

**FUNDAÇÃO GETULIO VARGAS  
ESCOLA BRASILEIRA DE ADMINISTRAÇÃO PÚBLICA E DE EMPRESAS  
CENTRO DE FORMAÇÃO ACADÊMICA E PESQUISA  
CURSO DE MESTRADO EM ADMINISTRAÇÃO PÚBLICA**

**AUDITORIA DE TECNOLOGIA DA  
INFORMAÇÃO NA ADMINISTRAÇÃO PÚBLICA  
NO ÂMBITO DOS MUNICÍPIOS DO ESTADO DO  
RIO DE JANEIRO.**

**DISSERTAÇÃO APRESENTADA À ESCOLA BRASILEIRA DE ADMINISTRAÇÃO PÚBLICA E  
DE EMPRESAS PARA OBTENÇÃO DO GRAU DE MESTRE**

**GUSTAVO BASTOS MONTEIRO**

**Rio de Janeiro-2008**

**FUNDAÇÃO GETULIO VARGAS**  
**ESCOLA BRASILEIRA DE ADMINISTRAÇÃO PÚBLICA E DE EMPRESAS**  
**CENTRO DE FORMAÇÃO ACADÊMICA E PESQUISA**  
**CURSO DE MESTRADO EM ADMINISTRAÇÃO PÚBLICA**

**TÍTULO**


**AUDITORIA DE TECNOLOGIA DA INFORMAÇÃO NA ADMINISTRAÇÃO PÚBLICA: O  
CASO DOS MUNICÍPIOS DO ESTADO DO RIO DE JANEIRO**

**DISSERTAÇÃO DE MESTRADO APRESENTADA POR:**  
**GUSTAVO BASTOS MONTEIRO**

E

APROVADO EM \_\_\_\_ / \_\_\_\_ / \_\_\_\_

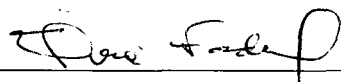
PELA COMISSÃO EXAMINADORA



**ALKETA PECCI**  
DOUTORA EM ADMINISTRAÇÃO



**LUIZ ANTONIO JOIA**  
DOUTOR EM CIÊNCIAS EM ENGENHARIA DE PRODUÇÃO



**ELVIA MIRIAM CAVALCANTI FADUL**  
PH.D EM URBANISME

## **RESUMO**

A difusão das doutrinas de gerenciamento orientadas para resultados no Brasil tem levado as organizações públicas a realizarem investimentos relevantes em tecnologia da informação como um componente de transparência para as ações governamentais e como suporte para a tomada de decisões pelos gestores públicos. O uso intensivo da informática em um mundo cada vez mais interconectado expõe a administração pública a novos tipos de ameaças e vulnerabilidades. Nesse contexto, as entidades de fiscalização devem ampliar sua forma de atuação, realizando controles mais rigorosos por meio de técnicas próprias de auditorias de tecnologia da informação, que visam assegurar a integridade e segurança dos dados que trafegam pelas redes e sistemas de informação. O objetivo da presente pesquisa consistiu em identificar as principais impropriedades associadas ao uso da informática nas administrações municipais sob a jurisdição do TCE-RJ, por meio do estudo de caso de sua experiência na realização de auditorias operacionais em tecnologia da informação. A pesquisa foi realizada com base na literatura e na análise dos achados das auditorias de sistemas, mostrando que este tipo de auditoria tem contribuído para tornar a gestão pública municipal mais eficiente, eficaz e transparente.

Palavras-chave: auditoria de tecnologia da informação; auditoria de sistemas; auditoria operacional; tribunal de contas; nova administração pública.

## **ABSTRACT**

The diffusion of results-oriented management doctrines has been leading the public organizations to make important investments in information technology as a component of transparency for government actions and support for decision-making by public administrators. The intensive use of information technology in an increasingly interconnected world exposes the government to new forms of threats and vulnerabilities. In this context, the Courts of Accounts must expand the scope of their acting, performing more stringent controls through specific technics in information technology (IT) audit to ensure the integrity and security of data that travel across networks and information systems. The purpose of this research consisted to identify main improprieties associated with the use of computers in the local public administrations under the jurisdiction of TCE-RJ, by means of the case study of its experience in the accomplishment of performance audit in information technology. The research is based on the literature and analysis of findings from systems audits, showing that this kind of audit has contributed to making local public administration more efficient, effective and transparent.

Key-words: information technology audit, systems audit, performance audit, court of accounts, new public management.

Dedico este trabalho

A minha esposa Rosimere, doce companheira e amiga de todas as horas, que suportou minhas ausências ao longo desta jornada, não deixando jamais de me apoiar.

A minhas amáveis filhas Julia, Leticia e Luiza pela força de suas presenças em minha vida, dando sentido e motivação.

A minhas avós Julieta (*in memoriam*) e Guiomar pelo exemplo de vida que nortearam meu caminho.

A meus pais Enir e Maria de Lourdes pelo amor e orientação dedicados em minha formação, fundamentais ainda hoje.

A meus irmãos Maria Fernanda e Marcelo pela amizade de todas as horas.

## **AGRADECIMENTOS**

Primeiramente agradeço a Deus por tudo, pela força e inspiração para superação de mais este desafio.

Aos Conselheiros José Maurício de Lima Nolasco e José Gomes Graciosa, que na condição de Presidentes do Tribunal de Contas do Estado do Rio de Janeiro, autorizaram e deram suporte para que a Instituição investisse na minha capacitação através do Mestrado.

Agradeço de modo especial aos amigos e colegas de trabalho Carlos Eduardo H. F. de Lemos e Sergio Lino da Silva Carvalho, que me apoiaram nesta longa jornada, dando sugestões e, principalmente, me incentivando a nunca desistir.

Aos colegas do Tribunal de Contas do Estado do Rio de Janeiro, especialmente à Dra. Paula Alexandra Nazareth e Celso Henrique de Oliveira, pelo apoio de todas as horas e pela extrema compreensão.

À Prof.<sup>a</sup> Alketa Peci pela orientação e valiosas sugestões para a melhoria deste trabalho.

Aos colegas da turma de mestrado, pelos momentos de estudo e dedicação compartilhados e pelas novas amizades conquistadas.

Aos professores do mestrado em administração pública da Fundação Getúlio Vargas pelos preciosos ensinamentos.

## LISTA DE QUADROS

	Pág.
Quadro 1 – Comparação entre auditoria tradicional e auditoria de desempenho.	40
Quadro 2 – Diferenças entre auditoria tradicional e auditoria operacional .....	42
Quadro 3 – Limitações da auditoria operacional .....	45
Quadro 4 – Aspectos técnicos verificados nos editais e contratos.....	58
Quadro 5 – Controle de Segurança da Informação.....	87
Quadro 6 – Categorias de análise identificadas .....	92

## LISTA DE FIGURAS

	Pág.
Figura 1 – Dimensões da Auditoria de Natureza Operacional.....	36
Figura 2 - Áreas de atuação da TI.....	55
Figura 3 – Fases de uma auditoria operacional .....	59
Figura 4 – Integração de Negócios à Arquitetura de Informações .....	68
Figura 5 – Governança de TI e Gerenciamento de TI .....	70
Figura 6 – Áreas de Domínio da Governança de TI .....	72
Figura 7 – Integração dos Modelos de Governança de TI.....	75
Figura 8 – Melhores práticas e padrões abrangidos pelo COBIT 4.1.....	77
Figura 9 – Arquitetura de TI.....	78
Figura 10 – <i>Framework</i> do COBIT .....	81
Figura 11 – Forma de Navegação nos processos do COBIT .....	82
Figura 12 - Modelo de Maturidade do COBIT.....	83

**LISTA DE TABELAS**

Pág.

Tabela 1 : Freqüências das categorias de análise ..... 93

**LISTA DE GRÁFICOS**

Pág.

Gráfico 1 – Planejamento estratégico na área de informática falho ou  
inexistente ..... 94

Gráfico 2 – Políticas de segurança da informação falhas ou inexistentes..... 97

Gráfico 3 – Procedimentos de contingência falhos ..... 99

Gráfico 4 – Procedimentos de cadastramentos de usuários na rede de  
computadores e nos sistemas de informação realizados sem  
formalidade..... 101

Gráfico 5 – Ausência de política de senha forte na rede de computadores e  
nos sistemas de informação ..... 103

Gráfico 6 – Ausência de campo específico nos sistemas de informação para  
registro de número do processo administrativo em operações  
críticas ..... 104

Gráfico 7 – Arquivos de log ausentes ou com registro falho nos sistemas de  
informação..... 106

Gráfico 8 – Sistema de informação em desacordo com legislação específica  
vigente ..... 107

Gráfico 9 – Divergência entre os valores registrados no sistema de controle  
da arrecadação e no sistema de contabilidade ..... 109

Gráfico 10 – Improriedades no instrumento contratual que ferem a legislação  
vigente, notadamente a Lei Federal nº 8.666/93 ..... 110

Gráfico 11 – Não execução ou execução parcial do objeto contratado..... 112



## LISTA DE SIGLAS

<b>ABNT</b>	.....	Associação Brasileira de Normas Técnicas
<b>CEDAE</b>	.....	Companhia Estadual de Águas e Esgoto
<b>ANOP</b>	.....	Auditorias de Natureza Operacional
<b>CERDS</b>	.....	Projeto de Aperfeiçoamento do Controle Externo com Foco na Redução da Desigualdade Social
<b>CRFB</b>	.....	Constituição da República Federativa do Brasil
<b>CPD</b>	.....	Centro de Processamento de Dados
<b>CPRH</b>	.....	Agência Estadual de Meio Ambiente e Recursos Hídricos
<b>DASP</b>	.....	Departamento Administrativo do Serviço Público
<b>DETRAN</b>	.....	Departamento de Trânsito
<b>EFS</b>	.....	Entidades de Fiscalização Superiores
<b>GAO</b>	.....	United States Government Accountability Office
<b>ILACIF</b>	.....	Instituto Latino-Americano e do Caribe de Ciências Fiscalizadoras
<b>INCOSAI</b>	.....	Congresso Internacional de Entidades Fiscalizadoras Superiores
<b>INTOSAI</b>	.....	Organização Internacional de Entidades Fiscalizadoras Superiores
<b>IPERJ</b>	.....	Fundo Único de Previdência Social do Estado do Rio de Janeiro
<b>IRE</b>	.....	Inspetoria Regional de Controle Externo
<b>LRF</b>	.....	Lei de Responsabilidade Fiscal
<b>MARE</b>	.....	Ministério da Administração Federal e Reforma do Estado
<b>NAO</b>	.....	National Audit Office
<b>OCDE</b>	.....	Organização para a Cooperação e o Desenvolvimento Econômico
<b>OLACEFS</b>	.....	Organização Latino-Americana e do Caribe de Entidades Fiscalizadoras Superiores
<b>PrND</b>	.....	Programa Nacional de Desburocratização
<b>PRODERJ</b>	.....	Centro de Tecnologia da Informação e Comunicação do Estado do Rio de Janeiro
<b>SGSI</b>	.....	Sistema de Gestão da Segurança da Informação
<b>TCE-RJ</b>	.....	Tribunal de Contas do Estado do Rio de Janeiro
<b>TCU</b>	.....	Tribunal de Contas da União
<b>TI</b>	.....	Tecnologia da Informação



## SUMÁRIO

1. INTRODUÇÃO.....	12
1.1 OBJETIVOS.....	14
1.2 DELIMITAÇÃO DO ESTUDO .....	15
1.3 RELEVÂNCIA DO ESTUDO .....	16
2. CONTROLE DA ADMINISTRAÇÃO PÚBLICA .....	18
2.1 CONTROLE INTERNO.....	20
2.2 CONTROLE EXTERNO.....	21
2.3 CONTROLES QUANTO AO MOMENTO .....	22
3. AUDITORIA OPERACIONAL.....	24
3.1 NOVA GESTÃO PÚBLICA E A AUDITORIA OPERACIONAL .....	24
3.2 AUDITORIA OPERACIONAL : EVOLUÇÃO HISTÓRICA.....	29
3.3 ASPECTOS GERAIS DA AUDITORIA OPERACIONAL.....	32
3.4 COMPARAÇÃO ENTRE A AUDITORIA OPERACIONAL E A AUDITORIA TRADICIONAL.....	39
3.5 LIMITAÇÕES DA AUDITORIA OPERACIONAL.....	43
4. AUDITORIA DE TI.....	47
4.1 DEFINIÇÃO DE AUDITORIA DE TI .....	47
4.2 A IMPORTÂNCIA DA AUDITORIA DE TI .....	48
4.3 A AUDITORIA DE TI NO TCE-RJ.....	49
4.4 DIFICULDADES À IMPLEMENTAÇÃO DE AUDITORIA DE TI NA ADMINISTRAÇÃO PÚBLICA.....	52
4.5 ÁREAS DE ATUAÇÃO .....	54
4.6 ETAPAS DA AUDITORIA DE TI NO TCE-RJ .....	59
4.7 METODOLOGIA DE AUDITORIA DE TI ADOTADA PELO TCE-RJ .....	65
5. GOVERNANÇA DE TECNOLOGIA DA INFORMAÇÃO .....	67
5.1 DIFERENÇA ENTRE GOVERNANÇA DE TI E GERENCIAMENTO DE TI.....	69
5.2 DOMÍNIOS DA GOVERNANÇA DE TI .....	71
5.3 MODELOS PARA SUPORTE A GOVERNANÇA TI.....	73
6. METODOLOGIA .....	88
6.1 TIPO DE PESQUISA .....	88
6.2 UNIVERSO E AMOSTRA .....	89
6.3 COLETA DE DADOS .....	90
6.4 TRATAMENTO DOS DADOS .....	90
6.5 LIMITAÇÕES DO MÉTODO .....	91
7. PESQUISA.....	92
8. CONCLUSÃO .....	113
9. REFERÊNCIAS BIBLIOGRÁFICAS .....	119
ANEXO A: LEGISLAÇÃO DE CONTROLE .....	126
ANEXO B: LEGISLAÇÃO APLICÁVEL À TI .....	127
ANEXO C: TABELA COBIT .....	128
ANEXO D: MATRIZ DE PLANEJAMENTO.....	129

## 1. INTRODUÇÃO

---

O fenômeno do desenvolvimento da auditoria operacional como modalidade de controle nas últimas décadas está relacionado a um conjunto de mudanças advindas da crise global do capitalismo ocorrida no final do século XX que afetaram um grande número de países desenvolvidos e a maioria dos países periféricos. No Brasil, a crise do Estado, como é conhecido o fenômeno, caracterizou-se como uma crise do Estado desenvolvimentista, em que o Estado foi sempre o indutor do desenvolvimento, por meio de uma enorme intervenção direta na economia.

No decorrer dos anos 90, com a crescente democratização do país, desenvolveram-se as medidas para reduzir o intervencionismo estatal, por intermédio de reformas como a privatização, a liberalização comercial e a abertura da economia.

O fenômeno da mudança de paradigma no controle da atividade estatal teve proporções mundiais, como é natural na era da globalização. As Entidades Fiscalizadoras perceberam a necessidade de extrapolar a atividade de verificação da legalidade e regularidade das contas públicas por informações e análises independentes acerca dos programas e projetos governamentais.

O Tribunal de Contas do Estado do Rio de Janeiro (TCE-RJ), órgão de controle externo ligado ao Poder legislativo, vem tradicionalmente exercendo um controle de natureza formal, que consiste na verificação da regularidade da execução dos gastos públicos, da legalidade dos atos administrativos e da fidedignidade dos demonstrativos financeiros. Essa forma de atuação corresponde ao modelo tradicional adotado no mundo capitalista e reflete a presença dominante da organização burocrática na administração pública.

Contudo, as transformações que vem sofrendo a sociedade moderna, principalmente com o fenômeno da globalização, que enfraqueceu a posição dos governos no controle dos fluxos financeiros e comerciais, impõem modificações

na forma de agir do Estado em relação às políticas públicas implementadas. O Estado deve agir como mediador entre o mercado e a sociedade, devendo garantir a implantação de políticas públicas que visem a minimizar as diferenças econômicas gritantes entre uma minoria abastada e uma maioria sem acesso à educação e sem condições de se inserir no mercado de trabalho.

Nesse contexto, a atuação do TCE-RJ é fundamental, pois como órgão fiscalizador do governo do estado e dos municípios, vem ampliando sua atuação, de forma a avaliar a qualidade dos serviços prestados pela administração pública, buscando orientar e redirecionar sua atuação.

Atualmente, as organizações públicas têm feito um uso cada vez mais intenso de Tecnologia da Informação (TI) como ferramenta de suporte às suas atividades. O tratamento das informações, conhecido como Tecnologia da Informação, Informática ou Sistemas de Informação, faz parte de toda cadeia de processos da organização, tendo se tornado componente crítico do planejamento, controle e execução das políticas públicas.

Surge daí a necessidade de se realizar procedimentos de auditoria em ambientes de TI para avaliar a eficácia dos controles aplicados sobre sistemas de informações em processamento eletrônico de dados.

O TCE-RJ realiza desde 1999 inspeções operacionais em Tecnologia da Informação (TI), com o objetivo de verificar o ambiente operacional dos sistemas de informação, sob a ótica da contingência e segurança da informação, e auditar um sistema aplicativo específico, buscando a prevenção e detecção de fraudes informatizadas, bem como o aperfeiçoamento dos controles lógicos existentes.

O propósito desta pesquisa consistiu em investigar a contribuição do TCE-RJ, por meio da auditoria da Tecnologia da Informação (TI), para o aperfeiçoamento da gestão pública.

Em nível prático, buscou-se verificar os achados de auditoria mais comuns, resultantes das inspeções de caráter operacional em Tecnologia da Informação realizadas pelo TCE-RJ, no âmbito das administrações municipais do estado do Rio de Janeiro.

Os dados analisados, aqui denominados impropriedades e deficiências, consistem nos principais achados de auditoria obtidos nas inspeções operacionais em TI nos municípios e referem-se a aspectos negativos da administração na área de informática, como práticas antieconômicas, ineficácia, ineficiência, desperdícios, uso indevido de recursos, gastos inadequados e descumprimento de leis e outras normas.

Sendo assim, o presente estudo visa responder à seguinte questão:

- Quais as principais impropriedades no uso da Tecnologia da Informação verificadas pelo TCE-RJ nas administrações municipais sob sua jurisdição?

## **1.1 OBJETIVOS**

### **Objetivo Final**

- Evidenciar as principais impropriedades constatadas nas auditorias de natureza operacional em TI realizadas pelo TCE-RJ nas administrações municipais sob sua jurisdição.

### **Objetivos Intermediários**

- A. Definir o que é auditoria operacional;
- B. Identificar na literatura disponível as normas, padrões e legislação aplicáveis à auditoria de natureza operacional em TI;
- C. Descrever a metodologia de auditoria de TI utilizada nas inspeções realizadas pelo TCE-RJ em âmbito municipal;
- D. Identificar e analisar os principais achados de auditoria das inspeções realizadas pelo TCE-RJ na área de TI à luz das principais normas adotadas pelas Entidades de Fiscalização Superiores (EFS).

## 1.2 DELIMITAÇÃO DO ESTUDO

Diante da ampla área de atuação do TCE-RJ, que engloba a estrutura do governo do Estado do Rio de Janeiro, com suas diversas secretarias e órgãos da administração indireta e empresas de economia mista, assim como os diversos municípios do Estado do Rio, com exceção da capital, faz-se necessária uma delimitação do escopo de atuação do estudo.

Com a importância dada pela Constituição de 1988 aos municípios, elevados a entes da federação, bem como por serem estes as instituições públicas mais próximas do cidadão, conhecendo como ninguém a realidade circundante, o estudo pretende restringir-se na avaliação, por parte do TCE-RJ, da utilização da Tecnologia da Informação como ferramenta estratégica de apoio às administrações municipais para a consecução de suas atividades.

Os municípios partilham parcelas de impostos federais e estaduais, existindo várias políticas sociais, particularmente nas áreas de saúde e educação fundamental, que contam com diretrizes e recursos federais, mas são implementadas principalmente pelos municípios. Estes entes federados dependem cada vez mais do uso intensivo de TI para realizar o controle tanto do planejamento quanto da execução de tais políticas.

O estudo pretende evidenciar as principais deficiências relacionadas à utilização de TI pelos municípios do estado do Rio de Janeiro nos aspectos ligados à gestão, execução, segurança da informação e gerenciamento de contratos relativos a bens e serviços de informática.

Os municípios foram selecionados para a pesquisa de forma a abranger as principais regiões do estado do Rio de Janeiro, com base na divisão utilizada pelo TCE-RJ para o exercício do controle externo em âmbito municipal. Para tal fim, o TCE-RJ divide o estado em sete grandes regiões, agrupando municípios de uma mesma área geográfica sob a jurisdição de uma Inspeção Regional de Controle Externo (IRE).

Pretende-se, com esse estudo, expor a importância das auditorias de TI para a melhoria na qualidade da gestão do ambiente de informática das administrações municipais.

### **1.3 RELEVÂNCIA DO ESTUDO**

O quadro de extrema desigualdade social que caracteriza a sociedade brasileira atual aliado à incapacidade do Estado em reverter essa situação impõe às entidades fiscalizadoras um papel cada vez mais importante no apoio às administrações públicas, no que tange ao aperfeiçoamento da gestão e, notadamente, neste trabalho, na gestão de políticas de TI.

A sociedade brasileira cobra mais resultados dos organismos governamentais, que dependem cada vez mais da Tecnologia da Informação para o suporte às atividades da máquina administrativa. A gestão de TI passa a ser fundamental para que os gestores públicos possam realizar o planejamento, controle e a efetiva execução das políticas públicas de que a sociedade brasileira tanto necessita, porque traz mais flexibilidade e transparência aos processos.

Faz-se necessário, portanto, avaliar a forma como as administrações públicas municipais vêm utilizando a Tecnologia da Informação como instrumento de apoio a suas atividades, buscando verificar a qualidade dos serviços prestados e identificar deficiências que obstaculizam sua operação de forma eficiente, eficaz e efetiva.

Nesse contexto, a atuação dos diversos Tribunais de Contas é fundamental, pois são eles os órgãos encarregados de realizar o Controle Externo da gestão dos recursos públicos.

A auditoria operacional ganha também grande destaque, visto que um de seus objetivos é o aprimoramento da qualidade do serviço público. Ao detectar deficiências nessa área e alertar sobre a necessidade de saná-las, o auditor estará alcançando estes objetivos.



A relevância deste trabalho reside no fato de mostrar que a adoção definitiva da auditoria de Tecnologia da Informação pelo Tribunal de Contas do Estado do Rio de Janeiro (TCE-RJ) irá contribuir para uma melhoria da gestão pública municipal, ao evidenciar deficiências relativas ao uso da informática e orientar sua atuação em direção às práticas adotadas pelo mercado.

O TCE-RJ, ao realizar auditorias de cunho operacional em TI, está, em última instância, realizando uma aproximação maior com a sociedade, respondendo prontamente aos anseios desta por melhor qualidade dos serviços públicos.

## 2. CONTROLE DA ADMINISTRAÇÃO PÚBLICA

---

Controle é a função administrativa que tem por finalidade observar se os fatos se passaram de acordo com o que a administração determinou. (SOUZA, 2006). No setor público, o controle tem como principal função, entre outras, a busca de melhores resultados pelas administrações públicas.

O controle administrativo, segundo Carvalho Filho (2005), representa o conjunto de mecanismos administrativos e jurídicos por meio dos quais se exerce o poder de fiscalização e de revisão da atividade administrativa em qualquer das esferas de Poder. Dessa forma, o controle da administração está fulcrado nas normas elaboradas pelos representantes do povo, estabelecendo tipos e modos de controle de toda atuação administrativa, para a defesa da própria administração e dos direitos inerentes a todos os administrados.

Segundo discorre Silva (2001), o controle do Estado, em termos genéricos, ocorre por meio da separação e independência dos poderes, conforme previsto no artigo 2.º da Constituição da República Federativa do Brasil, e que foram concebidos originariamente por Montesquieu, por meio de um sistema de freios e contrapesos. Afora este artigo, existem outros, na CRFB de 1988, que tratam do controle das ações do Estado e dos seus gestores (de recursos públicos), quando imbuídos de suas atribuições. Salienta-se que este controle compreende não somente atos do poder Executivo, bem como dos demais poderes, como gestores de atividades administrativas.

Para Di Pietro (2001), o controle na administração pública é definido como o poder de fiscalização e correção que sobre ela exercem os órgãos dos poderes Judiciário, Legislativo e Executivo, com o objetivo de garantir a conformidade de sua atuação com os princípios que lhes são impostos pelo ordenamento jurídico. Este conceito formal está balizado pelos princípios constitucionais previstos no artigo 37 da CRFB, a saber: legalidade, impessoalidade, moralidade, publicidade e eficiência. Este último foi adicionado pela Emenda Constitucional n.º 19, de 04 de junho de 1998.

Na visão de Meirelles (2003, p. 636), controle em tema de administração pública tem a seguinte abordagem:

O controle administrativo pode ser exercido pelos próprios órgãos internos da Administração (controle hierárquico propriamente dito) como por órgãos externos incumbidos do julgamento dos recursos (tribunais administrativos) ou das apurações de irregularidades funcionais (órgãos correcionais). Todos eles, entretanto, são meios de controle administrativo. (MEIRELLES, 2003, p. 637).

A Constituição Federal adotou dois sistemas de controle para a administração pública, quais sejam: o Controle Interno, realizado pelos próprios órgãos estatais, ou seja, é exercido pelo órgão controlador dentro da estrutura burocrática que pratica os atos sujeitos ao seu controle; e Controle Externo, quando o órgão controlador situa-se externamente ao órgão controlado, mais precisamente realizado pelo Poder Legislativo com o auxílio do Tribunal de Contas.

Observemos o que a Constituição Federal brasileira dispõe sobre o assunto:

Art. 70: A fiscalização contábil, financeira, orçamentária, operacional e patrimonial da União e das entidades da administração direta, indireta, quanto à legalidade, legitimidade, economicidade, aplicação de subvenções e renúncia de receitas, será exercida pelo Congresso Nacional, mediante controle externo, e pelo sistema de controle interno de cada poder.

Art. 71: O controle externo, a cargo do Congresso Nacional, será exercido com o auxílio do Tribunal de Contas da União. (BRASIL, 1988)

A Lei Complementar nº 101/2000, conhecida como Lei de Responsabilidade Fiscal (LRF), veio coroar, por meio de normas, toda a ação da administração pública, exigindo-lhe metas, prioridades e eficiência, fazendo com que o gestor direcione seus projetos e atividades às necessidades da comunidade. Por meio do Relatório Resumido de Execução Orçamentária e Financeira e Relatório de Gestão Fiscal, os controles interno e externo verificarão periodicamente a observância dos limites e condições da LRF. Os referidos demonstrativos ensejam o controle simultâneo da execução orçamentária.

Os Tipos de Controle variam segundo o Poder, órgão ou autoridade que o exercita e o momento de sua efetivação:

- Interno: é realizado pela entidade ou órgão responsável pela atividade controlada (âmbito interno).
- Externo: realizado por órgão estranho à Administração.
- Prévio ou preventivo: antecede a conclusão ou operatividade do ato, requisito de sua eficácia. Ex: a liquidação da despesa, para oportuno pagamento.
- Concomitante ou sucessivo: acompanha a realização do ato para verificar a regularidade de sua formação. Ex: realização de auditoria durante a execução do orçamento.
- Subseqüente ou corretivo: efetivado após a conclusão do ato controlado, visando às devidas correções. Ex: a homologação do julgamento de uma concorrência.

## 2.1 CONTROLE INTERNO

Gasparini (1989) se refere ao controle interno como autocontrole, que é exercido pelos órgãos dos três Poderes sobre suas próprias atividades, visando ratificá-las ou desfazê-las, conforme sejam ou não legais, oportunas, convenientes e eficientes. E afirma que é interno porque tanto o órgão controlador como o controlado integram a mesma organização.

Controle interno, segundo Meirelles (2003, p. 638),

É todo aquele realizado pela entidade ou órgãos responsáveis pela atividade controlada, no âmbito da própria Administração. Assim, qualquer controle efetivado pelo Executivo sobre seus serviços ou agentes é considerado interno, como interno será também o controle do Legislativo ou do Judiciário, por seus órgãos de administração, sobre seu pessoal e os atos administrativos que pratique.

O Controle Interno desenvolve-se de forma ininterrupta, principalmente na esfera do Poder Executivo, onde se situa parcela considerável das atividades administrativas básicas, e envolve a atividade-meio (organização e expedientes administrativos) e a atividade-fim (serviços públicos, poder de polícia, fomento).

Reúne, também, as atividades administrativas que servem de suporte aos Poderes Legislativo e Judiciário, bem como as atividades de outras instituições dotadas de autonomia, como o Tribunal de Contas e o Ministério Público. Abrange, ainda, o exercício das atividades delegadas pelo poder público aos particulares, como no caso das concessões e permissões de serviços públicos.

## **2.2 CONTROLE EXTERNO**

Para melhor entendimento do conceito de controle externo, MEIRELLES (2003, p. 632), define-o como a "faculdade de vigilância, orientação e correção que um poder ou órgão ou autoridade exerce sobre a conduta funcional de outro, com objetivo de garantir a conformidade de sua atuação com os princípios que lhe são impostos pelo ordenamento jurídico"

Silva (1989) afirma que o exercício do controle externo, consubstanciado na fiscalização contábil, financeira, orçamentária, patrimonial e operacional é coerente com o Estado Democrático de Direito:

(...) somente quando vigem os princípios democráticos em todas as suas conseqüências - e entre elas das mais importantes é a consagração da divisão de poderes - e é o orçamento votado pelo povo através de seus legítimos representantes, é que as finanças, de formal, se tornam substancialmente públicas, e a sua fiscalização passa a constituir uma irrecusável prerrogativa da soberania.(SILVA,1989, p. 627).

As entidades governamentais de direito público interno ou de direito privado, portanto, estão obrigadas a se organizar a fim de atender às suas finalidades precípuas e às determinações legais e constitucionais.

O Tribunal de Contas, ainda que integre o Poder Legislativo, conforme determinação expressa no artigo 71 da Constituição Federal, exerce o papel de

fiscalização como controle externo, cuja função precípua é verificar se a administração pública ou seus representantes estão obedecendo aos princípios de legalidade, impessoalidade, moralidade, publicidade e eficiência, consoante estabelece a Constituição Federal.

O sistema de tribunais de contas brasileiros é formado pelo Tribunal de Contas da União (TCU), Tribunal de Contas do Distrito Federal (TCDF), 26 tribunais de contas estaduais (TCE) e seis tribunais de contas com jurisdição municipal (TCM), totalizando 34 órgãos.

Os Tribunais de Contas do Estado têm jurisdição na administração pública do respectivo estado e da totalidade dos seus municípios, excetuados os seguintes casos:

- Bahia, Ceará, Pará e Goiás, que possuem um tribunal de contas com jurisdição apenas sobre a administração estadual (TCE) e um tribunal com jurisdição em todos os seus municípios (TCM);
- São Paulo e Rio de Janeiro, cujas capitais possuem tribunais de contas específicos (TCM), enquanto os TCE têm jurisdição na administração pública estadual e dos demais municípios do Estado.

Em seu art. 31, § 4º, a Constituição Federal de 1988 vedou a criação de novos tribunais, conselhos ou órgãos de contas municipais.

## **2.3 CONTROLES QUANTO AO MOMENTO**

Segundo Silva (2001), quanto à forma do controle no momento do seu exercício, a fiscalização dos atos praticados pelo administrador pode ser a priori, concomitante ou a posteriori.

No controle a priori, as ações de controle e avaliação acontecem antes da ocorrência do evento ou fato que se pretende controlar, com o intuito de prevenir ou impedir o sucesso de atos indesejáveis como erros, desperdícios ou

irregularidades. Neste tipo de controle, o ato tem sua eficácia suspensa até ser submetido à análise e aprovação formal do órgão de controle.

No controle concomitante, a verificação do ato é conjunto à ação do administrador. Tem a finalidade de detectar erros, desperdícios ou irregularidades, no momento em que eles ocorrem, permitindo a adoção de medidas tempestivas de correção. Dessa forma, ajusta-se o desempenho ainda em andamento, a fim de se conseguir o objetivo. Uma das vantagens na sua utilização é o ato tido como irregular poder ser abortado durante a sua consecução, impedindo maiores prejuízos ao erário.

O controle a posteriori aprecia o ato após a sua consumação, não permite qualquer ação corretiva relativamente ao desempenho completado, embora funcione como um mecanismo motivador, uma vez que uma variação desfavorável, informada por meio de relatórios gerenciais, leva o gestor a implementar ações para corrigir o desempenho de sua área ou da organização, no futuro. A reparação do dano e a restauração do *status quo ante* torna-se difícil.

No Brasil, a ênfase no modelo gerencial ou pós-burocrático para a administração pública se deu com a elaboração do Plano Diretor da Reforma do Aparelho do Estado em 1995, o qual incorporou as bases da administração pública gerencial - ou Nova Administração Pública (*New Public Management*), valendo-se das experiências de outros países, com o objetivo de tornar a administração pública mais eficiente. Esta reforma administrava também alterou a forma de controle dos recursos públicos, deslocando o seu enfoque dos meios (processos) para os fins (resultados), visando o aumento da satisfação dos usuários e dos níveis de eficiência, com base nas experiências anglo-americana do *managerialism*, *consumerism* e *public service orientation* (MÔNACO, 2007).

### **3. AUDITORIA OPERACIONAL**

---

Este capítulo examina, de início, os desafios para o novo gerencialismo público e a importância da auditoria operacional nesse contexto. Em seguida, aborda as principais questões relacionadas à adoção da auditoria operacional pela administração pública. Primeiramente, traça-se um panorama histórico de sua adoção pelas EFS no mundo e no Brasil. Em seguida, são mostradas as diversas definições de auditoria operacional adotadas pelas EFS e autores do assunto. É apresentada uma comparação entre a auditoria dita tradicional, como é conhecido o tipo de auditoria comumente adotado pelas EFS, e a auditoria operacional. Por fim, o capítulo termina com uma análise dos entraves que dificultam a adoção da auditoria operacional pelas EFS, abordando especificamente as particularidades dos tribunais de contas brasileiros.

#### **3.1 NOVA GESTÃO PÚBLICA E A AUDITORIA OPERACIONAL**

A segunda metade do século XX foi um período de significativas transformações tecnológicas, sociais e econômicas e que se destaca pelo predomínio do conhecimento e da informação. A partir dessas transformações, foram impostos novos padrões de gestão às organizações públicas e privadas, devido ao início de um processo de reestruturação produtiva apoiado no desenvolvimento científico e tecnológico e na globalização dos mercados. Nesse cenário, a capacidade de implementar formas flexíveis de gestão que possam fazer face às mudanças do mundo contemporâneo se torna um consenso entre estudiosos da teoria organizacional como a melhor forma de uma instituição obter o sucesso (GUIMARÃES, 2000).

Bresser Pereira (1998) destaca como desafio para a nova administração pública a transformação de estruturas burocráticas, hierarquizadas, com tendências ao insulamento, em organizações flexíveis e empreendedoras. Essa transformação implicaria a racionalização das organizações públicas através da adoção de padrões de gestão desenvolvidos para o ambiente das empresas privadas devidamente adaptados à natureza e necessidades do setor público.



A década de 1980 foi marcada por um grande crescimento do interesse em modificar o setor público, decorrente do processo de reforma do Estado pelo qual o Brasil atravessava. Faria (2005) destaca como propósitos no desenho da reforma do Estado a adoção de uma perspectiva de contenção dos gastos públicos, da busca de melhoria da eficiência e da produtividade, do aumento da flexibilidade gerencial e da capacidade de resposta dos governos, buscando obter o máximo de transparência na gestão pública e de responsabilização dos gestores priorizando o cidadão, visto como “consumidor” de bens e serviços do governo.

De acordo com Faria (2005), o controle governamental, durante o período burocrático, não se mostrou capaz de atender aos anseios da sociedade organizada quanto às prestações de contas dos recursos públicos aplicados pelos gestores. Os trabalhos se restringiam às análises do aspecto contábil, com observância rigorosa do cumprimento da legalidade e normatividade, demonstrando uma visão limitada por apresentar um caráter formal e punitivo.

Outro aspecto que predominava na administração pública burocrática era o enfoque em processos, não se preocupando com a análise do desempenho das organizações e o atingimento das metas e dos resultados dos programas.

Em palestra proferida no Congresso dos Tribunais de Contas do Brasil o então ministro Nelson Jobim afirma que:

O déficit público forçou a adoção de um novo modelo de controle pelo Poder Público apontando para uma perspectiva de se verificar a eficiência no serviço público. É evidente a necessidade de se examinar o grau de alcance das metas dos programas (juízo de resultados) pois já não mais satisfaz apenas o acompanhamento dos processos.(JOBIM, 2005)

Com o desenvolvimento dessa nova filosofia de administração pública por meio do modelo gerencial, ou pós-burocrático, a função do controle governamental passa a ser discutida como instrumento de grande relevância para que o Estado possa efetivamente garantir que os conceitos de eficiência e eficácia, propostos pelo paradigma gerencial, possam ser seguidos.

O paradigma gerencial estabelece para o controle governamental um novo escopo na análise dos gastos públicos, cuja ênfase passa a ser nos resultados alcançados, passando a inserir a perspectiva da transparência das ações governamentais, através da disponibilização de mecanismos que possibilitem a fiscalização dos atos dos gestores públicos.

A administração gerencial requer, por parte dos órgãos e entidades da administração pública, uma visão e missão estratégica bem definidas, os objetivos de longo prazo em função das metas, estabelecimento de metas de longo prazo, assim como de metas anuais de desempenho, as quais serão mensuradas através de indicadores desenvolvidos para esse propósito e também para contribuir para a melhoria da efetividade dos programas (NUNES, 2004).

Carneiro (2002) comenta acerca de outra modificação introduzida na administração pública que foi a mudança de papel dos chamados administradores públicos para gerentes ou gestores públicos a fim de satisfazer às exigências de um novo perfil gerencial de articulador e empreendedor, diferentemente do papel de supervisor ou administrador. São estabelecidos novos valores gerenciais: a primazia do cliente; a diversidade e flexibilidade; as habilidades multidimensionais; a delegação em lugar do controle e o gerente como um orientador focado em resultados.

As mudanças de paradigmas do modelo de Estado e de sua administração ocasionadas pelas transformações da pós-modernidade impulsionaram o desenvolvimento da auditoria operacional como modalidade de controle. A implantação da administração gerencial no setor público é tida como o fator responsável pelo surgimento das auditorias voltadas para resultados. Associada a esse fator passa a existir uma demanda crescente da sociedade pela responsabilização dos agentes políticos, isto é, por maiores níveis de *accountability*<sup>1</sup>.

É importante também destacar que a implantação progressiva da administração gerencial está freqüentemente associada à expansão e sofisticação

---

<sup>1</sup> *Accountability* segundo Campos (1990) não possui tradução literal na língua portuguesa mas pode-se afirmar que representa o compromisso ético e legal de se responder por uma responsabilidade delegada.

dos sistemas de informação, à ênfase no planejamento e à implantação de critérios de desempenho para os órgãos e entes públicos, o que colaborou para o desenvolvimento das auditorias voltadas para resultados (NUNES, 2004).

Organizações internacionais, a exemplo da Organização Internacional de Entidades de Fiscalização Superiores – INTOSAI, vêm buscando padronizar estruturas e processos de controle interno, baseados na eficiência e na efetividade, objetivando garantir a transparência no controle dos resultados dos dispêndios públicos.

No contexto da reforma do Estado, vários são os debates acerca da forma como o controle externo pode contribuir para o aumento da responsabilização dos agentes públicos, para o aperfeiçoamento das ações do governo e para o fornecimento de informações confiáveis à sociedade. Como resposta, desenvolve-se no âmbito das Entidades de Fiscalização Superiores (EFS<sup>2</sup>) um tipo de fiscalização - a auditoria operacional - que focaliza o mérito da ação pública ao invés de priorizar a conformidade dos procedimentos de gestão.

Barzelay (2002) coloca que a auditoria operacional é reconhecida por pesquisadores e pelas EFS de alguns países como o instrumento adequado para se formar juízo acerca do mérito da ação pública. Desse modo, se uma EFS possui competência para examinar a eficiência, a efetividade, a legitimidade da ação pública, a ferramenta utilizada para exercer esse poder-dever é a auditoria de desempenho, mesmo em países onde a burocracia é cética quanto a doutrinas administrativas orientadas para desempenho, como França e Alemanha.

Segundo Pollit (1999), após o estudo que realizou em EFS de cinco países (Inglaterra, Suécia, Dinamarca, Finlândia e França), é inegável a existência de uma interface<sup>3</sup> entre auditoria de desempenho e reformas administrativas, pois, a maior parte das iniciativas de reforma administrativa dos países que pesquisou mudou a ênfase no controle de insumos e processos para novas formas de controle baseadas na medida dos resultados e impactos. Pollit (1999) ainda cita Power (1997) para evidenciar que o desenvolvimento da gestão

---

<sup>2</sup> EFS é o nome pelo qual são conhecidas no mundo as organizações de controle externo

<sup>3</sup> Interface- meio que promove a comunicação ou interação entre dois ou mais grupos (FERREIRA, 1999: 1124)

do setor público e o desenvolvimento da auditoria de desempenho originam-se do mesmo conjunto de valores e estão entrelaçados no âmbito da mesma reforma ética.

Segundo a Controladoria Geral dos Estados Unidos da América (*United States Government Accountability Office* - GAO), os legisladores, os dirigentes do governo e o público em geral buscam não apenas informações sobre os serviços públicos e a observância quanto à eficiência, efetividade, economia e conformidade com as leis e regulamentos oficiais, mas também querem saber se os programas de governo estão alcançando seus objetivos e resultados propostos e a que custo (GAO, 2005).

As auditorias operacionais proporcionam avaliação independentemente do desempenho e da gestão dos programas de governo confrontados com critérios objetivos ou avaliações das melhores práticas e outras informações, sugerindo recomendações para a melhoria dos programas com a introdução de ações corretivas, auxiliando o processo de decisão, melhorando o monitoramento da gestão, enfim contribuindo para a *accountability* pública (GAO, 2005).

Derlien (2001) observou que dentro do contexto de avaliação das políticas públicas, em conjunto com o movimento do *New Public Management*, os atores principais não são mais os administradores dos programas de governo, mas os escritórios de auditoria, os Ministérios da Fazenda e as unidades centrais. Com isso, os avaliadores passam a ser os auditores cujos trabalhos buscam focar a medição dos resultados.

Assim, valores como eficiência, eficácia, efetividade e economicidade passaram a ter papéis relevantes, tornando-se parâmetros norteadores no processo de redefinição da estrutura do Estado.

Para enfrentar um dos muitos desafios do controle externo, a auditoria operacional se faz presente como instrumento capaz de subsidiá-lo no acompanhamento das inovações propostas para a reforma do Estado e, conseqüentemente da administração pública, no sentido de elevar os níveis de transparência, tornando o Estado mais permeável à participação e ao controle dos cidadãos e mais eficaz no atendimento das demandas da sociedade.

### 3.2 AUDITORIA OPERACIONAL : EVOLUÇÃO HISTÓRICA

No âmbito da administração pública, a expressão auditoria operacional foi utilizada inicialmente em 1971, durante o VII Congresso Internacional de Entidades Fiscalizadoras Superiores – INTOSAI, que fora apontado como um dos marcos históricos desse tipo de auditoria (ARAUJO, 2001).

Grande parte dos progressos da auditoria operacional são creditados ao GAO, sendo esse órgão considerado como o maior responsável pelos avanços dessa área. A normatização desse tipo de auditoria se deu a partir da publicação pelo GAO da primeira versão das normas de auditoria governamental, em 1972, denominada Normas para Auditoria de Organizações, Programas, Atividades e Funções Governamentais (*Standards for Audit Of Governmental Organizations, Programs, Activities and Functions*), que ficaram conhecidos como “Livro Amarelo” pela cor da sua capa (ARAUJO, 2001). Embora voltada, em geral, para todas as formas de auditoria, essa publicação é mais conhecida pela contribuição dada à auditoria operacional, constituindo-se, assim, em um documento significativo uma vez que definiu o conceito e o campo de atuação e editou as primeiras normas para a realização desse tipo de auditoria.

Em um estudo empírico e comparativo de análise organizacional realizado nos órgãos centrais de auditoria da OCDE, sobre os trabalhos de auditoria operacional, Barzelay (2002) verificou que, além do GAO, foram criadas várias organizações que desenvolveram e disseminaram esses trabalhos. Segundo o autor, pode-se citar, nos Estados Unidos da América (EUA), os Escritórios dos Inspectores Gerais (*Office of Inspectors General*), no Reino Unido, a Comissão de Auditoria para a Inglaterra e País de Gales (*Audit Comission for England and Wales*), cuja jurisdição inclui o governo municipal, o Serviço Nacional de Saúde e a Polícia; o *National Audit Office* (NAO), cuja jurisdição compreende o restante do governo central e uma gama de inspetorias de setores ou órgãos específicos em rápida expansão, como o Escritório de Normas de Educação (*Office of Standards in Education*). Para o autor, as organizações governamentais fundamentais na

área de auditoria operacional são aquelas responsáveis pela elaboração orçamentária, auditoria, avaliação e reforma administrativa (Barzelay, 2002).

Na América Latina, por sua vez, o termo foi inserido pelo Instituto Latino-Americano e do Caribe de Ciências Fiscalizadoras - ILACIF, que passou a ser denominado em 1990 de Organização Latino-Americana e do Caribe de Entidades Fiscalizadoras Superiores - OLACEFS (NASCIMENTO, 2002).

O IX Congresso Mundial de Tribunais de Contas, realizado em 1977, em Lima (Peru), recomendou que os organismos de controle deveriam ampliar seus trabalhos de auditoria financeira, buscando examinar aspectos de eficiência, economia e efetividade contemplados pela auditoria operacional. Em 1998, no Congresso Internacional de Entidades Fiscalizadoras Superiores – INCOSAI, realizado em Montevidéu, ficou definida a elaboração das Diretrizes para a aplicação da Auditoria Operacional pelo Comitê de Normas de Auditoria da INTOSAI, em conjunto com as EFS. O projeto final contendo essas diretrizes foi aprovado em 2003 (INTOSAI, 2005b).

Além dos Estados Unidos, países como Inglaterra e Canadá muito têm contribuído com a expansão e desenvolvimento e a aplicação de métodos da auditoria operacional. Na Inglaterra, a auditoria operacional é conhecida como auditoria de valor por dinheiro, *value for money*, não só porque tem por objetivo a verificação da irregularidade das contas, do ponto de vista contábil legal, mas também porque visa avaliar a possibilidade e prejuízo devido à perda de eficiência e não observância de requisitos de economicidade.

Cabe também destacar as observações de Barzelay (2002) acerca da institucionalização da auditoria operacional no mundo:

A forma pela qual os órgãos de auditoria lidam com a institucionalização da auditoria de desempenho muito provavelmente terá efeito significativo sobre a escala e a distribuição das atividades de revisão na esfera governamental. Tais reações tenderão a delinear o modo de operação e o impacto dos sistemas governamentais de responsabilização e prestação de contas [*accountability*] (BARZELAY, 2002, p. 28).

Oliveira (2000) afirma que a auditoria operacional teve a primeira perspectiva de aplicação no Brasil, a partir de 1986, na administração pública federal, através da edição do Decreto 93.874, cujo artigo 10, parágrafo segundo, estabelecia que além de examinar os atos da gestão, a fim de certificar a exatidão e a regularidade das contas, a auditoria deveria verificar a eficiência e a eficácia na aplicação dos recursos.

Com a promulgação da Constituição Federal de 1988, institucionalizou-se o controle operacional na legislação brasileira, quando foram incorporados, por força do "caput" do artigo 70, poderes ao Controle Externo exercido pelo Poder Legislativo com o auxílio do Tribunal de Contas da União, para exercer a "fiscalização contábil, financeira, orçamentária, operacional e patrimonial da União e das entidades da administração direta e indireta " (BRASIL,2004, p.40).

Sobre a institucionalização da auditoria operacional no texto constitucional, Da Silva assevera:

Em que pese o atraso na percepção da necessidade da realização de auditoria operacional no setor público no Brasil, a incorporação de sua concepção explicitamente no texto constitucional, representa uma tomada de consciência dos políticos e administradores públicos.[...] Este tipo de auditoria desempenha importante papel como instrumento gerencial na avaliação do grau de eficiência, economia, e eficácia com que são realizadas as operações e atividades governamentais.(DA SILVA,1993, p. 5),

O Tribunal de Contas da União, por sua vez, passou a contar com a competência constitucional de realizar "... inspeções e auditorias de natureza contábil, financeira, orçamentária, operacional e patrimonial, nas unidades administrativas dos Poderes Legislativo, Executivo e Judiciário, ..." conforme determina o art. 71, inciso IV, incluindo aí as fundações e as sociedades instituídas e mantidas pelo Poder Público Federal, nos termos do inciso II do citado artigo (BRASIL, 2004).

Embora a instituição da auditoria operacional tenha se dado desde 1988, pode-se afirmar que sua efetiva implementação ainda está se processando, pelo fato de ter uma natureza diferenciada, cuja complexidade exige uma metodologia

específica para assegurar a qualidade dos trabalhos, tendo como impulso definitivo a publicação da Lei de Responsabilidade Fiscal (LRF). A edição dessa Lei, ao atribuir aos Tribunais de Contas o dever de alertar as entidades públicas sobre os fatos que comprometem custos e os resultados dos programas governamentais, tornou o exame da eficiência e eficácia desses programas um procedimento obrigatório no âmbito do controle externo.

Dessa forma, os Tribunais de Contas, tiveram suas atribuições ampliadas a partir da inserção da auditoria operacional, renovando as concepções de controle consubstanciadas no controle operacional e no conceito de economicidade.

### **3.3 ASPECTOS GERAIS DA AUDITORIA OPERACIONAL**

As auditorias de cunho operacional possuem nomenclaturas as mais variadas, dependendo da organização ou país que a adote. Segundo Freitas, dentre os variados rótulos disponíveis, pode-se enumerar: auditoria operacional, auditoria de desempenho (*performance audit*), auditoria de valor pelo dinheiro (*value-for-money audit*), auditoria administrativa, auditoria de gestão, auditoria de rendimento e auditoria de resultados (FREITAS, 2005).

O TCU, órgão público pioneiro na realização deste tipo de auditoria no Brasil, adotou inicialmente o termo auditoria de desempenho, ao editar seu primeiro manual sobre o assunto (TCU, 1998). O atual Manual de Auditoria de Natureza Operacional, editado em 2000 (TCU, 2000), incorporou a denominação presente no artigo 70 da Constituição Federal.

A Organização Internacional de Entidades Fiscalizadoras Superiores (INTOSAI, 2005b) utiliza o termo *performance audit*, traduzido para o português como auditoria de desempenho. Esta Organização considera também o termo avaliação de programa como uma das numerosas ferramentas da auditoria operacional.



O Escritório do Auditor Geral do Canadá (OAG, 1995), órgão do governo canadense, adota o conceito de auditoria integrada (*comprehensive auditing*), com significado mais abrangente, que engloba tanto aspectos de auditoria de regularidade como de desempenho.

Araújo (2001) definiu auditoria operacional ou de otimização de recursos como sendo aquela que objetiva avaliar o desempenho e a eficácia das operações, os sistemas de informação e de organização, e os métodos de administração; a propriedade e o cumprimento das políticas administrativas; e a adequação e a oportunidade das decisões estratégicas.

Assim como as diversas designações, vários são também os conceitos de auditoria operacional. Esse tipo de auditoria pode ser estudada em dois setores distintos: público e privado. Entretanto, o foco desse trabalho está voltado para a auditoria operacional no setor governamental. Assim, os conceitos aqui expostos referem-se ao entendimento dos autores quanto à auditoria operacional nessa área.

As normas de auditoria governamental do GAO resumem a auditoria operacional como resultados de avaliações sobre uma evidência da seguinte forma:

As auditorias operacionais implicam exame objetivo e sistemático da evidência para apresentar uma avaliação independente do desempenho e da gestão de um programa com base em critérios objetivos, assim como avaliações que proporcionem um enfoque prospectivo ou que sintetizem informações sobre as melhores práticas ou análises de temas transversais. (GAO, 2005, p. 45)

Haller et al (1995) apresentam a auditoria operacional com sendo um processo de revisões metódicas de programas, organizações, atividades ou segmentos, confrontando o desempenho real com o esperado, tendo como finalidade avaliar e comunicar se os recursos da organização estão sendo usados eficientemente.

A INTOSAI, através das suas Diretrizes para a Aplicação de Normas de Auditoria Operacional (2005b), enfoca a eficiência e eficácia, sem desprezar a

observância da economicidade, conceituando assim: “a auditoria operacional é um exame independente da eficiência e da eficácia das atividades, dos programas e dos organismos da Administração Pública, prestando a devida atenção à economia, com o objetivo de realizar melhorias”.

Araújo (2001) entende que a auditoria operacional pode ser realizada no todo ou em partes de uma organização com o objetivo de propor recomendações e comentários que contribuirão para melhorar os aspectos da economia, eficiência e eficácia.

Peter e Machado (2003), numa definição um pouco semelhante à de Araújo, acreditam que a auditoria operacional avalia as ações gerenciais ou parte dos procedimentos do processo operacional das entidades da administração pública e dos programas de governo. Acrescenta, ainda, que esse tipo de auditoria avalia a eficácia dos resultados das entidades em relação aos recursos materiais, humanos e tecnológicos disponíveis, bem como a economicidade, eficiência, efetividade e qualidade dos controles internos existentes.

Féder (1988, p. 5) salienta que a auditoria operacional “preocupa-se com as operações atuais, enfatiza o presente e as melhorias possíveis”. Logo, deve-se concentrar nas áreas críticas, de risco relevante ou onde o controle interno está falhando.

Para Barzelay (2002) a expressão auditoria de desempenho é um rótulo impreciso para o conceito nela embutido. O autor argumenta que auditoria de desempenho é uma denominação incorreta pois não se trata de auditoria, mas sim de um conjunto de atividades de avaliação. A auditoria é uma forma de verificação, isto é, envolve o confronto de critérios usualmente aceitos com procedimentos efetivados.

Cunha (1998) conceitua a auditoria operacional de modo simples, afirmando que “nada mais é do que um exame objetivo, sistemático e profissional das operações financeiras e administrativas de uma empresa ou entidade, ou parte delas, com a finalidade de verificá-las e avaliá-las”.

O manual de auditoria de natureza operacional (TCU, 2000) adotou a seguinte definição: “auditoria de natureza operacional consiste na avaliação sistemática dos programas, projetos, atividades e sistemas governamentais, assim como dos órgãos e entidades jurisdicionadas ao Tribunal”.

Este manual divide a Auditoria de Natureza Operacional em duas modalidades: a auditoria de desempenho operacional, cujo objetivo é examinar a ação governamental quanto aos aspectos da economicidade, eficiência e eficácia, e a avaliação de programa, que busca examinar a efetividade dos programas e projetos governamentais. A figura a seguir mostra as dimensões da auditoria operacional explicitadas no manual do TCU.

**Figura 1 – Dimensões da Auditoria de Natureza Operacional**



Fonte: Manual de Natureza Operacional (TCU, 2000, p.13)

Assim, após analisar os diversos conceitos dos autores citados, a auditoria pode ser definida como um processo de avaliação das ações dos gestores públicos, relativas a um programa de governo ou a uma instituição para a verificação dos aspectos da economicidade, eficiência, eficácia e efetividade, visando à melhoria da gestão pública.

Os conceitos de auditoria operacional apresentados anteriormente mencionam, em níveis diferentes, os chamados 4 “Es” : economicidade, efetividade, eficiência e eficácia.

A Constituição Federal de 1988 (BRASIL, 2004) destaca a necessidade de avaliar a economicidade através do caput do seu artigo 70. Já o inciso II do art. 74 da mesma Lei ressalta a eficácia e eficiência como parâmetros da auditoria: “comprovar a legalidade e avaliar os resultados, quanto à eficácia e eficiência, da gestão orçamentária, financeira e patrimonial nos órgãos e entidades da

administração federal, bem como da aplicação de recursos públicos por entidades de direito privado” (BRASIL, 2004).

Torna-se, agora, necessário fazer-se um breve levantamento das definições dos termos economicidade (ou economia), eficiência, eficácia e efetividade, pois ainda que de ampla aceitação e relativa unanimidade quanto aos seus significados, destes dependem a correta compreensão do conceito de auditoria operacional.

Cruz (1997) fornece as seguintes definições para os “4 Es” da auditoria operacional: (a) economicidade refere-se aos prazos e condições nos quais são obtidos os recursos físicos, humanos e financeiros, logo uma operação econômica pressupõe recursos em qualidade, quantidade, menor custo e tempo hábil; (b) eficácia diz respeito ao atingimento de objetivos e metas e, aos resultados; (c) eficiência está relacionada a custo, a forma pela qual os meios são geridos. É a otimização dos recursos disponíveis, através da utilização de métodos, técnicas e normas, visando ao menor esforço e ao menor custo na execução das tarefas; (d) efetividade refere-se à preocupação da organização com o seu relacionamento externo, sua sobrevivência e atendimento das necessidades sociais, pressupondo ainda certo grau de eficiência e eficácia.

Alguns autores não abordam a efetividade em virtude desse método de avaliação se referir ao relacionamento externo da organização, daí, abordam apenas três “Es” na auditoria operacional.

O Código de Ética e Normas de Auditoria da INTOSAI (2005a) traz os seguintes conceitos:

(a) economicidade consiste em reduzir ao mínimo o custo dos recursos utilizados para desempenhar uma atividade em um nível de qualidade apropriado; (b) eficácia é a relação entre os resultados pretendidos e os resultados alcançados; (c) eficiência é a relação entre o produto — expresso em bens, serviços e outros produtos — e os recursos utilizados para produzi-los.

Rocha (1990) aborda os três “Es” da auditoria operacional de modo mais detalhado: (a) economicidade pressupõe a obtenção e utilização adequada dos

recursos humanos, materiais e financeiros, os quais devem estar disponíveis nas quantidades necessárias e suficientes e no momento adequado; (b) eficiência pressupõe a obtenção de níveis máximos de produção com o mínimo de recursos possíveis (c) eficácia pressupõe que os resultados obtidos estejam dentro dos objetivos propostos para a entidade. Significa dizer que, em uma entidade pública eficaz, os resultados produzidos pela sua atuação são aqueles para os quais ela foi criada (ou direcionada), constantes da legislação própria e cujos produtos ou serviços estejam dentro de padrões de quantidade e qualidade consentâneos.

Cunha (1998) define os 3 “Es” de forma sucinta : (a) eficiência é o máximo de rendimento sem desperdício de gastos ou tempo; (b) eficácia consecução das metas programadas; (c) economicidade traduz a operação ao menor custo possível.

Araújo (2001) ao resumir os conceitos dos 3 “Es” apresenta:

economia: é a capacidade de fazer, gastando pouco. É executar uma atividade ao menor custo possível, ou seja, gastar menos;

eficiência: é a capacidade de fazer as coisas direito. É apresentar um desempenho satisfatório sem desperdícios, ou seja, gastar bem;

eficácia: é a capacidade de fazer as coisas certas. É alcançar os objetivos ou metas previstas, ou seja, gastar sabiamente. (ARAÚJO, 2001, p. 39).

Assim, em resumo, é possível afirmar que o que se busca saber, a partir de uma auditoria operacional é se a entidade ou programa auditado vem obtendo os resultados esperados, incluindo-se os impactos provocados da melhor forma e ao menor custo possível.

### **3.4 COMPARAÇÃO ENTRE A AUDITORIA OPERACIONAL E A AUDITORIA TRADICIONAL**

A auditoria, de um modo geral, quer seja operacional quer seja tradicional<sup>4</sup>, caracteriza-se pela realização de verificações sistemáticas e análises objetivas das operações de uma entidade que resultam na elaboração de um relatório.

A maioria dos autores aponta que a diferença básica entre a auditoria operacional e a tradicional está nos objetivos propostos e na abrangência do trabalho.

Sobre este aspecto, Nascimento (2001) comenta que os limites entre as duas auditorias são quase os mesmos: revisão, avaliação e emissão de parecer, mas há uma diferença que reside no objetivo do estudo. Segundo o autor, a auditoria tradicional busca responder se a realidade patrimonial da entidade e a realidade de suas relações com terceiros estão compatíveis com os demonstrativos contábeis, enquanto a auditoria operacional volta sua atenção para o desempenho das operações da entidade ou órgão, examinando os métodos, processos, fluxos, programas, projetos, atividades, ações e metas quanto à economia, eficiência e eficácia.

Para Rocha (1990), a auditoria operacional “é uma evolução natural da auditoria tradicional, que deixou de ser especificamente contábil para tornar-se abrangente, acrescentando à verificação da legalidade e correção dos registros contábeis, a determinação da economicidade e eficácia das entidades”.

Barzelay (2002) faz a diferenciação entre o conceito de auditoria de desempenho e o conceito de auditoria tradicional através da seleção de modelos cognitivos idealizados. O significado do conceito de auditoria de desempenho caracteriza-se por uma série de Modelos Cognitivos Idealizados inter-relacionados, que variam sob a ótica de cinco diferentes dimensões referentes ao funcionamento de governo, ao tipo de funcionamento desejado, ao principal objetivo da revisão, à modalidade dominante de revisão e ao papel do revisor

---

<sup>4</sup> Neste trabalho será adotada a denominação de auditoria tradicional como sinônimo das auditorias contábeis, auditorias de conformidade, auditorias financeiras, auditorias de legalidade, auditoria de regularidade na área governamental.

(auditor). A mesma lógica aplica-se ao significado do conceito de auditoria tradicional. O quadro 2, a seguir, apresenta esta lógica.

**Quadro 1 – Comparação entre auditoria tradicional e auditoria de desempenho**

	Imagem de Governo	Imagem de bom funcionamento	Objetivo principal da revisão	Modalidade predominante	Papel do revisor/ auditor
Auditoria Tradicional	Máquina Burocrática	Execução das transações e tarefas efetivamente reguladas por sistemas	Accountability de conformidade	Auditoria	Verificar as informações; encontrar discrepâncias entre os procedimentos observados e as normas gerais; inferir consequências; relatar achados
Auditoria de Desempenho	Cadeia de Produção: insumos→ processos→ produtos → impactos	Procedimentos e produção organizacionais funcionam de forma otimizada	Accountability de desempenho	Inspeção	Avaliar os aspectos dos programas e das organizações envolvidas; relatar achados

Fonte: Barzelay (2002, p. 4)

O GAO (2005) distingue melhor os dois tipos de auditoria através da descrição dos objetivos de cada uma delas. Na auditoria tradicional, esses objetivos se relacionam com as exigências estabelecidas por leis, regulamentos, cláusulas ou condições de contratos ou de convênios de subvenções que poderão afetar a aquisição, proteção e uso dos recursos da organização, bem como a quantidade, qualidade, oportunidade e custo dos trabalhos que a organização produz ou fornece.

Os achados de auditoria correspondem, por sua vez, às observações e conclusões obtidas através da comparação de evidência suficiente, fiável e



pertinente do desempenho com critérios predeterminados de auditoria (CCAF, 1995).

Por outro lado, as auditorias operacionais buscam fornecer informações para melhorar o desempenho dos programas e facilitar o processo de tomada de decisões dos dirigentes responsáveis pelas ações corretivas e aperfeiçoar a *accountability* perante o público.

Seguindo essa linha de distinção entre a auditoria tradicional e a auditoria operacional, Villas argumenta:

Enquanto, no primeiro grupo, o objetivo principal está relacionado com a adequação das demonstrações financeiras, no segundo as demonstrações financeiras servem apenas como instrumento do seu processo, visto que seu objetivo está vinculado à apreciação das operações ou atividades de uma entidade segundo os benefícios por ela produzidos (VILLAS, 1990, p. 58).

Lima (2005) sintetiza os tipos de auditoria - tradicional, de desempenho e avaliação de programa - como fiscalizações. A distinção inicialmente estaria no tipo de questão que se deseja responder. A auditoria tradicional, utilizando de procedimentos padronizados, satisfaz à investigação das questões legais e regulamentares. Em auditoria operacional e em avaliação de programas, é necessário um planejamento de trabalho com formato específico para cada situação, a fim de que possam ser respondidas as questões ligadas ao funcionamento interno dos programas e órgãos (economia, eficiência e eficácia) e os impactos de suas operações em condições sociais (efetividade). Posteriormente, Lima (2005) elencou diversas diferenças ao realizar o confronto entre a auditoria tradicional e a operacional, as quais estão organizadas no quadro 2, a seguir.

**Quadro 2 – Diferenças entre auditoria tradicional e auditoria operacional**

Tradicional	Operacional
Agentes externos independentes	Agentes externos parceiros
Punição de falhas	Contribuição para sanar falhas
Fluxo de trabalho é padronizado e hierárquico	O fluxograma de trabalho assemelha-se a uma cadeia de produção, contendo insumos, produtos e efeitos
Ambiente de comando e controle	Ambiente político com prevalência de debate democrático
Utilizações de padrões legais	Utilização de boas práticas, modelos, conhecimento e experiência, valores voltados para resultados ( <i>Results Oriented Management – ROM</i> )
Obediência a procedimentos	Empreendedorismo e liderança, escolha política e administrativa
Uso dos conceitos de direito e da contabilidade	Uso de informações obtidas através da pesquisa social, análise de políticas, economia
Imperatividade	Convencimento
Pouca participação popular	Debate público
Individualização da responsabilidade	Nem sempre possível individualizar (resultado)
Controle hierárquico e administrativo	Controle democrático e social
Os responsáveis são punidos com multas e afastamento	A penalidade atribuída é o ostracismo, a censura, danos na reputação

Fonte: Elaboração própria com base na classificação estabelecida por Lima (2005).

É importante destacar o papel de cada uma das auditorias em relação à outra, ressaltando que a auditoria operacional não está substituindo a auditoria tradicional, mas complementando a fiscalização que pode ser, inclusive, de um mesmo objeto. Se eventualmente ambas as auditorias escolherem objeto idêntico, apresentarão conclusões diferentes, porém complementares, uma vez que o foco do trabalho é distinto.

Assim, enquanto a auditoria tradicional restringe sua abrangência à área contábil-financeira e ao cumprimento dos aspectos legais objetivando, principalmente, verificar; a auditoria operacional atinge toda a entidade, pretendendo, também, avaliar.

### **3.5 LIMITAÇÕES DA AUDITORIA OPERACIONAL**

A expansão da auditoria operacional, muitas vezes, tem encontrado vários aspectos que se constituem em dificuldades ou limitações para sua implementação por parte das entidades de controle.

Um primeiro aspecto que pode ser destacado é o da ausência de uma estrutura organizacional definida dentro da instituição, levando, assim, a pouca autonomia dos grupos de trabalho na execução de procedimentos internos e externos. A inexistência de institucionalização dos trabalhos de auditoria operacional nos Tribunais de Contas Estaduais prejudica o desempenho das funções de controle.

Associada a essa situação está uma infra-estrutura muitas vezes deficitária, com número insuficiente de servidores especializados em auditoria operacional, quantidade reduzida de equipamentos de informática, poucos veículos disponibilizados para a realização dos trabalhos de campo. Além disso, o orçamento para esse tipo de auditoria é limitado, impossibilitando a contratação de especialistas ou consultores para auxiliar nos trabalhos.

A complexidade do processo de uma auditoria operacional é outro ponto importante, pois reflete as peculiaridades do objeto em análise, o que torna a execução desse tipo de auditoria amplamente diferente de um trabalho para outro, ou até mesmo entre períodos de tempo do mesmo trabalho. Isso porque é imprescindível que sejam respeitadas as características individuais de cada auditoria. Essa complexidade exige tempo, desde o planejamento até o término da execução, assim como um maior volume de recursos humanos e financeiros.

Outra questão é a cultura organizacional relacionada à auditoria operacional, o que pode se transformar em um limitador do resultado dos trabalhos. É possível que alguns gestores não vejam nas auditorias operacionais qualquer valor a ser agregado ao seu desempenho. É possível também que os técnicos se preocupem mais com os aspectos característicos de auditorias tradicionais, devido a uma cultura forte desse tipo de auditoria entre os profissionais dessa área. O interesse e a receptividade do gestor são indispensáveis para que os resultados da auditoria revertam-se em melhorias para o programa ou a gestão analisada.

Há também obstáculos na coleta das evidências que irão respaldar as conclusões dos técnicos, principalmente nos casos em que os critérios de comparação não estão disponíveis no programa auditado, situação que exigirá uma busca por critérios em outras fontes.

Neste contexto, pode ser sugerida a utilização de uma metodologia específica ou de uma combinação de metodologias, aplicável a cada caso, que respeite as características individuais do objeto auditado. Em cada objeto deverão ser considerados, entre outros fatores, os seus objetivos, os recursos empregados na sua consecução e os resultados alcançados, assim como as variáveis ambientais que exercem influência sobre esses resultados. Essa ausência de uniformidade na aplicação dos procedimentos, muito comum nas auditorias operacionais é mais uma dificuldade na sua disseminação e evolução.

Greiner (1996), apud Barros (2000, p.38), agrupou as limitações em quatro classes de fatores que seriam os obstáculos para a expansão e implementação da auditoria operacional. O quadro 3, a seguir, enumera essas limitações dentro da classe em que ela se enquadra :

Quadro 3 – Limitações da auditoria operacional

Obstáculos institucionais	Obstáculos pragmáticos	Obstáculos Técnicos	Obstáculos Financeiros
Desconhecimento de medidas de desempenho pela maioria dos gerentes do setor público	Dificuldade no desenvolvimento de medidas de desempenho	Falta de definição do que é desempenho governamental e o que deveria se enfatizado na mensuração desse desempenho	Dispêndio substancial de tempo e dinheiro na implementação dos sistemas de mensuração de desempenho
Baixo grau de imparcialidade e autoconfiança do governo optando pela não divulgação de informações que julgue prejudicar sua imagem	Relutância dos administradores públicos em utilizar as informações oriunda das mensurações de desempenho	Dificuldade de oferecer aos usuários os dados de desempenho em tempo oportuno	
Receio dos gestores de implementar novas ferramentas de avaliação devido a saturação de inovações ditas revolucionárias		Multiplicidade dos objetivos propostos pelo governo e a diversidade de alguns serviços que exigem diferentes medidas para caracterizar adequadamente o desempenho	
		Carência de padrões predefinidos para avaliar o desempenho governamental;	
		Flutuações estatísticas nas medidas de desempenho	
		Dificuldade em correlacionar recursos investidos e resultados alcançados	
		Ausência de procedimentos bem definidos, no âmbito governamental para gerenciar por números	

Fonte: Elaboração própria com base em Greiner (1996) apud Barros (2000).

Mesmo diante dessas limitações, percebe-se que o interesse e a importância da auditoria operacional, nos últimos anos, tem crescido devido ao anseio da sociedade por um controle que ultrapasse os exames da legalidade e busque avaliar os resultados obtidos com o uso dos recursos públicos.

A evolução da auditoria operacional no Brasil, conforme comentado anteriormente, está justamente respaldada no interesse dos órgãos de controle externo, em especial, dos Tribunais de Contas, em aperfeiçoar suas ferramentas de trabalho com vistas a dar subsídios aos cidadãos para que possam acompanhar a gestão pública.

## 4. AUDITORIA DE TI

---

Como ressalta Nunes (2004), a implantação da administração pública gerencial está freqüentemente associada à expansão e sofisticação dos sistemas de informação. De fato, nos dias de hoje é ampla a utilização de sistemas de computação pela administração pública, não se imaginando um órgão que não faça uso desta poderosa ferramenta de apoio à gestão.

O quadro de mudança do modelo de Estado e de sua administração impulsionaram o desenvolvimento da auditoria operacional como modalidade de controle. Com a expansão do uso da informática pelo setor público advinda deste quadro, é natural o crescimento de uma nova modalidade de auditoria de cunho operacional, a auditoria de informática, ou auditoria de sistemas de informação, ou auditoria de Tecnologia da Informação, como é mais conhecida.

Neste capítulo abordaremos os principais aspectos que envolvem a adoção da auditoria de TI pela administração pública, como as dificuldades para sua expansão e as diferentes áreas ou enfoques associados a este tipo de auditoria. Por fim, é apresentada a metodologia de auditoria de TI adotada pelo TCE-RJ nas inspeções realizadas nos municípios sob sua jurisdição.

### 4.1 DEFINIÇÃO DE AUDITORIA DE TI

A auditoria de sistemas, inicialmente, uma típica auditoria de resultados, por força de suas origens na auditoria contábil-financeira, necessita de forte adaptação cultural e técnica para atuar em auditoria de processos computacionais, consoante alerta de Gil (1998).

Conforme salienta Albertin (2002), a filosofia de auditoria de tecnologia de informação está calcada em confiança e em controles internos. Estes visam confirmar se os controles internos foram implementados e se existem, se são efetivos.

A auditoria de sistemas é, na visão de Gil (1998), a área de atuação que exerce a função administrativa Controle Interno, que atua via sistemas de informações computadorizados de controle interno que validam e avaliam, com independência e duplicidade lógica:

- as funções administrativas planejamento, execução e controle e seus respectivos sistemas de informações computadorizados;
- o ciclo administrativo, isto é, a integração sistêmica das funções administrativas: planejamento, execução e controle (GIL, 1998, p. 25)

Dias (2000) define a auditoria de TI como sendo um tipo de auditoria essencialmente operacional, por meio da qual os auditores analisam os sistemas de informação, o ambiente computacional, a segurança de informações e o controle interno da entidade fiscalizada, identificando seus pontos fortes e/ou deficiências.

## **4.2 A IMPORTÂNCIA DA AUDITORIA DE TI**

Albertin (2002) afirma que o tratamento das informações, que pode ser denominado Informática ou Sistemas de Informações, faz parte de toda atividade de negócio de uma empresa que oferece um produto ou serviço – desde a concepção, planejamento e produção até a comercialização, distribuição e suporte.

Segundo Gil (1998), entidades governamentais e privadas, independentemente de porte ou ramo de atividade, convivem e subsistem graças a doses cada vez mais elevadas de tecnologia computacional.

De fato, a Tecnologia da Informação tornou-se um componente crítico do planejamento estratégico das organizações públicas e privadas e, diante desse quadro no qual os processos passam a ficar altamente dependentes de sistemas informatizados, a realização de auditorias por parte dos órgãos de controle



mostra-se essencial para garantir que a Gestão de TI esteja colaborando efetivamente para o atendimento dos objetivos da organização e para a mitigação das fragilidades que colocam em risco os sistemas de informação.

Com o crescimento da utilização de sistemas de informação e redes de computadores, as organizações ficam expostas a novos tipos de ameaças à sua segurança. Concomitantemente, deve-se garantir que a tecnologia seja implantada de maneira correta, alinhada com os objetivos da organização.

O uso intenso de sistemas de computação pelas administrações públicas obriga as entidades de controle a fazer uso de auditorias de TI, com o intuito de verificar aspectos relativos a confiabilidade, integridade, eficácia, eficiência, confidencialidade, disponibilidade e conformidade (com normas e legislação) das informações mantidas nos sistemas de informação da organização.

A auditoria de tecnologia da informação já está presente no controle interno de diversas instituições públicas, sendo mais atuantes, estruturadas e maduras nas instituições públicas financeiras, como o Banco Central e o Banco do Brasil.

Entretanto, na maioria dos órgãos de execução de programas e políticas públicas e, até mesmo, nos órgãos especializados em controle, esse tipo de auditoria apresenta-se em um nível de maturidade iniciante, não existindo padrões, metodologias ou normas gerais a serem seguidas para planejamento e execução das ações de controle.

#### **4.3 A AUDITORIA DE TI NO TCE-RJ**

O Tribunal de Contas da União – TCU foi pioneiro na realização de auditoria de TI na administração pública. No início da década de 1990 foram realizadas as primeiras auditorias de sistemas e desenvolvidos os primeiros estudos para elaboração de técnicas e procedimentos especializados na área.

Ao longo dessa década, foi elaborado o Manual de Auditoria de Sistemas, em 1998, e realizadas importantes auditorias no Sistema de Seguridade Social,

no Sistema de Comércio Exterior, no ambiente de informática da Empresa Brasileira de Pesquisa Agropecuária, no Sistema de Administração Financeira, nos Sistemas da Previdência Social, nos planos para evitar danos devido ao Bug do Ano 2000 e nos sistemas do Patrimônio da União, já no ano de 2000.

A crescente importância dada à área de TI pelo TCU culminou com a criação em 2006 da Secretaria de Fiscalização de TI - SEFTI, através da Resolução 193.

O Tribunal de Contas do Estado do Rio de Janeiro – TCE-RJ, por meio da Coordenadoria de Auditoria e Desenvolvimento, vem atuando junto aos órgãos jurisdicionados desde 1999 na área de auditoria de TI, conforme estabelecido no Ato Normativo nº 45 de 21/10/98, alterado pelo Ato Normativo nº 58 de 15/03/2001. Esta atividade está prevista, inclusive, no Plano Estratégico desta Corte de Contas, o que reflete o compromisso com a modernização e atualização de seus processos de trabalho.

A Equipe de auditores de sistemas do TCE-RJ realizou preliminarmente uma série de estudos específicos na área de auditoria de TI que resultaram na elaboração de documentos de suporte à nova atividade. Dentre estes documentos podemos destacar os elencados abaixo:

- Manual de Auditoria de Sistemas
- Procedimentos de Auditoria de Sistemas
- Matriz de Planejamento
- Check-list de Auditoria de Sistemas

O Manual de Auditoria de Sistemas tem como objetivos descrever as principais técnicas utilizadas pelo auditor e padronizar a execução dos trabalhos, servindo de apoio, inclusive, a novos profissionais que venham a integrar a Equipe.

Os Procedimentos de Auditoria de Sistemas detalham os pontos de controle a serem auditados nas diversas áreas que compõem a atividade de informática, devendo ser periodicamente revistos e atualizados face ao dinamismo das novas tecnologias da informação.

A Matriz de Planejamento é um instrumento de apoio à tarefa de auditoria, possibilitando a definição do escopo e objetivos das Inspeções realizadas na área de auditoria de sistemas, na qual ficam definidas questões de auditoria que devem ser respondidas pelo auditor durante a execução dos trabalhos e a forma como estas serão respondidas.

O check-list é uma ferramenta de suporte às atividades in loco, através da verificação objetiva de itens previamente selecionados de acordo com o foco estabelecido para a Inspeção, de forma a garantir que os principais pontos de controle serão verificados.

O início dos trabalhos ocorreu com a inspeção especial no PRODERJ, pelo fato desta Autarquia ser o principal órgão executor de atividades de informática do Estado do Rio de Janeiro. Em seguida foram realizadas Inspeções em outros Órgãos do Estado, como CEDAE, IPERJ, Secretaria Estadual de Fazenda e DETRAN.

Na área municipal, a equipe de auditoria de sistemas realizou uma Pesquisa do Nível de Informatização dos Municípios jurisdicionados, com vistas a conhecer a real situação das prefeituras quanto à utilização da informática e detalhes de seu ambiente operacional.

Esta Pesquisa subsidiou o planejamento das atividades de auditoria de sistemas, sendo, inclusive, um dos critérios de escolha dos municípios a serem visitados, aliado à materialidade da arrecadação.

Desde então, já foram realizadas inspeções ordinárias em diversos municípios do estado do Rio de Janeiro. Dentre as principais Questões de Auditoria verificadas pela equipe na realização das Inspeções Municipais destacamos:

- Diagnóstico geral da situação da informática no município;

- O grau de segurança do ambiente de informática;
- Confiabilidade, segurança e funcionamento de um Sistema de Informação específico a ser selecionado;
- Adequação deste sistema à legislação vigente.

Esta forma de atuação do TCE-RJ, não verifica aspectos relacionados a resultados alcançados, mas sim ao funcionamento e operação da estrutura administrativa do órgão. A auditoria de TI, nesse caso específico, aproxima-se das definições de auditoria operacional abordadas no capítulo anterior, pois verifica questões ligadas ao funcionamento interno dos órgãos, examinando os métodos, processos, programas e ações quanto à economia, eficiência e eficácia.

A experiência na área municipal vem demonstrando a existência de muitos problemas operacionais na área de Tecnologia da Informação das Prefeituras, sendo um dos objetivos deste trabalho identificar e analisar as principais deficiências encontradas na área de sistemas de informação.

#### **4.4 DIFICULDADES À IMPLEMENTAÇÃO DE AUDITORIA DE TI NA ADMINISTRAÇÃO PÚBLICA**

Faz-se necessário também trazer a lume o atual contexto legal e infra-legal da auditoria de TI. Por melhores que sejam as referências e metodologias implementadas, os órgãos de auditoria de TI enfrentam um problema maior do que sua própria infra-estrutura e capacidade fiscalizatória. Uma das grandes dificuldades é a sustentação, nas recomendações das auditorias, de que essas melhores práticas devem ser seguidas, já que não existem instruções normativas ou legislação dentro da administração pública que obrigue a utilização dessas práticas. O TCU como órgão pioneiro nesta modalidade de auditoria é, atualmente, o que possui mais avanços na área, por meio de diversos acórdãos que fazem recomendações baseadas nos principais normas e padrões existentes no mercado, como ITIL, COBIT, MPS.BR e NBR ISO/IEC 17799:2005.

Dessa forma, por mais bem estruturado que seja o processo de auditoria, ela ainda fica amarrada à falta de base legal ou normativa que possa dar suporte às suas recomendações, prevalecendo, muitas vezes, apenas o bom senso de ambas as partes auditor e auditado.

A mais recente iniciativa em direção à normatização de processos de TI dentro da administração pública pode ser visto nos Acórdãos 796/2006 — Plenário e 1480/2007 — Plenário do TCU. O primeiro recomenda que a Secretaria de Logística e Tecnologia da Informação (SLTI) do Ministério do Planejamento, Orçamento e Gestão elabore um modelo de licitação e contratação de serviços de informática para a administração pública federal. O segundo consiste na análise da minuta de instrução normativa encaminhada pela SLTI relativa a este modelo solicitado. Em sua análise, o TCU faz diversas ressalvas ao modelo com a finalidade de que este esteja alinhado com os valores da Governança de TI e, em suas recomendações, sugere o uso das melhores práticas do mercado relacionadas à terceirização, como ITIL, COBIT, MPS.BR e etc. Merece destaque também a auditoria realizada pelo TCU no Sistema Nacional de Integração de Informações em Justiça e Segurança Pública – Infoseg, que resultou no Acórdão 71/2007, em que foram feitas recomendações baseadas na NBR ISO/IEC 17799:2005 e no COBIT 4.0.

Outra importante iniciativa é o Projeto de Lei PLS-76/2000 que está no Congresso Nacional e que dispõe sobre crimes cometidos na área de informática, tipifica condutas que envolvam o uso de redes de computadores e Internet, ou praticados contra sistemas informatizados. O Projeto já foi aprovado na Câmara dos Deputados e na Comissão de Educação do Senado. Atualmente, encontra-se na Comissão de Constituição e Justiça.

Tal lacuna legislativa também é motivação para esse trabalho, pois quanto mais se trabalhar nessa área e mostrar suas fragilidades, maiores serão os estímulos para que se legisle e regule a área de Tecnologia da Informação dentro da administração pública.

O TCE-RJ tem procurado embasar suas decisões relativas a auditorias de segurança de informações na norma NBR ISO/IEC 17799, da Associação

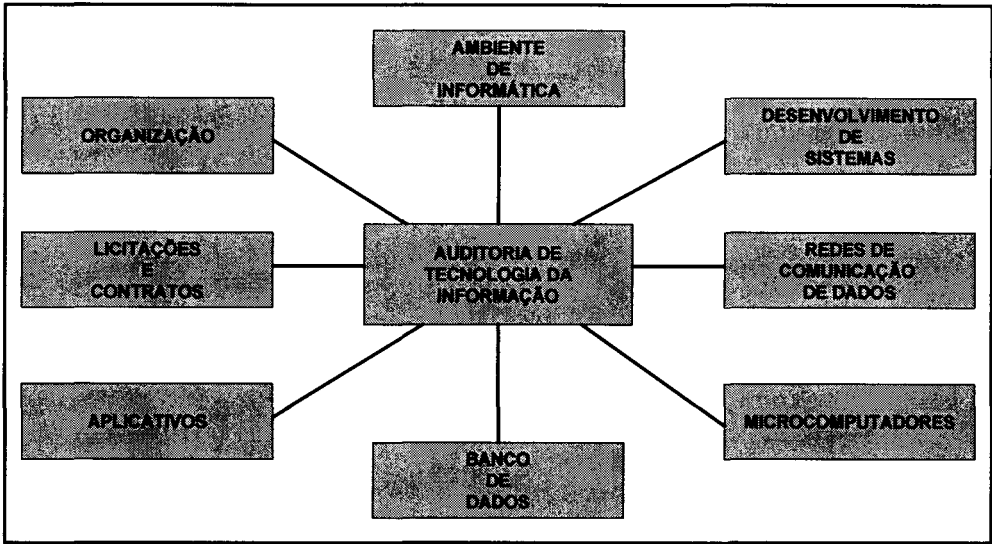
Brasileira de Normas Técnicas - ABNT, a qual trata de técnicas de segurança em Tecnologia da Informação, e funciona como um código de prática para a gestão da segurança da informação. Essa norma foi elaborada no Comitê Brasileiro de Computadores e Processamento de Dados, pela Comissão de Estudo de Segurança Física em Instalações de Informática.

A norma brasileira é baseada na ISO/IEC 17799, norma elaborada pelo ISO (International Organization for Standardization) e pelo IEC (International Electrotechnical Commission), sendo amplamente reconhecida e utilizada por Entidades Fiscalizadoras Superiores, órgãos de governo, empresas públicas e privadas nacionais e internacionais atentas ao tema Segurança da Informação. Os objetivos definidos nessa norma provêm diretrizes gerais sobre as metas geralmente aceitas para a gestão da segurança da informação, desde políticas de segurança da informação, controle de acesso, a gestão de ativos, de incidentes de segurança, de continuidade de negócios, entre outros.

#### **4.5 ÁREAS DE ATUAÇÃO**

Devido à complexidade da estrutura de um ambiente informatizado, o trabalho de auditoria de TI é dividido em diversos campos, diferenciados pelo enfoque e abrangência do trabalho a ser realizado. O TCE-RJ vem adotando a divisão mostrada na Figura 3 nos trabalhos de auditoria de TI realizados nas administrações municipais, em função do tamanho e complexidade do seu parque computacional, em geral composto por microcomputadores ligados em rede e por sistemas aplicativos com informações armazenadas em banco de dados.

Figura 2 - Áreas de atuação da TI



Fonte: Elaboração própria.

**Organização:**

Engloba aspectos como políticas, padrões e procedimentos da organização, responsabilidades organizacionais, gerência e planejamento de capacidade. Constitui área de alta relevância para a Auditoria de Sistemas pois, neste campo estão as definições de padrões e regras a serem seguidas no setor de Tecnologia da Informação, bem como procedimentos que garantam o efetivo cumprimento destas.

**Ambiente de Informática:**

Abrange as áreas de segurança física e lógica, planejamento de contingências e operação do Centro de Processamento de Dados (CPD).

**Banco de Dados:**

Abrange a verificação da integridade, consistência e disponibilidade dos dados, bem como do acesso aos mesmos.

**Redes de Comunicação de Dados:**

Envolve a tecnologia, gerência e segurança das informações transmitidas através das redes de computadores da organização. Tais controles de auditoria são altamente importantes pois envolvem as principais ferramentas de acesso a dados, contidas na maioria dos sistemas operacionais de rede. As políticas de acesso à Rede devem estar bem formuladas e seu gerenciamento bem executado de forma a garantir que os dados disponíveis neste poderoso instrumento de compartilhamento estejam seguros.

**Desenvolvimento de sistemas:**

Abrange as metodologias de desenvolvimento de sistemas, projeto, estudo de viabilidade, design, implementação, operação e manutenção de sistemas de informática. Estes itens são aplicáveis em caso de haver no órgão a atividade de desenvolvimento ou manutenção de um sistema de informação, haver a prestação deste tipo de serviço a um órgão jurisdicionado, ou até atividades de consultoria em algum sistema importante para a administração pública.

A observância destas normas visa a garantir a qualidade dos sistemas desenvolvidos e adequação dos mesmos à sua finalidade.

**Microcomputadores:**

O trabalho do auditor de sistemas em microinformática deve avaliar a atuação do Departamento de Informática para identificar ações implementadas, como inventário de micros, sua localização física e seus *softwares*, mecanismos para prevenir e detectar o uso ou instalação de programas não licenciados (*software* pirata), procedimentos para documentação e backup de programas, arquivos de dados e aplicativos, e tratamento dado ao ambiente de microinformática no Plano de Contingência.



**Aplicativos:**

É o trabalho de auditoria de um sistema de informação específico. Deve-se levar em conta o aspecto técnico (funcionamento) e o legal, relativos à área auditada. Este tipo de auditoria é crítico por verificar a legalidade de um sistema, isto é, se o seu produto final está de acordo com as leis em vigor e se está acarretando ou não desvio de recursos públicos.

Esta área é de extrema importância para o setor público, pois estando os controles dos recursos informatizados, estes sistemas devem conter instrumentos que garantam a confiabilidade, segurança e disponibilidade dos dados provenientes destes.

**Licitações e Contratos:**

Contratos e Editais de Licitação relativos à aquisição de produtos e serviços de Informática normalmente contêm cláusulas técnicas específicas, cuja avaliação requer conhecimentos especializados em Informática, devendo então sofrer análise técnica por um auditor de sistemas, sem prejuízo da análise legal cabível.

A análise técnica por parte do auditor de sistemas tem por objetivo evitar que um processo seja aprovado com imperfeições na descrição técnica do objeto que poderiam, inclusive, comprometer a análise legal, levando a um embasamento incorreto na legislação vigente.

O questionamento quanto à legalidade, nestes casos, passa, necessariamente, por uma correta identificação do objeto e conhecimento das modalidades de contratação existentes no mercado.

Além disso, é importante a verificação minuciosa das cláusulas técnicas que assegurem a completa execução dos serviços propostos e/ou aquisição de produtos.

Apresentamos no Quadro 4, uma série de características a serem examinadas nos trabalhos de exame técnico dos contratos e editais:

**Quadro 4 – Aspectos técnicos verificados nos editais e contratos**

Natureza dos contratos	Hardware	Software	Serviços
Compras ou locação	Análise da configuração técnica	Compatibilidade dos software com o sistema operacional	Cessão do código fonte dos programas
	Parecer do TCE sobre a exclusividade do fornecedor quando cabível	Atualização de novas versões quando cabível	Entrega de documentação técnica
	Compatibilidade do Hardware com o sistema operacional	Parecer do TCE sobre a exclusividade de fornecedor quando cabível	Definição de serviços
Manutenção	Cláusulas de condições de atendimento: <ul style="list-style-type: none"><li>- técnico residente</li><li>- horário comercial</li><li>- horas extras</li><li>- fins de semanas / feriados</li></ul>	Prazo de atendimentos às chamadas	
	Prazo máximo para solucionar os problemas	Implementações de novas versões	
	Prazo de atendimento às chamadas	Documentação de alterações ou correções	
	Equipamento de backup, quando cabível	Ambiente de backup, quando cabível	

Fonte: Elaboração própria.

O auditor de sistemas deve realizar a sua análise tendo em mente que um sistema de informação é um produto de *software* sujeito a uma constante manutenção ocasionada por fatores externos como, por exemplo, mudanças provocadas por motivos legais, mudança dos equipamentos utilizados etc.

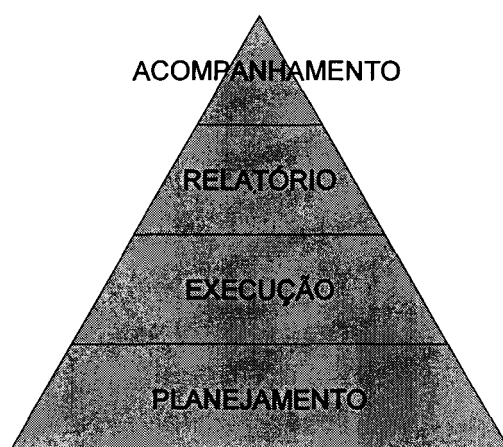
Ainda para o caso citado acima, a cláusula de propriedade dos dados deve mostrar de forma clara e precisa que os dados pertencem ao contratante. Devem estar presentes no contrato cláusulas que garantam ao contratante proteção de informações confidenciais.

## 4.6 ETAPAS DA AUDITORIA DE TI NO TCE-RJ

A Auditoria de TI por ser uma modalidade de auditoria operacional deve ser desenvolvida em quatro estágios: planejamento, execução, relatório e acompanhamento. Esta divisão está de acordo com as práticas adotadas pelas principais EFS.

A figura a seguir mostra as fases de uma auditoria operacional.

**Figura 3 – Fases de uma auditoria operacional**



**Fonte: Elaboração própria**

### PLANEJAMENTO

Segundo Araújo (2001), o planejamento de auditoria é a fase em que o auditor obtém uma visão geral do trabalho a ser realizado, ou seja, definem-se as finalidades da ação a ser realizada e identificam-se as questões que deverão ser respondidas.

Esta fase deve considerar os fatores mais relevantes na execução dos trabalhos, especialmente os seguintes:

- O conhecimento detalhado dos processos operacionais utilizados pela entidade;
- O conhecimento detalhado do sistema de controles internos da entidade e seu grau de confiabilidade;

- Os riscos de auditoria e a identificação das áreas importantes da entidade, quer pelo volume de transações, quer pela complexidade de suas operações;
- A natureza, oportunidade e extensão dos procedimentos de auditoria a serem aplicados;
- As questões relacionadas com a economia de recursos, aumento da eficiência etc;
- O cumprimento das metas e objetivos traçados pela administração para a atividade a ser auditada;
- A existência de indicadores de desempenho estabelecidos pela administração ou de outros dados que possam servir às exigências da auditoria;
- O uso dos trabalhos de outros auditores e de especialistas;
- A natureza, conteúdo e oportunidade dos relatórios a serem entregues à entidade;
- A necessidade de atender aos prazos estabelecidos por entidades fiscalizadoras e para a entidade prestar informações aos demais usuários externos, como, por exemplo, os agentes financiadores de programas governamentais (ARAÚJO, 2001).

O manual de auditoria operacional (TCU,2000) prescreve que as auditorias de desempenho devem ser precedidas de um levantamento de auditoria em seu objeto (programa, projeto, atividade, sistema, órgão ou entidade). A análise preliminar do objeto da auditoria visa compreender como esse objeto está estruturado, permitindo que a equipe identifique questões que mereçam ser examinadas mais detalhadamente.

A equipe deve buscar, acerca do objeto, informações como:

- Os objetivos (gerais ou parciais, dependendo da extensão do trabalho)
- As ações desenvolvidas, as metas fixadas, os clientes atendidos, os procedimentos e recursos empregados, os bens e serviços ofertados e os benefícios proporcionados;
- As linhas de subordinação e de assessoramento previstas e sua relação com as atividades desenvolvidas;

- As partes interessadas (reais ou em potencial) e as características do ambiente externo (dinâmico ou estático; previsível ou imprevisível);
- As restrições enfrentadas (imposições legais e limitações impostas pela concorrência, pela tecnologia, pela escassez de recursos ou pela necessidade de cooperar com outras entidades) (TCU,2000).

Ainda segundo o manual de auditoria operacional (TCU, 2000), essas informações podem advir de diversas fontes, dentre as quais:

- Legislação pertinente;
- Pronunciamentos feitos e decisões tomadas pelas autoridades competentes;
- Missão declarada, planos estratégicos e relatórios de gestão;
- Organogramas, diretrizes internas e manuais operacionais;
- Sistemas de informações gerenciais;
- Entrevistas com os gestores especialistas;
- Relatórios de auditoria do TCU, relatórios de auditoria interna e de avaliação de desempenho institucional (TCU,2000).

Com base nas informações coletadas sobre o órgão são definidos problemas de auditoria, que expressam de forma clara e objetiva o escopo do trabalho de auditoria. Os problemas de auditoria são desmembrados em diversas questões de auditoria, que deverão ser respondidas na fase de execução do trabalho *in loco*. A matriz de planejamento é o documento que detalha a forma como as diversas questões de auditoria podem ser respondidas.

A equipe de inspeção de TI do TCE-RJ utiliza-se da matriz de planejamento nessa fase da auditoria, em sintonia com o previsto no manual de auditoria operacional (TCU,2000). O objetivo da matriz de planejamento é auxiliar na elaboração conceitual do trabalho e na orientação da equipe na fase de execução. É uma ferramenta de auditoria que torna o planejamento mais

sistemático e dirigido, facilitando a comunicação de decisões sobre metodologia entre a equipe e os superiores hierárquicos e auxiliando na condução dos trabalhos de campo.

Os seguintes elementos compõem a matriz de planejamento de auditoria:

- questões de auditoria;
- informações requeridas;
- fontes de informação;
- estratégias metodológicas;
- métodos de coletas de dados;
- métodos de análise de dados;
- limitações;
- o que a análise vai permitir.

Ao formular as questões de auditoria a equipe está estabelecendo com clareza o foco de sua investigação e os limites e dimensões que deverão ser observados durante a execução dos trabalhos.

O ANEXO D apresenta um exemplo de matriz de planejamento utilizada nas inspeções operacionais de TI realizadas pelo TCE-RJ nos municípios. Faz-se necessário salientar que a matriz de planejamento é um instrumento flexível e o seu conteúdo é atualizado ou modificado pela equipe, de acordo com o órgão auditado ou com a evolução do trabalho de auditoria.

## **EXECUÇÃO**

A execução é a fase do trabalho realizado no órgão auditado. Araújo (2001) define a execução como sendo a fase de aplicação dos procedimentos de auditoria, objetivando a obtenção de provas ou evidências que deverão constar no relatório de auditoria. É nessa fase que o auditor realiza fundamentalmente seus exames.

Segundo o autor os procedimentos de auditoria são o conjunto de técnicas ou métodos que permitem ao auditor obter elementos probatórios de forma suficiente e adequada para fundamentar seus comentários, quando da elaboração de seu relatório. Os principais procedimentos de auditoria são: exame de registros, exame documental, conferência de cálculos, entrevistas, inspeção física, circularização, observação e correlação.

A equipe de inspeção em TI utiliza-se de diversos *checklists* durante a execução dos trabalhos de auditoria *in loco*. Os *checklists* de auditoria consistem em listas de elementos, pontos de controle, que vem a ser necessariamente verificados, de modo a assegurar a conformidade do ambiente analisado com normas, padrões técnicos e boas práticas adotadas pelo mercado.

## RELATÓRIO

Segundo Araújo (2001), o relatório de auditoria é a fase final do processo de auditoria e consiste numa narração ou descrição ordenada e minuciosa dos fatos que foram constatados, com base em evidência concreta, durante os exames de auditoria operacional. Representa a fase mais significativa do trabalho e se constitui no seu produto final.

O Tribunal de Contas da União, através da Portaria nº 63/96, assim define o relatório de auditoria:

Documento contendo as comprovações, conclusões e, eventualmente, recomendações que a instituição de fiscalização ou o auditor consideram útil levar ao conhecimento da entidade fiscalizada ou de qualquer outra autoridade competente.

O relatório de auditoria operacional em TI apresenta o resultado do trabalho de auditoria, tendo como objetivo responder às questões de auditoria formuladas na fase de planejamento e apontar os pontos positivos ou negativos encontrados na fase de trabalho *in loco* no órgão auditado. Esses pontos são denominados constatações, observações ou achados de auditoria.

Por se tratar de trabalho de natureza eminentemente operacional, o relatório de auditoria em TI resulta em proposição de uma série de recomendações ao órgão auditado, que objetivam garantir segurança ao ambiente informatizado e assegurar o correto processamento das informações pelos sistemas informatizados.

Como já assinalado neste trabalho, não existem instruções normativas ou legislação na administração pública que dêem suporte às recomendações realizadas e obrigue o seu cumprimento pelo jurisdicionado. As recomendações são baseadas em manuais de boas práticas na área de informática editados por organismos nacionais e internacionais, prevalecendo, muitas vezes, apenas um acordo entre ambas as partes, TCE-RJ e jurisdicionado, para que as recomendações sejam adotadas.

## **ACOMPANHAMENTO**

Após a entrega do relatório de auditoria e da ciência de seu conteúdo pelo órgão jurisdicionado, faz-se necessário realizar um acompanhamento para verificar a efetiva adoção das recomendações e determinações realizadas.

Via de regra, o órgão jurisdicionado envia ofício resposta para o TCE-RJ com o intuito de comprovar a adoção das medidas propostas no relatório de auditoria. Como a inspeção tem caráter operacional, é extremamente difícil a comprovação das medidas adotadas somente por meio do exame dos documentos e declarações enviadas pelo jurisdicionado.

Nesse contexto, é de grande importância a realização de inspeções posteriores para verificar a efetiva adoção pelo jurisdicionado das medidas recomendadas. As inspeções devem ter escopo limitado à verificação das ações implementadas e devem ter também caráter educacional, de forma a corrigir as possíveis falhas e desvios que possam continuar a existir.

Como atualmente existe apenas uma única equipe de auditores de TI no TCE-RJ, foram realizadas poucas inspeções de retorno para a verificação da adoção das medidas recomendadas.



#### **4.7 METODOLOGIA DE AUDITORIA DE TI ADOTADA PELO TCE-RJ**

A forma de atuação do TCE-RJ nas inspeções de auditoria de TI, aproxima-se da definição de auditoria integrada adotada pela Fundação Canadense de Auditoria Integrada - CCAF, em que o objetivo é avaliar se os recursos públicos têm sido utilizados obedecendo aos critérios de otimização de recursos.

A auditoria integrada abrange o exame dos controles, processos e sistemas usados na gerência dos recursos financeiros, humanos, materiais e de informações das organizações. A auditoria integrada não se limita ao exame do passado. Ela se utiliza das análises dos controles existentes, dos sistemas de informação e dos relatórios práticos para recomendar melhorias no planejamento que resultem em uma melhor economia, eficiência e eficácia (CCAF, 1995).

Uma metodologia completa de auditoria de TI dá parâmetros para a realização da Auditoria em todas as suas fases e funciona como um facilitador para o desenvolvimento de práticas e procedimentos a serem aplicados durante a execução do processo.

Para que se tenha como resultado essa metodologia, deve-se conciliar as práticas e normas de TI conhecidas no mercado, a legislação brasileira e as normas de auditoria. A partir daí, deve-se compilar e adaptar todas essas variáveis à necessidade da administração pública e seus princípios, de forma a gerar uma metodologia simples e aplicável na prática.

As práticas do mercado e as normas técnicas são descritas no próximo capítulo. A legislação brasileira refere-se tanto às normas relacionadas ao Sistema de Controle Interno e Externo brasileiro, constando do ANEXO A - LEGISLAÇÃO DE CONTROLE. As normas pertinentes ao uso da informação e da tecnologia constam do ANEXO B - LEGISLAÇÃO APLICÁVEL À TI.

Os principais princípios da administração pública devem nortear qualquer trabalho relacionado à área pública e consistem em legalidade, moralidade,

impressoalidade, publicidade, eficiência, supremacia do interesse público, indisponibilidade, continuidade dos serviços públicos e autotutela.

## 5. GOVERNANÇA DE TECNOLOGIA DA INFORMAÇÃO

---

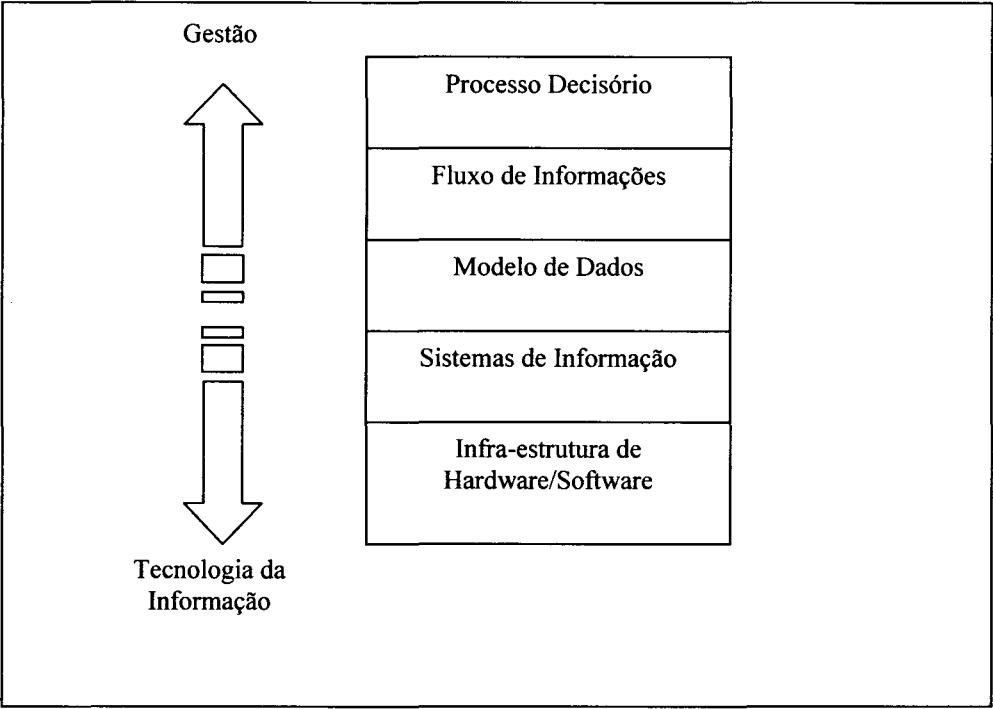
Este capítulo descreve, inicialmente, os conceitos de governança de TI e a importância de sua adoção para orientar o uso da tecnologia da informação como ferramenta de suporte aos negócios de uma organização. A seguir, são abordados os modelos e metodologias mais importantes que orientam a adoção da governança de TI. Por fim, são descritos mais detalhadamente o modelo Cobit e as normas técnicas relativas à área de segurança da informação, pelo fato de servirem de suporte às auditorias de TI realizadas pelo TCE-RJ no âmbito das administrações municipais.

Com o avanço tecnológico e a importância que a tecnologia tem hoje dentro das organizações, o planejamento e a implantação de uma arquitetura de informações se tornaram tarefas complexas.

Por arquitetura de informações, entende-se, segundo Rodriguez (2002), um conjunto de informações, modelos de dados e toda infra-estrutura tecnológica necessária para suportar os fluxos de informações gerados a partir dos processos decisórios de uma organização.

A integração entre a tecnologia e o negócio é a chave para o sucesso organizacional. A figura 4 apresenta um esquema dessa integração.

**Figura 4 – Integração de Negócios à Arquitetura de Informações**



**Fonte:** RODRIGUEZ, M.V.R. **Gestão Empresarial: organizações que aprendem.** Rio de Janeiro: Qualitymark, 2002.

Segundo o *IT Governance Institute* (2006), a sobrevivência e o sucesso de uma organização diante desse novo mercado globalizado, onde os tempos e as distâncias foram suprimidos, estão no efetivo gerenciamento das informações e de suas relativas tecnologias. As organizações precisam gerenciar sua arquitetura de informações como um todo, desde a infraestrutura até as informações, passando pelos sistemas e processos geradores dessas informações.

Para muitas empresas, essas informações e tecnologias que as suportam são seus principais ativos. Por isso, o gerenciamento da informação e suas tecnologias precisam garantir, entre outras coisas, a distribuição, a segurança e integridade das informações.

Nesse contexto em que a tecnologia da informação assume um papel estratégico dentro das organizações, surgem os modelos de governança em TI com o objetivo de auxiliar estas organizações a gerir suas áreas de tecnologia,

fornecendo ferramentas e métricas que garantam o alinhamento entre os processos de TI e os objetivos estratégicos da organização.

O conceito de governança em TI é derivado do conceito de governança corporativa. O *IT Governance Institute* (2006) afirma que a governança de TI integra a Governança da Empresa e consiste em mecanismos de liderança, estrutura organizacional e processos que garantem que a TI da organização mantenha e alcance as estratégias e objetivos da organização.

GREMBERGER et. al (2004) definem Governança de TI como a capacidade organizacional exercida pela Diretoria, Gerência Executiva e Gerência de TI para controlar a formulação e implementação da estratégia de TI e neste caminho assegurar a fusão do negócio e TI.

“Governança de TI é o modelo como as decisões são tomadas e responsabilidades direcionadas para encorajar um comportamento desejável no uso de TI” (WEILL, ROSS, 2004).

O trabalho de levantamento da governança de TI na administração federal realizado pelo TCU afirma que o objetivo da governança de TI é assegurar que as ações de TI estejam alinhadas com o negócio da organização, agregando-lhe valor. O desempenho da área de TI deve ser medido, os recursos propriamente alocados e os riscos inerentes mitigados. Assim, é possível gerenciar e controlar as iniciativas de TI nas organizações para garantir o retorno de investimentos e a adoção de melhorias nos processos organizacionais (TCU, 2007).

Embora as definições apresentadas sejam diferentes em alguns aspectos, elas têm como foco principal o mesmo assunto: a ligação entre negócio e TI.

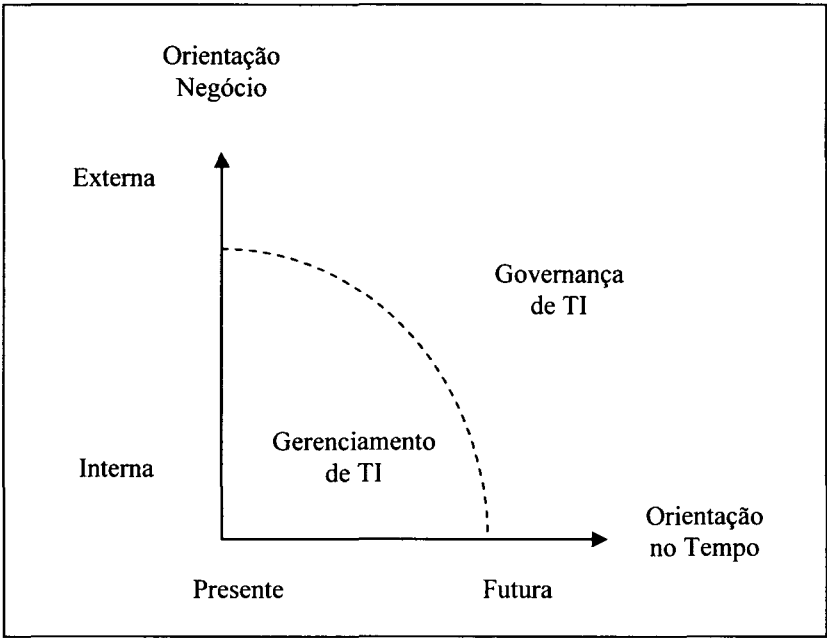
## **5.1 DIFERENÇA ENTRE GOVERNANÇA DE TI E GERENCIAMENTO DE TI**

Uma importante e comum preocupação da governança de TI é a ligação entre a TI e os objetivos atuais e futuros da organização. Esta preocupação nos remete a refletir sobre as diferenças entre governança de TI e gerenciamento de

TI, que nem sempre são claras (Gremberger et al. 2004). Esta distinção pode ser melhor visualizada na Figura 5.

Gerenciamento de TI tem como foco o fornecimento efetivo de serviços e produtos de TI internos, assim como o gerenciamento das operações de TI no presente. A governança de TI por sua vez é mais abrangente e concentra-se no desempenho e transformação de TI, para atender demandas atuais e futuras do negócio da corporação (foco interno) e negócio do cliente (foco externo). “Isto não diminui a importância e complexidade do gerenciamento de TI, ..., mas enquanto o gerenciamento de TI e fornecimento de serviços de TI e produtos podem ser realizados por um fornecedor externo, a governança de TI é específica da organização, e direção e controle sobre TI não podem ser delegados para o mercado” (PETERSON (2003) apud GREMBERGER et. al (2004)).

**Figura 5 – Governança de TI e Gerenciamento de TI**



**Fonte:** Gremberger et. al., 2004.

“Governança determina quem toma as decisões. Gerenciamento é o processo de fazer e implementar as decisões” (WEILL, ROSS, 2004).

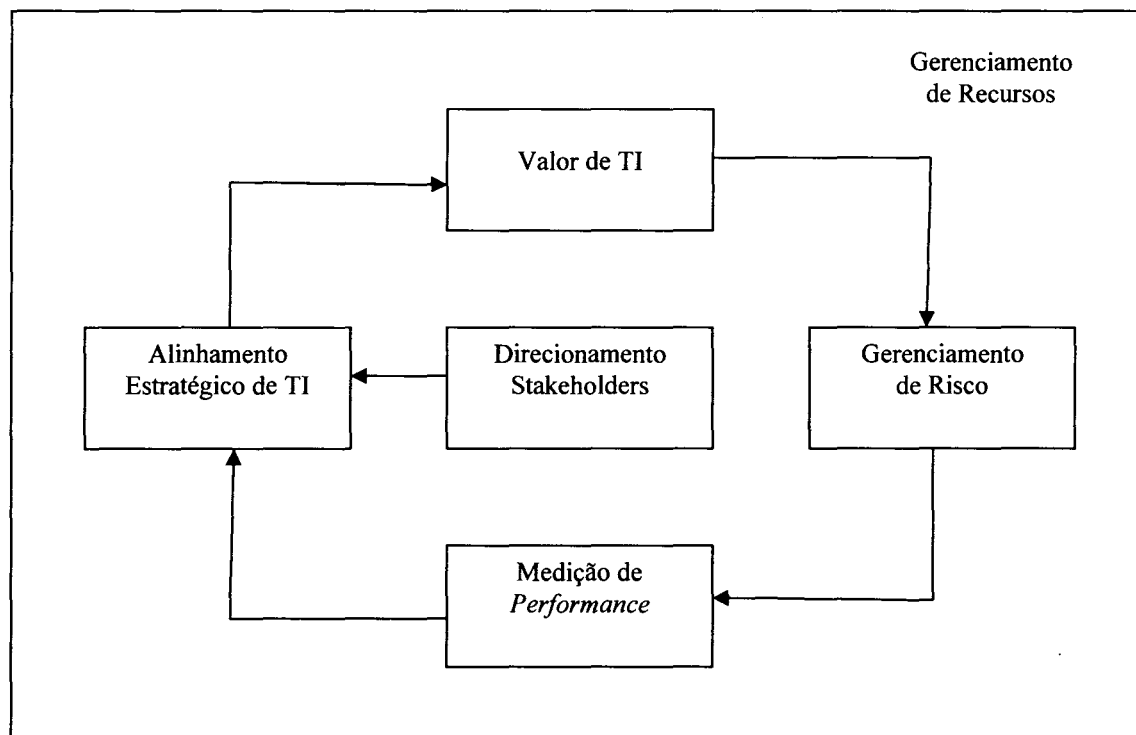
## 5.2 DOMÍNIOS DA GOVERNANÇA DE TI

A governança de TI está relacionada a dois focos: o valor dos serviços de TI para o negócio e mitigação dos riscos de TI. O primeiro item é suportado pelo alinhamento estratégico entre TI e o negócio. O segundo é suportado pela forma como as responsabilidades na empresa são divididas. Ambos os focos precisam ser suportados por recursos e medidas adequados para que os resultados desejados sejam alcançados.

Para suportar os focos acima a governança de TI lida com cinco domínios, todos alinhados com as diretrizes dos *stakeholders*, dos quais dois são resultados, Valor de TI e Gerenciamento de Risco, e três são direcionadores, Alinhamento Estratégico, Gerenciamento de Recursos e Medição de *Performance* (IT Governance Institute, 2006).

A Figura 6 abaixo mostra graficamente a relação entre os domínios da governança de TI.

**Figura 6 – Áreas de Domínio da Governança de TI**



**Fonte:** IT Governance Institute, 2006.

Apresenta-se a seguir um resumo sobre o objetivo de cada um dos domínios, conforme o “*Board Briefing on IT Governance*” (IT GOVERNANCE INSTITUTE, 2006):

- **Alinhamento Estratégico:** tem como objetivo manter o alinhamento entre as soluções de TI e o negócio da empresa.
- **Valor de TI:** tem como objetivo otimizar os custos dos investimentos de TI e o retorno dos mesmos.
- **Gerenciamento de Risco:** tem como objetivo assegurar a proteção dos ativos de TI, recuperação de informações em caso de desastres e manter a continuidade da operação dos serviços de TI.
- **Gerenciamento de Recursos:** tem como objetivo otimizar o conhecimento e infraestrutura de TI.
- **Medição de Performance:** tem como objetivo acompanhar a entrega dos projetos de TI e monitorar os serviços de TI.



### 5.3 MODELOS PARA SUPORTE A GOVERNANÇA TI

O *IT Governance Institute* (2006) define a Governança de TI como uma estrutura de relacionamentos e processos, para dirigir e controlar a organização no sentido de atender os objetivos dessa organização, adicionando valor, ao mesmo tempo em que equilibra os riscos em relação ao retorno da TI e seus processos.

Os diversos conceitos de governança apresentados têm influenciado as organizações, e a partir daí muitos modelos e metodologias foram criados e disseminados e já são utilizados pelas empresas.

Alguns dos modelos mais conhecidos são:

- Cobit – *Control Objectives for Information and related Technology*;
- ITIL - *IT Infrastructure Library*;
- BS7799 - *Information Security Standard*;
- CMM / CMMI - *Capability Maturity Model / Capability Maturity Model Integration*.

Cada um desses modelos tem focos distintos.

- Cobit (*Control Objectives for Information and related Technology*): Guia para a gestão de TI recomendado pelo *Information Systems Audit and Control Foundation* (ISACF) que fornece informações detalhadas para gerenciar processos baseados nos objetivos de negócios.

- ITIL (*IT Infrastructure Library*) : Elaborado pelo governo britânico para fornecer as diretrizes para implementação de uma infra-estrutura otimizada de TI. É um conjunto de melhores práticas para gerir o planejamento, gerenciamento de

incidentes e problemas, mudanças, configurações, operações, capacidade, disponibilidade e custos dos serviços de TI.

- CMM/CMMI (*Capability Maturity Model / Capability Maturity Model*) : É uma certificação concedida pelo *Software Engineering Institute* (SEI), da Universidade de Carnegie Mellon (USA), que mede o grau de maturidade no processo de desenvolvimento de software.

- BS7799 (*Information Security Standard*): Norma internacional, editada pelo Governo Britânico, para segurança em TI. Abrange os aspectos de segurança física do ambiente, passando por pessoas e detalhando cuidados essenciais das questões relacionadas à rede de comunicação, aplicativos e acesso remoto.

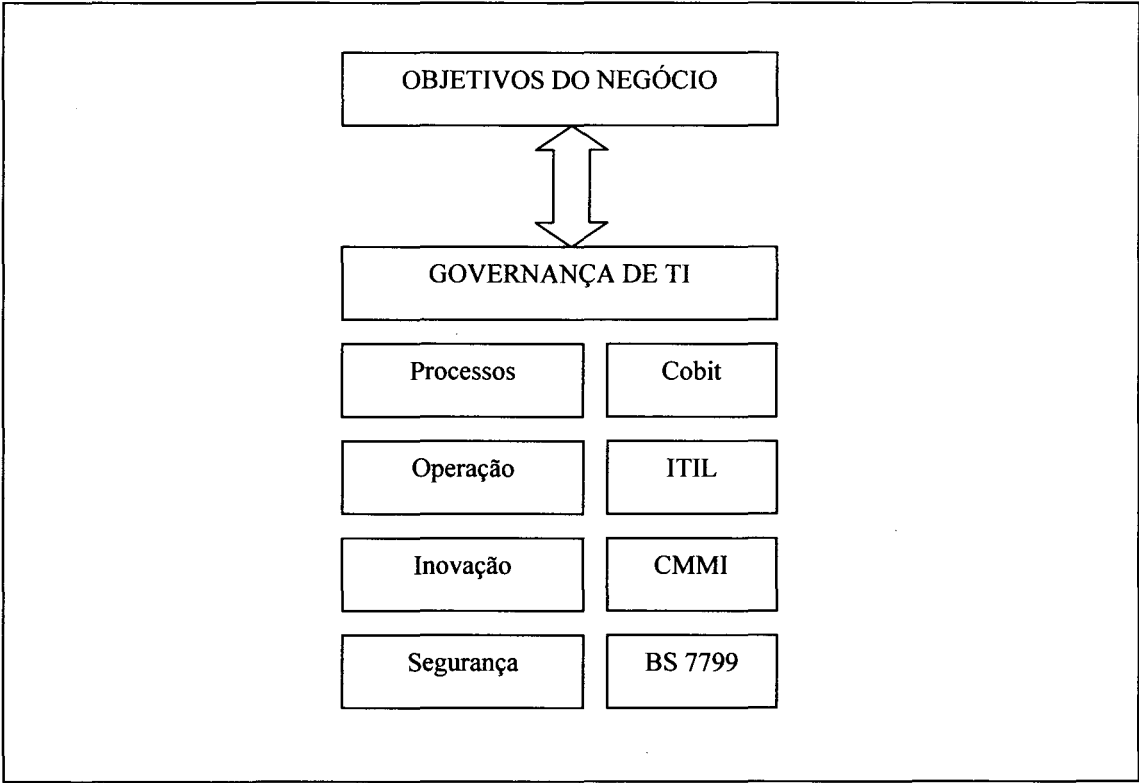
Neste trabalho é apresentada a norma NBR ISO/IEC 17799, norma voltada à gestão da segurança da informação, e que se originou da norma BS7799.

Apesar de cada modelo ter um foco diferente, eles não são mutuamente excludentes (MINGAY e BITTINGER, 2002), podem ser combinados para prover um melhor gerenciamento da tecnologia, garantindo não só o suporte tecnológico necessário, para que a organização atinja seus objetivos estratégicos com qualidade e preço competitivo, mas também a satisfação dos seus clientes.

De acordo com Barton (2003) os modelos de administração de TI se completam, uma vez que cada um deles tem um enfoque específico e atende a alguns dos aspectos da administração de TI.

A melhor opção pode ser a combinação de mais de um modelo, conforme demonstra a figura a seguir.

**Figura 7 – Integração dos Modelos de Governança de TI**



**Fonte:** Adaptado de CID, Miranda; PIMENTEL, Luis F. **Fundamentos de Governança de TI.** In. SEMINÁRIO SUCESU, 2005. Rio de Janeiro

O uso de modelos de gestão de TI vem crescendo à medida que a competitividade do mercado força as empresas a se preocuparem cada vez mais com a qualidade dos serviços prestados e com os custos de suas operações, pois esses modelos permitem um melhor gerenciamento do nível de serviço por meio da padronização.

No caso das empresas públicas brasileiras, em função da complexidade administrativa e das restrições orçamentárias, adotar um modelo de governança em TI e implantá-lo de forma integral pode ser um projeto difícil e muito longo.

A solução para essas empresas pode estar na implantação de parte do modelo ou da combinação deles, ou seja, adequar o modelo escolhido para a realidade de cada uma das empresas; colocando em prática as recomendações consideradas mais relevantes para a organização.

Apresentaremos a seguir algumas das práticas e normas conhecidas e bem aceitas no mercado, que objetivam garantir a utilização adequada de TI pelas organizações e servem como guia para as auditorias de TI realizadas pelo TCE-RJ.

### 5.3.1 COBIT

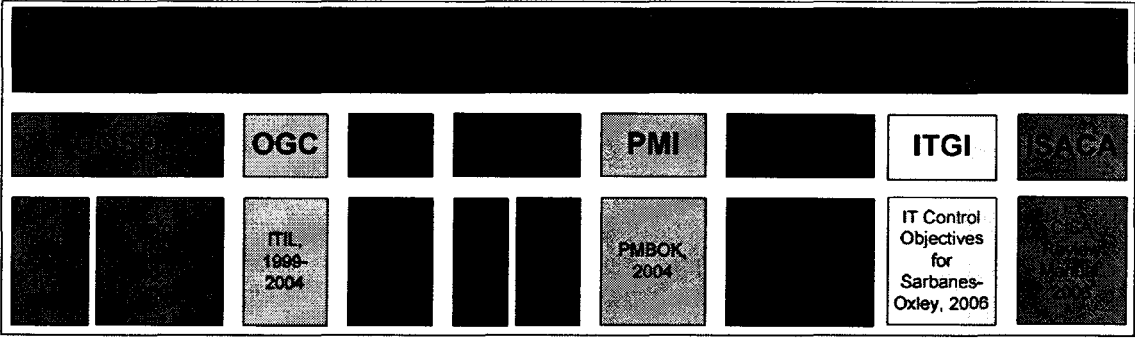
O COBIT - *Control Objectives for Information and Related Technology* (Diretrizes de Controle para Informação e Tecnologia Relacionada) - foi desenvolvido pelo ISACF - *The Information Systems Audit and Control Foundation*, tendo como base a metodologia COSO. Posteriormente, o COBIT passou a ser mantido pelo ITGI - IT Governance Institute.

Atualmente, o COBIT encontra-se na versão 4.1. Trata-se de uma estrutura conhecida mundialmente que busca garantir que a Tecnologia de Informação esteja alinhada aos objetivos corporativos, que os seus recursos sejam usados com responsabilidade e os seus riscos gerenciados apropriadamente.

As atualizações no COBIT 4.1 incluem medida de desempenho aperfeiçoada, melhores objetivos de controle e melhor alinhamento dos negócios e das metas de TI.

A versão 4.1 é baseada nas práticas e padrões reconhecidos internacionalmente, como PMBOK:2000, ITIL:1999-2004, CMM:1993, CMMI:2000, ISO/IEC 17799:2005, entre outros, como pode ser observado na Figura 8.

Figura 8 – Melhores práticas e padrões abrangidos pelo COBIT 4.1



Fonte: COBIT 4.1

A estrutura do COBIT busca atender às necessidades de controle relacionadas à Governança de TI e tem como características:

- Foco nos requisitos de negócio;
- Orientação para uma abordagem de processo;
- Base em controle; e
- Direcionamento para análise de medições e indicadores de desempenho.

5.3.1.1 FOCO NOS REQUISITOS DE NEGÓCIO

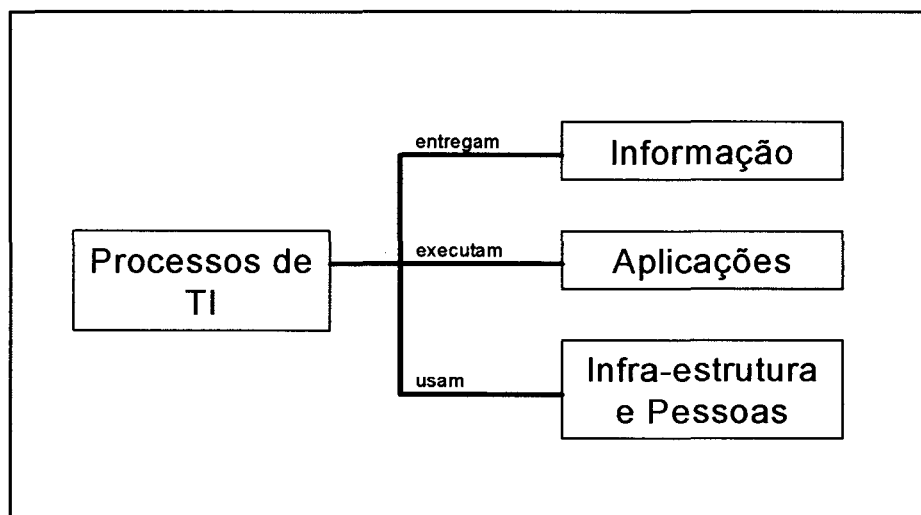
De acordo com o COBIT, a fim de se obter a informação necessária ao atendimento dos objetivos da organização, é necessário que os recursos de TI sejam gerenciados e controlados, utilizando-se de um conjunto estruturado de processos para garantir a entrega dos serviços de TI requeridos. Os recursos de TI são:

- **Aplicações:** são os sistemas automatizados e procedimentos manuais que processam a informação.

- **Informação:** é o dado em todas as suas formas, como entrada, processado ou como saída de um sistema informatizado, em qualquer forma utilizada pelo negócio.
- **Infra-estrutura:** é a tecnologia e facilidades (isto é, *hardware*, sistemas operacionais, sistemas de gerenciamento de banco de dados, rede, multimídia, e ambiente) que possibilita o processamento de aplicações.
- **Pessoas:** é o pessoal necessário para planejar, organizar, adquirir, implementar, entregar, dar suporte, monitorar e avaliar os sistemas de informação e serviços. Eles devem ser internos, terceirizados e/ou contratados como necessário.

Esses quatro recursos, juntamente com os processos, formam a arquitetura de TI representada na Figura 9. Assim, os processos de TI usam infra-estrutura e pessoal para serem realizados e executam aplicações com a finalidade de entregar informação na forma necessária para atingir os objetivos de negócio.

**Figura 9 – Arquitetura de TI**



Fonte: COBIT 4.1

Os processos do COBIT são constituídos por alguns princípios (Qualidade, Confiança e Segurança) que representam os requisitos do negócio para a informação. Eles são chamados de critérios de informação:

- **Efetividade:** Trata-se da capacidade da informação ser relevante e pertinente ao processo do negócio, bem como ser entregue de um modo oportuno, correto, consistente e útil.
- **Eficiência:** Diz respeito à provisão da informação através do uso ótimo (mais produtivo e econômico dos recursos)
- **Confidencialidade:** Diz respeito à proteção da informação sigilosa contra a divulgação não autorizada.
- **Integridade:** Relaciona-se à exatidão e à completeza da informação bem como à sua validade de acordo com os valores e expectativas do negócio.
- **Disponibilidade:** Relaciona-se à disponibilização da informação quando requerida pelo processo de negócio. Também diz respeito à salvaguarda dos recursos necessários e potencialidades associadas.
- **Conformidade:** Trata-se do cumprimento das leis, dos regulamentos e arranjos contratuais aos quais o processo de negócio está sujeito, isto é, critérios de negócio impostos externamente bem como políticas internas.
- **Confiabilidade:** Relaciona-se à provisão de informação apropriada para a gerência operar a entidade e exercer suas responsabilidades fiduciárias e de governança.

O grau de importância de cada um desses critérios é uma função do negócio e do ambiente em que a organização opera. Numa avaliação de riscos, esses critérios atribuem pesos diferentes aos processos do COBIT, em função da importância no alcance dos respectivos Objetivos de Controle.

### 5.3.1.2 ORIENTAÇÃO PARA PROCESSOS

Os componentes do COBIT são utilizados para fazer com que a TI seja orientada aos objetivos do negócio e cumpra seu papel na instituição. Para tanto, as boas práticas do COBIT são organizadas em processos, cada qual visando um Objetivo de Controle.

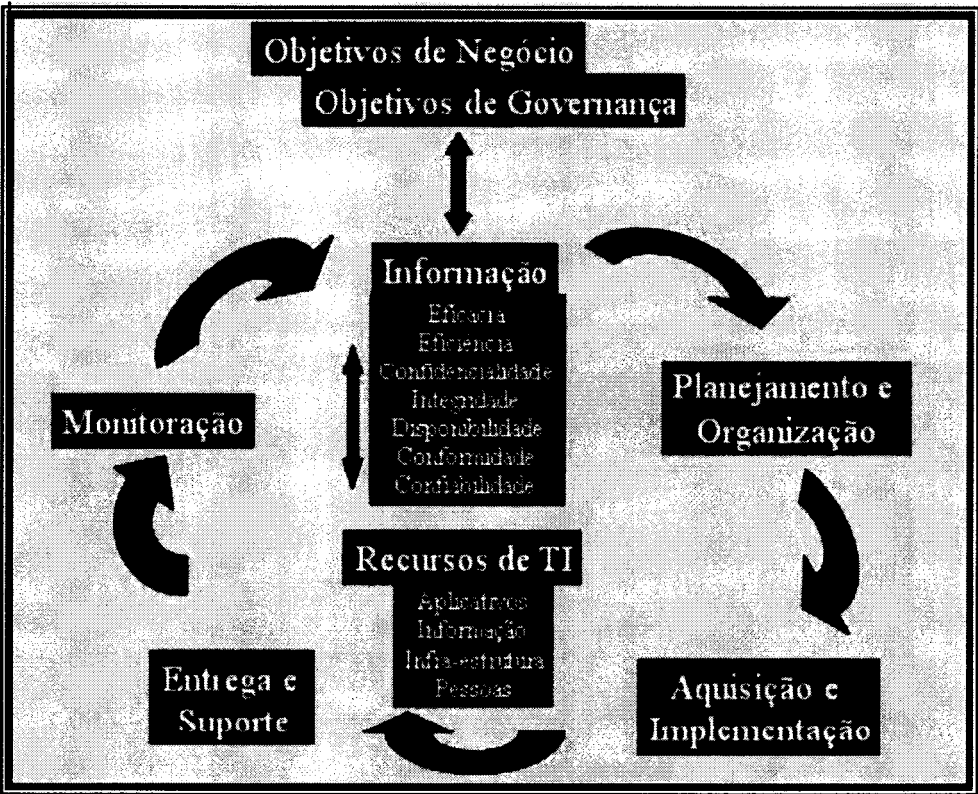
O COBIT identifica um conjunto de 210 Objetivos de Controles, organizados em 34 Processos que são agrupados em 4 Domínios, aplicáveis aos sistemas e à Tecnologia da Informação.

Um objetivo de controle é definido como uma declaração de um propósito ou resultado desejado a ser alcançado, por meio da implementação de controles em determinada atividade de TI. Esses objetivos de controle, se atingidos por meio da implementação eficaz dos respectivos controles, garantem o alinhamento da TI aos objetivos do negócio e que eventos indesejáveis sejam prevenidos, apagados ou corrigidos. A responsabilidade pelo sucesso dos sistemas de controles é, portanto, da alta direção, a qual deve torná-los efetivos.

Na Figura 10, podem ser identificados os domínios do COBIT (Planejamento e Organização, Aquisição e Implementação, Entrega e Suporte, e Monitoramento), que integram um ciclo de vida no sistema de gestão de TI.



Figura 10 – Framework do COBIT

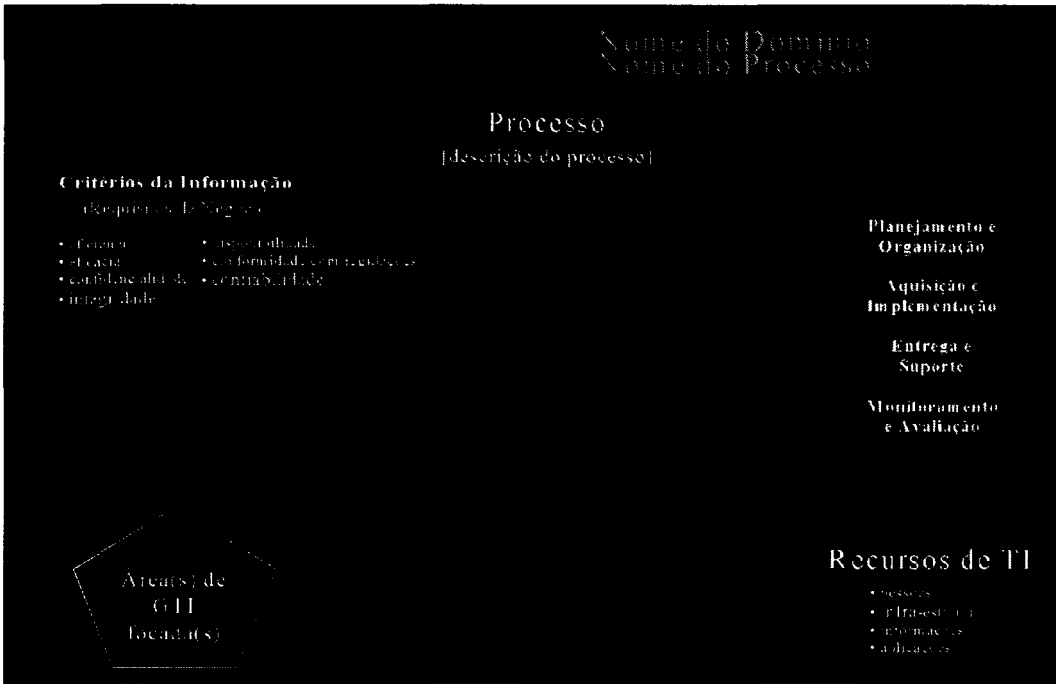


Fonte: COBIT 4.1

Os 34 processos que fazem parte destes domínios são identificados no ANEXO C: TABELA COBIT. Esta tabela também possui um mapeamento relativo aos critérios de informação e recursos de TI envolvidos nos processos.

Cada processo possui um mapa demonstrando os critérios da informação e recursos de TI envolvidos, o domínio a que pertence, a área de Governança de TI focada, os principais objetivos e a métrica usada para medição. A Figura a seguir mostra a forma de navegação no mapa de cada processo.

Figura 11 – Forma de Navegação nos processos do COBIT



Fonte: COBIT 4.1

5.3.1.3 BASE EM CONTROLE

Para cada processo são definidos objetivos de controle que definem um resultado esperado ou um propósito a ser atingido pela implementação de procedimentos de controle em uma atividade de TI específica. Os objetivos de controle do COBIT representam os requisitos mínimos necessários para que se possam controlar os processos de TI de forma eficaz.

Assim, colhem-se informações de controle da operação de cada processo de TI para compará-las aos objetivos de controle. Caso haja necessidade, são tomadas medidas preventivas ou corretivas.

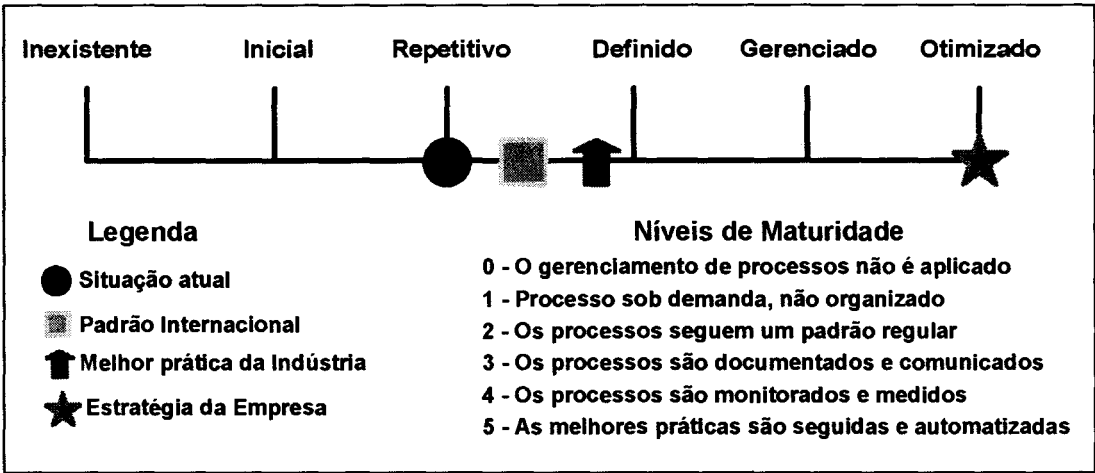
5.3.1.4 DIRECIONAMENTO PARA MEDIÇÕES E INDICADORES

A análise de medições e o uso de indicadores de desempenho são necessários para que a organização conheça sua situação atual, compare com padrões de mercado ou com organizações similares, identifique as melhorias necessárias e monitore tais melhorias.

Esse processo de autoconhecimento e melhoria da organização pode ser subsidiado pela análise de maturidade dos processos e pela avaliação de indicadores.

O Modelo de Maturidade de Governança é utilizado para o controle dos processos de TI e fornece um método eficiente para classificar o estágio da organização de TI em relação à indústria, aos padrões internacionais e ao objetivo de maturidade da organização. A governança de TI e seus processos podem ser classificados de acordo com os níveis apresentados na Figura a seguir.

Figura 12 - Modelo de Maturidade do COBIT



Fonte: COBIT

A maturidade deve ser avaliada em cada um dos processos. O nível ótimo correspondente é determinado individualmente, de acordo com a natureza da instituição, ameaças e oportunidades viabilizadas por TI. O COBIT fornece

orientações específicas para cada processo do que deve ser trabalhado para atingir determinado nível de maturidade.

O COBIT também oferece métricas para a medição dos objetivos. Existem dois tipos de métricas:

- Medidas de saídas: Indicam se os objetivos foram alcançados, podendo ser usadas somente após o acontecimento do fato;
- Indicadores de desempenho: Indicam a probabilidade de se alcançar os objetivos por medições realizadas antes da geração de saídas.

Esses dois tipos de métricas podem ser usadas para analisar objetivos de negócio, de TI, de processo e de atividade, medindo suas saídas e desempenhos.

O COBIT é uma excelente ferramenta para aperfeiçoar processos e adequar as funções de TI às normas da área de informática. A equipe de auditores de TI do TCE-RJ tem procurado selecionar aqueles controles que se aplicam na realidade do ambiente computacional encontrado nas administrações municipais, como forma de auxiliar os trabalhos de auditoria e servir como parâmetro para avaliar o nível de maturidade dos serviços prestados na área.

### **5.3.2 SEGURANÇA DA INFORMAÇÃO**

As principais normas internacionais relacionadas à segurança da informação são a ISO/IEC 27001:2005 e a ISO/IEC 17799:2005.

Estas normas originaram-se da norma BS 7799 (*British Standard*) editada pelo Governo Britânico. Em 1995, foi publicada a primeira versão da BS 7799-1 (BS 7799-1:1995 - Tecnologia da Informação - Código de prática para gestão da segurança da informação). Em 1998, foi publicada a primeira versão da BS 7799-2 (BS 7799-2:1998 - Sistema de gestão da Segurança da Informação - Especificações e guia para uso). A partir daí, estas normas passaram por

processos de revisão, tendo se tornado respectivamente nas normas ISO/IEC 17799 e ISO/IEC 27001, e evoluíram até a versão atual.

Em setembro de 2005, foi publicada, no Brasil, a segunda versão da norma NBR ISO/IEC 17799 (Tecnologia da Informação - Código de prática para gestão da segurança da informação), tradução literal da norma ISO.

Em Outubro de 2005, foi publicada a norma 150 27001 (ISO/IEC 27001:2005 - Tecnologia da Informação - Técnicas de segurança - Sistema de gestão da Segurança da Informação - Requisitos).

Neste ano, a ISO (*International Organization for Standardization*) e o IEC (*International Electrotechnical Commission*) lançaram a série 27000, em que, além da ISO/IEC 27001, contempla a ISO/IEC 27002 (em substituição à ISO 17799) e a ISO/IEC 27004 (que focará a melhoria contínua do sistema de gestão da segurança da informação).

Neste trabalho, faremos um pequeno resumo da NBR ISO/IEC 17799:2005, pois as recomendações relativas à segurança da informação constantes dos relatórios de auditoria de TI do TCE-RJ são baseadas fundamentalmente nesta norma.

#### **5.3.2.1 NBR ISO/IEC 17799:2005**

A NBR ISO/IEC 17799 estabelece diretrizes e princípios gerais para iniciar, manter e melhorar a gestão da segurança da informação em uma organização.

O objetivo da norma não é detalhar procedimentos de configuração, mas identificar os pontos de partida para a constituição de uma gestão de segurança da informação eficaz por meio de recomendações que se traduzem sob a forma de controles. Assim, serve como um guia prático para desenvolver os procedimentos de segurança da informação e práticas eficientes de gestão de segurança para a organização.

A norma é dividida em 11 seções de controles de segurança da informação, que juntas totalizam 39 categorias principais de segurança e uma seção introdutória que aborda a análise/avaliação e o tratamento de riscos.

Cada seção contém um número de categorias principais de segurança da informação. Cada categoria, por sua vez, contém um objetivo de controle que define o que deve ser alcançado e um ou mais controles que podem ser aplicados para se alcançar o objetivo do controle.

As descrições dos controles estão estruturadas da seguinte forma:

- **Controle:** define qual o controle específico para atender ao objetivo do controle.
- **Diretrizes para a implementação:** contém informações mais detalhadas para apoiar a implementação do controle e atender ao objetivo de controle. Algumas destas diretrizes podem não ser adequadas em todos os casos e assim outras formas de implementação do controle podem ser mais apropriadas.
- **Informações adicionais:** contém informações que podem ser consideradas como, por exemplo, considerações legais e referências a outras normas.

O Quadro mostrado a seguir apresenta as 11 seções de controles de segurança da informação e seus respectivos assuntos.

Quadro 5 – Controle de Segurança da Informação

Sistema	Assunto
Política de Segurança	Descreve a estrutura do documento de Política de Segurança, análise crítica e avaliação.
Segurança Organizacional	Aborda a infra-estrutura de segurança, o controle de acesso dos prestadores de serviço e o estabelecimento de responsabilidades e caso de terceirização.
Classificação e Controle de Ativos de Informação	Detalha a contabilização e o registro de ativos e a classificação da informação.
Segurança de Pessoas	Foca o risco decorrente de atos intencionais ou acidente realizado por pessoas. Além disso, aborda a inclusão de responsabilidades relativas à segurança da informação na descrição dos cargos, a forma de contratação e o treinamento em segurança.
Segurança Física e Ambiental	Define áreas de segurança, segurança dos equipamentos e controles gerais.
Gerenciamento das Operações	Aborda procedimentos e responsabilidades operacionais, planejamento e aceitação dos sistemas, proteção contra <i>softwares</i> maliciosos, salvamento e recuperação dos dados, gerenciamento de rede, segurança e tratamento de mídias, troca de informações e <i>software</i> .
Controle de Acesso	Aborda requisitos do negócio para controle de acesso, gerenciamento de acesso de usuários, responsabilidade do usuário, controle de acesso à rede, controle de acesso ao sistema operacional, controle de acesso às aplicações, monitoração de uso e acesso aos sistemas, computação móvel e acesso remoto.
Desenvolvimento e Manutenção de Sistemas	Aborda requisitos de segurança de sistemas, segurança de sistemas de aplicação, controles de criptografia, segurança de arquivos do sistema.
Gestão de Incidentes de Segurança	Aborda a notificação de fragilidades e eventos de segurança da informação e a gestão de incidentes de segurança da informação e melhorias.
Gestão de Continuidade do Negócio	Aborda processo de gestão, continuidade do negócio e análise de impacto, documentação e implementação do plano de continuidade dos negócios, testes, manutenção, e reavaliação dos planos de continuidade.
Conformidade	Aborda a necessidade de conformidade com requisitos legais, análise crítica da política de segurança e da conformidade técnica, considerações quanto à auditoria de sistemas.

Fonte: NBR ISO/IEC 17799:2005

## **6. METODOLOGIA**

---

Este capítulo apresenta algumas considerações metodológicas sobre o projeto de pesquisa, destacando-se os tipos de pesquisa que foram utilizados. São apresentados também o universo e a amostra com que se pretende trabalhar, os instrumentos de coleta de dados e seu tratamento, bem como se antecipam algumas das limitações do método proposto.

### **6.1 TIPO DE PESQUISA**

Segundo a taxonomia apresentada por Vergara (2006), os tipos de pesquisa dividem-se em dois critérios básicos: quanto aos fins e quanto aos meios.

A pesquisa proposta pode ser classificada quanto aos fins em:

Pesquisa descritiva – à medida que visa descrever as características da auditoria operacional e, em particular, da auditoria em TI que servirão de base à pesquisa explicativa.

Pesquisa explicativa – porque pretende estabelecer relações entre a adoção da auditoria de Tecnologia da Informação pelo TCE-RJ e seus efeitos na melhoria do papel do Tribunal de Contas, tornando-o mais amplo e em sintonia com as aspirações da sociedade.

Quanto aos meios, a pesquisa é:

Bibliográfica – o tema foi pesquisado em livros, revistas, jornais, redes eletrônicas e em manuais técnicos específicos sobre auditoria operacional em TI.

Documental – a investigação se valeu também de documentos internos ao TCE-RJ, que possuíam correlação com o objeto do estudo.



Estudo de Caso – a pesquisa está restrita à forma de atuação do TCE-RJ na realização de auditorias de TI.

## **6.2 UNIVERSO E AMOSTRA**

O universo desta pesquisa é constituído pelos municípios do estado do Rio de Janeiro, entes federativos jurisdicionados do Tribunal de Contas do Estado do Rio de Janeiro, onde é crescente o uso da informática como instrumento de apoio à gestão administrativa.

Foi realizado um estudo preliminar para selecionar os municípios que fariam parte da pesquisa, com o objetivo de selecionar vinte amostras que representem as sete grandes regiões geográficas em que o TCE-RJ divide o estado do Rio de Janeiro. O Tribunal possui em sua administração uma Inspeção Regional de Controle Externo (IRE) para cada uma das sete regiões, responsável por um controle mais próximo e especializado de municípios que apresentam características econômicas e sociais similares.

A seleção destes municípios visou, portanto, obter uma amostra significativa, no sentido de representar os diferentes tipos de administração municipal em suas diversas dimensões, como tamanho e estruturação do corpo administrativo e, principalmente, quanto a aspectos de abrangência e intensidade do uso de recursos de informática como apoio à gestão administrativa.

A avaliação da gestão municipal foi realizada por meio de auditoria de Tecnologia da Informação, tendo por finalidade analisar a utilização da informática pelo município, o grau de segurança do ambiente de informática, confiabilidade, segurança e funcionamento de um sistema de informação específico e a conformidade deste sistema à legislação da área.

### 6.3 COLETA DE DADOS

A coleta de dados começou com a pesquisa bibliográfica em documentos de domínio público emitidos pelo Tribunal de Contas da União (TCU), entidade pública brasileira precursora na realização de auditorias com enfoque operacional em TI, como também em documentos e papéis de trabalho do Tribunal de Contas do Estado do Rio de Janeiro (TCE-RJ).

Em seguida foram analisados documentos das entidades fiscalizadoras superiores de diversos países, como Estados Unidos, Inglaterra, Nova Zelândia e Austrália, pioneiros na realização de auditorias operacionais, como também normas e padrões de auditoria de TI nacionais e internacionais, adotados por entidades de fiscalização públicas e privadas.

A segunda fase consistiu na análise dos relatórios de inspeções em Auditoria de Sistemas realizados pelo TCE-RJ, buscando comprovar na prática a relevância desse instrumento de auditoria na avaliação da gestão municipal, especificamente em relação ao uso da tecnologia da informação.

### 6.4 TRATAMENTO DOS DADOS

Os dados colhidos no trabalho de campo, oriundos de relatórios de inspeções em Auditoria de Sistemas realizadas pelo TCE-RJ, foram submetidos à análise de conteúdo, numa abordagem qualitativa. Bardin (1977) define a análise de conteúdo como:

Um conjunto de técnicas de análise das comunicações visando obter, por procedimentos, sistemáticos e objetivos de descrição do conteúdo das mensagens, indicadores (quantitativos ou não) que permitam a inferência de conhecimentos relativos às condições de produção/recepção (variáveis inferidas) destas mensagens.

Foram criadas categorias com base em frases e parágrafos como unidades de análise, tendo sido selecionadas as mais frequentemente citadas, incluindo-se ainda aquelas consideradas relevantes para o tema da pesquisa.

Tais categorias representam achados de auditoria encontrados nas inspeções de Auditoria de Sistemas realizadas pelo TCE-RJ no período de 2003 a 2007, em âmbito municipal.

Procedeu-se então à classificação das categorias obtidas e da frequência relativa a cada uma delas dentro dos possíveis critérios de classificação identificados na literatura relativa à área de auditoria de TI.

## **6.5 LIMITAÇÕES DO MÉTODO**

Como toda pesquisa, o estudo em questão apresenta diversas limitações. A principal delas está certamente relacionada à abrangência dos municípios sob análise, visto que o estudo se limita à verificação de relatórios de vinte municípios. Esta limitação foi contornada por uma escolha dos municípios mais representativos de sete grandes regiões geográficas em que o TCE-RJ divide o estado. Desta forma, buscou-se retratar as diferentes realidades socioeconômicas e suas influências na utilização de tecnologia da informação pelos municípios.

Outra grande dificuldade consiste na dificuldade de obtenção de material técnico internacional, liberados somente com autorização dos organismos responsáveis.

7. PESQUISA

A pesquisa teve como objetivo principal responder o problema formulado inicialmente, que consistiu em identificar as principais impropriedades no uso da Tecnologia da Informação verificadas pelo TCE-RJ nas administrações municipais sob sua jurisdição.

Com este intuito, foi realizado, primeiramente, um trabalho de análise de conteúdo de caráter qualitativo sobre os relatórios de inspeções operacionais em TI efetuados pelo TCE-RJ nos municípios jurisdicionados.

Buscou-se identificar nos relatórios as principais deficiências relativas à utilização da informática pelas administrações municipais. Foram selecionadas onze categorias, levando-se em consideração aquelas que influenciam mais negativamente na correta execução da política de informática pelo município.

O quadro a seguir mostra as categorias identificadas.

**Quadro 6 – Categorias de análise identificadas**

<b>Categoria</b>	<b>Descrição</b>
1	Planejamento estratégico na área de informática falho ou inexistente
2	Implementação de políticas de segurança da informação falhas ou inexistentes
3	Procedimentos de contingência falhos
4	Procedimentos de cadastramento de usuários na rede de computadores e nos sistemas de informação realizados sem formalidade
5	Ausência de política de senha forte na rede de computadores e nos sistemas de informação
6	Ausência de campo específico nos sistemas de informação para registro de número do processo administrativo em operações críticas
7	Arquivos de log ausentes ou com registro falho nos sistemas de informação
8	Sistema de informação em desacordo com legislação específica vigente
9	Divergência entre os valores registrados no sistema de controle da arrecadação e no sistema de contabilidade
10	Impropriedades no instrumento contratual que ferem a legislação vigente, notadamente a Lei Federal nº 8.666/93
11	Não execução ou execução parcial do objeto contratado

Fonte: Elaboração própria, a partir da análise dos principais achados nos relatórios de auditoria de TI.

Em seguida, procedeu-se à contagem da presença de cada uma das categorias identificadas em relatórios de inspeção de vinte municípios, escolhidos com o objetivo de contemplar as sete principais regiões geográficas do estado do Rio de Janeiro. A escolha dos municípios foi orientada de forma a representar as diferentes realidades sociais, políticas e econômicas do estado, que resultam em administrações com tamanho e características distintas, e em que o uso da informática tem maior ou menor grau de importância. Cada região corresponde também a uma área de fiscalização de uma Inspeção Regional de Controle Externo (IRE) do TCE-RJ.

A tabela a seguir evidencia se para cada um dos vinte municípios selecionados há ou não a presença da respectiva categoria. A identificação dos municípios foi omitida propositalmente, pois o que se busca com o presente trabalho é a análise das principais impropriedades de informática e sua distribuição, e não analisar as deficiências de um município específico.

Tabela 1 : Frequências das categorias de análise

Categorias	Municípios																				Frequência
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	
1	1	1	1	1	-	1	1	1	1	1	1	-	1	1	1	1	1	1	1	1	18
2	1	1	-	1	1	1	1	1	1	1	1	-	1	1	1	1	1	-	1	1	17
3	1	1	-	1	1	-	1	1	1	-	1	1	1	1	1	1	1	-	1	1	16
4	1	1	1	1	1	1	-	1	-	1	1	1	-	1	-	1	1	1	1	1	16
5	-	1	-	1	-	1	1	1	1	1	1	1	1	-	1	1	-	1	1	1	15
6	-	1	-	1	-	-	1	1	-	1	-	1	1	-	-	-	-	1	-	-	8
7	-	1	-	1	-	1	1	1	-	1	-	1	1	-	1	-	-	1	-	1	11
8	-	1	-	1	-	-	-	-	-	1	-	-	-	-	-	-	-	-	-	-	3
9	-	1	-	1	-	1	1	1	-	1	-	1	1	1	1	-	-	1	1	1	13
10	1	-	1	1	1	-	1	-	-	-	-	-	-	1	1	-	1	-	1	-	9
11	-	-	-	-	-	-	-	-	-	1	-	-	-	-	-	-	-	1	-	-	2

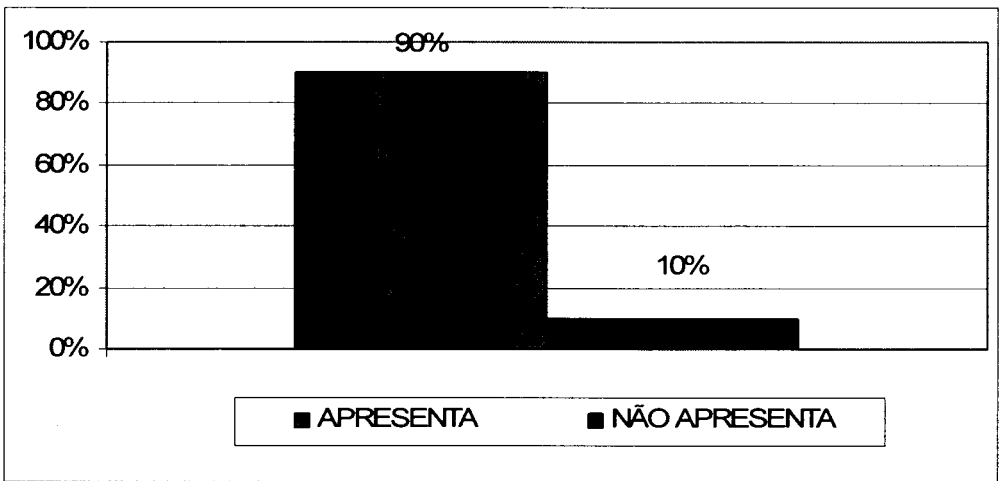
Fonte: Elaboração própria.

O próximo passo da pesquisa consistiu em analisar cada uma das categorias em função de suas respectivas frequências, evidenciando as consequências para o município em caso de ocorrência da impropriedade relativa ao uso de Tecnologia da Informação e as medidas que devem ser adotadas pela administração para sanar os problemas de gestão na área de sistemas de informação.

**1) Planejamento estratégico na área de informática falho ou inexistente**

A grande maioria dos municípios estudados apresenta a irregularidade em questão, 90 %, conforme gráfico a seguir, o que demonstra a pouca importância dispensada para o planejamento na área de informática.

**Gráfico 1 – Planejamento estratégico na área de informática falho ou inexistente**



**Fonte: Elaboração Própria**

O Planejamento é a primeira função administrativa e base para as demais. Sem o planejamento da área de Informática não é possível administrá-la, sendo entendido que administrar neste contexto é executar as outras funções administrativas.

Ein-Dor e Segev (1978) argumentam que o objetivo principal de um processo formal de planejamento estratégico de sistemas de informação é a produção de sistemas de informação gerenciais consistentes com a política geral da organização.

Cash, McFarlan e McKenney (1992) defendem um foco contingencial no planejamento de TI e definem pressões que são exercidas e que exigem a necessidade deste planejamento:

- pressões externas (à organização):
  - mudanças rápidas de tecnologia;
  - falta de pessoal;
  - falta de outros recursos corporativos;
  - tendência a projeto de banco de dados e sistemas integrados;
  - validação do plano corporativo pela TI;
  
- pressões internas (ao processo de TI):
  - fase 1: identificação e investimento em tecnologia;
  - fase 2: aprendizagem e adaptação tecnológica;
  - fase 3: racionalização e controle gerencial;
  - fase 4: maturidade e ampla transferência tecnológica.

Pyburn (1983) aponta que há consenso quanto à consideração de que o planejamento estratégico de sistemas de informação tem-se tornado crítico para o sucesso do esforço geral na área. Em sua visão, as causas da resistência dos próprios executivos da área em relação ao esforço de planejamento são:

- o planejamento é caro, consome tempo e requer a atenção e o compromisso das pessoas que são essenciais para a solução dos problemas atuais; e
- o planejamento é arriscado e é um processo que lida com compromissos públicos e, muitas vezes, escritos.

King (1978) definiu que o processo de planejamento estratégico de Sistemas de Informações Gerenciais (SIG) envolve a identificação e o estabelecimento de um conjunto de estratégias organizacionais, ou seja, um conjunto de informações que delinea a missão, os objetivos, as estratégias e outros atributos estratégicos da organização. Este conjunto pode ser transformado em outro conjunto de informações, um conjunto de estratégias de SIG, que delinea os objetivos, as restrições e as estratégias de projeto de sistemas.

Earl (1987) argumenta que as metodologias de formulação de estratégias de TI funcionam melhor em empresas com estratégias de negócio disponíveis ou onde a análise estratégica já tenha sido feita.

Embora os conceitos apresentados tenham origem na área de empresas privadas, é imediata a transposição para a área pública onde é fundamental a necessidade de planejamento para a consecução de seus objetivos finalísticos.

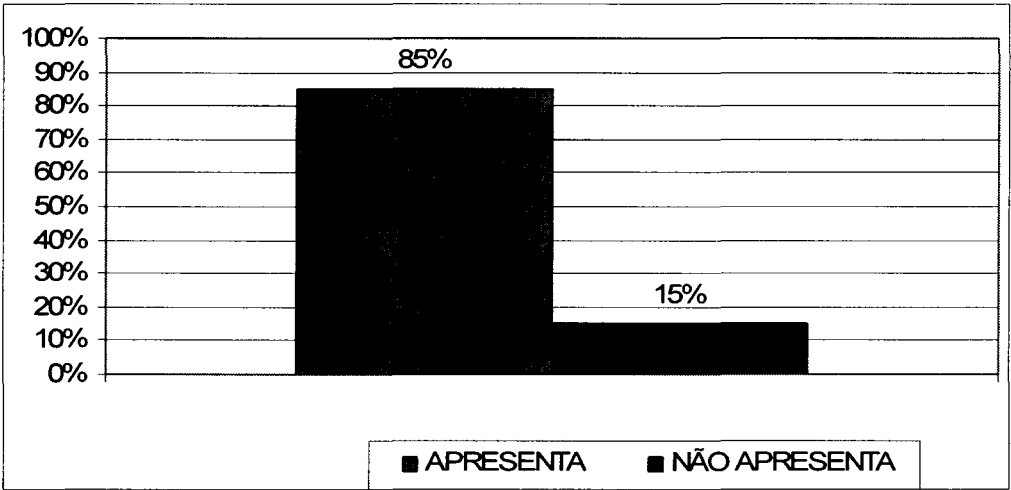
Muitos gerentes não assumem suas responsabilidades no planejamento da área de informática, delegando-as a suas equipes técnicas. Esta situação leva a planejá-la de forma não aderente aos objetivos e estratégias organizacionais. Uma abordagem semelhante defende a necessidade de apoio da alta hierarquia à área de informática, inclusive em seu planejamento, pelo alto investimento que ela representa, sua necessidade de visão de negócio, seu uso estratégico potencial e as mudanças organizacionais que representa, sob pena de fracassar em seus objetivos.

## **2) Implementação de políticas de segurança da informação falhas ou inexistentes**

A maioria dos municípios estudados não detém mecanismos de segurança da informação implementados de forma apropriada, com uma taxa de 85%, consoante apontado no gráfico. Este fato é preocupante em vista das inúmeras ameaças digitais existentes atualmente.



Gráfico 2 – Políticas de segurança da informação falhas ou inexistentes



Fonte: Elaboração Própria

A segurança da informação é tão importante que a literatura especializada a considera como uma área específica da Tecnologia da Informação, havendo inúmeras normas e instruções que orientam a sua aplicação.

Como já apresentado neste trabalho, o TCE-RJ utiliza-se principalmente da norma NBR ISSO/IEC 17799:2005 em auditorias de TI para verificar aspectos de segurança da informação. Esta norma ressalta que com o incrível aumento da interconectividade, a informação está agora exposta a um crescente número e a uma grande variedade de ameaças e vulnerabilidades. As organizações, seus sistemas de informação e redes de computadores são expostos a diversos tipos de ameaças à segurança da informação, incluindo fraudes eletrônicas, espionagem, sabotagem, vandalismo, incêndio e inundação. Danos causados por código malicioso, *hackers* e ataques de negação de serviço (*denial of service*) estão se tornando cada vez mais comuns, mais ambiciosos e incrivelmente mais sofisticados.

A segurança da informação é importante para os negócios, tanto do setor público como do setor privado, e para proteger as infra-estruturas críticas. Em ambos os setores, a função da segurança da informação é viabilizar os negócios como, por exemplo, o governo eletrônico (*e-gov*) ou o comércio eletrônico (*e-commerce*), e evitar ou reduzir os riscos relevantes. A interconexão de redes

públicas e privadas e o compartilhamento de recursos de informação aumentam a dificuldade de se controlar o acesso. A tendência da computação distribuída reduz a eficácia da implementação de um controle de acesso centralizado.

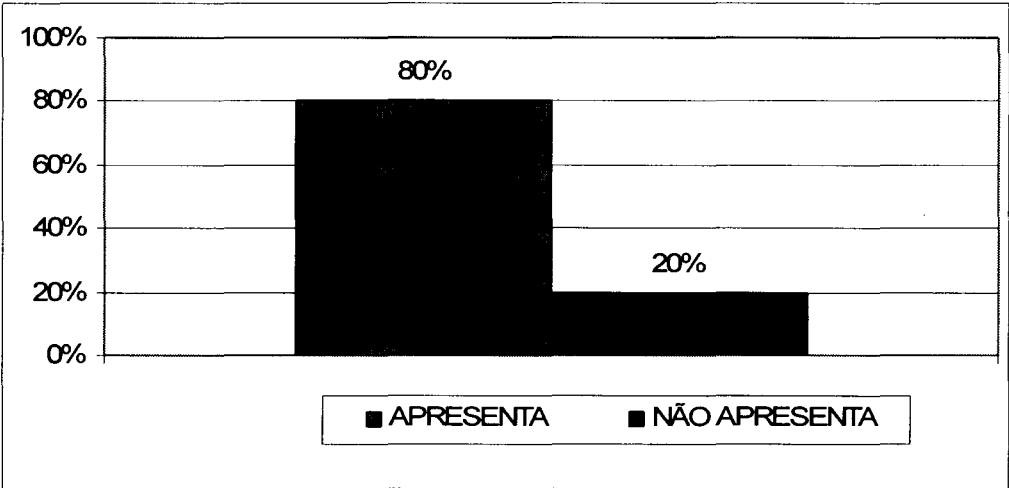
A segurança da informação é obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de *software* e *hardware*. Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados onde necessário, para garantir que os objetivos do negócio e de segurança da organização sejam atendidos.

Uma das fragilidades mais relevantes relativas à segurança da informação verificadas nas inspeções municipais é a ausência de um *firewall*, dispositivo da rede de computadores que tem por objetivo aplicar uma política de segurança a um determinado ponto de controle da rede. Sua função consiste em regular o tráfego de dados entre redes distintas e impedir a transmissão e/ou recepção de acessos nocivos ou não autorizados de uma rede para outra. No caso das administrações municipais verificou-se que sua rede interna está sujeita a ataques oriundos da rede mundial de computadores Internet.

### **3) Procedimentos de contingência falhos**

Procedimentos de contingência são as medidas operacionais estabelecidas e documentadas para serem seguidas em caso de ocorrência de algum desastre significativo que torne os recursos de informática indisponíveis. Também neste quesito a maioria dos municípios analisados apresenta elevado índice de impropriedades, com 80 % de procedimentos falhos, conforme ressaltado no gráfico.

Gráfico 3 – Procedimentos de contingência falhos



Fonte: Elaboração Própria

Os procedimentos de contingência mais falhos referem-se a *backups* realizados de forma incompleta ou sem a devida regularidade. Os *backups* são as atividades de salvaguarda dos dados armazenados nos computadores em fitas magnéticas ou discos óticos como CD ou DVD, para posterior recuperação em caso de falha dos equipamentos ou sinistros. A realização de *backups* incompletos ou não regulares faz com que seja alta a probabilidade de perda de informações críticas em caso de ocorrência de algum sinistro, como um incêndio.

Em geral, não há qualquer procedimento automatizado para a geração de *backups*, o que asseguraria a regularidade da execução das cópias. Os procedimentos de backup existentes também não são documentados e não há testes regulares de restauração das cópias armazenadas.

Outro problema encontrado com certa frequência refere-se ao não armazenamento das cópias de *backup* em instalações remotas, distantes da sede da administração municipal.

A norma NBR ISO/IEC 17799:2005 trata de aspectos relativos a cópias de segurança das informações em seu item 10.5.1.

#### **4) Procedimentos de cadastramento de usuários na rede de computadores e nos sistemas de informação realizados sem formalidade**

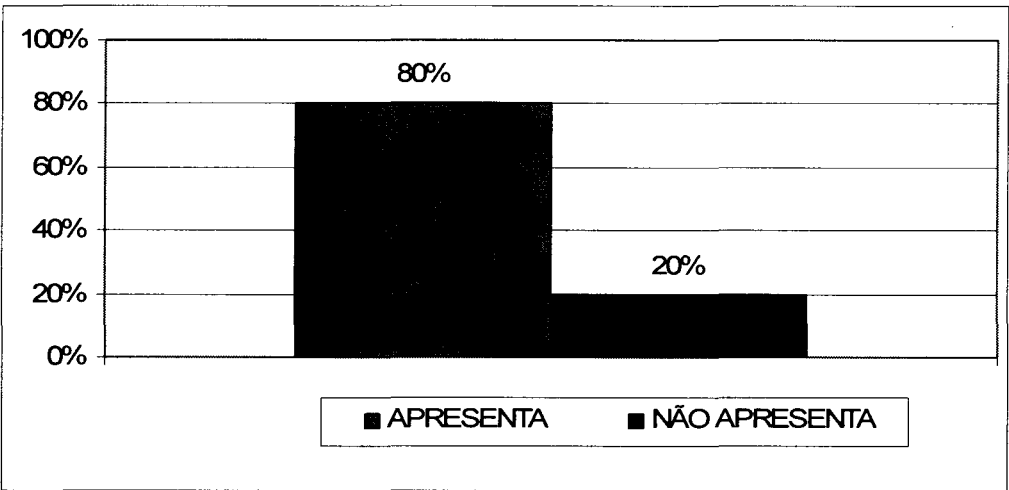
O cadastramento de usuários tanto na rede de computadores como nos sistemas de informação deve ser realizado através de um formulário padrão, que contenha a assinatura do usuário tomando ciência de que lhe foi atribuída uma chave de acesso, bem como as responsabilidades advindas de seu mau uso e as possíveis sanções cabíveis neste caso.

As solicitações de criação de novos usuários também devem ser formalizadas, por meio de um formulário padrão de solicitação, contendo o motivo da criação da conta, o perfil de acesso do novo usuário e a assinatura do superior responsável pela solicitação. O perfil de acesso consiste na descrição dos direitos de acesso do usuário aos diretórios do computador servidor, no caso da rede de computadores, ou a descrição dos direitos de acesso às funções do sistema aplicativo específico.

O formulário de solicitação deve conter inclusive as alterações que porventura venham a ser efetuadas no perfil do usuário, de forma a refletir com fidedignidade os direitos de acesso do usuário e permitir verificar se os direitos concedidos correspondem às suas atribuições administrativas. Os formulários de solicitação de cadastramento e de cadastramento podem ser os mesmos, sendo pacífico o entendimento de que deve haver um procedimento formal de cadastro com as características citadas.

É elevado o índice de municípios em que o cadastramento de usuários é realizado sem qualquer formalização, cerca de 80%, consoante apontado no gráfico. Geralmente o cadastramento é realizado por meio de solicitações verbais ou pelo envio de *e-mail* do superior para o técnico de informática responsável pela administração dos sistemas.

**Gráfico 4 – Procedimentos de cadastramento de usuários na rede de computadores e nos sistemas de informação realizados sem formalidade**



**Fonte: Elaboração Própria**

A norma NBR ISO/IEC 17799:2005 aborda no tópico 11.2 aspectos relacionados a controle de direitos de acesso a sistemas de informação e serviços, afirmando que convém que exista um procedimento formal de registro e cancelamento de usuário para garantir e revogar acessos.

Uma consequência direta da impropriedade verificada é a dificuldade ou até mesmo a impossibilidade de responsabilização de um usuário em caso de fraudes ou erros, intencionais ou não, ocorridos no uso dos ambientes de informação.

A ausência de um procedimento formal de registro faz com que funcionários com funções semelhantes recebam direitos de acesso diferentes, ou que funcionários recebam privilégios de acesso superiores à função desempenhada.

## **5) Ausência de política de senha forte na rede de computadores e nos sistemas de informação**

Uma política de senha deve ser composta dos seguintes itens, com o objetivo de assegurar um nível de segurança de acesso satisfatório:

- Senhas de, no mínimo, 06 caracteres;
- Não reutilização das últimas 05 senhas;
- A obrigatoriedade da combinação de caracteres alfabéticos, numéricos e caracteres especiais na composição da senha;
- Usuários que não utilizem o sistema por um período pré-determinado de dias, devem ter suas senhas automaticamente desativadas para evitar possível mau uso;
- travamento da conta de usuário após três tentativas de *logon* sem sucesso.

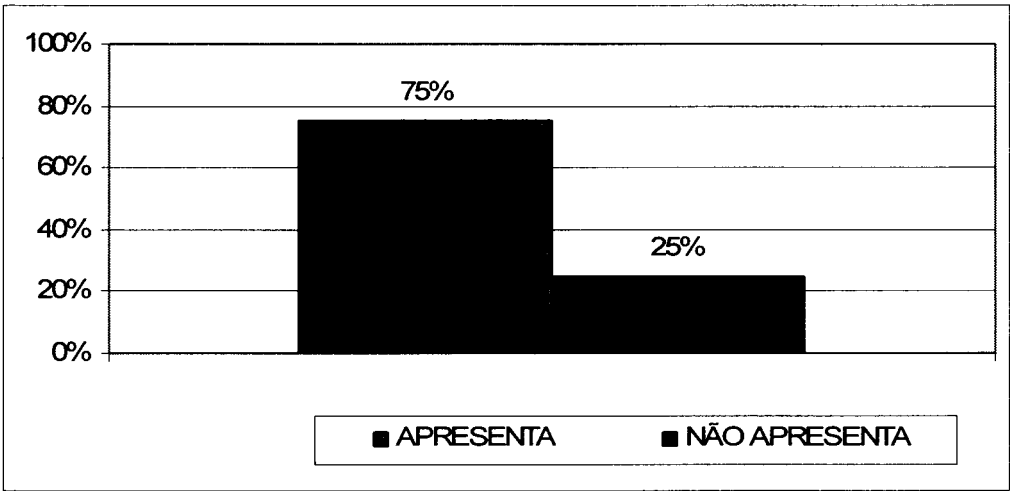
A política visa assegurar que a senha escolhida seja de difícil detecção por outros usuários ou por tentativas de invasão via ataque por dicionário ou força bruta. A Norma NBR ISO/IEC 17799:2005 aborda em seu item 11.3.1 as boas práticas segurança da informação na seleção e uso de senhas, notadamente na alínea d:

d) selecionar senhas de qualidade com um tamanho mínimo que sejam:

- 1) fáceis de lembrar;
- 2) não baseadas em nada que alguém facilmente possa adivinhar ou obter usando informações relativas à pessoa, por exemplo, nomes, números de telefone e datas de aniversário;
- 3) não vulneráveis a ataque de dicionário (por exemplo, não consistir em palavras incluídas no dicionário);
- 4) isentas de caracteres idênticos consecutivos, todos numéricos ou todos alfabéticos sucessivos;

A impropriedade em tela é de alta incidência, ocorrendo em 75% dos municípios analisados, sendo mais comum em aplicações desenvolvidas para automatizar uma atividade específica da administração municipal como, por exemplo, um Sistema de Contabilidade ou Sistema de Controle da Arrecadação. O gráfico a seguir destaca o elevado índice de municípios com esta deficiência.

**Gráfico 5 – Ausência de política de senha forte na rede de computadores e nos sistemas de informação**



**Fonte: Elaboração Própria**

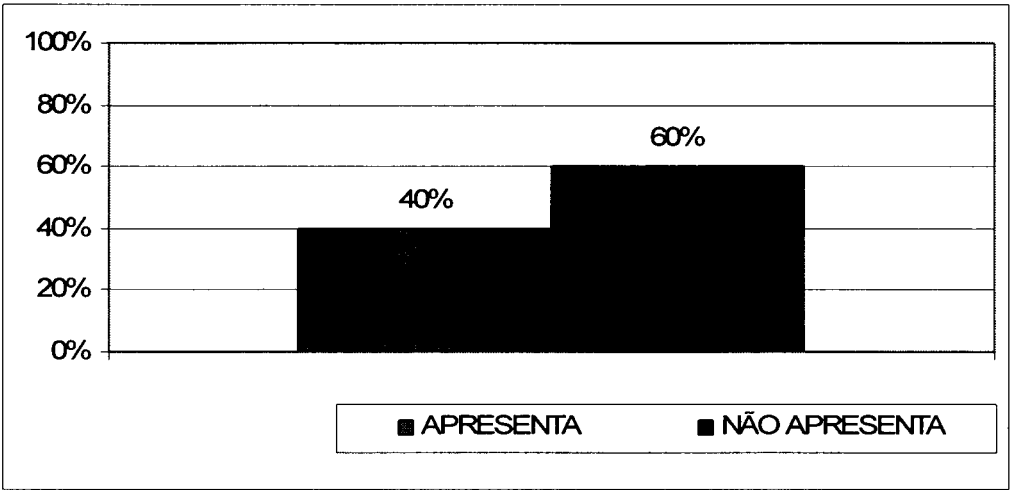
Sistemas operacionais de computadores servidores de uma rede como, por exemplo, Windows 2000 e Netware 4.12, são desenvolvidos por grandes empresas do ramo de informática e já possuem mecanismos de autenticação seguros implementados. Foi constatado, entretanto, que geralmente o profissional de informática da Prefeitura não realiza a ativação de tais funcionalidades.

Outras deficiências comuns verificadas na pesquisa foi a não ativação ou a ausência de mecanismos que obriguem o usuário a realizar a modificação da senha no primeiro acesso a uma aplicação, fazendo com que ele fique com uma senha padrão, de conhecimento do operador do sistema.

**6) Ausência de campo específico nos sistemas de informação para registro de número do processo administrativo em operações críticas**

O presente estudo procurou verificar a incidência desta impropriedade nos sistemas aplicativos utilizados pelas administrações municipais, tendo verificado que menos da metade dos municípios apresentam esta deficiência, 40% do total, conforme mostra o gráfico a seguir.

**Gráfico 6 – Ausência de campo específico nos sistemas de informação para registro de número do processo administrativo em operações críticas**



**Fonte: Elaboração Própria**

Operações críticas são muito comuns em sistemas de informação. Um sistema de Folha de Pagamento, por exemplo, deve exercer estrito controle sobre operações de alteração ou concessão de rubricas de pagamento, que resultam em aumento do salário do empregado. Sistemas de Controle da Arrecadação devem controlar operações que alterem o valor de um imposto cobrado do contribuinte, como alterações nas características de um imóvel que resultem em diminuição do valor cobrado de Imposto Predial e Territorial Urbano (IPTU). Nestes casos a operação deve ter suporte de um processo administrativo, em que o pedido é analisado e ganha pareceres do controle interno, procuradoria e do setor competente, para só então ser aprovado. É necessário, portanto, que o



sistema possua um campo específico para registrar o processo administrativo que dá suporte à operação.

A grande maioria dos municípios estudados utiliza-se de sistemas de informação desenvolvidos por empresas contratadas, sendo raros os municípios com uma estrutura de desenvolvimento de sistemas própria. Com isso, atividades essenciais em uma administração municipal como Contabilidade, Controle da Arrecadação e Folha de Pagamento são informatizadas por programas de empresas com experiência no mercado e que já possuem em seus aplicativos a funcionalidade de exigir o número de processo administrativo em operações críticas. O crescimento das empresas de desenvolvimento de *software* faz com que aumente seus conhecimentos do negócio e, conseqüentemente, haja melhoria dos produtos desenvolvidos. Existe uma tendência, portanto, de diminuição da incidência da impropriedade em tela, já que os sistemas de informação incorporam funcionalidades exigidas pelo contratante, a administração municipal.

## **7) Arquivos de *log* ausentes ou com registro falho nos sistemas de informação**

O arquivo de *log* em sistemas de informação consiste em um arquivo no qual são registradas todas as alterações realizadas no sistema, de forma a permitir a identificação dos campos alterados, o autor da alteração e quando ela foi realizada.

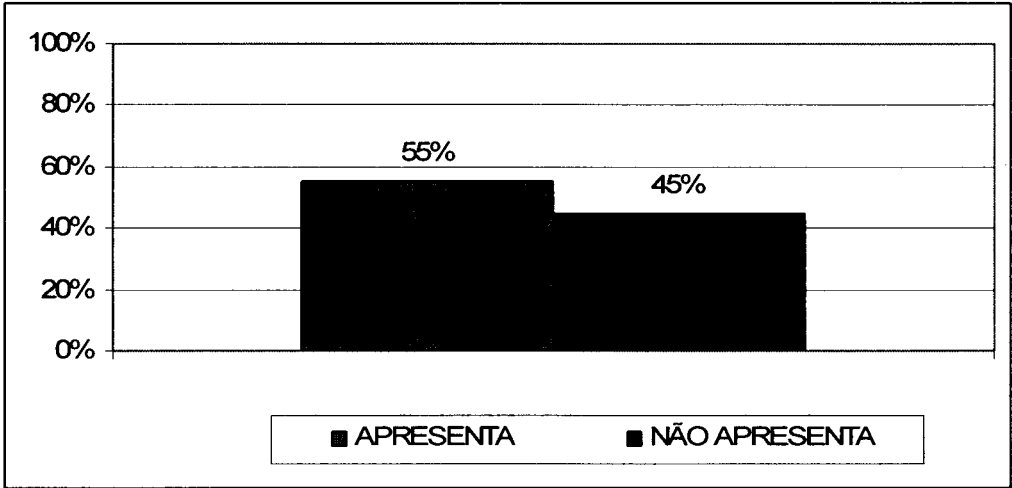
Um bom arquivo de *log* de um sistema de informação deve possuir todos os campos necessários a uma qualificação detalhada de uma alteração, incluindo a tabela alterada, identificação do campo alterado, nome do usuário que realizou a alteração, data e hora em que ela foi efetuada, o conteúdo anterior de cada campo alterado e o novo conteúdo.

O arquivo de *log* possibilita ao usuário gestor do aplicativo realizar um rastreamento das alterações realizadas, com o intuito de apurar responsabilidades em caso de fraudes ou erros ocorridos na utilização do

sistema. A própria existência de *log* em um sistema aplicativo é um fator altamente inibidor de tentativas de ações fraudulentas.

Um pouco mais da metade dos municípios estudados apresentavam a irregularidade, 55% do total, como mostra o gráfico a seguir.

**Gráfico 7 – Arquivos de log ausentes ou com registro falho nos sistemas de informação**



**Fonte: Elaboração Própria**

Embora exista uma tendência de aumento de sistemas aplicativos com registro de operações em arquivos de *log*, o estudo observou que em muitos casos o registro era incompleto, faltando informações importantes como o valor anterior do campo alterado e identificação do usuário autor da alteração, o que impossibilitava a sua utilização.

Em outros casos, o sistema aplicativo não possuía um módulo de consulta ao arquivo de *log*, impossibilitando o usuário gestor da administração municipal realizar estudos para identificar tentativas de fraude no sistema. Este fato faz com que o arquivo de *log* não seja utilizado na prática e, portanto, foi considerado uma impropriedade.

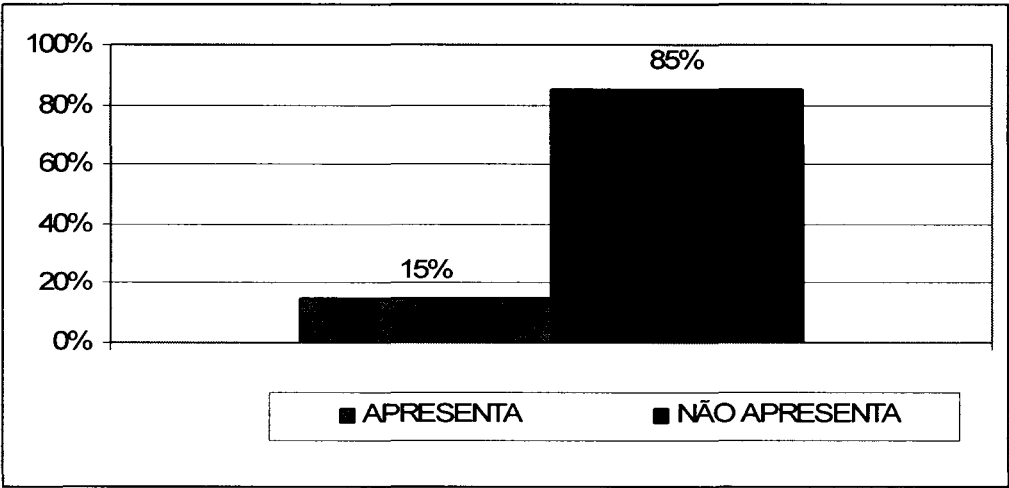
**8) Sistema de informação em desacordo com legislação específica vigente**

As inspeções operacionais em TI realizadas pelo TCE-RJ procuram verificar também aspectos de aderência do sistema aplicativo à legislação específica da área, como leis, decretos e portarias emanadas pelas três esferas do poder, municipal, estadual e federal, e que influenciam diretamente na forma de execução e nos relatórios emitidos pelos sistemas.

Sistemas de controle da arrecadação, por exemplo, devem realizar o cálculo dos impostos e taxas segundo alíquotas, definidas por Lei Municipal ou decretos executivos sancionados pelo poder legislativo.

O estudo verificou que é baixa a incidência de sistemas aplicativos em desacordo com a legislação, apenas 15 %, conforme gráfico a seguir, o que demonstra a preocupação da administração municipal com aspectos legais e formais de funcionamento dos sistemas. Este fato deve-se provavelmente à forma de atuação do Tribunal de Contas, que realiza tradicionalmente um controle de natureza formal de verificação da regularidade da execução dos gastos públicos, da legalidade dos atos administrativos e da fidedignidade dos demonstrativos financeiros.

**Gráfico 8 – Sistema de informação em desacordo com legislação específica vigente**



**Fonte: Elaboração Própria**

A impropriedade em tela constitui uma grave deficiência do sistema aplicativo, sujeitando a administração municipal a ações indenizatórias por parte dos contribuintes em caso de flagrante desobediência à norma legal, o que resultaria em graves prejuízos ao erário municipal.

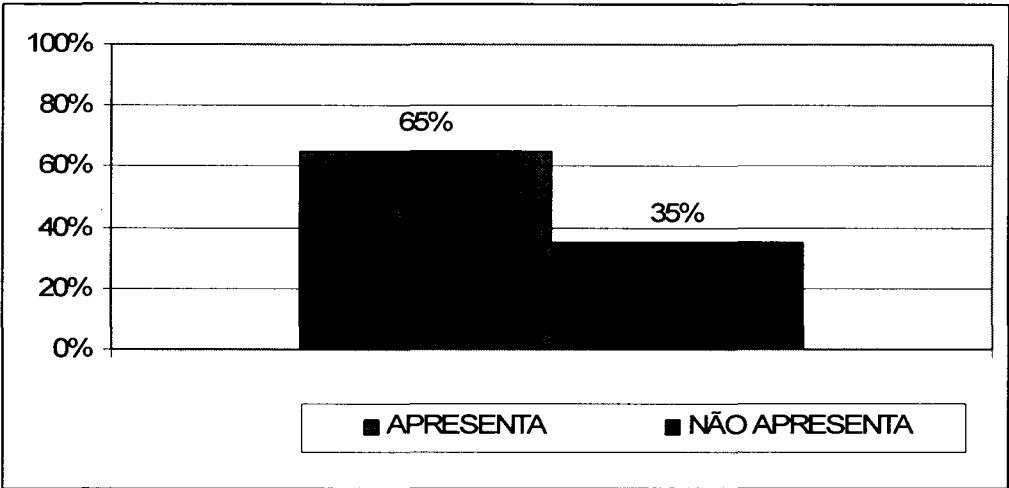
#### **9) Divergência entre os valores registrados no sistema de controle da arrecadação e no sistema de contabilidade**

A impropriedade consiste na ausência de registro no sistema de contabilidade de valores efetivamente arrecadados pelo sistema de controle da arrecadação, oriundos da cobrança de tributos de responsabilidade da própria administração municipal.

O sistema de contabilidade é o principal instrumento de controle da administração municipal, por meio dele é que são extraídos os principais relatórios exigidos pela Lei Federal nº 4.320/64, que rege as normas gerais de direito financeiro para elaboração e controle dos orçamentos e balanços da administração pública. A Constituição Federal de 1988 e emendas constitucionais posteriores estabelecem percentuais mínimos de vinculação de receitas municipais com gastos em saúde e educação. Com isso, uma divergência de registro de valores de arrecadação entre os sistemas de controle da arrecadação e contabilidade pode resultar em aplicação de recursos abaixo do mínimo legal em duas áreas fundamentais de assistência básica ao cidadão.

Os dados do estudo revelam que 65% dos municípios apresentam a irregularidade em tela, consoante gráfico abaixo, índice considerado alto devido aos riscos para a administração municipal.

**Gráfico 9 – Divergência entre os valores registrados no sistema de controle da arrecadação e no sistema de contabilidade**



**Fonte: Elaboração Própria**

A divergência entre os dois sistemas pode representar também uma grave ilegalidade sujeita às sanções da Lei, tendo em vista que o não registro de receitas do sistema de controle da arrecadação no sistema de contabilidade pode ser uma tentativa de mascarar o desvio da arrecadação própria dos cofres municipais. Este tipo de conduta sujeita o administrador público a sanções penais, visto que pode ser caracterizada como ato de improbidade previsto na Lei nº 8.429, de 2 de junho de 1992 – Lei de Improbidade Administrativa. Esse diploma regulamentou o art. 37, § 4º, da Constituição da República, disciplinando quais os atos que seriam classificados como ímprobos, quais as sanções aplicáveis e qual o procedimento para aplicá-las.

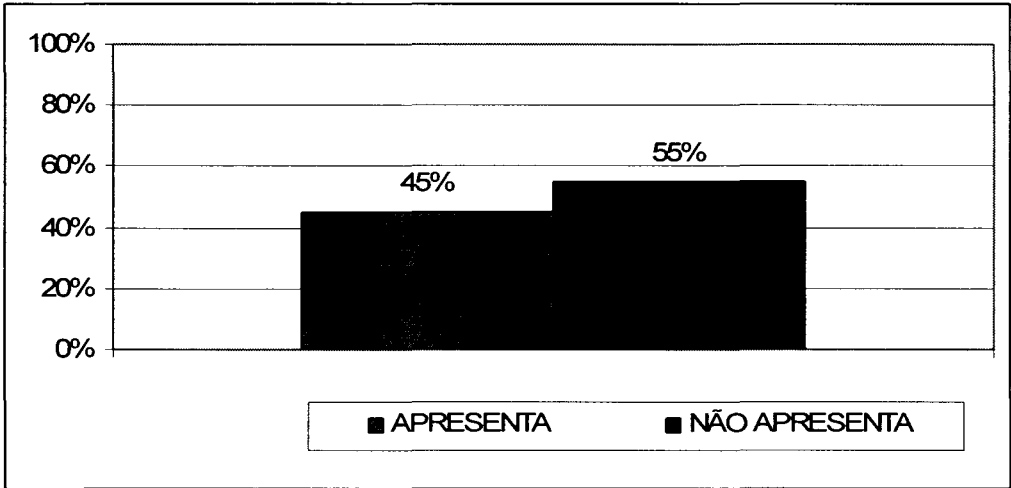
A conduta em questão pode ser caracterizada como sendo um dos três tipos de condutas que podem configurar ato de improbidade administrativa: atos que importam enriquecimento ilícito (art. 9º), atos que causam lesão ao erário (art. 10) e atos que atentam contra os princípios da administração pública (art. 11).

**10) Impropriedades no instrumento contratual que ferem a legislação vigente, notadamente a Lei Federal nº 8.666/93**

O TCE-RJ vem realizando também análise dos contratos firmados pela administração municipal na área de informática em suas auditorias operacionais em TI. Este tipo de atuação aproxima o Tribunal do modelo canadense de auditoria, conhecido como auditoria integrada ou de amplo escopo, em que são realizadas verificações tanto de aspectos operacionais quanto legais (CCAF, 1995).

O presente estudo constatou que quase a metade dos municípios, 45%, apresenta problemas relativos à contratação, mesmo sendo este um dos aspectos verificados pelo TCE-RJ com mais regularidade em suas inspeções e sujeito inclusive a análise prévia. O gráfico a seguir ressalta a distribuição desta irregularidade pelos municípios.

**Gráfico 10 – Impropriedades no instrumento contratual que ferem a legislação vigente, notadamente a Lei Federal nº 8.666/93**



**Fonte: Elaboração Própria**

Os municípios são obrigados, por força de deliberações expedidas pelo Tribunal, a enviar previamente para análise diversos tipos de atos jurídicos de licitações e contratos. Apesar desta obrigatoriedade, persiste a ocorrência de

irregularidades no objeto contratual, podendo ser considerado elevado o índice de 45%.

As análises de contratos realizadas pelas auditorias de TI limitam-se a verificar aspectos da legislação que se aplicam especificamente à contratação de bens e serviços de informática. Dentre as irregularidades mais comuns destacam-se o descumprimento ao prazo máximo de 48 meses de vigência contratual no aluguel de equipamentos e utilização de programas de informática, não haver designação de funcionário da administração municipal para o acompanhamento da execução do contrato, subcontratação de empresas para prestação do objeto sem previsão no instrumento contratual e contratação por dispensa ou inexigibilidade de objetos não singulares, ou seja, que podem ser fornecidos por diversas empresas do mercado e, portanto, há obrigação de se realizar concorrência.

As irregularidades verificadas sujeitam o administrador público a sanções impostas pelo TCE-RJ, como o pagamento de multas, e pelo Ministério Público, que podem resultar em crime de responsabilidade por descumprimento da Lei.

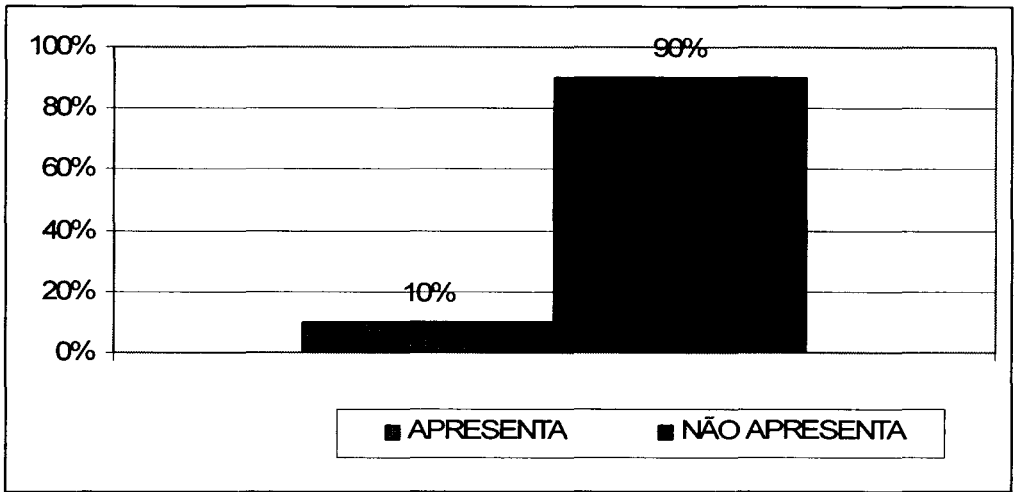
### **11) Não execução ou execução parcial do objeto contratado**

A auditoria operacional em TI realizada pelo TCE-RJ nos municípios busca verificar também aspectos técnicos relativos à contratação de bens e serviços de informática, notadamente a adequação dos serviços prestados ao objeto definido no contrato.

Este tipo de análise somente pode ser realizado por meio de inspeções *in loco*, possibilitando ao auditor comparar a situação encontrada na realidade com aquela definida no texto contratual.

Como mostra o gráfico a seguir é baixa a incidência desta impropriedade nos municípios, com um índice de apenas 10%.

**Gráfico 11 – Não execução ou execução parcial do objeto contratado**



**Fonte: Elaboração Própria**

A baixa ocorrência de problemas relativos à execução contratual deve-se provavelmente às cobranças realizadas pelos próprios técnicos municipais às empresas prestadoras dos serviços, tendo em vista a importância dos sistemas de informação contratados para a consecução das atividades básicas da administração. Enquadram-se neste caso os sistemas de folha de pagamento, contabilidade e controle da arrecadação, fundamentais para a gestão da máquina pública.

Quanto ao fornecimento de bens de informática é mais fácil a comparação do objeto definido no contrato com os produtos efetivamente fornecidos, tendo sido encontradas diferenças de especificação técnica entre o material entregue e aquele especificado. Como exemplo, pode-se citar computadores entregues com menos memória, com processadores de menor capacidade de processamento, ou sem placas de vídeo dedicadas, entre outros problemas.



## 8. CONCLUSÃO

---

O crescimento da influência do paradigma gerencial na administração pública contemporânea vem exigindo mecanismos de aferição dos investimentos públicos capazes de traduzir, com maior clareza e objetividade, a retórica política dos gestores públicos. Assim, ferramentas como a auditoria operacional, que busca precipuamente avaliar o nível de excelência das organizações públicas a partir de aspectos como eficácia, eficiência, economicidade e efetividade, surgem para auxiliar os órgãos de controle governamental, em especial os Tribunais de Contas, no atendimento das novas demandas sociais.

O estudo realizado proporcionou uma contribuição positiva para o processo de aprendizagem quanto à auditoria de sistemas, uma vez que ao traçar um perfil das principais deficiências associadas à utilização de informática pelas administrações municipais, possibilitou mostrar a efetividade desta modalidade de auditoria na detecção de falhas e na prescrição de melhorias.

A dinâmica dos trabalhos de auditoria na área de sistemas de informação não permitia, até hoje, uma avaliação mais detalhada dos resultados alcançados por este tipo de auditoria, de forma a contribuir para a melhoria da gestão pública.

A síntese dos principais resultados obtidos no estudo aponta para elevada incidência de certas impropriedades, indicando que a administração pública municipal ainda não alcançou o nível de maturidade que possa qualificá-la como gerencial.

Existem deficiências em sua forma de administração que dificultam sobremaneira a adoção de práticas gerenciais, com destaque para o nível incipiente de planejamento estratégico na área de informática pelos municípios. A falta de planejamento na área pode ocasionar sérios problemas para a gestão pública em médio prazo, com a diminuição de sua capacidade de implementar políticas públicas que sejam econômicas e eficazes.

A informação é, hoje em dia, um dos bens mais preciosos de uma organização e requer mecanismos de planejamento e controle cada vez mais

sofisticados. O processo de planejamento estratégico de sistemas de informações envolve a identificação e o estabelecimento de um conjunto de estratégias organizacionais, como missão e objetivos, sendo fundamental a adoção da governança na área de TI.

A administração pública gerencial caracteriza-se por ser orientada para o cidadão e para a obtenção de resultados. Nesse sentido, a governança de TI é fundamental para garantir que a informática suporte e maximize os objetivos e estratégias de negócio da administração municipal, contribuindo para a melhoria da qualidade dos serviços entregues ao cidadão.

O crescimento de uma sociedade que passa a organizar seus processos de trabalho e relacionamentos com base em estruturas e sistemas informatizados faz com que as organizações que exercem o controle administrativo, como o Tribunal de Contas, tenham de repensar sua forma de atuação.

Associada a essa necessidade, temos a própria evolução das condições tecnológicas que dão novas possibilidades para exercer atividades relativas ao controle administrativo que, em última análise, possibilitam um aprofundamento dos estudos possíveis de serem efetuados e abrem dimensões mais interessantes de serem abordadas como a eficiência, eficácia e efetividade das ações administrativas.

O TCE-RJ ao realizar auditorias de tecnologia da informação está ampliando sua forma de atuação, indo ao encontro das idéias e conceitos difundidos pela Administração Pública Gerencial e adequando-se às exigências da chamada era da informação.

As inspeções de TI ao verificar aspectos relativos à confiabilidade, disponibilidade, confidencialidade e integridade das informações armazenadas nos sistemas informatizados e que trafegam na rede de computadores, está nada mais do que ampliando as dimensões de análise efetuadas pelo Tribunal de Contas, caracterizando-se como uma nova forma de auditoria, conhecida como auditoria operacional ou de desempenho.

O estudo logrou êxito ao revelar achados de auditoria resultantes dessa nova forma de análise, como problemas comuns de ordem prática relativos à área de segurança da informação, que demonstram a pouca importância dispensada pela gerência de setores-chaves da administração municipal em relação a riscos de fraude, sabotagem, roubo e sinistros a que os sistemas de informação e redes de computadores estão expostos.

Os problemas de ordem operacional evidenciam também deficiências relativas à qualificação profissional dos funcionários de nível intermediário, responsáveis pela implementação dos controles lógicos e físicos, como políticas de segurança da informação, procedimentos de contingência, cadastramento de usuários e configuração das políticas de senha na rede de computadores e nos sistemas de informação.

Os resultados do presente trabalho mostram, portanto, a necessidade de treinamento dos profissionais de nível intermediário e de sensibilização da gerência de áreas estratégicas para a importância da questão da segurança das informações. Uma possível contribuição do TCE-RJ seria a elaboração e implementação de um curso de boas práticas no uso e manutenção de ambientes informatizados direcionado não só aos profissionais de nível intermediário, como também aos responsáveis de nível de gestão administrativa.

O TCE-RJ, com a experiência adquirida ao longo dos últimos oito anos em inspeções de caráter operacional no ambiente de informática das administrações municipais e pelo constante aprimoramento e atualização de seu corpo técnico, possui a capacidade e o dever de transmitir os ensinamentos necessários a seus jurisdicionados, em especial os municípios, pois estes possuem menos recursos e uma estrutura mais precária do ponto de vista material e de técnicos especializados.

Como órgão de controle externo, o TCE-RJ vem ampliando sua forma de atuação através da implantação de uma Escola de Contas e Gestão. Essa Escola tem como missão promover o ensino e a pesquisa na área de gestão pública, voltados para o desenvolvimento e a difusão de conhecimento, modelos e

metodologias comprometidas com a inovação, a transparência, a responsabilidade e a melhoria do desempenho e controle governamental.

A análise crítica presente no presente estudo aponta para a necessidade de criação pela Escola de Contas e Gestão do TCE-RJ de um curso nos moldes expostos, a ser ministrado pelos técnicos responsáveis pelas auditorias de TI nos municípios, permitindo também o intercâmbio de experiências e o aprimoramento da própria atividade de auditoria.

A pesquisa revelou também a ocorrência de falhas operacionais como a ausência de procedimento formal de cadastramento de usuários tanto na rede de computadores como nos sistemas de informação, assim como a ausência de arquivos de *log* ou com registro falho nos sistemas aplicativos, que possibilitam, em última instância, a preservação de mecanismos de impunibilidade. Um dos fatores que contribuem para este tipo de problemas de rotinas e procedimentos é a falta de continuidade da administração, sujeita a mudanças em seus quadros resultantes da alternância normal de poder.

Os critérios utilizados em auditoria com foco em tecnologia da informação possibilitam também a verificação da conformidade do sistema auditado com as regras do negócio, estabelecidas em leis, decretos e portarias. Apesar do estudo revelar uma baixa incidência deste tipo de impropriedade nos municípios analisados, é inegável a importância deste tipo de análise para o aprimoramento do controle exercido pelo Tribunal de Contas. Nessa categoria estão, por exemplo, os critérios para cálculo dos salários dos servidores no sistema de recursos humanos, a forma de cálculo dos impostos e taxas no sistema de controle da arrecadação, assim por diante.

Os tipos de deficiências encontradas pelas auditorias de TI, notadamente a não conformidade do sistema auditado com as regras do negócio, evidenciam a fragilidade da área de controle interno da administração pública municipal. Como o controle interno visa, principalmente, evitar a prática de fraudes, erros, desperdícios e abusos, é natural que ele seja exercido em caráter prévio, antes de concluído o ato administrativo.

Os relatórios de auditoria em TI têm sempre procurado invocar a responsabilidade do controle interno, fazendo constar em suas recomendações a efetiva participação deste importante setor administrativo na resolução das impropriedades e irregularidades encontradas. Por outro lado, a própria atividade do TCE-RJ serve de amparo para o controle interno, apoiando suas ações na defesa do patrimônio público.

A quantidade e diversidade de impropriedades na área de informática sugerem a necessidade do TCE-RJ em aumentar a fiscalização no setor, necessidade que esbarra no limitado quadro de técnicos especializados em auditoria de TI, atualmente composto por apenas três analistas.

Observa-se também a necessidade de se realizar inspeções de retorno a muitos municípios auditados, com o intuito de verificar se as recomendações efetuadas foram de fato implementadas, já que muitas são de caráter operacional e exigem a observação *in loco* para verificar seu cumprimento.

A auditoria de TI necessita também de maior integração com outras áreas de fiscalização do Tribunal em que a presença de sistemas informatizados é cada vez maior, com destaque para as áreas de pessoal, educação e saúde. Essas são áreas em que a informatização vem produzindo novos modelos de estruturas e novos processos de organização, todos com o objetivo de simplificar e agilizar os fluxos de informação.

Os resultados da pesquisa revelam também a necessidade de legislação específica na área de informática, como instruções normativas, de forma a dar suporte às recomendações resultantes dos trabalhos de auditoria realizados. Hoje, as auditorias de TI baseiam-se fortemente em normas técnicas e boas práticas da área de informática, prevalecendo, em muitos casos, a conscientização do auditado para a necessidade de cumprimento das recomendações para o aumento da segurança e melhoria de funcionamento do ambiente de informática.

A presente pesquisa evidencia, por fim, a importância da auditoria operacional de Tecnologia da Informação como forma de ampliação e

fortalecimento da atividade de controle externo exercida pelo Tribunal de Contas do Estado do Rio de Janeiro.

## 9. REFERÊNCIAS BIBLIOGRÁFICAS

---

ABNT. NBR ISO/IEC 17799:2005: **Tecnologia da Informação — Técnicas de segurança — Código de Prática para a gestão da segurança da informação**. Rio de Janeiro, Associação Brasileira de Normas Técnicas, 2005.

ABNT. NBR ISO/IEC 27001:2005: **Tecnologia da Informação — Técnicas de segurança — Sistemas de gestão de segurança da informação - Requisitos**. Associação Brasileira de Normas Técnicas.

ALBERTIN, Alberto Luiz. **Administração de Informática: funções e fatores críticos de sucesso**; colaboração de Rosa Maria de Moura. 4 ed. São Paulo: Atlas, 2002.

ALBUQUERQUE, Frederico de Freitas Tenório. **A auditoria operacional e seus desafios: um estudo a partir da experiência do Tribunal de Contas da União**. 2006, 152f. Dissertação (Mestrado Profissional em Administração) – Escola de Administração, Universidade Federal da Bahia, Salvador, 2006.

ARAÚJO, Inaldo da Paixão Santos. **Introdução à auditoria operacional**. Rio de Janeiro: Editora FGV, 2001.

BARDIN, Laurence. **Análise de Conteúdo**. Lisboa: Edições 70, 1977.

BARROS, Elizabeth Ferraz. **Auditoria de desempenho nos tribunais de contas estaduais brasileiros: uma pesquisa exploratória**. Dissertação (Mestrado). Faculdade de Economia, Administração e Contabilidade da USP. São Luís, 2000.

BARTON, R. **Global IT management**. Chichester: John Wiley & Sons, 2003.

BARZELAY, Michael. Instituições centrais de auditoria e auditoria de desempenho: uma análise comparativa das estratégias organizacionais na OCDE. **Revista do Serviço Público**, Brasília, ano 53, n. 2, p. 5-35, abr./jun. 2002.

BASTOS, Glória Maria Merola da Costa. A experiência do Tribunal de Contas da União em auditoria operacional e avaliação de programas governamentais. *In*: TCU – Tribunal de Contas da União. **O controle externo e a nova administração pública: uma visão comparativa**. Brasília: 2002.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil**. 10 ed. São Paulo: Rideel, 2004.

BRESSER PEREIRA, Luiz Carlos. **A reforma do Estado dos anos 90: lógica e mecanismos de controle**. Lua Nova. São Paulo, n.º 45, p. 49-95, 1998.

\_\_\_\_\_. A reforma gerencial do Estado de 1995. **Revista de Administração**, Rio de Janeiro: FGV, 34 (4), p.7-26, jul./ago.2000.

CAMPOS, Anna Maria, **Accountability**: quando poderemos traduzi-la para o português? **Revista de Administração Pública**. Rio de Janeiro. Vol. 24. Nº 2, fev/abr, 1990, pp. 30-50.

CARNEIRO, Roberto Antônio Fortuna. Avaliação: elemento vital e constituinte do planejamento e da gestão de resultados. **Revista Bahia análise e dados**. Salvador, v.12, n.2, p.91-100, setembro 2002.

CARVALHO FILHO, José dos Santos . **Manual de Direito Administrativo**. 14ª ed. Rio de Janeiro, 2005

CASH JR., J. I.; McFARLAN, F. W.; McKENNEY, J. L. **Corporate information systems management: the issues facing senior executives**. Homewood: Richard D.Irwin, 1992.

CCAF – Canadian Comprehensive Auditing Foundation. **Auditoria integrada: conceitos, componentes e características**. Trad. Inaldo da Paixão Santos Araújo. 1ª ed. Salvador: Tribunal de Contas do Estado da Bahia, 1995.

CRUZ, Flávio da. **Auditoria governamental**. São Paulo: Atlas, 1997.

CUNHA, Cyrino. Auditoria governamental e a auditoria operacional: uma introdução com algumas considerações. **Revista do Tribunal de Contas**, Porto Alegre, n 9, v. 6, dez.1998

DA SILVA, Roberto Carvalho. **Auditoria Operacional como instrumento de gerência no Setor Público**. Dissertação de Mestrado, São Paulo: FEA/USP, 1993.

DERLIEN, H-U . Uma comparación internacional em la evaluacion de lãs políticas públicas, **Revista do Serviço Público**, 52 (1); 105-123, 2001.

DI PIETRO, Maria Silvia Zanella. **Direito administrativo**. 13 ed. São Paulo:Atlas, 2001.

EARL, M. J. Information systems strategy formulation. In: BOLAND JR., R. J.; HIRSCHHEIM, R. A. (Org.). **Critical issues in information systems research**. New York: John Wiley, 1987.

EIN-DOR, P.; SEGEV, E. **Strategic planning for management information systems**. **Manegement Science**, v. 24, nº 15, p.1631-1641, Nov. 1978.

FARIA, C. A. .A política da avaliação de políticas públicas, **Revista Brasileira de Ciências Sociais**, 20 (59): 97-109. 2005.

FÉDER, João. Auditoria Operacional. **Revista do Tribunal de Contas do Estado de Santa Catarina**, Santa Catarina, n.4, p. 5-7, nov/dez.1988.



\_\_\_\_\_, João. Auditoria Operacional. **Revista do Tribunal de Contas de Minas Gerais**, Belo Horizonte, v.21,n.4, p. 13-53, out/dez.1996.

FERLIE, E. *et al.* **The new public management in action**. Oxford, Oxford University Press, 1996.

FERRAZ, J. A. R. *et al.* Etapas dos trabalhos. In: ENCONTRO DE AUDITORIA DE NATUREZA OPERACIONAL, 2., 2005, Recife:TCE/PE, 2005. 1 CD-ROM.

FREITAS, Carlos Alberto Sampaio. **Aprendizagem, isomorfismo e institucionalização**: o caso da atividade de auditoria operacional no Tribunal de Contas da União. 2005. Dissertação (Mestrado em Administração). Universidade de Brasília – UNB, Faculdade de Economia, Administração, Contabilidade e Ciência da Informação e Documentação – FACE. Brasília.

\_\_\_\_\_. Melhoria de Desempenho. In: OFICINA DE AUDITORIA DE NATUREZA OPERACIONAL, 1., 2004, Recife:TCE/PE, 2004. 1 CD-ROM.

FIGUEIREDO, Carlos Mauricio *et al.* **Comentários à Lei de Responsabilidade Fiscal**. 2ª ed. São Paulo: Editora Revista dos Tribunais. 2001, p.261-272.

FRANÇA, Junia Lessa; VASCONCELOS, Ana Cristina de **Manual para normalização de publicações técnico-científicas**. 7ed. Belo Horizonte: Ed. UFMG, 2004. 242p.

GASPARINI, Diógenes. *Direito Administrativo*. São Paulo, Saraiva, 1989

GENERAL ACCOUNTING OFFICE. **Normas de auditoria governamental do escritório da controladoria geral dos Estados Unidos**. Trad. Inaldo da Paixão Santos Araújo. Revisão 2003: Tribunal de Contas do Estado da Bahia, 2005 (Série Traduções – Nº. 12).

GIL, Antonio Loureiro. **Auditoria de Computadores**. 3 ed. São Paulo: Atlas, 1998.

GREINER, John M. In: BOUCKAERT, Geet na HALACHMI, Arie. **Organizational performance and measurement in the public sector**. London: quorum Books, 1996.

GREMBERGER, W.V, HAES, S., GULDENTOPS, E., **Structures, processes and relational mechanisms for Informations Technology Governance: Theories and practices**, 2004.

GUIMARÃES, Tomas de Aquino. **A nova administração pública e a abordagem da competência**. Revista de Administração Pública (RAP), Rio de Janeiro, FGV, 34(3), p.125-40, Mai./Jun. 2000.

HALLER, E.J.; BROWN R. E.; CLEMENTS, R.L. **Avaliação de desempenho operacional** : estabelecimento de uma auditoria operacional. EUA: Price Waterhouse, 1985.150p.

INTOSAI. **Código de ética e normas de auditoria**. Salvador: Tribunal de Contas do Estado da Bahia, 2005a (Série Traduções nº 10).

\_\_\_\_\_. **Diretrizes para aplicação de normas de auditoria operacional da INTOSAI**. Salvador: Tribunal de Contas do Estado da Bahia , 2005b.

IT GOVERNANCE INSTITUTE. **Board Briefing on IT Governance**, 2 Edição, 2006. Disponível em [www.itgi.org](http://www.itgi.org). Acesso em: 15 set. 2008.

IT GOVERNANCE INSTITUTE, **COBIT 3rd Edition Audit Guidelines**, 2000.

\_\_\_\_\_, **COBIT Control Practices: Guidance to Achieve Control Objectives for Successful IT Governance**, 2nd Edition, 2007.

\_\_\_\_\_, **IT Governance Implementation Guide: Using COBIT and Val IT**, 2nd Edition, 2007.

\_\_\_\_\_, **IT Assurance Guide using COBIT**, Rooning Meadows, 2007.

\_\_\_\_\_, **COBIT Security Baseline**, 2nd Edition, 2007.

\_\_\_\_\_, **COBIT Quickstart**, 2nd Edition, 2007.

JOBIM.Nelson. O controle exercido pelo Tribunal de contas na visão judicial. In: **CONGRESSO DOS TRIBUNAIS DE CONTAS DO BRASIL.23,2005**, Gramado.

KETTL, Donald F. **A revolução global**: reforma da administração do setor público. in. Reforma do Estado e administração pública gerencial, Orgs. Bresser Pereira, Luiz Carlos & Spink, Peter., 4. ed. Rio de Janeiro: Fundação Getúlio Vargas, 2001.

KING, W. R. Strategic planning for management information systems. **MIS Quartely**, v. 2, nº 1, p.27-37, Mar. 1978.

LIMA, Dagomar Henriques. **Avaliação de programas e responsabilização dos agentes públicos pelo resultado da ação governamental**: o papel do Tribunal de Contas da União. In: TCU – Tribunal de Contas da União. **Prêmio Serzedello Corrêa** : monografias vencedoras: 2005. p. 45-73.

MARINI, Caio. **Gestão pública**: o debate contemporâneo. Fundação Luiz Eduardo Magalhães. Salvador: FLEM: 2003. 104 p.

MATOS, Juliana M. O. **Auditoria operacional no Tribunal de Contas do Estado de Pernambuco: caminhos para sua institucionalização** 2006. 158f.

Dissertação (Mestrado Profissional em Gestão Pública) – Coordenação de Ciências Sociais, Universidade Federal de Pernambuco, Recife, 2006.

MEIRELLES, Hely Lopes. **Direito administrativo brasileiro**. 28 ed. São Paulo: Malheiros, 2003.

MEYER, John W., ROWAN, Brian. **Institucionalized Organizations: Formal Structure as Myth and Ceremony**, in Powell, Walter W., Di Maggio, Paul (eds.), *The New Institutionalism in Organizational Analysis*. Chicago: University of Chicago Press.

MINGAY, S; BITTINGER, S. **Combine CobiT and ITIL for Powerful IT Governance**, in Research Note, TG-16-1849, Gartner, 2002. Disponível em <http://www3.gartner.com>. Acesso em: mai. 2008

MÔNACO, Gabriel Santana. **Agências executivas e contratos de gestão. A possibilidade de ampliação da autonomia gerencial, orçamentária e financeira deve ficar restrita apenas às autarquias e fundações?**. Jus Navigandi, Teresina, ano 11, n. 1539, 18 set. . Disponível em: <<http://jus2.uol.com.br/doutrina/texto.asp?id=10423>>. Acesso em: 08 set. 2008.

NASCIMENTO, Roberto Sérgio do. Auditoria operacional versus auditoria operacional: uma ampliação do escopo da auditoria tradicional. **Revista do Tribunal de Contas**, Brasília, v.32, n.88, abr/jun. 2001

\_\_\_\_\_. Roberto Sérgio do. Auditoria como instrumento de Controle e de avaliação das organizações: estudo de Caso envolvendo o fundo de recuperação do estado do espírito santo (FUNRES) com base na auditoria operacional. **Revista do Tribunal de Contas**, Brasília, v.33, n.92, abr/jun. 2002

NORONHA, Maridel Piloto de. **A experiência do Tribunal de Contas da União do Brasil na avaliação de programas de governo**. In: *Congreso Internacional del CLAD sobre la Reforma del Estado y de la Administración Pública*. 8. Panamá, 28-31 out. 2003.

NUNES, Wanda Cláudia Galluzzi. **Auditorias de desempenho**. Revista do Tribunal de Contas do Município do Rio de Janeiro, Rio de Janeiro, n. 26, p. 64-74, abr./2004.

O'DONNELL, Guillermo. **Democracia delegativa?** Novos Estudos, S. Paulo: Cebrap, n. 31, p. 25-40, out. 1991.

OAG – Office of the Auditor General of Canada. **Auditoria de eficiência** – guia de auditoria – parte 1. 1993. Trad. Curso de Francês Lê Lyceé. 1ª ed. Salvador: Tribunal de Contas do Estado da Bahia, 1995, 28 p.

OLIVEIRA, Luiz Carlos Silva. **Auditoria operacional sob a ótica da eficácia – A relevância da sua utilização pelo sistema de controle interno federal**. Trabalho apresentado no XVI congresso brasileiro de contabilidade, Goiânia, 15 a 20 de outubro de 2000

PETER, Maria da Glória; MACHADO, M.V.V. **Manual de auditoria governamental**. São Paulo: Atlas, 2003.

PETERSON R. R., **Information Strategies and Tactics for Information Technology Governance**, in **Strategies for Information Technology Governance**, book edited by Van Grembergen W., Idea Group Publishing, 2003.

POLLITT, Christopher *et al.* **Performance or Compliance? Performance Audit and Public management in Five Countries**. Oxford: Oxford University Press: Addison-Wesley. 1999.

POWER, M. **The Audit Society: Rituals of Verification**. Oxford: Oxford University Press. 1997

PYBURN, P. J. Linking the MIS plan with corporate strategy: an exploratory study. **MIS Quartely**, v.7, nº 2, p. 1-15, June 1983.

REIDER, Harry R. **The complete guide to operational auditing**. New York, John Wiley, 1993.

ROCHA, Arlindo Carvalho. A função de Auditoria Operacional na avaliação de controle de Entidades Governamentais. **Revista do Tribunal de Contas da União**. v. 44, abr./jun. 1990.

RODRIGUEZ, M. V. R. **Gestão Empresarial: organizações que aprendem**. Rio de Janeiro. Qualitymark, 2002.

SILVA, De Plácido. **Vocabulário Jurídico**. Rio de Janeiro: Companhia Editora Forense, 2001.

SILVA, Francisco Carlos da Cruz. **Controle Social: reformando a administração para a sociedade**. Brasília/DF, Prêmio Serzedello Corrêa – Monografias Vencedoras –, 2001.

SILVA, José Afonso da. **Curso de Direito Constitucional Positivo**. São Paulo, Editora Revista dos Tribunais Ltda, 5ª ed. revista e ampliada de acordo com a nova Constituição, 1989, p.108.

SILVA OLIVEIRA, Luiz Carlos. **Auditoria operacional sob a ótica da eficácia – A relevância da sua utilização pelo sistema de controle interno federal**. In: CONGRESSO BRASILEIRO DE CONTABILIDADE, 16., 2002, Goiânia. 2002, p. 14

SOUZA, Jorge. **Controle interno municipal: uma abordagem prática**. Porto Alegre: Evangraf, 2006.

TCU – Tribunal de Contas da União. **Levantamento da governança de TI na administração federal**. Brasília: TCU, Secretaria de Fiscalização de Tecnologia da Informação, 2007.

\_\_\_\_\_. **Manual de auditoria de natureza operacional.** Brasília: TCU, Coordenadoria de Fiscalização e Controle, 2000.

\_\_\_\_\_. **Manual de auditoria de desempenho.** Brasília: TCU, Secretaria de Auditoria e Inspeções, 1998.

VERGARA, Sylvia Constant. **Projetos e relatórios de pesquisa em administração.** 7. ed. São Paulo: Atlas, 2006

\_\_\_\_\_. **Métodos de pesquisa em administração.** São Paulo: Atlas, 2005.

VILLAS, Marcio Martins. Auditoria Operacional em Entidades Governamentais. Brasília, **Revista do Tribunal de Contas da União**, Brasília, 21(44), abr/jun. 1990.

WEILL, P., ROSS, J. W. **IT Governance: How Top Performers Manage IT Decision Rights for Superior Results.** Harward Business School Press, 2004.

**ANEXO A: LEGISLAÇÃO DE CONTROLE**

<b>Legislação</b>	<b>Descrição</b>
Constituição Federal de 1988	A seção IX que trata da Fiscalização Contábil, Financeira e Orçamentária.
Lei Complementar nº 63, de 1 de agosto de 1990	Dispõe sobre a Lei Orgânica do Tribunal de Contas do Estado do Rio de Janeiro e dá outras providências.
Deliberação nº 167, de 10 de dezembro de 1992.	Aprova o Regimento Interno do Tribunal de Contas do Estado do Rio de Janeiro.
Deliberação nº 247, de 13 de março de 2008	Dispõe sobre o encaminhamento de dados relativos à área da receita dos municípios do Estado do Rio de Janeiro e dá outras providências.
Deliberação nº 245, de 18 de dezembro de 2007	Estabelece normas a serem observadas pelos órgãos e entidades municipais da Administração Pública Direta e Indireta de qualquer dos Poderes, sob a jurisdição do Tribunal de Contas, visando o controle e fiscalização dos atos administrativos que especifica.

## ANEXO B: LEGISLAÇÃO APLICÁVEL À TI

<b>Legislação</b>	<b>Descrição</b>
<b>Lei nº 7.232</b> , de 29 de outubro de 1984	Dispõe sobre a Política Nacional de Informática e dá outras providências.
<b>Lei nº 8.159</b> , de 8 de janeiro de 1991	Dispõe sobre a política nacional de arquivos públicos e privados.
<b>Lei nº 8.248</b> , de 23 de outubro de 1991	Dispõe sobre a capacitação e competitividade do setor de informática e automação, e dá outras providências.
<b>Lei nº 8.666</b> , de 21 de junho de 1993	Institui normas para licitações e contratos da Administração Pública.
<b>Lei nº 9.609</b> , de 19 de fevereiro de 1998	Dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País, e dá outras providências.
<b>Lei nº 9.610</b> , de 19 de fevereiro de 1998	Altera, atualiza e consolida a legislação sobre direitos autorais e dá outras providências.
<b>Lei nº 9.983</b> , de 14 de julho de 2000	Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal. Prevê penas específicas para crimes de inserção, alteração, exclusão e divulgação indevidas de dados nos sistemas informatizados ou banco de dados da Administração Pública.
<b>Medida Provisória nº 2.200-2</b> , de 24 de agosto de 2001	Institui a Infra-Estrutura de Chaves Públicas Brasileira – ICP-Brasil e transforma o Instituto Nacional de Tecnologia da Informação em autarquia.
<b>Decreto nº 3.555</b> , de 8 de agosto de 2000	Aprova o regulamento para a modalidade de licitação denominada pregão, para aquisição de bens e serviços comuns.
<b>Decreto nº 3.697</b> , de 21 de dezembro de 2000	Regulamenta o parágrafo único do art. 2º da Medida Provisória nº 2.026-7, de 23 de novembro de 2000, que trata do pregão por meio da utilização de recursos de tecnologia da informação.
<b>Decreto nº 3.872</b> , de 18 de julho de 2001	Dispõe sobre o Comitê Gestor da Infra-Estrutura de Chaves Públicas Brasileira – CG IGP-Brasil, sua Secretaria Executiva, sua Comissão Técnica Executiva.
<b>Decreto nº 3.931</b> , de 19 de setembro de 2001	Regulamenta o Sistema de Registro de Preços previsto no art. 15 da Lei nº 8.666, de 21 de junho de 1993, e dá outras providências.
<b>Lei nº 10.520</b> , de 17 de julho de 2002	Institui no âmbito da União, Estados, Distrito Federal e Municípios, nos termos do art. 37, inciso XXI, da Constituição Federal, modalidade de licitação denominada pregão, para aquisição de bens e serviços comuns, e dá outras providências.





## ANEXO D: MATRIZ DE PLANEJAMENTO

**PROJETO DE AUDITORIA:** Auditoria na área de Informática, objetivando descrever a situação geral da informatização e analisar um Sistema de Informação de forma mais acurada.

**PROBLEMA DE AUDITORIA:** O Sistema em análise realiza as principais funções para as quais foi projetado, oferecendo segurança aos dados da Prefeitura?

PRINCIPAIS QUESTÕES	INFORMAÇÕES NECESSÁRIAS	ESTRATÉGIAS METODOLÓGICAS	MÉTODOS DE COLETA DE DADOS	MÉTODOS DE ANÁLISE DE DADOS	LIMITAÇÃO	CONCLUSÕES POSSÍVEIS
1) O Sistema emite os principais relatórios que permitem acompanhar o processo informatizado?	Principais relatórios emitidos pelo Sistema. Identificação do Gestor.	Consulta aos relatórios. Entrevista.	Solicitação. Uso direto do Sistema.	Análise dos relatórios quanto à forma e conteúdo.	Pouca disponibilidade do Gestor do Sistema. Quadro técnico insuficiente.	Se o Sistema cumpre o objetivo de disponibilizar informações aos usuários.
2) Os dados armazenados são consistentes?	Projeto Lógico do Sistema (DFD, Dicionário de Dados, Modelo ER). Projeto Físico (Layout das Tabelas)	Consulta aos dados existentes. Navegação no Sistema	Solicitação. Uso direto do Sistema.	Testes de tipos de dados. Valores máximos, mínimos, repetidos. Teste de domínio. Cruzamentos de dados.	Pacote de Software fechado, adquirido no mercado.	Se o Sistema é confiável (Dados consistentes).
3) Os dados armazenados são atuais, ou seja, o Sistema é alimentado regularmente?	Registros mais atuais do Banco de Dados.	Consulta aos dados existentes. Navegação no Sistema.	Solicitação. Uso direto do Sistema.	Teste de valores armazenados no Banco de Dados.	Manutenção do Sistema Terceirizada.	Se a informação fornecida é confiável
4) O Sistema é seguro, ou seja, possui proteção contra acessos indevidos?	Descrição do Log do Sistema. Descrição da tabela de senhas. Regras de validação de senha.	Consulta aos dados existentes. Navegação no Sistema.	Solicitação. Uso direto do Sistema.	Testes utilizando técnicas de acesso privilegiado. Análise das informações obtidas.	Pacote de Software fechado, adquirido no mercado.	Se o Sistema oferece segurança razoável.
5) O Sistema registra adequadamente as operações efetuadas pelos usuários?	Arquivo de Log do Sistema (registro da ações dos usuários).	Análise do arquivo de Log.	Solicitação.	Análise do arquivo através de instruções SQL.	Pacote de Software fechado, adquirido no mercado.	Se o Sistema registra devidamente as operações ocorridas.
6) São realizados <i>backups</i> regulares dos dados?	Planilha de <i>Backup</i>	Consulta de dados existentes	Solicitação. Observação direta.	Restauração e testes para verificar confiabilidade dos <i>backups</i> .	Serviços de gerenciamento de CPD terceirizados.	Se há garantia da disponibilidade das informações
7) O Sistema está em conformidade com a legislação vigente?	Legislação atinente ao Sistema.	Consulta da legislação. Observação do código fonte do Sistema.	Solicitação.	Análise da legislação. Análise do código fonte do Sistema.	Falta de informação do Gestor quanto à legislação vigente.	Se o Sistema está em conformidade com a Legislação vigente.

PRINCIPAIS QUESTÕES	INFORMAÇÕES NECESSÁRIAS	ESTRATÉGIAS METODOLÓGICAS	MÉTODOS DE COLETA DE DADOS	MÉTODOS DE ANÁLISE DE DADOS	LIMITAÇÃO	CONCLUSÕES POSSÍVEIS
8) Há políticas de contingência implementadas?	Documentos com descrição dos procedimentos de contingência adotados.	Consulta à documentação. Entrevista com os profissionais de informática.	Observação direta. Entrevista.	Comparação. Estudo de Caso.	Ausência de documentação.	Se o Sistema e seu ambiente estão preparados para a ocorrência de eventuais sinistros.
9) Existem procedimentos de operação do Sistema bem definidos e implementados?	Manual do usuário.	Consulta à documentação.	Observação direta. Entrevista.	Triangulação. Observação direta.	Ausência de documentação.	Se há padronização e documentação dos procedimentos operacionais
10) A Performance do Banco de Dados e do Sistema é satisfatória?	Documentação do Banco de Dados.	Navegação no Sistema. Testes de acesso.	Solicitação. Uso direto do Banco de Dados.	Testes de Performance.	Limitações no acesso e utilização do Sistema.	Se a performance do Sistema é adequada.
11) O Banco de Dados utilizado é seguro?	Documentação do Banco de Dados.	Testes de acesso ao Banco de Dados. Consulta à documentação	Solicitação. Uso direto do Banco de Dados.	Testes de Segurança. Verificação dos principais controles lógicos.	Limitações no acesso ao Banco de Dados	Se o Banco de Dados é seguro.
12) O ambiente de produção e desenvolvimento do Sistema é seguro?	Projeto Físico (Descrição do Ambiente/ Hardware, Softwares, controles de acesso)	Observação direta. Consulta à documentação. Entrevista com os analistas responsáveis.	Solicitação. Observação direta. Entrevista.	Estudo de caso	Ausência de Documentação. Pouca disponibilidade dos técnicos.	Se o ambiente do Sistema é seguro.
13) Há registros de utilização indevida do Sistema?	Arquivo extraído da Base de Dados. Arquivo de Log do Sistema (registro dos acessos).	Solicitação dos arquivos.	Solicitação ou extração direta dos dados.	Formação de uma Base de Dados. Consultas à Base utilizando instruções SQL.	Sistemas e serviços Terceirizados.	Se houve utilização irregular do Sistema.

**PROBLEMA DE AUDITORIA:** O grau de Informatização e de segurança do ambiente atende às necessidades do jurisdicionado?

PRINCIPAIS QUESTÕES	INFORMAÇÕES REQUERIDAS	ESTRATÉGIAS METODOLÓGICAS	MÉTODOS DE OBTENÇÃO DE DADOS	MÉTODOS DE ANÁLISE DE DADOS	LIMITAÇÃO	CONCLUSÕES POSSÍVEIS
1. Existem Políticas de Informática definidas e adequadas?	PDI (Plano Diretor de Informática) ou documentação similar.	Consulta de documentação existente.	Solicitação de Documentos.	Análise do conteúdo dos documentos.	Documentação Insuficiente.	Se há Políticas de Informática adequadas.
2. Como é a estrutura organizacional?	Organograma da Informática.	Consulta aos dados.	Observação Direta. Questionário. Entrevista.	Análise de conteúdo.	Corpo Técnico insuficiente ou incapacitado.	Se a estrutura organizacional relativa à Informática é adequada.
3. O Parque de Informática é suficiente e adequado às necessidades do jurisdicionado?	Descrição do Parque de Informática e da Rede de computadores.	Visitas aos ambientes de Informática.	Entrevistas com usuários. Questionário. Observação direta.	Análise qualitativa e quantitativa.	Prazo de realização da Inspeção.	Se o grau de satisfação do usuário é alto.
4. O número de profissionais é adequado às necessidades?	Relação do pessoal técnico. Atribuições dos cargos.	Pesquisa.	Entrevistas. Observação direta.	Análise de conteúdo.	Prazo de realização da Inspeção.	Se o quantitativo e o perfil dos profissionais é adequado.
5. A Rede de Computadores está configurada de forma segura?	Diagrama da Rede. Perfis de acesso à Rede.	Consulta a dados.	Questionário. Utilização da Rede. Observação Direta.	Análise de conteúdo. Análise qualitativa das configurações.	Perfil de acesso inadequado.	Se a Rede de computadores é segura.
6. Quais são as garantias nos contratos acerca de hardware/software adquiridos de terceiros?	Contratos de Informática.	Consulta a dados.	Solicitação.	Análise de conteúdo	Ausência de contratos formalizados.	Se os contratos garantem a continuidade dos serviços essenciais.
7. Existe uma Política de Segurança Corporativa?	Documento descrevendo a Política de Segurança.	Pesquisa.	Entrevista. Solicitação.	Análise de conteúdo.	Falta de informação dos usuários da Rede.	Se há uma Política de Segurança vigente.
8. Existe um Plano de Contingência Corporativo?	Documento descrevendo o Plano de Contingência.	Pesquisa.	Entrevista. Solicitação.	Análise de conteúdo	Falta de documentação dos procedimentos adotados.	Se há um plano de Contingência para salvaguardar todo o ambiente informatizado.
9. Os links da Rede com a Internet são seguros?	Diagrama da Rede. Configuração das estações.	Consulta a Dados.	Entrevista. Utilização da Rede.	Análise de conteúdo. Análise das configurações.	Perfil de acesso inadequado.	Se o acesso à Internet é efetuado de forma segura.
10. Os softwares utilizados são devidamente licenciados?	Licenças de uso dos softwares.	Consulta a Dados.	Solicitação.	Análise de conteúdo.	Falta de informação dos profissionais de informática.	Se há o devido licenciamento dos softwares utilizados.

**PROBLEMA DE AUDITORIA: Há irregularidades nas contratações e execução contratual dos Sistemas de Informação da Prefeitura?**

<b>PRINCIPAIS QUESTÕES</b>	<b>INFORMAÇÕES REQUERIDAS</b>	<b>ESTRATÉGIAS METODOLÓGICAS</b>	<b>MÉTODOS DE OBTENÇÃO DE DADOS</b>	<b>MÉTODOS DE ANÁLISE DE DADOS</b>	<b>LIMITAÇÃO</b>	<b>CONCLUSÕES POSSÍVEIS</b>
1. Houve danos à administração municipal na contratação da empresa CCA?	Contrato e seus Termos Aditivos.	Consulta de documentação existente.	Solicitação de Documentos. Entrevista.	Análise do conteúdo dos documentos.	Documentação Insuficiente. Não entrega de documentos solicitados.	Se há dano à administração municipal.
2. Houve contratação em duplicidade, com mais de um Sistema contratado para a mesma finalidade ?	Demais Contratos e respectivos Termos Aditivos.	Consulta de documentação existente.	Solicitação de Documentos. Observação Direta. Entrevista.	Análise do conteúdo dos documentos e análise do discurso.	Documentação Insuficiente. Não entrega de documentos solicitados.	Se houve contratação em duplicidade para o mesmo objeto.
3. A execução contratual está de acordo com o previsto no instrumento contratual?	Contrato e seus Termos Aditivos.	Consulta de documentação existente.	Solicitação de Documentos. Observação Direta. Entrevista.	Análise do conteúdo dos documentos e análise do discurso.	Documentação Insuficiente. Não entrega de documentos solicitados.	Se há correspondência entre o previsto no contrato e o efetivamente executado.
4. Há irregularidades na atestação dos pagamentos?	Processos de pagamento relativos às contratações.	Consulta de documentação existente.	Solicitação de Documentos.	Análise do conteúdo dos documentos.	Documentação Insuficiente. Não entrega de documentos solicitados.	Se há irregularidades na atestação dos pagamentos efetuados às empresas contratadas.
5. Os processos licitatórios relativos a TI seguem o ordenamento jurídico em vigor?	Processos licitatórios das contratações das empresas envolvidas.	Consulta de documentação existente.	Solicitação de Documentos.	Análise do conteúdo dos documentos.	Documentação Insuficiente. Não entrega de documentos solicitados.	Se os processos licitatórios seguiram os preceitos legais.
6. Houve atuação do controle interno no que se refere a eventuais irregularidades?	Processos licitatórios das contratações das empresas envolvidas, respectivos pagamentos e sindicâncias.	Consulta de documentação existente.	Solicitação de Documentos. Entrevista.	Análise do conteúdo dos documentos e análise do discurso.	Documentação Insuficiente. Não entrega de documentos solicitados.	Se houve atuação do controle interno no sentido de sanar possíveis irregularidades.