Centro Universitário de Brasília

CENTRO UNIVERSITÁRIO DE BRASÍLIA
FACULDADE DE CIÊNCIAS SOCIAIS APLICADAS FASA
CURSO: CIÊNCIAS CONTÁBEIS
DISCIPLINA: MONOGRAFIA
ÁREA: AUDITORIA
PROFESSOR ORIENTADOR: CARLOS ANTONIO DIAS CHAGAS

AUDITORIA INTERNA COMO FERRAMENTA DE APOIO À GARANTIA DA SEGURANÇA DOS SISTEMAS DE INFORMAÇÃO

DANUZIA SILVESTRE PINHEIRO
2034357/0

Brasília/DF, maio de 2006.

DANUZIA SILVESTRE PINHEIRO

AUDITORIA INTERNA COMO FERRAMENTA DE APOIO À GARANTIA DA SEGURANÇA DOS SISTEMAS DE INFORMAÇÃO

Monografia apresentada à banca examinadora do Centro Universitário de Brasília – UniCeub – como requisito parcial para a conclusão do Curso de Ciências Contábeis.
Orientador: Carlos Antonio Dias Chagas

Brasília
2006

DANUZIA SILVESTRE PINHEIRO

AUDITORIA INTERNA COMO FERRAMENTA DE APOIO À GARANTIA DA SEGURANÇA DOS SISTEMAS DE INFORMAÇÃO

COMISSÃO EXAMINADORA

_____
Carlos Antonio Dias Chagas

_____
Examinador: Rogério R. Marques

_____
Examinador: João Alberto Arruda

Brasília, 06 de junho de 2006.

Àquele que foi o exemplo de trabalho e honestidade para todos da nossa família e que, mesmo em sonho, me enviou sua inspiração e seus incentivos para que eu continuasse meu estudo: Vovô Sérgio Pinheiro.

AGRADECIMENTO

Agradeço a todos que de alguma forma colaboraram para o meu sucesso, para as minhas conquistas e para a realização de mais este trabalho, em especial, aos meus pais, os quais foram apoio incondicional em todos os momentos da minha vida; ao meu chefe, que apostou em meu potencial e depositou em mim sua confiança; a todos os professores que, pacientemente, se empenharam em dividir sua bagagem de conhecimento ao longo destes anos; e, como não poderia deixar de ser, a Deus, por Sua infinita sabedoria.

“O problema não é o problema. O problema é a atitude com relação ao problema”. Kelly Young

RESUMO

A presença dos sistemas de informação é fato observável em qualquer organização. O adequado planejamento e a instituição de uma política de uso são fatores essenciais, porém não suficientes, para garantir a segurança das informações de uma empresa. A discussão proposta neste trabalho busca evidenciar a importância do papel da auditoria interna nesta tarefa de salvaguardar a confiabilidade, disponibilidade e fidedignidade das informações processadas e armazenadas em sistemas de informações da empresa. Esta tarefa, no entanto, depende também de confiabilidade do trabalho de auditoria, o qual deve, dentre outras tarefas, primar-se na avaliação dos controles internos, em especial, neste caso, nos controles focados em tecnologia de informação. Uma das contribuições desta pesquisa acadêmica é a de evidenciar as opiniões de especialistas sobre o assunto para que possam servir de embasamento para a tomada de decisões ou de argumentos a serem utilizados em futuros estudos. Trata-se de trabalho que será útil para consultas rápidas e mesmo como roteiro de estudo para a implementação de uma auditoria interna de sistemas.

Palavras-chave:

Auditoria. Auditoria interna. Contabilidade. Controle Interno. Segurança da Informação. Sistemas de informação. Tecnologia da Informação.

ABSTRACT

The presence of the information system is an undisputed fact in any organization. The adjusted planning and the institution of a user policy are essential; however, are not enough factors to guarantee the security of the company's information. The proposed discussion in this work looks for evidencing the importance of the internal auditor role in this task to safeguard the security, availability and reliability of the processed and stored information in information system of the company. This task, however, also depends on trustworthiness of the auditor's work, which must take care of the evaluation of the internal controls, especially, in this case, of the controls focused in information technology. One of the contributions of this academic research is to evidence of the specialists' opinions about the subject so that they can serve as a basis for making decisions or as the arguments to be used in future studies. One is about work that will be useful for fast consultations and even as script of study for an internal systems auditorship implementation.

Key words:

Accounting. Audit. Internal audit. Internal control. Information security. Information systems. Information technology.

LISTA DE FIGURAS

LISTA DE ABREVIATURAS E SIGLAS

AICPA	*American of Certified Public Accountants*
CFC	Conselho Federal de Contabilidade
EIS	*Enterprise Information System*
ERP	*Enterprise Resource Planning*
IEC	*International Electrotechnical Commission*
ISO	*International Organization for Standardization*
PCGA	Princípios de Contabilidade Geralmente Aceitos
SAD	Sistema de Apoio à Decisão
SIG	Sistema de Informação de Gestão
VPN	*Virtual Private Network*

SUMÁRIO

INTRODUÇÃO

O novo contexto empresarial, inserido em uma economia mundial globalizada (blocos econômicos, quebra de barreiras alfandegárias, menor intervenção governamental e quebra de monopólios) e calcado na revolução tecnológica e informacional (comércio eletrônico, telecomunicações e sistemas integrados), incitou a necessidade de uma reengenharia no enfoque de auditoria, para atender às novas exigências dos usuários das informações, sejam usuários internos ou externos.

O caminho irreversível do uso dos sistemas informatizados de processamento de dados e ainda a rede mundial de computadores tornaram as empresas e, principalmente, as suas informações cada vez mais vulneráveis. A interconexão destas redes públicas e ainda as conexões privadas (VPN – *Virtual Private Network)* e o compartilhamento de recursos entre fornecedores, parceiros, colaboradores e clientes aumentaram consideravelmente a vulnerabilidade das empresas, implicando em perigo real de perda ou roubo das informações e ainda de comprometimento da disponibilidade dos serviços, gerando novos riscos e ameaças para as organizações.

Diante deste cenário, aliado ao uso de plataformas de processamento distribuído, verifica-se a fragilidade dos controles de segurança e a necessidade de controle de acessos ao ambiente tecnológico bem como de auditoria periódica da utilização dos recursos tecnológicos e das informações armazenadas nos bancos de dados.

Para isso, é imprescindível a identificação das vulnerabilidades, ameaças e riscos ao sistema de informação, no sentido de priorizar as ações de segurança, de forma a levantarem-se os requisitos necessários à implementação de controles eficazes.

A segurança da informação é fundamental para a gestão de negócios de qualquer empresa. Com o objetivo de se alcançar tal propósito, deve-se agregar a utilização das melhores tecnologias e metodologias de análise do mercado com o envolvimento dos usuários das informações e constantes auditorias para que seja

assegurado o correto uso dos recursos tecnológicos.

A ampliação do espaço geográfico de atuação da empresa e o aumento da competitividade das operações no mercado revelam a dimensão da importância do papel da demonstração das informações contábeis de maneira adequada. Neste contexto, a auditoria assume relevante papel na contribuição para o fornecimento de tais informações. Pode-se afirmar, portanto, que é necessária uma supervisão além das que são adotadas pelo controle empresarial, com o objetivo de reduzir os riscos e aumentar a qualidade e transparência das informações para os tomadores de decisão.

Com o intuito de proporcionar uma maior credibilidade das informações apresentadas pelos gestores das empresas, o auditor deve, por meio de pareceres quanto à mensuração de desempenho, avaliação de riscos, confiabilidade nos sistemas, controle interno e auditoria interna, entre outros, explorar as oportunidades em agregar valor em todas as áreas do processo decisório das empresas, de forma a acrescentar transparência às informações divulgadas aos seus usuários, internos ou externos, para a tomada de decisão.

Este trabalho visa abordar a aplicação da auditoria interna como ferramenta de apoio à segurança da informação, o que facilitará a fiscalização da eficiência dos processos informatizados, a visualização da real situação econômica, patrimonial e financeira da empresa, além de apontar possíveis falhas na organização administrativa dos controles internos e garantir a adequada utilização dos recursos tecnológicos da organização.

O conjunto de variáveis interferentes no desempenho empresarial, tais como políticas, objetivos, estrutura organizacional, ambiente interno e externo e sistemas de informação poderão ser a base para a compreensão do sistema organizacional, o qual é monitorado, constantemente, pelo sistema de controle interno e por agentes externos (governo, auditores independentes, acionistas, entidades não governamentais, entre outros).

A auditoria, se for utilizada como uma ferramenta de acompanhamento da utilização de sistemas de informação e como apoio ao controle interno, poderá, ao ser instituída com suas normas, preceitos éticos, princípios básicos, metodologia, procedimentos essenciais de trabalho e pareceres elaborados, disponibilizar uma

fonte confiável de informações para o processo decisório dos administradores.

O presente trabalho, portanto, tem sua importância pelos seguintes aspectos: contribui para verificar a eficiência da auditoria interna como ferramenta de apoio ao controle interno; elenca técnicas e métodos de trabalho em auditoria de sistemas de informação; pode servir como instrumento de consulta para gestores de organizações; e consiste em material de avaliação requerida para a conclusão do curso de graduação em Ciências Contábeis do Centro Universitário de Brasília – UniCEUB.

O estudo proposto teve como objetivo apresentar conceitos e os benefícios da auditoria interna, bem como verificar a eficiência de sua utilização como ferramenta de acompanhamento do uso de sistemas de informação e como apoio ao controle interno.

Com o intuito de atender o proposto no objetivo geral, o presente trabalho tem os seguintes objetivos específicos:

1. apresentar conceitos e finalidades do controle interno e da auditoria;
2. apresentar definições e importância da auditoria interna em uma organização;
3. elencar técnicas, procedimentos, metodologia e principais documentos gerados pela auditoria interna de sistemas de informação;
4. constatar se há a crença de que a eficiência e o aumento da confiabilidade das informações organizacionais estão ligados à auditoria de sistemas.

Para o desenvolvimento da pesquisa, formulou-se o seguinte questionamento: A auditoria interna pode funcionar como uma ferramenta confiável de apoio na garantia da segurança dos sistemas de informações da entidade auditada?

O método de abordagem utilizado para encontrar a resposta ao problema formulado foi o dedutivo, pois, como afirma Köche (1992), ao se utilizar a inferência dedutiva, sendo as premissas verdadeiras, a conclusão sempre será verdadeira, desde que não se extrapole nunca o domínio da hipótese.

O presente estudo foi realizado sob o amparo de obras dos autores especialistas no assunto abordado, com enfoque nos campos específicos do conhecimento na área de auditoria, de forma a corroborar ou refutar a hipótese

formulada ao problema identificado de que a auditoria interna é essencial para salvaguardar a segurança dos sistemas de informação.

Para o desenvolvimento desta proposta de investigação bibliográfica, voltou-se a atenção aos conceitos, tipologia e metodologia do trabalho de auditoria interna, e ainda conceitos, riscos, tratamento e utilização dos sistemas de informação. A meta estipulada foi a compilação de conhecimentos e informações referentes a conceitos, funcionamento e as principais recomendações propostas pelos autores sobre os processos descritos no trabalho.

Dividiu-se o tema abordado em partes, para a melhor explanação do assunto. No primeiro capítulo, encontram-se as definições e os objetivos da função controle e auditoria, além de itens que tratam sobre fraudes e auditoria interna. No segundo capítulo, o foco está voltado para a conceituação de sistema de segurança de informação, além de englobar a importância e as principais técnicas de auditoria em sistemas de processamento de dados e elencar as melhores práticas de auditoria de sistemas adotadas no âmbito das organizações, de forma a consolidar-se um arcabouço de conhecimento para consultas posteriores.

Finalmente são apresentadas as discussões e conclusões sobre o tema pesquisado.

1 CONTROLE E AUDITORIA

Nesta primeira parte do trabalho, objetiva-se situar o leitor com relação à conceituação e explanações dos autores a respeito da função controle exercida pela administração, seus objetivos, sua forma de divisão e sua importância, além de tratar de suas falhas, as quais podem permitir existência de fraudes. Também serão abordados os conceitos de auditoria, suas finalidades e tipologia.

A diferenciação entre controle interno e auditoria interna é necessária para o desenvolvimento do presente trabalho, pois há uma tendência no sentido de se confundir estes dois conceitos. Por este motivo, apresentar-se-ão neste capítulo os conceitos de controle e controle interno encontrados na bibliografia sobre o assunto e, no próximo capítulo, os conceitos sobre auditoria e auditoria interna, com o objetivo de elucidar o leitor quanto à diferença básica entre os termos.

1.1 CONTROLE

O valor agregado e a importância dos controles passam pela análise dos casos já ocorridos de perdas, prejuízos, falências, bem como pela análise dos casos de melhoria, de sucesso e de sobrevivência das empresas.

Mautz (1985) enfoca a importância da revisão dos controles utilizados por uma organização para fins de auditoria. O autor diz:

> Afim de obter as informações necessárias para instruir-se sobre como todas as informações contábeis são coligadas e processadas, bem como saber a natureza do controle que torna essas informações dignas de confiança na proteção dos bens da empresa, muita perícia e conhecimento são necessários. (MAUTZ, 1985, p. 182-183).

Com base nesta observação, pode-se inferir que a adoção de controles internos é política fundamental a ser implementada pelas empresas com intuito de mitigar erros e melhorar continuamente os seus processos.

1.1.1 Definições de Controle

Segundo Kotler (1975), pode-se entender controle como a ação com o intuito de aproximar os resultados reais dos desejados.

Com o mesmo enfoque, Martins (1995, p. 259) afirma que controle significa "conhecer a realidade, compará-la com o que deveria ser, tomar conhecimento rápido das divergências e suas origens e tomar medidas para sua correção".

No que se refere à definição específica de controle interno, o AICPA, *American of Certified Public Accountants*, aponta como sendo:

> O plano da organização e todos os métodos e medidas coordenados, aplicados a uma empresa, a fim de proteger seus bens, conferir a exatidão e a fidelidade de seus dados contábeis, promover a eficiência e estimular a obediência às diretrizes administrativas estabelecidas. (apud ARIMA, 1994, p. 12).

De acordo com Cabral e Bleinat (1992, p. 51), essa é a definição mais conhecida e respeitada sobre controle interno.

Outra definição de controle interno é apresentada pelo AUDIBRA (1992, p. 48), o qual diz: "controles internos devem ser entendidos como qualquer ação tomada pela administração [...] para aumentar a probabilidade de que os objetivos e metas estabelecidos sejam atingidos". Segundo o AUDIBRA, adotou-se a expressão controle interno para diferenciarem-se os controles originados internamente na organização daqueles originados externamente, como, por exemplo, os controles exigidos pela legislação.

Attie (1992, p. 199-200) complementa com a seguinte afirmação:

> O controle interno compreende todos os meios planejados numa empresa para dirigir, restringir, governar e conferir suas várias atividades com o propósito de fazer cumprir os seus objetivos. Os meios de controle incluem, mas não se limitam a: forma de organizações, políticas, sistemas, procedimentos, instruções, padrões, comitês, planos de contas, estimativas, orçamentos, inventários, relatórios, registros, métodos, projetos, segregação de funções, sistemas de autorização e aprovação, conciliação, análise, custódia, arquivo, formulários, manuais de procedimentos, treinamento, carta de fiança etc.

Paula (1999, p. 32-33) apresenta algumas outras definições:

> Atividade de avaliação independente e de assessoramento da

> administração, voltada para o exame e para a avaliação da adequação, eficiência e eficácia dos sistemas de controle e da qualidade do desempenho das áreas, em relação às atribuições e aos planos, metas, objetivos e políticas definidos para elas.
> [...] Órgão responsável pelo exame e avaliação dos sistemas de controle interno e das operações de todas as áreas e atividades da empresa.
> [...] Atividade de avaliação e medição multidisciplinar e independente dentro da organização, que tem como objetivo a revisão dos controles e das operações, de forma a fornecer subsídios à administração na tomada de decisão.

Pode-se notar que controle interno é definido pelos autores citados tanto como ação, planejamento e atividade de avaliação, quanto como órgão da empresa encarregado de examinar e avaliar os sistemas operacionais.

No entanto, para clareza e unificação dos conceitos apresentados, adotar-se-á a idéia de controle interno como a tarefa de examinar, orientar, governar, avaliar, revisar, adaptar e checar as atividades empresariais e, ao mesmo tempo, proteger os planos, metas, objetivos e políticas empresariais como forma de auxiliar os gestores nas tomadas de decisão para o alcance da eficácia, da eficiência e da qualidade dos serviços e produtos oferecidos pela organização.

1.1.2 Objetivos do Controle

Considerando-se as definições aqui apresentadas, verifica-se que o controle exerce uma função de garantia de que os problemas referentes à execução do trabalho serão previstos e evitados ou, ao menos, corrigidos.

Assim, Dias (1994) explana que o sistema de controles internos representa o conjunto de procedimentos ou atos, os quais possibilitam certa segurança referente a aspectos lógicos e técnicos do processo.

O autor complementa:

> O entendimento do objetivo do controle, de forma ampla e irrestrita, é, de fato, o principal elemento para conclusão sobre a melhor forma de sua adoção. A identificação deste objetivo possibilita a correspondente averiguação sobre seu alcance, o que assegura o controle sobre a eficácia do processo. (DIAS, 2004. p. 4).

Segundo Dias (2004), não é mais aceitável que controles sejam adotados simplesmente por questões conceituais e que culminem apenas em morosidade

na execução do processo e acúmulo de trabalho desnecessário aos colaboradores. É imprescindível que sejam estabelecidos os objetivos dos controles a serem implementados.

Na opinião do autor, o controle pode ser dividido por funções, de acordo com o objetivo estabelecido, em:

- função preventiva: exercem papel de guia para a execução do processo ou ainda na definição de atribuições e responsabilidades inerentes a cada processo. Tem a finalidade de evitar a ocorrência de problemas.

- função detectiva: não se propõe a impedir que o problema ocorra. Apenas possibilita identificação da possibilidade de ocorrência do erro.

- função corretiva: não evita a ocorrência do problema, porém serve como base para correção das causas dos problemas depois de ocorridos.

Quanto à importância dos controles internos no processo produtivo da organização, Dias (2004) conclui que se deve priorizar a adoção de controles preventivos, pois, uma vez ocorrido o problema, de nada adianta a sua identificação e tentativa de correção. O foco do controle deve estar, então, em buscar a segurança quanto à não ocorrência dos problemas potenciais ou de desvios nos processos.

Segundo o *American Institute of Certified Public Accountants* – AICPA (2006), os principais objetivos dos controles internos são:

– proteger os ativos da empresa;
– obter informações adequadas;
– promover a eficiência operacional da organização; e
– estimular a obediência e o respeito às políticas da administração.

Portanto, os controles internos servem para assegurar que as várias fases do processo decisório e do fluxo de informações sejam as mais confiáveis e que sejam adotadas medidas necessárias para que esta confiabilidade seja preservada durante todas as instâncias.

1.1.3 Fraudes

Fraudes podem ocorrer decorrentes de falhas no controle interno de uma empresa.

Paula (1999) considera a respeito deste assunto que, de acordo com a sua pesquisa, algumas entidades têm utilizado a auditoria interna para apurar responsabilidade pelos atos fraudulentos praticados pela administração e para assessorar a alta administração na análise de fatos com vistas a esclarecer e determinar a extensão de eventos irregulares e a eventual responsabilização e ainda avaliar e apurar denúncias.

A autora esclarece que a falta de registro do produto da atividade de apuração de irregularidade como inerente à prática da auditoria interna deve-se ao fato de que essa apuração precisa ser vista como uma conseqüência das atividades normais de auditoria e não como um fim em si mesmo e ainda alerta a necessidade de evitar-se tal atividade, na medida do possível, para que o auditado não se sinta policiado, em lugar de assessorado.

É imprescindível efetuar-se uma diferenciação entre fraude e erro no âmbito da auditoria interna. Segundo Lima (2003), o termo fraude aplicar-se-ia a atos de caráter voluntário de omissão e manipulação de transações e operações, adulteração de documentos, registros, relatórios e demonstrações contábeis, tanto em termos físicos como monetários. Em contrapartida, o erro poderia caracterizar-se como atos involuntários de omissão, desatenção, desconhecimento ou interpretação equivocada de fatos na elaboração de registros e demonstrações contábeis, bem como de transações e operações da instituição, tanto em termos físicos quanto monetários.

A autora comenta que o papel do auditor interno, quanto à prevenção de erros e fraudes, é o de informar à administração sobre quaisquer indícios levantados no decorrer do seu trabalho na organização.

Em outra perspectiva, Barata (1999) explica que detectar erros e fraudes não é, em si mesmo, uma finalidade da auditoria, pois se assim fosse, admitir-se-ia que, em princípio, erros e fraudes seriam uma realidade, colocando, de

imediato, em causa a idoneidade moral e profissional das pessoas da empresa auditada.

O autor fundamenta-se na declaração de Bevis (apud BARATA, 1999) de que o principal objetivo da auditoria externa foi, em tempos remotos, a descoberta de erros e fraudes e, hoje, o auditor passou a interessar-se essencialmente pela integridade das demonstrações financeiras, tendo como preocupação básica a coleta rápida e completa de provas que lhe permitam estabelecer o seu valor e a autenticidade, bem como fundamentar o seu parecer.

Pode-se concluir que um sistema de controle interno bem elaborado tem a capacidade de minimizar a ocorrência de erros e fraudes e ainda possibilita ao auditor interno manter o foco na consistência das informações da empresa.

1.2 AUDITORIA

O sucesso de uma administração empresarial depende muito da verificação da exatidão e fidelidade das informações utilizadas pelos seus colaboradores. Por isso, auditoria é uma atividade crítica ao passo que possibilita aumentar a confiabilidade das medidas do controle interno adotado pela organização.

Para que a auditoria organizacional seja confiável e eficiente, deve-se, no entanto, seguir alguns passos imprescindíveis à sua acurácia. O primeiro deles é entender o significado de auditoria e suas finalidades, tarefa realizada a seguir.

1.2.1 Conceitos de Auditoria

Para Lima (2003), auditoria é um exame analítico de uma operação da empresa, com o intuito de verificar a sua validade. A autora explica que, segundo as Normas Internacionais de Auditoria, a auditoria das demonstrações contábeis

tem por objetivo possibilitar que o profissional expresse opinião sobre se essas demonstrações foram preparadas com as adequações e aderência às diretrizes e normas da organização, aos Princípios Fundamentais de Contabilidade e às normas usuais de auditoria, proporcionando credibilidade à Contabilidade.

Outro conceito encontrado é o formulado por Müller que diz:

> A auditoria deve ser compreendida como um conjunto de ações de assessoramento e consultoria. A verificação de procedimentos e a validação dos controles internos utilizados pela organização permitem ao profissional auditor emitir uma opinião de aconselhamento à direção ou ao staff da entidade em estudo, garantindo precisão e segurança na tomada de decisão. (MÜLLER, 2001, p. 1)

Para os efeitos de simplificação e melhor adequação da definição ao uso do termo no presente trabalho, a pesquisadora conceitua auditoria como exame das operações, dos sistemas de informação, dos recursos humanos e das estruturas organizacionais, como forma de se buscar integridade e confiabilidade das informações e registros empresariais, com o intuito de se alcançar eficiência e eficácia.

1.2.2 Finalidades da Auditoria

Dias (2004, p. 6-19) ressalta que, para que a confiabilidade da auditoria seja alcançada, a avaliação dos controles internos deve compreender três fases básicas, quais sejam:

- levantamento do processo;
- análise dos controles internos;
- verificação da conformidade dos procedimentos executados e da eficácia dos controles internos adotados no processo.

Quanto ao levantamento do processo, o autor salienta que é nesta fase que os auditores elaboram o fluxo do processo, documentam os procedimentos adotados, os objetivos e os riscos envolvidos, além da identificação de quais os controles utilizados para o alcance da eficácia. É a partir deste prévio

conhecimento sobre o funcionamento da empresa e de seu negócio que o auditor será capaz de, com o auxílio das fases seguintes, avaliar os processos de controles internos utilizados na organização.

Em uma segunda fase, já conhecendo os processos utilizados pela empresa, o auditor passa a fazer análise detalhada da performance dos controles que suportam cada etapa do sistema. Neste momento, o auditor checa se cada passo na execução dos procedimentos necessários tem seus respectivos possíveis riscos identificados e se o controle adotado pela administração é suficiente para garantir a prevenção de falhas, a detecção de possíveis problemas relacionados ao tipo de negócio praticado e para oferecer base para a correção de possíveis distorções decorrentes de ações ou eventos externos ao processo.

Por último, o auditor tem a tarefa de verificar a conformidade dos procedimentos executados e a efetiva aplicação, pelo auditado, dos controles internos adotados no processo.

Barata (1999, p. 84-85) apresenta uma síntese dos objetivos da auditoria, a saber:

> a) emitir um parecer sobre as contas e os resultados, sua veracidade e conformidade com os PCGA, aplicados de forma consistente e segundo a legislação aplicável;
> b) dar credibilidade às contas, nos planos interno e externo, por intermédio de uma entidade independente de reconhecido mérito;
> c) contribuir para a boa imagem da empresa no mercado;
> d) dar elementos de índole económica e financeira que fundamentem: aumentos, alienações e aquisições de capital próprio e eventuais empréstimos obrigacionistas;
> e) actuar como <<força>> persuadora na prevenção contra erros, fraudes e outras anomalias, nomeadamente por via da sua acção de controlo;
> f) velar pelo cumprimento dos normativos legais nas suas vertentes económica, financeira, ambiental e social;
> g) aconselhar a administração:
> - Fornecendo-lhe elementos para eventuais melhorias dos serviços e do reforço e qualidade do controlo interno;
> - Libertando-a, de alguma forma, das suas responsabilidades de administração;
> - Contribuindo para um melhor planejamento fiscal ao nível dos impostos sobre lucros e outros, salvaguardando a empresa de infracções fiscais.

Lima (2003) define o controle do patrimônio como o objeto de aplicação da auditoria. A autora identifica várias formas de controle, dentre elas o registro contábil, documentos, fichas e arquivos em geral que comprovem a veracidade dos registros, a legalidade e a legitimidade dos atos e fatos administrativos.

Já o objetivo da auditoria de demonstrações financeiras, segundo Aguiar (1992), é a emissão de um parecer sobre a adequação com que tais demonstrações representam a posição financeira, o resultado das operações e as modificações sofridas na situação financeira, de acordo com os princípios contábeis geralmente aceitos.

1.2.3 Auditoria Interna

De acordo com o Conselho Federal de Contabilidade – CFC (2006, p. 2), auditoria interna é "o conjunto de procedimentos técnicos que tem por objetivo examinar a integridade, adequação e eficácia dos controles internos e das informações sobre aspectos físicos, contábeis, financeiros e operacionais da entidade".

Rittenberg e Schiwieger (2001) definem auditoria interna como uma independente e objetiva garantia e atividade de consultoria projetada para adicionar valor e melhorar as operações de uma organização. Ajuda uma organização a alcançar seus objetivos ao trazer uma sistemática e disciplinada abordagem para avaliar e melhorar a eficácia da gerência de risco, do controle e do processo de governança. [1]

Lima (2003) identifica as seguintes características inerentes à auditoria interna:

Figura 01 – Principais características da auditoria interna

Agente	Auditor interno (empregado da própria instituição)
Ação	Auxílio à alta administração

[1] Tradução da pesquisadora ao original: "*An internal audit is defined as an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control and governance process".*

Atividade	Adequação do controle interno em relação à prevenção de fraudes e perdas e aderência às normas legais e às diretrizes da alta administração
Execução dos trabalhos	De acordo com as oportunidades das funções operacionais
Grau de independência	Baixo em relação à alta administração; satisfatório quanto aos demais níveis
Destino dos trabalhos	Diretoria, sócios, conselhos administrativo e fiscal e auditores externos

Fonte: LIMA, Diana Vaz de, 2003, p. 20.

2 SISTEMA DE SEGURANÇA DE INFORMAÇÃO

Os objetivos deste capítulo são o de evidenciar o papel da informação nas organizações e a ideal forma de utilização dos sistemas de informação para auxiliar os processos decisórios dos gestores e clientes (usuários).

A informação é a base para a tomada de decisões gerenciais e operacionais; por isso, torna-se imprescindível a otimização do fluxo de informações organizacionais e a adequada escolha e utilização das tecnologias, tais como, *softwares* ERP (*Enterprise Resource Planning)*, SAD (Sistema de Apoio à Decisão), SIG (Sistema de Informação de Gestão) e EIS (*Enterprise Information System*), Banco de Dados (*Data Warehouse*), Inteligência Artificial (*Data Mining*), que são as principais ferramentas de apoio à decisão disponíveis no mercado, e ainda o apropriado uso de sistemas de telecomunicação e da Internet.

As empresas hoje investem muito em sistemas de informação para criação e armazenamento de dados, porém, muitas vezes, esquecem-se de auditar o uso que está sendo feito das tecnologias e das informações disponibilizadas pelos meios tecnológicos. O resultado observado é uma grande perda de dados de clientes, informações estratégicas e, conseqüentemente, de poder competitivo.

2.1. CONCEITOS

Oliveira, define sistema de informação da seguinte forma:

> Sistema é um conjunto de rotinas que contém vários programas e subprogramas, rotinas essas que são desenvolvidas para a aplicação em áreas específicas da empresa por meio do uso de computador, com o objetivo de gerar informações e produzir relatórios de acompanhamento e controle interno. (OLIVEIRA, 2000. p. 33).

No glossário de termos de auditoria do *Office of the Auditor General of Canadá* (1995. p. 10), encontram-se as seguintes funções para auditoria baseada em sistemas:

> Na auditoria baseada em sistemas, a natureza, extensão e cronograma dos procedimentos detalhados de auditoria baseiam-se no estudo e avaliação organizados dos sistemas e controles relevantes da organização auditada. Esse estudo e avaliação, realizados na fase inicial da auditoria, determinam que sistemas são importantes para a administração da organização auditada e determinam até que ponto os testes são necessários, durante a fase de verificação, para avaliar o nível de confiabilidade dos controles e dos relatórios enviados ao Parlamento.
> A abordagem baseada em sistemas se destina a permitir que o auditor concentre o esforço da auditoria em áreas em que o desempenho não é adequadamente controlado e demonstrado, e onde os controles não existem ou não funcionam corretamente. Ao término da verificação, o auditor deverá ser capaz de destacar os pontos fortes e os pontos fracos dos sistemas-chave e dos controles respectivos, além de indicar as causas e efeitos dos pontos fracos. Estará também apto a elaborar conclusões e recomendações.

Por fim, auditoria de sistemas pode ser entendida, segundo Fontes (1991) pelo ramo da auditoria que revisa e avalia os controles internos informatizados visando proteção aos ativos da organização; integridade dos dados, e alcance eficaz e eficientemente os objetivos da organização.

2.2. IMPORTÂNCIA DA AUDITORIA EM SISTEMAS DE INFORMAÇÃO

A segurança de sistemas de informação é, evidentemente, um tema que transcende o tema auditoria e envolve desde questões relacionadas com o ambiente físico, eletromagnético ou ótico de funcionamento da comunicação, até a "engenharia social", que estuda o comportamento das pessoas em relação ao uso dos recursos tecnológicos, com relação à escolha ou ao uso de senhas e procura influenciar pessoas pelo poder da persuasão.

Conseqüentemente, não seria possível abordar neste trabalho todas essas questões. O presente estudo volta-se, portanto, para a importância da auditoria na análise ou no planejamento de uma política de segurança, como meio de correção e de prevenção de possíveis falhas e vulnerabilidades nos sistemas

informatizados de processamento de dados.

Na prática, muitos ou talvez a maior parte dos problemas de segurança que ocorrem nos sistemas de informação (como invasão de máquinas com destruição, alteração ou roubo de informações) são conseqüência direta da existência de *bugs* de *software*, os quais são explorados pelo agente, ou ainda de falha na segurança física ou lógica do ambiente informatizado. No entanto, o fator humano também tem grande influência na fragilidade da segurança dos ativos informacionais. Nesse sentido, todo conhecimento que o profissional de auditoria puder ter sobre programação e sobre comportamento humano será útil para a sua capacitação.

Segundo a Norma ISO (*International Organization for Standardization*) 17799, de 2001, são três itens básicos da segurança da informação, conforme se segue:

- confidencialidade: garantia de que a informação é acessada somente por pessoas autorizadas;

- disponibilidade: garantia de que os usuários autorizados têm acesso à informação e aos ativos correspondentes quando necessário;

- integridade: a segurança da informação é possibilitada a partir de quatro etapas básicas, quais sejam: identificação, quantificação, tratamento e monitoração dos riscos.

O gerenciamento de riscos é um processo contínuo, que não termina com a implementação de uma medida de segurança, e é nesta última etapa que entra o papel do auditor de sistemas informatizados. Através de uma monitoração constante, é possível identificar quais áreas foram bem sucedidas e quais precisam de revisões e ajustes.

Essa monitoração deve ser baseada em um modelo de gestão de segurança, que defina atribuições, responsabilidades e fluxos de comunicação interdepartamentais. Algumas atividades importantes são as seguintes:

- elaboração de uma política de segurança, composta por diretrizes, normas, procedimentos e instruções, indicando como deve ser realizado o trabalho; e

- auditoria de segurança, a fim de assegurar o cumprimento dos padrões definidos e, conseqüentemente, medir a eficácia da estratégia de segurança adotada. (LAUREANO, 2006)

As principais fases ou atividades da auditoria em sistema de informação podem assim serem subdivididas:

- identificação dos ativos: determinar quais os ativos deverão ser incluídos na lista de itens a serem auditados. Servidores, estações de trabalho, sistemas operacionais, *softwares, firewalls*, bancos de dados, roteadores, dentre outros recursos, podem fazer parte da análise;

- análise das vulnerabilidades: identificar, quantificar e analisar os riscos e vulnerabilidades dos ativos anteriormente listados e sugerir respectivas ações preventivas ou corretivas;

- plano de ação: nesta etapa, propõe-se um plano de ação para a implementação das ações corretivas ou preventivas, o qual eleve o nível de segurança.

De acordo com essas fases relacionadas acima, pode-se resumir os principais benefícios da realização de uma auditoria de sistemas informatizados como se segue:

- conhecimento da real situação da empresa;
- identificação das possíveis vulnerabilidades das aplicações e suas implicações para o negócio da organização;
- listagem das possíveis ameaças existentes no contexto das informações tratadas pelos *softwares* analisados;
- elaboração de recomendações e plano de ação para prevenir/ corrigir as vulnerabilidades apontadas;
- prevenção do desperdício de recursos na implementação de controles não prioritários;
- identificação das medidas de segurança apropriadas;
- minimização dos riscos identificados e maior garantia das informações corporativas relacionadas às aplicações utilizadas para processamento de dados; e
- tomada de decisão baseada em fatos reais.

Ao final da execução do serviço de auditoria poder-se-á entregar ao

cliente os seguintes produtos, conforme os benefícios acima apontados :

- relatório de riscos e vulnerabilidades;
- plano de ação, com devidas recomendações de mudanças necessárias.

2.3. TÉCNICAS DE AUDITORIA EM SISTEMAS DE PROCESSAMENTO DE DADOS

De acordo com Sales (2006), os trabalhos de auditoria desenvolvidos visando assegurar o correto uso dos sistemas de informação englobam os seguintes parâmetros do controle interno: fidelidade da informação em relação ao dado; segurança física; segurança lógica; confidencialidade; obediência à legislação; eficiência; eficácia e obediência às políticas da alta administração.

Para auxiliar o desenvolvimento dos trabalhos de auditoria, são adotadas algumas técnicas e metodologias. As técnicas utilizadas pelos auditores na análise de sistemas de informações computadorizados são procedimentos que auxiliarão o profissional no alcance de seu objetivo, qual seja, a formação de opinião sobre o objeto em questão.

As principais técnicas, conforme Gil (2000), são enumeradas a seguir:

- programa de computador: tem a finalidade de correlacionar os arquivos, tabular e examinar seu conteúdo para analisar os registros efetuados no sistema;

- questionários: conjunto de perguntas elaboradas com o objetivo de verificar a adequacidade de determinado ponto de controle do ambiente computacional aos parâmetros do controle interno (segurança lógica, segurança física, obediência à legislação, eficácia, eficiência);

- simulação de dados (*test-deck*): corresponde à elaboração de um conjunto de dados para serem submetidos à teste em um programa de computador específico, para que seja verificada a sua lógica de processamento;

- visita *in loco*: diz respeito à atuação pessoal do auditor no ambiente informatizado junto a sistemas, procedimentos e instalações físicas do ambiente

tecnológico;

- mapeamento estatístico (*mapping*): técnica computacional que pode ser utilizada pelo auditor com a finalidade de efetuar verificações em processamento de dados por programas computacionais para flagrar situações como rotinas não utilizadas e quantidade de vezes que determinada rotina foi utilizada quando da sua submissão a processamento de uma quantidade de dados;

- rastreamento dos programas (*tracing*): técnica para efetuar-se seguimento de caminho de uma transação durante o processamento do programa que possibilita a identificação de rotinas fraudulentas pela alimentação de transações particulares por meio de rastreamento das instruções dadas a essas transações;

- entrevista: freqüentemente utilizada em conjunto com outras técnicas de auditoria como visita *in loco*, aplicação de questionários e outras. Corresponde à realização de reunião entre o auditor e os auditados;

- análise de relatórios/ telas: implica em análise de documentos, relatórios e telas do sistema submetido à auditoria;

- simulação paralela: consiste na elaboração de um programa de computador utilizado para simulação das funções de rotina do sistema auditado;

- análise do *log*/ *accounting*: é a análise de arquivos gerados por uma rotina componente do sistema operacional, o qual contém registros de utilização do *hardware* e do *software* que compõem um ambiente computacional;

- análise de programa-fonte: análise virtual da linguagem de programação utilizada para desenvolver o sistema submetido à auditoria. Esta técnica exige profundos conhecimentos de processamento eletrônico de dados e das linguagens utilizadas no desenvolvimento dos sistemas auditados;

- exibição parcial da memória (*snap shot):* técnica utilizada como auxílio à depuração de programas por meio de análise de listagem ou de gravação do conteúdo das variáveis do programa quando determinado registro está em processamento.

Outras ferramentas de apoio ao trabalho do auditor são as normas ISO (*International Organization for Standardization*). No caso específico da auditoria de sistemas de informação, a norma a ser adotada é a ISO/ IEC 17799.

Essa norma pode assim ser resumida:

- objetivo: esta norma fornece recomendações de gestão da segurança da informação para uso por aqueles que são responsáveis pela introdução, implementação ou manutenção da segurança em suas organizações.

- termos e definições: para os efeitos desta norma, aplicam-se as seguintes definições:

- segurança da informação: preservação da confidencialidade, integridade e disponibilidade da informação.

- confidencialidade: garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.

- integridade: salvaguarda da exatidão e inteireza da informação e dos métodos de processamento.

- disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

- avaliação de risco: avaliação das ameaças, impactos e vulnerabilidades da Informação ou das instalações de processamento da informação e da probabilidade de ocorrência dos riscos identificados.

- gerenciamento de risco: processo de identificação, controle e minimização ou eliminação de riscos de segurança que podem afetar os sistemas de informação, a um custo aceitável.

Os domínios desta norma são os seguintes (SAINT-GERMAIN, 2005, p. 60-66):

- política de segurança da informação

Objetivo: prover à direção uma orientação e apoio para a segurança da informação.

Convém que a direção estabeleça uma política clara e demonstre apoio e comprometimento com a segurança da informação através da elaboração e manutenção de uma política de segurança da informação para toda organização.

- segurança organizacional

Objetivo: gerenciar a segurança da informação na organização.

Convém que uma estrutura de gerenciamento seja estabelecida para iniciar e controlar a implementação da segurança da informação dentro da organização. Convém que fóruns apropriados de gerenciamento com liderança da direção sejam estabelecidos para aprovar a política de segurança da informação, atribuir as funções da segurança e coordenar a implementação da segurança através da organização.

- classificação e controle dos ativos de informação

Objetivo: manter a proteção adequada dos ativos da organização.

Convém que todos os principais ativos de informação sejam inventariados e tenham um proprietário responsável. O inventário dos ativos ajuda a assegurar que a proteção está sendo mantida de forma adequada.

- segurança em pessoas

Objetivo: reduzir os riscos de erro humano, roubo, fraude ou uso indevido das instalações.

Convém que responsabilidades de segurança sejam atribuídas na fase de recrutamento, incluídas em contratos e monitoradas durante a vigência de cada contrato de trabalho.

- segurança física e do ambiente

Objetivo: prevenir acesso não autorizado, dano e interferência às informações e instalações físicas da organização.

Convém que os recursos e instalações de processamento de informações críticas ou sensíveis do negócio sejam mantidos em áreas seguras, protegidas por um perímetro de segurança definido, com barreiras de segurança apropriadas e controle de acesso.

Convém que estas áreas sejam fisicamente protegidas de acesso não autorizado, dano ou interferência.

- gerenciamento das operações e comunicações

Objetivo: garantir a operação segura e correta dos recursos de processamento da informação.

Convém que os procedimentos e responsabilidades pela gestão e

operação de todos os recursos de processamento das informações sejam definidos. Isto abrange o desenvolvimento de procedimentos operacionais apropriados e de resposta a incidentes.

- controle de acesso

Objetivo: controlar o acesso à informação. Convém que o acesso à informação e processos do negócio seja controlado na base dos requisitos de segurança e do negócio.

Convém que se leve em consideração as políticas de autorização e disseminação da informação.

- desenvolvimento e manutenção de sistemas

Objetivos: garantir que a segurança seja parte integrante dos sistemas de informação. Isto incluirá infra-estrutura, aplicações do negócio e aplicações desenvolvidas pelo usuário.

O projeto e a implementação dos processos do negócio que dão suporte às aplicações e aos serviços podem ser cruciais para a segurança.

Convém que requisitos de segurança sejam identificados e acordados antes do desenvolvimento dos sistemas de informação.

- gestão da continuidade do negócio

Objetivos: não permitir a interrupção das atividades do negócio e proteger os processos críticos contra efeitos de falhas ou desastres significativos.

Convém que o processo de gestão da continuidade seja implementado para reduzir, para um nível aceitável, a interrupção causada por desastres ou falhas de segurança (que pode ser resultante de, por exemplo, desastres naturais, acidentes, falhas de equipamentos e ações intencionais) através da combinação de ações de prevenção e recuperação.

- conformidade

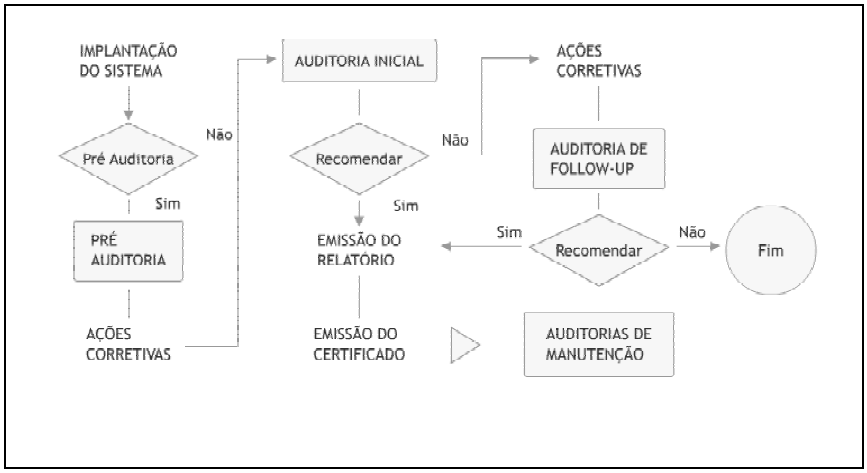
Objetivo: evitar violação de qualquer lei criminal ou civil, estatutos, regulamentações ou obrigações contratuais e de quaisquer requisitos de segurança.

O projeto, a operação, o uso e a gestão de sistemas de informação

podem estar sujeitos a requisitos de segurança contratuais, regulamentares ou estatutários.

Um modelo de fluxograma das atividades desenvolvidas por um auditor nas suas tarefas de auditoria de sistemas pode ser visualizado na figura a seguir:

Figura 02 – Fluxograma da atividade de auditoria de sistema



As fases ilustradas no fluxograma das atividades podem assim ser detalhadas:

- pré-auditoria: é realizada quando da implementação dos sistemas, como forma de prevenção e de identificação prévia de possíveis falhas ou vulnerabilidades.

- auditoria inicial: é realizada por meio da análise de documentos e de *logs* do sistema, para que seja assegurado o cumprimento das normas e das políticas de segurança da empresa e ainda para identificar possíveis problemas a serem corrigidos. Nesta fase são registradas as discrepâncias e apresentadas as sugestões para ações corretivas.

- auditoria de manutenção ou de supervisão: checa se as sugestões de correção foram implementadas e assegura a manutenção do nível de segurança já alcançado. Busca também a melhoria contínua e certifica-se de que não houve alterações nos procedimentos já adotados.

APRESENTAÇÃO E DISCUSSÃO DOS RESULTADOS

Para realizar o estudo exploratório proposto, foram empreendidas pesquisas bibliográficas no acervo da biblioteca do Centro Universitário de Brasília, leitura de matérias disponíveis em periódicos e revistas especializadas, além de consultas a artigos divulgados na rede mundial de computadores.

Os autores pesquisados alertaram quanto à importância dos controles internos para a garantia da eficácia e da eficiência do processo produtivo de uma organização. Percebe-se também uma preocupação no sentido de especificar qual o tipo de controle interno deve ser adotado, ficando evidente que há prioridade na adoção de controles preventivos, de forma a coibir a ocorrência de erros e fraudes, pois uma vez ocorrido o problema é de pouca valia a sua identificação e tentativa de correção. Há o consenso, então, de que o foco do controle deve estar na busca da segurança quanto à não ocorrência dos problemas potenciais.

A auditoria interna é definida pelos autores como responsável pela verificação de procedimentos e a validação dos controles internos utilizados pela organização. Esta verificação e validação permitem ao profissional auditor emitir uma opinião de aconselhamento à direção.

O papel da auditoria, então, é o de garantir que sejam adotadas medidas necessárias para manter a confiabilidade dos controles internos, de forma a assegurar que o fluxo de informações necessárias seja o mais confiável possível.

Quanto à auditoria de sistemas, o papel do auditor não é diferente das demais auditorias existentes. O profissional procura, na auditoria de sistemas de processamento de dados, assegurar o cumprimento dos padrões definidos a fim de garantir a confidencialidade, a disponibilidade e a integridade das informações. A sua atuação, conforme a literatura pesquisada revelou, deve ser no sentido de prevenir a ocorrência de erros e fraudes, além de medir a eficácia da estratégia de segurança adotada. Para isso, o auditor utiliza-se de técnicas específicas e de procedimentos descritos nas normas ISO como meio de facilitar a sua tarefa.

Seguindo-se estas técnicas e procedimentos descritos no presente estudo, o profissional auditor está apto a elaborar um relatório de riscos, ameaças e vulnerabilidades e a sugerir um plano de ação, com devidas recomendações de mudanças necessárias.

O importante neste trabalho de auditoria de sistemas, como em qualquer outro trabalho de auditoria, é que este processo deve ser cíclico. Sempre que um componente for implementado ou modificado no ambiente de informação, é necessária a realização de uma pré-auditoria para a prévia identificação de falhas, ameaças ou vulnerabilidades potenciais e para a prevenção de problemas. São necessárias ainda auditorias periódicas, previstas para assegurar o cumprimento das normas e das políticas de segurança adotadas pela empresa e ainda para identificar problemas que surgirem durante a execução das tarefas rotineiras da organização. Nesta fase são sugeridas as correções para os problemas identificados. Por fim, deve-se, como forma de checar se as sugestões de correção foram implementadas e garantir a manutenção do nível de segurança já alcançado, realizar a chamada auditoria de supervisão.

Seguindo-se as orientações dos autores, chega-se à dedução de que a auditoria interna de sistemas é uma ferramenta eficiente por testar os controles internos e identificar os possíveis erros e deficiências existentes bem como apontar soluções e ainda atuar de forma a evitar os riscos identificados.

CONCLUSÃO

Cada empresa possui suas particularidades no que diz respeito à tecnologia adotada e à cultura organizacional. No entanto, com o ascendente número de ameaças, internas e externas, torna-se obrigatório que as organizações auditem com freqüência os seus controles de segurança, seja de segurança de *software*, *hardware* ou *peopleware*, com o intuito de proteger seus principais ativos. Prevenir falhas e fraudes é o meio mais eficaz de se garantir disponibilidade e confiança da infra-estrutura tecnológica que suporta o negócio organizacional.

Assim, a importância do papel da auditoria dos sistemas de processamento eletrônico de dados está, principalmente, em garantir o uso seguro das informações e da infra-estrutura de sistemas de informação das empresas. A identificação das vulnerabilidades existentes nos sistemas e a recomendação de ações preventivas ou corretivas, de forma a assegurar a confidencialidade, a integridade e a disponibilidade das informações corporativas podem, inclusive, garantir a continuidade do negócio da organização.

Resguardar a conduta adequada para o seu manuseio, controle, proteção e descarte das informações é uma forma de preservar um dos ativos mais preciosos de uma empresa: as suas informações.

O auditor deve considerar que a segurança em ambientes computacionais não se restringe somente aos *softwares* e *hardwares* utilizados em uma rede ou instalados em servidores e nas estações de trabalho. Engloba também o acesso físico das pessoas no ambiente onde estão dispostos os equipamentos de informática e de telecomunicações. Desta forma, não seriam muito úteis os programas para prover a segurança das informações de seu ambiente empresarial, quando a porta principal de acesso às informações, ou seja, a porta do CPD (Centro de Processamento de Dados), está vulnerável.

Por fim, vale ressaltar que a auditoria em sistemas de informações define o arquétipo tecnológico e organizacional ideal visando a proteção das informações nas organizações, de forma a estabelecer uma arquitetura de

segurança compatível com a estrutura e com a cultura organizacionais.

Desta forma, observa-se que a auditoria de sistemas, conforme encontrado na literatura pesquisada, é fundamental para a monitoração e avaliação dos controles internos como forma de garantia da segurança da informação.

Como sugestão para estudos futuros, aponta-se para a necessidade de se pesquisar sobre a importância da auditoria interna no acompanhamento de aquisições, desenvolvimento e implementação de sistemas, visto que o presente trabalho teve o seu foco voltado à auditoria de sistemas já existentes em uma organização. Tal estudo poderá abordar questões como aquisição e manutenção de *softwares* e de infra-estrutura tecnológica, desenvolvimento e manutenção de *softwares*, instalação e atualização de sistemas de informação, além de monitoração dos serviços terceirizados em tecnologia da informação.

Para isso, a auditoria deverá atuar na definição e avaliação da infra-estrutura de tecnologia, segurança física do ambiente tecnológico, nos processos e seus controles internos, na operacionalização de bancos de dados, e no controle de acesso a *hardwares* e *softwares*.

A auditoria em sistemas de informação pode auxiliar a administração empresarial a transformar a abordagem da função de segurança de tecnologia com foco em atividades corretivas, ou seja, ação quando os problemas já ocorreram, para uma abordagem preventiva, coordenada para o estabelecimento e policiamento de princípios, comportamentos e procedimentos, o que culminará em uma política de segurança efetiva.

REFERÊNCIAS BIBLIOGRÁFICAS

AGUIAR, Amadeu R.; FACCO, Edimar; VAINI, Luiz Carlos. Conselho Regional de Contabilidade do Estado de São Paulo. *Curso básico de auditoria 1 : normas e procedimentos*. 2. ed. São Paulo : Atlas, 1992.

AMERICAN INSTITUTE OF CERTIFIED PUBLIC ACCOUNTANTS – AICPA (Estados Unidos) (Org.). *Practice Development/Financial Reporting:* The requirement to evaluate a company's. Disponível em: <http://www.aicpa.org/pubs/jofa/may2004/duffy.htm>. Acesso em: 25 mar. 2006.

ARIMA, Carlos Hideo. *Metodologia de auditoria de sistemas.* São Paulo : Érica, 1994.

ATTIE, William*. Auditoria: Conceitos e Aplicações*. 2 ed. São Paulo: Atlas, 1984.

_____, William*. Auditoria interna*. São Paulo : Atlas, 1992.

BARATA, Alberto da Silva. *Contabilidade, auditoria e ética nos negócios*. 2. ed. Lisboa : Editorial Notícias, 1999.

BRASIL. CONSELHO FEDERAL DE CONTABILIDADE. Resolução nº 780, de 24 de março de 1995. Aprova a NBC T 12 – Da Auditoria Interna. Disponível em: <http://www.cfc.org.br/resolucoes_cfc/RES_780.DOC>. Acesso em 05 mar. 2006.

_____. INSTITUTO DOS AUDITORES INTERNOS DO BRASIL - AUDIBRA. *Normas brasileiras para o exercício da auditoria interna*. 2. ed. São Paulo : Audibra, 1992.

CABRAL, Luiz Novaes; BLEINAT, Sergio Aparecido. Conselho Regional de Contabilidade do Estado de São Paulo. *Curso básico de auditoria 1 : normas e procedimentos*. 2. ed. São Paulo : Atlas, 1992.

DIAS, Sergio Vidal dos Santos. *Auditoria de processos: teoria, aplicabilidade, metodologia de trabalho e resultados alcançados.* 1. ed. Niterói : Impetus, 2004.

FONTES, Joaquim Rubens. *Manual de Auditoria de Sistemas*. Rio de Janeiro : Ciência Moderna, 1991.

GIL, Antonio de Loureiro. *Auditoria de Computadores.* 5. ed. São Paulo : Atlas. 2000.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION - Norma Nacional de Segurança de Informação [NBR ISO/IEC-17799:2001] Disponível na Internet em http://josers.cjb.net/. Acesso em 11 mar. 2006.

KÖCHE, José Carlos. Fundamentos de metodologia científica. 13. ed. Porto Alegre: Vozes, 1992.

KOTLER, Philip. *Administração de marketing*. São Paulo : Atlas, 1975.

LAUREANO, Marcos Aurelio Pchek. *Uma abordagem para a proteção de detectores de intrusão baseadas em máquinas virtuais*. Dissertação (Mestrado)-Programa de Pós-Graduação em Informática Aplicada, Pontifícia Universidade Católica do Paraná. 2004.

LIMA, Diana Vaz de. F*undamentos da auditoria governamental e empresarial: com modelos de documentos e pareceres utilizados*. São Paulo : Atlas, 2003.

MARTINS, Eliseu. *Contabilidade de custos*. 4. ed. São Paulo : Atlas, 1995.

MAUTZ, Robert Kuhn. *Princípios de auditoria*. 4. ed. São Paulo : Atlas, 1985.

MÜLLER, Aderbal Nicolas, Desmistificando o trabalho da auditoria. *Revista FAE Business*, Curitiba, p. 1**,** dez./ 2001.

OFFICE of the Auditor General of Canada. *Glossário de termos de auditoria do manual de auditoria integrada.* 1. ed. Salvador : Tribunal de Contas do Estado da Bahia, 1995.

OLIVEIRA, Edson. *Contabilidade Informatizada*. 2. ed. São Paulo: Atlas, 2000.

PAULA, Maria Goreth Miranda Almeida. *Auditoria interna: embasamento conceitual e suporte tecnológico*. São Paulo : Atlas, 1999.

PRADO, Larissa. *Quatro Passos no Gerenciamento de Riscos*. Disponível em <http://www.securenet.com.br/artigo.php?artigo=114>. Acesso em 23 abr. 2006.

RITTENBERG, Larry E., SCHIWIEGER, Bradley J. *Auditing : concepts for a changing environment*. 3. ed. Orlando : Hartcourt College Publishers, 2001.

SAINT-GERMAIN, René. *Information Security Management Best Practice Based on ISO/IEC 17799.* The Information Management Journal – July/August 2005. Disponível em HBSCO HOST Research Databases no Site do UniCEUB. Acesso em 25 fev. 2006.

SALES, Rafael Floriano Souza. *IT Governance módulo de política de segurança:* melhorando processos para melhores objetivos. Disponível em <http://www.tompast.org/opensource/files/TOMPAST_GOV_POLSEG_05MARC2006-001.pdf>. Acesso em 24.mar.2006.