ForRisco: um guia prático para gestão de riscos em instituições públicas

LISTA DE ILUSTRAÇÕES

Figura 1 – Processo genérico de Gestão de Riscos 9
Figura 2 – Metodologia de Gestão de Riscos do ERM-COSO – ERM-CUBE..... 12
Figura 3 – Metodologia de Gestão de Riscos da ISO 31000..... 13
Figura 4 – Relacionamento entre documentos do M_o_R – OGC..... 17
Figura 5 – Metodologia de Gestão de Riscos do M_o_R – OGC 17
Figura 6 – Comparativo entre metodologias de gestão de riscos. 21
Figura 7 – Metodologia de Gestão de Integridade, Riscos e Controle Interno. 28
Figura 8 – Metodologia de Gestão de Riscos do MGR-SISP..... 29
Figura 9 – Gestão de Riscos do IBGC – Avaliação de Maturidade 33
Figura 10 – Nível de Maturidade..... 37
Figura 11 – Mapa de riscos – Entre departamentos 38
Figura 12 – Mapa de Riscos – Riscos do departamento..... 39
Figura 13 – Relatório sumarizado – Ameaças e Oportunidades 40
Figura 14 – Grande visão das etapas 49
Figura 15 – Modelo das etapas..... 50
Figura 16 – Pré-requisitos para etapas da Gestão de Riscos 51
Figura 17 – Etapas do processo de gestão de riscos..... 53

LISTA DE QUADROS

Quadro 1 – Questões a serem respondidas pelas etapas das metodologias 10
Quadro 2 – Ferramentas utilizadas para o processo de avaliação de riscos 14
Quadro 3 – Abordagem de gestão de riscos – Documentos 16
Quadro 4 – Ferramentas e Técnicas presentes no Apêndice B do M_o_R 18
Quadro 5 – Escala de Maturidade do M_o_R 19
Quadro 6 – Comparativo entre as definições das principais metodologias de mercado 22
Quadro 7 – Guias e metodologias sobre Gestão de riscos da Administração Pública. .. 26
Quadro 8 – Tarefas presentes no MGR-SISP 30
Quadro 9 – Reflexões quanto aos componentes do GRCorp 33
Quadro 10 – Mensuração de maturidade em relação aos componentes 35
Quadro 11 – Leis e normativos sobre Gestão de Riscos. 41
Quadro 12 – Lista de software 44
Quadro 13 – Software avaliados e suas principais características. 46
Quadro 14 – Itens para o formulário de registro do risco. 64

LISTA DE ABREVIATURAS E SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
APF	Administração Pública Federal
AP	Administração Pública
BPM	*Business Process Management* – Gerenciamento de Processo de Negócio
CBOK	*Commom Body of Knowledge* – Corpo Comum de Conhecimento
CGU	Controladoria Geral da União
COSO	*Committee of Sponsoring Organizations of the Treadway Commission* – Comitê das Organizações Patrocinadores da Comissão Treadway
DSIC	Departamento de Segurança da Informação e Comunicações
ERM	*Enterprise Risk Management* – Gestão de Riscos Corporativos
GIRC	Gestão de integridade, riscos e controle interno
GRCorp	Gerenciamento de Riscos Corporativos
IBGC	Instituto Brasileiro de Governança Corporativa
INC01/2016	Instrução Normativa Conjunta 01 de 2016 do MP e CGU
ISO	*International Organization for Standardization* – Organização Internacional para Padronização
M_o_R	*Management of Risks* – Gestão de Riscos
MGR-SISP	Metodologia de Gestão de Riscos de Segurança da Informação e Comunicações
MP	Ministério do Planejamento, Desenvolvimento e Gestão
NBR	Norma Brasileira
OGC	*Office for Government Commerce* – Escritório para Comércio do Governo
SISP	Sistema de Administração dos Recursos de Tecnologia da Informação
TCU	Tribunal de Contas da União

SUMÁRIO

1. INTRODUÇÃO 7
2. MOTIVAÇÃO PARA A GESTÃO DE RISCOS 8
3. PRINCIPAIS METODOLOGIAS E FERRAMENTAS DE GESTÃO DE RISCOS 9
   3.1. Metodologias de mercado 10
      3.1.1. Enterprise risk management (ERM–COSO) 10
      3.1.2. ISO 31000 12
      3.1.3. Management of risks (M_o_R–OGC) 15
      3.1.4. Comparação entre as principais metodologias de mercado 20
   3.2. Metodologias da administração pública brasileira 26
      3.2.1. Metodologia de gestão de integridade, riscos e controle interno – GIRC 27
      3.2.2. Metodologia de gestão de riscos do SISP – MGR-SISP 29
      3.2.3. Metodologia de gestão de riscos do IBGC 32
   3.3. FERRAMENTAS PARA ACOMPANHAMENTO DOS RISCOS 38
      3.3.1. Mapa de riscos 38
      3.3.2. Relatórios sumarizados 39
      3.3.3. Comunicações e mensagens de alerta 40
4. LEIS E NORMATIVOS BRASILEIROS RELACIONADOS À GESTÃO DE RISCOS 40
5. FERRAMENTAS DE SOFTWARE PARA GESTÃO DE RISCO 43
6. A METODOLOGIA FORRISCO: GESTÃO DE RISCOS NO SETOR PÚBLICO 48
   6.1. Etapas da execução da gestão de riscos 48
   6.2. Exemplo da aplicação da metodologia FORRISCO 54
      6.2.1. Caso 1 – Iniciando a implantação da gestão de riscos com a metodologia FORRISCO 54
      6.2.2. Caso 2 – Aplicando a metodologia FORRISCO em uma organização que já iniciou a gestão de riscos 55
7. CONSIDERAÇÕES FINAIS 56

REFERENCIAS BIBLIOGRÁFICAS 57

APÊNDICE I – QUESTIONÁRIO 59

APÊNDICE II – FORMULÁRIO PARA REGISTRO DOS RISCOS 64

GLOSSÁRIO 66

1. INTRODUÇÃO

Indivíduos possuem percepção limitada sobre a realidade. Para lidar com esse fato, as pessoas buscam se reunir em grupos e organizações com a finalidade de moldar comportamentos observáveis em padrões racionais para, assim, contribuir para o cumprimento dos objetivos [1]. Uma organização é, ao mesmo tempo, um conjunto de propósito articulado e mecanismos estabelecidos direcionada para alcance de resultados. A partir disso, constantemente modifica e refina os mecanismos pelos quais alcançam seus propósitos, reorganizando sua estrutura, processos, papéis e relacionamentos [1].

Ao longo do tempo, diversas áreas de conhecimento têm buscado fundamentar o que se prova eficaz para o alcance dos objetivos nas organizações. Entretanto, era de se esperar que as lições aprendidas em um setor pudessem ser transferidas para o outro, formando uma teoria única das organizações. Todavia, além dessa adaptação não ser fácil, estudiosos sugerem que diferenças entre setores exigem métodos e práticas próprios de gestão [2–4]. Apesar de possuírem uma estrutura fundamental semelhante, há distinções entre organizações públicas e privadas, por exemplo.

Dentro do paradigma da "Nova Gestão Pública", tem sido crescente a adoção de práticas gerenciais oriundas da administração privada na pública. Uma das técnicas presentes no primeiro contexto que vem sendo aplicada com adaptações na esfera pública é a gestão de riscos. Esta prática possui no seu cerne a identificação e tratamento de incertezas de modo a não impactarem nos objetivos organizacionais [5].

As práticas de gestão, como a gestão de projetos, gestão de processos, gestão de serviços, entre outras, possuem um corpo de conhecimento genérico que pode ser aplicado tanto para organizações públicas quanto privadas. Estudos anteriores realizaram testes nos quais alguns tipos de princípios e técnicas de gestão foram adotados de modo semelhante nestas organizações [3, 6]. Neste sentido, tanto o setor público como o privado se beneficiaram destes modelos de gestão por contribuírem para que gestores adquiram um conjunto de conhecimentos para conduzirem seus trabalhos. No caso da gestão de riscos, observa-se este mesmo comportamento sendo adotado por ambos setores, embora possuam características específicas devido à natureza de sua atividade.

No âmbito da administração pública, as técnicas de gestão de riscos estão sendo incorporadas com a finalidade de aumentar o controle interno e governança. A Instrução Normativa Conjunta (INC) 01/2016 de 10 de maio de 2016, do Ministério do Planejamento (MP) e Controladoria Geral da União(CGU), dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo Federal [7]. Esta INC deve ser adotada pelos órgãos para que implantem medidas sistêmicas e práticas de gestão de riscos, e possui em seu texto uma forte ligação com melhores práticas de mercado relacionados à gestão de riscos, como o COSO II – Gestão de Riscos Corporativos, e ISO 31.000 [5, 8]. Adicionalmente, o MP desenvolveu outros guias para apoiar o gestor público na adoção destas práticas de gestão de risco, como a Metodologia de Gestão de Riscos do SISP – MGR-SISP [9].

A adoção de Gestão de Riscos como método de gestão complementar para organizações públicas pode contribuir para maior desempenho organizacional, por permitir controles e acompanhamentos sistêmicos nestes riscos [10–12]. Não obstante, a sociedade brasileira urge por melhores serviços da Administração Pública – AP. Os

gastos da AP precisam ser bem aplicados e gerenciados, e a cobrança por maior eficiência e gerenciamento dos recursos fazem com que a sociedade esteja mais ativa e participante.

Neste intuito, o presente trabalho apresenta uma metodologia de gestão de riscos embasada nas metodologias mais comuns de mercado e nas adotadas pela AP. Com base nisso, o trabalho justifica-se já que no cenário atual há um nível de maturidade baixo quanto ao assunto da gestão de riscos, mas uma alta cobrança para que seja implementada esta técnica de gestão.

A partir desta introdução, será explanado nas próximas seções sobre a motivação para a gestão de riscos na seção 2, sobre as metodologias de gestão de gestão de riscos na seção 3, seguido pelas leis e normativos brasileiros que estão relacionados à gestão de riscos. Na seção 5 há uma avaliação de ferramentas de software para gestão de riscos, e então é apresentado a seção 6 com a metodologia de gestão de riscos do FORRISCO. Finalmente são apresentadas as considerações finais quanto ao trabalho.

2. 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 que não há conhecimento quanto às consequências de determinado evento. O risco, por sua vez, está relacionado com o efeito da incerteza no alcance dos objetivos desta organização [5]. Assim, quando se fala em gerenciamento de riscos, buscam-se práticas recomendadas pela governança corporativa e o conselho de administração para identificar e listar preventivamente os principais riscos aos quais a organização está exposta, indicando a probabilidade, impacto e caminho para tratamento, com base em práticas sistemáticas [13].

A ocorrência de eventos como falhas no sistema bancário, catástrofes naturais, má gestão de recursos, e falta de conhecimento da organização, resultou no desenvolvimento da gestão de riscos elaborada por auditores, seguradoras, contadores, e outros praticantes de diversas organizações do setor privado [14]. Com o passar do tempo, estas 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 [14]. Com o desenvolvimento destes *frameworks*, a gestão de riscos corporativa atraiu a atenção de gerentes dos setores público e privado como um 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 avaliação de evidências quanto ao desempenho de departamentos, e auxiliar no estabelecimento de prioridades para ações de melhoria [15]. 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, esfera militar e terrorismo, fraudes e finanças, entre outros [16]. No Canadá a secretaria de tesouro (*Treasury Board of Canada Secretariat*) desenvolveu mecanismos

quanto aos riscos financeiros, auditoria interna, aquisição de serviços, tecnologia da informação e outros [17]. Estes exemplos ilustram a relevância e adoção do tema em diversos países.

No cenário nacional, foi desenvolvido pelo Ministério do Planejamento em conjunto com a Controladora-Geral da União a Instrução Normativa Conjunta MP/CGU Nº01 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 04/13 [18].

Ainda no cenário nacional, mas não relacionado diretamente ao setor público, o Instituto Brasileiro de Governança Corporativa (IBGC) elaborou uma metodologia para implantação da gestão de riscos na organização [13]. Este *framework* difere do que tem sido adotado pela IN01/2016 quanto ao processo de gestão de riscos, mas pode ser utilizada de forma complementar às outras metodologias de gestão de riscos. Além disso, contribui para que diferentes reflexões quanto ao tema de gestão de riscos ocorram, e analisar metodologias diferentes pode enriquecer e agregar valor na condução da gestão de riscos.

Todas estas iniciativas tanto no cenário internacional quanto no nacional permitem que os órgãos busquem eficiência, identificando lacunas e criando planos e ações para suprir carências. Ao alcançar estes resultados, tais organizações conseguem entregar maior satisfação e melhor serviço à sociedade. A seguir serão apresentadas algumas metodologias e ferramentas de gestão de risco que têm sido adotadas tanto em organizações privadas quanto públicas.

3. PRINCIPAIS METODOLOGIAS E FERRAMENTAS DE GESTÃO DE RISCOS

As metodologias de gestão de riscos possuem diversas similaridades entre si pelo fato de identificarem e tratarem as incertezas de forma sistemática para que haja uma comunicação precisa ao longo do processo de avaliação de riscos.

De modo geral ao longo da execução da 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 [19]. Estas questões estão presentes na Figura 1.

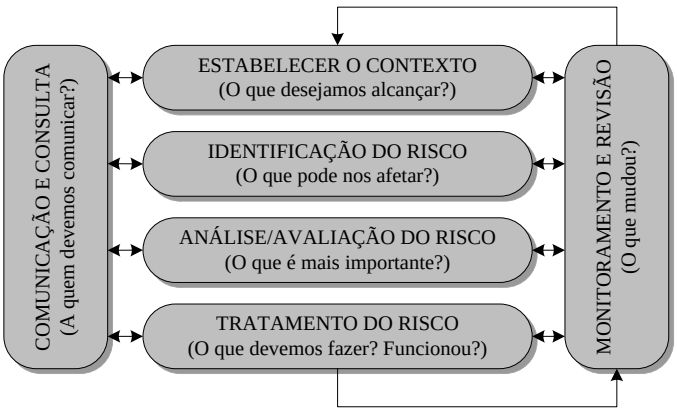

Figura 1 – Processo genérico de Gestão de Riscos
Fonte: Hillson (2017, p. 9), com adaptações

Estas questões estão presentes durante a execução das etapas contidas nas principais metodologias, como a ISO 31000 e o M_o_R-OGC [19]. O Quadro 1 relaciona estas questões com as etapas de cada metodologia.

Quadro 1 – Questões a serem respondidas pelas etapas das metodologias

Questões	ISO 31000 (2009)	OGC M_o_R (2010)
O que desejamos alcançar?	Estabelecer o 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 revisão	Incorporar e revisar
O que aprendemos?	-	-

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

Quanto à questão "O que aprendemos?", o autor sugere que esta etapa é pouco explorada nas metodologias, e que as lições aprendidas raramente são conduzidas ao final de projetos ou de decisões chave da organização, e por isso foram deixadas em branco. Justifica ainda que a não execução das lições aprendidas podem ser causadas por terem seus benefícios vindos de forma tardia para apoiar no que já aconteceu, por ausência de altruísmo dos funcionários em ajudar outros colegas com estas experiencias, ou porque os funcionários já precisam começar um novo desafio antes de se ter tempo para capturar as lições do desafio anterior. Não capturar e disseminar estas lições fazem com que a organização incorra no mesmo erro repetidas vezes, gastando recursos escassos e não entregando os resultados que a organização necessita [19].

Na próxima seção serão abordadas as metodologias de gestão de riscos mais recorrentes no mercado bem como uma comparação entre estas metodologias, e será também detalhado algumas metodologias desenvolvidas e adotadas pela administração pública brasileira.

3.1. Metodologias de mercado

Esta seção irá apresentar as principais metodologias de mercado utilizadas para a gestão de riscos corporativos[1], sendo estas o ERM–COSO – amplamente adotado pela administração pública brasileira – e também a ISO 31000 e o M_o_R–OGC, por serem recorrentes em organizações públicas e privadas de diversos países.

3.1.1. Enterprise risk management (ERM–COSO)

O ERM-COSO, também conhecido como COSO II ou ERM-CUBE, foi desenvolvido com base no COSO-I (1992) que tratava sobre auditoria e controle interno. Neste *framework* do ERM-COSO a premissa para a condução da gestão de riscos na

[1] Optou-se por traduzir "*Enterprise Risk Managemet*" como "Gestão de Riscos Corporativos". Entenda-se que Organizações, Instituições e Corporações possuem um nível similar, e que estes termos refletem "o todo" de um ambiente organizacional.

organização é que as organizações, ou entidades[2], existem para prover valor às partes interessadas, como acionistas, clientes, funcionários, entre outros. Todas as organizações enfrentam incertezas, e o desafio para a gestão é determinar o quanto de incerteza aceitar, já que estas podem causar impactos aos valores almejados. O valor é maximizado quando a gestão define objetivos e estratégias que acertam um equilíbrio ideal entre crescimento organizacional e alcance de objetivos frente aos riscos relacionados a estes objetivos [8].

Como a gestão de riscos não é um processo serial, na qual um único componente afeta apenas o componente seguinte, é necessária uma visão multidimensional em um processo iterativo no qual qualquer componente pode afetar os demais. Dessa forma, foi concebido um cubo que relaciona 4 dimensões de objetivos, com 3 dimensões de unidades de negócio, e com as 8 etapas da condução da gestão de riscos [8].

Na dimensão dos objetivos encontram-se os componentes:

- Estratégico: Objetivos de alto nível, alinhados e suportados pela missão;
- Operação: Uso eficiente e eficaz dos recursos;
- Relatório: Confiabilidade nos relatórios;
- Conformidade: Conformidade com leis e regulações vigentes.

Por sua vez na dimensão das unidades de negócio encontra-se uma lista não exaustiva das possíveis unidades de uma organização, sendo estas:

- Nível organizacional;
- Divisão;
- Unidade de negócio;
- Subsidiária.

Finalmente a dimensão que contém as etapas para a condução da gestão de riscos apresentam os seguintes componentes:

- Ambiente interno;
- Definição de objetivos;
- Identificação de evento;
- Avaliação de riscos;
- Resposta ao risco;
- Atividades de controle;
- Informação e comunicação;
- Monitoramento.

A Figura 2 representa este cubo, focando tanto no nível macro da organização quanto no nível micro em componentes mais granulares com objetivos específicos.

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

Figura 2 – Metodologia de Gestão de Riscos do ERM-COSO – ERM-CUBE
Fonte: ERM-COSO (2004, p. 7)

A metodologia possui ainda uma seção definindo papéis e responsabilidades quanto à gestão de riscos, já que está presente em toda organização. Define-se que:

- Para a alta direção há a necessidade de desenvolver uma filosofia sobre a gestão de riscos, promover a conformidade, disseminar o conhecimento e gerir assuntos estratégicos quanto aos riscos.
- Já os gestores do nível tático possuem responsabilidade de suporte na condução da gestão de riscos ao desdobrar estratégias para o nível operacional.
- Em nível operacional as atividades devem ser realizadas segundo as diretivas e protocolos estabelecidos para que forneçam as informações e relatórios necessários para a tomada de decisão dos níveis superiores.
- Há também os papéis dos membros externos, como reguladores, auditores, consultores, clientes, fornecedores e parceiros de negócio que contribuem para a obtenção de informações valiosas, mas não se responsabilizam pela efetividade da gestão de riscos na organização [8].

3.1.2. ISO 31000

A norma *ABNT NBR ISO 31000: Gestão de riscos – Princípios e diretrizes* também 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 risco. Ademais, pode ser aplicada a diferentes tipos de riscos, independentemente de sua natureza, seja aqueles que trazem impactos positivos ou negativos. A norma ainda sugere que sejam feitos tratamentos de acordo com as especificidades da organização. Por fim, deve ser utilizada para harmonizar o processo de gerenciamento de risco em padrões existentes e futuros fornecendo um suporte, mas não substituindo estes padrões mais específicos [5]. Ou seja, para ajudar na padronização

da gestão de riscos na organização, mas também entendendo que nem todo padrão atende todos os casos, e por isso, sugere tratamento específico para estes casos.

De acordo com a norma, risco é entendido como: “Efeito da incerteza nos objetivos”. Todas as organizações gerenciam riscos em algum grau e a norma estabelece princípios que precisam ser atendidos para tornar a gestão de riscos eficaz, de forma sistemática, transparente e confiável.

A norma está dividida em três componentes: definição de princípios, estrutura e processo. Partindo de um conjunto de regras e diretrizes, contida nos princípios, é então criada a estrutura para sustentar a implantação do processo de gestão de risco na organização, visando a melhoria contínua. A partir desse conjunto de componentes, o processo da norma objetiva estabelecer o contexto, identificar, analisar, avaliar e tratar o risco, e, ao longo do processo, comunicar e monitorar [5]. A Figura 3 representa o modelo geral da metodologia.

Quando a ISO 31000 é implementada e mantida, a gestão de risco contida nesta norma possibilita atingir diversos objetivos para atender necessidades das partes interessadas. Por intermédio desse conjunto de controles estruturados e com o entendimento claro do contexto e dos riscos existentes, são definidas as melhores ferramentas para tratamento dos riscos de acordo com sua natureza. Um plano de implantação para mitigação do risco é desenvolvido, executado, validado e reavaliado. Isso garante que riscos residuais sejam tratados. Assim, existirá qualidade no tratamento dos riscos e maior agregação de valor ao negócio por meio desta gestão.

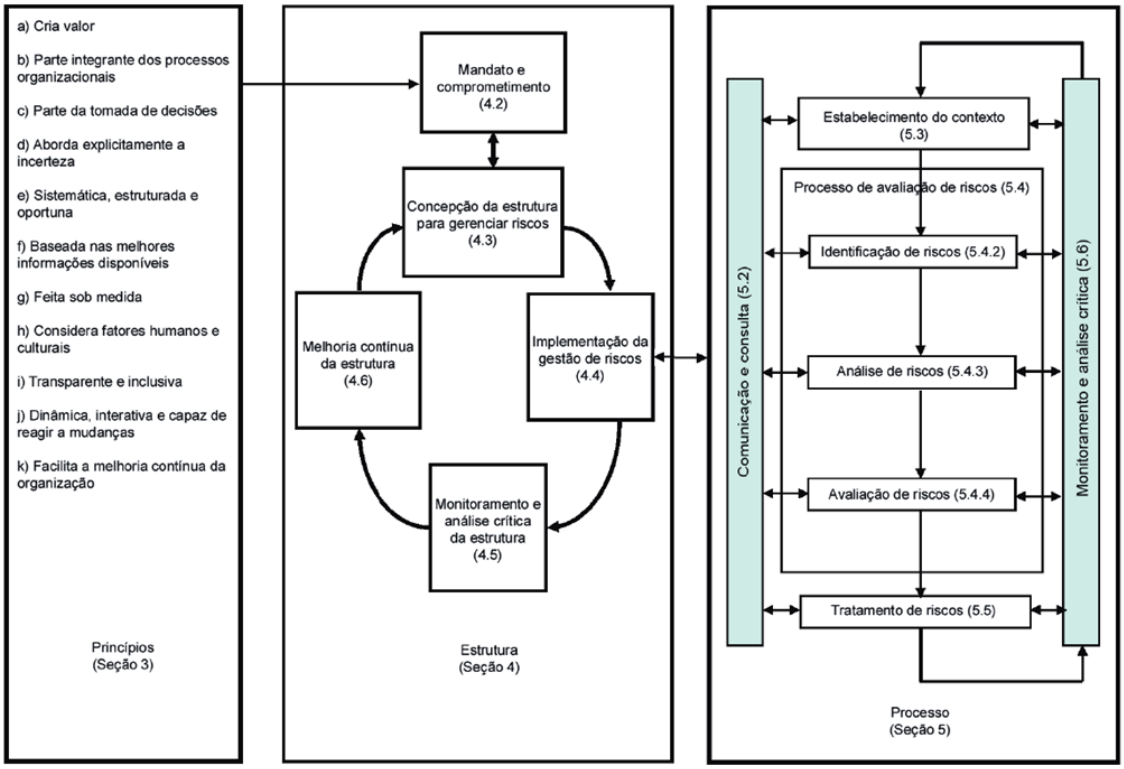

Figura 3 – Metodologia de Gestão de Riscos da ISO 31000
Fonte: ABNT NBR ISO 31000 (2009, p. vii)

Como uma complementação à norma ABNT NBR ISO 31000, a ABNT NBR ISO 31010: *Gestão de riscos – Técnicas para o processo de avaliação de riscos* fornece orientações sobre a seleção e aplicação de técnicas sistemáticas para o processo de avaliação de riscos, contribuindo para atividades de gestão de riscos. Pelo processo de avaliação dos riscos, utilizando as ferramentas e técnicas propostas na norma, pode-se apoiar para o entendimento dos riscos, angariando informações relevantes que auxiliam a tomada de decisão e o estabelecimento de priorização para o tratamento dos riscos [20]. O Quadro 2 apresenta estas ferramentas.

Quadro 2 – Ferramentas 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[1]	NA[2]	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[3]	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
Ténica etruturada "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	FA	FA	FA	FA	FA
Análise de árvore de falhas	A	NA	FA	A	A
Análise de árvore de eventos	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)* c	A	FA	A	A	NA
Árvore de decisões	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
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
[1] FA - Fortemente aplicável, [2] NA - Não aplicável, [3] A - Aplicável.					

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

Em suma, a norma ABNT NBR ISO 31000 apresenta um conjunto de etapas contendo desde o princípio, a estratégia e o processo de avaliação de riscos, e neste processo elenca as ferramentas e técnicas para permitir que se busque uma avaliação sistemática dos riscos.

Assim como o ERM-COSO, as preocupações recaem sobre o fator humano, como falta de entendimento, e outros problemas advindos da falha de comunicação e racionalidade limitada. Portanto, a estrutura de governança proposta pela norma corrobora para a redução dessas incertezas.

3.1.3. Management of risks (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 objetivos estratégicos de programas, projetos ou operações.

A metodologia engloba princípios, abordagem e processos em um conjunto de passos inter-relacionados nestas dimensões para o gerenciamento de riscos em organizações. Também é apoiada por ferramentas e técnicas para a identificação, avaliação e tratamento destes riscos. Existem apontamentos e referências da ISO 31000, o que a torna complementar em relação à gestão de riscos [21].

Na metodologia do M_o_R-OGC há uma forma mais prescritiva sobre como conduzir a gestão de riscos na organização. São apresentados oito princípios para que a gestão de riscos possa acontecer de forma prática, nos quais os sete primeiros são princípios habilitadores e o último de resultado [21]:

- Alinhamento aos objetivos: A gestão de riscos deve estar continuamente alinhada aos objetivos organizacionais;
- Adequação ao contexto: A gestão de riscos deve estar perfeitamente adequada ao contexto atual;
- Engajamento de partes interessadas: A gestão de riscos deve engajar partes interessadas e lidar com as diferentes percepções de risco;
- Fornecimento de um guia de processos claro: A gestão de riscos deve prover um guia de processos claro e coerentes para as partes interessadas;
- Apoio à tomada de decisão: A gestão de riscos deve informar adequadamente e estar vinculada à tomada de decisão em toda a organização;
- Apoio à melhoria contínua: A gestão de riscos deve utilizar dados históricos para facilitar o aprendizado e melhoria contínua;
- Criação de cultura suportiva: A gestão de riscos deve criar uma cultura que reconheça a incerteza e que considere que a organização corre riscos;
- Alcance de valores mensuráveis: A gestão de riscos permite o alcance de valores mensuráveis na organização.

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

Para alcançar o princípios citados, o M_o_R sugere uma abordagem com um conjunto de documentos (Registros, Planos e Relatórios) norteadores nas definições de como serão conduzidas as ações, o modo que serão comunicadas, geridas, e melhoradas ao longo do tempo [21]. O quadro 3 apresenta alguns destes documentos.

Quadro 3 – Abordagem de gestão de riscos – Documentos

Documento	Descrição
Política	O propósito da política é comunicar o "porquê" e o "como" a gestão de riscos será implementada em toda organização (ou 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 destes riscos até seu tratamento ou implementação. Reflete o cerne da metodologia de gestão de riscos do M_o_R.
Estratégia	A estratégia descreve atividades específicas para gestão de riscos que devem ser conduzidas para uma organização, ou parte desta, em uma forma particular considerando suas características.
Registro do Risco	O registro do risco deve capturar e manter informações das ameaças e oportunidades relativas a uma atividade organizacional específica. É o principal componente a ser avaliado em conjunto aos demais riscos, e que também permite a alocação de responsabilidades e distribuição de tarefas.
Registro da Questão	Questões são riscos materializados. Estes 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 para gestão de riscos 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 ao estado de maturidade atual para traçar rumo em busca de 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 identificados, avaliados e 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. Neste documento está estipulado quem é o dono do risco, o executor ou agente, como deve ser acompanhado e comunicado, entre outras características para seu tratamento. Assim, caso o evento de um risco seja materializado, ou ultrapasse seu limite de tolerância, não será necessário desenvolver um plano em tempo de execução, poupando 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 tratamento de riscos para os gerentes envolvidos ou partes interessadas. Este relatório permite agregar valor aos tomadores de decisão para que tenham as informações mais precisas e possam analisar tendências.

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

A Figura 4 representa o relacionamento destes documentos, sendo que existem alguns abrangentes, que valem para toda organização, como também materiais específicos para atividades da organização.

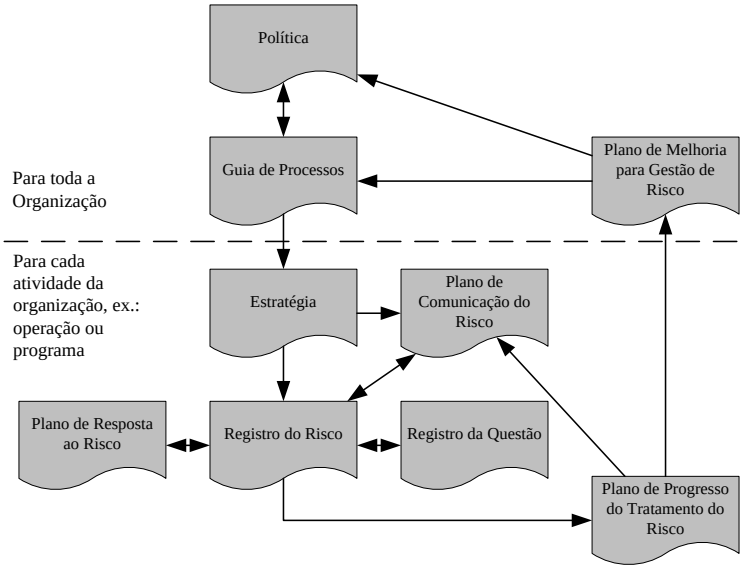

Figura 4 – Relacionamento entre documentos do M_o_R – OGC
Fonte: M_o_R (2010, p. 24), com adaptações.

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 contém várias etapas. A etapa "Comunicar" é central e deve ocorrer diversas vezes para que haja um alinhamento correto entre os envolvidos. As quatro etapas: "Identificar", "Estimar/Avaliar", "Planejar" e "Implementar", representam uma sequência lógica e a saída de uma etapa serve de insumo ou entrada para e etapa seguinte. A Figura 5 representa esta metodologia.

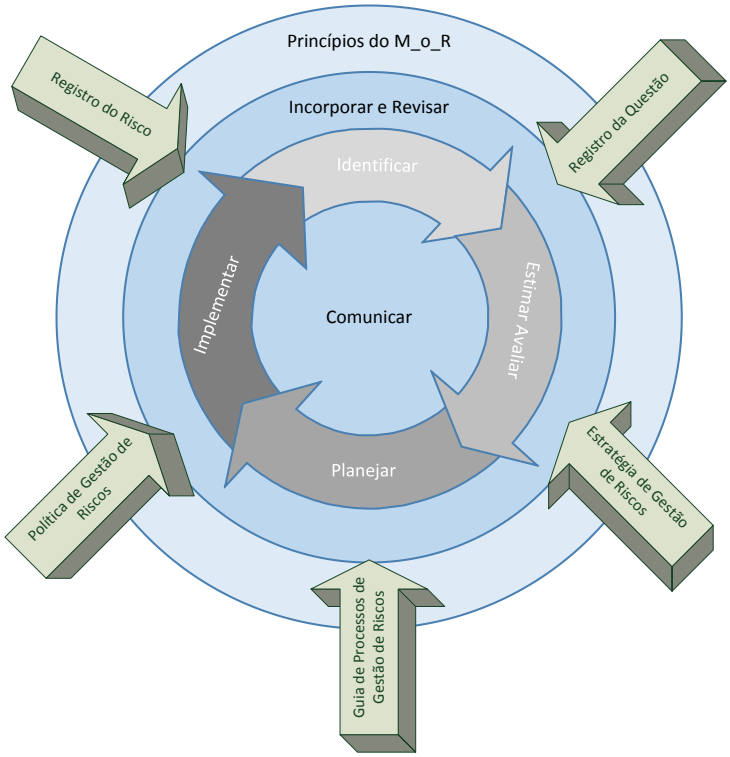

Figura 5 – Metodologia de Gestão de Riscos do M_o_R – OGC
Fonte: M_o_R – OGC (2010, p.3), com adaptações

Assim como na *ABNT NBR ISO 31010*, o *M_o_R* conta com um conjunto de ferramentas e técnicas para apoiar na execução do processo de gestão de riscos. O *M_o_R* apresenta técnicas propostas para a gestão de riscos classificadas conforme os passos do *framework*, representadas no Quadro 4. Este quadro tem por finalidade apoiar os gestores na definição das ferramentas e técnicas para a gestão, e se assemelha às ferramentas e técnicas presentes na *ABNT NBR ISO 31010*.

Quadro 4 – Ferramentas e Técnicas presentes no Apêndice B do M_o_R

Etapa do Processo	Técnica primariamente associada com a etapa do processo	Outra etapa do processo na qual a técnica pode ser útil
Identificar o Contexto	Análise de partes interessadas; Análise PESTLE; Análise SWOT; Escaneamento horizontal; Matriz probabilidade e consequência.	 Identificar o Risco 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; Avaliação de valor esperado para tratamento.	
Avaliar	Mapa de risco; Valor esperado para tratamento; Modelos de riscos probabilísticos; Árvore de probabilidade; Análise de sensibilidade.	Planejar
Planejar	Resposta ao risco; Análise custo benefício; Árvore de decisão.	 Avaliar Avaliar
Implementar	Atualização de relatório de mapa de risco; Tendências de exposição ao risco; Atualização de modelos probabilísticos de risco.	

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

Para apoiar estas atividades, o *M_o_R* 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 uma governança e controles internos, informações que devem ser reportadas, entre outras atividades;

- Os gerentes de programa, operação ou projeto, que possuem como responsabilidades garantir que o registro, revisão, avaliação, tarefas e outros controles estão sendo executados adequadamente;
- A equipe de qualidade, para garantir que existem controles contábeis, 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;
- As demais equipes, que participam da identificação ao tratamento dos riscos, implementam as regras das políticas e escalam os riscos quando necessário [21].

A metodologia ainda fornce uma escala de maturidade para apoiar gestores e a alta direção na definição dos objetivos quanto à evolução da gestão de riscos e sua maturidade na organização em questão. O Quadro 5 representa esta escala com os níveis de maturidade.

Quadro 5 – 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	Objetivos não estão definidos	Riscos associados a objetivos definidos	Objetivos definidos e atualizados durante gestão de riscos	Objetivos alterados conforme resposta dos riscos	Objetivos definidos conforme a gestão de riscos
Adequado ao contexto	Contexto não refletido na identificação de contexto	Contexto é examinado ao longo do processo de risco	O contexto é rigorosamente	Gerentes informam com antecedência sobre contexto	Contexto é usado para definições ações da gestão
Envolve stakeholders	Nem todos stakeholders são consultados	Stakeholders são identificados e minimamente engajados	Objetivos dos stakeholders são identificados, registrados, alinhados e atribuídos.	Stakeholders são ativamente envolvidos	Stakeholders são incentivados e envolvidos no ciclo de investimento
Processo definido	Política e processos não documentados e vagos.	Política e processos estão definidos.	Processos uniforme são adotados em toda organização	Gestão de riscos está totalmente integrada com as 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 sênior reportam em um formato consistente.	Existem análises quantitativa de qualidade.	Técnicas de planejamento de cenários são naturalmente utilizadas.

	Nível 1 Inicial	Nível 2 Repetitivo	Nível 3 Definido	Nível 4 Gerenciado	Nível 5 Otimizado
Melhoria Contínua	Ausência de treinamentos e conhecimento sobre gestão de riscos	Pessoas são treinadas ao longo da implantação da gestão de riscos.	Diferentes níveis de treinamento estão definidos.	Pessoal experiente analisando resultados quantitativos	Conhecimento e habilidades atualizadas constantemente.
Cultura colaborativa	Equipe age por conta própria em silos independentes.	Donos dos riscos, gerentes e agentes estão identificados	Times integrados na organização com papeis e responsabilidades são claros	Atitudes de gestão de riscos são reconhecidas e condecoradas	Riscos está embutida na organização, presente 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 stakeholders internos e externos.

Fonte: M_o_R (2010), com adaptações.

Em comparação ao ERM-COSO e ISO 31000, o M_o_R apresenta o maior arcabouço de orientações para a implantação e operacionalização da gestão de risco na organização. Embora seja mais prescritiva que as outras normas, ainda continua genérica o suficiente para ser adotada tanto por organizações do setor público quanto privado, de maior ou menor porte.

3.1.4. Comparação entre as principais metodologias de mercado

As metodologias de mercado possuem um conjunto comum de orientações aos profissionais de gestão de riscos. Como foram desenvolvidas em momentos diferentes, percebe-se uma evolução no foco nas técnicas de gestão, bem como um conjunto abrangente de ferramentas e técnicas para apoio aos gestores na condução dos riscos na organização. O Quadro 6 contém informações que sintetizam as principais ideias do processo de gestão de riscos, segundo as metodologias representadas nas colunas da tabela. Para facilitar o entendimento, foi elaborado na Figura 6 uma numeração de apoio para identificar etapas similares entre estas metodologias.

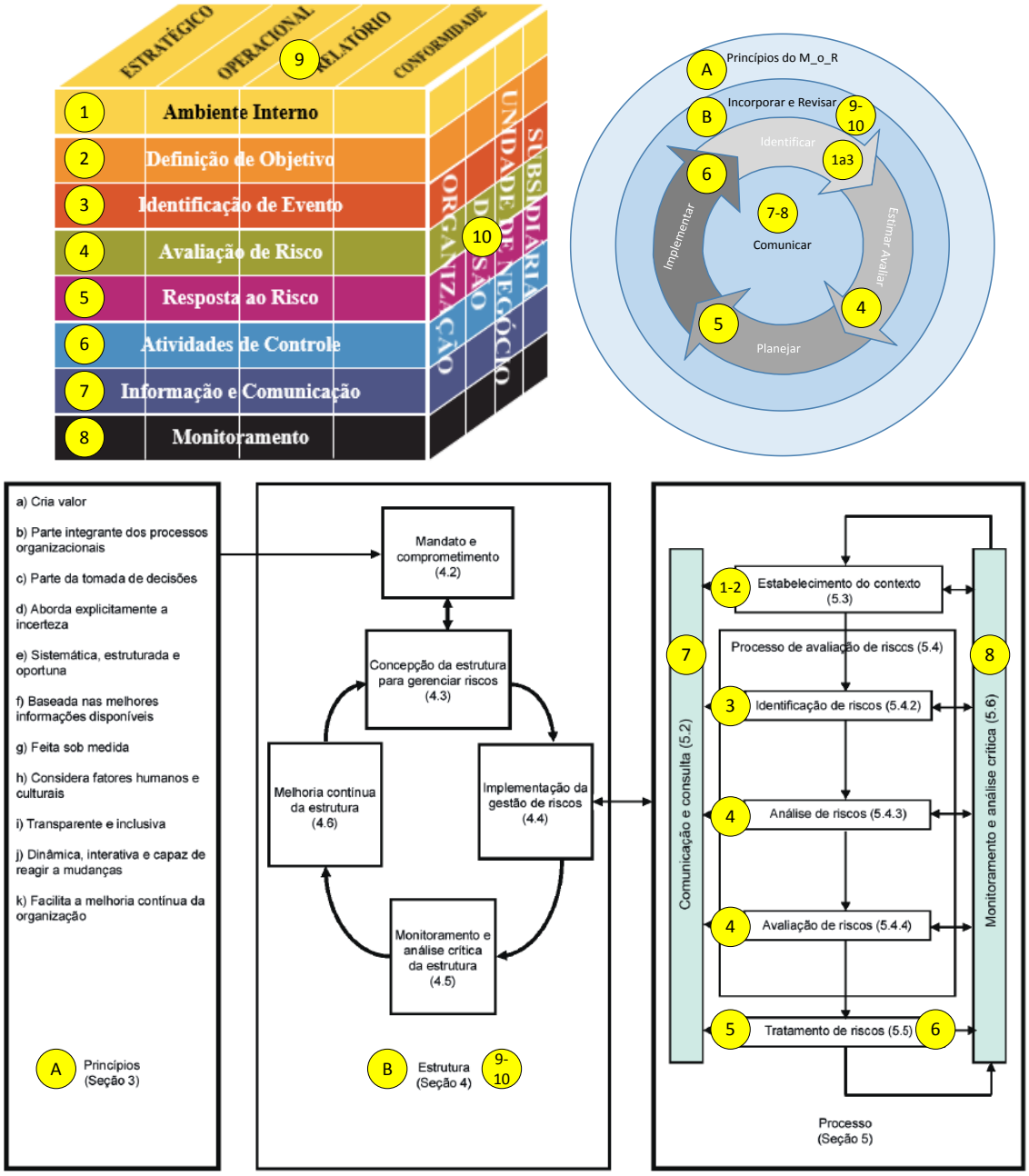

Figura 6 – Comparativo entre metodologias de gestão de riscos.
Fonte: ERM – COSO (2004), ISO 31000 (2009), M_o_R – OGC (2010), com adaptações

Estes identificadores estão registrados na coluna "Metodologia" do Quadro 6, a fim de facilitar o entendimento dos processos de gestão de riscos. Sugere-se que sejam lidos em conjunto tanto a Figura 6 quanto o Quadro 6.

Quadro 6 – Comparativo entre as definições das principais metodologias de mercado

Item	ERM-COSO (2004)	ISO 31000 (2009)	M_o_R-OGC (2010)
Risco	Risco é a possibilidade de ocorrência de um evento ocorrer e afetar o alcance dos objetivos (p. 13).	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).
Gestão de Riscos Corporativos	É um processo realizado por um comitê de diretores, gerentes e outras pessoas, aplicado na definição estratégica e em toda organização, designado para identificar eventos potenciais que podem afetar a organização, e o gerenciamento de riscos para que estejam contidos no apetite de riscos, fornecendo uma garantia razoável quanto ao alcance dos objetivos organizacionais (p. 16).	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).
Processo de avaliação de riscos	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 consideração tanto os riscos herdados quanto os residuais, com a avaliação considerando a probabilidade e impacto (p. 49).	O processo de avaliação de riscos é o processo global de identificação de riscos, análise de riscos e avaliação de riscos (p. 17).	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).
A – Princípios	Embora não haja uma definição específica de princípios no guia, há no Anexo B um sumário chave dos princípios de cada uma das oito etapas do processo (p. 101).	A norma apresenta onze princípios para que a gestão de riscos seja eficaz em todos os níveis da organização (p. 7).	O propósito do princípio é de comunicar o porquê 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).

Item	ERM-COSO (2004)	ISO 31000 (2009)	M_o_R-OGC (2010)
B – Estrutura	Não foi identificado no ERM-COSO a definição específica de uma estrutura específica para conectar princípios com os processos, assim como as definições encontradas nas outras normas.	O sucesso da gestão de riscos depende da eficácia da estrutura de gestão, que fornece os fundamentos e os arranjos para incorporá-la através de toda a organização. Esta estrutura serve para auxiliar a organização a integrar a gestão de riscos em seu sistema de gestão global, porém requer adaptação estes componentes às suas necessidades (p. 8).	A incorporação e 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 organização, e conta para isso com o uso de métodos e modelos para alcançar este resultado (p. 51).
1 – Contexto/ Ambiente interno	Define a base sobre como os riscos e controles são endereçados por pessoas na organização. O centro de qualquer negócio são suas pessoas – seus valores individuais, incluindo integridade, valore éticos, e competência – e o ambiente no qual estes operam (p. 27).	Definição dos parâmetros externos e internos a serem levados em consideração ao gerenciar riscos, e estabelecimento do escopo e dos critérios de risco para a política de gestão de riscos (p. 3).	O objetivo da identificação de contexto é obter informações sobre as atividades planejadas e como se encaixam em toda organização para atender o mercado ou a sociedade (p. 32).
2 – Definição de objetivos	Devem existir objetivos prévios para que o gerenciamento possa identificar eventos potenciais que afetem seu alcance (p. 35).	Convém que a política de gestão de riscos estabeleça claramente os objetivos e o comprometimento da organização em relação à gestão de riscos (p. 10).	A Gestão de riscos alinha-se continuamente com os objetivos organizacionais. A Gestão de Riscos está focada nas incertezas que tem o potencial de impactar o alcance de um ou mais objetivos da organização (p. 13).
3 – Identificação	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. 41).	Processo de busca, reconhecimento e descrição de riscos (p. 4). Convém que a organização identifique as fontes de risco, áreas de impactos, eventos (incluindo mudanças nas circunstâncias) e suas causas e consequências potenciais. A finalidade desta etapa é gerar uma lista abrangente de riscos baseada nestes eventos que possam criar, aumentar, evitar, reduzir, acelerar ou atrasar a realização dos objetivos (p. 17).	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; • Entender a visão de pessoas chave quanto ao risco (p. 36).

Item	ERM-COSO (2004)	ISO 31000 (2009)	M_o_R-OGC (2010)
4 – Análise	No ERM a análise e avaliação ocorrem na mesma etapa. Segundo o *framework,* a avaliação de riscos permite que a organização considere a abrangência e proporção na qual eventos potenciais podem impactar no alcance dos objetivos. A gestão dessa avaliação considera as perspectivas impacto e probabilidade relacionada com métodos qualitativos e quantitativos. Também se consideram os riscos herdados e residuais (p. 51).	Processo de compreender a natureza do risco e determinar o nível de risco. (p. 5) 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. 18).	O objetivo da estimativa é priorizar riscos individuais para esclarecer quais riscos são mais importantes e mais urgentes. Para isso é necessário entender sua probabilidade, impacto e proximidade (p. 38).
4 – Avaliação		Processo de comparar os resultados da análise de riscos com os critérios de risco para determinar se o risco e/ou sua magnitude é aceitável ou tolerável (p. 6). 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 a prioridade para a implementação do tratamento (p. 18).	A avaliação de risco serve para entender a exposição de risco da atividade olhando para a cadeia de efeitos das ameaças e oportunidades destas atividades em conjunto (p. 41).
5 e 6 – Tratamento/ Resposta	Pessoal identifica e avalia possíveis respostas ao risco que inclui a aceitação, redução, compartilhamento ou evitar o risco. A gerência seleciona um conjunto de ações para alinhar riscos com a tolerância e apetite de riscos da organização (p. 55).	Processo para modificar o risco (p. 6). O tratamento de riscos envolve a seleção de uma ou mais opções para modificar os riscos e a implementação dessas opções (p. 19).	O objetivo do plano é preparar uma resposta específica para reduzir ameaças e maximizar oportunidades para que o negócio e sua equipe não sejam surpreendidos caso um risco se materialize (p. 44). A implementação garante que as ações planejadas da gestão de riscos sejam implementadas e monitoradas quanto a sua efetividade, e para que ações corretivas sejam tomadas (p. 45).

Item	ERM-COSO (2004)	ISO 31000 (2009)	M_o_R-OGC (2010)
7 – Comunicação	Informações relevantes são identificadas, capturadas e comunicadas em um formato definido e frequência regular para que as pessoas executem suas responsabilidades (p. 67).	Processos contínuos e iterativos que uma organização conduz para fornecer, compartilhar ou obter informações e se envolver no diálogo com as partes interessadas, com relação a gerenciar riscos (p. 3).	A comunicação é conduzida ao longo de todo processo de gestão de riscos. Como a exposição da organização aos riscos não é estática a comunicação efetiva é componente chave para a identificação, alterações dos riscos existentes, ou novas ameaças e oportunidades (p. 31).
8 – Monitoramento	De forma abrangente, a gestão de riscos da organização é monitorada e modificações são realizadas quando necessário. Desta forma, pode-se reagir de forma dinâmica (p. 75).	Verificação, supervisão, observação crítica ou identificação da situação, executadas de forma contínua, a fim de identificar mudanças no nível de desempenho requerido ou esperado (p. 7). Convém que o monitoramento e a análise crítica sejam planejados como parte do processo de gestão de riscos e envolvam a checagem ou vigilância regulares. Podem ser periódicos ou acontecer em resposta a um fato específico (p. 20).	O monitoramento é necessário para entender se as respostas estão sendo implementadas de forma efetiva. Embora o monitoramento possua seu valor, é apenas um processo de observação. Deve ser mais abrangente que uma revisão de planos de ação (p. 47).
9-10 – Abordagem	Quanto à abordagem para condução da gestão de riscos o *framework* define quatro categorias (estratégico, operação, reporte e conformidade) relacionadas com quatro unidades organizacionais (Nível organizacional, Divisão, Unidade de negócio e Subsidiária) (p. 23)	A norma apresenta o mandato e comprometimento que compreende a 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, comunicação dos benefícios e manutenção da estrutura (p. 9).	Os princípios fornecem uma base para que a abordagem seja desenvolvida. Nesta abordagem estão descritas as atividades a serem executadas, a sequência em que são realizadas, os papéis e responsabilidades necessários para estas entregas. As entregas consistem em documentos como registros, planos e relatórios (p. 52).

Fonte: Elaboração própria.

Percebe-se que este conjunto de definições está presente em todas as metodologias, e que em diversos casos possuem sobreposições ou similaridades quanto a estas etapas da gestão de ricos. Por meio deste comparativo pode-se perceber a convergência das metodologias para um entendimento que remete a um processo genérico de gestão de riscos nos quais se destacam:

- O entendimento do contexto;
- A identificação e avaliação de riscos;
- A elaboração de planos para tratamento;
- A implementação destes planos de tratamento.

3.2. Metodologias da administração pública brasileira

Esta seção contém as principais metodologias de gestão de riscos identificadas nos órgãos da administração pública brasileira. O Quadro 7 apresenta os órgãos em que foi desenvolvida a metodologia, o título do documento e um breve descritivo.

Quadro 7 – Guias e metodologias sobre Gestão de riscos da Administração Pública.

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 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 diante da realidade de cada organização. Apesar de destinar-se primariamente a empresas com fins lucrativos, os conceitos e sugestões poderão ser utilizados também por entidades do primeiro e do terceiro setores.
Ministério do Planejamento, Orçamento e Gestão (2013)	Guia de orientação para o gerenciamento de riscos	Este Guia de Orientação para Gerenciamento de Riscos (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 SIC 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.

Órgão	Título	Descrição
Superior Tribunal de Justiça (2016)	Gestão de Riscos	Os processos de trabalho do STJ envolvem riscos. Logo, a consciência de sua existência e a capacidade de administrá-los, associada à disposição de correr riscos e de tomar decisões, é indispensável. 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 trazer 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 de GRCorp.
Ministério do Planejamento, Desenvolvimen-to e Gestão (2017)	Manual de gestão de integridade, riscos e controles internos da gestão	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).

Fonte: Elaboração própria.

Foram consideradas para análise as metodologias do Ministério do Planejamento (GIRC e MGR-SISP), por estarem mais alinhadas à Instrução Normativa Conjunta 01/2016, e a metodologia do IBGC 2017. Outras metodologias não foram consideradas para esta análise devido à similaridade às metodologias de mercado ou escopo especializado ao órgão em que foi desenvolvida.

3.2.1. Metodologia de gestão de integridade, riscos e controle interno – GIRC

Segundo o MP, o Programa de Integridade tem a finalidade de mitigar ocorrências de corrupção e desvios éticos a partir da mobilização e participação ativa dos gestores públicos por meio de medidas que assegurem a entrega de resultados esperados pela sociedade, pelo fortalecimento e aprimoramento da estrutura de governança, gestão de riscos e controles, e procedimentos de integridade [22].

Nesta metodologia estão descritas as premissas, conceitos, papéis e responsabilidade, taxonomia de eventos de riscos e lista de controles básicos. É constituída de quatros pilares:

- 1º Pilar - O Ambiente de Integridade: oferece as bases para que o programa seja efetivo; composto de ações de comprometimento; apoio da alta administração; de alinhamento ao planejamento estratégico;

- 2º Pilar - A 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 ao conflito de interesses e a presença de nepotismo, e implementação da Lei de Acesso à Informação;
- 4º Pilar - A Informação, Comunicação e o 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.

Estes pilares fornecem uma base para que ocorra a gestão de integridade, riscos e controle na organização por meio de um modelo representado na Figura 7. Neste modelo é apresentado:

- A política, que estabelece os princípios, diretrizes e responsabilidades;
- A instância de supervisão, que assessora a autoridade máxima do órgão na definição e implementação de diretrizes, políticas, normas e procedimentos;
- A metodologia de GIRC, que pressupõe que os processos da organização estejam mapeados, bem como a Cadeia de Valor, para aplicação do "Método de Priorização de Processos";
- A solução tecnológica, que serve como um instrumento de apoio à aplicação da metodologia de GIRC [22].

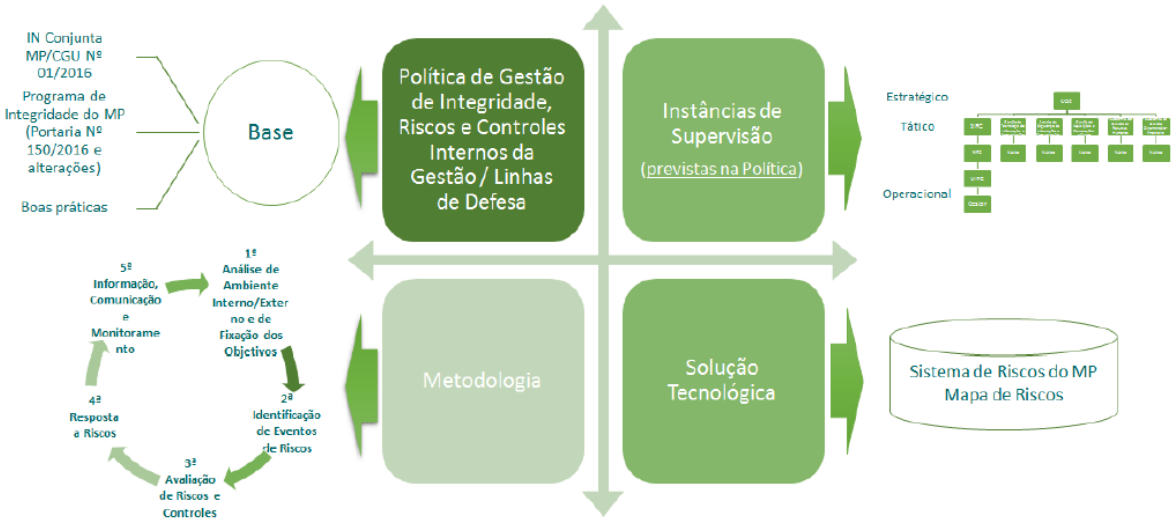

Figura 7 – Metodologia de Gestão de Integridade, Riscos e Controle Interno.
Fonte: GIRC (2017, p. 16), com adaptações

A metodologia inicia-se a partir do documento "Método de Priorização de Processos". Nele é possível identificar, avaliar e adotar respostas aos eventos de risco dos processos da unidade. Adicionalmente, este registro ainda fornece diretrizes básicas acerca de boas práticas, para despertar nos gestores a importância da gestão de integridade, riscos e controles internos da gestão [22].

Nesta metodologia, a maior contribuição é quanto à estrutura desenvolvida prévia à aplicação da gestão de riscos, definindo política a ser seguida, papéis e responsabilidades, uma metodologia para registro e acompanhamento dos riscos, e o alinhamento destas dimensões com a tecnologia da informação para viabilizar um sistema de informações a fim de facilitar a gestão de riscos na organização. Também realiza uma importante contribuição quanto à disponibilização de ferramentas de controle para viabilizar o registro e acompanhamento por meio da "Metodologia de Priorização de Processos" e "Planilha Documentadora".

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

O Ministério do Planejamento – MP desenvolveu uma metodologia de gestão de riscos 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), esta norma pode ser adaptada como um processo genérico de gestão de riscos.

A metodologia traz uma grande contribuição em relação ao contexto brasileiro, contendo referências a normativos e leis vigentes aplicados à gestão de riscos. Ainda apresenta os processos conforme ilustra a Figura 8. Neste, a comunicação e o monitoramento são tarefas que devem acontecer em paralelo com o conjunto de processos de gestão de riscos. Pode-se perceber uma forte similaridade com a metodologia do ISO 31000, em uma sequência lógica de passos para a resolução dos riscos.

Figura 8 – Metodologia de Gestão de Riscos do MGR-SISP
Fonte: MGR-SISP (2016, p. 36)

Esta metodologia possui 7 processos que contém 16 atividades totalizando 65 tarefas para a condução da gestão de riscos, conforme apresenta o Quadro 8. Também estão definidos os papéis para a condução destas tarefas que correspondem à:

- Autoridade Competente: Responsável por prover os recursos necessários à gestão de riscos; identificar responsáveis; iniciar as atividades de gestão de riscos; 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 melhorias necessárias para mitigar riscos, além de comunicar os resultados de análises a todos os interessados;
- Responsável pela Unidade da Organização: Responsável 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: Responsável por fornecer 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 8 estes responsáveis, e suas respectivas tarefas, estão representados pelas siglas: AC – Autoridade Competente, em preto; GR – Gestor de Riscos, em azul; RA – Responsável por Ativos, em laranja; RU – Responsável pela Unidade da Organização, em verde; e em cinza para mais de um papel [9].

Quadro 8 – Tarefas presentes no MGR-SISP

Processo	Atividade	Tarefa	Siglas
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
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 Vulnerabilida-des	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	RA
		2.2-D: Validar Ameaças, Controles e Vulnerabilidades dos Ativos da Unidade	RU
		2.2-E: Validar Informações Sobre as Ameaças, Controles e Vulnerabilidades	GR
3. ESTIMAR RISCOS	3.1 Avaliar Impactos	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 Probabilidades	3.2-A: Solicitar Avaliação de Probabilidades	GR
		3.2-B: Solicitar Definição de Probabilidades	RU
		3.2-C: Definir Probabilidades	RA

Processo	Atividade	Tarefa	Siglas
		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 as Estimativas de Riscos do Projeto de GRSIC	GR
4. AVALIAR RISCOS	4.1 Classificar os Riscos	4.1-A: Realizar a Classificação dos 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 Planos de Tratamento de Riscos	GR
		5.3-B: Elaborar Plano de Tratamento de Riscos	RU
		5.3-C: Avaliar Planos de Tratamento de Riscos	GR
		5.3-D: Validar Planos 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-A: Validar Tratamentos	RU
		7.2-B: Monitorar Execução dos PTRs	GR

Processo	Atividade	Tarefa	Siglas
	7.2 Monitorar o Tratamento de Riscos	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

Como pode ser visto, o GRSIC conta com ferramentas para apoiar gestores e ainda se adequa ao contexto nacional. Apesar de possuir tarefas específicas para o cenário da Segurança da Informação e Comunicação (GRSIC), é possível realizar generalizações para outros casos. Ademais, o MP ofereceu ferramentas em formato eletrônico para apoiar os gestores no registro e identificação destes riscos, como a "Planilha de Priorização de Processos" e a "Planilha Documentadora". Contudo, estas ferramentas apresentam limitações e restrições quanto ao tratamento e acompanhamento dos riscos. De toda forma, na metodologia do MGR-SISP, a explanação do conjunto de tarefas e papéis contribuem de sobremaneira para que as incertezas sejam dirimidas.

3.2.3. 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 também o mapa de riscos da organização. Isso consiste em identificar o grau de apetite a 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 [13].

É recomendável que os integrantes do conselho tenham conhecimentos sobre indicadores de desempenho para opinar sobre o assunto. Também sugere-se que a empresa tenha um programa para trazer a cultura de gestão de riscos para 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 têm a responsabilidade sobre os riscos;
- 2ª Linha de defesa – realizada pelos gestores corporativos de GRCorp, de conformidade ou de outras práticas de controle, por exemplo, e que 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 de GRCorp e para 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 desejado 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 [13].

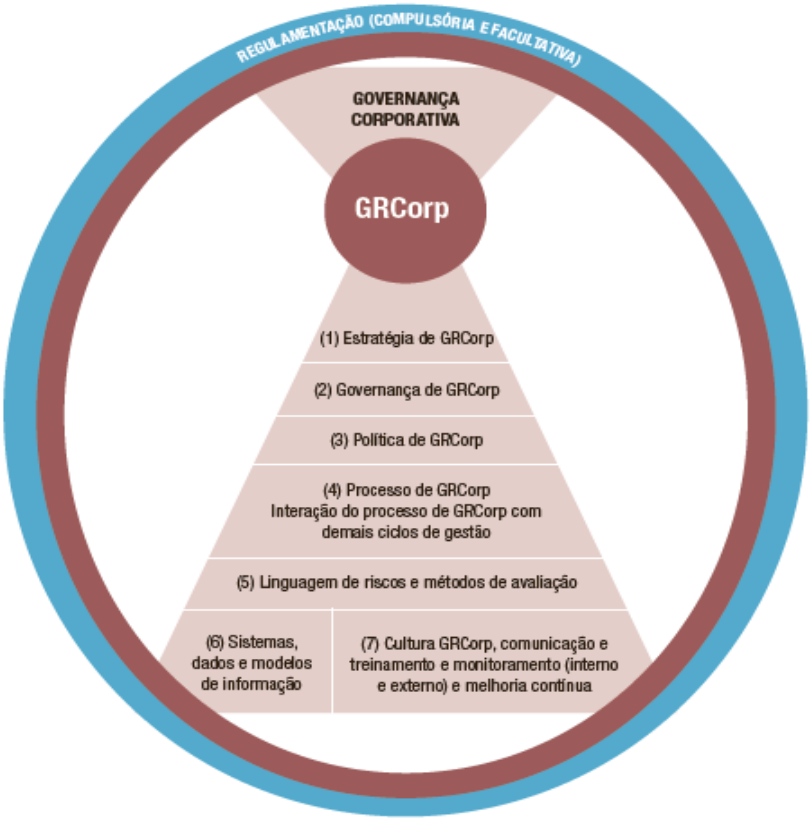

Figura 9 – Gestão de Riscos do IBGC – Avaliação de Maturidade
Fonte: IBGC (2017, p. 34), com adaptações

A Figura 9 contém uma visão geral dos componentes de GRCorp integrados ao processo de governança corporativa da organização, e seus principais elementos para a mensuração de maturidade. Nesta representação a "Regulamentação (Compulsória e Facultativa)" apoia na definição do contexto externo e interno que influencia a Governança Corporativa. Para cada componente devem haver reflexões a fim de identificar o nível de maturidade atual. No Quadro 9 estas reflexões, separadas por componente, estão registradas e devem ser lidas em conjunto com a Figura 9.

Quadro 9 – 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 papel 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?

Componente do GRCorp	Reflexões
(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 da organização e capturadas de forma consistente?
(7) Cultura de GRCorp, comunicação e treinamento e 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?

Fonte: IBGC (2017), com adaptações

As reflexões do Quadro 9 contribuem para a identificação do estágio de maturidade segundo os componentes do GRCorp. Uma vez refletido para cada contexto, pode-se entender em que nível de maturidade a organização está para este componente, e quais seriam as ações para que alcance o próximo nível. No Quadro 10 estão registrados estes níveis de maturidade para que contribuam na identificação do estado atual e passos futuros.

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

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

Quadro 10 – 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 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 em áreas históricas em resposta ao cumprimento das obrigações regulatórias.	As funções da 2ª linha de defesa cobrem os riscos de negócio e 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 do setor.
(3) Política de GRCorp				
Políticas e procedimentos não estão definidos e não há um processo consistente para seu desenvolvimento e manutenção.	Políticas e procedimentos são limitados a áreas direcionadoras-chave.	Políticas e procedimentos de GRCorp são formais e comunicadas 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.

Inicial	Fragmentado	Definido	Consolidado	Otimizado
(4) Processo de GRCorp e Interação do processo de GRCorp com 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, 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 stress e análise de cenários são utilizados em nível corporativo	Utiliza abordagem padronizada e consistente para definir o apetite e tolerância a riscos. Cenários futuros e testes de stress são usados para explorar a análise dos riscos
(6) Sistemas, dados e modelos de informação				
Modelos de informações e relatórios são direcionados por exigências externas e não são suficientemente definidos.	Modelos de informações e relatórios são definidos pela alta direção, mas não são compreendidos pela gestão ou alinhados na organização.	Os 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.

Inicial	Fragmentado	Definido	Consolidado	Otimizado
(7) Cultura, Comunicação e treinamento, monitoramento e melhoria contínua				
Não há um plano de disseminação implementado para formalizar as principais decisões da companhia em relação 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 mãos 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 de cada componente são independentes entre si, podendo estar posicionados em níveis diferentes.

Após a realização da avaliação do nível de maturidade, o conselho 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 fornece um guia estruturado e detalhado para a melhoria contínua, em busca de resultados de curto, médio e longo prazos para a estratégia de GRCorp [13].

Figura 10 – Nível de Maturidade
Fonte: IBGC (2017), M_o_R (2010), com adaptações

Por meio deste instrumento, a organização pode documentar, comunicar e programar melhorias quanto ao seu ambiente interno. A metodologia ainda recomenda realizar uma pesquisa por padrões na indústria e comparar a organização com as empresas líderes nestas práticas de GRCorp. Para esta aferição do nível de maturidade foi realizado 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 melhroria e outras ações.

3.3. 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 sejam comunicados e reportados de forma efetiva aos tomadores de decisão. Algumas ferramentas destinadas a este fim serão apresentadas a seguir.

3.3.1. Mapa de riscos

O mapa de riscos é uma ferramenta que permite avaliar os riscos segundo os critérios ou parâmetros fornecidos pelo especialista. Neste caso, o mapa reflete uma análise dos riscos em conjunto para permitir uma visão holística em um momento anterior e atual. Estes riscos podem ser filtrados para a organização ou departamento, quanto às oportunidades ou ameaças, e outros mecanismos de agrupamento que facilitem a visualização do tomador de decisão.

Nesta técnica devem ser desenhados (plotados) na matriz de probabilidade e impacto os riscos conforme sua priorização. Dessa forma auxiliará o especialista na identificação dos riscos que devem ser analisados ou tratados com mais urgência, além de permitir o acompanhamento da evolução deles.

A Figura 11 corrobora para o entendimento deste mapa de riscos:

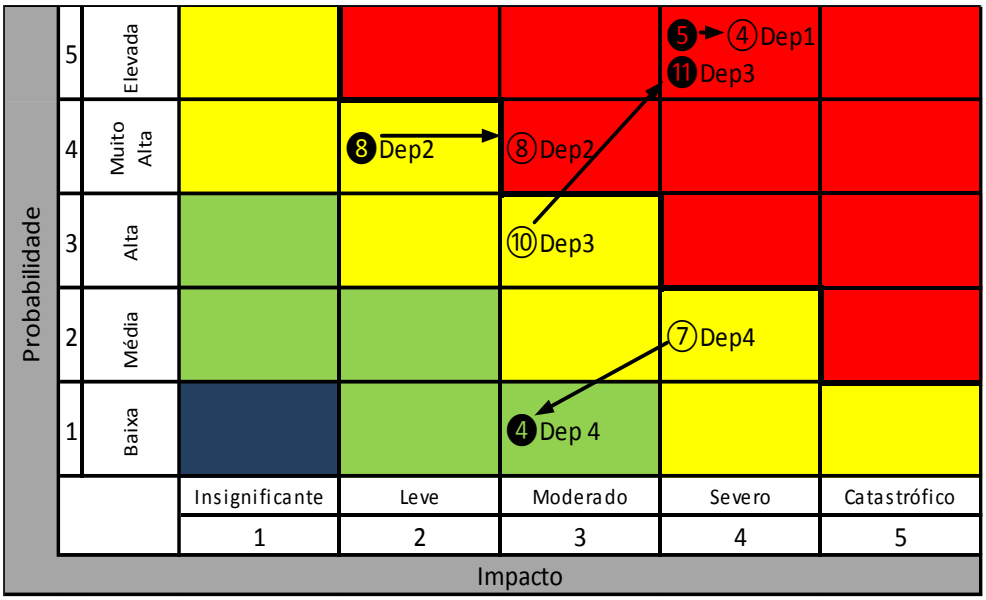

Figura 11 – Mapa de riscos – Entre departamentos
Fonte: Elaboração própria

Neste mapa de riscos, os círculos escuros representam o momento anterior e os claros o momento atual. Os números nos círculos representam a quantidade de riscos relacionadas ao departamento. Para o departamento 1 (Dep1) podemos notar que havia 5 riscos anteriormente e que no momento atual existem 4. Já o departamento 2 (Dep2) manteve a quantidade de riscos do momento anterior, porém, algum dos riscos teve seu impacto elevado, o que ocasionou no reposicionamento no gráfico. Já o departamento 3 (Dep3) foi acrescido de um risco e também teve pelo menos um dos riscos aumentado em sua probabilidade e impacto. Finalmente o departamento 4 (Dep4) teve 3 riscos resolvidos

e o risco mais grave possui baixa probabilidade e impacto moderado. Dessa forma é possível visualizar que os departamentos que requerem maior atenção são o departamento 1 e 3, pois estão posicionados na zona mais arriscada em relação aos outros riscos.

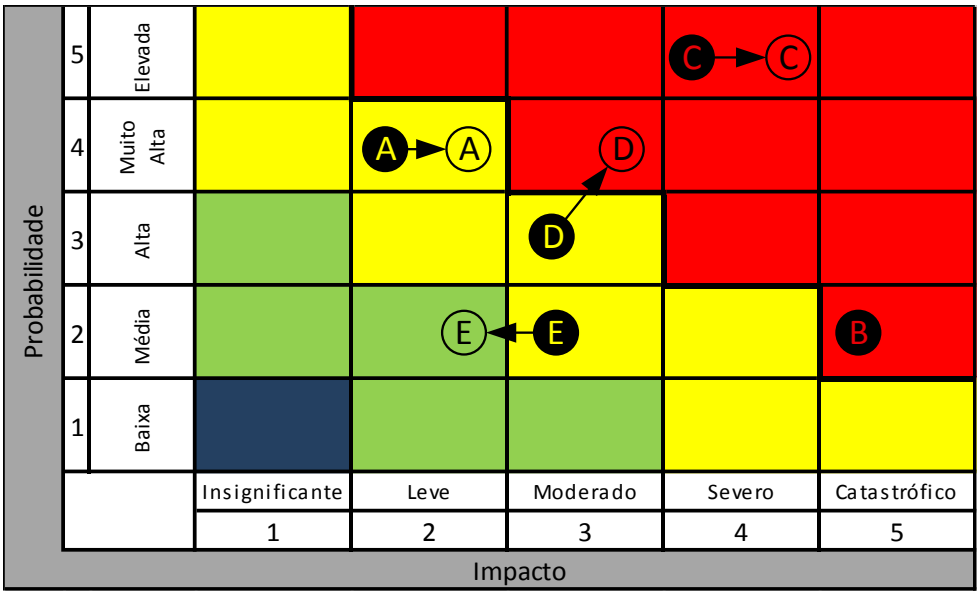

Figura 12 – Mapa de Riscos – Riscos do departamento
Fonte: Elaboração própria

Ao visualizar os riscos de um único departamento, como por exemplo o departamento 1, pode-se ver os riscos que afetam este departamento. Em cada círculo há uma letra para identificar de forma única o risco. A ilustração da Figura 12 reflete este cenário.

Podemos observar neste caso que o risco A manteve as mesmas características do momento anterior. Já o risco B foi resolvido. O Risco C também manteve as mesmas características. O Risco D por sua vez foi agravado e teve sua probabilidade aumentada. Finalmente, o risco E foi abrandado e teve seu impacto reclassificado para leve. Neste contexto observa-se que o risco C é o mais prioritário, seguido pelo risco D, depois o risco A e finalmente o risco E.

Estes mapas devem permitir uma visualização baseada nos critérios que o especialista em risco deseja visualizar. Dessa forma, pode-se priorizar e distribuir as tarefas aos agentes e especialistas, além de permitir rastreabilidade e acompanhamento dos riscos.

3.3.2. Relatórios sumarizados

O intuito dos relatórios é fornecer informações aos tomadores de decisão com uma visão sintética sobre o quantitativo dos riscos em um momento anterior em comparação ao momento atual. Esta técnica apresenta o somatório das ameaças e oportunidades por meio de um filtro, como por exemplo o departamento que estão afetando. A figura 13 representa este conjunto de informações.

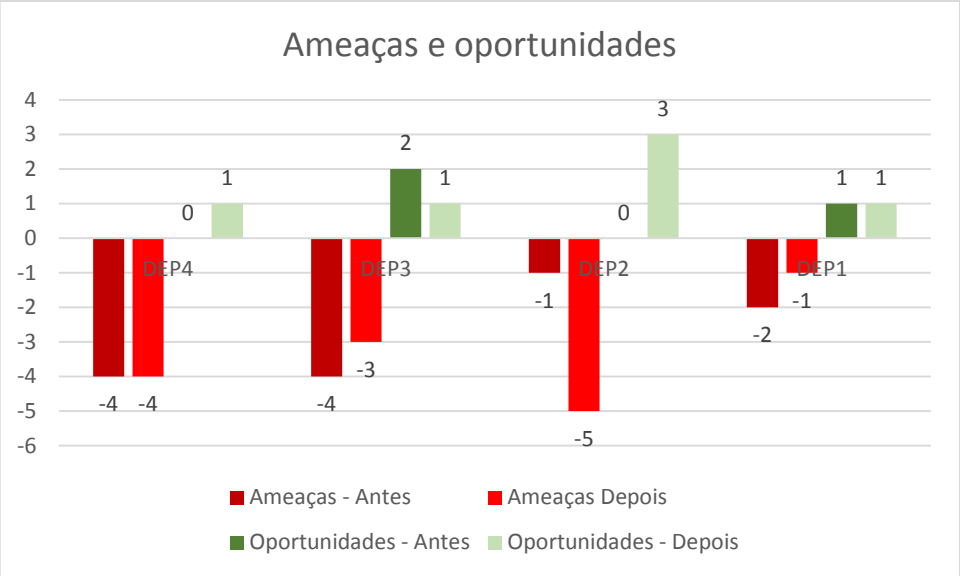

Figura 13 – Relatório sumarizado – Ameaças e Oportunidades
Fonte: Elaboração própria

Neste cenário podemos observar que o departamento 1 (Dep1) teve uma ameaça resolvida, e manteve a mesma quantidade de oportunidades. Já o departamento 2 (Dep2) teve 4 novas ameaças e 3 novas oportunidades. O departamento 3 resolveu uma ameaça e concluiu uma oportunidade. Finalmente o departamento 4 não teve novas ameaças e recebeu uma oportunidade.

Este relatório não contém a gravidade dos riscos, mas sim a quantidade de riscos em que os departamentos estão expostos. Permite uma visão rápida de quais departamentos podem estar enfrentando mais problemas e requerem mais atenção. Em conjunto com este relatório devem ser desenvolvidos textos sucintos e explicativos quanto aos riscos que estão incorrendo.

3.3.3. Comunicações e mensagens de alerta

Após o registro 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 a mais de 15 dias pode ocasionar um problema. Neste caso é recomendado que sejam revisitados para atualizar as informações do registro. Outro caso são os riscos que estão chegando no limite da data de proximidade. Podem ser realizados alertas ou comunicações aos responsáveis pelos riscos para que estes estejam no radar dos tomadores de decisão.

Por meio dos sistemas de informações podem ser criados alertas específicos por e-mail ou outro canal de comunicação para alertar os especialistas em riscos na condução de suas atividades. Estes lembretes corroboram para uma gestão mais eficiente.

4. LEIS E NORMATIVOS BRASILEIROS RELACIONADOS À GESTÃO DE RISCOS

Esta seção contém leis e normativos relacionados à Gestão de Risco encontrados em sites da administração pública a fim de apoiar os gestores quanto a recomendações e

obrigações em relação a gestão de ricos. Além disso, estes materiais devem ser lidos e entendidos em conjunto com as regulamentações e definições internas de cada organização.

Quadro 11 – Leis e normativos sobre Gestão de Riscos.

Legislação	Objeto/Assunto principal
LEI COMPLEMENTAR NO 101 (2000)	Estabeleceu que a Lei de Diretrizes Orçamentárias Anual (LDO) deve estabelecer meta de superávit 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 SIC e Comunicações
INSTRUÇÃO NORMATIVA GSI Nº 1 (2008)	Disciplina a Gestão de SIC e Comunicações na Administração Pública Federal, 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 Entidades da Administração Pública Federal
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 entidades da Administração Pública Federal
NORMA COMPLEMENTAR nº 06/IN01/DSIC/GSIPR (2009)	Estabelece Diretrizes para Gestão de Continuidade de Negócios, nos aspectos relacionados à SIC e Comunicações, nos órgãos e entidades da Administração Pública Federal, direta e indireta
NORMA COMPLEMENTAR nº 08/IN01/DSIC/GSIPR (2010)	Estabelece as Diretrizes para Gerenciamento de Incidentes em Redes Computacionais nos órgãos e entidades da Administração Pública Federal
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 Comunicações (SIC), dos órgãos e entidades da Administração Pública Federal, direta e indireta
NORMA COMPLEMENTAR nº 11/IN01/DSIC/GSIPR (2012)	Estabelece diretrizes para avaliação de conformidade nos aspectos relativos à SIC e Comunicações (SIC) nos órgãos ou entidades da Administração Pública Federal, 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 à SIC e Comunicações (SIC) nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta
NORMA COMPLEMENTAR nº 13/IN01/DSIC/GSIPR (2012)	Estabelece diretrizes para a Gestão de Mudanças nos aspectos relativos à SIC e Comunicações (SIC) nos órgãos e entidades da Administração Pública Federal, direta e indireta
NORMA COMPLEMENTAR nº	Estabelece diretrizes para a utilização de tecnologias de Computação em Nuvem, nos aspectos relacionados à SIC e

Legislação	Objeto/Assunto principal
14/IN01/DSIC/GSIPR (2012)	Comunicações (SIC), nos órgãos e entidades da Administração Pública Federal (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 entidades da Administração Pública Federal (APF), direta e indireta
NORMA COMPLEMENTAR nº 16/IN01/DSIC/GSIPR (2012)	Estabelece as diretrizes para o Desenvolvimento e Obtenção de Software Seguro nos Órgãos e Entidades da Administração Pública Federal, direta e indireta
NORMA COMPLEMENTAR nº 04/IN01/DSIC/GSIPR e seu anexo, (2013)	Diretrizes para o processo de Gestão de Riscos de SIC e Comunicações - GRSICC nos órgãos e entidades da Administração Pública Federal
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 as Diretrizes para as Atividades de Ensino em SIC e Comunicações (SIC) nos Órgãos e Entidades da Administração Pública Federal
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 administração pública federal 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 as Diretrizes para Implementação de Controles de Acesso Relativos à SIC e Comunicações, nos órgãos e entidades da Administração Pública Federal (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 entidades da Administração Pública Federal (APF), direta e indireta
NORMA COMPLEMENTAR nº 19/IN01/DSIC/GSIPR (2014)	Estabelece Padrões Mínimos de SIC e Comunicações para os Sistemas Estruturantes da Administração Pública Federal (APF), direta e indireta
NORMA COMPLEMENTAR nº 20/IN01/DSIC/GSIPR (2014)	Diretrizes de segurança da informação e comunicações para instituição do processo de tratamento da informação nos órgãos e entidades da administração pública federal
INSTRUÇÃO NORMATIVA SLTI/MP Nº 4 (2014)	Dispõe sobre o processo de contratação de Soluções de Tecnologia da Informação pelos órgãos integrantes do Sistema de

Legislação	Objeto/Assunto principal
	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 Administração Pública federal direta, autárquica e fundacional deverão ser realizadas por redes de telecomunicações e serviços de tecnologia da informação fornecidos por órgãos ou entidades da Administração Pública Federal, incluindo empresas públicas e sociedades de economia mista da União e suas subsidiárias, observando o disposto nesta Portaria
ACÓRDÃO TCU 4330 (2014)	Dispõe sobre gestão de riscos em contratações
DECRETO FEDERAL N. 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 2110 (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.

Esta lista está sujeita a mudanças e particularidades de cada órgão, portanto, recomenda-se que seja identificado para cada contexto as leis e normas vigentes a serem aplicadas para a gestão de riscos.

5. FERRAMENTAS DE SOFTWARE PARA GESTÃO DE RISCO

O alinhamento entre a fundamentação teórica e a concepção de ferramentas de cunho tecnológico mostra-se de fundamental importância para respaldar iniciativas de gestão em qualquer nível organizacional, considerando a natureza de seus processos, produtos, bem como, a realidade e a especificidade dos mais diversos cenários de atuação.

Sendo assim, para que a gestão de riscos possa ocorrer na organização são necessários alguns controles e centralizações de registros, a fim de permitir uma comunicação precisa, acompanhamento e controle dos riscos. Para isso, a Tecnologia da Informação desempenha um papel importante por permitir que esse conjunto de regras de negócio sejam operados da melhor forma, automatizando tarefas e disponibilizando uma interface para apoiar os gestores de riscos em suas atribuições.

O cenário quanto à gestão de riscos no setor público ainda está em desenvolvimento, por isso, foi realizada uma pesquisa utilizando-se da estratégia de

Benchmarking, para a avaliação de 27 ferramentas de software existentes no mercado, que se comprometem a criar processos e estratégias de gestão condizentes à realidade das organizações. Optou-se, de forma sintetizada, apresentar informações específicas sobre o módulo destinado à gestão de riscos em cada software pesquisado, assim como, informações de processos e estratégias que visam complementar o processo de gestão inicialmente citado.

Para que seja possível conhecer estas ferramentas, será disposto no Quadro 12 informações contendo o nome do software avaliado, seu website e se existe algum custo para a sua aquisição:

Quadro 12 – Ferramentas de software contempladas nesse estudo

Nome	Site	Custo de Aquisição
Eramba	http://www.eramba.org	Não
Open Risk	https://www.openriskmanagement.com	Não
OpenSource Risk	http://www.opensourcerisk.org	Não
Simple Risk	https://www.simplerisk.com	Não
ACL GRC	https://www.acl.com	Sim
ACCELUS	https://www.thomsonreuters.com	Sim
Active Risk Manager	http://www.sword-activerisk.com	Sim
Adaptive GRC	https://candf.com	Sim
Aris GRC	http://www2.softwareag.com	Sim
IntelligenceBank GRC	http://www.intelligencebank.com	Sim
BPS Resolver	http://www.resolver.com/	Sim
BRINQA	https://brinqa.com/	Sim
BWISE	http://www.bwise.com/solutions	Sim
TruComply	http://anxebiz.anx.com	Sim
Enablon	https://enablon.com/	Sim
IBM OpenPages GRC	https://www.ibm.com	Sim
I Touch Vision Governance & Risk	https://www.itouchvision.com	Sim
MasterControl	https://www.mastercontrol.com	Sim
MetricStream	https://www.metricstream.com	Sim
Optial Risk Management	http://www.optimalrisk.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
360factor	http://www.360factors.com	Sim

Fonte: Elaboração própria.

A análise das ferramentas de software disponíveis no mercado pode possibilitar, caso necessário, o desenvolvimento das especificidades e adequações de cenário no setor público brasileiro. Além disto, esta pesquisa se faz importante na contribuição ao desenvolvimento do próprio software e também para apoiar a comunidade, agregando novas particularidades que possam complementar ações de gestão de riscos.

Está registrado no Quadro 13, uma síntese com as principais informações do módulo de gestão de riscos e informações de processos e/ou módulos que complementem o processo supracitado. Esta lista de questões enumerada abaixo representa os itens da coluna “Informações sobre os módulos de Gestão de riscos” do Quadro 13:

1. O software permite a gestão completa de um determinado risco, desde a sua primeira detecção, até a sua devida solução e/ou aproveitamento. Permite uma gestão alinhada com os objetivos pré-estabelecidos de cada unidade / departamento ou da própria organização como um todo?
2. O software permite uma análise profunda das causas de um determinado risco, combinando técnicas de exploração de dados, objetivando permitir aos gestores utilizar estas causas, como fundamentação para tomada de decisão?
3. 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. Permite a personalização de métricas de avaliação, funcionalidades de avaliação e de telas de apresentação de dados mediante demanda de determinada organização
5. 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, permite a padronização de mecanismos de controle para garantir a continuidade de inciativas de gestão de riscos?
7. O software apresenta uma variedade interessante de medidas qualitativas e quantitativas para situar gestores sobre a maturidade de processos de controle de riscos? Exemplo: KPI, KRI.
8. A plataforma utiliza a gestão de processos de auditória como funcionalidade complementar à gestão de riscos?
9. Fornece a junção de um módulo de comunicação à gestão de riscos objetivando gerir o fluxo correto de informações e procedimentos à serem disseminados em toda à organização?
10. Permite a utilização de questionários para avaliação situacional e/ou para unir funcionalidades à gestão da comunicação?
11. Permite a gestão de leis e regulamentos vigentes para adequar a realidade organizacional, as exigências de mercado e de Governos?
12. Possuí módulo destinado à gestão pública?
13. Permite a conexão de múltiplos dispositivos, como por exemplo, celular, tablets, computadores?

Quadro 13 – Software avaliados e suas principais características.

Informações sobre os módulos de Gestão de riscos	360factor	ACCELUS	ACL GRC	Active Risk Manager	Adaptive GRC	Aris GRC	BPS Resolver	BRINQA	BWISE	Enablon	Eramba	I Touch Vision Governance & Risk	IBM OpenPages GRC	IntelligenceBank GRC	MasterControl	MetricStream	Open Risk	OpenSource Risk	Optial Risk Management	ORACLE GRC	ProcessGene GRC	RiskGAP	RIVO	RSA Archer	SAP GRC	Simple Risk	TruComply
1	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2			✓	✓	✓	✓		✓	✓	✓		✓	✓	✓		✓			✓	✓	✓		✓		✓	✓	✓
3	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓
4	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓			✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
5		✓	✓			✓	✓					✓	✓						✓	✓		✓		✓	✓	✓	
6	✓	✓	✓	✓	✓	✓			✓	✓			✓	✓	✓		✓	✓		✓	✓		✓	✓		✓	✓
7	✓		✓	✓	✓	✓		✓	✓	✓			✓			✓									✓		
8	✓	✓	✓	✓	✓	✓	✓		✓		✓	✓	✓	✓	✓	✓	✓		✓	✓	✓			✓	✓	✓	
9		✓	✓	✓	✓	✓			✓	✓	✓	✓	✓	✓	✓	✓				✓					✓		
10			✓			✓				✓		✓	✓	✓	✓												
11	✓	✓	✓	✓	✓	✓		✓	✓		✓					✓				✓	✓	✓		✓	✓		✓
12			✓			✓						✓															
13				✓			✓					✓	✓														

Fonte: Elaboração própria

Em consonância com aspectos já mencionados neste estudo, é possível observar que as ferramentas de software que se comprometem a realizar e respaldar processos e iniciativas de gestão de riscos partilham, de certa forma, de uma metodologia genérica e comum para a realização desta incumbência.

Como é possível visualizar em informações dispostas no Quadro 13, a abordagem utilizada pela maioria dos aplicativos de gestão de riscos, difere-se apenas na amplitude em que a análise e a gestão de riscos pode ocorrer. Em alguns, considera-se a organização como uma entidade única e com objetivos de gestão específicos e alinhados à toda a empresa. Já em outros, opta-se por observar os níveis organizacionais e departamentos, respeitando objetivos específicos para a realização/execução desta iniciativa.

Ainda, observa-se a existência de procedimentos complementares ao processo de gestão de riscos. Como exemplo, cita-se: a utilização de métricas de avaliação para situar e apresentar dados relevantes em formato de relatórios ou telas de apresentação; a centralização de informações, que consiste em uma propriedade impactante no desenvolvimento de software ou iniciativas ligadas a gestão de riscos; e a facilidade de exploração destes dados para encontrar informações e conhecimentos relevantes.

Quanto à possibilidade de acrescentar características positivas de modelos e/ou gestões de fatores distintas a de riscos, pode-se aferir que em quase todos os aplicativos há ou um módulo específico para a gestão da comunicação, ou processos que permitam o fluxo de informações indispensáveis para o sucesso de ações de gestão, como exemplo, notificações direcionadas, entrega de notícias através do serviço de e-mails, entrega de relatórios diários, dentre outros.

Garantir a disponibilidade de informações organizacionais a gestores e colaboradores inseridos em qualquer iniciativa de gestão é de fundamental importância para o alinhamento correto de ações em prol de um objetivo de controle. Além disso, funcionalidades como questionários e outras avaliações visam garantir o envolvimento de todos e o feedback dos mais diversos níveis organizacionais. É um elemento que garante a multidisciplinaridade para a gestão e sua efetiva adequação à realidades e cenários específicos.

Outro elemento que se destaca nas ferramentas de software é a utilização de módulos específicos para auditorias, que se configuram como processos metódicos de verificação e adequação de procedimentos. Este elemento é de suma importância para se aferir o sucesso na empregabilidade de iniciativas de gestão, já que permite avaliar criticamente um cenário em busca de procedimentos que impulsionem melhorias continuas, adequação de conduta, dentre outros fatores, que primem pela continuidade de processos.

Pode-se observar também, a massiva utilização de componentes extras para realizar a verificação de regulamentações vigentes, bem como, exigências legislativas que devem ser levadas em consideração durante as atividades de uma organização. Entretanto, é necessário ressaltar que, para a aplicabilidade destes processos de acompanhamento legislativo e de regulamentações, o módulo destinado a esta atividade deverá ser devidamente estudada e planejada para que se adeque às diversas realidades de mercado que podem influenciar processos e produtos das organizações.

6. A METODOLOGIA FORRISCO: GESTÃO DE RISCOS NO SETOR PÚBLICO

A metodologia FORRISCO foi elaborada de forma complementar à metodologia FORPDI – Plano de Desenvolvimento Institucional, e 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. No grupo do FORPLAD vem sendo discutido ações quanto à implantação da gestão de riscos nestas instituições.

O projeto que deu origem a este trabalho recebeu recursos da Fundação de Apoio à Cultura, Ensino, Pesquisa e Extensão de Alfenas – FACEPE, intitulado "Gestão de Riscos nas Universidades Federais: Elaboração de Modelo de Referência e Implantação de Sistema". Teve como principal objetivo apoiar as IFES em conjunto com o FORPLAD na disseminação e implantação da gestão de riscos. O projeto contou com um analista de planejamento especialista em gestão de riscos, um analista de sistemas, dois desenvolvedores e três auxiliares de desenvolvimento de software. Foi dividido em quatro etapas, sendo estas:

- Elaboração de um questionário para avaliação de maturidade;
- Avaliação das metodologias de gestão de riscos de mercado e as adotadas pela administração pública brasileira;
- Elaboração de uma metodologia de gestão de riscos adequada ao contexto nacional, a ser publicada em formato de livro;
- Desenvolvimento de um software para apoio aos gestores na condução da gestão de riscos;

Ao longo do projeto foi publicado um artigo 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 parciais quanto a aplicação do questionário. Este trabalho não era foco do projeto, mas permitiu o aumento do engajamento dos participantes do projeto e criar sinergia com outras iniciativas e projetos de interesse das IFES.

6.1. Etapas da execução da gestão de riscos

Para estas etapas sugere-se que seja pensado em quais atividades são genéricas e quais são específicas à gestão de riscos, e também, quais são de nível macro e de nível micro. Para isso foi elaborado a Figura 14 contendo a representação destas atividades.

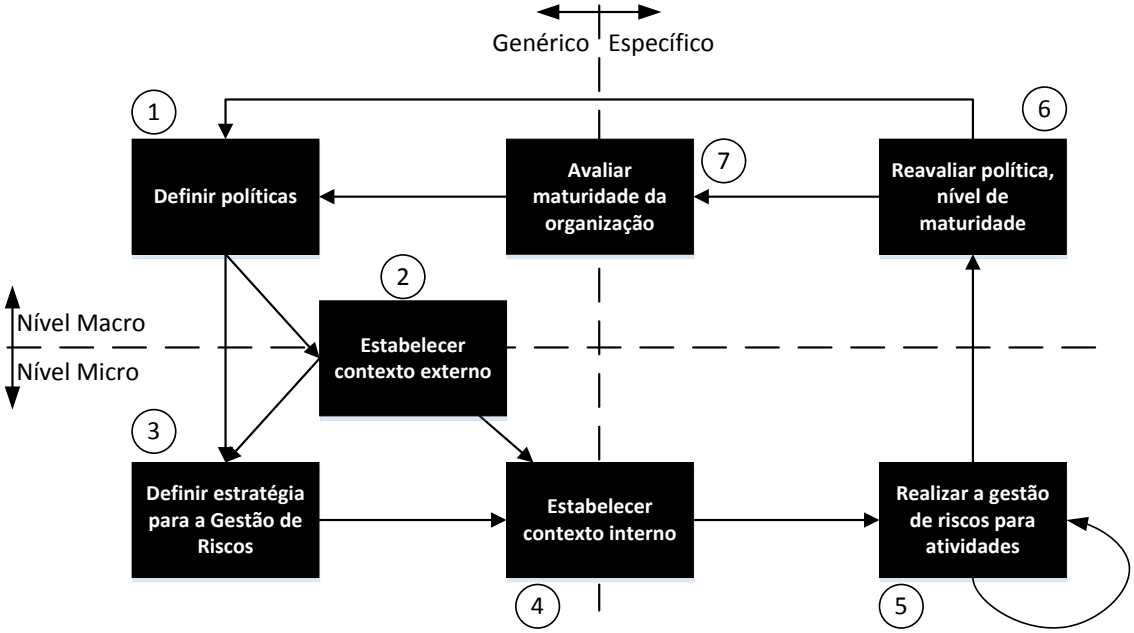

Figura 14 – Grande visão das etapas
Fonte: Elaboração própria

Recomenda-se como passos globais para a condução da gestão de riscos que sejam executados na seguinte ordem:

1. Definir a política de gestão de riscos em nível organizacional;
2. Estabelecer o contexto externo seguindo as orientações do GIRC, para identificar e entender as leis e normativos 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. Esta estratégia apoia para delinear os objetivos e resultados que se espera para os processos de negócio e projetos;
4. Estabelecer o contexto interno considerando as habilidades, capacidade, estratégia, contexto externo e política. Recomenda-se concluir as tarefas do MGR-SISP quanto ao passo "1. Estabelecer contexto", e definir as pessoas para os papeis 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 no processo "Etapas do processo da Gestão de Riscos";
6. Reavaliar a cada ano, ou quando necessário, a política, legislação, nível de maturidade e realinhar as ações quanto à gestão de riscos na organização;
7. Avaliar a maturidade da organização segundo as orientações do IBGC e também usando o questionário presente no Apêndice I.

A partir do entendimento da forma geral para a implantação da Gestão de Riscos, serão detalhados os componentes mais essenciais. As etapas dos processos da gestão de riscos possuem quatro componentes "Entradas", "Técnicas", "Objetivos, processos e tarefas" e "Saídas". Ao longo da execução do processo a saída de uma etapa anterior se torna a entrada

para a etapa seguinte. As técnicas darão o suporte necessário para apoiar os passos e tarefas da etapa no alcance das saídas. A Figura 15 representa este modelo.

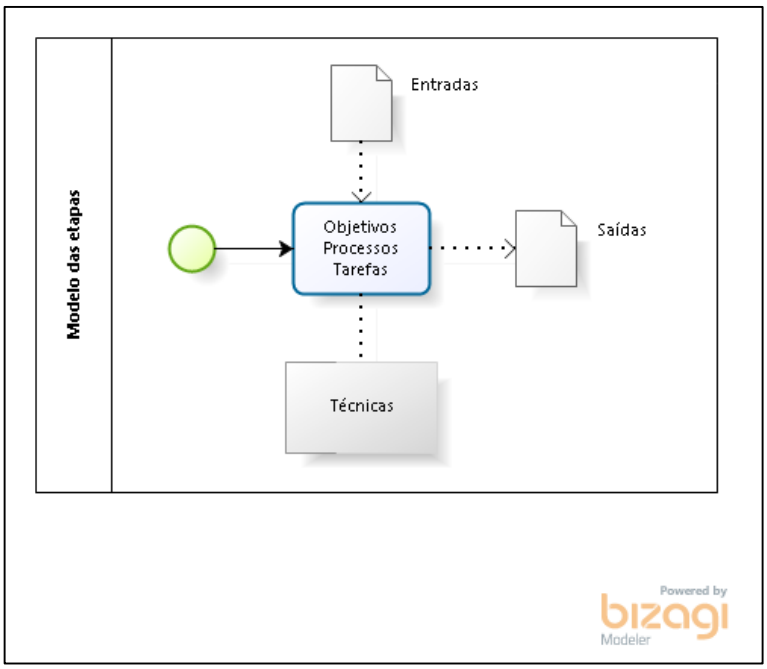

Figura 15 – Modelo das etapas
Fonte: Elaboração própria

É necessário que sejam executadas atividades antes de se iniciar as etapas da gestão de riscos. Recomenda-se que nesta etapa sejam usadas as informações do GIRC e IBGC. Para se entender e identificar o contexto externo pode-se utilizar um conjunto de técnicas para angariar informações importantes ao negócio e na realização das atividades desta organização. No processo da Figura 16 são sugeridas algumas técnicas, mas deve-se avaliar o que melhor se aplica para a identificação do contexto externo. Para esta etapa será utilizada como entrada informações quanto a regulamentações presentes em leis e normativos, documentos direcionadores como planos e políticas da organização, lições aprendidas em outras ocasiões e questões que se aplicam ao cenário. Como saída, será definido uma estratégia para conduzir as atividades da organização, aqui dividas entre projetos e processos, mas não limitadas a estes componentes.

Quanto aos projetos recomenda-se metodologia própria para o gerenciamento destes projetos, mas entende-se que ao final dos projetos serão entregues produtos ou serviços, e que, caso se tornem um serviço interno passará ao rol dos processos de negócio, e para estes deve-se ter outro conjunto de controle adequado. A gestão de riscos nos projetos ocorre ao longo de toda sua trajetória, sendo: 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 uma comunicação precisa e acompanhamento quanto às restrições dos projetos. Por fim, como os projetos são únicos deve-se garantir controles para que se acerte de primeira, evitando retrabalhos e custos adicionais.

Para os processos de negócio é necessário seu entendimento e controle. O mapeamento 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 pode-se 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 estas entregas precisam oferecer. Pode-se usar a técnica SIPOC (*Supplyer*, *Input*, *Process*, *Output*, *Customer* – Fornecedor, Entrada, Processo, Resultado, Cliente) para se ter um melhor entendimento destes processos. Os riscos quanto a estes processos devem possuir uma estratégia própria com vistas ao resultado do processo. Por fim, como os processos são contínuos deve-se buscar sua melhoria ao longo do tempo.

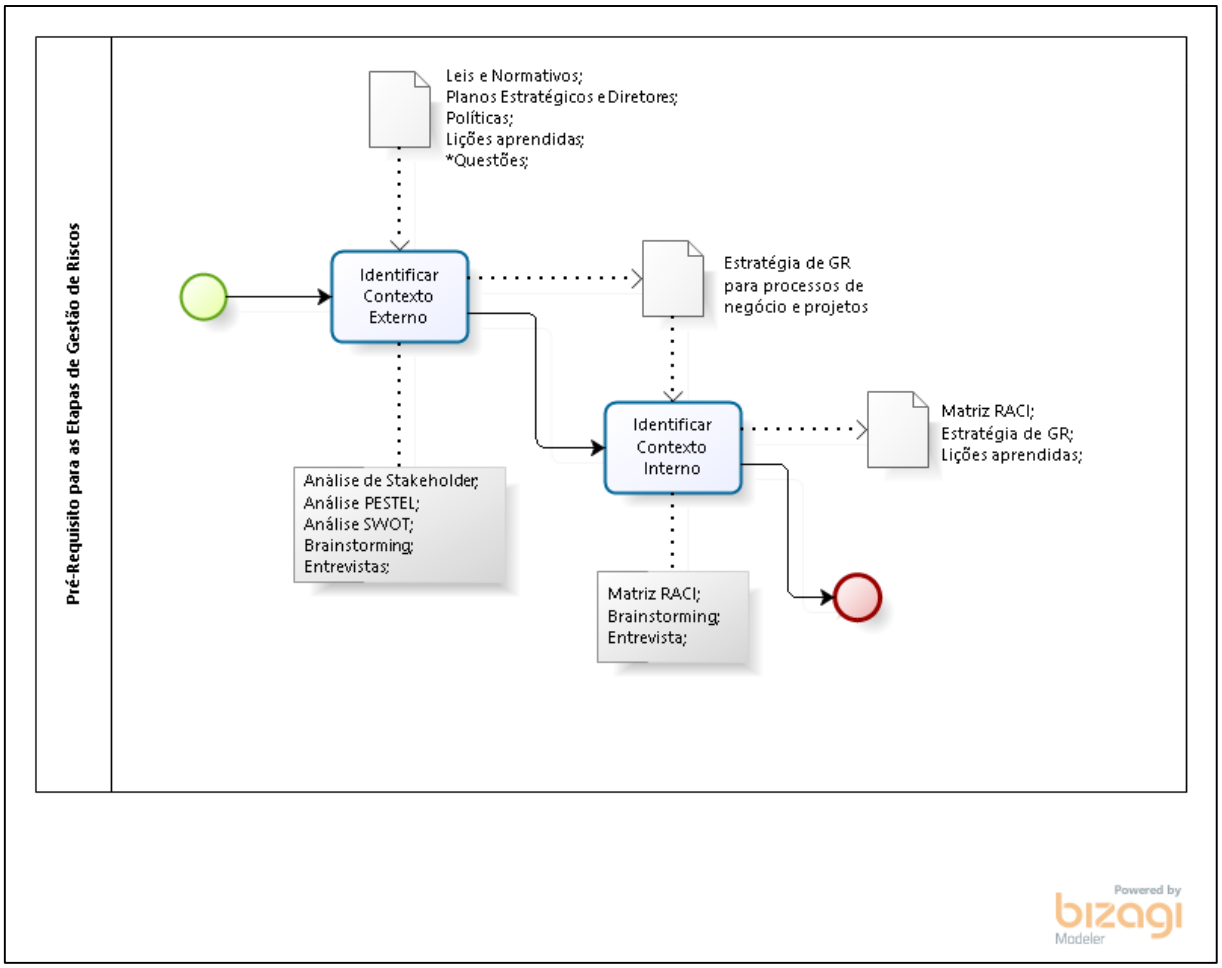

Figura 16 – Pré-requisitos para etapas da Gestão de Riscos
Fonte: Elaboração própria

Uma vez entendido o contexto, será iniciado as etapas do processo de gestão de riscos, presente na Figura 17. Recomenda-se nesta etapa que sejam usadas as informações das atividades presentes no MGR-SISP. O primeiro passo desse processo é "Identificar e Avaliar Risco", para isso recomenda-se usar como entrada as regras do órgão, a política e estratégia dos processos de GR, as responsabilidades dos participantes em forma de matriz RACI, as lições aprendidas e questões, entre outras informações que auxiliem nesta identificação e avaliação. Como técnicas para executar esta etapa sugere-se a matriz probabilidade e impacto, *brainstorming*, avaliação de impacto, probabilidade e proximidade, avaliação de valor esperado para tratamento, entre outras técnicas. Para esta etapa a principal saída é o registro do risco, que acumulará informações ao longo de todo processo. Também pode ser gerado um mapa de riscos e lições aprendidas como resultados auxiliares desta etapa.

Uma vez 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. Ao fazer isso haverá a garantia que o monitoramento e controle estejam ocorrendo. Nesta mesma linha podem ocorrer alterações no planejamento para o devido tratamento do risco. Os riscos podem ser acompanhados pela ferramenta "mapa de riscos" apresentada na seção 3.3.

A etapa de planejamento 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 e atividades que devem executar. Minimamente esta saída deve conter o dono do risco, responsável por controlar e monitorar este risco, o agente do risco, responsável por executar o plano de tratamento, o registro do risco, para continuar acumulando informações quanto ao risco, e o plano de resposta, contendo 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. Neste caso será usado como entrada as informações do registro do risco, contendo o dono do risco, o agente do risco e seu plano de resposta. Como técnica de apoio sugere-se que seja atualizado mapa de riscos. Como saída deve ser elaborado um relatório de progresso do tratamento do risco, e outros relatórios sumarizados. Estes relatórios contribuem para o monitoramento e controle para as partes interessadas.

Por meio desses processos acredita-se que a gestão de riscos será conduzida de maneira adequada. As etapas de monitoramento e controle devem ocorrer ao longo de todo processo, mas como não possuem uma entrada específica e um resultado definido optou-se por não escrever estes processos. Para o monitoramento e controle, o registro de risco e o relatório de progresso são componentes essenciais para que seja possível o acompanhamento adequado. Sobre a etapa do controle, de tempos em tempos devem ser realizadas as atividades de revisão dos processos, atualizações quanto às políticas e diretrizes, e reavaliação da maturidade para definir as ações de melhoria quanto à gestão de riscos. Para este caso de reavaliação recomenda-se a utilização do modelo de maturidade do IBGC em conjunto com o questionário do Apêndice I.

Para não tornar o processo de gestão de risco moroso deve-se garantir que a ferramenta de registro de riscos forneça uma interface descomplicada, com as informações minimamente necessárias para a condução da gestão de riscos, mas ao mesmo tempo permitindo que seja completa para dar visibilidade do estado atual do risco, sua magnitude, e também fornecendo um histórico dos riscos. Neste sentido, foi pensado um conjunto de variáveis para compor um formulário que será apresentado no Apêndice II.

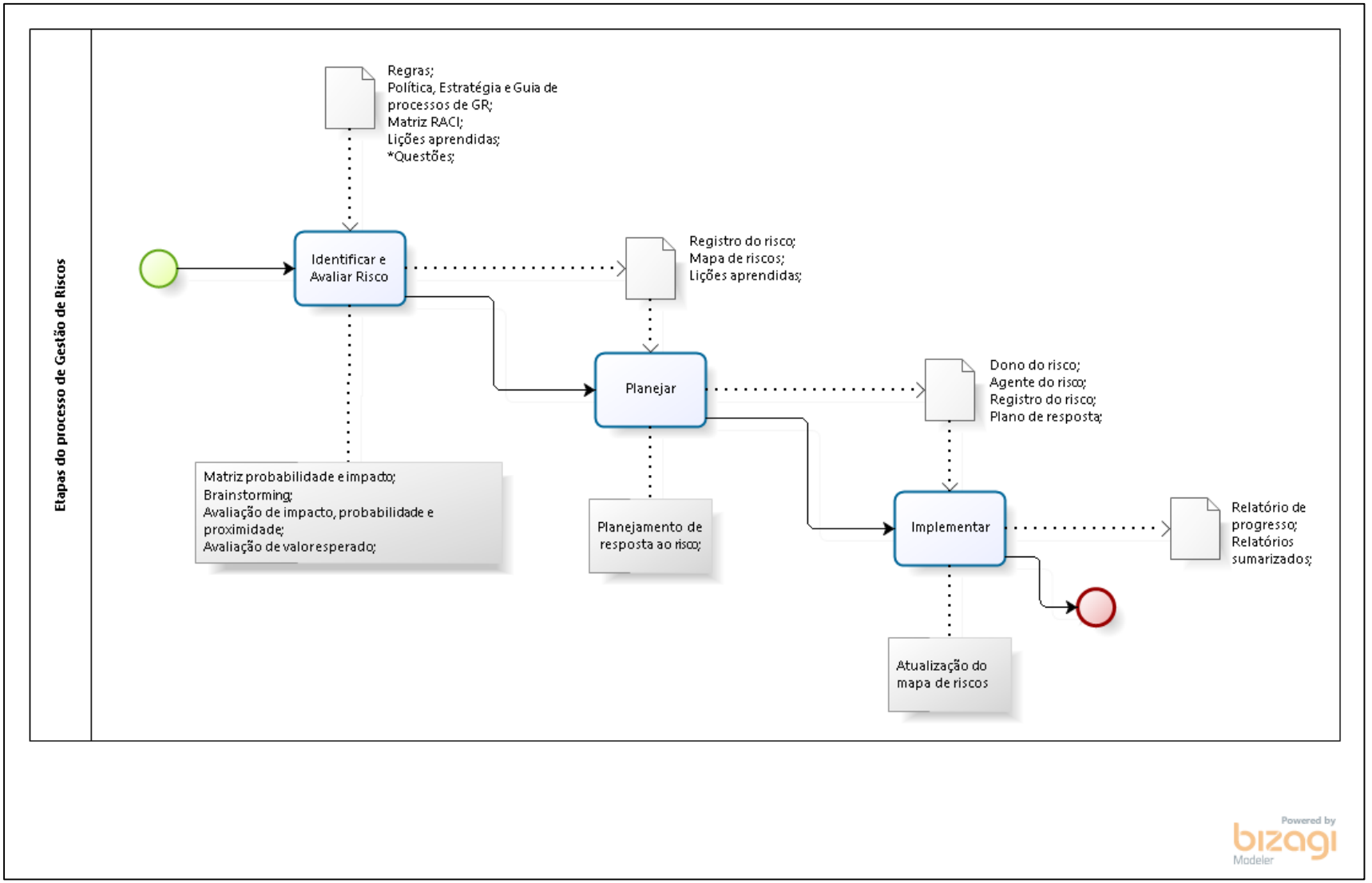

Figura 17 – Etapas do processo de gestão de riscos
Fonte: Elaboração própria

6.2. Exemplo da aplicação da metodologia FORRISCO

Nesta seção serão apresentados dois casos práticos da aplicação da metodologia de gestão de riscos FORRISCO. Deve-se usar como apoio as orientações e etapas presentes no capítulo 6.1.

6.2.1. 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 a gestão de riscos ainda é baixa e possivelmente os principais stakeholders ainda não estão envolvidos com estas iniciativas.

Neste cenário é necessário que se ganhe o patrocínio da alta gestão, que pode ser apoiado pelas obrigações quanto as legislações presentes no capítulo 4 – Leis e normativos brasileiros relacionados à gestão de riscos. Em seguida, é necessário oficializar, por meio de portaria ou documento equivalente, a política da gestão de riscos na organização.

Após essa oficialização, é interessante 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 acompanhamento futuro.

Para a identificação do contexto externo é necessário que sejam levantadas as leis, normativos e obrigações que esta instituição deve seguir. Existem casos que obedecem aos órgãos superiores, ou orientações de organismos internacionais. Estas definições de contexto externo variam de órgão para órgão, ou por regras dos estados brasileiros, ou outras definições.

Com este conjunto de informações é possível traçar uma estratégia para a gestão de riscos, que dependerá deste contexto e do tipo de risco que se irá enfrentar. Por exemplo: riscos de saúde serão tratados de forma diferentes 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 processos passarão por análises constantes. Estas análises podem ocorrer de forma espontânea na qual as pessoas interagem e percebem eventos ou também agendadas para que foquem nestas questões. Identificados estes eventos que causam incertezas é necessário realizar o registro deste evento, e para isso pode-se utilizar as técnicas sugeridas. Uma vez identificado este risco sugere-se que se escrito na forma Causa→Risco→Consequência ou Evento→Risco→Efeito. Isso facilita a reflexão e entendimento do cenário. Neste momento o registro do risco começa a ser preenchido com as melhores informações presentes até o momento.

Com o risco registrado será executado uma análise, que irá detalhar o risco para seu entendimento, de forma individualizada. Neste caso serão preenchidas as informações quanto ao impacto, probabilidade, proximidade e, se houver, o valor esperado para tratamento. Estas informações ajudam a definir este risco, e também permitir que possam ser comparados com outros riscos a fim de desenvolver primeiro os mais urgentes, e isto corre na etapa de avaliação de riscos. Ou seja, a avaliação de risco considera vários riscos em conjunto.

Uma vez avaliados os riscos, aqueles mais graves devem possuir um plano de tratamento. Quanto mais grave o risco, melhor e mais detalhado deve ser seu plano. Os riscos

mais brandos não necessitam obrigatoriamente de planos de tratamento, já os mais graves são mandatórios que existam estes planos.

A qualquer momento que o risco se materializar (transformar em questão), ou ultrapassar o limite de tolerância o plano de riscos deve ser implementado e será necessário o controle e monitoramento destes riscos.

Os riscos devem ser continuamente reavaliados, a fim de permitir que seu último estado esteja representado na ferramenta e que haja uma comunicação precisa quanto a estes riscos. Esta reavaliação faz parte da etapa de monitoramento.

Estes 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, legislações e reavaliar a maturidade deste período para permitir melhorias futuras.

6.2.2. 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 seus processos mapeados. Para agravar o cenário os servidores e colaboradores estão sobrecarregados com atribuições e há uma carência de recursos humanos e materiais na organização.

Existe conhecimento e vontade da alta administração quanto a aplicação da gestão de riscos, mas a força de trabalho para condução das atividades de riscos é escassa. Uma possível saída para este cenário é a otimização de tempo dos envolvidos para que a gestão de riscos não seja um estorvo às equipes.

O software de gestão de riscos será de fundamenta importância para automatizar notificações, lembrar prazos e datas, centralizar as informações quanto aos riscos e poupar tempo dos envolvidos.

Neste caso os gerentes devem acompanhar com mais frequência estes riscos, acessando a ferramenta diariamente para dar os devidos andamentos. Deve-se evitar reuniões com muitos participantes, apenas os responsáveis ou representantes devem estar nestas reuniões. É necessário que haja uma responsabilização para os participantes e uma cobrança para que deem o andamento nos riscos.

Mesmo sem os processos mapeados, as etapas de identificação e avaliação de riscos podem ocorrer. Estas etapas irão ajudar no planejamento e tratamento dos riscos, além de monitoramento e controle.

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

A gestão de riscos não é a solução para todos problemas organizacionais, mas permite que seja criada uma estrutura de registro e acompanhamento para que 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 estarão cobrando o desenvolvimento destas ações, e estar em conformidade com estas orientações é de suma importância para a organização.

7. CONSIDERAÇÕES FINAIS

A gestão de riscos corrobora para uma reflexão quanto às incertezas que influenciam a organização. Dirimir incertezas é uma necessidade que os gestores têm, para que possam entregar os resultados necessários à organização. O momento atual é muito rico e promissor quanto ao desenvolvimento do assunto, tanto no setor privado quanto público. Metodologias e outras publicações têm sido desenvolvidas para atender a essa necessidade de alterar a cultura de uma organização, envolvendo todos os níveis da estrutura organizacional, de modo que reflitam sobre os empecilhos e dificuldades na execução das atividades, e suas possíveis consequências. As instituições públicas e as instituições de ensino superior também estão no rol das organizações que podem receber os benefícios destas práticas de gestão.

Este material traz uma contribuição ao elencar as principais metodologias de gestão de riscos presentes no mercado e amplamente adotadas por organizações ao redor do mundo. Também contém as metodologias de gestão de riscos mais recentes no âmbito nacional e que podem ser amplamente aplicadas na administração pública. Outra contribuição é a lista de normas e legislações relacionadas à gestão de riscos, que geralmente encontram-se dispersas. Adicionalmente, a avaliação de ferramentas de software sobre gestão de riscos contribui para que seja percebido quais principais características devem conter em um sistema de informação para apoiar esta gestão. E finalmente, a própria metodologia do FORRISCO apresenta um relacionamento entre estes fatores para viabilizar um software em conjunto com uma forma de trabalho, bem como um instrumento para aferir o nível de maturidade da organização.

Em trabalhos futuros recomenda-se que seja avaliado o desempenho da organização antes e após a aplicação da metodologia FORRISCO, e também uma avaliação entre organizações que adotaram diferentes metodologias a fim de medir suas respectivas performances. Os fatores chave de sucesso identificados nestas avaliações permitirão uma evolução do FORRISCO, e uma maior assertividade em futuras implementações.

Por meio da gestão de riscos deseja-se que mais valor seja agregado à organização, resultando em melhorias na entrega de produtos e serviços das organizações públicas aos cidadãos brasileiros.

REFERENCIAS 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. 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
4. Boyne GA (2002) Public and private management: what's the difference? J Manag Stud 39:97–122. doi: 10.1111/1467-6486.00284
5. ABNT (2009) ABNT NBR ISO 31000 Gestao de Riscos - Princípios e Diretrizes. Associação Brasileira de Normas Técnicas
6. Murray MA (1975) Comparing Public and Private Management: An Exploratory Essay. Public Adm Rev 35:364–371.
7. BRASIL (2016) Instrução Normativa N 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 (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, 2º ed. Ministério do Planejamento Desenvolvimento e Gestão, Brasília, DF
10. Power M (2009) The risk management of nothing. Accounting, Organ Soc 34:849–855. doi: 10.1016/j.aos.2009.06.001
11. Power M (2004) The risk management of everything. J Risk Financ 5:58–65. doi: 10.1108/eb023001
12. 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
13. IBGC (2017) Gerenciamento de Riscos Corporativos: Evolução em Governança e Estratégia. IBGC, São Paulo
14. 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
15. HM Treasury (2009) Risk Management asse s sment framework: a tool for departments. 38.
16. U.S. (2016) Risk Management. United States - Government Accountability Office. Homeland Security. online.
17. CANADA (2010) Framework for the Management of Risk. Treasury Board of Canada Secretariat. 10.
18. BRASIL (2013) Gestão de riscos de segurança da informação e comunicações - GRSIC,

1º ed. Presidência da República - Gabinete de Segurança Institucional - Departamento de Segurança da Informação e Comunicações, Brasília, DF

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

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

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

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

APÊNDICE I – QUESTIONÁRIO

Foi elaborado um questionário para medir o nível de maturidade e aderência às práticas de gestão de riscos na organização. Este questionário estava dividido em quatro etapas: uma etapa preliminar para identificar o tipo de respondente, sendo este um responsável pela gestão de riscos, e neste caso desejava-se coletar informações quanto a gestão de riscos, ou um participante que não era responsável pela gestão de riscos na organização, e neste caso desejava-se coletar a percepção quanto a gestão de riscos; a segunda etapa continha perguntas específicas sobre gestão de riscos e só foi respondida pelos responsáveis de gestão de riscos, para estes casos buscou-se por meio de 32 perguntas dos oito princípios do M_o_R medir estas características; a terceira etapa coleta de todos os respondentes informações quanto a organização em que trabalham, seus colaboradores, e suas percepções quanto a gestão de riscos; finalmente, a quarta etapa coleta informações dos respondentes, e se estes desejam receber os resultados das análises.

Após esta primeira rodada do questionário, recomenda-se que sejam aplicadas novamente para medir evoluções e pontos de melhoria nestes ambientes.

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 a Gestão de Riscos estão definidas na Instrução Normativa Conjunta MP/CGU 01/2016 que completou 1 ano de vigência em 10/05/2017.

Este questionário é parte integrante de 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), 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, essa pesquisa visa realizar uma avaliação independente sobre Gestão de Riscos Organizacionais nas Instituições Federais de Ensino e demais órgãos da Administração Pública.

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

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.

As respostas enviadas até 20/06/2017 serão consideradas 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 Gestão de Riscos Corporativos

Esta seção contém questões quanto a Gestão de Risco Corporativo.

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 não deseje responder o 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 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, 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 se reflete ao contexto organizacional (abrangente, pertinente, viável, seguida).
Envolvimento das partes interessadas da sua instituição na gestão de riscos	No processo de identificação de risco é considerada a percepção das partes interessadas, suas atitudes e 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.
	Utiliza-se uma política de gerenciamento de riscos para a organização em questão.

Princípios	Item
Existência de um Processo de Gestão de Risco bem definido	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 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 em questão.
	As práticas são revisadas em face à 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, estrutura e conteúdo definidos para apresentar ações de revisão quanto ao tratamento de riscos.
Criação de uma cultura colaborativa quanto a 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 a 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 evidencias 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 contém perguntas abertas sobre as metodologias de gestão de riscos adotadas e uma escala de 1(Mais baixa) a 5(Mais alta) com a frequência com que mão de obra externa é contratada.

Pergunta	Tipo de resposta
Indique quais são as metodologias, técnicas ou 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 colaboradores

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

Afirmativa/ Questão	Item	Tipo de Resposta
Indique o seu grau de concordância com as sentenças a seguir:	A missão, visão e 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, visão e valores da minha instituição são formalizados e comunicados internamente e externamente.	
	A soma das metas a serem alcançadas refletem 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 a seguinte afirmação 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 para sua remuneração total (ex. carreira, salário, etc.) as métricas de desempenho a seguir?	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 de "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 em relação à excelência no trabalho.	
	Na conduta moral dos colaboradores.	

Esta seção contém questões abertas quanto a 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, dificuldades e 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 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 essa pesquisa, os resultados desse 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 essa 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 risco e deve conter um conjunto de informações para permitir o acompanhamento e 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 monitoramento destes riscos de forma individual. A seguir encontra-se um breve descritivo dos seus principais componentes:

Quadro 14 – 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 título obedecendo a sugestão: 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 empresa.
Categoria do risco	Os riscos devem ser classificados como: Estratégico, quando têm a possibilidade de afetar toda organização, Operacional, quando afetam apenas parte da organização, Orçamentário, quando estiver relacionado a aspectos financeiros, Reputação, quanto influenciar na imagem da organização, Integridade, quando afetar a honestidade e ética, Fiscal, quando influenciar em questões fiscais e contábeis, e Conformidade, quando estiver relacionada com o cumprimento de leis e regulamentos.
Descrição do risco	Detalhamento do risco contendo informações como Evento/Causa - Risco - Efeito/Consequência, e outras informações pertinentes.
Departamento	Departamento mais afetado pelo risco. Geralmente o gerente deste departamento será o dono do risco.
Estado do risco	Em suma o risco pode estar ativo ou encerrado. Caso tenha sido encerrado pode ter sido tratado com sucesso, se transformado em questão, ou não ter acontecido.
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.
Opção de resposta ao risco	Diferentes respostas ao risco a ser adotado pela organização. Para os riscos negativos (Ameaças) foram propostos os seguintes tipos: • Evitar a ameaça; • Reduzir a ameaça; • Transferir o risco; • Aceitar o risco. Para as oportunidades foram propostos os seguintes tipos de resposta: • Compartilhar risco; • Explorar oportunidade;

Item	Detalhamento
	• Melhorar oportunidade; • Aceitar o risco.
Etapa	Estado atual do tratamento, conforme guia de processos. Para simplificação foram consolidadas as etapas de "Identificação de Contexto", "Identificação do Risco", "Estimativa do Risco" e "Avaliação do Risco" em uma única etapa chamada "Identificar e Avaliar Risco". Foram mantidas as etapas de "Planejar Tratamento" e "Implantar Plano".
Dono do risco	Responsável principal por coordenar todas as ações do risco.
Agente do risco	Responsável por executar ações do risco.
Probabilidade	Chance de ocorrência do risco. Esta escala varia e 1 (Menos provável) a 5 (Mais provável).
Impacto	O impacto representa o resultado de uma ameaça ou oportunidade particular ocorrer realmente. 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	Foram adicionadas as funcionalidades de anexo e links externos para permitir a consolidação de informações em um único registro e para permitir o relacionamento com outros componentes, como os documentos de plano de tratamento de riscos e outras informações.

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

GLOSSÁRIO

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

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

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

Des-benefício
Resultado percebido como negativo por um ou mais stakeholders. São consequências de atividades nas quais, por definição, um risco possui alguma incerteza frente à sua materialização.

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 que informar sempre e nada ficará retido, evitando este vazamento.

Explorar
Tipo de resposta a risco positivo (oportunidade) 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 então no planejamento e implementação de respostas aos riscos. Provê um ambiente disciplinado para tomada de decisão proativa.

Impacto
Resultado de uma ameaça ou oportunidade particular ocorrer realmente.

Indicador Chave de Desempenho (KPI - *Key Performance indicator*)
Medida de desempenho que e utilizada para ajudar a organização a definir e avaliar quanto sucesso têm 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.

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

Nível de maturidade
Um platô evolucionário definido rumo ao atingimento de um processo amadurecido. Geralmente são citados 5 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 se dará 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 circunstâncias do mundo real. Resultados são desejados quando as

mudanças são concebidas. São atingidos quando atividades alcançam o resultado no efeito da mudança.

Risco – MOF
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 a magnitude do seu impacto nos objetivos.

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