Enap Escola Nacional de Administração Pública

Implementando a Gestão de riscos no setor público

Módulo 1 Introdução à Gestão de Riscos: Estruturas de Gerenciamento e Bases Normativas

Brasília - 2018

Conteúdo para impressão

Fundação Escola Nacional de Administração Pública

Presidente
Francisco Gaetani

Diretor de Educação Continuada
Paulo Marques

Coordenadora-Geral de Educação a Distância
Natália Teles da Mota Teixeira

Conteudista
Rodrigo Fontenelle de Araújo Miranda

Desenvolvimento do curso realizado no âmbito do acordo de Cooperação Técnica FUB/CDT/Laboratório Latitude e Enap.

Enap Escola Nacional de Administração Pública
Diretoria de Educação Continuada
SAIS - Área 2-A - 70610-900 — Brasília, DF
Telefone: (61) 2020 3096 - Fax: (61) 2020 3178

SUMÁRIO

Enap
Enap
Enap

Módulo 1 Introdução à Gestão de Riscos: Estruturas de Gerenciamento e Bases Normativas

1. Introdução

Olá! Seja bem-vinda(o) ao curso Implementando a Gestão de Riscos no Setor Público, concebido pelo Ministério do Planejamento, Desenvolvimento e Gestão (MP) em parceria com a Enap em 2017 e adaptado, no mesmo ano, para ser ofertado na modalidade a distância.

O curso foi desenvolvido com foco na necessidade de implementação da Metodologia de Gerenciamento de Riscos, no contexto do Modelo desenvolvido pelo MP (Política, Instâncias de Supervisão, Metodologia e Solução Tecnológica). Esta metodologia tem por finalidade orientar a identificação, a avaliação e a adoção de respostas aos eventos de riscos dos processos da unidade, bem como instruir sobre o monitoramento e reporte.

A incerteza ou o risco é inerente a praticamente todas as atividades humanas. No mundo corporativo onde as empresas estão expostas a uma miríade de incertezas originadas de fatores econômicos, sociais, legais, tecnológicos e operacionais, a gestão de integridade, riscos e controles internos é crucial para que se alcancem os objetivos estratégicos.

Algumas das funções da gestão de riscos são assegurar o alcance dos objetivos, por meio da identificação antecipada dos possíveis eventos que poderiam ameaçar o atingimento dos objetivos, o cumprimento de prazos, leis e regulamentos etc., implementar uma estratégia evitando o consumo intenso de recursos para solução de problemas quando esses surgem inesperadamente, bem como melhorar continuamente os processos organizacionais.

No ambiente de trabalho, muitas vezes as organizações se deparam com fatores internos e externos que tornam incerto o êxito do atingimento dos objetivos do projeto ou da atividade que se encontra em desenvolvimento. Independentemente da área em que se atua, e até na vida pessoal, os riscos podem afetar o andamento da ação, levando-a a uma direção completamente diferente daquela inicialmente planejada.

As responsabilidades do governo em relação ao bem público exigem a adoção de práticas e estratégias eficazes de gestão. Neste contexto, a gestão de riscos torna-se uma importante ferramenta para ajudar na tomada de decisões baseadas em metodologias e normas que geram, dentre outros benefícios, a redução ou a eliminação de retrabalhos.

A partir disso, e considerando que a implementação da gestão de riscos no setor público ainda é incipiente, elaboramos esse curso com o objetivo de agregar valor às organizações, por meio da capacitação teórica e prática de gestores, dando a eles ferramentas para desenvolverem o projeto de gestão de riscos em seus próprios órgãos.

O curso é baseado no Manual de Gestão de Riscos do Ministério do Planejamento, Desenvolvimento e Gestão (MP), que aprovou sua Política de Gestão de Riscos, Integridade e Controles Internos da Gestão por meio da Portaria MP nº 426/2016.

Desejamos um excelente estudo!

2. Gestão de riscos: base teórica

Embora exista uma grande quantidade de *frameworks* de gestão de riscos mundialmente reconhecidos, tais como ISO 31000, *Orange Book* do Tesouro Britânico, dentre outras, esse curso foi baseado na estrutura do COSO ERM, com a metodologia construída pelo MP. Esse *framework* é definido pela Portaria nº 426/2016, que aprovou a política de gestão de integridade, riscos e controles internos da gestão daquele Ministério.

Portanto, nos próximos tópicos, exploraremos o significado dos *frameworks* que formam a base teórica da referida portaria e que são fundamentais para o alcance dos objetivos de nosso curso. Vamos lá!

2.1 COSO ERM

Committee of Sponsoring Organizations (COSO) é o Comitê das Organizações Patrocinadoras da Comissão Nacional sobre Fraudes em Relatórios Financeiros. Criada em 1985, é uma entidade do setor privado – ou seja, iniciativa independente –, sem fins lucrativos, voltada para o aperfeiçoamento da qualidade de relatórios financeiros, principalmente para estudar as causas da ocorrência de fraudes em relatórios financeiros. Cabe ressaltar que a origem do modelo COSO está relacionada a um grande número de escândalos financeiros na década de 1970 nos Estados Unidos, que colocaram em dúvida a confiabilidade dos relatórios corporativos.

De acordo com o Comitê, Controle Interno é:

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

Em 2004, o COSO divulgou o trabalho "Gerenciamento de Riscos Corporativos – Estrutura Integrada (COSO ERM)", com um foco mais voltado para o gerenciamento de riscos corporativos, que definiu gerenciamento de riscos corporativos da seguinte forma:

> **É um processo conduzido em uma organização pelo conselho de administração, diretoria e demais empregados, aplicado no estabelecimento de estratégias formuladas para identificar, em toda a organização, eventos em potencial, capazes de afetá-la, e administrar os riscos de modo a mantê-los compatíveis com o apetite a risco da organização e possibilitar garantia razoável do cumprimento dos seus objetivos. (COSO ERM, 2004)**

2.2 ISO 31000

A ABNT NBR ISO 31000 foi elaborada pela Comissão de Estudo Especial de Gestão de Riscos (CEE- 63), sendo uma adoção idêntica, em conteúdo técnico, estrutura e redação, à ISO

31000:2009, que foi elaborada pela ISO *Technical Management Board Working Group on risk management* (ISO/TMB/WG), conforme ISO/IEC Guide 21-1:2005.

Quando implementada e mantida de acordo com essa Norma, a gestão dos riscos possibilita à organização inúmeros benefícios dos quais destacamos:

- aumentar a probabilidade de atingir os objetivos;
- encorajar uma gestão proativa;
- estar atento para a necessidade de identificar e tratar os riscos através de toda a organização;
- melhorar a identificação de oportunidades e ameaças;
- atender às normas internacionais e requisitos legais e regulatórios pertinentes;
- melhorar o reporte das informações financeiras;
- melhorar a governança;
- melhorar a confiança das partes interessadas;
- estabelecer uma base confiável para a tomada de decisão e o planejamento;
- melhorar os controles;
- alocar e utilizar eficazmente os recursos para o tratamento de riscos;
- melhorar a eficácia e a eficiência operacional;
- melhorar o desempenho em saúde e segurança, bem como a proteção do meio ambiente;
- melhorar a prevenção de perdas e a gestão de incidentes;
- minimizar perdas;
- melhorar a aprendizagem organizacional; e
- aumentar a resiliência da organização.

A ISO 31000 fornece princípios e diretrizes genéricas para a gestão de riscos, podendo ser utilizada por qualquer empresa pública, privada ou comunitária, associação, grupo ou indivíduo. Portanto, não é específica para qualquer indústria ou setor.

Embora forneça diretrizes genéricas, a ISO 31000 não pretende promover a uniformidade da gestão de riscos entre organizações. A concepção e a implementação de planos e estruturas para gestão de riscos precisarão levar em consideração as necessidades variadas de uma organização específica, seus objetivos, contexto, estrutura, operações, processos, funções, projetos, produtos, serviços ou ativos e práticas específicas empregadas.

Princípios da ISO 31000

Segundo essa norma, para a gestão de riscos ser eficaz, convém que uma organização, em todos os níveis, atenda aos princípios abaixo descritos.

A gestão de riscos cria e protege valor.

A gestão de riscos contribui para a realização demonstrável dos objetivos e para a melhoria do desempenho referente, por exemplo, à segurança e saúde das pessoas, à segurança, à conformidade legal e regulatória, à aceitação pública, à proteção do meio ambiente, à qualidade do produto, ao gerenciamento de projetos, à eficiência nas operações, à governança e à reputação.

A gestão de riscos é parte integrante de todos os processos organizacionais.

A gestão de riscos não é uma atividade autônoma separada das principais atividades e processos da organização. A gestão de riscos faz parte das responsabilidades da administração e é parte integrante de todos os processos organizacionais, incluindo o planejamento estratégico e todos os processos de gestão de projetos e gestão de mudanças.

A gestão de riscos é parte da tomada de decisões.

A gestão de riscos auxilia os tomadores de decisão a fazer escolhas conscientes, priorizar ações e distinguir entre formas alternativas de ação.

A gestão de riscos aborda explicitamente a incerteza.

A gestão de riscos explicitamente leva em consideração a incerteza, a natureza dessa incerteza, e como ela pode ser tratada.

A gestão de riscos é sistemática, estruturada e oportuna.

Uma abordagem sistemática, oportuna e estruturada para a gestão de riscos contribui para a eficiência e para os resultados consistentes, comparáveis e confiáveis.

A gestão de riscos baseia-se nas melhores informações disponíveis.

As entradas para o processo de gerenciar riscos são baseadas em fontes de informação, tais como dados históricos, experiências, retroalimentação das partes interessadas, observações, previsões, e opiniões de especialistas. Entretanto, convém que os tomadores de decisão se informem e levem em consideração quaisquer limitações dos dados ou modelagem utilizados, ou a possibilidade de divergências entre especialistas.

A gestão de riscos é feita sob medida.

A gestão de riscos está alinhada com o contexto interno e externo da organização e com o perfil do risco.

A gestão de riscos considera fatores humanos e culturais.

A gestão de riscos reconhece as capacidades, percepções e intenções do pessoal

interno e externo que podem facilitar ou dificultar a realização dos objetivos da organização.

A gestão de riscos é transparente e inclusiva.

O envolvimento apropriado e oportuno de partes interessadas e, em particular, dos tomadores de decisão em todos os níveis da organização assegura que a gestão de riscos permaneça pertinente e atualizada. O envolvimento também permite que as partes interessadas sejam devidamente representadas e tenham suas opiniões levadas em consideração na determinação dos critérios de risco.

A gestão de riscos é dinâmica, iterativa e capaz de reagir a mudanças.

A gestão de riscos continuamente percebe e reage às mudanças. Na medida em que acontecem eventos externos e internos, o contexto e o conhecimento modificam-se, o monitoramento e a análise crítica de riscos são realizados, novos riscos surgem, alguns se modificam e outros desaparecem.

A gestão de riscos facilita a melhoria contínua da organização.

Convém que as organizações desenvolvam e implementem estratégias para melhorar a sua maturidade na gestão de riscos juntamente com todos os demais aspectos da sua organização.

Por fim, em relação ao processo de gestão de riscos, segundo a ISO 31000, convém que ele seja parte integrante da gestão, incorporado na cultura e nas práticas e adaptado aos processos de negócios da organização. A imagem abaixo sintetiza o processo de gestão de riscos:

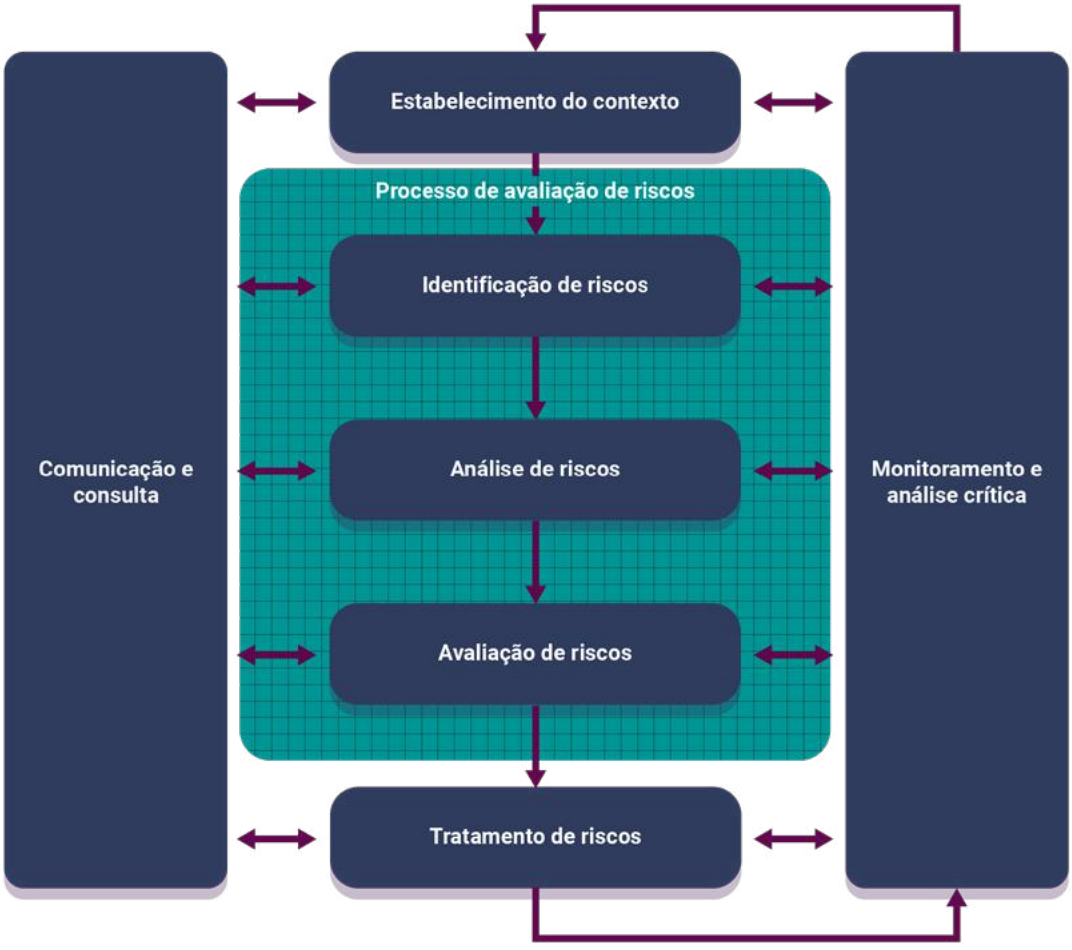

Figura 4 — Processo de gestão de riscos segundo a ISO 31000

2.3 ORANGE BOOK

O documento "*The Orange Book Management of Risk - Principles and Concepts*" (Gerenciamento de Riscos – Princípios e Conceitos) foi produzido e publicado pelo HM *Treasury* do Governo Britânico (Orange Book), sendo amplamente utilizado como a principal referência do Programa de Gerenciamento de Riscos do Governo do Reino Unido, iniciado em 2001. O documento foi atualizado em 2004.

Segundo o Projeto de Desenvolvimento do Guia de Orientação para o Gerenciamento de Riscos desenvolvido pelo MP, Programa Gespública, o *Orange Book* tem como vantagens, além de ser compatível com padrões internacionais de gerenciamento de riscos, apresentar uma introdução ao tema gerenciamento de riscos, tratando de forma abrangente e simples um tema tão complexo.

Ainda do ponto de vista do referido Projeto, riscos devem ser gerenciados em três níveis: estratégico, de programas e de projetos e atividades. A organização deve ser capaz de gerenciar riscos nos três níveis. Vejamos alguns detalhes sobre cada um destes níveis:

Nível Estratégico

Neste nível, acontece o contrato político do Governo com a sociedade e é estabelecida a coerência do seu programa de Governo. As decisões aqui tomadas envolvem a formulação dos objetivos estratégicos e as prioridades para a alocação de recursos públicos em alinhamento com as políticas públicas.

Nível Programa

Neste nível, encontram-se as decisões de implementação e gerenciamento de programas temáticos previstos no nível estratégico, através dos quais são executadas as políticas e as ações prioritárias de Governo.

Nível Projetos e Atividades

Neste nível, encontram-se os projetos que contribuirão para o atingimento dos objetivos dos Programas, e as atividades relativas aos processos finalísticos. As lideranças em todos os níveis da organização devem estar conscientes, capacitadas e motivadas com relação à relevância do gerenciamento de riscos nos três níveis, que são interdependentes.

A imagem abaixo representa a estrutura de apresentação hierárquica desses níveis e evidencia que a comunicação deve fluir tanto de cima para baixo, quanto de baixo para cima, vejamos:

Figura 5: A comunicação deve fluir nos três níveis de gerenciamento de riscos.

3. Declaração de posicionamento: as três linhas de defesa

Esse modelo ficou conhecido e foi amplamente difundido a partir da *Declaração de Posicionamento do The Institute of Internal Auditors* (IIA): o modelo de Três Linhas de Defesa no gerenciamento eficaz de riscos e controles é uma forma simples e eficaz de melhorar a comunicação do gerenciamento de riscos e controle por meio do esclarecimento dos papéis e responsabilidades essenciais.

O modelo apresenta um novo ponto de vista sobre as operações, ajudando a garantir o sucesso contínuo das iniciativas de gerenciamento de riscos, e é aplicável a qualquer organização – não importando seu tamanho ou complexidade.

No modelo de Três Linhas de Defesa, o controle da gerência é a primeira linha de defesa no gerenciamento de riscos, as diversas funções de controle de riscos e supervisão de conformidade estabelecidas pela gerência são a segunda linha de defesa, e a avaliação independente é a terceira. Cada uma dessas três “linhas” desempenha um papel distinto dentro da estrutura mais ampla de governança da organização. A imagem abaixo apresenta a esquematização deste modelo:

Figura 6: Modelo 3 Linhas de Defesa, adaptado de Guidance on the 8th EU Company Law Directive da ECIIA/FERMA, artigo 41.

Agora detalharemos alguns pontos importantes sobre esse modelo:

- 1ª Linha de Defesa: Gestão Operacional

Como primeira linha de defesa, os gerentes operacionais gerenciam os riscos e têm propriedade sobre eles. Eles também são os responsáveis por implementar as ações corretivas para resolver deficiências em processos e controles.

Sendo assim, a gerência operacional é responsável por manter controles internos eficazes e por conduzir procedimentos de riscos e controle diariamente. Faz parte de suas atribuições identificar, avaliar, controlar e mitigar os riscos, guiando o desenvolvimento e a implementação de políticas e procedimentos internos para garantir que as atividades estejam de acordo com as metas e objetivos.

Por meio de uma estrutura de responsabilidades em cascata, os gerentes do nível médio desenvolvem e implementam procedimentos detalhados que servem como controles e supervisionam a execução, por parte de seus funcionários, desses procedimentos.

- 2ª Linha de Defesa: Funções de gerenciamento de riscos e conformidade

As funções específicas variam entre organizações e indústrias, mas, quando se trata das funções típicas, temos três importantes características (ou atividades):

a) função (e/ou comitê) de gerenciamento de riscos: facilita e monitora a implementação de práticas eficazes de gerenciamento de riscos por parte da gerência operacional. Além disso, auxilia os proprietários dos riscos (ou seja, a alta administração da organização) a definir a meta de exposição ao risco e a reportar adequadamente informações relacionadas a riscos em toda a organização;

b) função de conformidade: monitora diversos riscos específicos, tais como a não conformidade com as leis e regulamentos aplicáveis. Nesse quesito, a função reporta diretamente à alta administração e, em alguns setores do negócio, diretamente ao órgão de governança. Múltiplas funções de conformidade existem frequentemente na mesma organização, com responsabilidade por tipos específicos de monitoramento da conformidade, como saúde e segurança, cadeia de fornecimento, ambiental e monitoramento da qualidade;

c) função de controladoria: monitora os riscos financeiros e questões de reporte financeiro.

- 3ª Linha de Defesa: Auditoria Interna

Os auditores internos fornecem ao órgão de governança e à alta administração avaliações abrangentes baseadas no maior nível de independência e objetividade dentro da organização.

É importante destacar que esse alto nível de independência não está disponível na segunda linha de defesa. A auditoria interna promove avaliações sobre a eficácia da governança, do gerenciamento de riscos e dos controles internos, incluindo a forma como a primeira e a segunda linhas de defesa alcançam os objetivos de gerenciamento de riscos e controle.

Embora os órgãos de governança e a alta administração não sejam considerados dentre as três "linhas" desse modelo, nenhuma discussão sobre sistemas de gerenciamento de riscos estaria completa sem considerar, em primeiro lugar, os papéis essenciais dos órgãos de governança e da alta administração. Os órgãos de governança e a alta administração são as principais partes interessadas atendidas pelas "linhas" e são as partes em melhor posição para ajudar a garantir que o modelo de Três Linhas de Defesa seja aplicado aos processos de gerenciamento de riscos e controle da organização.

4. Normas e regulamentações relacionadas

No âmbito da Administração Pública Federal, existe um conjunto de normas e regulamentações relacionadas à temática de gestão de integridade, riscos e controles, dentre elas destacamos as mais relevantes:

- Instrução Normativa Conjunta CGU/MP nº 1, de 10 de maio de 2016, dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo federal.

- Portaria nº 150, de 4 de maio de 2016, institui o Programa de Integridade e o Comitê de Gestão Estratégica do Ministério do Planejamento, Desenvolvimento e Gestão e Portaria nº 425, de 30 de dezembro de 2016, que altera a Portaria MP nº 150, de 4 de maio de 2016, que instituiu o programa de Integridade e o Comitê de Gestão Estratégica do Ministério do Planejamento, Desenvolvimento e Gestão.

- Política de Gestão de Integridade, Riscos e Controles Internos da Gestão, Portaria nº 426, de 30 de dezembro de 2016, dispõe sobre a instituição da Política de Gestão de Integridade, Riscos e Controles da Gestão do Ministério do Planejamento, Desenvolvimento e Gestão.

- Resolução CEG/MF nº 05/2014, que institui o Comitê de Gestão Integrada de Riscos Corporativos no âmbito do Programa de Modernização Integrada do Ministério da Fazenda (PMIMF).

- Portaria MPS nº 534/2014, que estabelece princípios e diretrizes para a gestão de riscos no âmbito do Ministério da Previdência Social e de suas entidades vinculadas, dá outras providências.

- Portaria MPS nº 08/2015, que aprova o Manual de Gerenciamento de Riscos, no âmbito do Ministério da Previdência Social e de suas entidades vinculadas.

Embora reconheçamos que a lista acima não é exaustiva, os normativos mencionados possibilitam às organizações uma excelente fonte de consulta para a implementação da gestão de riscos.

5. Revisando o módulo

Chegamos ao final do módulo 1. Nesta etapa inicial do curso, você aprendeu muitas informações importantes sobre gestão de riscos. Revise-as com atenção nos tópicos abaixo. Algumas das funções da gestão de riscos são assegurar o alcance dos objetivos, por meio da identificação antecipada dos possíveis eventos que poderiam ameaçar o atingimento dos objetivos, o cumprimento de prazos, leis e regulamentos etc., implementar uma estratégia evitando o consumo intenso de recursos para solução de problemas quando esses surgem inesperadamente, bem como melhorar continuamente os processos organizacionais.

- Neste módulo, vimos que existem diversas estruturas de gerenciamento de riscos mundialmente conhecidas e analisamos os principais pontos das três mais utilizadas, a saber: COSO ERM, ISO 31000 e *Orange Book.*

- No modelo de Três Linhas de Defesa, vimos que o controle da gerência é a primeira linha de defesa no gerenciamento de riscos, as diversas funções de controle de riscos e supervisão de conformidade estabelecidas pela gerência são a segunda linha de defesa, e a avaliação independente é a terceira.

Assista aos vídeos correspondentes a esse módulo e responda à Atividade Avaliativa. No próximo módulo, conheceremos a estrutura do COSO ERM. Até breve!

Referências

ABNT. Associação Brasileira de Normas Técnicas. **Gestão de Riscos**: Princípios e Diretrizes. Norma Brasileira ABNT NBR ISO 31000. 1. ed. São Paulo: ABNT, 2009.

AHP. Analytic Hierarchy Process. **Excel MS Excel 2010.** Modelo AHP desenvolvido por Goepel, Klaus D., modelo BPMSG AHP Excel. Disponível em: <http://bpmsg.com>. Acesso em 3 out. 2017. Versão de livre uso.

BB. Banco do Brasil. Diretoria de Controles Internos. **Priorização de Processos, Escopo de Atuação**. Visita Técnica em 26 jul. 2015.

BCB. Banco Central do Brasil. **Fundamentos de Gestão de Riscos Não-Financeiros**. Disponibilizada pela UniBacen. Curso realizado de 30/06 a 06/07/2015.

_____. Ministério do Planejamento. **Projeto de Desenvolvimento do Guia de Orientação para o Gerenciamento de Riscos**. Programa Gespública. Secretaria de Gestão Pública. Brasília, 2013.

_____. Ministério do Planejamento. **O Modelo de Excelência em Gestão Pública. Programa Gespública.** Secretaria de Gestão Pública. Brasília, 2014a.

_____. Ministério do Planejamento. **Instrumento para Avaliação da Gestão Pública. Programa Gespública.** Secretaria de Gestão Pública. Brasília, 2014b.

_____. Tribunal de Contas da União. Processo TC 020.905/2014-9. **Relatório de Levantamento de Auditoria,** Acórdão nº 927/2015 - TCU Plenário, Brasília, 2014c.

_____. Tribunal de Contas da União. **Avaliação de controles internos na administração pública federal,** 2012. Disponível em <http://portal2.tcu.gov.br/portal/pls/portal/docs/2436815.PDF>. Acesso em 14. set. 2013.

BRITO, Claudenir; FONTENELLE, Rodrigo. **Auditoria privada e governamental:** Teoria de forma objetiva e mais de 500 questões comentadas. 3. ed. Niterói: Impetus, 2016.

COSO ERM. **Gerenciamento de Riscos Corporativos** - Estrutura Integrada, 2004.

COSO. **Gerenciamento de Riscos Corporativos** – Estrutura Integrada. Tradução: Instituto dos Auditores Internos do Brasil (Audibra) e Pricewaterhouse Coopers Governance, Risk and Compliance, Estados Unidos da América, 2007.

IIA. **As Três Linhas de Defesa no Gerenciamento Eficaz de Riscos e Controles.** Disponível em: <https://na.theiia.org/standards-guidance/Public%20Documents>. Acesso em: 17. nov. 2015.
IBGC. INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA. Guia de Orientação para Gerenciamento de Riscos Corporativos.

INTOSAI GOV 9100. **Guidelines for Internal Controls Standards for the Public Sector.** 2004. Disponível em: <http://www.intosai.org/en/issai-executive-summaries/intosai- guidance-for-good-governance-intosai-gov.html >. Acesso em: 28 out. 2015.

ISO. International Organization for Standardization. **Risk Management System – Principles and Guidelines**. ISO 31000. Tradução: Associação Brasileira de Normas Técnicas (ABNT) Projeto 63:000.01- 001. Agosto, 2009.

_____. **Vocabulary for Risk Management,** ISO Guide 73, 2009.

KPMG. **The Audit Committee's Role in Control and Management of Risk.**

MIRANDA, Rodrigo F. A. **Implementando a Gestão de Riscos no Setor Público**. Belo Horizonte: Ed. Fórum, 2017.