



**AUDITORIA DE SISTEMAS DE
INFORMAÇÃO NA ADMINISTRAÇÃO
MUNICIPAL: UM ESTUDO DE CASO NA
PREFEITURA DE BELO HORIZONTE**

MARIA FERNANDA DE MORAIS

FUNDAÇÃO JOÃO PINHEIRO
ESCOLA DE GOVERNO DE MINAS GERAIS
MESTRADO EM ADMINISTRAÇÃO PÚBLICA

AUDITORIA DE SISTEMAS DE INFORMAÇÕES NA
ADMINISTRAÇÃO PÚBLICA MUNICIPAL: UM ESTUDO DE
CASO NA PREFEITURA DE BELO HORIZONTE

MARIA FERNANDA DE MORAIS

BELO HORIZONTE

2002

MARIA FERNANDA DE MORAIS

**AUDITORIA DE SISTEMAS DE INFORMAÇÕES NA
ADMINISTRAÇÃO PÚBLICA MUNICIPAL: UM ESTUDO DE
CASO NA PREFEITURA DE BELO HORIZONTE**

*Dissertação apresentada ao Programa de Mestrado da Escola
de Governo da Fundação João Pinheiro, como requisito parcial
para obtenção do título de Mestre em Administração Pública.*

Área de Concentração: Tecnologias da Informação

Orientador: ANTÔNIO ARTUR DE SOUZA, Ph.D.

Universidade Estadual de Maringá

Escola de Governo

Fundação João Pinheiro

Belo Horizonte

Julho/2002

FUNDAÇÃO JOÃO PINHEIRO
BIBLIOTECA
Nr. 20300
Vol. _____ Ex. _____
Data 05 / 06 / 03



ATA DA DEFESA PÚBLICA DE DISSERTAÇÃO
MESTRADO EM ADMINISTRAÇÃO PÚBLICA
ÁREA DE CONCENTRAÇÃO: TECNOLOGIAS DA INFORMAÇÃO

Aos 12 (doze) dias do mês de julho de 2002, foi realizada a defesa pública da dissertação intitulada **“Auditoria de sistemas de informações na Administração Pública Municipal: Um estudo de caso na Prefeitura de Belo Horizonte”**, elaborada por **MARIA FERNANDA DE MORAIS**, como requisito parcial para obtenção do título de mestre do Programa de Mestrado em Administração Pública: Tecnologias da Informação, da Escola de Governo da Fundação João Pinheiro. Após a apresentação do trabalho, a mestranda foi arguída pelos membros da Comissão Examinadora, composta por: Prof. Antônio Artur de Souza (Orientador); Prof. Hudson Fernandes Amaral e Prof. Ivan Beck Ckgnazaroff. A Comissão Examinadora reuniu-se para deliberar e, considerando que a dissertação atende aos requisitos técnicos e acadêmicos previstos na legislação do Programa, decidiu, por unanimidade, pela **aprovação** da mesma. Este documento expressa o que ocorreu na sessão da defesa e será assinado pelos membros da Comissão Examinadora.

Belo Horizonte, 12 de julho de 2002.

Prof. Antônio Artur de Souza (UEM)

Prof. Hudson Fernandes Amaral (UFMG)

Prof. Ivan Beck Ckgnazaroff (UFMG)

"BARUCH HA BA B'SHEM ADONAI: YE'OSHUA."

AGRADECIMENTOS

A Deus, Autor e Pedra Angular da minha vida, que me deu este sonho e a certeza de realizá-lo.

Aos meus pais, Fernando e Maria Natividade, por tanto carinho, apoio e pela compreensão quanto às minhas ausências, necessárias à consecução deste objetivo. Diante de todo o amor que sinto por vocês, jamais poderei ser suficientemente grata.

Ao querido Henrique, pelo nobre exemplo de dedicação a ser seguido.

Ao estimado Professor Antônio Artur de Souza, amigo e orientador, por compartilhar seu conhecimento e pela seriedade em suas valiosas orientações. Muitíssimo obrigada!

À AUDIM, pela minha liberação para cursar este mestrado e pela disponibilidade em servir de cenário para meu trabalho de campo.

À PRODABEL, que, ao oferecer a oportunidade de participar deste projeto, permitiu-me alcançar mais uma conquista.

Aos colegas de mestrado, pelo convívio fraterno e solidário que pudemos compartilhar.

E a todos aqueles que, direta ou indiretamente, auxiliaram-me e contribuíram para a efetivação deste trabalho.

SUMÁRIO

LISTA DE SIGLAS	10
LISTA DE QUADROS	13
LISTA DE FIGURAS	15
LISTA DE GRÁFICOS	16
LISTA DE TABELAS	17
RESUMO	18
<i>ABSTRACT</i>	20
1. INTRODUÇÃO	22
1.1 Tema e Problema de Pesquisa	22
1.2 Justificativa e Relevância	25
1.3 Objetivos da Pesquisa	27
1.3.1 Objetivo Geral	27
1.3.2 Objetivos Específicos	27
1.4 Organização da Dissertação	28
2. METODOLOGIA DA PESQUISA	31
2.1 Introdução	31
2.2 Delineamento e Perspectiva da Pesquisa	31
2.3 Escolha da Organização	33
2.4 Unidade de Análise	34
2.5 Coleta dos Dados	34
2.6 Tipos de Dados	34
2.7 Coleta dos Dados Primários	35
2.7.1 Pesquisa Documental	35
2.7.2 Observação Participante	36
2.7.3 Questionário	37
2.8 Análise dos Dados	40
2.9 Delimitação da Pesquisa	43

2.10 Protocolo da Pesquisa	43
2.11 Conclusão	46
3. SISTEMAS DE INFORMAÇÃO	47
3.1 Introdução	47
3.2 Informação	47
3.3 Sistema	50
3.4 Sistema de Informações	52
3.4.1 Definição	52
3.5 Sistema de Informações Computadorizados	54
3.6 Sistemas de Informações da Prefeitura Municipal de Belo Horizonte	58
3.7 Conclusão	64
4. SEGURANÇA DOS SISTEMAS DE INFORMAÇÃO	66
4.1 Introdução	66
4.2 Segurança dos Sistemas de Informações	66
4.3 Modalidades de Segurança	69
4.3.1 Segurança Legal	69
4.3.2 Segurança Administrativa	71
4.3.3 Segurança Física	72
4.3.4 Segurança Lógica	73
4.4 Política de Segurança	74
4.5 Riscos e seus Impactos nos Sistemas de Informações Computadorizados	75
4.6 Medidas de Segurança	78
4.6.1 Medidas de Segurança Legal	79
4.6.2 Medidas de Segurança Administrativa	79
4.6.3 Medidas de Segurança Física	79
4.6.4 Medidas de Segurança Lógica	81
4.7 Plano de Contingências	83
4.8 Conclusão	86

5. CONTROLE INTERNO	87
5.1 Introdução	87
5.2 Definição e Objetivos	88
5.3 Modalidades e Avaliação	90
5.4 O Controle Interno da Administração Pública Municipal: Aspectos Legais	93
5.5 O Controle Interno da Prefeitura Municipal de Belo Horizonte	97
5.6 Conclusão	100
6. AUDITORIA INTERNA	101
6.1 Introdução	101
6.2 Evolução	101
6.3 Conceito e Objetivos	105
6.4 Modalidades	109
6.4.1 Auditoria Contábil e Tributária	109
6.4.2 Auditoria Operacional	112
6.4.3 Auditoria Gestional	116
6.4.4 Auditorias Especiais	117
6.4.5 Auditoria de Sistemas	118
6.5 Modelagem e Programa de Auditoria	120
6.5.1 Introdução	121
6.5.2 Postulados Básicos do Programa de Auditoria	124
6.5.3 Estrutura do Programa de Auditoria	126
6.5.3.1 Objeto ou Área do Programa de Auditoria	126
6.5.3.2 Objetivos do Programa de Auditoria	127
6.5.3.3 Avaliação da Organização e seus Controles Internos	128
6.5.3.4 Roteiro Sequencial	129
6.5.3.5 Questionários Auxiliares	130
6.5.3.6 Diagnósticos e Comprovações Numéricas	132
6.5.4 Formatação Técnica	134
6.5.4.1 Exemplos de Formatação Técnica	134
6.6 Conclusão	136

7. AUDITORIA DE SISTEMAS OU AUDITORIA DAS	138
TECNOLOGIAS DA INFORMAÇÃO	
7.1 Introdução	138
7.2 Conceitos e Objetivos	138
7.3 Normas Aplicáveis	142
7.4 Técnicas de Auditoria de Sistemas	144
7.4.1 <i>Software</i> de Auditoria	145
7.4.2 Questionários	145
7.4.3 Simulação de Dados (<i>Test-Desk</i>)	146
7.4.4 Visita <i>In Loco</i>	146
7.4.5 Mapeamento (<i>Mapping</i>)	147
7.4.6 Rastreamento	148
7.4.7 Entrevistas	148
7.4.8 Análise de Relatórios e Telas	149
7.4.9 Simulação Paralela	149
7.4.10 Análise do <i>Log</i>	150
7.4.11 Análise do Programa-Fonte	150
7.5 Áreas de Atuação da Auditoria de Sistemas	151
7.5.1 Controles Gerais	153
7.5.1.1 Controles Organizacionais	153
7.5.1.2 Política de Segurança	154
7.5.1.3 Controles de Acesso	155
7.5.2 Controles de <i>Softwares</i> Aplicativos	156
7.5.3 Desenvolvimento de Sistemas	157
7.5.4 Banco de Dados	159
7.5.5 Redes de Computadores	162
7.5.6 Microcomputadores	164
7.6 O Auditor de Sistemas	166
7.7 Conclusão	171

8. AUDITORIA DO MUNICÍPIO: ESTUDO DE CASO	173
8.1 introdução	173
8.2 Histórico	173
8.3 Finalidades	174
8.4 Estrutura Organizacional	175
8.5 Auditores	178
8.6 Procedimentos Adotados	179
8.6.1 Programação Anual de Auditoria	181
8.6.2 Designação	181
8.6.3 Trabalho de Campo	181
8.6.4 Papéis de Trabalho	181
8.6.5 Fundamentação do Resultado	182
8.6.6 Relatório de Auditoria	182
8.6.6.1 Relatório Parcial	182
8.6.6.2 Relatório Extraordinário	184
8.6.7 Cronograma de implantação das Recomendações	184
8.6.8 Laudo de Avaliação	184
8.6.9 Notificação	185
8.6.10 Pasta de Relatório	185
8.7 Modalidades das Auditoria Realizadas	185
8.8 Conclusão	188
9. APRESENTAÇÃO E DISCUSSÃO DOS RESULTADOS	190
9.1 Introdução	190
9.2 Características da População Pesquisada	191
9.3 Percepção dos Auditores sobre os Sistemas de Informações da PMBH	194
9.4 Percepção dos Auditores sobre os Trabalhos de Auditoria	198
9.5 Capacitação dos Auditores Municipais	206
9.6 Conclusão	210

10. MODELO DE AUDITORIA DE SISTEMAS	212
10.1 Introdução	212
10.2- Programa de Auditoria de Sistemas	214
10.3- Conclusão	227
11. CONCLUSÕES, RECOMENDAÇÕES E SUGESTÕES	229
11.1 Introdução	229
11.2 Conclusões Quanto à Metodologia da Pesquisa	229
11.3 Conclusões Quanto ao Referencial Teórico	230
11.4 Conclusões Quanto aos Objetivos da Pesquisa	232
11.5 Recomendações para a AUDIM	235
11.6 Sugestões para Estudos Futuros	237
11.7 Considerações Finais	237
12. REFERÊNCIAS BIBLIOGRÁFICAS	239
GLOSSÁRIO	253
ANEXOS	256

LISTA DE SIGLAS

AGM	Auditoria Geral do Município
ABAS	Associação Brasileira de Auditoria de Sistemas
ABNT	Associação Brasileira de Normas Técnicas
ACL	<i>Audit Command Language</i>
ANATEL	Agência Nacional de Telecomunicações
AUDIBRA	Instituto dos Auditores Internos do Brasil
AUDIM	Auditoria do Município
BACEN	Banco Central do Brasil
BELOTUR	Empresa de Turismo de Belo Horizonte S.A.
BEPREM	Beneficência da Prefeitura de Belo Horizonte
BHTRANS	Empresa de Transportes e Trânsito de Belo Horizonte S.A.
BS	<i>British Standard</i>
CAAT's	<i>Computer Assisted Audit Techniques</i>
CF	Constituição da República Federativa do Brasil
CFC	Conselho Federal de Contabilidade
CISA	<i>Certified Information Systems Auditor</i>
CNASI	Congresso de Auditoria de Sistemas e Segurança da Informação
CRCRS	Conselho Regional de Contabilidade do Rio Grande do Sul
CRCSP	Conselho Regional de Contabilidade de São Paulo
DAUDIT	Departamento de Auditoria
DBMS	<i>Database Management System</i>
FJP	Fundação João Pinheiro
GEAFI	Gerência Administrativo-Financeira
GEATA	Gerência de Apoio aos Trabalhos de Auditoria
GETA	Gerência de Coordenação de Trabalhos de Auditoria
HMOB	Hospital Municipal Odilon Behrens

IBRACON	Instituto Brasileiro de Contabilidade
ICP	Infra-Estrutura de Chaves Públicas
IDEA	<i>Interactive Data Extraction and Analysis</i>
IFAC	<i>Internacional Federation of Accountants</i>
IIA	<i>Institute of Internal Auditors</i>
IPTU	Imposto Predial e Territorial Urbano
ISACA	<i>Information Systems Audit and Control Association</i>
ISDN	<i>Integrated Services Digital Network</i>
ISO	<i>International Organization for Standardization</i>
ISSQN	Imposto sobre Serviços de Qualquer Natureza
LOM	Lei Orgânica Municipal
OSI	<i>Open Systems Interconnection</i>
PED	Processamento Eletrônico de Dados
PGM	Procuradoria Geral do Município
PMBH	Prefeitura Municipal de Belo Horizonte
PRODABEL	Empresa de Informática e Informação do Município de Belo Horizonte
RAM	<i>Random Acces Memory</i>
RMI	Rede Municipal de Informática
ROM	<i>Read Only Memory</i>
SAS	<i>Statement of Auditing Standards</i>
SCOMARH	Secretaria Municipal da Coordenação de Administração e Recursos Humanos
SCOMF	Secretaria Municipal da Coordenação de Finanças
SCOMGER	Secretaria Municipal da Coordenação de Gestão Regional
SCOMPS	Secretaria Municipal da Coordenação de Política Social
SCOMURBE	Secretaria Municipal da Coordenação de Política Urbana e Ambiental
SCOPLAM	Secretaria Municipal de Governo, Planejamento e Coordenação Geral
SGBD	Sistema de Gerenciamento de Banco de Dados
SMED	Secretaria Municipal de Educação
SMMAI	Secretaria Municipal de Modernização Administrativa e Informação

SMPL	Secretaria Municipal de Planejamento
SMSA	Secretaria Municipal de Saúde
STN	Secretaria do Tesouro Nacional
SUCESU	Sociedade dos Usuários de Informática e Telecomunicações
SUDECAP	Superintendência de Desenvolvimento da Capital
TCEMG	Tribunal de Contas do Estado de Minas Gerais
TCP/IP	<i>Transmission Control Protocol/Internet Protocol</i>
TCU	Tribunal de Contas da União
UCP	Unidade Central de Processamento
URBEL	Companhia Urbanizadora de Belo Horizonte

LISTA DE QUADROS

QUADRO 1 -	Vantagens e Desvantagens dos Questionários	38
QUADRO 2 -	Protocolo do Instrumental de Coleta de Dados	45
QUADRO 3 -	Protocolo da Seqüência de Atividades	46
QUADRO 4 -	Conceitos de Dados e Informação	48
QUADRO 5 -	Atributos da Informação	49
QUADRO 6 -	Conceitos de Sistemas	50
QUADRO 7 -	Conceitos de Sistemas de Informações	52
QUADRO 8	Elementos de um Sistema Computadorizado	55
QUADRO 9 -	Principais Sistemas de Informações da PMBH	60
QUADRO 10	Objetivos da Segurança dos Sistemas de Informações	68
QUADRO 11 -	Legislação Brasileira Alusiva à Segurança da Informação	70
QUADRO 12	Riscos a que os Sistemas de Informações estão Sujeitos	76
QUADRO 13 -	Normas de Auditoria Interna	103
QUADRO 14 -	Conceitos de Auditoria Interna	106
QUADRO 15 -	Conceitos de Programa de Auditoria	122
QUADRO 16	Conceitos de Auditoria de Sistemas	140
QUADRO 17 -	Características Psico-Comportamentais do Auditor Interno	167
QUADRO 18 -	Escolaridade do Corpo Técnico de Auditores	193
QUADRO 19 -	Partes Integrantes do Programa de Auditoria de Sistemas	214
QUADRO 20 -	Parte 1 do Programa de Auditoria de Sistemas: Controles Gerais/Controles Administrativos	215
QUADRO 21 -	Parte 1 do Programa de Auditoria de Sistemas: Controles Gerais/Política de Segurança	216
QUADRO 22 -	Parte 1 do Programa de Auditoria de Sistemas: Controles Gerais/Plano de Contingências	218
QUADRO 23	Parte 2 do Programa de Auditoria de Sistemas: Controles de <i>Softwares</i> Aplicativos/Entrada de Dados	219
QUADRO 24	Parte 2 do Programa de Auditoria de Sistemas: Controles de <i>Softwares</i> Aplicativos/Processamento e Saída dos Dados	220

QUADRO 25	Parte 3 do Programa de Auditoria de Sistemas: Desenvolvimento de Sistemas	221
QUADRO 26	Parte 4 do Programa de Auditoria de Sistemas: Banco de Dados	223
QUADRO 27	Parte 5 do Programa de Auditoria de Sistemas: Rede de Computadores	224
QUADRO 28	Parte 6 do Programa de Auditoria de Sistemas: Microcomputadores	226

LISTA DE FIGURAS

FIGURA 01 -	Protocolo das Etapas da Pesquisa	44
FIGURA 02 -	Transformação de Dados em Informação	48
FIGURA 03 -	Funcionamento de um Sistema	51
FIGURA 04 -	Componentes dos Sistemas de Informações	53
FIGURA 05 -	Componentes Básicos de um Sistema Criptográfico	82
FIGURA 06 -	Áreas Enquadradas na Modalidade de Auditoria Operacional do Setor Público	114
FIGURA 07 -	Modelo de Roteiro Seqüencial da Área de Compras de uma Empresa Industrial	135
FIGURA 08 -	Modelo de Questionário Auxiliar da Área de Compras de uma Empresa Industrial	136
FIGURA 09 -	Áreas Analisadas na Auditoria de Sistemas	152
FIGURA 10 -	Estrutura Organizacional da AUDIM	176
FIGURA 11 -	Fluxo de Procedimentos da AUDIM	180

LISTA DE GRÁFICOS

GRÁFICO 01 -	Modalidades de Auditorias Realizadas pela AUDIM de 1994 a 2001	186
GRÁFICO 02 -	Distribuição da Escolaridade Excedente dos Auditores em Relação à Exigida para o Cargo em Exercício	194
GRÁFICO 03 -	Entendimento dos Auditores quanto à Necessidade de Controles Internos Rigorosos para um Ambiente Informatizado	196
GRÁFICO 04 -	Percepção dos Auditores se os Sistemas Informatizados da PMBH são Seguros e se as Informações por eles Geradas são Confiáveis	197
GRÁFICO 05 -	Comprometimento da Qualidade e Resultado de um Trabalho de Auditoria decorrente da Utilização de Informações Provenientes dos Sistemas Informatizados da PMBH Que não Foram Auditados	200
GRÁFICO 06 -	Utilização pelos Auditores de Informações Provenientes dos Sistemas Informatizados da PMBH para a Realização dos seus Trabalhos de Auditoria	201
GRÁFICO 07 -	Percepção dos Auditores se a Auditoria de Sistemas é um Instrumento Importante para a Qualidade e Segurança dos Sistemas de Informações	203
GRÁFICO 08 -	Utilização pelos Auditores de Manuais, Programas e Técnicas Próprias de Auditoria de Sistemas	204
GRÁFICO 09 -	Consideração dos Auditores Acerca de Serem Profissionais Capacitados para Desenvolver Auditoria de Sistemas	207
GRÁFICO 10 -	Iniciativa dos Auditores em Ingressar na Área de Auditoria de Sistemas	209
GRÁFICO 11 -	Leitura dos Auditores de Acervo Bibliográfico Referente ao Tema Auditoria de Sistemas	209
GRÁFICO 12 -	Percepção dos Auditores Sobre a Existência de Publicações Referentes ao Tema Auditoria de Sistemas no Acervo Bibliográfico da AUDIM	210

LISTA DE TABELAS

TABELA 01 -	Tempo de Serviço dos Auditores na AUDIM	192
TABELA 02 -	Sistemas de Informação da PMBH Citados pelos Auditores	195
TABELA 03 -	Quantitativo de Auditores que Realizaram Auditoria de Sistemas para a AUDIM	199
TABELA 04 -	Treinamentos Oferecidos pela AUDIM e Quantitativo de Auditores Participantes	208

RESUMO

A Administração Pública Brasileira vem passando por um processo de aperfeiçoamento, procurando adaptar-se às tendências mundiais. Isso tem levado as entidades públicas a realizarem investimentos relevantes em tecnologias da informação como um componente de transparência para as ações governamentais e como sustentáculo para a tomada de decisões pelos gestores públicos.

Perseguindo esse padrão de Administração Pública, a Prefeitura Municipal de Belo Horizonte (PMBH) vem investindo em recursos tecnológicos de informática e democratizando o acesso à informação pública. Nos últimos anos, a PMBH implementou diversos Sistemas de Informações Computadorizados, que abrangem, dentre outras, as áreas de Orçamento, Finanças, Saúde, Administração, Planejamento, Trânsito e Educação.

O uso intensificado desses sistemas proporciona possibilidades de novas soluções para a administração e gestão das atividades da PMBH. Entretanto, esse ambiente informatizado requer controles internos mais rigorosos, para os quais novos pontos de controle e técnicas próprias de Auditoria de Sistemas são cogentes para assegurar a integridade e segurança dos dados que trafegam pelos sistemas.

Esta dissertação faz uma abordagem sobre as principais técnicas e áreas de atuação da Auditoria de Sistemas e destaca os elementos fundamentais de uma Política de Segurança de Sistemas, modalidade de auditoria amplamente utilizada na atualidade, todavia de histórico restrito no âmbito da Administração Pública.

Baseado nesses subsídios teóricos, foi construído e proposto um Modelo de Auditoria de Sistemas para a Auditoria do Município (AUDIM), órgão responsável pela

auditoria interna municipal, vez que a informatização crescente na PMBH demanda peculiar atenção desta unidade de controle, porquanto a análise da segurança dos dados, da exatidão e confiabilidade dos relatórios e informações produzidos via processamento eletrônico, tornou-se uma nova incumbência para este órgão.

O trabalho ainda, apresenta importantes conclusões acerca do tema e ressalta as dificuldades enfrentadas pela AUDIM para auditar os Sistemas de Informações da PMBH. Por fim, apresentam-se algumas recomendações para que a AUDIM possa ampliar e aprimorar seus trabalhos na modalidade de Auditoria de Sistemas, buscando por conseguinte, a utilização pelos gestores municipais de informações fidedignas para a tomada de decisões e a contribuição para uma Administração Pública Municipal mais eficiente, eficaz e transparente.

Palavras-Chave

Auditoria das Tecnologias da Informação _ Auditoria de Sistemas _ Auditoria Interna _ Controle Interno _ Programa de Auditoria _ Segurança de Sistemas _ Sistemas de Informações

ABSTRACT

Public Administration in Brazil has been coming through a process of improvement, in order to adapt itself to worldwide tendencies, which have led public agencies to invest substantially in information technologies as a means of assuring transparent governmental actions and a sound basis for decision-taking.

In the search for such a model of Public Administration, the City Hall of Belo Horizonte (Prefeitura Municipal de Belo Horizonte _ PMBH) has invested in computer resources and democratized the access to public information. In the last years, PMBH implemented various Computerized Information Systems, which include, among others, areas such as Budget, Finances, Health, Management, Planning, Traffic and Education.

The continuous use of these systems brings about the likeliness of new solutions for the management and managerial activities of PMBH. However, this computerized environment demands stricter internal control. In order to have such control, new control posts and personalized techniques of System Audit are needed to assure the integrity and safety of data.

This dissertation discusses the main techniques and areas where Systems Audit can be applied, and points out the fundamental elements of a Safety System Policy, auditing modality largely used in present times, in spite of being restrictedly used in Public Administration.

Based on such theoretical evidence, a model of System Audit was devised for the Municipal Audit (Auditoria do Município _ AUDIM), the public agency which is responsible for municipal internal audit, since the increase in the amount of

information at PMBH demands close attention of this control unity, because the analysis of data safety, trustworthiness of reports and information produced via electronic processing became a new task for this public agency.

This work also draws important conclusions about the topic and emphasizes the difficulties that must be overcome by AUDIM to audit the Information Systems of PMBH. At last, some recommendations to AUDIM were made, so that it can expand and implement its work in the area of System Audit, therefore, aiming at the use of trustworthy information for decision-taking and the contribution for a more effective and transparent Municipal Public Administration.

Keywords

Information Technologies Audit _ Systems Audit _ Internal Audit _ Internal Control _
Audit Program _ Safety Systems _ Information Systems

1 INTRODUÇÃO

1.1- Tema e Problema de Pesquisa

A globalização da economia, alavancada pelos avanços tecnológicos da informática, é uma realidade inescapável. A expansão do sistema capitalista, o aumento do comércio internacional e a internacionalização dos mercados financeiros levaram à construção de um ambiente em que a competitividade entre organizações e a busca da eficiência tornaram-se essenciais.

Neste contexto, pode-se dizer que é quase impossível às organizações, independente do porte ou ramo de atividade, manterem-se sem o auxílio dessa tecnologia, que permite que dados relevantes da entidade concentrem-se em meios informatizados, cujas informações produzidas são utilizadas no processo de tomada de decisões.

Não se deve entender que por serem geradas por processamento eletrônico, as informações são confiáveis, ou seja, completas e exatas. Apesar de oferecerem vantagens para as organizações, os sistemas computadorizados podem originar grandes riscos. É preciso considerar a possibilidade de ocorrerem fraudes e erros em razão tanto da enorme quantidade de dados manipulados pelos sistemas, quanto dos fatores inerentes à intervenção humana nos processos.

SÁ (1998, p.128-129) afirma que:

“é enganoso imaginar que os controles de uma empresa são bons porque são computadorizados. As estatísticas comprovam que o número de fraudes aumentou com a utilização de computadores. A probabilidade de erros e fraudes deve ser examinadas com cautela redobrada quando os sistemas de produção e de recebimento de dados se tornam demasiadamente acessíveis, podendo alterar realidades.”

As informações produzidas por estes sistemas devem ser corretas e oportunas, vez que o sucesso de uma organização depende da eficiência de suas decisões gerenciais, cuja eficácia está diretamente relacionada à qualidade das informações nas quais se baseiam. Conforme DAVIS (1974, p. 35) a qualidade da informação está vinculada à sua exatidão e tempestividade. Dessa forma, quanto mais exata, completa e oportuna for a informação, melhor será sua qualidade.

Como a informática tornou-se um meio de suporte ao tratamento dos dados das organizações, o controle sobre os meios informatizados é fundamental para permitir que as informações sejam fidedignas e que o processo pelo qual são produzidas seja seguro.

Destarte, cabe principalmente à Auditoria Interna essa atribuição, conforme definição expressa na Norma Brasileira de Contabilidade n. 12:

“auditoria interna constitui o conjunto de procedimentos técnicos que tem por objetivo examinar a integridade, adequação e eficácia dos controles internos e das informações físicas, contábeis, financeiras e operacionais da Entidade.” (CFC, 2000, p.261).

Não diferente das organizações privadas, a Administração Pública Brasileira vem passando por um processo de aperfeiçoamento, procurando adaptar-se às tendências mundiais. A exemplo disso, através do Decreto Presidencial n. 3.294 de 15 de dezembro de 1999, foi instituído o Programa Sociedade da Informação. Este programa faz parte do conjunto de projetos que compõem o Plano Plurianual 2000-2003, com um aporte de recursos previsto de R\$ 3,4 bilhões¹.

Assim, vem-se investindo em tecnologias da informação como um artifício de transparência tanto para as ações administrativas como para o apoio à tomada de decisão. Com isto, amplia-se cada vez mais o uso de sistemas computadorizados nas diversas atividades da Administração Pública com o fim de proporcionar resultados eficientes e eficazes, e objetivando atender às necessidades dos cidadãos. Dessa

¹ Extraído de [http:// www.mct.gov.br](http://www.mct.gov.br)

forma, os Sistemas de Informações situam-se como instrumentos efetivos para as atividades governamentais diante dos desafios que lhe são colocados.

Contudo, problemas originados da fragilidade dos controles internos e do não cumprimento de normas ou procedimentos fazem com que a Administração Pública torne-se vulnerável e sujeita a erros e falhas, tornando-se ambiente propício para a prática de fraudes. Somente com um controle interno abrangente e eficaz sobre seus Sistemas de Informações é que a Administração Pública poderá melhorar a qualidade das informações que produz e utiliza.

Nesse sentido, a Prefeitura Municipal de Belo Horizonte (PMBH), no intuito de informatizar suas atividades, vem promovendo, através da Empresa de Informática e Informação do Município de Belo Horizonte (PRODABEL), um processo de informatização contínuo, utilizando para tanto recursos tecnológicos de vanguarda. Essa informatização crescente impõe especial atenção da Auditoria do Município (AUDIM), vez que a análise da segurança de dados, da proteção contra fraudes e perdas de dados e da exatidão e confiabilidade dos relatórios e informações produzidos via processamento eletrônico, tornou-se uma nova incumbência para tal órgão de controle.

Portanto, com o número cada vez maior de sistemas computadorizados que controlam operações de grande relevância da PMBH, torna-se imperativa a necessidade da AUDIM avaliá-los. Contudo, há um descompasso entre a atuação de tal órgão de controle interno e o ritmo dinâmico desse processo de informatização: a AUDIM não vem auditando esses Sistemas de Informações.

Essa falta de acompanhamento às mudanças tecnológicas constitui um fator preocupante, pois a AUDIM, além de não perseguir suas atribuições institucionais, deixa de examinar grande parte dos controles internos da PMBH. Portanto, a ausência de auditoria nesses ambientes informatizados constitui uma questão crítica e imprescindível a ser resolvida.

É exatamente essa não realização pela AUDIM da modalidade de Auditoria de Sistemas que constitui a problemática fundamental da presente dissertação. Assim, esta pesquisa, procurou responder às seguintes indagações:

Por que a AUDIM não vem realizando Auditoria de Sistemas?

Quais instrumentos este órgão de controle poderia adotar para avaliar os Sistemas de Informação Computadorizados da PMBH?

1.2- Justificativa e Relevância

A adequada utilização dos recursos públicos é condição indispensável para a validação e aprovação da gestão governamental pela população, sendo observada atualmente a crescente preocupação do cidadão com as contas públicas. Assim, uma Administração Pública transparente, voltada às aspirações da sociedade, vem sendo buscada. Isso tem levado as entidades públicas a realizarem investimentos expressivos em tecnologias de informação.

Na tentativa de perseguir esse modelo de administração, a PMBH vem investindo em recursos tecnológicos de informática e democratizando o acesso à informação. Nos últimos anos, a administração desta prefeitura implementou diversos Sistemas de Informações Computadorizados, que abrangem, dentre outras, as áreas de Orçamento, Finanças, Saúde, Administração, Planejamento, Trânsito e Educação. Esses sistemas têm por objetivo controlar e gerar informações necessárias à tomada de decisões.

Essa intensificação do uso de sistemas proporciona possibilidades de novas soluções à administração e gestão das atividades da PMBH. Entretanto, esse ambiente informatizado requer controles internos mais rigorosos, para os quais novos pontos de controle e novas técnicas de auditoria são necessárias para assegurar a integridade e segurança dos dados que trafegam pelos sistemas.

Uma tendência lógica desse processo é a Auditoria de Sistemas. BOVE (1995, p.162) preceitua que a Auditoria de Sistemas tem como objetivos avaliar os aspectos alusivos à eficácia, economicidade, eficiência e segurança do sistema, bem como à integridade dos dados.

Sem os procedimentos de auditoria, uma política de segurança dos Sistemas de Informações torna-se frágil e vulnerável a diversos riscos, como furtos e alterações de informações, perda de produtividade e dados, sabotagens, fraudes financeiras, violações de correio eletrônico e interrupção de funcionamento de aplicativos. Tal quadro ensejaria a produção e utilização de informações fragmentadas e incorretas, prejudicando não só a transparência buscada pela Administração Municipal como também a gestão dos serviços públicos, tendo por consequência a redução da qualidade no atendimento da sociedade.

Conforme os arts. 10 e 11 da Lei Municipal n. 8.146, de 29 de dezembro de 2000, à AUDIM compete as atribuições institucionais de executar a auditoria interna preventiva e de controle nas áreas administrativa, contábil, financeira, orçamentária, patrimonial, operacional e de custos nos órgãos e entidades do Poder Executivo Municipal, observando a legislação aplicável, bem como normas, planos, programas e procedimentos estabelecidos.

Não obstante, o órgão atua de forma a assegurar que se cumpram os princípios constitucionais da legalidade, impessoalidade, moralidade, publicidade e razoabilidade, todos acolhidos pela Lei Orgânica Municipal (LOM).

Neste sentido, a AUDIM, enquanto órgão responsável pela auditoria interna, deve proceder à avaliação dos Sistemas de Informações da PMBH, objetivando assegurar, em última instância, a utilização, pelo gestor público, de informações confiáveis. Ante o exposto, faz-se necessário promover um estudo das áreas de atuação e das técnicas de Auditoria de Sistemas, bem como do arcabouço teórico e jurídico, para que tal atribuição possa ser cumprida.

Portanto, esta pesquisa justifica-se, em termos práticos, pela intenção de se identificar instrumentos de Auditoria de Sistemas que adotados pela AUDIM, possam contribuir para a qualidade e segurança dos Sistemas de Informações da PMBH, propiciando ao gestor municipal a utilização de informações fidedignas para a tomada de decisões, o que contribuirá para uma Administração Pública mais eficiente, eficaz e transparente.

Esta pesquisa justifica-se também, em termos teóricos, pelo desenvolvimento do conhecimento, especialmente no que diz respeito à Auditoria e Segurança de Sistemas de Informação Computadorizados, atividades de ampla aplicação contemporânea, porém, de histórico restrito no campo da Administração Pública.

1.3- Objetivos da Pesquisa

A seguir, estão relacionados os objetivos desta pesquisa, divididos em: geral e específicos.

1.3.1- Objetivo Geral

O objetivo geral desta pesquisa é construir um Modelo de Auditoria de Sistemas para a AUDIM.

1.3.2- Objetivos Específicos

Em termos específicos, os objetivos alcançados podem ser assim sumarizados:

- a)** identificar os principais Sistemas de Informação Computadorizados da PMBH;
- b)** modelar a AUDIM, descrevendo o histórico, finalidades, estrutura organizacional, corpo técnico de auditores, procedimentos adotados e as modalidades de auditoria realizadas pela organização;
- c)** detectar os fatores que inibem a AUDIM de auditar os Sistemas de Informação Computadorizados da PMBH.

- d) identificar instrumentos de Auditoria de Sistemas e elementos de uma Política de Segurança de Sistemas de Informações.

O objeto do segundo objetivo específico consiste em efetuar um modelo² narrativo, no qual será descrita a realidade da organização AUDIM. STAIR (1998, p. 10-11) define modelo como uma abstração ou uma aproximação que é usada para simular a realidade.

1.4- Organização da Dissertação

Para expor o proposto nesta dissertação de maneira lógica e ordenada, propiciando ao leitor a efetiva compreensão do tema abordado, este trabalho foi constituído pelos capítulos adiante especificados.

O Capítulo 1 apresenta o tema escolhido para o estudo, a problemática que lhe deu origem, sua justificativa e relevância em termos práticos e teóricos e os objetivos da pesquisa.

O Capítulo 2 traz a metodologia utilizada para a realização deste trabalho, apresentando o escopo da mesma. Define o tipo da pesquisa praticada, demonstrando os métodos de coleta e de análise de dados que foram empregados, bem como a população estudada.

No Capítulo 3, são abordados aspectos relativos aos Sistemas de Informação, apresentando seu conceito e tipos. Finalizando o capítulo, são identificados os Sistemas de Informação Computadorizados da PMBH.

O Capítulo 4 versa sobre Segurança dos Sistemas de Informação, apresentando sua definição, objetivos e modalidades. Em seguida, são enfocados a Política de Segurança dos Sistemas de Informação e os Riscos e Impactos a que estes sistemas

² Para maiores informações sobre modelo, ver seção 6.5.

estão sujeitos. São dispostas, ainda, as principais Medidas de Segurança para os Sistemas de Informação e os tópicos essenciais de um Plano de Contingências.

O Capítulo 5 destina-se ao Controle Interno, mostrando seus objetivos, modalidades, características e importância dentro da organização. Indica a Auditoria Interna como a atividade de revisão e avaliação do controle. Aponta o controle interno na Administração Pública Municipal, especialmente na de Belo Horizonte, destacando a AUDIM como órgão de controle interno.

O Capítulo 6 explora o campo da Auditoria Interna, definindo esta como um elemento essencial do controle interno. Descreve sua evolução sucintamente e destaca seu conceito, seus objetivos e modalidades. O capítulo termina evidenciando o Programa de Auditoria Interna como um instrumento que contém as informações sobre o objetivo e o escopo da auditoria a ser executada, indicando os procedimentos a serem aplicados e dirigindo de maneira eficiente o trabalho do auditor.

O Capítulo 7 trata especificamente da Auditoria de Sistemas. Inicialmente, são destacados seu conceito e seus objetivos. Posteriormente, são enfocadas as normas que regulamentam essa modalidade de auditoria e as técnicas utilizadas na execução de um trabalho. Finalizando o capítulo, apresentam-se as áreas de atuação da Auditoria de Sistemas e o perfil do Auditor de Sistemas.

No Capítulo 8, apresenta-se a entidade na qual este estudo de caso foi realizado. Inicialmente, é feita uma abordagem sobre histórico, finalidades, estrutura organizacional da AUDIM e, ainda, sobre o Auditor Municipal. Posteriormente, são apresentados os procedimentos adotados e as modalidades de auditoria realizadas pela entidade.

No Capítulo 9 são apresentados e discutidos os resultados obtidos pelo trabalho de campo, cuja intenção foi levantar a percepção dos auditores tanto sobre os Sistemas de Informação da PMBH quanto sobre os trabalhos de auditoria, assim como apurar a capacitação deste corpo de técnicos. A partir da análise desses dados, foi possível

identificar os fatores que inibem a AUDIM de realizar Auditoria nos Sistemas de Informação Computadorizados da PMBH.

Está apresentado no Capítulo 10 um Modelo de Auditoria de Sistemas para a AUDIM, construído a partir do referencial teórico apresentado nos capítulos 4, 6 e 7.

Finalizando, no Capítulo 11 é apresentada a conclusão de todo o estudo, propondo-se recomendações à AUDIM e oferecendo sugestões para futuros estudos.

2 METODOLOGIA DA PESQUISA

2.1- Introdução

Este capítulo destina-se a apresentar o detalhamento da metodologia utilizada para a condução desta pesquisa, destacando o seu escopo e demonstrando os métodos de coleta e de análise de dados que foram empregados.

2.2- Delineamento e Perspectiva da Pesquisa

O presente trabalho consiste de um estudo de caso cuja unidade de análise é a AUDIM. Para sua realização, utilizou-se uma pesquisa exploratória-descritiva, na qual foram analisados os fenômenos atuais que ocorrem na AUDIM em relação à Auditoria de Sistemas.

A pesquisa teve caráter exploratório, na medida em que se constituiu numa das primeiras tentativas de construção de um Modelo para a Auditoria de Sistemas em organizações públicas. Todavia, existem algumas publicações sobre o assunto, mas poucos são os estudos científicos já elaborados sobre o tema Auditoria de Sistemas em organizações públicas. A pesquisa também teve cunho descritivo e analítico, pois descreveu as características de um determinado problema e as relações existentes na realidade pesquisada.

YIN (1984, p.15) relata que dentre os melhores e mais reconhecidos estudos de caso já desenvolvidos vários foram exploratórios e descritivos, o que confirma a utilização de um estudo de caso para uma pesquisa descritiva. O autor acrescenta que os estudos de

caso são extremamente usados nas pesquisas das ciências sociais, sendo uma tática habitualmente adotada em dissertações de mestrado e teses de doutorado.

Para POZZEBON & FREITAS (1997, p. 3), o estudo de caso examina um fenômeno em seu ambiente natural, através do uso de vários métodos de coleta de dados, objetivando alcançar informações de uma ou mais entidades. Para os autores, essa estratégia de pesquisa possui caráter exploratório.

Nesta pesquisa, foram utilizadas técnicas de análise qualitativa de dados. Conforme POZZEBON & FREITAS (1998, p. 1), os estudos qualitativos são eficazes na exploração de dados e descoberta de resultados com maior riqueza e são mais próximos da realidade que se quer compreender.

Segundo YIN (1984, p.11), os métodos qualitativos e, em especial, os estudos de caso dependem intrinsecamente da integração do pesquisador com o ambiente pesquisado, de sua habilidade na seleção da unidade de análise e dos métodos de coleta de dados. TRIVIÑOS (1987, p.128-133) menciona fatores que caracterizam a pesquisa qualitativa:

- a)** a pesquisa qualitativa tem ambiente natural como fonte direta dos dados e o pesquisador como instrumento-chave;
- b)** a pesquisa qualitativa é descritiva;
- c)** os pesquisadores qualitativos estão preocupados com o processo, e não somente com os resultados; e
- d)** os pesquisadores tendem a analisar seus dados indutivamente.

Os autores POZZEBON & FREITAS (1998, p. 3-4) mencionam as condições basilares para a condução de pesquisas qualitativas quando se procura impor um maior rigor metodológico. São elas:

- a)** fundamentar a escolha da unidade de análise;
- b)** apresentar quesitos para a definição do número de casos;

- c) apresentar os procedimentos utilizados na construção dos instrumentos de pesquisa; e
- d) organizar um protocolo para a execução da pesquisa.

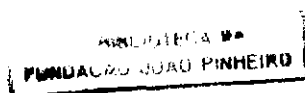
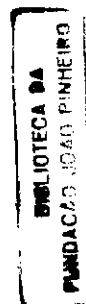
POZZEBON & FREITAS (1997, p.13) destacam que a elaboração de um protocolo é uma estratégia que aumenta a confiabilidade do estudo de caso. Os autores acrescentam que o protocolo deve contemplar quatro elementos: visão geral do projeto; procedimento de campo, incluindo credenciais e acesso aos locais de pesquisa; questões específicas que o pesquisador deve ter em mente durante a coleta de dados; e guia para o relatório, documentos para a condução da coleta de dados, estrutura de registro das observações e respostas.

Ante o exposto, os objetivos e a natureza da pesquisa, o estudo de caso demonstrou ser a estratégia mais apropriada para desenvolver este trabalho.

2.3- Escolha da Organização

O Mestrado em Administração Pública oferecido pela Escola de Governo da FJP, tem por objetivo promover a formação de alto nível, teórica e técnica, dos profissionais que atuam na esfera pública e em centros de pesquisa de ensino superior. Um dos pré-requisitos para o ingresso no curso de mestrado é a elaboração de um plano de trabalho que caracterize a vinculação da atuação profissional do candidato com a área de concentração do curso de mestrado.

Como a autora desta dissertação é Auditora da PMBH e a área de concentração do mestrado é Tecnologias da Informação, optou-se pelo tema Auditoria de Sistemas, pois satisfaz as exigências da atuação profissional e a linha de pesquisa proposta. Dessa forma, a escolha da organização AUDIM tornou-se a alternativa mais coerente para realizar o estudo de caso.



Não obstante tais fatores, o fato de a pesquisadora integrar o quadro de auditores municipais facilitou a condução dos trabalhos de coleta dos dados na AUDIM.

Apesar de constituir um estudo de caso único, este é plenamente admissível, pois, conforme concluem POZZEBON & FREITAS (1998, p.11):

“mesmo que seja um caso único pode ser considerado aceitável, desde que atinja o objetivo estabelecido.”

2.4- Unidade de Análise

De acordo com YIN (1984, p. 31), a unidade de análise constitui o foco do problema de pesquisa. Dessa forma, após a análise do problema de pesquisa e, ainda, dos seus objetivos, identifica-se que a unidade de análise da pesquisa refere-se à AUDIM.

2.5- Coleta dos Dados

TRIVIÑOS (1987, p. 137) entende que:

“o processo da pesquisa qualitativa não admite visões isoladas, parceladas, estanques. Ela se desenvolve em interação dinâmica, retroalimentando-se, reformulando-se constantemente, de maneira que, por exemplo, a Coleta de Dados num instante deixa de ser tal e é Análise de Dados, e esta, em seguida, é veículo para nova busca de informações”.

Mediante este processo interativo, serão destacados os tipos de dados e as técnicas de coleta e de análise de dados utilizados nesta pesquisa.

2.6- Tipos de Dados

MARCONI & LAKATOS (1999, p. 64) discorrem que a pesquisa documental refere-se aos dados primários; a pesquisa bibliográfica, aos dados secundários. Para os

autores, documentos são, de modo geral, todos os materiais que servem como fontes para a pesquisa científica e são encontrados em arquivos públicos e particulares, fontes estatísticas e fontes não escritas. Já a pesquisa bibliográfica trata do levantamento de toda bibliografia publicada que tenha relação com o tema em estudo.

Dessa forma, os dados primários desta pesquisa foram obtidos quase que totalmente através de um estudo de caso, cujas técnicas de coleta de dados serão abordadas na seção seguinte.

Os dados secundários foram coletados por meio da pesquisa bibliográfica disponível sobre o tema em estudo e constituíram-se de livros, teses, dissertações, monografias, artigos e anais, obtidos quer em bibliotecas físicas ou virtuais, através do acesso pela rede mundial de comunicação - *Internet*. O objetivo desta coleta de dados secundários foi efetuar o levantamento do referencial teórico, com o qual se conseguiu identificar os Instrumentos de Auditoria de Sistemas e de uma Política de Segurança de Sistemas de Informações Computadorizados e, ainda, fundamentar a construção de um Modelo de Auditoria de Sistemas para a AUDIM, que é a unidade de análise deste estudo.

2.7- Coleta dos Dados Primários

As técnicas de pesquisa correspondem à parte prática da coleta de dados. Para a coleta de dados primários necessários ao desenvolvimento deste estudo, foram utilizados a pesquisa documental, a observação participante e o questionário.

2.7.1- Pesquisa documental

Foi utilizada na pesquisa documental toda a norma aplicável à AUDIM, como leis, decretos, portarias e instruções de serviço, obtidos através de arquivos em papel e em meios magnéticos deste órgão e por meio da *Internet*, principalmente pelo *site*

<http://www.pbh.gov.br>. A finalidade desta fase da coleta de dados foi obter informações institucionais do órgão objeto de estudo.

Foram utilizados também na pesquisa documental os relatórios e pareceres de auditoria, bem como os Planos Anuais de Auditoria, programas, designações e ordens de serviço expedidos pela AUDIM, compreendendo o período de junho de 1986 a dezembro de 2001. O período definido justifica-se, pois apesar de ter sido criada através do Decreto n. 4.489, de 13 de julho de 1983, somente com a Lei n. 4.476, de 30 de maio de 1986, é que a AUDIM teve instituída sua estrutura administrativa e seu funcionamento efetivo. O objetivo desta fase da coleta de dados foi verificar as modalidades de auditoria desempenhadas pela AUDIM e avaliar a intenção desse órgão de realizar Auditoria de Sistemas nos Sistemas de Informações Computadorizados da PMBH.

Para a identificação dos Sistemas de Informações Computadorizados da PMBH, foram solicitados relatórios à PRODABEL, analisados manuais de vários sistemas e, ainda, realizadas pesquisas na RMI.

2.7.2- Observação Participante

Segundo MARCONI & LAKATOS (1999, p. 93), a observação participante é a forma de observação natural, pois consiste na participação real do pesquisador com a comunidade ou grupo que investiga. Na observação deste estudo, a pesquisadora faz parte do grupo que foi investigado, vez que integra o corpo técnico de auditores da AUDIM.

O uso desta técnica, aliado à pesquisa documental, proporcionou a modelagem da AUDIM. Além disso, a observação participante, conjugada com a aplicação dos questionários, permitiu a identificação dos fatores que inibem a AUDIM de realizar Auditoria nos Sistemas de Informações Computadorizados da PMBH.

2.7.3- Questionário

O questionário é um instrumento de coleta de dados constituído por uma série ordenada de perguntas que devem ser respondidas por escrito e sem a presença do entrevistador.

A necessidade de coletar um volume grande de dados, num determinado espaço de tempo, fez com que se optasse pelo uso do questionário. Este instrumental economiza tempo, atinge maior número de pessoas simultaneamente e obtém respostas rápidas e precisas, além de oferecer um custo baixo para a sua aplicação.

Uma vez definido o instrumento de pesquisa utilizado, o procedimento seguinte foi efetuar a sua construção. Primeiramente, foi feita a divisão de assuntos a serem tratados: Sistemas de Informação Municipais, Trabalhos de Auditoria e Capacitação dos Auditores Municipais. Posteriormente, foi feita a montagem dos questionários, utilizando questões fechadas (dicotômicas e tricotômicas) e questões abertas.

Os questionários foram previamente testados em alguns auditores, para identificar erros e possíveis correções, bem como para realizar a adequação de termos usados. Esse pré-teste permitiu detectar erros, como questões dúbias. Com isso, foi possível introduzir modificações e até eliminar questões.

Concluída a revisão dos questionários, foi desenvolvido o trabalho de campo. Os questionários foram entregues já impressos, vez que alguns auditores apresentaram resistência em utilizar computadores. Contudo, ficou à disposição dos entrevistados a versão dos questionários em meio magnético (disquete) e digital (CD-ROM). A pesquisa de campo foi realizada no período de 29 de outubro a 18 de novembro de 2001.

O universo pesquisado, como já referido, é a AUDIM. Para efeito desta pesquisa, a população investigada restringiu-se ao corpo de funcionários que realizam trabalhos de auditoria. Assim, a população base do universo pesquisado foi constituída pelos

dezoito Auditores, dentre os quais um é a pesquisadora e outro é o Gerente da GETA, além do Auditor-Chefe da AUDIM.

Foram aplicados questionários a estes dezenove profissionais. Apresentam-se nos ANEXOS A e B desta dissertação os questionários utilizados, cuja elaboração levou em consideração a tentativa de responder aos objetivos da pesquisa.

O instrumental utilizado, apresenta diversas vantagens e desvantagens, conforme apresentado no QUADRO 01:

QUADRO 01-VANTAGENS E DESVANTAGENS DO QUESTIONÁRIO	
VANTAGEM	DESVANTAGEM
Economiza tempo e obtém grande número de dados.	Percentagem pequena dos questionários que voltam.
Atinge maior número de pessoas simultaneamente.	Grande número de perguntas sem respostas.
Abrange uma área geográfica mais ampla.	Não pode ser aplicado a pessoas analfabetas.
Economiza pessoal.	Impossibilidade de ajudar o informante em questões mal-compreendidas.
Obtém respostas mais rápidas e mais precisas.	A dificuldade de compreensão por parte dos informantes leva a uma uniformidade aparente.
Há maior liberdade nas respostas, em razão do anonimato.	A leitura de todas as perguntas, antes de respondê-las, podendo uma questão influenciar a outra.
Há mais segurança, pelo fato de as respostas não serem identificadas.	A devolução tardia prejudica o calendário ou sua utilização.
Há menos risco de distorção, pela não influência do pesquisador.	O desconhecimento das circunstâncias em que foram preenchidos torna difícil o controle e a verificação.
Há mais tempo para responder e em hora mais favorável.	Nem sempre é o escolhido quem responde ao questionário, invalidando, portanto, as questões.
Há mais uniformidade na avaliação, em virtude da natureza impessoal do instrumento.	Exige um universo mais homogêneo.
Obtém respostas que materialmente seriam inacessíveis.	-

FONTE- MARCONI & LAKATOS (1999, p. 100)

Dentre as desvantagens aludidas, algumas foram suplantadas nesta pesquisa, como adiante relatado:

- a) percentagem pequena dos questionários que voltam:** dos 19 questionários distribuídos 16 foram devolvidos, o que representa um índice de retorno altamente relevante, de 84,22%;
- b) grande número de perguntas sem respostas:** consta da segunda instrução para o preenchimento do questionário que todas as questões deveriam ser respondidas e justificadas quando solicitado. Mediante essas orientações, todas as questões abertas e as questões fechadas que exigiam justificativas complementares foram integralmente respondidas pelos entrevistados;
- c) não pode ser aplicado a pessoas analfabetas:** o cargo de Auditor exige Bacharelado em Ciências Contábeis; o cargo de Auditor-Chefe, curso superior em qualquer área;
- d) impossibilidade de ajudar o informante em questões mal-compreendidas:** o fato de a pesquisadora fazer parte da equipe de funcionários investigados facilitou o esclarecimento das dúvidas quanto às questões mal-compreendidas;
- e) a leitura de todas as perguntas antes de respondê-las, podendo uma questão influenciar a outra:** tentou-se erradicar, ou pelo menos minimizar, esta desvantagem, vez que consta da primeira instrução para o preenchimento do questionário que as questões deveriam ser respondidas observando-se a sequência;
- f) a devolução tardia prejudica o calendário ou sua utilização:** o calendário da elaboração da dissertação não foi prejudicado em decorrência de atraso na devolução do questionário. Conforme consta da sétima instrução para o preenchimento do questionário, foi concedido aos informantes um prazo de cinco dias úteis para responder ao questionário, a partir da data do seu recebimento;
- g) nem sempre é o escolhido quem responde ao questionário, invalidando, portanto, as questões:** conforme consta das instruções para o preenchimento do questionário, foi solicitado que o instrumento fosse respondido individualmente e de forma consciente, destacando a importância do informante para a pesquisa. Além disso, como todos os auditores receberam o questionário e devido às características das questões elaboradas, somente profissionais que trabalham

especificamente com a atividade de auditoria executada pela AUDIM teriam condições de responder. Assim, entende-se que, de fato, quem recebeu, também foi quem respondeu o questionário.

Dessa forma, foram apresentadas e definidas as técnicas de coletas de dados utilizadas nesta pesquisa. A sua interação com os objetivos da pesquisa será apresentada na seção 2.10 - Protocolo de Pesquisa.

2.8- Análise de Dados

Os dados coletados foram objeto de análise e interpretação. Segundo MARCONI & LAKATOS (1999, p. 37), análise “é a tentativa de evidenciar as relações existentes entre o fenômeno estudado e outros fatores”, enquanto interpretação “é a atividade intelectual que procura dar um significado mais amplo às respostas, vinculando-as a outros conhecimentos”.

Os dados coletados foram submetidos à análise de conteúdo e à análise estatística.

Conforme preceitua BARDIN (1977, p. 42), a análise de conteúdo consiste em:

“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”.

BARDIN (1977, p. 95) dispõe que a análise de conteúdo contempla as fases: pré-análise; exploração do material; tratamento dos resultados, inferência, e interpretação. A pré-análise consiste em organizar o material, possuindo três missões principais: escolher os documentos a serem submetidos à análise; formular hipóteses e objetivos; e elaborar os indicadores que fundamentam a interpretação final. Para a autora, estas missões não possuem ordem ou sequência definidas ou obrigatórias. Nesta pesquisa não houve a intenção de estabelecer hipóteses.

A exploração do material inicia-se já na pré-análise, quando os documentos da pesquisa são submetidos a um estudo intenso, sob orientação do referencial teórico. Esta etapa consiste em identificar opiniões afins e divergentes sobre idéias, conceitos e concepções sem base teórica.

Por fim, BARDIN (1977, p. 101) doutrina que o tratamento dos resultados, a inferência e a interpretação consistem em estabelecer quadros de resultados, diagramas, figuras e modelos, os quais condensam e colocam em destaque as informações fornecidas pela análise. Os resultados são submetidos a testes estatísticos, proporcionando deduções e interpretações a intento dos objetivos estabelecidos.

A análise estatística ocorreu após a tabulação eletrônica dos dados. Os valores foram então convertidos em pontos percentuais que originaram gráficos e tabelas, utilizando como ferramenta de apoio o *software Excel* da *Microsoft®*, para efeito de melhor condensação e representação dos dados apurados.

Com base nestes tipos de análise de dados, foi possível identificar os tópicos seguintes, relacionados com os objetivos da pesquisa:

- a)** identificação dos Sistemas de Informação Computadorizados da PMBH;
- b)** modelagem da AUDIM;
- c)** detecção dos fatores que inibem a AUDIM de realizar Auditoria nos Sistemas de Informação Computadorizados da PMBH;
- d)** identificação de instrumentos de Auditoria de Sistemas e uma Política de Segurança de Sistemas; e
- e)** construção de um modelo de Auditoria de Sistemas para a AUDIM.

Segundo POZZEBON & FREITAS (1998, p. 6), através dos dados coletados a partir de percepções do pesquisador, dos respondentes e da transcrição de documentos, é possível recriar o contexto no qual os dados foram gerados.

Assim, para a identificação dos Sistemas de Informações Computadorizados da PMBH, foi utilizada a pesquisa documental, através do exame de relatórios da PRODABEL, da análise dos manuais de vários sistemas e da realização de pesquisas na RMI. A listagem destes sistemas está disposta no capítulo 3 desta dissertação.

Para a modelagem da AUDIM, foram utilizadas a pesquisa documental e a observação participante. A obtenção das informações institucionais e dos procedimentos adotados pela AUDIM se deu pela análise de toda a norma aplicável ao órgão, como leis, decretos, portarias e instruções de serviço. As características do corpo técnico de auditores foram obtidas através da legislação pertinente e da observação participante. Para identificar as modalidades de auditoria realizadas pela AUDIM, foram examinados os relatórios, pareceres, designações e ordens de serviço arquivados referentes ao período compreendido entre junho de 1986 e dezembro de 2001. A análise das programações anuais e dos programas de auditoria, aliada à observação participante, permitiu verificar a intenção da AUDIM em proceder Auditoria de Sistemas. Este estudo de caso compõe o capítulo 8 desta dissertação.

A percepção dos auditores sobre os Sistemas de Informações Municipais e sobre os trabalhos de auditoria e ainda, a capacitação técnica dos auditores em relação à Auditoria de Sistemas foi detectada por meio dos questionários aplicados aos Auditores, ao Gerente da GETA e ao Auditor-Chefe. A partir da análise desses dados, conjuntamente com a pesquisa documental e a observação participante, foi possível identificar os fatores que inibem a AUDIM de realizar Auditoria nos Sistemas de Informações Computadorizados da PMBH. A descrição e a análise dos resultados obtidos são o objeto do capítulo 9.

Os instrumentos de Auditoria de Sistemas e uma Política de Segurança de Sistemas foram identificados nos capítulos 4 e 7. A construção de um modelo de Auditoria de Sistemas para a AUDIM foi pautada no referencial teórico, especificamente nos capítulos 4, 6 e 7. Este modelo está apresentado no capítulo 10 desta dissertação.

2.9- Delimitação da Pesquisa

Delimitar a pesquisa é estabelecer limites para a investigação. Neste estudo, o universo pesquisado contempla a AUDIM. Para efeito desta pesquisa, a população investigada restringiu-se ao corpo de funcionários que realizam trabalhos de auditoria. Assim, a população base do universo pesquisado foi constituída pelos dezoito auditores, incluindo esta pesquisadora e o Gerente da GETA. Salienta-se que neste grupo não estava incluído um auditor afastado por licença sem vencimentos.

Foi entregue o questionário também ao Auditor-Chefe do Município, que não faz parte da equipe permanente de auditores, mas ocupa cargo político com *status* de Secretário Municipal. Destarte, por constituir uma população relativamente pequena, esta foi investigada em sua totalidade.

2.10- Protocolo da Pesquisa

Como já mencionado na seção 2.2, os autores POZZEBON & FREITAS (1997, p.13) destacam que a elaboração de um protocolo é uma estratégia que reforça a confiabilidade do estudo de caso.

Assim, de acordo com as sugestões e considerações desses autores, foram organizados três protocolos de pesquisa: o protocolo das etapas da pesquisa; o protocolo dos instrumentos da coleta de dados; e o protocolo da sequência das atividades adotadas.

O protocolo das etapas da pesquisa (FIG. 01) demonstra a coleta de dados e a análise destes como fases sequenciais. Todavia, estes fatos ocorreram muitas vezes simultaneamente.

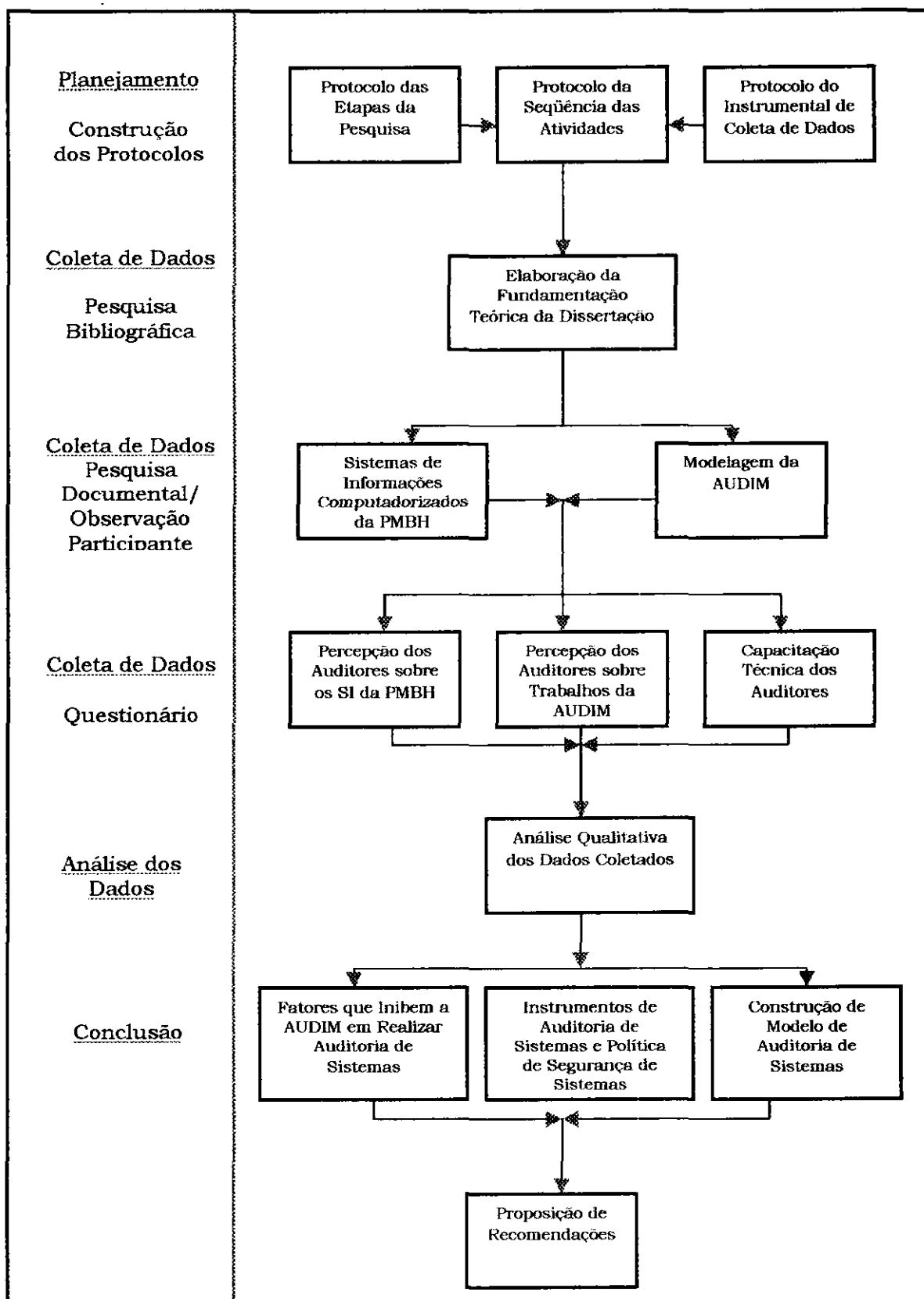


FIGURA 01 - Protocolo das etapas da pesquisa

FONTE - Elaborado pela autora.

O protocolo dos instrumentos de coleta de dados, apresentado no QUADRO 02, esboça as fontes dos dados utilizados, relacionado-as com os objetivos desta pesquisa.

QUADRO 02-PROTOCOLO DO INSTRUMENTAL DA COLETA DE DADOS

N.	INSTRUMENTAL	OBJETIVO	FONTE	REFERENCIAL
1	Pesquisa Bibliográfica	Efetuar a fundamentação teórica da dissertação	Acervo publicado sobre o tema em estudo	Livros, teses, dissertações, monografias, artigos e anais
2	Pesquisa Documental	Identificar os sistemas de informação computadorizados da PMBH	Intranet e documentos da PRODABEL	RMI, relatórios da PRODABEL e manuais dos sistemas de informação
3	Pesquisa Documental	Modelar a AUDIM: obter informações institucionais da AUDIM	Normas aplicáveis a AUDIM	Leis, decretos, portarias e instruções de serviço
4	Pesquisa Documental	Modelar a AUDIM: verificar as modalidades de auditoria e a intenção da AUDIM em realizar Auditoria de Sistemas	Documentos da AUDIM	Relatórios, pareceres, programas, roteiros, planos anuais, designações e ordens de serviço
5	Observação Participante	Modelar a AUDIM: percepção da pesquisadora sobre o órgão	Observação direta sobre o órgão	Operações diárias dos auditores, Gerente da GETA e Auditor-Chefe
6	Questionário	Identificar a percepção dos Auditores sobre os SI da PMBH	Auditores e Auditor-Chefe	Elaboração da pesquisadora
7	Questionário	Identificar a percepção dos Auditores sobre Trabalhos da AUDIM	Auditores e Auditor-Chefe	Elaboração da pesquisadora
8	Questionário	Identificar a capacitação dos Auditores	Auditores e Auditor-Chefe	Elaboração da pesquisadora

FONTE- Elaborado pela autora.

O protocolo da sequência das atividades (QUADRO 03) discrimina os procedimentos adotados, relacionado-os com os objetivos desta pesquisa.

QUADRO 03-PROTOCOLO DA SEQUÊNCIA DE ATIVIDADES

N.	ATIVIDADE ADOTADA	OBJETIVO
1	Instrumental 1	Efetuar a fundamentação teórica da Dissertação
2	Instrumental 2	Identificar os sistemas de informação computadorizados da PMBH
3	Instrumental 3	Modelar a AUDIM: obter informações institucionais da AUDIM
4	Instrumental 4	Modelar a AUDIM: verificar as modalidades de auditoria e a intenção da AUDIM em realizar Auditoria de Sistemas
5	Instrumental 5	Modelar a AUDIM: percepção da pesquisadora sobre o órgão
6	Instrumental 6	Identificar a percepção dos auditores sobre os SI da PMBH
7	Instrumental 7	Identificar a percepção dos auditores sobre os trabalhos da AUDIM
8	Instrumental 8	Identificar a capacitação técnica dos auditores em relação à Auditoria de Sistemas
9	Análise dos dados coletados	Análise qualitativa e quantitativa dos dados coletados
10	Estabelecer conclusões e propor recomendações	-Identificar fatores que inibem a AUDIM em realizar Auditoria de Sistemas; -Identificar instrumentos de Auditoria de Sistemas e de uma Política de Segurança de Sistemas; -Construção de Modelo de Auditoria de Sistemas para a AUDIM; -Propor recomendações para a AUDIM

FONTE- Elaborado pela autora.

Entretanto, estes procedimentos ocorreram muitas vezes concomitantemente.

2.11- Conclusão

Este capítulo apresentou a metodologia empregada para conduzir este estudo. Mediante a exposição dos objetivos e da natureza da pesquisa, o método do estudo de caso e as técnicas utilizadas para a coleta e análise dos dados demonstraram constituir o instrumental de pesquisa mais apropriado para realizar este trabalho. No capítulo seguinte, inicia-se o referencial teórico desta pesquisa.

3 SISTEMAS DE INFORMAÇÕES

3.1- Introdução

Este capítulo compõe com os quatro seguintes o referencial teórico desta dissertação. Destarte, a teoria que conduziu a pesquisadora às conclusões e à construção do modelo apresentado no capítulo 10 está aqui organizada e resumida.

Neste capítulo, serão abordados os aspectos relativos aos Sistemas de Informações. Inicialmente, faz-se uma breve referência à informação e aos sistemas. Posteriormente, é focado o Sistema de Informações, seu conceito e classificação. Serão dispostos, também, os Sistemas de Informações Computadorizados.

Finalizando o capítulo, serão identificados os Sistemas de Informações na Prefeitura Municipal de Belo Horizonte, buscando responder ao primeiro objetivo específico desta pesquisa.

3.2- Informação

Para MCGEE & PRUSAK (1994, p.3), "o mundo industrializado vem enfrentando a transição de uma economia industrial para uma economia de informação". Os autores acreditam que "nas próximas décadas, a informação, mais do que a terra ou o capital, será a força motriz na criação de riquezas e prosperidade".

Freqüentemente, as palavras **dado** e **informação** são usadas de modo intercambiável, assumindo, o mesmo significado. Entretanto, os dois termos são distintos, segundo diversos autores:

QUADRO 04- CONCEITOS DE DADOS E DE INFORMAÇÕES

AUTOR	DADO	INFORMAÇÃO
ALTER (1996, p.28-29)	“São fatos, imagens e sons que podem ou não ser conexos ou proveitosos para uma determinada tarefa.” (*)	“É um dado cuja forma e conteúdo são adequados para um determinado uso.” (*)
DAVIS (1974, p.32)	“É a matéria-prima para a informação, e é definido como o grupo de símbolos que representam quantidades, ações, letras e números.” (*)	“É o dado processado de forma significativa para o destinatário.” (*)
STAIR (1998, p.4)	“São fatos no formato elementar.” (*)	“É um conjunto de fatos organizados que adquirem valor acessório além do valor do fato em si.” (*)
ZWASS (1992, p 14-15)	“É o material cru a partir do qual se obtêm informações.” (*)	“É um incremento do conhecimento.” (*)

FONTE- Elaborado pela autora da dissertação.

(*) Tradução da autora.

Assim, os dados podem ser considerados como números ou fatos brutos, que depois de organizados e processados transformam-se em informações (FIG. 02).

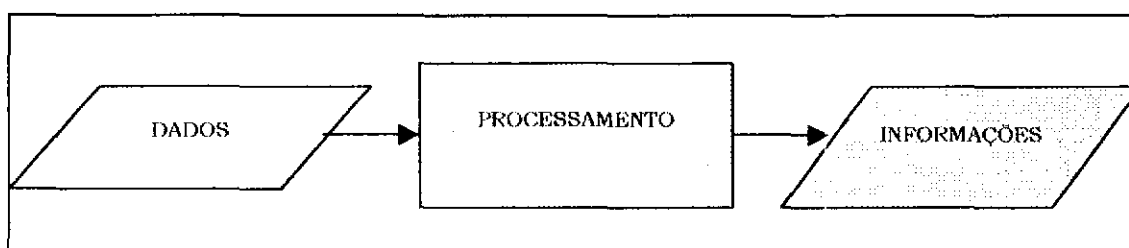


FIGURA 02- Transformação de dados em informações

FONTE- DAVIS 1974, p 32 (adaptada).

BURCH (1994, p.24) diz que a função básica da informação é aumentar o conhecimento ou diminuir a incerteza do usuário, quer seja o setor privado, o setor público ou o próprio cidadão. Para tanto, é necessário que a informação apresente certos atributos. ZANOTELI (2001, p.54), ao pesquisar diversos autores de Sistemas

de Informações, estabeleceu os principais atributos da informação, os quais podem ser visualizados no QUADRO 05.

QUADRO 05- ATRIBUTOS DA INFORMAÇÃO

ATRIBUTO	DEFINIÇÃO
Apresentação	Diz respeito ao estilo e à forma como a informação é disponibilizada, evidenciada. Estes devem ser simples e compreensíveis o suficiente para que a informação seja entendida e possa efetivamente ser útil na tomada de decisões;
Contextualização	Detalhamento da fonte da informação e sua comparação com o histórico que a cerca. Consiste em demonstrar o ambiente em que está inserida a informação, inclusive com suas interações.
Custo x Benefício	A informação deve apresentar um custo (gastos na obtenção da informação) menor que os seus benefícios (valor da informação).
Oportunidade	A informação tem que ser disponibilizada quando necessário, no momento oportuno, mantendo-se atualizada quando disponível.
Relevância	A informação é relevante se for necessária para a tomada de decisões. Como consequência, deve reduzir a incerteza e aumentar a qualidade da decisão tomada. A informação torna-se ainda mais relevante quando permite projeções — valor preditivo.
Completude	A informação deve abranger todos os aspectos relevantes da situação em análise
Concisão	A informação é concisa quando apresenta o essencial, aquilo que é importantes para o tomados de decisão, simplesmente o necessário a cada usuário.

FONTE- ZANOTELI 2001, p.54 (adaptado).

Portanto, a informação torna-se um instrumento básico para a organização, colaborando positivamente na relação custo/benefício e ainda, servindo como um elemento fundamental a gerência das atividades administrativas, econômicas, financeiras, políticas e sociais desta instituição.

DAVIS (1974, p. 35) preceitua que a qualidade da informação está diretamente relacionada com sua exatidão, completude e tempestividade. Para STONER & FREEMAN (1999, p. 489) quanto mais precisa a informação, maior sua qualidade e com mais segurança os administradores podem contar com ela para a tomada de decisões.

Através de sistemas, as informações são transformadas em uma forma utilizável para seus usuários, possibilitando a tomada de decisões .

3.3- Sistema

O termo **sistema** é definido por diversos autores, como apresentado no QUADRO 06.

QUADRO 06- CONCEITOS DE SISTEMA

AUTOR	CONCEITO
ALTER (1996, p.56)	“Constitui um conjunto de elementos que interagem entre si para realizar um propósito.” (*)
DAVIS (1974, p.82)	“É a composição de partes que interagindo, operam juntas para alcançar algum objetivo ou propósito.” (*)
STAIR (1998, p.6)	“É um conjunto de componentes que interagem para alcançar um objetivo.” (*)
ZWASS (1992,p 18)	“É um conjunto de subsistemas que operam juntos para atingir objetivos comuns.” (*)

FONTE- Elaborado pela autora da dissertação.

(*) Tradução da autora.

Diante dessas definições, o sistema pode ser entendido como um conjunto de elementos relacionados que interagem na perseguição de objetivos e ideais comuns.

Existem dois tipos de sistemas: o **sistema fechado** e o **sistema aberto**. A partir do estudo das acepções dos autores [STAIR (1998, p. 8), BIO (1985, P. 17-20) e DAVIS (1974, p.86-88)] pode-se definir a natureza desses sistemas.

Um sistema fechado é aquele que se presume estar isolado de seu meio ambiente. Desta forma, não possui interações externas.

Um sistema aberto é aquele que tem uma interação externa muito significativa, sem a qual não funcionaria. Os sistemas abertos são aqueles que recebem fontes externas, processando-as e fornecendo o produto final. Afetam e são afetados também por seu meio ambiente.

Todo sistema funciona a partir de três atividades basilares: entrada (*input*), processamento (*throughputs*) e saída (*output*). Outros sistemas ainda têm uma quarta atividade, denominada retroação (*feedback*). Este funcionamento é representado na FIG. 03.

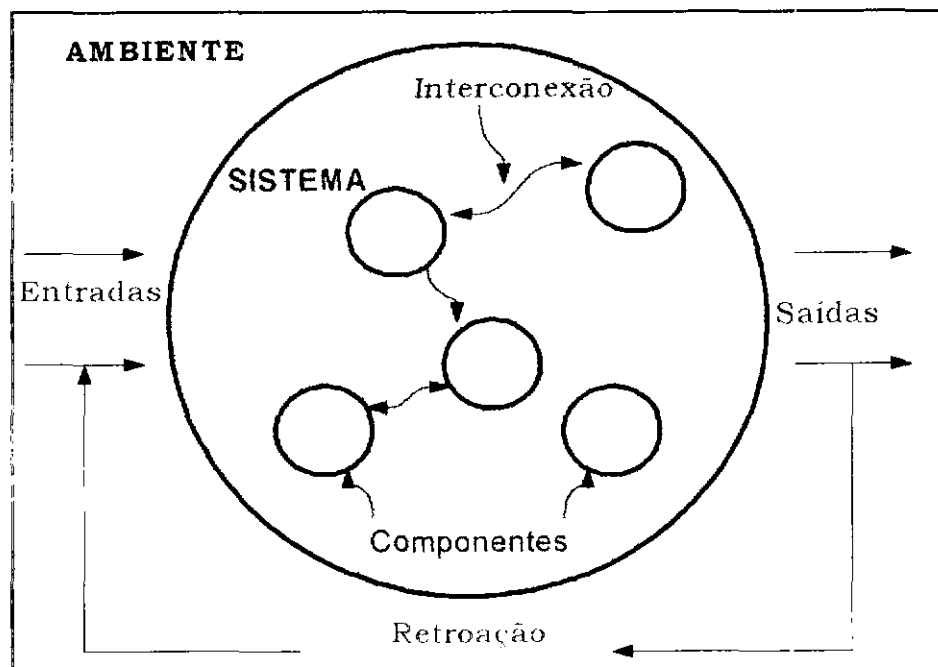


FIGURA 03- Funcionamento de um Sistema

FONTE- ZWASS 1992, p. 18 e BERTALANFFY, 1975, p.66 (adaptada).

Destarte, conclui-se que entrada é tudo o que será processado para alcançar determinado objetivo; processamento é o meio pelo qual este objetivo será atingido; e

saída é o resultado deste processamento. A retroação, segundo BERTALANFFY (1975, p.66) constitui o processo no qual parte da saída é reenviada de volta, como realimentação para a entrada.

3.4- Sistema de Informações

3.4.1- Definição

Os Sistemas de Informações estão direcionados à geração de informações para a tomada de decisões. Dessa forma, e segundo seu escopo, diversos Sistemas de Informações vão surgir para atender às necessidades de seus usuários. Como exemplo, pode-se citar o Sistema de Informações Contábeis e o Sistema de Informações de Recursos Humanos. O QUADRO 07 apresenta conceitos de Sistema de Informações.

QUADRO 07- CONCEITOS DE SISTEMA DE INFORMAÇÕES

AUTOR	CONCEITO
ALTER (1996, p.2)	“É um sistema que utiliza tecnologia para coletar, transmitir, registrar, restabelecer, manipular e apresentar informações usadas em um ou mais processos de negócios.” (*)
LAUDON & LAUDON (1999, p 4)	“É o conjunto de componentes inter-relacionados, trabalhando juntos para coletar, recuperar, processar, armazenar e distribuir informação com a finalidade de facilitar o planejamento, o controle, a coordenação, a análise e o processo decisório em empresas e organizações.”
STAIR (1998, p 11)	“É o conjunto de elementos inter-relacionados que coletam, manipulam, registram e difundem os dados e informações, fornecendo um mecanismo de retroação.” (*)

FONTE- Elaborado pela autora da dissertação.

(*) Tradução da autora.

Apesar de divergirem em um ou outro aspecto, os autores citados apresentam uma conclusão comum: o Sistema de Informações é um conjunto de recursos que transforma dados em informações, satisfazendo às necessidades dos usuários e organizações. Portanto, os Sistemas de Informações tornam-se importantes, vez que

podem ser um dos meios pelos quais as organizações podem alcançar seus objetivos precípuos, podendo, ainda, ser considerados como elemento diferencial de vantagem concorrente.

LAUDON & LAUDON (1999, p. 5) afirmam que um Sistema de Informações é composto de organizações, pessoas e tecnologia que devem interagir para que o sistema atinja seu objetivo. Na FIG. 04, observa-se a composição dos Sistemas de Informações e destaca-se a interação desses componentes entre si e com o ambiente externo:

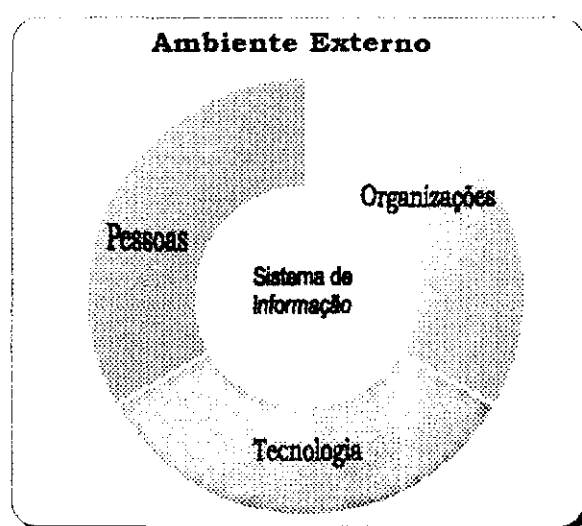


FIGURA- 04: Componentes dos Sistemas de Informações

FONTE- LAUDON & LAUDON, 1999, p. 5

Os autores ainda acrescentam acerca desses recursos:

- a) Organização: as organizações moldam os sistemas de informações, vez que estes existem para satisfazer às necessidades das organizações. A estrutura organizacional, o estilo de gerência e a cultura são exemplos deste tipo de recurso.
- b) Pessoas: são os usuários dos sistemas de informações, tanto aqueles que usam as informações provenientes desses sistemas quanto aqueles responsáveis pela entrada de dados.

- c) Tecnologia é o meio pelo qual os dados são transformados e organizados para uso das pessoas. Um sistema de informações pode ser manual, usando somente a tecnologia do lápis e papel. Todavia, os computadores substituíram a tecnologia manual de processamento de grandes volumes de dados e de trabalhos complexos de processamento.

A seção seguinte discorre sobre os Sistemas de Informações baseados em computadores, ou seja, aqueles sistemas que se baseiam em alguma forma de tecnologia de computação para entrada, saída, processamento e armazenamento de dados.

3.5. Sistemas de Informações Computadorizados

A tecnologia trouxe grandes modificações ao modo como as organizações conduzem suas atividades. Com o uso de Sistemas de Informações computadorizados, a tomada de decisão dentro das empresas passou a ser cada vez mais facilitada.

Um sistema computadorizado é um conjunto de componentes interatuantes, logicamente estruturado, formando um todo complexo capaz de receber dados como *input* e processá-los com a ajuda de um programa compilador de linguagem, fornecendo, a seguir, o produto final, apresentando-o como *output* do sistema (IMONIANA, 1994, p.23).

Segundo PRESSMAN (2000, p. 179), os elementos de um sistema baseado em computador freqüentemente incluem *software*, *hardware*, pessoas, banco de dados, documentação e procedimentos. Estes elementos são apresentados no QUADRO 8.

QUADRO 8- ELEMENTOS DE UM SISTEMA COMPUTADORIZADO

ELEMENTO	CONCEITO
<i>Software</i>	Consiste em algoritmos (instruções detalhadas que dizem como fazer algo) e suas representações para o computador, ou seja, os programas.
<i>Hardware</i>	Compreende os dispositivos físicos que fornecem capacidade ao computador e que oferecem funções ao mundo externo.
Pessoas	As pessoas são os usuários e operadores de <i>hardware</i> e <i>software</i> .
Banco de Dados	O banco de dados é uma grande e organizada coleção de informações a que se tem acesso pelo <i>software</i> e faz parte integrante da função do sistema.
Documentação	A documentação consiste em manuais, formulários e outras informações descritivas que retratam o uso e/ou operação do sistema.
Procedimentos	Os procedimentos constituem os passos que definem o uso específico de cada elemento do sistema ou o contexto processual em que o sistema reside.

FONTE- PRESSMAN 2000, p. 179-180

PRESSMAN (2000, p. 181) ainda explica, que o *software* pode ser classificado como *software de sistema* e *software aplicativo*. O *software* de sistema gerencia os recursos do computador como a unidade central de processamento e os periféricos. O *software* aplicativo consiste em programas elaborados para determinada aplicação, como um programa de processamento de folha de pagamentos.

Para TANENBAUM (2000, p. 8), um sistema de *hardware* compõe-se de uma Unidade Central de Processamento (UCP), de um armazenamento principal, de dispositivos de entrada e de saída e de armazenamento secundário.

A UCP é o componente que efetivamente efetua o processamento de instruções programadas. É composta por uma unidade de controle, que controla e coordena os demais componentes do computador, e por uma unidade lógico-aritmética, que executa operações aritméticas e lógicas sobre os dados.

O armazenamento principal, também chamado de **memória principal**, armazena instruções de programas e os dados que estão sendo utilizados por essas instruções. Esta memória divide-se em *Random Access Memory* (RAM), que é utilizada para

armazenamento de dados ou instruções programadas por curto espaço de tempo, e *Read Only Memory* (ROM), é uma memória apenas de leitura que armazena permanentemente as instruções importantes de programas.

Os dispositivos de entrada e saída permitem a interação dos seres humanos com os computadores. Os dados podem ser introduzidos diretamente em sistema de computados utilizando-se teclado, disquetes, Cd-Rom, *touch screens* (telas sensíveis ao toque), scanners digitais, mouse de computador, reconhecimento de caracteres óticos e dispositivos de entrada por voz. Como tecnologias de saída citam-se terminais de vídeo, impressoras e saída de áudio.

O armazenamento secundário refere-se à retenção por prazos relativamente prolongados de dados fora da UCP e do armazenamento principal. O armazenamento secundário não é volátil, ou seja, ele conserva os dados ainda que a energia elétrica seja desligada. As principais tecnologias deste tipo de armazenamento são a fita magnética, o disco magnético (disquete) e o disco ótico (CD-Rom).

A estes elementos de um sistema baseado em computador LAUDON & LAUDON (1999, p. 6) acrescentam os dispositivos de comunicações, que possibilitam que o computador seja interligado a redes de comunicação.

Segundo LEMOS (1995, p.10), “uma rede de computadores é formada por um conjunto de módulos processadores capazes de trocar informações e compartilhar recursos, interligados por um sistema de comunicação. O sistema de comunicação é um arranjo topológico (arranjo físico que compõem a rede), interligando os vários módulos processadores através de enlaces físicos (meios de transmissão) e de um conjunto de regras com o fim de organizar a comunicação (protocolos).”

Dessa forma, os dispositivos de comunicações necessários para que um computador seja interligado a redes de comunicação são a topologia, os meios de transmissão e o protocolo de comunicação.

LAUDON & LAUDON (1999, p. 150) apresentam as três topologias de rede mais comuns: a rede em estrela, que é controlada por um computador principal interligado a todos outros dispositivos da rede; a rede em barramento, que interliga os equipamentos por meio de um circuito e a rede em anel onde o canal de conexão de forma circular, permite que cada componente da rede se comunique diretamente com qualquer um dos outros.

Quanto aos meios de transmissão, TANENBAUM (1997, p. 93-98) descreve: o par trançado, que consiste em fios de cobre torcidos em pares; o cabo coaxial, fio de cobre encapsulado por um material isolante; fibras óticas, fios de fibra de vidro transparente; microondas, sinais de rádio de alta frequência através da atmosfera; e os satélites de comunicação. Ainda segundo este autor, alguns dos protocolos padrões utilizados são o *Transmission Control Protocol/Internet Protocol* (TCP/IP) e o *Integrated Services Digital Network* (ISDN).

Além dos elementos que compõem um sistema baseado em computador, outro fator relevante é a modalidade do processamento dos dados desses Sistemas de Informações. Segundo CAUTELA (1996, p. 177-200), as principais modalidades de processamento dos dados de Sistemas de Informações computadorizados são as seguintes:

- a) *Processamento em Batch*: nesta modalidade os dados são processados por lotes(*batch*), isto é, as informações são acumuladas durante um período preestabelecido. Formado o lote, este é processado de uma vez.
- b) *Processamento em Real Time On-line*: o processamento em *real time on-line* vale-se da capacidade de acesso direto e instantâneo aos dados oferecidos pelos computadores. Este tipo de processamento oferece acesso a dados armazenados pelo sistema sempre atualizados, através de terminais locais, situados próximos ao computadores, ou remotos, situados a grandes distâncias.
- c) *Processamento em Batch Remoto*: esta modalidade de processamento é uma combinação do processamento em *Real Time on-line* e do *Batch*, pois o processamento é feito à distância com a utilização de terminais, mas a intervalos pequenos, o que faz com que se acumulem pequenos lotes de informações.

- d) **Processamento Distribuído:** o uso de vários computadores ligados por uma rede de comunicação é chamado de processamento distribuído.

Por facilitarem a produção, gerenciamento e utilização de informações, os Sistemas Computadorizados estão cada vez mais presentes nas organizações, sejam privadas ou públicas. Na seção seguinte são apresentados os Sistemas de Informações Computadorizados utilizados na Prefeitura Municipal de Belo Horizonte.

3.6- Sistemas de Informações da Prefeitura Municipal de Belo Horizonte

A Administração Pública Brasileira vem adaptando seu aspecto e suas capacidades às tendências mundiais. Comprova tal afirmação o grande impulso que ocorreu na década de 90 da *Internet* brasileira, primeiramente na comunidade científica e, logo após, como plataforma de expansão do setor privado. Nas telecomunicações, houve a privatização de todo o sistema brasileiro e a criação da Agência Nacional de Telecomunicações (ANATEL)³. O conjunto desses fatores está permitindo maior agilidade na disponibilidade de acesso aos meios de comunicação.

Em 1999, através do Decreto Presidencial n. 3.294 de 15 de dezembro foi instituído o **Programa Sociedade da Informação**, concebido a partir de um estudo conduzido pelo Conselho Nacional de Ciência e Tecnologia e que faz parte do conjunto de projetos que compõem o **Plano Plurianual 2000-2003**, com um aporte de recursos previsto de R\$ 3,4 bilhões⁴, sendo coordenado pelo Ministério da Ciência e Tecnologia. O objetivo deste Programa é integrar, coordenar e fomentar ações para a utilização de tecnologias de informação e comunicação, de forma a contribuir para a inclusão social de todos os brasileiros na nova sociedade e, ao mesmo tempo, contribuir para que a economia do País tenha condições de competir no mercado global. A execução do Programa pressupõe o compartilhamento de responsabilidades entre os três setores: governo, iniciativa privada e sociedade civil.

³ Extraído de [http:// www.mct.gov.br](http://www.mct.gov.br)

⁴ Extraído de [http:// www.mct.gov.br](http://www.mct.gov.br)

Paralelamente a essa iniciativa, é cada vez maior a utilização de Sistemas de Informações Computadorizados nas diversas atividades da Administração Pública Brasileira com a intenção de provocar resultados eficientes e eficazes, e atender às necessidades e direitos da sociedade. Dessa forma, os Sistemas de Informações instituem-se como instrumentos efetivos e como um aspecto de contínua importância para os governos federal, estaduais e municipais e para a sociedade. Ou seja, a informação governamental é um recurso nacional valioso, pois contempla o público com conhecimentos do governo, da sociedade e da economia.

Portanto, o investimento em tecnologias da informação tornou-se um elemento de *transparência tanto para os atos administrativos como para o apoio à tomada de decisão* dos gestores públicos.

Na tentativa de perseguir esse modelo de administração, a PMBH vem investindo em recursos tecnológicos de informática e democratizando o acesso à informação. A PRODABEL coordena a informática pública na PMBH, com o objetivo de possibilitar ao cidadão, por meio da democratização do acesso à informação e da disponibilização de recursos tecnológicos, a garantia do direito à informação pública, de um atendimento público mais ágil e de uma maior participação na gestão pública.

Em 1993, a PRODABEL iniciou o processo de reestruturação de seu ambiente de telecomunicações e de informática. A partir daí foi efetivado um processo de descentralização do ambiente informacional da PMBH, que até então era baseado em equipamentos de grande porte (*mainframe*), instalados na PRODABEL e em terminais distribuídos nos órgãos municipais (ANEXO C). Para o suporte deste ambiente descentralizado foi implantada uma rede de comunicação de dados em âmbito municipal: a Rede Municipal de Informática (RMI). Hoje, a RMI está presente em 236 locais da Prefeitura, totalizando 64%, com 4.554 equipamentos interconectados e aptos à utilização de qualquer serviço, inclusive da Internet. A perspectiva para 2002 é alcançar mais de 234 locais (escolas e centros de saúde), o que representa uma

cobertura de 90% dos órgãos conectados à RMI, perfazendo um total de 6.000 equipamentos⁵.

Nos últimos anos, a administração da PMBH implementou diversos Sistemas de Informações Computadorizados, que abrangem, dentre outras, as áreas de Orçamento, Finanças, Saúde, Administração, Planejamento, Trânsito e Educação. Esses sistemas têm por objetivo controlar e gerar informações estratégicas e fundamentais à tomada de decisões pelos gestores públicos municipais. Os principais Sistemas de Informações da PMBH estão identificados no QUADRO 09.

**QUADRO 09 – PRINCIPAIS SISTEMAS DE INFORMAÇÕES DA
PMBH**

(Continua)

Nº	NOME DO SISTEMA	PRINCIPAIS USUÁRIOS
01	Sistema de Acesso ao Acervo de Processos Microfilmados	Administração Direta
02	Sistema Integrado de Gestão de Estoque	Administração Direta
03	Sistema Integrado Gerência de Documentos	Administração Direta
04	Portal Público PBH	Administração Direta e Indireta
05	Sistema de Orçamento	Administração Direta e Indireta
06	Sistema Financeiro de Contabilidade	Administração Direta e Indireta
07	Sistema Financeiro de Controle Bancário	Administração Direta e Indireta
08	Sistema Financeiro de Custos	Administração Direta e Indireta
09	Sistema Financeiro de Orçamento e Faturamento	Administração Direta e Indireta
10	Sistema Orçamentário Financeiro	Administração Direta e Indireta
11	Sistema Único de cadastro de Fornecedores	Administração Direta e Indireta

⁵ Extraído de <http://www.pbh.gov.br>

(Continuação)

Nº	NOME DO SISTEMA	PRINCIPAIS USUÁRIOS
12	Sistemas de Relatórios Gerenciais de Despesas	Administração Direta e Indireta
13	Sistema de Suprimentos	AUDIM, PGM, SCOPLAM, SCOMARH, SCOMURBE, SCOMPS, SCOMGER
14	Sistema de Ponto Eletrônico	BELOTUR, BEPREM, PRODABEL, SUDECAP, URBEL
15	CTB em Belo Horizonte	BHTRANS
16	CTB em Belo Horizonte	BHTRANS
17	Projeto Viário em CAD	BHTRANS
18	Projeto Viário em CAD	BHTRANS
19	Sistema de Auditoria do Transporte Coletivo	BHTRANS
20	Sistema de Auditoria do Transporte Coletivo	BHTRANS
21	Sistema de Cadastro Geral	BHTRANS
22	Sistema de Cadastro Geral	BHTRANS
23	Sistema de Controle de Tráfego	BHTRANS
24	Sistema de Controle de Infrações de Trânsito	BHTRANS
25	Sistema de Controle de Infrações de Trânsito	BHTRANS
26	Sistema de Controle de Multas	BHTRANS
27	Sistema de Controle de Multas	BHTRANS
28	Sistema de Controle de Passe Livre	BHTRANS
29	Sistema de Controle de Ponto Eletrônico	BHTRANS
30	Sistema de Controle de Projeto Operacional	BHTRANS
31	Sistema de Folha de Pagamento	BHTRANS
32	Sistema de Folha de Pagamento	BHTRANS
33	Sistema de Gerência Semafórica	BHTRANS
34	Sistema de Gerenciamento de Estacionamento Rotativo	BHTRANS
35	Sistema de Gerenciamento de Táxi	BHTRANS
36	Sistema de Gerenciamento de Transporte Coletivo	BHTRANS
37	Sistema de Gerenciamento dos Acidentes de Trânsito	BHTRANS
38	Sistema de Gestão Integrada DATASUL	BHTRANS
39	Sistema de Pesquisa Sobe-Desce	BHTRANS
40	Sistema de Pesquisas	BHTRANS
41	Sistema de Plano de Saúde	BHTRANS
42	Sistema de Registro de Solicitação	BHTRANS

(Continuação)

Nº	NOME DO SISTEMA	PRINCIPAIS USUÁRIOS
43	Sistema de Tabulação de Pesquisas	BHTRANS
44	Sistema do Plano Municipal de Classificação Viária	BHTRANS
45	Sistema Emme 2	BHTRANS
46	Sistema Geo-referenciado de Cadastro de Circulação	BHTRANS
47	Sistema Geo-referenciado de Cadastro de Itinerário e PED	BHTRANS
48	Sistema Integrado de Gerenciamento de Biblioteca	BHTRANS
49	Sistema Transit	BHTRANS
50	Sistema de Materiais e Compras	HMOB
51	Sistema de Ponto Eletrônico	HMOB
52	Sistema de Folha de Pagamento	HMOB
53	Sistema de Controle de Insumos	SCOMARH
54	Sistema de Controle de Patrimônio	SCOMARH
55	Sistema de Controle de Patrimônio Imobiliário do Município	SCOMARH
56	Sistema de Controle de Portaria e Vigilância	SCOMARH
57	Sistema de Materiais (SICAM)	SCOMARH
58	Sistema de Gerenciamento Contratos	SCOMARH
59	Sistema de Informações Municipais - SIM	SCOMARH
60	Sistema Integrado de Recursos Humanos	SCOMARH
61	Sistema Patrimônio Mobiliário do Município	SCOMARH
62	Sistema Temporalidade de Documentos	SCOMARH
63	Sistema de Arrecadação	SCOMF
64	Sistema de Controle de Emissão e Postagem	SCOMF
65	Sistema de Controle de Execuções Fiscais	SCOMF
66	Sistema de Controle do IPTU	SCOMF
67	Sistema de Dívida Ativa	SCOMF, SCOMURBE
68	Sistema de ITBI	SCOMF
69	Sistema de Remissão do IPTU	SCOMF
70	Sistema de Taxas Manutenção de Cemitério	SCOMF
71	Sistema de Transmissão de Dados	SCOMF
72	Sistema de Valor Adicionado Fiscal	SCOMF
73	Sistema Gerencial de Informações Orçamentárias	SCOMF
74	Sistema Integrado de Mobiliário Contribuinte (ISS)	SCOMF
75	Sistema Integrado Financeiro	SCOMF
76	Sistema Contábil	SCOPLAM
77	Sistema Contábil/Financeiro	SCOPLAM
78	Sistema de Informações Gerenciais de Despesas e Receitas	SCOPLAM
80	Sistema de Instrumento Jurídico	SCOPLAM
81	Sistema de Apoio à Terceira Idade	SMAS
82	Sistema de Bolsa-Escola	SMED
83	Sistema de Cadastro Escolar	SMED
84	Sistema de Educação Infantil	SMED

(Continuação)

Nº	NOME DO SISTEMA	PRINCIPAIS USUÁRIOS
85	Sistema de Ensino Noturno	SMED
86	Sistema de Estatística	SMED
87	Sistema de Jornada Excedente	SMED
88	Sistema de Realocação do Professorado	SMED
89	Sistema de Registro da Rede Física	SMED
90	Sistema Plural	SMED
91	Sistema RECAPE	SMED
92	Sistema de Protocolo	SMED
93	Sistema SAC	SMMAI
94	Sistema Gestão Suprimentos Materiais	SMSA
95	Sistema Integrado de Unidade de Saúde	SMSA
96	Farmácia Distrital	SMSA
97	Intranet SMSA	SMSA
98	Sistema SOS Saúde	SMSA
99	Sistema BH Vida na Internet	SMSA
100	Sistema Cadastro Programa de Saúde da Família	SMSA
101	Sistema Central de Marcação de Consultas	SMSA
102	Sistema Controle e Avaliação Hospitalar e Central de Internação	SMSA
103	Sistema de Acidentes de Trabalho	SMSA
104	Sistema de Agravos e Notificações de Doenças Infecto Contagiosas	SMSA
105	Sistema de Análise Laboratorial	SMSA
106	Sistema de Assistência Médica	SMSA
107	Sistema de Atendimento Médico	SMSA
108	Sistema de Autorização de Procedimento de Alto Custo	SMSA
109	Sistema de Avaliação de Maternidade	SMSA
110	Sistema de Avaliação e Desempenho	SMSA
111	Sistema de Benefícios	SMSA
112	Sistema de Complemento do SINASC	SMSA
113	Sistema de Complemento do Sistema de Mortalidade	SMSA
114	Sistema de Controle de Marcações de Consultas	SMSA
115	Sistema de Controle de Zoonoses	SMSA
116	Sistema de Diabéticos e Hiper-tensos	SMSA
117	Sistema de Doenças Ocupacionais	SMSA
118	Sistema de Doenças Respiratórias	SMSA
119	Sistema de Faturamento da Autorização de Internação Hospitalar	SMSA
120	Sistema de Gestão da Autorização de Internação Hospitalar	SMSA
121	Sistema de Informação Ambulatorial	SMSA
122	Sistema de Leitura de Boletas	SMSA

(Conclusão)

Nº	NOME DO SISTEMA	PRINCIPAIS USUÁRIOS
123	Sistema de Morbidade Ambulatorial	SMSA
124	Sistema de Mortalidade	SMSA
125	Sistema de Nascidos Vivos	SMSA
126	Sistema de Oncologia	SMSA
127	Sistema de Pesquisa de Preço	SMSA
128	Sistema de Produção Ambulatorial da Rede Própria da SMSA	SMSA
129	Sistema de Registro de Atendimento Ambulatorial	SMSA
130	Sistema de Saúde Mental	SMSA
131	Sistema de Vigilância Epidemiológica	SMSA
132	Sistema Laboratório de Patologia Clínica	SMSA
133	Sistema de Vigilância Sanitária	SMSA

FONTE- Relatório da PRODABEL (adaptado)

Além desses sistemas proeminentes, existem outros, menos complexos e de uso mais restrito aos órgãos, voltados a controles mais específicos e informações de menor relevância.

Essa intensificação de sistemas proporciona possibilidades de novas soluções à administração e gestão das atividades da PMBH. Portanto, com o número cada vez maior de sistemas informatizados que controlam operações de grande relevância da PMBH, maior é necessidade de controles despendidos sobre estes sistemas.

3.7- Conclusão

Este capítulo demonstrou que a informação constitui um instrumento basilar para uma organização, pois colabora para a gerência de suas atividades administrativas, econômicas, financeiras, políticas e sociais.

Através da utilização de sistemas computadorizados essas informações tornam-se acessíveis a seus usuários, facilitando a tomada de decisões.

É crescente a utilização de Sistemas de Informações Computadorizados nas diversas atividades da Administração Pública Brasileira. A PMBH já faz uso deles em diversas áreas das políticas públicas, como administração, educação, saúde, transporte, orçamento e finanças. Estes sistemas visam controlar, informar, gerenciar, organizar e integrar os serviços prestados desta Prefeitura.

No capítulo seguinte será abordada a questão da Segurança dos Sistemas de Informações.

4 SEGURANÇA DOS SISTEMAS DE INFORMAÇÕES

4.1- Introdução

Este capítulo aborda a questão da Segurança dos Sistemas de Informações, partindo da sua definição e apresentando seus objetivos e modalidades, destacando o arcabouço jurídico brasileiro que versa sobre o tema. Em seguida, são enfocados os Riscos e Impactos a que estes sistemas estão sujeitos.

Serão dispostos, também, as principais Medidas de Segurança para os Sistemas de Informações e os tópicos essenciais de um Plano de Contingências.

4.2-Segurança dos Sistemas de Informações

Os Sistemas de Informações Computadorizados têm importância crucial para as organizações, já que as informações neles contidas são fundamentais para a tomada de decisões, quer sejam de cunho governamental, político, social ou econômico. Devido à dependência das decisões nas informações, a segurança dessas deve ser absoluta, pois qualquer erro nos sistemas informatizados pode comprometer as organizações e afetar a sociedade de diversas maneiras, tamanho o vínculo com a tecnologia utilizada.

Para LEMOS (1995, p. 448), a segurança está relacionada à necessidade de proteção contra o acesso ou manipulação, intencional ou não, de informações confidenciais por agentes não autorizados e contra a utilização não autorizada do computador ou de seus dispositivos periféricos. Segundo o autor, a necessidade de proteção deve ser definida em termos dos possíveis riscos e dos objetivos de uma organização, formalizados nos termos de uma Política de Segurança.

Portanto, a Segurança dos Sistemas de Informações esta associada à proteção dos elementos de um sistema e das informações contra quaisquer desastres, erros e manipulações indevidas, na tentativa de reduzir a possibilidade de incidentes.

Os objetivos da segurança variam conforme o objeto da organização e a natureza do Sistema de Informações, ou seja, se é contábil, financeiro, de recursos humanos ou outros. Para identificar tais objetivos, é necessário efetuar um exame da aplicação do sistema e dos riscos e impactos a que esteja suscetível.

De acordo com o padrão ISO 7498-2, o qual aborda aspectos relacionados com segurança no modelo OSI (*Open Systems Interconnection*), os objetivos da Segurança compreendem o estabelecimento de medidas preventivas para combater ameaças identificadas. Apesar desse modelo se referir a serviços de segurança de redes, seus conceitos podem ser usados para qualquer tipo de ambiente computacional. Nesse modelo, os objetivos referem-se à autenticação, controle de acesso, confiabilidade, integridade e disponibilidade de dados.

Conforme alguns autores [DIAS (2000, p. 42-43), LEMOS (1995, p. 449-450), IMONIANA (1994, p.50-52), MOELLER (1989, p. 69-73) e PLEEGER (1996, p.95-97)], os objetivos da Segurança dos Sistemas de Informações são mais amplos, e estão relacionados no QUADRO 10.

**QUADRO 10- OBJETIVOS DA SEGURANÇA DOS SISTEMAS DE
INFORMAÇÕES**

OBJETIVO	DESCRIÇÃO
Autenticidade	Visa verificar se o dado inserido no sistema é fidedigno ao documento de origem. No caso de redes, ocorre a averiguação da identidade de quem está solicitando o acesso ao recurso.
Controle de acesso	Fornece proteção contra o uso não autorizado de recursos, como leitura, alteração ou destruição de dados, execução de programas e uso de meios de comunicação.
Confiabilidade	Garante que mesmo em condições adversas, o sistema atuará conforme o esperado.
Integridade	É a medida da acurácia do dado. Evita que apenas partes dos dados sejam inseridos no sistema e, ainda, que dados sejam apagados ou, de alguma forma, alterados sem a devida permissão do proprietário da informação. Em uma rede de computadores, preservar a integridade da informação significa assegurar que a mensagem enviada chegue ao receptor sem alterações
Disponibilidade	Garante que os recursos computacionais estejam em condições normais de funcionamento, disponíveis aos usuários. A informação deve sempre estar disponível quando requerida para uso legítimo.
Confidencialidade	Protege as informações contra acesso de qualquer pessoa não autorizada; ou seja, deve-se manter a informação tão privada quanto se possa desejar. Refere-se à proteção contra revelação não autorizada da informação.
Consistência:	Certifica-se de que o sistema atua conforme as expectativas dos usuários autorizados.
Auditoria	Protege os sistemas contra erros e atos maliciosos cometidos por usuários autorizados. Para identificar os autores e suas ações, são utilizadas trilhas de auditoria e <i>logs</i> , que registram tudo o que foi executado no sistema, por quem e quando.

FONTE- DIAS 2000, p. 42-43; LEMOS 1995, p. 449-450; IMONIANA 1994, p.50-52; MOELLER 1989, p. 69-73 e PLEEGER 1996, p.95-97 (adaptado).

Mediante os objetivos destacados, pode-se concluir que a segurança constitui um fator de extrema relevância para a qualidade de um Sistema de Informações.

4.3-Modalidades de Segurança

Partindo do pressuposto de que a segurança deve compreender todas as áreas da organização afetas aos Sistemas de Informações, é indispensável que sejam observadas as modalidades de segurança existentes, apresentadas nas seções seguintes.

4.3.1- Segurança Legal

Segundo IMONIANA (1994, p.54), a Segurança Legal é aquela provida pelos órgãos governamentais, através da determinação da legislação pertinente. Dada a importância da Segurança dos Sistemas de Informações, vários grupos de pesquisa iniciaram trabalhos que culminaram em convenções e, até mesmo, em projetos de leis.

As convenções geralmente são adotadas no âmbito internacional. As instituições internacionais que estabelecem convenções acerca da Segurança dos Sistemas de Informações, mais destacadas são: *International Organization for Standardization*⁶, *International Electrotechnical Commission*⁷, *International Telecommunications Union*⁸, *Comité Européen Normalisation Eléctrotechnique*⁹, *Comité Européen de Normalisation*¹⁰ e *European Telecommunications Standards Institute*¹¹.

Apesar de não constituir uma instituição internacional, o *National Computer Security Center*, órgão que avalia aspectos de segurança dos sistemas computadorizados, merece evidência devido à Criação do *Orange Book*, nome dado ao padrão norte-

⁶ Extraído de <http://www.iso.ch>

⁷ Extraído de <http://www.iec.ch>

⁸ Extraído de <http://www.itu.int>

⁹ Extraído de <http://www.cenelec.be>

¹⁰ Extraído de <http://www.cenorm.be>

¹¹ Extraído de <http://www.etsi.org>

americano *Department of Defense Trusted Computer System Evaluation Criteria*. Este padrão dispõe sobre as características da segurança definida para os sistemas computacionais.

No Brasil, a Associação Brasileira de Normas Técnicas (ABNT) está estudando o Padrão BS7799 (*British Standard 7799*) para definir a norma que irá dispor sobre os padrões de segurança de informações, como algoritmos de criptografia, senhas e controle de acesso para segurança física e ambiental.

Enquanto as convenções são de caráter internacional, a legislação é de cunho pátrio, apesar das similaridades entre as normas de países distintos. A legislação brasileira alusiva à Segurança da Informação apresenta-se consolidada no QUADRO 11:

QUADRO 11: LEGISLAÇÃO BRASILEIRA ALUSIVA À SEGURANÇA DA INFORMAÇÃO

(Continua)

DISPOSITIVO LEGAL	ASSUNTO
Resolução Comitê Gestor Infra-Estrutura de Chaves Públicas Brasileira- ICP Brasil n. 2, de 25/09/2001	Aprova a Política de Segurança da Infra-Estrutura de Chaves Públicas (ICP) Brasileira.
Medida Provisória n. 2.200-2, de 24/08/2001	Institui a Infra-Estrutura de Chaves Públicas Brasileira para garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras.
Decreto n. 3.505, de 13/06/2000	Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal.
Projeto de Lei do Senado n. 76, de 2000	Define e tipifica os delitos informáticos.
Projeto de Lei do Senado n. 84, de 1999	Dispõe sobre os crimes cometidos na área de informática e suas penalidades.

(Conclusão)

DISPOSITIVO LEGAL	ASSUNTO
Decreto n. 2.910, de 29/12/1998	Estabelece normas para a salvaguarda de documentos, materiais, áreas, comunicações e Sistemas de Informações de natureza sigilosa.
Decreto n. 2.556, de 20/04/98	Regulamenta o registro previsto no art. 3º da Lei n. 9.609, de 19.02.98, que dispõe sobre a proteção da propriedade intelectual de programa de computador e sua comercialização no País.
Lei n. 9.610, de 19/02/98	Altera, atualiza e consolida a legislação sobre direitos autorais.
Lei n. 9.609, de 19/02/98	Dispõe sobre a proteção de propriedade intelectual de programa de computador e sua comercialização no País.
Decreto n. 2.134, de 24/01/ 1997	Dispõe sobre a categoria dos documentos públicos sigilosos e o acesso a eles.
Lei n. 9.296, de 24/07/1996	Regulamenta o inciso XII, do art. 5º da Constituição Federal. Este dispositivo aplica-se à interceptação do fluxo de comunicações em Sistemas de informática.
Projeto de Lei do Senado n. 234, de 1996	Define crime contra a inviolabilidade de comunicação de dados de computador.
Projeto de Lei n. 1.713, de 1996	Dispõe sobre o acesso, a responsabilidade e os crimes cometidos nas redes integradas de computadores.
Decreto n. 79.099, de 06/01/1977	Aprova o regulamento para a salvaguarda de assuntos sigilosos.

FONTE- Elaborado a partir da legislação armazenada em <http://www.mct.gov.br>, <http://www.presidencia.gov.br> e <http://www.senado.gov.br>.

4.3.2- Segurança Administrativa

Para IMONIANA (1994, p.55), a Segurança Administrativa é aquela inerente aos recursos humanos da organização.

Essa segurança compreende as políticas de gerenciamento referentes à organização (normas e procedimentos formais e informais), à definição e segregação de funções entre os responsáveis pelos Sistemas de Informações, ao treinamento de segurança, à análise de trilhas de auditoria, aos procedimentos de controle sobre os equipamentos e à quebra de segurança.

4.3.3- Segurança Física

PLEEGER (1996, p.98-105) discorre que a Segurança Física corresponde à manutenção das condições operacionais e da integridade dos recursos materiais componentes dos ambientes computacionais e das informações contra usuários não autorizados. Os recursos a serem protegidos diretamente pela Segurança Física são os equipamentos (UCP, placas, vídeos, monitores, *mouses*, teclados, unidades de disco, *scanners*, *modems* e cabeamentos), a documentação (sobre *hardware* e *software*, aplicativos, política e procedimentos de segurança), os suprimentos (disquetes, fitas, formulários e papel) e as próprias pessoas.

Para o autor, a Segurança Física é dividida em dois enfoques: Segurança de Acesso e Segurança Ambiental.

A Segurança de Acesso visa proteger os equipamentos e as informações contra usuários não autorizados, prevenindo o acesso a estes recursos. Apenas as pessoas expressamente autorizadas podem ter acesso ao ambiente dos sistemas computadorizados.

A Segurança Ambiental é diretamente relacionada à infra-estrutura do ambiente de informática. Esta modalidade de segurança visa proteger os recursos computacionais contra danos provocados por desastres naturais, como enchentes e incêndios, pela falta de energia elétrica ou no sistema de ar condicionado, por exemplo.

A proteção física desses recursos constitui um obstáculo aditivo e precedente à Segurança Lógica. Deste modo, a Segurança Física protege também os recursos lógicos do ambiente computacional.

4.3.4- Segurança Lógica

Segundo MOELLER (1989, p. 75-78), a Segurança Lógica refere-se à segurança fornecida pelos recursos gerais tecnológicos de um sistema computacional. Esta modalidade de segurança visa proteger dados, programas e sistemas contra tentativas de acesso não autorizados feitas por usuários ou outros programas. Objetiva também garantir que não haja alteração ou perda desses recursos.

Para o autor, os recursos e informações normalmente protegidos pela Segurança Lógica são:

- a)** Aplicativos: o acesso não autorizado ao código fonte dos aplicativos pode ser usado para alterar suas funções e a lógica do programa.
- b)** Arquivos de dados: bases de dados, arquivos ou transações de bancos de dados devem ser protegidos para evitar que os dados sejam apagados ou alterados sem autorização adequada.
- c)** Utilitários e sistema operacional: o acesso a utilitários, como editores, compiladores, *softwares* de manutenção, de monitoração e diagnóstico deve ser restrito, já que essas ferramentas podem ser usadas para alterar arquivos de dados, aplicativos e arquivos de configuração do sistema operacional. O sistema operacional é sempre um alvo bastante visado, pois sua configuração é o ponto chave de todo o esquema de segurança. A fragilidade do sistema operacional compromete a segurança de todo o conjunto de aplicativos, utilitários e arquivos.
- d)** Arquivos de senha: a falta de proteção adequada aos arquivos que armazenam as senhas pode comprometer todo o sistema, pois uma pessoa não autorizada, ao obter uma identificação e a senha de um usuário privilegiado, pode, intencionalmente, causar danos ao sistema e dificilmente será barrado por

qualquer controle de segurança instalado, já que se faz passar por um usuário autorizado.

- e) Arquivos de *log*: os arquivos de *log* são usados para registrar as ações dos usuários, constituindo-se em ótimas fontes de informação para auditorias futuras e análises de quebras de segurança. Os *logs* registram quem acessou os recursos computacionais, aplicativos, arquivos de dados e utilitários, quando foi feito o acesso e que tipo de operações foram efetuadas. Se os arquivos de *log* não forem devidamente protegidos, um invasor poderá alterar seus registros para encobrir ações por ele executadas, tais como: alteração ou destruição de dados, acesso a aplicativos e alteração da configuração do sistema operacional para facilitar futuras invasões.

Após a definição de cada modalidade de segurança, conclui-se que cada uma delas contribui para reforçar a concretização os objetivos das demais modalidades.

4.4- Política de Segurança

As organizações que se preocupam efetivamente com a segurança dos seus Sistemas de Informações, seguem as orientações descritas no *Orange Book* e obedecem à legislação pertinente ao assunto. A adoção dessas proposições por uma organização caracteriza uma Política de Segurança.

LEMOS (1995, p. 450) doutrina que:

“Política de Segurança é um conjunto de leis, regras e práticas que regulam como uma organização gerencia, protege e distribui suas informações.”

Assim, um ambiente informatizado é considerado seguro em relação a uma Política de Segurança caso garanta o cumprimento das leis, regras e práticas definidas nessa política.

Uma Política de Segurança deve contemplar todas as modalidades de segurança e ser adotada a partir das peculiaridades de cada organização, vez que ambientes similares podem requerer políticas distintas. Contudo, o importante é que a finalidade da Política de Segurança seja alcançada, ou seja, a proteção dos recursos tecnológicos e das informações por eles processadas.

Além disso, faz-se mister que a política estabeleça a responsabilidade das pessoas envolvidas com os Sistemas de Informações quanto às funções que executam e que descreva os principais riscos e impactos a que estes sistemas estejam expostos.

Não obstante os fatores supracitados, é de suma importância que conste na Política de Segurança um **Plano de Contingências**, que explicita as medidas de recuperação de dados e informações para a continuidade dos serviços na área de informática.

4.5- Riscos e seus Impactos nos Sistemas de Informações Computadorizados

Embora apresentem soluções vantajosas para a organização, os Sistemas de Informações Computadorizados estão mais vulneráveis a riscos do os sistemas manuais.

DIAS (2000, p. 55) entende que o risco é a medida de exposição a qual o sistema computacional está sujeito. O risco envolve ameaças e vulnerabilidades. Vulnerabilidade é uma fraqueza ou deficiência, que pode ser explorada por uma ameaça. Já a ameaça é tudo aquilo que pode comprometer a segurança de um sistema, podendo ser acidental (falha de *hardware*, erros de programação, desastres naturais, erros do usuário, *bugs* de *software*, uma mensagem secreta enviada a um endereço incorreto) ou deliberada (roubo, espionagem, fraude, sabotagem, incursão de *hackers*).

As ameaças deliberadas podem ser subdivididas ainda em **passivas e ativas**. Ameaças passivas envolvem invasão e/ou monitoramento, mas sem alteração de informações. As ameaças ativas envolvem alterações de dados.

Muitos autores [LEMOS (1995, p. 451), MOELLER (1989, p. 60-66), PLEEGER (1996, p.81-87) DIAS (2000, p. 55-56), GIL (1998, p.21-22), PAULA (1999, p.95) e LAUDON & LAUDON (2000, p.262)] apresentam os principais riscos a que os Sistemas de Informações estão sujeitos. No QUADRO 12, estão evidenciados estes riscos.

QUADRO12- RISCOS A QUE OS SISTEMAS DE INFORMAÇÕES ESTÃO SUJEITOS

RISCO	DESCRIÇÃO
Catástrofes	Momentos de intensa e descontrolada destruição, como desabamento, incêndio e inundação; vazamento de informações.
Supressão de serviços	Falha na infra-estrutura, causada, por exemplo, pela interrupção de energia elétrica e queda de comunicações.
Vazamento de informações	Informações desprotegidas ou reveladas a pessoas ou programas não autorizados.
Violação de integridade	Modificação ou deturpação da informação; comprometimento da consistência de dados.
Interrupção de serviço	<i>Impedimentos deliberados de acesso aos recursos computacionais por usuários autorizados.</i>
Acesso e uso não autorizado	Um recurso computacional é utilizado por pessoa não autorizada ou de forma não autorizada.
Desvio	Roubo, remoção ou perda de equipamentos e informações.

FONTE- LEMOS 1995, p. 451; MOELLER 1989, p. 60-61; PLEEGER 1996, p.81-82; DIAS 2000, p. 55-56; GIL 1998, p.21-22; PAULA 1999, p.95 e LAUDON & LAUDON 2000, p.262 (adaptado).

Segundo estes autores, existem ainda outros tipos de riscos que, ao se efetivarem em um ataque, permitem a realização de uma ou mais das ameaças antes citadas. São elas:

- a) personificação (*masquerade*): uma entidade (pessoa ou programa) se faz passar por outra entidade;

- b)** desvio de controles (*bypass*): um *hacker*, por exemplo, explora falhas do sistema e as vulnerabilidades de segurança burlando os controles para obter direitos de acesso não autorizados;
- c)** violação autorizada (ataques internos): usuários legítimos comportam-se de modo não autorizado, ou seja, usam o sistema com propósitos não autorizados;
- d)** ameaças programadas: códigos de *software* que se alojam no sistema com intuito de comprometer sua segurança, alterando seu comportamento, violando controles de segurança, alterando ou destruindo dados.

Normalmente as ameaças programadas são chamadas de vírus, mas, existem outras nomenclaturas mais específicas. DIAS (2000, p. 63-64) cita os tipos principais de ameaças programadas:

- a)** vírus: são pequenos programas projetados para se replicarem e se espalharem de um computador a outro, atacando programas ou o setor de boot de um disco rígido. São seqüências de código inseridas em outro código executável, de forma que quando esses programas são ativados os vírus também são executados. Uma vez ativo, o vírus pode infectar imediatamente outras partes do computador (outros programas, arquivos, disquetes e setores de disco) ou permanecer na memória do computador e oportunamente infectar outros programas e disquetes. Normalmente são encontrados em microcomputadores. São exemplos de vírus: Italiano ou Ping-Pong, Jerusalém ou Sexta-Feira 13, e Michelangelo;
- b)** *worms*: são programas que se propagam de um computador a outro em uma rede, sem necessariamente modificar programas nas máquinas de destino. Podem rodar independentemente e trafegam de uma máquina a outra através das conexões de rede, podendo ter pedaços de si mesmos rodando em várias máquinas;
- c)** bactéria: é um programa que gera cópias de si mesmo com o intuito de sobrecarregar um sistema de computador;
- d)** bomba lógica: ameaça programada, camuflada em programas, que é ativada quando certas condições são satisfeitas. Permanece dormente em *softwares* por um longo período de tempo até que sejam ativadas. Quando isso ocorre, executam

funções que alteram o comportamento do *software* hospedeiro, como destruir dados, travar computador ou danificar o sistema;

- e) Cavalo de Tróia: programa que parece ter uma função, mas na realidade, executa outras funções. Análogo ao mito da história grega, o Cavalos de Tróia moderno assemelha-se a um programa que o usuário gostaria de rodar (jogo, planilha eletrônica, editor de texto). Enquanto parece executar o que o usuário deseja, na verdade, o Cavalo de Tróia está fazendo algo completamente diferente, como apagando arquivos, reformatando discos ou alterando dados. É utilizado como veículo para vírus, *worms* e outras ameaças programadas.

Diante da diversidade de riscos associados ao uso de Sistemas de Informações Computadorizados, é preciso adotar uma Política de Segurança abrangente para eliminar ou reduzir tais riscos, limitando, assim, os danos causados e seus impactos na organização.

Os impactos mais comuns provocados por estes riscos são: a perda de equipamentos e indisponibilidade dos Sistemas de Informações vitais para a organização; divulgação de informações sigilosas; perda de credibilidade e abertura de processo legal contra a organização; perda de clientes para a concorrência e até mesmo o comprometimento da sobrevivência da instituição.

4.6- Medidas de Segurança

Medidas de Segurança são mecanismos utilizados em caráter preventivo para atender aos objetivos de cada modalidade de segurança, evitando ou diminuindo os riscos que os Sistemas de Informações estão sujeitos. Portanto, para cada tipo de segurança existem medidas apropriadas a serem adotadas.

As Medidas de Segurança relatadas nas seções 3.6.1 a 3.6.4 são aquelas consolidadas a partir da doutrina dos autores: LEMOS (1995, p. 459), MOELLER (1989, p. 79-85),

PLEEGER (1996, p.89-93) DIAS (2000, p. 72-106), GIL (1998, p.65-107), PAULA (1999, p.100-104) e LAUDON & LAUDON (2000, p.270-271).

4.6.1- Medidas de Segurança Legal

As Medidas de Segurança Legal compreendem a observância da legislação, da ética e das convenções pertinentes aos Sistemas de Informações.

4.6.2- Medidas de Segurança Administrativa

As principais Medidas de Segurança Administrativa contemplam:

- a)* Organização: institui código de conduta, e definem as atribuições e responsabilidades dos profissionais de segurança.
- b)* Segregação de funções: as funções de desenvolvimento, manutenção, suporte técnico, operação e controle devem ser claramente separadas. Assim, a probabilidade de ocorrência de fraudes e alterações indevidas de programas, ou dados/transações, será fortemente minimizada.
- c)* Rotação de responsabilidades: rodízio periódico dos profissionais para evitar núcleos de controle sobre determinados procedimentos.
- d)* Formação adequada do pessoal para uso dos equipamentos e dos sistemas, atualização profissional contínua, no sentido do acompanhamento de mudanças tecnológicas.
- e)* Auditoria de sistemas para atuação como assessoria na otimização dos processos e resultados da informática.

4.6.3- Medidas de Segurança Física

As Medidas de Segurança Física são divididas em Medidas de Segurança de Acesso e Medidas de Segurança Ambiental.

As principais Medidas de Segurança Física de Acesso referem-se aos controles administrativos que requerem a utilização de crachás de identificação de funcionários

e visitantes, exigência da devolução de bens de propriedade da organização (crachás, chaves, documentos, livros) quando o funcionário é demitido, e controle da entrada e saída de visitante, registrando dia, horários e local de acesso.

As Medidas de Segurança Física de Acesso consistem também em controles explícitos que compreendem a utilização de fechaduras mecânicas ou cadeados comuns, fechaduras eletrônicas cujas chaves são cartões com tarja magnética com código secreto, fechaduras biométricas programadas para reconhecer características físicas dos usuários autorizados, câmeras de vídeo e alarmes, e guardas de segurança para verificar a identidade de todas as pessoas que entram nos locais de acesso controlado.

As principais Medidas de Segurança Ambiental consistem em:

- a)** Controles contra incêndios: utilização de material resistente ao fogo na construção das edificações, instalação de pára-raios; adoção de políticas anti-fumo; manutenção das salas sem acúmulo de materiais de fácil combustão e instalação de mangueiras, extintores de incêndio e sistemas automáticos de combate ao fogo.
- b)** Controles sobre energia elétrica: utilização de estabilizadores, *no-breaks* (equipamentos que mantêm os equipamentos em funcionamento até que seja restabelecido o fornecimento normal de energia elétrica) e geradores de energia alternativos (a *diesel* ou a gás).
- c)** Controles contra enchentes e ameaças que envolvam água: instalação dos equipamentos em local protegido contra água ou em local em que a presença de água seja detectada com facilidade.
- d)** Controles sobre temperatura e ventilação: evitar a exposição direta dos equipamentos a raios solares ou a fontes de calor; controle da temperatura e da ventilação do ambiente.
- e)** Controles sobre limpeza e conservação: limpeza periódica do ambiente computacional, evitando o acúmulo de matérias de fácil combustão; proibição do consumo de cigarros, líquidos e alimentos próximos aos equipamentos.

4.6.4- Medidas de Segurança Lógica

As principais Medidas de Segurança Lógica relacionam-se a:

- a) Processo de *logon*: instituição do processo de *logon*, que é usado para acessar aos dados e aplicativos em sistema computacional. Normalmente, este processo utiliza uma identificação e uma autenticação do usuário.

A identificação do usuário deve ser única e cada um deve ter uma identificação própria, que pode um código de caracteres ou um cartão inteligente contendo microprocessadores. Após a identificação do usuário, ocorre sua autenticação.

A maioria dos sistemas atuais solicitam uma senha, em geral de com 8 caracteres alfanuméricos. Em outros sistemas, utilizam-se um *token*, objeto que o usuário possui para se diferenciar das demais pessoas e habilitar-se a acessar um sistema. Cartões inteligentes e cartões com tarja magnética constituem exemplos de *token*.

Nos sistemas mais modernos, utiliza-se o reconhecimento da identificação biométrica, isto é, as características físicas do usuário. A exemplo, citam-se as impressões digitais, a voz, a configuração da retina e da íris e o reconhecimento facial por meio de um termograma, que é uma imagem tirada com uma câmara infravermelha que mostra os padrões térmicos de uma face.

- b) Monitoramento de registro de *log* e trilhas de auditoria.
- c) Limite do horário de uso dos recursos computacionais e, ainda, a quantidade de sessões concorrentes, impedindo que o usuário entre no sistema ou na rede a partir de mais de um computador simultaneamente.
- d) Implementação do controle de restrição do acesso dos usuários apenas às aplicações, arquivos e utilitários necessários para desempenhar suas funções na organização.
- e) Sistemas criptográficos: utilização da criptografia ou algoritmos cifrados para proporcionar confidencialidade de dados e de informações de fluxo de dados.

A vantagem da criptografia é que mesmo que outros métodos de proteção de dados falhem os dados ainda serão ininteligíveis ao invasor. Para compreendê-los, o invasor terá que descobrir a chave e o algoritmo utilizados no processo de criptografia.

Segundo DIAS (2000, p.75), criptografia é o estudo da grafia secreta; ou seja, é o estudo de métodos para ocultar o conteúdo de mensagens ou dados armazenados. O processo de cifragem corresponde à transformação da mensagem original em algo ininteligível, utilizando um código secreto: a chave criptográfica. A decifragem, por sua vez, é o processo inverso, isto é, de recuperação da mensagem original a partir de sua forma criptografada.

Na FIG. 05 estão dispostos os componentes básicos de um sistema criptográfico.

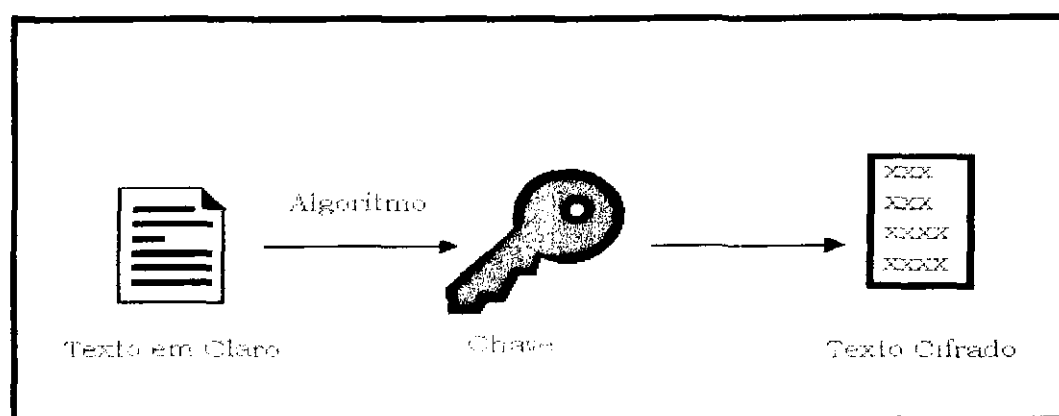


FIGURA 05- Componentes Básicos de um Sistema Criptográfico

FONTE- DIAS, 2000, p. 75 (adaptada)

O texto em claro corresponde à mensagem original, isto é, sem qualquer tratamento, antes de ser criptografada, a qual pode ser lida diretamente por uma pessoa ou por meio de *software* de uso comum, como um editor de textos. O texto cifrado, também chamado criptograma, corresponde ao texto em claro após ter sido submetido ao processo de criptografia e executado por determinado algoritmo.

- f)* Assinatura digital: é um conjunto de mecanismos que pode prover serviços de não repúdio, de autenticação da origem ou de integridade. É constituído de um procedimento de assinatura propriamente dita e outro de verificação de assinatura, permitindo a proteção das partes envolvidas na comunicação quanto à violação da autenticidade de uma delas e da integridade da mensagem.
- g)* *Firewall*: é um conjunto de componentes de *hardware* e *software* instalado entre redes com o propósito de segurança. A implementação deste dispositivo pode prevenir ou reduzir ataques ou invasões às bases de dados corporativas. Pode-se instalar *firewalls* na *internet* (rede global de computadores) e na *intranet* (rede interna da organização).
- h)* Uso restrito do correio eletrônico(*e-mail*): utilizar o correio eletrônico somente para fins da organização, evitando o envio de informações confidenciais.

Quanto maior for a utilização das medidas referidas, mais seguros serão os Sistemas de Informações e o ambiente computacional da organização.

4.7- Plano de Contingências

GIL (1998, p.20) doutrina que um Plano de Contingências constitui um conjunto de ações de segurança usadas pela organização para enfrentar as ameaças aos recursos de informática.

Dessa forma, o Plano de Contingências deve explicitar as alternativas de recuperação de dados para a continuidade dos serviços na área de informática da organização.

Segundo DIAS (2000, p. 116-120), as medidas adiante relacionadas constituem tópicos essenciais de um Plano de Contingências:

- a) *Backup*: é uma cópia dos arquivos, programas e sistemas computacionais. É um dos itens mais importantes em um Plano de Contingências na área de informática, pois se não houver dados para serem recuperados não faz sentido manter um plano para recuperação. Mesmo em caso de perda total dos equipamentos, os *backups* contendo os sistemas e informações vitais da empresa poderão ser processados em outra localidade, em outros equipamentos. Os *backups* contêm um tipo de patrimônio que os seguros são incapazes de cobrir, que são as informações institucionais.
- b) Armazenamento de dados: é conveniente que todos os *backups* efetuados estejam devidamente registrados para que não haja qualquer dúvida quanto ao seu conteúdo e data de atualização. Além disso, o próprio local de armazenamento deve ser suficientemente seguro.
- c) Recuperação de dados: a recuperação de dados define os procedimentos necessários ao retorno da operação normal dos sistemas. Para garantir a efetiva restauração dos sistemas e assegurar que todos os componentes necessários para restaurá-los estão sendo copiados corretamente, todos os procedimentos de recuperação precisam ser testados periodicamente. Se o processo de recuperação não funcionar, os *backups* não terão qualquer utilidade.
- d) Procedimentos manuais: embora muitos aplicativos não possam retornar aos procedimentos manuais de processamento, alguns podem, pelo menos por um limitado período de tempo. Normalmente, a volta a procedimentos manuais somente é exequível no caso de sistemas de pequeno porte ou como medida temporária.
- e) Seguros: como qualquer recurso com valor econômico os recursos computacionais também podem ser segurados contra perdas financeiras e danos materiais, cobrindo computadores e equipamentos de comunicação. É recomendável verificar também a possibilidade de contratar seguro para cobrir prejuízos causados por funcionários e despesas adicionais de trabalho emergencial e de restauração na ocorrência de desastres.
- f) Acordos comerciais: apesar de pouco utilizados no Brasil, os acordos comerciais também são alternativas para a restauração dos serviços de informática. Serão citados aqui três tipos de acordos comerciais:

- Uso de equipamentos do fornecedor de *hardware*: os fornecedores de computadores de pequeno porte costumam ter locais com equipamentos para demonstração, os quais podem ficar disponíveis no caso de um desastre ocorrer nas instalações de um cliente. Normalmente, cedem seus recursos computacionais enquanto as instalações dos clientes estão sendo restauradas.

- *Hot site*: algumas empresas são especializadas em serviços de restauração de sistemas computadorizados. Oferecem salas equipadas, compatíveis com os recursos computacionais do cliente, sempre prontas para operar em substituição à instalação original. Esses centros de recuperação provêem ainda suporte técnico e serviços de telecomunicação. Tal método, portanto, corresponde a uma instalação equipada e pronta para operar em um curto espaço de tempo. Para garantir seu perfeito funcionamento, é necessário testar periodicamente os sistemas aplicativos na instalação reserva.

- *Cold site*: instalação que oferece infra-estrutura básica. No caso de um desastre, o cliente só precisa deslocar seus equipamentos para o local preparado.

g) Sistemas espelhados: esta alternativa envolve o processamento de dois sistemas idênticos (equipamentos, *software* e aplicativos replicados) em localidades diferentes, atualizados paralelamente. Um dos sistemas executa o trabalho real, enquanto o outro opera em paralelo, de forma que seja possível transferir o processamento para o sistema reserva, caso seja necessário. É uma opção comparativamente cara, mas justificada para sistemas críticos, em que mesmo uma pequena parada do sistema pode acarretar um grande impacto para a organização.

h) Processamento em vários locais diferentes: a organização pode utilizar seus diversos centros de processamento de dados para servirem de *backup* uns dos outros em uma emergência. Esta abordagem não exige processamento paralelo. Em situações normais, cada centro processa seus próprios dados, como de costume.

- i) *Cold site* interno: a organização pode manter um local vazio, com todos os dispositivos ambientais necessários, preparado para receber os equipamentos no caso de uma eventualidade.

Por conter as estratégias fundamentais para a resolução dos problemas causados pelas ameaças num ambiente de *Sistemas de Informações*, o *Plano de Contingências* deve integrar as Políticas de Segurança da organização.

4.8- Conclusão

Os *Sistemas de Informações Computadorizados* são mais vulneráveis a erros, destruição, mau uso e crimes do que os sistemas manuais. Dessa forma, a segurança desses sistemas deve ser absoluta, vez que as informações que contêm são fundamentais para a organização.

Para tanto, é fundamental que a organização estabeleça uma Política de Segurança, da qual constem toda a norma pertinente à Segurança dos *Sistemas de Informações*, os riscos e impactos a que esses sistemas estão sujeitos, as medidas para combater tais riscos e um *Plano de Contingências* para enfrentar os danos causados.

5 CONTROLE INTERNO

5.1- Introdução

A expressão **controle interno** passou a ser usada com o intuito de distinguir os controles próprios da instituição daqueles de origem externa. Controle interno é o conjunto de normas mediante as quais se administra uma organização, e também a qualquer um dos recursos para que se possa supervisionar e dirigir uma operação determinada.

Cada sistema de controle interno, não obstante a semelhança que pode ter com os padrões usuais de organização e administração, é único em seus detalhes de composição, por ser desenvolvido para pessoas de diferentes capacidades de supervisão e de distinta aptidão para delegar ou assumir autoridade.

Em uma entidade qualquer, o controle interno conta com a adaptação e o cumprimento da política aprovada pela direção e continua nos outros níveis da estrutura administrativa, tomando forma na elaboração e operação de normas da direção e de regulamentações administrativas.

Um elemento importante para a manutenção do controle interno está representado pelo trabalho do auditor interno, pela sua capacidade de observar e informar imparcialmente, em quem a administração pode confiar como fonte de informações sobre o funcionamento geral da organização.

Os controles internos quando estabelecidos em sistema eficiente de funcionamento tornam-se fundamentais para o êxito da organização.

Neste capítulo, serão abordados aspectos relativos ao Controle Interno, descrevendo sua definição, objetivos, modalidades e avaliação dentro das organizações. Serão dispostos, também, o Controle Interno na Administração Municipal, com seu aparato legal e o Controle Interno na Prefeitura Municipal de Belo Horizonte.

5.2- Definição e Objetivos

De um modo geral, todas as empresas possuem controles internos. A diferença básica é que estes podem ser adequados ou não. A constatação dessas condições é fruto da análise da eficiência dos fluxos de operações e informações e da relação custo/benefício. A implantação ou aprimoramento de um determinado tipo de controle é tanto viável quanto positiva for a relação custo/benefício (ATTIE, 1992, p. 45).

COOK (1983, p.65) entende que o controle interno é um sistema próprio da organização. Dele constam seu plano de organização, a atribuição dos deveres e das responsabilidades, os relatórios e todas as medidas e procedimentos adotados para proteger seu ativo, elevar a exatidão e a fidedignidade das informações e demais dados operacionais, promovendo e avaliando a eficácia operacional de todas as atividades da organização, comunicando as metas e diretrizes administrativas, e estimulando e avaliando a observância das mesmas.

O controle interno abrange toda a organização. Compreende muito mais do que o sistema contábil, abrangendo aspectos tais como: práticas de emprego e treinamento, controle de qualidade, planejamento de produção e auditoria interna. Assim, pode-se afirmar que o controle interno abrange, indistintamente, todas as operações da empresa e os recursos empregados de forma integrada e sistemática.

Uma administração eficaz pressupõe a adoção de controle interno de boa qualidade. Entretanto, não basta apenas adotar bons controles; é necessário mantê-los e aprimorá-los, mediante o emprego de recursos humanos e tecnológicos adequados, gerando resultados e informações seguras para a direção da empresa.

Planejar, implantar, manter e aperfeiçoar controles internos é tarefa dos gestores e técnicos alocados em cada linha de negócio da organização, que muitas vezes não contam com disponibilidade integral para aferir com precisão e isenção os controles internos sob sua responsabilidade. O Instituto dos Auditores Internos do Brasil-AUDIBRA (1994, p.23) considera que este papel é da auditoria interna, que, pela sua *condição de órgão de assessoramento*, está apta a exercer essa função com independência e isenção, propiciando à administração diagnósticos da situação dos controles internos.

A importância do controle interno fica evidente a partir do momento em que se torna impossível conceber uma organização que não tenha um sistema de controles que possa garantir a continuidade do fluxo de operações e informações proposto. O fluxo de informações de uma organização permite o conhecimento dessas operações. Portanto, o controle interno abrange o controle dos Sistemas de Informações. É sobre os resultados gerados por esse fluxo, que transforma simples dados em informações importantes, que os administradores montam estratégias e tomam decisões, almejando os objetivos da empresa. Daí se conclui a importância do controle interno para o processo de tomada de decisões.

ATTIE (1992, p. 50-55) afirma que o controle interno tem quatro objetivos:

- a)** Salvarguardar os interesses da organização: refere-se à proteção do patrimônio contra quaisquer perdas e riscos devidos a erros ou irregularidades. Uma organização dispõe de bens, direitos e obrigações que se encontram divididos por diversos departamentos e setores, que devem cuidar individualmente da parte que lhes cabe.
- b)** Zelar pela precisão e confiabilidade das informações e relatórios contábeis, financeiros e operacionais: este objetivo compreende a geração de informações adequadas e oportunas, necessárias gerencialmente para administrar e compreender os eventos realizados na organização.

- c) Estimular à eficácia e eficiência operacional: este objetivo determina prover os meios necessários à condução das tarefas, de forma a obter entendimento, aplicação e ação tempestiva e uniforme. As inúmeras tarefas praticadas pelos diversos setores de uma organização necessitam de uma linha mestra de raciocínio e de conduta. Cada um dos segmentos tem suas particularidades e cada indivíduo precisa conhecer sua tarefa.
- d) Promover a aderência da organização às políticas existentes: assegura que os desejos da administração, definidos através de suas políticas e indicados por meio de seus procedimentos, sejam adequadamente seguidos pelos funcionários.

Pelo exposto, vê-se que o controle interno é fator preponderante para a harmonia organizacional, administrativa e financeira de qualquer organização, seja pública ou privada.

5.3- Modalidades e Avaliação

Os controles internos podem ser realizados de forma prévia, antecedendo o ato, procurando evitar que ocorram erros ou desperdícios quando da efetivação das atividades da empresa; concomitante, acompanhando a realização do ato; e subsequente, quando for realizado após a conclusão do ato, na intenção de detectar a ocorrência de erros nas fases anteriores, propiciando a adoção de medidas corretivas.

Além de serem realizados de formas diferentes, os controles internos são divididos em várias modalidades, conforme dispõe ATTIE (1992, p.198):

- a) Controles administrativos: abrangem o plano organizacional e todos os métodos e procedimentos referentes à eficiência operacional e à adesão à política traçada pela administração.
- b) Controles contábeis: abrangem o plano de organização e todos os métodos e procedimentos diretamente relacionados com a proteção do patrimônio e a fidedignidade dos registros contábeis.

- c) Controles gerenciais: compreendem a análise e avaliação das atitudes administrativas para alcançar os objetivos da empresa. Avaliam também as medidas imprescindíveis para que os recursos necessários sejam obtidos e aplicados nas operações da organização.
- d) Controles operacionais: referem-se às operações cotidianas da empresa, buscando garantir que essas se conduzam de acordo com o planejamento estabelecido. Coordenam os esforços individuais das pessoas que trabalham em grupos e regulam os recursos e fluxos de trabalho entre os grupos. Avaliam o desempenho dos funcionários.
- e) Controle de entradas, de saídas e de processamento de informação: buscam assegurar que todos os dados de entrada sejam precisos e registrados para o devido processamento, gerando informações fidedignas.

Assim, um sistema de controle interno deve abranger quantas modalidades forem aplicáveis à organização.

ATTIE (1992, p.202) entende que um sistema de controle interno eficiente deve compreender: um plano organizacional, um sistema de autorização e procedimentos de escrituração, práticas salutaras e pessoal qualificado.

Embora varie conforme as peculiaridades de cada organização, um plano organizacional deve ser simples e flexível, cujas linhas de autoridade e responsabilidade possam ser identificadas. Deve conter a independência estrutural das funções de operação, contabilidade e auditoria interna. Além dessa separação, deve-se estabelecer a responsabilidade dentro dos setores conforme o programa administrativo. A delegação de autoridade é imprescindível para que tais responsabilidades sejam efetivadas.

O sistema de autorização e procedimentos de escrituração deve incluir meios de controle das operações e transações através de métodos de aprovação conforme os riscos e responsabilidades envolvidos, além de atentar para os documentos originais

dos registros e a devida classificação desses dentro do plano de contas utilizado pela empresa.

As práticas salutaras devem prover os meios para assegurar a integridade das autorizações, registros e custódias, que são conseguidos através da divisão de funções e responsabilidades, de forma que nenhuma pessoa possa manejar uma operação por completo; ou seja, do início ao fim, sem haver a segregação de funções.

Destarte, o funcionamento correto do sistema de controle interno não depende somente do planejamento da organização e dos procedimentos adotados, mas principalmente de todo o pessoal envolvido para desenvolver as diretrizes determinadas.

A norma de n. 300, do AUDIBRA, intitulada “Normas para o Exercício Profissional da Auditoria Interna”, dispõe, nas seções 300.03.13, 300.03.14 e 300.03.16, sobre a revisão do controle interno :

“300.03.13- A finalidade da revisão da adequação do sistema de controle interno é determinar se o sistema estabelecido é eficaz no sentido de assegurar com eficiência a economia:

- a consecução de objetivos e metas estratégicos e táticos da organização;
- o cumprimento de normas e legislação;
- a proteção de ativos;
- a organização interna e os procedimentos;
- a segurança física e lógica;
- a qualidade das informações, serviços e produtos;
- a economicidade, eficiência, eficácia e efetividade na obtenção e uso dos recursos financeiros, materiais e humanos;
- a prevenção de erros, fraudes e desperdícios.

300.03.14- A finalidade da revisão para determinar a eficácia do sistema de controle interno é assegurar que esse sistema atinja seus objetivos.

.....

300.03.16- A finalidade da revisão do controle interno, por parte do auditor, é a de determinar sua qualidade, adequação e desempenho; a forma de como é monitorado pela Alta Administração e sua economicidade em relação aos custos do controle e atividades

controladas e finalmente, formar uma base para determinar a extensão de seus próprios testes, natureza e oportunidade de sua realização."

Consoante, a seção 300.03.04 da já citada norma, cabe aos auditores internos avaliar a adequação dos controles, apresentar as recomendações e sugestões para o seu aprimoramento, bem como apontar à administração a ocorrência de desvios, irregularidades e ilegalidades que venham a observar em decorrência de seus exames.

Dessa forma, fica evidente que a revisão e a avaliação do sistema de controle interno constituem função da auditoria interna. Em empresas de pequeno e médio porte essa função pode ser desempenhada pelo próprio dono ou por algum membro da alta administração. Nas empresas de grande porte, essa função fica a cargo do auditor interno ou de uma equipe de auditoria. COOK (1983, p.147) entende que essas atividades são essenciais para um eficaz funcionamento dos controles internos e que a revisão feita pelos auditores internos destina-se a avaliar a eficácia deste sistema de controle.

5.4- O Controle Interno da Administração Pública Municipal: Aspectos Legais

A descentralização da atividade pública, consoante a criação de autarquias, empresas públicas, sociedades de economia mista e outras entidades de administração indireta, determinou a necessidade de se ampliar e aprimorar o controle dessas atividades.

Da maior importância é a atividade de controlar exercida pela Administração da entidade governamental, conforme se depreende do art. 70, *caput*, da Constituição Federal da República Federativa do Brasil (CF):

"Art. 70- A fiscalização contábil, financeira, orçamentária, operacional e patrimonial da União e das entidades da administração direta e 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."

A fiscalização contábil, financeira e orçamentária municipal dá-se mediante o controle externo, exercido pela Câmara de Vereadores e pelo Tribunal de Contas, e o controle interno do Executivo Municipal, conforme disposição do art. 31 da CF:

"Art. 31- A fiscalização do Município será exercida pelo Poder Legislativo Municipal, mediante controle externo, e pelos sistemas de controle interno do poder executivo Municipal, na forma da lei.

Parágrafo 1º- O controle externo da Câmara Municipal será exercido com o auxílio dos Tribunais de Contas dos Estados ou do Município ou dos Conselhos ou Tribunais de Contas dos Municípios, onde houver."

Como se vê, a fiscalização financeira, contábil e orçamentária é um instrumento de controle. As normas gerais sobre a fiscalização financeira e orçamentária constam dos arts. 75 a 81 da Lei Federal n. 4.320/64, sob o título "Controle da Execução Orçamentária" dividido em controle interno e externo, recepcionados pela CF em seus arts. 31, 70 e 71.

O controle financeiro e orçamentário atribuído ao Executivo compreende os controles da legalidade, da fidelidade e da execução, como disposto nos arts. 75 e 76 da já citada Lei 4.320/64, *verbis*:

"Art. 75- O controle da execução orçamentária compreenderá:

I- a legalidade dos atos de que resultem a arrecadação da receita ou a realização da despesa, o nascimento ou a extinção de direitos e obrigações;

II- a fidelidade funcional dos agentes da administração responsáveis por bens e valores públicos; e

III- o cumprimento do programa de trabalho expresso em termos monetários e em termos de realização de obras e prestações de serviços.

Art. 76- O Poder Executivo exercerá os três tipos de controle a que se refere o artigo 75, sem prejuízo das atribuições do Tribunal de Contas ou órgão equivalente."

Constata-se que a lei orçamentária é também um instrumento de controle, e é com fulcro nesses artigos que se fundamenta o controle interno. Contudo, é no art. 74 da CF que fica explícita a ação do controle interno:

"Art. 74- Os Poderes Legislativo, Executivo e Judiciário manterão, de forma integrada, sistema de controle interno com a finalidade de :

I- avaliar o cumprimento das metas previstas no plano plurianual, a execução dos programas de governo e dos orçamentos da União;

II- comprovar a legalidade e avaliar os resultados, quanto à eficácia e eficiência, da gestão orçamentária, financeira e patrimonial nos órgãos e entidades da administração federal, bem como da aplicação de recursos públicos por entidades de direito privado;

III- exercer o controle das operações de crédito, avais e garantias, bem como dos direitos e haveres da União;

IV- apoiar o controle externo no exercício de sua missão institucional.

Parágrafo 1º- Os responsáveis pelo controle interno, ao tomarem conhecimento de qualquer irregularidade ou ilegalidade, dela darão ciência ao Tribunal de Contas da União, sob pena de responsabilidade solidária.

Parágrafo 2º- Qualquer cidadão, partido político, associação ou sindicato é parte legítima para , na forma da Lei, denunciar irregularidade ou ilegalidade perante o Tribunal de Contas da União."

Assim, fica evidente o estabelecimento de um sistema operacionalizado de forma integrada pelos Poderes, ainda que cada poder tenha o seu próprio controle interno. Este sistema deverá preparar a prestação de contas conjunta e anual. Para a elaboração dessa prestação de contas, a contabilidade do órgão consolidará as contas dos Poderes. Evidentemente, a contabilidade é um instrumento de controle interno, como disposto nos arts. 83 e 84 da Lei 4.320/64:

"Art. 83- A contabilidade evidenciará perante a fazenda Pública a situação de todos quantos, de qualquer modo, arrecadem receitas, efetuem despesas, administrem ou guardem bens a ela pertencentes ou confiados.

Art. 84- Ressalvada a competência do tribunal de Contas ou órgão equivalente, a tomada de contas dos agentes responsáveis por bens ou dinheiros públicos será realizada ou superintendida pelos serviços de contabilidade."

Em seu art. 37, inciso XXI, a CF determina que, ressalvados os casos específicos na legislação, as obras, serviços, compras e alienações serão contratados mediante processo de licitação pública que assegure igualdade de condições a todos os concorrentes. Com a Lei Nacional de Licitação, de n. 8.666/93 e com as alterações feitas pela Lei n. 8.883/94 reforçou-se o instituto legal, colocando em poder do cidadão o controle direto para tornar mais eficaz a fiscalização e o controle dos atos do governo. Constitui também a licitação um instrumento de controle.

Em 4 de maio de 2000, foi instituído outro instrumento de controle: a Lei de Responsabilidade Fiscal, editada através da Lei Complementar Federal n. 101, que estabelece normas de finanças públicas voltadas para a responsabilidade na gestão fiscal, com amparo no capítulo II, Título VI, da CF.

Não obstante a todos esses meios de controle, o Tribunal de Contas da União (TCU) através da Instrução Normativa n. 28, datada de 05/05/1999, estabeleceu as regras para a implementação da *homepage* "Contas Públicas", em conformidade com a Lei n. 9.755, de 16/11/1998. Esta lei dispõe sobre a criação de *homepage* na *Internet* pelo TCU, para divulgação de dados e informações da União, dos Estados, do Distrito Federal e dos Municípios referentes a: montantes de cada um dos tributos arrecadados, relatórios resumidos da execução orçamentária, recursos repassados, orçamentos anuais, balanços orçamentários, demonstrativos de receitas e despesas, contratos e seus aditivos e as relações mensais de todas as compras feitas pela administração direta ou indireta.

Apesar de o TCU ter criado a *homepage* "Contas Públicas", as informações mencionadas na Lei n. 9.755 ainda não foram disponibilizadas pelos Estados, Distrito Federal e Municípios.

Pelo exposto, vê-se que através do controle interno a Administração Pública consegue conciliar seus interesses com os da sociedade. O controle interno é vital para o êxito da Administração Pública, desde que bem estruturado e estabelecido de modo a propiciar aos Poderes o conhecimento pleno dos acontecimentos da organização. A institucionalização do controle interno é necessária e fundamental para permitir aos órgãos públicos e cidadãos conhecer a eficácia com que estão sendo gastos os recursos públicos.

5.5- O Controle Interno da Prefeitura Municipal de Belo Horizonte

Dentre os princípios emanados do Decreto-Lei n. 200/67, da Reforma Administrativa, que dispõe sobre planejamento, coordenação, descentralização, delegação de competência e controle, destaca-se, no caso, o **controle**, que deve ser exercido em todos os Poderes e Esferas do Governo. Outrossim, a CF estabelece a institucionalização deste instrumento nos arts. 31, 70 e 74.

Em 1989, a Instrução Normativa STN/MF n. 010, de 07/07/89, aprovou as Normas do Sistema de Auditoria aplicáveis ao Serviço Público Federal, com o objetivo de disciplinar e padronizar a realização da auditoria pelo Poder Executivo. Esta Instrução estabeleceu o Sistema de Auditoria, do qual constavam, a Subsecretaria de Auditoria e as Coordenadorias de Auditoria dos órgãos setoriais do Sistema de Controle Interno, além das unidades de Auditoria Supervisionais e o Comitê Técnico de Auditoria.

Contudo, em 06/02/2001, através da Lei n. 10.180, o Governo Federal organizou e disciplinou os Sistemas de Planejamento e de Orçamento Federal, de Administração Financeira Federal, de Contabilidade Federal e de Controle Interno do Poder Executivo Federal. Assim, a Administração Federal mantém um Sistema de Controle Interno do Poder Executivo Federal, que visa avaliar a ação governamental e a gestão dos administradores públicos federais, por intermédio da fiscalização contábil, financeira, orçamentária, operacional e patrimonial, apoiando também o controle externo no exercício de sua missão institucional.

Este Sistema conta com um órgão central: a Secretaria Federal de Controle Interno, cuja área de atuação abrange todos os órgãos do Poder Executivo Federal. Conta, ainda, com os órgãos setoriais que integram a estrutura do Ministério das Relações Exteriores, do Ministério da Defesa, da Advocacia-Geral da União e da Casa Civil.

A PMBH não mantém um sistema de controle interno como ocorre no âmbito federal. Contudo, está sujeita à fiscalização do Tribunal de Contas do Estado de Minas Gerais (TCEMG). Cabe a este órgão a fiscalização de todo o dinheiro público relacionado com o Estado de Minas Gerais, nos âmbitos estadual e municipal. Compete-lhe também examinar a legalidade, legitimidade, economicidade e razoabilidade de qualquer ato administrativo de que resulte receita ou despesa e ainda, dos atos que provoquem renúncia de receita. Essa fiscalização ocorre em todos os Poderes do Estado e dos seus 853 municípios, incluídas as entidades públicas com administração descentralizada, bem como aquelas mantidas ou instituídas pelo Poder Público. Essa ação fiscalizadora está prevista nos arts. 31 e 76 da Constituição Federal, art. 76 da Constituição Estadual e Lei Complementar n. 33 do TCEMG.

Além da sujeição a este controle externo, os princípios do controle interno municipal emanam da CF e da Lei Orgânica Municipal (LOM).

A LOM, fiel à CF, dispõe, em seu art. 15, sobre os princípios da Administração Pública, *verbis*:

"Art. 15- A atividade de administração pública dos Poderes do município e a de entidade descentralizada obedecerão aos princípios de legalidade, impessoalidade, moralidade, publicidade e razoabilidade.

Parágrafo 1º- A moralidade e a razoabilidade dos atos do Poder Público serão apuradas, para efeito de controle e invalidação, em face dos dados objetivos de cada caso.

Parágrafo 2º- O agente público motivará o ato administrativo que praticar, explicitando-lhe o fundamento legal, o fático e a finalidade."

Para fazer cumprir os dispositivos do Instrumento Constitucional, a LOM dispõe, em seus artigos iniciais sobre o controle municipal. Em seu art. 2º, parágrafo 2º, inciso V, prevê a ação fiscalizadora da Administração Pública. Não obstante, em seu art. 3º, inciso II, assegura o exercício, pelo cidadão, dos mecanismos de controle da legalidade e da legitimidade dos atos do Poder Público e da eficácia dos serviços públicos.

No art. 4º, parágrafos 4º e 6º, a citada lei estabelece o seguinte:

“Art. 4º- O Município assegura , no seu território e nos limites de sua competência, os direitos e garantias fundamentais que a Constituição da república confere aos brasileiros e aos estrangeiros residentes no país.

.....Parágrafo 4º- Todos têm o direito de requerer e obter informação sobre o projeto do Poder Público, ressalvada aquela cujo sigilo seja, temporariamente, imprescindível à segurança da sociedade e do Município, nos termos da lei, que fixará também o prazo em que deva ser prestada a informação.

.....Parágrafo 6º- É direito de qualquer cidadão e entidade legalmente constituída denunciar às autoridades competentes a prática, por órgão ou entidade pública ou por delegatário de serviço público, de atos lesivos aos direitos dos usuários, incumbindo ao Poder Público apurar sua veracidade e aplicar as sanções cabíveis, sob pena de responsabilização.”

É no art. 95 da LOM que se expressam as determinações do art. 70 da CF; ou seja, dispõe sobre a fiscalização contábil, financeira, orçamentária, operacional e patrimonial do município, atribuindo aos responsáveis pelo controle interno a iniciativa de dar ciência ao Tribunal de Contas e ao Defensor do Povo da evidência de qualquer irregularidade ou ilegalidade, sob pena de responsabilidade solidária. O Decreto Municipal n. 10.710/2001 vem também disciplinar sobre a programação, acompanhamento e avaliação da execução orçamentária e financeira, e sobre procedimentos administrativos de licitação e contratação.

Para que realize o controle interno determinado tanto pelo texto Constitucional quanto pela LOM, a PMBH mantém em sua estrutura administrativa a AUDIM e a Secretaria Municipal do Tesouro, pertencente à Secretaria Municipal da Coordenação de Finanças, *órgãos fundamentais para assegurar à Administração Pública Municipal seu êxito organizacional e o eficaz emprego dos recursos públicos.*

Compete à AUDIM executar a auditoria interna nos órgãos do Poder Executivo Municipal. À Secretaria Municipal do Tesouro compete a execução da contabilidade financeira, patrimonial e orçamentária, bem como assegurar a inspeção de atos e procedimentos como medida preliminar ao cumprimento das obrigações pecuniárias do Município.

5.6- Conclusão

Pelos assuntos tratados neste capítulo, vê-se que o controle interno é fator preponderante para uma perfeita harmonia organizacional, administrativa e financeira de qualquer instituição, seja pública ou privada. Para tanto, o sistema de controle interno adotado deve ser adequado às peculiaridades da organização, abrangendo quantas modalidades forem necessárias à sua estrutura, além de observar que a auditoria interna constitui um instrumento importante para o funcionamento deste sistema.

No próximo capítulo, será abordada a Auditoria Interna.

6 AUDITORIA INTERNA

6.1- Introdução

A auditoria interna é uma atividade importante para a administração das organizações. Isso se mostra evidente, pois é considerada como um instrumento fundamental dos controles internos.

As atividades da auditoria interna servem como fator basilar para o administrador reconhecer se todos os procedimentos internos e as políticas definidas pela instituição, bem como os sistemas contábeis e de controle interno estão efetivamente sendo cumpridos e se todas as transações realizadas estão refletidas contabilmente em concordância com os critérios previamente estabelecidos.

Este capítulo aborda a Auditoria Interna: descreve sua evolução sucintamente e destaca seu conceito, seus objetivos, modalidades e o programa de auditoria interna. Especificamente, a Auditoria de Sistemas será analisada com maior destaque nesta dissertação no capítulo 7.

6.2- Evolução

A auditoria interna, com esta denominação específica, é uma atividade relativamente nova. Desde o começo do século, as grandes organizações mundiais utilizavam os serviços de firmas de auditoria pública para assegurar aos administradores que seus balanços representavam fielmente a escrituração contábil dentro das convenções universalmente aceitas.

Assim, tal sistema de auditoria já estava sendo aplicado, embora não sob a nomenclatura de auditoria, pelos antigos mercadores dos tempos coloniais, que mantinham feitorias e armazéns distantes, justamente devido à difícil forma de controlar os investimentos feitos nas metrópoles, sejam em dinheiro, mercadorias e em outras terras.

Com o desenvolvimento dos mercados internacionais, as grandes organizações compreenderam que as perícias periódicas, realizadas por profissionais independentes, eram importantes para assegurar aos administradores a correção dos balanços, mas que não era possível às firmas de auditoria pública observar de perto as operações das organizações, e assim informar com segurança aos administradores que os procedimentos adotados eram concretizados.

Paulatinamente, foi surgindo a necessidade de manter dentro das próprias instituições um grupo de funcionários de confiança para exercer essas atividades de auditoria. Como estes pertenciam à própria entidade, foram chamados de auditores internos. A princípio, esses profissionais eram responsáveis pela revisão e conferência dos valores e documentos.

Com o desenvolver das atividades industriais e comerciais, constatou-se que esses auditores deveriam expandir suas atividades, sendo então responsáveis pela obtenção de controles internos funcionais, análise das contas de despesa e receita, colaborando, então, com a administração para um melhor desempenho organizacional.

A partir de 1940, a utilização dos serviços dos auditores internos começou a se difundir amplamente entre entidades públicas e privadas. Hoje, a função da auditoria interna está adquirindo maior reconhecimento e responsabilidade.

Atualmente, as organizações consideram a auditoria interna uma atividade imperiosa. Em alguns casos, investem valores altíssimos neste serviço. Um índice de notável desenvolvimento da atividade é o agrupamento de profissionais. *The Institute of*

Internal Auditors ¹², fundado em 1941 nos Estados Unidos, com 24 associados, conta atualmente com mais de 70.000 membros. Este crescimento é extensivo também ao Canadá, Europa, América Latina e África.

Segundo WADDELL (1982, p.57-58), o início do desenvolvimento técnico da Auditoria Interna no Brasil se deu em 1960, com a implantação do *The Institute of Internal Auditors*, em São Paulo. Essa iniciativa coube a um grupo de pessoas que exerciam cargos de auditores internos nas empresas subsidiárias de organização multinacionais. Em 1967, promoveu-se a nacionalização desta entidade, que, a princípio, foi intitulada “Instituto dos Auditores Internos de São Paulo” e, posteriormente, alterado para “Instituto dos Auditores Internos do Brasil”.

Mas foi em 1968, através da Resolução n. 88 do Banco Central do Brasil (BACEN) que a Auditoria tornou oficialmente reconhecida no Brasil. Em 1972, foi criado o Instituto Brasileiro de Contabilidade (IBRACON). No mesmo ano, foram editadas a Resolução n. 220 e as Circulares n. 178 e n.179 do BACEN e pelas Resoluções do Conselho Federal de Contabilidade (CFC) n. 317 e n. 321, respectivamente, criando o Cadastro Especial de Auditores Independentes nos Conselhos Regionais e aprovando as normas e procedimentos de auditoria elaborados pelo IBRACON. As normas vigentes relativas à execução dos trabalhos de auditoria interna e à pessoa do auditor interno emanadas pelo CFC foram aprovadas pelas resoluções identificadas no QUADRO 13.

QUADRO 13- NORMAS DE AUDITORIA INTERNA

RESOLUÇÃO Nº	ASSUNTO
780/95	Auditoria Interna
781/95	Normas Profissionais do Auditor Interno
828/98	Papéis de Trabalho e Documentação de Auditoria
836/99	Fraude e Erro

FONTE- CFC, 2000 (adaptado).

¹² Extraído de <http://www.theiia.org>

A Resolução n. 780/95, que trata da Auditoria Interna, apresenta a seguinte estrutura:

- a)** Conceituação e Disposições Gerais: conceituação, objetivos e procedimentos da Auditoria Interna, papéis de trabalho, fraude e erro.
- b)** Normas de Execução dos Trabalhos: planejamento da auditoria, aplicação dos procedimentos, documentação, amostragem estatística e Processamento Eletrônico de Dados (PED).
- c)** Normas Relativas ao Relatório do Auditor Interno.

A Resolução n. 781/95 apresenta as normas profissionais do auditor interno que disciplinam sobre a competência técnico-profissional, a autonomia profissional, a responsabilidade do auditor interno na execução dos trabalhos, o relacionamento com profissionais de outras áreas e o sigilo e cooperação com o auditor independente.

A Resolução n. 828/98 trata dos papéis de trabalho e da documentação de auditoria. Apresenta, após as considerações gerais, a forma, o conteúdo, a confidencialidade, a custódia e a propriedade dos papéis de trabalho.

A Resolução n. 836/98, que trata da fraude e do erro, apresenta o conceito dos referidos termos, a responsabilidade do auditor, a detecção de fraudes e erros, as limitações inerentes à auditoria, os procedimentos, a indicação de fraude ou erro, a avaliação dos resultados dos procedimentos, as comunicações de fraude e/ou erro e a renúncia ao trabalho.

O AUDIBRA elaborou em 1991 um manual de Auditoria Interna que contempla a organização básica do setor de auditoria, os procedimentos administrativos do setor de auditoria, os procedimentos técnicos de auditoria, os testes, exames de auditoria, programa de auditoria e relatório de auditoria.

O IBRACON publicou em 1998 as Normas Internacionais de auditoria, elaboradas pela *International Federation of Accountants* (IFAC) ¹³. O IFAC, com sede nos

¹³ Extraído de <http://www.ifac.org>

Estados Unidos, é integrada por 156 organismos contábeis de 114 países, representando mais de dois milhões de contadores. As Normas Internacionais de Auditoria abrangem: responsabilidades do auditor, planejamento, controle interno, evidência de auditoria, uso do trabalho de terceiros, conclusões e parecer de auditoria, áreas especializadas, serviços correlatos e procedimentos internacionais de práticas de auditoria.

6.3- Conceito e Objetivos

Em 1958, *The Institute of Internal Auditors*, apud BACON (1973, p.3), emitiu uma declaração definindo a extensão das funções e responsabilidades da Auditoria Interna, que está sendo adotada em quase todos os países, transcrita a seguir:

*"A Auditoria Interna é uma atividade de avaliação independente dentro de uma organização para revisar as operações contábeis, financeiras e outras, com a finalidade de prestar serviços à administração. É um controle administrativo cuja função é medir e avaliar a eficiência dos outros controles."*¹⁴

Vários autores apresentam suas definições de Auditoria Interna, conforme disposto no QUADRO 14. Contudo, sempre se mantêm a avaliação e o exame como ponto central e comum a todas elas.

¹⁴ Tradução da autora.

QUADRO 14- CONCEITOS DE AUDITORIA INTERNA

AUTOR	CONCEITO
ATTIE (1992, p. 26)	“Uma função independente de avaliação, criada dentro da empresa para examinar e avaliar suas atividades, como um serviço da empresa para examinar e avaliar suas atividades, como um serviço a essa mesma organização.”
AUDIBRA (1992, p. 33)	“É uma atividade de avaliação independente e de assessoramento da administração, voltada para o exame e avaliação da adequação, eficiência e eficácia dos sistemas de controle, bem como da qualidade do desempenho das áreas em relação às atribuições e aos planos, metas, objetivos e políticas definidos para as mesmas.”
BACON (1973, p.2)	“É uma atividade de avaliação independente dentro de uma organização, cuja finalidade é examinar as operações contábeis, financeiras e administrativas, como base para a prestação de um serviço efetivo aos mais altos níveis da direção.”(*)
CFC (2000, p.261)	“Conjunto de procedimentos técnicos que tem por objetivo examinar a integridade, adequação e eficácia dos controles internos e das informações físicas, contábeis, financeiras e operacionais da Entidade.”
KOHLER (1963, p.174)	“É exercida por pessoal da organização como uma função de assistência e assessoramento de alto nível e constitui um importante elemento de avaliação do controle interno.”(*)
IBRACON (1998, p.161)	“É uma atividade de avaliação organizada dentro de uma entidade, como um serviço para a entidade. Suas funções incluem, entre outras coisas, examinar, avaliar e monitorar a adequação e eficácia dos sistemas contábeis e de controle internos.”
HOLMES (1972, p.3)	“É um ato de avaliação independente dentro de uma organização para a revisão das operações contábeis, financeiras e outras como base de um serviço construtivo para a gerência. É um tipo de controle que mede e avalia outros controles. Trata, primordialmente, de assuntos contábeis e financeiros, porém, trata também com propriedade de assuntos de natureza operacional.” (*)

FONTE- Elaborado pela autora da dissertação.

(*) Tradução da autora.

Assim, a auditoria interna observa, indaga, analisa, verifica, investiga e avalia, de forma independente, dentro de uma organização, as operações contábeis, financeiras,

operacionais e administrativas, visando prestar relevantes serviços à administração. É uma atividade de assessoramento, e não de execução, cuja principal função é avaliar outros controles.

No Brasil a Lei n. 10.180/2001 estabelece normas de controle interno e fixa procedimentos de auditoria para o Serviço Público Federal. Transcrito a seguir está o art. 24 do referido diploma legal:

“Art. 24. Compete aos órgãos e às unidades do Sistema de Controle Interno do Poder Executivo Federal:

I - avaliar o cumprimento das metas estabelecidas no plano plurianual;

II - fiscalizar e avaliar a execução dos programas de governo, inclusive ações descentralizadas realizadas à conta de recursos oriundos dos Orçamentos da União, quanto ao nível de execução das metas e objetivos estabelecidos e à qualidade do gerenciamento;

III - avaliar a execução dos orçamentos da União;

IV - exercer o controle das operações de crédito, avais, garantias, direitos e haveres da União;

V - fornecer informações sobre a situação físico-financeira dos projetos e das atividades constantes dos orçamentos da União;

VI - realizar auditoria sobre a gestão dos recursos públicos federais sob a responsabilidade de órgãos e entidades públicos e privados;

VII - apurar os atos ou fatos inquinados de ilegais ou irregulares, praticados por agentes públicos ou privados, na utilização de recursos públicos federais e, quando for o caso, comunicar à unidade responsável pela contabilidade para as providências cabíveis;

VIII - realizar auditorias nos sistemas contábil, financeiro, orçamentário, de pessoal e demais sistemas administrativos e operacionais;

IX - avaliar o desempenho da auditoria interna das entidades da administração indireta federal;

X - elaborar a Prestação de Contas Anual do Presidente da República a ser encaminhada ao Congresso Nacional, nos termos do art. 84, inciso XXIV, da Constituição Federal;

XI - criar condições para o exercício do controle social sobre os programas contemplados com recursos oriundos dos orçamentos da União."

Segundo BACON (1973, p.3), o objetivo da auditoria interna "é prestar um serviço de assistência construtiva para a Administração, com o propósito de melhorar a condução das operações e obter maiores benefícios econômicos para a empresa e o cumprimento mais eficaz de seus objetivos institucionais." ¹⁵ O AUDIBRA (1991, p.34-35) entende que os objetivos da Auditoria Interna são:

- a)* Avaliar os componentes das demonstrações financeiras da organização, os procedimentos concernentes aos tributos, a integridade e confiabilidade das informações e os registros contábeis e operacionais.
- b)* Avaliar os sistemas estabelecidos para assegurar a observância das políticas, metas, leis, normas e regulamentos da organização, bem como os controles para proteção dos ativos.
- c)* Avaliar a economicidade, eficácia e eficiência da obtenção e utilização dos recursos, nos sistemas de operação da entidade, bem como alternativas possíveis para atingir os mesmos objetivos, comparativamente, com vantagens.
- d)* Avaliar se as atividades estão em consonância com os objetivos da organização, e se as normas, procedimentos, controles internos quanto ao aspecto de eficiência, efetividade, qualidade e segurança, inclusive prevenindo e relatando erros.
- e)* Avaliar a qualidade dos serviços prestados, especialmente quanto ao atendimento, à presteza, à segurança e à economicidade.
- f)* Prestar apoio ao administrador e acompanhar o cumprimento de recomendações decorrentes de trabalhos de auditoria interna e externa e a correção de problemas de caráter organizacional, estrutural, operacional e sistêmico sugeridos.
- g)* Elaborar o Plano Anual de Auditoria e o Relatório Anual de Auditoria e de seus resultados.

¹⁵ Tradução da autora.

Mediante tais objetivos, pode-se concluir que para atingi-los é necessário que a Auditoria Interna esteja vinculada ao nível mais alto da organização. Para atender à administração em seus anseios e necessidades, a Auditoria Interna deve ter autonomia e independência para atuar dentro da organização.

Atuar com independência significa ter liberdade de acesso a todas as áreas e informações da entidade, irrestritamente. Ter autonomia é poder definir seu papel dentro da organização, planejar e exercer com competência e eficácia a sua função de forma a ser aceita por todos os níveis da instituição.

6.4- Modalidades

Partindo do pressuposto de que o auditor executa seu trabalho contemplando todas as áreas da organização, fica claro que a auditoria interna deve ser estruturada no sentido de praticar todas as modalidades de auditoria.

Nesta dissertação, serão identificadas as modalidades de Auditoria Interna classificadas pelo AUDIBRA (1991, p.55). Dentre tais, incluem-se aquelas exercidas pela AUDIM, conforme será exposto no capítulo 7.

As modalidades adiante relatadas são: Auditoria Contábil e Tributária, Auditoria Operacional, Auditoria Gestional, Auditorias Especiais e Auditoria de Sistemas ou Auditoria das Tecnologias da Informação.

6.4.1- Auditoria Contábil e Tributária:

A Auditoria Contábil trata do exame das demonstrações financeiras, dos registros contábeis e dos demais documentos, para avaliar se os componentes desses instrumentos estão apresentados em conformidade com os princípios contábeis, com a sistemática dos controles internos, normas, regulamentos e padrões aplicáveis.

FRANCO e MARRA (1989) conceituam auditoria contábil como:

“a técnica contábil que - através de procedimentos específicos que lhe são peculiares, aplicados no exame de registros e documentos, inspeções, e na obtenção de informações e confirmações, relacionados com o controle do patrimônio de uma entidade - objetiva obter elementos de convicção que permitam julgar se os registros contábeis foram efetuados de acordo com os princípios fundamentais e normas de contabilidade e se as demonstrações contábeis deles decorrentes refletem adequadamente a situação econômica-financeira do patrimônio, os resultados do período administrativo examinado e as demais situações nelas demonstradas”.

Fica claro que o objetivo principal dessa auditoria é evidenciar se as demonstrações financeiras expressam a real situação econômica e financeira da organização e se estão em conformidade tanto com os princípios de contabilidade geralmente aceitos quanto com a legislação aplicável.

A Auditoria Tributária procede ao exame e avaliação de planejamento tributário, observando se os controles adotados para as operações, pagamentos e recuperação dos tributos e demais ônus afins estão sendo processados com eficácia e rigor no cumprimento da legislação tributária.

COOK (1981, p. 15) entende que:

“os aspectos mais difíceis do trabalho de assessoria fiscal estão justamente no planejamento tributário das entidades. Os auditores prestam serviço valioso a pessoas físicas e jurídicas, assessorando-as nas questões fiscais, buscando diminuir suas obrigações fiscais e cuidando para que cumpram as disposições legais desse campo”.

Conforme o AUDIBRA (1991, p. 58), os objetivos da Auditoria Contábil e Auditoria Tributária são:

- a) exatidão, fidedignidade, justeza, completabilidade e tempestividade da apresentação e da publicação das demonstrações financeiras e de quaisquer relatórios formais ou institucionais de natureza orçamentária, financeira, contábil ou tributária;

- b)* fidedignidade, integridade, adequação, confiabilidade e utilidade dos registros orçamentários, financeiros, econômicos e contábeis;
- c)* correção, eficácia e adequação dos controles da guarda, da divulgação, do arquivo, dos meios de consulta e da informatização da documentação pertinente à área contábil e tributária;
- d)* adequação e eficácia dos controles, registros e meios de proteção dos ativos e da comprovação da existência real, da utilidade, da ociosidade e da economicidade dos mesmos, bem como a comprovação da autenticidade e completabilidade dos passivos;
- e)* eficiência, eficácia e economicidade na utilização dos recursos e na administração contábil/financeira e tributária de fundos e programas;
- f)* cumprimento das políticas, procedimentos, normas legais e regulamentares, metas e objetivos com abrangência na área auditada;
- g)* exame e avaliação das aplicações de recursos, observando o cumprimento de normas legais, institucionais e aspectos contratuais pertinentes;
- h)* avaliação de alcance dos objetivos das operações financeiras, investimentos, imobilizações, obrigações, despesas, receitas, fundos e programas, etc.;
- i)* exame e avaliação das fontes de recursos, observando os aspectos econômicos sobre a tempestividade de sua aplicação;
- j)* exame e avaliação da rentabilidade das aplicações e sua contribuição na formação do resultado da entidade;
- k)* transparência, adequação e tempestividade das informações, particularmente em relação aos Princípios Fundamentais de Contabilidade aplicados;
- l)* emissão de opinião sobre as demonstrações financeiras, fundos e Programas e Planos de natureza financeira instituídos ou administrados pela entidade;
- m)* assessoramento ao Conselho Fiscal em matéria compreendida no âmbito da sua competência específica; e
- n)* acompanhamento dos trabalhos de Auditoria Externa.

Nas entidades governamentais, por exigência dos órgãos de fiscalização externa ao Poder Executivo, a preparação das contas para as tomadas de contas dos ordenadores da despesa é um objetivo que se acrescenta aos outros da Auditoria Contábil.

Salienta-se que a Administração Pública tem dois sistemas contábeis. O aplicável aos órgãos da Administração Direta, Autarquias e Fundações, recomendado pela Lei Federal n. 4.320/64; e o aplicável às Sociedades de Economia Mista e às Empresas Públicas, que obedece à legislação comercial e tributária concernente à Lei Federal n. 6.404/76.

6.4.2- Auditoria Operacional

Para compreender esta modalidade de auditoria, faz-se necessário definir os termos que lhes são afetos, quer sejam: eficácia, eficiência e economicidade.

Por eficácia entende-se a maior aproximação dos objetivos alcançados em relação aos objetivos almejados. Compreende a consecução dos objetivos do planejamento com os meios e recursos disponíveis.

A eficiência pode ser compreendida como a relação entre a produção de bens e serviços ou outros resultados obtidos por uma entidade ou unidade econômica e os recursos utilizados para produzi-los ou executá-los. Significa a capacidade de maximização de objetivos a partir de um orçamento de gastos determinados.

A economicidade refere-se às condições de aquisições dos recursos materiais, humanos e financeiros na quantidade e qualidade apropriadas e ao menor custo possível.

A Auditoria Operacional está voltada para a avaliação da eficácia, da eficiência e da economicidade empregadas nas atividades da organização, na aplicação de seus recursos e no cumprimento de objetivos e metas determinados.

Essa modalidade de auditoria surgiu, em 1947, da "Declaração de Responsabilidade do Auditor Interno", *apud* AUDIBRA (1991, p.59), que afirmava que auditor interno não lida somente com matéria contábil, mas também com assuntos de natureza

operacional. Em 1950, a Auditoria Operacional ganhou novo enfoque, pois, abrangeu áreas não previstas para a auditoria tradicional. Assim, uma situação abordada numa auditoria pode resultar num exame financeiro tradicional ou pode ter uma visão gerencial buscada pela Auditoria Operacional.

COOK (1981, p. 253) define a Auditoria Operacional como um exame e uma avaliação abrangente das operações de uma empresa, com a finalidade de informar a Administração se as várias atividades são ou não cumpridas de modo compatível com as políticas estabelecidas, com vistas à consecução dos seus objetivos. Faz parte da auditoria uma avaliação do uso profícuo de recursos humanos e materiais, assim como uma apreciação dos vários procedimentos operacionais. A auditoria deve compreender, também, recomendações para a solução dos problemas e de métodos para aumentar a eficiência e os lucros.

O TCU define na Portaria n. 63/96 que a Auditoria Operacional incide em todos os níveis de gestão sob o ponto de vista da economia, da eficiência e da eficácia, nas fases da programação, execução e supervisão.

Segundo ARTER (1995, p. 3), o Instituto Internacional de Auditores considera que:

"na Auditoria Operacional são examinadas a confiabilidade e a integridade da informação; a conformidade com políticas, planos, procedimentos, leis e regulamentos, bem como a proteção dos bens; a utilização econômica e eficiente dos recursos e a realização dos objetivos estabelecidos."

Dessa forma, a Auditoria Operacional pode começar por uma auditoria da legalidade, vez que existem normas que atuam como mecanismos de controle de eficiência e economicidade, como é o caso da Lei de Licitações para as aquisições e contratações da área governamental. Além disso, existem outras normas que regulam os aspectos tributários, financeiros, orçamentários e administrativos que influem na organização do setor público. Destarte, é comum enquadrar nesta modalidade as auditorias realizadas nas áreas de Pessoal, Patrimonial, Almoxarifado, Licitação e Contratos, que

são muito utilizadas pelas auditorias internas da Administração Pública. A FIG. 06 sintetiza esse enquadramento.

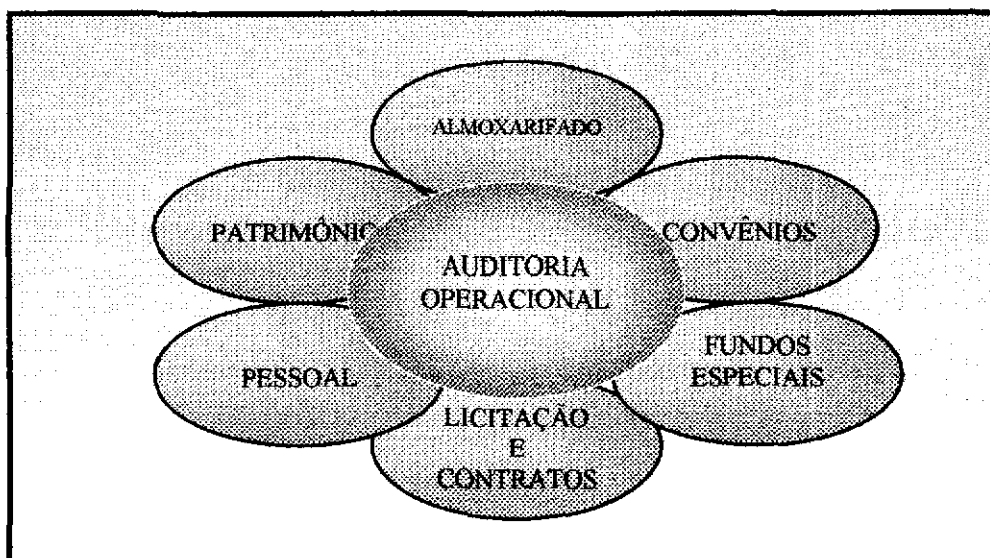


FIGURA 06- Áreas enquadradas na modalidade de Auditoria Operacional do Setor Público

FONTE- Elaborado pela autora da dissertação.

Conforme o AUDIBRA (1991, p. 61), os objetivos da Auditoria Operacional são:

- a)* avaliar os controles gerenciais internos quanto à sua adequação e eficácia;
- b)* identificar falhas e irregularidades no ciclo operacional;
- c)* avaliar a adequação e qualidade da entidade, administração e pessoal;
- d)* avaliar o desempenho do setor auditado e do seu ciclo operacional;
- e)* adequar os procedimentos operacionais;
- f)* cumprir e aperfeiçoar as normas aplicáveis;
- g)* integrar os órgãos e setores envolvidos na operação;
- h)* avaliar os registros e dos sistemas de informações gerenciais;
- i)* observar os contingenciamentos orçamentários e legais à operação;
- j)* promover a aderência das ações operacionais administrativas às políticas, planos e diretrizes;
- k)* examinar as alternativas quanto ao seu potencial para atingir os objetivos com maior economia e eficiência;

- l)* verificar as causas de ineficiência ou desperdícios;
- m)* avaliar as operações e programas quanto aos custos/benefícios, aos padrões de custo originalmente previstos e aos resultados esperados;
- n)* zelar pela fidedignidade e integridade das informações operacionais, gerenciais e meios utilizados para identificar, aferir, classificar e comunicar essas informações;
- o)* cuidar da economicidade, eficácia e eficiência da utilização dos recursos;
- p)* cuidar da qualidade e eficiência dos sistemas e fluxos estabelecidos para assegurar a observância das políticas, planos, procedimentos, leis, normas e regulamentos aplicáveis aos serviços, programas e operações e a sua observância efetiva em todos os níveis gerenciais;
- q)* cumprir os objetivos e metas estabelecidas para os serviços, operações e programas;
- r)* promover a adequação e grau de compreensão das normas operacionais; e
- s)* promover a adequação, fidedignidade e eficácia dos relatórios e informações adotados em relação às operações e programas.

ALMEIDA (1993, p.150) afirma que para o alcance dos objetivos da Auditoria Operacional, a Auditoria Interna da organização deve estabelecer indicadores de desempenho e padrões de desempenho.

Indicadores de desempenho são fatores qualitativos e quantitativos, que fornecem à Administração da organização os indícios do grau de eficiência e eficácia com que são conduzidas as operações. São classificados em três tipos:

- a)* indicadores de carga de trabalho, que medem a quantidade de serviço prestado ou de trabalho feito;
- b)* indicadores de economia e eficiência, que fazem a associação das cargas de trabalho com os recursos empregados ; e
- c)* indicadores de eficácia, que servem para avaliar se a atividade está atingindo suas metas e se são voltados para resultados e não para os custos.

Padrões de desempenho representam o nível desejado ou o grau de realização em confronto com o qual a Administração e o auditor medem o desempenho real, tentando determinar a economia, a eficiência ou a eficácia relativa conseguida de fato. Podem ser obtidos em diversas fontes. As fontes internas são por exemplo: dados históricos ou metas e objetivos pré-determinados pela organização. As fontes externas podem ser pesquisas independentes ou aquelas voltadas às entidades de classe. Pode-se também encontrá-las em legislação ou regulamentação externas.

Uma vez identificados os indicadores e padrões de desempenho mais significativos, coletados dados para medir o desempenho, passa-se para a sua análise, durante a qual o desempenho real é comparado com os padrões, a fim de se determinar quão econômica, eficiente e eficaz está a organização.

6.4.3- Auditoria Gestional

A Auditoria Gestional é um assunto abrangente e moderno. Envolve a complementação da Auditoria Operacional, valendo-se de todos seus instrumentos, concluindo sobre as áreas auditadas e os sistemas avaliados. Assim, todos os enfoques de operacionalização são rediscutidos e estudados profundamente, para ser definido o sistema organizacional que será aplicado no futuro. É um momento dinâmico de mudanças e transformações nas bases administrativas da empresa, visando a continuidade operacional da organização.

O Conselho Federal de Economia define, através da Resolução n. 1.612/95, que a Auditoria Gestional objetiva verificar a adequação da empresa quanto à formação de políticas de recursos humanos, do plano estratégico e do programa de qualidade, nos seus aspectos econômicos e financeiros.

Segundo GIL (1999, p.38-39), a Auditoria Gestional tem os seguintes objetivos:

- a)* participar da Auditoria Interna em todos os momentos empresariais;

- b)* contribuir com a Auditoria Interna para a manutenção da organização na vanguarda tecnológica e do segmento econômico de que participa;
- c)* avaliar o posicionamento/situação futura da organização, via auditoria de simulações e previsões organizacionais;
- d)* estimular os líderes empreendedores;
- e)* institucionalizar os critérios de rodízio, negociação e participação no ambiente auditoria/empresa; e
- f)* avaliar as iniciativas empresariais propostas.

Está estabelecido na Norma n. 310.04 do AUDIBRA que na execução de seu programa de auditoria com enfoque gestional o auditor tem a responsabilidade de examinar os sistemas, critérios, políticas e procedimentos utilizados pela organização na sua área de planejamento estratégico e tático, no seu processo decisório, bem como a qualidade de estrutura de controles internos gerenciais e sua observância.

A Auditoria Interna, utilizando-se dos recursos da Auditoria Gestional, poderá propiciar à administração que o desempenho da organização quanto ao seu planejamento estratégico e tático, às tomadas de decisão, bem como à definição de metas e alcance dos objetivos pretendidos, possa ser eficiente e eficaz, tanto no plano presente quanto no futuro.

6.4.4- Auditorias Especiais

A Auditoria Especial abrange a realização de trabalhos especiais de auditoria não compreendidos na programação anual de auditoria da organização. Visa ao exame de fatos ou situações consideradas relevantes, de natureza incomum ou extraordinária, podendo ser provocada por suspeita de irregularidade na gestão de recursos financeiros, fraudes ou verificações que envolvem desempenho dos administradores.

Conforme o AUDIBRA (1991, p. 63), os objetivos da Auditoria Especial relacionam-se ao exame de fraudes e irregularidades, desmobilização, aquisição de entidade, contratos especiais de grande vulto e outros trabalhos especiais de auditoria não

compreendidos na programação normativa da área e solicitados pelos membros dos Conselhos de Administração, Fiscal, Diretoria ou determinados em legislação específica.

Ao final dos trabalhos, deve ser emitido relatório constando os resultados dos fatos verificados, sendo este de caráter confidencial.

6.4.5- Auditoria de Sistemas

Com o crescimento do uso da informatização nas organizações, expandiu-se a necessidade de proteger dos dados e informações processados pelos sistemas baseados nesta tecnologia. Desse contexto, surgiu a Auditoria de Sistemas, também denominada Auditoria das Tecnologias da Informação.

Segundo GIL (1999, p.35), a Auditoria de Sistemas emerge da consolidação de três áreas distintas do conhecimento: auditoria, sistemas de informação e processamento eletrônico de dados ou informática. Conforme o CRCSP (1999, p. 93) a Auditoria de Sistemas certificar-se de que:

- a)* as informações são corretas e oportunas;
- b)* existe um processamento adequado das operações;
- c)* as informações estão protegidas contra fraudes;
- d)* existe a proteção das instalações e equipamentos; e
- e)* existe a proteção contra situações de emergência (paralisação de processamento, perda de arquivos, inundação, incêndios, etc.).

O AUDIBRA (1991, p. 63) sustenta que os objetivos da Auditoria de Sistemas contemplam:

- a)* o processo de planejamento, desenvolvimento, teste e aplicação de sistemas;
- b)* a estrutura lógica, física, ambiental e organizacional de controle, bem como a segurança e proteção dos ativos específicos, sistemas e documentações, *software* e informações; e

- c) a qualidade da estrutura de controles internos sistêmicos e de sua observância em todos os níveis gerenciais.

De acordo com o *Statement Of Auditing Standards* (SAS) n. 3, estabelecido pelo *American Institute of Certified Public Accountants* ¹⁶ os procedimentos de controle internos relacionados aos sistemas computadorizados que são avaliados na realização de uma Auditoria de Sistemas, são classificados em: **controles gerais e controles de aplicação.**

Os controles gerais envolvem todos os aspectos de Centro de Processamento de Dados da estrutura, quer sejam:

- a) plano de organização e de operação das atividades de processamento eletrônico de dados;
- b) procedimentos para documentação, revisão, teste e aprovação de sistemas ou programas;
- c) controles de equipamentos de processamento de dados; e
- d) controles de acesso ao equipamento e arquivos de dados.

Os controles de aplicação relacionam-se com o controle específico das aplicações do sistema computadorizado. Sua função é proporcionar segurança nos registros e processamento e exatidão nos relatórios de dados. São classificados em: **de entradas de dados; de processamento; e de saída de informações.**

Acrescentam-se a esses o controle de **desenvolvimento de sistemas**. Segundo FILOMENA (1988, p.22), este tipo de controle proporciona a implantação de sistemas mais seguros e eficientes. Nesta fase de desenvolvimentos de sistemas, é tarefa da auditoria interna assessorar o planejamento da inclusão de procedimentos e rotinas para a avaliação do desempenho dos sistemas, permitindo assim seu aperfeiçoamento.

¹⁶Extraído de [http:// www.aicpa.org](http://www.aicpa.org)

Diante o exposto, fica evidente que a Auditoria de Sistemas é uma modalidade de auditoria dinâmica e importante, vez que assegura a correta e oportuna utilização de bens, valores e recursos da organização.

O tema Auditoria de Sistemas será abordado minuciosamente no capítulo 7 desta dissertação.

6.5 Modelagem e Programa de Auditoria Interna

6.5.1- Introdução

A palavra **modelagem** pode ter sentidos distintos, em função da área de pesquisa em que estiver vinculada. Contudo, em seu cerne, significa construir um modelo, utilizar-se de um modelo ou representar por meio de modelo.

BUENO (1969, p. 820) define modelagem como a operação de modelar e modelar como aquilo que serve de modelo ou representa por meio de modelo.

O uso de modelos tem por objetivos simular, simplificar, tornar mais claros e concisos os processos, situações, operações, atividades e sistemas. Servem, também, como *orientadores de procedimentos para determinadas situações ou problemas*.

Segundo OLIVEIRA (1998, p. 91), modelo constitui a representação abstrata e simplificada de um sistema real, com a qual se pode ser explicado e testado o comportamento do mesmo, em seu todo ou em partes.

STAIR (1998, p. 10-11) define modelo como uma abstração ou uma aproximação que é usada para simular a realidade. Explica que o mundo real é complexo e dinâmico, e por isso, usamos modelos em lugar de sistemas reais. O autor apresenta vários tipos de modelos, dentre os quais destaca:

- a)* modelo narrativo: baseia-se em palavras e descrições da realidade, tanto verbais quanto escritas;
- b)* modelo matemático: é uma representação aritmética da realidade;
- c)* modelo esquemático: é uma representação gráfica da realidade, utilizando-se de gráficos, mapas, figuras, diagramas, ilustrações ou fotografias; e
- d)* modelo físico: é uma representação tangível da realidade, o qual permite obter informações.

Conforme a necessidade de informações, utiliza-se o tipo de modelo que for mais apropriado. Em auditoria, utiliza-se a modelagem para descrever sistemas administrativos, objetivando uma compreensão mais rápida e perfeita do funcionamento de sistemas complexos.

Para realizar uma auditoria adequada, é indispensável que o auditor saiba qual o objetivo da auditoria a ser realizada e quais os procedimentos e técnicas a serem adotados para a concretização dos seus trabalhos. Para alcançar isto, é necessária a preparação de descrições narrativas através de um programa detalhado que contenha informações sobre o objetivo e o escopo da auditoria a ser executada. O modelo que é objeto de análise nesta seção é o **Programa de Auditoria**, que possui as definições listadas no QUADRO 15.

QUADRO 15- CONCEITOS DE PROGRAMA DE AUDITORIA

AUTOR	CONCEITO
ATTIE (1995, p.85)	“Corresponde ao plano de ação voltado a orientar e controlar a execução exames de auditoria que está dividido em três partes: - Objetivo de auditoria: é o que o auditor quer atingir. - Determinação do escopo do trabalho: com base no conhecimento obtido do controle interno e a relevância e relatividade, é o estabelecimento da extensão dos procedimentos de auditoria e o momento de sua aplicação. - Procedimentos de auditoria: as investigações técnicas a serem praticadas pelo auditor para atingir os objetivos previamente definidos.”
AUDIBRA (1991, p.293)	“É a forma estruturada de orientar o trabalho do Auditor, no sentido de viabilizar a execução de um exame compreensivo, adequado às exigências e responsabilidades profissionais, revestido da necessária completabilidade, abrangência e utilidade para o fim a que se destina. É, portanto, um elemento técnico capaz de propiciar eficiência e eficácia ao trabalho do Auditor.”
BACON (1973, p.55)	“É a compilação racional, metódica e pormenorizada de práticas comuns de auditoria interna e de avaliação do controle interno, baseadas em preceitos oficiais de cumprimento obrigatório e em procedimentos técnicos geralmente aceitos, aplicáveis total ou parcialmente a todos os departamentos da organização. É uma orientação para o auditor e um guia para maior eficácia de seu trabalho.” (*)
HOLMES (1972, p.41-42)	“É um plano detalhado do procedimento da auditoria. A imaginação e a iniciativa devem entrar em jogo em todo momento, por mais cuidadosamente planejado que esteja o programa, já que não se podem prever todas as contingências concebíveis em cada auditoria diferente.” (*)

FONTE- Elaborado pela autora da dissertação.

(*) Tradução da autora.

Por ser um roteiro dirigido ao ciclo sistêmico, operacional e contábil, objeto da atenção do auditor, indicando passo a passo os procedimentos e técnicas a serem aplicadas pelo mesmo em cada fase da operação, garante um alto nível de qualidade nos trabalhos, padroniza procedimentos e norteia de maneira eficiente o trabalho do auditor, independentemente do grau de afinidade que tenha com a área; serve também para evitar lacunas e riscos similares no âmbito total do trabalho a ser executado pelo mesmo.

O programa, quando corretamente estruturado, serve não só como instrumento eficaz para o trabalho do auditor mas, também, para a supervisão e o treinamento.

Em termos de custo/benefício, o programa de auditoria se torna um instrumento essencial para a otimização das horas disponíveis para controle, possibilitando um maior rendimento de cada auditor.

Os objetivos do programa de auditoria, de acordo com o AUDIBRA (1991, p. 294), são:

- a)* estabelecer um plano de ação ordenado em relação ao trabalho do auditor;
- b)* dirigir a execução dos seus trabalhos;
- c)* registrar a forma de execução desses trabalhos;
- d)* proporcionar uma visão antecipada dos exames a serem efetuados; e
- e)* otimizar os tempos de execução, sem perda da eficácia, dimensionando esforços e composição de equipes de auditores.

Destarte, o programa objetiva obter uma visão completa dos exames a serem efetuados pelo auditor e sua seqüência de aplicação. Isso implica a necessidade de um certo rigor na sua estrutura, indicando da forma mais detalhada possível, tudo o que deve ser feito. DAVIES (1974, p.11) doutrina que:

“o costume de seguir um programa definido, especialmente para cada trabalho que se vá a empreender, tem vantagens definitivas, sobretudo quando este vai ser

feito principalmente por meio de ajudantes; quando se prepara um programa de auditoria, este deve ser suficientemente detalhado, e as instruções de tal maneira claras e definidas que não possa haver má interpretação delas. À medida que se completa uma parte do trabalho deve fazer-se anotações no programa, indicando quem a executou, o período coberto, em tal forma que o programa se converta em um registro permanente do trabalho efetivamente feito. Este programa assegura também a uniformidade e protege o auditor da possibilidade de descuidar de pontos importantes.”¹⁷

Contudo, o programa de auditoria não deve, pondera MONTGOMERY (1954, p.27), ser imutável e anular toda a independência de critério do auditor; ou seja, a criatividade e a percepção do auditor interno não devem ser neutralizadas pelos procedimentos sistematizados do programa.

6.5.2- Postulados Básicos do Programa de Auditoria

O AUDIBRA (1991, p.295) doutrina que o programa de auditoria baseia-se nos seguintes postulados:

- a) como instrumento de trabalho do auditor: um instrumento obrigatório para possibilitar ao auditor executar o exame no todo ou em parte de um ciclo operacional, sistêmico, contábil ou mesmo para efetuar uma verificação especial que estas apresentam no geral características muito diferenciadas, com a necessária completabilidade, segurança e profissionalismo. Como instrumento técnico que é deve ser completo, útil e apresentar condições adequadas de execução, possibilitando ao auditor o cumprimento de todos os requisitos técnico-profissionais que lhe são exigidos;*
- b) controle perfeito: por controle perfeito entende-se aquele que examina na integralidade, o efeito de uma operação ou do conjunto de algumas operações decorrentes da atividade da entidade, envolvendo nesse exame a comprovação e a análise da estrutura da organização, das normas, dos sistemas de controles, dos procedimentos, dos planos, dos registros e das informações delas decorrentes. O*

¹⁷ Tradução da autora.

conceito de controle perfeito, portanto, não significa que necessariamente deve ser examinada a totalidade das transações, mas, apenas que uma certa parte delas será individual e integralmente examinadas, sendo as demais, tratadas através de exceções, totais ou lotes;

- c) princípio do fluxo racional e harmônico: é estruturado dentro do princípio do fluxo racional e harmônico das operações da empresa. Entende-se por fluxo racional aquele que acompanha a seqüência lógica, etapa por etapa, de uma operação, sistema, procedimento ou processo. Entende-se por fluxo harmônico, aquele que propicia a interação das várias partes de um sistema ou processo, na própria área ou com as demais áreas da entidade ou fora dela, sem causar pontos de estrangulamento, congestionamento ou atraso da operação; e
- d) exigências profissionais: o programa de auditoria é um instrumento de trabalho preparado pela auditoria interna, para aplicação sistemática pelos auditores designados para efetuar os exames.

Como tal, deve abranger exatamente a tarefa a ser executada. Poderá, entretanto, ser alterados, na medida em que os procedimentos básicos da área, as normas e os sistemas em uso forem modificados. Cabe, novamente, à auditoria interna, efetuar essas manutenções do programa, de modo a mantê-lo atualizado e, portanto, em condições de aplicação pelo auditor incumbido do trabalho. Com respeito às exigências profissionais sobre a gerência de auditoria e o programa de auditoria, fazemos referência às seguintes “Normas para o Exercício Profissional de Auditoria Interna”:

“4 10.02 Para poder cumprir suas tarefas de modo eficaz e eficiente, em conformidade com os objetivos definidos em conjunto com a administração e com os requisitos profissionais exigidos, o órgão de Auditoria Interna deve contar com uma adequada estrutura de apoio logístico seus auditores.

410.02.01 A Auditoria Interna deve atuar sobre todos os setores e atividades da organização e sob diferentes enfoques técnicos. A efetividade do seu desempenho depende de maneira decisiva do apoio logístico fornecido ao auditor designado para a execução dos trabalhos.

4 10.02.02 Na elaboração do programa de auditoria, o gerente de Auditoria aplicará o seu julgamento profissional de maneira a assegurar que esse programa possibilitará ao seu executor o atingimento de forma dos objetivos nele estabelecidos.”

Segundo seu critério e conforme a capacitação de seus auditores assistentes o gerente de auditoria poderá delegar aos mesmos a execução das medidas preparatórias ou mesmo da elaboração do programa de auditoria.

- e) cobertura de riscos: é estruturado de forma a incluir no corpo da instrução ao auditor, os procedimentos e natureza de testes mais adequados a cada situação, visando obter maior precisão no resultado, melhor cumprimento dos objetivos e a mais ampla cobertura dos riscos no ciclo de operações sob exame.

6.5.3- Estrutura do Programa de Auditoria

Para servir ao propósito de otimizar a qualidade e o tempo de execução dos trabalhos, o AUDIBRA (1991, p. 299) preceitua que o programa deva ser estruturado de forma modular, abrangendo os tópicos referentes ao objeto, objetivos, avaliação da organização e seus controles internos, roteiro programado, questionários auxiliares, diagnósticos e comprovações numéricas.

As seções 6.5.31 a 6.5.4.1, foram consolidadas a partir do estudo da obra “Procedimento de Auditoria Interna” publicada pelo AUDIBRA (1991, p. 293-340).

6.5.3.1 – Objeto ou Área a ser Auditada

Este módulo trata de definir, de maneira sucinta as características da área ou da atividade a ser auditada. Isto propicia ao auditor um nível mínimo de informações que permita-lhe avaliar, desde logo, a importância, complexidade da área e, portanto, a problemática de controle que terá pela frente.

6.5.3.2 - Objetivos do Programa de Auditoria

Neste módulo, são definidos os objetivos determinados pela gerência da auditoria interna que devem ser alcançados através da execução do programa de auditoria.

A variedade e a natureza desses objetivos decorrem das responsabilidades atribuídas ao departamento, da programação combinada com a alta direção e com as exigências profissionais que recaem sobre o auditor interno.

A nítida determinação dos objetivos e a correta transmissão deles de maneira formal, ao auditor responsável pela execução do programa são de importância fundamental, na medida em que possibilitam a ele e ao seu supervisor analisar o resultado da sua aplicação e, ainda, na fase de pré-relatório, verificar em que extensão há evidências de que esses objetivos foram alcançados. Em caso de insuficiência, a revisão das causas poderá indicar a falta de execução de partes do programa de auditoria, a incompletabilidade do programa ou a deficiência do próprio programa ou dos auditores encarregados pela sua execução. Este caso extremo indicaria que o programa não foi orientado na direção adequada para atingir os objetivos determinados.

É importante notar que os objetivos não são elementos isolados no contexto do programa de auditoria, sendo que em geral um mesmo exame pode visar vários objetivos de maneira simultânea.

No caso da auditoria independente, seu objetivo básico quanto ao exame das demonstrações financeiras é a emissão de um parecer sobre a adequação com que tais demonstrações representam a posição econômico-financeira da organização. No caso da auditoria interna, dependendo da natureza e enfoque de cada trabalho, os objetivos podem ser mais amplos, abrangendo por exemplo, o/a:

- a)* cumprimento das normas administrativas e financeiras estabelecidas;
- b)* opinião sobre a exatidão, legitimidade, legalidade, regularidade, formalismo e tempestividade da tomada de contas dos responsáveis;

- c)* utilização de subvenções, doações e suprimentos de fundos repassados e ou recebidos pelo Estado;
- d)* cumprimento de acordos, convênios, contratos e programas;
- e)* cumprimento de processos licitatórios e de compras em geral;
- f)* exame do grau de execução orçamentária e observância de seus limites;
- g)* exame da regularidade e legalidade das contas;
- h)* exame da eficiência, eficácia e economicidade das atividades;
- i)* comprovação da veracidade das informações e relatórios contábeis, financeiros e operacionais dos órgãos e entidades do Estado;
- j)* uniformidade e correção dos registros contábeis;
- k)* segurança e proteção dos ativos;
- l)* opinião interna sobre as demonstrações financeiras;
- m)* avaliação do processo decisório, do sistema de planejamento estratégico e da qualidade das diretrizes e normas;
- n)* avaliação do plano sistêmico e da organização, custos e desempenho da área de sistemas informatizados;
- o)* avaliação dos sistemas de controle interno gerencial, contábil e sistêmico;
- p)* avaliação da adequação, eficiência, eficácia e economicidade nos fluxos operacionais; e
- q)* avaliação do desempenho geral e da qualidade da organização.

Esses objetivos devem ser determinados em função de cada trabalho que será examinado pelo auditor.

6.5.3.3- Avaliação da Organização e seus Controles Internos

A avaliação da organização e de seus controles internos permite à auditoria interna obter uma visão antecipada da qualidade das estruturas e dos fluxos operacionais e de controle da organização auditada. Essa visão assume papel fundamental na continuidade do seu trabalho. Tal análise envolve o questionamento sobre a qualidade, completabilidade, justificativa, razoabilidade, adequação e pertinência das normas, diretrizes e planos.

Uma das formas mais usuais e recomendadas pelo AUDIBRA (1991, p.308), consiste na utilização de fluxogramas dos procedimentos, normas, diretrizes e instruções operacionais e de controle, de forma a poder obter uma visão abrangente e compreensiva, em curto prazo, dos aspectos relevantes, dos pontos fracos e dos riscos latentes na estrutura operacional e de controle da entidade.

Esse procedimento apresenta as seguintes vantagens para o auditor:

- a)* serve, na fase de preparação do programa de auditoria, para obter uma visão abrangente dos fluxos operacionais e de controle da entidade;
- b)* ainda nessa fase, o resultado desse trabalho pode, ensejar a produção relatório de recomendação e de alerta sobre a eficiência, eficácia, lógica, completabilidade, razoabilidade dos sistemas de controles e dos fluxos operacionais;
- c)* passa a ser a base para a preparação do programa de auditoria, e de eventuais questionários para comprovação de pontos chaves de controle da operação;
- d)* serve de memória sobre os procedimentos e estruturas, objeto dos exames da auditoria e , portanto, facilita o treinamento de auditores; facilita discussão com as áreas operacionais de sistemas sobre pontos fracos no contexto global do sistema ou fluxo operacional; viabiliza a manutenção do programa de auditoria a baixo custo de horas, sem permitir cortes que redundariam em perda da visão global do fluxo operacional e de controle.

Pela sua importância para o auditor, os fluxos e os formulários e demais papéis oficiais da empresa utilizados nas operações nele descritas passam a se constituir em documento básico da auditoria interna. Como tal são tratados formalmente pelo seu sistema de arquivo.

6.5.3.4- Roteiro Sequencial

Este módulo se refere à fase de execução prática dos exames de auditoria. Esses exames são orientados através do Roteiro Sequencial.

Roteiro seqüencial é a instrução detalhada do programa de auditoria, onde cada passo a ser executado é estruturado de forma seqüencial e consistente com os procedimentos operacionais e de controle praticados na área examinada. Portanto, o roteiro harmônico de auditoria acompanha a mesma seqüência das operações. Para isso, esse roteiro é preparado pela área de auditoria, com base nos fluxogramas levantados pelo auditor ou pela entidade, sendo revisados pelo auditor.

Não significa, porém, que cada ato administrativo ou operacional fluxogramado deve resultar num controle específico do auditor, mas, apenas aqueles cujo controle é imprescindível para o julgamento do auditor com a finalidade de cobrir sua responsabilidade, em face dos riscos e pontos de crítica identificados, ou a necessidade de complementar o programa de forma compreensiva.

Os passos do programa a ser executado pelo auditor devem ser estruturados de tal forma que todas as técnicas adequadas a cada situação sejam devidamente observadas, cobrindo, forma ampla, suas responsabilidades profissionais. Isto significa que essas técnicas estarão incorporadas às instruções programadas para o auditor.

6.5.3.5 - Questionários Auxiliares

Os questionários auxiliares servem para complementar as instruções seqüenciais e detalhadas do programa, particularmente para certos tipos de verificações de natureza excepcional, tais como:

- a)* estruturas de segurança e proteção de sistemas, pessoas, documentos e bens;
- b)* *check-list* de completabilidade de lotes documentais;
- c)* levantamentos físicos de caixa, mercadorias, ativos, duplicatas e títulos de crédito;
- e
- d)* *check-list* para exame dos campos e condições de apólices de seguro e documentos similares;
- e)* estruturas de centro de processamento de dados.

Os questionários auxiliares podem ser na forma narrativa ou alternativa.

No primeiro caso, trata-se de questionários formados a partir de questões que requerem uma resposta extensiva e narrativa, completando a idéia básica do procedimento que o auditor busca conhecer. Esse tipo de questionário, embora permita ter uma visão adequada dos sistemas e procedimentos, requer:

- a)* cuidado para sua preparação, devido aos riscos de omissões;
- b)* experiência em entrevistas e assimilação das respostas para seu encadeamento seqüencial de forma a permitir visualizar o sistema sob análise; e
- c)* tempo para sua preparação, aplicação e análise. Alternativamente, o tempo pode ser reduzido quando o questionário é respondido diretamente pelo auditado, já que não envolve opiniões, apenas fatos.

O questionário na forma alternativa trata os assuntos em termos simplesmente de **sim**, **não** ou **não aplicável**. Em princípio, as perguntas são estruturadas de maneira tal que a resposta deva ser sempre positiva. A ocorrência de uma resposta negativa implicaria, desde logo, a constatação de uma deficiência ou inexistência de um controle necessário e, portanto, a incompletabilidade do sistema de controle interno. No caso de ser estruturado de maneira a obter sempre uma resposta negativa, a ocorrência de uma resposta positiva indicará o ponto falho.

A principal desvantagem desse tipo de questionário é que ele não permite visualizar o sistema como um todo através das respostas obtidas. Da mesma forma que o questionário narrativo, pode também ser preenchido pelo auditado.

Em ambos os casos, alternativos ou narrativos, o AUDIBRA (1991, p.315) recomenda limitar seu uso a situações específicas, como parte de um todo, em caráter auxiliar do programa seqüencial de auditoria.

6.5.3.6- Diagnósticos e Comprovações Numéricas

Pela avaliação da organização e de seus controles internos o auditor teve a oportunidade de obter uma visão antecipada da qualidade das estruturas e fluxos operacionais e de controle. Essa visão assume papel fundamental na continuidade do seu trabalho.

Se, de um lado, essa visão permite ao auditor elaborar de forma imediata relatórios de recomendações ou estabelecer discussões com as áreas auditadas, no que se refere à organização e aos controles, de outro lado, faz crescer as exigências técnico-profissionais sobre ele, no tocante à profundidade e abrangência dos testes de comprovação que deverá realizar. Esses testes serão tão mais críticos quanto forem as deficiências notadas através de sua análise dos fluxos e trâmites administrativos e operacionais.

Neste módulo de diagnósticos e comprovações numéricas, o auditor constrói no seu programa de auditoria uma série de instrumentos que possam propiciar um diagnóstico, agora, voltado às cifras, e não mais à organização e a seus controles.

Isto significa que, antes mesmo de iniciar os testes individualizados, o auditor procurará formar uma opinião global sobre a exatidão, completabilidade e razoabilidade das cifras, de maneira a identificar:

- a)* magnitude e risco;
- b)* séries numéricas de comportamento destoantes dos padrões e comparações estabelecidas;
- c)* exceções que requerem maior atenção; e
- d)* falta de consistências entre registros e informações disponíveis.

Nesse sentido, o auditor volta sua atenção às cifras, de maneira global, trabalhando com totais por atividade, por conta, por grupo e formatando essas cifras de maneira a possibilitar um diagnóstico sensível às flutuações, anormalidades e desvios de parâmetros internos ou externos.

A operacionalização dessa fase se dá através da montagem e utilização das chamadas “tabelas de cifras”. Essas tabelas são pré-formatadas pelo auditor de acordo com as necessidades e exigências dos exames a serem efetuados, podendo ser de preenchimento manual ou extraído diretamente dos sistemas informatizados. Constituem-se em evidência de auditoria e como tal devem ser formalmente tratadas pelo sistema de arquivo de documentos da área de auditoria interna.

Sua abrangência pode incluir: período anual, mensal ou, mesmo, o movimento de um dia apenas, conforme as circunstâncias indicarem ao auditor. As principais tabelas são classificadas sob os seguintes títulos:

- a)** tabelas de consistências onde as cifras referentes a uma certa atividade, sub-razão ou aplicações, são organizadas de maneira a indicar o grau de exatidão na sequência:

$$\text{Inicial} + \text{Entradas} - \text{Saídas} = \text{Final}$$

- b)** tabelas de inter-relações onde as cifras referentes às atividades ou operações, são organizadas para indicar a exatidão entre áreas distintas ou sub-razões diversos na sequência:

Entradas no Setor A

Saídas no Setor B

- c)** tabelas de apreciação de cifras onde as cifras de uma atividade, operação ou movimentos, referentes a determinados períodos, são arranjadas de maneira a poderem ser analisadas quanto à correlação com o orçamento, razoabilidade em relação à atividade, normalidade dos padrões de comportamento e exceções aparente. Aqui, buscam-se desvios em relação aos padrões ou a comportamentos normativos.

BIBLIOTECA DA
FUNDAÇÃO JOÃO PINHEIRO

BIBLIOTECA DA
FUNDAÇÃO JOÃO PINHEIRO I

6.5.4-Formatação Técnica

A formulação dos roteiros sequenciais, bem como dos questionários expeditos que fazem parte integrante do programa de auditoria, deve obedecer a padrões tais que possibilitem o cumprimento de certas exigências profissionais no tocante à documentação de trabalho, tais como:

- a)** em relação às instruções detalhadas do programa:
 - campo para referência entre cada instrução detalhada e os papéis de trabalho do auditor;
 - campo para registro da rubrica do auditor executante dos exames;
 - campo para registro da data de execução real do programa.
- b)** em relação aos volumes, datas e simultaneidade dos testes:
 - campo geral para indicação do tamanho dos testes;
 - campo geral para indicação da periodicidade ou data do teste.
- c)** em relação à supervisão
 - campo geral para registro de rubrica e data da supervisão dos trabalhos.

6.5.4.1- Exemplos de Formatação e de Peças Integrantes do Programa de Auditoria

O roteiro sequencial é elaborado com base na avaliação dos procedimentos e no fluxograma da área objeto do exame do auditor e tem a finalidade de instruir e orientar, passo a passo, seu trabalho.

O roteiro sequencial detalhado de exames, mostra um ordenamento que deixa aparente a observância da cronologia dos fatos decorrentes dos sistemas, operações e controles praticados pelo auditado. A FIG. 07. apresenta um modelo de roteiro de um trecho do ciclo operacional de compras em uma empresa industrial.

7 AUDITORIA DE SISTEMAS OU AUDITORIA DAS TECNOLOGIAS DA INFORMAÇÃO

7.1- Introdução

Com o uso cada vez mais freqüente das tecnologias da informação nas organizações, tornou-se necessário ampliar os controles sobre a proteção dos dados e informações processados pelos Sistema de Informações Computadorizados. Dessa exigência, emerge a Auditoria de Sistemas, também denominada Auditoria das Tecnologias da Informação.

A Auditoria de Sistemas consolida três áreas distintas do conhecimento: auditoria, sistemas de informações e informática.

Este capítulo aborda a Auditoria de Sistemas. Inicialmente, são destacados seu conceito e seus objetivos. Posteriormente, serão enfocadas as normas que regulamentam essa modalidade de auditoria e as técnicas utilizadas na execução de um trabalho.

Por fim, serão dispostos as áreas de atuação da Auditoria de Sistemas e o perfil do Auditor de Sistemas.

7.2- Conceito e Objetivos

Com a evolução da informática, as organizações públicas e privadas começaram a utilizar cada vez mais este instrumento, confiando suas informações em sistemas baseados nesta tecnologia. Destarte, diversas atividades das organizações estão

PROGRAMA DE AUDITORIA				
ENTIDADE: Indústria XX		ÁREA: Compras	CÓDIGO REFERÊNCIA:	
AMOSTRAGEM: 10 requisições		HORAS ORÇADAS: 8	MESES BASE: Janeiro	
OBJETIVO:				
INSTRUÇÕES		RUBRICA DO AUDITOR	DATA DA VERIFICAÇÃO	PAPEL DE TRABALHO N.
N.	DETALHAMENTO PROGRAMADO DE CONTROLE			
1.0	Tomar conhecimento dos tipos de material e quantidades constantes da programação de produção para o período.			
2.0	Apurar a posição dos estoques desses materiais disponíveis para o departamento de produção, na data de início da produção.			
3.0	Verificar a razoabilidade e exatidão da requisição de compras de material.			
AUDITOR RESPONSÁVEL:		SUPERVISOR:	DATA: __/__/__	

FIGURA 07- Modelo de Roteiro Sequencial da Área de Compras de uma Empresa Industrial

FONTE- AUDIBRA, 1991, p. 326 (adaptada).

Para alguns tipos de exames, o auditor tem a opção de utilizar questionários auxiliares de uso específico e que podem, conforme o caso, ser preenchidos até mesmo pelo próprio auditado.

Esses questionários não têm uma ligação direta com o fluxo sequencial da operação, pois referem-se a uma situação de caráter estático; portanto, podem ser preenchidos em qualquer fase dos exames.

Na redação dos questionários auxiliares, devem ser observados todos os requisitos de objetividade, clareza, utilidade, amplitude, etc. para poder cobrir de forma adequada a responsabilidade do auditor. O mesmo se aplica à atualização periódica dos questionários.

A FIG. 08. representa um modelo de questionário auxiliar de um trecho do ciclo operacional de compras numa empresa industrial.

PROGRAMA DE AUDITORIA				
ENTIDADE: Indústria XX		ÁREA: Compras		CÓDIGO REFERÊNCIA:
AMOSTRAGEM: 10 requisições		HORAS ORÇADAS: 8		MESES BASE: Janeiro
OBJETIVO:				
N.	INSTRUÇÕES QUESTIONÁRIO AUXILIAR Gerencial	ASSINALAR SIM NÃO	RUBRICA / DATA DA VERIFICAÇÃO	PAPEL DE TRABALHO N.
1.0	Há um organograma da área, aprovado e			
2.0	atualizado?			
	Os ativos do setor estão adequadamente protegidos			
3.0	contra uso não autorizado?			
	Há instruções regulando o uso dos ativos do setor?			
AUDITOR RESPONSÁVEL:		SUPERVISOR:		DATA: __/__/__

FIGURA 08- Modelo de Questionário Auxiliar da Área de Compras de uma Empresa Industrial

FONTE- AUDIBRA, 1991, p. 330 (adaptada).

6.6- Conclusão

Este capítulo demonstrou que a Auditoria Interna é um elemento importante para as organizações, pois o auditor, revisando e avaliando os controles internos, os procedimentos e as metas da instituição, oferecerá subsídios para o aprimoramento das atividades, para a melhoria dos resultados operacionais e para a tomada de decisão pelos administradores.

Os trabalhos de uma Auditoria Interna podem ser executados nas seguintes modalidades: Auditoria Contábil e Tributária, Auditoria Operacional, Auditoria de Gestão, Auditoria Especial e Auditoria de Sistemas Informatizados. Para cada uma dessas modalidades, a Auditoria Interna deve construir um **Programa de Auditoria** detalhado, pois, este indica os procedimentos e as técnicas a serem aplicadas em cada fase de uma auditoria e orienta, de maneira eficiente, o trabalho do Auditor, independentemente do grau de afinidade que tenha com a área auditada.

O próximo capítulo trata especificamente da Auditoria de Sistemas, também denominada, Auditoria das Tecnologias da Informação.

vinculadas, direta ou indiretamente, aos Sistemas de Informações Computadorizados. Conseqüentemente, torna-se necessário que as medidas de controle e segurança desses sistemas sejam sistematicamente revisadas e avaliadas.

Em função dessa informatização das atividades das organizações, a auditoria teve que ampliar suas modalidades, expandindo suas verificações sobre os Sistemas de Informações Computadorizados. Desse processo, surgiu a Auditoria de Sistemas, também denominada Auditoria das Tecnologias da Informação.

Conforme DIAS (2000, p.136) o termo **Tecnologia da Informação** surgiu inicialmente como uma classificação do Departamento de Comércio dos Estados Unidos da América para as empresas de serviços e produtos de informática e de comunicação. A princípio, a terminologia utilizada era “Tecnologia da Informação e Comunicação”, mas a denominação que mais se disseminou foi a sua forma sintetizada, ou seja, Tecnologia da Informação.

No Brasil, a expressão “Tecnologia da Informação” compreende aspectos inerentes à informática, aos sistemas computadorizados e às telecomunicações. A terminologia “Auditoria da Tecnologia da Informação”, vem da tradução do inglês *Information Technology Audit*. Hoje, “Auditoria de Sistemas” e “Auditoria da Tecnologia da Informação” são expressões sinônimas.

Vários autores apresentam suas definições de Auditoria de Sistemas, conforme disposto no QUADRO 16. Contudo, sempre se mantém a avaliação dos sistemas computadorizados e do ambiente em que estão inseridos como ponto central e comum a todas elas.

QUADRO 16: CONCEITOS DE AUDITORIA DE SISTEMAS

AUTOR	CONCEITO
CRCSP (1999, p. 92-93)	“Uma atividade voltada à avaliação dos procedimentos de controle e segurança vinculados ao processamento eletrônico das informações. Tem como funções: documentar, avaliar e monitorar sistemas de controles legais, gerenciais de aplicação e operacionais.”
ARIMA (1994, p. 34)	“A Auditoria de Sistemas promove a adequação, avaliação e aprimoramento dos controles internos nos sistemas de Informações da empresa, bem como a utilização dos recursos humanos, materiais e tecnológicos envolvidos no processamento dos mesmos.” .
DIAS (2000, p. 136)	“A Auditoria das Tecnologias da Informação analisa um conjunto de controles gerenciais e procedimentos que afetam todo o ambiente de informática e, conseqüentemente, todos os sistemas aplicativos. Neste tipo de auditoria são verificados os padrões e políticas adotados pela organização, a operação sobre sistemas e dados, a disponibilidade e a manutenção do ambiente computacional, a utilização de recursos computacionais, a gerência de banco de dados e de redes, além de todos aspectos relacionados à segurança de informações, como segurança física, lógica e ambiental, e continuidade dos serviços de informática.”
GIL (1999, p. 35)	“A Auditoria de Sistemas compreende terminologia, conceituação e técnicas de três áreas distintas do conhecimento: auditoria, sistemas de Informações e processamento eletrônico de dados.”
TCU (1998, p. 34)	“ Tipo de auditoria através da qual os auditores recorrem ao estudo dos sistemas e, em especial, ao estudo do controle interno da entidade fiscalizada e à identificação dos eventuais pontos fortes e/ou deficiências desse controle interno, com o fim de definir o local, a natureza e o âmbito dos trabalhos de auditoria que julguem necessários para formularem o seu parecer.”
INEI (2002, p. 3)	“A Auditoria de Sistemas é o conjunto de técnicas que permitem detectar deficiências de informática nos sistemas das organizações, permitindo efetuar ações preventivas e corretivas para eliminar as falhas e carências que se detectem.” (*)

FONTE- Elaborado pela autora da dissertação.

(*) Tradução da autora.

Portanto, a Auditoria de Sistemas avalia os Sistemas de Informações Computadorizados e o ambiente computacional, a fim de identificar e analisar os possíveis riscos que estejam ocorrendo, ou que possam ocorrer, para posterior recomendação de medidas saneadoras e melhoria dos controles internos para a diminuição dos riscos levantados. Como destacado no capítulo 4 desta dissertação, diversos são os riscos a que os Sistema de Informações Computadorizados estão sujeitos, como catástrofes, supressão e interrupção de serviços, violação de integridade, vazamento de informações, acesso e uso não autorizado de recursos, roubo, remoção ou perda de equipamentos e informações.

Conforme BOVE (1995, p.162), a Auditoria de Sistemas tem como objetivos a avaliação dos seguintes aspectos:

a) eficácia, economia e eficiência

- o sistema desempenha todas as tarefas para o qual foi desenvolvido;
- o sistema atende às necessidades dos usuários e da empresa, fornecendo as informações necessárias em tempo hábil e no formato adequado;
- coerência e compatibilidade dos sistemas com as metas e estratégias da instituição;
- otimização dos recursos do sistema.

b) integridade dos dados

- informações precisas, adequadas e exatas;
- eficiência dos controles internos, necessários à segurança e correção dos dados;

c) segurança do sistema

- eficiência e adequação dos controles internos;
- proteção dos recursos contra roubo, desperdício, fraude ou catástrofes naturais;
- segurança lógica do sistema.

d) observação da legislação

- cumprimento da legislação regulamentadora das atividades relacionadas aos sistemas;
- desenvolvimento das atividades do sistema em conformidade com os regulamentos políticas, diretrizes e orientações no setor público.

Em função dos objetivos citados, a Auditoria de Sistemas deve revisar e avaliar o controle interno inerente à área dos Sistemas de Informações Computadorizados da organização, devendo, para tanto, obedecer normas e adotar técnicas de trabalho.

7.3- Normas Aplicáveis

A Auditoria de Sistemas, como destacado no capítulo 6, constitui uma das modalidades da Auditoria Interna, devendo, portanto, pautar-se nas normas que regulamentam essa atividade e zelar pela observância da legislação alusiva aos Sistemas de Informações, exposta no capítulo 4 desta dissertação.

Não obstante estes preceitos, a Auditoria de Sistemas deve obedecer aos padrões definidos pela *Information Systems Audit and Control Association* (ISACA), órgão internacional certificador de Auditoria de Sistemas (*Certified Information Systems Auditor – CISA*), que conta com mais de 23.000 associados e está presente em mais de cem países¹⁸.

Os padrões para Auditoria de Sistemas de Informações determinados pela ISACA disciplinam sobre a competência técnico-profissional, a ética, autoridade e independência profissional, a responsabilidade do auditor no planejamento, execução e apresentação dos seus trabalhos, como adiante transcritos:

“010 Carta de Auditoria

010.010 Responsabilidade, Autoridade e Prestação de Contas

A responsabilidade, autoridade e prestação de contas sobre a função de auditor de sistemas de Informações devem ser apropriadamente documentadas em uma carta de auditoria ou de aderência.

020 Independência

020.010 Independência Profissional.

Em todas as questões relativas a auditoria, o auditor de sistemas de Informações deve ser independente do auditado em atitude e aparência.

020.020 Relacionamento Organizacional

¹⁸ Extraído de <http://www.isaca.org>

A função de auditor de sistemas de Informações deve ser suficientemente independente da área sob auditoria para permitir uma conclusão objetiva da auditoria.

030 Ética Profissional e Padrões

030.010 Código de Ética Profissional

O auditor de sistemas de Informações deve aderir ao Código de Ética Profissional da ISACA.

030.020 Devido Zelo Profissional

O devido zelo profissional e a observância dos padrões profissionais de auditoria aplicáveis devem ser exercidos em todos os aspectos do trabalho do auditor de sistemas de Informações.

040 Competência

040.010 Habilidades e Conhecimento

O auditor de sistemas de Informações deve ser competente tecnicamente, possuindo as habilidades e conhecimento necessários para a execução do trabalho do auditor.

040.020 Educação Profissional Contínua

O auditor de sistemas de Informações deve manter a competência técnica por meio de contínua e apropriada educação profissional.

050 Planejamento

050.010 Planejamento de Auditoria

O auditor de sistemas de Informações deve planejar o trabalho de auditoria de sistemas de Informações para direcionar os objetivos da auditoria e seguir os padrões profissionais de auditoria aplicáveis.

060 Desempenho do Trabalho de Auditoria

060.010 Supervisão

O staff de auditoria de sistemas de Informações deve ser supervisionado apropriadamente para assegurar que os objetivos de auditoria sejam alcançados e os padrões profissionais de auditoria aplicáveis sejam respeitados.

060.020 Evidência

Durante o curso da auditoria, o auditor de sistemas de Informações deve obter evidência suficiente, confiável, relevante e proveitosa para alcançar efetivamente os objetivos da auditoria. Os pontos e conclusões da auditoria devem ser fundamentadas por análise e interpretação apropriadas desta evidência.

070 Emissão de Relatório

070.010 Forma e Conteúdo do Relatório

O auditor de sistemas de Informações deve prover um relatório, em uma forma apropriada, aos devidos destinatários por ocasião da conclusão do trabalho de auditoria. O relatório de auditoria deve declarar o escopo, objetivos, período de abrangência e a natureza e extensão do trabalho de auditoria executado. O relatório deve identificar a organização, os destinatários desejáveis e quaisquer restrições à sua circulação. O relatório deve conter os pontos, conclusões, 10 recomendações e quaisquer ressalvas ou conceitos que o auditor possua a respeito da auditoria.

080 Atividades de Follow-Up

080.010 Follow-Up

*O auditor de sistemas de Informações deve requisitar e avaliar informações apropriadas sobre pontos, conclusões e recomendações anteriores e relevantes para determinar se ações apropriadas foram implementadas no momento certo.*¹⁹

No Brasil, existem quatro instituições que deliberam sobre a Auditoria de Sistemas: a Sociedade dos Auditores de Sistemas (SAS), que é o órgão certificador de Auditoria de Sistemas; a Associação Brasileira de Auditoria de Sistemas (ABAS); a Sociedade de Usuários de Informática e Telecomunicações (SUCEsu), estas duas últimas, responsáveis pela realização dos Congressos de Auditoria de Sistemas e Segurança da Informação (CNASI); e a Câmara de Informática, órgão componente do AUDIBRA, que está editando um obra acerca dos Procedimentos de Auditoria da Informática.

7.4- Técnicas de Auditoria de Sistemas

Ocorreram muitas mudanças na atividade de auditoria. Conseqüentemente, essas mudanças requerem a aplicação de técnicas mais avançadas de trabalho.

Dentre tais técnicas, o Auditor de Sistemas deve selecionar aquelas mais apropriadas e, provavelmente, mais convincentes quando de uma circunstância necessária para rever ou avaliar um sistema computadorizado.

Um estudo publicado pelo *The Institute of Internal Auditors*²⁰ em 1977 mostrou diversas técnicas que são praticadas nas avaliações dos sistemas computadorizados de várias organizações.

As principais técnicas são abordadas a seguir, segundo o aprendizado a partir da doutrina de CASH (1977, p. 815-825), GIL (1999, p.67-95) e IMONIANA (1994, p.97-114).

¹⁹ Extraído de <http://www.isaca.org>

7.4.1- *Software* de Auditoria

O *Software* de Auditoria foi desenvolvido para otimizar o processo de auditoria em que se faz necessária a análise de dados. É usado em arquivos e banco de dados, tanto em computadores de grande porte quanto em microcomputadores. Pode ser construído pelo próprio auditor de sistemas, através do conhecimento de uma linguagem de programação.

Basicamente, estes *softwares* executam os procedimentos de extração de dados, indexação e ordenamento de arquivos, estatísticas dos campos dos arquivos, comparação de arquivos, amostragens e cálculos. Com a utilização desta técnica, o Auditor de Sistemas pode capturar dados de um determinado sistema e transferi-los para outro computador, onde então serão executados seus testes. Dessa forma, o tempo para executar os testes é reduzido e o volume de dados examinados é bem maior em relação àquele que seria analisado manualmente.

A utilização de *Software* de Auditoria comercializados no mercado também oferece opções para aplicação desta técnica. Exemplos de *Softwares* de Auditoria utilizados no Brasil são o *Audit Command Language* (ACL®) e o *Interactive Data Extraction and Analysis* (IDEA®).

7.4.2- Questionários

O Questionário corresponde à elaboração de um conjunto de perguntas com o objetivo de verificar determinado ponto de controle do ambiente computacional. Essas questões buscam apurar a adequação do ponto de controle aos parâmetros do controle interno (segurança lógica, segurança física e obediência à legislação).

A técnica do Questionário é, normalmente, aplicada conjuntamente com outras técnicas de auditoria, como a Entrevistas e a *Visita in Loco*. Entretanto, o questionário

²⁰ Extraído de <http://www.theiia.org>

pode ser aplicado a distância; ou seja, pode ser enviado ao auditado. Esta abordagem permite ao auditor pesquisar um amplo universo de auditados.

Particularmente, em ambiente de microinformática, devido à quantidade e a intensidade de dispersão dos equipamentos e à quantidade de usuários por equipamento, a aplicação de questionários a distância permite uma auditoria constante com menor número de auditores.

7.4.3- Simulação de Dados (*Test-Deck*)

O *Test-Deck* é uma técnica aplicada para teste de processos computacionais. Corresponde à elaboração de um conjunto de dados de teste a ser submetido ao sistema computacional ou a determinada rotina que o compõe, que necessita ser verificada em sua lógica de processamento.

Uma vez comprovada a inadequação da lógica do processo auditado, conclui-se pela incorreção de todos os resultados que forem gerados por aquela rotina irregular.

Os dados simulados de teste necessitam prever situações corretas e situações incorretas de natureza como: transações com campos inválidos, transações com valores ou quantidades nos limites de tabelas de cálculos, transações incompletas, transações incompatíveis e transações em duplicidade.

Essa técnica é bastante completa e fundamental, já que através dela pode-se certificar da qualidade do sistema.

7.4.4- Visita *In Loco*

A *Visita In Loco* corresponde à atuação pessoal do auditor junto a sistemas, procedimentos e instalações do ambiente computadorizado.

Normalmente, combinada com outras técnicas de Auditoria de Sistemas, particularmente o Questionário, a Visita *In Loco* implica o cumprimento da seguinte sequência de procedimentos:

- a)** marcação da data e horário com a pessoa responsável que irá acompanhar as verificações,
- b)** anotação de procedimentos e acontecimentos, coleta de documentos e caracterização gráfica da situação via elaboração de fluxo de rotinas e de *layout* de instalações; e
- c)** análise dos papéis de trabalho obtidos e avaliação das respostas e da situação identificada.

A presença do auditor é fundamental tanto para a constatação física da existência de equipamentos computacionais da organização, quanto para seu estado de conservação e qualidade dos procedimentos de utilização.

7.4.5- Mapeamento (*Mapping*)

O *Mapping* é uma técnica computacional utilizada pelo Auditor de Sistemas para efetuar verificações durante o processamento dos programas através de caminhos lógicos, flagrando situações como rotinas não utilizadas e a quantidade de vezes que cada rotina foi utilizada quando submetida ao processamento de uma quantidade de dados.

A análise dos relatórios emitidos pela aplicação do *Mapping* permite a constatação de situações:

- a)** rotinas existentes em programas já desativadas ou de uso esporádico;
- b)** rotinas mais utilizadas, normalmente a cada processamento do programa;
- c)** rotinas fraudulentas e de uso em situações irregulares; e
- d)** rotinas de controle acionadas a cada processamento.

Para a utilização do *Mapping*, há necessidade processar um *software* de apoio em conjugação com o processamento do sistema aplicativo ou embutir rotinas específicas no sistema operacional utilizado.

7.4.6- Rastreamento

O Rastreamento é uma técnica que implica o trabalho manual de um fluxo que possibilita seguir o caminho de uma transação durante o processamento do programa, desde o ponto da entrada do dado até a saída do resultado.

Quando o teste de alimentação de determinada transação a um programa é realizado, podem-se identificar as inadequações e ineficiência na lógica de um programa.

7.4.7- Entrevistas

A Entrevista é uma técnica de trabalho que corresponde à realização de reunião entre o auditor e os auditados, profissionais usuários e profissionais de computação envolvidos com o ambiente ou o sistema de Informações computadorizado sob auditoria.

A sequência dos procedimentos da Entrevista corresponde a:

- a)* análise do ponto de controle e planejamento da reunião com os profissionais envolvidos;
- b)* marcação do dia e horário da entrevista;
- c)* elaboração de um questionário para realização da entrevista;
- d)* realização da reunião, com aplicação do questionário e anotação das respostas e comentários dos entrevistados a cada questão efetuada;
- e)* elaboração de uma ata de reunião com o registro dos principais pontos discutidos a cada questão apresentada; e
- f)* análise das respostas e formação de opinião acerca do nível de controle interno do ponto de controle.

A Entrevista deve ser combinada com outras técnicas de auditoria de sistema, particularmente com o Questionário e a Visita *In Loco*.

7.4.8- Análise de Relatórios e Telas

A Análise de Relatórios e Telas implica o exame de documentos, relatórios e telas do sistema sob auditoria no tocante a:

- a)* nível de utilização pelo usuário;
- b)* esquema de distribuição e número de vias emitido;
- c)* grau de confidencialidade de seu conteúdo; e
- d)* forma de utilização e integração entre relatórios/telas/documentos.

As conclusões do trabalho, freqüentemente, possibilitam redução de custos com a desativação total ou parcial de relatórios/telas/documentos.

7.4.9- Simulação Paralela

A Simulação Paralela compreende a elaboração e utilização de um programa de computador para simular as funções de rotina do sistema sob auditoria. Esta técnica utiliza-se dos dados rotineiros do sistema sob auditoria como entrada do programa de computador para a simulação.

Enquanto no *Test-Deck* são simulados os dados de entrada e submetidos ao programa de computador sob auditoria, na Simulação Paralela acontece o inverso, pois o programa é simulado e submetido aos mesmos dados de entrada que foram utilizados no programa da organização auditada.

7.4.10- Análise do Log

O *Log* é um arquivo, gerado por uma rotina componente do sistema operacional, que contém registros de utilização do *hardware* e do *software* que compõem um ambiente computacional.

A tabulação deste arquivo *Log* permite verificar a intensidade de uso dos dispositivos componentes de uma configuração ou rede de computadores, bem como o uso do *software* aplicativo e de apoio vigente.

Tanto a rotina quanto o correspondente arquivo de *Log* foram desenvolvidos para serem usados pelo pessoal de computação. Entretanto, representam, também, excelente ferramenta para a Auditoria de Sistemas para:

- a) identificar usuário, data , horário e transação realizada;
- b) flagrar uso de programas fraudulentos ou utilização indevida do computador; e
- c) captar tentativas indevidas de acesso a arquivos, ou seja, por senhas não autorizadas.

Evidentemente, deve haver na área de computação profissionais responsáveis pela análise do uso do computador. O trabalho desses profissionais precisa ser auditado, através da análise dos registros históricos e dos relatórios por eles produzidos.

Quando o arquivo *Log* é gravado em ambiente de microinformática, há necessidade da existência de normas estabelecendo de quem é a responsabilidade pela análise rotineira do uso do computador e por quanto tempo os registros do *Log* devem ser armazenados para a viabilização da atuação da auditoria em computador.

7.4.11- Analise do Programa-Fonte

Implica a análise visual do código-fonte (linguagem em que o usuário ou programador escreve o programa) do programa de computador componente do sistema sob auditoria.

O auditor de sistemas necessita assegurar-se de que está testando a versão correta do programa que foi processado ou que irá processar.

É importante ressaltar que esta técnica exige profundos conhecimentos de processamento eletrônico de dados por parte do auditor de sistemas. Entretanto, a análise visual do código-fonte do programa auditado permite ao auditor:

- a) verificar se o programador cumpriu as normas de padronização de código de rotinas, arquivos, programas;
- b) analisar a qualidade da estruturação dos programas; e
- c) detectar vícios de programação e o nível de atendimento às características da linguagem de programação utilizada.

Independente das técnicas usadas para a realização de um trabalho de auditoria e da forma como são utilizadas, seja manual ou informatizada, o mais importante é que o Auditor de Sistemas siga as orientações de um Programa de Auditoria, pois, este instrumento contém as informações sobre o objetivo e o escopo da auditoria a ser executada, indicando os procedimentos a serem aplicados e dirigindo de maneira eficiente o trabalho do auditor.

7.5- Áreas de Atuação da Auditoria de Sistemas

Na realização de uma Auditoria de Sistemas são avaliados todos os controles e procedimentos que afetam os Sistemas de Informações Computadorizados e o ambiente computacional.

Assim, nesta modalidade de auditoria são analisados os *softwares*, o departamento de tecnologia da informação, a segurança dos sistemas, o plano de contingências, os controles de acesso aos recursos computacionais, os banco de dados, as redes de comunicação, os microcomputadores e seus periféricos.

A partir do estudo de alguns autores [DIAS (2000, p. 136-180), ARIMA (1994, p. 21-25), MOELLER (1989, p. 69-73), TCU (1998, p. 41-94), BURCH (1974, p. 68-83), CHAMBERS (1981, p. 79-96) e PORTER (1981, p. 115-124)] pode-se constatar que existe um consenso sobre as áreas de atuação da Auditoria de Sistema. Embora a terminologia usada entre os autores não seja exatamente a mesma, a explanação feita por cada um deles é bastante similar. Por tal motivo, optou-se pela denominação utilizada pelo TCU, vez que a entidade objeto do estudo de caso desta dissertação, a AUDIM, trata-se de uma organização pública.

Assim, as áreas examinadas na Auditoria de Sistema estão demonstradas na FIG. 09.

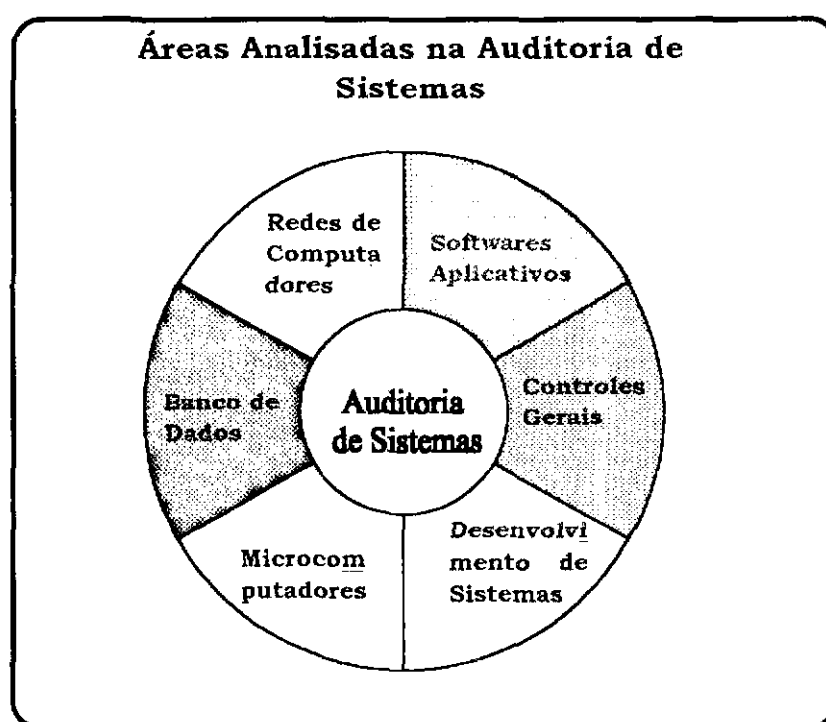


FIGURA 09- Áreas Analisadas na Auditoria de Sistemas

FONTE- TCU, 1998, p. 41-94 (adaptada).

Nas seções 7.5.1 a 7.5.6 serão abordadas cada uma das áreas examinadas na Auditoria de Sistemas, apresentando-se uma consolidação a partir do estudo da teoria dos autores antes mencionados.

7.5.1- Controles Gerais

Os Controles Gerais compreendem a estrutura organizacional, as políticas e os procedimentos que se aplicam às operações dos Sistema de Informações Computadorizados de uma organização, visando garantir que estes sistemas e o ambiente em que estejam inseridos sejam eficientes, eficazes, seguros e confiáveis.

Controles Gerais deficientes acarretam uma diminuição da confiabilidade a ser atribuída aos Sistema de Informações Computadorizados. Por tal motivo, durante a auditoria de um Sistema de Informações Computadorizados é preciso, inicialmente, avaliar os Controles Gerais que atuam sobre este sistema.

Existem três categorias de Controles Gerais em Auditorias de Sistemas: controles organizacionais, políticas de segurança e controles de acesso. Cada um desses controles será melhor detalhado adiante.

7.5.1.1- Controles Organizacionais

Os Controles Organizacionais referem-se às políticas, aos procedimentos e à estrutura organizacional estabelecidos para instituir as responsabilidades de todos os funcionários envolvidos nas atividades relacionadas à área da informática. Estes controles referem-se a:

- a) responsabilidade organizacional do departamento de informática: o departamento de informática é responsável por todos os serviços relacionados à área de informática. Este departamento precisa ter uma estrutura organizacional bem definida, com as responsabilidades de suas unidades organizacionais claramente estabelecidas, documentadas e divulgadas, e também políticas de pessoal adequadas, quanto à seleção, segregação de funções, treinamento e avaliação de desempenho. Essa estrutura deve gerenciar racionalmente os recursos computacionais da organização, de modo a suprir as necessidades de informações de forma eficiente e econômica; e

- b) segregação de funções:* a segregação de funções tem como objetivo evitar que um indivíduo venha a controlar todas as fases de um processo, por exemplo, um programador com permissão para independentemente escrever, testar e aprovar alterações de programa.

Geralmente, a segregação de funções é alcançada pela divisão de responsabilidades entre dois ou mais grupos da organização. Com essa divisão, a probabilidade de que erros e ações indevidas sejam detectados aumenta, vez que as atividades de um grupo ou indivíduo irão servir para conferir as atividades do outro.

A falta ou discordância da segregação de funções de informática aumenta o risco de ocorrência de transações errôneas ou fraudulentas, alterações impróprias de programa e danos em recursos computacionais.

A extensão da segregação de funções a ser aplicada em uma organização irá depender do seu tamanho e do risco associado às suas instalações e atividades. Uma organização de grande porte terá mais flexibilidade em separar funções que organizações pequenas, que dependem de poucos indivíduos para executar suas atividades. Da mesma forma, atividades que envolvem transações financeiras de alto valor ou que, de alguma outra forma, são bastante arriscadas devem ser divididas entre diversos indivíduos e sujeitas a uma supervisão mais rígida.

7.5.1.2- Política de Segurança

A Política de Segurança da organização, como já discorrido no capítulo 4, inclui todas as medidas de proteção dos recursos computacionais e das informações por eles processadas, bem como o plano de contingências, que deve explicitar as alternativas de recuperação de dados para a continuidade dos serviços na área de informática da organização.

Sem a adoção de uma política de segurança bem organizada, os controles de segurança podem ser inadequados, as responsabilidades dos funcionários podem não

estar claras, não serem compreendidas e propriamente implementadas e, ainda, os controles podem ser aplicados de forma inconsistente.

Além disso, pode ocorrer a perda da capacidade de processar, recuperar e proteger informações, o que leva a um impacto significativo na habilidade da organização em desempenhar sua missão. Devido a isso, as organizações precisam ter procedimentos estabelecidos para proteger seus recursos de informação, minimizar o risco de interrupções não planejadas e recuperar operações em caso de interrupções. Para garantir que os planos de contingências irão funcionar, eles devem ser examinados e simulados ocasionalmente.

Se os controles não são apropriados, mesmo interrupções menos graves podem resultar em perda ou processamento incorreto de dados, ocasionando prejuízos financeiros, esforços dispendiosos de recuperação e informações gerenciais ou financeiras inexatas ou incompletas. Para algumas operações, tais como as que envolvem cuidados médicos ou segurança pública, interrupções de sistema podem até mesmo resultar em danos pessoais ou perda de vidas.

Para atenuar as interrupções de serviço, é essencial que os controles estabelecidos sejam conhecidos e adotados pela gerência e pelo pessoal envolvido. O comprometimento da alta administração é importante para garantir que recursos adequados sejam dedicados para o planejamento de emergência, treinamento e testes necessários. O pessoal responsável por atividades de manutenção da continuidade de serviço, tais como realização de cópias de segurança de arquivos, precisa estar bem informado dos riscos da não realização dessas tarefas.

7.5.1.3- Controles de Acesso

Os Controles de Acesso, como disposto no capítulo 4, têm o propósito de oferecer a garantia de que os recursos computacionais são protegidos contra modificação ou divulgação não autorizada, perda ou dano. Eles incluem controles lógicos e físicos. X

Controles de acesso impróprios diminuem a confiabilidade dos dados processados pelo sistema e aumentam o risco de destruição ou divulgação indevida de dados.

Os objetivos da restrição do acesso visam: garantir que os usuários tenham acesso somente aos recursos necessários para executar suas tarefas; limitar o acesso a recursos de alto risco, tais como *softwares* de segurança, a poucos indivíduos; e impedir os funcionários de executar funções incompatíveis ou além da sua responsabilidade.

Se esses objetivos são alcançados, o risco de modificação ou de divulgação indevida de dados pode ser reduzido, sem produzir interferência nas necessidades práticas dos usuários. O equilíbrio adequado entre necessidades do usuário e requerimentos de segurança exige uma análise cuidadosa da vulnerabilidade e importância de cada recurso de informação disponível, em confronto com as tarefas executadas pelos usuários.

A prática de controles de acesso apropriados exige, a determinação do nível e tipo de proteção adequados a cada recurso e a identificação das pessoas que precisam ter acesso a esses recursos.

7.5.2- Controles de *Softwares* Aplicativos

Softwares aplicativos são projetados para executar determinado tipo de operação, como o cálculo do imposto de renda na fonte. Os Controles de Aplicativos são incorporados diretamente em *softwares* aplicativos, nas três áreas de operação (entrada, processamento e saída de dados), com o objetivo de garantir um processamento confiável e acurado.

A avaliação dos controles de aplicativo deve sempre ser executada em conjunto com a verificação dos controles gerais do sistema, bem como da legalidade do processamento.

Adiante são apresentados os controles que devem ser verificados em trabalhos de auditoria que incluam a avaliação de um ou mais programas aplicativos da organização auditada:

- a)* controles da entrada de dados: os controles desta categoria são projetados para garantir que os dados são convertidos para um formato padrão e inseridos na aplicação de forma precisa, completa e tempestiva. Os controles de entrada de dados devem detectar transações não autorizadas, incompletas, duplicadas ou errôneas e assegurar que sejam controladas até serem corrigidas;
- b)* controles do processamento de dados: os controles de processamento devem assegurar que todos os dados de entrada sejam processados e que o aplicativo seja executado com sucesso, usando os arquivos de dados, as rotinas de operação e a lógica de processamento corretos; e
- c)* controles da saída de dados: os controles da saída de dados são utilizados para garantir a integridade e a correta e tempestiva distribuição dos dados de saídas.

7.5.3 Desenvolvimento de Sistemas

A auditoria do Desenvolvimento de Sistemas objetiva examinar a adaptação das metodologias e procedimentos de projeto, desenvolvimento, implantação, revisão e pós-implantação dos sistemas produzidos dentro da organização. Essa avaliação abrange o ambiente de desenvolvimento da organização ou prevê a análise do processo de desenvolvimento de um sistema específico, ainda na fase de planejamento, já em andamento ou após sua conclusão.

O desenvolvimento de um Sistema de Informações representa um investimento que não pode ser assumido sem dados confiáveis e precisos sobre o custo do projeto, seus benefícios e os riscos envolvidos. Todos os projetos de desenvolvimento de sistemas precisam ter sido avaliados em profundidade, devendo ser precedidos de análises de custo/benefício, capacidade de satisfação dos usuários e de atendimento aos objetivos da organização, custos de desenvolvimento, medidas de desempenho, planos de implementação e previsão de recursos humanos. Além disso, são necessários

mecanismos gerenciais que auxiliem a definição da prioridade dos projetos e permitam sua avaliação e controle durante todo o processo de desenvolvimento.

O desenvolvimento de sistemas possui as seguintes fases: planejamento; elaboração do plano de desenvolvimento; organização do projeto; elaboração do projeto de sistema; revisão e aprovação pelos dirigentes; desenvolvimento e implantação e revisão de pós-implantação.

No planejamento, a organização identifica as necessidades de informação ainda não atendidas e estabelece um plano de ação para o desenvolvimento dos sistemas de maior prioridade. Nesta fase deve ser estabelecida e documentada as metodologias de desenvolvimento a serem adotadas e definidas as responsabilidades de todas as pessoas envolvidas no desenvolvimento de sistemas.

Na elaboração do plano de desenvolvimento, o projeto é avaliado mais minuciosamente quanto a análises de viabilidade técnica e custo/benefício. Sendo confirmada a conveniência do desenvolvimento do projeto, a organização estabelece e aprova um plano de desenvolvimento ou modernização do sistema específico, com elementos suficientes para permitir o seu projeto físico e lógico na próxima fase.

É selecionada a equipe de projeto, que deve ter habilidades e conhecimentos suficientes para conduzir com sucesso as atividades de elaboração do projeto físico e lógico, desenvolvimento e implantação do sistema.

A equipe de projeto, com base no plano de desenvolvimento aprovado, cria e submete à gerência um plano de trabalho, informando a abrangência e conteúdo do projeto, bem como os mecanismos de acompanhamento e controle (cronograma, datas-limite, processo de supervisão e acompanhamento das etapas), de acordo com o estabelecido na metodologia de desenvolvimento de sistemas. Os usuários após análise, manifestam se concordam com a abrangência e o conteúdo do sistema. Posteriormente, o plano de trabalho deve ser devidamente analisado e aprovado pela gerência de planejamento.

A equipe desenvolve o sistema e avalia sua qualidade. Os usuários testam o sistema e aprovam ou não sua implantação. O sistema aprovado é implantado, de acordo com planos detalhados de testes, transição, implantação e operação. Deve ser criado um plano detalhado para o teste do sistema, compatível com os padrões de teste estabelecidos pela organização e respeitando as responsabilidades definidas para cada parte envolvida (usuários, analistas de sistema, programadores e auditores).

Efetuada o teste de aceitação final junto a usuários selecionados, as deficiências de desempenho devem ser devidamente retificadas antes do sistema ser considerado em condições de entrar em operação.

A gerência de desenvolvimento de sistemas deve verificar o grau de satisfação dos usuários com os sistemas implementados e conferir se os requisitos iniciais do usuário foram ou não atendidos.

7.5.4- Banco de Dados

O termo **Banco de Dados** foi usado para descrever um arquivo contendo dados acessíveis a um ou mais programas ou usuários. Os arquivos de dados eram designados para aplicações específicas e o programa era projetado para acessá-los de uma forma predefinida. Contudo, essa abordagem oferecia dificuldades se porventura os dados ou o programa tivessem que ser alterados.

Posteriormente, o acesso do banco dados passou a ser realizado por meio de um Sistema Gerenciador de Banco de Dados (SGBD ou DBMS _ *Database Management System*).

O SGBD resolve problemas atinentes a dados duplicados e deficiências na integridade e segurança dos dados. Antes do SGBD, à medida que um aplicativo era desenvolvido, os dados necessários eram produzidos quase sempre em um formato específico para aquele programa. Se um sistema de recursos humanos era criado,

seguido por um sistema imposto de renda, eram feitas cópias separadas de elementos de dados comuns aos sistemas. Destarte, os dados eram duplicados e sua integridade ameaçada, já que as cópias de dados rapidamente perdiam o sincronismo.

Em suma, o objetivo do SGBD é manter e organizar os dados e torná-los disponíveis para programas aplicativos, quando requisitados. O SGBD é um software complexo, que se responsabiliza também pela segurança e integridade dos dados, eliminando diversas tarefas de administração que antes precisavam ser executadas pelos aplicativos. Assim, o SGBD tornou-se um requisito capital para a maioria dos ambientes de informática. Embora o custo de um SGBD seja alto, suas vantagens são compensatórias, dentre as quais citam-se:

- a)* manter os arquivos que constituem o banco de dados;
- b)* oferecer uma interface uniforme para usuários e aplicativos que utilizam os dados;
- c)* fornecer elementos de dados para aplicativos que os solicitem;
- d)* diminuir a necessidade do aplicativo de saber como os dados são armazenados (estruturas de arquivos e registros);
- e)* manter a integridade dos dados, quanto ao seu conteúdo (validação) e referência (dependência de um elemento na existência de outro); e
- f)* controlar o acesso aos dados por meio de mecanismos de segurança.

Geralmente, o banco de dados é armazenado em um sistema computacional único, estando disponível para usuários diretamente conectados a esse sistema, ou com acesso via rede. Esse banco de dados centralizado, muitas vezes satisfaz completamente as necessidades da organização.

Porém, existe a necessidade de acesso aos mesmos dados em diferentes localidades. Uma solução alternativa seria instalar banco de dados duplicados em cada localidade, com cópia de todos os dados. Isso oferece independência a cada localidade com relação à disponibilidade dos dados, caso seja interrompido o acesso ao sistema central, mas acarreta problemas de manutenção, integridade e duplicação dos dados.

Todavia, a solução mais plausível é o uso de um SGBD que permita um banco de dados distribuído, onde cada localidade participante executa uma cópia do SGBD, que coopera com as demais por meio da rede e, para todos os efeitos, forma um sistema único.

Os dados que são compartilhados por meio da rede pelas diversas localidades também são tratados pelo SGBD como um banco de dados único e completo. Os dados são distribuídos pela rede de acordo com as solicitações de cada localidade, aumentando a velocidade do acesso.

O tamanho e a complexidade das bases de dados exigem que as organizações possuam um pessoal especificamente designado para cuidar de todos os aspectos da administração do banco de dados, chamados de “administrador de banco de dados”. As tarefas do administrador de banco de dados incluem a manutenção de estruturas e sub-estruturas de dados, do *software* de SGBD e programas relacionados, documentação do banco de dados, verificação da compatibilidade de novos sistemas com o banco de dados, procedimentos de cópias de segurança, registros históricos e recuperação de falhas do banco de dados.

O administrador de banco de dados é responsável, também, pela manutenção de controles sobre os dados, podendo combinar responsabilidades que abranjam procedimentos e controles, que em sistemas convencionais seriam normalmente efetuados por pessoas diferentes. Quando esses procedimentos e controles estiverem muito concentrados no administrador de banco de dados, é importante, para preservar a adequada segregação de funções, que esse administrador seja impedido de obter acesso não supervisionado às instalações computacionais e aos sistemas em operação, bem como de iniciar transações.

A organização deve estabelecer políticas e procedimentos que garantam a disponibilidade do banco de dados e sua pronta recuperação após a ocorrência de falhas operacionais ou desastres..

7.5.5 Redes de Computadores

Muitas vezes os usuários de um sistema podem estar em localidades distantes de onde se encontram os recursos computacionais da organização. Assim, é necessário o uso de mecanismos de transporte de informações entre computadores .

As redes de comunicação de computadores permitem às pessoas o acesso instantâneo a dados e a usuários em diferentes locais da organização. Essas redes trazem benefícios como: acesso compartilhado a dados, aplicações, impressoras e outros dispositivos; correio eletrônico; acesso a usuários e dispositivos remotos; redução do custo de *software*, por meio de licenças de multiusuário; e acesso e execução de processamentos em sistemas remotos.

Entretanto, para o controle dessa comunicação de dados são utilizados alguns dispositivos como :

- a) arquivo *log* de comunicações, onde ficam registrados todos os blocos transmitidos corretamente e incorretamente para efeito estatístico e para tentativas de recuperação de dados transmitidos;
- b) *software* de comunicação de dados para verificações de protocolo de transmissão, gravação do arquivo *log* de transações e para codificação e decodificação de sinais de comunicação;
- c) protocolo de transmissão, que garante a recepção correta do bloco de informações transmitido; e
- d) *software* ou *hardware* para a realização de codificação e decodificação das informações transmitidas.

O maior risco oferecido pelas redes é o de acesso não autorizado a dados e programas da organização, que pode resultar em danos ou prejuízos intencionais ou acidentais.

Existe uma grande variedade de *software* e *hardware* especializados em limitar o acesso de indivíduos ou sistemas externos a uma rede de comunicação. Exemplos de componentes de rede que podem ser usados para limitar o acesso incluem *firewalls*

(dispositivos que restringem acesso entre redes, importantes para reduzir o risco associado ao uso da Internet), monitores de teleprocessamento (programas incorporados ao sistema operacional dos computadores para limitar o acesso) e dispositivos de proteção dos canais de comunicação.

Em alguns casos envolvendo telecomunicação, não é possível ou prático restringir o acesso à rede mediante controles físicos ou lógicos. Nesses casos, ferramentas de criptografia podem ser usadas para identificar e autenticar usuários, bem como para auxiliar na proteção da integridade e sigilo de dados e programas quando estes se encontram no sistema computacional, estão sendo transmitidos para outro sistema ou foram armazenados em meios removíveis (disquetes e outros).

Conforme relatado no capítulo 4, a criptografia envolve o uso de algoritmos e combinações de chaves que servem para transformar uma mensagem em códigos ininteligíveis para aqueles que não possuem a chave secreta necessária para decifrá-los, mantendo assim o conteúdo do arquivo ou mensagem confidencial. Servem também para fornecer uma assinatura eletrônica, a qual pode indicar se alguma alteração foi feita no arquivo, garantindo sua integridade e identificando o autor da mensagem.

Dessa forma, a auditoria das redes de comunicação deve abranger os seguintes elementos:

- a)* Gerência de rede: devem existir procedimentos e políticas para auxiliar a gerência do ambiente de rede e padrões definitivos para controle da *hardware* e do *software* envolvidos;
- b)* Segurança dos dados e da rede: devem existir mecanismos de controle de *hardware* e *software* que garantam a segurança e integridade dos dados mantidos no ambiente de rede e dos recursos físicos que a compõem; bem como limitem e controlem o acesso a programas e dados;
- c)* Operação da rede: a organização deve oferecer condições para uma operação eficiente da rede, incluindo normas e procedimentos de treinamento de pessoal,

execução de cópias de segurança, avaliação da eficiência do serviço e rotinas de recuperação da rede após interrupções inesperadas; e

- d) Software de rede:* a gerência de rede deve monitorar e controlar o *software* de comunicação e o sistema operacional instalado.

Além dos riscos associados à facilidade de acesso a dados e programas, a auditoria das redes de comunicação de computadores deve contemplar os riscos relativos a operação incorreta do sistema, perda de informações não protegidas por cópias de segurança e outras situações que podem causar dano ou prejuízo à organização em função do ambiente de rede.

7.5.6 Microcomputadores

Os microcomputadores podem ser utilizados isoladamente ou estar conectados a uma rede, com o propósito de compartilhar dados ou periféricos. Apesar de oferecerem às organizações diversas vantagens quanto ao aumento de eficiência e flexibilidade, em razão da necessidade de mecanismos de segurança próprios, que diferem daqueles tipicamente instalados num centro de processamento de dados, a organização também pode ficar exposta a riscos substanciais, como:

- a) Familiaridade:* por causa da aparente simplicidade e facilidade de uso, existe o risco de que o uso inadequado seja subestimado por usuários e pela gerência;
- b) Custo:* ainda que os microcomputadores em si possam ser considerados de baixo custo, é importante levar em conta o custo dos *softwares*, periféricos e manutenção, que pode elevar significativamente o custo de uma máquina;
- c) Localização:* microcomputadores normalmente estão localizados em escritórios comuns, com pouca proteção contra furto, acesso não autorizado ou dano acidental;

- d) *softwares* proprietários: apesar de ser mais barato adquirir programas do que desenvolvê-los internamente, os *softwares* oferecidos pelo mercado muitas vezes não apresentam mecanismos de segurança adequados; e
- e) conexão com outros computadores: quando os microcomputadores são usados como terminais de *mainframes* ou inseridos em uma rede de comunicação de computadores, o seu uso não autorizado pode levar ao acesso indevido a dados e programas de toda a organização.

Para proteger-se contra esses riscos, a organização precisa adotar políticas e procedimentos específicos quanto ao uso de microcomputadores pelos seus funcionários, compreendendo padrões de *hardware*, *software*, aquisição, treinamento e suporte, além dos controles gerais e de aplicativos.

Os microcomputadores precisam de controles específicos destinados a protegê-los da perda de dados e programas por furto ou acidente (a ser evitada por restrições físicas de acesso às máquinas e aos controles de *software*, tais como senhas de acesso e realização periódica de cópias de segurança) e do furto de equipamentos (por meio de mecanismos adequados de segurança no local de trabalho).

Existem três elementos críticos para a auditoria dos microcomputadores: os controles do *software* em uso, a segurança e os controles sobre operações.

Os controles do *software* em uso são destinados a garantir a consistência da operação do *software* instalados nos microcomputadores, impedindo a instalação de programas não autorizados e a alteração indevida do *software* instalado.

Os controles de segurança controlam o acesso a recursos computacionais, dados e programas, protegendo-os contra alterações indevidas, vírus de computador, furtos, divulgação de documentos sigilosos e a prática de pirataria.

Os controles sobre a operação protegem os recursos de microinformática contra prejuízos e danos causados por falta de treinamento de pessoal e de manutenção adequada.

Observa-se na seção 7.5 a importância e abrangência das áreas que a Auditoria de Sistemas compreende. Assim, a forma sistematizada de consolidar todos os controles que devem ser analisados numa Auditoria de Sistema é através de um **Programa de Auditoria**, vez que este instrumento pormenoriza os objetivos e o escopo do trabalho a ser executado, advertindo os procedimentos a serem apostos e conduzindo de modo adequado o trabalho do auditor.

7.6- O Auditor de Sistemas

O Auditor de Sistemas é o Auditor Interno da organização que executa trabalhos de auditoria nos Sistemas de Informações Computadorizados. Destarte, ele deve observar as Normas Profissionais do Auditor Interno emanadas pela Resolução n. 781 do CFC, o Código de Ética Profissional aprovado pela Resolução n. 803 do CFC, as Normas Brasileiras para o Exercício da Auditoria Interna publicadas pelo AUDIBRA (1991, p. 105), que incluem o Código de Ética da Auditoria Interna e, sobretudo, o Código de Ética do Auditor de Sistemas da Informações, determinado pelo ISACA.

O exercício da atividade de auditoria interna exige do profissional um perfil técnico e psicocomportamental compatível com sua ocupação. O AUDIBRA (1991, p. 128-131) apresenta as características psicocomportamentais que este profissional deve apresentar, conforme disposto no QUADRO 17.

**QUADRO 17 – CARACTERÍSTICAS PSICOCOMPORTAMENTAIS DO
AUDITOR INTERNO**

Espírito crítico muito desenvolvido	Rapidez de ação/julgamento
Capacidade analítica de síntese e objetividade	Raciocínio lógico
Compromisso permanente com a verdade	Dinâmica de grupo
Zelo e disciplina	Perspicácia e perseverança
Liderança e capacidade de motivação	Disciplina
Comportamento extremamente racional	Moderação
Comunicação objetiva, adequada e clara	Impulsividade
Sociabilidade	Segurança pessoal
Percepção visual e global	Tomada de decisão de maneira geral
Boa memória	Capacidade numérica
Concentração	Criatividade
Adaptabilidade a novas situações	Iniciativa
Organização	Sigilo

FONTE: AUDIBRA (1991, p. 128-131)

De igual forma, essas características psicocomportamentais do Auditor Interno são necessárias ao Auditor de Sistemas. Contudo, o perfil técnico do Auditor de Sistemas requer conhecimentos da tecnologia da informação e, se possível, experiência prática anterior, tendo trabalhado em centros de processamento de dados, desenvolvido sistemas ou prestado consultoria técnica na área de informática. Segundo o item n. 040.010 do **Padrão Internacional de Auditoria** definido pela ISACA, o Auditor de Sistemas de Informações deve ser competente tecnicamente, possuindo as habilidades e conhecimentos necessários para a execução do seu trabalho.

Ratificando este padrão, a **Norma Brasileira de Contabilidade** n. 12 preceitua:

“12.2.5.1 - O auditor interno deve dispor de conhecimento suficiente dos recursos de Processamento Eletrônico de Dados e dos sistemas de processamento da Entidade, a fim de avaliá-los e planejar adequadamente seu trabalho.

12.2.5.2 - O uso de técnicas de auditoria interna que demande o emprego de recursos de Processamento Eletrônico de Dados, requer que o auditor interno as domine completamente, de forma a implementar os próprios procedimentos ou, se for o caso, orientar, supervisionar e revisar os trabalhos de especialistas.”

Assim, o Auditor de Sistemas deve apresentar conhecimento suficiente de sistemas computadorizados, a fim de planejar, dirigir, supervisionar e revisar o trabalho executado.

Quanto mais complexo o Sistema de Informações Computadorizado a ser auditado, maior deverá ser a capacidade técnica do Auditor de Sistemas. Normalmente, os conhecimentos básicos em informática englobam desde sistemas operacionais, *softwares* básicos, bancos de dados e redes de comunicação até controle de acesso, segurança de informações, plano de contingências e de recuperação e metodologias de desenvolvimento de sistemas.

Em uma auditoria mais minuciosa, é provável que sejam necessários conhecimentos suplementares de técnicas, como CAATs - *Computer Assisted Audit Techniques*, que compreendem *softwares* de auditoria, de Simulação Paralela, *Mapping* e linguagens de programação específicas.

Para muitos auditores internos, auditar Sistemas de Informações Computadorizados é um trabalho aturado, pois a área de informática, além de ser extremamente técnica, é dinâmica, estando em constantes transformações tecnológicas. Desse modo, o auditor com formação em Ciências Contábeis, que domina conhecimentos e técnicas de auditoria geral, encontra dificuldades em auditar sistemas.

DIAS (2000, p. 19) entende que capacitar auditores em informática é uma tarefa bastante árdua, pois uma formação sólida em sistemas geralmente só pode ser conseguida com anos de estudos, treinamento ou experiência prática e aprimoramento contínuo, já que as tecnologias estão sempre avançando nesse campo.

A autora ainda discorre que podem-se obter resultados mais rápidos se a organização optar por treinar profissionais de informática em auditoria, vez que com o aumento da complexidade dos sistemas computacionais, o uso de *softwares* como ferramentas de apoio à auditoria e o desenvolvimento da área de segurança de informações, a capacitação de profissionais de informática em auditoria tornou-se uma alternativa mais simples do capacitar um auditor em informática.

Contudo, esta alternativa não pode ser adotada em qualquer organização pública, onde geralmente os auditores internos, cargo de caráter efetivado através de concurso público, são bacharéis em Ciências Contábeis. Neste caso, o ideal é que se estabeleça um plano de desenvolvimento técnico, segundo o qual medidas fundamentais para o treinamento do auditor em Auditoria de Sistemas sejam adotadas. Conforme DIAS (2000, p. 20-22) alguns fatores devem constar deste plano:

- a) Participação em seminários e cursos de especialização: para adquirir e manter atualizados os conhecimentos de Auditoria de Sistemas, além dos cursos formais na área, é necessário estimular a participação dos auditores em seminários, cursos de especialização e congressos. Os grupos de discussão, boletins e *homepages* de organizações especializadas, disponíveis na *Internet*, também são uma boa fonte de informações.
- b) qualificação profissional: os auditores devem ser encorajados a obter qualificações profissionais que testem se seus conhecimentos estão atualizados e compatíveis com os padrões profissionais. Em alguns países existem organizações que promovem certificações de qualificação profissional de auditores de sistemas, por meio de uma série de exames. A seguir, alguns exemplos de organizações certificadoras:
 - *Information Systems Audit and Control Association (ISACA)*: certificado de Auditor de Sistemas de Informações
 - *Institute of Internal Auditors (IIA)*: qualificação em Auditoria Computacional.

- Sociedade dos Auditores de Sistemas (SAS): certificado de Auditoria de Sistemas no Brasil.

O IIA e a ISACA, em especial, desempenham um papel ativo no desenvolvimento de padrões de auditoria e controle de sistemas de Informações. Sob demanda, provêem informações sobre suas publicações, padrões e qualificações.

Como a tecnologia da informação está em constante evolução, é essencial que o treinamento do Auditor de Sistemas acompanhe essa evolução, incluindo em seu currículo novas técnicas de auditoria e aspectos de informática de tecnologias mais avançadas. Conseqüentemente, a certificação de auditores de sistemas também é sempre atualizada. Para manter seu currículo compatível com a tecnologia corrente, o auditor deve prestar exames periodicamente. Algumas organizações, ao contratar auditores para seu quadro de funcionários, exigem a apresentação dos certificados atualizados e determinam que os auditores se submetam a outros testes com freqüência para manterem sua qualificação. O desenvolvimento profissional contínuo não é apenas desejável, mas essencial.

- c) Manuais de Auditoria de Sistemas: a equipe de especialistas em Auditoria de Sistemas, para orientar o trabalho dos auditores e difundir o conhecimento nessa área, deve ser responsável pela elaboração de um ou mais manuais contendo instruções para a condução de Auditorias de Sistemas, exemplos de objetivos de controle e procedimentos de auditoria, explanações técnicas sobre alguns tópicos considerados importantes na área de informática, técnicas e metodologias de auditoria e instruções sobre o uso de *softwares* de auditoria.

Cabe à chefia decidir se serão elaborados documentos específicos ou se serão utilizadas publicações de outras entidades de fiscalização e controle na área de tecnologia da informação. Elaborar sua própria documentação, a partir de um trabalho de pesquisa e de adaptação à sua realidade, de acordo com as técnicas adotadas pela organização, é, sem duvida, a melhor alternativa em termos de qualidade.

- d) Biblioteca técnica: o grupo de Auditores de Sistemas de uma organização deve ter à sua disposição uma biblioteca técnica para consulta. Dessa forma, poderão orientar seus trabalhos de acordo com os padrões conhecidos na área, manter-se atualizados com relação às novas tecnologias e utilizar publicações técnicas como fonte de consulta durante a auditoria e na elaboração do relatório. Além disso, é aconselhável manter arquivados todos os relatórios de Auditorias de Sistemas. Esta biblioteca pode conter a legislação e normas aplicadas, padrões de auditoria, manuais, livros de informática e auditoria de sistemas, manuais e folhetos de *hardware* e *software*, revistas especializadas, publicações de entidades de controle e auditoria e artigos de jornais relacionados com a área.

Como foi dito neste capítulo, a tecnologia está em contínua evolução. Portanto, o treinamento constante dos auditores de sistemas é imprescindível para que estejam preparados para realizar auditorias de qualidade e com grau de profundidade técnica adequado.

Todos os auditores, especialistas ou não em sistemas, devem receber treinamento básico de Auditoria de Sistemas, já que dificilmente irão auditar organizações que não utilizam informática em seus processos e controles.

Apesar de todos esses fatores, o essencial para a execução de uma Auditoria de Sistemas é que o auditor siga as orientações de um **Programa de Auditoria**, pois é a partir das informações constantes neste instrumento que o profissional irá conduzir de maneira eficiente seu trabalho.

7.7- Conclusão

Ao avaliar os sistemas e o ambiente computacional em que estão inseridos, com o propósito de identificar os possíveis riscos que estejam ocorrendo, ou que possam ocorrer, e de, principalmente, sugerir ações saneadoras e melhoria dos controles internos, constitui a Auditoria de Sistemas um instrumento extremamente importante

para assegurar a qualidade e a segurança dos Sistemas de Informações Computadorizados.

Para cumprir o propósito da Auditoria de Sistemas é necessário que o auditor ~~tenha~~ um perfil adequado, observe a legislação aplicável, adote as técnicas mais apropriadas para desenvolver o seu trabalho e, sobretudo, siga um **Programa de Auditoria de Sistemas**.

Este capítulo encerra o referencial teórico iniciado no capítulo 3 e estendido pelos capítulos 4, 5, 6 e 7.

No capítulo seguinte, desenvolve-se um estudo de caso sobre a AUDIM, que foi construído a partir da pesquisa documental, da observação participante e em uma monografia desenvolvida em 1997 pela autora desta dissertação, intitulada **Auditoria Geral do Município: atuação e reflexos na Administração Municipal** (MORAIS, 1997).

8 AUDITORIA DO MUNICÍPIO – ESTUDO DE CASO

8.1- Introdução

Este capítulo está baseado na pesquisa documental, na observação participante e em uma monografia desenvolvida em 1997 pela autora, intitulada **Auditoria Geral do Município: atuação e reflexos na Administração Municipal** (MORAIS, 1997), que constitui o trabalho de conclusão do IV Programa de Especialização em Administração Municipal, oferecido pela Escola de Governo da Fundação João Pinheiro.

Inicialmente, será feita uma abordagem sobre o histórico, finalidades e estrutura organizacional da AUDIM e, ainda, sobre o Auditor Municipal. Posteriormente, serão apresentados os procedimentos adotados e as modalidades de auditoria realizadas pelo órgão.

8.2 -Histórico

A Auditoria Geral do Município (AGM) foi criada em 13 de julho de 1983, através do Decreto n. 4.489, que dispôs sobre a organização administrativa da PMBH, na gestão do Prefeito Hélio de Carvalho Garcia. Com o Decreto n. 4.523, de 12 de setembro de 1983, foram definidas as incumbências do órgão. Contudo, o cargo de Auditor Geral não foi provido.

Somente com a Lei n. 4.476, de 30 de maio de 1986, na gestão do Prefeito Sérgio Ferrara, é que foi instituída a primeira fase da estrutura organizacional da AGM, definindo a competência do Auditor Geral, Auditor Adjunto, Diretor, Chefe de Seção

e dos Auditores, cargo na época comissionado e provido cinquenta por cento por recrutamento amplo e cinquenta por cento por recrutamento limitado. O primeiro Auditor Geral foi José Lincoln Magalhães, que permaneceu no cargo até o final do exercício de 1988.

Em 1989, na gestão do Prefeito Pimenta da Veiga, a Lei n. 5.562 modificou a estrutura organizacional da Administração Direta Municipal, consolidando as finalidades e competência da AGM. Tarcísio Antônio Rodrigues de Souza respondeu pelo cargo de Auditor Geral no período de 1989 a 1992.

A Lei n. 6.352 de 15 de julho de 1993, vigente na gestão do Prefeito Patrus Ananias de Sousa, alterou a estrutura da Administração Direta Municipal e determinou em seus arts. 7º, 8º e 9º as atribuições da AGM. Walter Alberto Prosdocimi Pinto respondeu pelo órgão no período de 1993 a fevereiro de 2000. Durante o período compreendido entre março a dezembro de 2000, Marco Antônio Resende, na época Procurador Geral do Município, respondeu interinamente pela AGM.

Com a Lei n. 8.146, de 29 de dezembro de 2000, foi modificada a estrutura da Administração Direta do Poder Executivo, dando nova denominação à AGM, que passou a ser intitulada AUDIM. Foi suprimido o cargo de Auditor Geral Adjunto e o de Auditor Geral foi alterado para Auditor-Chefe. Milton de Sousa Júnior é o titular da AUDIM desde janeiro de 2001.

8.3 -Finalidades

A AUDIM é um órgão componente da Administração Direta Municipal, escalonada no primeiro grau hierárquico da estrutura organizacional da PMBH, sendo assim subordinada diretamente ao Prefeito. É um órgão técnico, dotado de autonomia funcional, que planeja e exerce suas atividades atuando com liberdade de acesso aos órgãos e entidades do Poder Executivo Municipal, constantes do ANEXO C desta dissertação.

Conforme os arts. 10º e 11º da já citada Lei 8.146/00, a AUDIM tem por finalidade executar a auditoria interna, preventiva e de controle dos órgãos e entidades do Poder Executivo Municipal. É de sua competência dirigir, supervisionar e executar o serviço de auditoria nas áreas administrativa, financeira, patrimonial, operacional e de custos, observando a legislação aplicável, bem como normas, planos, programas e procedimentos estabelecidos.

8.4 -Estrutura Organizacional

A AUDIM está diretamente subordinada ao nível mais elevado do Poder Executivo Municipal, o que contribui para não ocorrer perda da autonomia profissional, condição indispensável à realização de um trabalho com independência nas entidades públicas do Poder Executivo. LOBO (1986, p.26) considera importante alocar corretamente a Auditoria Interna na estrutura organizacional como órgão de Assessoramento Direto e Imediato ao chefe do Poder Executivo, mantendo sua independência absoluta em relação aos demais órgãos de linha e assessoramento, e definindo com clareza e objetividade o seu escopo.

A AUDIM tem uma estrutura organizacional bastante simples, conforme apresentado na FIG. 10.

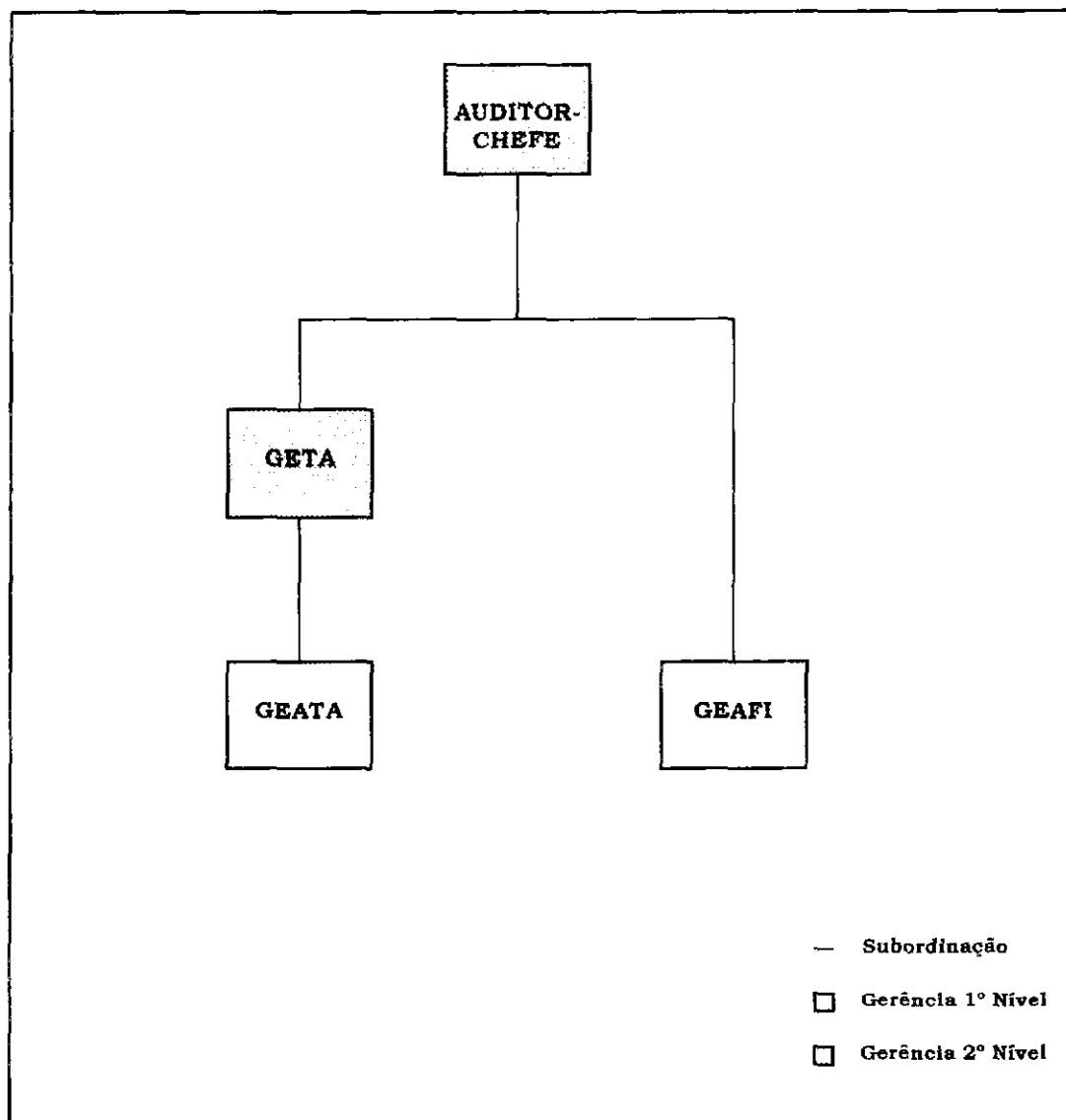


FIGURA 10- Estrutura Organizacional da AUDIM

FONTE- Decreto n. 10.545, de 09 de março de 2001(adaptada).

Na estrutura organizacional da AUDIM consta a posição do Auditor-Chefe, que é de nível de direção superior. Abaixo está posicionado a Gerência de Coordenação de Trabalhos de Auditoria (GETA), onde estão lotados os Auditores e o Gerente de Coordenação Técnica de Trabalhos de Auditoria. Cabe à GETA realizar auditorias, elaborar relatórios e pareceres, bem como a “Programação Anual de Auditorias”, os programa e normas específicas sobre os trabalhos de auditoria.

Logo abaixo da GETA, estão posicionadas a Gerência de Apoio aos Trabalhos de Auditoria (GEATA) e a Gerência Administrativo-Financeira (GEAFI). A GEATA

realiza a digitação, formatação, catalogação, organização e arquivamento dos relatórios de auditoria e outras atividades de apoio aos trabalhos do órgão. A GEAFI é responsável pelas atividades de controle sobre recursos humanos, materiais, patrimônio, contratos e instrumentos financeiros e orçamentários da AUDIM.

8.5 -Auditores

A atividade-fim da AUDIM é desenvolvida pelos Auditores, cargo de provimento efetivo de Auditor I, instituído pela Lei n. 5.447, de 30 de novembro de 1988. O Auditor I é o Bacharel em Ciências Contábeis, registrado no Conselho Regional de Contabilidade, aprovado em concurso público, nomeado, empossado e que efetivamente entrou no exercício de suas funções. Sua conduta é pautada nos Códigos de Ética do Contabilista e do Auditor Interno.

O primeiro concurso para o cargo de Auditor I foi realizado em 1994. As atribuições e a qualificação necessárias ao seu provimento estão definidas no art. 1º do Decreto n. 8.565, de 18 de janeiro de 1996, *verbis*:

"Art. 1º - As atribuições e demais requisitos ao provimento de cargo de Auditor I, do Subgrupo de Atividades de Administração Geral constante do Anexo IV da Lei n. 5.447, de 30 de novembro de 1988, com a redação dada pela Lei n.6.352, de 15 de julho de 1993, ficam assim definidas:

Classe: Auditor I

Qualificação: Curso superior de Ciências Contábeis e registro no Conselho Regional de Contabilidade

Atribuições:

- a) verificar a adequação dos procedimentos adotados pela contabilidade pública e comercial, durante e no encerramento de cada exercício financeiro da Administração Pública Municipal;*
- b) cumprir as prescrições dos roteiros de auditoria aplicáveis a cada caso;*
- c) assistir e orientar a Administração Pública Municipal no âmbito das atribuições de auditoria;*
- d) examinar o conteúdo de livros e controles internos de quaisquer órgãos ou entidades;*

- e) *examinar e opinar sobre quaisquer fontes de informações relacionadas com as atividades dos órgãos da Administração Pública Municipal;*
- f) *examinar e avaliar a solidez, eficiência e modo de aplicação dos controles contábeis e internos, financeiros e operacionais da Administração Pública Municipal, bem como de sua política e regulamentações internas;*
- g) *examinar e avaliar o cumprimento de toda classe de contratos e convênios firmados por órgão ou entidades da Administração Pública Municipal;*
- h) *examinar, avaliar e opinar sobre a correta utilização, localização e segurança dos bens patrimoniais da Administração Pública Municipal;*
- i) *determinar e opinar sobre a consistência e legitimidade das informações contábeis e demais dados oficiais da Administração Pública Municipal;*
- j) *examinar, avaliar e opinar sobre o cumprimento das prescrições legais e normativas aplicáveis a todos os órgãos da Administração Municipal.”*

A AUDIM conta com um corpo técnico de dezoito Auditores. Este quantitativo de Auditores representa apenas 60% do número de trinta vagas previsto na Lei n. 5.447/88.

Embora a exigência acadêmica para ingressar no cargo ser Bacharel em Ciência Contábeis, seis Auditores são detentores de outras graduações, sendo três bacharéis em Administração de Empresas, um bacharel em Direito e dois Licenciados Plenos em Contabilidade e Economia.

Por fim, acrescenta-se que cinco Auditores são pós-graduados em cursos de Especialização *Lato Sensu*, dentre os quais um em Análise de Sistemas e outro em Informática Pública. Outros três Auditores estão concluindo especialização *Lato Sensu* e uma Auditora é Mestranda em Administração Pública na área de concentração em Tecnologias da Informação.

Apesar da exigência para o cargo efetivo de Auditor, o cargo de Auditor-Chefe requer somente curso superior em qualquer área, sem necessidade do registro no Conselho ou Ordem da classe profissional.

8.6 -Procedimentos Adotados

A AUDIM tem como objetivo assegurar que se cumpram os princípios constitucionais da legalidade, impessoalidade, moralidade, publicidade e razoabilidade, apurando irregularidades, detectando deficiências dos controles internos, avaliando situações e propondo soluções aos órgãos auditados.

Os trabalhos da AUDIM consistem em Auditorias Programadas e Auditorias Extraordinárias. As Auditorias Programadas são desenvolvidas em concordância com uma programação preliminarmente elaborada. As Auditorias Extraordinárias podem ser deflagradas por determinação do prefeito, por solicitação de outros órgãos, por denúncia ou quando no curso do trabalho de auditoria, for detectado algum problema ou irregularidade, cujo caráter emergencial recomende providências imediatas.

São instalados trabalhos em todos os órgãos municipais (ANEXO C). Estes trabalhos se dão por inspeções no local auditado e por exame de documentos. Os roteiros aplicados são, dentre outros, de natureza contábil, patrimonial, de licitação e de pessoal.

Apresenta-se na FIG. 11 uma representação gráfica do fluxo dos procedimentos de auditoria e, em seguida, descreve-se, detalhadamente, cada fase do processo.

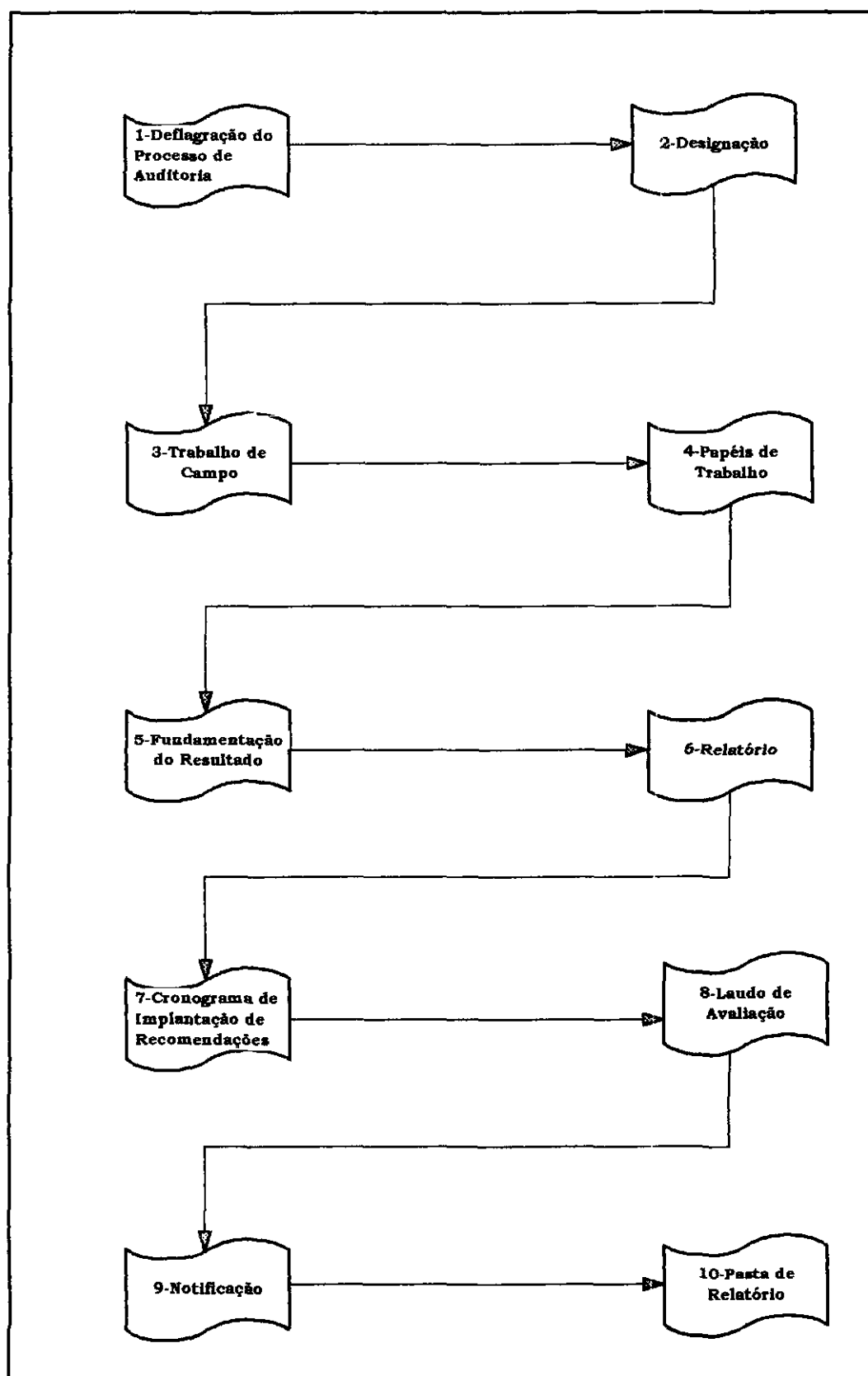


FIGURA 11- Fluxo de Procedimentos da AUDIM

FONTE- Instrução de Serviço DAUDIT n. 001/2001 (adaptada).

8.6.1- Programação Anual de Auditoria

A Programação Anual de Auditoria é elaborada por uma comissão composta por um representante dos Auditores, pelo Gerente da GETA e pelo Auditor-Chefe. Esta Programação destaca as modalidades de auditoria, o escopo dos trabalhos a serem realizados e os órgãos a serem auditados.

8.6.2- Designação

A Designação constitui uma ordem formal expedida pelo Auditor-Chefe, destacando o Auditor, indicando o órgão a ser auditado, o escopo da auditoria e fixando o prazo de execução do trabalho.

8.6.3- Trabalho de Campo

O Trabalho de Campo consiste em entrevistas, testes, exame de documentos e outras providências convenientes, visando à constituição dos papéis de trabalho e da documentação comprobatória da auditoria.

8.6.4- Papéis de Trabalho

Os Papéis de Trabalho têm como objetivo demonstrar formalmente as evidências reunidas ou resultantes das diversas fases do trabalho da auditoria no campo. Neles incluem-se programas de trabalho, testes, análises, estatísticas, pesquisas, entrevistas, fluxogramas, organogramas, questionários, informações coletadas e a documentação comprobatória de fatos ou situações consideradas relevantes para o trabalho, bem como a fundamentação dos resultados obtidos, comentada no item seguinte.

A forma dos papéis de trabalho varia de acordo com a natureza, a complexidade e as circunstância de cada trabalho, adotando-se formas específicas e padronizadas para tarefas de caráter objetivo. Os papéis de trabalho são colecionados em pasta própria,

organizados por assunto, de forma a possibilitar uma indexação que os relacione com os tópicos do relatório parcial de auditoria.

8.6.5- Fundamentação do Resultado

Tratar-se de um relato descritivo, parte integrante dos papéis de trabalho, elaborado para demonstrar, analiticamente, a evolução dos trabalhos de auditoria, de maneira a *permitir que se conheça a trilha e os fundamentos que conduziram a cada conclusão*, ainda que esta não se traduza numa irregularidade e apenas reflita a validação de um procedimento. O objetivo, em síntese, é sustentar o resultado da auditoria obtido a partir dos papéis de trabalho colecionados.

8.6.6- Relatório de Auditoria

Os Relatórios de Auditoria elaborados pela AUDIM são classificados em Relatórios Parciais e Relatórios Extraordinários.

8.6.6.1- Relatório Parcial

São elaborados Relatórios Parciais para as auditorias programadas ou extraordinárias. O relatório parcial é o documento no qual se busca expor, de forma sucinta e objetiva, os resultados decorrentes das averiguações procedidas, relacionando as irregularidades constatadas e com as recomendações propostas. Não se verificando nenhuma irregularidade ou, ainda, se as irregularidades verificadas forem sanadas no curso dos trabalhos de auditoria, o relatório, devidamente fundamentado, terá cunho definitivo.

O relatório-padrão da AUDIM tem a seguinte estrutura :

- a)** Folha de Rosto: identifica o órgão, a entidade e/ou unidade objetivo da auditoria e os respectivos titulares, registra o auditor ou a equipe de auditoria designada, bem como o coordenador técnico.

- b) Introdução: inclui os itens relacionados com a caracterização da auditoria de que trata o relatório, referenciando o ato que determinou a realização da auditoria, a coordenação técnica e a supervisão dos trabalhos, descrevendo o escopo da auditoria a realizar, o período auditado, o tempo despendido e os servidores contatados.*
- c) Procedimentos Adotados: descreve a forma de atuação e os procedimentos aplicados na realização da auditoria, relacionando métodos, técnicas e abordagens utilizadas e informando a amostra selecionada em relação ao universo, explicitada de forma percentual, quantitativa e qualitativa, bem como os critérios utilizados para sua seleção.*
- d) Pontos Verificados: descreve de forma resumida todos atos, fatos e procedimentos verificados e que fundamentaram o resultado.*
- e) Diagnóstico e Recomendações: trata-se da parte conclusiva do relatório parcial que descreve, clara e objetivamente, em tópicos numerados seqüencialmente, as irregularidades eventualmente levantadas, listadas na forma de diagnóstico, cada qual ilustrada com o respectivo caso concreto e seguida imediatamente de uma proposição de medidas saneadoras, na forma de recomendação. Sempre que couber, cada tópico deve ser complementado com a fundamentação legal em que se apoia a respectiva recomendação.*
- f) Proposta de Encaminhamento: manifestação do auditor indicando as medidas mais adequadas para efetivação das recomendações elencadas no relatório. Não se registrando nenhuma pendência, tal fato deve ser evidenciado juntamente com a proposição de arquivamento do relatório. Cabe comunicação, em separado, por meio de memorando, quando da constatação de ocorrências não relacionadas diretamente com o objetivo da auditoria, mas que possam demandar providências específicas.*

O relatório é emitido em três vias necessárias para atender à Secretaria Municipal de Coordenação, à Secretaria Municipal e o arquivo da AUDIM.

8.6.6.2- Relatório Extraordinário

Quando, no curso do trabalho de auditoria, for detectado algum problema ou irregularidade, cujo caráter emergencial recomende providências imediatas, a situação será retratada em um Relatório Extraordinário, devidamente fundamentado, explicitando a irregularidade ou o problema averiguado e recomendando a adoção das medidas saneadoras consideradas indicadas para o caso.

A estrutura deste relatório é idêntica à do relatório parcial.

8.6.7- Cronograma de Implantação das Recomendações

A etapa de cientificação ao auditado sobre o conteúdo do relatório parcial é destinada, num primeiro momento, a uma avaliação conjunta da natureza e a pertinência das irregularidades anotadas e a adequação das respectivas recomendações. Origina-se daí um documento, intitulado “Cronograma de Implantação das Recomendações”, que define e relaciona prazos para a execução das providências a serem adotadas em função das recomendações propostas e convencionadas.

8.6.8- Laudo de Avaliação

Esgotando os prazos para regularização definidos no Cronograma de Implantação das Recomendações, procede-se a uma verificação, observando se foram executadas as providências cronogramadas. O resultado desta fase é o “Laudo de Avaliação” que fará menção a cada uma das recomendações propostas ao auditado, comentando a extensão e eficácia das providências adotadas ou justificadas apresentadas e registrando a inobservância ou insuficiência das mesmas. Conterá, ainda, considerações conclusivas do trabalho.

8.6.9- Notificação

A Notificação consta de ofício da AUDIM dirigido ao titular do órgão de coordenação e ao titular do órgão temático auditado, dando-lhes ciência das pendências ainda existentes e do encaminhamento de relatório ao Secretário Municipal de Governo, Planejamento e Coordenação Geral, retratando as irregularidades não sanadas.

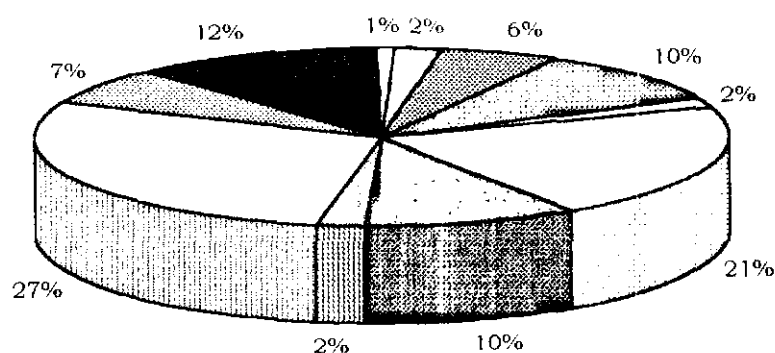
8.6.10- Pasta de Relatório

A Pasta de Relatório é a coletânea de todos documentos inerentes à auditoria realizada, quais sejam: papéis de trabalho, uma via dos relatórios, cronograma de implantações das recomendações, laudo de avaliação e uma via da notificação.

8.7- Modalidades das Auditorias Realizadas

Nesta seção, são apresentadas as modalidades de auditorias realizadas pela AUDIM no período compreendido entre 01/01/1994 a 31/12/2001. Optou-se por coletar dados deste período, vez que os detentores do cargo efetivo de Auditor I foram aprovados no primeiro concurso público realizado em 1994.

Devido ao sigilo sobre as informações da entidade estudada, não são apresentados os quantitativos de relatórios emitidos pela AUDIM, mas sim o percentual de cada modalidade de auditoria realizada em relação ao montante de trabalhos elaborados por ano. As modalidades de auditoria discriminadas no GRAF. 01, observam a Programação Anual de Auditoria da AUDIM.



- | | |
|-------------------------|-------------------------------------|
| ■ Almoxarifados | ■ Análise das Despesas |
| □ Caixas Escolares | □ Contábil, Financeira e Tributária |
| ■ Convênios | □ Fundos e Conselhos Municipais |
| □ Licitação e Contratos | ■ Patrimonial |
| ■ Pessoal | □ Sistemas Informatizados |
| ■ Precatórios | |

GRÁFICO 01- Modalidades de auditorias realizadas pela AUDIM de 1994 a 2001.

FONTE- Relatórios de auditorias realizadas pela AUDIM 1994 a 2001.

Observa-se que a AUDIM efetuou auditorias em diversas áreas da Administração Municipal, sendo que apenas 1% dos trabalhos referem-se à modalidade de Auditorias de Sistemas. Ressalta-se que, estes foram os três únicos trabalhos de Auditoria de Sistemas realizados durante os quinze anos de existência da AUDIM, ou seja, dos cento e trinta e três principais Sistemas de Informação da PMBH, somente três foram auditados.

Dois destes trabalhos foram executados em 1994 por um ex-funcionário da AUDIM, apesar de não ser tecnicamente qualificado. Tais trabalhos relatam algumas deficiências do Sistema de Arrecadação Municipal e do Sistema OPUS.

O terceiro trabalho foi realizado em 2000, no Sistema Integrado de Recursos Humanos, em seus subsistemas denominados Banco de Dados, Folha de Pagamento e

Lançamentos em Folha e no Sistema de Administração de Senhas e Perfis, denominado “Power-Lock”. Este trabalho enfocou pontos sobre consistência, segurança e integridade de dados e foi realizado por uma Auditora efetiva, no caso, a autora desta dissertação.

A iniciativa deste trabalho partiu desta Auditora, e como não há na AUDIM um programa específico para a modalidade de Auditoria de Sistemas, o que proporcionou a realização de tal auditoria foi o estudo do referencial teórico desta dissertação, que com os conhecimentos adquiridos foi possível elaborar um roteiro particular para os módulos do Sistema auditado.

Esta pequena quantidade de Auditorias de Sistemas é prejudicial à Administração Municipal, vez que a AUDIM, não realizando trabalhos nesta modalidade, deixa de examinar grande parte dos controles internos da PMBH que constituem importantes fontes de informações, tanto para os gestores públicos quanto para os munícipes. Além disso, a própria AUDIM utiliza informações provenientes desses sistemas informatizados que não são auditados, para a realização de seus trabalhos, o que pode comprometer o resultado de uma auditoria.

Não obstante, a AUDIM deixa de perseguir suas atribuições institucionais, principalmente, no tocante às atividades definidas no art. 1º do Decreto n. 8.565/96:

“Art. 1º -

- c) assistir e orientar a Administração Pública Municipal no âmbito das atribuições de auditoria;*
- e) examinar e opinar sobre quaisquer fontes de informações relacionadas com as atividades dos órgãos da Administração Pública Municipal;*
- i) determinar e opinar sobre a consistência e legitimidade das informações contábeis e demais dados oficiais da Administração Pública Municipal; “*

Neste sentido, a AUDIM, enquanto órgão responsável pela auditoria interna, deve proceder à avaliação dos sistemas informatizados da PMBH, objetivando assegurar, em última instância, a produção e utilização de dados e informações íntegras e oportunas.

Na análise das modalidades de auditorias executadas pela AUDIM não foram considerados os seguintes trabalhos:

- a)* visitas de retorno das auditorias realizadas;
- b)* programa de auditoria e fluxograma das atividades administrativas das entidades auditadas;
- c)* participação em eventos (cursos, congressos, palestras, etc.), seja como ouvinte ou como apresentador;
- d)* participação em Comissão de Estudos Técnicos e em Conselho Fiscal das Sociedades de Economia Mista;
- e)* manuais, a exemplo do *Manual de Prestação de Contas da Secretaria Municipal de Cultura*;
- f)* consultoria feita às entidades públicas através de pareceres ou ligação telefônica;
- g)* reuniões e visitas técnicas na AUDIM e nas entidades auditadas; e
- h)* visitas técnicas às entidades públicas.

Além dos relatórios elaborados, foram analisados os pareceres, manuais, programas de auditorias e o acervo da biblioteca da AUDIM. Nenhum material inerente à Auditoria de Sistemas Informatizados foi detectado.

8.8- Conclusão

Este capítulo consistiu de um Estudo de Caso que, além de caracterizar a AUDIM, proporcionou identificar as modalidades de auditoria realizadas pelo órgão, sobretudo os trabalhos desenvolvidos na modalidade de Auditoria de Sistemas.

O capítulo seguinte apresenta a descrição e a análise dos resultados obtidos através da pesquisa realizada junto ao Auditor-Chefe e aos Auditores Municipais.

9 APRESENTAÇÃO E DISCUSSÃO DOS RESULTADOS

9.1- Introdução

Este capítulo apresenta e analisa os resultados obtidos na pesquisa de campo, através da aplicação dos questionários (ANEXOS A e B), da pesquisa documental e da observação participante, a fim de responder ao terceiro objetivo específico desta pesquisa. Esse objetivo consistiu em identificar os fatores que inibem a AUDIM de realizar Auditoria nos Sistemas de Informações Computadorizados da PMBH.

O capítulo anterior baseou-se na pesquisa documental e na observação participante, buscando responder ao segundo objetivo específico da pesquisa, que consistiu em modelar a AUDIM. Este, complementando-o, apresenta-se através da análise de conteúdo e da análise estatística dos questionários respondidos pelos Auditores e pelo Auditor-Chefe da AUDIM.

As respostas dos questionários de cunho estatístico, foram apuradas através de tabulação eletrônica dos dados utilizando para tanto o *software Excel da Microsoft®*. Os números apurados foram então convertidos em pontos percentuais que originaram gráficos e tabelas, para efeito de melhor exposição, com as respectivas interpretações e conclusões dos fatos.

No entanto, as respostas dos questionários de cunho estatístico e de cunho qualitativo foram analisadas conjuntamente e permitiram o aprofundamento da interpretação acerca das características da população pesquisada, da avaliação da percepção dos auditores sobre os Sistemas de Informações da PMBH, sobre os trabalhos de auditoria da AUDIM e a capacitação técnica desses auditores em realizar Auditoria de Sistemas, que adiante serão expostas.

9.2- Características da População Pesquisada

A população investigada nesta pesquisa foi constituída pelos funcionários da AUDIM que realizam trabalhos de auditoria. Assim a população base do universo pesquisado foi composta por dezoito auditores e pelo Auditor-Chefe da AUDIM.

Como as informações solicitadas nos questionários inerentes ao tempo de serviço e à escolaridade dos auditores objetivaram somente a caracterização da população pesquisada, os nomes dos entrevistados não são citados.

Dos 19 questionários distribuídos, 16 foram devolvidos, sendo 1 do Auditor-Chefe e 15 dos auditores, o que representa um índice de retorno altamente relevante: 84,22% do total. Com a obtenção das informações constantes destes questionários, a população pesquisada ficou caracterizada como adiante relatado.

Dentre os quinze auditores que responderam ao questionário, somente um (5,56%) ocupa cargo comissionado, no caso o Gerente da GETA. Este fato justifica-se pelo recebimento da Gratificação de Desempenho de Auditoria, que é devida somente aos auditores no exercício de seu cargo efetivo ou no cargo comissionado de Gerente da GETA.

No período no qual os questionários foram respondidos, os 15 auditores já trabalhavam na AUDIM, em média, há seis anos e três meses, conforme demonstrado na TAB. 01.

TABELA 01- TEMPO DE SERVIÇO DOS AUDITORES NA AUDIM

AUDITOR	TEMPO TOTAL DE SERVIÇO NA AUDIM (EM ANOS)
A	7,4
B	4,4
C	5,6
D	7,2
E	6,7
F	7,5
G	7,3
H	6,7
I	4,2
J	5,5
L	7,6
M	7,4
N	7,3
O	2,9
P	6,9
MEDIA	6,3

FONTE- Elaboração da autora da dissertação a partir dos questionários aplicados.

Analisando o QUADRO 18, fica evidenciado que, apesar de a exigência acadêmica para ingressar no cargo de Auditor ser Bacharel em Ciências Contábeis com registro no Conselho Regional de Contabilidade, seis auditores são detentores de outras graduações, como Bacharelado em Direito, Bacharelado em Administração e Licenciatura Plena.

Não obstante, cinco auditores são pós-graduados em cursos de Especialização *Lato Sensu* e outros três auditores estão concluindo esta especialização. Verifica-se, ainda, que uma auditora é mestranda em Administração Pública.

Foi constatado também que essa qualificação é um pouco centrada, pois, dentre estes auditores, um possui duas graduações e uma especialização, outro possui uma graduação e duas especializações e uma auditora possui uma graduação, uma especialização *Lato Sensu* e cursa Mestrado.

QUADRO 18- ESCOLARIDADE DO CORPO TÉCNICO DE AUDITORES

AUDITOR	GRADUAÇÃO (ALÉM DO BACHARELADO EM CIÊNCIAS CONTÁBEIS)	PÓS-GRADUAÇÃO	
		LATO SENSU	STRICTO SENSU
A	Direito	-	-
B	-	Consultoria Contábil (em curso)	-
C	-	-	-
D	-	-	-
E	-	Finanças	-
F	Administração	Análises de Sistemas e Administração Municipal	-
G	-	Informática Pública	-
H	-	-	-
I	-	-	-
J	Administração	-	-
L	Licenciatura Plena (Contabilidade e Economia)	Administração Municipal	Mestrado em Administração Pública (Tecnologias da Informação) (em curso)
M	-	Auditoria Externa (em curso)	-
N	Licenciatura Plena (Contabilidade e Economia)	-	-
O	-	Auditoria Externa (em curso)	-
P	Administração e Licenciatura Plena em Contabilidade	Administração Financeira	-

FONTE- Elaboração da autora da dissertação a partir dos questionários aplicados.

O GRAF. 02 demonstra a distribuição dessa qualificação profissional extraordinária dos auditores em relação à exigência do cargo de auditor.

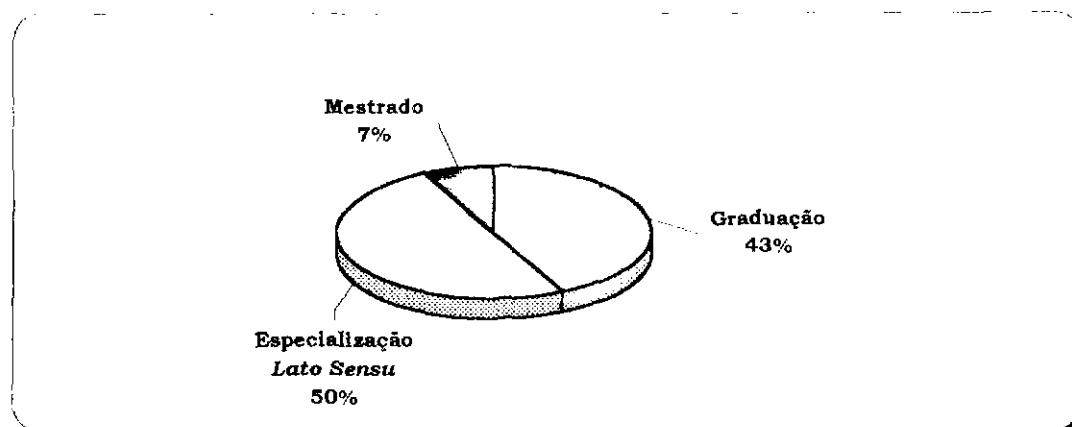


GRÁFICO 02- Distribuição da escolaridade excedente dos auditores em relação à exigida para o cargo em exercício

FONTE- Elaboração da autora da dissertação a partir dos questionários aplicados.

Para o exercício do cargo de Auditor-Chefe é indispensável a graduação em qualquer curso superior, sem haver necessidade do registro no Conselho ou Ordem da classe profissional. O atual Auditor-Chefe é Bacharel em Direito.

9.3- Percepção dos Auditores sobre os Sistemas de Informações da PMBH

Nesta primeira parte dos questionários, buscou-se verificar junto aos entrevistados a percepção destes sobre os Sistemas de Informações da PMBH.

Os conhecimentos dos auditores quanto aos Sistemas de Informações existentes na PMBH podem ser considerados insuficientes. Dentre os cento e trinta e três principais sistemas apresentados no capítulo 3, que têm por objetivo controlar e gerar informações estratégicas e fundamentais à tomada de decisões pelos gestores públicos municipais, somente dez foram mencionados por mais de um auditor, que neste caso é autora da dissertação. A TAB. 02 explicita esses dados.

**TABELA 02- SISTEMAS DE INFORMAÇÕES DA PMBH CITADOS PELOS
AUDITORES**

SISTEMA DE INFORMAÇÕES	QUANTITATIVO DE AUDITORES QUE CITARAM O SISTEMA
Sistema Integrado de Recursos Humanos	5
Sistema Orçamentário e Financeiro	4
Sistema de Arrecadação Municipal	2
Sistema de Controle do IPTU	2
Sistema de tributos Imobiliários	2
Sistema Integrado de Dívida Ativa	2
Sistema de Execuções Fiscais	2
Sistema de Tramitação de Processos	5
Sistema de Cadastro de Materiais	5
Sistema Único de Cadastro de Fornecedores	5
Demais Sistemas	1

FONTE- Elaboração da autora da dissertação a partir dos questionários aplicados.

De igual forma, o Auditor-Chefe fez alusão apenas a sete sistemas, todos já citados na TAB. 02.

Ressalta-se que, muitas vezes foram citados nomes de módulos integrantes dos sistemas em substituição ao nome desse sistema. Isso comprova o conhecimento somente de determinadas funções dos sistemas, como no caso do Sistema Integrado de Recursos Humanos, que foi citado simplesmente como Sistema de Folha de Pagamento. Na íntegra, este sistema engloba vinte e quatro módulos, dentre os quais citam-se o módulo de contagem de tempo de serviço, o módulo de perícia médica e o módulo de atividades correicionais.

Em outros casos foi citado o nome Rede Municipal de Informação, em lugar do nome correto que é Rede Municipal de Informática, e esta constitui uma rede de comunicação de dados e não um sistema de Informações.

Apesar do pouco conhecimento dos auditores em relação ao número de Sistemas de Informações Computadorizados da PMBH, estes profissionais acreditam que os

controles internos para um ambiente informatizado devem ser rigorosos, conforme apresentado no GRAF. 03.

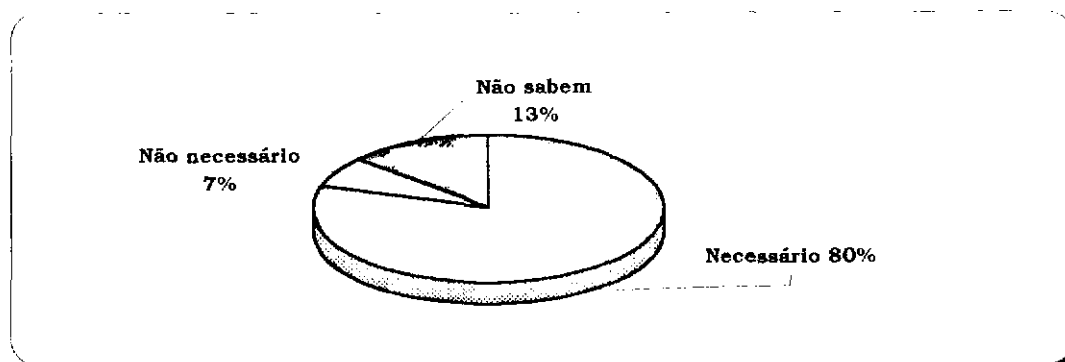


GRÁFICO 03- Entendimento dos auditores quanto à necessidade de controles internos rigorosos para um ambiente informatizado

FONTE- Elaboração da autora da dissertação a partir dos questionários aplicados.

Algumas das observações dos auditores acerca dessa necessidade de controle interno para ambientes informatizados foram reproduzidas:

"Independente de ser informatizado, qualquer sistema administrativo requer controle interno específico visando sua aderência aos objetivos a que se propõe considerando a fidedignidade e integridade dos procedimentos."

"Os controles internos conferem segurança e reduzem a probabilidade de falhas e fraudes."

"Controles internos rigorosos proporcionam sistemas informatizados seguros."

"As informações geradas por estes sistemas são aplicadas nas atividades operacionais da PMBH, o que enseja a veracidade destas."

"Sem o controle interno não existe consistência dos dados."

"A informatização, por si só, não garante a total confiabilidade das informações."

"Os dados contidos nos sistemas informatizados da Prefeitura são utilizados para a geração de informações que afetam significativamente a área financeira e também a parte processual das atividades municipais, por exemplo, geração de folha de pagamento, aquisição de serviços e materiais de fornecedores cadastrados."

"O ambiente informatizado só cumpre a sua finalidade se for baseado em informações seguras do ponto de vista da realidade e precisão. Esta situação somente pode ser obtida através de controles internos rigorosos."

"Porque nele estão contidas as informações estratégicas de cunho administrativo, financeiro e político que podem ser alterados através de um erro, uma pane ou até intencionalmente a fim de atender interesses próprios ou escusos."

"Os dados e informações fornecidos precisam ser seguros e confiáveis, pois vão embasar opiniões e decisões."

“Todos os sistemas devem ser reavaliados periodicamente para absorver as transformações tecnológicas e adaptações às novas exigências gerenciais.”

O Auditor-Chefe também concorda com essa necessidade de controles internos rigorosos para um ambiente informatizado. Ele ressalta que “todos os sistemas encerram informações econômicas e estratégicas relevantes”.

A evidência da necessidade de controles internos foi destacada no referencial teórico desta dissertação, onde a Auditoria de Sistemas foi mencionada como atividade específica de avaliação de um ambiente informatizado.

Quanto à percepção dos auditores se os Sistemas de Informações da PMBH são seguros e se as informações por eles geradas são confiáveis, verifica-se que a maioria dos respondentes, 60%, não sabem, porém, outros 40% acreditam que não são, como ilustrado no GRAF. 04.

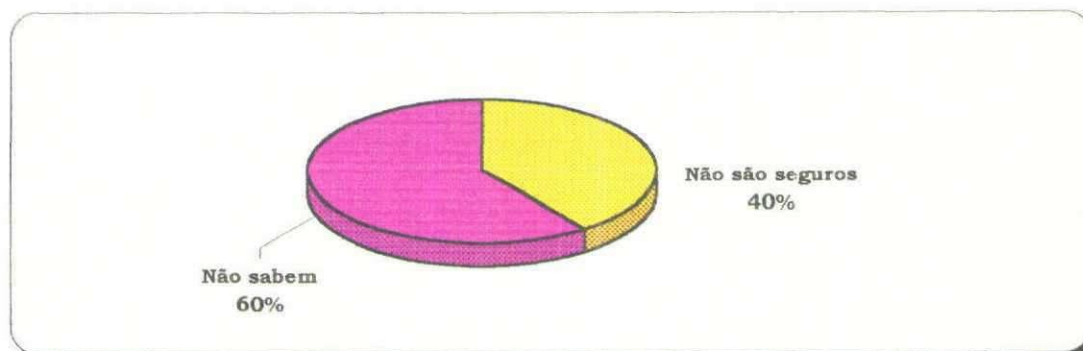


GRÁFICO 04- Percepção dos auditores se os sistemas informatizados da PMBH são seguros e se as informações por eles geradas são confiáveis

FONTE- Elaboração da autora da dissertação a partir dos questionários aplicados.

Determinados enxertos das justificativas apresentadas estão transcritos a seguir:

“Não sei. Em geral os sistemas em uso na PBH, não são objeto de auditoria específica.”

“Não sei. Diante da não realização de auditorias nos sistemas da Prefeitura de Belo Horizonte, não tenho como afirmar se estas informações são confiáveis e seguras.”

“Não sei. Não participei do desenvolvimento e implantação destes e desta forma não tenho competência para avaliá-los”.

“Não sei. Não tenho uma base segura para emitir essa opinião”

“Não sei. Em auditorias realizadas em folhas, pude notar problemas de processamento.”

“Não. O OPUS é um exemplo de sistema com dados desatualizados”.

“Não. Muitos programas possuem informações defasadas.”

“Não. Esses sistemas informatizados garantem a agilidade das informações, mas 100% de confiabilidade está longe de garantir.”

“Não. Existem muitas falhas já detectadas em diversos sistemas informatizados da PMBH. Algumas delas até bem primárias, como soma aritmética.”

“Não. O sistema por mim auditado apresentou diversas falha de autenticidade, consistência e integridade de dados. Além disso, quando do cruzamento das informações processadas pelos sistemas da PMBH e dos seus documentos- fonte várias divergências são detectadas”.

“Não. Porque às vezes os dados não foram atualizados ou não existem.”

Diante de tais explicações, aliadas à observação participante pode-se concluir que os Sistemas de Informações da PMBH não são seguros e que suas informações não confiáveis, visto a constatação de erros ou falhas nesses sistemas.

O Auditor-Chefe entende que esses sistemas são seguros e que suas informações confiáveis. Ele expõe que “sob a ótica do usuário é essa impressão que transparece”.

Da mesma forma que o Auditor-Chefe tem esse entendimento, outros gestores municipais podem ter a mesma percepção, vez que utilizam constantemente informações geradas por estes sistemas.

9.4- Percepção dos Auditores sobre os Trabalhos de Auditoria

Nesse segundo módulo do questionário, procurou-se conhecer a percepção dos auditores e do Auditor-Chefe sobre os trabalhos de auditoria, ou seja, acerca da utilização de informações geradas pelos Sistemas de Informações da PMBH nos trabalhos da AUDIM e do uso de manuais, programas e técnicas de Auditoria de Sistemas .

Durante o período de 1994 a 2001, somente uma auditora realizou trabalho de Auditoria de Sistemas para a AUDIM. Este número está evidenciado na TAB. 03.

**TABELA 03- QUANTITATIVO DE AUDITORES QUE REALIZARAM
AUDITORIA DE SISTEMAS PARA A AUDIM.**

RESPOSTAS DOS AUDITORES QUANTO AO QUANTITATIVO DE TRABALHOS DE AUDITORIA DE SISTEMAS REALIZADOS POR ELES PARA A AUDIM	QUANTITATIVO DE AUDITORES	
	ABSOLUTO	RELATIVO
Um	1	6,67
Nenhum	14	93,33
TOTAL	15	100,00

FONTE- Elaboração da autora da dissertação a partir dos questionários aplicados.

Como apresentado no capítulo 8, além desse único trabalho de Auditoria de Sistemas realizado por uma auditora no Sistema Integrado de Recursos Humanos, no caso a autora dessa dissertação, outros dois trabalhos foram realizados por antigos funcionários da AGM. Conclui-se, que é insignificante o quantitativo de trabalhos realizados pela AUDIM na modalidade de Auditoria de Sistemas, vez que durante seus quinze anos de existência somente três trabalhos foram efetuados, sendo apenas um desempenhado por auditor de cargo efetivo.

Dessa forma, fica a maioria dos cento e trinta três principais Sistemas de Informações Computadorizados da PMBH sem ser avaliada, deixando a AUDIM de examinar grande parte dos controles internos do Município, que constituem importantes fontes de informações, tanto para os gestores públicos quanto para os cidadãos.

Com isso, a AUDIM deixa de perseguir suas atribuições institucionais no tocante às atividades definidas no art. 1º do Decreto nº 8.565/96, que consistem em :

"Art. 1º -

c) assistir e orientar a Administração Pública Municipal no âmbito das atribuições de auditoria;

.....
e) examinar e opinar sobre quaisquer fontes de informações relacionadas com as atividades dos órgãos da Administração Pública Municipal;

i) determinar e opinar sobre a consistência e legitimidade das informações contábeis e demais dados oficiais da Administração Pública Municipal; “

Observando o GRAF. 05, verifica-se que a maioria dos auditores entende que a utilização de informações provenientes de Sistemas de Informações que não foram auditados podem comprometer a qualidade e/ou o resultados dos trabalhos de Auditoria.

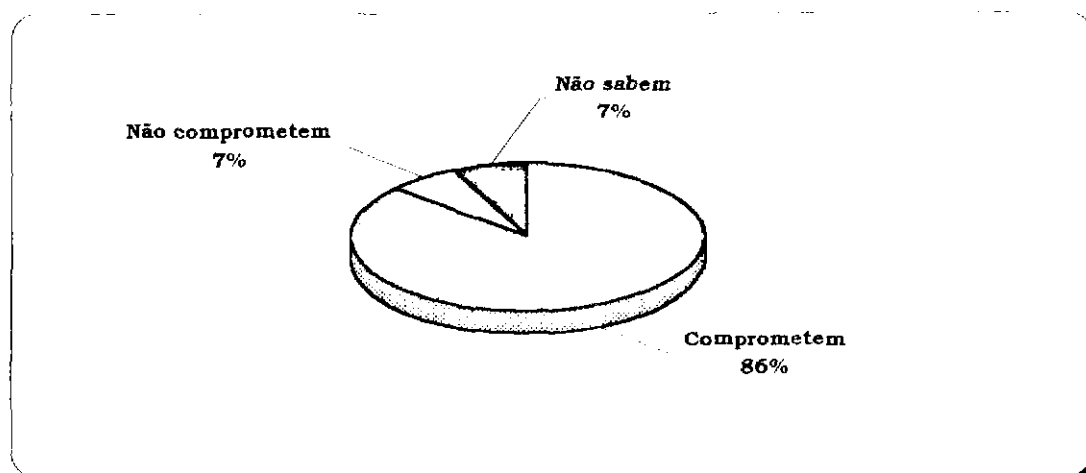


GRÁFICO 05- Comprometimento da qualidade e resultado de um trabalho de auditoria decorrente da utilização de informações provenientes dos sistemas informatizados da PMBH que não foram auditados

FONTE- Elaboração da autora da dissertação a partir dos questionários aplicados.

Esses profissionais apresentam considerações sobre essa utilização de informações:

"Não podemos trabalhar com informações incorretas e/ou desatualizadas, visto que isto torna o relatório de auditoria inócuo e sem crédito."

"Se nos baseamos em informações incorretas provenientes dos sistemas informatizados, os trabalhos de Auditoria, com certeza, ficam prejudicados."

"Se os trabalhos de auditoria foram realizados utilizando informações geradas por estes sistemas sem nenhum confronto com outros dados que comprovem a

veracidade, estes podem apresentar resultados distorcidos que não refletem a realidade."

"A informatização não garante 100% de autenticidade das informações."

"Grande parte dos nossos trabalhos são baseados nos dados provenientes dos sistemas existentes na Prefeitura de Belo Horizonte, portanto, se as informações não forem confiáveis podem alterar substancialmente os resultados dos nossos trabalhos".

"Muitas vezes a base da Informação para análise da auditoria é originada de sistemas informatizados, que se não forem revisados ou avaliados podem gerar informações inverídicas."

"Os resultados podem não ser os reais."

"Porque como disse anteriormente as informações podem estar erradas, danificadas ou até mesmo manipuladas."

"Considerando-se que há o risco do auditor formar sua opinião com base em informações cuja consistência do sistema gerador não tenha sido atestada, ou seja, pode haver erro."

"Acredito que faltará a necessária consistência no resultado final do trabalho."

O Auditor-Chefe também crê que o uso dessas informações pode comprometer os trabalhos da AUDIM, na medida em que contenham inconsistências.

Apesar de entenderem que empregar informações oriundas de sistemas não auditados pode ser arriscado, a maioria dos auditores as utilizam, conforme o GRAF. 06.

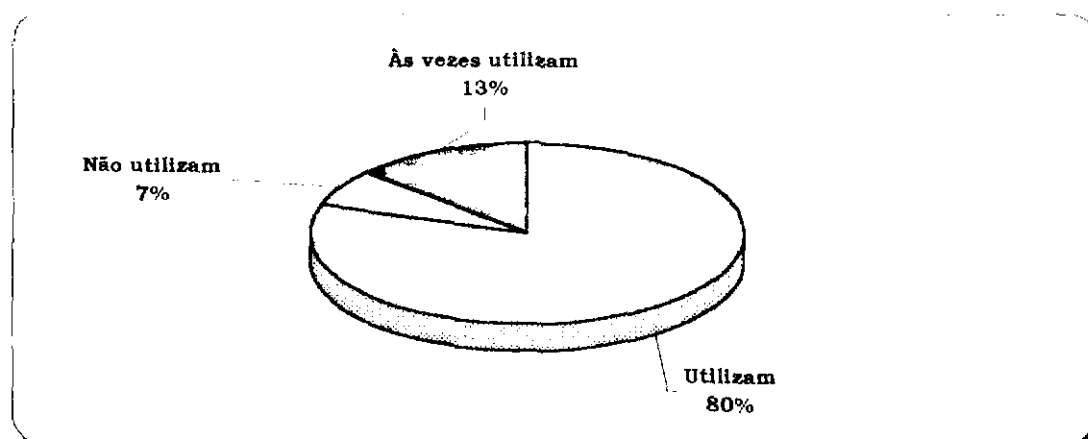


GRÁFICO 06- Utilização pelos auditores de informações provenientes dos Sistemas Informatizados da PMBH para a realização dos seus trabalhos de auditoria

FONTE- Elaboração da autora da dissertação a partir dos questionários aplicados.

Os auditores justificam o uso dessas informações:

“Existem sistemas que se mostram confiáveis proporcionando agilidade nos trabalhos de auditoria.”

“Dependendo do trabalho, utilizo o OPUS. Em um caso específico, solicitei relatório sobre as atividades prestadas na Central de Atendimento da SCOMGER-N, a PRODABEL.”

“Constantemente faço pesquisas no sistema OPUS e às vezes no Orçamentário.”

“Os inventários (almoxarifado e material), os Balanços e as Demonstrações contábeis são peças geradas pelo sistema, sendo utilizadas pelo auditor para execução do seu trabalho.”

“Vários trabalhos de auditoria, em diversas áreas, exigem informações advindas de sistemas informatizados.”

“Principalmente, os trabalhos relacionados à área de recursos humanos, controle de estoque, compras e licitações.”

“Sempre que necessário, a auditoria deve recorrer a dados dos sistemas informatizados.”

“Hoje a informação é utilizada ampla escala, não é diferente na PMBH.”

“No entanto aplico testes para aferir a veracidade destas informações, haja vista que atuo na área contábil e os relatórios é que norteiam o meu trabalho.”

“Para conhecimento do volume de operações e cálculo de amostra a ser objeto de exame auditorial.”

“Para agilizar o trabalho, mas com uma certa cautela porque não sei se os dados são confiáveis.”

“Quase todo os trabalhos, independente em que área estejam inseridos, ou seja, se é patrimonial, contábil, licitação, pessoal, sempre são utilizadas informações geradas pelos sistemas de Informações da PMBH, seja de forma direta ou indireta.”

“Às vezes. Quando auditamos os Balanços, necessitamos de suportes informatizados para o cruzamento de informações com o patrimônio, os estoques ou inventários, etc.”

O Auditor-Chefe considera que estes dados e informações provenientes dos Sistemas de Informações são valiosas ferramentas para a AUDIM.

Com a utilização dessas informações a AUDIM fica sujeita não só ao comprometimento do resultado de seus trabalhos, mas até a um descrédito perante o Município, vez que sendo um órgão técnico dotado de autonomia funcional que planeja e exerce suas atividades, esta vem utilizando dados oriundos de fontes que não foram auditadas, cuja auditoria deveria ser efetuada pela própria AUDIM.

A maioria dos auditores também considera a Auditoria de Sistemas muito importante para a qualidade e segurança dos Sistemas de Informações da PMBH, como evidenciado adiante no GRAF. 07 .

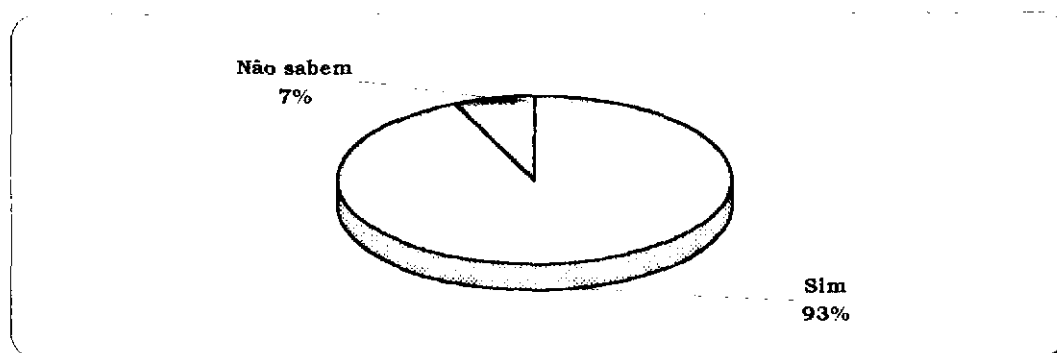


GRÁFICO 07- Percepção dos auditores se a Auditoria de Sistemas é um instrumento importante para a qualidade e segurança dos sistemas de Informações

FONTE- Elaboração da autora da dissertação a partir dos questionários aplicados.

Esta percepção é fundamentada em determinadas explicações dos auditores:

"Permite diagnosticar eventuais desvios relacionados com o desempenho, a vulnerabilidade, acessibilidade e a aplicabilidade."

"Os dados tornam-se muito mais confiáveis e as fraudes e/ou falhas passam a ser facilmente identificadas."

"Se os sistemas de Informações forem constantemente auditados, a margem de erros dos mesmos ficará cada vez menor."

"A funcionalidade do sistema é medida por estes elementos, sem os quais torna-se virtual."

"A auditoria sistêmica atesta maior segurança e qualidade dos sistemas sugerindo se for o caso aprimoramentos."

"Toda auditoria é importante para a validação de informações, inclusive as provenientes dos sistemas informatizados."

"Porque através da realização de auditoria de sistemas é que serão avaliados os aspectos de segurança, consistência e integridade dos dados gerados e armazenados nos bancos de dados informatizados."

"Verifica a veracidade das informações colocadas à disposição das pessoas, demonstrando a sua confiabilidade".

"Assim como qualquer máquina ou equipamento necessita de manutenção constante, os sistemas de Informações necessitam de revisões periódicas".

"Contribui para uma maior confiabilidade das informações recebidas."

"Tendo em vista que a atividade de Auditoria tem, em última instância, o objetivo de aferir o nível de eficácia, eficiência e economicidade das ações implementadas pela entidade, a qualidade e segurança dos sistemas de Informações amplamente utilizados num mundo globalizado, inserem-se perfeitamente."

"Proporciona uma boa qualidade e resultado ao trabalho."

"É o instrumento adequado para verificar a eficiência, eficácia e economia do sistema, bem como suas condições de segurança. Assim, com a realização dessa modalidade de auditoria um sistema poderá ter sua qualidade maximizada e sua segurança reforçada."

O Auditor-Chefe julga que esta modalidade de auditoria é importante para a qualidade e segurança dos Sistemas de Informações, principalmente por conferir confiabilidade às informações extraídas.

O estudo da literatura referida nesta dissertação demonstra a importância da Auditoria de Sistemas, vez que esta atividade avalia os Sistemas de Informações Computadorizados e o ambiente computacional, a fim de identificar e analisar os possíveis riscos que estejam ocorrendo, ou que possam ocorrer. Além disso, ela proporciona recomendar medidas saneadoras e melhoria dos controles internos para a diminuição dos riscos levantados.

Não obstante a consideração da importância da Auditoria de Sistemas, somente 13% dos auditores já utilizaram manuais, programas e técnicas próprias desta modalidade de auditoria. O GRAF. 08 apresenta esses dados.

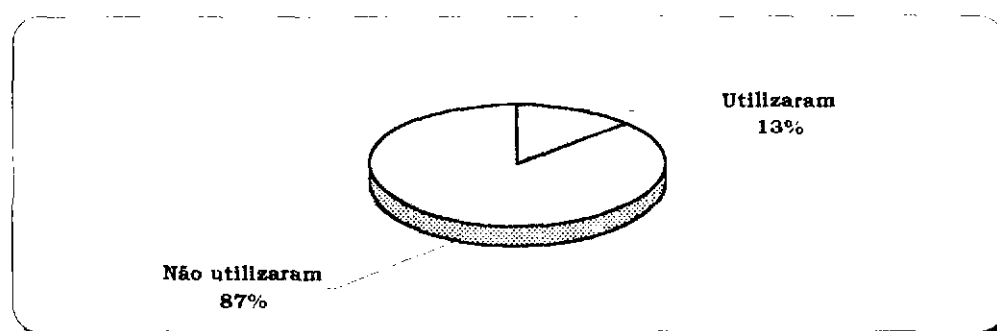


GRÁFICO 08- Utilização pelos auditores de manuais, programas e técnicas próprias de auditoria de sistemas

FONTE- Elaboração da autora da dissertação a partir dos questionários aplicados.

Esses auditores discorrem sobre essa utilização:

"Utilizei devido ao exercício de auditoria de sistemas na PRODABEL."

"Devido à elaboração da minha dissertação de mestrado estudei diversas obras acerca do tema Auditoria de Sistemas, dentre eles o Manual de auditoria de Sistemas do ICU. Além disso, para a realização de uma auditoria para a AUDIM, criei um roteiro próprio e adequado para o sistema que analisei".

Apesar de a AUDIM não manter manuais, programas nem técnicas de Auditoria de Sistemas, o Auditor-Chefe discorre que “considerando a relevância e inserção da informática na Administração Municipal, estamos programando avançar neste sentido”.

Foi contextualizado para os auditores que a PMBH vem implementando Sistemas Informatizados para controlar e gerar informações necessárias à tomada de decisões dos gestores municipais. Diante deste fato, foi indagado aos auditores o que a AUDIM, como órgão de controle interno, vem promovendo para que os gestores utilizem informações confiáveis e oportunas produzidas por esta tecnologia. Dois pontos de vista centraram as explicações dos auditores: o primeiro é o aqueles auditores que não têm conhecimento de qualquer implementação da AUDIM; segundo, daqueles auditores que apontam o investimento da AUDIM em especializar um dos auditores para a área de Auditoria de Sistemas. Os comentários adiante reproduzidos evidenciam essas respostas.

“Não sei.”

“Inicialmente, vem buscando familiarizar o corpo de auditores com os sistemas informatizados disponíveis com a ampliação dos recursos de informática, treinamento e conhecimento prático dos sistemas.”

“Pelo que tenho conhecimento, está preparando um de seus auditores para atuar na Auditoria de Sistemas e garantir maior confiabilidade das informações.”

“Atualmente, auditores especializados na área de sistemas estão sendo encaminhados para a realização do trabalho..”

“Não sei”

“Esta atuação em auditoria de sistemas está em fase embrionária na AUDIM e é óbvio que tudo que for feito para fomentar o processo é importantíssima e de grande utilidade.”

“Até o momento foi realizada apenas uma auditoria no sistema de folha de pagamento da Prefeitura de Belo Horizonte”.

“Essa informação não chegou ao meu conhecimento até o presente momento.”

“A AUDIM na medida do possível esta apoiando a iniciativa dos auditores em reciclar na área de auditoria de sistemas em parceria com a PRODABEL ou outras entidades.”

“Não sei”.

“Não tenho conhecimento do planejamento ou implemento de nenhuma ação de curto prazo. Não obstante, a médio e longo prazo, acredito que a capacitação de auditores em área específica possibilitará o planejamento e a auditoria dos sistemas de Informações de modo a propiciar aos gestores municipais a utilização de informações nos termos questionados.”

“Apoiando a iniciativa de uma auditora em analisar o Sistema Integrado de Recursos Humanos, e ainda, liberando parcialmente do horário de trabalho dois auditores para a conclusão de curso de especialização em Informática Pública e Mestrado em Tecnologias da Informação.”

“Se existe esta iniciativa da AUDIM eu não conheço.”

“Do meu conhecimento não existe nada a respeito.”

O Auditor-Chefe reconhece que a única medida adotada é a capacitação de auditores para a área de Auditoria de Sistemas.

Quando do questionamento ao Auditor-Chefe sobre a existência de algum planejamento para inserir ou ampliar a realização de Auditoria de Sistemas pela AUDIM, este relaciona medidas como a intenção de capacitar auditores e adquirir ferramentas, manuais, programas e técnicas de Auditoria de Sistemas. Contudo, não existe a previsão das implementações destas medidas.

Verificou-se, ainda, junto ao Auditor-Chefe, que a AUDIM não mantém nenhuma articulação ou contato com auditorias internas de outros órgãos governamentais que já realizam Auditoria de Sistemas.

9.5- Capacitação dos Auditores Municipais

Nesse último módulo do questionário, procurou-se evidenciar a capacitação dos auditores em relação à atividade de Auditoria de Sistemas.

A maioria dos auditores não se considera capacitada para realizar Auditoria de Sistemas, conforme destacado no GRAF. 09.

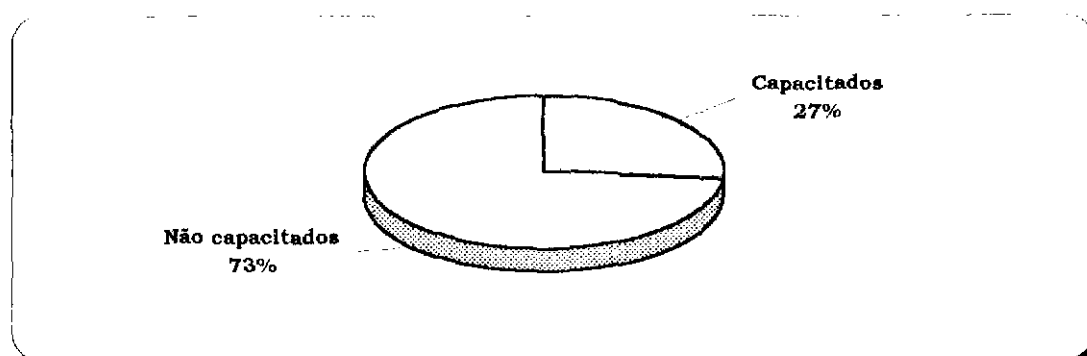


GRÁFICO 09- Consideração dos auditores acerca de serem profissionais capacitados para desenvolver Auditoria de Sistemas

FONTE- Elaboração da autora da dissertação a partir dos questionários aplicados.

Os auditores que se consideram aptos para a realização desta modalidade de auditoria justificam-se com os seguintes pronunciamentos:

"Experiência anterior na PRODABEL."

"Sou pós-graduado em análise de sistemas. É óbvio que um treinamento voltado para esse tipo de auditoria específica, seria imprescindível no início dos trabalhos. Conhecer mais profundamente os sistemas da PMBH seria fundamental."

"Tenho curso de especialização em Informática Pública, onde foram apresentados princípios de segurança de sistemas e que são utilizados na execução de auditoria de sistemas."

"No mestrado cursei diversas matérias relacionadas diretamente à Auditoria de Sistemas: linguagens de programação, sistemas de computação, rede de computadores, banco de dados, engenharia de software, sistemas de Informações, tecnologia www e bibliotecas digitais. Dentre tais disciplinas, desenvolvi monografias voltadas para a auditoria de sistemas, além desta dissertação de mestrado específica sobre o tema. Além disso, realizei auditoria em um dos sistemas de Informações da PMBH, para o qual criei roteiro próprio de auditoria. Não obstante participei de convenções e seminários que abordaram o tema."

Apesar de a maioria dos auditores não estar apta para realizar Auditoria de Sistemas, nunca foi efetuado treinamento relacionado ao tema afeto com recursos próprios da AUDIM, como adiante explicitado na TAB.04.

TABELA 04- TREINAMENTOS OFERECIDOS PELA AUDIM E QUANTITATIVO DE AUDITORES PARTICIPANTES

TREINAMENTO	QUANTITATIVO DE AUDITORES PARTICIPANTES	
	ABSOLUTO	RELATIVO
AUDITORIA DE SISTEMAS	0	0,00
OUTRAS ÁREAS	15	100,00
TOTAL	15	100,00

FONTE- Elaboração da autora da dissertação a partir dos questionários aplicados.

Com base nessa distribuição de treinamentos, conclui-se que a AUDIM não investe seus recursos disponíveis nesta modalidade de auditoria. Já em outras áreas há o investimento do órgão, como nos cursos sobre Auditoria no setor público, Licitações e Contratos, Informática (DOS, Word, Excel, Windows), Gestão Orçamentária, Técnicas de elaboração de papéis de trabalho, ISSQN, Contabilidade Pública e Qualificação na Lei de Responsabilidade Fiscal.

Ressalta-se que os cursos de pós-graduação em Informática Pública e mestrado em Administração Pública, foram custeados com recursos da PRODABEL, e não da AUDIM.

Apesar da falta de investimento em treinamentos com recursos próprios da AUDIM para assuntos relativos a Auditoria de Sistema, dois auditores tomaram a iniciativa de ingressar nessa área. O GRAF. 10 demonstra essa afirmação.

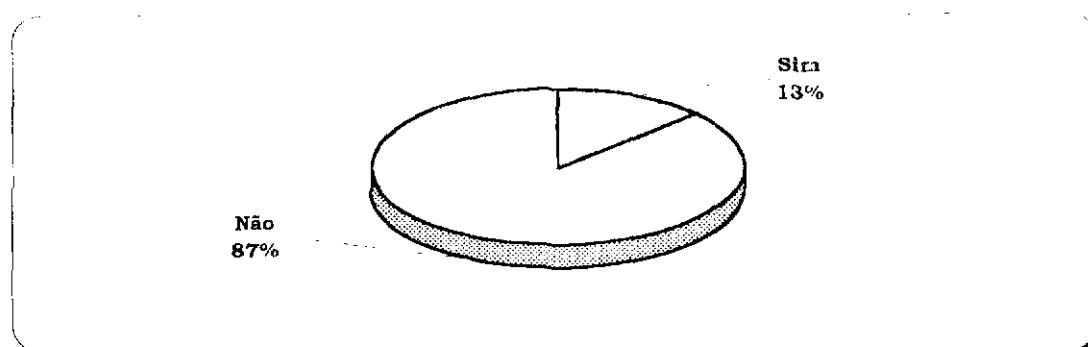


GRÁFICO 10- Iniciativa dos auditores em ingressar na área de Auditoria de sistema

FONTE- Elaboração da autora da dissertação a partir dos questionários aplicados.

A iniciativa destes auditores consistiu em participar de cursos de Especialização em Informática Pública e Mestrado em Administração Pública/Tecnologias da Informação e solicitação em realizar uma Auditoria de Sistema para AUDIM. Ressalta-se que houve o apoio da AUDIM a estes auditores com a indicação para a realização dos cursos, com a liberação do horário parcial de trabalho para assistirem às aulas e, ainda, a anuência para a realização da Auditoria no Sistema Integrado de Recursos Humanos da PMBH.

O interesse dos auditores pelo tema Auditoria de Sistemas foi considerado ínfimo, vez que somente 14% desses profissionais efetuaram leitura nos últimos doze meses de material referente ao assunto, conforme apresentado no GRAF. 11.

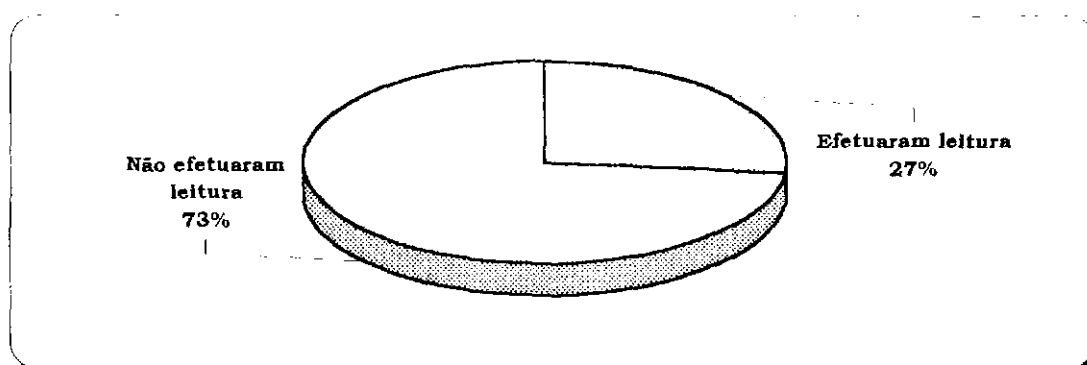


GRÁFICO 11- Leitura dos auditores de acervo bibliográfico referente ao tema Auditoria de Sistema

FONTE- Elaboração da autora da dissertação a partir dos questionários aplicados.

Além disso, dentre os 15 auditores, 13 não souberam afirmar se o acervo bibliográfico da AUDIM conta com alguma publicação sobre o tema Auditoria de Sistemas, conforme explicitado no GRAF. 12.

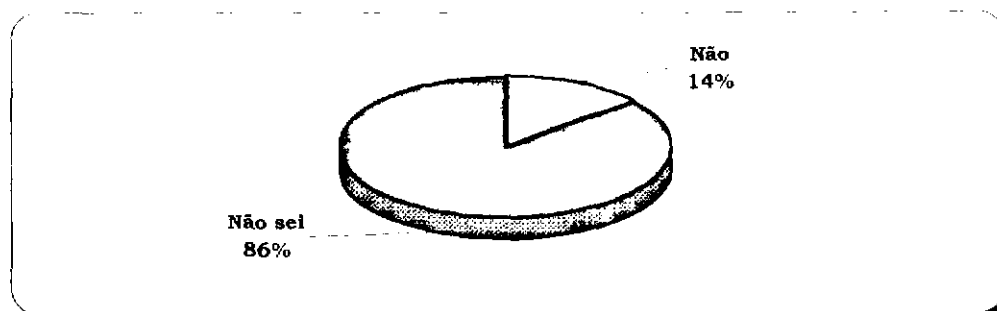


GRÁFICO 12- Percepção dos auditores sobre a existência de publicações referente ao tema Auditoria de Sistema no acervo bibliográfico da AUDIM

FONTE- Elaboração da autora da dissertação a partir dos questionários aplicados.

Tal fato demonstra que a maioria dos auditores não teve demanda para esta matéria, vez que se houvesse tal interesse saberiam precisar a existência ou não destas publicações. O Auditor-Chefe tem consciência da carência do acervo em relação à Auditoria de Sistemas.

9.6- Conclusão

Este capítulo, desenvolvido através da perspectiva dos entrevistados, preocupou-se em atender ao terceiro objetivo específico desta dissertação: a identificação dos fatores que inibem a AUDIM de realizar Auditoria nos Sistemas de Informações Computadorizados da PMBH.

Não obstante a consciência dos auditores e do Auditor-Chefe de que Auditoria de Sistemas constitui um instrumento muito importante para a qualidade e segurança dos Sistemas de Informações da PMBH e de que estes sistemas não são seguros nem suas informações não confiáveis, pode-se constatar que vários fatores servem como empecilhos para que a AUDIM não realize essa modalidade de auditoria.

Os fatores que se destacaram foram: pouco conhecimento dos auditores em relação aos *Sistemas de Informações da PMBH*; número restrito de auditores que já realizaram Auditoria de Sistemas e utilizaram manuais e técnicas próprias desta modalidade de auditoria; falta de implementação de medidas pela AUDIM, como elaboração ou aquisição de **Programas de Auditoria**, roteiros e técnicas de Auditoria de Sistemas; articulação ou contato com auditorias internas de outros órgãos governamentais que já realizam Auditoria de Sistemas; investimento em treinamentos com recursos próprios da AUDIM para assuntos relativos à Auditoria de Sistema; pouca iniciativa tanto da AUDIM como dos auditores em ingressar nessa modalidade de auditoria; e desinteresse da maioria dos auditores pelo tema Auditoria de Sistemas

Pode-se perceber que algumas das questões discutidas neste capítulo também foram abordadas no capítulo 8 desta dissertação

No próximo capítulo, apresenta-se o **Modelo de Auditoria de Sistemas** construído e proposto para a adoção pela AUDIM.

10 MODELO DE AUDITORIA DE SISTEMAS

10.1- Introdução

Neste capítulo é apresentada uma proposta de Modelo de Auditoria de Sistemas para a AUDIM, a fim de atender ao objetivo geral desta pesquisa.

Como citado na seção 6.5, o uso de modelos tem por objetivos simular, simplificar, tornar mais claros e concisos os processos, situações, operações, atividades e sistemas. Servem, também, como orientadores de procedimentos para determinadas situações ou problemas. Conforme a necessidade de informações, utiliza-se o tipo de modelo que for mais apropriado.

Em auditoria, utilizam-se modelos para descrever sistemas administrativos, objetivando uma compreensão mais rápida e perfeita do funcionamento de sistemas complexos.

Para desempenhar uma auditoria adequada é indispensável que o auditor saiba qual o objetivo da auditoria a ser realizada e quais os procedimentos a serem adotados para a concretização dos seus trabalhos. Para alcançar isto, é necessária a preparação de descrições narrativas através de um **Programa de Auditoria** detalhado que contenha informações sobre o objeto e o escopo da auditoria a ser executada.

O Programa de Auditoria por ser um roteiro dirigido e objeto da atenção do auditor, indica passo a passo os procedimentos a serem aplicados pelo mesmo em cada fase da operação, buscando garantir um alto nível de qualidade nos trabalhos, padronizando procedimentos e dirigindo de maneira eficiente o trabalho do auditor, independentemente do grau de afinidade que tenha com a área.

Além disso, o Programa de Auditoria quando corretamente estruturado, serve não só como instrumento eficaz para o trabalho do auditor mas, também, para a supervisão e o treinamento.

Em termos de custo/benefício, o Programa de Auditoria se torna um instrumento essencial para a otimização das horas disponíveis para controle, possibilitando um maior rendimento de cada auditor.

Dessa forma, o Programa de Auditoria objetiva estabelecer um plano de ação ordenado para o auditor, dirigindo a execução dos seus trabalhos, proporcionando uma *visão antecipada dos exames a serem efetuados e otimizando os tempos de execução da auditoria.*

O Modelo de Auditoria de Sistemas aqui apresentado, constitui-se de um **Programa de Auditoria**, construído a partir do referencial teórico apresentado nos capítulos 4, 6 e 7 desta dissertação.

Além de usufruir da formatação técnica disposta na seção 6.5, o que permitiu que fosse estruturado de forma modular e detalhada, o modelo procurou agrupar os pontos fundamentais das áreas de controles da Auditoria de Sistemas evidenciadas por vários autores [DIAS (2000), ARIMA (1994), MOELLER (1989), TCU (1998), BURCH (1978), CHAMBERS (1981) e PORTER (1981)] apresentadas no capítulo 7.

O modelo, ainda, integra os principais elementos referentes à Segurança dos Sistemas de Informação destacados no capítulo 4, propostos por diversos autores [LEMOES (1995), MOELLER (1989), PLEEGER (1996), DIAS (2000), GIL (1998), LAUDON & LAUDON (2000) e IMONIANA (1994)].

Ressalta-se que, apesar do modelo proposto ter sido criado com o intuito de ser adotado pela AUDIM, tal modelo pode ser utilizado por quaisquer organizações

públicas, bem como, privadas. Na seção seguinte apresenta-se o modelo de **Programa de Auditoria de Sistemas**.

10.2- Programa de Auditoria de Sistemas

Este **Programa de Auditoria** indica as áreas de controle de uma Auditoria de Sistemas e o objetivo que devem ser alcançados através da execução das suas instruções. Isto, propicia ao auditor um nível mínimo de informações que permite avaliar, desde logo, a importância e a complexidade da área auditada e, portanto, os controles que deverão ser examinados. O Programa de Auditoria de Sistemas foi estruturado conforme apresentado no QUADRO 19.

QUADRO 19- PARTES INTEGRANTES DO PROGRAMA DE AUDITORIA DE SISTEMAS

PARTE	ÁREA DE CONTROLE
1	Controles Gerais
2	<i>Softwares</i> Aplicativos
3	Desenvolvimento de Sistemas
4	Banco de Dados
5	Redes de Computadores
6	Microcomputadores

FONTE- Elaborado pela autora da dissertação.

A **Parte 1** do Programa de Auditoria de Sistemas, refere-se aos **Controles Gerais**, antes citados na seção 7.5.1. Os Controles Gerais consistem na estrutura organizacional, nas políticas e nos procedimentos que se aplicam às operações dos Sistemas de Informações Computadorizados de uma organização e na segurança destes sistemas.

A etapa de avaliação dos Controles Gerais contemplada no QUADRO 20 refere-se aos **Controles Organizacionais**. Por suas características mais genéricas e administrativas, estes controles são o ponto de partida para a realização de uma Auditoria de Sistemas.

Assim, as instruções do Programa de Auditoria visam: verificar a implementação de políticas e procedimentos relacionados à área de informática e sua divulgação na organização; adequar a distribuição das responsabilidades entre os funcionários da área de informática; observar o princípio da segregação de função; efetivar treinamento dos funcionários para utilização dos sistemas; e definir critérios para contratação de prestadores de serviços.

QUADRO 20- PARTE 1 DO PROGRAMA DE AUDITORIA DE SISTEMAS: CONTROLES GERAIS/CONTROLES ADMINISTRATIVOS

PROGRAMA DE AUDITORIA DE SISTEMAS	
ÁREA: CONTROLES GERAIS/ CONTROLES ORGANIZACIONAIS	
OBJETIVO: verificação quanto à: definição e implementação de políticas e procedimentos relacionados à área de informática e sua divulgação na organização; adequação da distribuição das responsabilidades entre os funcionários da área de informática; observância do princípio da segregação de função; efetivação do treinamento dos funcionários para utilização dos sistemas e o critério para contratação de prestadores de serviços da área de informática.	
INSTRUÇÕES DO PROGRAMA	
Verificar se:	
1) Foram estabelecidas, documentadas formalmente, aplicadas e divulgadas, a todos os funcionários, as políticas e os procedimentos de informática da organização.	
2) Foram definidas e divulgadas as responsabilidades de cada funcionário usuário dos sistemas de informações da organização auditada, e são compatíveis com suas reais habilidades e capacitação técnica.	
3) Existe segregação das funções entre os funcionários envolvidos na área de informática.	
4) Existe um programa de treinamento de pessoal para a utilização de cada sistema de informações.	
5) Existem funcionários que centralizam e monopolizam atividades e informações, cuja ausência deixaria a rotina da utilização dos sistemas de informações comprometida.	
6) Quando da contratação dos serviços de informática, existem critérios pré-determinados para triagem, treinamento, acompanhamento e cancelamento de prestadores de serviços.	
7) Os instrumentos contratuais firmados com os prestadores de serviços estipulam cláusulas que protejam a organização de possíveis fraudes por eles cometidas.	

FONTE- Elaborado pela autora da dissertação.

A segunda etapa integrante dos Controles Gerais, refere-se à **Política de Segurança**. A Política de Segurança da organização, como já discorrido no capítulo 4, inclui todas as medidas de proteção dos recursos computacionais e das informações por eles processadas. As instruções detalhadas no QUADRO 21, têm por objetivo verificar se a organização adota as medidas referentes à Segurança Legal, Administrativa, Física, e Lógica dos Sistemas de Informações.

QUADRO 21- PARTE 1 DO PROGRAMA DE AUDITORIA DE SISTEMAS: CONTROLES GERAIS/POLÍTICA DE SEGURANÇA

PROGRAMA DE AUDITORIA DE SISTEMAS
ÁREA: CONTROLES GERAIS/ POLÍTICA DE SEGURANÇA
OBJETIVO: verificação quanto à Segurança Legal, Administrativa, Física, e Lógica dos Sistemas de Informações.
INSTRUÇÕES DO PROGRAMA
Verificar se: 1) Existem políticas de segurança definidas e formalmente documentadas pela organização. 2) As políticas de segurança da organização instituem as responsabilidades dos usuários e do administrador de segurança. 3) As atividades desenvolvidas pelo administrador de segurança estão em conformidade com as políticas de segurança definidas pela organização. 4) A política de segurança dos sistemas de informações foi difundida entre as pessoas que trabalham nesta área, deixando-as conscientes da importância desta atividade para a organização. 5) A política de segurança dos sistemas de informações define formal e claramente as restrições de acesso aos computadores da organização. 6) Os locais de acesso aos computadores contam com dispositivos de segurança física suficientes para coibir a utilização dos recursos computacionais por pessoas não autorizadas. 7) As listagens das pessoas autorizadas a ingressar nos locais de acesso aos computadores são atualizadas e revisadas frequentemente. 8) Existe alguma rotina de vigilância ou instrumento de alarme para coibir o acesso não autorizado de pessoas aos computadores da organização fora do horário regular de trabalho. 9) São apropriadas as rotinas instituídas pela organização para identificar e acompanhar os visitantes aos locais de acesso aos computadores. 10) Existem e são eficientes as rotinas usadas para acrescentar, alterar e retirar indivíduos à listagem de pessoal autorizado ao acesso dos recursos computacionais da organização.

PROGRAMA DE AUDITORIA DE SISTEMAS	
ÁREA: CONTROLES GERAIS/ POLÍTICA DE SEGURANÇA	
OBJETIVO: verificação quanto à Segurança Legal, Administrativa, Física, e Lógica dos Sistemas de Informações.	
INSTRUÇÕES DO PROGRAMA	
Verificar se:	
11) Existem procedimentos instituídos para a alteração frequente de senhas, e que não aceitem que algumas senhas, por serem óbvias, sejam reutilizadas pelo mesmo usuário.	
12) Existe o hábito de vários usuários partilharem a mesma senha, ou confidencia-la a outros usuários não autorizados, infringindo o esquema de segurança de acesso.	
13) O formato determinado para as senhas é apropriado.	
14) Existem procedimentos de segurança que preservem a não visualização da senha na tela do computador no decurso de <i>logon</i> , ou que a senha seja impressa em relatórios ou alocada em arquivos não criptografados.	
15) A administração de segurança atualiza com frequência as capacidades de acesso dos usuários.	
16) Existem <i>logs</i> dos dados para que possam ser auditados, e estes <i>logs</i> são resguardados contra destruição proposital ou ocasional.	
17) Existem <i>logs</i> e relatórios de violações às rotinas de segurança.	
18) Há formalização da necessidade do usuário e respectiva autorização para o acesso aos recursos computacionais.	
19) As rotinas de proteção contra incêndios usadas pela organização estão em conformidade com as normas da ABNT e foram divulgadas por toda a organização.	
20) As salas dos computadores estão dotadas com <i>sprinklers</i> , extintores, alarmes ou demais instrumentos contra incêndio e estes são revisados periodicamente.	
21) Existem estabilizadores de energia e <i>no-break</i> que assegurem a disponibilidade dos recursos computacionais no caso de variações ou falta de energia elétrica.	
FONTE- Elaborado pela autora da dissertação.	

Outro aspecto integrante dos Controles Gerais refere-se ao **Plano de Contingências**. Como apresentado no capítulo 4, este plano deve explicitar as alternativas de recuperação de dados para a continuidade dos serviços na área de informática da organização.

As instruções apresentadas no QUADRO 22, objetivam constatar a existência e manutenção de um Plano de Contingências para processamento de aplicativos na ocorrência de uma falha de *hardware* ou *software*, ou ainda, de destruição temporária ou permanente dos recursos computacionais.

**QUADRO 22- PARTE 1 DO PROGRAMA DE AUDITORIA DE SISTEMAS: CONTROLES
GERAIS/PLANO DE CONTINGÊNCIAS**

PROGRAMA DE AUDITORIA DE SISTEMAS
AREA: CONTROLES GERAIS/ PLANO DE CONTINGÊNCIAS
OBJETIVO: verificação do Plano de Contingências da organização.
INSTRUÇÕES DO PROGRAMA
Verificar se: 1) Existe um plano de contingências divulgado na organização e testado freqüentemente. 2) É apropriado o tempo determinado pela organização para iniciar os procedimentos de emergência contidos no plano de contingências. 3) Os procedimentos evidenciados no plano de contingências são completos e compreendem todas as ocorrências imprevistas que podem incidir em um ambiente computacional. 4) Existe uma listagem de recursos computacionais considerados críticos pela organização e o plano de contingências identifica todos estes recursos computacionais e os arquivos de dados críticos. 5) Existe armazenamento em meios magnéticos ou digitais, onde estão os dados e programas críticos da organização, fora de suas dependências e estes arquivos são atualizados freqüentemente. 6) O plano de contingências prevê um local alternativo, com recursos compatíveis, a ser utilizado no reparo das operações de processamento de dados da organização após uma catástrofe; este local tem medidas de segurança apropriadas que garantam a integridade ou a restauração imediata dos dados nele mantidos. 7) Existe <i>backup</i> de arquivos de dados e estes são sempre atualizados pelos usuários.
FONTE- Elaborado pela autora da dissertação.

A ausência ou inadequação dos Controles Gerais, quer sejam sobre os Controles Organizacionais, Política de Segurança ou Plano de Contingências, deixam os Sistemas de Informações e o ambiente computacional sujeitos a diversos riscos, como a violação da segurança de acesso aos recursos computacionais e dados, o que implica em fraudes, erros, perda de dados e furto de equipamentos.

A **Parte 2** do Programa de Auditoria de Sistemas, refere-se aos **Controles de Softwares Aplicativos**. Conforme apresentado na seção 7.5.2, estes controles são incorporados diretamente em programas aplicativos, com o objetivo de garantir um processamento confiável e acurado. As instruções do Programa constantes do

QUADRO 23 referem-se a os **Controles de Entrada de Dados**, que são projetados a fim de que os dados sejam convertidos para um formato padrão e inseridos no aplicativo de forma precisa, completa e tempestiva.

QUADRO 23- PARTE 2 DO PROGRAMA DE AUDITORIA DE SISTEMAS: CONTROLES DE SOFTWARES APLICATIVOS/ENTRADA DE DADOS

PROGRAMA DE AUDITORIA DE SISTEMAS
ÁREA: CONTROLES DE SOFTWARES APLICATIVOS/ ENTRADA DE DADOS
OBJETIVO: verificação quanto aos controles sobre as entradas dos dados no sistema, para garantir que os dados sejam inseridos de forma precisa, completa e tempestiva.
INSTRUÇÕES DO PROGRAMA
Verificar se: 1) Os campos de dados, cujo preenchimento seja de caráter indispensável, são facilmente evidenciados na tela do computador. 2) Há identificação nas telas do computador dos códigos de entrada considerados inválidos. 3) Existe uma padronização das telas, no que diz respeito ao acionamento de teclas, à apresentação e à disposição dos campos de dados. 4) Existem rotinas formais para as atividades do processo de preparação de dados. 5) Quando a entrada de dados ocorre em microcomputadores, existem procedimentos formais de segurança que dispõem sobre a utilização, manutenção e controle dos códigos de identificação do usuário e do microcomputador. 6) A codificação de identificação do usuário e do microcomputador são usadas no processo de autorização de entrada de dados. 7) Os documentos-fonte são arquivados por tempo necessário para garantir a reconstrução de dados, e estes documentos podem ser recuperados com facilidade. 8) Os órgãos que originaram os documentos-fonte mantêm cópias desta documentação. 9) Os documentos-fonte arquivados são acessados somente por pessoas autorizadas. 10) Terminado o prazo de retenção, os documentos-fonte são destruídos de acordo com o estabelecido pela Tabela de Temporalidade do Município. 11) Existem informações de ajuda ao usuário dos sistemas de informações com o intento de promover a entrada de dados e diminuir o quantitativo de erros. 12) Existem procedimentos para a detecção e impedimento da entrada de dados errôneos ou incompletos nos sistemas de informações. 13) Os procedimentos de legitimação de dados examinam a existência de códigos de aprovação e autorização, valores válidos e preenchimento de campos de dados obrigatórios. 14) Existem procedimentos para evidenciar, retificar e re-submeter os dados errôneos nos sistemas de informações. 15) As mensagens de erro geradas pelos sistemas de informações são claras e de fácil entendimento pelos usuários.

FONTE- Elaborado pela autora da dissertação.

No QUADRO 24 estão apresentadas as instruções do Programa que se destinam aos **Controles do Processamento e de Saída dos Dados dos *Softwares* Aplicativos**. Os Controles de Processamento devem assegurar que todos os dados sejam processados e que o aplicativo seja executado corretamente. Os Controles da Saída são utilizados para garantir a integridade, a correta e tempestiva distribuição dos dados de saídas.

QUADRO 24- PARTE 2 DO PROGRAMA DE AUDITORIA DE SISTEMAS: CONTROLES DE SOFTARES APLICATIVOS/ PROCESSAMENTO E SAÍDA DOS DADOS

PROGRAMA DE AUDITORIA DE SISTEMAS
ÁREA: CONTROLES DE <i>SOFTWARES</i> APLICATIVOS/ PROCESSAMENTO E SAÍDA DE DADOS
OBJETIVO: exame dos procedimentos que garantam a integridade do processamento e verifiquem o trabalho executado, para a geração de relatórios e informações confiáveis, e ainda, a distribuição destes documentos.
INSTRUÇÕES DO PROGRAMA
Verificar se:
1) Os dados incorretos são rejeitados durante o processamento dos sistemas.
2) Existe um processo de legitimação dos dados anterior à sua gravação.
3) Existem procedimentos formais para evidenciar, corrigir e re-submeter os dados rejeitados no processamento.
4) As mensagens geradas pelos sistemas de informações referentes ao tratamento de erros de processamento são claras e de fácil entendimento pelos usuários.
5) Os arquivos provisórios de dados rejeitados pelos sistemas de informações são controlados apropriadamente e geram mensagens de alerta para que estes dados sejam vistoriados e retificados.
6) Os dados constantes nos relatórios emitidos pelos sistemas de informações são exatos.
7) Existem controles para que os relatórios sejam enviados somente aos devidos usuários das informações neles contidas.
8) Existem procedimentos formais para a distribuição dos dados de saída e se estes são adequados.
9) Os relatórios impressos são distribuídos dentro do prazo determinado pela organização.
10) Existem procedimentos de <i>logs</i> para os relatórios que tenham algum tipo de erros.
11) Há classificação formal para identificar os relatórios como sigilosos, críticos ou de acesso irrestrito.
12) Existem procedimentos que restrinjam o acesso a dados confidenciais apenas a pessoas autorizadas.
13) A eliminação dos relatórios sigilosos é feita de forma apropriada e em conformidade com a Tabela de Temporalidade do Município.

FONTE- Elaborado pela autora da dissertação

A falta ou ineficiência dos Controles dos Aplicativos pode acarretar perda de aplicativos e dados, funcionamento incorreto de aplicativos, gerando informações errôneas e ainda a disponibilidade de relatórios para usuários não autorizados.

A **Parte 3** do Programa de Auditoria de Sistemas é inerente ao **Desenvolvimento de Sistemas**. Estes controles, como disposto na seção 7.5.3, objetivam avaliar a adequação dos procedimentos de projeto, desenvolvimento, implantação e revisão pós-implantação dos sistemas da organização auditada. No QUADRO 25, estão detalhadas as instruções para o controle sobre o Desenvolvimento de Sistemas.

**QUADRO 25- PARTE 3 DO PROGRAMA DE AUDITORIA DE SISTEMAS:
DESENVOLVIMENTO DE SISTEMAS**

PROGRAMA DE AUDITORIA DE SISTEMAS
ÁREA: DESENVOLVIMENTO DE SISTEMAS
OBJETIVO: avaliar a adequação dos procedimentos do projeto, desenvolvimento, implantação e revisão dos sistemas produzidos dentro da organização ou adquiridos por ela.
INSTRUÇÕES DO PROGRAMA
Verificar se: 1) No projeto ou aquisição do sistema foram identificados os motivos para sua implementação, o ambiente operacional, os benefícios a serem alcançados com sua implementação e os futuros usuários. 2) Os usuários participam do processo de definição e autorização para a compra ou desenvolvimento de projetos ou alteração de sistemas de informações. 3) Os funcionários indicados para trabalhar no projeto ou na aquisição dos sistemas de informações têm experiência ou titulação para exercer os afazeres que lhes foram conferidos. 4) Todas as fases da aquisição ou desenvolvimento do projeto foram examinadas e aprovadas pelos usuários que utilizarão os sistemas de informações a serem implantados. 5) Foram feitas pesquisas de viabilidade tecnológica e econômica para definição sobre a opção de aquisição ou de desenvolvimento de projeto de sistemas. 6) As especificações do programa-fonte estipuladas são claras completas. 7) No desenvolvimento dos projetos foram inseridos controles de prevenção, retificação e de trilhas de auditoria apropriadas em cada parte crítica do sistema de informações. 8) Foi instituída uma estratégia de análise e teste do sistema de informações. 9) A documentação dos programas-fonte traz exposição lógica, objetivos a serem alcançados, diagrama de fluxo e formatação de relatórios a serem expedidos pelos sistemas. 10) Foram organizados manuais de operação e manutenção dos sistemas de informações e efetuado treinamento para seus usuários. 11) É feita análise para estimar se as demandas dos usuários foram atendidas.

FONTE- Elaborado pela autora da dissertação.

Como nos demais controles, alguns riscos estão associados à inexistência de controles sobre o Desenvolvimento ou Aquisição de Sistemas como: o uso de um sistema incompatível com os equipamentos da organização, processamento e relatórios incorretos, dificuldades de manutenção do *software* e insatisfação do usuário, acarretando perda de produtividade.

A **Parte 4** do Programa de Auditoria de Sistemas é relativa aos controles sobre os **Bancos de Dados**, que como discorrido na seção 7.5.4, devem manter e organizar os dados da organização e torná-los disponíveis para programas aplicativos, quando requisitados.

No QUADRO 26 estão relacionadas as instruções detalhadas do Programa que visam garantir a disponibilidade, integridade, confidencialidade, controle de uso e acesso dos dados.

QUADRO 26- PARTE 4 DO PROGRAMA DE AUDITORIA DE SISTEMAS: BANCO DE DADOS

PROGRAMA DE AUDITORIA DE SISTEMAS
ÁREA: BANCO DE DADOS
OBJETIVO: verificação quanto ao estabelecimento de procedimentos que visam garantir a disponibilidade, integridade, confidencialidade, controle de uso e acesso dos dados.
INSTRUÇÕES DO PROGRAMA
Verificar se: 1) Estão definidas e documentadas formalmente as políticas para administração do Banco de Dados. Estas políticas abrangem diretrizes de disponibilidade, integridade, confidencialidade, controle de uso e acesso dos dados. 2) O administrador do Banco de Dados tem habilitação e capacitação técnica compatível com suas funções. 3) Existem <i>logs</i> para as atividades de administração de dados. 4) Existem procedimentos para <i>backup</i> e recuperação dos dados. 5) Os dados da base são íntegros e consistentes. 6) A criação e a alteração de tabelas e descrição de dados são monitoradas por pessoal capacitado. 7) Os dados confidenciais podem ser acessados somente através do SGBD. 8) Existe procedimento de autorização formal de acesso aos dados da base. 9) Existe uma listagem dos sistemas que compartilham a base de dados. 10) O SGBD permite acesso concorrente a um mesmo componente de dados e é capaz de monitorar de forma apropriada.
FONTE- Elaborado pela autora da dissertação.

Os riscos mais comuns relacionados à falta de controles sobre os Bancos de Dados são a indisponibilidade de dados para os aplicativos, o uso de dados não íntegros e inconsistentes, a dificuldade de recuperação dos dados e o acesso de dados por pessoas não autorizadas.

A **Parte 5** do Programa de Auditoria de Sistemas é atinente aos controles sobre as **Redes de Computadores**. Como apresentado na seção 7.5.5, estes controles visam

verificar a existência de procedimentos e políticas para a gerência do ambiente de rede e garantir a segurança dos dados e da rede.

No QUADRO 27 estão detalhadas as instruções para o controle sobre as Redes de Computadores.

QUADRO 27- PARTE 5 DO PROGRAMA DE AUDITORIA DE SISTEMAS: REDE DE COMPUTADORES

PROGRAMA DE AUDITORIA DE SISTEMAS
ÁREA: REDE DE COMPUTADORES
OBJETIVO: verificação quanto à instituição de procedimentos para o controle de <i>hardware</i> e <i>software</i> e para a segurança da rede de computadores.
INSTRUÇÕES DO PROGRAMA
Verificar se: 1) Os procedimentos de controle de processamento de rede de computadores são testados e analisados freqüentemente. 2) Existem procedimentos formais que definam as atividades a serem processadas na rede. 3) Os procedimentos de operação da rede foram divulgados a todos os usuários da organização. 4) Foi instituída uma política de <i>backup</i> da rede de computadores, e existe controle sobre as alterações feitas nos dados compartilhados através da rede de computadores. 5) Os procedimentos de segurança da rede de computadores são suficientes e apropriados para resguardar os recursos físicos da rede, a integridade dos <i>softwares</i> e os dados armazenados na rede. Estes procedimentos são freqüentemente avaliados. 6) Há controle de acesso aos terminais da rede de computadores. 7) A configuração de rede de computadores usada propicia que a incidência de uma falha em um de seus terminais não acarrete queda de toda a rede. 8) Existem procedimentos de recuperação da rede de computadores. 9) São usadas senhas de identificação dos usuários de microcomputadores interligados à rede. 10) Os microcomputadores da rede de computadores são desconectados posteriormente a um determinado quantitativo de tentativas de acesso não permitido. 11) Foram instituídos perfis de acesso para usuários, determinando recursos, dados, aplicativos e operações que estes podem acessar e comandos que podem efetuar. 12) Foi definida uma política de segurança de correio eletrônico, observando os riscos de vírus e outras ameaças programadas.
FONTE- Elaborado pela autora da dissertação.

Os principais riscos decorrentes da inexistência de controles sobre as redes de computadores consistem na facilidade de acesso, alterações a dados e programas e perda de informações não protegidas por cópias de segurança.

A **Parte 6** do Programa de Auditoria de Sistemas é relativa aos controles sobre os **Microcomputadores**. Como discorrido na seção 7.5.6 estes controles visam garantir a consistência da operação do *software* instalado e a segurança dos recursos computacionais.

O QUADRO 28 evidencia instruções para os controles sobre os Microcomputadores.

**QUADRO 28- PARTE 6 DO PROGRAMA DE AUDITORIA DE SISTEMAS:
MICROCOMPUTADORES**

PROGRAMA DE AUDITORIA DE SISTEMAS	
ÁREA: MICROCOMPUTADORES	
OBJETIVO: estabelecer normas para aquisição de microcomputadores, garantir a consistência do <i>software</i> instalado, dos dados e a segurança dos recursos computacionais	
INSTRUÇÕES DO PROGRAMA	
Verificar se: 1) A organização estabeleceu normas formais para aquisição e utilização de microcomputadores e <i>software</i> compatível. 2) Foram estabelecidos procedimentos para a segurança sobre o uso de microcomputadores. 3) É elaborado inventário sobre os recursos computacionais de microinformática. 4) É feita uma análise de custo/benefício antes da aquisição de novos microcomputadores e <i>softwares</i>, através do devido procedimento licitatório, e ainda, feito o exame sobre a compatibilidade destes com o ambiente já existente. 5) Existem procedimentos que impeçam a pirataria de <i>software</i> de microcomputador. 6) A documentação de <i>software</i> de microcomputador é atual e arquivada em local adequado. 7) Existem procedimentos formais para catalogação, armazenagem e feitura de <i>backup</i> dos arquivos de dados e programas-fonte. 8) Existem em todos os microcomputadores <i>softwares</i> antivírus em versões atualizadas. 9) Os usuários de microcomputador têm o hábito de submeter ao <i>software</i> antivírus os arquivos em meio magnético e digital. 10) As cópias dos arquivos de dados críticos ou confidenciais são mantidas em local seguro. 11) O plano de contingências compreende a área de microcomputadores. 12) São usados estabilizadores de energia ou dispositivos análogos para preservação dos microcomputadores. 13) Os usuários dos microcomputadores receberam treinamento adequado e periódico. 14) São realizadas freqüentemente manutenções nos microcomputadores da organização. 15) Existe controle sobre os discos rígidos dos microcomputadores da organização. 16) Os microcomputadores conectados à <i>internet</i> têm mecanismos de proteção contra acesso indevido. 17) Existe um centro de suporte ao usuário mantido pela PRODABEL capaz de dar informações, tirar dúvidas de utilização e registrar problemas.	
FONTE- Elaborado pela autora da dissertação.	

Ressalta-se que os riscos mais comuns decorrentes da inexistência de controles sobre os Microcomputadores são os furtos de equipamentos e os acessos não autorizados aos dados dos sistemas.

Observa-se nesta seção, que o Programa de Auditoria de Sistemas proposto, compreendeu todas as áreas de controle da Auditoria de Sistemas e de uma Política de Segurança de Sistemas, centrando-se nos pontos mais críticos de controle. Destarte, a forma sistematizada de consolidar tais controles através da apresentação de objetivos claros e do escopo da auditoria a ser executada, permite a condução de modo adequado o trabalho do auditor.

Contudo, conforme preceitua MONTGOMERY (1954, p.27), o Programa de Auditoria não deve ser imutável e anular toda a independência de critério do auditor, ou seja, a criatividade e a percepção do Auditor de Sistemas não devem ser neutralizadas pelos procedimentos sistematizados do programa.

10.3- Conclusão

Neste capítulo foi apresentado um Modelo de Auditoria de Sistemas para a AUDIM, construído a partir do referencial teórico estudado.

O resultado obtido foi a junção em um único **Programa de Auditoria de Sistemas** dos pontos inerentes à **Segurança de Sistemas** e à **Auditoria de Sistemas**, provendo assim um maior número de controles sobre os **Sistemas de Informações Computadorizados** e o ambiente computacional.

O Programa de Auditoria de Sistemas proposto indica os procedimentos a serem aplicados pelo Auditor de Sistemas, padronizando procedimentos e orientando de maneira eficiente, seu trabalho.

Devido os pontos de auditoria detalhados no Programa, este modelo de Programa de Auditoria de Sistemas pode ser utilizado não somente pela AUDIM, mas também nas demais organizações públicas, bem como nas privadas.

No próximo capítulo, apresentam-se as conclusões finais da presente pesquisa, algumas recomendações para a AUDIM e sugestões para futuros estudos.

11 CONCLUSÕES, RECOMENDAÇÕES E SUGESTÕES

11.1- Introdução

Neste capítulo, são contempladas as conclusões desta dissertação alusivas à metodologia utilizada, ao referencial teórico estudado e aos objetivos de pesquisa propostos.

São também apresentadas recomendações à AUDIM e algumas sugestões que podem motivar estudos futuros. Encerra-se este trabalho com algumas considerações finais.

11.2- Conclusões Quanto à Metodologia da Pesquisa

A adoção do método de estudo de caso, ao permitir a interação da pesquisadora com o ambiente em que os fatos ocorreram, foi fundamental para a obtenção de dados e informações que envolviam o problema de pesquisa levantado.

Todavia, a utilização de várias técnicas de coleta e de análise de dados propiciou à obtenção de resultados mais precisos. Vez que nenhum instrumento de coleta de dados é completo, o uso de diversas fontes de dados permitiu que uma complementasse ocasionais deficiências de outra.

A utilização conjunta da análise de conteúdo com a análise estatística dos questionários aplicados diminuiu a subjetividade de interpretação das informações disponibilizadas pelos entrevistados.

Conclui-se, portanto, que a metodologia empregada mostrou-se adequada para que os

objetivos do presente trabalho fossem alcançados e para que o problema de pesquisa fosse respondido.

11.3- Conclusões Quanto ao Referencial Teórico

O referencial teórico apresentado e discutido nos capítulos 3 a 7 subsidiou tanto a condução da pesquisa quanto às conclusões alcançadas.

O capítulo 3 mostrou que a **informação** constitui um instrumento fundamental para uma organização, seja pública ou privada, pois colabora para a gerência de suas atividades. Por meio de **Sistemas de Informações Computadorizados**, essas informações tornam-se utilizáveis, assessorando o processo de tomada de decisões e permitindo aos gestores uma visão sistêmica da organização. O capítulo abordou ainda a crescente utilização de sistemas de informação computadorizados nas diversas atividades da Administração Pública Brasileira, citando como exemplo a PMBH. Dada a importância dos sistemas de informação para as organizações, concluiu-se que a maior relevância é a adoção de controles sobre estes sistemas.

O capítulo 4 demonstrou que os Sistemas de Informações Computadorizados são mais vulneráveis a riscos do que os sistemas manuais e que, portanto, a segurança desses sistemas deve ser priorizada, já que as informações contidas nos mesmos são essenciais para a organização. Concluiu-se que essa segurança almejada pode ser obtida através da implantação de uma **Política de Segurança** e de um **Plano de Contingências**.

Ao versar sobre o **Controle Interno**, o capítulo 5 demonstrou que este controle constitui um fator preponderante para o êxito de uma organização, tanto que é exigido legalmente para as organizações públicas. Com o disposto neste capítulo, conclui-se que a atividade da Auditoria Interna estabelece-se como um instrumento essencial do **Controle Interno**.

O capítulo 6, corroborando o exposto no capítulo antecessor, evidencia que a **Auditoria Interna** é a atividade de revisão e avaliação dos controles internos e que oferece subsídios para o aprimoramento desses controles, proporcionando a melhoria dos resultados operacionais da organização, e para a tomada de decisão pelos gestores. Conclui-se que para cada modalidade de auditoria o órgão de auditoria interna da organização deve construir um **Programa de Auditoria** detalhado, pois, este indica os procedimentos e as técnicas a serem aplicados em cada fase de uma auditoria e orienta de maneira eficiente o trabalho do auditor, independentemente do grau de afinidade que tenha com a área auditada.

Após o estudo do que a literatura apresenta acerca da **Auditoria de Sistemas**, o capítulo 7 demonstrou a importância desta atividade para assegurar a qualidade e a segurança dos Sistemas de Informações Computadorizados, pois, ela avalia os sistemas e o ambiente computacional em que estão inseridos, com o propósito de identificar os possíveis riscos que estejam ocorrendo, ou que possam ocorrer e de, principalmente, sugerir ações saneadoras e melhoria dos controles internos. Conclui-se também que para cumprir o propósito da Auditoria de Sistemas é necessário que o auditor tenha um perfil adequado, observe a legislação aplicável, adote as técnicas mais apropriadas para desenvolver o seu trabalho e, sobretudo, siga um **Programa de Auditoria de Sistemas**.

Finalizando, conclui-se que, apesar da Auditoria de Sistemas constituir uma modalidade de auditoria fundamental para as organizações, a literatura brasileira sobre o tema apresenta-se extremamente limitada e restrita a poucas obras, principalmente, quando a abordagem refere-se a uma organização pública.

11.4- Quanto aos Objetivos da Pesquisa

Esta seção é apresentada com base no objetivo geral e nos objetivos específicos da pesquisa, evidenciados no capítulo 1 da dissertação, especificamente nas seções 1.3.1. e 1.3.2.

Quanto ao primeiro objetivo específico desta pesquisa _ identificar os Sistemas de Informação Computadorizados da PMBH _ conclui-se que, conforme apresentado na seção 3.6, existem cento e trinta e três sistemas principais que têm por objetivo controlar e gerar informações estratégicas e fundamentais à tomada de decisões pelos gestores públicos. Além desses sistemas existem outros de menor complexidade e de uso mais restrito aos órgãos, voltados a controles mais específicos e informações de menor relevância.

Verificou-se que alguns destes sistemas não são seguros e suas informações não são confiáveis, visto a constatação de algum tipo de erro ou falha nos sistemas pelos auditores, como disposto na seção 9.3.

Conclui-se, quanto ao segundo objetivo da pesquisa _ modelar a AUDIM _ que apesar da AUDIM ser um órgão técnico, dotado de autonomia funcional, que planeja e exerce suas atividades, cuja finalidade é executar a auditoria interna nos órgãos e entidades do Poder Executivo Municipal, esta vêm deixando de perseguir algumas das suas atribuições institucionais, vez que não audita fontes de informação provenientes dos Sistemas de Informações da PMBH. Assim, não é observado o que preceitua o art. 1º do Decreto n. 8.565/96, *verbis*:

“Art. 1º -

c) assistir e orientar a Administração Pública Municipal no âmbito das atribuições de auditoria;

e) examinar e opinar sobre quaisquer fontes de informações relacionadas com as atividades dos órgãos da Administração Pública Municipal;

.....
 i) *determinar e opinar sobre a consistência e legitimidade das informações contábeis e demais dados oficiais da Administração Pública Municipal;* “

Comprovou-se também, que é insignificante o quantitativo de trabalhos realizados pela AUDIM na modalidade de Auditoria de Sistemas, vez que durante seus quinze anos de existência somente três trabalhos foram efetuados, sendo apenas um desempenhado por auditor de cargo efetivo.

Dessa forma, a AUDIM não examina grande parte dos controles internos da PMBH que constituem importantes fontes de informações, tanto para os gestores públicos, quanto para os munícipes.

Por fim, verificou-se que este órgão de controle interno utiliza informações provenientes dos Sistemas de Informações que não são auditados para a realização de auditorias, o que pode estar comprometendo o resultado de seus trabalhos. As seções 8.3, 8.7 e 9.4 serviram de embasamento para estas conclusões.

As conclusões acerca do terceiro objetivo da pesquisa _ detectar os fatores que inibem a AUDIM de realizar Auditoria nos Sistemas de Informação Computadorizados da PMBH _ foram pautadas nas seções 8.7, 9.4 e 9.5. De tal fundamentação, pôde-se concluir que são três os principais fatores que prejudicam à realização de Auditores de Sistemas pela AUDIM:

a) Pouca intenção da AUDIM em proceder Auditoria de Sistemas, vez que :

- as programações anuais de auditoria da AUDIM não contemplam a realização de Auditoria de Sistemas;
- não existem no órgão manuais, programas ou técnicas próprias desta modalidade de auditoria;
- inexistente planejamento formal para inserir ou ampliar a realização de Auditoria de Sistemas pela AUDIM;

BIBLIOTECA DA
FUNDAÇÃO JOÃO PINHEIRO

BIBLIOTECA DA
FUNDAÇÃO JOÃO PINHEIRO

- a AUDIM não mantém articulação ou contato com auditorias internas de outros órgãos governamentais que já realizam Auditoria de Sistemas;
- nunca foi efetuado treinamento sobre o tema Auditoria de Sistemas com recursos próprios da AUDIM;
- desprovisionamento completo do acervo da biblioteca da AUDIM em relação à Auditoria de Sistemas.

b) Conhecimento insuficiente da maioria dos auditores sobre os Sistemas de Informação Computadorizados da PMBH, o que implica no desconhecimento das relevantes informações processadas pelos sistemas.

c) Desinteresse e incapacidade técnica da maioria dos auditores pela atividade de Auditoria de Sistemas.

Quanto ao quarto e último objetivo específico _ identificar instrumentos de Auditoria de Sistemas e elementos de uma Política de Segurança de Sistemas de Informação _ pôde-se concluir que :

a) Consubstanciado nas seções 4.3, 4.4, 4.6 e 4.7 verificou-se que os principais elementos de uma política de segurança são: o estabelecimento de normas internas da organização para gerenciar, proteger e distribuir suas informações e recursos computacionais; o cumprimento da legislação inerente à segurança da informação; a observação dos controles sobre cada uma das modalidades de segurança ; e o estabelecimento do Plano de Contingências, no qual são explicitadas as alternativas de recuperação de dados para a continuidade dos serviços na área de informática da organização.

b) Com base nas seções 7.4 e 7.5 constatou-se que os principais instrumentos de Auditoria de Sistemas são: as técnicas próprias desta modalidade de auditoria (*softwares*, questionários, test-deck, mapping, rastreamento, análise de log e do programa-fonte, simulação paralela) e o Programa de Auditoria que compreenda as áreas de Controles Gerais, Controles de Aplicativos, Desenvolvimento de Sistemas, Banco de Dados, Redes de Computadores e Microcomputadores.

O objetivo geral da dissertação _ construir um Modelo de Auditoria de Sistemas para a AUDIM _ foi pautado no referencial teórico, especificamente, nos capítulos 4, 6 e 7. Conclui-se que este modelo, conforme apresentado no capítulo 10 desta dissertação, constitui-se de um Programa de Auditoria no qual foram abordados sistematicamente os principais pontos de controle inerentes a uma Política de Segurança de Sistemas e das áreas contempladas na Auditoria de Sistemas.

Partindo das conclusões acerca dos objetivos da pesquisa, foi possível responder às indagações do Problema da Pesquisa, ou seja: Por que a AUDIM não vem realizando Auditoria de Sistemas e quais instrumentos este órgão de controle poderia adotar para avaliar os Sistemas de Informação Computadorizados da PMBH.

11.5- Recomendações para a AUDIM

Como detalhado na seção anterior, diversos são os fatores que inibem a AUDIM de realizar a modalidade de Auditoria de Sistemas, o que deixa os Sistemas de Informações da PMBH, que são importantes fontes de informações tanto para os gestores públicos quanto para cidadão, sujeitos a vários riscos.

Dessa forma, é preciso que a AUDIM minimize tais fatores, quando não for possível nulificá-los. Para que este órgão consiga ampliar seus trabalhos na área de Auditorias de Sistemas, sugere-se que seja implementado um plano gerencial, do qual constem certos procedimentos, quais sejam:

- a) *Capacitação de Recursos Humanos:* a capacitação de recursos humanos é um fundamento básico para a alavancagem dos trabalhos da AUDIM. É imprescindível que a AUDIM invista no seu corpo técnico, patrocinando cursos de treinamento estruturado, de aperfeiçoamento e reciclagem, voltados para o tema Auditoria de Sistemas e para o conhecimento dos Sistemas de Informação Computadorizados da PMBH.

O auditor também deve investir no seu contínuo aprendizado, buscando participar de cursos, palestras, seminários, inteirando-se dos assuntos sobre o tema afeto, pois, o ambiente em que se atua está em constante mudança, onde somente um profissional com perfil empreendedor conseguirá acompanhá-lo.

- b)** Desenvolver um sistema de articulação e integração com as entidades de controles internos dos demais poderes em todos os níveis da Administração Pública e propiciar a realização de projetos conjuntos de pesquisas e de estudos com outras Auditorias Internas, com entidades de classe, com institutos de pesquisas e/ou entidades educacionais.
- c)** Adquirir literatura da área de Sistemas de Informação, Auditoria de Sistemas e Informática, mantendo o acervo da biblioteca atualizado em forma de livros, revistas, periódicos, CD-Rom, monografias, dissertações e teses.
- d)** Incluir a participação de auditores no processo de desenvolvimento ou na aquisição de Sistemas de Informação pela PMBH. Essa prática antecipa-se a problemas e corrigem disfunções que possam levar a erros vultuosos ou a situações insanáveis. Deve-se procurar a qualidade no processo, e não somente na sua inspeção final.
- e)** Adquirir ou desenvolver *softwares* utilizados como técnicas nas Auditorias de Sistemas.
- f)** Elaborar a Programação Anual de Auditoria, com inserção da Auditoria de Sistemas para os diversos Sistemas Informação da PMBH; e
- g)** Adotar o Programa de Auditoria de Sistemas disposto no capítulo 10 desta dissertação.

11.8- Sugestões para Estudos Futuros

Com base nas questões discutidas neste trabalho, sugerem-se algumas pesquisas para estudos futuros, como adiante relatadas:

- a) avaliação dos Sistemas de Informação da PMBH;
- b) avaliação dos principais CAATs - *Computer Assisted Audit Techniques*, existentes no mercado, mediante um estudo dos diferentes tipos de *softwares* existentes no mercado e utilizados pelas Auditorias Internas;
- c) proposição de um modelo de *software* de Auditoria de Sistemas próprio para a Administração Pública, que possa contribuir para a agilidade da realização de auditorias.

11.6- Considerações Finais

Uma administração eficiente, eficaz e transparente pressupõe a utilização de controles internos adequados e que sejam revisados e aprimorados periodicamente. Se os controles internos são inadequados, as organizações tornam-se vulneráveis e sujeitas a erros e falhas que podem resultar em danos ou prejuízos intencionais ou acidentais à uma organização. Dentre estes riscos, podem-se citar àqueles que incorrem sobre os Sistemas de Informações das organizações:

- a) acesso não autorizado a dados e sistemas;
- b) operação incorreta do sistema;
- c) perda de informações não protegidas por cópias de segurança;
- d) vazamento, modificação ou deturpação de informações;
- e) comprometimento da consistência de dados; e
- f) interrupção de serviços.

Com a adoção da modalidade de Auditoria de Sistemas, a AUDIM poderá avaliar periodicamente os controles internos inerentes aos Sistemas de Informação da PMBH,

tanto para validá-los ou para propor melhorias. Com isso, a PMBH poderá melhorar a qualidade de suas informações, pois, seus sistemas computadorizados gerarão resultados e informações mais confiáveis para o gestor público.

Assim sendo, acredita-se não só estar aprimorando as atividades da instituição municipal, a elevação dos resultados operacionais e subsídios para a tomada de decisões dos gestores, sobretudo o Prefeito, mas principalmente propiciando uma melhoria dos serviços prestados pela Administração Municipal, cujo maior beneficiário será o cidadão.

12 REFERÊNCIAS BIBLIOGRÁFICAS

1. ALMEIDA, Marcelo Cavalcanti. *Auditoria: um curso moderno e completo*. 5. ed. São Paulo: Atlas, 1993.
2. ALTER, Steven. *Information systems: a management perspective*. 2. ed. EUA: Addison-Wesley Educational Publishers Inc, 1996.
3. AMERICAN INSTITUTE OF CERTIFIED PUBLIC ACCOUNTANTS. Disponível na Internet: <<http://www.aicpa.org>> Acesso em: 15 jan. 2002.
4. ARIMA, Carlos Hideo. *Metodologia de auditoria de sistemas*. São Paulo: Érica, 1994.
5. ARTER, Dennis R. *Auditorias da qualidade para melhor desempenho*. Trad. Luiz Liske. Rio de Janeiro: Qualitymark, 1995. (Tradução de: Quality audits for improved performance).
6. ATTIE, William. *Auditoria interna*. São Paulo: Atlas, 1992.
7. ATTIE, William. *Auditoria: conceitos e aplicações*. São Paulo: Atlas, 1995.
8. AUDITORIA DO MUNICÍPIO. Instrução de Serviço DAUDIT n. 001/2001, de 22 de janeiro de 2001. Dispõe sobre o registro das evidências e relatórios de auditoria.
9. BACON, Charles A. *Manual de auditoria*. México: Uteha, 1973.
10. BARDIN, Laurence. *Análise de conteúdo*. Trad. Luís Antero Reto e Augusto Pinheiro. Lisboa: Edições 70, 1977. (Tradução de: L'analyse de contenu).

11. BELO HORIZONTE. Decreto n. 10.545, de 09 de março de 2001. Dispõe sobre alocação, denominação e atribuições de órgãos de terceiro grau hierárquico e respectivos sub-níveis da estrutura organizacional da Administração Direta do Executivo, na Auditoria do Município, e dá outras providências.
12. BELO HORIZONTE. Decreto n. 10.710, de 28 de junho de 2001. Dispõe sobre procedimentos administrativos de licitação e contratação, sobre programação, acompanhamento e avaliação da execução orçamentária e financeira, delega competências e dá outras providências.
13. BELO HORIZONTE. Decreto n. 4.489, de 13 de julho de 1983. Dispõe sobre a organização administrativa da Prefeitura Municipal de Belo Horizonte e dá outras providências.
14. BELO HORIZONTE. Decreto n. 4.523, de 12 de setembro de 1983. Dispõe sobre a estrutura administrativa e o funcionamento de órgãos da Administração Direta e dá outras providências.
15. BELO HORIZONTE. Decreto n. 7.878, de 02 de maio de 1994. Dispõe sobre procedimentos administrativos de licitação e contratação, sobre programação, acompanhamento e avaliação da execução orçamentária e financeira, delega competências e dá outras providências.
16. BELO HORIZONTE. Decreto n. 8.565, de 18 de janeiro de 1996. Aprova as atribuições e a qualificação necessária ao provimento da classe de cargo de provimento efetivo de Auditor I, instituída pela Lei n. 5.447 /1988.
17. BELO HORIZONTE. Lei n. 4.476, de 30 de maio de 1986. Dispõe sobre a primeira fase da estrutura administrativa da Auditoria Geral do Município e dá outras providências .
18. BELO HORIZONTE. Lei n. 5.447, de 30 de novembro de 1988. Dispõe sobre o Quadro de Pessoal da Prefeitura Municipal de Belo Horizonte.

19. BELO HORIZONTE. Lei n. 5.562, de 31 de maio de 1989. Dispõe sobre a estrutura organizacional da Administração Direta da Prefeitura Municipal de Belo Horizonte e dá outras providências.
20. BELO HORIZONTE. Lei n. 6.352, de 15 de julho de 1993. Dispõe sobre a estrutura organizacional da Administração Direta da Prefeitura Municipal de Belo Horizonte e dá outras providências.
21. BELO HORIZONTE. Lei n. 8.146, de 29 de dezembro de 2000. Dispõe sobre a estrutura organizacional da Administração Direta do Poder Executivo e dá outras providências.
22. BELO HORIZONTE. Lei Orgânica do Município de Belo Horizonte, de 21 de março de 1990.
23. BERTALANFFY, Ludwing Von. *Teoria geral dos sistemas*. 2. ed. São Paulo. Vozes, 1975.
24. BIO, Sérgio Rodrigues. *Sistemas de informação: um enfoque gerencial*. São Paulo: Atlas, 1985.
25. BOVE, Tatianna Cruz. *A informática e a auditoria*. Revista do Tribunal de Contas de Minas Gerais, Belo Horizonte, n. 2, p.147-168, 1995.
26. BRASIL, Decreto-Lei n. 200, de 25 de fevereiro de 1967. Dispõe sobre normas de administração financeira e de contabilidade.
27. BRASIL. Constituição da República Federativa do Brasil, 1988. Brasília: Senado Federal, Centro Gráfico, 1988.
28. BRASIL. Decreto n. 2.134, de 24 de janeiro de 1997. Dispõe sobre a categoria dos documentos públicos sigilosos e o acesso a eles.

29. BRASIL. Decreto n. 2.556, de 20 de abril de 1998. Regulamenta o registro previsto no art. 3º da Lei n. 9.609, que dispõe sobre a proteção da propriedade intelectual de programa de computador e sua comercialização.
30. BRASIL. Decreto n. 2.910, de 29 de dezembro de 1998. Estabelece normas para a salvaguarda de documentos, materiais, áreas, comunicações e Sistemas de Informações de natureza sigilosa.
31. BRASIL. Decreto n. 3.294, de 15 de dezembro de 1999. Institui o Programa Sociedade da Informação e dá outras providências.
32. BRASIL. Decreto n. 3.505, de 13 de junho de 2000. Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal.
33. BRASIL. Decreto n. 79.099, de 06 de janeiro de 1977. Aprova o regulamento para a salvaguarda de assuntos sigilosos.
34. BRASIL. Instrução Normativa do Tribunal de Contas da União n. 28, de 05 de maio 1999. Estabelece regras para a implementação da *homepage* Contas Públicas, de que trata a Lei n. 9.755/98.
35. BRASIL. Lei Complementar n. 101, de 04 de maio 2000. Estabelece normas de finanças públicas voltadas para a responsabilidade na gestão fiscal e dá outras providências.
36. BRASIL. Lei n. 10.180, 06 de fevereiro de 2001. Organiza e disciplina os sistemas de planejamento e de orçamento federal, de administração financeira federal, de contabilidade federal e de controle interno do Poder Executivo Federal, e dá outras providências.
37. BRASIL. Lei n. 4.320, de 17 de março de 1964. Estatui Normas Gerais de Direito Financeiro para elaboração e controle dos orçamentos e balanços da União, dos Estados, dos Municípios e do Distrito Federal.

38. BRASIL. Lei n. 6.404, de 15 de dezembro de 1976. Dispõe sobre as sociedades por ações.
39. BRASIL. Lei n. 8.666, de 21 de junho de 1993. Institui normas para licitações e contratos administrativos.
40. BRASIL. Lei n. 9.296, de 24 de julho de 1996. Regulamenta o inciso XII, do art. 5º da Constituição Federal. Este dispositivo aplica-se à interceptação do fluxo de comunicações em Sistemas de informática.
41. BRASIL. Lei n. 9.609, de 19 de fevereiro de 1998. Dispõe sobre a proteção de propriedade intelectual de programa de computador e sua comercialização no País.
42. BRASIL. Lei n. 9.610, de 19 de fevereiro de 1998. Altera, atualiza e consolida a legislação sobre direitos autorais.
43. BRASIL. Lei n. 9.755, de 16 dezembro de 1998. Dispõe sobre a criação de *homepage* na *Internet*, pelo Tribunal de Contas da União, para divulgação dos dados e informações que especifica, e dá outras providências.
44. BRASIL. Medida Provisória n. 2.200, de 24 de agosto de 2001. Organiza e disciplina os sistemas de planejamento e de orçamento federal, de administração financeira federal, de contabilidade federal e de controle interno do Poder Executivo, e dá outras providências.
45. BRASIL. Medida Provisória n. 2.200-2, de 24 de agosto de 2001. Institui a Infra-Estrutura de Chaves Públicas Brasileira para garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras.
46. BRASIL. Projeto de Lei do Senado n. 234, de 1996. Define crime contra a inviolabilidade de comunicação de dados de computador.

47. BRASIL. Projeto de Lei do Senado n. 76, de 2000. Define e tipifica os delitos informáticos.
48. BRASIL. Projeto de Lei do Senado n. 84, de 1999. Dispõe sobre os crimes cometidos na área de informática e suas penalidades.
49. BRASIL. Projeto de Lei n. 1.713, de 1996. Dispõe sobre o acesso, a responsabilidade e os crimes cometidos nas redes integradas de computadores.
50. BRASIL. Resolução Comitê Gestor Infra-Estrutura de Chaves Públicas Brasileira- ICP Brasil n. 2, de 25 de setembro de 2001. Aprova a Política de Segurança da Infra-Estrutura de Chaves Públicas (ICP) Brasileira.
51. BUENO, Francisco da Silveira. *Dicionário escolar da língua portuguesa*. 6. ed. Rio de Janeiro: Ministério da Educação e Cultura, 1969.
52. BURCH, J.G., STRATER, F.R. *Information systems: theory and practice*. New York: John Wiley & Sons, 1974.
53. CARDOSO, Douglas. *Avaliação do SAP R/3 como instrumento para a gestão financeira: um estudo de caso no setor siderúrgico brasileiro*. Belo Horizonte: Faculdade de Ciências Econômicas da Universidade Federal de Minas Gerais, 2001. (Dissertação, Mestrado em Administração).
54. CASH, James; BAILEY, Andrew D. & WHINSTON, Andrew B. *A Survey of techniques for auditing EDP*. New York: John Wiley & Sons, 1977.
55. CAUTELA, Alciney Lourenço; Polloni Enrico Giulio Franco. *Sistemas de informação*. 4. ed. São Paulo: Atlas, 1996.
56. CHAMBERS, Andrew D. *Computer auditing*. London: Pitman, 1981.
57. COMITÉ EUROPÉEN DE NORMALISATION ÉLECTROTECHNIQUE. Disponível na *Internet*: <<http://www.cenelec.be>> Acesso em: 15 jan. 2002.

58. COMITÉ EUROPÉEN DE NORMALISATION. Disponível na *Internet*. <<http://www.cenorm.be>> Acesso em: 15 jan. 2002.
59. CONSELHO FEDERAL DE CONTABILIDADE – CFC. *Princípios fundamentais de contabilidade e normas brasileiras de contabilidade*. Brasília: CFC, 2000.
60. CONSELHO FEDERAL DE CONTABILIDADE – CFC. Resolução n. 780, de 24 de março de 1995. Norma Brasileira de Contabilidade – Auditoria Interna.
61. CONSELHO FEDERAL DE CONTABILIDADE – CFC. Resolução n. 781, de 24 de março de 1995. Normas Profissionais do Auditor Interno.
62. CONSELHO FEDERAL DE CONTABILIDADE – CFC. Resolução n. 803, de 28 de julho de 1995. Das Características da Informação Contábil.
63. CONSELHO FEDERAL DE CONTABILIDADE – CFC. Resolução n. 821, de 17 de dezembro de 1997. Normas Profissionais de Auditor Independente.
64. CONSELHO FEDERAL DE CONTABILIDADE – CFC. Resolução n. 828, de 11 de dezembro de 1998. Papéis de Trabalho e Documentação de Auditoria.
65. CONSELHO FEDERAL DE CONTABILIDADE – CFC. Resolução n. 836, de 22 de fevereiro de 1999. Fraude e Erro.
66. CONSELHO FEDERAL DE CONTABILIDADE – CFC. Resolução n. 839, de 26 de fevereiro de 1999. Transações e Eventos Subseqüentes.
67. CONSELHO FEDERAL DE CONTABILIDADE – CFC. Resolução n. 851, de 13 de agosto de 1999. Informações aos Conselhos Regionais de Contabilidade.

68. CONSELHO REGIONAL DE CONTABILIDADE DO ESTADO DE SÃO PAULO – CRCSP. *Curso básico de auditoria 1: normas e procedimentos*. 2.ed. São Paulo: Atlas, 1992.
69. CONSELHO REGIONAL DE CONTABILIDADE DO ESTADO DE SÃO PAULO – CRCSP. *Controle interno nas empresas*. São Paulo: Atlas, 1998.
70. CONSELHO REGIONAL DE CONTABILIDADE DO ESTADO DE SÃO PAULO – CRCSP. *Auditoria por meios eletrônicos*. São Paulo: Atlas, 1999.
71. CONSELHO REGIONAL DE CONTABILIDADE DO RIO GRANDE DO SUL – CRCRS. *O que você precisa saber sobre auditoria interna*. Rio Grande do Sul: CRCRS, 1995.
72. COOK, John Wiliam, WINLE, Gary M. *Auditoria: filosofia e técnica*. Trad. Sonia Schwartz. São Paulo: Saraiva, 1981. (Tradução de: Auditing philosophy and technique).
73. COOK, John Wiliam, WINLE, Gary M. *Auditoria: filosofia e técnica*. Trad. Sonia Schwartz. São Paulo: Saraiva, 1983. (Tradução de: Auditing philosophy and technique).
74. DAVIES, Ernest Coulter. *Auditing*. México:Uteha, 1974.
75. DAVIS, Gordon Bitter. *Management information systems: conceptual foudations, structure and development*. Minnesota: McGraw–Hill Ltd., 1974.
76. DIAS, Cláudia. *Segurança e auditoria da tecnologia da informação*. Rio de Janeiro: Axcel Books, 2000.
77. DOUGLAS, Ian. *Computer audit and control handbook*. EUA: Butterworth-Heinermann, 1995.
78. EUROPEAN TELECOMMUNICCATIONS STANDARDS INSTITUTE - Disponível na Internet: <<http://www.etsi.org>> Acesso em: 15 jan. 2002.

79. FILOMENA, Sérgio Fernando E., BREDAS, Zulmir Ivânio. *Auditoria na administração pública*. Rio Grande do Sul : S/ editora, 1998.
80. FRANÇA, Júnia Lessa. et al. *Manual para normalização de publicações técnicos - científicas*. Belo Horizonte: UFMG, 2001.
81. FRANCO, Hilário, MARRA, Ernesto. *Auditoria contábil*. 2.ed. São Paulo: Atlas, 1989.
82. GIL, Antônio de Loureiro. *Auditoria de computadores*. 4. ed. São Paulo: Atlas, 1998.
83. GIL, Antônio de Loureiro. *Auditorias operacional e de gestão: qualidade da auditoria*. 4.ed. São Paulo: Atlas, 1999.
84. HOLMES, Arthur W. *Auditoria: Principio Y Procedimiento*. México: Uteha, 1972.
85. IBRACON. *Normas internacionais de auditoria 1997*. Trad. Vera Maria Conti Nogueira e Danilo A. Nogueira. São Paulo: IBRACON, 1998. (Tradução de: international norm Auditing 1997).
86. IMONIANA, Joshua Onome. *Auditoria de sistemas computadorizados*. São Paulo: Faculdade de Economia e Administração da Universidade de São Paulo, 1994. (Dissertação, Mestrado em Contabilidade).
87. INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION. Disponível na *Internet*: <<http://www.isaca.org>> Acesso em: 15 jan. 2002.
88. INSTITUTO DOS AUDITORES INTERNOS DO BRASIL - AUDIBRA. *Curso básico de auditoria interna*. São Paulo, 1994.
89. INSTITUTO DOS AUDITORES INTERNOS DO BRASIL - AUDIBRA. *Normas brasileiras para o exercício da auditoria interna*. 2. ed. São Paulo, 1992.

90. INSTITUTO DOS AUDITORES INTERNOS DO BRASIL - AUDIBRA. *Procedimentos de auditoria interna: organização básica da auditoria interna*. São Paulo, 1991.
91. INSTITUTO NACIONAL DE ESTADÍSTICA E INFORMÁTICA - INEI. *Auditoría para la seguridad informática*. Peru, 2002.
92. INTERNATIONAL ELECTROTECHNICAL COMISSION - Disponível na *Internet*: <<http://www.iec.ch>> Acesso em: 15 jan. 2002.
93. INTERNATIONAL FEDERATION OF ACCOUNTANTS - Disponível na *Internet*: <<http://www.ifac.org>> Acesso em: 15 jan. 2002.
94. INTERNATIONAL ORGANIZATION FOR STANDARDIZATION - Disponível na *Internet*: <<http://www.iso.ch>> Acesso em: 15 jan. 2002.
95. INTERNATIONAL TELECOMMUNICATIONS UNION - Disponível na *Internet*: <<http://www.itu.int>> Acesso em: 15 jan. 2002.
96. KOHLER, Eric L. *Dictionary for accountante*. EUA: Prentice-Hall, 1963.
97. LAUDON, Kenneth C., LAUDON, Jane P. *Management information systems: organization and technology in the networked enterprise*. 6. ed. EUA: Prentice-Hall, 2000.
98. LAUDON, Kenneth C., LAUDON, Jane P. *Sistemas de informação com internet*. 4. ed. Rio de janeiro: LTC Editora, 1999.
99. LEMOS, Guido. et al. *Redes de computadores: das Lans, Mans e Wans às redes ATM*. Rio de Janeiro: Campus, 1995.
100. LOBO, Francisco Gabriel de Souza, et al. *Recursos instrumentais na auditoria pública*. Revista do Instituto dos Auditores Internos do Brasil. Curitiba: AUDIBRA, p. 26-37, nov. 1986.

101. MACHADO JR., José Teixeira, REIS, Heraldo da Costa. *A Lei n. 4.320 comentada*. Rio de Janeiro: IBAM, 1991.
102. MARCONI, Marina de Andrade, LAKATOS, Eva Maria. *Técnicas de pesquisa: planejamento e execução de pesquisas, amostragens e técnicas de pesquisas, elaboração, análise e interpretação de dados*. 4.ed. São Paulo: Atlas, 1999.
103. MCGEE, J., PRUSAK, L. *Gerenciamento estratégico da informação*. Rio de Janeiro: Campus, 1994.
104. MINAS GERAIS. Lei Complementar n. 33, de 28 de junho de 1994. Lei Orgânica do Tribunal de Contas do Estado de Minas Gerais.
105. MINISTÉRIO DA CIÊNCIA E TECNOLOGIA – Disponível na *Internet*: <<http://www.mct.gov.br>> Acesso em: 15 jan. 2002.
106. MOELLER, Robert. *Computer audit, control and security*. New York: Jonh Wiley & Sons, 1989.
107. MONTGOMERY, R. *Auditing, theory and pratice*. 6. ed. New York: Ronald Press Company, 1954.
108. MORAIS, Maria Fernanda de. *Auditoria geral do município: atuação e reflexos na administração municipal*. Belo Horizonte: Fundação João Pinheiro, 1997. (Monografia , Especialização em Administração Municipal).
109. OLIVEIRA, Djalma de Pinho Rebouças. *Sistemas de informações gerenciais*. 5. ed. São Paulo: Atlas, 1998.
110. PAULA, Maria Goreth Miranda Almeida. *Auditoria interna: embasamento conceitual e suporte tecnológico*. São Paulo: Atlas, 1999.
111. PEDRON, Ademar João. *Metodologia científica*. 2.ed. Brasília: Edição do Autor, 1998.

112. PISCITELLI, Roberto B. *Contabilidade pública: uma abordagem da administração financeira pública*. São Paulo: Atlas, 1997.
113. PLEEGER., Charles. *Security in computing*. New York: Prentice Hall, 1996.
114. PORTER, R. *Generalized computer audit programs*. New York Jonh Wiley & Sons, 1981.
115. POZZEBON, Marlei, FREITAS, Henrique M. R. *Pela aplicabilidade com maior rigor científico dos estudos de caso em sistema de informações*. In: ENCONTRO NACIONAL DOS PROGRAMAS DE PÓS-GRADUAÇÃO EM ADMINISTRAÇÃO_ ENANPAD, 21., 1997, Rio das Pedras. Anais...Rio de janeiro: ANPAD, 1997.
116. POZZEBON, Marlei, FREITAS, Henrique M. R. *Modelagem de casos: uma nova abordagem em análise qualitativa de dados?*. In: ENCONTRO NACIONAL DOS PROGRAMAS DE PÓS-GRADUAÇÃO EM ADMINISTRAÇÃO_ ENANPAD, 22., 1998, Foz do Iguaçu. Anais...,Rio de janeiro: ANPAD, 1998.
117. PREFEITURA MUNICIPAL DE BELO HORIZONTE - Disponível na *Internet*: <<http://www.pbh.gov.br>> Acesso em: 15 jan. 2002.
118. PRESIDÊNCIA DA REPÚBLICA - Disponível na *Internet*: <<http://www.presidencia.gov.br>> Acesso em: 15 jan. 2002.
119. PRESSMAN, Roger S. *Engenharia de software*. 3. ed. São Paulo: Makron Books, 2000.
120. RODRIGUES, Marcelo. *Avaliação da auditoria interna do governo do Estado do Espírito Santo*. Belo Horizonte: Faculdade de Ciências Econômicas da Universidade Federal de Minas Gerais, 2001. (Dissertação, Mestrado em Administração).
121. SÁ, Antônio Lopes de. *Curso de auditoria*. 8.ed. São Paulo: Atlas, 1998.

122. SECRETARIA DO TESOUREIRO NACIONAL. Instrução Normativa n. 10, de 7 de julho de 1989. Dispõe sobre a aprovação das normas do Sistema de Auditoria da Administração Pública Federal e dá outras providências.
123. SENADO FEDERAL - Disponível na *Internet*: <<http://www.senado.gov.br>> Acesso em: 15 jan. 2002.
124. STAIR, Ralph M. *Princípios de sistemas de informação: uma abordagem gerencial*. 2. ed. Rio de Janeiro: LTC, 1998.
125. STONER, James A. F. & FREEMAN, R. Edward. *Administração*. 5. ed. Rio de Janeiro: Prentice-Hall, 1999.
126. TANENBAUM, Andrew S. *Organização estruturada de computadores*. 6. ed. São Paulo: Campus, 2000.
127. TANENBAUM, Andrew S. *Rede de computadores*. 4. ed. São Paulo: Campus, 1997.
128. THE INSTITUTE OF INTERNAL AUDITORS - Disponível na *Internet*: <<http://www.theiia.org>> Acesso em: 15 jan. 2002.
129. TRIBUNAL DE CONTAS DA UNIÃO. *Manual de auditoria de sistemas*. Brasília: TCU, 1998.
130. TRIBUNAL DE CONTAS DA UNIÃO. Portaria n. 63, de 10 de dezembro de 1996. Dispõe sobre as modalidades de auditorias realizadas pelo Tribunal de Contas da União.
131. TRIBUNAL DE CONTAS DA UNIÃO. *Procedimentos de auditoria: PA02 - sistemas*. Brasília: TCU, 1998.
132. TRIVIÑOS, Augusto N.S. *Introdução à pesquisa em ciências sociais: a pesquisa qualitativa em educação*. São Paulo: Atlas, 1987.

133. WADDELL, Harold R. *Auditoria independente aplicada*. São Paulo: Atlas, 1982.
134. YIN, Robert K. *Case study research: desing and methods series*. v. 5. Califórnia: SAGE Publications, 1984.
135. ZANOTELI, Eduardo José. *Sistemas de informações gerenciais: o uso da informação contábil como apoio à tomada de decisão*. Belo Horizonte: Faculdade de Ciências Econômicas da Universidade Federal de Minas Gerais, 2001. (Dissertação, Mestrado em Administração).
136. ZWASS. *Management information systems*. EUA: WCB, 1992.

GLOSSÁRIO

Autarquia - é o serviço autônomo, criado por lei, com personalidade jurídica, patrimônio e receitas próprias, para executar atividades típicas de Administração Pública que requeiram, para seu melhor funcionamento, gestão administrativa e financeira descentralizada. (PISCITELLI 1997, p. 42)

Chek List - conjunto de instruções para os auditores que serve como meio para controlar a execução adequada do trabalho. (AUDIBRA 1991, p. 29)

Computador - dispositivo capaz de resolver problemas ou manipular dados. O computador recebe dados, executa operações com esses dados e apresenta os resultados dessas operações. (TCU 1998, p. 50)

Documentação - conjunto de técnicas necessárias para apresentação, organização e comunicação, de forma ordenada, do conhecimento especializado empregado em um sistema. (TCU 1998, p. 52)

Documento-fonte - registro original que deverá ser convertido para linguagem computacional. (TCU 1998, p. 52)

Eficácia - é a medida em que uma entidade, programa, projeto, atividade ou função alcança objetivos, políticas, metas operacionais estabelecidas e outros resultados desejados. (AUDIBRA 1991, p. 227)

Eficiência - é a relação entre a produção de bens e serviços ou outros resultados obtidos por uma entidade ou unidade econômica e os recursos utilizados para produzi-los ou executá-los. Uma operação eficiente produz o máximo de resultado para um dado conjunto de recursos aplicados a um nível de qualidade satisfatório e com custos reduzidos. (AUDIBRA 1991, p. 227)

E-mail/Correio Eletrônico - transmissão de mensagens através de uma rede de comunicação. (TCU 1998, p. 51)

Empresa Pública - é a entidade dotada de personalidade jurídica de direito privado, com patrimônio próprio e capital exclusivo da União, Estado ou Município, criada por lei para exploração de atividade econômica que o Governo seja levado a exercer, por motivos de conveniência ou contingência administrativa. (PISCITELLI 1997, p. 42)

Escopo da Auditoria - Envolve a abrangência, os limites e os objetivos da auditoria. (AUDIBRA 1991, p. 228)

Estatutário - regime jurídico dos servidores públicos que são regidos por estatuto.

Falha - ausência eventual, por lapso ou outro motivo não desejado, de um passo ou providência. (AUDIBRA 1991, p. 228)

Follow-Up - Análise posterior à auditoria realizada, quando o auditor retorna à entidade auditada (ou procede à análise à distância) para verificação da aplicabilidade das recomendações inseridas no relatório de auditoria. É o instrumento para assegurar a alta administração que as recomendações da auditoria foram implementadas e também serve para validar os resultados obtidos pela Auditoria Interna. (AUDIBRA 1991, p. 352)

Fundação Pública - instituída pelo Poder Público, é uma entidade dotada de personalidade jurídica de direito privado, com patrimônio próprio, criação autorizada por lei, escritura pública e estatuto registrado e inscrito no Registro Civil das Pessoas Jurídicas, com objetivos de interesse coletivo. (PISCITELLI 1997, p. 43)

Independência - a liberdade da entidade de auditoria em auditar e em atuar de acordo com o seu mandato de auditoria sem direcionamento ou interferência externa de qualquer tipo. (AUDIBRA 1991, p. 230)

Log - arquivo em disco ou fita no qual são registrados todos os fatos relevantes relativos ao processamento de uma transação. Muito útil para a recuperação de informações para fins de auditoria ou recuperação após falhas. (TCU 1998, p. 92)

Manual de Auditoria - contém os princípios básicos de atuação do auditor, procurando relatar as atividades como elas ocorrem, escolhendo dentre as várias encontradas, a que melhor expectativa oferece à prática de auditoria. Ainda que estabeleça diretrizes, não inibe a criatividade do auditor, ficando ao arbítrio deste a decisão quanto à extensão e à profundidade do exame, conforme as circunstâncias o

exigirem. (AUDIBRA 1991, p. 25-26)

Microcomputador - um pequeno, mas completo, sistema de computação composto de *hardware* e *software*. (TCU 1998, p. 57)

Plano Anual de Auditoria - documento em que serão discriminados os trabalhos programados para cada área ou sistema no ano corrente. (AUDIBRA 1991, p. 85)

Plano Plurianual - estabelece as diretrizes, objetivos e metas da administração para as Despesas de Capital e outras delas decorrentes e para as relativas aos programas de duração continuada. (MACHADO JR. 1991, p. 58)

Procedimento - descrição lógica de um conjunto de ações necessárias para cumprir uma tarefa. (TCU 1998, p. 58)

Programa de Auditoria - estabelece a natureza, época da aplicação e extensão dos procedimentos de auditoria planejados, necessários para executar o plano de auditoria. Serve como conjunto de instruções para controlar a execução adequada do trabalho. (IBRACON 1997, p. 13)

Programa de Computador - conjunto de instruções escritas em alguma linguagem de computação, cujo objetivo é realizar uma tarefa útil ao ser executado em um computador. (TCU 1998, p. 59)

Relatório de Auditoria - opinião escrita do auditor e outras observações sobre um conjunto de demonstrações financeiras ou outras informações que sejam objeto da auditoria específica. (AUDIBRA 1991, p. 345)

Tecnologia da Informação - aplicação de ciência e engenharia no desenvolvimento de máquinas e procedimentos com o objetivo de melhorar as condições humanas de alguma forma. É o conjunto formado pelos sistemas de computador (*hardware*), telecomunicações, programas de computador (*software*) e bancos de dados, sendo quantificáveis e qualificáveis. (TCU 1998, p. 62)

Teste - execução de um programa, sistema ou rotina com intuito de identificar suas falhas. Prova para determinar a qualidade, funcionamento, legalidade, correção de cálculo ou desempenho sob certas condições. (TCU, 1998, p. 63)

ANEXOS

ANEXO A- QUESTIONÁRIO APLICADO AO AUDITOR- CHEFE

ANEXO B- QUESTIONÁRIO APLICADO AOS AUDITORES

ANEXO C- ESTRUTURA ORGANIZACIONAL DA PMBH

ANEXO A: QUESTIONÁRIO APLICADO AO AUDITOR- CHEFE

QUESTIONÁRIO DE PESQUISA

Responsável: Maria Fernanda de Moraes

Objetivo: Objeto de Pesquisa para a Dissertação a ser defendida ao Curso de Mestrado em Administração Pública, área de concentração em Tecnologias da Informação, da Escola de Governo de Minas Gerais - Fundação João Pinheiro.

Instruções para o preenchimento do questionário

1. As questões estão divididas em tópicos e devem ser respondidas na sequência.
2. Não deixe questão sem resposta e justifique todas que forem solicitadas.
3. Considere:

AUDIM = Auditoria do Município

PMBH = Prefeitura Municipal de Belo Horizonte.

4. As informações sobre o servidor solicitadas ao final do questionário são apenas para efeito de tabulação.
5. Solicita-se que o questionário seja respondido no prazo de cinco dias úteis.
6. E finalizando, seja sincero e consciente, pois, sua participação é indispensável.

Muito obrigada!

I _ SISTEMAS DE INFORMAÇÕES MUNICIPAIS

1.1 A PMBH vem implementando sistemas informatizados nas diversas áreas da Administração Municipal. Cite os principais sistemas existentes.

1.2 Esse ambiente informatizado requer controles internos rigorosos?

☐ Sim ☐ Não ☐ Não sei
Justifique.

1.3 Os sistemas informatizados existentes são seguros e as informações geradas são confiáveis?

☐ Sim ☐ Não ☐ Não sei
Justifique.

II _ TRABALHOS DE AUDITORIA

2.1 Durante o período de 1994 a 2001, qual o quantitativo de trabalhos de Auditoria de Sistemas a AUDIM realizou?

2.2 A utilização de informações provenientes de sistemas informatizados, que não foram auditados, pode comprometer a qualidade e/ou o resultado dos trabalhos de Auditoria?

☐ Sim ☐ Não ☐ Não sei
Justifique.

2.3 A AUDIM utiliza dados e informações provenientes dos sistemas informatizados da PMBH para a realização dos seus trabalhos de Auditoria?

☐ Sim ☐ Não ☐ Às vezes
Justifique.

2.4 A Auditoria de Sistemas é um instrumento importante para a qualidade e segurança dos sistemas de informação?

☐ Sim ☐ Não ☐ Não sei

Justifique.

2.5 A AUDIM mantém manuais, roteiros e técnicas próprias de Auditoria de Sistemas?

☐ Sim ☐ Não

Justifique.

2.6 A PMBH vem implementando sistemas informatizados para controlar e gerar informações necessárias à tomada de decisões dos gestores municipais. Diante esta realidade, o que a AUDIM, como órgão de controle interno, vem promovendo para que estes gestores utilizem informações confiáveis e oportunas produzidas por esta tecnologia?

2.7 Há algum planejamento para inserir ou ampliar a realização de Auditoria de Sistemas pela AUDIM?

☐ Sim ☐ Não

No caso de resposta afirmativa, qual a previsão da implementação deste plano estratégico e quais as principais medidas a serem adotadas?

2.8 A AUDIM mantém articulação ou contato com auditorias internas de outros órgãos governamentais?

☐ Sim ☐ Não

No caso de resposta afirmativa, citar quais órgãos.

III_ CAPACITAÇÃO DOS AUDITORES MUNICIPAIS

3.1 Dentre o corpo técnico de Auditores Municipais, existem profissionais capacitados para desenvolverem Auditoria de Sistemas?

☐ Sim ☐ Não

No caso de resposta afirmativa, mensurar o quantitativo de profissionais e citar o tipo de capacitação (experiência profissional anterior, graduação, especialização, mestrado, outros cursos).

No caso de resposta negativa, qual a qualificação ideal?

3.2 Há investimento com recursos orçamentários da AUDIM em treinamento (cursos, seminários, congressos) dos Auditores na área de Auditoria de Sistemas?

☐ Sim ☐ Não

No caso de resposta afirmativa, mensurar o quantitativo de profissionais e citar o tipo de treinamento.

3.3 E em outras áreas, há investimento com recursos orçamentários da AUDIM em treinamento dos Auditores?

☐ Sim ☐ Não

No caso de resposta afirmativa, mensurar o quantitativo de profissionais e citar o tipo de treinamento.

3.4 Há iniciativa dos Auditores em ingressar na área de Auditoria de Sistemas?

☐ Sim ☐ Não ☐ Não sei

No caso de resposta afirmativa:

Mensurar o quantitativo de profissionais e citar o tipo de iniciativa (projeto de pesquisa, planejamento e trabalho de auditoria).

Qual o apoio dado pela AUDIM a este(s) Auditor(es)?

3.5 O acervo bibliográfico da AUDIM conta com alguma publicação sobre a Auditoria de Sistemas?

☐ Sim ☐ Não ☐ Não sei

No caso de resposta afirmativa, citar os títulos que constituem o acervo.

IV - INFORMAÇÕES SOBRE O SERVIDOR

4.1 Cargo:

4.2 Tempo de Serviço no Cargo: ____ anos e ____ meses.

4.3 Escolaridade:

Graduação

☐ Ciências Contábeis

☐ Outra: _____

Pós-Graduação

Tipo (*Lato Sensu, Strictu Sensu*):

☐ Concluído _____ (ano) ☐ Em curso

Área de Concentração e Entidade Realizadora:

4.4 Data do Preenchimento: ____/____/2001

ANEXO B- QUESTIONÁRIO APLICADO AOS AUDITORES

QUESTIONÁRIO DE PESQUISA

Responsável: Maria Fernanda de Moraes

Objetivo: Objeto de Pesquisa para a Dissertação a ser defendida ao Curso de Mestrado em Administração Pública, área de concentração em Tecnologias da Informação, da Escola de Governo de Minas Gerais - Fundação João Pinheiro.

Instruções para o preenchimento do questionário

7. As questões estão divididas em tópicos e devem ser respondidas na sequência.

8. Não deixe questão sem resposta e justifique todas que forem solicitadas.

9. Considere:

AUDIM = Auditoria do Município

PMBH = Prefeitura Municipal de Belo Horizonte.

10. O questionário deve ser respondido **individualmente**.

11. As informações sobre o servidor solicitadas ao final do questionário são apenas para efeito de tabulação.

12. Esta pesquisa não será divulgada individualmente, seus resultados serão apresentados agregados.

13. Solicita-se que o questionário seja respondido no prazo de **cinco dias úteis**.

14. E finalizando, seja sincero e consciente, pois, sua participação é indispensável.

Muito Obrigada!

I _ SISTEMAS DE INFORMAÇÕES MUNICIPAIS

1.4 A PMBH vem implementando sistemas informatizados nas diversas áreas da Administração Municipal. Cite os principais sistemas existentes.

1.5 Esse ambiente informatizado requer controles internos rigorosos?

☐ Sim ☐ Não ☐ Não sei

Justifique.

1.6 Esses sistemas informatizados são seguros e as informações geradas são confiáveis?

☐ Sim ☐ Não ☐ Não sei

II _ TRABALHOS DE AUDITORIA

2.9 Durante o período de 1994 a 2001, qual o quantitativo de trabalhos de Auditoria de Sistemas você realizou para a AUDIM?

2.10 A utilização de informações provenientes de sistemas informatizados, que não foram auditados, podem comprometer a qualidade e/ou o resultado dos trabalhos de Auditoria?

☐ Sim ☐ Não ☐ Não sei

2.11 Você utiliza informações provenientes dos sistemas informatizados da PMBH para a realização dos seus trabalhos de Auditoria?

☐ Sim ☐ Não ☐ Às vezes

Justifique.

2.12 A Auditoria de Sistemas é um instrumento importante para a qualidade e segurança dos sistemas de informação?

☐ Sim ☐ Não ☐ Não sei

Justifique.

2.13 Você já utilizou manuais, roteiros e técnicas próprias de Auditoria de Sistemas?

☐ Sim

☐ Não

Justifique.

2.14 A PMBH vem implementando sistemas informatizados para controlar e gerar informações necessárias à tomada de decisões dos gestores municipais. Diante desta realidade, o que a AUDIM, como órgão de controle interno, vem promovendo para que os gestores utilizem informações confiáveis e oportunas produzidas por esta tecnologia?

III_ CAPACITAÇÃO DOS AUDITORES MUNICIPAIS

3.6 Você se considera um profissional capacitado para desenvolver Auditoria de Sistemas?

☐ Sim

☐ Não

Justifique.

No caso de resposta afirmativa, citar o tipo de capacitação (experiência profissional anterior, graduação, especialização, mestrado, outros cursos) e o período da realização.

3.7 Você já participou de treinamentos (cursos, seminários, congressos) na área de Auditoria de Sistemas, oferecidos pela AUDIM?

☐ Sim

☐ Não

No caso de resposta afirmativa, citar o tipo de treinamento e a data da realização.

3.8 E em outras áreas, você já participou de treinamentos oferecidos pela AUDIM?

☐ Sim

☐ Não

No caso de resposta afirmativa, citar o tipo de treinamento e a data da realização.

3.9 Houve iniciativa de sua parte em ingressar na área de Auditoria de Sistemas?

☐ Sim ☐ Não

No caso de resposta afirmativa:

Citar o tipo de iniciativa (solicitação de treinamentos à AUDIM, treinamentos por conta própria, desenvolvimento de trabalho técnico ou científico).

Qual o apoio dado pela AUDIM a sua iniciativa?

3.10 Nos últimos doze meses você leu algum artigo, livro, monografia, dissertação ou tese sobre o tema Auditoria de Sistemas?

☐ Sim ☐ Não

No caso de resposta afirmativa, citar o título, autor e a entidade que publicou a obra.

3.11 O acervo bibliográfico da AUDIM conta com alguma publicação sobre o tema Auditoria de Sistemas?

☐ Sim ☐ Não ☐ Não sei

No caso de resposta afirmativa, citar os títulos que constituem o acervo.

IV - INFORMAÇÕES SOBRE O SERVIDOR

4.5 Nome: _____

4.6 Cargo: Auditor

4.7 Tempo de Serviço no Cargo: _____ anos e _____ meses.

4.8 Escolaridade:

Graduação

☐ Ciências Contábeis

☐ Outra: _____

Pós-Graduação

Tipo (*Lato Sensu, Strictu Sensu*):

☐ Concluído _____ (ano) ☐ Em curso

Área de Concentração e Entidade Realizadora:

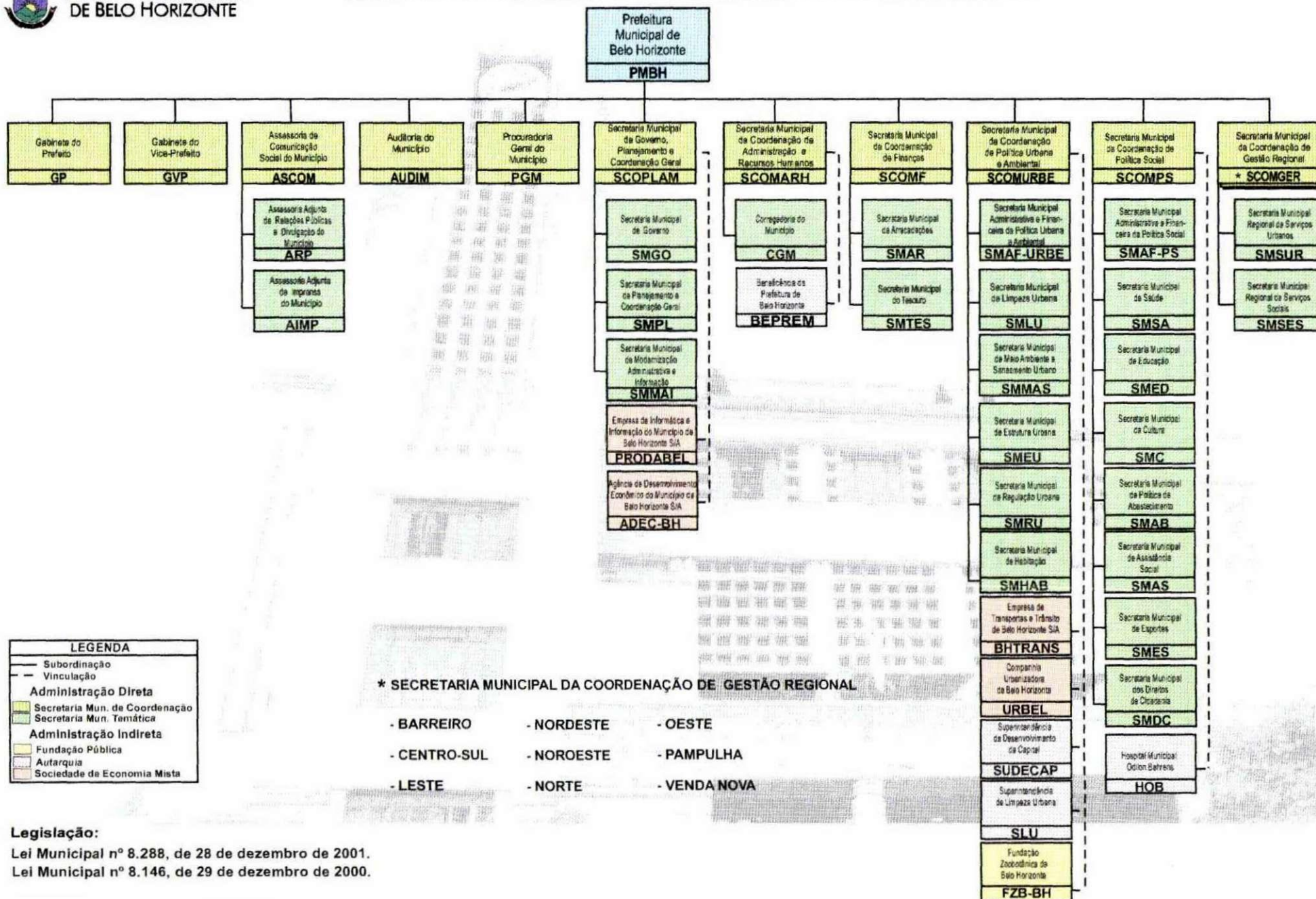
4.9 Data do Preenchimento: ____/____/2001

ANEXO C- ESTRUTURA ORGANIZACIONAL DA PMBH



PREFEITURA MUNICIPAL
DE BELO HORIZONTE

ESTRUTURA ORGANIZACIONAL DA PREFEITURA MUNICIPAL DE BELO HORIZONTE



Legislação:

Lei Municipal nº 8.288, de 28 de dezembro de 2001.

Lei Municipal nº 8.146, de 29 de dezembro de 2000.

ESCOLA DE GOVERNO

Alameda das Acácias, 70 - São Luís - Pampulha
Belo Horizonte - Minas Gerais - Brasil
CEP: 31275-150

Telefones

Diretoria Geral: 448 9713

Diretoria Adjunta: 448 9713

Secretaria Geral: 448 9593 - 448 9591

Secretaria de Ensino: 448 9595

Superintendência de Ensino: 448 9592

Superintendência de Extensão: 448 9594

Súp. de Pesquisa e Pós-Graduação: 448 9640

Fax: (031) 448 9613

E.mail: escgov@fjp.gov.br