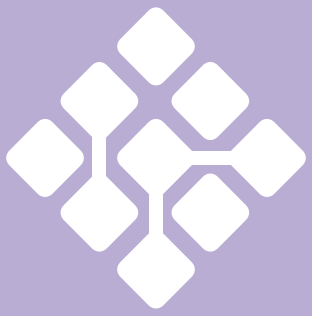


ForRisco

2ª edição

2ª Edição

Versão revisada e atualizada: alteração de formato, paginação e revisão na diagramação.

ForRisco: gerenciamento de riscos em instituições públicas na prática/Paulo Henrique de Souza Bermejo *et al*.

Brasília/DF: Editora Evobiz, 2019.

2ª edição

200 p.; 16x23cm
Contém bibliografia

1. Gestão de riscos - instituições públicas. 2. Gerenciamento de riscos na prática. 3. Metodologia para gerenciamento de risco. 4. Plataforma de software para gerenciamento de risco. 5. ForRisco. I. Bermejo, Paulo Henrique de Souza. II. Sant'Ana, Tomás Dias. III. Salgado, Eduardo Gomes. IV. Mendonça, Lucas Cezar. V. Anjos, Fábio Henrique dos. VI. Alves, Gustavo de Freitas. VII. Borges, Guilherme Henrique Alves. VIII. Pagotto, Daniel do Prado. IX. Pagliares, Rodrigo Martins. X. Pinheiro, Iara Ferreira. XI. Salomão, Inessa Laura. XII. Silva, Priscila Daniel de Paiva Gama. e XIII. Neves, Thiago José Galvão das.

ISBN: 978-85-53102-05-1

ForRisco

2ª edição

ForRisco:
gerenciamento de riscos em instituições públicas na prática

Sistema **For**

Ficha técnica

Autores

Paulo Henrique de Souza Bermejo, Dr.
Tomás Dias Sant'Ana, Me.
Eduardo Gomes Salgado, Dr.
Lucas Cezar Mendonça, Me.
Fábio Henrique dos Anjos, Me.
Gustavo de Freitas Alves, Me.
Guilherme Henrique Alves Borges, Me.
Daniel do Prado Pagotto, Me.
Rodrigo Martins Pagliares, Dr.
Iara Ferreira Pinheiro, Me.
Inessa Laura Salomão, Dra.
Priscila Daniel de Paiva Gama e Silva, Esp.
Thiago José Galvão das Neves, Me.

Apresentação dos autores

Paulo Henrique de Souza Bermejo

Doutor em Engenharia e Gestão do Conhecimento pela Universidade Federal de Santa Catarina (UFSC), com pós-doutorado em Inovação pela Universidade Bentley (EUA). Atualmente é professor associado do Departamento de Administração da Universidade de Brasília (UnB), coordenador do Núcleo de Pesquisa e Desenvolvimento para Excelência e Transformação do Setor Público (NEXT) da UnB e docente permanente do Programa de Pós-Graduação em Administração (mestrado e doutorado acadêmicos) e do Mestrado Profissional em Administração Pública, ambos da UnB.
Contato: paulobermejo@next.unb.br

Tomás Dias Sant'Ana

Doutorando em Administração pela Universidade de Brasília (UnB). Mestre em Ciência da Computação pela Universidade de São Paulo (USP). Atualmente é professor adjunto do Departamento de Ciência da Computação da Universidade Federal de Alfenas (UNIFAL-MG). Foi pró-reitor de Planejamento, Orçamento e Desenvolvimento Institucional entre 2010 e 2018 na UNIFAL-MG.
Contato: tomas@bcc.unifal-mg.edu.br

Eduardo Gomes Salgado

Doutor em Engenharia Mecânica pela Universidade Estadual Paulista (UNESP), com pós-doutorado pela University of Glasgow no Adam Smith Business School (Reino Unido). Mestre em Engenharia de Produção e graduado em Engenharia de Produção-Mecânica pela Universidade Federal de Itajubá (UNIFEI). Atualmente é professor e pró-reitor adjunto de Planejamento, Orçamento e Desenvolvimento Institucional na Universidade Federal de Alfenas (UNIFAL-MG).
Contato: eduardosalgado@bcc.unifal-mg.edu.br

Lucas Cezar Mendonça

Mestre em Administração Pública pela Universidade Federal de Lavras (UFLA), é pós-graduado em Finanças Corporativas pelo Centro Universitá-

rio do Sul de Minas (UNIS-MG). Graduado em Ciências Econômicas pela Faculdade Cenecista de Varginha (FACECA). Atualmente é pró-reitor de Planejamento, Orçamento e Desenvolvimento Institucional na Universidade Federal de Alfenas (UNIFAL-MG).
Contato: lucas.mendonca@unifal-mg.edu.br

Fábio Henrique dos Anjos

Mestre em Gestão Pública pela Universidade Federal de Alfenas (UNIFAL-MG). Bacharel em Administração pela Universidade Federal de Lavras (UFLA). Foi professor substituto no curso de Administração Pública do Instituto de Ciências Sociais Aplicadas da UNIFAL-MG – campus Varginha. Atualmente é Analista de Planejamento e Gestão Sênior no Projeto ForRisco e pesquisador no Núcleo de P&D para Excelência e Transformação do Setor Público (NExT) da UnB.
Contato: fabioanjos@next.unb.br

Gustavo de Freitas Alves

Doutorando em Administração pela Universidade de Brasília (UnB). Mestre em Computação Aplicada com ênfase em Gestão de Riscos também pela UnB. Bacharel em Ciência da Computação com ênfase em Redes de Computadores pela Universidade Católica de Brasília (UCB). Atualmente é consultor em Tecnologia da Informação e Gestão de Riscos.
Contato: gustavo.ucb@gmail.com

Guilherme Henrique Alves Borges

Mestre em Administração Pública pela Universidade Federal de Lavras (UFLA). Graduado em Sistemas de Informação pela mesma instituição. Especialista em gestão de processos e sistemas de gestão empresarial. Atualmente desempenha papel de gerente de empresa e projetos de software.
Contato: ghaborges@gmail.com

Daniel do Prado Pagotto

Mestre em Administração pela Universidade Federal de Goiás (UFG), com ênfase em empreendedorismo e inovação. Bacharel em Administração pela Universidade de Brasília (UnB), com período sanduíche na Kirkwood Community

College (EUA). Atualmente é pesquisador e líder de projeto no Núcleo de P&D para Excelência e Transformação do Setor Público (NExT) da UnB.
Contato: danielpagotto@next.unb.br

Rodrigo Martins Pagliares

Doutor em Ciências pelo Programa de Pós-Graduação em Engenharia Eletrônica e Computação do Instituto Tecnológico de Aeronáutica (ITA). Mestre em Ciência da Computação pela Universidade Federal de Santa Catarina (UFSC). Bacharel em Ciência da Computação pela Universidade Federal de Ouro Preto (UFOP). Atualmente é professor do curso de Bacharelado em Ciência da Computação da Universidade Federal de Alfenas (UNIFAL-MG), além de atuar como coordenador de desenvolvimento institucional na mesma instituição.
Contato: pagliares@bcc.unifal-mg.edu.br

Iara Ferreira Pinheiro

Mestre em Gestão e Avaliação da Educação Pública pela Universidade Federal de Juiz de Fora (UFJF). Pós-graduada em Controladoria e Finanças Empresariais pela Universidade Federal de Lavras (UFLA). Graduada em Ciências Contábeis pela Universidade de Brasília (UnB). Atualmente é servidora efetiva do Ministério da Educação, exercendo a função de subsecretária de Planejamento e Orçamento.
Contato: iarapinheiro@mec.gov.br

Inessa Laura Salomão

Doutora em Planejamento Energético pela Universidade Federal do Rio de Janeiro (UFRJ). Mestre em Engenharia de Produção pelo Instituto Alberto Luiz Coimbra de Pós-Graduação e Pesquisa em Engenharia (COPPE) e graduada em Ciências Econômicas pela Universidade de São Paulo (USP). Atualmente é professora adjunta do curso de Engenharia de Produção do Centro Federal de Educação Tecnológica Celso Suckow da Fonseca (CEFET/RJ).
Contato: inessa.salomao@cefet-rj.br

Priscila Daniel de Paiva Gama e Silva

Pós-graduada em Gestão Pública pela Faculdade Internacional Signorelli

e graduada em Administração pelo Centro Federal de Educação Tecnológica Celso Suckow da Fonseca (CEFET/RJ). Concursada, exerce o cargo de administradora no CEFET/RJ, onde atualmente ocupa a função de chefe do Departamento de Desenvolvimento Institucional.
Contato: priscila.paiva@cefet-rj.br

Thiago José Galvão das Neves

Mestre em Ciências Contábeis pela Universidade Federal de Pernambuco (UFPE). Especialista em Auditoria, Controladoria e Perícia Contábil pelo IBPEX. Graduado em Ciências Contábeis pela UFPE. Atualmente é pró-reitor de Planejamento, Orçamento e Finanças da UFPE, professor do curso de Especialização em Contabilidade e Controladoria Governamental, e contador da mesma instituição. É coordenador do Fórum Nacional de Pró-Reitores de Planejamento e de Administração das Instituições Federais de Ensino Superior (FORPLAD).
Contato: thiago.neves@ufpe.br

Associação Nacional dos Dirigentes das Instituições Federais de Ensino Superior
ANDIFES/BRASIL

Reinaldo Centoducatte (UFES)
Presidente

João Carlos Salles Pires da Silva (UFBA)
1º Vice-presidente

Margarida de Aquino Cunha (UFAC)
Suplente

Edward Madureira Brasil (UFG)
2º Vice-presidente

Cleuza Maria Sobral Dias (FURG)
Suplente

Gustavo Henrique de Sousa Balduino (ANDIFES)
Secretário executivo

Fórum Nacional dos Pró-Reitores de Planejamento e Administração das Instituições Federais de Ensino Superior

FORPLAD/IFES/BRASIL

Thiago José Galvão das Neves (UFPE)
Coordenador nacional
(Novembro/2017 – Novembro/2019)

Vilson Ongaratto (UTFPR)
1° Vice-coordenador

Tânia Mara Francisco (UNIFESP)
2ª Vice-coordenadora

Dulce Maria Tristão (UFMS)
1ª Secretária

Kleomara Gomes Cerquinho (UFAM)
2ª Secretária

Comissão de Administração

Inessa Laura Salomão (CEFET/RJ)
Coordenadora

Wilma Gomes Silva Monteiro (UNIFAP)
Vice-coordenadora

Comissão de Planejamento e Avaliação

Raquel Trindade Borges (UFPA)
Coordenadora

Pedro Fiori Arantes (UNIFESP)
Vice-coordenador

Grupo de Trabalho do Projeto ForRisco

Vander Matoso (UFGD)
Coordenador da Comissão de Administração

Joeder Campos Soares (UFSM)
Coordenador da Comissão de Planejamento e Avaliação

Membros do grupo de trabalho

Alessandra Dahmer
Universidade Federal de Ciências da Saúde de Porto Alegre (UFCSPA)
Alex Fraga
Universidade Federal da Grande Dourados (UFGD)
Álvaro Fabiano Pereira de Macedo
Universidade Federal Rural do Semi-Árido (UFERSA)
Aluízio Mário Lins Souto
Universidade Federal da Paraíba (UFPB)
Anailson Márcio Gomes
Universidade Federal do Rio Grande do Norte (UFRN)
André Macedo Santana
Universidade Federal do Piauí (UFPI)
Auton Peres de Farias Filho
Universidade Federal do Acre (UFCA)
Carlece Carvalho Duarte
Universidade Federal de Roraima (UFRR)
Carolina Guimarães Raposo
Universidade Federal Rural de Pernambuco (UFRPE)
Darizon Alves de Andrade
Universidade Federal de Uberlândia (UFU)
Deylon Gomes de Moraes
Universidade Federal do Tocantins (UFT)
Edson Nascimento
Universidade Federal do Maranhão (UFMA)
Eunice Alves de Oliveira
Universidade Federal de Roraima (UFRR)
Fernando Costa Archanjo
Universidade Federal dos Vales do Jequitinhonha e Mucuri (UFVJM)
Fernando Marinho Mezzadri
Universidade Federal do Paraná (UFPR)
Frank Leonardo Casado
Universidade Federal de Santa Maria (UFSM)
Jailton Gonçalves Francisco
Universidade Federal Fluminense (UFF)

Equipe de execução do Projeto ForRisco

Bruno Augusto Terra
Cléber Monterani Tavares
Daniel do Prado Pagotto
Débora Silva Barroso de Araújo
Diogo Guilherme Pereira
Edney Pereira Pinto
Eduardo Gomes Salgado
Everton Leonardo de Almeida
Fábio Henrique dos Anjos
Guilherme Henrique Alves Borges
Gustavo de Freitas Alves
Gustavo Soares Melo
Lucas Cezar Mendonça
Maik de Souza
Marcelo Cezar Costa
Marcelo Penha Fernandes
Paulo Henrique de Souza Bermejo
Pedro de Almeida Marques
Rebeca Nonato Domingos
Renato Resende Ribeiro de Oliveira
Romário da Silva Borges
Tomás Dias Sant'Ana
Vinícius Alex da Silva
Vinícius Nogueira da Silva
Wagner Vilas Boas de Souza

2ª Edição

Versão revisada e atualizada: alteração de formato, paginação e revisão na diagramação.

Lista de ilustrações

Lista de quadros

Lista de abreviaturas e siglas

ABNT	Associação Brasileira de Normas Técnicas
ANDIFES	Associação Nacional dos Dirigentes das Instituições Federais de Ensino Superior
APF	Administração Pública Federal
AP	Administração Pública
AUDIN	Auditoria Interna
BPM	Business Process Management
CBOK	Commom Body of Knowledge
CDI	Coordenadoria de Desenvolvimento Institucional
CEFET/RJ	Centro Federal de Educação Tecnológica Celso Suckow da Fonseca – Rio de Janeiro
CGRC	Comitê de Governança, Riscos e Controle
CGU	Controladoria-Geral da União
CGE	Coordenadoria-Geral
COBIT	Control Objectives for Information and Related Technologies
CODIR	Conselho Diretor
CONIF	Conselho Nacional das Instituições da Rede Federal de Educação Profissional, Científica e Tecnológica
COR	Coordenadoria de Orçamento
CPO	Coordenadoria de Projetos e Obras
COSO	Committee of Sponsoring Organizations of the Treadway Commission
CVM	Comissão de Valores Mobiliários
DEDIN	Departamento de Desenvolvimento Institucional
DIGES	Diretoria de Gestão Estratégica
DIPPG	Diretoria de Pesquisa e Pós-Graduação
DIRAP	Diretoria de Administração e Planejamento
DIREG	Direção-Geral
DIREN	Diretoria de Ensino
DIREX	Diretoria de Extensão
DSIC	Departamento de Segurança da Informação e Comunicações
ERM	Enterprise Risk Management
ETIR	Equipes de Tratamento e Respostas a Incidentes em Redes Computacionais
FACEPE	Fundação de Apoio à Cultura, Ensino, Pesquisa e Extensão de Alfenas

FDA	Food and Drug Administration's
FERC	Federal Energy Regulatory Commission
FMI	Fundo Monetário Internacional
FORPLAD	Fórum Nacional de Pró-Reitores de Planejamento e Administração
GIRC	Gestão de Integridade, Riscos e Controle Interno
GR	Gestão de Riscos
GRCORP	Gerenciamento de Riscos Corporativos
GRSIC	Gestão de Riscos de Segurança da Informação e Comunicação
IBGC	Instituto Brasileiro de Governança Corporativa
IFES	Instituição Federal de Ensino Superior
IFTO	Instituto Federal do Tocantins
ITIL	Information Technology Infrastructure Library
INC	Instrução Normativa Conjunta MP/CGU nº 01/2016
ISO	International Organization for Standardization
KPI	Key Performance Indicator
KRI	Key Risk Indicators
M_o_R	Management of Risks
MEC	Ministério da Educação
MGR-SISP	Metodologia de Gestão de Riscos de Segurança da Informação e Comunicações
MP	Ministério do Planejamento, Desenvolvimento e Gestão
MTP	Meios Técnicos Passivos
NEXT/UNB	Núcleo de P&D para Excelência e Transformação do Setor Público/ Universidade de Brasília
NBR	Norma Brasileira
NIST	National Institute of Standards and Technology
OCDE	Organização para Cooperação e Desenvolvimento Econômico
OGC	Office for Government Commerce
PDI	Plano de Desenvolvimento Institucional
PE	Plano Estratégico
PTRs	Plano de Tratamento de Riscos
RACI	*Responsible*, *Accountable*, *Consulted*, *Informed*
RH	Recursos Humanos
SETEC	Secretaria de Educação Profissional e Tecnológica
SIC	Segurança da Informação e Comunicação
SIEM	Security Information and Event Management
SISP	Sistema de Administração dos Recursos de Tecnologia da Informação

SOC	Security Operations Center
SOX	Sarbanes-Oxley
SWOT	*Strengths*, *Weakness*, *Opportunities*, *Threats*
TCU	Tribunal de Contas da União
TI	Tecnologia da Informação
UFLA	Universidade Federal de Lavras
UNB	Universidade de Brasília
UNIFAL-MG	Universidade Federal de Alfenas – Minas Gerais

Sumário

Prefácio

Com o advento da "nova gestão pública", ferramentas inovadoras precisam ser desenvolvidas para apoiar o processo decisório na Administração Pública, de forma a atender aos complexos desafios atuais.

Ressalta-se que o Sistema For, foco do presente livro, vem para colaborar exatamente nesse sentido, com o propósito de suportar as decisões dos gestores públicos sob a perspectiva gerencial de riscos, tendo como base as prioridades organizacionais.

Dessa forma, os autores definem o Sistema For como um conjunto de soluções que visam melhorias na gestão pública voltadas ao estímulo da cultura para inovação, ação estratégica e controle dos riscos organizacionais.

Para tanto, duas ferramentas foram desenvolvidas no âmbito do Sistema For:

- ForPDI, voltada para a gestão estratégica, visa acompanhar em tempo real, de forma colaborativa e eficiente, os resultados considerados prioritários pela organização; e
- ForRisco, destinada à gestão de riscos, tem como finalidade organizar e planejar recursos minimizando possíveis impactos negativos provindos de riscos organizacionais.

A riqueza de evidências positivas (vide os estudos de caso apresentados neste livro) não deixa dúvidas sobre as vantagens para os gestores públicos ao adotarem os métodos e as ferramentas propostos pelo Sistema For com vistas a melhorar os resultados organizacionais.

Portanto, a obra em questão é um convite provocativo para reflexões teóricas e inovadoras entre os estudiosos sobre a "nova gestão pública". Além disso, provém valor agregado e conhecimento técnico e gerencial aos gestores públicos para tratarem os riscos organizacionais com foco estratégico voltado ao atingimento dos resultados prioritários.

Welles Matias de Abreu
Diretor DRE/Ministério do Meio Ambiente

Prefácio

Governança, integridade, *compliance*, gestão de riscos... Nos últimos anos, temos sido bombardeados com esses termos que até pouco tempo atrás não eram usuais na Administração Pública.

Esses temas, que eram tratados apenas como boas práticas, constantes em recomendações de órgãos de controle, passaram a ser cobrados em normas e legislações infralegais, com destaque para a Instrução Normativa Conjunta MP/CGU nº 01/2016 e, mais recentemente, o Decreto nº 9.203/17, conhecido como "Decreto de Governança".

Diante de todas essas questões, e focando agora na gestão de riscos, objeto deste livro, é inevitável que os gestores tenham diversas dúvidas, a começar por uma que é bastante usual: precisamos mesmo disso?

Sim, precisamos! E muito!

Entretanto, para melhor entendermos a gestão de riscos (e principalmente estarmos de mente aberta para praticá-la), alguns pontos precisam ser desmitificados. Neste prefácio, gostaria de falar apenas de três.

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.

Um segundo mito é que a gestão de riscos aumentará os custos da organização. Em um cenário de grande restrição fiscal como o que estamos vivendo, é natural e louvável a preocupação com custo. Entretanto, isso não pode ser desculpa para a não implementação de uma boa gestão de riscos. Os benefícios decorrentes de um gerenciamento de riscos eficaz geralmente são muito maiores do que eventuais custos incorridos com a sua implementação. Os

ganhos começam desde a fase de identificação de riscos, que induz os gestores a repensarem os seus processos, otimizando-os até a fase de monitoramento, quando atividades podem ser priorizadas ou até mesmo deixar de ser feitas. Nesse sentido, a gestão de riscos é uma aliada na busca por redução de custos em uma organização, por meio da otimização de processos e priorização de demandas existentes.

Por fim, o terceiro mito é aquele que diz que a gestão de riscos vai engessar ainda mais os processos, pois trará mais controles. Aqueles que acreditam nesse mito são os que pensam que "isso é coisa de órgão de controle". Talvez por constar já há algum tempo nas recomendações contidas nos relatórios desses órgãos, muitos auditores pensam que a gestão de riscos apenas trará mais controles para a organização, engessando o processo e burocratizando em demasia o trabalho. Errado! Um bom gerenciamento de riscos fará com que os gestores conheçam melhor os seus processos e, consequentemente, o nível de risco envolvido nas atividades desenvolvidas. Isso permitirá, inclusive, que se retirem controles tidos como desnecessários, quando for o caso.

Esclarecidos alguns mitos, e partindo-se do pressuposto de que o gestor foi convencido da necessidade de implementar a gestão de riscos na sua organização, surge outra pergunta: ok, mas como fazer?

ForRisco!

De forma didática e com a bagagem adquirida a partir do ForPDI – Gestão de Plano Estratégico/PDI, o livro que tenho a honra de prefaciar aborda tudo o que o gestor precisa saber para começar a melhorar a maturidade em gestão de riscos da sua organização.

Nesta obra, você terá a oportunidade de entender melhor a motivação para que uma organização adote a gestão de riscos, ter contato com as estruturas conceituais sobre o tema, conhecer os principais marcos legais vigentes e, principalmente, "aprender a fazer" a partir de casos reais e da metodologia ForRisco.

Venha você também fazer parte do mundo da gestão de riscos. Sua organização agradece!

Prof. Me. Rodrigo Fontenelle
CGAP, CRMA, CCS

Prefácio

A forma de realizar a gestão pública vem sendo aprimorada ao longo dos anos. Desde a proposta de reforma administrativa que pregava uma aproximação da gestão pública com a privada e que culminou com a inclusão do Princípio da Eficiência no caput do artigo 37 da Carta Magna, têm-se buscado formas de se adotar a qualidade na prestação dos serviços públicos. Preceitos tais como eficácia, efetividade e eficiência têm ecoado cada vez mais alto no dia a dia do gestor público.

Diversas são as ferramentas utilizadas pela gestão privada no intuito de obter as suas metas e alcançar os seus objetivos. Ao longo do tempo, várias foram as tentativas de trazer os conceitos já sedimentados na esfera privada para dentro da pública, e muitas delas acabaram sendo deixadas de lado pelos atores e relegadas a modismos. Outras acabaram sendo implementadas e corroboraram uma melhora no cumprimento dos anseios administrativos. Contudo, ainda há muito para caminhar na busca por uma gestão pública de qualidade e que esteja dentro dos preceitos norteadores do interesse público.

Assim, outra onda surge e vem tomando conta dos debates técnicos dos pensadores da Administração Pública. Conceitos tais como governança, controle, risco, transparência e *accountability* passam a ser tratados nos documentos oficiais e discutidos nas agendas públicas. Os órgãos de controle são os primeiros a se debruçarem sobre tais assuntos por entenderem sua complexidade bem como seus benefícios para a atuação do gestor público.

Desde então, questionários, relatórios, acórdãos, instruções normativas e decretos vêm sendo utilizados a fim de levar tal discussão para dentro da esfera administrativa. A preocupação com o resultado e com a finalidade das ações da Administração Pública, assim como as responsabilizações por condutas que destoam da tônica ditada pelo interesse público, vem cada vez mais fazer com que os gestores busquem instrumentos que lhes auxiliem no difícil processo da tomada de decisão.

Nesse diapasão, a gestão de riscos surge para auxiliar o gestor na tomada de decisões, assim como para fornecer meios e elementos que permitam implantar ferramentas que contribuam para o atingimento das metas e dos objetivos

institucionais. Contudo, essa é uma cultura que deve ser assimilada e internalizada por toda a gestão, de tal sorte que não se veja a gestão de riscos como mais um modismo que será superado em breve. A diferença da gestão de riscos para outras ferramentas apresentadas no passado é que ela vem sendo aprimorada na iniciativa privada e inserida no ordenamento jurídico-administrativo por meio de normas que de certa forma impõem a sua adoção. Embora exista essa névoa da imposição, o que se almeja, na verdade, é demonstrar a relevância de se trabalhar sob uma atmosfera dinamicamente controlada e estruturada com foco na implementação e na otimização de controles que visam fornecer segurança razoável ao gestor para agir de uma forma mais eficiente, afastando-se de condutas que possam vir a impactar negativamente nos objetivos institucionais.

Foi então que, após a edição da Instrução Normativa Conjunta nº 01/2016, surgiu a ideia de se modular um sistema que pudesse auxiliar os órgãos da Administração Pública a efetivarem os seus gerenciamentos de risco. Iniciou-se, então, uma busca com o objetivo de se estabelecer uma metodologia baseada nos diversos modelos utilizados para o gerenciamento de riscos. Assim, *frameworks* de mercado como o COSO ICIF, o COSO ERM e a ISO 310000, o *framework* britânico Management of Risks M_o_R-OGC, conhecido como "*Orange Book*", voltado para a Administração Pública, assim como as metodologias da Administração Pública brasileira GIRC e MGR-SISP do Ministério do Planejamento e a metodologia do IBGC 2017, esta por propor a avaliação da maturidade da organização no que se refere à gestão de riscos, foram estudados para viabilizar a formatação da metodologia ForRisco.

Além das metodologias e dos *frameworks* mencionados, algumas ferramentas para identificação, avaliação e priorização de riscos são abordadas neste livro e também serviram de base para a tabulação do sistema e da metodologia ForRisco. Entre as inúmeras ferramentas sugeridas pelos documentos internacionais, foram abordados o mapa de riscos, os relatórios sumarizados, as comunicações e mensagens de alerta, a árvore de decisão, o brainstorming e a análise de cenários por meio da matriz SWOT.

O estabelecimento de uma metodologia-padrão que pudesse ser adotada por todos seria possível se estivéssemos inseridos em instituições com as mesmas características. Contudo, o que se observa é que o universo de peculiaridades e características próprias de cada órgão é imenso. Cada instituição, dentro da sua autonomia, desenvolve a sua administração em conformidade com as suas demandas locais e seguindo características próprias. Assim, qual-

quer tentativa de se tabular uma metodologia única não tem como prosperar. O que se objetiva ao traçar uma metodologia é mostrar o caminho de como seria possível a sua adoção, desde que devidamente adequada às realidades de cada instituição.

Posto isso, a apresentação das diversas estruturas integradas que estão no mercado, das ferramentas que podem ser utilizadas por cada instituição para identificar, avaliar e gerir seus riscos, assim como das metodologias adotadas por alguns órgãos públicos e da própria metodologia ForRisco, visa demonstrar que é possível a formatação de uma metodologia própria e a utilização da gestão de riscos para aprimorar os atos de gestão de tal sorte que as decisões passem a ser tomadas com base em uma concepção de risco. Esse aprimoramento dos atos de gestão corrobora o ideal de profissionalizar cada vez mais os órgãos administrativos, de modo que todas as decisões sejam mais bem fundamentadas em aspectos cada vez menos subjetivos. Claro que não se almeja eliminar por completo a subjetividade da tomada de decisões, até porque quem estabelece o apetite e a tolerância ao risco é o próprio gestor que assume a responsabilidade pelos atos. Contudo, quanto mais estruturada estiver a instituição e mais madura for a estrutura de gestão de riscos, maior a segurança da gestão, pois com os riscos mapeados é possível vislumbrar de forma mais clara as consequências de cada ato da gestão.

Com o intuito de confirmar a coerência das técnicas e dos métodos desenvolvidos no decurso do Projeto ForRisco, a equipe desenvolvedora confrontou a metodologia desenvolvida com a realidade prática das organizações. Para tanto, foram realizados estudos de caso em duas Instituições Federais de Ensino Superior (IFES), quais sejam: Universidade Federal de Alfenas – Minas Gerais (UNIFAL-MG); e Centro Federal de Educação Tecnológica Celso Suckow da Fonseca – Rio de Janeiro (CEFET/RJ). Da referida análise, foi possível avaliar o estabelecido até então e formatar alguns ajustes no intuito de auxiliar os demais gestores na adoção e na adequação às suas realidades tanto da metodologia quanto do sistema.

Dessa forma, por entender que a gestão de riscos é um caminho sem volta, até porque a sua adoção acabará por agregar valor à gestão, é que ferramentas gratuitas como a ForRisco devem ser fomentadas, pois auxiliarão os usuários a registrarem os seus dados de identificação de riscos, assim como viabilizarão um melhor gerenciamento desses dados. Como a gestão de riscos é dinâmica, cada ciclo de avaliação propiciará ao gestor uma visão crítica dos

seus processos e rotinas no intuito de estabelecer correções e aprimoramentos sempre sob a ótica da concretização dos seus objetivos da forma mais eficiente possível. Essa visão sistêmica das fragilidades e prováveis consequências dos atos corrobora o estabelecimento de ferramentas de controle cada vez mais otimizadas e que acabem por fornecer segurança razoável ao gestor no ato da tomada de decisões.

Assim, fortalecendo o que já foi dito, o propósito em se adotar a gestão de riscos não constitui um mero atendimento às demandas normativas, mas sim uma mudança cultural da gestão para a adoção de ferramentas que possam servir de apoio na consecução das suas atividades e no atingimento dos seus objetivos.

Jeferson Alves dos Santos
Auditor-chefe da UNIFAL-MG e presidente da Associação FONAI-MEC

Apresentação

O gerenciamento de riscos, tema central deste livro, permite ao leitor um despertar para uma percepção mais abrangente da realidade organizacional e o convida para reflexões sobre os benefícios de um bom planejamento e mapeamento dos processos gerenciados pela instituição. Apesar de o assunto ser relativamente novo no setor público brasileiro, vejo o gerenciamento de riscos como uma grande oportunidade de transformar o modelo de gestão utilizado por grande parte dos órgãos públicos.

Nesse sentido, um grupo de universidades públicas federais, por intermédio do Fórum Nacional de Pró-Reitores de Planejamento e Administração das Instituições Federais de Ensino Superior (FORPLAD) e do Núcleo de Pesquisa e Desenvolvimento para Excelência e Transformação do Setor Público (NExT) da Universidade de Brasília, resolveu contribuir para que os órgãos públicos federais, estaduais e municipais pudessem prestar um serviço público com mais eficiência, eficácia e efetividade. Do desejo de apoiar os gestores públicos e transformar a forma como são planejados e gerenciados os projetos e processos na Administração Pública, surgiu a ferramenta ForRisco.

Moderna, inovadora, de código aberto, adaptável às diversas realidades organizacionais e totalmente compatível com o sistema de planejamento estratégico também construído por esse grupo (ForPDI), a solução ForRisco é mais do que um novo sistema do Sistema For. Ela faz parte de um sonho de que seja possível, em um futuro muito próximo, ter políticas públicas que consigam demonstrar para a sociedade o quão efetivas podem ser as ações governamentais. Planejar, acompanhar e mitigar os riscos da não realização de seus objetivos pretendidos são os desafios que se tenciona com este livro e com os softwares do Sistema For.

Convido o leitor para um aprofundamento de conceitos e para o fomento de novas ideias transformadoras que irão contribuir com uma gestão pública cada vez mais justa, transparente, inclusiva e inovadora.

Thiago José Galvão das Neves
UFPE | Coordenador nacional

Núcleo de Pesquisa e Desenvolvimento para Excelência e Transformação do Setor Público – Universidade de Brasília **NExT/UnB**

Coordenados pelo professor Paulo Henrique de Souza Bermejo, somos um grupo de pesquisa e desenvolvimento interdisciplinar vinculado ao Departamento de Administração da Faculdade de Economia, Administração, Contabilidade e Gestão de Políticas Públicas (FACE) da Universidade de Brasília (UnB). A nossa equipe conta com pesquisadores, estudantes de graduação e pós-graduação especialistas em Administração Pública e está comprometida com a aplicação de metodologias e de técnicas científicas que visam promover a excelência e a transformação do setor público.

Nascemos com o ideal visionário de impulsionar a análise e a implantação efetiva de soluções inovadoras e de alto impacto nos serviços públicos e de nos aprofundarmos nesse processo. E como propósito desse ideal, queremos responder às mudanças diante dos novos paradigmas destacados pela Administração Pública brasileira, focada no cidadão cliente, demandante de uma maior oferta e de melhores serviços e políticas, e também na entrega de resultados aos cidadãos. Conheça a missão, a visão e os valores do NExT:

Missão:
- Oferecer soluções inovadoras que promovam a excelência e a transformação para produzir resultados e gerar valor em empresas e governos.

Visão:
- Ser reconhecido como líder nacional no desenvolvimento de soluções para inovação e eficiência na gestão empresarial e governamental.

Valores:
- Dinamismo, comprometimento e ousadia
- Respeito e simplicidade
- Reconhecimento e gratidão
- Eficiência e efetividade

Temos o compromisso com o desenvolvimento de estratégias e planejamento, com a gestão da inovação, com P&D para soluções específicas e reestruturação organizacional, e com o redesenho e a automatização de processos em empresas privadas e do setor público. Além disso, na condição de grupo de pesquisa, buscamos nos amparar na investigação de técnicas e de métodos para elaboração de planos estratégicos, em métodos ágeis para gestão da inovação, na automatização de programas estratégicos de inovação e na otimização de serviços baseados em inteligência artificial e em gestão do conhecimento.

O Ministério da Educação, o Ministério do Planejamento, o Superior Tribunal Militar, a Procuradoria-Geral da República, a Escola Nacional de Administração Pública, a Secretaria de Segurança Pública de Minas Gerais, a Universidade NOVA – Portugal e a Universidade de Bentley – EUA são alguns dos nossos clientes e parceiros. Mas é importante destacar também a parceria realizada entre o NExT/UnB e o FORPLAD, a UNIFAL-MG, a UFLA e outras instituições públicas para a construção deste livro, que, por meio da pesquisa e do desenvolvimento, acreditaram e acreditam na transformação positiva da Administração Pública no Brasil.

Tenha uma boa leitura!

1. Introdução

Indivíduos possuem percepção limitada sobre a realidade e, para lidar com esse fato, buscam reunir-se em grupos e organizações a fim de moldar comportamentos observáveis em padrões racionais ou modelos mentais, contribuindo para o cumprimento dos objetivos organizacionais. Uma organização é, ao mesmo tempo, um conjunto de propósitos articulados e de mecanismos estabelecidos direcionada para o alcance de resultados. A partir daí, constantemente modificam-se e refinam-se os mecanismos pelos quais se alcançam os seus propósitos, reorganizam sua estrutura e seus processos, papéis e relacionamentos [1].

Ao longo do tempo, diversas áreas do conhecimento, em especial aquelas das Ciências Sociais, têm buscado fundamentar o que se prova eficaz para o alcance dos objetivos nas organizações. Era de se esperar que as lições aprendidas em um setor pudessem ser transferidas para outro, formando uma teoria única das organizações. Entretanto, além de essa adaptação não ser fácil, estudiosos sugerem que diferenças entre setores – público ou privado, por exemplo – exigem métodos e práticas próprios de gestão [2–3]. Isso significa que, apesar de essas organizações possuírem estruturas fundamentalmente semelhantes, há distinções claras entre elas.

No paradigma da "nova gestão pública", é crescente a adoção de práticas gerenciais oriundas da administração privada. Tanto o setor público como o privado se beneficiam de modelos de gestão que contribuem para um conjunto de novos conhecimentos. Notadamente, é válido que as práticas de gestão, como a gestão de projetos, de processos, de serviços ou de riscos, possuam um corpo de conhecimento que pode ser aplicado em ambos os setores [4, 5]. Ao se destacar a gestão de riscos, observa-se um comportamento similar adotado nessas práticas de gestão, embora elas possuam peculiaridades devido à natureza de sua atividade. A prática de gestão de riscos possui no seu cerne a identificação e o tratamento de incertezas, de modo a não impactarem nos objetivos da organização [6].

Na Administração Pública (AP), as técnicas de gestão de riscos são incorporadas com a finalidade de aumentarem o controle interno e a governança. A Instrução Normativa Conjunta (INC) nº 01/2016, de 10 de maio de 2016, do

Ministério do Planejamento (MP) e da Controladoria-Geral da União (CGU), dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo Federal [7]. A INC deve ser adotada para que esses órgãos implantem medidas sistêmicas e práticas de gestão de riscos, e também está alinhada às melhores práticas de mercado relacionadas à gestão de riscos, a saber: COSO II, GRCorp e ISO 31000 [6, 8]. O MP também desenvolveu o seu próprio guia de gestão de riscos, por meio do Manual de Gestão de Integridade, Riscos e Controles Internos da Gestão (GIRC) [9], e a Metodologia de Gestão de Riscos de Segurança da Informação e Comunicações do Sistema de Administração dos Recursos de Tecnologia da Informação do Poder Executivo Federal – MGR-SISP [10].

O que se quer destacar é a importância em se adotar a gestão de riscos como método de gestão complementar para as organizações públicas. O gerenciamento dos riscos pode contribuir para um melhor desempenho organizacional por permitir controles e acompanhamentos sistêmicos dos riscos [11, 12 e 13]. Não obstante, as sociedades e os cidadãos urgem por maior efetividade na oferta dos serviços prestados pela AP. Além do mais, os gastos da AP precisam ser mais satisfatoriamente aplicados e gerenciados, e a cobrança por maior eficiência e gerenciamento dos recursos públicos traz à sociedade a responsabilização em posição ativa e participante.

Assim, com o argumento de que há um nível de maturidade relativamente baixo nas discussões quanto à gestão de riscos em organizações do setor público, em especial nas instituições públicas brasileiras e, de modo oposto, alta cobrança para que os órgãos públicos sejam mais eficientes, eficazes e transparentes em suas práticas, esta obra visa promover e motivar as melhores práticas de gerenciamento de riscos no setor público. O livro apresenta uma metodologia própria de gestão de riscos – a metodologia ForRisco – e garante ter embasado as suas pesquisas nas metodologias mais apreciadas no mercado e naquelas adotadas também pelas organizações da AP.

Em tempo, o presente livro parte desta introdução para o Capítulo 2, que propõe uma breve apresentação do Sistema For para a governança pública. O Capítulo 3 visa contextualizar a motivação para a gestão de riscos organizacionais. Na sequência, o Capítulo 4 trata sobre as metodologias de gestão de riscos adotadas tanto no setor privado quanto no público, e sobre as ferramentas para acompanhamento dos riscos. O Capítulo 5 apresenta as leis e as normas relacionadas à gestão de riscos no setor público, e para isso o estudo foca nas leis e

normas que incidem no setor público brasileiro. O Capítulo 6 trata das ferramentas de softwares mais comuns na condução do gerenciamento de riscos. No Capítulo 7, são realizados dois estudos de caso sobre a gestão de riscos em duas Instituições Federais de Ensino Superior (IFES) – UNIFAL-MG e CEFET/RJ – e apresentados os procedimentos que permitiram concretizar a investigação. O Capítulo 8 trata da metodologia ForRisco, apresentando conceitos importantes acerca da metodologia desenvolvida bem como as etapas para execução da gestão dos riscos. O Capítulo 9 traz uma discussão sobre como evoluir a gestão de riscos por meio da metodologia ForRisco. Para isso, nesse capítulo faz-se uma comparação entre o que é realizado na UNIFAL-MG e no CEFET/RJ, e o que recomenda a metodologia ForRisco. O Capítulo 10 faz uma breve apresentação do Sistema ForRisco, isto é, o software desenvolvido para administrar, controlar e monitorar os riscos de forma sistêmica. Por último, o Capítulo 11 estabelece as considerações finais, que destacam as principais realizações do Projeto ForRisco publicadas neste livro, e infere sugestões para novas pesquisas e projetos.

2. O Sistema For para governança pública

Nas últimas décadas, o processo de globalização está conduzindo transformações mundiais extraordinárias para mercados e sociedades. Nesse conjunto de transformações, cada vez mais são necessárias formas de manutenção da transparência, da estratégia e da inovação. Para tanto, a gestão estratégica dos processos e negócios tornou-se um aliado importante dos gestores para impulsionar o desenvolvimento e a competitividade nas organizações.

A administração ou gestão estratégica é vista como a arte de explorar condições favoráveis e/ou de aplicar os meios disponíveis com a finalidade de alcançar objetivos específicos [14]. Nesse entendimento, gerir estrategicamente uma organização refere-se a um processo racional-criativo que permeia as ações das equipes objetivando vantagens competitivas. A estratégia, nesse caso, serve para determinar os objetivos de curto e longo prazos, preparando as organizações para a tomada de decisão e ação.

Em resposta a essas mudanças significativas, no contexto das organizações públicas e privadas o que se percebe são instituições mais atentas, preocupadas em melhorar a alocação dos recursos e gastos, e focadas em proporcionar resultados confiáveis. Além do mais, quando se trata especialmente do setor público, a governança tornou-se a principal dialética capaz de fomentar mecanismos para direcionar e avaliar a gestão ao considerar o conjunto de políticas públicas e a prestação de serviços para a sociedade.

Nessa linha, ao longo dos anos, estruturas de governança foram criadas em diversos países para melhorar o desempenho, reduzir conflitos, alinhar ações e trazer mais segurança para proprietários e Estados [15]. Conforme está descrito no livro sobre governança pública do Tribunal de Contas da União, o Brasil e países como Estados Unidos, Inglaterra e todos os demais que compõem o G8 (Estados Unidos, Japão, Alemanha, Reino Unido, França, Itália e Canadá (antigo G7), mais a Rússia) estão concentrados nos aspectos relacionados à governança.

Além disso, várias organizações passaram a atentar-se para essa questão e a fomentar uma série de códigos que desvelam e recomendam práticas relacionadas à governança. O Banco Mundial, o Fundo Monetário Internacional (FMI)

e a Organização para a Cooperação e o Desenvolvimento Econômico (OCDE) são algumas dessas organizações. No Brasil, a Comissão de Valores Mobiliários (CVM), o Instituto Brasileiro de Governança Corporativa (IBGC) e o próprio Tribunal de Contas da União publicaram as suas proposições de governança [15].

Notadamente, o que se infere são as constantes transformações nos paradigmas das organizações, que estão, progressivamente, mais voltadas aos ganhos de todos aqueles que se relacionam, direta ou indiretamente, com as circunstâncias trazidas por suas instituições, isto é, todos os cidadãos em uma sociedade. Sejam organizações privadas, públicas ou os próprios Estados e governos, suas ações devem ser conscientes no sentido de garantir o propósito de direção para aproveitar oportunidades e evitar ameaças. Nesse ponto de vista, apresenta-se o Sistema For como um segmento inovador de planejamento, estratégia e gestão de riscos.

2.1. O Sistema For

A experiência bem-sucedida de uma solução aberta para a gestão de planos estratégicos, como o ForPDI, motivou o desenvolvimento de novos métodos e tecnologias agregadas, o que culminou na construção do Sistema For para governança pública. Esse sistema foi pensado e construído por uma equipe 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 nas organizações.

Dessa forma, o Sistema For se apresenta como um conjunto de soluções que tem a missão de motivar as melhores práticas de inovação e planejamento estratégico para a gestão nas organizações, provocar a reflexão e gerar valor agregado e conhecimento. Entre seus principais produtos, destacam-se: a solução ForPDI, incluindo o seu conjunto de artefatos, composta pela metodologia ForPDI, pela capacitação on-line e pelo software para a gestão de Planos Estratégicos (PE) e Planos de Desenvolvimento Institucionais (PDI); e a solução ForRisco, que se completa por meio da metodologia ForRisco (integração entre PE/PDI), capacitação on-line e software para a gestão dos riscos nas organizações.

A seguir, apresentamos uma breve descrição das soluções e dos produtos ofertados pelo Sistema For.

2.2. ForPDI – Gestão de Plano Estratégico/PDI

As ações estratégicas nas Instituições Federais de Ensino Superior e em outras instituições públicas ganharam sustentação por meio dos Planos Estratégicos/Planos de Desenvolvimento Institucional, uma espécie de instrumento que visa à fundamentação de diagnósticos sistêmicos e fornece uma estrutura de sustentação para reflexão, formulação, implementação e gestão dos objetivos, tarefas fundamentais ao desenvolvimento organizacional.

O ForPDI é um sistema aberto para gestão e acompanhamento do PE/PDI de universidades federais e outras instituições públicas. Surgiu da necessidade de uma ferramenta de acompanhamento do PE/PDI em tempo real, de forma colaborativa, eficiente, rápida e segura. Com o ForPDI, é possível cadastrar todo o planejamento estratégico do PDI, inserir os valores das metas alcançadas, monitorar o desempenho das metas, elaborar o documento do PDI e muito mais.

O projeto ForPDI foi concebido com o intuito de oferecer aos gestores suporte para a elaboração, a implementação e a execução até a avaliação do PE/PDI. Dessa forma, o ForPDI objetiva a sustentação do planejamento estratégico das instituições de ensino e de outras instituições de maneira integrada e interativa. Para isso, foram desenvolvidas a metodologia ForPDI, o software ForPDI e a capacitação on-line.

2.2.1 Metodologia ForPDI

Após a realização de um diagnóstico com 63 universidades federais brasileiras a fim de levantar informações sobre o Plano de Desenvolvimento Institucional (PDI) dessas universidades, identificou-se a necessidade da criação de um livro de referência sobre gestão do PDI. Com esse objetivo, foi desenvolvida a metodologia ForPDI para ser utilizada por todas as Instituições Federais de Ensino Superior (IFES) na elaboração do PDI. A metodologia tem como base diversas portarias normativas, resoluções e decretos que tratam do PDI. A partir dela, é proposta uma estrutura para a documentação do PDI.

2.2.2 Software ForPDI

Diante de uma metodologia própria para suportar a estruturação dos planos estratégicos e PDIs nas organizações públicas, foi reconhecida a necessidade de criação do software ForPDI. Trata-se de uma ferramenta de informatização do PDI para otimizar o acompanhamento dos resultados dos indicadores e das metas. Entre as principais funcionalidades desse software, destaca-se a sua flexibilidade e a capacidade de suportar diferentes estruturas de planos. Cabe ressaltar, ainda, o alinhamento entre a metodologia e o software ForPDI.

2.2.3 Capacitação On-line ForPDI

A capacitação on-line é um recurso complementar que visa à integração entre os princípios e objetivos da metodologia e do software ForPDI. A capacitação, assim como todos os demais produtos destacados, é disponibilizada gratuitamente no portal do Sistema For. Essa capacitação é composta por quatro módulos: (1) apresentação metodológica; (2) fundamentos sobre estratégia aplicada ao setor público; (3) Plano de Desenvolvimento Institucional: o método ForPDI; e (4) sistema de software ForPDI.

2.3. ForRisco – Gestão de Riscos

Riscos e incertezas são parte do desenvolvimento dos projetos em diferentes níveis e escalas locais ou globais. Dessa forma, a gestão de riscos torna-se, ao longo do tempo, um mecanismo efetivo na busca por resultados e impactos positivos. Isto porque gerir os riscos passou a ser reconhecido pelas instituições como uma forma concreta de planejar mais satisfatoriamente os recursos materiais, humanos e administrativos.

Nessa linha, a solução ForRisco é a soma de esforços para garantir excelência e compromisso no desempenho de importantes tarefas que visam administrar processos de identificação, análise, planejamento, monitoramento e controle dos riscos. Com essa solução, é possível organizar e planejar recursos de forma a reduzir os impactos dos riscos na instituição. Para isso, utiliza-se um conjunto de técnicas que visam minimizar os efeitos dos danos acidentais, direcionando o tratamento adequado aos riscos que possam causar danos ao projeto, às pessoas, ao meio ambiente e à imagem da organização.

O projeto ForRisco é, portanto, um conjunto de soluções abertas e gratuitas composto pela metodologia ForRisco, pela capacitação on-line e pelo software ForRisco. Dessa forma, o projeto tem o objetivo de prover artefatos teóricos e práticos para o acompanhamento e para a gestão de riscos advindos dos processos desenvolvidos pelas instituições.

2.3.1 Metodologia ForRisco

No intuito de motivar as práticas de gerenciamento de riscos no setor público, foi elaborado este documento de referência para apresentar e dar suporte à implementação da metodologia ForRisco. O livro apresenta uma série de informações sobre a motivação para gestão dos riscos bem como outras metodologias fortemente utilizadas no mercado e na AP. Além disso, traz um conjunto de ferramentas para administrar e controlar os riscos bem como exemplos de estudos de caso sobre o gerenciamento de riscos, destacando ainda uma metodologia própria, isto é, as etapas e os processos da metodologia ForRisco.

2.3.2 Software ForRisco

O software ForRisco é 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. A ferramenta conta com funcionalidades para captação das ocorrências de riscos, gestão de processos de monitoramento, análise dos aspectos alinhados à realidade organizacional, elaboração de diversos cenários realistas e planejamento de futuras estratégias de gestão, auxiliando a tomada de decisão pelos gestores.

2.3.3 Capacitação On-line ForRisco

Com o objetivo de estabelecer suporte para a metodologia e o software ForRisco, a capacitação on-line traz um conjunto de recursos disponíveis aos usuários. A ferramenta é vista como uma etapa complementar aos demais produtos ForRisco, permitindo integrar os objetivos e as técnicas da gestão dos riscos nas instituições. A capacitação é composta por cursos relacionados à metodologia ForRisco para utilização do software.

3. Motivação para a gestão de riscos

No âmbito organizacional, as incertezas ocorrem a todo momento. Uma incerteza se refere a situações em que não há informações suficientes para entendimento do cenário ou conhecimento quanto às consequências de determinado evento. O risco, por sua vez, está relacionado com o efeito da incerteza no alcance dos objetivos organizacionais [6]. Assim, quando se fala em gerenciamento de riscos, buscam-se práticas recomendadas pela governança corporativa e pelo Conselho de Administração para identificar e listar, preventivamente, os principais riscos aos quais a organização está exposta, indicando a probabilidade, o impacto e o caminho para tratamento com base em práticas sistemáticas [16].

Falhas no sistema bancário, catástrofes naturais, má gestão de recursos e falta de conhecimento da organização resultaram no desenvolvimento da gestão de riscos elaborada por auditores, seguradoras, contadores e outros praticantes de diversas organizações do setor privado. Com o passar do tempo, essas práticas de gestão convergiram para modelos genéricos de gestão de riscos corporativos – *frameworks* – que enfatizam a estrutura hierárquica de gestão, quantificam a exposição quanto ao risco e fornecem sistemas de controle para a gestão de riscos [17]. Com o desenvolvimento desses *frameworks*, a gestão de riscos corporativa atraiu a atenção de gerentes dos setores público e privado como meio para identificar e gerir de modo compreensivo e estratégico os riscos aos quais estariam expostos.

No âmbito público, a gestão de riscos já vem sendo adotada por vários órgãos governamentais ao redor do mundo. No cenário internacional, o departamento do tesouro britânico elaborou entre 2004 e 2009 um *framework* para avaliação de riscos (*Risk Management assessment framework: a tool for departments*) para auxiliar na coleta e na avaliação de evidências quanto ao desempenho de departamentos, e também para auxiliar no estabelecimento de prioridades para ações de melhoria [18]. Outras iniciativas menos genéricas foram desenvolvidas nos Estados Unidos pelo Government Accountability Office (Escritório de Contas do Governo, órgão equivalente ao Tribunal de Contas da União para o Brasil), incluindo diversos *frameworks* de riscos relacionados às áreas de segurança, militar e terrorismo, fraudes e finanças, entre outros [19]. No Canadá, a secretaria de tesouro (Treasury Board of Canada Secretariat)

desenvolveu mecanismos quanto a riscos financeiros, auditoria interna, aquisição de serviços, Tecnologia da Informação (TI) e outros [20]. Esses exemplos ilustram a relevância e a adoção do tema em alguns países.

No Brasil, foi desenvolvido pelo Ministério do Planejamento, em conjunto com a Controladoria-Geral da União, a Instrução Normativa Conjunta MP/CGU nº 1, de 2016, que dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo Federal [7]. Outras iniciativas sobre gestão de riscos de segurança da informação foram desenvolvidas pela Presidência da República, por meio do Departamento de Segurança da Informação e Comunicações (DSIC), na Norma Complementar n º 04/13 [21].

O Instituto Brasileiro de Governança Corporativa (IBGC) elaborou uma metodologia para implantação da gestão de riscos em organizações [16]. Este *framework* difere do que tem sido adotado pela IN nº 01/2016 sobre o processo de gestão de riscos, mas pode ser utilizado de forma complementar a outras metodologias. Além disso, a metodologia IBGC contribui para que diferentes reflexões quanto ao tema de gestão de riscos ocorram, e cabe frisar que analisar metodologias diferentes pode enriquecer e agregar valor na condução da gestão de riscos.

Todas essas iniciativas, tanto as do cenário internacional quanto as brasileiras, permitem que os órgãos ponderem sobre seus processos e sobre sua busca pela eficiência, identificando lacunas e criando planos e ações para suprir carências. Ao alcançar esses resultados, tais organizações conseguem entregar maior satisfação e melhores serviços à sociedade e aos cidadãos. Essa procura por respostas mais significativas ao desenvolvimento da gestão de riscos foi a condição motivadora para alavancar as pesquisas sobre os riscos organizacionais em instituições públicas no Brasil.

Notoriamente, este livro traz um aporte maior às organizações brasileiras, sobretudo aquelas de natureza pública, por estabelecer uma gama de informações sobre as legislações vigentes, softwares mais utilizados e casos práticos de processos de gestão de riscos em autarquias vinculadas ao Governo Federal do Brasil. Todavia, é importante acentuar a relevância do tema abordado, que, de maneira geral, abarca um conjunto de referências, metodologias e ferramentas essenciais a quaisquer organizações que tenham o interesse em garantir êxito na efetiva gestão de riscos.

A saber, revela-se este trabalho como resultado de um projeto intitulado "Gestão de riscos nas universidades federais: elaboração de modelo de referência e implantação de sistema". Para o desenvolvimento das pesquisas, o projeto contou com os recursos da Fundação de Apoio à Cultura, Ensino, Pesquisa e Extensão de Alfenas (FACEPE), órgão vinculado à Universidade Federal de Alfenas. Além disso, recebeu apoio de 63 Instituições Federais de Ensino Superior (IFES) pelo Fórum Nacional de Pró-Reitores de Planejamento e Administração (FORPLAD) e pela Associação Nacional dos Dirigentes das Instituições Federais de Ensino Superior (ANDIFES) do Brasil.

A seguir, são apresentadas algumas metodologias e ferramentas de gestão de riscos que têm sido adotadas tanto em organizações privadas quanto públicas.

4. Principais metodologias e ferramentas de gestão de riscos

As metodologias de gestão de riscos possuem diversas similaridades entre si, especialmente por identificarem e tratarem as incertezas de forma sistemática para que haja uma comunicação precisa ao longo do processo de avaliação de riscos. Vale considerar também que, de modo geral, qualquer processo de gerenciamento de riscos propiciará uma base segura para tomada de decisão, planejamento lógico, esclarecimento dos objetivos e, por último, risco mínimo do ponto de vista econômico.

Para tanto, ao longo da execução de um processo de gestão de riscos, existe um conjunto de questões encadeadas nas quais uma pergunta leva naturalmente à próxima, formando um processo genérico de gestão de riscos [22]. Estas questões estão presentes na Figura 1.

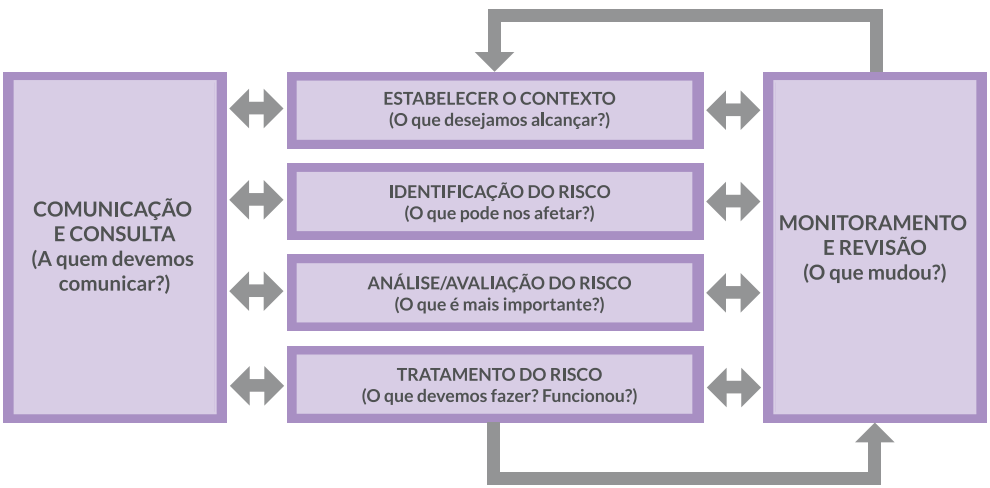


Figura 1 – Processo genérico de gestão de riscos
Fonte: Hillson (2017, p. 9), com adaptações

Conforme Hillson [22], todas essas questões estão presentes durante a execução das etapas contidas nas principais metodologias sobre gestão ou avaliação dos riscos, como a ISO 31000 e o M_o_R-OGC. Trata-se de perguntas orientadoras que auxiliam a equipe de desenvolvimento nas etapas da gestão de riscos e que tendem a garantir viabilidade ao seu desenvolvimento, sem perder

de vista o foco e demais objetivos propostos ainda na formulação do processo. O Quadro 1 relaciona essas questões com as etapas de cada metodologia.

Quadro 1 | Questões a serem respondidas pelas etapas das metodologias

Questões	ISO 31000 (2018)	M_o_R-OGC (2010)
O que desejamos alcançar?	Estabelecimento do contexto	Identificar o contexto
O que pode nos afetar?	Identificação do risco	Identificar riscos
O que é mais importante?	Análise de risco Avaliação de risco	Estimar Avaliar
O que devemos fazer? Funcionou?	Tratamento de risco	Planejar Implementar
A quem devemos comunicar?	Comunicação e consulta	Comunicar
O que mudou?	Monitoramento e análise crítica	Incorporar e revisar
O que aprendemos?	Registro e relato	-

Fonte: Hillson (2017, p. 8), com adaptações

Nitidamente, cada pergunta orientadora pode ser tratada em diferentes sentidos, a depender da metodologia ou do objetivo a que se destina, mas ressalta-se aqui o seu mérito. Quanto à questão "O que aprendemos?", Hillson [22] sugere que essa etapa é pouco explorada nas metodologias e que as lições rendidas, no caso do M_o_R-OGC, raramente são conduzidas ao final de projetos ou de decisões-chave da organização. Revela-se, entretanto, que a não execução das lições aprendidas normalmente tem como causa benefícios tardios devido à complexidade dos objetivos ou falta de clareza, ausência de altruísmo dos funcionários em ajudar outros colegas com as experiências ou porque os funcionários precisam começar um novo desafio antes de ter tempo para capturar as lições do desafio anterior. Não capturar e disseminar essas lições são ações que fazem com que a organização incorra no mesmo erro repetidas vezes, gastando recursos escassos e não entregando os resultados de que ela necessita.

A seguir, abordam-se as metodologias de gestão de riscos mais recorrentes no mercado bem como uma comparação entre essas metodologias. É válido frisar que serão também detalhadas algumas metodologias desenvolvidas e adotadas pela AP brasileira.

4.1. Metodologias de mercado

A seguir, são detalhadas as principais metodologias de mercado utilizadas para a gestão de riscos corporativos[1] . São elas: o ERM-COSO – amplamente adotado pela AP brasileira – e a ISO 31000 e o M_o_R-OGC – metodologias recorrentes em organizações públicas e privadas de diversos países.

4.1.1. Enterprise Risk Management (ERM-COSO)

O ERM-COSO é talvez o *framework* de maior aceitação no mercado para organizar os esforços de gerenciar os riscos. Desenvolvido pelo Committee of Sponsoring Organizations of the Treadway Commission (COSO), sua primeira versão, publicada em 1992 – *Internal Control – Integrated Framework*, propôs uma estrutura focada na implantação e na condução do controle interno nas organizações, bem como na avaliação da sua efetividade. Entre outras versões, em 2004, a obra *Enterprise Risk Management – Integrated Framework* (ERM-COSO) impulsiona o argumento de que a condução da gestão de riscos existe nas organizações ou entidades[2] para prover valor às partes interessadas, tais como acionistas, clientes, funcionários, entre outros [8].

Em sua mais recente narração, o ERM-COSO 2017, que é uma versão atualizada da *Enterprise Risk Management – Integrated Framework*, de 2004, aborda a evolução do gerenciamento de riscos corporativos e a necessidade de as organizações melhorarem a sua abordagem de gerenciamento de riscos para atender às demandas de um ambiente de negócios em evolução [23]. Conforme o COSO [23], a complexidade dos riscos mudou e, além disso, surgiram novos riscos, mas os gestores e os executivos também aprimoraram sua conscientização e supervisão acerca do gerenciamento de riscos corporativos, ao mesmo tempo que são necessários novos recursos mais aprimorados.

Em verdade, todas as organizações enfrentam incertezas, e o desafio da gestão é determinar o quanto de incertezas aceitar, já que estas podem causar

[1] Optou-se por traduzir *"Enterprise Risk Management"* como "Gestão de Riscos Corporativos". Entenda-se que organizações, instituições e corporações possuem um nível similar e que esses termos refletem "o todo" de um ambiente organizacional.

[2] A metodologia ERM-COSO sempre faz referência ao termo *"entity"*, ou entidade, mas neste livro optou-se por usar a tradução como "organização".

impactos nos valores organizacionais desejados [8]. Por isso, todas as organizações precisam definir as suas estratégias e ajustá-las periodicamente, devendo estar sempre atentas às oportunidades mutáveis de criação de valor e aos desafios que ocorrerão em busca desses valores. Para tanto, elas precisam da melhor estrutura possível para otimizar a estratégia e o desempenho. Nesse momento é que o gerenciamento de riscos corporativos entra em cena. A gestão de riscos visa à maximização do valor resultante de uma definição clara e precisa entre os objetivos e as estratégias para encontrar o equilíbrio ideal [23].

Conforme o ERM-COSO [23, p. 15-16], são muitos os benefícios para as organizações que integram a sua gestão de riscos corporativos às estratégias, destacando-se:

a. aumentar o leque de oportunidades: processos de gestão de riscos podem possibilitar a melhoria da capacidade da organização em identificar novas oportunidades e desafios únicos associados a essas oportunidades;

b. identificar e gerenciar toda a organização de risco: um risco pode se originar em uma parte da organização, mas impactar uma parte diferente. Consequentemente, a administração identifica e gerencia esses riscos em toda a organização para sustentar e melhorar o desempenho;

c. aumentar os resultados positivos e as vantagens, e reduzir as surpresas negativas: gerenciar os riscos permite que as organizações melhorem a sua capacidade de identificar novos riscos e de estabelecer respostas apropriadas, reduzindo surpresas e custos ou perdas relacionadas;

d. reduzir a variabilidade do desempenho: o gerenciamento de riscos corporativos permite às organizações preverem os riscos que afetariam o seu desempenho e possibilita implementar as ações necessárias para minimizar a interrupção e maximizar as oportunidades;

e. melhorar a alocação de recursos: a obtenção de informações robustas sobre os riscos permite que o gerenciamento, ante os recursos finitos, avalie e priorize a implantação desses recursos; e

f. reforçar a resiliência empresarial: a viabilidade a médio e longo prazos de uma organização depende da sua capacidade de antecipar e responder às mudanças não apenas para sobreviver, mas também para evoluir e prosperar. Em parte, isso é habilitado pelo gerenciamento eficaz de riscos corporativos.

Esses benefícios mostram, na verdade, a necessidade de uma visão holística das organizações em um processo interativo entre seus membros. De fato, o risco não deve ser visto apenas como uma potencial incerteza ou desafio para estabelecer e executar as estratégias. Longe disso, o risco precisa ser entendido como uma oportunidade estratégica e planejada que pode aperfeiçoar as respostas, os recursos e as entregas na organização que o procede [23].

Por meio dessa visão holística, o ERM-COSO estabelece a importância da integração da gestão de riscos corporativos, especialmente porque o risco influencia e alinha a estratégia e o desempenho das organizações em todos os departamentos e funções. Para explicar isso, o documento propõe o *framework* da gestão de riscos corporativos, representado na Figura 2:

Figura 2 – Metodologia de gestão de riscos proposta pelo ERM-COSO
Fonte: ERM-COSO (2017, p. 18)

O *framework* rege um conjunto de princípios organizados em cinco componentes principais, inter-relacionados [23, p. 18]:

1) Governança e cultura: a governança define o tom da organização, reforçando a importância da missão e da visão, e estabelecendo responsabilidades de supervisão para o gerenciamento de riscos corporativos. A cultura diz respeito a valores éticos fundamentais, comportamentos desejados e compreensão do risco na organização;

2) Estratégia e definição de objetivos: no gerenciamento de riscos corporativos, estratégia e definição de objetivos devem ser trabalhadas juntas no processo de planejamento estratégico. O apetite pelo risco é estabelecido e alinhado com a estratégia; e os objetivos dos negócios colocam a estratégia

em prática enquanto servem de base para identificar, avaliar e responder aos riscos;

3) Desempenho: os riscos podem afetar o alcance da estratégia, e os objetivos dos negócios precisam ser identificados e avaliados. Os riscos são priorizados pela gravidade no contexto do apetite ao risco. Na sequência, a organização seleciona respostas aos riscos e obtém uma visão do portfólio da quantidade de riscos que assumiu. Os resultados desse processo são reportados às principais partes interessadas (*stakeholders)* da organização;

4) Revisão: ao revisar o desempenho da organização, uma organização pode considerar o quão bem os componentes de gerenciamento de risco estão funcionando ao longo do tempo e quais mudanças são necessárias; e

5) Informação, comunicação e reporte: o gerenciamento de riscos corporativos requer um processo contínuo de obtenção e compartilhamento das informações necessárias tanto de fontes internas quanto externas, que fluem para cima, para baixo e por toda a organização.

Para além disso, os cinco componentes do *framework* são apoiados por um conjunto de princípios, os quais buscam atender a todos os requisitos da boa gestão de riscos em uma organização, desde a governança até o monitoramento. São, ainda, princípios gerenciáveis e descrevem práticas que podem ser aplicadas de diferentes maneiras, independentemente do tamanho da organização, do tipo ou do setor. No Quadro 2, estão explicitados e descritos os princípios para cada um dos componentes, conforme o ERM-COSO [23, p. 19]:

Quadro 2 – Componentes e princípios da gestão de riscos propostos pela revisão ERM-COSO

Componentes	Princípios	Descrição
1. Governança e cultura	a. Exercer a supervisão do risco por intermédio do Conselho.	A diretoria fornece supervisão para a estratégia e executa as responsabilidades de governança para apoiar a administração no alcance da estratégia e dos objetivos dos negócios.
	b. Estabelecer estruturas operacionais.	A organização estabelece estruturas operacionais na busca de objetivos estratégicos e dos negócios.
	c. Definir a cultura desejada.	A organização define os comportamentos desejados que caracterizam a cultura almejada por ela.
	d. Demonstrar compromisso com os valores fundamentais.	A organização demonstra um compromisso com os seus valores centrais.
	e. Atrair, desenvolver e reter pessoas capazes.	A organização está comprometida em construir capital humano alinhado com a estratégia e com os objetivos dos negócios.
2. Estratégia e definição de objetivos	f. Analisar o contexto dos negócios.	A organização considera os efeitos potenciais do contexto dos negócios no perfil de risco.
	g. Definir o apetite ao risco.	A organização define o apetite ao risco no contexto da criação, preservação e obtenção de valor.
	h. Avaliar as estratégias alternativas.	A organização avalia as estratégias alternativas e o impacto potencial no perfil de risco.
	i. Formular os objetivos dos negócios.	A organização considera o risco ao estabelecer os objetivos dos negócios em vários níveis. Esses objetivos darão suporte à estratégia.

3. Desempenho	j. Identificar os riscos.	A organização identifica o risco que afeta o desempenho da estratégia e os objetivos do negócio.
	k. Avaliar a severidade dos riscos.	A organização avalia a gravidade do risco.
	l. Priorizar os riscos.	A organização prioriza os riscos para selecionar as respostas a esses riscos.
	m. Implementar respostas aos riscos.	A organização identifica e seleciona as respostas aos riscos.
	n. Adotar uma visão de portfólio.	A organização desenvolve e avalia uma visão de portfólio do risco.
4. Revisão	o. Avaliar mudanças importantes.	A organização identifica e avalia mudanças que podem afetar substancialmente a estratégia e os objetivos dos negócios.
	p. Analisar riscos e performance organizacional.	A organização revisa o seu desempenho e considera o risco.
	q. Buscar o aprimoramento no gerenciamento de riscos corporativos.	A organização busca a melhoria do gerenciamento de riscos corporativos.
5. Informação, comunicação e reporte	r. Alavancar sistemas de informações e tecnologia.	A organização aproveita os seus sistemas de informação e tecnologia para dar suporte ao gerenciamento de riscos corporativos.
	s. Comunicar informações sobre o risco.	A organização usa canais de comunicação para suportar o gerenciamento de riscos corporativos.
	t. Divulgar informações de risco, cultura e performance por meio de relatórios.	A organização informa sobre risco, cultura e desempenho em vários níveis e em todo o seu conjunto.

Fonte: ERM-COSO (2017, p. 18-23), com adaptações

Cabe ressaltar, baseando-se nos componentes e nos princípios propostos pela revisão ERM-COSO [23] para gerenciamento dos riscos, que a adesão a esses princípios visa fornecer à administração, ao Conselho e aos gestores uma expectativa razoável de que a organização que entende e se esforça para gerenciar os riscos atende de maneira mais efetiva à sua estratégia e aos objetivos dos negócios. O resultado disso, independentemente do tipo de entidade, deverá refletir na integração de práticas de gerenciamento de riscos corporativos com outros aspectos dos negócios, aumentando a confiança pelas partes interessadas e gerando valor para a organização.

4.1.2. ISO 31000

A norma ABNT NBR ISO 31000: Gestão de riscos – Diretrizes – define princípios e diretrizes em gestão de riscos, e pode ser adotada por diferentes organizações nas atividades de decisão estratégica, operação, processo, função, projeto, serviço e avaliação de riscos. A metodologia pode ser aplicada a tipos diversos de riscos, independentemente de sua natureza, como, por exemplo, em objetivos qualitativos ou quantitativos e, ainda, impactos positivos ou negativos, estabelecendo e alcançando objetivos e melhorando o desempenho [6].

A norma sugere que sejam feitos tratamentos de acordo com as especificidades da organização que, inicialmente, utiliza a metodologia para harmonizar o processo de gerenciamento de risco em padrões existentes, fornecendo, desse modo, determinado suporte às ações [6]. Além disso, a ISO 31000 visa apoiar a padronização da gestão de riscos na organização sem deixar de lado o entendimento da necessidade de tratamento a casos e situações específicos, isto é, inerentes a cada instituição.

De acordo com a norma, risco é o "efeito da incerteza nos objetivos" [6, p. 1]. Tão logo, gerenciar os riscos corresponde a auxiliar as organizações no estabelecimento das estratégias para a tomada de decisão. O gerenciamento dos riscos integra as ações de governança e contribui para a melhoria da gestão [6]. Além do mais, todas as organizações gerenciam riscos em algum grau, e a norma estabelece princípios que precisam ser atendidos para tornar a gestão de riscos eficaz, sistemática, transparente e confiável.

A norma está, basicamente, dividida em três componentes: a) princípios, b) estrutura e c) processos. Ou seja, partindo da proposta de gestão de riscos da

ISO 31000 e de um conjunto de regras e diretrizes, contidas nos princípios, é criada a estrutura para sustentar a implantação dos processos de gestão de riscos nas organizações visando à melhoria contínua. A partir desse conjunto de componentes, o processo da norma objetiva estabelecer o contexto, identificar, analisar, avaliar e tratar o risco, e, no seu decorrer, comunicá-lo e monitorá-lo [6]. A Figura 3 representa o modelo geral da metodologia.

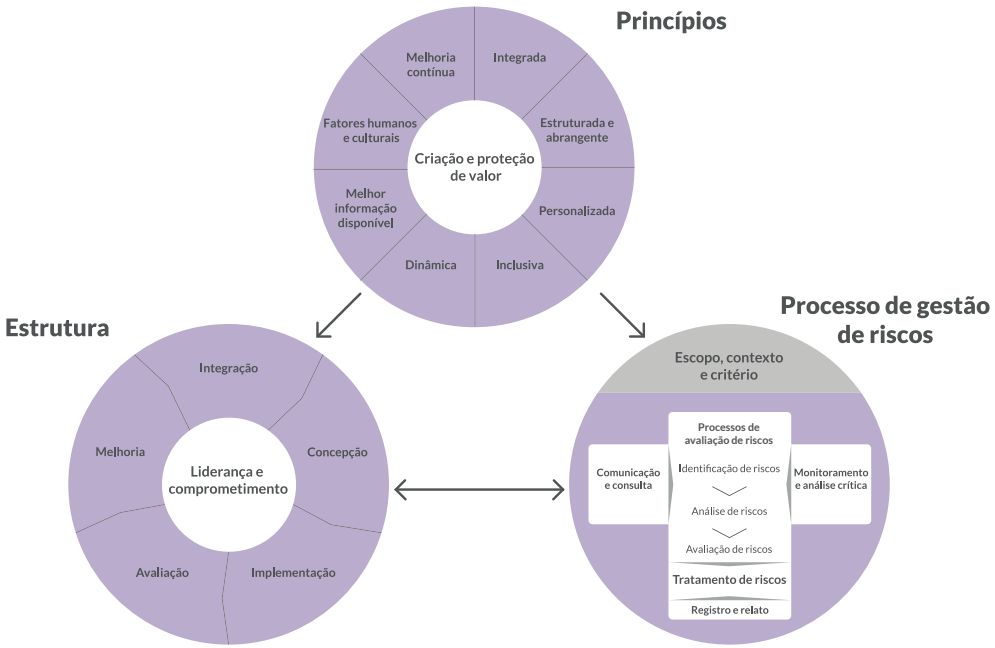


Figura 3 – Metodologia de gestão de riscos proposta pela ISO 31000
Fonte: ABNT NBR ISO 31000 (2018, p. vi)

a) Em **Princípios**, o propósito corresponde à criação e à proteção de valores. Por meio dessa estrutura de valores, as organizações devem desenvolver a sua base para gerenciar os riscos. Para tanto, a ISO 31000 destaca os seguintes princípios: criação de valor; integração; estrutura e abrangência; personalização; inclusão; dinâmica; melhor informação disponível; fatores humanos e culturais; e melhoria contínua.

b) Na **Estrutura**, a ISO 31000 permite que a organização reflita sobre a integração da gestão dos riscos em atividades significativas e funções. Para isso, a instituição deve avaliar as práticas e os processos existentes, e então identificar possíveis lacunas. É importante considerar todas as partes interessadas e

a alta administração. Os elementos da estrutura são: liderança e comprometimento; integração; concepção; implementação; avaliação; e melhoria.

c) Em **Processo**, a gestão de riscos compreende a construção e a implementação de políticas e práticas para controlar e monitorar as atividades. Em síntese, o processo de gestão de riscos começa com a definição do escopo das atividades da organização, dos contextos externo e interno, e da definição dos critérios para avaliação dos riscos. Adiante, é necessário identificar, analisar e avaliar os riscos para então tratá-los. Constantemente, esse processo deve ser comunicado e monitorado. Os riscos, seus tratamentos e todo o monitoramento devem ser relatados e registrados.

Quando a ISO 31000 é implementada e mantida, a proposta de gestão de riscos contida nesta norma possibilita atingir diversos objetivos para atender às necessidades das partes interessadas. Por intermédio desse conjunto de controles estruturados e propostos, e com o entendimento claro do contexto e dos riscos existentes, são definidas as melhores ferramentas para tratamento dos riscos de acordo com a sua natureza. Acredita-se, dessa forma, na qualidade do tratamento dos riscos e na maior agregação de valor ao negócio por meio da gestão.

De forma complementar, a norma ABNT NBR ISO 31000 – Diretrizes, a ABNT NBR ISO 31010: Gestão de riscos – Técnicas para o processo de avaliação de riscos fornece orientações sobre a seleção e a aplicação de técnicas sistemáticas para o processo de avaliação de riscos, contribuindo com as atividades de gestão de riscos. De acordo com o processo de avaliação dos riscos, ao empregar as ferramentas e as técnicas propostas na norma, é possível compreender melhor os riscos, angariando informações relevantes que auxiliam a tomada de decisão e o estabelecimento de priorizações para o tratamento dos riscos [24]. O Quadro 3 apresenta essas ferramentas e técnicas.

Quadro 3 – Ferramentas e técnicas utilizadas para o processo de avaliação de riscos

Ferramentas e técnicas	Processo de avaliação de riscos				
		Análise de riscos			
	Identificação de riscos	Consequência	Probabilidade	Nível de risco	Avaliação de riscos
Brainstorming	FA	NA	NA	NA	NA
Entrevistas estruturadas ou semiestruturadas	FA	NA	NA	NA	NA
Delphi	FA	NA	NA	NA	NA
Listas de verificação	FA	NA	NA	NA	NA
Análise preliminar de perigos (APP)	FA	NA	NA	NA	NA
Estudo de perigos e operabilidade (HAZOP)	FA	FA	A	A	A
Análise de perigos e pontos críticos de controle (APPCC)	FA	FA	NA	NA	FA
Avaliação de risco ambiental	FA	FA	FA	FA	FA
Técnica estruturada "E se"(SWIFT)	FA	FA	FA	FA	FA
Análise de cenários	FA	FA	A	A	A
Análise de impactos no negócio	A	FA	A	A	A
Análise de causa-raiz	NA	FA	FA	FA	FA
Análise de modos de falha e efeito (FMEA)	FA	FA	FA	FA	FA
Análise de árvore de falhas (FTA)	A	NA	FA	A	A
Análise de árvore de eventos (ETA)	A	FA	A	A	NA
Análise de causa e consequência	A	FA	FA	A	A
Análise de causa e efeito	FA	FA	NA	NA	NA
Análise de camadas de proteção (LOPA)	A	FA	A	A	NA
Árvore de decisão	NA	FA	FA	A	A
Análise da confiabilidade humana	FA	FA	FA	FA	A
Análise Bow-Tie	NA	A	FA	FA	A
Manutenção centrada em confiabilidade	FA	FA	FA	FA	FA
Análise de circuitos ocultos	A	NA	NA	NA	NA
Análise de Markov	A	FA	NA	NA	NA
Simulação de Monte Carlo	NA	NA	NA	NA	FA
Estatística bayesiana e Redes de Bayes	NA	FA	NA	NA	FA

Ferramentas e técnicas	Processo de avaliação de riscos				
		Análise de riscos			
	Identificação de riscos	Consequência	Probabilidade	Nível de risco	Avaliação de riscos
Curvas FN	A	FA	FA	A	FA
Índices de risco	A	FA	FA	A	FA
Matriz de probabilidade/consequência	FA	FA	FA	FA	A
Análise de custo/benefício	A	FA	A	A	A
Análise de decisão por multicritérios (MCDA)	A	FA	A	FA	A
FA - Fortemente aplicável; NA - Não aplicável; A - Aplicável.					

Fonte: ABNT NBR ISO 31010 (2012, p. 21-22), com adaptações

A norma ABNT NBR ISO 31000 apresenta um conjunto de etapas contendo os princípios, a estratégia e os processos de avaliação de riscos, e nesse processo elenca as ferramentas e técnicas para permitir que se busque uma avaliação sistemática dos riscos. Vale refletir que, assim como o ERM-COSO, as preocupações recaem sobre o fator humano, como a falta de entendimento e outros problemas advindos da falha de comunicação e racionalidade limitada. Entretanto, por meio da estrutura de governança proposta pela norma, é possível garantir um melhor desempenho organizacional e a redução de incertezas.

4.1.3.Management of Risk (M_o_R-OGC)

O *framework* M_o_R (Management of Risk – Gerenciamento de Riscos), desenvolvido pelo Office of Government Commerce (OGC), é um guia elaborado para auxiliar organizações na tomada de decisão sobre os riscos que possam afetar o alcance de seus objetivos estratégicos de programas, projetos ou operações.

A metodologia engloba princípios, abordagem e processos em um conjunto de passos inter-relacionados nessas dimensões para o gerenciamento de riscos em organizações. Também é apoiada por ferramentas e técnicas para identificação, avaliação e tratamento desses riscos. Existem algumas referên-

cias da ISO 31000 inclusas no M_o_R-OGC, o que a torna complementar no que tange à gestão de riscos [25].

No M_o_R-OGC, há uma forma mais prescritiva sobre como conduzir a gestão de riscos na organização. Desse modo, são apresentados a seguir oito princípios para que a gestão de riscos possa acontecer de forma prática segundo as orientações dessa metodologia – os sete primeiros são princípios habilitadores e o último é um princípio de resultado [25]:

1. Alinhamento aos objetivos: a gestão de riscos deve estar continuamente alinhada aos objetivos organizacionais.

2. Adequação ao contexto: a gestão de riscos deve estar perfeitamente adequada ao contexto atual.

3. Engajamento de partes interessadas: a gestão de riscos deve engajar partes interessadas e lidar com as diferentes percepções de risco.

4. Fornecimento de um guia de processos claro: a gestão de riscos deve prover um guia de processos claro e coerente para as partes interessadas.

5. Apoio à tomada de decisão: a gestão de riscos deve informar adequadamente e estar vinculada à tomada de decisão em toda a organização.

6. Apoio à melhoria contínua: a gestão de riscos deve utilizar dados históricos para facilitar o aprendizado e a melhoria contínua.

7. Criação de cultura suportiva: a gestão de riscos deve criar uma cultura que reconheça a incerteza e que considere que a organização corre riscos.

8. Alcance de valores mensuráveis: a gestão de riscos permite o alcance de valores mensuráveis na organização.

Para garantir que a gestão de riscos seja conduzida de forma apropriada e com sucesso em toda a organização, existem métodos e modelos para alcance dos resultados, como a avaliação da saúde atual (*HealthCheck*) ou a escala de maturidade baseada nas melhores práticas de mercado.

Para ser possível o alcance dos princípios citados, o M_o_R-OGC sugere uma abordagem por meio de um conjunto de documentos (registros, planos e relatórios, entre outros) norteadores nas definições de como serão conduzidas as ações, o modo como serão comunicadas, geridas e melhoradas ao longo do tempo [25]. O Quadro 4 apresenta alguns desses documentos.

Quadro 4 – Abordagem da gestão de riscos – Documentos

Documento	Descrição
Política	O propósito da política é comunicar "por que" e "como" a gestão de riscos será implementada em toda a organização (ou em parte desta) para suportar a concretização dos objetivos.
Guia de Processos	O guia de processos descreve como as etapas da gestão de riscos serão conduzidas, envolvendo desde a identificação desses riscos até o seu tratamento ou implementação. Reflete o cerne da metodologia de gestão de riscos do M_o_R-OGC.
Estratégia	A estratégia descreve atividades específicas para a gestão de riscos que devem ser conduzidas por uma organização, ou por parte desta, em uma forma particular considerando as suas características.
Registro do Risco	O registro do risco deve capturar e manter informações das ameaças e das oportunidades relativas a uma atividade organizacional específica. É o principal componente a ser avaliado em conjunto com os demais riscos e que também permite a alocação de responsabilidades e a distribuição de tarefas.
Registro da Questão	Questões são riscos materializados. Esses registros devem capturar e manter informações de forma consistente e estruturada sobre as questões que estão ocorrendo no momento e que requerem atenção.
Plano de Melhoria para Gestão de Riscos	O propósito do plano de melhoria é apoiar a incorporação da gestão de riscos na cultura organizacional. Este documento deve refletir as melhorias planejadas para o ambiente e conta com o estado de saúde atual (*HealthCheck* – questionário de avaliação, Anexo C da norma) em comparação com o estado de maturidade atual para traçar um rumo em busca do aumento de maturidade e melhoria contínua (Anexo D da norma).
Plano de Comunicação do Risco	O plano de comunicação do risco descreve como a informação será disseminada e assimilada por pessoas-chave da organização. Uma comunicação precisa é um fator crítico de sucesso para garantir que o contexto seja entendido, os riscos sejam identificados e avaliados, e para que as respostas apropriadas sejam planejadas e executadas.
Plano de Resposta ao Risco	O plano de resposta ao risco está vinculado ao registro de risco e deve conter detalhes específicos para um único risco. Nesse documento, está estipulado quem é o dono do risco, o executor ou agente, como o risco deve ser acompanhado e comunicado, entre outras características para o seu tratamento. Assim, caso o evento de um risco seja materializado ou ultrapasse o seu limite de tolerância, não será necessário desenvolver um plano em tempo de execução, o que poupará tempo e esforço.
Plano de Progresso do Tratamento do Risco	O plano de progresso do tratamento do risco deve fornecer um relatório com informações regulares sobre o progresso da implantação ou do tratamento de riscos para os gerentes envolvidos ou as partes interessadas. Esse relatório permite agregar valor aos tomadores de decisão para que tenham as informações mais precisas e possam analisar tendências.

Fonte: M_o_R-OGC (2010, p. 21-25), com adaptações

A Figura 4 representa o relacionamento desses documentos. Vale apontar que existem alguns documentos abrangentes, isto é, que são válidos para toda a organização, e documentos específicos para atividades exclusivas das organizações.

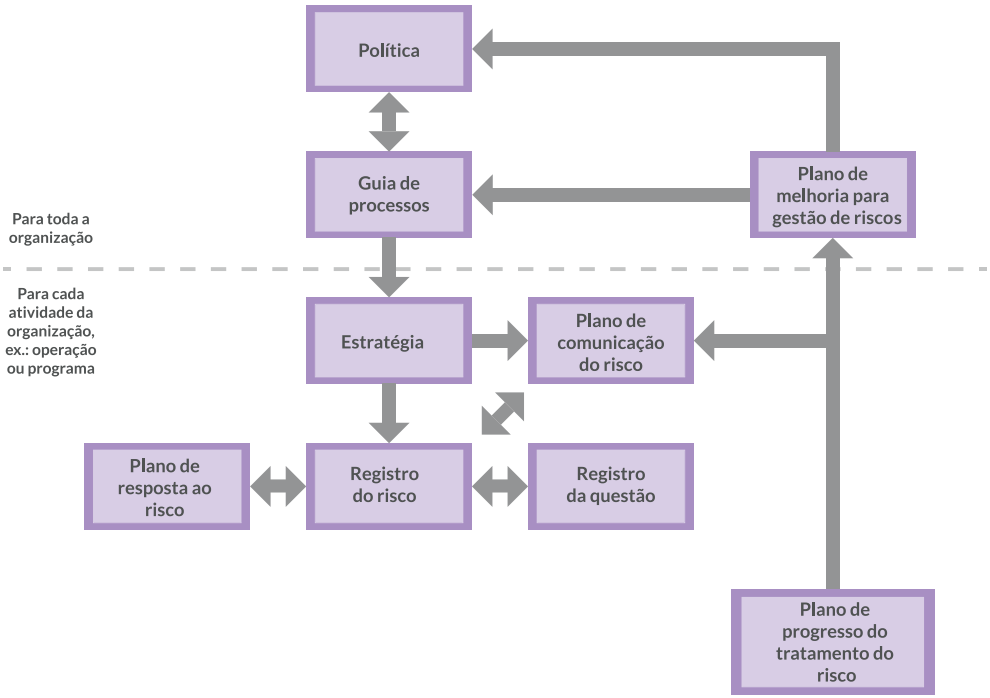


Figura 4 – Relacionamento entre documentos do M_o_R-OGC
Fonte: M_o_R-OGC (2010, p. 24), com adaptações

Uma vez estruturada a política e definida a abordagem da gestão de riscos em nível organizacional, iniciam-se os processos para os riscos de forma mais individualizada. O processo de gestão de riscos do M_o_R-OGC contém várias etapas, conforme a Figura 5. A etapa "Comunicar" é central e deve ocorrer diversas vezes para que haja um alinhamento correto entre os envolvidos. As etapas "Identificar", "Estimar/Avaliar", "Planejar" e "Implementar" representam uma sequência lógica, e a saída de uma etapa serve de insumo ou entrada para a etapa seguinte.

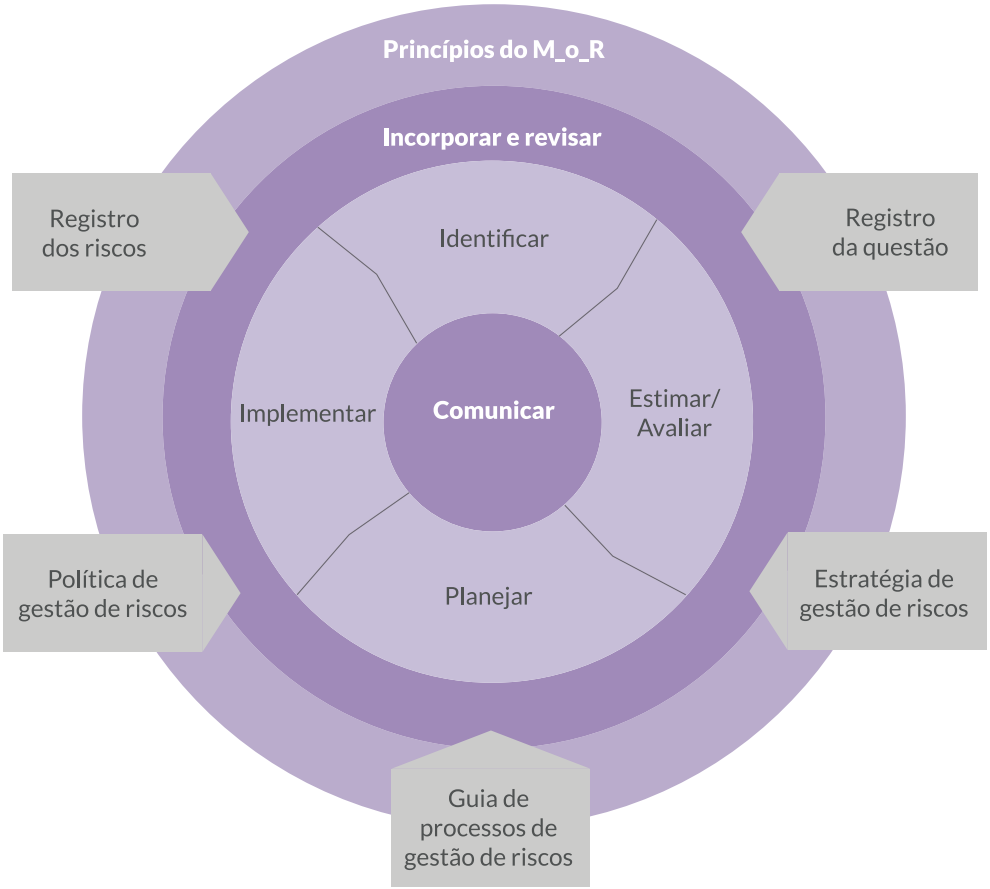


Figura 5 – Metodologia de gestão de riscos proposta pelo M_o_R-OGC
Fonte: M_o_R-OGC (2010, p. 3), com adaptações

Assim como na ABNT NBR ISO 31010, o M_o_R-OGC conta com um conjunto de ferramentas e técnicas para apoiar a execução do processo de gestão de riscos. Considerando apenas as técnicas para a gestão de riscos, é possível classificá-las conforme os passos do *framework* – Quadro 5. Este quadro tem por finalidade auxiliar os gestores na definição das técnicas para a gestão e se assemelha às ferramentas e às técnicas presentes na ABNT NBR ISO 31010.

Quadro 5 – Técnicas presentes no Apêndice B do M_o_R

Etapa do processo	Técnica primariamente associada à etapa do processo	Outra etapa do processo na qual a técnica pode ser útil
Identificar o contexto	Análise de partes interessadas Análise PESTEL Análise SWOT Escaneamento horizontal Matriz de probabilidade e consequência	Identificar o risco
Identificar o risco	Lista de verificação Lista de resposta Diagrama de causa e efeito Técnicas de grupo Delphi Questionários Entrevistas Análise de premissas Análise de restrições Descrições do risco	Planejar
Estimar	Avaliação de probabilidade Avaliação de impacto Avaliação de proximidade Valor esperado como critério de decisão	
Avaliar	Mapa de risco Valor esperado como critério de decisão Modelos de riscos probabilísticos Árvore de probabilidade Análise de sensibilidade	Planejar
Planejar	Resposta ao risco Análise custo/benefício Árvore de decisão	Avaliar
Implementar	Atualização de relatório de mapa de risco Tendências de exposição ao risco Atualização de modelos probabilísticos de risco	

Fonte: M_o_R-OGC (2010, p. 86), com adaptações

Para apoiar essas técnicas, o M_o_R-OGC sugere um conjunto de papéis e responsabilidades que envolvem:

- o time sênior ou Comitê da alta direção, com atribuições voltadas para atividades estratégicas, disseminação e incorporação da gestão de riscos;

- o representante do time sênior, com responsabilidades para garantir governança e controles internos, e demais informações que devem ser reportadas, entre outras atividades;

- os gerentes de programa, operação ou projeto, que possuem como responsabilidades garantir que o registro, a revisão, a avaliação, as tarefas e outros controles sejam executados adequadamente;

- a equipe de qualidade, para garantir que existam controles contábeis em conformidade com orientações internas, revisão do progresso dos planos e outras atividades de auditoria;

- os especialistas em riscos, para garantir que a Política de Gestão de Riscos está adequadamente implementada, além de facilitar a disseminação da metodologia pelo órgão; e

- as demais equipes, que participam da identificação do tratamento dos riscos, implementam as regras das políticas e classificam os riscos quando necessário.

A metodologia ainda fornece uma escala de maturidade para apoiar os gestores e a alta direção a definirem os objetivos quanto à evolução da gestão de riscos e sua maturidade na organização. O Quadro 6 representa essa escala com os níveis de maturidade.

Quadro 6 – Escala de maturidade do M_o_R

	Nível 1 Inicial	Nível 2 Repetitivo	Nível 3 Definido	Nível 4 Gerenciado	Nível 5 Otimizado
Alinhado aos objetivos	Os objetivos não estão definidos.	Riscos associados a objetivos definidos.	Objetivos definidos e atualizados durante a gestão de riscos.	Objetivos alterados conforme resposta aos riscos.	Objetivos definidos conforme a gestão de riscos.
Adequado ao contexto	Contexto não refletido na identificação.	O contexto é examinado ao longo do processo de risco.	O contexto é rigorosamente examinado para explorar ameaças e oportunidades.	Os gerentes informam com antecedência sobre o contexto.	O contexto é usado para definir ações da gestão.
Envolve *stakeholders*	Nem todos os *stakeholders* são consultados.	Os *stakeholders* são identificados e minimamente engajados.	Os objetivos dos *stakeholders* são identificados, registrados, alinhados e atribuídos.	Os *stakeholders* são ativamente envolvidos.	Os *stakeholders* são incentivados e envolvidos no ciclo de investimento.
Processo definido	Política e processos não documentados e vagos.	A política e os processos estão definidos.	Processos uniformes são adotados em toda a organização.	A gestão de riscos está totalmente integrada às atividades dos gerentes.	Melhores práticas são identificadas e compartilhadas na organização.
Tomada de decisão	Não há definição de limites operacionais, revisões ou relatórios.	Relatórios de gestão são emitidos consistentemente e em prazos definidos.	Gerentes seniores reportam em um formato consistente.	Existem análises quantitativas de qualidade.	Técnicas de planejamento de cenários são naturalmente utilizadas.
Melhoria contínua	Ausência de treinamentos e de conhecimento sobre gestão de riscos.	As pessoas são treinadas ao longo da implantação da gestão de riscos.	Diferentes níveis de treinamento estão definidos.	Pessoal experiente analisando resultados quantitativos.	Conhecimentos e habilidades atualizados constantemente.
Cultura colaborativa	A equipe age por conta própria em grupos independentes.	Os donos dos riscos, os gerentes e os agentes estão identificados.	Times integrados na organização com papéis e responsabilidades.	Atitudes de gestão de riscos são reconhecidas e condecoradas.	Riscos estão apensos na organização, presentes nas descrições dos cargos.
Valores mensuráveis	Sem mensurações.	Mensurações dos processos, mas não de desempenho.	Medidas de desempenho implantadas.	Medidas de desempenho demostram o alcance de valor.	Alcance de valor mensurável para partes interessadas internas e externas.

Fonte: M_o_R-OGC (2010), com adaptações

Em comparação ao ERM-COSO e à ISO 31000, o M_o_R-OGC apresenta o maior *framework* de orientações para implantação e operacionalização do gerenciamento de riscos nas organizações. Infere-se que, embora seja mais prescritiva do que as outras normas, o M_o_R-OGC ainda continua genérico o suficiente para ser adotado tanto por organizações do setor público quanto privado, de maior ou menor porte.

4.1.4. Comparação entre as principais metodologias de mercado

As metodologias de mercado possuem um conjunto comum de orientações aos profissionais da área de gestão de riscos. Como foram desenvolvidas em momentos diferentes, percebe-se uma evolução no foco das técnicas de gestão, bem como um conjunto abrangente de ferramentas e técnicas para apoiar os gestores na condução dos riscos organizacionais. Dessa forma, o Quadro 7 contém informações que sintetizam as principais ideias do processo de gestão de riscos segundo as metodologias de mercado. Para facilitar o entendimento, foi elaborada a Figura 6, que exemplifica um comparativo entre as metodologias de gestão de riscos com as seguintes especificações: A como representação dos princípios; B como a estrutura da metodologia; e a numeração (de 1 a 10) com as etapas de apoio e execução das metodologias.

As etapas e os processos compreendidos na Figura 6 estão registrados e interpretados no Quadro 7 a fim de facilitar o entendimento da gestão de riscos e das características individuais das metodologias de mercado. São apresentadas interpretações sobre riscos, gestão de riscos corporativos, processo de avaliação de riscos, princípios, estrutura, contexto/ambiente interno, definição dos objetivos, identificação, análise/avaliação, tratamento/resposta, comunicação, monitoramento e abordagem para cada uma das metodologias mencionadas.

(continua)

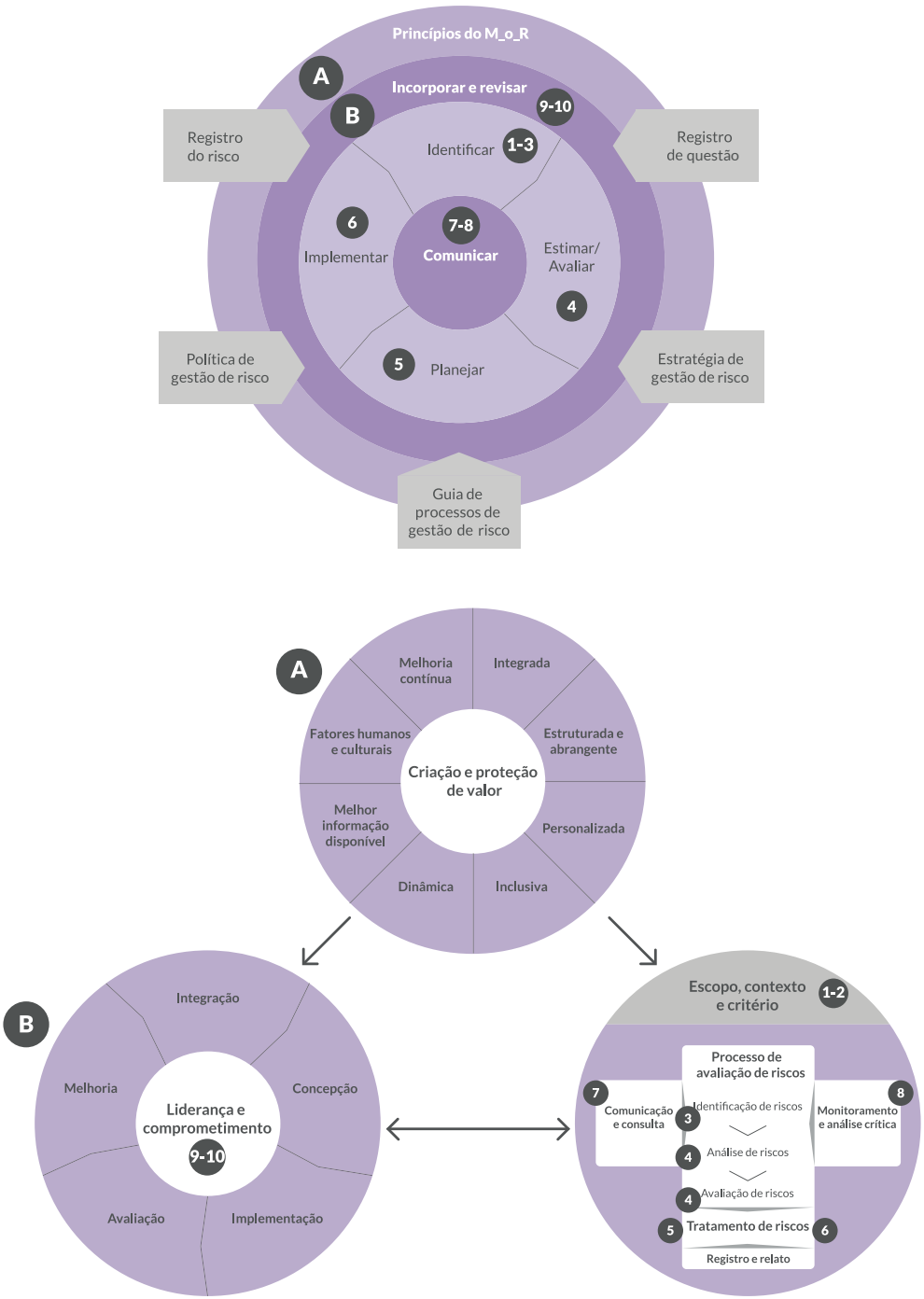


Figura 6 – Comparativo entre as metodologias de gestão de riscos
Fonte: ERM-COSO (2017), ISO 31000 (2018), M_o_R-OGC (2010), com adaptações

Quadro 7 – Comparativo entre as definições das principais metodologias de mercado

ERM-COSO (2017)	ISO 31000 (2018)	M_o_R-OGC (2010)	
Risco é a possibilidade de um evento ocorrer e afetar o alcance dos objetivos (p. 16).	Efeito da incerteza nos objetivos (p. 1).	Um evento ou conjunto de eventos incertos que, caso ocorram, terão um efeito no alcance dos objetivos (p. 135).	**Risco**
É um processo realizado por um Comitê de diretores, gerentes e outras pessoas, aplicado na definição estratégica e em toda a organização. É designado para identificar eventos potenciais que podem afetar a organização e o gerenciamento de riscos (p. 34-35).	Atividades coordenadas para dirigir e controlar uma organização no que se refere a riscos (p. 2).	Aplicação sistemática de princípios, abordagens e processos para as tarefas de identificação e avaliação de riscos, seguidas de planejamento e implantação de respostas aos riscos (p. 136).	**Gestão de riscos corporativos**
Os riscos identificados são analisados para formar uma base que determine como devem ser gerenciados. Em seguida, são associados aos objetivos que podem ser afetados. Por fim, são avaliados levando em conta tanto os riscos herdados quanto os residuais, com a avaliação considerando a probabilidade e o impacto (p. 59).	O processo de avaliação de riscos é o processo global de identificação de riscos, análise de riscos e avaliação de riscos. Deverá ser conduzido de forma sistemática, iterativa e colaborativa (p. 12).	Descreve como os passos do processo serão executados, desde a identificação até a implementação. Envolve identificar, analisar e estimar, planejar e implementar os planos de gestão de riscos desenvolvidos (p. 22).	**Processo de avaliação de riscos**

Há uma definição específica de princípios no guia, correlacionados com os cinco componentes para a gestão de riscos corporativos (p. 23).	A norma apresenta nove princípios para que a gestão de riscos seja eficaz em todos os níveis da organização (p. 3).	O propósito do princípio é comunicar por que e como o gerenciamento de riscos será implementado em nível organizacional para suportar a realização de seus objetivos. São apresentados oito princípios para a gestão (p. 21).	A – Princípios
O ERM-COSO propõe uma estrutura específica para conectar princípios com os processos das organizaçãos, conforme mostra o Quadro 2 deste livro.	O sucesso da gestão de riscos depende da eficácia da estrutura de gestão, que fornece os fundamentos e os componentes para incorporá-la em toda a organização. Seu propósito é apoiar a organização a integrar a gestão de riscos em atividades significativas e funções (p. 4).	A incorporação e a revisão têm como propósito integrar os princípios aos processos de gestão de riscos, realizando uma mudança na cultura organizacional. Deve garantir que a gestão de riscos esteja sendo conduzida de forma apropriada e com sucesso em toda a organização, e conta para isso com o uso de métodos e modelos que permitem alcançar esse resultado (p. 51).	B – Estrutura
Define a base sobre como os riscos e os controles são endereçados por pessoas na organização. O centro de qualquer negócio são suas pessoas – seus valores individuais, incluindo integridade, valores éticos e competência – e o ambiente no qual operam (p. 87).	Definição dos parâmetros externos e internos a serem levados em consideração no gerenciamento de riscos, e estabelecimento do escopo e dos critérios de risco para a Política de Gestão de Riscos (p. 11).	O objetivo da identificação de contexto é obter informações sobre as atividades planejadas para ver como se encaixam em toda a organização de modo a atender ao mercado ou à sociedade (p. 32).	1 – Contexto/ Ambiente
Devem existir objetivos prévios para que o gerenciamento possa identificar eventos potenciais que afetem o seu alcance (p. 101).	Convém que a Política de Gestão de Riscos estabeleça claramente os objetivos, os critérios para avaliar a significância do risco e o comprometimento da organização no que tange à gestão de riscos (p. 11).	A gestão de riscos alinha-se continuamente com os objetivos organizacionais. Está focada nas incertezas, que têm o potencial de impactar o alcance de um ou mais objetivos da organização (p. 13).	2 – Definição de objetivos

ERM-COSO (2017)	ISO 31000 (2018)	M_o_R-OGC (2010)	
Envolve identificar eventos potenciais de fontes internas ou externas que afetam o alcance dos objetivos. Isso inclui a distinção entre eventos que representam riscos, aqueles que representam oportunidades e aqueles que podem ser os dois (p. 109).	Processo de encontrar, reconhecer e descrever os riscos. Convém à organização identificar as fontes de risco, as áreas de impactos, os eventos (incluindo mudanças nas circunstâncias) e as suas causas e consequências potenciais. A finalidade desta etapa é gerar uma lista abrangente de riscos baseada nesses eventos que possam criar, aumentar, evitar, reduzir, acelerar ou atrasar a realização dos objetivos (p. 12).	Identificar riscos nas atividades para o alcance de objetivos a fim de minimizar ameaças enquanto maximiza oportunidades, o que inclui: • identificar oportunidades e ameaças na atividade; • preparar o registro do risco; • preparar indicadores-chave e outros indicadores; e • entender a visão de pessoas-chave quanto ao risco (p. 36).	3 – Identificação
No ERM, a análise e a avaliação ocorrem na mesma etapa, isto é, a etapa de revisão. Segundo o *framework*, a avaliação de riscos permite que a organização considere a abrangência e a proporção na qual eventos potenciais podem impactar no alcance dos objetivos. A gestão dessa avaliação considera as perspectivas, o impacto e a probabilidade relacionada com métodos qualitativos e quantitativos. Também se consideram os riscos herdados e os residuais (p. 138-141).	Processo de compreender a natureza do risco e determinar o seu nível. A análise de riscos envolve a apreciação das causas e as fontes de risco, suas consequências positivas e negativas, e a probabilidade de que essas consequências possam ocorrer (p. 13).	O objetivo da análise é priorizar riscos individuais para esclarecer quais deles são mais importantes e mais urgentes. Para isso, é necessário entender a sua probabilidade, o impacto e a proximidade (p. 38).	4 – Análise
	Processo de comparar os resultados da análise de riscos com os critérios de risco para determinar se o risco e/ou a sua magnitude são aceitáveis ou toleráveis. A finalidade da avaliação de riscos é auxiliar na tomada de decisões com base nos resultados da análise de riscos sobre quais riscos necessitam de tratamento e estabelecer a prioridade para a implementação desse tratamento (p. 13-14).	A avaliação de riscos serve para entender a exposição de risco da atividade na cadeia de efeitos das ameaças e oportunidades dessas atividades em conjunto (p. 41).	4 – Avaliação

O pessoal identifica e avalia possíveis respostas ao risco, as quais incluem aceitar, reduzir, compartilhar ou evitar o risco. A gerência seleciona um conjunto de ações para alinhar riscos com a tolerância e o apetite de riscos da organização (p. 127-129).	O propósito do tratamento de riscos envolve a seleção de uma ou mais opções para modificar os riscos e a implementação dessas opções (p. 14).	O objetivo do plano de gestão de riscos é preparar uma resposta específica para reduzir ameaças e maximizar oportunidades para que o negócio e a sua equipe não sejam surpreendidos caso um risco se materialize (p. 44). A implementação garante que as ações planejadas da gestão de riscos sejam postas em prática e monitoradas quanto à sua efetividade, e para que ações corretivas sejam tomadas (p. 45).	5 e 6 – Tratamento/ Resposta
Informações relevantes são identificadas, capturadas e comunicadas em um formato definido e com frequência regular para que as pessoas executem as suas responsabilidades (p. 157).	Processos contínuos e iterativos que uma organização conduz para fornecer, compartilhar ou obter informações e se envolver no diálogo com as partes interessadas, com o objetivo de gerenciar riscos por meio do registro e do relato destes (p. 16).	A comunicação é conduzida ao longo de todo o processo de gestão de riscos. Como a exposição da organização aos riscos não é estática, a comunicação efetiva é componente-chave para identificação, alterações dos riscos existentes ou novas ameaças e oportunidades (p. 31).	7 – Comunicação
De forma abrangente, a gestão de riscos da organização é monitorada, e modificações são realizadas quando necessário. Assim, é possível reagir de forma dinâmica (p. 161-164).	O objetivo do monitoramento e da análise crítica é assegurar e melhorar a qualidade e a eficácia da gestão. É necessário planejar como parte do processo de gestão de riscos e envolver checagem ou vigilância regulares (p. 16).	O monitoramento é necessário para entender se as respostas estão sendo implementadas de forma efetiva. Embora o monitoramento possua o seu valor, é apenas um processo de observação. Deve ser mais abrangente do que uma revisão de planos de ação (p. 47).	8 - Monitoramento
Quanto à abordagem para condução da gestão de riscos, o *framework* define cinco componentes: (1) governança e cultura; (2) estratégia e definição de objetivos; (3) desempenho; (4) revisão; e (5) informação, comunicação e reporte). Esses componentes estão relacionadas com vinte princípios organizacionais (p. 18-19).	A norma apresenta o mandato e o comprometimento, que compreendem os seguintes fatores: definição e aprovação da política; alinhamento entre cultura e política; indicadores de desempenho; alinhamento com objetivos e estratégias; conformidade; atribuição de responsabilidade e alocação de recursos; e comunicação dos benefícios e manutenção da estrutura (p. 9).	Os princípios fornecem uma base para que a abordagem seja desenvolvida. Nessa abordagem, descrevem-se as atividades a serem executadas, a sequência em que são realizadas, os papéis e as responsabilidades necessários para as entregas. Essas entregas consistem em documentos, tais como registros, planos e relatórios (p. 52).	9-10 – Abordagem

É possível afirmar que as metodologias de mercado possuem um conjunto comum de orientações aos profissionais de gestão de riscos, isto é, similaridades quanto aos temas abordados. Entretanto, como foram desenvolvidas em momentos diferentes, percebe-se uma evolução do foco nas técnicas de gestão, especialmente na ISO 31000 e no M_o_R-OGC, bem como um conjunto abrangente de ferramentas e de técnicas para apoio aos gestores na condução dos riscos na organização em todas as metodologias apresentadas. Por meio desse comparativo, pode-se depreender, ainda, a convergência das metodologias para um entendimento que remete a um processo genérico de gestão de riscos em que se destacam a compreensão do contexto, a identificação e a avaliação de riscos, a elaboração de planos para tratamento e a implementação desses planos.

4.2.Metodologias da Administração Pública brasileira

A seguir, apresentam-se as principais metodologias de gestão de riscos identificadas nos órgãos da AP brasileira. O Quadro 8 relaciona os órgãos em que foram desenvolvidas as metodologias, o título do documento e um breve descritivo.

Quadro 8 – Guias e metodologias sobre gestão de riscos da Administração Pública brasileira

Órgão	Título	Descrição
Escola Nacional de Administração Pública (2006)	Guia sobre a Gestão de Riscos no Serviço Público	Este guia não se propõe a fazer uma avaliação exaustiva da gestão de riscos ou a abordar todos os detalhes do tema. Sua intenção é criar um ponto de partida comum para se aprender e trabalhar em cima do que constitui uma boa gestão de riscos e assim se ter uma noção dos obstáculos que podem ser enfrentados na incorporação da gestão de riscos a processos decisórios governamentais. Para que o maior número possível de pessoas possa beneficiar-se da leitura deste guia, jargões técnicos foram evitados e foi feito um esforço para mantê-lo sucinto. Os leitores que desejarem ter informações mais abrangentes podem consultar a lista de recursos adicionais incluída no final do guia.
Instituto Brasileiro de Governança Corporativa (2007)	Guia de Orientação para Gerenciamento de Riscos Corporativos	As recomendações e sugestões contidas no guia devem ser avaliadas conforme a realidade de cada organização. Apesar de destinar-se primariamente a empresas com fins lucrativos, os conceitos e as sugestões poderão ser utilizados também por entidades do primeiro e terceiro setores.

Ministério do Planejamento, Orçamento e Gestão (2013)	Guia de Orientação para o Gerenciamento de Riscos	Este guia tem como objetivos principais apoiar o Modelo de Excelência do Sistema de Gestão Pública no que tange ao tema de gerenciamento de riscos e prover uma introdução ao tema gerenciamento de riscos.
Ministério da Fazenda (2014)	Frente Gestão de Riscos	Modelo de gestão integrada de riscos corporativos para o MF.
Ministério do Planejamento, Desenvolvimento e Gestão (2016)	Metodologia de Gestão de Riscos de Segurança da Informação e Comunicações do Sistema de Administração dos Recursos de Tecnologia da Informação do Poder Executivo Federal – MGR-SISP v 2.0	A metodologia visa padronizar e sistematizar a Gestão de Riscos de Segurança da Informação e Comunicação (GRSIC) na Administração Pública Federal (APF). Almeja-se assim atingir níveis satisfatórios de SIC e, ao mesmo tempo, racionalizar os investimentos por priorizar ações e evitar redundâncias na gestão de riscos.
Superior Tribunal de Justiça (2016)	Gestão de Riscos	Os processos de trabalho do STJ envolvem riscos. Logo, a consciência de que existem e a capacidade de administrá-los, associadas à disposição de correr riscos e de tomar decisões, são indispensáveis. Com a implantação desta metodologia de gestão de riscos baseada em experiências comprovadas, busca-se cada vez mais a excelência na prestação de serviços públicos de qualidade aos jurisdicionados com celeridade e transparência.
Instituto Brasileiro de Governança Corporativa – (2017)	Gerenciamento de Riscos Corporativos – Evolução em Governança e Estratégia	Integra a série de publicações denominada Cadernos de Governança Corporativa, cujo objetivo é trazer ao mercado informações práticas que contribuam para o processo da governança corporativa. Propõe apresentar reflexões e orientações para executivos e, sobretudo, conselheiros de administração interessados em implantar ou aprimorar o modelo de gerenciamento de riscos corporativos (GRCorp) das organizações em que trabalham. O documento tem o propósito de servir a organizações em diferentes estágios de maturidade do GRCorp.
Ministério do Planejamento, Desenvolvimento e Gestão (2017)	Manual de Gestão de Integridade, Riscos e Controles Internos da Gestão (GIRC)	Busca apresentar a metodologia de gerenciamento de integridade, riscos e controles internos da gestão do Ministério do Planejamento, Desenvolvimento e Gestão, no contexto do modelo em desenvolvimento no MP (política, instâncias de supervisão, metodologia e solução tecnológica).

Foram consideradas para análise as metodologias do Ministério do Planejamento, Desenvolvimento e Gestão, elaboradas pela Coordenação-Geral de Segurança da Informação – CGSIN/DESIN/STI/MP, a MGR-SISP, de agosto de 2016, e o Manual de Gestão de Integridade, Riscos e Controles Internos da Gestão, elaborado pela Assessoria Especial de Controle Interno do MP, a GIRC, de janeiro de 2017, por estarem alinhadas à Instrução Normativa Conjunta nº 01/2016, e a metodologia do IBGC 2017, por propor a avaliação da maturidade da organização no que se refere à gestão de riscos. Outras metodologias não foram consideradas nessa análise devido à similaridade com as metodologias de mercado ou ao escopo especializado do órgão em que foi desenvolvida.

4.2.1. Metodologia de Gestão de Integridade, Riscos e Controle Interno – GIRC

Segundo o Ministério do Planejamento, Desenvolvimento e Gestão, o Programa de Integridade tem a finalidade de mitigar ocorrências de corrupção e desvios éticos a partir da mobilização e da participação ativa dos gestores públicos por meio de medidas que assegurem a entrega dos resultados esperados pela sociedade, o fortalecimento e o aprimoramento da estrutura de governança, a gestão de riscos e controles, e os procedimentos de integridade [26].

Nesta metodologia desenvolvida pela Assessoria Especial de Controle Interno do MP, estão descritas premissas, conceitos, papéis e responsabilidade, taxonomia de eventos de riscos e lista de controles básicos para uma organização pública. É constituída de quatros pilares:

- 1º pilar - Ambiente de Integridade: oferece as bases para que o programa seja efetivo; é composto de ações de comprometimento, do apoio da alta administração e de alinhamento ao planejamento estratégico;

- 2º pilar - Gestão de Integridade, Riscos e Controles: definição de uma Política de Gestão de Riscos; instituição do Subcomitê de Integridade, Riscos e Controles (SIRC); e implementação do gerenciamento de riscos;

- 3º pilar - Instituição e Conformidade de Procedimentos de Integridade: a integridade envolve o desenvolvimento do código de conduta, canal de denúncias, plano de capacitação e educação interna; a conformidade envolve ações que fomentem a declaração de bens, combatem o conflito de

interesses e a presença de nepotismo, e implementação da Lei de Acesso à Informação; e

• 4º pilar - Informação, Comunicação e Monitoramento: processo de disponibilização da informação para as partes interessadas, relacionamento entre as instâncias de supervisão e de monitoramento das ações do programa para avaliar a qualidade do sistema de controle interno ao longo do tempo.

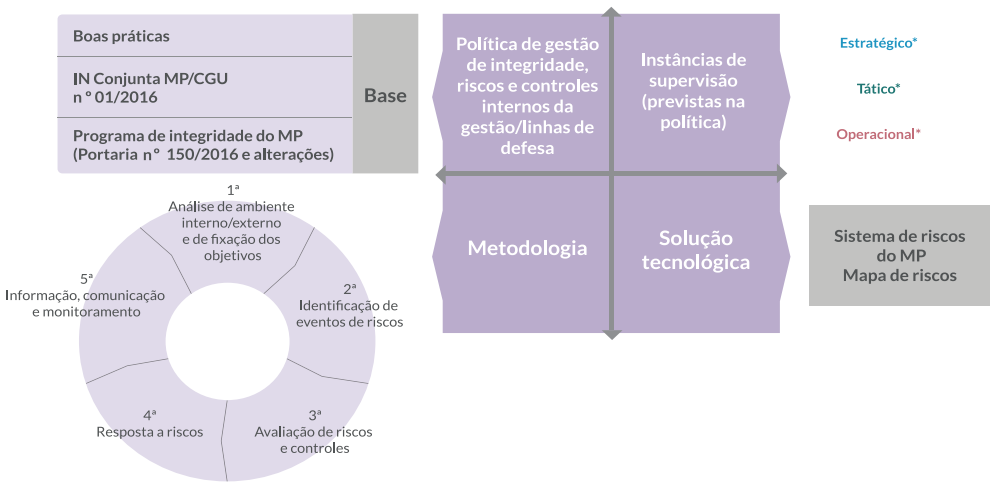
Esses pilares fornecem uma base para que ocorra a gestão de integridade, riscos e controle na organização por meio do modelo metodológico representado na Figura 7. Na metodologia, são apresentadas:

• a política, que estabelece os princípios, as diretrizes e as responsabilidades;

• a instância de supervisão, que assessora a autoridade máxima do órgão na definição e na implementação de diretrizes, políticas, normas e procedimentos;

• a metodologia GIRC, que pressupõe que a cadeia de valor e os processos da organização estejam mapeados para aplicação do "Método de Priorização de Processos"; e

• a solução tecnológica, que serve como um instrumento de apoio à aplicação da metodologia GIRC [26].



(continua)

Detalhamento das instâncias de supervisão

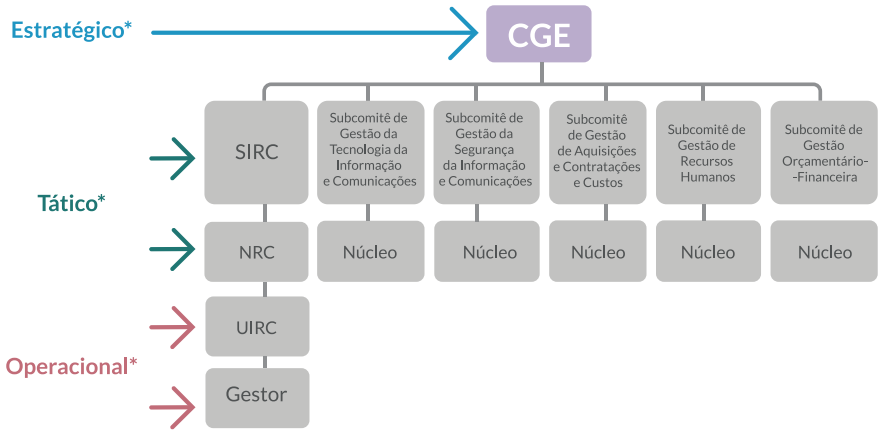


Figura 7 – Metodologia de gestão de integridade, riscos e controle interno
Fonte: GIRC (2017, p. 16), com adaptações

A metodologia se inicia a partir do documento "Método de Priorização de Processos". Nele é possível identificar e avaliar os processos e os eventos de risco, priorizar aqueles que apresentam os riscos mais críticos e adotar respostas aos eventos de risco dos processos da unidade. Adicionalmente, esse registro ainda fornece diretrizes básicas sobre boas práticas para despertar nos gestores a importância da gestão de integridade, riscos e controles internos [26].

A maior contribuição dessa metodologia corresponde à estrutura desenvolvida previamente à aplicação da gestão de riscos, que define uma política a ser seguida, os papéis e as responsabilidades, os métodos de registro e de acompanhamento dos riscos, e o alinhamento dessas dimensões com a Tecnologia da Informação (TI) para viabilizar um sistema de informações a fim de facilitar a gestão de riscos nas organizações. Realiza ainda uma importante contribuição quanto à disponibilização de ferramentas de controle interno para viabilizar o registro e o acompanhamento por meio da "Metodologia de Priorização de Processos" e da "Planilha Documentadora", constantes no site do Ministério do Planejamento.

4.2.2. Metodologia de gestão de riscos do SISP – MGR-SISP

O MP, por meio da Coordenação-Geral de Segurança da Informação – CGSIN/DESIN/STI/MP, desenvolveu uma metodologia de gestão de riscos

voltada à Segurança da Informação e Comunicações do Sistema de Administração dos Recursos de Tecnologia da Informação do Poder Executivo Federal, conforme Instrução Normativa Conjunta CGU/MP nº 01/2016. Embora tenha sido desenvolvida com foco na Gestão de Riscos de Segurança da Informação e Comunicação (GRSIC), a norma pode ser adaptada como um processo genérico de gestão de riscos.

A metodologia traz uma grande contribuição no que se refere ao contexto brasileiro ao compreender referências a normas e leis vigentes aplicadas à gestão de riscos e, ainda, por dispor de um conjunto de processos, atividades e tarefas de forma estruturada, conforme ilustra a Figura 8. No processo, a comunicação e o monitoramento são tarefas que devem acontecer em paralelo com o conjunto de processos de gestão de riscos. Infere-se, dessa maneira, uma forte similaridade com a metodologia ISO 31000 em uma sequência lógica de passos para a resolução dos riscos.

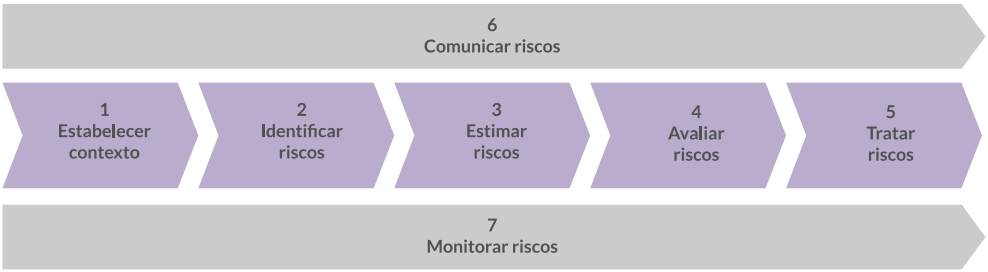


Figura 8 – Metodologia de gestão de riscos proposta pela MGR-SISP
Fonte: MGR-SISP (2016, p. 36)

Esta metodologia possui 7 processos que contêm 16 atividades, totalizando 65 tarefas para a condução da gestão de riscos, conforme apresenta o Quadro 9. Também estão definidos os papéis para a condução dessas tarefas, os quais correspondem a:

- Autoridade competente: responsável por prover os recursos necessários à gestão de riscos, identificar responsáveis, iniciar as atividades de gestão de riscos e aprovar pontos importantes relativos à gestão de riscos, tais como objetivo, restrições e aprimoramentos da MGR-SISP;

- Gestor de riscos: responsável por executar as atividades de gestão de riscos e coordenar esforços para identificar e estimar riscos, propor melho-

rias necessárias para mitigar riscos, além de comunicar os resultados de análises a todos os interessados;

• Responsável pela unidade da organização: responde por uma área da organização na qual a metodologia será implementada ou por uma área que deve prover informações para a gestão de riscos. Tem o papel de coordenar o fornecimento das informações necessárias à identificação e à estimativa de riscos, e realizar melhorias necessárias quando as análises indicarem;

• Responsável por ativos: responde pelo fornecimento de informações sobre os ativos que fazem parte da análise de riscos. Essas informações auxiliam a tomada de decisões sobre controles a serem implementados.

No Quadro 9, esses responsáveis e suas respectivas tarefas estão representados pelas seguintes siglas: AC – Autoridade Competente, em preto; GR – Gestor de Riscos, em azul; RA – Responsável por Ativos, em laranja; e RU – Responsável pela Unidade da Organização, em verde. A cor cinza foi utilizada para mais de um papel [10].

Quadro 9 – Tarefas presentes na MGR-SISP

Processo	Atividade	Tarefa	Papel(is)
1. Estabelecer contexto	1.1 Iniciar projeto de GRSIC	1.1-A: Definir gestor de riscos	AC
		1.1-B: Identificar objetivos, premissas, restrições e escopo do projeto de GRSIC	GR
		1.1-C: Validar objetivos, premissas, restrições e escopo do projeto de GRSIC	AC
		1.1-D: Definir responsáveis pelas unidades da organização	GR
		1.1-E: Definir responsáveis por ativos	RU
	1.2 Realizar pré-análise do escopo do projeto de GRSIC	1.2-A: Elaborar questionário	GR
		1.2-B: Identificar os profissionais para responder ao questionário	GR
		1.2-C: Obter respostas	GR
		1.2-D: Consolidar resultados	GR
		1.2-E: Validar resultados	AC

Processo	Atividade	Tarefa	Siglas
2. Identificar riscos	2.1 Identificar ativos	2.1-A: Definir abordagem da GRSIC	RU/GR
		2.1-B: Cadastrar ativos	RU
		2.1-C: Validar informações sobre os ativos	GR
	2.2 Identificar ameaças, controles e vulnerabilidades	2.2-A: Solicitar identificação de ameaças, controles e vulnerabilidades	GR
		2.2-B: Obter ameaças, controles e vulnerabilidades dos ativos da unidade	RU
		2.2-C: Informar ameaças, controles e vulnerabilidades dos ativos da unidade	RA
		2.2-D: Validar ameaças, controles e vulnerabilidades dos ativos da unidade	RU
		2.2-E: Validar informações sobre ameaças, controles e vulnerabilidades	GR
3. Estimar riscos	3.1 Avaliar impacto	3.1-A: Solicitar análise de impactos	GR
		3.1-B: Obter informações sobre as consequências	RU
		3.1-C: Identificar consequências	RA
		3.1-D: Definir impactos	RU
		3.1-E: Validar análise de impactos	GR
	3.2 Avaliar probabilidade	3.2-A: Solicitar avaliação de probabilidades	GR
		3.2-B: Solicitar definição de probabilidades	RU
		3.2-C: Definir probabilidades	RA
		3.2-D: Avaliar probabilidades	RU
		3.2-E: Validar avaliações de probabilidades	GR
	3.3 Estimar nível de risco	3.3-A: Solicitar estimativas de riscos de cada unidade	GR
		3.3-B: Solicitar estimativas de riscos	RU
		3.3-C: Definir estimativas de riscos	RA
		3.3-D: Avaliar estimativas de riscos da unidade	RU
		3.3-E: Validar estimativas de riscos do projeto de GRSIC	GR
4. Avaliar riscos	4.1 Classificar os riscos	4.1-A: Realizar classificação de riscos	GR
		4.1-B: Registrar ciência da classificação de riscos	RU
		4.1-C: Solicitar validação da classificação de riscos	GR
		4.1-D: Validar classificação de riscos	AC

5. Tratar riscos	5.1 Estimar recursos para o tratamento dos riscos	5.1-A: Solicitar estimativas de tratamento	GR
		5.1-B: Estimar custos, esforços, prazos e restrições	RU
		5.1-C: Validar estimativas	GR
	5.2 Definir resposta aos riscos	5.2-A: Definir tratamento	GR
		5.2-B: Definir controles e monitoramento	GR
		5.2-C: Analisar resposta aos riscos	RU
		5.2-D: Solicitar validação das respostas aos riscos	GR
		5.2-E: Validar respostas aos riscos	AC
	5.3 Implementar resposta aos riscos	5.3-A: Solicitar Plano de Tratamento de Riscos (PTRs)	GR
		5.3-B: Elaborar Plano de Tratamento de Riscos	RU
		5.3-C: Avaliar Plano de Tratamento de Riscos	GR
		5.3-D: Validar Plano de Tratamento de Riscos	AC
		5.3-E: Iniciar tratamento de riscos	RU
		5.3-F: Executar Plano de Tratamento de Riscos	RA
6.Comunicar riscos	6.1 Planejar comunicação de riscos	6.1-A: Elaborar Plano de Comunicação de Riscos	GR
		6.1-B: Validar Plano de Comunicação de Riscos	AC
	6.2 Executar plano de comunicação de riscos	6.2-A: Obter informações sobre a GRSIC	GR
		6.2-B: Enviar informações sobre a GRSIC às partes interessadas	GR
	6.3 Validar informações estratégicas	6.3-A: Obter informações estratégicas sobre a GRSIC	AC
		6.3-B: Avaliar informações estratégicas sobre a GRSIC	AC
7. Monitorar riscos	7.1 Monitorar a gestão de riscos de SIC	7.1-A: Verificar alterações que impactam a GRSIC	Todos
		7.1-B: Comunicar alterações que impactam a GRSIC	Todos
		7.1-C: Solicitar atualização da GRSIC	GR
		7.1-D: Atualizar informações da GRSIC	Todos
	7.2 Monitorar o tratamento de riscos	7.2-A: Validar tratamentos	RU
		7.2-B: Monitorar execução dos PTRs	GR
		7.2-C: Monitorar estrategicamente	AC
		7.2-D: Verificar necessidades de alteração no tratamento dos riscos	GR

Fonte: MGR-SISP (2016, p. 31-34), com adaptações

Compreende-se que a GRSIC conta com ferramentas para apoiar gestores e ainda se adéqua ao contexto nacional. Apesar de possuir tarefas específicas para o cenário da Segurança da Informação e Comunicação (SIC), é possível realizar generalizações para outros casos ou outras organizações. Ademais, o MP ofereceu ferramentas em formato eletrônico para apoiar os gestores no registro e na identificação desses riscos, como a Planilha de Priorização de Processos e a Planilha Documentadora". Contudo, essas ferramentas apresentam limitações e restrições quanto ao tratamento e ao acompanhamento dos riscos. De toda forma, na MGR-SISP, a explanação do conjunto de tarefas e de papéis contribui profundamente para que as incertezas sejam dirimidas.

4.2.3. Metodologia de gestão de riscos do IBGC

Segundo a metodologia do IBGC (2017) quanto ao gerenciamento de riscos corporativos (GRCorp), o Conselho de Administração deve ser responsável por determinar os objetivos estratégicos e o mapa de riscos da organização. Isso consiste em identificar o "grau de apetite" aos riscos da organização e as faixas de tolerância e desvios em relação aos níveis de riscos aceitáveis. A metodologia deve ainda estabelecer a política de responsabilidade da diretoria para avaliar a quais riscos a organização pode ficar exposta, desenvolver procedimentos para administrá-los e avaliar, discutir e aprovar a política de riscos proposta pelo Comitê Executivo de Riscos [16].

É recomendável que os integrantes do Conselho de Administração possuam conhecimentos de indicadores de desempenho para opinar sobre o assunto. Também se sugere que a empresa tenha um programa para trazer a cultura de gestão de riscos a novos conselheiros. O papel de implementar uma estrutura de gerenciamento de riscos e controle é atribuído aos gestores, com o Comitê de Auditoria exercendo a atividade de supervisão, auxiliado, quando necessário, pelas três linhas de defesa, respectivamente:

- 1ª linha de defesa – realizada pelos gestores das unidades e responsáveis diretos pelos processos: contempla as funções que gerenciam e tem a responsabilidade sobre os riscos;

- 2ª linha de defesa – realizada pelos gestores corporativos do GRCorp, gestores de conformidade ou de outras práticas de controle, por exemplo, e contempla as funções que monitoram a visão integrada dos riscos;

- 3ª linha de defesa – realizada pela auditoria interna: fornece avaliações independentes por meio do acompanhamento dos controles internos.

Existem distintas alternativas para a construção da governança do GRCorp e para se chegar ao nível de maturidade desejado. Cada organização deverá desenhar aquela mais adequada ao seu perfil de negócio, cultura organizacional, modelo de gestão e nível requerido de maturidade em relação às suas práticas de GRCorp. Para a medição da maturidade, é necessário que as organizações avaliem a capacidade atual em relação às práticas de riscos e que compreendam como e por que devem aperfeiçoá-las. Essa avaliação permitirá que as organizações possam documentar, comunicar e programar melhorias no seu modelo [16].

A Figura 9 apresenta uma visão geral dos componentes do GRCorp integrados ao processo de governança corporativa da organização e seus principais elementos para a mensuração de maturidade. Nessa representação, a Regulamentação (Compulsória e Facultativa) apoia a definição dos contextos externos e internos que influenciam a governança corporativa. Para cada componente, deve haver reflexões para se identificar o nível de maturidade atual. No Quadro 10, essas reflexões, separadas em componentes, estão registradas e devem complementar a Figura 9.

As reflexões do Quadro 10 contribuem para a identificação do estágio de maturidade segundo os componentes do GRCorp. Para cada contexto ou estágio, é necessário entender qual o nível de maturidade a organização está para a gestão de riscos e quais seriam as ações para o alcance do próximo nível. No Quadro 11, estão registrados esses níveis de maturidade, os quais devem contribuir na identificação do estado atual da organização e nos passos futuros.

A metodologia do IBGC (2017) propõe os seguintes níveis de maturidade em relação aos estágios do GRCorp de uma organização:

- Inicial;
- Fragmentado;
- Definido;
- Consolidado; e
- Otimizado.

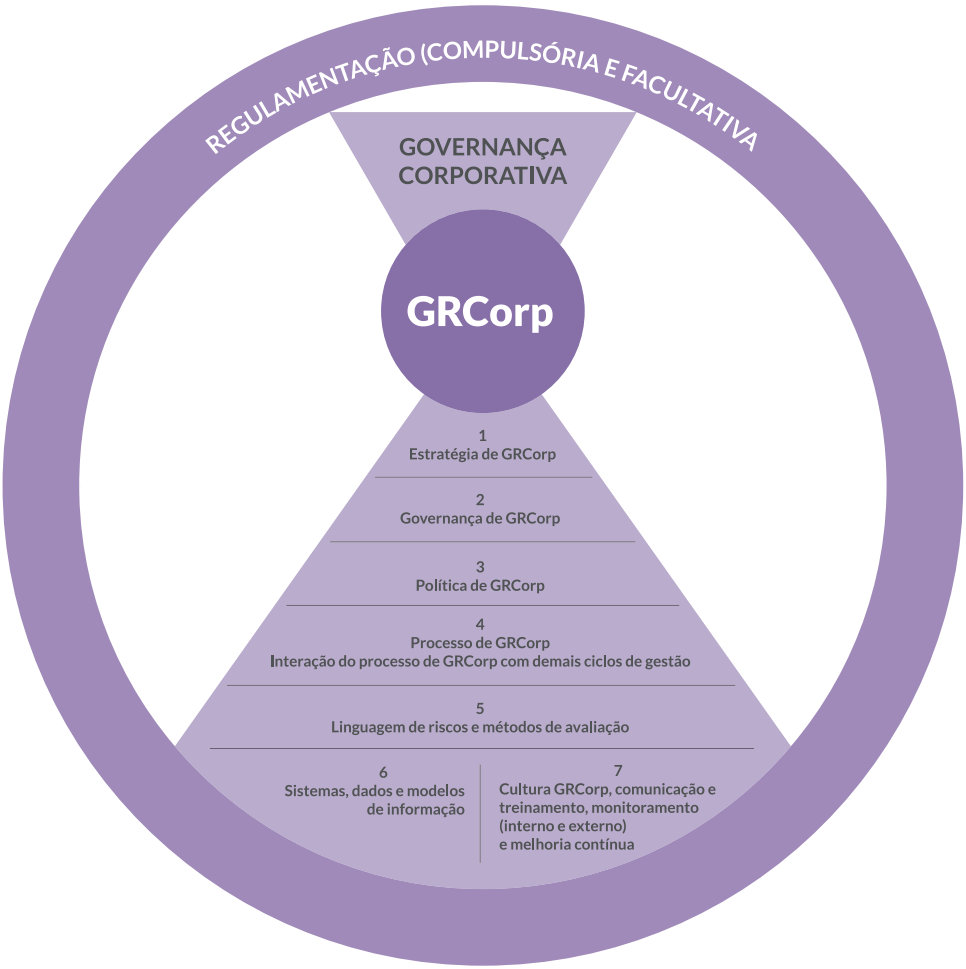


Figura 9 – Gestão de riscos do IBGC – Avaliação de maturidade
Fonte: IBGC (2017, p. 34), com adaptações

Quadro 10 – Reflexões quanto aos componentes do GRCorp

Componente do GRCorp	Reflexões
(1) Estratégia de GRCorp	• Existem estratégias, objetivos e metas de GRCorp estabelecidos?
(2) Governança de GRCorp	• Existe estrutura organizacional com papéis e responsabilidades claramente definidos nas práticas de GRCorp? • A estrutura considera os papéis do Comitê e da diretoria, e de todas as três linhas de defesas detalhadas no modelo de governança de GRCorp?
(3) Política de GRCorp	•As questões acima mencionadas estão regimentadas, aprovadas e divulgadas por meio de uma política de GRCorp?
(4) Processo de GRCorp e interação desse processo com os demais ciclos de gestão	• Existe processo de GRCorp definido e implementado com atividades de identificação de riscos, avaliação de riscos (incluindo cenários), avaliação das atividades de controle, resposta, monitoramento e comunicação? • Existe norma de gestão de riscos (ou documento equivalente) de divulgação interna que estabelece procedimentos, responsabilidades – inclusive de relato –, segregação de funções, fronteiras de atuação e o sistema geral de governança da gestão de riscos? • As práticas de GRCorp estão alinhadas às demais práticas de controle? • Existe um modelo definido para a incorporação do GRCorp nos processos decisórios e nos ciclos de gestão?
(5) Linguagem de riscos e métodos de avaliação	• Existe taxonomia de riscos (categorias) e métodos de avaliações definidos? • A organização utiliza-se de técnicas de mensuração?
(6) Sistemas, dados e modelos de informação	• As informações sobre a exposição de riscos da organização são compartilhadas com os diferentes níveis organizacionais e capturadas de forma consistente?
(7) Cultura de GRCorp, comunicação e treinamento, monitoramento (interno e externo) e melhoria contínua	• O GRCorp está incorporado no processo decisório, na cultura da organização e no dia a dia da gestão do negócio? • A organização avalia o entendimento dos empregados em relação à cultura, às práticas de GRCorp e ao sistema de controles internos? • As ações de comunicação e treinamento da cultura de GRCorp são realizadas com os diferentes públicos da organização? • Os órgãos de governança e as três linhas de defesa monitoram permanentemente as práticas de GRCorp? • O GRCorp é realizado de forma contínua?

Quadro 11 – Mensuração de maturidade em relação aos componentes

Inicial	Fragmentado	Definido	Consolidado	Otimizado
(1) Estratégia de GRCorp				
A organização não sabe como, quem, quando, onde e por que implementar a gestão de riscos. As metas de desempenho existem.	A organização sabe por onde começar, mesmo que não tenha claro aonde quer chegar. As metas de desempenho existem.	Estratégia de gestão de riscos claramente definida e implementada. As metas de desempenho são definidas.	Estratégia de gestão de riscos claramente definida e implementada. As metas de desempenho são monitoradas.	Estratégia de gestão de riscos claramente definida, implementada e integrada aos demais ciclos de gestão. As metas de desempenho estão alinhadas com a estratégia e a gestão de riscos.
(2) Governança de GRCorp				
As funções da 2ª linha de defesa são realizadas individualmente, não integradas à visão estratégica.	As funções da 2ª linha de defesa focam nas áreas históricas, em resposta ao cumprimento das obrigações regulatórias.	As funções da 2ª linha de defesa cobrem os riscos de negócio e os direcionadores de valor, podendo haver sobreposições. A estrutura organizacional está definida.	As funções da 2ª linha de defesa cobrem de forma abrangente os riscos da organização. A estrutura organizacional está bem definida e alinhada à estratégia e aos objetivos.	Os objetivos estão claramente definidos e alinhados entre as diversas funções da 2ª linha de defesa a fim de prover valor para a organização. O modelo é referência no setor.

Inicial	Fragmentado	Definido	Consolidado	Otimizado
(3) Política de GRCorp				
Políticas e procedimentos não estão definidos, e não há um processo consistente para o seu desenvolvimento e a sua manutenção.	Políticas e procedimentos são limitados a áreas direcionadoras-chave.	Políticas e procedimentos de GRCorp são formais e comunicados de forma consistente em toda a organização.	Políticas e procedimentos são bem desenvolvidos e aplicados consistentemente em toda a organização. São continuamente atualizados de acordo com as mudanças na estratégia de negócios.	Políticas e procedimentos são regularmente referenciados por terceiros e pelo setor. As políticas têm impacto sobre o ambiente de negócios externo.
(4) Processo de GRCorp e sua interação com os demais ciclos de gestão				
Processos e controles que dão apoio à gestão de riscos são pouco desenvolvidos. Mínimas atividades de monitoramento ocorrem.	Os processos de identificação e avaliação de riscos são executados como atividades distintas ou separadas acontecendo sob demanda.	Uma abordagem baseada em riscos é executada de maneira sistemática e consistentemente aplicada em nível corporativo e por toda a organização.	Os processos de identificação e avaliação de riscos estão bem definidos e estruturados. Os gestores de negócio monitoram sistematicamente os riscos associados aos seus processos.	Os processos de identificação e avaliação de riscos estão bem integrados aos objetivos estratégicos. Atividades de monitoramento eficientes e coordenadas.
(5) Linguagem de riscos e métodos de avaliações				
Não há abordagem padronizada para definir o nível aceitável de riscos. Análises qualitativas e quantitativas são realizadas.	Não há abordagem padronizada para definir o nível aceitável de riscos. Análises qualitativas e quantitativas são realizadas.	Há uma abordagem padronizada para definir o nível aceitável de riscos. No entanto, ela não é utilizada por todas as funções de maneira consistente.	Utiliza abordagem padronizada e consistente para definir o apetite e a tolerância a riscos. Testes de estresse e análise de cenários são utilizados em nível corporativo.	Utiliza abordagem padronizada e consistente para definir o apetite e a tolerância a riscos. Cenários futuros e testes de estresse são utilizados para explorar a análise dos riscos.

(6) Sistemas, dados e modelos de informação				
Modelos de informações e de relatórios são direcionados por exigências externas e não são suficientemente definidos.	Modelos de informações e de relatórios são definidos pela alta direção, mas não são compreendidos pela gestão ou alinhados na organização.	Modelos de informações e de relatórios são bem definidos e compreendidos. Os relatórios são elaborados com informações corretas, completas.	Tecnologias emergentes são aproveitadas para permitir que os objetivos de gestão de riscos sejam alcançados em nível corporativo.	Tecnologias integradas habilitam a organização a gerenciar os riscos e são consideradas altamente efetivas e reconhecidas como práticas líderes pelo mercado.
(7) Cultura, comunicação e treinamento, monitoramento e melhoria contínua				
Não há um plano de disseminação implementado para formalizar as principais decisões da organização no tocante às práticas de riscos.	Existem comunicações, mas não estão formalmente definidas. Treinamentos pontuais são realizados.	Protocolos claros de comunicação existem e são abertos a todos os empregados. A comunicação de duas vias com as partes interessadas é incentivada.	A cultura de riscos e controles está inserida nas atividades diárias da organização, e os riscos são proativamente tratados nos níveis de processo e de funções.	A cultura de riscos e controles é efetiva em todos os níveis da organização. Programas de disseminação são aplicados para a evolução contínua da gestão de riscos.

Fonte: IBGC (2017), com adaptações

Cabe lembrar que os níveis de maturidade dos componentes são independentes entre si. Isso significa que cada componente (individualmente) poderá se posicionar em diferentes níveis de maturidade.

Após realizar a avaliação do nível de maturidade, o Conselho de Administração deve refletir em qual estágio a organização deve estar e, na sequência, desenvolver ações necessárias para definir os prazos esperados a fim de atingir os próximos estágios. A escala de maturidade (Figura 10) fornece um guia estruturado e detalhado com vistas à melhoria contínua, em busca de resultados de curto, médio e longo prazos para a estratégia GRCorp [16].

Por meio deste instrumento disposto na Figura 10, a organização pode documentar, comunicar e programar melhorias quanto ao seu ambiente interno. A metodologia ainda recomenda realizar uma pesquisa por padrões na indústria, de modo a se comparar a organização com as empresas líderes nessas práticas de GRCorp. Para essa aferição do nível de maturidade, foi realizada uma junção das dimensões (princípios) do M_o_R (2010) com a forma de medição e apresentação contidas na metodologia do IBGC (2017). Esse ajuste facilita o entendimento e permite a criação de planos de melhorias e outras ações.

4.2.4. Comparação entre as principais metodologias da Administração Pública brasileira

As metodologias da AP, assim como as de mercado, foram desenvolvidas para atender a diferentes necessidades e instituições desse setor. No Brasil, como é possível perceber, algumas metodologias foram se estruturando, a partir de 2006, por órgãos distintos desse âmbito e para responder aos objetivos organizacionais nessas instituições ou ainda para apoiá-los. A seguir, realiza-se um comparativo entre os principais conceitos apresentados pelas metodologias destacadas neste estudo no que se refere à gestão de riscos pela AP brasileira. Os resultados desse comparativo estão apresentados no Quadro 12.

	Nível de maturidade							
Dimensão	Inicial	Fragmentado	Definido	Consolidado	Otimizado	Estágio atual	Estágio desejado	Plano de ação
						★	★	
Alinhado aos objetivos	★ →	★				2	2	Plano de ação A
Adequado ao contexto		★ →	★			3	3	Plano de ação B
Envolve *stakeholders*		★ →	★			3	3	Plano de ação C
Processo definido		★ →		★		4	4	Plano de ação D
Tomada de decisão		★ →			★	5	5	Plano de ação E
Melhoria contínua	★ →		★			3	3	Plano de ação F
Cultura colaborativa	★ →	★				2	2	Plano de ação G
Valores mensuráveis		★ →	★			3	3	Plano de ação H

Figura 10 – Estrutura de nível de maturidade para melhoria contínua
Fonte: IBGC (2017), M_o_R (2010), com adaptações

Quadro 12 – Comparativo entre as definições das principais metodologias da Administração Pública brasileira

GIRC (2017)	MGR-SISP (2016)	IBGC (2017)	Item
Neste modelo, a política é quem deve estabelecer os princípios, as diretrizes e as responsabilidades dos envolvidos e de toda a instituição.	Representa o propósito dos investimentos em gestão de riscos. Esse propósito deve estar associado à missão e aos objetivos da organização, e deve também ser documentado e aprovado por representantes da alta administração.	Deve ser de responsabilidade da diretoria da organização. Sua função é documentar e criar meios de avaliar os riscos aos quais a instituição pode estar exposta e desenvolver procedimentos para administrá-los.	Política
Visa mitigar ocorrências de corrupção e desvios éticos a partir da mobilização e da participação ativa dos gestores públicos por meio de medidas que assegurem a entrega dos resultados esperados pela sociedade, pelo fortalecimento e aprimoramento da estrutura de governança, gestão de riscos e controles, e procedimentos de integridade.	Busca garantir a gestão de riscos com foco na Segurança da Informação e Comunicação (SIC). Essa gestão de riscos deve permitir a melhor comunicação e a tomada de decisões mais adequada sobre as prioridades para a alocação de recursos de SIC.	Entende que o Conselho de Administração deve ser responsável por determinar os objetivos estratégicos e o mapa de riscos da organização. Isso consiste em identificar o "grau de apetite" aos riscos da organização e as faixas de tolerância e desvios em relação aos níveis de riscos aceitáveis. Em resumo, tem a finalidade de estabelecer e mensurar a maturidade da gestão de riscos da instituição.	Finalidade/Objetivo
O ambiente e a gestão de integridade, riscos e controle; a instituição e a conformidade de seus procedimentos; a informação, a comunicação e o monitoramento.	Racionalização do uso dos recursos: evitar proteções redundantes e proteger os recursos vitais.	O funcionamento de estratégias, política, processos, linguagens de riscos e métodos de avaliação, sistema de dados, cultura, comunicação e monitoramento para a governança corporativa.	Pilares
Pressupõe a análise dos ambientes interno e externo, a identificação de eventos de riscos, a avaliação de riscos e controle, respostas aos riscos, informação, monitoramento e controle.	Devem ser identificados os riscos existentes e a probabilidade de que de fato ocorram, assim como a extensão e a gravidade dos efeitos negativos produzidos. Isso é determinado por um conjunto de 65 tarefas agrupadas em 16 atividades, que são organizadas em 7 processos.	Visa ao estabelecimento da política, à divisão de responsabilidades (em linhas de defesa), à identificação e avaliação dos riscos, à obtenção do nível de maturidade (inicial, fragmentado, definido, consolidado, otimizado), à comunicação, ao treinamento, ao monitoramento e à melhoria contínua dos processos.	Metodologia

Notadamente, cada uma das metodologias avaliadas apresenta pensamento estruturado no que corresponde às suas políticas, finalidade e objetivos, pilares e à própria estruturação metodológica. A principal diferença entre elas, portanto, diz respeito à aplicação prática, visto que a GIRC (2017) tem foco em manter a integridade dos processos pelos gestores públicos que devem corresponder às expectativas da sociedade; a MGR-SISP (2016) intenciona melhorar a comunicação e a tomada de decisão direcionada à segurança da informação; e a metodologia IBGC (2017) pretende estabelecer o nível de maturidade das instituições. Em suma, não destacamos uma metodologia melhor do que a outra, mas, em verdade, uma metodologia poderá ser mais adequada do que a outra, dependendo do interesse de cada organização.

4.3. Ferramentas para acompanhamento dos riscos

Uma vez que o registro dos riscos está ocorrendo no ambiente, é necessário um conjunto de ações para permitir que esses riscos sejam comunicados e reportados de forma efetiva aos tomadores de decisão. Algumas ferramentas destinadas a esse fim são apresentadas a seguir.

4.3.1. Mapa de riscos

O mapa de riscos é uma ferramenta que permite avaliar os riscos segundo os critérios ou parâmetros fornecidos pelos especialistas, técnicos ou responsáveis pela identificação do risco. Nesse caso, o mapa deve refletir a análise dos riscos para permitir uma visão holística, isto é, indicar o risco no momento anterior ao tratamento e sua situação atual. Esses riscos podem ser filtrados para a organização ou o departamento tanto quanto as oportunidades ou ameaças e outros mecanismos de agrupamento que facilitem a visualização do tomador de decisão.

A técnica sugere a produção de uma matriz de probabilidade e impacto capaz de indicar a priorização das atividades e das ações correntes. Dessa forma, o mapa de risco auxilia o especialista na identificação dos riscos que devem ser analisados ou tratados com mais urgência, além de permitir o monitoramento e a evolução de cada risco identificado. A Figura 11 corrobora o entendimento do que é um mapa de risco:

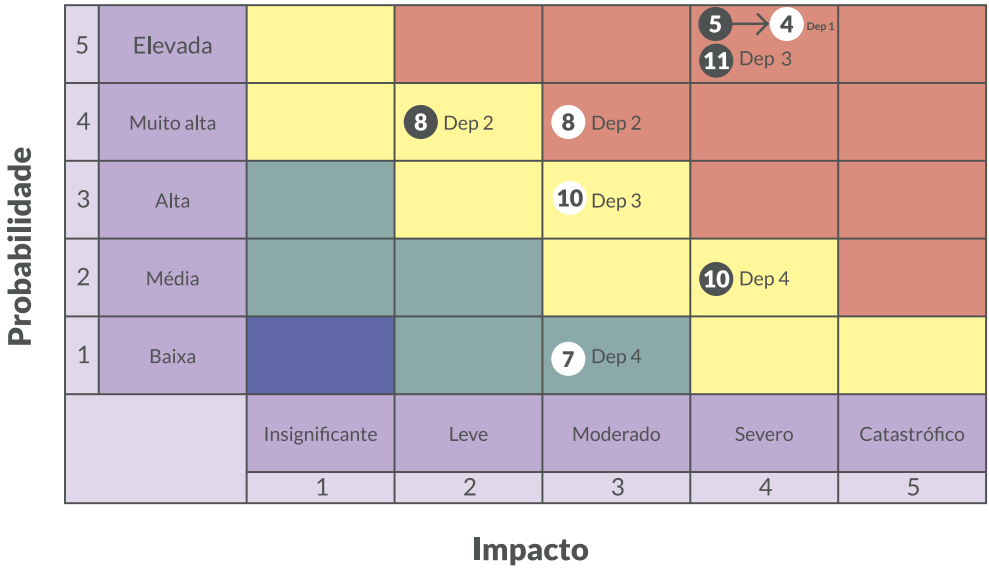


Figura 11 – Estrutura de mapa de riscos entre departamentos

No exemplo do mapa de riscos, os círculos escuros (preenchidos) representam o momento anterior – da identificação dos riscos – e os claros o momento atual. Os números indicados dentro dos círculos representam a quantidade de riscos relacionados ao departamento. Para o departamento 1 (Dep 1), podemos notar que havia cinco riscos anteriormente e que no momento atual existem apenas quatro riscos, ou seja, um risco já foi tratado. O departamento 2 (Dep 2) manteve a quantidade de riscos do momento anterior, porém seus riscos tiveram nível de impacto elevado, o que ocasionou reposicionamento no gráfico, saindo de impacto leve para moderado. Nota-se também que o departamento 3 (Dep 3) foi acrescido de um risco e, além disso, seus riscos aumentaram significativamente a probabilidade de acontecimentos, que passou de alta para elevada, e de impacto, que passou de moderado para severo. Finalmente, o departamento 4 (Dep 4) teve três riscos solucionados, e os riscos que permaneceram diminuíram em nível de probabilidade e impacto.

O segundo exemplo proposto refere-se à visualização dos riscos de um único departamento. A Figura 12 reflete esse cenário.

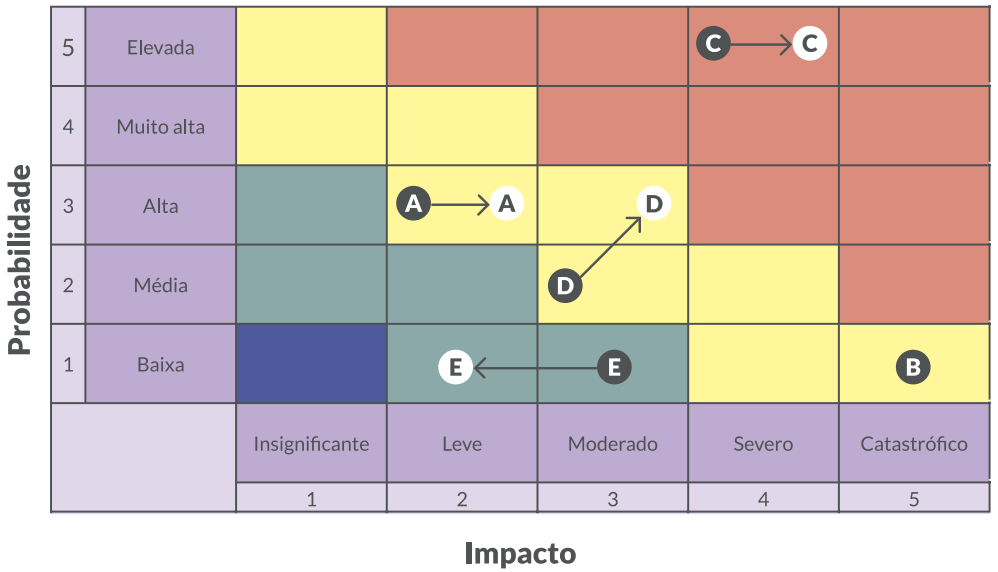


Figura 12 – Estrutura de mapa de riscos: riscos do departamento

Ao visualizar os riscos de um único departamento, como, por exemplo, o departamento 1 – Figura 12 –, pode-se ver os riscos que o afetam. Em cada círculo, há uma letra (A, B, C, D, E) para identificar de forma única o risco. Podemos observar nesse caso que o Risco A manteve os níveis do momento anterior e que no momento atual permanece sem solução. Enquanto isso, o Risco B foi resolvido. O Risco C também se manteve igual e ainda sem solução. O Risco D teve sua probabilidade de ocorrência acrescida. Finalmente, o Risco E foi abrandado no momento atual, tendo o seu nível de impacto reclassificado para leve. Infere-se que esses mapas devam permitir uma visualização baseada nos critérios que o especialista em riscos deseja visualizar. Dessa forma, pode-se priorizar e distribuir as tarefas aos agentes e especialistas, além de permitir rastreabilidade e acompanhamento dos riscos. As cores, em ambos os exemplos, ajudam a compreender visualmente a urgência dos casos. O azul indica a normalidade do risco, o verde, mínima urgência, o amarelo requer atenção e, por fim, o vermelho caracteriza os riscos mais urgentes.

4.3.2. Relatórios sumarizados

O intuito dos relatórios sumarizados é fornecer informações aos tomadores de decisão com uma visão sintética sobre o quantitativo dos riscos no

momento de sua identificação (momento anterior) e no momento atual, bem como uma comparação entre esses dois momentos. Essa técnica apresenta o somatório das ameaças e oportunidades por meio de um filtro. A Figura 13 exemplifica esse conjunto de informações em quatro departamentos de uma organização qualquer num determinado período.

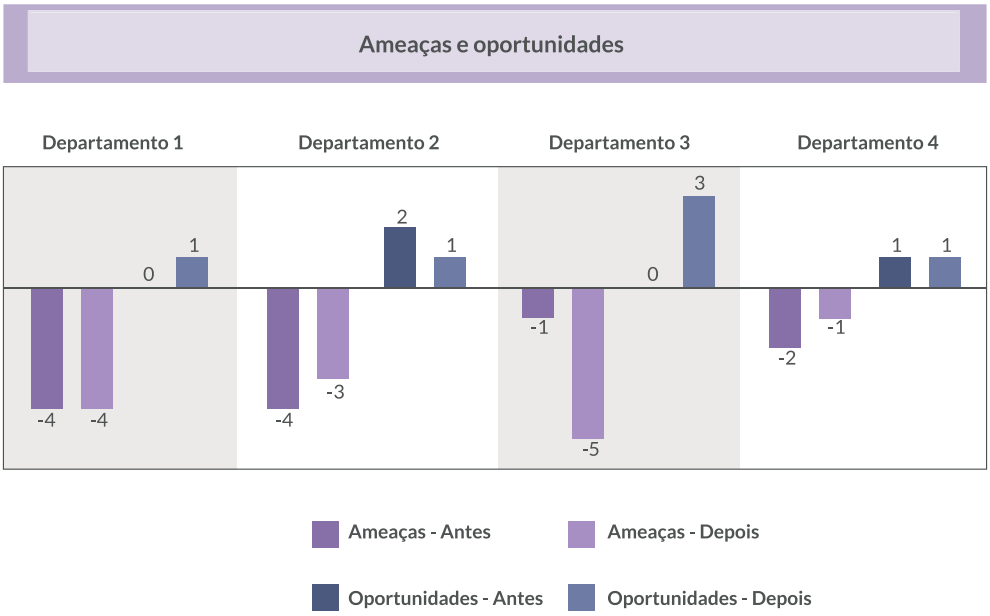


Figura 13 – Elaboração de relatório sumarizado: ameaças e oportunidades

Neste cenário, observa-se que o departamento 1 manteve a quantidade de ameaças do momento anterior, mas identificou uma oportunidade no momento atual. Já o departamento 2 resolveu uma ameaça e concluiu uma oportunidade. O departamento 3 identificou quatro novas ameaças e três novas oportunidades. Por último, o departamento 4 solucionou um ameaça, mas não concluiu a oportunidade anteriormente reconhecida.

O relatório sumarizado não contém a gravidade dos riscos, mas a quantidade de riscos e oportunidades a que os departamentos estão expostos. Permite uma visão rápida e ampliada de quais departamentos estão enfrentando mais problemas e requerem mais atenção. Em conjunto com esse tipo de relatório, devem ser desenvolvidos textos sucintos e explicativos quanto a riscos e oportunidades identificados.

4.3.3. Comunicações e mensagens de alerta

Após o registro quantitativo dos riscos, um conjunto de informações como data de levantamento, proximidade e última atualização podem contribuir para que revisões sistemáticas ocorram. Por exemplo, um risco grave que não é atualizado há mais de 15 dias pode ocasionar um problema. Nesse caso, é recomendado que os riscos sejam frequentemente revisitados para atualizar as informações do registro.

Um segundo exemplo corresponde aos riscos que estão próximos à data-limite de solução. Por meio das mensagens de alerta, pode-se manter atentos os tomadores de decisão. Destaca-se a utilização de sistemas de informações que podem ser criados para alertas específicos por e-mail ou por outro canal de comunicação, notificando os especialistas dos riscos na condução de suas atividades. Uma simples atitude que resulta em uma gestão de riscos mais segura e eficiente.

4.3.4. Árvores de decisão

Entre os modelos mais práticos que contribuem com a tomada de decisão organizacional, tem-se a árvore de decisão. O método caracteriza-se por sistematizar uma série de fatos, riscos, probabilidades e oportunidades – relacionados a uma situação, objetivo, metas ou, em maior escala, programas e projetos – cujos efeitos devem ser reconhecidos, manipulados e comparados. Visualmente, as árvores de decisão tomam a forma de diagramas e estruturam um mapa com possíveis escolhas para a melhor ação. A ferramenta, ainda que na sua forma simples, pode proporcionar lógicas à escolha de cursos alternativos de ação/decisão. Conforme Keeling [27], as árvores de decisão auxiliam em diversas situações, desde a avaliação dos riscos em uma organização, ou comparação entre propostas alternativas, até a discussão dos resultados de uma sessão de brainstorming. Ainda segundo Keeling [27, p. 217], o método garante que a qualidade de todas as decisões seja influenciada por: precisão das informações; qualidade dos julgamentos e avaliações; fatores de probabilidade; e atitude do tomador de decisão em relação ao gerenciamento de riscos. A Figura 14 exemplifica a lógica nas árvores de decisão.

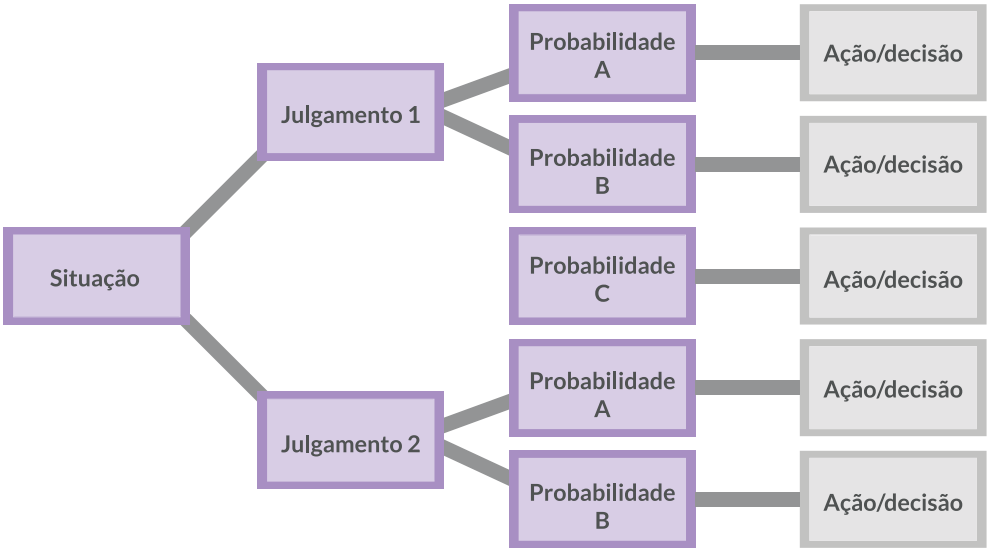


Figura 14 – Concepção da lógica em árvores de decisão
Fonte: Keeling (2002, p. 220), com adaptações

4.3.5. Brainstorming

Técnica focada na resolução de problemas ou na expansão das ideias para que esses problemas sejam solucionados. O primeiro passo da técnica e, talvez, o mais importante, é garantir a definição e/ou o reconhecimento do problema, pois somente assim será possível planejar ações corretivas. Ao tratar de "problemas" ou de situações específicas, o método estimula a reunião de um grupo de pessoas para que possam refletir e gerar pensamentos inovadores que intencionam uma solução. Entre outras vantagens do brainstorming, é possível destacar a sua capacidade de germinar as causas para os problemas, ajudar a decidir um passo a passo no desenvolvimento de um projeto e reconhecer oportunidades, além de encorajar a participação de todos os membros de uma equipe ou organização.

4.3.6. Análise de cenários

Extremamente difundida em estudos de consultoria e gestão, a análise de cenários objetiva a ação organizacional estratégica considerando informações do presente em um contexto de futuro. Conforme descreve o Portal da Estratégia da Secretaria de Política e Integração [28], a capacidade de anali-

sar cenários fundamenta a importância da concepção do planejamento estratégico e, por consequência, impulsiona a ação. Em resumo, a principal função das análises de cenário é o reconhecimento do contexto (interno e externo) no qual a organização está inserida, de forma a se identificarem fatores futuros que são passíveis de ocorrer. Simples atitudes como essas asseguram uma visão mais clara do cenário atual e permitem uma tomada de decisão mais fundamentada e precisa. Para ajudar no desenvolvimento dessa técnica, recomenda-se a utilização, em conjunto, dos procedimentos da Análise SWOT – *Strenghts* (Forças), *Weakness* (Fraquezas), *Opportunities* (Oportunidades) e *Threats* (Ameaças) –, que fortalecem a apuração e a formulação das estratégias organizacionais.

5. Leis e normas relacionadas à gestão de riscos no setor público: o caso do Brasil

Nas democracias mundiais, a Administração Pública tem sentido, cada vez mais, a presença dos cidadãos, demandantes de políticas públicas que anseiam pela oferta de serviços de qualidade. O controle social, por meio da exigência de maior transparência e *accountability* (prestação de contas), faz sentir-se com a regulamentação de leis e normas que regem uma melhor atuação da gestão pública para com as suas instituições e os seus servidores.

Além das pressões impostas pelo controle social, houve também uma necessidade quase que automática da Administração Pública de se reinventar. Notadamente, os modelos de Administração Pública foram assumindo, ao longo do tempo, formas peculiares de se apresentar e se organizar diante da globalização e das mudanças econômicas, ambientais, políticas e sociais. A gestão de riscos é um bom exemplo de transformação na Administração Pública e passou a ser praticada em diversos países recentemente.

No Brasil, o que se percebe é uma mudança paradigmática por parte dos órgãos públicos em tentar gerenciar melhor os seus recursos orçamentários, humanos e administrativos. Mas essa mudança, em boa medida, vem do interesse da cúpula da Administração Pública brasileira, por meio do Ministério do Planejamento, Orçamento e Gestão, e da Controladoria-Geral da União, em tentar prover leis e normas que fomentem a adoção de medidas sistematizadas para a gestão de riscos, controles internos e governança.

São os povos, em seus territórios estabelecidos, que definem as leis e normas a serem aplicadas em casos explícitos para disciplinar, limitar e organizar as suas sociedades. Leis, por via de regra, são orientações estabelecidas pelo poder constituinte para serem respeitadas por todos os membros de uma sociedade. Claramente, toda lei deverá estar em consonância com a Constituição Federal do país. Normas são, nesse caso, instruções, atos administrativos caracterizados em espécie, natureza e finalidade para satisfazer princípios e determinações contidos nas leis.

Este capítulo contém as leis e normas (Quadro 13) relacionadas à gestão de riscos e válidas no Brasil. As pesquisas foram realizadas em sites da Administração Pública a fim de apoiar os gestores quanto a recomendações e obrigações legais. Vale lembrar que a consulta a esse material é indispensável aos gestores, pois deverá fornecer embasamento legal para o desenvolvimento das regulamentações e das políticas internas de cada organização.

Quadro 13 – Leis e normas sobre gestão de riscos no Brasil

Legislação	Ano	Objeto/Assunto principal
LEI COMPLEMENTAR Nº 101	2000	Estabelece que a Lei de Diretrizes Orçamentárias Anual (LDO) deve determinar meta de superavit primário e conter anexo de riscos fiscais com a avaliação dos passivos contingentes e de outros riscos capazes de afetar as contas públicas.
NORMA COMPLEMENTAR Nº 02/IN01/DSIC/GSIPR	2008	Metodologia de gestão de Segurança da Informação e Comunicação (SIC).
INSTRUÇÃO NORMATIVA GSI Nº 1	2008	Disciplina a gestão de SIC e comunicações na APF, direta e indireta, e dá outras providências.
NORMA COMPLEMENTAR Nº 03/IN01/DSIC/GSIPR	2009	Diretrizes para a elaboração de política de SIC e comunicações nos órgãos e nas entidades da APF.
NORMA COMPLEMENTAR Nº 05/IN01/DSIC/GSIPR	2009	Disciplina a criação de Equipes de Tratamento e Respostas a Incidentes em Redes Computacionais (ETIR) nos órgãos e nas entidades da APF.
NORMA COMPLEMENTAR Nº 06/IN01/DSIC/GSIPR	2009	Estabelece diretrizes para gestão de continuidade de negócios, nos aspectos relacionados a SIC e comunicações, nos órgãos e nas entidades da APF, direta e indireta.
NORMA COMPLEMENTAR Nº 08/IN01/DSIC/GSIPR	2010	Estabelece diretrizes para gerenciamento de incidentes em redes computacionais nos órgãos e nas entidades da APF.
NORMA COMPLEMENTAR Nº 10/IN01/DSIC/GSIPR	2012	Estabelece diretrizes para o processo de inventário e mapeamento de ativos de informação para apoiar a SIC e as comunicações dos órgãos e das entidades da APF, direta e indireta.
NORMA COMPLEMENTAR Nº 11/IN01/DSIC/GSIPR	2012	Estabelece diretrizes para avaliação de conformidade nos aspectos relativos a SIC e comunicações nos órgãos ou nas entidades da APF, direta e indireta.
NORMA COMPLEMENTAR Nº 12/IN01/DSIC/GSIPR	2012	Estabelece diretrizes e orientações básicas para o uso de dispositivos móveis nos aspectos referentes a SIC e comunicações nos órgãos e nas entidades da APF, direta e indireta.

Legislação	Ano	Objeto/Assunto principal
NORMA COMPLEMENTAR Nº 13/IN01/DSIC/GSIPR	2012	Estabelece diretrizes para a gestão de mudanças nos aspectos relativos a SIC e comunicações nos órgãos e nas entidades da APF, direta e indireta.
NORMA COMPLEMENTAR Nº 14/IN01/DSIC/GSIPR	2012	Estabelece diretrizes para a utilização de tecnologias de computação em nuvem, nos aspectos relacionados a SIC e comunicações, nos órgãos e nas entidades da APF, direta e indireta.
NORMA COMPLEMENTAR Nº 15/IN01/DSIC/GSIPR	2012	Estabelece diretrizes de SIC e comunicações para o uso de redes sociais, nos órgãos e nas entidades da APF, direta e indireta.
NORMA COMPLEMENTAR Nº 16/IN01/DSIC/GSIPR	2012	Estabelece diretrizes para o desenvolvimento e a obtenção de software seguro nos órgãos e nas entidades da APF, direta e indireta.
NORMA COMPLEMENTAR Nº 04/IN01/DSIC/GSIPR e seu anexo	2013	Estabelece diretrizes para o processo de gestão de riscos de SIC e Comunicações (GRSICC) nos órgãos e nas entidades da APF.
NORMA COMPLEMENTAR Nº 17/IN01/DSCI/GSIPR	2013	Estabelece diretrizes nos contextos de atuação e adequações para profissionais da área de SIC e comunicações.
NORMA COMPLEMENTAR Nº 18/IN01/DSIC/GSIPR	2013	Estabelece diretrizes para as atividades de ensino em SIC e comunicações nos órgãos e nas entidades da APF.
INSTRUÇÃO NORMATIVA GSI Nº 2	2013	Dispõe sobre o credenciamento de segurança para o tratamento de informação classificada, em qualquer grau de sigilo, no âmbito do Poder Executivo Federal.
INSTRUÇÃO NORMATIVA GSI Nº 3	2013	Dispõe sobre os parâmetros e padrões mínimos dos recursos criptográficos baseados em algoritmos de estado para criptografia da informação classificada no âmbito do Poder Executivo Federal.
DECRETO Nº 8.135	2013	Dispõe sobre as comunicações de dados da APF direta, autárquica e fundacional, e sobre a dispensa de licitação nas contratações que possam comprometer a segurança nacional.
NORMA COMPLEMENTAR Nº 07/IN01/DSIC/GSIPR	2014	Estabelece diretrizes para implementação de controles de acesso relativos a SIC e comunicações, nos órgãos e nas entidades da APF, direta e indireta.
NORMA COMPLEMENTAR Nº 09/IN01/DSIC/GSIPR	2014	Estabelece orientações específicas para o uso de recursos criptográficos em SIC e comunicações, nos órgãos ou nas entidades da APF, direta e indireta.
NORMA COMPLEMENTAR Nº 19/IN01/DSIC/GSIPR	2014	Estabelece padrões mínimos de SIC e comunicações para os sistemas estruturantes da APF, direta e indireta.

NORMA COMPLEMENTAR Nº 20/IN01/DSIC/GSIPR	2014	Estabelece diretrizes de SIC para instituição do processo de tratamento da informação nos órgãos e nas entidades da APF.
INSTRUÇÃO NORMATIVA SLTI/MP Nº 4	2014	Dispõe sobre o processo de contratação de soluções de Tecnologia da Informação (TI) pelos órgãos integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP) do Poder Executivo Federal.
PORTARIA INTERMINISTERIAL MP/MC/MD Nº 141	2014	Dispõe que as comunicações de dados da APF direta, autárquica e fundacional deverão ser realizadas por redes de telecomunicações e serviços de TI fornecidos por órgãos ou entidades da APF, incluindo empresas públicas e sociedades de economia mista da União e suas subsidiárias, observando o disposto nesta portaria.
ACÓRDÃO TCU Nº 4.330	2014	Dispõe sobre gestão de riscos em contratações.
DECRETO FEDERAL Nº 8.420	2015	Regulamenta diversos aspectos da Lei Anticorrupção, tais como critérios para o cálculo da multa, parâmetros para avaliação de programas de *compliance*, regras para a celebração dos acordos de leniência e disposições sobre os cadastros nacionais de empresas punidas.
ACÓRDÃO TCU N º 2.110	2015	Dispõe sobre gerir riscos da organização.
INSTRUÇÃO NORMATIVA CONJUNTA CGU/MP Nº 1	2016	Dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo Federal.
DECRETO Nº 8.945	2016	Regulamenta, no âmbito da União, a Lei nº 13.303, de 30 de junho de 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.
LEI Nº 13.303	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.

Fonte: MGR-SISP (2016), com adaptações

O Quadro 13 constitui uma lista atualizada das leis e normas vigentes atualmente no Brasil, impactando e modificando a execução e o papel da gestão dos riscos. Cabe lembrar, entretanto, que processos de gestão de riscos estão sujeitos a mudanças e particularidades de acordo com cada órgão público, e recomenda-se que sejam identificadas, para cada contexto, as leis e as normas vigentes a serem aplicadas no gerenciamento desses riscos.

Para esta obra, destaca-se a Instrução Normativa Conjunta MP/CGU nº 1/2016 – IN, publicada no Diário Oficial da União em 11 de maio de 2016, que estabelece aos órgãos e às entidades do Poder Executivo Federal uma série de medidas para a sistematização de práticas relacionadas à gestão de riscos [29]. Em síntese, órgãos e entidades do Poder Executivo Federal devem viabilizar a implementação, a manutenção, o monitoramento e a revisão dos controles internos da gestão, bem como o gerenciamento dos riscos que possam inviabilizar o alcance dos objetivos dessas organizações [29].

A implementação do processo de gestão de riscos deve ocorrer "de forma sistemática, estruturada e oportuna, subordinada ao interesse público" [29, p. 77], e o mapeamento dos riscos deve ser utilizado para apoiar "a tomada de decisão e a elaboração do planejamento estratégico e melhoria contínua dos processos" [29, p. 77]. Por fim, conforme sugere a IN [7], a gestão de riscos deve ser competente ao identificar o nível de risco que a organização está disposta a aceitar, isto é, o seu apetite ao risco, e a razoável certeza quanto ao alcance dos objetivos organizacionais.

6. Ferramentas de software para gestão de riscos

O planejamento e o alinhamento entre a fundamentação teórica e a concepção de ferramentas de cunho tecnológico mostraram, ao longo dos anos, crucial importância para respaldar as iniciativas de gestão em qualquer nível organizacional, considerando a natureza de seus processos e produtos, bem como a realidade e a especificidade dos mais diversos cenários de atuação das instituições. Na atual realidade, o bom planejamento, capaz de conduzir com sucesso os projetos, baseia-se em princípios, técnicas, habilidades e ferramentas capazes de aumentar a efetividade da gestão, alcançando melhores resultados e otimizando as oportunidades.

Nesse sentido, para que as organizações possam incluir ações de gestão de riscos em suas tarefas, torna-se fundamentalmente necessário que ferramentas de controle e centralizações de registros estejam dispostas a auxiliar tais esforços a fim de permitir comunicação precisa, monitoramento e domínio dos riscos. Para isso, a Tecnologia da Informação (TI) desempenha um papel importante por permitir que esse conjunto de regras de negócio seja operado da melhor forma possível, automatizando tarefas e disponibilizando uma interface para apoiar os gestores de riscos em suas atribuições.

O cenário da gestão de riscos no setor público ainda está em desenvolvimento no Brasil, portanto foi realizada pesquisa utilizando a estratégia de benchmarking para a avaliação de 33 ferramentas de softwares existentes no mercado que se comprometem a criar processos e estratégias de gestão condizentes com a realidade das organizações que as utilizam. Optou-se por apresentar informações específicas – ainda que de forma sintetizada – sobre o módulo destinado à gestão de riscos em cada software examinado, assim como informações de procedimentos e estratégias que visam complementar o processo de gestão inicialmente citado.

A princípio, para que seja possível conhecer essas ferramentas, foi desenvolvido um quadro de informações contendo o nome do software avaliado, seu website e se existe algum custo para a sua aquisição. Todas essas referências estão sistematizadas no Quadro 14 a seguir:

Quadro 14 – Ferramentas de software contempladas na pesquisa

Nome	Site	Custo de aquisição
360factor	http://www.360factors.com	Sim
ACCELUS	https://www.thomsonreuters.com	Sim
ACL GRC	https://www.acl.com	Sim
Active Risk Manager	http://www.sword-activerisk.com	Sim
Adaptive GRC	https://candf.com	Sim
Ágatha	https://softwarepublico.gov.br/social/agatha	Não
Aris GRC	http://www2.softwareag.com	Sim
BPS Resolver	http://www.resolver.com	Sim
BRINQA	https://brinqa.com	Sim
BWISE	http://www.bwise.com/solutions	Sim
Convercent	https://www.convercent.com	Sim
Datalyzer FMEA	https://www.datalyzer.com/products/fmea-software	Sim
Enablon	https://enablon.com	Sim
Eramba	http://www.eramba.org	Não
IBM OpenPages GRC	https://www.ibm.com	Sim
IntelligenceBank GRC	http://www.intelligencebank.com	Sim
INTERISK – Inteligência em Riscos	https://www.brasiliano.com.br/software-interisk	Sim
ITouchVision Governance & Risk	https://www.itouchvision.com	Sim
MasterControl	https://www.mastercontrol.com	Sim
MetricStream	https://www.metricstream.com	Sim
Open Risk	https://www.openriskmanagement.com	Não
OpenSource Risk	http://www.opensourcerisk.org	Não
Optial Risk Management	http://www.optimalrisk.com	Sim
Oracle Fusion Governance Risk	http://www.oracle.com	Sim
ORACLE GRC	http://www.oracle.com	Sim
ProcessGene GRC	http://processgene.com	Sim

RiskGAP	http://riskgap.com	Sim
RIVO	https://rivosoftware.com	Sim
RSA Archer	https://www.rsa.com	Sim
SAP GRC	https://www.sap.com	Sim
SE Risk	https://www.softexpert.com/pt-br/produto/gestao-riscos-controles	Sim
Simple Risk	https://www.simplerisk.com	Não
TruComply	http://anxebiz.anx.com	Sim

As análises das ferramentas de softwares disponíveis no mercado podem possibilitar, se necessário, o desenvolvimento das especificidades e adequações do cenário no setor público brasileiro. Além disso, esta pesquisa mostra a sua importância ao contribuir para o desenvolvimento do próprio software ForRisco de gestão de riscos e ao apoiar as comunidades de maneira geral, criando processos de reflexão para novas ações mais eficientes, eficazes, voltadas à melhoria de resultados e transparência, de maneira que possam complementar as ações de organizações públicas e privadas, especialmente quando estas refletem diretamente no convívio em sociedade.

Dessa forma, com a finalidade de resumir as principais informações que moldam os softwares avaliados, está registrada no Quadro 15 uma síntese dos módulos de gestão de riscos e informações de processos e/ou módulos que complementem o processo supracitado. Essa lista de questões – enumeradas a seguir – corresponde aos itens da coluna "Informações sobre os módulos de gestão de riscos" do Quadro 15, que trata dos softwares e de suas principais características.

1. O software permite a gestão completa de um determinado risco, desde a sua primeira detecção até a sua devida solução? Possibilita uma gestão alinhada com os objetivos preestabelecidos de cada unidade/departamento ou da própria organização em seu conjunto?

2. O software permite uma análise profunda das causas de um determinado risco, combinando técnicas de exploração de dados com o objetivo de permitir aos gestores a utilização dessas causas como fundamentação para tomada de decisão?

3. O software permite a centralização de todas as informações acerca de medidas de gestão de riscos em um único repositório de informações (inclui todas as ações que serão realizadas para tratar um risco, exemplo, ações, informações de ocorrência, etc.)?

4. O software permite a personalização de métricas de avaliação, de funcionalidades de avaliação e de telas de apresentação de dados mediante demanda de determinada organização?

5. O software permite a delegação de responsabilidades e/ou a organização de grupos de trabalho para a construção de processos objetivando o tratamento de um determinado risco?

6. Através da construção de processos de controle, o software permite a padronização de mecanismos de controle para garantir a continuidade de iniciativas de gestão de riscos?

7. O software apresenta uma variedade significativa de medidas qualitativas e quantitativas para situar gestores sobre a maturidade de processos de controle de riscos? Exemplo: Key Performance Indicator (KPI), Key Risk Indicators (KRI).

8. A plataforma utiliza a gestão de processos de auditoria como funcionalidade complementar à gestão de riscos?

9. Possibilita a integração de um módulo de comunicação à gestão de riscos objetivando gerir o fluxo de informações e procedimentos a serem disseminados em toda a organização?

10. Admite a utilização de questionários para avaliação situacional e/ou para unir funcionalidades à gestão da comunicação?

11. Permite a gestão de leis e de regulamentos vigentes para adequar a realidade organizacional às exigências de mercado e de governos?

12. Possui módulo destinado à gestão pública?

13. Permite a conexão de múltiplos dispositivos, como, por exemplo, celulares, *tablets*, computadores?

Quadro 15 – Softwares avaliados e suas principais características

	Informações sobre os módulos de gestão de riscos												
	1	2	3	4	5	6	7	8	9	10	11	12	13
360factor	•		•	•		•	•	•			•		
ACCELUS	•		•	•	•	•		•	•		•		
ACL GRC	•	•	•	•	•	•	•	•	•	•	•	•	
Active Risk Manager	•	•	•	•		•	•	•	•		•		•
Adaptive GRC	•	•	•	•		•	•	•	•		•		
Ágatha	•	•	•		•								
Aris GRC	•	•	•	•	•	•	•	•	•	•	•	•	
BPS Resolver	•		•	•	•			•					•
BRINQA	•	•	•	•			•				•		
BWISE	•	•	•	•		•	•	•	•		•		
Convercent	•				•				•				
Datalyzer FMEA	•	•	•	•									
Enablon	•	•		•		•	•		•	•			
Eramba	•		•					•	•		•		
ITouchVision Governance & Risk	•	•	•		•			•	•	•		•	•
IBM OpenPages GRC	•	•	•	•	•	•	•	•	•	•			•
IntelligenceBank GRC	•	•		•		•		•	•	•			
INTERISK – Inteligência em Riscos	•	•	•	•	•	•		•	•		•		
MasterControl	•		•	•		•		•	•	•			
MetricStream	•	•	•	•			•	•	•		•		
Open Risk	•		•			•		•					
OpenSource Risk	•		•	•		•							
Optial Risk Management	•	•	•	•	•			•					
Oracle Fusion Governance Risk	•	•	•	•		•		•	•		•		
ORACLE GRC	•	•	•	•	•	•		•	•		•		
ProcessGene GRC	•	•	•	•		•		•			•		
RiskGAP	•		•	•	•						•		
RIVO	•	•	•	•		•							
RSA Archer	•		•	•	•	•		•			•		
SAP GRC	•	•	•	•	•		•	•	•		•		
SE Risk	•	•	•	•	•	•		•	•		•		
Simple Risk	•	•		•	•	•		•					
TruComply	•	•	•	•		•					•		

Desfrutando-se do interesse de garantir uma análise mais completa das ferramentas avaliadas, além das perguntas às quais "se tentou responder" por meio do Quadro 15, desenvolveu-se, através do acesso aos sites oficiais citados e a vídeos oficiais das ferramentas, além da experimentação dos softwares disponíveis na World Wide Web – especialmente no YouTube – uma série de informações sobre as principais funcionalidades de cada um dos softwares que estão contemplados nos quadros 14 e 15 deste estudo. A seguir, delineia-se e documenta-se a análise:

i. 360factor: este software oferece um módulo de auditoria que compreende e acompanha todo e qualquer processo de auditoria. Permite a visão dos riscos na organização inteira, implementado módulos integráveis em todos os departamentos. Oferta um módulo que objetiva desenvolver, gerenciar e controlar acordos, contratos com fornecedores e com terceiros, os quais visam, em geral, minimizar os custos e a exposição ao risco bem como direcionar excelência em serviço. O software oferece o serviço de gerenciamento de políticas e procedimentos, e a gestão de marcos regulatórios e de controles para manter a organização alinhada às melhores práticas de mercado. Para um controle mais apurado de riscos e incidentes, a ferramenta permite a criação de relatórios periódicos e gerenciáveis com o intuito de evidenciar os principais processos da organização avaliada. Como vantagem, a ferramenta possui um módulo de desempenho de avaliações, feedback contínuo, atingimento de metas e *coaching* de desenvolvimento para melhorar a organização.

ii. Accelus: a ferramenta Accelus permite o estabelecimento e a análise de regras, regulamentos e políticas no cenário em que a organização está inserida. Oferta aos usuários um mecanismo de acompanhamento de ações que permite à organização verificar a adequação aos regulamentos atuais. Permite ainda a gestão de um determinado risco, desde a sua identificação inicial até a aplicação de medidas corretivas. Em destaque, este software garante a distribuição de responsabilidades aos colaboradores inseridos nos processos de verificação e análise de riscos, e oferta um sistema completo de notificações com o intuito de informar os colaboradores da organização sobre mudanças em regulamentos legais e sobre mudanças internas em processos. Por último, permite a geração automática de relatórios, com o envio periódico via e-mail já definido, e centraliza uma biblioteca de ações e de processos já executados para consultas e adequações futuras.

iii. ACL GRC: permite criar uma visão macro de todos os possíveis riscos de uma situação, com a possibilidade de categorizá-los. Faculta atividades off-line – que são automaticamente sincronizadas na existência de conexão (com serviços de armazenamento de dados e segurança em nuvem) e permite gerenciar incidentes e possíveis falhas através da análise de dados. No que se refere à modelagem, facilita a organização de uma ou várias estruturas ou processos de trabalho fundamentadas em modelos/*frameworks* como COBIT, ITIL, SIEM, NIST, SOC e COSO. Além disso, oferece uma funcionalidade dedicada ao setor público com o intuito de gerenciar projetos desde a sua concepção até a sua conclusão.

iv. Active Risk Manager: oferece aporte para a gestão de riscos desde um projeto de TI até a gestão dos riscos de um planejamento estratégico de negócios. Permite a criação de alertas automatizados e a apresentação de dados em *dashboards* simples, além da atualização de dados através de qualquer dispositivo, seja ele computador, celular ou outros. Entre seus pontos fortes, a ferramenta oferece uma funcionalidade que permite encontrar oportunidades por meio da economia de custos, melhorias através de ideias, processos ou novos produtos. Por fim, facilita o controle de metas e o monitoramento de ações fazendo uso de medidas quantitativas e qualitativas.

v. Adaptive GRC: com esta ferramenta, é possível criar relatórios que apresentam informações sobre um determinado projeto, o que permite e facilita processos de auditoria. A ferramenta possibilita também a filtragem de informações, facultando a visualização de fluxos de trabalhos e ciclos de vida de processos relacionados a um determinado risco. Seus riscos identificados são facilmente rastreados pela ferramenta, estando eles resolvidos ou não. Somado a isso, a Adaptive GRC viabiliza gerar relatórios em tempo real para determinar as características dos principais processos. A hospedagem da aplicação é feita na nuvem.

vi. Ágatha: a ferramenta Ágatha permite o mapeamento de macroprocessos e de processos com informações das unidades organizacionais, informações sobre o ambiente interno, fixação de objetivos e análise SWOT. Esta solução identifica os eventos de risco, capturando as suas principais causas, consequências, categorias e naturezas e, além disso, permite o planejamento de respostas aos riscos relacionados às causas e às consequências do evento de risco. Todas as ações sobre o plano de controle de riscos ficam registradas, o que corresponde às respostas aos eventos de risco, bem como à vali-

dação e à decisão de recusa ou aceitação. No que se refere a processos de avaliação dos riscos, a ferramenta avalia riscos e controles contendo riscos inerentes e riscos residuais, os quais são registrados em mapas de riscos para probabilidade e impacto. Por fim, a ferramenta permite criar repositório de eventos de risco, causas de evento de risco, consequências de evento de risco, categoria de risco, controles de risco, desenhos de controle, operações de controle, taxonomias e glossário de termos, facilitando o reúso.

vii. Aris GRC: o sistema Aris GRC realiza as principais adequações regulatórias seguindo as especificações da União Europeia, com o intuito de assegurar as melhores práticas para armazenamento e processamento de dados. Permite a utilização de um sistema dedicado à detecção, análise e correção dos riscos, o que garante a facilidade no controle e na adequação de processos e fluxos de trabalho, e análises por auditorias internas. A ferramenta inclui a avaliação de riscos periódicos e riscos ligados ao financeiro e de segurança da informação, e possibilita ainda a divisão das responsabilidades ao redor de atividades para avaliar as principais características e influências de um risco. Vale destacar que este sistema possui módulo destinado à gestão pública.

viii. BPS Resolver: permite a visualização dos riscos desde a sua identificação até a sua resposta, análise e possível solução. Sua estrutura visa documentar e armazenar informações sobre controles e procedimentos, o que simplifica a realização de auditorias internas. O sistema comporta-se em diversos dispositivos, tais como computadores, celulares e *tablets*. Em vantagem, a ferramenta enseja a criação de grupos de avaliação e coordena a criação de votações dos grupos de discussão com o intuito de categorizar e classificar os riscos analisados. Nos grupos, é possível delegar papéis de atuação para resolver ou avaliar um determinado risco bem como criar relatórios com o intuito de verificar em gráficos a evolução e a análise dos riscos.

ix. BRINQA: propõe ser uma plataforma de gestão de riscos destinada ao armazenamento de dados empresariais. Sua estrutura permite a junção de diversas fontes de informação e a análise para verificar a existência de riscos, que engloba, ainda, a categorização e a classificação dos principais e mais evidentes riscos em que a organização pode estar inserida. A ferramenta permite a criação e a exposição de modelos de dados e processos que representam os relacionamentos dos agentes que apresentam riscos, fato que permite uma análise crítica da categorização e a ordenação das ações a serem exercidas. Por último, são possíveis ainda

a criação e a utilização de diversas métricas e sua apresentação em *dashboards* customizáveis em diversos cenários.

x. Bwise: com o intuito de adequar as organizações aos marcos regulatórios vigentes, a solução Bwise permite a conexão e a análise dos principais agentes regulatórios bem como a utilização de suas práticas para alinhamento da empresa. Com esta ferramenta, são garantidos o monitoramento e a análise do perfil organizacional, adequando-os aos modelos e padrões de mercado mais atuais como COBIT, FERC e FDA. Além disso, possibilita a criação de métricas e a utilização de painéis de dados destinados à análise da alta administração, a realização da análise de escopo com base nos principais riscos e a execução de avaliações flexíveis através da aplicação de filtros específicos. Cabe destacar, afinal, a sua capacidade de adequar informações de aplicações e fontes de dados externas.

xi. Convercent: o sistema Convercent traz a adequação dos processos e dos fluxos de trabalho como prática obrigatória para estabelecimento das políticas de conformidade. Com isso, a ferramenta oferta e constrói políticas eficientes e seguras para o armazenamento e a disponibilização de dados. Por via de regra, permite a elaboração de relatórios e análises personalizáveis e abrangentes, bem como a exportação desses relatórios.

xii. Datalyzer FMEA: agiliza a criação de processos e fluxos de trabalho adequados à realidade organizacional. Por meio desta ferramenta, é possível registrar e mapear todos os aspectos ao redor da concepção de um novo fluxo de trabalho, de riscos, de alternativas e centralizá-los em um mesmo local para consultas futuras. Seus *dashboards* e suas métricas podem acompanhar todas as ações relacionadas a um risco ou a um processo, o que permite à auditoria empresarial buscar falhas e problemas de execução. Por fim, a ferramenta verifica a criação e a classificação de usuários, atribuindo níveis de execução e atuação de acordo com o processo de gestão de riscos.

xiii. Enablon: visa ao controle e à avaliação de práticas e de processos de trabalho utilizados dentro das organizações. Através de suas análises, é possível verificar se os processos estão alinhados com as melhores práticas difundidas no mercado ou se podem ser alinhados a elas. Esta ferramenta preocupa-se em intensificar a comunicação e a divulgação de questões organizacionais internas por meio da geração de relatórios personalizáveis e aplicáveis aos mais diversos setores empresariais. Destaca-se a possibili-

dade de serem criadas tarefas específicas para um determinado processo atingir um nível de regulamentação adequado e, ainda, de serem criados controles e fluxos em processos que estão em fase de implementação ou que já foram implementados.

xiv. Eramba: tem foco no ambiente interno para realizar a gestão de riscos, permitindo a fixação de metas e de objetivos em todos os níveis da organização. Seu processo oferece etapas de identificação de riscos, criticidade dos riscos e impactos. Entre outros pontos, a ferramenta Eramba permite a criação da política dos riscos, fluxos de informações e de procedimentos para enfrentamento dos riscos. É possível realizar a distribuição de responsabilidades e criar em tempo real um banco de dados para consultas dos processos de gestão de riscos. Essa ferramenta também é utilizada para a realização de processos de auditoria, desde a sua concepção até a avaliação dos resultados.

xv. ITouchVision Governance & Risk: dispõe de consultas através de questionários que podem ser facilmente estruturados dentro da aplicação. Além disso, é possível determinar a atuação de cada usuário da aplicação e como esse colaborador poderá atuar em determinados cenários em que o risco existe. A solução fornece ferramentas de auditoria em processos e de auditoria de departamentos e pessoas, sendo possível, também, criar um instrumento de comunicação entre um usuário comum e o administrador. Permite a conexão de múltiplos dispositivos distintos, tais como microcomputadores, celulares, *tablets* e *smartphones*. Finalmente, a sua estrutura conta com um módulo direcionado à gestão pública, apresentando ferramentas de mineração de informações e funcionalidades para gerenciar e garantir a conformidade com processos legais, além de criar e explorar diversos canais de contato entre o cidadão e a gestão pública.

xvi. IBM OpenPages GRC: permite a identificação, a análise e a gestão dos riscos operacionais em uma única plataforma, garantindo e evidenciando a visualização dos riscos com a possibilidade de agir ou mitigar ações sobre um ou mais riscos identificados. É uma ferramenta rápida para encontrar possíveis dados ocultos e identificar as principais relações sobre um risco e, além disso, possibilita a utilização de análise de cenários, com oportunidade para monitorar e avaliar os impactos relacionados aos riscos verificados. Assim, é possível realizar o tratamento de dados através de seu armazenamento e de sua alta disponibilidade.

xvii. IntelligenceBANK GRC: oferece o registro de um risco e a sua gestão, que corresponde desde a identificação de um risco até a sua devida solução. Na prática, garante a utilização de métricas e de *dashboards* personalizáveis, e permite a visualização e o registro dos riscos utilizando como fonte de informação as mais disseminadas práticas de conformidade como ISO, COBIT e SOX. O sistema avançou no recebimento de feedback quase que em tempo real, através de consultas e de questionários difundidos em toda a organização, permitindo também exportar arquivos nos mais diversos formatos. A ferramenta inclui ainda calendário para o registro das atividades e oferece serviços de hospedagem na nuvem.

xviii. INTERISK – Inteligência em Riscos: possui três módulos integrados: (1) Gestão de Riscos Corporativos; (2) Auditoria Baseada em Riscos; e (3) Gestão da Continuidade dos Negócios. Essa integração possibilita definir os critérios para mensuração da Probabilidade e Impacto e da Matriz de Riscos alinhada com o Apetite ao Risco, conforme a estratégia da sua empresa, e permite ainda integrar inúmeras disciplinas de riscos, possibilitando que o gestor tenha visão holística e agilidade durante o trabalho. Seu funcionamento visa ao armazenamento seguro, à transparência e à linguagem-padrão.

xix. MasterControl – Risk Analysis Software Systems: permite o controle dos riscos em um módulo separado, em que é possível acompanhar o ciclo de vida de um determinado risco, desde a sua análise inicial até a sua definitiva resolução. Este software implementa uma série de controles, métricas e formas de avaliar os dados com o intuito de fundamentar e embasar decisões da alta gerência, além de possibilitar mecanismos de controle e avaliação de riscos padronizados. Oferece o envio periódico de formulários e de questionários relacionados a melhores práticas e torna possível criar relatórios customizáveis atendendo a demandas específicas de determinados cenários.

xx. MetricStream: a solução MetricStream tem sua infraestrutura disposta na nuvem, fator que favorece a segurança dos dados, além de centralizá-los em um único ambiente de dados. Oferta aos consumidores um banco de dados robusto e a verificação das melhores práticas/processos de trabalho. Em destaque, a ferramenta permite a criação de métricas e de *dashboard* com informações personalizáveis, e a automatização e o controle de fluxos de trabalhos com o intuito de reduzir riscos. Por fim, garante a gestão dos riscos adequando-os em processos que podem ou não ser estudados e alte-

rados conforme marcos regulatórios e boas práticas como ISO e *frameworks* como COBIT, ITIL, entre outros.

xxi. Open Risk: é uma ferramenta de código aberto direcionada para a análise dos riscos financeiros em uma instituição. Objetiva o gerenciamento dos riscos, de modo a possibilitar a sua identificação, a criticidade e os impactos. Além disso, é possível criar fluxos de informações e procedimentos para enfrentar os riscos. Permite o desenvolvimento da política de riscos e a distribuição de responsabilidades e, por fim, considera o controle e o monitoramento dos riscos como fundamentais para tornar possível enfrentá-los.

xxii. OpenSource Risk: com foco no gerenciamento dos riscos, a ferramenta permite a fixação dos objetivos em todos os níveis da organização. É voltada para a identificação/mapeamento de processos e enfrentamento/tratamento dos riscos. Permite criar fluxos de informações e painéis de informações para atualização das verificações dos riscos e para a distribuição de responsabilidade. São ainda possíveis a criação de banco de dados e a utilização de metodologias condizentes com a realidade de cada organização.

xxiii. Optial Risk Management: esta ferramenta possui a facilidade de se adequar às mais variadas estruturas organizacionais, além de possuir compatibilidade com marcos regulatórios atuais, como, por exemplo, SOX, ISO e COSO. É uma solução que permite o acompanhamento de todos os processos e ações através de um módulo de auditoria interna, propiciando a exportação de dados e a criação de métricas e de relatórios personalizados. Além disso, as funções e responsabilidades dos usuários podem ser designadas, o que permite a gestão das ações e de um risco desde a sua identificação inicial até a resolução da demanda. Em especial, é possível automatizar a avaliação de riscos escolhendo pilares de conteúdo, além de ser possível definir a periodicidade dessas ações e registrar informações pertinentes sobre um determinado risco, entre elas: valores de impacto, probabilidade e exposição em um nível de risco inerente.

xxiv. Oracle Fusion Governance Risk: através desta ferramenta, é possível controlar a execução e as atividades relacionadas a um processo, sendo permitido explorar riscos, pontos de melhoria e problemas em busca das melhores ações e processos mais eficientes. Esta solução possui uma vasta gama de relatórios e de métricas de avaliação pré-configuradas, mas permite a personalização. É possível ainda avaliar o status particular de cada atividade, entre

as quais medidas corretivas e adequações. Possibilita que a organização desenhe o seu cenário de atuação, bem como características específicas para verificar e analisar a influência de riscos. Como vantagem, esta ferramenta possui uma biblioteca de políticas já aplicadas por outras organizações com o intuito de fundamentar mudanças e adequações em processos e, além disso, consegue avaliar os modelos de negócios e sugerir anomalias em processos ou fluxos de trabalho. As análises podem ser feitas por meio de multicritérios.

xxv. Oracle GRC: este software é um módulo de gestão de riscos que busca o enfrentamento dos riscos identificados na organização em todos os seus níveis. Visa considerar os riscos de maneira distinta e possibilitar diferentes formas de controle e abordagens para cada um deles. É possível realizar a distribuição de responsabilidades dentro da ferramenta, bem como estabelecer processos internos e externos de auditoria, etapa entendida como complementar ao gerenciamento dos riscos. A ferramenta possibilita, ainda, a adequação de processos às normas e regulamentações pelas quais a organização é regida.

xxvi. ProcessGene GRC: atua em uma vasta gama de riscos, regulamentações e sistemas de auditorias para garantir ao usuário um local centralizado de informações. Possui painéis e métricas personalizáveis com o intuito de direcionar a apresentação de resultados e oferta um módulo que tem por objetivo servir como um histórico para mapear e armazenar a maior quantidade possível de informações. A ferramenta permite a distribuição de papéis de acesso e atuação e, ainda, a automação e a análise de fluxos de trabalho, bem como atividades relacionadas com o intuito de tornar cada processo eficiente e eficaz. A infraestrutura da aplicação está disponível na nuvem.

xxvii. RiskGAP: objetiva a utilização de grupos de trabalho na identificação e na classificação de riscos. Ela oferta aos gestores uma base de conhecimento em processos e regulamentos legais para alinhar ações e processos mais adequados aos objetivos da organização, intensificando a atuação dos usuários ao possibilitar a análise e a verificação dos riscos. Permite, ainda, que através de um módulo de pesquisa seja ofertado ao usuário um relatório sobre as melhores práticas segundo a mineração de informações e garante a seus usuários a integração dessas informações em diferentes sistemas corporativos.

xxviii. RIVO: permite uma visualização completa da organização em busca dos principais riscos aos quais ela pode estar sujeita. É uma ferramenta que busca facilitar a padronização das avaliações de riscos para análises futuras e basear decisões acerca de medidas corretivas, permitindo a utilização de diversas métricas e de quadros de visualização para situar os gerentes, influenciando-os diretamente na tomada de decisão em tempo real. Sua estrutura possibilita criar uma "biblioteca de riscos" com o objetivo de catalogar os principais riscos e permitir consultas futuras. Também possibilita criar um mapa de riscos que pretende mapear a organização e demonstrar os setores com as maiores tendências e as maiores taxas de incidentes bem como a classificação e a categorização dos riscos. Suas informações são disponibilizadas em arquitetura de nuvem.

xxix. RSA Archer: esta ferramenta possibilita o ajuste em políticas da organização nos processos internos já existentes e em novos processos, reconfigurando rapidamente aplicações, fluxos de trabalho, relatórios e painéis. Sua linguagem permite a adequação de processos aos guias de boas práticas mais atualizados disponíveis atualmente no mercado. É possível distribuir e elencar responsabilidades por gestores ou por departamentos para que atuem de forma a minimizar os efeitos de um determinado risco organizacional. Permite a utilização de métricas e de *dashboards* personalizáveis bem como de controles adicionais contra fraudes, danos financeiros, entre outros.

xxx. SAP GRC: com esta solução, é possível automatizar o provisionamento e certificar que o acesso a processos e a dados é feito apenas para aqueles que possuem responsabilidades sobre eles. Esta ferramenta possui um módulo de auditoria interna que objetiva verificar a integridade de processos, alinhamentos antifraudes, controle de processos, entre outros recursos. Permite a visualização dos riscos, classificando a sua influência bem como o seu impacto nos processos organizacionais. Além do mais, permite a gestão dos riscos desde o momento em que eles são inicialmente verificados até que medidas corretivas sejam tomadas para solucionar a demanda.

xxxi. SE Risk: estabelece uma infraestrutura de risco que produz relatórios regulamentares precisos e permite a gestão e o monitoramento dos riscos em tempo real. Como principais funcionalidades, esta ferramenta possibilita criar repositório de riscos, controles, atividades de mitigação e procedimentos operacionais-padrão facilitando o reúso e, ademais, permite identificar, capturar e gerenciar os processos mais críticos de risco. Os

riscos são avaliados levando em consideração as suas várias dimensões e critérios de impacto bem como probabilidade e fluxo de trabalhos para garantir o correto uso dos dados e, para tanto, a solução permite a aplicação de modelos de avaliação de riscos quantitativos e qualitativos, independentemente do tipo. Permite, ainda, a avaliação automática dos riscos e proporciona avaliações e comparações entre o risco residual e o risco inerente, com alertas proativos quando os limites são excedidos. Como vantagens, a ferramenta monitora a eficácia das atividades de mitigação, controles e políticas, assim como as mudanças nos riscos e nos requisitos através da gestão de testes, indicadores e incidentes, e oferece mapas de calor (*heat maps*) para análise e monitoramento dos riscos.

xxxii. Simple Risk: o software Simple Risk é um módulo destinado à realização de auditorias, permitindo a criação de fluxos de auditoria e gestão de processos, os quais podem ser processos por departamento ou ramos de negócios. Possibilita também a implementação de metodologias e a adequação de cenários para aplicação das etapas da auditoria, seja ela interna ou externa. A ferramenta considera os riscos tanto no nível departamental como no organizacional e oferece a possibilidade de criação de banco de dados para consultas futuras.

xxxiii. TruComply: possibilita a identificação e o rastreio de regulamentos e de padrões que podem ser aplicados em uma organização no que se refere a controle de riscos, de processos, etc. Esta solução permite a criação de quadros de controle com métricas e painéis de dados personalizáveis, o que atesta o desenvolvimento, a documentação e a comunicação em toda a organização de práticas, procedimentos e padrões alinhados com os objetivos e com a missão organizacional. Em suma, a ferramenta gerencia todas as atividades relacionadas a um risco, e isso pode ser feito desde o momento em que ele for identificado até a sua devida correção.

Diante das análises sistematizadas e em consonância com os aspectos já mencionados neste estudo, é possível observar que, em geral, as ferramentas de software se comprometem a realizar e respaldar processos e iniciativas de gestão de riscos. Todas as ferramentas apresentadas mostraram aptidão para executar ações e tarefas em diferentes etapas do gerenciamento de riscos, que vai desde o momento de identificação dos riscos, passando por sua análise, categorização, controle e monitoramento e etapas de respostas até chegar em planos de ação. De certa forma, é possível inferir múltiplas semelhanças entre as

ferramentas destacadas, atuando de maneira abrangente nas diversas situações que correlacionam a gestão dos riscos institucionais.

Como é possível visualizar nos dados apresentados no Quadro 15, a abordagem utilizada pela maioria dos aplicativos de gestão de riscos difere apenas na amplitude em que a análise e a gestão de riscos podem ocorrer. Para alguns aplicativos, como Accelus, SE Risk, RIVO, entre outros, considera-se a organização como uma entidade única, com objetivos de gestão específicos e alinhados a toda a empresa. Já em outros – exemplos SAP GRC, ProcessGene GRC, 360factor, entre outros –, opta-se por observar os níveis organizacionais e departamentos respeitando-se objetivos específicos para a realização/execução dessa iniciativa.

Observa-se, ainda, a existência de procedimentos complementares ao processo de gestão de riscos. Como exemplo, citam-se:

- a utilização de métricas de avaliação para situar e apresentar dados relevantes em formato de relatórios ou de telas de apresentação – Oracle Fusion Governance Risk, TruComply, RSA Archer, Optial Risk Management, MetricStream, entre outros;

- a centralização de informações, que consiste em uma propriedade impactante no desenvolvimento de software ou em iniciativas ligadas à gestão de riscos – Active Risk Manager, BRINQA, Eramba, ITouchVision Governance & Risk, entre outros; e

- a facilidade de exploração de dados para encontrar informações e conhecimentos relevantes – ORACLE GRC, Simple Risk, ACL GRC, BWISE, entre outros.

Adiante, foi possível notar que em quase todos os aplicativos há pelo menos um módulo específico para a gestão da comunicação ou de processos que permite o fluxo de informações indispensáveis para o sucesso de ações de gestão, como, por exemplo, notificações direcionadas, entrega de notícias através do serviço de e-mails, entrega de relatórios diários, entre outros. Como exemplos, citam-se as ferramentas Accelus, Adaptive GRC, BPS Resolver, Convercent, Enablon, MasterControl – Risk Analysis Software Systems, Optial Risk Management, Oracle Fusion Governance Risk e outras.

Garantir a disponibilidade de informações organizacionais a gestores e colaboradores inseridos em qualquer iniciativa de gestão é de fundamental importância para o alinhamento correto das ações em prol de um objetivo de controle. Sendo assim, funcionalidades como questionários e outras avaliações visam garantir o envolvimento de todos e o feedback dos mais diversos níveis organizacionais. São, ademais, elementos que garantem a multidisciplinaridade para a gestão e sua efetiva adequação a realidades e cenários específicos. Nesse sentido, os softwares que mais se destacaram foram: I Touch Vision Governance & Risk, IntelligenceBANK GRC e MasterControl – Risk Analysis Software Systems.

Outro elemento que se destaca nas ferramentas de software apresentadas é a utilização de módulos específicos para auditorias, que se configuram como processos metódicos de verificação e adequação de procedimentos. Esse elemento é de suma importância para se estimar o sucesso na empregabilidade de iniciativas de gestão, já que permite avaliar criticamente um cenário em busca de procedimentos que impulsionem melhorias contínuas, adequação de conduta, entre outros fatores que primem pela continuidade de processos. As ferramentas Optial Risk Management, ProcessGene GRC, SAP GRC, 360factor, Adaptive GRC e Aris GRC são os melhores exemplos dessa configuração.

Pode-se observar, por último, a massiva utilização de componentes extras para realizar a verificação de regulamentações vigentes, bem como exigências legislativas que devem ser levadas em conta durante as atividades de uma organização. Enablon, ProcessGene GRC e SE Risk são ferramentas que demonstraram essa preocupação. É necessário ressaltar, entretanto, que, para a aplicabilidade desses processos de acompanhamento legislativo e de regulamentações, o módulo destinado a essa atividade deverá ser devidamente estudado e planejado para que se adéque às diversas realidades que possam influenciar processos e produtos das organizações.

Finalmente, para quaisquer interessados nas ferramentas descritas, recomenda-se uma análise mais profunda e adequada à sua aplicabilidade nas práticas e nos objetivos organizacionais. De fato, não houve a pretensão de se estabelecer qual a melhor, mas sim de se fazer uma apresentação integral das ferramentas mais comuns disponíveis no mercado, com suas características e funcionalidades. Para tanto, entende-se a necessidade

de cada instituição reconhecer, de acordo com seu contexto e interesse, qual dessas ferramentas deverá atender melhor à sua finalidade. Como sugestão, caso o propósito organizacional seja a automação do processo de gestão de riscos – para instituições privadas ou públicas –, vê-se nos softwares SE Risk, INTERISK – Inteligência em Riscos, Active Risk Manager, Adaptive GRC e IBM OpenPages GRC maior viabilidade.

7. Investigando casos reais de gestão de riscos no setor público: os casos da UNIFAL-MG e do CEFET/RJ

7.1. Contexto e motivação

A realização de estudos de caso, quando se trata de algum contexto da vida real das pessoas, tem provado o seu valor às investigações empírico-científicas para compreender, de maneira holística, os fenômenos sociais. A análise desses fenômenos, observados em seu ambiente natural, propicia aos pesquisadores um conjunto de variáveis prevalecentes de fatos verdadeiros e concretos, e assegura o alcance de conclusões relevantes para aqueles que realizam as pesquisas e para as outras partes interessadas.

Para corroborar, portanto, o desenvolvimento das pesquisas em gestão de riscos, confrontar e confirmar a coerência das técnicas e dos métodos desenvolvidos no decurso do Projeto ForRisco com a realidade prática das organizações, optou-se pela realização de estudos de caso em duas Instituições Federais de Ensino Superior (IFES), autarquias vinculadas ao Ministério da Educação (MEC) brasileiro. São elas: (1) a Universidade Federal de Alfenas – Minas Gerais (UNIFAL-MG) e (2) o Centro Federal de Educação Tecnológica Celso Suckow da Fonseca – Rio de Janeiro (CEFET/RJ).

7.2. Objetos da pesquisa

A seguir, são apresentadas as duas IFES avaliadas no que diz respeito a seus atuais processos de gestão de riscos.

7.2.1.Universidade Federal de Alfenas – UNIFAL-MG/BRASIL

A UNIFAL-MG, originalmente Escola de Farmácia e Odontologia de Alfenas - EFOA, foi fundada em abril de 1914 e em 2005 foi transformada em universidade. Além da sede, na cidade de Alfenas-MG, teve sua ampliação por meio de mais dois campi avançados: o campus Varginha/MG e o campus Poços de Caldas/MG. Integralmente, a UNIFAL-MG tem sido responsável pela formação de várias gerações de profissionais através de seus cursos de graduação

e pós-graduação, pela consolidação de atividades de extensão, ocupando posição de destaque na prestação de serviços à comunidade local e regional e pelo crescimento expressivo de sua produção científica e tecnológica. Como missão, a instituição visa promover a formação plena do ser humano, gerando, sistematizando e difundindo o conhecimento, comprometendo-se com a excelência no ensino, na pesquisa e na extensão, com base nos princípios da reflexão crítica, da ética, da liberdade de expressão, da solidariedade, da justiça, da inclusão social, da democracia, da inovação e da sustentabilidade.

7.2.2. Centro Federal de Educação Tecnológica Celso Suckow da Fonseca – CEFET/RJ/BRASIL

O CEFET/RJ teve a sua origem em 1917 como Escola Normal de Artes e Ofícios Wenceslau Braz. Atualmente, é uma instituição federal de ensino que se compreende como um espaço público de formação humana, científica e tecnológica, oferecendo cursos técnicos integrados ao ensino médio, subsequentes (pós-médio), tecnológicos, de graduação e de pós-graduação *lato sensu* e *stricto sensu* (mestrado e doutorado), nas modalidades presencial e à distância. Desde 2010, e a partir do Programa de Expansão da Educação Profissional – PROEP, a instituição conta com o campus-sede Maracanã e com mais sete campi espalhados pelo Estado do Rio de Janeiro, que são: Angra dos Reis, Itaguaí, Maria da Graça, Nova Friburgo, Nova Iguaçu, Petrópolis e Valença. O CEFET/RJ atua na tríade ensino, pesquisa e extensão, e visa contribuir na formação de profissionais bem preparados para o desenvolvimento econômico e social de mesorregiões do Estado do Rio de Janeiro.

7.3. Procedimentos da investigação

Esta pesquisa é definida pelo método de investigação de base qualitativa, com profundas inferências em estudos de caso. A pesquisa qualitativa considera que há uma relação dinâmica, contextual e temporal entre a pesquisa e o objeto de estudo, por isso demanda uma interpretação demasiada dos fenômenos à luz do contexto e dos fatos [30]. Na pesquisa qualitativa, o pesquisador participa, compreende e interpreta os acontecimentos de maneira consciente e coerente, com precisão e objetividade, e deve garantir a argumentação lógica das ideias.

Para além da pesquisa qualitativa, encontra-se o estudo de caso como uma fundamentação científica que subsidia a coleta e a análise dos dados [31]. Em 1994, o pesquisador Creswell [32, p. 12] ressaltou uma definição muito próxima do que é aceito hoje, entendendo o estudo de caso como o processo em que "o pesquisador explora uma simples entidade ou fenômeno limitado pelo tempo e atividade, e coleta detalhadamente as informações utilizando uma variedade de procedimentos".

Nessa lógica, o estudo de caso deve ser considerado um delineamento material em que são utilizados diversos métodos ou técnicas de coleta de dados, como, por exemplo, a observação, a entrevista e a análise de documentos [31]. Prontamente, propõe-se que um estudo de caso deve ser entendido como uma investigação empírica que examina um fenômeno contemporâneo em seu contexto, especialmente quando os limites entre o fenômeno e o contexto não estão claramente definidos [33].

Partindo das definições apresentadas, é importante compreender que um estudo de caso traz características essenciais que o circundam em um nível estratégico e que foram levadas em consideração para o desenvolvimento deste conteúdo, a saber:

1. o caráter unitário do fenômeno pesquisado, isto é, a gestão de riscos em IFES;

2. a investigação de um fenômeno contemporâneo: embora considerados conjunções históricas, os processos de gestão de riscos dessas instituições ocorrem simultaneamente com a realização da pesquisa;

3. a utilização de múltiplos procedimentos de coleta de dados: a gestão de riscos vem sendo examinada levando em consideração diferentes meios de coleta de dados, tais como a entrevista, a observação participante e a análise de documentos;

4. ser um estudo de profundidade: a entrevista aplicada às IFES é semiestruturada, o que permite maior aprofundamento dos temas pesquisados e, em consequência, aumento do nível de interioridade nas organizações.

Do ponto de vista do nível operacional, ou melhor, considerando uma proposta de conteúdo e sequência para a condução do estudo de caso, foi

adaptado o estudo de Cauchick Miguel [34, p. 221], que oferece a estruturação para se conduzir o estudo de caso como detalhado na Figura 15 a seguir:

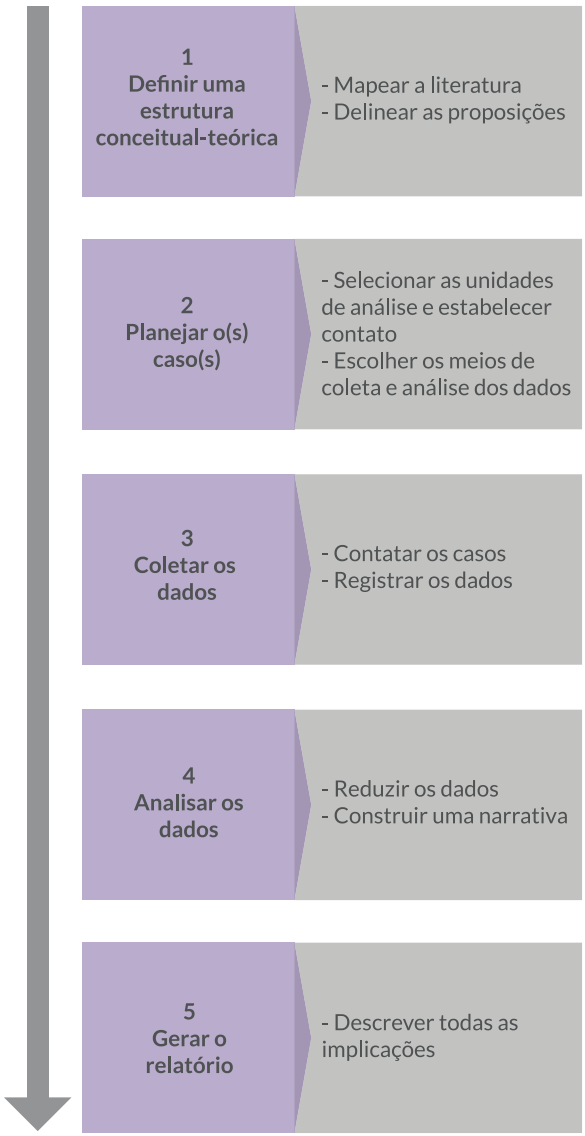


Figura 15 – Etapas para a condução do estudo de caso
Fonte: Cauchick Miguel (2007, p. 221), com adaptações

A princípio, foi realizado um mapeamento de literaturas relevantes sobre a gestão de riscos em organizações públicas e privadas, além das metodologias e ferramentas para execução desse gerenciamento. Todo esse levantamento é, inclusive, apresentado no decurso do livro. Dado o estudo sobre a gestão de riscos, viu-se a necessidade de se propor um estudo de caso em instituições que apresentassem seus processos já estruturados, delimitando as proposições deste capítulo. Para tal, foram escolhidas duas instituições de ensino superior no Brasil que estão desenvolvendo seus processos de formulação, implementação, monitoramento e controle dos riscos, o que em outras palavras se resume em gerenciamento ou gestão de riscos. A escolha da UNIFAL-MG e do CEFET/RJ para compor a pesquisa ocorreu por meio da participação dessas instituições no Fórum Nacional de Pró-Reitores de Planejamento e Administração, evento em que ambas divulgaram seus projetos para gestão de riscos.

Os métodos de coleta de dados selecionados foram: a entrevista, com membro responsável ou corresponsável pela implantação da gestão de riscos institucional; a observação participante, por meio da avaliação de apresentações em congressos dos seus respectivos processos de gestão, de ambas as organizações; e, por último, a disponibilização de documentos referentes à gestão dos riscos, como, por exemplo, a Política de Gestão de Riscos. No momento seguinte, as instituições foram contatadas, tendo sido ajustados os compromissos de cada uma delas para que pudessem se integrar ao estudo. Todos os dados, obtidos por meio das entrevistas, das apresentações e dos documentos, foram colhidos num prazo máximo de 30 dias. Para a análise, optou-se pela narrativa descritiva dos fatos e das implicações encontradas durante o processo da pesquisa.

A realização da pesquisa na UNIFAL-MG teve apoio da Pró-Reitoria de Planejamento, Orçamento e Desenvolvimento Institucional (Proplan), na figura do pró-reitor adjunto, que atua diretamente na Coordenadoria de Desenvolvimento Institucional (CDI). O pró-reitor deu suporte à aplicação do questionário da entrevista, que foi efetuado integralmente nos dias 6, 7 e 8 de março de 2018 via Skype. A entrevista semiestruturada possui 25 questões – APÊNDICE III – sobre as diferentes etapas para se executar a gestão de riscos em uma instituição. As etapas são: (1) definição da política [quatro perguntas]; (2) estabelecimento de contexto externo [três perguntas]; (3) definição das estratégias de gestão de riscos [quatro perguntas]; (4) estabelecimento de contexto interno [três perguntas]; (5) realização efetiva da gestão de riscos nas ativi-

dades [quatro perguntas]; (6) reavaliação da política [duas perguntas]; e (7) avaliação da maturidade da gestão de riscos na organização [cinco perguntas].

Foi também disponibilizada pela UNIFAL-MG a documentação sobre seus processos de gestão de riscos. A universidade cedeu os seguintes documentos: a Política de Gestão de Riscos, efetivada em 4 de maio de 2017 e utilizada pela atual gestão; a Minuta do Plano de Gestão de Riscos da UNIFAL-MG, que se define como um plano prático para desenvolvimento de procedimentos e ações de gerenciamento dos riscos em 2018; e, ainda, uma apresentação prévia de uma exposição feita pelos coordenadores da gestão de riscos da universidade no FORPLAD. Este Fórum aconteceu nos dias 14, 15 e 16 de março de 2018, na cidade de Natal, Rio Grande do Norte, onde foram apresentados detalhadamente os procedimentos e o andamento da gestão de riscos da UNIFAL-MG. O painel, intitulado "Projeto de Desenvolvimento do Sistema ForRisco", desenvolvido pela universidade e acompanhado pelos pesquisadores, foi também um objeto importante deste estudo.

Antes da realização da entrevista no CEFET/RJ, aconteceu uma reunião prévia entre o analista de planejamento e gestão júnior – membro do Projeto ForRisco – e a chefe do Departamento de Desenvolvimento Institucional (DEDIN) da instituição CEFET/RJ, na manhã de sexta-feira (23/2/2018) na cidade de Brasília/DF. Esse encontro teve a finalidade de permitir conhecer um pouco mais a gestão de riscos do CEFET/RJ e formalizar o convite para a realização do estudo de caso, que foi prontamente aceito. A aplicação do questionário da entrevista aconteceu nos dias 11, 12 e 13 de abril de 2018 via Skype. Vale destacar que as mesmas perguntas aplicadas à UNIFAL-MG foram também aplicadas ao CEFET/RJ, portanto o questionário segue a mesma estrutura de execução da gestão de riscos apresentada anteriormente.

Além da entrevista, os pesquisadores tiveram acesso à Política de Gestão de Riscos do CEFET/RJ, a uma apresentação desenvolvida pela Diretoria de Gestão Estratégica (DIGES) dessa instituição e a duas planilhas com detalhamento das etapas de mapeamento (processos críticos identificados, definição dos riscos, análises de probabilidade e impactos dos riscos) e gerenciamento dos processos dos riscos. Destaca-se que o CEFET/RJ também realizou uma apresentação no Fórum Nacional de Pró-Reitores de Planejamento e Administração, em Natal, Rio Grande do Norte, nos dias 14, 15 e 16 de março de 2018, intitulada "Gestão de riscos: a experiência do CEFET/RJ", e que serviu de embasamento para a realização do estudo de caso.

Por conseguinte, dá-se ênfase à busca por totalidade e profundidade nos objetos de pesquisa estudados, e nesse caso, pretende-se entender a realidade dos processos de formulação, implementação e execução da gestão de riscos em instituições públicas de ensino. Revela-se a importância de se compreenderem os estudos de caso realizados, objetivando-se o entendimento de técnicas distintas para a gestão dos riscos. Destaca-se também a padronização dos procedimentos de coleta de dados, efetuado em ambas as instituições, por meio de análise documental, entrevistas e observação participante. Finalmente, a seguir, são apresentadas as análises dos casos da gestão de riscos na UNIFAL-MG e no CEFET/RJ e, posteriormente, mostra-se um comparativo entre as instituições e a proposta de execução da gestão de riscos pela metodologia ForRisco.

7.4. Estudo de caso: a Universidade Federal de Alfenas – UNIFAL-MG/BRASIL

A Política de Gestão de Riscos da UNIFAL-MG é recente, mas desde o início se estabeleceu como referência dentro desta instituição. O desenvolvimento de uma Política de Gestão de Riscos na UNIFAL-MG foi pensado a partir do que prescreve o artigo 17 da Instrução Normativa Conjunta MPOG/CGU nº 1, de 10 de maio de 2016. A universidade, em cumprimento à Portaria nº 888, art. 3º, inciso VII, determina a sua política em 7 de julho de 2017.

O desenvolvimento da Política de Gestão de Riscos da UNIFAL-MG ocorreu, inicialmente, por meio da atuação da pró-reitora de Planejamento, Orçamento e Desenvolvimento Institucional. Nesse sentido, a Proplan é o órgão de assessoria da Reitoria responsável pela elaboração das propostas orçamentárias da instituição, pelas informações institucionais, pelo suporte técnico a todos os órgãos da UNIFAL-MG na elaboração de planos, projetos e propostas de convênios, bem como pelas iniciativas de modernização administrativa sustentável.

Atualmente, a Proplan é composta de: pró-reitor; pró-reitor adjunto; coordenadores (Coordenadoria-Geral (CGE); Coordenadoria de Desenvolvimento Institucional (CDI); Coordenadoria de Orçamento (COR); Coordenadoria de Projetos e Obras (CPO)); gestores das gerências (Gerência de Informação e Marketing Institucional; Gerência de Planejamento Estratégico; Gerência de Meio Ambiente e Desenvolvimento Sustentável; Gerência de Planejamento Orçamentário; Gerência de Execução e Controle Orçamentário; Gerência de Arquitetura; Gerência de Engenharia); e demais servidores.

Após ser elaborada, a política foi apresentada ao Comitê de Governança, Riscos e Controle (CGRC), uma entidade interna da UNIFAL-MG responsável por analisar, aprovar, tratar e monitorar os riscos da instituição. O CGRC tem sua composição estabelecida pela presença do reitor da UNIFAL-MG, na figura de presidente; o pró-reitor de Administração e Finanças; pró-reitor de Planejamento, Orçamento e Desenvolvimento Institucional; pró-reitor de Graduação; pró-reitor de Pesquisa e Pós-Graduação; pró-reitor de Extensão; pró-reitor de Assuntos Comunitários e Estudantis; pró-reitor de Gestão de Pessoas; e coordenador de Desenvolvimento Institucional, na condição de secretário.

Após aprovação da política pelo Comitê, este se torna o principal promotor das práticas e dos princípios previstos no documento, além de prover e institucionalizar estruturas adequadas de governança, gestão de riscos e controles internos. Dessa forma, cabe mencionar que o objetivo geral da política é propiciar elementos para que a UNIFAL-MG institua a gestão de riscos e promova a identificação, a avaliação, a estratégia de tratamento e o monitoramento dos riscos a que está sujeita.

Nesse sentido, a instituição entende que a gestão de riscos se destina a assegurar aos gestores o acesso às informações quanto aos riscos a que a organização está exposta, melhorando o processo de tomada de decisão e ampliando a possibilidade do alcance de objetivos. O CGRC tem por intuito elaborar, aprovar e implementar a Política de Gestão de Riscos da UNIFAL-MG, que será revisada anualmente, dando início a um novo ciclo de elaboração, aprovação e implementação.

Aliás, para implementação da Política de Gestão de Riscos, a UNIFAL-MG leva em consideração, a princípio, o Plano de Desenvolvimento Institucional (PDI) bem como os objetivos, as metas e os indicadores previstos naquele documento. Posteriormente, são retomados os objetivos estratégicos organizacionais (macroprocessos) da instituição, isto é, das unidades que a formam: Reitoria, Vice-Reitoria, Pró-Reitorias e Diretorias. E, em seguida, são explicitados os processos gerenciais e de apoio, e os subprocessos em dois níveis organizacionais: Pró-Reitorias e Diretorias. É a partir desse mapeamento de macroprocessos, processos e subprocessos que se compreende a quais riscos cada unidade organizacional poderá estar sujeita.

Desse modo, são mapeadas as principais ações a serem executadas, em seus diferentes níveis de responsabilidade. O mapeamento considera os seguintes tipos de risco, conforme o Quadro 16, a seguir:

Quadro 16 – Tipologia dos riscos

Tipologia do Risco	Interpretação
Operacionais	Eventos que podem comprometer as atividades do órgão ou da instituição, normalmente associados a falhas, deficiência ou inadequação de processos internos, pessoas, infraestrutura e sistemas.
Legais	Eventos derivados de alterações legislativas ou normativas que podem comprometer as atividades do órgão ou da instituição.
Financeiros/ Orçamentários	Eventos que podem comprometer a capacidade do órgão ou da instituição de contar com recursos orçamentários e financeiros necessários à realização de suas atividades, ou eventos que possam comprometer a própria execução orçamentária, tais como atrasos no cronograma de licitações.
Imagem/Reputação do Órgão ou da Instituição	Eventos que podem comprometer a confiança da sociedade (ou de parceiros, clientes ou de fornecedores) em relação à capacidade do órgão ou da instituição em cumprir a sua missão institucional.
Demais Riscos	Outros riscos, tais como riscos culturais, tecnológicos, de gestão, de recursos humanos, entre outros que podem comprometer o andamento das atividades da instituição.

Cabe ressaltar que o processo de identificação e mapeamento garante a compreensão de quais procedimentos podem oferecer riscos a uma unidade organizacional específica, visto que as unidades são também as responsáveis pela etapa de identificação. Os riscos identificados devem ser atribuídos ao chamado "proprietário do risco", que é responsável por assegurar que o risco seja monitorado, gerenciado e tratado adequadamente. Vale destacar ainda que a análise deve cobrir todas as atividades consideradas relevantes para a realização dos objetivos institucionais da UNIFAL-MG.

Nota-se, dessa forma, que as responsabilidades não estão concentradas somente nos membros do CGRC, mas em todos aqueles que fazem parte da organização. Esta foi a maneira encontrada pela UNIFAL-MG para garantir plena execução dos processos de monitoramento e controle dos riscos: a responsabilização. O Quadro 17 sintetiza os atores e as suas responsabilidades para com os riscos.

Quadro 17 – Atores e descrição de responsabilidades

Ator	Responsabilidade
Comitê	Elaborar o Plano de Gestão de Riscos. Realizar a gestão do Plano de Gestão de Riscos. Determinar medidas mitigadoras, monitorar ações e comunicar situações.
Reitor	Garantir a continuidade e o aperfeiçoamento da Política de Gestão de Riscos.
Pró-Reitores	Monitorar, no respectivo âmbito, os riscos mapeados. Comunicar sobre situações que envolvem risco e aplicar medidas de mitigação necessárias.
Coordenadores	Monitorar, no respectivo âmbito, os riscos mapeados. Comunicar sobre situações que envolvem risco e aplicar medidas de mitigação necessárias.
Servidores	Monitorar, no respectivo âmbito, os riscos mapeados. Comunicar sobre situações que envolvem risco e aplicar medidas de mitigação necessárias.

Com o intuito de garantir a excelência no desenvolvimento do Plano de Gestão de Riscos, a UNIFAL-MG teve o apoio de auditores da CGU, que receberam, entre os dias 27 e 29 de junho de 2017, um curso de capacitação sobre gestão de riscos e controles internos no setor público. O curso foi oferecido a todos os gestores, pró-reitores, dirigentes de institutos, diretores de campi e técnicos, com o propósito de garantir o mesmo entendimento sobre o gerenciamento de riscos na instituição. Cabe aos pró-reitores disseminarem a gestão de riscos dentro de cada unidade pela qual se responsabilizam. Além do mais, o curso da CGU foi intensificado pela CDI da UNIFAL-MG, garantindo coesão no entendimento do tema.

Assim, de um modo geral, a UNIFAL-MG estabeleceu a estrutura do seu processo de gestão de riscos em cinco etapas: (1) identificação dos riscos; (2) análise dos riscos; (3) planejamento; (4) rastreamento e monitoramento; e (5) controle dos riscos. A Figura 16 revela essa estrutura:

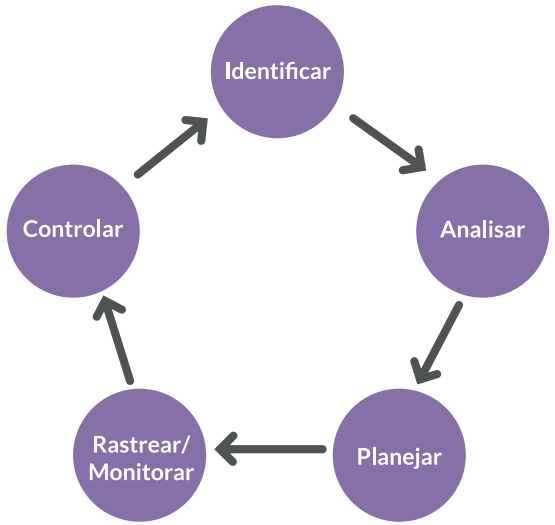


Figura 16 – Ciclo da gestão de riscos na UNIFAL-MG

Para o processo de identificação, sugere-se que o mapeamento dos processos das unidades seja realizado *in loco*, isto é, pelos próprios servidores envolvidos, por meio do levantamento de dados históricos, informações, realização de entrevistas e reuniões com dirigentes e técnicos em suas atividades. A identificação dos processos e dos riscos é inerente a cada área ou unidade e pode ocorrer por meio de dois contextos: o externo e o interno.

No caso do estabelecimento do contexto externo, a UNIFAL-MG conta com o apoio da Procuradoria Jurídica. É por meio dessa unidade legítima que a universidade responde às principais mudanças externas, que notadamente se referem às mudanças na legislação. A respeito do contexto interno, cada unidade deverá levar em conta suas habilidades, estratégias, atividades desenvolvidas e regimento interno ou política da instituição. Além das próprias unidades, que são responsáveis pela identificação e pelo monitoramento dos processos, cabe ao CGRC garantir ações contínuas sobre os riscos identificados.

No que se refere às ferramentas utilizadas para estabelecimento dos fatores externos e internos que podem afetar a instituição, as unidades são orientadas a utilizar Análise SWOT, brainstorming, Diagrama de Ishikawa, Bow-Tie e formulário para identificação do risco. A princípio, a Análise SWOT é uma ferramenta de gestão estratégica utilizada para a geração de diagnósticos ambientais que se propõe a oportunizar a ampliação dos aspectos positivos da organização e a eliminação dos aspectos negativos. A Análise SWOT permite

que se aprenda com o presente e se reflita acerca do que pode ser feito a partir dele por meio da avaliação global das forças e fraquezas (ambiente interno) e oportunidades e ameaças (ambiente externo).

O brainstorming, também conhecido como "tempestade de ideias", é uma metodologia que propõe estimular a participação e a integração dos envolvidos de forma aberta e espontânea, objetivando estimular a criatividade em prol da solução de um problema. Enquanto isso, o Diagrama de Ishikawa mantém o seu foco como facilitador no processo de identificação dos riscos. A metodologia Ishikawa possibilita identificar e analisar as causas dos riscos e desenvolver ações para mitigar, aceitar ou até mesmo compartilhar o risco de acordo com o nível de tolerância de riscos da instituição.

Para complementar, a técnica Bow-Tie permite visualizar o relacionamento entre as causas e consequências do risco evidenciado, com a intenção de minimizar as possíveis falhas durante o processo. Essa técnica estabelece, respectivamente, o risco, as causas e suas consequências, e as medidas de controle relacionadas com cada causa e cada consequência. Por fim, a UNIFAL-MG utiliza e recomenda um formulário para identificação do risco (Figura 17) que tem por finalidade a padronização e a clareza quanto aos riscos identificados, e estabelece a concepção do risco descrito da seguinte forma: o risco; as causas do risco; a probabilidade do risco; os impactos do risco; e o proprietário do risco.

O Formulário de Identificação de Riscos tem como base a metodologia qualitativa e o propósito de facilitar a tabulação das informações. Ao final de cada formulário descritivo, será possível averiguar a probabilidade de ocorrência do risco e o nível de impacto desse risco no que se refere à etapa de planejamento e classificação dos riscos. A Figura 17 representa o formulário.

Macroprocesso/Processo/Subprocesso									
Data:									
Setor:									
Nº	Evento	Risco	Causa(s) do risco	Impacto do risco	Proprietário do risco	Grau de risco	Probabilidade de risco	Medidas mitigadoras	Responsáveis
1									

Figura 17 – Formulário de Identificação de Riscos

Vale destacar que todas as técnicas e metodologias citadas integram o treinamento realizado pela CGU (treinamento externo) e o treinamento interno realizado pela Coordenadoria de Desenvolvimento Institucional (CDI). Além disso, a CDI faz acompanhamento da gestão de riscos nas unidades institucionais por meio de formulários preenchidos, conforme exemplificado na Figura 18. É feito também um acompanhamento direto com as Pró-Reitorias e, ao final de cada Plano de Gestão de Riscos proposto pela unidade desenvolvedora, o plano deverá ser avaliado, validado e aprovado pelo CGRC.

Macroprocesso/Processo/Subprocesso										
Data:										
Setor:										
Nº	Evento	Risco	Causa(s)	Grau de risco	(*) Controles/ procedimento existente	Melhoria requerida	Prazo	Responsável	Status	Observação
1										
* Implantar/desenvolver ações que atuem nas causas dos riscos. Justificar por que deve ser adotada determinada medida.										

Figura 18 – Formulário para Monitoramento das Unidades e dos Riscos

No que se refere a planejar e classificar os riscos, a probabilidade e o impacto interferem nessas ações. A UNIFAL/MG, por meio de sua política de gestão, propõe a seguinte interpretação, conforme mostra o Quadro 18:

Quadro 18 – Probabilidade e impacto

Probabilidade	Baixa	Média	Alta
Descritores	Possibilidade de ocorrer; passível de mitigar com as estratégias já programadas.	Possibilidade de ocorrer; passível de mitigar com custos e ações adicionais.	Alta possibilidade de ocorrer; dificuldades de mitigar mesmo com recursos e ações adicionais.
Impacto	**Baixo**	**Médio**	**Alto**
Descritores	Prejuízos (ainda que reduzidos) para as metas; exige novos projetos ou ações.	Perda de capacidade de gestão; demandas adicionais de tempo e de recursos.	Graves prejuízos aos objetivos e ao cumprimento da missão institucional.

Assim, os riscos são pensados e monitorados de acordo com os resultados da etapa de classificação. Para se avaliar a probabilidade de ocorrência dos riscos e ainda os impactos destes na unidade/instituição, é proposta uma Matriz de Classificação de Riscos, conforme mostra o Quadro 19.

Quadro 19 – Matriz de Classificação de Riscos

Probabilidade		Baixa	Média	Alta
Impacto	Baixo	Baixo	Baixo	Médio
	Médio	Baixo	Médio	Alto
	Alto	Médio	Alto	Alto

A partir desta matriz, a UNIFAL-MG define os riscos que serão constantemente monitorados e as estratégias para tratamento de cada um deles. Vale destacar que, em geral, os riscos obtêm a seguinte classificação: (1) risco baixo: risco tolerável, nenhuma ação imediata é necessária, porém o risco deve ser monitorado; deve-se tratar os riscos nessa classe apenas se as restrições (como custo e esforço de tratamento) não forem significativas; (2) risco médio: situação de atenção; se possível, o risco deve ser tratado em médio prazo; o risco deve monitorado frequentemente; restrições (como custo e esforço de tratamento) podem ser consideradas para priorizar o tratamento de riscos nessa classe; (3) risco alto: risco intolerável, situação de grande preocupação; as ações devem ser tomadas rapidamente, e os resultados precisam ser monitorados de forma frequente para avaliar se a situação mudou com as ações. Os riscos devem ser tratados independentemente de restrições (como custo e esforço de tratamento).

Adiante, a etapa de monitoramento ocorrerá ao longo de um ano, a contar da data de aprovação do Plano de Gestão de Riscos. Cada responsável deverá acompanhar o comportamento dos riscos pontuados, sugerindo intervenções quando necessário. Para a materialização desse processo, a universidade objeto do estudo propõe a utilização da ferramenta 5W2H, estabelecida anteriormente pela 11ª IN nº 1, de 2016 [7], conforme o Quadro 20 a seguir:

Quadro 20 – Ferramenta 5W2H

Ferramenta 5W2H	
O quê/Como	Definição
What	O que será feito? (Ação)
Why	Por que será feito?
Who	Nome do envolvido
When	Período/Prazo
Where	Local
How	Procedimento/Forma
How Much	Valor financeiro/Tempo

Tradução livre dos autores (2018)

O monitoramento é um processo contínuo e deverá ser realizado nas operações diárias da organização. Inclui a administração e as demais atividades de supervisão bem como outras ações que os servidores executam no cumprimento de suas responsabilidades. Por último, a etapa de controle deverá ocorrer por meio da participação entre Pró-Reitorias, Unidades de Apoio, Unidade Jurídica, CDI e CGRC. É também por meio dessas diferentes unidades que se concretizam todas as formas de comunicação e/ou divulgação de novas políticas e procedimentos na instituição averiguada.

Para finalizar, a UNIFAL-MG desenvolveu uma estrutura em organograma que representa e resume todo o seu processo de elaboração de gestão de riscos. A Figura 19 retrata o processo da gestão de riscos desde o início, com a criação do CGRC. Envolve as etapas de treinamento dos servidores públicos por meio da capacitação pela CGU (capacitação externa) e pela CDI (capacitação interna) e, ainda, estabelece o cenário entre o monitoramento dos processos, a identificação dos riscos, as escolhas das ferramentas de gestão e classificação dos riscos no que se refere à probabilidade e aos impactos. Vale acrescentar que nas etapas de monitoramento e controle dos riscos a UNIFAL-MG compreende as possibilidades entre aceitar o risco, mitigá-lo ou ainda compartilhá-lo.

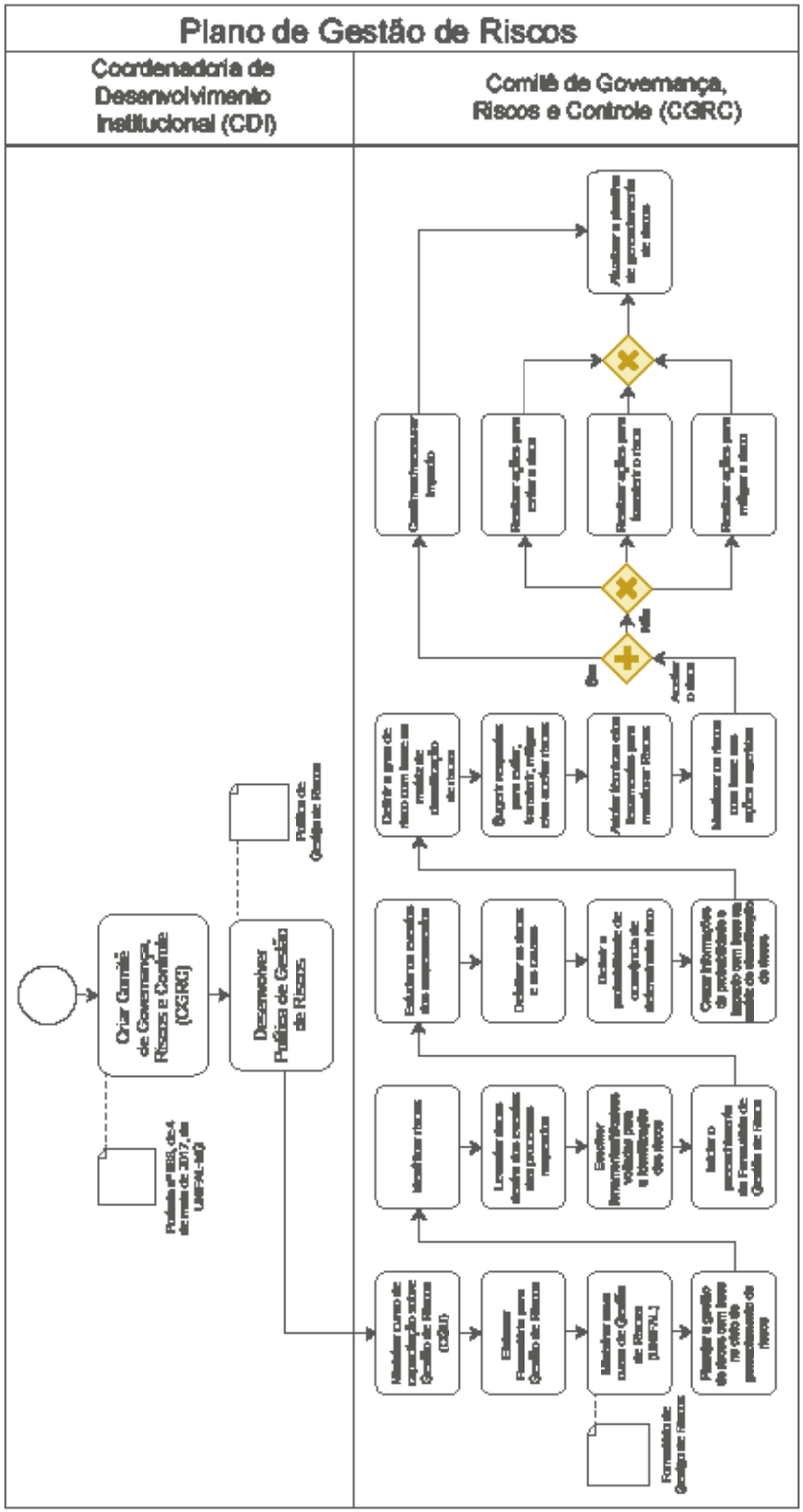


Figura 19 – Estrutura do Plano de Gestão de Riscos da UNIFAL-MG

Em tempo, torna-se importante manifestar que a UNIFAL-MG ainda não tem definido um processo de reavaliação da Política de Gestão de Riscos, o que se justifica pelo fato de sua política ainda ser recente e estar em processo de implementação. Assim, considerando-se o fato de a Política de Gestão de Riscos da UNIFAL-MG ainda identificar-se com status "em implementação", é também inviável avaliar a maturidade dessa política. Entretanto, infere-se que a gestão de riscos da instituição analisada prevê procedimentos, regras e rotinas que capacitam os seus gestores para avaliar a eficácia de suas ações e de seus planos de execução. Tem-se, por fim, a gestão de riscos da UNIFAL-MG como um processo atualizado, estruturado e desenvolvido conforme as necessidades de respostas preventivas esperadas de um processo de gerenciamento dos riscos, especialmente por se tratar de uma instituição pública de ensino.

7.5. Estudo de caso: o Centro Federal de Educação Tecnológica Celso Suckow da Fonseca – CEFET/RJ/BRASIL

Conforme a Resolução nº 44/2017, foi aprovada no dia 8 de dezembro de 2017 pelo CGRC, e promulgada pelo Conselho Diretor (CODIR) do Centro Federal de Educação Tecnológica Celso Suckow da Fonseca, a Política de Gestão de Riscos dessa instituição. A política foi elaborada pelo Departamento de Desenvolvimento Institucional, sob a coordenação da Diretoria de Gestão Estratégica, considerando a Instrução Normativa Conjunta [7] MP/CGU nº 01/2016 e a Norma ABNT NBR ISO 31000:2018, e estabelece os princípios e as diretrizes para gestão de riscos, controles internos e ações correlatas.

Ainda em estágio inicial de implementação, a política do CEFET/RJ visa desenvolver e assegurar a existência de um processo estruturado de gestão de riscos que garanta a adoção das melhores práticas aos seus processos, tecnologias e pessoas. Vale ressaltar, entre outras coisas, que essa instituição tem a premissa de alinhar a sua gestão de riscos às estratégias do PDI vigente, atendendo à sistematização e à integração dos processos organizacionais, e ao comprometimento e à tomada de decisão pelos gestores. São, portanto, objetivos da Política de Gestão de Riscos do CEFET/RJ:

I. estabelecer conceitos, diretrizes, atribuições e responsabilidades do processo de implementação da gestão de riscos;

II. orientar a identificação, a avaliação, o monitoramento e a comunicação dos riscos institucionais;

III. aumentar a probabilidade de alcance dos objetivos organizacionais, reduzindo os riscos a níveis aceitáveis; e

IV. agregar valor à organização por meio da melhoria dos processos de tomada de decisão.

O CEFET/RJ entende que a Política de Gestão de Riscos é de sua responsabilidade e, por isso, a implementação dessa política deve ser exercida de forma compartilhada pelos gestores, servidores, unidades sistêmicas, conselhos, comitês setoriais e comissões. Contudo, para fins de formulação da política, a instituição conta especificamente com o Departamento de Desenvolvimento Institucional e com o Comitê de Governança, Riscos e Controle, este último formado pela Direção-Geral (DIREG), na figura de seu diretor, e pelos demais diretores sistêmicos das seguintes diretorias: Diretoria de Ensino (DIREN), Diretoria de Pesquisa e Pós-Graduação (DIPPG), Diretoria de Extensão (DIREX), Diretoria de Administração e Planejamento (DIRAP) e Diretoria de Gestão Estratégica (DIGES).

Para a formulação e implementação da Política de Gestão de Riscos, a instituição de ensino priorizou, a princípio, a capacitação das equipes em todas as suas unidades e setores. Para essa capacitação, foi realizado um curso de gestão de riscos em parceria com o Instituto Federal do Tocantins (IFTO), além de estratégias de benchmarking para compreender profundamente a gestão de riscos nessa instituição. Dados os conhecimentos adquiridos na etapa da capacitação, foi elaborada a política da instituição pelo DEDIN, um departamento da Diretoria de Gestão Estratégica do CEFET/RJ. Uma vez formulada, a política passa por um sistema de aprovação e validação composto de três etapas: (1) validação pelo setor de auditoria interna da organização; (2) aprovação pelo Comitê de Governança, Riscos e Controles; e (3) aprovação da política pelo Conselho Diretor.

A próxima etapa refere-se à implementação da Política de Gestão de Riscos. Para tanto, o primeiro passo envolve a divulgação da política por meio da página on-line da instituição e, também, a realização de workshops sobre a gestão de riscos pelo DEDIN em todos os campi. Destaca-se que o CEFET/RJ é uma instituição multicampi, o que significa que sua estrutura está descentraliza-

da em oito campi no Estado do Rio de Janeiro. São eles: o campus Maracanã – sede da instituição – e os demais campi – Angra dos Reis, Itaguaí, Maria da Graça, Nova Friburgo, Nova Iguaçu, Petrópolis e Valença.

Dada a divulgação, foi elaborada uma planilha acessória para se definir a gestão de riscos em cada unidade institucional. Além disso, foi criado o Comitê de Desenvolvimento Institucional, responsável pela elaboração do Manual de Preenchimento da planilha e pela realização de workshop com os diferentes setores e as unidades institucionais para garantir o desempenho correto da ação. Cabe ainda ao Comitê estudar as fragilidades das planilhas finalizadas em cada unidade e aprovar a planilha. Após aprovadas pelo Comitê, as planilhas são encaminhadas para aprovação também pelo CGRC, para, posteriormente, dar-se início ao tratamento e ao controle dos riscos identificados.

De maneira geral, é possível estabelecer que as responsabilidades principais no que se refere à formulação e à implementação da Política de Gestão de Riscos do CEFET/RJ competem ao CGRC, e são elas: a) institucionalizar estruturas adequadas de gestão de riscos; b) promover o desenvolvimento contínuo dos agentes públicos e a adoção de boas práticas de gestão de riscos; c) garantir a aderência a regulamentações, leis, códigos, normas e padrões; d) aprovar diretrizes, metodologias e mecanismos para comunicar e institucionalizar a gestão de riscos; e e) emitir recomendação para aprimoramento da gestão de riscos.

No entanto, nesse processo de formulação e implantação da política, há ainda dois outros atores fundamentais: o diretor máximo do CEFET/RJ, principal responsável pelo estabelecimento da estratégia da organização e também por patrocinar a implantação da gestão de riscos; e o Comitê de Desenvolvimento Institucional, que se tornou o principal propositor das atualizações necessárias à Política de Gestão de Riscos do CEFET/RJ e quem realiza análises críticas periódicas sobre o processo de gestão de riscos por meio da DIGES, submetendo-o à Auditoria Interna (AUDIN), ao CGRC e ao Conselho Diretor (CODIR).

O estabelecimento da análise de contexto externo vem do controle realizado pelo CGRC, que, conforme mencionado anteriormente, visa garantir a aderência a regulamentações, leis, códigos, normas e padrões. Para identificação de oportunidades e ameaças, a principal metodologia descrita pela instituição foi a técnica de brainstorming, realizada pelos servidores que atuam

diretamente nos processos e registrada na planilha acessória de gestão de riscos. O objetivo da planilha é detectar, monitorar e tratar todos os riscos organizacionais identificados.

A metodologia de brainstorming é entendida pela instituição como uma ferramenta de grupo para exposição de um problema a fim de obter ideias e reflexões para resolvê-lo. É, também, uma ferramenta importante para definição das estratégias da gestão de riscos organizacionais. Somados a ela, são realizados os processos de mapeamento dos riscos, a simulação dos riscos e a identificação das vulnerabilidades. Somente após o desenrolar dessas atividades será possível estruturar o plano de ação, isto é, as ações estratégicas.

Por conseguinte, o mapeamento dos processos é uma atividade ocorrida em cada uma das unidades, coordenações, departamentos, divisões e setores, e não exclusivamente efetivada por uma equipe única. O mapeamento começa exatamente com a identificação dos processos realizados em uma área, seguido por uma etapa de priorização desses processos para detectar os mais importantes ou críticos. Toda a equipe passa por um treinamento em Bizagi, uma ferramenta utilizada para modelagem, monitoramento e controle dos processos identificados.

Dado o treinamento, os servidores encontram-se aptos a estruturar o mapeamento dos processos, o qual precisará ser validado. A validação é realizada pelo chefe do setor responsável pelo processo e, posteriormente, os processos mapeados são enviados ao DEDIN, que, após a análise, sugere uma reciclagem da equipe na ferramenta Bizagi ou divulga os processos mapeados aos departamentos institucionais. Esse processo está descrito na Figura 20 a seguir:

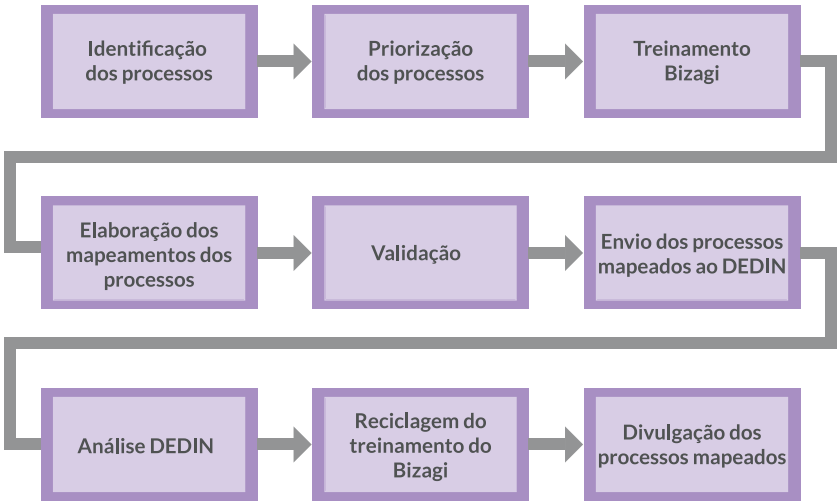


Figura 20 – Execução do mapeamento de processos no CEFET/RJ
Fonte: CEFET/RJ

Cabe ressaltar que durante a análise do DEDIN ocorre a revisão dos mapeamentos encaminhados e todos aqueles entendidos como "não processos", ou seja, que eram apenas atividades, foram retirados da análise de gestão de riscos. O CEFET/RJ entende as vulnerabilidades como a causa-raiz (nó crítico) ou as causas que aumentam a probabilidade de o risco acontecer. Notadamente, os riscos não são tratados de modo direto, mas são tratadas as vulnerabilidades (as causas e os nós críticos) que podem levar à ocorrência deles. A etapa final corresponde a um plano de ação que se desencadeia no tratamento individual pela área de cada nó crítico.

Para a realização do contexto interno, outras metodologias são utilizadas. Além da técnica de brainstorming e do mapeamento dos processos, são aplicadas a metodologia dos 5 (cinco) porquês e a 5W2H. A primeira é uma técnica para encontrar a causa-raiz de um defeito ou problema. Trata-se de uma técnica de análise que parte da premissa de que, após se perguntar cinco vezes "por que um problema está acontecendo?", sempre relacionado à causa anterior, será determinada a causa-raiz do problema. A segunda, 5W2H, vista inclusive no estudo de caso anterior, tem por finalidade compreender quem, quando, onde e como uma ação será executada, e ainda quanto custa para executar essa ação.

Cabe ser destacada a utilização da planilha acessória durante todo o mapeamento dos processos e da gestão dos riscos. Em verdade, a planilha

tem sido a base da identificação dos processos desde o princípio. Todos os macroprocessos são identificados e plotados na planilha, definindo-se o seu setor de atuação, isto é, a área em que o processo se encaixa, que pode ser administração, ensino, pesquisa, extensão ou gestão. Posteriormente, entende-se quais processos são críticos, e somente estes serão aprofundados em sua causa-raiz (vulnerabilidades). Para classificar os riscos, são propostos quatro grupos de processos – operacional, financeiro, legal ou imagem da instituição – em que será necessário estabelecer a qual desses grupos o processo pertence. Assim, o passo seguinte é a definição dos riscos, em que se pergunta: o que é risco naquele processo?

Continuamente, o CEFET/RJ analisa os riscos sob duas óticas: (1) a análise de probabilidade do risco e (2) a análise de impacto do risco. Na primeira ótica, levam-se em consideração sete fatores, explicitados no Quadro 21 abaixo:

Quadro 21 – Fatores considerados para a análise de probabilidade

Fatores	Interpretação
Ambiente Externo	Levantamento de cenários prospectivos que influenciam na concretização de perigos (criminalidade, mercados paralelos, estrutura do Judiciário, corrupção, movimento sindical, entre outros).
Ambiente Interno	Levantamento do nível de relacionamento entre os colaboradores e a alta administração, remuneração, clima organizacional, cultura organizacional, política de RH e ética.
Infraestrutura	Levantamento dos Meios Técnicos Passivos (MTP) e de recursos físicos.
Meios Organizacionais	Verificação se a organização dispõe de normas de rotinas e de emergência, políticas de tratamento de riscos e gerenciamento de riscos corporativos.
Recursos Humanos	Levantamento do nível de qualificação, quantidade e posicionamento tático da equipe.
Tecnologia da Informação (TI)	Levantamento da não existência de sistemas eletrônicos/informatizados.
Frequência/Exposição	Grau de ocorrência do "fator de risco" em cada área ou setor estudado. A frequência/exposição pode ser classificada em: muito baixa, baixa, média, alta e muito alta.

Fonte: CEFET/RJ

A segunda análise de impacto dos riscos considera os quatro grupos de processos anteriormente definidos – operacional, financeiro, legal ou imagem da instituição – e o grau de influência sobre eles. Com o objetivo de manter a significância proposta pelo CEFET/RJ, o Quadro 22 caracteriza essa classificação.

Quadro 22 – Classificação dos riscos por setor/departamento

Setor/Departamento	Interpretação
Operacional	1- Perturbações muito leves; 2- Leves; 3- Limitadas; 4- Graves; 5- Perturbações muito graves.
Financeiro	1- Insignificante; 2- Leve; 3- Moderado; 4- Severo; 5- Massivo.
Legal	1- Perturbações muito leves; 2- Leves; 3- Limitadas; 4- Graves; 5- Perturbações muito graves.
Imagem da Instituição	1- De caráter individual; 2- Local; 3- Regional; 4- De caráter nacional; 5- De caráter internacional.

Fonte: CEFET/RJ

Os resultados encontrados nas análises de probabilidade e impacto são expressos em uma matriz de riscos (Quadro 23) que deverá resultar no nível do risco. Esse nível corresponde a um resultado entre a probabilidade de o risco acontecer no departamento e o grau de impacto desse risco nas atividades desenvolvidas naquele setor. O nível do risco pode ser classificado em baixo, médio, alto e extremo e, a partir dessa definição, são formuladas e ajustadas as medidas para tratamento dos riscos por meio dos planos de ação. Nessa etapa, o registro será feito através do preenchimento do Plano de Ação na Planilha de Gestão de Riscos e busca aumentar a probabilidade de alcance dos resultados organizacionais por meio do tratamento dos riscos.

Os planos de ação visam aceitar, mitigar, evitar ou compartilhar os riscos. Aceitar o risco significa tolerá-lo; mitigar (reduzir ou modificar) o risco diz respeito a reduzir sua probabilidade e/ou impacto, trazendo-o a um nível aceitável; evitar o risco corresponde a eliminar a atividade que deu origem a ele; e, por último, compartilhar o risco com terceiros significa buscar cooperação para solucionar o problema. Além do mais, este é o momento em que se definem as respostas aos riscos por meio da execução de ações pensadas pela equipe do setor (donos do risco – isto é, diretorias sistêmicas e direção de campi), em parceria com o seu responsável para executar as ações de tratamento dos

riscos (lê-se agente do risco). São, ainda, definidos os prazos de respostas aos riscos e o total de investimento previsto em cada ação estratégica.

Quadro 23 – Matriz de Riscos Probabilidade x Impacto

Análise dos Riscos		Probabilidade				
		Muito baixa	Baixa	Média	Alta	Muito alta
Impacto	Muito alto	Alto	Alto	Alto	Extremo	Extremo
	Alto	Médio	Médio	Alto	Alto	Extremo
	Médio	Médio	Médio	Médio	Alto	Alto
	Baixo	Baixo	Médio	Médio	Médio	Alto
	Muito baixo	Baixo	Baixo	Baixo	Médio	Médio

Fonte: CEFET/RJ

As estratégias para mapeamento e tratamento dos riscos na instituição são definidas sempre pelo CGRC, o que revela que ainda não existe um processo fortemente descentralizado ou fragmentado em definições de objetivos, metas e indicadores pelas demais áreas do CEFET/RJ. Vale destacar, no entanto, que todas as ações estratégicas definidas são disseminadas nas diversas áreas por meio de reuniões, workshops, e-mails institucionais e pela página on-line da instituição. Cabe ainda apresentar que, ao longo do processo de tomada de decisão para a gestão de riscos, resumem-se cinco áreas e suas respectivas responsabilidades como fundamentais. São elas:

1. CGRC: comitê criado por meio da Portaria nº 803, de 6 de julho de 2016, tem como principal atribuição institucionalizar, promover, garantir e supervisionar a implantação e o desenvolvimento da gestão de riscos na instituição. É formado pelo diretor-geral e pelos diretores sistêmicos, sendo presidido pelo diretor-geral;

2. CODIR: comitê permanente e de natureza consultiva no apoio à gestão da Diretoria de Gestão Estratégica, tendo como uma de suas funções apoiar a implementação da gestão de riscos institucional. É formado por servidores representantes das diretorias sistêmicas e dos

campi, e atualmente é presidido pela chefe do Departamento de Desenvolvimento Institucional;

3. DIREG: responsável por presidir o CGRC e por garantir todo o apoio necessário para a implementação da gestão de riscos institucional;

4. DIGES: responsável pela implantação do mapeamento de processos e da gestão de riscos institucional; e

5. DEDIN: responsável por apoiar a Diretoria de Gestão Estratégica na implementação do mapeamento de processos e na gestão de riscos institucional.

De modo igual e geral, é possível estabelecer a gestão de riscos do CEFET/RJ em sete etapas principais, conforme ilustra a Figura 21 abaixo.

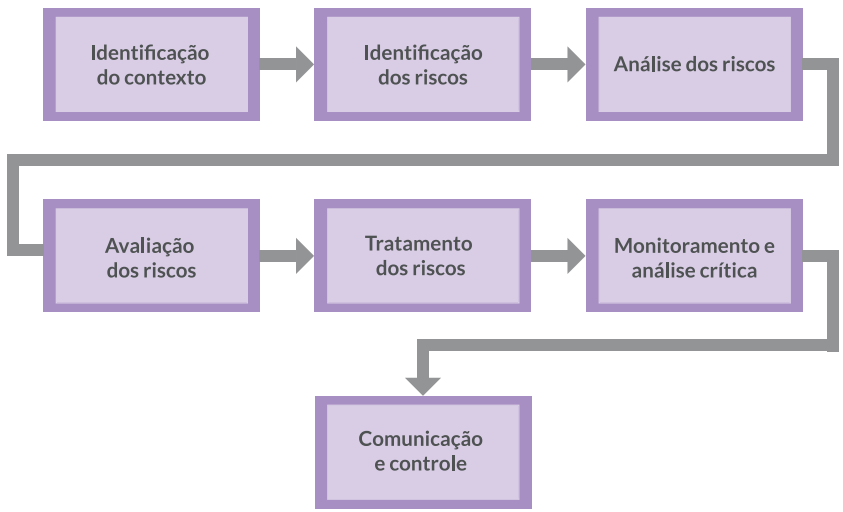


Figura 21 – Etapas da gestão de riscos no CEFET/RJ
Fonte: CEFET/RJ

Assim, entende-se que o estabelecimento do contexto, na Política de Gestão de Riscos, dispõe sobre a definição dos parâmetros externos e internos essenciais à execução de seus objetivos. Todos os níveis da organização devem ter objetivos fixados e comunicados. Deve, então, haver explicitação de objetivos claros, alinhados à missão e à visão organizacionais, e que são necessários para permitir a detecção de eventos. A identificação dos riscos envolve o reconhecimento e a descrição de eventos críticos que possam impactar na consecução dos objetivos. A análise dos riscos refere-se à determinação da

probabilidade e do impacto de eventos críticos que possam causar efeitos nos objetivos preestabelecidos.

A avaliação dos riscos tem por finalidade a análise quantitativa e qualitativa, que definirá os riscos a serem tratados e a sua ordem de priorização através do nível de risco identificado pela matriz de riscos. O tratamento dos riscos consiste na identificação e na seleção dos meios (ações) destinados a oferecer novos controles ou aprimorar os já existentes. O monitoramento e a análise crítica tratam da revisão e da análise periódica da gestão de riscos, objetivando o aprimoramento contínuo da instituição. No processo de monitoramento, deve-se acompanhar o desempenho dos indicadores de riscos, supervisionar a implantação e a manutenção dos planos de ação, e verificar o alcance das metas estabelecidas. Por fim, a comunicação e o controle constituem o fluxo de informações entre as partes envolvidas no processo de gestão de riscos a fim de assegurar a compreensão necessária à tomada de decisão envolvendo riscos e o controle da execução das ações planejadas.

Em tempo, é interessante descrever que o processo de monitoramento ocorre organizado em três dimensões. Na primeira linha de defesa, estão os departamentos, as coordenações, as seções e os agentes públicos, que têm como incumbência implementar ações preventivas para resolver deficiências em processos e controles. Na segunda linha de defesa, estão presentes o diretor-geral, os diretores sistêmicos e os diretores das unidades descentralizadas do CEFET/RJ, que têm como atribuições determinar as direções e apoiar a primeira linha. Por fim, na terceira linha de defesa, encontra-se a auditoria interna, que deve promover avaliações independentes dos controles internos.

Além disso, um aspecto relevante que vale ser também mencionado é a motivação para a gestão de riscos. Conforme apresentado na conferência FORPLAD em Natal, Rio Grande do Norte, a gestão de riscos, antes de ser concebida dessa forma, surgiu da iniciativa da DIRAP em mapear todos os processos vigentes na instituição, garantindo maior controle e eficiência sobre eles. Posteriormente, através da Portaria/CEFET/RJ nº 803, de 6 de julho de 2016 e alterações, esse projeto foi ampliado para toda a instituição, sob a coordenação da Diretoria de Gestão Estratégica (DIGES). Durante a fase de mapeamento de processos, foi identificado um total de 700 (setecentos) processos, agrupados em dois conjuntos: (1) processos por campus e (2) processos por diretorias. No mesmo período, entrou em vigor a legislação pertinente à

gestão de riscos propriamente dita, o que garantiu o encaixe dos processos de mapeamento ao contexto dessa nova legislação.

Torna-se provável relatar que o CEFET/RJ ainda não passou por uma reavaliação da sua Política de Gestão de Riscos, o que está justificado pelo fato de que o estabelecimento da sua primeira política é recente. No entanto, a instituição afirma que etapas de reavaliação da sua política serão efetivadas após um ano da vigência da atual política e/ou na implantação de um novo Plano de Desenvolvimento Institucional, assim como na realização de um Plano de Melhorias. O Plano de Melhorias refere-se aos processos de avaliação de maturidade, visto que a política de gestão dos riscos ainda está em fase de implementação, o que impede ações que meçam o seu grau de maturidade. Como recomendação, o CEFET/RJ sugere o mapeamento dos processos a fim de proporcionar uma identificação apropriada e eficaz dos riscos.

8. A metodologia ForRisco: gestão de riscos no setor público

Elaborada de forma complementar à metodologia ForPDI – Plano de Desenvolvimento Institucional [35], a metodologia ForRisco teve o apoio das Instituições Federais de Ensino Superior (IFES) pelo Fórum Nacional de Pró-Reitores de Planejamento e Administração (FORPLAD) e pela Associação Nacional dos Dirigentes das Instituições Federais de Ensino Superior (ANDIFES) do Brasil.

A metodologia ForRisco é o resultado de um projeto de pesquisa intitulado "Gestão de riscos nas universidades federais: elaboração de modelo de referência e implantação de sistema", o qual se dividiu nas cinco etapas descritas a seguir:

1. avaliação das metodologias de gestão de riscos no mercado adotadas pela AP brasileira;

2. elaboração de questionário para avaliação de maturidade das metodologias;

3. construção de uma metodologia de gestão de riscos adequada a organizações públicas e privadas, a ser publicada em formato de livro;

4. desenvolvimento de um software para apoiar os gestores na condução da gestão de riscos; e

5. capacitação presencial e on-line sobre a metodologia e a ferramenta de software ForRisco.

A primeira etapa está descrita no quarto capítulo deste livro. Para a segunda etapa, foi publicado um capítulo no livro *Lecture Notes in Business Information Processing*, da editora Springer, com o título *Perception of Enterprise Risk Management in Brazilian Higher Education Institutions*, contendo informações relevantes sobre a aplicação do questionário. A terceira etapa corresponde à construção e publicação deste livro. A quarta etapa refere-se a um software livre para executar a gestão de riscos nas organizações, apresentado no capí-

tulo 10. Já a quinta etapa diz respeito à capacitação presencial e on-line, com cursos que contemplam a metodologia e o software ForRisco.

Em sua origem, o projeto para gestão de riscos nas universidades federais busca, além da elaboração e disseminação do modelo de referência por metodologia própria, o desenvolvimento do software ForRisco, uma ferramenta de gestão de riscos que deverá suportar, diante da metodologia proposta, todos os processos para implementar, administrar, controlar e monitorar os riscos organizacionais.

A proposta ForRisco apresenta-se como um dos recursos mais atuais e promissores voltados à gestão eficiente dos riscos em organizações privadas e públicas. Primeiramente, por basear-se em renomados estudos internacionais e nacionais, a metodologia mostra-se capaz de atender a diferentes instituições e setores. Além do mais, para a sua concepção, foram levadas em consideração algumas das principais estruturas de mercado e da AP, o que reforça a capacidade da metodologia de responder às demandas de áreas e naturezas distintas.

Outro diferencial está na habilidade de integrar a metodologia e a ferramenta ForRisco em prol dos objetivos das organizações. De fato, essa integração permite alinhar os passos para condução da gestão dos riscos seguindo a lógica estrutural projetada pelo software. É relevante mencionar ainda que a metodologia ForRisco é a única que argumenta a correlação entre o desenvolvimento de políticas de gestão de riscos alinhadas com os planos de desenvolvimento institucionais.

A seguir, um esboço das etapas de execução da gestão de riscos proposto pela metodologia ForRisco bem como a descrição de cada uma delas serão apresentados.

8.1. Etapas da execução da gestão de riscos

Ao estabelecer o que se entende por etapas da execução da gestão de riscos, a metodologia ForRisco traz, no âmbito da gestão ou do gerenciamento, um processo composto de sete etapas fundamentais. São elas: (1) a definição da política; (2) o estabelecimento do contexto externo; (3) a definição da estratégia para a gestão de riscos; (4) o estabelecimento do contexto interno; (5) a realização da gestão de riscos para as atividades; (6) a reavaliação da política e o estabelecimento do nível de maturidade; e (7) a avaliação da maturidade da organização. O esquema da metodologia ForRisco está descrito na Figura 22.

Para estas etapas, sugere-se que seja interessante pensar em quais atividades são genéricas e quais são específicas para a gestão de riscos da organização e, ainda, quais são de nível macro e de nível micro. A Figura 22 contém um esquema dessa lógica:

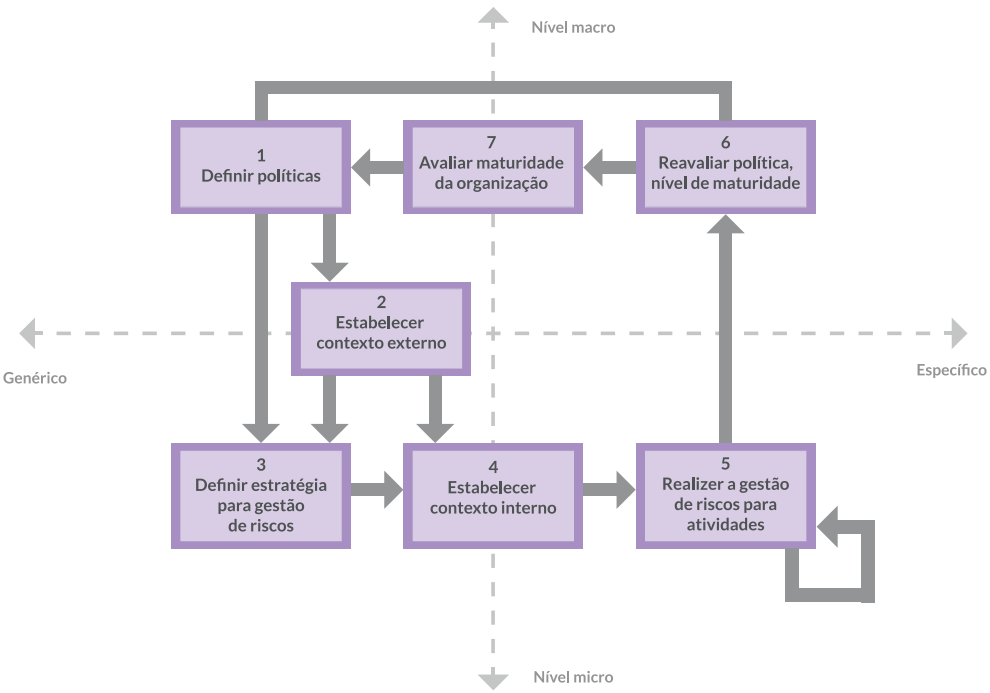


Figura 22 – Metodologia ForRisco para gestão de riscos na Administração Pública

A princípio, para estruturar cada uma das etapas em uma organização, é preciso pensar nas atividades genéricas e específicas, bem como nos níveis macro e micro dessa instituição. Entende-se por genérico o conjunto de atividades, processos, conceitos, recursos e decisões que são análogas (similares) nas áreas em um determinado órgão. Como específicos, compreende-se o mesmo conjunto de atividades, processos, conceitos, recursos e decisões que se referem exclusivamente a uma área específica no órgão ou ao próprio órgão integralmente.

Em seguida, é importante considerar de que forma as atividades, os processos, os conceitos, os recursos e as decisões podem impactar na organização. Para isso, é necessário se certificar dos níveis da organização. O nível macro

indica que toda a organização está propícia a receber ou sentir a repercussão das execuções estabelecidas por essas atividades, processos, conceitos, recursos e decisões tomadas. Ao contrário, o nível micro assinala que a repercussão de atividades, processos, conceitos, recursos e decisões será percebida somente pela área executora.

Vale destacar que, ao longo do tempo, todas as atividades refletem no contexto organizacional, no curto, médio ou longo prazos. Dessa forma, cabe à gestão de riscos possibilitar a redução dos impactos negativos das áreas, na totalidade da organização, especialmente no que se refere ao médio e ao curto prazo.

Para a metodologia ForRisco, cabem, portanto, os seguintes cenários:

- Primeiro quadrante – etapas 1, 2 e 7: são atividades que podem (ou devem) ser entendidas como genéricas e de nível macro. Isso ocorre porque são ações que envolvem a organização em seu conjunto e podem também afetar toda a organização, mesmo que no médio ou curto prazos;

- Segundo quadrante – etapas 2, 3 e 4: são atividades que podem (ou devem) ser entendidas como genéricas e de nível micro. Isto é, são atividades comuns em toda a organização, mas que são executadas também nas áreas organizacionais, refletindo os seus diferentes contextos;

- Terceiro quadrante – etapas 4 e 5: são atividades que podem (ou devem) ser entendidas como específicas e de nível micro. De fato, infere-se que cada área específica é capaz de entender o seu próprio contexto e, além disso, desempenhar todas as ações de gestão de riscos para as atividades que lhes são convenientes; e

- Quarto quadrante – etapas 6 e 7: são atividades que podem (ou devem) ser entendidas como específicas e de nível macro. Em suma, devem ser desempenhadas pelas áreas ou pela organização em seu conjunto, repercutindo de maneira genérica no contexto organizacional.

A seguir, são apresentados, um a um, os passos ou etapas globais para se conduzir a gestão de riscos nos termos da metodologia ForRisco:

1. Definir a Política de Gestão de Riscos em nível organizacional.

2. Estabelecer o contexto externo seguindo as orientações da GIRC para identificar e entender as leis e normas que formam a base para implementação de uma Política de Gestão de Riscos do órgão.

3. Com base na política e no contexto externo, definir a estratégia para a gestão de riscos contendo os papéis que formarão as linhas de defesa, treinar pessoas e disseminar a gestão de riscos. Definir estratégias é fundamental para garantir o delinear coeso entre os objetivos e os resultados esperados para os processos de negócios e para os projetos da organização.

4. Estabelecer o contexto interno significa considerar as habilidades, a capacidade, a estratégia, o contexto externo e a política da instituição. Recomenda-se concluir as tarefas da MGR-SISP no que se refere ao passo "1. Estabelecer contexto" e definir pessoas e papéis a fim de executar as tarefas recomendadas pela MGR-SISP.

5. Realizar a gestão de riscos para as atividades e ações da organização seguindo as etapas do processo apresentadas neste capítulo, contidas na Figura 25 – Etapas do processo da gestão de riscos proposto pela metodologia ForRisco.

6. Reavaliar a cada ano, ou quando necessário, a política e a legislação, de modo a estabelecer o nível de maturidade em relação aos estágios da gestão de riscos conforme mensuração de maturidade IBGC e realinhar as ações quanto à gestão de riscos na organização.

7. Avaliar a maturidade da organização segundo as orientações do IBGC e utilizar o questionário apresentado no Apêndice I.

A partir de um entendimento geral para a implantação da gestão de riscos, serão detalhados os componentes mais essenciais dessa ação. As etapas dos processos da gestão de riscos possuem quatro componentes: (1) Entradas; (2) Técnicas; (3) Objetivos, processos e tarefas; e (4) Saídas. Ao longo da execução do processo, a saída de uma etapa anterior torna-se a entrada para a etapa seguinte. Tais técnicas dão o suporte necessário para apoiar os passos e as tarefas da etapa no alcance das saídas. Cabe ressaltar que devem ser executadas atividades de mapeamento de projetos/processos antes de serem iniciadas as etapas da gestão de riscos. Para isso, recomenda-se que

sejam utilizadas as informações da metodologia GIRC. A Figura 23 representa o modelo descrito acima.

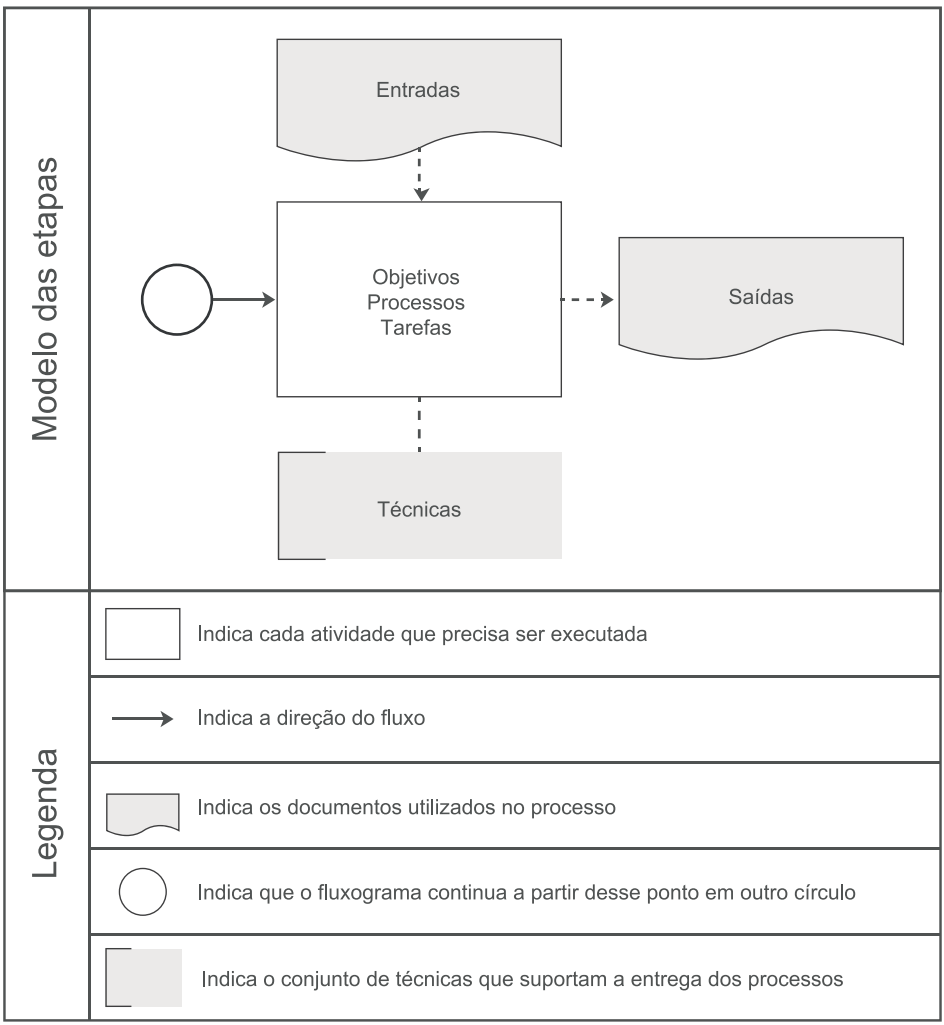


Figura 23 – Modelo das etapas de gestão de riscos da metodologia ForRisco

Em gestão de riscos, a política estabelece os princípios, as diretrizes e as responsabilidades. Com base no desenvolvimento dessa política a fim de entender e identificar os objetivos, os processos e as tarefas organizacionais, será viável utilizar um conjunto de técnicas para angariar informações importantes ao negócio e para realizar as atividades da organização. No processo da Figura 24, são sugeridas algumas técnicas, mas sempre será necessário

avaliar o que melhor se aplica para a identificação do contexto externo. Para esta etapa, serão utilizadas como entrada informações sobre regulamentações presentes em leis e normas, lições aprendidas em outras ocasiões e questões que se aplicam ao cenário. Como saída, será definida uma estratégia para conduzir as atividades da organização, aqui separadas entre projetos e processos, mas não limitadas a esses componentes.

Em seguida, para a identificação do contexto interno, será levada em consideração a estratégia de gestão de riscos anteriormente definida. Destaca-se a utilização de documentos direcionadores, tais como planos e políticas da organização, de modo a garantir o melhor entendimento do contexto interno. Cabe também relevar a utilização da matriz RACI (acrônimo dos termos *Responsible*, *Accountable*, *Consulted* e *Informed*) para reconhecimento das atribuições, tarefas e responsabilidades em determinado processo, projeto, serviço ou no contexto de departamento e organização. Sem pormenorizar, responsável (*Responsible*) é quem desenvolve a atividade; autoridade (*Accountable*) é quem aprova os produtos e as atividades entregues, e também se responsabiliza por eles; consultar (*Consulted*) significa verificar, com um tipo de consultor, o andamento do processo para agregar valor; e informar (*Informed*) é a ação de notificar todos os envolvidos/interessados.

Conforme mencionado, a metodologia ForRisco entende projetos e processos como diferentes. Quanto aos projetos, recomenda-se metodologia própria para o seu gerenciamento, mas entende-se que, ao final dos projetos, serão entregues produtos ou serviços e que, caso se tornem um serviço interno, passarão ao rol dos processos do negócio. Para esses casos, deve-se ter outro conjunto de controles adequado. A gestão de riscos nos projetos ocorre ao longo de toda a sua trajetória, envolvendo a iniciação, o planejamento, a execução, o monitoramento e controle, e o encerramento. Espera-se que a gestão de riscos contribua para as mudanças de escopo, prazo, custo, recursos e qualidade do projeto, permitindo comunicação precisa e acompanhamento quanto às restrições dos projetos. Visto que os projetos são entendidos como únicos e complexos, deve-se garantir formas de controle e monitoramento para que se acerte de primeira, evitando-se retrabalhos e custos adicionais.

Para os processos de negócio, são necessários o seu entendimento e seu controle. Processos são todas as atividades rotineiras de um departamento, divisão ou organização. Em verdade, os processos não necessariamente têm prazos para encerramento e, apesar disso, precisam ser monitorados. O mapea-

mento de processos contribui para que a informação seja disseminada de forma clara e que os participantes do processo saibam o que fazer, quando fazer, como fazer e qual é o resultado esperado para determinado processo. Contudo, como nem sempre todos os processos estão mapeados, é fundamental pensar minimamente em quais entregas estão sendo realizadas por um departamento ou divisão, o que é necessário para que ocorra a entrega e quais requisitos essas entregas precisam oferecer. Recomenda-se utilizar a técnica SIPOC (*Supplier*, *Input*, *Process*, *Output* e *Customer* – Fornecedor, Entrada, Processo, Resultado e Cliente) para se ter um melhor entendimento desses processos. Torna-se considerável manifestar que os riscos dos processos devem possuir uma estratégia própria com vistas aos resultados desses processos. Por fim, como os processos são contínuos, é preciso buscar a sua melhoria ao longo do tempo.

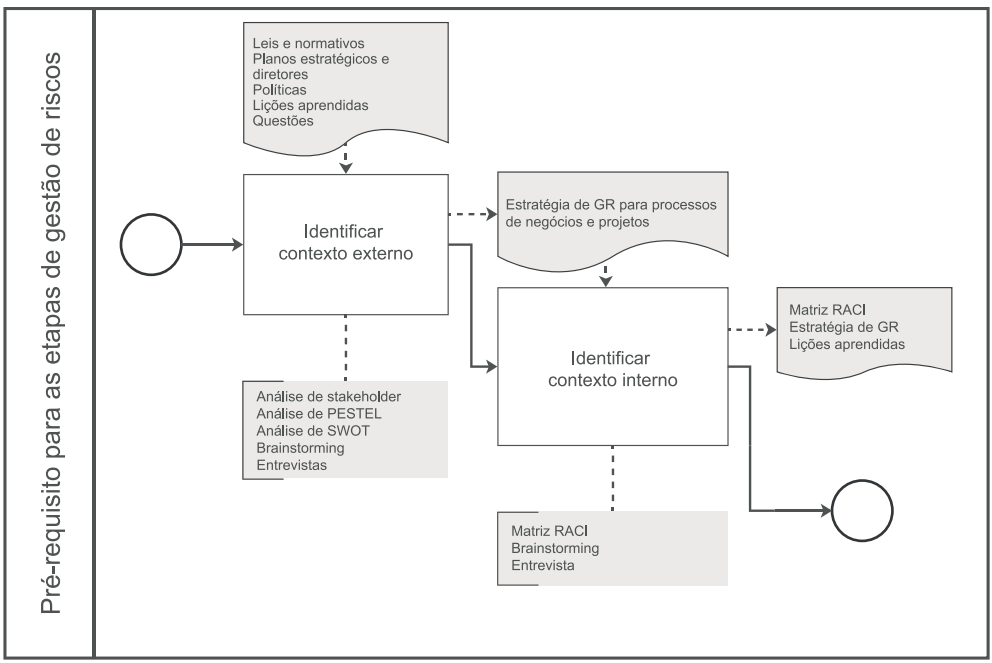


Figura 24 – Pré-requisitos para as etapas da gestão de riscos da metodologia ForRisco

Uma vez definidas as estratégias e reconhecidos os contextos externo e interno, serão iniciadas as etapas do processo de gestão de riscos, como mostra a Figura 25. Recomenda-se nesta etapa que sejam utilizadas as informações das atividades presentes na MGR-SISP. O primeiro passo desse processo é identificar e avaliar o risco e, para isso, sugerem-se como entrada as regras do órgão,

a política e a estratégia dos processos de GR, as responsabilidades dos participantes em forma de matriz RACI, as lições aprendidas, entre outras informações que auxiliem nessa identificação e avaliação. Como técnicas para executar esta etapa, propõe-se a matriz Probabilidade e Impacto, brainstorming, avaliação de impacto, probabilidade e proximidade, avaliação de valor esperado para tratamento, entre outras. Para esta etapa, a principal saída é o registro do risco, que acumulará informações ao longo de todo o processo. Também pode ser gerado um mapa de riscos e de lições aprendidas como resultado auxiliar.

Assim que o risco estiver identificado e avaliado, as informações do registro de risco serão utilizadas para o planejamento, mas nada impede que o risco seja revisitado e reavaliado de acordo com a necessidade da organização. Uma vez feito isso, haverá a garantia de que o monitoramento e o controle estejam ocorrendo. Nessa mesma linha, pode haver alterações no planejamento para o devido tratamento do risco. Os riscos podem ser acompanhados pelo mapa de riscos, apresentado na seção 4.3.1 deste livro. Vale lembrar que o mapa deve refletir a análise dos riscos para permitir uma visão holística, isto é, indicar o risco no momento anterior ao tratamento e sua situação atual.

A etapa "Planejar" usa como entrada o registro do risco já identificado e avaliado, o mapa de riscos e as lições aprendidas. Como técnica para esta etapa, deve ocorrer um planejamento de resposta ao risco, que terá como resultado a definição das pessoas (matriz RACI) e as atividades que devem ser executadas. Como saída, esta etapa deverá conter, minimamente, o dono do risco, responsável por controlá-lo e monitorá-lo, o agente do risco, responsável por executar o plano de tratamento, o registro do risco, de modo que se possa continuar acumulando informações quanto ao risco, e o plano de resposta, o qual deve conter as ações necessárias para tratar o risco.

A etapa "Implementar" será executada quando o limite de tolerância do risco alcançar um nível inaceitável ou quando o risco for materializado. Nesse caso, são utilizadas como entradas as informações do registro do risco, contendo o dono do risco, o agente do risco e a execução do plano de resposta. Como técnica de apoio, infere-se que seja atualizado o mapa de riscos, devendo-se manter atualizados o controle e o monitoramento dos riscos. Como saída, deverão ser elaborados relatórios de progresso do tratamento do risco e outros relatórios sumarizados. Esses relatórios reafirmam o interesse da organização em manter o monitoramento e o controle pelas partes interessadas.

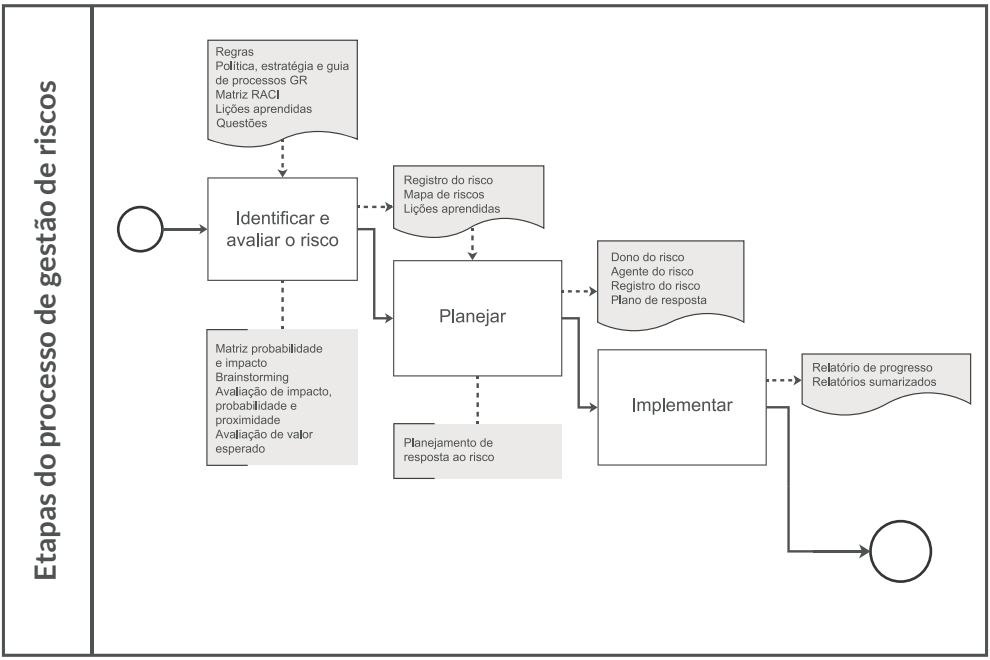


Figura 25 – Etapas do processo de gestão de riscos proposto pela metodologia ForRisco

Adiante, nas etapas para gestão de riscos da metodologia ForRisco, é preciso reconhecer o nível de maturidade. Nesse sentido, optou-se por recomendar a mensuração de maturidade no que tange aos componentes definidos na metodologia IBGC: (1) estratégias; (2) governança; (3) política; (4) processos, interação dos processos e ciclos de gestão; (5) linguagem e métodos de avaliação; (6) sistemas, dados e modelos de avaliação; e (7) cultura, comunicação e treinamento, monitoramento e melhoria contínua. Entre os níveis de maturidade definidos pela metodologia IBGC, apresentam-se as seguintes classificações: (1) inicial: uma organização que não sabe como, onde e por que implementar a gestão de riscos; (2) fragmentado: a organização sabe por onde começar, mas não sabe aonde quer chegar; (3) definido: a organização tem objetivos, metas e estratégias definidos; (4) consolidado: a organização tem objetivos, metas e estratégias definidos, implementados e monitorados; (5) otimizado: a estratégia de gestão de riscos foi revisitada e está claramente definida, implementada e integrada aos demais ciclos de gestão.

Assim, tomando-se por base a avaliação do nível de maturidade dos componentes na organização, será possível reconhecer e estabelecer a necessidade de reavaliar a Política de Gestão de Riscos. Conforme visto, a política é um dos

componentes que devem ser considerados nesta etapa e, de fato, será relevante determinar os procedimentos fundamentais para que seja efetiva aos anseios organizacionais e de seus interessados. Em consideração, o tempo é um fator significante e condicionante para a reavaliação da política. Dessa forma, a metodologia ForRisco prescreve a necessidade de reavaliar a cada ano, ou quando necessário, a política, a legislação e o nível de maturidade da organização, e realinhar as ações e práticas no que tange à gestão de riscos.

Como etapa final da gestão de riscos, a metodologia ForRisco incentiva, mais uma vez, a utilização da proposta IBGC, somada ao questionário apresentado no Apêndice I. Em suma, o questionário busca desenvolver o autoconhecimento organizacional admitindo questões específicas para a gestão de riscos e para os seus responsáveis e, ainda, coleta de informações quanto à execução do trabalho e percepções sobre a gestão de riscos pelos colaboradores. A aplicação do questionário, somada às estratégias de avaliação e mensuração da maturidade por meio da metodologia IBGC, prenuncia uma organização com resultados efetivos em sua gestão de riscos.

Por fim, por meio das etapas anteriormente descritas, defende-se a adequação ao se conduzir a gestão de riscos. Enfatiza-se que as etapas de monitoramento e controle devem ocorrer ao longo de todo o processo, mas como não possuem uma entrada específica e um resultado definido, optou-se por não descrever esses processos. O monitoramento e o controle, o registro de riscos e o relatório de progresso são componentes essenciais para que seja possível o acompanhamento adequado dos riscos identificados. Sobre a etapa de controle, de tempos em tempos – semestral ou anualmente, ou dependendo dos interesses de cada organização – devem ser realizadas 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.

Para não tornar o processo de gestão de riscos moroso, é necessário garantir que a ferramenta de registro forneça uma interface descomplicada, com informações estreitamente cruciais para a condução da gestão de riscos, mas ao mesmo tempo completa e eficaz no sentido de garantir visibilidade do estado atual do risco, sua magnitude e um histórico dos riscos. Nesse sentido, foi pensado um conjunto de variáveis para compor um formulário que permita o registro dos riscos, como apresentado no Apêndice II deste livro.

8.2. Exemplo da aplicação da metodologia ForRisco

A seguir, são apresentados dois casos práticos da aplicação da metodologia ForRisco.

8.2.1. Caso 1 – Iniciando a implantação da gestão de riscos com a metodologia ForRisco

No caso 1, os membros de uma organização estão iniciando a implantação da gestão de riscos, mas nenhuma ação foi executada até o momento. Provavelmente, o nível de maturidade quanto à gestão de riscos ainda é baixo, e é possível que os principais *stakeholders* ainda não estejam envolvidos nessas iniciativas.

Nesse cenário, é necessário que se ganhe o patrocínio da alta gestão, o qual pode ser apoiado pelas obrigações no tocante às legislações presentes no capítulo 5, que aborda as leis e normas brasileiras relacionadas à gestão de riscos.

Em seguida, deve-se oficializar, por meio de portaria ou documento equivalente, a política da gestão de riscos na organização. Após essa oficialização, é importante medir a maturidade da organização mesmo que ainda não se tenha iniciado a implantação. Isso ajuda a formar uma linha de base a fim de permitir um acompanhamento futuro de todo o processo.

Para a identificação do contexto externo, é necessário que sejam levantadas as leis, as normas e as obrigações que a instituição deve seguir. Existem casos que obedecem aos órgãos superiores ou a orientações de organismos internacionais. Essas definições de contexto externo variam de órgão para órgão, ou conforme as regras dos Estados brasileiros, ou ainda de acordo com outras definições. Com esse conjunto de informações, é possível traçar uma estratégia para a gestão de riscos que dependerá desse contexto e do tipo de risco a se enfrentar. Por exemplo: riscos de saúde serão tratados de forma diferente de riscos financeiros, ou de segurança da informação, ou de mobilidade urbana, e cada caso requer uma regulamentação própria.

A partir do momento em que já se possui uma estratégia de como tratar os riscos, os projetos e os processos passarão por análises constantes. Essas análises podem ocorrer de forma espontânea ou agendada, mantendo a finalidade da interação entre as pessoas para que possam perceber os eventos. Uma

vez identificados esses eventos que causam incertezas, é necessário registrá-los, e para isso pode-se utilizar as técnicas sugeridas. Assim que o risco for identificado, sugere-se que seja escrito na forma Causa→Risco→Consequência ou Evento→Risco→Efeito. Isso facilita a reflexão e o entendimento do cenário. Nesse momento, o registro do risco começa a ser preenchido com as informações presentes até o momento.

Com o risco registrado, será executada uma análise que detalhará a natureza desse risco para o seu melhor entendimento, de forma profunda e individual. Nesse caso, são preenchidas as informações quanto a impacto, probabilidade, proximidade e, se houver, quanto ao valor esperado para o tratamento. Tais informações ajudam a definir esse risco – diagnosticado – e permitir comparações com outros riscos a fim de tratar, em primeiro lugar, os mais urgentes. Esse processo brevemente descrito ocorre na etapa de avaliação de riscos. Em ressalva, a avaliação de riscos considera vários riscos em conjunto, apesar de avaliar individualmente cada um deles.

Uma vez avaliados os riscos, aqueles mais graves devem possuir um plano de tratamento. Quanto mais grave for o risco, melhor e mais detalhado deve ser o seu plano. Os riscos mais brandos não necessitam obrigatoriamente de planos de tratamento, já para os mais graves é mandatório que existam esses planos.

A qualquer momento que o risco se materializar ou ultrapassar o limite de tolerância, o plano de riscos deve ser implementado, sendo necessário o controle e o monitoramento desses riscos. Os riscos devem ser continuamente reavaliados a fim de permitir que o seu último estado esteja representado na ferramenta e que haja uma comunicação precisa no que tange a esses riscos. Essa reavaliação faz parte da etapa de monitoramento. Esses ciclos são iterativos e contínuos, já que os eventos acontecem em intervalos desconhecidos. No entanto, após um período de 6 meses a 1 ano, deve-se rever a política e as legislações, e reavaliar a maturidade desse período para melhorias futuras.

8.2.2. Caso 2 – Aplicando a metodologia ForRisco em uma organização que já iniciou a gestão de riscos

No caso 2, a organização já iniciou a implantação da gestão de riscos, mas ainda não tem os seus processos mapeados. Para agravar o cenário, os servi-

dores e os colaboradores estão sobrecarregados com atribuições, e há uma carência de recursos humanos e de materiais na organização.

Há conhecimento e vontade por parte da alta administração para aplicar a gestão de riscos, mas a força de trabalho para condução das atividades de riscos é escassa. Uma possível saída para esse cenário é a otimização de tempo dos envolvidos, de modo que a gestão de riscos não seja um estorvo para as equipes.

O software de gestão de riscos será de fundamental importância para automatizar notificações, lembrar prazos e datas, centralizar as informações sobre os riscos e poupar tempo dos envolvidos.

Nesse caso, os gerentes devem acompanhar com mais frequência esses riscos, acessando a ferramenta diariamente para dar os devidos andamentos. Deve-se evitar reuniões com muitos participantes, convocando-se apenas os responsáveis ou representantes. É necessário que haja uma responsabilização voltada aos participantes e uma cobrança para que deem andamento à questão dos riscos.

Mesmo sem os processos mapeados, as etapas de identificação e avaliação de riscos podem ocorrer. Essas etapas ajudarão no planejamento e no tratamento dos riscos, além de auxiliar no monitoramento e no controle.

Nesse cenário, é melhor haver um mínimo de controle e de registro do que não haver controle algum. Quando se dá mais visibilidade ao controle dos eventos e se permite uma comunicação mais eficaz, pode-se entender melhor o desempenho das equipes e solicitar apoio nas definições de relocação de pessoas e de recursos financeiros, já que se conhece o volume de trabalho.

A gestão de riscos não é a solução para todos os problemas organizacionais, mas permite que seja criada uma estrutura de registro e acompanhamento para que esses riscos sejam medidos e comunicados de forma mais precisa. Também contribui para a cultura interna quanto ao tratamento adequado de questões importantes ao negócio. Além disso, deve-se lembrar que órgãos de controle e auditoria cobrarão o desenvolvimento dessas ações e que estar em conformidade com essas orientações é de suma importância para a organização.

9. Como evoluir a gestão de riscos em uma instituição pública? Uma análise dos casos da UNIFAL-MG e CEFET/RJ à luz da metodologia ForRisco

Visando estabelecer uma apreciação da gestão de riscos atualmente desenvolvida nas IFES pesquisadas, este capítulo pretende realizar uma confrontação, isto é, um comparativo entre a realidade das organizações estudadas com o que preconizam os princípios e as etapas da metodologia ForRisco. Conforme evidenciado, a metodologia ForRisco nasceu de um projeto que tem o propósito de influenciar a gestão de riscos no setor público, especialmente na esfera da educação, onde tem ganhado apoio das IFES no Brasil. Prova disso está na possibilidade de realização dos estudos de caso na UNIFAL-MG e no CEFET/RJ, instituições reconhecidas pelo MEC e atuantes no âmbito da educação, pesquisa e extensão.

É válido ressaltar que a metodologia ForRisco objetiva tornar-se o principal modelo de referência para as instituições públicas ou privadas que desejam formular e implementar ou, ainda, otimizar os seus processos de gestão de riscos. Tomando-se como apoio, portanto, casos reais articulados em organizações públicas consolidadas, admite-se uma averiguação detalhada entre o que a proposta ForRisco sugere e como foram elaborados e implementados os processos de gestão de riscos na prática.

Para dar maior visibilidade ao que está estabelecido nas etapas da gestão de riscos na metodologia ForRisco, é importante relembrar que a metodologia designa sete etapas fundamentais: (1) definição da política; (2) estabelecimento do contexto externo; (3) definição de estratégias para a gestão de riscos; (4) estabelecimento do contexto interno; (5) realização da gestão de risco para as atividades; (6) reavaliação da política e do nível de maturidade; e (7) avaliação da maturidade da organização. Cabe destacar que a gestão de riscos é, por si, um ciclo contínuo e, em seguida, recomendam-se as etapas 6 e 7, respectivamente, a reavaliação da política e do nível de maturidade e a avaliação da maturidade da organização, de modo que o ciclo se reinicie.

A política é entendida pelo Projeto ForRisco como a direção dos rumos da gestão de riscos a ser implementada. É ela quem vai garantir a determinação

de parâmetros – externos e internos – para a plena execução das tarefas da gestão. Somente uma política estabelecida pode ser capaz de auxiliar e integrar a gestão de riscos na agenda global de qualquer instituição, por isso o seu mérito. Notadamente, tanto a UNIFAL-MG quanto o CEFET/RJ possuem uma Política de Gestão de Riscos já formulada e implementada (ou em implementação). Ambas as políticas são recentes – datam do ano de 2017 – e se institucionalizaram após a Instrução Normativa proposta pelo Governo Federal que incitava o gerenciamento de riscos nas organizações públicas.

Inicialmente, o que vale ser destacado são os diferentes âmbitos em que tais políticas foram formuladas, inclusive para atender a diferentes objetivos. A política de gestão de riscos na UNIFAL-MG vem da atuação ativa da Pró-Reitoria de Planejamento, Orçamento e Desenvolvimento Institucional em aperfeiçoar as propostas orçamentárias na instituição, bem como da iniciativa de uma administração mais moderna e sustentável. No CEFET/RJ, antes de a política ser concebida, surgiu por meio do Departamento de Administração e Planejamento a necessidade de mapeamento de todos os processos vigentes na instituição para garantir maior controle e eficiência destes. Com a vigência da legislação de risco, o processo foi adequado e mostrou-se eficiente na execução da gestão dos riscos.

No que se refere ao estabelecimento do contexto externo, a presente metodologia destaca a necessidade de identificar e compreender a legislação e as normas pertinentes à implementação de uma Política de Gestão de Riscos. O próprio livro traz uma série de leis, normas e decretos que dispõem sobre a gestão de riscos, governança e controles internos nos órgãos federais. O fato é que na UNIFAL-MG esse suporte é dado pela Procuradoria Jurídica da instituição, o que permite inferir a adequada posição da universidade no que se refere às mudanças legislativas e a seus prazos de execução. Cabe relevar que, por ter um setor específico que trata das mudanças legislativas e propõe as alterações nas políticas internas da organização, a UNIFAL-MG parece não depender de um sistema ou ferramenta para esse processo de identificação.

Para efetivação do contexto externo, o CEFET/RJ tem como órgão atuante o CGRC, e como principal ferramenta utilizada a técnica de brainstorming, que, segundo a instituição, é eficaz por garantir a participação de servidores das diferentes áreas da organização. Cabe destacar, porém, que esta não é a única função do Comitê de Governança, que deve ser o principal responsável por institucionalizar, promover, garantir e supervisionar a implementação da

Política de Gestão de Riscos na instituição. Para as duas instituições, infere-se a possibilidade de inserção de um software de gestão de riscos como garantia de maior efetividade na elaboração de contextos.

A terceira etapa prevista na metodologia ForRisco descreve a preocupação em determinar, com base na política e no contexto externo, as estratégias para a gestão de riscos, contendo os papéis que formarão as linhas de defesa dessa política, que prontamente estarão focadas nas respostas e no cumprimento das obrigações regulatórias e no planejamento da organização. Além disso, as ações estratégicas visam ao treinamento das pessoas e à disseminação da gestão de riscos com o objetivo de haver um entendimento comum e uniforme entre os entes institucionais. Tais estratégias asseguram, por último, o delinear dos objetivos e dos resultados esperados para os processos de negócio e projetos.

A gestão estratégica dos processos para formulação e implementação da política e para monitoramento e controle dos riscos na UNIFAL-MG é de responsabilidade exclusiva do CGRC. A estratégia começa, inclusive, na própria formação do Comitê, que garante a participação tanto da alta AP, na figura do reitor da universidade e dos pró-reitores, assim como de coordenadores de assuntos institucionais. É possível compreender que ser estratégico nesta instituição depende anteriormente de se estabelecer uma Política de Gestão de Riscos e de se conhecer a legislação pertinente, o que corresponde ao próprio estabelecimento do contexto externo.

É válido assegurar que "ser estratégico" não é a única função do CGRC, contudo vêm dele todas as ações estratégicas que garantem a eficácia da gestão. Por exemplo, o Comitê, além de aprovar e implementar a política de riscos, visa garantir o acesso às informações sobre os riscos aos quais a organização está exposta, aspirando, estrategicamente, a melhorias no processo de tomada de decisão e ampliação das possibilidades de alcance dos objetivos. Ademais, para a implementação da gestão de riscos, levam-se em consideração todos os objetivos, metas e indicadores previstos no Plano de Desenvolvimento Institucional da UNIFAL-MG, o que estimula a ação reflexiva em todas as áreas.

Para o CEFET/RJ, destaca-se o importante papel da DIGES por meio de um Comitê de Desenvolvimento Institucional. Apesar de também dispor de um CGRC, a DIGES é a principal responsável na instituição, por exemplo, pela realização de análises críticas periódicas nos processos de gestão de riscos. Para definição das estratégias, a metodologia mais comum é o brainstorming,

contudo é válido reconhecer que a tomada de decisão sobre as estratégias para mapeamento e tratamento dos riscos está centralizada nas mãos do CGRC.

Para o CEFET/RJ, destaca-se ainda que o seu processo de estabelecimento de contexto não ocorre em duas etapas, conforme proposto pela metodologia ForRisco. Talvez por apresentar uma Diretoria de Gestão Estratégica, a instituição não faz distinção, na prática, entre o momento de realização do contexto externo e o interno, mesmo garantindo que existem diferentes parâmetros para cada um deles. Em concordância com o que foi apresentado no estudo de caso do CEFET/RJ, o estabelecimento do contexto é a etapa inicial da gestão de risco, que dispõe, em sua política, de todos os objetivos a serem fixados e comunicados na organização.

Ao compreender o estabelecimento do contexto interno, a metodologia ForRisco pretende identificar todas as habilidades, a capacidade estratégica e as atividades desenvolvidas nas organizações. A recomendação é, a princípio, definir claramente as etapas internas da gestão de riscos, identificando os objetivos, as premissas, as restrições e o escopo dos projetos desenvolvidos. Torna-se necessário, ainda, definir os responsáveis pelas unidades da organização ou pelos projetos e atividades desenvolvidos, nesse caso os donos do risco e agentes do risco. Tais ações são importantes para assegurar a viabilidade das ações de contexto.

A UNIFAL-MG entende que a realização do contexto interno precisa ocorrer somente após a Política de Gestão de Riscos ser estabelecida e divulgada institucionalmente. Para esta universidade, apenas será possível uma identificação plena dos processos e de seus riscos quando toda a instituição tiver amplo conhecimento do que trata a gestão de riscos e das possibilidades de monitoramento, controle e tratamento destes. Além disso, utiliza-se uma série de metodologias e/ou ferramentas para a realização das atividades de contexto, tanto interno quanto externo, tais como Análise SWOT, brainstorming, Diagrama de Ishikawa, Bow-Tie e Formulário para Identificação dos Riscos. Cabe destacar que esse é um processo descentralizado realizado por cada unidade institucional, com responsabilização do dono e do agente do risco.

Para a realização do contexto interno, o CEFET/RJ utiliza outras metodologias além do brainstorming. Cabe relembrar que os contextos externo e interno são realizados numa mesma etapa, isto é, a primeira; o que difere são basicamente as metodologias e as ferramentas utilizadas em cada processo. Assim, é

comum a realização interna de contexto, nessa instituição, por meio da metodologia dos 5 porquês e da metodologia 5W2H. Acrescenta-se ao uso das metodologias apresentadas o emprego da planilha acessória, que elenca todos os aspectos relevantes para a gestão de riscos na instituição. A realização do contexto interno do CEFET/RJ também ocorre de maneira descentralizada, mas todo esse processo é suportado pelo CGRC.

A quinta etapa prevista pelo modelo de referência da metodologia ForRisco é a realização da gestão de riscos nas atividades. Este é o estágio prático da gestão de riscos, momento em que todas as atividades e ações realizadas nas organizações são identificadas, analisadas, monitoradas e tratadas quando necessário. Pode ser entendida como um ciclo permanente que monitora as tarefas, os negócios e os desempenhos com o objetivo de evitar problemas ou situações que inviabilizem o alcance dos objetivos preestabelecidos nas políticas, nos planos e nos programas institucionais.

Consoante o que foi apresentado no estudo de caso da UNIFAL-MG, o seu processo empírico de gestão de riscos ocorre por meio de cinco etapas/fases: (1) identificação dos riscos; (2) análise e avaliação dos riscos; (3) planejamento e classificação dos riscos; (4) monitoramento; e (5) controle. Em suma, identificar os riscos é o ato de mapear todos os processos e possíveis riscos que possam interferir negativamente em seu fluxo na instituição. A fase de análise objetiva trazer clareza e padronização aos riscos identificados conforme a política da universidade. O planejamento é a ação de classificar os riscos quanto à sua probabilidade de ocorrência e seus impactos. Monitorar significa que os riscos são observados continuamente ao longo das operações. O controle dos riscos é a fase final e representa o plano de ação instaurado para tratamento do risco por meio da tomada de decisão conjunta entre as Pró-Reitorias, as Unidades de Apoio, a Unidade Jurídica, a Coordenadoria de Desenvolvimento Institucional e o CGRC.

Na prática, a gestão de riscos no CEFET/RJ apresenta um processo descrito em sete etapas/fases: (1) identificação do contexto; (2) identificação dos riscos; (3) análise dos riscos; (4) avaliação dos riscos; (5) tratamento dos riscos; (6) monitoramento e análise crítica; e (7) comunicação e controle. Em resumo, a primeira etapa visa identificar questões externas e internas que afetam, direta ou indiretamente, as atividades da instituição, seguida da etapa 2, que reconhece os riscos. A terceira etapa trata sobre a determinação da probabilidade e sobre os impactos causados pelos riscos, e a avaliação dos riscos – quar-

ta etapa – tende a verificar, quanti e qualitativamente, o nível desses riscos. A quinta etapa é aquela que vai tratar os riscos de acordo com o seu grau de necessidade e, posteriormente, os riscos são monitorados a fim de se manter o aprimoramento contínuo da instituição, sendo por fim comunicados e controlados para garantir a transparência da gestão (etapas 6 e 7).

Uma vez compreendido o ciclo de um processo de gestão de riscos, a metodologia ForRisco apresenta como sexta etapa a necessidade de reavaliação da política e a identificação do seu nível de maturidade. Ressalta-se que a política deve ser revista pelo menos uma vez por ano, ou quando as instituições julgarem necessário. Além disso, identificar o nível de maturidade significa entender onde a organização está no seu processo de gestão, passando pelo nível inicial, fragmentado, definido, consolidado ou otimizado. Cabe destacar que todas essas definições estão descritas no Quadro 10 deste livro, conforme orientam as estratégias de gerenciamento dos riscos do IBGC/GRCorp.

É válido inferir que, na data de realização deste estudo, nenhuma das instituições analisadas havia completado um ano em sua Política de Gestão de Riscos, e ambas não entenderam a necessidade de reavaliação da política antes do prazo recomendado. A UNIFAL-MG estabeleceu a sua política em 4/5/2017 e previu em seu processo de gestão, controle e monitoramento dos riscos as etapas de reavaliação da política e identificação do nível de maturidade. A situação se repete no CEFET/RJ, que instituiu a sua política em 8/12/2017, data ainda mais recente, e garante as etapas de reavaliação da política e medição da maturidade da gestão na sua instituição. Depreende-se, dessa forma, que as duas instituições de ensino analisadas estão em processos de implementação de sua gestão de riscos e encontram-se no status "fragmentado" na mensuração do nível da maturidade segundo as estratégias do GRCorp.

A sétima e última etapa do processo de gestão de riscos nas organizações, proposta pela metodologia ForRisco, visa ao autoconhecimento da organização. É fundamental que todas as instituições públicas ou privadas, recém-estabelecidas ou já consolidadas, conheçam os seus processos e objetivos, bem como a sua missão. Aliás, avaliar a maturidade da organização se traduz no entendimento dos seus recursos humanos, no alinhamento dos seus objetivos estratégicos e na sua ordenação para que tenha claro "aonde a instituição quer chegar" e "como a instituição quer ser reconhecida". Ao mesmo tempo, a compreensão do amadurecimento das organizações permite a elas reconhecerem as suas fraquezas e, por consequência, os seus riscos. E, mais do que isso, a

clareza dos riscos impulsiona o seu tratamento, uma gestão mais eficiente e um alcance certeiro das oportunidades, dos objetivos e das metas organizacionais. Em tempo, nem a UNIFAL-MG nem o CEFET/RJ apresentaram uma avaliação da maturidade da sua organização.

Notadamente, é possível reconhecer o bom trabalho realizado pela UNIFAL-MG e pelo CEFET/RJ em seus processos de gestão dos riscos. Ambas as instituições pensaram e avançaram nas ações para identificar, avaliar, monitorar e controlar os riscos e, em razão disso, manifestaram a sua alta capacidade em lidar com situações adversas, problemas e vulnerabilidades em seus processos cotidianos. Desse modo, ainda que a gestão de riscos tenha sido pensada para traçar interesses, missões e objetivos diferentes, é possível reconhecer semelhanças em seus processos de gerenciamento. O Quadro 24 traz um contexto geral das etapas apresentadas nas organizações pesquisadas e a proposta ForRisco.

Quadro 24 – Confrontação entre as etapas da gestão de riscos da UNIFAL-MG e do CEFET/RJ e a metodologia ForRisco

Etapas	UNIFAL-MG	CEFET/RJ	FORRISCO
Política	Formulada como uma iniciativa de administração mais moderna e sustentável.	Formulada a partir da necessidade de mapear todos os processos vigentes na instituição para garantir maior controle e eficiência.	Entendida como a direção dos rumos da gestão de riscos a ser implementada por uma instituição. É ela quem vai garantir a determinação de parâmetros – externos e internos – para a plena execução das tarefas da gestão.
Contexto externo	O suporte é dado pela Procuradoria Jurídica da instituição, que trata das mudanças legislativas e propõe as alterações na política da organização.	Tem como órgão atuante o CGRC e utiliza a técnica de brainstorming para realização do contexto e atualização da política.	Destaca-se a necessidade de se identificar e compreender a legislação e se as normas pertinentes à implementação de uma Política de Gestão de Riscos.
Estratégias para a gestão de riscos	Atividade exclusiva do Comitê de Governança, Riscos e Controles. Ser estratégico depende de se estabelecer uma Política de Gestão de Riscos e de se conhecer a legislação pertinente.	A DIGES é a responsável pela implantação do mapeamento de processos e das estratégias para gestão de riscos.	Definir os papéis ou responsáveis que formarão as linhas de defesa para gerir os riscos, treinar pessoas e disseminar a gestão de riscos na organização.
Contexto interno	A realização do contexto interno somente deve ocorrer após uma Política de Gestão de Riscos estabelecida e divulgada institucionalmente. Utiliza determinadas metodologias e ferramentas para execução do contexto interno, entre elas: Análise SWOT, brainstorming, Diagrama de Ishikawa, Bow-Tie e Formulário para Identificação dos Riscos.	Não faz diferenciação entre os contextos externo e interno, executando-os como uma mesma etapa.	A recomendação é definir claramente as etapas internas da gestão de riscos, identificando objetivos, premissas, restrições, escopo e responsáveis pelas áreas ou pelos projetos desenvolvidos. Promove também a identificação das habilidades, da capacidade estratégica e das atividades desenvolvidas na organização.

Etapas	UNIFAL-MG	CEFET/RJ	FORRISCO
Gestão de riscos para as atividades	Ocorre por meio de cinco etapas/fases: (1) identificação dos riscos; (2) análise e avaliação dos riscos; (3) planejamento e classificação dos riscos; (4) monitoramento; e (5) controle.	Processo descrito em sete etapas/fases: (1) identificação do contexto; (2) identificação dos riscos; (3) análise dos riscos; (4) avaliação dos riscos; (5) tratamento dos riscos; (6) monitoramento e análise crítica; e (7) comunicação e controle.	Sugere a identificação e a avaliação dos riscos com base nas regras e nos procedimentos estabelecidos na política e nas ferramentas para gestão; etapa de planejamento, com o registro do risco, mapa de riscos e lições aprendidas; implementação das respostas ao risco pelos donos e pelo agente dos riscos. As etapas de monitoramento e de controle devem ocorrer ao longo de todo o processo, estabelecendo-se, portanto, como uma fase explícita no processo. Por fim, recomenda-se a elaboração de relatórios de progresso e relatórios sumarizados.
Reavaliação da política e definição do nível de maturidade	Não realizou reavaliação da política. Também não foi apresentado pela instituição o nível de maturidade definido.	Não realizou reavaliação da política. Também não foi apresentado pela instituição o nível de maturidade definido.	Ressalta que a política deve ser revisitada pelo menos uma vez por ano, ou quando da necessidade das instituições. Sobre identificar o nível de maturidade, significa entender onde a organização está no seu processo de gestão, passando pelo nível inicial, fragmentado, definido, consolidado ou otimizado.
Avaliação da maturidade da organização	Não foi apresentada pela instituição a avaliação do nível de maturidade.	Não foi apresentada pela instituição a avaliação do nível de maturidade.	Avaliar a maturidade da organização significa entender os recursos humanos, o alinhamento dos objetivos estratégicos e as perspectivas que envolvem “aonde a instituição quer chegar” e “como a instituição quer ser reconhecida”.

Percebe-se, dessa forma, que tanto a UNIFAL-MG quanto o CEFET/RJ reconhecem a necessidade de estabelecer uma Política de Gestão de Riscos que representa a pauta de todas as ações e estratégias posteriormente colocadas em prática. As duas instituições, apesar de apresentarem políticas e planos de gestão relativamente novos, deixam clara a necessidade de estabelecerem o contexto externo e interno, mesmo que seus processos sejam aplicados de forma distinta. São organizações que se conhecem, percebem os seus recursos e fazem uso deles para trabalhar de forma peculiar, própria. Revela-se, além disso, a proximidade dos seus ciclos de gestão de riscos, que, à maneira de cada instituição, contemplam basicamente as mesmas etapas de identificação de processos, análise e avaliação dos riscos, planejamento e tratamento dos riscos, e monitoramento e controle.

Por fim, entende-se a relevância e a pertinência da metodologia ForRisco em propor um pensamento estruturado, atualizado e completo para efetivação plena dos processos de gestão de riscos nas organizações públicas. A metodologia se apresenta como um instrumento inovador que visa à coerência com o que prescreve a legislação vigente sobre gestão de riscos, governança e controles internos no Brasil, e motiva as organizações na evolução dos seus processos de gestão de riscos. Além disso, é imprescindível evidenciar, subsequente a este trabalho, o desenvolvimento de software gratuito, ofertado pelo Projeto ForRisco, que traduz o alinhamento entre a fundamentação teórica apresentada neste livro e a ferramenta tecnológica que permite integralizar e operacionalizar todas as ações prováveis para o gerenciamento efetivo dos riscos.

10. O sistema de software ForRisco

Um dos principais objetivos do Projeto ForRisco era o de estabelecer, além de uma metodologia própria que embasasse e fomentasse a gestão de riscos, uma ferramenta capaz de atrelar conhecimento, inovação e praticidade para lidar com os possíveis riscos em uma organização. Para tanto, o Sistema ForRisco é uma base de código aberto para acompanhamento e gestão de riscos advindos dos processos desenvolvidos pelas instituições.

O Sistema ForRisco surgiu da necessidade de alinhar princípios teóricos e práticos para a gestão dos riscos que interferiam no planejamento estratégico das autarquias federais de ensino brasileiras. A gestão dos riscos foi uma carência reconhecida nas pesquisas desenvolvidas por um grupo de trabalho do Fórum Nacional de Pró-Reitores de Planejamento e Administração (FORPLAD), composto pela Universidade Federal de Alfenas (UNIFAL-MG), pela Universidade Federal de Lavras (UFLA), pela Universidade de Brasília (UnB) e por outras universidades participantes que auxiliaram nas discussões e na definição do software.

O principal objetivo do software ForRisco é possibilitar a aplicação de técnicas de gestão de riscos para entidades privadas e públicas, buscando aumentar o controle interno e a governança dessas instituições. Com este software, é possível organizar e planejar recursos de forma a reduzir ao mínimo possível os impactos dos riscos na instituição, utilizando-se para isso um conjunto de técnicas que visa minimizar os efeitos dos danos acidentais e direcionar o tratamento adequado aos riscos que possam causar danos ao projeto, às pessoas, ao meio ambiente e à imagem da organização.

Por meio do Sistema ForRisco, o usuário terá acesso a um conjunto de funcionalidades para garantir a gestão e o monitoramento dos riscos. Abaixo, são destacadas algumas possibilidades proporcionadas pelo software:

- 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; e

• desenvolver matriz de riscos: dispositivo para indicar, de maneira ordenada, a classificação dos riscos proposta pelo usuário a partir do grau do risco.

Além das funcionalidades em destaque, o sistema permite ainda 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. A seguir, as figuras 26, 27, 28, 29 e 30 correspondem a uma prévia apresentação do Sistema ForRisco.

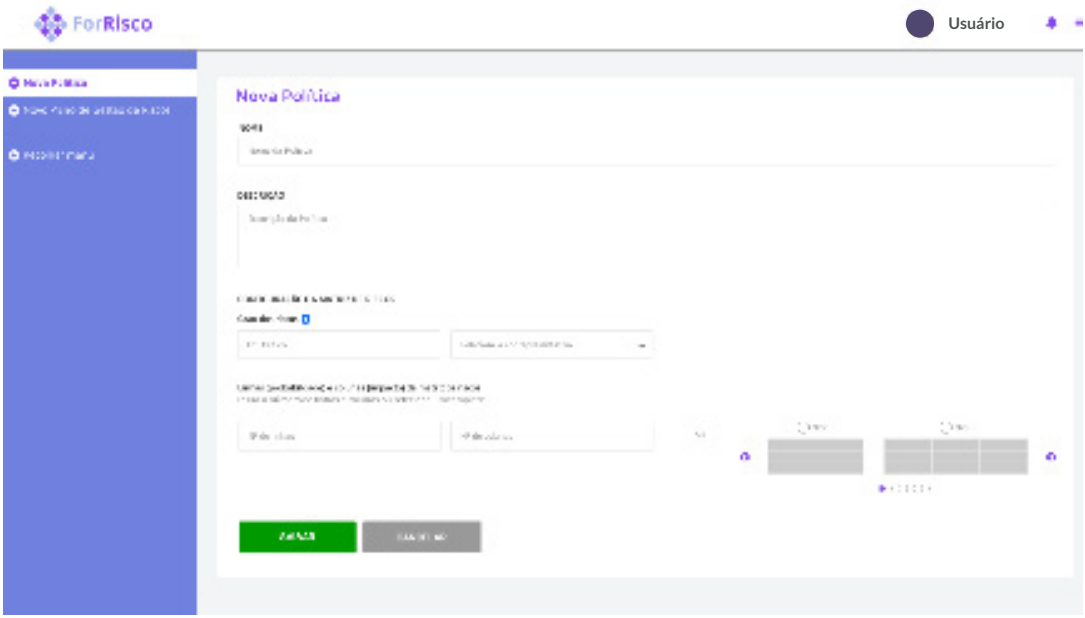


Figura 26 – Adição de nova política de gestão de riscos

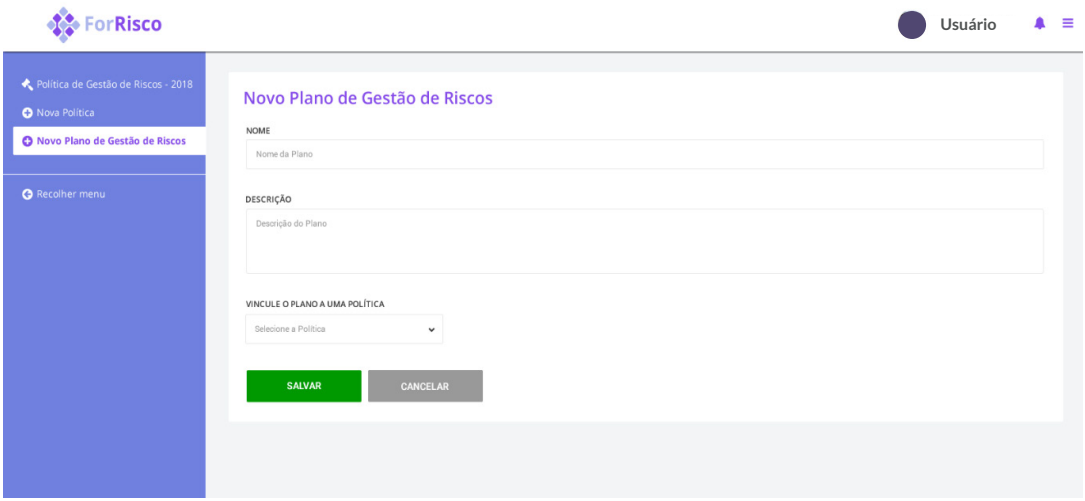


Figura 27 – Novo plano de gestão de riscos

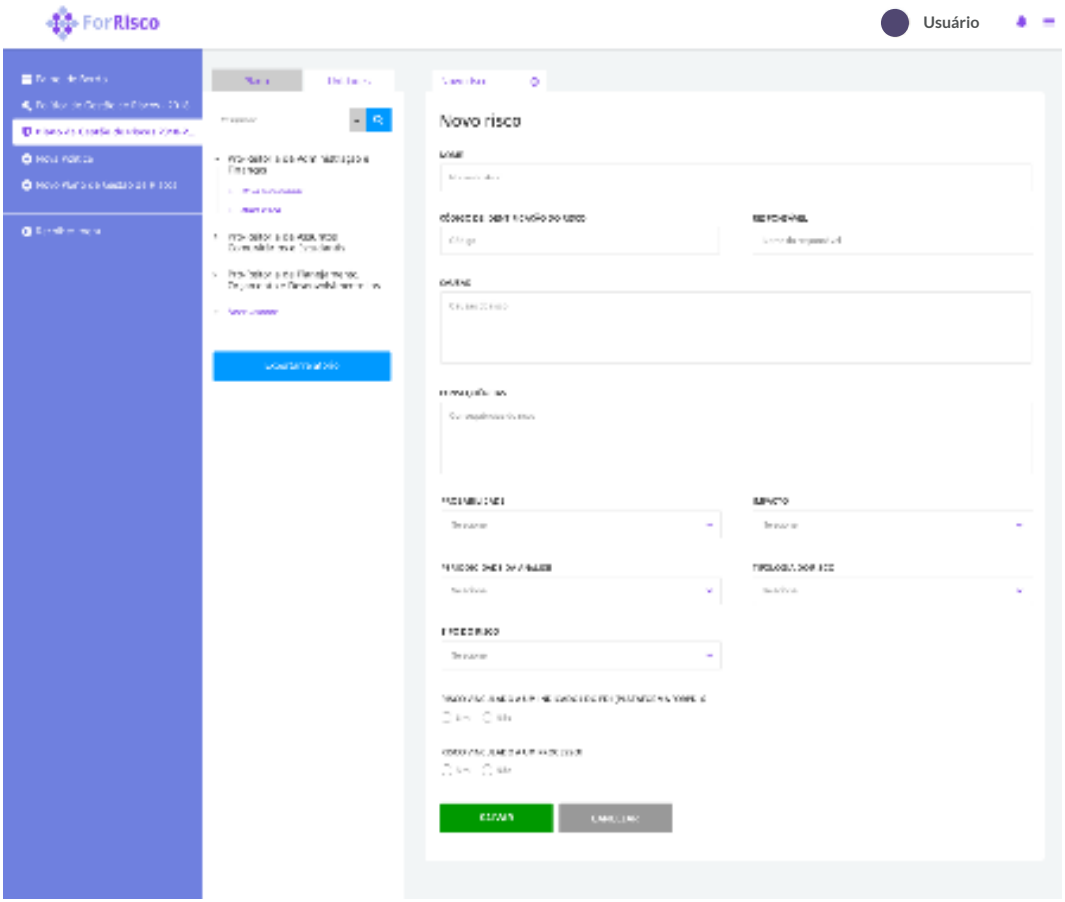


Figura 28 – Novo risco e informações do risco

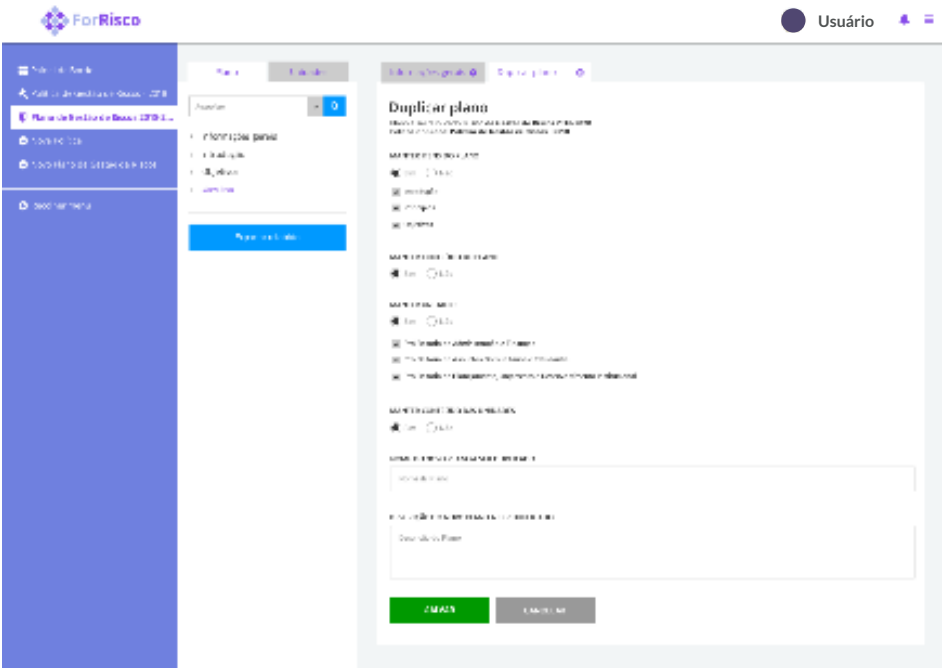


Figura 29 – Facilidade na criação de novos planos de risco: o recurso de duplicar plano

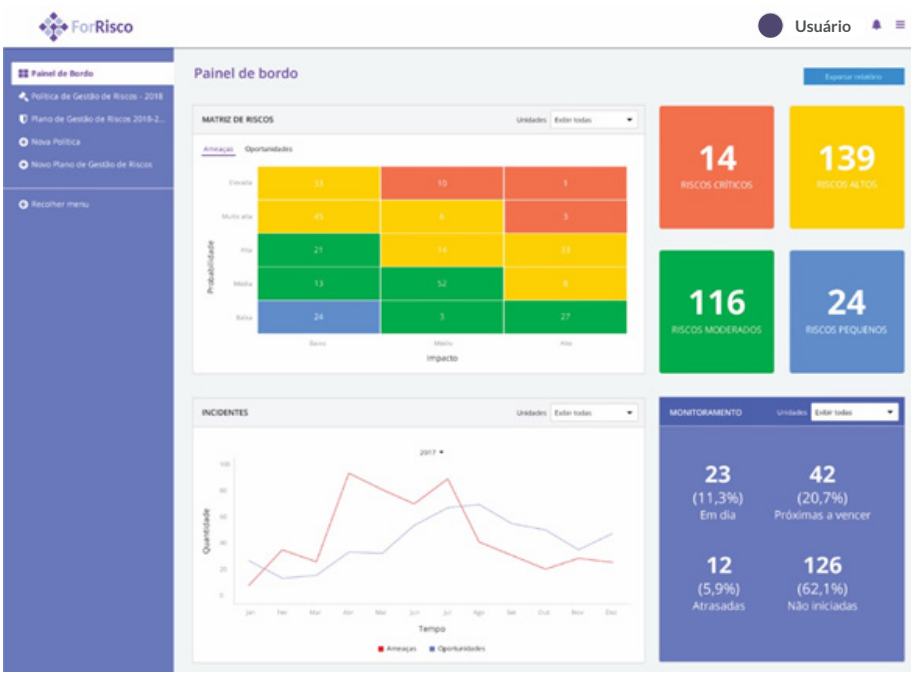


Figura 30 – Monitorando em tempo real a gestão de riscos com o Sistema ForRisco

Em síntese, as figuras representam os seguintes processos: criar e descrever uma política institucional de riscos (Figura 26); criar e descrever um Plano de Gestão de Riscos, com a possibilidade de vinculá-lo a uma política já estabelecida (Figura 27); definir o reconhecimento de um novo risco bem como codificá-lo, responsabilizar determinado usuário, indicar causas e consequências do risco, prover probabilidade de ocorrência do risco e do impacto desse risco, indicar periodicidade da análise e classificação quanto ao tipo e à tipologia do risco (Figura 28); duplicar o plano criado anteriormente, seja integralmente ou conforme o interesse do usuário (Figura 29); e visualizar o painel de bordo, o qual permite acompanhar o andamento do plano em tempo real bem como o monitoramento dos processos, incidentes e controle dos riscos (Figura 30).

Em tempo, vale destacar o alinhamento entre o sistema e a metodologia ForRisco, que, em tese, complementam-se. Conforme mostram as figuras apresentadas anteriormente, é possível reconhecer esse alinhamento, visto que o sistema viabiliza a criação de uma política de riscos e a estruturação detalhada do plano do risco por meio do estabelecimento de contextos externos e internos, causas e consequências dos riscos, definição e descrição de atividades e processos. Além disso, conforme a metodologia ForRisco propõe, o sistema torna possível estabelecer matriz de probabilidade e impacto (matriz de riscos), planejar respostas aos riscos e ações corretivas e de prevenção pela instituição ou pela unidade dona do risco, entre outras funcionalidades.

Em face do que foi apresentado, assume-se o Sistema ForRisco como a ferramenta apropriada para suportar as ações de gestão de riscos nas organizações, sejam elas de natureza privada ou pública. Cabe destacar, além da conformidade da ferramenta com os melhores sistemas ofertados tanto no mercado brasileiro quanto no internacional, e dos diversos recursos oferecidos, o caráter gratuito da ferramenta, que tem o seu código-fonte aberto assim como o manual do usuário do sistema e o curso de capacitação disponíveis no site do Projeto ForRisco.

11. Considerações finais

A gestão de riscos é uma prática constantemente recomendada por Conselhos de Administração e por governanças corporativas em todo o mundo, fato que decorre do conjunto de incertezas enfrentadas cotidianamente pelas organizações privadas e públicas. A gestão de riscos corrobora a construção de momentos reflexivos quanto às incertezas que influenciam a organização e provoca, por vezes, processos contínuos de ação. Dirimir incertezas é uma necessidade que os gestores têm para que possam entregar os objetivos e os resultados indispensáveis às organizações, e a gestão de riscos deve apoiar de modo eficiente as oportunidades de reflexão no tocante às incertezas que influenciam o funcionamento organizacional.

O momento atual é muito rico e promissor quanto ao desenvolvimento da gestão de riscos tanto no setor privado quanto no público. Em países como Inglaterra, Estados Unidos e Canadá, por exemplo, a gestão de riscos já é uma realidade na AP. No Brasil, a partir do ano de 2016, com a Instrução Normativa Conjunta CGU/MP nº 1 (2016) [7] – que dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo Federal –, entre outras leis e normas, gerenciar os riscos tem ganhado ênfase nas instituições. Decerto, boa parte dessa exaltação do tema decorre das legislações pertinentes, que passaram a se preocupar com a regulamentação dos processos de gestão de riscos, em especial das organizações que participam da esfera pública, o que traz a generalidade envolvendo tais processos.

É relevante mencionar que os estudos contemporâneos sobre metodologias de gestão de riscos, ferramentas e softwares, bem como outras publicações diversas sobre o tema, têm buscado atender a esta nova necessidade: alterar a cultura dos riscos nas organizações envolvendo todos os níveis da estrutura organizacional, de modo que reflitam sobre os empecilhos e as dificuldades na execução das atividades e sobre as possíveis consequências disso. No âmbito da AP, é possível inferir que são cada vez mais comuns técnicas de gestão de riscos incorporadas nessas organizações com a finalidade de aumentar o controle interno, a governança e o alcance eficaz dos objetivos e dos resultados esperados.

Entre os principais objetivos propostos e alcançados, pode-se inferir o empenho da pesquisa em avaliar as metodologias de mais destaque atual-

mente disponíveis sobre gestão de riscos tanto no mercado quanto aquelas adotadas no setor público. Para fins didáticos, as principais metodologias encontradas foram distinguidas em dois agrupamentos: (1) metodologias de mercado: ERM–COSO – também amplamente adotada pela AP – e ISO 31000 e M_o_R-OGC – metodologias recorrentes em organizações públicas e privadas de diversos países; e (2) metodologias da AP: GIRC, SISP – MGR-SISP e IBGC. Adicionalmente, ressalta-se que a avaliação dos softwares de gestão de riscos contribuiu para a percepção dos principais atributos em sistemas de informação que suportam a gestão de riscos.

Entre outros pontos importantes, destacam-se: um capítulo dedicado a estabelecer as leis e as normas que regulamentam os procedimentos para a gestão dos riscos; a identificação de um número significativo de ferramentas e técnicas utilizadas para a implementação e execução da gestão de riscos nas organizações; e a própria metodologia ForRisco, que visa difundir a importância da construção coesa das etapas do gerenciamento de riscos. Além disso, distingue-se o Sistema ForRisco, que possibilita a aplicação de técnicas de gestão de riscos e a administração e o planejamento dos recursos, de forma a reduzir os impactos dos riscos nas organizações.

Quanto à realização dos estudos de caso, a UNIFAL-MG e o CEFET/RJ mostraram, por meio de seus processos de gerenciamento de riscos, a necessidade e a importância do estabelecimento da gestão de riscos de modo racional, tencionada a compreender os objetivos e as peculiaridades de suas instituições. Ao mesmo tempo, foi possível perceber processos semelhantes na execução da gestão de riscos nas instituições pesquisadas, o que eleva a pertinência da metodologia ForRisco ao se propor uma reflexão estruturada em etapas para cumprimento dos requisitos e dos dispositivos legais da gestão dos riscos.

Conhecer os riscos significa identificar ameaças às quais a organização está exposta, mas, além disso, significa também perceber oportunidades. Em vista disso, o gerenciamento dos riscos visa contribuir para melhorar o desempenho organizacional ao permitir controles e acompanhamentos sistêmicos desses riscos. Cabe, então, destacar que este também é um dos objetivos da metodologia e do Sistema ForRisco, que, constituídos a partir do projeto "Gestão de riscos nas universidades federais: elaboração de modelo de referência e implantação de sistema", têm a missão de apoiar as organizações na implantação dos processos de gestão de riscos.

Para a realização de trabalhos futuros, recomenda-se que seja avaliado o desempenho das organizações antes e após a aplicação da metodologia e/ou Sistema ForRisco, bem como seja feita uma avaliação entre as organizações que adotaram diferentes metodologias a fim de medir as suas respectivas performances. Os fatores-chave de sucesso identificados nessas avaliações permitirão uma evolução tanto dos produtos ForRisco quanto das próprias organizações ao garantir etapas de reflexão e aprendizagem no contexto organizacional e, por consequência, maior assertividade em futuras implementações. Finalmente, o que se espera por meio da gestão de riscos é mais valor agregado às organizações, resultando em melhorias na entrega de seus produtos e serviços finais.

Referências bibliográficas

1. Miles RE, Snow CC, Meyer AD, Coleman HJ (1978) Organizational Strategy, Structure, and Process. Acad Manag Rev 3:546–562. doi: 10.5465/AMR.1978.4305755.

2. Rainey HG, Backoff RW, Levine CH (1976) Comparing Public and Private Organizations. Public Adm Rev 36:233–244. doi: 10.2307/975145.

3. Boyne GA (2002) Public and private management: what's the difference? J Manag Stud 39:97–122. doi: 10.1111/1467-6486.00284.

4. Hvidman U, Andersen SC (2014) Impact of performance management in public and private organizations. J Public Adm Res Theory 24:35–58. doi: 10.1093/jopart/mut019.

5. Murray MA (1975) Comparing Public and Private Management: An Exploratory Essay. Public Adm Rev 35:364–371.

6. ABNT (2018) ABNT NBR ISO 31000: 2018. Gestão de Riscos - Diretrizes. Associação Brasileira de Normas Técnicas, segunda edição, p. 17.

7. Brasil (2016) Instrução Normativa nº 01/2016. Ministério do Planejamento Orçamento e Gestão, Controladoria Geral da União, Brasília, DF.

8. COSO (2004) Enterprise Risk Management: Integrated Framework. 136.

9. Brasil (2017) Manual de gestão de integridade, riscos e controles internos da gestão - GIRC, 1.2. Ministério do Planejamento, Desenvolvimento e Gestão, Brasília, DF.

10. Brasil (2016) Metodologia de Gestão de Riscos de Segurança da Informação e Comunicações do Sistema de Administração dos Recursos de Tecnologia da Informação do Poder Executivo Federal - MGR-SISP, 2a. ed. Ministério do Planejamento, Desenvolvimento e Gestão, Brasília, DF.

11. Power M (2009) The risk management of nothing. Accounting, Organ Soc 34:849–855. doi: 10.1016/j.aos.2009.06.001.

12. Power M (2004) The risk management of everything. J Risk Financ 5:58–65. doi: 10.1108/eb023001.

13. Schiller F, Prpich G (2014) Learning to organise risk management in organisations: what future for enterprise risk management? J Risk Res 17:999–1017. doi: 10.1080/13669877.2013.841725.

14. Ferreira ABH (1986) Novo dicionário da língua portuguesa. 2a. ed. Rio de Janeiro: Nova Fronteira, p. 726.

15. Brasil (2014) Governança Pública: referencial básico de governança aplicável a órgãos e entidades da administração pública e ações indutoras de melhoria. Tribunal de Contas da União – Brasília: TCU, Secretaria de Planejamento, Governança e Gestão, p. 96.

16. IBGC (2017) Gerenciamento de Riscos Corporativos: Evolução em Governança e Estratégia. IBGC, São Paulo.

17. Andersen TJ (2010) Combining central planning and decentralization to enhance effective risk management outcomes. Risk Manag 12:101–115. doi: 10.1057/rm.2009.13.

18. HM Treasury (2009) Risk Management assessment framework: a tool for departments. 38.

19. U.S. (2016) Risk Management. United States - Government Accountability Office. Homeland Security. on-line.

20. Canada (2010) Framework for the Management of Risk. Treasury Board of Canada Secretariat. 10.

21. Brasil (2013) Gestão de riscos de segurança da informação e comunicações - GRSIC, 1a. ed. Presidência da República - Gabinete de Segurança Institucional - Departamento de Segurança da Informação e Comunicações, Brasília, DF.

22. Hillson D (2016) The Risk Management Handbook: A practical guide to managing the multiple dimensions of risk. KoganPage, London.

23. COSO (2017) Enterprise Risk Management. Integrating with Strategy and Performance. Committee of Sponsoring Organizations of the Treadway Commission: p. 202.

24. ABNT (2012) ABNT NBR ISO 31010 Gestão de Riscos - Técnicas para o processo de avaliação de riscos. Associação Brasileira de Normas Técnicas.

25. OGC (2010) Management of Risk : Guidance for Practitioners. Office of Government Commerce - Axelos, London.

26. Brasil (2017) Manual de gestão de integridade, riscos e controles internos da gestão - GIRC, 1.2. Ministério do Planejamento, Desenvolvimento e Gestão, Brasília, DF.

27. Keeling R (2002) Gestão de projetos: uma abordagem global. São Paulo: Saraiva.

28. Brasil (2016) A análise de cenários e o planejamento estratégico. Portal da estratégia - Secretaria de Política e Integração. Ministério dos Transportes, Portos e Aviação Civil.

29. Miranda RFA (2017) Implementando a gestão de riscos no setor público. Belo Horizonte: Fórum, p. 181.

30. Michel MH (2009) Metodologia e pesquisa científica em ciências sociais. São Paulo: Atlas.

31. Gil AC (2009) Estudo de caso. São Paulo: Atlas.

32. Creswell JW (2010) Projeto de pesquisa: métodos qualitativo, quantitativo e misto. Porto Alegre: Bookman: Artmed.

33. Yin RK (2016) Pesquisa qualitativa do início ao fim. Porto Alegre: Penso.

34. Cauchick Miguel PA (2007) Estudo de caso na engenharia de produção: estruturação e recomendações para sua condução. Production, 17(1), 216-229.

35. Sant'Ana TD et al. (2017) Plano de desenvolvimento institucional – PDI: um guia de conhecimentos para as Instituições Federais de Ensino. Livro Eletrônico - E-BOOK.

Apêndice I - Questionário

Elaborou-se um questionário para medir o nível de maturidade e aderência às práticas de gestão de riscos nas organizações, o qual foi dividido em quatro etapas:

1. Identificação do respondente – o responsável pela gestão de riscos, e nesse caso desejava-se coletar informações quanto à gestão de riscos; ou um participante que não era responsável pela gestão de riscos na organização, e nesse caso desejava-se coletar a percepção quanto à gestão de riscos;

2. Aplicação das perguntas específicas sobre gestão de riscos – respondidas pelos responsáveis de gestão de riscos;

3. Coleta de informações organizacionais – quanto à execução do trabalho e às percepções sobre a gestão de riscos de todos os colaboradores;

4. Coleta de informações dos respondentes – como, por exemplo, o contato (e-mail, telefone) para receber os resultados das análises.

Prezado(a) Sr.(a),

A gestão de riscos organizacionais é uma forma/processo para apoiar gestores no alcance dos objetivos de uma organização. Para a Administração Pública, as práticas relacionadas à gestão de riscos estão definidas na Instrução Normativa Conjunta MP/CGU nº 01/2016, que completou um ano de vigência em 10/5/2017.

Este questionário integra o projeto desenvolvido pelo Núcleo de P&D para Excelência e Transformação do Setor Público (NExT/UnB) a pedido do Fórum Nacional de Pró-Reitores de Planejamento e Administração das Instituições Federais de Ensino Superior (FORPLAD/IFES), com o apoio da Associação Nacional dos Dirigentes das Instituições Federais de Ensino Superior (ANDIFES), do Conselho Nacional das Instituições da Rede Federal de Educação Profissional, Científica e Tecnológica (CONIF) e da Secretaria de Educação Profissional e Tecnológica (SETEC/MEC). Com isso, esta pesquisa visa realizar uma avaliação independente sobre gestão de riscos organizacionais nas instituições federais de ensino e demais órgãos da Administração Pública.

Solicitamos a sua cordial participação no sentido de responder ao questionário apresentado a seguir. Pedimos que registre as suas respostas com o máximo rigor e veracidade. O tempo estimado de resposta é 20 minutos.

A sua participação será de grande importância para a construção e disseminação de conhecimentos sobre níveis de eficácia de práticas de gestão de riscos no serviço público.

Os questionários preenchidos e enviados até 20/6/2017 serão considerados parte das análises do projeto e receberão uma resposta quanto ao nível de maturidade de gestão de riscos da organização comparado com a média dos demais participantes.

Para receber os resultados desta pesquisa, informe o seu e-mail ao final do preenchimento do questionário. Os resultados serão divulgados sem identificação dos respondentes.

Cordialmente,
Coordenação do Projeto ForRisco (NExT/UnB)

1. Questões preliminares
Esta seção contém questões para definir o perfil do respondente.

Pergunta	Opções de resposta
1. Sua instituição já definiu um comitê e/ou os responsáveis pela gestão de riscos?	Sim, Não, Não sei responder.
2. Você faz parte deste comitê e/ou é responsável pela gestão de riscos na sua instituição?	Sim, Não.

2. Questões sobre a gestão de riscos corporativos
Esta seção contém questões quanto à gestão de riscos corporativos.
Para estas questões, informe a situação atual de sua organização, variando entre "Sim, totalmente", "Sim, parcialmente", "Sim, minimamente" e "Não, ausente". Caso o item não seja aplicável ao seu ambiente ou você não deseje responder ao item, marque a opção "N/A (Não aplicável)/Não desejo responder".

Princípios	Item
Alinhamento da gestão de riscos da sua instituição quanto aos seus objetivos estratégicos	Os objetivos da organização ou das atividades em análise foram claramente documentados antes da identificação de riscos?
	A análise de riscos foi conduzida levando em consideração os objetivos da organização e os objetivos da atividade?
	Os objetivos da organização são revisados quando novos riscos são identificados?
	As mudanças nos objetivos são consideradas e refletidas em mudanças da política e da estratégia de riscos?
Adequação da gestão de riscos ao contexto da instituição	Foram conduzidas análises externas ao ambiente da organização, projetos, programa ou operação (ex.: utilizando PESTEL, análise de *stakeholder*, técnica de brainstorming, planejamento de cenários, SWOT)?
	Utiliza-se um processo claramente definido para monitoramento e reavaliação do contexto de risco?
	Utiliza-se uma definição preliminar de quem (departamento/unidade) será o dono de certas categorias de risco num primeiro momento?
	Utiliza-se uma política de gerenciamento de riscos que descreve explicitamente como o risco intervém no contexto organizacional (abrangente, pertinente, viável, seguida)?
Envolvimento das partes interessadas da sua instituição na gestão de riscos	No processo de identificação de risco, são considerados a percepção das partes interessadas, as suas atitudes e os comportamentos?
	A aceitação dos níveis de riscos é debatida ou negociada com as partes interessadas de forma apropriada?
	Utiliza-se atualmente algum mecanismo de fundo de reserva (financeiro) para os níveis de risco acordados?
	A organização estabelece formalmente um registro sobre como evitar a atenuação (subavaliação) de riscos de alto impacto/probabilidade, ou exagero (superavaliação) de riscos de baixo impacto/probabilidade?
Existência de um processo de gestão de riscos bem definido	Utiliza-se uma política de gerenciamento de riscos para a organização em questão?
	Utilizam-se ferramentas e técnicas disponíveis e apropriadas para o gerenciamento de riscos?
	Utiliza-se um canal formalizado para atribuir à alta gestão a responsabilidade dos riscos que excederem a tolerância?
	Utiliza-se uma comunicação formal, por parte da alta gestão, para todos os principais envolvidos da instituição sobre as suas responsabilidades de gerenciamento de riscos?

Tomada de decisão baseada em informações resultantes da gestão de riscos	Os indicadores são regularmente examinados por tomadores de decisão para realizar ações corretivas?
	Utiliza-se uma rotina definida para gerar relatórios periódicos sobre como está sendo realizada a gestão de riscos na sua instituição?
	A alta gestão avalia regularmente o mapa de riscos e implicações financeiras na sua instituição, seus programas, seus projetos ou suas unidades operacionais?
	O nível de resposta ao risco é comensurável (proporcional, adequado) com o nível de risco (ex.: riscos altos possuem ações mais bem elaboradas)?
Facilitação para realização de melhorias contínuas	Existe uma pessoa ou time responsável para melhorar o gerenciamento de riscos na sua instituição, seus programas, seus projetos ou suas operações?
	As práticas são revisadas com base em modelos de maturidade para determinar o nível atingido (atual/presente) e os benefícios correspondentes que podem ser esperados (futuro)?
	A efetividade das respostas aos riscos é monitorada e revisada?
	Utiliza-se um formato, uma estrutura e um conteúdo definidos para apresentar ações de revisão quanto ao tratamento de riscos?
Criação de uma cultura colaborativa quanto à gestão de riscos	A boa gerência de riscos é estimulada pela alta gestão e reconhecida com algum tipo de estímulo/recompensa?
	Utiliza-se um processo de orientação, indução e treinamento sobre gestão de riscos para seus colaboradores, incluindo a alta gestão?
	Boas práticas de gestão de riscos são compartilhadas na instituição com regularidade?
	A alta gestão incentiva um clima de confiança para que os riscos possam ser abertamente discutidos e compartilhados sem temor?
Obtenção de valores mensuráveis associados à gestão de riscos	Utilizam-se medições associadas ao desempenho de gerenciamento de riscos?
	Utiliza-se uma análise de tendências elaborada a partir da gestão de riscos?
	Há evidências de gerenciamento utilizando os dados da análise de tendência para direcionar melhorias futuras?
	A instituição pode demonstrar o retorno de investimento obtido com o desenvolvimento da gestão de riscos?

Esta seção possui perguntas abertas sobre as metodologias de gestão de riscos adotadas e uma escala de 1 (Mais baixa) a 5 (Mais alta) contendo a frequência com que a mão de obra externa é contratada.

Pergunta	Tipo de resposta
Indique quais são as metodologias, as técnicas ou os artefatos de gestão de riscos utilizados pela sua instituição.	Resposta aberta
Com que frequência auditores externos e/ou consultores externos contribuem para gerenciar os riscos da sua instituição?	Escala de 1 a 5

3. Questões sobre a organização e os colaboradores

Esta seção contém perguntas referentes à sua instituição e aos seus colaboradores.

Afirmativa/ Questão	Item	Tipo de resposta
Indique o seu grau de concordância com as sentenças a seguir:	A missão, a visão e os valores da minha instituição são formulados de maneira clara, sem ambiguidade.	Discordo totalmente; Discordo parcialmente; Nem concordo nem discordo; Concordo parcialmente; Concordo totalmente; N/A/Não desejo responder
	A missão, a visão e os valores da minha instituição são formalizados e comunicados interna e externamente.	
	A soma das metas a serem atingidas reflete os resultados que a organização deseja alcançar.	
	As medidas de desempenho para a minha instituição estão relacionadas com os seus objetivos de forma clara.	
Indique o nível de sua influência nas decisões da alta gestão de sua instituição.	Decisões estratégicas (por exemplo, desenvolvimento de novos produtos ou serviços, desinvestimento de produtos e/ou serviços específicos, estratégias da sua unidade).	Eu possuo toda influência; Eu possuo influência parcial; Nem eu nem meu superior possuímos influência; Meu superior possui influência parcial; Meu superior possui toda influência; N/A/Não desejo responder
	Decisões de investimento (por exemplo, mudar para um novo edifício, renovar edifícios, estradas ou outros bens, comprar e implementar novos sistemas de informação).	
	Decisões sobre processos internos (determinação de orçamentos de projetos, definição de prioridades, contratos com fornecedores externos).	
	Decisões relativas às estruturas organizacionais (alteração das estruturas de informação, contratação/demissão de pessoal, compensação, perfis de competências e carreiras profissionais, alteração das estruturas dos comitês).	

Em que grau você concorda com as afirmações seguintes sobre as medidas de desempenho da sua instituição?	Minha instituição possui medidas de desempenho que indicam a quantidade de produtos ou serviços fornecidos.	Discordo totalmente; Discordo parcialmente; Nem concordo nem discordo; Concordo parcialmente; Concordo totalmente; N/A/Não desejo responder
	Minha instituição possui medidas de desempenho que indicam como está a eficiência operacional.	
	Minha instituição possui medidas de desempenho que indicam a satisfação do público atendido.	
	Minha instituição possui medidas de desempenho que indicam a efetividade dos seus resultados.	
Qual é a importância das métricas de desempenho seguintes para a sua remuneração total (ex.: carreira, salário, etc.)?	A importância das "métricas de quantidade" na minha instituição é...	Completamente irrelevante; Pouco relevante; Moderadamente relevante; Importante; Muito importante; N/A/ Não desejo responder
	A importância das "métricas de eficiência" na minha instituição é...	
	A importância das "métricas de satisfação do público atendido" na minha instituição é...	
	A importância das "métricas de resultado" na minha instituição é...	
Compare o desempenho da sua instituição com outras similares (ou compatíveis) nos seguintes itens:	Na quantidade ou montante de trabalho produzido.	Muito abaixo da média; Abaixo da média; Na média; Acima da média; Muito acima da média; N/A/Não desejo responder
	No alcance das metas de produção e de serviço.	
	Na qualidade ou precisão do trabalho produzido.	
	No número de inovações ou ideias novas geradas pelas unidades.	
	Na eficiência da operação.	
	Na reputação no tocante à excelência no trabalho.	
	Na conduta moral dos colaboradores.	

Esta seção contém questões abertas quanto à percepção de riscos dos respondentes.

Pergunta	Tipo de resposta
Justifique a importância da gestão de riscos para a obtenção de resultados pela sua instituição.	Resposta aberta
Na sua percepção, quais são os principais desafios, as dificuldades e as limitações para implantação e realização efetivas da gestão de riscos na instituição?	Resposta aberta

4. Identificação do respondente

Questão	Tipo de resposta
Gênero	Masculino; Feminino; Outro (especifique)
Qual a sua idade (anos)?	De 1 a 100
Qual o nível de escolaridade mais alto que você completou?	Resposta
Em que Estado brasileiro você nasceu?	Lista com os 27 Estados e uma opção Outro.
Em que Estado brasileiro você trabalha?	Lista com os 27 Estados e uma opção Outro.
Perfil do seu cargo atual	Gestor (ex.: secretário de estado, diretor, coordenador, reitor, pró-reitor, assessor, etc.); Técnico (ex.: analista, auditor, professor, etc.)
Instituição/órgão (Local de origem - lotação)	Resposta aberta
Instituição/órgão (Local de exercício - trabalho)	Resposta aberta
Tempo de experiência profissional (anos)	1 a 5; 6 a 10; 11 a 15; 16 a 20; 21 a 25; 26 a 30; acima de 30
Aproximadamente quantas pessoas trabalham na sua instituição?	Resposta aberta
Após o término do projeto que envolve esta pesquisa, os resultados deste questionário serão divulgados para os respondentes identificados. Caso você deseje recebê-los, informe o seu e-mail.	Resposta aberta
Caso tenha alguma sugestão, observação ou crítica sobre esta pesquisa, utilize o campo de comentário a seguir:	Resposta aberta

Apêndice II- Formulário para registro dos riscos

O registro do risco é o principal componente da gestão de riscos e deve conter um conjunto de informações para permitir o acompanhamento e a gestão. Os registros possuem uma característica de acumular as melhores informações ao longo do tempo, permitindo que sejam atualizados para transmitir uma comunicação precisa. Os planos serão elaborados levando em consideração o conjunto de informações presentes no registro do risco. Na implantação do plano, o registro do risco deverá permitir o controle e o monitoramento desses riscos de forma individual. A seguir, encontra-se um breve descritivo dos seus principais componentes:

Quadro 25 – Itens para o formulário de registro do risco

Item	Detalhamento
Identificador do risco	Identificador textual do risco associado a um número sequencial único. Sugere-se a definição do item obedecendo à relação Causa-Risco-Consequência.
Tipo de risco	Os riscos devem ser classificados como "Ameaça", quando impactam negativamente o ambiente, ou "Oportunidade", quando proveem chances positivas para a instituição.
Tipologia do risco	Os riscos devem ter a seguinte classificação: Estratégico, quando têm a possibilidade de afetar toda a organização; Operacional, quando afetam apenas parte da organização; Orçamentário, quando estiverem relacionados a aspectos financeiros; Reputação, quando influenciarem na imagem da organização; Integridade, quando afetarem a honestidade e a ética; Fiscal, quando influenciarem questões fiscais e contábeis; e Conformidade, quando estiverem relacionados com o cumprimento de leis e de regulamentos.
Descrição do risco	Detalhamento do risco contendo informações como Evento/Causa - Risco - Efeito/Consequência e outras informações pertinentes.
Departamento/Unidade/Setor	Departamento mais afetado pelo risco. Geralmente o gerente desse departamento/unidade/setor será o dono do risco.
Estado do risco	Em suma, o risco pode estar ativo – sendo monitorado e/ou tratado – ou encerrado.
Data de levantamento	Informação de data que representa o dia em que o risco foi identificado.
Levantado por	Pessoa responsável pela identificação do risco.
Proximidade	Intervalo de tempo em que o risco pode ser materializado.
Valor esperado de tratamento para cada risco	Cálculo que representa estimativa de valor financeiro para tratamento de um risco.

Item	Detalhamento
Opção de resposta ao risco	Diferentes respostas ao risco a serem adotadas pela organização. Para os riscos negativos (Ameaças), foram propostas as seguintes respostas: • evitar a ameaça; • reduzir a ameaça; • transferir o risco; e • aceitar o risco. Para os riscos positivos (Oportunidades), foram propostas as seguintes respostas: • compartilhar o risco; • explorar a oportunidade; • melhorar a oportunidade; e • aceitar o risco.
Etapa	Estado atual do tratamento, conforme o guia de processos. Para simplificação, as etapas "Identificação de contexto", "Identificação do risco", "Estimativa do risco" e "Avaliação do risco" foram consolidadas em uma única etapa chamada "Identificar e avaliar risco". Foram mantidas as etapas "Planejar tratamento" e "Implantar plano".
Dono do risco	Responsável principal por coordenar todas as ações do risco.
Agente do risco	Responsável por executar as ações do risco.
Probabilidade	Chance de ocorrência do risco. Esta escala varia de 1 (Menos provável) a 5 (Mais provável).
Impacto	Representa o resultado de uma ameaça ou oportunidade particular realmente ocorrer. Esta escala varia de 1 (Mais leve) a 5 (Mais grave).
Data de encerramento	Data em que o risco foi encerrado.
Anexos e links externos	Essas funcionalidades foram adicionadas para permitir (1) a consolidação de informações em um único registro e (2) o relacionamento com outros componentes, como os Planos de Tratamento de Riscos e outras informações.

Fonte: M_o_R (2010), MGR-SISP (2016), com adaptações

Apêndice III - Questionário sobre gestão de riscos em organizações do setor público

Perguntas Orientadoras

1. Esta instituição possui uma Política de Gestão de Riscos definida? Se sim, apresente o contexto histórico da política.

2. Quem participa do processo de formulação e implementação dessa política?

3. Quais são as etapas de formulação e implementação da política? Descreva todas elas.

4. Aponte quais são as responsabilidades e as tarefas de cada participante nas etapas de formulação e implementação da política.

5. De que forma esta organização estabelece o contexto externo no que se refere à gestão de riscos?

6. Quem são os responsáveis por executar essa(s) tarefa(s)?

7. São utilizadas uma ou mais ferramentas (softwares, métodos, etc.) para identificar ameaças ou oportunidades externas à organização? Se sim, quais? Se não, como funciona esse processo?

8. Como se dá o processo de definição das estratégias para a gestão de riscos?

9. Existe uma fragmentação desse processo de definição de estratégias por meio de objetivos, metas e indicadores? Poderia exemplificar?

10. Quem são os responsáveis pelo processo de definição das estratégias?

11. De que forma essas estratégias são disseminadas na organização?

12. A organização estabeleceu o contexto interno da gestão de riscos? Como ele é realizado?

13. Quem são os responsáveis pelo contexto interno? Descreva as suas funções.

14. Há validação dos objetivos propostos na etapa de contexto interno?

15. Descreva as etapas ou atividades para a realização efetiva da gestão de riscos nesta organização.

16. Aponte em tópicos e explique os métodos utilizados para identificar e avaliar os riscos.

17. Na etapa de planejamento para tratamento dos riscos, como é feito o registro dos riscos identificados?

18. Na etapa de implementação do tratamento dos riscos, aponte o "dono do risco" e o "agente do risco". Em seguida, explique de que forma a organização estabelece o Plano de Resposta ao Risco.

19. Quanto tempo a política de gestão de risco leva para ser reavaliada nesta instituição?

20. Descreva como funciona o processo de reavaliação dessa política.

21. A instituição realiza avaliação de maturidade? Como funciona?

22. Existe um plano de melhorias para a gestão de riscos na organização? Descreva-o.

23. Descreva como funciona a comunicação e/ou divulgação de novas políticas dentro da instituição.

24. A organização utiliza-se de métodos ou técnicas para mensurar o processo de avaliação de riscos?

25. De que forma ocorre o processo de monitoramento e controle dos riscos nesta organização?

Quadro 26 – Interpretação do nível de maturidade da gestão de riscos nas organizações públicas

Etapas da execução da gestão de riscos	Perguntas orientadoras
1. Definir as políticas	1 – 2 – 3 – 4
2. Estabelecer o contexto externo	5 – 6 – 7
3. Definir as estratégias para a gestão de riscos	8 – 9 – 10 – 11
4. Estabelecer o contexto interno	12 – 13 – 14
5. Realizar a gestão de riscos para as atividades	15 – 16 – 17 – 18
6. Reavaliar a política – nível de maturidade	19 – 20
7. Avaliar a maturidade da organização	21 – 22 – 23 – 24 – 25

Glossário

Aceitação
Uma resposta a risco que significa que a organização aceita a chance de que o risco irá ocorrer com todo o seu impacto nos objetivos se de fato acontecer. Assim, uma reserva de contingência será necessária se o risco se materializar.

Ameaça
Um evento incerto que pode influenciar negativamente ou gerar impactos negativos aos objetivos da organização.

Amplificar, melhorar (*enhance*)
Tipo de resposta a riscos positivos (oportunidades) que busca aumentar a probabilidade e/ou o impacto para tornar a situação mais viável.

Benefício
A melhoria mensurável de um resultado que foi percebido como uma vantagem para um ou mais *stakeholders*.

Evitar
Tipo de resposta de risco que procura eliminar a ameaça, tornando a situação certa. Ex.: não coletar as informações de cartão de crédito em um sistema para evitar vazamento dos dados. Assim, o usuário terá de informar sempre os seus dados, e nada ficará retido, evitando esse vazamento.

Explorar
Tipo de resposta a riscos positivos (oportunidades) que busca transformar uma situação incerta em certa.

Gerenciamento de riscos
Aplicação sistemática de políticas, procedimentos, métodos e práticas nas tarefas de identificação e avaliação e, consequentemente, no planejamento e na implementação de respostas aos riscos. Provê um ambiente disciplinado para a tomada de decisão proativa.

Impacto
Efeitos produzidos por eventos (ameaças e/ou oportunidades) ou riscos identificados.

Indicador-Chave de Desempenho (*KPI - Key Performance Indicator*)
Medida de desempenho que é utilizada para ajudar a organização a definir e avaliar quanto sucesso tem ao progredir em direção a seus objetivos organizacionais.

Indicador de Aviso Prévio (EWI - Early Warning Indicators)
Um indicador direcionador (*leading*) para um objetivo organizacional que é medido por um KPI.

Nível de maturidade
Um estágio evolucionário definido rumo ao atingimento de um processo amadurecido. Geralmente são citados cinco níveis: inicial, repetitivo, definido, gerenciado e otimizado.

Oportunidade
Um evento incerto que pode ocasionar um impacto favorável nos objetivos ou benefícios.

Proximidade
A temporalidade do risco (ex.: a ocorrência do risco) dar-se-á em um tempo específico, e a severidade de seu impacto irá variar dependendo de quando ocorra.

Resultado
O resultado da mudança, geralmente afetando o comportamento ou as circunstâncias do mundo real. Os resultados são desejados quando as mudanças são concebidas. São atingidos quando as atividades alcançam o resultado no efeito da mudança.

Risco
Um evento incerto ou conjunto de eventos que, caso ocorram, terão um efeito no alcance dos objetivos. Um risco é medido por uma combinação de probabilidade da ocorrência de uma ameaça ou oportunidade e pela magnitude do seu impacto nos objetivos.

Valor esperado de tratamento
Valor monetário aproximado para tratamento de determinado risco.

Créditos

Coordenação e conteúdo
Núcleo de P&D para Excelência e Transformação do Setor Público (NExT)

Design e diagramação
Sofia Ruiz Zapata
Gustavo Tognetti Oliveira Lima
Ana Clara Sousa de Matos
Jéssica Caixeta Maranhão

Revisão
Sandra Regina Martins

Este livro foi impresso com uma tiragem de 1500
exemplares em março de 2019, na cidade de Brasília, DF.

Conheça nossos outros projetos

next
Universidade de Brasília

www.next.unb.br

ForRisco

2ª edição

ForRisco:
gerenciamento de riscos em instituições públicas na prática

Sistema **For**