



UNIVERSIDADE FEDERAL DO PARANÁ

TATHIANE RECHI VAZ

**PROPOSTA DE IMPLEMENTAÇÃO E MANUTENÇÃO DA METODOLOGIA DE
CONTROL SELF-ASSESSMENT EM UMA EMPRESA MULTINACIONAL.**

CURITIBA

2020

TATHIANE RECHI VAZ

**PROPOSTA DE IMPLEMENTAÇÃO E MANUTENÇÃO DA METODOLOGIA DE
CONTROL SELF-ASSESSMENT EM UMA EMPRESA MULTINACIONAL.**

Monografia apresentada ao Departamento de Ciências Contábeis, do Setor de Ciências Sociais Aplicadas, da Universidade Federal do Paraná, como pré-requisito para obtenção do título de Especialista em MBA – Auditoria Integral.

Orientador: Prof. Dr. Blênio Cezar Severo Peixe.

CURITIBA

2020

RESUMO

A gestão de riscos dentro das organizações é cada vez mais relevante para o sucesso e continuidade dos negócios. Assim, as empresas reforçam seus mecanismos de governança, de forma a monitorar adequadamente os riscos a que estão expostas para garantir a confiabilidade de suas informações financeiras e contábeis. Em empresas multinacionais este processo é ainda mais relevante frente a descentralização dos processos e da complexidade no mundo dos negócios em escala global. As organizações utilizam diferentes formas e métodos para gestão de seus riscos, e uma das metodologias que vem ganhando força no mercado é o *Control Self-Assessment*, foco central do presente estudo. Esta metodologia é baseada na autoavaliação dos controles internos pela área de negócio, também denominada como primeira linha de defesa. Todas as informações levantadas nesta pesquisa estão focadas para o atingimento do objetivo geral do estudo, que foi descrever uma proposta de aplicação da metodologia de *Control Self-Assessment* para o ambiente de Controles Internos em uma empresa multinacional. O presente estudo trata-se de uma pesquisa descritiva e explicativa, de natureza bibliográfica e documental e quanto à abordagem do problema é qualitativa. Neste trabalho foi realizado a consolidação das informações sobre o tema, obtidos por meio de pesquisa e da contribuição da experiência de profissionais sobre o tema.

Palavras-chave: Risco, Controle Interno, *Control Self-Assessment*; Autoavaliação, Empresa Multinacional.

ABSTRACT

Risk management by organizations is increasingly relevant to business success and continuity. Thus, there is a need for companies to strengthen their governance mechanisms, in order to adequately monitor the risks that the companies are exposed and ensure the reliability in their financial and accounting information. In multinational companies this process is even more relevant due to the decentralization of processes and complexity in the business world on a global scale. The organizations use different forms and methods to manage their risks, and one of the methodologies that has been growing is the Control Self-Assessment, focus of this study. This methodology is based on the self-assessment of internal controls by the business area, also known as the first line of defense. All the information collected in this study is focused to achieve the general objective, defined to present a proposal for the application of the Control Self-Assessment methodology in a multinational company. This study is considered a descriptive and explanatory research, with a bibliographic and documentary nature. Regarding the approach to the problem it is qualitative. In order to develop this study, the consolidation of the information was obtained through research and also the contribution of the professional experience about the topic.

Keywords: *Risk, Internal Control, Control Self-Assessment; Self-Assessment, Multinational Company.*

AGRADECIMENTOS

Agradeço a Deus, pela saúde e disposição que permitiram a realização deste trabalho.

Ao meu marido, pelo suporte incondicional e compreensão ao longo desta jornada.

Aos meus pais, pelo carinho e pelo incentivo incessante para a continuidade dos estudos.

Ao meu orientador, pela disponibilidade em me orientar com os direcionamentos necessários.

Por fim, a todos que, direta ou indiretamente, contribuíram para a conclusão do curso e realização deste estudo.

TERMO DE APROVAÇÃO

TATHIANE RECHI VAZ

PROPOSTA DE IMPLEMENTAÇÃO E MANUTENÇÃO DA METODOLOGIA DE CONTROL SELF-ASSESSMENT EM UMA EMPRESA MULTINACIONAL.

Monografia apresentada ao curso de Pós-Graduação em Auditoria Integral, Setor de Ciências Sociais Aplicadas, Universidade Federal do Paraná, como requisito parcial à obtenção do título de Especialista em Auditoria Integral.

Prof. Dr. Blênio Cezar Severo Peixe

Orientador - Departamento Ciências Contábeis, Universidade Federal do Paraná.

Prof(a). Dr(a)./Msc. _____

Departamento _____

Prof(a). Dr(a)./Msc. _____

Departamento _____

Curitiba, 30 de Junho de 2020.

LISTA DE ILUSTRAÇÕES

FIGURA 1 – MODELO DAS TRÊS LINHAS DE DEFESA	29
FIGURA 2 – PROPOSTA DE ESTRUTURA DAS LINHAS DE DEFESA.....	39
FIGURA 3 – MATRIZ DE IMPACTO E PROBABILIDADE.....	45
FIGURA 4 – ESTRUTURA MATRIZ DE RISCO E CONTROLE.....	46
FIGURA 5 – PROPOSTA DE USUÁRIOS ENVOLVIDOS NO CSA.....	49

LISTA DE QUADROS E TABELAS

QUADRO 1 – MATURIDADE DE CONTROLE INTERNO	17
QUADRO 2 – ESTUDOS ANTECEDENTES.....	34
QUADRO 3 – MATRIZ DE RISCO E CONTROLE.....	47
QUADRO 4 – SUGESTÃO DE QUESTIONÁRIO CSA.....	52
QUADRO 5 – CLASSIFICAÇÃO DE EFETIVIDADE NO CSA.....	53
QUADRO 6 – PLANO DE REMEDIAÇÃO EXEMPLIFICADO.....	55

LISTA DE ABREVIATURAS E SIGLAS

AICPA – *American Institute of Certified Public Accountants*

COSO – *Committee of Sponsoring Organizations of the Treadway Commission*

CSA – *Control Self-Assessment*

ERP – *Enterprise Resource Planning*

GRC – Governança, Riscos e Compliance

IBGC – Instituto Brasileiro de Governança Corporativa

IIA – *The Institute of Internal Auditors*

NBC – Norma Brasileira de Contabilidade

SOx – Sarbanes-Oxley

SUMÁRIO

1.	INTRODUÇÃO	12
1.1	CONTEXTO E PROBLEMA	12
1.2	OBJETIVOS	13
1.2.1	Objetivo Geral	13
1.2.2	Objetivos Específicos	14
1.3	JUSTIFICATIVAS	14
2.	REVISÃO BIBLIOGRAFICA	16
2.1	CONTROLE INTERNO	16
2.1.1	Conceito de Controle Interno	16
2.2	COMPONENTES DE CONTROLE INTERNO	18
2.2.1	Ambiente de Controle	18
2.2.2	Avaliação de risco	19
2.2.3	Atividade de controle	19
2.2.4	Informação e comunicação	20
2.2.5	Atividades de monitoramento	20
2.3	TIPOS DE ATIVIDADES DE CONTROLES	21
2.3.1	Alçadas	21
2.3.2	Autorizações	22
2.3.3	Conciliação	22
2.3.4	Revisões de desempenho	22
2.3.5	Segurança física	23
2.3.6	Segregação de funções	23
2.3.7	Sistemas informatizados	23
2.3.8	Normatização interna	24
2.4	RISCOS	24
2.4.1	Conceito de risco	24
2.5	TIPOS DE RISCO	25
2.5.1	Origem dos eventos de risco	26

2.5.2	Natureza dos riscos	26
2.5.3	Tratamento dos riscos	28
2.6	AS TRÊS LINHAS DE DEFESA	29
2.6.1	Primeira linha de defesa	30
2.6.2	Segunda linha de defesa	30
2.6.3	Terceira linha de defesa	31
2.7	CONTROL SELF-ASSESSMENT	31
2.7.1	Conceito de <i>Control Self-Assessment</i>	31
2.7.2	Origem do <i>Control Self-Assessment</i>	32
2.8	ESTUDOS ANTECEDENTES	33
3.	METODOLOGIA DA PESQUISA	35
3.1	TIPOLOGIA DA PESQUISA QUANTO AOS OBJETIVOS.....	35
3.2	TIPOLOGIA DA PESQUISA QUANTO AOS PROCEDIMENTOS	35
3.3	TIPOLOGIA DA PESQUISA QUANTO ABORDAGEM DO PROBLEMA	36
3.4	LEVANTAMENTO DE DADOS E INFORMAÇÕES	36
4.	APLICAÇÃO DA METODOLOGIA DE CONTROL SELF-ASSESSMENT	37
4.1	ESTRUTURA EMPRESARIAL	37
4.1.1	Estrutura das 3 linhas de defesa	37
4.1.2	Definição dos recursos necessários	40
4.2	IDENTIFICAÇÃO DO ESCOPO	42
4.2.1	Mapeamento de processos.....	42
4.2.2	Matriz de riscos e controles	44
4.2.3	Validação da Matriz de riscos e controles	48
4.2.4	Usuários envolvidos no <i>Control Self-Assessment</i>	48
4.2.5	Definição da frequência de realização do <i>Control Self-Assessment</i>	50
4.3	DEFINIÇÃO DO QUESTIONÁRIO DE CONTROL SELF-ASSESSMENT	51
4.4	PLANO DE REMEDIAÇÃO	53
4.4.1	Critérios para definição de um plano de remediação efetivo	54
4.5	MONITORAMENTO E REPORTE DO <i>CONTROL SELF-ASSESSMENT</i>	55
4.6	FATORES CRÍTICOS PARA IMPLEMENTAÇÃO DO <i>CONTROL SELF-ASSESSMENT</i>	56

4.7	BENEFÍCIOS DO <i>CONTROL SELF-ASSESSMENT</i>	57
5.	CONSIDERAÇÃO FINAIS	59
	REFERÊNCIAS	61

1. INTRODUÇÃO

1.1 CONTEXTO E PROBLEMA

Desde o final do século XX e início do século XXI, o mundo vem passando por mudanças graduais que deram início ao processo que hoje conhecemos pelo nome de globalização. Pode-se definir o termo “globalização” como o processo de aproximação entre as nações de todo o mundo, seja no âmbito econômico, social, cultural ou político. Assim, atribui-se à globalização o aumento da integração de mercado existente entre os países. Como consequência, o processo de globalização contribuiu também para a expansão das empresas multinacionais, pois proporcionou melhores condições de atuação dessas empresas em escala mundial.

De outro lado, a globalização também trouxe maior complexidade para o mundo dos negócios, decorrente da descentralização das atividades e do aprimoramento das tecnologias. Esta complexidade e as incertezas do mundo moderno aumentaram a exposição das empresas aos diversos riscos, ocasionando maior probabilidade de erros, falhas e até mesmo fraudes nos processos empresariais. Atrelado a este cenário, diversos escândalos financeiros foram revelados nas últimas décadas, gerando muitas incertezas e desconfianças no mundo corporativo.

Frente a estes cenários, surge então a necessidade de as empresas reforçarem seus mecanismos de governança, de forma a monitorar adequadamente os riscos a que estão expostas e garantir maior confiabilidade em suas informações e processos internos. A partir deste momento, o conceito de controle interno passa a ganhar maior visibilidade dentro das organizações, auxiliando no aperfeiçoamento de processos, monitoramento e mitigação de riscos.

O monitoramento adequado dos riscos é essencial para a continuidade das organizações, pois permite a companhia maior confiabilidade de suas informações financeiras, contribui para o atendimento às leis e regulamentos aplicáveis à organização, além de melhorar a eficácia e eficiência de suas operações. Para este monitoramento, as organizações utilizam diferentes formas e métodos para gestão de seus riscos, podendo este monitoramento ser realizado de forma quantitativa (quando o risco é

avaliado por modelos probabilísticos) ou qualitativa (quando o risco é avaliado com base em dados analíticos, como por exemplo, sua frequência e severidade).

Uma das metodologias empregadas para avaliação qualitativa de riscos é o processo de autoavaliação, também conhecido como *Control Self-Assessment* (CSA). Este método consiste em avaliar a efetividade dos controles de forma descentralizada, possibilitando a detecção de exposições indesejadas e a implementação de medidas corretivas.

A metodologia do CSA vem ganhando espaço nas organizações, mas ainda não é um tema totalmente difundido. Desta forma, o presente estudo pretende chamar a atenção do leitor para a importância do ambiente de controle interno dentro das organizações, com foco na utilização da metodologia de *Control Self-Assessment* aplicada em empresas multinacionais.

Assim, o cenário descrito acima nos leva ao problema deste trabalho acadêmico: Como a metodologia de *Control Self-Assessment* contribui para o ambiente de controles internos em uma empresa multinacional?

1.2 OBJETIVOS

O presente trabalho foi desenvolvido com base nos objetivos apresentados nesta seção.

1.2.1 Objetivo Geral

Descrever uma proposta de aplicação da metodologia de *Control Self-Assessment* para o ambiente de Controles Internos em uma empresa multinacional.

1.2.2 Objetivos Especificos

- (a) Apresentar as etapas de implementação da metodologia de *Control Self-Assessment* para o ambiente de Controles Internos em uma empresa multinacional.
- (b) Apresentar as etapas de manutenção da metodologia de *Control Self-Assessment* para o ambiente de Controles Internos em uma empresa multinacional.
- (c) Demonstrar as diferenças de papéis e responsabilidades das três linhas de defesa dentro da empresa para a aplicação da metodologia de *Control Self-Assessment*.
- (d) Apresentar a contribuição do *Control Self-Assessment* para conscientização e valorização da cultura de controles internos dentro da empresa.

1.3 JUSTIFICATIVAS

Diante da complexidade dos processos empresariais e da alta quantidade de riscos que as empresas estão expostas, muitas empresas veem a necessidade de implementar ritos de governança que possam ajudar na mitigação de riscos, garantindo maior transparência e responsabilidade por parte dos executivos. Uma das metodologias de controles internos que vem ganhando espaço nas organizações é a metodologia do *Control Self-Assessment*, a qual permite maior envolvimento da primeira linha de defesa na avaliação e mitigação de riscos dentro da organização.

Um dos aspectos importantes dessa metodologia é que ela não se limita apenas a empresas de grande porte ou multinacionais, mas sim a todas as companhias que buscam um meio de monitoramento do seu ambiente de controle interno. Assim, as descobertas desta pesquisa acadêmica poderão ser utilizadas pela sociedade, principalmente por organizações que buscam entender a metodologia *de Control Self-Assessment*, bem como suas contribuições para o mundo empresarial.

O presente trabalho poderá contribuir também com ações práticas que poderão apoiar os profissionais da área na aplicação ou aprimoramento da metodologia. Portanto,

o presente estudo tem a pretensão de contribuir para a área de controles internos e aos profissionais que atuam nesta área com um trabalho para reflexão sobre o tema de *Control Self-Assessment*.

A implementação deste estudo se justifica também devido à falta de vasta literatura sobre o tema. Desta forma, o trabalho poderá auxiliar no desenvolvimento do tema, contribuindo para o ambiente acadêmico com o entendimento de como a metodologia *Control Self-Assessment* auxilia na mitigação de riscos, bem como na conscientização e valorização da cultura de controles internos. Esta contribuição possibilitará a utilização do estudo para futuros trabalhos ou publicações que venham a ser realizados sobre o tema.

2. REVISÃO BIBLIOGRAFICA

A revisão bibliográfica do presente trabalho visa contribuir com informações importantes para o seu desenvolvimento, englobando conceitos elaborados por autoridades nos assuntos abordados e verificados em bibliografias do tema em questão.

O primeiro tópico abordado nesta seção será o conceito de ambiente de controle interno, permitindo melhor contextualização do tema. Na sequência serão abordados temas complementares, como princípios de controle interno, conceito e tipos de riscos. Ainda, será contextualizada o conceito das três linhas de defesas em uma organização e a contextualização do conceito da metodologia de *Control Self-Assessment*. Por fim, estudos antecedentes sobre os temas abordados no presente projeto serão referenciados como forma de complemento dos conceitos aqui apresentados.

2.1 CONTROLE INTERNO

Nesta seção serão mencionados alguns conceitos e definições sobre Controle Interno que são fundamentais para referência teórica do presente estudo.

2.1.1 Conceito de Controle Interno

O conceito de controle interno pode ser interpretado como o conjunto de procedimentos, métodos ou rotinas que ajudam na proteção dos ativos e colaboram na geração de dados contábeis confiáveis, auxiliando a administração na condução ordenada dos negócios da empresa. O controle interno não abrange apenas os aspectos contábeis e financeiros, mas também os operacionais dentro da organização. (ATTIE, 1998).

Segundo o COSO (2013), o conceito de controle interno é definido da seguinte forma:

Processo conduzido pela estrutura de governança, administração e outros profissionais da entidade e desenvolvido para proporcionar segurança razoável com respeito à realização dos objetivos relacionados a operações, divulgação e conformidade. (COSO, 2013, p. 4).

Para o *American Institute of Certified Public Accountants* (AICPA), também conhecido como Comitê de Procedimentos de Auditoria do Instituto Americano de Contadores Públicos Certificados, o tema “controle interno” é entendido como “plano de organização e todos os métodos e medidas adotadas na empresa para salvaguardar seus ativos, verificar a exatidão e fidelidade dos dados contábeis, desenvolver a eficiência nas operações e estimular o seguimento das políticas executivas prescritas”.

Em virtude de sua abrangência, controle interno é classificado em três categorias, segundo a Norma Brasileira de Contabilidade (NBC) T 16.8: Operacional, Contábil e Normativo. De acordo com esta norma, enquanto o controle operacional está relacionado às ações que propiciam o alcance dos objetivos da entidade, o controle contábil relaciona-se com a veracidade e a fidedignidade dos registros e das demonstrações contábeis. Por fim, o controle normativo refere-se à observância da regulamentação pertinente.

Desta forma, observa-se que o controle interno assume uma função chave na empresa, tendo em vista que as empresas que possuem controles bem definidos tendem a ter menor erros na aplicação das práticas contábeis, maior eficiência operacional e diminuem o risco de práticas ilegais ou fraudulentas.

Para a adequada implementação ou melhoria do ambiente de controle interno, Assi (2012) reforça a necessidade de uma avaliação honesta do nível de maturidade de controle interno que a empresa se encontra, que pode ser dividido nos níveis abaixo:

QUADRO 1 – MATURIDADE DO CONTROLE INTERNO

Nível	Maturidade	Característica
1	Não confiável	Atividades de controle não são mapeadas.
2	Informal	Controles dependem principalmente das pessoas.
3	Padronizado	Atividades de controle são mapeadas e implementadas.
4	Monitorado	Controles padronizados e com testes periódicos
5	Otimizado	Automação e ferramentas apoiam controles internos.

FONTE: ASSI (2012)

Para que os controles internos implantados em uma empresa cumpram com a sua função e tragam ganhos para a empresa, se faz necessário que haja um ambiente de controle favorável, ou seja, deve-se implantar um sistema de controles internos, onde,

observado as rotinas de trabalho e formalizado estes procedimentos, todos os profissionais devem estar cientes dos processos que envolvem a sua rotina de trabalho para poder colocá-los em prática.

A implantação e aprimoramento de um sistema de controle é uma atividade complexa, que requer a atenção de algumas diretrizes básicas (Oliveira, Perez e Silva):

- a) **Primeira:** Cada empresa deverá desenvolver seu próprio sistema de controles.
- b) **Segunda:** Por melhor que seja, nenhum sistema de controles poderá compensar ou neutralizar as incompetências dos executivos da empresa.
- c) **Terceira:** Complexidade dos sistemas de controles internos não representa garantia de eficácia e eficiência.
- d) **Quarta:** Devem ser fixados prazos realistas e exequíveis no processo de implantação do sistema de controles.
- e) **Quinta:** É decisiva a participação das pessoas na implantação ou aprimoramento dos controles internos e na futura manutenção e operacionalização sistêmica.
- f) **Sexta:** Sistemas complexos e impraticáveis são inúteis.
- g) **Sétima:** No processo de implantação ou reformulação devem ser consideradas também as perspectivas futuras da empresa. (OLIVEIRA, PEREZ e SILVA, 2009, p. 78).

Tendo isto em vista, percebe-se que o levantamento dos fluxos de controles deve ser eficaz para cumprir a sua função, e se este estiver correto no que se propõe, a empresa terá ganho de eficiência e confiabilidade em suas informações.

2.2 COMPONENTES DE CONTROLE INTERNO

Nesta seção serão mencionados os componentes que devem ser observados para a manutenção adequada do ambiente de Controle Interno dentro de uma organização.

2.2.1 Ambiente de Controle

Conforme definido na metodologia de controle interno do COSO (2013), o componente “ambiente de controle” representa as normas, processos e estruturas que fornecem a base para a condução do controle interno por toda a entidade. A estrutura de governança e a alta administração devem estabelecer as diretrizes, políticas e normas de conduta esperadas por todos. Este componente abrange também a integridade e os

valores éticos da organização, os parâmetros que permitem à empresa cumprir com suas responsabilidades de supervisão, o processo de atrair e reter talentos bem como as medidas e incentivos de recompensas por performance. (COSO, 2013).

Para Dias (2010), o ambiente de controle interno é considerado a consciência de controle da entidade e sua cultura de controle. Assim, para o autor, o ambiente de controle interno é efetivo quando as pessoas da entidade conhecem suas responsabilidades e possuem a competência e comprometimento de fazerem suas atividades da forma correta.

2.2.2 Avaliação de risco

A metodologia do COSO define risco como a possibilidade de que um evento ocorra e afete de forma adversa a realização dos objetivos da organização. O processo de avaliação de riscos envolve um processo dinâmico para identificar os riscos à realização dos objetivos da empresa e a maneira como os riscos serão gerenciados. Assim, para que exista uma avaliação de riscos, se faz necessário o estabelecimento de objetivos ligados aos diferentes níveis da entidade. A administração deve especificar os objetivos dentro das categorias operacional, divulgação e conformidade, com clareza para identificar e analisar os riscos vinculados a estes objetivos. A avaliação de riscos requer ainda que a empresa considere o impacto de possíveis mudanças no ambiente externo e interno que possam tornar o controle interno não efetivo. (COSO, 2013).

Dias (2010) ressalta que as principais funções de controle interno estão relacionadas ao atingimento dos objetivos da entidade, e uma vez que estes objetivos estão estabelecidos, a organização deve identificar os riscos que ameacem o seu cumprimento e tomar as ações necessárias para o gerenciamento dos riscos identificados.

2.2.3 Atividade de controle

Para Dias (2010), as atividades de controle são aquelas que quando executadas de forma correta e tempestiva, permitem a redução ou administração dos riscos.

As atividades de controle representam as ações estabelecidas por meio de políticas e procedimentos que garantem o cumprimento das diretrizes definidas pela administração para mitigar os riscos à realização dos objetivos. Estas atividades de controle são desempenhadas por todos os níveis da entidade, dentro de vários processos e podem ocorrer de forma manual ou no ambiente tecnológico. Os controles podem ter natureza preventiva ou de detecção, podem ser classificados como manuais ou automáticas, ou ainda ser classificados como controles de autorizações, aprovações, verificações, reconciliações e revisões de desempenho do negócio (COSO, 2013).

2.2.4 Informação e comunicação

Para Dias (2010), a comunicação é fundamental para o bom funcionamento dos controles, devendo ser transmitida para toda a entidade as informações sobre planos, ambiente de controles, riscos, atividades de controle e desempenho.

De acordo com o COSO, a informação é necessária para que a organização cumpra as responsabilidades de controle interno com a finalidade de realizar os seus objetivos. Ou seja, a administração utiliza informações importantes a fim de apoiar o funcionamento de outros componentes do controle interno. Já a comunicação deve ser um processo contínuo pelo qual as informações são transmitidas para a organização, fluindo em todas as direções da entidade. Uma comunicação efetiva permite que os funcionários recebam a mensagem da alta administração de forma clara, entendendo as responsabilidades pelo controle. (COSO, 2013).

2.2.5 Atividades de monitoramento

O componente de monitoramento utiliza avaliações contínuas para se certificar da presença e do funcionamento dos demais componentes de controle interno, inclusive a eficácia dos controles. As avaliações contínuas, inseridas nos processos corporativos nos diferentes níveis da entidade, proporcionam informações oportunas. Já as avaliações independentes, conduzidas periodicamente, possuem escopos e frequências diferentes, dependendo da avaliação de riscos, da eficácia das avaliações contínuas e de outras

considerações da administração. Os resultados devem ser avaliados e as deficiências identificadas devem ser comunicadas dentro da estrutura de governança. (COSO, 2013).

Para Dias (2010), o monitoramento é a avaliação dos controles internos ao longo do tempo, sendo que o monitoramento contínuo é o melhor indicador para saber se os controles internos estão sendo efetivos ou não.

2.3 TIPOS DE ATIVIDADES DE CONTROLES

Após o entendimento do conceito de Controle Interno e de seus componentes, esta seção visa o detalhamento dos principais tipos de atividades de controles e sua aplicabilidade prática. Os controles podem ser divididos em categorias distintas, conforme a sua forma de execução. Assim, as atividades de controle são divididas em controles de alçadas, autorizações, conciliação, revisão de desempenho, salvaguarda de ativos, segregação de funções, controles sistêmicos e normatização interna.

2.3.1 Alçadas

Segundo Simmons (1997), os controles de alçadas são importantes, pois definem limites a um funcionário quanto à possibilidade de este aprovar valores ou assumir posições em nome da instituição. Como exemplo pode-se citar o estabelecimento de teto máximo assumido por cada nível hierárquico para realização de uma atividade.

Dias (2010) reafirma que as alçadas são os limites determinados a uma função quanto à possibilidade de este aprovar valores ou assumir posições em nome da organização. Dias (2010) exemplifica este tipo de controle como o estabelecimento de valor máximo para um caixa pagar um cheque, ou a alçada definida para o Comitê de Crédito de uma empresa.

2.3.2 Autorizações

Para Simmons (1997), os controles de autorizações são definidos por atividades e transações que necessitam de aprovação de um supervisor de forma prévia a sua efetivação.

Dias (2010) ressalta ainda que a aprovação de um supervisor implica que ele verificou e validou a atividade ou a transação e assegurou que a mesma está em conformidade com as políticas e procedimentos definidos pela organização. Para isso, os responsáveis pela autorização devem verificar a documentação suporte, questionar itens não usuais e assegurar que todos os processos foram verificados.

2.3.3 Conciliação

Tanto Simmons (1997) quanto Dias (2010) afirmam que o controle de conciliação consiste no confronto da mesma informação com dados vindos de bases diferentes, adotando as ações corretivas, quando necessário.

2.3.4 Revisões de desempenho

Segundo Simmons (1997), o controle de revisão ou avaliação de desempenho refere-se ao acompanhamento de uma atividade ou processo para avaliação de desempenho em relação aos objetivos traçados, de forma a antecipar mudanças que possam impactar negativamente a entidade.

Dias (2010) aponta alguns exemplos deste tipo de controle, tais como: monitoramento de valores realizados e orçados, com o intuito de monitorar desvios, monitoramento e questionamento de flutuações relevantes nos resultados, monitoramento de transações não usuais e até mesmo acompanhamento da concorrência, visando o lançamento de novos produtos.

2.3.5 Segurança física

Os controles de salvaguarda física têm seu destaque na definição do autor Simmons (1997), que afirma que os valores de uma entidade devem ser protegidos contra uso, compra ou venda não autorizados. Dias (2010) complementa afirmando que um dos melhores controles para proteção dos ativos é a segurança física, que pode compreender controles de acessos, controle de entrada e saída de funcionários e materiais, senhas para arquivos eletrônicos importantes, criptografia, entre outros. Outro controle muito comum citado por Dias (2010) é o controle de inventário, que consiste na conferência e contagem física dos bens.

2.3.6 Segregação de funções

Simmons (1997) expõe que os controles de segregação de funções reduzem o risco de erros humanos para ações indesejadas e reduzir o risco de omissão de erros ou fraudes.

Para Dias (2010), a segregação de funções é essencial para a efetividade dos controles internos, e destaca como segregações fundamentais entre os funcionários os seguintes processos: a contabilização e a conciliação dos números; a informação e a autorização da informação; a contratação e o seu pagamento; administração dos recursos e a sua fiscalização.

2.3.7 Sistemas informatizados

Simmons (1997) afirma que os sistemas informatizados têm a finalidade de garantir a integridade e veracidade dos dados e transações, bem como a interface de dados entre os sistemas.

Em complemento as definições trazidas por Simmons para o tema de sistemas informatizados, outras categorias de controles também são apresentadas por Assi (2012) como os controles de configurações, relatório de exceção, revisão da administração, e acesso restrito.

Para Assi (2012), os controles de configuração consideram parametrizações desenvolvidas para proteger os dados contra processamentos inapropriados, para ajudar na manutenção da integridade dos dados. Como exemplo pode-se citar o bloqueio sistêmico para contabilização de um evento em duplicidade.

Para o mesmo autor, enquanto os controles de relatórios de exceção são utilizados para monitorar algum item que se mostre como exceção em uma base de dados, os controles de revisão da administração consistem na revisão independente com o intuito de supervisão das atividades executadas.

Por fim, os controles de acesso ao sistema se baseiam na liberação do acesso apenas conforme necessidade, conforme direitos de acesso configurados.

2.3.8 Normatização interna

Para Dias (2010), a normatização interna é a definição formal das regras necessárias para o funcionamento da organização, por meio de normas e políticas. Para isso, o mesmo autor destaca que as normas devem ser de fácil acesso aos funcionários, devem definir claramente as responsabilidades, as políticas corporativas correlatas, os fluxos operacionais, as funções e procedimentos aplicáveis.

2.4 RISCOS

O principal objetivo para implementação de um ambiente de Controle Interno em uma organização é a adequada mitigação de riscos desta empresa. Desta forma, nesta seção, serão abordados temas relacionados ao tema “risco”, como seu conceito e os principais riscos enfrentados pelas organizações.

2.4.1 Conceito de risco

O Instituto Brasileiro de Governança Corporativa (IBGC) traz em sua cartilha “Guia de Orientação para Gerenciamento de Riscos Corporativos”, publicada em 2007, a definição do conceito de risco, conforme a seguir:

O termo risco é proveniente da palavra *risicu* ou *riscu*, em latim, que significa ousar (*to dare*, em inglês). Costuma-se entender “risco” como possibilidade de “algo não dar certo”, mas seu conceito atual envolve a quantificação e qualificação da incerteza, tanto no que diz respeito às “perdas” como aos “ganhos”, com relação ao rumo dos acontecimentos planejados, seja por indivíduos, seja por organizações. (IBGC, 2007, p.11).

O conceito de risco é definido por Assi (2012, p.20) como “uma ou mais condições de variáveis com potencial necessário de causar dano ao patrimônio da empresa, tangível ou intangível”. Ainda de acordo este autor, “muitos riscos são inerentes ao negócio, e cabe ao profissional de gestão de risco a seleção de quais riscos a empresa deve tratar.” Portanto, o risco estará sempre presente na organização, podendo variar em nível de perigo e nas medidas preventivas a serem tomadas.

A definição de risco também é trazida por Padovese (2005), como sendo “eventos incertos, que podem influenciar o alcance dos objetivos estratégicos, operacionais e financeiros da organização”.

Em finanças, o conceito de risco é definido por Gil, Arima e Nakamura (2013, p. 132) como a possibilidade de ocorrência de uma perda. Para estes autores, a questão fundamental do ponto de vista do tratamento do risco é entender como mensurá-lo, controlá-lo e gerenciá-lo.

A definição de risco também é descrita por Dias (2010, p.30), como “a probabilidade de perda ou incerteza associada ao cumprimento de um objetivo”. Desta forma, uma vez que a organização estabelece os seus objetivos, este mesmo autor define que esta deve identificar os riscos que ameacem o cumprimento dos objetivos e tomar as ações necessárias para o gerenciamento dos riscos identificados.

2.5 TIPOS DE RISCO

Nesta seção serão abordados os diferentes tipos de categorização dos riscos que uma organização pode ser exposta.

2.5.1 Origem dos eventos de risco

A origem dos eventos de riscos pode ser interna ou externa e determinam a forma de atuação da entidade. Os riscos internos são definidos pelo IBGC (2007) como:

Eventos originados na própria estrutura da organização, pelos seus processos, seu quadro de pessoal ou de seu ambiente de tecnologia. A organização pode e deve, em geral, interagir diretamente com uma ação proativa. (IBGC, 2007, p. 18)

Os riscos externos são definidos pelo IBGC (2007) como:

Ocorrências associadas ao ambiente macroeconômico, político, social, natural ou setorial em que a organização opera. Exemplos: nível de expansão do crédito, grau de liquidez do mercado, nível das taxas de juros, tecnologias emergentes, ações da concorrência, mudança no cenário político, conflitos sociais, aquecimento global, catástrofes ambientais, atos terroristas, problemas de saúde pública, etc. A organização, em geral, não consegue intervir diretamente sobre estes eventos e terá, portanto, uma ação predominantemente reativa. Isto não significa que os riscos externos não possam ser “gerenciados”; pelo contrário, é fundamental que a organização esteja bem preparada para essa ação reativa. (IBGC, 2007, p. 18)

De acordo com o IBGC (2007), é importante determinar a origem dos eventos de risco, pois auxilia na definição da abordagem a ser empregada pela organização.

2.5.2 Natureza dos riscos

O IBGC (2007) classifica os riscos em três naturezas distintas, sendo elas estratégica, operacional ou financeira. Entretanto, o Instituto reforça que os riscos podem pertencer a categorias distintas e em alguns casos podem se encaixar em duas ou até mesmo em todas as categorias concomitantemente.

De acordo com o IBGC (2007), os riscos estratégicos estão relacionados à tomada de decisão da alta administração e podem gerar perda substancial no valor econômico da organização. Como exemplos desta categoria, o IBGC (2007) comenta falhas na reação ao movimento dos concorrentes causadas por fusões e aquisições e diminuição de demanda do mercado por produtos e serviços da empresa causada por obsolescência.

Os riscos operacionais são definidos pelo IBGC (2007) como aqueles associados à possibilidade de perdas (de produção, ativos, clientes, receitas), resultantes de falhas ou deficiências de processos internos, de pessoas ou sistemas. Também podem ser considerados eventos externos como catástrofes naturais, fraudes, greves e atos terroristas. Os riscos operacionais geralmente acarretam redução, degradação ou interrupção (total ou parcial) das atividades, com impacto negativo na reputação da sociedade, podendo gerar ainda passivos contratuais, regulatórios e ambientais.

Por fim, o IBGC (2007) define os riscos financeiros como aqueles que geram a exposição das operações financeiras da organização. Este tipo de risco engloba a administração de fluxo de caixa, a administração financeira, a exposição cambial, taxa de juros, entre outros. O IBGC (2007) ressalta ainda que é comum que se destaque esta categoria o risco associado à confiabilidade das informações transmitidas nos relatórios financeiros divulgados pelas organizações.

Alguns autores realizam a classificação de natureza dos riscos de maneira diferente da apresentada pelo IBGC. Os autores Gil, Arima e Nakamura (2013), por exemplo, reconhecem a existência de diferentes tipos de riscos, salientando que os principais tipos de riscos de uma organização referem-se a risco de mercado, risco de crédito, risco operacional, risco cambial, risco sistemático, risco diversificável.

Para Assis (2012), as principais categorias de riscos às quais as organizações estão sujeitas compreendem risco operacional, risco legal, risco contratual, risco de conformidade, risco político, risco de liquidez, risco de taxa, risco de mercado, risco de terceirização, risco contábil, risco de controle, risco tributário, risco de crédito, risco de demanda, risco de reputação e risco de continuidade. Para este mesmo autor, o risco operacional está dividido em subáreas de riscos, definidos como risco de *overload*, risco de obsolescência, risco de equipamentos, risco de erro não intencional, risco de fraude, risco de qualificação, riscos de produtos e serviços, risco de regulamentação, risco de liquidação financeira, risco sistêmico, risco de imagem e risco de catástrofe.

2.5.3 Tratamento dos riscos

De acordo com o IBGC (2007), os riscos podem ser reduzidos por meio de prevenção ou de remediação. Enquanto a prevenção representa a diminuição da probabilidade de ocorrência ou diminuição do impacto financeiro esperado caso o evento ocorra, a remediação representa o controle dos danos após a ocorrência do evento. Ainda de acordo com o IBGC (2007), na prática, a eliminação total dos riscos é impossível, e por este motivo, é recomendável alinhar a estrutura de controles internos aos objetivos e ao nível de exposição desejado pela organização. Desta forma, depois de identificados, avaliados e mensurados, a organização deve definir qual o tratamento que será dado aos seus riscos.

O IBGC (2007) lista as várias alternativas para tratamento dos riscos, conforme descritas abaixo:

Evitar o Risco: decisão de não se envolver ou se retirar de uma situação de risco.
Reter o risco: decisão de manter o risco no nível atual de impacto e probabilidade.
Reduzir o risco: decisão de tomada de ações para minimizar a probabilidade e/ou o impacto do risco.
Transferir e/ou Compartilhar: decisão de reduzir o impacto e/ou a probabilidade de ocorrência do risco através da transferência ou compartilhamento de uma parte do risco com terceiros.
Explorar: decisão de aumentar o grau de exposição ao risco na medida em que isto possibilita vantagens competitivas.

Desta forma, o IBGC (2007) afirma que a organização terá uma resposta específica para cada evento significativo e recomenda que após a decisão do tratamento do risco, a organização avalie e monitore os impactos da ocorrência dos eventos, considerando o risco inerente e risco residual de cada processo.

De acordo com o IBGC (2007) o risco inerente representa o “risco natural ou ausência de qualquer ação que a direção possa realizar para alterar a probabilidade de ocorrência ou de impacto”. O risco residual é definido pelo mesmo Instituto como “resultante do processo de tomada de ações e aplicação das melhores práticas de controles internos ou da resposta da organização ao risco”.

2.6 AS TRÊS LINHAS DE DEFESA

O modelo das três linhas de defesa é apresentado pelo Instituto Internacional de Auditoria, o IIA – *The Institute of Internal Auditors*, como uma das melhores práticas para ajudar as organizações na delegação e coordenação das atividades essenciais de gerenciamento de riscos. Este modelo representa uma forma de melhorar a comunicação no processo de gerenciamento de risco por meio do esclarecimento dos papéis e responsabilidades dentro da organização.

O IIA defende que as três linhas de defesa deveriam existir, de alguma forma, em todas as organizações, não importando tamanho ou complexidade da organização, pois o gerenciamento de riscos normalmente é mais sólido quando há as três linhas de defesa separadas e claramente identificadas.

A seguir está apresentada a representação gráfica definida pelo IIA quanto a estrutura das três linhas de defesa:

FIGURA 1 – MODELO DAS TRÊS LINHAS DE DEFESA



FONTE: IIA (2013).

O modelo apresentado pelo IIA indica que existem três grupos (ou linhas) envolvidos no gerenciamento eficaz de riscos: primeira linha: funções que gerenciam e têm propriedade sobre riscos; segunda linha: funções que supervisionam riscos; terceira linha: funções que fornecem avaliações independentes.

A principal contribuição do modelo das três linhas de defesa é trazer a consciência das diferentes funções para os diferentes agentes dentro da organização, de forma que não haja lacunas nem duplicação de atividades. Ou seja, responsabilidades claras devem ser definidas para que cada grupo de profissionais entenda os limites de suas responsabilidades e como seus cargos se encaixam na estrutura de riscos e controle da organização.

2.6.1 Primeira linha de defesa

Na primeira linha de defesa estão presentes os responsáveis pelos processos, sob administração de seus gestores, conforme entendimento do IIA (2013). As áreas de operação são as responsáveis por identificar, avaliar, controlar e mitigar os riscos, por meio da implementação de políticas e procedimentos internos. Por meio de uma estrutura de responsabilidades em cascata, os gerentes de maior nível hierárquico implementam os procedimentos de controle e supervisionam a execução por parte de seus funcionários. A gerência operacional serve naturalmente como a primeira linha de defesa, porque os controles são desenvolvidos como etapas do seu processo e no caso de mudanças ou quebras destes controles, é este o primeiro grupo a perceber e atuar nos procedimentos de adequação.

2.6.2 Segunda linha de defesa

Na segunda linha de defesa encontram-se as áreas de suporte, como as áreas de controle interno, *compliance* e demais áreas de qualidade, que possuem como principal responsabilidade ajudar a desenvolver e monitorar os controles executados pela primeira linha de defesa. A segunda linha pode intervir, modificar e desenvolver o controle interno e os sistemas de riscos, servindo de suporte para a primeira linha. Por este motivo, este

grupo não oferece análises verdadeiramente independentes aos órgãos de governança. Por fim, este grupo possui também a função de comunicação à alta administração.

De acordo com o modelo apresentado pelo IIA (2013), as responsabilidades da segunda linha podem incluir o fornecimento de estruturas de gerenciamento de riscos, a identificação de questões atuais e emergentes, a identificação de mudanças no apetite ao risco implícito da organização e o auxílio a gerência no desenvolvimento de processos e controles para gerenciar riscos e questões.

2.6.3 Terceira linha de defesa

A terceira linha de defesa é composto pela auditoria interna, com total nível de independência em relação as demais áreas da organização. De acordo com o modelo apresentado pelo IIA (2013), as responsabilidades da terceira linha incluem a atuação de acordo com as normas internacionais reconhecidas para a prática de auditoria interna, o reporte a um nível suficientemente alto na organização, de modo a cumprir com suas responsabilidades de forma independente. Assim, este grupo representa uma linha de reporte ativa e eficaz também ao órgão de governança.

2.7 CONTROL SELF-ASSESSMENT

Nesta seção será abordado o conceito do tema central da pesquisa: *Control Self-Assessment*.

2.7.1 Conceito de *Control Self-Assessment*

O conceito de *Control Self-assessment* (CSA) é trazido por Assi (2012) como:

Metodologia utilizada para avaliação e revisão dos principais objetivos dos negócios da organização, dos riscos envolvidos na busca por atingir esses objetivos e dos controles internos projetados para administrar esses riscos, avaliando a sua eficácia. (ASSI, 2012, p.120).

Segundo o mesmo autor, o CSA permite que os diversos riscos associados às atividades sejam devidamente identificados, administrados e mitigados pelos gestores por meio de reuniões e/ou questionários utilizados. O autor destaca ainda como fator crítico o acultramento dentro da organização:

A questão crítica para o sucesso do CSA é o acultramento sobre os riscos e controles de sua atividade pelos gestores dos processos e por todos os funcionários da organização, de modo que o reporte e a identificação dos riscos não estejam associados a punições, mas enfatizando a melhoria dos processos e consequentemente dos resultados da organização. (ASSI, 2012, p.122).

Assi (2012) ainda cita os pontos fortes e benefícios na implementação do processo de autoavaliação, como a disseminação da cultura de controle de riscos, a melhoria da confiabilidade da informação gerencial e para de evitar surpresas, pois estimula a identificação e administração de riscos. Com isto, a autoavaliação padroniza a metodologia de identificação e avaliação de riscos na organização, centraliza informações a respeito dos riscos relevantes, facilita o conhecimento do negócio e suas vulnerabilidades, identifica atividades críticas com controles frágeis ou inexistentes, mantendo a alta administração informada sobre as formas de execução do trabalho. Pode-se atribuir a esta metodologia ainda o estabelecimento de planos de ação com responsabilidades e prazos definidos e a gestão participativa e melhor conhecimento para os funcionários envolvidos no processo.

2.7.2 Origem do *Control Self-Assessment*

De acordo com Moeller (2004), a metodologia de *Control Self-Assessment*, ou autoavaliação, foi iniciada na empresa petrolífera *Gulf Oil* em 1987 no Canadá. Esta empresa utilizou a metodologia para avaliar a eficácia de controle e processos no seu negócio para atendimento de um decreto legal local, que determinou que a *Gulf Oil* informasse dados sobre seus controles internos. Entretanto, a empresa passava por dificuldades para resolver os problemas de medição de petróleo e gás que foram identificados por meio do processo tradicional de auditoria, e assim, o grupo de auditoria da *Gulf Oil* lançou uma abordagem de autoavaliação por meio de reuniões, que envolvia a participação de gerência e da equipe para entrevistas e discussões de questões de

controles internos ou processos específicos. Segundo Moeller (2004), após este evento, o processo de autoavaliação se tornou um mecanismo bem-sucedido para avaliar controles e na sequência, o CSA foi adotado por várias grandes empresas e para se tornar parte dos padrões de prática profissionais do IIA.

Conforme afirmado por Champlain (2003), em meados dos anos 90, o interesse pelo CSA começou a tomar o mundo da auditoria. O IIA sediou sua primeira conferência de CSA em Orlando em 1995. Esta conferência foi tão bem-sucedida, que o IIA organizou uma segunda conferência sobre o tema em Toronto em 1996 e uma terceira em Las Vegas em 1997.

Em 1996, todas as *Big Six* (agora *Big Four*) começaram a oferecer serviços de consultoria de CSA e ajudaram a disseminar a metodologia junto as demais organizações.

2.8 ESTUDOS ANTECEDENTES

A apresentação de estudos antecedentes é relevante para complementação deste projeto e também para a ampliação do conhecimento do assunto sob outras visões e perspectivas. Os estudos antecedentes citados aqui abordam principalmente os temas: riscos, controle interno e *Control Self-Assessment*.

Para cada estudo referenciado, serão apresentados os temas dos trabalhos, seu ano de publicação, nome dos autores envolvidos, os objetivos e os resultados obtidos. Todos os estudos referenciados foram publicados entre os anos de 2001 a 2008, época em que os ritos de governança voltados para controles internos começaram a ganhar força em todo o mundo.

A seguir serão citados estudos antecedentes sobre os temas abordados neste projeto, como forma de complemento dos conceitos aqui apresentados:

QUADRO 2 – ESTUDOS ANTECEDENTES

Autor(es) / Ano	Título	Objetivo	Resultado
Joseph and Engle, 2001	<i>The use of Control Self-Assessment IN Audits.</i>	<i>Explore how the auditors can use CSA to assess financial statement risks.</i>	<i>CSA can be useful for effectiveness of audit process by providing insight on “soft issues.” The auditor can use a meeting or survey to explore these topics with employees that have direct involvement with the controls evaluated. If there is an agreement among employees on the issue, the auditor has strong evidence of inherent risk and can execute the audit more efficiently and effectively.</i>
Bordin e Saraiva, 2005	O Controle Interno como ferramenta fundamental para fidedignidade das informações contábeis.	Demonstrar a importância do controle interno como ferramenta para assegurar a fidedignidade e integridade das demonstrações contábeis.	Como resultado deste estudo, foi possível concluir que os objetivos da empresa só são alcançados efetivamente por meio de um controle interno adequado as suas necessidades. Controles internos eficientes ajudam a evitar o abuso de poder, os erros, as fraudes e principalmente a ineficiência, melhorando a qualidade da informação contábil.
Filho, Jacques e Marian, 2005.	O Controle Interno como ferramenta para o sucesso empresarial.	Demonstrar o papel fundamental do controle interno no exercício das atividades da empresa.	O artigo demonstra a importância do sistema de Controle Interno e seus procedimentos no exercício das atividades da empresa, devendo ser adaptado de acordo com as características e necessidades da entidade.
Paulo, Fernandes, Rodrigues e Eidit, 2007.	Riscos e controles internos: uma metodologia de mensuração dos níveis de controle de riscos empresariais.	Apresentar uma metodologia de mensuração do nível de riscos inerentes aos processos de qualquer entidade.	O modelo apresentado possibilita que o gestor de riscos identifique para quais riscos são necessárias ações de melhoria de controle, contribuindo para a otimização da aplicação dos recursos disponíveis para a gestão de riscos e controles internos nas empresas. O estudo conclui que a metodologia caracterizada pela matriz de desempenho de controle é uma ferramenta relevante no processo de mensuração e controle de riscos.
Pereira, 2008	A importância do Controle Interno para gestão de empresas.	Avaliar que a importância do controle interno para as empresas.	Por meio da pesquisa realizada pode-se considerar que o controle interno representa uma fonte relevante para informar e suportar as decisões dos gestores dentro de uma organização.

FONTE: Elaborado pela autora (2020)

Os estudos citados complementam a abrangência do tema estudados e reforçam a importância de controle interno para a mitigação de riscos nas empresas.

3. METODOLOGIA DA PESQUISA

Os procedimentos metodológicos adotados para a execução da pesquisa são apresentados nesta seção, considerando a tipologia da pesquisa quanto aos objetivos, aos procedimentos e abordagem do problema.

3.1 TIPOLOGIA DA PESQUISA QUANTO AOS OBJETIVOS

Metodologicamente este estudo possui características de ciências sociais aplicadas, pois contém embasamento teórico e simultaneamente pode ser aplicada no cotidiano. Para tal, são definidos os tipos de pesquisa como descritiva e explicativa.

A pesquisa é considerada como descritiva, pois segundo Gil (2009), esse tipo de pesquisa tem como objetivo “a descrição das características de determinada população ou fenômeno ou, então, o estabelecimento de relação entre variáveis”. Para Andrade (2002), a pesquisa descritiva “preocupa-se em observar os fatos, registrá-los, analisá-los, classificá-los e interpretá-los”.

O estudo também é considerado como explicativo, pois para Andrade (2002, p.20): “a pesquisa explicativa é um tipo de pesquisa mais complexa, pois além de registrar, analisar, classificar e interpretar os fenômenos estudados, procura identificar fatores determinantes. A pesquisa explicativa tem por objetivo aprofundar o conhecimento da realidade, procurando a razão, o porquê das coisas e por esse motivo, está mais sujeita a erros”.

3.2 TIPOLOGIA DA PESQUISA QUANTO AOS PROCEDIMENTOS

Os procedimentos de uma pesquisa referem-se à forma pela qual o estudo é conduzido e como os dados são obtidos. Desta forma, os procedimentos para coleta de dados para o presente estudo se resumem em: pesquisa bibliográfica e documental.

Sobre a pesquisa bibliográfica, Gil (1999) define que é a pesquisa desenvolvida mediante material já elaborado, principalmente livros e artigos científicos. O material consultado na pesquisa bibliográfica abrange um referencial público em relação ao tema

estudado, e com isso, é possível elaborar o trabalho acadêmico com uma perspectiva histórica com a reunião de diversas publicações isoladas e atribuir-lhes uma nova leitura.

De acordo com Santos (2009), a pesquisa documental é realizada com base em documentos que não receberam tratamento de análise. Embora seja similar a pesquisa bibliográfica, este tipo de pesquisa só se realiza sobre documentos analisados e pertencentes a autores que deram o estudo pronto e acabado.

3.3 TIPOLOGIA DA PESQUISA QUANTO ABORDAGEM DO PROBLEMA

A pesquisa se caracterizou como qualitativa. De acordo com Raupp; Beuren, 2004,

os estudos que empregam uma metodologia qualitativa podem descrever a complexidade de determinado problema, analisar a interação de certas variáveis, compreender e classificar processos dinâmicos vividos por grupos sociais. (RAUPP; BEUREN, 2004, p. 91).

Segundo Chizzotti (1995, p.52) a pesquisa qualitativa fundamenta-se em “dados coligidos nas interações interpessoais, na coparticipação das situações dos informantes, analisadas a partir da significação que estes dão aos seus atos. O pesquisador participa, compreende e interpreta”.

3.4 LEVANTAMENTO DE DADOS E INFORMAÇÕES

Para realização do pré-projeto, os dados e informações levantados para construção da referência bibliográfica foram obtidas com base em documentos elaborados, como livros e publicações a respeito do tema levantado. A definição dos temas abordados no referencial bibliográfico foi realizada com base na relevância dos temas para a melhor compreensão do desenvolvimento da pesquisa.

Para a realização do projeto de monografia, as informações foram levantadas com base na análise e interpretação dos dados destacados no referencial teórico e também no histórico e experiência profissional da autora.

4. APLICAÇÃO DA METODOLOGIA DE CONTROL SELF-ASSESSMENT

Nesta seção foram desenvolvidos temas práticos, abordando desde as características e estrutura que uma empresa multinacional precisa ter para aplicação da metodologia de *Control Self-Assessment* até a sugestão de questionários, monitoramento de planos de remediação e a manutenção da cultura de controle de interno dentro da organização.

A proposta de implementação e manutenção da metodologia de *Control Self-Assessment* neste trabalho tem como principal objetivo auxiliar e orientar empresas multinacionais na gestão de seus riscos.

4.1 ESTRUTURA EMPRESARIAL

O primeiro passo para a implementação da metodologia de *Control Self-Assessment* em qualquer organização é a tomada de decisão estratégica pela alta administração para alguns aspectos fundamentais, tais como definição de papéis e responsabilidades das 3 linhas de defesa e a definição dos recursos e investimentos a serem aplicados. Em uma empresa multinacional, estas decisões são ainda mais complexas, uma vez que existe a necessidade de definição da centralização ou descentralização das atividades e das responsabilidades envolvidas.

4.1.1 Estrutura das 3 linhas de defesa

Com base no modelo das 3 linhas de defesa descrito pelo IIA, é de fundamental importância que a empresa tenha definido claramente os papéis e responsabilidades de cada um destes agentes. Esta etapa envolve basicamente a definição estratégica da alta administração para definição da estrutura necessária para que as atividades operacionais possam ser iniciadas na sequência.

A primeira linha de defesa é caracterizada pelos responsáveis de cada processo e as responsabilidades atribuídas devem ser compatíveis ao ambiente de atuação deste grupo. As áreas de operação são as responsáveis por identificar, avaliar, controlar e mitigar os riscos, por meio da implementação de políticas e procedimentos internos. Em

uma empresa multinacional é comum que este grupo seja representado por usuários alocados em cada filial, pois são estes os usuários mais próximos do negócio e que conhecem o processo com maior riqueza de detalhes. Em uma organização multinacional, o mesmo processo pode estar sujeito a riscos e obrigações legais diferentes em cada país em que a empresa atua, motivo pelo qual os responsáveis de cada filial, na maioria dos casos, serão os mais indicados para atuar como primeira linha de defesa. Entretanto, não é incomum que alguns processos de empresas multinacionais sejam padronizados de tal forma que a matriz da empresa também possa ser definida como a primeira linha de defesa. Neste caso, a matriz da empresa ganha um papel ainda mais relevante, que é o de assegurar que todas as filiais estejam executando os controles conforme definido globalmente.

A segunda linha de defesa é caracterizada por áreas de suporte, neste caso, a área de Controles Internos. Como principal responsabilidade, esta equipe deve ajudar a desenvolver e monitorar os controles executados pela primeira linha de defesa. Assim, é fundamental uma relação de confiança e parceria entre segunda e primeira linha de defesa. Em uma empresa multinacional, recomenda-se que a segunda linha de defesa seja facilmente acessada pela primeira linha de defesa. Desta forma, é comum e recomendado que esta equipe também esteja alocada nas filiais, tendo maior conhecimento dos processos locais e autonomia para transitar entre os departamentos. Entretanto, para fins de padronização, é importante que exista também uma equipe de Controles Internos central e global ditando a forma de trabalho e metodologia para que todas as áreas de Controles Internos da empresa trabalhem em harmonia e de forma padronizada. Este papel global pode ser alocado na área de Controles Internos da Matriz.

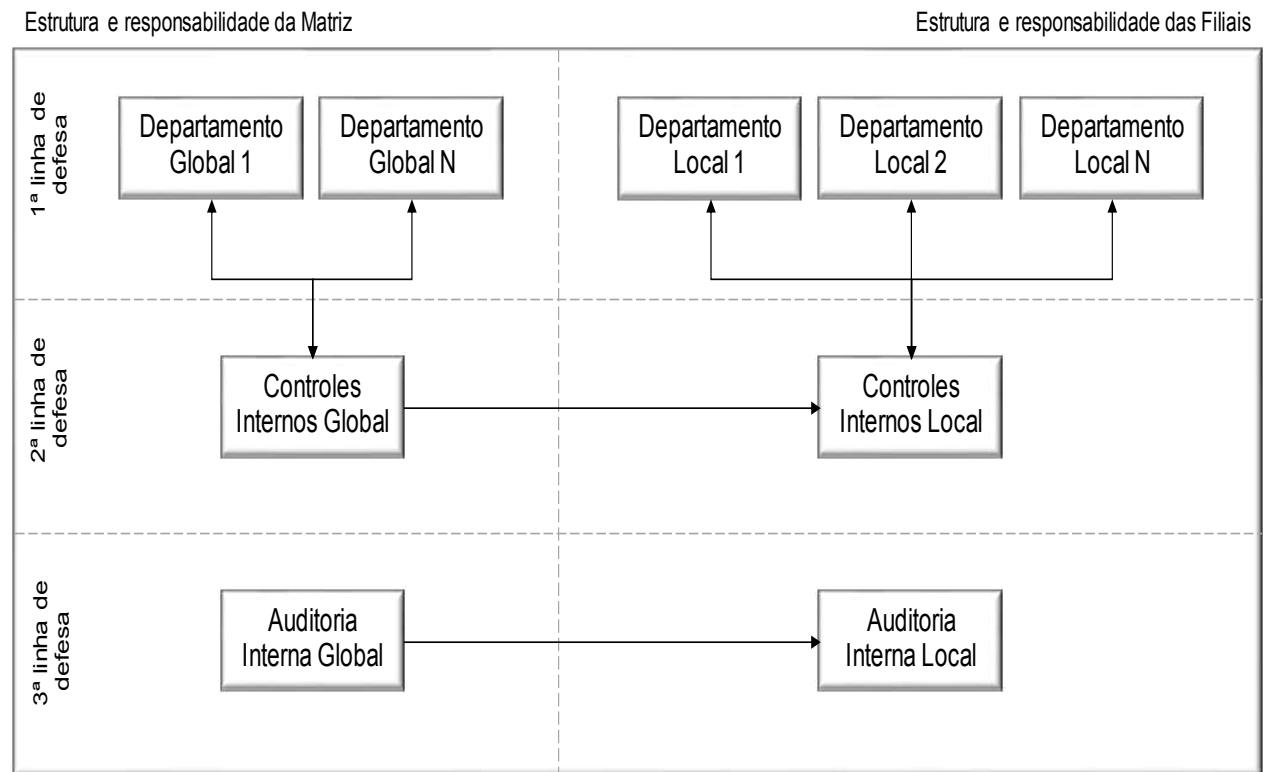
Na prática, na implementação e manutenção do *Control Self-Assessment*, é a segunda linha de defesa que irá definir o que se espera da metodologia, bem como é a área que irá coordenar e monitorar o andamento das atividades relacionadas a este tema. Por este motivo, é importante que o departamento de Controles Internos possua autonomia e influência sobre os demais departamentos (primeira linha de defesa) para obter a atenção e engajamento para realização dos trabalhos.

Por fim, a terceira linha de defesa é caracterizada pela auditoria interna, com total nível de independência em relação as demais áreas da organização. Na prática, a

auditoria interna busca realizar avaliações para concluir sobre a efetividade e conformidade dos processos e controles. A auditoria interna não tem participação efetiva no processo de *Control Self-Assessment*, entretanto, o resultado de suas avaliações pode servir de *input* para a primeira e a segunda linha de defesa para a melhoria de seus processos e controles. Em empresas multinacionais é possível encontrar esta equipe atuando de forma global ou também de forma individual nas filiais da empresa.

Abaixo segue uma proposta de estrutura das 3 linhas de defesa em uma empresa multinacional:

FIGURA 2 – PROPOSTA DE ESTRUTURA DAS LINHAS DE DEFESA



FONTE: Elaborado pela autora (2020)

Vale lembrar que a proposta acima foi desenhada pensando em uma empresa multinacional de grande porte com diversas filiais, entretanto, a estrutura e a quantidade de funcionários que irá compor cada uma das linhas de defesa deve estar em alinhada com o plano estratégico de cada empresa.

4.1.2 Definição dos recursos necessários

Outra decisão estratégica a ser definida pela alta administração refere-se ao investimento que a empresa está disposta a alocar para a implementação de um processo de *Control Self-Assessment*. A estruturação da equipe de Controles Internos, será necessário também a implementação de uma ferramenta sistêmica que assegure a realização das atividades de forma efetiva e passível de monitoramento e rastreamento histórico e de confiança.

A definição desta ferramenta sistêmica deve considerar a estrutura e o tamanho da empresa, entretanto, a ferramenta precisa entregar algumas funcionalidades mínimas que permitam a implementação de um processo robusto e adequado. Para os casos de empresas multinacionais, esta preocupação deve ser ainda mais redobrada, com a contratação de sistemas de fornecedores sérios, com suporte de funcionamento e com possibilidade de execução em diversas localidades e países.

As principais funcionalidades mandatórias de uma ferramenta de autoavaliação são:

- a) Possibilidade de formalização do *Control Self-Assessment*, contendo o registro de usuário responsável, data e hora de sua realização;
- b) Possibilidade de inclusão de anexo para evidenciação do resultado de avaliação;
- c) Workflow de revisão do *Control Self-Assessment*;
- d) Criação de plano de ação vinculado ao *Control Self-Assessment*, para os casos de controles definidos como não efetivos ou não adequados;
- e) Possibilidade de consultar o histórico de avaliações de períodos anteriores;
- f) Possibilidade de extração de relatórios de monitoramento de todos os processos executados na ferramenta.

Em algumas ferramentas utilizadas por grandes corporações, existem funcionalidades ainda mais avançadas, que empregam recursos tecnológicos para fins de automatização nas conferências de controle. Em outras palavras, a ferramenta de *Control Self-Assessment* é parametrizada para ler regras de controles automatizados, e sempre que é acionada, a própria ferramenta realiza a leitura desta parametrização sistêmica e emite um parecer favorável ou desfavorável ao parâmetro. Em casos

desfavoráveis, a ferramenta emite um alerta para a área responsável e/ou para a área de Controles Internos, indicando que um controle automatizado chave (como um bloqueio sistêmico por exemplo) pode ter sido alterado e estar afetando o processo em questão.

Existem diversas ferramentas e sistemas de *Control Self-Assessment* disponíveis no mercado, entre elas BWISE, MetricStream e SAP *Process Control*. Estes sistemas ajudam as empresas na documentação de seus processos, riscos e controles, bem como na captura de evidências de controles executados, monitoramento e acompanhamento de relatórios e status de conformidade de sua organização. Muitas empresas de grande porte, como as multinacionais, usam o SAP como seu sistema de ERP principal e tendem a escolher o SAP GRC *Process Control* como sistema de risco e controle. Inclusive, várias empresas de auditoria (exemplo as *Big Four*) estão familiarizadas com esta ferramenta e acabam utilizando alguns dos benefícios da ferramenta para o próprio processo de auditoria.

De acordo com o estudo “*A practical view on SAP Process Control*” de 2017 da KPMG, as principais funcionalidades entregues pelo SAP GRC *Process Control* são:

- a) Gerenciamento eficiente de riscos e controles através da funcionalidade do *workflow*;
- b) Avaliações de risco, análise de materialidade, planejamento de controles e testes;
- c) Suporte nos testes de desenho e testes de efetividade. Os testes de controle podem ser realizados manualmente, de forma semi automatizada e totalmente automatizada.
- d) Permite a documentação de deficiências de controle e fornece relatórios para rastrear e corrigir deficiências.
- e) Permite a realização do processo de *sign-off* (autoavaliação realizado pela alta gestão).
- f) Permite trilha de auditoria completa e registro das etapas de teste realizadas.

Vale lembrar que a escolha da ferramenta deve ser analisada por um time *cross* funcional dentro da organização, considerando as necessidades de todas as linhas de defesa e também do departamento de tecnologia da informação da empresa.

4.2 IDENTIFICAÇÃO DO ESCOPO

Nesta seção estão detalhadas as principais atividades para implementação e manutenção do *Control Self-Assessment* em uma empresa multinacional, incluindo desde a identificação dos processos e controles relevantes até a definição da frequência de realização do CSA.

4.2.1 Mapeamento de processos

Uma vez que a estrutura da empresa foi definida, a primeira decisão a ser tomada pela segunda linha de defesa (denominada área de Controles Internos para escopo deste trabalho) é a definição dos processos e subprocessos que serão incluídos no *Control Self-Assessment*. Para isso, fatores internos e externos à organização devem ser levados em conta neste momento de decisão. Como fatores internos, podem ser destacados como premissas para priorização dos processos a serem avaliados: os riscos inerentes do negócio, o histórico de erros ou fraudes, a materialidade de cada processo, o apetite ao risco e os objetivos da organização. Como fatores externos é importante observar o ambiente em que a empresa está inserida e identificar se existem obrigatoriedades legais e/ou regulatórias que demandem atenção especial. Por exemplo, instituições financeiras possuem obrigatoriedades adicionais junto ao BACEN que instituições industriais não possuem; ou ainda empresas com capital aberto no mercado norte-americano estão sujeitas às obrigatoriedades da lei Sarbanes-Oxley (SOx) que empresas com capital aberto local ou de capital fechado não estão sujeitas.

Além da análise dos fatores internos e externos na etapa de mapeamento dos processos que farão parte da autoavaliação de controles, é importante que os conceitos de processo, subprocesso, atividade e controle estejam claramente entendidos por todos.

Entende-se por processo a sequência de atividades que pode ser realizada por uma ou mais áreas e que possui um início e um fim determinado com um objetivo comum. Como exemplos de processos podem ser citados os processos de Vendas, Compras, Recursos Humanos, entre outros.

O termo subprocesso é utilizado para um conjunto de atividades estabelecidas dentro de um processo. Por exemplo, dentro do processo de Vendas, encontram-se diversos subprocessos, como o subprocesso de faturamento, contas a receber, cobrança, entre outros. Da mesma forma, no processo de Compras, observa-se diversos subprocessos, como a cotação e a compra em si, o recebimento do que foi comprado, o pagamento, entre outros. Já no processo de RH, observa-se variados subprocessos, como admissão, folha de pagamento, benefícios, desligamento, entre outros.

O termo atividade é o trabalho efetivamente realizado pelo funcionário e inclui a interação do profissional com o ambiente de trabalho e as ferramentas utilizadas. A atividade pode ser caracterizada por ações simples ou complexas, como o envio de uma proposta de negociação para o cliente, a emissão e envio de um contrato de compras para o fornecedor ou a elaboração do cálculo da folha de pagamento do mês corrente. As atividades em si não são avaliadas no processo de *Control Self-Assessment*, mas são importantes para o entendimento dos riscos e do processo como um todo.

Por fim, entende-se como controle tudo aquilo que é realizado para a mitigação de algum risco de erro ou fraude na realização das atividades para alcançar um objetivo final. Por exemplo, antes do envio de uma proposta para o cliente ou do envio de um contrato para o fornecedor, existem alçadas definidas que aprovam o valor proposto para a venda ou compra em questão; ou, após o cálculo da folha de pagamento e antes do pagamento financeiro, existe um controle de revisão por uma pessoa independente, a fim de garantir que todas as variáveis foram consideradas adequadamente no cálculo.

No processo de mapeamento inicial é fundamental que sejam determinados os processos e subprocessos que serão incluídos no processo de *Control Self-Assessment*. Esta definição é importante para definir o tamanho do projeto, a estrutura e o tempo necessário, bem como as pessoas que serão envolvidas. Para este tipo de definição, o departamento de Controles Internos poderá realizar entrevistas com gestores chaves e com a alta administração, obter as últimas demonstrações financeiras da Companhia, obter histórico de denúncias de fraudes junto ao Comitê de Ética, realizar *benchmarking* com empresas similares, entre outros. A definição dos controles a serem avaliados também é fundamental para o processo de *Control-Self Assessment*, e será descrito nos itens 4.2.2 e 4.2.3 deste estudo.

4.2.2 Matriz de Riscos e Controles

Com base nas definições dos processos e subprocessos a serem avaliados, torna-se possível realizar o mapeamento mais detalhado no nível operacional de controles. Para isso, a área de Controles Internos conta com um documento chamado de Matriz de Riscos e Controles, que é um documento formal em que são registrados todos os riscos e controles existentes em uma organização.

Para decidir quais serão os controles a serem incluídos na Matriz de Riscos e Controles e quais devem ser incluídos no processo de *Control Self-Assessment*, recomenda-se que a organização realize uma análise de probabilidade de ocorrência do risco e impacto que o risco pode representar para a organização.

Para a definição do grau de probabilidade de um risco, deve-se avaliar a quantidade de vezes esperada que um risco venha a ocorrer. Esta análise pode considerar a volumetria de transações do processo analisado, o histórico de erros conhecidos, a complexidade das transações e a dependência de pessoas para realização dos processos. Já para o levantamento do possível impacto, devem ser avaliados todos os impactos e problemas que podem ser gerados caso o risco venha ser materializado. O impacto não necessariamente precisa ser atrelado com fatores financeiros, mas também fatores negativos junto aos *stakeholders*, como clientes, fornecedores e funcionários.

O julgamento e a experiência profissional tanto da área de Controles Internos quanto da área mapeada também são fundamentais para a análise de impacto e probabilidade, sendo recomendado que esta análise seja realizada e construída em conjunto. Tanto o fator “impacto” quanto o fator “probabilidade” podem ser avaliados como “Baixo”, “Médio” e “Alto”, resultando em um grau de criticidade do risco, conforme a matriz a seguir:

Com base na Figura 3 apresentada, é possível concluir que os riscos com maior probabilidade de ocorrência e maior impacto para a organização são classificados como mais críticos, e assim, demandam maior atenção da administração. Assim, os controles que apresentarem maior impacto e maior probabilidade de ocorrência devem ter maior atenção e devem ser considerados como controles chaves para atingimento dos objetivos da empresa.

FIGURA 3 – MATRIZ DE IMPACTO E PROBABILIDADE

Probabilidade ↑	Risco Médio	Risco Alto	Risco Alto
	Risco Baixo	Risco Médio	Risco Alto
	Risco Baixo	Risco Baixo	Risco Médio
	Impacto →		

FONTE: Elaborado pela autora (2020)

Arelado a análise de impacto e probabilidade, a organização deve definir o tratamento a ser dado a cada controle: evitar, reter, reduzir, transferir ou explorar o risco. Para os riscos que forem classificados para tratamento de redução (também conhecido como mitigação), devem ser criados controles internos e posteriormente, estes devem ser formalizados na Matriz de Riscos e Controles.

A documentação dos processos, dos riscos e dos controles internos é realizada por meio da Matriz de Riscos e Controle, a qual é estruturada para garantir as informações necessárias que suportam a avaliação dos processos, sistemas e controles.

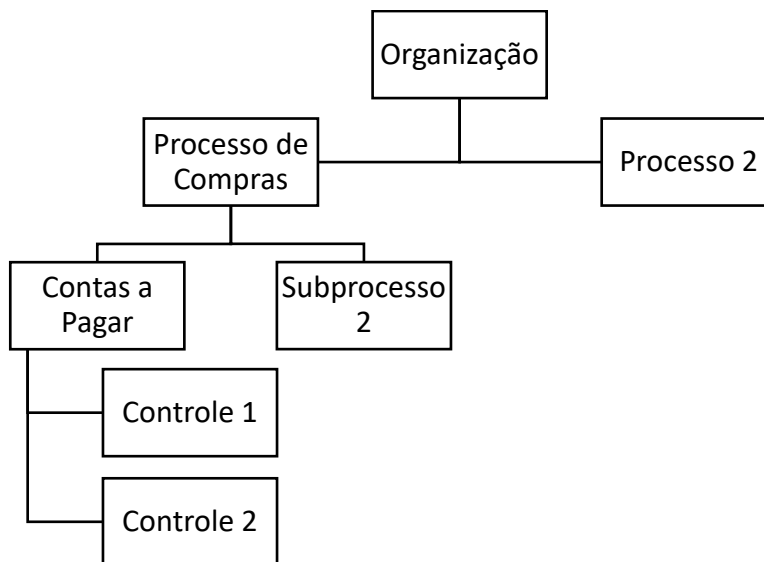
A Matriz de Riscos e Controles é um documento vivo e dinâmico, e desta forma, sempre que houver alguma alteração de processo, subprocesso, ou na forma que o controle é executado, existe a necessidade de atualização das informações neste documento.

Na estrutura de Matriz de Riscos e Controle, todos os controles de um mesmo processo e de um mesmo subprocesso devem ser agrupados e padronizados. Desta forma, esta Matriz facilita a visão de todos os riscos mitigados, permitindo a visão de um processo completo.

Assim, recomenda-se que todos os processos, subprocessos, riscos e controles definidos como chaves para mitigação estejam mapeados e formalizados na Matriz de Riscos e Controles.

Uma vez que apenas controles chaves são formalizados na Matriz de Riscos e Controles, é recomendável que estes sejam avaliados ao menos uma vez ao ano pela organização. A imagem a seguir auxilia no entendimento de como os controles estão vinculados aos subprocessos, que por sua vez, estão vinculados aos processos mapeados:

FIGURA 4 – ESTRUTURA MATRIZ DE RISCO E CONTROLE



FONTE: Elaborado pela autora (2020)

A Matriz de Riscos e Controles costuma ser apresentada em formato de tabela. Algumas informações devem estar formalizadas e atreladas adequadamente, de forma que facilite o entendimento adequado do controle executado, e por consequência, reflita na qualidade do *Control Self-Assessment*.

Na documentação de uma Matriz de Riscos e Controles, os controles internos costumam ser atrelados a um código de identificação. Este código pode ser sequencial ou seguir uma lógica definida pela própria administração. O importante é que o controle possa ser identificado facilmente por todos os envolvidos, de forma que não ocorram confusões desnecessárias. Outras informações que devem ser formalizadas na Matriz são: nome do processo, subprocesso, risco mitigado, objetivo do controle, descrição detalhada do controle e as evidências que suportam a existência de cada controle.

Abaixo segue exemplificado uma versão simplificada de uma Matriz de Riscos e Controles:

QUADRO 3 – MATRIZ DE RISCO E CONTROLE

Controle	Processo	Subprocesso	Risco	Objetivo	Descrição	Evidências
C.1	Compras	Contas a Pagar.	Perda financeira gerada por pagamento incorreto e/ou indevido.	Assegurar que todos os pagamentos sejam aprovados antes do desembolso financeiro.	Todo pagamento é aprovado de acordo com a política de Alçadas de Aprovação. A aprovação é realizada no sistema “ABC” de forma prévia ao desembolso financeiro.	1) Política de Alçadas de Aprovação; 2) Evidência de aprovação de pagamento no sistema “ABC”.

FONTE: Elaborado pela autora (2020)

Nos campos destacados no QUADRO 3, a Matriz de Riscos e Controles pode, e deve, conter também os seguintes campos:

Finalidade (Controle Detectivo ou Preventivo)

Frequência (Anual, Semestral, Trimestral, Mensal, Diário, Por ocorrência)

Tipo de automatização (Manual ou Automático)

Data de validade do controle

Usuário responsável.

É comum observar ainda que empresas multinacionais contam com um campo adicional na Matriz de Riscos e Controles, definindo um descritivo de controle genérico global como referência para todas as filiais, e um descritivo de controle local que atenda o controle genérico. Por exemplo, enquanto um descritivo genérico global pode ser descrito como: “Todos os pagamentos são aprovados antes do desembolso financeiro”, um descritivo local poderia ser descrito como “Todo pagamento é aprovado de acordo com a política de Alçadas de aprovação. A aprovação é realizada no sistema de forma prévia ao desembolso financeiro”. Para atender o mesmo descritivo genérico global, outra

filial poderia ter um descritivo local como “Todo pagamento é aprovado mediante assinatura de um formulário físico pelo gerente financeiro”. Em ambos os descritivos locais, mesmo sendo executados de formas distintas, os controles se propõem ao mesmo objetivo, que é mitigar o risco de “Perda financeira gerada por pagamento incorreto e/ou indevido”.

Vale ressaltar que quanto mais detalhes do controle estiverem formalizados na Matriz de Riscos e Controles, maior será a clareza da primeira linha de defesa quanto ao que é esperado na execução do controle, e mais rica poderá ser a sua contribuição para o processo de *Control Self-Assessment*.

4.2.3 Validação da Matriz de Riscos e Controles

Uma vez que a Matriz de Riscos e Controles foi finalizada e documentada, é essencial que exista uma validação formal por parte do departamento de Controles Internos com todos os demais departamentos envolvidos. Isso deve ocorrer para o primeiro mapeamento da Matriz e também para todas as alterações realizadas subsequentemente. Esta validação é importante pois permite que os departamentos envolvidos (primeira linha de defesa) conheçam os riscos, controles e evidências que devem ser considerados no momento de realizar sua autoavaliação. Diante disso, quando o departamento dono do controle aprova as informações da Matriz de Riscos e Controles, a consciência e a cultura de controles internos são reforçadas dentro da organização.

4.2.4 Usuários envolvidos no *Control Self-Assessment*

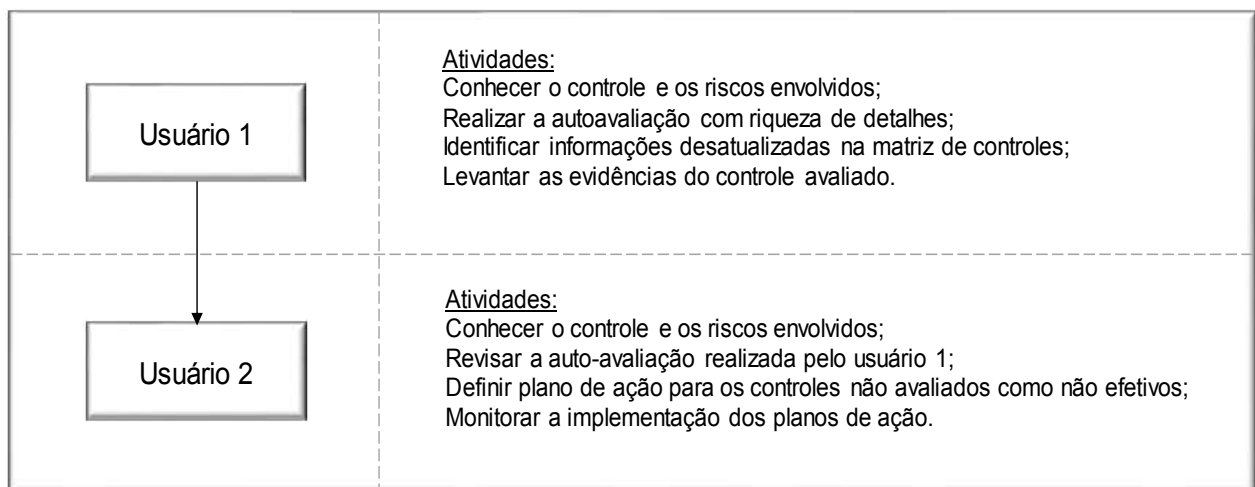
É fundamental que os usuários selecionados para realizar o *Control Self-Assessment* sejam definidos de forma adequada e responsável para que o resultado da autoavaliação ocorra com a qualidade esperada pela organização. Para isso, recomenda-se que pelo menos dois usuários sejam envolvidos na avaliação de cada controle:

Usuário 1: O primeiro usuário envolvido no *Control Self-Assessment* deve ter experiência e maturidade para realizar uma autoavaliação criteriosa e verdadeira. Para que a avaliação ocorra com a riqueza de detalhes esperada, é necessário que este

usuário conheça a execução do controle e também os riscos envolvidos. Este usuário nem sempre vai ser o executor do controle em sua totalidade, mas o conhecimento do processo, do controle e dos riscos envolvidos permitem que seja realizada uma avaliação holística e confiável. Portanto, é importante que este usuário tenha condições de consultar e obter as evidências que corroboram com a execução do controle, o que muitas vezes pode ser solicitada no próprio momento do *Control Self-Assessment*, ou também pode ser requerido pela segunda ou terceira linha de defesa em momentos oportunos.

Usuário 2: Este usuário deve possuir uma senioridade superior ao usuário 1, preferencialmente com cargo de gestão. A principal responsabilidade deste usuário é revisar com criticidade a autoavaliação realizada pelo usuário 1 e em caso de discordância, sinalizar e formalizar o seu posicionamento. Para os casos em que o controle é avaliado como ineficaz, este usuário possui a responsabilidade de coordenar as ações de melhoria para implementação da efetividade do controle e mitigação dos riscos. A Figura 5 a seguir detalha as atividades e as responsabilidades que são esperadas de cada usuário envolvido no processo de *Control Self-Assessment*:

FIGURA 5 – PROPOSTA DE USUÁRIOS ENVOLVIDOS NO CSA



FONTE: Elaborado pela autora (2020)

Vale lembrar que a proposta acima foi desenhada pensando em uma empresa multinacional de grande porte, entretanto, a definição dos usuários envolvidos na

realização do CSA deve estar alinhada com a estrutura de cada empresa, bem como seu plano estratégico e de gestão.

4.2.5 Definição da frequência de realização do *Control Self-Assessment*

Diferentemente da frequência do controle, já abordado no item 4.2.2, é fundamental que seja definido e comunicado a todos os *stakeholders* a frequência de realização do *Control Self-Assessment*. Esta frequência deve estar alinhada a estratégia e também a velocidade de mudanças dentro da organização.

Empresas que possuem um ritmo mais acelerado, forte tendência de inovação e mudanças frequentes em seus processos, requerem a realização de avaliação de seus controles com maior frequência, de forma a garantir que estas mudanças não impactem na efetividade de seus controles. Assim, é possível a realização de *Control Self-Assessment* mensais ou até trimestrais.

A realização de CSA trimestrais é interessante para aquelas organizações que realizam a publicação de demonstrações financeiras trimestrais, pois assim, eventuais desvios são identificados e corrigidos tempestivamente. Para as empresas que optarem por realizar o CSA de forma mensal, é importante destacar que durante o intervalo desta frequência, todos os *stakeholders* devem ter condições de avaliar e agir nas tratativas dos controles, caso necessário. Se por ventura um controle passar a ser avaliado como inefetivo por vários meses seguidos, sem nenhuma ação concreta pela primeira linha de defesa ou sem nenhum monitoramento pela segunda linha de defesa, o CSA perde a sua efetividade e passa a ser encarado como mera formalidade ou burocracia.

As empresas que possuem um ritmo menos acelerado no quesito de mudanças e/ou inovação, podem optar por realizar o *Control Self-Assessment* de forma mais espaçada, podendo ser realizado de forma semestral ou até mesmo anual. A frequência mínima sugerida para a realização de um CSA é a frequência anual, pois neste caso os usuários responsáveis conseguem avaliar um ciclo completo dos controles chaves.

4.3 DEFINIÇÃO DO QUESTIONÁRIO DE CONTROL SELF-ASSESSMENT

A execução de um *Control Self-Assessment* pode ocorrer por meio de entrevistas com pessoas chaves ou até mesmo por preenchimento de questionários ou formulários.

Este estudo recomenda a realização do CSA por meio de questionários formais, uma vez que permite ao usuário que está realizando a autoavaliação uma reflexão e levantamento de dados e informações com maior tranquilidade. No entanto, os questionários contribuem para a formalização da autoavaliação pelo próprio dono do controle, evitando assim, desvios de entendimento, ruídos de comunicação ou mesmo indução de respostas, que podem acabar ocorrendo por meio de entrevistas. A formalização das respostas por meio de um questionário gera evidências robustas do processo de *Control Self-Assessment*, além de proporcionar a formalização para consultas futuras.

A realização do CSA por meio de questionários é bastante simples, e baseia-se essencialmente em perguntas a respeito do controle que está sendo avaliado e da sua classificação da efetividade, com base na percepção do dono do controle.

Para a construção do questionário, sugere-se que as perguntas a respeito do controle avaliado sejam apresentadas no início do questionário, de forma a auxiliar o usuário em sua reflexão. Assim, a classificação da efetividade do controle pode ser apresentada ao final do questionário, como uma forma de conclusão do processo de *Control Self-Assessment (CSA)*.

O quadro abaixo apresenta algumas sugestões de perguntas que podem ser incluídas em um questionário de CSA. Todas as perguntas não precisam obrigatoriamente ser incluídas em todas as autoavaliações.

As empresas que decidirem por realizar CSAs com maior frequência (Ex: mensal ou trimestral), podem alternar as perguntas à medida que as autoavaliações são realizadas ao longo do ano. Assim, é interessante que todos os temas questionados sejam respondidos pelo menos uma vez ao ano, garantindo uma autoavaliação completa no período.

QUADRO 4 – SUGESTÃO DE QUESTIONÁRIO CSA

Objetivo	Pergunta	Resposta
Assegurar que o controle está sendo avaliado pelo seu respectivo dono.	Você é o responsável por esta atividade de controle? Caso não seja o responsável, favor interromper essa avaliação e entrar em contato com a equipe de Controles Internos para reatribuir ao responsável correto.	Sim / Não / N/A Comentário obrigatório para as respostas "Não" e "N/A".
Estimular o dono do controle a avaliar se a atividade ocorre conforme descrito no campo de descrição do controle.	O descritivo do controle apresentado na "Matriz de Riscos e Controles" descreve exatamente o processo atual? Caso exista alguma informação divergente, favor detalhá-la nos comentários para que a equipe de Controles Internos possa avaliar e ajustar o que for necessário.	Sim / Não / N/A Comentário obrigatório para as respostas "Não" e "N/A".
Estimular o dono do controle a revisar as evidências de controle listadas.	As evidências listadas na "Matriz de Riscos e Controles" e consideradas como mandatórias para assegurar a efetividade deste controle foram anexadas nesta autoavaliação? Caso exista alguma informação divergente, favor detalhá-la nos comentários para que a equipe de Controles Internos possa avaliar e ajustar o que for necessário.	Sim / Não / N/A Comentário obrigatório para as respostas "Não" e "N/A".
Estimular o dono do controle a avaliar a eficiência do controle.	Existe outro modo mais eficiente de executar o controle do que aquele descrito na "Matriz de Riscos e Controles"? Caso exista, favor detalhá-lo nos comentários para que a equipe de Controles Internos possa avaliar e ajustar o que for necessário.	Sim / Não / N/A Comentário obrigatório para as respostas "Sim" e "N/A".
Estimular o monitoramento dos planos de ação identificados em CSA anteriores.	Há algum ponto de controle em aberto notificado para este controle? Caso positivo, favor descrever o andamento do plano de remediação e o prazo previsto para conclusão.	Sim / Não / N/A Comentário obrigatório para as respostas "Sim" e "N/A".
Estimular o dono do controle a relacionar os desvios identificados.	Você teve algum problema na execução deste controle para o período que está sendo avaliado? Caso positivo, favor descrever o andamento do plano de remediação e o prazo previsto para conclusão.	Sim / Não / N/A Comentário obrigatório para as respostas "Sim" e "N/A".
Estimular o dono do controle a sugerir inclusão e/ou exclusão de controles.	O risco descrito na "Matriz de Riscos e Controles" está sendo mitigado por este controle? Caso não esteja, favor descrever o motivo e sua sugestão de melhoria, para que a área de Controles Internos possa avaliar e ajustar o que for necessário.	Sim / Não / N/A Comentário obrigatório para as respostas "Não" e "N/A".
Estimular o dono do controle a avaliar a mitigação do risco.		

FONTE: Elaborado pela autora (2020)

Para encerrar o processo de *Control Self-Assessment*, o usuário precisa definir a classificação de efetividade de cada controle. Caso o controle seja considerado como

suficiente ou efetivo pelo usuário dono do controle, este deve selecionar esta opção e incluir os comentários e as evidências que corroborem com a classificação positiva. Entretanto, caso o controle seja classificado como inefetivo ou insuficiente, vale destacar os comentários e evidências aplicáveis, a ferramenta utilizada para realizar a autoavaliação deve direcionar o usuário para a criação de um plano de ação, permitindo a formalização das ações necessárias para correção dos desvios relatados.

QUADRO 5 – CLASSIFICAÇÃO DE EFETIVIDADE NO CSA

Pergunta	Resposta	Tarefa adicional
Na sua percepção, qual é a classificação de efetividade do controle avaliado?	Controle considerado como efetivo Controle considerado como suficiente	Obrigatório incluir comentário justificando a resposta e as evidências aplicáveis.
	Controle considerado como inefetivo Controle considerado como insuficiente	Obrigatório incluir comentário justificando a resposta, incluir as evidências aplicáveis e criar plano de ação para tratativa do desvio.

FONTE: Elaborado pela autora (2020)

Vale lembrar que empresas multinacionais possuem filiais em diversos países e muitas vezes conta com profissionais expatriados trabalhando em países diferentes de sua origem. Assim, é importante que o questionário do *Control Self-Assessment* seja padronizado na língua definida como padrão pela empresa, muitas vezes sendo definido o inglês como língua padrão e obrigatória para formalização deste processo por todos os usuários da empresa.

4.4 PLANO DE REMEDIAÇÃO

Após o término da etapa de autoavaliação, tanto a primeira quanto a segunda linha de defesa, possuem o conhecimento dos controles que foram considerados como inefetivos. Para estes controles, os usuários donos pelo controle possuem a autonomia para definir os planos de remediação necessários para mitigar os riscos descobertos dentro do próprio processo de *Control Self-Assessment*.

A implementação das mudanças necessárias é um processo subsequente ao CSA, e dependendo do desvio identificado, as ações podem requerer desde atividades simples e rápidas, como mudanças nos procedimentos da área ou estabelecimento de

novas políticas, até ações mais complexas e demoradas, que podem envolver investimentos financeiros e mudanças sistêmicas.

É importante destacar que a responsabilidade pela efetividade de um controle é do departamento que o executa (dono do controle), bem como a definição e implementação dos planos de remediação propostos.

4.4.1 Critérios para definição de um plano de remediação efetivo

A definição de um plano de ação deve ser realizada pela área dona do controle e obrigatoriamente deve conter algumas informações mínimas para que as ações possam ser colocadas em prática de forma adequada. As principais informações que devem ser apresentadas em um plano de ação são: a descrição das ações práticas a serem realizadas, o usuário responsável por tais ações e o prazo previsto para implementação de todas as ações desenhadas.

Para a realização de um plano de ação mais robusto e efetivo, pode-se utilizar uma ferramenta chamada de 5W2H. Esta ferramenta consiste basicamente em uma *checklist* de atividades, prazos, responsabilidades e informações adicionais para implementação de um projeto ou plano de ação. Em resumo, a ferramenta permite definir de forma objetiva o que será feito, porque, onde, quem irá fazer, quando será feito, como e quanto custará. Em resumo, a sigla 5W2H é formada pelas iniciais, em inglês, de sete diretrizes que, quando bem estabelecidas, eliminam quaisquer dúvidas que possam aparecer ao longo de um processo ou de uma atividade. São elas:

Os 5W:

What (o que será feito?)

Why (por que será feito?)

Where (onde será feito?)

When (quando será feito?)

Who (por quem será feito?)

Os 2H:

How (como será feito?)

How much (quanto vai custar?)

A seguir, o quadro abaixo exemplifica a criação de um plano de ação:

QUADRO 6 – PLANO DE REMEDIAÇÃO EXEMPLIFICADO

Controle	What (O que)	Why (Por que)	Where (Onde)	When (Quando)	Who (Quem)	How (Como)	How much (Quanto)
C.2	Implementar uma revisão de acessos ao sistema de Compras.	Assegurar o acesso restrito a transações críticas de Compras.	Depart. Compras na Filial de Curitiba.	Implementação até 31/12/XX.	User Y	Revisão mensal de acessos ao sistema de Compras. Acessos indevidos serão removidos.	R\$ 0,00

FONTE: Elaborado pela autora (2020)

É interessante que dentro da ferramenta utilizada para a gestão dos planos de ações, seja incluída uma opção de percentual de conclusão do plano de ação, que possibilite o usuário responsável ir monitorando e atualizando o andamento das ações, com percentuais que variem de 0% a 100%. Assim, tanto o departamento dono do controle quanto o departamento de Controles Internos podem acompanhar a evolução do plano de remediação e antecipar eventuais problemas de cronograma.

Uma vez que o plano de remediação foi estabelecido, as ações devem ser implementadas por seus responsáveis, para assegurar que no momento da reavaliação do controle, os mesmos estejam classificados novamente como efetivos/suficiente. Caso o departamento responsável identifique a necessidade de alteração do plano de remediação estipulado, em decorrência de fatores não identificados anteriormente, este departamento deve procurar o suporte da segunda linha de defesa, ou seja, o departamento de Controles Internos, para que em conjunto, possam definir a melhor alternativa para cada caso.

4.5 MONITORAMENTO E REPORTE DO *CONTROL SELF-ASSESSMENT*

O departamento de Controles Internos é o responsável pela coordenação e monitoramento da execução do *Control Self-Assessment* por todos os demais

departamentos da empresa. Este monitoramento inclui tanto o monitoramento do atendimento dos prazos estabelecidos quanto também dos resultados obtidos na autoavaliação.

O não cumprimento dos prazos poderá acarretar em algum tipo de penalização para o departamento em atraso, se assim for definido pela empresa. Outro desdobramento que pode ocorrer é a comunicação dos atrasos para a alta administração, para que o tema seja uma determinação *top down* a ser priorizada. Estes tipos de efeitos colaterais não são desejáveis, e é sempre importante que em casos de atrasos justificáveis, o próprio departamento procure a área de Controles Internos para explicar a situação e permitir que em conjunto, seja definida a melhor alternativa para cada caso.

Quanto ao monitoramento e reporte dos resultados do *Control Self-Assessment*, a área de Controles Internos deve realizar a comunicação dos resultados obtidos no CSA para cada departamento envolvido no processo de autoavaliação e também para a alta administração da empresa. Nos casos de empresas multinacionais em que o CSA local é monitorado pelo departamento de Controles Internos de cada filial, existe também a necessidade de reporte dos resultados para o departamento de Controles Internos alocado na Matriz da empresa. Nestes casos, a matriz poderá comparar os resultados das filiais, e sugerir melhorias e *benchmarking* entre as filiais, caso identifique controles similares com resultados muito discrepantes.

4.6 FATORES CRÍTICOS PARA IMPLEMENTAÇÃO DO *CONTROL SELF-ASSESSMENT*

Toda implementação de uma nova metodologia possui alguns fatores críticos de sucesso que devem ser observados e entendidos antes mesmo do início do processo de implementação. Caso estes fatores sejam negligenciados, a organização corre o risco de não obter sucesso em seu projeto.

Todo processo dentro de uma organização é dependente das ações das pessoas que trabalham nesta organização. E para a implementação da metodologia de *Control Self-Assessment* não é diferente, uma vez que demanda o envolvimento de pessoas certas e comprometidas na organização para apoiar, promover e executar o processo de

CSA. Neste sentido, é fundamental também o apoio e o exemplo da alta administração, que estimule uma cultura de Controles Internos voltada para a melhoria contínua dos processos, com a visão para mitigação de riscos. Adicionalmente, é fundamental que sejam alocados profissionais qualificados para a gestão do processo, tanto na equipe de Controles Internos (segunda linha de defesa), quando nas áreas gestoras dos riscos (primeira linha de defesa). É importante que ambas as áreas entendam o objetivo e os benefícios do *Control Self-Assessment*, e que realizem análises verdadeiras do processo, sem medo de repreensão em casos de inefetividade. Caso contrário, o processo de autoavaliação acaba ocorrendo apenas de maneira pró forma para cumprimento de mais uma tarefa, e perde o seu significado e objetividade.

Outro fator crítico de sucesso que deve ser observado é a alocação de tempo e recursos suficientes para preparar e realizar o *Control Self-Assessment* de forma adequada. Este critério engloba desde o investimento em equipe e *softwares*, como também a realização de treinamentos recorrentes.

Por fim, é importante observar ainda um *design* adequado de *Control Self-Assessment* estruturado para a sua organização, ou seja, a definição de quantidade de controles a serem avaliados, a quantidade e complexidades das perguntas inseridas no questionário e a frequência de realização do CSA. É importante definir uma estrutura flexível e adaptada à realidade da empresa, evitando a criação de tarefas excessivamente confusas e que conflitem com as demais entregas das áreas da organização.

4.7 BENEFÍCIOS DO CONTROL SELF-ASSESSMENT

A implementação de um processo de *Control Self-Assessment* pode trazer inúmeros benefícios para a organização, em especial as empresas multinacionais que possuem maior descentralização e processos distintos. Os benefícios para a alta administração, que passa a compartilhar de maneira formal a responsabilidade pela conformidade dos processos com as demais áreas, a própria área de Controles Internos (segunda linha de defesa) e toda a primeira a linha de defesa passam a ter mais visibilidade e recursos para atuar nos processos chaves e nos processos não adequados.

A equipe de Auditoria também pode se beneficiar de forma indireta com este processo, permitindo avaliar o risco das empresas que possuem um programa de *Control Self-Assessment* como um risco menor em relação as empresas que não possuem este tipo de governança.

Dentre os principais benefícios da implementação de um programa de *Control Self-Assessment*, podem ser destacados:

- a) O entendimento claro e compartilhado das principais atividades e objetivos de cada processo;
- b) Conscientização aprimorada dos riscos e controles entre a gerência e a equipe;
- c) Abordagem flexível e estruturada para melhorar o ambiente de controles interno da organização;
- d) Maior responsabilização por riscos e controles pela primeira linha de defesa;
- e) Melhores práticas e oportunidades para melhorar o desempenho dos negócios;
- f) Padronização de avaliação de risco e controles nas diversas localidades de uma empresa multinacional;
- g) Maior facilidade de *benchmark* de processos e controles de funções executadas em diferentes locais;
- h) Apoio a alta administração no cumprimento de suas responsabilidades de governança corporativa;
- i) Redução no tempo e no esforço necessários para os auditores internos coletarem informações de controles chaves.

Os benefícios citados podem ser percebidos logo após a implementação da metodologia de *Control Self-Assessment*, ou podem ser percebidos à medida que o processo de autoavaliação vai amadurecendo, o que pode não ser tão rápido quanto esperado, mas com a certeza que trará bons frutos para o sucesso da organização.

5. CONSIDERAÇÃO FINAIS

O objetivo da pesquisa, como exposto na seção 1, foi descrever uma proposta de aplicação da metodologia de *Control Self-Assessment* para o ambiente de Controles Internos em uma empresa multinacional. O referencial teórico deste estudo permitiu a ampliação do conhecimento e da visão crítica a respeito de termos e conceitos relacionados ao tema do trabalho, permitindo assim, um melhor desenvolvimento da proposta central do estudo.

Sintetizando os objetivos alcançados no estudo, foi possível observar as etapas necessárias para a implementação da metodologia de *Control Self-Assessment* em uma empresa multinacional. Para iniciar o processo de implementação, o mapeamento dos processos e a definição da Matriz de Riscos e Controles possuem papel fundamental para definição do escopo do *Control Self-Assessment*. Ao definir como os controles devem ser avaliados, se faz necessário também definir os usuários chaves responsáveis pela autoavaliação, para que o resultado final agregue o valor esperado para a organização. Por fim, durante o processo de implementação da metodologia, se faz necessário definir quais aspectos devem ser avaliados pelas áreas de negócios, para a definição de um questionário que reflita a realidade da companhia, além de definir uma frequência de execução do CSA.

Após a execução das etapas de implementação, é fundamental que a organização implemente processos que garantam a manutenção da metodologia de *Control Self-Assessment*. Para isso, a criação de planos de ação e a posterior implementação das ações desenhadas são de extrema importância para a manutenção e efetividade do processo de *Control Self-Assessment*. Vale ainda ressaltar a importância do monitoramento e do reporte dos resultados obtidos para a alta administração, que possui um papel fundamental na gestão de riscos e cultura de controles internos.

Além das contribuições e conclusões citadas acima, também foi possível demonstrar as diferenças de papéis e responsabilidades das três linhas de defesa dentro da empresa para a aplicação da metodologia de *Control Self-Assessment*. Foi observado que para esta metodologia, a primeira e segunda linha de defesa são mais envolvidas, e a importância de interação entre estes dois grupos. Foi observado também que a

implementação da metodologia contribui para aumentar a visibilidade e os recursos para que estas áreas atuem nos processos chaves e nos processos não adequados, além de contribuir para a conscientização e valorização da cultura de controles internos dentro da empresa.

Considerando todos os aspectos expostos acima, pode-se afirmar que este trabalho alcançou o objetivo proposto. Como sugestão de novos estudos a serem realizados, recomenda-se a realização de estudos com viés de estudo de caso envolvendo a implementação da proposta apresentada, com a finalidade de avaliar os benefícios e as dificuldades enfrentadas, bem como complementar alguma etapa ou informação relevante para o tema.

REFERÊNCIAS

- AICPA - *American Institute of Certified Public Accountants*. **SAS Statement on Auditing Procedures n.29**. Disponível na internet via endereço: <www.aicpa.org> Acesso em 06 de julho de 2019.
- ANDRADE, M. M. **Como preparar trabalhos para cursos de pós-graduação: noções práticas**. 5. Ed. São Paulo: Atlas, 2002.
- ASSI, M. **Gestão de riscos com controles internos**. 1 ed. São Paulo: Saint Paul Editora, 2012.
- ATTIE, W. **Auditoria – Conceitos e aplicações**. São Paulo: Atlas, 1998.
- BORDIN, P.; SARAIVA, C. J., 2005. Disponível na internet via endereço: <https://periodicos.ufsm.br/contabilidade/article/view/200/3725>. Acesso em 01 de março de 2020.
- CHAMPLAIN, J. J.; **Auditing Information Systems, Second Edition** United States: John Wiley & Sons, Inc., 2003.
- CHIZZOTTI, A. **Pesquisa em ciências humanas e sociais**. 2 ed. São Paulo: Cortez, 1995.
- Committee of Sponsoring Organizations of the Treadway Commission (COSO). **Internal Control — Integrated Framework: Executive Summary, 2013**. Disponível em: <http://www.coso.org/IC.htm>. Acesso em 18 de março de 2020.
- DIAS, S. V. S. **Manual de Controles Internos**. São Paulo: Editora Atlas, 2010.
- FILHO, A. R.; JACQUES, E.A.; MARIAN, P. D., 2005. Disponível na internet via endereço: <https://periodicos.ufsm.br/sociaisehumanas/article/view/1395/816>. Acesso em 08 de março de 2020.
- GIL, A. C. **Como elaborar projetos de Pesquisa**. São Paulo: Atlas, 2009.
- GIL, A. C. **Métodos e técnicas de pesquisa social**. 5 ed. São Paulo: Atlas, 1999.
- GIL, A. C; ARIMA C. H.; Nakamura W. T. **Gestão: controle interno, risco e auditoria**. 1 ed. São Paulo: Editora Saraiva, 2013.
- IBGC – Instituto Brasileiro de Governança Corporativa. **Guia de Orientação para Gerenciamento de Riscos Corporativos, 2007**. Disponível na internet via endereço:[https://conhecimento.ibgc.org.br/Lists/Publicacoes/Attachments/22121/Orienta%
%c3%a7%c3%b5es%20sobre%20Risco%20cad3.pdf](https://conhecimento.ibgc.org.br/Lists/Publicacoes/Attachments/22121/Orienta%c3%a7%c3%b5es%20sobre%20Risco%20cad3.pdf)> Acesso em 28 de março de 2020.

IIA - Institute of Internal Auditors. **The Three lines of defense in effective Risk Management and Control, 2013.** Disponível na internet via endereço: <https://na.theiia.org/standards-guidance/Public%20Documents/PP%20The%20Three%20Lines%20of%20Defense%20in%20Effective%20Risk%20Management%20and%20Control.pdf> Acesso em 06 de julho de 2019.

JOSEPH, G. W.; ENGLE, T, J., 2001. Disponível na internet via endereço: <http://archives.cpajournal.com/2001/0800/dept/d084601.htm>. Acesso em 15 de março de 2020.

KPMG. **A practical view on SAP Process Control, 2017.** Disponível na internet via endereço: <https://www.compact.nl/en/articles/a-practical-view-on-sap-process-control/> Acesso em 01 de maio de 2020.

MOELLER, R. R.; **Sarbanes-Oxley and the new internal auditing rules.** United States: John Wiley & Sons, Inc., 2004.

NBC - Norma Brasileira de Contabilidade. Disponível na internet via endereço: http://www1.cfc.org.br/sisweb/sre/detalhes_sre.aspx?codigo=2008/001135. Acesso em 07 de julho de 2019.

OLIVEIRA, L. M.; PEREZ Jr. C. H.; SILVA, C. A. S. **Controladoria Estratégica: 5ª ed.** São Paulo: Atlas, 2009.

PADOVESE, C. L. **Controladoria estratégica e operacional.** 1 ed. São Paulo. 2005.

PAULO, W. L.; FERNANDES, F. C.; RODRIGUES, L. G. B.; EIDIT, J., 2007. Disponível na internet via endereço: http://www.scielo.br/scielo.php?pid=S1519-70772007000100005&script=sci_arttext. Acesso em 08 de março de 2020.

PEREIRA, A. N., 2008. Disponível na internet via endereço: <http://www.atena.org.br/revista/ojs-2.2.3-08/index.php/pensarcontabil/article/view/68/68>. Acesso em 08 de março de 2020.

RAUPP, F. M.; BEUREN, I. M. **Metodologia da pesquisa aplicável as Ciências Sociais. Como elaborar trabalhos monográficos em contabilidade: teoria e prática.** 2ª ed. São Paulo: Atlas, 2004.

SANTOS, I. E. **Manual de métodos e técnicas de pesquisa científica.** Niterói: Editora Impetus, 2009.

SIMMONS, M. R. **COSO: Committee of Sponsoring Organizations of the Treadway Commission Based Auditing.** Altamont Springs, Internal Auditor, 1997