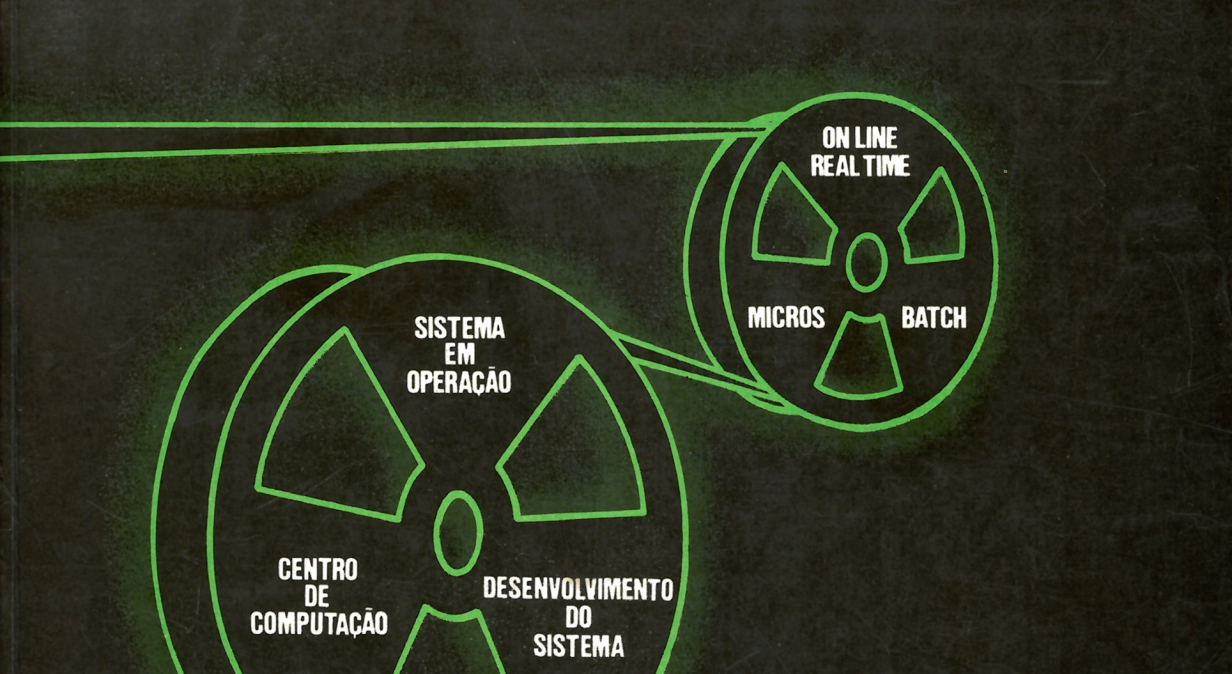
ANTONIO DE LOUREIRO GIL

AUDITORIA DE COMPUTADORES



atlas

Auditoria de Computadores

EDITORA ATLAS S.A.
Rua Conselheiro Nébias, 1384 (Campos Elísios)
Caixa Postal 7186 — Tel.: (011) 221-9144 (PABX)
01203 São Paulo (SP)

ANTONIO DE LOUREIRO GIL

Auditoria de Computadores

SÃO PAULO
EDITORA ATLAS S.A. – 1989

Rua Conselheiro Nébias, 1384 (Campos Elísios)
Caixa Postal 7186 – Tel.: (011) 221-9144 (PABX)
01203 São Paulo (SP)

ISBN 85-224-0395-3

Impresso no Brasil/**Printed in Brazil**

Depósito legal na Biblioteca Nacional conforme Decreto nº 1.825, de 20 de dezembro de 1907.

Capa
José Ribamar Lins S. Junior

Dados de Catalogação na Publicação (CIP) Internacional
(Câmara Brasileira do Livro, SP, Brasil)

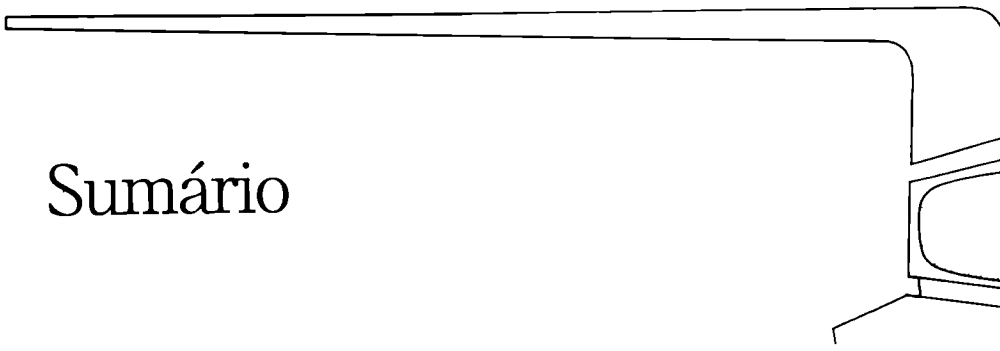
G392a	Gil, Antonio de Loureiro. Auditoria de computadores / Antonio de Loureiro Gil. São Paulo : Atlas, 1989 Bibliografia. ISBN 85-224-0395-3 1. Auditoria 2. Centros de processamento de dados Avaliação 3. Computadores – Avaliação I. Título.
88-1571	CDD-001.640684

Índices para catálogo sistemático:

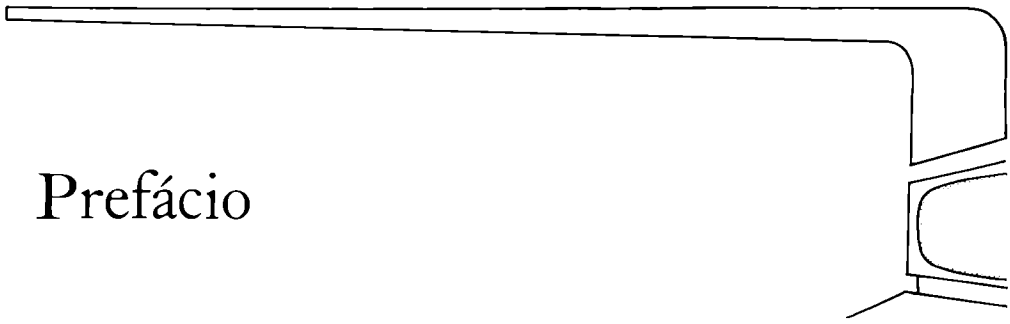
1. Auditoria de computadores : Informática 001.640684
2. Auditoria técnica : Informática 001.640684
3. Computadores : Auditoria : Informática 001.640684

A minha esposa
Maria Tereza
por termos construído
juntos o GRUPO
GIL TECNOLOGIA – ACI/
SECUR/CQA

Sumário



Prefácio



O verdadeiro ativo de uma empresa é o seu recurso humano. E este tem maior ou menor valor segundo seu conhecimento e seu comportamento. Para obter, armazenar, processar e criar conhecimentos dentro de uma empresa, todo um sistema é criado e implementado, mas está sempre sujeito aos efeitos da qualidade; qualidade do conhecimento de quem o criou e de quem o faz funcionar, qualidade do equipamento usado (que reflete qualidade de conhecimento e de comportamento de quem o produziu), qualidade do comportamento de quem trabalha no sistema ou dele se serve etc.

Ou seja, da qualidade do conhecimento e da qualidade do comportamento depende essencialmente o sucesso empresarial.

Como o sistema de informações é vital hoje em todo o processo gerencial, fica extremamente visível a necessidade e a utilidade de se garantir sua qualidade, a fim de que se maximize o conhecimento dentro da empresa (e se minimizem os problemas de comportamento, por que não dizer).

Daí a extraordinária importância da auditoria do sistema computacional, que assume cada vez mais esse papel de assegurador da qualidade da informação (e conseqüentemente do conhecimento) e participa também cada vez mais no processo de garantia quanto a possíveis e indesejáveis problemas de comportamento.

O Prof. Antonio de Loureiro Gil é uma das maiores autoridades nesse campo no Brasil, estando, há muitos anos, na Universidade de São Paulo (Departamento de Contabilidade, na FEA) e no mercado, desenvolvendo trabalhos práticos, teses, cursos, artigos e palestras nesta área.

Tarefa, portanto, muito fácil a minha (e honrosa também) de dar essas palavras iniciais ao feliz leitor deste livro.

São Paulo, dezembro de 1988.

ELISEU MARTINS

Apresentação

A auditoria de computador cresce e participa do ambiente empresarial em função dos vetores principais:

- total participação da tecnologia de processamento eletrônico de dados nas atividades das organizações;
- complexidade e crescimento das atividades empresariais.

Os computadores eletrônicos são os instrumentos que permitem a evolução empresarial e dão sustentação para enfrentarmos e expandirmos o intenso entrelaçamento das tarefas de administração da organização moderna.

A variedade de opções de emprego da tecnologia computacional viabilizou o uso de computadores em todas as áreas das empresas e sedimentou conceitos como:

- distribuição do processamento via mini/microcomputadores independentes (*stand alone*) ou através de ambiente *on-line* com redes locais ou teleprocessamento;
- unicidade da informação com a estruturação de banco de dados;
- descentralização do desenvolvimento de sistemas computadorizados com a colocação de poderosas linguagens de programação à disposição dos usuários, tornando-os independentes para a concepção e implantação de novos usos da tecnologia de processamento eletrônico de dados em seu ambiente de trabalho;
- automação de escritórios (*office automation*) com o apoio do computador para a execução e interligação das tarefas básicas da administração.

A atividade de auditoria, por sua vez, evoluiu e foi exigida, ultrapassando os seus limites originais de auditoria contábil e de auditoria tributária – cuja expressão máxima, em termos de tecnologia está abraçada pelas empresas de auditoria independente – assumindo postura de auditoria operacional, culmi-

nando, atualmente, com a auditoria de sistemas computadorizados, sendo esta levada a participar de todos os momentos das organizações à medida que o computador eletrônico permeia e é partícipe em todos os instantes da vida empresarial.

A auditoria operacional de sistemas computadorizados tornou-se um canal de comunicação, por excelência, de que se vale a Alta Administração para enfrentar, simultaneamente, a complexidade e o crescimento das atividades empresariais e a total participação do computador na vida das organizações.

Este livro aborda a problemática empresarial e a utilização dos computadores vistas sob o enfoque de atuação da auditoria de sistemas.

Contemplamos a filosofia e as diretrizes de participação dos auditores de sistemas num ambiente computacional das empresas, enfocando aspectos como conceitos, técnicas e metodologia.

A auditoria de sistemas computadorizados atua sob a ótica da validação e avaliação do controle interno do ambiente computadorizado e pode ser estudada segundo três momentos distintos:

- auditoria de sistemas computadorizados em operação normal;
- auditoria durante o desenvolvimento de sistemas computadorizados;
- auditoria do centro de computação.

A tecnologia do auditor de computador varia de acordo com o momento de atuação da auditoria e as metodologias de atuação adaptam-se a cada situação.

Finalmente, dedicamos espaço também aos aspectos gerenciais da auditoria de computador segundo duas situações bem características:

- a auditoria de gestão do centro de computação via auditoria de computadores;
- a gestão da auditoria de computadores.

A auditoria de gestão via computadores é o mais recente e espetacular campo de aplicação da tecnologia de auditoria de sistemas computadorizados e só foi possível com o advento da tecnologia de quarta geração em processamento eletrônico de dados (descentralização de desenvolvimento, distribuição do processamento, "office-automation", teleprocessamento, ambiente "on-line", microinformática, banco de dados).

A gestão da auditoria de computador contempla tópicos como:

- planejamento e controle da auditoria de sistemas;

- plano diretor de auditoria de sistemas computadorizados;
- relatório anual de auditoria de computador;
- indicadores de qualidade de auditoria de computador.

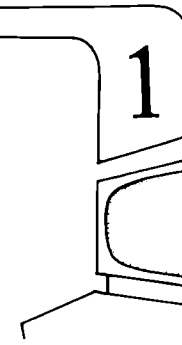
Buscamos, outrossim, representar a tecnologia que vivenciamos, há quinze anos, em auditoria de informática através de artigos e conferências proferidas no Brasil, Estados Unidos, Israel, Argentina e Portugal. É verdade, também, que a participação de cerca de 50 (cinqüenta) auditores de computador se faz representar neste livro; são os profissionais que tive a honra de comandar na ACI – Assessoria e Controles Internos, como diretor executivo, nestes últimos doze anos.

Esta tecnologia exposta é usada nas Metodologias TAMDIS® – Técnicas de Auditoria de Micro à Distância; MACC® – Metodologia de Auditoria de Centro de Computação; FATO-ON® e FATO-DS® – Metodologias para Sistemas Computadorizados e em Desenvolvimento, todas da ACI.

A complexidade empresarial, o total uso da tecnologia de computação e a auditoria de computadores como o canal que flui via tecnologia computacional e que usa computadores para dar sua participação na otimização do funcionamento das organizações é o ambiente em que se justifica este livro.

PROF. DR. ANTONIO DE LOUREIRO GIL

1 Introdução



1.1 O AMBIENTE EMPRESARIAL EM QUE VIVE A AUDITORIA DE COMPUTADORES

Presentemente, nossas organizações não sobrevivem sem a utilização da tecnologia de processamento eletrônico de dados (PED), ou seja, os conceitos e a utilização de *hardware* e de *software* são assuntos corriqueiros no ambiente empresarial de nossos dias.

Na realidade, entidades governamentais e privadas, independente de porte ou ramo de atividade, convivem e subsistem graças a doses cada vez mais elevadas da tecnologia computacional.

É evidente que, dependendo do porte e da área de atuação da entidade, a forma e a intensidade do uso da computação diferem. Assim, temos as instituições financeiras que não conseguem funcionar nem poucas horas com a ausência dos computadores, bem como as microempresas que, apesar de poderem conviver com a ausência da tecnologia de PED, necessitam, para maior agilidade e diferenciamento em relação à concorrência, da participação de microcomputadores pessoais ou profissionais em suas atividades.

Embora a auditoria de computadores seja uma atividade recente, é abrangente na economia brasileira e não cessa de crescer sua atuação e participação no cenário nacional. Na realidade, a auditoria de sistemas computadorizados é participativa em todas as entidades nacionais, quer inserida no grupo de auditoria interna, quer via uma empresa externa. Essa atuação pode ser, portanto, permanente ou esporádica, mas, certamente, é uma constante na vida empresarial.

Obviamente, a auditoria de sistemas é estimulada e ganha realce à medida que a penetração do computador nas atividades organizacionais se aprofunda.

Porém, a auditoria de sistemas computadorizados não perde sua diretriz básica, ou seja, é um instrumento da direção da entidade, dos acionistas, do ambiente externo à organização, do povo para, independentemente, opinar, isto é, validar e avaliar a qualidade em termos de segurança, eficiência dos trabalhos desenvolvidos com a tecnologia dos computadores.

A opinião independente de um profissional, ou grupo de profissionais, que não participa de dado ambiente computadorizado é, portanto, o vetor sobre o qual caminha a atuação do auditor de computador.

O ambiente empresarial aclimatou, então, à medida da evolução de processamento eletrônico de dados (PED), a atuação do auditor de sistema computadorizado.

Um fator determinante da atuação da auditoria de computador é a colocação do comando de PED ou a forma de direção do ambiente computadorizado na organização.

O advento do microcomputador provocou pulverização acentuada da tecnologia de PED, e a distribuição e a descentralização da criação e da execução de processos computadorizados constituem a tônica empresarial atual.

Várias são, portanto, as formas de comando das atividades de PED; um parâmetro, porém, pode ser referido como de tendência e de aplicação firme: a direção e o próprio centro de computação pertencerem à entidade para a qual trabalham. Podemos considerar que PED apóia e sustenta todas as atividades meio e fim das organizações, sendo imprescindível a aproximação dos profissionais de computação dos profissionais responsáveis pelas atividades meio e fim das empresas.

Na realidade, o modelo de implantação de PED é a transferência dessa tecnologia diretamente ao usuário, através de linguagens de programação de quarta geração ou da instalação da inteligência artificial, eliminando ou diminuindo a participação de uma série de profissionais de computação (programadores, digitadores, operadores de computador etc.).

O advento da microinformática e das redes de computadores torna exeqüível este processo. Dessa forma, podemos considerar como bom modelo de posicionamento da área de computação e da área de auditoria de sistemas o espelhado na Figura 1.1.

Obviamente, existem variações na colocação da auditoria de sistemas e quanto mais independente da estrutura orgânica ou do ambiente empresarial em que irá atuar, melhor posicionamento terá. Assim, a auditoria de sistemas poderá reportar-se não só ao Conselho de Administração de uma entidade ou à em-

presa *holding* de um grupo empresarial, como também à diretoria executiva; a hipótese primeira é melhor do que a última, evidentemente.

De forma análoga à passagem intensa da tecnologia de PED para os usuários, evitando-se a intermediação de profissionais de computação, é cada vez mais intensa a absorção da tecnologia de auditoria de computador por parte dos auditores contábeis e operacionais. Tal atitude provoca o aumento da discussão e da utilização da tecnologia de auditoria de sistemas.

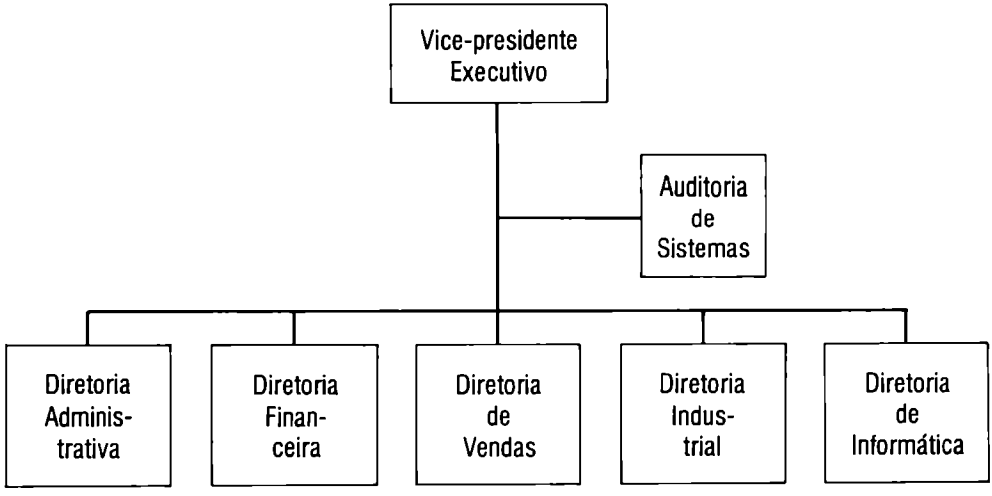


Figura 1.1. *Ambiente empresarial e situação da área de informática e da área de auditoria de sistemas.*

A Figura 1.2 resume, em termos de objetivos, características do ambiente computacional, o atual estágio e, provavelmente, a situação de futura normalidade da problemática *empresa-computação-auditoria de sistemas*.

A integração da auditoria de sistemas ao ambiente empresa computadorizada é complexa em face dos seguintes fatores:

- defasagem tecnológica da auditoria de sistemas em relação ao ambiente empresa computadorizada. Enquanto as empresas começaram seu processo de utilização do computador no final da década de 50, a auditoria de sistemas só ganhou consistência dez anos depois, ou seja, no final da década de 60;
- a característica de grande falta de bons profissionais no ambiente computacional, o que determina, no mínimo, por aderência, proporcional ausência de profissionais competentes na auditoria de sistemas. A auditoria de sistemas, inicialmente, uma típica auditoria de resultados, por

força de suas origens na auditoria contábil-financeira, necessita de forte adaptação cultural e técnica para atuar em auditoria dos processos computacionais;

- necessidade de educação dos executivos das empresas quanto à forte transformação de enfoque da auditoria de sistemas, em relação à auditoria contábil-financeira, acrescentando às suas características de auditoria de resultado a postura principal de auditoria de processos.

ATIVIDADE	OBJETIVOS	CARACTERÍSTICAS COMPUTACIONAIS
EMPRESARIAL	– Evolução tecnológica – Poder de competição – Capacidade de adaptação – Especialização – Crescimento	– Crescentes investimentos em tecnologia de computação – Necessidade de treinamento em processamento eletrônico de dados aos funcionários – Iniciando convívio com o conceito de inteligência artificial
COMPUTAÇÃO	– Apoio e envolvimento do usuário – Disseminação da inteligência artificial – Total integração empresarial	– Falta de profissionais de computação, com a necessidade de investimentos nos profissionais existentes, para o posterior repasse de tecnologia e sustentação do pessoal usuário – Necessidade de especialização de profissionais de computação
AUDITORIA DE SISTEMAS	– Velocidade no acompanhamento do binômio "computação-empresa" – Agente de maior participação do computador na empresa	– Forte evolução da área em termos de compreensão do papel da auditoria de sistemas por parte do auditor contábil-financeiro – Tecnologia em intensa evolução – Escassez de profissionais

Figura 1.2. *Evolução da computação no ambiente empresarial e conseqüente acompanhamento pela auditoria de sistemas.*

O processo de aculturação da auditoria de sistemas é tão dramático que temos necessidade de inserir nos conceitos de administração das empresas:

a) a idéia de que o controle interno não é o controle inserido nas atividades empresariais, mas a função administrativa, desenvolvida por um

novo tipo de profissional – auditor de sistemas – que valida e avalia as demais funções administrativas exercidas na empresa, particularmente planejamento, execução e controle;

b) a ênfase da auditoria de sistemas é realçada nos processos computacionais, os quais são a causa de inconveniências ou irregularidades detectadas, quando for feita a auditoria dos resultados computacionais;

c) o processo computacional é, em certos esquemas de processamento – *"batch"*, *"on-line"* *"data collection"* –, substitutivo ou operado em lugar de processos manuais, mas em outros esquemas de processamento é participativo, confundindo-se processos e resultados computacionais, por causa de uma intensa interação HOMEM-COMPUTADOR ou por causa do uso de tecnologia computacional nos processos empresariais, como no caso de processamento *"on-line realtime"*, no ambiente de microinformática ou quanto aos processos de inteligência artificial.

Como vemos, mais uma vez, realçamos a variada gama de tecnologia e a multiplicidade de formas de atuação da auditoria de sistemas, permeando a tecnologia de computação e sua integração com a mecânica empresarial.

1.2 O AMBIENTE COMPUTACIONAL

A multiplicidade de conexões e formas de aplicação do *hardware* estimula e determina o nível de sofisticação do *software*.

Podemos valer-nos de computadores que trabalham com independência ou em redes, com arquivos singelos (seqüenciais ou indexado-seqüenciais) ou com bancos de dados, com processamento local ou interligados por redes de comunicação, com integração a grandes distâncias, por exemplo, via satélite.

A Figura 1.3 busca dar uma visão panorâmica desse ambiente computacional.

A diversidade de tecnologia é muito grande na área de processamento eletrônico de dados, já que podemos fazer elevada combinação entre os dispositivos (terminais, impressoras, unidades de disco etc.) que compõem uma configuração de computador, bem como entre diversas configurações.

Assim, podemos usar unidades periféricas, discos magnéticos, por exemplo, da configuração A como componente e monitorados pela UCP – Unidade Central de Processamento – da Configuração B. Podemos, também, unificar as UCPs das configurações A e B gerando nova configuração de computador em que as UCPs A e B se intercambiam e agem como se fossem uma única. Esse processo pode ser multiplicado quantas vezes for necessário.

AMBIENTE COMPUTACIONAL	CARACTERÍSTICAS OPERACIONAIS	PROBLEMÁTICA DE UTILIZAÇÃO
HARDWARE INDEPENDENTE	– Processamento em **batch** – **Software** aplicativo de baixo nível de integração no ambiente de micro, alcançando médio nível de integração no ambiente de mini/supermini/grande porte – Arquivos seqüenciais/indexados/banco de dados – **Software** de apoio e básico de pequeno nível de sofisticação no ambiente de micro e de média sofisticação no ambiente mini/supermini/grande porte	A – **AMBIENTE DE MICRO** – Domínio pelo usuário de tecnologia de Computação trabalhando com: – Planilha eletrônica – Linguagem de 4ª geração – Editor de textos B – **AMBIENTE DE MINI/SUPERMINI/GRANDE PORTE** – Domínio dos profissionais de computação intermediando o desenvolvimento e a aplicação da tecnologia de computação
HARDWARE EM REDES LOCAIS	– Processamento **on-line** em termos **data collection** ou **real time** – **Software** aplicativo de médio nível de integração com intensidade de atuação no ambiente interno da empresa – Arquivos em banco de dados – **Software** de apoio e básico de médio nível de sofisticação nas redes de micros locais e de alto nível de sofisticação nas redes locais micro-mainframe – Diminuição da importância de relatórios impressos substituindo-os por telas – Elevada capacidade de armazenamento de dispositivos de discos magnéticos.	A – **REDES DE MICROS LOCAIS** – Participação de especialistas em PED no desenvolvimento de sistemas – Utilização local dos micros com as características do item A, Ambiente de Micro, acrescido da característica de uso do Correio Eletrônico Local B – **REDES LOCAIS MICRO-MAINFRAME** – Atuação dos profissionais de PED no desenvolvimento e operação, particularmente a nível de mainframe dos sistemas – Utilização local dos micros com todas as características já descritas
HARDWARE COM TELEPROCESSAMENTO	– Processamento **on-line**, principalmente **real time** – **Software** aplicativo de alto nível de integração tanto no ambiente interno quanto no ambiente externo da organização – Arquivos em bancos de dados – **Software** de apoio e básico de alto nível de sofisticação, principalmente sistema operacional, **software** de gerenciamento de banco de dados e de comunicação de dados – Intenso uso de telas – Enorme capacidade de armazenamento dos dispositivos de discos magnéticos	– Redes de teleprocessamento com os equipamentos enlaçados em nível permitindo a utilização e integração total tecnológica computacional tanto a nível interno quanto externo da organização – Existência de alto nível de especialização dos profissionais de computação, com intensa participação dos mesmos para montagem das redes, desenvolvimento e integração dos aplicativos, bem como apoio desses especialistas ao uso da rede pelos usuários – Grande participação operacional a nível de mainframe dos profissionais de computação – Total domínio de utilização e operacionalização nas pontas das redes por parte dos usuários

Figura 1.3 *Modalidades de atuação de* hardware.

O ambiente computacional de atuação do auditor de sistemas pode ser visto como:

I – Ambiente de micro

É subdividido em quatro modalidades de operacionalização dos micros:

a) Micros independentes

É a situação de micros profissionais que trabalham como uma configuração mínima, composta de UCP com 64/512 *kbytes*, unidades de disquete ou mesmo com discos fixos, um terminal de vídeo e uma impressora.

b) Micros independentes e multiusuários

Trabalha com a configuração análoga à do item anterior, porém com maior capacidade e vários terminais para o atendimento a diversos usuários conforme o porte e as características do equipamento segundo seus fabricantes.

c) Rede de micros

Reúne configurações de micros independentes ou multiusuários e, via canal de comunicação, consegue estabelecer conexão entre várias UCPs de micros.

d) Micros conectados a mainframe

Através dos micros e de toda a sua configuração, podem ser acessados os dispositivos (disco magnético), de grande capacidade, da configuração de um grande computador central, via conexão da UCP do micro com UCP do computador central.

II – Ambiente de mini/supermini/computadores de grande porte

Pode ser visto segundo os momentos:

a) Mini/supermini/computador de grande porte operando em batch

Nele há configuração forte: UCP de 512 K a 16 Megabytes, unidades de disco magnético de alta capacidade, impressoras, terminais.

b) Mini/supermini/computador de grande porte operando como mainframe

Nele há configurações montadas como no item II, *a* anterior, porém com conexão com terminais, microcomputadores ou outros minis, superminis ou computadores de grande porte.

A tecnologia do auditor de sistemas é variada e abrangente. Auditar um micro independente requer muito menos tecnologia do que auditar uma rede de computadores em que se tenham agregado redes de micros.

Enquanto na auditoria do micro independente bastariam ao auditor conhecimentos do funcionamento básico de um sistema operacional simples, de *software* de apoio e linguagens de programação, também de uso extremamente simples, esse mesmo auditor teria, na rede de mainframe e suas correspondentes redes de micros associadas, de conhecer:

- o funcionamento de um complexo sistema operacional, como as características de geração do LOG;
- a mecânica operacional do *software* de gerenciamento de banco de dados e dos *softwares* de comunicação de dados;
- a estrutura de sistemas aplicativos altamente integrados e de processamento instantâneo, com elevado número de operações e dados processados.

1.3 AUDITORIA DE COMPUTADORES COMO FATOR DE DINAMISMO EMPRESARIAL

Os dispêndios em computação são acentuados nas organizações, e a tendência é aumentar. Cada vez mais é aceita a idéia de que o verdadeiro patrimônio de uma entidade é a sua tecnologia, que compõe seus *sistemas, processos* e *informações;* instalada em seus recursos humanos, determina toda a cultura e capacidade de competição.

As instituições financeiras caminham para dispêndios da ordem de 5% em computação em relação à sua receita operacional e um sem-número de entidades caminha para patamares superiores a 2% na relação despesas com PED versus faturamento.

Portanto, a eficácia dos resultados gerados e a eficiência dos processos concluídos necessitam ser validadas e avaliadas, e a auditoria de sistemas com-

putadorizados é o campo de ação para a certeza do alcance da qualidade de computação necessária.

A segurança dos computadores e respectivos sistemas computadorizados é outro campo de atuação da auditoria de computador; neste particular, as necessidades só têm crescido. O auditor de sistemas tanto é responsável pela segurança física de equipamentos, pessoal, suprimentos e instalações, quanto pela segurança lógica e confidencialidade de sistemas, arquivos e informações.

O posicionamento e atuação da auditoria de sistemas é, portanto, de correlação e comprovação da funcionalidade e da efetividade dos sistemas de informações computadorizados.

Uma entidade progride e se aprimora em face de desafios externos e internos.

Os desafios externos são colocados pelas entidades concorrentes, pelo governo, pelos clientes e pelos acionistas.

Os desafios internos são gerados intrinsecamente em termos de:

- confrontação de seus resultados contábeis – financeiros – operacionais ao longo dos anos;
- novos parâmetros e fatores estabelecidos pelas chefias para alcance em diversos níveis, particularmente em termos de qualidade;
- atuação da auditoria de sistemas, pela argumentação em termos da efetividade e correção de processos e resultados.

A ótica é a de que a organização possui suas funções administrativas clássicas:

- **Planejamento** – determinação via sistemas de informações computadorizados de padrões, ou seja, informações que exprimem uma expectativa de comportamento futuro.
- **Execução** – caracterização via sistemas de informações computadorizados de medidas, ou seja, informações que são os registros das operações ocorridas.
- **Controle** – acompanhamento, via sistemas de informações computadorizados, de desvios, ou seja, informações obtidas da confrontação de *medidas* com *padrões*, e obtenção, em termos quantitativos, da intensidade, abaixo ou acima, em que ficaram as medidas em relação aos padrões.

A auditoria de sistemas contribui para o dinamismo organizacional atuar em cima do ciclo administrativo (planejamento, execução, controle). Essa atuação se dará segundo as ações de validação e avaliação do ciclo administrativo e corresponde a uma ação independente, duplicada logicamente, contemplando a integração das funções administrativas componentes do ciclo administrativo.

Validação é o conceito que exprime a idéia de teste.

Avaliação é o conceito que exprime a idéia de julgamento e emissão de opinião.

Dessa forma, a atuação da auditoria de sistemas difere profundamente das demais atividades exercidas em um ambiente empresarial. As etapas básicas de qualquer atuação da auditoria de sistemas implica:

- compreensão do ambiente a ser auditado, via levantamento e documentação do mesmo;
- análise desse ambiente com a determinação das situações mais sensíveis; é comum o uso das técnicas de análise de risco;
- elaboração de uma massa de testes, ou seja, definição de escopo do teste, geração dos dados para teste, determinação dos resultados a serem alcançados para consideração da correção dos processos ou dos resultados sob auditoria;
- aplicação da massa de testes, ou seja, a auditoria de sistemas não se limita a uma análise do ambiente sob auditoria, ela é obrigada a exercer simulações de laboratório ou de campo para a comprovação da efetividade de processos e resultados;
- análise das simulações empreendidas, como o julgamento dos resultados alcançados;
- emissão de opinião quanto ao ambiente auditado via apresentação de recomendações, como soluções alternativas a serem implantadas;
- debates com os profissionais do ambiente auditado para detalhamento da viabilidade das soluções alternativas recomendadas, com o conseqüente ajustamento e substituição, quando do alcance de alternativas de solução mais adequadas;
- acompanhamento da institucionalização da alternativa de solução alcançada;
- auditoria do nível de funcionalidade da alternativa de solução implantada;
- novas auditorias de sistemas do ambiente empresarial.

Destaque-se que a independência da auditoria de sistemas consiste em o auditor não haver concebido a solução sozinho, já que submete sua alternativa ao auditado, que tem a oportunidade de adequar e otimizar essa alternativa de solução proposta, nem a haver implantado. A institucionalização da alternativa de solução é sempre do auditado.

A duplicidade lógica reside no conceito de que os diversos níveis de chefia já poderão ter feito processos análogos aos da auditoria, embora normalmente fracionados, não estruturados, ou seja, segmentados.

Dessa forma, vemos que a auditoria de sistemas exerce uma função administrativa, casada, segundo o enfoque sistêmico, com as demais funções administrativas do ciclo administrativo, denominada função administrativa *Controle Interno*.

O Controle Interno é, portanto, a validação e avaliação do planejamento, da execução e do controle. Estas quatro funções administrativas podem ser casadas conforme apresentado na Figura 1.4.

Ora, o Controle Interno, a função administrativa que justifica a auditoria de sistemas, é exercida via sistemas de informações computadorizados e compreendem:

- **dados** – massa de testes gerada pelo auditor;
- **processamento** – atividades ou ações para coleta dos dados, para operações de simulação e para análise dos resultados alcançados;
- **informações** – resultados julgados e sobre os quais uma opinião é formada e emitida.

Desta forma, Controle Interno não é o controle existente dentro do sistema. Controle inserido no sistema é controle mesmo e tem como característica uma correspondência biunívoca com o planejamento, ou seja, controle sem planejamento, ou vice-versa, é uma atividade inócua.

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

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

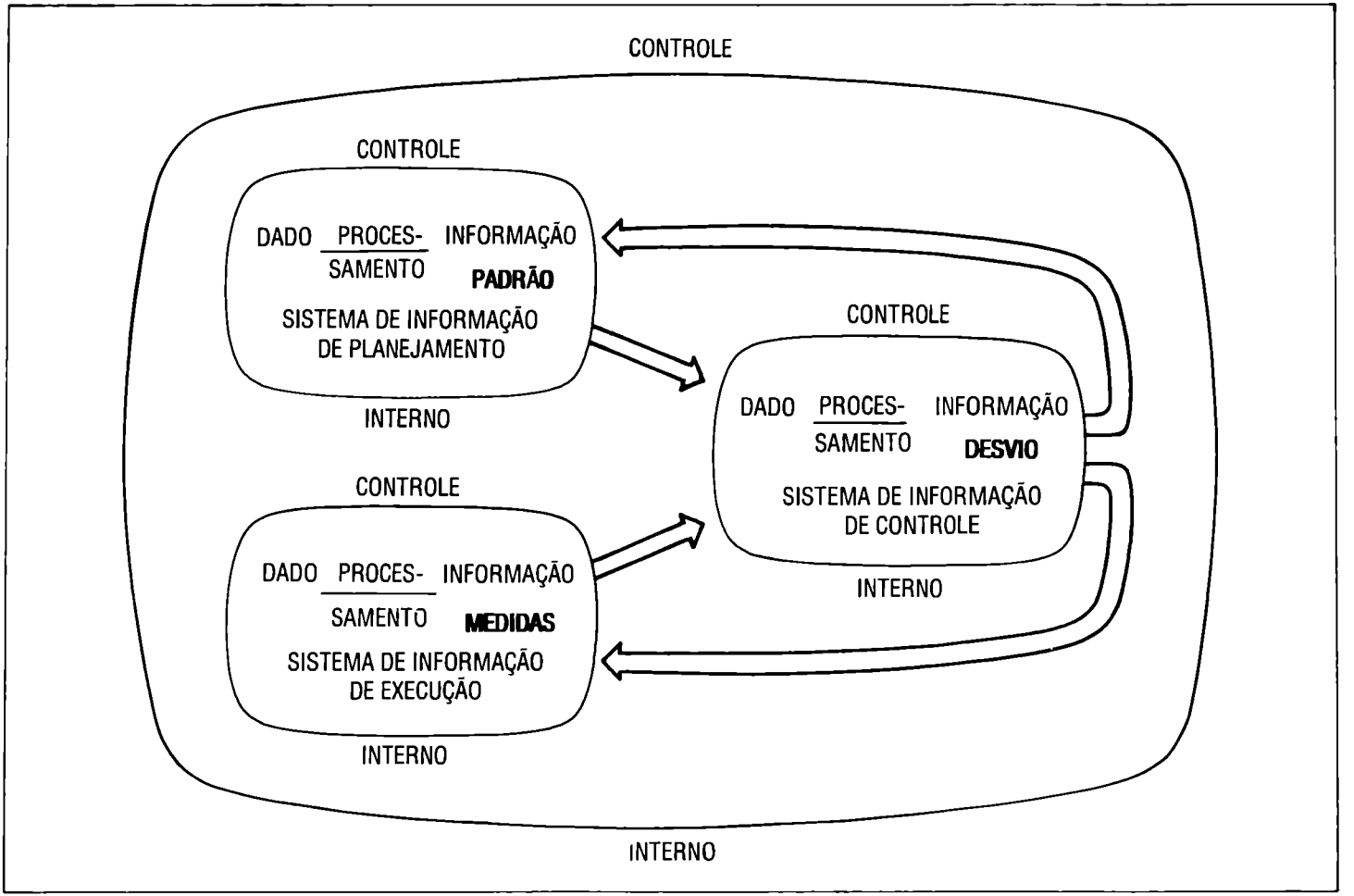


Figura 1.4. *O controle interno e sua atuação junto ao ciclo administrativo.*

Esta mecânica de atuação da auditoria de sistemas gera enorme potencial dinâmico para a organização, já que nossas entidades carregam intrínsecas a si um processo de permanente contestação e mutação.

Esta abordagem é cada vez mais necessária por causa do fator oportunidade. Presentemente, os volumes de dados, a velocidade necessária de tratamento desses dados, a dinâmica da evolução tecnológica com a pouca estabilidade ou pequeno ciclo de vida dos processos tecnológicos redundam na necessidade de ágeis sistemas de informações computadorizados de controle interno.

O enfoque a esta altura a ser transmitido é que a auditoria de sistemas atua por exceção, ou seja, podemos enquadrá-la segundo os conceitos de:

I – Administração por confronto

A auditoria de sistemas exerce o papel de correlação de idéias, impondo aos processos empresariais todo um ambiente de contestação, buscando otimizações, melhores relações benefícios versus custos, maior eficiência, eficácia e segurança.

II – Administração por exceção

- o momento nevrálgico do trabalho do auditor de sistemas está na determinação de onde atuar;
- a escolha dentro do ambiente empresarial computadorizado, do subconjunto merecedor de validação e avaliação corresponde ao escopo de aplicação de técnicas e processos de análise de risco;
- na realidade, a auditoria de computador *não audita* todo o ambiente computadorizado e o segredo de uma boa auditoria de sistemas está na otimização da análise de risco feita;
- o subconjunto do processo ou do resultado determinado como de alto risco e que será submetido à auditoria é denominado *Ponto de Controle*.

1.4 FUTURO DA AUDITORIA DE COMPUTADORES

A auditoria de computadores carece de uma série de investimentos em tecnologia para consolidar suas atividades. Dentre as áreas merecedoras de maiores estudos e estrutura destacamos:

- robustecimento das técnicas de auditoria de sistemas para atuação no complexo e abrangente ambiente computadorizado empresarial (vide item 1.2 – O Ambiente Computacional);

- debates e criação de novas técnicas de análise de risco que componham o planejamento, justifiquem e direcionem a auditoria de sistemas para achados substanciais em termos de melhorias e eliminação de erros do ambiente computacional;

- geração de metodologias de auditoria de sistemas que explicitem o caminho ótimo, retratem o ambiente, caracterizem os achados e permitam a posição de soluções otimizadas pelos esforços despendidos pela auditoria de sistemas;

- aplicação da tecnologia computacional na área de auditoria de sistemas tanto como instrumental operacional de trabalho do auditor, como ferramenta de administração das atividades das auditorias de sistemas realizadas;

- estudo do benefício/custo de auditoria de sistemas, com a quantificação das economias de dispêndios, advindas da implantação das alternativas de solução, disparadas em função dos achados do auditor de sistemas, em face das despesas incorridas com sua atuação;

- estabelecimento de processos de formação do auditor de sistemas com a definição de conteúdo programático, parte prática e nível de tecnologia a ser repassada aos auditores de sistemas, consolidando dessa forma a carreira profissional;

- ampliação do campo de atuação da auditoria de sistemas, estabelecendo critérios, parâmetros de atuação e conceituação para:
  - auditoria de sistemas atuando intrinsecamente à empresa, ou seja, sob um prisma interno mais próximo e integrado à organização;
  - auditoria de sistemas sob o prisma de atuação externo, isto é, como um agente contestador do comportamento empresarial, movido por forças que não participam da operacionalidade diária da entidade, mas que enxergue a empresa sob a ótica de seu posicionamento em um contexto amplo da economia nacional ou internacional, confrontando as empresas com suas concorrentes;
  - auditoria de sistemas, como a sustentação para a auditoria de gestão, viabilizando e referendando, assim, a validação e avaliação organizacional para a Alta Administração, Direção Executiva, Gerência da Entidade.

É verdade, há mais por fazer do que tudo que já foi feito no escopo de atuação de trabalho da auditoria de sistemas, e esta explosão de necessidades tecnológicas caminha sobre dois vetores distintos que não são conflitantes e só fazem alargar o campo de atuação dos sistemas de informações computadorizados de controle interno:

- ênfase da auditoria de sistemas na validação e avaliação de processos em intensidade igual àquela que vinha sendo exercida para resultados;
- variedade e amplitude da tecnologia computacional com sua multiplicidade de facetas e acelerada evolução, mal permitindo a aclimatação de procedimentos e já exigindo novos investimentos em aprendizado para manutenção da eficiência empresarial.

Outra abordagem e discussão interessante corresponde ao papel de auditor contábil/operacional, em face do auditor de sistemas. As situações seguintes merecem consideração:

I – não será mais adequada a formação de equipes de atuação mistas com a composição de auditores de sistemas especialistas e auditores contábeis/operacionais com pequena ou nenhuma noção de auditoria de sistemas?

II – optaremos pela formação de todos os auditores com a tecnologia de auditoria de computação em todos os graus de dificuldade possível?

III – teremos uma equipe de auditores com formação básica e forte em auditoria de computador, dispensando a formação de auditores de computadores especialistas, internamente à empresa, e contratando, em determinada área de computação, auditores especialistas de empresas de consultoria externas à organização?

IV – não será melhor um ambiente mesclado de uma equipe com auditores contábeis/operacionais (com sólida formação em auditoria de computador), auditores de computação (especialistas em tecnologia de computação de intenso uso na organização) e solicitações esporádicas a empresas externas quando de necessidades específicas de tecnologia de auditoria de sistemas?

Obviamente, as situações serão diversas, em função do porte da empresa e do estágio em computação e em auditoria de computação. Entretanto, algumas constatações e diretrizes devem ser seguidas:

a) todos os auditores devem ter formação em auditoria de computação, necessitando ser definido o patamar de tecnologia a ser incorporado à

equipe, a qual é, evidentemente, condicionada pela tecnologia de computação utilizada pela empresa;

b) há necessidade de atuação de auditores de computação especialistas, particularmente em campos como Teleprocessamento, Banco de Dados, Sistema Operacional, Inteligência Artificial, Administração de Centro de Computação, Gerenciamento de Auditores de Sistemas, entre outros.

Consideramos, ainda, que, para a efetividade do trabalho de auditoria de sistemas, é necessária a compreensão da problemática tanto por parte do auditor de sistemas quanto pelo auditado – profissional de computação ou profissional usuário de computador.

Neste momento, um novo canal se abre para atuação do auditor de sistemas a nível de sedimentação de seu trabalho.

O treinamento dos auditados, tanto profissionais de computação quanto profissionais usuários de computador, deve ser feito abrangendo no mínimo:

- conceituação de auditoria de sistemas;
- controle interno;
- momentos de atuação da auditoria de sistemas (auditoria de sistemas em operação; auditoria de sistemas em desenvolvimento; auditoria do centro de computação);
- produtos finais da auditoria de computador;
- mecânica de implantação das recomendações da auditoria;
- postura do auditado durante a atuação de auditoria de computador.

A problemática, como apresentada, implica a necessidade de especialização dos auditores de sistemas e de intensos investimentos em incorporação de tecnologia por parte da área de auditoria de sistemas.

Obviamente, a área de computação adapta-se e evolui com os novos desafios, que lhe são apresentados e novas funções e atividades surgem e ganham realce, como:

- atuação do profissional de segurança patrimonial/empresarial em segurança de computação, com a conseqüente criação, pelo centro de computação, de um especialista de segurança de computação, internamente à sua área – o analista de segurança de computação;

- preocupação com qualidade, tanto a nível de processos computadorizados, em termos de eficiência, quanto a nível de resultados computadorizados, em termos de eficácia, e a conseqüente criação da função analista de qualidade da computação.

A Figura 1.5 estratifica e apresenta o posicionamento, em termos de estrutura orgânica do auditor de sistemas, do analista de segurança em computação e do analista de qualidade em computação.

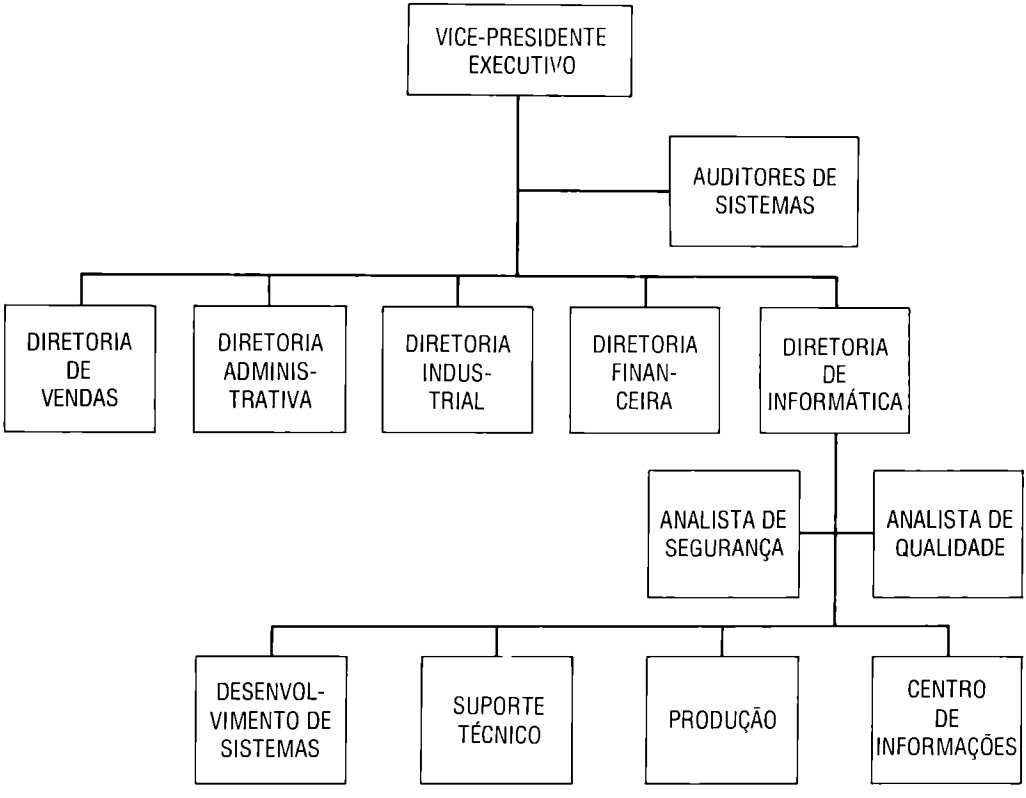


Figura 1.5. *Problemática futura de atuação do auditor de sistemas.*

Com o surgimento do analista de segurança em computação e do analista de qualidade em computação, a atuação do auditor de sistemas irá requerer maior tecnologia e nível de sofisticação, em face de:

a) o analista de segurança em computação ter por função o planejamento e o controle das atividades de segurança em computação; para tal, terá de:

I – criar normas de segurança em computação;

II – gerar e institucionalizar o plano de segurança e o plano de contingência;

III – promover o treinamento dos profissionais de computação em segurança;

IV – acompanhar e verificar o nível de segurança em computação instalada;

b) o analista de qualidade em computação terá de planejar e controlar a qualidade, em termos de eficiência e de eficácia, dos trabalhos de computação via:

I – estabelecimento de normas e padrões operacionais no ambiente computacional;

II – institucionalização de indicadores de qualidade e respectivos sistemas de informações computadorizados para acompanhamento da qualidade em computação;

c) o auditor de sistemas deverá, prioritariamente, inserir em seu plano de trabalho a validação e avaliação do planejamento e do controle dos trabalhos do analista de segurança e do analista de qualidade e das atividades dos demais profissionais de computação no atendimento das especificações de qualidade e segurança pretendidas.

À medida que a área de computação sofistica o exercício das funções administrativas de planejamento, execução e controle, a área de auditoria de sistemas deverá sofisticar sua função administrativa de controle interno.

Na verdade, há a tendência, em termos operacionais, de a auditoria de sistemas ser composta por um pequeno mas seleto grupo de especialistas, que assessore a alta administração em aspectos cruciais da problemática de processamento eletrônico de dados.

O futuro da auditoria de sistemas depende de prioridade para as atividades de planejamento e controle. Assim sendo, o auditor de sistemas atuará de forma direcionada, usando maciçamente no planejamento técnicas de análise de risco, Método Delphi, estatísticas etc. e, no controle, análise dos resultados de sua atuação com o estabelecimento de indicadores de qualidade de seu desempenho, análise de benefício/custo etc.

Os conceitos da administração por confronto, justificativos da existência do auditor de sistemas e da administração por exceção, tônica da atuação do auditor de sistemas, são definitivos e serão exacerbados à medida que a cultura de auditoria de sistemas tornar-se instalada nas entidades.

RESUMO

Nesta introdução foi apresentado o atual estágio, o espectro de atuação e a tendência dos trabalhos da auditoria de sistemas computadorizados. A colocação principal é mapeada por:

- ambiente empresarial atual e futuro, em face do impacto da era da informática;
- ambiente computacional e seus desdobramentos tecnológicos previsíveis;
- auditoria de sistemas e seus desafios presentes e futuros.

Foram descritas as variedades de opções da tecnologia computacional em termos de combinação de *hardware* e as conseqüentes implicações a nível de *software*.

A organização, presentemente, é forçada a reciclar-se pela tecnologia de computação, por agressiva disponibilidade de recursos, possibilitando confrontações e deslocamentos fortes, tanto internos quanto externos.

A deficiência empresarial é uma realidade, em face dos recursos computacionais e da necessidade de adaptação de funcionários/clientes, fornecedores, comunidades etc. Nesse contexto, a auditoria de sistemas é chamada, estimulada e necessita intrinsecamente criar tecnologia e pessoal qualificado para poder acompanhar o ritmo alucinante do impacto da informática nas entidades.

QUESTÕES

1. Descreva o impacto da Era da Informática junto às entidades. Contemple o papel da computação junto ao funcionário, cliente, povo.
2. Qual a diretriz que justifica a existência da auditoria de sistemas? Discuta o papel desta área de atividades (auditoria de sistemas) perante a coletividade, a Nação, as entidades públicas e privadas.

3. Qual a sua opinião sobre a necessidade de treinamento dos profissionais usuários em tecnologia de computação e como a auditoria de sistemas pode ser considerada um canal indutor para aceleração desse treinamento?

4. Quais as características da problemática de colocação da auditoria de sistemas na estrutura orgânica da empresa? Como você vê a atuação de uma auditoria externa a uma entidade? Por exemplo, a correlação empresa de consultoria de auditoria de sistemas *versus* empresa informatizada.

5. Desenvolva o raciocínio acerca da Figura 1.2. Com o que você concorda, do que você discorda, a que aspecto dessa problemática você daria mais ênfase? Quais os pontos fortes e quais os pontos fracos do relacionamento apresentados no quadro?

6. Discorra sobre os fatores que determinam a integração de auditoria de sistemas ao ambiente empresa informatizada.

7. Apresente seu enfoque quanto à auditoria de processos computadorizados e à auditoria de resultados computadorizados.

8. Como você apresentaria oito configurações de computador? Procure atender desde a microempresa até um grande conglomerado financeiro ou industrial. Discorra sobre a problemática de utilização de cada configuração.

9. O que é auditoria de computador?

10. Discuta as etapas básicas da atuação da auditoria de sistemas.

11. O que você entende por independência e duplicidade lógica da atuação da auditoria de sistemas?

12. O que é um sistema de informações computadorizado de controle interno?

13. Debata os conceitos de administração por confronto e de administração por exceção.

14. Quais os tópicos do ambiente de auditoria de sistemas, carentes de maiores investimentos para o futuro dessa área de atividade?

15. Discuta a problemática de treinamento e de composição de uma equipe de auditoria de sistemas. Coloque sua opinião ao final.

16. Qual o papel do analista de segurança em computação?

17. Qual o papel do analista de qualidade em computação?

18. Discuta o trinômio auditoria de sistemas – analista de segurança em computação – analista de qualidade em computação.

2 A Auditoria de Computadores

2.1 CONCEITUAÇÃO

A área de Auditoria de Processamento Eletrônico de Dados (PED) compreende terminologia, conceituação e técnicas de três áreas distintas de conhecimento:

- auditoria;
- sistemas de informações;
- processamento eletrônico de dados.

Evidentemente, outras áreas do conhecimento humano contribuem para a execução de uma auditoria de computador, mas as três áreas citadas formam a base.

A Figura 2.1 estrutura essa situação.

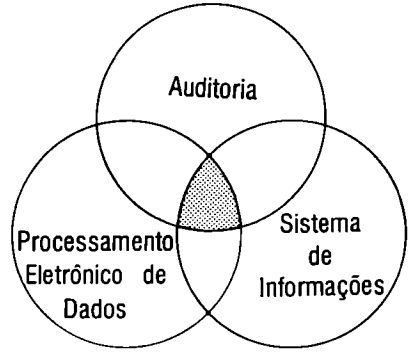


Figura 2.1 *Áreas de conhecimento que formam a base da atividade de auditoria de computador.*

O segmento hachurado da Figura 2.1 mostra o núcleo de onde emerge a auditoria de computador; entretanto, como em seguida veremos, a auditoria de sistemas de informações computadorizados varre, interliga-se e permeia as três áreas do conhecimento que lhe servem de base.

A área de Processamento Eletrônico de Dados é aquela que começa com os conceitos de *hardware* e de *software* e cresce enlaçando-se com a área de telecomunicações, criando ambientes altamente sofisticados e abrangentes de atuação.

No tópico 1.2 do Capítulo 1, pudemos rapidamente descrever estruturas variadas e crescentes de uso da tecnologia computacional.

Para melhor estruturação da área de Processamento Eletrônico de Dados, podemos compô-la da seguinte forma:

1. **Hardware:** compreende dispositivos e equipamentos que compõem uma configuração de computador (Unidade Central de Processamento, Unidades de Disco Magnético, cabos de conexão de periféricos e dispositivos de computação, terminais, impressoras etc.)
2. **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*.
3. **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.
4. **Software aplicativo:** conjunto de instruções e programas escritos pelos programadores ou usuários de computação para a conversão do dado em informação, com a conseqüente solução do problema que enfrentam.
5. **Teleprocessamento:** entrelaçamento da área de computação com a área de telecomunicações, permitindo a conexão de equipamentos de processamento eletrônico de dados localizados a grandes distâncias físicas. Permite 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.

Os sistemas de informações fazem parte da vida intelectual do homem, e existem para servi-lo. Entretanto, necessitamos caracterizar sistemas de informações e, por isso, vamos utilizar a definição a seguir:

> *"Sistemas de informações compreendem um conjunto de recursos humanos, materiais, tecnológicos e financeiros, combinados segundo uma seqüência lógica para transformar dados em informações."*

No ambiente de auditoria de computadores podemos detalhar da seguinte forma essa definição:

- 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, fitotecários 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 de computador) 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);
- recurso financeiro é a transformação dos recursos humanos, materiais e tecnológicos, segundo o denominador comum moeda;
- a 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 (instruções de computador formando programas);
- os dados e as informações são estáticos e são os resultados – inicial e final – dos processos executados.

Tanto processos quanto resultados são intangíveis e, portanto, correspondem a recursos tecnológicos que, para serem acionados, necessitam estar agregados a recursos humanos e a recursos materiais.

A área de auditoria implica a validação e avaliação do controle interno de sistemas de informações em processamento eletrônico de dados.

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

a) **Fidelidade 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 mesmo 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 compõem 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 dos 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 às políticas 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.

É importante notar que os parâmetros apresentados retratam a definição de controle interno do AICPA – American Institute of Certified Public Accountants – e traduzida pelo IBRACON – Instituto Brasileiro de Contadores do Brasil.

A caracterização do AICPA/IBRACON estabelece ainda que o controle interno é dividido em dois subconjuntos:

- controle interno contábil;
- controle interno administrativo.

Os parâmetros de *a* a *f* dizem respeito a controle interno contábil e os parâmetros *g, h, i* dizem respeito a controle interno administrativo.

Entretanto, consideramos de maior objetividade para atuação da auditoria interna e da auditoria de computador o trabalho com os parâmetros como apresentados.

Temos utilizado metodologias em que a definição de sistemas de informações e de controle interno facilitam a elaboração de papéis de trabalho, o uso de matrizes, a administração da qualidade da auditoria de sistemas e a análise de risco a ser feita.

Dessa forma, as palavras-chave para uma adequada auditoria de computador são:

- recurso humano;
- recurso material;
- recurso tecnológico;
- recurso financeiro;
- dados;
- informações;
- seqüência lógica;
- fidelidade da informação em relação ao dado;
- segurança física;
- segurança lógica;
- segurança ambiental;
- confidencialidade;
- obediência à legislação em vigor;
- eficiência;
- eficácia;
- obediência às políticas da alta administração.

2.2 FORMA DE ATUAÇÃO

A auditoria de computador pode ocorrer:

- via sistema de informação computadorizado ou centro de computação;
- em nível de processo ou de resultados.

Quando atuamos via sistema computadorizado, temos como primeira tarefa retratar o fluxo do sistema e para tal temos usado a técnica de Diagrama de Fluxo de Dados (D.F.D.). (Ver Capítulo 4, Figuras 4.2 e 4.3).

Na atuação via centro de computação necessitamos do *layout* da instalação física, da estrutura orgânica e das normas administrativas, técnicas e operacionais vigentes.

Os trabalhos de auditoria desenvolvidos via sistema computadorizado contemplam os parâmetros do controle interno:

- fidelidade da informação em relação ao dado;
- segurança física;
- segurança lógica;
- confidencialidade;
- obediência à legislação;
- eficiência;
- eficácia;
- obediência às políticas da alta administração.

Os trabalhos de auditoria do centro de computação contemplam os parâmetros:

- segurança ambiental;
- obediência à legislação;
- eficiência;
- eficácia;
- obediência às políticas da alta administração.

Na realidade, o parâmetro segurança ambiental contempla os parâmetros segurança física dos recursos humanos e materiais, segurança lógica quanto a erros, fraudes, modificações de recursos tecnológicos e confidencialidade quan-

to a captação indevida de recursos tecnológicos, todos estes recursos componentes da infra-estrutura do centro de computação ou, então, de uso comum por diversos sistemas de informações aplicativos computadorizados.

Outrossim, o parâmetro fidelidade da informação em relação ao dado atende à necessidade de integridade do dado, isto porque precisamos, como auditores, garantir que todos os dados de que foram alimentados os sistemas computadorizados receberam tratamento pelos programas que compõem esse sistema computadorizado e, mais ainda, que durante o processo ocorrido não foram introduzidos outros dados espúrios ao sistema computadorizado sob auditoria.

O parâmetro fidelidade da informação casa-se adequadamente com o conceito de *audit-trail* ou trilha de auditoria, a qual estabelece a necessidade de, a partir das informações, podermos recompor os dados.

Para garantirmos a fidelidade da informação em relação ao dado, devemos criar o arquivo de informações de controle (AIC), o qual materializa o conceito de *audit-trail* em um sistema computadorizado.

O AIC deverá conter acumuladores que, por natureza de registro, permitam a monitorização, tanto imediata quanto a posteriori, do processamento de todos os dados e só deles pelo sistema sob auditoria.

A Figura 2.2 especifica uma trilha de auditoria computadorizada.

Portanto, o parâmetro fidelidade da informação busca a veracidade do recurso tecnológico, enquanto o parâmetro segurança lógica busca a correção dos recursos tecnológicos.

Assim, a rotina que verifica se o líquido a pagar é negativo faz parte do instrumental para garantir a segurança lógica do sistema computadorizado de folha de pagamento.

A auditoria de computador em nível de processos trata com rotinas operacionais e com rotinas de controle e em nível de resultados trata com informações/registros/arquivos operacionais e de controle.

Processos ou rotinas operacionais são aqueles que efetivamente transformam os dados em informações. Assim, por exemplo, a rotina de cálculo do Imposto de Renda, a rotina de atualização do cadastro de funcionários estão dando tratamento aos dados e gerando informações que implicam a existência do sistema computadorizado de folha de pagamento.

Processos ou rotinas de controle são aqueles agregados aos processos operacionais e que os monitoram ou controlam, gerando informações de controle em função da natureza das informações operacionais criadas pelas rotinas operacionais.

Em sistemas de informações computadorizados podemos, portanto, caracterizar como rotinas de controle:

a) Rotinas de crítica que verificam a validade de informações operacionais e geram informações de controle, apontando a incorreção nessas informações operacionais. Por exemplo, o código do produto que deveria ser numérico e foi submetido ao sistema com caracteres alfabéticos; outro exemplo são rotinas de controle que identificam informações operacionais ou de controle fora de limites, que é o caso de informações operacionais alimentadas no sistema fora de prazo ou de erros ocorridos no sistema e não corrigidos em tempo oportuno.

b) Rotinas de consistência que dão tratamento à não-oportunidade de atuação de rotinas operacionais. Por exemplo, listar a inclusão de um item no cadastro por impossibilidade de a operação ser feita, já que foi constatada pela rotina operacional a existência de um item idêntico no cadastro.

Obviamente, as rotinas de controle geram informações, registros e arquivos de controle.

O Quadro 2.1 resume e exemplifica os conceitos emitidos.

Naturalmente, em arquivos operacionais encontramos, também, registros e informações de controle que monitoram registros e informações operacionais. Assim o arquivo Cadastro de Funcionários tem registros com informações operacionais quanto aos funcionários, como nome do funcionário, salário-base etc. e tem registros de controle, como os registros *header*, que contêm a identificação do arquivo e *trailer*, que contêm totais de controle.

Analisando sob a ótica de parâmetros do controle interno, podemos ter:

a) Para fidelidade da informação em relação ao dado:

- o Arquivo de Informações de Controle (AIC) citado na Figura 2.2;
- o arquivo de erros pendentes a *n* ciclos de processamento: arquivo que monitora todo dado submetido ao sistema;
- a listagem de erros pendentes e não corrigidos a *n* ciclos de processamento: esta listagem é encaminhada para a controladoria, por exemplo, tomar conhecimento da manutenção de um erro no processo por período de tempo indevido;
- a informação código do arquivo gravada no registro *header*: para evitar a alimentação de geração de arquivo indevida no processamento do sistema;
- a informação data de gravação do arquivo no registro *header*.

Quadro 2.1. *Rotinas e informações operacionais e de controle.*

NATUREZA DO PROCESSO/ /RESULTADO	EXEMPLOS
Rotina operacional	– Rotina de atualização do cadastro de itens em estoque. – Rotina de cálculo do saldo em estoque.
Informação operacional	– Informações do cadastro de estoque atualizado. – Informação do saldo em estoque.
Rotina de controle	– Rotina de gravação ou impressão de tentativa de inclusão de item já existente no cadastro de estoque. – Rotina de verificação quanto ao fato de o saldo do item em estoque ser negativo.
Informação de controle	– Item a ser incluído, já existente no cadastro de estoques e listado no relatório de erros na atualização. – Item em estoque com saldo negativo e impresso em relatório de erros.

b) Para segurança lógica:

- informação *password* gravada no registro *header* do arquivo;
- informação de saldo de item em estoque negativo gravada ou impressa em relatórios de exceção;
- informações dos relatórios de crítica e de consistência referentes a incorreções dos dados de que foi alimentado o sistema;
- informações de *hash* total do registro *trailer:* o somatório da quantidade de dependentes do funcionário. Esta informação é importante para o cálculo do Imposto de Renda.

c) Para confidencialidade:

- rotina de criptografia das informações operacionais sensíveis.

É importante notar que podemos também casar o parâmetro do controle interno com a natureza do achado da auditoria:

1. O parâmetro segurança lógica busca a identificação de: erros, omissões, falhas e falta de procedimentos.
2. O parâmetro eficiência quando não atendido pode indicar:
   - duplicidade de procedimentos e resultados;
   - desbalanceamento ou inadequação na aplicação de recursos humanos, materiais e tecnológicos.
3. O parâmetro eficácia busca a correção e adequabilidade dos resultados.
4. O parâmetro fidelidade da informação em relação ao dado lida com falta ou erros de resultados.
5. O parâmetro confidencialidade diz respeito à captação indevida de processos e resultados.
6. Os parâmetros obediência à legislação e as políticas de alta administração referem-se à correção dos procedimentos em atendimento a normas estabelecidas.

Toda a problemática apresentada visa ao debate acerca das atividades de auditoria de sistemas que se voltam para o conceito de ponto de controle.

Ponto de controle é a situação do ambiente computacional caracterizada pelo auditor como de interesse para validação e avaliação.

Ora, esta caracterização de ponto de controle expõe toda a abrangência do trabalho de auditoria de computador em face da independência de o auditor ser o responsável único pela determinação do que, como e com que objetivos auditar.

Assim, o ponto de controle tanto pode ser o sistema integrado contábil-financeiro, quanto o banco de dados de materiais, quanto o campo *password* do registro *header* do Arquivo Cadastro de Estoque.

O objetivo da auditoria do Ponto de Controle tanto pode ser sob a ótica do parâmetro do controle interno-segurança lógica, eficiência, confidencialidade etc. – quanto sob a ótica da fraqueza passível de ser identificada – erro, omissão, falha, falta, omissão de procedimentos ou falta, erro, correção de resultados.

O como auditar o Ponto de Controle será apresentado quando da discussão das técnicas de auditoria de computador, no Capítulo 3, e na auditoria do ambiente computacional, no Capítulo 4.

O Ponto de Controle necessita ser caracterizado e podemos estabelecer sua composição em termos de:

- uma combinação de rotinas e informações operacionais e de controle;
- recursos humanos, materiais e tecnológicos agrupados.

A dissecação ou a redução a suas unidades é capital para o entendimento e a validação e avaliação do Ponto de Controle.

Portanto, o Ponto de Controle "Programa de Atualização" normalmente é composto de:

- rotina operacional de atualização do cadastro;
- rotina de controle: inclusão, exclusão, alteração do Arquivo Movimento indevida e sua correspondente listagem;
- informação operacional: conteúdo do registro significativo ou detalhe do Arquivo Cadastro Anterior;
- informação de controle: conteúdo do Arquivo Erros na atualização.

Outra forma de se decompor o Ponto de Controle "Programa de Atualização" é:

- recursos tecnológicos: informações componentes dos arquivos trabalhados e instruções componentes do programa de atualização;
- recursos materiais:. configuração do computador onde é processado o programa de atualização e dispositivos (*disk-pack, drive* de disco, carretel de fita magnética, formulário contínuo) onde são colocadas as informações;
- recurso humano: operador do computador no momento do processamento do programa de atualização;
- recurso financeiro: valor que representa a combinação dos recursos humanos, materiais e tecnológicos componentes do programa de atualização.

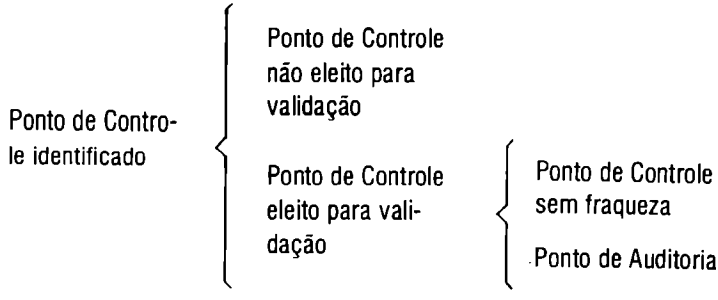
O Ponto de Controle deve ser, durante o processo de auditagem:

- identificado dentro do ambiente computadorizado;
- caracterizado em termos de seus recursos componentes e estabelecido em termos de processos e resultados;
- analisado em termos de risco; para tal é discutido sob a ótica dos parâmetros do controle interno, segundo a natureza da fraqueza passível de ocorrer.

E ainda deve ser:

- determinada a técnica de auditoria que se identifique com os objetivos de risco parametrizados;
- aplicada a técnica de auditoria correspondente;
- analisados os resultados apurados das técnicas de auditoria aplicadas, enquadrados pelos objetivos de risco definidos;
- apresentada uma opinião que consubstancie a avaliação do Ponto de Controle validado.

Existe um ciclo de vida do Ponto de Controle estabelecido em termos de:



A Auditoria de Posição ocorre desde o momento em que o Ponto de Controle é identificado até o instante em que, via avaliação dos resultados de sua validação, ele é determinado como apresentando fraqueza, consoante a análise de risco realizada.

A Auditoria de Acompanhamento reflete as etapas e momentos em que, uma vez caracterizada a fraqueza do Ponto de Auditoria, alternativas de solução são apresentadas e discutidas pela auditoria com o auditado, até o momento em que as correções são efetuadas e declaradas pelo auditado, tornando o Ponto de Auditoria novamente um Ponto de Controle.

Para apoio à hierarquização dos pontos de controle com vistas no nível de interesse de sua avaliação ou de análise dos riscos potenciais que corre a organização, usamos os seguintes conceitos:

a) *Walkthrough:*

- corresponde à representação gráfica de todo o ambiente computacional sob auditoria;

- mais uma vez, usamos o DFD (ver capítulo 4, Figuras 4.2 e 4.3) para representar todos os processos e resultados operacionais e de controle de determinado sistema de informação;
- temos representado também, via DFD, o *walkthrough* da área de produção e a mecânica de desenvolvimento de sistemas, ou seja, a aplicação de uma metodologia de desenvolvimento de sistemas.

b) *Walktruth:*

- o caminho verdade, isto é, o conjunto de rotinas e informações operacionais mínimas e indispensáveis para a transformação do dado em informação.

c) *Audit trail:*

- o conjunto de rotinas e arquivos de controle que permitem, a partir das informações, reconstituírmos os dados.

d) Rotinas e resultados operacionais e de controle considerados não pertencentes ao *Walktruth,* nem ao *Audit trail.*

É importante notar que o somatório de processos e resultados componentes dos itens *b, c, d* deve ser igual à quantidade de processos e resultados que compõem o item *a.*

Classifica-se também o controle pela sua colocação dentro da seqüência de tempo em que ocorre um processo. Assim podemos ter:

1. **Pré-controle:**
   - rotinas e resultados embutidos e obtidos no início de um processamento, com o objetivo de garantir às rotinas operacionais a qualidade dos dados de que elas são alimentadas;
   - o programa de crítica e as primeiras rotinas de controle do programa de atualização são parte integrante do segmento de pré-controle;
   - a monitoração do erro via Arquivo de Erros Pendentes é das principais peças do pré-controle.

2. **Controle corrente:**
   - rotinas e informações de controle que acompanham o processamento ou que validam e dão o aval às informações operacionais geradas a cada seqüência de rotinas operacionais, concordando que as rotinas

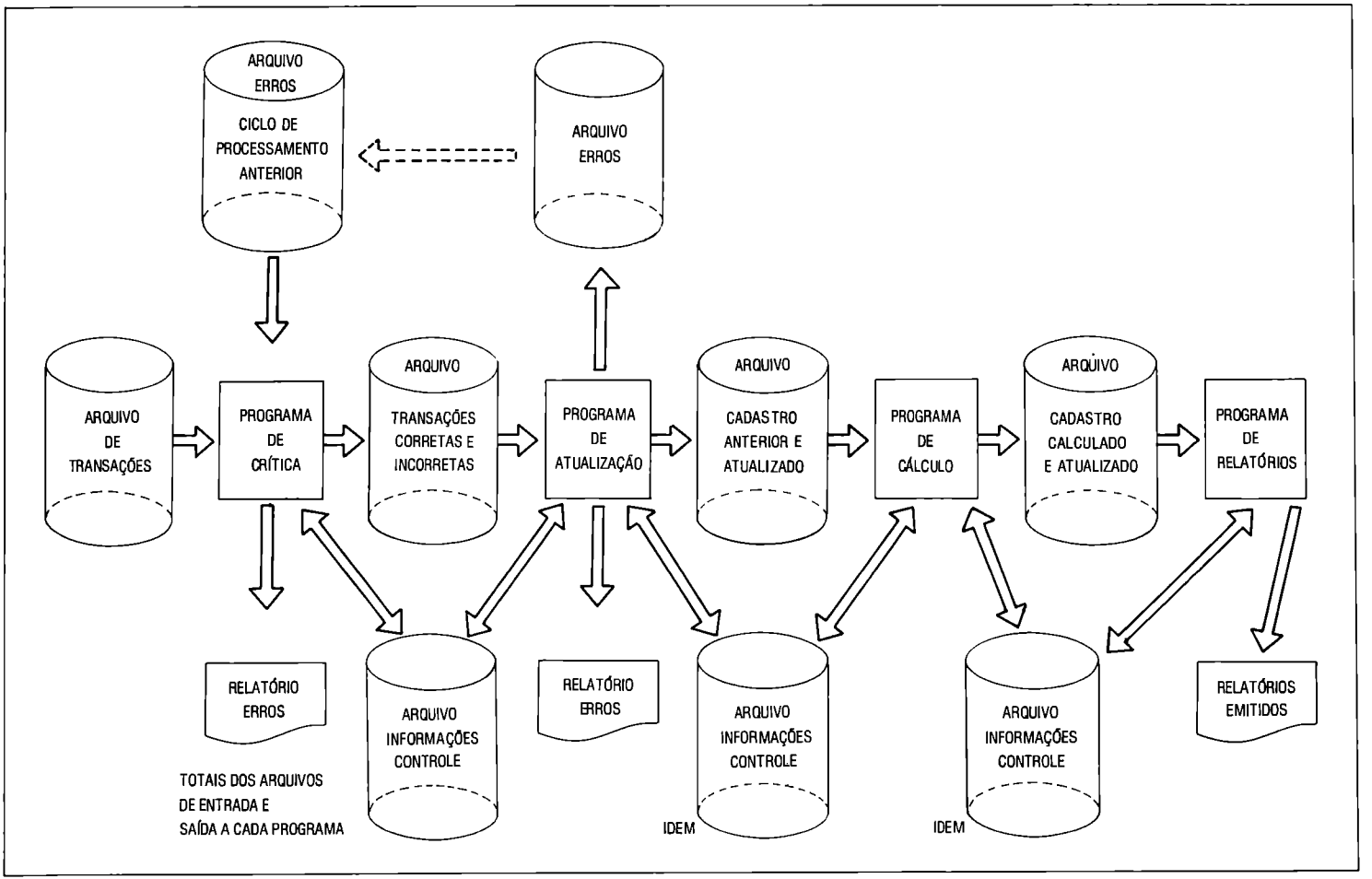


Figura 2.2. *Trilha de auditoria: o Arquivo de Informações de Controle (AIC) de um sistema computadorizado clássico.*

operacionais subseqüentes continuem a dar tratamento às informações operacionais semi-elaboradas;

- o Arquivo de Informações de Controle (AIC) (vide Figura 2.2) e os arquivos estatísticos de acompanhamento de informações no limite do erro, as rotinas de verificação de informações operacionais negativas ou dentro de limites estabelecidos em tabelas, todos são exemplos de recursos tecnológicos componentes do controle corrente.

3. **Pós-controle:**

   - são rotinas que fazem cruzamentos entre diversas informações operacionais finais geradas, ou entre informações finais e informações iniciais;
   - no tocante à correlação entre informações finais tem-se que o total do líquido a pagar da folha de pagamento deve ser igual ao total dos valores depositados como líquido a pagar na conta bancária de cada funcionário;
   - quanto ao cruzamento de informações finais e iniciais poder-se-á ter a operação do total de funcionários da folha de pagamento do mês anterior menos o total de funcionários excluídos e mais o total de funcionários incluídos, obtendo-se o total de funcionários da presente folha de pagamento.

Como foi visto, o controle interno atua por cima de rotinas e resultados operacionais e de controle. Realmente, o controle sempre pressupõe um planejamento, mesmo que seja um padrão arbitrado. A auditoria de sistemas, valendo-se de sua função administrativa de controle interno, atua prioritariamente na validação da função administrativa de controle, voltando-se subseqüentemente para as funções administrativas de execução e planejamento.

2.3 ANÁLISE DE RISCO

A escolha do Ponto de Controle em termos de sua identificação, caracterização e hierarquização implica a tarefa de planejamento da auditoria.

A atividade primeira do auditor de sistemas é, na verdade, conhecer o ambiente a ser auditado. Para o conhecimento da problemática, onde ocorrerá a atuação do auditor, uma série de tarefas será desempenhada pelo auditor de sistemas:

a) levantamento de dados acerca do ambiente computacional como:

- fluxo de processamento;
- inventário de recursos humanos e materiais envolvidos;
- arquivos processados;
- relatórios e telas produzidos;
- divisão do ambiente em subambientes;

b) estudo da documentação do ambiente computacional;

c) complementação de informações acerca do ambiente computacional;

d) visita ao ambiente computacional;

e) entrevistas com os recursos humanos componentes do ambiente computacional.

A atividade de planejamento da auditoria do ambiente computacional pode ser descrita, então, em:

a) conhecimento do ambiente computacional;

b) determinação dos Pontos de Controle;

c) estabelecimento dos objetivos de validação e de avaliação dos Pontos de Controle:

- os objetivos de validação do Ponto de Controle implicam:
  - a caracterização das técnicas de auditoria a serem aplicadas;
  - prazos de execução da validação;
  - custos incorridos com a validação;
  - nível de tecnologia para a validação necessária do auditor;
- os objetivos de avaliação do Ponto de Controle correspondem a:
  - natureza da fraqueza de controle interno passível de ser alcançada;

d) análise de sensibilidade do nível de interesse de validação e avaliação de cada Ponto de Controle:

  - estabelecimento de critérios para análise de risco em função do planejamento já efetuado;

e) hierarquização dos Pontos de Controle:

- via votação com a eleição e o estabelecimento de prioridades dos pontos de controle vigentes;

f) documentação de todo o processo de planejamento da auditoria de sistemas.

O momento inicial deste planejamento da auditoria de sistemas é aquele em que um ou mais profissionais deverão enxergar os Pontos de Controle de maneira isenta e independente, buscando a ausência de preconceitos e de posições tendenciosas, para o desempenho de um trabalho de auditoria com qualidade.

Duas posições ocorrem quando o auditor de sistemas enfrenta a problemática de análise de sensibilidade de um elenco de Pontos de Controle:

a) o auditor de sistemas conta com fontes referenciais históricas documentadas e estatisticamente tratadas para apoio na tomada de decisões a ser efetuada;

b) o auditor de sistemas não conta com fontes referenciais precisas, mas tão-somente com informações de memória esparsas e registradas como acontecimentos de sua vida profissional.

Dados estatísticos sobre auditorias, anteriormente realizadas, dificilmente são encontrados; entretanto, é de interesse capital para a melhoria da qualidade das futuras auditorias.

As estatísticas necessitam contemplar informações como:

- tipo de técnica de auditoria aplicada por natureza de Ponto de Controle;
- tempo médio de validação despendido por tipo de técnica e de natureza de Ponto de Controle;
- quantidade de Pontos de Controle validados por classe de Pontos de Controle estruturada;
- parâmetros do controle interno mais validados;
- parâmetro do controle interno e tipo de técnica aplicada e natureza de Ponto de Controle;
- espécie de fraqueza de controle interno identificada por classe de Ponto de Controle;
- tempo médio de adoção de solução por tipo de fraqueza caracterizada.

Na realidade, as estatísticas necessitam quantificar e cruzar essas quantificações referentes a:

- classe de Ponto de Controle;
- técnica de auditoria de sistemas aplicada;
- parâmetro do controle interno contemplado;
- prazo de validação;
- natureza da fraqueza de controle interno achada;
- prazo de adoção de solução para a fraqueza encontrada.

No Capítulo 5 item 5.4 está detalhada uma experiência que vivemos desde 1977, na coleta e tabulação do conteúdo de Pontos de Controle, com a criação e manutenção de um cadastro de Pontos de Controle.

Se o auditor de sistemas possuir fonte de referência em termos de um cadastro de Pontos de Controle devidamente tabulado, realizará sua análise de risco com excelente base de sustentação:

- terá um elenco de Pontos de Controle detalhados;
- saberá que fraquezas são possíveis e qual o nível de intensidade de sua ocorrência;
- quais os prováveis custos incorridos com a auditoria de cada Ponto de Controle;
- qual o nível de tecnologia necessário para sua atuação;
- quais os benefícios que podem ser esperados de sua atuação.

Normalmente, o auditor de sistemas não conta com fontes referenciais para sua atuação e lança-se à auditoria do ambiente computacional a cada vez como se fosse a primeira vez, esforçando-se por relembrar casos vividos, lidos ou ouvidos do ambiente de computação, os quais formam a sua cultura de atuação em auditoria de computação e que servirão de base para sua eleição e priorização dos Pontos de Controle.

Em qualquer dos casos que o auditor tenha melhor ou pior caracterização da problemática de auditoria de computação, uma mecânica de análise de risco deve ser disparada.

Neste momento, o auditor de sistemas poderá estar fazendo seu planejamento sozinho ou poderá contar com a participação de outros profissionais, por exemplo:

- um representante da alta administração;
- um executivo da área usuária;
- um executivo de computação;

- um profissional de consultoria externa em auditoria de computação, com experiência no ambiente computacional específico.

O ambiente computacional poderá ser de teleprocessamento com banco de dados, ou de microinformática, ou de sistemas especialistas na área de inteligência artificial, ou, ainda, sistemas CAD *(Computer Aided Design)*.

Quer o auditor de sistemas esteja sozinho ou faça parte de uma comissão, para o planejamento de auditoria de sistemas, um sistema de pontos necessita ser estruturado. Temos adotado a seguinte pontuação:

1 = muito fraco
2 = fraco
3 = regular
4 = forte
5 = muito forte

O auditor de sistemas poderá, então, exercer seu poder de votação segundo um elenco de matrizes que poderão ser moldadas conforme o projeto de auditoria de sistemas disparado. Assim, teremos a matriz Ponto de Controle/Parâmetro Controle Interno/Voto.

Quadro 2.2. *Matriz ponto de controle/parâmetro controle interno/voto.*

NOME:PONTO DE CONTROLE	PARÂMETRO CONTROLE INTERNO CONTEMPLADO	VOTO APURADO
Cadastro de funcionários atualizado	Segurança lógica Eficiência Obediência à legislação	3 2 1
Programa de cálculos	Confidencialidade	5

Outra matriz de votação para efeito de análise de risco é a matriz Ponto de Controle/Natureza da Fraqueza de Controle Interno/Voto.

Quadro 2.3. *Matriz ponto de controle/natureza da fraqueza de controle interno/voto.*

NOME: PONTO DE CONTROLE	NATUREZA FRAQUEZA CONTROLE INTERNO	VOTO APURADO
Relatórios emitidos pelo sistema Contas a Receber	Duplicidade de relatórios Falta de relatórios Omissão de relatórios	4 3 2
Arquivo Tabelas Sistema Controle de Estoques.	Falha na organização do arquivo	5

A matriz Ponto de Controle/Técnica de Auditoria Aplicada constitui também uma matriz de votação em termos de análise de risco correspondente.

Quadro 2.4. *Matriz ponto de controle/técnica de auditoria aplicada.*

NOME: PONTO DE CONTROLE	TÉCNICA DE AUDITORIA APLICADA	VOTO APURADO
Uso do **hardware** e **software**	– Programa de computador para análise do arquivo **Log** ou **Job accounting** – Análise da listagem da **console** – Análise do livro de ocorrências	4 3 2

Evidentemente, o auditor de sistema poderá fazer sua análise de risco:

a) considerando apenas uma matriz;

b) usando uma combinação de matrizes de graus de importância idêntica;

c) dando maior peso a determinadas matrizes em relação às outras;

d) tendo sempre um conjunto de matrizes-padrão a ser aplicado junto a todos os projetos de auditoria, com grau de importância de matriz ponderado ou não.

Quadro 2.5. *Folha-padrão para análise de risco de pontos de controle.*

NOME: PONTO DE CONTROLE	PARÂMETRO CONTROLE INTERNO CONTEMPLADO	VOTO APURADO	NATUREZA FRAQUEZA CONTROLE INTERNO	VOTO APURADO	TÉCNICA AUDITORIA APLICADA	VOTO APURADO	VOTO MÉDIO
Cadastro de funcionários	Segurança lógica	3	Erro no conteúdo do arquivo	4	Programa de computador	3	3,3
					Análise das rotinas de controle do conteúdo do arquivo	5	4
			Falha na organização do arquivo	5	Análise do layout do arquivo	4	4
	Segurança física	5	Falta de arquivo back-up	2	Visita à fitoteca de back-up	3	3,3

Nos exemplos apresentados foi variado o Ponto de Controle, porém pode-se considerar em uma matriz única e mais abrangente, para cada Ponto de Controle, mais de um tipo de parâmetro, para efeito de análise de risco. Vota-se e estabelece-se a média aritmética para a determinação da hierarquia dos Pontos de Controle a serem validados e avaliados. A Figura 2.3 detalha a problemática discutida.

A lógica de votação corresponde à sensibilidade de intensidade de ocorrência de fraqueza e o voto é dado em função de ocorrências passadas registradas e tratadas estatisticamente ou, então, da sensibilidade do eleitor.

Assim, no Quadro 2.5 há um voto 5 para segurança física e um voto 3 para segurança lógica em face de, estatisticamente, em dado universo ter havido mais identificação de fraquezas sob a ótica de segurança física do que de segurança lógica.

Da mesma forma, falha na organização do arquivo recebeu voto 1 e falta de arquivo *back-up* voto 2, em função da natureza de a primeira fraqueza ser de maior possibilidade de ocorrência.

Outro vetor para a lógica de votação é dar o ponto em termos de comparação entre fatores de mesmo ambiente; assim, naquele momento histórico ou naquele projeto de auditoria, no Quadro 2.5, para o Ponto de Controle Cadastro de Funcionários, segurança física é mais importante que segurança lógica e falha na organização do arquivo é mais importante que erro no conteúdo do arquivo e, ainda, a análise das rotinas de controle do conteúdo do arquivo é mais efetiva que programa de computador.

Outro vetor para a lógica de votação é o caráter linear ou a coerência entre os fatores parâmetro controle interno contemplado; natureza da fraqueza controle interno; técnica de auditoria aplicada.

A realidade é que a pontuação impõe ao leitor uma análise de sensibilidade que segue um ou mais vetores (parâmetros de controle interno) para a lógica de votação, como aqui apresentados.

Neste momento, observa-se a necessidade de o planejamento da auditoria de sistemas:

a) contar com efetivo sistema computadorizado de administração de Pontos de Controle, com o devido tratamento estatístico efetuado, para dar sustentação às prioridades a serem estabelecidas;

b) ser realizado por mais de um profissional, para que haja a oportunidade de serem variados e considerados vários enfoques de atuação.

Estamos empregando o Método Delphi para a determinação das prioridades, já que estabelecemos notas, ponderadas ou não, dadas por profissionais distintos ou por um mesmo profissional que atua segundo lógicas ou enfoques distintos de votação.

Consideramos muito importante que o planejamento da auditoria de sistemas seja feito por mais de um profissional, no mínimo dois – o gerente de auditoria e o auditor de sistemas.

Devemos destacar que consideramos cada auditoria de computador realizada como um projeto de auditoria de sistemas que, como tal, tem suas etapas de planejamento, execução e controle; possui um orçamento financeiro ou em termos de tempo e sobre o qual é feita uma análise do retorno do investimento, isto é, uma análise de benefício/custo, determinando a validade de cada projeto ocorrido.

O orçamento financeiro ou de tempo está enquadrado no plano diretor anual de auditoria de sistemas.

A análise do retorno do investimento para cada projeto de auditoria de sistemas corresponde à apuração e confrontação do valor despendido com a auditoria versus o valor advindo dos benefícios identificados com a adoção das alternativas de solução propostas para as fraquezas de controle interno determinadas.

A análise de benefício/custo é feita com a pontuação tanto dos esforços despendidos com a auditoria de sistemas, quanto com os benefícios advindos do ambiente computacional pela atuação da auditoria.

O planejamento da auditoria de sistemas é vital, principalmente, por dar objetividade ao processo de auditagem e permitir a otimização das auditorias.

2.4 PRODUTOS GERADOS

A auditoria de sistemas necessita retratar o resultado de seus trabalhos e, para tal, vale-se dos seguintes relatórios:

a) relatório de fraquezas de controle interno;
b) certificado de controle interno;
c) relatório de redução de custos;
d) manual de auditoria do ambiente computadorizado auditado.

O relatório de fraquezas de controle interno tem por objetivo apresentar os resultados do trabalho da auditoria de sistemas, estruturado em:

- objetivos do projeto de auditoria;
- pontos de controle auditados;
- conclusão alcançada a cada ponto de controle;
- alternativas de solução propostas para correção das fraquezas de controle interno identificadas.

CERTIFICADO DE CONTROLE INTERNO

Certificamos que o sistema . . . . . da empresa . . . . . /... /... , atende satisfatoriamente aos requisitos básicos de controle interno, exigido para a validação do sistema, no mercado brasileiro, com as ressalvas estabelecidas no relatório de fraquezas de controle interno do sistema . . . . . (Relatório ACI . . . . . .)

Assinatura/executivo do projeto

É inerente ao trabalho do auditor de sistemas a apresentação de soluções para a resolução dos pontos fracos determinados.

Há necessidade da emissão do certificado de controle interno com a colocação clara se o ambiente computacional auditado se encontra em boa, razoável ou má situação no tocante aos parâmetros do controle interno.

O certificado de controle interno apresenta a opinião da auditoria em termos globais e sintéticos, permitindo a colocação e reunião dos achados, de fraquezas de controle interno, dos vários pontos de controle auditados, sob uma ótica de avaliação e de emissão de opinião total.

O certificado de controle interno permite a venda imediata dos resultados dos trabalhos de auditoria de sistemas para a alta administração. Podemos, inclusive, fazer referência, neste certificado, aos pontos de auditoria com fraquezas de maior intensidade ou gravidade.

O relatório de redução de custos é um subconjunto do relatório de fraquezas de controle interno que tem por objetivo explicitar as economias financeiras a serem feitas com a adoção das recomendações efetuadas.

O relatório de redução de custos serve de base para a realização das análises de retorno do investimento e de benefício/custo a serem realizadas como parte do momento controle dos projetos de auditoria de sistemas.

O manual de auditoria do ambiente computadorizado auditado armazena o planejamento da auditoria feito, os pontos de controle inventariados, os pontos de controle testados e os pontos de auditoria flagrados. Serve, portanto, esse manual como referencial e base para as futuras auditorias daquele mesmo ambiente computacional a serem realizadas.

O manual de auditoria, ao longo dos trabalhos de auditoria realizados, irá tratar da evolução tanto do ambiente computadorizado, quanto dos processos de auditagem.

O conjunto de manuais de auditoria irá, ao longo dos anos, servir como comprovação histórica das atividades de auditoria de sistemas.

Entretanto, outro conjunto de papéis de trabalho é elaborado durante o projeto de auditoria de sistemas:

a) pasta permanente;
b) pasta de acompanhamento;
c) pasta-mestre.

A pasta permanente possui todo o levantamento, todo o estudo e a caracterização do ambiente computacional, sob auditoria.

O índice de uma pasta permanente contempla, basicamente:

- relação de sistemas computadorizados;
- *layout* do centro de computação;
- resumo da metodologia de desenvolvimento de sistemas vigente;
- relação de arquivos trabalhados pelos sistemas;
- relação de relatórios/telas emitidos;
- relação de programas;
- fluxo do sistema de informação computadorizado sob auditoria;
- relação dos cargos existentes no centro de computação;
- relação das normas;
- relação da legislação pertinente ao ambiente sob auditoria.

A pasta de acompanhamento é administrativa; dela constam cópias de atas de reunião, cronograma de desenvolvimento do projeto de auditoria, correspondências trocadas com os auditados e para solicitação de meios para a realização da auditoria, como:

- reserva de horas de computador;

- autorização para serem efetuadas visitas a locais reservados do centro de computação;
- marcação de entrevistas com o pessoal de computação;
- requisição de documentação de sistemas e de normas do ambiente computacional;
- encaminhamento dos produtos finais da auditoria realizada.

A pasta-mestre é técnico-operacional; dela constam os guias de auditoria que retratam o Ponto de Controle e todas as características de sua validação e avaliação realizadas.

Apresentamos a seguir exemplo de estrutura da mecânica operacional de auditoria do Ponto de Controle, via detalhamento do guia de auditoria.

O conteúdo básico do guia de auditoria é:

- nome do Ponto de Controle;
- número do guia de auditoria;
- número do Ponto de Controle;
- ambiente de auditoria a que pertence o Ponto de Controle;
- código do projeto de auditoria;
- parâmetros do controle interno sob cuja ótica será efetuada a auditoria;
- auditores de sistema que realizarão a validação;
- técnica de auditoria a ser aplicada;
- data de início e término da auditagem do Ponto de Controle;
- tempo de duração da auditoria;
- breve descrição da mecânica de auditoria daquele Ponto de Controle;
- conclusão da auditoria;
- alternativas de solução/recomendações consideradas pertinentes.

O aspecto crucial da auditoria de sistemas é a apresentação do resultado de seus trabalhos à alta administração da organização.

Vários fatores precisam ser atendidos para perfeita comunicação entre a auditoria e a alta administração:

- objetividade na transmissão dos resultados da auditoria;
- esclarecimento dos debates realizados entre a auditoria e os auditados;
- clareza nas recomendações de alternativas de solução;
- explicitação da coerência de atuação de auditoria.

GUIA DE AUDITORIA SISTEMA _____	Nº_____ / _____(ano) SUBSISTEMA _____ ETC.
DESENVOLVIDO POR: _____ _____	EXECUTADO POR: _____ ___/___/___
TEMPO ESTIMADO DE EXECUÇÃO: PRIORIDADE: _____ ____hs.	TEMPO REAL DE EXECUÇÃO: _____ hs.
PONTO DE CONTROLE A SER AUDITADO:	
TÉCNICAS DE AUDITORIA DE SISTEMAS A SEREM UTILIZADAS:	
PROCEDIMENTOS A SEREM SEGUIDOS: (anexar todos os papéis de trabalho utilizados e a utilizar)	

Dois parâmetros devem ser atendidos, prioritariamente, em termos de forma para a adequada apresentação dos resultados da auditoria:

- apresentação do resultado em aproximações sucessivas e do geral para o particular. Assim, a seqüência de explicitação dos relatórios deve ser:
  - certificado de controle interno;
  - relatório de fraquezas de controle interno;
  - relatórios de redução de custos, de análise benefício/custo, de análise do retorno do investimento;

- apresentação do conteúdo de cada documento final segundo uma escala de valores ou consoante um esquema de prioridades:
  - o certificado de controle interno apresenta a situação auditada em *BOA, RAZOÁVEL, MÁ;*
  - os relatórios finais listam, de início, os Pontos de Controle, de fraqueza de maior gravidade, ou de maior redução de custo/retorno de investimento, ou de melhor relação benefício/custo.

Com a repetição da auditoria de um mesmo ambiente computacional podemos passar, no decorrer do tempo, a emitir um relatório comparativo da presente auditoria com as anteriores.

Neste caso, o estabelecimento de um intervalo de conceito/nota mais elástico é interessante.

A auditoria de ambiente de microinformática é outro momento em que a idéia de conceito/nota em um intervalo de maior amplitude é desejável.

Temos dado notas no intervalo de zero a 10 para ambas as situações declaradas nos dois parágrafos anteriores.

Valemo-nos também, aqui, da tecnologia de análise de risco e de esquemas de ponderação análogos aos apresentados no item 2.3. Entretanto, é bom esclarecer que, enquanto, no Capítulo 2, apresentamos esta mecânica em nível de planejamento da auditoria de sistemas, estamos, no momento, trabalhando na intersecção da auditoria de posição com a auditoria de acompanhamento.

A agilidade desta diretriz de atuação da auditoria é tal que podemos auditar à distância um ambiente de microinformática, preestabelecendo Pontos de Controle vários e aplicando, por exemplo, a técnica de auditoria, questionário, cujas respostas dadas pelos auditados, uma vez tabuladas preferencialmente via computador, indicarão o nível de fraqueza de controle interno.

Os Pontos de Controle de maior fraqueza ou segundo a aplicação de uma tabela de números aleatórios serão selecionados para visitas e confirmação, *in loco,* pelos auditores de sistemas às respostas emitidas pelos auditados.

O custo da auditoria do ambiente de micro, a dispersão dos equipamentos, a rápida evolução da microinformática, a necessidade de apoio empresarial a ser dada pela área de computação permitem e impõem o uso de processos de auditagem mais dinâmicos.

A apresentação de resultados pela auditoria precisa ser cada vez mais constante e dirigida, mostrando uma participação efetiva da auditoria junto à mecânica operacional empresarial.

2.5 A FUNÇÃO AUDITOR DE COMPUTADOR

O auditor de computador necessita de conhecimento das áreas de Auditoria, Sistemas de Informações e Processamento Eletrônico de Dados (PED). Dessa forma, a carreira do auditor de sistemas impõe treinamento constante e forte embasamento cultural.

Das três áreas básicas, a de PED é a que tem apresentado maior intensidade de mudanças, de sorte que temos hoje a existência de especializações e de patamares na função de auditor de computador:

- auditores que atuam em sistemas aplicativos em operação, sistemas aplicativos em desenvolvimento e em centro de computação;
- auditores com tecnologia para trabalhar em ambiente de teleprocessamento e banco de dados, na área de microinformática ou com *software* básico.

Obviamente, o auditor de computador necessita conhecer computação e esse conhecimento básico alcança no mínimo o manuseio de uma linguagem de programação, podendo ser BASIC, COBOL, dBASE etc.

Mas, no transcorrer de sua carreira profissional, além da captação de novas tecnologias de computação, terá de se especializar mais em determinadas áreas computacionais do que em outras.

O auditor de sistemas deverá:

1. Ao auditar sistemas em operação, conhecer:
   - documentação de sistemas;
   - fluxogramação;
   - uma linguagem de programação.

2. Ao auditar sistemas em desenvolvimento, conhecer:
   - metodologia de desenvolvimento de sistemas;
   - técnicas de prototização;
   - elaboração de Plano Diretor de Informática.

3. Ao auditar centros de computação, conhecer:
   - apuração de custos em centro de computação;
   - normas administrativo-técnico-operacionais;

- funções e mecânica operacional da área de computação;
- contratos de *software* e de *hardware*.

O auditor de computador atua na área de informática, mas, à medida do avanço do microcomputador, acentua-se sua atuação em todas as áreas da organização.

A função do auditor de sistemas é buscar a otimização do emprego dos recursos de PED e a melhoria das atividades empresariais com a aplicação desses recursos.

O auditor de sistemas desempenha o papel de assessoria da alta administração e até do conselho de administração.

RESUMO

A conceituação principal de auditoria em computador contempla as idéias de:

- sistema de informações;
- controle interno;
- ponto de controle;
- identificação do ponto de controle em um diagrama de fluxo de dados;
- processos e resultados operacionais e de controle;
- ponto de auditoria;
- auditoria de posição e de resultado;
- *Walkthrough/walktruth/audit trail;*
- pré-controle/controle corrente/pós-controle;
- análise de risco;
- tratamento estatístico para análise de risco;
- relatório de fraquezas de controle interno;
- certificado de controle interno;
- relatório de redução de custos;
- manual de auditoria;
- pasta permanente;
- pasta de acompanhamento;
- pasta-mestre;
- guia de auditoria;
- degraus e tecnologia da função auditor de sistemas.

Este capítulo apresenta a filosofia e as diretrizes da auditoria de sistemas; tem também uma série de exemplos tanto dos controles existentes em sistemas de PED, quanto das formas de atuação do auditor.

A tecnologia apresentada responde a questões do tipo:

- o que faz a auditoria de sistemas;
- por que a auditoria de sistemas atua desta ou daquela forma;
- o que busca a auditoria de sistemas;
- como a auditoria de sistemas justifica seus trabalhos e sua existência como função nobre no ambiente empresarial.

A apresentação é feita em termos de planejamento e controle da auditoria de sistemas, preparando o espírito do leitor para a execução da auditoria de sistemas – como fazer – que será objeto do Capítulo 3, Técnicas de auditoria de computador.

QUESTÕES

1. Discorra sobre cada uma das três áreas básicas de conhecimento que formam a auditoria em computador.
2. Defina sistema de informações. Discorra sobre cada um de seus elementos componentes.
3. Por que existe a área de auditoria de sistemas?
4. Explique e dê exemplos a cada um dos conceitos: processo, resultado, rotina de controle, rotina operacional, informação de controle, informação operacional.
5. Discorra sobre cada parâmetro que compõe a definição de controle interno.
6. Discuta e exemplifique cada um dos conceitos: arquivo de informações de controle; arquivo de erros pendentes; arquivos estatísticos para monitoração das informações operacionais.
7. Explique a idéia de *walkthrough, walktruth* e *audit trail*.
8. Como caracterizar a independência do auditor de sistemas?
9. O que é Ponto de Controle?
10. Discuta a composição do Ponto de Controle.

11. Como auditar um Ponto de Controle?
12. O que é auditoria de posição e auditoria de acompanhamento?
13. Discuta e exemplifique pré-controle; controle corrente; pós-controle.
14. Discorra sobre o ciclo de vida/ponto de controle/ponto de auditoria.
15. O que é análise de risco?
16. Como fazer o planejamento da auditoria de sistemas?
17. Como caracterizar um ambiente de computação?
18. Qual a necessidade e o que devem contemplar as estatísticas dos Pontos de Controle de auditorias de sistemas já realizadas?
19. Cite três matrizes para análise de sensibilidade de Ponto de Controle. Apresente exemplos.
20. Descreva a mecânica de análise de risco para efeito de auditoria de Pontos de Controle.
21. Discuta a Figura 2.2. – Trilha de Auditoria: o Arquivo de Informações de Controle (AIC) de um sistema computadorizado clássico.
22. Por que cada auditoria de computador deve ser considerada como um projeto?
23. Quais as pastas que compõem os papéis de trabalho de um projeto de auditoria de sistemas? Discorra sobre cada uma.
24. O que é o guia de auditoria? Qual o seu conteúdo?
25. Quais os produtos gerados ao término de uma auditoria de sistemas?
26. Como é feito o controle de cada projeto de auditoria de sistemas?
27. Discuta a problemática de apresentação dos resultados da auditoria de sistemas à alta administração.
28. Por que o auditor de computador tem de se especializar em áreas de auditoria de sistemas? Cite algumas dessas áreas.

3

Técnicas de Auditoria de Computador

Para execução de trabalhos, na fase de validação dos Pontos de Controle, há necessidade de conhecimento da tecnologia de computação e da forma como aplicar essa tecnologia para a verificação do sistema/ambiente computacional, segundo o conceito de controle interno.

Ora, as técnicas de computação são aplicadas tanto a nível de análise de sistemas quanto de programação, ou seja, o leque de tecnologia necessária ao auditor de sistemas é amplo.

Para facilidade de abordagem das técnicas de auditoria de computador, vamos seguir a estrutura apresentada na Figura 3.1.

Realmente, as técnicas poderão ser utilizadas em mais de um momento estruturado na Figura 3.1; entretanto, a tecnologia do auditor de sistemas, forçosamente, terá de ser diferenciada.

Apresenta-se a seguir uma relação de técnicas passíveis de aplicação pelo auditor de sistemas que deverá levar em consideração:

a) parâmetro do controle interno a ser atendido;
b) momento da aplicação da técnica;
c) ambiente tecnológico de computação vivenciado;
d) situação dinâmica (processos) ou estática (resultados) do sistema/ambiente computacional.

A apresentação das técnicas mostra não somente sua lógica/objetivo de aplicação, como também as características de seu conteúdo a cada momento da aplicação/tecnologia de computação.

1. Programa de computador.
2. Questionários.
3. Simulação de dados *(test-deck)*.
4. Visita *in loco*.
5. Mapeamento estatístico *(mapping)*.
6. Rastreamento-programas *(tracing)*.
7. Entrevista.
8. Análise de relatórios/telas.
9. Simulação paralela.
10. Análise *log/accounting*.
11. Análise do programa-fonte.
12. Exibição parcial da memória *snap shot*.

	PROCESSOS			RESULTADOS		
TECNOLOGIA DE COMPUTAÇÃO / MOMENTOS APLICAÇÃO	BATCH	TP DB	MICRO	BATCH	TP DB	MICRO
AUDITORIA DE SISTEMA EM OPERAÇÃO						
AUDITORIA DE SISTEMA EM DESENVOLVIMENTO						
AUDITORIA DE CENTRO DE COMPUTAÇÃO						

Figura 3.1. *Momentos de aplicação/tecnologia de computação.*

3.1 PROGRAMA DE COMPUTADOR PARA AUDITORIA

3.1.1 Introdução

O programa de computador para auditoria correlaciona arquivos, tabula e analisa o conteúdo dos mesmos. É usado em arquivos seqüenciais, indexado

seqüenciais, banco de dados, tanto em computadores de grande porte, quanto em microcomputadores. Pode ser construído pelo auditor via conhecimento de uma linguagem de programação. A utilização de programas utilitários e a aquisição de pacotes prontos, comercializados no mercado, também são opções para aplicação da técnica.

Algumas opções para aplicação do programa de computador para auditoria são:

a) Tabulação de campos

- somatório de datas de vencimento de títulos gerando um *hash-total* que deverá ser confrontado com o campo correspondente gravado no registro *trailler*, ou monitorado fora do sistema aplicativo pelo auditor;
- somatório de campos de valores quantitativos para efeito de confrontação ou acompanhamento de acumuladores análogos.

b) Contagem de campos/registros

- apuração de totais por tipo de registro ou campo.

c) Análise conteúdo campos/registros

- verificação da existência de campos ou registros em um arquivo;
- correlação entre campos de um mesmo arquivo para verificação da coerência e validade desses campos;
- cruzamento horizontal entre campos em um registro com vistas à integridade do registro.

d) Correlação de arquivos

- confronto de campos entre registros com vistas à garantia de ambos os arquivos.

e) Estatísticas dos campos dos arquivos

- apuração de média; desvio-padrão etc. em um universo de registros/campos de um arquivo para efetuarmos análises do comportamento desse universo.

A tendência no uso dessa técnica é aplicá-la no microcomputador existente na auditoria interna, mas tal prática implica a discussão de algumas atividades, como:

a) Situação do micro da auditoria interna:

- independente;
- rede de micros;
- conexão micro-mainframe.

b) Existência de arquivos no micro com capacidade de armazenamento para receber os arquivos cuja análise é necessária.

c) Possibilidade de o *software* de conexão do micro da auditoria com a rede de micro ou o mainframe efetuar a transferência de dados entre arquivos.

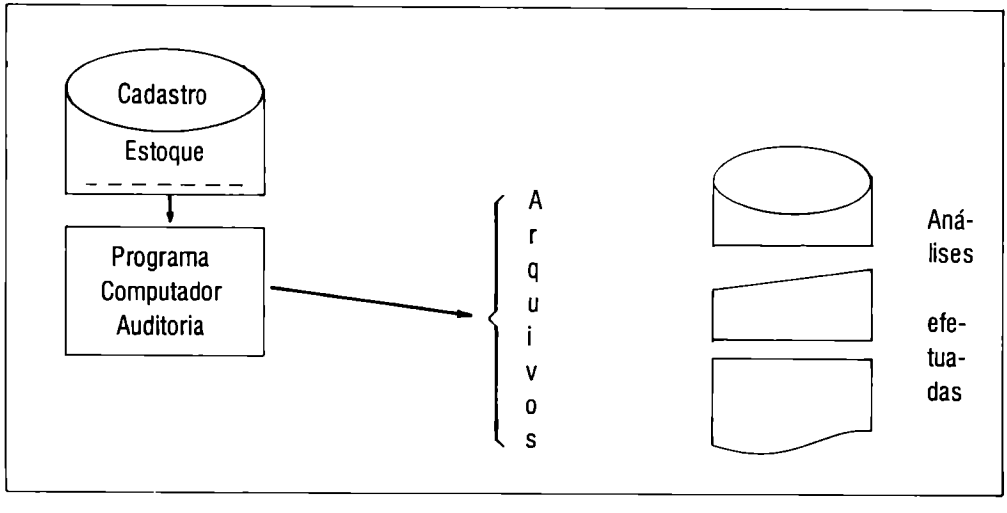
d) Tecnologia do auditor de sistemas no manuseio do micro com *software* adquirido ou desenvolvido internamente na auditoria.

O uso do micro na auditoria interna proporciona maior flexibilidade e independência ao auditor de sistemas, permitindo análises mais específicas no conteúdo dos arquivos.

3.1.2 Operacionalização

A estrutura a seguir especifica as características de uso de programa de computador para auditoria.

I – *Na modalidade análise/tabulação de arquivo*



1. A saída com as análises pode ser impressa via vídeo ou gravada em outro arquivo magnético.

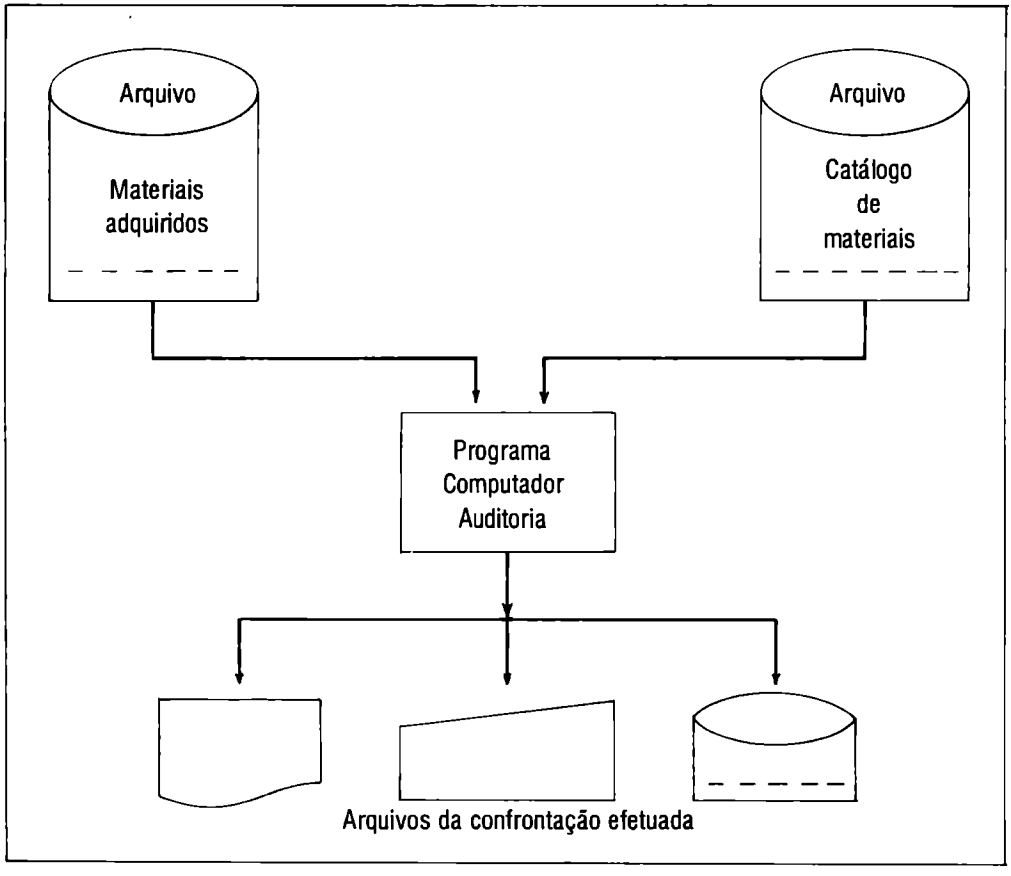
2. O conteúdo dos registros do Cadastro Estoque pode ser:

   - código item em estoque;
   - código localização física do item;
   - nome do item;
   - valor unitário do item;
   - quantidade em estoque;
   - valor total do item em estoque;
   - data da última movimentação;
   - ponto de ressuprimento.

3. As análises a serem feitas pelo programa de computador para auditoria podem ser:

   - verificar se cada campo de cada registro está preenchido; caso contrário, listar, exibir o campo no vídeo ou gravar no arquivo de saída;
   - listar código do item e código da localização física dos itens para efeito de verificação física segundo os critérios:
     - não movimentado há mais de um ano;
     - quantidade em estoque menor que ponto de ressuprimento;
     - quantidade em estoque zero ou negativa;
     - valor total do item em estoque duas vezes maior que o valor médio de item em estoque;
   - enquadramento do item segundo tabela de números aleatórios;
   - somar data da última movimentação de cada item em estoque e verificar se o total cruza com o total correspondente gravado no registro *trailler;*
   - multiplicar, a cada registro de item, o campo quantidade em estoque pelo campo valor unitário do item e verificar se é igual ao campo valor total do item em estoque.

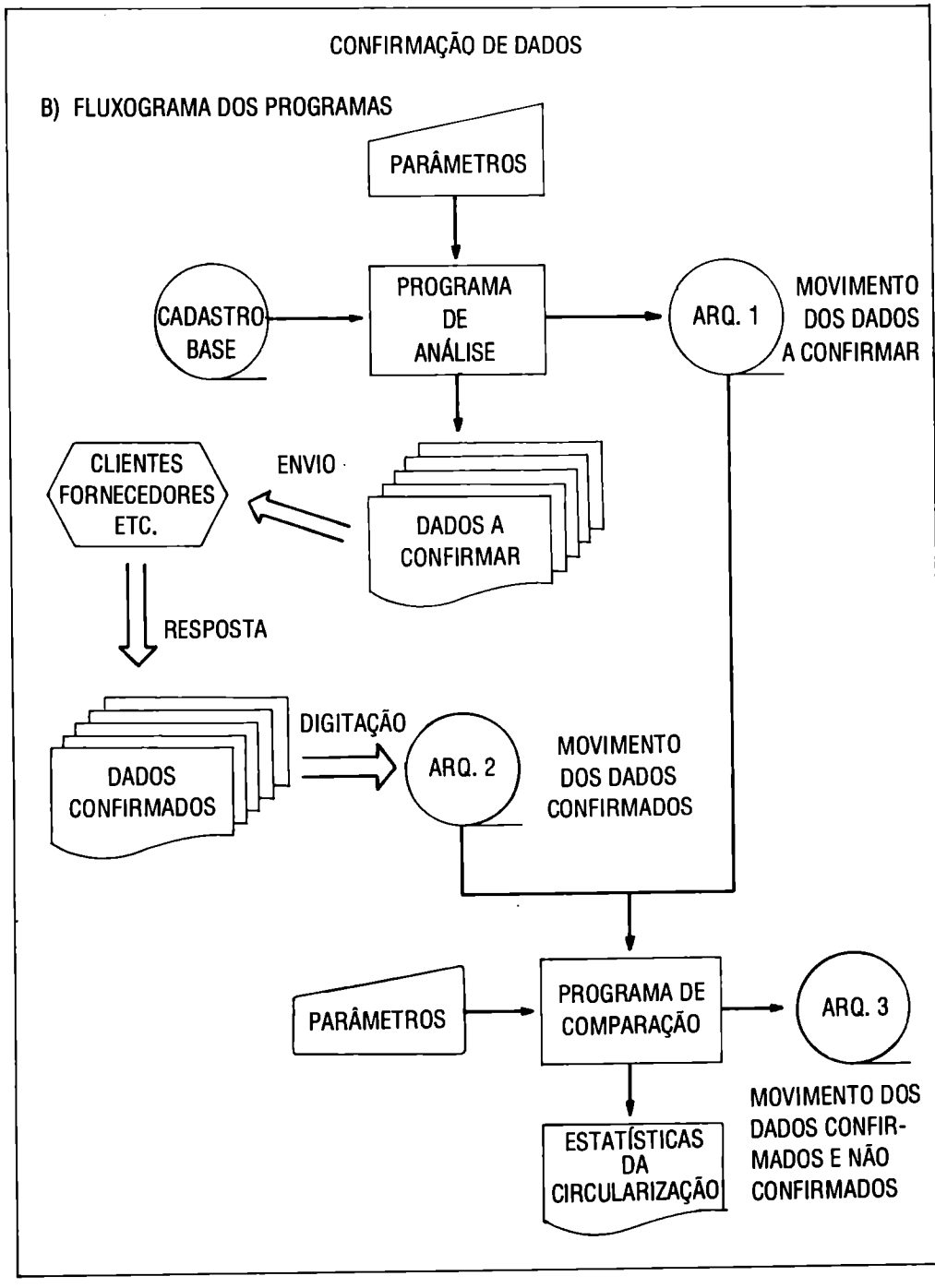
II – *Na modalidade confrontação de arquivos*



1. As análises obtidas desse programa de auditoria de confrontação de arquivos correspondem a:

   - obtenção dos registros que estão no arquivo A e não estão em B; aqueles registros que existem em ambos os arquivos e os registros que estão em B, mas não se encontram no arquivo A;
   - como exemplo podemos ter:
     - materiais adquiridos que não se encontram catalogados;
     - materiais adquiridos, que se acham catalogados, cujo conteúdo dos campos deve ser confrontado, tais como:
       a) valor de aquisição;
       b) características técnicas ou especificações do material;
     - materiais catalogados não adquiridos há determinado período de tempo.

III – *Na modalidade circularização de dados*



1. Esta mecânica de aplicação é uma combinação do uso dos dois programas de computador para auditoria, anteriormente citados, os quais são utilizados segundo a seguinte seqüência:

   - o programa análise de arquivos extrai do cadastro-base clientes, fornecedores etc. uma amostra de dados – segundo uma lei de formação definida –, gerando o *arquivo de movimento dos dados a confirmar* e a *listagem de dados a confirmar;*
   - a amostra de dados contida na listagem de dados a confirmar é encaminhada aos responsáveis por esses dados (clientes, fornecedores etc.) para confirmação dos dados apresentados;
   - as confirmações dos dados, retomadas por seus responsáveis, são digitadas formando o *arquivo de movimento dos dados confirmados;*
   - o programa de confrontação de arquivos cruza o *arquivo de movimento dos dados a confirmar* com o *arquivo movimento dos dados confirmados* obtendo os registros iguais ou desiguais e respectivas análises estatísticas da circularização realizada.

3.1.3 Preparação do ambiente do teste

A identificação do arquivo correto a ser validado é o primeiro passo para realizarmos a aplicação do programa de computador para auditoria, uma vez que, como auditores, temos o objetivo de validar os dados efetivamente processados pelo sistema computadorizado sob auditoria.

Dessa forma, vários procedimentos do teste de auditoria deverão ser executados:

a) Análise do fluxo do sistema para identificação do momento no processo sistêmico em que teremos o conteúdo do arquivo desejado.

b) Entrevista com o analista de sistemas ou com o usuário para confirmação do ponto exato no fluxo em que se têm os dados a analisar.

c) Identificação do código do arquivo e de seu *layout* pela análise da documentação do sistema disponível, ou pela análise do programa do sistema que trabalha o referido arquivo, ou pela análise do *book* de arquivos existentes no centro de computação.

d) Elaboração do(s) programa(s) de computador para auditoria em uma linguagem de programação (COBOL, BASIC, dBASE etc.) ou preparação de parâmetros para uso de programas utilitários ou de *softwares* de auditoria.

e) Análise do LOG/ACCOUNTING de utilização do computador para determinação do ciclo de operação/utilização do arquivo. Solicitação à área de produção do centro de computação, via ordem de produção, para realização de cópia do(s) arquivo(s) de dados a serem auditados. Normalmente, a operação do computador é acionada via ordem de serviço ou ordem de produção e o auditor deverá estar enquadrado na mecânica operacional da área computacional. A ordem de produção feita pelo auditor poderá ser entregue, previamente, à área de produção, ou, caso o fator surpresa seja primordial, o auditor deverá monitorar o cronograma de execução da produção (normalmente elaborado pela área de planejamento e controle da produção do centro de computação) e a respectiva Ordem de Produção para execução do programa que gere o(s) arquivo(s) a ser(em) trabalhado(s) pela auditoria. No momento em que o(s) arquivo(s) for(em) salvo(s) deverá(ão) ser transmitido(s)/levado(s) para ser(em) gravado(s) no disco WINCHESTER do microcomputador da auditoria interna.

f) Aplicação do programa de computador para auditoria sobre o(s) arquivo(s) no ambiente do micro da auditoria interna. Caso a auditoria do arquivo seja feita no computador de grande porte, o auditor deverá preparar comandos de JCL (linguagem de operação do computador) para chamada do programa do auditor da biblioteca de programas e, conseqüentemente, trabalho em cima do arquivo de dados sob auditoria. O auditor deverá também preparar uma Ordem de Produção para a execução de seu programa de auditoria. Dois aspectos devem ainda ser considerados:

- o auditor, ao elaborar seu programa de computador para auditoria, deverá catalogá-lo na biblioteca de programas;
- para ter certeza de que seu arquivo de dados sob auditoria não sofreu modificações entre o dia de sua geração e o dia de seu processamento pelo programa de auditoria, poderá o auditor analisar o arquivo LOG/ACCOUNTING.

g) Análise dos resultados da auditoria do arquivo efetuada, via leitura dos relatórios obtidos ou acesso via terminal ao arquivo com os resultados da auditoria.

h) Emissão de opinião com a elaboração do Relatório de Auditoria, acerca das fraquezas identificadas.

i) Documentação de todo o processo de auditagem com a elaboração de pastas de auditoria consolidando os papéis de trabalho.

A Figura 3.2 detalha a mecânica "preparação do ambiente de teste".

É importante destacar que a técnica programa de computador para auditoria valida resultados computacionais integralmente e valida, parcialmente, processos computacionais, já que não encontrar fraquezas nos dados dos arquivos não significa que os processos computacionais que geravam esses dados estão totalmente corretos, mas apenas que no processamento que gerou os dados sob auditoria não ocorreram situações de erros.

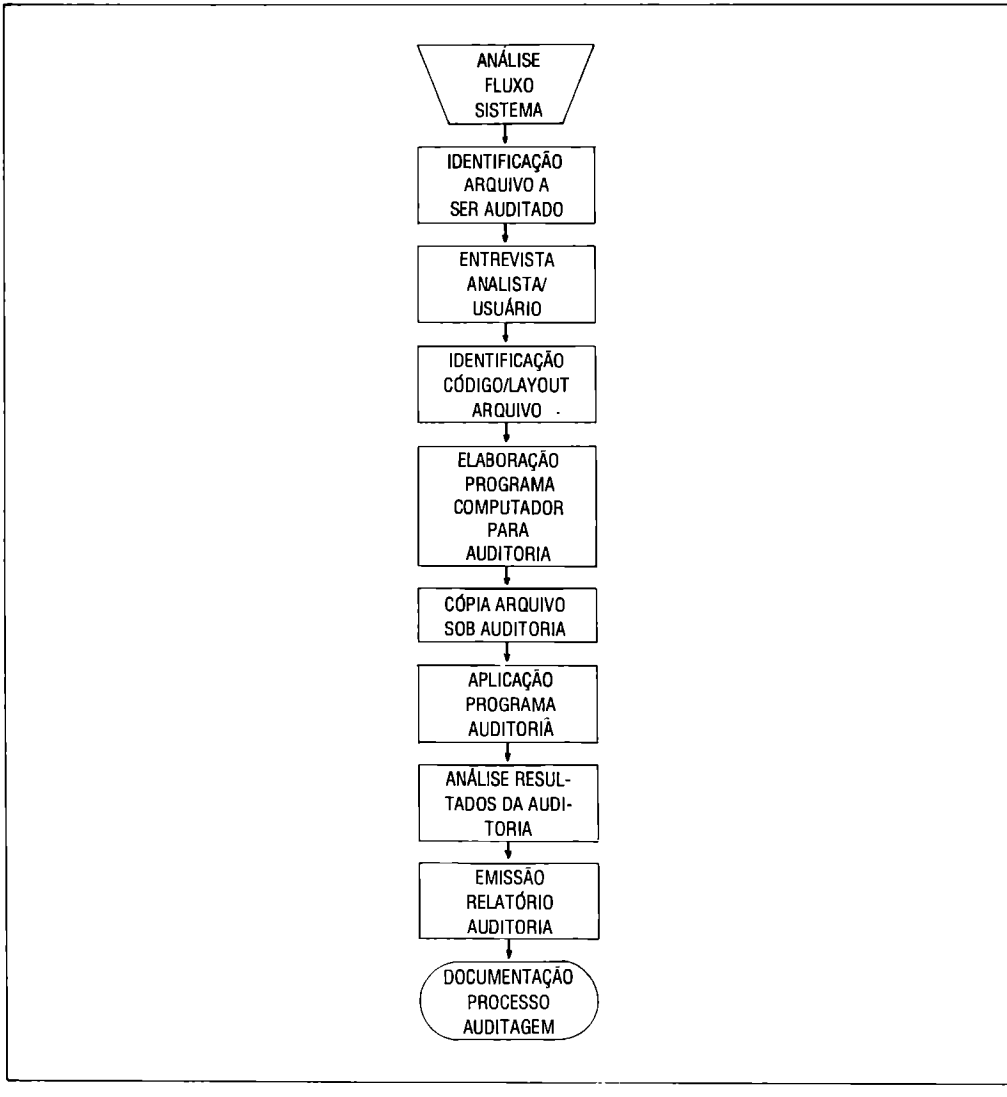


Figura 3.2. *Diagrama lógico de aplicação de programa de computador para auditoria.*

Quadro 3.1. *Matriz para elaboração de questionários.*

AMBIENTE P.E.D. / PARÂMETRO CONTROLE INTERNO	MICRO		SISTEMAS APLICATIVOS						CENTRO COMPUTAÇÃO			REDES DE COMPUTAÇÃO			BANCO DE DADOS	
			EM OPERAÇÃO			DESENVOLVIMENTO						ESTAÇÃO		CANAL DE COMUNICAÇÃO		
	PROCESSOS	RESULTADOS	ENTRADA	PROCESSAMENTO	SAÍDA	ETAPAS	TÉCNICAS	FORMULÁRIOS	INFRA-ESTRUTURA	PESSOAL	CONTRATOS	EMISSORA	RECEPTORA		ADMINISTRAÇÃO DADOS	SOFTWARE GERENCIAMENTO
SEGURANÇA FÍSICA																
SEGURANÇA LÓGICA																
CONFIDENCIALIDADE																
SEGURANÇA AMBIENTAL																
OBEDIÊNCIA À LEGISLAÇÃO																
OBEDIÊNCIA ÀS DIRETRIZES EMPRESARIAIS																
EFICÁCIA																
EFICIÊNCIA																
PRODUTIVIDADE																

Como pudemos ver, a técnica tem por objetivo básico a análise de um universo e a seleção de registros segundo determinados critérios. Duas abordagens muito comuns em auditoria interna podem ser intensamente ativadas com o computador:

a) *Aging* – seleção de dados por idade:

- ocorre por data de vencimento de títulos, por estratificação, no tempo, do universo, em termos passados ou futuros.

b) *Indexação* – seleção de dados segundo uma fórmula arbitrada com o estabelecimento de uma *base*, um *índice* e uma *regra* de combinação do índice na base, gerando uma *nova base*, e assim sucessivamente. Em função de cada base alcançada é extraída uma amostra do universo que se quer analisar.

- se quero em um universo de mil títulos analisar somente cem títulos, posso arbitrar a base cinco e o índice dez e selecionar os títulos 5, 15, 25, 35 . . . . . ., 975, 985, 995.

Naturalmente, a aplicação do programa de computador para auditoria irá impor ao auditor a necessidade do estabelecimento de regras que busquem o alcance dos objetivos da auditoria proposta.

3.2 QUESTIONÁRIOS PARA AUDITORIA EM COMPUTADOR

Corresponde à elaboração de um conjunto de perguntas com o objetivo de verificação de determinado ponto de controle do ambiente computacional.

Essas questões buscam verificar a adequacidade do ponto de controle aos parâmetros do controle interno (segurança lógica, segurança física, obediência à legislação, eficácia, eficiência etc.).

Dois aspectos são críticos na aplicação da técnica questionário:

- características do ponto de controle;
- momento histórico empresarial ou objetivos da verificação do ponto de controle.

Os objetivos de verificação do ponto de controle vão determinar a ênfase a ser dada ao parâmetro do controle interno.

As características do ponto de controle têm agregada a natureza da tecnologia computacional e o correspondente perfil técnico do auditor que irá aplicar o questionário.

Dessa forma, podemos ter questionários voltados para pontos de controle cujas perguntas guardarão características intrínsecas referentes a:

a) Segurança em redes de computadores
   - segurança física dos equipamentos computacionais;
   - segurança lógica e confidencialidade do *software*/informações que trafegam nos canais de comunicação.

b) Segurança do centro de computação
   - controle de acesso físico e lógico às instalações de processamento de dados;
   - segurança ambiental no tocante à infra-estrutura de combate a incêndio, para enfrentar inundação, contra atentados e sabotagem, em situações de greve etc.

c) Eficiência no uso dos recursos computacionais
   - tempo médio de resposta em terminal;
   - tempo de uso dos equipamentos a cada dia;
   - quantidade de rotinas catalogadas existentes.

d) Eficácia de sistemas aplicativos
   - quantidade de informações geradas pelo computador e consumidas pelos usuários;
   - prazo de atendimento de novos sistemas, aos usuários;
   - tempo médio de solução dos problemas dos usuários da rede de computação, provida pelo *help-desk*.

Os pontos de controle podem ser mapeados em momentos específicos da aplicação da tecnologia computacional; o Quadro 3.1 abre um leque amplo para a confecção de questões.

A técnica questionário é, normalmente, aplicada de forma casada a outras técnicas de auditoria como Entrevistas, Visita *in loco* etc. Entretanto, o questionário pode ser aplicado à distância, ou seja, pode ser enviado ao auditado, respondido e analisado pelo auditor centralizadamente.

Esta abordagem permite ao auditor varrer um amplo universo de auditados. Particularmente, em ambiente de microinformática, devido à quantidade, à intensidade de dispersão dos equipamentos e à quantidade de usuários por

equipamento a aplicação de questionários à distância permite uma auditagem constante com menor número de auditores.

Esta auditoria básica via aplicação de questionários à distância possibilita o diagnóstico de pontos relevantes que possam ser auditados em maior nível de detalhamento em momento posterior no processo de auditagem.

Um inconveniente da abordagem aplicação de questionários a distância é a possibilidade de interpretações subjetivas tanto para questões quanto para respostas.

A seqüência básica de aplicação de questionários à distância é:

- analisar o ponto de controle e elaborar o questionário;
- selecionar os profissionais auditados que deverão responder ao questionário;
- elaborar um conjunto de instruções de como responder às questões;
- distribuir/remeter o questionário para os profissionais selecionados;
- controlar o recebimento dos questionários respondidos;
- analisar as respostas às questões;
- formar uma opinião do ponto de controle auditado em decorrência das respostas obtidas;
- elaborar relatório de auditoria.

O conhecimento da tecnologia computacional do ambiente auditado é fundamental para o sucesso da aplicação do questionário à distância. A correlação entre as respostas alcançadas de diversos profissionais auditados é uma das principais mecânicas de análise do ponto de controle neste procedimento de auditoria.

Outro fator para o sucesso dessa forma de aplicação do questionário é a elaboração de perguntas que imponham respostas conclusivas e, de preferência, quantificáveis.

Não se deve fazer perguntas do tipo "o que é feito no momento A ou B?" ou, então, "como é feita a tarefa A ou B?", mas para perguntas do tipo "você exerce a função A ou B?", a resposta tem de ser "sim" ou "não" ou, ainda, "quantas horas você gasta nas tarefas A, ou B, ou C?"

A quantificação das respostas é básica porque permite o estabelecimento de índices e indicadores que podem ser apurados em diversos momentos, constituindo-se séries históricas passíveis de tratamento matemático.

O maior problema na aplicação de questionários à distância está no trabalho administrativo de entrega do questionário e recebimento das respostas dos

auditados. Entretanto, esta barreira está sendo ultrapassada à medida que a rede local e em teleprocessamento (TP) de computação se torna mais distribuída, em que a tecnologia de automação de escritórios evolui e, conseqüentemente, as práticas de correio eletrônico são incorporadas à empresa.

Os questionários podem ser remetidos e as respostas captadas via canal de comunicação, colocando o auditor com atuação interativa com os auditados e permitindo agilidade e rapidez na aplicação da técnica.

Outro fator importante desta mecânica interativa de auditagem via rede é a possibilidade do estabelecimento de um corte *(cut-off)* na aplicação do questionário; via agenda eletrônica, uma negociação interativa pode ser realizada entre auditor e auditado, estabelecendo-se o último dia de um mês para a realização e obtenção das respostas, por exemplo.

Esta providência possibilita adequada programação de trabalhos de auditor e auditados, economizando tempo de ambas as partes e garantindo maior homogeneidade nas respostas pela eliminação do fator diferenciado tempo.

A aplicação do programa de computador para auditoria no ambiente de microcomputador da auditoria interna proporciona independência, maior intensidade e flexibilidade ao processo de auditagem. A participação do micro da auditoria interna na rede permite acesso instantâneo do auditor às bases de dados e às tarefas operacionais dos auditados no ambiente de computador de grande porte, flexibilizando a mecânica de auditoria.

3.3 SIMULAÇÃO DE DADOS PARA AUDITORIA EM COMPUTADOR (TEST-DECK)

É a técnica por excelência aplicada para teste de processos computacionais. Corresponde à elaboração de um conjunto de dados de teste a ser submetido ao programa de computador ou a determinada rotina que o compõe, que necessita ser verificada em sua lógica de processamento.

Evidentemente, uma vez comprovada a inadequação da lógica do processo auditado, podemos concluir 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:

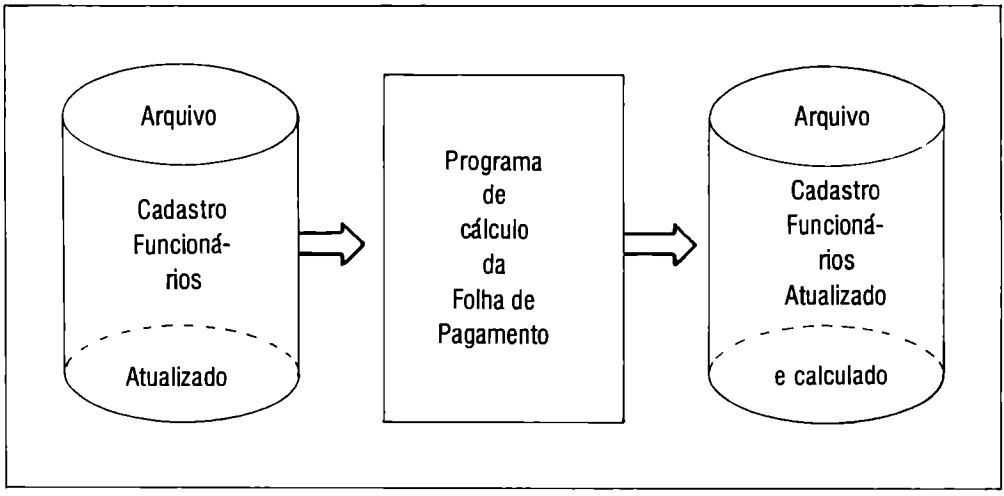
- transações com campos inválidos;
- transações com valores ou quantidades nos limites de tabelas de cálculos;
- transações incompletas;
- transações incompatíveis;
- transações em duplicidade.

A mecânica de aplicação do *test-deck* implica as etapas:

1. Compreensão do módulo do sistema a ser avaliado/identificação de programas e arquivos via:
   - análise da documentação do sistema;
   - levantamento de dados via entrevistas com analistas e usuários para complementação do entendimento da documentação;
   - estudo do diagrama de fluxo de dados (DFD) ou outra representação gráfica da lógica do sistema para determinação da rotina ou rotinas componentes dos programas a serem testados;
   - caso a rotina seja catalogada/padronizada, a simulação de dados será efetuada uma única vez e, se tivermos convicção de seu uso no programa de computador sob auditoria, poderemos dispensar sua validação toda vez que essa mesma rotina aparecer no ambiente sob teste. Um exemplo desta situação é a rotina de cálculo do dígito-verificador de módulo onze.

2. Simulação dos dados de teste pertinentes. Este momento impõe o alcance do parâmetro do controle interno objetivado. Se a obediência à legislação for considerada no caso do programa de cálculo da folha de pagamento, devemos simular dados no Arquivo Cadastro Atualizado que objetivem testes de:
   - tabela de imposto de renda;
   - parâmetros para cálculo do INPS; FGTS; salário-família; desconto do clube etc.

O fluxo do programa de cálculo da folha de pagamento a seguir espelha essa lógica de atuação.



3. Elaboração dos formulários de controle do teste. Apurar resultados esperados e pré-calculados para confrontação com os resultados alcançados no teste e gravados nos arquivo Cadastro de Funcionários, atualizado e calculado.

   Obviamente, o auditor deverá conhecer a lógica do sistema tanto em termos dos procedimentos necessários à operacionalização da área usuária, quanto no tocante às saídas ou opções dadas pelos profissionais de computação a situações irregulares.

4. Transcrição dos dados de teste para um meio aceito pelo computador. Uma opção do auditor de sistemas é copiar partes do arquivo real de entrada no programa e fazer, via programa de computador, as alterações desejadas para alimentação da simulação de dados necessária.

   É importante destacar que o auditor deverá ter bons conhecimentos de computação para atuar com a técnica simulação de dados, particularmente, se for ambiente de banco de dados, ocasião em que o suporte técnico de analistas de *software* básico e de *software* de banco de dados se torna importante para a utilização de programas utilitários, de cópia de segmentos de banco de dados e de acesso e alteração de seu conteúdo.

5. Preparação do ambiente necessário para execução do teste. Criação de comandos de operação do programa de computador sob auditoria. Alimentação dos arquivos de dados simulados, com *labels* e códigos específicos desses arquivos de teste da auditoria.

Preparação da Ordem de Produção, geração de arquivos-tabela, negociação de horário de utilização do computador central (*mainframe*).

6. Processamento dos dados de teste com utilização do programa real que contém as rotinas do sistema sob auditoria a serem validadas.

   Diferentemente dos programas de computador para auditoria que podem trabalhar no microcomputador da auditoria interna, em função da possibilidade de copiarmos os arquivos de dados reais no disco Winchester do micro, no caso da simulação de dados devemos testar o programa sob auditoria na própria UCP e com o mesmo sistema operacional do computador onde é processado, normalmente, esse programa.

7. Avaliação dos resultados do teste via análise das listagens obtidas a partir do arquivo magnético gerado; no nosso caso, arquivo Cadastro de Funcionários, atualizado e calculado.

   Há necessidade de ser feita Ordem de Produção e JCL – *Job Control Language* (comandos de operação) para obtenção dos dados de teste gerados.

8. Emissão de opinião acerca do ponto de controle processo computadorizado (rotina ou programa) com a elaboração da documentação, ou seja, papéis de trabalho referentes à simulação de dados realizada.

A Figura 3.3 estrutura os "procedimentos para aplicação da técnica *test-deck*".

Esta técnica é bastante completa e fundamental, já que o auditor tem por atividade básica a otimização e certificação da qualidade dos processos empresariais. Podemos mesmo dizer que esta técnica é a primeira e aquela insubstituível na segurança que transmite aos trabalhos do auditor.

Entretanto, algumas características revestem a técnica simulação de dados:

a) o auditor necessita conhecer computação em termos de análise de sistemas;

b) a documentação dos sistemas é deficiente, o que implica o auditor precisar atualizar ou complementar a documentação existente, principalmente no tocante a fluxos de informação e de programas. Muitas vezes a documentação existente compreende somente listagens de programa e fluxo ou seqüência de execução de programas na produção;

c) a elaboração do ambiente de testes é complexa, particularmente em programas principais que manipulem grande quantidade de arquivos de entrada, saída e de trabalho.

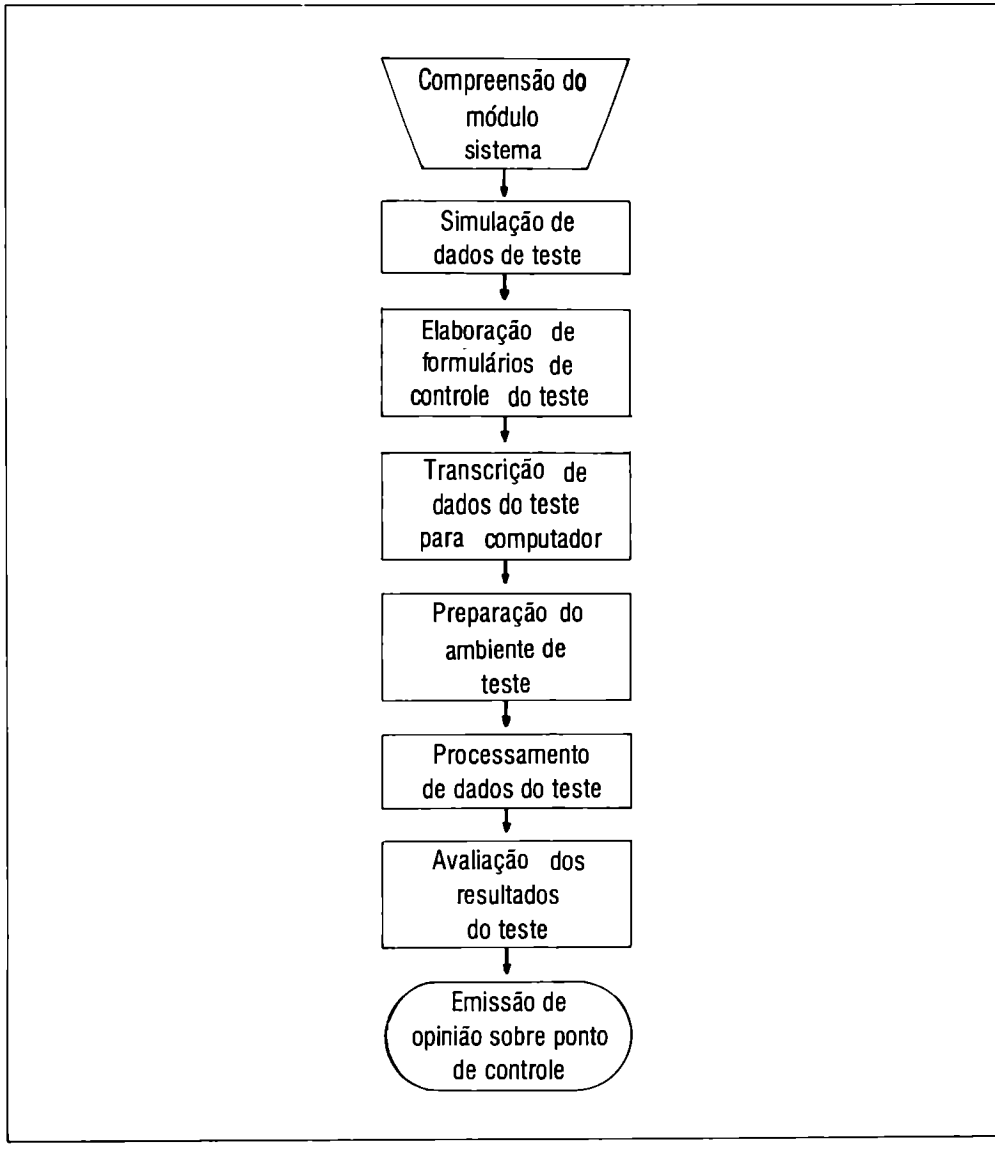


Figura 3.3. *Diagrama lógico de aplicação-simulação de dados.*

3.4 VISITA IN LOCO COMO FERRAMENTA DE AUDITORIA DE COMPUTADOR

Corresponde à atuação pessoal do auditor junto a sistemas, procedimentos e instalações do ambiente computadorizado.

Normalmente, combinada com outras técnicas de auditoria de computador, particularmente questionário, a visita *in loco* implica o cumprimento da seguinte seqüência de procedimentos:

a) marcar data e hora com a pessoa responsável que irá acompanhar as verificações, ou convocá-la no momento da verificação quando o fator surpresa se tornar necessário:

   - a participação do auditado na mecânica, visita *in loco*, normalmente, é importante para o sucesso da aplicação da técnica por serem necessários esclarecimentos quanto a pontos nebulosos que ocorram;

b) anotar procedimentos e acontecimentos, coletar documentos, caracterizar graficamente a situação via elaboração de fluxo de rotinas e de *layout* de instalações.

   - a aplicação do questionário e a cópia das respostas são particularmente importantes, pois permitirão, no trabalho futuro de elaboração do relatório de auditoria, consulta e recuperação fácil de fatos referentes à verificação *in loco* feita;

c) anotar nomes completos das pessoas e data e hora das visitas realizadas;

d) analisar os papéis de trabalho obtidos, avaliar respostas e a situação identificada;

e) emitir opinião via relatório de fraquezas de controle interno.

A presença do auditor é fundamental para a constatação física da existência de ativos computacionais da empresa, bem como seu estado de conservação e qualidade dos procedimentos de utilização.

Esta técnica é aplicada em vários pontos de controle clássicos de auditoria de sistemas, dentre os quais destacamos:

- inventário de volumes de arquivos magnéticos (discos, fitas, disquetes) armazenados nas fitotecas;
- inventário de insumos computacionais armazenados em almoxarifado (fitas de impressora, formulários contínuos etc.);
- visita à sala de operação/utilização de computadores com o objetivo de verificação da problemática de controle de acesso, do uso de Ordens de Produção, do preenchimento de documentação para movimentação de formulários, arquivos magnéticos etc.;

- acompanhamento da rotina de *back-up* de arquivos magnéticos com a constatação do preenchimento correto, no momento adequado da movimentação dos volumes magnéticos entre a fitoteca central e a fitoteca de *back-up;* verificação do uso de equipamentos adequados para o transporte dos volumes magnéticos etc.

3.5 MAPEAMENTO ESTATÍSTICO DOS PROGRAMAS DE COMPUTADOR (MAPPING)

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.

Há necessidade da inclusão de instruções especiais junto aos programas em processamento na produção.

3.6 RASTREAMENTO DOS PROGRAMAS DE COMPUTADOR

Técnica que 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 das instruções segundo sua ordem de execução.

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 conseqüência, 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 *trqcing,* rastrear as instruções que dão tratamento a essas transações específicas.

3.7 ENTREVISTAS NO AMBIENTE COMPUTACIONAL

O método de trabalho corresponde à realização de reunião entre o auditor e os auditados – profissionais usuários e de computação envolvidos com o ambiente ou o sistema de informação computadorizado sob auditoria.

A seqüência de procedimentos corresponde a:

a) analisar o ponto de controle e planejar a reunião com os profissionais envolvidos.

- marcar, antecipadamente, data, hora e local com os auditados, bem como comunicar a natureza do trabalho a ser desenvolvido. Devem-se realizar estas tarefas via carta ou memorando;

b) elaborar um questionário para realização da entrevista.

- as questões devem ser divididas por parâmetro do controle interno, por área ou assunto de processamento eletrônico de dados. Deve, também, ser estimado o tempo de duração da entrevista;

c) realização da reunião, com aplicação do questionário e anotação das respostas e comentários dos entrevistados a cada questão efetuada.

- dependendo do nível de sensibilidade das questões, as reuniões devem ser individuais;
- os níveis hierárquicos das áreas auditadas devem ser respeitados, comunicando-se aos superiores a natureza das entrevistas com os subordinados;

d) elaboração de uma ata de reunião com o registro dos principais pontos discutidos a cada questão apresentada.

- distribuir cópia da ata da reunião para cada participante de entrevista;

e) análise das respostas e formação de opinião acerca do nível de controle interno do ponto de controle;

f) emissão do relatório de fraquezas de controle interno.

A técnica de entrevistas é freqüentemente casada com outras técnicas de auditoria, visita *in loco,* aplicação de questionários, *test-deck* etc.

3.8 ANÁLISE DE RELATÓRIOS/TELAS

Implica a análise de documentos, relatórios e telas do sistema sob auditoria no tocante a:

- nível de utilização pelo usuário;
- esquema de distribuição e número de vias emitido;
- grau de confidencialidade de seu conteúdo;
- forma de utilização e integração entre relatórios/telas/documentos;
- distribuição das informações segundo o *layout,* vigente.

A mecânica de aplicação da técnica implica o cumprimento das etapas:

a) relacionar por usuário todos os relatórios/telas/documentos que pertençam ao ponto de controle a ser analisado.

- poderá ser feita uma classificação desses relatórios para efeito de estabelecimento de prioridades na análise;

b) obtenção de modelo ou cópia de cada relatório/documento/tela para compor a pasta de papéis de trabalho;

c) elaborar um *check-list*/questionário para a realização dos levantamentos acerca dos relatórios/telas/documentos;

d) marcar antecipadamente a data e hora com as pessoas que fornecerão opinião acerca dos relatórios;

e) realizar as entrevistas e anotar as observações e comentários dos usuários;

f) analisar as respostas, formar e emitir opinião acerca do nível de controle interno.

As principais fraquezas identificadas são:

- relatórios/telas/documentos não mais utilizados;
- *layout* inadequado;
- distribuição indevida de vias;
- confidencialidade não estabelecida ou não respeitada.

Esta técnica é primordial para avaliação do parâmetro eficácia do sistema.

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

No tocante a telas, a aplicação da técnica pode ser dificultada, no ambiente de microinformática, pela facilidade que os usuários têm na criação e descarte de telas.

3.9 SIMULAÇÃO PARALELA

Elaboração de um programa de computador para simular as funções de rotina do sistema sob auditoria.

Esta técnica utiliza-se dos dados rotineiros alimentados à rotina do sistema sob auditoria como entrada do programa de computador para auditoria, simulado e elaborado pelo auditor.

Enquanto no *test-deck* simulamos dados e os submetemos ao programa de computador que, normalmente, é processado na produção, na simulação paralela simulamos o programa e submetemos ao mesmo os dados que foram alimentados ao programa em processamento normal.

A estrutura de aplicação desta técnica corresponde a:

a) Levantamento e identificação, via documentação do sistema, da rotina a ser auditada e respectivos arquivos de dados trabalhados.

b) Elaboração de programa de computador com a lógica da rotina a ser auditada. Compilação e teste deste programa que irá simular em paralelo a lógica do programa de computador sob auditoria.

c) Preparação do ambiente de computação para processamento do programa de computador elaborado pelo auditor.

3.10 ANÁLISE DO LOG/ACCOUNTING

O *Log/Accounting* 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/Accounting* permite a verificação da 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/Accounting* foram desenvolvidos para serem usados pelo pessoal de computação. Entretanto, representam, também, excelente ferramenta para a auditoria de sistemas para:

- identificação de ineficiência, no uso do computador;
- apuração do desbalanceamento da configuração do computador, pela caracterização de dispositivos (unidades de disco, fita magnética, impressoras, terminais) que estão com folga ou sobrecarregados;
- determinação de erros de programas ou de operação do computador;
- flagrar uso de programas fraudulentos ou utilização indevida do computador;
- captar tentativas de acesso a arquivos indevidas, ou seja, por senhas/*passwords* não autorizadas.

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

O trabalho da área de computação sobre o *Log/Accounting* deve gerar Indicadores de Qualidade (IQ) do monitoramento do computador, bem como estudos de planejamento de capacidade da configuração/rede de equipamentos,

com a finalidade de obter maior rendimento do parque computacional dentro de um nível de segurança adequado.

O auditor poderá construir um *software* para auditoria de *Log/Accounting*, o qual trabalhará registros de:

a) *Contabilização*

- mostram quais usuários utilizaram quais programas e por quanto tempo;
- incluem identificação do usuário, características do *hardware* necessário para trabalhar o *job* (seqüência de programas) e como o *job* foi completado.

b) *Atividade do data set (arquivos)*

- providenciam informações acerca de quais arquivos de dados foram utilizados durante o processamento e que usuário solicitou o uso do *data set;*
- as informações contidas nestes registros são: nome do *data set*, tamanho do registro, número de série do volume e o usuário do *data set*.

A rotina de *job accounting/log*, portanto, registra a hora de início e término do *job*, o uso dos arquivos *(data sets)* e o uso das facilidades do *hardware* dando elementos para avaliação do uso do *hardware* e do *software* que são:

a) *Elementos para avaliação de hardware*

- tempo de UCP por dia;
- tempo de uso de unidades de entrada e saída;
- quantidade de vezes de utilização de unidades de entrada e saída.

b) *Elementos para avaliação de software*

- tempo de utilização;
- quantidade de vezes de *software* utilizado por usuário;
- quantidade de cancelamento por erro de programa;
- quantidade de cancelamento por erro de unidade de entrada e saída;
- quantidade de cancelamentos efetuados pelo operador;
- quantidade de cancelamentos por estouro baseados em algum parâmetro (tempo/linhas etc.).

Para aplicar esta técnica o auditor deverá adotar esta seqüência de trabalho:

a) Entrevistar o pessoal de *software* básico e do planejamento e controle da produção para entender:

- o sistema de monitoração de uso de *software* e de *hardware* existente;
- o *layout* dos registros gerados no arquivo *log/accounting;*
- as opções possíveis de rotina de *job/accounting;*
- o tempo de retenção do arquivo *log/accounting*.

b) Decidir que tipos de verificação serão efetuados em cima dos dados do arquivo *Log*, que período de tempo será contemplado, quando será efetuado o teste, reservar tempo de computador para a realização do teste, preparar ordem de serviço e comandos de operação do computador para processamento do programa de computador para auditoria do *Log*.

c) Elaborar e aplicar o programa de computador de auditoria do *Log*, ou utilizar a mecânica de análise do *Log* praticada pelos profissionais de computação.

d) Analisar os resultados da tabulação do *Log*.

e) Emitir opinião acerca da qualidade do uso do *hardware* e do *software* em determinado período de tempo.

Uma alternativa para avaliação do *Log* é o estudo da mecânica de análise do *Log* praticada pelos profissionais de computação.

A observação crítica da qualidade dessa análise e a discussão dos dados obtidos, com a aplicação da mecânica do pessoal de computação, em dado intervalo de tempo, e a conseqüente conclusão da adequacidade ou não da utilização de *hardware* e de *software* é a tarefa do auditor de sistemas.

A técnica de auditoria análise do *Log/Accounting* é um poderoso instrumento de auditoria, porém sua aplicação requer grande conhecimento de computação. Uma de suas aplicações é identificar o uso de programas fraudulentos ou não pertencentes à empresa. Neste caso uma série de análises complementares necessitam ser feitas para a constatação da irregularidade, tais como:

- confrontar o código/*label* do programa registrado no *Log* com os códigos dos programas gravados na Biblioteca Fonte ou Objeto, existentes no disco do sistema operacional;

- verificar se não houve compilação ou catalogação de programas entre dois momentos, aqueles de sua execução e utilização.

No ambiente de microcomputadores, muitas vezes o emprego desta técnica é inviável pela inexistência de um *software* que grave o arquivo *Log*.

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, por quanto tempo os registros do *Log* devem ser armazenados para a viabilização da atuação da auditoria em computador.

É importante registrar que existem dois tipos de arquivo *Log:*

a) Aqueles que registram o uso da UCP, dos arquivos magnéticos, da carga e do nível de utilização dos dispositivos computacionais (a técnica discorrida neste tópico foi sobre a tabulação deste tipo *Log*).

b) *Log* de transações, ou seja, um arquivo que registra todos os dados que foram processados/transmitidos. Este tipo de arquivo *Log* é comum em ambiente *on-line* no qual todas as transações processadas ficam registradas em um arquivo magnético - chamado *Log* de Transações – para posterior uso ou análise. Um exemplo deste *Log* de Transações é aquele gravado em um ambiente *real time* que permita a qualquer instante a recuperação do Banco de Dados no caso de uma parada normal do processamento.

3.11 ANÁLISE 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 "rodou" ou irá "rodar". Para tal, ele compara o *label* do programa-fonte gravado na biblioteca-fonte com o *label* do programa-objeto gravado na biblioteca-objeto (onde os programas estão em linguagem de máquina, ou seja, módulo de carga executável).

O auditor pode, ainda, para maior certeza de que verifica as instruções que efetivamente compõem o programa em linguagem de máquinas, executar os seguintes procedimentos:

a) preencher uma Ordem de Serviço determinando à produção que compile o módulo-fonte que se encontra na biblioteca-fonte;

b) executar um programa *(software* específico) que compare o código-objeto gerado em *a*, com o código-objeto do programa que se encontra gravado na biblioteca-objeto da produção;

c) efetuar verificações em eventuais divergências que ocorram em *b*.

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:

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

3.12 SNAPSHOT

Técnica que fornece uma listagem ou gravação do conteúdo das variáveis do programa (acumuladores, chaves, áreas de armazenamento) quando determinado registro está sendo processado. A quantidade de situações a serem extraídas é predeterminada.

Corresponde na realidade a um *dump* parcial da memória, basicamente, das áreas de dados.

À semelhança do *mapping* e do *tracing,* necessita de um *software* especial "rodando" junto com o programa aplicativo, ou que as características *SNAPSHOT* estejam embutidas no sistema operacional.

É uma técnica usada como auxílio à depuração de programas, quando há problemas e realmente exige fortes conhecimentos de PED (processamento eletrônico de dados) por parte do auditor de sistemas.

RESUMO DO CAPÍTULO

As técnicas de auditoria de sistema ora apresentadas são aquelas aplicáveis, principalmente, quando o sistema estiver em operação. Entretanto, sua uti-

lização está condicionada à tecnologia computacional vigente no ambiente sob auditoria. Isto é, terá formas diferentes, cada técnica de auditoria, caso o sistema esteja sendo processado em ambiente *batch* ou *on-line*, ou de microinformática. Inclusive várias dessas técnicas serão, ou não, aplicáveis em função desses mesmos ambientes.

A combinação e a intensidade no uso das técnicas dependerão da cultura de cada departamento de auditoria interna e da natureza e características intrínsecas a cada ponto de controle auditado.

Seria conveniente que os departamentos de auditoria interna conduzissem estatísticas acerca do uso das técnicas de auditoria a cada projeto de auditoria realizado.

QUESTÕES

1. Discuta as características, as vantagens e as desvantagens da aplicação das técnicas de auditoria de computador segundo cada "janela" da matriz "momentos de aplicação *versus* tecnologia de computação" (Figura 3.1).
2. Discorra sobre a mecânica de aplicação da técnica de auditoria em computador "programa de computador para auditoria".
3. Detalhe uma situação hipotética de circularização usando programas de computador para auditoria.
4. Como preparar o ambiente de teste para a aplicação da técnica "programa de computador para auditoria" em arquivo-cadastro?
5. Quais os tipos de teste que podem ser feitos em um arquivo de computador submetido a um programa de computador para auditoria?
6. Quais as características para aplicação de questionários para auditoria de computador?
7. Caracterize pontos de controle em que se podem aplicar questionários de auditoria de computador.
8. Discuta a Figura 3.2-Matriz para elaboração de questionários.
9. Como você analisa a aplicação da técnica questionário de auditoria em computador aplicado a distância, isto é, enviado e respondido pelo auditado sem a participação física do auditor no momento da aplicação do questionário de auditoria?

10. Faça uma análise comparativa da utilização das três técnicas:

    - programa de computador para auditoria;
    - questionários para auditoria;
    - simulação de dados para auditoria de computador *(test-deck)*.

11. Descreva os tipos de teste que você fará com a preparação de um *test-deck*.
12. Descreva a mecânica de aplicação do *test-deck*.
13. Como é aplicada a técnica de auditoria visita *in loco?*
14. Dê um exemplo de ponto de controle com a aplicação da técnica visita *in loco*.
15. Descreva, confronte e explique as três técnicas de auditoria em computador: *mapping, tracing* e *snapshot*.
16. Como se desenrola a aplicação da técnica "entrevistas no ambiente computacional"?
17. Estabeleça um ponto de controle e discorra sobre a aplicação conjugada das técnicas: visita *in loco,* questionários e entrevistas.
18. Como aplicar a técnica de auditoria de computador "análise de relatórios/telas"?
19. O que é a técnica de auditoria de computador "simulação paralela"?
20. Quais os objetivos da auditoria de computador quando for feita a aplicação da técnica "análise do *log/accounting*"?
21. O que é a técnica "análise do programa-fonte"?
22. Que técnicas você usaria para identificar fraudes em um ambiente computacional?

4 Auditoria do Ambiente Computacional

4.1 AUDITORIA DE SISTEMAS COMPUTADORIZADOS EM OPERAÇÃO

O auditor deve seguir uma carreira incorporando ao seu conjunto de conhecimentos, logo no início de seu aprendizado, a tecnologia de auditoria de sistemas computadorizados em operação, para tal, ele deverá apreender técnicas que permitam a sua gradativa atuação no ambiente computadorizado.

Um dos Pontos de Controle (PC) mais auditados é aquele correspondente ao parâmetro do controle interno eficácia – Análise dos Relatórios Emitidos pelo sistema de informação computadorizado.

Este PC pertence, prioritariamente, ao momento de atuação do auditor – auditoria do sistema em operação – já que irá ser verificado o nível de satisfação dos usuários com:

- natureza, correção e qualidade das informações recebidas;
- periodicidade e conseqüente intensidade das informações recebidas;
- forma de apresentação da informação em termos de sintética ou analítica e de distribuição no relatório.

Este PC poderá também ser verificado segundo outros parâmetros do controle interno, tais como:

a) *Confidencialidade*

- verificação do nível de sigilo das informações contidas nos relatórios, distribuição dos mesmos e características para a destruição física desses relatórios.

b) *Segurança física*

- caracterização de relatórios distribuídos rasgados, sujos, faltando vias ou partes etc.

PONTO DE CONTROLE	PARÂMETRO CONTROLE INTERNO	TÉCNICA DE AUDITORIA	CARACTERÍSTICAS DA AUDITORIA
1. Rotina de Atualização	Segurança lógica	Test-deck	• Verificação do correto balanceamento de inclusões, exclusões e alterações do arquivo movimento contra o cadastro anterior, flagrando: – inclusões provenientes do arquivo movimento e já existentes no cadastro anterior e que foram incluídas no cadastro atualizado; – exclusões vindas no arquivo movimento que não encontraram correspondentes no cadastro anterior e não foram apontadas em relatório de erros; – exclusões vindas no arquivo movimento que encontraram registros correspondentes no cadastro anterior, os quais foram mantidos no cadastro atualizado; – alterações vindas no arquivo movimento e que não foram consideradas no arquivo cadastro atualizado.
2. Programa de cálculos	Eficiência	Mapping	• Aplicada durante determinada quantidade de vezes de processamento do Ponto de Controle com o objetivo de determinação de rotinas do programa de cálculos não mais utilizadas, com a conseqüente análise para sua eliminação.
	Segurança lógica	Test-deck	• Submissão de dados referentes a situações específicas: – cálculo do imposto de renda do programador que fez o programa, ou do responsável pela área de pessoal; – cálculo de vantagens e descontos da alta administração.
3. Cadastro clientes	Segurança lógica	Programa de computador para auditoria	• Somatório do produto data vencimento do título versus código do cliente criando um hash total que deverá ser calculado a cada nova atualização do cadastro para evitar retirada indevida de títulos de cliente do cadastro ou modificação de data de vencimento de título.
	Eficácia	Programa de computador para auditoria	• Estratificação via parâmetro valor, ou, aging, com a emissão de informações acerca do conteúdo do cadastro.

4. Rotina de back-up de arquivos	Segurança física	Questionário	• Perguntas para constatar: – quantidade de volumes magnéticos exigidos para cópia dos arquivos magnéticos; – características do invólucro para transporte de armazenamento dos arquivos magnéticos. • Identificação e verificação dos formulários de controle para tramitação e arquivamento dos arquivos magnéticos, ou alternativamente, utilização de software para monitoração, nas situações de: – guarda de arquivo magnético na fitoteca central; – utilização de arquivo magnético na operação do computador; – tramitação de arquivo magnético da: I – fitoteca central para a sala de operação do computador; II – fitoteca central para o cofre ou a fitoteca de back-up; III – fitoteca central para fitotecas de centros regionais; IV – fitoteca central para ambiente externo da empresa; – guarda de arquivo magnético no cofre ou fitoteca de back-up.
5. Documentação do sistema	Segurança lógica	– Questionário – Entrevista	• Identificação da equipe de manutenção do sistema. • Aplicação de perguntas que visem verificar: a) natureza da documentação do sistema: – automatizada ou manualizada; – tipos de informação existentes; b) estrutura da documentação: – manual de análise; – manual do usuário; – manual de operação; – manual de programa; c) nível de back-up da documentação; d) estrutura de manutenção do sistema; e) esquema de revisão da documentação.

Figura 4.1. *Matriz PC-ON.*

Outro Ponto de Controle, normalmente, validado nos sistemas em operação é *Análise de Cadastro,* o qual poderá ser verificado sob a ótica de:

a) *Segurança física*

- verificação dos cuidados com transporte, armazenagem e manuseio dos dispositivos (fita magnética, disquete) que possuem as informações componentes do cadastro;
- os cuidados podem ser identificados como:
  - contra calor, poeira, magnetismo, quedas, empenamento etc.
  - em função de sabotagem, displicência, falta de treinamento etc.

b) *Segurança lógica*

- existência de campos de controle, tais como:
  - somatório de campos de valor;
  - *password;*
  - data de gravação e de expiração de arquivo;
  - *hash total* – somatório de data de vencimento de títulos, por exemplo;
  - quantidade de registros existentes no arquivo.

c) *Eficiência*

- forma de organização do arquivo;
- campos ou registros não mais utilizados e existentes no arquivo.

Estes pontos de controle são classificados como PC-ON (Pontos de Controle do momento Operação Normal), ou seja, sua validação é de interesse quando da utilização rotineira do sistema de informação computadorizado.

A Figura 4.1 apresenta uma seqüência de situações de auditoria dos sistemas de informações computadorizados segundo a estrutura de:

- nome do Ponto de Controle;
- parâmetro do Controle Interno;
- características da auditoria;
- técnica de auditoria a ser aplicada.

Evidentemente, cada ponto de controle pode ser auditado segundo mais de uma ótica (parâmetro do controle interno) e ambiente (rotinas, dados), implicando a utilização de técnicas de auditoria em computador diferenciadas.

Para a determinação do Ponto de Controle (PC), o auditor deverá entender o ambiente/sistema sob auditoria e para tal precisará estar de posse ou construir uma documentação do sistema.

A principal forma de representação do sistema é gráfica via a elaboração de um fluxograma.

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 conseqüência, representa as informações geradas/usadas por esses mesmos processos;
- permite a representação gráfica até o nível de detalhamento que o auditor de sistemas considere suficiente para o entendimento do sistema e a determinação dos PC's; por conseguinte, por não exigirem a representação detalhada de todos os processos e resultados, economizam tempo ao trabalho de auditagem.

Como conseqüência, o DFD é representado em níveis à medida que explosões de processos são efetuadas, com o detalhamento a um nível mais analítico da mecânica de funcionamento do sistema.

A simbologia básica do DFD está representada na Figura 4.2.

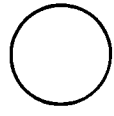
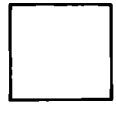
SÍMBOLO	DESCRIÇÃO
	– PROCESSO
	– FLUXO DE DADOS
	– ARQUIVOS
	– ÁREAS EXTERNAS AO SISTEMA – OUTROS SISTEMAS

Figura 4.2. *Simbologia DFD – Diagrama de Fluxo de Dados.*

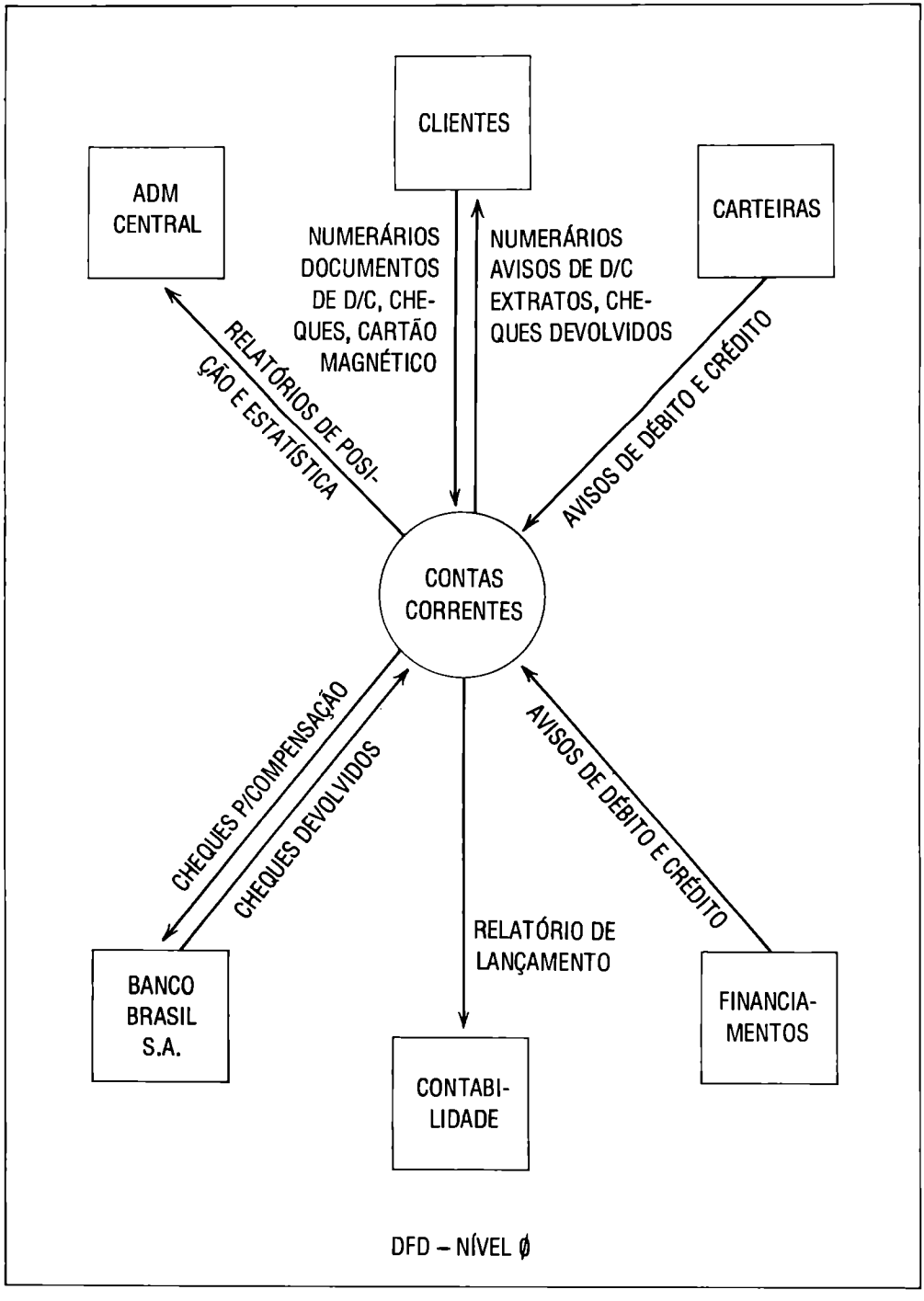


Figura 4.3. *DFD – Sistema contas-correntes bancário.*

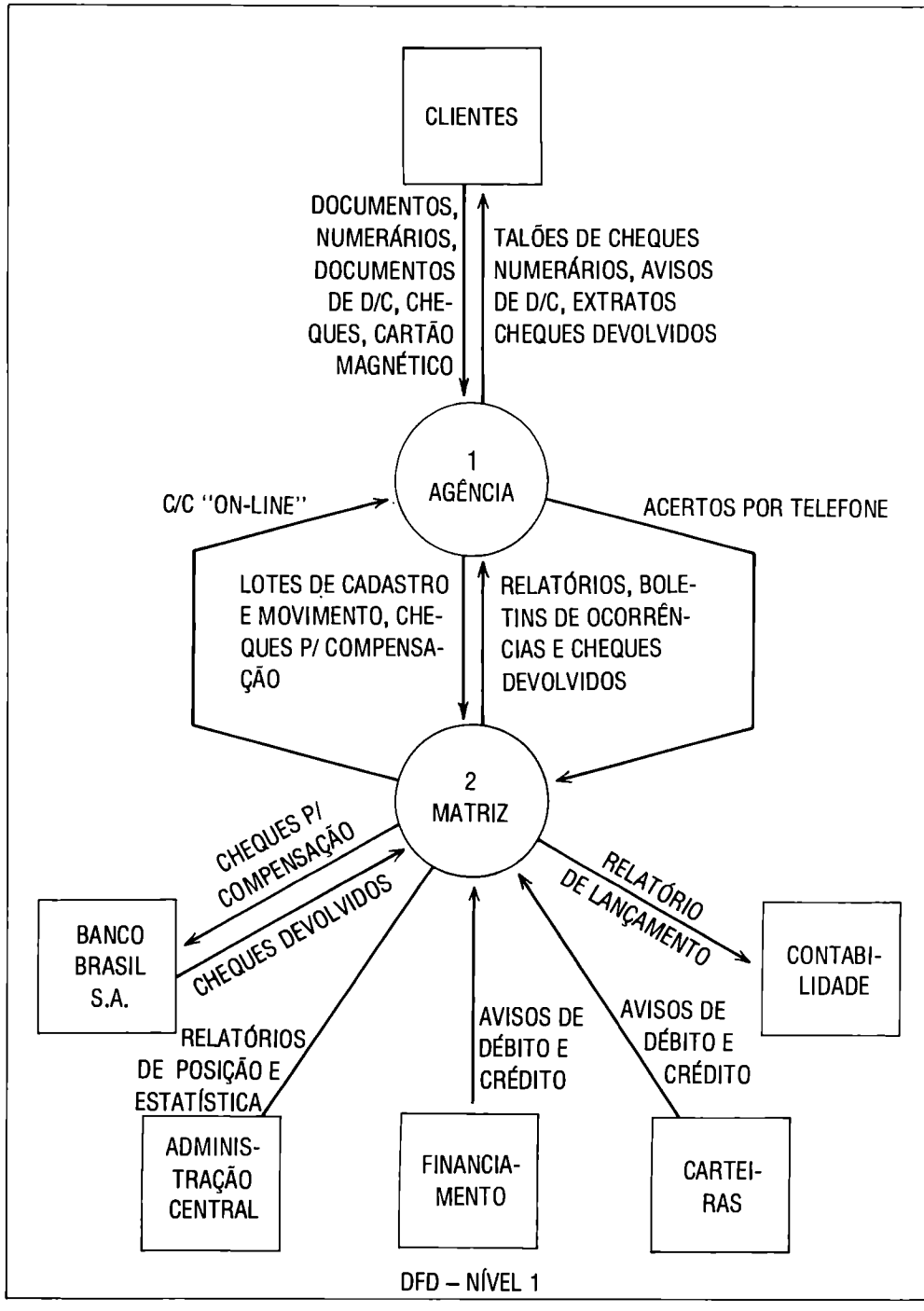


Figura 4.3. *DFD – Sistema contas-correntes bancário.*

Figura 4.3. *DFD – Sistema contas-correntes bancário.*

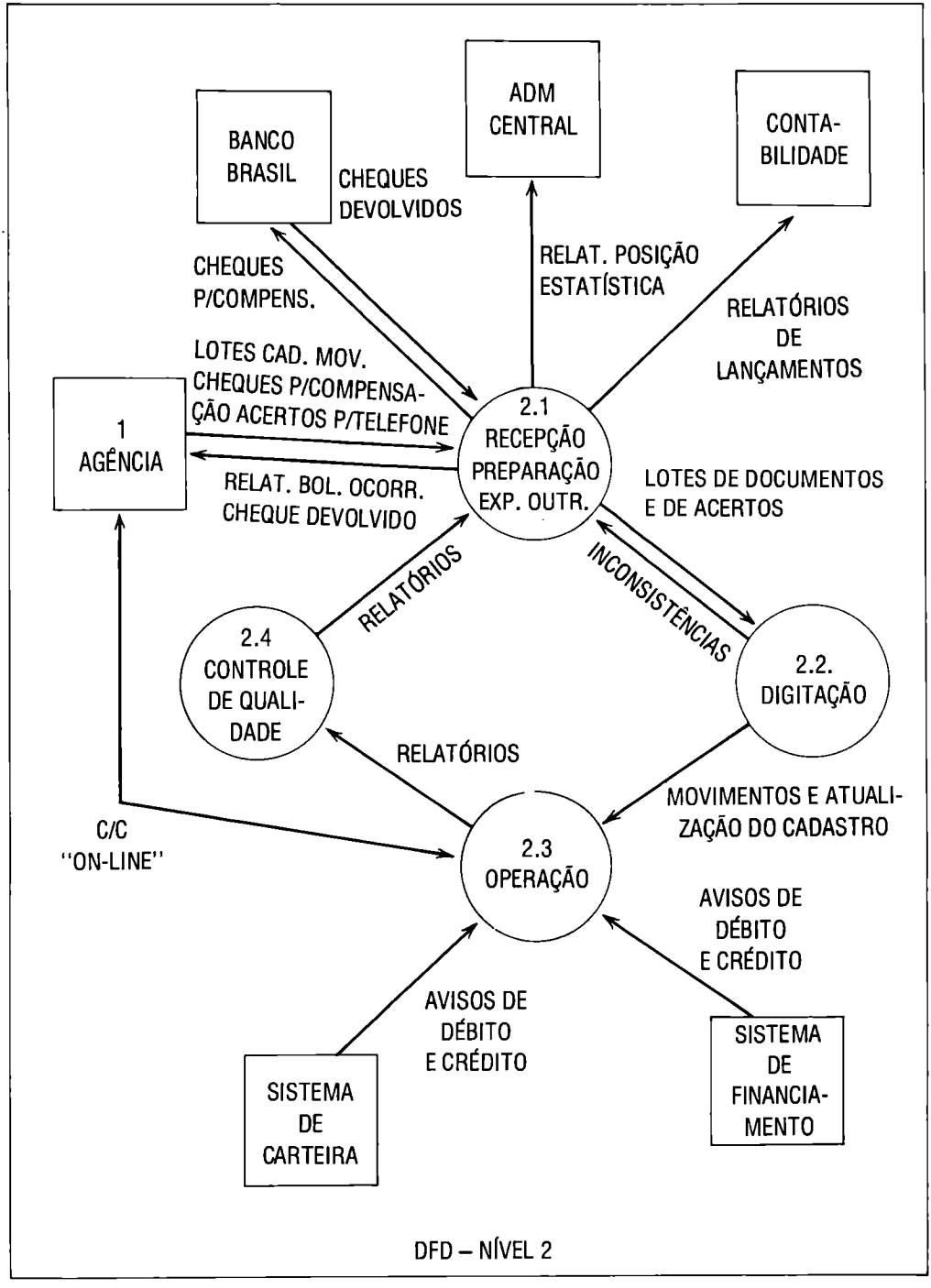


Figura 4.3. *DFD – Sistema contas-correntes bancário.*

A Figura 4.3 apresenta o DFD de um sistema de contas-correntes bancário do nível zero ao nível dois. Podemos plotar PC em qualquer um dos níveis, havendo, evidentemente, nos níveis mais analíticos maior facilidade na caracterização do PC.

Desta forma podemos identificar como PC:

a) Avisos de débito e crédito que fluem entre a Matriz e o Ambiente Externo/Sistema de Carteiras, caracterizado no nível 1 ou, se quisermos em um momento mais analítico, podemos flagrar no nível 2, Avisos de débito e crédito que fluem entre a área de operação do computador da Matriz (Processo 2.3) e o Sistema de Carteiras.

b) Subsistema de C/C-*ON-LINE* sendo processado na Operação da Matriz (processo 2.3) e no Caixa/Terminal *on-line* da Agência (processo 1.3) e correspondentes informações transacionadas, consoante DFD nível 2.

Os PC's poderão ser analisados e testados via:

- Sua caracterização em um Guia de Auditoria que irá detalhar a composição do PC, a ótica de sua validação etc.
- Seu detalhamento com o uso de técnicas de fluxogramação de auditoria analítica (fluxo de colunas) ou de computação (representação de programas, arquivos etc.).
- Sua explicitação em termos narrativos, via programa de auditoria ou seqüência de atividades para sua validação.

4.2 AUDITORIA DO DESENVOLVIMENTO DE SISTEMAS DE INFORMAÇÃO COMPUTADORIZADOS

A auditoria do desenvolvimento de sistemas computadorizados exige fortes conhecimentos de análise de sistemas por parte do auditor e isto implica que na carreira do auditor de sistemas ele deverá ter conhecimentos para atuar na auditoria de sistemas em operação antes de poder atuar na auditoria no desenvolvimento de sistemas.

Esta colocação pode parecer paradoxal, já que, logicamente, a auditoria de um sistema computadorizado deve iniciar-se quando da concepção construção e implantação desse mesmo sistema. Entretanto, os seguintes parâmetros remeteram os auditores a uma atuação inicial nos sistemas computadorizados em operação:

a) a auditoria de computador começou no Brasil com uma defasagem de dez anos em relação à área de computação e, desta forma, deu prioridade às verificações dos sistemas que já estavam operando, em detrimento daqueles que estavam sendo construídos;

b) na auditoria durante o desenvolvimento o auditor posta-se frente a frente com analistas e programadores, necessitando, portanto, de bons conhecimentos de computação e de análise de sistemas, bem como de uma postura de auditagem e de um exercitamento do "espírito de auditoria", que garanta uma atuação imparcial, concatenada e não embaralhada com os profissionais de computação;

c) a auditoria durante o desenvolvimento exige uma metodologia de atuação que garanta a independência dos trabalhos do auditor, estabelecendo os momentos e as formas de aplicação das técnicas de auditoria adequados para o estabelecimento das diferenças dos trabalhos do auditor e dos auditados.

Por conseguinte, o auditor de sistemas em desenvolvimento deve conhecer:

a) uma metodologia de desenvolvimento de sistemas computadorizados, com suas etapas, técnicas, formulários e conceitos que as caracteriza, bem como o papel desempenhado por analistas, programadores, profissionais de suporte e de produção na construção de um sistema computadorizado;

b) uma metodologia de auditoria que delineie a conceituação e a forma de participação do auditor na elaboração do sistema em computador.

4.2.1 Ciclo de desenvolvimento de sistemas de informação computadorizados

Um sistema de informações em computador possui um ciclo de vida caracterizado por:

- ciclo de desenvolvimento;
- ciclo de operação.

O ciclo de desenvolvimento pode ser dividido em etapas, tais como:

- inicialização do projeto;
- estudo de viabilidade;
- análise da situação atual;
- projeto lógico;
- projeto físico;
- desenvolvimento e testes;
- implantação;
- administração do projeto;
- manutenção.

A Figura 4.4 apresenta, segundo uma fluxogramação do tipo DFD, a mecânica com processos e resultados de operacionalização de uma metodologia para o cumprimento do ciclo de desenvolvimento de sistemas computadorizados.

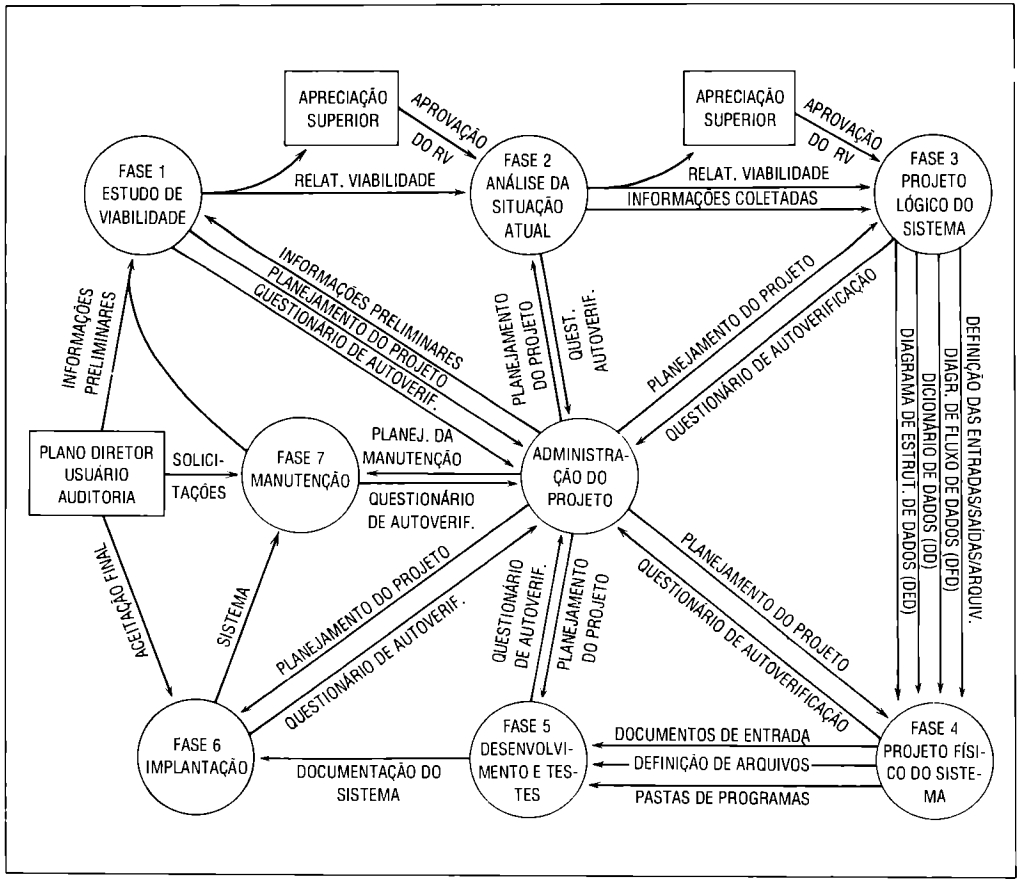


Figura 4.4. *Ciclo de desenvolvimento de sistemas de informação computadorizados.*

O ciclo de operação corresponde às fases, para a transformação do dado em informação, a serem exercidas pelo sistema quando de seu uso normal e rotineiro. Estas fases podem ser compostas de:

- captação e registro de dados;
- conversão dos dados;

- consistência dos dados;
- atualização de arquivos;
- armazenamento e recuperação de dados;
- apresentação das informações;
- utilização das informações.

Estas fases do ciclo de operação vão ser realizadas em função dos programas de computador e dos procedimentos definidos caracterizados e materializados quando do ciclo de desenvolvimento.

A fase de manutenção do ciclo de desenvolvimento irá ocorrer de forma entremeada com as várias utilizações do sistema.

A manutenção é um subconjunto do ciclo de desenvolvimento implicando o cumprimento, de forma abreviada, de todas as fases deste ciclo.

Com o conceito de ciclo de vida do sistema constatamos que um sistema de informação computadorizado nasce, vive e morre, ou seja, não é mais utilizado ou é substituído por um sistema mais moderno – em termos de tecnologia computacional – e mais atualizado – em termos de tecnologia da área usuária.

A morte de um sistema, sua substituição e, mesmo, muitas de suas manutenções ocorrem como conseqüência de Relatórios de Auditoria. A Figura 4.5 busca retratar a participação da auditoria de sistemas computadorizados.

O ciclo de vida de um sistema pode ser extremamente curto (de apenas alguns minutos ou horas) ou pode ser longo, ou seja, durar anos.

A vigência de sistemas computadorizados de ciclo curto é sentida no ambiente de microinformática, em que, devido à facilidade de programação dada pelas linguagens de quarta geração, à necessidade de tomada de decisão, à capacidade de o usuário poder elaborar seus próprios programas, um sistema pode ser concebido, construído e usado em poucas horas e ser abandonado ou destruído, não mais sendo utilizado. São os sistemas computadorizados descartáveis ou *one way*.

Esta situação pode ocorrer, também, via terminais utilizando-se de um computador de grande porte; entretanto, sua intensidade de ocorrência é predominante a nível de microcomputadores.

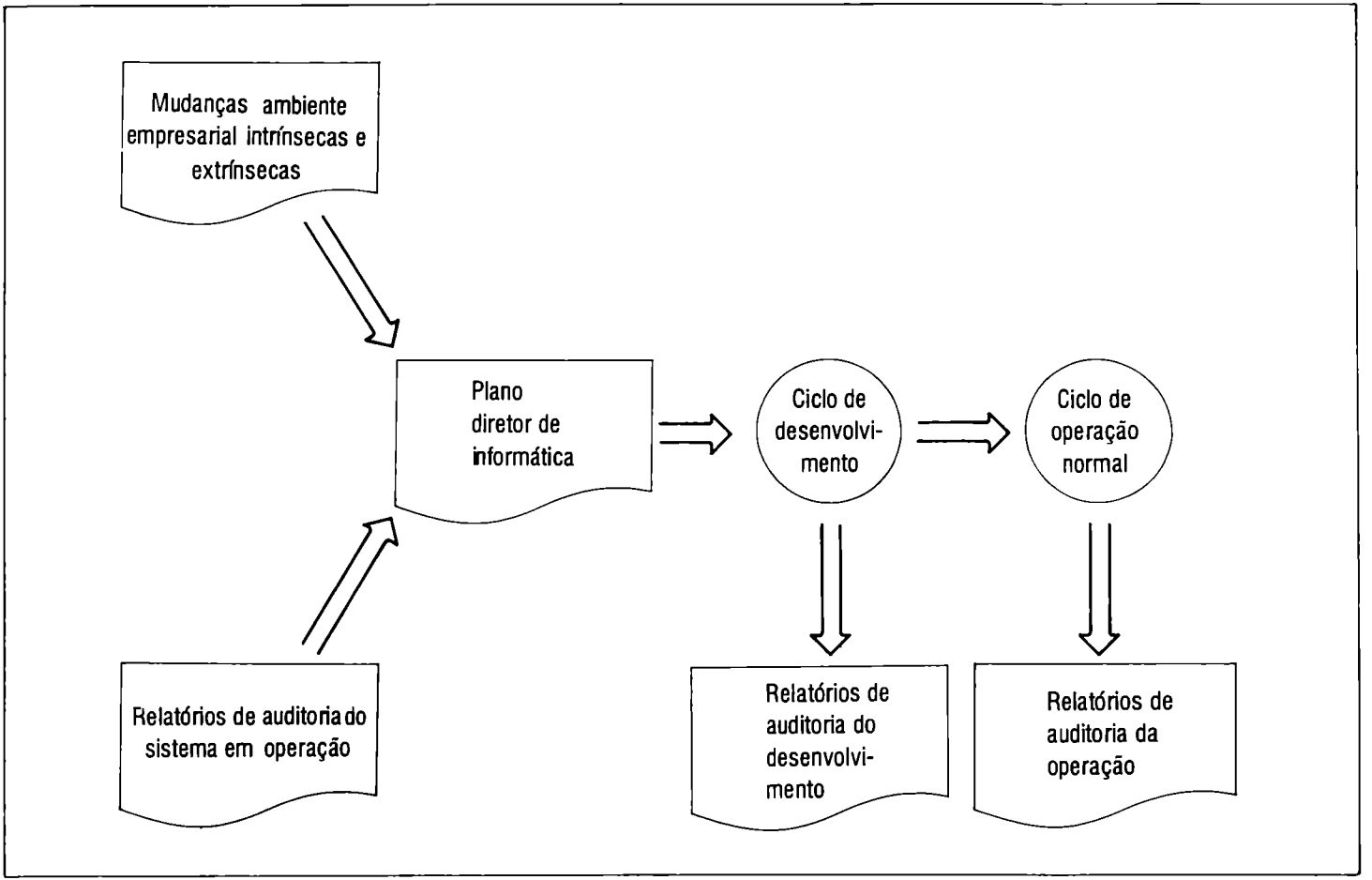


Figura 4.5. *Participação da auditoria de sistemas no ciclo de vida do sistema computadorizado.*

No ciclo de desenvolvimento de sistemas trabalham prioritariamente dois tipos de profissionais, que executam as seguintes tarefas:

a) *Analistas de sistemas*

- contata órgãos requisitantes de serviços de PED, coletando informações e estudando a viabilidade dos mesmos;
- elabora orçamento para implantação do sistema;
- efetua estudos e análises para elaboração de novos sistemas;
- documenta o sistema, via fluxogramação, elaboração de normas e manuais para sua caracterização;
- faz o projeto lógico e o projeto físico do sistema;
- elabora instruções para a programação do computador;
- prepara informações para operação do sistema;
- executa trabalho de manutenção nos sistemas implantados;
- utiliza uma metodologia visando ao alcance da eficácia, eficiência e segurança dos sistemas construídos.

b) *Programador de computador*

- traduz em linguagem de computador o serviço desenvolvido pela análise de sistemas;
- desenvolve trabalhos de montagem, depuração e testes de programas;
- executa serviços de manutenção em programas em produção;
- utiliza padrões e métodos para a organização, codificação e testes de programas.

Para a criação dos sistemas são concretizadas equipes de desenvolvimento com a aglutinação de analistas e programadores dedicados a determinado projeto de sistemas.

Outra esquematização é manter os analistas em equipes de projetos e os programadores em uma equipe única, podendo ser alocados para a programação de qualquer programa em qualquer projeto de sistemas.

Normalmente há um líder de projeto que exerce as atividades de administração de projetos como:

- estabelecer um cronograma para o projeto;
- alocar recursos ao projeto;
- controlar o orçamento.

Cada equipe de projeto de sistemas mantém relacionamento com outras áreas do centro de computação:

- com o administrador de dados para o uso ou definição de dados;
- com o analista de banco de dados para dirimir dúvidas quanto ao uso do *software* e banco de dados;
- com o analista de *software* básico para elucidar eventuais problemas com o sistema operacional;
- com o analista de teleprocessamento para equacionar aspectos técnicos da rede de computação usado pelo novo sistema aplicativo;
- com o analista de segurança para estruturar rotinas de *back-up* e enquadrar o sistema aplicativo ao plano de contingência;
- com o analista de qualidade para o acompanhamento do uso das técnicas de computação exigidas, do cumprimento de etapas etc.
- com os profissionais do centro de informações para a caracterização do nível de processamento e da disponibilidade de informações no ambiente microusuário.

4.2.2 Processo e técnicas de auditoria durante o desenvolvimento de sistemas

O Ponto de Controle tanto pode ser um processo como um resultado, e podemos exemplificar:

a) PC-DS – Ponto de Controle de vigência durante o ciclo de desenvolvimento do sistema.

b) PC-ON – Ponto de Controle caracterizado durante o ciclo de desenvolvimento mas cujo interesse de validação dar-se-á quando o sistema estiver em operação normal. Portanto, o PC-ON é de vigência durante o ciclo de vida do sistema.

O Ponto de Controle tanto pode ser um processo como um resultado e podemos exemplificar:

a) PC de natureza processo:

- etapa do ciclo de desenvolvimento;
- etapa da manutenção de sistemas;
- rotina operacional;
- rotina de controle.

b) PC de natureza resultado:

- documentação do desenvolvimento/manutenção de sistemas;
- relatórios do projeto;
- estrutura lógica do sistema;
- estrutura física do sistema;
- modelo conceitual da base de dados;
- projeto de arquivos;
- *layout* de documentos e relatórios;
- definição de programas.

PC-DS – são pontos de controle existentes nas diversas fases da metodologia de desenvolvimento de sistemas que podem ser validados segundo os enfoques:

a) Validação do *processo* de geração das especificações nas respectivas fases da metodologia, examinando e acompanhando as técnicas aplicadas e os procedimentos seguidos.

b) Validação dos *resultados* gerados em cada fase da metodologia, no tocante ao cumprimento das normas e da qualidade das especificações.

PC-ON – são pontos de controle componentes do sistema aplicativo, segundo suas diversas fases de operacionalização, que vão desde a captação e registro dos dados até a apresentação e utilização da informação, validados segundo os enfoques:

a) Validação do *processo* de transformação de dados em informações através da identificação das rotinas operacionais e de controle componentes dos sistemas aplicativos.

b) Validação do resultado gerado em cada processamento do sistema aplicativo, pela análise de arquivos gravados e de relatórios/telas emitidos.

A Figura 4.6 apresenta exemplos de pontos de controle do desenvolvimento de sistemas tanto do tipo DS quanto ON, quer no momento processo ou resultado.

PONTO DE CONTROLE	PARÂMETRO CONTROLE INTERNO	TÉCNICA DE AUDITORIA	CARACTERÍSTICAS DA AUDITORIA
1. Análise da aplicação da técnica de análise estruturada na concepção do projeto lógico do sistema de folha de pagamento (PC-DS-Processo)	Eficiência	– Questionário – Entrevistas	Aplicação de questionários para a realização de entrevistas com a equipe de projeto para avaliação de: a) Utilização da técnica de análise estruturada. b) Que entidades foram consideradas do ambiente externo e por quê? c) Quais as funções/atividades foram estudadas no processo de análise estruturada? d) Quantos níveis foram necessários retratar para um adequado entendimento do sistema?
2. Análise do relatório de anteprojeto do sistema aplicativo (PC-DS-Resultado)	Eficácia	– Visita **in loco** – Análise da documentação	Verificação do relatório de anteprojeto em face do estabelecido na metodologia de desenvolvimento de sistemas em termos de: a) Conteúdo. b) Forma de apresentação. c) Quem aprovou o relatório? d) Quais os objetivos para o sistema aplicativo estabelecidos no anteprojeto?

PONTO DE CONTROLE	PARÂMETRO CONTROLE INTERNO	TÉCNICA DE AUDITORIA	CARACTERÍSTICAS DA AUDITORIA
3. Rotina estatística automatizada de erros/informações fora de parâmetros normais (PC-ON-Processo)	Segurança lógica	**Test-deck**	Simulação de dados para testar: a) A intensidade de monitoração e de acompanhamento estatístico com operações/informações erradas ou fora de limites considerados de normalidade. b) Opções para modificação dos parâmetros/critérios de enquadramento das situações pela rotina.
4. Arquivos gerados pela aplicação de um protótipo em um processamento paralelo (PC-ON-Resultado)	Segurança lógica	Programa de computador para auditoria	Verificação dos totais de controle componentes dos campos do registro **trailer** e da validade do conteúdo dos campos de registro **header.**
5. Análise do funcionamento do sistema (PC-ON-Processo)	Segurança lógica	**Base case system evaluation**	– Determinação do nível de operacionalidade do sistema em termos de correção das rotinas operacionais e de opções na identificação de erros das rotinas de controle. – Conjunto básico de dados simulados, que permite o acompanhamento das alterações efetuadas no sistema, pela aplicação intermitente desse conjunto de dados, durante o ciclo de operação normal do sistema.

Figura 4.6. *Pontos de controle do desenvolvimento de sistemas.*

A validação dos PC requer técnicas que agilizem e viabilizem o processo de auditagem. Estas técnicas de auditoria durante o desenvolvimento estão estruturadas na Figura 4.7.

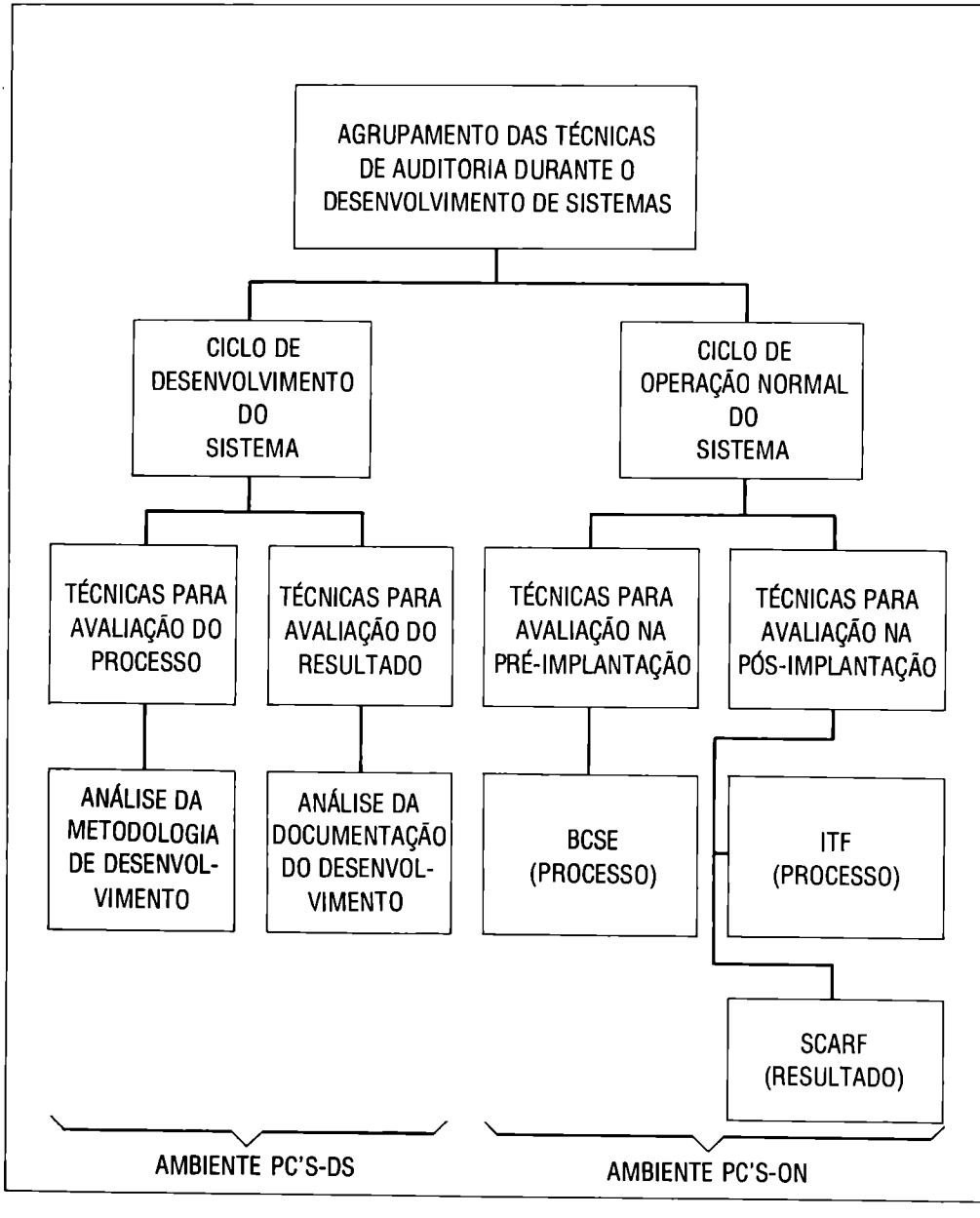


Figura 4.7. *Técnicas de auditoria durante o desenvolvimento de sistemas.*

A – *Técnicas do ciclo de desenvolvimento do sistema*

As características a seguir estabelecem a natureza das técnicas de auditoria durante o desenvolvimento de sistemas computadorizados:

I – *Técnica "Análise da metodologia de desenvolvimento de sistemas"*

Corresponde à avaliação da metodologia adotada pelo centro de computação e que será utilizada pela equipe de projeto do sistema aplicativo em desenvolvimento.

Os procedimentos a serem seguidos para aplicação desta técnica são:

a) Entendimento da metodologia através da leitura de seus manuais componentes e via esclarecimentos junto à gerência de desenvolvimento de sistemas.

b) Identificar pontos de controle na metodologia de desenvolvimento, tais como:
   - encadeamento lógico das etapas;
   - objetivos de cada etapa;
   - técnicas de análise de sistemas utilizadas (análise estruturada, funcional etc.);
   - produtos gerados em cada etapa;
   - responsabilidade pela execução de cada etapa e geral;
   - documentação exigida em cada etapa;
   - controles de execução de cada etapa e geral;
   - mecânica de avaliação da qualidade do desenvolvimento do sistema.

c) Avaliar a adequacidade desses PC's à cultura de informática da empresa – em termos de *hardware*, de *software* e de pessoal de computação e usuário. Levar em consideração as aplicações da metodologia já feitas junto a aplicativos da empresa e às práticas do mercado no tocante às metodologias de desenvolvimento de sistemas.

d) Emitir opinião, debater com a equipe de computação e continuar a fazer avaliações na continuidade da aplicação da metodologia a novos sistemas em desenvolvimento.

Quando *não houver metodologia de desenvolvimento*, tal fato se constituirá em fraqueza de controle interno e para a continuidade dos trabalhos o auditor deverá levantar com o analista de sistemas responsável pelo projeto de desenvolvimento as etapas, as técnicas e os formulários que irão ser usados.

A técnica exige do auditor de sistemas conhecimentos de análise de sistemas e de uma metodologia de desenvolvimento de sistemas.

II – *Técnica "Análise da documentação do desenvolvimento do sistema"*

O método consiste na avaliação das especificações e/ou construções geradas para o sistema, ao final de cada etapa da metodologia (ou roteiro) de desenvolvimento de sistemas.

As etapas de aplicação da técnica implicam:

a) Entendimento das especificações e/ou construções através da leitura da documentação gerada.

b) Identificação dos pontos fracos das especificações, no tocante a:

- objetivos do sistema;
- análise custo/benefício do novo sistema;
- levantamento e conclusões do sistema atual;
- anteprojeto do sistema;
- projeto lógico;
- projeto físico (arquivos, programas, relatórios, telas);
- testes isolados e integrados;
- programação;
- implantação;
- prototipagem;
- treinamento para institucionalização do novo sistema;
- documentação geral do projeto.

c) Analisar e avaliar os resultados obtidos emitindo o relatório de fraquezas de controle interno.

As fraquezas identificadas poderão, de imediato, reciclar o projeto, permitindo ao coordenador do projeto atender a requisitos mínimos de controle e eficiência de sistemas.

Obviamente, o auditor de sistemas deverá ter fortes conhecimentos de controles de entrada, processamento e saída em sistemas computadorizados *batch*, TP/DB, microinformática.

B – *Técnicas de operação normal do sistema desenvolvidas durante o desenvolvimento de sistemas*

As três técnicas BCSE, ITF e SCARG serão criadas quando se der o desenvolvimento de sistemas computadorizados, e usadas segundo os critérios:

a) BCSE – Base Case System Evaluation – criada e usada na implantação do sistema e, também, utilizada durante o ciclo de operação do sistema com o objetivo de plotar as alterações ocorridas com o sistema.

b) ITF – Integrated Test Facility – criada quando se der o desenvolvimento do sistema e usada durante o ciclo de operação do sistema.

c) SCARF – System Control Audit Review File – criada quando do desenvolvimento do sistema e usada durante o ciclo de operação do sistema.

Cada uma das técnicas guarda as seguintes características de aplicação pelo auditor:

I – *BCSE – Base Case System Evaluation*

Técnica semelhante ao *test-deck,* quando uma massa de testes, feita pelo auditor, é submetida ao novo sistema computadorizado, antes de sua implantação, permitindo a avaliação do controle interno e tendo como conseqüência a emissão de um relatório de fraquezas de controle interno, quando inconveniências são identificadas.

A massa de teste deve cobrir, integralmente, o sistema, isto é, devem ser testados procedimentos a nível dos usuários e a nível de processamento eletrônico de dados.

A aplicação desta técnica traz as seguintes vantagens ao novo sistema:

a) a documentação do sistema é geralmente superior;

b) correção de falhas e realização de ajustes são antecipadas, permitindo maior tranqüilidade aos primeiros processamentos reais do sistema;

c) o auditor integra-se com os usuários e os profissionais de computação, colaborando para o treinamento deles em virtude da realização do teste.

Um alto grau de planejamento das atividades de teste é exigido do auditor, usuários e profissionais de PED.

II – *ITF – Integrated Test Facility*

Corresponde ao desenvolvimento de rotinas de auditoria, dentro dos programas de computador a serem auditados, com o objetivo de separar os dados de teste da auditoria, quando estes forem submetidos aos programas sob auditoria.

Os dados de teste da auditoria serão submetidos em conjunto com os dados normais que são processados pelo programa sob auditoria.

As etapas de aplicação do ITF são:

a) por ocasião do desenvolvimento do sistema aplicativo:
   - o auditor participa com usuários e profissionais de PED da criação do sistema para entender seu conteúdo;
   - o auditor cria rotinas ITF para serem agregadas aos programas do sistema aplicativo, de sorte que estas rotinas retirem as transações ITF dos arquivos e resultados correspondentes às transações normais;

b) durante a operação normal do sistema:
   - o auditor simula transações marcadas como sendo ITF e as submete juntamente com as transações normais ao programa sob auditoria;
   - o auditor prepara formulários de teste identificando os resultados que deverão ser alcançados após o processamento do programa sob auditoria;
   - analisa e avalia os resultados alcançados.

A implantação das rotinas ITF geralmente ocorre com a criação de uma empresa *dummy* no sistema, que conterá transações exclusivas da auditoria.

III – SCARF – System Control Audit Review File

O método implica a criação de rotinas específicas de auditoria dentro dos programas do sistema, para selecionar transações reais, segundo condições preestabelecidas, gravando um arquivo específico para efeito de auditoria.

É uma técnica usada intensamente em sistemas *real-time*, por permitir analisar/auditar a tempo de processamento transações com características particulares, tais como:

a) movimentação de item de estoque ou conta corrente paralisada há determinado período de tempo;
b) saque, em conta, com valor dez vezes maior que o saque médio;
c) quantidade de dependentes três vezes superior à média de dependentes por funcionário.

A estrutura de aplicação da técnica é:

- durante o desenvolvimento do sistema:
  - participação do auditor junto a usuários e profissionais de computação para entendimento do sistema;
  - caracterização dos critérios para seleção das transações;
  - desenvolvimento, pelo auditor, das rotinas SCARF, e inclusão nos programas, para efeito de atendimento aos critérios de seleção de transações definido;
- durante o processamento do sistema sob auditoria:
  - analisar e avaliar os arquivos SCARF gerados durante o processamento do sistema;
  - emitir opinião sobre os resultados considerados fraquezas de controle interno.

A aplicação da técnica permite variações a partir de:

- alteração de tabelas com parâmetros determinantes dos critérios de seleção;
- manutenção de programas com inclusão de novas rotinas SCARF para novos critérios de seleção.

A seleção e gravação de transações acontece sempre que os programas sob auditoria são executados.

4.3 AUDITORIA DO CENTRO DE COMPUTAÇÃO

Nos itens 4.1 e 4.2 foi vista a auditoria de um sistema aplicativo, respectivamente, em operação normal e em desenvolvimento, cobrindo o ciclo de vida de um sistema computadorizado.

Entretanto, para que um sistema aplicativo exista há necessidade de uma infra-estrutura que dê sustentação ao mesmo.

Esta infra-estrutura é composta de:

- instalações;
- profissionais que executam tarefas comuns a todos os aplicativos;
- contratos de *hardware* e *software;*
- equipamentos;

- *software* básico e de apoio;
- redes de comunicação para integração local e remota dos computadores;
- procedimentos administrativos, técnicos, gerenciais;
- planos para a integração de toda essa tecnologia.

Vamos discutir a auditoria do centro de computação segundo os segmentos apresentados na Figura 4.8 e colocaremos em evidência outros momentos da auditoria de sistemas no item 4.4.

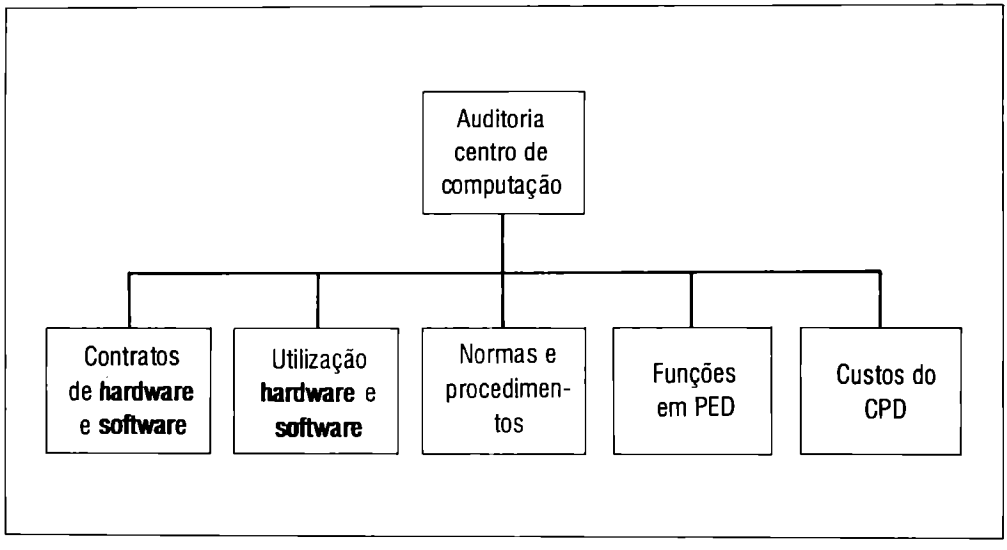


Figura 4.8. *Áreas de atuação de auditoria de um centro de computação.*

Os tópicos da auditoria do centro de computação, evidentemente, dependem do ambiente computacional em que são discutidos.

4.3.1 Auditoria de contratos de hardware e de software

A auditoria deste tópico tem por objetivo assegurar que as transações de compra, venda, aluguel, *leasing*, seguros e manutenção dos equipamentos *(hardware)* disponíveis no ambiente computacional, bem como as transações de compra, locação e manutenção de *software* (básico, de apoio e aplicativo) estão respaldadas pelos respectivos contratos, assim como as cláusulas componentes, no tocante a aspectos financeiros, operacionais, técnicos e administrativos, são do interesse da organização.

Uma verificação geral dos contratos inclui:

- aprovação pelo departamento jurídico;
- data da celebração;
- validade e autenticidade das assinaturas;
- vigência e situações de rescisão;
- condições de pagamento;
- critérios de reajustes de preços;
- adendos e suas implicações.

A Figura 4.9 apresenta uma série de características a serem constatadas pela auditoria.

RECURSO COMPUTACIONAL / NATUREZA CONTRATO	HARDWARE	SOFTWARE
Compra locação e **leasing**	Intermediação da transação (**leasing**). Apólices de seguros (contratos/adendos). Abrangência da cobertura do seguro.	
Compra e locação		Condições de adaptação e locação. Contratos mistos (locação/compra). Cessão de programas-fontes.
Manutenção	Períodos cobertos pelo contrato: – técnico residente; – horário comercial; – madrugada; – fins de semana/feriados. Prazo de atendimento às chamadas. Tempo máximo para solucionar problemas. Multas contratuais.	Implementação de novas versões. Prazo de atendimento às chamadas. Tempo máximo para solucionar problemas. Multas contratuais.

Figura 4.9. *Parâmetros para verificação de contratos.*

A verificação do *hardware* e do *software* contratado implica as tarefas:

- identificação contratual do equipamento ou *software;*
- identificação física do *hardware* e constatação da existência do *software* catalogado na biblioteca de programas (disco do sistema operacional residente);
- condições e intensidade de uso dos equipamentos contratados;
- nível de utilização do *software;*
- verificação da existência de *back-up* do *software* contratado.

Quanto aos aspectos financeiros, os contratos devem ser verificados em termos de:

- cálculo de valores das últimas parcelas pagas, com base no contrato;
- conciliação dos valores faturados com valores pagos e com valores calculados;
- acompanhamento dos preços vigentes no mercado e confronto com os pagamentos efetuados.

As cláusulas técnico-operacionais vão depender de cada situação, mas alguns momentos de análise são:

- verificar características de *software* no momento da montagem de redes de computadores;
- verificar capacidade de memória do equipamento e características do sistema operacional no momento da contratação de *software;*
- identificar o nível de aceitação e de treinamento dos usuários/profissionais de computação antes da contratação de *software*.

4.3.2 Auditoria da utilização de hardware e de software

A técnica para a realização desta auditoria está detalhada no item 3.10 (Análise de *log/accounting*).

A partir do controle do uso dos equipamentos e programas podemos criar indicadores que nos permitam:

a) devolver/alienar *hardware* e *software;*

b) estabelecer critérios para treinamento de usuários e profissionais de PED;

c) desclassificar em termos de idoneidade de fornecedores;

d) conduzir a inovação tecnológica do ambiente computacional;

e) estabelecer critérios de depreciação de equipamentos;

f) montar um plano diretor de informática factível de ser cumprido;

g) manter um orçamento de *hardware, software* e pessoal de computação equilibrado, ou seja, otimizado em termos de mínimos dispêndios financeiros e máximos resultados.

A aplicação de questionários e realização de entrevistas são duas outras técnicas que complementam a análise do *log/accounting* porque:

- permitem identificar as causas de mau uso de equipamentos e programas;
- são uma oportunidade de entendimento e convencimento entre auditor e auditados em PED.

4.3.3 Auditoria de funções

Compreende a análise de funções, da estrutura e do posicionamento do CPD e do fluxo de informações/de trabalho do ambiente computacional.

A análise das funções de PED guarda as seguintes características:

a) *Objetivo:* assegurar a qualidade, o rendimento, a eficácia e a produtividade do trabalho da área sob auditoria.

b) *Forma de atuação:*

- análise do perfil da função;
- análise do processo administrativo versus níveis da empresa.

c) *Técnicas de auditoria:*

- para análise do perfil da função-questionário;
- para análise do processo administrativo versus níveis da empresa-questionário, entrevista, análise de documento/relatório/telas.

A Figura 4.10 instrumenta a análise do perfil da função e a Figura 4.11, a análise do processo administrativo versus níveis da empresa.

CARGO / ITENS	GERENTE DE SISTEMAS	COORDENADOR DE SISTEMAS	ANALISTA DE SISTEMAS
Tempo na organização			
Tempo no cargo			
Experiência em PED			
Cursos técnicos			
Escolaridade			

Maturidade profissional

Capacitação profissional

Formação profissional

Figura 4.10. *Análise do perfil da função.*

PROCESSOS / NÍVEIS	PLANEJAMENTO	EXECUÇÃO	CONTROLE
Estratégico	Tarefas de planejamento estratégico e de determinação de objetivos.	Tarefas de determinação de políticas e diretrizes para direção e condução de pessoal.	Tarefas de controles globais e de avaliação de desempenho empresarial.
Gerencial	Tarefas de planejamento tático e de alocação de recursos.	Tarefas de gerência e de aplicação dos resultados.	Tarefas de controles e de avaliações de desempenho departamentais.
Operacional	Tarefas de elaboração de planos operacionais.	Tarefas de chefia, supervisão, coordenação, motivação de pessoal e execução dos trabalhos e das operações.	Tarefas de controle e avaliação de desempenho individuais.

Figura 4.11. *Análise do processo administrativo versus níveis da empresa.*

A análise da estrutura e do posicionamento do CPD implica:

a) *Objetivo*

- assegurar o aproveitamento da especialização, a maximização dos recursos, o controle e a coordenação;
- assegurar a integração do CPD com o ambiente e a minimização dos conflitos.

b) *Forma de atuação*

- análise das atividades do CPD segundo sua departamentalização.
- análise do posicionamento do CPD na estrutura da empresa.

A análise do fluxo de informações atende a:

a) *Objetivo*

- assegurar a adequação do fluxo de informação entre os setores do CPD e entre o CPD e os usuários.

b) *Forma de atuação*

- análise do fluxo de procedimentos e das respectivas informações de controle.

A Figura 4.12 retrata o fluxo de procedimentos da área de produção.

Na realidade, a dinâmica do centro de computação sempre sofreu grandes modificações ao longo dos anos e passa, presentemente, por sua mais forte alteração, em função da microinformática.

A distribuição de sistemas é intensa, o que contribui decisivamente para o enfraquecimento e, até, desaparecimento de funções do centro de computação, bem como de sua atuação e posicionamento perante os demais departamentos da empresa.

A tendência quanto ao centro de computação é regida pelas seguintes diretrizes:

a) diminuição da quantidade de profissionais no centro de computação;
b) aparecimento de novas funções altamente especializadas;
c) o centro de computação transforma-se em uma entidade de consultoria técnica em processamento eletrônico de dados dentro das organizações;
d) descentralização de *hardware* e de procedimentos de PED, impondo aos usuários:

- absorção das tecnologias de desenvolvimento de sistemas e das tarefas de produção e de criação de aplicativos.

4.3.4 Auditoria de normas e procedimentos

Esta auditoria deve atender a:

a) *Objetivos:*

- assegurar a divulgação e o uso de informações referentes a política, diretrizes, organização e serviços de forma sistematizada, criteriosa e segmentada;
- assegurar o treinamento e a capacitação dos recursos humanos e o funcionamento do CPD.

b) *Forma de atuação:*

- verificação da existência e da qualidade das normas e procedimentos;
- verificação da aderência das normas e procedimentos à capacitação técnica dos recursos humanos e à cultura do centro de computação.

c) *Técnicas usadas:*

- questionário, visita *in loco,* entrevistas, análise da documentação.

A Figura 4.13 apresenta os parâmetros de caracterização versus os níveis de destino de normas e procedimentos.

Alguns itens a serem verificados na formalização são:

- informações completas sobre o objeto da normalização;
- facilidade de atualização;
- distribuição dos manuais;
- compatibilidade da segmentação das normas com as peculiaridades da organização;
- existência de padrão estético (redação e apresentação);
- consistência do conteúdo;
- codificação que permita referência ao manual;
- atualização das informações.

As normas devem estabelecer as diretrizes e os vetores segundo os quais a organização funciona.

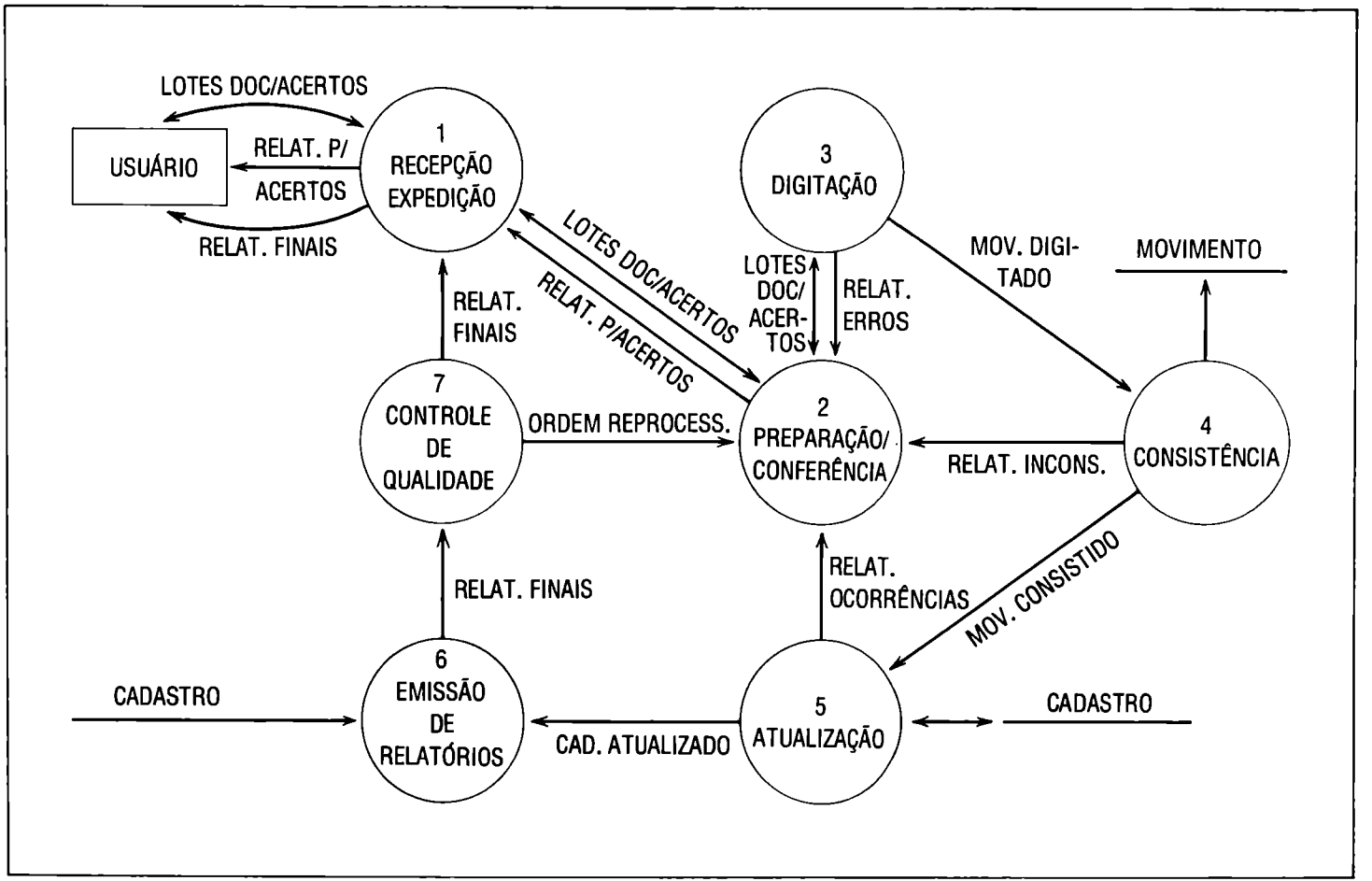


Figura 4.12. *Fluxo de procedimentos – área de produção.*

PARÂMETROS CARACTERIZAÇÃO / NÍVEIS	FORMALIZAÇÃO	ESCOPO	TIPOS DE NORMALIZAÇÃO
Estratégico	Através das regras e regulamentos.	Empresa	– Manual de organização. – Manual de estrutura. – Manual de normas.
Gerencial	Através das fases e operações de cada rotina.	Fluxo do trabalho (o que fazer)	– Manual de normas e procedimentos. – Manual de rotinas. – Manual de procedimentos.
Operacional	Através das instruções e procedimentos detalhados.	Cargos (como fazer)	– Manual de instruções. – Manual de técnicas. – Manual de serviços. – Manual de formulários.

Figura 4.13. *Estrutura para análise das normas e procedimentos.*

4.3.5 Auditoria de custos em PED

Os custos de um centro de processamento de dados (CPD) necessitam ser determinados em função de:

a) a área de computação ser um departamento que presta serviço aos demais departamentos-fim e aos departamentos-meio da organização:
   - da ótica do CPD, normalmente, seus custos totais são rateados aos demais departamentos, por hora consumida ou volume mensal de transações processadas.

b) a empresa considerar o dado um ativo fundamental e, como tal, as várias fases de sua elaboração necessitam ser custeadas, a fim de que otimizações possam ser realizadas:

- desta ótica é necessário identificarmos:
  - custo da digitação de um pedido;
  - atualização de funcionário no cadastro de folha de pagamento;
  - custo da utilização do mainframe por item de estoque processado.

A auditoria de custos do CPD será realizada sobre os vetores:

- critérios para apuração de custos estabelecidos;
- indicadores de custos apurados e sua correspondente evolução histórica ou confrontação de suas métricas com os padrões de mercado;
- esquema de análise de custos vigentes;
- ações tomadas e pendências existentes para a minimização dos custos em PED.

Um dos critérios para embasar/sustentar um sistema de custos em PED é o estabelecimento de um sistema de custos-padrão no CPD que obedeceria às seguintes etapas:

- identificação dos tipos de serviços de informática a serem prestados;
- identificação dos recursos a serem utilizados e dimensionamento das respectivas capacidades, com a atribuição de um valor unitário nominal de uso;
- análise do consumo de cada um dos recursos em cada tipo de serviço com o estabelecimento do respectivo roteiro de cálculo;
- elaboração de uma tabela de custos para cada serviço de determinado tipo, com base no roteiro de cálculo estabelecido;
- apropriação dos custos a cada usuário (serviço, de acordo com a tabela de custos estabelecida);
- revisão e ajuste da tabela de custos com base na análise do consumo real dos recursos.

Finalmente, é importante destacar os seguintes tópicos referentes a um esquema de custos em computação:

a) a apuração do custo unitário de cada produto/serviço é de responsabilidade do analista de sistemas com base na tabela de utilização de recursos;

b) na fase de anteprojeto do sistema aplicativo deve haver uma previsão de custos;

c) resistência do pessoal é uma das barreiras a serem vencidas quando se adota um sistema de custos;

d) o auditor de sistemas, além de avaliar os controles operacionais existentes, deve também avaliar a relação custo x benefício do CPD.

4.4 TÓPICOS ESPECIAIS DA AUDITORIA DE SISTEMAS

A explosão da microinformática e das redes de computadores implicou a atuação, em todas as frentes empresariais, do auditor de sistemas. Novos momentos e novas abordagens fizeram-se sentir e a abrangência da auditoria de sistemas cresceu.

4.4.1 Auditoria em ambiente de microinformática

O trabalho do auditor de sistemas em microinformática guarda as seguintes características:

a) Prioritariamente, o auditor deve atuar junto ao centro de informações (CI) para identificar:

- inventário de micros, sua localização física, seus usuários, sua configuração, seus *softwares*, tempo de instalação etc.;
- política de microinformática na empresa, o papel do CI, profissionais de PED que o compõem, posicionamento do CI na estrutura do CPD, esquema de trabalho do CI, indicadores de gerenciamento dos trabalhos do CI etc.

b) a estratégia de atuação do auditor de sistemas junto aos micros deve ser de aproximações sucessivas com a finalidade de identificação, uso e:

- constatação da veracidade do inventário de características de micro feito no CI;
- aplicação de estatística para estratificação do universo de micros, caracterizando:
  1. tempo médio de utilização do micro;
  2. natureza de seu uso:
     - planilha eletrônica;
     - correio eletrônico;

- editor de texto;
- *software* de desenvolvimento próprio;
- uso de *softwares* de terceiros;

3. indicadores de qualidade do uso do micro;
4. características de segurança física, lógica e confidencialidade do trabalho com o micro;
5. nível de apoio dado pelo CI aos usuários, segundo a opinião destes;

- envio de questionário preliminar para efeito de sondagem e de viabilização da estratificação do universo de micros. A monitoração, em um primeiro estágio de auditagem do micro, é desejável em face do dinamismo, da pulverização e da quantidade de micros existentes em nossas organizações;
- caracterização do universo de micros em termos de:
  - micros independentes;
  - rede de micros;
  - micros multiusuários;
  - rede de micros x *mainframe*.

c) atuação junto a todas as áreas da empresa impondo ao auditor de sistemas diálogo com as mais diversas técnicas de aplicação do computador:

- em nível industrial em sistemas CAD-CAM-CAE, ou seja, em projetos desenvolvidos com computador e em aplicação do computador na manufatura. Na realidade, o auditor defrontar-se-á com a área de inteligência artificial, particularmente com o segmento de robótica;
- em nível de automação de escritório com a monitoração dos trabalhos administrativos pelo microcomputador;

d) aparecimento ou ênfase em novas situações de auditoria, tal como a documentação dos sistemas e de seu uso quando construídos pelos usuários, particularmente no tocante a sistemas descartáveis.

A abordagem da auditoria em microinformática pode, portanto, ser vista em dois subconjuntos:

I – *Auditoria do CI caracterizado por:*

a) Problemática do relacionamento usuários *versus* CPD.

- grande fila de espera (*back-up*) para o desenvolvimento de novas aplicações;

- a área de desenvolvimento de sistemas concentrada, de forma quase total, na manutenção dos sistemas existentes;
- não-atendimento de projetos pequenos pelo pessoal de sistemas;
- alto custo de desenvolvimento dos projetos pequenos;
- demanda reprimida de serviços não tradicionais nem solicitados pelos usuários (processamento de textos, sistemas não estruturados etc.);
- custo de *hardware* diminuindo e custo de desenvolvimento de sistemas aumentando;
- consciência do usuário das potencialidades do computador sem poder beneficiar-se do mesmo;
- produtos de *hardware* e *software* que facilitam o uso de computação com um mínimo de treinamento do usuário.

b) Objetivos do Centro de Informações:

- possibilitar ao usuário o acesso às informações em tempo mais curto para a tomada de decisões;
- prover o usuário de ferramenta útil (microcomputador) para aumentar a sua produtividade;
- reduzir a carga de manutenções nos sistemas que são processados no *mainframe;*
- aumentar a concentração dos recursos do CPD (análise e programação) no desenvolvimento de novos sistemas;
- permitir e facilitar o acesso de usuários autorizados aos recursos do computador central;
- treinar os usuários em operação, programação e análise em microcomputadores;
- dar suporte para o desenvolvimento, manutenção e utilização de programas aplicativos em microcomputadores;
- apoiar a escolha e aquisição de microcomputadores e respectivos *softwares*;
- orientar e controlar a utilização de microcomputadores;
- disseminar os conceitos de microinformática em todos os níveis da organização.

c) Técnicas de auditoria aplicadas ao CI:

- análise das funções do CI:
  - avaliação das atividades de suporte;
  - avaliação das atividades de treinamento e disseminação dos conceitos;

- avaliação das atividades de controle da utilização e dos custos de *hardware* e *software* (inventário de *hardware* e de *software*);
- avaliação da estrutura e do posicionamento do CI;

- análise das normas e procedimentos do CI:
  - normas administrativas de existência de *back-up* de programas e arquivos;
  - normas operacionais no tocante a linguagens de programação usadas, uso de editor de texto, planilha eletrônica, sistemas aplicativos em termos de sua operação etc.;
  - normas de documentação do desenvolvimento de programas (criar um DFD) e de operacionalização do micro (existência de *log* automático e de folha de registro de utilização);
  - análise das contratações/aquisições de *hardware* e *software*;
  - análise do atendimento às necessidades dos usuários.

II – Auditoria dos microcomputadores e seus correspondentes usuários:

a) Envio do questionário preliminar aos usuários para identificação do micro e de seu ambiente com a captação dos seguintes dados, como pontos de verificação inicial de um ambiente de microcomputadores:

- *hardware* existente;
- *software* existente;
- organização da área de microinformática;
- uso das interfaces de comunicação;
- procedimentos de segurança;
- procedimentos para *back-up* e contingência;
- nível de documentação existente;
- nível de treinamento do usuário;
- características ergonômicas do uso do micro.

b) Recebimento das respostas, tabulação e estratificação com a determinação dos micro/usuários merecedores de auditoria mais detalhada com a aplicação das técnicas, visita *in loco*, entrevista e questionários abrangendo:

- detalhamento do ambiente de microinformática;
- verificação dos controles administrativos;
- validação dos controles de segurança física;
- avaliação dos controles de utilização de micro;
- verificação de controles de *back-up*;
- validação dos controles de manutenção dos equipamentos;
- avaliação do Plano de Contingência.

Finalmente, guardadas as características do ambiente de microinformática, as técnicas de auditoria em computador já apresentadas são aplicáveis e úteis à avaliação dos microcomputadores.

4.4.2 Auditoria em ambiente de teleprocessamento e de banco de dados

A tecnologia de teleprocessamento e de banco de dados necessária à operacionalização dessas técnicas junto aos sistemas aplicativos, bem como os controles necessários ao correto funcionamento de sistemas nesse ambiente TP/DB, deve ser do conhecimento dos auditores de sistemas.

As técnicas para auditar o uso da tecnologia TP/DB e de seus controles associados são aquelas já apresentadas.

O conceito de banco de dados implica a criação de um arquivo corporativo com todas as informações a serem tratadas pelos sistemas aplicativos da organização, com o conceito de unicidade do dado, ou seja, o código de chamada, o tamanho e as características de cada dado são únicos, e o dado está registrado em meio físico, disponível ao uso e acesso de qualquer usuário.

Na prática as organizações têm trabalhado com mais de um banco de dados no *mainframe* e vários bancos de dados disponíveis em micro.

Os seguintes aspectos são determinantes em um ambiente de banco de dados:

- existência da função administrador de dados que dará unicidade ao dado via a aprovação das características de cada dado a ser gravado no banco de dados corporativo;
- elaboração de um dicionário de dados, pelo administrador de dados, com o auxílio de *software* específico que tornará possível a criação do banco de dados a partir do dicionário de dados criado;
- existência de um SGBD-Software de Gerenciamento de Banco de Dados, o qual irá monitorar os acessos dos sistemas aplicativos aos bancos de dados;
- o SGBD é tratado pelo analista de banco de dados, o qual executará procedimentos de controle, de operacionalização e de treinamento de usuários na recuperação das informações contidas no SGBD;
- em nível de controle o banco de dados é guardado por tabelas de acesso, que administram *passwords* e seus correspondentes dados recuperados.

Em termos de comunicação de dados, o auditor defrontar-se-á com redes locais de computadores e redes utilizando tecnologia de comunicações estabelecendo o conceito de teleprocessamento.

A comunicação dos dispositivos de entrada e saída com a UCP, ou a comunicação entre UCPs, ou ainda de memórias auxiliares (discos) com a UCP caracterizam a modalidade processamento com o auxflio da tecnologia de comunicação de dados.

Quando a distância entre os equipamentos, que compõem a configuração da rede, é pequena, usam-se sinais digitais para transmissão de dados e somente um modem – modulador/demodulador – para reforçar o sinal.

Quando as distâncias são grandes, os sinais digitais do computador devem ser transformados em sinais analógicos – na codificação própria da área de comunicações – e, além do modem, são usadas unidades de controle de transmissão, que podem ser programadas para uma monitoração mais adequada da transmissão.

O meio da comunicação de dados será um cabo físico, quando de redes locais de comunicações, ou cabo físico, circuito de microondas, satélites, quando de redes de teleprocessamento (TP).

Para o perfeito funcionamento da comunicação de dados são utilizados:

a) arquivo *log* de comunicações, onde ficam registrados todos os blocos transmitidos correta e incorretamente para efeito estatístico e para tentativas de recuperação de dados transmitidas;

b) *software* de comunicação de dados para verificações do protocolo de transmissão, gravação do arquivo *log* de transações e para codificação e decodificação de sinais de comunicação;

c) protocolo de transmissões-registro, que garantem a recepção correta do bloco de informações transmitidos;

d) *software* ou *hardware* para a realização de cifragem e da decifragem de registros transmitidos.

A penetração nos sistemas de TP/DB é o ato de ganhar acesso não autorizado a dados, procedimentos ou recursos computacionais através de ações não autorizadas, tais como:

a) observação e extração de dados por entidade não autorizada. Esta tarefa não altera os dados armazenados, mas permite que sejam copiados por pessoas não autorizadas a tomarem conhecimento do conteúdo de determinados arquivos ou programas;

b) alteração de dados ou procedimentos de programas. Implica a modificação lógica do conteúdo de arquivos ou do funcionamento de programas;

c) adição é a inclusão de dados estranhos ao arquivo ou de rotinas estranhas aos programas;

d) utilização de equipamentos, de *software*, ou de ambos para a realização de um trabalho com o computador, sem o usuário estar aprovado para a execução da tarefa referida.

Como conseqüências das situações de insegurança referidas, os seguintes tipos de ameaça podem ocorrer:

a) acesso a dados não autorizados, ou seja, consulta/atualização em *real time* a arquivos de dados ou de programas;

b) execução/alteração não autorizada de programas, na modalidade RJE (Remote Job Entry) entrada de programas remota;

c) perda total ou parcial de transações durante uma transmissão (*batch* local; *batch* em teleprocessamento; *real time* local; *real time* em teleprocessamento). É utilizado o protocolo de transmissões para a certeza do sucesso, da correção e da integridade da mensagem transmitida;

d) distorções de dados durante a transmissão. Identificadas pelo *software* de comunicação de dados;

e) consulta de dados não atualizados quando o acesso é em *real time;*

f) erros na entrada (digitação) e conseqüente atualização de dados errados, particularmente no ambiente *real time*, quando não é feita crítica e consistência aos dados primários;

g) perda de arquivos/banco de dados em ambiente *on-line*, ou seja, por *scratch* de disco ou qualquer outro tipo de falha de *hardware* ou *software*.

Os principais controles no ambiente TP/DB a serem validados e avaliados pelo auditor de sistemas são:

a) Verificação de *password*:

- testar se o código de identificação digitado pelo usuário coincide com algum já cadastrado previamente (autoriza o acesso ao computador);
- teste geralmente realizado pelo *software* monitor de comunicação;
- o procedimento padrão é o usuário alterar sua *password* através de transação própria;
- existência de um arquivo de usuários autorizados.

b) Verificação de autorização de acesso aos dados:

- testar se o código de acesso digitado pelo usuário é compatível com a execução de transação (autoriza o acesso aos dados);
- teste efetuado pelo *software* de gerência de banco de dados ou pelo próprio sistema aplicativo;
- existência de uma tabela de autorização de acessos (código de acesso x dados).

c) Confirmação de digitação de dados (*read back*):

- solicitar a confirmação do dado recebido – consistência dos dados da transação – antes da efetivação da consulta ou modificação do banco de dados.

d) Verificação da integridade do banco de dados:

- balanceamento do banco de dados através de nova atualização, em *batch*, da cópia do banco de dados – gravada em um momento anterior; pelo arquivo *log* de transações do sistema – gerado durante o período entre a cópia do banco de dados e sua posição atual – com a criação do banco de dados atual e a confrontação deste banco de dados atual, gerado em *batch*, com o banco de dados atual, oriundo do processamento normal em *real time;*
- a verificação de integridade compreende a aplicação deste teste, periodicamente, com o acompanhamento de campos de valores e de quantidades de registros atualizados.

e) Verificação da última transação processada *versus* a última transação recuperada em um ambiente de banco de dados:

- implica o teste, após a queda de um banco de dados, que está sendo acessado em *real time*, dos procedimentos de recuperação e reinício (*recovery/restart*), para verificar se a última transação processada coincide com a última transação recuperada;
- corresponde à existência dos arquivos: *log* de transações; última transação processada; *back-up* do banco de dados;
- o procedimento implica o usuário comparar a última requisição de materiais, por ele digitada, com a transação gravada no arquivo, última transação processada. Este procedimento do usuário será efetuado após a recuperação do banco de dados feita por utilitários do SGBD ou feita pela rotina de recuperação de dados do arquivo *log* do CICS da IBM. Desta forma o usuário terá condições de começar a digitar a primeira transação, ainda não processada, evitando duplicidade de processamento.

f) Verificação de protocolos de arquivos:

- testar a validade das informações constantes nos registros *header* e *trailer* dos arquivos a serem transmitidos em *batch*;
- teste realizado pelos programas do sistema aplicativo;
- os protocolos de arquivos possuem informações para identificação do arquivo e teste da integridade lógica do mesmo (quantidades e valores).

g) Verificação de protocolos de linhas:

- testar a validade das informações constantes nos protocolos de linha de transmissão de dados;
- teste geralmente realizado pelo *software* monitor de comunicações ou por *hardware* (*firmware*);
- o protocolo de linha possui informações para identificação do posto e teste da integridade física do bloco de dados transmitido (testes horizontal e vertical).

h) Verificação da utilização de terminais:

- testar, periodicamente, se as transações executadas em cada terminal estão compatíveis com a utilização prevista;
- implica a emissão e análise de um relatório baseado no arquivo *log* de transações dos sistemas contendo as transações executadas em cada terminal, bem como as tentativas de acesso negadas;
- podem-se identificar tentativas de acesso ao arquivo "transações de compra de matéria-prima" por terminal/micro instalado na área de vendas.

Alguns procedimentos que minimizam a ocorrência de ameaças em ambiente TP/DB são:

a) Criação da função administrador de dados:

- define clara e formalmente as responsabilidades e autoridade da administração de dados, no tocante a:
  - descrição do banco de dados;
  - manutenção do dicionário de dados;
  - monitoramento da utilização do banco de dados;
  - controle de acessos e integridade de banco de dados.

b) Segurança física dos terminais:

- instalar nos locais onde se situam terminais/micro barreiras físicas que impeçam a sua utilização por pessoas não autorizadas.

c) Normas para o uso de *passwords*:

- estabelecer rotina formal para atribuição e cancelamento de *passwords*;
- estabelecer rotina formal para confirmação periódica do uso de *passwords*.

4.4.3 Auditoria da segurança física e ambiental do centro de computação

A auditoria dos recursos humanos e materiais e da infra-estrutura do ambiente computacional é o ambiente de atuação do auditor de sistemas, que trata de:

- infra-estrutura do centro de computação (sistema de alimentação elétrica, de ar condicionado, hidráulica, controle de condições ambientais, ergonomia, segurança contra fogo, inundação);
- problemática de acesso físico (*layout* do centro de computação, localização física);
- segurança da rede de comunicação de dados;
- segurança física de recursos humanos e materiais;
- plano de contingência em computação.

O auditor de sistemas irá usar as técnicas normais de auditoria de sistemas, tais como:

- questionários;
- entrevistas;
- visita *in loco*.

Entretanto, esse auditor deverá ter conhecimentos da dinâmica de funcionamento do centro de computação e de sua infra-estrutura necessária.

Alguns aspectos a serem validados pelo auditor de sistemas no tocante a segurança física e ambiental são:

I – *Sistema de alimentação elétrica*

As principais características para o seu bom funcionamento são:

a) Existência de *no break* para manter o processamento em ambiente *real time* por ocasião de queda de alimentação de força da fonte principal.

b) Acionamento de geradores para substituir a força principal desativada.

c) Operação dos estabilizadores para a manutenção da força em condições ideais para o funcionamento dos computadores (voltagem e ciclos).

d) Blindagem dos cabos de força para evitar água e ataque de predadores.

e) Calhas de suporte para manter os cabos de força acima do chão e protegidos.

f) Caixas de distribuição instaladas em locais seguros e fechadas.

g) Depósito de combustíveis para manter os geradores em funcionamento.

II – *Controle de condições ambientais*

a) Existência de piso elevado ou rebaixado para facilitar a circulação do ar condicionado e para correrem os cabos elétricos que interligam os equipamentos com os comandos de força.

b) Climatização do ambiente, em termos de:

- nível de poeira;
- temperatura ambiente;
- nível de umidade.

III – *Segurança contra fogo e outros riscos*

A prevenção contra incêndio consta de:

a) Sistema de detecção via sensores de fumaça e calor.

b) Manutenção permanente do sistema de detecção.

c) Treinamento de pessoal via formação de brigadas de incêndio.

d) Sistema de combate a incêndio automático ou manual e a água, CO_2 ou Halon.

IV – *Sistema de controle de acesso*

a) Sistemas não automáticos:

- porteiro ou recepcionista para administrar o acesso via identificação por carteira de identidade ou crachá.

b) Sistemas semi-automáticos:

- via interfones e porteiros eletrônicos que caracterizam:
  - a redução dos recursos empregados;
  - identificação via voz ou imagem do requerente ao acesso;
  - pode ser aplicado um circuito fechado de TV.

c) Sistemas automáticos:

- via teclados e equipamentos de identificação combinados a micro-computadores:
  - diminuição de recursos humanos;
  - usa cartões magnéticos e senhas;
  - identificação via voz, impressões digitais, geometria da mão, retina, assinatura.

V – *Localização de construção de um centro de computação*

Deve atender a requisitos tais como:

a) Evitar subsolos por causa de inundações.

b) Ser distante de locais de aglomerações e manifestações públicas.

c) Guardar distância de interferências eletromagnéticas, tais como antenas de TV; torres de microondas, de rádio; radar; linhas de metrô.

d) Evitar imediações de bombas de gasolina, garagens, fábricas ou depósitos de ácido, depósitos de inflamáveis e corrosivos, estacionamentos.

e) Não localizar o CPD nos últimos andares por causa da propagação de gases e fumaça.

f) A construção deve ser de concreto e alvenaria ou de aço e alvenaria.

g) Canos de água e esgoto não devem atravessar ambientes com equipamentos de computação.

h) As portas e paredes devem ser resistentes ao fogo e ir do chão ao teto.

i) Divisórias, pisos, acabamentos, tetos falsos, revestimentos acústicos devem ser de material resistente ao fogo.

VI – *Segurança dos recursos humanos pode ser vista como:*

a) Mecânica de recrutamento do pessoal técnico de PED.

b) Treinamento dos profissionais de PED em situações de insegurança no ambiente computacional.

c) Monitoração de situações agressivas ao ser humano como:

- necessidade de ter férias regulares;
- acompanhamento de doenças do trabalho como a *tenossinovite*.
- segregação de funções para evitar sobrecarga de trabalho;
- estabelecimento de uma política de técnicos substitutos para evitar interrupções na continuidade operacional do centro de computação.

d) Estabelecer um plano de greves para o centro de computação.

e) Criar a função analista de segurança em computação para o tratamento profissionalizado da segurança.

VII – *Segurança dos recursos materiais pode ser vista como:*

a) Armazenagem externa de dados:

- armazenar fitas de *back-up* em local físico distinto do CPD;
- limitar o acesso autorizado ao ambiente de *back-up*;
- realizar a reprodução periódica do *back-up* para evitar dificuldades em futuras leituras.

b) Transporte de meios magnéticos:

- realizado em dispositivos que evitem choque térmico, físico ou desmagnetização.

c) Aspectos gerais:

- cuidados com limpeza, guarda e manuseio de equipamentos e suprimentos de computação.

O momento principal da segurança em computação é a elaboração e manutenção de um plano de contingência, o qual é configurado pelos parâmetros:

a) Montar equipes para o enfrentamento de contingências, identificando pessoas envolvidas, nível de importância, função e responsabilidade de cada um.

b) Reduzir o impacto durante e após o desastre, através de definições claras e precisas das ações a serem tomadas.

c) Identificação da configuração de *hardware* de *back-up* necessária para processamento dos principais sistemas.

d) Criação do manual de contingências.

e) Testar periodicamente os esquemas de contingência.

Particularmente, é importante a auditoria dos trabalhos desenvolvidos pelo analista de segurança em computação, para que o auditor de sistemas, rapidamente, tenha compreensão do esquema de segurança em computação adotado e da qualidade de segurança vigente.

4.4.4 Auditoria da segurança lógica e da confidencialidade em computação

A segurança lógica diz respeito à modificação inadequada dos recursos tecnológicos, informações e *software*, e a confidencialidade diz respeito à captação indevida desses mesmos recursos tecnológicos. Para a manutenção da segurança lógica e da confidencialidade necessitamos validar e avaliar controles lógicos inseridos, bem como para proteger informações e programas.

Alguns desses controles lógicos são:

1. Programa de crítica e de consistência que, através de um conjunto de rotinas, são verificadas a integridade do dado e sua compatibilidade com as informações constantes do cadastro. Essas rotinas de controle lógico são:

   a) verificação de numeração/seqüência:

      - testar se a identificação (numeração) da transação e/ou lote foi processada e está na seqüência adequada;

   b) o dado só será aceito se houver dupla informação a seu respeito:

      - pagamento de uma compra de material só com pedido de compra mais nota de recebimento;

   c) formato dos dados:

      - valor do cheque só pode ser numérico;

   d) preenchimento dos dados nos campos:

      - campo código do material deve estar preenchido para – registro de requisição de materiais;

e) verificação de datas:
   - $1 \leq$ dia ≤ 31
   - $1 \leq$ mês ≤ 12

f) bidigitação de campos alfanuméricos:
   - confrontação de duas entradas distintas do mesmo dado para evitar erros em letras e símbolos especiais;

g) verificação de coerência:
   - verificar, entre si, a coerência dos campos que compõem um registro:
     – por exemplo, data de nascimento não pode ser maior que a data de contratação na empresa;

h) verificação de transações pendentes:
   - implica a criação e manutenção do arquivo de transações pendentes aguardando correção, ou de contas ou registros de pendências aguardando solução;

i) dígito de verificação:
   - aplicado a campos numéricos-chave com o objetivo de garantir a sua integridade;
   - implica a resolução de um algoritmo matemático aplicado aos dígitos significativos da chave com a geração do correspondente dígito de verificação que irá complementar essa mesma chave;

j) verificação de limites:
   - transação do caixa pequeno não pode ter campo de valor superior a determinada quantia;

l) verificação de totais de lote:
   - usando o esquema de que determinada quantidade de transações gera uma "capa de lote" e o somatório de capas de lote gera uma folha resumo que fecha determinado ciclo de processamento;

m) formulários pré-preenchidos:
   - evita a reprodução ou reescrita de dados fixos reduzindo erros de digitação;
   - um exemplo é o uso de caracteres magnéticos na pré-magnetização do cheque com o número da conta-corrente do cliente;

n) entrada por exceção:
   - o sistema assume no início do processamento certa condição ou valor e só a altera no caso de receber dado de entrada que indique condição ou valor diferente.

2. Nos programas de processamento é verificada a correção do funcionamento do sistema e a alimentação dos arquivos corretos. Alguns desses controles são:

   a) verificação da identificação dos arquivos:

      - testar a validade do registro *header*;

   b) verificação da integridade do arquivo:

      - testar o conteúdo do registro *trailer;*

   c) verificação de totais entre processamentos:

      - testar se os totais das saídas de um programa cruzam com os totais das entradas dos programas subseqüentes;
      - por exemplo: saldo anterior de duplicatas a receber mais novas duplicatas menos pagamentos é igual ao novo saldo de duplicatas a receber;

   d) verificação de estouro de campo:

      - testar se a quantidade de posições do resultado de operações aritméticas ou de movimentação de campos excedeu a quantidade de posições/tamanho do campo receptor;

   e) balanceamento entre arquivos analítico e sintético:

      - testar, periodicamente, a igualdade de totais de valores entre os arquivos analítico e sintético;
      - por exemplo: o total monetário apresentado pela conta de materiais na contabilidade não coincide com o apresentado pelo cadastro de materiais no controle de estoques;

   f) verificação de totais de fechamento dentro do ciclo de processamento:

      - implica a existência de um arquivo de informações de controle (AIC), que grava os totais dos arquivos gerados por dado programa e permite a existência de uma rotina de controle no programa subseqüente, para verificar se os totais dos arquivos lidos conferem com aqueles do AIC, que expressam esses mesmos arquivos de entrada, quando foram saída nos programas anteriores (vide Figura 2.2);

   g) sugestão automática para correção de erros:

      - emissão periódica de relatório que aponta dados errados no cadastro;

   h) apontar erros mantidos em processamento a *n* ciclos:

      - emissão de relatório, para uma área de controle geral, com erros mantidos em arquivos a vários ciclos de processamento.

3. Nos programas de saída são feitas verificações para evitar a passagem de informações erradas para os usuários. Alguns desses controles são:

   a) classificação de relatório quanto ao nível de sigilo:
      - elaborar normas que estabelecem, formalmente, o nível de sigilo de cada relatório emitido;

   b) destruição de relatórios sigilosos:
      - estabelecer normas de destruição de relatórios;

   c) fixação de horários e estabelecimento de protocolo de tramitação de relatórios:
      - teste do nível de atendimento ao usuário na tramitação de relatórios;

   d) tempo de resposta em terminal/micro:
      – verificar se o tempo decorrido entre a consulta e o recebimento da resposta no terminal atende às condições operacionais da área usuária.

A segurança lógica e a confidencialidade dos recursos tecnológicos devem ser institucionalizadas:

a) quando se der o desenvolvimento do sistema;
b) quando se der a tramitação, via canal de voz, ou manualmente, de programas e informações;
c) quando se der o funcionamento dos sistemas na produção.

4.4.5 Auditoria de plano diretor de informática (PDI)

O PDI constitui-se numa documentação que formaliza o planejamento estratégico de informática para uma organização seguindo os parâmetros:

- estabelece a filosofia de PED para a empresa;
- define os objetivos e a estrutura da área de informática;
- apresenta o plano de sistemas a serem desenvolvidos e mantidos;
- estabelece o dimensionamento e critérios para seleção e aquisição de *hardware* e de *sofware*;
- define as necessidades de recursos humanos;
- apresenta um orçamento de custos da área de informática;
- enumera os benefícios a serem alcançados e as restrições previstas.

A mecânica de atuação do auditor no PDI implica:

- discutir se os novos sistemas a serem desenvolvidos estão priorizados segundo a gravidade da fraqueza de controle interno identificada;
- acompanhar se os relatórios de auditoria serviram de base para a elaboração do PDI;
- analisar o item benefícios e restrições do PDI para verificar o atendimento às fraquezas de controle interno estabelecidas nos relatórios de auditoria;
- verificar a adequabilidade do plano de sistemas a serem desenvolvidos consoante as fraquezas dos relatórios de auditoria;
- avaliar o conteúdo do PDI e seu entrosamento com Plano Estratégico da Empresa, Plano Diretor Anual da Empresa e Plano Diretor Anual de Auditoria;
- acompanhar o cumprimento dos objetivos estabelecidos no PDI para os novos sistemas à medida que eles são desenvolvidos;
- analisar a metodologia aplicada e o conteúdo do PDI gerado;
- verificar se o PDI contemplou cenários discutindo alternativas para as novas políticas de informática a serem conduzidas;
- avaliar a qualidade dos levantamentos efetuados para a construção do PDI (questionários de diagnóstico estratégico, de diagnóstico organizacional e de diagnóstico operacional aplicado).

A Figura 4.14 estrutura a atuação da auditoria de PDI.

4.4.6 Uso do microcomputador na auditoria interna

Os momentos de uso do microcomputador na auditoria interna contemplam:

a) Micro aplicado aos processos de auditagem com sua utilização nas atividades técnico-operacionais de:
   - auditoria contábil-operacional;
   - auditoria em computador;

b) Micro aplicado, intrinsecamente, à auditoria interna com sua utilização nas atividades administrativo-operacionais:
   - em nível operacional;
   - em nível gerencial.

MOMENTO PC / PARÂ-METRO CONTROLE INTERNO	METODOLOGIA PDI	DOCUMENTO FINAL PDI	TÉCNICAS DE LEVANTAMENTO E ANÁLISE	DISCUSSÃO DE ALTERNATIVAS	INTEGRAÇÃO PDI COM DEMAIS PLANOS	NÍVEL CUMPRIMENTO PDI
SEGURANÇA						
EFICIÊNCIA						
EFICÁCIA						
PRODUTIVIDADE						

Figura 4.14. *Matriz determinação PC para auditoria PDI.*

As características da aplicação do micro nas atividades técnico-operacionais da auditoria interna são:

a) Na auditoria contábil-operacional:
   - realização de circularização;
   - apoio a inventários;
   - emissão de *check-lists* e questionários diversos de auditoria contábil-operacional;
   - tabulação de relatórios contábeis-financeiros;
   - tabulação de respostas a questionários aplicados em ambiente empresarial.

b) Na auditoria em computador:
   - análise de arquivos em computador;
   - confronto de arquivos em computador;
   - circularização a partir de arquivos em computador;
   - emissão de *check-lists* e questionários diversos de auditoria em computador;
   - preparação de arquivos simulados a serem submetidos a programas de computador;
   - análise de *log* de *mainframe* e de micro;
   - tabulação de respostas a questionários aplicados em ambiente computacional.

Aplicação do micro às atividades administrativo-operacionais da auditoria interna:

a) Acompanhamento de projetos de auditoria:
   - controle de horas;
   - controle de alocação de recursos.

b) Plano de treinamento/carreira do auditor interno:
   - cursos realizados;
   - tempo no cargo.

c) documentação automatizada dos papéis de trabalho e relatórios de auditoria.

d) Monitoração do cadastro de pontos de controle.

e) Monitoração do cadastro de indicadores de qualidade de auditoria.

f) Treinamento dos auditores internos na aplicação das técnicas de auditoria em computador.

g) Atuação com sistemas especialistas.

Quando o micro da auditoria estiver em rede com os demais micros da empresa, o auditor poderá executar a auditoria no micro do ambiente auditado e poderá transmitir os resultados da auditoria diretamente para o micro da auditoria. Na realidade, em momentos mais avançados, o auditor poderá a partir do micro em sua mesa de trabalho:

a) Acessar o *log* do micro sob auditoria. Tabular o conteúdo desse *log* e estabelecer critérios e condições para a realização da auditoria.

b) Solicitar arquivos, aplicar questionários e fazer boa parte da auditoria, via rede, recebendo os arquivos a serem analisados e as respostas aos questionários aplicados diretamente no micro da auditoria. Entretanto, por amostragem, determinadas confirmações deverão ser realizadas via presença física (visita *in loco* do auditor na área auditada).

4.4.7 Auditoria no ambiente de inteligência artificial

O ambiente de inteligência artificial em seu subconjunto sistemas especialistas influencia fortemente os trabalhos de auditoria de sistemas a partir da exacerbação de determinados conceitos e diretrizes de auditagem, assim, temos:

a) o momento principal da auditoria é no ambiente processos computacionais, em que, a partir da existência de novos conceitos de computação – banco de dados do conhecimento, *software* de inferência, *software* com as regras de decisão – o auditor terá de plotar pontos de controle que garantam a qualidade das decisões tomadas.

b) O aparecimento de duas novas funções – engenheiro do conhecimento (para estruturação dos sistemas especialistas e, principalmente, do *software* de inferência) e especialistas (para alimentação do banco de dados do conhecimento e criação das novas regras de decisão) –, bem como a possibilidade de o usuário atuar, também, como especialista ou alimentador primário das decisões tomadas ao sistema.

c) As constantes mudanças no modelo computacional do sistema especialista impõem que o desenvolvimento e o uso do sistema ocorram praticamente ao mesmo tempo.

Neste ambiente o auditor terá novos desafios como:

a) A extrema dificuldade na manutenção de uma documentação atualizada do sistema.

b) A constante mudança de objetivos no uso do sistema especialista, por parte do usuário.

c) O caráter extremamente interativo de manutenção e uso do sistema especialista.

4.5 CONSIDERAÇÕES BÁSICAS

Algumas técnicas de auditagem ganham realce, particularmente o *test-deck* (simulação de dados para identificar o nível de correção do sistema) e o SCARF (para captar consultas e decisões mais freqüentes, bem como aquelas pouco usuais ou alimentadas pela primeira vez).

O auditor deverá aprofundar seu nível de conhecimento de computação e, ainda, manter-se atualizado na evolução tecnológica de redes de computadores – *software* e *hardware* pertinentes e de banco de dados – características de distribuição de banco de dados com a problemática de controle de acesso às suas informações.

Outro ambiente determinante na atuação do auditor de sistemas na década de 90 será sua atuação com a tecnologia de inteligência artificial tanto a aplicada no ambiente auditado quanto a de uso intrínseco à própria auditoria interna.

RESUMO DO CAPÍTULO

A auditoria em computador é explicada em seus momentos de auditagem que são:

- auditoria do sistema em operação;
- auditoria do sistema em desenvolvimento;
- auditoria do centro de computação;
- momentos especiais da auditoria de sistemas.

A tecnologia computacional é discutida a cada um desses momentos e a aplicação das técnicas de auditoria de computador discutidas no Capítulo 3 é viabilizada.

Apresenta a abordagem mais avançada do binômio auditoria e computação com a discussão de:

- uso do micro na auditoria interna;
- auditoria de sistemas especialistas;

- auditoria em redes de computadores e banco de dados;
- auditoria da segurança em computação;
- auditoria de plano diretor de informática.

Além de todo o cenário atual de auditoria em computador apresentam-se, constantemente, pontos de controle a serem validados, sua forma no ambiente computacional e a tecnologia para sua verificação, validação e avaliação.

Os controles que cobrem o ambiente de computadores, tanto em nível físico quanto lógico, são intensamente discutidos.

Este capítulo consubstancia metodologias e mecânicas de auditagem numa constante apresentação de:

- problemática do ambiente computacional a cada cenário de auditagem discutido;
- etapas para a auditoria ser concretizada;
- pontos de controle pertinentes ao ambiente;
- técnicas de auditoria passíveis de serem empregadas.

QUESTÕES

1. Quais os momentos da auditoria de sistemas?
2. Identifique pontos de controle em cada um dos momentos da auditoria de sistemas.
3. Estabeleça três pontos de controle no momento da auditoria do sistema em operação caracterizando:
   - nome do ponto de controle;
   - parâmetro do controle interno a ser atendido;
   - técnica de auditoria a ser aplicada;
   - características da auditoria a ser efetuada.
4. Qual a utilidade do DFD para a determinação de pontos de controle?
5. Caracterize a participação do auditor no desenvolvimento de sistemas computadorizados.
6. O que é o ciclo de vida de um sistema computadorizado?
7. Discuta o ciclo de desenvolvimento de sistemas computadorizados.
8. Quais as fases do ciclo de operação normal do sistema computadorizado?

9. O que é PC-DS e PC-ON? Caracterize cada um em termos de processos e resultados computacionais.
10. Quais as técnicas de auditoria do ciclo de desenvolvimento de sistemas? Discorra sobre cada uma. Caracterize pontos de controle para cada uma.
11. Discuta a técnica BCSE – Base Case System Evaluation.
12. Discuta a técnica ITF – Integrated Test Facility.
13. Discuta a técnica SCARF – System Control Audit Review File.
14. Quais os momentos da auditoria do centro de computação?
15. Discuta a auditoria de contratos de *hardware* e *software*.
16. Discuta a auditoria da utilização de *hardware* e *software*.
17. Discuta a auditoria das funções de PED.
18. Discuta a auditoria de normas e procedimentos.
19. Discuta a auditoria de custos do centro de computação.
20. Que testes você faria em uma auditoria de centro de informações (CI)?
21. Que abordagem você usaria para auditar os micros em nível de seus usuários em cada uma das situações:
    - auditoria da infra-estrutura do micro;
    - auditoria do desenvolvimento de sistemas em micro pelos usuários;
    - auditoria do processamento dos sistemas em micro.
22. Que situações você consideraria para fazer auditoria de banco de dados?
23. Que situações você consideraria para fazer auditoria de redes de computadores?
24. Quais as ações não autorizadas de penetração nos sistemas TP/DB?
25. Quais são os principais controles do ambiente TP/DB?
26. Discorra sobre alguns procedimentos que minimizem a ocorrência de ameaças em ambiente TP/DB.
27. Qual é o ambiente de atuação da auditoria da segurança física e ambiental do centro de computação?
28. Que técnicas de auditoria serão usadas para validação da segurança física e ambiental?
29. Quais as principais características de um sistema de alimentação elétrica?
30. Quais as características do controle de condições ambientais?
31. Estabeleça a estrutura de um esquema de prevenção contra incêndio.
32. Quais as condicionantes de um sistema de controle de acesso?

33. Quais os requisitos para localização e construção de um centro de computação?
34. Sob que ótica pode ser vista a segurança dos recursos humanos?
35. Sob que ótica pode ser vista a segurança dos recursos materiais?
36. Por que devemos elaborar e manter um plano de contingência em computação?
37. Quais as rotinas de controle lógico na entrada dos sistemas, isto é, a nível do programa de crítica e consistência?
38. Quais os procedimentos de controle lógico nos programas de processamento?
39. Quais os momentos de controle lógico nos programas de saída dos sistemas?
40. Que parâmetros determinam o PDI?
41. O que implica a mecânica de atuação do auditor no PDI?
42. Discuta a aplicação do micro nas atividades técnico-operacionais da auditoria interna.
43. Discuta a aplicação do micro nas atividades administrativo-operacionais da auditoria interna.
44. Quais os conceitos e diretrizes realçados na auditoria do ambiente de inteligência artificial?
45. Que seqüência de etapas devem ser seguidas para a transformação do auditor interno em auditor de computador?

5

A Gestão da Auditoria de Sistemas

5.1 O AMBIENTE AUDITORIA INTERNA

A Figura 5.1 apresenta uma estrutura básica de um departamento de auditoria interna, na qual podemos identificar áreas de especialistas em:

- auditoria contábil;
- auditoria fiscal;
- auditoria operacional;
- auditoria de computação.

Entretanto, cada vez mais, todos os segmentos da auditoria atuam em ambientes computadorizados, principalmente em nível de microinformática e estes segmentos começam a valer-se dos microcomputadores para a realização de seus trabalhos.

Portanto, o enfoque da moderna auditoria interna contempla o treinamento de todos os auditores em auditoria de computação, ganhando maior especialização os auditores operacionais, à medida que ascendem na carreira de auditor, graças a treinamentos cada vez mais específicos e dirigidos em auditoria de computador.

Desta forma a Figura 5.2 resume o nível de treinamento em auditoria de computador agregado à carreira do auditor.

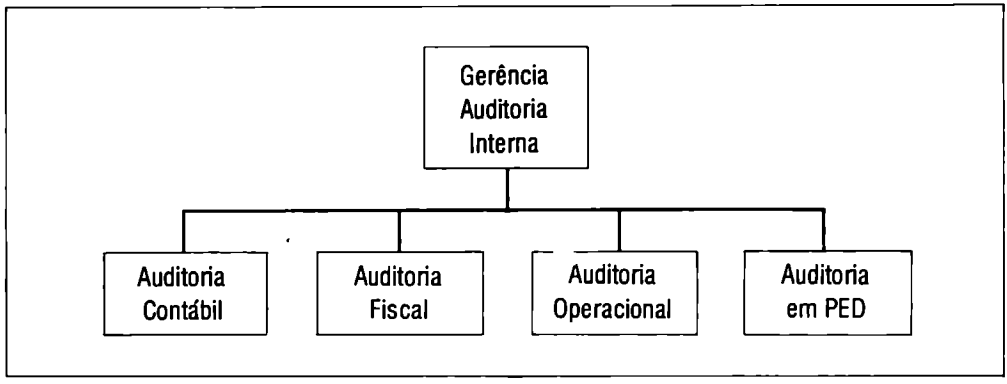


Figura 5.1. *Estrutura funcional da auditoria interna.*

CARGO	NÍVEL TREINAMENTO AUDITORIA EM PED
GERENTE	– Gerencia atividade de auditoria de sistemas.
SUBGERENTE	– Gerencia atividade de auditoria de sistemas.
SUPERVISOR	– Audita centro de computação, plano diretor de informática e sistemas especialistas.
AUDITOR SÊNIOR	– Audita sistemas em desenvolvimento e com tecnologia TP/DB. – Conhece metodologia de desenvolvimento. – Audita segurança em computação.
AUDITOR SEMI-SÊNIOR	– Realiza auditoria de sistemas em operação **mainframe.** – Conhece linguagem de programação **mainframe.**
AUDITOR JÚNIOR	– Realiza auditoria em microinformática. – Conhece uma linguagem de programação em micro/usa micro na auditoria.

Figura 5.2. *Treinamento em auditoria em PED na carreira do auditor interno.*

Uma das características da auditoria de sistemas vai ser a atuação junto aos trabalhos desenvolvidos por:

- analista de segurança em computação;
- analista de qualidade em computação;
- profissionais de segurança empresarial.

As atividades de gerenciamento da auditoria interna valer-se-ão, então, do microcomputador e poderão ser estruturadas em:

a) Atividades intrínsecas à área de auditoria interna:
   - planejamento e controle dos trabalhos/projetos de auditoria interna;
   - treinamento dos auditores internos;
   - administração da qualidade dos trabalhos de auditoria interna:
     - absenteísmo;
     - revisão de papéis de trabalho;
     - análise de risco dos pontos de controle sensíveis;
     - elaboração de relatórios de auditoria a cada projeto;
     - controle de relacionamento auditor *versus* auditado;
   - elaboração plano diretor anual de auditoria interna.

b) Atividades extrínsecas à auditoria interna:
   - coordenação do comitê de auditoria interna;
   - visita/contatos com os executivos/chefes das áreas auditadas para abertura de projetos/trabalhos;
   - participação nas reuniões de apresentação e discussão de relatórios de auditoria com os auditados;
   - apresentação do plano diretor anual de auditoria e do relatório anual das atividades de auditoria à empresa, com os indicadores de qualidade de auditoria pretendidos e aqueles alcançados;
   - discussão do orçamento do departamento de auditoria interna.

Para a integração da auditoria interna com a alta administração há a necessidade da criação de um Comitê de Auditoria, o qual, composto pelo executivo principal e demais componentes da diretoria da organização, receberá informações e orientará a atuação da auditoria interna no sentido de alcançar os objetivos desejados.

5.2 GERENCIAMENTO DA AUDITORIA INTERNA

O planejamento e o controle das atividades de auditoria é o papel principal a ser desempenhado pelo gerente de auditoria interna, portanto, dois documentos são de sua exclusiva responsabilidade:

a) plano diretor de auditoria de sistemas;

b) relatório anual das atividades de auditoria de sistemas.

O plano diretor de auditoria de sistemas consubstancia as atividades, o cumprimento às diretrizes da alta administração, os momentos de atuação, os projetos de auditoria de sistemas a serem executados, segundo a seguinte estrutura:

a) Estabelecimento dos indicadores de qualidade de auditoria de sistemas e correspondentes métricas a serem aplicadas.

b) Deve ser estruturado em capítulos com um conteúdo mínimo de:
   - objetivos;
   - indicadores de qualidade (IQ) da auditoria de sistemas;
   - recursos necessários aos trabalhos de auditoria;
   - treinamento preconizado para os auditores;
   - custos a serem incorridos;
   - cronograma de atividades a cada projeto;
   - suporte à auditoria operacional a ser dado pela auditoria de sistemas;
   - relação dos trabalhos pertinentes à auditoria de sistemas.

O relatório anual das atividades de auditoria de sistemas resume o controle exercido pelo gerente de auditoria sobre as atividades de auditoria de sistemas e deve ter a seguinte estrutura básica:

1. *Introdução*

   - descrição dos objetivos propostos no plano diretor anual de auditoria de sistemas;
   - detalhamento das mudanças de objetivos porventura ocorridas.

2. *Indicadores de qualidade da auditoria de sistemas*

   - caracterização dos indicadores de qualidade (IQ) usados;
   - quadros dos IQ e suas correspondentes métricas;
   - estatísticas quanto à evolução das métricas dos IQ alcançados;
   - comentários quanto aos IQ, singelamente, no ano e em relação aos anos anteriores.

3. *Observações quanto ao ano em termos de auditoria de sistemas*

- comentários quanto à atuação da auditoria de sistemas em termos de:
  - situações delicadas enfrentadas;
  - parâmetros do ano que nortearão a auditoria de sistemas no próximo ano;
  - dificuldades intrínsecas à auditoria de sistemas ocorridas.

Ambos os relatórios serão apresentados e debatidos pelo gerente de auditoria com o comitê de informática, sustentados ou embasados pelos produtos finais gerados ao término de cada projeto de auditoria:

- relatório de fraquezas de controle interno;
- relatório de redução de custos;
- certificado de controle interno.

Portanto, para a avaliação do desempenho das atividades de auditoria de sistemas, o gerente de auditoria irá valer-se de:

- acompanhamento de cada projeto de auditoria executado, em face da sua participação no comitê de auditoria;
- análise do conteúdo, conclusões e recomendações, principalmente, dos relatórios de fraquezas de controle interno;
- administração dos projetos de auditoria de sistemas via o uso do *software* SISPC–Sistema de Administração de Pontos de Controle;
- monitoração da qualidade dos trabalhos de auditoria de sistemas, via indicadores de qualidade (IQ).

5.3 INDICADORES DE QUALIDADE (IQ) DA AUDITORIA DE SISTEMAS

Objetivos dos IQ de auditoria de sistemas:

a) Atendem ao planejamento e ao controle da auditoria de sistemas.

b) São criados principalmente com base na análise e tabulação dos pontos de controle (PC) auditados.

c) Servem de referência para a organização da qualidade dos trabalhos de auditoria de sistemas realizados.

d) São estabelecidos segundo o consumidor final que se identifica como alta administração/gerente de auditoria.

e) Permitem a administração por exceção.

f) Atendem aos parâmetros do controle interno.

Por conseguinte, a avaliação da qualidade dos trabalhos da auditoria de sistemas permite caracterizar:

a) Produtividade dos trabalhos efetuados.

b) Eficiência dos processos de auditagem (uso de técnicas mais otimizadas de auditoria).

c) Eficácia dos resultados das auditorias de sistemas efetuadas (alcance dos objetivos estabelecidos).

d) Segurança dos recursos tangíveis e intangíveis alocados a processos e resultados.

Um exemplo de IQ da auditoria de sistemas é:

$$\text{QPCHR} = \frac{\text{Quantidade de horas auditoria sistemas}}{\text{Quantidade PC validados}}$$

O QPCHR é a quantidade média de horas de auditoria aplicadas por ponto de controle no ano.

Para a apuração desse IQ necessitamos tabular todas as horas gastas de auditagem em todos os PC validados em determinado ano.

Portanto, é necessária a existência de um *software* SISPC que faça tabulações, a cada projeto de auditoria de sistemas, dos pontos de controle considerados.

O *software* de administração dos PC atua segundo os seguintes fatores municipais:

- tempo disponível para realização da auditoria;
- análise de risco com o inventário e eleição dos pontos de controle a serem validados;
- técnicas mais adequadas a serem aplicadas a cada ponto de controle;
- evidências de auditoria obtidas das validações efetuadas;
- natureza das fraquezas de controle interno obtidas dos pontos de controle validados;
- tipo de alternativas de solução propostas para correção das fraquezas de controle interno identificadas;
- relação custo/benefício da atuação da auditoria interna.

A integração do SISPC com a mecânica de acompanhamento da qualidade da auditoria de sistemas é imediata e natural, tendo em vista que o SISPC é o acompanhamento analítico dos trabalhos de auditagem de cada PC e que o acompanhamento via IQ é a atuação em nível sintético ou macro efetuada pelo gerente de auditoria, via *software* SISQA-IQ – Sistema de Qualidade da Auditoria via Indicadores de Qualidade.

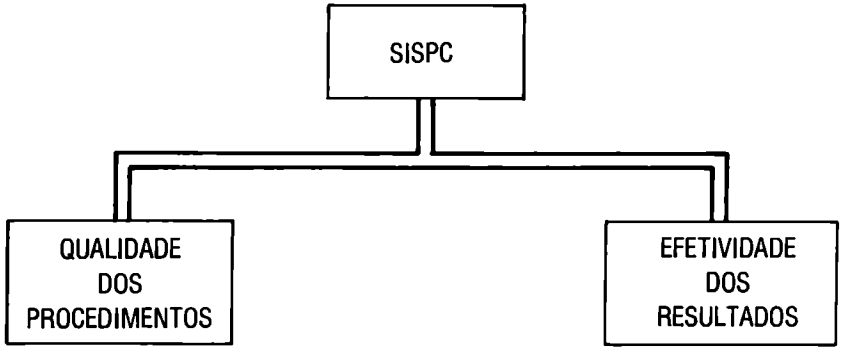
É importante lembrar que o PC é a unidade de auditagem correspondendo à base para a institucionalização de todo um processo de administração da auditoria de sistemas e que o IQ é a base de todo o processo de direção realizado pelos executivos, já que quantifica fatos empresariais de seu interesse e assegura tratamento matemático, como suporte ao processo decisório.

5.4 SISPC – SISTEMA DE ADMINISTRAÇÃO DE PONTOS DE CONTROLE

A monitoração dos pontos de controle é atividade primordial para o planejamento e o controle da auditoria de sistemas. Para fazer frente a esta situação consideramos útil a criação de um cadastro de pontos de controle e sua correspondente tabulação, com os objetivos de:

- melhorar a qualidade dos procedimentos de auditagem;
- obter maior efetividade dos resultados da auditoria.

A estrutura do SISPC compreende os seguintes vetores de atuação:



A qualidade dos procedimentos busca identificar:

a) técnica de auditoria em computador aplicada a cada ponto de controle auditado;

b) parâmetro do controle interno segundo o qual o ponto de controle foi validado;

c) procedimentos de auditoria em computador adotados.

A efetividade dos resultados torna-se expressa via a classificação das fraquezas de auditoria interna identificadas em termos de:

a) erros de procedimentos ou resultados;
b) omissão de procedimentos;
c) duplicidade de procedimentos;
d) falta de procedimentos ou de resultados;
e) fraude em procedimentos ou em resultados.

O tratamento estatístico dos pontos de controle irá permitir a correlação entre:

I – técnicas aplicadas e natureza da fraqueza identificada;
II – parâmetro do controle interno e correspondente técnica de auditoria mais adequada;
III – fraqueza identificada e tipo do parâmetro do controle interno.

O *software* SISPC poderá trabalhar em conjunto com o *software* de administração de projetos estabelecendo:

I – natureza do técnico *versus* técnica de auditoria em computador aplicada;
II – quantidade de horas gastas no ponto de controle e o parâmetro de controle interno atendido;
III – quantidade de horas gastas e a natureza da fraqueza identificada.

Os correlacionamentos são inúmeros e permitem análises da atuação da auditoria de sistemas ocorrida para a obtenção de melhorias nos futuros projetos a realizar.

RESUMO DO CAPÍTULO

Discussão da problemática de gerenciamento da auditoria interna e da auditoria de sistemas segundo os tópicos:

- o ambiente auditoria interna;
- o gerenciamento da auditoria interna/auditoria de sistemas;
- indicadores de qualidade da auditoria de sistemas.

Dá ênfase ao aspecto de que todo auditor interno deve ser um auditor de sistemas, estabelecendo a fusão da área de auditoria operacional com a área de auditoria de sistemas.

Apresenta a mecânica de gerenciamento da auditoria, particularmente, em seus momentos planejamento e controle via os documentos:

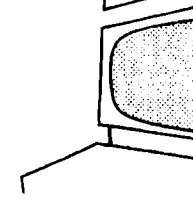
- plano diretor de auditoria de sistemas;
- relatório anual das atividades de auditoria de sistemas.

Finalmente, reforça o conceito de ponto de controle, construindo a administração da auditoria de sistemas em cima dos conceitos de ponto de controle e indicador de qualidade.

QUESTÕES

1. Estabeleça uma estrutura de departamento de auditoria interna.
2. Que tipo de treinamento em auditoria em PED você daria aos vários cargos de auditoria?
3. Estruture as atividades de gerenciamento da auditoria interna.
4. Qual o papel do comitê de auditoria no planejamento e controle das atividades de auditoria de sistemas?
5. Descreva o conteúdo de um plano diretor de auditoria de sistemas.
6. Descreva o conteúdo do relatório anual das atividades de auditoria de sistemas.
7. Com que base o gerente de auditoria avalia o desempenho das atividades de auditoria de sistemas?
8. Quais os produtos finais, gerados ao término de cada projeto de auditoria, que permitem a elaboração dos relatórios de planejamento e controle para gerenciamento da auditoria de sistemas?
9. Quais os objetivos dos IQ de auditoria de sistemas?
10. O que permite caracterizar a avaliação da qualidade dos trabalhos de auditoria de sistemas?
11. Quais os fatores principais do *software* de administração de PC?
12. Por que é importante a integração do *software* de administração de PC com o acompanhamento da qualidade da auditoria de sistemas?

6 Questionários e Documentação de Auditoria em Computador



Apresentamos a seguir alguns questionários e documentos/relatórios/papéis de trabalho de interesse do auditor de sistemas, tanto para agilizar quanto para registrar sua atuação.

Na realidade, esses questionários e a documentação apresentada servem como base para a obtenção, pelos profissionais de auditoria em computador, de uma estrutura básica de atuação consoante suas necessidades técnicas, momento histórico e ambiente organizacional.

Os questionários estão apresentados, segundo a estrutura clássica, para as respostas SIM (S), NÃO (N), NÃO APLICADO (N/A) e dividem-se nos grupos:

a) sistemas aplicativos *batch* em operação;
b) sistemas aplicativos *batch* em desenvolvimento;
c) sistemas aplicativos *on-line* em operação;
d) sistemas aplicativos *on-line* em desenvolvimento;
e) centro de computação;
f) microinformática no ambiente usuário;
g) plano diretor de informática;
h) ambiente banco de dados;
i) segurança física e ambiental;
j) segurança lógica e confidencialidade;
l) ambiente auditoria interna.

Na estrutura dos questionários agregamos ainda as colunas:

I – *Comentários*

- para o detalhamento da resposta do auditado, bem como adequação ou esclarecimento da forma como a questão foi colocada ou sua aderência ao momento histórico/ambiente sob auditoria.

II – *Referência, documentação e auditoria*

- para identificação do formulário/papel de trabalho/ pasta de auditoria/relatório de auditoria depositário ou interessado na questão proposta.

A documentação de auditoria em computador compreende a estrutura e o conteúdo dos seguintes formulários:

I – *Memorandos administrativos*

- memorando de abertura do projeto de auditoria em computador;
- memorando com o planejamento do projeto de auditoria – cronograma; discriminação de recursos necessários; determinação de datas fatais; estabelecimento de reuniões;
- memorando estabelecendo a passagem da auditoria de posição para a auditoria de acompanhamento, ou seja, a determinação dos pontos de auditoria em face da identificação de fraquezas nos pontos de controle auditados;
- memorando de cobrança ou aceitação da institucionalização de uma solução para a fraqueza existente, tornando o ponto de auditoria novamente em ponto de controle;
- atas de reuniões realizadas – de trabalho; de término de fase de auditoria; final de conclusão do projeto de auditoria de posição ou de auditoria de acompanhamento.

II – *Relatórios/papéis de trabalho técnico-operacionais*

- guia de auditoria;
- certificado de controle interno (vide página 60):
- relatório de redução de custos;
- relatório de fraquezas de controle interno;
- inventário e eleição de pontos de controle.

A seguir detalhamos o conteúdo de alguns questionários e da estrutura da documentação pertinente à auditoria de sistemas computadorizados.

ATA DE REUNIÃO
Nº /ANO

Projeto: _____

Data Realização: _____

Participantes: _____

_____

_____

Objetivos da Reunião: _____

_____

_____

Breve Descrição: _____

_____

_____

_____

_____

Conclusões alcançadas: _____

_____

_____

_____

_____

Assinatura

Auditor _____

Relator

PLANEJAMENTO PROJETO DE AUDITORIA

Nome Projeto: _____ Código: _____

Equipe Projeto: _____

_____

_____

Data início: ___/___/___ *Data fim:* ___/___/___

Datas Fatais: ___/___/___ Término de Levantamentos

___/___/___ Eleição de Pontos de Controle

___/___/___ Término de Validação PC's

___/___/___ Emissão Relatório Auditoria

Comitê Auditoria: _____

(composição) _____

_____

_____

_____

Datas Reuniões ___/___/___

Comitê Auditoria: ___/___/___

(assunto) ___/___/___

___/___/___

___/___/___

Objetivos macro do projeto: _____

_____

_____

Observação: em anexo cronograma detalhado

auditor coordenador: _____ Data: ___/___/___

Data		Página
Visto	Sistema Descrição: Inventário e eleição dos pontos de controle	

Inventário nº	
SEQ.	
PONTO DE CONTROLE	
PRIORIDADE E DATA DE ELEIÇÃO	
DESCRIÇÃO	
OBJETIVOS	
PARÂM. CI MAIS AFETADO	
TÉCNICAS DE AUDITORIA	

Data		Página
Visto	Sistema Descrição: Cronograma de atividades	

REF.	DESCRIÇÃO	NOME	SIT.																					
			PREV.										DATA DE APROVAÇÃO / /	APROVADO POR
			REAL											
			PREV.										DATA DE ELABORAÇÃO / /	ELABORADO POR
			REAL											
			PREV.										DATA	INICIAL
			REAL											FINAL
			PREV.											
			REAL											
			PREV.											
			REAL											
			PREV.											
			REAL											
			PREV.											
			REAL											
			PREV.											
			REAL											
			PREV.											
			REAL											
			PREV.											
			REAL											

QUESTIONÁRIO

SISTEMAS APLICATIVOS *BATCH* EM OPERAÇÃO

Questão	Sim Não N/A	Comentários	Referência Documentação Auditoria
1. Há padrão de documentação para os sistemas *batch*?			
2. Está sendo usado o padrão de documentação?			
3. Estão descritos fluxos do sistema com a tecnologia (DFD) e o fluxo de serviços está registrado?			
4. Há *softwares* de apoio à documentação de sistemas?			
5. Existe trilha de auditoria no sistema?			
6. Existem arquivos/relatórios/registros de controle no sistema?			
7. Há totais de controle no sistema?			
8. Há um inventário atualizado dos arquivos usados pelo sistema?			
9. Existe fitoteca de *back-up*?			
10. Na fitoteca de *back-up* estão os arquivos-tabelas de programas e de transações sensíveis?			
11. As alterações de programas são controladas e registradas?			
12. Existe Ordem de Produção para alimentação dos *jobs* e para movimentação dos arquivos com a fitoteca?			

QUESTIONÁRIO

SISTEMAS APLICATIVOS *BATCH* EM OPERAÇÃO

Questão	Sim Não N/A	Comentários	Referência Documentação Auditoria
13. Existe grau de sigilo de arquivos e programas consoante norma estabelecida?			
14. Existe duplicata da documentação do sistema?			
15. Existem procedimentos documentados descrevendo como os dados-fonte são entregues e alimentados ao computador, bem como os relatórios de saída são gerados e entregues aos usuários?			
16. Há segregação de funções entre as atividades de operação e de controle na produção do sistema aplicativo?			
17. Há monitoração, via arquivos/totais de controle entre fases/ciclos de processamento do sistema?			
18. Há segregação de funções na catalogação/operação dos programas do sistema em relação à equipe de desenvolvimento/manutenção do sistema aplicativo?			

QUESTIONÁRIO

SISTEMAS APLICATIVOS *BATCH* EM DESENVOLVIMENTO

Questão	Sim Não N/A	Comentários	Referência Documentação Auditoria
1. Existe uma metodologia de desenvolvimento de sistemas?			
2. A metodologia está sendo aplicada?			
3. São usados os conceitos de análise e programação estruturada na metodologia?			
4. O usuário é o coordenador do projeto de desenvolvimento de sistemas?			
5. Existe a atividade administração de projetos no desenvolvimento de sistemas?			
6. É feito *walk-through* pela administração de projetos no desenvolvimento de sistemas?			
7. Existe *time sheet* para controle do trabalho de analistas e programadores?			
8. Há a atuação do analista de segurança em computação no desenvolvimento de sistemas?			
9. Há a atuação do analista de qualidade em computação no desenvolvimento de sistemas?			
10. Foi incluído arquivo de auditoria (SCARF) no novo sistema?			
11. O novo sistema foi aprovado pelos usuários?			
12. Existe um sistema de *quality assurance* e de controle de qualidade do desenvolvimento de sistemas acompanhando análise e programação?			

QUESTIONÁRIO

SISTEMAS APLICATIVOS *BATCH* EM DESENVOLVIMENTO

Questão	Sim Não N/A	Comentários	Referência Documentação Auditoria
13. Foi feito paralelo para implantação do sistema?			
14. Existe um arquivo-tabela para monitoração dos parâmetros utilizados pelo novo sistema?			
15. Foi estabelecido um esquema de *back-up* para os arquivos vitais do sistema?			
16. A catalogação do sistema foi feita pelo pessoal da produção?			
17. Foi utilizada a técnica de prototipagem para o desenvolvimento do sistema?			
18. Foi providenciada uma empresa *dummy* para os registros de auditoria a serem inseridos, quando do processamento normal do sistema (técnica ITF – *Integrated Test Facility*)?			
19. Foi feito um teste geral do sistema?			
20. O sistema foi formalmente aceito pelo usuário?			
21. O sistema foi desenvolvido em módulos de forma a facilitar a aplicação do conceito de segregação de funções?			
22. O sistema utiliza a tecnologia de microfilmagem?			
23. Os usuários e profissionais da produção foram adequadamente treinados para usar/operar o sistema?			

QUESTIONÁRIO

SISTEMAS APLICATIVOS *ON-LINE* EM OPERAÇÃO

Questão	Sim Não N/A	Comentários	Referência Documentação Auditoria
1. O *log* de comunicações é verificado, regularmente, pela área de produção ou de suporte técnico para evidenciar a qualidade do uso do sistema?			
2. A área de telecomunicações monitora, regularmente, via mesa de TP, as condições do canal de comunicações e realiza estatísticas quanto ao uso do sistema pelos usuários?			
3. O esquema de substituição de *passwords* vem sendo cumprido quanto ao aplicativo?			
4. Os terminais utilizados para interagir com os aplicativos encontram-se em bom estado de conservação?			
5. Os *log's* de comunicações foram guardados por tempo adequado que permita ao auditor validar os ciclos de processamento desejados?			
6. É adequada a segurança física e lógica dos terminais de entrada de dados no aplicativo?			
7. Os procedimentos padronizados para assinalar os terminais são cumpridos?			

QUESTIONÁRIO

SISTEMAS APLICATIVOS *ON-LINE* EM OPERAÇÃO

Questão	Sim Não N/A	Comentários	Referência Documentação Auditoria
8. A topologia da rede e os procedimentos para seu uso pelo aplicativo estão documentados? 9. O conteúdo do protocolo de comunicações permite a integridade da mensagem transmitida/recebida? 10. São mantidos *log's* nos terminais com totais de controle ou de transações?			

QUESTIONÁRIO

SISTEMAS APLICATIVOS *ON-LINE* EM DESENVOLVIMENTO

Questão	Sim Não N/A	Comentários	Referência Documentação Auditoria
1. O Manual do Usuário descreve telas incluindo conteúdo e seu uso?			
2. O Manual do Sistema estabelece os procedimentos em nível terminal/micro interface com o *mainframe*?			
3. Existe submissão de programas remota (RSE) no aplicativo?			
4. Existe discussão da relação custo/benefício do desenvolvimento do aplicativo em ambiente *on-line* em substituição ao ambiente *batch*?			
5. Existe ambiente de teste separado do ambiente de produção para submissão *on-line* de alterações de programas?			
6. É utilizada alguma técnica de controle (*mapping*, por exemplo) para identificar rotinas de programas aplicativos desativadas?			
7. Em ambiente conexão micro/*mainframe*, os usuários conhecem uma linguagem de programação para desenvolvimento de programas no computador central?			
8. O desenvolvimento do sistema atendeu às normas de acesso lógico ao aplicativo?			

QUESTIONÁRIO

SISTEMAS APLICATIVOS *ON-LINE* EM DESENVOLVIMENTO

Questão	Sim Não N/A	Comentários	Referência Documentação Auditoria
9. Foi utilizado no aplicativo o conceito de segregação de funções *on-line* via o casamento de duas ou mais *passwords* para a realização de alterações em arquivos-tabelas e rotinas sensíveis dos programas? 10. Foram estabelecidos arquivos estatísticos de acesso de *passwords* a registros sensíveis? 11. Existem *softwares* para facilitar o desenvolvimento de sistemas *on-line*? 12. A produtividade do desenvolvimento de sistemas *on-line* é mensurada?			

QUESTIONÁRIO

CENTRO DE COMPUTAÇÃO

Questão	Sim Não N/A	Comentários	Referência Documentação Auditoria
1. O posicionamento do Centro de Computação na Organização é adequado?			
2. A estrutura interna do Centro de Computação é adequada?			
3. Existe um sistema formal de apuração de custos em computação?			
4. Há normas técnico-operacionais e administrativo-operacionais em vigor e sendo aplicadas no Centro de Computação?			
5. Os contratos de *hardware* e de *software* são aprovados pelo Departamento Jurídico?			
6. A eficácia dos sistemas é, periodicamente, medida pelo Centro de Computação?			
7. Há uma definição de cargos e funções no Centro de Computação? Está sendo aplicada?			
8. Existe orçamento no Centro de Computação?			
9. Existe a atividade de planejamento de capacidade?			
10. São utilizados os conceitos de Coordenação de Problemas e de Coordenação de Mudanças?			
11. Existe Manual de Procedimentos e de Descrição das Áreas de Atividades, Coordenação de Problemas e de Mudanças?			

QUESTIONÁRIO
CENTRO DE COMPUTAÇÃO

Questão	Sim Não N/A	Comentários	Referência Documentação Auditoria
12. Existe estatística da efetividade das mudanças efetuadas?			
13. Há banco de dados registrando problemas e mudanças?			
14. Existe uma sistemática institucionalizada de identificação/captação de problemas e o correspondente alcance de soluções com as conseqüentes mudanças realizadas?			
15. É boa a imagem do Centro de Computação perante a empresa?			
16. É dado tratamento ao *Log/Accounting* do Sistema para efeito de apuração da eficiência no uso dos recursos computacionais (*hardware* e *software*)?			
17. O orçamento do Centro de Computação está engrenado com a dinâmica de orçamento empresarial?			
18. É adequada a divisão de responsabilidades estabelecida na estrutura orgânica do CPD?			
19. Existe um plano de treinamento formal para a área de computação? É cumprido?			
20. O salário de computação está em níveis competitivos com o mercado?			

QUESTIONÁRIO
CENTRO DE COMPUTAÇÃO

Questão	Sim Não N/A	Comentários	Referência Documentação Auditoria
21. Existe um plano de carreira formal para os profissionais de computação?			
22. Existem contratos formais para manutenção de *hardware* e de *software*?			
23. Existe compatibilidade entre os programas catalogados na biblioteca de programas e aqueles registrados no *Log/Accounting* do Sistema?			
24. São efetivos os controles existentes no almoxarifado de suprimentos de computação?			
25. Os controles na área de microfilmagem permitem a manutenção da confidencialidade de dados e programas?			
26. A configuração do equipamento está adequadamente balanceada?			
27. Existem formulários impressos pelo computador negociáveis? São adequados os controles sobre eles?			
28. Há utilização de serviços de terceiros pelo Centro de Computação?			
29. É satisfatório o atendimento dos prestadores de serviços em computação?			

QUESTIONÁRIO

MICROINFORMÁTICA NO AMBIENTE USUÁRIO

Questão	Sim Não N/A	Comentários	Referência Documentação Auditoria
1. O microcomputador é usado, estritamente, para os negócios da empresa?			
2. O Centro de Informações (CI) está adequadamente colocado na estrutura orgânica do Centro de Computação?			
3. A quantidade de profissionais do Centro de Informações é adequada?			
4. Existem programas "piratas" sendo usados na empresa?			
5. O CI está preparado para enfrentar "vírus" em programas de microcomputador?			
6. O CI só treina e dá apoio aos usuários ou desenvolve programas em micro também?			
7. O CI/Suporte Técnico está preparado para enfrentar os *hackers*?			
8. Há normas com esquemas de *back-up* no ambiente de microinformática?			
9. Os contratos de *hardware/software* em termos de aquisição, *leasing*, aluguel, manutenção estão conforme as normas empresariais?			
10. Existe um inventário atualizado de *hardware* e *software* no ambiente de microinformática administrado pelo CI?			

QUESTIONÁRIO

MICROINFORMÁTICA NO AMBIENTE USUÁRIO

Questão	Sim Não N/A	Comentários	Referência Documentação Auditoria
11. Existe um banco de dados para intercâmbio de *softwares* em micro entre as diversas áreas usuárias de micro na organização?			
12. A quantidade de micros, no CI, disponíveis para treinamento do usuário é suficiente?			
13. Os micros são usados, somente, como planilha eletrônica e editor de texto?			
14. Os micros estão conectados em rede?			
15. O microcomputador aumentou a produtividade da área usuária?			
16. Os micros possuem chaves de segurança para administrar seu uso por profissionais indevidos?			
17. Existe *log* para monitoração do uso do micro ou há folha de registro de utilização?			
18. Existe programa formal de treinamento dos usuários de micro?			
19. O CI administra o uso dos micros, via tabulação semanal de seus *log's*?			
20. Há capacidade ociosa nos micros?			
21. Existe norma recomendando uma documentação padronizada para programas/sistemas desenvolvidos em micros?			

QUESTIONÁRIO

PLANO DIRETOR DE INFORMÁTICA

Questão	Sim Não N/A	Comentários	Referência Documentação Auditoria
1. Existe um Comitê de Informática?			
2. O PDI está entrosado com o Plano Diretor Anual da empresa e com seu Plano Estratégico?			
3. No PDI está justificada a prioridade de desenvolvimento de novos sistemas?			
4. No PDI está definida a estratégia de informática da empresa, particularmente, no tocante à centralização e à descentralização do processamento?			
5. Estão estabelecidos no PDI os objetivos a serem atingidos e a relação custo/benefício pretendida?			
6. Foram definidos os níveis de produtividade desejados?			
7. O Plano de Contingência atende às diretrizes do PDI?			
8. Os Relatórios de Auditoria foram considerados quando da elaboração do PDI?			
9. O PDI define o nível tecnológico de computação desejado para a empresa?			

QUESTIONÁRIO

AMBIENTE BANCO DE DADOS

Questão	Sim Não N/A	Comentários	Referência Documentação Auditoria
1. Existe *software* de controle de acesso aos bancos de dados corporativos?			
2. É cumprida a norma que caracteriza os procedimentos de *recovery/restart* do processamento *on-line/real time* em banco de dados?			
3. Existe a função administrador de dados?			
4. O banco de dados usa o conceito de segmento de controle para monitoração do processamento realizado?			
5. Existe *software* para gerenciamento do banco de dados?			
6. O dicionário de dados é automatizado?			
7. A atividade normalização de dados está sendo realizada adequadamente?			
8. Os usuários trabalham com linguagem de consulta ao banco de dados corporativo?			
9. O *log* do Banco de Dados é analisado pelo analista de segurança em computação?			
10. É feito diariamente *back-up* do banco de dados e do *log* de transações?			
11. Estão sendo cumpridas as normas para funcionamento da área de Administração de Dados?			

QUESTIONÁRIO
AMBIENTE BANCO DE DADOS

Questão	Sim Não N/A	Comentários	Referência Documentação Auditoria
12. É elaborado o diagrama de estrutura de dados quando do desenvolvimento de sistemas com banco de dados?			
13. Foi fornecida/ensinada aos usuários uma linguagem de trabalho com banco de dados em microcomputador?			
14. Existe *software* instalado no CPD para transferência de banco de dados na conexão micro/*mainframe* (*up loading* e *down loading*)?			
15. É proibido a analistas e programadores testar programas com banco de dados real?			
16. Existem critérios de reorganização de banco de dados?			
17. É adequado o tempo de resposta para acesso dos usuários aos bancos de dados?			
18. Existem critérios adequados para a contingência *scratch* em banco de dados?			
19. As modificações em tabelas de acesso a banco de dados são feitas, somente, com autorização do executivo principal da área usuária?			
20. O plano de treinamento em linguagens de acesso a banco de dados é adequado?			

QUESTIONÁRIO
AMBIENTE BANCO DE DADOS

Questão	Sim Não N/A	Comentários	Referência Documentação Auditoria
21. Há contrato de manutenção e apoio técnico à utilização do *software* de gerenciamento de banco de dados?			
22. Existe seguro contra perda do conteúdo do banco de dados?			
23. Os sistemas que se utilizam de banco de dados estão, corretamente, analisados segundo o conceito de consulta/atualização *batch* ou *real time*?			
24. Há unidades de discos suficientes para suportar os bancos de dados atuando em *real time*?			
25. Os analistas de banco de dados utilizam técnicas estatísticas para reestruturação dos segmentos/dados dos bancos de dados?			
26. Aos profissionais de banco de dados e de administração de dados o treinamento é adequado para dar suporte necessário a usuários, analistas e programadores?			

QUESTIONÁRIO

SEGURANÇA FÍSICA E AMBIENTAL

Questão	Sim Não N/A	Comentários	Referência Documentação Auditoria
1. O CPD está localizado em ambiente adequado às atividades computacionais?			
2. Existe sistema adequado de combate a incêndio no CPD?			
3. Há risco de inundação no CPD?			
4. O sistema de controle de acesso ao Centro de Computação é adequado?			
5. Existe plano antigreve no Centro de Computação?			
6. O CPD possui um sistema de informação e contra-informação para identificar insatisfações/ações hostis aos sistemas?			
7. Existe um esquema de substitutos para as funções/profissionais-chave do CPD?			
8. Há um plano de abandono do CPD em caso de catástrofe?			
9. Existe um programa formal de treinamento em segurança no CPD?			
10. Há sistema de detecção de fumaça e calor no CPD?			
11. O CPD é monitorado por sistema computadorizado de controle de incêndio e de acesso?			
12. Existe norma para prevenir tramitação de volumes magnéticos em condições inadequadas de trânsito?			

QUESTIONÁRIO

SEGURANÇA FÍSICA E AMBIENTAL

Questão	Sim Não N/A	Comentários	Referência Documentação Auditoria
13. Existe risco de desabamento no CPD?			
14. O CPD obedece aos bons preceitos de ergonomia?			
15. Existe *no-break* no CPD?			
16. Existe gerador no CPD?			
17. A vigilância está treinada para atuar no ambiente computacional?			
18. Existe a política de mesa vazia após o expediente no CPD?			
19. As condições de limpeza do CPD são adequadas?			
20. Existe um plano de contingências testado e viável no CPD?			
21. Existem redes de comunicação alternativas?			
22. Existe sistema automático de gás *halow* no CPD?			
23. Existem computadores alternativos àqueles existentes no Centro de Computação?			
24. Existe grande parentesco entre os profissionais que atuam no Centro de Computação?			
25. Quando da contratação é verificada a vida dos profissionais do CPD?			
26. A área de segurança patrimonial tem atuado junto à segurança do CPD?			

QUESTIONÁRIO
SEGURANÇA FÍSICA E AMBIENTAL

Questão	Sim Não N/A	Comentários	Referência Documentação Auditoria
27. Há um manual de padrões para segurança física e ambiental no CPD?			
28. Os profissionais de computação têm acesso livre, somente, às suas respectivas salas de trabalho?			
29. Existe esquema de revista do pessoal do Centro de Computação?			
30. O CPD está longe de garagens, postos de gasolina, áreas com radiações eletromagnéticas etc.?			
31. Há detectores de temperatura e umidade?			
32. O sistema de ar condicionado é adequado?			
33. Existe seguro para os equipamentos e instalações do Centro de Computação?			
34. Houve inspeção do CPD pela empresa de seguros ou pelo Corpo de Bombeiros nos últimos 12 meses?			
35. Existe no CPD uma lista com nomes, telefones e endereços da Polícia, Corpo de Bombeiros, Empresas de Manutenção, Executivo de Segurança?			
36. Existe uma política de análise de risco para o CPD?			

QUESTIONÁRIO

SEGURANÇA FÍSICA E AMBIENTAL

Questão	Sim Não N/A	Comentários	Referência Documentação Auditoria
37. O esquema de armazenamento de volumes magnéticos e de suprimentos de computação é adequado?			
38. Há cópia da documentação de segurança em local seguro?			
39. O esquema de férias do pessoal de computação é cumprido?			
40. É feito rodízio de funções a cada três anos entre os profissionais de computação?			
41. Foi realizada este ano a semana de prevenção de acidentes em computação?			

QUESTIONÁRIO

SEGURANÇA LÓGICA E CONFIDENCIALIDADE

Questão	Sim Não N/A	Comentários	Referência Documentação Auditoria
1. Existe norma estabelecendo nível de confidencialidade de relatórios/telas?			
2. É utilizada criptografia no Centro de Computação?			
3. Há norma obrigando o uso de registros *heades* e *trailler*, bem como de seu conteúdo?			
4. Os relatórios/telas de controle são verificados por profissionais independentes?			
5. Os programas de crítica/consistência contra cadastro identificam os seguintes tipos de erros: a) inexistência de chave; b) dígito verificador; c) campo numérico; d) campo com sinal; e) inexistência de tipo de transação; f) campo em branco; g) seqüência de registros; h) teste de limite e razoabilidade; i) combinação de campos; j) cruzamento de campos; l) inclusão já existente; m) exclusão/alteração inexistente.			
6. Existe cruzamento de totais entre o pessoal de computação e o pessoal usuário?			

QUESTIONÁRIO

SEGURANÇA E CONFIDENCIALIDADE

Questão	Sim Não N/A	Comentários	Referência Documentação Auditoria
7. São utilizados *hash-totals* nos processamentos?			
8. Existem normas explicitando e impondo o uso de rotinas catalogadas?			
9. O analista de segurança em computação estabelece normas para segurança lógica?			
10. Existem relatórios com controles de totais de processamento?			
11. Os sistemas vitais já foram processados no Centro de Computação de *back-up* para garantir a efetividade do plano de contingência?			
12. A distribuição das listagens atende às condições de confidencialidade?			
13. A submissão de *jobs* ao computador atende ao esquema de prioridades adequado?			
14. Existe *software* de gerenciamento de arquivos?			
15. Existe norma para *check-point*/reinício do processamento?			
16. Há rodízio de operadores no tocante ao processamento de operações sensíveis?			
17. Existem normas restringindo o uso de programas "quebra-galho"?			

QUESTIONÁRIO

SEGURANÇA LÓGICA E CONFIDENCIALIDADE

Questão	Sim Não N/A	Comentários	Referência Documentação Auditoria
18. Existem totais de controle para prevenir inadequadas inserções de registros em arquivos de integração?			
19. Há norma caracterizando a necessidade de existência de um arquivo de fechamento do processamento?			
20. Existe um Manual de Controles do Aplicativo?			
21. Existe norma estabelecendo o cruzamento de arquivos analíticos com sintéticos para o correto fechamento do processamento?			
22. É controlado estouro de campo?			
23. É registrada a atuação dos profissionais de *software* básico sobre o Sistema?			
24. Existe implantada uma hierarquia de *passwords*?			
25. São testados os arquivos da fitoteca de *back-up* para identificar se se encontram em bom estado?			
26. Há uma norma estabelecendo critérios para a criação de *back-up's*?			
27. Os arquivos *back-up* são copiados, anualmente, quando devem ficar retidos por longo prazo?			

QUESTIONÁRIO

SEGURANÇA LÓGICA E CONFIDENCIALIDADE

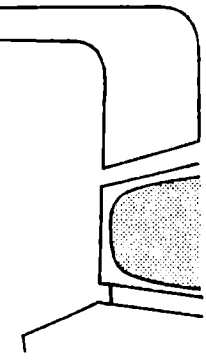
Questão	Sim Não N/A	Comentários	Referência Documentação Auditoria
28. Há controle de utilização de volumes magnéticos para efeito de sua desativação antes que apresentem *data-check*? 29. Existe *label* externo em seu volume magnético? 30. É utilizado o campo data de expiração do arquivo no registro *header?*			

QUESTIONÁRIO

AMBIENTE AUDITORIA INTERNA

Questão	Sim Não N/A	Comentários	Referência Documentação Auditoria
1. O uso do micro na auditoria interna atende aos aspectos administrativo-operacionais e aos aspectos técnico-operacionais? 2. Todos os auditores internos são treinados em operação e programação de micro? 3. O micro tem capacidade ociosa? 4. Existem *softwares* de apoio à auditoria interna adquiridos de terceiros? 5. Os micros da auditoria interna estão conectados em rede? 6. Há documentação dos programas rodados nos micros da auditoria? 7. Os *logs*/folhas de registros de utilização dos micros são verificados pela gerência de auditoria semanalmente? 8. Há classificação de sigilo para arquivos/programas/relatórios/telas usados no micro da auditoria?			

Bibliografia



BRASIL. Secretaria Especial de Informática. *Relatório da comissão especial de proteção de dados nº 021*. 1986.

DAVIS, Keagle W. & PERRY, William E. *Auditing computer aplications*. New York, John Wiley & Sons, 1982.

GIL, Antonio de Loureiro. *A atuação da auditoria de sistemas computadorizados para obtenção de uma maior produtividade de processamento eletrônico de dados*. São Paulo, Faculdade de Economia e Administração da USP, 1985. Tese de Doutorado.

——— *O estágio atual da auditoria de sistemas de informações computadorizados no Brasil*. São Paulo, Faculdade de Economia e Administração da USP, 1976. Dissertação de Mestrado.

——— *Sistemas de informações contábeis*. São Paulo, Atlas, 1976.

IIA – The Institute of Internal Auditors. *System auditability and control*. Florida, Altamonte Springs, 1977.

PERRY, E. William. EDP Audit work papers. In: AUDIT GUIDE SERIES. EDP Auditors Foundations, 1981.

STREAMS, Carol. *Control objectives*. EDPAA – Eletronic Data Processing Auditors Association, 1980.

MANUAIS

MAUD – Manual de Auditoria de Sistemas das Metodologias FATO® – ON, FATO®-OS e MACC®

MFAS – Manual de Formulários das Metodologias FATO® – ON, FATO® – OS e MACC®.

Manual da Metodologia Tamdis-Técnicas de Auditoria de Microcomputadores à Distância.

1989

Impressão e acabamento
(com filmes fornecidos):
EDITORA SANTUÁRIO
Fone (0125) 36-2140
APARECIDA - SP

AUDITORIA DE COMPUTADORES

Os computadores eletrônicos são instrumentos que permitem a evolução empresarial e dão sustentação para a expansão e entrelaçamento das tarefas de administração da organização moderna.

Auditoria de computador é atividade recente no meio empresarial brasileiro e suas técnicas e forma de abordagem carecem de consagração. Uma atuação, a nível dos vários momentos e da tecnologia vigente, do auditor de computador é apresentada, com ênfase nos vetores: o que é auditoria de computador; qual o ambiente empresarial em que ocorre a auditoria de sistemas; quais os momentos de atuação do auditor; o atual estudo da auditoria em processamento eletrônico de dados; para onde vai a auditoria de sistemas; gerenciamento da auditoria em computador.

A atividade de auditoria, por sua vez, evoluiu e é exigida, ultrapassando os seus limites originais de auditoria contábil. Sua expressão máxima, em termos de tecnologia, está abraçada pelas empresas de auditoria independente. A auditoria assume posturas de auditoria operacional e auditoria de computador, culminando, atualmente, com a auditoria de sistemas, sendo esta levada a participar de todos os momentos das organizações à medida que o computador eletrônico permeia e participa de todos os instantes da vida empresarial.

Este livro lida com a problemática empresarial e a utilização dos computadores vista sob o enfoque de atuação da auditoria de sistemas. Contempla a filosofia e as diretrizes de participação dos auditores de sistemas junto ao ambiente computacional das empresas em aspectos tais como **conceitos, técnicas** e **metodologias.**

A auditoria de sistemas computadorizados atua sob a ótica de validação e avaliação do controle interno do ambiente computadorizado.

NOTA SOBRE O AUTOR

ANTONIO DE LOUREIRO GIL é mestre, em 1976, e doutor, em 1985, pela Universidade de São Paulo com trabalhos que versam sobre auditoria e segurança em computadores. Professor desde 1973 da Faculdade de Economia e Administração da USP. É autor do livro **Sistemas de informações contábeis** publicado pela Atlas. Atua há mais de 25 anos na área de processamento eletrônico de dados. É sócio-diretor do grupo de empresas ACI-Assessoria e Controles Internos (auditoria de computador); CQA-Computer Quality Assurance (qualidade em computação); SECUR-Computer Security Enterprise (segurança em computação). Desde 1986 é professor de mestrado e doutorado na FEA-USP das disciplinas: Informática na Empresa; Sistemas de Controladoria Gerencial; Análise de Sistemas Contábeis/Financeiros; Auditoria, Controles e Segurança em Computação.

APLICAÇÃO

Leitura de interesse profissional em computação na área de auditoria de sistemas. Livro-texto para a disciplina AUDITORIA EM COMPUTADORES.

publicação atlas

ISBN 85-224-0395-3