MANUAL
Plano de Gestão de Riscos da UFRPE

UFRPE

Recife, 2020

UNIVERSIDADE FEDERAL RURAL DE PERNAMBUCO

MARCELO BRITO CARNEIRO LEÃO
Reitor

GABRIEL RIVAS DE MELO
Vice-Reitor

MOZART ALEXANDRE MELO DE OLIVEIRA
Pró-Reitor de Administração

MOISÉS DE MELO SANTANA
Pró-Reitor de Extensão e Cultura

MARIA DO SOCORRO DE LIMA OLIVEIRA
Pró-Reitora de Ensino de Graduação

SEVERINO MENDES DE AZEVEDO JÚNIOR
Pró-Reitor de Gestão Estudantil e Inclusão

MARIA MADALENA PESSOA GUERRA
Pró-Reitora de Pesquisa e Pós-Graduação

PATRICIA GADELHA XAVIER MONTEIRO
Pró-Reitora de Gestão de Pessoas

CAROLINA GUIMARÃES RAPOSO
Pró-Reitora de Planejamento e Desenvolvimento Institucional

FERNANDO JOSÉ DE ALBUQUERQUE
Coordenador de Gestão de Riscos

Comitê de Governança, Gestão de Riscos e Controle Interno criado conforme Portaria nº. 185/2017-GR, de 14 de fevereiro de 2017.

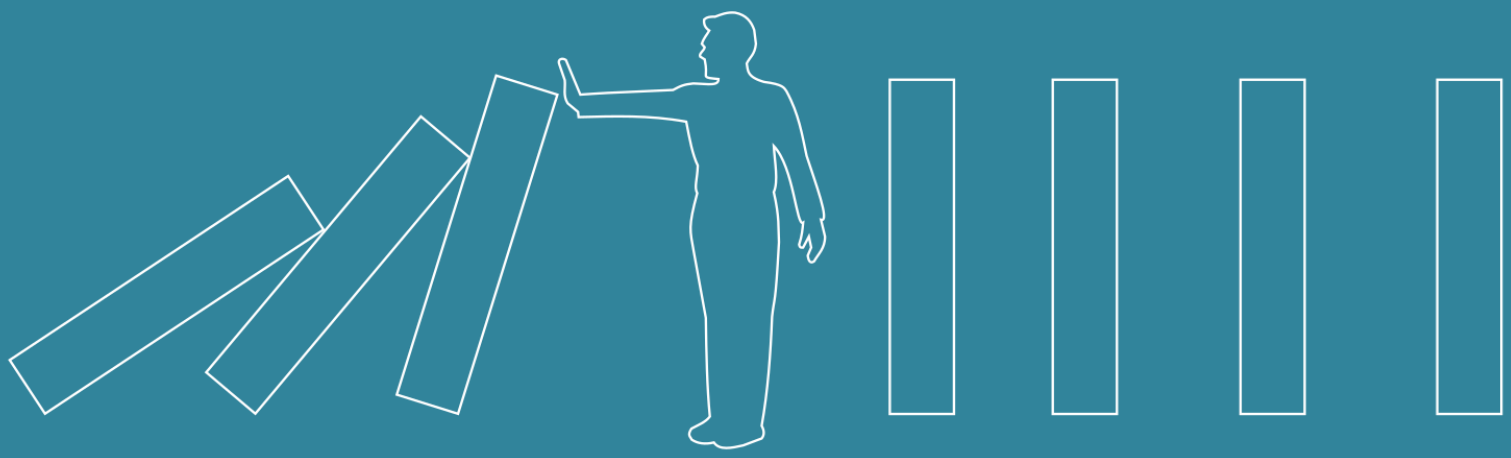
APRESENTAÇÃO

O objetivo deste manual é apresentar a Metodologia de Gerenciamento de Riscos da Universidade Federal Rural de Pernambuco.

Em conformidade com a Instrução Normativa (IN) Conjunta Nº.1, do Ministério do Planejamento, Orçamento e Gestão e da Controladoria-Geral da União, de 10 de maio de 2016, e com a Política de Gestão de Riscos (PGRiscos) da Universidade Federal Rural de Pernambuco, o Comitê de Governança, Gestão de Riscos e Controle Interno, apresenta o Plano de Gestão de Riscos da instituição.

O Plano de Gestão de Riscos tem a finalidade de especificar os controles; a estrutura; a tipologia; a criticidade; a matriz e níveis de riscos; a definição do apetite e da tolerância; e o tratamento dos riscos; bem como definir as metodologias e ferramentas necessárias ao apoio da Gestão de Riscos.

Fornece, também, diretrizes básicas acerca de boas práticas, com objetivo de despertar os gestores para a importância da gestão de riscos. Assim, é um ponto de partida que não esgota o tema, cujo aprofundamento pode ser adquirido em publicações especializadas, num processo de contínuo aprendizado.



SUMÁRIO

1. INTRODUÇÃO

Eventos que causam incertezas e venham a impactar o alcance dos objetivos estratégicos, são inerentes a qualquer organização, seja ela pública ou privada, oriundos de fatores econômicos, sociais, legais, tecnológicos, operacionais, entre outros. A gestão de riscos tem a função de assegurar que a instituição atinja seus objetivos, além de ser uma importante ferramenta para ajudar na tomada de decisões e na redução ou na eliminação de retrabalhos.

Podemos dizer que a cultura da Gestão de Riscos está em uma fase inicial nos órgãos públicos do Brasil, e que o marco regulamentar sobre o tema é a Instrução Normativa Conjunta Nº 01, de 10 de maio de 2016, do Ministério do Planejamento, Orçamento e Gestão e da Controladoria-Geral da União, que dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo Federal, bem como o Decreto nº 9.203, de 22 de novembro de 2017, que dispõe sobre a política de governança da administração pública federal, que trata, entre outros temas, da gestão de riscos na administração pública.

Desde a publicação da Instrução Conjunta MP/CGU nº 01/2016, que a UFRPE vem adotando medidas para o cumprimento dessa norma. Em 14 de fevereiro de 2017 publicou a Portaria nº 185/2017-GR, que instituiu o Comitê de Governança, Gestão de Riscos e Controle Interno, e em 04 de abril de 2017 aprovou a Política de Gestão de Riscos (PGRiscos), conforme Resolução nº 022/2017-CONSU, que tem a finalidade de identificar, avaliar, administrar, controlar e comunicar os riscos das atividades da Instituição, fornecendo, dessa forma, razoável certeza de que os objetivos da Universidade serão alcançados.

2. DOS OBJETIVOS E DOS PRINCÍPIOS DA GESTÃO DE RISCOS NA UFRPE

A UFRPE adotou os princípios e objetivos expressos na Instrução Normativa Conjunta Nº 01, de 10 de maio de 2016, do MP e CGU, conforme segue:

2.1. OBJETIVOS

I – assegurar que os responsáveis pela tomada de decisão, em todos os níveis, tenham acesso tempestivo a informações suficientes quanto aos riscos aos quais está exposta a Organização, inclusive para determinar questões relativas à delegação, se for o caso;

II – aumentar a probabilidade de alcance dos objetivos da Organização, reduzindo os riscos a níveis aceitáveis;

III – agregar valor à Organização por meio da melhoria dos processos de tomada de decisão e do tratamento adequado dos riscos e dos impactos negativos decorrentes de sua materialização.

2.2. PRINCÍPIOS

I - gestão de riscos de forma sistemática, estruturada e oportuna, subordinada ao interesse público;

II - estabelecimento de níveis de exposição a riscos adequados;

III - estabelecimento de procedimentos de controle interno proporcionais ao risco, observada a relação custo-benefício, e destinados a agregar valor à organização;

IV - utilização do mapeamento de riscos para apoio à tomada de decisão e à elaboração do planejamento estratégico; e

V - utilização da gestão de riscos para apoio à melhoria contínua dos processos organizacionais.

3. OBJETOS E ESTRUTURA DA GESTÃO DE RISCOS NA UFRPE

3.1. OBJETOS DA GESTÃO DE RISCOS

São objetos da gestão de riscos qualquer processo de trabalho, atividade, projeto, iniciativa ou ação de plano institucional, assim como os recursos que dão suporte à realização dos objetivos da UFRPE. Unidades Organizacionais também podem ser objeto da gestão de riscos.

3.2. INSTÂNCIAS DE SUPERVISÃO, LINHAS DE DEFESA E COMPETÊNCIAS

A Gestão de Riscos da UFRPE é gerida de forma integrada. A Política de Gestão de Riscos (PGRiscos) define competências específicas sobre o gerenciamento de riscos para a estrutura de governança da UFRPE.

A Gestão de Riscos na UFRPE está assim estruturada:

Figura 1: Estrutura da Gestão de Riscos na UFRPE

3.2.1. ALTA GESTÃO (REITORIA)

- Definir e atualizar as estratégias de implementação da Gestão de Riscos, considerando os contextos externo e interno;
- Definir os níveis de apetite a risco dos processos organizacionais;
- Definir os responsáveis pelo gerenciamento de riscos dos processos organizacionais;
- Definir a periodicidade máxima do ciclo do processo de gerenciamento de riscos para cada um dos processos organizacionais;
- Aprovar as respostas e as respectivas medidas de controle a serem implementadas nos processos organizacionais;
- Aprovar a Metodologia de Gestão de Riscos e suas revisões;
- Aprovar os requisitos funcionais necessários à ferramenta de tecnologia de suporte ao processo de gerenciamento de riscos;
- Monitorar a evolução de níveis de riscos e a efetividade das medidas de controle implementadas;
- Avaliar o desempenho da arquitetura de Gestão de Riscos e fortalecer a aderência dos processos à conformidade normativa;

- Garantir o apoio institucional para promover a Gestão de Riscos, em especial os seus recursos, o relacionamento entre as partes interessadas e o desenvolvimento contínuo dos servidores;
- Garantir o alinhamento da gestão de riscos aos padrões de ética e de conduta, em conformidade com o Programa de Integridade da UFRPE; e
- Supervisionar a atuação das demais instâncias da Gestão de Riscos.

3.2.2. COMITÊ DE GOVERNANÇA, GESTÃO DE RISCOS E CONTROLE INTERNO

- Auxiliar a Alta Gestão na definição e nas atualizações da estratégia de implementação da Gestão de Riscos, considerando os contextos externo e interno;
- Auxiliar na definição dos níveis de apetite a risco dos processos organizacionais;
- Auxiliar na definição dos responsáveis pelo gerenciamento de riscos dos processos organizacionais;
- Auxiliar na definição da periodicidade máxima do ciclo do processo de gerenciamento de riscos para cada um dos processos organizacionais;
- Auxiliar na aprovação das respostas e das respectivas medidas de controle a serem implementadas nos processos organizacionais;
- Avaliar a proposta de Metodologia de Gestão de Riscos e suas revisões;
- Avaliar os requisitos funcionais necessários à ferramenta de tecnologia de suporte ao processo de gerenciamento de riscos;
- Auxiliar no monitoramento da evolução dos níveis de riscos e a efetividade das medidas de controle implementadas; e
- Auxiliar na avaliação do desempenho e da conformidade legal e normativa da Gestão de Riscos.
- Gerenciamento do Plano de Gestão de riscos;
- Apoiar em todos os níveis a implementação da Gestão de Riscos na UFRPE;
- Elaboração e revisão da Política de Gestão de Riscos.

3.2.3. COORDENADORIA DE GESTÃO DE RISCOS

- Propor a Metodologia de Gestão de Riscos e suas revisões;
- Propor os requisitos funcionais necessários à ferramenta de tecnologia de suporte ao processo de gerenciamento de riscos;
- Monitorar a evolução dos níveis de riscos e a efetividade das medidas de controle implementadas;
- Dar suporte a identificação, análise e avaliação dos riscos dos processos organizacionais selecionados para a implementação da Gestão de Riscos;
- Consolidar os resultados das diversas áreas em relatórios gerenciais e encaminhá-los ao Comitê de Governança, Gestão de Riscos e Controle Interno;
- Propor capacitação continuada em Gestão de Riscos para os servidores da UFRPE, com o apoio da Alta Gestão e do Comitê de Governança;
- Medir o desempenho da Gestão de Riscos objetivando a sua melhoria contínua;
- Requisitar aos responsáveis pelo gerenciamento de riscos dos processos organizacionais as informações necessárias para a consolidação dos dados e a elaboração dos relatórios gerenciais.
- Coordenar a implantação e manutenção da PGRiscos; e
- Orientar, disseminar e promover temas que envolvam gestão de riscos.

3.2.4. GESTORES DO RISCO

- Identificar, analisar e avaliar os riscos dos processos sob sua responsabilidade, em conformidade ao que define a PGRiscos;
- Propor respostas e respectivas medidas de controle a serem implementadas nos processos organizacionais sob sua responsabilidade;
- Monitorar a evolução dos níveis de riscos e a efetividade das medidas de controles implementadas nos processos organizacionais sob sua responsabilidade;
- Informar a Coordenadoria de Gestão de Riscos (PROPLAN) sobre mudanças significativas nos processos organizacionais sob sua responsabilidade;
- Responder às requisições do Comitê de Governança, Gestão de Riscos e Controle Interno; e da Coordenadoria de Gestão de Riscos; e
- Disponibilizar as informações adequadas quanto à gestão dos riscos dos processos sob sua responsabilidade a todos os níveis da UFRPE e demais partes interessadas.

3.2.5. PROPRIETÁRIOS DO RISCO

- Monitoramento da evolução dos níveis de riscos e da efetividade das medidas de controles implementadas nos processos organizacionais em que estiverem envolvidos ou que tiverem conhecimento;
- Monitorar, no respectivo âmbito, os riscos mapeados;
- Comunicar sobre situações que envolvam risco; e
- Aplicar medidas de mitigação necessárias.

3.2.6. LINHAS DE DEFESA

Para coordenar os papéis dos atores envolvidos na Gestão de Riscos, a IN CGU/MP nº 01/2016 apresenta a estrutura de três linhas de defesa, as linhas de defesa na UFRPE estão definidas da seguinte forma:

Figura 2: Modelo de três linhas de defesa na UFRPE

I – PRIMEIRA LINHA DE DEFESA: É a gestão operacional, sendo assim, o Proprietário do Risco e o Gestor do Risco são responsáveis por manter controles internos eficazes e por conduzir procedimentos de riscos e controles diariamente. Faz parte de suas atribuições identificar, avaliar, controlar e mitigar os riscos, guiando o desenvolvimento e a implementação de políticas e procedimentos internos para garantir que as atividades estejam de acordo com as metas e objetivos.

II – SEGUNDA LINHA DE DEFESA: São as funções específicas de gerenciamento de riscos e conformidade, facilita e monitora a implementação de práticas eficazes de gerenciamento de riscos por parte do Proprietário e Gestor do Risco.

III – TERCEIRA LINHA DE DEFESA: É a Auditoria Interna, os auditores internos fornecem ao órgão de governança e à alta gestão avaliações abrangentes baseadas no maior nível de independência e objetividade dentro da UFRPE.

4. METODOLOGIA DE GESTÃO DE RISCOS

A Metodologia de Gestão de Riscos da UFRPE objetiva estabelecer e estruturar as etapas necessárias para a sua operacionalização, por meio da definição de um processo de gerenciamento de riscos.

Primeiramente, o ideal é que a Cadeia de Valor / Base de Processos e os processos da Instituição estejam mapeados. A Cadeia de Valor é a representação de modelo que permite a visão lógica dos processos organizacionais, enquanto que os Processos de Trabalho representam detalhadamente as atividades, o processamento, as entradas e saídas de cada processo. Ambos são essenciais para que a aplicação da metodologia de gerenciamento de riscos e controles internos da gestão tenha maior efetividade.

Dessa forma, a base para o gerenciamento de riscos da gestão são os processos de trabalho, o procedimento adequado é que cada Unidade Organizacional verifique quais os processos devem ser priorizados e posteriormente mapeá-los, após essa priorização a metodologia pode ser aplicada.

A metodologia é composta por cinco etapas, conforme ilustrado de forma resumida na Figura 3.

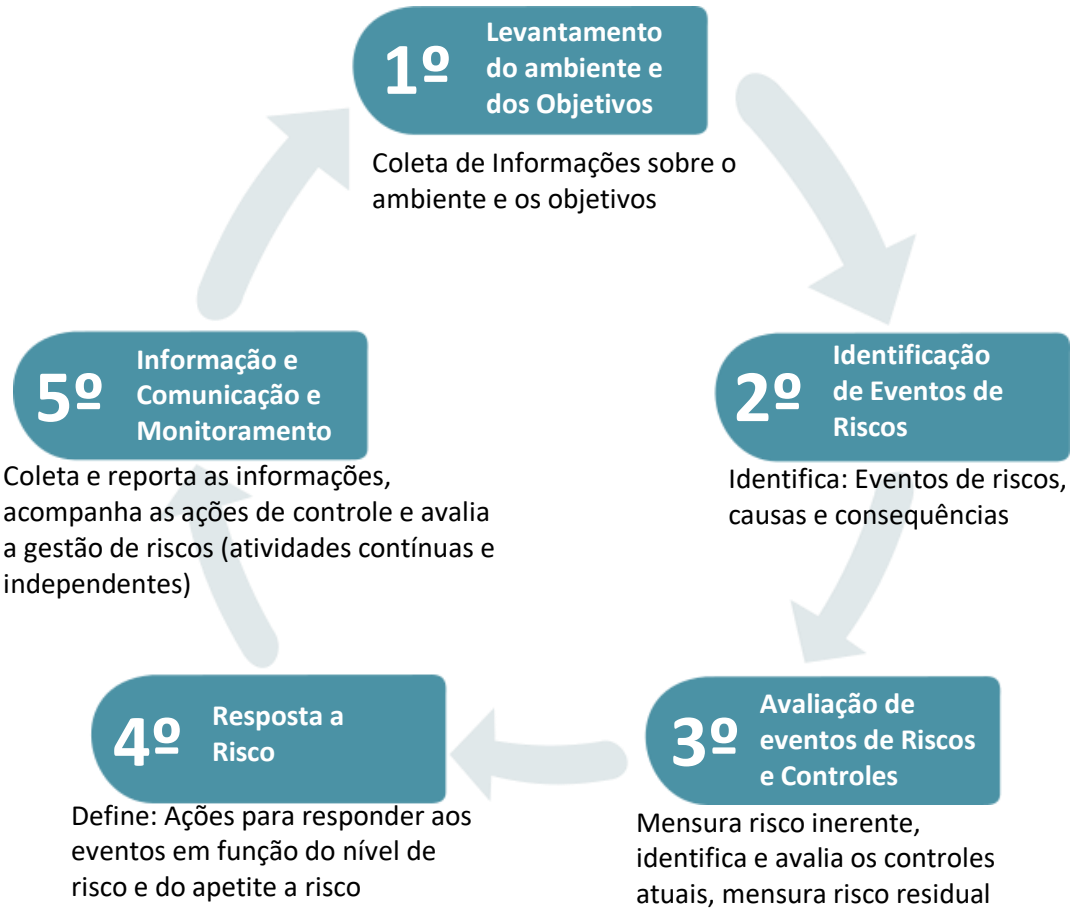


Figura 3: Metodologia e etapas do Gerenciamento de Riscos

4.1. LEVANTAMENTO DO AMBIENTE E FIXAÇÃO DE OBJETIVOS

A análise do ambiente tem a finalidade de colher informações para apoiar a identificação de eventos de riscos, bem como contribuir para a escolha de ações mais adequadas para assegurar o alcance dos objetivos do macroprocesso/processo. Podemos dizer que esta é a etapa do planejamento, da definição da missão, visão, valores e objetivos; bem como da análise dos ambientes interno e externo no que diz respeito as suas forças, fraquezas, ameaças e oportunidades; findando no levantamento das ações que serão realizadas para que os objetivos que foram determinados sejam alcançados.

Definidos pela alta gestão, os objetivos devem ser divulgados a todos os componentes da organização, antes da identificação dos eventos que possam modificá-los. Eles devem estar alinhados à missão da Organização e devem ser compatíveis com o apetite a riscos. Os objetivos de cada Unidade Organizacional da UFRPE devem estar alinhados com os objetivos estratégicos.

Nesta etapa, o processo organizacional e seus objetivos são analisados à luz de seus ambientes interno e externo.

Nesta etapa, devem ser identificados, pelo menos:

- Descrição resumida do processo. A descrição é um breve relato sobre o processo que permite compreender o seu fluxo, a relação entre os atores envolvidos e os resultados esperados;
- Fluxo (mapa) do processo organizacional;
- Objetivos do processo organizacional. É importante apontar qual ou quais objetivos são alcançados pelo processo organizacional. Sendo possível, devem ser indicados o objetivo geral e os objetivos específicos do processo, considerando perspectivas como estratégicas, temporais, relacionais, financeiras, orçamentárias, metas, entre outras. Para identificação dos objetivos, pode-se buscar responder à questão “O que deve ser atingido nas diversas dimensões para se concluir que o processo ocorreu com sucesso?”;
- Relação de Objetivos Estratégicos da UFRPE alcançados pelo processo;
- Justificativa para o gerenciamento de riscos no processo. Apresentar os motivos que levaram a implementar a gestão de riscos no processo organizacional;
- Unidade responsável pelo processo organizacional;
- Leis e regulamentos relacionados ao processo organizacional;
- Ciclo médio do processo organizacional (em dias);
- Sistemas tecnológicos que apóiam o processo organizacional;
- Partes interessadas no processo, podendo ser internas ou externas;
- Informações sobre o contexto externo do processo, considerando cenário atual ou futuro, oportunidades e ameaças relacionadas, percepções das partes interessadas externas e outros fatos relevantes;
- Informações sobre o contexto interno do processo, considerando políticas, objetivos, diretrizes e estratégias que o impactam, forças e fraquezas relacionadas, percepções das partes interessadas internas, principais ocorrências de problemas e outros fatos relevantes.

- ✓ Realizar o Planejamento da Unidade Organizacional;
- ✓ Definição da missão, visão, valores e objetivos da Unidade Organizacional. Identificar quais objetivos ou resultados devem ser alcançados;
- ✓ Análise SWOT (análise dos ambientes interno e externo no que diz respeito as suas forças, fraquezas, ameaças e oportunidades);
- ✓ Definição das ações que serão realizadas para que os objetivos que foram definidos sejam alcançados
- ✓ Identificar os processos de trabalho relevantes para o alcance dos objetivos/resultados;
- ✓ Identificar as pessoas envolvidas nesses processos e especialistas na área;
- ✓ Mapear os principais fatores internos e externos que podem afetar o alcance dos objetivos/resultados (pessoas, sistemas informatizados, estruturas organizacionais, legislação, recursos, stakeholders etc.);
- ✓ Leis e Regulamentos: listar todas as leis, regulamentos e normas que afetam ou influenciam o macroprocesso/processo. Essas informações são importantes para verificar se há riscos e descumprimento de leis, regulamentos e normas, bem como auxilia na adoção de ações de controle; e
- ✓ Sistemas: listar os sistemas e outras ferramentas (ex: planilhas) que operacionalizam o processo. Essas informações são importantes para verificar se os controles são manuais ou eletrônicos.

4.2. IDENTIFICAÇÃO DE EVENTOS DE RISCO

Esta etapa tem por finalidade identificar e registrar tanto os eventos de riscos que comprometem o alcance do objetivo do processo, assim como as causas e efeitos/consequências de cada um deles. Considere, neste momento, o resultado do **Levantamento do Ambiente e de Fixação de Objetivos**, Etapa 1.

Considerando o resultado da etapa de Entendimento do Contexto, o fluxo do processo organizacional e a partir da experiência das pessoas envolvidas no processo, deve-se construir uma lista abrangente de eventos que podem evitar, atrasar, prejudicar ou impedir o cumprimento dos objetivos do processo organizacional ou das suas etapas críticas.

Os riscos podem ser identificados a partir de perguntas, como:

- Quais eventos podem EVITAR o atingimento de um ou mais objetivos do processo organizacional?
- Quais eventos podem ATRASAR o atingimento de um ou mais objetivos do processo organizacional?
- Quais eventos podem PREJUDICAR o atingimento de um ou mais objetivos do processo organizacional?
- Quais eventos podem IMPEDIR o atingimento de um ou mais objetivos do processo organizacional?
- Os eventos identificados inicialmente podem ser analisados e revisados, reorganizados, reformulados e até eliminados nesta etapa, e, para tanto, podem ser utilizadas as seguintes questões:
  - ✓ O evento é um risco que pode comprometer claramente um objetivo do processo?
  - ✓ O evento é um risco ou uma falha no desenho do processo organizacional?
  - ✓ À luz dos objetivos do processo organizacional, o evento identificado é um risco ou uma causa para um risco?
  - ✓ O evento é um risco ou uma fragilidade em um controle para tratar um risco do processo?
- Para eventos identificados e analisados como riscos do processo, deve-se indicar:
  - ✓ Objetivo do processo organizacional/etapa impactado pelo risco;
  - ✓ Causas: motivos que podem promover a ocorrência do risco;
  - ✓ Consequências: resultados do risco que afetam os objetivos;
  - ✓ Controles preventivos: controles existentes e que atuam sobre as possíveis causas do risco, com o objetivo de prevenir a sua ocorrência. Exemplos de controles preventivos: requisitos/checklist definidos para o processo e capacitação dos servidores envolvidos no processo;
  - ✓ Controles de atenuação e recuperação: controles existentes executados após a ocorrência do risco com o intuito de diminuir o impacto de suas consequências. Exemplos de controles de atenuação e recuperação: plano de contingência; tomada de contas especiais; procedimento apuratório.

Por meio da identificação de eventos de riscos, pode-se planejar a forma de tratamento adequado e qual o tipo de resposta a ser dada a esse risco, destacando que os eventos de riscos devem ser entendidos como parte de um contexto, e não de forma isolada.
São componentes do Evento de Risco:

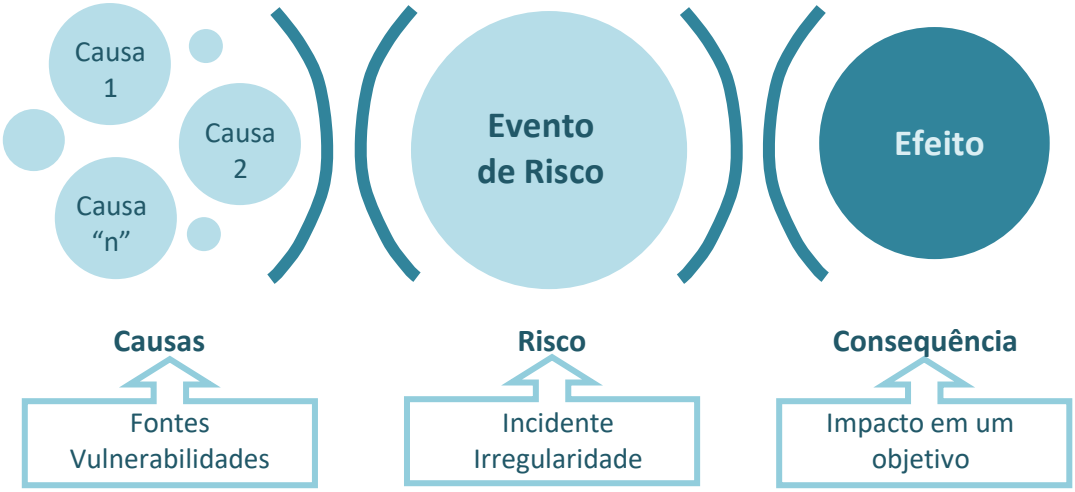


Figura 4: Componentes do evento de risco

Causas: condições que dão origem à possibilidade de um evento ocorrer, também chamadas de fatores de riscos e podem ter origem no ambiente interno e externo.

Risco: possibilidade de ocorrência de um evento que venha a ter impacto no cumprimento dos objetivos.

Consequência: o resultado de um evento de risco sobre os objetivos do processo.

O processo de identificação de riscos requer a participação de servidores com conhecimento do processo, visão holística dos serviços da unidade nos seus diferentes níveis. É importante também que tenham conhecimento da metodologia de gerenciamento de riscos.

Há diversas técnicas que podem ser utilizadas nesta etapa, para facilitar, sugerimos que seja aplicada a técnica *bow-tie,* nada impede que o grupo de trabalho responsável pelo gerenciamento de riscos da unidade venha a utilizar outra ferramenta.

O método *bow-tie* ou gravata borboleta, consiste em identificar e analisar os possíveis caminhos de um evento de risco, dado que um problema pode estar relacionado a diversas causas e consequências. Portanto, identifica-se o problema e em seguida suas possíveis causas e consequências. Para finalizar, identifique as formas de prevenir a ocorrência do risco e as formas de mitigar as consequências caso o risco se materialize. Veja a figura 5 para uma melhor compreensão.

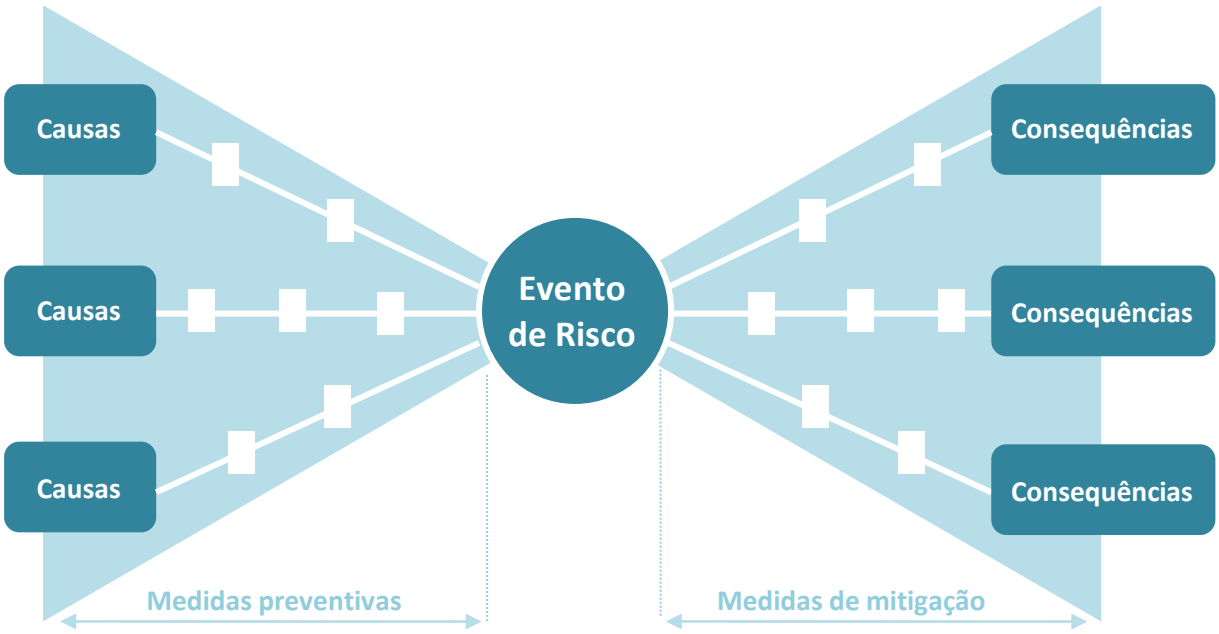


Figura 5: Método Bow-Tie

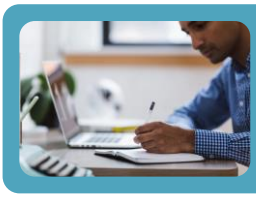
- ✓ Identificar com clareza o(s) objetivo(s)/resultado(s);
- ✓ Listar, para cada objetivo/resultado, os eventos que possam vir a ter impacto negativo no alcance do objetivo/resultado;
- ✓ Identificar os motivos que podem promover a ocorrência do risco (causa e probabilidade);
- ✓ Descrever como cada risco impacta o objetivo/resultado a ele associado (impacto e consequência);
- ✓ Responder à seguinte pergunta-chave: o que pode atrapalhar o alcance do objetivo/resultado?
- ✓ Considerar os fatores de sucesso para a consecução dos objetivos –qualquer evento que afete o fator de sucesso potencialmente afeta o objetivo/resultado;
- ✓ Considerar as principais fontes de riscos: infraestrutura, pessoal, processos e tecnologia.

A sintaxe a seguir para descrição de um evento risco poderá auxiliar no desenvolvimento desta etapa:

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

As Unidades Organizacionais, ao efetuarem o seu levantamento e identificação de riscos, deverão considerar as seguintes tipologias de riscos:

RISCOS ESTRATÉGICOS - Eventos que possam impactar na missão, nas metas ou nos objetivos estratégicos da unidade/órgão, caso venham ocorrer.



RISCOS OPERACIONAIS - Eventos que podem comprometer as atividades do órgão ou entidade, normalmente associados a falhas, deficiência ou inadequação de processos internos, pessoas, infraestrutura e sistemas.

RISCOS FINANCEIROS/ORÇAMENTÁRIOS - Eventos que podem comprometer a capacidade do órgão ou entidade de contar com os recursos orçamentários e financeiros necessários à realização de suas atividades, ou eventos que possam comprometer a própria execução orçamentária.

RISCOS DE IMAGEM/REPUTAÇÃO - Eventos que podem comprometer a confiança da sociedade (ou de parceiros, de clientes ou de fornecedores) em relação à capacidade do órgão ou da entidade em cumprir sua missão institucional.

RISCOS DE INTEGRIDADE - Eventos que podem afetar a probidade da gestão dos recursos públicos e das atividades da organização, causados pela falta de honestidade e desvios éticos.

RISCOS LEGAIS/DE CONFORMIDADE - Eventos derivados de alterações legislativas ou normativas que podem comprometer as atividades do órgão ou entidade.

RISCOS AMBIENTAIS - Resultam da associação entre os riscos naturais e os riscos decorrentes de processos naturais agravados pela atividade humana e pela ocupação do território.

Figura 6: Tipologia dos Riscos na UFRPE

4.3. AVALIAÇÃO DE EVENTOS DE RISCOS E CONTROLES

4.3.1. AVALIAÇÃO DE RISCOS

Esta etapa tem por finalidade avaliar os eventos de riscos identificados considerando os seus componentes (causas e consequências). Os eventos devem ser avaliados sob a perspectiva de PROBABILIDADE e IMPACTO, e o resultado dessas duas variáveis será o que chamamos de NÍVEL DE RISCO. As causas se relacionam à probabilidade de o evento ocorrer e as consequências ao impacto, caso o evento se materialize.

O nível de risco será avaliado de forma qualitativa e quantitativa através de uma matriz de Impacto e Probabilidade com amplitude em quatro níveis, definida em uma matriz cinco por cinco.

Podemos definir o NÍVEL DE RISCO com a seguinte equação:

NÍVEL DE RISCO = IMPACTO x PROBABILIDADE (NR = I x P)
O NÍVEL DE RISCO é o resultado da multiplicação do IMPACTO pela PROBABILIDADE.

Segue exemplo simplificado de uma avaliação de Risco:

EVENTO DE RISCO	PROBABILIDADE	IMPACTO	NÍVEL DE RISCO
Greve de docentes e técnicos administrativos	3	3	9 – RISCO ALTO
Restrição e redução orçamentária para a educação	5	5	25 – RISCO CRÍTICO

As tabelas abaixo trazem as escalas de probabilidade e impacto, respectivamente:

Tabela 1: Escala de Probabilidade

PESO	ESCALA	DESCRIÇÃO DA PROBABILIDADE
1	**RARO**	O evento ocorrerá em situações excepcionais. Não há histórico conhecido do evento ou não há indícios que sinalizem sua ocorrência.
2	**POUCO PROVÁVEL**	De forma inesperada ou casual, o evento poderá ocorrer e as circunstâncias pouco indicam essa possibilidade. Ao se analisar suas causas, conclui-se que o histórico conhecido do evento de risco, aponta para uma baixa frequência de ocorrência.
3	**PROVÁVEL**	De alguma forma, o evento poderá ocorrer, pois as circunstâncias indicam moderadamente essa possibilidade. O evento de risco repete-se com frequência razoável no prazo associado ao objetivo ou há indícios que possa ocorrer nesse horizonte.
4	**MUITO PROVÁVEL**	De forma até esperada, o evento poderá ocorrer, pois as circunstâncias indicam fortemente essa possibilidade. O evento de risco repete-se com elevada frequência no prazo associado ao objetivo ou há muitos indícios que ocorrerá nesse horizonte.
5	**PRATICAMENTE CERTO**	De forma inequívoca, o evento ocorrerá, as circunstâncias indicam claramente essa possibilidade. Ocorrência quase garantida no prazo associado ao objetivo.

Tabela 2: Escala de Impacto

PESO	ESCALA	DESCRIÇÃO DO IMPACTO
1	MUITO BAIXO	Mínimo impacto nos objetivos (sejam eles estratégicos, operacionais, de informação/comunicação, de conformidade, etc.) Compromete minimamente o atingimento do objetivo; para fins práticos, não altera o alcance do objetivo/resultado.
2	BAIXO	Pequeno impacto nos objetivos. Compromete em alguma medida o alcance do objetivo, mas não impede o alcance da maior parte do objetivo/resultado.
3	MÉDIO	Moderado impacto nos objetivos, porém recuperável. Compromete razoavelmente o alcance do objetivo/resultado.
4	ALTO	Significativo impacto nos objetivos, de difícil reversão. Compromete a maior parte do atingimento do objetivo/resultado.
5	MUITO ALTO	Catastrófico impacto nos objetivos, de forma irreversível. Compromete totalmente ou quase totalmente o atingimento do objetivo/resultado.

A partir do resultado do cálculo, o Nível de Risco pode ser classificado dentro das seguintes faixas:

Tabela 3: Classificação do Risco

CLASSIFICAÇÃO	FAIXA
Risco Pequeno - RP	quadrante >= 1 <=3
Risco Moderado - RM	quadrante >= 4 <=6
Risco Alto – RA	quadrante >= 8 <=12
Risco Crítico - RC	quadrante >= 15 <=25

A seguinte matriz representa os possíveis resultados da combinação das escalas de PROBABILIDADE e IMPACTO (matriz cinco por cinco em quatro níveis):

Tabela 4: Matriz de Risco

IMPACTO	Muito Alto 5	5 RM	10 RA	15 RC	20 RC	25 RC
	Alto 4	4 RM	8 RA	12 RA	16 RC	20 RC
	Médio 3	3 RP	6 RM	9 RA	12 RA	15 RC
	Baixo 2	2 RP	4 RM	6 RM	8 RA	10 RA
	Muito Baixo 1	1 RP	2 RP	3 RP	4 RM	5 RM
		Raro 1	Pouco Provável 2	Provável 3	Muito Provável 4	Praticamente Certo 5
		PROBABILIDADE				

4.3.2. PRIORIZAÇÃO DOS RISCOS (DO APETITE A RISCOS)

Nesta etapa, devem ser considerados os valores dos níveis de riscos calculados na etapa anterior, bem como verificar se existem controles internos e se os mesmos são eficazes, e posteriormente identificar quais riscos serão priorizados para tratamento.

A faixa de classificação do risco deve ser considerada para a definição da atitude da unidade em relação à priorização para tratamento. A tabela 5 mostra, por classificação, quais ações devem ser adotadas em relação ao risco.

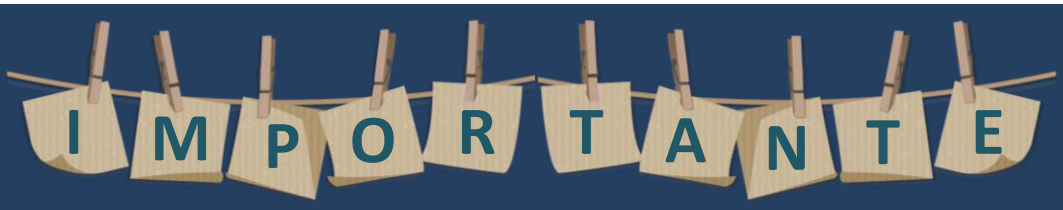
Tabela 5: Atitude perante o risco para cada classificação

CLASSIFICAÇÃO	AÇÃO NECESSÁRIA
RISCO PEQUENO	Risco que representa pequeno problema e causa pouco prejuízo, portanto controlável, devendo ser somente gerenciado por estar na zona de conforto. **Nível de risco dentro do apetite a risco**, mas é possível que existam oportunidades de maior retorno que podem ser exploradas assumindo-se mais riscos, avaliando a relação custo x benefício, como diminuir o nível de controles.
RISCO MODERADO	**Nível de risco dentro do apetite a risco.** Geralmente nenhuma medida especial é necessária, porém requer atividades de monitoramento específicas e atenção da unidade na manutenção de respostas e controles para manter o risco nesse nível, ou reduzi-lo sem custos adicionais. Risco que deve ser quantificado e monitorado de forma rotineira e sistemática, porque suas consequências são gerenciáveis, podendo também possuir planos de contingência.
RISCO ALTO	**Nível de risco além do apetite a risco.** Qualquer risco nesse nível deve ser comunicado ao Comitê de Governança e ao dirigente máximo da UFRPE e ter uma ação tomada em período determinado. Postergação de medidas só com autorização do dirigente máximo da Instituição. Pode ser tanto um risco provável, que possui alta probabilidade de ocorrência e baixo impacto na consecução dos objetivos; bem como um risco inesperado, que possui baixa probabilidade de ocorrência e alto impacto na consecução dos objetivos, também conhecido como “cisne negro”. A estas ameaças, devem-se possuir respostas rápidas ao serem detectadas, portanto, devem estar planejadas e testadas em um plano de contingência, emergência, continuidade de negócios, além de ações preventivas.
RISCO CRÍTICO	**Nível de risco muito além do apetite a risco.** Qualquer risco nesse nível deve ser objeto de Avaliação Estratégica, comunicado ao Comitê de Governança, Gestão de Riscos e Controle Interno e ao dirigente máximo da UFRPE e ter uma resposta imediata. Postergação de medidas só com autorização do Comitê de Governança, Gestão de Riscos e Controle Interno validado pelo dirigente máximo.

Tabela 6: Apetite a Riscos na UFRPE através da Matriz de Risco

IMPACTO						
	Muito Alto 5	5 RM	10 RA	15 RC	20 RC	25 RC
	Alto 4	4 RM	8 RA	12 RA	16 RC	20 RC
	Médio 3	3 RP	6 RM	9 RA	12 RA	15 RC
	Baixo 2	2 RP	4 RM	6 RM	8 RA	10 RA
	Muito Baixo 1	1 RP	2 RP	3 RP	4 RM	5 RM
		Raro 1	Pouco Provável 2	Provável 3	Muito Provável 4	Praticamente Certo 5
		PROBABILIDADE				

Riscos acima do apetite: Riscos que se encontram nas faixas LARANJA e VERMELHA, riscos que devem ser tratados.
Riscos dentro do apetite: Riscos que se encontram nas faixas VERDE e AMARELA, riscos que geralmente são aceitos e podem ser monitorados.



Apetite a Risco é o "nível de risco que a unidade está disposta a aceitar". Na UFRPE está aprovado pelo Comitê de Governança, Gestão de Riscos e Controle Interno, através deste Plano e Manual de Gestão de Riscos (vide Tabela 6).

É importante que o Apetite a Risco seja estabelecido no início do processo de gerenciamento de riscos. Uma vez definido, a unidade declara que:

- todos os riscos cujos níveis estejam dentro da(s) faixa(s) de apetite a risco podem ser aceitos, e uma possível priorização para tratamento deve ser justificada;
- todos os riscos cujos níveis estejam fora da(s) faixa(s) de apetite a risco serão devidamente tratados, e uma possível falta de tratamento deve ser justificada.
- todas as justificativas devem ser reportadas ao Comitê de Governança, Gestão de Riscos e Controle Interno e aprovadas pelo dirigente máximo da UFRPE.

OBSERVAÇÃO: A avaliação dos riscos fornece subsídios para a tomada de decisão, não se constituindo em fator determinante para eventual tratamento do risco. Ou seja, cabe ao Gestor da Unidade Organizacional em conjunto com os Gestores de Risco, diante da lista de riscos ordenados por nível de risco, decidir quais merecerão ações mitigadoras de acordo com o apetite a riscos definidos pelo Comitê de Governança, Gestão de Riscos e Controle Interno neste Plano de Gestão de Riscos. Portanto, é permitido alterar a resposta a risco, tanto para adotar uma ação onde poderia aceitar o risco e não adotar controle, como deixar de adotar uma ação onde deveria adotar uma ação de controle, tudo isso com apresentação de justificativa ao Comitê de Governança, Gestão de Riscos e Controle Interno da UFRPE, que irá se reportar a Alta Gestão da Instituição (Reitoria).

- ✓ Avaliar a probabilidade de ocorrência do risco (exemplo: um evento cuja ocorrência seja quase certa de acontecer é um evento de alta probabilidade);
- ✓ Avaliar o impacto do risco sobre o objetivo/resultado – o impacto mede o potencial comprometimento do objetivo/resultado (exemplo: um risco com potencial para comprometer um objetivo na sua totalidade ou na sua quase totalidade é considerado um risco de alto impacto);
- ✓ Definir o nível do risco com base na matriz probabilidade x impacto e na análise dos controles existentes;
- ✓ Identificar, na matriz PROBABILIDADE x IMPACTO, os riscos cujos níveis estão acima do limite de exposição a risco (apetite a riscos);
- ✓ Identificar, para os riscos acima do limite, as respectivas fontes, causas e eventuais consequências sobre a organização como um todo;
- ✓ Identificar os riscos que estão abaixo do limite de exposição (apetite a riscos) e realizar o adequado monitoramento.

4.4. RESPOSTA A RISCO

Esta etapa objetiva definir as opções e as medidas de tratamento (controles) para os riscos priorizados na etapa de Avaliação de Eventos de Riscos.

Compreende o planejamento e a realização de ações para modificar o nível do risco.

O nível do risco pode ser modificado por meio de medidas de resposta ao risco que mitiguem, transfiram ou evitem esses riscos.

Cada risco priorizado deve ser relacionado a uma opção de tratamento. A escolha da opção depende do nível do risco, conforme apresentado na tabela a seguir:

Tabela 7: Opções de tratamento do risco

TRATAMENTO	DESCRIÇÃO
MITIGAR/REDUZIR	Um risco normalmente é mitigado/reduzido quando é classificado como "Alto" ou "Crítico". A implementação de controles, neste caso, apresenta um custo/benefício adequado. Mitigar o risco significa implementar controles que possam diminuir as causas e/ou as consequências dos riscos, identificadas na etapa de Identificação e Análise de Riscos.
COMPARTILHAR	Um risco normalmente é compartilhado quando é classificado como "Alto" ou "Crítico", mas a implementação de controles não apresenta um custo/benefício adequado. Pode-se compartilhar o risco por meio de terceirização ou apólice de seguro, por exemplo.
EVITAR	Um risco normalmente é evitado quando é classificado como "Alto" ou "Crítico", e a implementação de controles apresenta um custo muito elevado, inviabilizando sua mitigação, ou não há entidades dispostas a compartilhar o risco com a UFRPE. Evitar o risco significa encerrar o processo organizacional. Nesse caso, essa opção deve ser aprovada pelo Comitê de Governança, Gestão de Riscos e Controle Interno em conjunto com a Alta Gestão.
ACEITAR	Um risco normalmente é aceito quando seu nível está nas faixas de apetite a risco (risco pequeno e risco moderado). Nessa situação, nenhum novo controle precisa ser implementado para mitigar o risco, podendo o mesmo ser monitorado.

A identificação das medidas de resposta ao risco, assim como a identificação de riscos, deve ser realizada em oficinas de trabalho ou, conforme o caso, pelo próprio Gestor do Risco e Proprietário do Risco, com a participação de pessoas que conheçam bem o objeto de gestão de riscos. Se a opção de tratamento do risco for MITIGAR, devem ser definidas medidas de tratamento para esse risco. Essas medidas devem ser capazes de diminuir os níveis de probabilidade e/ou de impacto do risco a um nível dentro ou mais próximo possível das faixas de apetite a risco (risco "Pequeno" ou "Moderado"). Para isso deve ser elaborado um **Plano de Tratamento** de gerenciamento de risco do processo organizacional.

As medidas mitigadoras podem envolver, por exemplo, a adoção de controles, o redesenho de processos, a realocação de pessoas, a realização de ações de capacitação, o desenvolvimento ou aperfeiçoamento de soluções de TI, a adequação da estrutura organizacional, entre outros.

É importante que, em uma primeira abordagem da elaboração do Plano de Tratamento, avalie-se a necessidade de melhorar ou extinguir controles já existentes. Somente depois dessa avaliação, e se ainda identificada a necessidade de redução do nível do risco, podem ser

propostos novos controles, observados sempre critérios de eficiência e eficácia da sua implementação.

- ✓ Identificar medidas de resposta ao risco;
- ✓ Avaliar se há controles e se os mesmos são eficazes;
- ✓ Responder às seguintes perguntas-chave:
  - que medidas poderiam ser adotadas para reduzir a probabilidade de ocorrência do risco?
  - que medidas poderiam ser adotadas para reduzir o impacto do risco no objetivo/resultado?
  - é possível adotar medidas para transferir o risco?
- ✓ Considerar as fontes e causas dos riscos – a princípio, as medidas devem atacar as causas do risco, de modo a reduzir a probabilidade de ocorrência, ou também podem consistir em planos de contingência que amenizem os impactos, caso o risco se concretize, ou uma combinação das duas abordagens;
- ✓ Na decisão quanto à implantação das medidas de resposta ao risco, considerar a quantidade e o nível dos riscos mitigados por cada medida, bem como o grau de redução do nível do risco gerado pela medida;
- ✓ Avaliar a viabilidade da implantação dessas medidas (custo-benefício, viabilidade técnica, tempestividade, efeitos colaterais do tratamento etc.);
- ✓ Decidir quais ações serão implementadas;
- ✓ Elaborar plano de implementação das medidas para inclusão nos planos institucionais;
- ✓ Na proposição de ações é importante instituir:
  1. Controles automatizados em substituição aos manuais, quando possível;
  2. Indicadores de desempenho: estabelecimento de indicadores (índice de rotação de pessoal, cumprimento de prazos legais, entre outros);
  3. Segregação de funções: atribuição de obrigações entre pessoas com a finalidade de reduzir risco, erro ou fraude;
  4. Limites para transações;
  5. Combinação de controles manuais e informatizados (automatizados);
  6. Políticas e procedimentos.

4.5. INFORMAÇÃO, COMUNICAÇÃO E MONITORAMENTO

Os resultados das etapas anteriores do processo de gestão de riscos (entendimento do contexto, identificação e análise dos riscos, avaliação dos riscos, priorização dos riscos e definição de respostas aos riscos) devem ser formalizados através da elaboração da **"PLANILHA DE GERENCIAMENTO DE RISCOS (Ferramenta criada e disponibilizada pela Coordenadoria de Gestão de Riscos)"** com o respectivo **"PLANO DE TRATAMENTO DE AÇÕES DE CONTROLE"**, que deverão ser avaliados e aprovados pelo **"Gestor da Unidade Organizacional"**.

Após a aprovação desses resultados, o Gestor da Unidade Organizacional e o Gestor do Risco responsável pelo processo de gerenciamento de riscos com o auxílio da PROPLAN (Coordenadoria de Gestão de Riscos) devem:

- Encaminhar esses resultados ao Comitê de Governança, Gestão de Riscos e Controle Interno;
- O Comitê de Governança, Gestão de Riscos e Controle Interno irá validar os resultados (Planilha de Gerenciamento de Riscos e Plano de Tratamento de Ações de Controle) e encaminhar para a Alta Gestão (Reitoria) para validação;
- Após a validação por parte da Alta Gestão, a **"PLANILHA DE GERENCIAMENTO DE RISCOS"** e o **"PLANO DE TRATAMENTO DE AÇÕES DE CONTROLE"** serão encaminhados aos responsáveis, neste caso os Proprietários do Risco, para que seja dado inicio as ações previstas.

A implementação do **"Plano de Tratamento de Ações de Controle"** envolve a participação da Unidade Organizacional responsável pelo processo organizacional e das unidades relacionadas como corresponsáveis em cada iniciativa, se previstas.

A responsabilidade primária pelo **"Plano de Tratamento de Ações de Controle"** permanece com a Unidade Organizacional responsável pelo processo organizacional. No Plano de Tratamento, deve ser definido o principal responsável pela implementação da iniciativa (servidor ou cargo), que também deverá monitorar e reportar a evolução das iniciativas.

O monitoramento compreende o acompanhamento e a verificação do desempenho ou da situação de elementos da gestão de riscos, podendo abranger a política, as atividades, os riscos, os planos de tratamento de riscos, os controles e outros assuntos de interesse.

O monitoramento de todo o funcionamento do ***Sistema de Gestão de Riscos*** da UFRPE está a cargo da Alta Gestão e do Comitê de Governança, Gestão de Riscos e Controle Interno com o apoio da Coordenadoria de Gestão de Riscos (PROPLAN).

O monitoramento das ações de tratamento de riscos envolve a verificação contínua ou periódica do funcionamento da sua implementação e dos resultados das medidas mitigadoras por parte do Gestor da Unidade Organizacional e do Gestor do Risco.

O monitoramento deve considerar o tempo necessário para que as medidas mitigadoras produzam seus efeitos.

O monitoramento é parte integrante do processo de gestão e de tomada de decisão e deve acompanhar o ciclo de planejamento institucional.

O monitoramento deve ser efetivo sem onerar demasiadamente o processo.

Os riscos-chave identificados serão monitorados a cada ciclo de avaliação da estratégia organizacional pelo Gestor do Risco com o auxílio da Coordenadoria de Gestão de Riscos e comunicados ao Comitê de Governança, Gestão de Riscos e Controle Interno.

O monitoramento consistirá na atualização da análise e avaliação do risco, assim como do estágio de execução das medidas de tratamento do risco e dos resultados dessas medidas.

A evolução do nível dos riscos que não mereceram tratamento (riscos pequenos e moderados) serão acompanhados pelo Gestor do Risco e Proprietário do Risco.

Todo o monitoramento deve ser encaminhado ao Comitê de Governança, as ações que não forem efetivadas devem estar justificadas no Relatório do Plano de Tratamento elaborado pelos Gestores e Proprietários do Risco. O Relatório será informado a Alta Gestão (Reitoria) através do Comitê de Governança, e ficarão a cargo da Alta Gestão as cobranças das ações não efetivadas.

OBSERVAÇÃO 1: Ao final do processo de gerenciamento de riscos, os riscos altos e críticos que afetem diretamente os objetivos estratégicos, devem ser comunicados pelo Gestor da Unidade Organizacional ao Comitê de Governança, Gestão de Riscos e Controle Interno, que irá avaliar e encaminhar à Alta Gestão (Reitoria) para que sejam tomadas as devidas providências.

OBSERVAÇÃO 2: Os riscos altos e críticos, que impactem nos objetivos estratégicos, considerados relevantes pela Alta Gestão, podem ser encaminhados ao CONSU (Conselho Universitário) através de relatório específico com as devidas justificativas. O CONSU após análise poderá incluir no planejamento de trabalho da Auditoria Interna (3ª linha de defesa), os riscos altos e críticos apontados no relatório da Alta Gestão, com a finalidade de verificar se os pontos e ações de controle definidos estão adequados, procedendo com os devidos testes de auditoria específicos.

5. CAPACITAÇÃO

O Comitê de Governança, Gestão de Riscos e Controle Interno em conjunto com a Coordenadoria de Gestão de Riscos, com o apoio de outras unidades de capacitação da UFRPE, oferecerá capacitações com o objetivo de formar ***Coordenadores Setoriais de Riscos (CSR)*** nas diversas Unidades Organizacionais, que serão multiplicadores de Gestão de Riscos na UFRPE.

Outros treinamentos sobre a aplicação da Metodologia de Gestão de Riscos podem ser solicitados pelas unidades. Os treinamentos devem ocorrer, preferencialmente, antes do início do processo de gerenciamento de riscos nos processos organizacionais da UFRPE.

Espera-se que o ***Coordenador Setorial de Risco*** atue como incentivador da gestão de riscos na sua Unidade Organizacional com os seus gestores. Essa atuação pode incluir a sugestão de processos de trabalho que devam ter seus riscos geridos, bem como o acompanhamento da evolução da gestão de riscos na Unidade e Subunidades Organizacionais e das medidas mitigadoras a cargo dos responsáveis por implementá-las. Os coordenadores exercerão o papel de interlocução entre a Coordenadoria de Gestão de Riscos e Comitê de Governança com os Gestores das Unidades Organizacionais e Gestores do Risco.

É importante ressaltar que o ***Coordenador Setorial de Risco*** será uma atividade de caráter voluntário, realizada por servidor que goste do tema Gestão de Riscos e que tenha comprometimento na sua implementação em seu setor de trabalho, lembrando que ele será um auxiliar do gestor, bem como elo de ligação com a Coordenadoria de Gestão de Riscos e o Comitê de Governança. Portanto a responsabilidade da implementação da Gestão de Risco é do gestor da Unidade Organizacional, e ele decide se indicará e terá ou não a figura do ***Coordenador Setorial de Risco.***

6. INTEGRAÇÃO DO GERENCIAMENTO DE RISCOS NAS UNIDADES ORGANIZACIONAIS

Dois dos princípios da Gestão de Riscos da UFRPE são apoiar a melhoria de seus processos organizacionais e subsidiar a tomada de decisão.

Para isso, cada Unidade Organizacional da UFRPE deve elaborar um Plano Interno de Gestão de Riscos, através da construção de um Mapa Estratégico com a identificação dos objetivos da Unidade, identificando e mapeando os principais processos que contribuem para o alcance desses objetivos (vide seção 4.1 – levantamento do ambiente e fixação de objetivos) e finalmente iniciar seu trabalho de gerenciamento de riscos de acordo com a metodologia explicada neste manual, priorizando os processos considerados mais relevantes à Unidade Organizacional.

O Gestor da Unidade Organizacional em conjunto com seus Gestores de Risco devem realizar reuniões que abordem as etapas do processo de gerenciamento de riscos. Essas reuniões devem ter a participação de servidores que conheçam os processos, seus objetivos, contextos, atores envolvidos, resultados e controles já existentes.

Além disso, é importante a participação de servidores com conhecimento acerca da Metodologia de Gestão de Riscos da UFRPE. Essas pessoas podem ser servidores que participaram da Formação de Multiplicadores em Gestão de Riscos (Coordenadores Setoriais de Risco) ou que compõem a Coordenadoria de Gestão de Riscos.

O gerenciamento de riscos deverá ser implementado de forma gradual em todas as áreas da UFRPE, iniciando no nível operacional, e conforme seu amadurecimento na Gestão de Riscos, passando para o nível tático e estratégico. Devem ser priorizados os processos e Unidades Organizacionais que impactam diretamente no atingimento dos objetivos estratégicos definidos no Plano de Desenvolvimento Institucional, essa priorização será definida pelo Comitê de Governança, Gestão de Risco e Controle Interno.

7. SÍNTESE DA METODOLOGIA DE GERENCIAMENTO DE RISCOS

SÍNTESE

1) Gestor da Unidade Organizacional reúne sua equipe para elaborar o Mapa Estratégico da Unidade;

2) Definir os objetivos e os resultados que devem ser alcançados;

3) Identificar os processos que contribuem para o alcance dos objetivos da Unidade Organizacional;

4) Elaborar um fluxo ou mapeamento dos principais processos, priorizar os mais relevantes para o atingimento dos objetivos;

5) Identificar os Gestores do Risco e Proprietários do Risco na Unidade Organizacional;

6) Com base nos objetivos e nos processos mapeados, levantar os eventos de risco que venham a impactar negativamente o alcance dos objetivos definidos no Mapa Estratégico;

7) Identificar para cada evento de risco as causas (motivos que podem promover a ocorrência do risco) e consequências (no caso do evento de risco se materializar, qual o seu impacto no objetivo);

8) Após a identificação dos eventos de risco, verificar a sua tipologia (risco estratégico, risco operacional, risco financeiro, risco de imagem, risco de integridade, risco legal ou risco ambiental);

9) Avaliar a probabilidade de ocorrência do risco;

10) Avaliar o impacto do risco sobre o objetivo/resultado – o impacto mede o potencial comprometimento do objetivo/resultado;

11) Avaliar se há controles e se os mesmos são eficazes;

12) Definir o nível do risco com base na matriz probabilidade x impacto e na análise dos controles existentes;

13) Identificar, na matriz PROBABILIDADE x IMPACTO, os riscos cujos níveis estão acima do limite de exposição a risco (apetite a riscos). Para os riscos que estão abaixo do limite de exposição (apetite a riscos) realizar o adequado monitoramento;

14) Identificar, para os riscos acima do limite, as respectivas fontes, causas e eventuais consequências sobre a organização como um todo;

15) Identificar medidas de resposta ao risco (mitigar, compartilhar, evitar), elaborar um Plano de Tratamento;

16) Após a elaboração do Gerenciamento de Riscos e do respectivo Plano de Tratamento, o Gestor da Unidade Organizacional deve comunicar esses resultados à CGRI e ao Comitê de Governança, Gestão de Riscos e Controle Interno para aprovação.

8. CONSIDERAÇÕES FINAIS

Este manual apresentou a Metodologia da Gestão de Riscos da UFRPE, que tem como principal objetivo auxiliar, sistematizar e padronizar o gerenciamento de riscos e controles internos nas unidades da Instituição, bem como contribuir para a implantação de boas práticas de Governança.

A Metodologia de Gestão de Riscos é composta pelas etapas: Levantamento do Ambiente e dos Objetivos; Identificação de Eventos de Riscos; Avaliação de Eventos de Riscos e Controles; Resposta a Riscos; e Informação, Comunicação e Monitoramento. Cada etapa visa atingir os objetivos específicos do processo de Gerenciamento de Riscos e controles internos da gestão.

A metodologia incorpora boas práticas reconhecidas, e é aderente a Instrução Normativa Conjunta CGU/MP nº 01, de 10 de maio de 2016, e à Política de Gestão de Riscos da UFRPE, estabelecida pela Resolução CONSU nº 022/2017 de 04 de abril de 2017.

Na aplicação dessa metodologia, é importante registrar, organizar, documentar e referenciar os dados e informações considerados, visando evidenciar o embasamento do resultado e subsidiar a sua aprovação pela instância competente, que neste caso é o Comitê de Governança, Gestão de Riscos e Controle Interno.

Cabe ressaltar que em qualquer iniciativa de desenvolvimento de metodologias, é fundamental a realização de ajustes para se adequar ao contexto e as necessidades da UFRPE, portanto este Manual/Plano estará sempre em avaliação e em constante processo de melhoria.

Por fim, ressalta-se que o levantamento e gerenciamento de riscos devem fazer parte dos processos das Unidades Organizacionais da UFRPE, assim, é necessário elaborar cronograma para a realização dos trabalhos, observando os prazos institucionais, e submeter às instâncias para aprovação e acompanhamento.

9. TERMOS E DEFINIÇÕES (GLOSSÁRIO)

Ação: Processo para desenvolver um projeto. Atividade para obter determinado resultado.

Accountability: Responsabilidade e Prestação de Contas. Obrigação que têm as pessoas, físicas ou jurídicas, públicas ou privadas, às quais se tenha confiado recursos públicos, de assumir as responsabilidades de ordem fiscal, gerencial e programática que lhes foram conferidas, e de informar à sociedade e a quem lhes delegou essas responsabilidades sobre o cumprimento de objetivos e metas e o desempenho alcançado na gestão dos recursos públicos. É, ainda, obrigação imposta a uma pessoa ou entidade auditada de demonstrar que administrou ou controlou os recursos que lhe foram confiados em conformidade com os termos segundo os quais eles lhe foram entregues.

Alta Gestão: Conjunto de gestores que integram o nível estratégico da organização, com poderes para estabelecer políticas, objetivos e direção geral da organização. É sinônimo de "alta direção" e de "alta administração". Abrange órgãos colegiados compostos por esses gestores (ex. "Comitê Gestor Institucional"). Como exemplos mais conhecidos de gestores de nível estratégico, podem ser citados: Ministros e Secretários de Estado, titulares de cargos de natureza especial, secretários-executivos, secretários ou autoridades equivalentes ocupantes de cargo do Grupo-Direção e Assessoramento Superiores - DAS nível seis, presidentes, diretores-gerais e secretários-gerais de tribunais, presidentes e diretores de agências nacionais, autarquias, fundações mantidas pelo Poder Público, presidentes de empresas públicas e sociedades de economia mista, bem como a diretoria executiva.

Análise de riscos: Processo de compreender a natureza e determinar o nível (magnitude, severidade) de um risco ou combinação de riscos, mediante a combinação das consequências e de suas probabilidades. A análise de riscos fornece a base para a avaliação de riscos e para as decisões sobre o tratamento de riscos.

Apetite a risco: Nível de risco que a Universidade está disposta a aceitar.

Atividades: Termo genérico utilizado para expressar operações, ações ou transações que uma organização, pessoa ou entidade realiza com vistas ao alcance de objetivos determinados, refletindo os fluxos de trabalho cotidianos que formam os processos de trabalho. É caracterizada pelos seguintes elementos: nome, descrição, diagrama de fluxo de tarefas, tarefas e respectivos responsáveis; condição para ser realizada; informações utilizadas; informações produzidas; condição para ser finalizada; e *templates* e exemplos.

Auditoria interna: A auditoria interna é uma atividade independente e objetiva de avaliação (assurance) e de consultoria, desenhada para adicionar valor e melhorar as operações de uma organização. Ela auxilia uma organização a realizar seus objetivos a partir da aplicação de uma abordagem sistemática e disciplinada para avaliar e melhorar a eficácia dos processos de gestão de riscos, controle e governança.

Avaliação de riscos: Processo de comparar os resultados da análise de riscos com os critérios de risco para determinar se o risco e/ou sua magnitude é aceitável ou tolerável.

Categoria de riscos: É a classificação dos tipos de riscos que podem afetar o alcance de seus objetivos estratégicos, observadas as características de sua área de atuação e as particularidades do setor público.

Componentes dos controles internos da gestão: são o ambiente de controle interno da entidade, a avaliação de risco, as atividades de controles internos, a informação e comunicação e o monitoramento.

Consequência: resultado de um evento que negativamente os objetivos da instituição.

Controles internos: Ações estabelecidas por meio de políticas e procedimentos que ajudam a garantir o cumprimento das diretrizes determinadas pela administração para mitigar os riscos à realização dos objetivos. Compreende o plano de organização e todos os métodos e procedimentos utilizados pela Administração e conduzidos por todos os seus agentes para salvaguardar ativos, desenvolver a eficiência nas operações, avaliar o cumprimento dos programas, objetivos, metas e orçamentos, verificar a exatidão e a fidelidade das informações e assegurar o cumprimento da lei.

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 e pelo corpo de servidores das organizações, destinados a enfrentar os riscos e fornecer segurança razoável de que, na consecução da missão da entidade, os seguintes objetivos gerais serão alcançados:

a) Execução ordenada, ética, econômica, eficiente e eficaz das operações.

b) Cumprimento das obrigações de *accountability*.

c) Cumprimento das leis e regulamentos aplicáveis.

d) Salvaguarda dos recursos para evitar perdas, mau uso e danos. O estabelecimento de controles internos no âmbito da gestão pública visa essencialmente aumentar a probabilidade de que os objetivos e metas estabelecidas sejam alcançados, de forma eficaz, eficiente, efetiva e econômica.

Dirigente máximo: Membro da alta gestão, sendo a maior autoridade administrativa do órgão ou entidade. Por exemplo: Chefes de Poderes, Presidentes dos Tribunais, Ministros de Estado, Secretário da RFB, Presidentes de Tribunais, presidentes de autarquias, comandantes militares, secretários-executivos, secretários-gerais, diretores-presidentes de estatais; reitores; presidentes de fundação e institutos; e ainda outros gestores ocupantes de cargo do Grupo-Direção e Assessoramento Superiores - DAS níveis seis e cinco.

Eficácia: Grau de alcance de metas programadas (bens e serviços) em um determinado período de tempo, independentemente dos custos implicados. O conceito de eficácia diz respeito à capacidade da gestão de cumprir objetivos imediatos, traduzidos em metas de produção ou de atendimento, ou seja, a capacidade de prover bens ou serviços de acordo com o que foi planejado.

Estratégia: O principal papel da estratégia é mapear o curso da organização para que ela navegue coesa em seu ambiente. A estratégia promove a coordenação das atividades.

Gerenciamento de Riscos: Processo para identificar, avaliar, administrar e controlar potenciais eventos ou situações, visando fornecer razoável certeza quanto ao alcance dos objetivos da organização.

Gestão: Estruturas responsáveis pelo planejamento, execução, controle, ação, enfim, pelo manejo dos recursos e poderes colocados à disposição de órgãos e entidades para a

consecução de seus objetivos, com vistas ao atendimento das necessidades e expectativas dos cidadãos e demais partes interessadas. A gestão consiste em planejar, construir, executar e monitorar atividades alinhadas com a direção estratégica estabelecida pela governança para atingir os objetivos estratégicos da organização.

Gestão de Riscos: Atividades coordenadas para dirigir e controlar uma organização no que se refere ao risco. A gestão de riscos pode ser aplicada a toda uma organização, em suas várias áreas e níveis, a qualquer momento, bem como a funções, atividades e projetos específicos.

Gestor: Profissional que exerce formalmente função de gestão em qualquer nível hierárquico da organização. Profissional da organização que tem outros profissionais formalmente subordinados a ele (ex. gerentes, supervisores, chefes).

Gestores de Riscos: Responsáveis por executar as atividades de Gestão de Riscos e coordenar esforços para identificar e estimar riscos, bem como propor melhorias necessárias para mitigar riscos, além de comunicar os resultados de análises a todos os interessados.

Governança no setor público: Compreende essencialmente os mecanismos de liderança, estratégia e controle postos em prática para avaliar, direcionar e monitorar a atuação da gestão, com vistas à condução de políticas públicas e à prestação de serviços de interesse da sociedade. É o sistema pelo qual as organizações são dirigidas e controladas. Pode ser entendido como o conjunto de ações e responsabilidades exercidas pela alta administração da empresa, órgão ou entidade, com o objetivo de oferecer orientação estratégica e garantir que os objetivos sejam alcançados, com simultânea gerência de riscos e verificação de que os recursos são utilizados de forma responsável.

Identificação de riscos: Processo de busca, reconhecimento e descrição de riscos, que envolve a identificação de suas fontes, causas e consequências potenciais. A identificação de riscos pode envolver dados históricos, análises teóricas, opiniões de pessoas informadas e de especialistas, e as necessidades das partes interessadas.

Impacto: Efeito resultante da ocorrência do evento.

Mensuração de Risco: Significa estimar a importância de um risco e calcular a probabilidade e o impacto de sua ocorrência.

Monitoramento: É um componente do controle interno que permite avaliar a qualidade do sistema de controle interno ao longo do tempo.

Objetivo: Alvo, finalidade, propósito. Os objetivos irão variar de acordo com fatores internos e externos, e podem mudar ao longo do tempo; exigindo assim um acompanhamento constante, revisões e alterações, conforme necessário.

Objetivos estratégicos: São os fins a serem perseguidos pela organização para o cumprimento de sua missão e o alcance de sua visão de futuro. Constituem elo entre as diretrizes de uma organização e seu referencial estratégico. Traduzem, consideradas as demandas e expectativas dos cidadãos, os desafios a serem enfrentados num determinado período.

Organização: As organizações são grupos estruturados de pessoas que se juntam para alcançar objetivos comuns. Surgem como resposta à necessidade dos indivíduos de alcançar metas que, isoladamente, não conseguiriam atingir, em virtude da complexidade e da variedade das tarefas inerentes ao trabalho a se efetuar. A organização formal compreende estrutura organizacional, diretrizes, normas e regulamentos da organização, rotinas e procedimentos,

enfim, todos os aspectos que exprimem como a organização pretende que sejam as relações entre os órgãos, cargos e ocupantes, a fim de que seus objetivos sejam atingidos e seu equilíbrio interno seja mantido. Em síntese, a organização formal é a determinação dos padrões de inter-relações entre os órgãos ou cargos, definidos logicamente por meio das normas, diretrizes e regulamentos da organização, para o alcance dos seus objetivos. Assim, a estrutura organizacional é um meio de que se serve a organização para atingir eficientemente seus objetivos.

Probabilidade: Possibilidade de ocorrência de um evento de risco.

Processo de gestão de riscos: Aplicação sistemática de políticas, procedimentos e práticas de gestão para as atividades de comunicação, consulta, estabelecimento do contexto, e na identificação, análise, avaliação, tratamento, monitoramento e análise crítica de riscos.

Política de gestão de riscos: Documento que contém a declaração das intenções e diretrizes gerais relacionadas à gestão de riscos e estabelece claramente os objetivos e o comprometimento da organização em relação à gestão de riscos. Não se trata de uma declaração de propósitos genérica, mas de um documento que, além de declarar os princípios, explica porque a gestão de riscos é adotada, o que se pretende com ela, onde, como e quando ela é aplicada, quem são os responsáveis em todos os níveis, dentre outros aspectos.

Projeto: Esforço temporário planejado e empreendido para criar um produto, serviço ou resultado exclusivo, mediante a realização de um conjunto de atividades inter-relacionadas ou interativas, com início e término bem definidos.

Transparência: Caracteriza-se pela possibilidade de acesso a todas as informações relativas à organização pública, sendo um dos requisitos de controle do Estado pela sociedade civil. A adequada transparência resulta em um clima de confiança, tanto internamente quanto nas relações de órgãos e entidades com terceiros. A organização transparente se obriga voluntariamente à divulgação oportuna de todas as questões relevantes a ela relacionadas, inclusive situação financeira, desempenho, composição e governança da organização. Há transparência nas informações, especialmente nas de alta relevância, que impactem os negócios e que envolvam resultados, oportunidades e riscos. A transparência deve situar-se dentro dos limites de exposição que não sejam conflitantes com a salvaguarda de informações que justificadamente devam ser protegidas. Transparência ativa é a promoção, por parte dos órgãos e entidades, independentemente de requerimentos, da divulgação de informações de interesse coletivo ou geral por eles produzidas ou custodiadas, em local de fácil acesso, no âmbito de suas competências.

Tratamento de riscos: Consiste em selecionar e implementar uma ou mais opções de resposta a riscos para modificar os níveis de risco. Definição das ações para reduzir a probabilidade de ocorrência dos eventos ou suas conseqüências.

Unidade organizacional: Designa-se a um segmento organizacional destinado para o desempenho de atividade especifica, dentro de uma determinada Organização.

10. REFERÊNCIAS BIBLIOGRÁFICAS

ABNT. **Gestão de Riscos – Princípio e diretrizes.** NBR ISO 31000. Associação Brasileira de Normas Técnicas. 2009.

IBGC, **Guia de Orientação para Gerenciamento de Riscos Corporativos**.

BRASIL. **Instrução Normativa Conjunta MP/CGU Nº 01**, de 10 de maio de 2016, que estabelece a adoção de uma série de medidas para a sistematização de práticas relacionadas a gestão de riscos, controles internos e governança.

BRASIL. Ministério do Planejamento, Desenvolvimento e Gestão. Assessoria Especial de Controles Internos. **Manual de Gestão de Integridade, Riscos e Controles Internos da Gestão.** Brasília. 31/01/2017.

BRASIL. Ministério da Transparência e Controladoria-Geral da União. **Metodologia de Gestão de Riscos**. Brasília. Abril de 2018.

BRASIL. Tribunal de Contas da União. **Manual de Gestão de Riscos do TCU**. Segepres/Seplan. Brasília. Maio de 2018.

COSO. *Committee of Sponsoring Organizations of the Treadway Commission*. **Gerenciamento de Riscos Corporativos – Estrutura Integrada**. 2007. Tradução: Instituto dos Auditores Internos do Brasil (Audibra) e *Pricewaterhouse Coopers Governance, Risk and Compliance*, Estados Unidos da América, 2007.

MIRANDA, Rodrigo Fontenelle de A.; BRASIL. **Implementando a Gestão de Riscos no Setor Público**. Editora Fórum. 2017.