Universidade de Brasília
Faculdade de Economia, Administração, Contabilidade e Gestão de Políticas Públicas
Departamento de Administração

FERNANDA MANCINI QUEIROZ

A GESTÃO DE RISCOS CORPORATIVOS E SUA IMPORTÂNCIA NA ADMINISTRAÇÃO PÚBLICA INDIRETA: A experiência da implantação da GRC por uma Autarquia Federal

Brasília – DF
2019

FERNANDA MANCINI QUEIROZ

A GESTÃO DE RISCOS CORPORATIVOS E SUA IMPORTÂNCIA NA ADMINISTRAÇÃO PÚBLICA INDIRETA: A experiência da implantação da GRC por uma Autarquia Federal

Monografia apresentada ao Departamento de Administração como requisito parcial à obtenção do título de Bacharel em Administração.

Professor Orientador: Dr., Roque Magno de Oliveira

Brasília – DF

2019

FERNANDA MANCINI QUEIROZ

A GESTÃO DE RISCOS CORPORATIVOS E SUA IMPORTÂNCIA NA ADMINISTRAÇÃO PÚBLICA INDIRETA: A experiência da implantação da GRC por uma Autarquia Federal

A Comissão Examinadora, abaixo identificada, aprova o Trabalho de Conclusão do Curso de Administração da Universidade de Brasília do (a) aluno (a)

Fernanda Mancini Queiroz

Dr., Roque Magno de Oliveira

Professor-Orientador

Me, Bárbara Novaes Medeiros
Professor-Examinador

Me, Marcos Alberto Dantas
Professor-Examinador

Brasília, 29 de maio de 2019

RESUMO

Os riscos permeiam todos os níveis de uma organização e, se não gerenciados ou controlados, podem resultar em impactos negativos no alcance de sua missão institucional. Desse modo, a Gestão de Riscos Corporativos (GRC) busca mitigar riscos por meio de controles apropriados e vem se transformando em uma estratégia de governança vital para as organizações públicas. Este trabalho teve por objetivo descrever o processo de implantação da GRC no Conselho Administrativo de Defesa Econômica (Cade) para servir como estudo de caso para outras organizações públicas, por meio de pesquisa documental de caráter qualitativo. A Política de Governança, Gestão de Integridade, Riscos e Controles da Gestão no âmbito do Cade é uma declaração das intenções e diretrizes gerais da autarquia relacionada a GRC que segue os modelos *Committee of Sponsoring Organizations of the Treadway Comission* (COSO) e *International Organization for Standardization* ISO 31000:2009 e inclui: metodologia de gestão de riscos, plano de riscos, capacitação continuada, normas, manuais e procedimentos e solução tecnológica, conforme determinado pela Instrução Normativa Conjunta Controladoria Geral da União e antigo Ministério do Planejamento, Orçamento e Gestão (CGU/MP) 01/2016. Essa Política busca fortalecer a governança, o cumprimento da missão e o alcance dos objetivos estratégicos, além de promover maior transparência e aprimorar o ambiente de controles internos da gestão do Cade.

Palavras-chave: Gestão de Riscos Corporativo. Governança Corporativa. Administração Pública Indireta.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

ABNT – Associação Brasileira de Normas Técnicas

Cade – Conselho Administrativo de Desenvolvimento Econômico

Cerisc – Comitê Executivo de Gestão de Riscos

CGU – Controladoria Geral da União

Corisc – Comitê de Governança, Riscos e Controles

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

DA – Diretoria Administrativa

DEE – Departamento de Estudos Econômicos

ERM – *Entreprise Risk Management*

GRC – Gestão de Riscos Corporativos

IN – Instrução Normativa

ISO – *International Organization for Standardization*

MGCR – Metodologia de Gerenciamento de Risco do Cade

MJ – Ministério da Justiça

MP – Ministério do Planejamento, Orçamento e Gestão

OE – Objetivos Estratégicos

PDTIC – Plano de Gestão de Tecnologia da Informação e Comunicação

PNPC – Programa Nacional de Proteção ao Conhecimento Sensível

ProCade – Procuradoria Federal Especializada junto ao Cade

RC – Risco de Controle

RI – Risco Inerente

RR – Risco Residual

SEI- Sistema Eletrônico de Informação

SG – Superintendência-Geral

TCU – Tribunal de Contas da União

TIC – Tecnologia da Informação e Comunicação

SUMÁRIO

1. INTRODUÇÃO

Quaisquer tipos de organizações públicas ou privadas enfrentam influências e fatores internos e externos que tornam incerto se elas alcançarão ou não seus objetivos. O efeito que essa incerteza tem sobre os objetivos da organização é chamado de risco (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2018). Desse modo, se considerarmos que todas as atividades de uma organização envolvem riscos, gerenciá-los faz parte da governança e liderança, e é fundamental para a maneira como a organização é gerenciada em cada nível. Assim, o presente capítulo apresenta os subtópicos: contextualização sobre o tema da gestão de riscos corporativos no Brasil; formulação do problema; objetivo geral; objetivos específicos; e por fim, justificativa do trabalho.

1.1. Contextualização

No Brasil, a temática de riscos vem adquirindo relevância crescente nos últimos anos tanto no campo da pesquisa acadêmica quanto no âmbito das políticas públicas (NOGUEIRA et al., 2014), visto que na contemporaneidade, o ato de enfrentar os riscos não é mais pura sorte, ou seja, ele tem o apoio da teoria da administração do risco. Dessa forma, na realidade de uma organização, cabe ao gestor saber gerir as incertezas para que seja realizada a melhor tomada de decisão para o benefício dela e das partes interessadas. A melhor forma de gerir riscos é com a da gestão de riscos corporativos (GRC), que é definido como processo de natureza permanente, estabelecido, direcionado e monitorado pela alta administração, que contempla as atividades de identificar, avaliar e gerenciar potenciais eventos que possam afetar a organização, destinado a fornecer segurança razoável quanto à realização de seus objetivos (BRASIL, 2017).

A fim de intensificar ações que promovam a melhoria da governança, da gestão de riscos e dos controles internos na administração pública, o Tribunal de Contas da União (TCU), desenhou, em 2012, após pesquisas e estudos, um indicador que avaliasse o nível de maturidade das instituições públicas no que se refere à implantação da gestão de riscos. Diante dos distintos graus de maturidade em gestão de riscos encontrados entre as dez agências reguladoras que participaram do levantamento, foi concluído que há um longo caminho de aprimoramento a ser percorrido para que essas apresentem uma gestão de riscos

compatível com as exigências de suas áreas de atuação (MARTINS, 2018).

Associado a isso, a Controladoria Geral da União (CGU) e o extinto Ministério do Planejamento, Orçamento e Gestão (atual Ministério da Economia) determinaram aos órgãos e entidades do Poder Executivo Federal, em 2016, a adoção de uma série de medidas para a sistematização de práticas relacionadas à gestão de riscos, controles internos e governança. Assim, no dia 1º de maio de 2016, foi publicada a Instrução Normativa Conjunta CGU/MP nº 01, que dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo Federal. Este marco regulatório impõe o dever de instituir, em até doze meses a contar da data de sua publicação, uma política de gestão de riscos. Ele também orienta os órgãos e as entidades públicas à estruturação de mecanismos de controles internos, gestão de riscos e governança e apresenta conceitos, princípios, objetivos e responsabilidades relacionados aos temas.

Dessa maneira, um ano após a publicação da IN nº 01/2016 e com o intuito de se empenhar para a implantação da gestão de riscos, o Cade publicou a Portaria nº 173/2017, que aprovou a Política de Gestão de Riscos, Governança, e Controles Internos no âmbito da autarquia com a finalidade de estabelecer os princípios, diretrizes e responsabilidades mínimas a serem observados e seguidos para a gestão de integridade, de riscos e de controles internos dos planos estratégicos, programas, projetos e processos do Cade. Ainda em 2017, foi publicado o Decreto nº 9.203, de 22 de novembro de 2017 que dispõe sobre a política de governança da administração pública federal direta, autárquica e fundacional, tendo como princípios, a governança pública, a capacidade de resposta, a integridade, a confiabilidade, a melhoria regulatória, a prestação de contas e responsabilidade e a transparência.

Em abril do ano seguinte, a CGU publicou a Portaria nº 1.089/2018 que estabelece orientações para que os órgãos e entidades da administração pública federal direta, autárquica e fundacional adotem procedimentos para a estruturação, a execução e o monitoramento de seus programas de integridade e dá outras providências, Assim, diante da necessidade de consolidar os aspectos referentes ao risco de integridade, que envolve, por exemplo, o desenvolvimento do código de conduta, do canal de denúncias, da transparência, do sistema de correição, à sistemática da gestão de risco da autarquia, em maio de 2018, foi publicada a Portaria nº 283/2018 que aprova a Política de Governança, Gestão de Integridade,

Riscos e Controles da Gestão no âmbito do Cade e revogada a Portaria anterior.

1.2. Formulação do Problema

O Cade como integrante da administração pública indireta desempenha atividade administrativa típica de estado (ROSA, 2004) tendo como missão zelar pela livre concorrência no mercado, sendo a entidade responsável, no âmbito do Poder Executivo, não só por investigar e decidir, em última instância, sobre a matéria concorrencial, como também fomentar e disseminar a cultura da livre concorrência no país (CADE, 2016).

Para cumprir sua missão institucional, o Cade, assim como toda organização, está vulnerável a riscos os quais podem impactar no alcance dos seus objetivos (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2018). Nesse ponto, um aspecto essencial a ser observado é que no setor público há uma preocupação central com o dever de cuidar do bem público. Desse modo, os riscos sempre devem ser gerenciados de modo a manter o interesse público em primeiro plano, e a tomada de decisão acerca de como equacionar os benefícios e perdas potenciais deve ser o principal aspecto da gestão de riscos nas organizações (Ávila, 2013). Nesse aspecto, a implantação da gestão de riscos corporativos (GRC) constitui uma importante ferramenta estratégica da governança corporativa, uma vez que auxilia a tomada de decisão e possibilita que a organização, por exemplo, aumente a probabilidade de atingir seus objetivos, melhore a governança e identifique oportunidades e ameaças (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2018). Desse modo, este trabalho buscou esclarecer: como o Cade estruturou a implantação da GRC e qual a sua importância para o cumprimento da sua missão institucional?

1.3. Objetivo Geral

Analisar o processo de implantação da Gestão de Riscos Corporativos no Conselho Administrativo de Defesa Econômica – Cade, de forma que possa ser utilizado como estudo de caso para outras organizações.

1.4. Objetivos Específicos

A fim de alcançar o objetivo geral, foram definidos objetivos específicos:

- Estudar e explorar as metodologias ISO 31000:2009 e COSO utilizadas

como bases delineadoras para a implementação da gestão de riscos no Cade;

- Descrever as normas legais que tornaram obrigatória a implementação da gestão de riscos na administração pública brasileira;
- Mapear estudos de caso sobre implementação da gestão de riscos nas organizações públicas e privadas e comparar com a experiência do Cade.

1.5. Justificativa

O risco é inerente à atividade humana. Toda organização, seja pública ou privada, enfrenta influências e fatores internos e externos que a insere em um ambiente de incerteza, tornando-a vulnerável ao risco. O efeito que essa incerteza tem sobre o alcance dos seus objetivos é chamado de risco e cabe a organização encontrar soluções para lidar com esse desafio (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2009).

Segundo a norma ISO 31004:2015, a gestão de riscos é parte integrante de todos os processos organizacionais. Desse modo, uma gestão eficaz de risco busca obter impactos positivos para a organização e, assim, dar continuidade no negócio ou serviço.

A gestão de riscos corporativos (GRC) na administração pública se tornou uma ferramenta estratégica importante para a eficiência do serviço público nos últimos anos. Ressalta-se que para muitas instituições públicas, esse é, ainda, um tema novo e, portanto, um desafio (MATINS et al., 2018). Nesse aspecto, a Instrução Normativa MP/CGU Nº 01/2016, que dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo Federal, é um importante marco normativo no que concerne à implementação da gestão de riscos no país, visto que traz conceitos e elementos que orientam os gestores na elaboração de suas políticas, a exemplo do Conselho Administrativo de Defesa Econômica (Cade), objeto deste estudo que, numa demonstração do seu compromisso institucional na implementação da gestão de riscos, publicou a Portaria nº 173/2017, que aprovou a Política de Gestão de Riscos, Governança, e Controles Internos. Em maio 2018 esta Portaria foi revogada pela Portaria nº 283/2018, que incluiu a gestão de integridade à referida política.

Desta forma, este estudo descreve o processo de implantação da gestão de

riscos no Cade com o intuito de instigar o debate sobre questões afetas ao tema e contribuir para o conhecimento científico acerca deste processo no âmbito da administração pública, podendo assim constituir em um exemplo factível para o setor.

2. REVISÃO TEÓRICA

Para a fundamentação teórica deste estudo, o capítulo a seguir reúne um conjunto de informações que discorrem sobre a temática gestão de riscos corporativos de modo a tornar possível a total compreensão sobre o assunto no contexto proposto. Para tanto, foi feito um levantamento de referências bibliográficas que subsidiaram a definição e discussão sobre riscos, gestão de riscos, governança corporativa e as metodologias de gestão de riscos, a saber a norma ISO 31000:2009 da *International Organization for Standardization* e Gestão de Risco Empresarial ERM*: Enterprise Risk Management Framework* (COSO, 2007).

2.1. Governança Corporativa

A partir do início dos anos 1980, principalmente nos Estados Unidos, surgiu a governança corporativa, resultado de abusos de dirigentes de empresas. Acionistas, administradores e demais partes interessadas nos negócios, perceberam a necessidade de haver mais estudos e pesquisas no âmbito acadêmico, empresarial e governamental para que houvessem mudanças na legislação, criação de procedimentos e práticas de gestão e maior cobrança dos administradores na condução dos negócios das empresas (AZEVEDO et al., 2017).

De acordo com Gonzalez (2012, p. 25), a Governança corporativa é definida como:

> [...] todo o processo de gestão e monitoramento desta que leva em consideração os princípios da responsabilidade corporativa (fiscal, social, trabalhista, comunitária, ambiental, societária), interagindo com o ambiente e os públicos estratégicos, os chamados *stakeholders*, em busca da sustentabilidade para ser longeva. (GONZALEZ, 2012, p. 25).

Ou seja, a governança corporativa dá suporte para o processo de tomada de decisão da organização.

Segundo Azevedo et al. (2017), a governança corporativa procura estabelecer atribuições e responsabilidades em uma estrutura adequada para garantir melhores práticas de gestão nas organizações; é sustentada em quatro princípios fundamentais, que são: transparência, integridade/equidade, prestação de contas e *compliance*. Ainda de acordo com os autores, a transparência está intimamente relacionada com a prestação de informações aos acionistas, investidores e mercado em geral e deve deixar clara a verdadeira situação da sociedade e apontar os rumos que ela deve tomar. Já a integridade está associada ao respeito, aos direitos e

interesses dos minoritários e ao efetivo cumprimento das leis e do estatuto, sem perder de vista a lealdade dos administradores para com os interesses da companhia. *Compliance,* por sua vez, significa cumprir leis, diretrizes, regulamentos internos e externos para mitigar risco atrelado à reputação de uma empresa.

No setor público, a governança segue os mesmos princípios da governança empresarial, porém na administração pública destaca-se a obrigatoriedade da prestação de contas (*accountability*) quanto à aplicação e a gestão dos recursos públicos (ÁVILA, 2013).

Entende-se *accountability* como um conjunto de procedimentos adotados pelas organizações públicas e pelos indivíduos que as integram, que evidenciam a responsabilidade com a ética e remete à obrigação, à transparência nas tomadas de decisões e ações implementadas (BRASIL, 2016). A aplicação do *accountability* no setor público é mais complexa e desafiadora do que no setor privado, uma vez que na esfera pública o administrador só pode agir dentro daquilo que está previsto e autorizado por lei.

É fundamental acrescentar que, em se tratando da administração pública, questões de governança estão associadas ao nível macro, e compreendem mecanismos de liderança, estratégia e controle colocados em prática para avaliar, direcionar e monitorar a atuação da gestão, a fim de conduzir políticas públicas e prestar serviços de interesse da sociedade. Desse modo, o mecanismo de governança mais apropriado na atualidade é o processo de gestão de riscos corporativos, uma vez que permite tratar com eficiência as incertezas, quer seja pelo aproveitamento das oportunidades, quer seja pela redução da probabilidade e/ou impacto de eventos negativos, a fim de melhorar a capacidade de gerar valor e de fornecer uma base sólida e segura para a tomada de decisão, além de aumentar a probabilidade de atingir os objetivos da organização (MARTINS, 2018).

Como abordado anteriormente, ao considerar que a governança corporativa trata de mecanismos que visam dar suporte ao processo de tomada de decisão, de modo a maximizar a geração de valor para o setor público, compreende-se que a adoção desta prática envolve não apenas benefícios, mas inclusive custos (DOMINGUES, 2016). Nessa linha, segundo Ramos (2015, apud MARTINS et al., 2018) o fator crítico de sucesso da implementação de um processo eficaz e eficiente de gestão de riscos consiste na definição e a adoção simultânea de princípios de governança claros e transparentes, além do desenho de regras de controles internos

de gestão consolidados em forma de política. Neste contexto, percebe-se a importância de que uma boa gestão de riscos é, na verdade, uma necessidade em uma organização, uma vez que traz benefícios como diminuição dos custos de atividades incertas e aumento dos benefícios sociais e econômicos (ÁVILA, 2013).

2.2. A Gestão de Riscos Corporativos

Para este estudo é pertinente abordar o entendimento sobre o risco de maneira genérica, visto que toda organização, seja pública ou privada, pois depende da tomada de decisão diária para a sua subsistência, o que a torna vulnerável às diferentes possibilidades de riscos. Segundo Daft (2005, p. 198), risco significa “uma decisão com metas bem definidas e boas informações disponíveis, mas mesmo assim com resultados futuros associados a cada alternativa, sujeitos a mudança”. Já a norma ISO 31000:2009 define risco como o efeito da incerteza nos objetivos, onde um efeito é um desvio em relação ao esperado -positivo e/ou negativo. Logo, a “incerteza surge quando não há informações suficientes para os gerentes serem precisos sobre as alternativas e os eventos futuros ou para estimarem seus riscos” (DAFT, 2005, p. 198). A incerteza, ou o risco, pode mudar ao longo do tempo devido a, por exemplo, competição, tendências, novas informações e mudanças nos fatores subjacentes (BRASIL, 2015). Segundo Guimarães et al., (2009), risco não é necessariamente algo negativo, uma vez que um resultado inesperado pode produzir impactos positivos, ou seja, o risco pode gerar oportunidades ou benefícios para a organização. Ávila (2013) vai em acordo com essa ideia ao afirmar que risco:

> [...] é a possibilidade de que aquilo que é esperado não aconteça, o risco não implicará necessariamente em algo indesejável, já que os resultados entorno do esperado podem apresentar tanto benefícios como malefícios, dependendo se resultado estiver abaixo ou acima do esperado. (ÁVILA, 2016, p. 4).

Notadamente, o risco possui características positivas e negativas, e pode afetar diretamente o bom funcionamento das instituições a depender da forma como ele for gerenciado. Portanto, é fundamental fazer uma análise contextual para cada situação correlacionada com determinado risco e considerar a existência de seus diversos tipos (SENA, 2016).

Uma vez identificado o tipo de risco, mensurar e calcular a probabilidade de ele acontecer é essencial para auxiliar no processo de tomada de decisão da organização, visto que qualquer oportunidade que surge pode acarretar novos riscos

para a mesma. Assim, é necessário ter informações suficientes que permitam estimar a probabilidade de um resultado bem-sucedido para cada alternativa (DAFT, 2005). Dependendo do resultado encontrado, a análise do risco pode ser qualitativa, semiquantitativa, quantitativa ou uma combinação delas (BRASIL, 2017). Quando a análise é quantitativa, Portela (2014) ressalta que, apesar dos esforços em prover números para a tomada de decisão, a percepção do risco e a percepção do que é aceitável não são totalmente exatas.

As organizações enfrentam incertezas todos os dias e encontrar soluções para a tomada de decisão eficaz é um desafio rotineiro. Sendo assim, cabe aos gestores saber lidar com o risco, uma vez que este é um indicativo de maturidade tanto para o mundo empresarial quanto em cenários políticos (ÁVILA, 2013). A partir dessa afirmativa, percebe-se que a melhor forma de lidar com o risco é a implementação da gestão de riscos na organização. Segundo Destro (2014, p 53), “faz parte da gestão de riscos a elaboração de um estudo profundo de todos os problemas que podem acometer a organização, desde os mais óbvios aos mais distantes da realidade”. De acordo com a autora, após analisar este estudo, é possível consertar tanto os erros de gestão quanto os operacionais.

Para Guimarães et al. (2009), o GRC tem dois objetivos principais: a mitigação dos efeitos dos riscos e a minimização dos custos. Destro (2014) explica que a minimização dos custos ocorre porque a organização consegue poupar recursos que seriam gastos para conter crises, recuperar a imagem e a reputação com o público e salvar o negócio. Logo, os recursos destinados a gestão de riscos não são um desperdício, uma vez que evitam perdas muito maiores para a organização.

Já Portela (2014), afirma que o objetivo central do gerenciamento de riscos consiste em aceitar aqueles que são absolutamente necessários para a organização e compatíveis com as pessoas, com a sociedade e o meio ambiente em que se insere, ou seja, são riscos que precisam ser aceitos e enfrentados para a sobrevivência das partes envolvidas. O autor ainda conclui que gerenciar riscos se resume na decisão de aceitar ou recusar os riscos.

Muito presente no setor financeiro, nos desastres naturais e na segurança de trabalho, Braga (2017) afirma que o gerenciamento de riscos aplicado às políticas públicas entrou na pauta nacional com mais vigor no novo milênio. Segundo o autor, em tempos de crise fiscal e da necessidade de um Estado regule e conduza políticas

de forma efetiva, é necessário identificar os caminhos e contemplar as ameaças, tais como desperdícios e corrupção, e é a isso que a gestão de riscos e um bom sistema de controle interno se prestam, uma vez que, dentro do contexto atual de Estado, a gestão de riscos busca a entrega de serviços públicos de qualidade.

De acordo com Ávila (2013), em quase todos os casos, a gestão de riscos exige que os gestores públicos ponderem e avaliem entre os interesses conflitantes até identificarem uma solução ótima e aceitável. Essa solução quase sempre envolve opções políticas e não técnicas, no entanto, não podem se afastar do dever de cuidar do bem público, ou seja, devem sempre manter em primeiro plano o interesse público. De acordo com o artigo 37º da Constituição da República Federativa do Brasil de 1988, a administração pública deve obedecer a cinco princípios, quais sejam: a legalidade, a impessoalidade, a moralidade, a publicidade e a eficiência (BRASIL, 1988), ou seja, para o bom desempenho de suas atividades no setor público, o administrador só pode fazer o que a Lei autoriza (legalidade), deve atuar sempre em nome do interesse público (impessoalidade), trabalhar com bases éticas, lembrando que não pode ser limitada na distinção de bem ou mal, portanto, não deve visar apenas esses dois aspectos, adicionando a ideia de que o fim sempre será o bem comum (moralidade), além disso, todos os seus atos administrativos devem ser publicados (publicidade) e por fim, deve buscar o melhor resultado possível (eficiência) (ROSA, 2004). Logo, os riscos devem ser gerenciados de forma a manter a primazia do interesse público e para que isso aconteça, equacionar os benefícios e as perdas potenciais é o principal aspecto da gestão de riscos.

A gestão de riscos corporativos, além de auxiliar na tomada de decisão, contribui para assegurar comunicação eficaz entre as equipes de gestão, o cumprimento de leis e regulamentos, bem como evitar danos à reputação da organização e suas consequências (SANTOS, 2014). A comunicação deve ser realizada regularmente, pois pode ocorrer alteração nos riscos ou mudança no ambiente em que a organização está inserida.

Depreende-se que, ao implementar a gestão de riscos, a organização terá maior probabilidade de sucesso na identificação e controle da ocorrência e tratamento dos riscos de impacto potencialmente negativo e de tirar vantagens e oportunidades dos riscos potencialmente positivos (FREIRE, 2017).

Nesse aspecto, de acordo com o modelo COSO (2007), o gerenciamento de

riscos corporativos é definido como:

> [...] processo conduzido em uma organização pelo Conselho de Administração, pela diretoria executiva e pelos demais funcionários, aplicado no estabelecimento de estratégias formuladas para identificar, em toda a organização, eventos em potencial, capazes de afetar a referida organização, e administrar os riscos para mantê-los compatíveis com o seu apetite a risco e possibilitar garantia razoável de cumprimento dos objetivos da entidade. (*COSO*, 2007, p. 4).

As atividades da gestão de riscos consistem, na identificação, mensuração e controle dos riscos, e não à eliminação deles. Ou seja, o risco deve ser explorado de tal forma que traga benefícios para a organização.

O *Committee of Sponsoring Organizations of the Treadway Commission* (COSO) é uma entidade sem fins lucrativos, dedicada à melhoria dos relatórios financeiros por meio da ética, efetividade dos controles internos e governança corporativa (ÁVILA, 2013). Em 2001, o COSO iniciou um projeto para desenvolver uma estratégia de fácil utilização pelas organizações para avaliar e melhorar a gestão de riscos. Foi publicada, então, a tradução para o português da versão original em inglês da obra “Gerenciamento de Riscos Corporativos – Estrutura Integrada” elaborada pelo comitê com a colaboração da *PricewaterhouseCoopers* (COSO, 2007*)*.

Nessa publicação, o gerenciamento de riscos corporativos possibilita aos administradores tratar com eficácia as incertezas – que representam riscos e oportunidades – bem como os riscos e as oportunidades a elas associadas, a fim de melhorar a capacidade de gerar valor.

Ainda segundo essa obra, o gerenciamento de riscos corporativos tem por finalidade:

- Alinhar o apetite a risco com a estratégia adotada – os administradores avaliam o apetite a risco da organização ao analisar as estratégias, definindo os objetivos a elas relacionados e desenvolvendo mecanismos para gerenciar esses riscos;
- Fortalecer as decisões em resposta aos riscos – o gerenciamento de riscos corporativos possibilita o rigor na identificação e na seleção de alternativas de respostas aos riscos - como evitar, reduzir, compartilhar e aceitar os riscos;
- Reduzir as surpresas e prejuízos operacionais – as organizações adquirem melhor capacidade para identificar eventos em potencial e estabelecer respostas a estes, reduzindo surpresas e custos ou prejuízos associados;

- Identificar e administrar riscos múltiplos e entre empreendimentos – toda organização enfrenta uma gama de riscos que podem afetar diferentes áreas da organização. A gestão de riscos corporativos possibilita uma resposta eficaz a impactos inter-relacionados e, também, respostas integradas aos diversos riscos;
- Aproveitar oportunidades – pelo fato de considerar todos os eventos em potencial, a organização posiciona-se para identificar e aproveitar as oportunidades de forma proativa; e
- Otimizar o capital – a obtenção de informações adequadas a respeito de riscos possibilita à administração conduzir uma avaliação eficaz das necessidades de capital como um todo e aprimorar a alocação desse capital (COSO, 2007).

O gerenciamento de riscos corporativos é um processo contínuo e fluido que evita perigos e surpresas no percurso e contribui para que a organização atinja suas metas. É, também, um processo multidirecional e interativo segundo o qual quase todos os componentes influenciam os outros (COSO, 2007). Dessa forma, numa ótica tridimensional, o gerenciamento de riscos corporativos é representado por quatro categorias de objetivos na face superior, oito componentes inter-relacionados nas linhas horizontais da parte frontal, e, por fim, quatro unidades de uma organização na lateral do cubo.

Figura 1 - Visão tridimensional da metodologia COSO — ERM
Fonte: COSO, 2007

De acordo com a obra, alguns objetivos como manter uma reputação favorável tanto no segmento empresarial quantos com seus clientes, fornecer informações confiáveis às partes interessadas e operar em conformidade com as leis e a regulamentação, são comuns a todas as organizações. Dessa forma, conforme demonstrado na parte superior do cubo, são estabelecidas quatro categorias de objetivos para a organização:

- Estratégico – referem-se às metas no nível mais elevado. Alinham-se e fornecem apoio à missão da organização.
- Operacional – têm como meta a utilização eficaz e eficiente dos recursos.
- Comunicação – relacionados à confiabilidade dos relatórios.
- Conformidade – fundamentam-se no cumprimento das leis e dos regulamentos pertinentes.

A parte frontal do cubo indica os oito componentes que se originam com base no modo como a administração gerencia a organização, e que se integram ao processo de gestão, ou seja, esses componentes devem estar presentes e em funcionamento para que a gestão de riscos seja eficaz (SANTOS, 2018). Por fim, a terceira dimensão na lateral do cubo representa a organização e as unidades desta.

Adicionalmente, em 2009 foi lançada a norma ABNT NBR ISO 31000:2009 Gestão de Riscos – Princípios e Diretrizes. Esta norma internacional é específica sobre a gestão de riscos e fornece princípios e diretrizes para gerenciar qualquer tipo de risco de forma sistemática, transparente e confiável. Ela foi adotada como norma brasileira para a Gestão de Riscos, sendo traduzida para o português sem modificações da versão original em inglês (FREIRE, 2017), e traz vários elementos de uma estrutura para gerenciar riscos que podem ser aplicados em toda ou em parte de uma organização. Apesar dessa norma ter sido cancelada e substituída em 2018 pela ISO 31000:2018, neste trabalho, fez-se necessário descrever sobre a ISO 31000:2009, visto que o Cade, objeto do estudo, se baseou nesta norma para implantar sua política de gestão de riscos. Conforme demonstrado na figura 2, a ISO 31000:2009 é estruturada em três partes inter-relacionadas: princípios, estrutura e processo.

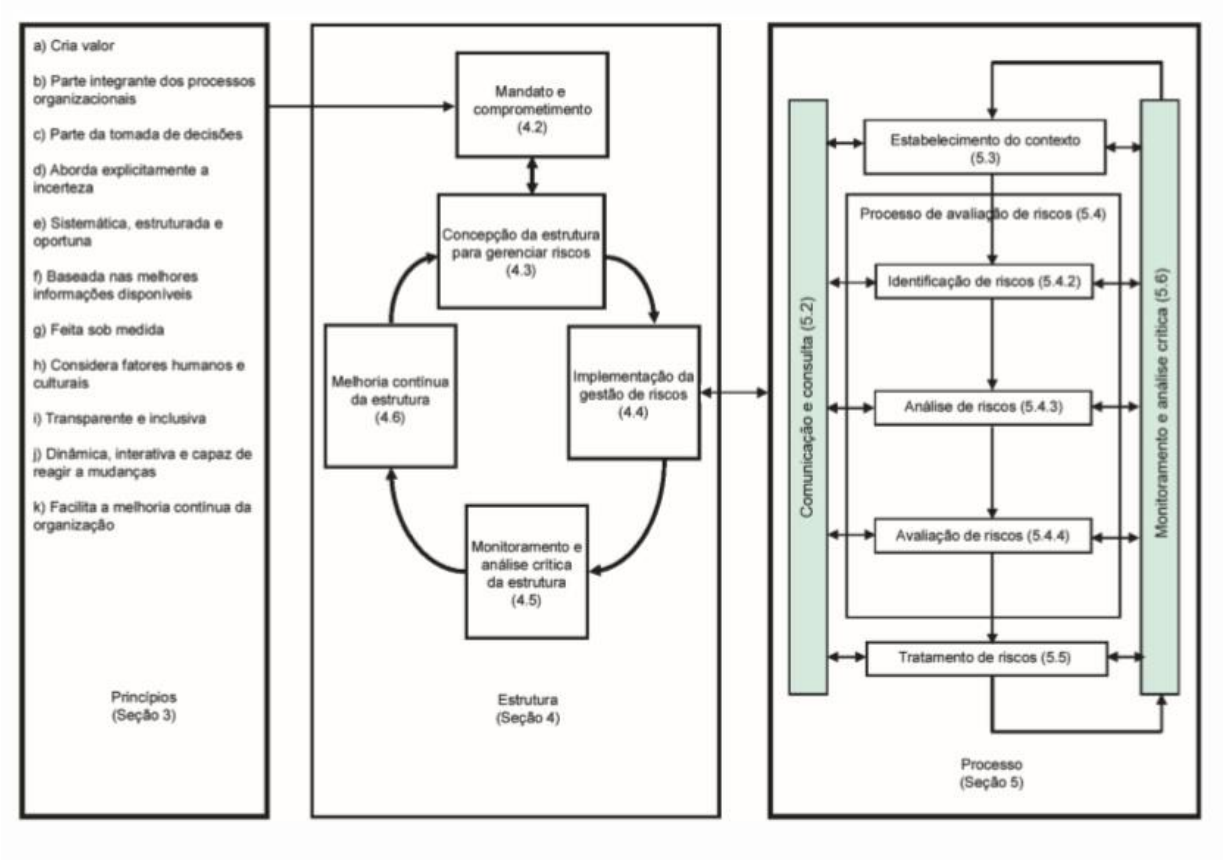

Figura 2 - ISO 31000:2009 - Relacionamento entre Princípios, Estrutura e Processo
Fonte: ABNT, 2009.

Apesar de cada organização ter suas peculiaridades, uma abordagem de implementação genérica e sistemática pode ser aplicável em todos os casos (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2015). Sendo assim, para que a implementação da gestão de riscos seja eficaz em uma organização, a norma estabelece 11 princípios que servem para informar e orientar sobre os aspectos da abordagem da organização para o gerenciamento de riscos e devem ser atendidos por todos os níveis da instituição, são eles:

- A gestão de riscos cria e gera valor;
- A gestão de riscos é parte integrante de todos os processos organizacionais;
- A gestão de riscos é parte da tomada de decisões;
- A gestão de riscos aborda explicitamente a incerteza;
- A gestão de riscos é sistemática, estruturada e oportuna;
- A gestão de riscos baseia-se nas melhores informações disponíveis;
- A gestão de riscos é feita sob medida;
- A gestão de riscos considera fatores humanos e culturais;

- A gestão de riscos é transparente e inclusiva;
- A gestão de riscos é dinâmica, interativa e capaz de reagir a mudanças;
- A gestão de riscos facilita a melhoria contínua da organização.

Além dos princípios, a norma recomenda que as organizações desenvolvam, implementem e melhorem continuamente a estrutura para integrar o processo de gerenciar riscos na governança, na estratégia e planejamento, nos processos, nas políticas, nos valores e cultura em toda a organização. A estrutura da gestão de riscos, segundo a ISO 31000:2009, é:

> [...] o conjunto de componentes que fornecem os fundamentos e os arranjos organizacionais para a concepção, implementação, monitoramento, análise crítica e melhoria contínua da gestão de riscos através de toda a organização (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2009, p 2).

Ou seja, a estrutura da gestão de riscos assegura que a informação sobre riscos provenientes desse processo seja adequadamente reportada e utilizada como base para as tomadas de decisões e a responsabilização em todos os níveis da organização. Além disso, as organizações devem adaptar os elementos da estrutura às suas necessidades específicas, uma vez que esta busca auxiliar a organização a integrar a gestão de riscos em seu sistema de gestão global.

Para a implementação da gestão de riscos, as organizações devem desenvolver atividades que consistem no estabelecimento do contexto, na identificação, na análise e avaliação dos riscos, no tratamento de riscos e monitoramento e análise crítica. Observa-se na Figura 2, que as atividades centrais do processo de gestão de riscos estão ligadas a comunicação e consulta o que indica a necessidade de que isso aconteça durante todas as fases do processo, uma vez que as partes interessadas devem ter acesso fácil as informações verdadeiras, pertinentes, exatas e compreensíveis (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2009).

Para o processo de gestão de riscos, a primeira etapa que a organização deve seguir é o estabelecimento do contexto, pois é a fase em que a organização articula seus objetivos e define seus parâmetros internos e externos a serem levados em consideração ao gerenciar riscos, além de estabelecer o escopo e os critérios de risco para o restante do processo.

A fase identificação de riscos é a etapa inicial de busca, descrição ou

mapeamento dos riscos. Nessa etapa é recomendável identificar as fontes de riscos, as áreas de impactos e eventos (FREIRE, 2017). A ISO 31000:2009 indica criar uma lista abrangente de riscos que possam impactar de alguma forma a realização dos objetivos da organização, uma vez que essa etapa pode envolver dados históricos, análises teóricas, opiniões de pessoas e especialistas e as necessidades das partes interessadas. Essa fase deve ser feita por pessoas diferentes, para evitar vícios e percepções por pontos de vista únicos (FREIRE, 2017).

A análise de riscos é a atividade de compreensão da natureza do risco e determinação do nível do risco, ou seja, aponta a magnitude do risco ou combinação de riscos, expressa em termos da combinação das consequências e de suas probabilidades (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2009). Essa etapa permite que os gestores verifiquem o nível do risco e encontrem soluções para os riscos de maior prioridade. De acordo com o Roteiro de Auditoria de Gestão de Riscos do Tribunal de Contas da União, o risco é uma função da probabilidade e do impacto, portanto, o nível de risco é expresso pela combinação da probabilidade de ocorrência do evento e de suas consequências, em termos da magnitude do impacto nos objetivos (BRASIL, 2017). Ainda segundo o Roteiro, foram definidos três tipos de riscos:

- Risco inerente (RI): nível de risco antes da consideração de qualquer ação de mitigação;
- Risco residual (RR): nível de risco depois da consideração das ações adotadas pela gestão (por exemplo, controles internos) para reduzir o risco inerente;
- Risco de controle (RC): consiste na possibilidade de que os controles adotados pela gestão não sejam eficazes para prevenir, detectar e permitir corrigir, em tempo hábil, a ocorrência de eventos que possam afetar adversamente a realização de objetivos.

Por fim, com base nos resultados da análise de riscos, a avaliação de riscos auxilia a tomada de decisão em relação àqueles que necessitam de tratamento e estabelece os riscos que terão prioridade para implementação do tratamento. Nessa etapa é importante definir qual o tratamento será dado ao risco, uma vez que a incerteza identificada pode ser uma oportunidade ou uma ameaça. De acordo com Santos (2014), as opções para o tratamento do risco podem incluir ações para: a) evitar o risco; b) remover a fonte de risco; c) alterar a probabilidade de ocorrer o

evento; d) alterar as consequências; e) compartilhar o risco; ou f) reter o risco. Além desses, a norma 31000:2009 acrescenta outra ação g) assumir ou aumentar o risco, a fim de buscar uma oportunidade.

Ademais, a norma ISO 31000:2009 aborda outras vantagens da gestão de riscos como encorajar uma gestão proativa, melhorar a identificação de oportunidades e ameaças, melhorar a governança e a confiança das partes interessadas, minimizar perdas, aumentar a resiliência da organização, entre outros.

Observa-se que a norma ISO 31000:2009 explica como gerenciar os riscos de forma eficaz, mas não aborda como integrar a gestão de riscos aos processos de gestão da organização. Essa lacuna é suprimida pela norma ABNT NBR ISO 31004:2015, que consiste em um relatório voltado para os tomadores de decisão e fornece orientações para que as organizações aumentem a eficácia dos seus esforços de gestão de riscos, pelo alinhamento com a ABNT NBR ISO 31000:2009 de forma contínua, dinâmica e interativa. Enquanto que na norma 31000:2009 descreve de forma sucinta os 11 princípios que a organização deve atender, a norma 31004:2015 avança ao descrever exemplos práticos para cada um desses princípios com a finalidade de fazer com que o gestor internalize esses princípios para colocá-los em prática na rotina da organização. Ressalta-se que no caso do setor público, os agentes públicos precisam enxergar a aplicabilidade da gestão de riscos e o grau de customização da ferramenta para que esta seja absorvida mais facilmente (BRAGA, 2018).

Tendo em vista que nesse estudo será realizada uma descrição das ações que o Conselho Administrativo de Defesa Econômica (Cade) realizou para implantar a gestão de riscos a partir da metodologia ISO 31000:2009, é de fundamental importância entender como se estrutura um sistema de gestão de riscos. Dessa forma, será abordado a seguir, o relatório técnico 31004:2015 que fornece as diretrizes de como se estrutura a gestão de riscos numa organização.

Conforme demonstrado na Figura 3, a estrutura da gestão de riscos engloba os componentes (i) mandato e comprometimento, (ii) concepção da estrutura para gerenciar riscos, (iii) implementação da gestão de riscos, (iv) monitoramento e análise crítica da estrutura e melhoria contínua da estrutura. Nota-se que a estrutura é cíclica – ou seja, sugere a necessidade de se manter em constante atualização – e portanto, reforça a ideia de que os esforços de gestão de riscos dos tomadores de decisão devem ser contínuos, dinâmicos e interativos conforme já mencionado

anteriormente. Além disso, é importante ressaltar que a estrutura da gestão de riscos auxilia na organização, na clareza e na definição de elementos para elaborar, por exemplo, uma política de gestão de riscos.

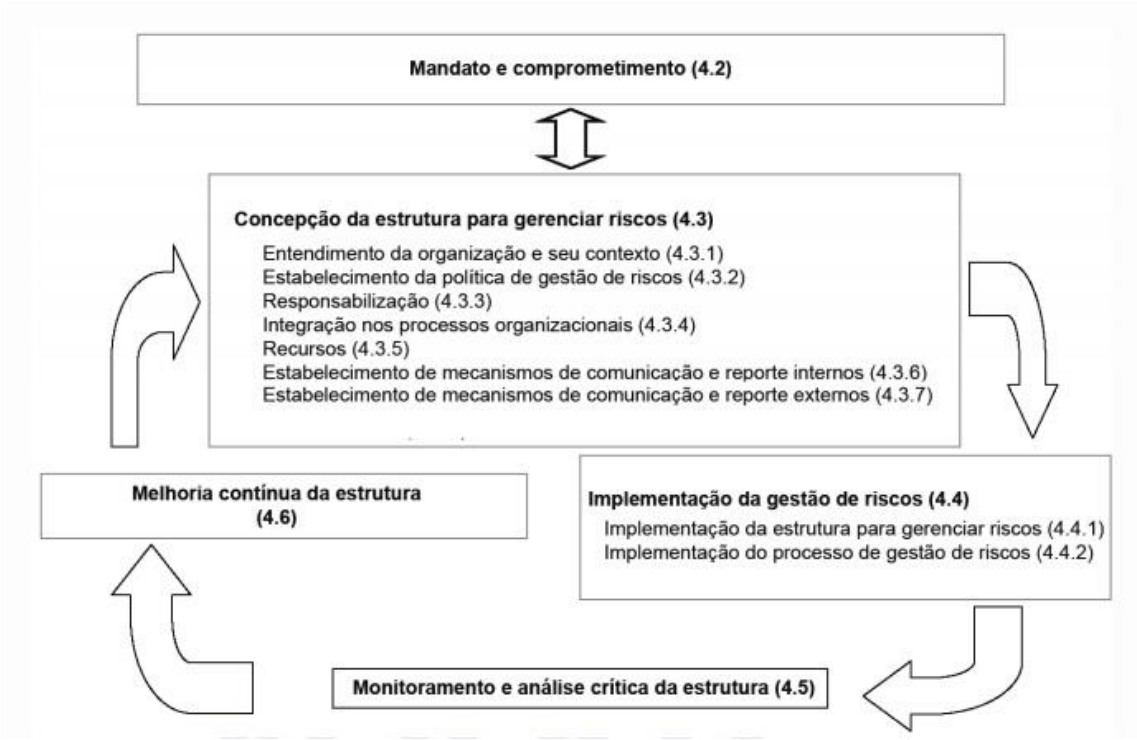

Figura 3 - ISO 31000:2009 - entre os componentes da estrutura para gerenciar riscos
Fonte: ABNT, 2009

Nesse contexto, para garantir a eficácia da implementação da gestão de riscos, a alta direção da organização é responsável por estabelecer e aprovar a política de gestão de riscos (mandato). Desse modo, deve comprometer-se para assegurar a conformidade legal e regulatória da política e outros atos legais (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2009).

Caso necessário, o mandato e comprometimento devem refletir os onze princípios já mencionados, além de serem documentados e comunicados de forma apropriada pela Alta Direção e o organismo de supervisão para todas as partes interessadas (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2015). Normalmente o mandato envolve mudanças no comportamento, na cultura, na política, nos processos e no desempenho da organização. Ademais, Ávila (2013, apud MARTINS et al., 2018) ressalta que para o processo de formação da cultura na organização, é fundamental ouvir as partes interessadas, pois de algum modo elas estarão envolvidas no processo de gerenciamento de riscos.

Para a concepção da estrutura da gestão de riscos, os contextos internos e externos da organização devem ser avaliados, visto que podem influenciar de forma significativa essa etapa. Ela é composta por seis elementos:

- Entendimento do contexto: responsável por identificar objetivos e contextos internos e externos para serem considerados no gerenciamento de riscos;
- Estabelecimento da política de gestão de riscos: etapa para estabelecer objetivos e comprometimento da organização de forma clara;
- Responsabilização das unidades e agentes: deve garantir que haja responsabilização, autoridade e competência apropriadas para gerenciar riscos;
- Integração aos processos organizacionais: a gestão de riscos deve ser incorporada em todas as práticas e processos da organização, de forma que seja pertinente, eficaz e eficiente, ou seja, o processo de gestão de riscos deve ser parte integrante, e não separado, desses processos organizacionais;
- Recursos: para essa etapa, a organização é responsável por alocar recursos necessários para a gestão de riscos;
- Formas de comunicação interna e externa: a comunicação interna se faz necessária a fim de apoiar e incentivar a responsabilização e a propriedade dos riscos. Para a comunicação externa, a organização deve desenvolver e implementar um plano sobre como se comunicará com partes interessadas externas. (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2009).

Para a etapa seguinte, deve ser elaborado um plano detalhado de implementação de riscos para assegurar que as alterações necessárias ocorram em uma ordem coerente e que os recursos envolvidos possam ser fornecidos e aplicados (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2015). O plano deve conter informações pormenorizadas sobre as ações a serem tomadas, indicar os tomadores de decisão, estabelecer o prazo de conclusão; identificar quais ações serão implementadas e definir as responsabilidades pela implementação. Notadamente, a implementação da gestão de riscos requer tempo para ser concluída e pode ser feita em etapas.

O monitoramento e a análise crítica são atividades fundamentais para determinar se as decisões tomadas pelos gestores continuam válidas, isto é, são duas atividades que demandam vigilância periódica. Para o relatório técnico

31004:2015, o monitoramento e a análise crítica têm por objetivo garantir que os riscos estão adequadamente gerenciados, e juntos fornecem garantias de que o desempenho da gestão de riscos está como o esperado. Segundo Santos (2014), se essas atividades forem aplicadas conforme prevê a norma 31000:2009, elas protegem e geram valor - primeiro princípio. Se os resultados do monitoramento e da análise crítica demonstrarem que melhorias podem ser feitas, convém que estas sejam implementadas tão logo quanto possível.

2.3. Panorama de estudos da Gestão de Riscos Corporativos nas organizações

A gestão de riscos, tanto no setor privado quanto na administração pública, é recente no Brasil e, portanto, existem poucos trabalhos publicados. Ainda assim, foram encontradas algumas experiências na literatura sobre as estratégias aplicadas para a implementação da gestão de riscos pelas organizações que usaram como balizadoras, as metodologias ISO 31000:2009 e COSO. Ressalta-se que em um dos estudos pesquisados, a organização empregou outra metodologia de Gestão de Riscos. O Quadro 1 abaixo apresenta resumos de estudos de casos sobre a implementação da gestão de riscos nas organizações.

QUADRO 1 – Estudos de caso

Bibliografia	Resumo
1. MARTINS, Mary Anne Fontenele et al. Política de gestão de riscos corporativos: o caso de uma agência reguladora da saúde. Revista do Serviço Público, v. 69, n. 1, p. 7-32, 2018.	Este estudo relata a experiência do processo de elaboração da Política de Gestão de Riscos Corporativos (PGRC) da Agência Nacional de Vigilância Sanitária (Anvisa). O processo de elaboração da política supracitada foi desenvolvido em cinco etapas inter-relacionadas, sendo: 1ª sensibilização da alta liderança: etapa responsável por explicar aos cinco adjuntos de diretores a Instrução Normativa MP/CGU nº 01/2016 e apresentar o projeto de implementação da política de GRC no âmbito da agência. Foi criado um Grupo de Trabalho (GT) responsável pela elaboração da minuta PGRC a ser discutida e aprovada pela diretoria da Anvisa. 2ª desenvolvimento de competências e *benchmarking*: realizadas as primeiras reuniões do GT para o alinhamento conceitual sobre GRC em formato de oficinas de trabalho em que o GT pôde se aproximar de metodologias ABNT NBR ISO 31000 e *COSO*. Foi identificada a necessidade de conhecer como o processo de GRC foi aplicado em outras instituições públicas, e assim, foi realizada a técnica de *benchmarking*. 3ª consulta interna aos

	servidores: ocorreu por meio de um formulário eletrônico e teve por objetivo incluir o tema aos gestores e servidores, e provocar o interesse em participar na consulta e no processo de implementação da política GRC. Conclui-se nessa etapa que a grande maioria concorda com a política de GRC e demonstra preocupação em operacionalizá-la na organização. 4ª comunicação e disseminação interna dos conceitos e andamento dos trabalhos: foram criadas estratégias para a comunicação, sendo uma delas postar notícias na intranet, no portal e no Boletim da Estratégia da Anvisa. Além disso foram criados *e-mail* e pasta corporativos na rede interna da agência para troca de informações e guarda de documentos. 5) discussão e aprovação da política pela diretoria colegiada da agência: para a elaboração da minuta da política de GRC, o GT foi dividido em três grupos para facilitar o processo de elaboração dos capítulos, sendo realizadas reuniões para apresentação e discussão de cada parte do conteúdo da minuta.
2. DESTRO, Mayara Coutinho Análise da estruturação da gestão de risco institucional: o caso Embrapa. 2014. 121 f., il. Monografia (Bacharelado em Comunicação Social)—Universidade de Brasília, Brasília, 2014.	O trabalho analisou a gestão de risco e como ela está sendo implementada na Empresa Brasileira de Pesquisa Agropecuária (Embrapa). A gestão de riscos na Embrapa surgiu após uma demanda vinda do Tribunal de Contas da União (TCU) que tinha o objetivo de analisar a existência de práticas de gestão de riscos institucionalizadas. Para isso, o TCU aplicou um questionário às instituições sorteadas para conhecer e classificar o nível de maturidade em gestão de riscos. A área responsável por responder a demanda foi a Coordenadoria de Gestão de Riscos e Suporte à Decisão (CGR) da Embrapa, com a finalidade implementar uma política integrada de gestão de riscos e de segurança da informação, gerenciar as bases de dados de métodos quantitativos e a sua aplicabilidade na pesquisa agropecuária. A criação dessa Coordenadoria foi a primeira ação por parte da Embrapa para iniciar a sua gestão de riscos corporativos.
3. FREIRE, Antonio Emilio Bastos de Aguiar. Implementação da gestão de riscos em empresas estatais: estudo de Caso do METRÔ-DF. 2017. 57 f., il. Trabalho de conclusão de Curso (Especialização em Controle Externo)—Universidade de Brasília, Brasília, 2017. .	O estudo fez um diagnóstico sobre a implementação da gestão de riscos em empresas estatais com base em um estudo de caso: a Companhia do Metropolitano do Distrito Federal - METRÔ-DF. Em 2015, uma vez que a Controladoria-Geral do Distrito Federal (CGDF) começou a modernizar técnicas de auditoria por meio da implementação da auditoria baseada em riscos e boas práticas de governança corporativa. Dessa maneira, houveram capacitações em gestão de riscos e em COSO que serviram como início da adoção da norma ISO 31000:2009 como uma guia mestre para gestão de riscos. A ISO 31000:2009 funcionou como base delineadora para a implementação da gestão de riscos, e auxiliou na elaboração de uma planilha contendo elementos para a

	identificação, análise e avaliação na aplicação do estudo de caso que, dividida em variáveis (número do processo ou da ação estratégica, risco identificado, evento, causa, áreas impactadas, consequências, categoria, probabilidade, impacto e nível de risco), teve por objetivo identificar, analisar e avaliar os riscos do metaprocesso de aquisições. Foram identificados fatores que afetaram a implementação da gestão de riscos na empresa, sendo: estrutura não integrada, planejamento errático, ausência de uma cultura voltada à otimização de resultados previamente definidos por meio de metas e indicadores, e falta de clareza nos objetivos estratégicos, táticos e operacionais. O principal obstáculo identificado está relacionado à resistência a mudanças.
4. GASPARY, Lisiane Valdez et al. Implementação da gestão de risco e disseminação da cultura de segurança: desafios de um hospital público. **Revista Acreditação**, v. 7, n. 13, p. 60-76, 2017.	O artigo é um estudo de caso descritivo que foi desenvolvido em um hospital público no período de 2005 a 2015 o Hospital Geral de Itapecerica da Serra (HGIS) - São Paulo. É um estudo que relaciona a gestão de riscos com a cultura de segurança e tem por objetivo descrever o processo de implementação desses dois elementos no hospital público. Em 2005 foi criada a Comissão Multiprofissional de Gerenciamento de Risco focada na gestão de riscos sanitários, e a partir de então, foram criados núcleos responsáveis por coordenar o sistema de gerenciamento e vigilância de riscos. Por exemplo, em 2008 foi criado o Serviço de Vigilância de Risco (SVR) que definiu bases para notificações de incidentes, mapeou riscos das atividades assistenciais e definiu estratégias para estimular às notificações de riscos. Em 2013 foi criado um sistema eletrônico de notificação de riscos na intranet, que permite categorizar os tipos de incidentes. Durante o processo de implementação da gestão de riscos, foram apontados desafios quanto a disseminação da cultura de segurança para os colaboradores do hospital e propiciar um ambiente favorável para que os colaboradores se sentissem a vontade para relatar possíveis riscos.
5. DA SILVA, Carlos Eduardo Sanches et al. Aplicação do gerenciamento de riscos no processo de desenvolvimento de produtos em empresas de autopeças. **Production**, v. 20, n. 2, p. 200-213, 2010.	O trabalho avaliou a aplicação do gerenciamento de riscos no processo de desenvolvimento de produtos de empresas de autopeças. Para a implementação da gestão de riscos, foram realizadas reuniões com a equipe de projeto, sendo programada para cada etapa do planejamento uma reunião específica. A metodologia utilizada foi *Project Management Body of Knowledge* (PMBOK), que contém conjunto de práticas na gestão de projetos organizado pelo instituto PMI. As etapas do PMBOK implementadas foram: 1ª planejamento e gerenciamento de riscos: para essa etapa foi elaborado *Work Breakdown Structure* (WBS) e para isso foi realizada uma análise documental,

	utilizando conhecimentos do pesquisador e validação pelo gerente da planta. 2ª identificação dos riscos: foram utilizadas técnicas de revisão de documentação e *brainstorming*, e na sequência os riscos identificados foram classificados em qualitativos e quantitativos. Os autores destacaram que a participação da equipe de projeto e o clima descontraído favoreceram a identificação dos riscos. 3ª análise qualitativa dos riscos: etapa responsável por classificar os riscos qualitativos em função dos objetivos do projeto, bem como para a definição acerca da probabilidade de ocorrência do risco. 4ª análise quantitativa dos riscos: para os riscos quantitativos, foi simulada a duração do projeto utilizando o *software* @RISK. Assim, por meio da análise quantitativa foi possível estimar a probabilidade de cumprirem o projeto no prazo acordado. 5ª planejamento das respostas a riscos: fase responsável pelas análises dos riscos qualitativos e quantitativos. Para a análise qualitativa foi adotado um formulário que contribuiu para a simultaneidade. Já para a análise quantitativa foram redefinidos os prazos atribuídos às atividades e foi executada uma simulação, para aumentar a probabilidade de cumprir o prazo acordado com o cliente. 6) monitoramento e controle de riscos: durante essa etapa, foram realizadas reuniões-relâmpagos a cada cinco dias para acompanhamento do projeto com o objetivo de atualizar os prazos previstos X realizados. O estudo conclui que o gerenciamento de riscos tende a concentrar os maiores esforços nas etapas de planejamento em relação às etapas de controle além de auxiliar na tomada de decisão.
6. SOUZA, Jackson Gomes Soares et al. Gestão de riscos de segurança da informação e sua apresentação na governança de TI da administração pública. In: **X WORKSHOP DE PÓS-GRADUAÇÃO E PESQUISA DO CENTRO PAULO SOUZA**. 2015.	Trata-se de um estudo qualitativo e exploratório, que buscou proporcionar uma visão de como a gestão de riscos de segurança da informação pode ser apresentada à governança de Tecnologia da Informação (TI) em organizações públicas. Para verificar como o processo de implementação da Gestão de Risco de Segurança da Informação (GRSI) ocorreu, foi sugerido levantamento de indicadores e verificação da conformidade destes às boas práticas. Para isso, os autores dividem os indicadores obtidos em dois grupos (grupo de indicadores Governança de TI (GTI) e grupo de indicadores GRSI), e explicam e exemplificam como obter informações de cada grupo e quais questionamentos devem ser feitos para que o pesquisador possa verificar o grau de comprometimento da organização com a governança de TI e com a GRSI.
7. FERNANDES, Eduardo da Silva. Aplicação de sistemática de gestão de riscos no processo de aquisição de suprimentos em uma instituição pública	O trabalho aplicou uma sistemática de Gestão de Riscos em uma instituição pública brasileira, mais precisamente no processo de aquisição de suprimentos. A sistemática aplicada levou em

brasileira. 2019.	consideração apenas o modelo da ISO 31000:2009. Este estudo foi dividido em três artigos, sendo que o artigo 1 engloba etapas preliminares de identificação e análise de riscos; o artigo 2 engloba a etapa de análise de riscos com o objetivo de identificar efeitos e causas dos riscos e priorizá-las; e o artigo 3 engloba etapas de tratamento e monitoramento de riscos. No primeiro artigo, os riscos foram identificados por meio do método *brainstorming*, e percebeu-se que houve uma predominância de riscos de origem interna da instituição. A análise de riscos visou a priorização dos mesmos utilizando o método Processo Hierárquico Analítico (método qualitativo de avaliação de risco, devendo ser aplicado tanto para a probabilidade quanto para o impacto). O segundo artigo buscou identificar e analisar as causas raízes e efeitos de riscos identificados no processo de aquisição de suprimentos em uma instituição pública brasileira, utilizando o método *Failure Mode and Effect Analysis* (FMEA). Para isso, foi feito o estudo de caso do risco de Interrupção de contrato de fornecimento, considerado como tendo alto impacto e probabilidade no processo de aquisição de suprimentos em uma instituição pública de ensino superior. Por meio do FMEA, foram identificadas 09 causas raiz, sendo a maioria delas de origem interna à instituição. Por fim, no último artigo, tanto para o tratamento de riscos quanto para o monitoramento foram feitas propostas por meio do método *brainstorming*, para o tratamento realizaram propostas de ações para controlar cada causa raiz do risco de Interrupção de contrato de fornecimento e para o monitoramento foram propostos indicadores de desempenho para o processo de aquisição de suprimentos.

Fonte: Elaborado pela autora.

3. MÉTODOS E TÉCNICAS DE PESQUISA

Segundo Prodanov et al., (2013), a metodologia de um trabalho é a aplicação de procedimentos e técnicas que devem ser observados para construção do conhecimento, com o propósito de comprovar sua validade e utilidade nos diversos âmbitos da sociedade. Desse modo, este capítulo tem por objetivo apresentar métodos e técnicas de pesquisa utilizados para a realização do trabalho.

3.1. Tipologia e descrição geral dos métodos de pesquisa

Para a realização deste trabalho, foi feita uma pesquisa documental, a partir de documentos legais (decretos e leis, instrução normativa) disponibilizados pelo Conselho Administrativo de Defesa Econômica e levantamento bibliográfico de artigos para o embasamento teórico requerido ao trabalho.

Diante do objetivo proposto, de acordo com Vergara (2009), o presente trabalho apresenta-se em virtude de um aspecto que pode ser denominado quanto aos fins. Quanto aos fins, classifica-se como descritivo e exploratório. Descritivo porque através da observação, interpretação e comparação das informações coletadas, será possível caracterizar o órgão estudado. Exploratório em virtude de que o gerenciamento de riscos corporativos ainda é um tema novo para as instituições públicas no país.

A pesquisa tem caráter qualitativo, uma vez que não há dados numéricos. Gil (2002) considera que há uma relação dinâmica entre o mundo real e o sujeito, ou seja, existe um vínculo indissociável entre o mundo objetivo e a subjetividade sujeito, que não pode ser traduzido em números.

Os dados qualitativos para a pesquisa documental foram coletados a partir da Lei de Acesso à Informação nº 12.527/2011. Em resposta a solicitação de informação feita no dia 28 de maio de 2019, o Cade informou o número de seis processos do Sistema Eletrônico de Informações (SEI), relacionados a implantação da Gestão de Riscos Corporativos na autarquia, sendo que um dos processos não foi encontrado no *site*, assim, todos demais processos foram analisados e organizados em ordem cronológica em uma tabela, conforme demonstrado abaixo:

Tabela 1 – Processos do SEI

Processo	Tipo de documento	Data	Assunto
322585	Memorando Circular nº 8-2018- AECI/GM	06/04/2017	Sistematização de práticas relacionadas à gestão de riscos, aos controles internos e à governança
322588	Ofício Circular nº 41 - 2017 - SE - CGU	06/04/2017	Implementação dos dispositivos da Instrução Normativa Conjunta MP/CGU nº 01/2016
327900	Ata de reunião	04/05/2017	Recomendações CGU e TCU; Minuta de portaria da política de gestão de riscos do MJSP; Situação atual da gestão de riscos do Cade
331071	Minuta de portaria	04/05/2017	Minuta de portaria que institui a política de gestão de riscos
331120	Publicação no DOU - IN MP/CGU nº 1/2016	10/05/2017	Publicação da instrução normativa MP/CGU nº 1/2016 no Diário Oficial da União
333852	Portaria 173	10/05/2017	Portaria nº 173 de 10 de maio de 2017 que aprova a política de gestão de riscos
453832	Ofício Circular nº 1/2018/AECI/GM-MJ	14/03/2018	Consulta pública do manual de gerenciamento de riscos e controles internos
453836	Publicação no DOU - Portaria 31	14/03/2018	Publicação da Portaria nº 31/2018/MJ
453840	Publicação no DOU - Portaria 32	14/03/2018	Publicação da Portaria nº 32/2018/MJ
453844	Manual gerenciamento de risco do Ministério da Justiça	14/03/2018	-
455621	Folheto divulgação consulta manual gestão de riscos MJ1	19/03/2018	Folheto para divulgação para que haja participação da consulta pública.

455623	Folheto divulgação consulta manual gestão de riscos MJ2	19/03/2018	Folheto para divulgação para que haja participação da consulta pública.
458153	Anexo aviso circular nº 2/2018/GM/CGU	23/03/2018	Programas de Integridade - Decreto 9.203 de 22 de novembro de 2017. Este aviso informa que a partir de abril de 2018 a CGU publicará informativo estabelecendo os procedimentos necessários à estruturação, à execução e ao monitoramento de programas a integridade, conforme instituído pelo Decreto supracitado.
461927	Decreto nº 9.203 de 22 de novembro de 2017	05/04/2018	Dispõe sobre a política de governança da administração pública federal direta, autárquica e fundacional. Apresenta os princípios da governança pública, suas diretrizes, quais são as competências dos comitês internos de governança, etc.
475352	Portaria nº 283	11/05/2018	Portaria nº 283 de 11 de maio de 2018 que aprova a política de governança, gestão de integridade, riscos e controles da gestão no âmbito do Cade.
477847	Publicação no DOU - Portaria 283	16/05/2018	Publicação da portaria nº 283 no Diário Oficial da União
522972	Apresentação da reunião 1/2018	11/09/2018	Reunião inaugural do Comitê de Governança, Riscos e Controle - Corisc. Foram tratados assuntos sobre a composição do Corisc, marco legal citando a IN MP/CGU nº 01/2016; Decreto nº 9.203/2017. Marco legal Cade portaria nº 173/2017 que aprova a política de Gestão de Riscos, Governança e Controles Internos e portaria nº 283/2018 que aprova a política de Governança, Gestão da Integridade, Riscos e Controles da Gestão.
531218	Despacho ordinário	28/09/2018	Minuta de portaria contendo a relação dos servidores indicados para compor o Comitê Executivo de Gestão de Riscos (Cerisc)
535640	Apresentação reunião Cerisc	10/10/2018	Reunião inaugural do Comitê Executivo de Gestão de Risco - Cerisc. Contém definição de risco de acordo com a ISSO 31000:2009, suas tipologias de acordo com a portaria nº 283/2018. Há uma tabela que identifica a Governança Corporativa do Cade
532042	Portaria nº 498 de 16/10/2018	17/10/2018	Portaria com o nome dos servidores para comporem o Comitê Executivo de Gestão de Riscos (Cerisc)

522971	Ata de reunião	24/10/2018	-
542737	Apresentação reunião Subcomitê Integridade	01/11/2018	Definição de diretrizes. Contém informações sobre as **etapas** da metodologia de Gestão de Riscos do Cade, sendo: Etapa 1) mapeamento do processo crítico; Etapa 2) Identificação de Riscos do Processo Crítico; Etapa 3) Análise e avaliação dos riscos do processo crítico; Etapa 4) Proposta-tratamento e estratégia de implementação da Gestão de Riscos do Processo crítico. Os slides apresentam sugestões do CGU na Gestão de Riscos e modelo do Plano de Integridade.
543082	E-mail	01/11/2018	Encaminhamentos da reunião do Subcomitê de Integridade.
545778	Apresentação 1ª oficina Laboratório de Gestão de Risco	08/11/2018	Tema: Compartilhamento de Informações orientadas para Ações Civis de Reparação por Danos Concorrenciais (ACRDC). Contém planilhas de riscos, sendo etapa 2) identificação de risco; etapa 3)análise e avaliação de riscos e etapa 4) tratamento de riscos.
547211	Registro dos principais riscos Integridade	12/11/2018	Relacionado aos servidores. Foram listados os principais riscos.
553974	Portaria 616	30/11/2018	Portaria nº 616 de 30 de novembro de 2018, aprova o Plano de Integridade do Cade.
554262	Plano de Integridade do Cade	30/11/2018	Plano de Integridade do Cade
554232	Ata de reunião	03/12/2018	Plano de Integridade do Cade; Plano de Riscos do Cade e metodologia de Gestão de Riscos do Cade (MGCR); Estratégia de Implantação da Gestão de riscos para o processo crítico.
554643	Plano de Integridade Cade	03/12/2018	Publicação do Plano de Integridade do Cade
554853	Minuta Metodologia Gestão de Riscos do Cade	03/12/2018	Minuta formatada
554569	Publicação no DOU - Portaria 616	03/12/2018	Publicação da Portaria nº 616 de 30 de novembro de 2018.
562189	Metodologia de Gestão de Riscos do Cade	21/12/2018	

	Fluxogramas	18/02/2019	Proposta de fluxos Integridade: conflito, corregedoria, denúncia, nepotismo, ouvidoria

Fonte: Elaborado pela autora.

A partir disso, após leitura de todos os conteúdos dos processos localizados no SEI, foram selecionadas informações consideradas importantes para descrever a implantação da GRC nas organizações públicas e empresas privadas para compor os resultados. Sendo assim, foram desconsideradas minutas de portaria, fluxogramas e encaminhamento de *e-mails*.

3.2. Caracterização da organização

A administração pública no Brasil compreende órgãos e entidades que desempenham a atividade administrativa do estado e se divide em administração direta (União, Estados, Distrito Federal e Municípios) e indireta (Autarquia, Fundação Pública, Empresa Pública e Sociedade de Economia Mista). Há ainda as chamadas entidades paraestatais, as quais não integram a administração indireta e compreendem os serviços sociais autônomos, entidades de apoio, organizações sociais, e organizações da sociedade civil (ROSA, 2004).

Criado pela Lei nº 4.137, de 10 de setembro de 1962 como um órgão do Ministério da Justiça (MJ), somente em 1994 o Conselho Administrativo de Defesa Econômica (Cade) se tornou uma autarquia federal em regime especial vinculada ao do Ministério da Justiça e Segurança Pública, com sede e foro no Distrito Federal pela lei nº 8.884, de 11 de junho de 1994 e reestruturado em decorrência da entrada em vigor da lei nº 12.529, em 30 de novembro de 2011 (CARTILHA DO CADE, 2016).

Apesar de ser uma autarquia em regime especial, o Cade não é uma agência reguladora da concorrência, e sim uma autoridade de defesa da concorrência. Sua missão é zelar pela manutenção de um ambiente concorrencial saudável no Brasil, portanto, tem como responsabilidade julgar e punir administrativamente em instância única pessoas físicas e jurídicas que pratiquem infrações à ordem econômica, não havendo recurso para outro órgão; além de analisar atos de concentração, de modo a minimizar possíveis efeitos negativos no ambiente concorrencial de determinado mercado. Não estão entre as atribuições da autarquia regular preços e analisar aspectos criminais das condutas que investiga. Suas competências também não se confundem, por exemplo, com as de órgãos e entidades de defesa do consumidor

(por exemplo, Instituto de Defesa do Consumidor – Procon, Secretaria Nacional do Consumidor – SENACON/MJ, entre outros) ou dos trabalhadores (CADE, 2016). Desse modo, o Cade exerce três funções:

- Preventiva – controle de fusões, incorporações e outros atos de concentração econômica entre grandes empresas, que possam colocar em risco a livre concorrência;
- Repressiva – combate a cartéis e outras condutas nocivas ao ambiente concorrencial;
- Educativa – disseminar a cultura da concorrência, instruir o público em geral sobre as diversas condutas que possam prejudicar a livre concorrência; incentivar e estimular estudos e pesquisas acadêmicas sobre o tema, firmando parcerias com universidades, institutos de pesquisa, associações e órgãos do governo; realizar ou apoiar cursos, palestras, seminários e eventos relacionados ao assunto; editar publicações, como a Revista de Defesa da Concorrência e cartilhas (CARTILHA DO CADE, 2016).

Neste contexto, a autarquia é composta por três órgãos: Tribunal Administrativo de Defesa Econômica (Tribunal), Superintendência-Geral (SG) e o Departamento de Estudos Econômicos (DEE). Possui ainda unidades que prestam apoio às suas atividades: Procuradoria Federal Especializada junto ao Cade (ProCade) e Diretoria Administrativa (DA).

Organograma do Cade

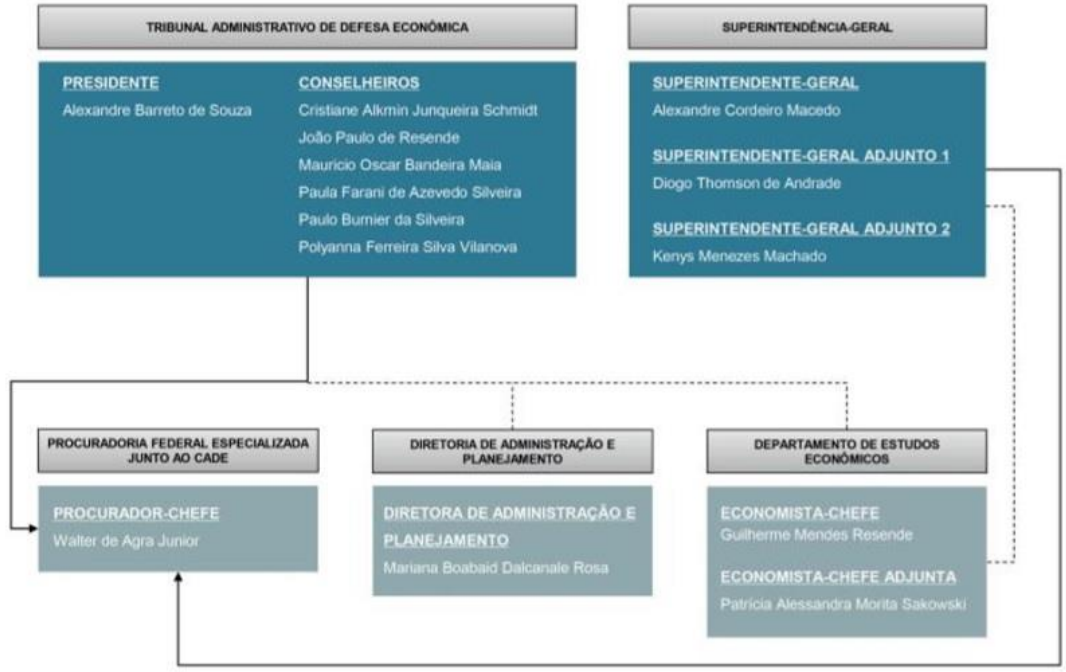

Figura 4 – Organograma do Conselho Administrativo de Defesa Econômica.
Fonte: Brasil, 2018b

Legenda:
Relação de subordinação - - - - - - -
Relação de vínculo ⟶

A alta direção do Cade é composta por um presidente e seis conselheiros, que integram o Tribunal Administrativo, todos com mandatos de quatro anos, vedada a recondução. Compreende ainda por um Superintendente-Geral da Superintendência-Geral, que possui mandato de dois anos, permitida a recondução para um único período subsequente. Todos são nomeados pelo Presidente da República depois de aprovados pelo Senado Federal (BRASIL, 2011).

4. RESULTADO E DISCUSSÃO

Nesta sessão são apresentados os resultados da análise documental realizada. A partir da publicação da Portaria nº 283/2018, que aprova a Política de Governança, Gestão de Integridade, Riscos e Controles da Gestão no âmbito do Cade, a primeira medida adotada pela autarquia para implementar a gestão de riscos foi estabelecer instâncias da liderança e gestão conforme mostra a Tabela 1.

Tabela 2 – Instâncias de lideranças e gestão de risco do Cade

Instância	Integrantes	Responsabilidades
1ª Comitê de Governança, Riscos e Controles – Corisc	Presidente do Cade; Conselheiro mais antigo; Superintendente-Geral; Procurador Chefe; Economista-Chefe; Diretor de Administração e Planejamento.	Estabelecer limites de exposição a riscos globais do Cade e de competência das unidades; Aprovar e supervisionar priorização de temas/macroprocessos para gerenciamento de riscos e controles internos; Supervisionar o mapeamento e avaliação dos riscos-chaves referentes à prestação de serviços; Zelar pela conformidade legal da prestação dos seus serviços e pelo padrão de comportamento ético de todos os servidores.
2ª Comitê Executivo de Gestão de Riscos – Cerisc	Representante de cada órgão do Cade.	Responsável por implementação a Política de Gestão de Riscos.
3ª Subcomitês	Criados para tratar de tema específicos sob demanda do Cerisc.	
4ª Gestores de Risco	Ocupante de cargo ou função de chefia institucionalmente definido no regimento interno	Responsáveis pela avalição dos riscos no âmbito da sua unidade.
5ª Servidores	Servidores	Responsáveis pela operacionalização dos controles internos da gestão; Comunicação de possíveis riscos às instâncias superiores.

Fonte: Elaborado pela autora.

Como determinado pela norma ISO 31000:2009, o Cade envolveu a alta direção nas duas primeiras instâncias, sendo estabelecidas a composição e responsabilidades. Da mesma forma, para as demais instâncias e, de acordo com suas competências, atribuiu responsabilidades à todos os níveis da autarquia incluídos no processo de gestão de riscos.

A respeito desta etapa de criação de instâncias no Cade, observa-se nos estudos (1) e (4) que as instituições também instituíram comissões ou grupo de trabalhos, sendo que no estudo (1) foi criado um grupo de trabalho responsável por elaborar minuta da política de gestão de riscos e no estudo (4) foi formada uma comissão multiprofissional de gerenciamento de riscos além de núcleos responsáveis por coordenar o sistema de gerenciamento de riscos no hospital.

Para viabilizar a execução da gestão de riscos no Cade, além de determinar a criação de instâncias de liderança, a Portaria nº 283/2018, apontou os seguintes instrumentos do Modelo de Gestão de Riscos que asseguram o alcance dos objetivos estratégicos e auxilia a tomada de decisão dos colaboradores, dirimindo possíveis riscos negativos:

- A Política de Governança, Gestão de Integridade, Riscos e Controles de Gestão do Cade;
- As Instâncias de Liderança e Gestão de Risco do Cade;
- A Metodologia de Gerenciamento de Risco do Cade (MGCR) o modelo de gestão de riscos deve ser estruturado com base *Committee of Sponsoring Organizations of the Treadway Commission* – COSO, ISO 31000 e boas práticas;
- O plano de riscos;
- A capacitação continuada;
- As Normas, Manuais e Procedimentos; e
- Solução Tecnológica.

De acordo com o Relatório de Gestão do Exercício de 2017, no que se refere a capacitação continuada, em 2017 foi realizada a programação de capacitação em gestão de risco integrada ao processo de implementação da Política de Gestão de Risco do Cade. Essa programação foi dividida em duas etapas, em que a primeira compreendeu a realização de um Seminário de Gestão de Riscos voltado para a sensibilização sobre o tema para os servidores do Cade e a segunda voltada à capacitação dos servidores que atuarão como gestores de riscos (4ª instância da

liderança e gestão de risco no Cade). Para essa etapa, foram abertas duas turmas do curso de Introdução à Gestão de Riscos e teve como objetivo uniformizar os conceitos básicos sobre Gestão de Riscos dos servidores do Cade, capacitando-os para executar o processo de avaliação de riscos de acordo com a série de normas ISO 31.000.

Sobre a capacitação, verifica-se que nos estudos de casos (1), (3) e (5) foram realizadas capacitações para o alinhamento conceitual sobre a gestão de riscos a fim de aproximar os servidores à metodologia COSO e ABNT 31000:2009, com exceção do estudo (5), cujas reuniões capacitaram a equipe na metodologia PMBOK.

O instrumento Metodologia de Gestão de Riscos do Cade (MGRC) foi aprovado em dezembro de 2018 e elaborado de acordo com as premissas da metodologia COSO e ISO 31000:2009, ou seja, o documento descreve cada um dos componentes do processo da Gestão de Riscos a saber:

- Estabelecimento do contexto;
- Identificação dos riscos;
- Análise de riscos;
- Avaliação de riscos; e
- Tratamento de riscos.

Para o estabelecimento do contexto, o Cade assume que o conhecimento e a visão crítica sobre os processos de trabalho (ou processos organizacionais) são fundamentais para que a organização possa alcançar sua Estratégia. Desse modo, sua proposta é atuar sobre os processos críticos: os processos críticos são os principais processos de trabalho que a autarquia executa para entregar valor à sociedade, assim como os processos de gerenciamento e suporte. Para a autarquia, os processos críticos se constituem em elementos base para a identificação de eventos de riscos, a avaliação de riscos e a escolha das ações mais adequadas para o seu tratamento, tendo em vista o alcance dos Objetivos Estratégicos.

Os objetivos a serem atingidos e a forma para alcançá-los constam no seu Planejamento Estratégico 2017-2020, que alinhado ao Plano Plurianual, foram estabelecidos sob três perspectivas: resultados para a sociedade; objetivos habilitadores, e fundamentos, conforme demonstrado na Tabela 2.

Tabela 3 – Objetivos Estratégicos do Cade por Perspectiva

Perspectivas	Objetivos estratégicos
Resultados para a sociedade	• Assegurar a qualidade e a eficácia do controle de concentrações; • Fortalecer o combate e condutas anticompetitivas; • Promover a cultura da concorrência no Brasil; • Exercer protagonismo na agenda antitruste internacional.
Objetivos habilitadores	• Adotar melhores práticas e inovação; • Ampliar os serviços ofertados eletronicamente pelo Cade; • Aprimorar os mecanismos de gestão da informação e do conhecimento; • Aprimorar processos de comunicação interna e externa.
Fundamentos	• Promover a valorização e o desenvolvimento dos servidores; • Ampliar o quadro de servidores, com perfil adequado às necessidades do Cade; • Prover adequada infraestrutura, suporte logístico e tecnológico.

Fonte: Brasil, 2018b

Vale lembrar que em uma organização, os OE direcionam os caminhos que buscam tornar operacional a missão (COSO, 2007) e realizar sua visão. Desse modo, com o intuito de medir o sucesso do alcance dos seus OE, o Planejamento Estratégico 2017-2020 do Cade estabeleceu indicadores e metas conforme demonstrado na Tabela 3

Tabela 4 – Perspectiva Habilitadores

Objetivo Estratégico	**OE5 – Aprimorar os processos de trabalho com adoção de melhores práticas e inovação**	**Meta**		
Item	**Indicador**	**2018**	**2019**	**2020**
5.2	Índice de Governança e Gestão Pública (IGG-TCU)	> 0,75	> 0,75	> 0,75
Iniciativas estratégicas	**Projetos**	**2018**	**2019**	**2020**
Adotar boas práticas de gestão e governança	Implantação do Plano de Integridade	x	x	
	Implantação da governança da gestão de riscos	x		
	Implantação da gestão de riscos em processos críticos	x	x	x

Fonte: Brasil, 2018b

Nesses termos, a gestão de riscos no âmbito do Cade se integra ao seu planejamento estratégico e aos seus processos organizacionais, atendendo ao que está estabelecido na Política de Governança, Gestão da Integridade, Riscos e Controles da Gestão do Cade.

Para a etapa de identificação de riscos, a metodologia considera que os eventos de risco são situações em potencial, de origem interna ou externa, que podem impactar de forma negativa (riscos propriamente ditos) ou de forma positiva (oportunidade de fazer com mais excelência) a execução das atividades ou tarefas de determinado processo organizacional. Portanto, estabelece que a identificação de riscos será realizada no nível dos processos críticos com ênfase naqueles que contribuem para o alcance dos Objetivos Estratégicos do Cade uma vez que se não forem identificados e tratados poderão comprometer a qualidade dos processos e das entregas para a sociedade.

Desse modo, o processo de identificação parte de uma abordagem inicial, de caráter exploratório sobre os potenciais eventos que impliquem em riscos a determinado processo crítico. Passo seguinte, conforme indicado pela norma 31000:2009, é gerada uma lista abrangente de riscos baseada nos eventos que possam criar, aumentar, evitar, reduzir, acelerar ou atrasar a realização dos objetivos; e, assim, é estabelecida uma lista com os principais eventos de riscos daquele processo crítico. Esta lista é analisada, sendo destacadas informações sobre as causas e as consequências desses eventos de riscos e por fim, são definidos e sistematizados um conjunto de informações sobre o ambiente de riscos (quais riscos, suas causas e consequências) que servirá de apoio ao gerenciamento de riscos.

A fase de análise de risco estabelece a natureza do risco e determina seu nível. A MGRC considera impacto, os efeitos da ocorrência de um risco e os critérios utilizados para a análise desses efeitos são: custo, prazo, reputação, qualidade, entre outros. A probabilidade é medida analisando as causas ou o evento de risco e considera aspectos como frequência observada ou esperada.

Para a avaliação dos riscos inerentes (RI) de cada processo crítico, foram criadas duas tabelas de escalas de classificações de probabilidade e impacto.

Tabela 5 – Escala de Probabilidade

Probabilidade	Descrição da probabilidade	Frequência	Peso
Muito Alta	Evento esperado, repetitivo e constante	>90%	5
Alta	Evento usual, provavelmente ocorra	>50%<=90%	4
Média	Evento esperado, deve ocorrer em algum momento	>=30%<=50%	3
Baixa	Evento inesperado, pode ocorrer em algum momento	>10%<=30%	2
Muito Baixa	Evento extraordinário	<10%	1

Fonte: Brasil, 2018a

Tabela 6 – Escala de impacto

Probabilidade	Descrição da probabilidade	Peso
Catastrófico	Impacto no processo crítico de forma irreversível	5
Forte	Impacto no processo crítico de difícil reversão	4
Moderado	Impacto no processo crítico, porém recuperável	3
Fraca	Pequeno impacto no processo crítico	2
Insignificante	Mínimo impacto no processo crítico	1

Fonte: Brasil, 2018a

Em conformidade com o Roteiro de Auditoria de Gestão de Riscos do Tribunal de Contas da União (TCU), a MGRC parte do princípio de que o risco é uma função da probabilidade e do impacto, ou seja, o quanto ele pode afetar determinado processo crítico. Desse modo, o produto da probabilidade pelo impacto é uma forma de classificar os níveis de riscos:

Nível do Risco Inerente (NRI) = P (probabilidade) x I (impacto)

Neste aspecto, a MGRC propõe o seguinte Modelo Matriz de Risco – Forma Qualitativa:

Tabela 7 - Modelo Matriz de Risco – Forma Qualitativa

Impacto Probabilidade	Insignificante (1)	Fraca (2)	Moderada (3)	Forte (4)	Catastrófica (5)
Muito Alta (>90%)	Médio	Alto	Alto	Extremo	Extremo
Alta (>50% <=90%)	Médio	Médio	Alto	Extremo	Extremo
Média (>=30% <50%)	Baixo	Médio	Alto	Alto	Extremo
Baixa (>=10% <=30%)	Baixo	Baixo	Médio	Médio	Médio
Muito Baixa (<10%)	Baixo	Baixo	Baixo	Baixo	Médio

Fonte: Brasil, 2018a

A fim de avançar a análise sobre os controles adotados pelo Cade aos RI, a metodologia estabelece a escala de avaliação de controles, que permite verificar os efeitos dos controles existentes na mitigação dos riscos. Para isso, foi estipulada uma forma de classificar os controles: Nível de Confiança (NC).

Tabela 8 - Escala Avaliação de Controle

Nível de Confiança (NC)	Avaliação do desenho e operação dos controles	Risco de Controle (RC)
Inexistente NC = 0% (0,0)	**Desenho:** não há sistema de controle **Operação:** controle não executado	Muito Alto 1,0
Fraco NC = 20% (0,2)	**Desenho:** há procedimento de controle para algumas atividades, porém informais **Operação:** controle parcialmente executado e com deficiências	Alto 0,8
Mediano NC = 40% (0,4)	**Desenho:** controles não planejados formalmente, mas são executados controle para algumas atividades, porém informais **Operação:** controle parcialmente executado	Médio 0,6
Satisfatório NC = 60% (0,6)	**Desenho:** controles não foram planejados formalmente, mas são executados de acordo com a experiência dos servidores **Operação:** controle implantado e executado de maneira periódica e quase sempre uniforme. Avaliação dos controles é feita com alguma periodicidade	Baixo 0,4
Forte NC = 80% (0,8)	**Desenho:** o sistema de controle é eficaz na gestão de riscos (adequadamente planejado, discutido, testado e documentado com correções ou aperfeiçoamentos planejados de forma tempestiva) **Operação:** controle implantado e executado de maneira uniforme pela equipe e na frequência desejada. Periodicamente os controles são testados e aperfeiçoados.	Muito Baixo 0,2

Fonte: Brasil, 2018a

A partir do NC definido, determina-se o Risco de Controle (RC) o qual é definido como complementar ao nível de controle.

Risco de Controle (RC) = 1 – Nível de Controle (NC)

Uma vez definidos os níveis de NRI e os RC, estima-se o nível de risco residual (NRR), ou seja, é o risco remanescente depois de considerado o efeito das respostas adotadas pela autarquia para reduzir a probabilidade e/ou consequências dos riscos. Este risco é o produto do NRI e o RC.

Nível de Risco Residual (NCR) = Nível de Risco Inerente (NRI) x Risco de Controle (RC)

Com base nos resultados da análise de riscos, realiza-se a avaliação de riscos que corresponde ao processo de tomada de decisão sobre quais riscos precisam de tratamento e quais serão as estratégias para a implementação do tratamento. Desse modo, a Tabela 8 mostra as diretrizes para a priorização e tratamento de riscos:

Tabela 9 – Diretrizes para priorização e tratamento de riscos

Nível de Risco	Critérios para priorização e tratamento de riscos
Risco Extremo (RE)	Nível de risco **muito além do apetite a risco**. Qualquer risco nesse nível deve ser comunicado à governança e alta administração e ter uma resposta imediata. Postergação de medidas só com autorização do dirigente máximo
Risco Alto (RA)	Nível de risco **além do apetite a risco**. Qualquer risco nesse nível dever ser comunicado a alta administração e ter uma ação tomada em período determinado. Postergação de medidas só com autorização do dirigente de área.
Risco Médio (RM)	Nível de risco **dentro do apetite a risco**. Geralmente nenhuma medida especial é necessária, porém requer atividades de monitoramento específicas e atenção da gerência na manutenção de respostas e controles para manter o risco nesse nível, ou reduzi-lo sem custos adicionais.
Risco Baixo (RB)	Nível de risco **dentro do apetite a risco.** É possível que existam oportunidades de maior retorno que podem ser exploradas assumindo-se mais riscos, avaliando a relação custos x benefícios, como diminuir o nível de controles.

Fonte: Brasil, 2018a

O tratamento de riscos no Cade prevê as seguintes opções que podem ser aplicadas de forma individual ou combinadas para alterar a probabilidade de ocorrência ou o impacto dos riscos (ou ambos):

- Aceitar o risco – conviver com o evento de risco mantendo práticas e procedimentos existentes, ou seja, os riscos precisam ser aceitos e enfrentados para a sobrevivência das partes envolvidas (PORTELA, 2014). Aceitar o risco também pode contribuir para buscar uma oportunidade conforme descrito na norma 31000:2009.

- Transferir o risco – reduzir a probabilidade ou impacto pela transferência ou compartilhamento de uma parte do risco, como por exemplo, seguro, transações de hedge, ou terceirização da atividade, etc.
- Evitar o risco - promover ações que evitem, eliminem ou atenuem em caráter de urgência as causas e/ou consequências.

Por fim, a metodologia estabelece que a estratégia para implementação da gestão de riscos para cada processo crítico do Cade deve conter 10 elementos:

1) Evento/Nível de risco
2) Resposta ao risco
3) Controle proposto
4) Tipo de controle
5) Objetivo do controle
6) Área responsável
7) Responsável pela implementação do controle proposto
8) Como será implementado
9) Interveniente
10) Período de execução

A respeito da Solução Tecnológica, conforme o Relatório de Gestão do Exercício de 2017, foi aprovado o Plano de Gestão de Tecnologia da Informação e Comunicação (PDTIC) 2017-2020 que tem por objetivo ser uma ferramenta de planejamento, gestão e governança das ações relacionadas à tecnologia da informação e comunicação. Algumas medidas no campo da segurança da informação foram listadas, tais como:

- Implantação das soluções de gerenciamento de acessos privilegiados, gerenciamento e correlação de eventos de segurança, gerenciamento de identidades e acessos e gerenciamento de dispositivos móveis;
- Implantação das soluções de segurança para *endpoints*, *datacenters* e ameaças avançadas e de contrainteligência;
- Formalização das normas do Gabinete de Segurança Institucional da Presidência da República (GSI/PR);
- Implementação de processos de governança de TIC, de gestão de riscos, de continuidade de serviços de TIC, de gestão de serviços de TIC, de gestão de programas, portifólios e projetos de TIC;

- Restruturação do *datacenter*;
- Implantação do *site backup*;
- Aprimoramento da solução de Auditoria Interna;
- Implementação da solução de monitoramento inteligente de redes sociais e da *web*.

Sobre esta iniciativa observa-se que o estudo (3) relacionou a gestão de riscos à segurança e um dos resultados apresentados foi o desenvolvimento de um sistema eletrônico de notificação de riscos na intranet do hospital público que permite categorizar os tipos de incidentes que podem ocorrer.

Ademais, para a execução do PDTIC ficou estabelecido um plano de gestão de riscos que contém atividades de planejamento, identificação, análise, planejamento das respostas, monitoramento e controle de riscos do planejamento de TIC. Este plano utiliza análise qualitativa dos riscos que consiste em priorizar os riscos para análise ou ação adicional por meio da avaliação e combinação de sua probabilidade e impacto.

Quanto ao Plano de Riscos, de acordo com a Portaria nº 283/2018, o prazo para a aprovação era até novembro de 2018 após a aprovação da MGRC, entretanto, conforme mencionado anteriormente, a metodologia foi aprovada apenas no final de 2018 e dessa forma, o Plano de Riscos ainda não foi publicado. Além disso, não foram encontradas normas, manuais e procedimentos que, de acordo com a referida Portaria, constituem instrumentos do Modelo de Gerenciamento de Integridade, Riscos e Controles Internos da Gestão do Cade.

5. CONCLUSÃO E RECOMENDAÇÃO

Neste estudo a abordagem sobre risco foi apresentada de maneira genérica, uma vez que toda organização, seja pública ou privada, enfrenta influencias e fatores internos e externos que tornam incerto o alcance dos seus objetivos (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2009), portanto, dependem da tomada de decisão diária para sua subsistência.

Em se tratando da administração pública, foco deste estudo, questões de governança estão associadas ao nível macro, e compreendem mecanismos de liderança e estratégia que na prática permitem avaliar, direcionar e monitorar a atuação da gestão, a fim de conduzir políticas públicas e prestar serviços de interesse da sociedade. Desse modo, o mecanismo de governança mais apropriado na atualidade é o processo de gestão de riscos corporativos que consiste em um processo contínuo destinado a tratar com eficiência os riscos capazes de afetar os objetos ou processos de trabalho nos níveis estratégico, tático e operacional.

Este tema é consideravelmente novo no país, e por esta razão este trabalho teve por objetivo, por um lado, descrever o processo de implantação da gestão de riscos corporativos no Cade para contribuir com o conhecimento científico sobre o tema no âmbito da administração pública no Brasil e, por outro, servir como estudo de caso para outras organizações que desejam implantar a GRC.

Assim, tendo como marco regulatório a IN nº 01/2016, que determinou a todos os órgãos e entidades do Poder Executivo Federal a publicação das suas políticas de gestão de riscos, em 2017 o Cade publicou a Portaria nº 173/2017 que aprovou a Política de Governança, Gestão de Integridade, Riscos e Controles da Gestão. No ano seguinte, esta norma foi revogada pela Portaria nº 283/2018 que incluiu o risco de integridade. A política segue os modelos COSO e ISO 31000:2009.

Para a efetividade da norma, foram instalados o Comitê de Governança, Riscos e Controles – Corisc e o Comitê de Gestão de Riscos – Cerisc, ambos sob o comando da alta direção do Cade indo ao encontro do que determina a norma ISO 31000:2009. Além disso, como o objeto deste estudo é uma autarquia em regime especial, a alta direção tem um prazo de mandato estabelecido de quatro anos, ou seja, diferente das organizações da administração pública direta, não há tanta rotatividade de gestores, o que faz com que seja deduzido que o risco de haver interrupção na implantação da GRC seja menor. Quanto aos gestores de risco, o

Cade estabeleceu que serão detentores de cargo ou função de chefia, institucionalmente definidos no regimento interno como responsável por um ou mais processos de trabalho, cabendo a eles assegurar o gerenciamento de riscos, monitorá-los ao longo do tempo e garantir que as informações necessárias sejam produzidas e estejam disponíveis em todos os níveis da organização. Das sete experiências de estratégias de implantação da GRC que estão no Quadro 1, verifica-se que que os estudos (1) e (4) envolveram todos os níveis da organização para elaborarem suas Políticas de GRC. E nos estudos (1) e (3) realizaram cursos de capacitação para alinhamento conceitual sobre a gestão de riscos. Percebe-se que essas experiências possuem um ponto em comum com as estratégias utilizadas pelo Cade quanto a implantação da GRC.

Como parte do processo de implantação da política, em 2017 foi realizado um Seminário de Gestão de Riscos voltado para os servidores com a finalidade de sensibilização sobre o tema e um curso de introdução à gestão de riscos que teve por objetivo uniformizar conceitos básicos sobre gestão de riscos entre os servidores que atuarão como gestores de riscos. Além disso, foi publicado o Plano de Gestão de Tecnologia da Informação e Comunicação com adoção de medidas no campo da segurança da informação. Capacitação continuada e solução tecnológica são os instrumentos que podem ser considerados como parte da melhoria continuada da estrutura e monitoramento e análise crítica do processo da gestão de riscos. Por ser interativo e dinâmico, as necessidades mudam e deve ser monitorado para saber se a Política permanece válida. No final de 2018 foi concluída a metodologia de gerenciamento de risco, um dos instrumentos estabelecidos na Portaria nº 283/2018 e por fim, gestão de riscos foi contemplada no Planejamento Estratégico 2017-2020 que entre seus objetivos estratégicos destacam-se os projetos implantação do planos de integridade; implantação da governança da gestão de riscos e impantação da gestão de riscos que fazem parte da iniciativa estratégica descrita como adotar boas práticas de gestão e governança relacionada ao OE5; Aprimorar processos de trabalhos com adoção de melhores práticas e inovação.

Estas iniciativas demonstram o compromisso do Cade em garantir o processo de gerenciamento de riscos totalmente integrado em todos os níveis da organização e fortemente alinhado com os objetivos da autarquia. A Política é a declaração das intenções e diretrizes gerais relacionadas à gestão de riscos corporativos e tem a finalidade de fortalecer a governança, o cumprimento da missão do Cade e alcance

dos objetivos institucional, além de promover maior transparência e aprimorar o ambiente de controles internos de gestão da autarquia.

Ressalta-se que a norma ISO 31000:2009, a qual o Cade se baseou para a implantação da GRC, foi cancelada e substituída pela norma 31000:2018. Assim, por ser um processo ainda em fase de implantação e por ser dinâmico, deduz-se que o Cade irá atualizar alguns documentos como a sua Metodologia de Gestão de Riscos, com base na norma de 2018 e agregar o relatório ISO 31004:2015 que apresenta exemplos práticos dos princípios e diretrizes de como se estrutura a gestão de riscos em uma organização.

Além disso, este trabalho limitou-se na coleta de dados secundários, e diante disso, recomenda-se que, para os próximos estudos, sejam realizadas entrevistas para coleta de dados primários, para saber se os gestores da alta direção (Corisc e Cerisc), gestores de riscos, servidores e subcomitês consideram a implantação da GRC necessária e eficaz, se estão de fato envolvidos na implantação da GRC no Cade, e para saber o processo de formação da cultura de gestão de riscos na organização, no intuito de verificar se, após todas as etapas e resultados da implantação da GRC, o Cade pode iniciar a etapa de implementação da GRC.

REFERÊNCIAS

ABNT. Associação Brasileira de Normas Técnicas. ABNT NBR ISO 31000:2009 – Gestão de Riscos: Princípios e Diretrizes, 2009.

ABNT. Associação Brasileira de Normas Técnicas. ABTT NBR 31000:2018 – Gestão de Riscos: Princípios e Diretrizes, 2018.

ABNT. Associação Brasileira de Normas Técnicas. ABNT NBR 31004:2015 – Gestão de Riscos: Guia para implementação, 2015.

ÁVILA, M. D. G. Gestão de riscos no setor público: controle estratégico para um processo decisório eficiente. Revista Científica Semana Acadêmica, v. ano MMXIII, p. 32, 2013. Disponível em: <ttps://semanaacademica.org.br/ artigo/gestao-de-riscos-no-setor-publico-controle-estrategico-para-um-processodecisorio-eficiente>. Acesso em: 04 jun. 2018.

Azevedo, Mateus Miranda de et al. O compliance e a gestão de riscos nos processos organizacionais. Revista de Pós-Graduação Multidisciplinar (RPGM), v. 1, n. 1, p. 1–25, 2017. Disponível em: fics.edu.br/index.php/rpgm/article/view/507. Acesso em: 18 jun. 2018.

BRASIL. Conselho Administrativo de Defesa Econômica. Metodologia de Gestão de Riscos do Cade. Brasília, DF, 2018a.

BRASIL. Conselho Administrativo de Defesa Econômica. Relatório de Gestão do Exercício de 2017. Brasília, DF, 2017.

BRASIL. Conselho Administrativo de Defesa Econômica. Planejamento Estratégico 2017-2020. Brasília, DF, 2018b.

BRASIL. Conselho Administrativo de Defesa Econômica. Plano de Gestão de Tecnologia da Informação e Comunicação. Brasília, DF, 2018c.

BRASIL. **Constituição (1988)**. Constituição da República Federativa do Brasil. Disponível em: < http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 20 jun. 2018.

BRASIL. **Controladoria Geral da União** – CGU. Portaria nº 1.089 de 25 de abril de 2018.

BRASIL. **Decreto**, de 22 de novembro de 2017. Disponível em: https://www2.camara.leg.br/legin/fed/decret/2017/decreto-9203-22-novembro-2017-785782-publicacaooriginal-154277-pe.html. Acesso em 17 abr de 2019.

BRASIL. **Instrução Normativa**, de 10 de maio de 2016. Disponível em: < https://www.cgu.gov.br/sobre/legislacao/arquivos/instrucoes-normativas/in_cgu_mpog_01_2016.pdf>. Acesso em: 23 jun. 2018.

BRASIL. **Lei,** de 11 de junho de 1994. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8884.htm. Acesso em: 15 abr. 2019.

BRASIL. **Lei**, de 30 de novembro de 2011. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2011/Lei/l12529.htm. Acesso em: 15 abr. 2019.

BRASIL. **Tribunal de Contas da União** – TCU. Portaria nº 9, de 18 de maio de 2017.

BRAGA, M. A. V. Risco Bottom Up: Uma reflexão sobre o desafio da implementação da gestão de riscos no setor público brasileiro. Revista da Controladoria-Geral da União. V. 9, n. 15, 2017. Disponível em < https://ojs.cgu.gov.br/index.php/Revista_da_CGU/article/view/103/pdf_41>. Acesso em 20 ago. 2018.

CADE. Histórico do Cade. Cade, 2016. Disponível em < http://www.cade.gov.br/acesso-a-informacao/institucional/historico-do-cade>. Acesso em 5 abr 2019.

COSO – Committee of Sponsoring Organizations of the Treadway Commission. Gerenciamento de Riscos Corporativos - Estrutura Integrada. Edição brasileira patrocinada pela PriceWaterhouseCoopers e Audibra. 2007. Disponível em: < https://www.coso.org/Documents/COSO-ERM-Executive-Summary-Portuguese.pdf>. Acesso em 20 jun. 2018.

Conselho Administrativo de Defesa Econômica (Cade). Cartilha do Cade. Disponível em http://www.cade.gov.br/acesso-a-informacao/publicacoes-institucionais/cartilha-do-cade.pdf. Acesso em 20 abr. 2019.

DA SILVA, Carlos Eduardo Sanches et al. Aplicação do gerenciamento de riscos no processo de desenvolvimento de produtos em empresas de autopeças. Production, v. 20, n. 2, p. 200-213, 2010.

DAFT, R. L. **Administração**. São Paulo: Thomsom, 2005.

DESTRO, Mayara Coutinho Análise da estruturação da gestão de risco institucional: o caso Embrapa. 2014. 121 f., il. Monografia (Bacharelado em Comunicação Social) — Universidade de Brasília, Brasília, 2014.

DOMINGUES, I, O. Práticas de controle interno e gestão de riscos corporativos em

um grupo de companhias aéreas brasileiras. Dissertação (Mestrado em Ciências Contábeis) – Fundação Escola de Comércio Álvares Penteado. São Paulo, 2016.

FERNANDES, Eduardo da Silva. Aplicação de sistemática de gestão de riscos no processo de aquisição suprimentos em uma instituição pública brasileira. 2019.

FREIRE, Antonio Emilio Bastos de Aguiar. Implementação da gestão de riscos em empresas estatais: estudo de Caso do METRÔ-DF. 2017. 57 f., il. Trabalho de conclusão de Curso (Especialização em Controle Externo)—Universidade de Brasília, Brasília, 2017.

GASPARY, Lisiane Valdez et al. Implementação da gestão de risco e disseminação da cultura de segurança: desafios de um hospital público. **Revista Acreditação**, v. 7, n. 13, p. 60-76, 2017.

GIL, Antonio Carlos. Administração de Recursos Humanos: um enfoque profissional. São Paulo: Atlas, 2002.

GONZALEZ, R. S. **Governança Corporativa**. São Paulo: Trevisan Editora. 2012.

GUIMARÃES, I. C; PARISI, C; WEFFORT, E. F. J. A importância da Controladoria na gestão de riscos das empresas não-financeiras: um estudo da percepção de gestores de riscos e controllers. **Revista Brasileira de Gestão de Negócios**, v. 11, n 32, p. 260-275, 2009.

MARTINS, Mary Anne Fontenele et al. Política de gestão de riscos corporativos: o caso de uma agência reguladora da saúde. Revista do Serviço Público, v. 69, n. 1, p. 7-32, 2018.

NOGUEIRA, Fernando Rocha et al. Políticas públicas regionais para gestão de riscos: o processo de implementação no ABC, SP. **Ambiente & Sociedade**, v. 17, n. 4, 2014.

PORTELA, Gerardo. **Gerenciamento de Riscos Baseado em Fatores Humanos e Cultura de Seg: Estudo de Caso de Simulação Computacional do Comportamento Humano**. Elsevier Brasil, 2014.

PRODANOV, Cleber Cristiano; DE FREITAS, Ernani Cesar. **Metodologia do trabalho científico: métodos e técnicas da pesquisa e do trabalho acadêmico-2ª Edição**. Editora Feevale, 2013.

ROSA, M. F. E. Direito Administrativo. São Paulo: Saraiva, 2004.

SANTOS, M. J. A. Auditoria de Gestão de Riscos: o novo olhar do Tribunal de Contas da União. Revista de Auditoria Governança e Contabilidade. Rio de Janeiro.2018. Disponível em: <

http://www.fucamp.edu.br/editora/index.php/ragc/article/view/1195>. Acesso em 23 ago. 2018.

SANTOS, Rubens Ferreira dos. Gestão de riscos aplicada a processo de concessão de financiamento imobiliário. 2014. xiii, 202 f., il. Dissertação (Mestrado Profissional em Computação Aplicada) Universidade de Brasília, Brasília, 2014.

SENA, R. R.C. O gerenciamento de risco das atividades de Defesa Civil no estado do Ceará. **Revista Diálogos Acadêmicos**, v. 5, n. 2, 2016.

SOUZA, Jackson Gomes Soares et al. Gestão de riscos de segurança da informação e sua apresentação na governança de TI da administração pública. In: X WORKSHOP DE PÓS-GRADUAÇÃO E PESQUISA DO CENTRO **PAULO SOUZA**. 2015.

VERGARA, S. C. Projetos e relatórios de pesquisa em administração. São Paulo: Atlas, 2009.