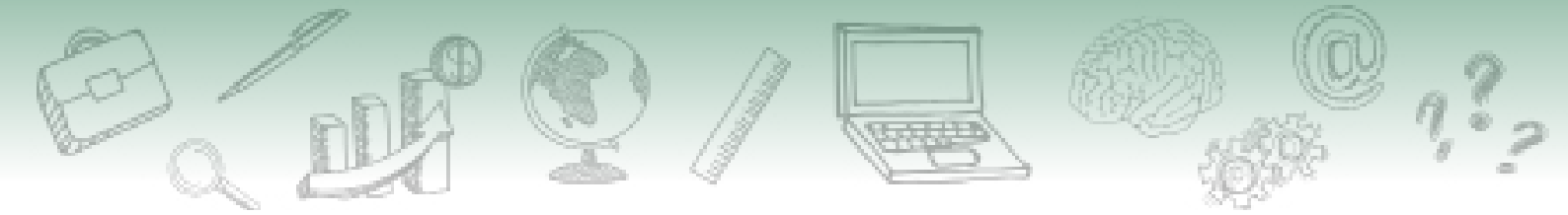
Governança de TIC no contexto da transformação digital

Módulo 4

Gestão de Riscos



Fundação Escola Nacional de Administração Pública

Presidente

Diogo Godinho Ramos Costa

Diretor de Desenvolvimento Profissional

Paulo Marques

Coordenador-Geral de Produção de Web

Carlos Eduardo dos Santos

Equipe

Laura Estela Carvalho (Conteudista, 2020)

Maysa Barreto Ornelas (Coordenadora, 2020)

Thaís de Oliveira Alcantara (Coordenadora, 2020)

Haruo Silva Takeda (Coordenação Web, 2021)

Caio Henrique Caetano (Revisão de texto, 2021)

Patrick Oliveira Santos Coelho (Implementação Articulate e Moodle, 2021)

Ana Paula Medeiros Araújo (Direção e produção gráfica, 2021)

João Paulo Albuquerque Cavalcante (Diagramação, 2021)

Curso produzido em Brasília 2020. Desenvolvimento do curso realizado no âmbito do acordo de Cooperação Técnica FUB / CDT / Laboratório Latitude e Enap.

Enap Escola Nacional de Administração Pública

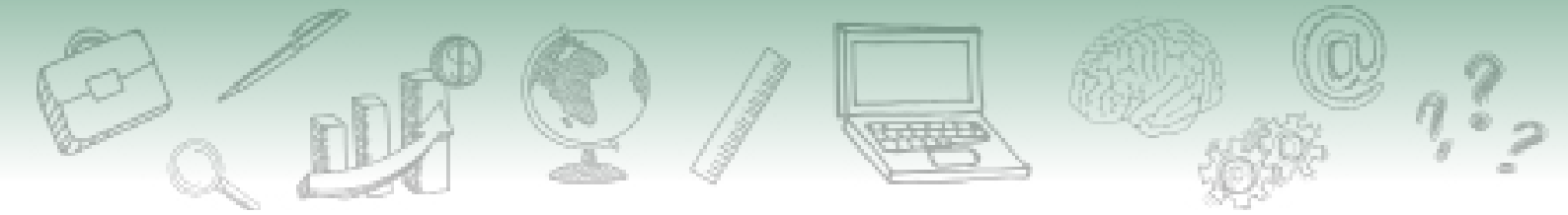
Enap, 202

Enap Escola Nacional de Administração Pública

Diretoria de Educação Continuada

SAIS - Área 2-A - 70610-900 — Brasília, DF

Sumário



Módulo 4

Gestão de Riscos

1. Gerenciando riscos no setor público

Neste módulo, você compreenderá o conceito e a importância do risco na organização, entenderá o processo de gestão de riscos e conhecerá os principais modelos de gestão de riscos adotados no mercado, identificando suas principais características e abordagens.

1.1. Riscos: principais conceitos e importância

Você certamente conhece a definição do termo risco, não é? E a gestão de riscos? Sabe para que ela serve? Acompanhe no podcast a seguir o que vamos falar sobre riscos, riscos na administração pública e riscos na transformação digital.

Podcast – Riscos, riscos na administração pública e riscos na transformação digital

SAIBA MAIS

> Dentro da definição de riscos, o Instituto Brasileiro de Governança Corporativa entende risco, no mundo corporativo, como algo além da possibilidade de alguma coisa não dar certo. Envolve a quantificação e a qualificação da incerteza, tanto no que diz respeito às perdas quanto aos ganhos por indivíduos ou organizações. Sendo o risco inerente a qualquer atividade – e impossível de eliminar –, a sua administração é um elemento-chave para a sobrevivência das companhias e demais entidades.

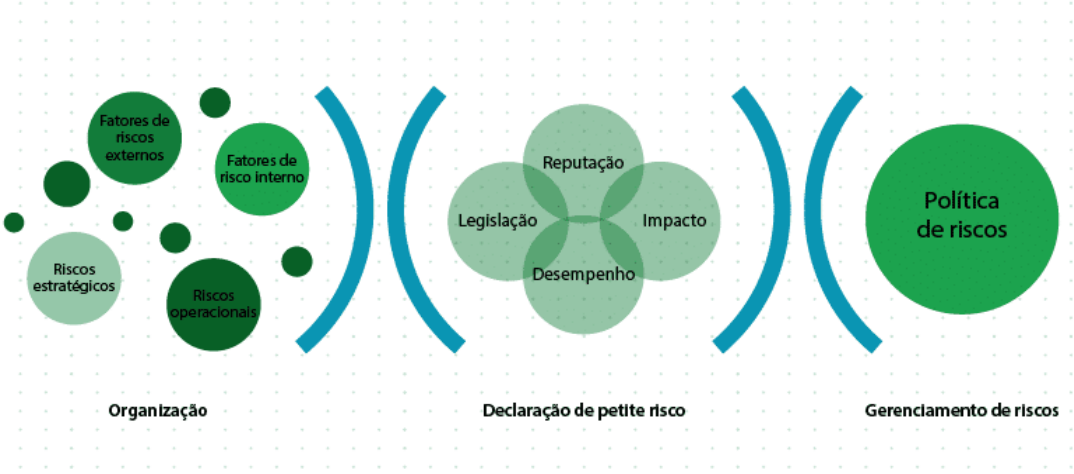
O que podemos fazer com os riscos?

Quando falamos de riscos, estamos lidando com a incerteza: algo que pode ou não acontecer. Caso o risco ocorra na organização, haverá uma consequência. Além disso, esses riscos podem ser positivos ou negativos. Parece estranho, mas é isso mesmo!

> Riscos positivos podem ser traduzidos como oportunidades (mas eles precisam ser planejados e não ocorrer por acaso ou sorte).

Um exemplo de risco positivo pode ser a entrega antecipada de um projeto que irá facilitar resultados para a organização. De acordo com o PMBOK, um evento totalmente desconhecido, ocorrido por pura sorte ou acaso, não deve ser considerado um risco positivo.

Veja, na imagem a seguir, uma demonstração de como ocorre a política de riscos.:



Política de riscos

Riscos inerentes, por sua vez, são os riscos associados ao negócio, independentemente de haver qualquer ação sobre eles.

Há algumas categorias de riscos elencados na literatura que têm relações e influências entre si e não podem ser considerados de forma isolada. Observe as relações entre os riscos, esquematizadas na figura a seguir.

Fonte: adaptado de Digital Financial Services Risk Management

No Brasil, o Código de Governança Corporativa, elaborado pelo IBGC, apresenta um quadro com um conjunto de situações/insumos para fatores de riscos relacionados ao ambiente externo e interno da organização. Veja:

CONTEXTO EXTERNO	CONTEXTO INTERNO
RISCOS ECONÔMICOS	**RISCOS FINANCEIROS**
- Disponibilidade de capital - Emissões de crédito, inadimplência - Concentração - Liquidez - Mercados financeiros - Desemprego - Concorrência - Fusões / aquisições.	- Falta de liquidez - Disponibilidade de bens - Acesso ao capital.
RISCOS SOCIOAMBIENTAIS	**RISCOS DE PESSOAL**
- Emissões e dejetos - Energia - Desenvolvimento sustentável	- Capacidade dos empregados - Atividade fraudulenta - Saúde e segurança
RISCOS SOCIAIS	**RISCOS OPERACIONAIS**
- Características demográficas - Comportamento do consumidor - Cidadania coorporativa - Privacidade - Terrorismo	- Capacidade - Design - Execução - Dependências / fornecedores
RISCOS TECNOLÓGICOS	**RISCOS TECNOLÓGICOS**
- Interrupções - Comércio eletrônico - Dados externos - Tecnologias emergentes	- Integridades de dados - Disponibilidade de dados a sistemas - Seleção de sistemas - Desenvolvimento - Alocação - Manutenção
RISCOS NATURAIS	**RISCOS DE IMAGEM**
- Desastres naturais	- Exposição negativa em meios de comunicação - Perda de confiança de partes interessadas
RISCOS LEGAIS / REGULATÓRIOS	**RISCOS LEGAIS / REGULATÓRIOS**
- Multas, sanções aplicadas por órgãos reguladores	- Suspensão de licenças de funcionamento - Legislação - Politica publica - Regulamentos

Fonte: Referencial para a Gestão de Riscos (TCU)

SAIBA MAIS

O quadro *Categoria de riscos de TI* (COBIT, 2019) traz uma relação que inclui riscos operacionais, que podem influenciar a estratégia da organização.

Reference	Risk Category
1	IT investment decision making, portfolio definition and maintenance
2	Program and projects lifecycle management
3 4	IT cost and oversight IT expertise, skills and behavior
5	Enterprise/IT architecture
6 7	IT operational infrastructure incedents Unauthorized actions
8	Software adoption/usage problems
9 10	Hardware incidents Software failures
11	Logical attacks (hacking, malware, etc.)
12	Third party/supplier incidents
13	Noncompliance
14	Geopolitical issues
15	Industrial action
16 17	Acts of nature Technology-based innovation
18	Environmental
19	Data and information management

Fonte: Cobit (2019)

Riscos e transformação digital

A transformação digital tem inserido novos desafios em relação aos riscos organizacionais. Nessa trajetória, podemos observar que os riscos fazem cada vez mais parte do processo de transformação digital.

É recomendável que as organizações incorporem o gerenciamento de riscos no processo de digitalização desde o início e em todas as etapas do planejamento e execução.

O COBIT é um *framework* abrangente e maduro em relação à governança e gestão de tecnologia da informação e ajuda as organizações a manterem riscos relacionados com a TI em um nível aceitável. Para ele, a gestão do risco relacionado à Informação e Tecnologia (I & T) deve ser integrada dentro da abordagem de gerenciamento de riscos corporativos para garantir um foco em TI pela empresa.

Áreas de riscos digitais

No contexto de rápidas mudanças promovidas pela necessidade de transformação digital das organizações, é importante identificar as áreas de risco que uma organização pode estar exposta em um ambiente digital.

De acordo com o relatório de riscos da Consultoria Deloitte, as áreas de riscos digitais são:

Tecnológicos
Potencial de perdas devido a falhas tecnológicas ou obsolescência. Os riscos relacionados à tecnologia têm um impacto em sistemas, pessoas e processos. As principais áreas de risco podem incluem escalabilidade, compatibilidade e precisão da funcionalidade da tecnologia implementada.

Cibersegurança
Proteção do ambiente digital contra -ataques não autorizados, acessos /, uso e garantia de confidencialidade e integridade dos sistemas de tecnologia. Os principais controles podem incluir proteção da plataforma, arquitetura de rede, segurança na aplicação, gerenciamento de vulnerabilidades e monitoramento da segurança.

Estratégico
Geralmente deriva dos objetivos de uma organização. Pode ser externo à organização e, na ocorrência, força uma mudança na direção estratégica da organização. Normalmente teria um impacto na experiência do cliente, valor da marca, reputação e vantagem competitiva no mercado.

Operações
Um evento, interno ou externo, que afeta uma capacidade da organização de atingir os objetivos de negócios através de suas operações definidas. Inclui riscos decorrentes de controles inadequados nos procedimentos operacionais.

Vazamento de informações
Garantir a proteção de dados em todo o ecossistema digital em vários estágios do ciclo de vida dos dados -– dados em uso, dados em trânsito e dados em repouso. As principais áreas de controle de foco estariam em torno de classificação de dados, retenção de dados, processamento de dados, dados e criptografia etc.

Terceiros
Compreende os riscos decorrentes de controles inadequados de fornecedores/ ambiente operacional de terceiros. Os principais controles seriam sobre compartilhamento de dados, integração tecnológica, dependência de operações, resiliência de fornecedor etc.

Privacidade
Risco decorrente do manuseio inadequado de dados pessoais sensíveis do cliente / funcionário, que podendo impactar a privacidade do indivíduo. Os controles principais incluem aviso, escolha, consentimento, precisão e outros princípios de privacidade. Vamos lembrar aqui da LGPD!

Legal
A capacidade do ambiente digital de permitir a investigação no evento de uma fraude ou violação de segurança, incluindo a captura de evidências de dados que possam ser apresentadas no tribunal.

Regulatório
Adesão a requisitos legais, incluindo tecnologias, leis, leis setoriais e regulamentos.

Resiliência
Risco de interrupção nas operações ou indisponibilidade de serviços, devido à alta dependência de equipamentos com tecnologia fortemente acoplados. As principais áreas de consideração incluiriam continuidade dos negócios, recuperação de desastres de TI / rede, cyber resiliência e gerenciamento de crises.

Essas áreas de riscos precisam ser amplamente consideradas pela organização na avaliação e no gerenciamento de riscos.

Riscos no setor público brasileiro

No setor público há uma preocupação central com o dever de cuidar do bem público. A própria definição do TCU, no escopo da definição de governança de TI inserida no Acórdão 2.308, de 2010, estabelece que se tenha um nível aceitável de risco em relação ao controle da utilização atual e futura da TI da organização. Assim define o TCU:.

> Governança de TI é o conjunto estruturado de políticas, normas, métodos e procedimentos destinados a permitir à alta administração e aos executivos o planejamento, a direção e o controle da utilização atual e futura de tecnologia da informação, de modo a assegurar, a um nível aceitável de risco, eficiente utilização de recursos, apoio aos processos da organização e alinhamento estratégico com objetivos desta última. Seu objetivo, pois, é garantir que o uso da TI agregue valor ao negócio da organização.” (TCU, Acórdão 2.308BRASIL,/ 2010 – Plenário).

O Decreto nº 9.203, de 2017, que dispões sobre a política de governança da APF traz que a gestão de riscos é estabelecida como um mecanismo de governança (art. 5º, III), que deve ser implementada pela alta administração das organizações (art. 17) e contemplada no Programa de Integridade (art. 19, III) de cada uma dessas entidades da administração pública federal direta, autárquica e fundacional.

Nesse sentido, os riscos sempre devem ser gerenciados de modo a manter o interesse público em primeiro plano, tendo como desafio da governança corporativa "equilibrar riscos e benefícios", além da otimização dos recursos utilizados.

O TCU desenvolveu um modelo de avaliação da maturidade organizacional em gestão de riscos, publicado pela Portaria-Segecex nº 9, de 18 de maio de 2017. Tal modelo tem por referência boas práticas dos principais modelos de gestão de risco do mercado - COSO GRC, ABNT NBR ISO 31000 Gestão de Riscos e Orange Book, e a Instrução Normativa IN-MP/CGU Nº 1/2016.

SAIBA MAIS

Segundo o Referencial Básico de Gestão de Riscos elaborado pelo TCU em 2018:

O modelo tem como premissas que a maturidade da gestão de riscos de uma organização é determinada pelas capacidades existentes em termos de liderança, políticas e estratégias, e de preparo das pessoas para gestão de riscos, bem como pelo emprego dessas capacidades aos processos e parcerias e pelos resultados obtidos na melhoria do desempenho da organização no cumprimento de sua missão institucional de gerar valor para as partes interessadas com eficiência e eficácia, transparência e accountability, e conformidade com leis e regulamentos. (BRASIL, 2018)

Decreto nº 9.203, de 22 de novembro de 2017

Art. 17. A alta administração das organizações da administração pública federal direta, autárquica e fundacional deverá estabelecer, manter, monitorar e aprimorar sistema de gestão de riscos e controles internos com vistas à identificação, à avaliação, ao tratamento, ao monitoramento e à análise crítica de riscos que possam impactar a implementação da estratégia e a consecução dos objetivos da organização no cumprimento da sua missão institucional, observados os seguintes princípios [...]. (BRASIL, 2017)

O setor público tem uma referência sólida em segurança da informação, que são os normativos do Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República.

Papéis e responsabilidades

De acordo com o *Referencial básico de gestão de riscos* (TCU,2018), "persiste a necessidade não apenas de estruturas e processos, mas também de uma cultura de gerenciamento de riscos, a fim de contribuir para que a organização obtenha resultados com desempenho otimizado".

A abordagem das três linhas de defesa, apresenta o fluxo de informações e os papéis e responsabilidades essenciais das áreas envolvidas.

Fonte: Referencial básico para gestão de riscos (TCU, 2018) Adaptado

Todos os profissionais, com divisão de funções e de responsabilidades dentro da organização, compõem suas três linhas de defesa, que são:

Primeira linha de defesa – operacional
Formada pelos gestores dos processos como dono do risco e corresponsável pelos controles dentro dos processos. Por vezes é necessário treinar usuários.

Segunda linha de defesa – corporativa
Representa a Política de Riscos elaborada e aprovada pela Diretoria e o Conselho de Administração, mais o processo de gestão de riscos.

Terceira linha de defesa – auditoria interna
Avalia de forma independente a eficácia do plano de controle para riscos corporativos. O Conselho de Aadministração tem obrigação de cobrar da diretoria e da presidência que o processo rode devidamente.

1.2. Gerenciamento de riscos

Você já ouviu falar de gerenciamento de riscos? É sobre isso que vamos falar neste tópico. O gerenciamento de riscos é um processo contínuo que envolve toda organização, desde o Conselho de Administração até o pessoal técnico, requerendo determinadas práticas de todos.

Referencial básico de gestão de riscos

De acordo com o Referencial básico de gestão de riscos do TCU, gestão de riscos é um conjunto de atividades coordenadas para identificar, analisar, avaliar, tratar e monitorar riscos. É o processo que visa conferir razoável segurança quanto ao alcance dos objetivos.

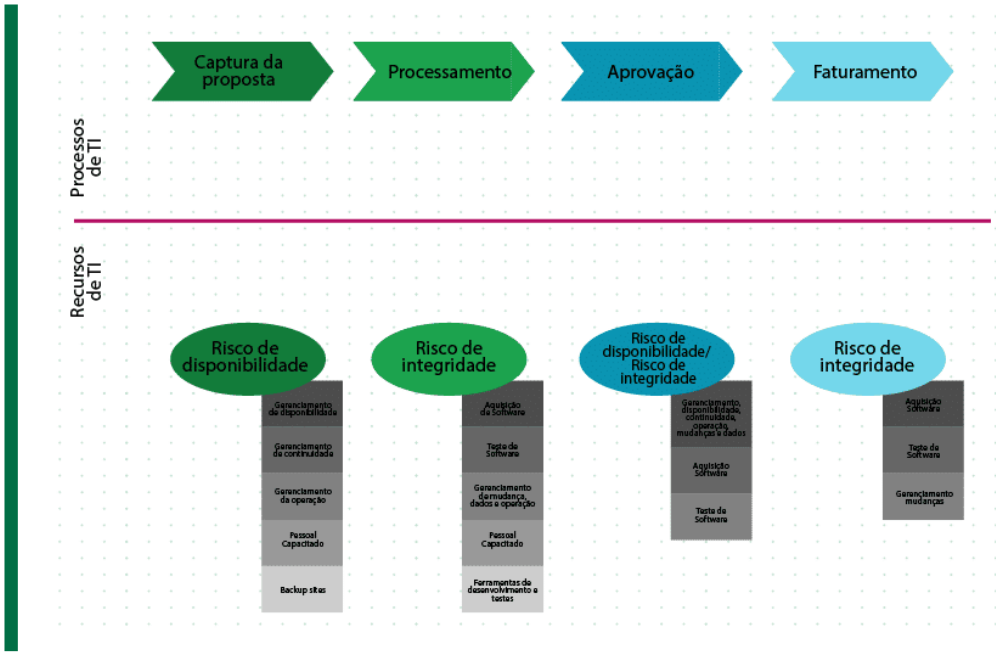
A TI assume papel estratégico dentro das organizações e assim, como uma das práticas de Governança de TIC, a gestão de riscos de tecnológicos deve ser integrada com a gestão de riscos da organização e compor sua política de riscos.

A literatura voltada para a Governança de TIC recomenda que a organização elabore seu mapa do processo do negócio e identifique qual serviço mais importante requer apoio da TIC.

SAIBA MAIS

Os autores Fernandes e Abreu apresentam, no livro Implantando a Governança de TI (2014),. um exemplo de mapa de risco com os principais riscos de TI para cada etapa do processo de negócio e relaciona os principais processos e recursos de TI que podem ser causadores da ocorrência de risco.

Fonte: Fernandes e Abreu (2014) com adaptações



Acompanhe, no podcast a seguir, o que vamos falar sobre gerenciamento de riscos.

Podcast – Gerenciamento de riscos

E como inovar e lidar com o risco?

A resposta pode ser simples, mas requer um amadurecimento e uma sólida política de riscos da organização. Somam-se a isso o alinhamento estratégico dos projetos inovadores e a declaração de apetite a riscos da organização, que precisam ser instrumentos habilitadores e delimitadores para a atuação inovadora da organização.

Provavelmente, você deve acompanhar as constantes reportagens sobre vazamento de dados, notadamente em ambientes digitais. Elas revelam fatos que não desejamos ver acontecer em nossa organização. Veja um exemplo:

A matéria traz ainda, as seguintes informações:

A pesquisa mostra também que o Brasil é o país mais propenso a sofrer violações de segurança: o risco é de 43% em uma empresa brasileira sofrer um ataque, muito acima de países com cultura de segurança cibernética, como Alemanha (com 14%) e Austrália (17%). Segundo Isaac Ferreira, superintendente de Engenharia de Produtos da Tecnobank, esse tipo de ataque tem como alvo pequenas e médias companhias por conta da menor quantidade de investimento em segurança da informação. (TECMUNDO, 2020)

Esse é apenas um exemplo, dentre os diversos casos que acontecem todos os dias no Brasil e no mundo. Você mesmo, se parar para refletir um pouco, pode se lembrar de casos ocorridos com você, com familiares e amigos e, inclusive no órgão em que trabalha. Então, vale a pena lembrar:

> **Na gestão de riscos, não basta identificar, classificar e tratar os riscos, é fundamental monitorar suas evoluções e, também, estar atento à ocorrência de riscos emergentes. A gestão de riscos não é um processo estático, one-shot. É preciso um acompanhamento constante. (SOUZA NETO)**

1.3. Principais modelos de mercado e escopo das abordagens

Agora vamos falar dos principais modelos de mercado para gerenciamento de riscos. A identificação do risco somada às boas práticas estabelecidas em modelos (COSO I, COSO II, ISO 31000, e The Oorange Bbook) são instrumentos para o gerenciamento de riscos.

Qual o significado da sigla COSO?

COSO significa Committee of Sponsoring Organizations of the Treadway Commission. O COSO é uma instituição sem fins lucrativos que reúne as principais instituições americanas. Em 1992, lançou um primeiro framework (COSO I) com foco em fraudes, em demonstrações financeiras e controle interno. Já se falava em rRiscos nas demonstrações financeiras.

O modelo COSO I

Podcast - COSO I

De acordo com o COSO I, o gerenciamento de riscos é um processo que envolve formulação de estratégias e ações para mitigar riscos negativos e aproveitar as oportunidades. O COSO I foi revisto em 2013 e tem ênfase na gestão de fraude.

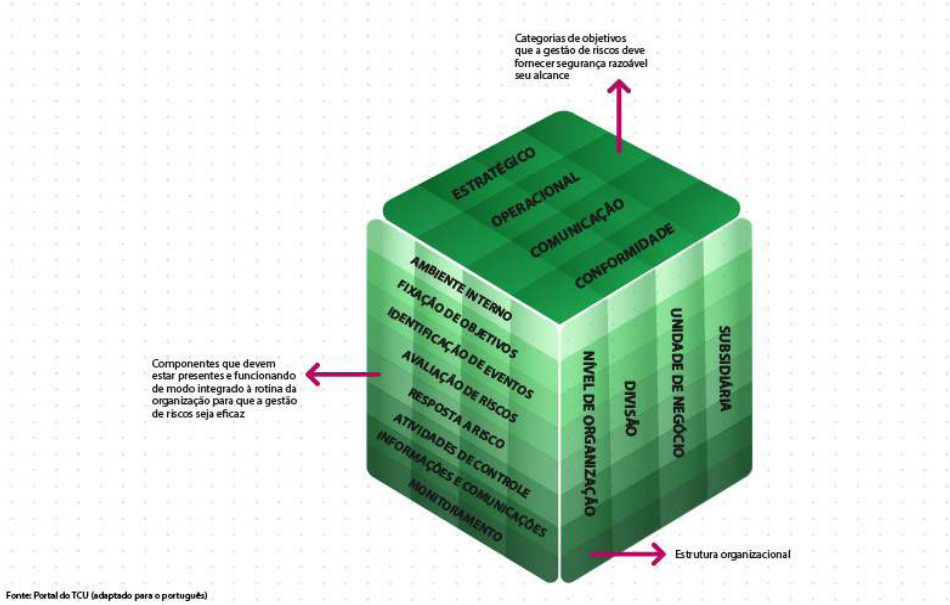
O modelo COSO II

Em 2004, o COSO quis ampliar sua abrangência. As disciplinas de risco falaram entre si e foi lançado o COSO 2 – ERM (gestão de riscos integrada) com foco na gestão de riscos corporativos.

Esse *framework* faz a gestão de risco de várias disciplinas, tais como financeiro, – operacional, – segurança do trabalho e– patrimonial,; consolidado numa matriz de risco.

Seu objetivo é identificar quais riscos são mais importantes e "fornecer estratégia de fácil utilização pelas organizações para avaliar e melhorar a gestão de riscos." (BRASIL, 2018).

Conheça a estrutura do COSO II pelo infográfico a seguir.



Fonte: Portal do TCU (adaptado para o português)

Em 2016, após uma consulta e revisão do COSO II, foi publicado o COSO GRC, que simplificou as definições e inseriu a gestão de riscos em três dimensões fundamentais à gestão de uma organização:

1. Missão, visão e valores centrais.
2. Objetivos estratégicos e de negócios.
3. Desempenho organizacional.

As etapas do processo de gestão de riscos nos modelos COSO II e ISO 31000 possuem a mesma essência, com diferença apenas em algumas terminologias.

O modelo ISO 31000

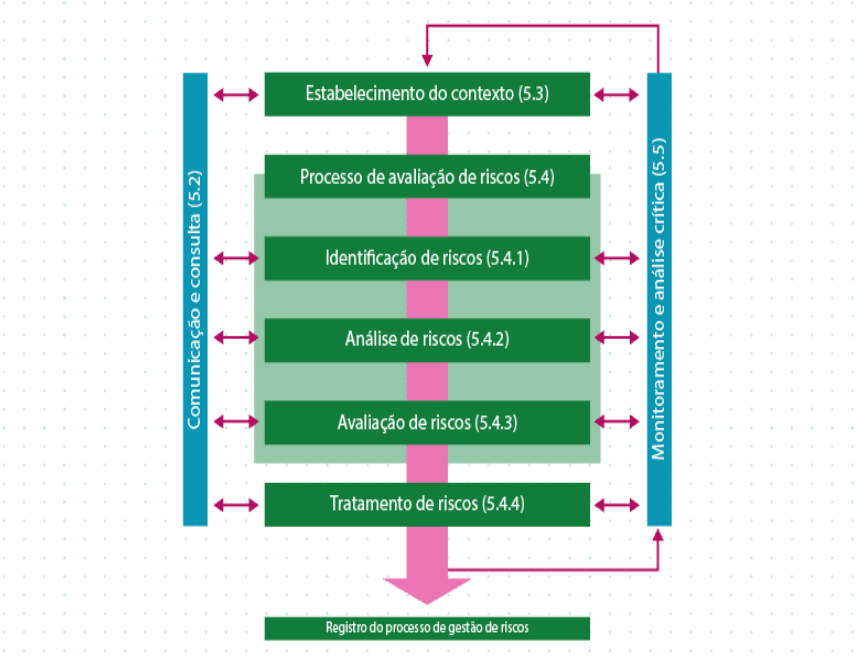
A ISO 31000 nasceu em 2009 para uniformizar a linguagem, se apresentando como uma norma de convergência, com princípios e boas práticas para o processo de gestão de riscos. Em 2018, foi publicada uma nova versão desse modelo.

Sua proposta é harmonizar os processos de gestão de riscos entre os diversos modelos, fornecendo uma abordagem comum para aplicação em ampla gama de atividades.

Segundo a norma ABNT NBR ISO 31000:2009, o processo de gestão de riscos, envolve:

- Comunicação e consulta.
- Estabelecimento do contexto.
- Processo de avaliação de riscos.
- Identificação de riscos.
- Análise de riscos.
- Avaliação de riscos.
- Tratamento de riscos.
- Monitoramento e análise.

Agora, observe estes passos e o fluxo entre as atividades, apresentados na imagem a seguir.



Fonte: Referencial básico para gestão de riscos (TCU, 2018)

Entenda um pouco mais sobre esses passos a seguir:

- **Passo 1 – Estabelecimento do contexto**

Parâmetros externos, e internos e dos critérios de risco a serem levados em consideração ao gerenciar riscos.

- **Passo 2 – Avaliação de riscos**

É o processo de compreender a natureza e determinar o nível de risco, de modo a subsidiar a avaliação e o tratamento de riscos. A avaliação de riscos envolve dois processos:

Identificação

É o processo de busca, reconhecimento e descrição dos riscos. A identificação de riscos pode basear-se em dados históricos, análises teóricas, opiniões de pessoas informadas e especialistas, assim como em necessidades das partes interessadas.

Análise do risco

É o processo de compreender a natureza e determinar o nível de risco, de modo a subsidiar a avaliação e o tratamento de riscos (ABNT, 2009).

O resultado final desse processo será o de atribuir a cada risco identificado uma classificação, tanto para a probabilidade como para o impacto do evento, cuja combinação determinará o nível do risco, dentro da matriz de classificação de riscos.

Dentro da etapa da avaliação de riscos, entenda as definições de escala de probabilidade e escala de impacto, bem como sua matriz:

Escala de probabilidade

Chances de um evento ocorrer, atribuindo pesos para as variações de muito baixa (improvável) até muito alta probabilidade (praticamente certa de ocorrer).

Escala de impacto

Consequências, e como elas serão medidas nas diversas áreas, com pesos para as variações de muito baixo, com impacto mínimo, até muito alto, com efeito catastrófico nos objetivos da organização.

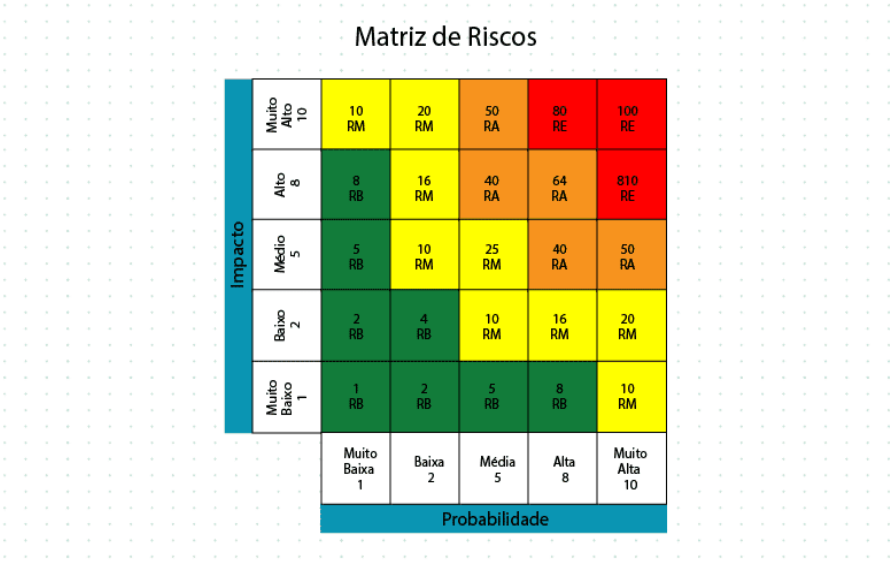
Matriz "impacto versus probabilidade"

Define como o nível de risco deve ser determinado, em escalas nos eixos e os pesos para as situações

- **Passo 3 – Matriz de classificação de riscos**

Define como os riscos serão classificados quanto à significância. Adota-se abordagens qualitativas e quantitativas para essa qualificação dos riscos, de acordo com o entendimento da organização sobre o mesmo este.

Para entender melhor o passo 3, observe a matriz de riscos apresentada a seguir. As cores sinalizam cada situação. Desde riscos com baixo impacto e baixa probabilidade, na cor verde, até os da área vermelha, que representam muito risco para a organização.



Fonte: adaptado do Referencial básico para gestão de riscos (TCU, 2018)

- **Passo 4 – -Tratamento dos riscos**

Define qual tipo de resposta será dada aos riscos identificados. Aqui, em especial, vamos detalhar um pouco mais sobre o que podemos fazer em relação aos riscos identificados:

Eliminar

Alterar o plano do projeto para eliminar totalmente o risco, protegendo os objetivos do projeto dos impactos deste risco eliminado.

Transferir

Transferir o risco para um terceiro, transferindo os impactos e a responsabilidade. É preciso ter em mente que o risco não é eliminado, e quase sempre envolve o pagamento de prêmios a parte que está assumindo o risco.

Mitigar

Reduzir a probabilidade ou impacto de um risco até um nível aceitável.

Aceitar

Quando não é possível aplicar nenhuma das outras estratégias, e a equipe do projeto decide correr o risco.

Modelo The orange book

O modelo *The Orange Book* é utilizado pelo TCU como uma das bases para a avaliação de maturidade das organizações públicas em relação à gestão de riscos.

De acordo com o TCU, todas as normas relativas à ISO falam do *The Orange Book: Management of Risk – Principles and Concepts*. Produzido e publicado pelo HM Treasury Britânico, foi a principal referência do programa de gestão de riscos do governo do Reino Unido, iniciado em 2001.

O modelo tem como vantagens: ser compatível com padrões internacionais de gestão de riscos e introduzir e tratar esse tema complexo de forma simples e abrangente.

SAIBA MAIS

O modelo está estruturado em quatro processos, que são: a identificação e avaliação do risco para determinar sua prioridade e como será gerenciado,; as formas para o tratamento do risco,; o monitoramento integrado e a comunicação do risco para tomada de decisão.

Fonte: The Orange Book Management of Risk (adaptado)

O COBIT

O COBIT é um *framework* abrangente e maduro em relação à governança Governança e gestão de tecnologia da informação, que ajuda as organizações a manterem riscos relacionados com a TI em um nível aceitável. Para ele, a gestão do risco relacionado à Informação e Tecnologia (I & T) deve ser integrada dentro da abordagem de gerenciamento de riscos corporativos, para garantir um foco em TI pela empresa.

O *framework* possui duas áreas foco associadas a risco: riscos e segurança. Dentro do objetivo de governança EDM03, elenca-se a matriz de responsabilidades entre os envolvidos e estabelece-se as atividades relacionadas a cada um dos processos envolvidos.

O objetivo de governança	EDM03 Assegurar a otimização de riscos.	Assegura que o apetite e tolerância a riscos da organização são compreendidos, articulados e comunicados e que o risco ao valor da organização relacionado ao uso de TI é identificado e controlado.
Processos	APO12 – Gerenciar riscos. APO13 – Gerenciar segurança. DSS05 – Gerenciar serviços de segurança .	Identificar continuamente, avaliar e reduzir os riscos relacionados a TI, dentro dos níveis de tolerância estabelecidos pela diretoria executiva da organização .

No âmbito dos processos, a indicação é identificar continuamente e, avaliar e reduzir os riscos relacionados a TI, dentro dos níveis de tolerância estabelecidos pela diretoria executiva da organização.

SAIBA MAIS

Veja, a seguir, curiosidades sobre a gestão de riscos corporativos e algumas notas sobre organizações internacionais relacionadas ao tema.

Curiosidades

- No início do século XXI, houve a consolidação e disseminação de práticas de gestão de risco corporativo. Entre as publicações que se tornaram referências internacionais no tema estão: o *The Orange Book*, a lei Sarbanes-Oxley, o COSO-ERM, o Acordo de Basileia II, a AS/NZS 4360:2004 e a ISO 31000:2009.

- Com base no Orange Book, em 2013, o então Ministério do Planejamento, Orçamento e Gestão produziu o Guia de Orientação para o Gerenciamento de Riscos, para apoiar o Modelo de Excelência do Sistema de Gestão Pública

(GESPÚBLICA) e prover uma introdução ao tema gerenciamento de riscos (BRASIL, 2013).

Notas

- **CenturyLink:** is a global communications, hosting, cloud and IT services company enabling millions of customers to transform their businesses and their lives through innovative technology solutions. CenturyLink offers network and data systems management, Big Data analytics and IT consulting, and operates more than 55 data centers in North America, Europe and Asia. The company provides broadband, voice, video, data and managed services over a robust 250,000-route-mile U.S. fiber network and a 300,000-route-mile international transport network.

- **Deloitte:** refere-se a uma ou mais empresas da Deloitte Touche Tohmatsu Limited ("DTTL"), sua rede global de firmas-membro e suas entidades relacionadas (coletivamente, a "organização Deloitte").

- **IFC:** A member of the World Bank Group, is the largest global development institution focused on the private sector in emerging markets. Working with more than 2,000 businesses worldwide, we use our capital, expertise, and influence, to create opportunity where it's needed most. In FY15, our long-term investments in developing countries rose to nearly $18 billion, helping the private sector play an essential role in the global effort to end extreme poverty and boost shared prosperity. For more information, visit www.ifc.org

- **PwC:** refere-se à PricewaterhouseCoopers Brasil Ltda., firma membro do network da PricewaterhouseCoopers.

O processo de gerenciamento de risco da organização precisa utilizar as metodologias de pelo menos um dos frameworks apresentados.

Vimos, nesta unidade, os principais conceitos sobre riscos e gerenciamento de riscos. Na administração pública, busca-se atuar com um nível aceitável de risco. Por isso, é muito importante que você se aprofunde no tema gerenciamento de riscos.

SAIBA MAIS

Referencial básico de gestão de riscos do TCU (2018), além de publicações que orientem detalhadamente acerca da ISO 31000 (Gestão de Riscos) e da Família 27000 – ISO/IEC 27000 series – ISO 27001:2019, que envolve a privacidade da informação, e da Lei Geral de Proteção de Dados - LGPD.

Glossário

Apetite a riscos - Declaração da organização quanto a um risco ser aceitável ou inaceitável.

COBIT - Control Objetives for Information and Related Technology

Compliance - Conformidade. No âmbito institucional e corporativo, compliance é o conjunto de disciplinas a fim de cumprir e se fazer cumprir as normas legais e regulamentares.

ERM - Sigla para Enterprise Risk Manager

ISACA - Information System Audit and Control Association

ISO - International Organization for Standardization (Organização Internacional de Normalização)

Framework - Termo utilizado na área de tecnologia para designar estruturas de modelos.

Oone-shot - Termo para designar a realização única, fazer uma vez só.

PMBOK - Sigla de Project Management Body of Knowledge. é É um conjunto de práticas na gestão de projetos organizado pelo instituto PMI e é considerado a base do conhecimento sobre gestão de projetos por profissionais da área.

TCU - Tribunal de Contas da União

TIC - Tecnologia da Informação e Comunicação

Referências

ABNT. NBR ISO – 31000/2018. Rio de Janeiro: ABNT, 2018.

BRASIL. **Referencial básico de gestão de riscos**. Brasília: TCU, 2018.

BRASILIANO A. C. R. **Gestão de Riscos (videoaula)**. Fundação Dom Cabral. 2018.

CAPGEMINI. **The digital culture challenge: closing the employee-leadership gap**. [S.l.] Capgemini, 2017.

CENTURE LINK. **Effective risk management in digital transformation.** [S.l.] Century Link, 2017. Disponível em: https://www.insightbrief.net/wp-content/uploads/Effective-Risk-Management-in-Digital-Transformation-InsightBrief.pdf. Acesso em: 21 jan. 2021.

DELLOITE. **Managing risk in digital transformation. [**S.l.] Deloitte, 2018. Disponível em: https://www2.deloitte.com/content/dam/Deloitte/za/Documents/risk/za_managing_risk_in_digital_transformation_112018.pdf. Acesso em: 21 jan. 2021.

FERNANDES, A. A.; ABREU F. V. **Implantando a governança de TI: da estratégia à gestão dos processos e serviços**. Rio de Janeiro: BRASPORT, 2014. 4ª. ed. 630p.

IBGC. **Gerenciamento de riscos corporativos: evolução em governança e estratégia**. São Paulo: IBGC, 2017.

IFC. **Digital financial services and risk management.** [S.l.] IFC, 2016. Disponível em: https://www.ifc.org/wps/wcm/connect/92ac1a71-6bd5-43db-84ff-1b6794f82653/Digital+Financial+Services+and+Risk+Management+Handbook.pdf?MOD=AJPERES&CVID=mxxEJFZ. Acesso em: 21 jan. 2021.

ISACA. **COBIT 2019 Framework: governance and management objectives**. [S. l.], ISACA, 2018. 302p.

ISACA. **Selected COBIT 5 processes for essential enterprise security.** [S.l] ISACA Journal, 2015. Disponível em: https://www.isaca.org/resources/isaca-journal/issues/2015/volume-2/selected-cobit-5-processes-for-essential-enterprise-security. Acesso em: 21 jan. 2021.

MARTINS M., A. F.; SANTOS, W. O.; BRITO, R. L.; ALVES, G. F. **Política de gestão de riscos corporativos: o caso de uma agência reguladora da saúde**. Revista do Serviço Público. Brasília 69 (1). p. 7-32. Jan/mar 2018.

PMI. **Preparação para o risco.** PM NETWORK, [S.l.], v. 33, n. 7, p. 7-7, jul. 2019.

SOUZA NETO, J. C**urso Gestão de Riscos Digitais (slides)**. Universidade Católica de Brasília. 2019.

SOUZA NETO, J. **Workshop de Cobit 2019**. In: 5º Fórum IBGP de Governança de TI. 2019.

RIPLEY, M. T**he orange book: management of risk – principles and concepts**. [S.l.] HM Treasury Britânico, 2020. Disponível em: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/866117/6.6266_HMT_Orange_Book_Update_v6_WEB.PDF. Acesso em: 21 jan. 2021.

Welcome to COSO. COSO. Disponível em: https://www.coso.org/Pages/default.aspx. Acesso em: 21 jan. 2021.