A AUDITORIA CONTÁBIL EM COMPUTADORES

Artur Olavo Ferreira
Heber Luiz de Souza
Alunos do Programa de Mestrado em Ciências Contábeis da UERJ

Prof.ª Gilcina Guimarães Machado
Prof.ª Doutora do Mestrado em Ciências Contábeis da UERJ

RESUMO

Este artigo tem por objetivo mostrar algumas peculiaridades da auditoria a ser realizada em empresas que utilizam computadores para o processamento de dados e para a elaboração de demonstrações contábeis, alertando para a importância da segurança (física e lógica) do sistema da empresa auditada como elemento de avaliação do risco da auditoria.

ABSTRACT

This article has for objective to show the peculiarities of the auditing to be accomplished in that modern business atmosphere, alerting for the importance of the safety of the data of the audited company as element of evaluation of the risk of the auditing.

1 INTRODUÇÃO

Para atender às exigências do mundo globalizado, em que a rapidez no processamento de grande volume de dados pode significar a sobrevivência da empresa, cada vez mais os recursos e programas computacionais passam a assumir extrema importância no seu processo administrativo. Tarefas repetitivas e de controle são os principais trabalhos a serem realizados pelos computadores, com a vantagem de, se bem definidos, reduzirem a possibilidade de falhas.

Castells, ao tecer comentários relativos aos efeitos dos novos recursos de processamento de dados, observa que

> O processo atual de transformação tecnológica expande-se exponencialmente em razão de sua capacidade de criar uma interface entre campos tecnológicos mediante uma linguagem digital comum na qual a informação é gerada, armazenada, recuperada, processada e transmitida. Vivemos em um mundo que se tornou digital. (1999)

Os procedimentos contábeis a serem efetuados pelas empresas também enquadraram-se nessa nova ordem administrativa, com a evolução dos costumes em decorrência da utilização de computadores em todos os seus setores, principalmente na maneira como as transações são realizadas e

nos tipos de tarefas executadas simultaneamente.

Há de se ficar alerta para os riscos que as empresas correm ao investir na digitalização do seu acervo e na informatização de seus ambientes sem considerar a questão dos "vírus", do "hackers" e das quebras de segurança feitas pelo usuário interno no intuito de ter acesso a informações privilegiadas, buscando auferir vantagem pessoal ou utilizá-la para fins de fraude ou espionagem industrial. (Lima, 2001, p. A-2)

Em que pese o ambiente computacional reinante nas empresas, o objetivo da auditoria independente continua sendo o mesmo, ou seja, o de verificar a fidedignidade das informações contidas nas demonstrações contábeis. As diferenças referem-se, basicamente, a como atingir esse mesmo objetivo dentro do novo cenário empresarial existente.

2 UMA VISÃO GERAL

Até a metade da década de 80, a utilização de computadores nas atividades contábeis das empresas era bem restrita, servindo, normalmente, para efetuar registros contábeis de forma automática em substituição aos procedimentos manuais. O auditor examinava os relatórios iniciais, que continham os registros e documentos de entrada, e os finais, que contemplavam as listagens de arquivos e do processamento e as saídas impressas, sem, no entanto, analisar as rotinas de processamento dos dados.

Com a evolução dos computadores e a amplitude de sua utilização na transformação de dados contábeis iniciais em informações contábeis finais, tais exames já não mais satisfaziam às necessidades da auditoria. O auditor passou a analisar profundamente o sistema de processamento de dados da empresa auditada e a utilizar diversos software em apoio às suas tarefas.

Os métodos atuais utilizados em auditoria convergem para um exame do processamento propriamente dito, além das entradas e saídas. Pode-se dividir os procedimentos de auditoria basicamente em: procedimentos gerais e procedimentos específicos.

2.1 **Procedimentos gerais**

Consiste na fase de identificação do ambiente computacional instalado para levantamento de áreas a serem inspecionadas e conhecidas.

Um sistema informatizado deve atender às seguintes premissas:

a) integridade – representa a certeza de que os dados que entram são processados corretamente;
b) confidencialidade - representa a certeza de que só têm acesso ao sistema os usuários autorizados; e
c) disponibilidade - estar disponível para ser utilizado sempre que necessário.

Com o incremento da utilização de processamento de dados pelas empresas cresce a necessidade de que os sistemas operados sejam seguros, inclusive para que o auditor possa avaliar o risco da auditoria. A indisponibilidade ou a falha de sistemas têm sido grandes causadoras de perdas financeiras.

Não existe um sistema 100% seguro. Podem ser identificados como os dois principais problemas relativos à segurança dos sistemas:

a) Falta de conscientização dos usuários – é importante que todos os usuários possuam a mentalidade de segurança, evitando: dar conhecimento de sua senha a outrem, permitir o acesso indevido a relatórios com dados confidenciais, etc. Existem estudos que mostram que cerca de 70% dos danos causados aos sistemas das empresas têm origem, voluntária ou involuntariamente, no usuário interno.
b) Falta de orçamento para que se invista na segurança do sistema – Todos os procedimentos e dispositivos que visam aumentar a

segurança do sistema (em especial software de proteção) implicam custos elevados. A empresa tem que avaliar a relação custo-benefício antes de implementar o procedimento ou adotar o dispositivo.

A análise do ambiente do sistema computacional da empresa pelo auditor divide-se, basicamente, em: segurança física e segurança lógica.

2.1.1 *Segurança física*

Refere-se às condições de acesso e à guarda dos equipamentos. Dentre os principais itens a serem verificados, incluem-se:

a) Se o local do equipamento possui acesso restrito, com fechadura ou dispositivos eletrônicos, de tal forma que somente tenha acesso o pessoal autorizado;
b) As condições de segurança quanto a incêndios e inundações, abrangendo a prevenção, detecção e extinção do sinistro;
c) As condições das instalações no tocante a umidade, temperatura, etc;
d) A existência de geradores e *no-breaks*; e
e) O cumprimento das rotinas de manutenções dos equipamentos.

Esta classe de segurança era a mais enfocada da época dos *main-frames,* quando os terminais dos usuários, chamados *terminais burros*, somente introduziam ou recebiam dados do computador central, não tendo capacidade de processamento. Confinava-se o computador central em um local revestido de todas as condições que asseguravam a segurança física.

2.2.2 *Segurança lógica*

Com o desenvolvimento do computador pessoal e da tecnologia de rede (LAN, WAN e internet), com estações de trabalho passando a ser capazes de processar e alterar os banco de dados e programas existentes, a segurança física perdeu importância para a segurança lógica.

Principais aspectos a serem observados com relação a segurança lógica:

1. Política de segurança da empresa e os procedimentos para implantação dessa política;
2. Gerenciamento dos usuários, com seus perfis de acesso bem definidos. Só deve ter acesso a dados ou possibilidade de alterações do sistema quem tiver a necessidade para o cumprimento de sua tarefa.
3. Gerenciamento de senhas:
   - Padrão de formação das senhas – 6 a 8 caracteres
   - Não compartilhamento de senhas por usuários
   - Troca periódica das senhas
4. Segregação de funções, de forma que qualquer tentativa de burlar o sistema tenha que ter a participação de pelo menos duas pessoas;
5. Monitoramento (controle detectivo) – feito por meio da análise dos *logs* do sistema;
6. Nível de exposição a acesso externo indevido - No mínimo, a utilização de um software (*firewall*) que venha inibir o acesso por *hackers*, de forma que o sistema da empresa não fique vulnerável;
7. Segurança das transmissões, dificultando que pessoas estranhas à empresa possam ter acesso a informações confidenciais. Dentre muitas existentes, podem-se citar:

a) Criptografia - consiste na transformação de dados por um algoritmo de forma que fique difícil ser entendida por alguém que intercepte a transmissão de dados, podendo ser decifrada facilmente pela parte receptora autorizada.
b) Certificado digital - uma assinatura eletrônica, mediante senha ou código, de forma que possa atestar a origem

do arquivo enviado.

2.2 **Procedimentos específicos**

Após a avaliação dos controles gerais da empresa e verificado que os mesmos propiciam segurança ao setor computacional da mesma, realiza-se a execução dos procedimentos específicos, cujo principal objetivo é avaliar os programas aplicativos utilizados.

Dentre as principais técnicas utilizadas pela auditoria independente nesta avaliação destacam-se: os testes de dados e a simulação paralela.

2.2.1 *Testes de dados*

O Teste de Dados envolve o processamento de dados no sistema computacional da empresa como parte dos teste de controle. O seu objetivo é verificar se o software do cliente é capaz de processar corretamente dados válidos e inválidos e como irá reagir aos diferentes tipos de dados.

Os dados utilizados pelo auditor têm como base um arquivo-mestre da própria empresa, no qual são inseridos dados fictícios de forma que possam testar os diversos controles existentes nos programas utilizados.

Como exemplo, podemos citar a checagem do total de pagamentos efetuados a fornecedores, em que um dos controles a ser testado é um determinado valor-limite, acima do qual o sistema deveria exigir uma autorização prévia para pagamento. O auditor introduzirá dados com valores bem próximos (acima e abaixo) ao limite para poder avaliar o perfeito funcionamento do controle.

2.2.2 *Simulação paralela*

A técnica de simulação paralela envolve o processamento dos dados do cliente em um outro programa de mesma aplicação, comparando os resultados obtidos ao final dos dois processamentos. É utilizada, principalmente, para facilitar os testes substantivos dos saldos das contas dos demonstrativos.

Como exemplo desta técnica, podemos citar o processamento de contas a receber, feito pelo cliente e pelo programa do auditor. A partir da mesma base de dados (registro de vendas a prazo), o auditor verifica a precisão dos resultados encontrados pelo programa da empresa em comparação com os constantes do seu programa.

As técnicas de teste de dados e simulação paralela são complementares. No teste de dados o auditor avalia a habilidade do sistema do cliente em lidar com diferentes tipos de transações, enquanto na simulação paralela o auditor testa se as saídas dos programas estão corretas.

O uso de tais técnicas passou a ser indispensável pelo fato das trilhas de auditoria já não poderem ser identificadas por meio das técnicas de auditoria tradicionais.

Ao abordarmos tal questão, vale observar que

> Na verificação da integridade dos programas de um computador deve ser estabelecida uma trilha de auditoria, que permita ao auditor rastrear qualquer saída do sistema computacional de volta aos documentos-fonte. Em muitos dos sistemas de tempo real e de tempo compartilhado hoje disponíveis, é extremamente difícil seguir uma trilha de auditoria. Em muitos casos simplesmente não há registro das entradas do sistema; dessa forma a trilha de auditoria é destru[illegible] Stair, 1998)

3 CONCLUSÃO

O volume de dados e de transações hoje processados por computadores, bem como a alteração do padrão da trilha de auditoria (do papel para a eletrônica) exigem, antes do emprego de qualquer técnica de auditoria, que o auditor verifique a segurança e a adequabilidade dos sistemas de informática em

uso pela empresa a ser auditada.

Para que uma equipe de auditoria contábil possa realizar os procedimentos de auditoria para obtenção das necessárias evidências é necessário que, previamente, o pessoal da auditoria de sistemas valide o sistema utilizado, bem como aponte as áreas mais sensíveis a erros ou fraudes. Nessa validação do sistema, o requisito de segurança (física e lógica) reveste-se da mais alta importância, tendo em vista que quão mais seguro for o sistema, menor o risco da auditoria a ser realizada.

Dada a abrangência alcançada pela utilização dos recursos computacionais nos trabalhos contábeis no mundo de hoje, é de se supor que todo auditor contábil deva estar, no mínimo, familiarizado com os recursos computacionais ao seu dispor, de tal que forma que possa realizar de maneira mais eficiente o trabalho a que se destina. Para aquilatar a importância de tal familiarização, o exame de CPA (*Certified Public Accounting*) a partir de 2003 deverá ser modificado, incluindo questões que requeiram, por exemplo, a construção de planilhas eletrônicas.

Impõe-se, pois, ao auditor a necessidade de conhecer os recursos e as técnicas de informática disponíveis para a realização dos trabalhos de auditoria de forma adequada e compatível com os atuais sistemas informatizados de contabilidade.

BIBLIOGRAFIA

ARENS, Alvin A., LOEBBECKE, James K. *Auditing:* An Integrated Approach. 7. ed. New Jersey: Prentice Hall, 1997.

CANEPA, Michael, SHRIVES, Philip. Automação da Auditoria. *HSM Management,* n. 4, set./out., 1997.

CASTELLS, Manuel. *A Sociedade em Redes.* São Paulo: Editora Paz e Terra, 1999.

CRC-SP. *Auditoria por meios eletrônicos.* São Paulo: Atlas, 1999.

HELMS, Glenn L., MANCINO, Jane. The Eletronic Auditor. *Journal of Accontancy,* abr., 1998.

HOLDER, William W., MILLS, Craig N. Pencils Down, Computers Up – The New CPA Exam. *Journal of Accontancy,* Mar, 2001.

LIMA, Vicente. Segurança com as portas abertas? *Gazeta Mercantil,* Brasília, vol. 80, n.22.020, 12/02/2001.

RITTENBERG Larry E., SCHWIEGER, Bradley J. *Auditing:* concepts for a Changing Enviroment. 2 ed. Orlando: Harcourt Brace & Company, 1997.

STAIR, Ralph M. *Princípios de Sistemas de Informação.* Rio de Janeiro: LTC, 1998.