UNIVERSIDADE FEDERAL DO PARANÁ

ANDRÉ KUCEK

PROPOSTA DE METODOLOGIA DE DEFINIÇÃO E AVALIAÇÃO DE CONTROLES INTERNOS EM EMPRESAS DE GRANDE PORTE

CURITIBA
2015

UNIVERSIDADE FEDERAL DO PARANÁ

ANDRÉ KUCEK

PROPOSTA DE METODOLOGIA DE DEFINIÇÃO E AVALIAÇÃO DE CONTROLES INTERNOS EM EMPRESAS DE GRANDE PORTE

Monografia apresentada ao Programa do Curso de Pós-Graduação do Departamento de Contabilidade do Setor de Ciências Sociais Aplicadas da Universidade Federal do Paraná como requisito para obtenção do título de especialista em Auditoria Integral.

Prof.ª. Orientadora Márcia M. S. Bortolocci Espejo

CURITIBA
2015

RESUMO

KUCEK, André. **Proposta de metodologia de definição e avaliação de controles internos em empresas de grande porte.** A gestão de riscos e a implementação de controles capazes de mitigá-los são temas de grande relevância para a governança corporativa, e ganharam espaço principalmente após a criação da lei norte-americana Sarbanes-Oxley, em 2002, conhecida como SOX. Dessa forma, guias metodológicos destinados à definição de boas práticas na gestão de controles internos, como o *Internal Controls - Integrated Framework* publicado pelo COSO, ganharam visibilidade. As empresas então, cada vez mais, passaram a buscar maneiras de implementar de forma efetiva as premissas definidas nos guias metodológicos. Sendo assim, este trabalho propõe uma metodologia para definição e avaliação de controles internos que possa ser implementada de maneira geral em empresas de grande porte, definindo as principais etapas de execução e as ferramentas necessárias, de forma exploratória.

Palavras-chave: risco, controle interno, auditoria, metodologia de controles internos, COSO.

LISTA DE TABELAS

TABELA 1 - TAMANHO DA AMOSTRA DE TESTE.....53

LISTA DE FIGURAS

FIGURA 1 – MACRO-FLUXO DA METODOLOGIA DE CONTROLES INTERNOS..29
FIGURA 2 – MODELO DE FLUXOGRAMA.....44
FIGURA 3 – LEGENDAS DO FLUXOGRAMA.....45
FIGURA 4 – MATRIZ DE CRITICIDADE DAS INEFETIVIDADES.....59

SUMÁRIO

1. INTRODUÇÃO 6
1.1. PROBLEMA DE PESQUISA 6
1.2. OBJETIVOS 6
1.2.1. Objetivos gerais 6
1.2.2. Objetivos específicos 7
1.3. JUSTIFICATIVA 7
1.4. ESTRUTURA DO TRABALHO 8
2. REFERENCIAL TEÓRICO 9
2.1. RISCO 9
2.2. CONTROLE INTERNO 10
2.3. FRAUDE 16
2.4. LEI SARBANES-OXLEY (SOX) 17
2.5. *INTERNAL CONTROL - INTEGRATED FRAMEWORK* 20
2.6. MAPEAMENTO DE PROCESSOS 23
2.6.1. Entrevistas 24
2.6.2. Elaboração do fluxo macro 24
2.6.3. Elaboração dos fluxos detalhados dos processos 24
2.6.4. Identificação dos pontos de controle, riscos e problemas 24
2.7. KPI - *KEY PERFORMANCE INDICADOR (*INDICADOR-CHAVE DE PERFORMANCE) 25
3. METODOLOGIA 27
3.1. CLASSIFICAÇÃO DA PESQUISA 27
3.2. PROCEDIMENTOS METODOLÓGICOS 27
4. PROPOSTA DE METODOLOGIA DE CONTROLES INTERNOS 29
4.1. DIRECIONAMENTO E ESTRUTURA DE CONTROLES INTERNOS 32
4.2. DEFINIÇÃO DO ESCOPO 37
4.3. MAPEAMENTO DOS PROCESSOS 40
4.3.1. Preparação para o mapeamento 41
4.3.2. Mapeamento 41
4.3.3. Teste de desenho 42
4.4. IDENTIFICAÇÃO DE RISCOS E CONTROLES 43
4.4.1. Fluxograma 44
4.4.2. Matriz de riscos e controles 45
4.5. CLASSIFICAÇÃO DOS CONTROLES 50
4.5.1. Categorias de controle 50
4.5.2. Tipos de controle 52
4.5.3. Frequências de controle e amostra para teste de efetividade 53
4.6. DEFINIÇÃO DOS PROCEDIMENTOS E VALOR DOS TESTES DE CONTROLE 54
4.7. VALIDAÇÃO DO MAPEAMENTO E DA MATRIZ DE RISCOS E CONTROLES 54
4.8. AVALIAÇÃO DOS CONTROLES INTERNOS 55
4.8.1. Definição das amostras de teste 55
4.8.2. Autoavaliação de cada departamento 56
4.8.3. Avaliação pelo departamento de controles internos 57
4.9. PLANOS DE REMEDIAÇÃO 58
4.9.1. Classificação das inefetividades 58
4.9.2. Definição dos planos de remediação 59

4.10. IMPLEMENTAÇÃO DOS PLANOS DE REMEDIAÇÃO 60
4.11. REAVALIAÇÃO DOS CONTROLES INEFETIVOS 60
4.12. REDEFINIÇÃO DOS PLANOS DE REMEDIAÇÃO 61
4.13. CÁLCULO E REPORTE DOS RESULTADOS 61
4.13.1. Reporte dos resultados aos departamentos 63
4.13.2. Reporte dos resultado à alta administração 63
4.14. APLICAÇÃO DA MERITOCRACIA 63
4.15. NOVO CICLO DA METODOLOGIA 64
5. CONSIDERAÇÕES FINAIS E RECOMENDAÇÕES 66
REFERÊNCIAS BIBLIOGRÁFICAS 68

1. INTRODUÇÃO

Diante de diversos crimes relacionados à manipulação das demonstrações financeiras ocorridos nos últimos anos, a importância dos controles internos em uma organização vem sendo ressaltada, tanto pelos órgãos reguladores através de exigências legais, quanto nas próprias auditorias externas das demonstrações financeiras. Um exemplo disso é a criação da Lei Sarbanes-Oxley em 2002 nos Estados Unidos, que obriga todas as empresas de capital aberto com comercialização de ações nas bolsas de valores norte-americanas a atestar que seus controles internos proporcionam um grau de confiabilidade adequado às suas demonstrações financeiras. Esta iniciativa serviu como base para que outros países também passassem a regulamentar a efetividade dos controles internos, como o Japão, que aprovou a Lei “Financial Instruments Exchange” em 2008, conhecida como J-SOX.

Neste cenário, criou-se a demanda por parte de diversas grandes empresas de implementação de um modelo para definição e avaliação de controles internos, que tanto atendesse às regulamentações necessárias, quanto proporcionasse uma melhoria contínua na eficácia e eficiência operacional, agregando valor ao negócio. Neste contexto, este trabalho busca definir uma proposta com as principais diretrizes e etapas de uma metodologia para definição e avaliação de controles internos em uma empresa de grande porte, de modo a incorporar tanto os fundamentos tradicionais de auditoria interna, quanto um modelo que possibilite a otimização dos processos organizacionais.

1.1. PROBLEMA DE PESQUISA

Diante dos diversos desafios para implementar um método que proporcione uma maneira adequada de gerir riscos e agregar valor aos processos, quais são as etapas de trabalho e as principais ferramentas necessárias para a efetiva definição e avaliação de controles internos em uma empresa de grande porte?

1.2. OBJETIVOS

1.2.1. Objetivos gerais

Descrever uma metodologia para a definição e a avaliação contínua de controles internos em uma empresa de grande porte.

1.2.2. Objetivos específicos

- Determinar as etapas de trabalho para a definição e a avaliação contínua de controles internos em uma empresa de grande porte.
- Definir as responsabilidades das áreas de negócio para implementação da metodologia.
- Determinar os principais papéis de trabalho a serem utilizados para implementação da metodologia.

1.3. JUSTIFICATIVA

A efetiva implementação de controles internos é capaz de proporcionar maior confiabilidade para as demonstrações financeiras, adequação às leis e regulamentações aplicáveis ao negócio, reduzir os riscos de fraude e gerar maior eficiência e eficácia operacional. Dessa forma, as empresas que forem capazes de gerir de melhor maneira seus controles internos, tendem a gerar maior vantagem competitiva, bem como reduzir o grau dos diversos riscos aos quais ela está sujeita. Além disso, percebe-se a existência de uma série de publicações e livros nesta área de estudo que definem as melhores práticas e as premissas a serem adotadas para criar uma metodologia de controles internos, como "Gestão de Riscos e Controles Internos", de Marcos Assi, "Manual de Controles Internos", de Sergio Vidal dos Santos Dias e "Gestão: controle interno, risco e auditoria", de Antônio Loureiro Gil, Carlos Hideo Arima e Wilson Toshiro Nakamura. Contudo não é tão comum encontrar pesquisas que abordem aspectos mais práticos, ou seja, que desdobrem os conceitos e proponham um fluxo de trabalho, envolvendo as principais ferramentas, responsabilidades de cada departamento e etapas de trabalho. Sendo assim, este trabalho busca preencher uma lacuna entre as boas práticas consagradas para controles internos e sua operacionalização efetiva nas grandes empresas.

1.4. ESTRUTURA DO TRABALHO

No primeiro capitulo deste trabalho constam a introdução, o problema da pesquisa, os seus objetivos e a estrutura do trabalho. Desta forma, nele expõe-se o que se espera atingir com sua execução, bem como as motivações para a definição do tema.

No segundo capítulo consta o referencial teórico do trabalho, envolvendo as definições de risco, controle interno, fraude, lei Sarbanes-Oxley, *Internal Control - Integrated Framework* (COSO), mapeamento de processos e KPI (indicadores chave de desempenho). Através destas torna-se possível embasar a metodologia de definição e avaliação de controles internos em empresas de grande porte, que representa o principal objetivo do trabalho.

No terceiro capítulo consta a metodologia para execução do trabalho, envolvendo a classificação da pesquisa e a descrição dos procedimentos metodológicos utilizados.

O quarto capítulo consiste na proposta de metodologia para definição e avaliação de controles internos em empresas de grande porte. Este está dividido entre as principais etapas para implementação da metodologia.

Por fim, no quinto e último capítulo constam as conclusões obtidas com o desenvolvimento do trabalho e recomendações para a execução de trabalhos futuros.

2. REFERENCIAL TEÓRICO

2.1. RISCO

Segundo o IBGC (2007), através de sua publicação “Guia de Orientação para Gerenciamento de Riscos Corporativos”, o termo risco é proveniente para palavra *risicu* ou *riscu*, em latim, que significa “ousar” e está comumente associado à chance de “algo não dar certo”. Seu conceito atual o relaciona à quantificação e qualificação da incerteza, tanto na perspectiva das perdas quanto dos ganhos. Dessa forma, o IBGC, ainda na mesma publicação, descreve:

> O risco é inerente a qualquer atividade na vida pessoal, profissional ou nas organizações, e pode envolver perdas, bem como oportunidades. Em finanças, a relação risco-retorno indica que quanto maior o nível de risco aceito, maior o retorno esperado dos investimentos. Esta relação vale tanto para investimentos financeiros quanto para os negócios, cujo “retorno” é determinado pelos dividendos e pelo aumento do valor econômico da organização. (IBGC; 2007; p.11).

Pode-se perceber que a conceituação de risco do IBGC articula em torno de uma perspectiva de expectativa de retorno através da aceitação de determinado risco, uma aposta, que está diretamente relacionada a uma forma de investimento. Contudo, conforme Assi (2012), o risco é a possibilidade de haver um acontecimento incerto, fortuito (ou acidental, que não dependa da vontade da empresa) e danoso (sendo necessária a ocorrência de perda). O autor cita como exemplo a possibilidade de cortar o dedo com uma faca de plástico, o que pode parecer impossível.

Vale citar ainda que o risco é inerente à atividade de negócios, e dessa forma a capacidade de compreendê-los e administrá-los, bem como a disposição a correr riscos, são elementos-chave (IBGC, 2007). Neste contexto encaixa-se o papel da gestão de riscos, através das medidas preventivas adotadas por uma empresa.

Segundo o COSO (2013), uma entidade encara uma variedade de riscos, de fontes internas e externas, sendo risco definido como a possibilidade de que um evento ocorra e cause um efeito adverso para o atingimento dos objetivos. Neste cenário, atrelando-se o fato de que o risco é inerente ao negócio, é crescente a discussão a cerca da avaliação de riscos. Segundo o COSO, ela é um processo dinâmico e interativo, que visa identificar e avaliar os riscos para o atingimento dos objetivos. Dessa forma, ela forma a base para uma empresa determinar como os riscos serão gerenciados.

> O estabelecimento de objetivos nos diversos níveis organizacionais é um pré-requisito para a avaliação de riscos. A gerência determina os objetivos entre as categorias de operação, reporte e conformidade de maneira clara o suficiente para identificar e analisar os riscos aplicáveis aos seus objetivos. A gerência também considera a adequação e aplicabilidade dos objetivos definidos para a empresa. Adicionalmente, a avaliação de riscos requer que a gerência leve em conta o impacto que possíveis mudanças no ambiente externo podem causar na estrutura interna da organização, uma vez que elas podem levar os controles internos à inefetividade. (COSO; 2013; p.04; tradução nossa).

Para Assi (2012), o principal desafio em termos de gestão de riscos nas empresas é fazer com que a estratégia global e a perspectiva de risco sejam comunicadas e entendidas por todos em todos os níveis da organização, refletindo no processo de tomada de decisões. Para o autor, é papel de todos da empresa entender e identificar os riscos inerentes às atividades, visando a melhor gestão dos riscos.

Dias (2010) ressalta, em uma abordagem prática, a definição de prioridades para avaliação dos processos – logo, riscos - com base na relevância para execução do negócio fim da empresa. Segundo ele, cabe ao profissional avaliador definir o grau de risco envolvido em cada processo, para determinação da amplitude exigida perante os riscos. Ainda segundo o autor, o profissional deve mapear os macroprocessos da empresa, identificando sua importância dentro do negócio no momento e situação mercadológica ao qual a empresa atravessa. Neste contexto, as prioridades podem ser alteradas dependendo do que é considerado imprescindível para o sucesso do negócio naquele momento. Para Dias (2010), esse processo é importante para que as empresas não deixem de lado riscos relevantes e ao mesmo tempo não se perca tempo nem munição em algo que não possa representar um ganho prioritário. O autor ainda expõe que isso não significa ser apropriado deixar de lado processos que não envolvem grandes riscos, uma vez que perdas e falhas também podem ocorrer nos mesmos, porém o foco principal deve ser direcionado aos processos que podem gerar danos à continuidade e eficácia do negócio.

2.2. CONTROLE INTERNO

Conforme COSO (2013), controle interno é um processo, conduzido pela diretoria, gerência e outros profissionais, desenhado para prover segurança razoável

em relação ao cumprimento de objetivos no que diz respeito às operações, divulgações e conformidades.

Essa definição envolve alguns conceitos fundamentais, de forma que um controle interno é:

> - Conduzido para atingir objetivos em uma ou mais categorias – operacional, divulgação e conformidade.
> - Um processo formado por tarefas e atividades contínuas – um meio para atingir um resultado, não um resultado em si.
> - Desempenhado por pessoas – não formado simplesmente por políticas e procedimentos, sistemas e formulários, mas por pessoas e pelas ações que elas tomam nos diferentes níveis organizacionais para executar os controles internos.
> - Capaz de proporcionar segurança razoável – porém não segurança absoluta, para a alta gerência e diretoria.
> - Adaptável à estrutura organizacional – flexível para implementação em toda a organização ou em uma subsidiária, divisão, unidade operacional ou processo específico. (COSO; 2013; p. 03; tradução nossa).

Por mais que os diversos autores, em linhas gerais, concordem no que diz respeito à definição de controles internos, vale citar que para Franco e Marra (2001), eles são todos os instrumentos da organização destinados à vigilância, fiscalização e verificação administrativa, que permitem prever observar e dirigir ou governar os acontecimentos que se verificam dentro da empresa e que produzem reflexos no patrimônio.

Uma vez compreendida a definição de controles internos, vale mencionar seus objetivos:

> a) verificar e assegurar os cumprimentos às políticas e normas da companhia, incluindo o código de éticas nas relações comerciais e profissionais;
> b) obter informações adequadas, confiáveis, de qualidade e em tempo hábil, que sejam realmente úteis para as tomadas de decisões;
> c) comprovar a veracidade de informes e relatórios contábeis, financeiros e operacionais;
> d) proteger os ativos da entidade, o que compreende bens e direitos;
> e) Prevenir erros e fraudes. Em caso de ocorrência dos mesmos, possibilitar a descoberta o mais rápido possível, determinar sua extensão e atribuições de corretas responsabilidades;
> f) servir como ferramenta para a localização de erros e desperdícios, promovendo ao mesmo tempo a uniformidade e correção;
> g) registrar adequadamente as diversas operações, de modo a assegurar a eficiente utilização dos recursos da empresa;
> h) estimular a eficiência do pessoal, mediante a vigilância exercida por meio dos relatórios;
> i) assegurar a legitimidade dos passivos da empresa, com o adequado registro e controle das provisões, perdas reais e previstas;
> j) assegurar o processamento correto das transações da empresa, bem como a efetiva autorização de todos os gastos incorridos no período; e

> k) permitir a observância e estrito cumprimento da legislação em vigor. (OLIVEIRA, PEREZ JR. e SILVA; 2002; p. 84-85).

Os principais objetivos dos controles internos são sintetizados por Assi (2012) como: proteção aos ativos da empresa, obtenção de informações adequadas, promoção da eficiência operacional da organização e estímulo à obediência e ao respeito às políticas da administração. Ainda para Assi (2012), os controles internos devem assegurar que as fases do processo decisório e do fluxo de informações possuam a necessária confiabilidade, estando localizados em todas as áreas da organização, e envolvendo por exemplo o desenvolvimento do produto, a comercialização, a tesouraria, os departamentos de informação e contabilidade. Sendo assim, um sistema adequado de controles internos em cada área assume fundamental importância para que os resultados mais favoráveis sejam atingidos. O autor ainda menciona que onde não existem controles internos, ou eles existem mas são negligenciados, frequentemente ocorrem erros e desperdícios. Este fator ressalta a relação existente entre os controles internos e os riscos, de forma que estes sejam administrados através daqueles.

Para Assi (2012), alguns fatores devem ser considerados para a melhor gestão de controles internos:

> Tamanho e complexidade da organização: quanto maior for a entidade/organização, muito mais complexa será sua estruturação. Para dimensionar o tamanho das operações a serem controladas, a administração deverá implementar relatórios e métodos de análise e avaliação com critérios bem definidos, que reflitam a situação a cada momento na organização e, quando possível, de maneira tempestiva.
> Responsabilidades: quem deve zelar pelos ativos, patrimônio e pela prevenção a erros e fraudes, por mais que delegue responsabilidades aos gestores, é a administração, que é a principal responsável pela instituição. A manutenção do sistema de controle interno adequado é indispensável para a execução correta desse item.
> Caráter preventivo: o principal objetivo dos controles internos é prevenir, podendo-se tornar a mais importante proteção para a empresa. As rotinas de monitoração, verificação e revisão são características essenciais para um bom sistema de controles internos. Reduzem a possibilidade de erros ou tentativas de fraude quando tratados com a devida importância permitem que a administração tenha mais confiança e demais dados gerados pelos sistemas. (Assi; 2012; p.32).

Assi (2012) ainda ressalta a importância da incorporação da cultura de controles pela alta administração para que todo o processo seja mais efetivo e funcional, pois, segundo ele, o exemplo vem de cima.

Outro fator ressaltado por Assi (2012) é a importância de um procedimento ou política de execução contínua de controles internos – e não de tempos em tempos –

em todos os níveis da organização. Para o autor, estas revisões devem ser feitas pela área de *compliance* e verificadas pela área de auditoria interna. Além disso, a fidelidade de representação, a verificabilidade e a neutralidade devem ser consideradas.

Em uma abordagem prática, Dias (2010) expõe que o entendimento do objetivo do controle é o principal elemento para a conclusão sobre a melhor forma de sua adoção. Este objetivo possibilita a averiguação de seu alcance, o que assegura o controle sobre a eficácia do processo. Para o autor, no mundo globalizado não é mais possível a ocorrência de controles que não objetivem a eficácia das operações e que, por questões meramente conceituais, criem um processo moroso e com acúmulo de trabalho aos colaboradores envolvidos. Dessa forma, para ele, quando é estabelecido um controle para qualquer processo, a finalidade determinada para sua existência estabelecerá sua função, ou seja, seu objetivo.

> Preventivo: atua como uma forma de prevenir a ocorrência dos problemas, exercendo o papel de uma espécie de guia para a execução do processo ou na definição das atribuições e responsabilidades inerentes.
> Detectivo: como o nome indica, detecta algum problema no processo, sem impedir que ele ocorra.
> Corretivo: serve como base para a correção das causas de problemas no processo, mas após os mesmos já terem ocorrido. (Dias; 2010; p.05).

Neste contexto, para Dias (2010), o ideal para fins de controles internos seria a atuação em conjunto das três formas conceituadas. Sendo assim, haveria controles internos preventivos, que proporcionassem segurança quanto à inexistência de falhas inerentes aos processos; controles internos detectivos, através dos quais se definisse a forma com que as ocorrências de erros seriam identificadas; e controles internos corretivos, visando a identificação das causas de possíveis falhas ocorridas, para embasamento da forma de correção.

Vale citar ainda os cinco componentes integrados que compõem o controle interno, conforme definição do COSO (2013), que são: ambiente de controle, avaliação de riscos, atividades de controle, informação e comunicação e atividades de monitoramento. A definição de cada um deles segue abaixo:

> **Ambiente de controle**
> O ambiente de controle é um conjunto de normas, processos e estruturas que fornece a base para a condução do controle interno por toda a organização. A estrutura de governança e a alta administração estabelecem uma diretriz sobre a importância do controle interno, inclusive das normas

> de conduta esperadas. A administração reforça as expectativas nos vários níveis da organização.
> O ambiente de controle abrange a integridade e os valores éticos da organização; os parâmetros que permitem à estrutura de governança cumprir com suas responsabilidades de supervisionar a governança; a estrutura organizacional e a delegação de autoridade e responsabilidade; o processo de atrair, desenvolver e reter talentos competentes; e o rigor em torno de medidas, incentivos e recompensas por performance. O ambiente de controle resultante tem impacto pervasivo sobre todo o sistema de controle interno. (COSO; 2013; p.07-08; traduzido por IIA e PWC).

Pode-se perceber a relação direta entre o ambiente de controle e a cultura organizacional, uma vez que diversos fatores relacionados ao perfil da empresa compõem este componente, como a estratégia de atração e retenção de talentos, recompensas e inventivos por performance, valores éticos da empresa, entre outros.

> **Avaliação de riscos**
> Toda entidade enfrenta vários riscos de origem tanto interna quanto externa. Define-se risco como a possibilidade de que um evento ocorra e afete adversamente a realização dos objetivos. A avaliação de riscos envolve um processo dinâmico e iterativo para identificar e avaliar os riscos à realização dos objetivos. Esses riscos de não atingir os objetivos em toda a entidade são considerados em relação às tolerâncias aos riscos estabelecidos. Dessa forma, a avaliação de riscos estabelece a base para determinar a maneira como os riscos serão gerenciados.
> Uma condição prévia à avaliação de riscos é o estabelecimento de objetivos, ligados aos diferentes níveis da entidade. A administração especifica os objetivos dentro das categorias: operacional, divulgação e conformidade, com clareza suficiente para identificar e analisar os riscos à realização desses objetivos. A administração também considera a adequação dos objetivos à entidade. A avaliação de riscos requer ainda que a administração considere o impacto de possíveis mudanças no ambiente externo e dentro de seu próprio modelo de negócio que podem tornar o controle interno ineficaz. (COSO; 2013; p.07-08; traduzido por IIA e PWC).

Como pode-se perceber através da descrição acima, o COSO (2013) possui uma visão de riscos voltada para eventos que possam causar um impacto negativo na organização, diferentemente da visão de finanças, que, segundo o IBGC (2007), intera a premissa de que quanto maior o nível de risco aceito, maior o retorno esperado. Por mais que ambas as visões sejam coerentes em sua área de estudo, percebe-se que na perspectiva de gestão de riscos organizacionais, os riscos estão mais comumente relacionados à possibilidade de perdas; porém, a própria gestão e mitigação de riscos é uma maneira de transformar os riscos e oportunidades e, logo, em vantagem competitiva.

> **Atividades de controle**
> Atividades de controle são ações estabelecidas por meio de políticas e procedimentos que ajudam a garantir o cumprimento das diretrizes determinadas pela administração para mitigar os riscos à realização dos objetivos. As atividades de controle são desempenhadas em todos os níveis

> da entidade, em vários estágios dentro dos processos corporativos e no ambiente tecnológico. Podem ter natureza preventiva ou de detecção e abranger uma série de atividades manuais e automáticas, como autorizações e aprovações, verificações, reconciliações e revisões de desempenho do negócio. A segregação de funções é geralmente inserida na seleção e no desenvolvimento das atividades de controle. Nos casos em que a segregação de funções seja impraticável, a administração deverá selecionar e desenvolver atividades alternativas de controle. (COSO; 2013; p.07-08; traduzido por IIA e PWC).

Conforme exposto, percebe-se a relação existente entre riscos e controles, através da qual busca-se criar mecanismos através destes para que se torne possível evitar eventos adversos causados por aqueles.

> **Informação e comunicação**
> A informação é necessária para que a entidade cumpra responsabilidades de controle interno a fim de apoiar a realização de seus objetivos. A administração obtém ou gera e utiliza informações importantes e de qualidade, originadas tanto de fontes internas quanto externas, a fim de apoiar o funcionamento de outros componentes do controle interno. A comunicação é o processo contínuo e iterativo de proporcionar, compartilhar e obter as informações necessárias. A comunicação interna é o meio pelo qual as informações são transmitidas para a organização, fluindo em todas as direções da entidade.
> Ela permite que os funcionários recebam uma mensagem clara da alta administração de que as responsabilidades pelo controle devem ser levadas a sério. A comunicação externa apresenta duas vertentes: permite o recebimento, pela organização, de informações externas significativas, e proporciona informações a partes externas em resposta a requisitos e expectativas. (COSO; 2013; p.07-08; traduzido por IIA e PWC).

O COSO (2013) traz à luz a importância da confiabilidade dos dados e informações geradas ao longo dos diversos processos dentro da empresa, bem como das recebidas e divulgadas para fora dela. Além disso, enfatiza aspectos de comunicações por entre os níveis organizacionais, seja de baixo para cima ou de cima para baixo. Em outras palavras, se os direcionamentos da alta administração são claramente transmitidos aos níveis operacionais e, ao mesmo tempo, se as informações geradas nos níveis operacionais chegam à alta administração com a devida confiabilidade e integridade, para análise e tomada de decisões.

> **Atividades de monitoramento**
> Uma organização utiliza avaliações contínuas, independentes, ou uma combinação das duas, para se certificar da presença e do funcionamento de cada um dos cinco componentes de controle interno, inclusive a eficácia dos controles nos princípios relativos a cada componente. As avaliações contínuas, inseridas nos processos corporativos nos diferentes níveis da entidade, proporcionam informações oportunas. As avaliações independentes, conduzidas periodicamente, terão escopos e frequências diferentes, dependendo da avaliação de riscos, da eficácia das avaliações contínuas e de outras considerações da administração. Os resultados são avaliados em relação a critérios estabelecidos pelas autoridades normativas, órgãos normatizadores reconhecidos ou pela administração e a

> estrutura de governança, sendo que as deficiências são comunicadas à estrutura de governança e administração, conforme aplicável. (COSO; 2013; p.07-08; traduzido por IIA e PWC).

Percebe-se que as atividades de monitoramente possuem a função de transformar o que poderia ser um processo pontual em contínuo, o que se torna a base para as identificações e implementações de melhorias, tanto nos processos organizacionais quanto na própria estrutura de gestão de cotroles internos da organização.

Por fim, torna-se possível identificar que há uma forte relação entre os cinco componentes do COSO (2013), de forma que um torna-se a base para a efetiva implementação do outro. Dessa forma, todos tornam-se igualmente importantes para gestão de riscos e controles de uma organização.

2.3. FRAUDE

Conforme Assi (2012), a cultura de controle sempre envolve preocupações a cerca da prevenção de perdas, seja por erros não intencionais ou fraudes. Neste contexto destacam-se as fraudes corporativas, envolvendo grandes empresas, que acabam por reduzir seus resultados, gerar perdas financeiras, danos à imagem e reputação e até mesmo levar a empresa à falência. Como exemplos mundialmente conhecidos de fraudes corporativas pode-se citar Enron, Arthur Andersen e WorldCom, que inclusive serviram como motivação para a criação da lei norte-americana Sarbanes-Oxley (abordada no capítulo subsequente). Dessa forma, é uma tendência que as empresas busquem aprimorar o entendimento das causas das fraudes, justamente para implementar melhores controles de prevenção, expõe Assi (2012).

Tendo em vista o interesse do mercado quanto ao entendimento das causas da fraude, a PWC (2014) realizou a 7ª Pesquisa Global sobre Crimes Econômicos, na qual 5.128 executivos de mais de 95 países foram entrevistados, envolvendo 132 no Brasil. Quando perguntados se "a sua organização sofreu algum tipo de crime econômico nos últimos 24 meses" (PWC; 2014; p.07), 69% responderam "roubo de ativos", 29% "fraude em compras", 27% "suborno e corrupção", 24% "fraudes digitais" e 22% "fraude contábil", entre outras respostas com menor percentual. As respostas não somam 100% devido à existência de mais de um tipo de fraude na

mesma organização. Uma consideração relevante é de que, se consideradas apenas as respostas da Brasil, o índice de "fraude em compras" passa para 44%.

No que diz respeito à motivação da fraude, PWC (2014) aponta que no Brasil 74% das fraudes foram motivadas por oportunidade, 13% por pressão, e 13% por racionalização.

> Esses resultados mostram que o meio mais eficaz para combater as fraudes é, sem dúvida alguma, a prevenção e a mitigação de riscos em processos e métodos. Tanto aqui quanto em qualquer parte do mundo. Em muitos casos verificamos que os controles estão presentes, mas a pessoa que comete a fraude os conhece bem e sabe como burlá-los. São profissionais com muitos anos de empresa e conhecimento para fazer isso. (PWC; 2014; p. 13).

Outra questão relevante abordada pela PWC (2014) é a de identificação da fraude. Na pesquisa, 21% dos entrevistados no Brasil apontaram como método de detecção da fraude a "notificação de transações suspeitas e análise de dados", 17% a auditoria interna e 14% "denúncia interna". As alternativas "sistema formal de denúncia" e "denúncia externa" foram apontadas, cada uma, por 10% dos entrevistados, enquanto "rotatividade de pessoal" e "segurança corporativa", 7%.

Por fim, vale citar como as empresas reagem às fraudes. Neste contexto, 87% dos entrevistados do Brasil apontaram "demissão", 30% "ação civil" e "informação às forças de segurança pública", enquanto 13% "advertência" e 4% "notificação para as autoridades regulatórias" e "nenhuma ação".

2.4. LEI SARBANES-OXLEY (SOX)

Conforme Assi (2012), a Lei norte-americana Sarbanes-Oxley foi sancionada em julho de 2002 visando moralizar o mercado, devido a uma série de escândalos de fraude que marcaram os anos anteriores. Segundo o autor, a lei foi uma reação rápida e desesperada dos Estados Unidos na tentativa de recuperar a confiança dos investidores, pondo fim à tradicional “autorregulação” baseada no modelo dos melhores princípios e a substituindo por uma lei dura e abrangente. A lei, idealizada pelos parlamentares Paul Sarbanes e Michael Oxley, faz com que qualquer empresa que queira ter suas ações listadas nos Estados Unidos tenha que atender a todos os seus critérios. Neste contexto, Dias (2010) cita que a Lei Sarbanes-Oxley expande sua aplicação às empresas que não são de origem norte-americana.

Assi (2012) expõe a criação da nova unidade reguladora para o setor de contabilidade, instaurada através da lei Sarbanes-Oxley, o Conselho de Supervisão das Companhias Abertas (Public Company Accounting Oversight Board – PCAOB). Os auditores foram proibidos de prestar uma variedade de serviços não ligados à auditoria para seus clientes (de auditoria externa), para evitar conflitos de interesse. Além disso, ainda conforme o autor, as empresas tiveram que estabelecer comitês de auditoria independentes, empréstimos das empresas para seus executivos foram proibidos, altos executivos tiveram que certificar as contas de suas empresas e informantes ganharam maior proteção ao emprego nos casos em que reportassem suspeitas de atividades fraudulentas.

Desde a criação da SEC – Security Exchange Act (CVM dos EUA), em 1934, para Assi (2012), a Lei Sarbanes-Oxley é considerada o fato jurídico mais relevante para o mercado de capitais norte-americano, que veio restaurar a segurança das práticas contábeis e relatórios corporativos, tornando transparentes e confiáveis os procedimentos de gestores em assuntos diretamente relacionados com os resultados financeiros.

Dias (2010) destaca dentre as principais disposições da lei a certificação do CEO (*Chief Executive Officer*) e CFO (*Chief Financial Officer*). Para ele, esta medida busca desencorajar a alegação por parte dos executivos, quanto ao desconhecimento de práticas indevidas, o que foi um fato comum nos recentes escândalos contábeis norte-americanos. O autor ainda cita que a maior parte das discussões a cerca da Sarbanes-Oxley estão concentradas nas seções 302 e 404.

Conforme Dias (2010), através da seção 302 definiu-se a responsabilidade pessoal da alta gestão quanto à divulgação dos controles e procedimentos da empresa. Dessa forma, uma certificação de que a eficiência dos controles foi avaliada deve ser emitida trimestralmente. Esta deve declarar que todas as deficiências de controle, deficiências materiais e fraudes foram informadas ao comitê de auditoria e aos auditores independentes.

> - A Seção 302 (a) do Ato passa a requerer que o *CEO* e o *CFO* certifiquem as informações financeiras e não financeiras contidas nos relatórios anuais.
> - Esta certificação também inclui controles internos, definidos em duas dimensões:
>
> a) controles internos propriamente ditos;
>
> b) controles e procedimentos de divulgação (*disclosure controls and procedures*).

> - O modelo de certificação a ser assinada pelo *CEO* e *CFO* deve ser exatamente o mesmo apresentado no Ato, não sendo permitidas modificações.
> - Este ato introduziu responsabilidades criminais que, em certos casos, podem envolver prisão de até 20 anos para *CEOs* e *CFOs* pelo fornecimento, proposital ou não, de certificações incorretas ou não verdadeiras. (Dias; 2010; p.34-35).

Neste contexto, Dias (2010) descreve os seguintes requerimentos impostos no processo de certificação, aplicáveis às empresas e aos seus administradores, ainda abordados pela seção 302:

> - O *CEO* e o *CFO* devem certificar as informações financeiras e não financeiras contidas nos relatórios anuais.
> - As empresas devem manter controles internos, definidos em duas dimensões: controles internos propriamente ditos e controles e procedimentos de divulgação (*disclosure controls and procedures*).
> - O *CEO* e o *CFO* estarão certificando que avaliaram a efetividade desses controles até, no máximo, 90 dias da data de arquivamento das informações (*Form* 20-F). O *Form* 20-F deve informar sobre o resultado dessa avaliação. (Dias; 2010; p.35).

Quanto a Seção 404, conforme Deloitte (2003), determina-se a necessidade de uma avaliação anual dos controles e procedimentos internos relacionados à emissão de relatórios financeiros da empresa. Dessa forma, ela obriga as companhias a incluir em seus relatórios anuais um relatório sobre controles internos emitido pela administração que:

> - afirme sua responsabilidade pelo estabelecimento e pela manutenção de controles e procedimentos internos para a emissão de relatórios financeiros;
> - avalie e atinja conclusões acerca da eficácia dos controles e procedimentos internos para a emissão de relatórios financeiros;
> - declare que o auditor independente da companhia atestou e reportou a avaliação feita pela administração sobre seus controles e procedimentos internos para a emissão de relatórios financeiros. (Deloitte; 2003; p.09-10).

Para Dias (2010) a seção 404:

> Determina uma avaliação anual dos controles e procedimentos internos, para elaboração dos reportes financeiros. Adicionalmente, os auditores independentes devem emitir um relatório separado, atestando a aderência da administração em prover eficientes controles internos e procedimentos, para os reportes financeiros. (Dias; 2010; p.36).

Adicionalmente, Assi (2012) descreve que a seção 404 exige a apresentação à SEC de relatórios de controles internos, juntamente com as demonstrações financeiras. Também deve ser informado: quem é responsável por estabelecer e

manter uma estrutura interna de controles internos, os procedimentos para relatórios financeiros na organização e como é feita a avaliação da eficácia dos controles e procedimentos. O autor ainda expõe que a seção 404 gerou polêmica ao ser aprovada devido aos altos custos para sua implementação. Conforme exposto pelo autor, segundo avaliação do Financial Executives International (FEI), o custo total de um processo de adesão à seção 404 pode exceder US$ 4,6 milhões ao longo de cinco anos, para cada uma das grandes companhias dos Estados Unidos. Em contra partida, Assi (2012) comenta que o processo gera uma compensação para as empresas, que passam a entender melhor seus processos e adotar novas formas de reduzir custos.

De maneira geral, percebe-se que há alinhamento quanto às descrições e interpretações da lei Sarbanes-Oxley entre Deloitte (2003), Assi (2012) e Dias (2010), que convergem quanto à interpretação de que a lei estabelece, de forma explícita, a responsabilidade da alta gestão pelo estabelecimento, avaliação e monitoramento dos controles internos sobre os relatórios financeiros.

Por fim, Dias (2010) ainda relaciona alguns temas que estão relacionados à Sarbanes-Oxley, envolvendo boas práticas de governança e ética corporativa:

> - Código de ética corporativo.
> - Restrição a empréstimos e concessão de crédito para diretores.
> - Código de ética para executivos financeiros e *insiders*.
> - Restrição à contratação de serviços dos auditores externos.
> - Quarentena para a contratação de funcionários que já atuaram como auditores externos (nível executivo para a área financeira).
> - Comitê de auditoria (transferido para 2005).
> - Combate a fraudes financeiras.
> - Estruturação e monitoramento dos controles internos.
> - Governança em tecnologia da informação.
> - Gestão e gerenciamento de riscos. (Dias; 2010; p.35).

2.5. *INTERNAL CONTROL - INTEGRATED FRAMEWORK*

Conforme Dias (2010), em 1985 foi criada a *National Comission on Fraudulent Financial Reporting* (Comissão Nacional sobre Fraudes em Relatórios Financeiros), nos Estados Unidos. Esta comissão era composta por membros das principais associações de classe de profissionais ligados à área financeira e teve como primeiro objeto de estudo os controles internos, publicando em 1992 o trabalho *Internal Control - Integrated Framework (*Controles Internos - Um Modelo Integrado).

Posteriormente, a comissão transformou-se em um comitê, sem fins lucrativos, conhecido como COSO (*The Committee of Sponsoring Organizations),* em português "Comitê das Organizações Patrocinadoras". Este se dedica à melhoria dos relatórios financeiros, com foco em ética, efetividade de controles internos e governança corporativa, segundo Dias (2010).

Conforme Gil, Arima e Nakamura (2013), o *Internal Control - Integrated Framework* publicado pelo COSO em 1992 se tornou o *framework* para avaliação de controles internos de maior aceitação nos Estados Unidos da América. Segundo os autores, ele constitui um modelo de controle a ser utilizado nas organizações, observando suas particularidades, resultando em uma metodologia de controle interno. Para Dias (2010), o *framework* tornou-se referência em nível mundial para o estudo e aplicação de controles internos.

Em 2013, o COSO foi atualizado, em virtude de que:

> Nos vinte anos desde a introdução do primeiro *Integrated Framework*, os ambientes operacionais e corporativos passaram por uma transformação significativa, tornando-se cada vez mais complexos, globais e orientados pela tecnologia. Ao mesmo tempo, os *stakeholders* têm se tornado mais participativos, buscando maior transparência e responsabilidade pela integridade dos sistemas de controle interno que suportam as decisões corporativas e de governança das organizações. (COSO; 2013; p.02; tradução nossa).

Algumas mudanças foram realizadas da versão de 1992 para a de 2013, em virtude do exposto acima. Estas são comentadas no próprio prefácio do *Internal Control - Integrated Framework: Executive Summary*, conforme abaixo:

> O *framework* mantém a definição principal de controle interno e seus cinco componentes. A exigência de se considerar os cinco componentes para avaliação da eficácia do sistema de controle interno basicamente não sofreu alterações. O *framework* também continua a enfatizar a importância do julgamento feito pela administração para o desenho, a implementação e a condução de controles internos, assim como na avaliação da eficácia do sistema de controle interno.
> Ao mesmo tempo, o *framework* inclui melhorias e esclarecimentos para facilitar seu uso e sua aplicação. Uma das melhorias mais significativas é a formalização de conceitos fundamentais introduzidos no *framework* original. Agora, esses conceitos se transformaram em princípios, que são associados aos cinco componentes e que proporcionam ao usuário clareza no desenvolvimento e na implementação dos sistemas de controle interno, além de compreensão quanto aos requisitos de um controle interno eficaz.
> O *framework* foi aprimorado com a expansão da categoria de objetivos de divulgação financeira, a fim de incluir outros formatos importantes de divulgação, como as divulgações internas e não financeiras. O *framework* também inclui considerações sobre as diversas mudanças nos ambientes operacionais e corporativos durante as últimas décadas, incluindo:
> - Expectativas sobre a supervisão da governança.

> - Globalização dos mercados e das operações.
> - Mudanças e o aumento da complexidade nos negócios.
> - Exigências e complexidades nas leis, regras, regulamentações e normas.
> - Expectativas em relação às competências e responsabilidades pela prestação de contas.
> - Uso, e confiabilidade, de tecnologias em transformação.
> - Expectativas em relação à prevenção e detecção de fraudes. (COSO; 2013; p.02; tradução nossa).

As diretrizes do *Internal Control - Integrated Framework* definem que controle interno é um processo aplicado pela alta administração e demais pessoas da empresa, tais como o conselho, os administradores, empregados, etc. e que fornece razoável segurança para alcançar os objetivos do negócio, conforme descrevem Gil, Arima e Nakamura (2013).

Conforme o próprio COSO (2013), o *Internal Control – Integrated Framework* permite que as organizações desenvolvam estruturas de controle interno, tendo em vista a adaptação necessária nos ambientes operacionais e corporativos, em meio às constantes mudanças. Além disso, o *framework* tem como objetivo prover a redução dos riscos para níveis aceitáveis e suportar um processo robusto de tomada de decisões e de governança corporativa.

Outra característica do *framework,* segundo COSO (2013), é a necessidade de julgamento por parte daqueles que atuam na estrutura de controles internos, como a administração e o conselho, não sendo suficiente apenas a adequação às políticas e procedimentos da empresa. Isso significa dizer que além de cumprir estritamente as normas, é necessário julgar se os níveis de controle aplicados mitigam suficientemente os riscos, tornando o sistema de controle interno eficaz. COSO (2013) ainda menciona o papel dos auditores internos, no que tange a execução do monitoramento e da avaliação.

Vale citar ainda que - conforme COSO (2013) - o *framework* proporciona para a gestão e para a diretoria:

> - uma forma de aplicar o controle interno em qualquer tipo de organização, independentemente da indústria ou de sua estrutura legal, nos níveis de entidade, unidade operacional ou função.
> - uma abordagem baseada em princípios que fornece flexibilidade e permite julgar o desenho, a implementação e a condução do controle interno – princípios que podem ser aplicados nos níveis de entidade, unidade operacional ou função.
> - requisitos para um sistema eficaz de controle interno, considerando como os componentes e princípios estão aplicados e em funcionamento, assim como a maneira com que os componentes operam em conjunto.

> - um modo de identificar e analisar riscos e de desenvolver e gerenciar respostas adequadas aos riscos, com níveis aceitáveis e maior foco em medidas antifraude.
> - uma oportunidade de expandir a aplicação do controle interno da divulgação financeira para outras formas de divulgação, operação e conformidade.
> - uma oportunidade para eliminar controles ineficazes, redundantes ou ineficientes que proporcionam valor mínimo na redução de riscos para alcançar os objetivos da entidade. (COSO; 2013; p.04; tradução nossa).

COSO (2013) menciona também os benefícios para os agentes externos à entidade, que de alguma forma possuem um meio de interação:

> - maior confiança nos sistemas de controle interno implementados pela estrutura de governança da empresa.
> - maior confiança em relação ao atingimento dos objetivos da entidade.
> - maior confiança na capacidade da organização de identificar, analisar e responder aos riscos e às mudanças nos ambientes operacional e organizacional.
> - maior entendimento quanto à necessidade de possuir um sistema eficaz de controle interno.
> - melhor entendimento de que, através do uso de julgamento, a administração tende a ser capaz de eliminar controles ineficazes, redundantes ou ineficientes. (COSO; 2013; p.05; tradução nossa).

Por fim, vale ressaltar outra característica importante do *Internal Control - Integrated Framework,* que é a inexistência de um processo em série, mas sim dinâmico e integrado, de forma que ele possa ser empregado tanto em empresas de grande quanto pequeno porte, independentemente de sua forma jurídica. Isso porque cada organização pode optar por implementá-lo de uma maneira diferente, conforme COSO (2013). Um exemplo é o fato de uma empresa de pequeno porte poder implementar as premissas do *framework* de um modo menos formal e estruturado, mas mesmo assim eficaz.

2.6. MAPEAMENTO DE PROCESSOS

Assi (2012) propõe quatro etapas para mapear processos, com foco na identificação de riscos e controles. São elas, ordenadas cronologicamente: entrevistas, elaboração do fluxo macro, elaboração dos fluxos detalhados dos processos e identificação dos pontos de controle, riscos e problemas. Segue abaixo uma condensação dos fatores-chave de cada etapa:

2.6.1. Entrevistas

Esta é a primeira etapa a ser executada pelo gestor de riscos, na qual deve-se inicialmente avaliar o organograma geral da empresa e obter o entendimento de sua estrutura. Isso envolve a identificação de todas as diretorias, departamentos e seus respectivos responsáveis. Feito isso, as entrevistas em si devem ser executadas, com os responsáveis diretos ou indicados de cada área de negócio. O objetivo geral é obter entendimento a cerca dos processos da empresa, suas principais atividades, organização e as responsabilidades de cada diretoria e departamento.

2.6.2. Elaboração do fluxo macro

Após a identificação dos processos existentes na empresa, um fluxograma macro deve ser desenvolvido, visando:

1) Visualizar toda a organização de uma forma sistêmica pela complexidade de seus processos.
2) Definir junto ao comitê específico e/ou alta administração a prioridade de análise dos processos.
3) Permitir o controle dos processos mapeados e pendentes.

2.6.3. Elaboração dos fluxos detalhados dos processos

Após a definição das prioridades, o profissional de riscos deve entrevistar novamente todos os responsáveis diretos e indiretos pela elaboração dos fluxogramas de modo detalhado. Isto é fundamental para o sucesso do mapeamento, pois o material preparado nesta etapa servirá como suporte para a identificação de riscos, elaboração dos pontos de controle e formalização de normas e procedimentos.

Na elaboração dos fluxogramas, é importante que as atividades estejam segregadas conforme as áreas que as executam, visando melhor visualização dos documentos. Isso permite uma otimização das análises para racionalização, avaliação de riscos e identificação de melhorias.

2.6.4. Identificação dos pontos de controle, riscos e problemas

Com base nos fluxogramas detalhados, os pontos de controle, riscos e problemas devem ser identificados. Para todo risco existente, deve haver um ponto de controle para sua mitigação, de acordo com o que é mais viável. Avaliar o

controle é de fundamental importância, pois sua efetividade reduz a possibilidade de materialização dos riscos e auxiliam na proposição de melhorias nos processos.

Durante o mapeamento é possível encontrar riscos que já estejam materializados, ou seja, problemas que já resultaram em um impacto negativo. Para estes casos, um plano de ação deve ser definido e a situação deve ser tratada com prioridade.

2.7. KPI - *KEY PERFORMANCE INDICADOR (*INDICADOR-CHAVE DE PERFORMANCE)

Segundo Assi (2012), um KPI (indicador-chave de performance) tem como objetivo mensurar a etapa ou o resultado de um processo, de forma periódica. Dessa forma, eles estão comumente inseridos nas organizações, tendo em vista a existência de diversas metas e atividades exercidas pelos colaboradores. Assi (202) ainda aponta que, se aplicados com responsabilidade, os KPIs podem auxiliar na avaliação e identificação de problemas e dificuldades.

> Métricas:
> - Dados (*count*): unidade básica de medição. Exemplo: visitas = 2.343.
> - Razão (*ratio*): divisão entre dois dados ou mesmo entre outras razões. Exemplo: ocorrências por visitas = 4,3. (Assi; 2012; p.115).

Conforme o exposto acima, um KPI pode ser um dado ou uma razão, contudo, Assi (2012) destaca que é mais comum que um KPI seja uma razão. O autor ainda expõe que os KPIs estão diretamente ligados a um objetivo de determinada empresa e, dessa forma, mesmo que haja um concorrente no mesmo mercado, provavelmente ele terá objetivos diferentes e, dessa forma, KPIs diferentes. Pode-se interpretar esta característica válida devido às diferentes formas operacionais existentes, mesmo dentro do mesmo mercado, que tendem a variar dependendo da estrutura organizacional, sua cultura, da maturidade dos processos e até mesmo de preferências e estilos de cada gestor.

Para que a definição de qual KPI deve ser utilizado, Assi (2012) descreve 03 fatores:

> - Iniciar o processo de definição dos objetivos estratégicos.
> - Dividir em objetivos operacionais para cada área da empresa.
> - Controlar os objetivos definidos para todas as áreas para garantir que os objetivos da empresa sejam alcançados. (Assi; 2012; p.115).

Por fim, Assi (2012) ainda expõe que, de maneira geral, pode-se dividir os objetivos de uma empresa em três macro-grupos: diminuir custos, aumentar receita e aumentar a satisfação do cliente. Desta forma, os objetivos tendem a variar dependendo da estratégia organizacional.

3. METODOLOGIA

A seguir, a classificação da pesquisa e os procedimentos metodológicos deste trabalho são descritos.

3.1. CLASSIFICAÇÃO DA PESQUISA

A metodologia deste trabalho é definida como qualitativa, quanto à abordagem do problema e descritiva, quanto aos seus objetivos. No que diz respeito aos procedimentos utilizados, a metodologia é classificada como exploratória, bibliográfica e fundamentada nas observações do pesquisador, que atuou como consultor de controles internos em uma empresa *big four* e atualmente exerce a função de analista sênior de controles internos em uma multinacional de grande porte, sendo o responsável pelo desenvolvimento da metodologia de controles internos da mesma.

3.2. PROCEDIMENTOS METODOLÓGICOS

Este trabalho propõe uma metodologia de definição e avaliação de controles internos que possa ser aplicada - mesmo que com variações em virtude de características específicas de cada negócio, mercado ou organização - em empresas de grande porte em geral. Além disso, ele procura definir as ferramentas a serem utilizadas na prática para a definição do escopo, mapeamento, descrição e avaliação de riscos e controles, bem como para a definição e implementação dos planos de remediação, de forma que haja alinhamento com os conceitos e boas práticas expostos nos materiais que compõem o referencial teórico deste trabalho. Desta forma, vale ressaltar que através dos procedimentos metodológicos, visa-se desdobrar os conceitos e boas práticas de controles internos já consagradas no mercado em um modelo que proporcione a sua operacionalização.

Para isso, o *Internal Control - Integrated Framework 2013*, publicado pelo COSO, é utilizado como principal guia bibliográfico, por ser uma das principais estruturas em nível mundial para controles internos. Atrelado às suas definições, a experiência e observação do pesquisador - em trabalhos de definição e avaliação de

controles internos em empresas de grande porte - é utilizada para a apresentação da proposta de metodologia de controles internos descrita neste trabalho.

Sendo assim, os procedimentos metodológicos utilizados combinam conceitos teóricos, ou seja, bibliográficos, à experiência prática do pesquisador, a fim de desenvolver um modelo que permita a implementação de uma estrutura e de um fluxo de trabalho para definir e avaliar controles internos em grandes empresas, de modo exploratório. Para isso, ao longo de cada etapa do modelo, seu objetivo e os fatores críticos para seu sucesso são descritos. Dessa forma, busca-se permitir a adequação de cada etapa conforme a necessidade de cada empresa, o que é possível uma vez que o leitor compreenda a razão pela qual cada etapa existe e cada ferramenta é utilizada.

4. PROPOSTA DE METODOLOGIA DE CONTROLES INTERNOS

A proposta de metodologia para definição e avaliação de controles internos descrita neste trabalho tem como principais objetivos auxiliar a administração da empresa a gerir riscos no nível operacional, agregar valor aos processos e implementar um fluxo que proporcione melhoria contínua.

Para isso, a metodologia foi dividida em etapas a serem executadas cronologicamente, conforme exposto no fluxo a seguir.

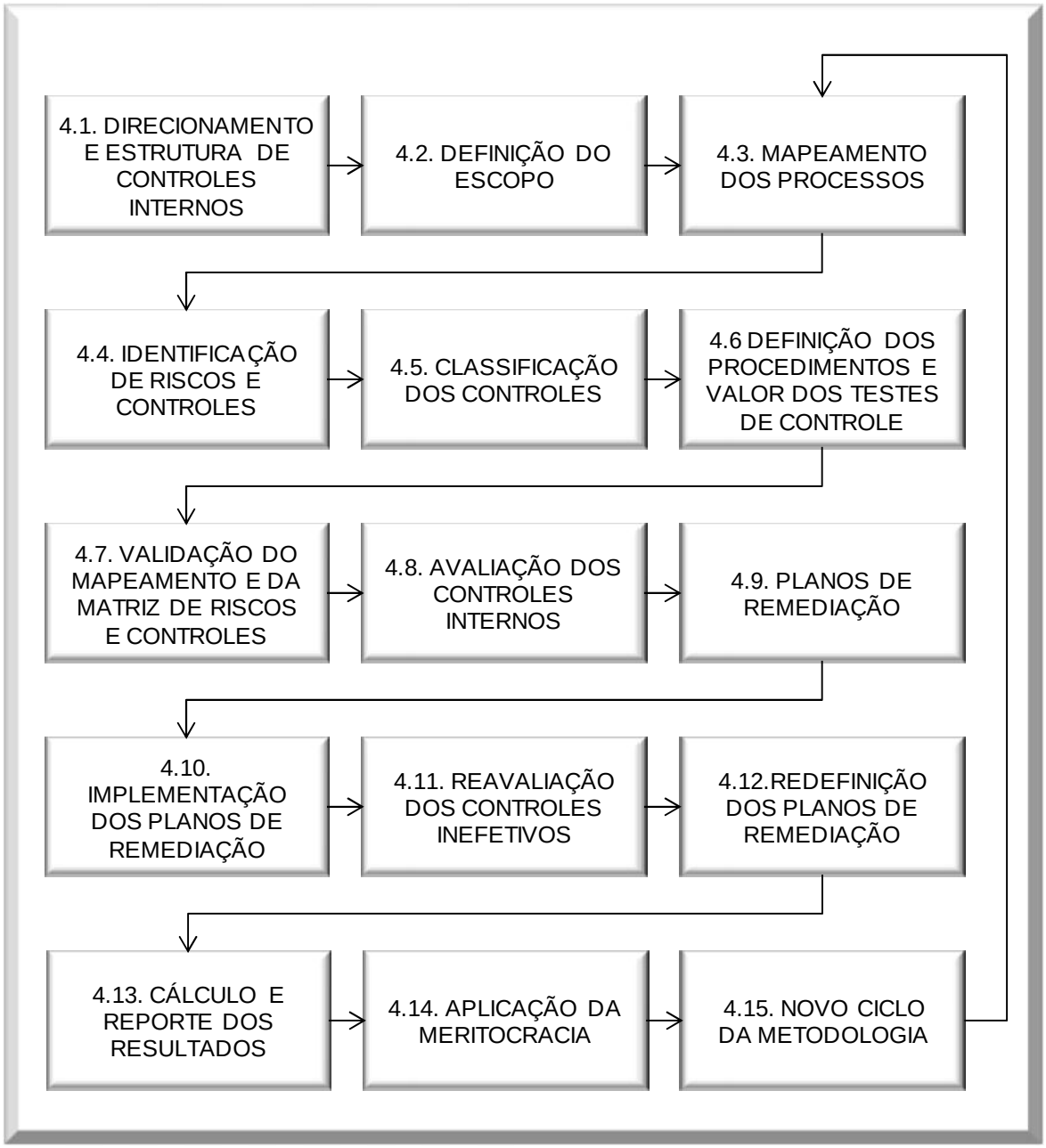

FIGURA 1 – MACRO-FLUXO DA METODOLOGIA DE CONTROLES INTERNOS

Conforme exposto no fluxo acima, a primeira tarefa para implementar a metodologia de definição e avaliação de controles internos é definir a estrutura de controles internos e direcionar os trabalhos a serem realizados. Na prática, isso significa definir o que se espera do projeto e como estará organizado o departamento responsável por implementar o projeto.

Feito isso, torna-se possível iniciar o processo de definição do escopo de trabalho, ou seja, quais processos e subprocessos deverão ser abordados através da metodologia, de forma que os objetivos definidos na etapa anterior possam ser alcançados.

Dessa forma, as duas primeiras etapas propostas por esta metodologia possuem objetivos de preparação e direcionamento, e envolvem quase exclusivamente decisões a serem tomadas pela alta gestão da empresa. Ao finalizá-las, torna-se possível iniciar na prática as atividades de definição e avaliação de controles internos, sendo o primeiro passo a realização do mapeamento dos subprocessos sob escopo. Esta etapa visa proporcionar o entendimento adequado de cada subprocesso ao departamento responsável pela implementação desta metodologia (chamado neste trabalho de "departamento de controles internos"). Cada subprocesso deve ser mapeado conforme o cronograma previamente definido. Dessa forma, desta etapa em diante, cada subprocesso deve ser tratado separadamente, ou seja, alguns serão iniciados antes que os outros, fazendo com que cada subprocesso esteja cronologicamente em momentos diferentes ao longo das etapas seguintes da metodologia.

Após obter o entendimento das atividades desempenhadas no subprocesso em questão - ou até mesmo durante o próprio mapeamento do subprocesso -, torna-se possível identificar os riscos e controles existentes no mesmo, bem como descrevê-los. Estas atividades são abordadas na etapa "4.4 - Identificação de riscos e controles" e exigem um elevado conhecimento técnico a cerca de riscos e controles para ser desempenhada.

Identificados os controles, torna-se possível classificá-los e definir os procedimentos para avaliá-los, atividades que são executadas nas etapas 4.5 e 4.6, respectivamente. Elas possuem o principal objetivo de proporcionar uma avaliação adequada da efetividade dos controles internos, que é realizada na etapa 4.8, logo após validar o mapeamento e os riscos e controles identificados com o responsável pelo subprocesso, na etapa 4.7.

Dessa forma, a etapa "4.8 - Avaliação dos controles internos" divide-se em dois principais momentos: a autoavaliação realizada por cada departamento envolvido no subprocesso e a avaliação realizada pelo departamento de controles internos.

Ao término da etapa de avaliação, o conhecimento dos controles inefetivos será obtido, sendo possível definir os planos de remediação necessários para mitigar os riscos descobertos e, em seguida, implementar as mudanças necessárias. Estas atividades são executadas nas etapas 4.9 e 4.10, respectivamente.

Vale ressaltar que logo após o término da etapa 4.9, quando os planos de remediação já estarão definidos e alinhados com os departamentos responsáveis por implementá-los, há uma pausa na implementação da metodologia pelo departamento de controles internos. Esta visa proporcionar o tempo necessário para que cada departamento tenha o tempo necessário para implementar os planos de remediação. Neste período, o departamento de controles internos deve focar seus esforços nas outras etapas dos outros subprocessos, bem como suportar os departamentos que estejam implementando os planos de remediação.

Ao término do prazo concedido para implementação dos planos de remediação, o departamento de controles internos deve iniciar a etapa "4.11 - Reavaliação dos controles internos". Esta é similar à etapa 4.8, mas visa apenas avaliar os controles anteriormente classificados como inefetivos e ainda, caso julgado necessário pelo departamento de controles internos, demais controles que anteriormente foram classificados como efetivos, mas que são considerados críticos.

Ao término da etapa de reavaliação, novos planos de remediação devem ser definidos para os controles internos que permanecerem inefetivos.

Sendo assim, termina-se um ciclo de implementação da definição e avaliação de controles internos, que habitualmente possui um ano de duração. Dessa forma, torna-se necessário calcular, avaliar e reportar os resultados a cerca da efetividade dos controles internos de cada subprocesso e de cada departamento. Este cálculo deve ser realizado pelo departamento de controles internos e os níveis de efetividade atingidos por cada departamento devem ser reportados para os mesmos. Além disso, o nível de efetividade de cada subprocesso deve ser avaliado e apresentado à alta administração, de maneira formal. Esta atividade é de extrema importância para a análise dos riscos estratégicos da empresa, pois proporciona entendimento quanto à efetividade e confiabilidade de cada subprocesso aos níveis

com poder de decisão. Estas atividades são desempenhadas na etapa "4.13 - Reporte dos resultados".

Dessa forma, torna-se possível atingir os objetivos da etapa "4.14 - Aplicação da meritocracia", que visa retribuir os gestores com melhor desempenho na gestão de riscos e controles em suas atividades, independentemente do subprocesso de atuação. Para isso são utilizados KPIs (*key performance indicators)* padronizados para todos os departamentos envolvidos no projeto de definição e avaliação de controles internos.

Por fim, a preparação para iniciar um novo ciclo da metodologia de controles internos deve ser realizada. Nesta, a alta administração deve revisar a estrutura de controles internos e o escopo de implementação da metodologia, ajustando-os caso necessário. Dessa forma, a etapa 4.15 substitui as etapas 4.1 e 4.2 no novo ciclo de implementação da metodologia. Além disso, diversas atividades das etapas 4.3 e 4.4 já terão sido realizadas, pois o fluxograma e a matriz de riscos e controles de cada subprocesso sob escopo do ciclo anterior já estarão elaborados. Dessa forma, cabe a implementação destas etapas no novo ciclo apenas para os novos subprocessos que passarem a compor o escopo. Para os subprocessos já mapeados, torna-se necessário apenas validá-los e atualizá-los com os departamentos responsáveis. Feito isso, pode-se implementar as atividades da etapa 4.5 em diante no novo ciclo, igualmente ao primeiro ciclo da metodologia.

Segue abaixo a descrição detalhada de cada etapa da metodologia de controles internos proposta.

4.1. DIRECIONAMENTO E ESTRUTURA DE CONTROLES INTERNOS

A primeira medida a ser tomada para que seja possível definir e avaliar controles internos em uma empresa é definir como estará organizada a área responsável por estas atividades. Isso envolve algumas decisões por parte da alta administração da empresa, que dependerão de quanto ela está disposta a investir na atividade, bem como características próprias do mercado e da empresa. Fatores como a obrigatoriedade ou não da avaliação de controles internos (devido à SOX, por exemplo), as regulamentações aplicáveis para o ramo de atividade, os riscos inerentes ao negócio, o ambiente ao qual a empresa está inserida, as perspectivas

para o mercado nos próximos anos e o apetite ao risco da organização devem ser considerados.

Para iniciar a avaliação de como estruturar as atividades de controles internos deve-se primeiramente obter entendimento da atual estrutura da empresa, envolvendo a existência ou não de um departamento de auditoria interna, controles internos e/ou *compliance*, bem como as atividades relacionadas a controles internos que estas áreas já estão executando. É importante que esteja claramente definida a responsabilidade pela gestão dos controles internos da empresa, o que pode ser impactado pela existência de mais de uma área atuando - cada uma com uma perspectiva - sob a mesma matéria de estudo.

Na prática, o departamento de auditoria interna costuma focar seus esforços em evitar e identificar irregularidades, mas não tão comumente a identificar oportunidades de melhoria para a operação, reduzindo o tempo necessário para executar uma atividade e o retrabalho, por exemplo, ou ainda a elevar a qualidade de determinada análise caso ela já cumpra com os padrões mínimos necessários para não ser considerada inefetiva. Em outras palavras, pode-se dizer que há um objetivo principal de avaliar se os processos são efetivos, mas não necessariamente a identificar maneiras de torná-lo ainda melhor.

Por outro lado, em uma perspectiva de gestão de riscos, os departamentos designados como “controles internos” tendem a ser mais consultivos, procurando não apenas evitar irregularidades, mas também otimizar a operação da empresa. Neste contexto, controles internos podem ser vistos como uma ferramenta para gerir processos.

Há ainda a possibilidade de atuação de uma área de *compliance*, que comumente foca seus esforços em impedir e investigar fraudes e outros crimes econômicos, como lavagem de dinheiro, formação de cartel e corrupção, entre outros.

Dessa forma, caso uma empresa já possua uma área de auditoria interna e/ou de *compliance*, porém com um escopo de atuação restrito, cabe à alta administração optar por delegar à uma destas áreas as responsabilidades por definir e avaliar controles internos de forma contínua, estruturar um único departamento responsável por todas as atividades (de controle interno, auditoria e *compliance*), ou então estruturar um novo departamento com objetivo de definir e avaliar controles internos, não alterando as áreas de auditoria interna e/ou *compliance* já existentes.

Fatores como o tamanho da empresa e o capital que se dispõem para investimento devem ser considerados.

Sendo assim, o primeiro direcionamento a ser definido pela alta administração da organização é a profundidade com a qual deseja-se que a área de controles internos (ou outra área com esta função) atue. Esta definição é de extrema importância para o sucesso de todo o projeto de definição e avaliação de controles internos, pois eles se tornam a base para a auditoria da efetividade dos processos, para a definição de planos de otimização na operação da empresa e ainda para prevenção e identificação de fraudes e outros crimes econômicos. Neste contexto, caso não haja apoio adequado da alta administração para a implementação dos eventuais planos de melhoria identificados, a chance de que eles não sejam levados a diante é aumentada substancialmente.

Dessa forma, pode-se definir o suporte da alta administração como um – se não o principal – fator crítico de sucesso para a definição e avaliação de controles internos, bem como a efetiva gestão e implementação dos planos de melhoria. Isso porque, além do apoio para cobrar a implementação dos planos de melhoria, em diversos momentos haverá a necessidade de investimentos financeiros, que dependerão da aprovação da alta administração. Um exemplo são as mudanças nos sistemas de informação, muito comuns em trabalhos de controles internos.

Outro fator crítico para definir a estrutura de controles internos é o apetite ao risco da organização, que pode ser maior ou menor. Isso significa o quão exposta ao risco uma empresa deseja estar. Por mais que sob uma primeira perspectiva haja tendência a acreditar que quanto menor o risco, melhor, esta afirmativa nem sempre é verdadeira.

As diversas empresas, nos diversos ramos do mercado, possuem diferentes culturas organizacionais. Isso envolve, entre outros fatores, o principal objetivo da empresa e sua estratégia, o que faz com que algumas foquem em um crescimento rápido (e mais arriscado) enquanto outras abram mão de um ritmo tão acelerado de crescimento, por optarem por um modelo de gestão mais seguro. Esta definição não envolve apenas os investimentos financeiros da empresa e seu projeto de expansão, por exemplo, mas também a maneira com que os seus processos estão estruturados. Isso pode ser claramente percebido na relação entre custo e segurança, na perspectiva de processos.

Quanto maior a quantidade de controles em um processo, maior tende a ser a quantidade de horas trabalhadas para executá-los. Por exemplo, se em determinado processo um funcionário específico realiza uma análise X, ele levará um certo tempo para executá-la. Porém, se além disso for determinada a necessidade de que outro funcionário revise a análise, mais horas de trabalho serão despendidas. Em contrapartida a análise será mais segura, pois o risco de haver erros na mesma é reduzido através da revisão. Porém mais horas de trabalho foram gastas, o que gera a necessidade de mais funcionários, acarretando em um custo maior com mão de obra. Dessa forma, percebe-se que a implementação de controles nos processos geram um custo financeiro, mesmo que não diretamente.

Dessa forma, se a estratégia da empresa é estar mais exposta a riscos, visando reduzir custos, não se pode dizer que a inexistência do controle descrito no exemplo acima é uma inefetividade de controle, pois o apetite ao risco definido pela alta administração o considera desnecessário. Em outras palavras, a empresa prefere correr o risco de sofrer as consequências que o erro da análise do exemplo acima pode ocasionar do que gastar mais para reduzir a probabilidade de sua ocorrência.

Sendo assim, pode-se perceber que é primordial que haja alinhamento entre o apetite ao risco da organização e os trabalhos de controles internos para o sucesso do projeto. Além disso, este entendimento deve estar claro ao definir a estrutura de controles internos, que precisará ser maior se o apetite ao risco da organização for menor, e vice-versa.

Contudo, em algumas situações, mesmo que o apetite ao risco da organização seja elevado, pode ser necessária uma estrutura robusta de auditoria/ controles internos/ *compliance*. Estes são os casos em que por determinação de alguma lei ou regulamentação a empresa é obrigada a comprovar a efetividade de seus controles, como é no caso de aplicabilidade da Lei norte-americana Sarbanes-Oxley (SOX). Sendo assim, este fator também deve ser considerado ao definir como será a estrutura da empresa.

Vale ainda citar como critério relevante, tanto para a definição do apetite ao risco da empresa, quanto para a estrutura de controles internos, o ambiente no qual a empresa está inserida. Isso envolve uma análise das regulamentações locais – como leis trabalhistas, ambientais, entre outras – e também outros acordos e regras impostas à empresa, assim como a legislação local para a comercialização ou

produção do objeto de negócio da organização. Estas variáveis devem ser consideradas por interferirem no risco inerente do negócio, ou seja, os riscos que existem simplesmente pelo fato da organização operar. Um exemplo é o risco de perdas financeiras devido a processos trabalhistas, pois uma vez que a empresa tenha funcionários, ela estará sujeita a este risco. Dessa forma, quanto mais acirradas forem as leis e regulamentações aplicáveis à empresa - devido às leis do país em que ela opera -, maiores tendem a ser os riscos, fazendo com que a estrutura para mitigá-los adequadamente tenha que ser maior.

Sabendo-se de todas essas variáveis, cabe à alta administração definir qual será o departamento responsável por gerir os controles internos da organização (mesmo que, conforme exposto nos capítulos a seguir, fique claro que todos os departamentos são responsáveis pela efetividade dos controles internos). Um fator a ser considerado nesse processo é a independência do departamento, ou seja, seu reporte direto para a presidência e/ou para um comitê de auditoria, por exemplo. Essa estrutura visa proporcionar imparcialidade nas análises realizadas, bem como evitar conflitos de interesse entre a área avaliadora e avaliada.

Em alguns casos, para empresas em que não haja obrigatoriedade de uma área independente de auditoria, e ao mesmo tempo a alta administração não julgue necessária sua criação, uma área de controles internos pode ser alocada sob a diretoria financeira e assumir a responsabilidade pela gestão dos controles internos da empresa. Esta estrutura pode ser justificada pelo impacto que os controles interno exercem sob as demonstrações financeiras, bem como ao foco de redução de custos ou até mesmo prevenção de fraudes. Contudo, vale ressaltar que por mais que seja possível, esta estrutura não é a mais indicada para grandes empresas, por haver possível conflito de interesse dentro da própria diretoria financeira com as atividades de controle interno, que estão comumente relacionadas à aspectos de auditoria e *compliance*. Dessa forma, perde-se confiabilidade quanto à identificação de possíveis fraudes que podem acontecer na própria diretoria financeira, por exemplo. Por esse motivo, deve ficar clara a limitação das avaliações realizadas, não sendo possível considerá-las equivalentes às avaliações realizadas por uma área independente. Porém, no âmbito “consultivo”, visando identificar melhorias nos processos e na operação da empresa, a estrutura é possível.

Por fim, vale ressaltar que independentemente de qual estrutura seja adotada, é fundamental que os trabalhos executados pelo departamento responsável estejam

alinhados ao tom definido pela alta administração, bem como haja evidente suporte desta para a execução dos trabalhos. Em outras palavras, uma vez que certamente serão identificadas necessidades de mudanças nos processos - e naturalmente haverá, em algum momento, resistência em implementá-las -, é importante que o departamento responsável “tenha força” suficiente para obter a atenção necessária dos outros departamentos e para fazer as mudanças se concretizarem.

4.2. DEFINIÇÃO DO ESCOPO

Uma vez definida a estrutura que a empresa adotará para gerir seus controles internos e o departamento responsável pela execução desta atividade – que será denominado “departamento de controles internos” neste trabalho -, cabe a ela definir qual será o escopo dos trabalhos de controles internos. Vale lembrar que tanto o escopo, quanto a quantidade de funcionários que irão compor o departamento devem estar alinhados com a estrutura definida para a área. Além disso, cabe ressaltar que o “departamento de controles internos” não precisa necessariamente possuir esta nomenclatura, bem como executar apenas as atividades descritas neste trabalho.

À luz do exposto, torna-se possível abordar os fatores relevantes para a definição do escopo, que será composto por diversos processos a serem mapeados. Entende-se como processo, neste contexto, o grupo de atividades desempenhadas por um ou diversos departamentos da empresa, que visam um objetivo em comum. Um exemplo é o processo de vendas, que pode-se considerar iniciado na prospecção de clientes, passando pela análise de crédito, cadastro do cliente, realização da venda, contratação do frete, carregamento, entrega, cobrança, recebimento e contabilização do pagamento, por exemplo. Sendo assim, o processo de vendas não envolve apenas o departamento de vendas, mas também o de análise de crédito, logística, fiscal, contas a receber e contábil, por exemplo, além do de tecnologia da informação, que está presente como suporte em todas as etapas do processo que envolvem um sistema de informação.

Dessa forma, para definir quais processos devem ser mapeados, a alta administração deve avaliar em quais deles estão os principais riscos para a empresa, que representem maior ameaça aos seus objetivos.

Por mais que essa atividade possa parecer simples, na prática ela se torna extremamente desafiadora, pois nem sempre a alta administração irá convergir na classificação dos riscos. Além disso, o entendimento da empresa pelos membros da alta administração é diferenciado pela área de atuação de cada um, em outras palavras, cada membro conhece no detalhe suas atividades, porém conhece de maneira superficial as demais atividades da empresa. Adicionalmente, empresas que não possuem seus controles internos definidos e avaliados periodicamente (o que é subentendido neste momento, já que este capítulo busca justamente definir um escopo para esta atividade), dificilmente possuem reuniões periódicas da alta administração com o objetivo principal de discutir riscos. Habitualmente as reuniões são direcionadas à discussão de problemas que já afetam a organização, mas não tão comumente a alinhar o entendimento sobre os riscos que podem vir a afetar a empresa. Mesmo que isso aconteça, sem um direcionamento metodológico adequado, dificilmente haverá um suficiente grau de confiabilidade de que todos os principais riscos estão sendo considerados.

Dessa forma, a primeira atividade do departamento de controles internos deve ser a condução de um projeto de gestão de riscos no nível organizacional, com os principais objetivos de identificar quais são os principais riscos para os objetivos do negócio e definir como mitigá-los. Para isso, um profissional de alto conhecimento e experiência na área de controles internos deve estar a frente do projeto. Ele deverá conduzir entrevistas individuais e, quando necessário, em grupo, com os principais membros da alta administração da empresa. Além disso, deverá coletar as informações históricas da organização, disponíveis através de diversos documentos, como atas de reunião da diretoria, demonstrações financeiras, análises realizadas pelo comitê de ética, pesquisas de mercado ou de cunho estratégico, entre outros. Através da análise dos documentos e das entrevistas, devem ser identificadas as principais causas para que as metas anteriores da organização não tenham sido alcançadas. Além disso, as atuais metas da organização devem ser entendidas pelo profissional.

Através dessas medidas, e de outras que o profissional de controles internos julgue necessárias, um entendimento holístico da organização deve ser atingido, ou seja, por ouvir todos os principais membros da alta administração e estudar as metas e o histórico da empresa, o profissional de controles internos deve ser capaz de identificar os principais riscos existentes, de forma inter-relacionada. Estes devem

ser descritos e classificados conforme sua probabilidade de ocorrência e grau de impacto. O resultado desta análise faz com que os riscos com maior probabilidade de ocorrência e maior impacto para a organização sejam classificados como mais críticos.

Uma vez preparada esta análise, a mesma deve ser apresentada a todos os membros da alta administração, que deverão avaliá-la e discuti-la. Neste momento todos os ajustes necessários na identificação e classificação inicial dos riscos devem ser realizados, o que é comum, pois várias opiniões serão expostas. O julgamento profissional e a competência na área de atuação devem ser utilizados ao classificar os riscos quanto à probabilidade de ocorrência e grau de impacto.

Esta discussão, além de permitir o direcionamento dos trabalhos de controles internos, proporciona um entendimento melhor por parte de todos os membros da alta administração quanto aos riscos existentes nos processos que não estão sob sua responsabilidade direta. Dessa forma, há um ganho em aspectos de comunicação e, logo, maior tendência à sinergia entre a alta administração.

Após uma série de reuniões e discussões a cerca dos principais riscos estratégicos aos quais a empresa está sujeita, uma classificação final deve ser elaborada, por meio de consenso. Com base nesta classificação, a alta administração deverá definir quais riscos devem ser trabalhados inicialmente através das atividades do departamento de controles internos. Dessa forma, a alta administração direciona os esforços da empresa para aquilo que é mais importante para que ela atinja seus objetivos. Vale citar que a estrutura do departamento de controles internos deve ser condizente com a quantidade e complexidade dos riscos definidos para o início dos trabalhos. O profissional de controles internos deve formalizar a relação dos riscos que serão abordados inicialmente através de ata da reunião, coletando as devidas assinaturas dos membros presentes.

Uma vez que o departamento de controles internos conheça os principais riscos para a organização, cabe a ele desdobrar os riscos estratégicos selecionados para os processos da empresa. Essa tarefa exige grande conhecimento técnico e experiência, pois através dela serão definidos os subprocessos que formarão o escopo de trabalho de controles internos. Uma definição equivocada pode fazer com que a empresa não seja capaz de gerir adequadamente os seus riscos mais relevantes.

Ao analisar um processo e sua composição, percebe-se que ele não passa de um conjunto de atividades e controles desenhados para mitigar riscos e atingir um ou mais objetivos. Um exemplo é o processo de tesouraria. Um de seus principais objetivos é gerir e disponibilizar os recursos financeiros necessários para a empresa. Para isso, ao longo do processo, uma série de controles são desenhados no nível operacional, visando atingir este objetivo. Além disso, os controles visam mitigar um risco, por exemplo, de que não haja disponibilidade de recursos suficientes para a empresa, afetando a sua capacidade de operar, o que geraria quebras de contrato, perdas financeiras, deterioração de sua imagem, entre outros. Dessa forma, pode-se dizer que para mitigar estes riscos é que o próprio processo de tesouraria existe, ou seja, se não houvesse riscos, não haveria a necessidade de se estruturar um processo.

Contudo, em diversos momentos um mesmo risco está alocado em diversos processos da empresa. Por exemplo, o risco de que não haja a disponibilidade necessária de recursos para a operação da empresa, além de estar inserido no processo de tesouraria, também está inserido no processo de análise de crédito de clientes. Isso porque, através da análise de crédito define-se a política e o limite de crédito que será concedido a cada cliente, o que afeta diretamente a possibilidade de inadimplência. Logo, quanto maior a inadimplência, menor será a disponibilidade de recursos. Sendo assim, se a indisponibilidade de recursos para a operação da empresa for classificada como um dos riscos estratégicos que a alta administração definiu como crítico, ambos os processos de tesouraria e análise de crédito de clientes deverão compor o escopo de subprocessos a serem mapeados pelo departamento de controles internos.

Dessa forma, todos os subprocessos relevantes para que seja possível mitigar de forma adequada os riscos estratégicos selecionados pela alta administração devem ser definidos, integrando o escopo de controles internos.

4.3. MAPEAMENTO DOS PROCESSOS

Sabendo-se os subprocessos que deverão ser mapeados, torna-se possível iniciar o mapeamento no nível operacional. Porém, antes disso, algumas atividades devem ser desempenhadas pelo departamento de controles internos, visando menor

resistência dos demais departamentos e maior eficácia na identificação e avaliação de riscos e controles, conforme abaixo.

4.3.1. Preparação para o mapeamento

A comunicação adequada entre o departamento de controles internos e os demais da organização é um fator crítico de sucesso. O objetivo do projeto de definição e avaliação de controles internos precisa estar claro pra todos os envolvidos. Por esse motivo, uma apresentação deve ser elaborada para todos os gerentes que estarão envolvidos direta ou indiretamente no mapeamento dos processos. Esta deve esclarecer qual o objetivo do projeto, para que ele serve, quais são as responsabilidades do departamento de controles internos e dos demais departamentos, qual é o fluxo de trabalho e as etapas envolvidas, o escopo do projeto, qual será o produto final do mesmo, entre outros. Adicionalmente, o suporte recebido pelo presidente e pela alta administração deve ficar explícita.

4.3.2. Mapeamento

Uma vez que a comunicação esteja estabelecida com os demais departamentos, torna-se possível iniciar na prática o mapeamento dos subprocessos que compõem o escopo de definição e avaliação de controles internos. Para isso, o responsável pelo departamento de controles internos deve elaborar um cronograma com os processos e subprocessos sob escopo e realizar uma reunião de abertura com o gestor e/ou diretor do departamento envolvido naquele momento do projeto. Esta reunião é importante pois semanas ou meses podem ter se passado da reunião de apresentação inicial do projeto, uma vez que todos os departamentos da empresa dificilmente serão envolvidos de uma única vez, mas sim gradativamente, ao decorrer do cronograma definido.

Além disso a reunião visa validar com cada departamento o seu envolvimento nos subprocessos que serão mapeados naquele momento do projeto. Adicionalmente os responsáveis por cada subprocesso - usualmente os respectivos gerentes - deverão indicar quais funcionários devem ser entrevistados para o entendimento da operação de cada subprocesso.

É importante que os entrevistados possuam um vasto conhecimento da operação do subprocesso a ser mapeado. Sendo assim, normalmente as entrevistas são conduzidas com supervisores ou analistas.

As entrevistas constituem a principal fonte de informações para o mapeamento dos processos. Elas devem ser conduzidas por um profissional experiente de controles internos, responsável por realizar todos os questionamentos necessários a fim de elaborar um fluxograma do subprocesso, que deve possuir um nível de detalhe suficiente para responder: o que, quando, onde, quanto e como para cada atividade descrita. Além disso, o elaborador deve se preocupar com a racionalização do fluxograma, ou seja, o leitor deve conseguir concluir um "por que" das atividades mapeadas.

Uma vez elaborado o fluxograma, torna-se necessário validar as informações registradas no mesmo. Para isso, um procedimento chamado "teste de desenho" deve ser executado pelo profissional de controles internos.

4.3.3. Teste de desenho

Visando certificar-se de que o fluxograma elaborado na etapa anterior está em conformidade com as atividades e controles desempenhados no subprocesso, o profissional de controles internos deve executar um teste de desenho para cada controle.

Os testes de desenho devem ser realizados utilizando uma amostra recente dos documentos envolvidos no subprocesso em questão, de forma que o profissional de controles internos possa analisar se, na prática, a maneira com que as atividades vêm sendo desempenhadas estão desenhadas de uma maneira capaz de mitigar os riscos existentes no processo.

Sendo assim, os testes de desenho possuem uma função importante na validação do fluxograma e na avaliação dos controles do subprocesso, ainda que esta avaliação não seja capaz de julgar quanto à efetividade ou não dos controles em si, mas sim apenas quanto à maneira com que os mesmos foram propostos.

Uma cópia dos documentos utilizados na execução dos testes de desenho deve ser mantida pelo profissional de controles internos, para futuras análises e formalização dos testes. Além disso, a descrição dos procedimentos executados deve ser inserida na matriz de riscos e controles (que é apresentada ao leitor na

etapa seguinte da metodologia). Além disso, na matriz ainda deve ser inserido o resultado do teste, ou seja, o julgamento do profissional de controles internos quanto à capacidade do controle em mitigar o risco em questão, avaliando a maneira com que o mesmo foi proposto. O resultado pode ser ’efetivo" ou "inefetivo".

Vale ainda mencionar que por mais que os testes de desenho estejam inseridos na etapa "4 - Mapeamento", eles também poderiam ser considerados o início da etapa "5 - Identificação de Riscos e Controles". Isso acontece pois, em certo momento, o mapeamento do processo e a identificação de riscos e controles se misturam. Porém, visando uma melhor disposição desta metodologia, optou-se por deixar os testes de desenho na etapa de mapeamento.

4.4. IDENTIFICAÇÃO DE RISCOS E CONTROLES

Juntamente com o entendimento das atividades executadas - obtido ao longo das entrevistas -, os riscos e controles existentes no subprocesso devem ser identificados pelo profissional de controles internos que estiver responsável por elaborar o fluxograma. Esta atividade acontece tanto através das entrevistas quanto através dos testes de desenho. Sendo assim, a elaboração do fluxograma é um meio para realizar a análise de riscos e controles do subprocesso, conduzida pelo profissional de controles internos, com o suporte do entrevistado. Além disso, o fluxograma e os testes de desenho servem como formalização do mapeamento e fonte de consulta para posteriores análises.

É primordial a definição de regras e direcionamentos para a descrição padronizada de riscos e controles e a descrição dos mesmos, bem com suas classificações, que devem ser realizadas na matriz de riscos e controles. Atualmente já existem softwares capazes de gerar uma matriz de riscos e controles a partir de um fluxograma. Porém, na ausência desta ferramenta, uma planilha excel pode substituí-la adequadamente.

Sendo assim, estão apresentadas as duas principais ferramentas utilizadas para a avaliação de riscos e controles: fluxograma e matriz de riscos e controles. Os modelos padrão a serem utilizados nesta metodologia, para ambos, seguem abaixo.

4.4.1. Fluxograma

Os fluxogramas são habitualmente preparados com base em formas padronizadas, que indicam a descrição de uma atividade, uma decisão, ou a conexão com outro fluxograma, por exemplo. Segue abaixo o modelo de fluxograma e também as descrições referente à utilização de cada forma a serem utilizadas nesta metodologia.

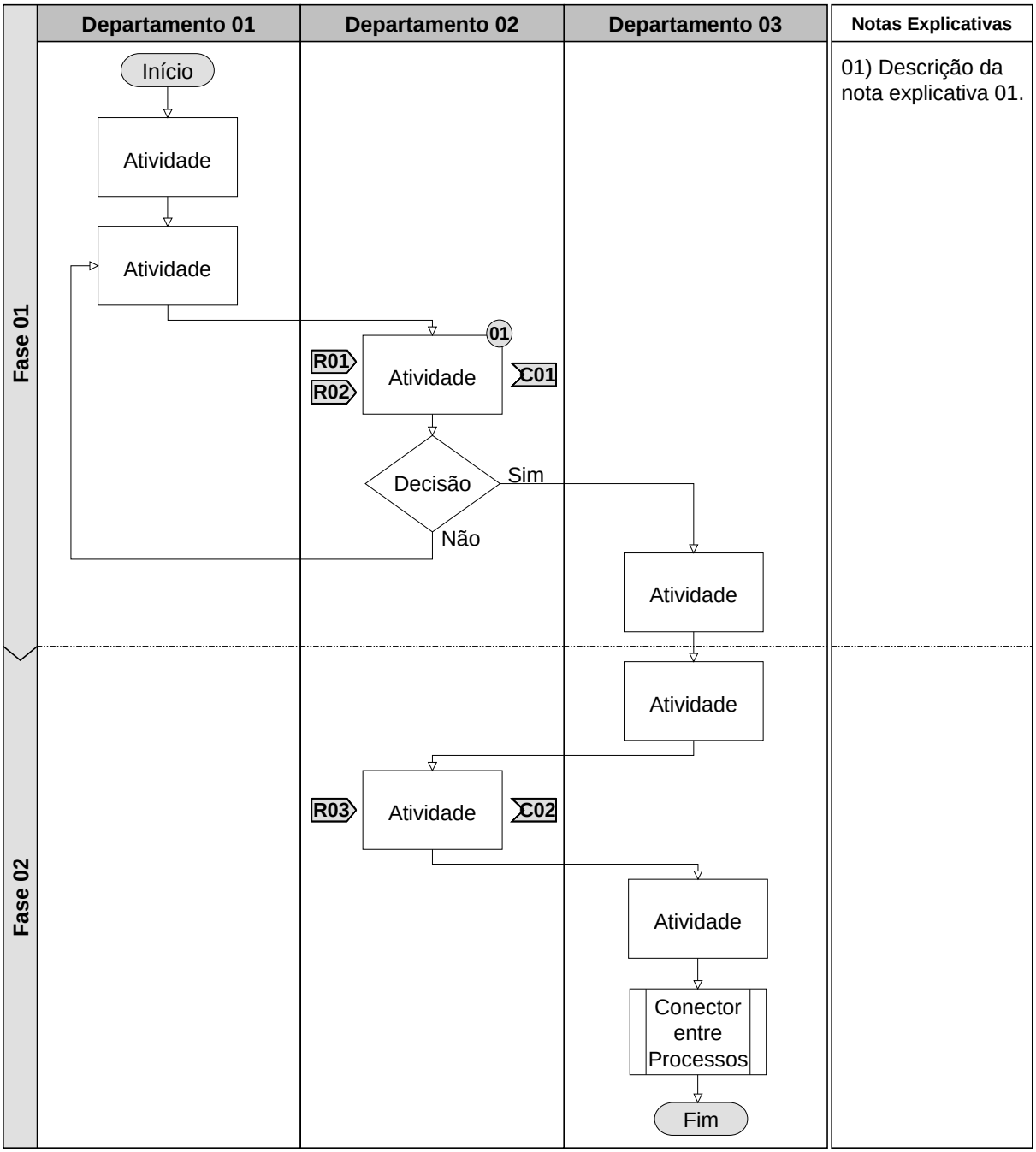

FIGURA 2 – MODELO DE FLUXOGRAMA

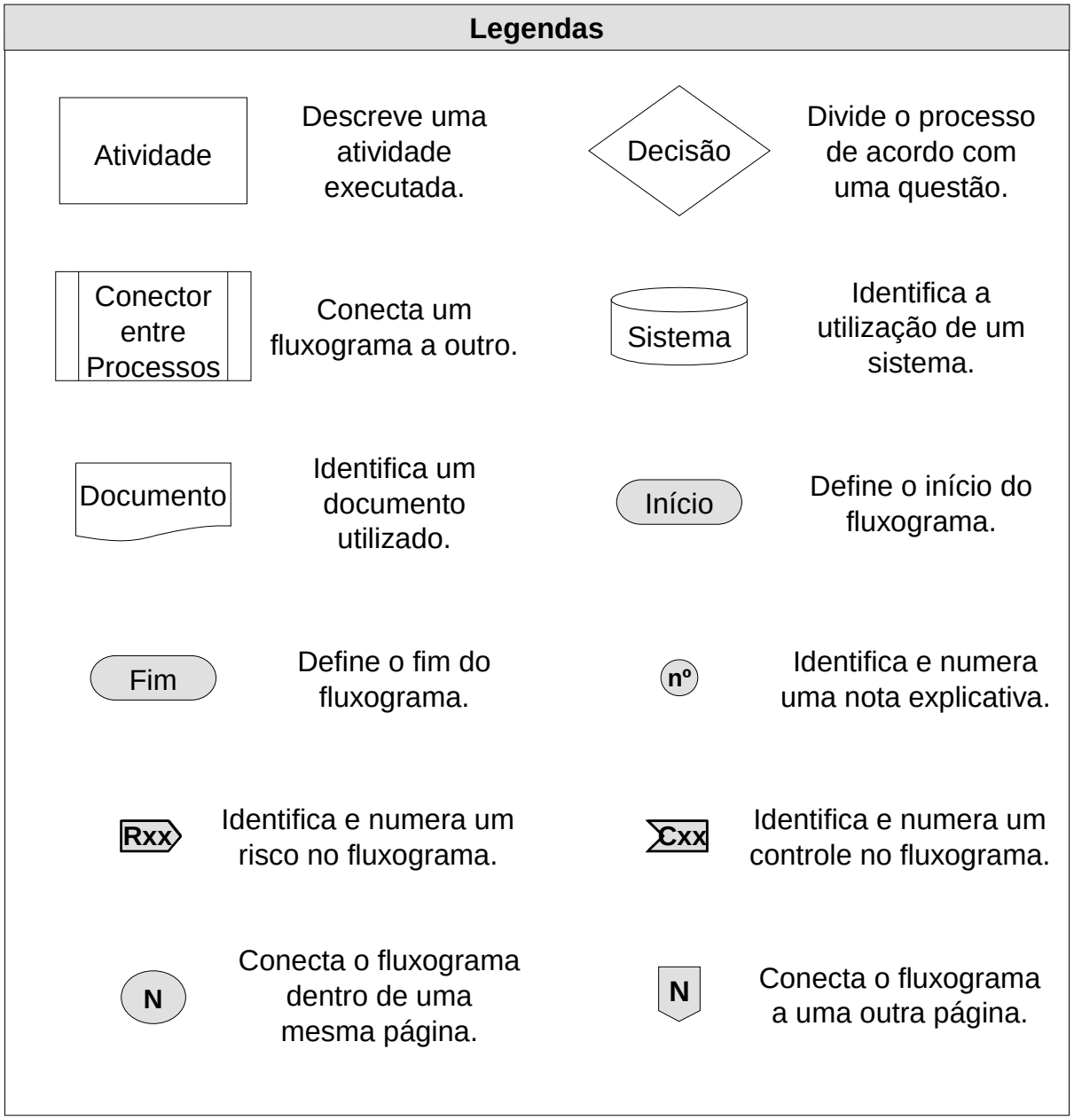

FIGURA 3 – LEGENDAS DO FLUXOGRAMA

4.4.2. Matriz de riscos e controles

A matriz de riscos e controles tem como principal objetivo relacionar os riscos identificados ao longo do processo com os respectivos controles. Dessa forma, nela estão inseridas diversas informações, como descrição dos riscos, descrição dos controles, responsável pelo controle, classificação do controle, entre outras. Vale mencionar ainda que a matriz de riscos e controles deve referenciar o fluxograma ao qual o subprocesso se refere. Dessa forma, a mesma numeração utilizada para

identificar os riscos e controles ao longo do fluxograma deve ser utilizada na matriz de riscos e controles.

Habitualmente é possível dividir a matriz de riscos e controles em três principais blocos de mapeamento, denominados “processo”, “riscos” e “controles”. Além disso, pode-se adicionar na matriz campos para a avaliação do processo – nos blocos "autoavaliação pelo departamento" e “avaliação pelo departamento de controles internos” – e para a definição dos planos de remediação – no bloco “planos de remediação”. Estes, em outras metodologias, podem constituir um outro documento, complementar à matriz de riscos e controles, com objetivo de testar os controles, descrever as inefetividades e definir os planos de remediação. Porém, visando uma maior praticidade na avaliação de riscos e controles, esta metodologia define a unificação do mapeamento com estas atividades. Segue abaixo a relação das colunas que devem compô-la, subdivididas entre os blocos propostos.

O primeiro bloco, “processo”, contempla:

Departamento: Nome do departamento responsável pelo subprocesso. Exemplo: compras.

Processo: nome do processo mapeado. Exemplo: compras.

Subprocesso: nome do subprocesso mapeado. Exemplo: cadastro de fornecedores.

Responsável pelo subprocesso: cargo do responsável pelo subprocesso mapeado. Exemplo: gerente de compras.

Referência do fluxograma: nomenclatura única dada ao fluxograma do subprocesso em questão. Exemplo: FL.01.

Objetivo de Controle: descrição do objetivo que o controle pretende atingir. Exemplo: realizar compras com a melhor opção de fornecedores do mercado, levando em conta aspectos técnicos e de preço.

O segundo bloco, denominado “riscos”, contém:

Risco: descrição do risco em questão, ou seja, do efeito negativo que pode incorrer devido à inexistência ou inefetividade de um controle. O risco não deve ser descrito como a ausência de um controle, mas sim como a possibilidade de um efeito negativo. Exemplo incorreto de descrição de risco: ausência de aprovação de compras. Exemplo correto: perdas financeiras por compra de mercadorias acima do preço de mercado.

Número do risco: numeração única do risco. Deve ser a mesma utilizada nos fluxogramas dos subprocessos mapeados. Exemplo: R01.

O terceiro bloco, “controles”, engloba:

Descrição do controle: descrição do controle em questão, que deve permitir ao leitor compreender “o que”, “quem”, “como”, “quando” e “aonde” o mesmo é desempenhado. Através dela, a racionalização do “por que” deve ser possível. Exemplo: todas as compras de materiais indiretos acima de R$ 2000,00 reais são revisadas e aprovadas pelo gerente de compras, através de assinatura no formulário X. Para isso, no mínimo três cotações com diferentes fornecedores são realizadas pelo analista de compras, que preenche o formulário X, assina-o e o encaminha ao gerente de compras. O formulário X permanece arquivado no departamento por cinco anos.

Número do controle: numeração única do controle. Exemplo: C01.

Teste de desenho: descrição do teste de desenho executado pelo profissional de controles internos para avaliar o desenho do controle. Exemplo: verificou-se "in loco", através do sistema X, que as ordens de compra precisam ser aprovadas pelo gestor da área para terem seu status alterado para "aprovado".

Resultado do teste de desenho: o resultado do teste de desenho deve ser "efetivo" ou "inefetivo". Ao julgar que o desenho do controle é efetivo, entende-se que a maneira com que o mesmo foi proposto é capaz de mitigar o risco em questão de maneira suficiente.

Categoria do controle: a categoria de um controle pode ser: acesso, autorização, configuração, indicador de performance, interface, reconciliação, relatório de exceções, revisão gerencial ou segregação de funções. O detalhamento de cada possibilidade está inserido no capítulo "4.5 Classificação dos Controles".

Manual/ automático: o controle pode ser classificado como "manual" ou "automático". O detalhamento de ambas as possibilidades está inserido no capítulo "4.5 Classificação dos Controles".

Preventivo/ detectivo: o controle pode ser classificado como "preventivo" ou "detectivo". O detalhamento de ambas as possibilidades está inserido no capítulo "4.5 Classificação dos Controles".

Frequência: definição da periodicidade com que um controle é executado. Algumas possibilidades são: sob demanda, diário, semanal, mensal, semestral, anual, etc..

Mais detalhes sobre a frequência de um controle estão inseridos no capítulo "4.5 Classificação dos Controles".

Para elaboração dos três blocos descritos acima, deve-se levar em conta o estado atual dos processos, e não a maneira como pretende-se que eles sejam executados. Esta medida é fundamental para evitar análises incorretas a cerca da conformidade dos desenhos dos controles.

Vale ressaltar que o preenchimento dos campos acima deve ser realizado no mesmo momento em que o fluxograma estiver sendo elaborado, pelo profissional de controles internos. Dessa forma, a matriz de riscos e controles permite complementar o entendimento e o mapeamento de um subprocesso.

Além disso, ela serve como base para realização dos testes de efetividade, que são o principal objeto do quarto bloco da matriz de riscos e controles proposta, denominado “autoavaliação do departamento”, que contém:

Referência de teste: **n**omenclatura única para referenciar um teste. Exemplo: P01.S01.C01.R01.

Evidências: descrição de todos os documentos necessários para realizar o teste de efetividade do controle. Exemplo: nota fiscal e pedido de compras.

Amostra: definição da amostra a ser testada. Exemplo: Pedido de Compras nº 111.

Responsável pelo controle: cargo do responsável pela execução do controle.

Procedimento de teste: descrição do procedimento de teste que deve ser executado pelo responsável pela autoavaliação do controle. Este procedimento é descrito previamente pelo profissional de controles internos e deve ser seguido como um guia de autoavaliação.

Descrição da inefetividade (autoavaliação): descrição da inefetividade identificada através da autoavaliação do controle, caso haja. Exemplo: os materiais indiretos inseridos no pedido de compras nº 111 foram recebidos sem que o pedido de compras estivesse previamente aprovado.

Resultado de teste: o resultado de teste pode ser "efetivo" ou "inefetivo".

Valor do teste: definição do valor que a efetividade do controle representa. Este campo pode ser melhor compreendido através da etapa "4.6 - Definição dos Procedimentos e Valor dos Testes de Controle".

No quinto bloco da matriz de riscos e controles, "avaliação pelo departamento de controles internos", consta a avaliação realizada pelo departamento de controles internos. Esta é preparada com base na autoavaliação de cada departamento, como pode ser observado na etapa "4.8 - Avaliação de Controles Internos". O bloco conta com os respectivos campos:

Procedimento de teste (por controles internos): descrição do procedimento de teste executado pelo profissional de controles internos para avaliar a autoavaliação elaborada previamente pelo departamento. Exemplo: a nota fiscal nº 111 e o pedido de compra nº 222 foram verificados, sendo constatada adequação do valor, descrição do item, unidade de medida e fornecedor entre os documentos. Adicionalmente, verificou-se “in loco” que, para os recebimentos de materiais indiretos, há conferência dos documentos supracitados com a quantidade física durante o recebimento.

Descrição da inefetividade (controles internos): descrição da inefetividade identificada através da avaliação do controle realizada pelo profissional de controles internos, caso haja. Exemplo: os materiais indiretos inseridos no pedido de compras nº 111 foram recebidos sem que o pedido de compras estivesse previamente aprovado.

Resultado de teste (controles internos): o resultado de teste pode ser "efetivo" ou "inefetivo".

Por fim, o último bloco da matriz de riscos e controles, “planos de remediação”, contempla a classificação das inefetividades e a definição das ações necessárias para tornar os controles classificados como “inefetivos” em “efetivos”:

Probabilidade de ocorrência: classificação da frequência esperada para a materialização do risco, em virtude da inefetividade do controle. Pode ser “alta”, “média” ou “baixa” e sua definição está detalhada no capítulo “4.9 – Planos de Remediação”.

Grau de impacto: classificação do impacto que a materialização do risco pode provocar. Pode ser “alto”, “médio” ou “baixo” e sua definição está detalhada no capítulo “4.9 – Planos de Remediação”.

Criticidade: é resultado do produto entre "probabilidade de ocorrência" e "grau de impacto". Pode ser “alta”, “média” ou “baixa” e sua definição está detalhada no capítulo “4.9 – Planos de Remediação”.

Prazo: prazo definido para implementação do plano de remediação. Deve ser definido com base na complexidade para implementar o plano de remediação e na criticidade da inefetividade do controle.
Plano de Remediação: descrição do plano de remediação para que o controle passe a ser efetivo. Exemplo: o assistente de recepção 1 realizará a contagem física dos materiais indiretos recebidos e a anotará no formulário X. Este será entregue ao assistente de recepção 2, que verificará se a quantidade está de acordo com a Ordem de Compra e a Nota Fiscal.

Ao término da etapa “4.4 – Identificação de Riscos e Controles”, o fluxograma do subprocesso em questão deve estar finalizado. Além disso, os blocos “processo” e “riscos” da matriz de riscos e controles também já devem estar preenchidos, enquanto para o bloco “controles”, a coluna “descrição do controle” também já deve estar elaborada. Dessa forma, torna-se possível iniciar o processo de classificação dos controles, descrito no capítulo a seguir. Vale ressaltar que até a etapa “4.7 – Validação do Mapeamento e da Matriz de Riscos e Controles”, é possível – e comum – a realização de ajustes conforme a necessidade no fluxograma e na matriz de riscos e controles.

4.5. CLASSIFICAÇÃO DOS CONTROLES

A classificação dos controles auxilia o profissional de controles internos a avaliar o processo em questão, pois direciona os procedimentos de teste de efetividade. Dessa forma, na matriz de riscos e controles deve constar a classificação dos controles conforme as suas possíveis categorias, tipos e frequências, conforme a seguir.

4.5.1. Categorias de controle

A categoria do controle está diretamente relacionada ao seu principal objetivo e busca sintetizar a maneira com que o mesmo é desempenhado. Em alguns momentos, pode-se perceber que um mesmo controle pode ser classificado em mais de uma categoria. Nestes casos, deve-se optar por aquela que melhor se enquadre, direcionando os procedimentos de testes - a ser realizados na etapa de avaliação

dos controles - de forma mais objetiva, indo de encontro ao que o profissional de controles internos considera mais relevante.

Dessa forma, cabe ao profissional de controles internos responsável pela identificação, definição e descrição dos controles, optar por uma das categorias abaixo:

Acesso: controla a capacidade dos indivíduos a operar sistemas, realizar transações ou acessar locais específicos da organização, por meio de definições de alçada ou perfis de acesso. Os controles de acesso possuem grande relevância para o controle de transações críticas da empresa, como realização de pagamentos, lançamentos contábeis, baixas de contas a receber, entre outras. Podem ainda assumir um papel importante para a salvaguarda de ativos físicos, evitando que funcionários não autorizados ou outros indivíduos, tenham acesso a locais de guarda de bens de grande valor.

Autorização: determina a necessidade de aprovação para a execução de atividades ou transações relevantes, por meio de políticas, procedimentos e níveis hierárquicos. Os controles de autorizações podem ser realizados tanto em meios físicos, por exemplo, através de assinaturas em formulários específicos, quanto em meios sistêmicos, através da aprovação eletrônica de transações.

Configuração: buscam preservar a integridade de informações da empresa, evitando o processamento incorreto de dados. Estão comumente inseridos em sistemas de informação, através de parametrizações de sistema. Dessa forma, costumam ser eficazes para mitigar riscos de esquecimento ou erro.

Indicador de performance: objetiva a avaliação e o monitoramento contínuo de fatores importantes para a operação da empresa, que permitam comparabilidade e expressem eficiência e/ou eficácia. São reportados às diferentes esferas de gestão, que os utiliza para acompanhar os resultados obtidos e as metas definidas. Comumente são chamados de KPIs (*Key Performance Indicators*) e assumem um papel importante para a controladoria e governança empresarial.

Interface: refere-se à transferência de informações entre sistemas, que pode ser realizada de maneira manual ou automática. Visa assegurar a precisão e a integridade das informações transferidas. A interface entre sistemas de suporte operacional - como de gestão de estoques, folha de pagamento, etc. - e o sistema contábil da empresa costuma ser um importante fator para a confiabilidade das informações.

Reconciliação: compara a conformidade entre duas diferentes bases de dado, visando averiguar a existência de divergências, que, caso existam, devem ser apontadas e tratadas de forma tempestiva. As reconciliações são utilizadas habitualmente nos processos de fechamento contábil, visando validar os saldos existentes nos módulos operacionais do sistema de informações com o módulo contábil.

Relatório de exceções: refere-se à identificação de desvios ou exceções em transações específicas e normalmente são gerados de forma automatizada pelos sistemas de informação. Costumam ser utilizados para identificar e tratar erros de forma otimizada.

Revisão gerencial: refere-se à análise crítica desempenhada por um profissional com conhecimento suficiente para avaliar a razoabilidade de números, resultados ou outros aspectos relevantes. Ele pressupõe a necessidade de habilidade técnica do revisor, que pode assumir um cargo de gerência ou não. Vale ainda ressaltar que o controle de revisão gerencial comumente assume a segregação de funções em grandes empresas.

Segregação de funções: busca prevenir que indivíduos tenham a possibilidade de executar e/ou autorizar transações e atividades incorretamente, de forma intencional ou não. Dessa forma, o controle de segregação de funções separa funções e responsabilidades, não deixando que duas etapas críticas de um processo estejam concentradas sob responsabilidade de um mesmo indivíduo. Um exemplo é a segregação de funções entre criação e a aprovação de ordens de compra.

4.5.2. Tipos de controle

Os controles podem ser preventivos ou detectivos, e ainda manuais ou automáticos. A definição de cada possibilidade segue abaixo.

Controle preventivo: possui como objetivo evitar a ocorrência de uma inconformidade. Dessa forma, são estruturados para prevenir a materialização de um risco.

Controle detectivo: possui como objetivo a identificação de uma inconformidade, de forma que seja possível realizar a correção cabível, em tempo hábil.

Controle manual: é aquele que necessita de interação humana para sua execução. Vale ressaltar que o mesmo pode ser realizado através de um sistema informatizado, não deixando de ser manual.

Controle automático: é aquele realizado por um sistema informatizado, sem necessidade de intervenção humana, ou seja, que acontecem automaticamente, por meio de parametrizações sistêmicas, por exemplo.

4.5.3. Frequências de controle e amostra para teste de efetividade

Cada controle possui uma frequência, ou seja, uma periodicidade específica para execução, que afeta diretamente o tamanho da amostra necessária na etapa de avaliação. Controles que são desempenhados com maior frequência necessitam de uma amostra de teste maior. Isso acontece porque, estatisticamente, quanto maior for a população total (ou seja, o número de vezes que o controle foi executado), maior deve ser o tamanho da amostra testada para que se mantenha o mesmo grau de confiabilidade. Dessa forma, segue abaixo algumas sugestões de frequência, com a respectiva quantidade mínima de amostras a ser testadas:

Frequência do Controle	Tamanho da Amostra
Sob Demanda	25
Diário	25
Semanal	10
Mensal	03
Bimestral	02
Trimestral	02
Anual	01

TABELA 1 - TAMANHO DA AMOSTRA DE TESTE

Novas opções de frequência podem ser criadas conforme a necessidade, por exemplo, para controles desempenhados a cada quinze dias. Nestas situações, o tamanho da amostra a ser utilizada deve ser no mínimo igual à da frequência anterior. Sendo assim, no caso de um controle quinzenal, o tamanho de amostra equivalente seria o mesmo de um controle semanal, ou seja, no mínimo dez amostras.

Vale ressaltar que em circunstâncias específicas, o profissional de controles internos pode julgar necessária a extensão do tamanho da amostra. Sendo assim, a definição acima não deve limitar o julgamento do profissional.

4.6. DEFINIÇÃO DOS PROCEDIMENTOS E VALOR DOS TESTES DE CONTROLE

Tendo como base a descrição do controle, os riscos e as documentações envolvidas - que nesta altura já deverão estar devidamente documentadas na matriz de riscos e controles -, o profissional de controles internos deverá determinar os procedimentos de teste a serem executados, isso é, quais etapas e requisitos devem ser seguidos e avaliados ao analisar um determinado controle. Dessa forma, neste momento a descrição do procedimento de teste deve ser adicionada na matriz de riscos e controles. Esta será utilizada por cada departamento para a realização da autoavaliação dos controles internos. Por esse motivo, a descrição dos procedimentos deve ser clara e metódica, visando minimizar a possibilidade de dupla interpretação.

Além disso, o profissional de controles internos deverá definir a pontuação que cada teste de controle valerá, isso é, o valor que a efetividade do teste proporciona. Para isso, 1000 pontos (pontuação máxima) devem ser distribuídos entre a totalidade de controles do subprocesso, conforme a criticidade de cada um deles.

A definição de valores para os controles tem como objetivos a quantificação, de maneira numérica, do grau de efetividade que um determinado subprocesso possui em termos de controles internos, o direcionamento de prioridades para implementação dos planos de remediação por parte dos departamentos e ainda o estímulo ao engajamento dos gestores de cada departamento, atrelando o resultado da avaliação de controles internos à avaliação de desempenho de cada gestor. A maneira com que pretende-se atingir esses objetivos são explicados com maior detalhe ao longo das próximas etapas da metodologia.

4.7. VALIDAÇÃO DO MAPEAMENTO E DA MATRIZ DE RISCOS E CONTROLES

Uma vez finalizadas as etapas anteriores, os documentos elaborados (Fluxograma e Matriz de Riscos e Controles) devem ser revisados e validados por

cada departamento envolvido, confirmando desta forma a maneira como as atividades e controles são desempenhados. Neste momento cada departamento é responsável por identificar quaisquer possíveis equívocos ocorridos nas fases anteriores, que devem ser discutidos com o profissional de controles internos e corrigidos. A validação deve ser formalizada por meio da assinatura do gestor do departamento na matriz de riscos e controles e no fluxograma. Esta etapa possui grande importância para a consistência da avaliação dos controles, bem como para que todos os departamentos tenham pleno entendimento de como deverão realizar sua autoavaliação e dos itens que serão avaliados, das documentações envolvidas, dos procedimentos de teste, entre outras informações relevantes.

4.8. AVALIAÇÃO DOS CONTROLES INTERNOS

Uma vez que o mapeamento dos processos, a identificação e classificação dos riscos e controles e a determinação dos procedimentos de teste estejam preparados e validados, torna-se possível iniciar a etapa de avaliação. Esta se divide em três momentos. No primeiro, o Departamento de Controles Internos deve definir as amostras para teste, se necessário por meio de “bases” solicitadas aos departamentos envolvidos. No segundo, cada departamento deve realizar uma autoavaliação de seus processos, com base na Matriz de Riscos e Controles. Já no terceiro, a autoavaliação de cada departamento será revisada e validada pelo Departamento de Controles Internos. Os momentos seguem descritos abaixo.

4.8.1. Definição das amostras de teste

O profissional de controles internos é responsável pela definição das amostras para execução dos testes, ou seja, quais documentos - e de quais períodos - devem ser utilizados como evidência. A seleção deve ser feita de maneira aleatória ou com base em premissas criadas pelo profissional de controles internos. Caso seja necessário, este solicitará uma “base” para selecionar a amostra, ou seja, a relação de cem por cento de determinadas ocorrências dentro de um período. As “bases” deverão ser solicitadas ao gestor do departamento envolvido e deverão ser encaminhadas dentro do prazo ao profissional de controles internos.

O não atendimento do prazo em até 01 semana deverá acarretar na penalização da avaliação final do departamento em 50% do valor do controle em questão. Caso o prazo de entrega seja ultrapassado em mais de 01 semana, a penalização deverá ser de 100%.

A penalização pelo não cumprimento ao prazo definido busca estimular engajamento dos gestores de cada departamento. Isso porque o não atendimento dos prazos pode comprometer de maneira significativa a avaliação dos controles internos, etapa em que costuma-se ter o um grande volume de atividades no mesmo período de tempo.

Após receber as "bases" de teste, o profissional de controles internos deverá definir as amostras, ou seja, quais itens especificamente devem ser avaliados. Sendo assim, o mesmo deve informar por e-mail a cada gestor dos departamentos envolvidos quais itens compõem a amostra de teste. Neste mesmo momento, a matriz de riscos e controles - com os blocos de um a três já preenchidos - deve ser encaminhada a cada gestor de departamento, com os controles sob sua responsabilidade de teste. Adicionalmente, um modelo padrão de formulário de teste deve ser encaminhado aos gestores, que deverá ser utilizado como base para a descrição detalhada dos testes. Neste devem constar todos os itens da amostra de teste. O formulário padrão deve ser desenvolvido de forma que seja possível identificar, através dos procedimentos de autoavaliação de cada departamento, quais requisitos do procedimento de teste foram atendidos e quais não foram.

Vale ainda mencionar que o profissional de controles internos deverá informar aos departamentos qual é o prazo para entrega da autoavaliação.

4.8.2. Autoavaliação de cada departamento

Ao receber a relação da amostra de documentos que deve ser testada e os modelos padrão de formulário de teste, cada departamento envolvido deve realizar sua autoavaliação. Para isso, os procedimentos de teste descritos na matriz de riscos e controles devem ser seguidos.

No formulário de testes, todas as evidências avaliadas pelo departamento devem estar listadas. Ao mesmo tempo, todos os requisitos do procedimento de teste devem estar descritos. Dessa forma, ao realizar o teste, o departamento deve

apontar quais itens do procedimento de testes foram atendidos para cada evidência analisada.

Sempre que uma inefetividade for identificada, ela deve ser descrita no formulário de teste. Após verificar todas as amostras em relação a todos os requisitos dos procedimentos de teste, o profissional responsável pela execução do teste de controle deverá concluir por um resultado: "efetivo" ou "inefetivo".

Concluída a autoavaliação, cada departamento deverá enviar ao departamento de controles internos todas as evidências utilizadas, juntamente com a matriz de riscos e controles com os campos de autoavaliação preenchidos e os formulários de teste. É fundamental que o reporte seja realizado dentro do prazo estipulado pelo departamento de controles internos.

O não atendimento do prazo em até 01 semana deverá acarretar na penalização da avaliação final do departamento em 50% do valor do controle em questão. Caso o prazo de entrega seja ultrapassado em mais de 01 semana, a penalização deverá ser de 100%.

4.8.3. Avaliação pelo departamento de controles internos

Uma vez recebida a autoavaliação realizada por cada departamento, o profissional de controles internos deverá realizar sua avaliação quanto à efetividade dos controles internos. Para isso, todas as evidências recebidas deverão ser verificadas, bem como as descrições dos testes realizados, envolvendo a matriz de riscos e controles e os formulários de teste.

Feita sua avaliação, o profissional de controles internos deverá descrever na matriz de riscos e controles quais procedimentos realizou, bem como inefetividade - caso haja - e sua conclusão a cerca do controle, ou seja, se ele é "efetivo" ou inefetivo".

Caso seja identificado durante a revisão pelo Departamento de Controles Internos que a autoavaliação de um departamento foi realizada de maneira incorreta, de forma a beneficiar a própria avaliação do departamento (por exemplo, atribuindo o resultado de “efetivo” para um controle que na realidade é “inefetivo”), a pontuação deste departamento será deduzida em duas vezes o valor do controle com resultado incorreto. Neste caso, ainda poderá ser realizada uma análise aprofundada da situação e, sendo caracterizada tentativa de fraude nos resultados da autoavaliação,

uma penalização ao responsável pela sua execução deverá ser aplicada, partindo de uma advertência formal até a dispensa do funcionário. Adicionalmente, a pontuação do departamento será deduzida a zero. A definição das punições fica a cargo da diretoria da empresa, devendo ser aprovada pelo presidente.

4.9. PLANOS DE REMEDIAÇÃO

Após a avaliação realizada pelo Departamento de Controles Internos, deve-se iniciar a etapa de elaboração dos planos de remediação, que envolve todos os controles classificados como “Inefetivo”, dividida em duas fases:

4.9.1. Classificação das inefetividades

As inefetividades identificadas deverão ser classificadas conforme sua "probabilidade de ocorrência" e seu "grau de impacto", conforme as definições abaixo.

Probabilidade de ocorrência: classificação conforme a quantidade de vezes que se acredita ser possível que um risco venha a se materializar. A probabilidade de ocorrência pode ser Alta, Média ou Baixa. Quando possível, deve-se utilizar o histórico de incidência de problemas gerados em razão da ausência ou da inefetividade do controle.

Grau de Impacto: Refere-se à magnitude que a materialização do risco está atrelada, ou seja, a dimensão dos problemas que podem ocorrer. Para isso devem ser levados em conta não apenas fatores financeiros, mas também outros impactos negativos, como na imagem da empresa, na satisfação dos funcionários, na confiabilidade das demonstrações financeiras, entre outras possibilidades. O grau de impacto pode ser classificado como: “Alto”, “Médio” ou “Baixo”.

Através da classificação acima, pode ser identificado o grau de "criticidade" da inefetividade, conforme a matriz a seguir:

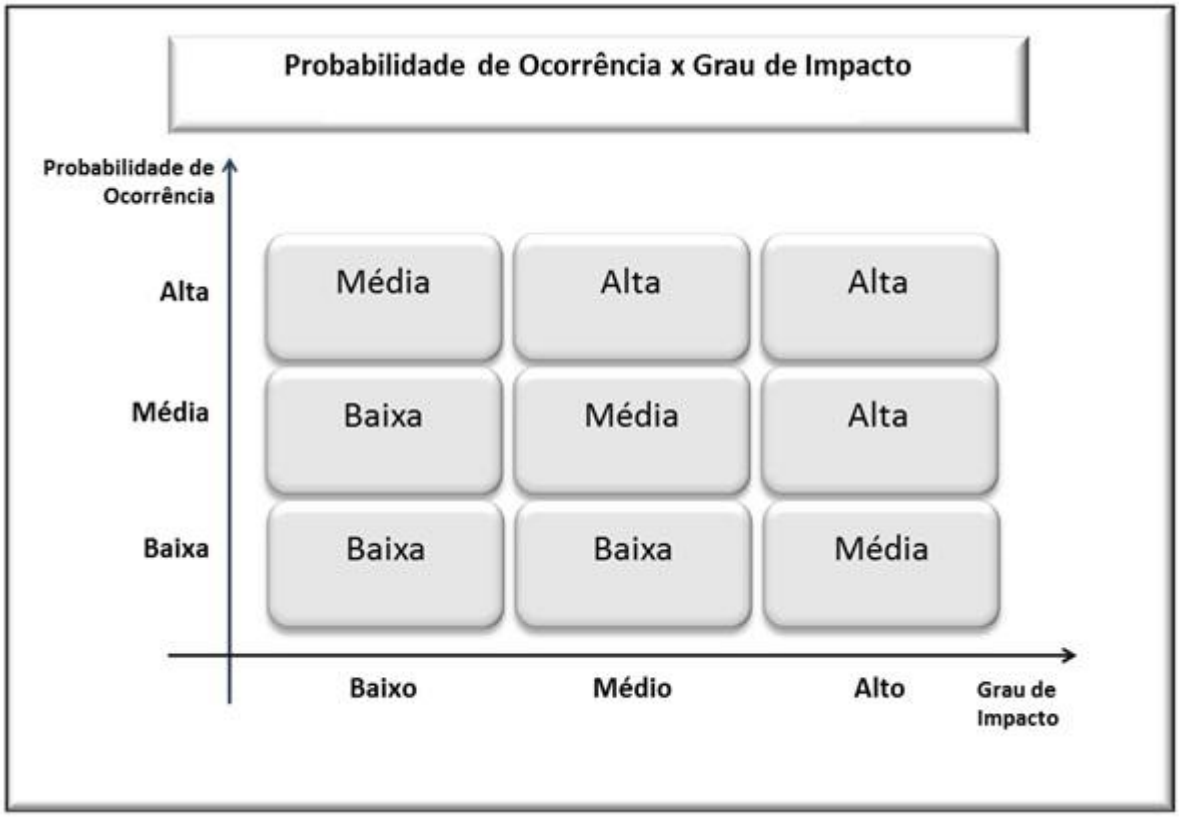

FIGURA 4 – MATRIZ DE CRITICIDADE DAS INEFETIVIDADES

Dessa forma, pode-se perceber que quanto maior forem a probabilidade de ocorrência e o grau de impacto, maior será a criticidade da inefetividade. Esta classificação deve ser utilizada como base para a priorização da implementação dos planos de remediação, de forma que os itens mais críticos sejam tratados com maior urgência.

4.9.2. Definição dos planos de remediação

Após a identificação e classificação das inefetividades de controle, torna-se possível a definição dos planos de remediação necessários. Dessa forma, o departamento de controles internos deve estruturar uma proposta de plano de ação, escrevendo-a na matriz de riscos e controles, bem como um prazo para implementação da mesma. Feito isso, a proposta deve ser apresentada ao gestor do departamento responsável pelo controle inefetivo, que é responsável pela sua validação.

É importante lembrar que a responsabilidade pela efetividade dos controles é do departamento que o executa, bem como a implementação dos planos de remediação.

Ao definir os planos de remediação, deve-se levar em conta o custo para implementá-lo e o benefício alcançado, ou seja, ele deve ser viável. A análise de viabilidade deve estar alinhada ao apetite ao risco da organização, conforme exposto na etapa "4.1 - Direcionamento e Estrutura de Controles Internos" desta metodologia.

A validação dos planos de remediação e o comprometimento em implementá-los devem ser formalizados por e-mail, no qual o gestor do departamento responsável os confirma. O e-mail deve ser arquivado pelo departamento de controles internos, como evidência da ciência e comprometimento do departamento responsável.

4.10. IMPLEMENTAÇÃO DOS PLANOS DE REMEDIAÇÃO

Uma vez alinhados, os planos de remediação devem ser implementados por cada departamento envolvido, de forma que no momento da reavaliação dos controles, os mesmos estejam “Efetivos”. Caso os departamentos identifiquem alguma necessidade de alteração nos planos de remediação estipulados, em decorrência de fatores não identificados anteriormente, devem entrar em contato com o Departamento de Controles Internos para discussão da melhor alternativa. Toda a alteração nos planos de remediação deve ser aprovada pelo departamento de controles internos, de forma a evitar que um plano implementado não seja o suficiente para proporcionar a efetividade do controle.

4.11. REAVALIAÇÃO DOS CONTROLES INEFETIVOS

A reavaliação dos subprocessos tem como objetivo verificar se a implementação do plano de remediação foi efetiva e, dessa forma, se os problemas identificados nos controles foram solucionados. Para isso, uma nova seleção de amostras deve ser feita pelo Departamento de Controles Internos, por meio do recebimento de “bases” dos departamentos, se necessário. Este processo deve seguir o mesmo fluxo descrito na etapa "4.8.1 - Definição das amostras de teste",

sendo finalizado com o envio da amostra de teste, da matriz de riscos e controles e dos formulários de teste aos departamentos envolvidos.

Uma vez conhecidas as amostras que devem ser utilizadas para cada teste, cada departamento deverá executar sua reavaliação, envolvendo apenas os controles que anteriormente tiveram como resultado “Inefetivo” ou “Requer Melhoria”. Adicionalmente, o departamento de controles internos pode definir a necessidade de reavaliação de outros controles, mesmo que estivessem efetivos na primeira avaliação realizada. A reavaliação deve ser desempenhada da mesma maneira descrita na etapa "4.8.2 - Autoavaliação de cada departamento". Esta etapa é finalizada com o reporte da autoavaliação de cada departamento ao departamento de controles internos.

Sendo assim, torna-se possível que o departamento de controles internos realize a revisão da autoavaliação de cada departamento, chegando desta maneira à pontuação final para o subprocesso, calculada através do valor de cada controle. Esta etapa deve seguir o mesmo fluxo descrito na etapa "4.8.3 - Avaliação pelo departamento de controles internos".

A reavaliação dos controles, descrita nesta etapa da metodologia, deve ser realizada conforme o cronograma definido pelo departamento de controles internos, e não após a implementação de cada plano de remediação individualmente. Dessa forma, torna-se possível avaliar todos os controles de uma única vez, facilitando a organização e o fluxo das atividades.

4.12. REDEFINIÇÃO DOS PLANOS DE REMEDIAÇÃO

Após a reavaliação dos controles, torna-se necessário reclassificar a criticidade das inefetividades e definir novos planos de remediação para os controles que permanecerem inefetivos. Dessa forma, o mesmo fluxo definido na etapa "4.9.1 - Definição dos planos de remediação" deve ser seguido.

4.13. CÁLCULO E REPORTE DOS RESULTADOS

Ao finalizar a reavaliação dos controles internos de cada subprocesso, o departamento de controles internos já possui conhecimento da pontuação total atingida em cada um deles. Esta é calculada através da soma do valor individual de

cada controle, na matriz de riscos e controles. Vale ressaltar que para o cálculo da pontuação do subprocesso não devem ser realizados descontos devido ao atraso do envio das documentações pelos departamentos, ou ainda devido aos erros - intencionais ou não - cometidos na autoavaliação de cada departamento. Isso porque o objetivo do cálculo da pontuação total do subprocesso é avaliar o nível de controle do mesmo, e não de cada departamento envolvido. A realização de qualquer tipo de descontos neste cálculo poderia comprometer a avaliação da alta direção quanto à efetividade dos controles do subprocesso. Dessa forma, a pontuação total atingida em um subprocesso é chamada de "pontuação do subprocesso" e difere da pontuação individual atingida por cada departamento.

Sendo assim, a pontuação individual atingida por cada departamento, chamada de "nível de efetividade do departamento", deve ser calculada pelo departamento de controles internos. Para isso, todos os controles sob responsabilidade de um departamento devem ser consolidados em uma matriz. Este processo consiste em criar novas matrizes de riscos e controles, divididas por departamento, mas não em alterar as colunas ou o conteúdo das matrizes previamente utilizadas, que estão dispostas por subprocesso.

Uma vez criadas as novas matrizes incluindo apenas os controles sob responsabilidade de um único departamento, basta realizar o cálculo da pontuação máxima que poderia ter sido atingida pelo departamento e a pontuação obtida de fato, através da efetividade dos controles. A divisão desta por aquela, deduzidos os valores de penalização por atraso de entrega e/ou erros da autoavaliação, resulta no nível de efetividade atingido pelo departamento. Para ser considerado satisfatório, este deve ser de ao menos 90%. Após realizar este método de cálculo para todos os departamentos envolvidos, os departamentos devem ser ranqueados conforme o seu nível de efetividade.

Outra análise relevante é a de quais departamentos concentram em suas operações os principais controles para a empresa, e, logo, os principais riscos. Para obter essa visibilidade, deve-se classificar os departamentos conforme a pontuação máxima que poderia ser atingida por cada um, já que a pontuação individual de cada controle foi previamente definida de forma diretamente proporcional ao seu grau de relevância no subprocesso. Por esse motivo, pode-se dizer que os departamentos que poderiam atingir uma maior pontuação total, possuem maior representatividade nas atividades de controles internos.

Uma vez calculados os indicadores descritos acima, torna-se possível realizar o reporte dos resultados, que é dividido em dois tipos. O primeiro deve ser realizado para cada departamento envolvido no processo de definição e avaliação de controles internos e o segundo para toda a alta administração da empresa, incluindo o presidente. Os fluxos seguem descritos a seguir.

4.13.1. Reporte dos resultados aos departamentos

O departamento de controles internos deve reportar a cada departamento a matriz de riscos e controles que contém apenas os controles sob responsabilidade do mesmo. Nesta deve constar o cálculo do "nível de efetividade do departamento".

O reporte deve ser realizado por e-mail ao gestor e diretor do departamento avaliado. Relatórios adicionais podem ser preparados pelo departamento de controles internos caso haja necessidade.

4.13.2. Reporte dos resultados à alta administração

Um relatório com a análise detalhada da efetividade de controles internos deve ser preparado pelo departamento de controles internos e reportado por e-mail à alta administração, incluindo o presidente. Neste deve constar o resultado das análises de todos os departamentos e subprocessos. Um sumário executivo, compreendendo um resumo dos principais resultados, de forma objetiva, deve compor o relatório.

Após o reporte dos resultados por e-mail, uma reunião deve ser agendada com toda a alta administração e o presidente, sendo apresentada pelo líder do departamento de controles internos. Nesta, todas as inefetividades relevantes devem ser expostas e discutidas, incluindo os planos de remediação definidos para as mesmas. A reunião deve ser formalizada através de ata.

4.14. APLICAÇÃO DA MERITOCRACIA

Um dos objetivos da metodologia proposta é permitir a classificação dos departamentos que mais contribuem para um ambiente adequado de controles internos, recompensando-os por isso. Essa medida visa demonstrar, na prática, a

importância dada pela alta administração às atividades de controle. Dessa forma, um KPI (*key performance indicator)* deve ser obrigatório para todos os gestores cujos processos são escopo da definição e avaliação de controles internos. Este deve compor, ao menos, 25% da avaliação individual do gestor e também da base de cálculo para o recebimento de bônus ou remuneração variável, caso a empresa adote esta política.

Esta medida tem como objetivo fazer com que os gestores deem maior importância à efetividade de seus controles internos, bem como estimular a melhoria contínua dos processos e das atividades de controle desenvolvidas. Dessa forma, busca-se equilibrar a comum priorização dada à pura execução da atividade em detrimento ao cumprimento de boas práticas de controles internos e, até mesmo, das políticas da empresa. Em outras palavras, espera-se estimular a cultura de executar atividades de maneira sustentada e não a qualquer custo, já que estas poderiam expor a empresa a riscos não aceitáveis pela alta administração.

4.15. NOVO CICLO DA METODOLOGIA

Realizado o reporte dos resultados, encerra-se o ciclo de definição e avaliação de controles internos. Dessa forma, torna-se necessário realizar atividades de preparação para o novo ciclo da metodologia, que impreterivelmente deve ser de implementação contínua.

Após a implementação do primeiro ciclo da metodologia, a execução do mapeamento dos controles internos dos subprocessos já mapeados não precisa ser realizada novamente, pois já haverá fluxogramas e matrizes de riscos e controles para os mesmos. Contudo, é fundamental realizar uma revisão de ambos os documentos, antes de iniciar a etapa de avaliação. Essa medida visa ajustar o fluxograma com as alterações nos processos que aconteceram desde sua elaboração, bem como a matriz de riscos e controles.

Também deve ser levado em consideração antes de iniciar o novo ciclo da metodologia, a avaliação do escopo definido e as possíveis necessidades de alteração. Estas podem ocorrer devido a diversos fatores internos, como os resultados da avaliação de controles internos do ciclo anterior, uma mudança na estratégia da empresa ou em suas operações, ou ainda uma reestruturação de suas atividades. Fatores externos também devem ser considerados, como a existência de

novas regulamentações aplicáveis à organização, mudanças no mercado de atuação ou da conjuntura social, política e econômica.

5. CONSIDERAÇÕES FINAIS E RECOMENDAÇÕES

Conclui-se que a definição e avaliação de controles internos em empresas de grande porte assume um papel fundamental na gestão de riscos e na otimização dos processos. Para isso, todos os departamentos que executam atividades críticas para atingir os objetivos da empresa devem estar alinhados sob uma mesma perspectiva, direcionamento e metodologia, definidos e suportados pela alta administração.

Dessa forma, a alta administração possui um papel fundamental para a efetiva gestão de riscos e controles, assim como o departamento responsável por implementar a metodologia proposta por este trabalho. Este - aqui chamado de departamento de controles internos - deve ser capaz de auxiliar a alta administração a identificar os principais riscos no nível organizacional e também operacional, relacionando-se com todos os departamentos envolvidos no projeto.

Para atingir os objetivos propostos por este trabalho, o adequado mapeamento dos processos assume um papel crítico. Neste, as ferramentas "fluxograma" e "matriz de riscos e controles" são fundamentais para que o entendimento dos processos e a identificação de riscos e controles possam ser realizados adequadamente. Além disso, este material serve como base para a gestão de processos e a avaliação da efetividade dos controles da empresa.

Além de definir como os controles devem ser executados, a avaliação da efetividade dos mesmos é de extrema importância para proporcionar maior confiabilidade na tomada de decisões, agregar valor aos processos, implementar a melhoria contínua e reduzir riscos de fraude e outras inconformidades, como nas demonstrações financeiras. Isso porque é através da avaliação dos controles que torna-se possível identificar as inefetividades e, dessa forma, definir os planos de remediação necessários. Para estas atividades, o fluxograma e a matriz de riscos e controles também são fundamentais.

Vale ainda ressaltar a importância do reporte dos resultados, tanto para cada departamento envolvido no projeto quanto para a alta administração, pois ele permite que os principais riscos sejam conhecidos pelos níveis com poder de decisão. Dessa forma, gestores passam a conhecer inefetividades até então não percebidas em seus processos, bem como a diretoria pode direcionar seus esforços e recursos para mitigar os riscos com maior nível de criticidade e relevância.

Por fim, recomenda-se como tema de trabalhos futuros, um estudo de caso envolvendo a implementação desta metodologia, com objetivo de avaliar os

principais benefícios que ela pode oferecer na prática a uma organização e ainda quais serão os maiores desafios para implementá-la.

REFERÊNCIAS BIBLIOGRÁFICAS

ASSI, Marcos. **Gestão de riscos com controles internos**. 1. ed. São Paulo: Saint Paul, 2012.

Committee of Sponsoring Organizations of the Treadway Commission (COSO). ***Internal Control — Integrated Framework***: Executive Summary. Disponível em: http://www.coso.org/IC.htm. Acessado em: 08 de março de 2015.

DE CARVALHO MATTOS, Claudio; MARIANO, Rosimar Pereira. Controle interno: uma abordagem teórica. **Contabilidade Vista & Revista**, v. 10, n. 1, p. 34-39, 2009.

DIAS, Sergio Vidal dos Santos. **Manual de controles internos: desenvolvimento e implantação, exemplos e processos organizacionais**. São Paulo: Atlas, 2010.

FRANCO, Hilário; MARRA, Ernesto. **Auditoria Contábil**. 4. ed. São Paulo: Atlas, 2001.

GIL, A. L.; ARIMA, C. H.; NAKAMURA, W. T..**Gestão: Controle Interno, Risco e Auditoria**. 1. ed. São Paulo: EDITORA SARAIVA, 2013.

INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA; LA ROCQUE, Eduarda. **Guia de orientação para o gerenciamento de riscos corporativos**. IBGC, 2007.

BERGAMINI JUNIOR, Sebastião. **Controles internos como instrumento de governança corporativa**. Revista do BNDS, Rio de Janeiro, v. 12, n. 24, p. 149-188, 2005.

OLIVEIRA, Luiz M.; PEREZ JR., José H.; SILVA, Carlos A. S. **Controladoria Estratégica**. 4. ed. São Paulo: Atlas, 2007.

PEREIRA, Antônio Nunes. Controles Internos Empresariais e Gestão: Visões e Importância - Uma Abordagem Exploratória. **Contabilidade Vista & Revista**, v. 15, n. 3, p. 27-44, 2009.

PWC - PRICEWATERHOUSECOOPERS. **Pesquisa Global Sobre Crimes Econômicos 2014 - Brasil**. Pricewaterhousecoopers, 2014.

DELOITTE - Deloitte Touche Tohmatsu. **Lei Sarbanes-Oxley: guia para melhorar a governança corporativa através de eficazes controles internos**. São Paulo: Deloitte, 2003.