

Mariana Bicalho Machado

**TAXONOMIA DE EVENTOS DE RISCO OPERACIONAL DO  
PODER JUDICIÁRIO**

**Brasília – DF**

**Março/2018**

# **TAXONOMIA DE EVENTOS DE RISCO OPERACIONAL DO PODER JUDICIÁRIO**

Trabalho de Conclusão de Curso apresentado  
como parte dos requisitos para a obtenção do  
título de Especialista em Gestão Pública.

Autora: Mariana Bicalho Machado  
Orientador: Prof. Dr. Humberto Falcão  
Martins

**Brasília - DF**

**Março/2018**

# **TAXONOMIA DE EVENTOS DE RISCO OPERACIONAL DO PODER JUDICIÁRIO**

Aluna: Mariana Bicalho Machado

Gestão de Riscos. Taxonomia de Eventos. Poder Judiciário.

O escopo magno do presente trabalho é conceber uma linguagem comum aos órgãos do Poder Judiciário em relação à identificação de riscos operacionais, assim como o Acordo de Capital de Basileia II fez com o sistema bancário internacional. Tal desiderato se justifica ao se verificar a escassez de experiências de gestão de riscos nos tribunais pátrios, em manifesto contraste à *expertise* apresentada pelo Banco Central do Brasil - BCB. A metodologia adotada previu ampla revisão bibliográfica acerca dos principais conceitos atrelados à gestão de risco, seus princípios e processo, bem como a sua relevância ao aprimoramento da governança pública. Após, perscrutou-se a experiência do BCB em gerir riscos operacionais, a partir das diretrizes estabelecidas por Basileia II. Ao final, examinaram-se algumas experiências relevantes encontradas na Justiça brasileira, as quais, em conjunto com os subsídios teóricos levantados, permitiram a proposição de uma taxonomia de eventos de risco operacional ao Poder Judiciário.

## SUMÁRIO

1. INTRODUÇÃO	4
2. JUSTIFICATIVA	4
3. METODOLOGIA	5
4. FUNDAMENTAÇÃO TEÓRICA	6
4.1 Conceito de Risco	6
4.2 Risco Operacional	8
4.3 Definição de gestão de riscos	11
4.4 Princípios e processo de gestão de risco	12
4.5 Histórico da gestão de riscos	16
4.6 Gestão de riscos como mecanismo fundamental de governança no setor público	20
4.7 O Acordo de Basileia II e sua contribuição à gestão de riscos operacionais no setor financeiro internacional	23
4.8 A implementação do Acordo de Basileia II pelo Banco Central do Brasil	27
4.9 Análise da gestão de riscos no contexto do Poder Judiciário brasileiro	32
5. PROPOSTA DE TAXONOMIA DE EVENTOS DE RISCO OPERACIONAL DO PODER JUDICIÁRIO	36
6. CONCLUSÃO	42
7. REFERÊNCIAS BIBLIOGRÁFICAS	44

## **1. INTRODUÇÃO**

Atualmente, um dos maiores desafios enfrentados pelo setor público brasileiro é o aperfeiçoamento dos mecanismos de governança. No Poder Judiciário, tal preocupação é traduzida como Macrodesafio da Estratégia Nacional, estabelecida pelo Conselho Nacional de Justiça para o período de 2015-2020.

Nesse contexto, destaca-se que a gestão de riscos é considerada um dos principais instrumentos de governança, em face de sua capacidade de aumentar a eficiência dos órgãos e entidades no tratamento de incertezas, contribuindo, assim, para o aprimoramento da geração de valor público.

Em que pese o seu destacado benefício, a implementação da gestão de riscos na área pública ainda se encontra em fase inicial, sendo esparsas e isoladas as experiências encontradas no Poder Judiciário. Esta pesquisa surge, portanto, como uma alternativa de modificação dessa realidade, ao propor a definição de uma taxonomia de eventos de risco operacional para a justiça brasileira.

O escopo magno do presente trabalho, portanto, é conceber uma linguagem comum aos órgãos do Judiciário em relação à identificação de riscos operacionais, assim como o Acordo de Capital de Basiléia II fez com o sistema bancário internacional. Dessa forma, busca-se facilitar a etapa de identificação de riscos pelos tribunais e aperfeiçoar os sistemas de controle interno, tendo, como fim último, possibilitar ao Conselho Nacional de Justiça, em um futuro próximo, realizar avaliações sistêmicas e integrais dos riscos operacionais da justiça brasileira.

## **2. JUSTIFICATIVA**

Ao se considerar o estágio inicial de discussão sobre gerenciamento de risco na administração pública e a baixa maturidade dos tribunais em inseri-lo em suas práticas de gestão, vislumbra-se alto potencial de desenvolvimento de metodologias dessa natureza na Justiça brasileira.

Nessa toada, ressalta-se o ambiente propício para o progresso de tal intento, face à atuação cada vez mais incisiva do Tribunal de Contas da União, que, gradualmente, tem aumentado as suas exigências em relação à necessidade de os órgãos gerenciarem riscos, firme na convicção da natureza estratégica desse processo às instituições.

Dessa forma, para a realização do supracitado objetivo pelos tribunais, mister o aprofundamento do estudo sobre o tópico, inclusive por meio da análise de experiências

exitosas de gestão de risco em organizações públicas, a fim de avaliar a possibilidade de adaptação de suas características à Justiça pátria.

Nesse sentido, tem-se que, no âmbito da administração pública brasileira, o Banco Central do Brasil - BCB destaca-se como uma autarquia com vasta *expertise* no tema, que remonta ao ano de 1997, quando formalizou as ferramentas para análise de riscos de crédito.

Atualmente, já formulou e implementou metodologia própria para gestão de riscos tanto estratégicos como operacionais, que, de forma conjunta, atuam no sentido de consolidar estrutura de governança hábil a aprimorar o processo de tomada de decisão.

Uma boa prática que avulta da experiência do BCB é a existência de um formulário com mais de 30 eventos de risco operacional previamente identificados, o qual é utilizado nas oficinas junto às unidades da autarquia como um norte aos servidores na etapa de levantamento e identificação de riscos, considerada a mais crítica dentro da metodologia prevista na ISO 31.000 (ABNT, 2009), a ser detalhada em tópico posterior.

Além de otimizar a aludida etapa, a taxonomia existente é comum a todo o sistema financeiro mundial, uma vez que proposta no Acordo de Capital de Basiléia II, documento considerado referência pelos bancos internacionais no tocante à definição de riscos operacionais. Assim, há a possibilidade de supervisão sistêmica e global dessa categoria de riscos, facilitando a avaliação e controle do gerenciamento do risco operacional em todas as instituições bancárias.

Nesse contexto, apropriando-se da experiência do BCB, o presente trabalho surge como uma alternativa de modificação da fase ainda conceitual de gestão de riscos encontrada no Poder Judiciário, a partir da proposição de uma taxonomia de eventos de risco operacional para a justiça brasileira.

### **3. METODOLOGIA**

A metodologia adotada pelo presente artigo centrou-se em realizar ampla revisão bibliográfica acerca dos principais conceitos atrelados à gestão de risco, seus princípios e processo, bem como a sua relevância ao aprimoramento da governança pública.

Consolidados os conceitos fundamentais à exata compreensão do tema, avançou-se ao aprofundamento da análise da experiência do Banco Central do Brasil, a fim

compreender como se deu a implementação das recomendações de Basiléia II relativas ao gerenciamento e controle de riscos operacionais.

Para tanto, fez-se necessário revisar a própria formulação dos Acordos de Basiléia, com o intuito de compreender a cronologia histórica da relevância do controle do risco operacional, seu conceito e técnicas de análise, no âmbito das instituições financeiras.

Em seguida, valendo-se da coleta de dados secundários, extraídos dos sítios eletrônicos dos tribunais brasileiros, buscou-se compreender como os órgãos do Poder Judiciário têm identificado e categorizado riscos, destacando-se as principais definições de riscos operacionais encontradas, suas fontes, características e formas de gestão, com o intuito de absorver as peculiaridades da justiça relativas ao gerenciamento de riscos.

De posse de todo o subsídio teórico levantado, foram selecionadas as fontes e as categorias de eventos operacionais mais aderentes à realidade do Poder Judiciário, bem como foi dado à autora da pesquisa conceber eventos customizados à rotina da justiça brasileira com base em todo o aprendizado realizado.

O objetivo, portanto, foi estabelecer uma taxonomia de eventos de risco operacional do Poder Judiciário, no formato de uma matriz hábil a ser aplicada nas unidades funcionais de cada Tribunal, a fim de possibilitar a universalização da linguagem e do entendimento acerca desta categoria de riscos, viabilizando o seu controle pelo Conselho Nacional de Justiça.

## **4. FUNDAMENTAÇÃO TEÓRICA**

### **4.1 Conceito de Risco**

A fim de realizar qualquer análise a respeito de gestão de riscos e avançar sobre as suas características principais, deve-se, primeiramente, compreender o próprio conceito de risco.

Para tanto, destaca-se que o risco é inerente à atividade humana, sendo, inclusive, “uma variável determinante da evolução [...], pois a sua ausência implica a certeza de resultados e a restrição à construção de conhecimentos” (HENTGES, 2012 apud WEBER, 2014, p. 42).

Nesse sentido, ressalta-se que, segundo Bernstein (1997), risco deriva do italiano *riscare*, que pode ser traduzido como *ousar*. Dessa forma, o autor salienta que risco “é uma opção, e não um destino”.

É possível considerá-lo uma opção, vale destacar, porque risco é compreendido como “um evento futuro **identificado**, ao qual **é possível** associar uma distribuição de probabilidades de ocorrência” (FABER et al., 1996 apud IBGC, 2017, p. 11, grifo nosso).

Dessa forma, o conceito se diferencia do de incerteza e mesmo de ignorância, os quais podem ser assim definidos:

**“Incerteza:** evento futuro identificado, ao qual **não é possível** associar uma distribuição de probabilidades de ocorrência.

**Ignorância:** eventos futuros que, no momento da análise, **não poderão sequer ser identificados, muito menos quantificados**”. (FABER et al., 1996 apud IBGC, 2017, p. 11, grifo nosso)

Em outras palavras, “riscos descrevem situações nas quais probabilidades são avaliadas, enquanto incertezas referem-se a situações em que a informação é muito imprecisa para ser colocada como probabilidade” (KNIGHT, 1921 apud MORAES, 2017, p. 23).

Nessa toada, de acordo com a ABNT ISO 31.000 (2009, p. 1), o risco é o “efeito da incerteza nos objetivos”, isto é, envolve a “quantificação e a qualificação da incerteza, tanto no que diz respeito às perdas quanto aos ganhos” (IBGC, 2017, p. 11).

Assim, é possível avaliar o efeito da incerteza - isto é, o desvio em relação ao planejado – sob duas óticas: a positiva e a negativa. Os eventos hábeis a gerar impacto negativo representam riscos que podem inibir a geração de valor ou ainda eliminar o valor existente. Os de impacto positivo, por outro lado:

“podem contrabalançar os de impacto negativo ou podem representar oportunidades, que, por sua vez representam a possibilidade de um evento ocorrer e influenciar favoravelmente a realização dos objetivos, apoiando a criação ou a preservação de valor. A direção da organização canaliza as oportunidades para seus processos de elaboração de estratégias ou objetivos, formulando planos que visam ao aproveitamento destes” (COSO, 2007, p. 4).

Em uma economia de mercado cada vez mais dinâmica e competitiva, as organizações encontram-se expostas a uma infinidade de riscos, que podem advir de fontes internas e externas, “como a adoção de uma estratégia equivocada, ser atingida por desastres naturais ou acidentes, ou ainda cair em desgraça aos olhos do público, seja por problemas de reputação, ou por problemas de mudança de preferências dos clientes” (CARVALHO, 2003 apud WEBER, 2014, p. 43).

Voltando a análise para a dimensão específica do setor público, os riscos podem ser:

“decorrentes da natureza de suas atividades, de realidades emergentes, de mudanças nas circunstâncias e nas demandas sociais, da própria dinâmica da administração pública, bem como da necessidade de mais transparência e prestação de contas e de cumprir variados requisitos legais e regulatórios” (BRASIL, 2017, p. 5)

Dessa forma, considerando as múltiplas fontes de riscos, diversas são também as categorias existentes para classificá-los, merecendo destaque as propostas por Crouhy et al (2008 apud WEBER, 2014, p. 44), que abrangem: (i) risco de mercado, (ii) risco de crédito, (iii) risco de liquidez, (iv) risco operacional, (v) risco legal e regulatório, (vi) risco de negócio, (vii) risco estratégico e (viii) risco de reputação.

Dentre as categorias de risco identificadas, o presente artigo limitará a sua análise ao risco operacional, em razão de seu gerenciamento apresentar manifesta relevância ao desenvolvimento institucional e ao aumento da eficiência na prestação do serviço público.

Sua importância, inclusive, foi ressaltada em pesquisa realizada em 2012 pela Câmara Americana de Comércio, com funcionários de mais de 140 empresas, na qual o risco operacional foi apontado como o mais importante (25,7%), tendo 33% das empresas respondido possuir área exclusiva para o controle de perdas potenciais (MORAES, 2017, p.16).

## **4.2 Risco Operacional**

Em primeiro lugar, salienta-se que, em face da miríade de eventos que podem levar ao risco operacional e do fato de não estar diretamente vinculado à atividade fim da organização, não há, na doutrina, definição consensual sobre o tema.

A título de ilustração, para Chorafas (2004, p. 4, tradução nossa), os riscos operacionais estão presentes em absolutamente todos os tipos de organizações, seja:

“O negócio regulado ou desregulado, centralizado ou descentralizado, procedimentalizado ou livre, de tecnologia antiga ou alta tecnologia, base local, nacional ou internacional; caracterizado por produtos simples ou por produtos complexos, ou de negociação através de um único canal ou múltiplos canais”.

Ao se deter sobre as suas possíveis fontes, Bergamini Júnior (apud SALGADO et al., 2010, p. 4) estabelece que o risco operacional é:

“Resultado de fraudes praticadas por empregados, falhas nos processos e nos sistemas informatizados, ocorrendo em função de desenho organizacional inadequado, falta de planejamento e de monitoração na delegação de poderes, de procedimentos sem conformidade e da obsolescência de produtos e processos”.

A abrangência de sua ocorrência permite à Marshall (2002, p. 40) afirmar que os “riscos operacionais se relacionam a todas as fases do processo de negócios, desde sua origem, até sua execução e entrega, abrangendo a linha de frente, o apoio intermediário e o *back office*”.

Nessa toada, Saunders (apud LIMA, p. 43) salienta que tais riscos se referem "à produção de suas operações e são fatores que influenciam em custos e receitas adicionais em decorrência da gestão e controle de recursos humanos e tecnológicos pelos administradores”.

O setor financeiro, por sua vez, apresenta definição mais consolidada, proposta pelo Acordo de Capital de Basileia II, posteriormente traduzida e normatizada pelo BCB como a “possibilidade de ocorrência de perdas resultantes de falha, deficiência ou inadequação de processos internos, pessoas e sistemas, ou de eventos externos” (BRASIL, 2006).

Salienta-se que uma forma de facilitar a compreensão do conceito de risco operacional é perscrutar os seus distintos tipos de eventos, os quais têm o condão de gerar perdas quando da exposição da organização ao risco.

Assim, com base nos quatro aspectos destacados na supracitada conceituação dada pelo BCB, a Federação Brasileira de Bancos - FEBRABAN (apud SALGADO et al., 2010, p. 04, grifo nosso) traz como exemplos de eventos de riscos operacionais os seguintes:

**“Processos** – falha no registro, processamento ou liquidação de transações, contas de clientes, negócios diários e falhas em relatórios obrigatórios.

**Pessoas** – perdas causadas por funcionários ou com participação indireta deles (intencional ou não) advindas de relacionamentos com clientes, acionistas ou terceiros.

**Sistemas** – perdas decorrentes de interrupção de negócios ou falha de sistemas, por indisponibilidade de infra-estrutura de TI.

**Eventos externos** – perdas causadas por terceiros, danos ao patrimônio ou ativos”.

Trabalhando o tema de maneira mais pormenorizada, Duarte propõe 16 categorias de eventos de risco operacional aos quais as instituições financeiras encontram-se expostas, abaixo compiladas:

Risco de <i>Overload</i>	Risco de perdas por sobrecargas nos sistemas elétrico, telefônico, de processamento de dados, etc
Risco de Obsolescência:	Risco de perdas pela não substituição frequente de equipamentos e softwares antigos
Risco de presteza e confiabilidade	Risco de perdas pelo fato de as informações não poderem ser recebidas, processadas, armazenadas e transmitidas em tempo hábil e de forma confiável
Risco de equipamento	Risco de perdas por falhas nos equipamentos elétricos, de processamento e transmissão de dados, segurança da informação, etc.
Risco de erro	Risco de perdas em decorrência de equívoco, omissão, distração ou negligência de funcionários
Risco de fraudes	Risco de perdas como resultado de comportamentos fraudulentos como adulteração de controles, descumprimento intencional de normas da empresa, desvio de valores, divulgação de informações erradas, etc
Risco de qualificação	Risco de perda pelo fato de os funcionários desempenharem tarefas sem qualificação profissional apropriada à função, como uso de estratégias de hedge com derivativos sem conhecimento, por parte do operador, das limitações correspondentes
Risco de produtos e serviços	Risco de perdas originário da venda de produtos ou prestação de serviços de forma indevida ou sem atender às necessidades e demandas de clientes, tal como envio de cartões de crédito sem a consulta prévia ao cliente
Risco de regulamentação	Risco de perdas diante de alterações, impropriedades ou inexistência de normas para controles internos e externos, tal como uma alteração de margens de garantia ou de limites de oscilação em bolsas de derivativos sem aviso antecipado
Risco de modelagem	Perdas pelo desenvolvimento, utilização ou interpretação incorreta de resultados fornecidos por modelos, inclusive a utilização de dados incorretos, tal como o uso de modelos matemáticos sem conhecimento de suas hipóteses simplificadoras
Risco de Liquidação financeira	Risco de perdas decorrentes de falhas nos procedimentos e controles de finalização de transações, tal como envio e recebimento de divisas em praças com diferentes fusos horários, feriados, regras operacionais, etc.
Risco sistêmico	Risco de perdas oriundo de alterações no ambiente operacional, tal como alteração abrupta de limites operacionais em bolsas, levando

	todas as instituições financeiras a dificuldades.
Risco de concentração	Risco de perdas pela dependência de poucos produtos, clientes e mercados, tal como uma instituição com receita concentrada em um único produto, dependente de habilidade operacional de um único operador, funding em um único mercado, etc.
Risco de imagem	Risco de perdas em decorrência de alterações na reputação junto a clientes, concorrentes, órgãos governamentais etc.
Risco de catástrofe	Perdas devido a catástrofes (naturais ou não) como enchente, incêndio e terremoto, que dificultem a continuidade operacional diária da instituição, processamento de dados, comunicação, etc.
Risco legal	Perda resultante de sanções por órgãos reguladores e indenizações por danos a terceiros, interpretação indevida de incidência de tributos, contratos omissos ou mal redigidos, etc

Tabela 1: Categorias de Risco Operacional de Instituições Financeiras

Fonte: Adaptado de Duarte (apud LIMA, 2007, p. 58-60)

O Ministério da Fazenda - MF, por sua vez, em seu Manual de Gestão Integrada de Riscos Corporativos (2016, p. 36-7), apresenta uma taxonomia de riscos operacionais mais abrangente, envolvendo a exposição, além dos 4 fatores acima divulgados pela FEBRABAN, de 16 subfatores, acompanhados de múltiplos exemplos de eventos operacionais comuns ao órgão.

Tal enumeração de eventos de risco realizada pelo MF, excelente *benchmark* para o presente artigo, demonstra a relevância do gerenciamento deste tipo de risco, que permite às instituições desenvolverem maior controle sobre eventuais perdas, potencializando a sua performance e diminuindo a probabilidade de desastres financeiros (FEBRABAN, 2006 apud SALGADO et al., 2010, p. 5).

Ao evoluir a análise para a gestão de risco em sentido mais amplo, no qual o risco é compreendido como elemento intrínseco à atividade organizacional, não podendo, portanto, ser por completo extinto, o seu gerenciamento torna-se fator crucial para o atingimento de objetivos e da estratégia da instituição, e para a sua própria sobrevivência.

#### 4.3 Definição de gestão de riscos

Inicialmente, em busca de um refinamento conceitual, o Tribunal de Contas da União destaca que o processo de gestão de riscos que possui a organização como foco tem como denominação original na literatura o termo “gestão de riscos corporativos”,

tradução literal do conceito em inglês de *Enterprise Risk Management* (BRASIL, s.d., p. 1).

Para instituições sem fins comerciais, como as do setor público, também pode ser adotado o termo “gestão institucional de riscos” ou a sua simplificação, gestão de riscos, a qual será amplamente utilizada no presente trabalho (BRASIL, s.d., p. 1).

Feito tal ressalva, salienta-se que a implementação de um processo estruturado e sistematizado de gestão de riscos permite:

“(...) tratar com eficiência as incertezas, seja pelo melhor aproveitamento das oportunidades, seja pela redução da probabilidade e/ou impacto de eventos negativos, a fim de melhorar a capacidade de gerar valor e fornecer garantia razoável do cumprimento dos seus objetivos.” (BRASIL, 2014, p. 22)

Nesse sentido, ressalta-se que a gestão de riscos proporciona às empresas “assumir riscos calculados, reduzir a volatilidade dos seus resultados e aumentar a previsibilidade de suas atividades, a fim de se tornar mais resilientes em cenários extremos” (IBGC, 2017, p. 14).

Dessa forma, ao permitir a tomada de decisão embasada, possibilita que a organização aumente a sua confiança em alcançar os objetivos definidos, bem como viabiliza aos *stakeholders* o aumento de sua confiança na governança corporativa e na capacidade deste arranjo de entregar valor (REINO UNIDO, 2004, p. 7, tradução nossa).

Nessa seara, o Instituto Brasileiro de Governança Corporativa (2017, p. 14) compreende o gerenciamento de riscos corporativos tanto como um sistema inerente ao planejamento estratégico - direcionado a identificar e tratar eventos que possam impactar os objetivos da organização - como uma estrutura de governança, estabelecida para por em prática e manter esse sistema em pleno funcionamento.

Assim, em breve síntese, é possível conceituar gestão de riscos como “a cultura, as capacidades e as práticas que as organizações integram com a definição da estratégia e aplicam quando da realização desta, com o propósito de gerenciar riscos na criação, preservação e concretização de valor” (COSO, 2017, p. 3, tradução nossa).

#### **4.4 Princípios e processo de gestão de risco**

Como princípios orientadores, a ISO 31.000 (ABNT, 2009, p. 7-8) preconiza que a gestão de riscos eficaz deve ser transparente e inclusiva, abrangendo todos os

processos organizacionais e todos os agentes tomadores de decisão, nos três níveis da organização. Além disso, deve ser dinâmica, iterativa e capaz de reagir a mudanças, visto o ambiente altamente mutável no qual está inserida.

Em adição, deve ser sistemática, estruturada e oportuna, razão pela qual se alicerça em uma estrutura que permite a customização da gestão à realidade do órgão e a transmissão das informações entre todos os níveis organizacionais, a fim de assegurar o embasamento das decisões da alta cúpula.

Nesse sentido, a sua estrutura fundamenta-se na concepção de melhoria contínua, a partir da implementação de práticas de monitoramento e análise crítica, viabilizadas pela retroalimentação constante de informações oportunas sobre os riscos.

Para além dos mecanismos apurados de comunicação e consulta, e monitoramento e análise crítica, acima apresentados, o processo de gestão de riscos também deve envolver as etapas de estabelecimento do contexto, identificação, análise, avaliação e tratamento dos riscos, conforme figura abaixo:

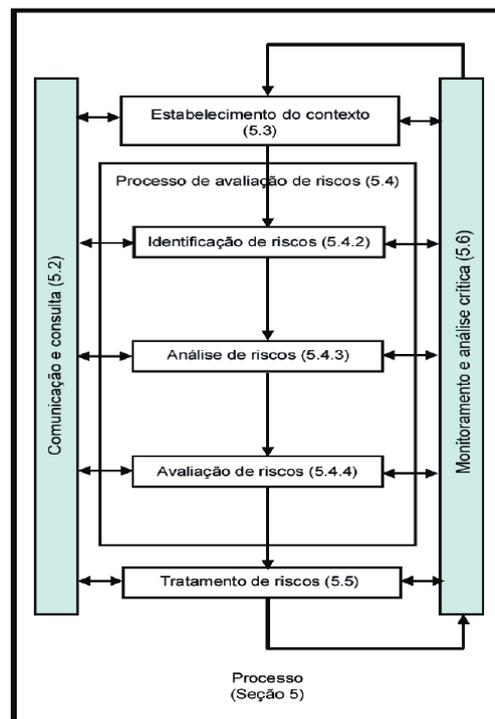


Figura 1: Processo de Gestão de Riscos  
Fonte: ABNT ISO 31.000 (2009, p. 14)

Na fase de estabelecimento de contexto, avaliam-se as características do ambiente interno e externo da organização, a fim de articular os seus objetivos para definir os parâmetros, critérios e o escopo do processo de gestão de riscos.

Nesse momento, devem ser considerados, por exemplo, os aspectos legais, regulatórios, políticos e econômicos do ambiente de negócio, bem como a cultura, valores, estrutura, processos e estratégia da instituição. A amplitude da análise de contexto se relaciona à natureza da abordagem a ser adotada pela organização para a gestão de riscos, a fim de customizá-la à realidade do órgão e habilitá-la a gerir as incertezas que efetivamente impactem os seus objetivos.

Compreendido o contexto, passa-se à fase de identificação, na qual serão levantados os eventos de risco, suas causas e consequências, de forma bastante abrangente, a fim de consolidar uma relação significativa de riscos “que possam criar, aumentar, evitar, reduzir, acelerar ou atrasar a realização dos objetivos” (ABNT, 2009, p. 17).

As causas, também por vezes denominadas fatores de risco, são condições ou ações que possibilitam a materialização de um evento que impacta os objetivos. Logo, são resultado da combinação de fontes de risco com as vulnerabilidades (BRASIL, 2015a, p. 7).

Para maior elucidação do tema, vide explicação apresentada pelo Tribunal Superior do Trabalho:

**“Fonte de Risco**

É um elemento (pessoas, processos, sistemas, estrutura organizacional, infraestrutura física, tecnologia, eventos externos) que, individualmente ou de maneira combinada, tem o potencial intrínseco para dar origem ao risco. São consideradas fontes de riscos: ameaças, oportunidades e perigos.

**Vulnerabilidade**

Ausência, inadequação ou deficiência em uma fonte de risco, a qual pode vir a contribuir com a concretização de um evento indesejado.”(BRASIL, 2015a, p. 8-9)

O levantamento exaustivo das causas é de suma importância para a criação de controles pela instituição, os quais atuarão exatamente na origem do risco, a fim de diminuir a probabilidade de sua ocorrência.

O evento, por sua vez, pode ser compreendido como o “incidente ou ocorrência, proveniente de fontes internas ou externas, que afeta a implementação da estratégia ou a realização de objetivos” (INTOSAI, 2007 apud BRASIL, 2014b, p. 58). Assim, ele pode se traduzir em uma ou mais ocorrências, inclusive em algo deixar de ocorrer (ABNT, 2009, p. 4).

Por fim, a consequência diz respeito ao resultado da materialização do evento nos objetivos da organização, podendo ser positivo ou negativo. A sua identificação

detalhada também é relevante, pois favorece a implementação de controles capazes de diminuir o seu impacto, auxiliando diretamente a elaboração de Planos de Contingência.

Em suma, a sintaxe para descrição do risco, que une causa, evento e consequência, além de ressaltar o objetivo impactado pelo risco, é a seguinte:

Devido a <CAUSA/FONTE>, poderá acontecer <DESCRIÇÃO DO EVENTO DE RISCO>, o que poderá levar a <DESCRIÇÃO DO IMPACTO/EFEITO/CONSEQUÊNCIAS> impactando no/na <OBJETIVO DE PROCESSO >.

Figura 2: Sintaxe para descrição de Riscos

Fonte: Manual de Gestão de Integridade, Riscos e Controles Internos da Gestão do Ministério do Planejamento, Desenvolvimento e Gestão (2017a, p. 29)

Considerando o exposto, para essa etapa de identificação de riscos, recomenda-se a aplicação de técnicas e instrumentos que sejam pertinentes aos objetivos e capacidades da organização, bem como aos riscos que serão tratados.

Nessa toada, poderão ser empregadas as ferramentas de *brainstorming*, análise SWOT, metodologia Delphi, diagramas de causa e efeito (*Bow-tie*), questionários, *checklist*, entrevista com especialistas, exame de dados históricos, dentre outros (BRASIL, 2015, p. 34).

Após estabelecer a lista de riscos, avança-se para a fase de análise, na qual serão ponderados a probabilidade e o impacto dos riscos, a fim de se obter um denominador chamado nível de risco, que subsidiará a etapa seguinte. Ressalta-se que o exame realizado deve levar em consideração a existência, eficácia e eficiência dos controles e a possível divergência de opiniões entre os especialistas, bem com a disponibilidade de informações pertinentes sobre o risco em observação.

A partir do nível de risco coletado, torna-se possível, já na fase de avaliação, estabelecer os riscos que necessitam ser tratados e a ordem de priorização para o início do tratamento, considerando a atitude definida pela organização perante o risco, além de aspectos legais, regulatórios, econômicos, e outros.

Em seguida, os gestores devem, a partir do insumo gerado na fase de avaliação, selecionar uma ou mais opções de tratamento do risco, que podem envolver evitar, mitigar, compartilhar ou mesmo aceitar o risco.

Nesse ponto, é importante considerar o custo-benefício de cada ação avaliada, a eventual geração de novos riscos com a implementação de medidas de tratamento - denominados riscos secundários - e, ainda, a extensão dos riscos que poderão

remanescer mesmo com os controles implantados (riscos residuais) (ABNT, 2009, p. 20).

Considerando todo o exposto, é possível sumarizar o processo de gestão de riscos como:

“aplicação sistemática de políticas, procedimentos e práticas de gestão para as atividades de comunicação, consulta, estabelecimento do contexto, e na identificação, análise, avaliação, tratamento, monitoramento e análise crítica de riscos” (ABNT, 2009, p. 2)

Ressalta-se, por fim, que a integração dos planos de tratamento de riscos com os processos organizacionais, a partir da definição clara dos papéis e responsabilidades dos atores chaves desse processo, associada à implantação de um rito eficaz de monitoramento e análise crítica, são considerados fatores chave de sucesso da gestão de riscos para qualquer organização.

#### **4.5 Histórico da gestão de riscos**

A gestão de riscos, em que pese se tratar de assunto em voga nas organizações nas últimas décadas, tem origem em período bem mais remoto. É possível encontrar os seus contornos nas decisões dos primeiros chefes de clã que optaram por fortificar muralhas ou estocar provimentos para períodos vindouros, ou ainda, na previsão de indenizações para perdas em casos de roubos e inundações na antiga Babilônia (HUBBARD, 2009 apud BRASIL, s.d., p. 6).

De acordo com Bernstein (1997), o aprofundamento da temática relativa a riscos iniciou-se no período do Renascimento. Nessa época, foi desenvolvido o estudo matemático do conceito de risco, a partir da formulação da teoria da probabilidade, da lei dos Grandes Números e da amostragem estatística, com a definição de desvio padrão (BRASIL, 2017b, p. 5).

Tal arcabouço teórico fundamentou o desenvolvimento dos métodos quantitativos em gestão de riscos, que, até o início do século XX, encontravam-se focados em áreas específicas, como seguros, indústria financeira e saúde pública (HUBBARD apud BRASIL, s.d., p. 6).

No setor financeiro, o marco para implementação do gerenciamento de riscos se deu na década de 1980, quando a falta de registro de operações em balanços cumulada com a emergente necessidade de empréstimos para países do então terceiro mundo culminaram com o Acordo de Capital da Basiléia, também denominado Basiléia I. O

objetivo do documento foi orientar os bancos quanto à alocação de recursos para mitigar riscos de crédito (IBGC, 2017, p. 16).

O final do século XX também trouxe à baila o início do estudo da gestão de riscos com foco em organizações, isto é, alinhada a práticas de gestão corporativa. O seu desenvolvimento teve como grande incentivador a reforma na legislação de financiamento de campanhas políticas americanas e a publicação do *Foreign Corrupt Practices Act* (FCPA), que obrigou que as empresas implantassem e consolidassem programas de controle interno (BRASIL, 2017b, p. 5).

Como resposta, foi criado o *Committee of Sponsoring Organizations of the Treadway Commission* – COSO - organização do setor privado com a missão de prevenir fraudes financeiras corporativas -, o qual foi responsável pela publicação do primeiro marco teórico dessa abordagem, qual seja, o guia *Internal Control – Integrated Framework* (COSO-IC), datado de 1992. O intuito do documento foi nortear as organizações quanto a definições comuns, princípios e melhores práticas de controle interno, dentre as quais se destacava a gestão de riscos.

Posteriormente, uma miríade de documentos foi publicada sobre gestão de riscos corporativos, que envolveram desde a compreensão da relevância da alta gestão como formuladora da política de gestão de riscos e supervisora de sua implementação – estabelecidos no Relatório de *Cadbury* (REINO UNIDO, 1992, p. 20), como a definição de padrões oficiais a serem seguidos, presentes inicialmente no *Risk Management Standard*, AS/NZ 4360:1995 (BRASIL, s.d., p. 7).

O século XXI, por sua vez, veio acompanhado de escândalos corporativos financeiros e contábeis, tendo como caso exemplar o da empresa norte-americana Enron, que abriu insolvência após ocultar dívidas, fraudar balanços e apresentar lucros irreais.

Para atender à demanda crescente por maior regulação e transparência, foi aprovada a Lei *Sarbanes-Oxley*, que obrigou as empresas que operavam na bolsa americana a adotar ferramentas efetivas de governança, enaltecendo as metodologias até então criadas para aperfeiçoar o controle interno e o gerenciamento de riscos corporativos (IBGC, 2017, p. 18).

Nesse contexto, o COSO divulgou mais um referencial, denominado *Enterprise Risk Management – Integrated Framework* (COSO-ERM), que agregou o COSO I na definição de uma estrutura de gerenciamento de riscos, representada por uma matriz no formato de um cubo, envolvendo três dimensões: i) objetivos a serem alcançados pela instituição; ii) componentes do gerenciamento de riscos que traduzem o que deve ser

feito para alcançá-los e iii) estrutura organizacional capaz de realizá-los (COSO, 2017, p. 13).

No mesmo ano, isto é, 2004, a demanda por regulamentação e estabilidade do mercado financeiro levou o Comitê de Supervisão Bancária de Basileia, ligado ao Banco de Compensações Internacionais<sup>1</sup>, a propor uma nova estrutura de adequação do capital, a fim de incluir, além dos riscos de crédito e de mercado, os riscos operacionais, dando origem ao Novo Acordo de Capital, conhecido como Basileia II.

Vale destacar que tal documento impulsionou sobremaneira o gerenciamento do risco operacional, uma vez que demandou a alocação de capital específico para esta categoria de risco, com recomendação de taxonomia própria e detalhamento de formas e abordagens para cálculo.

Ressalta-se, ainda, a publicação de um importante referencial pelo governo do Reino Unido, o *Management of Risks – Principles and Concepts*, mais conhecido como *Orange Book* - que permitiu a aplicação de um modelo de gestão de riscos multinível, abrangendo desde a dimensão de tarefas até a integridade da organização, levando em consideração inclusive os relacionamentos de interdependência com outras instituições - que dá origem ao conceito de organização estendida (REINO UNIDO, 2004, p. 37).

Outra publicação de grande relevância foi a ABNT ISO 31.000 *Risk Management – Principles and Guidelines*, ocorrida em 2009, que estabeleceu definições, princípios, estrutura e o processo de gestão de riscos, aplicável a qualquer tipo de organização. Tratou-se de um aperfeiçoamento das normas e referenciais produzidos até a época, como a AS/NZS 4360 (BRASIL, s.d., p. 8).

Ressalta-se, ainda, movimento internacional de formulação de leis anticorrupção, destacando-se o *Bribery Act 2010*, do Reino Unido, que veio aperfeiçoar a já mencionada FCPA, e a Lei 12.846/2013, posteriormente regulamentada pelo Decreto nº 8.420/2015 (IBGC, 2017, p. 18).

Buscou-se, no Brasil, inspirado pelos normativos acima, responsabilizar, administrativa e civilmente, pessoas jurídicas pela prática de atos: (i) contra o patrimônio público, nacional ou estrangeiro; (ii) contra compromissos internacionais

---

<sup>1</sup> “Em 1930, foi criado o BIS (*Bank for International Settlements*), o Banco de Compensações Internacionais ([www.bis.org](http://www.bis.org)). O BIS é uma organização internacional que fomenta a cooperação entre os bancos centrais e outras agências, em busca da estabilidade monetária e financeira. Em 1975, foi estabelecido o Comitê de Supervisão Bancária da Basileia (*Basel Committee on Banking Supervision – BCBS*), ligado ao BIS, que funciona como um fórum mundial para discussão e cooperação em matéria de regulação bancária prudencial; seu objetivo consiste em reforçar a regulação, a supervisão e as melhores práticas no mercado financeiro”. BANCO CENTRAL DO BRASIL. *Recomendações de Basileia*. Disponível em: < <https://www.bcb.gov.br/fis/supervisao/basileia.asp>>. Acesso em: 19 ago. 2017.

assumidos ou (iii) contra princípios da administração pública. O objetivo maior era evitar subornos, fraudes a licitação e contratos, e diversos outros atos de corrupção.

Assim, passou a ser legalmente demandada das empresas a adoção de mecanismos e procedimentos internos de integridade e auditoria, a fim de garantir transparência aos processos (BRASIL, 2013).

Para maior elucidação do breve histórico de gestão de riscos ora exposto, segue figura desenvolvida pelo Instituto Brasileiro de Governança Corporativa:

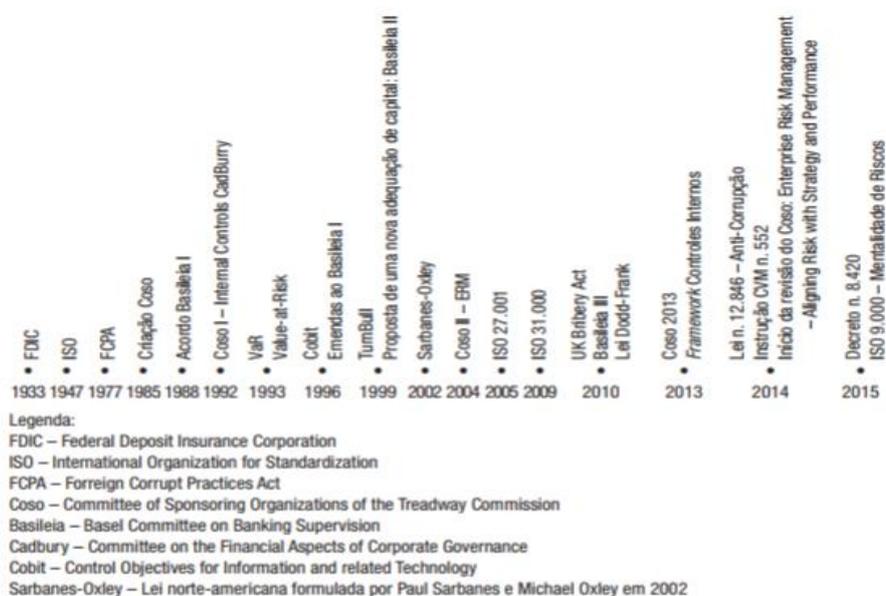


Figura 3 – Evolução da gestão de riscos

Fonte: IBGC (2017, p. 19)

Acresça-se à linha do tempo o recém-publicado *Enterprise Risk Management – Integrating with Strategy and Performance*, datado de junho de 2017, que se apresenta como atualização do COSO-ERM de 2004. O escopo do documento é permitir que as organizações obtenham maior valor de seus programas de gerenciamento corporativo de riscos, a partir da integração destes com a estratégia e o desempenho organizacional (COSO, 2017, p. 2).

Ante o exposto, verifica-se que a crescente complexidade e dinamismo do ambiente de negócio, provocada pela multiplicidade de normas, regulamentações, exigências do mercado e anseios da sociedade, impulsionou as organizações a se dedicarem ao longo dos anos ao aperfeiçoamento de modelos e referenciais de gestão de risco e controle interno, inexistindo um padrão consensual adotado no mundo.

#### **4.6 Gestão de riscos como mecanismo fundamental de governança no setor público**

Atualmente, um dos maiores desafios enfrentados pelo setor público brasileiro é o aperfeiçoamento da governança. Como salientado por MARTINS et al (2014, p. 51), “cada vez mais os governos serão pressionados a colocarem em prática efetivas políticas de gestão pública para melhorar sua governança”.

Tal afirmação é possível em um contexto no qual se compartilha da compreensão de que “a boa governança leva a uma boa gestão, a um bom desempenho, a uma boa administração de dinheiro público, a um bom comprometimento público e, em última instância, a bons resultados” (CIPFA, 2004, p.61, tradução nossa).

No Poder Judiciário, tal preocupação é traduzida como Macrodesafio da Estratégia Nacional definida para o período de 2015-2020, conforme Resolução do Conselho Nacional de Justiça nº. 198/2014. Nos exatos termos do normativo, os tribunais pátrios devem envidar esforços para instituir a Governança Judiciária, visando:

“(…) à eficiência operacional, à transparência institucional, ao fortalecimento da autonomia administrativa e financeira do Poder Judiciário e à adoção das melhores práticas de comunicação da estratégia, de gestão documental, da informação, de processos de trabalho e de projetos” (BRASIL, 2014d).

Tendo em vista a multiplicidade de conceitos e significados atribuídos à governança<sup>2</sup>, considerado por Pollitt et al (2009, p.5) , inclusive, um “conceito mágico”, com alta carga de abstração, mister a tentativa de definição de uma orientação conceitual a ser adotada no presente artigo.

Conforme Martins et al (2014, p. 44), governança pública:

“é um processo de geração de valor público a partir de determinadas capacidades e qualidades institucionais; de colaboração entre agentes públicos e privados na coprodução de serviços, políticas e bens públicos e da melhoria de desempenho”.

Nesse contexto, o Tribunal de Contas da União estabelece que governança no setor público:

---

<sup>2</sup> Para uma compilação de diferentes conceitos utilizados para governança, conferir CIPFA e IFAC. *Good Governance in the Public Sector— Consultation Draft for an International Framework*. Disponível em: < <http://www.ifac.org/system/files/publications/files/Good-Governance-in-the-Public-Sector.pdf>>. Acesso em: 17 set. 2017.

“compreende essencialmente os mecanismos de liderança, estratégia e controle postos em prática para avaliar, direcionar e monitorar a atuação da gestão, com vistas à condução de políticas públicas e à prestação de serviços de interesse da sociedade” (BRASIL, 2014b, p. 26).

Com o escopo de perscrutar de forma mais detalhada os componentes encontrados na definição acima, o aludido Tribunal salienta que a governança no setor público pode ser analisada sob quatro perspectivas, sendo elas: i) sociedade e Estado; ii) entes federativos, esferas de poder e políticas públicas; iii) órgãos e entidades; e iv) atividades intraorganizacionais.

Nas palavras do mencionado órgão de controle:

“Enquanto a **primeira** define as regras e os princípios que orientam a atuação dos agentes públicos e privados regidos pela Constituição e cria as condições estruturais de administração e controle do Estado; a **segunda** se preocupa com as políticas públicas e com as relações entre estruturas e setores, incluindo diferentes esferas, poderes, níveis de governo e representantes da sociedade civil organizada; a **terceira** garante que cada órgão ou entidade cumpra o seu papel; e a **quarta** reduz os riscos, otimiza os resultados e agrega valor aos órgãos e entidades.” (BRASIL, 2014b, p. 18-19)

Destarte, a perspectiva de órgãos e entidades, ao se preocupar com o atingimento dos propósitos organizacionais e otimização de desempenho, com foco principal em resultado, traz à baila a vertente corporativa da governança.

Essa vertente debruça-se sobre o desafio posto à organização de que, para atingir os objetivos traçados e ofertar serviço de qualidade, deverá enfrentar e responder aos mais diversos riscos, esmerando-se em estabelecer quanto de risco poderá aceitar, em uma atividade constante de equilíbrio entre riscos, custos e benefícios, “a fim de maximizar as possibilidades de a instituição alcançar a sua missão” (INTOSAI, 2007, p. 21).

Nessa seara, a gestão de riscos se apresenta como um processo estratégico para as organizações do setor público, sendo um componente fundamental de seus sistemas de governança.

Sob a perspectiva mais limitada de atividades intraorganizacionais, a governança é definida como “o sistema pelo qual os recursos de uma organização são dirigidos, controlados e avaliados” (BRASIL, 2014b, p 21). Dessa forma, são examinados:

“os processos decisórios, as estruturas específicas de governança e as relações intraorganizacionais, que visam, entre outras coisas, otimizar o uso de recursos, reduzir riscos e agregar valor a órgãos e entidades e contribuir para o alcance de resultados esperados por partes interessadas internas e externas à organização” (BRASIL, 2014b, p 21).

O desdobramento apurado dessas duas perspectivas possibilita a compreensão mais efetiva da relação e relevância da gestão de riscos para a governança no setor público, ao migrar o foco de análise das condições estruturais da administração e da relação entre esferas e poderes para o aperfeiçoamento do desempenho organizacional.

Feita tal consideração, destaca-se que o Tribunal de Contas da União, ao definir os 10 passos para a Boa Governança, determinou como um deles a exigência de os órgãos gerenciarem riscos e instituírem mecanismos de controle interno necessários (BRASIL, 2014a, p 22).

Ressalta-se, ainda, que o vínculo entre boa governança e gestão de riscos já era conhecido e enaltecido desde 2001, quando a *International Federation of Accountants – IFAC* publicou estudo no qual ressaltava a necessidade de implementação de um processo de gestão de riscos institucional como ferramenta para efetivar a governança corporativa (BRASIL, s.d., p 8).

Em estudo mais recente, datado de 2013, a IFAC demonstra inclusive que tal entendimento é compartilhado por diversas instituições com destaque na área, como o “*The Chartered Institute of Public Finance and Accountancy – CIPFA*, o *Office for Public Management ltd – OPM*, a *Independent Commission for Good Governance in Public Services – ICGGPS*, o Banco Mundial e o *Institute of Internal Auditors – IIA*” (BRASIL, s.d., p 8).

Na esfera do Judiciário, já há iniciativas consolidadas que internalizam o supracitado entendimento, merecendo destaque um dos critérios estabelecidos para se avaliar a governança da Justiça Federal, o qual diz respeito ao fato de o órgão possuir plano de riscos elaborado e adotar ações de controle interno para tratar os riscos identificados em processos críticos de trabalho (BRASIL, 2015b, p. 34).

A relevância da gestão de riscos como instrumento de governança é tamanha que o próprio Ministério do Planejamento, Orçamento e Gestão, junto com a Controladoria-Geral da União, publicou a Instrução Normativa n. 01/2016, que versa sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo Federal.

Tal ato normativo determina que os órgãos e entidades desse Poder devem implementar, manter, monitorar e revisar o processo de gestão de riscos, o qual deve ser compatível com sua missão e seus objetivos estratégicos (BRASIL, 2016b).

Dessa forma, a referida Instrução Normativa explicita a concepção da gestão de riscos como ferramenta de desenvolvimento institucional, capaz de alavancar os processos de gestão do órgão. Além disso, ressalta a importância da gestão de riscos como fornecedora de insumos ao controle interno e à continuidade do negócio, com o fim último de aperfeiçoar a geração de valor público.

Em que pesem todos os benefícios atribuídos pela literatura especializada à gestão de riscos, sendo componente fundamental e estratégico dos sistemas de governança corporativa, não há, no Poder Judiciário, ato normativo congênere à Instrução Normativa MP/CGU 01/2016, nem órgão com notável experiência no tema.

Por essa razão, mister a análise da experiência do Banco Central do Brasil relativa à gestão de riscos operacionais, a fim de examinar a possibilidade de adaptação de sua metodologia à realidade da justiça brasileira.

Para tanto, necessário perscrutar, de início, o próprio conteúdo do Acordo de Capital de Basiléia II, responsável por prever a exigência de gerenciamento de riscos operacionais por todo o sistema financeiro internacional.

#### **4.7 O Acordo de Basiléia II e sua contribuição à gestão de riscos operacionais no setor financeiro internacional**

A partir de meados dos anos 70, em meio ao crescente processo de globalização financeira - esteado na integração de mercados e no constante aperfeiçoamento da tecnologia - o sistema bancário internacional testemunhou a progressiva complexificação de seus riscos corporativos.

Por essa razão, em 1975, os presidentes dos bancos centrais dos países integrantes do G-10 instituíram o Comitê de Supervisão Bancária de Basiléia, ligado ao Banco de Compensações Internacionais (BIS), com o escopo de intensificar a regulação e a supervisão do mercado financeiro, além de disseminar as melhores práticas<sup>3</sup>.

---

<sup>3</sup> “Atualmente, o Comitê para Supervisão Bancária da Basiléia reúne autoridades de supervisão bancária e bancos centrais da Bélgica, Canadá, França, Alemanha, Itália, Japão, Luxemburgo, Holanda, Espanha, Suécia, Suíça, Reino Unido e Estados Unidos”. Ver BANCO CENTRAL DO BRASIL. Princípios Fundamentais para uma Supervisão Bancária Efetiva. Disponível em: <[http://www.bcb.gov.br/fis/supervisao/docs/core\\_principles\\_traducao2006.pdf](http://www.bcb.gov.br/fis/supervisao/docs/core_principles_traducao2006.pdf)>. Acesso em: 14 out. 2017.

O primeiro acordo definido pelos países membros do aludido Comitê, assinado em 1988, foi denominado Acordo de Capital da Basileia, e teve como objetivo a criação de requisitos mínimos de capital para as instituições financeiras para enfrentar os riscos de crédito.

Sucessivos escândalos financeiros e contábeis, a partir da década de 90, e o maior grau de subjetividade envolvido na identificação e tratamento dos riscos não financeiros - como operacional, reputacional e ambiental (IBGC, 2017, p. 17) - deram início a maiores demandas por regulamentação, estabilidade e transparência do mercado financeiro.

Tal contexto levou, inicialmente, à publicação da Emenda 96 ao Basileia I, a fim de incluir a cobertura dos riscos de mercado. Posteriormente, já no ano de 2004, o Comitê publicou ampla revisão do aludido acordo, denominada Convergência Internacional de Mensuração de Capital e Padrões de Capital - Estrutura Revisada, que ficou conhecido como Basileia II.

É importante destacar que o Acordo de Capital de Basileia II, ao buscar o aperfeiçoamento das práticas de gestão e governança dos bancos internacionais, inovou ao trazer a exigência de alocação de capital específico para o risco operacional.

Em breve síntese, tal Acordo propôs uma estruturação de adequação do capital sustentada em três pilares, que, conjuntamente, teriam o condão de gerar maior segurança e consistência ao sistema financeiro, a saber:

“(…) o primeiro tratava da adequação do capital regulatório mínimo com base nos riscos de mercado, de crédito e operacionais; o segundo reforçava a capacidade dos supervisores bancários em avaliar e adaptar o capital regulatório às condições de cada instituição financeira; e o terceiro atribuía à transparência e à divulgação de informações um papel importante e relevante no fomento à disciplina de mercado” (IBGC, 2017, p. 17).

No tocante ao Pilar I, destaca-se que o Basileia II propôs três abordagens para a mensuração do capital mínimo adequado à cobertura de riscos operacionais, em uma ordem crescente de sofisticação e sensibilidade ao risco: Indicador Básico; Padronizada/Padronizada Alternativa; e Mensuração Avançada (AMA).

Nesse sentido, destaca-se que:

“As três primeiras abordagens são caracterizadas como sintéticas, dado que a exigência de capital é estimada com base em dados agregados, sem que haja identificação dos eventos de perda de forma individualizada. A Abordagem Avançada (Modelo Interno) assume

caráter analítico, pois proporciona maior conhecimento do perfil de risco da instituição e melhor adequação à qualidade dos controles” (BANCO DO BRASIL, [2008]).

Destarte, o Acordo estabelece, sob a ótica da abordagem de Mensuração Avançada, que o capital regulamentar deverá igualar a medida de risco gerado pelo sistema interno de mensuração do risco operacional do banco, usando critérios qualitativos e quantitativos definidos no documento.

Em adição, estabelece que a instituição financeira, para se qualificar na utilização da supracitada abordagem, deve convencer a autoridade de supervisão bancária que:

“O conselho de administração e a alta administração, conforme apropriado, estão ativamente envolvidos na supervisão do quadro de gerenciamento de riscos operacionais;  
Possui um sistema operacional de gerenciamento de riscos que é conceitualmente sólido e implementado com integridade; e  
Tem recursos suficientes no uso da abordagem nas principais linhas de negócios, bem como as áreas de controle e auditoria” (BIS, 2004, p. 155, tradução nossa)

Como padrões qualitativos exigidos para a adoção da AMA, os bancos devem:

- (i) possuir uma função de gerenciamento de risco operacional independente;
- (ii) desenvolver um sistema interno de medição do risco operacional integrado aos processos diários de gerenciamento de riscos da instituição;
- (iii) produzir relatórios regulares de exposição ao risco operacional e experiência de perdas, que estejam disponíveis a todos os níveis organizacionais, com ampla documentação de todo o processo; e
- (iv) realizar, por meio de auditores internos e/ou externos, revisões periódicas dos processos de gerenciamento de riscos operacionais e dos sistemas de medição (BIS, 2004, p. 155, tradução nossa).

No tocante aos padrões quantitativos, o Basileia II preconiza que qualquer sistema interno de mensuração do risco operacional deve ser consistente com o escopo da definição de risco operacional estabelecido pelo documento, traduzida, como visto anteriormente, pelo Banco Central do Brasil na Resolução 3.380/2006. Ressalva-se que essa definição “inclui os riscos legais, mas exclui os estratégicos e de reputação” (BIS, 2004, p. 149, tradução nossa).

O documento também apresenta uma relação entre categorias de causas, eventos e efeitos, a fim de facilitar a identificação dos riscos operacionais e o seu gerenciamento, conforme figura abaixo:

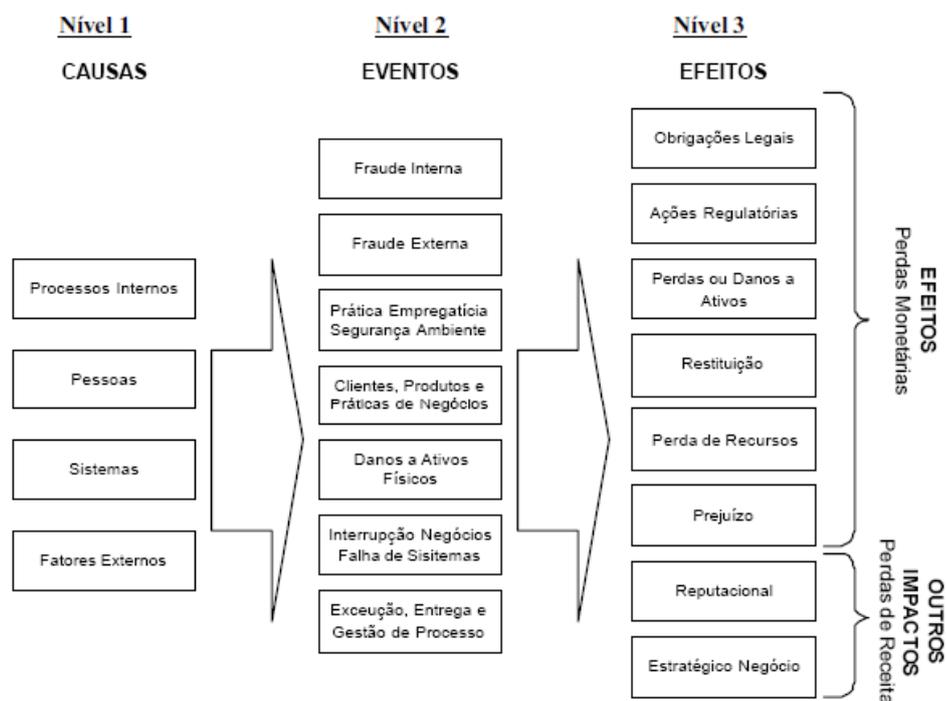


Figura 4: Estrutura de Risco Operacional segundo Basileia II  
 Fonte: Adaptado Guimarães (apud LIMA, 2007, p. 61)

Em adição, o Acordo propõe, em seu Anexo 7 (BIS, 2004), uma taxonomia de eventos de risco operacional, a qual orienta todos os sistemas de mensuração do risco operacional das instituições financeiras.

Nesse contexto, ao considerar a multiplicidade de causas que podem estar associadas a um evento, o Novo Acordo estabelece categorias de tipos de evento, subdivididas em três níveis hierarquizados.

No primeiro nível, há 07 tipos de evento operacional, os quais são mais detalhados no nível 2. O nível 3, por sua vez, traz à baila apenas exemplos de atividades relacionadas ao nível 2, sendo dado às instituições financeiras customizá-las aos seus respectivos processos de trabalho.

Ao examinar a supracitada categorização proposta por Basileia II, Lima, com base nas lições de Guimarães et al<sup>4</sup>, salienta que:

“Essa hierarquização, além de facilitar o processo de modelagem e de coleta de dados do risco operacional, auxilia no processo de análise do comportamento de cada uma dessas categorias, cujas distribuições de probabilidade são diferentes entre si. Portanto, basta coletar, tratar e armazenar os dados da transação correspondente a um evento de nível 3, para se obter informações nos demais níveis de tipos de eventos. O

<sup>4</sup> Ver GUIMARÃES, T. A.; STERN, J. M. Implementação do método de distribuição de perdas para risco operacional. 2003.[s.n.], São Paulo, 2003.

efeito é a perda monetária ou não-monetária acarretada pelo evento” (LIMA, 2007, p. 62).

Nesse contexto, destaca-se que o Comitê de Basileia considera, como um dos três temas que englobam os oito princípios orientadores das instituições financeiras no tocante ao desenvolvimento de uma estrutura adequada de gestão de risco operacional, a necessidade de estabelecimento de uma linguagem comum de identificação de risco (BIS, 2003, p. 8).

Isto é, determinar quais eventos devem estar vinculados ao risco de pessoas, ao risco de processo, de tecnologia, e assim por diante. Tal padronização de linguagem tem como objetivo auxiliar tanto na etapa de auto-avaliações qualitativas realizadas pela administração do negócio, quanto no momento próprio de avaliação estatística integral (CROUHY et al., 2006, p. 330, tradução nossa).

Destaca-se que a adesão ao Basileia II é obrigatória somente para os países que compõem o G-10. Contudo, em face do prestígio internacional do Comitê de Supervisão Bancária de Basileia, os países não-membros tendem a adotar as suas recomendações.

Nesse sentido, destaca-se pesquisa realizada pelo *Financial Stability Institute* (FSI), ligado ao mencionado Comitê, que verificou que, dentre os 108 países que participaram, 88 manifestaram-se favorável à implementação do Basileia II. Caso se incluíssem os países membros do Comitê da Basileia para Supervisão Bancária, o número superaria 100. Ademais, os ativos bancários nesses países “excediam 90% dos totais regionais para África, América Latina, Oriente Médio e países europeus não membros do BCBS, e atingia quase 90% para a Ásia” (CORNFORD, 2006, p. 1).

Tamanha participação possibilita o desenvolvimento de processos de avaliação sistêmica e global da implementação das recomendações do Comitê da Basileia, aprimorando as ferramentas de fiscalização do sistema financeiro internacional e, conseqüentemente, promovendo maior segurança e solidez ao sistema.

#### **4.8 A implementação do Acordo de Basileia II pelo Banco Central do Brasil**

No âmbito da administração pública brasileira, o Banco Central do Brasil, autarquia federal criada pela Lei 4.595/1964 e vinculada ao Ministério da Fazenda, tem como missão assegurar a estabilidade do poder de compra da moeda e um sistema financeiro sólido e eficiente.

Dessa forma, encontra-se sob a égide das diretrizes do Comitê de Supervisão Bancária de Basileia, tendo oficialmente aderido ao Acordo de Basileia I em 1994, quando da publicação da Resolução BCB de nº. 2.099.

Tal ato normativo inovou ao exigir a compatibilização de valor de patrimônio líquido ajustado com o grau de risco das operações ativas, inaugurando o desenvolvimento de metodologias de gestão de risco pela instituição financeira, com foco, há época, em riscos de crédito e, posteriormente, de mercado (BRASIL, 1994).

O Comunicado BCB 12.746, de 9 de dezembro de 2004, por sua vez, apresentou os procedimentos para a implementação da nova estrutura de capital proposta pelo Basileia II (Brasil, 2004).

Em seguida, a Resolução 3.380, de 29 de junho de 2006, trouxe a determinação, às instituições financeiras e demais organizações autorizadas a funcionar pelo Banco Central do Brasil, de implementação de estrutura de gerenciamento do risco operacional. Para tanto, o BCB consolidou, no artigo 2º do aludido ato normativo, definição de risco operacional, apresentada anteriormente no presente artigo.

Em adição, apresentou, no § 2º do mesmo artigo, enumeração de eventos de risco operacional extraídos da taxonomia apresentada pelo Comitê de Basileia, nos seguintes termos:

Art. 2º (...)

§ 2º Entre os eventos de risco operacional, incluem-se:

I - fraudes internas;

II - fraudes externas;

III - demandas trabalhistas e segurança deficiente do local de trabalho;

IV - práticas inadequadas relativas a clientes, produtos e serviços;

V - danos a ativos físicos próprios ou em uso pela instituição; VI - aqueles que acarretem a interrupção das atividades da instituição;

VII - falhas em sistemas de tecnologia da informação;

VIII - falhas na execução, cumprimento de prazos e gerenciamento das atividades na instituição. (BRASIL, 2006)

Ademais, determinou que a estrutura de gerenciamento do risco operacional adotada pelas instituições contivesse as etapas de identificação, avaliação, monitoramento, controle e mitigação do risco, demonstrando, assim, o seu alinhamento às melhores práticas de gestão de riscos propostas pelos referenciais da ISO 31000:2009 e COSO ERM, discutidos em tópicos anteriores.

Debruçando-se especificamente sobre a realidade do BCB, verifica-se que dispõe de um setor específico para executar a política de gerenciamento de riscos da autarquia, denominado Departamento de Riscos Corporativos e Referências

Operacionais (Deris), subordinado ao Diretor de Assuntos Internacionais e de Gestão de Riscos Corporativos (Direx).

O Deris encontra-se subdividido em Risco Financeiro, Risco Não Financeiro – dentro da qual se inclui a análise do risco operacional - e Gestão de Continuidade do Negócio.

Recortando a análise somente para riscos operacionais, tem-se que o processo de gestão definido para essa categoria é executado em 5 etapas: (i) identificação e mensuração; (ii) avaliação e integração,; (iii) priorização e decisão, (iv) tratamento e controle e, por fim, (v) monitoramento e revisão.

Cada uma das etapas dispõe de suas próprias ferramentas de gestão de riscos operacionais, conforme figura abaixo:

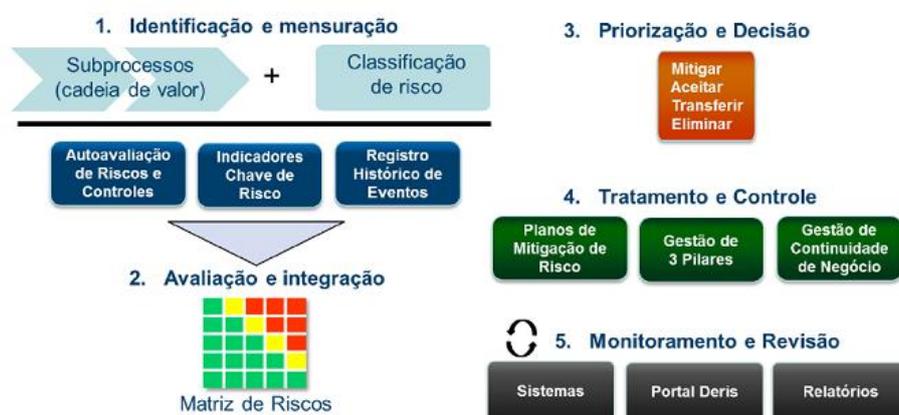


Figura 5: Processo de Gestão de Riscos Operacionais do Banco Central do Brasil  
Fonte: BRASIL, 2014c, p. 9

É possível extrair da figura que o BCB trabalha com 3 técnicas distintas para a identificação de riscos operacionais, quais sejam, Autoavaliação de Riscos e Controles (*Risk and Control Self Assessment - RSCA*), Registro Histórico de Eventos e Indicadores Chave de Risco.

O Registro Histórico de Eventos permite o armazenamento de todos os eventos ocorridos na autarquia em sistema próprio, denominado Sistema de Registro de Eventos de Risco (SRE). A técnica de Indicadores Chave de Risco, por sua vez, vale-se do suporte de outro sistema, chamado Helena, que possibilita a observação de séries históricas de indicadores específicos que sinalizam a possível ocorrência de eventos de risco no futuro (BRASIL, 2014c, p. 14).

No tocante à técnica RSCA, destaca-se que ela “identifica eventos em potencial a que está exposta a entidade, por meio de painéis de referência realizados com os

servidores” (BRASIL, 2014c, p. 14). A referência adotada pelo BCB, como classificação de risco, é a taxonomia recomendada pelo Basileia II, a qual tem o condão de orientar, padronizar e facilitar o levantamento de eventos pelos servidores.

De forma mais detalhada, a Diretoria Colegiada estabelece uma ordem de prioridade para as unidades/departamentos da autarquia, a partir da análise dos processos de 3º nível da Cadeia de Valor. Após, realiza *workshops* com as áreas selecionadas, os quais são conduzidos por servidores do Deris, auxiliados, ainda, pelo denominado Agente de Risco, isto é, um servidor previamente capacitado pelo referido Departamento na metodologia de gestão de riscos.

Nessas reuniões, os facilitadores percorrem toda a taxonomia de eventos de risco operacional alicerçada em Basileia II, a fim de identificar os eventos mais representativos de suas rotinas, suas causas e consequências, além dos controles existentes, com o intuito de definir a probabilidade e impacto de ocorrência do risco, que fornecerão subsídio às etapas posteriores.

Para maior elucidação do tema, segue abaixo taxonomia de eventos utilizada pelo BCB, estruturada a partir dos níveis de processo da Cadeia de Valor:

**3** Ficha de Risco  
Identificação do Risco

Nível 1	Nível 2	Nível 3
Fraude interna	<ul style="list-style-type: none"> <li>✓ Atividade não autorizada</li> <li>✓ Furto</li> </ul>	
Fraude externa	<ul style="list-style-type: none"> <li>✓ Furto e fraude externos</li> <li>✓ Invasão de sistemas</li> </ul>	
Dano a bens físicos	Desastres e outros eventos	<ul style="list-style-type: none"> <li>✓ Desastres</li> <li>✓ Terrorismo e vandalismo</li> </ul>
Interrupção de atividade e falha de sistema	Sistemas	<ul style="list-style-type: none"> <li>✓ Software/ hardware/ rede</li> <li>✓ Serviços de infraestrutura e fornecimentos essenciais</li> </ul>

Nível 1 e 2: definido por Basileia II  
Nível 3: detalhamento do BCB

 BANCO CENTRAL DO BRASIL      Departamento de Riscos Corporativos e Referências Operacionais DERIS      [deris@bcb.gov.br](mailto:deris@bcb.gov.br)

Figura 6: Identificação de Risco do BCB parte 1

Fonte: Cópia de Slide apresentado pelo Deris em visita técnica realizada em 22 de junho de 2017

### 3 Ficha de Risco Identificação do Risco

Nível 1	Nível 2	Nível 3
Execução e Gerenciamento de Processos e de Informação	Execução e Gerenciamento de Processos	<ul style="list-style-type: none"> <li>✓ Erro de informação</li> <li>✓ Falha na execução de processos/ práticas de compliance</li> <li>✓ Perda de prazo/ atraso atendimento de demandas</li> <li>✓ Erro contábil</li> <li>✓ Falha na transferência de recursos</li> </ul>
	Contraparte	<ul style="list-style-type: none"> <li>✓ Perda de prazo da contraparte</li> <li>✓ Falha na transferência de recursos da contraparte</li> <li>✓ Erro de informação/ comunicação da contraparte</li> </ul>
	Gerenciamento da informação	<ul style="list-style-type: none"> <li>✓ Erro/ não de divulgação de informação interna</li> <li>✓ Erro/ não divulgação de informação externa</li> </ul>
	Fornecedor	<ul style="list-style-type: none"> <li>✓ Produto/ serviço não conforme</li> <li>✓ Disputas legais</li> </ul>
Prática Trabalhista e Segurança do Trabalho	<ul style="list-style-type: none"> <li>✓ Recursos Humanos e Cultura</li> <li>✓ Segurança do Trabalho</li> </ul>	
Práticas de Negócio e legal	Partes interessadas	<ul style="list-style-type: none"> <li>✓ Obrigação legal</li> </ul>

Nível 1 e 2: definido por Basileia II  
Nível 3: detalhamento do BCB

 BANCO CENTRAL DO BRASIL
Departamento de Riscos Corporativos e Referências Operacionais  
DERIS
deris@bcb.gov.br

Figura 7: Identificação de Risco do BCB parte 2

Fonte: Cópia de Slide apresentado pelo Deris em visita técnica realizada em 22 de junho de 2017

O produto dos *workshops* é o preenchimento da Ficha de Risco, com todas as informações acima apresentadas de qualificação do risco, dentre as quais se destaca o campo *taxonomia do evento*, que possibilita a uniformização e consequente avaliação sistêmica dos riscos operacionais da instituição.

### 3 Ficha de Risco Identificação do Risco

**Identificação do Risco**

Taxonomia de Evento: Erro de Informação

Descrição do Risco

Repasso de informação indevida/ incorreta ao usuário (help desk interno e externo/Sisbacen)

Observações

Não há.

Figura 8: Ficha de Risco - Identificação do Risco

Fonte: Cópia de Slide apresentado pelo Deris em visita técnica realizada em 22 de junho de 2017.

Ressalta-se, apenas, que, para facilitar as etapas seguintes, principalmente a de tratamento do risco, é dado ao gestor da unidade, após selecionar a taxonomia do

evento, descrever o risco de forma mais detalhada, a fim de customizá-lo à sua realidade, com maior fidedignidade

Ante o exposto, destaca-se que, dentre as recomendações implementadas pelo BCB relativas ao Acordo de Basiléia II, a boa prática de orientação da fase de identificação de riscos por meio de taxonomia previamente definida contribui para fortalecer tanto a metodologia de gestão de riscos operacionais adotada, como o próprio sistema de governança da autarquia, ao permitir a realização de controle sistêmico e integral dos riscos operacionais.

#### **4.9 Análise da gestão de riscos no contexto do Poder Judiciário brasileiro**

Dentre os Tribunais Superiores brasileiros, o exame de dados secundários leva à conclusão de que apenas o Tribunal Superior do Trabalho e o Superior Tribunal de Justiça possuem Política de Gestão de Riscos publicada, com posterior desenvolvimento de metodologia própria.

O Tribunal Superior do Trabalho, por meio do Ato ASGE.SEGP.GP nº 93, de 25 de fevereiro de 2015, instituiu o Comitê de Gestão de Riscos da Secretaria do TST, o qual formulou a Política de Gestão de Riscos do órgão, que foi publicada por meio do Ato nº 131/ASGE.SEGP.GP, de 13 de março de 2015.

Nesta Política, o Tribunal define as seguintes categorias de riscos: estratégicos, operacionais, de comunicação e de conformidade. Os operacionais, por sua vez, “estão associados à ocorrência de perdas (produtividade, ativos e orçamentos) resultantes de falhas, deficiências ou inadequação de processos internos, estrutura, pessoas, sistemas, tecnologia, assim como de eventos externos (catástrofes naturais, greves, fraudes)” (BRASIL, 2015c).

A descrição detalhada das fases, dos procedimentos e dos instrumentos necessários ao processo de gestão de riscos foi apresentada no Plano de Gestão de Riscos da Secretaria do TST, tornado público em 16 de junho de 2015 (BRASIL, 2015a).

Tal documento estabelece, em seu anexo IX, o contexto geral do órgão, definindo, para tanto, categorias de eventos de riscos, classificadas em: Conformidade e Fiscalização, Regulamentação, Econômicos, Recursos Humanos, Fornecedores, Tecnologia da Informação, Desastres, Controles Físicos, Reputação, Cultura Organizacional, Ambiente Cultural, Social e Político.

Essas categorias, por sua vez, são distribuídas pelos contextos externo e interno, da seguinte forma:

Contexto Interno	Contexto Externo
<b>Conformidade e Fiscalização:</b> <ul style="list-style-type: none"> <li>• Normatização, controle e fiscalização interna;</li> <li>• Gestão dos elementos que influenciam o alcance dos objetivos estratégicos.</li> </ul>	<b>Regulamentação:</b> <ul style="list-style-type: none"> <li>• Ambiente regulatório;</li> <li>• Aderência aos principais requisitos regulatórios externos.</li> </ul>
<b>Recursos Humanos:</b> <ul style="list-style-type: none"> <li>• Carga de trabalho;</li> <li>• Segregação de funções;</li> <li>• Clima organizacional.</li> </ul>	<b>Fornecedores:</b> <ul style="list-style-type: none"> <li>• Relação com os fornecedores;</li> <li>• Sanções ao contratado;</li> <li>• Cláusulas contratuais sobre a entrega do objeto contratado.</li> </ul>
<b>Tecnologia da Informação:</b> <ul style="list-style-type: none"> <li>• Abrangência dos benefícios da TI;</li> <li>• Demanda interna por recursos de TI;</li> <li>• Alinhamento da TI ao plano corporativo de continuidade de negócios;</li> <li>• Definição de parâmetros mínimos de qualidade e eficiência dos serviços prestados pela TI.</li> </ul>	<b>Desastres:</b> <ul style="list-style-type: none"> <li>• Inundação, incêndio, etc.;</li> <li>• Vandalismo, terrorismo.</li> </ul>
<b>Controles Físicos:</b> <ul style="list-style-type: none"> <li>• Controles de segurança física;</li> <li>• Alinhamento entre os controles de segurança física e lógica;</li> <li>• Existência do Plano de Continuidade de Negócios ou Plano de Recuperação de Desastres</li> </ul>	<b>Reputação:</b> <ul style="list-style-type: none"> <li>• Percepção da sociedade.</li> </ul>
<b>Cultura Organizacional</b> <ul style="list-style-type: none"> <li>• Adaptação da cultura organizacional às mudanças no contexto interno.</li> </ul>	<b>Ambiente Cultural, Social e Político:</b> <ul style="list-style-type: none"> <li>• Mudanças de governo.</li> </ul>
<b>Econômicos</b> <ul style="list-style-type: none"> <li>• Disponibilidade financeiro-orçamentária.</li> </ul>	

Figura 9: Tabela de Contexto Interno e Externo do TST

Fonte: Plano de Gestão de Riscos da Secretaria do Tribunal Superior do Trabalho (BRASIL, 2015a, p. 23)

O referido documento também destaca que cabe ao gestor da unidade, com base no contexto geral apresentado, definir o seu contexto específico, a partir do ajuste das categorias apresentadas, seja pela exclusão daquelas que não condizem com o processo de trabalho avaliado, seja pela inclusão das não previstas.

Em seu Anexo X, encontram-se alguns exemplos de riscos, sendo relevante destacar os enquadrados na categoria Riscos Operacionais e de Recursos Humanos, assim exemplificados: responsáveis por atividades operacionais não definidos; falta de execução dos testes do plano de recuperação de desastres e funções e responsabilidades não segregadas.

O Superior Tribunal de Justiça, por sua vez, instituiu sua Política de Gestão de Riscos por meio da Instrução Normativa STJ/GP n. 17, de 17 de dezembro de 2015, a qual subsidiou a criação do Plano de Gestão de Riscos do órgão no ano seguinte.

Neste documento, o STJ apresenta a sua metodologia de gestão de riscos, que trabalha a partir das seguintes categorias de risco: ambiental, conformidade, econômico, jurisdicional, pessoal, tecnológico (BRASIL, 2016c, p.18-19).

Dessa forma, verifica-se que, no que tange aos Tribunais Superiores, a adoção de políticas de gestão de riscos ainda é um fenômeno recente e não majoritário. Ademais, dentre os supracitados órgãos que a detêm, não há consenso entre as categorias de riscos adotadas - em que pese vivenciarem eventos de riscos semelhantes - o que impossibilita a implementação de um controle sistêmico dos riscos gerenciados.

No âmbito da Justiça Federal, no entanto, a realidade é distinta. O Conselho da Justiça Federal – CJF – aprovou, por meio da Resolução n. 447, de 07 de junho de 2017, a Política de Riscos do Conselho e da Justiça Federal de primeiro e segundo grau.

Tal documento trouxe a determinação de que suas diretrizes teriam que ser implantadas pelos Tribunais Regionais Federais e Seções Judiciárias no prazo de 180 dias, a contar de sua publicação. Dessa forma, o CJF avançou no sentido de estabelecer critérios gerais sobre os princípios, conceitos, diretrizes, níveis e estrutura do gerenciamento de riscos, além da definição dos papéis e responsabilidades dos atores envolvidos.

Para tanto, propôs uma Estrutura de Governança da Gestão de Riscos do Conselho e da Justiça Federal de primeiro e segundo grau, composta pelo Comitê Gestor de Estratégia da Justiça Federal - de que trata o art. 3º da Resolução CJF n. 313/2014 - pelo Comitê Permanente de Gestão de Riscos do CJF, Comitês Gestores Regionais e Seccionais de riscos e pelos Proprietários dos Riscos, assim denominados todos os ocupantes de cargo comissionados e os responsáveis pelos processos de trabalho.

Em breve síntese, ao primeiro foi concedida a atribuição de fomento e disseminação da cultura de gestão de riscos, aos Comitês em 2º nível na hierarquia, coordenar o processo de gestão de riscos, enquanto os proprietários do risco ficaram responsáveis pela identificação, análise, avaliação, tratamento e monitoramento dos riscos em suas respectivas áreas de atuação (BRASIL, 2017d, p.7).

Contudo, a análise pormenorizada da mencionada Política demonstra a inexistência de definição quanto à categorização de riscos, não se constatando, assim, uma preocupação do Conselho da Justiça Federal em estabelecer uma padronização na linguagem adotada para a identificação dos riscos, deixando a cargo de cada ator a definição de qual categoria de risco utilizar.

Nesse contexto, dentre os Tribunais Regionais Federais, apenas o da 3ª Região desenhou uma classificação de seus riscos, ao determinar, no artigo 3º da Resolução PRES 136/2017, que a Administração do Tribunal definirá o grau de tolerância aos riscos operacionais, de informações e de conformidade, os quais poderão ser assumidos pelos diversos níveis da gestão (BRASIL, 2017e).

Para o recorte metodológico realizado no presente artigo, vale destacar também que o Tribunal Regional Federal da 4ª Região apresentou uma lista de fatores internos e externos que devem ser considerados quando do estabelecimento do contexto geral da instituição, que subsidiará a fase seguinte de identificação de riscos:

FATORES	
Contexto Externo	Contexto Interno
<ul style="list-style-type: none"> <li>*Ambiente cultural, social, político, legal, regulatório, financeiro, tecnológico, econômico, natural e competitivo, quer seja internacional, nacional, regional ou local</li> <li>*Fatores-chave e tendências que tenham impacto sobre os objetivos da entidade</li> <li>*Relações com partes interessadas externas e suas percepções e valores</li> </ul>	<ul style="list-style-type: none"> <li>*Governança, estrutura organizacional, funções e responsabilidades</li> <li>*Políticas, objetivos e estratégias implementadas para atingi-los</li> <li>*Capacidades, entendidas em termos de recursos e conhecimentos</li> <li>*Sistemas de informação, fluxos de informação e processos de tomada de decisão, formais e informais</li> <li>*Relações com partes interessadas externas e suas percepções e valores</li> <li>*Cultura institucional</li> <li>*Normas, diretrizes e modelos adotados pela entidade</li> <li>*Norma e extensão das relações contratuais.</li> </ul>

Tabela 2: Contexto Interno e Externo TRF 4

Fonte: Adaptado da Política de Gestão de Riscos do TRF da 4ª Região (BRASIL, 2015d).

No âmbito da Justiça Eleitoral, mister salientar o Plano de Gestão de Riscos do Tribunal Regional Eleitoral do Ceará, que determina que os riscos identificados na Corte devem ser categorizados conforme a Estrutura Analítica de Riscos determinada abaixo:

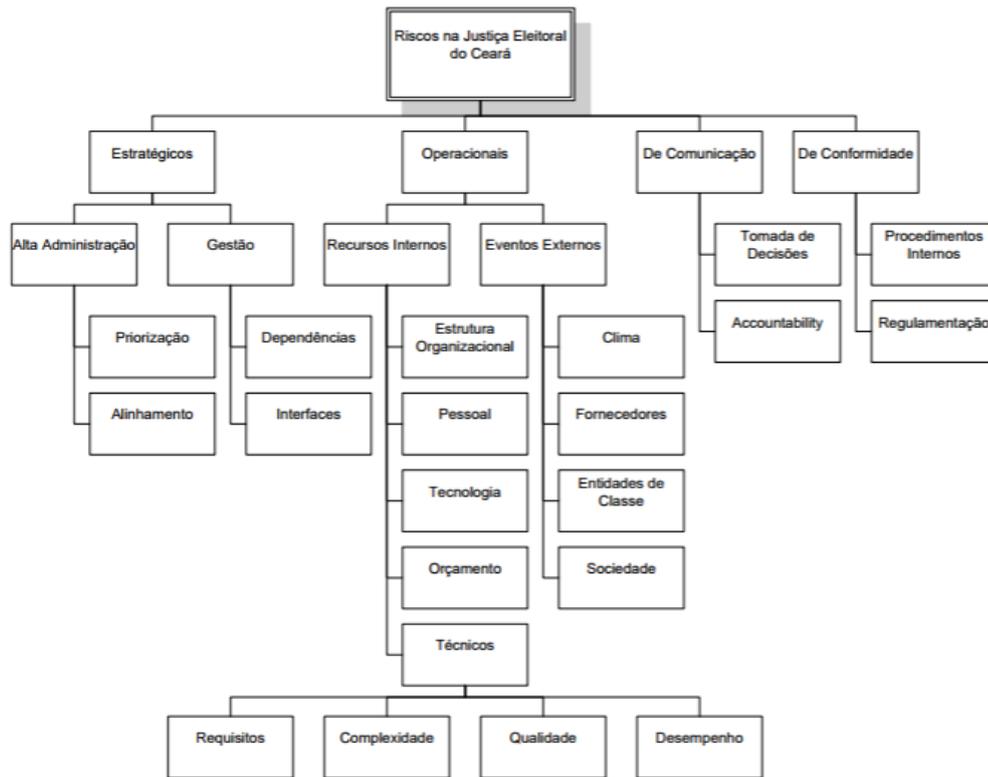


Figura 10: Estrutura Analítica de Riscos da Justiça Eleitoral do Ceará  
 Fonte: Plano de Gestão de Riscos da Justiça Eleitoral do Ceará (BRASIL, 2015e, p. 5)

Nitidamente, verifica-se o esforço do aludido Tribunal em definir uma categorização comum aos riscos, aprofundando a classificação - amplamente utilizada no Poder Judiciário - de riscos estratégicos, operacionais, de comunicação e de conformidade, ao estabelecer também as fontes de risco vinculadas a cada um dos referidos tipos.

Para finalizar, salienta-se ainda não ser possível extrair boas práticas do segmento da justiça estadual, uma vez que vivencia estágio inicial de adoção da gestão de riscos, destacando-se apenas o Tribunal de Justiça do Distrito Federal e Territórios e o do Rio Grande do Norte como detentores de Políticas formalizadas sobre o tema, nos termos da Portaria Conjunta TJDFT 15/2017 e Portaria TJRN 1.110/2017, respectivamente.

## 5. PROPOSTA DE TAXONOMIA DE EVENTOS DE RISCO OPERACIONAL DO PODER JUDICIÁRIO

Considerando todo o arcabouço teórico levantado, em conjunto com o exame do gerenciamento de riscos pelo Banco Central do Brasil e de alguns relevantes normativos de tribunais brasileiros, propõe-se a seguir uma taxonomia de eventos de risco operacional para o Poder Judiciário:

## TAXONOMIA DE EVENTOS DE RISCO OPERACIONAL DO PODER JUDICIÁRIO

FONTE	CATEGORIA NÍVEL 1	CATEGORIA NÍVEL 2	EXEMPLOS DE EVENTOS DE RISCO	DESCRIÇÃO
1. PROCESSOS	1.1 MODELAGEM		Falha de metodologia de gestão de processos Deficiência na atualização dos fluxos de processos Falta de revisão periódica da pertinência do desenho do fluxo	Perdas decorrentes de falhas no desenho, redesenho e documentação de processos
	1.2 GERENCIAMENTO	1.2.1 Planejamento	Baixa capacidade de planejamento Não-envolvimento de todos os atores que compõem o processo Definição equivocada de esforço/prazos para execução do processo	Perdas decorrentes de falhas no gerenciamento do processo, incluindo todos os eventos relativos às etapas de planejamento, execução e monitoramento
		1.2.2 Execução	Falhas diversas na execução do processo Fraudes internas Descumprimento de normas regimentais/legais Perda de prazo/atraso no atendimento das demandas Deficiência de recursos necessários para a execução das tarefas	
		1.2.3 Monitoramento	Falha nos indicadores de processo Não-realização de ciclos de avaliação e melhoria do processo Ineficiência do sistema de controle interno	
	1.3 COMUNICAÇÃO INTERNA	1.3.1 Erro de Informação	Baixa transparência de dados Armazenamento disperso de informações Divulgação interna/externa de dados imprecisos	Perdas derivadas de informações imprecisas, incorretas, desatualizadas ou incompletas, geradas pelo processo de trabalho
		1.3.2 Relacionamento entre atores	Deficiência na comunicação entre os atores envolvidos no processo Falhas nos canais próprios para comunicação	

<b>2. PESSOAS</b>	<b>2.1 CARGA DE TRABALHO</b>		Dimensionamento inadequado da capacidade operacional Inadequação da segregação de funções Alta rotatividade ( <i>turnover</i> ) que impacta o desempenho do processo	Perdas relativas a falhas na compatibilização entre as atividades exigidas pelo cargo, a força de trabalho disponível e a jornada laboral
	<b>2.2 COMPETÊNCIAS</b>	<b>2.2.1 Organizacionais</b>	Desempenho de tarefas por servidores com baixa qualificação profissional Desconhecimento, pelo servidor, de suas atividades e/ou responsabilidades Centralização do conhecimento em servidores específicos (falta de gestão do conhecimento) Deficiência dos planos de capacitação do órgão/ferramentas de gestão de desempenho	Perdas derivadas de deficiência de conhecimento, habilidades e atitudes necessários à execução do processo
		<b>2.2.2 Gerenciais</b>	Seleção de gestores com baixa qualificação para o cargo Perseguições pessoais	
	<b>2.3 AMBIENTE ORGANIZACIONAL</b>		Insatisfação do servidor com o ambiente de trabalho/clima organizacional Condições insalubres ou inapropriadas de trabalho Conflitos pessoais Alta resistência à mudança Greves	Perdas referentes a deficiências no clima organizacional ou nas condições de trabalho
<b>3. ESTRUTURA</b>	<b>3.1 ARQUITETURA</b>		Inadequação da estrutura de hierarquia das unidades Inadequação do espaço físico disponível para desempenho das atividades Criação/extinção de unidades sem necessário estudo prévio Deficiência no tratamento de demandas transversais	Perdas decorrentes da modelagem da estrutura organizacional, envolvendo desde o desenho adotado, seus componentes e condicionantes, até o seu alinhamento à estratégia da organização
	<b>3.2 ESTRATÉGIA</b>		Falha no alinhamento da estrutura à estratégia Definição de atribuições legais de unidade em descompasso com os objetivos estratégicos	

4. AMBIENTE TECNOLÓGICO	4.1 AMBIENTE INTERNO	4.1.1 Sistemas	<p>Falha de sistema crítico ao desempenho das atividades</p> <p>Acesso indevido aos sistemas/rede</p> <p>Instabilidade de sistemas operacionais</p> <p>Deficiência ou indisponibilidade de rede</p> <p>Ataques à rede</p> <p>Intempestividade das atualizações do sistema</p> <p>Geração de informações não-confiáveis ou insuficientes</p> <p>Inadequação do grau de informatização do processo</p>	Perdas decorrentes de indisponibilidade ou falhas de sistemas e da infraestrutura tecnológica
		4.1.2 Infraestrutura	<p><i>Overload</i> (sobrecarga no sistema elétrico, de processamento de dados)</p> <p>Deficiência na proteção dos bancos de dados</p> <p>Perda de dados (deficiência de <i>backup</i>)</p>	
	4.2 TECNOLOGIA		<p>Obsolescência de equipamentos</p> <p>Inadequação da solução tecnológica à necessidade do processo</p> <p>Complexidade da solução tecnológica que impede/dificulta a sua utilização</p> <p>Adoção de tecnologia com baixa interoperabilidade com outros sistemas</p>	Perdas decorrentes de obsolescência ou inadequação de tecnologia às necessidades do processo
5 ORÇAMENTO	5.1 GERENCIAMENTO	5.1.1 Planejamento	<p>Planejamento das atividades em descompasso ao ciclo orçamentário</p> <p>Não-inclusão de despesas relevantes no planejamento do gasto</p> <p>Deficiência de planejamento de médio e longo prazo</p>	Perdas decorrentes de falhas na gestão do orçamento, incluindo os eventos relativos às etapas de planejamento, execução e monitoramento
		5.1.2 Execução	<p>Inadequação do quantitativo planejado de recursos</p> <p>Ausência não programada de recurso</p>	
		5.1.3 Monitoramento	<p>Baixa transparência dos dados orçamentários</p> <p>Inadequação dos mecanismos de controle</p>	

<b>6. EVENTOS EXTERNOS</b>	<b>6.1 REGULAMENTAÇÃO</b>		Alteração normativa inesperada Necessidade de adaptação a novo marco regulatório	Perdas referentes a alterações na legislação e regulamentação que impactam o processo de trabalho	
	<b>6.2 FRAUDE</b>		Recebimento de documentação falsa Apropriação, por terceiros, de valores financeiros Obtenção, por terceiros, de informação sigilosa	Perdas decorrentes de atos de terceiros com o propósito de obter vantagem ilícita, por meio da adoção de comportamento arдил	
	<b>6.3 FORNECEDORES</b>		Descontinuidade de fornecimento Entrega de produto defeituoso Execução ineficiente de serviço Sanções	Perdas relativas a falhas no relacionamento com fornecedores	
	<b>6.4 REPUTAÇÃO</b>		Cobertura negativa da mídia Avaliação negativa dos usuários Fragilidade institucional	Perdas relativas a danos na imagem e reputação da organização	
	<b>6.5 DANOS A BENS FÍSICOS</b>	<b>6.5.1 Ação Humana</b>		Vandalismo, terrorismo	Perdas decorrentes da ação humana ou de desastres naturais que causem danos ao patrimônio da organização, prejudicando a continuidade de suas atividades
		<b>6.5.2 Desastres Naturais</b>		Inundação, incêndio, desabamento	
	<b>6.6 CONTEXTO POLÍTICO, ECONÔMICO E SOCIAL</b>			Contingenciamento orçamentário Mudança repentina de orientação política	Perdas referentes a alterações na situação econômica, financeira e/ou social do país, que interfiram na execução do processo

A taxonomia proposta foi construída à luz da estrutura matricial de Basiléia II, também adotada pelo BCB. O objetivo foi facilitar a identificação, por parte dos servidores, de eventos de risco operacional, a partir da disposição hierarquizada das fontes e suas respectivas categorias de eventos, acompanhadas de exemplos de eventos de risco mais comuns na rotina das organizações.

Assim, procurou-se definir, de início, as principais fontes de risco internas e externas presentes na realidade dos tribunais. Para tanto, valeu-se das fontes propostas pelo Manual de Gestão Integrada de Riscos Corporativos do Ministério da Fazenda

(BRASIL, 2016a), acrescidas de “Estrutura” e “Orçamento”, retiradas do Plano de Gestão de Riscos da Justiça Eleitoral do Ceará (BRASIL, 2015e, p. 5).

Após, incorporou-se o conceito de categoria de evento de risco, apresentado pelo Plano de Gestão de Riscos da Secretaria do Tribunal Superior do Trabalho (BRASIL, 2015a, p. 23), a fim de detalhar as fontes selecionadas.

Esse processo levou à pormenorização das fontes em dois níveis de categorias, sendo que o segundo nível só foi explicitado quando se observou a necessidade de definição mais apurada do termo apresentado no primeiro.

Em adição, explicitaram-se, com base no Manual de Gestão Integrada de Riscos Corporativos do Ministério da Fazenda (BRASIL, 2016a), alguns exemplos de eventos de risco operacional vinculados às suas respectivas categorias, com o escopo de consolidar o entendimento dos conceitos utilizados, assim como municiar os tribunais com subsídios básicos para iniciar a etapa de identificação de riscos.

Destaca-se, ainda, o esforço realizado para descrever o escopo de cada categoria de evento apresentada no nível 1 - inspirado no *modus operandi* do BCB - considerando o fim último de unificação da linguagem adotada pela justiça brasileira, necessário à implementação de um sistema de controle integral pelo Conselho Nacional de Justiça.

Ademais, o arranjo matricial escolhido permite e facilita a avaliação do desempenho de cada categoria de evento, bastando, para tanto, a coleta e análise dos dados de um evento de nível 3, por exemplo.

Tal vinculação em cadeia tem o condão, portanto, de fornecer ao CNJ subsídios suficientes para mapear as categorias mais críticas de eventos operacionais do Poder Judiciário, aperfeiçoando não apenas os mecanismos de supervisão, mas também o próprio debate acerca dos caminhos e mecanismos necessários para tratá-los.

## 6. CONCLUSÃO

Ao se examinar os principais conceitos relacionados à gestão de risco, esmiuçando-se os seus princípios, processo e estrutura, afiguram-se como evidentes os benefícios advindos de sua implementação no âmbito da administração pública.

Nesse contexto, o aperfeiçoamento do processo de tomada de decisão, a partir do fornecimento de informações objetivas e seguras sobre riscos e oportunidades, têm reflexos diretos na melhoria da alocação de recursos, no atingimento dos objetivos organizacionais, na conformidade às exigências legais e na diminuição de custos e perdas pela instituição.

Tais reflexos, quando analisados em conjunto, tem o condão não apenas de aprimorar os sistemas de controle interno, mas a própria estrutura de governança corporativa, destacando-se o gerenciamento de riscos, portanto, como uma importante ferramenta de desenvolvimento institucional e de geração de valor público.

Inobstante a manifesta relevância desta ferramenta, vislumbram-se tímidos avanços no Poder Judiciário relativos à sua adoção. O panorama atual dispõe de isoladas iniciativas - dispersas nos diferentes segmentos de justiça -, ainda na fase inicial de estabelecimento de princípios e diretrizes, sendo, portanto, escassos os tribunais com robustas metodologias desenvolvidas sobre o tema.

Por essa razão, a experiência do Banco Central do Brasil destaca-se como um *benchmark* necessário ao desiderato de alterar a realidade da justiça pátria, especialmente no que se refere à boa prática de adoção de taxonomia de eventos de risco operacional hábil a orientar a identificação de riscos e, mais importante, a padronizar a linguagem adotada pelas instituições financeiras.

Relevante destacar que não se desconhece o fato de que qualquer classificação que se pretende aplicável a todas as organizações de uma área de negócio tem um viés utópico, haja vista não ser possível apresentar de forma exaustiva qualquer categorização que agregue as especificidades de cada setor de atuação.

Ademais, conforme bem ressaltado por Crouhy et al (2006, p. 15), ao mesmo tempo em que classificações facilitam o reconhecimento de eventos, o seu gerenciamento e controle, elas apresentam o risco de não identificar eventos que fluam através das arbitrárias linhas de divisão propostas, uma vez que o observador encontra-se centrado apenas nos limites definidos.

Entretanto, considerando a baixa maturidade dos órgãos do Poder Judiciário na temática em apreço, acredita-se que a eventual não-identificação de riscos em face do

estabelecimento de uma categorização comum não sobrepujará os benefícios advindos da facilitação da etapa inicial de levantamento de riscos e da possibilidade de controle sistêmico e integral de riscos pela Justiça.

Por essa razão, à luz de todos os referenciais teóricos apresentados, formulou-se uma taxonomia que procurou estabelecer as principais fontes de risco internas e externas a uma organização, pormenorizadas em categorias de eventos. Estas, por sua vez, foram hierarquizadas em dois níveis, a depender do grau de detalhamento necessário. Ao final, foram sugeridos múltiplos exemplos de eventos de risco operacional, a fim de guiar os tribunais na fase de identificação de riscos.

Nesse ponto, salutar o aparte de que os riscos operacionais neste artigo levantados não se exaurem na realidade dos tribunais brasileiros, podendo ser orientadores de instituições tanto do Poder Executivo como do Legislativo, uma vez que não são atrelados à atividade fim do Judiciário, mas sim a pessoas, processos, sistemas, isto é, aos componentes intrínsecos à gestão organizacional em sua essência.

Feita tal consideração, assevera-se que a unificação do entendimento sobre a categoria de riscos operacionais e a prévia identificação dos seus mais relevantes eventos carrega, como fim último, habilitar o Conselho Nacional de Justiça a supervisionar e acompanhar o gerenciamento de riscos operacionais por parte dos tribunais brasileiros, fortalecendo a sua competência de controle da atuação administrativa e financeira das Cortes de Justiça pátrias.

Frise-se, contudo, não ter sido o escopo deste trabalho propor um modelo de gestão de riscos, a ser adotado por todo o Poder Judiciário, mas tão somente estabelecer uma taxonomia de eventos de risco, que, por natureza, é parte integrante de um modelo, mas não deve com ele ser confundida.

Por fim, destaca-se que este artigo realizou um estudo exploratório que não tem a intenção de esgotar o tema em análise. Inclusive, como objeto de pesquisa para ulterior aprofundamento, identifica-se a possibilidade de envolvimento da Rede de Governança Colaborativa do Poder Judiciário, instituída pela Portaria CNJ n. 138/2013, na discussão e posterior validação da taxonomia ora proposta.

Por congrega servidores e magistrados dos variados segmentos de Justiça, distribuídos por todas as regiões geográficas, acredita-se que a atuação da Rede, além de propiciar valorosas contribuições extraídas das práticas rotineiras de cada Corte, possibilitará a disseminação da cultura de risco, fator crítico de sucesso a uma gestão de riscos efetiva.

Em adição, considerando a unicidade do Poder Judiciário, o mesmo método proposto por esta pesquisa poderia ser aplicado à definição de riscos inerentes à função judicante e até mesmo a riscos estratégicos, visto a obrigatoriedade de alinhamento dos planos estratégicos dos órgãos do Judiciário à Estratégia Nacional definida na Resolução CNJ n. 198/2014.

O método proposto também poderia ser usado para a definição de controles básicos para cada categoria de nível operacional estabelecida na taxonomia proposta, a fim de orientar e auxiliar os tribunais na etapa de tratamento de seus riscos. Como *benchmark* possível, vislumbra-se o Ministério da Fazenda, que já tem definição própria nesse sentido, disposta no Manual de Gestão Integrada de Riscos Corporativos (BRASIL, 2016).

## 7. REFERÊNCIAS BIBLIOGRÁFICAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS - ABNT. NBR ISO 31.000. **Gestão de Riscos – Princípios e Diretrizes**. Rio de Janeiro: ABNT, 2009.

BANCO DO BRASIL. **Acordo de Basiléia**. [2008]. Disponível em: <<http://www.bb.com.br/portalbb/page51,136,3696,0,0,1,8.bb?codigoNoticia=7724>>. Acesso em: 16 out. 2017.

BANK FOR INTERNATIONAL SETTLEMENTS – BIS. **Basel II: International Convergence of Capital Measurement and Capital Standards: a Revised Framework**. 2004. Disponível em: <<http://www.bis.org/publ/bcbs107.pdf>>. Acesso em: 17 ago. 2017.

\_\_\_\_\_. **Sound Practices for the Management and Supervision of Operational Risk**. 2003. Disponível em: <<https://www.bis.org/publ/bcbs96.htm>>. Acesso em: 20 out. 2017.

BASILÉIA II (Basel II): **International Convergence of Capital Measurement and Capital Standards: A Revised Framework**. 2005. Disponível em: <<http://www.bis.org>>. Acesso em: 15 ago. 2017.

BERNSTEIN, P.L. **Desafio aos Deuses: a fascinante história do risco**. São Paulo: Campus, 1997. 389 p.

BRASIL. BANCO CENTRAL DO BRASIL. **Comunicado nº 12.746, de 9 de dezembro de 2004**. Comunica os procedimentos para a implementação da nova estrutura de capital - Basiléia II. Disponível em: <<https://www3.bcb.gov.br/normativo/detalharNormativo.do?N=104206982&method=detalharNormativo>>. Acesso em: 22 out. 2017.

\_\_\_\_\_. BANCO CENTRAL DO BRASIL. **Resolução nº 3.380, de 22 de junho de 2006**. Dispõe sobre a implementação de estrutura de gerenciamento do risco operacional. Disponível em: <

[http://www.bcb.gov.br/pre/normativos/res/2006/pdf/res\\_3380\\_v2\\_L.pdf](http://www.bcb.gov.br/pre/normativos/res/2006/pdf/res_3380_v2_L.pdf)>. Acesso em: 15 set. 2017.

\_\_\_\_\_. PRESIDÊNCIA DA REPÚBLICA. **Lei nº 12.846, de 1º de agosto de 2013.** Dispõe sobre a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira, e dá outras providências. Disponível em: <[http://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2013/lei/112846.htm](http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/112846.htm)>. Acesso em: 16 set. 2017.

\_\_\_\_\_. TRIBUNAL DE CONTAS DA UNIÃO. **Dez passos para a boa governança.** Brasília: TCU, Secretaria de Planejamento, Governança e Gestão, 2014a. 28 p.

\_\_\_\_\_. TRIBUNAL DE CONTAS DA UNIÃO. **Referencial Básico de Governança - Aplicável a Órgãos e Entidades da Administração Pública.** Brasília: TCU, 2014b. 80 p.

\_\_\_\_\_. TRIBUNAL DE CONTAS DA UNIÃO. **Relatório de Auditoria da Tomada de Contas 020.137/2014-1.** 2014c. Disponível em: <[www.tcu.gov.br/Consultas/Juris/Docs/judoc/Acord/.../AC\\_0548\\_09\\_15\\_P.doc](http://www.tcu.gov.br/Consultas/Juris/Docs/judoc/Acord/.../AC_0548_09_15_P.doc)>. Acesso em: 23 out. 2017.

\_\_\_\_\_. CONSELHO NACIONAL DE JUSTIÇA. **Resolução nº 198, de 1º de julho de 2014.** Dispõe sobre o Planejamento e a Gestão Estratégica no âmbito do Poder Judiciário e dá outras providências. 2014d. Disponível em: <<http://www.cnj.jus.br/busca-atos-adm?documento=2733>>. Acesso em: 13 set. 2017.

\_\_\_\_\_. TRIBUNAL SUPERIOR DO TRABALHO. **Plano de Gestão de Riscos da Secretaria do Tribunal Superior do Trabalho.** Brasília: TST, 2015a. 49 p.

\_\_\_\_\_. CONSELHO DA JUSTIÇA FEDERAL. **Manual de Governança da Justiça Federal.** Brasília: CJF, 2015b. 48 p.

\_\_\_\_\_. TRIBUNAL SUPERIOR DO TRABALHO. **Ato nº 131/ASGE.SEGP.GP, de 13 de março de 2015.** Dispõe sobre a Política de Gestão de Riscos da Secretaria do Tribunal Superior do Trabalho e dá outras providências. 2015c. Disponível em: <[https://juslaboris.tst.jus.br/bitstream/handle/1939/58884/2015\\_ato0131.pdf?sequence=1&isAllowed=y](https://juslaboris.tst.jus.br/bitstream/handle/1939/58884/2015_ato0131.pdf?sequence=1&isAllowed=y)>. Acesso em: 27 out. 2017.

\_\_\_\_\_. TRIBUNAL REGIONAL FEDERAL (4ª Região). **Resolução nº 115, de 13 de novembro de 2015.** Dispõe sobre a Política de Gestão de Riscos do TRF da 4ª Região. 2015d. Disponível em: <<https://www.escavador.com/diarios/506967/TRF4/A/2016-01-07?page=2>>. Acesso em: 20 set. 2017.

\_\_\_\_\_. TRIBUNAL ELEITORAL DO CEARÁ. **Plano de Gestão de Riscos da Justiça Eleitoral do Ceará.** 2015e. Disponível em: <[www.justicaeleitoral.jus.br/arquivos/tre-ce-plano-de-gestao-de-riscos](http://www.justicaeleitoral.jus.br/arquivos/tre-ce-plano-de-gestao-de-riscos)>. Acesso em: 29 out. 2017.

\_\_\_\_\_. MINISTÉRIO DA FAZENDA. **Manual de Gestão Integrada de Riscos Corporativos.** 2ª Ed. Brasília: MF, 2016a. 45 p.

\_\_\_\_\_. MINISTÉRIO DO PLANEJAMENTO, ORÇAMENTO E GESTÃO. CONTROLADORIA-GERAL DA UNIÃO. **Instrução Normativa Conjunta nº 01, de 10 de maio de 2016.** Dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo federal. 2016b. Disponível em: <[http://www.cgu.gov.br/sobre/legislacao/arquivos/instrucoes-normativas/in\\_cgu\\_mpog\\_01\\_2016.pdf](http://www.cgu.gov.br/sobre/legislacao/arquivos/instrucoes-normativas/in_cgu_mpog_01_2016.pdf)>. Acesso em: 17 jul. 2017.

\_\_\_\_\_. SUPERIOR TRIBUNAL DE JUSTIÇA. **Gestão de riscos / Superior Tribunal de Justiça.** Ed. rev. e atual. em janeiro/2016. Brasília: STJ, 2016c. 21 p.

\_\_\_\_\_. MINISTÉRIO DO PLANEJAMENTO, DESENVOLVIMENTO E GESTÃO – MP. **Manual de Gestão de Integridade, Riscos e Controles Internos da Gestão.** Brasília: Assessoria Especial de Controles Internos, 2017a. 52 p.

\_\_\_\_\_. MINISTÉRIO DA TRANSPARÊNCIA, FISCALIZAÇÃO E CONTROLADORIA-GERAL DA UNIÃO. **Curso: Gestão de Riscos e Controles Internos no Setor Público.** Apostila. Brasília: CGU, 2017b. 53 p.

\_\_\_\_\_. TRIBUNAL DE CONTAS DA UNIÃO. **Roteiro de Auditoria de Gestão de Riscos.** Brasília: TCU, Secretaria de Métodos e Suporte ao Controle Externo, 2017c.

\_\_\_\_\_. CONSELHO DA JUSTIÇA FEDERAL. **Política de Riscos do Conselho e da Justiça Federal de primeiro e segundo graus.** 2017d. Disponível em: <<https://www2.cjf.jus.br/jspui/bitstream/handle/1234/49515/Res%20447-2017.pdf?sequence=1>>. Acesso em: 29 out. 2017.

\_\_\_\_\_. TRIBUNAL REGIONAL FEDERAL (3ª Região). **Políticas de Gestão por Processos e de Gerenciamento de Riscos no âmbito da Justiça Federal da 3ª Região.** 2017e. Disponível em: <<http://web.trf3.jus.br/diario/Consulta/VisualizarDocumento?CodigoTipoPublicacao=1&CodigoOrgao=1&CodigoDocumento=0&IdMateria=496941&NumeroProcesso=0>> Acesso em: 29 out. 2017

\_\_\_\_\_. TRIBUNAL DE CONTAS DA UNIÃO. **O que é gestão de riscos.** Sem data. Disponível em: <<http://portal.tcu.gov.br/gestao-e-governanca/gestao-de-riscos/o-que-e-gestao-de-riscos/>>. Acesso em: 28 ago. 2017.

CHORAFAS, D.N. **Operational Risk Control With Basel II: Basic Principles and Requirements.** Oxford: Elsevier Butterworth-Heinemann, 2004. 388 p.

CIPFA (The Chartered Institute of Public Finance and Accountancy). **Good Governance standard for public services.** Londres: Hackney Press, 2004. 38 p.

CORNFORD, A. **Basiléia II em meados de 2006 : Perspectivas para implementação e outros desenvolvimentos recentes.** Economia Política Internacional – Análise Estratégica. Campinas: Centro de Estudos de Relações Econômicas Internacionais – CERI, n. 8 – jan./jun. 2006. Disponível em: <[www.eco.unicamp.br/docprod/downarq.php?id=112&tp=a](http://www.eco.unicamp.br/docprod/downarq.php?id=112&tp=a)>. Acesso em: 17 out. 2017

COSO (Committee of Sponsoring Organizations of the Treadway Commission). **Gerenciamento de Riscos Corporativos - Estrutura Integrada.** Sumário Executivo. 2007. 141 p.

\_\_\_\_\_. **Enterprise Risk Management: Integrating with Strategy and Performance. Executive Summary.** 2017. 10 p.

CROUHY, M.; GALAI, D.; MARK, R. **The Essentials of Risk Management**. New York: McGrawHill, 2006. 431 p.

INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA - IBGC. **Gerenciamento de riscos corporativos: evolução em governança e estratégia**. Série Cadernos de Governança Corporativa, 19. São Paulo: IBGC, 2017. 64p.

INTERNATIONAL ORGANIZATION OF SUPREME AUDIT INSTITUTIONS – INTOSAI. **Diretrizes para as normas de controle interno do setor público**. Tradução: Cristina Maria Cunha Guerreiro, Delanise Costa e Soraia de Oliveira Ruther. Salvador: Tribunal de Contas do Estado da Bahia, 2007. 99 p.

LIMA, L. F. **Estudo sobre a Gestão Qualitativa do Risco Operacional como Prática de governança corporativa em Instituições Financeiras no Brasil**. 2007, 168 p. Dissertação (Mestrado em Ciências Contábeis e Financeiras). Pontifícia Universidade Católica de São Paulo, São Paulo, 2007.

MARSHALL, C. **Medindo e Gerenciando riscos operacionais em instituições bancárias**. Rio de Janeiro: Qualitymark, 2002.

MARTINS, H.F.; MARINI, C. **Governança Pública Contemporânea: uma tentativa de dissecação conceitual**. Revista do Tribunal de Contas da União. Ano 46, n. 130, maio/ago 2014, p. 42-53.

MORAES, W. **Implementação do gerenciamento de riscos operacionais na área de recebimento integrado: uma abordagem intervencionista em uma editora nacional**. 2017. 95 p. Dissertação (Mestrado em Ciências Contábeis) - Centro de Ciências Sociais e Aplicadas. Universidade Presbiteriana Mackenzie, São Paulo, 2017.

POLLITT, C.; HUPE, P. **Talking Governance: The Role of Magic Concepts**. Conference of the European Group for Public Administration, Saint Julian's, Malta, September 2-5, 2009. 32p.

REINO UNIDO. **Report of the Committee on the Financial Aspects of Corporate Governance**. Londres: Cadbury Committee, 1992. 90 p.

REINO UNIDO. **The Orange Book: Management of Risk - Principles and Concepts**. Londres: HM Treasury, 2004. 52 p.

SALGADO, M.H; CARETA, C.B. **Análise da Gestão de Riscos Operacionais – Caso de uma instituição bancária**. VI Congresso Nacional em Excelência em Gestão, 2010, 13 p.

WEBER, E. L.; DIEHL, C.A. **Gestão de riscos operacionais: um estudo bibliográfico sobre ferramentas de auxílio**. Revista de Contabilidade do Mestrado em Ciências Contábeis da UERJ (online), Rio de Janeiro, v. 19, n. 3, p. 41-58, set/dez, 2014.