



**UNIVERSIDADE FEDERAL DE SERGIPE  
PRÓ-REITORIA DE PÓS-GRADUAÇÃO E PESQUISA – POSGRAP  
MESTRADO PROFISSIONAL EM ADMINISTRAÇÃO PÚBLICA EM  
REDE NACIONAL – PROFIAP**

**RIVALDO JOSÉ RODRIGUES DE LIMA**

**GESTÃO DE RISCOS NA ADMINISTRAÇÃO PÚBLICA:  
UMA PROPOSTA DE CONTRIBUIÇÃO PARA O GERENCIAMENTO DE RISCOS  
NA UNIVERSIDADE FEDERAL DE SERGIPE**

SÃO CRISTÓVÃO  
2022

RIVALDO JOSÉ RODRIGUES DE LIMA

**GESTÃO DE RISCOS NA ADMINISTRAÇÃO PÚBLICA:  
UMA PROPOSTA DE CONTRIBUIÇÃO PARA O GERENCIAMENTO DE RISCOS  
NA UNIVERSIDADE FEDERAL DE SERGIPE**

Trabalho de Conclusão apresentado ao Programa de Mestrado Profissional em Administração Pública em Rede Nacional – PROFIAP – realizado na Universidade Federal de Sergipe, como requisito para a obtenção do título de Mestre em Administração Pública.

Orientador: Professor Dr. Marcos Eduardo Zambanini

SÃO CRISTÓVÃO  
2022

**FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECA CENTRAL  
UNIVERSIDADE FEDERAL DE SERGIPE**

L732g Lima, Rivaldo José Rodrigues de  
Gestão de riscos na administração pública : uma proposta de  
contribuição para o gerenciamento de riscos na Universidade  
Federal de Sergipe / Rivaldo José Rodrigues de Lima ; orientador  
Marcos Eduardo Zambanini. – São Cristóvão, SE, 2022.  
166f. : il.

Dissertação (mestrado Profissional em Administração Pública)  
– Universidade Federal de Sergipe, 2022.

1.Administração. 2. Administração pública. 3. Universidade  
Federal de Sergipe. I. Zambanini, Marcos Eduardo, orient. II.  
Título.

CDU 658:005. 6(813.7)

**UNIVERSIDADE FEDERAL DE SERGIPE**  
**PRÓ-REITORIA DE PÓS-GRADUAÇÃO E PESQUISA**  
**MESTRADO PROFISSIONAL EM ADMINISTRAÇÃO PÚBLICA**

**ATA DA DEFESA DO TRABALHO DE CONCLUSÃO FINAL**

Aos vinte e um dias de janeiro de dois mil e vinte e dois foi realizada através de apresentação on-line a Banca de Defesa de Dissertação de Mestrado Profissional do discente **Rivaldo José Rodrigues de Lima, Matrícula: 201921000573** com o título do trabalho de conclusão final: "**GESTÃO DE RISCOS NA ADMINISTRAÇÃO PÚBLICA: Uma proposta de contribuição para o gerenciamento de riscos na Universidade Federal de Sergipe.**" A banca examinadora foi composta pelos seguintes membros: Prof. Dr. Marcos Eduardo Zambanini (Presidente/Orientador), Dr. Marcos Vinícius Nascimento Gonzalez Castaneda (Economista/UFS) e Prof. Dr. Álvaro Fabiano Pereira de Macedo (PROFIAP/UFERSA). Após a apresentação, foi passada a palavra a banca que arguiu o discente e o mesmo respondeu aos questionamentos. O presidente e orientador fez as considerações e em seguida deliberaram pela **APROVAÇÃO** do aluno.

Cidade Universitária Prof. José Aloísio de Campos. São Cristóvão - SE, 21 de janeiro de 2022.

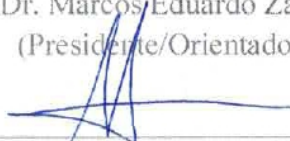
Documento assinado digitalmente

gov.br

Marcos Eduardo Zambanini  
Data: 21/01/2022 16:21:03-0300  
Verifique em <https://verificador.iti.br>

---

Prof. Dr. Marcos Eduardo Zambanini  
(Presidente/Orientador)



---

Dr. Marcos Vinícius Nascimento Gonzalez Castaneda  
(Economista/UFS)

ALVARO FABIANO  
PEREIRA DE MACEDO  
Assinado de forma digital por  
ALVARO FABIANO PEREIRA DE  
MACEDO  
Dados: 2022.01.21 16:14:03 -03'00'

---

Prof. Dr. Álvaro Fabiano Pereira de Macedo  
(PROFIAP/UFERSA)

Documento assinado digitalmente

gov.br

RIVALDO JOSE RODRIGUES DE LIMA  
Data: 27/01/2022 13:47:07-0300  
Verifique em <https://verificador.iti.br>

---

Rivaldo José Rodrigues de Lima  
(Discente/PROFIAP/UFS)

## **AGRADECIMENTOS**

Dignos da minha profunda gratidão são todos aqueles que, de alguma forma, contribuíram para permitir que o objetivo buscado nesta jornada fosse alcançado. São familiares, amigos, professores, colegas de trabalho e de curso que, cada um ao seu modo, me proporcionaram a energia necessária para seguir em frente sempre que uma nova barreira surgia.

À minha senhora, Sandra Araújo, e aos meus filhos e netos, mãe e irmãos, meus especiais agradecimentos, sobretudo pela compreensão da ausência, ainda que não física.

À Rede PROFIAP, por me permitir acessar o seu corpo discente e, por consequência, receber lições de professores primorosos, a exemplo de César Henriques, Florence Cavalcanti, Jussara Jacintho, Kleber Fernandes, Marcos Zambanini, Rozana Rivas, Tácito Farias e Thaís Ettinger, assim como por me possibilitar conviver, na condição de colega de turma, com pessoas de mentes brilhantes, como são os meus colegas Arthur Lincoln, Baby de Fátima, Claudimir Júnior, Daniel Almeida, Diego Rodrigues, Kátia Ferreira, Luiz Gustavo Gurgel, Marcela Felizola, Valdemar Neto e Vinícius Nascimento, aos quais agradeço imensamente.

Ao meu querido líder, mestre e orientador, Marcos Eduardo Zambanini, por toda a paciência e dedicação dispensadas ao longo desta caminhada.

Aos meus colegas de trabalho no Departamento de Administração da UFS, pelas palavras de incentivo e o inarredável apoio de sempre, o que estendo aos nobres colegas integrantes do laborioso Comitê de Gestão de Riscos e Controle da Universidade Federal de Sergipe.

À prestimosa colega Elisângela Andrade, pessoa que, com descomunal dedicação e respeito, honra a expressão “serviço público” à frente da Secretaria do PROFIAP/UFS.

Por fim, me utilizando da máxima “antes tarde do que nunca”, registro meus agradecimentos póstumos ao colega Charles Micael que, embora vinculado ao Mestrado de Economia da UFS, durante dois semestres letivos abrilhantou nossas aulas com o seu vasto conhecimento e firme defesa dos seus ideais. Sua triste e precoce partida me fez refletir sobre o real sentido da vida e despertar para circunstâncias até então adormecidas.

É a quem dedico os meus sinceros e eternos agradecimentos, sem a menor intenção de aqui estabelecer qualquer ordem hierárquica.

## RESUMO

Ao longo das últimas décadas, a necessidade de gerenciar eventos incertos e com potencial de impactar na consecução de estratégias e objetivos de negócios, sobre os quais se convencionou denominar riscos organizacionais, vem sendo uma constante preocupação em organizações, que buscam se colocar em condição de razoavelmente compreender suas causas e, sobretudo, consequências, sejam elas negativas ou positivas, a fim de adotar a providência mais adequada no afã de tratá-los. Nesse sentido, a gestão de riscos surge como um mecanismo de controle que pode oferecer um conjunto estruturado de instrumentos e procedimentos visando à identificação e o tratamento dos riscos incidentes sobre as atividades, a estratégia e os objetivos da organização, seja ela privada ou pública. Na Administração Pública, muito mais que recomendável, a implementação da gestão de riscos se apresenta como compulsória, o que se infere dos diversos instrumentos normativos editados ao longo dos últimos anos, a exemplo, dentre outros, da Lei Complementar 101/2000; da Instrução Normativa Conjunta MP/CGU nº 01/2016; da Lei 13.303/2016; e do Decreto nº 9.203/2017. Assim, versa a presente pesquisa sobre a gestão de riscos, sobretudo na Administração Pública, tendo por objetivo precípuo a formulação de uma proposta de contribuição para a gestão de riscos na Universidade Federal de Sergipe – UFS, de maneira que se apresente viável e alinhada à realidade e necessidade da organização. Para tanto, à pesquisa fora empregada uma abordagem qualitativa, enquadrando-se como exploratória quanto aos seus objetivos, e delineada como estudo de caso, tendo como fontes de evidências entrevistas que foram realizadas junto a responsáveis pela gestão de riscos tanto na UFS quanto em duas outras instituições federais de ensino, bem como documentação igualmente coletada, de onde foi possível extrair que a implantação da gestão de riscos na UFS se encontra em avançado estágio no que pertine à edição de instrumentos normativos relativos ao tema e que visam regulamentar a implementação e execução dos procedimentos propostos, mas, por outro lado, ainda se encontra em estágio incipiente no que diz respeito à disseminação da cultura da gestão de riscos entre os servidores e unidades da instituição. De igual modo, verificou-se que as ações de monitoramento e controle de riscos carecem de melhor detalhamento no Plano de Gestão de Riscos e Controle da instituição para o período 2021/2022. Ao final, tendo por base o exame dos dados coletados, concluiu-se pela oportunidade de formulação de proposta de plano de monitoramento e controle de riscos, a qual integra o corpo textual do presente estudo.

**Palavras-Chave:** Gestão de Riscos. Riscos Organizacionais. Gestão de Riscos em Instituições Públicas.

## ABSTRACT

Over the last few decades, the need to manage uncertain events with the potential to impact the achievement of business strategies and objectives, which is conventionally called organizational risks, has been a constant concern in organizations that seek to put themselves in a position to reasonably understand their causes and, above all, consequences, whether negative or positive, in order to adopt the most appropriate measure in the eagerness to treat them. In this sense, risk management emerges as a control mechanism that can offer a structured set of instruments and procedures aimed at identifying and dealing with risks that affect the organization's activities, strategy and objectives, whether private or public. In Public Administration, much more than recommendable, the implementation of risk management is mandatory, which can be inferred from the various normative instruments issued over the last few years, such as, among others, Complementary Law 101/2000; of the Joint Normative Instruction MP/CGU No. 01/2016; of Law 13,303/2016; and Decree No. 9.203/2017. Thus, this research focuses on risk management, especially in Public Administration, with the main objective of formulating a contribution proposal for risk management at the Federal University of Sergipe - UFS, in a way that is viable and aligned with reality and need of the organization. For this purpose, a qualitative approach was used to the research, framing it as exploratory in terms of its objectives, and outlined as a case study, having as sources of evidence interviews that were carried out with those responsible for risk management both at the UFS and in two other federal educational institutions, as well as similarly collected documentation, from which it was possible to extract that the implementation of risk management at UFS is at an advanced stage in terms of the issue of normative instruments related to the subject and which aim to regulate the implementation and execution of the proposed procedures, but, on the other hand, it is still at an incipient stage with regard to the dissemination of the risk management culture among the servers and units of the institution. Likewise, it was found that the risk monitoring and control actions lack better detailing in the institution's Risk Management and Control Plan for the period 2021/2022. In the end, based on the examination of the collected data, it was concluded that there was an opportunity to formulate a proposal for a risk monitoring and control plan, which is part of the textual body of this study.

**Keywords:** Risk Management. Organizational Risks. Risk Management in Public Institutions.

## GLOSSÁRIO DE SIGLAS

ABNT .....	Associação Brasileira de Normas Técnicas
CGRC.....	Comitê de Gestão de Riscos da Universidade Federal de Sergipe
CGU .....	Controladoria Geral da União
COSO.....	Comitê das Organizações Patrocinadoras da Comissão <i>Treadway</i>
ISSO.....	Organização Internacional de Normalização
MP .....	Ministério do Planejamento, Orçamento e Gestão
TCU.....	Tribunal de Contas da União
UFCA .....	Universidade Federal do Cariri
UFERSA.....	Universidade Federal Rural do Semi-Árido
UFS .....	Universidade Federal de Sergipe



## LISTA DE FIGURAS

<b>Figura 1</b> – Cubo do COSO II.....	51
<b>Figura 2</b> – Aplicação do COSO ERM 2017.....	54
<b>Figura 3</b> – Componentes do COSO 2017 .....	55
<b>Figura 4</b> – Estruturação do modelo ABNT ISO 31000:2018.....	59
<b>Figura 5</b> – Estrutura de Gerenciamento de Riscos - Orange Book 2020.....	64
<b>Figura 6</b> – Exemplo de escala de classificação de riscos.....	67
<b>Figura 7</b> – Modelo de matriz de riscos.....	67
<b>Figura 8</b> – Exemplo de diagrama de espinha de peixe (Ishikawa).....	70
<b>Figura 9</b> – Esboço de diagrama “ <i>bow tie</i> ”.....	71
<b>Figura 10</b> – Exemplo de diagrama de loop de causalidade (CLD).....	73
<b>Figura 11</b> – Instrumentos normativos editados pela UFS e relacionados à gestão de riscos na instituição.....	98

## LISTA DE QUADROS

<b>Quadro 1</b> – Eventos críticos sobre gestão de riscos.....	18
<b>Quadro 2</b> – Componentes e Princípios da estrutura COSO ERM 2017.....	55
<b>Quadro 3</b> – Pontos fortes e pontos fracos das fontes de evidências empregadas....	85
<b>Quadro 4</b> – Objetivos específicos, categorias de análise e elementos de análise....	87
<b>Quadro 5</b> – Protocolo de estudos.....	89

## SUMÁRIO

<b>1 INTRODUÇÃO</b> .....	<b>12</b>
1.1 OBJETIVOS .....	13
<b>1.1.1 Objetivo Geral</b> .....	<b>14</b>
<b>1.1.2 Objetivos Específicos</b> .....	<b>14</b>
1.2 JUSTIFICATIVA .....	14
<b>2 REFERENCIAL TEÓRICO</b> .....	<b>17</b>
2.1 BREVE EVOLUÇÃO HISTÓRICA DA GESTÃO DE RISCOS .....	17
2.2 A ADMINISTRAÇÃO PÚBLICA NO BRASIL.....	21
2.3 DEFINIÇÕES DE RISCO .....	30
2.4 CATEGORIAIS DE RISCOS EM ORGANIZAÇÕES .....	33
2.5 A GESTÃO DE RISCOS NAS ORGANIZAÇÕES .....	37
2.6 A GESTÃO DE RISCOS NA ADMINISTRAÇÃO PÚBLICA .....	42
2.7 MODELOS E TÉCNICAS DE GESTÃO DE RISCOS APLICÁVEIS À ADMINISTRAÇÃO PÚBLICA .....	49
<b>2.7.1 Os modelos COSO II – Gerenciamento de Riscos Corporativos – Estrutura Integrada (2004); e COSO – Gerenciamento de Riscos Corporativos – Integrado com Estratégia e Performance (2017), e seus desdobramentos</b> .....	<b>49</b>
<b>2.7.2 O modelo ABNT ISO 31000:2018</b> .....	<b>57</b>
<b>2.7.3 O modelo <i>Orange Book e Risk Management Assessment Framework</i></b> .....	<b>63</b>
<b>2.7.4 Roteiro e técnicas para gestão de riscos apresentados pelo TCU</b> .....	<b>66</b>
2.8 O SISTEMA FORRISCO E A SUA CAPACIDADE DE CONTRIBUIÇÃO PARA A GESTÃO DE RISCOS EM INSTITUIÇÕES PÚBLICAS.....	73
<b>3 METODOLOGIA</b> .....	<b>77</b>
3.1 CARACTERIZAÇÃO DO ESTUDO .....	78
3.2 QUESTÕES DE PESQUISA .....	79
3.3 DELINEAMENTO E PROCEDIMENTOS DA PESQUISA.....	80
3.4 UNIDADE DE ANÁLISE E CRITÉRIOS PARA ESCOLHA DO CASO .....	81
3.5 FONTES DE EVIDÊNCIA.....	84
3.6 DEFINIÇÕES CONSTITUTIVAS.....	86
3.7 CATEGORIAS ANALÍTICAS E ELEMENTOS DE ANÁLISE.....	87
3.8 PROTOCOLO DE ESTUDO.....	88

3.9 ANÁLISE DOS DADOS.....	89
3.10 FORMULAÇÃO DE PROPOSTA DE INTERVENÇÃO A PARTIR DO DIAGNÓSTICO OBTIDO COM A ANÁLISE DOS DADOS .....	90
<b>4 DIAGNÓSTICO DA GESTÃO DE RISCOS NA UNIVERSIDADE FEDERAL DE SERGIPE .....</b>	<b>92</b>
4.1 INSTRUMENTOS NORMATIVOS EDITADOS .....	92
4.2 EVENTOS E OUTRAS INICIATIVAS DE DISSEMINAÇÃO DA GESTÃO DE RISCOS NO ÂMBITO DA INSTITUIÇÃO PESQUISADA.....	99
4.3 DIAGNÓSTICO SITUACIONAL .....	101
4.4 PONTO DE OPORTUNIDADE IDENTIFICADO VISANDO À FORMULAÇÃO DA PROPOSTA DE CONTRIBUIÇÃO.....	107
4.5 COLETA DE DADOS JUNTO A OUTRAS IFES VISANDO À FORMULAÇÃO DA PROPOSTA DE CONTRIBUIÇÃO.....	109
<b>5 FORMULAÇÃO DA PROPOSTA .....</b>	<b>114</b>
<b>6 CONCLUSÃO .....</b>	<b>124</b>
6.1 RESPONDENDO ÀS QUESTÕES DE PESQUISA .....	124
6.2 SUGESTÕES PARA PESQUISAS FUTURAS.....	126
6.3 CONSIDERAÇÕES FINAIS .....	126
<b>REFERÊNCIAS.....</b>	<b>129</b>
<b>APÊNDICE A .....</b>	<b>134</b>
<b>APÊNDICE B .....</b>	<b>136</b>
<b>APÊNDICE C .....</b>	<b>137</b>
<b>ANEXO A.....</b>	<b>138</b>

## 1 INTRODUÇÃO

Lidar com eventos incertos é tarefa que persegue a humanidade desde os seus primórdios (BERNSTEIN, 2011). Hodiernamente, porém, sobretudo nas organizações, o enfrentamento prévio de situações do acaso, que ao longo dos anos se convencionou classificar como riscos, tomou proporção de fundamental importância, uma vez observado que tais riscos podem trazer consequências capazes de comprometer a estratégia e os objetivos do negócio (ASSI, 2012; BEZERRA, 2013).

Por meio de questões do tipo “por que o domínio do risco é um conceito tão tipicamente moderno?” e “por que a humanidade esperou os milhares de anos até o Renascimento, para romper a barreira que impedia a medição e o controle do risco?” Bernstein (2011) ensina que, embora indubitável que a humanidade sempre esteve submetida a riscos, o que diferencia o passado dos dias atuais é exatamente a capacidade alcançada de se dominar o risco, ou seja, “a noção de que o futuro é mais do que um capricho dos deuses e de que homens e mulheres não são passivos ante a natureza” (BERNSTEIN, 2011, p. 01).

De modo a desvendar tal libertação da humanidade acerca do tratamento místico conferido aos riscos, Bernstein (2011, p. 01) crava que “até os seres humanos descobrirem como transpor essa fronteira, o futuro era um espelho do passado ou o domínio obscuro de oráculos e adivinhos”, aclarando como a probabilidade enquanto ciência veio a fomentar, ao longo dos anos, os modelos hoje disponíveis para o gerenciamento de riscos, sobretudo nas organizações.

Daí se extrai que a gestão de riscos passou a ser considerada como necessária em todo tipo de organização, seja ela pública ou privada, pois tem como finalidade criar métodos e estratégias com vistas a monitorar, de forma sistemática, adequada e sustentável, sua exposição ao risco, objetivando o alcance dos objetivos ou resultados tencionados (PADOVEZE, 2008).

Na Administração Pública, mais precisamente, dado que os recursos envolvidos na consecução dos objetivos originam-se de impostos e contribuições vertidas ao erário pela sociedade em geral, mais relevante se revela a existência de uma estruturação para identificação e controle dos eventos incertos supramencionados, tanto que ao longo dos últimos anos vêm sendo editados

instrumentos normativos que tornam compulsória a adoção de tal procedimento, a exemplo da Lei Complementar 101/2000 (Lei de Responsabilidade Fiscal); da Instrução Normativa Conjunta MP/CGU nº 01/2016, que “dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo federal”; da Lei 13.303/2016, que “dispõe sobre o estatuto jurídico da empresa pública, da sociedade de economia mista e de suas subsidiárias, no âmbito da União, dos Estados, do Distrito Federal e dos Municípios”; e do Decreto nº 9.203/2017, que “dispõe sobre a política de governança da administração pública federal direta, autárquica e fundacional”.

Em que pese todo o esforço empreendido, o Relatório de Políticas e Programas de Governo (RePP) – desenvolvido pelo TCU “em cumprimento ao disposto no art. 123 da Lei de Diretrizes Orçamentárias - LDO 2018”, cujas conclusões resultam assentadas no Acórdão nº 2.127/2017, aponta para um cenário deficitário no tocante à governança e gestão de riscos nas instituições públicas federais que, segundo o documento, é circunstância responsável pela ineficiência “generalizada” na aplicação dos recursos públicos, capazes de “perenizar” a baixa eficácia dos bens e serviços ofertados (TCU, 2018, p. 30), de forma a tornar premente a estruturação do gerenciamento de riscos em tais instituições.

Assim, delineado o tema gerenciamento de riscos, mormente na Administração Pública e, partindo do princípio de que a Universidade Federal de Sergipe integra o rol de instituições públicas federais, teve a presente pesquisa o escopo de responder à seguinte pergunta:

O que pode ser feito em prol da melhoria da gestão de riscos na Universidade Federal de Sergipe, de forma que se apresente uma proposta viável e alinhada à realidade e necessidade da organização?

## 1.1 OBJETIVOS

O objetivo geral, consoante ensinam Lakatos e Marconi (2003), está ligado a uma visão global e abrangente do tema, relacionando-se com o conteúdo intrínseco, tanto dos fenômenos e eventos, quanto das ideias estudadas.

Quanto aos objetivos específicos, esses devem conduzir ao alcance do objetivo geral, como bem lecionam Lakatos e Marconi (2003, p. 219), para os quais

“os objetivos específicos têm função intermediária e instrumental, permitindo, de um lado, atingir o objetivo geral e, de outro, aplicá-lo a situações particulares”.

### **1.1.1 Objetivo Geral**

Formular proposta de contribuição para a gestão de riscos na Universidade Federal de Sergipe, visando ao seu aprimoramento, de maneira que se apresente viável e alinhada à realidade e necessidade da organização.

### **1.1.2 Objetivos Específicos**

a) Identificar normativos internos e demais documentos relacionados à estratégia e aos objetivos da Universidade Federal de Sergipe no que tange à gestão de riscos na instituição;

b) Diagnosticar o estágio atual de implantação da gestão de riscos na instituição pesquisada;

c) Identificar ponto de oportunidade de formulação da proposta de contribuição;

d) Examinar estruturas de gestão de riscos implantadas em outras instituições públicas federais de ensino superior, no que se refere ao ponto de oportunidade identificado;

e) Elaborar, com base nos resultados obtidos nas ações anteriores, uma proposta de contribuição para a gestão de riscos na instituição pesquisada.

## **1.2 JUSTIFICATIVA**

A pesquisa encontra relevância no fato de que a Administração Pública, submetida que está aos princípios insculpidos no art. 37 da Constituição Federal de 1988 - com ênfase, no presente caso, para os princípios da eficiência e da precaução -, não pode e não deve se eximir dos mecanismos de controles exigidos pelas normativas infraconstitucionais de governança e controle interno, de maneira que contribuições que de alguma forma auxiliem nesse alinhamento não devem ser tidas por despiciendas.

É que não se pode olvidar que a gestão de riscos constitui um dos instrumentos ao alcance da Administração Pública capazes de contribuir para a obtenção dos melhores resultados na prestação dos serviços à coletividade, tendo em vista que os seus princípios basilares também apontam para a necessidade de um emprego eficiente dos recursos públicos, por meio da instrumentalização de mecanismos para o enfrentamento de eventos incertos que possam incidir sobre as atividades que desempenha, com vistas à maior efetividade dos princípios constitucionais retro destacados, pois, conforme sustenta Ávila (2014, p. 184), em primeiro plano deve estar sempre o interesse público, de modo que “a decisão acerca de como equacionar os benefícios e perdas potenciais é o principal aspecto da gestão de riscos” no setor público.

De igual forma, a necessidade de se compreender as nuances de tão importante instrumento de administração da coisa pública, como se apresenta o gerenciamento de riscos, revela a conveniência da presente pesquisa, sobretudo se considerado que o seu objetivo se encontra alinhado com a implementação da gestão de riscos na Universidade Federal de Sergipe, conforme demonstrado em tópico anterior.

Ademais, trata-se a Universidade Federal de Sergipe de instituição pública de reconhecida importância para o desenvolvimento do estado de Sergipe, sendo ao longo de décadas responsável pela formação de profissionais nas mais diversas áreas, cuja missão é “contribuir para o progresso da sociedade por meio da geração de conhecimento e da formação de cidadãos críticos, éticos e comprometidos com o desenvolvimento sustentável” (PDI/UFS 2016-2020, p. 15)<sup>1</sup>, múnus que cumpre com louvor desde 1968.

Deste modo, formular proposta capaz de auxiliar no gerenciamento de riscos de uma instituição pública de incontestável relevância, sobretudo por ser a única universidade pública do estado de Sergipe, além de constituir contribuição de cunho técnico, também atende a requisito estabelecido pelo Programa de Pós-graduação do qual resulta o trabalho, que elucida no art. 20 do seu Regimento Nacional, aprovado em 09/07/2021, que a dissertação abordará tema afeto à Administração

---

<sup>1</sup> Até a conclusão do presente estudo o PDI/UFS 2021-2025 ainda não havia sido publicado.



Pública, dela devendo resultar “uma Análise situacional e recomendações, Análise situacional e Plano de Ação ou Análise situacional e produto técnico/tecnológico”, com observância das “normas da NBR/ABNT e as premissas do método científico” (PROFIAP, 2021).

Por fim, mas de igual importância, necessário se faz registrar que o resultado da presente pesquisa integrará o acervo do Mestrado Profissional em Administração Pública em Rede Nacional – PROFIAP, de modo a contribuir para o conhecimento gerado pelo programa desde a sua implantação.

## 2 REFERENCIAL TEÓRICO

O capítulo em questão se propõe a apresentar o referencial teórico que sustentou a realização desta pesquisa, iniciando com uma breve exposição da evolução histórica do gerenciamento de riscos, seguida da apresentação conceitual da Administração Pública brasileira, da definição de risco, da gestão de riscos nas organizações em geral, e, de forma específica, do gerenciamento de riscos na Administração Pública, respectivamente, culminando com a apresentação de modelos, técnicas e sistema de gestão de riscos aplicáveis à Administração Pública.

### 2.1 BREVE EVOLUÇÃO HISTÓRICA DA GESTÃO DE RISCOS

Em que pese não necessariamente sob a denominação atual ou ostentando a roupagem contemporânea, a história da gestão de riscos organizacionais remonta às antigas civilizações, conforme Hubbard (2020), para quem a decisão de um determinado rei ou chefe tribal no sentido de erguer ou fortalecer muralhas, firmar com outros povos alianças visando à segurança mútua, ou armazenar provisões extras para enfrentar períodos de escassez já representava uma preocupação em administrar riscos.

Hubbard (2020) ressalta que a gestão de risco formalizada por pacto entre as partes parece ser uma característica das primeiras civilizações, tanto que já na antiga Babilônia os comerciantes gerenciavam os riscos envolvidos no transporte de mercadorias para longas distâncias por meio de empréstimos fornecidos pelos compradores aos vendedores, cujo pagamento só ocorreria, ainda que com juros, quando as mercadorias chegassem ao destino em segurança.

Ainda na civilização babilônica, o Código de Hamurabi previa indenizações ou compensações para aqueles prejudicados pela ação de bandidos ou da natureza, além de ter sido o berço do que atualmente se compreende como instituições financeiras, na medida em que os credores, por meio de criteriosa seleção dos devedores, já buscavam administrar os riscos das operações de crédito (HUBBARD, 2020).

Aliada às novas informações, a experiência acumulada desde os primeiros passos da gestão de riscos permitiu ao homem, cada vez mais, pensar de forma

inteligente sobre o futuro e se planejar para enfrentar possíveis resultados inesperados (FRASER; SIMKINS, 2010), ainda que durante a maior parte da história humana a gestão de riscos tenha se apresentado como uma mitigação de riscos (HUBBARD, 2020).

No século XVII, o desenvolvimento da teoria da probabilidade e estatística abriu caminho para que o risco fosse quantificado de forma significativa, embora sua aplicação ficasse restrita a jogos bem definidos e indústrias selecionadas - nestas, ainda que de forma lenta -, enquanto que do século XVIII ao início do século XX, a avaliação quantitativa do risco estivesse quase que limitada a seguros e instituições financeiras (HUBBARD, 2020).

Em semelhante sentido, Fraser e Simkins (2010, p. 21) afirmam que o conhecimento acumulado ao longo dos séculos trouxe importante contribuição “para nossa capacidade crescente de destilar e usar informações”, sem deixar de ressaltar, entretanto, que os eventos relacionados à gestão de riscos, inclusive obras lançadas sobre o tema, desde 1900, se mostram ainda mais relevantes para a compreensão do que hodiernamente se conhece sobre a temática.

Por tal razão, Fraser e Simkins (2010, p. 21) traçam um panorama do que classificam como “eventos críticos” relacionados à gestão de riscos desde 1900, sendo de alguns desses eventos/obras trazidos pelos sobreditos autores que se ocupa o Quadro 1.

<b>Quadro 1 – Eventos críticos sobre gestão de riscos (continua)</b>	
<b>ANO</b>	<b>EVENTO CRÍTICO</b>
1914	Criação da <i>Robert Morris Associates</i> por agentes de créditos e empréstimos da Filadélfia, Estados Unidos, com o objetivo de analisar risco de crédito nas instituições financeiras. No ano 2000 a organização passa a ser intitulada <i>Risk Management Association</i> (Associação de Gestão de Riscos).
1915	Friedrich Leitner publica em Berlim, Alemanha, a dissertação intitulada <i>Die Unternehmensrisiken</i> (Os Riscos do Negócio), pela qual aborda o tema risco e algumas de suas respostas, inclusive seguro.
1921	Frank Knight publica o livro <i>Risk, Uncertainty and Profit</i> (Risco, Incerteza e Lucro), obra que se torna fundamental para a literatura do gerenciamento de risco, na qual o autor distingue “incerteza” de “risco”, aduzindo que a incerteza não pode ser mensurada, enquanto o risco pode ser objeto de mensuração.
1921	John Maynard Keynes publica a obra <i>A Treatise on Probability</i> (Um Tratado sobre Probabilidade), na qual despreza a dependência da “Lei dos Grandes Números”, e enfatiza a importância da percepção e do julgamento relativos na determinação de probabilidades.
1928	John Von Neumann apresenta na Universidade de Göttingen seu primeiro artigo sobre uma teoria de jogos e estratégia, onde sugere que o objetivo de não perder pode ser superior ao de vencer.

<b>Quadro 1 – Eventos críticos sobre gestão de riscos (continua)</b>	
1952	O <i>Journal of Finance</i> (No. 7–, 77–91) publica <i>Portfolio Selection</i> , de autoria do Dr. Harry Markowitz, pelo qual o autor “explora aspectos de retorno e variação em uma carteira de investimentos”, dando azo a muitas das sofisticadas medidas de riscos aplicadas atualmente pelas instituições financeiras.
1956	Publicação pela <i>Harvard Business Review</i> da obra <i>Risk Management: A New Phase of Cost Control</i> (Gestão de Risco: Uma Nova Fase de Controle de Custos), de Russell Gallagher, então gerente de seguros da <i>Philco Corporation</i> na Filadélfia, ressaltando a importância do seguro como resposta ao risco.
1962	Em Toronto, no Canadá, Douglas Barlow, gerente de risco de seguros da Massey Ferguson, desenvolve a ideia de “custo de risco”, “comparando a soma de recursos autofinanciados, perdas, prêmios de seguro, custos de controle de perdas e custos administrativos, custos para receitas, ativos e patrimônio líquido”.
1962	A obra <i>The Silent Spring</i> (Primavera Silenciosa), de Rachel Carson, convida para uma reflexão acerca da degradação do meio ambiente, discutindo a necessidade de avaliação e respostas para os riscos ambientais.
1965	Ralph Nader lança o livro <i>Unsafe at Any Speed</i> (Inseguro em qualquer velocidade), pelo qual expôs os potenciais perigos de se conduzir carros fabricados nos Estados Unidos, denunciando a resistência da indústria automobilística em melhorar os níveis de segurança. A obra despertou os consumidores para a necessidade de se exigir regulamentações capazes de obrigar a indústria, sobretudo automobilística, a considerar os “riscos do produto” e assim fornecer artefatos mais seguros.
1966	O <i>Insurance Institute of America</i> “desenvolve um conjunto de três exames que levaram ao programa ‘Associate in Risk Management’ (ARM)” (Associado em Gestão de Riscos), pioneiro na certificação de profissionais dedicados ao gerenciamento de riscos, sobretudo na gestão de seguro corporativo.
1972	Juntamente com Sir John Hicks, o Dr. Kenneth Arrow ganha o Prêmio Nobel de Ciências Econômicas, e defende a ideia de “um mundo perfeito no qual cada incerteza é ‘segurável’”. Um mundo em que a Lei dos Grandes Números funciona sem falhas”, de modo que a melhor maneira de se preparar para o risco é aceitar seu potencial como estimulante e pena.
1974	Gustav Hamilton, gerente de risco da <i>Statsforetag</i> da Suécia, desenvolve um “círculo de gerenciamento de risco”, no qual descreve graficamente a interação de todos os “elementos do processo, desde a avaliação e controle até o financiamento e comunicação”.
1975	A Sociedade Americana de Gestão de Seguros muda seu nome para <i>Risk &amp; Insurance Management Society</i> (RIMS) e, com o seu apoio, a revista <i>Fortune</i> publica o artigo intitulado <i>The Risk Management Revolution</i> (A Revolução da Gestão de Riscos), pelo qual sugere a coordenação de funções de gerenciamento de risco anteriormente desconectadas dentro de uma organização, atribuindo à alta administração a responsabilidade pela instituição de política de gestão de riscos e a coordenação e supervisão das funções e atividades a ela relacionadas.
1979	Daniel Kahneman e Amos Tversky publicam a obra <i>Prospect Theory</i> (Teoria da perspectiva), “demonstrando que a natureza humana pode ser perversamente irracional, especialmente diante do risco, e que o medo da perda muitas vezes supera a esperança do ganho”.
1980	Defensores de políticas públicas, acadêmicos e profissionais de gestão de riscos formam a <i>Society for Risk Analysis</i> (SRA) em Washington, constituída como um fórum aberto onde qualquer pessoa de qualquer parte do mundo possa trocar informações, ideias e metodologias para análise de risco e solução de problemas de risco, dando origem, no mesmo ano, a sua revista <i>Risk Analysis</i> (Análise de Risco).
1983	William Ruckelshaus profere discurso sobre <i>Science, Risk and Public Policy</i> (Ciência, Risco e Política Pública) para a Academia Nacional de Ciências, lançando a ideia de gestão de risco nas políticas públicas e a conduzindo para a agenda política nacional americana.
1986	Surge em Londres, Inglaterra, o <i>Institute for Risk Management</i> , que mais tarde passaria a oferecer o primeiro programa de educação continuada com vistas à certificação para a gestão de riscos em todos os seus enfoques.

<b>Quadro 1 – Eventos críticos sobre gestão de riscos (conclusão)</b>	
1992	O Relatório publicado pelo Comitê Cadbury, do Reino Unido, confere à Administração Superior das entidades a responsabilidade pela definição da política de gestão de riscos e a supervisão do processo de gerenciamento de riscos, bem como pela compreensão de todos os riscos aos quais estão expostas tais organizações.
1995	Fruto de uma força-tarefa multidisciplinar da Austrália e da Nova Zelândia, surge a primeira Norma de Gestão de Risco, a AS/NZS 4360:1995, reunindo pela primeira vez várias das diferentes subdisciplinas, cujo padrão restou seguido por iniciativas do Canadá, Japão e Reino Unido, de forma a ser reconhecida como um importante passo rumo a um quadro de referência global para a gestão de riscos.
1995	Um trader do <i>Barings Bank</i> – instituição sediada no Reino Unido – operando em Cingapura sob desastrosa sobrecarga de trabalho, como resultado de uma combinação de ganância e arrogância com “imperdoáveis falhas de controle”, provocou a liquidação do banco para o qual operava, fato que se tornou manchete mundial e lançou holofotes para a necessidade de gestão dos riscos operacionais.
1996	Obras sobre risco e gerenciamento de risco fazem parte da lista de <i>best-sellers</i> na América do Norte e Europa, sobretudo com a publicação de <i>Against the Gods: The Remarkable Story of Risk</i> (Desafio aos Deuses: A Fascinante História do Risco) de Peter Bernstein, onde o autor apresenta as nuances do risco e da gestão desses eventos, sem deixar de alertar para a contraindicação do excesso de confiança na quantificação, o que faz ao afirmar que “o aparato matematicamente orientado do gerenciamento de risco moderno contém as sementes de uma tecnologia desumanizante e autodestrutiva”.
2000	Os possíveis efeitos deletérios do amplamente propalado “bug do milênio” ou “bug Y2K” não se concretizam, muito em razão de altas somas de recursos destinados à atualização dos sistemas de informática, o que representa um sucesso dedicado ao gerenciamento de riscos.
2001	As ações terroristas de 11 de setembro, assim como o colapso da empresa Enron, atribuída a um colossal esquema de ocultação e manipulação de dados contábeis e auditorias fraudulentas, além de servirem para alertar o mundo para a constatação de que nada é tão grande que não possa colapsar, também atuaram para revigorar a gestão de riscos em diferentes aspectos.
2001	É criada nos Estados Unidos e no Reino Unido a <i>PRMIA - Professional Risk Manager's International Association</i> (Associação Internacional de Profissionais em Gerenciamento de Risco), que mais tarde viria a oferecer programas de certificação em gestão de riscos de reconhecimento global.
2002	Em resposta ao colapso da empresa Enron e outros escândalos semelhantes, o Congresso dos Estados Unidos sanciona a Lei <i>Sarbanes-Oxley</i> , com observância obrigatória por todas as empresas instaladas no país, sejam nacionais ou não, se notabilizando como “um impulso para combinar gestão de riscos com governança e conformidade regulatória”.
2004	O Acordo de Basileia II foi publicado pelo Comitê de Supervisão Bancária de Basileia, que trouxe em seu bojo diretrizes relacionadas ao gerenciamento de riscos operacionais aplicáveis a instituições bancárias de todo o globo.
2005	A <i>ISO - International Organization for Standardization</i> (Organização Internacional para Padronização) cria um grupo de trabalho com vistas à elaboração de uma nova diretriz universal para definição, aplicação e prática da gestão de riscos, que quatro anos depois culminou com a edição da ISO 31.000:2009.
2007	A publicação de <i>The Black Swan</i> (traduzido para o português como A lógica do Cisne Negro), de Nassim Nicolas Taleb, surge como um alerta de que o “nosso mundo é dominado pelo extremo, o desconhecido, e o muito improvável... enquanto passamos nosso tempo engajados na conversa fiada, focando no conhecido e no repetido”.
2008	O resgate (da insolvência) do banco <i>Bear Stearns</i> pelo <i>Fed - Federal Reserve</i> dos Estados Unidos soou para muitos como o fracasso da gestão de riscos convencional nas instituições financeiras.

Fonte: adaptado de Fraser e Simkins (2010)

Por sua vez, ainda à guisa de evolução histórica da gestão de riscos, o Referencial Básico de Gestão de Riscos elaborado pelo TCU (2018) destaca como iniciativas de relevo<sup>2</sup>: Em 1992, a publicação pelo *Committee of Sponsoring Organizations of the Treadway Commission* – COSO do guia *Internal Control - Integrated Framework* (COSO I); em 2001, a produção e publicação pelo *HM Treasury* Britânico do *The Orange Book - Management of Risk - Principles and Concepts*; em 2004, a publicação pelo COSO do *Enterprise Risk Management - Integrated Framework* (COSO-ERM ou COSO II); e, em 2009, a publicação da norma técnica ISO 31000 *Risk Management – Principles and Guidelines*, revisada em 2018.

Em arremate, Fraser e Simkins (2010, p. 27) sustentam que administrar riscos, independentemente da denominação que se atribua (gestão de risco; gerenciamento de riscos; gestão estratégica de riscos, etc.), continuará a fazer parte da experiência humana, de modo que nenhuma das retrospectões apresentadas terá qualquer significado ou valor, caso não atue como um estimulante para um uso mais prudente, inteligente e otimista das ideias e ferramentas do passado.

## 2.2 A ADMINISTRAÇÃO PÚBLICA NO BRASIL

Embora o presente trabalho tenha como foco o gerenciamento de riscos em instituições públicas federais de ensino superior, mais precisamente na Universidade Federal de Sergipe, não soa despiciendo nele tecer algumas considerações e definições relacionadas à Administração Pública no Brasil e seus agentes, a fim de proporcionar uma melhor compreensão acerca das nuances que regem o gerenciamento da coisa pública, posto que, em muitas oportunidades, aspectos a eles relacionados são mencionados no transcorrer do estudo.

Tem-se por oportuno, de partida, dada a indissociabilidade com o tema proposto no presente capítulo, trazer uma breve definição acerca da figura do agente público. De acordo com Alexandrino e Paulo (2017, p. 138), por agente público deve-se entender todas as pessoas físicas que exerçam, “ainda que

---

<sup>2</sup> Os modelos mencionados são apresentados no tópico 2.7 do presente estudo, que cuidou de abordar, quando houver, a versão atualizada de cada um deles.

transitoriamente ou sem remuneração, por eleição, nomeação, designação, contratação ou qualquer forma de investidura ou vínculo, mandato, cargo, emprego ou função” junto à Administração Pública, indivíduos esses que, em razão do vínculo mantido, exteriorizam, por meio de atos administrativos e dentro do limite de suas competências, a vontade do Estado em suas três esferas (federal, estadual e municipal, além do Distrito Federal), e nos três Poderes da República (Executivo, Legislativo e Judiciário).

Acerca da Administração Pública, Matias-Pereira (2014, p. 77), sem deixar de alertar para a dificuldade de se definir de forma terminativa o significado da expressão, sobretudo em razão da complexidade do que representa, define-a como “o conjunto de serviços e entidades incumbidos de concretizar as atividades administrativas, ou seja, da execução das decisões políticas e legislativas”, cujo objetivo é, observando princípios fincados pelo Direito e pela Moral, direcionar os bens e recursos públicos para o atendimento dos interesses coletivos, seja na esfera federal, estadual ou municipal.

Trata ainda o autor de definir Administração Pública Direta e Indireta, apontando para as formações administrativas que as integra:

**Administração Direta:** (i) estrutura administrativa da Presidência da República e dos Ministérios; (ii) conjunto de unidades organizacionais que integram a estrutura administrativa de cada um dos poderes da União, dos Estados e dos Municípios, abrangendo não só as unidades destituídas de autonomia, mas também os órgãos autônomos e os fundos.

[...]

**Administração Indireta:** Conjunto de entidades públicas dotadas de personalidade jurídica própria, compreendendo: autarquias; empresas públicas; sociedades de economia mista; e fundações públicas (MATIAS-PEREIRA, 2014, p. 201).

Di Pietro (2018, 117) define Administração Pública tendo por base o “sentido subjetivo, formal ou orgânico”, consubstanciado nas pessoas jurídicas, órgãos e agentes públicos que exercem a função administrativa propriamente dita; e em “sentido objetivo, material ou funcional”, que representa as funções administrativas exercidas pelos referidos entes, função esta que incumbe, sobretudo, ao Poder Executivo.

Apresenta ainda a mesma autora uma distinção entre os sentidos supramencionados (subjetivo, formal ou orgânico e objetivo, material ou funcional),

desta feita contemplando a ideia de administração (pública) como planejamento e execução de atividades:

- a) em sentido amplo, a Administração Pública, **subjctivamente** considerada, compreende tanto os órgãos **governamentais**, supremos, constitucionais (Governo), aos quais incumbe traçar os planos de ação, dirigir, comandar, como também os **órgãos administrativos**, subordinados, dependentes (Administração Pública, em sentido estrito), aos quais incumbe executar os planos governamentais; ainda em sentido amplo, porém **objetivamente** considerada, a Administração Pública compreende a **função política**, que traça as diretrizes governamentais e a **função administrativa**, que as executa;
- b) em sentido estrito, a Administração Pública compreende, sob o aspecto subjetivo, apenas os órgãos administrativos e, sob o aspecto objetivo, apenas a função administrativa, excluídos, no primeiro caso, os órgãos governamentais e, no segundo, a função política (DI PIETRO, 2018, p. 117).

Em semelhante sentido, Meirelles, Burle Filho e Burle (2016, p. 68) ensinam que a Administração Pública, “em sentido formal, é o conjunto de órgãos instituídos para consecução dos objetivos do Governo; em sentido material, é o conjunto das funções necessárias aos serviços públicos em geral”, destacando ainda um sentido operacional para a expressão, assim considerado como o “desempenho perene e sistemático, legal e técnico, dos serviços próprios do Estado ou por ele assumidos”, ou seja, a operacionalização do aparelho estatal na busca pela satisfação dos anseios e necessidades da sociedade, por meio de atos de execução que variam de acordo com a competência e autonomia dos órgãos e agentes públicos envolvidos.

Das definições esposadas vê-se que a Administração Pública congrega um conjunto de esforços e atividades visando pôr em marcha uma engrenagem estatal na direção de satisfazer os interesses da sociedade em geral (interesse público), engrenagem esta movida com os recursos vertidos em favor do Estado por essa mesma sociedade, tudo sem se afastar de determinados postulados.

Tais postulados são os princípios fundamentais que regem a Administração Pública em todas as suas esferas (federal, estadual e municipal), de modo que ditam toda a forma de proceder dos entes e agentes públicos, servindo de balizas normativas a pautar a atuação estatal no desenvolvimento das suas atividades e na busca pelo alcance dos seus objetivos, e que se encontram tanto expressos na Constituição Federal de 1988 (art. 37) - razão pela qual Carvalho Filho (2019) os intitula “princípios expressos” - quanto derivam de entendimentos doutrinários e



jurisprudências que, dada sua relevância e aceitação, também são “princípios reconhecidos” (CARVALHO FILHO, 2019).

Nesse sentido, o art. 37 da Constituição Federal de 1988 estatui que “a administração pública direta e indireta de qualquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios obedecerá aos princípios de legalidade, impessoalidade, moralidade, publicidade e eficiência”, de modo a aclarar que qualquer ato ou procedimento adotado pela Administração Pública deve se enquadrar em tais balizas, sob pena de incorrerem em invalidade (CARVALHO FILHO, 2019).

Relevante, pois, se mostra apresentar, ainda que brevemente, cada um dos princípios constitucionais elencados no art. 37 da CF/88, assim como aqueles intitulados por Carvalho Filho (2019) como “princípios reconhecidos”, cujo rol a ser seguido é aquele apresentado pelo sobredito autor.

a. Princípios Expressos na Constituição Federal:

- Princípio da Legalidade: Preceitua que nenhuma atividade da Administração Pública pode ser tida por lícita se não autorizada por lei, o que significa dizer que a atuação do Estado e seus agentes não pode, sob nenhuma hipótese, ultrapassar os limites legais quando do exercício do seu mister, razão pela qual o princípio em comento constitui preceito basilar da atuação estatal (CARVALHO FILHO, 2019).

Acerca do fundamental princípio, Mello (2015) traz definição que demonstra, em sua plenitude, a abrangência e força normativa do preceito em questão:

o princípio da legalidade é o da completa submissão da Administração às leis. Esta deve tão somente obedecê-las, cumpri-las, pô-las em prática. Daí que a atividade de todos os seus agentes, desde o que lhe ocupa a cúspide, isto é, o Presidente da República, até o mais modesto dos servidores, só pode ser a de dóceis, reverentes, obsequiosos cumpridores das disposições gerais fixadas pelo Poder Legislativo, pois esta é a posição que lhes compete no Direito brasileiro. (MELLO, 2015, p. 104)

Para Alexandrino e Paulo (2017), tal princípio é inerente ao próprio Estado de Direito, pois submete a todos, particulares e agentes públicos, à vontade da lei, de modo a tornar inválido qualquer ato emanado pelo Poder Público que dela não decorra, porquanto a Administração Pública ostenta posição de gestora da coisa pública, cuja titularidade recai sobre o povo e, como tal, “não é suficiente a ausência de proibição em lei para que a administração pública possa agir”, mas sim que haja lei lastreando o seu proceder, sob pena de sua atuação ser considerada inválida.

• Princípio da impessoalidade: também intitulado princípio da “finalidade e igualdade” por Meirelles, Burle Filho e Burle (2016), a impessoalidade exigida da Administração Pública impõe ao agente público que todo ato administrativo dele emanado deve decorrer da estrita finalidade legal a qual se destina, sempre com vistas ao interesse público, sendo vedado, pois, sob pena de nulidade por desvio de finalidade, qualquer direcionamento que vise favorecer, discriminar ou perseguir pessoa determinada (ALEXANDRINO; PAULO, 2017).

Na mesma linha são os ensinamentos de Mello (2015, p. 117), que sustenta ser o referido princípio “o próprio princípio da igualdade ou isonomia”, na medida em que é vedado a Administração tratar os administrados de forma discriminatória, seja ela benéfica ou detrimetosa, com favoritismos ou perseguições, de modo que “simpatias ou animosidades pessoais, políticas ou ideológicas não podem interferir na atuação administrativa e muito menos interesses sectários, de facções ou grupos de qualquer espécie”.

Di Pietro (2018), por sua vez, ressalta que o princípio em tela pode ser observado por dois diferentes ângulos, sendo o primeiro no que diz respeito ao administrado, pois pressupõe que os atos da Administração Pública não podem ser realizados com o fito de privilegiar ou causar prejuízos a indivíduos determinados, tendo em vista que o seu objetivo deve sempre ter como norte o interesse público, sob pena de desviar-se da finalidade pública; ao passo que o segundo refere-se à despersonalização de todo e qualquer ato da Administração Pública, porquanto, embora emanado da ação de agente público, tal ato não deve ser a ele atribuído, e sim à instituição estatal que representa naquele instante.

Como exemplos de vedação à personificação e ao direcionamento pessoal dos atos da Administração Pública, Di Pietro (2018) aponta para os preceitos dos artigos 37, §1º, e 100 da Constituição Federal de 1988, os quais preveem que:

Art. 37, § 1º.

A publicidade dos atos, programas, obras, serviços e campanhas dos órgãos públicos deverá ter caráter educativo, informativo ou de orientação social, dela não podendo constar nomes, símbolos ou imagens que caracterizem promoção pessoal de autoridades ou servidores públicos.

[...]

Art. 100.

Os pagamentos devidos pelas Fazendas Públicas Federal, Estaduais, Distrital e Municipais, em virtude de sentença judiciária, far-se-ão exclusivamente na ordem cronológica de apresentação dos precatórios e à conta dos créditos respectivos, proibida a designação de casos ou de

pessoas nas dotações orçamentárias e nos créditos adicionais abertos para este fim.

No entanto, Carvalho Filho (2019) alerta que o princípio em tela pode ser excepcionado, citando como exemplo a implementação pelo governo federal de ações afirmativas que incidem sobre o ingresso nas instituições de ensino superior levando em conta o critério étnico-social do administrado.

- Princípio da moralidade: Confere caráter jurídico ao dever de proceder de acordo com a moral e a ética que recai sobre os agentes públicos no desenvolvimento das suas atividades, sob pena de invalidação dos atos praticados (ALEXANDRINO; PAULO, 2017).

Conforme Carvalho Filho (2019, p. 97), o agente público “deve não só averiguar os critérios de conveniência, oportunidade e justiça em suas ações, mas também distinguir o que é honesto do que é desonesto”, proceder que deve adotar não apenas em relação aos administrados, mas também no trato dele agente com a própria Administração.

Di Pietro (2018, p. 143-145), por fim, traz à lume a emblemática situação do ato administrativo que, embora coberto pela legalidade, se afigura imoral, aludindo que sobre tal ato, nada obstante a legalidade verificada, devem incidir os efeitos jurídicos decorrentes da imoralidade administrativa, sobretudo a sua invalidação, seja na própria seara administrativa, seja por decisão judicial, isso porque, conforme a autora, “a lei pode ser imoral e a moral pode ultrapassar o âmbito da lei”.

- Princípio da publicidade: Postulado que condiciona a eficácia dos atos da Administração Pública não protegidos por sigilo previsto em lei à ampla divulgação por meio oficial, bem como determina seja a coisa pública gerida de modo transparente, com o fito de possibilitar o controle dos administrados sobre tais atos praticados (ALEXANDRINO; PAULO, 2017; CARVALHO FILHO, 2019; DI PIETRO, 2018).

Assim, o princípio da publicidade visa possibilitar que o administrado tenha pleno conhecimento acerca da condução dos interesses coletivos por parte da Administração Pública, pois, conforme afirma Mello (2015, p. 88), “se os interesses públicos são indisponíveis, se são interesses de toda a coletividade, os atos emitidos a título de implementá-los não de ser exibidos em público.”

- **Princípio da eficiência:** Exige que as atividades desenvolvidas pela Administração Pública busquem a máxima otimização dos recursos empregados, a fim de evitar desperdícios e imposição de prejuízos ao erário e, sobretudo, com o fito de bem atender aos anseios da sociedade, empregando qualidade aos serviços públicos prestados (DI PIETRO, 2018; MEIRELLES; BURLE FILHO; BURLE, 2016), constituindo-se, por tais razões, numa faceta do princípio da boa administração, conforme classifica Mello (2015).

Decorrente da reforma do Estado empreendida em 1998 e que tinha, dentre outros, o objetivo de implementar a Administração gerencial – com foco na eficiência – em substituição à Administração burocrática, focada, sobretudo, no princípio da legalidade (ALEXANDRINO; PAULO, 2017), o princípio da eficiência foi inserido na Carta Magna por meio da Emenda Constitucional nº 19/1998 e, conforme Carvalho Filho (2019, p. 106-107), “revela o descontentamento da sociedade diante de sua antiga impotência para lutar contra a deficiente prestação de tantos serviços públicos, que incontáveis prejuízos já causou aos usuários.”

Ainda acerca da incorporação do princípio da eficiência no texto constitucional, Carvalho Filho (2019) tece relevante crítica, pela qual aclara seu entendimento no sentido de que a constitucionalização, por si só, não tem o condão de conferir eficiência às atividades desenvolvidas pelos órgãos públicos:

[...]de nada adianta a referência expressa na Constituição se não houver por parte da Administração a efetiva intenção de melhorar a gestão da coisa pública e dos interesses da sociedade. Com efeito, nenhum órgão público se tornará eficiente por ter sido a eficiência qualificada como princípio na Constituição (2019, p. 107).

Prega ainda o autor que o alcance da eficiência tencionada pelo texto constitucional passa por uma conscientização dos gestores públicos acerca do papel do Estado enquanto defensor (que deve ser) dos interesses da sociedade, o que implica em deixar de lado os interesses pessoais desses próprios gestores, pois, do contrário, inútil será falar em eficiência (CARVALHO FILHO, 2019).

b. Princípios Reconhecidos:

- **Princípio da supremacia do interesse público:** Crava que o interesse público deve sempre prevalecer sobre o interesse do particular, tendo em vista que a atuação do Estado tem em mira o benefício da coletividade, de modo que eventual interesse privado não pode sobrepujar a consecução desse objetivo, a exemplo do que ocorre

na desapropriação, onde a vontade do proprietário é deixada de lado para dar lugar ao interesse público (CARVALHO FILHO, 2019). De acordo com Di Pietro (2018), tal princípio se confunde com o próprio sentido da expressão serviço público, onde público indica a atuação do Estado, cuja ação se destina ao atendimento dos interesses, das necessidades e dos anseios da sociedade, estes de prevalência indiscutível sobre o interesse privado.

- Princípio da Autotutela: decorrente do princípio da legalidade, refere-se ao poder/dever do qual está investida a Administração Pública de rever seus próprios atos a fim de restituir a regularidade da atuação (CARVALHO FILHO, 2019), de modo que pode ser exercido por iniciativa própria (de ofício) por parte da autoridade da qual tenha emanado o ato ilegal, inconveniente ou inoportuno, ou mediante provocação do administrado em sede de recurso administrativo, conforme ensina Di Pietro (2018).
- Princípio da Indisponibilidade: postula que a Administração Pública só pode atuar diante da existência de lei e dentro dos limites pela lei estabelecidos, posto não ser proprietária do patrimônio público, tampouco titular do interesse público, de maneira a não poder dispor de forma discricionária daquilo cuja titularidade recai sobre o povo. Do princípio decorre, por exemplo, “a necessidade de realizar concurso público para admissão de pessoal permanente [...], a necessidade, em regra, de realizar licitação prévia para celebração de contratos administrativos [...], as restrições à alienação de bens públicos” (ALEXANDRINO; PAULO, 2017, p. 13).
- Princípio da Continuidade dos Serviços Públicos: corolário do princípio da eficiência e do princípio da supremacia do interesse público, traz como regra que os serviços públicos (aí inclusas toda e qualquer atividade administrativa) não podem sofrer solução de continuidade, sob pena de causar impactos negativos na qualidade dos serviços e prejuízos à coletividade (CARVALHO FILHO, 2019).
- Princípio da Segurança Jurídica (Proteção à Confiança): visa conferir estabilidade às relações jurídicas mantidas pela Administração Pública, por meio de institutos como prescrição, decadência, direito adquirido e ato jurídico perfeito, proporcionando ao administrado, “de um lado, a *perspectiva de certeza*, que indica o conhecimento seguro das normas e atividades jurídicas, e, de outro, a *perspectiva de estabilidade*, mediante a qual se difunde a ideia de consolidação das ações administrativas” (CARVALHO FILHO, 2019, p. 115-116).

- Princípio da Precaução: embora tenha como nascedouro o Direito Ambiental, a aplicabilidade do princípio em questão à toda atividade e conduta administrativa visando à tutela do interesse público vem sendo amplamente defendida, porquanto “se determinada ação acarreta risco para a coletividade, deve a Administração adotar postura de precaução para evitar que eventuais danos acabem por concretizar-se” (CARVALHO FILHO, 2019, p. 118-119).
- Princípio da Razoabilidade: Também tratado como Princípio da proibição de excesso, objetiva “aferir a compatibilidade entre os meios empregados e os fins visados na prática de um ato administrativo, de modo a evitar restrições aos administrados inadequadas, desnecessárias, arbitrárias ou abusivas por parte” do Poder Público (ALEXANDRINO; PAULO, 2017, p. 259).
- Princípio da Proporcionalidade: reza, em síntese, que ao realizar intervenções nas atividades que a lei estabelece o seu controle, o Poder Público deve agir de forma proporcional à atuação que o caso exige, ou seja, “deve atuar porque a situação reclama realmente a intervenção, e esta deve processar-se com equilíbrio, sem excessos e proporcionalmente ao fim a ser atingido” (CARVALHO FILHO, 2019, p. 121-122).

Sem olvidar da importância de cada um dos princípios aos quais está submetida à Administração Pública, sejam eles expressos ou reconhecidos – conforme classifica Carvalho Filho (2019) –, cumpre aqui registrar que os princípios da eficiência e da precaução guardam maior relação com o presente estudo, tendo em vista que o gerenciamento de riscos constitui um dos instrumentos que a Administração deve lançar mão a fim de assegurar os melhores resultados na prestação dos serviços à coletividade.

Não à toa, os princípios basilares da gestão de riscos na Administração Pública também apontam para a necessidade de um emprego eficiente dos recursos públicos, no qual se inclui a instrumentalização de mecanismos visando ao enfrentamento de eventos incertos que possam incidir sobre a atividade pública, cujo propósito não é outro, que não o de conferir maior efetividade aos sobreditos princípios constitucionais, porquanto, conforme sustentam Hill e Dinsdale (2003, p. 9), as responsabilidades e deveres que recaem sobre a Administração Pública no seu mister de gerir a coisa pública “exigem a adoção de práticas e estratégias eficazes de gestão de riscos”, dada a necessidade cada vez mais premente e

forçosa de se “tomar decisões difíceis sobre riscos de saúde, riscos ambientais, riscos ao bem-estar econômico, riscos tecnológicos e riscos envolvidos na prestação de serviços”, dentre inúmeros outros.

## 2.3 DEFINIÇÕES DE RISCO

As definições de riscos no contexto da gestão organizacional diferem relativamente daquelas trazidas pelos dicionários em geral, posto que enquanto os glossários definem risco como probabilidade e/ou perigo relacionado a evento negativo, na gestão de riscos seu conceito circunda em torno da probabilidade que um evento, seja ele negativo ou positivo, venha a incidir sobre determinada situação ou procedimento (ASSI, 2012; LEAL, 2019).

Em obra intitulada “Desafios aos Deuses, a Fascinante História do Risco”, Bernstein (2011, p. 8) traz o risco como algo inerente à condição de pessoa humana, ensinando que “a palavra ‘risco’ deriva do italiano antigo *risicare*, que significa ‘ousar’”, de modo que o risco se afigura como “uma opção, e não um destino”, pois “é das ações que ousamos tomar que dependem de nosso grau de liberdade de opção, que a história do risco trata”.

Bezerra (2013, p. 4), por sua vez, define risco como a “combinação da probabilidade (chance da ameaça se concretizar) de um evento indesejado ocorrer e de suas consequências [...]”, trazendo à lume o caráter incerto da ocorrência do evento risco e os ocasionais impactos dele decorrentes.

Em estudo realizado tendo por base a realidade do Canadá, Hill (2006, p. 37) esclarece que o Conselho do Tesouro daquele país conceituou risco como sendo “a incerteza em torno de eventos e resultados futuros”, constituindo-se na “expressão da probabilidade e do impacto de um evento que pode influenciar a consecução dos objetivos de uma organização”.

Na mesma obra, o autor define risco como sendo “a probabilidade de que um evento, seja ele bom ou mau, ocorra no futuro”, probabilidade esta incidente sobre “coisas futuras com as quais estamos preocupados, como nossa situação financeira, nossa saúde, nossos empregos, nossos filhos ou o meio ambiente”, sem deixar de ressaltar que, embora no mais das vezes o enfoque recaia sobre o aspecto negativo

do risco, não se pode olvidar que o risco também pode contemplar aspectos positivos, traduzidos em oportunidades (HILL, 2006, p. 37).

Em semelhante linha, Assi (2012, n.p) ressalta que apesar de o risco ser comumente entendido como a probabilidade de “algo não dar certo”, na atualidade a definição conferida ao tema deve abarcar tanto “perdas” quanto “ganhos” no que se refere “ao rumo dos acontecimentos planejados, seja por indivíduos, seja por organizações”, de maneira a elucidar que o fenômeno risco incide sobre atividades tanto da vida pessoal e profissional de indivíduos quanto “nas organizações, e pode envolver perdas, bem como oportunidades.”

O *Committee of Sponsoring Organizations of the Treadway Commission* (Comitê das Organizações Patrocinadoras da Comissão *Treadway*) - COSO, entidade privada e sem fins lucrativos sediada nos Estados Unidos que elabora recomendações que servem de referência quando se trata de estruturação de controles internos nas organizações, define risco como “a possibilidade de que venham a ocorrer eventos capazes de afetar a realização da estratégia e dos objetivos do negócio”, definição que engloba todo e qualquer risco incidente sobre a estratégia e objetivos da organização, sejam eles positivos ou negativos (COSO, 2020, p. 1).

A norma ABNT ISO 31000/2018, por seu turno, conceitua risco como “efeito da incerteza nos objetivos”, cujas consequências podem ser positivas, negativas ou ambas, e “que pode abordar, criar ou resultar em oportunidades e ameaças” e, numa abordagem voltada a projetos, o Guia PMBOK (2017) define risco como “um evento ou condição incerta que, se ocorrer, provocará um efeito positivo ou negativo em um ou mais objetivos do projeto”.

Por sua vez, a Instrução Normativa 84/2020, do Tribunal de Contas da União, define risco como a “possibilidade de algo acontecer e ter impacto nos objetivos da unidade prestadora de contas, sendo medido em termos de consequências e probabilidades”, ao passo que a Instrução Normativa Conjunta MP/CGU nº 01/2016, editada conjuntamente pelo então Ministério do Planejamento, Orçamento e Gestão e pela Controladoria-Geral da União para dispor “sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo federal”, conceitua risco como sendo a “possibilidade de ocorrência de um evento que venha a ter impacto no cumprimento dos objetivos”, e que “é medido em termos de impacto e de



probabilidade” (art. 2º, XII), definindo como “apetite a risco” o “nível de risco que uma organização está disposta a aceitar” (art. 2º, II).

A ideia de “risco” como evento decorrente de decisão tomada, defendida por Bernstein, também surge no conceito de risco trazido pelo Tribunal de Contas da União no Referencial Básico de Gestão de Riscos (2018, p. 8).

Risco é o efeito da incerteza sobre objetivos estabelecidos. É a possibilidade de ocorrência de eventos que afetem a realização ou alcance dos objetivos, combinada com o impacto dessa ocorrência sobre os resultados pretendidos.

Os riscos existem independentemente da atenção que damos a eles. Seja na nossa vida cotidiana, seja no mundo corporativo, estamos imersos em ambiente repleto de riscos, oportunidades e ameaças que, se não gerenciados, podem comprometer o alcance de objetivos almejados.

A cada tomada de decisão, a cada movimento que executamos, ou deixamos de executar, alteramos a probabilidade de ocorrência de eventos futuros e, por conseguinte, ampliamos ou reduzimos o nível de riscos a que estamos expostos.

Na vida, existem pessoas com maior apetite a riscos, que se dispõem a aceitar maiores níveis de risco por avaliarem que os impactos positivos superam os negativos.

No extremo oposto, há pessoas que não se sentem confortáveis com possíveis efeitos da incerteza sobre seus objetivos.

Desse modo, diante de um mesmo risco pessoas podem ter reações diferentes, a depender de sua maturidade e experiências pregressas, de sua capacidade de evitar, mitigar ou potencializar sua ocorrência, bem como de reduzir ou tolerar seu impacto.

Sem se afastar, na essência, das definições até aqui apresentadas, a UFS, por meio da Resolução nº 015/2020/CONSU, de 28 de setembro de 2020 - que institui sua política de Governança -, busca, em termos conceituais, definir “risco” de maneira dissociada de “incerteza”, sendo esta última definida como a “incapacidade de saber com antecedência a real probabilidade ou impacto de eventos futuros” (Art. 2º, VIII), ao passo que o primeiro (risco) é tido por “quantificação e qualificação da incerteza”, relacionada “à possibilidade de ocorrência de um evento que venha a interferir no cumprimento dos objetivos, sendo medido em termos de impacto e de probabilidade” (Art. 2º, XIII).

Das definições acima se pode extrair que o risco permeia as ações, das mais simples e cotidianas às mais complexas, a elas podendo trazer consequências negativas ou positivas, cujo grau pode variar de acordo com o nível de exposição que o indivíduo ou a organização se permita aceitar.

## 2.4 CATEGORIAS DE RISCOS EM ORGANIZAÇÕES

Padoveze (2008) aduz que não há como definir um modelo de gerenciamento de riscos que se revele adequado sem antes identificar as categorias de risco que podem incidir sobre as atividades da organização. Assim, no que classifica como “Pirâmide de tipos de riscos”, o autor categoriza tais eventos como *riscos estratégicos*, *riscos de gestão* e *riscos operacionais*, estando a primeira categoria no topo da pirâmide, e a última em sua base.

Por **riscos estratégicos** o autor define aqueles decorrentes das estratégias da organização, estas que se encontram delineadas no seu planejamento estratégico, e que estão relacionados às atividades fins da organização, ao padrão gerencial nela estabelecido, e às estruturas das organizações que operacionalizam tanto as atividades quanto a realização da gestão, caracterizando-se como riscos estruturais, porquanto “decorrem das macrovariáveis econômicas, políticas, ambientais e etc. capazes de afetar” seus resultados. Embora incidam em menor quantidade, o impacto causado por tais eventos nos resultados da organização tende a ser maior dada a importância da estratégia para o alcance de objetivos (PADOVEZE, 2008, p. 7-8).

Os **riscos de gestão** são definidos pelo autor como episódios futuros, advindos de decisões administrativas e da assunção de riscos administrativos - cuja responsabilidade é da alta administração -, e que tenham potencial de causar impactos negativos ou positivos nos resultados da organização, nos quais se enquadram, por exemplo, os modelos de gestão tributária, contábil e financeira, de gestão de recursos humanos e de tecnologia da informação (PADOVEZE, 2008, p. 7-8).

**Riscos operacionais**, por fim, conforme o autor, são aqueles decorrentes de eventos que podem ser causados por todos e qualquer colaborador da organização, o que aumenta em muito a sua possibilidade de ocorrência, cujos impactos podem variar a depender da situação específica. Como exemplo, o autor cita a compra de um determinado item por um valor acima do esperado e do possível (PADOVEZE, 2008, p. 7-8).

Por sua vez, Assi (2012) faz uma descrição pormenorizada do que define como algumas categorias de riscos com as quais as organizações podem se

deparar na busca pelos seus objetivos, abordando algumas espécies de riscos incidentes sobre as organizações em suas mais diversas esferas de atuação.

Nada obstante, seguindo a linha traçada para o presente estudo, abordar-se-á adiante apenas as espécies de riscos de alguma forma incidentes sobre as atividades das instituições públicas de ensino superior - ou seja, riscos que, dada a natureza da atividade que exercem tais instituições, possam incidir sobre objetivos, processos e atividades inerentes a cada um dos seus níveis organizacionais (estratégico, tático e operacional, sem prejuízo de outras categorizações que porventura venham a adotar) -, reservando-se o Apêndice A para a apresentação das demais classificações trazidas pelo sobredito autor:

•**Risco operacional:** Trata-se das “possibilidades de perdas diretas e indiretas, em função de fraquezas ou ausências de processos e controles internos adequados, e também como perdas decorrentes de eventos externos”, sendo exemplos “fraudes, erros de sistemas de informações, erros de escrituração, extrapolação de autoridade dos empregados, desempenho insatisfatório, incêndios, catástrofes, crises sociais, problemas com infraestrutura pública e crises sistêmicas”, tendo como subcategorias: Risco de Overload, traduz o “risco de perdas por sobrecargas nos sistemas elétricos, telefônicos, de processamento de dados, internet etc.”; Risco de obsolescência, compreende o “risco de perdas pela falta de substituição frequente dos equipamentos e softwares antigos”; Risco de presteza e confiabilidade, caracterizado pela “probabilidade de perdas pelo fato de as informações não poderem ser recebidas, processadas, armazenadas e transmitidas em tempo hábil e de modo confiável”; Risco de equipamento, que consiste na “probabilidade de perdas por falhas nos equipamentos elétricos, de processamentos de dados, telefônicos, de segurança, por falta de manutenção ou negligência humana etc.”; Risco de erro não intencional, em geral “identificado por perdas em decorrência de equívocos, omissões, distração, despreparo ou negligência operacional de funcionários ou colaboradores”; Risco de fraude, decorrente “de comportamento fraudulento, tais como adulteração de controles e de relatórios, descumprimento intencional de normas da empresa, ausência de conduta ética, desvio de valores, divulgação de informações restritas ou indevidas”; Risco de qualificação, assim entendido como as “perdas por problemas de ausência de qualificação profissional apropriada à função ou por contratação sem a devida validação do colaborador”;

Risco de produtos e serviços, a incidir “quando a venda de produtos ou prestação de serviços ocorrerem de modo indevido ou sem atender às necessidades e demandas dos clientes”; Risco de regulamentação, caracterizado por “perdas em decorrência de alterações, impropriedades ou inexistência de normas para controles internos e externos”; Risco de modelagem, definido “como perdas ocasionadas no desenvolvimento, utilização ou interpretação incorreta dos resultados fornecidos por modelos, incluindo a utilização de dados incorretos, por falhas no projeto”; Risco sistêmico, decorrente de “mudanças no ambiente operacional, alterações de limites, alteração de sistemas e ausência de homologação dos sistemas”; Risco de imagem, caracterizado por “perdas decorrentes do impacto negativo na marca da organização, por falha de controle interno, de procedimentos, de atendimento e de qualidade, e a perda tem caráter intangível”; e Risco de catástrofe, que envolvem “perdas por desastres naturais, que possam dificultar as operações diárias, ou destruição por desastres como incêndios, colisões, explosões, terremotos, tsunamis, furacões etc.”.

•**Risco legal**: Envolve eventos decorrentes de demandas jurídicas oriundas de negócios relacionados à organização com potencial de provocar perdas ou impactos não levados em consideração quando do firmamento do negócio, “como documentação das transações incorretas, descumprimento da legislação vigente, novas leis, decisões judiciais, análise de processos e defesas inadequadas etc.”.

•**Risco contratual**: Caracterizado como a “possibilidade de perda relacionada à inadequação formal do contrato, à interpretação errônea de suas cláusulas e à sua desconformidade com a legislação pertinente”.

•**Risco de conformidade**: Definido pelo autor como a “possibilidade de perda ocasionada pela inobservância, violação ou interpretação indevida de regulamentos e normas”. Conforme o COSO (2020, p. 1), os riscos de conformidade estão “relacionados a possíveis violações de leis, regulamentos, termos contratuais aplicáveis, padrões, ou políticas internas” cuja inobservância possa trazer consequências negativas para a “organização ou seu pessoal”.

•**Risco político**: Decorrente “de mudanças promovidas por autoridades políticas” capazes de afetar a gestão da organização e os seus resultados.

•**Risco de terceirização**: Reside na “possibilidade de perdas decorrentes da transferência da gestão e operação de processos internos para outras entidades,”

uma vez que, ao contratar um terceiro, a organização está “transferindo somente as atividades, pois o risco continua sob a responsabilidade do contratante”.

•**Risco contábil:** Decorre da adoção de procedimentos de contabilidade que não atenda aos princípios e regras da boa prática contábil, seja por “acidentes ou casos fortuitos, erro de valorização de carteiras, erros de comunicação e discrepâncias no tratamento contábil”, e que podem trazer impactos negativos à organização, como “sanções dos órgãos reguladores [...] e reputação maculada”.

•**Risco de controle:** Se afigura “mais amplo que o risco contábil e inclui os riscos de falhas dos sistemas internos de informação, por meio de operações negligentes, projetos de TI ruins ou fraude deliberada”, tendo em vista que as decisões costumam ter por base informações constantes de relatórios gerenciais.

•**Risco de desastre:** “Decorre de desastres naturais e pode ser segurado”, cujo “efeito pode ser minimizado por planos de contingência, planos de recuperação de desastres ou sistemas de cópia de segurança”.

Cumprido destacar que o rol trazido por Padoveze (2008) e Assi (2012) e aqui apresentado não é taxativo, embora represente uma gama de categorias de riscos incidentes sobre as organizações nos seus mais variados ramos de atuação, sobretudo porque, conforme sustenta Ávila (2014, p. 186), “a eliminação ou redução de um tipo de risco variavelmente acarretará na criação de outros, potencialmente imprevistos”.

De fundamental importância para o presente estudo também se revelam as definições de **risco inerente** e **risco residual**, sendo que o primeiro diz respeito ao “risco a que uma organização está exposta sem considerar quaisquer ações gerenciais que possam reduzir a probabilidade de sua ocorrência ou seu impacto”, ao passo que o segundo refere-se ao risco remanescente “após a implementação de ações gerenciais para o tratamento do risco”, conforme conceitua em seu art. 2º, XIV e XV a Instrução Normativa Conjunta MPOG/CGU nº 01/2016.

Assim, embora a título de conhecimento não se discuta a importância da categorização trazida pelos autores supracitados, necessário se faz esclarecer que valeu-se o presente estudo apenas das categorias de riscos incidentes também sobre as organizações públicas que, como evidenciado, constituem o objeto da presente pesquisa.

## 2.5 A GESTÃO DE RISCOS NAS ORGANIZAÇÕES

Com base nas definições de risco trazidas nos tópicos anteriores é possível inferir que gerir/gerenciar/administrar riscos constitui atividade essencial para que uma organização, seja ela pública ou privada, venha a desenvolver suas estratégias com eficiência, e por meio delas se tornar eficaz quanto ao alcance dos seus objetivos.

Nesse sentido, as lições de Matias-Pereira (2014) acerca da definição e distinção entre eficácia e eficiência se revelam valiosas para a compreensão do tema proposto no presente estudo, porquanto aclaram ser a eficácia uma “medida normativa do alcance de resultados, enquanto a eficiência é uma medida normativa da utilização de recursos nesse processo”, ou seja, refere-se a eficiência ao método pelo qual são desenvolvidas as ações que buscam o alcance do resultado, e a eficácia “ao grau de qualidade do resultado” alcançado (p. 76).

Acerca da gestão de riscos, Padoveze (2008, p. 194), aduz que pode ser organizada a partir de visões relacionadas aos ambientes internos e externos da organização, de modo que no primeiro ambiente o risco é visto por uma perspectiva de conformidade, ao passo que no segundo é encarado por uma perspectiva de desempenho.

Assi (2012), por sua vez, esclarece que, com base na análise SWOT, no ambiente interno estarão localizados os pontos fortes e fracos da organização, resultantes da sua estratégia e representados, dentre outros, por seus recursos físicos, humanos e financeiros, enquanto no ambiente externo à organização surgirão as ameaças e oportunidades, capazes de sobre ela exercer influência, embora fora dos seus limites.

Quanto aos objetivos, Florencio (2018, p. 9) elucida que gerenciar riscos de forma estratégica visa proteger contra efeitos das incertezas o que de mais caro há para organização e os objetivos do negócio, que é justamente o que a faz diferente de todas as outras, de forma que “gerir os riscos significa conhecer se a empresa conta com objetivos estratégicos ou se conhece os fatores com poder de influência na realização desses objetivos”.

No mesmo estudo, defende a autora uma maior importância da gestão de riscos na atualidade, a ponto de indicar a conveniência de sua departamentalização nas organizações:

O objetivo principal do gerenciamento de riscos corporativos é gerar valor aos envolvidos na empresa, administrando as incertezas – riscos ou oportunidades – que podem reduzir ou aumentar esse valor; a organização busca atingir seus objetivos e evitar danos e imprevistos no caminho. A nova função do gerenciamento de riscos corporativos – inteligência em riscos – alerta que as empresas devem ter uma visão holística em relação ao gerenciamento dos riscos, devendo os seus gestores terem conhecimento consolidado desses riscos nas esferas legal, financeira, operacional e estratégica, com departamento próprio responsável por essas avaliações (Departamento de Gestão de Riscos), dispondo de estrutura e processos que permitam o amplo e contínuo conhecimento desses riscos. (2018, p. 10)

No entanto, em Sumário Executivo lançado em 2017, o COSO (2017) traz ressalvas quanto ao que trata como interpretações equivocadas sobre o gerenciamento de riscos, o que faz ao afirmar que não se trata o instituto de uma mera função ou um departamento, mas sim da conjugação estruturada de cultura, competências e práticas implementadas na organização com vistas ao delineamento e execução da sua estratégia, cujo objetivo é o enfrentamento das incertezas incidentes na criação, preservação e realização de valor, de forma que seus princípios devem ser aplicados a todos os níveis e funções da organização.

Ainda a título do que classifica como esclarecimentos acerca de interpretações equivocadas, o COSO (2017) enfatiza que o gerenciamento de riscos não deve ser observado apenas como um inventário dos riscos incidentes sobre a organização ou um mero *checklist* de procedimentos, e sim compreendido também como as práticas das quais lança mão a organização para estruturar seu gerenciamento de riscos, que não se restringe ao controle interno, pois deve abranger a definição da estratégia, a governança, a comunicação com as partes interessadas, assim como a aferição do desempenho, visando à melhoria da performance e o aprendizado contínuo.

Sobre o mesmo tema, Portela (2014) ressalta como papel central da gestão de riscos a atividade de identificação dos riscos necessários, cujo enfrentamento se traduz em necessidade:

O objetivo central do gerenciamento de riscos é o de não aceitar riscos desnecessários, e apenas aceitar aqueles riscos que sejam absolutamente necessários para a organização e compatíveis com as pessoas, com a sociedade e o meio ambiente em que se insere. Entenda-se por “absolutamente necessários” aqueles riscos que, independentemente de seu valor, por alguma razão subjetiva ou objetiva precisam ser aceitos e enfrentados para a sobrevivência das partes envolvidas, sejam estas organizações, indivíduos ou sociedades (2014, p. 45-46)

No que pertine à atribuição de papéis aos envolvidos no processo de gestão de riscos, o modelo das três linhas de defesa – ofertado na Declaração de Posicionamento do IIA - *The Institute of Internal Auditors*<sup>3</sup>: As Três Linhas de Defesa no Gerenciamento Eficaz de Riscos e Controles (2013) – oferece um delineamento de atribuição de responsabilidades entre os envolvidos no processo de gerenciamento de riscos dentro da organização, estruturando na primeira linha ou camada de defesa as responsabilidades operacionais da execução, na segunda linha aquelas relacionadas à supervisão e ao monitoramento, e na terceira e última linha ou camada a responsabilidade pela avaliação dos processos e seus resultados, cuja independência permite fornecer informações confiáveis aos órgãos de governança e à alta administração.

Voltando-se para o gerenciamento dos riscos em projetos de forma geral, o Guia PMBOK (2017, p. 395) atribui a tal instrumento “os processos de condução do planejamento, da identificação, da análise, do planejamento das respostas, da implementação das respostas e do monitoramento dos riscos”, cujo objetivo precípua é “aumentar a probabilidade e/ou o impacto dos riscos positivos e diminuir a probabilidade e/ou o impacto dos riscos negativos”, e assim fazer com que as chances de sucesso de um determinado projeto sejam aumentadas, pois, para o Guia em questão, um projeto cujo gerenciamento de riscos não se mostre eficaz acumula grande chance de estar fadado ao insucesso.

Com enfoque para riscos em matéria de segurança, Portella (2014, p. 43) aduz que gerenciar riscos passa por métodos e técnicas capazes de lidar com o imprevisível, o imponderável e o subjetivo, “seja por influência de forças naturais,

---

<sup>3</sup> Criado em 1941, The Institute of Internal Auditors (IIA) é uma associação profissional internacional, com sede global em Altamonte Springs, Flórida, EUA. O IIA é o líder reconhecido, principal defensor e educador em auditoria interna. Declarações de Posicionamento fazem parte da Estrutura Internacional de Práticas Profissionais (IPPF) do IIA, a estrutura conceitual que organiza as orientações oficiais promulgadas pelo IIA.



falhas de projeto, falhas de equipamento, falhas de operação, falhas de gestão ou qualquer tipo de erro humano”.

Abordando questões proeminentes acerca do tema, cuja relevância justifica a transcrição no presente estudo, Bezerra (2013, p. 5-6) apresenta princípios que reputa imprescindíveis para que uma organização possa implementar, em todos os seus níveis, uma gestão de riscos eficaz, destacando que:

a. **A gestão de riscos cria e protege valor**, pois, em razão do seu caráter preventivo e continuado, possibilita ao gestor um panorama do desempenho da organização no caminho trilhado rumo aos seus objetivos, direcionando-o para a proteção do que lhe é mais caro em termos de princípios e valores, bem como lhe indicando eventuais oportunidades.

b. **A gestão de riscos é parte integrante de todos os processos organizacionais**, não podendo ser vista como ação pontual e isolada na organização, pois, “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.”

c. **A gestão de riscos é parte da tomada de decisões**, posto que “auxilia os tomadores de decisão a fazer escolhas conscientes, priorizar ações e distinguir entre formas alternativas de ação.”

d. **A gestão de riscos aborda explicitamente a incerteza**, levando “em consideração a incerteza, a natureza dessa incerteza, e como ela pode ser tratada”.

e. **A gestão de riscos é sistemática, estruturada e oportuna**, de modo que “uma abordagem sistemática, oportuna e estruturada para a gestão de riscos contribui para a eficiência e para os resultados consistentes, comparáveis e confiáveis.”

f. **A gestão de riscos baseia-se nas melhores informações disponíveis**, tendo em vista que “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”, o que não exclui a responsabilidade do gestor acerca da consideração quanto à fonte mais adequada.

g. **A gestão de riscos é feita sob medida**, uma vez que “está alinhada com o contexto interno e externo da organização e com o perfil do risco.”

h. **A gestão de riscos considera fatores humanos e culturais**, de forma que deve reconhecer “as capacidades, percepções e intenções do pessoal interno e externo, que podem facilitar ou dificultar a realização dos objetivos da organização.”

i. **A gestão de riscos é transparente e inclusiva**, de modo que a adequada participação das partes interessadas e “dos tomadores de decisão em todos os níveis da organização assegura que a gestão de riscos permaneça pertinente e atualizada”, assim possibilitando que todas as partes participem da “determinação dos critérios de risco”.

j. **A gestão de riscos é dinâmica, iterativa e capaz de reagir a mudanças**, vez que propõe, como rotina cíclica, identificar e reagir a eventuais mudanças, sejam elas de cunho interno ou externo, pois, diante delas, “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.”

k. **A gestão de riscos facilita a melhoria contínua da organização**, razão pela qual “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.”

Na linha dos princípios tratados, Vieira e Barreto (2019, p. 144) ressaltam a importância da técnica 5W2H para o gerenciamento das atividades, sobretudo no que se refere ao tratamento de riscos, cujo planejamento deve contemplar as informações sobre as atividades que serão executadas (*What* – o que será feito?), o objetivo que se pretende alcançar (*Why* – Por que será feito?), o responsável pela execução (*Who* – Por quem será feito?), o momento da execução (*When* - Quando será feito?), o local da execução da atividade (*Where* – Onde será feito?), o modo pelo qual será executada (*How* – Procedimento ou forma de realização) e, por fim, o custo envolvido (*How Much* – Investimento/Tempo envolvidos).

Assim, antever e lidar com as incertezas pode ser crucial para a subsistência de uma organização, circunstância esta que reclama a implementação de procedimentos estruturados e voltados à identificação, avaliação, controle e monitoramento de riscos, envolvendo todos os níveis da organização, o que, conforme defende ÁVILA (2014, p. 186), “exige um esforço interdisciplinar, pessoas de diferentes setores e áreas devem trabalhar em conjunto para desenvolver uma perspectiva holística e sistemática de fatores de risco existentes em cada caso”.

Portanto, conforme o COSO (2017), desde que conte com missão, estratégia e objetivo, e que considere necessário tomar decisões que digam respeito ao enfrentamento das incertezas incidentes sobre as atividades relacionadas ao atingimento de tais preceitos, toda e qualquer organização, inclusive órgãos governamentais, pode e deve implementar a gestão de riscos, posto que aplicável às organizações independentemente do porte que ostentem.

## 2.6 A GESTÃO DE RISCOS NA ADMINISTRAÇÃO PÚBLICA

O fato de tratar da coisa pública sempre impôs à Administração Pública o dever de exercer seu múnus observando princípios que miram o melhor aproveitamento dos recursos disponíveis e a satisfação dos anseios da coletividade, consoante tratado no item 2.1 deste trabalho. Hodiernamente, no entanto, tal observância vem sendo cada vez mais exigida do gestor público, de forma a se fazer necessária a implantação de instrumentos de controle capazes de identificar, avaliar, controlar e monitorar eventuais riscos que possam impactar na consecução desse objetivo precípuo.

Não por acaso, em seu Manual de Gestão de Riscos (TCU, 2018), o Tribunal de Contas da União já ressalta que adoção estratégica de procedimentos visando à gestão de riscos no âmbito de uma instituição pública é providência com potencial de aumentar sua capacidade “para lidar com incertezas, estimular a transparência e contribuir para o uso eficiente, eficaz e efetivo de recursos, bem como para o fortalecimento da imagem da instituição”, de forma a evidenciar não apenas a conveniência da implantação da prática nos órgãos da Administração Pública, mas também a sua necessidade para cumprimento da missão de bem atender aos anseios da sociedade.

Baseando-se nas melhores práticas de gestão de riscos conhecidas em nível internacional, o mesmo Manual recomenda “a adoção de sistemas de gerenciamento de riscos associados aos processos de planejamento, de tomada de decisão e de execução dos trabalhos relevantes”, porquanto capazes de assegurar sejam atingidos os objetivos da Administração Pública, “com a melhor relação custo-benefício” (TCU 2018), sem descuidar de traçar um breve (mas elucidativo) histórico acerca da gestão de riscos no setor público, consoante adiante transcrito:

A iniciativa de implantar a gestão de riscos no setor público é relativamente recente no Brasil, embora, em alguns países, tenha começado há mais tempo. No Reino Unido, no início dos anos 1990, foi implantada com a finalidade de aumentar o empreendedorismo no setor público e, desde então, vem se consolidando como parte integrante do processo de gestão. Atualmente, a *Commonwealth* conta com uma política de gestão de riscos para o setor público.

No contexto brasileiro, é importante lembrar a Emenda Constitucional nº 19, de 1998, que acrescentou o conceito da eficiência no rol dos princípios que regem toda a administração pública federal (CF, art. 37, *caput*). O objetivo principal da gestão de riscos é aumentar o grau de certeza na consecução dos objetivos, o que tem impacto direto na eficiência.

O Ministério do Planejamento, Desenvolvimento e Gestão (MP), Ministério da Transparência e Controladoria-Geral da União (CGU) expediram, em 2016, a Instrução Normativa Conjunta nº 01, que dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo Federal.

O MP lançou, em 2017, o Manual de Gestão de Integridade, Riscos e Controles Internos da Gestão.

Ainda em 2017, foi editado o Decreto nº 9.203, de 22 de novembro de 2017, que dispõe sobre a política de governança da administração pública federal, que trata, entre outros temas, da gestão de riscos na administração pública.

Nesse sentido, importante registrar que o retro mencionado Decreto nº 9.203/2017, que “dispõe sobre a política de governança da administração pública federal direta, autárquica e fundacional”, define, em seu art. 2º, IV a gestão de riscos 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.

Ainda, aponta o mesmo Decreto para a gestão de riscos como um mecanismo de governança na modalidade controle, que compreende:

processos estruturados para mitigar os possíveis riscos com vistas ao alcance dos objetivos institucionais e para garantir a execução ordenada, ética, econômica, eficiente e eficaz das atividades da organização, com preservação da legalidade e da economicidade no dispêndio de recursos públicos” (Art. 5º, III).

Por fim, crava a obrigatoriedade da estruturação da gestão de riscos no art. 17, *in verbis*:

Art. 17. A alta administração das organizações da administração pública federal direta, autárquica e fundacional deverá estabelecer, manter, monitorar e aprimorar sistema de gestão de riscos e controles internos com vistas à identificação, à avaliação, ao tratamento, ao monitoramento e à análise crítica de riscos que possam impactar a implementação da

estratégia e a consecução dos objetivos da organização no cumprimento da sua missão institucional, observados os seguintes princípios:

I - implementação e aplicação de forma sistemática, estruturada, oportuna e documentada, subordinada ao interesse público;

II - integração da gestão de riscos ao processo de planejamento estratégico e aos seus desdobramentos, às atividades, aos processos de trabalho e aos projetos em todos os níveis da organização, relevantes para a execução da estratégia e o alcance dos objetivos institucionais;

III - estabelecimento de controles internos proporcionais aos riscos, de maneira a considerar suas causas, fontes, consequências e impactos, observada a relação custo-benefício; e

IV - utilização dos resultados da gestão de riscos para apoio à melhoria contínua do desempenho e dos processos de gerenciamento de risco, controle e governança.

Na esfera da Administração Pública Indireta, a Lei nº 13.303/2016, que “dispõe sobre o estatuto jurídico da empresa pública, da sociedade de economia mista e de suas subsidiárias, no âmbito da União, dos Estados, do Distrito Federal e dos Municípios”, determina em seus artigos 6º e 9º que os atos constitutivos das sobreditas pessoas jurídicas e de suas subsidiárias deverão observar, dentre outros preceitos, práticas estruturadas de gestão de riscos e de controle interno, inclusive com a implantação de área responsável pela verificação quanto à observância dos preceitos e atividades inerentes ao controle em questão.

A supra aludida Instrução Normativa Conjunta MP/CGU nº 01/2016, por sua vez, define o gerenciamento de riscos como o “processo para identificar, avaliar, administrar e controlar potenciais eventos ou situações, para fornecer razoável certeza quanto ao alcance dos objetivos da organização” (Art. 2º, VII).

No âmbito da UFS, a gestão de riscos resulta assim definida no art. 2º, VI, da Resolução 15/2020/CONSU:

processo de natureza permanente, estabelecido, direcionado e monitorado pela alta administração, que contempla as atividades de identificação, avaliação e gerenciamento das consequências de potenciais eventos que possam afetar a organização, destinado a fornecer grau de segurança razoável quanto à realização de seus objetivos.

Para Ávila (2014, p. 184), levando-se em consideração a premissa de que a Administração Pública tem como dever precípua o cuidado para com a coisa pública, a gestão de riscos deve sempre estar voltada para o interesse público, sendo necessário que os tomadores de decisão estejam investidos da capacidade de equacionar probabilidade de benefícios e perdas em potencial decorrentes de eventos incertos, pois o “objetivo do gerenciamento de riscos na Administração Pública é, em última análise, o interesse coletivo e deve resultar em melhorias na

qualidade dos serviços ofertados pelo governo e a eficácia de suas políticas públicas”.

No mesmo sentido, Vieira e Barreto (2019, p. 97) explicam que a consecução das finalidades inerentes ao setor público “envolve riscos decorrentes da natureza de suas atividades, de realidades emergentes, de mudanças nas circunstâncias e nas demandas sociais, da própria dinâmica da administração pública”, dentre outros advindos da necessidade de transparência e *accountability*, o que justifica uma maior necessidade de sistematização do gerenciamento de riscos, a fim de “assegurar que os objetivos sejam alcançados” (VIEIRA; BARRETO, 2019, p. 97).

Na mesma linha de entendimento, Hill (2006) ressalta o fundamental papel do gestor público na busca pela eficiência dos serviços públicos, enfatizando que a gestão de riscos visa possibilitar que, sempre que a situação assim exigir, o decisor possa identificar as melhores escolhas:

A intenção da gestão de riscos é aumentar os benefícios e diminuir os custos de atividades incertas. O governo lida com riscos por meio de diversas funções, como, por exemplo, a função de proteger direitos, criar condições para a prosperidade econômica, manter a integridade do meio ambiente, melhorar a saúde humana ou de prestar serviços governamentais.

Em quase todos os casos, a gestão de riscos exige que os decisores ponderem e aceitem meios-termos entre interesses conflitantes em seus esforços para identificar uma solução ótima e aceitável. As soluções para problemas relacionados à gestão de riscos provavelmente envolverão opções em termos de políticas com vistas a identificar e advertir pessoas no sentido de que modifiquem seus comportamentos, reduzir riscos por meio de regulação (ou de outros instrumentos) ou compensar pessoas que sofreram impactos negativos de um evento de risco (HILL, 2006, p. 38).

Observa-se que o autor alerta também para a necessidade de mudança de comportamento e cultura organizacional sempre que necessária para melhoria contínua da gestão de riscos, de modo a elucidar a importância de todos os envolvidos no processo, e não apenas da alta administração, embora deva o processo se desenvolver sob a coordenação desta.

Nesse sentido, Hill e Dinsdale (2003, p. 13) ressaltam o caráter humano da gestão de riscos, sustentando que os riscos, além de atrelados à probabilidade, também são produtos de “contextos culturais, sociais e políticos que afetam as reações e percepções das pessoas diante de eventos incertos”, destacando a essencialidade do servidor público para uma gestão de riscos que se pretenda eficaz.

Corroborando tal entendimento, ao prefaciando a obra de Bermejo *et al.* (2019), o professor Rodrigo Fontenelle aponta para alguns mitos que ainda distanciam o servidor público da gestão de riscos, dentre eles:

O primeiro grande mito fala que a gestão de riscos vai aumentar o trabalho, ou seja, se eu introduzir essa tarefa na minha organização, no meu departamento, terei de trabalhar mais. Não foi uma nem duas vezes que ouvi: “Eu já trabalho 8, 9 e até 10 horas por dia. Você quer que agora, além disso, eu faça gestão de riscos?”. A partir desse comportamento, percebemos claramente que o gestor não entendeu o que é a gestão de riscos. Percebe-se que a premissa utilizada por ele está errada. Gestão de riscos não é “mais uma atividade”. É uma mudança de cultura, uma nova forma de olhar o seu próprio negócio/processo.

Respondendo a questionamento próprio, consubstanciado na interrogativa direta “Por que a gestão de riscos é importante?”, Hill e Dinsdale (2003) trazem a lume a ideia de riscos como eventos negativos ou positivos vista em capítulo antecedente, com a ênfase tanto para a gestão de riscos proativa quanto para as oportunidades que dão ensejo à inovação (responsável), que constitui predicado em muito perseguido no âmbito da Administração Pública:

**Ela ajuda a evitar eventos indesejáveis**

A gestão eficaz de riscos reduz a probabilidade e a severidade de eventos indesejáveis. Podemos evitar eventos indesejáveis ou negativos prevenindo sistematicamente os riscos, avaliando a sua importância, gerenciando suas consequências e aprendendo enquanto atravessamos esse ciclo.

No entanto, a gestão eficaz de riscos implica também prever os riscos futuros e saber lidar de maneira proativa com eles – gestão proativa em vez de reativa. Frequentemente, podemos superar adversidades sendo proativos na previsão de riscos e na criação de condições que nos permitam evitá-los.

**Ela abre oportunidades para inovação**

Proteger-se contra todos os riscos é impossível, porque qualquer oportunidade invariavelmente acarreta riscos. Aaron Wildavsky (1979), um acadêmico conhecido, caracterizou esse dilema em artigo que escreveu para a revista *American Scientist*, intitulado “No risk is the highest risk of all”. Assumir riscos é uma pré-condição essencial para o desenvolvimento humano; se parássemos de assumir riscos, inovações técnicas e sociais necessárias para solucionar muitos dos problemas mundiais desapareceriam. De fato, muitos dos riscos existentes na sociedade moderna resultam de benefícios gerados por inovações sociais e tecnológicas. Por outro lado, a imprudência insensata também não é uma boa ideia. Em vez disso, precisamos definir um caminho intermediário no qual o acaso – com suas incertezas e ambigüidades inerentes – seja levado em consideração de maneira objetiva, racional e eficiente. (HILL; DINSDALE, 2003, p.17)

No que tange à força de trabalho na Administração Pública diante da inovação, Hill e Dinsdale (2003, p.17) defendem que “nenhum servidor público inovador pode evitar decisões que envolvam riscos”, de modo que “todos devem

possuir as habilidades e competências necessárias para gerenciar” tais eventos, o que, segundo os autores, pode ser alcançado das três seguintes maneiras:

- 1) **com base na experiência pessoal passada e nas experiências de outros**, alternativa na qual “os estudos de casos são ferramenta útil para dotar os servidores de conhecimentos provenientes de ampla variedade de experiências passadas”;
- 2) **com base em técnicas de tentativa e erro em áreas em que não se tenha experiência própria**, abordagem pela qual “é importante permitir que os gerentes de serviços públicos participem ativamente de experimentos gerenciais baseados em tentativa e erro – também conhecidos como gestão adaptativa”; e
- 3) **com base em abordagens mais dedutivas extrapoladas a partir de teoria ou modelo mental geral (ou seja, da teoria para a observação e desta para a ação)**, na qual se recomenda “ajudar os gerentes a perceber como os seus modelos mentais afetam a sua compreensão dos riscos – talvez por meio do desenvolvimento de cenários, esforços interdisciplinares ou diálogos públicos.”

No entanto, nada obstante as premissas trazidas no estudo apontado, realizado no Canadá no início dos anos 2000, a gestão de riscos na Administração Pública brasileira ainda caminha a passos curtos, o que se pode extrair do Relatório de Políticas e Programas de Governo (RePP) – desenvolvido pelo TCU “em cumprimento ao disposto no art. 123 da Lei de Diretrizes Orçamentárias (LDO) 2018”, que atribui ao referido órgão de controle a responsabilidade por enviar ao Congresso Nacional “um quadro-resumo relativo à qualidade da implementação e ao alcance de metas e objetivos dos programas e ações [...] para subsidiar a discussão do Projeto de Lei Orçamentária Anual” – cujas conclusões resultam assentadas no Acórdão nº 2.127/2017 (TCU-Plenário), aqui extraído do Referencial básico de Gestão de Riscos, desenvolvido pelo TCU, em sua edição 2018 (p. 130).

Referido acórdão aponta para um cenário deficitário no tocante à governança e gestão de riscos nas instituições públicas federais, responsáveis pela ineficiência “generalizada” na aplicação dos recursos públicos, capazes de “perenizar” a baixa eficácia dos bens e serviços ofertados, consoante abaixo transcrito:



O Relatório de Políticas e Programas de Governo (RePP) **apresenta como achado fundamental que a existência de déficits institucionais de governança e de gestão da administração pública federal produzem ineficiências generalizadas no gasto público federal. As ineficiências apontadas no relatório implicam consideráveis desperdícios e desvios sistêmicos na aplicação dos recursos públicos federais.** Com base na análise dos achados consolidados, conclui-se que **os referidos déficits institucionais, se não corrigidos, são capazes de perenizar a baixa eficácia dos bens e serviços públicos ofertados pelo Estado, que têm sido percebidos pela sociedade, em regra, como inadequados e de pouca qualidade.**

No tocante aos problemas estruturantes na Administração Pública Federal, verificou-se a existência de falhas na estratégia do Estado, como ausência de plano de longo prazo, fragilidades do PPA, ausência generalizada de planos estratégicos institucionais e falta de uniformidade e padronização dos planos nacionais setoriais, que dificultam o desenvolvimento sustentável de políticas e programas públicos e prejudicam a efetividade das ações governamentais.

Além disso, o relatório afirma que **a baixa capacidade do Estado em planejar e coordenar as diversas políticas públicas tem levado a aumento do risco de desperdício de recursos, do comprometimento de resultados e da baixa qualidade dos serviços à população.** Ademais, existem impropriedades na Governança Orçamentária do país que comprometem a alocação efetiva e eficiente do gasto público. (sem destaques no original).

O Emblemático aresto aponta, ainda, para a “ineficiência dos mecanismos de monitoramento e avaliação governamental e gestão de riscos”, ali indicados como fatores que “dificultam o acompanhamento e aferição de resultados e impedem o alcance dos objetivos almejados”, concluindo pela premente e imprescindível necessidade de adoção de medidas nos mais diversos órgãos da Administração Pública Federal para fins de sistematização de uma eficiente e eficaz gestão de riscos (TCU, 2018, p. 131).

De tudo quanto até aqui visto se pode extrair que, dada a natureza de sua atuação e, sobretudo, em razão dos princípios aos quais deve estar submetida, a Administração Pública, seja ela direta, autárquica ou fundacional, tem o dever de instituir programas de governança que necessariamente incluam a sistematização estruturada de um efetivo controle de riscos, com o fito de conferir razoável segurança à busca pelo alcance dos objetivos, estes indissociáveis do interesse público.

Assim, no afã de gerenciar riscos incidentes sobre a sua atuação, os entes da Administração Pública, igualmente como ocorre nas organizações de natureza privada, têm ao seu alcance uma gama de modelos, metodologias e ferramentas capazes de proporcionar análises das mais singelas e gerais às mais completas e

específicas, de acordo com as necessidades e características de cada organização (TCU, 2018), e é acerca de tais instrumentos que versa o item adiante apresentado, tendo por base referencial publicado pelo TCU.

## 2.7 MODELOS E TÉCNICAS DE GESTÃO DE RISCOS APLICÁVEIS À ADMINISTRAÇÃO PÚBLICA

Objetivando auxiliar os órgãos da Administração Pública na implementação do gerenciamento de riscos determinada no Decreto nº 9.203/2017 e demais normativas que compõem o novo marco regulatório da governança pública, o TCU publicou, em abril de 2018, o “Referencial Básico de Gestão de Riscos”, pelo qual apresenta orientações técnicas com vistas à implantação de boas práticas de gestão de riscos nas organizações públicas, inclusive modelos e ferramentas das quais podem tais instituições lançar mão para estruturação do gerenciamento de riscos nos seus respectivos âmbitos (TCU, 2018).

O referido guia traça uma evolução histórica dos modelos de gerenciamento de riscos conhecidos, cravando acerca da existência de quatro modelos de referência, cujo exame prévio se revela obrigatório para toda e qualquer organização que deseje implementar uma estrutura de gerenciamento de riscos, sendo eles: 1. COSO II – Gerenciamento de Riscos Corporativos – Estrutura Integrada (2004); 2. COSO – Gerenciamento de Riscos Corporativos – Integrado com Estratégia e Performance (2017); 3. ISO 31000 – Gestão de Riscos – Princípios e Diretrizes (2018); e 4. *Orange Book e Risk Management Assessment Framework* (TCU, 2018).

Portanto, é de uma concisa exposição dos modelos mencionados, bem com da apresentação de ferramentas e técnicas propostas pelo TCU para um gerenciamento de riscos que se pretenda adequado, que se ocupa o presente item.

### **2.7.1 Os modelos COSO II – Gerenciamento de Riscos Corporativos – Estrutura Integrada (2004); e COSO – Gerenciamento de Riscos Corporativos – Integrado com Estratégia e Performance (2017), e seus desdobramentos**

O *Committee of Sponsoring Organizations of the Treadway Commission* (Comitê das Organizações Patrocinadoras da Comissão *Treadway*) – COSO é

entidade privada e sem fins lucrativos criada nos Estados Unidos em 1985 com o fito de desenvolver instrumentos de controle capazes de prevenir e coibir a prática de fraudes contábeis por parte de organizações (ASSI, 2012), e que, desde então, elabora recomendações que servem de referência quando se trata de estruturação de controles internos nas organizações de diversos países.

Por meio do guia *Internal Control - Integrated Framework* (COSO I), de 1992, a entidade apresentou ao mundo das organizações um conjunto estruturado de princípios e boas práticas de controle interno que, embora voltado às especificidades do processo de controle interno como um todo - e, por tal razão, não abordando detalhadamente um processo de gestão de riscos -, serviu para consolidar a ideia disseminada de gestão de riscos corporativos (TCU, 2018).

Em 2004, o COSO fez publicar o guia *Enterprise Risk Management - Integrated Framework - COSO ERM* (Gerenciamento de Riscos Corporativos – Estrutura Integrada ou, simplesmente, COSO II) pelo qual ampliou o componente de avaliação de riscos trazidos pelo COSO I, mantendo-se, entretanto, os componentes de controle interno, sob a justificativa de que controles internos efetivos são condição essencial para um gerenciamento de riscos eficaz (COSO, 2004).

O modelo de gerenciamento de riscos proposto pelo COSO II pressupõe uma relação indissociável entre os objetivos da organização e os componentes de gerenciamento de riscos, componentes estes entendidos como etapas e caminhos essenciais que deve a organização percorrer rumo ao alcance dos sobreditos objetivos, pressuposto representado na forma de cubo, conforme Figura 1.

Consoante se extrai da Figura 1, a dimensão superior (linhas verticais) alberga as categorias de objetivos da organização, objetivos estes que, inter-relacionadas que são, devem estar alinhados a sua missão ou visão, de modo a proporcionar uma abordagem completa dos diferentes aspectos relacionados ao gerenciamento de riscos da organização (COSO, 2004).

Acerca de cada uma das quatro categorias de objetivos, o COSO (2004) aponta como de cunho:

a) **estratégico** aqueles relacionados às metas gerais da organização, com o necessário alinhamento a tudo aquilo que permita executar sua missão;

**Figura 1 – Cubo do COSO II**



Fonte: TCU – Modelos de referências de gestão de riscos corporativos (adaptado do COSO, 2004)

- b) **operacional** os que visam alcançar eficácia e eficiência no emprego dos recursos da organização;
- c) de **comunicação** aqueles que dizem respeito à confiabilidade dos dados gerados na organização, a exemplo de relatórios e demais documentos que servem de base para a tomada de decisão; e
- d) de **conformidade** os que se preocupam com a observância de leis e demais normativos aplicáveis à esfera de atuação da organização.

Por sua vez, as linhas horizontais apontadas na dimensão esquerda do cubo apresentam os oito componentes para o gerenciamento de riscos proposto pelo modelo, que caracterizam, repise-se, como o caminho inter-relacionado a ser percorrido na busca pelo alcance dos objetivos da organização (COSO, 2004). Sobre tais componentes, aponta o COSO (2004) que:

- a) **Ambiente Interno** – refere-se ao comportamento e a cultura da organização, servindo de base para a sistematização do gerenciamento de riscos, sua forma de abordagem, seu apetite a riscos, integridade e valores éticos, além do ambiente no qual estão inseridos;
- b) **Fixação de Objetivos** – compreende a necessidade de o gerenciamento de riscos assegurar o estabelecimento de objetivos na organização, porquanto necessários à identificação dos eventos incidentes sobre a sua realização, objetivos estes que devem estar alinhados à missão da organização e ao seu apetite a risco;

- c) **Identificação de Eventos** – reflete a necessidade de identificação e classificação em riscos ou oportunidades dos eventos com potencial para impactar na realização dos objetivos da organização, com vistas, também, a direcionar as oportunidades identificadas para o estabelecimento de novas estratégias e objetivos;
- d) **Avaliação de Riscos** – compreende a análise dos riscos tendo por base a sua probabilidade e o impacto que pode causar na consecução dos objetivos, a fim de identificar a melhor forma de gerenciá-lo, levando em consideração a sua condição de risco inerente ou residual;
- e) **Resposta a Risco** – consiste na forma de ação eleita pela administração após identificado e avaliado o risco, que pode ser no sentido de evitar, aceitar, reduzir ou compartilhar o risco<sup>4</sup>, com vistas ao alinhamento dos riscos à tolerância e ao apetite a risco definidos pela organização;
- f) **Atividades de Controle** – diz respeito às práticas e procedimentos de controle definidos e implementados pela organização no intuito de se certificar que as formas de resposta aos riscos escolhidas estão sendo aplicadas de forma adequada e eficaz;
- g) **Informações e Comunicações** – componente que pressupõe sejam devidamente identificadas, colhidas e comunicadas as informações tidas por relevantes para o ambiente do gerenciamento de riscos, na forma e prazo que assegurem a sua utilidade, de modo que a comunicação ocorra de forma fluída e eficaz em todos os níveis da organização; e
- h) **Monitoramento**: implica no desenvolvimento de atividades contínuas, realizadas pela administração ou avaliadores independentes, cujo objetivo é acompanhar a integridade do gerenciamento de riscos implementado na organização, procedendo-se com as modificações que se apresentarem necessárias.

Por fim, a dimensão lateral direita (terceira dimensão) busca evidenciar a premissa de que o gerenciamento de riscos “é relevante a toda a organização ou a

---

<sup>4</sup> Conforme o COSO II (2004), **evitar o risco** passa por cessar as atividades nas quais incidiu o evento, o que pode implicar, por exemplo, na descontinuidade de um determinado projeto ou venda de um ativo a fim de fazer desaparecer o risco. **Reduzir o risco**, por outro lado, implica na adoção de medidas que visam à redução da probabilidade de sua ocorrência, do impacto provocado pelo evento ou de ambos. **Compartilhar riscos**, por sua vez, diz respeito a reduzir o risco transferindo-o para ou compartilhando com terceiros uma parte de tal evento, por meio de terceirização da atividade ou contratação de seguro, dentre outras formas. **Aceitar o risco**, por fim, implica em não adotar qualquer medida que vise mitigar a probabilidade ou o nível de impacto do risco.

qualquer uma de suas unidades” (COSO, 2004, p. 24), e representa a estrutura organizacional em seus diferentes níveis, ou seja, “os diversos níveis e/ou funções da organização, incluindo projetos, processos e demais atividades que concorrem para a realização dos seus objetivos” (TCU, 2018), o que, dada a diversidade de constituição das organizações, pode justificar o menor detalhamento apresentado pela publicação para essa face do cubo.

Quanto ao grau de eficácia do modelo, o COSO (2004) alerta que vai depender da existência e do adequado funcionamento de todos os oito componentes da dimensão esquerda - pois constituem critérios para mensuração da eficácia -, o que implica que a organização não deve estar acometida de fraquezas significantes, bem como que os riscos estejam devidamente enquadrados no apetite a risco por ela definido. Esclarece, no entanto, que os oito componentes não encontram igual aderência em todos os tipos de organização, pois a sua aplicabilidade conjunta se revela menos viável em organizações de médio e pequeno portes, embora possam elas igualmente se valerem de um gerenciamento de riscos eficaz, desde que assegurem o adequado funcionamento de cada um dos componentes aplicáveis à sua realidade.

O modelo ressalta ainda que a eficácia do gerenciamento de riscos pode ser mensurada pelo grau de conhecimento/entendimento que a administração detém sobre cada uma das categorias de objetivos, que lhe permite compreender razoavelmente os motivos pelos quais os **objetivos estratégicos e operacionais** estão ou não sendo alcançados, se o seu sistema de **comunicação** é merecedor de confiança, e se todas as normativas incidentes sobre a organização estão sendo devidamente respeitadas (**conformidade**) (COSO, 2004).

No que pertine às limitações, aduz o COSO (2004, p. 8) que decorrem, sobretudo, da falibilidade do julgamento humano no processo decisório; da necessidade de estabelecimento de uma relação custo x benefício quando da implantação dos controles; de “falhas causadas por erro ou engano humano”, pois “os controles podem ser anulados por conluio entre duas ou mais pessoas”; e da faculdade que detem a administração de aderir ou não às deliberações emanadas do gerenciamento de riscos, de forma que tais circunstâncias atuam para impedir “que o conselho de administração e a diretoria executiva tenham absoluta garantia da realização dos objetivos da organização.”

Durante mais de uma década, o modelo originário trazido pelo COSO ERM 2004 serviu de base para o gerenciamento de riscos em organizações presentes no cenário internacional, resultando atualizado em 2017 para contemplar a estratégia e o desempenho organizacional no gerenciamento de riscos, recebendo a nova versão o título de Gerenciamento de Riscos Corporativos – Integrado com Estratégia e Performance (*Enterprise Risk Management – Integrating with Strategy and Performance*) que, resultante das mudanças na complexidade dos riscos e da necessidade de evolução e aperfeiçoamento das abordagens em seu gerenciamento, destaca a importância de se gerenciar riscos desde o instante de definição das estratégias até as ações que miram a melhoria do desempenho da organização (COSO, 2017; TCU, 2018), assim representando um alargamento na estrutura de gestão de riscos proposta pelo modelo, que surge representado na Figura 2.

**Figura 2 – Aplicação do COSO ERM 2017**



Fonte: TCU – Modelos de referências de gestão de riscos corporativos (adaptado do COSO, 2017)

O modelo também batizado pelo COSO de *Framework* enfatiza o quanto importante para o planejamento estratégico e demais atividades da organização é o gerenciamento de riscos, dada a influência que o risco exerce sobre a estratégia e o desempenho em todos os níveis e funções da estrutura organizacional (COSO, 2017), conforme ilustra a Figura 3.

**Figura 3 – Componentes do COSO 2017**



Fonte: *Enterprise Risk Management – Integrating with Strategy and Performance* (COSO, 2017)

Ainda, o modelo reduz de 08 (oito) para 05 (cinco) o número de componentes da estrutura, se comparado com o COSO II, sendo representado por um conjunto de 20 (vinte) princípios distribuídos nos cinco componentes inter-relacionados, sendo eles: 1. Governança e cultura; 2. Estratégia e definição de objetivos; 3. Performance; 4. Análise e revisão; e 5. Informação, comunicação e divulgação (COSO, 2017), conforme demonstrado no Quadro 2.

<b>Quadro 2 – Componentes e Princípios da estrutura COSO ERM 2017 (continua)</b>	
<b>COMPONENTES</b>	
<b>1.</b>	<b>Governance and Culture (Governança e cultura):</b> a governança dá o tom da organização, reforçando a importância e instituindo responsabilidades de supervisão sobre o gerenciamento de riscos corporativos. A cultura diz respeito a valores éticos, a comportamentos esperados e ao entendimento do risco em toda a entidade.
<b>PRINCÍPIOS</b>	<p><b>1. Exerce supervisão do risco por intermédio do conselho</b> - O conselho de administração supervisiona a estratégia e cumpre responsabilidades de governança para ajudar a administração a atingir a estratégia e os objetivos de negócios.</p> <p><b>2. Estabelece estruturas operacionais</b> - A organização estabelece estruturas operacionais para atingir a estratégia e os objetivos de negócios.</p> <p><b>3. Define a cultura desejada</b> - A organização define os comportamentos esperados que caracterizam a cultura desejada pela entidade.</p> <p><b>4. Demonstra compromisso com os valores fundamentais</b> - A organização demonstra compromisso com os valores fundamentais da entidade.</p> <p><b>5. Atrai, desenvolve e retém pessoas capazes</b> - A organização tem o compromisso de formar capital humano de acordo com a estratégia e os objetivos de negócios.</p>



<b>Quadro 2 – Componentes e Princípios da estrutura COSO ERM 2017 (conclusão)</b>	
<b>COMPONENTES</b>	
<b>2.</b>	<b>Strategy and Objective-Setting (Estratégia e definição de objetivos):</b> gerenciamento de riscos corporativos, estratégia e definição de objetivos atuam juntos no processo de planejamento estratégico. O apetite a risco é estabelecido e alinhado com a estratégia; os objetivos de negócios colocam a estratégia em prática e, ao mesmo tempo, servem como base para identificar, avaliar e responder aos riscos.
<b>PRINCÍPIOS</b>	<p><b>6. Analisa o contexto de negócios</b> - A organização leva em conta os possíveis efeitos do contexto de negócios sobre o perfil de riscos.</p> <p><b>7. Define o apetite a risco</b> - A organização define o apetite a risco no contexto da criação, da preservação e da realização de valor.</p> <p><b>8. Avalia estratégias alternativas</b> - A organização avalia estratégias alternativas e seu possível impacto no perfil de riscos.</p> <p><b>9. Formula objetivos de negócios</b> - A organização considera o risco enquanto estabelece os objetivos de negócios nos diversos níveis, que se alinham e suportam a estratégia.</p>
<b>3.</b>	<b>Performance:</b> os riscos que podem impactar a realização da estratégia e dos objetivos de negócios precisam ser identificados e avaliados. Os riscos são priorizados com base no grau de severidade, no contexto do apetite a risco. A organização determina as respostas aos riscos e, por fim, alcança uma visão consolidada do portfólio e do montante total dos riscos assumidos. Os resultados desse processo são comunicados aos principais <i>stakeholders</i> envolvidos com a supervisão dos riscos.
<b>PRINCÍPIOS</b>	<p><b>10. Identifica o risco</b> - A organização identifica os riscos que impactam a execução da estratégia e os objetivos de negócios.</p> <p><b>11. Avalia a severidade do risco</b> - A organização avalia a severidade do risco.</p> <p><b>12. Prioriza os riscos</b> - A organização prioriza os riscos como base para a seleção das respostas a eles.</p> <p><b>13. Implementa respostas aos riscos</b> - A organização identifica e seleciona respostas aos riscos.</p> <p><b>14. Adota uma visão de portfólio</b> - A organização adota e avalia uma visão consolidada do portfólio de riscos.</p>
<b>4.</b>	<b>Review and Revision (Análise e revisão):</b> ao analisar sua performance, a organização tem a oportunidade de refletir sobre até que ponto os componentes do gerenciamento de riscos corporativos estão funcionando bem ao longo do tempo e no contexto de mudanças relevantes, e quais correções são necessárias.
<b>PRINCÍPIOS</b>	<p><b>15. Avalia mudanças importantes</b> - A organização identifica e avalia mudanças capazes de afetar de forma relevante a estratégia e os objetivos de negócios.</p> <p><b>16. Analisa riscos e performance</b> - A organização analisa a performance da entidade e considera o risco como parte desse processo.</p> <p><b>17. Busca o aprimoramento no gerenciamento de riscos corporativos</b> - A organização busca o aprimoramento contínuo do gerenciamento de riscos corporativos.</p>
<b>5.</b>	<b>Information, Communication, and Reporting (Informação, comunicação e divulgação):</b> o gerenciamento de riscos corporativos demanda um processo contínuo de obtenção e compartilhamento de informações precisas, provenientes de fontes internas e externas, originadas das mais diversas camadas e processos de negócios da organização.
<b>PRINCÍPIOS</b>	<p><b>18. Alavanca sistemas de informação</b> - A organização maximiza a utilização dos sistemas de informação e tecnologias existentes na entidade para impulsionar o gerenciamento de riscos corporativos.</p> <p><b>19. Comunica informações sobre riscos</b> - A organização utiliza canais de comunicação para suportar o gerenciamento de riscos corporativos.</p> <p><b>20. Divulga informações de riscos, cultura e performance</b> - A organização elabora e divulga informações sobre riscos, cultura e performance abrangendo todos os níveis e a entidade como um todo.</p>

Fonte: Elaborado a partir do COSO (2017).

Por fim, em novembro de 2020, o COSO lançou o guia Gerenciamento de Riscos de Conformidade: Aplicando a estrutura COSO ERM (*Compliance Risk Management: Applying The COSO ERM Framework*), cujo objetivo é “fornecer orientações sobre a aplicação da estrutura COSO ERM para a identificação, avaliação e gestão de riscos de conformidade, alinhando-a com estrutura do Programa C&E” (Ética corporativa e Conformidade), assim criando uma robusta ferramenta de gestão que integra as abordagens e definições conceituais de cada uma das mencionadas estruturas, inclusive do COSO 2013 (Controle Interno - Estrutura Integrada) e o COSO 2017 (COSO, 2020, p. 1).

O modelo embrenha por cada um dos 20 (vinte) princípios distribuídos nos cinco componentes trazidos pelo COSO ERM 2017 e representados no Quadro 2, objetivando mapear seus requisitos específicos e emergentes, e fornecer elementos necessários a um programa de C&E eficaz para cada um dos princípios. No mais, ressalta a importância da definição estruturada de responsabilidades quanto aos riscos de conformidade e o compromisso com a ética profissional na organização.

Por fim, o modelo traz como público alvo, dentre outros, os profissionais atuantes na gestão de riscos, a exemplo de auditores internos, gerentes de riscos e responsáveis pela gestão de riscos de conformidade; profissionais de *compliance* e que visem alinhar seu programa de C&E ou integrá-lo com um programa de gestão de riscos para toda a organização; membros de equipe de gestão sênior, para melhor compreensão do risco de conformidade e do programa de C&E; e membros da alta administração, visando auxiliá-la em seu papel de supervisão.

### **2.7.2 O modelo ISO 31000 – Gestão de Riscos – Princípios e Diretrizes (2018)**

Conforme a ABNT (2018), a Norma ABNT ISO 31000:2018 e o modelo de gerenciamento de riscos nela proposto foi elaborado pelo *Technical Committee Risk Management* (ISO/TC 262) com o fito de cancelar e substituir a edição anterior (ABNT NBR ISO 31000:2009), esta que, conforme Leal (2019), desde a sua criação apresentou às organizações um abrangente padrão de gerenciamento de riscos, que envolve processos de fácil aplicação em toda e qualquer tipo de organização, inclusive àquelas de natureza pública.

O modelo em questão está estruturado em três círculos que se inter-relacionam, que compreendem os princípios, a estrutura e o processo de gerenciamento de riscos propriamente dito, e é representado pela Figura 4.

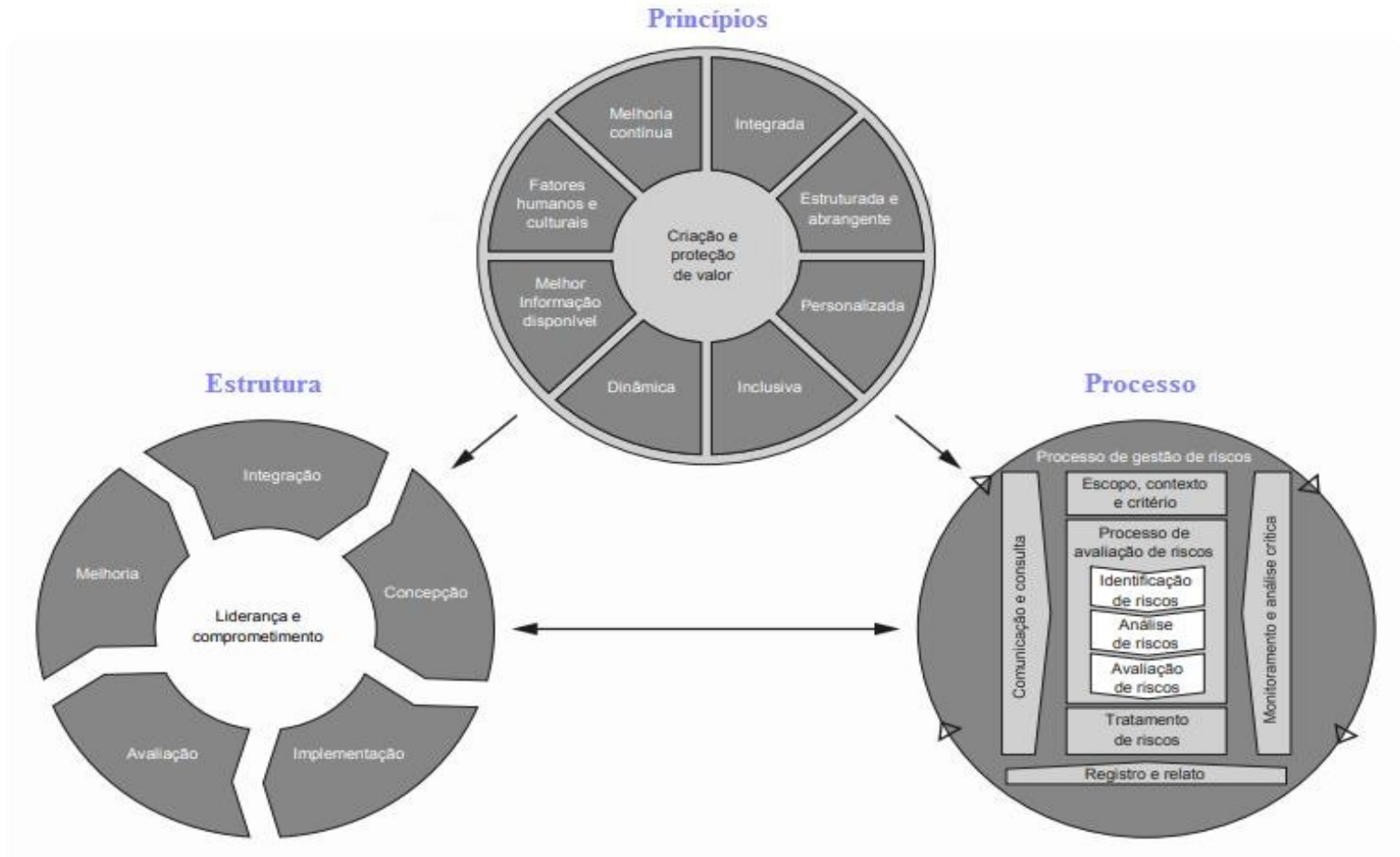
Consoante se vê, os **princípios** ocupam o círculo central e orbitam o propósito do gerenciamento de riscos que, segundo o modelo, é a criação e proteção do valor, por meio da melhoria do desempenho, do incentivo à inovação e do apoio ao alcance dos objetivos. Tais princípios apontam para as características de um gerenciamento de riscos eficaz e eficiente, por meio da comunicação do seu valor e da elucidação da sua intenção e propósito (ABNT, 2018).

Assim, os princípios constituem o norte a ser mirado quando do estabelecimento da estrutura e dos processos de gerenciamento de riscos, de forma a possibilitar que a organização possa gerenciar os impactos das incertezas para a consecução dos seus objetivos (ABNT, 2018).

Por tais razões, conforme a ISO 31000 (2018, p. 3-4), uma gestão de riscos eficaz só pode ser alcançada se desenvolvida de forma e/ou com base em:

- a) **Integrada**, pois a gestão de riscos deve ser compreendida como parte integrante de todas as atividades organizacionais;
- b) **Estruturada e abrangente**, com vistas a contribuir para resultados consistentes e comparáveis;
- c) **Personalizada**, uma vez que a estrutura e o processo de gestão de riscos devem se apresentar moldados ao perfil da organização e proporcionais aos seus contextos externo e interno relacionados aos seus objetivos;
- d) **Inclusiva**, pois o necessário, adequado e oportuno envolvimento das partes interessadas possibilita que seus conhecimentos, pontos de vista e percepções sejam considerados, o que resulta em melhor conscientização e gestão de riscos fundamentada;
- e) **Dinâmica**, de forma a considerar uma oscilação no cenário dos riscos, onde alguns podem surgir, mudar ou desaparecer à medida que os contextos externo e interno de uma organização mudem, cabendo à gestão de riscos se antecipar, detectar, reconhecer e responder a tais movimentos de uma forma apropriada e oportuna;

Figura 4 – Estruturação do modelo ABNT ISO 31000:2018



Fonte: ABNT ISO 31000:2018 (Adaptado).

f) **Melhor informação disponível**, porquanto as entradas para a gestão de riscos têm por base informações históricas e atuais, além de expectativas futuras, o que exige que tais informações sejam oportunas, claras e disponíveis para as partes interessadas a elas relacionadas, levando-se em conta toda e qualquer limitação e incertezas a elas associadas.

g) **Fatores humanos e culturais**, tendo em vista que o comportamento humano e a cultura constituem fatores capazes de influenciar de forma significativa em todos os aspectos da gestão de riscos em cada nível e estágio da estrutura.

h) **Melhoria contínua**, que pressupõe o continuado aprimoramento da gestão de riscos por meio do aprendizado e das experiências.

A **estrutura**, por sua vez, circundando o elemento Liderança e comprometimento – que pressupõe a capacidade da Alta Direção e dos órgãos de supervisão de assegurarem a integração da gestão de riscos em todos os níveis e atividades da administração, conferindo, para tanto, o necessário suporte em todos os aspectos inerentes ao gerenciamento de riscos – engloba os componentes Integração, Concepção, Implementação, Avaliação e Melhoria da gestão de riscos que, conforme o modelo, devem ser personalizados de forma a atender as necessidades e peculiaridades de cada organização (ABNT, 2018).

Acerca dos componentes da **estrutura**, tem-se que:

a) **Integração** – Consiste em um processo dinâmico e iterativo, visando assegurar que o risco seja gerenciado em todos os níveis da estrutura organizacional, e que todo o seu pessoal conscientize-se do seu papel e responsabilidade na gestão de riscos, de modo que esteja ela integrada ao propósito da organização, à governança, à liderança e ao comprometimento, à estratégia, aos objetivos e às operações.

b) **Concepção** – O componente pressupõe que a organização: compreenda os seus contextos externo e interno; articule o comprometimento contínuo da Alta Direção com a gestão de riscos, fazendo-o chegar, da forma apropriada, ao conhecimento de toda a organização e das partes interessadas; atribua, por meio da Alta Direção e os órgãos de supervisão, autoridades, responsabilidades e responsabilizações para os papéis pertinentes à gestão de riscos, deles dando pleno conhecimento a todos os níveis da organização; assegure, por meio da Alta Direção e os órgãos de supervisão, a alocação dos recursos necessários à gestão de riscos, observadas as

capacidades e restrições de recursos disponíveis; estabeleça uma abordagem aprovada para comunicação e consulta para apoiar a estrutura e facilitar a aplicação eficaz da gestão de riscos; estabeleça uma forma de comunicação e consulta capaz de apoiar a estrutura e facilitar a aplicação eficaz da gestão de riscos, envolvendo o compartilhamento de informações com o público-alvo (comunicação), e o retorno dos participantes como subsídio para tomada de decisão e como aprendizado.

c) **Implementação** – Parte do princípio de que, para que se mostre eficaz, a gestão de riscos deve ser implementada atendendo a um plano apropriado e que inclua prazos e recursos, com a precisa identificação dos diferentes tipos de decisões tomadas na organização e da posição dos respectivos decisores, modificando o processo de tomada de decisão, quando se fizer necessário; e assegurando que o delineamento da gestão de riscos foi plenamente compreendido e será praticado.

d) **Avaliação** – Diz respeito à necessidade de a organização mensurar periodicamente o desempenho da gestão de riscos implementada quanto ao seu propósito, planos de implementação, indicadores e comportamento esperado, como o fito de determinar se a estrutura permanece ou não adequada para os fins que se destina.

e) **Melhoria** – Implica na necessidade da organização, considerando alterações no cenário interno e externo, monitorar e adaptar continuamente a estrutura da gestão de riscos implementada (adaptação), bem como, visando ao aprimoramento dessa mesma gestão de riscos, melhorar continuamente sua adequação, suficiência e eficácia, e o formato de sua integração.

Assim, vislumbra-se que a **estrutura** tem por objetivo apoiar a integração da gestão de riscos com suas atividades e funções essenciais, posto que uma sistematização eficaz pressupõe a sua integração na governança e em todas atividades e níveis da organização, inclusive no que se refere à tomada de decisão, o que exige o apoio das partes interessadas, sobretudo da alta administração que, conforme o modelo, tem a responsabilidade de gerenciar riscos, ao passo que os órgãos de supervisão são responsabilizados por supervisionar a gestão de riscos (ABNT, 2018).

O **processo de gestão de riscos**, por fim, estruturado no círculo direito da representação, compreende “a aplicação sistemática de políticas, procedimentos e práticas para as atividades de comunicação e consulta, estabelecimento do contexto

e avaliação, tratamento, monitoramento, análise crítica, registro e relato de riscos”, constituindo-se num processo iterativo, embora apresentado como sequencial (ABNT, 2018, p. 9-10), e comporta os seguintes componentes:

a) **Comunicação e consulta**, que tem como objetivo auxiliar as partes interessadas na compreensão dos riscos, cabendo à comunicação empreender esforços a fim de que haja por parte dos envolvidos no processo a conscientização e o necessário entendimento acerca dos eventos incertos, ao passo que a consulta visa colher informações que possam auxiliar na tomada de decisão.

b) **Escopo, contexto e critérios**, cujo estabelecimento tem como propósito personalizar o processo de gestão de riscos, tomando-se por base o contexto interno e externo, de modo a alinhá-lo à realidade da organização, inclusive quanto aos critérios de assunção de risco, assim permitindo um processo de avaliação de riscos eficaz e um tratamento de riscos apropriado.

c) **Processo de avaliação de riscos**, que compreende os subprocessos de identificação de riscos, análise de riscos e avaliação de riscos, o qual deve ser conduzido de forma sistemática, iterativa e colaborativa, levando-se em conta o conhecimento e as perspectivas das partes interessadas, com o emprego da melhor informação disponível e complementada por investigação adicional, quando necessário.

d) **Tratamento de riscos**, que tem como propósito escolher e pôr em prática as opções para enfrentamento dos riscos, o que envolve um processo igualmente iterativo de “formular e selecionar opções para tratamento do risco; planejar e implementar o tratamento do risco; avaliar a eficácia deste tratamento; decidir se o risco remanescente é aceitável; se não for aceitável, realizar tratamento adicional” (ABNT. 2018, p. 14).

As opções para tratamento de riscos, por sua vez, compreendem evitar o risco atalhando ou excluindo a atividade que o ensejou; assumir ou aumentar o risco diante da perspectiva de uma oportunidade; “remover a fonte de risco; mudar a probabilidade; mudar as consequências; compartilhar o risco (por exemplo, por meio de contratos, compra de seguros); reter o risco por decisão fundamentada” (ABNT. 2018, p. 14).

e) **Monitoramento e análise crítica**, que deve ser compreendido como uma atividade planejada do processo de gestão de riscos, inclusive mediante o

estabelecimento de responsabilidades, e cujo desiderato é assegurar e aprimorar a qualidade e eficácia da concepção, implementação e resultados do processo, por meio de uma análise crítica periódica dos procedimentos e de seus resultados, com vistas a refletirem em todas as atividades de gestão de desempenho, medição e relatos da organização.

f) **Registro e relato**, que compreende a necessidade de que o processo de gestão de riscos e os resultados dele provenientes sejam devidamente consignados por meios de mecanismos desenvolvidos para tal finalidade, visando tornar-se de conhecimento de toda a organização; subsidiar com informações na tomada de decisão; contribuir para a melhoria das próprias atividades de gestão de riscos; e subsidiar a interação com as partes interessadas.

Conforme se vislumbra, o modelo aqui concisamente apresentado, na mesma linha dos demais instrumentos, permite que a organização pública, sem descuidar dos princípios, da estrutura e dos processos apontados, possa desenvolver e implementar uma gestão de riscos estruturada, e, sobretudo, de maneira que se apresente viável e alinhada à sua realidade da organizacional.

### **2.7.3 O modelo *Orange Book* e *Risk Management Assessment Framework***

Ancorado no guia *The Orange Book - Management of Risk - Principles and Concepts* (O livro laranja – Gestão de Riscos – Conceitos e Princípios), desenvolvido e publicado no Reino Unido no ano de 2004, o modelo em questão figura como referência principal para o programa de gerenciamento de riscos do governo do reino Unido, apresentando como vantagens a compatibilidade com a padronização internacional para o segmento, bem como a forma acessível, embora abrangente, com a qual trata o tema (TCU, 2018).

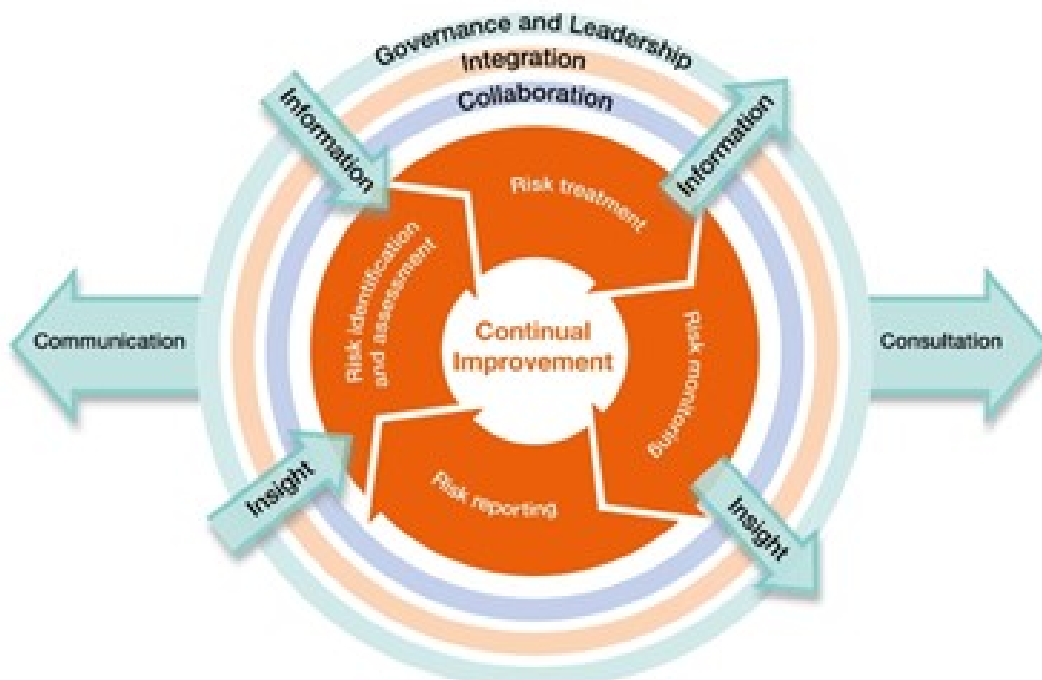
Conforme o TCU (2018), em 2009, como desdobramento do referido modelo, o governo do Reino Unido publicou o guia *Risk Management Assessment Framework: a Tool for Departments*, consistente em ferramenta estruturada em sete componentes: Liderança para Risco; Pessoas; Políticas e Estratégias para Risco; Parcerias; Processos de Gestão de Riscos; Eficácia da Gestão de Riscos; e Resultados, e que tem como objetivo a aferição dos níveis de gerenciamento de riscos das instituições públicas daquele país.



Ainda conforme o TCU (2018), a ferramenta supramencionada, em razão da peculiaridade de ter sido desenvolvida com destinação específica para a aferição do gerenciamento de riscos em organizações públicas, bem como por contemplar o componente “Parcerias”, relevante para a Administração Pública na atualidade, integra a base conceitual do modelo proposto pelo órgão com vistas a avaliar o nível de maturidade em gerenciamento de riscos nas instituições públicas brasileiras.

Em 2020, uma nova versão do modelo foi lançada pelo governo britânico visando atualizar a versão publicada em 2004 e, a exemplo daquela, estabelecer conceitos e princípios básicos necessários a um gerenciamento de riscos eficaz em todos os órgãos públicos daquele país. Conforme a publicação, a estrutura de gerenciamento de riscos encartada no modelo oferece suporte à identificação consistente e robusta de ameaças e oportunidades, dentro dos níveis de aceitação desejados em uma organização, de modo a apoiar a transparência, a inovação e a excelência na busca pelo alcance dos objetivos (ORANGE BOOK, 2020), conforme estrutura representada pela Figura 5.

**Figura 5** – Estrutura de Gerenciamento de Riscos - Orange Book 2020



Fonte: *The Orange Book - Management of Risk - Principles and Concepts* (UK, 2020)

Preceitua o modelo que não há como uma estrutura de gerenciamento de riscos ser considerada eficaz caso deixe de aplicar os seguintes princípios (ORANGE BOOK, 2020):

a) ***Governance and Leadership (Governança e liderança)*** – O gerenciamento de riscos deve ser uma parte essencial da governança e liderança, e estas vistas como fundamental para a maneira como a organização é dirigida, gerenciada e controlada em todos os níveis;

b) ***Integration (Integração)*** – O gerenciamento de riscos deve ocorrer de forma integrada entre todos os níveis organizacionais, funcionando como um suporte para a tomada de decisão visando à realização dos objetivos da organização;

c) ***Collaboration and Best Information (Colaboração e melhor informação)*** – A gestão de riscos deve ser colaborativa e alimentada pelas melhores informações e técnicas disponíveis;

d) ***Risk Management Processes (Processos de gerenciamento de riscos)*** – Os processos de gerenciamento de riscos devem ser estruturados de forma a contemplar: 1. Uma identificação e avaliação de risco capaz de determinar e priorizar como os riscos devem ser gerenciados; 2. Seleção, design e implementação de opções de tratamento de risco que permitam a mitigação dos riscos e a sua redução a níveis aceitáveis, a fim de proporcionar o necessário apoio à realização dos resultados pretendidos pela organização; 3. O delineamento de procedimentos de integração capazes de promover um contínuo monitoramento de risco perspicaz e informativo; e 4. Relatórios de risco oportunos, precisos e úteis para melhorar a qualidade da tomada de decisão e para apoiar a gestão e supervisão de todos os níveis envolvidos no cumprimento de suas responsabilidades.

e) ***Continual Improvement (Aprimoramento contínuo)*** – O gerenciamento de riscos deve ser continuamente aprimorado por meio de aprendizado e experiência.

Consoante visto, a exemplo das demais estruturas apresentadas no presente estudo, o modelo em questão ressalta que o gerenciamento de riscos deve integrar todos os níveis da organização - não sendo, pois, algo isolado -, tendo como objetivo precípuo a identificação, avaliação, resposta e monitoramento aos riscos capazes de impactar na consecução dos seus objetivos.

### 2.7.4 Roteiro e técnicas para gestão de riscos apresentados pelo TCU

No já mencionado Referencial Básico de Gestão de Riscos, o TCU (2018, p. 9) traça um roteiro capaz de guiar a organização pública para a implementação de uma gestão de riscos estruturada, o que faz por meio de um conjunto de onze questionamentos concatenados que, na sua essência, representam uma possível forma de gerenciar riscos, sendo eles:

1. Que empreendimento você deseja proteger ou ver bem-sucedido? Pode ser um projeto, um processo, um departamento, uma organização, uma política.
2. Quais são os objetivos desse empreendimento?
3. Que fatores (fraquezas, ameaças, erros, falhas...) podem afetar o alcance desses objetivos?
4. Que riscos podem se originar da ocorrência desses fatores?
5. Qual seria a probabilidade e o impacto da ocorrência de cada um desses riscos se nada tivesse sido feito para mitigá-los até o momento? Calcule o nível de risco inerente (probabilidade inicial x impacto inicial).
6. Qual é o seu apetite e a sua tolerância a risco? Qual nível de risco você considera aceitável?
7. Quais medidas mitigadoras já foram adotadas e que controles internos já estão implantados? Qual a eficácia dessas medidas e controles? Algum deles pode ser eliminado?
8. Que outras medidas mitigadoras e controles internos podem ser adotados para adequar o nível de risco ao apetite e à tolerância a risco?
9. Qual é a probabilidade e o impacto esperado da ocorrência desses riscos após a avaliação de eficácia e adequação das medidas mitigadoras e controles internos? Calcule o nível de risco residual (nível de risco inerente x risco de controle).
10. Com que frequência esses riscos devem ser monitorados?
11. Quem são os responsáveis por monitorar os riscos? Quem deve ser comunicado acerca desses? Com que frequência isso deve ser feito e por quais mecanismos?

Elenca, ainda, um conjunto de passos/procedimentos que a organização pública pode empreender no afã de implementar a gestão de riscos no seu âmbito, com base em experiências de outras instituições que:

- a) montaram um grupo de trabalho;
- b) realizaram estudos preliminares;
- c) definiram a estratégia de implantação e a arquitetura de gestão de riscos;
- d) definiram a política de gestão de riscos;
- e) definiram a responsabilidade das partes interessadas;
- f) definiram o processo de gestão de riscos;
- g) implementaram a gestão de riscos, por meio da implantação em unidades, processos e projetos piloto e, posteriormente, adaptação e disseminação para outros objetos e contextos;
- h) monitoram e revisam. (TCU, 2018, p. 63).

De igual forma, a publicação apresenta uma série de técnicas aplicadas ao gerenciamento de riscos, dentre as quais:

a) **Matriz de riscos** (ou matriz de probabilidade / consequência):

Conforme visto nos modelos estudados, a gestão de riscos passa por identificar tais eventos e pela definição de como proceder diante de cada um deles. Nesse contexto, os riscos identificados são organizados em classes, faixas ou categorias, a fim de que lhe sejam atribuídos níveis de acordo com as diretrizes traçadas pela política de gerenciamento de riscos, levando-se em consideração os limites de exposição e assunção de riscos definidos pela organização (TCU, 2018).

Observadas tais premissas, os riscos podem ser classificados em escalas de pontuação que, de acordo com o definido pela organização, possam indicar quando o risco, por exemplo, deve ser considerado baixo, médio, alto ou extremo, tanto quanto à probabilidade que venha a ocorrer, quanto em relação aos impactos que podem gerar na consecução dos objetivos (TCU, 2018), conforme exemplificado na Figura 6.

**Figura 6** – Exemplo de escala de classificação de riscos

RB (Risco Baixo)	RM (Risco Médio)	RA (Risco Alto)	RE (Risco Extremo)
0 – 9,99	10 – 39,99	40 – 79,99	80 – 100

Fonte: TCU (2018).

Assim, a matriz de riscos constitui técnica capaz de representar de maneira organizada os resultados de combinações entre a probabilidade e o impacto de determinados riscos (probabilidade x impacto), como representado na Figura 7.

**Figura 7** – Modelo de matriz de riscos

<b>IMPACTO</b>	Muito Alto A 10	10 RM	20 RM	50 RA	80 RE	100 RE
	Alto B 8	8 RB	16 RM	40 RA	64 RA	80 RE
	Médio 5	5 RB	10 RM	25 RM	40 RA	50 RA
	Baixo 2	2 RB	4 RB	10 RM	16 RM	20 RM
	Muito Baixo 1	1 RB	2 RB	5 RB	8 RB	10 RM
		Muito Baixa 1	Baixa 2	Média 5	Alta 8	Muito Alta 10
<b>PROBABILIDADE</b>						

Fonte: TCU (2018)

**b) Priorização de processos:**

A técnica parte do princípio que, ainda que a gestão de riscos incida sobre todos os processos da organização, consoante visto nos modelos estudados, um maior esforço deve ser empreendido em relação aos processos que mais entregam ou devem entregar valor para as partes interessadas, bem como em relação às atividades com potencial para impactá-los, o que pode ser aferido por meio da organização dos processos tendo por base a Cadeia de valor, onde os macroprocessos finalísticos e de suporte e seus desdobramentos são graficamente representados no afã de demonstrar, de forma acessível, a proeminência de cada processo, bem como a interação entre eles (TCU, 2018).

A priorização de processos enquanto técnica se revela ainda mais indicada para nortear o direcionamento de recursos para o gerenciamento de riscos, assim como para casos nos quais a organização opta por implementar de forma gradual o seu processo de gestão de riscos, ocasião na qual prioriza os processos que primordialmente serão objetos de avaliação (TCU, 2018).

Acerca do mapeamento dos processos organizacionais, cuida o Referencial em exame de definir como a “representação gráfica da sequência de atividades que compõem um processo, fornecendo uma visão dos fluxos operacionais do trabalho, incluindo [...] a evidenciação dos agentes envolvidos, os prazos, o fluxo de documentos, o processo decisório”, dentre outros aspectos, de acordo com o nível de detalhamento que se pretenda alcançar (TCU, 2018, p. 151/152).

**c) *Brainstorming*:**

Também denominada tempestade de ideias, a técnica consiste na reunião de pessoas detentoras de conhecimento do contexto organizacional com vistas a estimular a livre exposição de argumentos dos quais seja possível extrair contribuições para o gerenciamento de riscos na organização, e encontra maior aplicação na identificação de riscos em novas atividades, novas tecnologias ou diante da indisponibilidade de dados sobre determinada atividade (TCU, 2018).

**d) *Entrevista*:**

Tem por base a formulação prévia de questionamentos, estruturados ou semiestruturados, que serão lançados ao entrevistado a fim de que sejam respondidos, sendo indicada para casos nos quais a reunião de pessoas para análise conjunta de determinada matéria se revela difícil ou onerosa, ou ainda

quando se pretende ouvir as opiniões individuais sem que estejam submetidas à influência ou interferência de terceiros (TCU, 2018).

e) **Delphi:**

Visa alcançar o consenso diante de opiniões de um grupo de especialistas por meio da aplicação de questionário semiestruturado a ser respondido de forma individual e anônima por cada especialista, cujas respostas são consolidadas e levadas ao conhecimento dos especialistas em sucessivas rodadas de questionários, de modo a assim possibilitar a mudança de opinião e ao final se alcançar o consenso.

f) **Análise Preliminar de Perigos (APP):**

Recomendada para situações nas quais existam poucas informações disponíveis sobre o que se pretende analisar, constitui técnica caracterizada pela reunião de pessoas detentoras de informações acerca do objeto da análise, visando, por meio de suas experiências e considerando todo o contexto nele envolvido (atividades, recursos, ambiente, interfaces entre os diversos elementos e os objetivos a alcançar), exarar uma lista de situações perigosas ou de riscos incidentes sobre aquele objeto de análise, e que podem servir de base para avaliações mais completas (TCU, 2018).

g) **Listas de Verificação:**

A técnica tem como base a utilização de documentos já produzidos em outras avaliações, a exemplo de experiências, boas práticas e lista de situações perigosas ou de riscos, dentre outros, e se dá por meio da análise da lista existente, fazendo-se “um batimento entre o que ela contém – eventos, fontes de risco, controles etc. – e a situação ou objeto que está sendo avaliado”, com o objetivo de se obter “listas de situações ou riscos inaceitáveis, de controles inadequados ou faltantes, entre outros produtos” (TCU, 2018, p. 44).

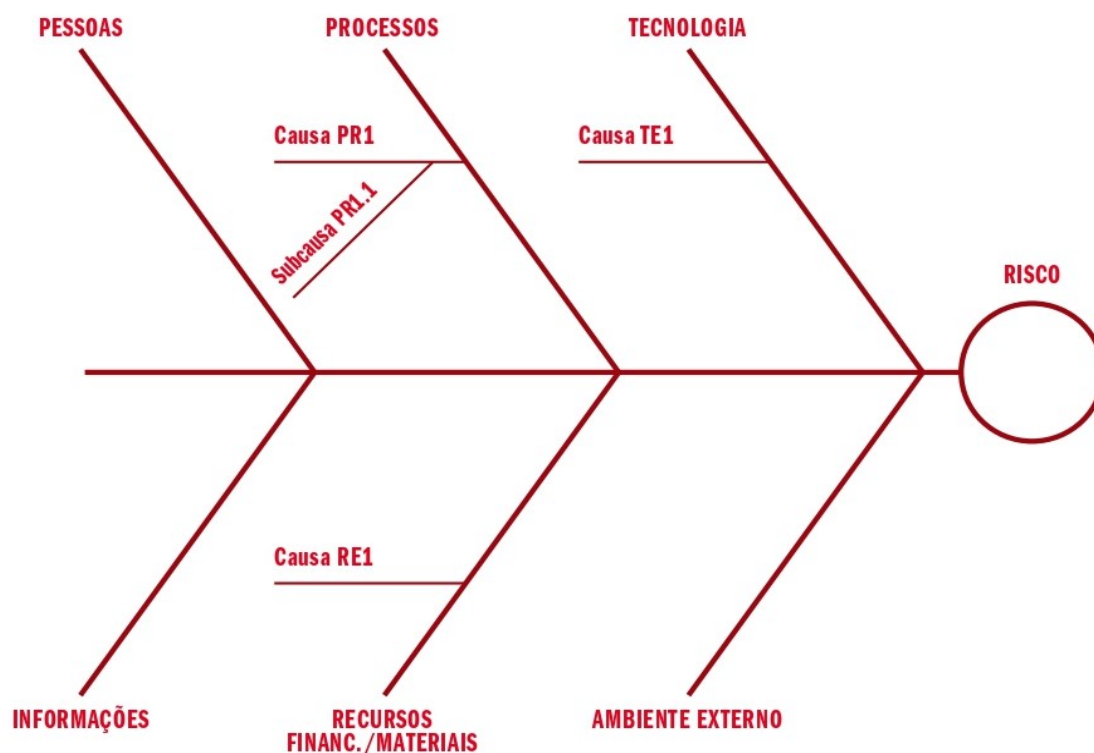
h) **Análise de Causa Raiz:**

Técnica que possibilita a identificação da raiz ou causas originais dos riscos - por ser mais relevante que a identificação apenas dos seus sinais mais claros e imediatos -, privilegia uma avaliação progressiva das causas dos riscos, partindo das mais evidentes para as subjacentes, analisando fatores humanos, tecnológicos, materiais e ambientais, dentre outros, de modo que pode ser utilizada tanto para

estimar a probabilidade de um risco quanto para direcionar ações que visem ao tratamento das suas principais causas (TCU, 2018).

Ainda sobre a aplicação da técnica, o TCU (2018, p. 45) ressalta que “mais do que buscar identificar grande quantidade de causas, é mais eficaz identificar e tratar o menor conjunto de causas que mais contribua para a materialização do risco (aplicação da regra 20-80, de Pareto)”, consignando que além da análise de Pareto, à técnica em questão podem ser aplicadas ainda as ferramentas “5 Porquês”, árvore de falhas e diagrama de espinha de peixe (Ishikawa), esta última demonstrada na Figura 8.

**Figura 8** – Exemplo de diagrama de espinha de peixe (Ishikawa)



Fonte: TCU (2018).

#### i) Técnica “E SE” estruturada (SWIFT)

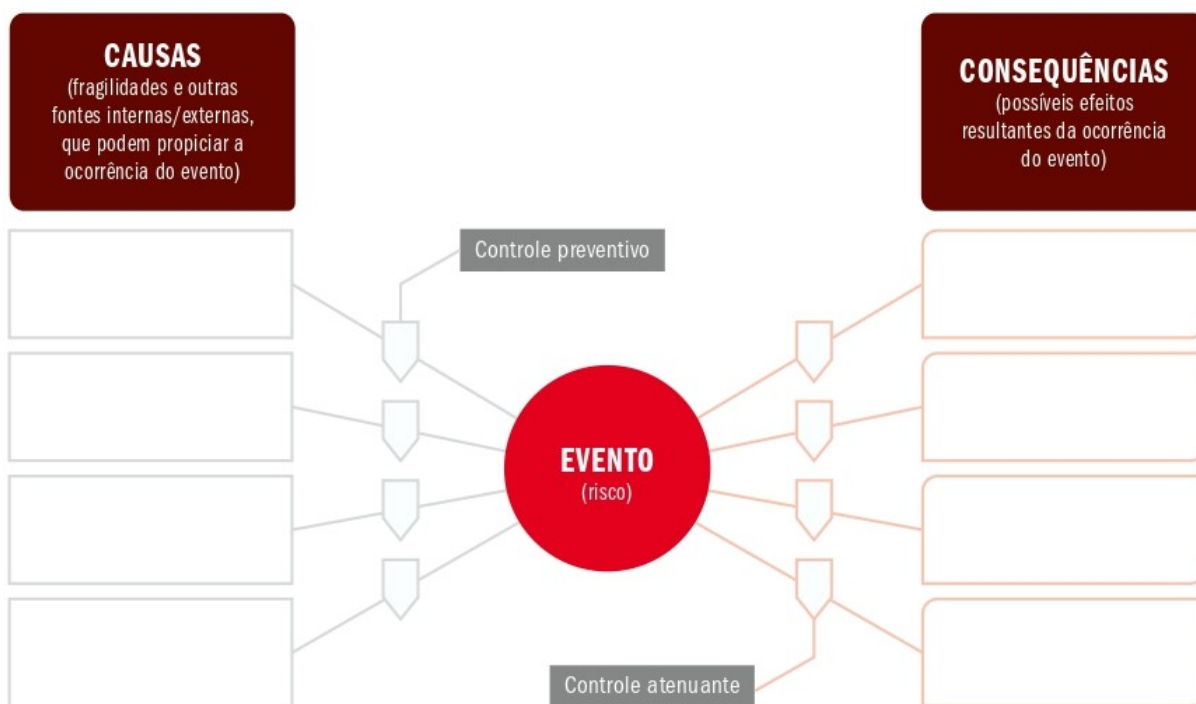
Constitui técnica que visa identificar riscos de desvios em determinado processo, sistema ou atividade, por meio da reunião de pessoas envolvidas com o objeto analisado ou que sobre ele detenham informações, sob a mediação de um facilitador, a quem incumbe instigar a participação dos presentes no grupo com questionamentos do tipo “e se”, “o que aconteceria se”, “alguém ou algo pode ...?”,

“alguém ou algo nunca...?”, de forma a estimulá-los a refletir acerca de diversas alternativas e cenários para o funcionamento do objeto da análise, com potencial para auxiliar, inclusive, na identificação de controles e na mensuração de sua eficácia. Sua aplicação pode resultar em “listas de possíveis eventos, fontes de riscos, consequências e controles, bem como de ações de tratamento prioritizadas”, e facilitar “a criação de um registro de riscos e de plano de tratamento, que podem ser obtidos com pequeno esforço adicional” (TCU, 2018, p. 46).

j) **Análise BOW TIE:**

Consiste em técnica que visa descrever, de forma simplificada, os caminhos de um evento de risco, partindo das causas até as consequências do risco, com o fito de que se possa definir e constituir barreiras entre as causas e o risco e entre este evento e suas consequências, utilizando-se, para tanto, de um diagrama em formato de gravata borboleta, no qual o nó da gravata representa o evento risco, do lado esquerdo suas causas e do lado direito suas consequências, de modo que entre as causas e o risco, e, de igual forma, entre o risco e as consequências, possam ter lugar as barreiras definidas, seja para prevenir o risco (no primeiro caso), seja para atenuar suas consequências (TCU, 2018), conforme se avista na Figura 9.

**Figura 9** – Esboço de diagrama “bow tie”



Fonte: TCU (2018).



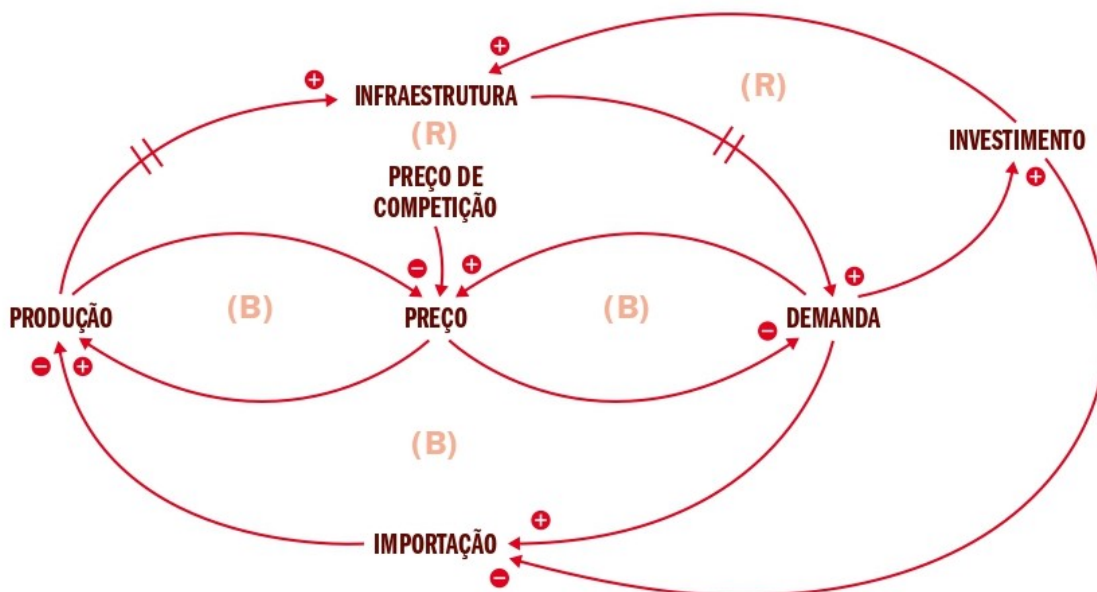
**l) Análise de Decisão por Multicritério (MCDA):**

A técnica visa subsidiar no processo de tomada de decisão por meio da identificação e classificação de alternativas “por ordem de valor ou prioridade, a partir da percepção de um grupo de pessoas”, o que passa pela identificação do conjunto de opções a serem avaliadas e a definição e classificação hierárquica de fatores e critérios de avaliação, tendo por base pesos atribuídos a cada um dos fatores e critérios avaliativos a partir de notas conferidas por avaliadores e consolidadas por algum método matemático de comparação, dentre eles o *Analytic Hierarchy Process (AHP)*, de modo a resultar numa classificação das alternativas baseada nas notas finais recebidas por cada uma delas. Tem como ponto forte a característica de abrir “a possibilidade de tomada de decisão mesmo quando as partes envolvidas possuem objetivos e critérios distintos”, de modo que na gestão de riscos, pode ser aplicada, dentre outras finalidades, para classificar riscos ou priorizar ações de tratamento (TCU, 2018, p. 47-48).

**m) Pensamento Sistêmico:**

Conforme o TCU (2018, p. 48), a técnica se refere “a um conjunto de conceitos, comportamentos e ferramentas que auxiliam na compreensão de estruturas interdependentes de sistemas complexos”, com o objetivo de apontar relações de causalidade entre fatores que se relacionam entre si, de modo a permitir análises holísticas e integradas de questões/problemas postos, “vislumbrar conjuntos dinâmicos de comportamento, identificar e compreender interconexões que conferem ao sistema características únicas”, bem como identificar comportamentos prováveis, por meio da utilização, dentre outras, de ferramentas como o diagrama de *loop* de causalidade (CLD), representado na Figura 10.

**Figura 10** – Exemplo de diagrama de *loop* de causalidade (CLD)



Fonte: TCU (2018)

Por fim, o referencial mencionado neste subitem registra que as técnicas apresentadas não são as únicas existentes, tampouco são excludentes entre si, sendo comum a utilização conjunta de duas ou mais técnicas, o que vai depender da etapa da gestão de riscos na qual estejam sendo aplicadas e do objeto a ser avaliado.

Assim, observa-se uma crescente preocupação de órgãos da Administração Pública na apresentação e/ou desenvolvimento de instrumentos capazes de auxiliar o setor público no seu dever de gerenciar riscos, sendo de uma dessas iniciativas que exsurge o Software ForRisco, que será objeto de concisa apresentação no tópico seguinte.

## 2.8 O SISTEMA FORRISCO E A SUA CAPACIDADE DE CONTRIBUIÇÃO PARA A GESTÃO DE RISCOS EM INSTITUIÇÕES PÚBLICAS

Consiste o ForRisco<sup>5</sup> em ferramenta de gestão de riscos inserida no “Sistema For” para governança pública, sistema este que, conforme Bermejo *et al.* (2019, p.

<sup>5</sup> Trata-se da Versão 01 da plataforma, abordada por Bermejo *et al.* (2019).

42), resulta do esforço e visão comum de um grupo de “professores, pesquisadores e especialistas em gestão estratégica, inovação e gestão de riscos para fomentar o aperfeiçoamento dos métodos, processos e softwares de planejamento e gestão” nos órgãos da Administração Pública, cujo objetivo é oferecer soluções capazes de incentivar práticas de inovação e planejamento estratégico em organizações públicas.

Além do ForRisco, o “Sistema For” alberga o ForPDI – Gestão de Plano Estratégico/PDI, destinado à gestão e acompanhamento do Planejamento Estratégico / Plano de Desenvolvimento Institucional de universidades e demais instituições públicas, o qual possibilita o “acompanhamento do PE/PDI em tempo real, de forma colaborativa, eficiente, rápida e segura”, porquanto permite “cadastrar todo o planejamento estratégico do PDI, inserir os valores das metas alcançadas, monitorar o desempenho das metas, elaborar o documento do PDI”, dentre outras atividades, de modo a proporcionar “a sustentação do planejamento estratégico das instituições de ensino e de outras instituições de maneira integrada e interativa (BERMEJO *et al.*, 2019, p. 43).

Por sua vez, o ForRisco é apresentado por Bermejo *et al.* (2019, p. 44-45) como “um conjunto de soluções abertas e gratuitas composto pela metodologia ForRisco, pela capacitação on-line e pelo software ForRisco”, cujo propósito é o de “prover artefatos teóricos e práticos para o acompanhamento e para a gestão de riscos advindos dos processos desenvolvidos pelas instituições”, com vistas à gestão de “processos de identificação, análise, planejamento, monitoramento e controle dos riscos” (BERMEJO *et al.*, 2019, p. 44-45).

Mais precisamente acerca do software ForRisco, destaca ainda o sobredito autor que trata-se de “um módulo de gestão de riscos integrado que permite alterações e adequações dos riscos por membros das instituições e das equipes, facilitando a prevenção de desastres advindos de tais riscos”, dentre outros benefícios, de modo a contribuir para tomada de decisão (BERMEJO *et al.*, 2019, p. 45).

Acerca das funcionalidades do Sistema ForRisco, Bermejo *et al.* (2019, p. 179-180) apontam para uma série de possibilidades oferecidas pelo software visando assegurar a implementação e o acompanhamento da gestão de risco em instituições públicas, destacando que, por meio da ferramenta, é possível:

- criar Política de Gestão de Riscos: dimensão concreta dos mecanismos de orientação para a decisão e a ação das atividades e dos processos de gestão dos riscos;
- criar Plano de Gestão de Riscos: refere-se ao projeto ou conjunto de medidas estabelecidas como guia prático para identificar, administrar e monitorar os riscos;
- avaliar e classificar a tipologia do risco: a classificação está organizada em operacional, legal, imagem/reputação do órgão e financeiro/orçamentário;
- definir o grau do risco: refere-se a uma classificação, pelo usuário, do posicionamento ou nível do risco em um determinado momento. Recomenda-se que o risco seja classificado em crítico, alto, moderado e pequeno;
- estabelecer ações corretivas: são as atividades e as práticas que visam à execução da tomada de decisão para corrigir os incidentes;
- permitir níveis de acesso diferentes: a ferramenta possibilita hierarquizar e controlar o acesso dos usuários por seus gestores;
- reconhecer ameaças ou oportunidades atreladas aos riscos: ameaças são situações de incerteza, externas e/ou internas às organizações, que podem atrapalhar ou impedir o alcance dos objetivos definidos; oportunidades são situações ou circunstâncias favoráveis, externas e/ou internas às organizações, que podem ser aproveitadas e afetar positivamente o alcance dos objetivos;
- definir periodicidade da análise: refere-se aos intervalos regulares em que o risco deverá ser analisado. O sistema oferece os seguintes intervalos: diário, semanal, quinzenal, mensal, bimestral, trimestral, semestral e anual;
- identificar causas e consequências dos riscos: a causa é considerada o princípio, a razão, o motivo ou a origem para que o risco aconteça; a consequência é tudo aquilo que foi produzido (ou poderá ser produzido) diante dos riscos identificados; efeitos ou resultados dos riscos;
- desenvolver matriz de riscos: dispositivo para indicar, de maneira ordenada, a classificação dos riscos proposta pelo usuário a partir do grau do risco; e
- estabelecer ações de prevenção, registrar data e horário de edição das informações, duplicar planos e políticas de gestão de riscos para facilitar a edição, criar ou basear-se nos indicadores do Sistema ForPDI, criar planejamento por unidade, adicionar e editar informações sobre os riscos e realizar pesquisa avançada, entre outras ações.

Assim, pelas características que ostenta, o Sistema ForRisco se apresenta como importante ferramenta à disposição da Administração Pública no desenvolvimento do seu mister de gerenciar riscos, sobretudo em razão da completude de funcionalidades apresentadas por Bermejo *et al.* (2019).

Desta forma, ao transitar pelos princípios constitucionais norteadores da Administração Pública no Brasil, passando pelas definições e categorização de riscos, assim como pela gestão de riscos nas organizações em geral e, em especial, nas instituições públicas, culminando com a apresentação de modelos, técnicas e sistema de gestão de riscos aplicáveis à Administração Pública, o referencial teórico que aqui se finda visou traçar um panorama geral sobre o tema estudado, com vistas a permitir a aplicação do conhecimento colhido às etapas posteriores do estudo, sobretudo visando à formulação da pretendida proposta de contribuição, razão pela qual, doravante, apresenta-se a metodologia que regeu a presente pesquisa.

### 3 METODOLOGIA

Gil (2008, p. 8) afirma que a ciência tem como objetivo primordial alcançar a veracidade dos fatos, enfatizando que “para que um conhecimento possa ser considerado científico” essencial se faz “determinar o método que possibilitou chegar a esse conhecimento”, por método devendo-se entender o “caminho para se chegar a determinado fim”, ao passo que método científico possa ser compreendido “como o conjunto de procedimentos intelectuais e técnicos adotados para se atingir o conhecimento.” Semelhante definição de método científico é apresentada por Vergara (2004, p. 12), que o conceitua como “um caminho, uma forma, uma lógica de pensamento”.

Lakatos e Marconi (2003, p. 83), embora defendam não serem os métodos científicos instrumentos de aplicabilidade exclusiva da ciência, ressaltam que “não há ciência sem o emprego de métodos científicos”, que resultam assim definidos pelas autoras:

o conjunto das atividades sistemáticas e racionais que, com maior segurança e economia, permite alcançar o objetivo - conhecimentos válidos e verdadeiros -, traçando o caminho a ser seguido, detectando erros e auxiliando as decisões do cientista (LAKATOS; MARCONI, 2003, p. 83).

Por sua vez, Richardson (2012, p. 70) classifica “método em pesquisa” como “a escolha de procedimentos sistemáticos para a descrição e explicação de fenômenos”, e define método científico como o ato de “delimitar um problema, realizar observações e interpretá-las com base nas relações encontradas, fundamentando-se, se possível, nas teorias existentes.”

Sinteticamente traçadas as definições de método e método científico, tem-se por relevante registrar que aplica-se à presente pesquisa o método dedutivo, porquanto o estudo buscou apropriar-se do conhecimento sobre o tema proposto com vistas a compreender a necessidade de sua aplicação no objeto de estudo (RICHARDSON, 2012, p. 37).

Assim, cumpre esclarecer que dedica-se o presente capítulo à definição da tipologia da presente pesquisa, bem como a apresentação dos procedimentos que a regeram, pois como sustenta Vergara (2004, p. 46), “o leitor deve ser informado sobre o tipo de pesquisa que será realizada, sua conceituação e justificativa à luz da investigação específica.”

### 3.1 CARACTERIZAÇÃO DO ESTUDO

A presente pesquisa se enquadra naquilo que Richardson (2012, p. 16-17) classifica como “pesquisa para resolver problemas” de abordagem qualitativa, porquanto inclinada à “procura coletiva de solução de problemas práticos”, não estando, por conseguinte, voltada a formular ou testar teorias, mas sim interessada “em descobrir a resposta para um problema específico ou descrever um fenômeno da melhor forma possível”.

Com ela buscou-se conhecer o estágio atual do gerenciamento de riscos na Universidade Federal de Sergipe por meio de diagnóstico situacional e visando à identificação de oportunidade para formulação de proposta de contribuição, e, após, definido o escopo da proposta, procurou-se conhecer a realidade de outras instituições públicas de ensino superior naquele aspecto específico, a fim de que se pudesse formular uma proposta de contribuição para a gestão de riscos aplicável à realidade da instituição pesquisada. Daí pode-se extrair que, quanto à sua natureza, a pesquisa é aplicada, posto que por meio dela buscou-se a geração de conhecimento dirigido à “aplicação imediata numa realidade circunstancial” (GIL, 2008, p. 27).

Acerca da abordagem qualitativa, Vergara (2004) ensina que pesquisas nela baseadas não demandam testagem ou utilização de métodos estatísticos, pois têm como preocupação a confirmação ou não de suposições por meio de métodos outros, inclusive “observações detalhadas e minuciosas do mundo real” (YIN, 2001, p. 34).

Gil (2008, p. 175), por sua vez, leciona ser a abordagem qualitativa isenta de “fórmulas ou receitas predefinidas para orientar os pesquisadores”, de modo que a análise dos dados está intrinsecamente ligada aos predicados subjetivos de cada pesquisador, e atenta ao caráter oscilante que tais dados por natureza ostentam, como explica com maestria Mansano (2014, p. 124-125):

É nesse sentido que os problemas analisados podem ganhar contornos incômodos e provocar estranhamento e, por isso mesmo, pôr os investigadores em contato mais direto com os limites do desconhecido. As pesquisas qualitativas mantêm-se precisamente na vizinhança desse desconhecimento, já que não se sabe, de antemão, o que advirá dos dados e que tipo de análise poderá ser elaborado sobre eles. Daí seu caráter radicalmente aberto que tende, até mesmo, a dispensar a formulação de hipóteses.

[...]

Assim, está-se diante de um processo de investigação que busca conhecer a produção diferenciada e mutante do participante nas redes relacionais (uma heteroprodução), visto que o objetivo dessa metodologia de pesquisa consiste em conhecer as múltiplas dimensões colocadas em curso por esse movimento, as quais, por sua vez, podem ser transformadas com o passar do tempo, incluindo-se aí o tempo dedicado à pesquisa. Daí a necessidade de escolher um método aberto para possíveis desvios, que se mantenha em movimento e seja capaz de acompanhar as minúcias dos depoimentos (dados) cedidos pelos sujeitos participantes que [...] também estão em movimento e, em função disso, poderão fornecer um material por vezes confuso, díspar e contraditório sobre as maneiras como experimentam o problema que está sendo investigado.

Quanto aos seus objetivos, tem-se que a pesquisa se enquadra como exploratória, porquanto “tem como principal finalidade desenvolver, esclarecer e modificar conceitos e ideias, tendo em vista a formulação de problemas mais precisos ou hipóteses pesquisáveis para estudos posteriores” (GIL, 2008, p. 28), ou seja, objetiva “conhecer as características de um fenômeno para procurar, posteriormente, explicações das causas e consequências de dito fenômeno” (RICHARDSON, 2012, p. 326).

Ademais, apesar de gestão de riscos não ser um tema novo ou desconhecido, o estudo deste tema no objeto de estudo (Universidade Federal de Sergipe) é algo que ainda não foi explorado, circunstância que reforça o caráter exploratório da pesquisa.

### 3.2 QUESTÕES DE PESQUISA

As questões de pesquisa surgiram para que fossem respondidas no transcorrer do trabalho e refletiram um roteiro de estudos alinhado aos objetivos específicos, e estão correlacionadas com a coleta e tratamento de dados (VERGARA, 2004). No presente estudo, as questões de pesquisa que surgiram foram as elencadas abaixo:

- a) O que trazem os normativos internos e demais documentos disponíveis relacionados à estratégia, aos objetivos e ao gerenciamento de riscos na UFS?
- b) Qual o estágio atual de implantação da gestão de riscos na instituição pesquisada?
- c) Qual o ponto de oportunidade identificado para formulação da proposta de contribuição?



d) Como se apresentam as estruturas de gestão de riscos implantadas em outras instituições públicas federais de ensino superior, no que se refere ao ponto de oportunidade identificado?

### 3.3 DELINEAMENTO E PROCEDIMENTOS DA PESQUISA

Consoante ensina Gil (2008, p. 49), o delineamento da pesquisa constitui “etapa em que o pesquisador passa a considerar a aplicação dos métodos discretos, ou seja, daqueles que proporcionam os meios técnicos para a investigação”, de modo a retirar o foco dos aspectos teóricos presentes nas fases anteriores para dar espaço aos problemas práticos que envolvem a coleta e verificação de dados, assim correspondendo, conforme Lakatos e Marconi (2003, p. 222), “à parte prática da coleta de dados”.

Assim, a verificação passa a ser viabilizada por procedimentos técnicos que, considerados “um conjunto de preceitos ou processos de que se serve uma ciência, são, também, a habilidade para usar esses preceitos ou normas, na obtenção de seus propósitos” (LAKATOS; MARCONI, 2003, p. 222), e que devem considerar “o ambiente em que são coletados os dados, bem como as formas de controle das variáveis envolvidas” (GIL, 2008, p. 49).

Prodanov e Freitas (2013, p. 54) apontam para o delineamento como sendo o *design* conceitual e operativo da investigação, porquanto objetiva expressar “as ideias de modelo, sinopse e plano”, de modo a representar a idealização da pesquisa “em sua dimensão mais ampla, envolvendo diagramação, previsão de análise e interpretação de coleta de dados, considerando o ambiente em que são coletados”.

Ainda, destacando o procedimento de coleta de dados como o mais relevante elemento para identificação do *design* da pesquisa, Prodanov e Freitas (2013, p. 54) indicam a existência de dois grandes grupos que podem definir o delineamento, sendo eles: a. pesquisas que se baseiam em fontes escritas, tratadas pelos autores como *fontes de papel*, grupo no qual se enquadram a pesquisa bibliográfica e a pesquisa documental; b. pesquisas lastreadas em dados fornecidos por pessoas, nas quais se incluem “a pesquisa experimental, pesquisa *ex-postfacto*, o levantamento, o estudo de caso, a pesquisa-ação e a pesquisa participante”.

Classificação em muito semelhante também é trazida por Gil (2008, p. 50), que alerta para a relativa flexibilidade no delineamento da pesquisa, porquanto “algumas pesquisas, em função de suas características, não se enquadram facilmente num ou noutro modelo”, embora, no mais das vezes, não se encontre dificuldades para enquadrar o estudo numa das categorias acima definidas.

Assim, a presente pesquisa se enquadra como Estudo de Caso, porquanto inserida numa “categoria de investigação que tem como objeto o estudo de uma unidade de forma aprofundada” (PRODANOV; FREITAS, 2013, p. 54), ou seja, caracterizada “pelo estudo profundo e exaustivo de um ou de poucos objetos, de maneira a permitir o seu conhecimento amplo e detalhado”, com o propósito de “explorar situações da vida real cujos limites não estão claramente definidos” (GIL, 2008, p. 57-58).

Em palavras outras, buscou-se investigar, de forma profunda e exaustiva, o gerenciamento de riscos no âmbito da Universidade Federal de Sergipe, ainda pouco explorado, de modo a se permitir conhecer, detalhadamente, as nuances do mecanismo de controle de riscos na instituição, a ponto de se tornar possível a propositura de uma intervenção visando ao seu aprimoramento.

### 3.4 UNIDADE DE ANÁLISE E CRITÉRIOS PARA ESCOLHA DO CASO

A presente pesquisa tem como escopo o estudo do tema gestão de riscos, sobretudo na Administração Pública, e mais especificamente na Universidade Federal de Sergipe – UFS, visando à elaboração de proposta capaz de contribuir com o aprimoramento da gestão de riscos na instituição que, embora formalmente criada em 15 de maio de 1968, iniciou em 1948, por meio dos cursos que adiante viria a absorver, a sua trajetória de contribuição para o desenvolvimento do estado de Sergipe, consoante historiado em seu sítio na internet:

A criação da Faculdade de Ciências Econômicas e da Escola de Química (1948), seguida da Faculdade de Direito e Faculdade Católica de Filosofia (1950), Escola de Serviço Social (1954) e Faculdade de Ciências Médicas (1961), fez com que fosse atingido o número mínimo necessário de escolas superiores para que se pleiteasse a fundação de uma universidade em Sergipe.

Em 1963, a então Secretaria de Educação do Estado deu início ao processo de criação da universidade, concretizado em 1967 pelo Decreto-Lei nº 269 e efetivado em 15 de maio de 1968. À época, havia duas possibilidades de regime para a instituição: a autárquica, defendida pelo diretor da então Faculdade de Medicina, Antônio Garcia Filho, e a Fundação Federal,

defendida por Dom Luciano José Cabral Duarte, então presidente do Conselho Federal de Educação (CFE).

Instituiu-se, então, a Fundação Universidade Federal de Sergipe integrada ao sistema federal de ensino superior, incorporando todos os cursos superiores existentes no estado. (UFS, 2020)

A fim de proporcionar uma reforma administrativo-acadêmica, em 1978 novas diretrizes do Ministério da Educação fizeram com que a UFS reformulasse o currículo dos seus até então 23 cursos e os distribuisse em quatro unidades de ensino existentes até hoje: Centro de Ciências Exatas e Tecnologia (CCET), Centro de Ciências Biológicas e da Saúde (CCBS), Centro de Ciências Sociais Aplicadas (CCSA) e Centro de Educação e Ciências Humanas (CECH).

A década de 1980 marca o início da transferência gradativa da universidade para suas novas instalações no campus universitário em São Cristóvão (Grande Aracaju). Em 1987, em observância à Resolução 01/87 do Conselho Universitário (CONSU), o campus passou a ser denominado “Cidade Universitária Prof. José Aloísio de Campos”.

A partir dos anos 2000, a UFS iniciou um vigoroso processo de expansão, que culminou com a criação de mais um Centro, o Centro de Ciências Agrárias Aplicadas – CCAA e outros cinco campi, que, atualmente, juntos ofertam 113 (cento e treze) cursos de graduação nas mais diversas áreas de conhecimento, sendo 82 (oitenta e dois) no Campus São Cristóvão - distribuídos entre o Centro de Ciências Exatas e Tecnologia – CCET (27), Centro de Educação e Ciências Humanas - CECH (29), Centro de Ciências Sociais Aplicadas – CCSA (12), Centro de Ciências Biológicas e da Saúde – CCBS (08) e Centro de Ciências Agrária Aplicadas – CCAA (06); 10 (dez) no Campus Itabaiana, 08 (oito) no Campus Lagarto; 05 (cinco) no Campus Aracaju; 04 (quatro) no Campus Laranjeiras; e 04 (quatro) no Campus Nossa Senhora da Glória, conforme se extrai do informativo “UFS Em números 2020”, igualmente disponível na página mantida pela instituição na internet.

Conforme sobredito informativo, no ano de 2019 foram graduados 2460 (dois mil quatrocentos e sessenta) alunos, o que representa uma taxa de sucesso global de 41,7%, ao passo que no semestre 2020.1 o documento aponta para 4.806 (quatro mil, oitocentos e seis) ingressantes e 25.163 (vinte e cinco mil, cento e sessenta e três) alunos de graduação matriculados.

Assim, presente na capital de Sergipe e em mais 05 (cinco) municípios do estado (Itabaiana, Lagarto, Laranjeiras, São Cristóvão e Nossa Senhora da Glória), a UFS vem há mais de 05 (cinco) décadas, desempenhando sua missão de oferecer à comunidade, sobretudo sergipana, serviços educacionais de qualidade reconhecida, capazes de modificar realidades.

Criada sob a forma de Fundação Pública de Direito Público Federal vinculada ao Ministério da Educação, a UFS vem se notabilizando como a única universidade pública do estado de Sergipe, cuja missão é “contribuir para o progresso da sociedade por meio da geração de conhecimento e da formação de cidadãos críticos, éticos e comprometidos com o desenvolvimento sustentável” (UFS, 2021).

Assim, como instituição pública federal de ensino superior que é, não há dúvidas de que a UFS deve estar submetida aos ditames de normativas que estabelecem a necessidade de implantação de uma série de mecanismos e estratégias de governança no âmbito da Administração Pública Federal, dentre eles a sistematização da gestão de riscos, cujo objetivo, conforme Vieira e Barreto (2019, p. 111-112), é gerar e preservar valor à partes interessadas, por meio do adequado enfrentamento das incertezas decorrentes de fontes internas e externas capazes de influenciar nas atividades que conduzem ao alcance dos objetivos da organização, de modo a ser “fundamental para o sucesso no cumprimento da missão da agência pública em entregar serviços de qualidade, ajudando a melhorar a eficiência, a eficácia e a efetividade da gestão”, e os índices de confiança da sociedade em relação a tais serviços e quanto à aplicação dos recursos públicos.

À guisa de exemplo das normativas supramencionadas, tem-se a Lei Complementar 101/2000 (Lei de Responsabilidade Fiscal), em seu art. 1º, §1º; o Decreto nº 9.203/2017, que “dispõe sobre a política de governança da administração pública federal direta, autárquica e fundacional”, e a Instrução Normativa Conjunta MP/CGU nº 01/2016, que “dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo federal”.

Ademais, o já mencionado Relatório de Políticas e Programas de Governo (RePP) – desenvolvido pelo TCU e cujas conclusões resultam assentadas no Acórdão nº 2.127/2017 – aponta para um cenário deficitário no tocante à governança e gestão de riscos nas instituições públicas federais, de modo a revelar ser premente a estruturação do gerenciamento de riscos em tais instituições (TCU, 2018).

### 3.5 FONTES DE EVIDÊNCIA

Cumpra aqui registrar as fontes das quais os dados necessários à realização da pesquisa foram coletados. Nesse sentido, Yin (2001), sem descuidar de alertar para a existência de outras fontes de evidências, apresenta seis fontes que considera de maior proeminência, sendo elas: Documentação, Registros em arquivos, Entrevistas, Observação direta, Observação participante e Artefatos físicos.

Nesse sentido, tomando-se como base as lições de Yin (2001) acima esposadas, tem-se que o presente estudo teve como fonte de evidência a “documentação”, cuja análise é definida por Richardson (2012, p. 228) como “a observação que tem como objeto não os fenômenos sociais, quando e como se produzem, mas as manifestações que registram estes fenômenos e as ideias elaboradas a partir deles”, o que se deu por meio do exame de normativos internos e demais documentos relacionados à estratégia e aos objetivos da UFS, assim como ao gerenciamento de riscos na instituição, bem como àqueles relativos às instituições públicas federais de ensino pesquisadas, pois, conforme Yin (2001, p. 107), “exceto para os estudos que investigam sociedades que não dominam a arte escrita, é provável que as informações documentais sejam relevantes a todos os tópicos do estudo de caso”.

Conforme GIL (2008, p. 147), a utilização da fonte de evidência em questão é caracterizada pela coleta de dados por meio de documentos, a exemplo daqueles lavrados por órgãos da Administração Pública, ou seja, materiais ainda não submetidos a tratamento analítico, desde que tenham potencial para fornecer elementos com vistas à verificação do fenômeno ou fato pesquisado.

De igual forma, teve também como fonte de evidências “entrevistas” que, conforme Lakatos e Marconi (2003), constituem uma metódica confabulação com o interlocutor entrevistado, por meio da qual o pesquisador coleta as informações que compreende necessárias à investigação, oportunidade na qual buscou-se junto ao responsável pela gestão de riscos na UFS dados acerca da implementação do mecanismo na instituição – por meio das questões formuladas no Roteiro de Entrevista constante do Apêndice B –, de igual forma procedendo em relação a envolvidos na implantação da gestão de riscos em duas instituições públicas

federais de ensino superior, neste caso especificamente quanto ao ponto de oportunidade de formulação da proposta identificado na UFS, utilizando-se, para tanto, das questões dispostas no Roteiro de Entrevistas constante do Apêndice C.

No que se refere às duas instituições cujos dados foram coletados, a realização de pesquisa prévia indicou que ambas as IFES já haviam deflagrado o processo de implantação da gestão de riscos nos seus respectivos âmbitos, tendo este sido o critério que conduziu à escolha da UFCA – Universidade Federal do Cariri, localizada no estado do Ceará, e da UFERSA – Universidade Federal Rural do Semi-Árido, estabelecida no estado no Rio Grande do Norte.

Sobre as fontes de evidências que subsidiaram a pesquisa - documentação e entrevista - Yin (2001) se ocupa de trazer um quadro que apresenta os pontos fortes e pontos fracos de cada uma delas, que pela sua relevância, foi aqui adaptado, de forma a contemplar apenas as fontes empregadas na presente pesquisa, conforme se apresenta no Quadro 3.

<b>Quadro 3 – Pontos fortes e pontos fracos das fontes de evidências empregadas</b>		
Fonte de Evidência	Pontos Fortes	Pontos Fracos
Documentação	<ul style="list-style-type: none"> <li>●Estável – pode ser revisada inúmeras vezes;</li> <li>●Discreta – não foi criada como resultado do estudo de caso;</li> <li>●Exata – contém nomes, referências e detalhes exatos de um evento;</li> <li>●Ampla cobertura – longo espaço de tempo, muitos eventos e muitos ambientes distintos.</li> </ul>	<ul style="list-style-type: none"> <li>●Capacidade de recuperação – pode ser baixa;</li> <li>●Seletividade tendenciosa, se a coleta não estiver completa;</li> <li>●Relato de visões tendenciosas – reflete as ideias preconcebidas (desconhecidas) do autor;</li> <li>●Acesso – pode ser deliberadamente negado.</li> </ul>
Entrevistas	<ul style="list-style-type: none"> <li>●Direcionadas – enfocam diretamente o tópico do estudo de caso;</li> <li>●Perceptivas – fornecem inferências causais percebidas.</li> </ul>	<ul style="list-style-type: none"> <li>●Visão tendenciosa devido a questões mal elaboradas;</li> <li>●Respostas tendenciosas;</li> <li>●Ocorrem imprecisões devido à memória fraca do entrevistado;</li> <li>●Reflexibilidade – o entrevistado dá ao entrevistador o que ele quer ouvir.</li> </ul>

Fonte: Adaptado de Yin (2001)

A compreensão dos pontos fortes e fracos trazida por Yin (2001) se mostra relevante para o presente estudo na medida em que permite ao pesquisador direcionar seus esforços para a exploração dos pontos fortes de cada uma das fontes de evidências, e ao mesmo tempo buscar meios para eliminar ou, ao menos, mitigar a incidência dos pontos fracos.

Ademais, ainda conforme Yin (2001), a utilização conjunta de duas ou mais fontes de evidências trazem maior confiabilidade às informações coletadas, conferindo, por consequência, maior nível de confiança aos resultados obtidos na pesquisa.

### 3.6 DEFINIÇÕES CONSTITUTIVAS

Delineada a pesquisa e apresentados os procedimentos técnicos que a subsidiaram, e, ainda, aclaradas as questões atinentes aos critérios de escolha do caso, torna-se indicado traçar algumas importantes definições constitutivas que, conforme Gil (2008, p. 79), constitui “a operacionalização das variáveis, que pode ser definida como processo em que sofre uma variável (ou um conceito) a fim de se encontrar os correlatos empíricos que possibilitem sua mensuração ou classificação”.

O autor exemplifica o sustentado tendo por base a hipotética variável ou conceito “*status* socioeconómico” que pode ser definido “teoricamente como a posição de um indivíduo na sociedade, tomando-se como referência a posição dos outros indivíduos em relação à sua” (GIL 2008, p. 79).

Assim, tem-se por pertinente apresentar as seguintes definições constitutivas:

**1. Instituições públicas federais de ensino superior:** Refere-se às Universidades e aos Institutos Federais mantidos por recursos públicos e vinculados ao Ministério da Educação e, portanto, sujeitos à legislação atinente à obrigatoriedade do gerenciamento de riscos;

**2. Riscos organizacionais:** Eventos incertos incidentes nas atividades da organização que se mostrem capazes de impor consequências negativas ou positivas na busca pelo alcance dos seus objetivos;

**3. Gerenciamento de riscos:** Também tratado no presente estudo como gestão de riscos, é o conhecimento, enfrentamento e capacidade de respostas, à nível organizacional, quanto aos riscos incidentes em suas atividades que apresentem potencial para impactar negativa ou positivamente no alcance dos seus objetivos;

**4. Estruturação do gerenciamento de riscos:** Implementação sistemática e estruturada de procedimentos que visem à gestão de riscos.

### 3.7 CATEGORIAS ANALÍTICAS E ELEMENTOS DE ANÁLISE

Acerca das categorias de análise, Richardson (2012) faz uma importante ressalva sobre a necessidade de equilíbrio por ocasião da criação de tais categorias por parte do pesquisador, a fim de que - em última análise - não haja desperdício de tempo e acúmulo de informações despiciendas, que podem criar embaraços à pesquisa, sobretudo quando da análise de dados:

[...] os problemas que suscitam análise qualitativa exigem do pesquisador trato especial na condução das observações e habilidades quanto ao uso ou criação das categorias, pois, mesmo que se obtenha um conjunto de observações bastante amplo e não se tomem como referencial certas categorias, é quase certo que sejam encontradas dificuldades quando da análise ordenada das informações. E, nesse aspecto, alguns pesquisadores inexperientes ou outros profissionais chegam a levantar informações detalhadas e extensas sobre um problema, porém não sabem delas fazer uso apropriado nas fases de análise (2012, p. 83).

Nesse sentido, o Quadro 4, a seguir apresentado, trata de correlacionar os objetivos específicos às respectivas categorias de análise e elementos de análise tidos por necessários, e que serviram de base para a presente pesquisa, reservando ainda o espaço para fontes de evidências utilizadas para o atingimento desses elementos de análise, com vistas ao alcance dos sobreditos objetivos.

<b>Quadro 4 – Objetivos específicos, categorias de análise e elementos de análise (continua)</b>			
<b>Objetivos específicos</b>	<b>Categorias de análise</b>	<b>Elementos de análise</b>	<b>Fonte de Evidência</b>
Identificar normativos internos e demais documentos relacionados à estratégia e aos objetivos da Universidade Federal de Sergipe no que tange à gestão de riscos na instituição.	Instrumentos normativos editados	-Manuais, Portarias, Resoluções e demais normativos que versam sobre a estratégia, os objetivos e a gestão de riscos;	Documentação



<b>Quadro 4 – Objetivos específicos, categorias de análise e elementos de análise (conclusão)</b>			
Diagnosticar o estágio atual de implantação da gestão de riscos na instituição pesquisada.	Eventos e outras iniciativas de disseminação da gestão de riscos no âmbito da instituição pesquisada	-Cursos e/ou eventos de qualificação de pessoal voltados ao tema gestão de riscos.	Documentação e Entrevista Questão 4 do Roteiro de Entrevista constante do Apêndice B.
	Diagnóstico situacional	-Estágio atual de implantação; -Prevalência de modelos e/ou estruturas; -Envolvimento do quadro de pessoal; -Dificuldades enfrentadas. -Efeitos da implantação para a estratégia e objetivos da instituição.	Entrevista Questões 1, 2, 3, 5 e 6 do Roteiro de Entrevista constante do Apêndice B..
Identificar ponto de oportunidade de formulação da proposta de contribuição.	Ponto de oportunidade identificado visando à formulação da proposta de contribuição	-Necessidade/conveniência da proposta a ser formulada.	Documentação
Conhecer estruturas de gestão de riscos implantadas em outras instituições públicas federais de ensino superior, no que se refere ao ponto de oportunidade identificado.	Coleta de dados junto a outras IFES visando à formulação da proposta de contribuição	-De que forma a instituição aborda o tema; -Envolvimento do quadro de pessoal; -Dificuldades enfrentadas; -Lições aprendidas.	Entrevista Questões 1 a 4 do Roteiro de Entrevista constante do Apêndice C.

Fonte: Elaborado pelo autor (2021).

### 3.8. PROTOCOLO DE ESTUDO

Conforme define Yin (2001), o protocolo de estudo consiste em formalização que visa traçar orientações procedimentais a fim de que o pesquisador possa conduzir, de forma estruturada e coesa, a sua pesquisa, como o fito de conferir ao estudo a máxima confiabilidade possível.

Assim, se presta o Quadro 5 a exprimir o protocolo de estudo que orientou a realização da presente pesquisa.

<b>Quadro 5 – Protocolo de estudos</b>	
<b>Questão de pesquisa</b>	O que pode ser feito em prol da implantação e/ou melhoria da gestão de riscos na Universidade Federal de Sergipe, de forma que se apresente uma proposta viável e alinhada à realidade e necessidade da organização?
<b>Unidade de análise</b>	Área de Gestão de Riscos da Universidade Federal de Sergipe – UFS.
<b>Organizações</b>	Universidade Federal de Sergipe – UFS.
<b>Limite de tempo</b>	Até o mês de novembro do ano de 2021.
<b>Fontes de dados e confiabilidade</b>	Cruzamento entre dados coletados mediante entrevistas semiestruturadas e análise documental.
<b>Validade dos dados</b>	Fontes múltiplas de evidência (entrevistas e documentos).
<b>Questões do estudo de caso</b>	<p>a) O que trazem os normativos internos e demais documentos disponíveis relacionados à estratégia, aos objetivos e ao gerenciamento de riscos na UFS?</p> <p>b) Qual o estágio atual de implantação da gestão de riscos na instituição pesquisada?</p> <p>c) Qual o ponto de oportunidade identificado para formulação da proposta de contribuição?</p> <p>d) Como se apresentam as estruturas de gestão de riscos implantadas em outras instituições públicas federais de ensino superior, no que se refere ao ponto de oportunidade identificado?</p>
<b>Procedimento de campo do protocolo (PREPARAÇÃO)</b>	Elaboração do roteiro de entrevista. Contato com os participantes – unidade de análise.
<b>Procedimento de campo do protocolo (AÇÃO)</b>	Agendamento das entrevistas. Realização das entrevistas. Transcrição das entrevistas.
<b>Relatório do estudo de caso</b>	Consolidação dos dados. Confronto dos dados com os objetivos da pesquisa.

Fonte: Elaborado a partir de Yin (2001).

### 3.9 ANÁLISE DOS DADOS

Para exame dos dados que foram coletados, a presente pesquisa valeu-se da Análise Qualitativa classificada por Gibbs (2009, p. 20) como “nomotética”, e que “tenta mostrar o que as pessoas, eventos e contextos têm em comum e explicá-los em termos dessas características comuns”.

Conforme o autor, na pesquisa qualitativa, “isso se faz procurando variações e diferenças e tentando relacioná-las ou mesmo correlacioná-las com outras características observadas, como comportamentos, ações e resultados” (GIBBS, 2009, p. 20).

Em relação aos critérios tomados para a análise, adotou-se a seguinte ordem:

- a. Pré-análise: Fase representada pela seleção de documentos, definição de objetivos, categorias analíticas e elementos de análise, visando à estruturação da análise de resultados.
- b. Exploração do material: Fase na qual se buscou proceder com a análise da documentação de lavra da UFS acerca dos objetivos, estratégia e gestão de riscos; documentação relacionada ao gerenciamento de riscos nas instituições pesquisadas; bem como dos dados coletados por meio das entrevistas semiestruturadas.
- c. Tratamento e interpretação dos resultados obtidos: Etapa na qual buscou-se a consolidação e a interpretação dos dados obtidos na fase de exploração do material, sendo traçada uma discussão acerca de pontos de divergência e de convergência identificados entre o levantado no referencial e o coletado por meio das fontes de evidência, e pela qual se tornou possível identificar o ponto de oportunidade para formulação da proposta de contribuição.
- d. Verificação de como o ponto de oportunidade para formulação da proposta de contribuição resultou tratado nas duas instituições pesquisadas (UFCA e UFERSA).
- e. Elaboração da proposta de contribuição, tendo por base os achados advindos das etapas anteriores.

### 3.10 FORMULAÇÃO DE PROPOSTA DE INTERVENÇÃO A PARTIR DO DIAGNÓSTICO OBTIDO COM A ANÁLISE DOS DADOS

Consoante trazido ao longo de toda a apresentação da metodologia do trabalho, a presente pesquisa está delineada como “Estudo de caso”, pois consiste numa pesquisa “empírica que investiga um fenômeno contemporâneo dentro de seu contexto da vida real, especialmente quando os limites entre o fenômeno e contexto não estão claramente definidos” Yin (2001, p. 32), e, quanto à sua natureza, é classificada como “aplicada”, porquanto, conforme Prodanov e Freitas (2013, p. 51),

“objetiva gerar conhecimentos para aplicação prática dirigidos à solução de problemas específicos”, envolvendo “verdades e interesses locais”.

Assim, a fim de atender às premissas traçadas acima, após realizado o diagnóstico organizacional quanto à gestão de riscos no objeto do estudo, foi formulada uma proposta de intervenção, que versa sobre aspectos de gerenciamento de riscos na UFS, de acordo com a necessidade diagnosticada.

## **4 DIAGNÓSTICO DA GESTÃO DE RISCOS NA UNIVERSIDADE FEDERAL DE SERGIPE**

Trata o presente capítulo do exame das normativas e demais instrumentos existentes e voltados à gestão de riscos na Universidade Federal de Sergipe, com o fito de identificar o estágio atual de implantação e/ou aplicação do gerenciamento de eventos incertos no âmbito da instituição federal de ensino superior objeto do estudo.

### **4.1 INSTRUMENTOS NORMATIVOS EDITADOS**

A análise dos instrumentos normativos editados pela UFS acerca do tema Gestão de Riscos, em conjunto com o tratado no tópico seguinte, visou responder à questão de pesquisa “o que trazem os normativos internos e demais documentos disponíveis relacionados à estratégia, aos objetivos e ao gerenciamento de riscos na UFS?”, por meio da identificação de “Manuais, Portarias, Resoluções e demais normativos que versam sobre a estratégia, os objetivos e a gestão de riscos na instituição”, consoante previsto no Quadro 4.

De partida, na linha traçada pela Instrução Normativa Conjunta MP/CGU nº 01/2016, observa-se que a UFS iniciou, no ano de 2017, um conjunto de ações que visam à implantação da gestão de riscos na instituição, as quais são aqui apresentadas, seguindo ordem cronológica.

Antes, porém, o Plano de Desenvolvimento Institucional (PDI 2016-2020), de lavra da Comissão instituída pela Portaria nº 2054/2014/GR sob a coordenação da Pró-Reitoria de Planejamento – PROPLAN/UFS e em parceria com a comunidade universitária, apresentou “um diagnóstico da Universidade, sua missão, visão, políticas acadêmicas e administrativas, fundamentadas em sua realidade institucional”, no qual resultam consignados objetivos e metas estratégicas para o período de referência (PDI UFS 2016/2020, p. 5), que no curso da sua vigência viriam a ser observados pelos instrumentos normativos relacionados à gestão de riscos editados pela instituição.

Neste sentido, o PDI 2016-2020 esclarece que a missão, visão e objetivos gerais da UFS carregam na proa os seguintes fundamentos:

**MISSÃO**

- Contribuir para o progresso da sociedade por meio da geração de conhecimento e da formação de cidadãos críticos, éticos e comprometidos com o desenvolvimento sustentável.

**VISÃO**

- Ser uma instituição pública e gratuita que se destaque pelo seu padrão de excelência, no cumprimento de sua missão.

**OBJETIVOS GERAIS**

- Formar profissionais cidadãos, produzir, difundir e conservar conhecimentos de forma interativa com a sociedade, visando contribuir, assim, para o fortalecimento da democracia e a melhoria da qualidade de vida da população.

- Cultivar o saber em suas várias formas de conhecimento puro e/ou aplicado, propondo-se a:

Formar recursos humanos de nível superior, em graduação e pós-graduação, para atender às necessidades locais, regionais e nacionais;

Realizar pesquisas e incentivar atividades criadoras nos campos do conhecimento filosófico, científico, técnico e artístico;

Estender à comunidade, com a qual deverá manter permanente intercâmbio, os programas de ensino e pesquisa, através de cursos ou atividades similares, e da prestação de serviços especiais;

Investigar e oferecer soluções para os problemas relacionados com o desenvolvimento socioeconômico e cultural do estado, da região Nordeste e do país;

Manter a indissociabilidade entre o ensino, a pesquisa e a extensão;

Estimular a elevação do desempenho institucional, alocando e valorizando recursos humanos e viabilizando recursos materiais para isso necessários;

Ser instrumento de equidade social, ofertando vagas indistintamente às diferentes camadas da população. (PDI UFS 2016/2020, p. 15)

Assim, ainda que de forma bastante incipiente, o PDI em comento já revelava uma preocupação com a gestão de riscos na área de Tecnologia da Informação, conforme se extrai do “Quadro 14 - Acompanhamento da governança de TI - UFS, 2016-20”, que, ao se referir ao indicador “Índice de Interrupção de serviços (Redes e Sistemas)”, cujo propósito é mensurar “o número de ocorrências de queda da rede e dos sistemas ao longo do ano”, apresenta como diagnóstico situacional a falta de monitoramento, avaliação e gerenciamento de riscos (PDI UFS 2016/2020, p. 77).

No entanto, do ponto de vista normativo e, especificamente sobre gestão de riscos, observa-se que a Portaria nº 772/2017/GR, de 08/05/2017, ao estabelecer “princípios e diretrizes relativos à Política de Gestão de Riscos da UFS” e instituir o “Comitê de Governança, Riscos e Controle”, surge como o passo inaugural da implantação da gestão de riscos no âmbito da UFS, cuidando de traçar objetivos e definir conceitos inerentes ao gerenciamento de riscos, a exemplo de risco e apetite a risco, dentre outros, visando ao atendimento das determinações contidas na Instrução Normativa Conjunta 01/2016/MPOG/CGU que, em seu art. 1º, cravou a obrigatoriedade da adoção do procedimento, aduzindo que “os órgãos e entidades

do Poder Executivo federal deverão adotar medidas para a sistematização de práticas relacionadas à gestão de riscos, aos controles internos, e à governança”.

Por sua vez, a Portaria nº 648, de 01 de setembro de 2020, que instituiu o Comitê de Gestão de Riscos e Controles da Universidade Federal de Sergipe (CGRC), definindo-o, na oportunidade, como “a unidade colegiada responsável por conduzir a execução do Plano de Gestão de Riscos e Controles da UFS”, revogou em parte os termos da Portaria nº 772/2017/GR, na medida em que criou um Comitê específico para tratar da gestão de riscos (CGRC), mantendo o tema Governança sob a tutela de outro Comitê com finalidade igualmente específica.

A Portaria nº 648/2020/GR/UFS elucida, dentre outros aspectos, que “a gestão de riscos visa apoiar melhorias contínuas nos processos organizacionais, projetos e iniciativas estratégicas no âmbito da UFS, provendo razoável segurança no cumprimento do propósito e no alcance dos objetivos organizacionais” (Art. 3º), enumerando as seguintes competências e atribuições do CGRC/UFS:

**Art. 2º** O CGRC é a unidade colegiada responsável por conduzir a execução do Plano de Gestão de Riscos e Controles da UFS, possuindo as seguintes competências e atribuições:

- I - elaborar o Plano de Gestão de Riscos e Controles da UFS;
- II - prestar apoio e orientação técnica às unidades administrativas da Universidade, visando o cumprimento das determinações estabelecidas nesta política;
- III - supervisionar e auxiliar na implementação e execução da Política de Gestão de Riscos e Controles, com o apoio permanente de outras unidades de gestão na UFS;
- IV - elaborar proposta de metodologia para gestão de riscos e suas revisões;
- V - propor a definição dos requisitos funcionais necessários à ferramenta de tecnologia de suporte ao processo de gerenciamento de riscos;
- VI - propor a definição dos níveis de apetite a risco dos processos organizacionais;
- VII - propor a definição dos responsáveis pelo gerenciamento de riscos dos processos organizacionais;
- VIII - dar suporte à identificação, análise e avaliação dos riscos dos processos organizacionais selecionados para a implementação da Política de Gestão de Riscos e Controles;
- IX - monitorar a evolução dos níveis de riscos e a efetividade das medidas de controle implementadas;
- X - requisitar aos responsáveis pelo gerenciamento de riscos dos processos organizacionais as informações necessárias para a consolidação dos dados e a elaboração dos relatórios gerenciais;
- XI - consolidar os resultados das unidades monitoradas em relatórios gerenciais;
- XII - propor, em articulação com a Pró-Reitoria de Gestão de Pessoas, capacitações continuadas em Gestão de Riscos e Controles para os servidores da UFS.

As atribuições balizadas pela supracitada Portaria se mostram em consonância com as metodologias de gestão de riscos estudadas, expressando, sobretudo, a liderança e o comprometimento tratados como núcleo da estrutura proposta pela norma ABNT NBR ISO 31000:2018, onde prega que “a Alta Direção e os órgãos de supervisão” devem assegurar “que a gestão de riscos esteja integrada em todas as atividades da organização, e convém que demonstrem liderança e comprometimento” com vistas a “personalizar e implementar todos os componentes da estrutura; emitir uma declaração ou política que estabeleça uma abordagem, plano ou curso de ação da gestão de riscos, atribuir autoridades, responsabilidades e responsabilização nos níveis apropriados” (ABNT, 2018, p. 5).

A Resolução nº 15/2020/CONSU, de 28 de setembro de 2020, e que “institui a Política de Governança da Universidade Federal de Sergipe - UFS e dá outras providências”, por seu turno, ao estabelecer as diretrizes da governança pública da UFS, já o faz atentando também para os princípios norteadores e os objetivos da gestão de riscos, consoante se extrai do seu art. 4º, infratranscrito:

**Art. 4º** São diretrizes da governança pública na UFS:

- I. direcionar ações para a busca de resultados para a sociedade, encontrando soluções tempestivas e inovadoras para lidar com a limitação de recursos e com as mudanças de prioridades;
- II. promover a simplificação administrativa, a modernização da gestão pública e a integração dos serviços públicos, especialmente aqueles prestados por meio eletrônico;
- III. monitorar o desempenho e avaliar a concepção, a implementação e os resultados das políticas e ações prioritárias para assegurar que as diretrizes estratégicas sejam observadas;
- IV. articular as unidades acadêmicas e administrativas e coordenar processos para melhorar a integração entre os diferentes segmentos da Universidade, com vistas a gerar, preservar e entregar valor público;
- V. fazer incorporar padrões elevados de conduta pela alta administração para orientar o comportamento dos agentes públicos, em consonância com as funções e atribuições dos setores da instituição;
- VI. implementar controles internos fundamentados na gestão de risco, que privilegiará ações estratégicas de prevenção antes de processos sancionadores;
- VII. manter processo decisório orientado pelas evidências, pela conformidade legal, pela qualidade regulatória, pela desburocratização e pelo apoio à participação da sociedade;
- VIII. editar e revisar atos normativos, pautando-se pelas boas práticas regulatórias e pela legitimidade, estabilidade e coerência do ordenamento jurídico, realizando consultas públicas sempre que conveniente;
- IX. definir formalmente as funções, competências e responsabilidades das estruturas e dos arranjos institucionais; e
- X. promover a comunicação aberta, voluntária e transparente das atividades e dos resultados da organização, de maneira a fortalecer o acesso público à informação.



E foi no uso de suas atribuições que o Comitê de Gestão de Riscos e Controles – CGRC elaborou e aprovou em 18/05/2021 a publicação “Metodologia de Gestão de Riscos da UFS”, que se ocupa de delinear os procedimentos que devem ser observados com vistas à operacionalização do gerenciamento de riscos na instituição, apresentando “critérios que deverão ser seguidos pela unidade executiva de gestão de riscos da Universidade e acompanhadas pelas instâncias de gestão, conforme competências e responsabilidades estabelecidas na Política de Gestão de Riscos e Controles da UFS”.

Referida publicação evidencia que o processo de gestão e controle de riscos proposto contempla os princípios e componentes trazidos pela norma ABNT ISO 31000/2018, destacando a necessidade e importância do mapeamento dos processos para a implementação propriamente dita do gerenciamento pretendido, o que faz ao definir etapas que visam delinear o escopo dos processos organizacionais, consoante a seguir transcrito:

- Identificar o processo e o nível em que este se insere (estratégico, tático ou operacional) na Universidade;
- Avaliar e registrar os objetivos do processo e como estão alinhados aos objetivos organizacionais da UFS;
- Identificar e registrar o macroprocesso ao qual o processo em análise esteja associado, as leis e regulamentos e os sistemas utilizados para sua execução.

Na mesma linha e, acolhendo parecer do Comitê Institucional de Governança da UFS, o CGRC cuidou de definir em 21/05/2021 o apetite a risco da instituição como BAIXO/MÉDIO, o que fez observando as orientações constantes da publicação Referencial básico de gestão de riscos (TCU, 2018) e da Metodologia de Gestão de Riscos da Controladoria Geral da União (2021), e esclarecendo que “o nível de risco de cada evento é calculado com base na probabilidade de realização do evento de risco e no impacto que este risco causa na consecução dos objetivos do processo” (UFS, 2021).

Ademais, revogando em todos os seus termos a Portaria nº 772/2017/GR que, como já visto, estabeleceu “princípios e diretrizes relativos à Política de Gestão de Riscos da UFS”, a Resolução nº 9/2021/CONSU, de 14 de junho de 2021, veio instituir as novas “Políticas de Integridade e de Gestão de Riscos e Controles” da UFS, apontando como objetivo precípua o de “disseminar princípios, estabelecer diretrizes e estimular a cultura institucional para a gestão da integridade, riscos e

controles, no âmbito da Política de Governança da Instituição”, de modo a apresentar, em seu art. 23, as instâncias da Gestão de Riscos e Controle da UFS, com seguinte delineamento:

- Art. 23. São instâncias responsáveis pela Gestão de Riscos e Controles, no âmbito de suas atribuições:
- I. Conselho Universitário (CONSU) e Conselho do Ensino, da Pesquisa e da Extensão (CONEPE);
  - II. Reitoria;
  - III. Auditoria Interna;
  - IV. Comitê Institucional de Governança (CIG);
  - V. Comitê de Gestão de Riscos e Controles (CGRC);
  - VI. Unidade executiva de gestão de riscos e controles, e,
  - VII. Gestor de processo organizacional.

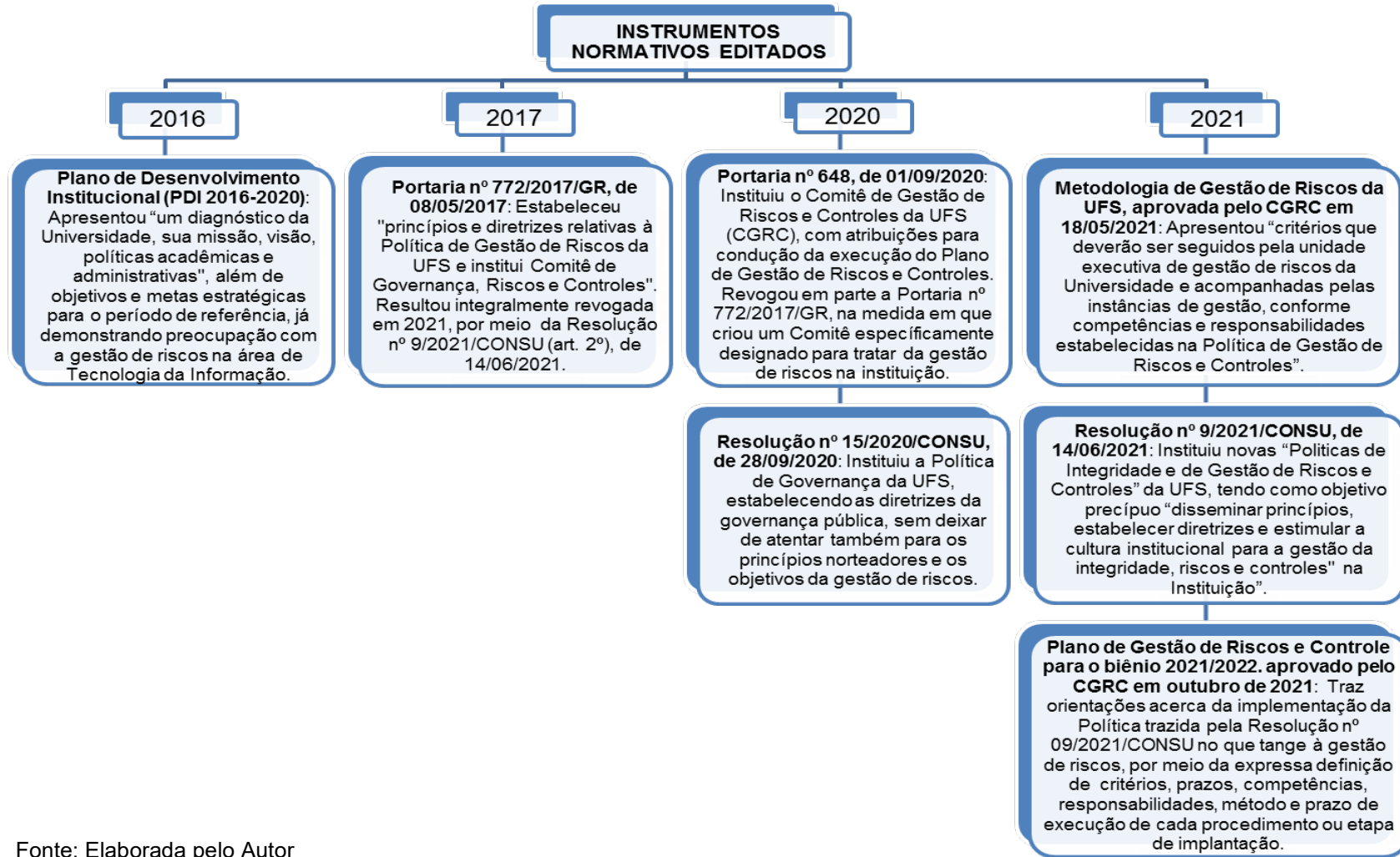
Sobredita normativa bem espelha os princípios “Governança e liderança” e “Integração” trazidos pelo modelo Orange Book, os quais preceituam que “o gerenciamento de riscos deve ser uma parte essencial da governança e liderança, e estas vistas como fundamental para a maneira como a organização é dirigida, gerenciada e controlada em todos os níveis”, de modo a possibilitar que a gestão de riscos ocorra “de forma integrada entre todos os níveis organizacionais, funcionando como um suporte para a tomada de decisão visando à realização dos objetivos da organização” (ORANGE BOOK, 2020).

De igual forma, alinha-se com o 2º (segundo) princípio do componente “Governança e cultura” trazido pelo COSO (2017), de onde se extrai que a organização deve estabelecer “estruturas operacionais para atingir a estratégia e os objetivos de negócios”.

Necessário se faz assinalar, ainda, que resultou aprovada pelo CGRC/UFS, em data recente, proposta de Plano de Gestão de Riscos e Controle para o biênio 2021/2022, cuja finalidade é orientar a implementação da Política trazida pela Resolução nº 09/2021/CONSU no que tange ao gerenciamento de riscos, estabelecendo os procedimentos que conduzam ao alcance do objetivo, por meio da expressa definição de critérios, prazos, competências, responsabilidades, método e prazo de execução de cada procedimento ou etapa de implantação, com o fito de possibilitar o estabelecimento de “um processo contínuo de gestão de riscos na UFS”.

O fluxo de edição dos instrumentos normativos supramencionados segue representado na Figura 11.

**Figura 11** – Instrumentos normativos editados pela UFS e relacionados à gestão de riscos na instituição.



Fonte: Elaborada pelo Autor

Registra-se, por fim, que na esteira do preconizado pela Declaração de Posicionamento do IIA - *The Institute of Internal Auditors: As Três Linhas de Defesa no Gerenciamento Eficaz de Riscos e Controles* (2013), assim como pela Instrução Normativa Conjunta MP/CGU nº 01/2016, acerca das três camadas ou linhas de defesa, o referido Plano de Gestão de Riscos e Controle para o biênio 2021/2022 traz que resultam internalizadas da seguinte forma:

No âmbito da UFS, a **primeira linha de defesa** organizacional é representada pela atuação dos servidores e do gestor do processo organizacional. Esses atores executam as atividades e tarefas associadas aos macroprocessos institucionais.

Já a **segunda linha de defesa** é composta por várias instâncias administrativas que, de acordo com suas competências organizacionais, atuam na supervisão e no monitoramento da gestão de riscos e dos controles internos na UFS. Os arts. 24, 25, 27 e 28, todos da Resolução 09/2021/CONSU, discrimina as competências do CONSU, CONEPE, Reitoria, CIG, CGRC e da unidade executiva de gestão de riscos e controles, que são as unidades administrativas que integram a segunda linha de defesa.

Por fim, a **terceira linha de defesa** na UFS é executada pela Auditoria Interna da Instituição, de acordo com as diretrizes estabelecidas no art. 26 da Resolução 09/2021/CONSU. (UFS, 2021) (sem destaque no original).

Com base nos dados coletados e acima apresentados, observa-se uma maior movimentação normativa rumo à implantação da gestão de riscos na Universidade Federal de Sergipe a partir do ano de 2020.

#### 4.2 EVENTOS E OUTRAS INICIATIVAS DE DISSEMINAÇÃO DA GESTÃO DE RISCOS NO ÂMBITO DA INSTITUIÇÃO PESQUISADA

Da entrevista prestada pelo Coordenador do CGRC/UFS<sup>6</sup> tornou-se possível extrair que a UFS iniciou, no ano de 2020, um “processo de sensibilização” dos seus quadros acerca das nuances e importância da gestão de riscos para instituição, que vai desde a realização de eventos de capacitação – inclusive cursos regulares oferecidos pela Pró-Reitoria de Gestão de Pessoas – à publicação de vídeo informativo por meio do seu canal na plataforma Youtube, o qual apresenta, de

---

<sup>6</sup> Conforme Portaria nº 619/GR/UFS, de 20 de maio de 2021.

maneira didática, os aspectos gerais da gestão de riscos e sua importância para a instituição.

Assim, compulsando os portais de internet da UFS voltados ao tema deste trabalho, pôde-se observar um esforço tanto do Comitê de Gestão de Riscos e Controles (CGRC) quanto do Comitê de Integridade em disseminar conhecimento acerca da gestão de riscos por toda a estrutura da UFS, no afã de familiarizar os servidores e demais envolvidos com o tema, o que se coaduna com o 5º (quinto) princípio do elemento “Governança e cultura” trazido pelo COSO (2017), ao propor que “a organização tem o compromisso de formar capital humano de acordo com a estratégia e os objetivos de negócios”, por meio de ações que visem atrair, desenvolver e reter pessoas capazes.

Neste contexto, verifica-se que no dia 21/07/2020 fora promovido pelo Comitê de Integridade (que até então comportava também as atribuições do CGRC) a palestra “Gestão de Riscos no Setor Público: responsabilidade de todos?”, ministrada pelo servidor público Rodrigo Fontenelle, auditor de carreira da CGU, bem como o curso denominado “Capacitação em Gestão de Riscos: Governança e Integridade”, ministrado pelas professoras Roberta Codignoto e Vivian Nicele nos dias 25 e 27/08 e 01/09/2020, cujo objetivo foi “apresentar os conhecimentos necessários para que gestores e servidores, de qualquer área de formação, façam análise de riscos, contribuindo para a implantação e manutenção de um sistema de gerenciamento de riscos adequado e eficaz”.

Por sua vez, o já instituído CGRC promoveu, nos dias 21, 22, 26 e 27/10/2020, o curso “Oficina Online de Gestão de Riscos Aplicadas as IFES”, ministrado com carga horária de 16 (dezesesseis) horas pelo servidor público Tiago de Alencar Viana, Coordenador de Transparência, Governança e Gestão de Riscos da UFCA – Universidade Federal do Cariri, pelo qual foram apresentados aos servidores de diversos níveis da estrutura organizacional os conceitos elementares da gestão de riscos, além de alguns *framework* aplicáveis ao gerenciamento de tais eventos em instituições federais de ensino superior.

Mais recentemente, no período de 27 a 29/07/2021, o CGRC fez divulgar entre os servidores da UFS o evento intitulado “I Ciclo de Palestras sobre Gestão de Riscos do Forplad”, promovido pela coordenação do FORPLAD - Fórum Nacional de Pró-Reitores de Planejamento e de Administração das Instituições Federais de

Ensino Superior e apresentado por meio da plataforma Youtube, evento no qual foram tratados diversos temas relacionados à gestão de riscos em instituições públicas, dentre eles: Riscos Estratégicos na Administração Pública: o caso de Minas Gerais; Alinhamento da gestão de riscos nos três níveis organizacionais (Estratégico, tático e operacional); Sistema GERIFES: visão geral; e Aspectos gerais e operacionais do Sistema ForRisco.

Tais iniciativas vão ao encontro dos ensinamentos de Hill e Dinsdale (2003, p. 13), quando ressaltam o caráter humano da gestão de riscos, sustentando que os riscos, além de atrelados à probabilidade, também são produtos de “contextos culturais, sociais e políticos que afetam as reações e percepções das pessoas diante de eventos incertos”, oportunidade na qual destacam a essencialidade do servidor público para uma gestão de riscos que se pretenda eficaz.

Por fim, há ainda que se destacar como iniciativa de relevo a edição da Portaria nº 555/GR/UFS, de 29 de Julho de 2020, que instituiu o Grupo de Trabalho para mapeamento dos processos da Universidade Federal de Sergipe, na esteira do que preceitua o Referencial Básico de Gestão de Riscos do TCU, ao esclarecer que objetiva a atividade coletar informações acerca do fluxo dos processos organizacionais da instituição, com vistas à elaboração de “representação gráfica da sequência de atividades que compõem um processo, fornecendo uma visão dos fluxos operacionais do trabalho”, inclusive identificando “os agentes envolvidos, os prazos, o fluxo de documentos, o processo decisório”, dentre outros aspectos, de acordo com o nível de detalhamento que se pretenda alcançar (TCU, 2018, p. 151/152).

#### 4.3 DIAGNÓSTICO SITUACIONAL

Seguindo o roteiro estabelecido pelo Quadro 4 - Objetivos específicos, categorias de análise e elementos de análise, assim como visando à obtenção de resposta para a questão de pesquisa que objetiva conhecer “o estágio atual de implantação da gestão de riscos na instituição pesquisada”, realizou-se entrevista com o Coordenador do CGRC/UFS, que assim respondeu a cada uma das questões formuladas no Apêndice B, de modo a trazer elucidativos dados para a presente pesquisa, conforme adiante aludidos.

De início, o entrevistado expressa sua compreensão de que “a Gestão de Riscos na UFS está em fase intermediária”, ressaltando a aprovação da Política de Gestão de Riscos, do Plano de execução (Plano de Gestão de Riscos 2021/2022) e da “Metodologia base para a operacionalização das ações”, instrumentos normativos que, como visto em item antecedente, cuidam, dentre outros aspectos, de traçar objetivos e definir conceitos, metodologias e planejamento de execução inerentes ao gerenciamento de riscos da instituição.

Tal estágio encontra consonância com o que preceitua o segundo elemento apresentado pela metodologia COSO (Estratégia e definição de objetivos), o qual carrega como princípios a análise do contexto organizacional, a definição do apetite a risco, a avaliação de estratégias e alternativas e, por fim, a formulação dos objetivos, e vincula a esta “fase” a premissa de que “estratégia e definição de objetivos atuam juntos no processo de planejamento estratégico”, de modo que “o apetite a risco é estabelecido e alinhado com a estratégia” assim como “os objetivos de negócios colocam a estratégia em prática e, ao mesmo tempo, servem como base para identificar, avaliar e responder aos riscos” (COSO, 2017).

Registra, ainda, o entrevistado, que o início da caminhada rumo à efetiva implementação da gestão de riscos na UFS se deu com o mapeamento de “alguns processos na PROPLAN e no Gabinete do Reitor, além de projetos como a LGPD”, ao passo que se encontra em “andamento o mapeamento de macroprocessos ligados a aquisições, gestão de pessoas e gestão da integridade”, o que reflete o início de uma imersão no terceiro elemento (Performance) apontado pela metodologia COSO (2017), cujos princípios indicam que a organização deve identificar “os riscos que impactam a execução da estratégia e os objetivos de negócios”, avaliar a severidade do risco, priorizar os riscos como base para a seleção das respostas a eles, identificar e selecionar respostas aos riscos e, por fim, adotar e avaliar uma visão consolidada do portfólio de riscos.

Acerca das principais metodologias adotadas na estruturação da gestão de riscos da instituição, o entrevistado esclarece que:

A base metodológica utilizada na gestão de riscos da UFS é amparada sobretudo nas diretrizes estabelecidas pela Norma Técnica ABNT NBR ISO 31000:2018 com apoio da ABNT NBR ISO/IEC 31010:2012 que “fornece orientações sobre a seleção e aplicação de técnicas sistemáticas para o processo de avaliação de riscos”.

Além disso, foram utilizadas algumas diretrizes da metodologia COSO ERM (COSO II), com destaque para a gestão de riscos nos objetivos estratégicos da Instituição e a introdução do conceito de apetite a risco, demonstrando a importância do estabelecimento do nível de riscos que a Instituição está disposta a aceitar em suas operações.

Esclarece, ademais, a influência da Instrução Normativa Conjunta MP/CGU 01/2016, além das publicações “Manual de Gestão de Integridade, Riscos e Controles Internos da Gestão” (2017), desenvolvido pelo então Ministério do Planejamento Desenvolvimento e Gestão; “Metodologia de Gestão de Riscos” (2021), elaborado pelo Ministério da Transparência e Controladoria Geral da União (CGU); “Gestão de Riscos: Avaliação de Maturidade” (2018), desenvolvido pelo Tribunal de Contas da União; e “ForRisco: gerenciamento de riscos em instituições públicas na prática” (2018), de lavra do Fórum Nacional dos Pró-Reitores de Planejamento e Administração das Instituições Federais de Ensino Superior (FORPLAD).

Das metodologias e trabalhos utilizados para formulação da estrutura documental da gestão de riscos na UFS se pôde extrair que a instituição buscou lastrear-se não apenas em modelos de ampla aplicabilidade e reconhecida consistência, mas também em manuais e obras científicas voltadas especificamente para instituições públicas, o que denota uma preocupação da Alta Administração com a formulação de uma base normativa consistente e alinhada com os preceitos capazes de conduzir a uma eficaz gestão de riscos, consoante apontado no referencial teórico do presente estudo.

No que pertine ao envolvimento do pessoal com a gestão de riscos na instituição, explana o entrevistado que ocorre de acordo com o advento do instrumento em cada “unidade/projeto”, oportunidade na qual “é designada uma equipe para o mapeamento e gerenciamento de riscos, composta por agentes de diferentes níveis de responsabilidades e de conhecimentos dentro da unidade” - equipe essa que deverá receber capacitação e treinamento em gestão de riscos visando à execução do trabalho -, momento no qual “deverá ser identificado o gestor do processo organizacional, o servidor responsável pelo monitoramento dos riscos e pela efetividade das medidas de controle sugeridas (proprietário do risco)”.

Sobre a realização de cursos e/ou eventos de qualificação de pessoal voltados ao tema gestão de risco, o entrevistado elucida que a instituição iniciou, no



ano de 2020, “um processo de sensibilização e capacitações visando ao estabelecimento da Política de Gestão de Riscos com a metodologia adequada à realidade da Universidade”, que envolve os eventos de capacitação já mencionados no item 4.2 do presente estudo.

No mais, ressaltou a existência de cursos regulares de capacitação oferecidos aos servidores com a temática gestão de riscos, disponibilizados no Catálogo de Cursos da UFS e ofertados pela PROGEP, arrematando que o conjunto de eventos realizados “têm permitido à Universidade a definição efetiva do seu processo de gestão de riscos”.

Neste particular, a postura da instituição se coaduna com os pressupostos apontados por Hill e Dinsdale (2003, p.17), quando defendem que “nenhum servidor público inovador pode evitar decisões que envolvam riscos”, de modo que “todos devem possuir as habilidades e competências necessárias para gerenciar” eventos incertos.

Ainda, questionado sobre as maiores dificuldades enfrentadas até o momento para implantação da gestão de riscos na UFS, o entrevistado manifesta compreensão no sentido de que “a gestão de riscos é uma temática que exige o aprofundamento do conhecimento e a sensibilização de servidores para que se possa ter maior efetividade”, enfatizando que, a despeito da realização de diversos cursos e eventos ofertados e “do apoio da alta gestão, ainda há uma necessidade de maior sensibilização sobre o tema” entre os servidores da instituição.

A dificuldade apontada na resposta supra tratada reflete uma maior necessidade de exame do ambiente interno da instituição, pois, conforme a norma ABNT ISO 31000:2018, “ao conceber a estrutura para gerenciar riscos, convém que a organização examine e entenda seus contextos externo e interno”, referindo-se o contexto interno também à “cultura da organização” e às “capacidades entendidas em termos de recursos e conhecimento”, nas quais se inclui o fator “pessoas”. Em semelhante direção, Assi (2012) esclarece que no ambiente interno estarão localizados os pontos fortes e fracos da organização, resultantes da sua estratégia e representados, dentre outros, por seus recursos físicos, humanos e financeiros.

Por fim, perguntado acerca da possível identificação de efeitos ou resultados da implantação da gestão de riscos para a estratégia e objetivos da instituição, o entrevistado aduziu que “no projeto de implantação da LGPD na UFS já se percebeu

que os objetivos são alcançados de uma melhor forma quando se tem o acompanhamento dos riscos levantados”, sem deixar de registrar, no entanto, que “a gestão de riscos é algo continuado o que exige certo tempo para sua maturação”, o que se coaduna com o preceito de “melhoria contínua” trazido pela ABNT ISO 31000:2018, o qual sugere que, “à medida que lacunas ou oportunidades de melhoria pertinentes são identificadas, convém que a organização desenvolva planos e tarefas e os atribua àqueles responsabilizados pela implementação”.

Assim, das respostas obtidas com a entrevista roteirizada no Apêndice B, juntamente com os dados levantados nos itens 4.1 e 4.2 do presente estudo foi possível extrair que a UFS tem conseguido evoluir no que se refere à normatização do seu processo de implantação da gestão de riscos, o que faz se utilizando de metodologias consolidadas e altamente recomendadas para a gestão de riscos em organizações de qualquer natureza - a exemplo da Norma Técnica ABNT NBR ISO 31000:2018 e do COSO ERM -, além de instruções normativas e manuais emanados dos Órgãos de Controle (sobretudo o TCU), assim como orientações de entidades ligadas a gestores de instituições federais de ensino superior, sendo exemplo a publicação “ForRisco: gerenciamento de riscos em instituições públicas na prática”, estas últimas próprias para instituições públicas.

No que diz respeito ao envolvimento do quadro de pessoal com a gestão de riscos, nota-se que não ocorre com o mesmo dinamismo empregado para a normatização, sobretudo porque o mapeamento dos processos organizacionais ainda se encontra em fase embrionária, o que se extrai da análise conjunta das respostas às questões 1 e 3 do Apêndice B, de modo que a participação em maior grau do quadro de pessoal ocorrerá na medida em que haja o avanço do sobredito procedimento.

Quanto às dificuldades enfrentadas, observa-se que, mais uma vez, o envolvimento do quadro de pessoal da UFS com a gestão de riscos da instituição destoa do avançado estágio de normatização, pois, consoante explanado pelo entrevistado, a efetividade da implantação exige dos servidores um profundo conhecimento dos processos organizacionais e um comprometimento com as boas práticas da gestão de riscos, de modo que, embora tenham sido empreendidas inúmeras iniciativas nesse sentido – conforme se extrai dos tópicos 4.1 e 4.2 –, ainda se verifica “uma necessidade de maior sensibilização sobre o tema”.

Por fim, a resposta à Questão 6 demonstra que a instituição já consegue vislumbrar resultados positivos com a implantação da gestão de riscos, verificados em projeto onde o mapeamento dos processos organizacionais e a consequente identificação dos riscos incidentes sobre eles já se encontram maturados.

Dessa forma, dos dados coletados e apresentados no presente tópico, assim como nos anteriores (4.1 e 4.2), se extrai que a implantação da gestão de riscos na UFS se encontra em avançado estágio no que pertine à edição de instrumentos normativos relativos ao tema, e que visam regulamentar a implementação e execução dos procedimentos propostos, mas, por outro lado, ainda se encontra em estágio incipiente no que diz respeito à disseminação da cultura da gestão de riscos entre os servidores e unidades da instituição, o que pode justificar o estágio “intermediário” apontado pelo entrevistado em sua exposição inicial.

No mesmo sentido, observa-se um esforço da Alta Administração no afã de propalar entre os servidores dos mais diversos níveis da estrutura organizacional conhecimentos acerca do tema em estudo, como forma de incutir na cultura organizacional a importância da gestão de riscos para a estratégia e o alcance dos objetivos da instituição, antes mesmo da efetiva implantação dos procedimentos, o que faz por meio dos diversos eventos ofertados e demais iniciativas mencionadas nos tópicos antecedentes.

Nada obstante, o exame das normativas mencionadas de partida pelo entrevistado, notadamente, do Plano de Gestão de Riscos com vigência para 2021/2022, revela que o monitoramento e controle de riscos carece de melhor detalhamento quanto às ações que serão executadas, tendo em vista que limita-se apontar para a utilização do Sistema ForRiscos, ferramenta inserida em “plataforma ofertada pelo Ministério da Educação (PlataformaFor) que integra o Plano Estratégico das Instituições Federais de Ensino (ForPDI) à gestão de riscos das Instituições” (UFS, 2021), de modo a denotar um ponto de oportunidade para formulação de proposta de contribuição.

#### 4.4 PONTO DE OPORTUNIDADE IDENTIFICADO VISANDO À FORMULAÇÃO DA PROPOSTA DE CONTRIBUIÇÃO

A resposta para a questão de pesquisa “qual o ponto de oportunidade identificado para formulação da proposta de contribuição?” deriva da análise do já mencionado Plano de Gestão de Riscos e Controle para o biênio 2021/2022, devidamente aprovado pelo CGRC/UFS, e cuja finalidade é orientar a implementação da Política trazida pela Resolução nº 09/2021/CONSU no que tange ao gerenciamento de riscos, estabelecendo os procedimentos que conduzam ao alcance do objetivo, por meio da expressa definição de critérios, prazos, competências, responsabilidades, método e prazo de execução de cada procedimento ou etapa de implantação, com vistas a estabelecer um processo de gestão de riscos que se apresente viável, adequado e, sobretudo, contínuo.

Da análise do referido plano se pode extrair a mensagem de que uma gestão de riscos que se pretenda eficaz tem como ponto de partida o mapeamento dos processos organizacionais e a criteriosa identificação dos riscos e oportunidades que sobre eles incidam, com o fito de que sejam devidamente monitorados e controlados por meio de procedimentos predefinidos.

De igual forma, do exame do sobredito Plano de Gestão de Riscos e Controle para o biênio 2021/2022, constante do Anexo A, é possível concluir que as ações de monitoramento e controle de riscos resultam nele tratado de forma breve, o que reflete uma oportunidade de contribuição por meio do presente estudo, ainda mais se considerado que uma revisão no referido planejamento deverá ser procedida antes de expirado o prazo ao qual se refere (2021-2022).

Acerca das ações de monitoramento e controle de riscos, traz o referido Plano de Gestão de Riscos e Controle para o biênio 2021/2022:

#### **7. SISTEMA DE MONITORAMENTO DE RISCOS**

A UFS adotará o Sistema ForRiscos como ferramenta tecnológica para o monitoramento e o controle dos riscos da Instituição. Esta ferramenta é parte de uma plataforma ofertada pelo Ministério da Educação (PlataformaFor) que integra o Plano Estratégico das Instituições Federais de Ensino (ForPDI) à gestão de riscos das Instituições.

A adesão ao sistema contemplará o acompanhamento dos riscos e controles previstos nesse plano e permitirá aos setores o contínuo monitoramento dos riscos tendo em vista ser uma plataforma de livre acesso aos servidores cadastrados. A comunicação e a consulta também

serão permitidas pela geração de relatórios gerenciais disponíveis na própria ferramenta.

Nesse sentido, observa-se que a adoção da ferramenta tecnológica ForRiscos se coaduna com o 18º (décimo oitavo) princípio trazido pela metodologia COSO ERM (2017, p. 10), pelo qual preceitua que “a organização maximiza a utilização dos sistemas de informação e tecnologias existentes na entidade para impulsionar o gerenciamento de riscos corporativos”.

Por outro lado, ao tratar do tema em análise, a norma NBR 31000:2018 propõe que “o monitoramento contínuo e a análise crítica periódica do processo de gestão de riscos e seus resultados sejam uma parte planejada do processo de gestão de riscos, com responsabilidades claramente estabelecidas”, com vistas à incorporação de tais resultados “em todas as atividades de gestão de desempenho, medição e relatos da organização” (ABNT, 2018, p. 16), o que confirma a importância de um maior detalhamento das ações de monitoramento e controle de riscos e, por consequência, corrobora a conveniência da proposta formulada, ante a constatação acima demonstrada.

Assim, consiste a proposta de contribuição pretendida no presente trabalho na elaboração de um projeto de “Plano de Monitoramento e Controle de Riscos” capaz de ser incorporado no item 7 do Plano de Gestão de Riscos e Controle da UFS, com o fito de apresentar as atividades e procedimentos previstos na publicação “Metodologia de Gestão de Riscos da UFS”, elaborada pelo Comitê de Gestão de Riscos e Controles – CGRC da instituição e aprovada em 18/05/2021, no que se refere às ações de monitoramento e controle de riscos (Item 2, Etapa 5).

Para tanto, seguindo as diretrizes metodológicas traçadas no item 3 deste trabalho, por meio de entrevistas semiestruturadas, buscou-se conhecer estruturas de gestão de riscos implantadas em outras instituições públicas federais de ensino superior, no que se refere ao ponto de oportunidade identificado, com o intuito de coletar elementos capazes de subsidiar a elaboração da proposta, conforme adiante tratado.

#### 4.5 COLETA DE DADOS JUNTO A OUTRAS IFES VISANDO À FORMULAÇÃO DA PROPOSTA DE CONTRIBUIÇÃO

Para consecução do objetivo em comento e consequente obtenção de resposta para a questão de pesquisa “como se apresentam as estruturas de gestão de riscos implantadas em outras instituições públicas federais de ensino superior, no que se refere ao ponto de oportunidade identificado?”, foram selecionadas duas Instituições Federais de Ensino Superior, sendo elas a UFCA-Universidade Federal do Cariri e a UFERSA – Universidade Federal Rural do Semi-Árido ambas localizadas na região Nordeste do Brasil, mais precisamente nos estados de Ceará e Rio Grande do Norte, respectivamente.

Conforme se extrai do Roteiro de Entrevistas constante do Apêndice C, foram formuladas 04 (quatro) perguntas - todas relacionadas ao monitoramento e controle de riscos na instituição pesquisada -, as quais resultaram devidamente respondidas pelos entrevistados, que doravante seguem identificados apenas como Entrevistado 1 e Entrevistado 2.

De partida, o Entrevistado 1 esclarece que o Plano de Gestão de Riscos da instituição que representa, a exemplo do que ocorre na UFS, englobará o plano de monitoramento e controle de riscos, e está em fase de conclusão, por meio de trabalho conjunto desenvolvido entre a Coordenadoria de Transparência, Governança e Gestão de Riscos e a Coordenadoria de Gestão de Projetos e Processos, porquanto, conforme enfatizou, o gerenciamento de riscos da instituição ocorre de forma alinhada com o gerenciamento de processos organizacionais.

Ressaltou, no entanto, que a despeito do referido plano ainda carecer de finalização, o gerenciamento de riscos já é realizado em alguns setores da instituição por meio de planilha documentadora de processos e riscos, pela qual é realizado o monitoramento e controle de tais eventos, englobando causa, consequência, matriz de probabilidade e impacto e as ações de controle estabelecidas para cada um dos riscos identificados.

Acerca da planilha documentadora de riscos mencionada pelo Entrevistado 1, o já conhecido Referencial Básico de Gestão de Riscos elaborado pelo TCU, ao tratar da “Documentação da identificação e análise de riscos”, aduz que no registro de riscos a documentação da identificação e análise de tais eventos deve conter

elementos suficientes para apoiar a adequada gestão de riscos, incluindo pelo menos:

o registro dos riscos identificados e analisados em sistema, planilha ou matriz de avaliação de riscos, descrevendo os componentes de cada risco separadamente com, pelo menos, suas causas, o evento e as consequências e/ou impactos nos objetivos identificados na etapa de estabelecimento do contexto (TCU, 2018, p. 110).

Ainda, registrou a existência de uma segunda planilha (planilha setorial), pela qual os setores resumem os planos de ação relacionados aos controles estabelecidos, com vistas ao acompanhamento do próprio setor envolvido e da Coordenadoria de Transparência, Governança e Gestão de Riscos.

Além das planilhas mencionadas, relatou o Entrevistado 1 que a Auditoria Interna da instituição faz um trabalho contínuo de acompanhamento, monitoramento e controle dos riscos, por meio da edição de relatórios que contemplam recomendações e orientações que são constantemente analisadas tanto pelo setor envolvido quanto pela Coordenadoria de Transparência, Governança e Gestão de Riscos da instituição.

Por sua vez, acerca do mesmo aspecto, o Entrevistado 2 respondeu que as ações de monitoramento e controle de riscos da instituição, de forma geral, integram a sua Política de Gestão de Riscos, que contempla o ordenamento normativo incidente sobre as instituições públicas federais, bem como designa a Pró-Reitoria de Planejamento como unidade responsável pelo processo de implementação da gestão de riscos.

Registrou o Entrevistado 2 que, após a definição da responsabilidade pela implantação, buscou-se realizar o mapeamento dos processos organizacionais e diversas ações de capacitação tanto em mapeamento de processos quanto em gerenciamento de riscos propriamente dito, a fim de possibilitar a disseminação paulatina desse conhecimento entre todos os setores da instituição, obedecendo ao cronograma estabelecido e que leva em consideração a complexidade do tema e o seu reflexo na cultura organizacional.

Aduziu, por fim, que fora implementado um projeto piloto na Superintendência de Infraestrutura da instituição, visando ao mapeamento dos processos e à identificação, monitoramento e controle dos riscos incidentes sobre cada um deles, que serviu para identificar inconsistências e saná-las antes da implementação nos demais setores, o que vem ocorrendo de forma gradual.

A providência mencionada pelo Entrevistado 2 igualmente encontra eco no preceito de “melhoria contínua” trazido pela ABNT ISO 31000:2018, o qual, consoante já dito, sugere que “à medida que lacunas ou oportunidades de melhoria pertinentes são identificadas, convém que a organização desenvolva planos e tarefas e os atribua àqueles responsabilizados pela implementação”.

No que tange a forma envolvimento do quadro de pessoal nas ações que visam monitorar e controlar os riscos, o Entrevistado 1 esclareceu que, na instituição que se encontra vinculado, além dos servidores que desempenham suas funções na Coordenadoria de Transparência, Governança e Gestão de Riscos e na Auditoria Interna, os gestores e demais servidores lotados nas unidades onde o gerenciamento de riscos já é realizado estão diretamente envolvidos também com o monitoramento e controle de riscos.

O Entrevistado 2, por seu turno, elucidou que devido ao atual estágio de implantação, o envolvimento do quadro de pessoal está mais relacionado à participação em ações de capacitação tanto em mapeamento de processos quanto em gerenciamento de riscos propriamente dito e conscientização acerca da sua importância – sobretudo para melhoria dos trabalhos e eficiência dos processos –, assim como à designação de um responsável pelo risco em cada setor cuja implementação seja iniciada.

Arrematou citando a Pró-Reitoria de Administração e a Superintendência de Infraestrutura como exemplos de setores nos quais a identificação, o monitoramento e o controle dos riscos incidentes já estão sendo geridos e, por consequência, os servidores ali lotados diretamente envolvidos com as práticas da gestão de riscos.

Sobre as maiores dificuldades enfrentadas para o desenvolvimento das atividades previstas no plano de monitoramento e controle de riscos da instituição, o Entrevistado 1 apontou para: 1. Limitação de pessoal, pois a área de gestão de riscos não conta com a quantidade de servidores que se deseja, bem como não vislumbra possibilidade de realocação de servidores, tendo em vista se tratar de realidade enfrentada em todas as unidades da instituição; 2. Desconhecimento da gestão de riscos por parte de gestores e demais envolvidos nos processos organizacionais, situação que gera resistência, mas que vem sendo enfrentada com a adoção de medidas que visam à sensibilização do quadro de pessoal para a importância de incorporar a gestão de riscos na cultura organizacional.



No mesmo sentido, o Entrevistado 2 respondeu que: 1. De modo geral, a falta de pessoal para se dedicar exclusivamente às ações de gerenciamento de riscos - sobretudo para atuar como disseminador da cultura da gestão de riscos na organização; 2. A resistência de alguns servidores, dada a necessidade de alteração da sua rotina de trabalho e o considerável acréscimo de atribuições e responsabilidades decorrentes do imperativo de gerenciar os riscos incidentes sobre os processos nos quais atua; e 3. Dissolução, ainda que parcial, da equipe capacitada em gestão de riscos e responsável pela implementação do processo e difusão do tema, decorrente de mudança na alta gestão da instituição, de modo a gerar danosa descontinuidade nas ações de implementação.

Vale registrar que o segundo aspecto abordado pelo Entrevistado 2 (resistência de alguns servidores às atividades de gestão de riscos) corrobora o “mito” apontado pelo professor Rodrigo Fontenelle ao prefaciar a obra de Bermejo *et al.* (2019), que consiste no entendimento de alguns servidores públicos no sentido de que a gestão de riscos representa um acréscimo de trabalho, e não uma necessária mudança de cultura organizacional.

Por derradeiro, quanto às principais lições aprendidas desde o processo de elaboração do plano de monitoramento e controle de riscos até o seu estágio atual de execução, o Entrevistado 1 esclareceu que, embora o Plano de Gestão de Riscos esteja em fase de finalização, muitas das ações previstas no referido plano vêm sendo desenvolvidas, paulatinamente, desde o ano de 2017, de modo que algumas lições foram aprendidas no transcorrer do tempo, dentre elas: 1. Necessidade de, antes de dar início à execução dos procedimentos de gerenciamento propriamente dito, estruturar documentalmente (Política, Planos e etc.) toda a gestão de riscos da instituição, bem como realizar capacitações e pôr em prática projeto piloto, o que serve para evitar desalinhamento entre os níveis organizacionais, bem como outros embarços futuros. Salientou que, no caso da instituição ao qual está vinculado os exíguos prazos estabelecidos para implantação da gestão de riscos, cumulados com a necessidade de realização de outras tarefas extraordinárias, contribuíram sobremaneira para inobservância, ainda que parcial, do preceito do qual se extraiu a lição em comento; 2. Necessidade de alinhamento claro e objetivo com todos os setores envolvidos, por meio de planos de comunicação claros, oportunos e adequados entre as partes interessadas.

O Entrevistado 2, por sua vez, apontou para as seguintes lições aprendidas:

1. Que se bem conduzido, o processo de gestão de riscos como um todo tende a proporcionar resultados positivos que vão da redução de gastos e retrabalho, à melhoria da qualidade de trabalho do servidor e melhoria dos resultados operacionais e acadêmicos da instituição, derivados do melhor conhecimento dos processos desenvolvidos; 2. Que é imprescindível a conscientização de todos os servidores envolvidos acerca da importância da obtenção dos resultados antes mencionados, bem como no sentido de que as mudanças decorrentes dessa nova realidade, embora desafiadoras, visam, antes de tudo, trazer melhorias em todos os aspectos e, principalmente, que a implementação não deve ser vista apenas como o cumprimento de uma exigência legal, mas sim como “uma busca de aperfeiçoamento de processos”.

Assim, das respostas às questões formuladas se tornou possível extrair que ambas as instituições pesquisadas se encontram em estágio inicial da implementação da gestão de riscos e, embora ainda não possuam em vigência um Plano que especifique as ações de monitoramento e controle de riscos, já desenvolvem atividades de gestão de riscos em setores específicos, tendo como perspectiva a disseminação do processo para toda a instituição, situações nas quais em muito se assemelham ao estágio ora vivenciado pela Universidade Federal de Sergipe.

Ademais, a coleta dos dados em comento apontou para a viabilidade do uso, ainda que não isolado, da planilha documentadora de processos e riscos que, conforme o Entrevistado 1, se mostra eficiente para monitorar e controlar riscos.

## 5 FORMULAÇÃO DA PROPOSTA

Resultado do diagnóstico situacional realizado na instituição objeto do estudo, a proposta formulada lastreia-se no referencial teórico colhido na primeira fase da pesquisa e incorpora lições vivenciadas pelas duas IFES pesquisadas, de modo a contar com subsídios extraídos das entrevistas realizadas, assim como da análise documental procedida.

O escopo da proposta é o de conferir nova redação ao item “7. SISTEMA DE MONITORAMENTO DE RISCOS” do Plano de Gestão de Riscos da UFS (2021/2022) - aprovado pelo CGRC/UFS em outubro de 2021 -, com o fito de incorporar ao referido plano o detalhamento nela sugerido, dada a brevidade com a qual o tema surge abordado no sobredito documento, conforme pode ser observado no Anexo A do presente estudo.

Assim, visa incrementar o já aprovado Plano de Gestão de Riscos da UFS (2021/2022) no tocante ao monitoramento e controle de riscos (item 7) ou, ainda, servir de base para revisão que se avizinha, especificamente quanto ao aspecto abordado, tendo em vista a vigência atribuída para o texto atual.

A proposta de Plano de Monitoramento e Controle de Riscos segue adiante delineada, juntamente com as referências bibliográficas que lastream a formulação, assim como o seu Apêndice I, e, destacada por quadro na íntegra (p. 114 a 123), carrega em seu bojo os termos que propõe sejam incorporados ao item 7 do mencionado Plano de Gestão de Riscos ou, ainda, considerados na próxima revisão pela qual haverá de passar o teor do referido documento.

### PLANO DE MONITORAMENTO E CONTROLE DE RISCOS

O Plano de Monitoramento e Controle de Riscos é delineado com o fim de apresentar as atividades e procedimentos previstos na publicação “Metodologia de Gestão de Riscos da UFS”, elaborada pelo Comitê de Gestão de Riscos e Controles da UFS – CGRC e aprovada em 18/05/2021, no que se refere às ações de monitoramento e controle de riscos (Item 2, Etapa 5).

Para tanto, parte do princípio que monitorar e controlar riscos constitui a etapa de “verificação, supervisão, observação crítica ou identificação da situação,

executadas de forma contínua, a fim de identificar mudanças em relação ao nível de desempenho requerido ou esperado” pela instituição em relação ao processo de gestão de riscos implementado (TCU, 2018), por meio do desenvolvimento de ações “associadas à sistematização e à manutenção dos ganhos obtidos com as ações de resposta ao risco” (PADOVEZE, 2008).

Nesse sentido, conforme Padoveze (2008), mostra-se conveniente considerar monitoramento e controle de riscos sobre dois diferentes prismas: o **monitoramento** deve ser considerado como o conjunto de ações de acompanhamento contínuo do desempenho obtido com o processo implantado, incorporado às atividades cotidianas e enraizado na cultura da organização, de modo a permitir rápida identificação e resposta às condições mutantes, sendo exemplos “atividades regulares de gerenciamento e supervisão, análises de variância, testes de stress, comparações, reconciliações e outras ações de rotina”; e o **controle**, por sua vez, envolve ações sistemáticas de controle, sejam manuais ou computadorizadas, a exemplo de políticas, procedimentos, auditorias e relatórios (internos e externos).

A norma NBR 31000:2018, por seu turno, aduz que o objetivo do monitoramento e análise crítica dos riscos é aprimorar “a qualidade e eficácia da concepção, implementação e resultados do processo” de gestão de riscos da instituição, que deve envidar esforços para que a ação ocorra de forma contínua e constitua uma etapa planejada e incidente sobre todos os estágios do processo de gerenciamento de riscos, na qual as responsabilidades devem estar claramente estabelecidas (ABNT, 2018, p. 16).

Ainda conforme a mesma norma, monitoramento e análise crítica dos riscos “incluem planejamento, coleta e análise de informações, registro de resultados e fornecimento de retorno”, resultados esses que devem “ser incorporados em todas as atividades de gestão de desempenho, medição e relatos da organização” (ABNT, 2018, p. 16).

Assim, conforme previsto na já mencionada “Metodologia de Gestão de Riscos da UFS”, o monitoramento e controle do processo de gestão de riscos da instituição (Etapa 5) se dará, principalmente, por meio do módulo pertinente disponibilizado pelo Sistema ForRisco, além da ferramenta Planilha Documentadora de Processos e Riscos, auxiliada pela emissão de relatórios de controle.

Sobre a utilização do Sistema ForRisco, registra-se que as suas funcionalidades, apresentadas por Bermejo *et al.* (2019, p. 179/180) e adiante reproduzidas, serão capazes de proporcionar um conjunto de ações necessárias à adequada gestão de riscos na UFS, sobretudo naquilo que pertine à etapa monitoramento, dentre elas:

- Criar Plano de Gestão de Riscos: refere-se ao projeto ou conjunto de medidas estabelecidas como guia prático para identificar, administrar e monitorar os riscos;
- Avaliar e classificar a tipologia do risco: a classificação está organizada em operacional, legal, imagem/reputação do órgão e financeiro/orçamentário;
- Definir o grau do risco: refere-se a uma classificação, pelo usuário, do posicionamento ou nível do risco em um determinado momento. Recomenda-se que o risco seja classificado em crítico, alto, moderado e pequeno;
- Estabelecer ações corretivas: são as atividades e as práticas que visam à execução da tomada de decisão para corrigir os incidentes;
- Permitir níveis de acesso diferentes: a ferramenta possibilita hierarquizar e controlar o acesso dos usuários por seus gestores;
- Reconhecer ameaças ou oportunidades atreladas aos riscos: ameaças são situações de incerteza, externas e/ou internas às organizações, que podem atrapalhar ou impedir o alcance dos objetivos definidos; oportunidades são situações ou circunstâncias favoráveis, externas e/ou internas às organizações, que podem ser aproveitadas e afetar positivamente o alcance dos objetivos;
- Definir periodicidade da análise: refere-se aos intervalos regulares em que o risco deverá ser analisado. O sistema oferece os seguintes intervalos: diário, semanal, quinzenal, mensal, bimestral, trimestral, semestral e anual;
- Identificar causas e consequências dos riscos: a causa é considerada o princípio, a razão, o motivo ou a origem para que o risco aconteça; a consequência é tudo aquilo que foi produzido (ou poderá ser produzido) diante dos riscos identificados; efeitos ou resultados dos riscos;
- Desenvolver matriz de riscos: dispositivo para indicar, de maneira ordenada, a classificação dos riscos proposta pelo usuário a partir do grau do risco;
- Estabelecer ações de prevenção; e,
- Registrar data e horário de edição das informações.

O desenvolvimento e implantação da Planilha Documentadora de Processos e Riscos, por sua vez, constitui etapa subsequente ao mapeamento dos processos que, conforme o Referencial Básico de Gestão de Riscos elaborado pelo TCU, é definido como a “representação gráfica da sequência de atividades que compõem um processo, fornecendo uma visão dos fluxos operacionais do trabalho”, inclusive identificando “os agentes envolvidos, os prazos, o fluxo de documentos, o processo decisório”, dentre outros aspectos, de acordo com o nível de detalhamento que se pretenda alcançar (TCU, 2018, p. 151/152).

Da definição supra se extrai que o mapeamento dos processos da organização permite o conhecimento pleno do passo a passo necessário para o desenvolvimento de cada atividade ou processo, possibilitando, também, a identificação dos eventos incertos incidentes sobre eles, bem como o potencial que cada evento risco tem de afetá-los - seja negativamente (ameaça) ou positivamente (oportunidade) -, de modo a permitir sejam tais eventos elencados no Mapa de Riscos visando ao devido monitoramento e controle de cada um deles.

O Mapa de Riscos será delineado em planilha documentadora e/ou módulo equivalente no Sistema ForRisco, levando em conta a identificação de cada objetivo, processo e/ou atividade sobre os quais incidam riscos, deles devendo constar, sem prejuízo de outros aspectos que se revelem necessários: Unidade(s) Responsável(eis); Objetivo/Processo/Atividade; Evento Risco; Categoria do Risco; Causa do Risco; Probabilidade de Ocorrência; Impacto Causado; Proprietário do Risco; Informações e Comunicações Necessárias; e Medida de Tratamento do Risco/ Ações de Controle - consoante ilustrado na planilha constante do Apêndice I - que será alimentada tendo por base a categorização de riscos e a matriz de classificação de riscos definidas pela Metodologia de Gestão de Riscos da UFS.

Acerca dos elementos constantes da Planilha Documentadora de Processos e Riscos, apresenta-se uma breve descrição de cada um deles:

- Unidade Responsável - Setor onde se desenvolve a atividade ou o procedimento sobre o qual incide o evento incerto;
- Objetivo/Processo/Atividade - Escopo almejado, ação ou procedimento a ser desenvolvido;

- Evento Risco - Conforme a norma ABNT ISO 31000/2018, trata-se do “efeito da incerteza nos objetivos”, cujas consequências podem ser positivas, negativas ou ambas, e “que pode abordar, criar ou resultar em oportunidades e ameaças”;
- Categoria do Risco - Categorização do risco de acordo com o nível organizacional (estratégico, tático ou operacional) onde está inserido o objetivo, processo ou atividade na qual incide;
- Causa do Risco - Ação ou omissão capaz de deflagrar a ocorrência do evento incerto;
- Probabilidade de Ocorrência - Expectativa de ocorrência do risco, de acordo com o nível previamente definido;
- Impacto Causado - Expectativa dos efeitos do risco, de acordo com o nível previamente definido;
- Proprietário do Risco - “Gestor de processo organizacional, servidor responsável pelo monitoramento dos riscos e pela efetividade das medidas de controle sugeridas” (UFS, 2021) em relação a cada risco identificado;
- Informações e Comunicações Necessárias - Conjunto de informações que envolvem o objetivo/processo/atividade, dentre elas a (in)existência de normativos incidentes, manuais ou controles específicos; e
- Medida de Tratamento do Risco/ Ações de Controle - Delineamento das ações que visam evitar, mitigar ou potencializar a ocorrência do evento incerto (risco ou oportunidade), além de reduzir ou tolerar seu impacto (TCU, 2018).

De acordo com a publicação “ForRisco: gerenciamento de riscos em instituições públicas na prática”, o processo de identificação e mapeamento garante a compreensão das atividades sobre as quais incidem riscos a uma unidade organizacional específica - porquanto as unidades são também as responsáveis pela etapa de identificação -, de modo a permitir sejam os riscos identificados atribuídos ao chamado “proprietário do risco”, que será o “responsável por assegurar que o risco seja monitorado, gerenciado e tratado adequadamente” (BERMEJO *et al.*, 2019, p. 135).

Com tal afirmação, a publicação ressalta o caráter descentralizado da responsabilidade pela gestão dos riscos, que não deve, em nenhuma hipótese, ficar restrita aos membros do Comitê de Gestão de Riscos e Controles da UFS – CGRC, mas sim ser distribuída entre os diversos atores envolvidos nos processos

organizacionais mapeados, conforme ilustrado no Quadro 1, adaptado da mencionada obra.

**Quadro 1 – Atores e distribuição de responsabilidades de monitoramento e controle de riscos**

<b>Ator/Responsável</b>	<b>Responsabilidades</b>
CGRC	Elaborar o Plano de Gestão de Riscos, do qual constará o Plano de Monitoramento e Controle de Riscos; Realizar a gestão do Plano de Gestão de Riscos, inclusive quanto ao monitoramento e controle; Determinar medidas mitigadoras, monitorar ações e comunicar situações, por meio de relatórios de controle; Revisar, de acordo a periodicidade predefinida, o Plano de Monitoramento e Controle de Riscos.
Reitor	Garantir a continuidade e o aperfeiçoamento da Política de Gestão de Riscos, de modo a assegurar o sistemático monitoramento e controle dos riscos identificados.
Pró-Reitores	Monitorar, no âmbito de suas Pró-Reitorias, os riscos mapeados; Comunicar sobre situações que envolvem risco, por meio de relatórios de controle, e aplicar medidas de mitigação necessárias.
Coordenadores e Chefes de Unidades	Monitorar, no âmbito de suas unidades, os riscos mapeados; Comunicar sobre situações que envolvem risco e aplicar medidas de mitigação necessárias.
Servidores em geral	Monitorar, nos seus respectivos âmbitos de atuação, os riscos mapeados; Comunicar sobre situações que envolvem risco e aplicar medidas de mitigação necessárias.
Servidor Designado como Proprietário do Risco	Monitorar os riscos sob sua responsabilidade e zelar pela efetividade das medidas de controle implementadas.

Fonte: Adaptado de Bermejo *et al.* (2019).

Consoante trazido pela sobredita Metodologia de Gestão de Riscos da UFS, o mapeamento deverá ser realizado por uma equipe “composta por agentes de diferentes níveis de responsabilidades e de conhecimentos dentro da unidade”, com vistas à identificação do “gestor de processo organizacional, servidor responsável pelo monitoramento dos riscos e pela efetividade das medidas de controle sugeridas (proprietário do risco)”.

Assim, de acordo com a atribuição de responsabilidades apontada no Quadro 1, os responsáveis deverão acompanhar o comportamento dos riscos identificados e vinculados à sua atuação, sem deixar de sugerir intervenções sempre que se mostrar necessário. Para aferição e acompanhamento do monitoramento e controle implementados dentro da periodicidade definida, a UFS fará uso da ferramenta 5W2H – que, conforme Vieira e Barreto (2019, p. 144), é uma das “técnicas mais conhecidas para gerenciamento de atividades” –, de modo a contemplar os aspectos da etapa apontados no Quadro 2:



**Quadro 2 – Ferramenta 5W2H**

O que fazer / Como fazer	Definição
What	O que será feito?
Why	Por que será feito?
Who	Por quem será feito?
When	Quando será feito?
Where	Onde será feito?
How	Procedimento ou forma de realização
How Much	Investimento/Tempo envolvidos

Fonte: Adaptado de Bermejo *et al.* (2019).

No que se refere aos relatórios de controle a serem utilizados, a NBR 31000:2018 propõe que não apenas o processo de gerenciamento de riscos da instituição, mas também seus resultados sejam devidamente documentados por meios apropriados, com vistas aos seguintes propósitos: a) comunicar atividades e resultados de gestão de riscos em toda a organização; b) fornecer informações para a tomada de decisão; c) melhorar as atividades de gestão de riscos; d) auxiliar a interação com as partes interessadas, incluindo aquelas com responsabilidade e com responsabilização por atividades de gestão de riscos (ABNT, 2018, p. 16).

Acerca do conteúdo e destinação dos relatórios de controle, Padoveze (2008) ressalta que devem ser ajustados às necessidades da organização, de modo que retratem informações claras, concisas, padronizadas e integradas aos demais procedimentos de monitoramento e controle implementados, a serem estrategicamente dirigidas a quem cabe conhecê-las, em todos os níveis da organização, conforme exemplificado no Quadro 3:

**Quadro 3 – Necessidades das Partes Interessadas / Resposta Sugerida (continua)**

<b>Necessidades das Partes Interessadas Alta Administração</b>	<b>Resposta sugerida</b>
Conhecer as mais significativas exposições da organização, a fim de lograr desenvolver um planejamento estratégico que alinhe os objetivos e a estratégia da organização ao apetite a risco estabelecido.	Apresentação dos principais riscos, inclusive de conformidade, incidentes sobre os objetivos e a estratégia da organização, bem como sobre os macroprocessos.
Ter segurança de que o processo de gerenciamento do risco se desenvolve de forma eficaz.	Capacidade para relatar riscos emergentes e outras informações excepcionais que retratem da forma mais fiel possível o nível de exposição da organização a oportunidades e ameaças.

<b>Quadro 3 – Necessidades das Partes Interessadas / Resposta Sugerida (conclusão)</b>	
Observar a tendência da exposição no tempo, atentando-se para mutações.	Comparações periódicas.
Assegurar-se da implementação de respostas aos riscos eficazes e adequadas.	Informações periódicas sobre o gerenciamento de riscos na organização, notadamente sobre a adequação das respostas aos riscos.
<b>Necessidades das Partes Interessadas Unidades Envolvidas</b>	<b>Resposta sugerida</b>
Informação sobre riscos significativos que incidam sobre os processos e/ou atividades sob a responsabilidade da unidade.	Relatório matricial por área principal do risco envolvido.
Uma indicação de <i>Quick Wins</i> <sup>7</sup> na implementação de resposta ao risco.	Controle relativo da gerencia sobre a resposta ao risco avaliada.
Segurança de que o processo de gerenciamento do risco opere eficazmente.	Informações sobre riscos incidentes sobre os processos/atividades sob a responsabilidade da unidade são analisadas e documentadas em bancos de dados.
Dados suficientes para monitorar e avaliar adequadamente o desempenho do gerenciamento do risco em relatórios funcionais.	Relatório por gerente responsável.
Processo renovável para apoiar a melhoria contínua.	Movimentos dos riscos no tempo refletidos em matrizes de perfil de riscos.
<b>Necessidades das Partes Interessadas Servidores Envolvidos</b>	<b>Resposta sugerida</b>
Pleno conhecimento do contexto e estrutura para compreender o gerenciamento de riscos na organização, sobretudo quanto às respostas ao tratamento dos riscos incidentes sobre as atividades/processos nos quais atua.	Disponibilização de todos os dados relevantes sobre risco contidos no banco de dados de riscos, incluindo, o plano de ação do gerenciamento do risco.
Informações contínuas sobre os fatores de risco para acompanhar mudanças na intensidade do risco.	Fatores de risco são analisados e documentados.
Propriedade dos riscos individuais e compreensão das responsabilidades nos riscos da organização.	Determinação de responsabilidades.
Compreensão do contexto do risco para viabilizar melhoria contínua da resposta ao risco.	Esclarecimentos contínuos sobre o contexto e significância do controle de riscos estabelecido.
Fonte: Adaptado de Padoveze (2008).	
<hr/> <p><sup>7</sup> <i>Quick Wins</i> podem ser definidas como oportunidades de melhorias que podem ser alcançadas por meio da adoção de medidas de baixa complexidade e executadas em curto prazo, mas com considerável potencial de benefício.</p>	

No mesmo sentido, a NBR 31000:2018 destaca que os relatórios devem observar a sensibilidade da informação a ser consignada e o contexto (externo e interno) na qual está inserida, posto que, como mecanismo de governança que representam, destinam-se a aprimorar a qualidade do diálogo com as partes interessadas e a apoiar a Alta Direção e os órgãos de supervisão na tomada de decisão, a fim de que cumpram a contento com as suas responsabilidades, sem deixar de atentar, dentre outros, para os seguintes aspectos: a) diferentes partes interessadas e suas necessidades específicas de informação e requisitos; b) custo, frequência e pontualidade do relato; c) método de relato; d) pertinência da informação para os objetivos organizacionais e para a tomada de decisão (ABNT, 2018, p. 16).

Por fim, tem-se que os relatórios internos devem possibilitar um adequado acompanhamento dos riscos mapeados, sendo capazes de apontar para a necessidade de realização periódica de “atividades de revisão dos processos, atualizações quanto às políticas e diretrizes, bem como reavaliação da maturidade para definir as ações de melhoria no que se refere à gestão de riscos” (BERMEJO *et al.*, 2019, p. 165).

## REFERÊNCIAS

ABNT. Associação Brasileira de Normas Técnicas. ABNT NBR ISO 31000. **Gestão de riscos: princípios e diretrizes**, 2018.

BERMEJO, Paulo Henrique de Souza *et al.* **ForRisco: gerenciamento de riscos em instituições públicas na prática**. 2. Ed. Brasília. Editora Evobiz, 2019.

PADOVEZE, Clóvis Luis. BERTOLICCI, Ricardo Galinari. **Gerenciamento de Risco Corporativo em Controladoria: Enterprise Risk Management (ERM)**. São Paulo. Editora: Cengage Learning, 2008.

TCU. Tribunal de Contas da União. **Referencial básico de gestão de riscos**. 2018. Disponível em: <<https://bitly.com/kjGXz>>. Acesso em: 05 jun. 2021.

UFS. UNIVERSIDADE FEDERAL DE SERGIPE. **Metodologia de Gestão de Riscos da UFS**. São Cristóvão: UFS, 2021.

VIEIRA, James Batista; BARRETO, Rodrigo Tavares de Souza. **Governança, gestão de riscos e integridade**. Brasília: ENAP, 2019.



## 6 CONCLUSÃO

Por meio deste estudo buscou-se responder às questões de pesquisa delineadas no item 3.2 do presente trabalho, as quais visam permitir o alcance de cada um dos objetivos específicos definidos, estes que, se bem trilhados, tendem a possibilitar o atingimento do objetivo geral que moveu a pesquisa.

### 6.1 RESPONDENDO ÀS QUESTÕES DE PESQUISA

#### **a) O que trazem os normativos internos e demais documentos disponíveis relacionados à estratégia, aos objetivos e ao gerenciamento de riscos na UFS?**

A análise dos dados trouxe à lume que, desde o ano de 2017, após a edição da Instrução Normativa Conjunta MP/CGU nº 01/2016, a UFS vem continuamente desenvolvendo um arcabouço normativo no afã de implementar e regulamentar a gestão de riscos na instituição, tendo, mais recentemente, instituído o Comitê de Gestão de Riscos e Controles da Universidade Federal de Sergipe – CGRC (Portaria nº 648, de 01/09/2020); e incorporado à estrutura normativa existente uma nova Política de Gestão de Riscos (Resolução nº 9/2021/CONSU, de 14/06/2021); a Metodologia de Gestão de Riscos da UFS (aprovada pelo CGRC em 18/05/2021); e o Plano de Gestão de Riscos (aprovado pelo CGRC em outubro de 2021), este último sobre o qual recai a proposta de intervenção formulada no presente estudo.

Acerca do sobredito Plano de Gestão de Riscos, importante observar que traz em seus termos vigência por período de dois anos, a demonstrar a disposição da instituição de revisar em curto período os procedimentos ali postos e conferir um caráter de continuidade ao gerenciamento de riscos, dada a dinamicidade envolvida nas atividades planejadas.

Na mesma linha, observa-se um largo esforço empreendido pela Alta Administração no sentido de capacitar servidores e disseminar a cultura da gestão de riscos para todos os setores da instituição.

Assim, da análise dos normativos internos e demais documentos disponíveis torna-se possível concluir que a UFS caminha a passos largos na direção de uma estruturação normativa consistente, e com possibilidade de aprimoramento contínuo.

**b) Qual o estágio atual de implantação da gestão de riscos na instituição pesquisada?**

Os dados coletados e apresentados neste trabalho apontam que a implantação da gestão de riscos na UFS se encontra em avançado estágio no que pertine à edição de instrumentos normativos relativos ao tema e que visam regulamentar a implementação e execução dos procedimentos propostos, mas, por outro lado, ainda se encontra em estágio embrionário no que diz respeito à disseminação da cultura da gestão de riscos entre os servidores da instituição, em que pese o inegável esforço da Alta Administração no afã de disseminar entre os servidores dos mais diversos níveis da estrutura hierárquica conhecimentos acerca do tema, como forma de inculcar na cultura organizacional a importância da gestão de riscos para a estratégia e o alcance dos objetivos da instituição, antes mesmo da efetiva implantação dos procedimentos.

**c) Qual o ponto de oportunidade identificado para formulação da proposta de contribuição?**

O exame do Plano de Gestão de Riscos e Controle para o biênio 2021/2022 permitiu concluir que o monitoramento e controle de riscos é nele tratado de forma breve, o que - importante frisar -, embora não implique dizer que se apresenta insuficiente ou incompleto, reflete uma oportunidade de contribuição por meio do presente estudo, ainda mais se considerado que uma revisão no referido planejamento deverá ser procedida antes de expirado o prazo ao qual se refere (2021-2022).

Nesse contexto, a formulação de proposta de Plano de Monitoramento e Controle de Riscos se revelou oportuna e suficientemente adequada à realidade institucional conhecida após a análise dos dados coletados.

**d) Como se apresentam as estruturas de gestão de riscos implantadas em outras instituições públicas federais de ensino superior, no que se refere ao ponto de oportunidade identificado?**

A coleta de dados decorrente das entrevistas realizadas junto à UFCA e UFERSA demonstra que, embora ainda não contem com um Plano de Gestão de Riscos devidamente delineado, ambas as instituições já desenvolvem ações de monitoramento e controle de riscos em setores específicos, tendo como perspectiva

o avanço contínuo na quantidade de unidades e processos organizacionais cobertos pelo gerenciamento de riscos.

Na UFCA, por exemplo, como instrumento de monitoramento e controle de riscos, apontou-se para utilização de Planilha Documentadora de Riscos e Relatórios de Comunicação que permitem o acompanhamento das ações por todos os envolvidos, além da constante atuação da Ouvidoria Interna na edição de relatórios contendo recomendações e orientações destinadas aos setores nos quais a gestão de riscos já resulta implementada.

Ademais, em ambas as instituições foram apontadas como dificuldades encontradas a limitação de pessoal e o desconhecimento ou resistência dos servidores em relação à novel circunstância trazida pela necessidade de gerenciar riscos, o que permite concluir que, embora constitua providência de caráter compulsório para ambas as instituições federais de ensino pesquisadas, a gestão de riscos ainda representa instituto relativamente distante da realidade dos servidores.

## 6.2 SUGESTÕES PARA PESQUISAS FUTURAS

Tendo em vista a natureza específica do presente estudo que, ao fim e ao cabo, teve como objetivo geral a formulação de uma proposta de contribuição para o gerenciamento de riscos na UFS e, considerados os dados coletados nas demais instituições pesquisadas, não parece despiciendo sugerir a realização de pesquisa que vise conhecer o grau de conhecimento e comprometimento dos servidores da UFS em relação às nuances da gestão de riscos, a fim de se alcançar o melhor direcionamento possível para as ações que visem à capacitação dos servidores e, sobretudo, à sensibilização pretendida pela instituição.

## 6.3 CONSIDERAÇÕES FINAIS

A presente pesquisa evidenciou que a adoção de processos visando à gestão de riscos no âmbito das organizações em geral constitui providência essencial para o alinhamento dos níveis organizacionais e o conseqüente alcance dos objetivos. Para os órgãos da Administração Pública, entretanto, além da conveniência que motiva as demais organizações, a natureza pública e o interesse público que lhe

cabe proteger tornam a gestão de riscos ainda mais imprescindível, o que se reflete nos comandos normativos apresentados por ocasião do referencial teórico.

No mesmo sentido, permitiu conhecer a estrutura normativa que lastreia a gestão de riscos na Universidade Federal de Sergipe e o seu estágio atual de implementação, de modo a possibilitar fosse elaborada uma proposta de contribuição para o instituto, visando ao atendimento do objetivo geral delineado.

As contribuições extraídas dos dados fornecidos pelas demais IFES, por sua vez, foram de grande valia para a formulação da proposta de intervenção, e suas lições aprendidas podem servir de orientações a serem observadas durante o transcurso do caminho que levará à implementação plena da gestão de riscos na Universidade Federal de Sergipe.

Lado outro, a consecução da formulação do referencial teórico representou relativa dificuldade, tendo em vista que boa parte das publicações sobre o tema “gestão de riscos” direcionam-se à implementação do instituto em organizações privadas, sobretudo ligadas ao mercado financeiro.

Ainda a título de dificuldades enfrentadas, não constitui exagero afirmar que a pandemia da COVID-19 também funcionou como fator limitador para o melhor desenvolvimento do estudo, tendo em vista que a pesquisa teve início e fim em período abarcado pelas restrições, inclusive de locomoção, impostas pela sobredita pandemia.

Ademais, é possível antever que a necessidade de se detalhar o ponto de oportunidade identificado no diagnóstico situacional pode atuar como fator limitador do acolhimento da proposta de contribuição por parte da UFS, porquanto o plano de execução no qual se propõe incorporar resultou delineado pela instituição em termos mais objetivos.

Nada obstante, importante registrar que, em linhas gerais e a despeito das dificuldades enfrentadas, ao alcançar os objetivos geral e específicos traçados, a pesquisa buscou cumprir o papel ao qual se destinou e, como resultado reflexo – e não menos importante – proporcionou a este pesquisador conhecer sobre tema até então incógnito, de modo a abrir caminho para a possibilidade de, na qualidade de servidor público, difundir o conhecimento aqui adquirido para outros servidores da instituição a qual está vinculado.



Por fim, cabe assinalar que a disciplina exigida para o propósito de mergulhar no tema gestão de riscos – que como visto, ainda que em menor intensidade, pode ser aplicada também nos aspectos cotidianos da pessoa humana –, despertou neste acadêmico o anseio de enveredar pelo caminho da pesquisa, diante da certeza de que novos conhecimentos têm o condão de apresentar a todo e qualquer indivíduo novas perspectivas de vida e comportamento.

## REFERÊNCIAS

ABNT. Associação Brasileira de Normas Técnicas. ABNT NBR ISO 31000. **Gestão de riscos: princípios e diretrizes**, 2018.

ALEXANDRINO, Marcelo; PAULO, Vicente. **Direito administrativo descomplicado**. 25. ed. São Paulo: Método, 2017.

ASSI, Marcos. **Gestão de Riscos com Controles Internos: Ferramentas, Certificações e Métodos Para Garantir a Eficiência dos Negócios**. Saint Paul Editora. Edição do Kindle, 2012.

ÁVILA, Marta Dulcéia Gurgel. **Gestão de riscos no setor público**. Revista Controle, Doutrina e Artigos. TCE-CE, Fortaleza, v. 12, n. 2, p. (179-198), dezembro, 2014. Disponível em: <<https://bityli.com/6AE5g>>. Acesso em: 06 jan. 2021.

BERMEJO, Paulo Henrique de Souza *et al.* **ForRisco: gerenciamento de riscos em instituições públicas na prática**. 2. Ed. Brasília. Editora Evobiz, 2019.

BERNSTEIN, Peter L. **Desafio aos Deuses: A Fascinante História do Risco**. Rio de Janeiro: Campus, 2011.

BEZERRA, Edson Kowask. **Gestão de Riscos de TI**. Rio de Janeiro: Escola Superior de Redes, 2013.

BRASIL. **Constituição da República Federativa do Brasil (1988)**. Promulgada em 05 de outubro de 1988. Disponível em: <<https://bityli.com/p7Yoi>>. Acesso em: 29 mai. 2020.

\_\_\_\_\_. **Decreto nº 9.203, de 22 de novembro de 2017**. Dispõe sobre a política de governança da administração pública federal direta, autárquica e fundacional. Disponível em: <<https://bityli.com/OFpvV>> Acesso em: 07 jan. 2021.

\_\_\_\_\_. **Lei Complementar nº 101, de 4 de maio de 2000**. Estabelece normas de finanças públicas voltadas para a responsabilidade na gestão fiscal e dá outras providências. Disponível em: <<https://bityli.com/3BOY5>> Acesso em: 12 jan. 2021.

\_\_\_\_\_. **Lei nº 13.303/2016, de 30 de junho de 2016**. Dispõe sobre o estatuto jurídico da empresa pública, da sociedade de economia mista e de suas subsidiárias, no âmbito da União, dos Estados, do Distrito Federal e dos Municípios. Disponível em: <<https://bityli.com/mlPMD>> Acesso em: 07 jan. 2021.

CARVALHO FILHO, José dos Santos. **Manual de direito Administrativo**. 33. ed. São Paulo: Atlas, 2019.

COSO. *Committe Of Sponsoring Organizations of the Treadway Commission (Org.)* **Gerenciamento de Riscos Corporativos: Estrutura Integrada: Sumário Executivo e Estrutura (COSO GRC, 2004)**. Tradução: Price Waterhouse Coopers e Instituto dos

Audidores Internos do Brasil, São Paulo, 2007. Disponível em: <<https://bityli.com/kxVHz>>. Acesso em: 10 dez. 2020.

\_\_\_\_\_. **Enterprise Risk Management: Compliance Risk Management: Applying the COSO ERM Framework. Executive Summary.** Novembro, 2020. Disponível em: <<https://bityli.com/xFdRo>>. Acesso em: 06 jan. 2021.

\_\_\_\_\_. **Enterprise Risk Management: Integrating with Strategy and Performance. Executive Summary.** Junho, 2017a. Disponível em: <<https://bityli.com/UPTxj>>. Acesso em: 10 dez. 2020.

DI PIETRO, Maria Sylvia Zanella. **Direito administrativo.** 31. ed. Rio de Janeiro: Forense, 2018.

FLORENCIO, Roseni Teresinha. A estratégia do contexto à inteligência em gestão de riscos. **Revista Gestão de Riscos**, ed. 119, São Paulo, p. (8-13), março, 2018. Disponível em: <<https://bityli.com/vCwHG>>. Acesso em: 06 jan. 2021.

FRASER, J.; SIMKINS, B. J. **Enterprise risk management: today's leading research and best practices for tomorrow's executives.** New Jersey (EUA): John Wiley & Sons, Inc., 2010.

GIBBS, Braham. **Análise de Dados Qualitativos.** Porto Alegre: Artmed, 2009.

GIL, Antonio Carlos. **Métodos e técnicas de pesquisa social.** 5. ed. São Paulo: Atlas, 2008.

HILL, Stephen; DINSDALE, Geoff. **Uma base para o desenvolvimento de estratégias de aprendizagem para a gestão de riscos no serviço público;** traduzido por Luís Marcos B. L. de Vasconcelos. Brasília. Escola Nacional de Administração Pública - ENAP, 2003. Cadernos ENAP, 23)

HILL, Stephen. **Guia sobre a gestão de riscos no serviço público.** Traduzido por Luís Marcos B. L. de Vasconcelos Brasília: Escola Nacional de Administração Pública, 2006. (Cadernos ENAP, 30).

HUBBARD, Douglas W. **The Failure of Risk Management: Why It's Broken and How to Fix It.** 2. Ed. New Jersey (EUA): Wiley, 2020.

INSTITUTO DOS AUDITORES INTERNOS (IIA). **Declaração de posicionamento do IIA: as três linhas de defesa no gerenciamento eficaz de riscos e controles.** São Paulo: IIA, 2013.

LAKATOS, Eva Maria; MARCONI, Marina de Andrade. **Fundamentos de metodologia científica.** 5. ed. São Paulo: Atlas, 2003.

LEAL, Marcelo Mafra. **Processo de gestão de riscos no Diário Oficial do Distrito Federal: ISO 31000:2018.** 2019. xix, 186 f., il. Dissertação (Mestrado Profissional

em Computação Aplicada) - Universidade de Brasília, Brasília, 2019. Disponível em: <<https://repositorio.unb.br/handle/10482/36123>>. Acesso em: 18 dez. 2020.

MANSANO, Sônia Regina Vargas. O método qualitativo nos estudos sociais aplicados: Dimensões éticas e políticas. **Revista Economia & Gestão**. V. 14, Belo Horizonte, p. (119-136), jan./mar, 2014.

MATIAS-PEREIRA, José. **Curso de administração pública**: Foco nas instituições e ações governamentais. 4 ed. São Paulo: Atlas, 2014.

MEIRELLES, Hely Lopes; BURLE FILHO, José Emmanuel; BURLE, Carla Rosado. **Direito administrativo brasileiro**. 42. ed. São Paulo: Malheiros, 2016.  
MELLO, Celso Antônio Bandeira de. **Curso de direito administrativo**. 32. ed. São Paulo: Malheiros, 2015.

MPOG-MINISTÉRIO DO PLANEJAMENTO ORÇAMENTO E GESTÃO;  
CONTROLADORIA GERAL DA UNIÃO. **Instrução Normativa Conjunta nº 01, de 10 de maio de 2016**. Dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo federal. Disponível em: <<https://bitly.com/Z6efH>>. Acesso em: 05 jan. 2021.

ORANGE BOOK. **Management of Risk**: Principles and Concepts. Reino Unido: HM Government, 2020. Disponível em: <<https://bitly.com/AXruP>>. Acesso em: 11 fev 2021.

PADOVEZE, Clóvis Luis. BERTOLICCI, Ricardo Galinari. **Gerenciamento de Risco Cooperativo em Controladoria: Enterprise Risk Management (ERM)**. São Paulo. Editora: Cengage Learning, 2008.

PMI-PROJECT MANAGEMENT INSTITUTE. **Guia PMBOK (2017)**: Um Guia para o Conjunto de Conhecimentos em Gerenciamento de Projetos, Sexta edição, Pennsylvania: PMI, 2017.

PORTELA, Gerardo. **Gerenciamento de riscos baseado em fatores humanos e cultura de segurança**. Rio de Janeiro: Elsevier, 2014.

PRODANOV, Cleber Cristiano; FREITAS, Ernani Cesar de. **Metodologia do trabalho científico**: Métodos e Técnicas da Pesquisa e do Trabalho Acadêmico. 2. ed. Novo Hamburgo: Universidade Freevale, 2013.

PROFIAP, Mestrado Profissional em administração Pública. **Regimento Nacional do PROFIAP**, de 9 de set. de 2021. Disponível em: <<http://www.profiap.org.br/profiap/o-curso/profiap-regimento-nacional-aprovado-em-09-07-2021-versao-02.pdf/view>>. Acesso em: 01 out. 2021.

RICHARDSON, Roberto Jarry. **Pesquisa social**: Métodos e técnicas. 3. ed. São Paulo: Atlas, 2012.

SOUZA, Rodrigo Tavares de; VIEIRA, James Batista. **Governança, gestão de riscos e integridade**. Brasília: ENAP, 2019.

TCU. Tribunal de Contas da União. **ACÓRDÃO Nº 2.127/2017, de 27 de setembro de 2017** Trata-se de Relatório de Políticas e Programas de Governo (RePP) destinado a dar cumprimento ao disposto no art. 123 da Lei 13.473/2017 (Lei de Diretrizes Orçamentárias do exercício de 2018 - LDO/2018). Relator MARCOS BEMQUERER. Acórdão 27 de set, 2017. Disponível em: <<https://bit.ly/3rEmoTA>>. Acesso em: 07 out. 2021.

\_\_\_\_\_. **Instrução Normativa nº 84, de 22 abril de 2020**. Estabelece normas para a tomada e prestação de contas dos administradores e responsáveis da administração pública federal, para fins de julgamento pelo Tribunal de Contas da União, nos termos do art. 7º da Lei 8.443, de 1992, e revoga as Instruções Normativas TCU 63 e 72, de 1º de setembro de 2010 e de 15 de maio de 2013, respectivamente. Disponível em: <<https://bityli.com/9sQMr>>. Acesso em: 05 jan. 2021.

\_\_\_\_\_. **Manual de gestão de riscos**. 2018. Disponível em: <<https://bityli.com/cAQBB>>. Acesso em: 05 jan. 2021.

\_\_\_\_\_. **Referencial básico de gestão de riscos**. 2018. Disponível em: <<https://bityli.com/kjGXz>>. Acesso em: 05 jan. 2021.

TV UFS. **Campanha Gestão de Riscos na UFS**. Youtube, 21 out. 2020. Disponível em: <<https://www.youtube.com/watch?v=C6Cez7gKYyk>>. Acesso em: 11 out. 2021.

UFS. UNIVERSIDADE FEDERAL DE SERGIPE. **Comitê de Gestão de Riscos e Controles**, c.2021. Disponível em: <<https://gestaoderiscos.ufs.br/pagina/22306>>. Acesso em: 05 nov. 2021.

\_\_\_\_\_. **Integridade**, c.2021. Disponível em: <<https://integridade.ufs.br/pagina/21646>>. Acesso em: 06 nov. 2021.

\_\_\_\_\_. **Metodologia de gestão de riscos da UFS**. 1º ed. São Cristóvão: UFS, 18 de maio 2021. Disponível em: <<https://bit.ly/3gAaNyC>>. Acesso em: 18 jun. 2021.

\_\_\_\_\_. **Plano de gestão de riscos e controles da UFS**. Aprovada pelo CGRC/UFS, em outubro de 2021.

\_\_\_\_\_. **Portaria nº 772, de 08 de maio de 2017**. Estabelece princípios e diretrizes relativas à Política de Gestão de Riscos da UFS e institui Comitê de Governança, Riscos e Controle. São Cristóvão: UFS, 2017. Disponível em: [https://audint.ufs.br/uploads/page\\_attach/path/4383/Portaria\\_772\\_2017\\_UFS.pdf](https://audint.ufs.br/uploads/page_attach/path/4383/Portaria_772_2017_UFS.pdf). Acesso em: 10 out. 2021.

\_\_\_\_\_. **Portaria nº 648, de 01 de setembro de 2020**. Institui o Comitê de Gestão Riscos e Controles e determina outras providências. São Cristóvão: UFS, 2020. Disponível em: <<https://bit.ly/34piN3f>>. Acesso em: 18 out. 2021.

\_\_\_\_\_. **Resolução nº 9/2021/CONSU, de 14 de junho de 2021.** Institui as Políticas de Integridade e de Gestão de Riscos e Controles da Universidade Federal de Sergipe - UFS e dá outras providências. São Cristóvão: UFS, 2020. Disponível em: < <https://bit.ly/3JiPk9H>> Acesso em: 21 set. 2021.

\_\_\_\_\_. **Resolução nº 015/2020/CONSU, de 28 de setembro de 2020.** Institui a Política de Governança da Universidade Federal de Sergipe - UFS e dá outras providências. São Cristóvão: UFS, 2020. Disponível em: <<https://bitly.com/hC4kB>>. Acesso em: 21 jan. 2021.

\_\_\_\_\_. UNIVERSIDADE FEDERAL DE SERGIPE. **Plano de desenvolvimento institucional (PDI) 2016-2020.** São Cristóvão: UFS, 2016. Disponível em: <<https://bitly.com/oYvGd>>. Acesso em: 18 jan. 2021.

\_\_\_\_\_. **UFS em números 2020.** São Cristóvão: UFS, 2016. Disponível em: <<https://bitly.com/zDh9W>>. Acesso em: 18 jan. 2021.

VERGARA, Sylvia Constant. **Projetos e relatórios de pesquisa em administração.** 5 ed. São Paulo: Atlas, 2004.

VIEIRA, James Batista; BARRETO, Rodrigo Tavares de Souza. **Governança, gestão de riscos e integridade.** Brasília: ENAP, 2019.

YIN, Robert K. **Estudo de Caso, planejamento e métodos.** 2ª ed. São Paulo: Bookman, 2001.

## APÊNDICE A

### OUTRAS CATEGORIAS DE RISCOS APRESENTADAS POR MARCOS ASSI

CATEGORIA DE RISCO	DEFINIÇÃO
Risco de liquidação financeira	Caracteriza-se por perdas decorrentes de “falhas nos procedimentos e controles de finalização das transações, por falta de procedimentos, ou ainda por inexistência de controle sistêmico”.
Risco de concentração	Envolve “perdas por dependência de clientes, fornecedores e mercados”;
Risco de taxa	Decorre da “correlação imperfeita das taxas de captação e aplicação da organização”, de modo a ser mais incidente nas instituições financeiras, embora deva-se considerar “que uma instituição não financeira terá risco essencialmente na possibilidade dos seus passivos à taxa variável acarretarem um acréscimo de custos perante uma subida das taxas de juro”. Tal categoria pode ser subdividida em quatro outros tipos de riscos, estes trazidos pelo autor como: <u>Risco de base (<i>basis risk</i>)</u> , assim considerado “o risco que advém de quando as taxas de juro dos ativos são remuneradas segundo bases/indexados diferentes das taxas de juro dos passivos”; <u>Risco de curva de taxas de juro (<i>yield curve risk</i>)</u> , que consiste no advindo “dos movimentos desfavoráveis em vários segmentos da curva de taxas de juro, o qual pode provocar problemas a uma entidade em que os ativos e passivos estejam em diferentes segmentos da curva com proporções diferentes”; <u>Risco de (<i>repricing risk</i>)</u> , definido como “o risco que advém de diversos ativos e passivos que venham a reindexar a taxas diferentes”; <u>Risco de opção (<i>option risk</i>)</u> , “que advém da opção inerente a alguns passivos e ativos, que pode levar, por exemplo, os detentores de hipotecas à taxa fixa e venham a refinanciar perante uma baixa de taxas de juros”
Risco de taxas de câmbio	É definido como “o risco de perdas devido a mudanças adversas nas taxas de câmbio”, sendo exemplos a “variação nos preços de títulos públicos indexados à moeda estrangeira, de ativos internacionais negociados em moeda estrangeira, devido à apreciação/depreciação relativa de moedas” e o “descasamentos em carteiras indexadas a alguma moeda estrangeira”.
Risco de mercado	Decorre da variação dos preços de serviços e/ou produtos, “pode ser definido como uma medida numérica da incerteza relacionada aos retornos esperados de um investimento, em decorrência de variações em fatores como taxas de juros, taxas de câmbio, preços de ações e commodities.”
Risco de derivativos e hedge	Presente no mercado financeiro, consiste no “risco de perdas devido ao uso de derivativos (seja para especulação, seja para hedge)”, tendo como exemplo a, dentre outros, a “variações no valor de posições de contratos de swaps, futuros, a termo, opções etc.”
Risco de liquidez	Advindo da insuficiência de recursos para adimplir “compromissos assumidos em decorrência de gestão insatisfatória do caixa da empresa, justamente pela incapacidade de honrar os pagamentos, pela falta de posição sustentada de caixa e pela fonte de captação de recursos”.

Risco tributário	“Possibilidade de perda ocasionada por interpretação indevida da legislação tributária”, cujo enfrentamento exige que “as alíquotas e obrigações acessórias estejam bem definidas e mapeadas, para segurança da gestão tributária da organização”.
Risco-país	Consiste numa “medida que visa classificar o risco geral de um país”, visando “calcular o nível de instabilidade econômica de uma nação”, por meio da análise da situação econômica, e “aspectos sociais e políticos do país”.
Risco de demanda	Caracterizado pela “incerteza que cerca a demanda futura por um produto ou por um serviço devido à interação de fatores inesperados e incontroláveis, como mudanças imprevistas na regulamentação e mudanças no gosto dos clientes”.
Risco de novos produtos	Decorre do lançamento pela organização, sem o planejamento, conhecimento e suporte técnico adequados, de um novo produto no mercado, sendo certo que “os erros tendem a ser mais altos nos estágios iniciais de desenvolvimento de um novo produto ou quando o novo produto é espetacularmente mais popular que o previsto, causando perdas em potencial de reputação e custos de oportunidade”.
Risco de reputação	“Pode ser visualizado como as perdas monetárias e financeiras que se seguem à perda de reputação de uma organização”, e que podem pôr em risco a confiança e provocar o descrédito dos seus produtos ou serviços.
Risco de continuidade	Incide sobre a possibilidade de solução de continuidade do negócio diante de eventos que podem comprometê-la, cujo enfrentamento exige um plano de contingência que possa abranger “sucessão do corpo diretivo, de pessoas-chave, backup, unidades de negócio, plano de negócios, acesso ao prédio em caso de distúrbios naturais, greve, protestos, entre outros”, bem como sistemas de tecnologia da informação, a fim de “evitar interrupções dos serviços e prejuízos em potencial”.
Risco de crédito	Representa a “incerteza relacionada ao recebimento de um valor contratado/compromissado a ser pago por um tomador de um empréstimo, contraparte de um contrato ou emissor de um título, descontadas as expectativas de recuperação e realização de garantias”.



## **APÊNDICE B**

### **ROTEIRO DE ENTREVISTA**

**INSTITUIÇÃO PESQUISADA: UNIVERSIDADE FEDERAL DE SERGIPE**

**ENTREVISTADO:**

1. Qual a fase atual de implantação da gestão de riscos na UFS?
2. Qual ou quais as principais metodologias predominantemente adotadas na estruturação da gestão de riscos da instituição?
3. Qual a forma de envolvimento do quadro de pessoal nas ações que visam à gestão de riscos?
4. A instituição vem organizando cursos e/ou eventos de qualificação de pessoal voltados ao tema gestão de riscos?
5. Quais as maiores dificuldades enfrentadas até o momento para implantação da gestão de riscos?
6. Já é possível identificar efeitos ou resultados da implantação da gestão de riscos para a estratégia e objetivos da instituição?

## **APÊNDICE C**

### **ROTEIRO DE ENTREVISTAS**

#### **INSTITUIÇÃO PESQUISADA:**

#### **ENTREVISTADO:**

1. De que forma está estruturado o plano de monitoramento e controle de riscos da Instituição?
2. Qual a forma de envolvimento do quadro de pessoal nas ações que visam monitorar e controlar os riscos?
3. Quais as maiores dificuldades enfrentadas para o desenvolvimento das atividades previstas no plano de monitoramento e controle de riscos da instituição?
4. Quais as principais lições aprendidas desde o processo de elaboração do plano de monitoramento e controle de riscos até o seu estágio atual de execução?

**ANEXO A**

Universidade Federal de Sergipe

**PLANO DE GESTÃO DE RISCOS E  
CONTROLES DA UFS**

**2021/2022**

**PLANO DE GESTÃO DE RISCOS E CONTROLES DA UFS**

**2021/2022**

**ELABORAÇÃO**

**COMITÊ DE GESTÃO DE RISCOS E CONTROLES DA UFS – CGRC**

**Membros do CGRC**

(Portaria 619 de 20 de maio de 2021)

Marcos Vinícius Nascimento Gonzalez Castaneda  
Coordenador

Adriana de Lima – Pró Reitoria de Administração.

Fred Amado Martins Alves - Comitê de Gestão da Integridade.

Gustavo Torres de Brito Daier - Superintendência de Tecnologia da  
Informação.

Jefferson David Araújo Sales – Prof.º do Departamento de Administração.

Patrícia Tavares de Araújo – Auditoria Interna.

Rivaldo José Rodrigues de Lima - Departamento de Administração.

**PLANO DE GESTÃO DE RISCOS E CONTROLES DA UFS****2021/2022**

## SUMÁRIO

## APRESENTAÇÃO

1. INTRODUÇÃO
2. FUNDAMENTOS DA GESTÃO DE RISCOS
  - 2.1. FUNDAMENTOS LEGAIS
  - 2.2. BASE TEÓRICA
3. PRINCÍPIOS, OBJETIVOS E DIRETRIZES DA GESTÃO DE RISCOS NA UFS
  - 3.1. PRINCÍPIOS
  - 3.2. OBJETIVOS
  - 3.3. DIRETRIZES
4. ESTRUTURA DA GESTÃO DE RISCOS NA UFS
  - 4.1 INSTÂNCIAS DE SUPERVISÃO, LINHAS DE DEFESA E COMPETÊNCIAS;
5. METODOLOGIA DE GESTÃO DE RISCOS DA UFS
6. PLANO DE AÇÃO
7. MONITORAMENTO E CONTROLES
8. CONCLUSÃO

## APRESENTAÇÃO

A gestão de riscos e controles é parte primordial da governança institucional. Com ela é possível apoiar os agentes públicos para o alcance dos objetivos da organização a partir de ações que minimizem os riscos inerentes à natureza, muitas vezes complexas, das atividades realizadas nas instituições públicas.

Partindo desse princípio, a Universidade Federal de Sergipe estabeleceu em sua Política de Gestão de Riscos e Controles a missão de aprimorar continuamente os processos organizacionais, projetos e iniciativas estratégicas a partir da operacionalização (em consonância com as demais unidades responsáveis pela estrutura de governança da UFS) da gestão de riscos e controles em toda a Instituição, de forma a assegurar a produção de informações relevantes que auxiliem os gestores na tomada de decisão e no cumprimento dos serviços de forma clara e eficiente, respondendo adequadamente aos anseios da sociedade.

Para o TCU (2017)

*“a gestão de riscos corretamente implementada e aplicada de forma sistemática, estruturada e oportuna gera benefícios que impactam diretamente cidadãos e outras partes interessadas da organização ao viabilizar o adequado suporte às decisões de alocação e uso apropriado dos recursos públicos, o aumento do grau de eficiência e eficácia no processo de criação, proteção e entrega de valor público, otimizando o desempenho e os resultados entregues à sociedade.” (TCU, 2017)*

Assim, se faz necessário estabelecer a sistemática de ações que oriente a Universidade no sentido de estabelecer os procedimentos da gestão de riscos, baseados em critérios bem definidos de competências, responsabilidades, métodos e prazos de execução.

Nesse sentido, o presente Plano de Gestão de Riscos e Controles da Universidade Federal de Sergipe apresenta a metodologia de gerenciamento de riscos a ser implementada na Instituição, detalhando a operacionalização, as normas e os critérios técnicos a serem seguidos pela Universidade a fim de se estabelecer um processo contínuo de gestão de riscos na UFS.

## 1. INTRODUÇÃO

Este Plano tem o objetivo de orientar a implementação da Política de Gestão de Riscos e Controles (Resolução 09/2021 CONSU) na Universidade Federal de Sergipe e definir as diretrizes para operacionalização da Gestão de Riscos na Universidade.

O plano está dividido em oito partes, iniciando pela apresentação dos normativos que dispõem sobre a implementação da gestão de riscos nas instituições públicas federais. Esses normativos formam a base de entendimentos e instruções para a melhor organização do processo, em conformidade com as boas práticas sugeridas pelos órgãos de controles federais.

Também será apresentada a estrutura organizacional responsável pela implementação e operacionalização da Política de Gestão de Riscos na Instituição. O objetivo é registrar as competências e responsabilidades das unidades que compõem as instâncias de supervisão e execução da gestão de riscos na Universidade, as quais, em seu conjunto, formam as linhas de defesa para o gerenciamento de riscos da UFS. Essas camadas (ou modelo de três linhas de defesa, conforme estabelecido pelo IIA)<sup>1</sup> estão previstas na principal Instrução Normativa (IN 01/2016 MP/CGU) que orienta os órgãos públicos na “*adoção de medidas para a sistematização de práticas relacionadas à gestão de riscos, aos controles internos e à governança*”.

Um capítulo deste Plano detalhará as áreas de atuação da UFS na gestão de riscos. A ideia é uma implementação gradual, contínua e abrangente nas unidades administrativas e acadêmicas da Universidade, focada em três vertentes: gestão de riscos estratégicos, relacionados aos objetivos definidos no Plano de Desenvolvimento Institucional (PDI) da UFS e em outros planos setoriais de nível estratégico; gestão de riscos operacionais, com relação direta, mas não exclusiva, ao mapeamento de processos organizacionais<sup>2</sup> realizados na UFS<sup>3</sup> e; gestão de riscos de Integridade com relação direta ao Plano de Gestão de Integridade da Universidade.

Finalmente, será apresentada a metodologia de gerenciamento de riscos a ser adotada na UFS. Esta metodologia está baseada nas melhores práticas realizadas pelos

---

<sup>1</sup> *Institute of Internal Auditors (IIA) - Declaração de Posicionamento: As três Linhas de Defesa no Gerenciamento Eficaz de Riscos e Controles, 2013.*

<sup>2</sup> A falta de mapeamento de processos não exclui a possibilidade de gerenciamento de riscos em projetos ou processos específicos que necessitem desse acompanhamento.

<sup>3</sup> Nesta vertente também se encontra o acompanhamento do gerenciamento de riscos nas contratações, estabelecidas pela IN 05/2017 do Ministério do Planejamento, Desenvolvimento e Gestão (atual ministério da Economia).

órgãos do Poder Executivo federal (sobretudo o antigo Ministério do Planejamento, Orçamento e Gestão, agora Ministério da Economia, e do Ministério da Transparência e Controladoria Geral da União - CGU ) e em orientações direcionada às Universidade pelos órgãos de controles, como a própria CGU e o Tribunal de Contas da União (TCU).

O conjunto de ações deste Plano segue, assim, todas as etapas de execução previstas nas principais metodologias de gestão de riscos comumente empregadas na gestão pública, a saber: ISO 31000 e a COSO ERM. Portanto, todo o processo de gerenciamento de riscos será detalhado de forma que este Plano sirva também como um normativo para as etapas de execução da gestão de riscos na Universidade.

Por fim, o cronograma de atividades aqui previsto definirá os prazos e metas da execução do Plano de Gestão de Riscos e Controles da Universidade Federal de Sergipe para o período de 2021-2022.

## **2. FUNDAMENTOS DA GESTÃO DE RISCOS**

### **2.1 Fundamentos legais**

A incorporação da gestão de riscos na Administração Pública federal teve seu marco normativo inicial com a publicação da Instrução Normativa Conjunta nº 01, de 10 de maio de 2016. De acordo com o art. 2º da mencionada IN, *“os órgãos e entidades do Poder Executivo federal deverão adotar medidas para a sistematização de práticas relacionadas à gestão de riscos, aos controles internos e à governança”*.

A IN Conjunta 01/2016 traz expressamente em seu texto definições essenciais de termos comumente utilizados no processo de gestão de riscos, tais como apetite ao risco, controles internos da gestão, governança no setor público, incerteza, risco, dentre outros. Além disso, o normativo discorre acerca dos princípios, objetivos, estrutura e responsabilidades referentes aos controles internos da gestão.

Ainda na IN Conjunta 01/2016, encontram-se os princípios, os objetivos, as responsabilidades e a estrutura do modelo de gestão de riscos, bem como as diretrizes para a formulação das políticas de gestão de riscos nos órgãos e entidades do Poder Executivo federal.

Por fim, em relação à governança, a IN Conjunta 01/2016 estabelece os princípios da boa governança e prevê a criação de comitês de governança, riscos e controles nos órgãos e entidades federais, os quais, dentre outras funções, serão responsáveis por institucionalizar estruturas adequadas de governança, gestão de riscos e controles internos (art. 23, § 2º, inc. II, da IN Conjunta MP/CGU 01/2016).



O Decreto 9.203, de 22 de novembro de 2017, por sua vez, dispondo sobre a sobre a política de governança da administração pública federal direta, autárquica e fundacional, institui que a alta administração deve estabelecer o sistema de gestão de riscos e controles internos com vistas à identificação, à avaliação, ao tratamento, ao monitoramento e à análise crítica de riscos que possam impactar a implementação da estratégia e a consecução dos objetivos da organização no cumprimento da sua missão institucional, observando, dentre outros, a integração da gestão de riscos ao processo de planejamento estratégico da instituição (Art. 17, inciso II).

Em âmbito federal, tem-se ainda a Instrução Normativa MP nº 05, de 25 de maio de 2017, que dispõe sobre as regras e diretrizes do procedimento de contratação de serviços sob o regime de execução indireta no âmbito da Administração Pública federal direta, autárquica e fundacional, e a Instrução Normativa ME nº 01, de 04 de abril de 2019, que dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação - TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal.

Em que pese os citados decretos e instruções normativas tratem de áreas específicas da gestão pública (terceirização de serviços e contratações de TIC), ambas apresentam diretrizes e regras específicas voltadas para a gestão de riscos no âmbito de seus objetos. Referidos normativos são mandatórios para todos os órgãos e entidades da Administração Pública federal e servem como referência de boa prática para as demais áreas de atuação da gestão pública que ainda não possuam normativos específicos.

Já no âmbito da Universidade Federal de Sergipe, foram editados normativos e documentos administrativos que internalizaram as diretrizes e regras estabelecidas pelo Governo Federal no tocante à governança, gestão de riscos e controles. São eles:

- Política de Governança da UFS (Resolução nº 15/2020/CONSU);
- Portaria nº 648/2020, que instituiu o Comitê de Riscos e Controles da Universidade Federal de Sergipe;
- Política de Integridade e de Gestão de Riscos e Controles da UFS (Resolução nº 09/2021/CONSU);
- Metodologia de Gestão de Riscos da UFS (elaborada pelo Comitê de Gestão de Riscos e Controles da UFS – Portaria 887/2020)

- Definição do Apetite a Risco da UFS (pelo Comitê de Gestão de Riscos e Controles da UFS – Ata de Reunião Ordinária do Comitê Institucional de Governança de 21/05/21).

Conforme será detalhado nos itens subsequentes, cada um desses documentos, dentro das respectivas áreas abordadas, atuou como referência para desenhar o presente Plano de Gestão de Riscos e Controles da Universidade Federal de Sergipe.

## 2.2 Base teórica

Para a construção do Plano de Gestão de Riscos e Controles da Universidade Federal de Sergipe, além dos parâmetros normativos, buscou-se ainda orientações e inspirações nas metodologias e boas práticas adotadas por outras organizações, especialmente aquelas referenciadas como positivas pelo Tribunal de Contas da União – TCU.

Na elaboração do presente Plano, priorizou-se as diretrizes apontadas pela ISO 31000:2018 e o COSO ERM. Ambas as metodologias gozam de grande aceitação tanto no ambiente corporativo como perante as instituições de natureza pública. Além disso, são metodologias que foram desenvolvidas por organizações internacionais que buscam nivelar, em escala global, padrões de excelência no que se refere à gestão de riscos organizacionais.

A influência dessas metodologias no processo de implementação da gestão de riscos na UFS pode ser observada especialmente nos documentos que consolidam a Política de Integridade e de Gestão de Riscos e Controles e na Metodologia de Gestão de Riscos da UFS.

A principal contribuição adotada neste Plano, obtida a partir do COSO ERM, é a adoção do conceito das *3 linhas (ou camadas) de defesa* da instituição. De forma escalonada e coordenada, foram previstos três níveis de proteção institucional que atuam de forma alinhada objetivando proteger os valores organizacionais e orientar a atuação dos agentes públicos para atingir os objetivos estratégicos da UFS.

Em relação à ISO 31000:2018, foram absorvidas as dinâmicas estabelecidas pela metodologia nos processos de avaliação, tratamento, monitoramento e comunicação dos riscos identificados.

Registre-se, ainda, as contribuições obtidas a partir da análise da metodologia desenvolvida pelo Fórum Nacional de Pró-Reitores de Planejamento e de Administração das Instituições Federais de Ensino Superior (Forplad). A metodologia ForRiscos, além de ter sido desenvolvida com base nas principais metodologias existentes no mercado, tem como ponto de destaque aproximar a gestão de riscos (vista de forma geral) do contexto singular e multifacetado que existe no âmbito das instituições federais de ensino.

Conforme usualmente os especialistas em riscos pontuam, a gestão de riscos “não é uma receita de bolo”. Cada organização deve adequar as diretrizes propostas pelas metodologias existentes aos seus contextos interno e externo. Gradativamente, a UFS tem avançado em estabelecer bases sólidas para atingir a maturidade organizacional no tocante à gestão de riscos. O presente Plano constitui uma ferramenta para orientar a execução desse processo de amadurecimento organizacional.

### **3. PRINCÍPIOS, OBJETIVOS E DIRETRIZES DA GESTÃO DE RISCOS NA UFS**

#### **3.1 Princípios**

A Gestão de Riscos e Controles na Universidade Federal de Sergipe deverá observar os seguintes princípios:

- I. *Alinhamento estratégico e sistêmico*: deve considerar a missão, a visão, os valores e demais elementos relevantes dispostos no Plano de Desenvolvimento Institucional/PDI da UFS e demais planos estratégicos da Instituição, bem como observar as diretrizes que vieram a ser emanadas dos órgãos centrais dos sistemas federais;
- II. *Consistência de análise*: deve estar suportada em informações e indicadores consistentes e de fácil validação por instâncias independentes;
- III. *Economicidade*: deve ser vantajosa a relação entre custo e risco, na implementação de mecanismos de controle;
- IV. *Transparência*: deve divulgar as ações e atividades relativas à gestão de riscos e controles da UFS, prestando informações confiáveis, relevantes e tempestivas à sociedade visando à participação social na proposição e no monitoramento da execução das políticas públicas;
- V. *Uniformidade*: deve observar os mesmos conceitos, parâmetros, referenciais técnicos e procedimentos em todas as unidades e níveis da UFS;

- VI. *Universalidade*: deve abranger, gradual e permanentemente, todos os processos organizacionais da UFS.

### 3.2 Objetivos

A Gestão de Riscos e Controles na Universidade Federal de Sergipe não deve ser entendida como um fim em si mesma, mas sim como uma abordagem sistematizada tendo como objetivo geral dar suporte aos gestores da Instituição, fornecendo-lhes uma visão mais abrangente dos contextos em que a Universidade está inserida e informações estratégicas para subsidiar a tomada de decisões. Como objetivos específicos, a gestão de riscos institucional pretende:

- I. Assegurar que as informações produzidas sejam íntegras e confiáveis à tomada de decisão, ao cumprimento de obrigações de transparência e à prestação de contas;
- II. Assegurar que os responsáveis pela tomada de decisão, em todos os níveis, tenham acesso tempestivo a informações suficientes quanto aos riscos aos quais os serviços estão expostos;
- III. Assegurar a conformidade com as leis e regulamentos aplicáveis, incluindo normas, políticas, programas, planos, procedimentos e diretrizes internas e externas à UFS de forma a melhorar o controle da gestão;
- IV. Proporcionar eficiência, eficácia e efetividade operacional, mediante execução controlada, ordenada, ética e econômica das operações;
- V. Agregar valor à UFS por meio da melhoria dos processos organizacionais e do tratamento adequado dos riscos e dos impactos decorrentes de sua materialização.

### 3.3 Diretrizes

A Gestão de Riscos e Controles na Universidade Federal de Sergipe observará as seguintes diretrizes:

- I. a formalização da gestão de riscos e controles por meio de metodologias, normas, manuais e procedimentos;
- II. a obtenção de informações úteis à tomada de decisão, por meio de metodologias e ferramentas, visando o alcance dos objetivos institucionais, mediante o gerenciamento e a manutenção dos riscos dentro de padrões definidos pelas instâncias supervisoras;
- III. a realização da medição do desempenho da gestão de riscos mediante atividades contínuas ou de avaliações independentes;

- IV. a avaliação de mudanças internas e externas que contribuam para identificação de vulnerabilidades que impactam nos objetivos institucionais, no desenvolvimento e na implementação de atividades de controles da UFS;
- V. a utilização de procedimentos de controles proporcionais aos riscos e baseados na relação custo-benefício e na agregação de valor à instituição, e,
- VI. a promoção pela alta administração, de condições para que procedimentos efetivos de controles integrem as práticas de gestão de riscos.

#### **4. ESTRUTURA DA GESTÃO DE RISCOS NA UFS**

##### **4.1 Instâncias de supervisão, linhas de defesa e competências**

A IN Conjunta MP/CGU 01/2016 pode ser considerada como o marco normativo inicial para a institucionalização da gestão de riscos no âmbito do Poder Executivo federal. O modelo adotado pela citada Instrução Normativa prevê a adoção das três linhas (ou camadas) de defesa das organizações.

A *primeira linha de defesa* corresponde aos controles internos existentes nas instituições. Esses controles são operados por todos os agentes públicos na execução de atividades e tarefas no âmbito dos macroprocessos finalísticos. De acordo com o art. 2º, inc. V, da IN Conjunta MP/CGU 01/2016, controles internos são:

*“conjunto de regras, procedimentos, diretrizes, protocolos, rotinas de sistemas informatizados, conferências e trâmites de documentos e informações, entre outros, operacionalizados de forma integrada pela direção e pelo corpo de servidores das organizações, destinados a enfrentar os riscos e fornecer segurança razoável de que, na consecução da missão da entidade”.*

A *segunda linha de defesa* refere-se a instâncias de supervisão e monitoramento dos controles internos estabelecidos nas instituições (art. 6º da IN Conjunta MP/CGU 01/2016). Essa supervisão poderá ser executada por comitês, diretorias ou assessorias criadas especificamente para tratar de riscos, controles internos, integridade e *compliance*, por exemplo.

A *terceira linha de defesa* alcança a atuação da unidade de auditoria interna nas instituições. A atuação da auditoria interna tem por objetivo auxiliar a organização a realizar seus objetivos, a partir da aplicação de uma abordagem sistemática e disciplinada para avaliar e melhorar a eficácia dos processos de gerenciamento de riscos, de controles internos, de integridade e de governança (art. 2º, inc. III, da IN Conjunta MP/CGU 01/2016).

As linhas (ou camadas) de defesa foram internalizadas na Universidade Federal de Sergipe por intermédio da Resolução 09/2021/CONSU, que institui as Políticas de Integridade e de Gestão de Riscos e Controles da UFS, observando-se as instâncias administrativas existentes na Instituição. De acordo com o art. 23, combinado com o art. 30, ambos da citada Resolução, são instâncias responsáveis pela Gestão de Riscos e Controles na UFS:

- a) Conselho Universitário (CONSU) e Conselho do Ensino, da Pesquisa e da Extensão (CONEPE);
- b) Reitoria;
- c) Auditoria Interna;
- d) Comitê Institucional de Governança (CIG);
- e) Comitê de Gestão de Riscos e Controles (CGRC);
- f) Unidade executiva de gestão de riscos e controles;
- g) Gestor de processo organizacional;
- h) Servidores da instituição.

No âmbito da UFS, a primeira linha de defesa organizacional é representada pela atuação dos servidores e do gestor do processo organizacional. Esses atores executam as atividades e tarefas associadas aos macroprocessos institucionais.

Já a segunda linha de defesa é composta por várias instâncias administrativas que, de acordo com suas competências organizacional, atuam na supervisão e no monitoramento da gestão de riscos e dos controles internos na UFS. Os arts. 24, 25, 27 e 28, todos da Resolução 09/2021/CONSU, discrimina as competências do CONSU, CONEPE, Reitoria, CIG, CGRC e da unidade executiva de gestão de riscos e controles, que são as unidades administrativas que integram a segunda linha de defesa.

Por fim, a terceira linha de defesa na UFS é executada pela Auditoria Interna da Instituição, de acordo com as diretrizes estabelecidas no art. 26 da Resolução 09/2021/CONSU.

## **5. METODOLOGIA DE GESTÃO DE RISCOS DA UFS<sup>4</sup>**

### **5.1 O Processo de Gestão de Riscos e Controles**

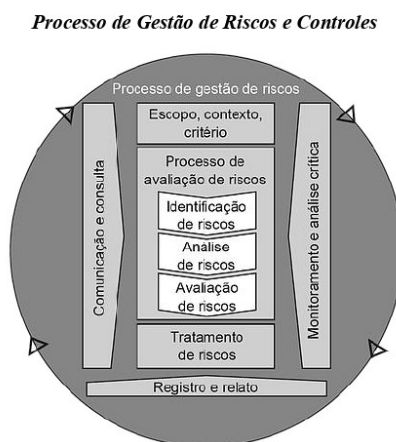
---

<sup>4</sup> Este tópico refere-se à Metodologia de Gestão de Riscos e Controles da UFS, 1ª Edição, aprovada em 18/05/2021. Para maiores detalhes e identificação de atualizações, ver: [www.gestaoderiscos.ufs.br](http://www.gestaoderiscos.ufs.br)

Conforme estabelecido na Política de Gestão de Riscos e Controles da Universidade Federal de Sergipe, o processo de gestão de riscos e controles deverá ser realizado em consonância com as demais unidades responsáveis pela estrutura de governança da Universidade, observando, no mínimo, os seguintes componentes:

- I. Comunicação e consulta;
- II. Estabelecimento do contexto;
- III. Identificação de riscos;
- IV. Análise de riscos;
- V. Avaliação de riscos;
- VI. Tratamento de riscos; e
- VII. Monitoramento e análise crítica.

De forma geral, esses componentes podem ser destacados em seis grandes eixos (etapas), conforme diagrama abaixo:



- a) *Comunicação e Consulta*: objetivando conscientização acerca da importância da gestão de riscos na Universidade e o retorno das informações que auxiliarão na tomada de decisões das unidades mapeadas;
- b) *Escopo, Contexto e Critério*: com a definição clara do escopo do processo em análise e seu alinhamento aos objetivos Institucionais, a classificação de nível em

- que se encontra o processo analisado<sup>5</sup> (estratégico, tático ou operacional) e a análise do contexto interno e externo no qual o processo se encontra;
- c) *Processo de avaliação de riscos*: compreendendo as etapas de identificação, análise e avaliação dos riscos;
  - d) *Tratamento dos riscos*: tendo como objetivo a identificação e a seleção de controles para mitigar os riscos, a níveis aceitáveis pela Instituição;
  - e) *Monitoramento e a análise crítica*: tendo por finalidade o acompanhamento dos riscos identificados e o aprimoramento contínuo do processo de trabalho sob avaliação;
  - f) *Registro e o Relato*: definindo o processo de documentação e registro dos resultados e a exposição dos mesmos nas instâncias de gestão.

A comunicação e consulta, assim como o monitoramento e a análise crítica, se caracterizam como componentes dinâmicos que devem ser observados de forma contínua ao longo da execução de todas as etapas do gerenciamento de riscos no âmbito da Instituição. Portanto, o processo de gestão de riscos envolve a coordenação sistemática e iterativa dessas ações para as quais deverão ser seguidos os procedimentos descritos abaixo.

## 5.2 Etapas para o gerenciamento de riscos na UFS

Para a aplicação dessa metodologia é necessário que a Universidade tenha estabelecido o seu apetite ao risco<sup>6</sup> e que as unidades avaliadas possuam macroprocessos ou processos de trabalho mapeados, o que permitirá a compreensão da lógica organizacional da unidade e o detalhamento das atividades a serem analisadas<sup>7</sup>.

É necessário também que seja designada uma equipe para o mapeamento e gerenciamento de riscos, composta por agentes de diferentes níveis de responsabilidades e de conhecimentos dentro da unidade. Nesse momento, deverá ser identificado o gestor de processo organizacional, servidor responsável pelo monitoramento dos riscos e pela

---

<sup>5</sup> Convém observar que a gestão de riscos pode ser aplicada a programas, projetos ou atividades específicas (ISO 31000:2018). Portanto esta metodologia se aplica a qualquer atividade da Instituição, sem perda de qualidade.

<sup>6</sup> O Apetite ao risco é o nível de risco que uma organização está disposta a aceitar para atingir seus objetivos estratégicos.

<sup>7</sup> Essa metodologia também pode ser aplicada a atividades, programas ou projetos institucionais, sendo necessário, por parte do gestor do programa/projeto, o pleno conhecimento das atividades realizadas ao longo de todo trabalho.



efetividade das medidas de controle sugeridas (proprietário do risco). Essa equipe deverá receber capacitação e treinamento em gestão de riscos para execução do trabalho.

Após a definição da unidade, dos processos a serem trabalhados, da equipe e do gestor de processo, a metodologia deverá ser aplicada com a adoção das seguintes etapas:

#### ***Etapa 1 – Comunicação e Consulta***

A comunicação e consulta representa um processo regular e constante de fluxo de informações entre os envolvidos, promovendo a conscientização da importância da gestão de riscos e a obtenção de informações necessárias para a tomada de decisão.

Nessa etapa deve-se estabelecer um processo de comunicação e consulta eficaz entre as partes envolvidas de forma que a gestão de riscos auxilie:

- a) No estabelecimento adequado do contexto em análise;
- b) Na garantia que os interesses das partes sejam amplamente compreendidos e considerados;
- c) Na integração de pessoas com diferentes níveis de conhecimento, assegurando uma abordagem mais plural na identificação e análise dos riscos;
- d) Na aprovação e no apoio das partes para a implementação de um plano adequado de tratamento dos riscos identificados.

Para este fim, a unidade executiva de gestão de riscos da UFS deve estabelecer um plano de comunicação e consulta envolvendo os seguintes instrumentos, sem prejuízos da adoção de outras ferramentas que contribuam para aprimorar a comunicação dos riscos na Instituição:

- a) Elaboração de cartilha com apresentação da importância da gestão de riscos para os objetivos institucionais;
- b) Apresentação de um manual básico com as etapas do gerenciamento de riscos;
- c) Elaboração de modelos de documentos padronizados a serem utilizados no processo de gerenciamento de riscos; e
- d) Plano de capacitação dos servidores em gestão de riscos.

#### ***Etapa 2 – Escopo, Contexto e Critério***

É fundamental que todas as partes envolvidas no gerenciamento de riscos tenham o conhecimento do direcionamento estratégico estabelecido pela Universidade no período em que se iniciar o processo de análise em sua unidade. Na UFS, o documento

que estabelece essas informações é, principalmente, o Plano de Desenvolvimento Institucional (PDI), onde se identifica a missão, a visão, os objetivos gerais e os valores da Universidade.

Vale lembrar que a presente etapa pode estar contemplada na atividade de mapeamento de processos realizada pelo Escritório de Processos da UFS. Portanto, em unidades em que o trabalho de mapeamento esteja completo, deve-se utilizar o referido material para o preenchimento das atividades descritas a seguir:

#### Definição do Escopo

A partir do reconhecimento do direcionamento estratégico da Instituição é necessário avaliar o escopo do processo. Para esse fim, deve-se:

- a) Identificar o processo e o nível em que este se insere (estratégico, tático ou operacional) na Universidade;
- b) Avaliar e registrar os objetivos do processo e como estão alinhados aos objetivos organizacionais da UFS;
- c) Identificar e registrar o macroprocesso ao qual o processo em análise esteja associado, as leis e regulamentos e os sistemas utilizados para sua execução.

O próximo passo é a compreensão dos ambientes interno e externo onde o processo se encontra.

#### Contexto

A compreensão do contexto em que se desenvolve o processo é fundamental para a identificação dos eventos de riscos que possam impactar na consecução dos seus objetivos. Para a análise do contexto, devem ser consideradas as informações a seguir:

- a) *Objetivos da Processo*: deve-se verificar se os objetivos dos processos analisados na unidade (ou do macroprocesso) foram estabelecidos e comunicados entre os servidores. Deve-se registrar o objetivo geral e específicos do processo em análise, sempre que possível. O registro dos objetivos, em consonância com o conhecimento do direcionamento estratégico da Universidade, permite uma melhor identificação de eventos de riscos que prejudicam a realização dessas atividades.
- b) *Ambiente Interno*: deve-se verificar a existência de programa de integridade e de código de ética ou código de conduta na Instituição; das competências e

disponibilidade dos recursos humanos existentes e a forma como estes são organizados e como suas responsabilidades são delegadas; verificar também a existência de planos e políticas associadas às atividades desenvolvidas. As orientações da Auditoria Interna também devem ser registradas sempre que possível, como auxílio para compreensão do ambiente interno. Todas essas informações podem ser avaliadas do ponto de vista do macroprocesso ou processo em análise.

- c) *Ambiente externo*: deve-se verificar a existência de orientações ou acórdãos de órgãos de controle externo (CGU e TCU, por exemplo), relacionados ao macroprocesso ou ao processo analisado. Também é adequado o entendimento do contexto econômico, político e social em que se insere o órgão/unidade analisada.

É sugerida ainda a utilização de ferramentas de análise de ambiente (como Análise de SWOT) para identificar os pontos fortes e fracos relacionados à execução do processo em análise bem como identificar as possíveis influências do ambiente externo na execução do processo (oportunidade e ameaças).

#### Crerios

Os critérios de riscos utilizados nessa metodologia estão apresentados ao longo das etapas seguintes, onde são definidas as categorias de riscos, as escalas de probabilidade e impacto e o nível de risco definido pela Instituição.

### ***Etapa 3 – Processo de Avaliação de Riscos***

#### Identificação de Riscos

O risco é definido como a possibilidade de que um evento ocorra e afete, positivamente (risco positivo ou oportunidade) ou negativamente (risco negativo), o cumprimento dos objetivos da Instituição, sendo avaliado em termos de impacto e de probabilidade (PGRC/UFS).

A presente etapa, portanto, tem a finalidade identificar e registrar os eventos de riscos que comprometem (ou colaborem) o alcance do objetivo dos processos definidos na *Etapa 2*, além das causas e consequências de cada um dos riscos no andamento das

atividades<sup>8</sup>. Esse procedimento deve ser realizado pela unidade executiva de gestão de riscos em conjunto com os servidores designados para esse fim.

Dessa forma, a equipe designada para a identificação dos riscos deverá seguir os seguintes procedimentos:

- a) A partir dos processos definidos na *Etapa 2*, deve-se registrar todos os subprocessos/atividades que são desenvolvidas para alcançar o objetivo geral estabelecido para o processo;
- b) Com base nos subprocessos/atividades, deve-se identificar e registrar os eventos de risco (negativos ou positivos) que podem comprometer ou colaborar com a execução das atividades registradas no item anterior.

Os eventos de riscos podem ser identificados a partir de perguntas como (ver anexo 1)<sup>9</sup>:

- a) Quais são os eventos de riscos que podem comprometer (atrasar, prejudicar) a execução das atividades do projeto?
- b) Quais são os eventos de riscos que podem impedir que o objetivo do projeto seja alcançado?

Identificado os riscos, estes deverão ser categorizados conforme estabelecido na PGRC/UFS e descritos a seguir:

Quadro 1: Categoria dos Eventos de Riscos

<b>Categoria do risco</b>	<b>Descrição do evento de risco</b>
Estratégico	Eventos que ameacem diretamente os objetivos estratégicos organizacionais, afetando o alcance da sua visão e a sustentabilidade da instituição no longo prazo
Financeiros/Orçamentários	Eventos que podem comprometer a capacidade da UFS de contar com os recursos orçamentários e financeiros necessários à realização de suas atividades, ou eventos

<sup>8</sup> Para cada processo a ser analisado, existem diversos subprocessos ou atividades que são realizados a fim de alcançar os objetivos estabelecidos.

<sup>9</sup> O anexo 1 apresenta um conjunto de questões para a identificação dos riscos inerentes aos subprocessos/atividades do setor. Esse questionário deve ser apresentado para a equipe de mapeamento de riscos a fim de orientar o levantamento das informações necessárias para o cumprimento dessa etapa.

	que possam comprometer a própria execução orçamentária;
Operacionais	Eventos que podem comprometer as atividades da UFS, normalmente associados a falhas, deficiência ou inadequação de processos internos, de pessoas, de infraestrutura e de sistemas;
Legal/De Conformidade	Eventos derivados de alterações legislativas ou normativas que podem comprometer as atividades da UFS;
Imagem/Reputação	Eventos que podem comprometer a confiança da sociedade (ou de parceiros e fornecedores) em relação à capacidade da UFS em cumprir sua missão institucional;
Integridade	Eventos relacionados à corrupção, fraudes, irregularidades e/ou desvios éticos e de conduta que podem comprometer os valores e padrões preconizados pela UFS.

Esses procedimentos permitirão a identificação e categorização dos riscos envolvidos na execução do processo examinado.

No entanto, é necessário ainda o reconhecimento das causas que geram esses riscos e as consequências que tais riscos podem trazer para a execução do processo. Essas informações serão necessárias para o tratamento dos riscos nas etapas posteriores.

Para esse fim é necessário que a equipe de mapeamento de riscos busque respostas para os seguintes questionamentos (ver Anexo1):

- a) Quais são as causas que levam a ocorrência do evento de risco? (Identificação das causas).
- b) O que pode acontecer no andamento do processo se o evento de risco acontecer? (Identificação das consequências).

O levantamento de todas essas informações será feito pela aplicação do questionário (Anexo 1) junto à equipe de mapeamento de riscos designada para esse fim

e pela realização de reuniões para discussão, consolidação e registro das informações em sistema eletrônico<sup>10</sup>.

#### Análise de Riscos

O propósito dessa etapa é a compreensão da natureza dos riscos identificados e suas características, determinando o *nível de riscos* a que está sujeito o processo em análise.

A análise de riscos é um procedimento que permite identificar a necessidade e a prioridade no tratamento dos riscos a partir da atribuição de pesos relacionados tanto ao impacto (I) que o risco causa na consecução dos objetivos do processo como à probabilidade (P) que esse evento de riscos realmente se realize. Dessa combinação de fatores é computado o nível de risco (NR) a que está sujeito o processo em seus eventos de risco.

Há que se considerar ainda que o nível de risco deverá ser computado em duas situações assim classificadas:

- a) *Risco inerente*: risco a que uma organização está exposta sem considerar quaisquer ações gerenciais que possam reduzir a probabilidade de sua ocorrência ou seu impacto. (Art. 2º, XIV, IN Conjunta MP/CGU Nº 01/2016);
- b) *Risco residual*: risco a que uma organização está exposta após a implementação de ações gerenciais para o tratamento do risco (Art. 2º, XV, IN Conjunta MP/CGU Nº 01/2016).

Portanto a realização desta etapa ocorrerá em três fases:

#### ***Fase 1 - Cálculo do Risco Inerente***

Para essa fase, a equipe de mapeamento de riscos deverá atribuir uma pontuação para cada evento de risco identificado com base nas questões abaixo destacadas:

- i. ***Em uma escala de 1 a 5 qual é a possibilidade (probabilidade) de o evento de risco mapeado acontecer?*** A resposta para essa questão, deve ser baseada no quadro 2, abaixo:

---

<sup>10</sup> A UFS adota o Sistema ForRisco como plataforma de registro e monitoramento dos riscos mapeados nas unidades.

Quadro 2: Escala de Probabilidades de o evento de risco ocorrer

Nota	Probabilidade	Descrição da probabilidade
1	Muito baixa	<b>Improável.</b> Em situações excepcionais, o evento poderá até ocorrer, mas nada nas circunstâncias indica essa possibilidade.
2	Baixa	<b>Rara.</b> De forma inesperada ou casual, o evento poderá ocorrer, pois as circunstâncias pouco indicam essa possibilidade.
3	Média	<b>Possível.</b> De alguma forma, o evento poderá ocorrer, pois as circunstâncias indicam moderadamente essa possibilidade.
4	Alta	<b>Provável.</b> De forma até esperada, o evento poderá ocorrer, pois as circunstâncias indicam fortemente essa possibilidade.
5	Muito Alta	<b>Praticamente certa.</b> De forma inequívoca, o evento ocorrerá, as circunstâncias indicam claramente essa possibilidade.

Fonte: TCU, 2018 (Adaptado)

- ii. *Se o evento de risco acontecer, qual é o impacto desse evento no alcance dos objetivos do processo?* A resposta a essa questão também resulta em níveis de impacto que podem variar de 1 (impacto insignificante) a 5 (impacto catastrófico), conforme escala abaixo:

Quadro 3: Escala de Impacto se o risco ocorrer

Nota	Impacto	Descrição do Impacto
1	Muito Baixo	<b>Mínimo</b> impacto no alcance do objetivo do processo.
2	Baixo	<b>Pequeno</b> impacto no alcance do objetivo do processo.
3	Médio	<b>Moderado</b> impacto nos objetivos do processo, porém recuperável.
4	Alto	<b>Significativo</b> impacto nos objetivos do processo e de difícil reversão.
5	Muito Alto	<b>Catastrófico</b> impacto nos objetivos do processo, de forma irreversível.

Fonte: TCU, 2018 (Adaptado)

Finalmente, com base nas pontuações atribuídas à probabilidade e ao impacto do risco, o resultado do Nível de Risco (NR) será dado por:

$$NR = I \times P$$

O resultado do NR classifica os riscos associados ao processo, conforme quadro abaixo:

Quadro 4: Escala de Nível de Risco

Nível de Risco	Pontuação
Risco Baixo – RB	0 a 4
Risco Médio – RM	5 a 11
Risco Alto – RA	12 a 19
Risco Extremo - RE	20 a 25

Assim, é possível registrar e documentar a matriz de riscos representativa da análise dos riscos identificados, conforme esquema abaixo:

**Matriz de Riscos da UFS**

<b>IMPACTO</b>	<b>Muito Alto</b>	5 RM	10 RM	15 RA	20 RE	25 RE
	<b>Alto</b>	4 RB	8 RM	12 RA	16 RA	20 RE
	<b>Médio</b>	3 RB	6 RM	9 RM	12 RA	15 RA
	<b>Baixo</b>	2 RB	4 RB	6 RM	8 RM	10 RM
	<b>Muito Baixo</b>	1 RB	2 RB	3 RB	4 RB	5 RM
	<b>Muito Baixa</b>	<b>Baixa</b>	<b>Médi a</b>	<b>Alta</b>	<b>Muito Alta</b>	
						<b>PROBABILIDADE</b>



Calculado o risco inerente a equipe de mapeamento de riscos deve partir para identificação de controles existentes nos processos avaliados. Parte-se então para a 2ª fase dessa etapa.

***Fase 2 - Identificação dos Controles:***

Nessa fase, deve-se avaliar o desenho e operacionalidade dos controles existentes (se houver) nos eventos de riscos identificados. A equipe deve identificar quanto ao desenho dos controles, se:

- a) Não há procedimento de controle;
- b) Há procedimentos de controles, mas não são adequados e nem estão formalizados;
- c) Há procedimentos de controles formalizados, mas não estão adequados (insuficientes);
- d) Há procedimentos de controles adequados (suficientes), mas não estão formalizados;
- e) Há procedimentos de controles adequados (suficientes) e formalizados.

E quanto à operação desses controles, se:

- a) Não há procedimentos de controle;
- b) Há procedimentos de controle, mas não são executados;
- c) Os procedimentos de controle estão sendo parcialmente executados;
- d) Os procedimentos de controle são executados, mas sem evidência de sua realização;
- e) Procedimentos de controle são executados e com evidência de sua realização.

***Fase 3 - Cálculo do Risco Residual:***

Nessa fase, a equipe de mapeamento dos riscos deve indicar novas pontuações para a probabilidade e o impacto do risco após a identificação dos controles e o resultado da avaliação quanto ao desenho e à operação destes. Esse cálculo permitirá identificar a viabilidade dos controles adotados até o momento.

Existem situações nas quais a verificação do risco inerente se torna inviável. Isto ocorre quando não é possível realizar de forma objetiva a separação entre processo e controle. Nessas situações excepcionais, pode-se considerar a fase I prejudicada (cálculo do risco inerente) e realizar apenas o cálculo do risco residual. Tais situações devem ser avaliadas pela equipe de mapeamento de riscos.

### Avaliação de Riscos

Essa etapa requer a tomada de decisões para priorização e tratamento dos riscos a partir da avaliação dos resultados observados na matriz de riscos. Os resultados da matriz permitem identificar quais riscos devem ser evitados, reduzidos, compartilhados ou mesmo acatados como inerentes ao desenvolvimento do processo.

Para esse fim, deve-se utilizar o quadro de critérios para priorização e tratamento dos riscos estabelecidos pelo TCU (2018), em conjunto com o apetite ao risco definido pela Universidade.

Quadro 5: Critérios para Priorização e Tratamento dos Riscos

<b>Nível de Risco</b>	<b>Critérios</b>
<b>Risco Extremo - RE</b>	<b>Nível de risco muito além do apetite a risco da UFS.</b> Qualquer risco nesse nível deve ser comunicado ao Comitê Institucional de Governança e ao dirigente máximo da unidade. Postergação de medidas para tratamento do risco só com autorização do Comitê Institucional de Governança da UFS.
<b>Risco Alto – RA</b>	<b>Nível de risco além do apetite a risco.</b> Qualquer risco nesse nível deve ser comunicado ao dirigente máximo da unidade e ter uma ação tomada em período determinado. Postergação de medidas só com autorização do dirigente máximo da unidade.
<b>Risco Médio – RM</b>	<b>Nível de risco dentro do apetite a risco.</b> Geralmente nenhuma medida especial é necessária, porém requer atividades de monitoramento específicas e atenção da unidade na manutenção de respostas e controles para manter o risco nesse nível, ou reduzi-lo sem custos adicionais.
<b>Risco Baixo – RB</b>	<b>Nível de risco dentro do apetite a risco,</b> mas 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.

Essas informações deverão ser documentadas pela unidade executiva de gestão de riscos e enviadas ao gestor de processo organizacional (proprietário do risco) e ao dirigente da unidade após a finalização do mapeamento.

#### ***Etapa 4 – Tratamento de Riscos***

A equipe de gerenciamento de riscos deverá identificar opções que possam modificar os riscos que se encontram acima do nível de apetite ao risco definido pela Universidade. As opções devem ser pensadas no sentido de reduzir o impacto ou a probabilidade (ou ambos) dos riscos identificados. Para isso, devem ser produzidos planos de tratamento que sugiram adoções de medidas de controles mais eficientes ao processo.

Um Relatório de Implementação de Controles deve ser elaborado pela unidade executiva de gestão de riscos juntamente com a equipe de mapeamento, com sugestões de ações necessárias para adequar os níveis de riscos, por meio da adoção de novos controles ou a otimização dos controles já existentes.

As ações propostas devem ser registradas, orientando-se pelas seguintes informações:

- a. *Controles Propostos/Ações Propostas*: registrar controles ou ações para responder ao evento de risco;
- b. *Tipo de controle proposto/ Ação Proposta*: preventivo (atua na causa), corretivo (atenua o efeito) ou compensatório (mitiga eventos de risco temporariamente até a implementação de controle definitivo);
- c. *Objetivo do Controle Proposto/ Ação Proposta*: melhorar o controle existente ou adotar controle novo;
- d. *Área responsável pela implementação do controle proposto/ ação proposta*: informar a coordenação/diretoria responsável pelo controle;
- e. *Responsável pela implementação do controle proposto/ ação proposta*: gestor do processo ou servidor designado;
- f. *Como será implementado*: informar se por meio de projeto, melhoria no sistema, criação de norma, plano de contingência, etc;
- g. *Intervenientes*: outras áreas e servidores intervenientes na ação;
- h. *Data do início*: informar data prevista para início da implementação dos controles;
- i. *Data da conclusão*: informar data prevista para a conclusão.

#### ***Etapa 5 - Monitoramento e análise crítica***

O Mapa de Risco será a principal ferramenta de monitoramento do processo de gestão de riscos. Além dele, a elaboração do Relatório de Implementação de Controles

será de suma importância para o acompanhamento dos trabalhos realizados pela unidade executiva de gestão de riscos.

A implementação dos controles deve ser continuamente avaliada no que diz respeito ao seu desenho e operação. Essa avaliação deverá ser efetuada, inicialmente, pelo gestor de processo organizacional, de uma forma contínua, assegurando que o controle esteja presente e funcionando (primeira linha de defesa).

No monitoramento, deverão ser verificados se os controles estão menos eficazes ou obsoletos ou mesmo não estão sendo aplicados na forma como foram criados, tomando-se insuficientes para mitigar o risco (segunda linha de defesa). Também deverão ser utilizadas reclamações e denúncias registradas na ouvidoria da Universidade, relatórios, recomendações ou demandas da Auditoria Interna, Controladoria Geral da União e do Tribunal de Contas da União, como fontes de controles (terceira linha de defesa).

#### ***Etapa 6 - Registro e Relato***

Por fim, a unidade executiva de gestão de riscos da UFS, em conjunto com as unidades mapeadas, deve desenvolver um relatório sobre a gestão de riscos e controles da unidade, com as seguintes informações:

- a) Apresentação da unidade avaliada;
- b) Informações dos processos avaliados e o período de avaliação;
- c) Os riscos identificados e analisados;
- d) As medidas de tratamento dos riscos;
- e) A avaliação e o plano de implementação dos controles;
- f) Conclusão;

Cabe à unidade de gestão de riscos e controles produzir periodicamente relatórios gerenciais das unidades monitoradas e encaminha-los ao Comitê de Gestão de Riscos e Controles. A unidade executiva também deverá emitir relatório final do exercício (Relatório Anual de Gerenciamento de Riscos e Controles) para emissão de parecer pelo CGRC.

O relatório final do exercício, juntamente com o parecer do CGRC, será encaminhado ao Comitê Institucional de Governança/CIG para apreciação.

## **6. PLANO DE AÇÃO**

Este Plano de Gestão de Riscos e Controles será executado em etapas contínuas dentro do período de vigência do Plano de Desenvolvimento Institucional da UFS. Assim, o gerenciamento de riscos deverá ser implementado de forma gradual em todas as áreas da Universidade, iniciando no nível operacional e, conforme o amadurecimento na gestão de riscos, passando para o nível tático e estratégico.

Devem ser priorizados os processos e Unidades Organizacionais que impactam diretamente no atingimento dos objetivos estratégicos definidos no Plano de Desenvolvimento Institucional.

O Comitê Institucional de Governança deverá aprovar e supervisionar método de priorização de temas e macroprocessos para gerenciamento de riscos e implementação dos controles da gestão (Art. 9º, XVII, da Resolução 15/2020/CONSU).

O seguinte cronograma de ação estabelece as medidas para a implementação deste Plano no período 2021/2022:

AÇÃO	UNIDADES ENVOLVIDAS	META	PERIODICIDADE	PRAZO
Levantamento de processos organizacionais para gerenciamento de riscos com base nos objetivos estratégicos do PDI	Unidade de Gestão de Riscos e Controles / Pró-Reitorias/Campi/Centros	Selecionar unidades prioritárias e definir processos organizacionais para o gerenciamento de riscos no exercício.	Semestral	- Novembro de 2021 - Maio de 2022 - Novembro de 2022
Aprovação do cronograma de gestão de riscos nas unidades organizacionais	Unidade de Gestão de Riscos e Controle / Comitê de Gestão de Riscos e Controles (CGRC)	Aprovar o cronograma de atividades para a gestão de riscos nas unidades selecionadas.	Semestral	- Dezembro de 2021 - Junho de 2022 - Dezembro de 2022
Capacitação e/ou sensibilização de servidores em Gestão de Riscos	Unidade de Gestão de Riscos e Controles	Apresentar à PROGEP oferta de curso de capacitação em gestão de riscos e proceder com ações de sensibilização dos servidores das unidades a serem mapeadas.	Semestral	- Dezembro de 2021 - Julho de 2022 - Dezembro de 2022
Gerenciamento de riscos nos processos organizacionais	Unidade de Gestão de Riscos e Controles/ Unidades responsáveis pelos processos selecionados	Executar o gerenciamento de riscos e apresentar relatórios gerenciais (e relatório final do	Semestral	- Julho de 2022 - Dezembro de 2022 (Relatório final do exercício)

		exercício) das unidades organizacionais previstas no cronograma aprovado pelo CGRC.		
Gerenciamento de riscos de integridade	Unidade de Gestão de Riscos e Controles / Unidade de Gestão da Integridade	Elaborar relatório gerencial de riscos à integridade da UFS a partir da execução das ações de gestão de riscos previstas no Plano de Integridade	Semestral	- Julho de 2022 - Dezembro de 2022
Aprovação do cronograma de ações para gerenciamento de riscos nos objetivos estratégicos (PDI)	Comitê de Gestão de Riscos e Controles (CGRC) / Comitê Institucional de Governança (CIG)	Definir os objetivos estratégicos prioritários para a gestão de riscos e elaborar cronograma de ação para gerenciamento de riscos estratégicos da UFS.	Anual	- Julho de 2022
Gerenciamento de riscos nos objetivos estratégicos selecionados (PDI)	Unidade de Gestão de Riscos e Controles/ Unidades envolvidas nos objetivos estratégicos	Elaborar relatório gerencial de riscos estratégicos da UFS a partir do gerenciamento de riscos dos objetivos estratégicos aprovados pelo Comitê Institucional de Governança.	Anual	- Dezembro de 2022
Gerenciamento de riscos dos processos de compras e contratações (IN 05/2017 e IN 01/2019)	Unidade de Gestão de Riscos e Controles/COPCON/Equipes de planejamento das contratações	Elaborar relatório gerencial de riscos das contratações da UFS a partir do assessoramento e acompanhamento dos mapas de riscos elaborados pelas equipes de planejamento das contratações.	Semestral	- Janeiro de 2022 - Julho de 2022 - Dezembro de 2022
Monitoramento e controle dos riscos identificados (Sistema ForRiscos)	Unidade de Gestão de Riscos e Controles/ Unidades responsáveis pelos riscos	Acompanhar periodicamente os controles estabelecidos (conforme prazos definidos no próprio sistema de gestão de riscos) e registrar o monitoramento dos riscos identificados nas unidades.	Mensal	- Janeiro a Dezembro de 2022.

## **7. SISTEMA DE MONITORAMENTO DE RISCOS**

A UFS adotará o Sistema ForRiscos como ferramenta tecnológica para o monitoramento e o controle dos riscos da Instituição. Esta ferramenta é parte de uma plataforma ofertada pelo Ministério da Educação (PlataformaFor)<sup>11</sup> que integra o Plano Estratégico das Instituições Federais de Ensino (ForPDI) à gestão de riscos das Instituições.

A adesão ao sistema contemplará o acompanhamento dos riscos e controles previstos nesse plano e permitirá aos setores o contínuo monitoramento dos riscos tendo em vista ser uma plataforma de livre acesso aos servidores cadastrados. A comunicação e a consulta também serão permitidas pela geração de relatórios gerenciais disponíveis na própria ferramenta.

## **8. CONCLUSÃO**

A gestão de risco configura-se como importante ferramenta de gestão para a identificação de possíveis eventos que possam impactar negativamente no alcance dos objetivos institucionais. Permite às instituições administrar de forma mais eficiente as incertezas inerentes a qualquer ação organizacional, maximizando os valores institucionais estabelecidos pela Universidade.

Portanto, com a implementação do presente Plano de Gestão de Riscos e Controles, a Universidade Federal de Sergipe pretende seguir com o aperfeiçoamento dos seus serviços, garantindo à sociedade a eficiência administrativa e o zelo aos recursos públicos utilizados em seus processos de trabalho.

---

<sup>11</sup> Ver <https://www.gov.br/mec/pt-br/plataformafor>.