2
Da auditoria tradicional à auditoria contínua

Este capítulo busca descrever a evolução das metodologias de auditoria interna até a abordagem de auditoria contínua, com aplicação de novas tecnologias e ferramentas automatizadas. Essa visão permite contextualizar a importância da auditoria contínua nas empresas de capital aberto, particularmente na empresa do setor elétrico foco do estudo de caso (capítulo 5). Além da apresentação dos conceitos básicos de auditoria interna, controle interno e auditoria contínua, discutem-se os resultados de estudos empíricos sobre auditoria contínua, buscando-se identificar as tecnologias necessárias, bem como descrever os níveis dessa metodologia de auditoria (OLA, DLA e PLA).

2.1.
Breve histórico

Segundo os autores Gil (1992) e Araujo (2001) a palavra "auditoria" deriva do latim "*auditore" ou* "*audire"* que significa "aquele que ouve". É comum afirmar que o termo auditoria é um exame minucioso e sistemático das atividades de um setor ou uma empresa na função de estabelecer se estas atividades estão em conformidade com disposições previamente estabelecidas ou planejadas.

É de difícil precisão estabelecer quando a atividade passou a ser considerada em nossos primórdios, mas sabe-se da existência de documentos históricos de trabalhos correlacionados, nos impérios caldeu e babilônio.

A prática também é verificada em registros arqueológicos descobertos na Suméria, datados de 4.500 a.C, assim como em territórios romanos (Sá, 2002).

Segundo Madeira (2010), a prática da auditoria, em todos esses eventos iniciais de sua formação estaria comumente relacionada com as atividades econômicas na verificação da gestão sobre a propriedade do homem e organizações.

Com a revolução industrial novos conceitos, diretrizes e técnicas foram sendo incorporadas à função de auditoria de forma a atender as necessidades de

emergentes corporações. Na medida do aumento da produção em escala, cresceram também incidentes mercantis por consequência da não presença constante de seus proprietários no cotidiano dos negócios, levando aos primeiros trabalhos de auditoria realizados por acionistas, que não eram os administradores de fato das empresas. A evolução desta forma de trabalho se deu pela alteração da legislação que passou a permitir que outras pessoas, não acionistas, pudessem fazer o trabalho de auditoria. Nesse período, surgiram empresas independentes e especializadas em auditar, tais como Deloitte & Co., Peat, Marwick & Michell e Price Waterhouse & Co (Boynton, Johnson e Kell, 2002).

Ainda segundo esses autores, a experiência britânica foi disseminada nos EUA no final do século XIX, principalmente por investidores escoceses e ingleses do ramo de cervejarias e construção de estradas de ferro, que queriam inibir ou bloquear o surgimento de fraudes em suas atividades.

Naquela época, o estado de New York passava a ser o pioneiro na certificação dos trabalhos específicos de auditoria independente, através da emissão dos CPAs (*Certified Public Accountants – CPAs*). A partir de 1921, os demais estados da federação seguiram o mesmo conceito.

Com a crise da bolsa de valores em 1929, as deficiências do então sistema contábil e de informações das empresas foram evidenciadas em auditorias. A constatação dessas anomalias apontou a necessidade de acrescentar outros conceitos de lucro e desempenho operacional que pudessem gerar confiabilidade aos acionistas (Boynton, Johnson e Kell, 2002).

A partir de 1934, foi criada a *Security and Exchange Comission* (*SEC*), que fomentou o estímulo, crescimento e destaque para a profissão de auditor às empresas que negociavam na bolsa de valores. A regulamentação foi inserida com a promulgação da Lei de Negociação de Títulos, de 1934, que obrigou a utilização de serviços de auditoria para confiabilidade das demonstrações financeiras (Madeira, 2010).

Ainda que os trabalhos de auditoria estivessem nos primórdios vinculados à área contábil financeira, o seu conceito foi se modificando ao longo tempo, evoluindo para uma abordagem mais abrangente com inserção na sistemática de gestão das empresas, conformidade das transações operacionais à legislação e aos normativos internos (Madeira, 2010).

Mostra-se, a seguir, a evolução desse conceito a partir das percepções de

alguns autores em suas respectivas épocas.

Segundo William H. Bell e Ralph S. Johns (1942):

"auditoria é a verificação geral das contas de uma empresa para determinar sua posição financeira, o resultado de suas operações e a probidade de seus administradores, com o fim de comunicar o resultado do exame aos proprietários, acionistas, gerentes, conselheiros, bolsas e outros órgãos oficiais, síndicos, atuais ou prováveis arrendatários, futuros interventores ou compradores, juntas de credores, agências mercantis, hipotecários ou quaisquer outros interessados. Para verificar se houve prestação justa de contas de um patrimônio e se os negócios foram convenientemente administrados, para satisfação ao público, aos doadores etc. Para verificar custos, lucros ou prejuízos de um negócio. Para descobrir e impedir fraudes."

De acordo com Arthur Warren Holmes (1956):

"... a auditoria é o exame de demonstrações e registros administrativos. O auditor observa a exatidão, integridade e autenticidade de tais demonstrações, registros e documentos."

Esse autor evidencia ainda, a atividade de auditoria como uma crítica e sistemática verificação do controle interno da contabilidade e demais documentos em geral que circulam em uma empresa, uma vez que até fatos de natureza extrapatrimonial são elementos necessários à fundamentação de conclusões.

Conforme José Alvarez Lopez (1989):

"as palavras auditoria ou censura de contas se relacionam com a revisão e verificação de documentos contábeis, registros, livros e listagens de contas, utilizadas no processo de captação, representação e interpretação da realidade econômico-financeira da empresa."

Hilário Franco e Ernesto Marra (2000) define auditoria como:

"uma técnica contábil que compreende o exame de documentos, livros e registros, inspeções e obtenção de informações e confirmações, internas e externas, relacionadas com o controle do patrimônio, objetivando mensurar a exatidão desses registros e das demonstrações contábeis deles decorrentes."

Segundo Boynton, Johnson e Kel (2002):

"auditoria é um processo sistemático de obtenção e avaliação de evidências sobre ações e eventos econômicos, com objetivo de mensurar o grau de correspondência com os critérios estabelecidos e de comunicar os resultados a usuários interessados."

Pelas definições acima, observa-se que a evolução dos conceitos das atividades de auditoria, além de representar a tendência moderna de não só atribuir-lhe o papel de simples verificador, mostra que ao longo do tempo outras importantes funções foram adicionadas no sentido de incorporar toda a estrutura da empresa e de sua administração.

Sob essa perspectiva, Ramamoorti (2003) ressalta que, com o crescimento e complexidade dos novos negócios, em meados do século XX, houve a necessidade da separação das verificações internas de sistemas contábeis daquelas informações

que suportam a tomada de decisão de seus gestores.

De fato, os gestores careciam de instrumentos para avaliar não só a eficiência do trabalho realizado, mas também a honestidade dos seus subalternos. Dessa forma, como será abordada nas seções seguintes, a auditoria interna se mostrou necessária a esse fim.

2.2. Auditoria interna: conceitos, normas e funções

As primeiras definições do papel do auditor interno foram reforçadas pela criação internacional do *Institute of Internal Auditors* (IIA) em 1947. A partir desse evento, os fatores contábeis e financeiros passaram a ser as premissas da auditoria interna, assim como assuntos de abrangência operacional. Dessa forma, a auditoria interna passou a cobrir todas as áreas da administração, sendo estruturalmente subordinada diretamente à alta administração, na condição de manter-se independente.

Segundo Barros (2007), a declaração de responsabilidade dos auditores internos elaborada pelo IIA ampliar-se-ia anos depois, contemplando: (i) revisão e avaliação da qualidade, adequação e aplicação do controle contábil, financeiro e operacional; (ii) determinação da extensão de cumprimento das políticas, planos e procedimentos estabelecidos; (iii) determinação em que proporção os ativos da empresa são corretamente registrados e protegidos contra danos ou perdas de quaisquer naturezas; (iv) determinação da confiabilidade dos dados contábeis e de outros dados originados dentro da organização; e (v) avaliação do desempenho dos gerentes em cumprirem as responsabilidades definidas.

No Brasil, a iniciativa de criar um instituto voltado para as atividades de auditoria foi concretizada em 1960, com o desenvolvimento do Instituto dos Auditores Internos do Brasil (IIA Brasil).

Filiado ao IIA americano, este instituto vem promovendo desde sua criação, a difusão de técnicas, capacitações e certificações de profissionais de auditoria. As atividades exercidas e sua principal missão encontram-se definidas em seu estatuto, como segue:

> "...defender, difundir e desenvolver a profissão de Auditoria Interna assim como os profissionais que a exerçam para que possam ajudar no efetivo gerenciamento de riscos, governos corporativo e processos de controles internos das organizações, visando a defesa dos interesses dos acionistas, cotistas e outros grupos de interesse e da sociedade em seu

> conjunto" (IIA Brasil, 2014).

A definição de auditoria interna pelo IIA americano, traduzido na sua forma para sua filiada brasileira é a seguinte:

> "...é uma atividade independente e objetiva de avaliação (*assurance*) e de consultoria, desenhada para adicionar valor e melhorar as operações de uma organização. Ela auxilia uma organização a realizar seus objetivos a partir da aplicação de uma abordagem sistemática e disciplinada para avaliar e melhorar a eficácia dos processos de gerenciamento de riscos, controle e governança..." (IIA Brasil, 2014).

Segundo Barros (2007), não é por acaso a presença do termo *assurance* no texto do IAA Brasil, porque a simples substituição pela palavra "avaliação" não traduz todo o seu significado, visto que o serviço de *assurance* constitui-se do exame objetivo de evidências para se obter avaliação independente.

Em 2012, com o objetivo de uniformizar a atividade de auditoria interna globalmente, o *Institute of Internal Auditors* promoveu a emissão de normas e padrões internacionais com os seguintes propósitos:

- delinear os princípios básicos que representam a prática de auditoria interna;
- fornecer uma estrutura para a execução e promoção de um amplo espectro de auditoria interna de valor agregado;
- estabelecer as bases para a avaliação de desempenho da auditoria interna;
- promover a melhoria dos processos e operações organizacionais.

A representação esquemática da Figura 2.1 mostra a estrutura conceitual das práticas profissionais de auditoria interna, conforme adaptação dos autores Boynton, Johnson e Kell (2002, p. 933) e Barros (2007). Nessa estrutura, a definição de auditoria interna apresenta-se como referência mais ampla para a prática profissional da atividade, que inclui o código de ética, as normas ou padrões de atributo e desempenho, as normas ou padrões de implementação dos serviços de *assurance* e de consultoria, as diretrizes e manuais de orientações e métodos de execução, sendo essas últimas aplicadas e adaptadas de acordo com as peculiaridades sociais de países e organizações.

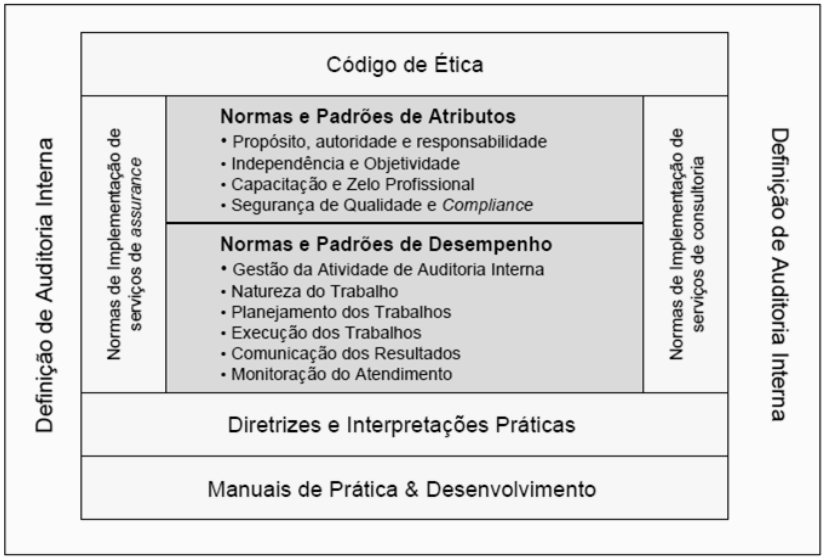

Figura 2.1 - Estrutura conceitual de práticas profissionais em auditoria interna
Fonte: Barros (2007), adaptado de Boyton, Johnson e Kell (2002).

Esse conjunto hierárquico de orientações sugere a adoção voluntaria pelas auditorias internas, podendo tornar-se obrigatório, por força de normas emitidas por autoridades reguladoras ou por decisão estatutária ou deliberativa da própria organização (Barros, 2007).

O *Institute of Internal Auditors* (IIA) orienta que o escopo do trabalho de auditoria interna seja desenvolvido de maneira a avaliar se os controles, processos de governança e gestão de riscos estão sendo administrados conforme planejados e de forma a garantir que:

- os riscos estejam mapeados e gerenciados;
- a interação com os grupos de governança ocorram como necessário;
- as informações relevantes no plano financeiro, gerencial e operacional sejam precisas, confiáveis e prestadas de forma pontual;
- as atividades desempenhadas pelos empregados estejam conformes com as políticas, normas, procedimentos, leis e regulamentos estabelecidos;
- os recursos necessários estejam sendo adquiridos de forma econômica, com destinação eficiente e adequadamente protegidos;
- programas, planos e metas sejam atingidos;
- a qualidade e a melhoria contínua sejam pertencentes aos processos de controles da organização;
- aspectos legais que impactam a organização sejam apropriadamente reconhecidos e resolvidos.

O controle interno representa um dos importantes pilares de atuação da auditoria interna dentro das organizações.

Segundo o *American Institute of Certified Public Accountants* (AICPA), conselho federal de auditores americanos (em tradução livre), através de seus relatórios especiais de procedimentos de auditoria (AU Section 110, 1972) definiu ser de responsabilidade da administração a manutenção e o estabelecimento de controles internos para registrar, processar, autorizar e informar por meio de relatórios, transações consistentes com as afirmações prestadas pela organização em seus relatórios contábeis e financeiros.

Já o IIA define que o controle interno é qualquer ação adotada pela a administração, conselho, ou por outros interessados que aprimorem a probabilidade dos objetivos e metas serem alcançados. Tais controles podem ser: (i) de prevenção de ocorrência de eventos indesejáveis; (ii) de detecção, de forma a identificar e corrigir eventos não desejáveis após sua constatação; e (iii) de direção, com estímulo e orientação para a ocorrência de eventos desejáveis.

Os controles internos podem funcionar de forma automática ou manual, conforme a presença de sistemas automatizados ou de procedimentos manuais para serem seguidos.

A divulgação de relatório pela *Treadway Comission* (1987) expôs a necessidade da importância dos controles internos na coibição de fraudes e detecção de anomalias contábeis antes da divulgação de demonstrações de resultados. Constatou ainda que a fragilidade dos controles internos nas organizações eram uma das principais causas de fraudes. Nesse sentido, a *Treadway Comission* recomendou uma conceituação mais robusta para controles internos de forma a prover certa segurança na detecção de fraudes.

Tal recomendação foi seguida pelas diversas entidades e institutos responsáveis pelos assuntos de auditoria, como o *Committee of Sponsoring Organizations of the Treadway Comission* (COSO); o *Control Objectives for Information and Related Technology* (COBIT); e o *Institute of Chartered Accountants in England & Wales* (*Turnbull Report).*

Como observado por Barros (2007), as normas e padrões aplicáveis à auditoria interna no setor privado são diferentes das estabelecidas para a auditoria externa. Essas normas se diferenciam em relação ao órgão regulador e pela própria natureza do trabalho.

O que se verifica é que as normas e padrões estabelecidos para a atividade de

auditoria interna são elaborados pelos institutos, sem caráter mandatório ou legal, como é o caso do IIA (Madeira, 2010). Entretanto existem normas dirigidas às auditorias internas emitidas pelo Conselho Federal de Contabilidade (CFC) que estabelecem regulamentos às atividades profissionais e técnicas para a atividade de auditoria, como, por exemplo, a Norma Brasileira de Contabilidade (NBC) PI - do Auditor Interno e a norma técnica NBC TI - de Auditoria Interna (Lelis, 2010).

Madeira (2010) evidencia ainda que por meio da resolução 986/2003, o CFC (2003) apresentou uma norma relativa a procedimentos de auditoria interna contábil, aplicáveis a empresas públicas e privadas. Essa norma discorre sobre o planejamento de auditoria, riscos, procedimentos, amostragem e relatório.

Já o IIA, estabelece normas e padrões aplicáveis mundialmente. No Brasil, desempenha o papel de seguir as diretrizes do instituto americano, na capacitação de profissionais e difusão de suas práticas.

Os propósitos das normas e padrões definidos pelo IIA são:

- estruturação dos princípios básicos para a prática de auditoria interna;
- construção de uma estrutura para a execução e promoção de auditorias internas que agreguem valor organizacional;
- estabelecimento de critérios na avaliação de desempenho da auditoria interna;
- fomento da melhoria dos processos e operações na organização.

Recentemente, o IIA aprovou uma nova Estrutura Internacional de Práticas Profissionais (IPPF). As principais alterações revisadas em outubro de 2012, foram:

- a fixação da responsabilidade de todos os auditores internos quanto a conformidade, objetividade, proficiência e zelo profissional;
- a alteração do termo "revisor" para "avaliador";
- passa a considerar o alcance dos objetivos estratégicos definidos previamente como objeto a ser avaliado;
- passa também a avaliar os critérios a qual a administração e/ou conselho definiram os objetivos e metas da organização;
- pontua que a responsabilidade pelo trabalho final de auditoria sempre será do executivo chefe de auditoria, mesmo que delegada.

As modificações incluíram o agrupamento de normas e padrões, em classificação que as define como mandatórias ou fortemente recomendadas para a boa prática da auditoria interna.

Na classificação mandatória encontram-se: (i) definição dos objetivos da auditoria interna; (ii) normas e padrões internacionais; e (iii) código de ética.

Como fortemente recomendados, situam-se: (i) os guias práticos com orientações detalhadas, ferramentas e técnicas, entre outras; (ii) orientações voltadas para a prática, abordando questões específicas de cada país ou setor industrial, código de ética e padrões que promovem boas práticas; (iii) declarações de posicionamento, abordando o papel da auditoria interna no gerenciamento do risco (IIA, 2009); no suprimento de recursos para a atividade (IIA, 2009); além das três linhas de defesa no gerenciamento eficaz de riscos e controles (IIA, 2013).

As normas podem ser classificadas também em três grupos, a saber: (i) normas de atributo; (ii) normas de desempenho; e (iii) normas de implantação. A seguir descrevem-se esses três tipos de normas

2.2.1. Normas de atributo

São normas a serem aplicadas a todos os serviços de auditoria interna. Essa família de normas rege as peculiaridades dos indivíduos que executam a tarefa de auditar, bem como a natureza da organização auditada.

As principais séries das normas de atributo são:

- 1000 – Propósito, autoridade e responsabilidade: o propósito, a autoridade e a responsabilidade da atividade de auditoria interna devem ser formalmente definidos em um regulamento ou estatuto de auditoria interna, aderente com a Definição de Auditoria Interna, com o Código de Ética e com as Normas aplicáveis. O estatuto ou regulamento deve ser periodicamente revisado pelo executivo chefe de auditoria e submetido à aprovação da alta administração;
- 1100 – Independência e objetividade: a atividade de auditoria interna deve ser independente e os auditores internos devem ser objetivos, imparciais ao executar suas atividades. Qualquer ameaça a esta independência deve ser comunicada às partes apropriadas. O executivo chefe tem acesso irrestrito e direto à alta administração;
- 1200 – Proficiência e zelo profissional devido: os trabalhos de auditoria devem ser executados com zelo e a devida proficiência. Entende-se por proficiência como conhecimento e habilidades requeridas pelos auditores internos, que devem ser encorajados a demonstrar sua proficiência obtendo as certificações e qualificações profissionais apropriadas.
- 1300 – Programa de avaliação da qualidade e melhoria: cabem ao executivo chefe de auditoria o desenvolvimento e a manutenção de um programa de avaliação da qualidade que incorpore todas as atividades de auditoria interna, permitindo sua evolução contínua.

2.2.2.
Normas de desempenho

Também de abrangência a todos os serviços de auditoria interna, esse tipo de norma estabelece os parâmetros e critérios de qualidade na avaliação da auditoria interna.

As principais séries das normas de desempenho são:

- 2000 – Gerenciamento da atividade de auditoria interna: o executivo chefe de auditoria deve realizar uma gestão eficaz da atividade, agregando valor à organização. Fazem parte de suas atribuições o planejamento periódico baseado em análise de riscos da organização, a comunicação dos resultados à alta administração, a garantia dos recursos necessários ao cumprimento do plano aprovado e o estabelecimento de políticas e procedimentos internos, dentre outros;
- 2100 – Natureza do trabalho: com a utilização de uma abordagem sistemática e disciplinada, a atividade de auditoria interna deve avaliar e contribuir para a evolução e melhoria dos processos de governança coorporativa, gerenciamento de riscos e controles;
- 2200 – Planejamento do trabalho de auditoria: os auditores internos devem estruturar e documentar planos para cada trabalho de auditoria, traçando seus objetivos, definindo o escopo, o prazo, riscos associados e a previsão de recursos de trabalho necessários;
- 2300 – Execução do trabalho de auditoria: para atingir o objetivo, os auditores internos devem basear suas conclusões e resultados através da coleta de informações e o seu devido registro.
- 2400 – Comunicação dos Resultados: os auditores internos devem comunicar os resultados dos trabalhos de auditoria, que devem conter opiniões ou conclusões, quando apropriado;
- 2500 – Monitoramento do progresso: o executivo chefe de auditoria deve estabelecer e manter um processo para monitoramento das ações necessárias apontadas em relatórios de auditoria, verificando se essas mesmas ações foram implementadas ou que a alta administração tenha aceitado os riscos de não executá-las.

2.2.3.
Normas de implantação

São aplicadas a trabalhos específicos diferenciados entre consultoria e avaliação (*assurance*).

2.3.
A Lei Sarbanes & Oxley (SOX) e sua influência na auditoria interna

A Lei Sarbanes-Oxley, promulgada em julho de 2002 nos EUA, foi um marco na regulamentação do mercado de capitais. A lei foi uma resposta à crise de confiança devido aos inúmeros escândalos contábeis que envolveram grandes corporações americanas, tais como, Enron e WorldCom.

Com o objetivo de proteger os investidores de fraudes, a Lei SOX, como ficou conhecida, estabelece dispositivos que determinam penas e responsabilidades aos executivos pela qualidade das informações contábeis e financeiras disponibilizadas ao mercado de capitais. Ela estabelece ainda a avaliação da administração sobre os controles internos, expondo suas fraquezas quando presentes.

Em outra definição de objetivos, Borgerth (2007) atribui:

> "o grande objetivo da SOX é de restaurar o equilíbrio dos mercados por meio de mecanismos que assegurem a responsabilidade da alta administração de uma empresa sobre a confiabilidade da informação por ela fornecida".

Com o estabelecimento de rígidos padrões de responsabilidade corporativa suportando a criação de mecanismos de segurança e auditoria das informações, a SOX limita à livre atuação de seus agentes em seu benefício e prejuízo dos investidores (Lelis, 2010).

Borgeth (2007) ressalta que, mesmo antes do escândalo contábil da Enron, a agência federal americana responsável por títulos mobiliários *Securities and Exchange Commission* (SEC), já havia manifestado sua preocupação com aumento da prestação de serviços independentes e não relacionadas à auditoria em grandes corporações. O receio era que com o crescimento dessa prática, os serviços de consultoria voltados à auditoria de fato fossem desestimulados à especialização em assuntos pertinentes.

Dessa forma, após os escândalos, a SOX procurou estabelecer novas regras para a compreensão do conceito de independência dos auditores.

A SOX determina que para a prestação de serviços não relacionados em sua lista da Seção 201, o Comitê de Auditoria da organização deverá pré-aprovar e seguir as seguintes imposições:

- respeitar o prazo de no mínimo um ano para contratação entre uma empresa e outra de serviços de auditoria da mesma entidade;
- o auditor deverá se reportar ao Comitê de Auditoria, ao invés da diretoria financeira da empresa;
- a cada cinco anos deve ser feito um rodízio do sócio encarregado das finanças.

A Lei SOX exige ainda a divulgação das aprovações do Comitê de Auditoria aos investidores através de relatórios periódicos registrados na SEC.

Com essa nova disposição, a SEC fica responsável pela revisão e divulgação dos relatórios contábeis e demonstrações financeiras, com objetivo de evidenciar alterações significativas nas demonstrações.

Como mencionado anteriormente, cabe aos executivos a responsabilização pela qualidade das informações contábeis e financeiras disponibilizadas ao mercado de capitais. Em sua seção 302, a Lei SOX impõe aos diretores executivos e financeiros das organizações a responsabilidade de declarar: (i) a ação realizada de revisão dos relatórios financeiros; (ii) a não existência de relatórios com informações incorretas e omissas em fatos materiais; e (iii) que as informações financeiras do relatório representem a condição financeira da empresa no período.

Os executivos devem se declarar responsáveis pelo estabelecimento e manutenção da estrutura de controles internos, reportando ao Comitê de Auditoria e à Auditoria Externa, as deficiências e franquezas materiais significativas encontradas nos controles internos.

A fim de que possam assinar tais declarações, os executivos precisam adquirir como suporte, uma sólida estrutura de controles internos. Na seção 404, a SOX determina que a organização deve avaliar os controles internos quanto à sua eficácia.

Grumet (2007) atribui à lei SOX o crescimento da confiança dos investidores, o fortalecimento da responsabilidade corporativa e a transparência.

Em seus estudos, Silva (2012) comenta que alguns pesquisadores afirmam que a SOX estabeleceu uma maior demanda para a auditoria contínua facilitando a avaliação global e testes dos controles internos sobre os relatórios financeiros. No entanto, muitas organizações vêm reclamando das numerosas exigências da Lei

SOX, seja pelo excesso de documentação e testes dos controles internos (Patterson e Smith, 2007), seja pelos custos de adequação à Lei (Bedard et al., 2007; Graziano e Sinnett, 2007). Apesar dessas afirmativas, Leuz (2007) não encontrou evidências de custos elevados para a adequação da Lei.

Atualmente, a avaliação quanto à eficácia de controles internos ocupa grande parte do tempo de trabalho dos auditores, em cumprimento às exigências da Lei SOX (Lelis, 2010). Além disso, atualmente muitas áreas de auditorias realizam atividades relacionadas às exigências da Lei SOX que incluem o apoio consultivo às áreas responsáveis pelos controles na elaboração de planos de ação para solução de hiatos entre a estrutura de controles existente e a demandada pela lei norte-americana.

Outros autores como Sarens (2009) e De Beelde (2006) destacam a função de monitoramento e a melhoria dos processos de gestão de risco e controles internos, que se tornam uma importante contribuição da auditoria interna para a governança corporativa, no intuito de redução do conflito de agência.

2.4. Metodologias de auditoria interna

As profundas mudanças ocorridas no ambiente de negócios para suporte e funcionamento das operações em uma organização, forçaram por sua vez a evolução dos processos de auditagem, seja pela criação de complexos sistemas de informação ou pela qualificação de colaboradores.

Segundo Gonçalves (2008), as metodologias podem ser classificadas como:

- auditoria baseada em controles (*control-based audit*): função de garantir o cumprimento da legislação e regulamentos aplicáveis, tais como normativos contábeis, fiscais e setoriais;
- auditoria baseada em processos (*process-based audit*): com ênfase nos controles operacionais críticos ao negócio;
- auditoria baseada em risco (*risk-based audit*): o auditor assume a responsabilidade de deter o conhecimento da organização e sua atividade, assim como do seu sistema de controle interno;
- auditoria baseada na gestão de risco empresarial (*Enterprise Risk Management*): pretende alinhar os objetivos estratégicos, com os mecanismos de identificação de riscos pelos auditores internos, auditores externos e membros das comissões de auditoria ou órgãos com características semelhantes.

Até o início dos anos 80, as atividades de auditoria constituíam-se na análise e validação de documentos de balanço e transações, com respeito a normas e regulamentos específicos (*control-based audit)*. Essa abordagem foi alterada com a evolução dos sistemas de informação e aumento da complexidade operacional das organizações, que passaram a considerar a implementação de metodologias orientadas para a análise crítica de processos (*process-based audit).*

Com a situação de insolvência de algumas entidades americanas, durante a segunda metade da década de 80, algumas questões surgiram quanto ao aspecto das limitações do trabalho de auditagem que não previram tal problema, assim como o reconhecimento das limitações nas metodologias de gestão empregadas e como poderiam ultrapassá-las.

De acordo com Gonçalves (2008), a reflexão sobre essas duas questões importantes levaram à concepção de dois projetos com impactos observados ainda em nossos dias de hoje: o *Treadway Report* e o *Committee of Sponsoring Organizations*.

Sob o aspecto do controle interno nas organizações, foi publicado em 1987 o documento *Treadway Report*, que identificava a necessidade de implementação de um mesmo referencial para controles internos enfatizando os elementos chaves desse sistema. O documento também descrevia sobre a responsabilidade dos gestores em assumir a efetividade do funcionamento do sistema, reportando seus resultados a uma comissão de auditoria integrada por profissionais competentes e conhecedores da atividade.

Na sequência, o *Committee of Sponsoring Organizations* (COSO), formado por representantes e associações privadas da área de auditorias, elaborou um projeto específico sobre o controle interno em 1992, com o título "*Internal Control-Integrated Framework*".

Constava desse documento a proposição de um referencial comum a respeito da conceituação de um controle interno e procedimentos para sua avaliação.

A partir daí, o termo controle interno passou a ser aceito em sua forma conceitual proposta abaixo:

> "o controle interno consiste num processo concebido e desenhado pelos responsáveis da governança e gestão, assim como outros colaboradores, que visam fornecer garantias relativamente à capacidade da entidade em prosseguir em seus objetivos nas seguintes áreas: (i) eficiência operacional; (ii) confiabilidade do relato financeiro; e (iii) cumprimento da legislação e regulamentos aplicáveis" (COSO, 1992).

Esse novo conceito de controle interno, juntamente com os aspectos da contabilidade das operações, alterou a metodologia dos processos de auditoria interna nas organizações, enfatizando-se sua relevância na avaliação de riscos (*based risk audit*), como segue:

- pela garantia de solvência e liquidação de ativos e passivos em suas operações;
- pelos riscos do negócio devido a natureza da atividade exercida;
- pelas deficiências em seu próprio sistema de controle interno (risco do controle);
- pela não identificação de eventuais falhas do sistema de controle interno devido a um não adequado planejamento do processo de auditoria (risco de detecção).

Com a crescente importância do desenvolvimento e aprimoramento desses controles internos, outras iniciativas foram sendo propostas. Um desses exemplos foi a publicação do artigo de Kaplan e Norton (1992), intitulado "*The Balanced Scorecard: measures that drive performance*" pela *Harvard Business Review* no início dos anos 90.

O artigo dispunha de uma pesquisa que demonstrava o grau de insatisfação de multinacionais americanas com o então presente método baseado em indicadores contábeis e financeiros, que prejudicavam a geração de valor das organizações a médio e longo prazo.

A fundamentação desse artigo iria dar origem mais tarde ao *Balanced Scorecard* da forma como se conhece hoje, o qual dá o enfoque na gestão estratégica da organização, traçando objetivos, iniciativas e indicadores em quatro dimensões: (i) financeira; (ii) clientes; (iii) processos internos; e (iv) crescimento e aprendizado organizacional.

No entanto, não obstante as iniciativas evolutivas dos controles internos e sistemas, outra crise seria necessária para que o conceito de alinhamento da estratégia com a estrutura de ambiente de controle interno tivesse o reconhecimento da necessidade de sua forma sistematizada e integrada (Gonçalves, 2008).

A crise de confiança que se abateu entre as organizações e os investidores, após constatações de fraudes contábeis a exemplo das ocorridas na empresa Enron (2001), foram uma das razões principais da criação da Lei SOX, como resposta do governo americano para esse conflito.

Como abordado na seção anterior deste capítulo, dentre as diversas ações advindas desta Lei, a questão dos controles internos passou a ser de importância fundamental para constituição de relatórios de qualidade aos investidores.

Um sistema eficaz de controles internos contribui com a fidelidade e segurança nas informações, resguardando os interesses da empresa. Permite ainda, a observação e previsão dos eventos que se apresentam dentro da empresa e que produzem reflexos em seu patrimônio, assim minimizando em grande escala os custos e a quantidade de trabalho gasto no processo de adequação as exigências da Lei SOX (Henrique, 2007).

No contexto atual de gestão de riscos e controles internos nas empresas, uma estratégia que vem sendo amplamente utilizada é a de implantar ou aprimorar os controles internos com base na identificação e mensuração dos riscos corporativos. É possível considerar a existência de duas abordagens de mensuração de riscos – a qualitativa e a quantitativa.

Pela abordagem qualitativa, o nível de risco é avaliado a partir da atribuição de critérios de classificação à probabilidade de ocorrência e ao impacto (impacto financeiro e outros). Uma das técnicas empregadas para avaliação qualitativa de riscos é o processo de auto-avaliação conhecido como *Control Self Assessment* (CSA), que consiste em avaliar, de maneira descentralizada e contínua, a efetividade dos controles e a potencialidade (probabilidade de ocorrência *versus* impacto) dos riscos, possibilitando a detecção de exposições indesejadas e a implantação de medidas preventivas e corretivas.

A adoção dessas ferramentas tem gerado bons resultados no que se refere à: (i) identificação dos eventos (riscos ou oportunidades) que podem afetar as atividades empresariais; (ii) avaliação dos níveis de exposição; e (iii) definição de planos de melhoria que conduzam a empresa a um ambiente de controle adequado.

No entanto, é necessário evitar que os controles em operação estejam aquém do necessário ou que se configure um dispêndio excessivo para controlar riscos que não representem um potencial de perda relevante. Trata-se, portanto, de um problema de otimização da relação entre o nível de controle desejado e os custos dos controles necessários.

Buscando equacionar esse problema de otimização o *Committee of Sponsoring Organizations of the Treadway* (COSO) desenvolveu uma metodologia de avaliação baseada na relação custo/benefício associada a cada

alternativa de controle.

A metodologia proposta nesta dissertação para estabelecimento e hierarquização de regras de monitoramento contínuo associadas a eventos de risco baseia-se fundamentalmente no modelo conceitual do COSO, mais especificamente em sua versão mais recente – o COSO ERM (ver capítulo 4).

Esse modelo foi o escolhido para fins do desenvolvimento da metodologia proposta no capítulo 4, porque desde sua criação tornou-se referência para empresas e outras organizações avaliarem e aperfeiçoarem seus sistemas de controle interno. Sua estrutura analítica vem sendo incorporada na formulação de políticas públicas e em normas e regulamentos adotados por milhares de organizações em todo o mundo.

O modelo '*Enterprise Risk Management – Integrated Framework'* (COSO ERM) é aplicável a qualquer área de negócio e provê orientações para a investigação da origem dos riscos, permitindo monitorar suas causas e providenciar a mitigação.

Pela sua importância para a presente pesquisa, dedica-se a seção seguinte aos fundamentos do modelo conceitual COSO ERM ou COSO II.

2.5. Auditoria baseada em gestão de risco: o modelo conceitual COSO ERM

Define-se gestão de riscos corporativos como o processo de identificação e análise dos riscos associados ao não cumprimento das metas e objetivos operacionais, de informação e de conformidade, formando uma base de conhecimento que permita definir como esses riscos deverão ser gerenciados.

Segundo o modelo COSO ERM, o processo de gestão de riscos compreende oito componentes inter-relacionados que servem de critério para determinar se a gestão de riscos na empresa é eficaz ou não. A gestão de riscos corporativos requer:

- alinhar o apetite a risco e a estratégia;
- otimizar as decisões de resposta a risco;
- reduzir surpresas e prejuízos operacionais;
- identificar e administrar os riscos inerentes aos empreendimentos;
- fornecer respostas integradas aos diversos riscos;
- aproveitar as oportunidades;

- melhorar a alocação de capital.

Os administradores devem definir os níveis de riscos operacionais, de informação e conformidade que estão dispostos a assumir. A avaliação de riscos é uma responsabilidade da alta administração, mas cabe à área de Auditoria Interna fazer uma avaliação própria dos riscos. A identificação e a gestão de riscos corporativos são, portanto, ações proativas.

2.5.1. Componentes da gestão de riscos corporativos

Os oito componentes da gestão de riscos corporativos são: (i)ambiente interno; (ii) fixação de objetivos; (iii) identificação de eventos; (iv) avaliação de riscos; (v) resposta a risco; (vi) atividades de controle; (vii) informações e comunicações; e (viii) monitoramento.

No Quadro 2.1, a seguir, definem-se os oito componentes apresentados na matriz tridimensional como representado adiante na Figura 2.2, mostrada adiante.

Quadro 2.1 - Componentes da gestão de riscos corporativos segundo o modelo COSO ERM

Componente	**Definição**
Ambiente interno	O ambiente interno determina a forma como os riscos e os controles serão abordados pela organização. Atributos individuais dos participantes da organização como a integridade, os valores éticos e a competência fazem parte do ambiente interno.
Definição dos objetivos	Os objetivos devem ser definidos pela administração antes que as situações com potencialidades para prejudicar sua realização sejam identificadas. Uma adequada gestão de riscos pressupõe que a administração estabeleça objetivos alinhados com a missão da organização e compatíveis com o apetite a risco.
Identificação de eventos	Os eventos externos e internos com potencialidade para afetar o cumprimento dos objetivos da empresa devem ser identificados e classificados como riscos, oportunidades, ou ambos.
Avaliação dos riscos	Os riscos identificados na etapa anterior são analisados e associados aos objetivos e processos que podem influenciar. Avaliam-se os riscos considerando-se seus efeitos inerentes e residuais, bem como sua probabilidade de ocorrer e seu impacto.
Respostas aos riscos	Identificam-se e avaliam-se as possíveis respostas aos riscos: evitar, aceitar, reduzir ou compartilhar. Seleciona-se o conjunto de ações destinadas a alinhar os riscos às respectivas tolerâncias e apetite.
Atividades de controle	Estabelecem-se e implantam-se políticas e procedimentos para assegurar que as respostas aos riscos selecionados pela adminstração sejam executadas com eficácia.
Informação e comunicação	Para identificar, avaliar e responder ao risco, a empresa necessita de informações provenientes detodos os níveis hierárquicos. A comunicação eficaz ocorre quando as informações fluem na organização em todas as direções e quando os gestores e empregados recebem informações claras acerca de suas funções e responsabilidades.
Monitoramento	O monitoramento é realizado por meio de atividades gerenciais contínuas, avaliações independentes ou uma combinação desses dois procedimentos.

Fonte: COSO, 2004.

Nesse novo modelo, a premissa subjacente da gestão de riscos corporativos é a existência de um relacionamento direto entre os objetivos da empresa e os componentes da gestão de riscos – necessários para o alcance desses objetivos.

2.5.2. Relações entre objetivos empresariais e componentes de risco

As relações entre objetivos empresariais e os componentes de risco são apresentadas em uma matriz tridimensional em forma de cubo, como mostra a Figura 2.2.

As quatro categorias de objetivos (estratégicos, operacionais, de comunicação e conformidade) estão representadas nas colunas verticais. Os oito componentes nas linhas horizontais e a abrangência organizacional na terceira dimensão.

O cubo COSO ERM mostra a habilidade que uma organização tem para focar no gerenciamento de risco corporativo, podendo ser por categoria de objetivo, por componente da gestão de risco, por unidade de negócio ou por qualquer outro subconjunto.

Em razão da exigência de que a avaliação dos controles internos seja realizada com base em uma estrutura analítica reconhecidamente eficaz, esse modelo tornou-se referência para as empresas que estejam passando por processos de reestruturação ou de adaptação de seus ambientes de controle para atender às novas demandas regulatórias e de sustentabilidade.

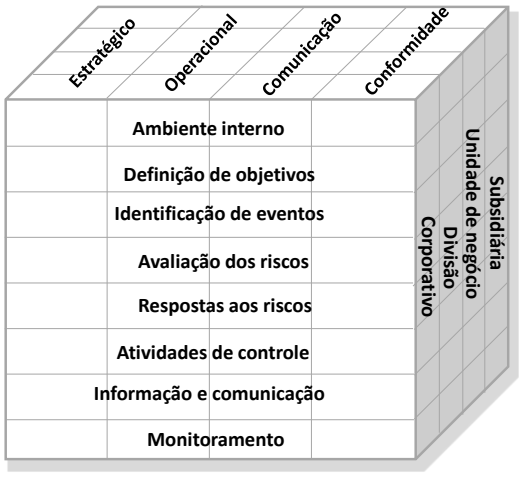

Figura 2.2 - Matriz tridimensional COSO ERM (COSO II)
Fonte: COSO, 2004.

Da mesma forma como representado no cubo da Figura 2.2, com base na

missão uma vez estabelecida, a administração define os principais objetivos, selecionando as estratégias e planos a serem seguidos e compartilhados por toda a organização.

Por exemplo, os objetivos comuns a praticamente todas as entidades são alcançar e manter uma reputação favorável tanto no segmento empresarial quanto com seus clientes, fornecer informações confiáveis às partes interessadas e operar em conformidade com as leis e a regulamentação.

Assim, dentro desse raciocínio, pode-se classificar um processo de gestão de riscos, em quatro categorias de objetivos descritas no Quadro 2.2, a seguir:

Os objetivos na gestão de risco aparecem no topo do cubo da Figura 2.2 e se inter-relacionam aos processos de gestão de risco de uma organização.

Ainda dentro desse contexto, cabe destacar o papel crescente da influência dos meios de comunicação, novas tecnologias e metodologias, que em cenário futuro, exigirão dos auditores internos maior qualidade e assertividade no fornecimento de seus resultados (Madeira, 2010).

Quadro 2.2 - Categorias de objetivos na gestão de riscos

Objetivos na Gestão de Risco	**Definição conforme COSO (2013)**
Estratégico	Referem-se às metas no nível mais elevado. Alinham-se e fornecem apoio à missão.
Operacional	Têm como meta a utilização eficaz e eficiente dos recursos.
Comunicação	Relacionados à confiabilidade dos relatórios.
Conformidade	Fundamentam-se no cumprimento das leis e dos regulamentos pertinentes.

Fonte: COSO (2004).

Tal afirmativa é corroborada pelo *Institute of Internal Auditors*, que em 1996, apresentou algumas tendências futuras sobre o perfil dos novos auditores internos, conforme destacado a seguir:

- preocupação com a segurança dos dados da organização;
- crescente complexidade nos negócios, com maior rigidez nos princípios, regulamentações e culturas presentes.
- crescimento da competição e consequentemente aumento da pressão para que as auditorias internas sejam mais produtivas;
- a modernização dos processos está forçará a uma remodelagem dos relacionamentos, responsabilidades gerenciais e estruturas hierárquicas tradicionais;

- o reconhecimento de que os auditores internos são um valioso recurso para a mudança e sucesso da empresa no futuro.

2.6. Governança coorporativa

Na primeira metade dos anos 90, acionistas americanos perceberam a necessidade de criação de novas regras que os protegessem dos abusos da diretoria executiva das empresas, de conselhos de administração não eficientes ou não atuantes e das omissões das auditorias externas.

Desta forma o conceito de governança corporativa surgiu para superar o "conflito de agência", decorrente do distanciamento entre a propriedade e a gestão empresarial. Nesta situação, o proprietário (acionista) delega a um agente especializado (executivo) o poder de decisão sobre sua propriedade. Contudo, os interesses desse gestor nem sempre estão alinhados com os do proprietário, resultando em um conflito de agência ou conflito agente-principal.

O atributo da governança corporativa é estabelecer um eficiente conjunto de mecanismos, tanto de incentivos quanto de monitoramento, de forma a garantir com o que o comportamento dos executivos esteja conforme os interesses dos acionistas (Instituto Brasileiro de Governança Corporativa - IBGC, 2013).

Conceitualmente, o IBGC (2010) define como governança corporativa:

> "...é o sistema pelo qual as organizações são dirigidas, monitoradas e incentivadas, envolvendo os relacionamentos entre proprietários, Conselho de Administração, Diretoria e órgãos de controle. As boas praticas de Governança Corporativa convertem princípios em recomendações objetivas, alinhando interesses com a finalidade de preservar e otimizar o valor da organização, facilitando seu acesso a recursos e contribuindo para sua longevidade."

2.6.1. Princípios básicos da governança coorporativa

Apresentam-se, a seguir, os princípios básicos da governança coorporativa: (i) transparência; (ii) equidade; (iii) prestação de contas (*accountability*); e (iv) responsabilidade corporativa.

Transparência

Obrigação de informar às partes interessadas, as informações que sejam de seu interesse e não somente aquelas impostas por disposições de leis ou regulamentos. Tais informações não devem ser somente quanto às questões de desempenho econômico-financeiro, mas incluir também os demais fatores

(inclusive intangíveis) que norteiam a ação gerencial e que agregam valor.

Equidade

É caracterizada pelo tratamento justo de todos os sócios e demais partes interessadas (*stakeholders*). Atitudes ou políticas discriminatórias são totalmente inaceitáveis.

Prestação de contas (*accountability)*

Os agentes de governança (sócios, conselheiros de administração e executivos/gestores, conselheiros fiscais e auditores) devem prestar contas de suas ações, assumindo a totalidade das consequências de seus atos e omissões.

Responsabilidade corporativa

Atribui-se aos agentes de governança o zelo em detrimento da sustentabilidade das organizações, de forma a manter sua longevidade, incorporando conceitos ambientais e de ordem social na organização.

2.6.2. Modelos de governança corporativa

Hawley e Williams (1996, *apud* Lélis, 2010) fundamentam a discussão sobre a governança corporativa em quatro modelos: (i) financeiro; (ii) *stakeholders*; (iii) procuradoria; e (iv) político.

Sob a perspectiva do modelo financeiro, cabe à governança corporativa desenvolver sistemas de controles adequados que garantam que os recursos empresariais dispostos sejam aplicados de forma eficiente e eficaz na missão, objetivos e metas da organização (Martin, Santos e Dias Filho, 2004).

Os mesmos autores sugerem ainda que o exercício de poder da governança corporativa está importantemente atrelado a um sistema de controle de riscos que identifique e avalie seus impactos, cabendo inclusive à própria governança, dotar a administração de recursos para implementação de um sistema de controle e gestão.

Conforme embasado por Silveira (2004), a teoria do conflito de agência é definida por um conjunto de atributos e mecanismos internos e externos que alinham interesses entre agentes da administração e investidores, no aumento das probabilidades desses últimos, na garantia de remuneração de seus recursos aplicados. Dessa forma, os mecanismos de governança corporativa provém o alinhamento dos contratos que vigoram dentro da organização.

Já o modelo dos *stakeholders* reconhece a empresa como um sistema de públicos relevantes que, segundo Clarkson (1995), reivindicam interesses na firma e são de grande importância para a sobrevivência da organização ao longo do tempo.

A procuradoria considera a motivação de administradores através de responsabilidades e metas, em prol do interesse dos proprietários.

Já no modelo político, o contexto organizacional e as políticas públicas interferem na denominação de poder dentro das organizações, assim como a distribuição de lucros entre os agentes, proprietários e demais *stakeholders*.

2.7. Auditoria contínua

Como visto anteriormente, a auditoria nasceu da necessidade de conferência de documentos contábeis e financeiros. Leitch e Chen (2003, *apud* Silva, 2012) salientam que os auditores antigamente conferiam todos os procedimentos de escrituração dos livros financeiros e contábeis. Com a evolução dos processos e métodos para modelos estatísticos de amostragem, a atividade do auditor passou a gerar hipóteses assertivas, eliminando os erros de uma análise embasada em procedimentos analíticos.

Com a evolução tecnológica de processos informatizados, surgiram novos métodos automáticos que deram suporte à eficiência e à qualidade das análises do auditor dentro das organizações. Emerge assim, com esse novo formato, o pensamento da automação da auditoria e com ele o conceito de auditoria contínua (Silva, 2012).

Esse novo conceito pode ser considerado complementar à auditoria tradicional que, segundo Moeler (2004) é:

> "... o processo de instalar monitores baseados em controle nos sistemas automatizados de forma que enviem sinais para auditores – usualmente auditores internos – quando o processo automatizado acusa desvio de limites ou parâmetros definidos pela auditoria".

Vasarhelyi (1991) e Heffes (2006) destacam que a auditoria contínua em conjunto com a auditoria tradicional, permite a produção de resultados em curto tempo, possibilitando ainda, o relato de alterações nos controles em tempo real.

Segundo a visão de Silva (2012), a auditoria contínua relaciona-se à disponibilidade de dados em tempo real, na medida do possível. Nas suas palavras:

> "... relacionada com a disponibilidade de dados mais próximos de um evento, se possível em

tempo real, com capacidade de serem processados e correlacionados em um ambiente computadorizado seguro, que traga informações eletrônicas fidedignas, que serão tratadas pelos auditores e gestores da organização".

Segundo Vasarhelyi e Halper (1991):

"...é uma metodologia usada para monitorar analiticamente processos corporativos de negócios, aproveitando a automação e integração dos processos e da tecnologia da informação".

De acordo com Yu, Yu, e Chou (2000):

"...compreende as funções do processo de auditoria periódica, usando um sistema de supervisão de transações em tempo real, com *software* que monitora continuamente as transações e compara as suas características com os resultados esperados".

Conforme Rezaee et al. (2002):

"um processo de auditoria eletrônica que permite aos auditores prover certo grau de garantia contínua de forma simultânea com a informação gerada ou em um curto período após a informação ser gerada".

Groomer e Murthy (2004) definem como:

"...é um método que permite a auditores prover opinião sobre um objeto usando uma série de relatórios emitidos simultaneamente, em um período curto de tempo, após a ocorrência de um evento importante".

E, finalmente, de acordo com Coderre (2005):

"...é uma metodologia para emissão de relatórios simultâneos ou em um curto período de tempo, após a ocorrência de um evento relevante".

Para fins da presente dissertação, adota-se o conceito de Moeler (2004), complementado pela definição de Yu, Yu, e Chou (2000).

2.7.1. Estudos sobre auditoria contínua

Diversas abordagens têm sido exploradas pelos pesquisadores no intuito de enquadrar e analisar a evolução da auditoria contínua para os próximos anos.

Nesse sentido, em destaque, Costa (2012) reuniu uma série de recentes estudos com suas respectivas contribuições, que permitiu classificá-los nos seguintes grupos: (i) revisões bibliográficas; (ii) estudos exploratórios; e (iii) estudos empíricos.

Revisões bibliográficas

Dentro da linha de estudos dirigidos à revisão bibliográfica, Costa (2012) cita os trabalhos de Chan e Vasarhelyi (2011); Kanellou e Spathis (2011); Kuhn e Sutton (2010); Murcia et al. (2008); Lin et al. (2010); e Alles, Kogan e Vassarhelyi

(2008).

Chan e Vasarhelyi (2011) recomendam: (i) definir de que forma a inovação contínua contribui para as inovações práticas na auditoria tradicional; (ii) uma sugestão de um padrão a ser seguido de quatro fases para futuros estudos em auditoria contínua; e (iii) um conjunto de métodos para profissionais e investigadores acadêmicos.

Kanellou e Spathis (2011) entendem que os sistemas integrados de gestão empresarial ou *Enterprise Ressource Planning (ERP)* levaram aos avanços da auditoria contínua e à necessidade de alteração de procedimentos dos auditores financeiros no que diz respeito aos controles internos;

Kuhn e Sutton (2010) ressaltam que o enfoque de pesquisas recentemente realizadas a partir do surgimento dos sistemas ERP estão direcionadas para as limitações, vantagens e viabilização da auditoria contínua em duas abordagens: (i) no módulo de auditoria incorporado e responsável por monitorar atividades eletrônicas (*EAM - Embedded Audit Module*); e (ii) no módulo de controle externo, que funciona independente do sistema regular de monitoração, utilizando a base de dados (*MCL - Monitoring Control Layer*).

Os trabalhos de Murcia et al.(2008) e de Lin et al. (2010) apresentam o estado da arte na auditoria contínua. Murcia et al.(2008) evidenciaram que a maioria da literatura emitida sobre este tema não são empíricos. Em uma amostragem de 57 trabalhos deste universo, apenas um deles foi focado em estudo de caso particular sobre a empresa Siemens. No universo dos estudos não empíricos, 50% adotavam uma abordagem conceitual de modelos teóricos de auditoria contínua.

Já Lin et al. (2010) abordaram de forma diferente o estado da arte sobre o tema. Procuraram observar se havia amadurecimento suficiente da tecnologia da informação para suporte amplo à auditoria contínua. Seu estudo apontou para a necessidade do aprofundamento da investigação da operação, portabilidade e confiança nos quesitos de tecnologia de *middleware* (ferramenta de programa responsável por mediar a relação entre os software e as aplicações do sistema). Enfatizou ainda, a necessidade de desenvolver novas ferramentas amigáveis e de inteligência no auxílio aos auditores no cumprimento às normas e em respeito à política de controles internos.

Alles, Kogan e Vassarhelyi (2008) chamam a atenção para a crescente

demanda de boa parte dos profissionais do ramo e investidores para a necessidade de informações em tempo real, impulsionando as argumentativas de se intensificar a atuação da auditoria contínua.

Estudos exploratórios

Em continuação aos estudos classificados por Costa (2011), os de aspectos exploratórios são destacados por Alles, Kogan e Vasarhelyi (2011) e Santos et al. (2008).

Amplamente aplicado à área de auditoria contínua, o estudo de Alles, Kogan e Vasarhelyi (2011) sugere uma híbrida metodologia colaborativa entre entidades de pesquisa empresarial e parceiros da indústria, a qual denominaram *Collaborative Design Research* (CDR). Consideram a auditoria contínua como uma área emergente e que seus processos estão sendo amadurecidos em colaboração com o meio acadêmico e nos departamentos de auditoria interna das organizações, levando a uma abordagem de combinação entre o teórico e o prático.

Santos et al. (2008) sugerem que os mecanismos de um sistema de controle estejam incorporados aos processos operacionais, visando à execução de processos de auditoria contínua em tempo real. Dessa forma, os objetivos desejados seriam constantemente comparados com o comportamento dos processos de negócio, permitindo aos auditores trabalharem nas exceções, corrigindo-as em tempo real ou alterando os perfis de riscos previamente definidos.

Estudos empíricos

Costa (2011) ressalta a existência de poucos estudos desta última categoria, com destaque para os trabalhos de Omotesco, Patel e Scott (2008); El-Marsy e Rack (2008) e Masli et al. (2010).

Omotesco, Patel e Scott (2008) analisaram os possíveis impactos da auditoria contínua em tempo real no Reino Unido, sob a ótica de suas vantagens e desvantagens e principalmente sua importância para o futuro. Em síntese, concluíram se tratar de matéria controversa, porém com a necessidade de redefinições importantes de competências do futuro profissional e suas respectivas empresas atuantes no mercado de auditagem.

El-Marsy e Rack (2008) procuraram entender as perspectivas de riscos de uma empresa na visão dos investidores na contribuição da auditoria contínua nesta percepção, em dois momentos: (i) se as auditorias contínuas em tempo real são

impactantes na percepção de riscos pelos investidores; e (ii) se esse mesmo impacto de percepção dos investidores do item anterior se aprofunda com a adição da componente da Lei Sarbanes-Oxley. A conclusão que chegaram é que os investidores percebem uma redução dos riscos em ambas situações.

Masli et al. (2010) buscaram determinar os benefícios potenciais das empresas que aplicam a tecnologia de acompanhamento de seus controles internos após a exigência da lei Sarbanes-Oxley.

Em síntese, a necessidade em cumprir obrigações cada vez mais impositivas por controles internos eficazes, segurança em ambientes, tecnologia e regulamentação, obrigarão as organizações a direcionarem sua procura por auditoria contínua. Em consequência, esse novo ambiente exigirá uma maior especialização de auditores e construção de processo.

2.7.2. Auditoria contínua *versus* auditoria tradicional

De uma maneira geral, alguns autores apresentam a argumentação de que a auditora contínua seja uma transformação tecnológica da auditoria tradicional interna e externa (Alles et al., 2006; Chan e Vasarhelyi, 2011).

Vasarhelyi (2004), apud Costa (2012), atribui que as bases de construção gradativa da atual auditoria contínua estão fundamentadas em sistemas ERP nas organizações, que por sua vez carregam a herança das características de monitoração analítica continuada.

Dessa forma, como evidenciado por Kuhn e Sutton (2010), a auditoria contínua evolui e se expande em escopo e abrangência ao longo do tempo, em um território inexplorado.

Brown et al. (2007), *apud* Costa (2012), diferencia a auditoria contínua em relação à auditoria tradicional pela aplicação técnica da auditoria, conforme destaca: (i) mais frequentemente aplicada com resultados relevantes em momento exato.; (ii) procedimentos automáticos de baixo custo; e (iii) análises complexas com uso de ferramentas que podem ser melhoradas com uso de inteligência artificial.

De uma forma genérica, Silva (2012) identifica as fases dos modelos de auditoria tradicional e contínua como sendo as mesmas, a saber: (i) planejamento; (ii) avaliação do controle interno; (iii) execução de testes; e (iv) comunicação.

Segundo Silva, no planejamento das atividades manuais e automáticas, o sistema de auditoria deve realizar testes de controle e transações que garantam que os dados estão confiáveis em uma base de tempo contínuo.

Em outras palavras uma vez que a transação é testada, seus controles serão igualmente testados e incorporados aos procedimentos de auditoria. E, uma vez estabelecidos os procedimentos de auditoria contínua, os auditores necessitarão de relatórios de exceção definidos, que podem ser por meio de alarmes durante o processo contínuo da atividade.

Green e Trotman (2003), *apud* Silva (2012), destacam que a utilização de critérios estatísticos e indicadores habilitarão o auditor realizar sua tarefa com melhor entendimento e julgamento.

Corroborando a ideia de que a auditoria contínua é uma evolução da tradicional, Chan e Vasarhelyi (2011, *apud* Costa, 2012), apresentam uma abordagem de sete dimensões básicas para implementação de sistemas de auditoria, que permitam a segurança em tempo real de controles operacionais e de contabilidade. Tal abordagem encontra-se em destaque na Figura 2.3 abaixo.

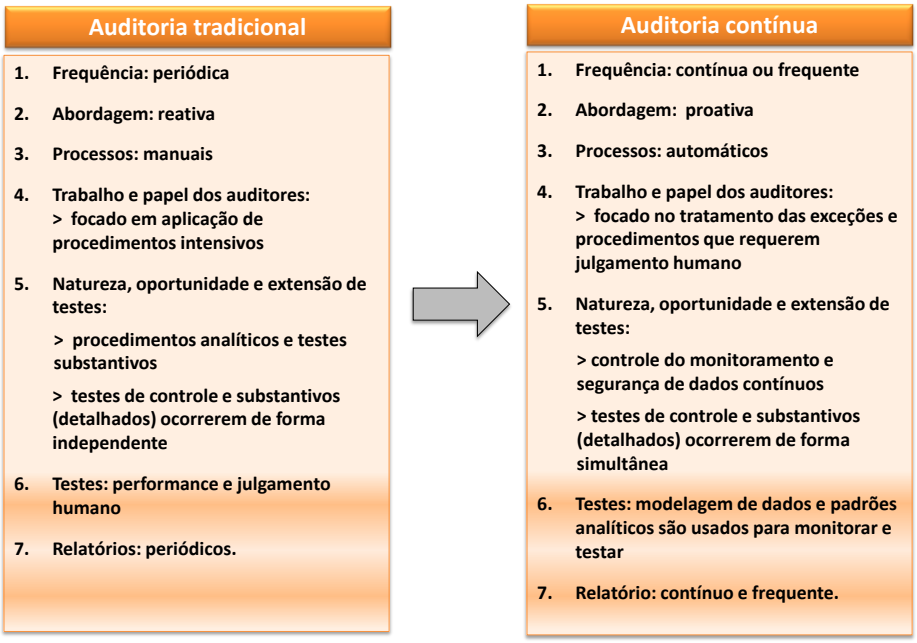

Figura 2.3 - Dimensões básicas para implementação de auditoria contínua
Fonte: Chan e Vasarhelyi (2011) *apud* Costa (2012).

Conforme Silva (2012), tecnologias mais avançadas serão necessárias às metodologias de auditoria interna em um contexto de auditoria contínua.

A auditoria com base em análises periódicas deverá evoluir a um novo

modelo que incorpore softwares específicos de auditoria que testam os controles e as operações em base contínua.

Com esta evolução, ferramentas de auditoria serão capazes de tratar simultaneamente tanto dados auditáveis de controles internos, quanto das operações, sendo capazes ainda de realizar testes analíticos rigorosos em modelos de negócios estimados e estratégicos à alta administração (Silva, 2012). Outra grande vantagem do uso de ferramentas de auditoria é o cumprimento às exigências da Lei Sarbanes-Oxley em termos de transparência de informações e avaliação de eficácia dos controles internos.

2.7.3. Níveis de auditoria contínua: OLA, DLA e PLA

Segundo Silva (2012), novas preocupações foram surgindo com a evolução da tecnologia e transformação das organizações, motivando o desenvolvimento de uma auditoria em tempo real e próxima do evento de origem. A necessidade de cumprir com as obrigações da Lei SOX fez aumentar ainda mais o grau dessa preocupação.

Nesse sentido, Vasarhelyi e Alles (2008, *apud* Silva, 2012), observam a importância na criação de novos métodos de integração dos fluxos de informação a três níveis de assertividade: (i) *Opinion Level Assurance* (OLA) ou garantia do nível do parecer; (ii) *Data Level Assurance* (DLA) ou garantia do nível de dados; e (iii) *Process Level Assurance* (PLA) ou garantia do nível de processo.

Opinion Level Assurance (OLA) ou garantia do nível do parecer

Trata-se da auditoria tradicional junto com as aplicações da auditoria contínua que suporta informações e pareceres anuais financeiros da organização, garantindo que não há erros materiais no relatório apresentado. Esse parecer pode indicar erros de compensação de nível material, no entanto o resultado não interfere na decisão do investidor.

Data Level Assurance (DLA) ou garantia do nível de dados

A evolução das fontes de dados e sua pulverização fazem emergir algumas situações de não precisão de dados em diferentes níveis. Como por exemplo, trazendo essa análise para o domínio financeiro, pode-se afirmar que a medida do valor de caixa muitas vezes é mais precisa do que os dados de inventário ou itens

intangíveis, que podem apresentar ainda diferenças entre um armazém local e um central. Frente a este desafio, novas ferramentas de dados deverão ser desenvolvidas e o auditor responsável deverá ser capaz de opinar sobre a qualidade e integridade de tais dados.

Process Level Assurance (PLA) ou garantia do nível de processo

O nível PLA focaliza um processo específico ou subprocesso interno da cadeia de valor da organização, mesmo que este tenha sido terceirizado. Assim com OLA, o nível PLA emitirá um parecer de auditoria com referência aos processos que servirá de suporte para auditorias contínuas. Somente para efeitos de comparação, cabe destacar que o nível PLA gera um parecer por um processo específico, enquanto o nível OLA emite um parecer englobando todos os processos que suportam os relatórios contábeis e financeiros.

2.8. Considerações finais sobre a adoção da auditoria contínua baseada em gestão de risco

As crises financeiras que se sucederam no mundo intensificaram a necessidade de aprimoramento de metodologias eficazes na mitigação de riscos e restabelecimento da confiança entre agentes da organização e investidores. Abordaram-se neste capítulo o ‘endurecimento’ de leis e, principalmente, o aprimoramento de ferramentas de controle interno que redefiniram as funções e responsabilidades dos administradores no âmbito das organizações.

De maneira abrangente e observando as referências históricas na formação conceitual e ferramental da gestão de riscos, Macieira (2008) reúne nos Quadros 2.3 e 2.4, as metodologias de referência de gestão de risco e legislação associada à auditoria baseada em gestão de risco, respectivamente.

Como apresentado e evidenciado por Macieira (2010), há uma significativa base de metodologias e processos consagrados que vêm amadurecendo e contribuindo para identificação, avaliação, tratamento e monitoração de riscos e fraudes.

O emprego da utilização da gestão de risco, juntamente com várias técnicas de identificação e a avaliação de riscos, não apenas torna mais acessível ao estabelecimento dos controles internos, mas alinha o debate para a importância de que os mecanismos de governança corporativa não impeçam o desenvolvimento

dos negócios. Como evidenciado pelos autores Spira e Page (2003):

> "...a redefinição do controle interno como gestão de risco enfatiza sua relação com a formulação da estratégia e caracteriza o controle interno como um suporte à organização".

Quadro 2.3 - Metodologias de referência e boas práticas em gestão de risco

Metodologia de referência	**Ano**	**Descrição geral**	**Autor**
COSO Internal Control Integrated Framewok	1992	Uma das principais metodologias existentes e aplicadas ainda hoje para controles internos a partir de cinco componentes centrais: ambiente de controle; avaliação de risco; atividades de controle; informação e comunicação e monitoração	*COSO – Committee of Sponsoring organizations of the Treadway Commission*
FSA Handbook	2001	*Handbook* online completo com orientações e boas práticas para instituições financeiras. Permite personalização de conteúdo conforme características da organização	*FSA - Financial Services Authority. Órgão regulador de instituições financeiras no Reino Unido*
FERMA	2002	Cartilha que difunde a gestão de riscos na Europa a partir da perspectiva do processo de gestão de riscos. Apresenta um conjunto de *templates* para descrição e análise de riscos.	*FERMA – Federation of European Risk Managers Association*
AS/NZS 4360	1995 (1a versão) 2004 (última versão)	Uma das importantes referências para processos de gestão de riscos no mundo. Apresenta um conjunto de *templates* e práticas de gestão de riscos sob a perspectiva de processos em uma organização ou até mesmo individualmente para pessoas.	*Standards Australia e Standards New Zealand*
COSO Enterprise Risk Management – Integrated Framewok	2004	Esta metodologia amplia o conceito de *COSO Internal Contro*l, de forma a maximizar o valor gerado pela gestão de riscos em conformidade com a estratégia da organização. Este manual apresenta os conceitos de apetite de riscos e visão integrado de riscos (ERM).	*COSO – Committee of Sponsoring Organizations of the Treadway Commission*
Orange Book	2004	Abordagem de gestão de riscos e de que forma esta se subdivide em vários níveis de uma organização, desde o planejamento estratégico, até suas operações específicas.	*Her Majesty's Treasury* - Ministério econômico e financeiro do Reino Unido
Best practices inqualitative operational risk management	2006	Prático *handbook* para a gestão de riscos operacionais baseado na melhores práticas reais em instituições financeiras e na estrutura do *COSO Enterprise Risk Management – Integrated Framewok.*	*TransConstelation*.- Associação de empresas da área de processamento de transações financeiras

Quadro 2.3 - Metodologias de referência e boas práticas em gestão de risco (cont.)

Metodologia de referência	**Ano**	**Descrição geral**	**Autor**
Red Book	2007	Metodologia constituída de nove componentes para a implantação de um programa de integração de diversas iniciativas organizacionais de Governança, riscos e *compliance* (GRC). Cada componente é subdividido em outras diretrizes. Trata-se de um dos mais completos manuais em termos de Gestão de Riscos.	*OCEG – Open Compliance and Ethics Group*
BS 31100	2008	Este manual apresenta dez princípios-chaves para gestão de riscos: um modelo de gestão de riscos, um modelo de processo de gestão de riscos e um capítulo dedicado à implantação.	*BSI – British Standard Institution*
ISO 31000	2009	Trata dos aspectos positivos e negativos da ocorrência de um risco, e tem como objetivo fornecer princípios, guias e terminologias comuns para o gerenciamento de riscos, deforma a padronizar as metodologias já existentes.	*ISO – International organization for standardization*

Fonte: Adaptado de Macieira (2008)

O Quadro 2.4, a seguir, complementa o panorama de metodologias de referência e boas práticas em gestão de risco com um resumo da legislação associada à auditoria baseada em gestão de risco.

Quadro 2.4 – Legislação associada à auditoria baseada em gestão de risco

Legislação	**Ano**	**Descrição geral**	**Autor**
Basiléia II	2004	Desenvolvida por diversas empresas e instituições do setor financeiro com o objetivo de criar um padrão internacional de formulação de leis e regulamentos para a gestão de riscos em bancos. O documento é dividido em três pilares: requerimento mínimo de capital, processo de revisão para supervisão e disciplina de mercado. É um documento detalhado e muito embasado em ferramentas matemáticas não triviais.	*Basel Committee on Banking Supervision*
Sarbanes-Oxley Act	2002	Lei federal americana que estabelece a prática de controles internos em relatórios financeiros para todas as organizações com papéis na bolsa de Nova York. A Lei responsabiliza, civil e criminalmente, os principais executivos destas organizações pela confiabilidade das informações financeiros e contábeis disponibilizadas. Determina ainda que as organizações realizem autoavaliações dos seus sistemas de controle submetendo-os a auditoria independente.	*SEC - Security Exchange Comission*

Quadro 2.4 – Legislação associada à auditoria baseada em gestão de risco (cont.)

Legislação	**Ano**	**Descrição geral**	**Autor**
Financial Instruments and Exchange Act - J-SOX	2006	Versão japonesa da SOX.	Parlamento Japonês
Combined Code of Corporate Governance (Turnbull Cadbury Report)	1992 (1ª versão) 2005 (última versão)	Código de práticas de governança corporativa e controles internos sobre relatórios financeiros em organizações com papéis negociados na bolsa de Londres. As organizações devem demonstrar conformidade com a lei através da publicação de relatórios públicos. O código consiste da combinação de dois documentos: o *Cadbury Report*, que trata de governança corporativa e o *Turnbull Report* que aborda controles internos sobre relatórios financeiros.	*FRC - Financial Reporting Council*, Órgão regulador independente do Reino Unido responsável pela promoção da confiança nos relatórios e da governança corporativa
BSA (Bank Secrecy Act)	1970 (1ª versão) 2001 (última versão)	Determina a colaboração de todas as instituições financeiras norte americanas com o Governo objetivando a prevenção da lavagem de dinheiro	Governo Federal dos Estados Unidos
Resoluções do Banco Central Nº 2554, 3056, 3380 e 3490	2554 (1998); 3056 (2001); 3380 (2006); 3490 (2007).	Rege sobre a implementação de práticas de gestão de risco em instituições financeiras brasileiras: i) 2554 – implementação de um sistema de controles internos; ii) 3056 – Dispõe sobre a auditoria interna; iii) 3380 – Implementação de uma área de riscos operacionais; iv) 3490 – Trata da apuração do Patrimônio de Referência Exigido (capital econômico).	Banco Central do Brasil
Resoluções do Banco Central No 2554, 3056, 3380 e 3490	2554 - 1998; 3056 - 2001; 3380 - 2006; 3490 - 2007	Rege sobre a implementação de práticas de gestão de risco em instituições financeiras brasileiras: i) 2554 – implementação de um sistema de controles internos; ii) 3056 – Dispõe sobre a auditoria interna; iii) 3380 – Implementação de uma área de riscos operacionais; iv) 3490 – Trata da apuração do Patrimônio de Referência Exigido (capital econômico).	Banco Central do Brasil
Circular SUSEP 249, 280, 327	249 - 2004 280 - 2004 327 – 2006	Rege sobre a implementação de práticas de controles internos em seguradoras, através de circulares: i) 249 que dispões sobre a criação de uma estrutura de controle internos em uma seguradora; ii) 280 que estabelece os procedimentos mínimos associados aos controles internos e sobre o descumprimento de dispositivos legais e regulamentares; iii) 327 que dispõe sobre os controles internos específicos para o tratamento de situações relacionadas a crimes como lavagem de dinheiro, etc.	SUSEP - Superintendência de Seguros Privados

Fonte: Adaptado de Macieira, 2008.

Em síntese, destacam-se importantes transformações nas metodologias de auditoria até a abordagem de auditoria contínua, com novas metodologias aplicadas. Não que represente o fim de uma em detrimento de outra, mas de forma complementar o surgimento da auditoria contínua, como apresentado neste capítulo, permitirá uma real aplicação de métodos automatizados visando à redução de riscos dos processos e à melhoria dos controles internos (em tempo real ou quase real) em uma empresa do setor elétrico brasileiro.

Sua conceituação e estruturação baseada em métodos de integração de fluxo de informações e gestão de risco constituem-se um poderoso ferramental que permite a identificação de processos e controles internos críticos para alcance dos objetivos de uma organização, com mitigação dos riscos e fraudes.