AUDITORIA INTERNA: EMBASAMENTO CONCEITUAL E SUPORTE TECNOLÓGICO

Maria Goreth Miranda Almeida Paula *

Introdução

O contexto competitivo mundial tem impulsionado as entidades a se enquadrarem em um universo de evolução tecnológica, onde o tempo e a qualidade no atendimento às demandas e na obtenção de informações são fundamentais.

O enorme crescimento das comunicações e dos negócios em âmbito internacional tornou o mundo mais dinâmico e mutável. A concorrência acirrada trouxe maior complexidade às transações, e as operações passaram a trazer maior incerteza. Competência, tecnologia e criatividade são valores indispensáveis no contexto.

As questões aqui discutidas são, principalmente, fruto da inquietação quanto à forma de atuação da Auditoria Interna (AI) nesse novo contexto econômico-político-social, conseqüência da globalização. A pesquisa feita por meio da aplicação de questionário, as entrevistas realizadas em AI de 17 entidades de grande porte, situadas em diversas regiões do país, e as consultas bibliográficas, propiciaram a obtenção de dados e o suporte à discussão do assunto ora tratado e à formação da opinião registrada neste trabalho.

O resultado da pesquisa citada demonstra que os auditores, em vários casos, têm conhecimento do planeja-

* Artigo baseado na dissertação de mestrado da autora, defendida na Universidade de São Paulo – USP, em 1998.

mento apenas da atividade objeto de auditoria. Outros, nem isto. Quando questionadas se os auditores conhecem o planejamento da área auditada antes do início das trabalhos de auditoria, três declararam que não; um que isso ocorre somente na auditoria de agências; um declarou que não totalmente; quatro nada declararam e nove declararam conhecer o planejamento antes do início dos trabalhos. Observou-se que aqueles que dizem conhecer o planejamento, em parte, conhecem apenas o planejamento operacional da atividade/sistema auditado, não da entidade como um todo.

A falta de participação da Auditoria Interna em assembléias onde se decidem os rumos da entidade limita o seu conhecimento acerca do planejamento e das diretrizes da entidade. Em 11 das 17 entidades pesquisadas, o chefe da AI não participa das reuniões de diretoria; dois participam como ouvintes; um como consultor; um com direito a voto; um participa eventualmente, quando convidado, e uma das entidades pesquisadas não respondeu a essa questão.

Com relação à participação do chefe da AI em reuniões do conselho de administração, a pesquisa revela que 12 não participam; dois participam como ouvintes; um participa de um comitê de auditoria; um assessora quando convidado e uma das entidades pesquisadas não respondeu a esta questão.

Observa-se, pelas informações apresentadas e pelos demais dados obtidos na pesquisa, que o conhecimento que alguns auditores internos têm acerca do planejamento e das diretrizes empresariais é limitado e, por vezes, insuficiente para permitir-lhes uma visão sistêmica, necessária ao bom desempenho do seu trabalho.

✳

Metodologia de pesquisa

Para fins de elaboração deste estudo, foi realizada pesquisa, por meio da aplicação de um um questionário, entrevistas aos responsáveis pelas AI de 17 entidades em diversas regiões do país, consultas a livros, jornais, revistas, publicações e obtidas informações junto a profissionais atuantes em AI, informática e pesquisa.

As entidades foram selecionadas mediante a identificação, junto ao Instituto dos Auditores Internos do Brasil, das companhias de grande porte, com avançada tecnologia na área de AI, em condições de serem pesquisadas.

As referidas entidades possuem

CONSOLIDAÇÃO DO RESULTADO DA PESQUISA JUNTO ÀS ENTIDADES QUANTO AOS CONHECIMENTOS NECESSÁRIOS AO EXERCÍCIO DA PROFISSÃO DE AUDITOR INTERNO

CONHECIMENTOS NECESSÁRIOS	FORMAÇÃO ACADÊMICA	TREINAMENTO	PUBLICAÇÕES ESPECIALIZADAS
Conhecimento Atual e global da Entidade	Economia Contabilidade Administração Outros	Curso Superior	
Missão/Objetivos/ Atividades Empresariais	Economia Contabilidade Administração Outros	Curso Superior	
Contabilidade	Contabilidade	Práticas contábeis Análise de Balanço	Revista Assoc. dos Contadores
Área a ser auditada	Contabilidade Economia Administração Outros	Curso Superior	
Mercado Financeiro	Economia Contabilidade Administração	Matemática Financeira Curso Superior	Gazeta Mercantil Conjuntura Econômica
Informática	Processamento de Dados	Informática	Data Processing Revista de Informática Clipping de Informática Jornal Eletrônico
Direito Legislação (Federal, Estadual e Municipal) Impostos	Direito Contabilidade	Leg. Fiscal e Social Leg. Contratos e Licitações	IOB Mapa Fiscal Diário Oficial MNI
Comunicação verbal e escrita Português		Técnicas de Redação Português	
País			Gazeta Mercantil
Economia	Economia		Gazeta Mercantil Conjuntura Econômica
Finanças	Matemática Economia	Matemática Financeira	Gazeta Mercantil
Todos os ramos do saber	Medicina	Idiomas, principalmente inglês e espanhol	
Técnica de Auditoria	Contabilidade	Avaliação de riscos Técnicas de entrevistas Técnicas de Auditoria Auditoria em Ambiente Informatizado Aud. fisco-tributária Análise de Op. de crédito Aud. Operacional Aud. Gestional Aud. Analítica	Report Revistas das Associações dos Auditores Internal Audit Alert
Administração Técnicas gerenciais O & M Análise de Processo Controles Internos	Administração Contabilidade Marketing O & M	Avaliação de Riscos Qualidade Total Gestão Corporativa Consultoria Gerência de Projetos	Gazeta Mercantil Exame Rev.Assoc.dos Administ. Harvard Business Review Fortune

equipamentos e *softwares* de última geração para as atividades de suporte ou atividades-fim da AI. A avaliação e seleção foi feita pelo Audibra.[1]

A pesquisa foi basicamente descritiva. Observa, registra, analisa e correlaciona o conjunto das variáveis envolvidas. Os nomes das entidades não são citados, e qualquer referência será feita de forma codificada.

Segundo a pesquisa, das 17 entidades consultadas o preenchimento do cargo de chefe da AI ocorre da seguinte forma: sete, por designação do presidente; sete, por indicação da diretoria e nomeação do presidente do conselho de administração; um por designação da Diretoria Mundial de Auditoria Interna, no exterior; dois, as entidades não declararam.

✳

Missão da AI

A identificação da missão da AI, obtida entre as entidades pesquisadas e em publicações especializadas, permitirá o estabelecimento de um parâmetro com o qual se confrontará a prática da auditoria, propiciando a melhor compreensão do esforço que tem sido desenvolvido para atingi-la e das formas alternativas de fazê-lo.

Segundo as entidades pesquisadas, a missão da AI é:

- *assessorar a administração*, por meio do exame da adequação e eficácia dos controles internos da entidade; da verificação da integridade e confiabilidade dos sistemas; da constatação da observância às políticas, metas, planos, procedimentos, leis, normas e regulamentos; da garantia da eficiência, eficácia e economicidade do desempenho e da utilização dos recursos; da avaliação dos procedimentos e métodos para a salvaguarda dos ativos; da análise da exatidão dos ativos e passivos; e da compatibilidade das operações e programas com os objetivos, planos e meios de execução estabelecidos;
- assessorar, mediante ação integrada de sua equipe de trabalho, todos os níveis da administração, *contribuindo de forma efetiva para o desempenho de suas atribuições e responsabilidades*, visando cumprir a missão da entidade;
- *agregar valor* aos produtos oferecidos pela entidade;
- *certificar aos acionistas o grau de*

1 O Institudo dos Auditores Internos do Brasil – Audibra foi fundado em 20 de novembro de 1960. Seu quadro de associados é composto por profissionais da área de Auditoria Interna e correlatas.

confiabilidade do gerenciamento e da condução do negócio por parte dos responsáveis pela entidade.

O perfil do profissional de Auditoria Interna foi abordado no Congresso Latino Americano de AI,[2] ocorrido em Cancún, México, no período de 7 a 9 de setembro de 1995, oportunidade em que os debates resultaram na conclusão de que o Nafta, o Mercosul e outros mercados mundiais requerem multidisciplinariedade das equipes e tecnologia de ponta, frente às exigências da modernidade, da globalização, da integração de culturas diferentes e da flexibilidade de ações conjuntas e oportunas.

O quadro foi construído de forma consolidada, ou seja, todas as AI pesquisadas, juntas, indicaram os conhecimentos necessários, a formação acadêmica exigida, o treinamento e as publicações acessíveis. Nenhuma das entidades dispõe de tudo o que foi indicado no quadro.

A maioria delas está suprida com informações fiscais, três entidades assinam a *Gazeta Mercantil*, e apenas a AI de uma entidade assina a *Exame*, a *Revista de Administração de Empresa FGV*, a *Harvard Business Review* e a *Fortune*. Duas assinam o *Diário Oficial da União*, uma a *Conjuntura Econômica* e uma, *Internal Audit Alert*.

As informações obtidas por meio de assinatura de revistas e publicações especializadas, portanto, não suprem completamente os auditores, para que se mantenham atualizados nas áreas de conhecimento que foram indicadas na pesquisa. Segundo a norma 250.03, do Audibra, todo auditor interno deve conhecer a organização onde atua, seus produtos e serviços, seus processos de produção e comercialização, seus mercados, sua estrutura operacional e funcional, bem como todos os demais quesitos organizacionais necessários ao bom entendimento dos aspectos vitais dos negócios.

A norma 300.03.06, dispõe que é parte essencial do trabalho do auditor a verificação do grau de atualização dos instrumentos utilizados pela administração, assim como da existência de uma mentalidade voltada para o controle, dentro da organização.

a) Formação Acadêmica do Auditor

Para o Conselho Federal de Contabilidade – CFC, a AI é de competência exclusiva de contador registrado em Conselho Regional. Segundo a entidade, o contador, na função de auditor interno deve manter o seu nível de

2 Instituto dos Auditores Internos do Brasil – Audibra. Congresso Latino Americano de AI, *Revista do Auditor*, São Paulo, ano II, n. 10, dez 1995, p. 13.

competência profissional pelo conhecimento atualizado das Normas Brasileiras de Contabilidade, das técnicas contábeis, especialmente na área de auditoria, da legislação inerente à profissão, dos conceitos e técnicas administrativas e da legislação aplicável à entidade. O Conselho acrescenta que o auditor deve dispor de conhecimento suficiente dos recursos de processamento de dados e dos sistemas de processamento da entidade, a fim de avaliá-los e planejar adequadamente seu trabalho.

As entidades pesquisadas, no entanto, não cumprem o que o CFC dispõe quanto à competência exclusiva do contador para o exercício da AI. Isso porque:

- a prática da auditoria operacional não exige a formação em ciências contábeis, especificamente;
- a formação pode ser complementada com cursos;
- as normas da empresa divergem das do CFC;
- os funcionários são recrutados mediante concurso que não exige essa formação, necessariamente;
- a área de auditoria é muito abrangente;
- os trabalhos desenvolvidos abrangem aspectos técnicos, operacionais, administrativos e de informática que não se limitam à verificação de dados constantes dos demonstrativos financeiros;
- a representação formal da área é feita por profissional formado em ciências contábeis;
- as equipes compostas por auditores com formação acadêmica diferenciada proporciona um produtivo intercâmbio de conhecimento;
- a auditoria não é um mero segmento contábil;
- a auditoria atua de forma multidisciplinar;
- não é fundamental nem essencial.

Após compreender-se o desafio que representa selecionar corretamente um auditor, visto ser necessário observar critérios de conhecimento multidisciplinar, entende-se parte das razões que levaram algumas entidades a não exigirem, para o preenchimento do cargo de auditor interno, a formação acadêmica em ciências contábeis.

b) Treinamento

Com relação ao treinamento, 16 das 17 entidades pesquisadas declararam ter programa de treinamento; uma nada declarou.

Das Normas Brasileiras para o Exercício da Auditoria Interna da Audibra, constam orientações sobre a necessidade de treinamento, o grau de conhecimento exigido e o alvo que o auditor precisa atingir.

O treinamento realizado nas entidades pesquisadas não trata de questões teóricas, conceituais e estratégicas que

devem embasar a visão do auditor e se restringe a questões práticas e operacionais. O treinamento que trata da utilização de *softwares*, do conhecimento de novas técnicas ou da interpretação de uma determinada legislação, apesar de importante e necessário porque instrumentaliza o auditor, não o capacita a definir metas específicas, ou seja, formar uma visão estratégica.

As entidades dispõem de bons equipamentos e *softwares*, mas tais instrumentos não são aproveitados em sua totalidade. Todos os recursos disponíveis seriam melhor aproveitados se os profissionais militantes na área tratassem com mais atenção das questões conceituais, teóricas e estratégicas.

O número de programas auditores,[3] trilhas de auditoria,[4] suporte eletrônico de auditoria para a gerência e auditores é mínimo, com relação ao potencial de equipamento disponível. Constata-se, pois, a falta de uma posição proativa do auditor, de uma visão sistêmica frente aos grandes desafios da entidade.

O grau de conhecimento do auditor representa um desafio nas condições atuais devido, também, à limitação de publicações especializadas. Observou-se, na pesquisa, que as divulgações técnicas veiculadas eletronicamente, por meio da Internet, continuam não sendo consultadas por grande número de auditores, por não estarem familiarizados com a rede mundial, por não terem uma rotina específica de consulta e o tempo necessário para desenvolvê-la, e ainda, por dificuldades com o idioma, basicamente inglês.

Os cursos e os encontros oferecidos são em número reduzido e nem sempre capazes de suprir as necessidades específicas da AI de cada entidade. A participação nesses cursos é restrita a parte dos auditores, conforme se pôde identificar na pesquisa, e não há a transmissão adequada das informações para o grupo.

A AI deveria assessorar a administração quanto à influência de variáveis externas nos rumos da entidade, mas a sua grande maioria não participa de reuniões de diretoria nem do conselho de administração, onde se discutem as diretrizes, as metas e as políticas da organização.

Como a AI poderia cumprir sua mis-

---

3 *Programas Auditores* são *softwares* desenvolvidos para avaliação de controles. Podem confrontar as informações constantes de bancos de dados distintos, para verificar a consistência dos dados ou para, atentando para as diferenças, identificar eventuais desvios.

4 *Trilhas de Auditoria* são *softwares* desenvolvidos para fornecer determinada informação ao auditor. Como exemplo, a trilha poderia disponibilizar a informação de quem, quando, quanto tempo etc., acessou um sistema considerado crítico quanto à importância das informações nele contidos.

são se não dispõe de condições básicas para tal? Por que a auditoria não tem sido chamada a participar do estabelecimento dos rumos da entidade, dando suporte à ação do gestor, se essa é a sua função, subsidiar a tomada de decisões?

São perguntas complexas. Uma das razões para que este fato ocorra está, certamente, relacionada à postura *reagente* de algumas AIs e não *proativa*. Desse modo, o desenvolvimento de uma atividade somente seria realizada a partir de uma demanda da chefia.

O auditor, conhecendo as necessidades da entidade e o processo decisório do gestor, poderia sugerir a adoção de linhas de ações, independentemente de ter se requerido a sua opinião nesse assunto específico. Muitas vezes, o auditor não é solicitado para opinar sobre determinado assunto porque o gestor não conhece a importância da sua contribuição. Não se procura onde não se acredita que se encontrará. A falta de tempo, de oportunidades, de apoio da alta direção administrativa podem ser outras razões.

Proposta de suporte informatizado para os trabalhos do auditor

Assim como a entidade precisa de instrumentos tecnológicos que suportem a sua evolução, a AI, como instrumento da administração da entidade, precisa, também, utilizar-se de todos os recursos que a levem a otimizar os seus esforços.

Visando instrumentalizar o auditor interno para que execute satisfatoriamente seu papel, diante do grande volume de informações a serem tratadas, das rotinas automatizadas e da evolução tecnológica, este artigo apresenta uma proposta de sistema integrado de suporte aos trabalhos de AI, fruto da pesquisa empírica e bibliográfica realizada.

O Sistema Informatizado de Suporte à Auditoria Interna representa um instrumento adicional para o auditor desenvolver as suas atividades. As técnicas consagradas pela Auditoria Interna são descritas dentro de um sistema tecnológico. Neste artigo, o Sistema é composto pela integração de três subsistemas — Programa, Dossiê e Relatório —, demonstrados a seguir.

Subsistema Programa

O nome de cada atividade, ou a sua codificação, seria a chave para o acesso ao Subsistema Programa correspondente, onde constariam as funções de atualização, consulta, impressão e outras, para os seguintes cadastros:

1. Cadastro das Atividades Identificadas;

2. Plano de Auditoria;
3. Objeto;
4. Objetivos da Auditoria;
5. Questionário de Avaliação do Controle Interno – QACI;
6. Procedimentos de Auditoria (PA);.
7. Fluxograma;
8. Tabelas de Números;
9. Avaliação de Risco;
10. Papéis de Trabalho.

1. *Cadastro das Atividades Identificadas*

Relação das atividades identificadas, passíveis de serem auditadas e da codificação correspondente. Essa relação estaria distribuída por áreas, grupos, atividades e subatividades, conforme exemplificado abaixo.

a. Área de Atividade (ex: área-meio);
b. Grupo de Atividade (ex: recursos humanos);
c. Atividade (ex: folha de pagamento);
d. Subatividade (ex: consignações).

2. *Plano de Auditoria*

Identificação especial dada às atividades eleitas para integrarem o Plano Anual de Auditoria Interna do período, dentro do Cadastro das Atividades. Essa identificação possibilitará a geração do relatório Plano Anual de Auditoria Interna e, em fase posterior, o de Atividades Planejadas × Atividades Executadas.

O Plano Anual de Auditoria Interna é a relação de atividades a serem auditadas no exercício, elaborado em consonância com as diretrizes da alta administração. Geralmente, é elaborado pela AI e submetido ao seu superior hierárquico para apreciação. O cronograma das atividades, a previsão de recursos humanos (auditores que deverão ser designados) e materiais (equipamentos, *softwares*, treinamento etc.) necessários à consecução do Plano de Auditoria, também integram este campo.

3. *Objeto*

Informações sobre a atividade a ser auditada sob os seguintes aspectos: conceituação, normas existentes e sua manualização, áreas envolvidas, competência das unidades e subunidades, resumo dos sistemas operacionais de controle em processamento de dados e outros. Ele deve ser revisto e atualizado, se necessário, a cada trabalho.

4. *Objetivos*

Propósitos específicos dos trabalhos de auditoria naquela atividade. São sujeitos a alterações a cada trabalho, para adequá-los às peculiaridades do momento.

5. *Questionário de Avaliação do Controle Interno – QACI*

Questões formuladas com o objetivo de obter informações gerais a respeito do sistema e fazer uma análise

SUBSISTEMA DOSSIÊ

O *Subsistema Dossiê* acessaria do *Subsistema Programa* os cadastros na forma de papéis de trabalho, para serem utilizados naquela auditoria, oportunidade em que seria permitido promover ajustes ou alterações para adequá-los às necessidades e peculiaridades do momento. Esse subsistema estaria dividido nos seguintes campos:

1. Identificação do Trabalho;
2. Auditor Responsável;
3. Supervisor Responsável;
4. Objetivos;
5. QACI;
6. PA;
7. Fluxograma;
8. Tabelas de Números;
9. Papéis de Trabalho;
10. Tempo de Execução.

Os papéis de trabalho elaborados seriam arquivados e referenciados eletronicamente, permitindo que, ao final de cada trabalho, o auditor deixasse de ter preocupações com o aspecto formal da documentação, atendo-se, apenas, à elaboração do relatório.

Os papéis que não forem elaborados eletronicamente poderiam ser arquivados por meio de *scanner*, ou recebidos por ele via *fax-modem*.

SUBSISTEMA RELATÓRIO

Definiria as seguintes informações:

1. *Identificação do Relatório*

Informações sobre a unidade administrativa auditada, o período de realização dos trabalhos, a data do relatório, sistemas auditados e outros dados julgados necessários. Com base na codificação dos sistemas auditados, seria promovido o confronto eletrônico entre o *planejado* e o *executado*, gerando, quando necessário, relatórios gerenciais.

2. *Pontos identificados na auditoria*

Informações sobre os fatos identificados nos trabalhos de auditoria, se o objeto da auditoria está controlado adequadamente, se é passível de melhoria ou se é incompatível com as metas da entidade.

3. *Recomendação correspondente*

Informações sobre as recomendações feitas pelos auditores, decorrentes dos fatos identificados.

4. *Resposta da unidade*

Comentários e informações prestadas pela unidade auditada, com referência aos dois itens anteriores.

5. *Observação da auditoria*

Comentários da auditoria com relação às providências tomadas por parte da unidade auditada.

6. *Status da auditoria*

Código indicativo da situação em que se encontra a atividade auditada com relação às providências adotadas (ex: pendente de resposta; resposta insatisfatória; a ser analisada em trabalhos posteriores; entre outros).

7. *Reavaliação de risco*

Classificação de risco promovida após cada auditoria, mediante a atribuição de pontos a cada critério previamente definido quando da avaliação de riscos.

A totalização seria processada eletronicamente, permitindo, a qualquer tempo, a geração do relatório *Matriz de Risco*, que visa subsidiar o gerenciamento da auditoria no estabelecimento de prioridades e diretrizes. O Subsistema Relatório trataria as informações constantes dos itens anteriormente descritos visando a geração de relatórios para a área auditada, alta administração e para o acompanhamento das recomendações por atividade, por unidade administrativa ou das formas que se fizerem necessárias.

É conveniente acrescentar a importância de a alta administração empresarial estabelecer, por meio de normas, um prazo máximo para que a unidade administrativa auditada se pronuncie, com relação aos pontos levantados e às recomendações propostas.

SUPORTE AUTOMATIZADO DE AUTITORIA INTERNA

SUBSIST. PROGRAMA
Cadastro
Plano de Auditoria
Objeto
Objetivos
Quest.Aval.Controle Interno
Procedimentos
Fluxograma
Tabela de Números
Avaliação de Risco
Papéis de Trabalho

SUBSISTEMA DOSSIÊ
Identificação do Trabalho
Auditor Responsável
Supervisor Responsável
Objetivos
Quest.Aval.Controle Interno
Procedimentos
Fluxograma
Tabela de Números
Tempo de Execução
Papéis de Trabalho

SUBSISTEMA RELATÓRIO
Identificação do Relatório
Pontos Identificados
Recomendação Correspond.
Resposta da Unidade
Observação da Auditoria
Status da Auditoria
Reavaliação de Risco

SISTEMAS AUDITORES

Como instrumentos para a AI, integrando os sistemas *Programa* e *Dossiê*, quando for o caso, pode-se também utilizar sistemas que confrontem informações de bancos de dados distintos, que selecionem informações para que o auditor trabalhe com um volume de informações menor e tratadas, ou que sejam usados como teste para assegurar que os sistemas em produção (usados nas rotinas da entidade) atendem às expectativas.

Para viabilizar tais sistemas, torna-se necessário conhecer o universo das informações geradas e gerenciadas pela entidade, de acordo com as pe-

culiaridades de cada banco de dados, com seu conteúdo e com os objetivos definidos no trabalho de auditoria. Cria-se, então, de forma temporária ou permanente, um sistema auditor.

Para tais fins, poder-se-ia relacionar algumas das informações a serem obtidas. Em especial, podemos citar a identificação dos bancos de dados gerados e gerenciados por cada segmento administrativo, que deverá ser feita a partir dos seguintes tópicos:

1. ambiente eletrônico onde se processa o armazenamento de dados;
2. interação com outros bancos de dados;
3. ambiente eletrônico desse(s) outro(s) banco de dados interativo(s);
4. natureza da informação armazenada (ex: fornecedores, estoques etc.);
5. distribuição dos campos para armazenamento dos dados;
6. data de criação do banco de dados;
7. quem insere os dados no sistema;
8. que informação é inserida;
9. se existe crítica no sistema — pontos de controle —, visando a segurança da informação, e, em caso positivo, se atende satisfatoriamente;
10. pontos positivos e negativos identificados na operacionalização do sistema;
11. que tipo de informações são geradas (técnicas, gerenciais, outras);
12. quem se utiliza dessas informações;
13. para que são utilizadas essas informações.

Após a identificação perfeita do universo de dados a ser trabalhado pela auditoria, é possível estabelecer um planejamento eficaz e eficiente, considerando o aspecto tecnológico e o estratégico.

Vantagens/Objetivos Propostos

a) Redução da permanência física do auditor nas áreas auditadas, devido parte do seu trabalho ser desenvolvida de forma indireta, por meio de sistemas informatizados, permitindo um monitoramento a distância.

b) Melhor preparação dos auditores para o trabalho de campo, por meio da obtenção de informações acerca das áreas auditadas antes de se deslocar a unidade executora/controladora da atividade.

c) Maior qualidade nos resultados obtidos (relatório/assessoramento), em decorrência da melhor preparação dos auditores e da disponibilização de informações tratadas pela Auditoria Interna às demais unidades administrativas.

d) Aumento do universo monitorado por meio do acompanhamento de bancos de dados; conseqüentemente, na obtenção de informações que subsidiarão a análise.

e) Incremento no universo dos trabalhos de auditoria em decorrência do melhor aproveitamento do tempo dos auditores em campo, pela facilidade encontrada no suporte e na obtenção e tratamento de dados.
f) Possibilidade de o trabalho de campo ser desenvolvido por apenas um auditor, sendo supervisionado por meio de rede, otimizando a administração de recursos humanos da AI.
g) Facilidade no armazenamento de papéis e na forma de acessá-los, realizado eletronicamente.
h) Redução de arquivos de papéis e de processos burocráticos, que ocupam espaços físicos e impõem um custo de controle com o armazenamento, nem sempre correspondente ao benefício, comparativamente com as opções existentes.
i) Direcionamento do trabalho do auditor, em alguns casos, restringindo a sua análise aos casos de exceção, identificados pelo sistema nos bancos de dados.
j) Aumento da motivação e produtividade, vez que um maior volume de informações tratadas propiciará a liberação do auditor de trabalhos burocráticos e rotineiros.
l) Facilidade na disponibilização de algumas informações solicitadas pela Auditoria Externa ou órgãos de controle externo, quando for o caso.
m) Redução das atividades de suporte, pela redução das rotinas com a administração de processos, seu trânsito e arquivamento.
n) Maiores condições para o pleno atingimento dos objetivos propostos pela Auditoria Interna e conseqüente cumprimento de sua missão.

ESFORÇOS ENVOLVIDOS

1. Disponibilização de *Note Books* para cada auditor, conectados à Rede da entidade.
2. Desenvolvimento de um programa de treinamento, visando:
   - rediscutir a estratégia da auditoria, revisando-a ou reafirmando-a;
   - padronizar os procedimentos de auditoria;
   - fornecer novos instrumentos e técnicas para os trabalhos de Auditoria, ou fortalecer às já conhecidas, consideradas mal compreendidas ou aplicadas de forma limitada;
   - permitir a utilização da nova tecnologia de suporte, por parte dos auditores e gerentes de auditoria.
3. Custos financeiros correspondentes aos itens anteriores e outros, envolvidos com a implantação do projeto.

Desafios

Os desafios apresentados foram identificados, considerando sua complexidade, os fatores limitantes de controle, sua materialidade e importância estratégica.

Muitos outros aspectos de controle poderiam ser, também, aqui classificados como desafios, porém espera-se que a compreensão dos tópicos selecionados permitam a percepção da importância da AI na vida empresarial como especialista em controles internos, com uma visão abrangente da entidade, não somente quando sugere soluções disponíveis, mas principalmente para colaborar na administração de riscos.

Foram abordados de forma a caracterizá-los como tal, sem uma preocupação de indicar soluções ou de fazer pronunciamentos críticos acerca das informações obtidas na pesquisa empírica ou bibliográfica.

Para compreender-se o desafio que representa para o gestor e, conseqüentemente, para o auditor, o controle das informações em trânsito na rede mundial – Internet, as operações com derivativos, o "*bug* do milênio" e a adaptação dos recursos humanos às mudanças, é necessário entender o que representam. Nesse contexto, abordar-se-á as características gerais da cada item citado, principalmente as questões correlacionadas ao controle.

Internet

A Internet traz consigo uma avalanche de novos conceitos e mudanças generalizadas na área de informática.

Para cumprir sua missão, a auditoria precisa manter sua abordagem atualizada, já que a forma de tratamento da informação está em constante evolução.

A auditoria da área de informática que, inicialmente, tinha seu foco no conceito de Mainframe, evoluiu para redes locais, e agora enfoca a Internet, Intranet, Extranet, redes privadas virtuais e servidores de objetos, procurando se manter preparada para a evolução contínua do processo.

Segurança da informação

No mundo dos computadores, segurança significa permitir o acesso à informação somente para aqueles que estão autorizados para tal. Os conceitos de segurança, nesse caso, seriam: confidencialidade, integridade e disponibilidade.

O item segurança é fundamental. O contato com os clientes diretamente pela rede pode causar danos a quem não estiver devidamente protegido. Os esquemas de segurança exigem despesas extras. Na prática, quanto mais sofisticada for a proteção, mais dinheiro será desembolsado.

Criptografia, bloqueio antivírus e

paredes corta-fogo (*firewalls*) são algumas das tecnologias disponíveis.

Os elementos de segurança passam a ter importância redobrada, neste contexto, necessitando para a sua eficácia de uma política de segurança da informação, cultura dirigida para controle, ferramentas apropriadas e monitoração.

Hackers e Crackers – Segundo Derneval Rodrigues da Cunha,[5] que faz a primeira revista *hacker* do Brasil, a *Barata Elétrica*, distribuída na Internet, *crackers* são aqueles que não respeitam a ética *hacker*: não mexer, não destruir, não deixar pistas. Qualquer computador equipado com modem — aparelho que liga o micro às linhas telefônicas — corre o risco de ser invadido.

> Eles já entraram nos computadores da Nasa, do Pentágono e de várias instituições brasileiras. Alguns chegam, olham e não fazem nada. Outros destroem programas e arquivos. São os hackers, espiões cibernéticos sem rumo que sabem tudo sobre computadores e se divertem quebrando a segurança dos sistemas. A Internet é um dos caminhos para suas invasões.

Conforme publicação em *A Tribuna*, de 22 de fevereiro de 1995, os números de ataques de *hackers* nos Eestados Unidos são assustadores: em 1989, calcula-se que cerca de 340 mil entidades privadas foram atacadas e, em 1991, esse número saltou para 684 mil. Isto é, em dois anos houve um aumento de 100%. O FBI estima que, anualmente, são perdidos entre US$ 500 milhões e US$ 5 bilhões em decorrência da ação desses invasores.

No primeiro semestre de 1995, a Empresa Brasileira de Pesquisas Agropecuárias – Embrapa, a Universidade de São Paulo – USP, a Universidade Estadual de Campinas – Unicamp e a Universidade Federal de Pernambuco – UFPe tiveram seus computadores invadidos. Isso resultou na destruição de pesquisas e arquivos importantes.[6]

Os *hackers* estão se organizando. Para tentar invadir um site, procuram identificar o sistema operacional, a versão, os recursos disponíveis e a vulnerabilidade, ou seja, as portas abertas pelas quais eles tentarão entrar.

No caso hipotético de algum *hacker* encontrar no seu caminho um roteador desconhecido, poderá consultar diversas pessoas do mundo, solicitando ajuda.[7] Até o próprio criador do roteador, ligado à Internet, pode

---

5 *Apud* Heitor Shimuzi e Ricardo B. Setti, op. cit., p. 27.

6 Idem, p. 27.

7 Os roteadores são dispositivos capazes de conectar redes diferentes, incluindo aqueles que usam tipos diferentes de cabos e de velocidades de comunicação, enviando o tráfego de uma para outra. São utilizados na busca de endereço para viabilizar o acesso. Enviam pacotes de um lugar para outro, levando em consideração a situação atual da rede.

indicar uma solução para o problema, sugerir uma porta, um caminho. Se, por qualquer meio, o *hacker* descobrir a senha de acesso da entidade ou do usuário, ele não correrá, sequer, o perigo de ser descoberto, pois estará usando um acesso permitido.

Há formas de evitar a ação dos *hackers*. Segundo Carlos Campana Pinheiro,[8] da Rede Nacional de Pesquisas – RNP, órgão público que regulamenta a atuação da Internet no Brasil, cerca de 90% das invasões se devem ao uso de *password* (senha, em inglês) ou *guest* (visitante), com nomes ou datas. O ideal, diz ele, é criar palavras esdrúxulas ou em outra língua, ou mesmo misturar letras e números.

A mudança da senha de um usuário, dentro da entidade, deve ser exigida periódica e automaticamente, e não por opção deste.

Engenharia Social – No jargão da Internet, engenharia social é o nome que se dá à técnica pela qual *o hacker*, ou alguém ligado a ele, comunica-se com um operador de sistema de rede de computadores dizendo ser um funcionário de alto nível da entidade que esqueceu a senha, pedindo-lhe que a troque para que possa acessar o sistema. Pode denominar, também, a utilização de relacionamentos pessoais com o objetivo de descobrir a senha de alguém, baseando-se no conhecimentos de seus dados pessoais, visando invadir determinado sistema.

É uma espécie de espionagem.[9] Senhas com datas de nascimento, sobrenome ou nome dos filhos são muito comuns. Se o *hacker* tiver acesso a essas informações do usuário, vai tentá-las como primeira opção para descobrir a senha. Alguns chegam a arrumar emprego temporário na entidade que pretendem invadir. Lá dentro, observam os usuários dos computadores. Não é comum se cobrir o teclado na hora de digitar a senha, mesmo que tenha alguém por perto. Esse alguém pode ser um *hacker*.

Vírus de Computador – Apesar dos riscos, que vão desde a queda de performance dos sistemas até a perda total dos dados, o índice de máquinas sem proteção no Brasil chega a 88%, segundo levantamentos da Compusul, distribuidora no país do antivírus VirusScan, da McAfee.[10] O aumento da sofisticação dos vírus e a complexida-

8 *Apud* Heitor Shimuzi e Ricardo B. Setti, op. cit., p. 32.

9 Heitor Shimuzi e Ricardo B. Setti, op. cit., p. 31.

10 Katia Jucá, "Proteja sua rede dos invasores", *Revista Informática Exame*, São Paulo, Abril, jan, 1996, p. 24.

de das redes agrava o problema. Nas redes, a proteção antivírus deve ser feita nas estações (micros ligados à rede) e no servidor. A autonomia de cada usuário sobre o seu micro dificulta o controle nas estações.

Cavalo de Tróia – O Cavalo de Tróia é um programa semelhante a um vírus. Mas, em lugar de destruir programas e arquivos, tem a função de descobrir senhas. O Cavalo de Tróia pode ser enviado escondido em uma mensagem na Internet ou em um disquete que o *hacker* passa, com jogos ou outros programas, para usuários do computador que ele quer invadir.

Cada vez que o usuário escreve nome e senha, o Cavalo de Tróia grava os dados. Como é programado para conectar-se com seu criador, por meio de *modem*, em circunstâncias definidas, ele transmite os dados que copiou. Elementar, para quem conhece muito bem as linguagens de computador.

Bomba Lógica – É um tipo de vírus e, provavelmente, uma das formas de modificação não autorizada em sistemas mais difíceis de ser identificada. É conhecida, também, como bomba-relógio, já que, na maioria dos casos, é acionada por meio do ingresso de uma data ou de dados no sistema. Como exemplo, pode-se citar o vírus sexta-feira 13.

Alçapão – O alçapão tem esse nome porque seu funcionamento é similar às passagens secretas dos castelos medievais. Ele, portanto, permanece oculto e somente é usado quando necessário, estando disponível apenas para aqueles que sabem usá-lo. Os alçapões são mais comuns em ambiente *Mainframe* IBM, e quase sempre são obra dos próprios profissionais internos que desejam manter uma via de acesso que contorne a segurança.

Farejamento de redes – Para acelerar a sua transmissão, os dados provenientes de vários computadores que entram nas redes são agrupados em pacotes. O *hacker* cria programas farejadores que monitoram a circulação desses pacotes nas redes e procuram neles palavras como *password* (senha). Quando as encontra, o programa copia e envia para o computador do *hacker*. Os dados chegam codificados, mas isso nem sempre é problema para ele, que em geral conhece bem criptografia.

Quebra-cabeça – É um jeito de desvendar senhas, utilizando-se da tentativa e erro. Para isso, o *hacker* cria programas capazes de montar todo tipo de combinação de letras e números. O sistema funciona bem para senha de até seis caracteres. O processo pode levar muito tempo, porque as tentativas precisam ser feitas em períodos

curtos, com grandes intervalos (dias, se for possível) entre um e outro, para não despertar suspeitas. No Brasil é um método muito difundido, pois as senhas em geral são simples e dificilmente os computadores possuem sistema de proteção quanto ao número de tentativas de acesso indevidas.

Falta de Documentação – A documentação pode ser definida como um conjunto de instruções que, geralmente, acompanha um programa (*software*), uma unidade de *hardware* ou uma estrutura montada a partir de recursos informatizados.

A falta de documentação do procedimento administrativo pode inviabilizar a manutenção da segurança. Quando o administrador pensa alguma forma de segurança e a executa, sem documentar devidamente esse procedimento, seu sucessor não conseguirá dar continuidade ao processo, ou encontrará dificuldades.

A rede cresce de tal forma que fica difícil manter a disciplina da configuração.[11] Deve-se ter em mente a necessidade de documentar a operação e evitar depender da intuição da administração, o que torna a auditoria impossível.

Mesmo que a auditoria aprendesse os conceitos mais complexos de rede, seria dificílimo conseguir desenvolver seu trabalho sem um padrão. Até mesmo um especialista em sistemas teria dificuldades em manter a segurança em um ambiente configurado sem a documentação.

Legislação – Todo programa de computador é protegido pela legislação de direitos autorais, tanto no Brasil como no resto do mundo. A Lei nº 7.646/87 prevê a pena de seis meses a dois anos de detenção e indenização que pode chegar ao valor de 2 mil cópias para o caso de uso não permitido de *softwares*.

Em 1986, o Congresso Americano aprovou a primeira lei contra a fraude e abuso de computadores. O primeiro condenado, a cinco anos de cadeia, foi Robert Tappan Morris Junior. Em 2 de novembro de 1988, Robert T. Morris Jr., na época estudante de ciência da computação na Universidade de Cornell, criou um programa que se autoduplicava e autopropagava, denominado *worm (minhoca)*, e o injetou na Internet. O programa infectou 50 mil computadores, em uma velocidade mais rápida que a esperada.[12]

---

11 Disciplina de configuração: organização racional dos equipamentos e *softwares* disponíveis para viabilizar o gerenciamento.

12 Conforme Brendan P. Kehoe, *Zen e a arte da internet*, 3. ed., Rio de Janeiro, Editora Campos, 1995, p. 93.

Robert T. Morris Jr. foi processado por crime com base no *Computer Fraud and Abuse Act* (Título 18 do United of States Code, seção 1030). Foi sentenciado, em maio de 1990, a três anos de liberdade condicional, com 400 horas de serviço comunitário e a pagar uma multa de US$ 10.050 e os custos de sua supervisão.

MODELO DE SEGURANÇA

a) *Política de uso*

Os usuários devem utilizar esses recursos de forma disciplinada, já que 100% de segurança não existe. Devem estar conscientizados de que segurança é responsabilidade de todos. A alta administração, os diversos níveis hierárquicos e os demais funcionários devem entender a necessidade da política de segurança da informação, ou seja, de orientações estratégicas e normativas que visam a segurança das informações.

É necessário estabelecer diretrizes que permitam garantir a integridade, a confidencialidade e a disponibilidade das informações.

Toda segurança gera custo e deve ser viabilizada em função da necessidade e criticidade, importância e sigilo das operações.

b) *Prevenção contra riscos internos*

Deve-se considerar o risco potencial de algum usuário interno facilitar o acesso a alguém externo à entidade de forma a permitir que opere o sistema.

O bom funcionamento dos sistemas empresariais estará assegurado se forem dotados de segurança capaz de preservar a disponibilidade, a inviolabilidade e a confiabilidade das informações.

A entidade Módulo,[13] especializada em segurança de informações, fornece indicações visando esse fim, ou seja, providências que poderão fortalecer a segurança dos dados empresariais. São elas:

- implementar recursos de contagem de uso (número de vezes que o sistema é acessado) e trilha de Auditoria, obtendo relatórios estatísticos e gráficos com informações estratégicas sobre a quantidade de equipamentos e usuários e a utilização dos recursos disponibilizados. Com estas informações, diretores, gerentes e administradores de microinformática tomarão decisões de expansão ou contenção de investimentos em *hardware* e

13 *Módulo* – Consultoria e Informática. Fundada em 1985, presta consultoria e desenvolvimento de produtos voltados para as áreas de segurança, administração e auditoria em microcomputadores e redes locais. Fonte: prospecto de divulgação da empresa.

software, treinamento de usuários e redirecionamento de recursos;

- proteger o armazenamento e o trânsito de documentos, mensagens e informações estratégicas e confidenciais;
- garantir a integridade de informações disponibilizadas apenas para consulta, impedindo a alteração indevida;
- elaborar e testar a metodologia e os procedimentos de *backup* e de contingência para a recuperação de dados em caso de acidentes e desastres;
- implementar segurança nos *notebooks*;
- viabilizar uma política de segurança para conexões externas via Internet, ou outras redes públicas de computadores, inibindo a ação de *hackers* e *crackers*;
- capacitar os profissionais da entidade a atuar na implementação e na manutenção da política de segurança e administração das redes.

OUTROS MÉTODOS PREVENTIVOS

Criptografia – É o conjunto de técnicas que permite codificar dados. O processo de criptografia, segundo Caruso e Steffen,[14] implica a existência de um algoritmo criptográfico que, por meio de uma chave de cifragem, transforma um texto claro em criptograma, ou seja, em um texto codificado. Disto resulta a necessidade de conhecimento do algoritmo de cifragem por parte dos envolvidos no processo e da chave de cifração/decifração.

Devido ao risco de quebra de cifração por meio da análise do criptograma, as chaves devem ser trocadas freqüentemente. Além do risco de intercepção, a lista de chaves precisa ser arquivada em algum meio de registro, e isso é passível de ser descoberto.

Apesar de não ser totalmente segura, de acordo com o que foi citado, a criptografia é mais um obstáculo a quem pretenda acessar indevidamente os dados da entidade. As senhas de acesso, quando armazenadas ou em trânsito na rede, devem estar criptografadas.

Conforme Sarah L. Roberts,[15] enquanto o comércio transforma a Internet, a necessidade de criptografia confiável tornou-se fundamental. No entanto, as entidades que usam tecnologia de criptografia desenvolvida nos Estados Uni-

14 Carlos A.A. Caruso e Flávio Deny Steffen, *Segurança em informática*, São Paulo, Livros Técnicos e Científicos Editora, 1991.

15 Sarah L. Roberts, "Globalizando a Criptografia – A indústria de *software* faz pressão", *Revista PC Magazine Brasil - Network Edition*, São Paulo, Editorial América do Brasil Ltda., Vol. 6, n. 3, mar. 1996, p. 14.

dos podem ter sua capacidade de competir globalmente limitada. Pela política atual dos Estados Unidos, a tecnologia de criptografia forte não pode ser exportada. Algumas organizações, incluindo a Business Software Alliance (Aliança de Negócios em Software), que representa Microsoft, Lotus e outras, estão pressionando o governo americano no sentido de derrubar essas restrições.

Firewall – Pode ser definido como barreira de segurança (na Internet), que isola partes da rede, criada para proteção de mensagens e transações, incluindo variados tipos de controle por *software* ou *hardware*.

As entidades devem instalar programas de segurança, os *firewalls* (paredes de fogo, em inglês) para limitar o acesso exterior à rede interna. Ele limita os tipos de conexões que podem ser feitas entre o interior e o exterior e quem pode fazê-las. O *firewall* é conectado tanto à rede interna quanto à rede externa, e assim, qualquer tráfego entre elas passa por ele.

Um controle adicional pode ser viabilizado por meio da implantação de uma trilha de auditoria, programa que permite a obtenção de todos os acessos às informações confidenciais e a identificação dos usuários, data, hora, estação de acesso e dos respectivos recursos em uso, servindo como instrumento de análise do auditor.

Uso restrito do e-mail – O *e-mail* funciona como caixas-postais de uso de assinantes, em rede que administra essa troca de mensagens. Permite que os usuários se comuniquem, transportando documentos formatados, arquivos de imagem e de som. É importante evitar o envio de informação confidencial pelo *e-mail*, pois esse tem sido objeto do ataque dos *hackers*.

Backup – Os controles devem garantir que a entidade possa recuperar-se, num período razoável de tempo, em função da criticidade, importância e sigilo, atribuídas às operações, de qualquer dano aos sistemas informatizados ou às suas informações. *Backup* é a cópia de segurança que, normalmente, preserva os dados armazenados em computadores contra uma eventual pane do equipamento em uso ou mesmo perda parcial ou total dos dados originais. Tornar o *backup* um hábito freqüente pode parecer uma idéia desagradável, perda de tempo, contudo, o potencial dos prejuízos advindos de pane ou a destruição dos dados informatizados podem ser expressivos ou mesmo irreversíveis.

A integração do *backup* com *software* antivírus é muito importante. Sem essa proteção, as fitas de *backup* podem tornar-se verdadeiras bombas-relógio ao invés de oferecer a desejada proteção. Para maior praticidade, o *software* deve efetuar o *backup* em altas velocidades.

software, treinamento de usuários e redirecionamento de recursos;
- proteger o armazenamento e o trânsito de documentos, mensagens e informações estratégicas e confidenciais;
- garantir a integridade de informações disponibilizadas apenas para consulta, impedindo a alteração indevida;
- elaborar e testar a metodologia e os procedimentos de *backup* e de contingência para a recuperação de dados em caso de acidentes e desastres;
- implementar segurança nos *notebooks*;
- viabilizar uma política de segurança para conexões externas via Internet, ou outras redes públicas de computadores, inibindo a ação de *backers* e *crackers*;
- capacitar os profissionais da entidade a atuar na implementação e na manutenção da política de segurança e administração das redes.

Outros Métodos Preventivos

Criptografia – É o conjunto de técnicas que permite codificar dados. O processo de criptografia, segundo Caruso e Steffen,[14] implica a existência de um algoritmo criptográfico que, por meio de uma chave de cifragem, transforma um texto claro em criptograma, ou seja, em um texto codificado. Disto resulta a necessidade de conhecimento do algoritmo de cifragem por parte dos envolvidos no processo e da chave de cifração/decifração.

Devido ao risco de quebra de cifração por meio da análise do criptograma, as chaves devem ser trocadas freqüentemente. Além do risco de intercepção, a lista de chaves precisa ser arquivada em algum meio de registro, e isso é passível de ser descoberto.

Apesar de não ser totalmente segura, de acordo com o que foi citado, a criptografia é mais um obstáculo a quem pretenda acessar indevidamente os dados da entidade. As senhas de acesso, quando armazenadas ou em trânsito na rede, devem estar criptografadas.

Conforme Sarah L. Roberts,[15] enquanto o comércio transforma a Internet, a necessidade de criptografia confiável tornou-se fundamental. No entanto, as entidades que usam tecnologia de criptografia desenvolvida nos Estados Uni-

14 Carlos A.A. Caruso e Flávio Deny Steffen, *Segurança em informática*, São Paulo, Livros Técnicos e Científicos Editora, 1991.

15 Sarah L. Roberts, "Globalizando a Criptografia – A indústria de *software* faz pressão", *Revista PC Magazine Brasil - Network Edition*, São Paulo, Editorial América do Brasil Ltda., Vol. 6, n. 3, mar. 1996, p. 14.

Software não pirata – Qualquer *software* só deveria, por questões de segurança, ser utilizado na entidade, dentro das condições pactuadas entre a entidade e o fornecedor.

Todo disquete (ou outro que tenha função equivalente) gravado por equipamento estranho à entidade deve ser submetido a tratamento de segurança, antes do seu uso, visando detectar possíveis contaminações.

Técnica de combate a vírus – O vírus de computador imita o da natureza, atuando de maneira semelhante. Trata-se de *software* cujo objetivo, além de acessar os dados da entidade, sem que para isto tenha autorização, consiste em instalar-se, reproduzir-se e dominar o sistema e, por vezes, impor-lhe perdas e alterações.

Segundo Kátia Jucá,[16] em função das próprias características dos vírus atuais, que se enquadram em categorias complexas como mutantes (atuam diferentemente em situações diversas), *encriptados* (criptografados) e *stealth* (furtivos), hoje todas as chamadas vacinas trabalham como múltiplas camadas de defesa.

Isso envolve o emprego de metodologias como varredura periódica (*scanning*) e o monitoramento contínuo do sistema. No primeiro caso, o usuário pode vasculhar periodicamente os arquivos à procura de parasitas. Já no segundo, um módulo residente em memória se encarrega do bloqueio permanente de uma possível ação virótica.

Os programas antivírus para redes, quando não conseguem evitar, totalmente, a ação do vírus, podem permitir a determinação dos grupos de usuários que devem ser avisados em caso de infecção. Os alertas são feitos por meio de alertas sonoros e mensagens na tela do computador. De acordo com a forma como o antivírus é configurado, o usuário pode receber orientações de como proceder no momento da detecção de um desses invasores. Entre várias alternativas de solução, existem possibilidades como tentativa de remoção do vírus, eliminação ou mudança de nome do arquivo, ou sua transferência para um outro diretório, onde possa ser isolado dos arquivos sadios.

Quando Kátia Jucá fala em vírus *atuais*, enfatiza o dinamismo com que o processo se reveste. Trabalha-se para dificultar a ação dos vírus, infelizmente, eles evoluem da mesma forma que as técnicas para combatê-los. A opção é continuar tentando dificultar sua ação. A idéia de impedi-los completamente parece pretensiosa, frente ao

16 Kátia Jucá, op. cit., p. 25.

desafio que representa. A eficácia dos antivírus se perde, portanto, se o usuário não utilizar versões atualizadas.

Como auditar

Utilizar-se da parceria, de equipes ecléticas de auditoria, recorrer a especialistas em determinados ambientes e linguagens de informática para preencher necessidades específicas e eventuais são recursos que podem ser utilizados na auditoria de redes, conforme demonstrou a pesquisa. Otimizar a integração entre a auditoria, a área de informática, de segurança e de telecomunicações é importante para maximizar os resultados almejados. A auditoria precisa compreender as mudanças, principalmente a dinâmica que essa área vivencia. Deve identificar, analisar e sugerir controles, assim como disseminar a política de segurança da informação, bom como indicar recursos disponíveis, de acordo com a necessidade.

O conhecimento das técnicas utilizadas visando a segurança da informação, comentadas anteriormente, e a identificação de sua utilização por parte da entidade é um ponto de partida para o desenvolvimento de um trabalho de auditoria. Precisa estar consciente, no entanto, de que não existe segurança total. O aperfeiçoamento dos controles e o acompanhamento das descobertas e do processo evolutivo devem ser uma constante na rotina do auditor.

✳

Controle das operações com derivatiovos

Recentemente, os derivativos foram objeto de publicações negativas. Casos como o da Kashima Oil do Japão, que teve um prejuízo de US$ 1,5 bilhão porque fez contratos cambiais de alto risco; da Procter & Gamble, dos Estados Unidos, que perdeu cerca de US$ 157 milhões em contratos futuros de juros; da alemã Metallgesellschaft, com uma perda estimada em US$ 1,4 bilhão com derivativos de petróleo; e o Banco Barings, da Inglaterra, com perda de US$ 1 bilhão, chamaram a atenção de muitos investidores.

A necessidade de formação de uma cultura sobre derivativos, análise de riscos e da forma de tratá-los, contabilização e controles das operações e a adoção de políticas preventivas face a problemas ocorridos em nível internacional têm sido objeto de reflexão das autoridades das áreas monetária e de supervisão bancária.

Tais reflexões levaram à formação de um grupo de trabalho, por parte do Centro de Estudios Monetários Latinoamericanos – Cemla para estudar as operações com derivativos, levan-

do-o a fazer recomendações.[17] A identificação de responsabilidades, bem definidas e respaldadas em normas legais, de cada membro do processo é fundamental, como a do administrador, das entidades de auditoria externa e dos auditores internos, o que promoverá uma maior exigência quanto aos controles internos, amenizando o risco.

Nelson Carvalho[18] considera que os esforços dos auditores encontram-se em estágios diversos de maturidade quanto à adoção de procedimentos específicos para auditar o risco de instrumentos financeiros derivativos, e que os esforços da classe deles, assim como de reguladores, como um todo, estão ainda muito incipientes e relativamente primários.

Segundo ele,

> constata-se uma necessidade quase imperiosa de treinamento especializado do auditor no jargão e nas práticas do mercado de derivativos e a exigência de apreciação, pelo auditor, dos efeitos econômicos e financeiros das transações efetuadas, dos resultados pendentes de realização e suas tendências respectivas, e da divulgação dos mesmos nos relatórios gerenciais internos e nas informações públicas por meio das demonstrações contábeis periódicas.

✳

Adaptação dos recursos humanos às mudanças

É sempre um grande desafio para qualquer segmento profissional rever a sua linha de ação, principalmente quando os fatos que determinaram a necessidade da mudança continuam sendo alterados, dentro de uma dinâmica constante.

Também o é para a Auditoria Interna no Brasil rever a sua linha de atuação, deixando de analisar as ocorrências empresariais como partes para vê-las dentro de um contexto global. Esse tema é tratado neste trabalho em um item próprio, por aplicar-se a todos os demais, já que a forma de o auditor interpretar os fatos empresariais é a base do seu trabalho.

Para superar tal disposição mental, é necessário analisar cada ação, identificando a sua importância com relação ao cumprimento da

17 Centro de Estudios Monetários Latinoamericanos – Cemla, *Riscos dos novos instrumentos financeiros e das operações fora de balanço e sua relação com o sistema de pagamentos*, 15 de fevereiro de 1995.

18 Luiz Nelson Guedes de Carvalho, "Uma contribuição à auditoria do risco de derivativos", São Paulo, Departamento de Contabilidade e Atuária da FEA/USP, 1996, p.143, mimeo, tese apresentada para obtenção do título de doutor em contabilidade.

missão empresarial. Tudo o que não agrega valor deve ser eliminado. O treinamento precisa incluir questões estratégicas, teóricas, não apenas operacionais. O auditor precisa estar despojado de rotinas burocráticas por meio de um bom suporte e investir o seu tempo em aperfeiçoar-se para assistir aos gestores de forma mais completa.

Comentários finais e Conclusões

Ao analisar os assuntos tratados até então, observa-se um descompasso entre o embasamento conceitual da AI e sua forma de atuação no Brasil, refletido notadamente na distinção entre a ação necessária para que cumpra sua missão e a ação praticada.

A compreensão do novo universo e a adaptação a ele constituem as maiores dificuldades, causadas, principalmente, pela ausência de uma visão sistêmica. A falta de uma visão sistêmica, por sua vez, decorre do desconhecimento ou deficiência no conhecimento do planejamento da entidade e pela falta de treinamento apropriado e contínuo.

Constatou-se que quase todas as auditorias pesquisadas reservam recursos para treinamento. No entanto, em grande parte delas, o treinamento deixa a desejar por não guardar um vínculo direto com o Plano de Auditoria e por contemplar apenas questões técnicas, fiscais e operacionais, sem incluir temas como ação estratégica ou variáveis que influenciam os rumos da entidade.

A literatura e as publicações especializadas, conforme se pode constatar na pesquisa junto às entidades, não suprem suficientemente os auditores para que se mantenham atualizados.

Pode-se concluir que a AI é importante e necessária à entidade, para que cumpra sua missão com eficiência. Hoje, enfrenta uma série de dificuldades por estar em fase de adaptação ao cenário que vem se alterando constantemente pela avalanche de mudanças.

As dificuldades nesse processo ocasionadas pela recente abertura do Brasil ao mundo, no entanto, não atingem particularmente a AI, mas a todos os segmentos econômicos, de uma maneira geral, de forma diferenciada.

Sua missão e objetivos, constantes dos manuais e diretrizes ditados pelos órgãos de classe, não mudaram, apesar de não estarem sendo atingidos completamente.

A descoberta por parte do auditor da sua identidade neste novo contexto representa o maior desafio a ser enfrentado, ***ser o que diz ser***, compreender completamente sua missão e envi-

DESCOMPASSOS IDENTIFICADOS

Treinamento	Treinamento insuficiente, sem vinculação ao Plano de Auditoria E sem Considerar aspectos da estratégia empresarial	Elaboração do Plano de Auditoria elaborado a partir de uma visão estratégica. Treinamento baseado no Plano de Auditoria
Avanço tecnológico	Ritmo incompatível com o Dinamismo do processo	Abordagem e análise considerando O Ritmo de alterações constantes
Agregação de valor	Abordagem *policialesca*. Ênfase na identificação de erros. Custo da Ineficiência	Ação voltada para a melhoria dos controles E não para a Identificação de erros
Análise simultânea quando da implantação de controles	Análise dos controles após a sua implantação, permitindo que uma falha permaneça despercebida por algum tempo	Análise dos controles de forma a Identificar qualquer falha nos controles, se possível antes que Gere dificuldades para a entidade ou de forma a minimizar os problemas dela derivados
Visão sistêmica	Análise da relevância dos sistemas distorcidas por falta de Visão Sistêmica Desconhecimento do planejamento, das diretrizes empresariais e do mercado onde a entidade se insere	Formação de visão sistêmica por Meio do conhecimento do planejamento, das diretrizes empresarias e do mercado onde a entidade se insere. Análise da relevância de cada fato com relação à missão da entidade
Ação pró-ativa	Ação reagente. A ação ocorre, basicamente, a partir de uma demanda do superior hierárquico, em se tratando de questões estratégicas para a Entidade	Disponibilização, por parte da Auditoria Interna, de análises, pareceres e de quaisquer Informações úteis para subsidiar o gestor na tomada de decisões, independentemente de uma solicitação expressa
Análise da natureza integrada Das operações	Ausência de análises que identifiquem os efeitos sobre as operações gerados a partir de inúmeras, freqüentes e/ou simultâneas mudanças	Análise dos fatos de forma Integrada e não Como se fossem um sistema fechado
Autoridade Técnica e bom relacionamento interpessoal	Atitude *policial*, identificadora de erros sem atentar para a melhoria do processo	Colaboração com as áreas auditadas, recomendando ações que visem a Melhoria do sistema
Análise inadequada do controle interno	Desconhecimento do planejamento. Falta de visão sistêmica, comprometendo a análise da materialidade e relevância	Conhecimento do planejamento. Abordagem sistêmica
Capacidade de se adaptar	Ritmo incompatível com o dinamismo do processo	Discussão do embasamento conceitu da AI
Atualização	Informações, obtidas por meio de assinatura de revistas e publicações especializadas, insuficientes	Criação de ambiente propício ao contínuo intercâmbio e discussão de idéias dentro e fora da em tidade, inclusive em grupos pela *Internet*, e leitura de revistas e publicações especializadas
Flexibilidade na forma de atuação	Discussão do embasamento conceitual e estratégico da Auditoria Interna insuficiente e insatisfatório	Discussão do embasamento Conceitual e estratégico da Auditoria Interna
Utilização de sistemas para suportar os trabalhos do auditor	Subutilização da estrutura de informática disponível	Utilização dos sistemas Informatizados para dar suporte aos trabalhos de

dar esforços no sentido de cumpri-la, servindo-se de um bom suporte tecnológico para tal.

O avanço tecnológico tem-se dado de forma tão surpreendente que, por vezes, o homem subestima-se em relação a ele. *O criador sentindo-se ultrapassado pela criação.* Em algumas circunstâncias, perde-se a visão do essencial. De que adianta, no entanto, um excelente suporte se não se sabe como ou em que utilizá-lo?

A visão estratégica, sistêmica, do auditor, é o seu norte. Tudo o mais passa a ser utilizado em relação a essa visão. A forma de pensar, a capacidade de aprender, de se adaptar, é o ponto crucial, determinante para a consecução da missão da AI.

Os gestores exigem de suas entidades, cada vez mais, um desempenho compatível com as exigências do mercado.

Compete ao auditor interpretar, entender e colaborar com o estabelecimento de estratégias que suportem o futuro da entidade. É ele quem precisa alertar a alta administração do custo/benefício relacionados aos investimentos, inclusive com relação à área de informática, considerando a importância de a companhia ser competitiva e viável.

Cabe a ele assessorar os gestores no seu papel de agentes de transformação, para evitar que a omissão e o comodismo possam gerar um descompasso entre a entidade e o mercado onde ela atua.

Vivencia-se o desencadear de uma avalanche de novos meios tecnológicos e conceitos. Pode-se interagir com as mudanças participando delas ou sendo por elas ultrapassados. A compreensão dessa dinâmica e a habilidade de a empresa assimilar informações e conhecimentos deverá ser o diferencial que impulsionará cada entidade em uma ou em outra direção, culminando com o seu sucesso ou fracasso.

À AI cabe contribuir, colaborando com os gestores no estabelecimento de controles nos novos ambientes virtuais, administrativos e de negócios, para que se desincumbam de suas atividades com eficiência e eficácia.

Referências bibliográficas

ACKOFF, Russel L. *Planejamento empresarial*, Rio de Janeiro, Livros Técnicos e Científicos, 1974.

AOKI, Shigeo & SAKURAI, Michiharu. *Japanese management accounting: A world class approach to profit management. Internal auditing in Japan: A Survey*, Cambridge, Produtiv Press, 1989.

AUDIBRA, Instituto dos Auditores Internos do Brasil. *Normas Brasileiras para o exercício da auditoria interna*, 2. ed., São Paulo, Audibra, 1992.

———— . *Procedimentos de Auditoria Interna – Organização Básica.* São Paulo, Audibra, 1991.

———— . "Congresso Latino Americano de AI", *Revista do Auditor*, São Paulo, Ano II, n. 10, dez. 1995.

ARIMA, Carlos Hideo. *Metodologia de Auditoria de Sistemas*, São Paulo, Editora Érica, 1994.

BASÍLIO, Sérgio. "Segurança em redes: o papel do *backup*", *Revista PC Magazine Brasil – Network Edition*, São Paulo, Editorial América do Brasil, Vol. 6, n. 3, jul. 1996.

BERTALANFFY, Ludwig Von. *Teoria Geral dos Sistemas*, Petrópolis, Vozes, 1975.

BASILE, Oswaldo. "Agregação de valor", XXI Congresso Brasileiro de Auditoria Interna, resumo de transparências, Palestra não publicada, Fortaleza, nov. 1997.

BIO, Sérgio Rodrigues. *Sistemas de informação – Um enfoque gerencial*, São Paulo, Atlas, 1987.

BITTAR, Rodrigo. "Bug 2000 ajuda Politec a consolidar liderança no mercado", *Gazeta Mercantil*, Distrito Federal, Ano I, n. 34, 27 nov. 1997.

BRITO, Manoel Francisco. "De Graça", *Veja*, São Paulo, Abril, Ano 29, n. 50, 11 dez. 1996.

CARVALHO, Luiz Nelson Guedes de. "Uma contribuição à auditoria do risco de derivativos", São Paulo, Faculdade de Economia, Administração e Contabilidade da Universidade de São Paulo, 1996, tese apresentada ao Departamento de Contabilidade e Atuária para obtenção do título de doutor em contabilidade, mimeo.

CARVALHO, L. Nelson & SANTOS, Ariovaldo dos. "As melhores e as maiores", *Exame Melhores e Maiores*, São Paulo, Abril, jul. 1997.

CARUSO, Carlos A. A. & STEFFEN, Flávio Deny. *Segurança em informática*, São Paulo, Livros Técnicos e Científicos Editora, 1991.

CEMLA, Centro de Estudios Monetários Latinoamericanos. *Riscos dos novos instrumentos financeiros e das operações fora de balanço e sua relação com o sistema de pagamentos*, 15 fev. 1995.

CHIAVENATO, Idalberto. *Administração – Teoria, processo e prática*, 2. ed., São Paulo, McGraw Hill, 1987.

CONSELHO FEDERAL DE CONTABILIDADE. *Normas Profissionais do Auditor Interno*, Portaria n. 781, 24 mar. 1995.

CONESA, Ubiratan Zaccaro & BISPO, Ronaldo José. "Uma gestão de futuro", *Revista Brasileira do Auditor*, São Paulo, Ano I, n. 4, abr. 1993.

DECRETO Nº 84.128, de 29.10.79.

DELGADO, Maria Lúcia; EDWARD, José & OLTRAMARI, Alexandre. "Quando a emoção é inteligência", *Veja*, n. 1.478, São Paulo, Abril, Ano 30, n. 2, 15 jan. 1997.

DIÁRIO OFICIAL Nº 151, 6 de agosto de 1996, seção 1.

DIAS, Donaldo de Souza. *O sistema de informação e a empresa*, Rio de Janeiro, Livros Técnicos e Científicos, 1985.

DUBNER, Alan Gilbert. "Pague suas compras na rede em bits", *Revista Informática Exame*, São Paulo, Abril, Ano 11, n. 126, set. 1996.

ENCICLOPÉDIA NAÇÕES DO MUNDO. *Grã-Bretanha*, São Paulo, Abril, 1992.

FIGUEIREDO, Sandra & CAGGIANO, Paulo Cesar. *Controladoria*, São Paulo, Atlas, 1992.

GAZETA MERCANTIL. "As maiores empresas do Brasil", São Paulo, Ano XXI, 31 out. 1997.

GENESINI, Sílvio." O Brasil está perdendo o bonde – Comunicação e conhecimento são tão importantes quanto a informática", *Revista Informática Exame*, São Paulo, Abril, Ano 10, n. 116, nov. 1995.

GOMES, Josir Simeone & AMAT, Joan M. "Controle de gestão: Um enfoque contextual e organizacional", *Anais do IV Congresso Internacional de Custos*, Campinas, jun. 1995.

GOYA, Denise Hideko; MOURÃO, Liane Vitorio & CENTOLA, Nicolau. "Internet: Pegue essa onda", *Revista PC Magazine Brasil – Network Edition*, São Paulo, Editorial América do Brasil, Vol. 6, n. 3, mar. 1996.

GREGO, Maurício. "Como montar sua Intranet", *Revista Informática Exame*, São Paulo, Abril, Ano 11, n. 121, abr. 1996.

JUCÁ, Kátia. "Proteja sua rede dos invasores", *Revista Informática Exame*, São Paulo, Abril, jan. 1996.

KEHOE, Brendan P. *Zen e a arte da internet*, 3. ed., Rio de Janeiro, Campos, 1995.

KOITI, Fabio. "Sua empresa + internet = intranet – Crescem os negócios na Internet", *Revista PC Magazine Brasil – Network Edition*, São Paulo, Editorial América do Brasil, Vol. 6, n. 3, mar. 1996.

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

MACHADO, Carlos. "Uma revolução no mercado de softwares", *Revista Informática Exame*, São Paulo, Abril, Ano 11, n. 118, jan. 1996.

MARINS, L. A.. "O capital humano – O segredo do sucesso empresarial", apresentação gravada em fita de vídeo.

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

MILITELLO, Katia. "O dinheiro escapa do bug?", *Revista Info Exame*, São Paulo, Abril, dez. 1997.

MÓDULO Consultoria e Informática. Prospecto de Divulgação da Empresa.

NAKAGAWA, Masayuki. *Introdução à controladoria – Conceitos, sistemas, implementação*, São Paulo, Atlas, 1993.

NAKAMURA, Angela Mie. "Contribuição ao estudo de procedimentos e evidenciação contábeis aplicáveis a operações com derivativos voltados a instituições financeiras", São Paulo, Faculdade de Economia, Administração e Contabilidade da Universidade de São Paulo, 1996, tese apresentada ao Departamento de Contabilidade e Atuária para obtenção do título de doutor em contabilidade, mimeo.

NERY, Fernando. "Redes integradas à Internet – Vulnerabilidade e soluções de segurança", *XX Congresso Brasileiro de Auditoria Interna*, Fortaleza, nov. 1996.

ONU, Organização das Nações Unidas. "Princípios fundamentais de contabilidade", *Revista IOB: Temática Contábil e Balanço*, São Paulo, bol.33/90.

RATLIFF, Richard L. & BECKSTEAD, Stephen M. "Como o gerenciamento de nível internacional está transformando o sistema de auditoria interna", *Boletim do Ibracon*, São Paulo, dez. 1996.

ROBERTS, Sarah L. "Globalizando a criptografia – A indústria de *software* faz pressão", *Revista PC Magazine Brasil – Network Edition*, São Paulo, Editorial América do Brasil Ltda., Vol. 6, n. 3, mar. 1996.

SENGE, Peter M. *A quinta disciplina – Arte, teoria e prática da organização de aprendizagem*, 11. ed., São Paulo, Best Seller, 1990.

SETTI, Ricardo Balabachevsky. "O beco tem saída", *Superinteressante*, São Paulo, Abril, Ano 11, n. 2, fev. 1997.

SHIMIZU, Heitor & SETTI, Ricardo B. "Tem boi na linha", *Superinteressante*, São Paulo, Abril, Ano 9, n. 10, out. 1995.

TREVISAN, Auditores e Consultores. *Auditoria – Suas áreas de ação*, São Paulo, Atlas, 1996.

WALTON, Richard E. *Tecnologia de Informação*, São Paulo, Atlas, 1994.

YANAKIEW, Monica. "Governo pode perder corrida contra o 'bug'", *Gazeta Mercantil*, São Paulo, 20 out. 1997.

ZINI JUNIOR, Álvaro Antonio. "'Derivativos' explodem no mercado externo", *Folha de S. Paulo*, São Paulo, 25 set. 1994.