Universidade Federal da Paraíba
Pró-Reitoria de Administração (PRA)

MANUAL DE PROCEDIMENTOS:

Gestão de Riscos

João Pessoa - PB
29 de outubro de 2024

Sumário

1 Apresentação **4**

2 Conceitos e Glossário de Termos e Siglas **6**

3 Legislação Aplicada e Documentos de Referência **8**

a) Legislação Aplicada 8

b) Documentos de referência 8

4 Implementação da Gestão de Riscos **9**

Passo 1: Entendimento do Contexto **10**

a) Objetivos do processo 10

b) Contextos interno e externo 10

c) Partes interessadas 10

d) Ferramentas de apoio 10

Passo 2: Identificação de Riscos **12**

a) Técnicas de identificação 12

b) Categorias de riscos 13

Passo 3: Identificação e Avaliação dos Controles **15**

a) Tipos de controles 15

b) Métodos de avaliação de controles 16

c) Documentação e integração do processo 16

Passo 4: Cálculo dos Níveis de Risco **17**

a) Mensurando probabilidade 17

b) Mensurando impacto 17

c) Nível de risco e Matriz de risco 18

d) Importância do cálculo dos níveis de risco 19

Passo 5: Respostas ao Risco (Plano de Ação) **20**

a) Tipos de respostas ao risco 20

b) Elaboração do plano de ação 20

c) Critérios de sucesso 21

Passo 6: Validação dos Resultados **22**

a) Critérios da validação 22

b) Etapas do processo de validação 22

Passo 7: Comunicação e Monitoramento **23**

a) Comunicação 23

b) Monitoramento 23

c) Processo contínuo e ininterrupto 24

1 Apresentação

A Gestão de riscos pode ser entendida como o processo sistemático de identificar, avaliar e controlar potenciais eventos ou situações que possam impactar negativamente os objetivos e operações de uma organização. Seu objetivo principal é minimizar a probabilidade e o impacto de eventos adversos, ao mesmo tempo em que se busca maximizar as oportunidades. Isso envolve a identificação de riscos (financeiros, operacionais, tecnológicos, regulatórios ou estratégicos), a avaliação de sua gravidade, a implementação de estratégias para mitigá-los ou transferi-los, e o monitoramento contínuo desses riscos ao longo do tempo.

A gestão de riscos é essencial para instituições de ensino superior, como a UFPB, promovendo sustentabilidade organizacional e eficiência. A redução de riscos melhora os serviços públicos e fortalece a confiança da sociedade na instituição. Além disso, apoia a tomada de decisões, oferecendo informações valiosas aos gestores, prevenindo perdas e protegendo os recursos da universidade, o que resulta em uma administração mais responsável.

A política de gestão de riscos é um documento formal que define os princípios, objetivos e diretrizes que a organização seguirá no gerenciamento de riscos. Ela reflete o compromisso da alta administração em gerenciar riscos de forma proativa, integrando essa prática à cultura e operações diárias. Além disso, comunica claramente o papel do gerenciamento de riscos para colaboradores e partes interessadas, alinhando-se aos valores da organização e proporcionando uma base sólida para a gestão disciplinada de incertezas e oportunidades.

A **implementação da gestão de riscos** na Pró-Reitoria de Administração (PRA) seguiu um cronograma estruturado, com etapas-chave para garantir seu sucesso. Inicialmente, foi formado um grupo de trabalho para conduzir o procedimento, que começou com a análise de processos, unidades e projetos críticos da PRA. Neste ponto, a equipe definiu a estratégia de implantação e a arquitetura da gestão de riscos, estabelecendo objetivos, estruturas e processos essenciais, além de criar diretrizes específicas. Além disso, as responsabilidades foram claramente atribuídas, assegurando que cada membro da equipe entendesse seu papel e suas obrigações.

Este documento, que toma como base o Referencial Básico de Gestão de Riscos do Tribunal de Contas da União (TCU), visa informar os servidores sobre os procedimentos de gerenciamento de riscos adotados pela PRA. Este manual oferece diretrizes detalhadas sobre a aplicação da metodologia da unidade e os procedimentos seguidos. Focado em uma abordagem prática, o documento não aborda teorias subjacentes nem inclui referências bibliográficas, recomendando a consulta a publicações especializadas para um aprofundamento no tema.

Mais informações podem ser consultadas no processo **23074.027133/2024-11** via sipac.ufpb.br ou por meio do LINK da planilha que contém o registro dos macroprocessos analisados por cada unidade, de modo a visualizar cada uma das etapas executadas, tais como identificação, mensuração e tratamento de riscos. Outras informações ou dúvidas, entrar em contato com a Secretaria Executiva da PRA, pelo e-mail: secretaria@pra.ufpb.br ou telefone: **(83)3216-7410**.

Cássio da Nóbrega Besarria
Pró-Reitor de Administração

Laryssa Brilhante Catanduba
Assessora da Pró-Reitoria de Administração

Gustavo Rodrigues da Rocha
Coordenador de Administração e Patrimônio

Hallilson Cosmo de Melo
Coordenador da Divisão de Materiais

Rubens Alberto Falcão Ferreira
Coordenador de Contabilidade e Finanças

Gilmara de Lima Nóbrega
Diretora de Administração

Rebeca Honorato Neiva
Administradora da Assessoria de Contratos e Licitação

Italo Simplício de Freitas Paiva
Diretor da Divisão de Materiais

Alexandro Fernandes da Silva
Administrador do Setor Requisitante

Alexandre Paulo Lopes
Contador da Divisão de Contabilidade

Thiago da Silva Lins
Contador da Divisão de Administração Financeira

Gleydson Kelson Correia e Castro
Assistente em Administração da Secretaria Executiva

2 Conceitos e Glossário de Termos e Siglas

- **Aceitar**: Estratégia de resposta ao risco em que a organização decide não tomar medidas adicionais para tratar o risco, normalmente utilizada para riscos com baixo impacto e baixa probabilidade.
- **Apetite ao Risco**: O nível de risco que uma organização está disposta a aceitar na busca pelo alcance de seus objetivos.
- **Causas** - Fatores, ações ou eventos que levam ao surgimento ou à ocorrência de um risco.
- **Comunicação de Riscos**: Processo de disseminação de informações sobre os riscos identificados, suas implicações e as ações adotadas para mitigá-los, tanto internamente quanto externamente.
- **Consequências** - Impactos ou danos que podem ocorrer se um risco se concretizar.
- **Controles**: Medidas, ações ou procedimentos estabelecidos para reduzir a probabilidade de ocorrência de um risco ou minimizar seus impactos. Podem ser classificados como preventivos (atuam nas causas) ou corretivos (atuam nas consequências).
- **Controles Corretivos**: Controles que visam mitigar os efeitos ou consequências de um risco, após sua materialização.
- **Controles Preventivos**: Controles que visam prevenir a ocorrência de um risco, agindo sobre suas causas.
- **Evitar**: Estratégia de resposta ao risco que implica eliminar completamente a causa do risco, evitando que ele se materialize.
- **Gestão de Riscos**: Processo de identificar, avaliar, tratar e monitorar os riscos que podem impactar os objetivos da organização. Inclui a definição de políticas e procedimentos para garantir o controle adequado dos riscos.
- **Impacto**: O efeito ou consequência que a materialização de um risco pode ter sobre os objetivos da organização.
- **Mitigar**: Estratégia de resposta ao risco que visa reduzir a probabilidade de ocorrência ou o impacto de um risco, por meio da implementação de controles ou ações corretivas.
- **Monitoramento**: Processo contínuo de acompanhamento do desempenho das ações de controle e da evolução dos riscos, para garantir que os níveis de risco estejam dentro do aceitável.
- **Plano de Ação**: Documento que descreve as medidas a serem adotadas para implementar as respostas aos riscos, incluindo prazos, responsáveis e recursos necessários.
- **Política de Gestão de Riscos**: Conjunto de diretrizes e procedimentos que guiam a forma como a organização identifica, avalia, responde e monitora os riscos.
- **Probabilidade**: A chance de um risco se materializar. Refere-se à frequência esperada de ocorrência de um evento de risco.

- **Risco**: Situações ou eventos incertos que podem afetar adversamente, no todo ou em parte, os objetivos de uma organização, projeto ou atividade.
- **Risco Residual**: Risco que permanece após a aplicação das ações de controle. Ele deve ser monitorado continuamente para garantir que está dentro dos níveis aceitáveis.
- **Stakeholders**: Todas as partes interessadas que podem influenciar ou ser impactadas pelos riscos e pelas respostas adotadas pela organização, como colaboradores, acionistas, clientes e reguladores.
- **TCU** - Tribunal de Contas da União.
- **Tolerância ao Risco**: O grau de variação que a organização está disposta a aceitar nos níveis de risco, de acordo com seu apetite ao risco.
- **Transferir**: Estratégia de resposta ao risco que consiste em transferir a responsabilidade do risco para outra parte, como por meio de um contrato de seguro ou terceirização.

3 Legislação Aplicada e Documentos de Referência

a) Legislação aplicada:

- Acordão TCU Nº 2.467/2013 – Plenário - Enfatiza a importância da gestão de riscos nas entidades públicas, recomendando a adoção de práticas proativas para identificar, avaliar e mitigar riscos. Destaca diretrizes para implementação, monitoramento contínuo e a responsabilização dos gestores, visando melhorar a governança e a transparência na administração pública.

- Acordão TCU Nº 1.273/2015 – Plenário - Destaca a importância do planejamento e controle na execução orçamentária, enfatizando que a gestão de riscos deve ser integrada a esses processos. O acórdão ressalta a necessidade de identificar e mitigar riscos, monitorar continuamente os processos e garantir a transparência e a responsabilidade dos gestores na administração dos recursos públicos.

- Instrução normativa conjunta MP/CGU Nº 01/2016 - Dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo federal.

- Acordão TCU Nº 2.127/2017 – Plenário - Trata da gestão de riscos no contexto da fiscalização e controle das contas públicas. O TCU recomenda que as entidades adotem práticas robustas de gestão de riscos para garantir a integridade e a eficiência na utilização dos recursos públicos. O acórdão enfatiza a necessidade de identificar, avaliar e monitorar riscos, além de integrar esses processos ao planejamento estratégico das instituições, visando melhorar a governança, a transparência e a *accountability* na administração pública..

- Resolução TCU Nº 287/2017 - Dispõe sobre a política de gestão de riscos do Tribunal de Contas da União e altera as Resoluções TCU 266, de 30 de dezembro de 2014, que define a estrutura, as competências e a distribuição das funções de confiança das unidades da Secretaria do Tribunal de Contas da União; a 261, de 11 de junho de 2014, que dispõe sobre a Política de Segurança Institucional (PSI/TCU) e o Sistema de Gestão de Segurança Institucional do Tribunal de Contas da União (SGSIN/TCU); e a 247, de 7 de dezembro de 2011, que dispõe sobre a Política de Governança de Tecnologia da Informação do Tribunal de Contas da União.

- Resolução CONSUNI Nº 07/2024 - Aprova a nova Política de Gestão de Riscos da Universidade Federal da Paraíba.

b) Documento de referência:

- Referencial Básico de Gestão de Riscos do TCU - Manual que objetiva prover orientações técnicas aos responsáveis pela governança e gestão das organizações públicas, especialmente no que diz respeito à incorporação de boas práticas de gestão de riscos nas instituições, com vistas a ajudar os gestores a implementar o novo marco regulatório da governança pública.

4 Implementação da Gestão de Riscos

A **implementação da gestão de riscos** envolve a adoção prática das etapas previamente definidas no processo. A partir da identificação dos riscos até o monitoramento contínuo, a implementação deve garantir que todas as atividades planejadas sejam executadas de forma integrada e eficaz. Para que a gestão de riscos seja implementada com sucesso, é fundamental seguir as etapas essenciais do processo:

Passo 1: Entendimento do Contexto

Passo 2: Identificação de Riscos

Passo 3: Identificação e Avaliação dos Controles

Passo 4: Cálculo dos Níveis de Risco

Passo 5: Resposta aos Riscos (Plano de Ação)

Passo 6: Validação dos Resultados

Passo 7: Comunicação e Monitoramento

Analogamente, as etapas podem ser expressas em formato esquematizado, como o demonstrado abaixo:

A implementação da gestão de riscos segue essas etapas de maneira integrada, garantindo que a organização esteja preparada para identificar, avaliar, mitigar e monitorar os riscos de forma eficaz e proativa. A etapas, anteriormente mencionadas, são detalhadas nas seções a seguir.

Passo 1: Entendimento do Contexto

O primeiro passo no processo de gestão de riscos é o **Entendimento do Contexto**. Nesta etapa, busca-se compreender completamente os processos envolvidos, seus objetivos, os fatores que podem afetá-los e as partes interessadas. Esta fase é crucial para garantir que a gestão de riscos seja bem-sucedida, pois fornece as bases sobre as quais as decisões serão tomadas.

Os processos a serem analisados, inicialmente, podem ser selecionados por meio da *expertise* (conhecimento especializado) do servidor no setor em que atua. Por meio desse primeiro filtro, os processos definidos como prioritários (que demandam uma maior atenção) são analisados de forma detalhada, especialmente com relação aos seus objetivos (ou resultados) pretendidos.

a) Objetivos do processo: o entendimento do contexto deve iniciar com a definição clara dos objetivos do processo a ser analisado. Pergunte-se:

- Qual é o objetivo principal deste processo?
- Quais são os resultados esperados?
- Como este processo se relaciona com os objetivos estratégicos da organização?

b) Contextos interno e externo: em seguida, devem ser caracterizados os contextos interno e externo ao processo para compreender o ambiente em que a organização opera. Isto inclui:

- **Contexto interno**: Quais são os fatores internos que podem afetar o processo? Isso pode incluir a estrutura organizacional, recursos disponíveis, cultura organizacional e governança;
- **Contexto externo**: Quais fatores externos podem impactar o processo? Considere o ambiente econômico, político, regulatório e social em que a organização está inserida.

c) Partes Interessadas: por fim, é importante identificar as partes interessadas e entender suas expectativas e preocupações em relação ao processo. Isto pode ser feito por meio de:

- **Análise de *stakeholders* (interessados)**: identificando quem são os principais envolvidos e qual o seu papel no processo.
- **Consultas com as partes interessadas**: para assegurar que suas visões e preocupações sejam levadas em conta na gestão de riscos.

d) Ferramentas de Apoio: nesta fase, recomenda-se o uso de ferramentas que auxiliem a mapear fatores relevantes sobre os processos analisados, tais como:

- **SWOT**: Uma análise de *Strengths* (forças), *Weaknesses* (fraquezas), *Opportunities* (oportunidades) e *Threats* (ameaças), que ajuda a mapear as forças, fraquezas, oportunidades e ameaças do processo;

- **AS-IS/TO-BE**: Essa ferramenta permite mapear o estado atual (*AS-IS*) do processo e o estado desejado (*TO-BE*), identificando as lacunas entre ambos.
- **Análise de Cenários**: Considera diferentes cenários que possam afetar os objetivos do processo e como cada um deles pode modificar os riscos envolvidos.

Obs.: Toda a análise realizada deve ser devidamente documentada. Isso inclui os objetivos do processo, os fatores internos e externos que podem influenciá-lo, a análise das partes interessadas e os resultados obtidos a partir das ferramentas de análise. Esta documentação servirá de base para as etapas seguintes da gestão de riscos e facilitará o monitoramento contínuo do processo. Além disso, a comunicação contínua com as partes interessadas deve ser mantida durante todo o ciclo de gestão de riscos.

Passo 2: Identificação de Riscos

A segunda etapa da gestão de riscos é a **Identificação de Riscos**. Essa etapa tem como objetivo identificar eventos que possam prejudicar o alcance dos objetivos definidos na etapa anterior. É importante capturar o máximo de informações sobre potenciais riscos, suas causas e consequências. A **Identificação de Riscos** visa à criação de uma lista abrangente de eventos que podem impactar os objetivos do processo. Esses eventos podem se originar de fatores internos ou externos e devem ser analisados quanto à sua probabilidade de ocorrência e impacto.

Uma forma de sintetizar a análise realizada nesta etapa pode ser expressa pela seguinte sintaxe, proposta pelo TCU, para a descrição de um risco:

> Devido a <CAUSA/FONTE>, poderá acontecer <DESCRIÇÃO DA INCERTEZA>, o que poderá levar a <DESCRIÇÃO DO IMPACTO/CONSEQUÊNCIA/EFEITO>, impactando no/na <DIMENSÃO DE OBJETIVO IMPACTADA>.

Exemplo:

- Objetivo: apresentar propostas para licitações até as datas fixadas em editais;
- Evento: não participação da empresa em licitações;
- Causa/Fonte: não entrega de cotações de preços por parte de fornecedores;
- Consequência: interrupção das atividades;
- Dimensão do objetivo impactada: custos e despesas fixas.

> **Descrição do risco:** Devido a não entrega de cotações de preços por parte de fornecedores, poderá acontecer a não participação da empresa em licitações, o que poderá levar a interrupção das atividades, impactando nos custos e nas despesas fixas.

a) Técnicas de identificação: diversas técnicas podem ser utilizadas para garantir uma identificação completa e precisa dos riscos. A escolha da técnica depende do contexto da organização e dos recursos disponíveis. A seguir, destacam-se algumas das principais abordagens recomendadas:

- **Brainstorming:** Um método colaborativo em que uma equipe se reúne para gerar o maior número possível de ideias sobre os riscos. O objetivo é incentivar a criatividade, evitando julgamentos imediatos, e permitir que diferentes perspectivas sejam compartilhadas.
- **SWIFT (Structured What-If Technique):** Consiste em fazer perguntas estruturadas do tipo "e se..."para identificar possíveis eventos de risco. Essa técnica é útil para explorar diferentes cenários e como eles podem impactar os objetivos.

- **Entrevistas:** Realizar entrevistas com pessoas que possuem conhecimento profundo sobre o processo em questão. Essas entrevistas podem fornecer *insights* valiosos sobre riscos que não seriam identificados apenas com métodos grupais.
- **Delphi:** Um método estruturado para coletar opiniões de especialistas de maneira anônima e iterativa. Após várias rodadas, os especialistas chegam a um consenso sobre os riscos mais relevantes.
- **Diagrama de Ishikawa (Causa ⇒ Evento ⇒ Efeito):** Nessa técnica, os riscos são descritos em termos de causa (o fator que pode desencadear o evento), o evento (o risco em si) e o efeito (as consequências do evento se ele ocorrer). Esse modelo ajuda a organizar os riscos de maneira lógica e compreensível.
- **Checklists:** Listas de verificação pré-definidas com potenciais riscos baseados em experiências anteriores ou em práticas recomendadas.
- **Análise de Fluxo de Processos:** Examinar o fluxo de processos ajuda a identificar riscos ao observar as interações entre entradas, saídas e responsáveis em cada etapa.
- **Análise de Causa Raiz:** Aprofundar-se nas causas subjacentes de um risco identificado pode revelar outros riscos correlacionados.

b) Categorias de riscos: os riscos identificados podem ser classificados em diferentes categorias, para facilitar o entendimento e o tratamento futuro. Algumas categorias comuns incluem:

- **Riscos Estratégicos:** Estão associados à tomada de decisão que pode afetar negativamente o alcance dos objetivos da organização;
- **Riscos Operacionais:** Estão associados à ocorrência de perdas (produtividade, ativos e orçamentos) resultantes de falhas, deficiências ou inadequação de processos internos, infraestrutura, pessoas, sistemas, tecnologia, assim como de eventos fortuitos (catástrofes naturais, greves, entre outros);
- **Riscos de Comunicação:** Estão associados a eventos que podem impedir ou dificultar a disponibilidade de informações para a tomada de decisões e para cumprimento das obrigações e responsabilizaçao, avaliação e prestação de contas às instâncias controladoras e à sociedade;
- **Riscos de Integridade:** Estão associados a eventos de risco que podem resultar em desvios éticos, irregularidades administrativas, fraude e corrupção;
- **Riscos de Imagem/Reputação:** Estão associados a eventos que podem comprometer a confiança da sociedade (ou de parceiros, usuários ou de fornecedores) em relação à capacidade da UFPB em cumprir sua missão institucional;
- **Riscos Legais:** Estão associados a eventos derivados de alterações legislativas ou normativas que podem comprometer as atividades da Instituição; e

- **Riscos Financeiros/Orçamentários:** Estão associados a eventos que podem comprometer a capacidade da Instituição de contar com os recursos orçamentários e financeiros necessários à realização de suas atividades, ou eventos que possam comprometer a própria execução orçamentária, com atrasos no cronograma de licitações.

Obs.: Nesta etapa, é fundamental não apenas identificar e catalogar os riscos em si, mas, também, deve-se destacar as suas causas e consequências. As causas correspondem aos elementos que podem desencadear os riscos, ou seja, tratam-se de uma análise retrospectiva, focada nos fatores que antecedem e possibilitam a ocorrência do evento. Por outro lado, as consequências refletem os principais impactos que podem resultar do risco identificado. Elas representam uma visão prospectiva, projetando os efeitos que podem surgir caso o risco se concretize.

Passo 3: Identificação e Avaliação dos Controles

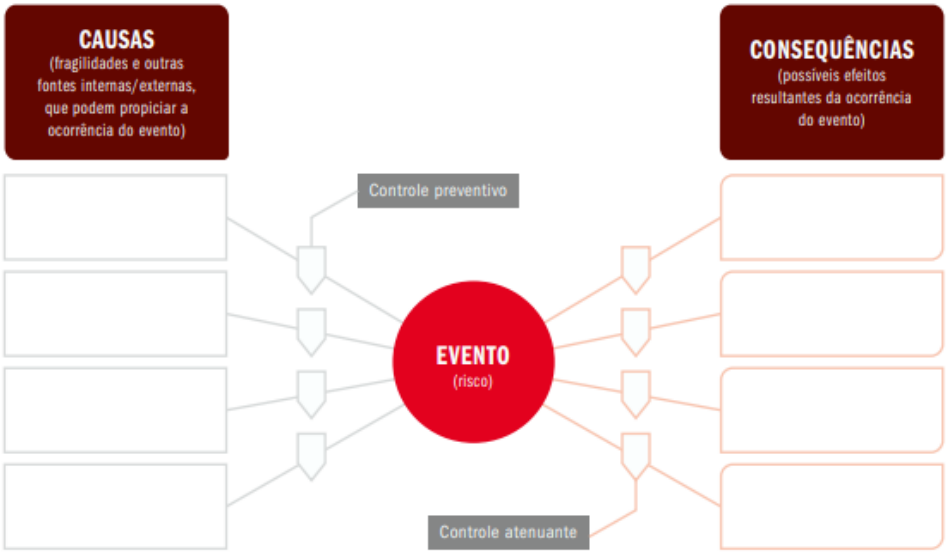
A terceira etapa do processo de gestão de riscos é a **Identificação e Avaliação dos Controles**. Esta etapa é dedicada a identificar os mecanismos de controle existentes, propor a construção de novos controles (em caso de ausência ou ineficiência) e avaliar sua eficácia na mitigação dos riscos previamente identificados. Os controles são ações ou processos implementados pela organização com o objetivo de minimizar a probabilidade de ocorrência de riscos ou reduzir seus impactos.

O principal objetivo desta fase é mapear os controles já existentes, classificá-los como preventivos ou corretivos, e avaliar se são suficientes para lidar com os riscos identificados na etapa anterior. Caso sejam considerados insuficientes, essa avaliação serve de base para o desenvolvimento de novos controles ou o aprimoramento dos existentes.

a) Tipos de controles: os controles podem ser classificados de acordo com sua função no processo de gestão de riscos:

- **Controles Preventivos:** São medidas que atuam sobre as causas do risco, buscando evitar sua ocorrência. Seu foco é antecipar-se ao evento de risco e eliminá-lo ou reduzi-lo antes que aconteça.
- **Controles Corretivos:** São medidas que atuam sobre as consequências, sendo acionados após a ocorrência do risco. Seu objetivo é minimizar os danos e restaurar a normalidade o mais rápido possível.

Nesse sentido, uma ferramenta útil é o *Bowtie*, ou gravata-borboleta. É uma metodologia e ferramenta de gestão de riscos que consiste em um diagrama que relaciona o objetivo, o risco, as suas causas e consequências, e os controles existentes. Sua formulação, conforme Referencial Básico de Gestão de Riscos do TCU, pode ser expressa da seguinte maneira:



O esquema *Bowtie* centraliza o evento de risco em análise, conectando-o às suas causas (no lado esquerdo) e às suas consequências (no lado direito). A partir dessa estrutura, são definidas

duas barreiras de controle. No lado esquerdo, encontram-se os controles preventivos, que têm como objetivo reduzir a probabilidade de ocorrência do evento, atuando diretamente sobre suas causas. No lado direito, estão os controles corretivos (ou atenuantes), que visam mitigar ou minimizar as consequências do evento, caso ele ocorra, atuando diretamente sobre suas consequências.

b) Métodos de avaliação de controles: a avaliação dos controles envolve analisar se as medidas existentes são eficazes e adequadas para reduzir os riscos a níveis aceitáveis. Alguns dos métodos utilizados incluem:

- **Análise de Eficácia:** Avaliar se o controle atinge os resultados esperados, ou seja, se realmente consegue mitigar o risco. Isso pode ser feito por meio de auditorias, testes práticos e revisões de desempenho.
- **Avaliação de Adequação:** Verificar se o controle é apropriado para o risco específico que pretende mitigar. Controles mal dimensionados ou inadequados podem não ser eficazes, mesmo se bem implementados.
- **Teste de Controles:** Aplicação de simulações ou cenários para verificar o desempenho dos controles em situações que simulam a ocorrência do risco. Isso ajuda a avaliar sua robustez e capacidade de resposta.

c) Documentação e integração do processo: durante essa etapa, todos os controles identificados e avaliados devem ser documentados de maneira clara e precisa. A documentação deve incluir:

- A descrição do controle.
- O tipo de controle (preventivo ou corretivo).
- A eficácia do controle (baseada na avaliação realizada).
- Quais áreas ou partes interessadas são responsáveis pela implementação e monitoramento do controle.
- As sugestões de melhoria para controles que se mostraram insuficientes.

Obs.: Os controles devem ser integrados ao processo de gestão de riscos de forma contínua e natural. Isso significa que os responsáveis pelo monitoramento e execução desses controles precisam estar cientes de suas funções e comprometidos com a aplicação eficaz dessas medidas. Além disso, a organização deve garantir que haja uma cultura de revisão periódica dos controles para assegurar que eles permaneçam adequados e eficazes ao longo do tempo.

Passo 4: Cálculo dos Níveis de Risco

A quarta etapa do processo de gestão de riscos é o **Cálculo dos Níveis de Risco**. Esta fase é essencial para quantificar e classificar os riscos identificados, permitindo à organização priorizar aqueles que demandam maior atenção. O cálculo dos níveis de risco é realizado combinando dois fatores principais: a **probabilidade de ocorrência** e o **impacto** do risco.

a) Mensurando probabilidade: a probabilidade de ocorrência representa a chance de um determinado risco acontecer. Esse fator pode ser medido de forma qualitativa (como "alta", "média"ou "baixa") ou quantitativa (com valores numéricos, como 1 a 5).

Uma probabilidade alta indica que o risco é mais provável de se materializar, enquanto uma probabilidade baixa sugere que o evento de risco é menos provável de ocorrer. A probabilidade pode ser classificada da seguinte forma (adaptado do Referencial Básico de Gestão de Riscos do TCU):

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

b) Mensurando impacto: o impacto, por sua vez, refere-se às consequências ou danos que o risco pode causar caso ocorra. Assim como a probabilidade, o impacto pode ser avaliado qualitativamente ou quantitativamente. Impactos altos significam que, se o risco se concretizar, os efeitos serão graves, enquanto impactos baixos indicam que as consequências seriam menores.

Os impactos podem ser financeiros, operacionais, legais ou relacionados à imagem da organização. Os impactos podem ser mensurados da seguinte maneira (adaptado do Referencial Básico de Gestão de Riscos do TCU):

IMPACTO	DESCRIÇÃO DO IMPACTO NOS OBJETIVOS, CASO O EVENTO OCORRA	PESO
Muito baixo	**Mínimo** impacto nos objetivos (estratégicos, operacionais, de informação/ comunicação/divulgação ou de conformidade).	1
Baixo	**Pequeno** impacto nos objetivos (idem).	2
Médio	**Moderado** impacto nos objetivos (idem), porém recuperável.	3
Alto	**Significativo** impacto nos objetivos (idem), de difícil reversão.	4
Muito alto	**Catastrófico** impacto nos objetivos (idem), de forma irreversível.	5

c) Nível de risco e Matriz de risco: a matriz de risco é uma ferramenta visual que auxilia na avaliação dos riscos ao cruzar os fatores de probabilidade e impacto. Ela organiza os riscos em níveis de gravidade com base em um sistema de pontuação, ou *score*, calculado multiplicando a probabilidade pelo impacto. A fórmula básica utilizada é:

$$Nível\ de\ Risco\ (Score) = Probabilidade \times Impacto \tag{1}$$

A matriz de risco é estruturada em uma tabela, onde a probabilidade de ocorrência é disposta em um eixo (geralmente no eixo horizontal) e o impacto no outro eixo (geralmente no eixo vertical). O resultado da multiplicação desses dois fatores gera um **nível de risco**, que pode ser categorizado em diferentes escalas, como:

- **Baixo:** Os riscos com menor score, geralmente considerados aceitáveis sem necessidade de ação imediata.
- **Moderado:** Riscos que demandam monitoramento e, se necessário, medidas mitigatórias adicionais.
- **Alto:** Riscos que exigem atenção prioritária e a implementação de controles para reduzir seu impacto ou probabilidade.
- **Crítico:** Riscos que requerem ações imediatas para evitar impactos severos ou inaceitáveis na organização.

A matriz de riscos pode ser ilustrado da seguinte maneira (adaptado do Referencial Básico de Gestão de Riscos do TCU):

RB (Risco Baixo)	RM (Risco Médio)	RA (Risco Alto)	RE (Risco Extremo)
0 – 4,99	5 – 11,99	12 – 19,99	20 – 25

MATRIZ DE RISCOS

IMPACTO						
Muito Alto	5	5 RM	10 RM	15 RA	20 RE	25 RE
Alto	4	4 RB	8 RM	12 RA	16 RA	20 RE
Médio	3	3 RB	6 RM	9 RM	12 RA	15 RA
Baixo	2	2 RB	4 RB	6 RM	8 RM	10 RM
Muito Baixo	1	1 RB	2 RB	3 RB	4 RB	5 RM
		Muito Baixa 1	Baixa 2	Média 3	Alta 4	Muito Alta 5
		PROBABILIDADE				

Neste exemplo, riscos com pontuação entre 1 e 5 seriam considerados de **risco baixo**, enquanto aqueles com pontuação acima de 20 seriam classificados como **risco extremo**.

d) Importância do cálculo dos níveis de risco: por meio do cálculo do nível de risco, a organização consegue:

- Priorizar os riscos com maior potencial de impacto, alocando recursos de forma eficiente;
- Compreender a gravidade de cada risco, facilitando a tomada de decisões estratégicas;
- Fornecer uma base objetiva para definir as ações necessárias na etapa seguinte, de resposta aos riscos.

Passo 5: Respostas ao Risco (Plano de Ação)

Na gestão de riscos, após a identificação e análise dos riscos, a próxima etapa é o desenvolvimento de respostas apropriadas para lidar com esses riscos. O objetivo dessa fase é reduzir a probabilidade e o impacto dos riscos negativos ou maximizar as oportunidades de eventos positivos.

a) Tipos de respostas ao risco: as respostas ao risco podem ser categorizadas nas seguintes estratégias:

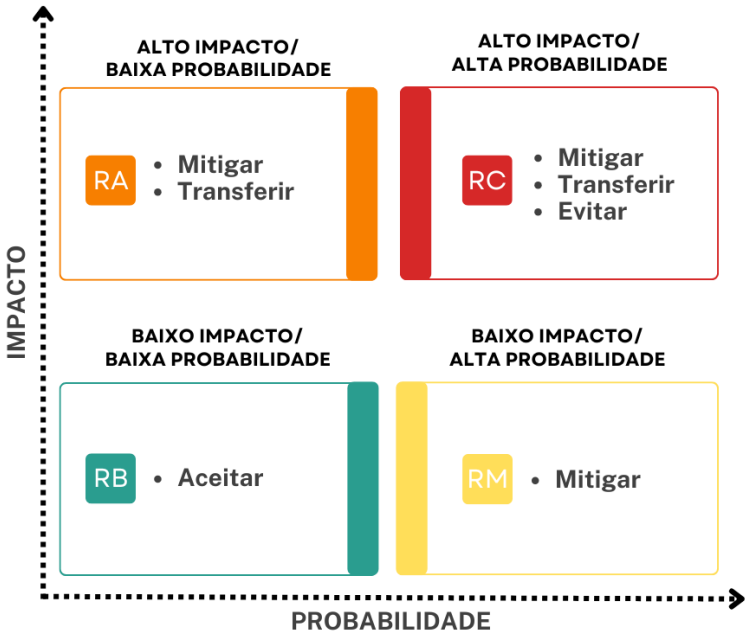
- **Aceitar**: A organização opta por aceitar o risco quando ele está dentro dos níveis toleráveis e seu impacto é considerado insignificante. Não são necessárias ações corretivas imediatas, mas o risco deve ser monitorado continuamente.
- **Mitigar**: A estratégia mais comum, que visa reduzir a probabilidade de ocorrência ou o impacto do risco. A mitigação envolve a implementação de controles preventivos e/ou corretivos, como procedimentos que possam minimizar as chances de materialização e/ou impacto do risco.
- **Transferir**: A responsabilidade pelo risco é transferida para terceiros, como através de seguros ou contratos, diminuindo o impacto na organização.
- **Evitar**: Consiste em evitar completamente o risco, o que pode implicar em modificar ou cancelar o processo que dá origem ao risco.

b) Elaboração do plano de ação: o plano de ação descreve as medidas que serão adotadas para implementar a resposta ao risco selecionada. Ele deve ser claro, garantindo que cada risco identificado tenha uma ação correspondente. As etapas incluem:

1. **Identificação da Ação a Ser Tomada**: Descrever em detalhes os controles implementados e as ações específicas que serão executadas para tratar cada risco.
2. **Definição dos Responsáveis**: Atribuir claramente os responsáveis pela implementação e monitoramento da ação. As equipes devem estar cientes de suas funções para garantir uma execução eficaz.
3. **Prazos e Recursos**: O plano de ação deve incluir prazos claros e indicar os recursos necessários para a execução, como financeiros, humanos e materiais.

A esquematização abaixo pode auxiliar na definição da resposta ao risco de acordo com o nível de risco mensurado na etapa anterior.

- Os riscos com **baixo impacto e baixa probabilidade** geralmente podem ser aceitos, pois seu efeito sobre os objetivos é mínimo e o custo para mitigá-los pode não justificar a ação.



- Riscos com **baixo impacto e alta probabilidade** devem ser mitigados, já que, embora o impacto seja pequeno, sua ocorrência frequente contribui para acumular prejuízos ao longo do tempo.
- Riscos com **alto impacto e baixa probabilidade** podem ser mitigados ou transferidos, dependendo da capacidade da organização de gerenciá-los.
- Já os riscos com **alto impacto e alta probabilidade** demandam uma resposta mais rigorosa e podem ser abordados de três formas: mitigar, transferir ou evitar completamente, dependendo da gravidade e da capacidade de gerenciamento da organização. Nesse caso, evitar pode ser a melhor opção se as consequências forem intoleráveis.

c) Critérios de sucesso: para garantir a eficácia das respostas ao risco, é fundamental definir **indicadores de desempenho**, que avaliarão o sucesso das medidas implementadas. Exemplos de indicadores incluem:

- Redução do impacto estimado;
- Diminuição da probabilidade de ocorrência do risco;
- Resposta mais rápida a incidentes.

Passo 6: Validação dos Resultados

A **validação dos resultados** é um passo essencial para garantir que o processo de gestão de riscos atenda aos seus objetivos. Ela assegura que os riscos foram tratados adequadamente e que as ações tomadas foram eficazes, proporcionando uma base sólida para a continuidade das operações da organização. Esta fase envolve a aprovação das respostas aos riscos implementadas e a análise do desempenho das ações em relação aos objetivos estabelecidos.

a) Critérios da validação: a validação tem por objetivo avaliar o processo de gestão de riscos quanto aos seguintes critérios:

- **Efetividade das Ações**: Verificar se as respostas ao risco foram implementadas conforme o plano de ação e se os controles aplicados reduziram efetivamente os níveis de risco a um patamar aceitável.
- **Eficiência na Utilização de Recursos**: Garantir que os recursos (tempo, orçamento e equipe) foram utilizados de maneira eficiente para alcançar os resultados desejados.
- **Conformidade com os Objetivos**: Confirmar que as ações tomadas estão em conformidade com os objetivos estratégicos da organização e não comprometeram outras áreas.
- **Riscos Residuais**: Avaliar se os riscos residuais, aqueles que permanecem após a aplicação das respostas, estão dentro dos níveis aceitáveis pela organização.

b) Etapas do processo de validação: o processo de validação dos resultados envolve as seguintes etapas:

1. **Revisão das Ações Implementadas**: Analisar se todas as ações planejadas foram concluídas dentro do prazo e com os recursos previstos. Avaliar o desempenho dos controles implementados na mitigação ou tratamento dos riscos.
2. **Avaliação dos Indicadores de Desempenho**: Medir a eficácia das respostas aos riscos através dos indicadores definidos, como a redução na probabilidade e impacto do risco ou a melhoria nos prazos de resposta.
3. **Monitoramento dos Riscos Residuais**: Identificar os riscos residuais que ainda permanecem após a implementação das ações e verificar se eles estão dentro dos níveis toleráveis.
4. **Aprovação pelo Gestor Responsável**: A validação final requer a aprovação do gestor do processo, que deve revisar os resultados, garantir que os riscos foram tratados de acordo com o plano e autorizar a conclusão da gestão de riscos do processo analisado.

Obs.: Após a validação dos resultados, deve-se documentar as lições aprendidas, as ações implementadas e os resultados obtidos. Esse documento serve como registro e deve ser comunicado às partes interessadas para garantir transparência no processo de gestão de riscos.

Passo 7: Comunicação e Monitoramento

A **comunicação e o monitoramento** não devem ser tratados como etapas isoladas no processo de gestão de riscos, mas como atividades contínuas e interligadas que permeiam todas as fases da gestão, desde a elaboração da política de riscos até a avaliação e tratamento dos riscos identificados.

a) Comunicação: a comunicação desempenha um papel crucial ao garantir que todas as partes interessadas estejam bem informadas sobre os riscos identificados, suas implicações e as medidas adotadas para mitigá-los. Uma comunicação eficaz permite a disseminação de informações claras e precisas sobre os riscos, facilitando a tomada de decisões em todos os níveis da organização.

Desde o início do processo de gestão de riscos, é fundamental criar canais de comunicação abertos e contínuos entre as partes envolvidas. Esses canais devem incluir:

- **Comunicação Interna**: Entre os gestores, equipes de risco e outras partes relevantes dentro da organização, assegurando que todos compreendam as ameaças e oportunidades e os planos de ação definidos.
- **Comunicação Externa**: Para informar e envolver *stakeholders* externos, como órgãos reguladores, parceiros e a sociedade, sobre os riscos que podem impactar as atividades organizacionais.

A clareza nas informações permite uma resposta ágil e alinhada ao risco, minimizando mal-entendidos e garantindo que as ações sejam coordenadas conforme necessário.

b) Monitoramento: o monitoramento é uma atividade contínua que garante que o processo de gestão de riscos esteja sendo executado de maneira eficaz ao longo do tempo. Como os riscos podem mudar, o monitoramento contínuo é essencial para detectar novas ameaças ou oportunidades e para ajustar as respostas conforme necessário.

Entre as principais atividades de monitoramento, incluem-se:

- Acompanhamento do desempenho dos controles implementados;
- Revisão periódica dos níveis de risco, avaliando se os riscos residuais continuam dentro dos níveis aceitáveis;
- Atualização das estratégias de resposta, caso sejam detectadas mudanças no contexto ou na gravidade dos riscos;
- Relatórios periódicos aos gestores, com indicadores de desempenho que demonstrem a eficácia do processo de gestão de riscos.

c) Processo contínuo e ininterrupto: tanto a comunicação quanto o monitoramento não ocorrem de forma isolada, mas são atividades integradas a todas as etapas do ciclo de gestão de riscos. A comunicação é crucial na fase de estabelecimento do contexto, onde os objetivos e os riscos são definidos, assim como na fase de resposta, garantindo que as partes interessadas estejam cientes das ações planejadas e executadas.

O monitoramento, por sua vez, deve ocorrer após a implementação das respostas aos riscos, verificando a eficácia das medidas e permitindo a revisão e correção quando necessário. Como o ambiente organizacional é dinâmico, a gestão de riscos precisa ser continuamente ajustada às novas realidades.

Ambas as atividades sustentam a eficácia de todo o processo de gestão de riscos, garantindo que ele seja atualizado, eficiente e adaptável às mudanças do contexto organizacional.

Obs.: A **comunicação** e o **monitoramento** são fundamentais para assegurar que a gestão de riscos seja um processo dinâmico e eficaz. Ao integrá-los de forma contínua e ininterrupta em todas as fases, a organização se prepara melhor para responder a novos desafios e oportunidades, garantindo a segurança e sustentabilidade de suas operações.

João Pessoa, 29 de outubro de 2024.

Gleydson Kelson Correia e Castro