PAULO PINHEIRO JÚNIOR

AUDITORIA INTERNA CONVENCIONAL E AUDITORIA INTERNA BASEADA EM RISCOS – ESTUDO SOBRE A IMPORTÂNCIA DA AUDITORIA INTERNA NO FORTALECIMENTO DOS CONTROLES INTERNOS, NO GERENCIAMENTO DE RISCOS E NO SUPORTE DE GOVERNANÇA CORPORATIVA

Monografia apresentada ao curso de pós-graduação em Auditoria Externa e Interna do Centro de Pós-graduação e Pesquisas em Contabilidade e Controladoria da Universidade Federal de Minas Gerais, como requisito parcial à obtenção do título de Especialista em Auditoria.

Orientador: Prof. Carlos Maurício Vieira

Belo Horizonte

2014

RESUMO

Este trabalho apresenta um estudo sobre a evolução da auditoria interna com foco nos controles internos e na gestão de riscos. Os conceitos de controle interno, gestão de riscos e governança corporativa foram apresentados no referencial teórico. O conceito de auditoria interna baseada em riscos foi desenvolvido inicialmente com a apresentação de um caso prático de gestão de riscos. O estudo mostra o impacto da evolução desses conceitos no modo de atuação dos auditores internos.

As novas abordagens de controles internos com enfoque na gestão de riscos, a expansão e valorização da auditoria interna, nos últimos anos, devido ao aumento das exigências no mercado de capitais em relação à robustez da estrutura de controles internos das empresas aumentaram a importância da auditoria interna no contexto da governança corporativa.

O estudo é suportado por uma análise qualitativa dos dados. O posicionamento da auditoria interna foi analisado por meio de uma pesquisa on-line de fonte secundária. Os participantes eram constituídos por diretores de auditoria, diretores gerais, diretores financeiros, diretores de riscos, diretores de compliance e diretores jurídicos.

Esse estudo mostra a importância crescente da gestão de riscos e as expectativas cada vez maiores dos stakeholders em relação à participação da auditoria interna no desafio da gestão de riscos, para oferecer benefícios ao negócio. Para que o apoio da auditoria interna aos esforços organizacionais de gestão de riscos seja eficiente, o padrão mínimo de desempenho precisa aumentar.

Auditores e Stakeholders devem manter um diálogo constante sobre os riscos da empresa, para que a auditoria interna seja realmente eficiente. As organizações enfrentam uma quantidade elevada de riscos. O entendimento entre auditores e stakeholders sobre os riscos mais críticos é essencial para a alocação eficiente de recursos. Na ausência desse entendimento, a auditoria pode deixar de direcionar recursos às áreas consideradas mais importantes pelos stakeholders, perdendo assim a oportunidade de adicionar valor ao negócio.

Os stakeholders definiram a função tradicional da auditoria interna de auditar os controles financeiros e a conformidade como a mais importante, mas a assessoria sobre riscos e controles vem bem perto, em segundo lugar. A auditoria interna deve fornecer a auditoria tradicional com análises aprofundadas e perspectivas de negócio.

Diante das demandas, a auditoria interna precisa atuar no novo nível, direcionando o monitoramento de riscos e a auditoria com base em avaliações de cima para baixo dos riscos estratégicos, concentrando recursos nos riscos críticos, fornecendo análises mais aprofundadas e usando técnicas mais eficientes de comunicação.

Palavras-chave: controle interno, gestão de riscos, governança corporativa.

LISTA DE FIGURAS

LISTA DE GRÁFICOS

LISTA DE QUADROS

LISTA DE TABELAS

LISTA DE SIGLAS E SIGNIFICADOS

ABR-	Auditoria Baseada em Riscos
COSO -	Committee of Sponsoring Organizations of the Treadway Comission
Framework -	Estrutura que explica uma metodologia
IIA -	Institute of Internal Auditors
Stakeholders -	Partes interessadas. Partes que são afetadas pela organização, como os acionistas, as comunidades nas quais a organização opera, os empregados, os clientes e os fornecedores.
TAG ALONG-	A possibilidade atribuída ao minoritário de alienar suas ações ao novo controlador, por ocasião da transferência do controle de companhia aberta.

SUMÁRIO

1. Introdução

Para que uma organização tenha sucesso, cumpra os objetivos propostos com eficiência, eficácia e economicidade, além de alcançar longevidade, é essencial que tenha uma boa governança, gestão de riscos e controles internos. A auditoria interna tem por finalidade auxiliar a organização no cumprimento de suas responsabilidades, desenvolvendo um plano de ação para avaliar a eficácia do desenho e da execução do sistema de controles internos e processos de gestão de riscos.

O IIA — The Institute of Internal Auditors define Auditoria Baseada em Riscos (ABR) como uma metodologia que associa a auditoria interna ao arcabouço (framework) global de gestão de riscos de uma organização. A ABR possibilita que uma auditoria interna dê garantias ao conselho diretivo de que os processos de gestão de riscos estão gerenciando os riscos de maneira eficaz em relação ao apetite por riscos.

A análise de risco inerente a cada atividade traz consigo grande complexidade pelos fatores subjetivos envolvidos, como o julgamento de quem o avalia, as influências políticas e econômicas do momento e a incerteza do que pode nos trazer o futuro.

Mesmo considerando a impossibilidade de uma percepção completa do risco, a estimativa dele é considerada importante subsídio ao planejamento e direcionamento dos trabalhos de auditoria.

A responsabilidade pela gestão de riscos é da direção da empresa. A auditoria interna, em um de seus principais papéis, tem a função de garantir que tais riscos tenham sido gerenciados adequadamente.

A auditoria interna tradicional se limitou a identificar e testar os controles internos. Conforme Castanheira (2007 apud LÉLIS, 2010), a atividade já passou por dois paradigmas. Primeiro, o enfoque na observação e na contabilização e, a partir da década de 40, o foco no sistema de controles internos, encontrando-se hoje num terceiro, o desafio de alinhar a visão dos processos aos riscos do negócio, tornando-se, assim, mais eficaz. A garantia de continuidade dos negócios não pode apenas recomendar e realizar controles internos, com base no histórico organizacional. Em vez de olhar para os processos de negócio como algo que está dentro de um sistema de controle, o auditor os analisa numa envolvente de riscos.

A Auditoria Baseada em Riscos (ABR) é uma metodologia que está evoluindo rapidamente em todo o mundo. Ainda não há um consenso sobre a melhor maneira de implementá-la.

Entender esse processo em seus detalhes e nuances é primordial para fomentar a mudança de paradigma da auditoria interna.

1.1. Problema

O que muda na atuação do auditor interno considerando-se o novo enfoque da auditoria interna convencional para auditoria interna baseada em riscos?

1.2. Objetivo Geral

Conhecer o conceito de auditoria baseada em riscos e o modo de atuação do auditor interno diante do novo paradigma da Auditoria Baseada em Riscos (ABR).

1.2.1. Objetivos específicos

Estudar a relação entre controle interno, gestão de risco e governança corporativa;

Estudar a mudança de paradigma da auditoria interna convencional para a auditoria interna com foco em riscos;

1.3. Justificativas

A atividade de auditoria interna tem passado por significativa expansão e valorização nos últimos anos, o que se deve, em parte, ao aumento das exigências no mercado de capitais em relação à robustez da estrutura de controles internos das empresas. Isso motivou novas abordagens de controles internos com enfoque na gestão de riscos.

Os mecanismos de avaliação vêm evoluindo ao longo do tempo. Coderre (2006 apud LÉLIS, 2010) afirma que a globalização, pressões regulatórias e de mercado e as rápidas mudanças do ambiente de negócios criaram a necessidade de procedimentos de monitoramento mais frequentes e tempestivos para assegurar a eficácia dos controles e a mitigação dos riscos.

A auditoria convencional está centrada nos controles internos que envolvem os processos operacionais enquanto a auditoria baseada em riscos está focada nos riscos que envolvem o negócio. Este estudo se propõe a entender o modo de atuação da auditoria interna com foco na gestão de riscos.

2. Revisão de literatura

Os auditores internos auxiliam a organização a alcançar seus objetivos através da aplicação de uma abordagem sistemática e disciplinada para avaliar e melhorar a eficácia dos processos de gerenciamento de governança, riscos e controle. Governança, riscos e controle são conceitos inter-relacionados e fundamentais no campo da auditoria interna.

2.1. Governança Corporativa

Segundo o Instituto Brasileiro de Governança Corporativa – IBGC (www.ibgc.org.br):

> 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 práticas de governança corporativa convertem princípios em recomendações objetivas, alinhando interesses com a finalidade de preservar e otimizar o valor da organização, facilitando seu acesso ao capital e contribuindo para a sua longevidade.

Andrade e Rossetti (2009, p. 137, 138 e 140) definem que pode-se relacionar um conjunto de diversidades que cerca as questões relacionadas à governança corporativa:

> 1. Dimensões das empresas; 2.estruturas de propriedade; 3. Fontes de financiamento predominantes; 4. Tipologia dos conflitos de agência e harmonização dos interesses em jogo; 5. Tipologia das empresas quanto ao regime legal; 6. Tipologia das empresas quanto à origem dos grupos controladores; 7. Ascendência das empresas, que se modifica por fusões e aquisições; 8. Abrangência geográfica de atuação das empresas; 9. Traços culturais das nações em que as empresas operam; e 10. Instituições legais e marcos regulatórios estabelecidos nas diferentes partes do mundo.
>
> A diversidade de conceitos de governança corporativa é muito grande, devido a esse conjunto de diversidades e ao seu desenvolvimento ainda recente. Pode-se dividi-los em 04 grupos:
>
> - Guardiã de direitos das partes com interesse em jogo nas empresas;
> - Sistema de relações pelo qual as sociedades são dirigidas e monitoradas;
> - Estrutura de poder que se observa no interior das corporações;
> - Sistema normativo que rege as relações internas e externas das companhias.
>
> Uma das mais importantes dimensões da governança corporativa são os valores que lhe dão sustentação, amarrando concepções, práticas e processos de alta gestão. São eles:
>
> - Fairness – Senso de justiça, equidade no tratamento dos acionistas. Respeito ao direito dos minoritários, por participação equânime com a dos majoritários, tanto no aumento da riqueza corporativa, quanto no resultado das operações, quanto ainda na presença ativa em assembleias gerais.

- Disclosure – Transparência das informações, especialmente das de alta relevância, que impactam os negócios e que envolvem resultados, oportunidades e riscos;
- Accountability – Prestação responsável de contas, fundamentada nas melhores práticas contábeis e de auditoria;
- Compliance – Conformidade no cumprimento de normas reguladoras, expressas nos estatutos sociais, nos regimentos internos e nas instituições legais do país.

Consultoria Ernst & Young (2013, p. 5 e 6) define que:

> a preocupação da Governança Corporativa é criar um conjunto eficiente de mecanismos a fim de assegurar que o comportamento dos executivos esteja sempre alinhado com o interesse dos acionistas. A empresa que opta pelas boas práticas de Governança Corporativa adota como linhas mestras a transparência, a prestação de contas, a equidade e a responsabilidade corporativa.
>
> A ausência de conselheiros qualificados e de bons sistemas de Governança Corporativa tem levado empresas a fracassos decorrentes de:

- Abusos de poder – do acionista controlador sobre minoritários, da diretoria sobre o acionista e dos administradores sobre terceiros;
- Erros estratégicos – resultado de muito poder concentrado no executivo principal;
- Fraudes – uso de informação privilegiada em benefício próprio, atuação em conflito de interesses.

> A necessidade de aderir às práticas de boa governança surge devido a:

- Processo de globalização;
- Privatização e desregulamentação da economia;
- Surgimento de um ambiente corporativo mais competitivo;
- Aumento de investimentos estrangeiros no mercado de capitais.

Ambiente competitivo: globalização, privatização e desregulamentação da economia: surgimento de conselheiros profissionais e independentes; movimento pelas boas práticas de Governança Corporativa; modernização da alta gestão; ser uma empresa atraente para o mercado.

2.1.1 Fatos relevantes sobre Governança Corporativa no Brasil:

Conforme consultoria Ernst & Young (2013, p. 7 e 8), pode-se relacionar os seguintes fatos relevantes sobre a governança corporativa no Brasil:

- 2000 – Lançamento dos segmentos diferenciados de governança corporativa (Bovespa);
- 2001 – Alteração da Lei das Sociedades Anônimas pela lei 10.303;

- 2002 – A Comissão de Valores Mobiliários (CVM) lança sua cartilha sobre o tema Governança, visando orientar sobre as questões que afetam o relacionamento
- administradores, conselheiros, acionistas e auditores independentes;
- 2002 – Primeira listagem na Bovespa incluindo o Novo Mercado.

BM&F BOVESPA – Segmentos de Listagem

Nível 1 – Exige práticas adicionais às exigidas pela Lei das SAs:

- Mínimo de 25% de free float (manter ações em circulação);
- Não acumulação de cargos (Presidente do conselho e CEO);
- Reunião pública anual e calendários de eventos corporativos;
- Divulgação de informações adicionais (Código de Conduta e Ética, por exemplo).

Nível 2 – Além das exigências do "Nível 1", tem por obrigação práticas adicionais relativas aos direitos dos acionistas e conselho de administração:

- Conselho de Administração composto por no mínimo 5 membros (pelo menos 20% independentes);
- Demonstrações traduzidas para o inglês;
- Concessão de tag along para 100% dos acionistas.

Novo Mercado – Possui padrão de governança corporativa altamente diferenciado, firmando-se como uma seção destinada à negociação de ações de empresas que adotam práticas de governança corporativa adicionais às que são exigidas pela legislação brasileira.

A listagem nesse segmento implica na adoção de regras societárias que ampliam os direitos dos acionistas, além da adoção de uma política de divulgação de informações mais transparente e abrangente.

Exigências além das obrigações no "Nível 2": - 100% de ações ordinárias (ON).

As Normas de Auditoria Interna fazem menção à governança dentro do papel do auditor:

...

2100 – Natureza do Trabalho

...

2130 – Controle – A atividade de auditoria interna deve avaliar e fazer recomendações apropriadas para a melhoria do processo de governança corporativa, no cumprimento dos seguintes objetivos:

- Promoção à ética e valores apropriados dentro da organização;
- Assegurar a gestão do desempenho eficaz da organização e a responsabilidade por prestação de contas;

- Comunicar de forma eficaz às áreas apropriadas da organização, as informações relacionadas ao risco e controle;
- Coordenar de forma eficaz as atividades e divulgar a informação para o conselho, os auditores externos e a administração.

2.2. Gestão de Riscos

Segundo Paula (1999, p.64) "Poder-se-ia definir risco como condições ou fatos significativos que podem criar uma situação de impossibilidade para a consecução dos objetivos estabelecidos".

> O risco normalmente é definido como a incerteza de um resultado ou de um evento. Ele pode referir-se tanto a uma ameaça negativa quanto a uma oportunidade positiva para uma empresa assumir um risco que vale a pena e pode trazer uma vantagem competitiva sobre concorrentes avessos ao risco. Porém, considerando o potencial de perdas significativas e também dos lucros, é importante que os riscos sejam avaliados com exatidão, calculando-se a probabilidade dos resultados assim como seu impacto em um negócio (LISBOA, 2014)[1].

Segundo o COSO II – ERM Integrated Framework (2007, p. 4),

> Gestão de Riscos é o processo conduzido em uma organização pelo conselho de administração, pela diretoria executiva e pelos demais funcionários, aplicado no estabelecimento de estratégias formuladas para identificar, em toda a organização, eventos em potencial, capazes de afetar a referida organização, e administrar os riscos para mantê-los compatíveis com o seu apetite a risco e possibilitar garantia razoável de cumprimento dos objetivos da entidade.

A Gestão de Riscos do Negócio é um processo contínuo de atividades integradas, pelas quais a alta gerência, suportada pelos responsáveis pelos processos de negócio, minimiza o impacto potencial dos riscos da organização sobre os objetivos e estratégias, criando e aumentando valor para os acionistas.

Uma condição prévia para a avaliação de riscos é, portanto, o estabelecimento de objetivos, vinculados aos diversos níveis hierárquicos, coerentes com a missão da entidade, considerando que deve haver sinergia entre os objetivos globais da entidade e de cada área

---

[1] http://www.portaldeauditoria.com.br/artigos/O-Papel-da-Auditoria-Interna-na-Prevencao-de-Riscos.html

administrativa separadamente e que existe o risco de que as expectativas quanto ao cumprimento da missão da entidade sejam frustradas.

O processo de avaliação de riscos compreende a identificação das atividades que devem ser auditadas, a vulnerabilidade pertinente a cada uma delas e a sua importância relativa.

2.2.1. Conceitos gerais:

ERM – Enterprise Risk Management – É uma abordagem de gerenciamento de riscos dentro de uma organização através da utilização de esforços integrados de todas as funções de gerenciamento de riscos, com todos os envolvidos assumindo responsabilidades pelos mesmos, incluindo a alta administração e as unidades de negócio. Reflete a necessidade de entender o complexo universo de riscos. ERM é uma abordagem integrada para gerenciar riscos. Otimiza o processo de análise de riscos. Um processo de ERM bem estruturado pode contribuir de forma direta para a melhoria e excelência dos padrões de Governança de uma Corporação. Essa melhora pode trazer benefícios concretos como redução de taxa de juros e processo de captação e melhoria no desempenho de papéis no mercado, entre outros.

Apetite a Risco – A quantidade total de riscos que uma companhia ou outra organização está disposta a aceitar na busca de sua missão (ou visão).

Controle Interno – Processo efetuado pelo conselho, administração ou qualquer outro funcionário de uma empresa, desenhado para fornecer garantia razoável em relação à realização dos objetivos corporativos.

Entidade – Uma organização de qualquer porte estabelecida para o atendimento de uma determinada finalidade. A entidade poderá ser, por exemplo, uma empresa comercial, uma organização sem fins lucrativos, um órgão do governo ou uma instituição acadêmica. Entre os termos empregados como sinônimos estão “organização e empresa”.

Evento – Incidente ou ocorrência, a partir de fontes internas ou externas a uma entidade, capaz de afetar a realização dos objetivos.

Garantia razoável – O conceito que o gerenciamento de riscos corporativos, independentemente de seu desenho e sua operação, não é capaz de propiciar uma garantia em relação à realização dos objetivos de uma organização. Isso ocorre em razão das Limitações Inerentes do gerenciamento de riscos corporativos.

Fraude – Operações em não conformidade com leis e regulamentos que visam obter ganho pessoal.

Impacto – Resultado ou efeito de um evento. Poderá haver uma série de impactos possíveis associados a um evento. O impacto de um evento pode ser positivo ou negativo em relação aos objetivos correlatos de uma empresa.

Incerteza – Incapacidade de conhecer antecipadamente a probabilidade exata ou o impacto de eventos futuros.

Limitações inerentes – Limitações do gerenciamento de riscos corporativos. Dizem respeito a limitações do julgamento humano; restrições de recursos e a necessidade de se considerarem os controles de custos em relação aos benefícios esperados; a realidade que podem ocorrer falhas; e a possibilidade de neutralização de controles e de conluio pela administração.

Oportunidades – A possibilidade que um evento ocorrerá e afetará favoravelmente a realização dos objetivos.

Partes interessadas / Stakeholders – Partes que são afetadas pela organização, como os acionistas, as comunidades nas quais a organização opera, os empregados, os clientes e os fornecedores.

Probabilidade – A possibilidade de ocorrência de um dado evento. Os termos podem adquirir conotações mais específicas como indicar "possibilidades" de que um dado evento ocorrerá em termos qualitativos, como elevada, média e reduzida, ou outras escalas de julgamento; e "probabilidade" indicando uma medida quantitativa, como porcentagem, frequência de ocorrência ou outra unidade numérica de medida.

Processo – Constituem um conjunto de ações relacionadas entre si de forma lógica e coerente a fim de promover um output favorável à empresa (qualidade total e satisfação do cliente), tanto a nível interno quanto externo.

Risco – A possibilidade de que um evento ocorra e afete desfavoravelmente a realização dos objetivos.

Risco Inerente – O risco que se apresenta a uma organização na ausência de qualquer medida gerencial que poderia alterar a probabilidade ou o impacto de um risco.

Risco residual – O risco que resta após a administração ter adotado medidas para alterar a probabilidade ou o impacto dos riscos.

Tolerância a riscos – A variação aceitável relativa à realização de um objetivo.

QUADRO 1
Diferenças entre gestão de riscos corporativos e auditoria interna

Gestão de Riscos Corporativos	Auditoria Interna
Prática que visa tratar o grau de exposição de uma organização à fatores adversos e desenvolver oportunidades perante incertezas.	Prática que visa verificar e testar a eficiência dos processos e controles da Companhia.
Gestão de riscos enxerga fatores internos e externos (ex.: concorrência, regulação).	Audita processos de forma independente.
Auxilia as áreas de negócio a conhecer e gerenciar seus riscos de forma a agregar valor para as organizações e auxiliá-las a atingir seus objetivos.	Auxilia as organizações a cumprirem seus objetivos, avaliando e desenvolvendo a efetividade dos processos de gestão de riscos, controles e governança.

Fonte: Apostila Ernest Young – Capacitação em Gestão de Riscos Corporativos – maio 2014

QUADRO 2
Relações entre gestão de riscos corporativos e auditoria interna

Gestão de Riscos Corporativos	Auditoria Interna
É auditada pela Auditoria Interna, como os demais processos da Companhia.	Audita os processos de Gestão de Riscos Corporativos para prover segurança de que os principais riscos estão sendo devidamente tratados.
Desenvolve a Matriz de Riscos, que contém informações sobre os riscos e a exposição da Companhia a eles. Este trabalho pode servir de insumo para a Auditoria Interna e para o Planejamento Estratégico desenvolverem suas atividades.	Utiliza informações sobre a exposição dos riscos da Companhia para identificar processos críticos a serem auditados.

Fonte: : Apostila Ernest Young – Capacitação em Gestão de Riscos Corporativos – maio 2014

Existem diversas categorias e classificações de riscos (dependendo da natureza do negócio da organização) que podem ser muito úteis durante os trabalhos da Auditoria Baseada em Riscos.

A seguir algumas categorias de riscos mais comuns aos diversos tipos de negócios:

Risco Estratégico – Risco de perda pelo insucesso das estratégias adotadas, levando-se em conta a dinâmica dos negócios e da concorrência, as alterações políticas no País e fora dele e as alterações na economia nacional e mundial. Exemplos:

- Satisfação do Cliente (Governança Corporativa, Reputação e Imagem, Retenção de talentos, etc);
- Crescimento do Negócio (Fusão e Aquisição);
- Rentabilidade
- Cenário Externo (Econômico,

    - Marco Regulatório, Mercado e Concorrência).
- Risco Financeiro – Riscos financeiros são aqueles que ocasionam ganhos ou perdas de recursos financeiros para a instituição. Exemplos:
    - Crédito
    - Liquidez
    - Inadimplência
    - Disponibilidade de capital
- Risco Operacional – É definido como a possibilidade de ocorrência de perdas resultantes de falhas, deficiência ou inadequação de processos internos, pessoas e sistemas, ou de eventos externos. Exemplos:
    - Tecnologia da Informação
    - Parceiros e Fornecedores
    - Fraude
    - Obrigações Contratuais
    - Logística

A gestão de riscos corporativos abrange os elementos do processo administrativo que possibilitam à administração tomar decisões. As decisões selecionadas pela administração (a partir de uma série de escolhas possíveis) por si só não são capazes de determinar se o gerenciamento de riscos corporativos está sendo eficaz. Mesmo considerando-se que as respostas aos riscos (por exemplo, atividades de controle) selecionadas sejam uma questão de julgamento administrativo, as escolhas devem possibilitar a redução dos riscos a níveis aceitáveis, conforme determinados pelo apetite ao risco e à razoável garantia de realização dos objetivos da organização.

O ambiente interno da organização exerce papel relevante na gestão do risco, porque abrange a cultura da organização, ou seja, a base para como o risco é visto e dirigido por uma entidade. Isto inclui a gestão do risco, a consciência interna sobre risco, a integridade, os valores éticos e o ambiente em que a empresa opera.

O exercício de identificação de eventos de riscos torna-se algo vital para a manutenção da operação e para garantir o cumprimento dos objetivos da organização. A identificação de riscos determina quais riscos podem afetar a organização positivamente ou negativamente dentro do processo de garantir que os objetivos da organização possam ser realizados:

- Eventos de impacto positivo representam oportunidades que são canalizadas de volta aos processos e objetivos da organização;
- Eventos de impacto negativo representam riscos e exigem avaliação e resposta.

2.2.2. COSO e seu padrão internacional para gestão de riscos

Em 1985, foi criada, nos Estados Unidos, a National Commission on Fraudulent Financial Reporting (Comissão Nacional sobre Fraudes em Relatórios Financeiros), uma iniciativa independente, para estudar as causas da ocorrência de fraudes em relatórios financeiros contábeis. Essa comissão era composta por representantes das principais associações de classe de profissionais ligados à área financeira.

Seu primeiro objeto de estudo foram os controles internos Internal Control – Integrated Framework (Controles Internos – Um Modelo Integrado, COSO I). Esta publicação tornou-se referência mundial para o estudo e aplicação dos controles internos.

Posteriormente a Comissão transformou-se em Comitê, que passou a ser conhecido como COSO – Committee of Sponsoring Organizations of the Treadway Commission. O COSO é uma entidade sem fins lucrativos, dedicada à melhoria dos relatórios financeiros através da ética, efetividade dos controles internos e governança corporativa.

Em 2004, publicaram o trabalho Enterprise Risk Management – Integrated Framework (COSO II). Este documento é hoje utilizado como referência para que as organizações possam implantar a Gestão Integrada de Riscos, pois compila os conceitos e técnicas sobre o assunto.

Controles internos (tratado no COSO I), é parte integral da Gestão de Riscos Corporativos (COSO II), de forma que o segundo framework pode ser considerado como uma extensão/complemento do primeiro.

O COSO II adiciona um quarto ambiente ao framework, o ambiente Estratégico. Os demais ambientes devem estar alinhados a este quarto ambiente, de acordo com a metodologia COSOII.

COSO II inclui três novos elementos-chave: Definição de objetivos, identificação de riscos e tratamento de riscos.

Conceitos relacionados a gestão de riscos são tratados e discutidos de forma aprofundada no COSO II, introduzindo conceitos como apetite e tolerância a risco. O COSO I foca

principalmente nos riscos relacionados a fraude. O COSO II introduz também a necessidade de uma visão de Portfólio de riscos.

2.2.3 Componentes chave do COSO II

O gerenciamento de riscos corporativos é constituído de oito componentes inter-relacionados, pela qual a administração gerencia a organização, e estão integrados com o processo de gestão. Esses componentes são:

Ambiente Interno – o ambiente interno compreende o tom de uma organização e fornece a base pela qual os riscos são identificados e abordados pelo seu pessoal, inclusive a filosofia de gerenciamento de riscos, o apetite a riscos, a integridade e os valores éticos, além do ambiente em que estes estão.

Fixação de Objetivos – os objetivos devem existir antes que a administração possa identificar os eventos em potencial que poderão afetar a sua realização. O gerenciamento de riscos corporativos assegura que a administração disponha de um processo implementado para estabelecer os objetivos que propiciem suporte e estejam alinhados com a missão da organização e sejam compatíveis com o seu apetite a riscos.

Identificação de Eventos – os eventos internos e externos que influenciam o cumprimento dos objetivos de uma organização devem ser identificados e classificados entre riscos e oportunidades. Essas oportunidades são canalizadas para os processos de estabelecimento de estratégias da administração ou de seus objetivos.

Avaliação de Riscos – os riscos são analisados, considerando-se a sua probabilidade e o impacto como base para determinar o modo pelo qual deverão ser administrados. Esses riscos são avaliados quanto à sua condição de inerentes e residuais.

Resposta a Risco – a administração escolhe as respostas aos riscos - evitando, aceitando, reduzindo ou compartilhando – desenvolvendo uma série de medidas para alinhar os riscos com a tolerância e com o apetite a risco.

Atividades de Controle – políticas e procedimentos são estabelecidos e implementados para assegurar que as respostas aos riscos sejam executadas com eficácia.

Informações e Comunicações – as informações relevantes são identificadas, colhidas e comunicadas de forma e no prazo que permitam que cumpram suas responsabilidades. A

comunicação eficaz também ocorre em um sentido mais amplo, fluindo em todos os níveis da organização.

Monitoramento – a integridade da gestão de riscos corporativos é monitorada e são feitas as modificações necessárias. O monitoramento é realizado através de atividades gerenciais contínuas ou avaliações independentes ou de ambas as formas. A rigor, o gerenciamento de riscos corporativos não é um processo em série pelo qual um componente afeta apenas o próximo. É um processo multidirecional e interativo segundo o qual quase todos os componentes influenciam os outros.

2.2.3.1. Cumprimento dos Objetivos

Com base na missão estabelecida, a administração planeja objetivos principais, seleciona as estratégias e estabelece outros planos a serem adotados por toda a organização, alinhados com a estratégia e a ela vinculados. Embora muitos objetivos sejam específicos a uma determinada organização, alguns deles são amplamente compartilhados. 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.

Essa estrutura estabelece quatro categorias de objetivos para a organização:

Estratégicos – referem-se às metas no nível mais elevado. Alinham-se e fornecem apoio à missão e visão da empresa. Geralmente estão associados aos mapas estratégicos da empresa.

Operacionais – têm como meta a utilização eficaz e eficiente dos recursos.

Comunicação – relacionados à confiabilidade dos relatórios que são gerados e emitidos interna ou externamente sobre informações financeiras e não financeiras.

Conformidade – fundamentam-se no cumprimento das leis e dos regulamentos pertinentes.

2.2.3.2. Relacionamento entre Objetivos e Componentes

Existe um relacionamento direto entre os objetivos que uma organização se empenha em alcançar e os componentes do gerenciamento de riscos corporativos, que representam aquilo que é necessário para o seu alcance. Esse relacionamento é apresentado a seguir por meio de uma matriz tridimensional, em forma de cubo:

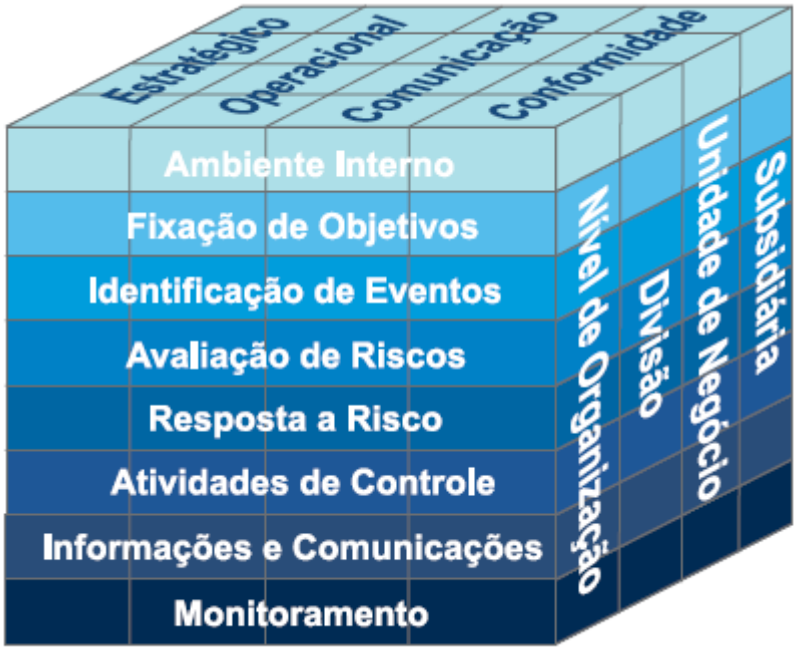

FIGURA 1: Cubo COSO II – Interação entre os componentes e os objetivos do gerenciamento de riscos corporativos.
Fonte: COSO – Gerenciamento de Riscos Corporativos – Estrutura Integrada

As quatro categorias de objetivos - estratégicos, operacionais, de comunicação e conformidade - estão representadas nas colunas verticais.

Os oito componentes, nas linhas horizontais.

A organização e as unidades de uma organização, na terceira dimensão do cubo.

A linha de cada componente "atravessa" e se aplica a todas as quatro categorias de objetivos. Por exemplo, os dados financeiros e não financeiros gerados a partir de fontes internas e externas, pertencentes ao componente de informação e comunicação, são necessários para estabelecer a estratégia, administrar as operações comerciais com eficácia, comunicar com eficácia e certificar-se de que a organização esteja cumprindo as leis aplicáveis.

2.2.4. ISO 31000:2009

Em 2009, a International Organization of Standadization (ISO) publicou a norma relativa à gestão de riscos corporativos objetivando prover princípios e regras para gerenciamento de riscos de forma aplicável e adaptável a qualquer tipo de empresa, independente do seu negócio, porte ou sistema de gestão. O processo de gestão de riscos proposto pela ISO é apresentado no framework a seguir:

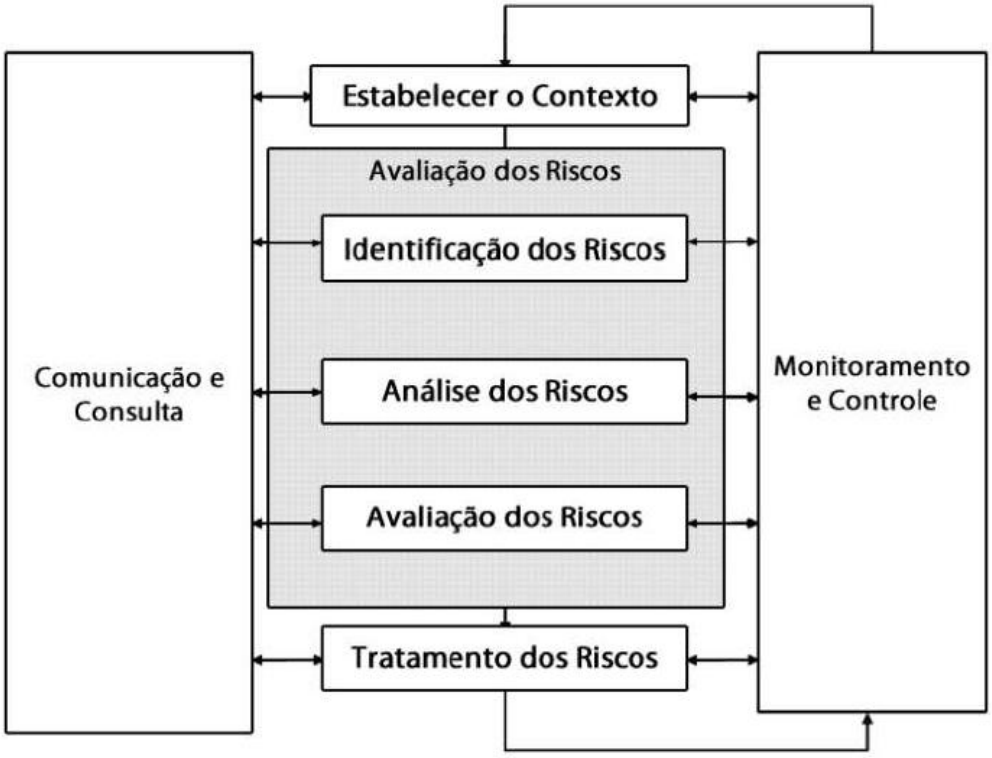

FIGURA 2: Processo de gerenciamento de riscos da ISO 31000

Fonte: ISO 31000

- Estabelecer o contexto – Consiste na contextualização do ambiente interno da Companhia onde poderão ocorrer os riscos.
- Identificar o risco – Consiste na identificação dos eventos internos ou externos que podem impedir ou dificultar o alcance dos objetivos empresariais da Companhia (Estratégicos, Operacionais, Conformidade e Reporte).
- Analisar o risco – Esta etapa consiste na análise preliminar sobre as variáveis consideradas para avaliar o risco (frequência e impactos) e respectivas medidas de controle/mitigação.
- Avaliar o risco – Consiste na avaliação quantitativa da frequência de ocorrência e impactos (operacional, ambiental, imagem e financeira) geradas com a ocorrência do risco.
- Tratar o risco – Consiste na decisão adotada para tratar ou responder aos riscos que estão acima dos limites aceitáveis pela Companhia.
- Monitorar e revisar – Consiste nas ações de monitoramento e revisão contínua dos riscos e respectivas medidas de controle/mitigação.

- Comunicar e consultar – Consiste nas ações de comunicação e consulta entre os diferentes agentes que compõe a estrutura de Gestão de Riscos da Companhia.

2.2.5. Avaliação de Riscos

Uma vez identificados, os riscos devem ser avaliados. Os riscos são avaliados numa base inerente ao nível da entidade, isto é, sem a consideração dos efeitos de controles. A organização, ao avaliar os riscos, deve considerar até que ponto os eventos previstos e imprevistos podem impactar a realização de seus objetivos. Em sua análise, levam-se ainda em consideração (1) a probabilidade e (2) o impacto de sua ocorrência.

Os objetivos da avaliação de riscos são aumentar a probabilidade e o impacto dos eventos positivos e diminuir a probabilidade e o impacto dos eventos adversos (negativos). Impacto e probabilidade determinam a classificação do risco global.

- Impacto – a extensão pela qual o risco, caso realizado, poderia afetar a empresa.
- Probabilidade – a probabilidade de o risco ocorrer em um período pré-definido.

Na análise dos riscos, pode-se recorrer a análises qualitativas ou quantitativas dos mesmos. A análise qualitativa faz a priorização dos riscos através de avaliação e combinação de sua probabilidade de ocorrência e impacto, utilizando para isso a classificação de “alto”, “médio” e “baixo” através de um critério matricial. Já a análise quantitativa faz a análise numérica do efeito dos riscos identificados nos objetivos gerais.

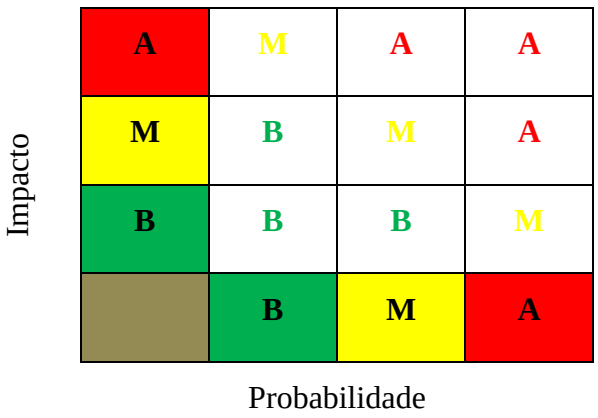

FIGURA 3: Análise de Riscos
Fonte: Apostila Capacitação em Gestão de Riscos Corporativos – Ernest Young

RISCO: Molhar-se com água de chuva durante o percurso de sua casa até o escritório.

A chance (ou probabilidade) de isto ocorrer é o número de dias que choveu, no horário de ida ao trabalho, durante o ano passado, dividido por 365.

As consequências (ou impactos) deste evento, são:

- Outro risco: gripe;
- Constrangimento;
- Desconforto durante o expediente.

As possíveis escolhas para este evento são:

- Aceitar o risco (...não me importo de me molhar e odeio guarda-chuvas);
- Descobrir um conjunto de controles que minimizem (ou mitiguem) as chances de ser vitimado pelo evento, caso ele ocorra.

Ausência de controles não é um risco!

QUADRO 3
Riscos VS. Ausência de Controles

Documentação incorreta de riscos	**Documentação correta de riscos**
Reconciliação bancária não foi preparada	Saldos em Conta Corrente existentes e não contabilizados e/ou contabilizados de forma imprecisa
Ordens de compras não foram autorizadas	Compras inadequadas foram realizadas, resultando em gastos adicionais desnecessários
Análise dos níveis de inventário não têm consistência	Níveis adequados de inventário não são mantidos, resultando em estoques fictícios e perdas de vendas a clientes

Fonte: Apostila Capacitação em Gestão de Riscos Corporativos – Ernest Young

- **Riscos Externos VS. Riscos Internos**

Riscos Externos – exposições resultantes das condições de mercado que a empresa normalmente não pode influenciar, como por exemplo:

- Mudanças na economia/mercado;
- Mudanças no ambiente competitivo;
- Mudanças regulatórias/legislativas.

Riscos Internos – Exposições devido à tomada de decisões corporativas e uso interno ou externo de recursos, como por exemplo:

- Roubo de estoque;
- Pagamentos em duplicidade;
- Acesso inadequado ao sistema de TI.

Consequências da materialização de riscos:

- Danos à imagem da Companhia;
- Perdas financeiras;
- Sanções de órgãos reguladores;
- Perda de participação no mercado;
- Perda de uma oportunidade, entre outros.

2.2.6. Gestão de Riscos Corporativos na Prática

- **Mapeamento de Riscos** – para a implantação da Gestão de Riscos Corporativos, a primeira etapa é o mapeamento dos riscos, que engloba:
- Identificação de riscos;
- Avaliação de riscos;
- Priorização de riscos.

- **Identificação de Riscos** – para a identificação de riscos, foram utilizados diretrizes do COSO-ERM e ISO 31000. Documentos internos da empresa e informações sobre o setor e empresas semelhantes foram analisados. Análise de biblioteca de riscos do setor de Utilities da empresa de consultoria. Além desses materiais, os riscos foram identificados por meio de reuniões com Diretores e Superintendentes da Companhia, levantando questões sobre os principais riscos inerentes ao negócio da Companhia, principais desafios, o que a Companhia faz atualmente para gerenciar seus principais riscos, quais fatores poderiam afetar a Companhia no alcance dos seus principais objetivos estratégicos.

Foram identificados vários riscos na Companhia. Os riscos identificados foram transcritos para uma Biblioteca de Riscos, contendo as seguintes informações:

- Número do risco #;
- Diretoria associada ao risco;
- Área responsável pelo risco;
- Macro processo do risco;

- Natureza do risco sendo: Corporativo; Financeiro; Regulatório, Legal e Compliance; Operacional.
- Nome do risco;
- Descrição do risco ao qual a Cia. está exposta;
- Fatos que caso ocorressem contribuiriam para a materialização do risco.

QUADRO 4
Mapeamento de riscos - Identificação – Exemplo

Dir.	**Unidade**	**Macro-Processo**	**Natureza de Risco**	**#**	**Risco**	**Descrição do Risco**	**Fatores de Risco**
DITE	Empreendimentos	Avaliação, seleção e hierarquização de empreendimentos	Corporativo	R022	Priorização de empreendimentos	Priorização e seleção inadequada de empreendimentos	. Interferência política na priorização de empreendimentos; . Estudo de viabilidade econômico-financeiro inadequado; . Dificuldade de balancear as questões sociais e econômicas para priorização de empreendimentos; . Elaboração de projetos inviáveis ou inadequados, em desacordo com os objetivos estratégicos e condicionantes técnicas, legais e ambientais; . Informações utilizadas para realizar os estudos de viabilidade não são precisas ou confiáveis.
DITE	Empreendimentos	Avaliação, seleção e hierarquização de empreendimentos	Financeiro	R023	Retorno de Empreendimentos	Retorno econômico financeiro de empreendimentos não ocorre conforme previsto nos estudos de viabilidade	.Informações utilizadas para realizar os estudos de viabilidade não são precisas ou confiáveis; .Inexistência de follow-up dos estudos de viabilidade econômico-financeira; . Efeitos inflacionários podem não ser refletidos adequadamente para garantir a assertividade dos estudos de viabilidade; . Execução de projetos inviáveis ou inadequados; . Inexistência de uma função específica e independente de gerenciamento e acompanhamento de projetos e empreendimentos (PMO).

Fonte: Apostila Capacitação em Gestão de Riscos Corporativos – Ernest Young

- **Dados sobre os riscos da Companhia:**

Natureza dos riscos:

- Operacional – 49%
- Corporativo – 31%
- Financeiro – 12%
- Regulatório, Legal e Compliance – 8%

As diversas unidades da Cia. são responsáveis por N riscos cada uma.

Diversas análises podem ser feitas com relação aos riscos, destacando:

- Classificação dos riscos como internos e externos;
- Classificação dos fatores de riscos como internos e externos;
- Link de riscos com objetivos e iniciativas estratégicas;
- Inter-relação de riscos;
- Relação de riscos com os macroprocessos da Companhia.

QUADRO 5
Classificação dos riscos e fatores de risco como internos e externos

Descrição do risco	**Origem dos eventos**	**Fatores de risco internos**	**Fatores de risco externos**
Priorização e seleção inadequada de empreendimentos	Interno	• Inexistência de políticas e procedimentos formais para auxiliar o processo de priorização de empreendimentos; • Estudo de viabilidade econômico financeiro inadequado; • Insuficiência de informações para a tomada de decisão; • Priorização e seleção de empreendimentos em desacordo com os objetivos corporativos da Companhia; • Dificuldades de balancear as questões sociais e econômicas para priorização/seleção de empreendimentos.	• Interferência política na priorização de empreendimentos.
Retorno econômico financeiro de empreendimentos não ocorre conforme previsto nos estudos de viabilidade	Interno	• Informações utilizadas para realizar os estudos de viabilidade não são precisas ou confiáveis; • Inexistência de follow-up dos estudos de viabilidade econômico-financeira; • Efeitos inflacionários podem não ser refletidos adequadamente para garantir a assertividade dos estudos de viabilidade;	N/A

Fonte: Treinamento Capacitação em Gestão de Riscos Corporativos – Ernest Young

QUADRO 6
Link de riscos com objetivos e iniciativas estratégicas

Descrição do Risco	Objetivos relacionados	Iniciativas relacionadas
Priorização e seleção inadequada de empreendimentos	• Elevar o valor de mercado • Otimizar a estrutura de capital	• Priorizar carteira de investimentos com retorno maior ou igual ao WACC; • Aprimorar e implementar modelo econômico-financeiro de longo prazo de forma sustentável; • Alinhar orçamento, programa de investimentos e planejamento estratégico com as necessidades empresariais; • Identificar macroprocessos (ponta a ponta) e implantar gestão por processos.
Retorno econômico-financeiro de empreendimentos não ocorre conforme previsto nos estudos de viabilidade.	• Elevar o valor de mercado • Otimizar a estrutura de capital • Assegurar sustentabilidade econômico-financeira. • Aumentar a eficiência e eficácia dos processos.	• Priorizar carteira de investimentos com retorno maior ou igual ao WACC; • Alinhar orçamento, programa de investimentos e planejamento estratégico com as necessidades empresariais; • Identificar macroprocessos (ponta a ponta) e implantar gestão por processos.

Fonte: Treinamento Capacitação em Gestão de Riscos Corporativos – Ernest Young

QUADRO 7
Inter-relação de riscos

Descrição do Risco	Riscos relacionados
Priorização e seleção inadequada de empreendimentos.	• Retorno econômico-financeiro de empreendimentos não ocorre conforme previsto nos estudos de viabilidade; • Elaboração de projetos inviáveis ou inadequados, em desacordo com os objetivos estratégicos e condicionantes técnicas, legais e ambientais; • Estudo de apuração de custos e elaboração de orçamentos de empreendimentos não exato e/ou em desacordo com os objetivos corporativos e políticas da Companhia; • Ineficiência no planejamento de empreendimentos; • Exposição a fatores políticos que possam refletir negativamente nas operações da Companhia; • Incapacidade de avaliar e selecionar as melhores alternativas para alocação de recursos para execução do programa de investimentos.
Retorno econômico-financeiro de empreendimentos não ocorre conforme previsto nos estudos de viabilidade.	• Conclusão do empreendimento fora do prazo determinado e/ou com custos superiores ao valor orçado e/ou com a qualidade aquém do desejado; • Priorização e seleção inadequada de empreendimentos; • Elaboração de projetos inviáveis ou inadequados, em desacordo com os objetivos estratégicos e condicionantes técnicas, legais e ambientais; • Estudo de apuração de custos e elaboração de orçamento de empreendimentos não exato e/ou em desacordo com os objetivos corporativos e políticas da Companhia; • Ineficiência do processo de aquisição para a execução dos empreendimentos (obras, serviços e materiais), incluindo não conformidade com a lei 8.666/93; • Dificuldades/morosidade no processo de aquisição e desapropriação de imóveis/terrenos para continuidade das operações da Companhia; • Ineficiência no planejamento de empreendimentos; • Realizar projeções pouco confiáveis, tanto financeiras, operacionais, dentre outros, para auxiliar na tomada de decisão.

Fonte: Treinamento Capacitação em Gestão de Riscos Corporativos – Ernest Young

- **Avaliação de Riscos -** A avaliação de riscos ocorre da seguinte forma:

Exposição = Probabilidade VS. Impacto

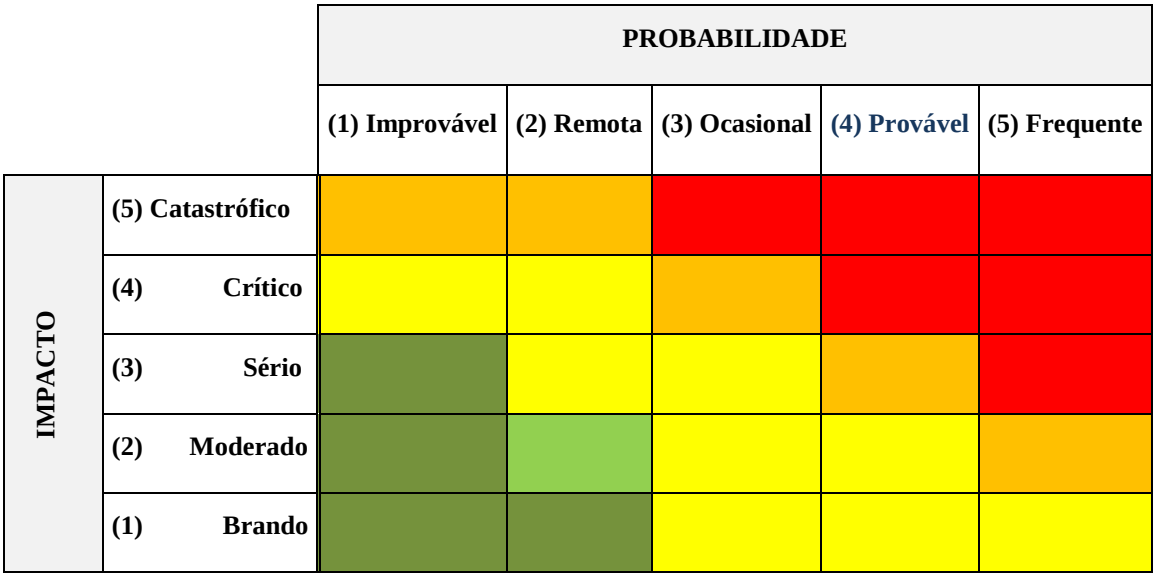

FIGURA 4: Avaliação de Riscos
Fonte: Treinamento Capacitação Gestão de Riscos Corporativos – Ernest Young

Os critérios de Avaliação de Riscos apresentados a seguir foram utilizados como guia para avaliar os riscos na Companhia.

TABELA 1
Frequência VS. probabilidade de materialização do risco

Análise de Frequência/Probabilidade de materialização do risco		
	PROBABILIDADE ESTIMADA DE MATERIALIZAÇÃO DO RISCO	**FREQUÊNCIA ESTIMADA DE MATERIALIZAÇÃO DO RISCO**
(5) Frequente	> 90%	< 1 MÊS
(4) Provável	≤ 90%	> 1 MÊS < 12 MESES
(3) Ocasional	≤ 60%	> 01 ANO < 02 ANOS
(2) Remota	≤ 30%	> 02 ANOS < 05 ANOS
(1) Improvável	≤ 10%	> 05 ANOS

Fonte: Treinamento Capacitação em Gestão de Riscos Corporativos – Ernest Young

QUADRO 8
Impacto do risco

	Análise do Impacto				
	VETOR PRINC.	**VETORES AUXILIARES DE ANÁLISE DE IMPACTO**			
ESCA-LA	**Financeiro**	**Regulatório e Compliance**	**Operação**		**Reputação e imagem**
			Dias (x)	**População atingida (y)**	
(5) Catas-trófico	Maior que R$ 180.000.000	Acusações de larga escala resultando em grandes penalizações, multas e exposição de imagem da Companhia.	Interrupção das operações da Cia por mais de 05 dias	Interrupção nas operações da Cia atingindo mais de 1.400.000 pessoas (10% da população atendida).	Publicidade negativa amplamente divulgada atingindo o ambiente nacional e/ou internacional, afetando profundamente a credibilidade da Cia.
(4) Crítico	Até R$ 180.000.000	Grandes desafios de responsabilidades legais com possibilidade de multas dos órgãos fiscalizadores/ regulatórios	Interrupção das operações da Cia por até de 05 dias	Interrupção nas operações da Cia atingindo até 1.400.000 pessoas (10% da população atendida.	Publicidade negativa em âmbito estadual, com desgastes marcantes na imagem da Cia.
(3) Sério	Até R$ 90.000.000	Investigação regulatória com necessidade de estabelecer provisão para multa	Interrupção das opera-ções da Cia por até 4 dias	Interrupção nas operações da Cia atingindo até 700.000 pessoas (5% da população atendida)	Publicidade negativa com desgastes na imagem da Cia e divulgação à região metropolitana
(2) Moderado	Até R$ 55.000.000	Atenção regulatória, sem multas ou necessidade de proceder com provisão	Interrupção das opera-ções da Cia por até 3 dias	Interrupção nas operações da Cia atingindo até 420.000 pessoas (3% da população atendida)	Publicidade negativa com divulgação restrita ao âmbito municipal
(1) Brando	Até R$ 20.000.000	Responsabilização limitada	Interrupção das operações da Cia por até 2 dias	Interrupção nas operações da Cia atingindo até 140.000 pessoas (1% da população atendida)	Publicidade negativa apenas para o público interno sem comprometimento da confiança da Cia

Fonte: Treinamento Capacitação Gestão de Riscos Corporativos – Ernest Young

TABELA 2
Análise da probabilidade VS. impacto de ocorrência dos riscos

			Probabilidade/Frequência de Ocorrência do Risco				
			(1) Improvável	(2) Remota	(3) Ocasional	(4) Provável	(5) Frequente
			2	3	5	8	13
Impacto do Risco	(5) Catastrófico	32	64	96	160	256	416
	(4) Crítico	16	32	48	80	128	208
	(3) Sério	8	16	24	40	64	104
	(2) Moderado	4	8	12	20	32	52
	(1) Brando	2	4	6	10	16	26

Fonte: Treinamento Capacitação Gestão de Riscos Corporativos – Ernest Young

- **Os riscos da Companhia foram avaliados em dois momentos:**

I. Workshop de avaliação de riscos – participação de chefes de departamento, superintendentes e analistas; Compreensão de metodologia e avaliação dos riscos identificados.

II. Refinamento dos resultados obtidos no workshop: adequação dos resultados do workshop com base no conhecimento da metodologia e a experiência da consultoria em Gestão de Riscos Corporativos.

Os participantes do workshop discutiram sobre os riscos apresentados e preencheram as seguintes informações sobre cada um desses riscos:

QUADRO 9
Avaliação de Riscos - Workshop

Inerente		Justificativa	Ações de Tratamento	Residual		Justificativa
Impacto (1 a 5)	Probabilidade (1 a 5)			Impacto (1 a 5)	Probabilidade (1 a 5)	

Fonte: Treinamento Capacitação Gestão de Riscos Corporativos – Ernest Young

Os participantes adicionaram também novos riscos e fatores de riscos. Devido à maturidade inicial da Companhia em Gestão de Riscos Corporativos, alguns pontos de atenção foram identificados:

- Avaliação realizada sobre perspectiva da área e não da Companhia;
- Dificuldade de aplicação dos critérios de avaliação de riscos e compreensão da metodologia;
- Tendência de avaliar muitos riscos como críticos gerando necessidade de refinamento dos resultados do workshop.

O refinamento dos resultados foi realizado por meio de reuniões adicionais com alguns superintendentes e gerentes e adequação da avaliação do workshop à metodologia de Gestão de Riscos Corporativos.

QUADRO 10
Mapeamento de Riscos – Avaliação

(Continua)

Descrição do Risco	Prob	Imp	Risco Inerente	Ações de Tratamento	Prob	Imp	Risco Residual
Priorização e seleção inadequada de empreendimentos	5	5	416	• Unidade específica para gerenciar o processo de seleção e hierarquização de empreendimentos; • Todos os empreendimentos hierarquizados são levados para conhecimento da Diretoria Executiva para revisão, priorização e aprovação; • Premissas como análises técnicas de engenharia, aspectos ambientais e sociais, projeção de fluxo de caixa, TIR, VPL e Payback são documentadas e estruturadas na planilha "Matriz de Análise de Viabilidade", que permitirá a gestão do "score" de viabilidade do empreendimento; .Ordenação dos projetos das diretoria operacionais é realizada por um departamento independente (Superintendência de Coordenação de Apoio); • As premissas para elaboração dos estudos de viabilidade global são baseadas em uma ferramenta de BI (DW Oracle). Este banco de dados não permite adições ou exclusões e é o espelho das informações dos sistemas transacionais da Companhia; • Os estudos de viabilidade global são elaborados por engenheiros especialistas e revisado pelo Gerente da Divisão de Hierarquização de Empreendimentos.	4	3	64

QUADRO 10
Mapeamento de Riscos – Avaliação

(Conclusão)

Descrição do Risco	Prob	Imp	Risco Inerente	Ações de Tratamento	Prob	Imp	Risco Residual
Retorno econômico financeiro de empreendimentos não ocorre conforme previsto nos estudos de viabilidade	5	3	104	• Premissas como análises técnicas de engenharia, aspectos ambientais e sociais, projeção de fluxo de caixa, TIR, VPL e Payback são documentados e estruturados na planilha "Matriz de Análises de Viabilidade", que permitira a gestão do "score" de viabilidade do empreendimento; .Os estudos de viabilidade global são elaborados por engenheiros especialistas e revisados pelo Gerente da Divisão de Hierarquização de Empreendimentos; • As premissas para elaboração dos estudos de viabilidade global são baseadas em uma ferramenta de BI (DW Oracle). Este banco de dados não permite adições ou exclusões e é o espelho das informações dos sistemas transacionais da Companhia	4	2	32

Fonte: Treinamento Capacitação Gestão de Riscos Corporativos – Ernest Young

- **Priorização de Riscos**

Os riscos avaliados foram priorizados de acordo com sua exposição inerente, e separados em níveis:

Nível 1 – Riscos de relevância crítica, definidos de acordo com a exposição inerente do risco e percepção dos diretores da Companhia. Foram identificados 25 riscos.

Nível 2 – Riscos de relevância alta, de acordo com exposição inerente. Foram identificados 30 riscos.

Nível 3 – Riscos de relevância moderada, de acordo com exposição inerente. Foram identificados 90 riscos.

A Unidade de Gestão de Riscos deve conduzir periodicamente, com o apoio dos Chefes de Departamento e Superintendentes, a avaliação inerente e residual da Companhia, para verificar variações na exposição de cada evento, e garantir que as avaliações estejam de acordo com a realidade.

- **Operação da Gestão de Riscos Corporativos**

Tratamento de Riscos

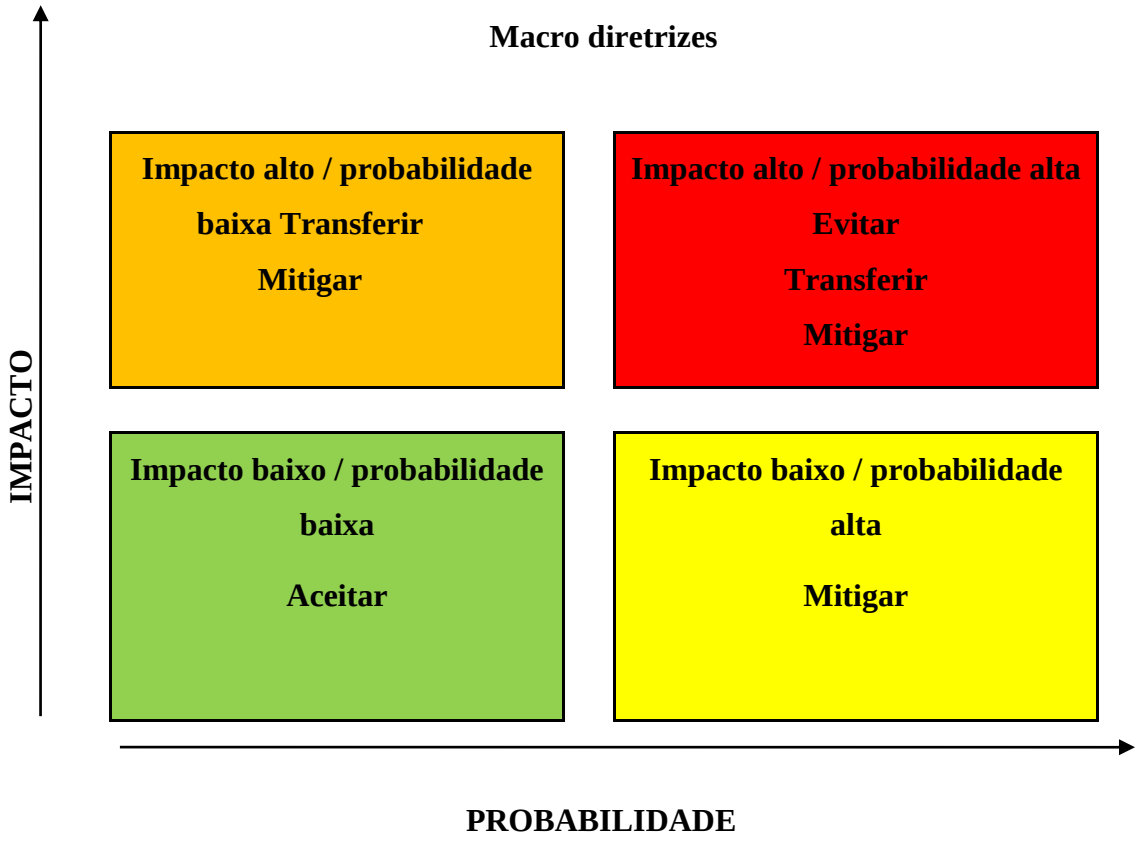

FIGURA 5: Tratamento de Riscos – Macro diretrizes
Fonte: Treinamento Capacitação Gestão de Riscos Corporativos – Ernest Young

- **O tratamento dos riscos é realizado de forma diferente para os riscos de cada nível:**

Nível 1: Tratamento realizado por meio de ficha de risco, que contempla informações essenciais do risco e os planos de ação da Companhia que o tratam;

Nível 2: Tratamento de riscos é associado aos planos de ação da Companhia;

Nível 3: Realização de auto avaliações – as áreas da Companhia analisam seus próprios processos de gerenciamento de riscos corporativos.

EX.: Risco – Custos

Descrição do Risco – Inabilidade de gestão dos custos e despesas da Companhia para manter a rentabilidade do negócio.

Planos de Ação Associados – Otimizar despesa de pessoal; otimizar custo com serviços operacionais primarizados; otimizar custos com serviços operacionais terceirizados; otimizar outras despesas operacionais; definir e implantar política de gerenciamento de custos.

Monitoramento de riscos – os riscos devem ser monitorados para que a Companhia possa prever e caso aplicável, tomar ações para evitar sua materialização.

Considerando que a Gestão de Riscos Corporativos na Companhia está em desenvolvimento inicial, a Companhia não teria condições de monitorar os 145 riscos identificados, além disso, o custo-benefício poderia não ser adequado. Foram escolhidos 15 riscos, nível 1, para serem monitorados, à princípio.

Para o monitoramento destes riscos, é necessário compreender no detalhe os processos que envolvem os riscos. Após compreensão do processo, são desenvolvidos Indicadores Chave de Risco – KRIs (Key Risk Indicators). São métricas que permitem a percepção tempestiva e antecipada da materialização de riscos.

KRIs funcionam como alertas de que algo pode dar errado. São baseados nos fatores que podem levar à materialização dos riscos – os fatores de risco.

Quanto mais crítico o risco, mais elevado deve ser o cargo do responsável por monitorá-lo.

- **Comunicação de Riscos**

A comunicação em gestão de riscos corporativos tem como propósito:

- Transmitir a importância da Gestão de Riscos Corporativos;
- Informar o papel e responsabilidade de cada área com relação ao gerenciamento de riscos;
- Comunicar os riscos identificados e avaliados, bem como as ações de tratamento e monitoramento;
- A comunicação varia de acordo com a relevância do risco.

2.3. Controle Interno

Jung (2006, p. 381, apud Lisboa) entende sobre controles internos que eles são “todos os instrumentos da organização destinados à vigilância, fiscalização e verificação administrativa, que permitam prever, observar, dirigir ou governar os acontecimentos que verificamos dentro da empresa e que produzam reflexos em seu patrimônio”.

Segundo o COSO - Committee of Sponsoring Organizations of the Treadway Commission (2013, pg12) “Controle interno é um processo conduzido pela estrutura de governança, administração e outros profissionais da entidade, e desenvolvido para proporcionar segurança razoável com respeito à realização dos objetivos relacionados a operações, divulgação e conformidade.”

Essa definição reflete alguns conceitos fundamentais. O controle interno é:

• Conduzido para atingir objetivos em uma ou mais categorias – operacional, divulgação e conformidade.

• Um processo que consiste em tarefas e atividades contínuas – um meio para um fim, não um fim em si mesmo.

• Realizado por pessoas – não se trata simplesmente de um manual de políticas e procedimentos, sistemas e formulários, mas diz respeito a pessoas e às ações que elas tomam em cada nível da organização para realizar o controle interno.

• Capaz de proporcionar segurança razoável - mas não absoluta, para a estrutura de governança e alta administração de uma entidade.

• Adaptável à estrutura da entidade – flexível na aplicação para toda a entidade ou para uma subsidiária, divisão, unidade operacional ou processo de negócio em particular.

O IIA (2010 apud Lélis, 2010) afirma que um sistema de controle interno representa um conjunto de atividades e componentes de controle utilizados por uma organização para alcançar seus objetivos e metas.

Algumas Considerações sobre Controles:

- Controles ajudam as companhias a alcançar objetivos por meio da mitigação de riscos;
- O significado do controle se remete ao significado do risco que ele está mitigando;
- Riscos podem ocorrer em um ambiente controlado (custo vs. benefício);
- Um mesmo controle pode mitigar múltiplos riscos;
- Múltiplos controles podem ser necessários para mitigar somente um risco.

Quem não mede não controla, quem não controla não gerencia.

Os objetivos básicos a serem alcançados pelo sistema de controle interno são quatro, a saber:

1. Proteção do ativo;
2. Obtenção de informações adequadas;
3. Promoção da eficiência operacional;
4. Estimular a observância das políticas estabelecidas pela direção.

O Controle Interno refere-se não apenas aos aspectos diretamente relacionados às funções de contabilidade e finanças, mas sim a todos os aspectos das operações de uma empresa. O conhecimento dos controles internos obtidos pelo auditor fará com que este chegue a uma das seguintes conclusões:

a) O sistema de controles internos é adequado;

b) O sistema de controles internos é adequado, podendo, entretanto, ser aprimorado;

c) O sistema de controles internos é adequado, existindo, porém, fraquezas que deterioram e podem vir a comprometer o sistema em sua totalidade;

d) O sistema de controles internos é inadequado, pois não atende aos princípios básicos vitais para a obtenção de um sistema de controle interno.

Tendo em vista as hipóteses acima, o auditor deverá determinar as consequências e implicações, quais os procedimentos de auditoria a serem aplicados e sua extensão, para a cobertura dos referidos objetos da auditoria, analisando-os na amplitude que merecem.

A American Institute of Certified Public Accountants – AICPA classificou os controles internos em:

- contábeis (envolvem segregação de funções, sistema de autorização e sistema de registro); e
- administrativos (envolvem pessoal qualificado, estímulo à eficiência operacional e obediência às normas).

Segundo o Instituto dos Auditores Independentes do Brasil (Ibracon -1998, apud Lisboa 2012), no enfoque do auditor, os controles internos podem ser classificados da seguinte forma:

Ambiente de controle: base em que se apoiam os controles, tais como a filosofia, os valores e os compromissos emanados dos dirigentes.

Controles diretos:

- gerenciais - correspondem aos controles aplicados por níveis hierárquicos que estejam acima dos processos operacionais;
- independentes - aplicados por pessoas que não participam do processo, por exemplo, a auditoria interna;
- de processamento - aplicado dentro do processo;
- de salvaguarda de ativos.

Controles gerenciais: permeiam toda a empresa, como, por exemplo, a segregação de funções e salvaguarda de ativos. Abrangem os controles que permeiam todos os processos da entidade

e estão ligados à organização empresarial. São a segregação de funções e a delimitação de responsabilidades.

Como se pode observar, existe mais de uma classificação, não existe um único sistema-modelo a ser seguido, mas alguns princípios são essenciais à elaboração e ao estabelecimento de um sistema de Controle Interno.

Assim, Pinho (2007, p. 48, apud Lisboa 2012) afirma que um adequado sistema de controle interno está baseado nos seguintes pilares:

- Delimitação de responsabilidade: determina quem faz o quê;
- Segregação de funções: separa atividades complementares entre diferentes responsáveis. Entende-se como tal: execução, aprovação, conferência, registro e autorização;
- Definição do manual da organização: quando viável é importante;
- Qualificação de pessoal (seleção e contínuo treinamento): sem pessoal não há controle;
- Rodízio de atividades: evita problemas de afastamento, demissões. Confere versatilidade ao funcionamento;
- Procedimentos que permitam confrontação periódica com registros contábeis: com vistas a garantir a confiabilidade dos dados;
- Criação de controles físicos, limitando o acesso aos ativos;
- Auditoria interna: quando viável é um controle controlando os demais;
- Relação custo x benefício: aplicável quando da implantação de uma norma de controle interno;
- Comprovação da veracidade dos informes e relatórios contábeis, financeiros e operacionais;
- Prevenção de fraudes e, em caso de ocorrência delas, possibilidade de descobri-las o mais rapidamente possível e determinar sua extensão;
- Localização de erros e desperdícios promovendo, ao mesmo tempo, a uniformidade e a correção ao registrarem-se as operações;
- Estímulo à eficiência do pessoal, mediante o controle que exerce por meio dos relatórios;
- Salvaguarda dos ativos e, de maneira geral, obtenção de um controle eficiente sobre todos os aspectos vitais do negócio.

Diante da classificação dos cuidados a serem considerados ao elaborar um sistema de controle interno apresentado, vamos trazer no subitem a seguir alguns ambientes que podemos definir como grupos patrimoniais.

2.3.1. Ambientes do Controle Interno

Lisboa (2012, p. 35 e 36),

> define como ambientes do controle interno os diversos grupos patrimoniais e operações existentes nas organizações e empresas, destacando que, para garantir a sua eficácia no sistema de controle interno, cada organização ou empresa, de acordo com suas necessidades e dimensões dos diversos grupos patrimoniais e operações que mantém ou possui, deve adotar um padrão próprio a ser seguido.
>
> Apresentam-se grupos patrimoniais e operações a serem implantados nos controles internos das organizações e empresas:

- Caixa;
- Bancos;
- Clientes;
- Outros créditos;
- Estoques;
- Investimentos;
- Imobilizado;
- Fornecedores;
- Outras obrigações;
- Vendas;
- Recebimentos;
- Compras;
- Pagamentos em geral;
- Folha de pagamento;
- Assuntos diversos de interesse da organização.

> É importante salientar que um sistema de controle interno deve procurar atender às necessidades de acordo com os interesses da organização, lembrando que o controle deve ser o mais simples possível, porém respeitando os pilares conforme apresentado anteriormente.

2.3.2. Princípios Básicos de Controle Interno

Ainda segundo Lisboa (2012, p. 36 a 38),

> os princípios básicos para estabelecer um sistema de controles internos envolvem as necessidades da administração da organização ou empresa que será responsável pelo estabelecimento de acordo com suas necessidades, dimensões e com as informações que desejam obter. Desta forma, não devemos definir um modelo de controle, tal como um manual que pudesse ser seguido e implantado em qualquer empresa, pois isso certamente seria de grande dificuldade para a execução.
>
> Há que se levar em conta as particularidades e os detalhes específicos que são inerentes a cada organização ou empresa, de acordo com o seu ramo de atividade e porte. Mas vale ressaltar que alguns critérios e princípios mínimos básicos devem ser observados no momento da implantação para um adequado sistema de controle interno.

- Relação custo versus benefício

  Consiste na minimização da probabilidade de falhas e desvios quanto ao atendimento dos objetivos e metas. O custo do controle interno não deve exceder os benefícios que dele espera-se obter. Vale dizer que os sistemas mais sofisticados, normalmente mais onerosos, devem ser estabelecidos para transações de valores relevantes, enquanto os menos rígidos, para as transações de menor importância.

- Responsabilidade

  As atribuições dos funcionários ou setores internos da empresa devem ser claramente definidas e limitadas, de preferência por escrito, mediante o estabelecimento de manuais internos de organização.

- Rotinas internas e instruções devidamente formalizadas

  A empresa deve definir no manual de organização todas as suas rotinas internas, compreendendo atividades e funções. E para atingir um grau de segurança adequado, é indispensável que as ações, os procedimentos e as instruções sejam disciplinados e formalizados por instrumentos eficazes, ou seja, claros e objetivos, e emitidos por autoridades competentes.

- Segregação de funções

  A estrutura de um controle interno deve prever a separação entre as funções de autorização/aprovação, de operações, execução, controle e contabilização de tal forma que nenhuma pessoa detenha competência e atribuições em desacordo com este princípio.

- Controles sobre transações

  É imprescindível estabelecer o acompanhamento de fatos contábeis/financeiros e operacionais, objetivando que sejam efetuados mediante atos legítimos, relacionados com a finalidade da organização ou empresa e autorizados por quem de direito.

- Aderência às diretrizes e normas legais

  É necessária a existência, no órgão/entidade, de sistema estabelecido para determinarem e assegurarem a observância de diretrizes, planos, normas, leis, regulamentos e procedimentos administrativos internos.

- Acesso restrito e limites de alçadas

  A empresa deve limitar o acesso dos funcionários a seus ativos e estabelecer controles físicos sobre eles, obedecendo ao regimento/estatuto e organograma adequados, em que a definição de autoridades e consequentemente responsabilidades sejam claras e satisfaçam as necessidades da organização.

- Controles de acesso e salvaguarda dos ativos

  A custódia dos bens da organização ou empresa é uma das principais responsabilidades de uma administração. Evidentemente, um sistema contábil bem estruturado, sólido e que conte com pessoal suficiente é um meio eficaz de proteger os bens da organização ou empresa. Ao mesmo tempo, existem outros tipos de proteção que aumentarão a eficácia do controle interno, quais sejam as medidas físicas e intrínsecas de proteção.

- Auditoria interna e operacional

  Não adianta a empresa implantar um excelente sistema sem que alguém verifique periodicamente se os funcionários estão cumprindo o que foi determinado no sistema, ou se o sistema interno está exatamente de acordo com o grau de observância das políticas estabelecidas pela administração.
  Um controle adequado demonstra se o gerenciamento planejou sua concepção de tal maneira que forneça razoável segurança de que os riscos da organização tenham sido administrados efetivamente e que as metas da organização tenham sido atingidas eficiente e economicamente.

- Avaliação dos Controles Internos

Os controles internos devem ser avaliados observando todos os instrumentos da organização ou empresa em determinar e cumprir seu papel de vigilância, fiscalização e verificação administrativa, que permitam prever, observar, dirigir ou controlar as atividades que

acontecem na organização ou empresa e venham a produzir modificações em seu patrimônio. Marra e Franco (1992, p. 207, apud Lisboa) afirmam que:

> O principal meio de controle de que dispõe uma administração é a contabilidade. Esta, entretanto, através da escrituração, registra os fatos após sua ocorrência (controle consequência), enquanto outros meios de controle são utilizados para constatar a ocorrência no momento em que ela se verifica (controle concomitante), existindo ainda aqueles que preveem a ocorrência do fato por antecipação (controle antecedente).

Os controles internos a serem avaliados podem ter diversos meios, como registros, livros, fichas, mapas, boletins de produção, papéis, formulários, pedidos de compras, notas fiscais, faturas, documentos, guias, impressos, ordens internas, regulamentos e demais instrumentos da organização ou empresa, que formam o sistema de segurança contemplando a vigilância, fiscalização e verificação das atividades e ocorrências de todos os fatos que acontecem no dia a dia das organizações e empresas que estão relacionadas com o funcionamento e o patrimônio da organização ou empresa.

Os sistemas de controles internos podem ser avaliados utilizando:

- Fluxograma;
- Revisão analítica;
- Questionários de controles internos.

O fluxograma fornece ao auditor que está fazendo a avaliação uma visão mais completa do fluxo da documentação e das informações na organização ou empresa.

Herzmann (2009, p. 45 apud Lisboa, 2012) define revisão analítica como “a análise estatística dos controles contábeis, com o objetivo gerencial. Tem como finalidade dar segurança a respeito da exatidão do sistema contábil através da determinação da consistência e razoabilidade de variáveis estatísticas, relatórios, etc.”.

Os questionários de controles internos são um conjunto sistemático de perguntas que incorporam os pontos principais de um sistema de controle interno com o objetivo de permitir a análise dos controles. Eles têm como finalidade verificar se as instruções e normas vigentes estão sendo corretamente aplicadas e realizadas pelo setor ou pessoa responsável.

2.4. Auditoria interna

A auditoria interna surgiu com a expansão das atividades das empresas e da necessidade de maior ênfase nos controles internos e nas normas de procedimentos. Devido a essa expansão, os proprietários não poderiam supervisionar pessoalmente todas as etapas das diversas atividades do negócio. A preocupação dos dirigentes era com a fraude.

O grande salto da auditoria ocorreu após a crise econômica americana de 1929. No início dos anos 30, foi criado o Comitê May, um grupo de trabalho instituído com a finalidade de estabelecer regras para as empresas que tivessem suas ações cotadas em bolsa, tornando obrigatória a Auditoria Contábil Independente nos demonstrativos financeiros dessas empresas.

Os auditores independentes, no desenrolar de suas atividades, necessitavam ter acesso a informações e documentos que levassem ao conhecimento mais profundo e análises das diferentes contas e transações. Para tanto, foram designados funcionários da própria empresa. Estava lançada a semente de Auditoria Interna, pois os mesmos, com o decorrer do tempo, foram aprendendo e dominando as técnicas de Auditoria e utilizando-as em trabalhos solicitados pela própria administração da empresa.

As empresas notaram que poderiam reduzir seus gastos com auditoria externa, se utilizassem melhor esses funcionários, criando um serviço de conferência e revisão interna, contínua e permanente, a um custo mais reduzido. Os auditores externos, também ganharam com isso, pois puderam se dedicar exclusivamente ao seu principal objetivo que era o exame da situação econômico-financeira das empresas.

Dentro da organização, o auditor interno não deve estar subordinado àqueles cujo trabalho examina. O auditor também não deve executar atividades que possa um dia vir a examinar, para que não interfira em sua independência.

Attie (2006, p. 52 apud Lisboa, 2012) explica que:

> A importância que a auditoria interna tem em suas atividades de trabalho serve para a administração como meio de identificação de que todos os procedimentos internos e políticas definidas pela companhia, os sistemas contábeis e de controles internos estão sendo efetivamente seguidos, e todas as transações realizadas estão refletidas contabilmente em concordância com os critérios previamente definidos.

Pela atual definição do IIA (2010 apud Lélis, 2010), a auditoria interna é uma atividade independente e objetiva, que presta serviços de avaliação e consultoria e tem como objetivo adicionar valor e melhorar as operações de uma organização. A auditoria interna auxilia a organização a alcançar seus objetivos por meio de uma abordagem sistemática e disciplinada para avaliação e melhoria da eficácia dos processos de gestão de riscos, controles e governança corporativa.

Os elementos chave da definição de auditoria interna são:

- É independente e objetiva;

- Realiza atividades de avaliação e consultoria;
- Adiciona valor e melhora as operações;
- Tem uma abordagem sistemática e disciplinada para avaliar e melhorar a eficácia dos processos de gerenciamento de riscos, controle e governança.

Conforme Castanheira (2007 apud LÉLIS, 2010),

> atualmente a auditoria interna é orientada para os principais riscos corporativos. Um de seus objetivos é contribuir para que tais riscos encontrem-se nos níveis aceitos pela companhia, de modo a evitar que objetivos organizacionais não sejam alcançados devido à materialização de riscos não mitigados pelas áreas e nem cobertos pelo escopo da auditoria.

A auditoria interna cumpre um papel fundamental na empresa ao subsidiar o Comitê Executivo com dados e informações tecnicamente elaborados (a partir da aplicação de uma abordagem sistemática e disciplinada), relativos às atividades específicas da corporação, mediante o exame da:

- Adequação e eficácia dos controles;
- Integridade e confiabilidade das informações e registros;
- Integridade e confiabilidade dos sistemas estabelecidos para assegurar a observância das políticas, metas, planos, leis, normas e regulamentos, e da sua efetiva aplicação pela empresa;
- Eficiência, eficácia e economicidade do desempenho e da utilização dos recursos; dos procedimentos e métodos para salvaguarda dos ativos e a comprovação de sua existência, assim como a exatidão dos ativos e passivos;
- Compatibilidade das operações e programas com os objetivos, planos e meios de execução estabelecidos.

QUADRO 11
Auditoria externa VS. Auditoria interna

Elementos	Auditoria externa	Auditoria Interna
Profissional	Profissional independente	Funcionário da empresa
Ação e objetivo	Exame das demonstrações contábeis e trabalhos especiais.	Exame dos controles internos e operacionais
Finalidade	Opinar sobre as demonstrações contábeis	Promover melhorias nos controles internos e operacionais
Produto final	Parecer	Recomendações de controle interno e eficiência administrativa
Grau de independência	Mais amplo	Menos amplo
Interesse no trabalho	A empresa, público em geral, clientes e fornecedores, governo	A empresa
Responsabilidade	Profissional, civil e criminal	Trabalhista
Número de áreas cobertas pelo exame durante um período	Maior	Menor
Intensidade dos trabalhos em cada área	Menor	Maior
Continuidade dos trabalhos	Periódico	Contínuo

Fonte: Ibraim Lisboa (2012)

2.4.1. Natureza dos Trabalhos de Auditoria Interna

Os pronunciamentos do The IIA – The Institute of Internal Auditors definem a natureza dos trabalhos dos auditores internos, onde descrevem os serviços realizados pela Auditoria Interna.

De acordo com o pronunciamento 2100 (Natureza do Trabalho) das Normas Internacionais para a Prática Profissional de Auditoria Interna – IPPF, o trabalho de auditoria interna inclui a aplicação de uma abordagem sistemática e disciplinada para avaliar e contribuir para a melhoria da (1) adequação e (2) eficácia dos processos de governança, gerenciamento de risco e controles, além de desempenhar suas responsabilidades com qualidade. O objetivo de avaliar a adequação dos processos existentes de governança é proporcionar razoável certeza de que estes processos funcionam conforme determinado e irão possibilitar que a organização alcance suas metas e objetivos.

Quanto aos objetivos e natureza, os trabalhos de auditoria interna podem ser distribuídos como segue:

a) Auditoria de Processos – um dos principais focos da auditoria interna moderna.
   Nesta auditoria, o auditor pode realizar estudos e mapeamento de processos de negócios específicos da organização, com objetivo de validar e identificar:
   - Riscos inerentes ao negócio não mitigados por processos de controles;
   - Falhas no design de processos, excesso de trabalho manual, etc;
   - Possíveis oportunidades de melhorias de processos (eficiência, eficácia e melhoria do ambiente de controle);

b) Auditoria de Tecnologia da Informação (TI) – destina-se a avaliar os sistemas informatizados nas operações de uma organização e suas consequências e impactos no ambiente de negócios. Por se tratar de uma auditoria muito técnica, dependendo do tipo de revisão as organizações necessitam alocar auditores especiais (auditores de TI) para desenvolver o trabalho de auditoria;

c) Auditoria de Compliance – verificação da conformidade dos procedimentos em relação a padrões estabelecidos, por exemplo, políticas e procedimentos, códigos de conduta e ética, normas, etc;

d) Auditoria de Fraudes – realizada por demanda, suspeita ou preocupação relacionada a uma suposta existência de fraude, quer seja interna ou externa. Geralmente estas auditorias seguem um padrão específico de plano de trabalho, muitas vezes de caráter sigiloso;

e) Auditorias de Qualidade e Certificação – realizada para verificar se produtos, serviços, projetos, etc, seguem padrões de qualidade pré-estabelecidos e adequados, por exemplo, auditorias de certificação ISO-9000;

f) Auditorias Contábeis e Financeiras – apesar de ser uma função específica de auditores externos, é muito comum no mercado corporativo a função de auditoria interna desempenhar trabalhos de revisão de demonstrações financeiras específicos. Estes trabalhos, apesar de similares à auditoria externa, possuem objetivos distintos.
   A auditoria externa tem como seu objetivo “emitir um parecer independente sobre a veracidade e razoabilidade dos informes financeiros e contábeis das organizações”, seguindo critérios de testes por materialidade.

A auditoria interna pode perfeitamente investigar contas contábeis ou grupos de contas contábeis que não são necessariamente auditadas pela auditoria externa por não apresentarem materialidade suficiente.

g) Auditorias Ambientais, da Segurança e Saúde no Trabalho, etc.

Nota – Para praticamente todos os casos expostos acima, a auditoria externa pode utilizar os resultados dos trabalhos da auditoria interna para reduzir seu escopo de trabalho e horas de campo da organização auditada. Esta "confiança" da auditoria externa sobre os trabalhos e resultados da auditoria interna está suportada pela objetividade e independência da função de auditoria interna. Este é um fator de economia financeira para companhia auditada, e pode ser utilizado como um fator positivo para a manutenção da função de auditoria interna nas organizações.

2.4.2. Estudos Especiais

Devido à posição hierárquica da auditoria interna, subordinada diretamente ao Conselho de Administração e consequentemente elevado grau de relacionamento com a alta administração da Companhia, a Gerência da auditoria interna recebe solicitações diversas para a execução de trabalhos que podem não ser considerados do âmbito da auditoria interna.

Esses trabalhos, em geral de caráter confidencial ou prioritário para o processo de tomada de decisão, são solicitados á gerência de auditoria interna em vista da confiança depositada na mesma, nos conhecimentos que tem a companhia, e ainda, pela natureza dos trabalhos que implicam em pesquisas, levantamentos, análises contábeis, etc.

2.4.3. O processo de auditoria

De acordo com o Statement of Responsabilities of Internal Auditing, do IIA, o propósito da auditoria interna consiste em (1) examinar e avaliar as atividades da organização e (2) fornecer análises, avaliações, recomendações, conselhos e informação sobre as atividades analisadas. Em cada ação de auditoria, há um objetivo relacionado com o fornecimento dos resultados do exame e avaliação das atividades.

A atividade de auditoria engloba uma sequência de etapas, executadas por meio de procedimentos geralmente baseados em normas e padrões e com o uso de ferramentas de apoio específicas a cada tipo de trabalho. A gerência da área de auditoria é responsável pela elaboração do plano de trabalho, geralmente de periodicidade anual ou de médio prazo. O IIA

(2010 apud Lélis, 2010) recomenda que o planejamento periódico de processos e unidades auditáveis considere os riscos existentes em cada processo e seja formalmente aprovado pela área à qual a auditoria interna se subordina funcionalmente.

Um trabalho de auditoria é composto basicamente de 4 estágios:

1. Planejamento – Etapa inicial dos trabalhos de auditoria. Um bom planejamento garante que os trabalhos de auditoria possam ser executados eficiente e eficazmente para garantir que os objetivos da auditoria possam ser alcançados. Todo trabalho de auditoria deve ser previamente planejado e serve para definir a amplitude do trabalho a ser realizado de acordo com as diretrizes estabelecidas pela administração;
2. Execução do trabalho de auditoria – trata-se do trabalho de campo dos auditores internos, seguindo aquilo que foi definido durante a etapa de planejamento;
3. Comunicação dos resultados – terminado o trabalho de campo, os auditores internos comunicam formalmente a que conclusão chegaram, para a parte auditada;
4. Monitoramento da evolução das ações corretivas – Os trabalhos de auditoria interna

   resultam em ações corretivas relacionadas à área auditada, que visam melhorar processos, mitigar riscos, melhorar e implantar controles, etc. O auditado cofirma e aceita formalmente as ações corretivas reportadas pelos auditores internos, e acorda uma data de conclusão para a implantação dessas ações corretivas. A auditoria interna monitora a evolução das ações corretivas com o propósito de garantir que sejam efetivamente implantadas dentro dos parâmetros e prazos acordados.

Para execução desse trabalho podem ser utilizadas as seguintes ferramentas:

a) Questionário de controle interno;
b) Fluxogramas;
c) Descrição dos processos;

Obtido o conhecimento sobre o nível de controle existente, o auditor irá então elaborar o planejamento dos trabalhos.

Na execução dos trabalhos são efetuados testes de observância e testes substantivos:

a) Testes de Observância: visam à obtenção de uma razoável segurança de que os controles internos estabelecidos pela administração estão em efetivo funcionamento, inclusive quanto ao seu cumprimento pelos funcionários da entidade.

b) Testes Substantivos: visam à obtenção de evidência quanto à suficiência, exatidão e validade dos dados produzidos pelos sistemas de informações da entidade.

Os métodos usados na auditoria incluem os seguintes procedimentos:
- Exame físico: quantidade, existência, identificação, autenticidade, qualidade.
- Confirmação: obtenção de declaração formal e isenta de pessoas alheias à empresa.
- Exame dos documentos originais: evidências de documentos comprobatórios.
- Conferência dos cálculos: adequação das operações aritméticas.
- Exame da escrituração: constatação da veracidade das informações contábeis.
- Investigação minuciosa: profundidade dos exames da matéria auditada.
- Inquérito: formulação de perguntas e obtenção de respostas satisfatórias.
- Exame dos registros auxiliares: suporte da autenticidade dos registros principais.
- Correlação das informações obtidas: Exemplos: depreciação do imobilizado, com a conta de depreciação acumulada no resultado, receitas de vendas do balanço com as contas de impostos como ICMS ou IPI.
- Observação: constatação visual de qualquer imperfeição.

Os trabalhos realizados mediante a aplicação das técnicas descritas deverão ser devidamente formalizados nos papéis de trabalho do auditor e servirão de suporte para a elaboração do relatório com as recomendações para aprimorar os controles internos e para correção das imperfeições detectadas.

2.4.4. Auditoria Baseada em Riscos – ABR

A implementação e a operação contínua da ABR constituem-se de três estágios:

1. Avaliação da Maturidade da Gestão de Riscos da Companhia – obtenção de um panorama do quanto o conselho e a direção determinam, avaliam, manejam e monitoram os riscos. Isso dá uma indicação da confiabilidade do cadastro de riscos para fins de planejamento da auditoria.
2. Planejamento de auditorias periódicas – identificação de auditorias de garantia e consultorias para um período específico, através da identificação e priorização de todas as áreas nas quais o conselho requer a garantia objetiva, incluindo os processos de gestão de riscos, o manejo dos riscos-chave e o registro e relato dos riscos.
3. Auditorias individuais – realização de tarefas individuais baseadas em riscos, para dar garantias sobre partes do arcabouço de gestão de riscos, incluindo a mitigação de riscos individuais ou de grupos de riscos.

- **Avaliação da maturidade de riscos da Companhia**

O primeiro estágio da ABR é analisar criticamente o nível de maturidade de riscos. A abordagem da auditoria interna deverá ser compatível com o nível de maturidade de gestão de riscos implementado, visto que nem todas as organizações têm o mesmo grau de implementação de processos de gestão de risco. Os objetivos dessa análise são:

- Avaliar a maturidade de riscos da organização.
- Relatar tal avaliação à direção.
- Definir uma estratégia de auditoria.

A avaliação da maturidade é feita discutindo com diretores e gerentes sêniores sobre o entendimento que existe sobre a maturidade de riscos, o que já foi realizado para melhorar essa maturidade, tais como: treinamentos, workshops sobre riscos, enquetes sobre riscos e entrevistas com gerentes. Determinar se os gerentes acreditam que o cadastro de riscos é abrangente. Verificar se o entendimento sobre gestão de riscos está difundido de tal forma que os gerentes se sentem responsáveis não somente pela identificação, avaliação e mitigação dos riscos, mas também pelo monitoramento do arcabouço e das respostas aos riscos.

Obter documentos que detalhem todo o processo de gestão de riscos da Companhia. Através desses documentos e das informações coletadas, chegar a uma conclusão em relação à maturidade dos riscos.

QUADRO 12
Abordagem da Auditoria Interna face à maturidade de riscos

(Continua)

Maturidade de Risco	Características chave	Abordagem da Auditoria Interna
Ingênuo	Nenhuma abordagem formal desenvolvida para a gestão de riscos	Promove a Gestão de Riscos e se baseia em método alternativo de planejamento de auditorias
Consciente	Abordagem tradicional de gestão de riscos, onde cada área da organização gere seus próprios riscos	Promove um processo formal de gestão de riscos (ERM) e se baseia em método alternativo de planejamento de auditorias
Definido	Estratégia e políticas implementadas e comunicadas. Apetite por riscos (o nível de risco que a gestão decidiu aceitar) definido	Facilita a gestão de riscos/se relaciona com a gestão de riscos e utiliza a avaliação de riscos feita pela Gestão, conforme apropriado

QUADRO 12
Abordagem da Auditoria Interna face à maturidade de riscos
(Conclusão)

Maturidade de Risco	Características chave	Abordagem da Auditoria Interna
Gerenciado	Abordagem corporativa para a gestão de riscos desenvolvida e comunicada	Audita os processos de gestão de riscos e utiliza a avaliação de riscos feita pela Gestão, conforme apropriado.
Habilitado	Gestão de riscos e controles internos totalmente incorporados às operações	Audita os processos de gestão de riscos e utiliza a avaliação de riscos feita pela Gestão, conforme apropriado.

Fonte: De Cicco – 2007, pgs. 34 e 35

Relatar as conclusões sobre a maturidade de riscos para a direção e para o comitê de auditoria. Este estágio fornecerá uma garantia inicial de alto nível sobre os processos de gestão, o manejo dos riscos-chave e o registro e relato dos riscos. Um grau de maturidade de riscos ingênuo ou consciente implica que o sistema de controles internos da organização e a capacidade da direção de avaliá-lo pode ser ineficaz. Identificar com a direção ações a serem tomadas como resultado dessa avaliação.

A estratégia de auditoria selecionada depende da maturidade de riscos da organização. Organizações com maturidade de riscos ingênuo ou consciente não conseguirão implementar a ABR imediatamente. A auditoria interna pode ajudar a melhorar os processos de gestão de riscos e governança, relatando sua avaliação da maturidade de riscos da organização.

Em uma estratégia de auditoria ABR há três elementos potenciais: primeiro, o tipo de garantia que se espera dar; segundo, o arcabouço que será utilizado para o planejamento da auditoria; e terceiro, o tipo de consultoria que se espera fornecer.

Para organizações de riscos habilitado e risco gerenciado, a conclusão sobre a maturidades de riscos é o primeiro passo para garantir os processos de gestão de riscos, manejo dos riscos-chave e relato dos riscos. A estratégia de garantia da atividade de auditoria interna é dar garantia para essas áreas. Para outras organizações, a conclusão sobre maturidade de riscos significa que tais garantias não estão disponíveis.

- **Elaboração de um plano de auditorias periódicas**

A ABR não trata de auditar os riscos, mas sim auditar o manejo dos riscos. Seu foco está nos processos aplicados pela equipe de gestão às respostas a cada risco e aos processos utilizados para avaliar os riscos, monitorar essas respostas e relatá-las ao conselho.

Os objetivos de elaborar um plano de auditorias periódicas são: harmonizar todas as respostas de gestão de riscos e os processos de gestão de riscos para os quais é necessária a garantia objetiva da auditoria interna e elaborar um plano de auditoria que enumere todas as auditorias a serem realizadas durante um período especificado, normalmente 01 ano.

A avaliação da maturidade de riscos da Companhia proporcionou o embasamento necessário para a compreensão de como a direção identifica e avalia os riscos, e como e onde o restante das informações precisa ser registrado.

O cadastro de riscos mostra as respostas, as ações e os controles de monitoramento. Na ABR, a auditoria interna não cria nenhuma dessas informações, mas procura interpretá-las e usá-las para fins de planejamento.

A elaboração do plano de auditorias periódicas (plano anual) tem como etapas:

- Identificar as respostas e os processos de gestão de riscos para os quais é necessária a garantia objetiva.

QUADRO 13
Garantias de auditoria em relação às respostas dadas aos riscos

Resposta ao risco	**Processos de auditoria**
Descontinuar atividades se os riscos por elas apresentados forem muito altos ou muito caros	Planos de ação e projetos para encerrar a atividade
Tolerar os risco	Monitoramento do risco
Transferir o risco	Processos para a transferência de riscos
Tratar o risco	Estes incluem os já familiares controles contábeis e operacionais, que têm sido o foco da auditoria interna durante muitos anos

Fonte: De Cicco – 2007, pg. 15

A auditoria interna deve fornecer garantias em partes do arcabouço de gestão de riscos em si, isto é, nos processos utilizados para identificar e avaliar os riscos e para decidir quais são as respostas apropriadas; nos processos para relatar os riscos para toda a organização; e controles de monitoramento desses processos.

- Categorizar e priorizar os riscos

Se houver uma grande quantidade de riscos, deverão ser agrupados em uma ordem lógica, ajudando a compilar o plano de auditoria. Podem ser agrupados por unidade de negócio; por função ou sistemas como vendas, compras ou controle de estoque e por objetivos.

A priorização sempre é feita por referência ao tamanho dos riscos e à contribuição que a resposta dá ao manejo dos riscos. Quanto maior o risco maior a prioridade. Quanto mais a resposta reduz o risco, maior a prioridade.

- Associar riscos a tarefas de auditoria

Esta etapa irá gerar uma lista de tarefas de auditorias potenciais. A prioridade de cada auditoria tem como base o tamanho do processo de gestão de riscos para o qual ela fornece garantia.

- Elaborar o plano de auditorias periódicas

Todas as auditorias a serem incluídas no plano já devem agora ter sido determinadas. Entretanto, muitas organizações adicionam auditorias com base em outros critérios que não o de riscos. Tais critérios podem incluir áreas sujeitas a mudanças, auditorias obrigatórias ou auditorias solicitadas pela direção. Esta é uma razão para ‘verificar o sentido’ do trabalho de ABR até o momento, porque qualquer tópico que mereça uma auditoria deve ter vindo à tona através do arcabouço de gestão de riscos. Por exemplo, uma quantidade significativa de mudanças em uma área pode resultar no aumento da probabilidade de um evento de risco se materializar, e isso deve estar visível no cadastro de riscos. Se uma auditoria tiver que ser incluída devido a uma solicitação da direção, ela estará deixando de lado uma auditoria incluída com base na pontuação de riscos, e a direção deverá justificar tal substituição.

- Relatar à direção e ao comitê de auditoria

- **Realização de uma auditoria individual de garantia**

O foco da ABR recai sobre as ações tomadas pela equipe da direção para responder aos riscos. Os auditores internos precisam dedicar tempo aos gerentes, discutindo e observando os controles de monitoramento que aplicam, em vez de trabalhar controles ou outras respostas, ou analisando dados por eles mesmos.

O objetivo da realização de uma auditoria individual é dar garantia de que, em relação ao negócio, atividade ou sistema que está sendo analisado criticamente, e para o processo identificado no plano de auditoria, a direção identificou, avaliou e respondeu aos riscos acima

e abaixo do apetite por riscos; as respostas aos riscos são eficazes, mas não em excesso, no gerenciamento dos riscos inerentes, dentro do apetite por riscos; quando os riscos residuais não são compatíveis com o apetite por riscos, são tomadas ações para remediar tal situação; os processos de gestão de riscos, incluindo a eficácia das respostas e a conclusão das ações, estão sendo monitorados pela direção, para garantir que continuam operando de maneira eficaz; riscos, resposta e ações estão sendo classificados e relatados adequadamente.

As etapas para a realização de uma auditoria individual de garantia são:

- Estabelecimento do escopo planejado da tarefa

Os auditores, através da compreensão dos resultados das etapas de avaliação da maturidade de riscos da Companhia e elaboração de um plano anual de auditorias, elabora o esboço do escopo do trabalho.

- Avaliação da maturidade de riscos da unidade que está sendo auditada

Avaliação de maneira mais detalhada do que foi possível no primeiro estágio.

- Conclusões sobre a maturidade de riscos da unidade auditada

As conclusões de cada auditoria individual devem confirmar ou questionar a avaliação original no âmbito da Companhia.

Se a maturidade de riscos atual (a mr) for maior ou igual à maturidade de riscos esperada (E mr), a tarefa terá continuidade como planejado.

Se (a mr) for menor do que (E mr), a auditoria interna deve reportar isso à direção, juntamente com a conclusão de que as resposta incluídas no escopo da auditoria não estão funcionando de maneira eficaz.

- Confirmação do escopo da tarefa

A abordagem ABR deve ser divulgada pelos líderes da auditoria, ganhando a confiança da direção. Na ABR, os auditores internos precisam utilizar mais o tempo da direção do que normalmente precisariam em outras abordagens de auditoria interna.

- Discussão e observação dos controles de monitoramento

Este é o estágio inicial dos testes de auditoria. Tem o propósito de determinar se os controles utilizados pela direção, para garantir que o arcabouço de gestão de riscos esteja funcionando, são capazes de atingir esse objetivo, e demonstrar que tais controles estão funcionando como previsto.

- Verificação das evidências, explicações, reexecuções, etc

São atividades necessárias para dar evidência adicional de que as respostas aos riscos-chave estão funcionando de maneira eficaz, e para dar suporte à conclusão de que os controles de monitoramento também estão funcionando.

- Documentação dos resultados do trabalho de auditoria

Na ABR deve-se deixar claro a ligação entre riscos, respostas a riscos, garantias dadas e o trabalho feito para dar suporte a essas garantias.

- Análise da avaliação dos riscos residuais realizada pela direção

Produz conclusões sobre pontuações específicas no cadastro de riscos, e deve levar a constatações sobre como a direção determina os riscos residuais em geral. Se houver uma falha sistêmica, a auditoria interna deve garantir que ela seja refletida nas conclusões, no âmbito da organização, sobre a maturidade de riscos.

- Conclusões sobre respostas e processos de gestão de riscos cobertos pela tarefa

Engloba tanto seu desenho como quão bem estão funcionando.

- Relato e realimentação

As constatações devem ser discutidas com a direção, de forma que ela assuma a responsabilidade pela decisão em relação às ações corretivas apropriadas, incluindo toda e qualquer alteração no cadastro de riscos.

As constatações podem alterar as conclusões sobre a maturidade de riscos e podem precisar estar refletidas em todo o plano de auditoria, na próxima vez que for atualizado.

As constatações precisam estar refletidas no relato de riscos, de forma que a direção e o comitê de auditoria compreendam onde a garantia objetiva foi dada.

- **Benefícios e dificuldades da ABR**

- Conclusões claras e não ambíguas sobre a gestão de riscos

A ABR está diretamente ligada ao framework da gestão de riscos (COSO II por exemplo). Durante o estágio 1 é possível se chegar a uma conclusão sobre a maturidade de riscos da organização. Caso a maturidade não seja alta, a auditoria interna relata prontamente esse fato à direção e ao comitê de auditoria, de forma que eles possam tomar ações imediatamente.

- Contribuição direta para os objetivos da organização

Um arcabouço de gestão de riscos eficaz melhorará a governança da organização e suas chances de atingir seus objetivos de longo prazo. A metodologia da ABR dá uma contribuição clara e valiosa para o arcabouço de gestão de riscos, pois fornece garantia objetiva e facilita os

esforços da direção para melhorar esse arcabouço. Ela garante que os recursos de auditoria interna sejam direcionados à avaliação do manejo dos riscos mais significativos.

- Relação com a direção

A ABR enfatiza a responsabilidade da direção pela gestão de riscos. Isso deve ser destacado durante todas as reuniões com os gerentes. A reunião de encerramento tem menos a ver com a direção aceitar as recomendações da auditoria interna e mais a ver com a direção concordar que uma questão ou problema existe, e determinar quais ações serão tomadas e qual relato deverá ser fornecido ao próximo nível diretivo.

- Responsabilidade da direção pela gestão de riscos

A ABR pode ser implementada plenamente somente em organizações de risco habilitado e de risco gerenciado. Uma característica desse nível de maturidade de riscos é que os gerentes têm que assumir a responsabilidade pela gestão de riscos. Implementar a ABR significa que a atividade de auditoria interna comporta-se de tal maneira que reforça essa responsabilidade dos gerentes e, dessa forma, contribui para que se tenha uma cultura de gestão de riscos mais robusta.

- Conhecimentos dos auditores

Os auditores internos envolvidos na ABR necessitam de mais habilidades administrativas e para lidar com pessoas, tais como saber entrevistar, influenciar, facilitar e solucionar problemas.

A expansão do universo de auditorias para cobrir todos os riscos que ameaçam os objetivos da organização requer que o auditor interno tire conclusões sobre o desenho e a operação das respostas aos riscos em áreas que talvez sejam novas para ele.

- Uma trilha para as auditorias

A ABR amarra todos os aspectos da auditoria interna; objetivos, riscos, processos de respostas e de controles de monitoramento, testes e relatórios, conforme figura a seguir:

- **Impacto do paradigma da ABR no perfil do auditor interno**

O atual conceito de auditoria interna do IIA altera substancialmente o modo de atuação do auditor interno. O auditor deixa de focar no passado e passa a focar no futuro. Deixa de conduzir o carro olhando pelo espelho retrovisor e passa a conduzi-lo olhando pelo parabrisa.

O auditor analisa os processos de acordo com o potencial de risco. Na auditoria tradicional, os processos do negócio são verificados como algo que está dentro de um sistema de controle.

"Conduzir o carro olhando pelo espelho retrovisor" é uma metáfora que caracteriza o auditor como alguém que dá recomendações com base em análise do registro histórico das operações do sistema de controles internos. A mudança é sutil. O auditor passa a revisar os riscos e testar os controles com os quais a gestão reduz esses riscos. A pergunta "os controles sobre esses riscos são adequados e eficazes?" será substituída por "quão corretamente os riscos estão sendo gerenciados?".

Castanheira (2007, p.12) afirma que "a atual definição de auditoria interna alinha o trabalho dos auditores com os fatores críticos de sucesso das organizações e os seus processos essenciais, pelo que a mudança do conceito de auditoria interna deve ser acompanhada da mudança do perfil do auditor interno".

No atual paradigma, todo o processo de auditoria interna se baseia na gestão de risco, o que requer uma evolução técnica dos auditores internos para alterar a orientação, objetivos e resultados dos seus trabalhos. Evidentemente, esta transformação da função implica algumas alterações no perfil do auditor interno, pois deixa de ser um profissional que inspeciona e revê atuações e decisões históricas, convertendo-se num profissional qualificado, conhecedor do negócio da atividade auditada, que adquire um maior compromisso com o futuro da organização, salienta Zárate (2001 apud Castanheira, 2007).

Neves (1999 apud Castanheira, 2007) afirma que o auditor interno do "controle" apesar de ter uma grande capacidade para analisar o controle interno e identificar áreas e procedimentos de risco potencial, não deixa de ser um auditor interno conservador e avesso ao risco. Por outro lado, o auditor interno do "risco" tem que conhecer a atividade aos vários níveis e saber identificar os riscos que podem ameaçar os objetivos estratégicos.

Castanheira (2007) afirma que, atualmente todos os auditores internos necessitam de ter um pensamento lógico, conhecer o negócio da empresa, ter habilidade para investigar e flexibilidade. O desenvolvimento profissional contínuo é fundamental para que possam acompanhar as alterações nas práticas de negócio.

QUADRO 14
Comparação entre o velho e o novo

Área de Auditoria	Velho Paradigma	Novo Paradigma
Foco da auditoria	Sistema de controles internos	Riscos do negócio
Foco dos testes	Atividades de controle	Atividades de tratamento de todos os riscos
Foco do relatório	Adequação e eficácia dos controles internos	Adequação e eficácia do tratamento dos riscos
Resultados da auditoria	Controles novos ou melhorados	Tratamento adequado dos riscos

Fonte: David Mc Namee (1997 apud Francesco De Cicco 2006)

Conforme David Mc Namee (1997 apud Francesco De Cicco 2006) a ABR começa e acaba com a consideração dos riscos do negócio. Os controles internos são uma parte importante do tratamento de riscos, mas não são a solução completa. Os auditores tenderão a notar e recomendar o nível apropriado de controle e de outros meios para reduzir os riscos.

3. Metodologia

Quanto aos objetivos, esta pesquisa foi exploratória e descritiva, uma vez que busca explorar os termos e conceitos utilizados, descrevendo-os no contexto organizacional. No tocante aos procedimentos, refere-se a uma pesquisa bibliográfica. A pesquisa utiliza fontes secundárias. O estudo é suportado por uma análise qualitativa dos dados.

A pesquisa foi on-line conduzido em novembro e dezembro de 2011 pela PricewaterhouseCoopers Serviços Profissionais Ltda. A Pesquisa sobre a Situação da Profissão de Auditoria Interna em 2012 foi realizada com 1.530 executivos de 16 setores e 64 países. Compartilharam seus pontos de vista 660 stakeholders e 870 diretores de auditoria. Além disso, cerca de 100 diretores de auditoria e outros stakeholders participaram de entrevistas presenciais. As entrevistas foram feitas com executivos de organizações dos EUA, Oriente Médio, Índia, Canadá, Austrália, África do Sul e Suíça. A maioria (57%) dos participantes era constituída por diretores de auditoria. Os demais eram membros de comitês de auditoria, diretores financeiros, controladores de riscos, diretores de compliance e diretores jurídicos. A pesquisa abrangeu um amplo leque de setores, nenhum dos quais representou mais de 15% da amostra total. Mais da metade dos participantes da pesquisa trabalha em empresas sediadas nos EUA. Os demais estão espalhados por outros 64 países. Cerca de 75% dos pesquisados estavam ligados a empresas com faturamento superior a US$ 1 bilhão de dólares, sendo que 18% eram de companhias com vendas anuais de pelo menos US$ 20 bilhões.

O estudo destaca as expectativas crescentes dos stakeholders e como eles desejam que a auditoria interna participe do desafio da gestão de riscos para oferecer o máximo de benefícios ao negócio. Tanto os stakeholders quanto os diretores de auditoria reconheceram que, para que a auditoria interna seja eficiente no apoio aos esforços organizacionais de gestão de riscos, o padrão mínimo de desempenho precisa aumentar. A auditoria interna não pode se contentar em simplesmente reagir aos eventos. Ela precisa adotar uma mentalidade estratégica de reação aos riscos e que ajude a preparar a organização para novas ameaças e oportunidades.

Dos 1.530 entrevistados, a esmagadora maioria (80%) afirmou que os riscos para sua organização estão aumentando. Os 15 riscos críticos mencionados com maior frequência pelos entrevistados foram:

- Incerteza econômica;
- Regulamentação e políticas governamentais;

- Concorrência;
- Mercados financeiros;
- Sigilo e segurança dos dados;
- Talento e mão de obra;
- Reputação e marca;
- Mudanças no mercado comercial;
- Custos de energia e commodities;
- Gastos públicos e tributação;
- Lançamento de produtos;
- Fraudes e ética;
- Continuidades dos negócios;
- Fusões, aquisições e joint venture;
- Riscos de grandes projetos.

Menos da metade (45%) dos pesquisados afirmaram estar confortáveis com a forma como seus riscos mais críticos estão sendo administrados. Os pesquisados identificaram os riscos associados a talento e mão de obra como significativos, mas apenas 23% mostraram confiança na capacidade de suas organizações para administrá-los bem. 33% dos diretores de auditoria sentem que os riscos de fusões e aquisições são bem administrados.

- **A necessidade de conciliar a área de negócios com a auditoria interna**

Ouvir os stakeholders na pesquisa permitiu comparar seus pontos de vista com os dos diretores de auditoria em um nível macro. Essas visões macro fornecem dados indicativos sobre áreas nas quais o entendimento está sendo atingido e aquelas em que é necessário maior diálogo entre os stakeholders e os diretores de auditoria.

Para que a auditoria interna seja realmente eficiente, a organização deve criar uma cultura que promova o diálogo sobre os riscos da empresa entre os stakeholders e o diretor de auditoria. Com isso chegarão a um consenso sobre o papel da auditoria interna em relação aos riscos mais críticos, para a alocação eficiente de recursos. Na ausência desse entendimento, os diretores de auditoria podem deixar de alocar recursos às áreas consideradas mais importantes pelos stakeholders, perdendo assim a oportunidade de adicionar valor ao negócio.

- **Tamanho e setor são importantes**

Entrevistados de todos os tipos de empresas demonstraram níveis de confiança relativamente baixos na gestão de riscos. A análise do resultado por empresa mostra que o tamanho da organização afeta essa percepção. Nas empresas com faturamento igual ou superior a US$ 10 bilhões, a confiança dos entrevistados na gestão de riscos de suas organizações era 20% maior do que naquelas com faturamento inferior. Essa constatação da pesquisa mostra que empresas maiores têm processos e ferramentas mais avançados para vencer seus desafios de gestão de riscos. Apesar disso, a gestão eficiente dos riscos não é menos importante em empresas médias e de menor porte.

Aparentemente, o porte da organização é importante, mas a questão para os diretores de auditoria de grandes e pequenas empresas é saber quais esforços adicionais a auditoria interna deve fazer para promover a confiança na gestão de riscos. As especificidades do papel da auditoria interna podem diferir segundo o porte da empresa, mas a necessidade de agir continua a mesma.

Na figura abaixo, uma classificação dos três riscos com melhor e pior gerenciamento por grupo setorial:

Serviços financeiros	*CIPS**	*Saúde*	*TICE***
Pior gerenciamento			
• Talento e mão de obra • Gastos públicos e tributação • Risco de grandes projetos	• Talento e mão de obra • Risco de grandes projetos • Continuidade dos negócios	• Talento e mão de obra • Continuidade dos negócios • Fraudes e ética	• Talento e mão de obra • Continuidade dos negócios • Lançamento de produtos
Melhor gerenciamento			
• Mercados financeiros • Sigilo e segurança de dados • Concorrência	• Mercados financeiros • Concorrência • Reputação e marca	• Reputação e marca • Regulamentação e políticas governamentais • Gastos públicos e tributação	• Concorrência • Regulamentação e políticas governamentais • Mercados financeiros

* Produtos e serviços industriais para consumidores
** Tecnologia, informação, comunicações e entretenimento

FIGURA 6: Riscos com melhor e pior gerenciamento por grupo setorial
Fonte: Pesquisa PricewaterhouseCoopers – 2012, p.13

As empresas líderes diferenciam-se na arena da gestão de riscos por deixarem para trás uma mentalidade reativa e assumirem uma postura proativa, que prevê os riscos e ajuda a

posicionar a organização para enfrentar novas ameaças e tirar proveito das novas oportunidades.

- **Expectativas dos stakeholders em relação à auditoria interna**

Durante as entrevistas, ouviu-se diversas vezes que os stakeholders valorizam a capacidade da auditoria interna de identificar riscos, avaliar a ameaça que representam e recomendar processos e controles para gerenciá-los.

Os resultados da pesquisa mostraram que os stakeholders estabelecem como sua primeira expectativa a função tradicional da auditoria interna de auditar os controles financeiros e a conformidade, mas que a assessoria sobre riscos e controles vem bem perto, em segundo lugar.

69% dos stakeholders consideram muito importante a contribuição da auditoria interna para o monitoramento dos riscos de sigilo e segurança dos dados.

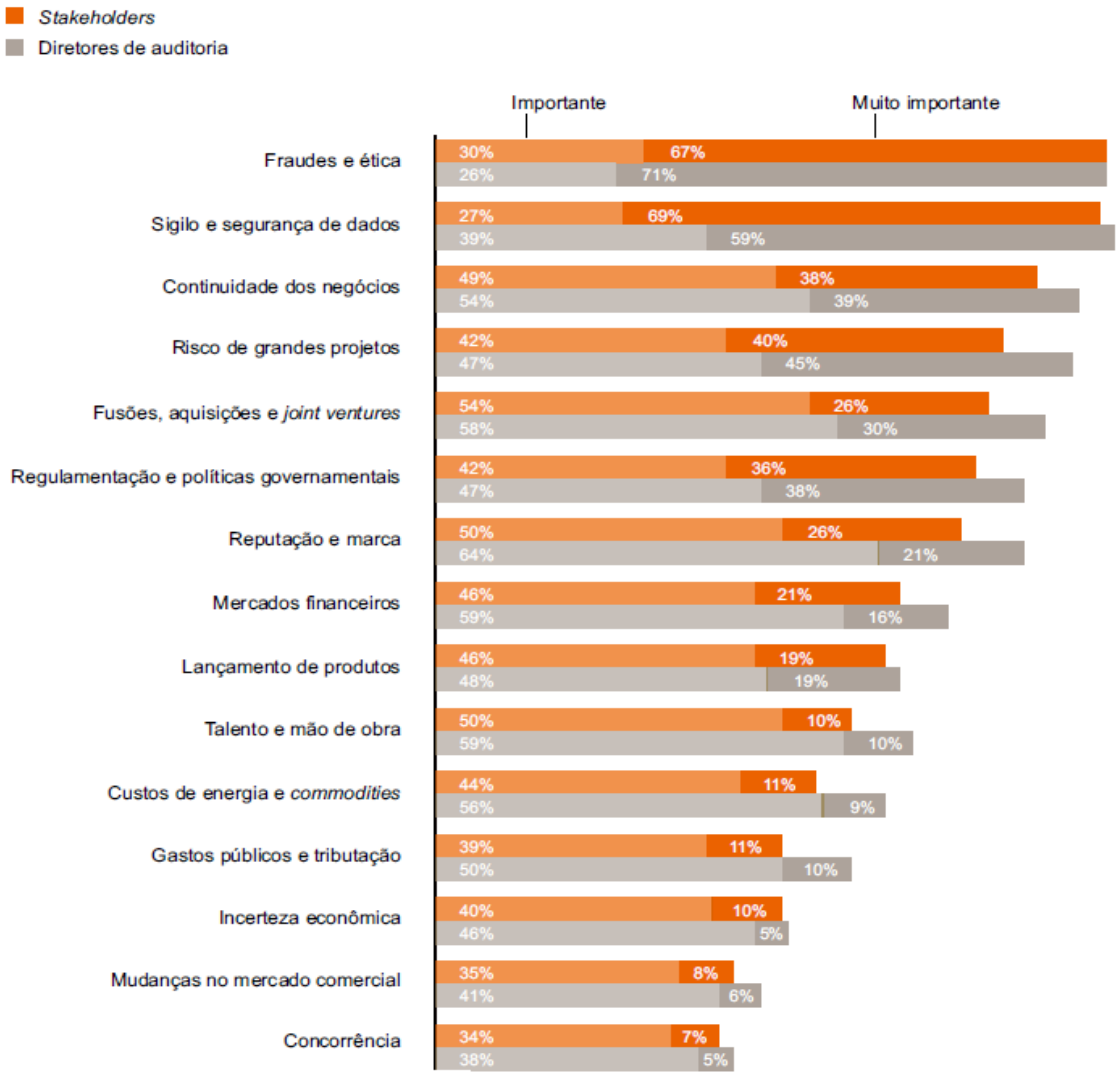

GRÁFICO 1: Importância da contribuição da auditoria interna para o monitoramento de cada risco
Fonte: Pesquisa PricewaterhouseCoopers – 2012, p.15

- **Os stakeholders valorizam a contribuição da auditoria interna**

Entre os participantes que selecionaram fraudes e ética e sigilo e segurança dos dados como seus principais riscos, 97% e 96% (respectivamente) valorizam a contribuição da auditoria interna.

Mais de três quartos dos pesquisados que classificaram continuidade dos negócios, risco de grandes projetos, fusões e aquisições, regulamentação e políticas governamentais e reputação e marca entre seus principais riscos também deram importância elevada à contribuição da auditoria interna para monitorá-los. Apenas duas áreas de risco (mudança no mercado comercial e concorrência) em que menos de 50% dos stakeholders encaram o papel da auditoria interna como importante. Conclusão: a maioria dos stakeholders espera que a

auditoria interna esteja ativamente engajada em auxiliar a organização a monitorar e gerenciar seus riscos mais críticos.

Mais de 20% dos stakeholders informaram que a auditoria interna dava pouca atenção à grande maioria dos riscos pesquisados, conforme figura a seguir:

GRÁFICO 2: Riscos que recebem pouca atenção da auditoria interna
Fonte: Pesquisa PricewaterhouseCoopers – 2012, p.17

- **Os stakeholders querem atenção para todas as áreas críticas de risco**

A demanda por maior atenção geral foi constatada nos resultados da pesquisa, com 65% dos stakeholders respondendo que desejam um papel de maior destaque da auditoria interna no monitoramento dos riscos. Sobre as áreas específicas nas quais desejam que a auditoria interna mantenha, aumente ou reduza seu foco, praticamente nenhum dos stakeholders respondeu que a auditoria interna deve reduzir a atenção dada às principais áreas de risco. Isso indica uma crescente espectativa dos stakeholders em relação à auditoria interna, em um cenário de risco sempre crescente e em constante mudança.

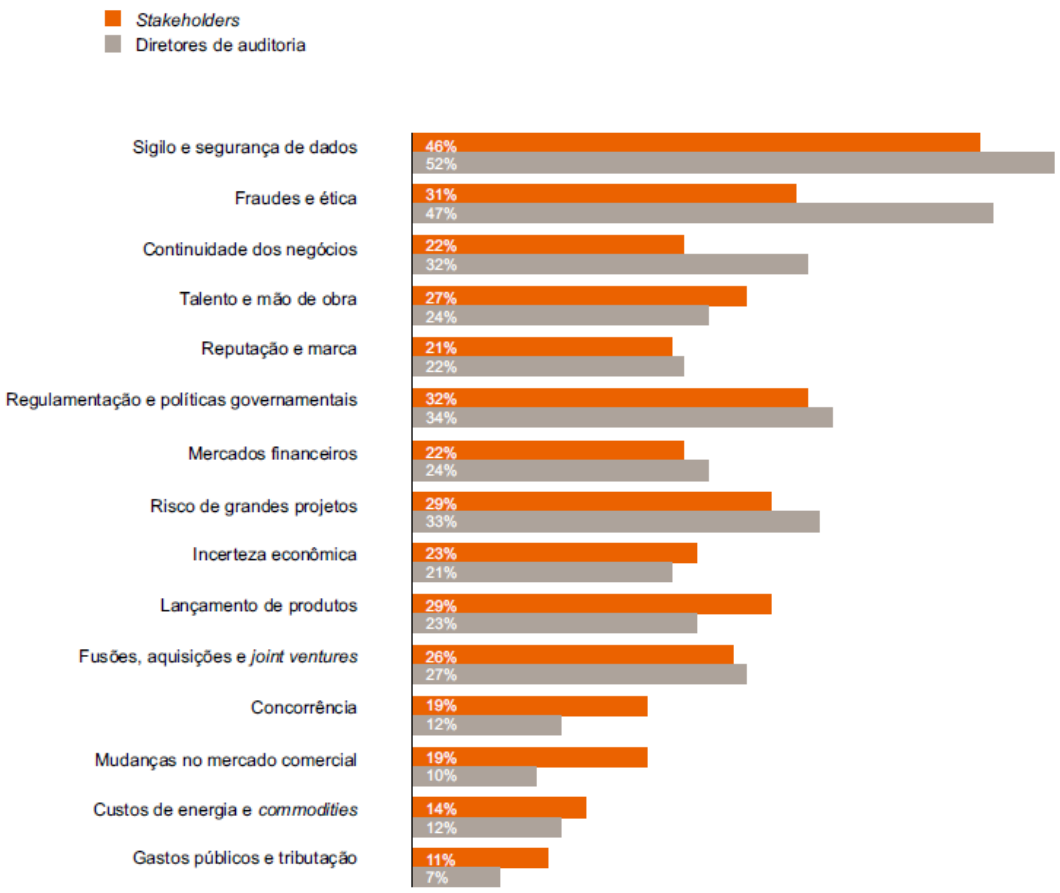

GRÁFICO 3: Áreas de risco nas quais os stakeholders e os diretores de auditoria desejam/planejam aumentar a capacidade da auditoria interna.
Fonte: Pesquisa PricewaterhouseCoopers – 2012, p.19

- **Os stakeholders querem linhas de defesa coordenadas**

Podemos nos referir à gestão de riscos como "linhas de defesa", as várias camadas de atividades que ajudam a assegurar que os riscos sejam gerenciados e monitorados de forma eficaz e eficiente, segundo os interesses de executivos e não executivos.

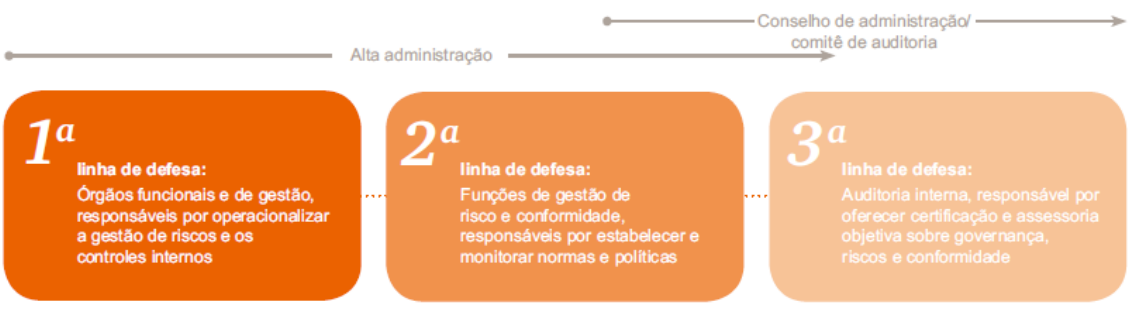

FIGURA 7: três linhas de defesa
Fonte: Pesquisa PricewaterhouseCoopers – 2012, p. 20

Como terceira linha de defesa, a auditoria interna avalia, para o conselho de administração e o comitê de auditoria, o funcionamento dos processos de governança, risco e conformidade da organização – em especial a primeira e a segunda linhas de defesa.

74% das organizações pesquisadas disseram ter grupos formais de gestão de riscos empresariais, mas menos de 50% acreditam que exista boa coordenação entre a auditoria interna e esses grupos. À medida que as áreas de gestão de riscos tomam forma, os diretores de auditoria e os stakeholders devem buscar um acordo sobre a atuação da auditoria. Esses acordos permitirão que a auditoria interna se envolva melhor na identificação dos riscos, na condução de avaliações de risco mais completas e, em última análise, a posicionará para desempenhar um papel de mais destaque nos esforços de gestão de riscos como um todo.

- **Os stakeholders querem um ponto de vista esclarecedor e objetivo**

A maioria, 88% dos stakeholders classificou "controles financeiros e garantia de conformidade" entre suas três principais expectativas em relação à auditoria interna. "Prestar assessoria sobre riscos e controles" recebeu de 82% dos pesquisados como entre as três principais funções da auditoria.

Durante as entrevistas, ficou comprovado que os stakeholders estão buscando visões mais esclarecedoras da auditoria interna. Além de assegurar a adoção de níveis de controle adequados para atenuar os riscos, os auditores devem também ter conhecimentos profundos para recomendar controles.

Além de auditoria e análises, a pesquisa também mostrou que a característica mais valorizada pelos stakeholders na auditoria interna é a objetividade (citada entre as três mais valiosas por 85% dos stakeholders).

- **Novo nível da auditoria interna**

As conversas com os stakholders e diretores de auditoria indicaram a importância de oito atributos centrais que contribuem para a eficiência da função de auditoria interna, independentemente de seu escopo ou tamanho, conforme figura a seguir:

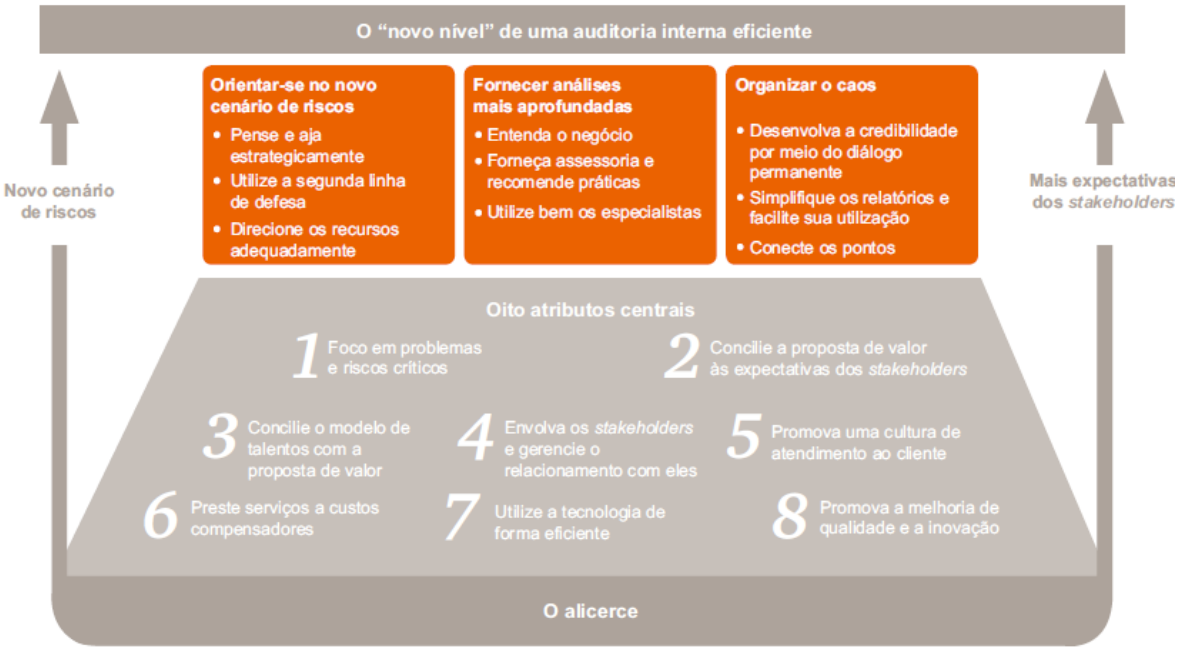

FIGURA 8: Ascensão para o novo nível
Fonte: Pesquisa PricewaterhouseCoopers – 2012, p. 23

- **Oriente-se no novo cenário de riscos**

A pesquisa indicou que apenas 55% das organizações, aproximadamente, criam planos de auditoria e alocam recursos usando uma abordagem vertical avançada para a avaliação dos riscos.

O melhor planejamento vertical, baseado em riscos, começa com a busca do ponto de vista da administração sobre suas principais prioridades, identifica os riscos associados e prossegue com uma análise meticulosa de como a auditoria interna pode incorporá-los de modo eficiente a seus planos.

4. Considerações Finais

Neste trabalho, estudou-se o conceito de Auditoria Interna Baseada em Riscos - ABR e a relação entre controle interno, gestão de riscos e governança corporativa. O referencial teórico utilizado serviu de embasamento para melhor compreensão desses conceitos.

Evidenciou-se a evolução do paradigma da auditoria interna, comparando as práticas da auditoria interna baseadas no controle às práticas baseadas no risco. O IIA define como um dos objetivos da auditoria interna a avaliação e a melhoria da eficácia dos processos de gestão de riscos, controles e governança corporativa. A descrição da gestão de riscos na prática permitiu associar a teoria à prática da gestão de riscos.

Finalmente, através de pesquisa com fonte secundária, destacou-se o nível de atuação esperado da auditoria interna, frente a um cenário complexo de riscos, expectativas elevadas dos stakeholders e recursos restritos. A auditoria interna precisa atuar em um novo nível, direcionando o monitoramento de riscos e a auditoria com base em avaliações de cima para baixo dos riscos estratégicos, concentrando recursos nos riscos críticos, fornecendo análises mais aprofundadas e usando técnicas eficientes de comunicação.

A internacionalização e globalização da economia, o aumento da competitividade e as constantes alterações no ambiente de negócios aumentaram os esforços de gestão de riscos das organizações. Na pesquisa apresentada, menos da metade dos participantes consultados estão satisfeitos com a forma como os riscos mais críticos de suas empresas estão sendo gerenciados, entre eles, a incerteza econômica, a regulamentação crescente e as ameaças à segurança de dados.

Nesse contexto, os auditores internos estão sendo exigidos pelas empresas para que elevem seus padrões de desempenho para apoiar os esforços de gestão de riscos da organização. Atualmente, os auditores internos além de auditar controles financeiros e garantir a conformidade com as regulamentações, devem fornecer assessoria sobre riscos e os controles adotados para monitorá-los.

Na sequência deste estudo, visando ampliar a base de conhecimentos sobre a Auditoria Baseada em Riscos – ABR, sugere-se a realização de trabalhos que avaliem a implantação da ABR em termos de contribuição para a realização dos objetivos de negócio da empresa.

Outro ponto a ser estudado seria o estágio de desenvolvimento da auditoria interna baseada em riscos nos diversos segmentos da economia brasileira.

REFERÊNCIAS BIBLIOGRÁFICAS

ANDRADE, Adriana; ROSSETTI, José Paschoal. **Governança corporativa:** fundamentos, desenvolvimento e tendências. 4. Ed. São Paulo: Atlas, 2009.

BEUREN, Ilse Maria. **Como Elaborar Trabalhos Monográficos em Contabilidade:** teoria e prática. São Paulo: Atlas, 2004.

BOYNTON, William C.; JOHNSON, Raymond N.; KELL, Walter G. Auditoria. São Paulo: Atlas, 2002.

CASTANHEIRA, Nuno. Auditoria interna baseada no risco. 2007. 147f. Dissertação (Mestrado em Contabilidade e Auditoria) – Escola de Economia e Gestão, Universidade do Minho, Portugal.

CICCO, Francesco De. **AUDITORIA BASEADA EM RISCOS.** Como implementar a ABR nas organizações: uma abordagem inovadora. São Paulo: Risk Tecnologia Editora Ltda, 2007.

COSO (Committee of Sponsoring Organizations of the Treadway Commission). **Gerenciamento de Riscos Corporativos:** estrutura integrada. 2 Volumes. New York: COSO, 2007.

Ernest & Young. **Capacitação Gestão de Riscos Corporativos.** Belo Horizonte: 2013.

Ernest & Young. **Reforço – Capacitação Gestão de Riscos Corporativos.** Belo Horizonte: 2014.

http://www.ibgc.org.br/inter.php?id=18161/governanca-corporativa. Acesso em: 02 jul. 2014

LÉLIS, Débora Lage Martins. *Percepção de auditores e auditados sobre as práticas de auditoria interna em uma empresa do setor energético*. 2010. 182f. Dissertação (mestrado) – UFMG, FACE, CEPCON, Belo Horizonte, 2010.

LISBOA, Ibraim. O papel da auditoria interna na prevenção de riscos. Disponível em: http://www.portaldeauditoria.com.br/artigos/O-Papel-da-Auditoria-Interna-na-Prevencao-de-Riscos.html. Acesso em: 12 jul. 2014.

LISBOA, Ibraim. **Auditoria Interna Operacional:** Teoria e prática para execução eficaz.Maph Editora. Ebook. Distribuição: Portal de Auditoria (www.portaldeauditoria.com.br) e Maph Editora (www.maph.com.br). [2012]

PAULA,Maria Goreth Miranda Almeida. **Auditoria Interna**: Embasamento Conceitual e Suporte Tecnológico. São Paulo: Ed. Atlas, 1999

PRICEWATERHOUSECOOPERS Serviços Profissionais Ltda. **Posicionamento da auditoria interna:** Estudo sobre a Situação da Profissão de Auditoria Interna em 2012. Disponível em:http://www.pwc.com.br/pt_BR/br/publicacoes/servicos/assets/auditoria/posi-cionamento-auditoria-interna-12.pdf. Acesso em: 02 ago. 2014.