UNIVERSIDADE FEDERAL DO CEARÁ

FACULDADE DE ECONOMIA, ADMINISTRAÇÃO,
ATUÁRIA E CONTABILIDADE

CURSO DE CONTABILIDADE

- AUDITORIA DE SISTEMAS –
CONTROLES INTERNOS E SEGURANÇA DE SISTEMAS

RAQUEL QUINTINO NUNES

FORTALEZA, FEVEREIRO, 1999

- AUDITORIA DE SISTEMAS – CONTROLES INTERNOS E SEGURANÇA DE SISTEMAS

RAQUEL QUINTINO NUNES

Orientador: VICENTE CRISÓSTOMO

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

FORTALEZA – CE
1999

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

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

Média

Raquel Quintino Nunes

Nota

Prof. Vicente Crisóstomo
Prof. Orientador

Nota

Prof. Josué Viana de Oliveira Neto
Membro da Banca Examinadora

Nota

Prof. Pedro Paulo Monteiro Vieira
Membro da Banca Examinadora

Monografia apresentada em 01 de março de 1999

SUMÁRIO

RESUMO

Este trabalho aborda os principais temas necessários à compreensão do que seja Auditoria de Sistemas. Dentro desta área concentramo-nos nos aspectos de auditoria de sistemas em produção e em desenvolvimento. Um posicionamento do trabalho é feito no contexto dos sistemas de informações mediante uma apreciação teórica que evidencia a necessidade, conceituação e área de atuação da função da AUDITORIA para sistemas informatizados.

Igualmente são abordados as diversas etapas de uma auditagem intra-sistema e extra-sistemas, suas técnicas de tratamento e os métodos aplicáveis nas diversas etapas.

INTRODUÇÃO

A tecnologia desenvolve-se numa velocidade e amplitude jamais vista. Chegamos a "sucatear" tecnologias sem que estas tenham sequer chegado ao conhecimento do público, mesmo às pessoas, às entidades que diretamente deveriam consumir.

Observe que estamos falando tanto de mudanças técnicas de gestão quanto no ferramental de nossas indústrias, na maneira como negociamos, nos relacionamentos com as pessoas, em suma, em todo o âmbito da atuação humana, incluindo o nosso comportamento e as nossas atitudes.

Já é tecla batida, portanto, que os tempos são de mudanças e que essas mudanças são amplas, velozes e profundas. Desse modo, teorias e práticas administrativas que até ontem eram tidas e havidas como eficientes e eficazes, colocadas em prática hoje, sem a adequada flexibilidade, podem levar as empresas à concordata e ao desaparecimento.

Por outro lado, uma série de "novas" técnicas de gestão ganha expressão no momento atual, causando "demolições" de verdades antigas – ou reforçando-as (depende do ângulo de visão). Ao mesmo tempo, grandes evoluções, em todas as áreas de telecomunicações e informática, quebram as estruturas centralizadas que tanto dominaram o processo, como o acesso às informações no passado.

A auditoria teve, tem e sempre terá uma razão básica para a sua existência: a não lealdade, a não confiabilidade dos seres humanos. Sim, porque, se todos e cada um de nós fôssemos leais e confiáveis, não existiriam fraudes, roubos, ações dolosas, não haveria necessidade de ser exercido controle sobre as atitudes e o comportamento das pessoas.

Embora triste, é verdade que todas as pessoas são falíveis e que, além disso, muitas procuram aproveitar-se de seus dotes de inteligência, de seu conhecimento técnico e dos postos que ocupam, nas empresas públicas ou privadas, para "levar vantagem", ou seja, lesar os outros, cometendo fraudes, roubos e os mais variados delitos.

Por essa razão, as pessoas físicas vêem-se forçadas, na medida de suas possibilidades financeiras, a mandar construir muros altos, instalar grades e sistemas de alarme em suas propriedades e, sempre que possível, a manter um belo cão de guarda e seguros contra roubos e as várias modalidades de sinistros.

As empresas, que são organizações humanas, agem de modo semelhante ao descrito, tomando todas aquelas medidas de precaução e, em especial, criando, mantendo e aprimorando, continuamente, os seus sistemas de controle interno.

A auditoria encontra sua missão, sua razão de ser, na realização de trabalhos de verificação e avaliação do sistema de controle interno aplicado pela empresa na efetivação de suas operações, de suas transações e, é claro, do impacto que essas operações e transações acarretam ou possam vir a acarretar na adequada continuidade de negócios da empresa.

Abordamos aqui a maneira como se executa os procedimentos para cumprimento dessa missão. Sua evolução tem que ter a mesma velocidade e amplitude com que evoluem os métodos, os processos, enfim, toda a tecnologia de gestão da empresa.

Primeiramente, propomo-nos apontar os rumos teóricos necessários à compreensão adequada do que sejam controles internos e segurança de sistemas, ou, em outras palavras, do que seja "auditoria de sistemas", deixando claro que o homem, só ou em equipe, é o responsável por provocar fraudes e danos dentro das organizações. Por outro lado, é ele, o próprio homem, que cria as estruturas, os sistemas, os processos, em suma, os mecanismos que evitam ou dificultam a ocorrência desses prejuízos, financeiros e morais, às empresas.

Após a função Auditoria de Sistemas é abordada como atividade permanente e necessária em CPDs. Face ser uma função já existente nas Organizações antes mesmo da introdução de Processamento Eletrônico de Dados será discutida a evolução e caracterização de uma área especializada para controles de Processamento de Dados.

Uma rápida conceituação de sistemas é feita como introdução no capítulo seguinte, onde mostramos a importância dos recursos, objetivos, componentes, meio ambiente e administração. Uma visão do ciclo de vida dos sistemas prepara a abordagem dos maiores riscos e problemas a eles afetados, caracterizando a incidência da fraude. Uma análise da vulnerabilidade é feita levando-se em conta os objetivos a que servem e a participação do homem.

A seguir as técnicas de abordagem usadas para auditagem de sistemas são aqui apresentadas, fazendo-se uma análise de suas características, vantagens e desvantagens. Independente da técnica utilizada são dadas informações sobre os grupos que realizam os trabalhos de auditoria de sistemas. Abstraímos a qualificação dos componentes, visto julgarmos que a ausência de qualquer requisito de qualificação invalidaria o estudo. Assim a análise dos grupos restringe-se à apreciação se os auditores são externos ou internos à Organização e que reflexos ou resultados podem trazer para a empresa.

Finalmente os estudos são dirigidos para os métodos utilizados nas auditagens dos sistemas através de descrição sumária das etapas do trabalho.

AUDITORIA E CONTROLES INTERNOS

Auditoria

Expor um conceito é sempre perigoso. Isso devido a diferentes leituras que cada objeto, cada matéria, cada assunto nos permite, e estas sempre serão efetuadas em face dos objetivos que a pessoa tenha em vista atingir.

Dentro de muitas organizações, entidades de classe e até em nível pessoal, ao longo dos anos, firmou-se um conceito de que a auditoria fosse uma função essencialmente contábil.

Através desse contexto, podemos entender que auditoria seja. "Uma técnica contábil empregada para avaliar as informações contábeis, constituindo, assim, um complemento indispensável para que a contabilidade atinja sua finalidade."

Aceitando-se essa visão como válida, poderemos chegar a um conceito para auditoria como sendo. "Uma técnica contábil que, através de procedimentos que lhe são peculiares, objetiva obter elementos de convicção que permitam julgar se os registros contábeis foram efetuados de acordo com os princípios fundamentais e normas de contabilidade e se as demonstrações contábeis refletem adequadamente a situação econômica-financeira da empresa num determinado período."

Restrito ao campo contábil, tal conceito é bastante válido, mas sobre auditoria existe um ponto de vista mais amplo. Ela não se restringe à contabilidade e/ou aos temas contábeis, ela engloba toda a organização e vai muito além, estendendo seu campo de ação para todas as interações da organização com a comunidade, seus clientes, fornecedores, instituições públicas e privadas com as quais a empresa se relaciona.

Contudo, a principal responsabilidade pelo sucesso ou fracasso da empresa, pública ou privada, independente da sua área de negócios é, e tem que ser assumida pelo seu principal executivo. Claro que dentro do processo de delegação de atribuições ele divide a responsabilidade com os demais membros do corpo de executivos da empresa, mas, apesar disso, ele continua sendo o único responsável diante dos proprietários e acionistas. Daí que uma das principais chaves para o sucesso de um executivo se refere à sua capacidade de apresentar uma equipe capaz, confiável, motivada e coesa.

Aceitando-se essa visão podemos chegar a um conceito mais amplo para auditoria como sendo. "Auditoria é uma função de assessoria à alta administração que, mediante aplicação dos procedimentos de trabalho adequadamente planejados, obedecendo às

normas e padrões geralmente aceitos, contribui para o cumprimento das funções de controle das operações da empresa."

Esse conceito deixa claro que, independente do seu posicionamento na estrutura da empresa, o órgão de auditoria não tem poder de decisão sobre os atos e fatos empresariais. Cabe-lhe a responsabilidade de examinar e avaliar a ocorrência desses atos e fatos, no sentido de assegurar que eles se realizem em obediência à harmonia com as políticas, diretrizes e normas da alta administração.

Auditoria Interna e Externa

Os trabalhos de auditoria podem ser realizados, em qualquer tipo e porte de empresa, por pessoal interno ou externo a ela. Quando realizados por pessoal interno, portanto pela auditoria interna, eles, prioritariamente, visam assessorar a alta administração no cumprimento de suas funções de controle das operações da empresa. Se executados por pessoal externo, empresas ou profissionais liberais oficialmente estabelecidos como prestadores de serviços técnico-profissionais de auditoria, os trabalhos têm como finalidade principal assegurar aos proprietários e acionistas, ao conselho de administração e ao mercado em geral que as demonstrações financeiras espelham o real resultado que as transações de um dado período provocam na situação patrimonial (econômico-financeira) da empresa.

Como os objetivos finais são claramente diferenciados, um trabalho não exclui o outro, e sim há uma interação, uma complementariedade entre ambos. Portanto, normalmente encontra-se, principalmente nas empresas organizadas com sociedades anônimas, ambos os trabalhos.

Os auditores deverão aplicar procedimentos de trabalho adequadamente planejados, quer seja por equipes internas e/ou externas, obedecendo as normas e padrões geralmente aceitos. Instrumentos estes desenvolvidos pelas entidades que congregam os contabilistas ou pelo próprio governo do País.

O principal objetivo da atividade de auditoria é a revisão e avaliação do conjunto de diretrizes, políticas, sistemas e procedimentos criados pela empresa no sentido de, por um lado, nortear a atuação de todos na empresa, e, por outro, assegurar o seu patrimônio contra danos, fraudes, roubos, prejuízos, etc., de natureza material ou não.

Controles Internos

Na Exposição de Normas de Auditoria estão esclarecidos o conceito e a amplitude do que constitui o sistema de controle interno da empresa:

"O sistema de controle interno compreende o plano de organização e o conjunto coordenado de sistemas, métodos e procedimentos adotados por uma empresa para a salvaguarda do seu patrimônio, a eficiência operacional e a exatidão e confiabilidade dos registros e informações contábeis-financeiras.

O sistema de controle interno deve atender pelo menos quatro objetivos, quais sejam:

- Assegurar que as transações estejam sendo adequadamente registradas de modo a permitir a elaboração de demonstrações financeiras segundo os princípios contábeis geralmente aceitos ou outros critérios aplicáveis e manter a responsabilidade pelos bens.
- Assegurar que o acesso aos bens e informações e que a utilização destes ocorra com a autorização formal da administração.
- Garantir que as transações sejam feitas com autorização formal da administração.
- Possibilitar, com freqüência razoável, o confronto entre os registros contábeis-financeiros e os respectivos bens, direitos e obrigações.

Com isso, o intercâmbio de ativos e serviços dentro da empresa ou entre esta e o mercado com o qual interage e as suas ocorrências, constituem o assunto primordial do sistema de controle interno.

Esse intercâmbio de transações dá origem a deveres e direitos entre as várias áreas da empresa e entre a comunidade com a qual interage, os seus clientes, os fornecedores, as instituições financeiras, os órgãos públicos, etc.

Para que o sistema de controle interno seja adequado, ele deve contribuir para que o fluxo de transações ocorra de modo seguro, formal e autorizado, seguindo os seguintes passos: autorização para que se faça a transação, sua ocorrência (de fato), o registro dessa ocorrência e o controle do processo e a avaliação dos efeitos que essa ocorrência tenha causado ou possa vir a provocar à empresa.

É também na Exposição de Normas de Auditoria que é estabelecido que o sistema de controles internos de uma empresa se decompõe em dois tipos de grupos de controle, os de natureza contábil e os de natureza administrativa e os diferencia.

Os controles contábeis compreendem o plano de organização e todos os sistemas, métodos e procedimentos relacionados à salvaguarda dos bens, direitos e obrigações, fidedignidade dos registros financeiros, o sistema de autorização e aprovação de transações,

os princípios de segregação de tarefas, os controles físicos sobre os bens e informações e a custódia de bens e direitos.

Os controles administrativos compreendem o plano de organização, os sistemas, métodos e procedimentos estabelecidos pela direção com a finalidade de contribuir para a eficiência e eficácia operacional, obediência a diretrizes, políticas, normas e instruções da administração, os programas de treinamento e desenvolvimento pessoal, os métodos de programação e controle de atividade, os sistemas de avaliação do desempenho e os estudos de tempos e movimentos.

Assim podemos observar que os controles administrativos relacionam-se indiretamente com os registros contábeis financeiros.

Vamos deixar isso mais claro mediante um exemplo: os programas que uma empresa desenvolve para o treinamento e desenvolvimento de seu pessoal têm por finalidade contribuir para que tenhamos pessoas mais capacitadas, e tais pessoas, sendo mais e melhor capacitadas, tendem a provocar menor quantidade de erros durante a execução de suas funções, colaborando para a maior qualidade do fluxo de transações da empresa que é base para os trabalhos de auditoria.

Normas e procedimentos de auditoria

Voltamos à primeira Exposição de normas de Auditoria, e podemos verificar que ela não se limita a fixar quais sejam as normas básicas que regulam o trabalho de auditoria. Ela vai além, esclarecendo a diferença existente entre o que sejam normas e o que sejam procedimentos. Os procedimentos relacionam-se com os atos que o auditor deve praticar para realizar seu trabalho; enquanto as normas tratam da medida de qualidade na execução desses atos para o entendimento dos objetivos do trabalho.

As normas básicas ou gerais de auditoria agrupam-se em três conjuntos, conforme refiram-se à pessoa do auditor, à execução do trabalho e à emissão do parecer, ou, mediante adaptação, do relatório do trabalho executado.

Quanto às normas relativas à pessoa do auditor, os trabalhos deverão ser executados por pessoas tecnicamente treinadas e capacitadas; o auditor deverá ser independente em relação aos assuntos do trabalho a realizar; o trabalho e a emissão do parecer ou do respectivo relatório deverão ser realizados cuidadosamente, com enfoque totalmente profissional.

Quanto às normas relativas da execução do trabalho , o planejamento dos trabalhos a realizar e a supervisão de sua realização devem ser adequados; os trabalhos devem

ser executados com vistas a ser determinado o grau de confiança que se poderá depositar no sistema de controle interno da empresa e, com isso, determinar a natureza e extensão dos testes a serem realizados; deverão ser colhidos elementos adequados e suficientes para comprovar a funcionalidade do sistema de controle interno e os resultados por ele apresentados.

Quanto à emissão do parecer do auditor, como o próprio título deixa claro, essas normas têm sua aplicação específica no preparo e emissão do mesmo sobre a correção e fidedignidade com que as demonstrações contábeis e financeiras foram preparadas e demonstram a real situação patrimonial da empresa.

O parecer é um documento oficial emitido por uma empresa ou por um profissional de auditoria externo à empresa auditada, mediante o qual ela(e) concorda ou não com a fidedignidade das demonstrações contábeis financeiras da empresa. Se concordar, dizemos que o parecer é "limpo". Caso descorde, há que deixar bastante claro em que aspecto, em que pontos ele discorda, e, então, o parecer recebe o nome de "com ressalva". A empresa ou o especialista de auditoria pode, ainda, realizar o seu trabalho e negar a emissão do seu parecer. Isso quer dizer que as irregularidades detectadas durante a realização dos trabalhos foram de tal magnitude que ela(e) não tem condições de emitir opinião sobre a real situação econômica.

As normas estabelecem que o parecer deverá declarar se as demonstrações financeiras foram declaradas e estão sendo apresentadas de acordo com os princípios de contabilidade geralmente aceitos, e se esses princípios foram aplicados no período atual com uniformidade em relação ao período anterior; as informações são consideradas adequadas, salvo o que se declare diversamente no parecer; o parecer deve expressar uma opinião sobre as demonstrações financeiras tomadas em conjunto ou conter uma declaração no sentido de que não se pode dar opinião. Nesse caso, há que dizer claras as razões que impedem a emissão da opinião, do parecer. O auditor deve declarar, a natureza dos exames realizados, e, se for o caso, o grau de responsabilidade por ele assumido.

Base de aplicação

A aplicação das normas, a execução dos procedimentos de auditoria apoiam-se em dois princípios: o de relevância ou de materialidade que diz respeito à importância de itens que, se apresentarem erros ou fraldes poderão acarretar maiores ou menores danos à empresa e o grau de risco que é a possibilidade de virem a ocorrer erros ou fraudes.

Um exemplo seria as transações envolvendo dinheiro (em moeda, cheques ou títulos) terem maior grau de risco de virem a apresentar fraudes do que as que envolvem inventários (compra e venda de equipamentos – exemplo).

Podemos classificar os graus de risco em três níveis. O pequeno, quando o sistema de controle interno for bastante eficiente e eficaz. Não existe sistema seguro, todo e qualquer seguro pode ser objeto de fraudes, manipulações, violações, etc. O médio, quando o sistema de controle interno aplicado no assunto ou tema sob auditoria não for razoavelmente adequado, contando com outro sistema, em outra área, que seja considerado como eficiente e eficaz para evitar ou detectar erros ou fraudes no primeiro sistema. Nesse caso, dizemos que existem controles paralelos adequados. O alto, quando o sistema de controle interno se mostrar falho sem contarmos com o sistema paralelo que possa dar-lhe cobertura.

Verificamos que quanto mais eficiente e eficaz for o sistema de controle interno da empresa, menores serão os riscos envolvidos, mas sempre haverá possibilidade de ocorrer erros e fraudes, uma vez que não existem sistemas, métodos ou procedimentos totalmente seguros.

Procedimentos de Auditoria

Os principais procedimentos de auditoria, pelo menos aqueles mais ligados à contabilidade do que ao todo da empresa, estão relacionados com atos referentes à contagem física de bens, às confirmações de posições com terceiros (circularização), às conferências de cálculos e às inspeções de documentos.

Evidente que o enfoque deve ser mais amplo, deixando claro que o primeiro e básico procedimento a cumprir, em qualquer trabalho de auditoria, interna ou externa, é o de respeitar, de atender aos preceitos das normas reguladores da profissão, e, agindo assim, devemos iniciar colocando em ação a primeira norma do conjunto das relacionadas à execução do trabalho. "O planejamento dos trabalhos a realizar e a supervisão de sua realização devem ser adequados."

Portanto, a primeira providência a tomar é planejar como iremos agir para executar o trabalho. O planejamento deve indicar as estratégias que seguiremos, as etapas de trabalho que realizaremos, os recursos que serão necessários, em termos de moeda, pessoal, tecnologia, etc., deixando claro quem irá executar o trabalho e a quem compete exercer a sua supervisão.

Como decorrência do planejamento, devemos criar um programa de trabalho, indicativo dos passos a seguir, das entrevistas a serem realizadas, dos levantamentos que

precisaremos executar, das observações, etc., e, ao longo do trabalho, conforme formos conhecendo e podendo avaliar a adequação do sistema de controle interno, deveremos decidir pelo grau de aprofundamento dos testes a realizar. Quanto melhor o sistema, menores e menos profundos os testes a realizar. Quanto mais falho o sistema, maiores e mais profundos testes serão necessários.

Para o cumprimento desse programa, o auditor deverá agir, executando procedimentos tais como, analisar, revisar, observar, inspecionar, confirmar, calcular e indagar, e, enquanto assim estiver procedendo, deverá tomar o cuidado de reunir os documentos que comprovem o trabalho realizado, e que possam servir de base para sua análise e verificação. O auditor não pode apresentar uma crítica, uma sugestão, uma observação em seu relatório sem ser capaz de comprovar, junto a alta administração, o quanto diz ou propõe, por falta de material que documente aquilo que ele afirma.

Por maior que seja o grau de informatização da empresa, por mais hábil que seja o auditor para executar seus trabalhos via recursos computacionais, ele nunca prescindirá da necessidade de sair a campo, de entrevistar pessoas, de "pedir para ver", uma vez que, não são os equipamentos e/ou a tecnologia que provocam os principais erros, que cometem fraudes, roubos, e ações dolosas. São as pessoas, e mesmo nos sistemas operados em rede, a exemplo da Internet, mais de 60% dos casos, comprovadamente, envolvem uma ou mais pessoas internas à própria empresa lesada ou prejudicada.

A Exposição de Normas de Auditoria, dirigida totalmente ao impacto do emprego de recursos computacionais, ressalta que "a fase de planejamento dos trabalhos de auditoria deverá incluir a revisão preliminar da estrutura computacional da empresa, de modo a obter informações sobre os controles internos, operacionais e administrativos, incorporados, e a extensão de uso dos recursos computacionais".

A expressão "auditor de sistemas", nunca teve e nem tem sentido, uma vez que o auditor sempre foi, é e sempre será auditor de sistemas, pois é este o seu campo de atuação: os sistemas em que se decompõe, se organiza uma dada empresa.

Como justificativa dessa opinião, eis algumas modalidades de trabalho executadas pela auditoria: revisão e avaliação dos controles internos do sistema de contas a pagar; do sistema de aplicações financeiras; do sistema de compras; do sistema de crédito direto ao consumidor, etc.

Na execução desses trabalhos de auditoria devemos examinar e avaliar o plano de organização, os sistemas, os métodos e os procedimentos necessários à realização desses sistemas. Sempre foi assim, assim é e assim continuará sendo. O que tem ocorrido, ao longo

dos anos, é a pura e simples mudança de equipamentos, de tecnologias utilizadas para executar, para processar as funções dos vários sistemas da empresa.

AUDITORIA DE SISTEMAS

Os trabalhos de auditoria, de uma forma padrão já eram conhecidos desde a Idade Média. Em 1314 na Inglaterra, já se praticava auditoria mediante o exame das contas públicas. Portanto desde épocas passadas até hoje, e com certeza para sempre, são indiscutíveis a necessidade e a importância dos trabalhos de auditoria.

O que realmente ocorreu, é que nos anos finais do século passado, surgiram máquinas (de registro unitário, de cartões perfurados) para registrar, acumular e fornecer informações de maior poder de trabalho, base dos computadores atuais.

O avanço do processamento eletrônico de dados, com o emprego de recursos computacionais , casou um grande impacto no trabalho do auditor, principalmente pelo fato de que os registros das transações não eram mais visíveis a olhos humanos. Esses registros ficavam e ainda ficam em meios magnéticos. Calcule que susto, que impacto teve o auditor ao constatar que haviam mexido em sua área de trabalho!

Como sempre acontece nos processos de mudança, a maioria dos profissionais, ao menos de início, resistiram, enquanto uma minoria mais ousada ou mais esclarecida, sempre dependendo do ponto de vista de cada um, partiu para conhecer a nova tecnologia e, principalmente, empregá-la como um recurso técnico a mais para execução de seus trabalhos.

O conceito da função de Auditoria de Sistemas pode ser encontrado em diferentes definições. Para "The Institute of Internal Auditors" o objetivo da auditoria é assistir a todos os níveis de gerência no efetivo desempenho de suas responsabilidades, fornecendo-lhes análises, avaliações e recomendações concernentes às suas atividades. Já outros autores vêem a Auditoria como uma atividade permanente a toda Organização e que visa verificar a adequação e eficiência de controles, correção e integração com os dados processados ou a processar.

Ao analisarmos os conceitos verificamos que não apresentam substanciais diferenças, mas revelam dois estágios que podem ser tratados com bastante independência. No segundo conceito a atividade de auditoria preocupa-se com a verificação dos dados, atendimento a normas, controles e registros das transações ocorridas nos diversos processos. Aqui encontramos a tendência da constatação da evidência, onde é julgada a substância e

materialidade dos fatos, a fim medir ou deduzir a importância das observações face aos valores sob análise. Já em outro conceito temos uma apreciação mais dinâmica, onde o objetivo é medir a produtividade, custos e viabilidade dos processos inclusive a econômica.

Encontramos nesse segundo estágio o envolvimento de fatores menos palpáveis e mais subjetivos. Esta conceituação envolve um maior grau de complexibilidade, um conhecimento mais geral das ferramentas de produção e controle e uma maior dose do poder de observação. Não temos muitas vezes a possibilidade de constatar a evidência, nesse estágio, pois os fatores componentes de um processo estão sempre variando com o tempo, espaço e constituição. Face a essas dificuldades e ser a auditoria uma atividade já conhecida e desenvolvida, no tempo, antes da de Processamento de Dados, portanto antes da introdução do computador, existe uma ênfase para auditar os sistemas computadorizados atentando somente para verificação de registros e atendimento às normas de controle, dirigindo portanto todas as observações para as transações processadas.

Uma abordagem tradicional oriunda do tratamento dado quando de auditagem de sistemas com processamento manual, quando aplicada a sistemas computadorizados não obtém o mesmo sucesso. A abordagem, todavia, continua a ser feita por muitos e a explicação para o fato, face mesmo ao insucesso, pode ser encontrada no pouco ou nenhum conhecimento especializado das ferramentas técnicas de processamento de dados que é exigido dos auditores, cuja formação geralmente está voltada para auditagem de sistemas manuais.

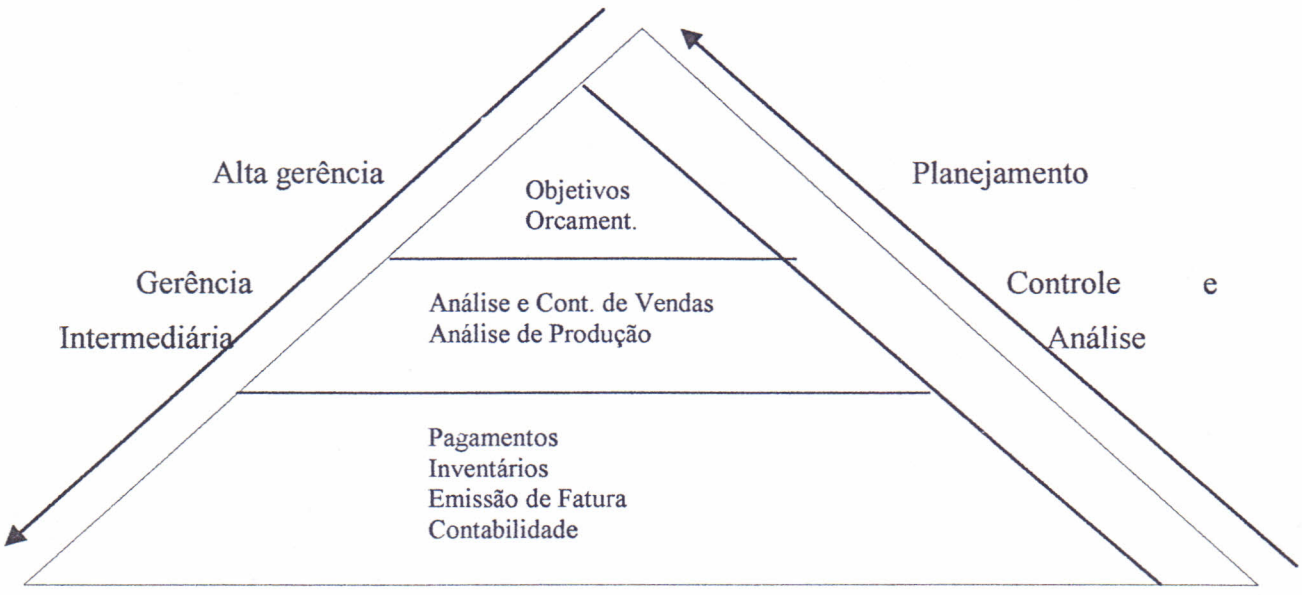
A abordagem precisa ser dinâmica incluindo entre suas atividades básicas controles que englobem a gerência de programas e sistemas; a organização, distribuição de trabalhos dentro de uma estrutura; o plano e projeção que deve ser usado como guia de gerência e avaliação da organização; os manuais de operação de sistemas de segurança de sistemas e instalações e de processos de recuperação de dados.

Como a auditoria tem por finalidade assessorar a alta administração da empresa, e, em obediência às normas de auditoria, tem de estar o mais possível independente para poder ter liberdade de atuação, ela deveria estar estruturada na empresa, no organograma da empresa, como um dos órgãos de assessoria do seu principal executivo.

Contudo, na maioria das empresas, a auditoria acha-se subordinada ao "controller" ou ao principal executivo financeiro, o que não é correto, uma vez que essa é uma das áreas mais visadas e onde com maior freqüência ocorrem as fraudes, os erros e as ações dolosas que mais prejuízos ocasionam à empresa.

Qualquer que seja a estrutura das organizações, existem gerências em vários níveis que têm por responsabilidade a direção de seus segmentos. Os conjuntos de atividades dos gerentes compõem-se de tarefas de planejamento, controle e execução de processos, que estão a envolver decisões sempre apoiadas em informações fornecidas por processos executados em níveis hierarquicamente inferiores. Observamos portanto um alargamento das atividades executivas e uma sensível diminuição das de decisão, planejamento ou controle à medida que caminhamos para níveis inferiores da organização.

Tal fato leva-nos a apresentar a figura da clássica pirâmide administrativa já discutida por muitos autores.



O fluxo de dados ou informações que percorre a pirâmide, tem sentido ascendente que flui um grande número de informações partindo de diversos níveis, e possibilita aos gerentes de nível mais elevado tomarem suas decisões. Estas resultam em comandos que fluem em sentido descendente, ativando ou desativando processos.

Não existe um nível de área específico responsável por todas as informações ou processos em execução, quer estejam baseados em computadores ou não. Em todos os níveis da Organização há processos e controles que necessitam ter um entendimento adequado. Uma estreita interrelação e complementaridade entre as atividades de execução de processos (processamentos de dados) e de controle (auditoria de sistemas) é sempre exigida. Processos

desenvolvidos e operados em qualquer nível geram informações que automatizam ou não decisões e necessitam ser controlados.

A auditoria de sistemas, em algumas decisões, atua como responsável pela fixação de controles no objetivo de garantir a correlação e segurança dos sistemas, mas a seguir através de *feedback* ela recebe informações dos próprios sistemas que podem sugerir modificações radicais nos controles anteriormente fixados.

Ao processamento de dados, porém, é dada a responsabilidade de desenvolver e operar os subsistemas da Organização e manter registros de transações para todas as áreas do sistema.

Hoje em dia, como mais e mais funções são automatizadas, gerando informações para decisões, as áreas dos profissionais de Processamento de Dados e de Auditoria de Sistemas têm-se expandido nos diversos níveis das estruturas organizacionais. Esses profissionais para ter real sucesso em suas atribuições deverão reunir em si mesmo características fundamentais como: adequada vivência em auditoria; bons conhecimentos de informática, quer no que respeita ao uso do computador para o dia-a-dia, quer para a realização de levantamentos e testes sobre as transações dos vários sistemas da empresa e; expressiva habilidade no relacionamento humano, nos vários níveis desde a alta administração até os menores níveis hierárquicos de empresa.

Nessa expansão, atividade de processamento de dados deverá preocupar-se com os procedimentos manuais e fases automatizadas para aplicação em computadores, ao passo que a auditoria de sistemas deverá ter sua atenção sempre voltada para os procedimentos e controles dentro e fora das fases automatizadas pelo computador.

Essa complementaridade de áreas de atuação leva a responsabilidade de auditoria de sistemas ao topo da pirâmide organizacional. Todavia tal responsabilidade pode sempre ser fragmentada nos diversos níveis de gerência, seja ela de processamento de dados ou não.

Agora ficou muito fácil saber quais sejam os papéis, as responsabilidades dos auditores e do pessoal de informática, de sistemas, seja qual for a nomenclatura que se use para os especialistas desta área. Tanto os auditores como os "informáticos" têm exatamente o mesmo objetivo para existir que é assessorar os gerentes, contribuindo positivamente para que eles possam cumprir com seus objetivos e atender suas finalidades.

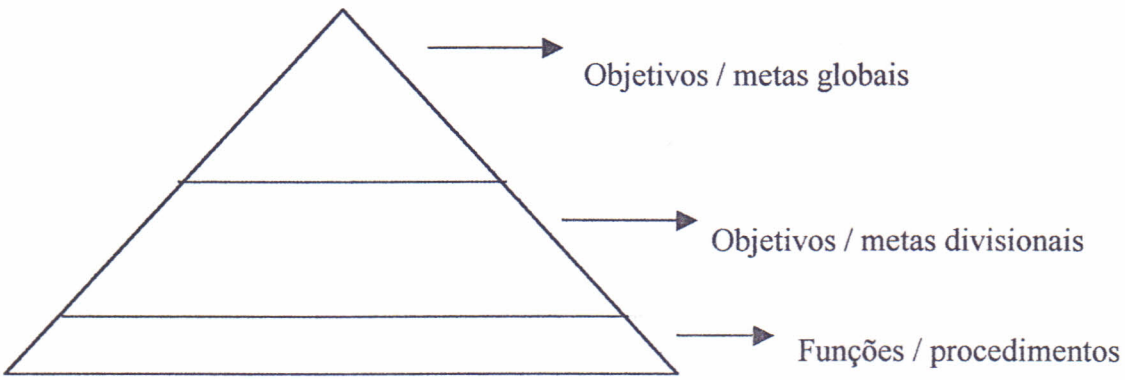
As atividades de sistemas têm por missão assessorar o gerentes no cumprimento de suas funções gerenciais notadamente no tocante à função gerencial "organizar". O pessoal da auditoria tem por missão auxiliar os gerentes na sua função de

controle. Logo, atuam pesadamente na função "controlar". Essas atividades são complementares, daí a necessidade de somar esforços sendo assim o único caminho para o sucesso de ambas as atividades e, por conseqüência da própria empresa.

Para entendermos melhor o que seja um sistema, o que sejam as responsabilidades básicas dos auditores, mencionaremos sobre a "teoria dos sistemas" partindo da visão da empresa como um macrossistema.

Uma empresa, seja ela pública ou privada, é um grande sistema, aberto, dinâmico, que mantém uma gama de relações internas e externas.

Cada departamento depende dos trabalhos dos demais para atingir os seus objetivos, e a empresa como um todo depende de seus fornecedores, de seus clientes, das instituições públicas e privadas com as quais interage, em suma, da comunidade em que se insere.



Compete à alta administração a determinação das missões, políticas, objetivos / metas de longo alcance (planejamento estratégico), bem como as orientações estratégicas básicas para a condução dos negócios da empresa (planejamento tático e operacional).

Essas decisões estratégicas, tomadas participativamente, envolvendo toda a cúpula e os níveis gerenciais, caem, descem para esses níveis gerando aí os objetivos e metas departamentais divisionais bem como as estratégias, os cursos de ação a serem seguidos, possíveis políticas específicas e normas de conduta.

Sendo assim, para que as coisas ocorram, é necessário que o trabalho perseverante e árduo seja executado. O trabalho dos técnicos de informática é de desenvolver e implantar sistemas, métodos e procedimentos enquanto que o trabalho dos auditores é de verificação desses sistemas, métodos e procedimentos, observando se estão sendo aplicados e proporcionando os resultados esperados.

O trabalho de assessoramento por parte dos auditores requer um mínimo de conhecimento do trabalho realizado pelos gerentes da empresa, devendo conhecer o que ele faz e como deve ser o relacionamento entre assessoria e gerência.

SISTEMA

O campo de um sistema

Genericamente um sistema pode ser considerado "um todo organizado para atender a todas as finalidades". Do ponto de vista físico, material, outro conceito bastante divulgado é que um sistema seja "um conjunto de partes e componentes, logicamente estruturado com a finalidade de atender a um dado objetivo". O que nos permite concluir que, no campo empresarial, dentro de uma empresa um sistema possa ser "um conjunto de funções, logicamente estruturadas, com a finalidade de atender um dado objetivo".

Considerando-se toda a empresa como um sistema, cada uma de suas áreas de atividade pode ser considerada um subsistema. Assim, uma empresa industrial ou comercial que é um macrossistema, pode ser decomposta em inúmeras partes menores, em vários subsistemas, tais como: projeto de engenharia; desenvolvimento de produtos; produção, abastecimento; distribuição e etc. cada um desses subsistemas poderia ser decomposto em outras partes menores, outros subsistemas. Por exemplo, o sistema de produção pode ser decomposto nos sistemas de preparação, usinagem, acabamento e etc.

Vários fatores podem motivar a abrir um sistema em partes menores, tais como: maior facilidade para planejamento, coordenação e controle dos trabalhos de desenvolvimento dos sistemas, do processo; a urgência do trabalho, a particularização de um dado problema e a relação do custo-benefício, etc.

Para se obter e manter sucesso, o trabalho de auditoria deverá ser feito em contínua interação com as diretorias, gerências e chefias envolvidas, fixando-se, o que será feito, onde começará, onde terminará, que objetivos deverão ser alcançados, etc.

O campo de trabalho do sistema é definido por seus parâmetros inicial e final. É preciso esclarecer o que está incluso neste campo, ou seja, os alcances, a abrangência de nosso trabalho, e como isso deve ser formalizado para conhecimento de todas as pessoas com poder de comando envolvidas.

Saber definir clara e adequadamente, os parâmetros e alcances de um sistema, de um processo, exige muito conhecimento técnico-profissional e muita habilidade de relacionamento humano. Se isso não for feito de modo adequado, fatalmente surgirá problemas graves na execução dos trabalhos de auditoria. Os auditores serão cobrados por coisas que não precisam realizar ou realizarão coisas que não deveriam ou necessitariam ter sido realizadas.

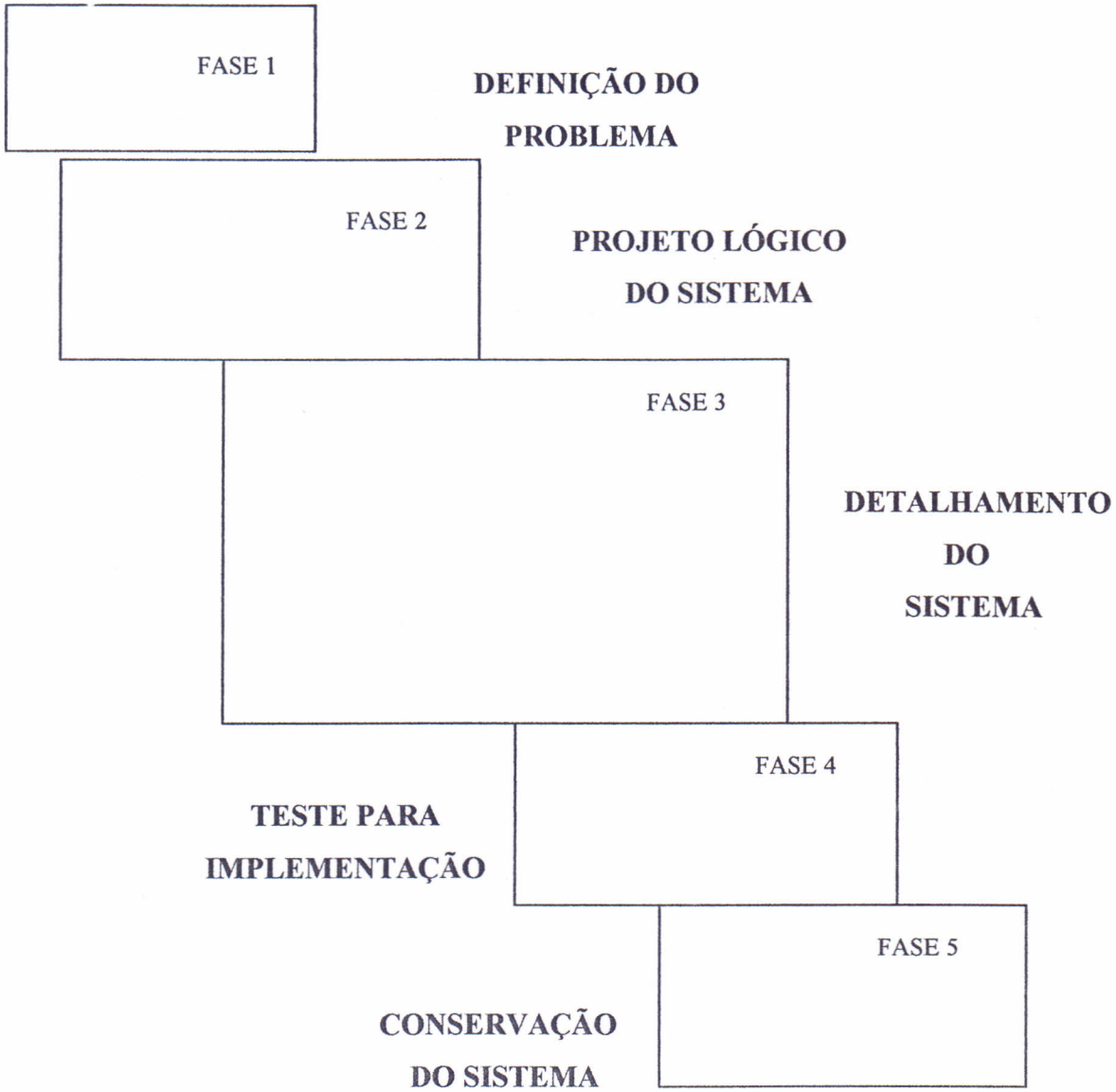
Ciclo de vida de um sistema

Uma das melhores técnicas encontradas para estudos de sistemas e seu desenvolvimento baseia-se no ciclo de vida de um sistema. Dividindo todo um processo sistêmico, desde o seu desenvolvimento até sua operação em um pequeno número de fases torna-se permitido a colocação de controles gerenciais entre e durante cada fase.

Esta metodologia permite que sejam alcançados dois objetivos: promover gerência estruturada para controles de qualidade de custos e assegurar propriedade das informações e dois canais de comunicação entre usuários, auditores, analistas/programadores e gerentes.

A divisão das fases do ciclo de vida de um sistema não tem sido feita de maneira uniforme, variando o número de fases entre cinco e onze, dependendo do autor.

A divisão do número de fases, a um observador menos avisado, poderia parecer que a metodologia não teria um suporte racional ou seria feita segundo a vontade do interessado. Todavia, isso não ocorre e a variação encontrada está em função do detalhamento requerido para uma melhor visão de algum subsistema que deve ter um controle mais detalhado face a tarefa a ser executada. Para melhor compreensão apresentamos uma destas abordagens a seguir.



Fases do ciclo de vida de um sistema considerando a existência de cinco fases. Divisão destinada ao estabelecimento de controle para a Auditoria de Sistemas.

1) **Definição do problema**. Esta atividade consiste em caracterizar os objetivos primários do sistema e requisitos do usuário. Subdivide-se na execução das tarefas:

- organização do projeto;
- avaliação do sistema atual;
- custo do sistema atual;
- fixação dos novos requisitos;
- projeto conceitual do novo sistema;
- custos e benefícios do novo sistema, exigidos pelo usuário e pelo auditor.

2) **Projeto lógico do sistema**. Atividade na qual é dada uma visão panorâmica do sistema em projeto. O trabalho é executado compreendendo as seguintes etapas:

- levantamento de dados;
- definição de entidades;
- definição dos processos do sistema;
- elaboração do diagrama de fluxos de sistemas;
- projeto dos requisitos de entrada.

3) **Projeto físico**. A definição dos componentes do sistema e desenvolvimento dos programas é atendida nesta fase, cujas tarefas podem ser vista como:

- detalhamento no projeto dos documentos-fonte;
- documentação dos arquivos;
- especificação dos programas;
- projeto dos requisitos de equipamentos;
- fluxos, codificação, detalhamento do plano de teste, detalhamento do plano de conversão;
- detalhamento dos planos de controle;
- desenvolvimento de procedimentos manuais.

4) **Implementação**. Diríamos que a fase constitui a criação do sistema. As tarefas aqui envolvidas podem ser resumidas em:

- criação dos dados de teste;
- realização dos testes;
- criação dos arquivos;
- implementação dos programas.

5) **Implantação**. Constitui fase em que o sistema já testado é posto em operação. Esta fase é vista compreendendo as tarefas de:

- controle do desempenho;
- aceitação do sistema.
- treinamento dos usuários e pessoal do CPD.
- entrega dos manuais aos usuários.

6) Operação e manutenção. Ë a fase de vida útil do sistema quando a organização quer obter resultados.

A utilização do método possibilita pois ao auditor, ao longo do desenvolvimento destas fases do sistema, o estabelecimento de uma série pontos para verificação do atendimento dos padrões de segurança, eficácia e eficiência.

Em tais pontos de controle, há sempre duas preocupações básicas presentes:

- qualidade e segurança do sistema do ponto de vista de processamento de dados;
- interligações entre usuários ou outros departamentos com o CPD.

O método prevê atender na seqüência de controles os seguintes princípios.

a) Princípio de padrões. Todo controle requer objetivos definidos com precisão para evitar que sejam camuflados pela personalidade de quem os executa.

b) Princípio do ponto estratégico. Seria inconveniente e dispendioso estabelecer controles a todos os detalhes da execução de um projeto. Não há regras de bolso que determinem a colocação de controles. Talvez o auditor possa perguntar a si mesmo: Que coisas são mais importantes a controlar em relação ao desenvolvimento de um sistema? Neste ponto cremos acertado o posicionamento dado pelo método.

c) Princípio da ação. Qualquer controle só se justifica possibilidade de corrigir os desvios detectados com relação a uma linha ou padrão estabelecido, porque na prática muitas vezes é esquecido. O método do ciclo de vida para auditar o desenvolvimento de sistemas possibilita o entendimento deste princípio.

Tais princípios são apontados como essenciais ao estabelecimento de controles.

Quanto à implementação o método requer conhecimentos profundos dos auditores em:

- processamento de dados (procedimentos);
- estabelecimento de controles para sistemas;
- controles administrativos para CPDs;
- linguagem de programação;
- análise e desenvolvimento de sistemas.

Tal fato é visto como razoável restrição a seu uso vez que a quase totalidade dos auditores pouco conhecimento dispõem dos itens acima alinhados.

O desempenho previsto com o uso do método, todavia, permite antever benefícios e controles bem mais efetivos e imediatos na operação dos sistemas, e sensível redução dos esforços da auditoria, que já terá fornecido todos ou quase todos os dados de que precisa para

testar a completeza e segurança dos sistemas. Cuidadosamente conduzido o método permite tirar bom proveito com a eliminação de erros antes do sistema tornar-se operacional, o que sem dúvida reduz os custos, riscos e prejuízos destes decorrentes.

A adoção dessa abordagem possibilita o *feedback* e só permitindo o avanço quando os requisitos exigidos em uma fase tenham sido satisfeitos em sua totalidade.

A abordagem permite igualmente a determinação de outros pontos tais como a alocação de recursos no devido tempo, possibilitando então o correto desenvolvimento do sistema sem que ocorra a carência ou a ociosidade de recursos.

Os principais riscos em sistemas

Uma das maiores preocupações com que se defrontam os nossos gerentes, auditores e analistas de processamento de dados é a identificação no ciclo de vida dos sistemas, dos problemas e riscos a que os mesmos estarão expostos, a repercussão que tais riscos terão nos sistemas e a probabilidade de sua ocorrência.

A característica e definição de um problema ou risco potencial face à falta de um detalhamento de recurso ou ausência de algum controle, pode começar já na primeira fase do ciclo de vida de um sistema e se estender até a sua efetiva operação.

Igualmente pode ocorrer que os riscos ou problemas façam parte do próprio meio onde vive ou atua o sistema.

A complexidade dos sistemas, a diversidade dos recursos e de equipamentos, os diversos graus de dependência das empresas aos sistemas baseados em Centros de Processamento de Dados (CPD), o envolvimento de um diversificado grupo de profissionais, a especialização exigida de cada profissional e as catástrofes da natureza aparecem como fatores que, agindo com intensidade de força sempre diversificada, armam a intricada rede de riscos e problemas que estão sempre presentes nos sistemas de informações.

Mesmo assim, muitos gerentes têm aceitado computadores e sistemas automatizados sem a mínima apreciação ao estudo do grau de sua vulnerabilidade, fator que passa a acrescentar à já extensa rede de riscos mais um; a imprevidência dos administradores.

Ao analisar os riscos que estão sujeitos os centros de processamento de dados, podemos apresentar um conjunto de cinco itens como maiores causadores de problemas. São eles: fogo; roubo; sabotagem; fraude e água.

Embora aceitando o conjunto de riscos , entendemos ser difícil estabelecer medidas de proteção mesmo sendo reduzido o número de componentes deste conjunto. Isto

decorre do fato dos riscos alinhados apresentarem seus efeitos em várias áreas de um Centro de Processamento, para as quais as medidas acauteladoras são de ordem diversa.

Uma classificação que melhor atende aos propósitos de medidas preventivas será:

a) Alvos: instalações; *hardware*; *software*; arquivos; relatórios ou outras saídas emitidas pelo computador; usuários; o pessoal do processamento;
b) Vítimas: usuários; clientes; público generalizado; indústria;
c) Conseqüências: perdas financeiras; perda de reputação; perda de segurança; perda de vantagens competitivas;
d) Agentes: pessoal de direção de Processamento de Dados; técnicos em Processamento de Dados; usuários internos e externos; profissionais ou amadores do crime, atuando isoladamente ou em grupo;
e) Motivos: negligência; incompetência; fraude com o intuito de obter ganhos pecuniários ou políticos; sabotagem industrial, comercial ou política; competição comercial; atos da natureza.

Adotada a classificação acima, as condições para estudar os riscos e a decisão a adoção de medidas preventivas tornam-se melhores, pois a análise de probabilidade da ocorrência estará baseada em alvos previamente determinados.

Sistemas mais sujeitos a fraude

A ferramenta mais utilizada na burla de sistemas de informações, a fraude, pode ser conceituada como uma quebra proposital das ligações existentes entre a realidade e a sua representação manual ou automatizada, com o alvo de obterem-se vantagens direta ou indiretamente.

Nos sistemas de informação automatizados a fraude assume aspectos de uma tecnologia bastante avançada e sofisticada, envolvendo a produção de complexos sistemas de *software* e até mesmo *hardware.*

A potencialidade da fraude já aceita e admitida como um fator quase sempre presente ao meio ambiente dos sistemas, tornou-se crescente com o uso dos computadores e atua sempre com características próprias. Assim a fraude é vista:

* Manipulando indevidamente dados de entrada e saída;
* Desenvolvendo *software* para atuar junto ou em substituição aos do sistema;
* Alterando, revelando ou destruindo arquivos;
* Transmitindo, interceptando, destruindo ou desviando informações para canais diferentes da empresa;

* Diminuindo o desempenho de sistema com a finalidade de retardar o fluxo de informações necessárias à tomada de decisões, ou

* Atuando para provocar pane nos equipamentos de suporte, nas instalações, a fraude tem sido apontada como o maior perigo potencial para as atividades de um Centro de Processamento de Dados.

A enumeração acima não visou esgotar todas as características que a fraude pode assumir quando em atuação um em CPD, pos a própria caracterização constitui tarefa bastante árdua. Todavia detectá-la e impedir que desfalques ou perturbações semelhantes sejam produzidas nos sistemas computadorizados, constitui a área de trabalho da Auditoria de Sistemas.

Esta complexidade, aliada à pouca familiaridade que têm os auditores de sistemas no trato do problema ou em relação aos equipamentos de computação, tem demonstrado que são modestas as pretensões de detecção e prevenção do crime nos sistemas de informações automatizados.

Assim, embora saibamos que por si só um computador não tem possibilidade de fraudar sistemas, os CPD's sempre estarão sujeitos a atos criminosos ou ações fraudulentas, visto que sempre estará presente um processo preparado por pessoas que dirigem e alimentam o sistema.

Para diminuir a incidência destas ações, deverão ser desenvolvidos trabalhos a cargo da Auditoria de Sistemas, estabelecendo controles internos certos e em ocasiões apropriadas, onde a principal chave deve ser evitar erros ou desvios, e prover meios para corrigir problemas encontrados tão depressa quanto possível, enfim, tornando auditáveis os sistemas.

Aceito o conceito de fraude, podemos discutir os sistemas potencialmente mais volúveis. A análise quanto à vulnerabilidade aqui feita não terá por base a ausência ou ineficiência de controles visto que, via de regra, a falta de controles enfraquece todos os sistemas. O enfoque aqui será feito tendo em vista o objetivo a que se destina o sistema.

Sabemos que a introdução do computador tanto no desenvolvimento quanto na operação de sistema deve atender a fatores como: necessidade de manipular o maior número de informações, com tempestividade e correlação; atender a solução de problemas complexos, que sem a utilização do computador teriam sua solução retardada ou impossibilitada; obter rapidez de respostas aos dados que são fornecidos/emitidos de longas distâncias; em alguns casos, melhorar a imagem da empresa.

Qualquer que seja a razão motivadora da introdução do computador nos sistemas de uma Organização, ele passa a executar atividades que manipulam dinheiro, suprimento ou informações. Trabalha portanto com o "ativo" de uma Organização seja ele caixa ou outros bens.

De um modo geral, sistemas que manipulam dados relativos a finanças ou a mercadorias ou quaisquer outros instrumentos negociáveis têm sido mais comumente fraudados, existam ou não computadores no processo. Isto é normalmente feito com a emissão de faturas fictícias, reivindicações de seguros, aumento de salários, transferências de fundos ou outros créditos, etc.

Em recente estudo realizado nos E.U.A. onde foram analisados vários casos, constatou-se que os sistemas mais fraudados atendiam a controles de inventários, de pagamento ou crédito e emissão de faturas.

Outra característica interessante revelada foi que a maior incidência de fraude ocorreu nos sistemas que atendem a bancos, educação, entidades governamentais, seguindo-se outras atividades. Tal fato foi atribuído à diversidade das tarefas e ao volume a que os sistemas atendem, o que sem dúvida diminui a flexibilidade para estabelecer controles. Vale ressaltar que algumas organizações após a detecção da fraude negaram-se a revelar o montante dos valores perdidos, por medida de políticas administrativas. Então se conclui que a fraude tem registrado sua presença um sistemas nos quais o ganho ilícito pode ser obtido diretamente, ou seja, onde a disponibilidade do produto da fraude seja mais imediata e onde a participação de agentes fraudulentos seja minimizada.

As maneiras de analisarmos as estatísticas de fraude não se limitam à finalidade dos sistemas. Uma dessas, particularmente interessante para a Auditoria de Sistemas, vê a fraude nos sistemas sob dois aspectos. No primeiro são fraudes praticadas, utilizando os computadores dentro das especificações corretas, ou seja, a fraude baseia-se na manipulação dos dados para a entrada no sistema ou dele saídos. No segundo os computadores são usados de forma não prevista ou autorizada portanto em desacordo com as instruções. Neste caso situam-se as modificações de sistemas, utilitários que alteram arquivos, etc. Para estas é necessária a participação de elementos conhecedores da tecnologia de computadores.

A importância desta apreciação reside no fato de fraudes praticadas com a manipulação de dados exigirem menos conhecimentos técnicos da área de computação,que aqueles requeridos para realização de modificação em sistemas. Para a Auditoria de Sistemas as fraudes de dados são mais fáceis de detecção, uma vez que podem ser analisadas na maneira tradicional de auditagem, o que não ocorre quando há utilização de programas.

Dentro de um universo de trezentos e trinta e quatro (334) casos detectados nos E.U.A., cento e setenta e um (171) foram registrados com fraudes com apoio em *software*, cento e vinte e seis (126) como de dados e trinta e sete de natureza outra que não envolvia operação de sistemas.

Conhecidos os sistemas que potencialmente apresentam um grau de risco mais elevado, torna-se interessante analisar em que nível da estrutura organizacional as fraudes são freqüentes. Tem-se discutido que a ação criminosa ocorre junto à operação dos sistemas. Acredita-se que a premissa ocorra da aparente facilidade que os operadores de computadores possuem quanto ao acesso à máquina ou face à possibilidade de intervir no sistema através do periférico que lhe permite assídua comunicação com o sistema.

Todavia convém lembrar que para uma intervenção no sistema de aplicação por intermédio desse periférico, seria necessário que os operadores dispusessem de conhecimentos detalhados dos programas e processos em operação, além da própria habilidade de manipulá-los, o que não é comum. Com isso não estamos pretendendo afastar a possibilidade de que tal venha ocorrer, ou que tais funcionários não possam executar ações criminosas por outros métodos. Sabemos que os operadores podem selecionar outros métodos de programar fraudes sós ou em conjunto. Porém antes de os apontarmos como os maiores responsáveis, façamos algumas considerações. As organizações, sejam elas grandes ou pequenas, ao projetarem seus ambientes de operação, definem racional ou empiricamente alguns pontos de controle, com os quais seus dirigentes pretendem tomar conhecimento do estado em que se encontram os sistemas de que se servem. Não nos deteremos aqui em analisar a propriedade ou não dos controles, nem tão pouco a eficiência e eficácia. Interessa-nos registrar a existência de certo grau de controle, que via de regra atinge os empregados menos graduados da organização.

Em processamento de dados, e logicamente em sistemas automatizados, as atividades são distribuídas a diversos empregados cujas funções variam como: gerente de CPD, de departamentos clientes do CPD, supervisores de operação, analistas, usuários, programadores e operadores de sistemas.

Todos estes elementos estão alocados em diferentes níveis da Organização, onde existem controles cuja intensidade varia, ficando os níveis mais elevados com maior responsabilidade e menor controle e os níveis mais baixos com posição inversa, ou seja, mais controles e menos responsabilidades.

Aqui encontramos um novo fator bastante subjetivo e muitas vezes de difícil caracterização: a atribuição de responsabilidade às diversas pessoas envolvidas no sistema.

Tal atribuição comumente é feita em função do conhecimento que as pessoas possuem do campo onde atuam e de uma avaliação da sinceridade e honestidade que conseguem incutir nos demais integrantes da Organização. "Um homem não pode ser classificado como honesto, responsável ou desonesto, ele caminha pela vida e pode suportar certas pressões por amor a seus ideais. Mais suportará até um ponto, não mais." Ao fazer essa observação, não se fixa tal ponto. Sabemos todavia que embora não localizado de maneira uniforme, o ponto existe com graus e ocasiões diferentes e para diferentes pessoas. Estas, tendo identificado a oportunidade para fraudar e racionalizar os planos de fraude, passam a atuar.

O fator determinante que detém a ação do fraudador é o grau de controle que sobre ele é exercido. Estudos realizados por diversos autores nos casos detectados de fraude levaram a duas caracterizações: as fraudes de maior monta são praticadas por altos funcionários das empresas, onde o fator responsabilidade prepondera sobre o controle, que normalmente é fraco e inexistente; fraudes menores, mas em maior número, são realizadas em nível de entrada de dados e seus agentes são os operadores de sistemas ou usuários.

Isso refere-se a fraudadores que de alguma maneira estão ligados aos sistemas. As fraudes praticadas por indivíduos totalmente alheios aos sistemas não estão sob este enfoque, e os fatores que inibem sua prática não podem ser vistos sob aspectos de controle. Em tais casos o estímulo parte dos montantes de benefícios esperados por parte do fraudador. Os fatores econômicos que determinam as medidas de proteção são igualmente vistos pelos fraudadores em suas atuações. Devemos registrar, porém, que esta ocorrência é bem maior, visto que os controles existentes, inclusive para os níveis hierárquicos inferiores da Organização, passam a atuar sobre quaisquer entrada de elementos exógenos à empresa.

Como evitar fraudes e prejuízos ou detectar erros

Como estar imune a fraudes é tema muito importante e também polêmico. Tal questão é levantada por muitos, sempre bem intencionados e que afirmam que se não for detectada a ocorrência de fraudes ou prejuízos durante os trabalhos realizados pela equipe de auditoria, esses trabalhos não terão sido realizados a contento. Longe de questionar quem tenha tal opinião, pois, isso é uma questão de ponto de vista, e, por mais importante que seja o tema, cada um tem o seu e devemos possuir a sabedoria de respeitar o do outros, sem ter a ousadia de imaginar que o nosso seja o melhor.

A auditoria não tem função de inspecionar, não é polícia! Ela deve trabalhar segundo regras estatísticas. Não pode, nem tem condições, de examinar todas as transações ocorridas num dado sistema, num período qualquer. Podemos citar como exemplo, em um

banco, no sistema de descontos de títulos e duplicatas, o auditor pretender examinar uma a uma todas as transações ocorridas nos últimos seis meses. Ele não reúne condições humanas ou técnicas para isso. Compreendidas as dificuldades decorrestes da complexidade do sistema de computação, analisemos um pouco que medidas temos para assegurar um nível de segurança aceitável.

Um sistema de grandes proporções exige para a sua operação, uma série de programas que residem em dispositivos de armazenamento e executam todas as funções previstas para o sistema. Atuando sempre em bases privilegiadas, constituem o *software* do computador. Em outras palavras tais programas são responsáveis pela automatização dos processos previstos pelo homem e constam de milhares de instruções.

O risco de fraude, destruição ou ocorrência de qualquer reação indesejável sempre presente no desenvolvimento de tais processos, reside normalmente no fascínio que o indivíduo tem na tarefa de penetrar e comprometer o sistema, sempre com novas forma inteligentes e desafiadoras. Face a tal situação não temos ainda condições de assegurar a total salvaguarda de um sistema de computador, e impedir que algum ato lhe tire a segurança. Quanto maiores os sistemas em razão de sua própria complexibilidade, mais difícil é a implantação de testes que cubram sua totalidade. Mesmo assim a necessidade de segurança subsiste e medidas que garantam a integridade e fidedignidade são exigidas.

A segurança para um sistema de computador deve ser vista sobre três aspectos:

- Segurança física na qual tratamos das medidas que proporcionarão proteção e controle às áreas onde se desenvolvem os trabalhos de processamento; Aqui se incluem todos os equipamentos e dispositivos de suporte;
- Segurança operacional onde nos ocupamos do controle e proteção dos processos e pessoas envolvidas. Duplo controle, divisão de trabalho e responsabilidade, manutenção de cópias de dados e instruções importantes, relação de deveres e as proibições, métodos de desenvolvimento de sistemas, de verificação, de eliminação de dados inaproveitáveis, e inservíveis, controles de bibliotecas do sistema, documentação adequada e atualizada;
- Segurança do computador onde estudamos as medidas de proteção a componentes eletro-eletrônicos, sistema de lógica, sistema operacional e circuitos de comunicação. Senhas para usuários, criptografia de dados que transitam, autorizações para uso excepcional, redução do contato de tempo real de pessoas com o sistema são pontos comumente abordados nesta proteção.

Portanto, a proteção mais aconselhada consiste no estabelecimento de processos de prevenção e disuasão que evitam atos indesejáveis que possam resultar em prejuízo. A existência ou constatação de eventos prejudiciais deverá desencadear processos que impeçam a continuação da ocorrência e determinem imediata recuperação das perdas ocasionalmente sofridas.

Assim a principal proteção aos sistemas de computadores poderá ser feita com o desenvolvimento de planos de segurança que atuem em função de alvos, vítimas, conseqüências, agentes e motivos.

Em alguns países a proteção a sistemas de computadores já encontra legislação que permite a execução de seguros como o ato de reparação aos prejuízos sofridos. Tais seguros cobrem os danos decorrentes de atos praticados contra processamento de dados mesmo que os agentes sejam seus próprios integrantes. Onde tal prática for possível é aconselhado o seu uso.

Entretanto, todas as medidas envolvem altos custos cuja determinação deve ser feita quantificando-os em função dos valores a salvaguardar, a fim de não cairmos em uma paranóia quanto à segurança. Os problemas de segurança são antes de tudo um problema humano cuja proteção técnica poderá estar em reduzir a confiança e fragmentar o conhecimento especializado do sistema; porém a necessidade de um grupo do qual é exigido alto grau de integridade e confiabilidade, devido ao conhecimento que tem do sistema, sempre se fará sentir.

No trabalho de estabelecimento de um plano de medidas de segurança, devemos pensar como o inimigo, o fraudador, enfim o provocador do ato indesejável, pode agir. O Instituto de Pesquisas de Stanford desenvolveu um método que determinou " Análise das possibilidade de ameaça" onde a análise de valores, ameaças e riscos decorrem do desenvolvimento de cenários, onde tais problemas são retratados. O êxito de tal análise fica muito dependente do conhecimento e da experiência real que se tenha sobre o assunto.

Outros tipos de análises das medidas se segurança podem ser feitos. Em todos eles devemos destacar dois fatores importante:

a) determinação do impacto que sofrerá o sistema com a ocorrência da ação indesejável;
b) determinação da probabilidade de ocorrência no campo e espaço.

A probabilidade de ocorrência certamente será mais difícil determinar com confiança se comparada com a medição do impacto que tem a ação sobre o sistema, principalmente porque estamos acostumados a julgamentos subjetivos quando tratamos do

assunto, e a sua formalização torna-se bastante difícil. A ocorrência de impactos catastróficos porém de baixa probabilidade, respondem pelo grau de dificuldade normalmente encontrado quando da determinação da probabilidade.

Em resumo, alguns pontos que devem ser abordados na avaliação das medidas de proteção e segurança são:

- **Redução de risco** – Toda e qualquer medida sugerida deve possibilitar a redução de risco.
- **Custo e redução da eficiência** – Deve ser sempre efetuada a avaliação da medida de proteção em função do investimento necessário à sua implantação, manutenção, à possível queda de eficiência dos sistemas.
- **Desconfiar da segurança do sistema** – Admitir sempre a possibilidade de que o sistema pode não estar seguro.
- **Compartimentalização** – Considerar medidas que circunscrevam os problemas às áreas afetadas, não permitindo o enfraquecimento de áreas adjacentes.
- **Isolamento** – Considerar medidas que estabeleçam os fluxos de áreas sensíveis sem interferências.
- **Instrumentação de vigilância** – A medida adotada deve ser vigiada e instrumentada a fim de permitir observações das tentativas de violações.
- **Completeza e consistência** – Toda medida de segurança deve ser completa e consistente em relação às suas especificações, funcionamento de preferência sem intervenção humana.
- **Determinação da tolerância** – Deve-se obter a aceitação pelo grau de limitação que ela impõe.
- **Continuidade** – Deve permitir funcionamento continuado e não apenas quando de sua implantação.
- **Fiscalização** – Toda medida deve ser fiscalizável, ou seja, deve permitir testes a fim de assegurarmo-nos de seu adequado funcionamento.
- **Apoio ético e jurídico** – As medidas adotadas devem vigir sem impor constrangimento.
- **Desconfiança interna** – As medidas devem sempre prever um ambiente hostil.
- **Previsão dos efeitos secundários** – As medidas antes de serem adotadas devem ser examinadas quanto aos efeitos negativos que podem trazer.

TÉCNICAS DE ABORDAGEM PARA A AUDITORIA DE SISTEMAS

Auditoria Intra-sistema

A literatura de auditoria para sistemas automatizados apresenta dois enfoques básicos de abordagem, cuja variação reside na maneira de como é feita a verificação dos sistemas:

Os dois enfoques podem ser assim conceituados:

a) auditoria intra-sistemas onde a preocupação é verificar e revisar os processos;
b) auditoria extra-sistema cuja preocupação é verificar a eficiência e eficácia dos métodos operacionais do CPD.

A adoção de prioridade para uma ou outra abordagem decorre de decisão administrativa, uma vez que não constituem trabalhos mutuamente exclusivos e sim complementares.

Os trabalhos de uma auditoria intra-sistema para sistemas automatizados apresentam variações que decorrem do grau de detalhe com que é feita a análise do processo.

Dentro de tal conceituação existem as seguintes variações:

a) Verificação dos resultados. Nestas auditagens o objetivo é verificar se os resultados são realistas com relação aos dados-fonte. Esta variação é conhecida como "em torno do computador".
b) Verificação da correção dos programas: Constituem a auditagem discretamente dirigida para análise de programas e verificação do que os procedimentos deveriam fazer para atenderem corretamente as exigências e necessidades do usuário. Neste trabalho esta variação de auditoria intra-sistema é apresentada "através do computador".
c) Verificação da execução: São auditagens programadas para contínua análise dos programas constando que os sistemas em produção operam tal como foram propostos. Neste trabalho esta variação é tratada como "com o computador".

Auditagem de sistema "em torno do computador"

A auditagem em torno do computador tem sido mais comum e mais difundida. Tal fato decorre da familiaridade que tem o auditor em lidar com verificação dos resultados onde não lhe é requerido nenhum conhecimento técnico adicional ao que ele já dispõe como profissional de auditoria. Neste caso o auditor testa o sistema selecionando transações que

tenham sido previamente processadas. Tais transações, tidas como representativas de documentos-fonte, produziram após algum processamento relatórios intermediários ou finais que estarão então sob exame. Constitui uma análise estática de uma determinada situação. Esse tipo de auditagem deixa à margem uma grande faixa de atividades que constituem o processo que trabalha os dados-fonte, e que são potencialmente centro de risco em Centros de Processamento de Dados.

A auditagem considera que se o documento-fonte pode ser aprovado correto, via de conseqüência o sistema que o processou também está correto. Mesmo sendo uma verificação estática poderá exigir do auditor a criação de alguns fluxos ou diagramas ou uso de pacotes que lhe permitam a seleção dos dados e comparação após sucessivos processos. Neste caso os pacotes são igualmente vistos como autênticas caixas pretas, onde o conhecimento do auditor é exigido apenas para fornecer parâmetros de seleção.

As vantagens encontradas para utilização de tal auditagem podem ser resumidas como:

a) não exige treinamento especializado na área de computação para o trabalho do auditor;
b) torna praticamente nulo o tempo de setup.

Já como desvantagem podemos citar:

a) baixo nível de confiança nos resultados;
b) condição para determinar períodos ou série, se constituem normalmente em árdua tarefa;
c) os exemplos selecionados podem não estaticamente válidos;
d) pode ser praticamente impossível a verificação do universo;
e) é impedida a revisão do processamento como um sistema.

A aplicação da técnica de auditagem "em torno do computador", deixa à margem as faixas do sistema que envolvem o *software* e o Centro, fazendo com que grandes riscos sejam assumidos consciente ou inconscientemente. O não exame da correção de todos os componentes de todo o sistema baseados na suposição de que os mesmos não apresentam variações de comportamento revela-se a maior falha. A tal fato acrescenta-se a impossibilidade do auditor atestar a validade dos processos de controle.

Auditagem de Sistemas "através do computador"

O objetivo desta abordagem consiste em verificar a correção dos programas através de documentos-fonte, que submetidos a processamento, fornece relatórios

intermediários ou finais que devem estar de acordo com os previamente determinados. Procura-se com tal técnica conhecer que procedimentos e controles existem na operação do sistema.

A premissa aceita é de que os resultados podem ser considerados corretos e aceitos se as entradas e resultados de processamento são julgados certos.

Nota-se a existência de um certo grau de preocupação entre determinar qual será o produto do sistema face às condições predeterminadas do auditor.

As vantagens para o emprego desse tipo de auditagem são:

a) os programas sofrem alguma verificação, ocasião em que se pode determinar sua correção e sentir o seu desempenho;
b) o sistema (computador) é utilizado para certificar certas partes do trabalho, face à realização dos testes com programas;
c) exige que o auditor dedique a atenção a certos aspectos do controle, principalmente quando os testes revelarem tratamento dos dados de execução.

As desvantagens:

a) controles apropriados devem ser desenvolvidos para impedir que no período de auditagem os arquivos sejam destruídos por manuseio inadequado;
b) o sistema não pode ser verificado em seu todo;
c) cálculos manuais para predeterminar resultados podem ser estafantes e apresentarem por isso mesmo incidência de erros;
d) não assegura que determinado programa seja o usado durante todo o período;
e) pode causar prejuízos a todo o sistemas se operações forem incorretamente executadas.

A auditagem "através do computador" já envolve uma nova visão de auditagem de sistemas. Porém nos grandes sistemas ela consome muito tempo, gasto para testar transações, a fim de poder, com segurança, fornecer informação sobre a exatidão dos registros e dados.

Freqüentemente as transações selecionadas incluem o não usual, o que resulta no manuseio de execuções, com conseqüentes riscos face à alteração de critérios que regem as mesmas execuções. O resultado desta auditagem poderá não assegurar que a realização de um particular teste, reflita exatamente o processo presente no sistema ou o que dele se espera.

A concentração da auditagem é dirigida para realização de testes de programas que produzem os registros que estarão sob exame, para se afirmar a propriedade e exatidão. Entende-se que os resultados podem ser dados como corretos para os dados que foram

fornecidos, o processamento estará correto. A auditagem assim procedida não garante confiabilidade quanto ao software utilizado face à possível troca dos programas em uso.

Auditagem de sistemas "com o computador"

O escopo da auditoria de sistema com o uso de computadores consiste na utilização de *software* para a realização das tarefas, praticando uma verificação contínua da execução dos processos. Tal *software* pode ser obtido pelos seguintes meios: programas desenvolvidos pelo próprio usuário, programas escritos sob supervisão de grupos de auditoria e programas generalizados para auditoria.

A escolha do processo para obtenção do software já envolve algumas considerações: ao utilizar os programas escritos ou desenvolvidos pelo usuário, o auditor deve estar ciente que utiliza software produzido internamente, para o qual há necessidade de testes e, aplicação de auditagem para a fase de desenvolvimento. O grau de confiança destes programas repousará em grande parte na credibilidade dada às instalações do CPD.

Já a utilização de programas escritos sob a supervisão de grupos de auditoria de auditoria, embora possam ser *software* desenvolvidos com objetivos perfeitamente definidos, deve ser visto e analisado quanto: a linguagem-fonte adotada nos programas; o conhecimento de processamento de dados por parte dos auditores; competência comprovada no desenvolvimento de sistemas; capacidade técnica e operacional para prestar assistência continuada; documentação existente atualizada e de fácil entendimento e a portabilidade do *software*.

Para os programas generalizados de auditoria devemos ter em mente que constitui *software* desenvolvido para atender a múltiplos objetivos e funções. Estes programas atendem a uma grande variedade de sistemas, o que lhes pode trazer uma razoável diminuição de desempenho. Sobre tal *software*, excetuados os cuidados sobre a competência em desenvolvimento de sistemas, vez que a grande parte é desenvolvida por *software-house*, ou seja, casas especializadas no produção de programas, devemos ter as mesmas preocupações previstas para os programas escritos por grupos.

As vantagens para este tipo de auditagem podem ser alinhadas como:

a) expansão do escopo de Auditoria com a realização de um maior número de revisões;
b) maior salvaguarda para os programas em uso;
c) possibilidade de analisar o desempenho do software ;
d) melhor definição do universo a ser examinado;
e) possibilidade para utilizar a técnica de simulação;

f) possibilidade de treinamento de auditores nas atividades de processamento de dados;

g) *feedback* que permite melhor analisar as discrepâncias.

Já as desvantagens para esta abordagem podem ser vistas como:

a) existência de grandes recursos humanos e de equipamentos;

b) possibilidade de exigir grande consumo de tempo de máquina.

A técnica permite que se faça uma auditoria mais profunda nos processos que se desenvolvem em um Centro de Processamento de Dados. A desvantagem apresentada como excessivo uso de tempo de máquina, poderá ser surpresa desde que a tarefa analisada sobre o aspecto custo/benefício, demonstre principalmente o alívio das tarefas manuais a cargo da auditoria ou equipe que lhe preste suporte.

Auditoria Extra-sistema

A auditagem extra-sistema caracteriza-se pela atenção voltada para o Centro onde se desenvolvem os processos. Nesta auditagem são vistos os procedimentos que se relacionam com:

a) utilização eficiente dos recursos humanos;

b) atendimento às políticas administrativas da Organização;

c) práticas operacionais;

d) exercício da segurança com vistas à proteção física e divisão de responsabilidades;

e) documentação existente para exame de sistemas em desenvolvimento, revisões em sistemas desenvolvidos, eficiência na utilização dos equipamentos, racionalização e eliminação de relatórios.

Como vantagens desta auditagem poderemos apontar a possibilidade da verificação de objetivos independentes existentes em um CPD, por pessoas especializadas em controle de rotinas ou atividades.

Já como desvantagem teríamos a apontar que para a auditagem de itens ou pontos específicos de um CPD, não bastariam conhecimentos relativos a controles e sim exigiria um extensivo grau de conhecimento de sistemas de computadores, afora os conhecimentos específicos de auditoria.

Ao contrário da abordagem intra-sistema a auditagem extra-sistema se preocupa com a gerência administrativa dos Centros de Processamento de Dados, abstraindo qualquer verificação de processos e dados. Face a isto achamos que a auditagem extra-sistema constitui o necessário complemento às tarefas de auditoria intra-sistemas em qualquer de suas abordagens. Convém registrar ainda que qualquer que seja o enfoque dado às auditagens intra

ou extra-sistemas, os trabalhos podem ser desenvolvidos ou aplicados por equipes de auditoria que pertençam às próprias organizações ou sejam por elas contratadas. Isto leva à observação da existência de dois grupos que praticam a atividade: auditoria interna e auditoria externa.

Convém registrar logo ao início que esta não se aplica com exclusividade às atividades de processamento de dados. O conceito mais simples e aceito para diferenciação dos dois tipos de auditoria, consiste em determinar se os auditores pertencem ao quadro da empresa onde exercem atividade (auditoria interna) ou se constituem grupos independentes, firmas especializadas que são contratadas para execução de auditagens. Ao lado desta conceituação há que se considerar igualmente um outro ponto de capital importância, que pode ser entendido como as pessoas ou requisitos a que se destina o trabalho de auditagem.

Concluímos então que as auditorias internas ou externas não são atividades mutuamente exclusivas ou representam trabalhos que se superponham.

Auditoria Interna e Externa

A auditoria interna de qualquer organização constitui uma função que é exercida por elementos pertencentes à própria organização. Isto faz antever que a sua linha de subordinação hierárquica deve situar-se o mais próximo do ápice da pirâmide administrativa. Esta exigência decorre do seu maciço envolvimento em processos que se desenvolvem em todas as áreas da organização, e para os quais há de existir necessidade do estabelecimento de procedimentos-padrão e revisões freqüentes para atestar correções. O não entendimento desta norma poderá indicar não só a dependência hierárquica a níveis inferiores, mas um impedimento de auditagem dos órgãos de posição hierárquica superior. Admitindo a sua localização no nível mais próximo das cúpulas administrativas, sua situação de empregados da empresa pode tirar-lhes a completa liberdade que necessitam para o desempenho de suas tarefas, inibindo alguns aspectos de fiscalização o que reduzirá em muito a eficiência de uma boa auditagem.

Todavia se atentarmos para o aspecto do conhecimento mais profundo que podem ter tais elementos, da Organização a que pertencem, veremos que o trabalho de uma auditoria interna permite, quando atuando dentro de determinados padrões, conseguir uma eficiente participação quanto ao trabalho para sugerir controles que devem ser incluídos no desenvolvimento de novos sistemas, assegurar que a auditoria se sistemas para computadores seja realizada mesmo antes do sistema tornar-se operacional, prover detalhados testes para sistemas, prover a inclusão de controles específicos para entradas e saída, verificação de

arquivos, verificação dos padrões de documentação e determinação de procedimentos operacionais e de backup.

O nível de envolvimento nestes problemas exige intensa participação dos auditores em todas as fases dos sistemas, principalmente no que se refira a projeto e desenvolvimento de sistemas, estabelecimento de planos de controles de testes dos sistemas antes de se tornarem operacionais, estabelecimento de controles quando alterações de programas e avaliação e verificação dos sistemas em produção e tarefas de suporte.

Diríamos em resumo que os trabalhos de uma auditoria interna respondem às necessidades que têm os gerentes e outros níveis de chefia de conhecer o comportamento dos sistemas sob sua responsabilidade.

As relações de uma organização não são orientadas somente para si mesmo. Participando do seu relacionamento com acionistas, governo, entidades financeiras ou empresas similares envolve aspectos para os quais há necessidade de que os mesmos controles atribuídos internamente sejam vistos e aceitos por elementos estranhos à organização. Temos então a auditoria externa.

Da mesma maneira que definimos a auditoria interna, a análise aqui apresentada estará restrita às atividades de auditoria de sistemas computadorizados.

Os elementos que desenvolvem esta tarefa são independentes à organização e devem possuir grandes conhecimentos da área onde atuam e desempenham o seus trabalhos, atendendo a fases ou a pontos específicos sobre os quais apresentam relatórios ou pareceres de forma abrangente ou restrita.

Embora independentes na sua maneira de trabalho e quanto à hierarquia da organização, os executores das tarefas de auditoria externa conduzem suas atividades atendendo a padrões determinados por normas de associações que os credenciam para o exercício da função.

O trabalho destas equipes visa primordialmente atestar a adequação dos sistemas em uso à legislação vigente; fornecer relatórios e certificados que dão fé para o ambiente externo de que o desempenho dos sistemas da empresa são adequados, eficientes e eficazes; apresentar e introduzir na empresa específicos conhecimentos técnicos postos à disposição da área de sistemas, cujo suporte interno não possuía ainda o conhecimento e implementação; apresentar sugestões para melhoramento para o próprio programa de auditoria interna.

Para a execução destas tarefas os auditores externos apoiam seu trabalho em um *staff* interno da organização comumente visto na auditoria interna; tal fato reside na necessidade de suprir o pouco conhecimento que as equipes externas têm das empresas onde

atuam, necessidade esta que deve ser atendida para um perfeito atendimento das tarefas que lhe são cometidas.

Diríamos em resumo que a auditoria externa visa atender a empresa quanto a exigências legais atestando a coordenação e completeza dos dados para as entidades externas ou possibilitando a aquisição mais rápida de conhecimentos especializados postos a disposição na área onde atuam. Podemos portanto dizer que as auditorias de sistema interna e externa não se duplicam no desempenho de suas atividades. Em muitos dos casos é registrada até a presença das duas. A complementaridade dos dois grupos apresenta até vantagens para as organizações, pois se de uma obtemos a certeza da correção dos processos e dados, da outra usufruímos a certificação externa e os conhecimentos especializados mais recentes. Vale ressaltar que em nenhum momento procuramos analisar as características que devem ter os auditores, quer sejam legais ou técnicas, visto considerarmos que o desempenho das funções por pessoas não qualificadas significa a completa falha de toda tarefa aqui analisada e exposta.

MÉTODOS E FERRAMENTAS DISPONÍVEIS PARA AUDITORIA

Hoje em dia, além do desenvolvimento encontrado no campo da auditoria de sistemas, podemos considerar também grande o número de métodos e ferramentas que dão suporte à realização dos trabalhos de auditar sistemas informatizados.

A seleção e adoção de qualquer um deles é encontrada sempre condicionada ao nível de experiência e conhecimento que possuem os auditores e profissionais de processamento de dados, e ao grau de sofisticação de que dispõe o Centro de Processamento de Dados e a área a ser atendida. Em cada caso, o método ou ferramenta utilizado não decorre simplesmente do grau de sofisticação existente em cada Centro, mas é igualmente função da área de trabalho que atende no Centro de Processamento. Este tratamento será aqui mantido quando da apreciação de cada método ou ferramenta, não porque a auditoria deva assim ser exercida, mas para atender a uma maior clareza e facilitar a comparação. Assim a apreciação dos métodos ou ferramentas são agrupados conforme a área que atendem ou dão suporte. São eles:

a) Preparo de planos e seleção de sistemas ou de áreas que deverão ser auditadas;
b) Auditagem dos sistemas de aplicação em operação;
c) Auditagem do Centro de computação (instalações, serviços auxiliares, etc...);
d) Auditagem dos sistemas de aplicação, em desenvolvimento ou manutenção.

Examinaremos aqui cada método ou ferramenta dentro do conjunto de atividades a que servem, procurando dar uma visão rápida, mas ao mesmo tempo abrangente do que representa para a auditoria de sistemas. Os métodos apresentados devem ser vistos sempre como atividade automatizada, enfoque que admitimos com o objetivo de otimizar o uso de recursos disponíveis dos centros e da auditoria. Isso porém não os invalida se fortes impedimentos o aconselharem para execução manual.

A apreciação de custos será otimizada, visto que para qualquer dos métodos ou ferramentas tal análise deve ser feita à luz do binômio custo/benefício, elementos que variam em cada Organização, e situação específica.

Seleção de sistemas ou áreas para auditar

A seleção de sistemas ou áreas nos quais se concentrarão as atividades de uma auditoria de sistemas deve constituir a tarefa inicial de todos os trabalhos.

Há casos em que os sistemas ou áreas a serem auditados são selecionados em função dos problemas ou prejuízos que já se fizeram notar. Em tais situações os objetivos dos trabalhos são entendidos como correção de métodos de trabalho, com forte inclinação para apuração de responsabilidades, ficando a tarefa de assistência relegada a um plano secundário. Em tais situações, embora sejam grandes os esforços, os resultados não se mostram muito compensadores. A explicação para isto é que os controles e ajustes de correção são aplicados a pontos que normalmente não correspondem à origem real dos problemas. Acresça-se, ainda, uma auditoria que trabalha em tais condições sempre atua pressionada, o que não lhe permite a realização de completa análise de todos os fatos que ocorrem nas áreas ou sistemas.

Auditoria de Sistemas, movida pela necessidade de racionalizar e obter resultados que lhe dêem mais confiabilidade e segurança, desenvolveu entre outros os métodos de: atribuição de pontos "escore" para determinar a procedência e a seleção por análise de matriz construída com indicadores-chave do sistema ou área.

Método de "escore"

O método do escore visa estabelecer um planejamento onde as atividades se ajustem em relação de precedência, em função do potencial de riscos que podem trazer para as organizações. Isto permite que seja obtida a máxima eficiência no uso dos recursos da auditoria.

Trabalhando com índices previamente fixados para cada sistema, o "escore" quantifica as características significativas de cada sistema mediante atribuição de pontos que,

combinados com pesos, fornecem uma maneira objetiva de aplicar a prioridade das aplicações ou áreas a serem examinadas em termos de potencial de riscos.

O procedimento para aplicação do método pode ser visto considerando cinco etapas:

a) determinação de indicadores-chave para o CPD. Esta tarefa é feita através da elaboração de uma lista que, em período determinado, traduz as atividades desenvolvidas em cada sistema. Nesta etapa é importante verificar o grau de intensidade da cada tarefa. Exemplos de tais indicadores podem ser vistos como:

   i) importância do sistema para a Organização;

   ii) sistema batch ou on-line;

   iii) números de pessoas envolvidas;

   iv) arquivos utilizados;

   v) ligação com outros sistemas;

   vi) esforço de manutenção;

   vii) número de programas previstos ou em uso no sistema;

   viii) vulnerabilidade do sistema;

   ix) envolvimento do sistema em controles financeiros;

   x)outros julgamentos importantes para a instalação.

Na fixação e determinação dos indicadores devemos procurar agrupá-los quanto a pontos como criticidade do sistema ou área, custos/benefícios decorrentes, etc.

b) Completada a lista de indicadores o método prevê uma avaliação individual por parte dos envolvidos no trabalho, para cada sistema ou área do CPD. Logicamente sendo uma avaliação pessoal é pouco provável que seja obtida igualmente. Se tal fato não apresentar grandes discrepâncias não trará nenhum prejuízo na determinação da precedência;

c) O trabalho a ser desenvolvido nesta etapa consiste na manipulação da avaliação por algum algoritmo, elaborado pelo auditor, onde fatores de pesos previamente fixados, para cada indicador e suas variações, permitam obter um escore para cada característica importante do sistema ou área;

d) Nesta etapa a tarefa é manipular ainda com o algoritmo os fatores dos grupos de indicadores formulados na primeira etapa, considerada sua situação quanto a: criticidade do sistema ou área; custos/benefícios decorrentes; necessidade de auditoria; outros critérios de agrupamento. Tal procedimento visa estabelecer o grau de importância ou determinar o grau de vunerabilidade do sistema ou área.

e) A última etapa de trabalho do método se resume em aplicar ou julgamento. Deste julgamento decorre o plano de auditagem apoiando na relação de precedência obtida para sistemas ou áreas. Os sistemas que obtiverem um número mais alto no escore são os indicados para serem os primeiros a serem auditados.

As principais dificuldades para aplicação do método podem ser apontadas como as dificuldades na identificação dos indicadores; atribuição do peso como fator para ponderar a variação dos indicadores; atribuição do peso para grupos indicadores; além da necessidade de julgamentos arbitrários quando da avaliação feita para cada indicador, vez que em muitos deles é exigido conhecimento que só é adquirido no trato com problemas de computação, e da empresa.

Mesmo diante de tais dificuldades o método permite rápida implementação, uma vez que não apresenta alto grau de complexidade na programação de seu algarismo e muitos dos dados podem ser extraídos de sistemas que controlam os custos de desenvolvimento e operação existentes em cada Centro.

Face à própria facilidade de implementação, o método requer pouco tempo de preparo e os resultados podem ser colhidos a curto prazo.

Convém, todavia, registrar que o método pode conduzir a uma tendência de mais quantificar os benefícios em prol de auditoria, ao invés da obtenção de melhor qualificação de suas tarefas. Isto decorre da determinação das características a serem usadas, pesos e outras combinações que constituem o ponto crítico do método. Face a isto chamamos atenção dos auditores para tratar com bastante clareza o que eles estão tentando medir e a que resultados pretendem chegar.

Método de seleção por análise de matriz

As organizações onde o processamento de dados é descentralizado apresentam um novo aspecto que deve ser examinado e definido com bastante clareza, quando da seleção de áreas de atuação, traduzido na escolha do subcentro que deve ser auditado.

A importância desta atenção caracteriza-se pelo fato de subcentros de computação constituírem-se em áreas que desempenham, via de regra, todas as atividades de um CPD ou operam sistemas, podendo, portanto, responder por grandes prejuízos face à maneira com que desempenham suas tarefas. Esta preocupação propiciou o desenvolvimento do método de seleção por análise de matriz, que aqui chamaremos de método "matricial". Este consiste em coletar dados financeiros e operacionais de sistemas previamente escolhidos em cada subcentro da organização e submetê-los a uma análise e avaliação conjunta. Tais informações

são transpostas como dados de uma matriz e são avaliadas e julgadas. Isto possibilita uma fácil comparação de comportamento entre as diversas instalações da Organização, ou entre padrões estabelecidos e dados coletados.

Embora o método matricial seja indicado para aplicação em organizações com processamento, nada impede que seja utilizado em instalações descentralizadas. Apenas em tais casos o confronto dos dados coletados deverá ser feito com indicadores de desempenho estabelecidos como padrão, ou com indicadores históricos do mesmo centro.

Igualmente como vimos quando na análise do método "escore", o "matricial" visa melhorar a eficiência das operações de auditoria e permitir a aplicação dos recursos nas áreas onde o potencial de risco for mais alto. Neste método parte dos dados fornecidos para implementação pode advir de relatórios gerenciais já existentes na Empresa e em contrapartida os obtidos por exigência de sua aplicação servem às gerências para melhor conhecer as atividades sob seu comando.

Os procedimentos para implementação incluem três etapas:

a) Seleção de indicadores – A determinação de indicadores financeiros ou operacionais a serem utilizados na avaliação de desempenho de cada subcentro ou área deste, constitui a primeira etapa da tarefa. Como fator determinante o indicador financeiro deve responder ao potencial de risco de uma área ou centro. Já nos indicadores operacionais a ênfase é dada à eficiência em controles e consecução dos objetivos.

b) Atribuição de pesos – Atribuir pesos para indicadores financeiros e operacionais constitui o passo seguinte a que todos os envolvimentos no trabalho de seleção devem atender. O peso deverá refletir o risco que o indicador representa para a organização.

c) Desenvolvimento do programa para montagem da matriz – O sucesso do método reside na análise que é feita sobre a matriz em função dos dados extraídos dos sistemas. Para as atividades de desenvolvimento de sistema ou manutenção, os indicadores podem ser obtidos de sistemas que controlam os custos operacionais ou de desenvolvimento de que cada centro dispõe.

Os relatórios fornecidos pelo programa que manipula a matriz devem atender a:

i) grau de cada indicador comparado com o desempenho-padrão pré-estabelecido;

ii) estudo comparativo, do desempenho obtido por cada centro ou área englobando todos os indicadores;

iii) estudo do comportamento dos dados coletados para cada indicador dentro de determinado período, consignando-se a percentagem alcançada dos objetivos inicialmente propostos, por área ou sistema.

Para a obtenção de um bom desempenho do método matricial é desejável que a organização tenha um alto grau de integração dos sistemas automatizados, cobrindo as diversas áreas de aplicações, a fim de permitir a obtenção de informação diretamente de tais sistemas. Este método atende bem a instalações sofisticadas e on-line face à medição através de indicadores operacionais que cada sistema fornece. Face a tal situação o método requer para sua implementação um elevado grau de conhecimento em processamento de dados por parte dos auditores.

Igualmente importante á a aptidão para selecionar os indicadores na massa de informações que geralmente flui dos diversos sistemas, o que exige um extensivo conhecimento de todas as aplicações que se desenvolvem no centro, aliado a razoáveis conhecimentos de auditoria.

Vale registrar que os indicadores devem ser extraídos de preferência dos sistemas em operação, tornando-se desnecessário desenvolver uma coleção de dados que possibilite a montagem da matriz para análise, o que sem dúvida reduz o tempo de implementação que fica restrito a:

a) força de trabalho formada para determinar os indicadores e especificar os dados a serem coletados; e

b) força de trabalho necessária à programação de montagem e análise da matriz.

No que se refere a operação o método utiliza os recursos existentes em qualquer dos subcentros em serviço na Organização sendo aconselhada a utilização das instalações que apresentarem maior disponibilidade de horário.

Assim o método permite estabelecer eficientes e confiáveis planos de auditoria, onde os recursos são convenientemente alocados, face à maior ou menor concentração de riscos em subcentros, sistemas ou áreas. Todavia o conjunto de registros aconselháveis, traduzido por um alto grau de automatização e extensivos conhecimentos de processamento de dados por parte dos auditores coloca o método além das possibilidades de muitas organizações.

Auditagem de Sistemas de Aplicação em Operação

A operação dos sistemas de informação automatizados constitui-se em uma das áreas críticas do trabalho dos auditores, visto que dela decorrem mais diretamente a correção e

completeza dos resultados dos dados processados. A tarefa dos auditores nesta área pode ser analisada em seis fases:

1) Origem das transações – Entendemos nesta fase todo o preparo ou trabalho executado antes de os dados serem alimentados para o sistema.
2) Entrada de dados – Fase que inclui a manipulação dos dados-fonte para a alimentação do sistemas seja para a operação batch ou on-line.
3) Comunicação de dados – Os trabalhos pertinentes a esta fase revelam-se como controles no sentido de assegurar a completeza e integridade do fluxo de dados entre terminais remotos e o Centro.
4) Processamento do sistema – Controles de validade, integridade do processamento, correção no uso de programas e fluxos, processos de recuperação, constituem as tarefas que devem ser verificadas nesta fase.
5) Armazenamento e recuperação de dados – Fase em que são vistos os processos de manipulação, com os arquivos fora do computador.
6) Processamento dos relatórios – Fase que trata do exame dos processos que manipulam os relatórios fornecidos pelo sistema, a fim de assegurar correção e completeza de todos os elementos fornecidos pelos sistemas. Aqui incluem-se as rotinas manuais de distribuição dos relatórios.

Para atendimento da verificação de tais tarefas a auditoria de sistemas conta caom alguns métodos entre os quais: módulos, ou critérios embutidos no *software; software* generalizado para auditores; controle por fluxogramas; seleção de dados para teste, entre outros.

Módulos ou critérios embutidos no *software*

O método consiste basicamente na inserção de elementos que sirvam aos objetivos da auditoria nos programas que compõem o sistema. Tal inserção pode envolver três itens básicos:

- módulos completos para manipular dados;
- parâmetros que indiquem critérios na seleção de dados;
- comandos padronizados disponíveis em algumas linguagens de programação.

A inserção de tais elementos deve sempre atender a critérios que, preferencialmente, são estabelecidos ao tempo de desenvolvimento dos sistemas. Não se considera, todavia, exigência obrigatória. Alguns auditores defendem a idéia de que, se os requisitos necessários à auditoria forem inseridos no sistema somente quando estiver em

operação, será obtida uma maior flexibilidade. Tal procedimento não pode possibilitar uma maior flexibilidade pois trará maior risco à integridade do sistema e obrigará a realização de uma nova fase de testes para atestar-se sua correção.

Os dados fornecidos pelos programas em atenção ao processamento dos dados por tais módulos, atendimento a critérios ou comandos padronizados, constituem arquivos que podem ser reformulados, classificados, resumidos ou simplesmente impressos para os trabalhos de análise e avaliação.

Os procedimentos para implantação do método resumem-se a cinco etapas de trabalho:

1) Fixação de requisitos – Tal trabalho constitui tarefa a ser desenvolvida pelo auditor que determina o que deve ser cumprido para atender às necessidades da auditoria de sistemas. Nesta ocasião identificados dados, freqüência com que são exigidos, volumes e flexibilidade.
2) Projeto funcional – Nesta etapa, à luz do fluxo do sistema o auditor seleciona onde deverão ser embutidos módulos, parâmetros, ou outras instruções, determinando igualmente as condições em que tais elementos devem atuar. A etapa favorece igualmente a revisão das especificações do sistema, para assegurar os requisitos de entrada e saída impostos aos dados estão corretos.
3) Detalhamento do módulo, codificação – Atenção especial deve ser dada nesta etapa, a fim de que o detalhamento dos requisitos do módulo não venha prejudicar o plano, face ao nível muito particular dos detalhes, o que geralmente provoca um grande volume de informações de valor irrelevante. Quando ao trabalho de codificação pode ser facilmente absorvido pelas equipes de programação e análise e não deve apresentar maiores preocupações.
4) Teste do sistema – Considerando que a inclusão de módulo ou outros elementos nos programas são da responsabilidade dos auditores, é necessário assegurar a participação de auditores na fase de testes do sistema ou programa, a fim de assegurar que os requisitos estão sendo cumpridos, e não se constituirão em embaraços aos sistemas de aplicação.
5) Manutenção – O método de embutir módulos ou outros elementos para atender as exigências da auditoria obriga a que os auditores acompanhem as mudanças dos requisitos gerais do sistema após sua implantação ou quando sejam necessárias manutenções. Para tal em que pese poder ser o trabalho atendido pelas equipes de manutenção de processamento de Dados, há necessidade de que a auditoria

mantenha uma documentação completa, atual e compreensiva dos sistemas de aplicação em operação.

O emprego do método de embutir elementos que atendam a auditoria nos programas de aplicação exige inicialmente um grande esforço que pode ser traduzido no tempo exigido para desenvolver e implementar a programação. Nos sistemas em uso e que foram desenvolvidos sem o auxílio do método aconselha-se que a política de implementação fique condicionada às necessidades de manutenção dos sistemas. O esforço da auditoria estará tremendamente reduzido ao tempo em que o método estiver atingindo a totalidade dos sistemas.

O sucesso do método é bastante condicionado ao entrosamento existente nas organizações entre os auditores e profissionais de processamento de dados. Para facilitar o relacionamento é exigido que o auditor possua extensivos conhecimentos de processamento de dados, da estrutura dos sistemas de aplicação e de desenvolvimento de sistemas e programação.

Em contrapartida o método permite:

- atender com eficiência a auditoria de sistemas com alto grau de sofisticação;
- manter extrema flexibilidade na seleção de critérios;
- reduzir o tempo gasto por computadores para atender aos requisitos da auditoria;
- realizar o exame do sistema durante a sua operação;
- estabelecer um alto grau de confiança para auditagem dos sistemas on-line, incluindo-se aqui os controles de acessos necessários a terminais.

O método de embutir módulos, critérios de seleção de dados ou outros comandos em programas tem apresentado como método diferentes. O fato decorre muitas vezes da particularidade dos critérios estabelecidos no âmbito do processamento que podem produzir relatórios com características padronizadas.

Tais critérios são muitas vezes traduzidos em instruções já existentes em algumas linguagens de programação e que podem ajudar a fase de depuração de programas.

Alguns dos relatórios decorrentes do uso de tais instruções apresentam acentuado grau de detalhes, o que torna difícil a auditores pouco experientes em processamento de dados, uma eficiente análise e interpretação.

Chamamos, pois, atenção que quaisquer que sejam as instruções ou conjuntos de instruções a serem inseridas nos programas devemos ter em mente o volume de relatórios delas decorrentes, que sem dúvida pode comprometer a análise.

Pacotes de software para auditar sistemas

Pacotes de *software* para auditoria constituem programas que são desenvolvidos por grupos especializados com a finalidade de dar suporte às tarefas de auditar sistemas.

A ferramenta apresenta um grande índice de utilização em decorrência da constante participação de auditorias externas para as quais o período de atuação junto aos Centros de Processamento de Dados constitui-se em ponto crítico face às necessidades de conclusão do trabalho no tempo da vigência do Exercício Fiscal ou período legal.

Enfatizando sua atuação junto a arquivos que diariamente são manipulados a ferramenta permite um trabalho de análise totalmente independente dos processos e sistemas utilizados, mesmo considerando a diversidade de organização e dispositivos presentes.

As mudanças solicitadas em cada caso são feitas com o fornecimento de parâmetros, o que permite atender às necessidades de cada usuário ou de cada equipamento em uso do CPD.

Os pacotes procuram fornecer ao auditor funções básicas para análise de arquivos e que podem ser resumidas em:

- seleção e impressão de dados;
- atensimento de várias operações lógicas;
- estatísticas das informações;
- pesquisa específica de dados, tais como elementos duplicados, perdidos;
- comparação de gerações diferentes de um mesmo arquivo;
- sumários capazes de fornecer uma visão geral do conteúdo de arquivos;
- atendimento de cálculos elementares.

Embora os pacotes já constituam software prontos e testados, em sua aplicação são requeridas algumas tarefas:

a) Definição dos objetos da auditoria. Nesta fase são feitas as revisões dos sistemas a serem auditados ocasião em que os planos para determinar o que deve ser testado são desenvolvidos. Um bom conhecimento do sistema é solicitado do auditor, a fim de que os elementos ou dados de cada arquivo possam ser testados e analisados com propriedade. Para tanto o auditor deve servir-se da documentação, ocasião em que verifica o estado de sua atualização quanto a fluxos, formatos de registros, campos etc.

b) Preparo dos dados para entrada. A especialização dos elementos que constituirão a entrada do software deve ser tarefa do auditor. Normalmente tais informações envolvem:

i) localização dos dados nos registros;

ii) extensão dos dados;

iii) nomes para cada dado;

iv) outras informações que traduzem as características como, dado numérico, alfabético, binário, etc;

v) descrição sumária da organização dos arquivos.

c) Preparo de especificações para processamento. A ferramenta para ser operada pelos elementos de processamento de dados de fluxos que orientam os procedimentos. Assim cabe ao auditor elaborar as especificações de processamento que devem ser seguidas, instruções sobre o manuseio de arquivos gerados pelo software sejam intermediários ou finais.

d) Preparo das especificações dos relatórios de saída. As saídas dos pacotes em uso apresentam grande flexibilidade. Em tal trabalho é possível definir tabulações, listagens com diversos níveis de totalização, relatórios intermediários em fita ou disco para comparações após ciclos de processamento, o que requer que o auditor dedique algum esforço no preparo dos formatos de saída.

e) Processamento dos arquivos. Concluídos os trabalhos de especificação, os pacotes devem ser postos em operação, devendo-se sempre assegurar que os arquivos que constituem a entrada estão selecionados corretamente. Alguns destes pacotes possuem parâmetros que permitem testar a validade dos arquivos em funções de sua identificação magnética o que deve ser usado para monitorar e operação do sistema. Em tal etapa é sempre conveniente a presença do auditor.

f) Avaliação do trabalho. A fase final do trabalho de auditagem com uso de pacotes consiste em documentar todos os procedimentos que foram praticados ou desenvolvidos. Esta tarefa não deve ser relegada a plano inferior, pois que freqüentemente, são requeridas passagens adicionais para testar variações ou desvios, e que só poderão ser confirmadas se fornecidas as mesmas condições que estiveram presentes no processamento anterior.

Embora os pacotes tenham sido desenvolvidos com o objetivo de atender a múltiplas atividades, tais sistemas apresentam limitações que são impostas pelo próprio desenvolvedor ou pela capacidade instalada do usuário.

Isso implica que o uso da ferramenta quando não praticado por grupos de auditoria externa, que já padronizaram seu sistema de atuação, fique condicionado a uma análise para seleção do pacote. Tal seleção já envolve, por si, um conjunto de fatores, como custo, suporte operacional que dão bastante complexidade à tarefa.

Abstraindo os fatores econômicos cuja análise pode ser procedida à luz binômio custo/benefício, alinhamos algumas considerações técnicas que necessitam ser analisadas por ocasião da seleção do pacote para auditoria:

a) liguagem-fonte do pacote;
b) documentação existente;
c) desempenho do pacote no manuseio de arquivos cujas características se assemelham às existentes no centro de processamento a ser auditado;
d) nível de especialização do pacote;
e) treinamento requerido para sua operação;
f) suporte operacional e técnico que é proporcionado pelos fornecedores ou outros usuários do pacote;
g) teste para avaliação da correção e propriedade no que se refere ao manuseio dos dados.

Assim a tarefa de escolha eficiente de um sistema de auditoria pode constituir um trabalho bastante técnico e árduo para a auditoria.

Devemos igualmente considerar que a auditoria executada com o uso de pacotes, normalmente, traduz-se em processamento paralelo que é desenvolvido sobre os arquivos dos sistemas, ou que representa maior tempo de utilização dos equipamentos.

Teste de condições

O método de teste de condições constitui-se em uma das metodologias mais difundidas em auditagens de sistemas de informações em operação. Através dele o auditor de sistema consegue verificar a correção de rotinas e módulos dos programas e obter dados que o certifiquem da existência e adequação de controles.

O objetivo essencial deste método é atestar a confiança dos programas em função das especificações do usuário, ou das políticas administrativas e operacionais da empresa.

Na utilização do método o auditor procura projetar e selecionar transações que simulem as condições dos dados que podem ocorrer em um processamento normal, e ao obter

os relatórios compara com os elementos que foram previamente estabelecidos como saída correta e esperada.

O método apresenta-se como de fácil aplicação e pode ser desenvolvido para atender isoladamente a cada programa que compõe o sistema. Procedimentos especiais não são requeridos e a correção dos dados finais é obtida por inferência dos testes dos testes realizados com o objetivo de verificar e avaliar o funcionamento do sistema.

Os procedimentos gerais para a realização de auditagem utilizando o teste de condições podem ser resumidos no atendimento das seguintes etapas:

a) Definições das condições a serem testadas. A definição de condições visa possibilitar que os objetivos específicos da auditagem sejam fixados e bem definidos. Para tal o auditor disporá da documentação detalhada do sistema que lhe permitam definir com propriedade todas as condições que devem ser atendidas.

b) Criação de dados. No atendimento de tal tarefa o auditor procura gerar os dados de transações que irá submeter como teste para o sistema. Além de selecionar os dados o responsável pela auditagem devem predeterminar os resultados esperados, antecipando-se em seus relatórios aos produzidos pelo sistema em processamento.

c) Conversão dos dados para possibilitar leitura pelo sistema. Esta tarefa constitui a terceira etapa do método e é de vital importância que principalmente quando o sistema é testado isolando cada programa. Tal fato decorre de muitos programas terem como entrada de dados que já sofreram processamento e apresentam modificações ou em seu formato ou no dispositivo a que o programa acessa como entrada. Nessa etapa a observação e estudo dos fluxos de transações possibilitam determinar com a devida propriedade como e quando fornecer os dados de teste.

d) Realização do teste. Esta constitui a etapa em que é feita a execução do processamento tendo como entrada de dados criados pelo auditor. A presença do auditor por ocasião da realização do teste é tida essencial e cuidados especiais devem ser tomados para que os arquivos do sistema não venham a sofrer danos, por perdas ou inclusões de informações indevidas. A falha nesta etapa deve determinar o reexame de todas as etapas anteriores, afim de que possa ser determinada a razão.

e) Análise e documentação. Executados os testes o auditor deve dedicar-se às tarefas de análise e comparação de resultados. Desvios que necessitem de correção ou exceções que devam ser confirmadas necessitam ser documentadas. Esta atividade

minimiza esforços em novos ciclos de testes sobre o mesmo sistema que mereçam ser repetidos por exigências de correção, manutenção ou determinações administrativas.

O método não se revela prático quando os sistemas a serem auditados são grandes e complexos ou trabalham on-line, face a dificuldades em dispor-se dos recursos do computador e arquivos para a realização da tarefa.

Considera a necessidade de se prepararem previamente os resultados , o que por si já constitui tarefa bastante árdua, predomina a tendência de se reduzir ao mínimo o número de dados que determinam as condições do processamento, o que poderá resultar na escolha de dados que não representem estatisticamente a posição e conteúdo dos arquivos ou ainda não verifiquem as rotinas lógicas que os programas encerram.

Dadas tais condições a aplicação do método exige conhecimentos de processamento de dados, conhecimentos dos sistemas de testes e das técnicas de controles, além dos naturais conhecimentos de auditoria.

Testando programas por inferência, uma vez que os dados fornecidos constituem uma simulação das condições reais, não se pode atestar a absoluta segurança dos programas. Acresça-se que constituindo uma metodologia de tratamento estático, onde os testes são realizados independentes do processamento da produção , não podemos assegurar que os programas estejam isentos de alterações em parte ou em seu todo, sejam setas a priori ou a posteriori à verificação.

A todas estas condições ainda pode ser alinhado o fato do teste não possibilitar a verificação do conteúdo dos arquivos em seu estado atual, o que exige que sua aplicação seja secundada por outros métodos.

Métodos para Auditar Sistemas em Desenvolvimento

É sabido que a adequação e eficiência de um sistema não residem somente na maneira com que o mesmo é operado ou que resultados deles são obtidos. Entre os pressupostos básicos de um sistema são alinhados os objetivos, meios e recursos como fatores determinantes de condições para o seu desenvolvimento e existência.

Para os sistemas de informação onde os são componentes fundamentais para o seu correto funcionamento é extremamente importante atender-se à fixação dos objetivos de maneira clara e compreensiva.

A esta etapa várias questões que se responsabilizam pelo desempenho ou restrições do sistema devem ser examinadas, atendidas e equacionadas adequadamente, pois

se o problema surge neste estágio as alterações e controles então determinados não terão reflexos em extensas modificações.

Face a isto, engajar o trabalho de auditar nas fases onde os sistemas já são operacionais e onde já foi definido todo o disciplinamento do uso de recursos é restringir o trabalho de uma auditagem ao exame e correção dos efeitos de causas muitas vezes indeterminadas e que continuam a produzir eventos por vezes bastante indesejáveis.

Constitui, pois, preocupação dos auditores acompanhar o desenvolvimento de sistemas e através das diversas fases de seu ciclo de vida estabelecer controles que permitam confiabilidade a todas as tarefas que diretamente ou indiretamente deles dependam.

Todavia, o envolvimento da auditoria no processo de desenvolvimento é ainda novo, e os métodos desenvolvidos para este trabalho ainda carecem de confirmação experimental.

Auditagem Extra-Sistema

Centros de computação constituem a terceira área de vital importância para a auditoria de sistemas face a envolvimento que têm com a correção, completeza e oportunidade dos resultados de processamento.

A correção e completeza dos dados e relatórios produzidos dependem diretamente da qualidade, eficácia e eficiência das tarefas desenvolvidas na operação de um Centro de Processamento. Por isso para muitos gerentes de CPDs ainda não ficou suficientemente esclarecido por que os auditores necessitam modificar sua linha de ação e não simplesmente incrementar o atendimento de suas tarefas fazendo a auditagem em torno dos computadores, envolvendo-se em atividades que venham requerer conhecimentos de processamento de dados que ainda não possuem.

Apontamos quatro áreas de aplicação de controles:

1) controle de entrada e saída de dados;
2) controle de procedimentos com a biblioteca do sistema;
3) controle dos recursos e divisão de responsabilidades; e
4) controle do meio ambiente e segurança física.

A estas áreas tem sido dada toda a ênfase dos trabalhos de auditoria. Para dar suporte e possibilitar diretamente a continuidade dos trabalhos de um CPD, as áreas a seguir respondem igualmente pela eficiência e eficácia da operação dos sistemas:

5) planos de contingência;
6) controles de falhas e manutenção;

7) projeção de recursos necessários ao desenvolvimento dos trabalhos;

8) controle da produção e conseqüente repasse de custos.

Analisemos de modo resumido o significado de cada área, para assegurar uma clara e definida compreensão da auditoria de um Centro de Processamento de Dados.

1) Controle de entrada e saída

O objetivo primeiro deste controle é assegurar a correção e completeza dos dados recebidos e distribuídos. A interligação dos processos manuais automatizados de um sistema em operação ocorre nesta área.

Assim planos bem definidos e documentos para a operação das aplicações e suas seqüências são exigidos. Em tais processamentos devem existir controles para dados recebidos dos usuários, verificações de entradas para processamento em batch, controles dos erros ou transações rejeitadas condições exceções ocorridas no processamento e que devem ser aceitas, além de rotinas para controlar a distribuição de relatórios.

2) Controle de Procedimentos com a biblioteca do sistema

Os dados que são processados em sistemas automatizados residem temporariamente em dispositivos do sistema (comumente fitas ou discos) sobre os quais devem ser exercidos controles face não só ao caráter de confidencialidade, mas também da importância que representam para o sistema.

Nesta área o interesse dos auditores se deve voltar para:

a) segurança física e controle de acessos a arquivos;

b) estudo dos locais de guarda ou armazenamento de dados em áreas diferentes nos CPDs;

c) procedimento de retenção de dados e outros arquivos adotados e utilizados nos CPDs;

d) procedimentos de atualização das bibliotecas.

3) Controle dos recursos e divisão de responsabilidades.

Nota-se quando o estudo da ocorrência de fraudes que é nesta área que a potencialidade de ações indesejáveis esta mais presente. O uso e abuso do computador esta sempre mais facilitado se a responsabilidade de manipulação de programas e dados estiverem dependentes de uma mesma pessoa ou autoridade.

Assim a atenção dos auditores deve estar voltada para procedimentos que regulem definições de área de atuação de processamento e autorização para uso dos recursos computacionais da empresa.

4) Controle do meio ambiente e segurança física

Um centro de processamento de dados requer para o seu contínuo funcionamento a existência de algumas condições que compondo um conjunto criam o ambiente necessário ao funcionamento do sistema "computador".

Assim condições de instabilidade no fornecimento de força, no nível de uma umidade e temperatura constituem fatores que podem determinar o mau funcionamento de um CPD. Igualmente fatores decorrentes da falta de proteção do ambiente podem responder por ações indesejáveis ou perturbações no CPD. Face a isto os auditores de vem estar interessados em examinar aspectos tais como:

- segurança física, neste caso traduzida por medidas que dêem proteção aos equipamentos eletrônicos e de suporte principalmente contra eventuais incêndios;
- limitação do acesso de pessoas não autorizadas a áreas de operação, para garantir a salvaguarda de todo o patrimônio utilizado pelo Centro, seja o processamento feito batch ou on-line.

5) Planos de Contingência

Planos e processos de funcionamento das diversas atividades de qualquer organização, são eventualmente perturbados pela ocorrência de eventos tais como acidentes ou falhas e que tornam inoperantes ou paralisam temporariamente todas as atividade. Em se tratando de sistemas automatizados onde via de regra há alta concentração de dados e informações que determinam as políticas e decisões das organizações, e paralisação ou perda temporária de controles pode provocar uma situação cujas conseqüências são de difícil previsão.

Assim, planos que simulem as situações de emergência seja alta ou baixa a probabilidade de ocorrência, devem ser devolvidos, mantidos e testados. Logicamente alguns eventos de conseqüências catastróficas não poderão ser testados com um nível de realidade desejável, mas mesmo para estes é válida a realização de testes como simulação.

O benefício decorrente de tais planos será visto em função da rapidez que responde pela regularização das situações excepcionais, causem elas prejuízos totais ou parciais às instalações de um CPD.

Portanto devem constitui preocupação dos auditores a verificação das rotinas uso de *back-up* quer de arquivos ou instalações, métodos de utilização destas, pontos de controles e procedimentos que garantam a integridade dos dados durante os períodos de transição.

6) Controles de falhas e manutenção

Relatórios de falhas e da sistemática de manutenção são elementos que possibilitam os gerente de processamento de dados tomar decisões que previnam a ocorrência

de paralisações. A um mau funcionamento ocasional onde torna-se difícil determinar responsabilidades podem decorrer muitas vezes prejuízos incalculáveis. Todavia a participação tempestiva de tais falhas permite que se tomem decisões que atuam com correção ou põem em funcionamento planos de contingência.

Face a isto o interesse dos auditores deve se revelar para exame de programas de manutenção que logicamente são normais e peculiares a cada instituição. Embora tais programas sejam sempre de responsabilidade dos vendedores dos equipamentos decorrência natural do conhecimento que tem do hardware que fabricam, as instalações devem possuir controles que permitam assegurar que os procedimentos adotados em tais ocasiões não vão perturbar a integridade dos sistemas da organização.

Assim a situação dos auditores nesta fase pode incidir sobre os planos para procedimento de manutenção preventiva ou apreciação de contratos entre as empresas e os vendedores ou organização qualificada para manutenção, onde são fixados os limites de responsabilidades.

7) Projeção dos recursos necessários do Desenvolvimento

O constante desenvolvimento das atividades de processamento de dados exige uma alocação quase contínua de recursos materiais ou humanos para possibilitar um continuado e adequado atendimento aos trabalhos que dia a dia são cometidos.

A aquisição de tais recursos constitui tarefa quase sempre demorada e de resultados duvidosos que poderá resultar em dificuldades ou atrasos para os planos da organização.

Assim planos e processos de expansão de atividade e de recursos devem caminhar em paralelo. Em tal área os auditores devem verificar o grau de confiabilidade das projeções que prevêem a alocação de recursos, as técnicas usadas em tais estudos e os controles administrativos observados.

Especificamente o trabalho é traduzido em planos estratégicos ou táticos, elaborados e aprovados pela alta administração da organização, onde aspectos de investimentos e outros custos são considerados.

8) Controle de produção e repasse dos custos.

Sendo processamento de dados uma atividade meio, a determinação dos custos de produção e conseqüente repasse aos usuários internos ou externos constitui preocupação administrativa. O repasse de custos deve ser encarado com bastante preocupação a fim de que através da devida avaliação dos gastos com a produção dos sistemas automatizados, o computador não venha a se converter em um brinquedo caro na mão de técnicos talentosos.

Assim, processos de controles adotados para a análise das atividades de processamento devem atender a:

a) identificação das entidades usuárias envolvidas no sistema em operação;
b) acompanhamento de orçamentos previstos para cada entidade usuária;
c) custos de reprocessamento;
d) algoritmos de fixação de custos, taxas de remuneração dos trabalhos.

Em resumo diríamos que numa apreciação conjunta de todas estas oito áreas atinentes a um CPD, verificamos a existência de um grande número de controles que devem ser postos em prática para assegurar a correção e completeza dos dados, tarefa que, sem sombra de dúvida, deve ser preocupação da auditoria ao realizar tarefas de auditagem em CPDs.

As quatro primeiras por afetarem mais diretamente os sistemas em produção têm revelado maior importância e maior desenvolvimento. Todavia, o exame completo de todas as áreas acima citadas tem por objetivo assegurar a continuidade dos serviços do qual sempre mais e mais dependerão as Organizações. Dentro deste critério de abrangência selecionamos o método de auditar centros com o uso de questionários de auditorias que passaremos a apreciar.

Auditoria com o uso de questionários

O método de auditar centros com o uso de questionários visa assistir ao auditor na realização de suas tarefas junto ao CPD. Basicamente consiste em abordar uma série de questões ou ações com sugestão de medidas ou critérios que devem ser postos em prática para verificação dos controles.

Embora o método possa ser dirigido para atuação em qualquer área de processamento, sua utilização mais eficaz se faz junto a centro de serviços e produção de um CPD, face à mais fácil materialização dos itens que fornecem respostas às diversas questões que integram o guia.

Consistindo de questionários prédeterminados que o auditor utiliza no desenvolvimento de seu trabalho a realização da tarefa envolve os seguintes passos:

a) definição dos propósitos e objetivos da auditagem;
b) análise do guia a ser adotado para eliminação de itens que não dizem respeito ao serviço ou introdução de custos exigidos ou aconselhados pelos objetivos anteriormente definidos;

c) preparo do plano de ação da auditoria junto ao CPD, para determinar os suportes requeridos;

d) desenvolvimento da etapa de coleta de informações junto ao centro a ser auditado. Tal passo envolve conhecimento da documentação, organização, equipamentos e políticas de atendimentos;

e) seguinte passo de desenvolvimento dar-se-á junto aos usuários, onde devem ser colhidos dados atinentes a cada sistema cujo trabalho foi iniciado na etapa anterior;

f) análise dos dados em função dos controles existentes e necessários. À etapa de análise seguem-se os relatórios de conclusões e recomendações.

A aplicação do método não constitui tarefa de grande complexidade e como vantagens decorrentes de seu uso podem ser apontadas:

- redução do tempo de preparação do trabalho;
- apoio do trabalho em extensivas listas de verificação já objeto de sucessivas depurações em diversas organizações;
- uniformização das auditagens das diversas instalações de uma mesma organização;
- possibilidade de obtenção de guias junto a organizações especializadas;
- acúmulo de experiências para futuras auditorias.

Todavia, mesmo diante de tais vantagens a adoção do método deve ser analisada em função de adequação do questionário aos trabalhos de organização, face à padronização adotada e limitação de visão que pode incutir nos auditores. Por isso em todas as aplicações exige-se a participação de auditores experientes a fim de que as ações não previstas no questionário possam ser detectadas e analisadas com eficiência e propriedade.

CONCLUSÃO

A principal conclusão que podemos tirar desse trabalho é que por maior que sejam os investimentos feitos na melhoria dos sistemas de controle e nos aspectos de segurança física e de danos, não existe sistema totalmente seguro.

Atos da natureza, erros, sabotagens, fraudes e até mesmo má gerência sempre vão existir, prejudicando assim o bom desenvolvimento dos processos e sistemas.

Com isso, o principal papel dos auditores desses sistemas, já que não podem impedir tais riscos, é o de tomar as melhores medidas preventivas ou acauteladoras para que o desenvolvimento de controles capazes de favorecer os sistemas automatizados, continuem a ter a segurança, eficiência, eficácia e correção necessária. Assim, o auditor com esse ofício, afasta a idéia, ainda hoje dominante, de que a função da Auditoria tem como escopo principal fiscalizar sistemas e apurar responsabilidades.

A metodologia usada nas diversas fases e atividades da auditoria é fator determinante para atender a todas as exigências nas auditagens dos sistemas automatizados, utilizando-se de um controle mais efetivo, face principalmente ao aumento das possibilidades de falhas processadas, casual ou intencionalmente.

Assim há que se empregar um grande esforço no desenvolvimento e implementação de controles tanto no que se referir a administração e gerência de Centros de Processamento de Dados, quanto no que se referir ao desenvolvimento de software, seja ele básico ou operacional.

BIBLIOGRAFIA CONSULTADA

AMÉRICO, M. F. **Programa de Administração e Gerência.** Rio de Janeiro, FGV, 1997.

BRATZ, W. **Sistema de Informação Gerencial; o conceito e o modelo.** IBM do Brasil.

CÂMARA BRASILEIRA DE AUDITORIA INFORMÁTICA. **Procedimentos de Auditoria informática.** São Paulo, 1993.

CASSARRO, A. C. **Sistemas de Informações para Tomada de Decisões**. São Paulo: LTr, 1997.

COMER, M. J. **Fraude, Corrupção e Desonestidade nos Negócios**, Makron Books, 1994.

FONTES, J. R. **Manual de Auditoria de Sistemas.** Rio de Janeiro: Ciências Modernas, 1991.

ICHAK, A. **Os Ciclos de Vida das Organizações e Gerenciando Mudanças,** Pioneira, 1993.

MARTINS, J. **Computador, Sociedade e Desenvolvimento.** Rio de Janeiro, livro técnico, 1993.

MOLLER, C. **O Lado Humano da Qualidade – Maximizando a Qualidade de Produtos e Serviços através de Desenvolvimento das Pessoas,** Pioneira, 1992.

MORAIS, J. B. **Auditoria de sistemas "através do computador"**. Fortaleza: BNB, 1982.

PETER F. D. **Administrando para o Futuro e As Novas Realidades,** Pioneira, 1992.

RODRIGUES, S. **Sistemas de Informações,** Bio, 1997.

SKINNER & ANDERSON, **Auditoria Analítica,** LTC, 1995.