Gestão de **Riscos Corporativos** do **Sescoop**

manual técnico

2ª edição

SESCOOP

Serviço Nacional de Aprendizagem do Cooperativismo

Coordenação
Giulianna Fardini

Gestão de Riscos Corporativos do Sescoop

manual técnico

Brasília-DF
2ª edição - 2020

SESCOOP
Serviço Nacional de Aprendizagem do Cooperativismo

Ficha Técnica

Conselho Nacional

Titulares
Márcio Lopes de Freitas
Ronaldo Ernesto Scucato
Luiz Vicente Suzin
Celso Ramos Régis
Ricardo Benedito Khouri
Alberto Alves Silva de Oliveira
Fernando Henrique Kohlmann Schwanke
Thaisis Barboza de Souza
Dênio Aparecido Ramos
Carlos Felipe Alencastro F. de Carvalho
João Edilson de Oliveira

Suplentes
Carlos André Santos de Oliveira
Leonardo Boesche
Remy Gorga Neto
Malaquias Ancelmo de Oliveira
Andréia Lúcia Araújo da Cruz de Carvalho
Fabiano Maluf Amui
Roberta Carolina C.T. Rios Bosco Soares
Alex Pereira Freitas
Joel Amaral Júnior
Luizita Fonseca Leite Pina

Conselho Fiscal

Titulares
José Arilo Carneiro Pereira
André Pacelli Bezerra Viana
Alessandro Roosevelt Silva Ribeiro
Ricardo da Costa Nunes
João Francisco Adrien Fernandes
Evaristo Lunz Gomes

Suplentes
Ary Célio de Oliveira
Jeferson Adonias Smaniotto
Rogério Nagamine Costanzi
Luciana Maria Rocha Moreira
Juliana Felício dos Santos

Diretoria Executiva

Superintendente
Renato Nobile

Gerência Geral Sescoop
Karla Tadeu Duarte de Oliveira

Gerência de Controladoria
Giulianna Fardini

Equipe Técnica
Bruna F. da Silva do Espírito Santo
Luciana Alves dos Santos Peres
Pedro Henrique de Sousa Malvezzi

Gerência de Comunicação
Daniela Lemke
Ana Troiano Vaz
Cristiano Hosannah de Carvalho

SUMÁRIO

LISTA DE FIGURAS

APRESENTAÇÃO

Vivemos num mundo marcado pela volatilidade. O cenário muda a todo instante e pede a atenção mais cuidadosa dos gestores das empresas. E o Sescoop, como entidade do Sistema S, deve estar atento às incertezas que rodeiam seu ambiente de negócios.

Incertezas representam riscos ao cumprimento de objetivos em todos os níveis da organização e ameaça ao alcance dos resultados desejados. Esse cenário volátil e incerto pede uma reação à altura da gestão.

No intuito de enfrentar de forma mais eficiente esse cenário, o Sescoop aprovou a Política de Gestão de Riscos Corporativos, que institui o processo para gestão de riscos e dá diretrizes para a atuação dos gestores, dirigentes e conselheiros no que diz respeito ao tratamento dos riscos corporativos.

O presente Manual tem o objetivo de apoiar os gestores na implantação da Política de Gestão de Riscos Corporativos em todas as unidades do Sescoop e potencializar o alcance de objetivos por meio da diminuição do efeito das incertezas.

Esta segunda edição, traz ajustes na metodologia adotada, frutos do amadurecimento alcançado no primeiro ano da vigência da Política.

Fazendo isso, o Sescoop se alinha às melhores práticas do mercado e reafirma o compromisso com suas partes interessadas de manter uma gestão pautada na integridade, conformidade e eficiência.

Sucesso a todos!

RENATO NOBILE
Superintendente

INTRODUÇÃO

A governança e a gestão das organizações buscam, de maneira integrada, por meio da definição de estratégias, entregar o máximo de valor possível para suas partes interessadas. Entretanto, o mundo atual é marcado por incertezas e mudanças constantes. Esse cenário faz com que o alcance dos objetivos organizacionais seja ameaçado por eventos diversos e, consequentemente, a entrega de valor para as partes interessadas. Os eventos com potencial de comprometer o alcance de objetivos são denominados "riscos". Logo, riscos são produtos da incerteza presente no ambiente de negócios.

O desafio da governança nas organizações é determinar quanto risco aceitar no processo de geração de valor para as suas partes interessadas, o que significa prestar serviços da melhor maneira possível, equilibrando riscos e benefícios.
Para minimizar o grau de incerteza com relação ao alcance dos seus objetivos, as organizações vêm implantando mecanismos de gerenciamento dos eventos que possam comprometer seus resultados. Esses mecanismos compõem o Processo de Gestão de Riscos Corporativos. Trata-se de uma medida estratégica e fundamental para as organizações e um componente relevante do sistema de governança. Gerenciar riscos de maneira eficaz gera confiança nas partes interessadas e confiança gera bons relacionamentos e sustentabilidade para os negócios. Não se trata de um processo separado dos demais, mas sim parte de todos os processos organizacionais, sendo indissociável da responsabilidade administrativa.

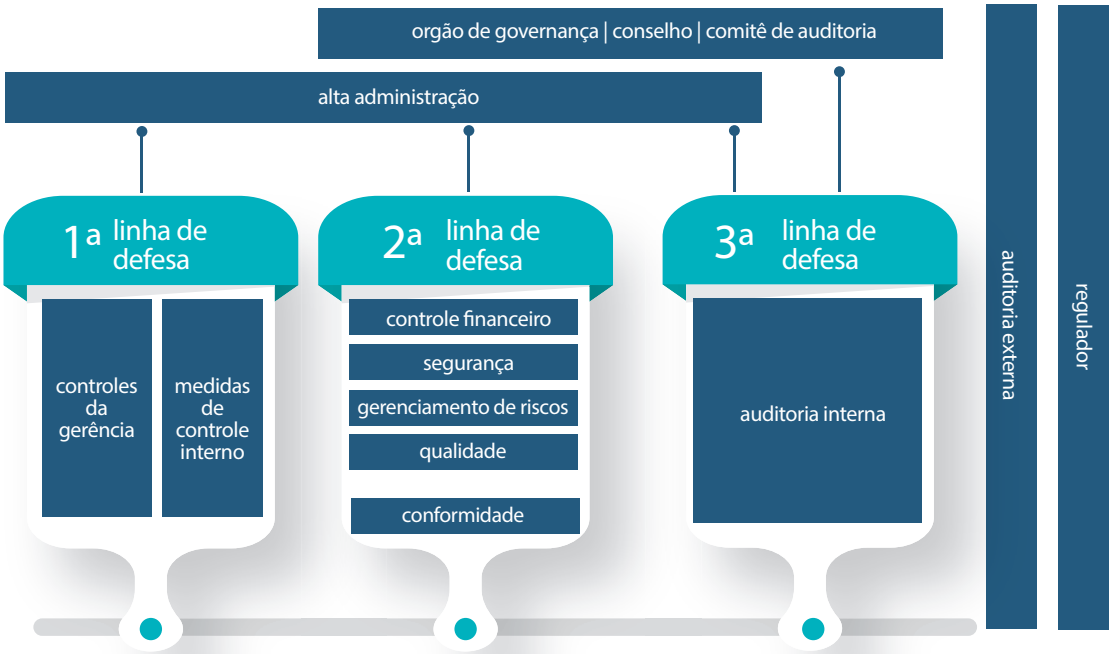
Uma gestão de riscos eficaz melhora as informações para o direcionamento estratégico e para as tomadas de decisões de responsabilidade da governança, contribui para a otimização do desempenho na realização dos objetivos e serviços, aumenta a confiança, previne perdas e auxilia na gestão da conformidade e da integridade.

Para viabilizar a implantação do processo de gestão de riscos, a governança deve aprovar a Política de Gestão de Riscos Corporativos, que define os papéis das instâncias de governança e de gestão da organização no processo de gestão de riscos, além de determinar os objetivos, os conceitos, as etapas, as categorias de riscos que serão gerenciados e como se dará o processo de gerenciamento dos riscos corporativos.

A estrutura da gestão de riscos vem sendo tratada a partir do modelo das "Três Linha de Defesa", difundida pelo Instituto de Auditores Internos em mais de 170 países, que define três grupos de responsáveis envolvidos com o gerenciamento de riscos.

A alta administração e os órgãos de governança têm, coletivamente, a responsabilidade e o dever de prestação de contas sobre o estabelecimento dos objetivos da organização, a definição de estratégias para alcançar esses objetivos e o estabelecimento de estruturas e processos de governança para melhor gerenciar os riscos durante a realização desses objetivos. O modelo de Três Linhas de Defesa é implementado melhor com o apoio ativo e a orientação do órgão de governança e da alta administração da organização. (IIA, 2013)

Figura 1 – Modelo de Três Linhas de Defesa



Fonte: IIA, 2013

O Tribunal de Contas da União entende que as Três Linhas de Defesa são uma segurança para a Governança de que os controles internos implementados para a gestão dos riscos são eficazes, diminuem o nível de incerteza e, logo, sinalizam para uma probabilidade maior de alcance dos objetivos organizacionais. Tendo recepcionado o modelo, caracteriza assim as três linhas de defesa:

1ª linha – Funções que gerenciam e têm propriedade de riscos: a gestão operacional e os procedimentos diários de controles constituem a primeira linha de defesa, porque os controles são desenvolvidos como sistemas e processos sob sua orientação e responsabilidade. É nesse nível que se identificam, avaliam e controlam riscos, guiando o desenvolvimento e a implementação de políticas e procedimentos internos e garantindo que as atividades estejam de acordo com as metas e objetivos.

2ª linha – Funções que supervisionam riscos: a segunda linha de defesa é constituída por funções estabelecidas para garantir que a primeira linha funcione como pretendido no tocante ao gerenciamento de riscos e controles. As funções específicas variam muito entre organizações e setores, mas são, por natureza, funções de gestão. Seu papel é coordenar as atividades de gestão de riscos, monitorar riscos específicos (funções de compliance ou de conformidade), ajudar a desenvolver controles e ou monitorar riscos e controles da primeira linha de defesa.

3ª linha – Funções que fornecem avaliações independentes: a auditoria interna constitui a terceira linha de defesa no gerenciamento de riscos, fornecendo avaliações (asseguração) independentes e objetivas sobre os processos de gerenciamento de riscos, controle e governança aos órgãos de governança e à alta administração, abrangendo uma grande variedade de objetivos (incluindo eficiência e eficácia das operações; salvaguarda de ativos; confiabilidade e a integridade dos processos de reporte, conformidade com leis e regulamentos) e elementos da estrutura de gerenciamento de riscos e controle interno em todos os níveis da estrutura organizacional da entidade.

Figura 2 – Atribuições gerais das Três Linhas de Defesa

1ª LINHA DE DEFESA	2ª LINHA DE DEFESA	3ª LINHA DE DEFESA
Proprietários/ Gestores de Riscos	Controle de Riscos e Conformidade	Avaliação de Riscos
Gerência operacional	Independência limitada Reporta primariamente à gerência	Auditoria interna Maior independência Reporta ao órgão de governança

Fonte: IIA, 2013

A Política de Gestão de Riscos Corporativos do Sescoop definiu que a gestão de riscos será realizada seguindo a lógica das "Três Linhas de Defesa", sendo a "1ª Linha" representada pelos gestores das áreas (Gestores de Riscos), a "2ª Linha" composta pela Controladoria e pelo Comitê de Riscos; e a "3ª Linha" representada pela Auditoria Interna. Os Gestores de Riscos são responsáveis pela gestão dos riscos propriamente, desde a sua identificação, análise, avaliação, classificação e tratamento. A Controladoria é responsável por, em linhas gerais, instrumentalizar, capacitar e apoiar os Gestores de Riscos, e monitorar o nível de exposição a riscos geral da organização. O Comitê de Riscos tem o papel de acompanhar e propor ajustes na política e no processo de gestão de riscos, bem como recomendar o apetite e a tolerância ao risco à Diretoria Executiva. E a Auditoria Interna tem o papel de avaliar periodicamente o processo de gestão de riscos a fim de averiguar a sua eficácia.

Para potencializar a eficácia da gestão de riscos corporativos, é importante contar com uma solução de informática. Porém, o fator mais determinante do sucesso da gestão de riscos é a cultura organizacional orientada para riscos. Uma organização que não contar com um software próprio, mas contar com o engajamento dos gestores terá uma gestão de riscos mais eficiente do que outra organização que tiver o melhor software de gerenciamento de riscos do mundo, mas não tiver a cultura de gestão de riscos incorporada na sua equipe.
É por isso que o Sescoop inicia o processo de implantação da gestão de riscos com a realização de oficinas, sem considerar o software a ser utilizado. Porque entende que o mais importante é ter toda a equipe capacitada para pensar riscos segundo a mesma metodologia, definindo como contexto os seus processos críticos.

O presente manual tem como objetivo subsidiar a capacitação e apoiar os gestores na implantação da gestão de riscos corporativos. Portanto, seu conteúdo é técnico, de caráter mais prático, não fazendo parte do seu escopo a reprodução de algumas das definições institucionais dadas pela Política de Gestão de Riscos Corporativos. É dedicado a detalhar as etapas do Processo de Gestão de Riscos Corporativos, bem como a explicar as categorias dos riscos a serem tratados.

DEFINIÇÕES

A gestão de riscos corporativos é uma matéria bastante técnica - apesar de não ser complexa – e muitos são os termos técnicos utilizados pelos profissionais que atuam nessa área. Para melhor entendimento deste manual, a seguir são apresentadas as definições para os termos técnicos utilizados ao longo do material.

Apetite ao risco: quantidade e tipos de riscos corporativos que o Sescoop está disposto a aceitar.

Cadeia de valor: principais macroprocessos e processos organizacionais realizados pelo Sescoop para atingir seus resultados.

Categorias de riscos corporativos: classificação dos tipos de riscos corporativos definidos pelo Sescoop que podem afetar o alcance de seus objetivos, observadas as características de sua área de atuação.

Causa: fonte de risco que, sozinha ou em combinação, tem o potencial intrínseco de gerar riscos.

Consequência: resultado de um evento que afeta os objetivos pretendidos.

Controle: qualquer medida que mantém ou modifica o risco.

Controles internos da gestão: conjunto de regras, procedimentos, diretrizes, protocolos, rotinas de sistemas informatizados, conferências e trâmites de documentos e informações, entre outros, operacionalizados de forma integrada pela direção, destinados a enfrentar os riscos e fornecer segurança razoável na consecução da missão do Sescoop.

Critério de risco: referências contra os quais o impacto e a probabilidade do risco são avaliados.

Evento: ocorrência gerada com base em fontes internas ou externas que pode causar impacto negativo ou positivo.

Gestão de riscos corporativos: processo contínuo, que consiste no desenvolvimento de um conjunto de ações destinadas a identificar, analisar, avaliar, priorizar, tratar e monitorar riscos corporativos, capazes de afetar os objetivos, programas, projetos ou processos de trabalho do Sescoop nos níveis estratégico, tático e operacional.

Governança: mecanismos de liderança, estratégia e controle postos em prática para avaliar, direcionar e monitorar a atuação da gestão, com vistas à condução de políticas e à prestação de serviços de interesse das partes interessadas do Sescoop.

Impacto: efeito resultante da ocorrência do evento.

Incerteza: incapacidade de saber com antecedência a real probabilidade ou impacto de eventos futuros.

Nível de risco: magnitude do risco, expressa pela combinação de sua probabilidade e impactos.

Nível estratégico: nível de gestão responsável pela formulação dos objetivos estratégicos e as decisões sobre as prioridades para a alocação dos recursos institucionais.

Nível tático: nível de gestão responsável pela implementação dos objetivos e gerenciamento das prioridades definidas no nível estratégico.

Nível operacional: nível de gestão que trata da execução dos projetos, programas e atividades relativas aos processos finalísticos e de suporte.

Oportunidade: possibilidade de que um evento afete positivamente o alcance de objetivos.

Probabilidade: chance de ocorrência do evento.

Problema: é o risco consumado.

Processo organizacional: conjunto de atividades inter-relacionadas que envolve pessoas, equipamentos, procedimentos e informações e, quando executadas, transformam entradas (insumos) em saídas (produtos ou serviços), que atendem a uma necessidade de um cliente interno ou externo e que agregam valor e produzem resultados para instituição.

Resposta ao risco: qualquer ação de tratamento adotada para lidar com risco.

Risco: efeito da incerteza, evento capaz de afetar negativamente os objetivos, processos de trabalho, programas e projetos nos níveis estratégico, tático ou operacional.

Risco inerente: risco a que uma organização está exposta sem considerar quaisquer medidas de controle que possam reduzir a probabilidade de sua ocorrência ou seu impacto.

Risco residual: risco a que uma organização está exposta após a implementação de medidas de controle para o tratamento do risco.

Tratamento do risco: processo de seleção e implementação de ações, controles ou respostas para modificar o risco.

Tolerância ao risco: nível de variação aceitável quanto à realização dos objetivos.

O PROCESSO DE GESTÃO DE RISCOS

O **Processo de Gestão de Riscos Corporativos** consiste na aplicação sistemática de metodologias, procedimentos e práticas de gestão, incorporadas na cultura organizacional e adaptadas aos processos de trabalho do Sescoop.

O Processo de Gestão de Riscos Corporativos será composto das seguintes etapas:

1. Entendimento do contexto
2. Identificação dos riscos
3. Análise e avaliação dos riscos
4. Tratamento dos riscos
5. Monitoramento, revisão e comunicação

Figura 3 – Fluxo do Processo de Gestão de Riscos Corporativos

Fonte: Guia Simplificado de Gestão de Riscos – Sescoop Nacional, 2019

A seguir passaremos a explicar cada uma dessas etapas:

1. Entendimento do contexto

A etapa de entendimento do contexto consiste em entender o ambiente interno e externo no qual o objeto a ser avaliado pela gestão de riscos se encontra inserido. O objeto pode ser um processo, um projeto, uma área ou a organização como um todo.

A reflexão aprofundada sobre o contexto é fundamental para a identificação dos eventos de riscos. Sem uma visão ampliada do contexto do processo, a visão de riscos ficará prejudicada.

O referencial elaborado pelo COSO diz que os eventos de riscos estão relacionados a fatores externos e internos da organização. Como **fatores externos** ligados a eventos de riscos são listados os seguintes - considerando empresas em geral:

a. **Econômicos:** disponibilidade de capital, emissões de crédito, inadimplência, concentração, liquidez, mercados financeiros, desemprego, concorrência, fusões/ aquisições;

b. **Meio ambiente:** emissões e dejetos, energia, desastres naturais, desenvolvimento sustentável;

c. **Políticos:** mudanças de governo, legislação, política pública, regulamentos;

d. **Sociais:** características demográficas, comportamento do cliente, cidadania corporativa, privacidade, terrorismo;

e. **Tecnológicos:** interrupções, comércio eletrônico, dados externos, tecnologias emergentes.

Como **fatores internos** relacionados a eventos de riscos, são apresentados:

a. **Infraestrutura:** disponibilidade de bens, capacidade dos bens, acesso a capital, complexidade;
b. **Pessoal:** capacidade dos empregados, atividade fraudulenta, saúde e segurança;
c. **Processo:** capacidade, design, execução, dependências/fornecedores;
d. **Tecnologia:** integridade de dados, disponibilidade de dados e sistemas, seleção de sistemas, desenvolvimento, alocação e manutenção.

O Sescoop definiu, como parte da metodologia de implantação da gestão de riscos, o início pelos processos críticos. Logo, o objeto será o processo em questão e o contexto envolverá: a maturidade do processo, a maturidade dos controles existentes, as áreas e pessoas envolvidas com o processo, as leis e normas relacionadas ao processo, as tecnologias disponíveis ou envolvidas com a execução do processo, a importância do processo para a organização, quem são os fornecedores e os clientes do processo, etc.

Para definir a criticidade do processo, usa-se fazer uma avaliação do impacto na continuidade do negócio no caso de paralisação do processo. E "continuidade", segundo a norma ISO 22.301, é "a capacidade da organização de continuar a entregar produtos e serviços, em um nível aceitável, previamente definido, após incidentes de interrupção".
Existe uma técnica chamada de BIA – Business Impact Analysis, que leva à classificação da criticidade do impacto da paralisação dos processos em relação ao tempo, e à consequente identificação dos processos mais críticos sob essa perspectiva de continuidade das operações. Na metodologia BIA, são estabelecidos critérios de análise dos processos e graus de impacto para esses critérios para determinados horizontes de tempo.

Não é objetivo deste manual abordar o critério para a definição dos processos mais críticos para efeito de início da gestão de riscos. O próprio gestor pode fazer essa identificação com base na sua avaliação, ou seguir uma orientação institucional ou lançar mão da técnica mencionada. Mas é importante que todos os processos e objetivos relevantes da instituição sejam incluídos na gestão de riscos assim que possível.

2. Identificação dos riscos

Depois de entender bem o contexto do objeto, pela análise de fatores externos e internos, passa-se para a etapa de identificação dos riscos, que consiste na identificação e catalogação dos eventos de riscos relacionados aos objetivos definidos, bem como na definição da categoria dos riscos.

Pensar em eventos de risco consiste em responder à pergunta: **o que pode acontecer que pode impactar negativamente o alcance do objetivo definido?**

Assim, se o objeto for um processo, a pergunta será: o que pode acontecer para atrapalhar o alcance do objetivo do processo? Usando como exemplo o processo de "Contratação de instrutores", algumas respostas a essa pergunta seriam:

a) Inexistência de instrutores na área do conhecimento desejada
b) Preço praticado pela Unidade não é atrativo para os profissionais de referência no tema
c) Indisponibilidade de agenda dos instrutores para a data desejada
d) Morosidade no processo de contratação.

Estas respostas são riscos que podem comprometer o alcance do objetivo do processo de Contratação de instrutores. Além de identifica-los, é importante definir a qual **categoria de riscos** eles pertencem.

Não existe uma categorização padrão; cada entidade define as categorias que deseja trabalhar. E o Sescoop definiu quatro categorias de riscos para o seu processo de gestão de riscos corporativos:

Risco Estratégico: eventos que possam impactar as decisões estratégicas e que podem gerar perda substancial do valor econômico/financeiro ou da imagem da organização.

Risco Operacional: está associado à possibilidade de ocorrência de perdas (ativos, clientes, receitas) resultantes de falhas, deficiências ou inadequação de processos internos, pessoas e sistemas, assim como de eventos externos, como catástrofes naturais, que paralisem as operações da organização.

Risco de Conformidade: está associado ao não cumprimento de princípios constitucionais, legislações específicas ou regulamentações externas aplicáveis ao negócio, bem como de políticas, normas e procedimentos internos. Inclui, também, o risco associado à confiabilidade das informações financeiras transmitidas para usuários internos e externos.

Risco de Integridade: eventos relacionados a corrupção, fraudes, irregularidades e/ou desvios éticos e de conduta que podem comprometer os valores da organização e a realização dos objetivos.

É comum que um risco se enquadre em mais de uma categoria. O que o Gestor de Riscos deve fazer nestes casos é definir a categoria com a qual o risco tem maior afinidade. Por exemplo, o risco de uma pessoa favorecer um fornecedor no processo de contratação pode ser enquadrado como Risco de Conformidade, se existir uma norma que trate do assunto; mas também é um Risco de Integridade, pois trata-se de desvio de conduta. Neste caso, o específico se sobrepõe ao geral: como existe uma categoria própria para os eventos relacionados a desvios de conduta, deve-se utilizar essa classificação. Logo, usaríamos a classificação de Risco de Integridade para esse evento.

3. Análise e avaliação dos riscos

Identificados os eventos, é necessário analisar todos os riscos e fazer sua avaliação sob a perspectiva de probabilidade e impacto, para se ter uma visão da criticidade e da necessidade de tratamento.

Há várias metodologias para se definir probabilidade e impacto. O Sescoop fez a opção por um método mais simples para iniciar a gestão de riscos, em que são considerados aspectos apenas qualitativos.

Assim, ao avaliar um risco sob a ótica da probabilidade, deve-se definir se a chance de ocorrência do evento é muito baixa, baixa, média, alta ou muito alta. E ao avaliar um risco sob a ótica do impacto, deve-se definir se o efeito negativo resultante da ocorrência do evento é muito baixo, baixo, médio, alto ou muito alto.

A seguir são apresentados referenciais sugeridos pela Auditoria Interna para a definição da probabilidade e impacto.

Figura 4 – Classificação da Probabilidade

PESO	PROBABILIDADE	DESCRIÇÃO DA PROBABILIDADE
5	Muito Alta	Praticamente certa. De forma precisa, o evento ocorrerá, as circunstâncias indicam claramente essa possibilidade.
4	Alta	Provável. De forma até esperada, o evento poderá ocorrer, pois as circunstâncias indicam claramente essa possibilidade.
3	Média	Possível. De alguma forma, o evento poderá ocorrer, pois as circunstâncias indicam moderadamente essa possibilidade.
2	Baixa	Rara. De forma inesperada ou casual, o evento poderá ocorrer, pois as circunstâncias pouco indicam essa possibilidade.
1	Muito Baixa	Improvável. Em situações excepcionais, o evento poderá até ocorrer, mas nada nas circunstâncias indica essa possibilidade.

Fonte: Guia Simplificado de Gestão de Riscos – Sescoop Nacional, 2019

Figura 5 – Classificação do Impacto

PESO	IMPACTO	DESCRIÇÃO DO IMPACTO
5	Muito Alto	Compromete totalmente ou quase totalmente o alcance do objetivo.
4	Alto	Compromete a maior parte do alcance do objetivo.
3	Médio	Compromete razoavelmente o alcance do objetivo.
2	Baixo	Compromete em alguma medida o alcance do objetivo, mas não impede o alcance da maior parte dos objetivos.
1	Muito Baixo	Compromete minimamente o alcance do objetivo, não alterando o alcance final do objetivo.

Fonte: Guia Simplificado de Gestão de Riscos – Sescoop Nacional, 2019

A multiplicação entre os valores de probabilidade e impacto define a escala do risco inerente e, por consequência o seu respectivo nível de criticidade. O nível de criticidade do risco inerente não considera quaisquer controles que podem reduzir a probabilidade da sua ocorrência ou que minimizem o seu impacto.

Com o resultado do cálculo, o risco pode ser classificado em níveis de criticidade, conforme a seguir:

Figura 6 – Classificação do Nível de Risco

ESCALA DE VALOR DOS NÍVEIS DE RISCO	NÍVEL DO RISCO	
20,1 a 25	Crítico	Nível dos riscos com potencial de comprometer o alcance dos objetivos de forma massiva.
15,1 a 20	Muito Alto	Nível dos riscos com potencial de comprometer substancialmente o alcance dos objetivos.
10,1 a 15	Alto	Nível dos riscos com potencial de comprometer significativamente o alcance dos objetivos.
5,1 a 10	Médio	Nível dos riscos com potencial de comprometer razoavelmente o alcance dos objetivos.
0 a 5	Baixo	Nível dos riscos com potencial de comprometer minimamente o alcance dos objetivos.

Com o amadurecimento da gestão de riscos, será possível definir critérios quantitativos para avaliação da probabilidade e impacto. Por exemplo, em função de dados históricos ou pela experiência do gestor será possível estimar, por exemplo, que a probabilidade do evento "Inexistência de instrutores na área do conhecimento desejada" ocorrer é de 20% ao invés de simplesmente "baixa"; ou que o impacto do "Preço praticado pela Unidade não é atrativo para os profissionais de referência no tema" é de R$20.000,00 e não simplesmente "médio".

Depois de avaliar os riscos, é necessário fazer a comparação do nível de risco com o limite de exposição a riscos, para identificar se o risco é ou não aceitável, além da identificação das causas e consequências dos eventos de risco.

A definição de "aceitável" deve ser dada pela alta administração da organização. E o apetite a risco da administração pode variar: há dirigentes que têm mais disposição para aceitar certos tipos de riscos e outros menos.

Entretanto, via de regra, **não se deve considerar aceitáveis riscos nos níveis crítico e muito alto** – zona vermelho escuro e vermelho claro da Matriz de Risco. Riscos críticos e muito alto são os que têm alta probabilidade de acontecer e têm potencial de causar impacto (efeito negativo) muito alto, conforme apresentado a seguir.

Figura 7 – Matriz de Riscos Inerentes

RISCO INERENTE		PROBABILIDADE				
		Muito Baixa 1	**Baixa 2**	**Média 3**	**Alta 4**	**Muito Alta 5**
IMPACTO	**Muito Alto 5**	Baixo 5	Médio 10	Alto 15	Muito Alto 20	Crítico 25
	Alto 4	Baixo 4	Médio 8	Alto 12	Muito Alto 16	Muito Alto 20
	Médio 3	Baixo 3	Médio 6	Médio 9	Alto 12	Alto 15
	Baixo 2	Baixo 2	Baixo 4	Médio 6	Médio 8	Médio 10
	Muito Baixo 1	Baixo 1	Baixo 2	Baixo 3	Baixo 4	Baixo 5

Essa avaliação de riscos, sem considerar a existência de controles, produz o que se chama de **"riscos inerentes"** – pois são os riscos naturalmente vinculados ao objeto em análise – seja processo, projeto ou organização.

Entretanto, é possível aprofundar a análise dos riscos, considerando os eventuais controles existentes. Por exemplo, no processo de Pagamento de Compras, pode existir a separação das atribuições de: solicitar compra, autorizar compra, realizar compra, receber compra, autorizar pagamento e realizar pagamento, com duas assinaturas. Dessa forma, o risco inerente de "Desvio de recursos por superfaturamento", que poderia ser crítico, passa a ser, talvez, um risco médio, dada a eficiência dos controles existentes. A esse risco que permanece existindo após a consideração dos controles existentes dá-se o nome de **"risco residual"**.

A seguir é apresentado critério sugerido pela Auditoria Interna para a avaliação da eficácia dos controles.

Figura 8 – Classificação dos Controles Internos

EFICÁCIA DO CONTROLE	DESCRIÇÃO DO CONTROLE	FATOR DE CONTROLE
Inexistente	Controles inexistentes, mal desenhados ou mal implementados, isto é, não funcionais.	1
Fraco	Controles que são aplicados caso a caso, a responsabilidade é individual, havendo elevado grau de confiança no conhecimento das pessoas.	0,8
Mediano	Controles implementados mitigam alguns aspectos do risco, mas não contemplam todos os aspectos relevantes do risco devido a deficiências no desenho ou nas ferramentas utilizadas.	0,6
Satisfatório	Controles implementados e sustentados por ferramentas adequadas e, embora passíveis de aperfeiçoamento, mitigam o risco satisfatóriamente.	0,4
Forte	Controles implementados podem ser considerados a "melhor prática", mitigando todos os aspectos relevantes do risco.	0,2

Após a consideração dos controles existentes, é interessante calcular a Matriz de Riscos Residuais, que representa o nível de risco real ao que a organização está exposta.

Figura 9 – Matriz de Riscos Residuais

RISCO RESIDUAL		Eficácia do Controle				
		Forte	Satisfatório	Mediano	Fraco	Inexistente
Nível de Risco Inerente	Crítico	Baixo	Médio	Alto	Muito Alto	Crítico
	Muito Alto	Baixo	Médio	Alto	Muito Alto	Muito Alto
	Alto	Baixo	Médio	Médio	Alto	Alto
	Médio	Baixo	Baixo	Médio	Médio	Médio
	Baixo	Baixo	Baixo	Baixo	Baixo	Baixo

Cabe ressaltar que a inexistência de controles internos ou a existência de controles fracos manterá o nível de exposição a riscos em nível equivalente aos riscos inerentes (podendo ser "Crítico"), demandando atenção especial dos Gestores de Riscos no tratamento dos riscos.

Para todos os riscos que permanecerem com o status de "Crítico", "Muito Alto" ou "Alto", é recomendável que se investigue suas causas e consequências , visto que as formas existentes de tratar os riscos são diminuindo a probabilidade de que suas causas ocorram ou diminuindo o impacto das consequências caso o evento ocorra.

Figura 10 – Causa, Evento e Consequência do Risco

Fonte: Guia Simplificado de Gestão de Riscos – Sescoop Nacional, 2019

As causas de riscos podem estar vinculadas a fatores internos da organização e que, por conseguinte, estão sob sua gestão, como pessoas, processos, sistemas, infraestrutura, tecnologia; ou a fatores externos à organização, que, neste caso, poderão não ser gerenciáveis, como, por exemplo, a estabilidade do abastecimento de energia.

1- Para início de implantação da gestão de riscos o Sescoop fez a opção de identificar causas e consequências na etapa de tratamento dos riscos, ou seja, após a priorização pela classificação em função da criticidade. Entretanto, muitas metodologias identificam as causas na fase de avaliação dos riscos, seguindo a ideia de que se entende melhor a criticidade dos riscos após conhecer suas causas. É possível que em fase mais avançada da gestão de riscos, o Sescoop adote essa prática. Por ora, vamos utilizar a identificação das causas e consequências para melhor tratamento dos riscos, ou seja, definição de controles internos.

As causas poderão ser categorizadas conforme a tabela abaixo:

Figura 11 – Categorias de Causa

CATEGORIA CAUSA	DESCRIÇÃO
Falha Humana	Inclui as causas relacionadas a falhas humanas não intencionais, características de erro por imperícia, imprudência ou negligência por parte de quem realiza as atividades da organização.
Falha de Sistema	Inclui as causas relacionadas a falhas de sistemas informatizados – software, aplicativos, sites, internet, redes, etc., de uso da entidade.
Desvio de Conduta	Inclui as causas relacionadas à exposição a riscos de forma intencional e dolosa, características de conluios, fraudes, corrupção, etc.
Falha de Processo	Inclui as causas relacionadas a falhas nos processos internos, seja nos procedimentos, seja nos controles existentes.
Falha Operacional	Inclui as causas relacionadas a falhas de equipamentos em geral e hardware, não provocadas por falha humana ou por falha de sistemas informatizados (software).
Ação de Terceiros	Inclui as causas relacionadas à influência de terceiros nas atividades da organização, podendo ser fornecedores de bens ou serviços, agentes públicos, parceiros, representantes, etc., que, independentemente de vontade ou intenção, geram riscos para a organização.
Eventos da Natureza	Inclui as causas relacionadas aos eventos da natureza, não controláveis ou previsíveis, e que podem gerar riscos aos objetivos da organização.

Assim, se, por exemplo, for identificado o risco de "Contratação não ser realizada no tempo necessário", deve-se identificar as causas para que seja possível seu tratamento. Poder-se-ia pensar nas seguintes causas:

1. Inexistência de planejamento da ação
2. Antecedência insuficiente para a realização da contratação
3. Prospecção de mercado falha
4. Nota Técnica mal elaborada

Dando seguimento à análise desse risco, seria possível pensar nas seguintes consequências, caso ele se concretize:

1. Necessidade de adiamento do projeto
2. Insatisfação das pessoas
3. Multas contratuais em eventuais outras contratações
4. Dano à imagem institucional

As consequências poderão ser agrupadas de acordo com as categorias abaixo:

Figura 12 – Categorias de Consequência

CATEGORIA CONSEQUÊNCIA	DESCRIÇÃO
Jurídica	Inclui as consequências relacionadas a processos judiciais contra o Sescoop, incluindo os relacionados a fornecedores e terceirizados/prestadores de serviços, assim com responsabilização pessoal de dirigentes.
Econômico-Financeira	Inclui as consequências que trazem prejuízo financeiro e danos ao patrimônio do Sescoop.
Integridade e Imagem	Inclui as consequências que causam danos à imagem do Sescoop e afetam a integridade da instituição, em função de desvios de conduta.
Resultado	Inclui as consequências que comprometem a entrega dos resultados, englobando o alcance de objetivos e metas, cumprimento de prazos, qualidade das entregas, atendimento das necessidades e expectativas das partes interessadas, etc.
Conformidade	Inclui as consequências relacionadas aos normativos internos, leis, normas técnicas, acórdãos e demais recomendações dos órgãos de controle.
Relação de Trabalho	Inclui as consequências relacionadas à relação de trabalho entre Sescoop e seus colaboradores e todo o ambiente envolvido nessa relação, como aspectos culturais e clima organizacional.
Política	Inclui as consequências relacionadas à relação com as demais partes interessadas, excetuando-se os colaboradores, e destacando-se as Unidades integrantes do Sistema OCB e as cooperativas.

Existe uma técnica chamada de **Análise Bow Tie**, que significa "gravata borboleta", em função da figura que é formada; essa técnica é muito interessante para a análise de causas e consequências de riscos, pois as dispõe visualmente de forma bastante clara, auxiliando nas escolhas de respostas aos riscos.

Os números de 1 a 4 da figura 13 representam os **"controles preventivos"**, que se destinam a diminuir a probabilidade de ocorrência das causas do risco; os números de 5 a 8 da figura representam os **"controles atenuantes"**, que se destinam a diminuir o impacto das consequências do risco.

Figura 13 – Análise de Bow Tie

Como controles preventivos das causas do risco do exemplo dado, poderíamos listar:

1. Elaboração de planejamento das contratações, considerando o tempo necessário para o cumprimento de todas as etapas envolvidas com o processo licitatório.

2. Fazer o cálculo reverso do prazo necessário para a contratação, considerando ao menos 30 dias de margem de segurança.

3. Fazer consulta prévia ao mercado para todos os produtos/serviços para os quais não houver características e preços conhecidos.

4. Elaborar Nota Técnica com antecedência suficiente para ao menos duas revisões pela área técnica.

Como controles atenuantes das consequências do risco do exemplo dado, poderíamos pensar:

5. Elaborar plano de contingência para o caso de ser necessário o adiamento da data do evento.

6. Elaborar plano de comunicação para o caso de ser necessário comunicar o adiamento da ação.

7. Prever cláusula contratual que elimine a aplicação de multas quando houver justificativa de força maior.

8. Incluir, no plano de comunicação, ampla divulgação e contatos pessoais com pessoas chave, caso seja necessário adiar a ação.

4. Tratamento dos riscos

Os controles preventivos e atenuantes da Análise Bow Tie são, na verdade, medidas de mitigação, que é uma das formas de tratar riscos. Tratamento de riscos, portanto, consiste na elaboração do planejamento das ações de resposta aos riscos com o objetivo de modificar o seu nível, por meio de ações que mitiguem, transfiram ou evitem suas consequências.

Todo o processo de gestão de riscos existe, na verdade, para produzir eficácia no tratamento de riscos. Não adianta identificar e avaliar riscos e não tratar. Logo, essa é a etapa mais importante da gestão de riscos e deve ser realizada com critério, dando respostas adequadas aos diversos riscos.
As respostas aos riscos são basicamente quatro:

a. **Mitigar**: reduzir a probabilidade e ou o impacto da ameaça.

b. **Evitar**: eliminar ou remover totalmente a ameaça, pela descontinuação das atividades que geram os riscos.

c. **Transferir**: transferir, total ou parcialmente, o impacto negativo a terceiros (contratando seguro, por exemplo).

d. **Aceitar**: não fazer nada, pela disposição de lidar com os impactos negativos.

A resposta ao risco está intimamente relacionada ao apetite à risco (quanto de risco está disposta a assumir) e à tolerância ao risco (nível aceito de variação da realização de objetivos) da administração. Quanto

menores forem o apetite e a tolerância ao risco, maior será a tendência de adotar respostas que eliminem ou mitiguem os riscos. Quanto maiores forem o apetite e a tolerância ao risco, maior será a tendência a aceitar riscos, não se adotando nenhuma medida para evitar, mitigar ou transferir os riscos.

A resposta ao risco deve guardar coerência com a criticidade do risco e o apetite a risco da organização. Mas, de maneira geral, "Riscos Críticos e Muito Alto" devem ser evitados ou mitigados imediatamente à sua identificação.

A tabela a seguir é um referencial a ser seguido.

Figura 14 – Diretrizes para Priorização e Tratamento dos Riscos

NÍVEL DO RISCO	AÇÃO DE TRATAMENTO	DIRETRIZES PARA PRIORIAZAÇÃO E TRATAMENTO DE RISCOS
Crítico	Evitar ou Mitigar	Nível de risco **inaceitável**. Requer tratamento imediato do Gestor de Risco, com respaldo da Diretoria Executiva e, se Risco Estratégico, do Conselho.
Muito Alto	Evitar ou Mitigar	Nível de risco **muito acima do apetite a risco**. Requer tratamento em curto prazo pelo Gestor de Riscos, devendo ser levado ao conhecimento da Diretoria Executiva.
Alto	Mitigar	Nível de risco **acima do apetite a risco**. Requer tratamento do Gestor de Riscos em período aceitável pela Diretoria Executiva.
Médio	Aceitar, Mitigar ou Transferir	Nível de risco **no limite do apetite a risco**. Requer atenção do Gestor de Riscos para manter o risco neste nível ou reduzi-lo.
Baixo	Aceitar	Nível de risco **dentro do apetite a risco**. Não é necessária nenhuma medida de tratamento.

Fonte: Guia Simplificado de Gestão de Riscos – Sescoop Nacional, 2020

No processo de gestão de riscos, seja qual for a resposta escolhida, deve ser feito o registro formal da decisão do Gestor de Riscos e, quando for o caso, do Comitê de Riscos e da Diretoria Executiva, para manter a responsabilidade pelas consequências da resposta na instância adequada.

Se não houver um software específico, pode ser elaborado um formulário intitulado "Plano de Tratamento de Risco", onde conste: a identificação do objeto analisado, o objetivo do objeto analisado, a identificação dos riscos, a categoria dos riscos, a criticidade dos riscos, as respostas aos riscos escolhidas, as ações de controle definidas, os responsáveis pelas ações de controle, o prazo de implementação das ações de controle.

O controle interno é definido da seguinte forma pelo COSO:

> Controle interno é um processo conduzido pela estrutura de governança, administração e outros profissionais da entidade, e desenvolvido para proporcionar segurança razoável com respeito à realização dos objetivos relacionados a operações, divulgação e conformidade.

São exemplos de ações de controle:

a. **Revisões da alta direção:** a alta direção compara o desempenho atual em relação ao orçado, às previsões, aos períodos anteriores e aos de concorrentes; as principais iniciativas são acompanhadas, como campanhas de marketing, processos de melhoria de produção e programas de contenção ou de redução de custo, para medir até que ponto as metas estão sendo alcançadas; a implementação de planos é monitorada no caso de desenvolvimento de novos produtos ou novos financiamentos.

b. **Administração funcional direta ou de atividade:** gerentes, no exercício de suas funções ou atividades examinam relatórios de desempenho, verificando resumos e identificando tendências e associando os resultados a estatísticas econômicas e metas; são realizadas reconciliações dos fluxos de caixa diários, com as posições líquidas relatadas centralmente para transferências e investimentos.

c. **Processamento da informação:** uma variedade de controles é realizada para verificar a precisão, a integridade e a autorização das transações; os dados inseridos ficam sujeitos a verificações de edição on-line ou à combinação com arquivos aprovados de controle; o desenvolvimento de novos sistemas e as mudanças nos já existentes são controlados da mesma forma que o acesso a dados, arquivos e programas.

d. **Controles físicos:** os equipamentos, estoques, títulos, dinheiro e outros bens são protegidos fisicamente, contados periodicamente e comparados com os valores apresentados nos registros de controle.

e. **Indicadores de desempenho:** relacionar diferentes conjuntos de dados, sejam eles operacionais sejam financeiros, em conjunto com a realização de análises dos relacionamentos e das medidas de investigação e correção, funciona como uma atividade de controle; os indicadores de desempenho incluem, por exemplo, índices de rotação de pessoal por unidade; ao investigar resultados inesperados ou tendências incomuns, a administração poderá identificar circunstâncias nas quais a falta de capacidade para concluir processos fundamentais pode significar menor probabilidade dos objetivos serem alcançados; a forma como a administração utiliza essas informações determinará se a análise dos indicadores de desempenho por si só atenderá às finalidades operacionais, bem como às finalidades de controle da comunicação.

f. **Segregação de funções:** as obrigações são atribuídas ou divididas entre pessoas diferentes com a finalidade de reduzir o risco de erro ou de fraude; por exemplo, as responsabilidades de autorização de transações, do registro e da entrega do bem em questão são divididas.

Os próprios normativos internos e os mecanismos instituídos para verificar seu cumprimento, integram a estrutura de controles internos da organização.

Dependendo da complexidade e da criticidade, pode ser necessária uma combinação de controles internos como resposta ao risco. Entretanto, deve se ter em mente que o custo dos controles não deve exceder o impacto econômico-social do risco, caso ele se concretize.

5. Monitoramento, revisão e comunicação

O monitoramento dedica-se a verificar se os controles internos estabelecidos formalmente para a mitigação dos riscos estão sendo eficazes, ou seja, estão conseguindo manter a organização em nível aceitável de exposição a riscos.

Para além da rotina dos Gestores de Riscos, o monitoramento no âmbito de toda a organização deve ser feito pela "Segunda Linha de Defesa", que, no Sescoop, é composta pela Controladoria e pelo Comitê de Riscos. E o objetivo é garantir que a exposição global a riscos da organização se mantenha dentro do apetite ao risco definido pelo nível de governança.

A revisão periódica, por sua vez, busca aprimorar de forma efetiva o processo da gestão de riscos. Esta também é uma atividade da Segunda Linha, com o objetivo de garantir que o processo de gestão de riscos está dando a melhor visão possível da exposição da organização a riscos ou, se não estiver, promover as melhorias necessárias para que isso aconteça.

A atividade de comunicação está presente em todo o ciclo da gestão de risco com o objetivo de fornecer e receber as informações relativas às etapas do processo de avaliação para todos aqueles que possam influenciar ou ser influenciados pelos riscos sob análise. Convém que todas as etapas tenham seus resultados documentados e comunicados às partes interessadas na avaliação. O Comitê de Riscos tem papel importante nesse processo, por meio da emissão de relatório periódico sobre a gestão de riscos da organização. E a Diretoria Executiva, por sua vez, é o elo de comunicação com o Conselho, especialmente quando riscos críticos e muito alto são identificados e pedem medidas que extrapolam a governabilidade das áreas técnicas.

AVALIAÇÃO INDEPENDENTE DO PROCESSO DE GESTÃO DE RISCOS

Os procedimentos de monitoramento contínuo geralmente fornecem importante feedback sobre a eficácia de outros componentes do gerenciamento de riscos corporativos. Entretanto, é importante se fazer uma avaliação voltada à eficácia do gerenciamento de riscos corporativos e dos próprios procedimentos de monitoramento contínuo.

As avaliações do gerenciamento de riscos corporativos podem variar em termos de escopo e frequência, dependendo da significância dos riscos e da importância das respostas a risco e dos respectivos controles para a administração dos riscos.

Frequentemente, as avaliações têm a forma de autoavaliações nas quais as pessoas responsáveis por uma determinada unidade ou função determinam a eficácia do gerenciamento de riscos corporativos em relação às suas atividades.

Os auditores internos geralmente avaliam controles como parte de seus deveres normais. Entretanto, a Política de Gestão de Riscos Corporativos do Sescoop definiu, no art. 19, que:

O Processo de Gestão de Riscos Corporativos da Unidade Nacional do Sescoop será avaliado anualmente, a partir do segundo ano de sua implantação, pela Auditoria Interna, visando verificar sua adequação, suficiência e eficácia para o controle dos riscos corporativos.

A alta administração também poderá utilizar informações dos auditores externos ao considerar a eficácia do gerenciamento de riscos corporativos. Pode-se utilizar uma combinação de esforços na realização de procedimentos de avaliação que a administração julgue necessários.

CONCLUSÃO

A gestão de riscos visa diminuir o efeito das incertezas sobre os objetivos institucionais. Não é um processo isolado, mas incorpora-se à rotina de gestão da organização, com o intuito de orientar a implantação de controles internos eficazes, que garantam a implantação das respostas aos riscos, de forma que diminuam a probabilidade de ocorrência ou reduzam o seu impacto.

É fundamental que toda a organização esteja comprometida com a gestão dos riscos. Desde a alta administração, por meio da definição de políticas e diretrizes, até os colaboradores de todos os níveis e funções.

Quando a cultura de gestão de riscos não está incorporada na organização, impera a cultura das justificativas, dos porquês os objetivos não foram alcançados. E, via de regra, as justificativas se referem a eventos de risco que não foram tratados previamente.

É possível fazer gestão de riscos sem o uso de software, usando planilhas eletrônicas. Para a fase inicial, é até recomendável que seja assim, para construir aprendizado e amadurecer a metodologia. Entretanto, para a complexidade de uma organização como o Sescoop, é necessária a informatização do processo de gestão de riscos, de forma que sejam possíveis consolidações em tempo real, a atribuição de perfis adequados aos diversos envolvidos e a auditoria do processo.

Este manual tem o objetivo de auxiliar todas as Unidades do Sescoop na implantação do Processo de Gestão de Riscos Corporativos definido em sua Política de Gestão de Riscos Corporativos. Mas nada será mais eficaz do que o efetivo compromisso das pessoas com a implantação da gestão de riscos visando aumentar a eficácia no alcance dos objetivos organizacionais.

REFERÊNCIAS

ABNT – Associação Brasileira de Normas Técnicas. **NBR ISO 31000 – Gestão de Riscos – Princípios e Diretrizes**. Acessado em 21/05/2019. https://gestravp.files.wordpress.com/2013/06/iso31000-gestc3a3o--de-riscos.pdf.

BRASIL. Tribunal de Contas da União. **Manual de Gestão de Riscos do TCU**. Acessado em 21/05/2019. https://portal.tcu.gov.br/main.jsp?lumPageId=8A8182A24ED12B19014ED646CE5E1FC0&previewItemId=8A81881F64480C8C016466C18121556C&lumItemId=FF8080816364D79801641D8093CE4F64

BRASIL. Tribunal de Contas da União. **Gestão de Riscos – Avaliação da Maturidade**. Brasília: TCU, 2018.

COSO – Committee Sponsoring Organizations of the Treadway Commission. **Gerenciamento de Riscos Corporativos – Estrutura Integrada**. Acessado em 21/05/2019. https://www.coso.org/Documents/COSO-ERM-Executive-Summary-Portuguese.pdf.

IIA – The Institute of Internal Auditors. **Declaração de Posicionamento do IIA: As Três Linhas de Defesa no Gerenciamento Eficaz de Riscos e Controles**. Acessado em 21/05/2019. https://iiabrasil.org.br/korbilload/upl/ippf/downloads/as-trs-linhas-d-ippf-00000001-21052018101223.pdf.

SESCOOP – Serviço Nacional de Aprendizagem do Cooperativismo. **Guia Simplificado de Gestão de Riscos Corporativos**. Brasília: 2019.

SESCOOP – Serviço Nacional de Aprendizagem do Cooperativismo. **Política de Gestão de Riscos Corporativos. Brasília: 2019**.

SESCOOP
Serviço Nacional de Aprendizagem do Cooperativismo

somos coop

Setor de Autarquias Sul - SAUS - Quadra 4 - Bloco "I"
CEP: 70070-936 | Brasília-DF
Tel.: +55(61) 3217-2119

www.somoscooperativismo.coop.br