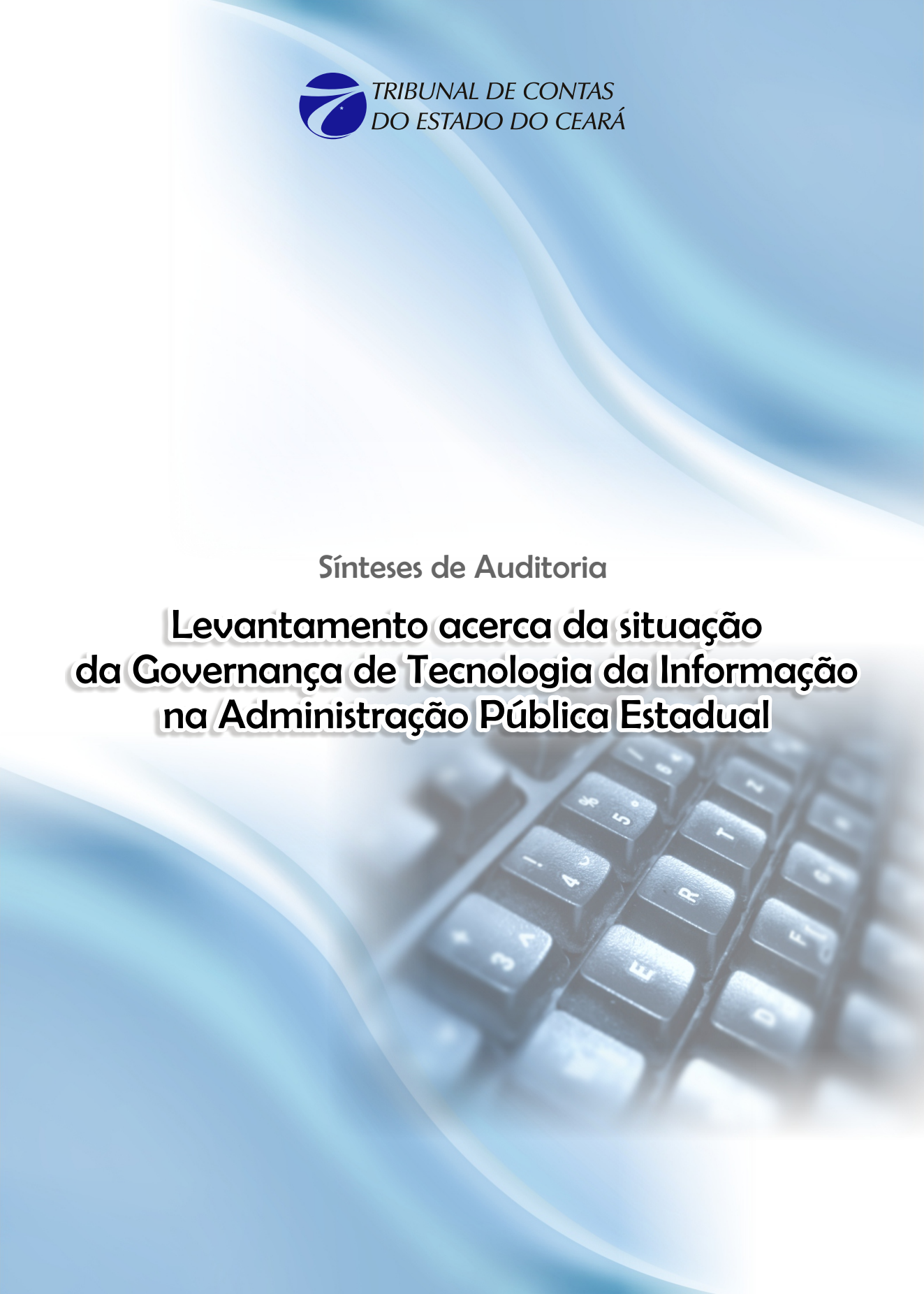
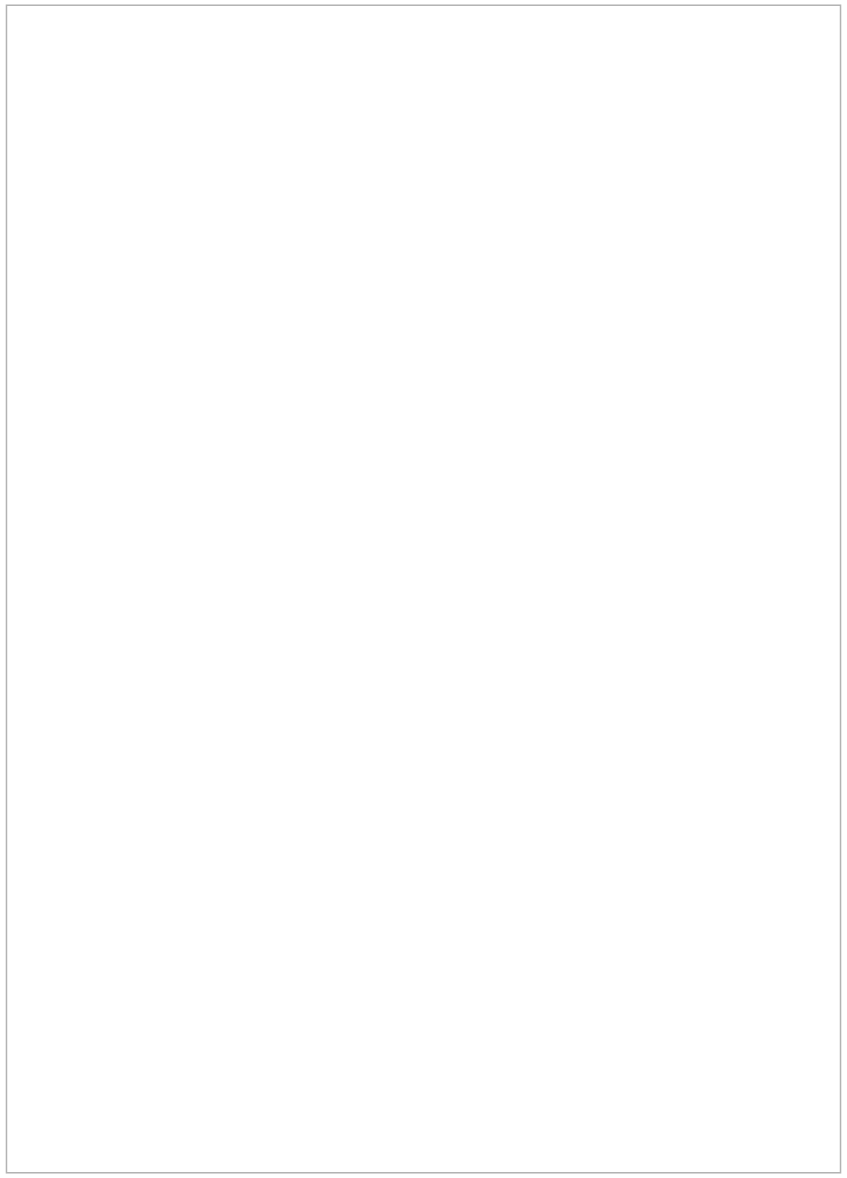
TRIBUNAL DE CONTAS
DO ESTADO DO CEARÁ

Sínteses de Auditoria

Levantamento acerca da situação da Governança de Tecnologia da Informação na Administração Pública Estadual





TRIBUNAL DE CONTAS
DO ESTADO DO CEARÁ

Sínteses de Auditoria

Levantamento acerca da situação da Governança de Tecnologia da Informação na Administração Pública Estadual

Relator
Conselheiro Edilberto Carlos Pontes Lima

Fortaleza, Ceará 2011

C387s

Ceará. Tribunal de Contas

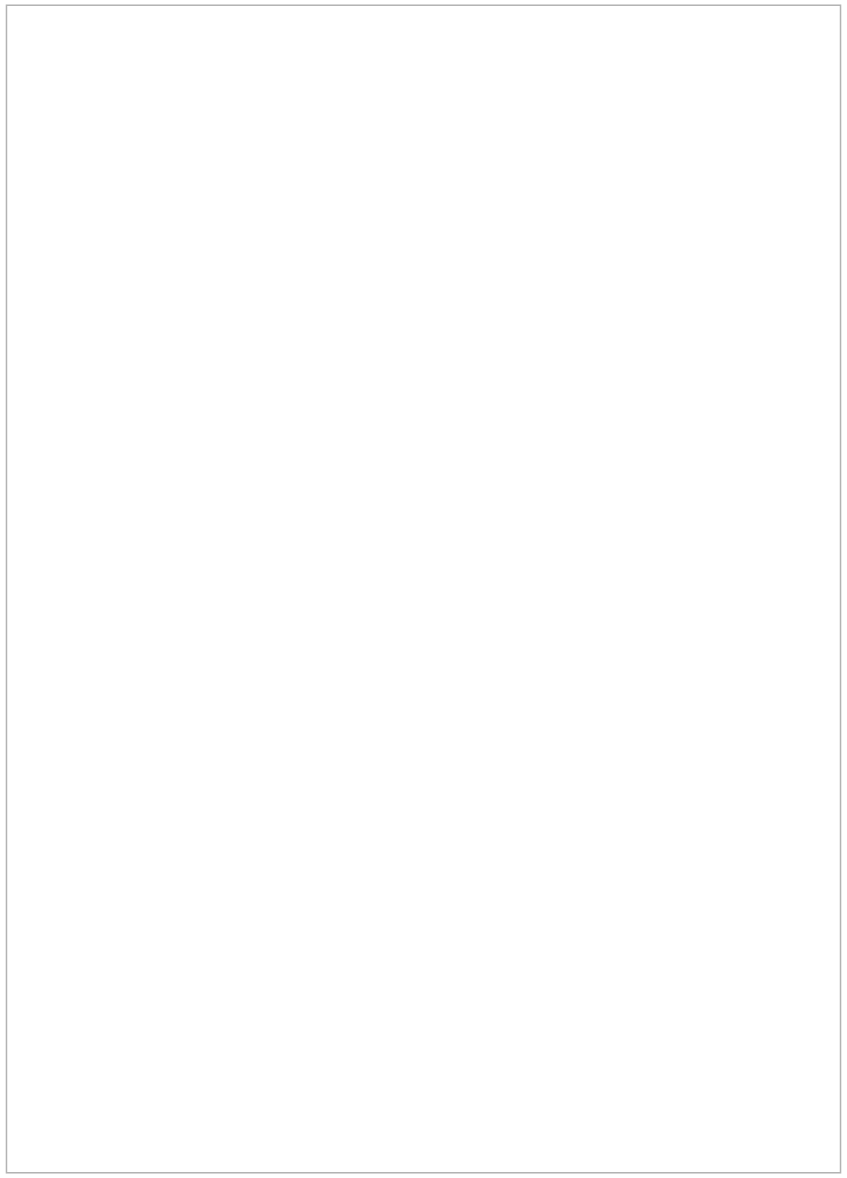
Levantamento acerca da situação da Governança de Tecnologia da Informação da Administração Pública Estadual/ Tribunal de Contas do Estado do Ceará. – Fortaleza: TCE, 2011.

32 p. : il. color. - (Sínteses de Auditoria)

1. TECNOLOGIA DA INFORMAÇÃO 2.TRIBUNAL DE CONTAS DO ESTADO DO CEARÁ. 3. GOVERNANÇA I.Título.II.Série.

CDU – 681.3:007

Sumário



1. APRESENTAÇÃO

As Sínteses de Auditoria da Comissão Especial de Auditoria de Tecnologia da Informação (CEATI), editadas pelo Tribunal de Contas do Estado do Ceará (TCE-CE), têm por objetivo divulgar os principais resultados das fiscalizações na gestão e no uso de recursos da Tecnologia da Informação (TI) pela Administração Pública Estadual, realizadas por este Tribunal. Esta publicação contêm, de forma resumida, aspectos importantes verificados durante as auditorias, boas práticas identificadas, bem como recomendações e determinações para melhorar o desempenho na área de TI na Administração Pública Estadual.

O foco das fiscalizações de TI realizadas pelo Tribunal é a verificação da conformidade com as melhores práticas, normas e legislação e do desempenho das ações governamentais nessa área, a partir das avaliações da Governança de TI, das iniciativas de governo eletrônico, dos sistemas informatizados da Administração Pública, da gestão e uso dos recursos de TI e das aquisições de bens e serviços pertinentes à TI. O objetivo principal dessas fiscalizações é orientar os dirigentes das organizações sobre o uso eficaz, eficiente e aceitável da TI dentro de suas organizações.

Pretende-se também, com a divulgação desse trabalho, oferecer à sociedade informações suficientes e fidedignas para que possam exercer o controle das ações de governo nesta área.

Esta publicação traz o resumo da situação encontrada, à época do levantamento da Governança de TI na Administração Pública Estadual, realizado em dezembro/2009. O respectivo processo (Nº 07836/2009-6) foi apreciado em sessão do Plenário de 14/12/2010, sob a relatoria do Conselheiro Edilberto Carlos Pontes Lima, resultando na RESOLUÇÃO Nº 3550/2010 que autorizou a divulgação dos resultados dela decorrentes.

Conselheiro Teodorico José de Menezes Neto
PRESIDENTE

2. OBJETIVOS DO LEVANTAMENTO

Autorizada por meio da Solicitação de Auditoria/Inspeção Nº 03/2009 de 04/11/2009, a Comissão Especial de Auditoria de Tecnologia da Informação realizou inspeção com o objetivo de "obter informações acerca da situação da Governança de Tecnologia da Informação – TI, para identificar corretamente o quê e como fiscalizar a gestão e o uso de TI pelos órgãos e entidades estaduais".

O objetivo principal deste levantamento foi coletar informações relevantes sobre a Governança de TI para subsidiar os trabalhos futuros da Comissão Especial de Auditoria de Tecnologia da Informação, 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.

Como complemento ao levantamento, foi incluída uma pesquisa quanto à demanda de capacitação em temas relacionadas à Governança de TI. O objetivo desta pesquisa era identificar as áreas de conhecimento mais deficientes, bem como, orientar o Instituto Plácido Castelo (IPC), a Escola de Contas do TCE-CE, na elaboração do planejamento de capacitações que possam ser ofertadas aos jurisdicionados.

3. METODOLOGIA UTILIZADA

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 (NBR ISO/IEC 15999-1:2007), 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 (NBR ISO/IEC 20000-1:2008), dentre outros processos relacionados a TI.

A norma NBR ISO/IEC 27002:2005 estabelece diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização. Os objetivos definidos nesta norma estabelecem diretrizes gerais sobre as metas geralmente aceitas para a gestão da segurança da informação.

A norma NBR ISO/IEC 15999-1:2007 estabelece o processo, os princípios e a terminologia da gestão de continuidade de negócios (GCN), e tem como principal objetivo fornecer uma base para que se possa entender, desenvolver e implementar a continuidade de negócios em uma organização, além de obter confiança nos negócios da organização com clientes e outras organizações.

O COBIT é um guia de boas práticas dirigido para a gestão de Tecnologia de Informação. Criado e mantido pela Isaca (*Information Systems Audit and Control*

Association), possui uma série de recursos que podem servir como um modelo de referência para gestão da TI, incluindo um sumário executivo, um framework, controle de objetivos, mapas de auditoria, ferramentas para a sua implementação e principalmente, um guia com técnicas de gerenciamento. Especialistas em gestão e institutos independentes recomendam o uso do COBIT como meio para otimizar os investimentos de TI, melhorando o retorno sobre o investimento e fornecendo métricas para avaliação dos resultados.

O PMBOK identifica e descreve o subconjunto do universo do conhecimento de Gerenciamento de Projetos reconhecido como boas práticas em muitos projetos na maior parte do tempo, havendo consenso pelos praticantes sobre seus valores e aplicabilidade. Outro propósito do PMBOK é prover um vocabulário único para a área de projetos padronizando seus termos.

A norma NBR ISO/IEC 20000-1:2008 tem o objetivo de regulamentar um padrão para o Gerenciamento de Serviços de TI, através da formalização dos conceitos e da visão dos processos que o implementam, permitindo assim que os provedores de serviços de TI compreendam os meios através dos quais poderão planejar, executar, verificar e melhorar continuamente a qualidade dos serviços entregues, em conformidade com os requisitos estabelecidos junto ao negócio e a seus clientes.

O questionário desenvolvido pela CEATI buscou contemplar as seguintes áreas relativas ao tema “Governança de TI”: 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.

Na fase de execução do levantamento, os órgãos/entidades selecionados receberam, por meio do Ofício Circular Nº 2/2009-GAB.PRES. de 06/11/2009 da presidência do TCE-CE, a solicitação de que fosse indicado o gestor de TI ou responsável pelo preenchimento do questionário. Após o recebimento do responsável de cada órgão/entidade, foi enviada uma mensagem eletrônica contendo a senha individual e o link de acesso ao questionário eletrônico. Adotou-se para o desenvolvimento deste questionário o uso do software lime-survey, baseado em plataforma livre.

Durante o preenchimento do questionário, foi solicitado aos gestores de TI dos órgãos/entidades que anexassem documentos eletrônicos para servirem de evidências às respostas apresentadas. Em geral, esses documentos solicitados são planos, documentos formais de procedimentos, relatórios e políticas. Deve-se ressaltar que as informações coletadas através do questionário eletrônico foram declaradas pelo responsável que o preencheu e não verificadas pela equipe da CEATI junto aos órgãos/entidades. Além disso, nesse primeiro momento, não foi avaliada a pertinência e a qualidade dos documentos produzidos e anexados pelos órgãos/entidades.

Também foi solicitado, quando cabível, que fosse informado o tempo de utilização daquela prática ou processo, o que ajudará a identificar o grau de maturidade daquele órgão/entidade com relação ao ponto questionado.

É importante destacar que dos 58 órgãos/entidades pesquisados, apenas 2 (dois) não responderam ao ofício da presidência no prazo estabelecido. Depois de

várias tentativas de contato, esta Corte de Contas autorizou, através dos ofícios da presidência Nº 1686/2009 e Nº 1688/2009, que 2 (dois) membros da Comissão Especial de Auditoria de TI fizessem a aplicação do questionário *in loco* no órgão/entidade, bem como requisitassem a documentação necessária para a validação de alguma pergunta do questionário. Após a realização das inspeções, os dados dos questionários foram cadastrados na ferramenta e os documentos arquivados.

Ao final da coleta de informações, as respostas apresentadas nos questionários foram tabuladas e as evidências armazenadas para consulta e tratamento posterior.

4. LEVANTAMENTO ACERCA DA GOVERNANÇA DE 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.

4.1 Planejamento estratégico institucional e de TI

O planejamento estratégico é um processo gerencial que diz respeito à formulação de objetivos para a seleção de programas de ação e para sua execução, levando em conta as condições internas e externas à instituição e sua evolução esperada. Também considera premissas básicas que a instituição deve respeitar para que todo o processo tenha coerência e sustentação.

Qualquer ação requer planejamento para ser executada de forma adequada, sob pena de não se alcançar a meta pretendida. No setor público isto é mais imprescindível ainda, pois as demandas da sociedade em geral são maiores do que a capacidade de atendimento do Estado.

Dos 58 órgãos/entidades pesquisados, 57% não possuem planejamento estratégico institucional em vigor. Isso deixa claro que mais da metade das organizações estaduais pesquisadas não tem a prática de planejar suas ações, ou seja, reagem de acordo com as situações demandadas no seu âmbito de atuação.

Apesar da existência da Resolução Nº1 de 11 de junho de 2008 do Conselho Superior de Tecnologia da Informação e Comunicação (CSTIC) do Governo do Estado do Ceará, que determina que todas as áreas de Tecnologia da Informação e Comunicação – TIC setoriais dos órgãos/entidades da Administração Pública Estadual (Poder Executivo) devem realizar seu planejamento estratégico, ficou demonstrado pelo levantamento que existem cerca de 33% dos pesquisados que ainda não possuem planejamento estratégico de Tecnologia da Informação.

Deve-se deixar claro que o planejamento estratégico institucional deve anteceder o planejamento estratégico de TI, que deve ser elaborado tendo como base os objetivos da organização. Observou-se que dos 39 órgãos/entidades que possuem planejamento estratégico de TI, 21 não possuem o institucional, ou seja, não estavam alinhados com os objetivos estratégicos da organização. O planejamento de TI é um planejamento setorial, e como tal, faz parte do planejamento corporativo, devendo ser portanto

elaborado a partir deste, e não de forma isolada. Essa situação pode comprometer a área de TI devido a possíveis descontinuidades de projetos, insatisfação dos clientes e o não alcance de resultados, influenciando negativamente o desempenho do órgão/entidade.

A pesquisa destacou também que 12 órgãos/entidades não possuem planejamento estratégico institucional e de TI, e que apenas 18 possuem os dois planejamentos. O Gráfico 1 a seguir mostra o relacionamento encontrado entre o planejamento institucional e o de TI.

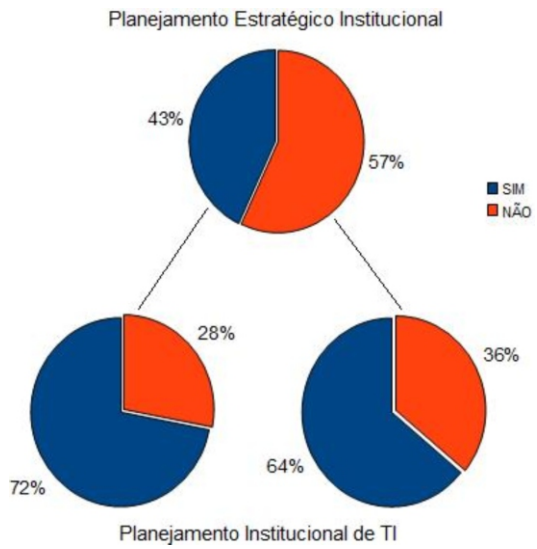


Gráfico 1 – Planejamento estratégico institucional e de TI

Considerando a relevância do tema a importância do alinhamento do planejamento estratégico institucional com o de TI, e as possíveis consequências de prejuízos ou da ineficiente aplicação dos recursos públicos por parte da administração pública, espera-se que sejam adotadas medidas de âmbito geral com o objetivo de se criar a consciência da importância do planejamento estratégico para o desenvolvimento das atividades com eficiência e eficácia e que garantam os objetivos das instituições bem como a satisfação da sociedade.

Dentro do conceito de Governança de TI, a implantação de um comitê diretivo que decida sobre a priorização das ações e investimentos de TI é importante para que as decisões gerenciais de alto nível sobre TI sejam tomadas de forma compartilhada entre os principais gestores da organização, e não apenas pela área de TI. Este comitê também deverá se envolver de forma ativa na definição do orçamento de TI, o qual deverá estar em plena conformidade com o orçamento global da instituição. Desta forma, o comitê poderá promover a utilização planejada e coordenada dos serviços de Tecnologia da Informação pela organização.

Dos órgãos/entidades pesquisados, 71% não possuem comitê diretivo para definir como os investimentos em TI são realizados. A falta de um comitê diretivo que estabeleça critérios na aplicação dos gastos em TI, bem como na priorização de

projetos e aquisições de novas tecnologias, faz com que a área de TI funcione como um setor à parte da organização, ou seja, esteja em desarmonia com os objetivos da organização.

4.2 Segurança da informação

A segurança da informação, como demonstrou a pesquisa, encontra-se crítica nos órgão/entidades da Administração Pública Estadual. A falta de planejamento e 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.

O Plano de Continuidade do Negócio (PCN) é um plano elaborado para garantir a recuperação de um ambiente de TI, independentemente de ocorrências que suspendam suas operações e dos danos nos componentes (*softwares, hardwares*, infraestrutura, etc.) por ele utilizados. Isto é, um PCN tem como objetivo assegurar a disponibilidade de recursos de sistemas críticos, recuperar um ambiente avariado e promover o retorno à sua normalidade.

A pesquisa deixou claro que 98% dos órgãos/entidades, quase que a totalidade, não possuem um PCN, aumentando os riscos de perda de informações, paralisação de serviços, bem como prejuízo à Administração Pública Estadual devido ao atraso no restabelecimento da normalidade de suas atividades.

A importância de se ter um inventário atualizado de hardwares, softwares e de sistemas informatizados, além de demonstrar o que a organização possui em termos de ativos de TI e permitir controlá-los, serve também como fonte para a decisão de novos investimentos em TI. A pesquisa demonstrou que 71% dos órgãos/entidades possuem atualizado seu inventário de TI, mas ainda existem 16 instituições que não possuem inventários de seus ativos.

A Política de Segurança da Informação de uma instituição tem por objetivo prover uma orientação quanto à segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes. Ela é um documento que contém as diretrizes da instituição quanto ao tratamento seguro da informação. De acordo com a norma NBR ISO/IEC 27002:2005 da ABNT (Associação Brasileira de Normas Técnicas), uma política de segurança deve declarar explicitamente o comprometimento da alta direção da instituição com a segurança da informação.

A profundidade da política de segurança da informação será tanto maior quanto mais interconectada estiver a instituição e mais estratégico for o papel que a TI representa para o negócio, já que qualquer evento de risco relacionado com a segurança da informação poderá trazer grandes prejuízos para a instituição.

Dos pesquisados, 79% não possuem política de segurança da informação, ou seja, não possuem procedimentos formais de segurança. Os riscos para os órgãos/entidades são altos, possibilitando o vazamento de informações, perda de dados, acesso de pessoas não autorizadas a sistemas, furtos e paralisação dos sistemas de informação entre outros.

No âmbito do Poder Executivo já existe legislação sobre o tema conforme o Decreto Nº29.227 de 13 de março de 2008, que disciplina a Política de Segurança da Informação dos Ambientes de TIC do Governo do Estado do Ceará e cria o Comitê Gestor de Segurança da Informação do Governo do Estado do Ceará (CGSI), com sua composição e competências. Cabe portanto ao CGSI planejar a forma de disseminar a Politica de Segurança da Informação, disciplinada pelo Decreto, e acompanhar sua implementação em todos os órgãos/entidades estaduais. Esta iniciativa é importante e deve ser seguida pelos demais poderes públicos estaduais, de forma a diminuir a ocorrência de incidentes e elevar o nível de segurança no trato com a informação.

O gestor do processo de segurança da informação é responsável pela gestão da segurança da informação em toda a organização. Para isso, ele precisa saber de suas responsabilidades, deve ser capaz de conduzir adequadamente este processo e ter uma visão geral do negócio e objetivos da instituição. O gestor tem a competência de fazer com que a política de segurança seja seguida e conhecida por todos os envolvidos, deixando claro seus direitos e obrigações e o papel de cada um dentro da instituição.

A pesquisa mostrou que 71% dos órgãos/entidades não possuem formalmente um gestor ou área específica para lidar com a segurança da informação, aumentando mais ainda os riscos inerentes a falha de segurança nessas instituições.

A classificação da informação está diretamente relacionada com a cultura organizacional e área de atuação, ou seja, os níveis de confidencialidade dependem da importância que aquela informação tem para a organização. Para cada nível de confidencialidade da informação, podem ser definidos aspectos, tais como: sua guarda física, forma de transporte, transmissão por correio eletrônico, autorização de cópias, descarte e destruição física.

Dos órgãos/entidades pesquisados 78% não possuem uma política de classificação da informação. Isso é preocupante principalmente em se tratando de instituições governamentais, que tratam muitas vezes com informações confidenciais, e que têm impacto significativo na vida das pessoas e funcionamento da economia. Se não existe nenhum critério para se tratar as informações dentro dessas instituições, o risco dessas informações serem usadas de forma indevida pelos usuários é muito grande, bem como a possibilidade de serem usadas por pessoas externas com propósitos fraudulentos.

A Norma NBR ISO/IEC 27002:2005 estabelece que os ambientes físicos onde estão os recursos (ativos) de informação devem ser protegidos contra ameaças que podem danificá-los e prejudicar a utilização da informação para o negócio. A organização deve estabelecer procedimentos que garantam a integridade dos ativos, bem como um controle de acesso físico das pessoas aos ambientes internos de TI.

A pesquisa mostrou que 90% dos órgãos/entidades não possuem um controle de acesso físico de pessoas aos setores de TI. Isso possibilita um grande risco de acesso de pessoas não autorizadas a esses ambientes, podendo ocasionar a perda de dados, furtos de informação e de ativos, instalação de vírus ou outros softwares mal intencionados, paralisação de sistemas e acesso indevido a informações sigilosas.

Uma política de cópia de segurança *(backup)* tem como principal finalidade

garantir a recuperação da informação no caso de alguma falha de hardware ou software. *Backups* podem ser necessários também por solicitação de um usuário ou por necessidade de um sistema, quando se quer voltar uma versão de um documento ou dado a um instante anterior. Os procedimentos devem ser seguidos em conformidade com a política estabelecida.

Deve-se destacar dois aspectos importantes: o primeiro é o estabelecimento de testes para as cópias de segurança, ou seja, verificar se o procedimento de *backup* adotado garante a integridade e a confiabilidade dos dados. O segundo ponto é a forma de armazenamento adotado, ou seja, quem vai ter acesso às cópias e se elas estão no ambiente de TI da própria instituição ou em um ambiente externo ao de TI ou da própria instituição.

A pesquisa demonstrou que 67% dos órgãos/entidades não possuem uma política de cópia de segurança de dados. Essas instituições correm um grande risco de perder dados que muitas vezes foram fruto de longos trabalhos, causando retrabalho, atrasando os projetos e, dependendo da informação, um grande prejuízo para a instituição.

O acesso lógico é a maneira pela qual as pessoas acessam os dados, programas e sistemas computacionais da organização. Uma política de acesso lógico tem por objetivo garantir que os usuários acessem apenas as informações necessárias ao desempenho das suas funções profissionais. Os acessos devem ser previamente autorizados sendo de caráter individual e intransferível.

A pesquisa demonstrou que 69% dos órgãos/entidades não possuem uma política formal de acesso lógico. Dentre os riscos que essas instituições estão sujeitas destacam-se: acesso a informações confidencias por pessoas não autorizadas, fraudes em relação à autoridade de acesso, uso indevido de arquivos, programas e sistemas de informação, inclusão de vírus e softwares maliciosos na rede, perda de dados, paralisação de sistemas, entre outros.

O uso de equipamentos móveis (*notebook, smartphone*, entre outros) é cada vez mais comum na administração pública, uma política formal de acesso para equipamentos móveis tem a finalidade de criar restrições ou regras para o uso desses equipamentos, pois a possibilidade de uma falha de segurança é muito alta já que não existem barreiras físicas, uma vez que o acesso é via sinal de rádio, o que possibilita uma invasão ao ambiente computacional mesmo de fora da organização.

A pesquisa demonstrou que 86% dos órgãos/entidades não possuem uma política formal de acesso para equipamentos de TI móveis. Dentre os riscos que essas instituições estão sujeitas pode-se destacar: acesso a informações confidencias por pessoas não autorizadas, fraudes em relação à autoridade de acesso, uso indevido de arquivos, programas e sistemas de informação, inclusão de vírus e softwares maliciosos na rede, perda de dados, paralisação de sistemas, entre outros.

A Análise de Riscos de TI permite verificar quais as vulnerabilidades que o setor de TI da instituição possui. Ela serve para criar meios de mitigar ou evitar possíveis falhas de segurança, ou interrupções no ambiente computacional (sistemas, equipamentos, rede, arquivos, informações, etc). A análise de riscos deve levar em consideração os objetivos da organização, tendo um papel importante para que esses objetivos sejam alcançados.

A pesquisa demonstrou que 91% dos órgãos/entidades pesquisadas não fazem análise dos riscos de TI. As consequências para essa falta de planejamento são diversas tais como: interrupção de sistemas, descontinuidade de atividades, perda de dados, fraudes, furtos de ativos, acessos indevidos, sobrecarga elétrica, desastres naturais, impactos financeiros, entre outros.

O Gráfico 2 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.

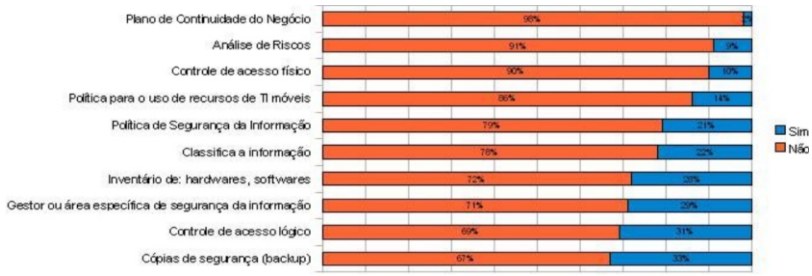


Gráfico 2 – Cenário geral da situação segurança da informação

4.3 Processo de desenvolvimento de software

O Processo de Desenvolvimento de *Software* (PDS) é um conjunto de atividades, parcialmente ordenadas, com a finalidade de obter um produto de software. É considerado um dos principais mecanismos para se obter software de qualidade e cumprir corretamente os contratos de desenvolvimento a um custo relativamente baixo. O PDS busca não só garantir que as várias etapas típicas do desenvolvimento (levantamento, projeto, programação, testes e homologação) sejam executadas de forma sistemática e documentada, mas também permite a avaliação e melhoria do processo, com vistas à produção de software de qualidade.

A pesquisa demonstrou que os órgãos/entidades da Administração Pública Estadual, não possuem a prática de desenvolver seus sistemas através de processo de desenvolvimento de software, ou seja, não existe um planejamento baseado em um procedimento definido que contenha: quais os documentos que devem ser utilizados e de que forma devem ser preenchidos, armazenados e atualizados, quais as métricas de acompanhamento, que tipo de testes devem ser feitos, quais os critérios de aceitação, quais os critérios de implantação e de que forma será entregue a documentação final.

A inexistência de um PDS em 86% dos pesquisados preocupa devido ao aumento do risco dos softwares possuírem falhas de segurança e baixa qualidade de desempenho. Isto aumenta as possibilidades de não se possuir uma documentação confiável do desenvolvimento ocasionando uma maior dificuldade em correções ou atualizações, ou até mesmo a inviabilidade de se manter o software, bem como um aumento nos custos financeiros e constantes transtornos, prejudicando o andamento das atividades e os objetivos da organização.

Considerando a existência de *softwares* (sistemas de informação, aplicativos, utilitários, etc) que são utilizados por diversos órgãos/entidades estaduais, bem como

softwares que interagem com softwares de outros órgãos/entidades, entende-se que o processo de desenvolvimento de *software* na Administração Pública Estadual é fundamental para a manutenção e integração desses softwares de forma eficiente, segura e com o menor impacto para os usuários, bem como para garantir a documentação do que foi realizado.

A existência do Decreto Nº29.255, de 09/04/2008, no âmbito do Poder Executivo, que institui o uso preferencial de *software* livre como ferramenta corporativa padrão de execução e gestão da Política Estadual de Tecnologia da Informação e Comunicação, reforça a importância de se ter um processo de desenvolvimento de *software* instituído, tendo em vista a grande variedade de soluções e ferramentas de desenvolvimento utilizadas, requerendo uma forte demanda por padronização e documentação.

4.4 Estrutura de pessoal de TI

É de fundamental importância que o gestor de TI do órgão seja servidor efetivo do Estado, pois assim sendo, há uma maior probabilidade de que haja um maior comprometimento daquele no desempenho de suas funções. Este comprometimento vêm do fato de o vínculo do servidor efetivo ser direto com o Estado, diferentemente de ocupantes apenas de cargos comissionados. Há ainda o caso extremo, quando o gestor de TI é um profissional terceirizado, situação esta que deve ser evitada, pois fragiliza o relacionamento gerencial, uma vez que inexiste vínculo entre o profissional e o Estado (a contratação é com a empresa de fornecimento de mão-de-obra).

Segundo as informações levantadas no questionário, 60% dos órgãos pesquisados possuem como gestor de TI, um servidor público efetivo. Este dado traz uma certa preocupação, pois 40% dos jurisdicionados questionados, percentual considerado alto, ainda possuem como gestor de TI servidores apenas ocupantes de cargo comissionado ou terceirizados.

O setor de TI das organizações não é mais visto como uma área coadjuvante. Há um tempo ele deixou de ser apenas apoio para tornar-se também estratégico. Sendo assim, a necessidade de servidores nesta área aumentou bastante, tanto no aspecto quantitativo quanto qualitativo. É importante que os colaboradores de TI sejam servidores públicos efetivos, para evitar a dependência em indivíduos sem vínculo com o órgão/entidade para a execução de atividades críticas da instituição, o que pode acarretar descontinuidade de projetos e atividades e perda do conhecimento organizacional. Contudo, não basta que os colaboradores do setor de TI sejam servidores, eles precisam ser selecionados e considerados como servidores especializados. Para que isto ocorra, faz-se necessário que existam cargos específicos de TI no Plano de Cargos e Carreiras da instituição.

Na pesquisa realizada, foi constatado que 79% dos órgãos/entidades pesquisados não possuem cargos específicos de TI no Plano de Cargos e Carreiras. Este resultado mostra que a grande maioria dos jurisdicionados questionados ainda não se preocupa em ter, no seu quadro efetivo, servidores especializados na área de TI, o que pode acarretar na necessidade de contratação de mão-de-obra terceirizada especializada.

O levantamento mostrou que a Estrutura de Pessoal de TI nos órgãos/entidades da Administração Pública Estadual pesquisados, encontra-se com excesso de pessoal

terceirizado, uma vez que 67% do quadro é composto por este tipo de colaborador. Esta situação não é desejável pois é recomendável que funções estratégicas e sensíveis em um ambiente de TI sejam desempenhadas por pessoal efetivo do órgão/entidade, facilitando a manutenção do conhecimento técnico e gerencial na instituição, e possibilitando a capacitação do pessoal envolvido. Além disso, no caso de atividades sensíveis (segurança da informação, por exemplo), a responsabilização de pessoal terceirizado é menos efetiva, devido à ausência de vínculo com o órgão/entidade público. O levantamento também mostrou que 40% das instituições possuem como gestor de TI, uma pessoa que não é servidora estadual.

Outro fato preocupante é a existência de desvio de finalidade destes contratos de terceirização, uma vez que existem pessoas contratadas para a área de TI, que, na verdade, estão exercendo funções distintas da área de TI.

O levantamento apontou que 21% dos órgãos/entidades pesquisados possuem pessoas terceirizadas em funções de TI sem exercerem na prática atividades específicas da área de TI. Quando este tipo de situação ocorre, pode-se estar diante de um desvio de finalidade na utilização do pessoal terceirizado, possivelmente ocasionado por uma falha no processo de contratação ou na gerência do contrato de terceirização.

A terceirização deve ser usada apenas para funções de cunho mais operacional e que não possuam fortes requisitos de segurança ou que sejam estratégicas para a organização. Não é recomendável também se terceirizar a "inteligência" da instituição. Neste sentido, é importante que os gestores de TI dos órgãos/entidades sejam servidores efetivos do Estado, admitidos segundo a regra do concurso público, em harmonia com a carta constitucional. Também, é importante que se crie, quando couber, cargos específicos de TI no Plano de Cargos e Carreiras e que se evite, ao máximo, o desvio de finalidade dos contratos de terceirização de TI.

4.5 Auditoria de TI

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.

Nesta perspectiva, a auditoria de TI consiste em verificar um ou vários aspectos da Governança de TI de uma organização. Assim, uma auditoria de TI pode, por exemplo, avaliar desde controles de acesso lógico ao ambiente de TI, por meio de análise de vulnerabilidade, até a segurança de sistemas de informação; ou ainda, verificar se a contratação de bens e serviços de TI é feita de acordo com as normas da organização e a legislação vigente.

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.

Os dados obtidos no questionário mostraram que a quase totalidade dos órgãos/entidades da Administração Pública Estadual não possui processo formalizado

de auditoria de Tecnologia da Informação. Este é um fato preocupante, já que 93% dos jurisdicionados pesquisados não fazem a verificação, avaliação e controle dos diversos aspectos da governança corporativa de TI, gestão de riscos e procedimentos de aderência às normas regulatórias.

4.6 Gerência de projetos

Gerenciar um projeto é atuar de forma a atingir os objetivos propostos dentro de parâmetros de qualidade determinados, obedecendo a um planejamento prévio de prazos (cronograma) e custos (orçamento). Ou seja, dadas as metas e as restrições de recursos e tempo, cabe ao gerente de projetos garantir que ele atinja os objetivos propostos.

Em toda e qualquer instituição é necessário estar com os projetos alinhados visando o sucesso da organização como um todo. Com práticas cada vez mais desenvolvidas, a Gerência de Projetos é uma realidade totalmente presente na vida dos profissionais de TI. O gerenciamento de projetos tem como objetivo principal simplificar a avaliação das diversas iniciativas em andamento e em planejamento, de forma a garantir a otimização dos recursos nos projetos vitais.

Uma vez que os projetos de TI tornaram-se cada vez mais estratégicos dentro da instituição, e muitas vezes importando em valores significativos, é de suma importância a utilização de um processo formal de Gerenciamento de Projetos de TI.

O *Project Management Body of Knowledge* (PMBOK) é um conjunto de práticas em gerência de projetos levantado pelo *Project Management Institute* (PMI) e constitui uma base da metodologia de gerência de projetos.

Este levantamento buscou identificar se as instituições do estado utilizam algum processo formal de Gerenciamento de Projetos de TI, tal como o PMBOK.

De acordo com o questionário, 84% dos órgãos/entidades pesquisados não possuem um processo formal de Gerenciamento de Projetos de TI. Este dado mostra que a grande maioria dos jurisdicionados ainda não se preocupa em gerenciar os seus projetos, o que pode acarretar na ineficácia do cumprimento de metas e prazos, assim como no desperdício dos recursos utilizados.

O PMI é uma organização mundial de referência no que se refere a Gerenciamento de Projetos, fazendo um trabalho de avanço da área e aplicação das modernas técnicas relacionadas a este assunto. Um dos mais significativos feitos desta instituição é a certificação formal de gerentes de projetos, *Project Management Professional* (PMP). Esta certificação auxilia a garantir os mais altos padrões profissionais e éticos na comunidade de profissionais de Gerenciamento de Projetos.

A certificação PMP é amplamente reconhecida como evidência de formação, conhecimento e experiência em gerenciamento de projetos e é uma das mais valorizadas por diversas instituições do mercado.

Na pesquisa realizada, foi constatado que 84% dos órgãos/entidades participantes não possuem servidores/empregados com certificação PMP. Com este dado, tem-se que a grande maioria dos jurisdicionados pesquisados ainda não possui

colaboradores com conhecimento certificado em Gerência de Projetos, o que pode acarretar na dificuldade destes órgãos em implantarem e utilizarem a Gerência de Projetos de forma eficiente.

O Escritório de Projetos é o local destinado a centralizar a condução, planejamento, organização, controle e finalização das atividades dos projetos. É o ambiente onde se pode obter uma visão global e panorâmica de todos os projetos. Seu modelo pode variar de acordo com a maturidade da organização, mas, em geral, sugere uma administração centralizada do portfólio de projetos, oferecendo um ponto único de contato e de apoio à decisão.

Na área de Tecnologia da Informação, o Escritório de Projetos tem crescido enormemente, pois, simplifica e otimiza o gerenciamento de projetos a um custo baixo. Ele tem se mostrado muito útil em organizações que gerenciam muitos projetos simultaneamente, aliviando o trabalho dos gerentes de projetos ao compartilhar a execução das tarefas de planejamento e acompanhamento.

A pesquisa realizada mostrou que apenas 7% dos órgãos/entidades abordados possuem um Escritório de Projetos formalmente implantado. Portanto, a grande maioria 93% dos jurisdicionados ainda não têm a cultura da utilização de Escritórios de Projetos, o que pode acarretar na ineficiência da gerência dos projetos.

4.7 Gerenciamento de serviços

Ponto único de contato caracteriza-se por um setor específico dentro da área de TI que tem atendentes de primeiro nível que recebem os chamados dos usuários. Tal área coordena o ciclo de vida dos incidentes desde o registro até o fechamento. Sua missão é restabelecer a operação normal dos serviços dos usuários o mais rápido possível, utilizando soluções de contorno, além de acompanhar os chamados até a solução definitiva do problema.

Conforme informações levantadas através do questionário, verificou-se que 34% dos órgãos/entidades pesquisados não possuem ponto único de contato para atender às necessidades de TI. Uma informação preocupante, pois a inexistência de um ponto único de contato dificulta a comunicação entre os usuários e as equipes de TI, bem como aumenta os riscos de impacto no negócio causados por falhas nos serviços de TI, não restaurados nos prazos pré-estabelecidos pela organização.

Incidente é qualquer evento que causa redução ou interrupção do serviço do usuário. Problema é quando a causa responsável por um ou mais incidentes não é conhecida. O processo de Gerenciamento de Incidentes visa restaurar o serviço o mais rápido possível, além de fornecer um nível de serviço com mais qualidade, dando apoio ao cumprimento dos Acordos de Nível de Serviço (ANS). O processo de Gerenciamento de Problemas tem por objetivo principal identificar a causa-raiz dos incidentes, prevenindo a recorrência dos mesmos.

A maioria dos órgãos/entidades participantes do levantamento (67%) informou que não possui formalmente implantado processo de Gerenciamento de Incidentes/Problemas. A ausência desses processos pode causar aumento do tempo de indisponibilidade dos serviços, baixa qualidade dos serviços e incidentes recorrentes, gerando, com isso, impacto negativo na organização.

Mudança é qualquer alteração realizada na infra-estrutura de TI, seja ela relativa a hardware ou software, visando atender aos requisitos de negócio da organização, como por exemplo, a substituição de um computador servidor de correio eletrônico por outro com maior poder de processamento ou a alteração de uma rotina de um sistema de informação.

O objetivo do processo de Gerenciamento de Mudanças é gerenciar todas as mudanças que possam causar impacto na capacidade da área de TI de entregar serviços, através de um ponto único e centralizado de aprovação, programação e controle da mudança, para assegurar que a infra-estrutura de TI permaneça alinhada aos requisitos do negócio, com menor risco possível.

Um percentual expressivo dos órgãos/entidades pesquisados (88%) não possuem formalmente implantado um processo de Gerenciamento de Mudanças e, com isso, correm o risco do aparecimento de falhas e incidentes em decorrência de mudanças realizadas no ambiente operacional.

Os Acordos de Níveis de Serviço (ANS) balanceiam a demanda dos serviços de TI e o custo da provisão desses serviços, com base no conhecimento dos requisitos dos usuários e nas capacidades de TI da organização. É o principal instrumento de negociação de qualidade de serviço entre a área de TI e os seus usuários. Um ANS estabelece como um determinado serviço deve ser prestado pelo fornecedor aos clientes daquele serviço, definindo o nível de qualidade que o usuário espera receber. Obviamente para isso, a área de TI deve estar estruturada adequadamente para poder entregar os serviços dentro dos parâmetros, ou do nível, de qualidade acordada com seus usuários.

A sua ausência em 84% dos pesquisados preocupa, considerando que as consequências mais prováveis para este cenário são usuários insatisfeitos, baixa qualidade dos serviços e investimentos inadequados.

Como citado acima, um Acordo de Níveis de Serviço (ANS) busca estabelecer o nível de qualidade da prestação de um determinado serviço entre o prestador e quem recebe aquele serviço. Um ANS entre a área de TI e seus fornecedores externos é estabelecido através de um Contrato de Apoio (CA) para garantir a entrega dos serviços prestados, com base na relação entre o custo e a qualidade.

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 atender às necessidades dos seus usuários, a ausência da gestão dos fornecedores externos resulta em usuários insatisfeitos, baixa qualidade dos serviços e investimentos inadequados.

O processo de Gerenciamento Financeiro de TI controla os custos da entrega de serviços de TI que suportam as necessidades de negócio da organização. Ajuda a área de TI a gerenciar os recursos de TI necessários para o fornecimento de serviços de TI a um custo compensador.

Através do levantamento verificou-se que a grande maioria dos órgãos/entidades

pesquisados (88%) não possui processo de Gerenciamento Financeiro de Serviços de TI, fato que poderá resultar em serviços com alto custo e/ou pouco benefício para a organização.

O processo de Gerenciamento da Capacidade tem por objetivo determinar a capacidade da infra-estrutura de TI de forma correta, e com custos justificáveis, visando o atendimento dos níveis de serviço acordados com os clientes.

A ausência de um processo de Gerenciamento da Capacidade em 88% dos pesquisados expõe o risco de indisponibilidade dos serviços desses órgãos/entidades, e de inviabilidade de expansão e implantação de novos serviços.

O processo de Gerenciamento da Continuidade visa garantir que, depois de um desastre, ou qualquer outro incidente imprevisível, a infra-estrutura e os serviços de TI exigidos (sistemas, redes, aplicações, telecomunicações, etc) possam ser restaurados dentro dos limites de tempo pré-estabelecidos, e em níveis acordados para suportar os requisitos mínimos do negócio da organização. O objetivo é evitar ou reduzir ao máximo a descontinuidade de atividades críticas da instituição.

A ausência de um processo de Gerenciamento da Continuidade em 91% dos pesquisados constitui um alto risco para essas instituições em caso de interrupção de serviços por causas naturais ou intencionais.

O objetivo da Pesquisa de Satisfação é mensurar o que os usuários estão pensando e sentindo sobre os serviços prestados pela área de TI da organização, provendo informações necessárias para a identificação de oportunidades de melhoria. O cliente é quem pode melhor avaliar a qualidade da prestação de um serviço.

A sua ausência foi identificada em mais da metade dos órgãos/entidades pesquisados (60%), caraterizando pouca preocupação, por parte dessas instituições, em serem avaliadas por seus usuários, bem como baixo interesse na melhoria da qualidade de seus serviços.

O Gráfico 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.

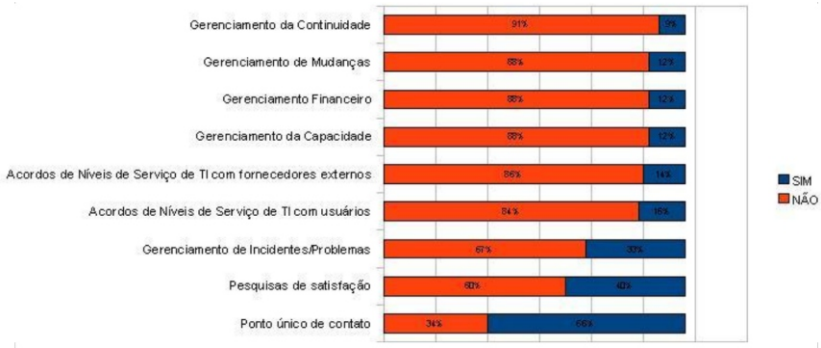


Gráfico 3 – Situação geral do Gerenciamento de Serviços de TI na Administração Pública Estadual

4.8 Processo de gestão de contratos de TI

De acordo com a pesquisa realizada, observou-se que em 40% dos órgãos/entidades da Administração Pública Estadual não existe a prática de designar formalmente um gestor ou fiscal para acompanhar a execução dos contratos de TI.

A Lei nº 8.666/1993, em seu Art. 67, traz a seguinte previsão: "A execução do contrato deverá ser acompanhada e fiscalizada por um representante da Administração especialmente designado, permitida a contratação de terceiros para assisti-lo e subsidiá-lo de informações pertinentes a essa atribuição".

Assim como qualquer tipo de contrato, um contrato de TI precisa ser fiscalizado por um conhecedor da área referente ao seu objeto, bem como por alguém que participe diretamente da execução e entrega dos serviços/produtos contratados.

4.9 Processo orçamentário de TI

Conforme recomendações do Tribunal de Contas da União (TCU) e melhores práticas de Governança de TI, como por exemplo, o processo PO5 (Gerenciar o investimento de TI) do *framework* COBIT v4.1, o gestor de TI deverá realizar o planejamento orçamentário de TI da instituição com, no mínimo, um ano de antecedência em relação ao exercício fiscal a que se refere. O referido planejamento deverá contemplar os gastos pretendidos com bens e serviços de TI, com detalhes suficientes para fundamentar a proposta do órgão/entidade e posterior verificação de alinhamento com o planejamento institucional. Além disso, o planejamento orçamentário de TI deverá prever o acompanhamento de execução do planejamento institucional, sem prejuízo da possibilidade de ajustes em decorrência de variações no suprimento orçamentário ou de mudanças nas demandas do órgão/entidade.

Dos 58 órgãos/entidades pesquisados, 22 (38%) informaram a não participação do gestor de TI na elaboração do orçamento da instituição. Essa é uma situação preocupante e sua causa pode estar associada à falta de visão e cultura da organização, com relação ao planejamento dos gastos de TI. Isso poderá dificultar, ou até mesmo inviabilizar, a obtenção de recursos financeiros necessários para aquisição de bens e serviços de TI. Outra possível consequência indesejável é o não alinhamento do planejamento de TI com o planejamento institucional, com a área de TI não produzindo os resultados esperados pela instituição.

4.10 Conclusão

O objetivo deste levantamento foi coletar informações relevantes sobre a Governança de TI para subsidiar os trabalhos futuros da Comissão Especial de Auditoria de Tecnologia da Informação, 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. Participaram do levantamento os 58 órgãos/entidades jurisdicionados do TCE-CE.

O levantamento sobre a Governança de TI contemplou as seguintes áreas relativas aos temas: Governança de TI, 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.

O Relatório de Inspeção apontou que entre os maiores problemas relativos a Governança de TI encontrados entre os jurisdicionados, estão:

I) ausência de planejamento estratégico de TI – dos 58 jurisdicionados apenas 39 responderam que possuem planejamento estratégico de TI;

II) ausência de Plano de Continuidade do Negócio (PCN) em todos os órgãos /entidades;

III) ausência de processo de desenvolvimento de software – apenas 8 jurisdicionados possuem processo de desenvolvimento de software;

IV) deficiência de Segurança da Informação – apenas 12 órgãos responderam que possuem Política de Segurança da Informação;

V) ausência de quadro de pessoal próprio na área TI – apenas 12 órgãos possuem no Plano de Cargos e Carreiras cargos específicos para a área de TI. A grande maioria dos colaboradores na área de TI são terceirizados, com um percentual de 67%. Servidores próprios do órgão correspondem a 27%, estagiários 3% e servidores cedidos 3%;

VI) ausência de processo formalizado de auditoria de TI – apenas 4 órgãos informaram possuir auditoria interna de TI;

VII) ausência de processo formalizado de gerenciamento de projetos – apenas 9 órgãos responderam possuir processo formal de gerenciamento de projetos de TI;

VIII) ausência de processo formalizado de gerenciamento de serviços – apenas 5 órgãos responderam possuir formalmente implantado processo de gerenciamento da continuidade abordando a capacidade da organização de TI em continuar a fornecer serviços acordados com os usuários

IX) ausência de processo de gestão de contratos de TI - 23 órgãos informaram não possuir formalmente designação de gestor/fiscal para os contratos de TI;

X) ausência de processo orçamentário de TI – 22 órgãos informaram que os gestores de TI não participam da elaboração e planejamento orçamentário;

Diante desse cenário, existe um campo vasto para atuação desse Tribunal na área de Governança de TI da Administração Pública Estadual, possibilitando oportunidades de melhorias na gestão e no uso de recursos de Tecnologia da Informação e Comunicação (TIC) por parte dos órgãos/entidades estaduais.

5. BENEFÍCIOS

As informações coletadas no presente trabalho possibilitarão à Comissão Especial de Auditoria de Tecnologia da Informação o planejamento e a realização das ações de controle de forma mais efetiva e auxiliará no planejamento das auditorias que farão parte do Plano Anual de Auditoria do TCE-CE e do Plano de Ações Anual da Comissão.

As determinações e recomendações contidas na RESOLUÇÃO Nº 3550/2010, sob a relatoria do Conselheiro Edilberto Carlos Pontes Lima, fornecerão instrumentos para a Comissão realizar o monitoramento das ações a serem realizadas pelos órgãos/entidades, permitindo às equipes de futuras fiscalizações na área de TI otimizar os recursos utilizados nos seus trabalhos.

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 a alta administração por recursos orçamentários para a área.

6. RESOLUÇÃO

RESOLUÇÃO Nº 3550/2010
PROCESSO Nº 07836/2009-6

VISTOS, ETC...

CONSIDERANDO que cuidam os autos sobre inspeção realizada pela Comissão Especial de Auditoria de Tecnologia da Informação, constituída no âmbito desta Corte de Contas para atuar na fiscalização de gestão e uso de recursos de Tecnologia da Informação e Comunicação (TIC) pela Administração Estadual, objetivando levantar informações acerca da situação da governança de tecnologia da informação (TI) da Administração Pública Estadual, identificando como fiscalizar a gestão e o uso de TI pelos órgãos e entidades estaduais;

CONSIDERANDO que a Comissão Especial de Auditoria de Tecnologia iniciou os trabalhos levantando os órgãos que compõem a Administração Estadual, identificando 58 órgãos/entidades jurisdicionados do TCE-CE;

CONSIDERANDO que os órgãos/entidades responderam a um questionário eletrônico desenvolvido pela CEATI contemplando as seguintes áreas relativas aos temas: 1) Governança de TI, 2) Planejamento Estratégico Institucional e de TI, 3) Segurança da Informação, 4) Processo de Desenvolvimento de Software, 5) Estrutura de Pessoal de TI, 6) Auditoria de TI, 7) Gerência de Projetos, 8) Gerenciamento de Serviços, 9) Processo de Gestão de Contratos de TI e 10) Processo Orçamentário de TI;

CONSIDERANDO que as respostas apresentadas revelaram os principais problemas de tecnologia da informação na Administração Pública Estadual, concluindo a CEATI, no Relatório de Inspeção Nº 0002/2009, pela necessidade de recomendações aos órgãos jurisdicionados, sugerindo, às fls. 45/47, verbis:

> **'5.1 recomendar a este Tribunal através de sua Secretaria de Controle Externo, que promova um seminário com a participação dos jurisdicionados desta Corte de Contas para que seja dado conhecimento do conteúdo do presente relatório;**
> **5.2 recomendar à Controladoria e Ouvidoria Geral do Estado – CGE que realize regularmente auditorias de TI e/ou promova ações para estimular a realização dessas auditorias nos órgãos/entidades da Administração Pública Estadual (Poder Executivo);**
> **5.3 recomendar à Secretaria do Planejamento e Gestão do Estado – SEPLAG que, nos órgãos/entidades da Administração Publica Estadual (Poder Executivo):**
> **5.3.1 promova 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;**
> **5.3.2 oriente sobre a importância do gerenciamento da segurança da informação, promovendo ações que visem estabelecer e/ou aperfeiçoar a gestão da continuidade do**

negócio, a análise de riscos de TI, os procedimentos de controle de acesso a recursos de TI, a política para o uso de TI móvel, a política de segurança da informação, a classificação da informação, o inventário de hardware e software, implantação de área específica para gerenciamento da segurança da informação e a política de cópia de segurança (*backup*);[ressaltando-se a existência do Decreto Nº29.227, de 13/03/2008, que trata sobre a Política de Segurança da Informação dos Ambientes de Tecnologia da Informação e Comunicação (TIC) para os órgãos/entidades do Poder Executivo Estadual];

5.3.3 estimule a adoção de processo de desenvolvimento de *software,* procurando assegurar, nesse sentido, níveis razoáveis de padronização e bom grau de confiabilidade e segurança;

5.3.4 atente para a necessidade de dotar a estrutura de pessoal de TI do quantitativo de servidores efetivos necessário ao pleno desempenho das atribuições do setor, notadamente atividades sensíveis e estratégicas, garantindo a sua capacitação, como forma de evitar o risco de perda de conhecimento organizacional, pela atuação excessiva de colaboradores externos não comprometidos com a instituição;

5.3.5 introduza 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;

5.3.6 estimule a adoção de um processo formal de Gerenciamento de Projetos, garantindo recursos para a capacitação e certificação dos servidores da instituição;

5.3.7 promova 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, orientando quanto ao gerenciamento de continuidade, gerenciamento de mudanças, gerenciamento financeiro, gerenciamento de capacidade e o gerenciamento de incidentes/problemas, baseando-se em normas e melhores práticas do mercado, como por exemplo, ITIL, NBR ISO/IEC 20000 e COBIT;

5.3.8 envide esforços visando à implementação de processo de gestão de contratos de TI, conforme recomendado no Art. 67 da Lei nº 8.666/1993;

5.3.9 adote providências com vistas a garantir a participação da área de TI no processo de elaboração do orçamento da instituição, de forma a garantir a inclusão dos projetos de TI e o alinhamento destes aos objetivos institucionais.

5.4 recomendar ao Tribunal de Contas dos Municípios – TCM e ao Tribunal de Justiça do Ceará – TJ, que adotem, no âmbito de sua instituição, as providências contidas nos itens 5.3.2 a 5.3.9;

5.5 recomendar à Assembleia Legislativa do Ceará e a Procuradoria Geral de Justiça do Ceará – PGJ que adotem, no âmbito de suas instituições, as providências contidas no item 5.3;

5.6 recomendar à Presidência deste Tribunal, que seja dado conhecimento do presente relatório à Controladoria e à Secretaria de Tecnologia da Informação desta Corte de Contas para que sejam adotadas as providências contidas no item 5.3;

5.7 determinar à Secretaria do Planejamento e Gestão do Estado – SEPLAG que oriente os órgãos/entidades da Administração Publica Estadual (Poder Executivo), que não elaboraram o planejamento estratégico de TI, que o realizem conforme previsto na Resolução Nº 01 de 11/06/2008;
5.8 determinar à Assembleia Legislativa do Ceará, Procuradoria Geral de Justiça do Ceará – PGJ, ao Tribunal de Contas dos Municípios – TCM, ao Tribunal de Justiça do Ceará – TJ e à Secretaria do Planejamento e Gestão do Estado – SEPLAG que elabore um cronograma para a realização das recomendações elencadas neste relatório, dando ciência ao TCE para que seja realizado o monitoramento do andamento destas atividades.";

CONSIDERANDO que, instado a se manifestar o MP Especial emitiu Parecer Nº 427/2010, às fls. 115/118, da lavra do Procurador Geral, Gleydson Antônio Pinheiro Alexandre, opinando no sentido de que, verbis:

'a) sejam acatadas as sugestões propostas pela Comissão Especial de Tecnologia da Informação;
b) recomende-se aos 58 (cinquenta e oito) jurisdicionados desta Corte de Contas:
b.1.) a criação de cargos efetivos específicos para área de Tecnologia da Informação;
b.2.) caso a sugestão anterior não seja acolhida, a realização de concurso público pelo Estado do Ceará através da Empresa de Tecnologia da Informação do Estado do Ceará, ETICE, para a contratação de servidores voltados ao setor de TI, com a posterior cessão desses agentes aos demais órgãos e entidades do Estado do Ceará;
b.3.) que o agente responsável pelo setor de Tecnologia da Informação do órgão ou entidade seja um servidor público efetivo;
c.) determine-se às entidades pesquisadas possuidoras de terceirizados de TI sem exercer atividades específicas na área em comento (fl. 105) que promovam a readequação dos contratos de terceirização de serviços de TI correspondentes.
d.) determine-se à Empresa de Tecnologia da Informação do Estado do Ceará, ETICE, que promova a substituição dos terceirizados atuantes na área de TI por servidores efetivos, a fim de que seja dado cumprimento ao art. 37, II, da CF/88;";

CONSIDERANDO que o relator, inicialmente ressaltou, o trabalho desenvolvido pela Comissão Especial de Tecnologia da Informação, analisando que o Relatório de Inspeção Nº 0002/2009, apontou que entre os maiores problemas encontrados entre os jurisdicionados, estão:

I) ausência de planejamento estratégico de TI – dos 58 jurisdicionados apenas, 39 responderam que possuem planejamento estratégico de TI;

II) ausência de Plano de Continuidade do Negócio (PCN) em todos os órgãos /entidades;

III) ausência de processo de desenvolvimento de software – apenas 8 jurisdicionados possuem processo de desenvolvimento de software;

IV) ausência de Segurança da Informação – apenas 12 órgãos responderam que possuem Política de Segurança da Informação;

V) ausência de quadro de pessoal próprio na área TI – apenas 12 órgãos possuem no Plano de Cargos e Carreiras cargos específicos para a área de TI (grande

maioria dos colaboradores na área de TI são terceirizados, correspondem 67%, servidores próprios do órgão, correspondem 27%, estagiários 3% e servidores cedidos 3%);

VI) ausência de processo formalizado de auditoria de TI – apenas 4 órgãos informaram possuir auditoria interna de TI;

VII) ausência de processo formalizado de gerenciamento de projetos – apenas 9 órgãos responderam possuir processo formal de gerenciamento de projetos de TI;

VIII) ausência de processo formalizado de gerenciamento de serviços – apenas 5 órgãos responderam possuir formalmente implantado processo de gerenciamento da continuidade abordando a capacidade da organização de TI em continuar a fornecer serviços acordados com os usuários

IX) ausência de processo de gestão de contratos de TI- 23 órgãos informaram não possuir formalmente designação de gestor/fiscal para os contratos de TI;

X) ausência de processo orçamentário de TI – 22 órgãos informaram que os gestores de TI não participam da elaboração e planejamento orçamentário;

CONSIDERANDO que o relator votou, na sessão plenária de 29/06/2010, adotando a manifestação da Comissão Especial de Auditoria de Tecnologia da Informação como suas razões de decidir, acolhendo integralmente a proposta alvitrada pelo representante do Ministério Público de Contas;

CONSIDERANDO que, na mesma sessão, a Conselheira Soraia Victor pediu vistas, apresentando em 19/10/2010 declaração de voto, no qual usou o termo determinação ao invés de recomendação, utilizado no voto apresentado pelo relator, e estabeleceu prazo para o cumprimento das determinações contidas nas alíneas “a” a “k” de seu voto;

CONSIDERANDO que, após a apresentação do voto-vista, o relator solicitou o retorno dos autos ao seu gabinete para melhor análise, reapresentando na sessão de 14/12/2010, com voto mantendo o posicionamento anteriormente proferido, no sentido de recomendar à administração, ao invés de determinar, como manifestado no voto-vista apresentado, por entender que as sugestões apontadas pela Inspetoria tratam de atuação gerencial, que competem ao administrador a forma como melhor desenvolvê-las, assim manteve o voto proferido anteriormente, aderindo às recomendações traçadas pela Comissão Especial de Auditoria de Tecnologia da Informação e em parte ao voto-vista prolatado pela Conselheira Soraia Victor, da forma a seguir:

> 1. recomendar a este Tribunal através de sua Secretaria de Controle Externo, que promova um seminário com a participação dos jurisdicionados desta Corte de Contas para que seja dado conhecimento do conteúdo do presente relatório;
> 2. recomendar à Controladoria e Ouvidoria Geral do Estado – CGE que realize regularmente auditorias de TI e/ou promova ações para estimular a realização dessas auditorias nos órgãos/entidades da Administração Pública Estadual (Poder Executivo);
> 3. recomendar à Secretaria do Planejamento e Gestão do Estado – SEPLAG que, nos órgãos/entidades da Administração Publica Estadual (Poder Executivo):
> 3.1 promova 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;
3.2 oriente sobre a importância do gerenciamento da segurança da informação, promovendo ações que visem estabelecer e/ou aperfeiçoar a gestão da continuidade do negócio, a análise de riscos de TI, os procedimentos de controle de acesso a recursos de TI, a política para o uso de TI móvel, a política de segurança da informação, a classificação da informação, o inventário de hardware e software, implantação de área específica para gerenciamento da segurança da informação e a política de cópia de segurança (*backup*);[**ressaltando-se a existência do Decreto Nº29.227, de 13/03/2008, que trata sobre a Política de Segurança da Informação dos Ambientes de Tecnologia da Informação e Comunicação (TIC) para os órgãos/entidades do Poder Executivo Estadual**];
3.3 estimule a adoção de processo de desenvolvimento de software, procurando assegurar, nesse sentido, níveis razoáveis de padronização e bom grau de confiabilidade e segurança;
3.4 atente para a necessidade de dotar a estrutura de pessoal de TI do quantitativo de servidores efetivos necessário ao pleno desempenho das atribuições do setor, notadamente atividades sensíveis e estratégicas, garantindo a sua capacitação, como forma de evitar o risco de perda de conhecimento organizacional, pela atuação excessiva de colaboradores externos não comprometidos com a instituição;
3.5 introduza 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;
3.6 estimule a adoção de um processo formal de Gerenciamento de Projetos, garantindo recursos para a capacitação e certificação dos servidores da instituição;
3.7 promova 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, orientando quanto ao gerenciamento de continuidade, gerenciamento de mudanças, gerenciamento financeiro, gerenciamento de capacidade e o gerenciamento de incidentes/problemas, baseando-se em normas e melhores práticas do mercado, como por exemplo, ITIL, NBR ISO/IEC 20000 e COBIT;
3.8 envide esforços visando à implementação de processo de gestão de contratos de TI, conforme recomendado no Art. 67 da Lei nº 8.666/1993;
3.9 adote providências com vistas a garantir a participação da área de TI no processo de elaboração do orçamento da instituição, de forma a garantir a inclusão dos projetos de TI e o alinhamento destes aos objetivos institucionais;

4. recomendar ao Tribunal de Contas dos Municípios – TCM e ao Tribunal de Justiça do Ceará – TJ, que adotem, no âmbito de sua instituição, as providências contidas nos itens 3.2 a 3.9;

5. recomendar à Assembleia Legislativa do Ceará e a Procuradoria Geral de Justiça do Ceará – PGJ que adotem, no âmbito de suas instituições, as providências contidas no item 3;

6. recomendar à Presidência deste Tribunal, que seja dado conhecimento do presente relatório à Controladoria e à Secretaria de Tecnologia da Informação desta Corte de Contas para que sejam adotadas as providências contidas no item 3, no prazo de 180 (cento e oitenta) dias;

7. determinar à Secretaria do Planejamento e Gestão do Estado – SEPLAG que oriente os órgãos/entidades da Administração Publica Estadual (Poder Executivo), que não elaboraram o planejamento estratégico de TI, que o realizem conforme previsto na Resolução Nº 01 de 11/06/2008;

8. determinar à Assembleia Legislativa do Ceará, Procuradoria Geral de Justiça do Ceará – PGJ, ao Tribunal de Contas dos Municípios – TCM, ao Tribunal de Justiça do Ceará – TJ e à Secretaria do Planejamento e Gestão do Estado – SEPLAG que elaborem um cronograma para a realização das recomendações elencadas neste relatório, dando ciência ao TCE para que seja realizado o monitoramento do andamento destas atividades, nos prazos ali estabelecidos.

CONSIDERANDO que o relator votou, ainda, no que tange às recomendações do Ministério Público de Contas quanto à determinação de substituição dos terceirizados atuantes na área de TI por servidores efetivos, acompanhou o voto-vista da Conselheira Soraia Victor no sentido de que seja definido o modelo de TI para o Estado e, após tal providências, sejam adotadas as medidas para a realização de concurso público;

CONSIDERANDO o contido na instrução processual do presente feito;

CONSIDERANDO a legislação inerente à matéria;

RESOLVE O TRIBUNAL DE CONTAS DO ESTADO DO CEARÁ, por maioria de votos: 1) acolher a proposta do Parecer nº 427/2010-MP-TCE/CE, do Ministério Público de Contas, com a cientificação de todos os 58 (cinquenta e oito) órgãos/entidades inspecionados que compõem a Administração Pública Estadual por meio dos seus respectivos gestores de TI, como também a Empresa de Tecnologia da Informação do Estado do Ceará (ETICE), sobre o teor da decisão proferida por esta Corte, remetendo-lhes cópias do Relatório de Inspeção e da presente decisão; 2) acatar as recomendações traçadas pela Comissão de Tecnologia da Informação, além daquelas apontadas nos itens 1 a 8 do relatório às fls. 153/156; 3) determinar que seja definido o modelo de TI para o Estado e, após tais providências, sejam adotadas as medidas para a realização do concurso público, nos termos da Resolução.

Vencida a Conselheira Soraia Thomaz Dias Victor, com declaração de voto.

Participaram da votação os Exmos. Conselheiros Luís Alexandre Albuquerque Figueiredo de Paula Pessoa, José Valdomiro Távora de Castro Júnior, Pedro Augusto Timbó Camelo e o Exmo. Conselheiro Substituto Paulo César de Souza.

Transcreva-se e Cumpra-se.
Sala das Sessões, em 14 de dezembro de 2010.

Conselheiro Teodorico José de Menezes Neto
PRESIDENTE

Conselheiro Edilberto Carlos Pontes Lima
RELATOR

Gleydson Antônio Pinheiro Alexandre
PROCURADOR GERAL DO MINISTÉRIO PÚBLICO DE CONTAS

RESPONSABILIDADE EDITORIAL

Secretaria de Controle Externo
Comissão Especial de Auditoria de Tecnologia da Informação

Equipe de Auditoria
Paulo Alcântara Saraiva Leão(coordenador)
Cláudio Moreira Vinagre
José Alexsandre Fonseca da Silva
José Auriço Oliveira
Reuben Bezerra Barbosa

Elaboração
Paulo Alcântara Saraiva Leão
José Auriço Oliveira

TRIBUNAL DE CONTAS
DO ESTADO DO CEARÁ

CONSELHEIROS

Teodorico José de Menezes Neto
Presidente

José Valdomiro Távora de Castro Júnior
Vice-Presidente

Pedro Augusto Timbó Camelo
Corregedor

Luís Alexandre A. Figueiredo de Paula Pessoa
Soraia Thomaz Dias Victor
Edilberto Carlos Pontes Lima

AUDITORES
Itacir Todero
Paulo César de Souza

PROCURADORES DE CONTAS DO MINISTÉRIO PÚBLICO ESPECIAL
Gleydson Antônio Pinheiro Alexandre
Procurador-Geral

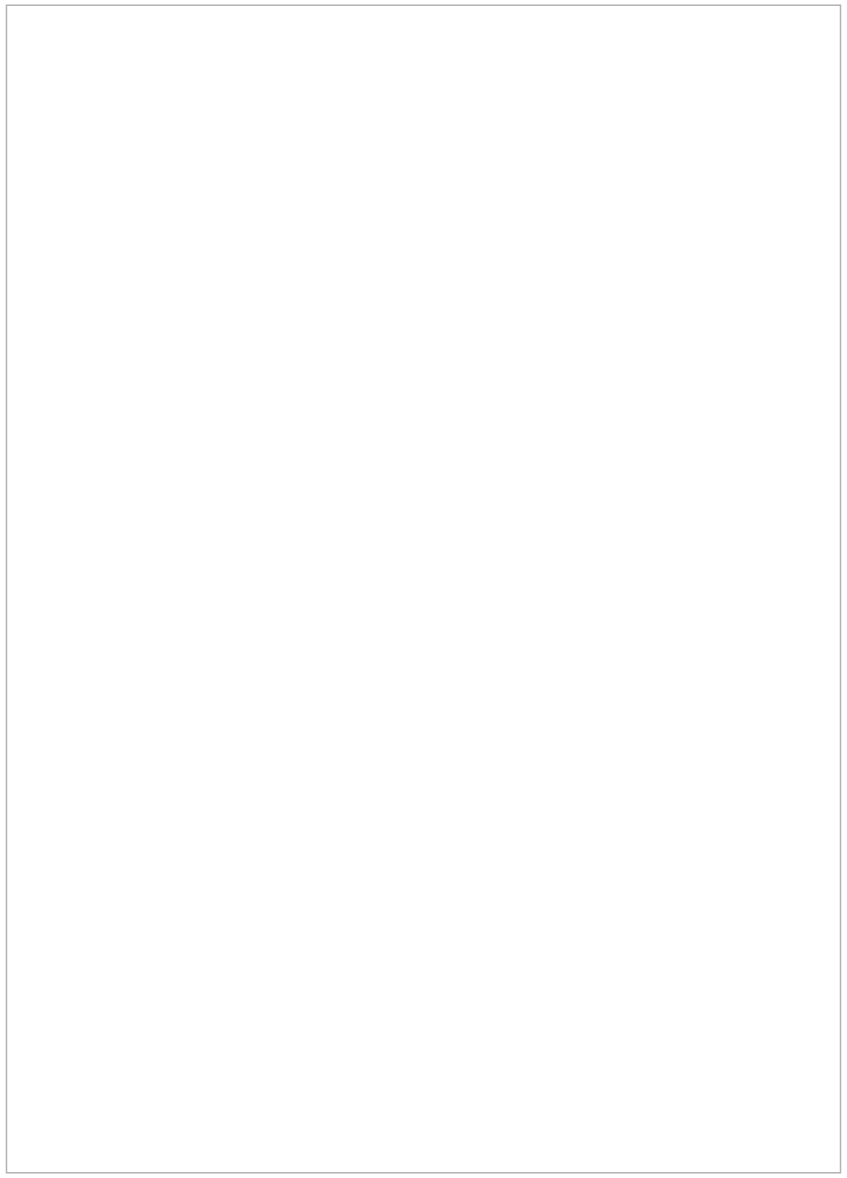
Rholden Botelho de Queiroz

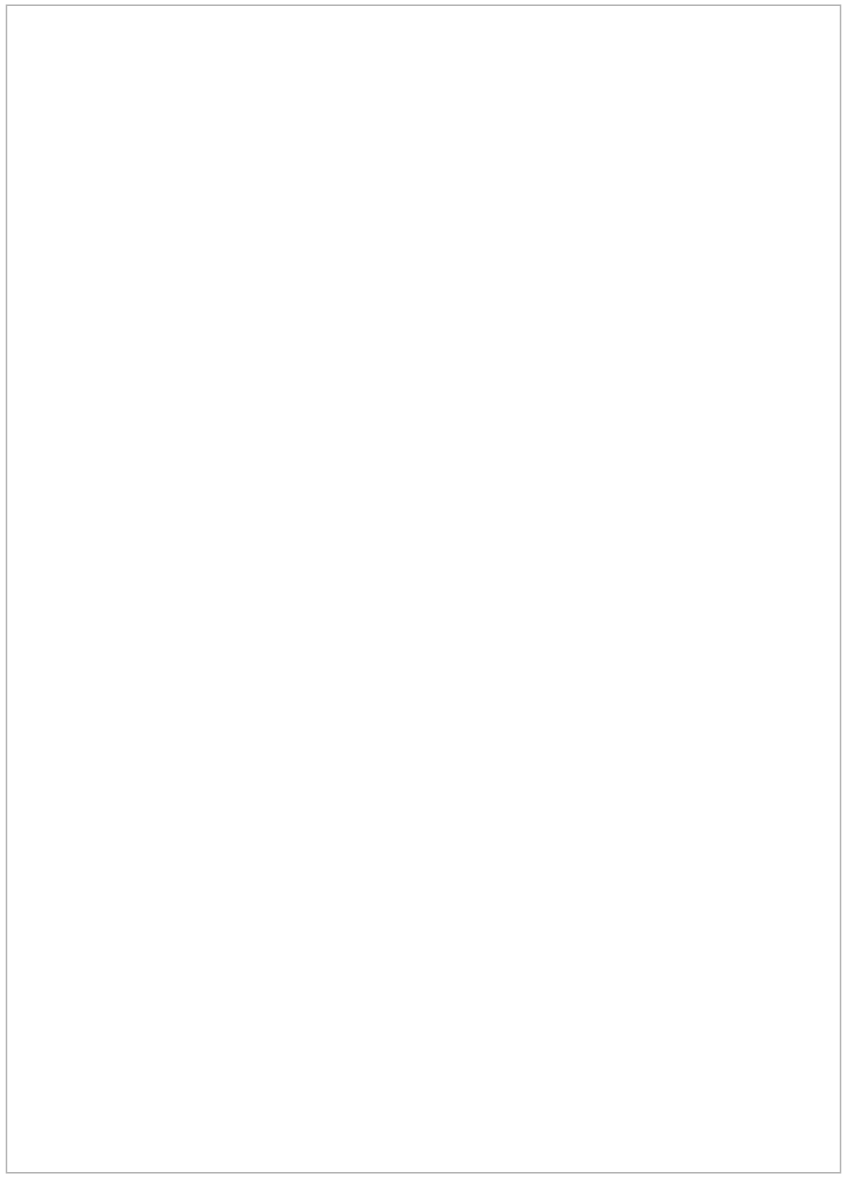
SECRETARIA DE CONTROLE EXTERNO
Giovanna Augusta Moura Adjafre
Secretária de Controle Externo

José Teni Cordeiro Júnior
Chefe da Coordenadoria Técnica

COMISSÃO ESPECIAL DE AUDITORIA DE TECNOLOGIA DA INFORMAÇÃO
Paulo Alcântara Saraiva Leão
Coordenador

SERVIDORES
Delinda Maria Almeida de Oliveira
José Auriço Oliveira
Raimir Holanda Filho
Claudio Vinagre Moreira
Reuben Bezerra Barbosa
José Alexsandre Fonseca da Silva





TRIBUNAL DE CONTAS DO ESTADO DO CEARÁ
Rua Sena Madureira, 1047 - Centro
CEP: 60-055-080 - Fortaleza - Ceará

www.tce.ce.gov.br