altos na estrutura hierárquica do Tribunal. Desde

2006, está estruturada como uma secretaria, a Secretaria de Fiscalização de Tecnologia da Informação (SEFTI).

Além do TCU, foram realizadas consultas a sítios de outras instituições que são referência na área de auditoria, durante a fase inicial de estruturação da Comissão (ver relação no Anexo I).

A Comissão funcionou no período de 08/07/2009 a 31/08/2011, quando foi extinta e suas atribuições transferidas para a 13ª ICE, que havia sido instituída em 22/03/2011, por meio da Resolução Administrativa TCE Nº 02/2011, com a finalidade específica de realizar auditorias de TI.

Competências

As seguintes competências foram estabelecidas para a área de auditoria de TI:

- Fiscalização, levantamento, acompanhamento, avaliação, inspeção e auditoria na gestão e no uso de recursos da Tecnologia da Informação pela Administração Pública estadual;
- Representação de irregularidades ou ilegalidades relativas à gestão e ao uso de recursos da Tecnologia da Informação pela Administração Pública estadual;
- Realização de pesquisas e o desenvolvimento de técnicas, métodos e padrões para orientar as fiscalizações em sua área de competência;
- Desenvolvimento de rotinas, procedimentos, normas, manuais e ações relativas a projetos de TI financiados com recursos estaduais, bem como as que visem ao aperfeiçoamento das atividades decorrentes de suas competências;
- Análise e emissão de laudos técnicos nos processos relativos à área de TI encaminhados pelos Gabinetes de Conselheiros, Gabinetes de Auditores, Gabinetes de Procuradores do Ministério Público de Contas, ou pela Secretaria de Controle Externo do TCE-CE;
- Emissão de pareceres técnicos, quando solicitada, para subsidiar o processo interno de contratação de bens e serviços de TI no âmbito do TCE-CE;
- Planejamento, coordenação e execução de auditoria nos sistemas

computacionais do TCE-CE em conjunto com a controladoria interna.

Para o bom desempenho das atividades, as seguintes competências individuais deverão estar atendidas pelos integrantes do setor:

- Estrutura e funcionamento do TCE-CE;
- Processo de tomada e prestação de contas;
- Técnicas de auditoria;
- Auditoria governamental;
- Auditoria de sistemas;
- Auditoria de Tecnologia da Informação;
- Legislação sobre TI;
- Gestão pública;
- Legislação sobre licitações e contratos;
- Contabilidade e finanças públicas;
- Gestão de projetos;
- Gestão de patrimônio público;
- Conhecimento de padrões, modelos, referências e técnicas relativas à área.

Além dos temas acima, outros poderão ser agregados conforme o necessário e de acordo com a evolução técnica da área. Para o atendimento das competências, as capacitações das pessoas envolvidas são supridas pelo Instituto Escola Superior de Contas e Gestão Pública Ministro Plácido Castelo (IPC), órgão do TCE-CE.

Atribuições

Dentre as atribuições definidas para a área de auditoria de TI, podemos citar:

- Auditar programas, projetos, processos e atividades de TI nos jurisdicionados, de acordo com as áreas de auditoria definidas (ver mais adiante neste texto);
- Auditar processos de aquisições de TI, gestão de contratos e convênios de TI, gestão de fornecedores de TI, processos de terceirização de TI, bem como outros processos específicos da área;
- Realizar inspeções em campo, quando necessário;

- Emitir pareceres técnicos;
- Propor resoluções e outras regulamentações sobre a área de TI dos jurisdicionados;
- Participar do Processo de Prestação e Tomada de Contas dos jurisdicionados;
- Participar de auditorias solicitadas pela Assembléia Legislativa;
- Realizar auditorias operacionais;
- Interagir com outros órgãos de controle da Administração Pública;
- Apresentar palestras e participar de eventos relacionados ao tema;
- Promover eventos;
- Publicar orientações e entendimentos relativos à área de auditoria de TI;
- Editar recomendações de boas práticas de governança de TI, gestão de TI, qualidade de software, governo eletrônico, segurança da informação, dentre outros temas;
- Realização de consultas públicas sobre planejamento na área de TI pública, governança de TI, segurança da informação, novas tecnologias, melhores práticas em TI e outros temas correlatos.

Ações realizadas

No âmbito da então Comissão Especial de Auditoria de TI, foram realizadas diversas ações e projetos com o objetivo de estruturar esta nova área de conhecimento dentro do TCE-CE. Dentre as principais iniciativas, podemos citar:

- Elaboração do projeto de implantação da área de auditoria de TI no TCE-CE;
- Definição dos objetivos, atribuições e competências da área e da equipe;
- Organização dos trabalhos da Comissão, compreendendo:

    - Identificação das áreas de auditoria a serem trabalhadas prioritariamente; seleção de objetos para cada área identificada; definição de escopos de auditoria; identificação de pontos de controle para auditoria de TI e sistemas de informação; estabelecimento de método de acompanhamento dos trabalhos (reuniões de avaliação, relatórios, etc); definição do processo de auditoria de Tecnologia da

Informação a ser adotado, contemplando as entradas, os critérios, as técnicas de auditoria e os produtos gerados; definição das normas, procedimentos e modelos de documentos a serem utilizados, com base nos padrões do TCE-CE; dentre outros;

- Elaboração do Plano de Capacitação e Certificação para os Auditores de Tecnologia da Informação;
- Compilação do marco regulatório de Tecnologia da Informação da Administração Estadual e Federal;
- Pesquisa em sítios de órgãos e consulta a publicações relacionadas com a área de auditoria de TI;
- Pesquisa e estudo comparativo em metodologias, padrões e melhores práticas na área de auditoria de TI;
- Participação de analistas em cursos e eventos da área;
- Elaboração da Metodologia de Seleção de Auditorias de TI;
- Visita à Secretaria de Fiscalização de TI (SEFTI) do Tribunal de Contas da União (TCU), para conhecimento e estabelecimento de contatos;
- Desenvolvimento do sítio web da Comissão no Sitio Institucional do TCE-CE;
- Elaboração de estudo para auditoria sem papel no escopo de atuação do TCE-CE;
- Realização do diagnóstico "Levantamento acerca da situação da Governança de Tecnologia da Informação na Administração Pública Estadual";
- Realização do Seminário "Governança de Tecnologia da Informação na Administração Pública Estadual" com os jurisdicionados do TCE-CE em 08/04/2011;
- Contratação de consultoria especializada para estabelecimento de planos, processos e métodos de trabalho.

Capacitações

- Capacitações em "Contratação/Aquisição de Bens e Serviços de TI" e "Formação de Auditores Líderes em Segurança da Informação – ISO/IEC 27.001:2005" (realizadas como parte da consultoria contratada);

- Curso preparatório para a certificação "Certified Information Systems Auditor (CISA)". A certificação profissional CISA é reconhecida mundialmente como um padrão para os profissionais que exercem auditoria, controle, monitoramento e avaliação dos sistemas de informação nas organizações;
- Capacitação em auditoria governamental (ministrado por técnicos do Tribunal de Contas da União - TCU);
- Outras capacitações (Cobit, Direito Digital, etc).

Certificações

- Obtenção, pelos membros da Comissão, da certificação "Auditor Líder em Segurança da Informação – ISO 27.001".

Levantamento da Governança de TI na Administração Pública Estadual

Uma das ações mais relevantes realizadas pela Comissão foi a realização do diagnóstico "Levantamento acerca da situação da Governança de Tecnologia da Informação na Administração Pública Estadual", que teve como objetivo traçar um perfil, ou "tirar uma fotografia", da situação da governança de TI nos órgãos e entidades estaduais.

A forma de realizar o diagnóstico foi por meio de um questionário eletrônico enviado aos jurisdicionados, que o responderam via interface web, disponibilizada no sítio da Comissão. Com essa estratégia adotada, conseguimos que a totalidade dos jurisdicionados participassem do levantamento, respondendo as questões postas.

A relação das questões apresentadas aos jurisdicionados pode ser consultada no Anexo II.

Após as respostas serem recebidas, a equipe tabulou os dados, gerou gráficos e compilou suas conclusões em um relatório de inspeção, que foi analisado por um conselheiro, que relatou o processo e o apresentou no Pleno do Tribunal. O Pleno, ao apreciar o relatório do Relator, emitiu a Resolução TCE Nº 3550/2010, com determinações e recomendações a serem seguidas por todos os jurisdicionados. O cumprimento às decisões tomadas pelo Tribunal vem sendo acompanhado atualmente pela 13ª ICE.

O perfil traçado no levantamento tem servido de base para os trabalhos da área de auditoria de TI, principalmente como subsídio na seleção das fiscalizações a serem conduzidas.

Este trabalho gerou um documento integrante da coleção "Síntese de Auditoria" do TCE-CE, que pode ser consultado no sítio institucional do TCE-CE na Internet, na área destinada à auditoria de TI.

Consultoria para definição de procedimentos e métodos

Para a estruturação da área de auditoria de TI, entendeu-se como necessária a definição dos procedimentos e métodos de trabalho sob a responsabilidade da Comissão. Esta ação ajudou a padronizar os procedimentos realizados nas diversas atividades de auditoria, bem como trouxe maior produtividade e efetividade aos trabalhos da área.

Com financiamento do Banco Mundial, foi contratada uma consultoria especializada na área para desenvolver, conjuntamente com a equipe de auditores da Comissão, os ditos procedimentos e métodos, além de realizar o planejamento estratégico do setor e ministrar alguns cursos.

Os produtos desenvolvidos pela empresa de consultoria contratada foram os seguintes:

- Plano Estratégico de Auditoria de TI (2011-2015);
- Manual de Auditoria de TI;
- Procedimento de Auditoria de TI, contemplando:
    - 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;
    - Auditoria de Segurança da Informação;
- Realização dos cursos "Contratação/Aquisição de Bens e Serviços de TI" e "Formação de Auditores Líderes em Segurança da Informação – ISO/IEC 27.001:2005"

Processo de Trabalho

O processo de trabalho estabelecido para a realização das auditorias de TI pela Comissão seguiu o mesmo padrão de trabalho das Inspetorias de Controle Externo do TCE-CE (as ICE´s), dentro do âmbito da Secretaria de Controle Externo.

Como base desse processo, foi desenvolvida uma metodologia para a seleção das auditorias a serem realizadas. A metodologia visa a tornar o processo de identificação de auditorias mais formal e objetivo, reduzindo o empirismo e evitando decisões com base em critérios subjetivos. Mais adiante neste texto, apresentamos a metodologia de forma detalhada.

As fiscalizações realizadas nos jurisdicionados são de dois tipos básicos: "*ex-ante*" e "*ex-post*". As ações "*ex-ante*" podem ser iniciadas em qualquer tempo, por iniciativa da própria área de auditoria de TI, a partir de critérios e condições identificadas em planejamentos e diagnósticos prévios, visando a uma atuação pró-ativa. Já as ações "*ex-post*" têm um caráter reativo e podem acontecer a partir de denúncias, solicitações da Assembleia Legislativa, representações ou mesmo dentro do processo normal de prestação e tomada de contas.

Nos trabalhos de fiscalização são adotados os padrões, normas e modelos de referência mais utilizados para a área de TI, e observadas as melhores práticas do setor consagradas internacionalmente. Além do padrão COBIT (*Control Objectives for Information and related Technology*), que deverá ser adotado amplamente para as atividades de auditoria de TI, outros modelos, tais como ITIL, ISO, ABNT, dentre outros, poderão ser utilizados quando aplicável, e a depender dos objetos e do escopo da auditoria.

A prática de realizar *benchmark´s* em organizações similares também foi adotada, principalmente durante a fase inicial de funcionamento da Comissão.

A atuação da área de auditoria de TI, a exemplo de como é desempenhado em outros órgãos congêneres, tais como o TCU, buscam orientar, além de fiscalizar, os gestores públicos nas melhores práticas de governança de TI, visando a garantir a correta aplicação dos recursos públicos em projetos e atividades dependentes de TI. Nos trabalhos, os auditores tentam obter respostas para várias perguntas, que poderão traduzir o estado da área de TI dentro da organização do auditado, podendo ser gerados, a partir daí, diversos indicadores

de resultado. Como exemplos de perguntas a serem respondidas pelas auditorias realizadas, podemos citar:

1. Os sistemas de informação e sítios são seguros? Estão bem documentados? Foram desenvolvidos seguindo normas e padrões de qualidade?
2. Os investimentos em TI apresentam relação custo-benefício adequada?
3. Soluções de TI estão sendo usadas convenientemente para dar transparência aos gastos públicos?
4. As regulamentações estão bem elaboradas? Estão amplamente divulgadas e de fácil acesso e leitura? Estão em concordância com normatizações superiores?
5. O modelo de gestão de TI está bem definido e proporcionando uma boa governança de TI?
6. Os processos de aquisição de TI estão em conformidade com os normativos legais? E os contratos e convênios?
7. Há real efetividade nos projetos e ações de governo baseados em TI? A sociedade está realmente sendo direta ou indiretamente beneficiada com o uso dos recursos tecnológicos utilizados?
8. O pessoal da área de TI e usuários dos serviços estão capacitados adequadamente? Estão certificados?

Em prol de uma boa realização das atividades de auditoria, todos os procedimentos seguidos no âmbito da Comissão foram devidamente formalizados e documentados. Isso permite que os trabalhos sejam sempre realizados com método e obedecendo a padrões estabelecidos.

Da mesma forma que as demais áreas do TCE-CE, a área de auditoria de TI também tem seu desempenho mensurado por meio de indicadores de produtividade.

Áreas de Auditoria

As atividades de auditoria de TI no âmbito do TCE-CE foram distribuídas em áreas, visando à categorização dos trabalhos realizados. O intuito com isso foi definir os objetivos e objetos das auditorias. As seguintes áreas são consideradas nas fiscalizações:

ÁREA DE AUDITORIA	OBJETIVO DA AUDITORIA	OBJETOS A SEREM AUDITADOS
Sistemas de Informação	Auditar sistemas de informação e sítios de Intranet/Internet	Sistemas de informação, sítios na Intranet/Internet, etc
Programas, projetos, processos e atividades de TI (resultado para a sociedade)	Fiscalizar se as iniciativas baseadas em TI estão sendo eficazes para a sociedade; se a qualidade dos serviços prestados é aceitável; se estão atingindo os objetivos esperados	Programas, projetos, processos e atividades de TI, sítios e portais na Internet
Aquisições de TI	Verificar se os processos de aquisição de bens e serviços de TI (licitações, adesões a registros de preços, inexigibilidades e dispensas de licitação) estão regulares	Processos de aquisição de bens e serviços de TI
Contratos e convênios de TI	Auditar os contratos e convênios de TI e a gestão de fornecedores	Contratos e convênios de TI
Patrimônio de TI	Auditar o controle patrimonial de TI	Controle patrimonial e inventário de TI
Regulamentação de TI	Avaliar se as regulamentações para a área de TI estão elaboradas de forma adequada, e verificar se o modelo de gestão de TI definido está adequado às melhores práticas de governança de TI	Decretos, instruções normativas, resoluções, políticas, diretrizes, modelos de gestão, outros procedimentos formalizados, etc
Prestação de serviços de TI aos servidores públicos	Averiguar a efetividade da prestação dos serviços públicos baseados em TI aos servidores públicos e outros colaboradores	Sítios na Intranet e sistemas de informação disponibilizados internamente aos colaboradores do governo

ÁREA DE AUDITORIA	OBJETIVO DA AUDITORIA	OBJETOS A SEREM AUDITADOS
Capacitação e competências no uso de recursos de TI	Averiguar se os usuários TI estão capacitados para utilizar adequadamente os recursos disponibilizados (contempla os servidores públicos e os cidadãos)	Planejamento e gestão de capacitação e de competências, sistemas de gestão de treinamentos, resultados de avaliações, e documentações de cursos ministrados
Segurança da Informação	Avaliar a organização da segurança da informação e os controles existentes	Políticas de segurança da informação, controles na área de segurança da informação, capacitação da equipe de TI na área de segurança, dentre outros
Infraestrutura de TI	Investigar sobre a infraestrutura de TI existente, verificando a adequação da mesma às atividades do ente público, inclusive quanto à capacidade de ampliação visando a atender demandas futuras e os controles pertinentes	Descrição da infraestrutura de TI existente, diagramas de rede, Data-Center, controles existentes, modelos e frameworks utilizados, capacitação da equipe de TI no tema, etc

ÁREA DE AUDITORIA	OBJETIVO DA AUDITORIA	OBJETOS A SEREM AUDITADOS
Governança de TI	Auditar o estado atual da governança de TI e verificar os controles existentes	Planejamento Estratégico Institucional, Planejamento Estratégico de TI, Política de Gestão de TI, manuais de governança de TI, registros de acompanhamento e execução dos planejamentos, controles existentes, modelos e frameworks utilizados, capacitação da equipe de TI no tema, etc

TABELA 1 – Áreas de Auditoria

Dentro das diversas áreas de auditoria, deverão ser definidos escopos das auditorias a serem conduzidas. O escopo poderá envolver processos completos dos jurisdicionados ou parte dos mesmos.

Metodologia de Seleção de Auditorias

Para seleção das auditorias de Tecnologia da Informação a serem realizadas nos jurisdicionados do TCE-CE, foi desenvolvida uma metodologia baseada em critérios relativos a características dos objetos a serem auditados. A metodologia teve como finalidade a otimização dos recursos e a padronização dos trabalhos realizados pela Comissão Especial de Auditoria de Tecnologia da Informação. Esta metodologia de seleção permite o planejamento das auditorias que farão parte do Plano Anual de Auditoria do TCE-CE e do Plano de Ações Anual da área de auditoria de TI. Além destas auditorias selecionadas, e com base no quadro efetivo de técnicos da Comissão, também são consideradas, na elaboração do

cronograma de trabalho, auditorias que são determinadas pela Lei Orgânica do TCE-CE e outras que forem identificadas como prioritárias, por outros motivos que não os dos critérios de seleção.

A metodologia para seleção de auditorias de Tecnologia da Informação para o TCE-CE é dividida em 4 (quatro) etapas:

1. Seleção dos trabalhos de auditoria de acordo com 4 (quatro) critérios de seleção: relevância, risco, materialidade e desempenho dos serviços públicos na Internet(conforme Tabela 2);
2. Estudo de viabilidade de execução das auditorias;
3. Priorização dos trabalhos de auditoria;
4. Planejamento das auditorias para o exercício corrente.

1. Seleção dos trabalhos de auditoria de acordo com critérios

1.1. Relevância

▪ No âmbito do Poder Executivo, o analista seleciona os programas, projetos, processos e atividades de TI que sejam aderentes ao critério de relevância, utilizando o sistema de planejamento governamental (no caso do Estado do Ceará, o Sistema de Monitoramento de Ações e Projetos Prioritários – MAPP), além da Lei Orçamentária Anual (LOA) e a Lei de Diretrizes Orçamentárias (LDO). Para os demais poderes, são avaliadas a LOA e LDO. As iniciativas de TI que forem destaque na mídia também devem ser relacionadas neste critério. Para este critério, devem ser relacionadas para a próxima etapa, no mínimo 5 (cinco) auditorias.

1.2. Risco

▪ No âmbito do Poder Executivo, o analista seleciona os programas, projetos, processos e atividades de TI que sejam aderentes ao critério de risco, utilizando o sistema de planejamento governamental, além da LOA e LDO. Para os demais poderes, são avaliadas a LOA e a LDO. As vulnerabilidades detectadas no diagnóstico sobre a governança de TI dos jurisdicionados do TCE-CE, realizada pela Comissão, ou em outras auditorias anteriores, devem servir de insumo para a escolha das áreas e dos órgãos/entidade a serem auditados.

Também deverão ser pesquisados editais e contratos que possuam riscos significativos que justifiquem auditorias. Para este critério, devem ser relacionadas para a próxima etapa, no mínimo 5 (cinco) auditorias.

1.3. Materialidade

▪ No âmbito do Poder Executivo, o analista seleciona os programas, projetos, processos e atividades de TI que sejam aderentes ao critério de materialidade, utilizando o sistema de planejamento governamental, além da LOA e LDO. Para os demais poderes, são avaliadas a LOA e a LDO. Devem ser relacionadas para a próxima etapa, no mínimo 5 (cinco) auditorias.

1.4. Desempenho de Serviços Públicos na Internet

▪ São relacionados 5 (cinco) serviços relevantes disponibilizados na *Internet* pelos jurisdicionados. Os serviços disponibilizados para a sociedade de forma eletrônica devem ser analisados com a intenção de se perceber como eles estão estruturados, e como são avaliados pelo cliente (cidadão-usuário). Para a seleção dos serviços a serem auditados, poderão ser utilizados estudos, pesquisas e *rankings,* como o "*Ranking Sites*", elaborado pelo Governo do Estado do Ceará.

Auditorias anteriores (incluindo o diagnóstico sobre a governança de TI), meios de comunicação (mídia) e outros sistemas de informação governamentais também podem ser utilizados como fontes para identificação de possíveis auditorias dentro dos critérios estabelecidos.

CRITÉRIO	FONTES
RELEVÂNCIA Importância e impacto que um programa, projeto, processo ou atividade de TI tem para a Administração Pública, ainda que não seja financeiramente significativo	MAPP [(1),] LOA / LDO (2), Meios de comunicação (mídia), Auditorias anteriores

CRITÉRIO	FONTES
RISCO Relação entre probabilidade e impacto de ocorrência de eventos indesejáveis advindos do uso e da gestão de sistemas de TI	Editais, Contratos, MAPP [1], LOA / LDO (2) Auditorias anteriores
MATERIALIDADE Importância relativa ou representatividade do volume de recursos envolvidos	MAPP [1], LOA / LDO [2], Sistemas orçamentários e financeiros, Auditorias anteriores
DESEMPENHO DE SERVIÇOS PÚBLICOS NA INTERNET Qualidade da prestação de serviços públicos disponibilizados para a população via Internet	Estudos, Pesquisas, Rankings, Meios de comunicação (mídia), Auditorias anteriores

TABELA 2 – Critérios de Seleção para Trabalhos de Auditoria

1.Monitoramento de Ações e Projetos Prioritários
2.Lei Orçamentária Anual / Lei de Diretrizes Orçamentárias

2. Estudo de viabilidade de execução das auditorias

▪ Após a seleção feita na etapa anterior, o analista deve verificar se existe viabilidade técnica e financeira para a execução das auditorias selecionadas. Nesta etapa, é verificado se será necessária a contratação de alguma assessoria técnica ou consultoria. Deve também ser verificado se existem recursos tecnológicos, de logística, e tempo disponível para a realização das auditorias.

3. Priorização dos trabalhos de auditoria

▪ Nesta etapa, a área de auditoria de TI realiza reuniões para que sejam definidos os trabalhos de auditoria que poderão ser executados no exercício corrente, de acordo com o quadro de pessoal disponível, a demanda de outras atividades internas e a relação das auditorias consideradas viáveis. Devem ser priorizados inicialmente os trabalhos de auditoria que aparecem relacionados em

mais de um critério.

4. Planejamento das auditorias do exercício corrente

▪ Após a priorização das auditorias, é elaborado um Plano Anual de Auditoria de TI, com as auditorias selecionadas, o cronograma e os recursos humanos, tecnológicos e financeiros que serão alocados para cada trabalho. Neste momento, são alimentados o Plano Anual de Auditoria do TCE-CE e o Plano de Ações anuais da área de auditoria de TI. Oportunamente, outras auditorias poderão ser incluídas no Plano Anual de Auditoria de TI, durante o exercício, a partir de novas demandas da própria área ou de outras origens previstas na Lei Orgânica do TCE-CE.

Aplicando a metodologia prevista, sempre se buscou designar pelo menos dois analistas para cada auditoria, com o objetivo de dividir o esforço de trabalho, propiciar uma melhor análise da situação a partir de múltiplas visões e entendimentos e reduzir pressões sobre os integrantes da equipe de fiscalização.

Fase atual: a Inspetoria

Confirmando as expectativas, em 01/09/2011, foi implantada a 13ª Inspetoria de Controle Externo (ICE), que havia sido instituída em 22/03/2011, por meio da Resolução Administrativa TCE Nº 02/2011, com a missão de realizar auditorias de TI no âmbito da Administração Pública estadual no Estado do Ceará, absorvendo as funções da Comissão Especial de Auditoria de TI, que foi extinta. A partir desta data, os membros da então Comissão, integrantes do corpo de servidores efetivos do Tribunal, passaram a compor a nova inspetoria. A partir da implantação da inspetoria, a gestão da área passou a ser conduzida por um diretor e um subdiretor, selecionados dentre os próprios servidores da equipe, conforme prática existente no TCE-CE. A nova ICE é, portanto, a unidade organizacional que responde atualmente pela área de auditoria de TI no Tribunal.

A nova inspetoria vem dando continuidade ao planejamento de certificações para a equipe de auditores, com o foco inicial na obtenção da certificação CISA.

Conclusão

Entendemos que foi bastante relevante a implantação da área de auditoria de TI no Tribunal de Contas do Estado do Ceará, pois veio suprir uma deficiência nesta área no âmbito da Administração Pública estadual. Antes da criação da Comissão de Auditoria de TI não existia atuação específica e especializada do controle externo nessa área junto aos órgãos e entidades estaduais. Da mesma forma, as ações de controle interno nessa área eram muito incipientes, pelo menos dentro do Poder Executivo.

A área de auditoria de TI, além de fiscalizar os jurisdicionados, presta também o serviço de consultoria interna para as demais áreas de fiscalização do TCE-CE, emitindo pareceres e apoiando-as na elaboração dos seus trabalhos, em temas específicos de TI. As equipes de fiscalização do Tribunal frequentemente se deparavam com dúvidas técnicas da área de TI e não tinham um setor específico para consultar e apoiá-las, quando da elaboração de seus relatórios de auditoria e inspeção.

Adicionalmente, a área de auditoria de TI também pode eventualmente realizar auditorias internas no próprio TCE-CE, de forma a buscar garantir a boa governança de TI, segundo as recomendações ditadas pelo próprio Tribunal e preparando-o para ser um bom exemplo a ser seguindo pelos seus jurisdicionados.

Além do papel de fiscalização, a atuação da Comissão junto aos jurisdicionados foi vista pelos gestores de TI dos órgãos e entidades como importante para respaldá-los no processo interno de aprovação de investimentos para a área de TI. O trabalho de diagnóstico da governança de TI realizado tornou evidente a necessidade de maiores investimentos na aquisição de infraestrutura de TI e na qualificação de pessoal nessa área no âmbito estadual. Chamou a atenção o fato de vários gestores terem solicitado para serem os primeiros a serem auditados (após o diagnóstico, a Comissão passou a realizar auditorias mais específicas e aprofundadas nos jurisdicionados).

Dentre os principais resultados e benefícios advindos com a implantação da área de auditoria de TI, podemos citar:

- Aperfeiçoamento do controle externo na área de TI no âmbito no TCE-CE;

- Melhoria na governança da TI na Administração Pública estadual;
- Maior controle dos sistemas computacionais estaduais, por parte dos jurisdicionados;
- Aprimoramento da qualidade dos softwares desenvolvidos pelos órgãos e entidades estaduais;
- Melhoria dos processos de aquisição de bens e serviços de TI, tanto em termos de economicidade e racionalidade, quanto de qualidade das aquisições;
- Melhor aplicação dos recursos de TI nos processos intra e interorganizacionais dentro do escopo da Administração Pública estadual, aperfeiçoando a geração das informações e os controles necessários a uma efetiva gestão pública;
- Melhoria da efetividade dos serviços prestados à população de forma eletrônica;
- Melhoria da qualidade das informações disponibilizadas à sociedade através dos sítios e portais oficiais;
- Melhor suporte às demais áreas de fiscalização do TCE-CE, em questões relativas à TI;
- Estímulo à criação de áreas de controle interno de TI nos órgãos e entidades jurisdicionados.

Como resultado do trabalho de auditoria especializada de TI, acreditamos que, com uma melhor governança de TI, haja uma sensível melhoria na prestação dos serviços públicos à sociedade, aperfeiçoamento da gestão pública e aumento da transparência dos atos governamentais, através de um uso mais adequado, racional e efetivo da Tecnologia da Informação por parte da Administração Pública estadual.

Por fim, esperamos que nossa experiência no TCE-CE, relatada neste texto, possa contribuir com outras instituições públicas que desejem implantar ou que já estejam implantando áreas de auditoria de TI.

Referências bibliográficas

CEARÁ, Tribunal de Contas do Estado do. **Lei Orgânica**. 3ª edição. Fortaleza: TCE, 2010.

FERRER, Florência. **Gestão pública eficiente**.2ª edição. Rio de Janeiro: Elsevier, 2007.

GUERRA, Evandro Martins. **Os controles externo e interno da administração pública**. 2ª edição. Belo Horizonte: Fórum, 2005.

KNIGHT, Peter Titcomb; FERNANDES, Ciro Campos Christo; CUNHA, Maria Alexandra (organizadores). **E-Desenvolvimento no Brasil e no mundo – subsídios e Programa e-Brasil**. São Paulo: Yendis, 2007.

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

ANEXO I

Instituições de referência em auditoria

- ANAO – Australian National Audit Office
- GAO – US General Accounting Office
- IIA – Institute of Internal Auditors
- INTOSAI – International Organization of Supreme Audit Institutions
- ISACA – Information Systems Audit and Controle Association
- NAO – National Audit Office
- TCU – Tribunal de Contas da União
- ASUL – Associação de Entidades Oficiais de Controle Público do Mercosul
- EUROSAI – Organização das Entidades Fiscalizadoras Superiores da Europa
- ASOSAI – Organização Asiática de Entidades Fiscalizadoras Superiores
- EURORAI – Organização Européia das Instituições Regionais de Controle Externo do Setor Público
- OLACEFS – Organização Latino-americana e do Caribe de Entidades Fiscalizadoras Superiores

ANEXO II

Questionário sobre a Situação da Governança de Tecnologia da Informação

Objetivo: realizar levantamento sobre a gestão e uso da Tecnologia da Informação na Administração Pública estadual.

Questões:

- A instituição possui planejamento estratégico?
- O setor de TI da instituição possui planejamento estratégico?
- Há um Plano de Continuidade do Negócio (PCN) formalmente estabelecido capaz de garantir as necessidades operacionais da instituição?
- A instituição utiliza Processo de Desenvolvimento de Software formalmente estabelecido?
- Há comitê diretivo na instituição que decida sobre a priorização das ações e investimentos de TI?
- O gestor de TI da instituição é servidor do Estado?
- O gestor é servidor / empregado público? É da própria instituição?
- Há cargos específicos para a área de TI no plano de cargos e carreiras da instituição?
- A instituição possui e mantém atualizado inventário de: hardwares, softwares, sistemas informatizados e bases de dados?
- A instituição possui uma Política de Segurança da Informação alinhada aos requisitos do negócio e com as leis e regulamentações relevantes?
- Existe formalmente um gestor ou área específica, com responsabilidades definidas, para lidar estrategicamente com segurança da informação?
- A instituição classifica a informação (por exemplo, em termos do seu valor, requisitos legais, sensibilidade e criticidade)?
- Existem procedimentos formais de controle de acesso físico de pessoas ao setor de TI da instituição?
- A instituição possui uma política formal de realização de cópias de segurança (backup)?
- Existe na instituição uma política formal de controle de acesso lógico aos

recursos de TI (rede, Internet, sistemas de informação, arquivos, correio, etc)?

- Existem política formal e medidas de segurança para a proteção contra os riscos do uso de recursos de TI móveis?
- Existe processo formalizado de auditoria de Tecnologia da Informação na instituição?
- A instituição possui um processo formal de Gerenciamento de Projetos de TI?
- A instituição possui servidores / empregados com certificação PMP (Project Management Professional) do PMI (Project Management Institute)?
- A instituição possui um escritório de projetos formalmente implantado para os projetos de TI?
- A instituição possui um ponto único de contato para atender às necessidades de TI (Central de Serviços, Help Desk, etc)?
- A instituição possui formalmente implantado processo de Gerenciamento de Incidentes/Problemas, contemplando no mínimo, o registro e o monitoramento de incidentes/problemas, verificação de status de recursos de sistemas, preenchimento de pedidos de serviço padrão e gerenciamento de conhecimento?
- A instituição possui formalmente implantado processo de Gerenciamento de Mudanças, contemplando no mínimo, a verificação e a aprovação de pedidos de mudança na infraestrutura de TI e também a coordenação de mudanças aprovadas a serem implementadas?
- A instituição possui formalmente implantado processo de Gerenciamento de Acordos de Níveis de Serviço de TI, com o objetivo de estabelecer e manter acordos da área de TI com os seus usuários, quanto à qualidade dos serviços prestados?
- A instituição possui formalmente implantado processo de Gerenciamento de Acordos de Níveis de Serviço de TI, com o objetivo de estabelecer e manter acordos com os fornecedores de TI, quanto à qualidade dos serviços prestados?
- A instituição possui formalmente implantado processo de Gerenciamento Financeiro de Serviço de TI, que identifica os custos de fornecimento dos serviços e viabiliza considerações sobre custo e benefício (ou preço e

desempenho) nas decisões sobre mudanças na infraestrutura de TI ou nos serviços de TI?
- A instituição possui formalmente implantado processo de Gerenciamento da Capacidade, que aborda a estruturação dos recursos de TI, dentro das perspectivas de otimização de custos e tempo, para suportar os acordos feitos com os usuários?
- A instituição possui formalmente implantado processo de Gerenciamento da Continuidade, abordando a capacidade da organização de TI em continuar a fornecer serviços em níveis previamente acordados com os usuários, após a ocorrência de um evento de interrupção das atividades?
- É designado formalmente gestor/fiscal para os contratos de TI?
- Há pesquisa de satisfação dos usuários internos/externos dos serviços de TI?
- Os gestores de TI participam da elaboração do orçamento da instituição?
- A instituição possui procedimentos formais de Análise de Riscos na área de TI?
- Há pessoas terceirizadas em funções de TI sem exercerem na prática atividades específicas da área de TI (trabalhando no setor de TI da instituição)?
- Informe a quantidade de servidores da instituição que trabalham na área de TI
- Informe a quantidade de terceirizados que trabalham na área de TI
- Informe a quantidade de estagiários que trabalham na área de TI
- Informe a quantidade de servidores do Estado cedidos de outras instituições que trabalham na área de TI
- Em quais das seguintes áreas a instituição tem necessidade de receber capacitação para o seu pessoal de TI? Coloque em ordem de prioridade (PMBOK, ITIL, COBIT, Segurança da Informação, Governança de TI)

Obs.: Deverão ser anexados documentos que possam comprovar as respostas, caso sejam afirmativas.