

UNIVERSIDADE FEDERAL DO CEARÁ

FACULDADE DE ECONOMIA, ADMINISTRAÇÃO, ATUÁRIA E CONTABILIDADE

CURSO DE CIÊNCIAS CONTÁBEIS

AUDITORIA DE SISTEMAS INFORMATIZADOS

Renee Andrade Amorim

Fortaleza, Fevereiro de 1999

AUDITORIA DE SISTEMAS INFORMATIZADOS

Renee Andrade Amorim

Orientador: Prof. Vicente Lima Crisóstomo

Monografia apresentada à
Faculdade de Economia,
Administração, Atuária e
Contabilidade, para
obtenção do grau de
Bacharel em Ciências
Contábeis.

Fortaleza-CE

1999

Esta monografia foi submetida à Coordenação do Curso de Ciência Contábeis, como parte dos requisitos necessários à obtenção do título de Bacharel em Ciências Contábeis, outorgado pela Universidade Federal do Ceará – UFC e encontra-se à disposição dos interessados na Biblioteca da referida Universidade.

A citação de qualquer trecho desta monografia é permitida, desde que feita de acordo com as normas de ética científica.

<hr/> <p>Renee Andrade Amorim</p> <hr/>	Média
<hr/> <p>Prof. Vicente Lima Crisóstomo Prof. Orientador</p> <hr/>	Nota
<hr/> <p>Prof.(a) RUTH P. PINHO..... Membro da Banca Examinadora</p> <hr/>	Nota
<hr/> <p>Prof.(a) PRETEXTATO S. D. G. DE O. MELLO Membro da Banca Examinadora</p> <hr/>	Nota

Monografia aprovada em 03 de março de 1999

AGRADECIMENTOS

A DEUS, que sempre me deu força para seguir em frente nas horas mais difíceis.

Ao professor Vicente Lima Crisóstomo pelo incentivo e sugestões dadas na realização desse trabalho.

Aos meus pais, Francisco Alberto Monte Amorim e Maria Goreth Andrade Amorim pela educação, o amor e a compreensão que têm me proporcionado em toda a minha vida.

À minha irmã Christiani Andrade Amorim e ao meu cunhado Sérgio Roberto Mapurunga pelo exemplo que são.

À memória do meu avô Godofredo Marques de Andrade.

À minha amiga Raquel Nunes por toda sua fraternidade e amizade acolhedora nesses quatro longos anos de faculdade.

Aos demais que de alguma forma contribuíram na elaboração desta monografia.

SUMÁRIO

AGRADECIMENTOS	III
SUMÁRIO	IV
RESUMO	VI
1. INTRODUÇÃO	01
2. AUDITORIA: UM BREVE HISTÓRICO	02
1.1 Auditoria de Sistemas: sua evolução	05
3. CONCEITOS	10
4. AUDITORIA DE SISTEMAS: TIPOS	14
4.1 Auditoria Operacional	14
4.2 Auditoria de Sistemas	16
4.2.1 Auditoria de Sistemas “em torno” do computador	18
4.2.2 Auditoria de Sistemas “através” do computador	18
4.2.3 Auditoria de Sistemas: que tipo escolher ?	19
5. APLICANDO A AUDITORIA DE SISTEMAS “ATRAVÉS” DO COMPUTADOR	22
5.1 Auditando sem usar o computador	23
5.1.1 Peculiaridades	24
5.1.2 Quando auditar sem usar o computador	26
5.1.3 Requisitos básicos	26
5.1.3.1 Planejamento	27
5.1.3.2 Uso de listagens de erros	27
5.1.4 Vantagens e desvantagens	28
5.2 Auditando com o computador	28
5.2.1 Etapas da Auditoria de sistemas “com ” o computador	29
5.2.2 O computador como ferramenta de trabalho do auditor	31
5.2.3 Técnicas de auditoria de computador	32
5.2.3.1 Técnicas para testar os controles dos programas de computador	33
5.2.3.1.1 Método “test data”	33
5.2.3.1.2 Método Base Case System Evaluation”	36
5.2.3.1.3 Simulação Paralela	36
5.2.3.1.4 “Integrated Test Facility” – ITF	37
5.2.3.2 Técnicas para analisar os programas de computador	37
5.2.3.2.1 SNAPSHOT	37
5.2.3.2.2 Mapeamento estatístico dos programas do computador	39
5.2.3.2.3 Rastreamento do programas de computado (tracing)	39
5.2.3.2.4 Fluxograma de controles	40
5.2.4 Pacotes de software de auditoria	42
5.2.4.1 Características e funções	42
6. AUDITANDO SISTEMAS EM OPERAÇÃO	43
6.1 Origem da transação	44
6.1.1 Áreas de controle	45
6.2 Entrada de transação no PED	46
6.2.1 Áreas de controle	47
6.3 Comunicação de dados	48
6.3.1 Áreas de controles	48

BRUNO

6.4 Processamento no computador	49
6.4.1 Áreas de controle	49
6.5 Armazenamento e recuperação de dados	49
6.5.1 Áreas de controle	49
6.6 Saídas do processamento	50
6.6.1 Áreas	50
7. CONCLUSÃO	53
8. BIBLIOGRAFIA CONSULTADA	54

RESUMO

Desenvolve-se um histórico tanto da Auditoria propriamente dita, como da evolução da Auditoria de Sistemas, procurando evidenciar os fatos mais marcantes.

Conceitua-se, então, os principais tipos de Auditoria de Sistemas, a fim de melhor situar a Auditoria de Sistemas “através” do computador, apresentando suas técnicas e ferramentas disponíveis ao auditor para realização destas auditagens.

Discorre-se, a partir daí, à respeito da aplicação da Auditoria de Sistemas “através” do Computador nos sistemas informatizados em operação.

1. INTRODUÇÃO

A sempre crescente evolução da informática que acompanhamos há quase quarenta anos tem levado as empresas a, gradativamente, substituir uma infinidade de processos manuais por sistemas computadorizados.

Deste modo, o computador vem adquirindo um papel fundamental na vida das organizações, estimulando mais e mais estudos, pesquisas e serviços voltados a sua utilização.

Como a principal função do auditor é proteger os ativos da companhia, fazendo uso de técnicas adequadas para avaliação dos controles existentes, sua posição junto aos procedimentos computadorizados se faz extremamente necessária.

O auditor vem encontrando assim grande aplicação de seus conhecimentos nas tarefas de auditoria de sistemas informatizados, tanto na elaboração e desenvolvimento destes “softwares” como em sua fase de operação. Isso talvez possa ser explicado como o resultado de muitos casos de colapsos de controles, fraudes, roubos de dados, etc.

2. AUDITORIA: BREVE HISTÓRICO

É praticamente impossível concebermos nosso mundo de hoje, com sua economia globalizada, empresas transnacionais e capital volante dos megainvestidores passeando pelos países em questão de segundos, sem a instituição Auditoria. É elemento indispensável nas operações financeiras: envolve bancos, o próprio governo, fornecedores, investidores, empresas em processo de cisão, fusão ou incorporação, etc. Enfim, pode-se afirmar que a Auditoria, nesses tempos de grande instabilidade econômica representa a palavra final na hora de se fechar um bom negócio.

No entanto, os primeiros indícios do processo de Auditoria datam bem antes do desenvolvimento do capitalismo. A civilização Suméria, povo do Antigo Oriente que habitava o vale do rio Eufrates, já se utilizava de sistema semelhante. Os proprietários dos grandes campos de trigo e outros cereais confiavam sua produção aos comerciantes locais. Ao final da venda da safra, técnicos avaliavam se a importância arrecadada realmente condizia com o volume de cereais negociado.

Não se sabe ao certo de onde proveio originalmente o termo Auditor. Tem-se registros de que no final do século XIII, mais precisamente em 1285, na Inglaterra, Eduardo I mencionava o termo Auditor quando referia-se àqueles funcionários contratados pelo reino com a finalidade de avaliar a real constituição patrimonial dos cidadãos. Estes, por sua vez, eram obrigados a uma declaração fidedigna dos bens que possuíam, documento o qual os Auditores analisavam. A pena para quem sonegava ia desde multas altíssimas a castigos corporais.

Com a evolução da ciência contábil a partir do advento do método das partidas dobradas elaborado pelo frei italiano Luca Pacioli em 1494, as associações profissionais que se incumbiam de executar os exames dos atos e fatos contábeis tiveram que se amoldar ao progresso da contabilidade e assim também o fizeram, por exemplo, o Tribunal de Contas de Paris, o Colégio dei Raxonati de Veneza, a

Academia dei Ragionieri de Milão, todos esses institutos que exerciam funções de Auditoria na época.

Mas é no século XVIII que a Auditoria vem a consolidar-se como uma ferramenta realmente útil nas operações comerciais. A Revolução Industrial reequacionou a economia européia da época, fazendo com que as atividades econômicas evoluíssem de artesanais para empresariais. Assim, houve um grande acúmulo de riquezas pelas entidades com fins lucrativos, o volume de negócios aumentou em larga escala e, por conseguinte, veio a necessidade de se controlar os novos atos e fatos contábeis que o processo industrial envolvia. Portanto, a contabilidade passa novamente por um processo de adaptação ao progresso econômico, fazendo também com que a auditoria se aperfeiçoasse mais uma vez.

Dáí em diante, a Auditoria se especializa. A conquista do oeste norte-americano exerceu papel primordial nesse desenvolvimento. As grandes companhias, principalmente de estradas de ferro que se organizavam com capital do leste do país, tinham de oferecer alguma forma de segurança a seus investidores impossibilitados de acompanhar de perto suas aplicações. Por essa razão, o “Railway Companies Consolidation Acts” (Consolidação das Leis de Estradas de Ferro) em 1845 obrigava que os balanços anuais dessas companhias fossem examinados por auditores.

Com o aparecimento e proliferação de muitos profissionais incompetentes e negligentes, surge a preocupação de se criar associações com a finalidade de resguardar o respeito, a confiança e a imagem do auditor. Assim, surgem as primeiras associações na Escócia e na Inglaterra e, depois, em vários países da Europa. Os auditores que quisessem exercer sua profissão tinham de pertencer a estas instituições de classe que, ao mesmo tempo que controlavam o exercício de sua profissão, conferiam títulos a seus associados, habilitando-os legalmente. É, então, criada em 1853 a Sociedade dos Contadores de Edimburgo, a primeira instituição formada por contadores, portanto. Na América, a organização mais difundida é a “American Institute of Certified Public Accountants” (Instituto

Americano dos Contadores Públicos Certificados) fundada em 1887. Hoje, conta com milhares de auditores como membros e é responsável por importantes pronunciamentos técnicos a respeito da ciência contábil.

No Brasil, a Auditoria chegou por volta de 1940, a tiracolo das grandes companhias multinacionais que aqui começavam a se instalar. Os escritórios de auditores dessas empresas foram abertos no decorrer do tempo, treinando cada vez mais auditores brasileiros.

Até 1946, a atividade de auditoria no Brasil praticamente não existia, exceto em empresas estrangeiras, como uma continuidade dos hábitos adotados por suas matrizes. A esta altura só se recorria aos contadores de maior gabarito profissional, quando se desejava apurar alguma fraude, esclarecer suspeita de desfalque ou falência fraudulenta. Era basicamente um trabalho pericial, bem diferente de uma auditoria.

A partir desse mesmo ano, com o advento do Decreto Lei No. 9295 que regulamentou a profissão de contador no Brasil, nos moldes atuais, estabeleceu-se para o contador a prerrogativa de exclusividade na execução dos trabalhos de auditoria e perícia.

Para o desenvolvimento da auditoria no Brasil, o decreto-lei No. 9205/46 teve o indiscutível mérito de preservar a qualidade dos trabalhos, a partir do momento que exigiu maior qualificação técnica para profissionais executores, reservados aos bacharéis em ciência contábeis o direito de praticar a auditoria. Ainda hoje, as regras estabelecidas pelo referido decreto-lei encontram-se em pleno vigor, de sorte que os contadores brasileiros contam com prerrogativas legais bem mais amplas do que aquelas conquistadas por seus colegas de países economicamente mais adiantados. É interessante notar que, na Grã-Bretanha, pátria mãe da auditoria, não há regulamentação tão poderosa a favor dos contadores.

Em 1960, os auditores se organizaram em associação de classe, que se chamou de “Instituto dos Contadores Públicos do Brasil”, que em 1971, já com uma estrutura bastante respeitável mudou de nome para “Instituto de Auditores Independentes do Brasil” e depois para IBRACON (Instituto Brasileiro de Contadores), o qual foi legalmente reconhecido através da resolução No. 317, do conselho Federal de Contabilidade e da Resolução No. 220, do Banco Central do Brasil.

Do lado governamental a profissão foi formalizada e exigida principalmente após a publicação da Lei No. 4.728 de 14-07-1965, a primeira Lei de Mercado de Capitais, que exigia que as companhias que tinham ações negociadas em bolsa de valores publicassem, juntamente com suas demonstrações financeiras, o parecer dos auditores independentes.

A Circular No. 179, do Banco Central do Brasil, baixou Normas Gerais de Auditoria e Princípios e Normas de Contabilidade, simultaneamente à Resolução No. 321/72 do CFC. No entanto, a Lei No. 6.404, de 15-11-1976, que dispões sobre as sociedades por ações e o decreto-lei No. 1598 de 26-12-1977, representam os dois trabalhos mais importantes para a evolução da profissão no Brasil, porque, além dos princípios contábeis neles contidos, ainda consolidaram a presença dos auditores nas sociedades anônimas de capital aberto.

2.1 Auditoria de Sistemas: Sua evolução

Crescer ou morrer. Foi esse o dilema enfrentado pelas empresas nas últimas décadas. O mercado cada vez mais se ampliava, as oportunidades surgiam de toda a parte, a concorrência se fortalecia, a quantidade de dados a manipular tomava um vulto impossível de ser controlado pelas formas convencionais. Rotinas mais sofisticadas eram necessárias e o PED oferecia todas as conveniências, como: a facilidade no tratamento de grandes volumes de informações, a velocidade de operação e a confiabilidade dos resultados.

Em meados da década de 70, iniciou-se uma grande corrida por parte das organizações financeiras pelo uso do computador. As poucas indústrias de informática da época, como IBM, UNIVAC e BULL, não supriam demanda tão latente. Estavam sempre abarrotadas de pedidos, os quais tinham seus prazos de entrega dilatados. O preço alto cobrado por parte destas indústrias contrastava com a qualidade e a assistência oferecida ao produto elaborado finalmente. Os *softwares* e os técnicos relacionados também deixavam a desejar. Pacotes de programas ainda não eram tão populares até então e sua aquisição, quase sempre mal sucedida, implicava na necessidade de mão-de-obra especializada, que era escassa. Houve uma explosão de cursos e *bureaus* para a formação de analistas e programadores. No entanto, era grande a carência de estrutura, organização e bons professores da área. O nível dos formandos destes estabelecimentos era baixo e deixava a desejar, restando para o estudante adquirir boa parte do conhecimento em sua vida profissional. Apesar de tudo, foi essa geração de técnicos, mal preparada e assessorada que, com esforço, tentativas e autodidatismo e experiência atendeu às exigências do progresso e implantou os sistemas.

A evolução dos sistemas informatizados aplicativos deu-se sob um processo relativamente rápido, mas, digamos tortuoso. Em menos de trinta anos, as empresas moldaram a informática de acordo com seus interesses e necessidades. Adaptaram sistemas informatizados em grande parte de seus setores, aumentando a produtividade consideravelmente.

No entanto, o processo contínuo de busca por sistemas seguros, eficazes e eficientes esbarrou num conjunto de fatores desconhecidos, pelos analistas, porém preponderantes na elaboração destes *softwares*.

Algumas variáveis esquecidas ou desconhecidas, na implantação dos sistemas foram gerando conseqüências, as mais desagradáveis. Pouco ou nenhuma importância havia sido dedicada à questão de segurança e, menos ainda, à possibilidade de futuras alterações das rotinas.

Poucos aspectos de segurança, a princípio, foram considerados. O CPD era localizado ao rés do chão, com largas portas envidraçadas, independentemente da vizinhança, e construindo de madeira, tapetes e cortinas. Mínimos cuidados eram dispensados a cabos e fios que transportavam energia elétrica e, nenhuma restrição havia ao acesso de estranho ou à saída de objetos.

A segurança lógica era também negligenciada. Ninguém se preocupava em prevenir possíveis erros de usuário, falhas de *hardware*, de *software* básico, de programas de aplicação ou de procedimentos de proteção aos dados.

E outras causas, não menos graves atuavam para degradar a qualidade de alguns sistemas, encurtando seu ciclo vital e levando-os, muito cedo, ao obsoletismo. A rapidez com que se mudam as leis e as políticas no país fez com que qualquer rotina logo se transformasse numa colcha de retalhos, com emendas por todos os lados, mostrando a pressa com que foi feita a alteração. Por exemplo, uma folha de pagamento implantada em janeiro de 1986, já operou com quatro padrões monetários, 5 leis salariais, mudanças no tratamento das alíquotas do Imposto de Renda (IR), do FGTS, da Previdência, etc. Sem falar que , nesse período a empresa também deve ter mudado suas próprias políticas para se adequar ao mercado.

Vacilava-se muito no tocante à preparação das rotinas. Não se previam suas alterações futuras. Uma simples mudança na alíquota de IR ou da Previdência demandava muito tempo, com mexidas nos programas, recompilações, testes e implantações, com riscos de erros muito graves.

Tais mudanças implicavam numa degradação da eficiência dos sistemas e diminuían sua segurança. A primeira medida importante tomada pelo mercado, em todo mundo, visando implementar segurança no PED e nos sistemas implantados ocorreu, no início dos anos 70 no Canadá. Numa iniciativa singular, *The Canadian Institute of Chartered Accountants* publicou em 1970 a primeira edição, em três volumes de seu trabalho denominado *Computer Control Guide Lines* . No Brasil, porém a obra passou por quase completo desconhecimento.

Nos anos 80, porém, a necessidade de solver problemas quanto às questões de PED impeliu o mercado brasileiro a esgotar em pouco tempo obras como Segurança do Computador (John M. Carrol, 1977), crime por Computador (Dam Parker, 1977), etc.

Paralelamente, escolas iniciaram a oferta de cursos especializados, com propostas ambiciosas. Foram atraídos por nosso mercado inúmeros técnicos estrangeiros que aqui tentaram passar seus conhecimentos e experiências. Muitos profissionais surgiram nesta época, porém não reuniam conhecimento o bastante para trabalharem completamente na área de informática e auditoria de sistemas. O auditor contábil, por sua vez, era inapto a julgar a segurança e a confiabilidade dos dados, a eficiência dos programas, ou para atestar que o sistema não sofria soluções de continuidade. Era preciso algo mais.

A solução proposta foi a contratação de assessores que conhecessem o processamento de dados. Mas, sem uma linguagem comum que unisse auditores e analistas, sem uma clara definição dos métodos de trabalho avançou-se pouco. E, por isto, a necessidade de aumentar a segurança e a eficiência dos sistemas, e a inexistência de metodologias adequadas provocaram o surgimento de um sem número de soluções, que o mercado era convencido a aceitar.

É a partir daí que vai se formando a figura do profissional de auditoria de sistemas. Concluiu-se finalmente que para a formação desse serviço especializadíssimo tal profissional deveria reunir conhecimentos básicos de Auditoria, avaliação de controles internos, informática e de funções desempenhadas pelos técnicos no CPD.

Algumas empresas, faculdades e, principalmente, o IAB (Instituto de Auditores do Brasil) tentaram resolver o problema da auditoria de sistemas, promovendo cursos e seminários buscando racionalizar e metodizar os procedimentos e valorizar a classe. Outro aspecto importante foi a criação do quadro de auditoria de

sistemas pelas empresas de auditoria independente. Para atender às exigências de seus maiores clientes, essas organizações puseram-se a contratar profissionais de informática, preparando-os com a transferência de conhecimentos adquiridos em outros ramos da auditoria e oferecendo-lhes treinamento, o mais vezes organizado e coordenado por técnicos estrangeiros.

3. CONCEITOS

A área de auditoria de sistemas compreende terminologia, conceituação e técnicas de três áreas distintas de conhecimento:

- Auditoria
- Sistemas de Informação
- Processamento Eletrônico de Dados

A área de processamento eletrônico de dados é aquela que começa com os conceitos de *hardware* e *software* e cresce enlaçando-se com a área de telecomunicação, exteriorizando as atividades da empresa sem ter necessidade de espaço físico.

Para melhor compreensão da área de processamento eletrônico de dados, podemos compô-lo da seguinte forma:

- a) **Hardware:** em linguagem simples, é a configuração do computador (CPU, Disco rígido (HD), periféricos, terminais, impressoras, etc)
- b) **Software básico:** conjunto de instruções e Programas de computador que cumprem as funções básicas de acionamento e controle do computador. Algumas vezes essas instruções são incorporadas ao próprio hardware, gerando o conceito de firmware.
- c) **Software de apoio:** conjunto de instruções e programas de computador que cumprem funções de uso freqüente e que podem ser padronizados para rapidez de acesso e uso. Neste contexto temos programas utilitários, gerenciadores de banco de dados, monitores de comunicação, etc.
- d) **Software aplicativo:** conjunto de instruções e programas escritos pelos programadores ou usuários de computação para conversão dos dados em informação, com a conseqüente solução do problema que enfrentam.
- e) **Teleprocessamento:** entrelaçamento da área de computação com a área de telecomunicações, permitindo a conexão de equipamentos de PED localizados a

grandes distâncias físicas. Permita que a área de computação atinja um espaço geográfico ilimitado e que a tecnologia de computadores se torne fisicamente presente nas mãos dos usuários.

A área de Sistemas de Informações corresponde a todos os processos exercidos e resultados apurados, segundo objetivos e necessidades operacionais do ser humano.

Segundo Gil (1993), sistemas de informações compreendem um conjunto de recursos humanos, materiais, tecnológicos e financeiros, combinados segundo uma seqüência lógica para transformar dados em informações .

Assim, temos:

- **Recursos humanos** → compreendem os usuários dos sistemas computadorizados (funcionários da área administrativa, da área de vendas ou da área industrial), os profissionais de computação (operadores de computador, analistas de sistemas, programadores, etc).
- **Recursos materiais** → tanto abrangem suprimentos (disquetes, formulários contínuos, etc.) quanto equipamentos (terminais, unidade central de processamento, impressoras, etc.) quanto instalações e utensílios (sala de operação, rede de energia elétrica, móveis, etc.);
- **Recursos tecnológicos** → correspondem ao intangível dos sistemas de informações, ou seja, são os softwares (programas informatizados) e as informações geradas. É importante destacar que os recursos tecnológicos vivem agregados a recursos humanos e a recursos materiais. Assim, o usuário (recurso humano) obtém da tela de seu terminal (recurso material) a informação de seu saldo bancário (recurso tecnológico).

ESFEAL

- **Recurso financeiro** → é a transformação de recursos humanos, materiais e tecnológicos, sendo o denominador comum a moeda.
- **Seqüência lógica** → exprime a idéia de dinamismo e compreende as tarefas ou atividades a serem cumpridas para a transformação do dado em informação. Corresponde, portanto, ao processo que é, por sua vez, um elenco de procedimentos manuais ou computadorizados (instrução de computador formando programas).
- **Dados e informações** → são estatísticos. São os resultados iniciais e finais dos processos executados.

A área de Auditoria implica a validação e a avaliação do controle interno de sistemas de informações em PED.

Entende-se por **Controle Interno** “o plano de organização e todos os métodos adotados numa empresa para proteger seu ativo, verificar exatidão e fidedignidade de seus dados contábeis, incrementar a eficiência operacional e promover a obediência às diretrizes administrativas estabelecidas.” (Fontes, 1991, p.34).

O controle interno corresponde ao exercício de um ou mais dos seguintes parâmetros:

- a) **Fidedignidade da informação em relação ao dado**: deve o auditor de sistemas validar e avaliar que informações (produto final), criadas por um sistema de informações computadorizado, são corretas em relação aos dados (matéria-prima) alimentadas por esse sistema. Em outras palavras, o auditor deve certificar-se de que não foram inseridos nem perdidos dados ou informações semi-elaboradas durante o processo de transformação do dado em informação.
- b) **Segurança física** : corresponde à constatação de bom estado operacional dos recursos humanos (condições de saúde, ergonomia, sistemas de proteção) e dos

recursos materiais (instalações, hardware, suprimentos) que compõe e dão sustentação aos sistemas de informações computadorizadas.

- c) **Segurança lógica:** diz respeito a alterações, modificações ou erros dos recursos tecnológicos (processos e resultados) componentes de certo sistema de informação computadorizado.
- d) **Confidencialidade:** compreende a quebra de sigilo do sistema computadorizado, seu processo e informações. É a captação, por entidade não autorizada, dos recursos tecnológicos componentes do ambiente computacional. Essa entidade não autorizada pode ser um recurso humano ou um recurso tecnológico.
- e) **Segurança ambiental:** implica a validação e a avaliação das condições de operacionalidade dos recursos humanos, materiais e tecnológicos componentes da infra-estrutura do centro de computação.
- f) **Obediência à legislação em vigor:** é o atendimento pelos sistemas de informações computadorizados à legislação federal, estadual e municipal.
- g) **Eficiência:** é a combinação ótima de recursos humanos, materiais e tecnológicos, impondo a melhor relação benefício/custo aos processos computacionais.
- h) **Eficácia:** abrange a avaliação do nível de satisfação do usuário do sistema computadorizado. Avalia-se se a informação foi gerada segundo os objetivos que determinam sua utilidade.
- i) **Obediência à política da alta administração:** consiste em verificar se o sistema computadorizado atende às normas vigentes, às diretrizes e políticas para a organização traçadas pela alta administração.

4. AUDITORIA DE SISTEMAS : TIPOS

De acordo com o objetivo com que é feita a auditoria, do grupo envolvido no trabalho ou da unidade funcional que está sendo auditada, muitos podem ser os tipos de auditoria de computador utilizados. Os títulos destas auditagens estarão sempre relacionados com o fim escolhido ou com a concepção do auditor ou examinador.

Dentro da auditoria de sistemas, basicamente, podemos relacionar duas áreas de aplicação, ambas interligando-se diretamente com os controles internos para os relatórios financeiros. São elas:

- **Auditoria Operacional**
- **Auditoria de Sistemas**

4.1 Auditoria Operacional

A auditoria operacional é, na verdade, a aplicação dos princípios de auditoria no exame do setor ou departamento de informática (Centro de Processamento de Dados - CPD) como uma unidade funcional restrita. O CPD é o departamento que administra os equipamentos, opera os sistemas e produz os resultados. Seu porte e organização dependem da empresa assim como a distribuição de *hardware/software*. O trabalho desenvolvido neste tipo de auditoria é semelhante ao que o auditor aplicaria em qualquer outra unidade funcional da empresa. O auditor evidenciará na auditoria operacional os seguintes itens:

- estrutura e organograma da organização;
- mapa de funções;
- atendimento às políticas gerais da empresa;
- critérios para medir e auferir o desempenho;
- custos do sistema e respectivos orçamentos;

- planificação dos projetos e procedimentos de controle;
- avaliação em profundidade do CPD, ao longo das linhas de serviços, tempestividade e utilização adequada dos recursos;
- aspectos relativos à segurança física e dos dados;
- análise geral dos sistemas utilizados, compreendendo sua operacionalidade, confiabilidade e controles de processamento;
- conhecimento das normas internas do CPD relacionadas à minimização de ações desautorizadas (fraudes, roubo de informações e dados, alterações danosas dos sistemas, etc.).
- controle dos dados de entrada e saída do sistema;
- procedimentos de emergência para os casos de catástrofes;
- manutenção de equipamentos e programas e
- pesquisa quanto à satisfação dos usuários com os serviços de informática.

A necessidade de auditoria de CPD pode ser constatada por alguns dos sintomas abaixo:

- atitudes hostis dos usuários frente ao CPD, que passa a ser responsabilizado por todas as dificuldades operacionais e administrativas enfrentadas pela empresa;
- descumprimento de prazos, cronogramas ou orçamento;
- omissão de etapas;
- falta de capacidade para atender com tempestividade as requisições da organização;
- histórico de interrupção ou suspensão de projetos que estavam sendo desenvolvidos;
- constantes requisições de expansão do parque de máquinas e softwares;
- novas necessidades dos usuários em razão da expansão da companhia;
- custos excessivos, etc.

Diante do exposto acima, conclui-se que a auditoria de operacional, basicamente, relaciona-se com a **segurança ambiental, obediência à legislação e às políticas da alta administração, eficiência e eficácia.**

Na realidade, o parâmetro segurança ambiental contempla os parâmetros segurança física dos recursos humanos e materiais, segurança lógica quanto à erros, fraudes, modificações de recursos tecnológicos e confidencialidade quanto a captação indevida de recursos tecnológicos, todos estes recursos componentes da infra-estrutura do centro de processamento de dados, ou, então, de uso comum por diversos sistemas de informações aplicativos computadorizados.

Os itens analisados na auditoria operacional, em sua grande maioria, não requerem substancial conhecimento em informática por parte do auditor encarregado, podendo ser até examinados com sucesso por auditores convencionais.

O fato de que um conhecimento em profundidade em PED não é requerido para todas as áreas a serem examinadas, é indicativo da razão por que a maioria das auditorias, feitas pelas firmas de auditores independentes, seja do tipo operacional.

4.2 Auditoria de Sistemas

Até bem recentemente a aplicação da auditoria operacional era feita mais freqüentemente que a auditoria de sistemas. No entanto, esta última vem se tornando bem mais popular que aquela, ultimamente. O fato deve-se a :

- o crescimento do grau de complexidade dos sistemas desenvolvidos;
- a necessidade de saber o que o sistema faz e com faz, tem também aumentado;
- roubo de informações, captura de dados por pessoas estranhas à empresa por meios ilícitos, etc. têm se tornado uma constata na vida das empresas;
- preservação da *audit trail* (trilha de auditoria);

- a relevância de testar-se a validade e a integridade dos sistemas e seus controles internos.

O termo “auditoria de sistemas” envolve todos os tipos de auditagens realizados no que diz respeito ao processo de desenvolver, controlar e auditar sistemas individuais.

As áreas de aplicação de auditoria de sistemas são, basicamente, duas:

1. Análise e levantamento dos sistemas através do ciclo de desenvolvimento. O processo deve ser anterior à formal adoção do sistema em estudo pela administração.
2. Análise dos sistemas importantes que já se encontram em operação (nível operacional). O auditor enfatiza o acompanhamento das atividades e transações, a validação e a integridade dos dados, podendo, inclusive, melhorar os controles e a segurança desses sistemas.

Os sistemas em desenvolvimento devem ser analisados em três fases distintas. A primeira dá-se mesmo antes do sistema ser aprovado pela administração, ou seja, na fase de viabilização. A partir daí o sistema estará sendo desenvolvido, devendo o auditor direcionar seu exame no que diz respeito à utilidade do sistema, sua programação e implantação. A última fase da auditoria de sistemas se dá quando o *software* se encontra em plena utilização. O auditor certifica-se aí se o sistema atende as especificações originais e se os objetivos foram atingidos.

A auditoria de sistemas em operação envolve a análise, revisão e o acompanhamento dos sistemas sob o ponto de vista da integridade dos programas, dados e arquivos; exatidão das transações e dos resultados produzidos, e adequação dos controles internos existentes no sistema, inclusive exame dos procedimentos de *interface* entre os usuários e o sistema.

Segundo Milko (1988), de acordo com a profundidade com que se pretende analisar o sistema e do nível de conhecimentos técnicos em informática por parte do auditor, a auditoria de sistemas pode ser realizada sob dois enfoques básicos:

- Auditoria de Sistemas “em torno” do computador e
- Auditoria de Sistemas “através” do computador.

4.2.1 Auditoria de Sistemas “em torno” do computador

A auditoria de sistemas em torno do computador tem seu processo iniciado com a escolha de sistemas representativos que realizam transações correntes dentro da empresa. Tais transações, primeiramente, devem ser analisadas pelo auditor ainda na faixa inicial, ou seja, nos documentos fontes. A análise segue as transações até os registros finais produzidos. A auditoria de sistemas “em torno” do computador objetiva principalmente verificar a integridade dos resultados obtidos. Assim, o auditor baseia-se na premissa de que se os dados-fontes ou entradas do sistema podem mostrar-se corretos, e desde que os resultados do sistema reflitam exatamente estes dados, então as saídas devem estar corretas e a maneira como o sistema processa os dados é de menor importância.

A auditoria de sistemas “em torno” do computador tem sido o método mais adotado, pois não requer conhecimento técnico do equipamento de informática. No entanto, apresenta a grande falha de não oferecer um bom nível de confiança nos resultados, em virtude de não ser examinada a correção de todos os componentes do sistema, assumindo que os mesmos não apresentam variações.

4.2.2 Auditoria de sistemas “através” do computador

Segundo Woodworth (78), a auditoria de sistemas “através” do computador baseia-se na premissa de que os resultados só podem ser aceitos se tanto as entradas quanto os processamentos foram examinados e julgados corretos.

Portanto, neste tipo de metodologia de análise serão verificadas os dados-fontes, enfatizando-se, principalmente, a revisão e os testes de procedimentos.

A auditoria de sistemas “através” do computador também envolve a técnica em que o próprio computador é utilizado para examinar ou selecionar os dados para testes do sistema. Podemos, inclusive, afirmar com segurança que o aumento da popularidade deste tipo de auditoria deve-se exatamente à efetiva utilização do computador como instrumento de trabalho do auditor.

A maior vantagem oferecida por este tipo de auditoria está na efetiva verificação dos programas do sistema. Isto exigirá do auditor, no entanto, perícia e tempo, pois será necessário o desenvolvimento de controles apropriados para evitar que os arquivos do sistema, e dados reais, sejam destruídos quando dos testes.

4.2.3 Auditoria de Sistemas: Que tipo Escolher ?

O tipo de auditoria a ser usado depende, primeiramente, do levantamento que o auditor fizer acerca dos sistemas em questão da empresa.

Algumas indagações devem ser feitas, como:

- a) Devemos fazer auditoria de ambos os tipos e por quê ?
- b) Se ambos, a qual deve ser dada preferência quando há limitações de mão-de-obra ?
- c) Quais os méritos relativos a cada tipo de auditoria ?

Em face do que foi posto na primeira questão, ambos os tipos de auditoria são importantes e devem ser feitos sempre que possível, quando se deseja total segurança e controle sobre o complexo de PED.

A auditoria Operacional cobre todas as áreas de do complexo de PED que, por sua vez, afetam todos os sistemas e atividades. Tal é o caso quando olhamos as práticas e procedimentos e quaisquer controles de processamento que afetam o sistema, estejam eles no estágio de desenvolvimento ou operacional.

Por exemplo, quando auditamos os padrões, a documentação, a gerência de projetos, os procedimentos de controle no CPD sua estrutura organizacional e separação de funções, estamos auditando aspectos importantes que influem decisivamente em todos os sistemas ou como atividades são conduzidos no departamento de PED.

No entanto, quando auditamos um sistema específico, digamos folha de pagamento, temos uma visão em profundidade daquele sistema, sem nos importarmos muito com os demais sistemas que possam influir naquele sob exame. Este tipo de auditoria nos dá uma visão em profundidade dos emaranhados de sistema em análise, mas não oferece uma visão multilateral como seria no caso da auditoria operacional.

Recentemente, a questão de qual tipo de auditoria deve ser preferido envolve um número de fatores que devem ser postos sob análise. No caso, por exemplo, de termos um pessoal pouco qualificado no que se diz respeito à informática, melhor seria a aplicação de auditoria operacional, pois não requer grande conhecimento em PED, restando ao Auditor já identificar possíveis áreas problemáticas no futuro.

Contudo, se o problema concentra-se nas, digamos, áreas que incorrem distúrbios, começar com a auditoria de sistemas deve ser o caminho mais lógico. É necessário porém, um conhecimento maior na área de PED e o objetivo do trabalho limitar-se-á ao sistema inspecionado.

Basicamente, no planejamento dos procedimentos de auditoria, o auditor deve determinar quando os propósitos de auditoria serão melhor servidos pelo teste

do sistema e em que circunstância a avaliação será melhor coordenada pelo exame de dados.

5. APLICANDO A AUDITORIA DE SISTEMAS “ATRAVÉS” DO COMPUTADOR

Nos primeiros estágios de desenvolvimento dos sistemas informatizados, pequenas mudanças foram necessárias nos métodos de auditoria. Inicialmente, os sistemas que eram realizados de forma manual foram simplesmente substituídos por sistemas computadorizados, sem grandes alterações. Registros e relatórios eram comumente convertidos para o computador como uma exata semelhança dos procedimentos manuais respectivos.

Os controles manuais existentes eram transportados para dentro do computador de tal modo que as operações de processamentos de dados ficavam quase que transparentes para o auditor. Em consequência os auditores simplesmente ignoravam o processamento de dados e continuavam com seus tradicionais procedimentos de auditoria.

Contudo, com a evolução da informática e com a multiplicação das oportunidades de aplicação do PED no dia-a-dia das empresas, provocaram profundas mudanças nos métodos de trabalho do auditor de sistemas. Agora, a maior ênfase dada era aos sistemas em si e aos controles dos programas.

Cada vez mais, temos um maior número de procedimentos manuais sendo substituídos por sistemas informatizados. Como exemplo clássico de ilustração dessa evolução, podemos citar o caso dos supermercados. Há alguns anos, as compras feitas nesses estabelecimentos eram registradas manualmente, uma a uma. Os sistemas computacionais dos mercantis de hoje lêem os preços das mercadorias através de leitor ótico, identificam o produto e a seção a qual pertencem, somam, e de acordo com a forma de pagamento, ligam para operadoras de cartão e até preenchem cheques, etc.

Os sistemas, ao longo do tempo, passaram então a se interligar, obrigando a alteração dos procedimentos de controle:

- a) com o aumento da quantidade de registros nos arquivos-mestre, sistemas automatizados têm sido projetados para exibir o conteúdo destes arquivos através da utilização de programas geradores de relatórios ou de procedimentos de acesso a terminais.
- b) O grande número de interligações entre os sistemas tem permitido que as transações alimentadas em um sistema possam eventualmente afetar outros sistemas, sem qualquer intervenção manual. Além disso, há casos em que condições de exceção provocam a geração de transações e registros sem analogia com os dados comandados;
- c) Como muitas organizações têm adotado processamento de transações usando comunicação de dados, com entradas através de pontos remotos, comandos individuais podem ser introduzidos pelos próprios usuários diretamente para os arquivos do sistema, sem qualquer tabulação ou conferência de totais.

De acordo com situações dessa natureza, a precisão e a segurança estão mais dependentes dos controles embutidos nos programas do que naqueles sistemas do passado. Em função disto, auditores de sistemas têm procurado avaliar mais detalhadamente esses controles e julgar se sua a segurança é realmente eficaz.

Dependendo do grau de complexidade do sistema a ser auditado e do nível de conhecimento de PED do auditor, os trabalhos de auditoria podem ser realizados com ou sem auxílio do computador.

5.1 Auditando sem usar o computador

A abordagem que passamos a introduzir agora leva em consideração que, apesar da não utilização do computador pelo auditor na condução de seus trabalhos,

ele deve considerar a estrutura dos controles sobre a qual os programas foram desenvolvidos.

5.1.1 Peculiaridades

A auditoria de sistemas de sem o uso do computador resume-se a, basicamente:

- 1) Levantamento do sistema com o objetivo de se conhecer a utilidade do mesmo e sua necessidade de controle;
- 2) Teste do sistema para o entendimento de como este realmente funciona;
- 3) Avaliação das saídas do sistema

Sistemas cujo processamento não seja relativamente muito complicado e que produzam saídas bem detalhadas, podem ser auditados sem a necessidade de verificação dos programas do computador.

Todos os registros do computador a serem analisados devem estar disponíveis em formatos impressos, ou, pelo menos, capazes de serem listados à medida que o auditor necessite. Portanto, um dos pontos de controles mais auditados é aquele correspondente ao parâmetro do controle interno EFICÁCIA, ou seja, a análise através dos relatórios emitidos pelo sistema de informação computadorizado.

É imprescindível o exame destes relatórios, pois é aí que será verificado o nível de satisfação dos usuários com:

- Natureza e correção das informações recebidas
- Forma de apresentação da informação em termos sintético ou analítico e de distribuição no relatório

A auditoria de um sistema através do teste de entradas e saídas, ao invés do teste dos programas do computador, pode não detectar os erros destes programas, no entanto, certas evidências poderão apresentar-se.

Uma auditoria que não utilize o computador pode ser implementada pelos seguintes passos gerais:

a) Revisão do sistema

- i. entrevista com o pessoal de informática;
- ii. uso de questionários;
- iii. exame da descrição geral do sistema;
- iv. revisão geral dos principais controles;
- v. revisão dos controles para cada aplicação vital para a auditoria

b) Testes dos sistemas:

- i. exame de evidências para os controles (listagens de erro, tabulações de grupo, autorizações, etc.);
- ii. uso de saídas impressas para acompanhamento dos documentos-fonte, relatórios de totais de controle, etc.;
- iii. verificação de transações por amostragem;
- iv. outros testes típicos.

c) Avaliação de registros:

- i. testes de verificação dos relatórios de resumo;
- ii. testes de amostras para a confirmação, testes de razoabilidade, etc.

O auditor não se limitará a revisar apenas a parte do processamento. Os passos e procedimentos são seguidos através do sistema inteiro: manuais, eletromecânicos e computadorizados - através de todos os departamentos envolvidos. Assim, os controles específicos de cada aplicação são considerados dentro da estrutura de controles gerais da administração da empresa.

5.1.2 Quando Auditar sem usar o Computador

Os sistemas computadorizados que podem ser auditados sem o uso do computador são, normalmente, os sistemas de processamento e controle por grupo em lote (“batch”) e que contenham trilhas de auditoria bem detalhadas. Este tipo de sistema é caracterizado por grupos de transações classificados e processados seqüencialmente contra um arquivo mestre (este processamento normalmente envolve o desenvolvimento de totais por grupo, para controle do movimento de dados dentro do sistema); transcrição manual de transações, seguida pela conversão para a forma legível pela máquina e produção de grande quantidade de saídas impressas para cada execução de sistema.

A obtenção de resultados satisfatórios na realização de auditorias de sistemas sem testar os programas depende diretamente da habilidade do auditor em saber evidenciar a qualidade do processamento por meio de testes das entradas e saídas, amostras de cálculos, etc. Situações mais complexas, que podem complicar a capacidade do auditor na obtenção desta evidência, podem incluir o seguinte:

- a) processamento produzindo uma saída final sumarizada, de maneira que dificulte a identificação de itens individuais. Um conhecimento de informática é então necessário para acompanhar transações da fonte para a saída e dos relatórios para as entradas;
- b) grande quantidade de tipos de transações, que o acompanhamento do processamento torna-se difícil sem o uso do computador;

5.1.3 Requisitos básicos

A realização de testes de auditoria de sistemas sem usar o computador pode ser conduzida praticamente da mesma maneira que os testes de sistemas manuais. As poucas mudanças incluem novos ou ampliados requisitos para planejamento com antecedência e uso de listagens de erro.

5.1.3.1 Planejamento

Antes do desenvolvimento da auditoria, o auditor deve fazer levantamentos para assegurar sua conscientização das condições que devem afetar a auditoragem.

A trilha de auditoria de um sistema de processamento de grupo (“batch”) é normalmente semelhante à trilha de um sistema manual. Algumas vezes, porém, certas informações importantes permanecem no sistema somente por um período limitado de tempo, e não são produzidas saídas impressas de todos os caminhos normais do sistema, Nestes casos, o auditor deve fazer planejamento antecipado tanto dos dados que deverão ser salvos, como das listagens que serão necessárias.

5.1.3.2 Uso de listagens de erro

Na condução de seus trabalhos de revisão e avaliação dos sistemas, o auditor deve examinar todos os procedimentos e controles associados com cada aplicação que afete as transações financeiras. Estas verificações podem ser realizadas através da utilização de técnicas aceitas, tais como a verificação dos documentos-fonte.

Tanto na realização das revisões como nos testes de auditoragem, o auditor normalmente faz uso das listagens de erro, produzidas durante as execuções diárias dos sistemas de dados. Aquelas listagens de todas as transações rejeitadas durante o processamento, por conterem erros, são conservadas para assegurar que a ação corretiva foi efetuada.

Elas também constituem documentação valiosa da eficácia dos controles do sistema, por indicarem os tipos de erros detectados pelos programas do computador.

Se algum método, tal como acompanhamento de transações, descobre um erro, a referência à listagem de erro deve revelar que nenhum erro deste tipo está sendo detectado e que, portanto, alguma característica de controle está ausente.

5.1.4 Vantagens e desvantagens

A principal vantagem de auditar sem usar o computador resume-se no fato de que o auditor estará usando técnicas simples e familiares. Ele faz a revisão da estrutura dos controles de processamento de dados, sem, no entanto, ter que trabalhar com as compilações dos programas do computador. Esta abordagem adequadamente realizada, além de mais econômica, tem apresentado resultados satisfatórios.

As desvantagens de auditar um sistema sem usar o computador concentram-se no fato de que o auditor não usa da capacidade do computador no processo e os trabalhos de implementação da auditoria podem tornar-se bastante difíceis se o sistema é complicado ou se não possuir trilhas de auditoria bem definidas.

5.2 Auditando “com” o Computador

O uso do computador como auxiliar do auditor no processo de levantamento de dados, análise de resultados, etc., através das diversas técnicas disponíveis, pode, se utilizado eficazmente, trazer inúmeros benefícios, a começar pela economia de tempo. O computador amplia o raio de ação dos levantamentos, proporcionando acesso a todos os registros e programas do sistema, de forma a tornar a auditoria mais completa e eficiente.

São duas áreas, basicamente, de atuação do computador no processo de auditoria de sistemas:

- Teste e Análise do sistema: aqui, o trabalho objetiva o teste do sistema em si e sua conseqüente validação ou não. Segue-se a premissa de que se o sistema que produz os resultados e informações está perfeito, com bons controles, então os resultados gerados podem ser validados.
- Teste dos dados que são processados pelo sistema: testes de prolongamento e condições, seleção e impressão de confirmações, amostras para a auditoria, comparação de dados duplicados para a consistência, comparação de dados de auditoria com registro do sistema.

O crescimento da utilização dos computadores neste processo tem se tornado tão difundido durante a última década que várias companhias especializaram-se na criação de programas de testes e validações. Os *softwares* têm sido ferramentas auxiliares do auditor e podem ser encontrados hoje em dia em pacotes vendidos por empresas especializadas. Dedicamos parte desta seção à técnica de auditoria com tais tipos de sistemas.

5.2.1 Etapas da Auditoria de Sistemas “com” o Computador

Apesar dos procedimentos na auditoria de sistemas muitas vezes não serem formalizados pelas próprias empresas, nem por parte dos auditores, as abordagens seguem com poucas variações, dividindo-se comumente em 3 fases:

Na primeira fase, objetiva-se o levantamento dos processamentos e funções de controles relacionados com os propósitos da auditoragem:

a) Revisão inicial e avaliação da área a ser auditada e preparação do plano de auditoria:

1. revisão da descrição do serviço;
2. procedimentos de documentação e organogramas;

3. estrutura básica dos controles do sistema;
4. revisão do fluxo das transações;
5. acompanhamento de transações selecionadas e interpretação da seqüência do processamento;
6. identificação dos controles e elementos de dados importantes para os objetivos da auditoria.

Em seu segundo passo, o auditor primará pelo conhecimento da estrutura do sistema, lay-out dos registros e fluxogramas do processamento:

b) Revisão detalhada e avaliação lógica do processamento e dos controles:

1. avaliação dos controles internos;
2. análise dos procedimentos do processamento;
3. exame do conteúdo dos arquivos mestre;
4. avaliação dos procedimentos nas áreas dos usuários;
5. acompanhamento de transações;
6. análise da lógica dos controles e registros.

Na terceira fase, o auditor deve concluir se os procedimentos estão sendo cumpridos em forma de rotinas e se os dados são perfeitos e precisos:

c) Teste para a verificação da segurança dos controles estabelecidos e para exame dos registros selecionados

1. acompanhamento das transações;
2. verificação das autorizações;
3. reconciliação das transações diárias.

Através da utilização do computador, os auditores podem, eficaz e eficientemente, realizar testes diretamente envolvidos com a lógica dos programas e com o conteúdo dos arquivos-mestre do processamento de dados.

5.2.2 O computador como ferramenta de trabalho do auditor

O computador pode ser usado para realizar uma grande variedade de rotinas e tarefas, de maneira rápida e eficaz. Assim, pode ser usado para pesquisar todos os registros dos arquivos para consistência interna, perfeição e validade, o que significa a possibilidade de exame de todos os registros, ao invés de uma pequena amostra, ao mesmo tempo que o computador oferece como subproduto a checagem de extensões e controle de totais.

Naquelas situações em que o auditor teria que gastar mais tempo na preparação dos testes detalhados, o computador poderá resolvê-las de maneira útil e produtiva, provavelmente possibilitando ainda testes mais complexos e preciosos, além de análises dos arquivos do sistema e de dados financeiros que, de outro modo, teriam que ser feitos manualmente.

Como programas do computador podem ser utilizados para analisar os registros dos arquivos do sistema, para pesquisar atributos nos quais o auditor esteja interessado, ou para selecionar registros de dados com irregularidades, o auditor poderá, neste intermédio, analisar detalhadamente aqueles relatórios de exceção emitidos pelo sistema.

Desta maneira, rotinas ou itens usuais podem ser manuseados rapidamente, permitindo ao auditor utilizar seu tempo na investigação ou confirmação em profundidade daqueles casos considerados mais anormais. Além do que o auditor poderá usar o computador para classificar, compilar e analisar grandes volumes de dados.

Finalmente, outra grande utilidade proporcionada pelo computador ao auditor na seleção de amostras para os propósitos da auditoria. Estas amostras podem ser selecionadas de acordo com os critérios preestabelecidos pelo auditor, ou então o auditor pode usar o computador para gerar números randômicos e selecionar amostras baseadas nesta técnica. Além do que o computador poderá calcular

tamanhos de amostras desejáveis para os diversos níveis de confiança, assim ajudando a facilitar um plano de amostragem estatística.

5.2.3 Técnicas da auditoria de computador

Depois que o auditor determinou os objetivos da auditoria e chegou a uma conclusão sobre as espécies de dados a serem examinados, bem como sobre os critérios a serem utilizados na seleção dos dados para a verificação, deve-se escolher os procedimentos específicos para executar estes objetivos.

Esta escolha é função dos requisitos da auditoria e é influenciada pela conveniência de várias alternativas. O auditor deve avaliar o custo da realização de um procedimento particular e compará-lo com os benefícios proporcionado pelo procedimento escolhido.

A identificação das áreas de fraqueza no sistema, durante a avaliação dos controles internos, justifica maior atenção e exames mais detalhados do que aqueles itens sobre os quais o auditor já adquire um certo grau de confiança a partir do exame preliminar.

Quando os testes a serem realizados são bastante fáceis, mas envolvem grande número de registros, procedimentos manuais representam uma abordagem extremamente consumidora de tempo, podendo ser substituída pelas vantagens de alta velocidade de uma análise de computador.

Vários métodos de processamento de dados têm sido utilizados pelos auditores na realização de seus trabalhos de avaliação de sistemas. O desenvolvimento destas técnicas sofreu um processo evolucionário que cresceu em intensidade nos últimos anos. Apesar disso, algumas ainda encontram-se em seus estágios iniciais e tratam, em sua maioria, de adaptações de técnicas de processamento de dados já existentes.

Pesquisa realizada pelo SRI junto a equipes de auditoria interna constatou a existência de 28 técnicas e ferramentas de auditoria de PED, as quais foram classificadas de acordo com a principal área para qual foram projetadas. Destas, selecionamos aquelas que, ao nosso ver, estão mais diretamente ligadas com as auditorias de sistemas “através” do computador.

5.2.3.1 Técnicas para testar os Controles dos Programas do Computador

As técnicas para testar os controles dos programas do computador objetivam compreender os procedimentos e ferramentas usadas para testar rotinas de programas, programas, ou sistemas internos, a fim de avaliar os controles ou verificar a precisão do processamento e a continuidade do cumprimento das especificações originais dos usuários.

5.2.3.1.1 Método “Test Data”

O método “test data” é utilizado para verificar a segurança dos processamento de sistemas de computador, através da execução destes sistemas com conjuntos de dados de entrada especificamente preparados, para produzirem resultados preestabelecidos.

O uso deste método proporciona aos auditores um procedimento adequado de verificação de sistemas e programas de computador. Até mesmo auditores, com restrito conhecimento de PED, podem utilizar este método, desde que dirigido para específicas e limitadas funções dos sistemas.

É uma técnica ideal para iniciar a verificação de sistemas porque os testes podem ser ampliados vagarosamente, proporcionando uma situação de aprendizagem propícia para aos auditores menos experientes. Sua utilização limita-se à verificação e avaliação do processamento no computador, não sendo uma técnica adequada para o exame de dados.



Fig.1

As maiores vantagens desta técnica é que ela proporciona a visualização do cumprimento das políticas, especificações e dos procedimentos definidos pelos usuários; requer um mínimo de assistência de processamento de dados tanto na preparação dos dados do teste como na especificação dos resultados; normalmente, não requer programação especial, sendo necessário ao auditor apenas um conhecimento rudimentar de PED.

Os custos modestos do método “test data” e os requisitos limitados de implementação tornam-no atrativo para verificação de sistemas, constituindo-se uma técnica de auditoria eficaz para teste e avaliação de sistema de aplicação no computador que tenham sofrido quaisquer alterações.

A mecânica de aplicação do “test data” implica nas seguintes etapas:



Fig.2

5.2.3.1.2 Método “Base Case System Evaluation”

O BCSE é uma técnica que utiliza um grupo padronizado de dados (entradas, parâmetros e saídas) para testar um sistema de aplicação no computador. Este grupo de dados é estabelecido pelos usuários, com a cooperação de auditores, como um critério indispensável ao correto funcionamento do sistema a ser examinado.

Este processo de testes tem sido mais largamente utilizado como uma técnica de validação de sistemas. Algumas empresas, no entanto, têm usado o BCSE como um meio de testar programas durante um fase de desenvolvimento a fim de garantir uma operação do sistema bem sucedida, antes da sua instalação, e para verificar a continuidade da segurança durante sua vida.

5.2.3.1.3 Simulação Paralela

Neste método, Simulação Paralela, transações e arquivos dos sistemas em operação são processados por programas especificamente preparados para simular a lógica daqueles utilizados na operação normal do sistema.

Apenas aquelas funções de processamento mais importantes devem ser selecionadas para inclusão nestes programas de simulação.

Após o processamento dos programas simulados, seus resultados devem ser comparados com aqueles de produção efetiva, a fim de se identificar possíveis diferenças.

Em virtude de serem utilizados dados reais de produção, tal técnica tem a vantagem de evitar a preparação de dados de teste. No entanto, acrescenta a necessidade da elaboração de programas de computador, o que implica na obrigação do conhecimento, por parte do auditor, de técnicas de programação.

Por outro lado, “softwares” generalizados com este propósito, simplificando a preparação de programas de simulação paralela.

5.2.3.1.4 “Integrated Test Facility” - ITF

O ITF é uma técnica para rever aquelas funções de uma aplicação. Dados de teste preparados pelos auditores são utilizados para comparar os resultados processados pelo ITF com os resultados do teste pré-calculados.

O método é mais freqüentemente usado para testar e verificar grandes sistemas de aplicação no computador, onde não é prático o ciclo de teste de dados separadamente.

A técnica ITF é utilizada para verificação e validação de processamentos computadorizados, e é de valor limitado para o exame de dados de produção ou arquivos de dados, pois proporciona evidência restrita com relação a estes aspectos.

5.2.3.2 Técnicas para Analisar os Programas do Computador

Nesta categoria estão incluídas as ferramentas e técnicas de auditoria de usadas para verificar a lógica do processamento e os procedimentos internos dos sistemas e programas. Tanto podem ser utilizadas durante o processo de desenvolvimento dos sistemas, como nos testes periódicos de cumprimento de pós-implementação, para aceitação pela auditoria destes sistemas.

5.2.3.2.1 “SNAPSHOT”

O SNAPSHOT é uma técnica que possibilita a visualização daquelas partes da memória do computador que contém os elementos dos dados utilizados pelo processo de decisão, ao mesmo tempo que a decisão é tomada. Os resultados do SNAPSHOT são impressos em formato de relatórios, para fins de reconstrução do processo de tomada de decisão.

Esta técnica ajuda os auditores a responder questões como porque o sistema produziu um determinado resultado questionável. Ela proporciona informações para explicar por que uma particular decisão foi tomada pelo sistema.

O SNAPSHOT sendo utilizado juntamente com outras técnicas de auditoria, como o ITF ou o TRACING (vide item 5.2.3.2.3) por exemplo, proporciona a determinação de que resultados ocorrerão se um certo tipo de transação entrar no sistema.

A técnica SNAPSHOT também pode ser uma inestimável ajuda para o pessoal de sistemas e programação, na depuração dos sistemas, em virtude de ela tornar possível a visualização da memória do computador no momento desejado. O SNAPSHOT permite que se isole o problema economicamente, pois as rotinas predeterminadas podem rapidamente imprimir os dados necessários aos propósitos analíticos. Tal técnica constitui-se numa poderosa ferramenta de depuração para o pessoal de sistemas e programação. Esta vantagem é um aspecto que normalmente paga o uso deste procedimento.

O SNAPSHOT requer um indispensável planejamento detalhado tanto para elaboração de rotinas como para identificação das transações que deverão ativá-las. Para obtermos os resultados do processamento de uma determinada transação, é necessário identificá-la, antes mesmo que ela entre no sistema.

Este procedimento também necessita de, pelo menos, uma pessoa com bom conhecimento de sistemas de computador, pois o tipo de informação normalmente produzido contém dados em formato de linguagem de máquina.

Exceto para circunstâncias não usuais, o benefício proporcionado pelo SNAPSHOT é bastante questionável. Outras técnicas, tais como ITF e o "test data", tendem a atingir os mesmos objetivos de auditoria, mas como uma utilização eficaz do tempo.

5.2.3.2.2 Mapeamento estatístico dos Programas de Computador (MAPPING)

O MAPPING é uma técnica de computação que pode ser utilizada pelo auditor para efetuar verificações durante o processamento dos programas, flagrando situações como:

- Rotinas não utilizadas;
- Quantidade de vezes que cada rotina foi utilizada quando submetida a processamento de uma quantidade de dados.

A análise dos relatórios emitidos pela aplicação do mapeamento estatístico permite a constatação de situações:

- Rotinas existentes em programas já desativadas ou de uso esporádico;
- Rotinas mais utilizadas, normalmente, a cada processamento do programa;
- Rotinas fraudulentas e de uso em situações irregulares;
- Rotinas de controle acionadas a cada processamento.

Para a utilização do MAPPING há necessidade de ser processado um software de apoio em conjugação com o processamento do sistema aplicativo, ou rotinas específicas deverão estar embutidas no sistema operacional utilizado.

5.2.3.2.3 Rastreamento dos programas de Computador (TRACING)

O método TRACING possibilita seguir o caminho de uma transação durante o processamento do programa.

Durante a aplicação da técnica, a seqüência de instruções executadas é listada. Dessa forma obtemos os números de instruções segundo sua ordem de execução, como por exemplo:

**00001-00002-00003-001150-001151-001152-001153-
90190-90191-90192-90193-90194-90195-53018-
53019- etc.**

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

Esta abordagem, como consequência, viabiliza a identificação de rotinas fraudulentas pela alimentação de transações particulares. Por exemplo, podemos adicionar ao programa de cálculos da folha de pagamento as transações dos profissionais da área de computação ou da área de pessoal e, marcando esses registros para o acionamento da condição *tracing*, rastrear as instruções que dão tratamento a essas transações específicas.

5.2.3.2.4 Fluxograma de Controle

O método de fluxograma de controle usa as técnicas de fluxograma de programas de computador para identificar e apresentar caminhos e pontos de controle dentro dos sistemas de computador.

O DFD- Diagrama de Fluxo de Dados é o esquema de fluxogramação mais adequado para o rápido entendimento do sistema e para uma fácil e pronta visualização do ponto de controle.

O DFD guarda características singulares, como:

- Obedece ao esquema *top down*, ou seja, representa o sistema do geral para o particular – do sintético para o analítico;
- Dá prioridade à representação dos processos e, como consequência, representa as informações geradas/usadas por eles;
- Permite representação gráfica até o nível de detalhamento que o auditor de sistemas considere suficiente para o entendimento do sistema; por conseguinte, por não exigirem a representação detalhada de todos os processos e resultados, economizam tempo ao trabalho de auditoria.

A simbologia básica do DFD é

SÍMBOLO	DESCRIÇÃO
	<p>PROCESSO</p>
	<p>FLUXO DE DADOS</p>
	<p>ÁREAS EXTERNAS AO SISTEMA</p>
	<p>OUTROS SISTEMAS</p>

Fig.3

5.2.4 Pacotes de *software* para a Auditoria

Pacotes de auditoria de computador são apenas outra espécie de programas generalizados de computador, projetados para satisfazer às necessidades particulares do auditor.

Estes programas representam ferramentas que permitem ao auditor alcançar um maior entendimento de análise de informação, como parte do seu trabalho de auditoria.

Durante os últimos anos, muitos destes pacotes generalizados de auditoria têm surgido no mercado. Todos têm diferentes características, de modo que o auditor deve determinar aqueles que proporcionam as capacidades convenientes para as suas particulares necessidades.

5.2.4.1 Características e Funções

Segundo Porter (69), algumas das funções de auditoria que devem ser consideradas na avaliação de um programa generalizado de auditoria são:

- a) teste de extensões e condições;
- b) tabulação de dados e realização de análises úteis ao auditor;
- c) exame da qualidade dos registros – correção, consistência condições inválidas, etc.;
- d) seleção e impressão de amostras para a auditoria;
- e) comparação dos dados da auditoria com os registros dos sistemas.

Desta forma, um programa de computador pode ser usado para qualquer tarefa de comparação ou de cálculos, desde que os critérios desejados possam ser estabelecidos. Uma característica comum destes pacotes é o fato de que o auditor pode definir claramente o que deve ser calculado, comparado, resumido, etc.

6. AUDITORIA DE SISTEMAS EM OPERAÇÃO

A precisão e a perfeição do processamento de dados são diretamente dependentes dos controles dos sistemas do computador. A auditoria dos sistemas em operação tem como objetivo principal a revisão destes controles, que englobam o fluxo e o processamento das transações, a manutenção dos registros e arquivos, e a preparação e manutenção dos relatórios de saída.

A metodologia aqui desenvolvida apresentará a seqüência lógica a ser adotada pelos auditores, quando da revisão e avaliação do processamento dos sistemas de computador em produção normal, bem como as oportunidades de utilização das diversas técnicas e ferramentas de auditoria.

Esta seqüência lógica se compõe de seis fases distintas, abrangendo os controles relacionados com a origem da transação, a entrada da transação no processamento de dados, a comunicação de dados, o processamento no computador, a armazenagem e recuperação de dados e as saídas do processamento, como mostra a figura seguinte:

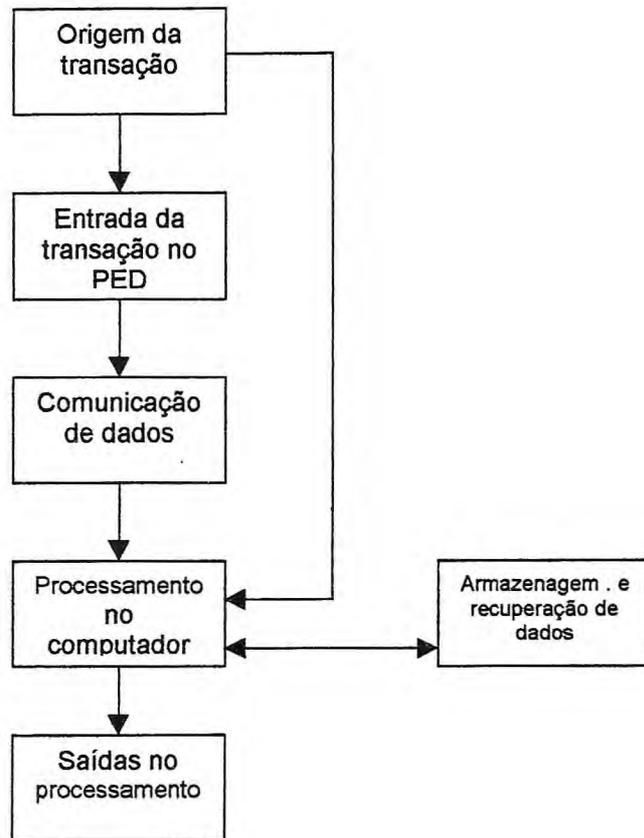


Fig.4

6.1 Origem da transação

Os controles da origem da transação abrangem a preparação manual e o processamento da transação, antes de sua entrada no processamento de dados. Estes controles são, por definição, mais manuais do que automatizados, e excluem os usuários de terminais de entrada de dados, que serão tratados separadamente.

Esta primeira fase inclui a origem propriamente dita da transação e os procedimentos externos ao processamento de dados. Estas transações podem, eventualmente servir de entrada do sistema, como também podem ser usadas para preparar outros documentos que, por seu turno, serão enviados ao processamento de dados.

6.1.1 Áreas de Controle

As áreas importantes do controles da origem da transação podem ser vistas na figura abaixo, que mostra a relação existente entre elas:

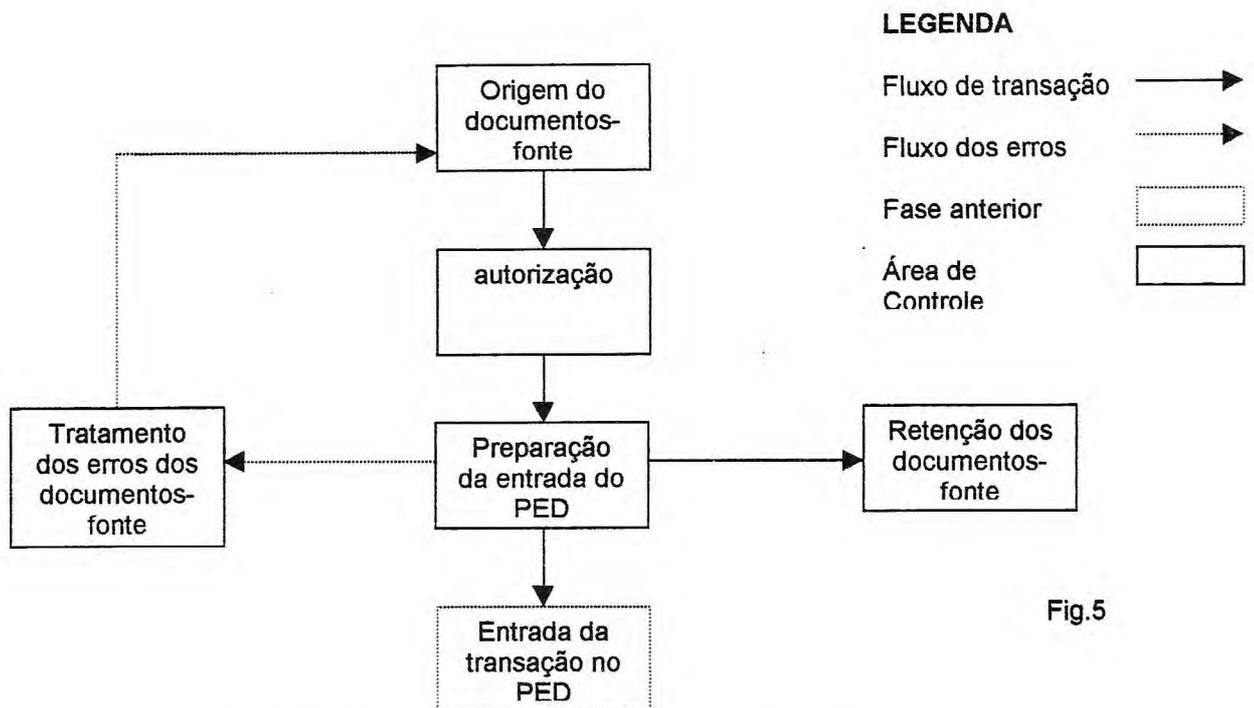


Fig.5

As cinco áreas de controle da origem da transação são:

- a) **Origem do documento fonte:** procedimentos escritos que regulamentam a origem e processamento do documento-fonte, bem como o desenho deste documento. Tais controles visam assegurar arquivamento correto, preparação e processamento manual dos documentos-fonte;
- b) **Autorização:** só documentos-fonte devidamente autorizados são admitidos para subsequente entrada no PED;
- c) **Preparação da entrada do processamento de dados:** inclui reunião dos documentos, verificação manual dos erros, separação de lotes, etc.
- d) **Retenção dos documentos-fonte:** os controles relacionados com esta área incluem tanto a retenção definitiva dos documentos-fonte,

remessa para os respectivos setores e destruição destes documentos nos prazos estabelecidos;

- e) **Tratamento dos erros dos documentos-fonte:** separação dos documentos-fonte incorretos, identificação dos erros, procedimentos de comunicação com os setores responsáveis e elaboração dos acertos.

As técnicas utilizáveis pelos auditores para a revisão da eficácia dos controles relacionados com a origem das transações incluem a verificação dos procedimentos, acompanhamento manual das transações, revisão de documentos e grades de remessa e revisão dos relatórios de erros emitidos pelo computador.

6.2 Entrada de Transação no PED

Os controles relacionados com a entrada da transação no processamento de dados podem se apresentar sob dois aspectos: grupos (“batch”) de entrada de dados e terminais de entrada de dados.

O escopo desta fase limita-se a: digitação dos dados, conferência de digitação, validação da entrada no computador, identificação de erros, procedimentos de acertos e de reentrada das transações corrigidas.

Nos dias de hoje, observa-se significativa redução do volume de documentos a serem digitados, sendo muitas transações entradas no sistema no momento de sua ocorrência onde há um ponto do sistema com um terminal.

6.2.1 Áreas de Controle

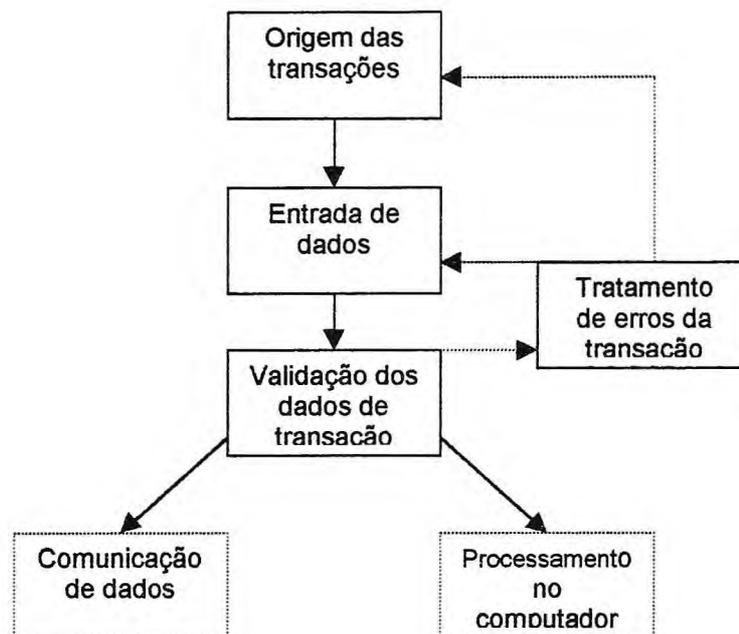


Fig.6

A figura acima representa as quatro áreas de controle relacionadas com a entrada da transação no processamento de dados.

Estas são:

- a) **Terminal de entrada de dados:** controles relacionados com as funções do terminal, tais como entrada de dados, recuperação, formatação de transações, etc.
- b) **Entrada de dados "batch":** recebimento dos lotes, conversões para os meios legíveis do computador, verificação de dados, etc.
- c) **Validação de dados da transação:** controles de programas de computador, para assegurar a precisão e correção de transações a serem processadas pelo sistema.
- d) **Tratamento de erros da transação:** controles do sistema, tanto manuais como dos programas do computador, para identificar, relacionar ou afastar erros ou omissões.

As técnicas utilizadas pelos auditores nesta fase são:

- Softwares generalizados de auditoria;
- Rotinas embutidas na auditoria;
- Método “test data”.

6.3 Comunicação de dados

Os controles de comunicação de dados visam assegurar a integridade e a precisão do fluxo dos dados entre as diversas localizações dos terminais remotos e os centros de processamento de dados, e garantir que mensagens adequadas, proteção de dados e relatórios de erros sejam proporcionados.

6.3.1 Áreas de Controle

São três as áreas de controle:

- a) **Entrada de mensagens:** controles nos terminais, como códigos de identificação, e funções de terminais dirigidas pelo software, tais como “passwords”, tabelas de segurança, etc.
- b) **Transmissão de mensagens:** correta transmissão de mensagem entre os terminais e os centros de processamento de dados.
- c) **Recepção de mensagens:** controles no centros de processamento de dados, incluindo transmissões, técnicas de validação, seqüência numérica, etc.

As técnicas utilizadas nesta fase são: softwares, ITF, etc.

6.4 Processamento no Computador

Os controles aqui estão relacionados com a fase subsequente à validação da transação. Tais controles incluem procedimentos manuais, tais como interação console/operador, e controles residentes dentro dos programas dos diversos sistemas desenvolvidos para realizar funções específicas como controle de estoques, folhas de pagamento, etc.

6.4.1 Áreas de Controle

São cinco as áreas de controle nesta fase:

- a) **Integridade do Processamento:** controles que evitam erros e omissões no fluxo de dados dentro e entre os programas e sistemas de computador.
- b) **Reinício e recuperação:** garantem a reiniciação do programa em caso de interrupção.
- c) **Precisão no processamento:** controles que asseguram a precisão e a razoabilidade dos resultados das operações.
- d) **Intervenção do Operador:** controles que regulamentam a intervenção do operador.
- e) **Tratamento de erros:** controles que garantem que transações com erros sejam identificadas.

6.5 Armazenamento e recuperação de dados

Os controles aqui asseguram a existência de arquivos-mestre precisos e corretos.

6.5.1 Áreas de Controle

Os controles desta fase devem incluir as seguintes áreas:

- a) **Atualização de arquivos-mestre:** controles relacionados com o casamento de arquivos-mestre com arquivos de movimentos.
- b) **Segurança e Privacidade dos dados:** controles lógicos e físicos relacionados com o acesso aos arquivos durante os procedimentos de leitura e gravação.
- c) **Tratamento de erros:** asseguram a perfeição dos procedimentos de acerto dos erros identificados durante a manutenção e/ou recuperação dos dados dos arquivos.

As técnicas utilizáveis são:

- Sistemas generalizados de auditoria;
- Método “test data”;
- ITF.

6.6 Saídas do Processamento

Os controles de saídas são usados para assegurar a perfeição e a precisão de todas as fases componentes do ciclo de processamento do sistema. Elas incluem a conferência visual dos relatórios de saídas e totais de controle dos arquivos-mestre com as transações e comandos de entrada.

6.6.1 Áreas de Controle

A figura a seguir mostra as cinco áreas de controle desta fase:

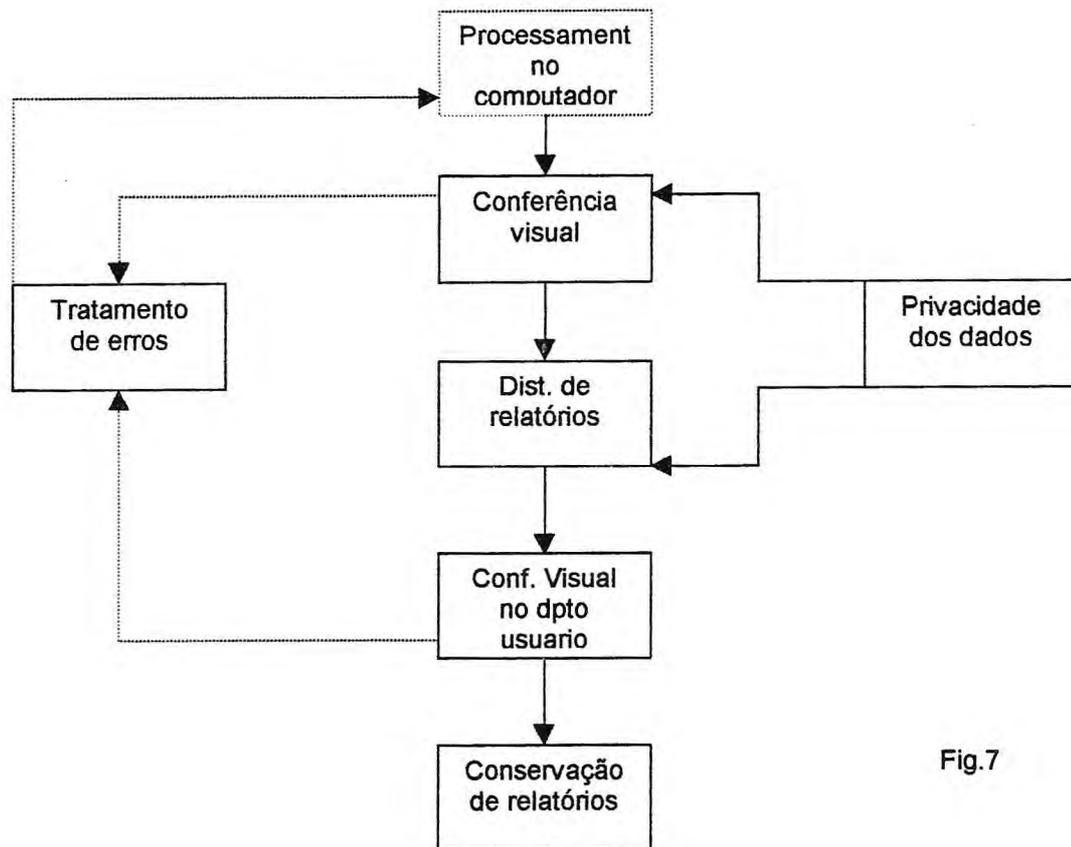


Fig.7

- a) **Conferência visual:** controles sobre os procedimentos para comparar as saídas com as entradas, e assim assegurar que todos os itens tenham sido processados correta e completamente.
- b) **Distribuição de relatórios:** controles para assegurar que as saídas do processamento, quer impressas ou em meios digitais, sejam distribuídas na sua totalidade para os usuários certos.
- c) **Privacidade de dados:** garantem que o uso das saídas do processamento seja controlado.
- d) **Conservação de relatórios:** relatórios de saídas sejam mantidos em arquivos.

- e) **Tratamento de erros:** controles relacionados com a adequação dos procedimentos dos erros e sua correção e realimentação no sistema com a devida tempestividade.

As técnicas utilizáveis incluem a observação nas áreas de entrada/saída no processamento de dados, áreas de arquivo dos formulários, etc.; sistemas especializados, técnica ITF, etc.

7. CONCLUSÃO

Com a evolução dos sistemas informatizados, houve essencial necessidade de controlá-los. A auditoria, então, foi sendo cada vez mais envolvida neste processo, principalmente no que diz respeito ao desenvolvimento dos sistemas de processamento eletrônico de dados.

Na criação de sistemas informatizados, o auditor objetiva, com seu trabalho complementar, garantir a correta implantação destes sistemas, fazendo com que atendam aos requisitos de eficácia, eficiência e segurança.

O auditor também encontra vasto campo de atuação nos sistemas informatizados em operação. Sua preocupação maior aqui refere-se aos controles relacionados com o processamento destes sistemas, analisando desde as rotinas manuais de preparação das transações, o processamento destes dados, até atingir os controles finais relativos à distribuição, utilização e destruição dos relatórios emitidos pelo sistema.

O trabalho ora apresentado trouxe uma metodologia que orientasse o auditor em suas atividades junto aos sistemas informatizados. No entanto, como citamos anteriormente, a auditoria de sistemas informatizados não traz consigo regras a serem seguidas metodicamente, cabendo ao auditor guiar-se pela metodologia que mais lhe traga benefícios no desenrolar de suas atividades.

8. BIBLIOGRAFIA CONSULTADA

- ALMEIDA, M. **Auditoria**. 5^a ed. São Paulo: Atlas, 1996.
- ATTIE, W. **Auditoria: conceitos e aplicações**. 7^a ed. São Paulo: Atlas, 1993.
- FANTINATTI, J. **Auditoria em informática**. São Paulo: Mc Graw Hill, 1988.
- FONTES, J. **Manual de auditoria de sistemas**. 1^a ed. Rio de Janeiro: Ciência Moderna, 1991.
- GIL, A. **Auditoria de computadores**. 1^a ed. São Paulo: Atlas, 1993.
- MORAIS, J. **Auditoria de sistemas "através" do computador**, 1982, 124p. Dissertação (Mestrado em Informática) – Pontifícia Universidade Católica do Rio de Janeiro, 1982.
- MOTTA, J. **Auditoria: Princípios e técnicas**. 1^a ed. São Paulo: Atlas, 1988.
- TREVISAN AUDITORES. **Auditoria: suas áreas de atuação**. 1^a ed. São Paulo: Atlas, 1996.