Relatório de Auditoria - Consultoria em Gestão de Riscos

2020

RELATÓRIO DE AUDITORIA Nº 03/2020: Consultoria

Relatório de Auditoria como atividade de consultoria do processo nuclear Gerir Riscos

JOÃO PESSOA
2020

UNIDADE DE AUDITORIA INTERNA GOVERNAMENTAL DO IFPB

Missão

Desempenhar uma atividade independente e objetiva de avaliação e consultoria desenhada para adicionar valor e melhorar as operações do Instituto Federal da Paraíba, buscando auxiliá-lo a realizar seus objetivos, através da aplicação de uma abordagem sistemática e disciplinada, para avaliar e melhorar a eficácia dos processos de governança, de gerenciamento de riscos e de controles internos.

Visão

Ser reconhecida, em longo prazo, no Brasil, como órgão de excelência competente pela avaliação e consultoria dos controles internos, da governança e da gestão de risco contribuindo para o fortalecimento da gestão e para o desenvolvimento institucional.

Valores

I) Comportamento ético;
II) Cautela e zelo profissional;
III) Independência;
IV) Imparcialidade;
V) Objetividade;
VI) Conhecimento técnico e capacidade profissional;
VII) Atualização dos conhecimentos técnicos;
VIII) Cortesia;
IX) Intransferibilidade de Funções;
X) Sigilo e Discrição;
XI) Responsabilidade;
XII) Interesse Público;
XIII) Comunicação eficaz;
XIV) Alinhamento com as estratégias, objetivos e riscos da organização;
XV) Atuação respaldada na eficiência, eficácia, efetividade e economicidade;
XVI) Controle de qualidade; e
XVII) Transparência dos resultados.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DA PARAÍBA

Relatório de Auditoria - Gerir Riscos

Natureza da Auditoria
Consultoria

Período de abrangência
2020

Unidade
Diretoria de Planejamento Institucional

Responsáveis
Cícero Nicácio do Nascimento Lopes – Reitor
Elaine Pereira de Brito – Diretora de Planejamento Institucional

Relatório nº
03/2020

Equipe de Trabalho
Kléber Cordeiro Costa - Auditor Interno
Bruno Rodrigues Cabral - Auditor Geral

JOÃO PESSOA
2020

Sumário

Introdução

Em 2019, a Unidade de Auditoria Interna Governamental - UAIG do IFPB realizou avaliação do processo Gerir Riscos, emitindo o relatório de Auditoria n. 03/2019. Esta ação tinha como objetivo avaliar o grau de maturidade da gestão de riscos do IFPB.

Ao término da ação de avaliação, a UAIG expediu 19 recomendações de melhorias inerentes ao processo de gestão de riscos. Vislumbrou-se, portanto, a oportunidade de realização de um serviço de consultoria, que visa o aperfeiçoamento dos processos de governança, de gerenciamento de riscos e a implementação de controles internos na organização.

Gerir Riscos está previsto como processo nuclear de suporte no sistema PLANEDE, sob a gerência da Diretoria de Planejamento Institucional - DPI. Definiu-se, em conjunto com a referida Diretoria, como expectativas para esta ação de consultoria o foco na disseminação da cultura de riscos em todos os níveis do IFPB, compreendida como medida basilar para o aperfeiçoamento da gestão de riscos como um todo na organização.

Para tanto, a UAIG realizou análises de processos de gestão de riscos de outras organizações públicas, a exemplo do Ministério do Planejamento - MP, Tribunal de Contas da União - TCU, Controladoria Geral da União - CGU, Tribunal Superior do Trabalho - TST, Instituto Nacional da Propriedade Industrial - INPI e da Agência Nacional de Saúde Suplementar - ANS. Procedeu, ainda, à revisão dos instrumentos da gestão de riscos no IFPB.

Após a análise das experiências de outros órgãos em comparação com a situação atual do IFPB, e a expectativa desta ação de consultoria, definiu-se os seguintes eixos para a ação de consultoria:

1. Elaboração de proposta de Manual de Gestão de Riscos compilando as experiências dos outros órgãos com as definições da Política de Gestão de Riscos do IFPB delineadas na Portaria 2025/2017-Reitoria e no sistema PLANEDE;
2. Revisão do processo de Gestão de Riscos do IFPB; e
3. Ação de capacitação dos membros do Comitê de Gestão de Riscos.

Objetivo

A presente ação de consultoria tem como objetivo identificar oportunidade de melhoria no processo de Gestão de Riscos, especificamente quanto ao aumento do entendimento das pessoas da organização sobre suas responsabilidades no gerenciamento de risco.

Do Manual de Gestão de Riscos

Realizando análise nas experiências de gestão de riscos em outros órgãos da Administração Pública, constatou-se a frequente adoção de manual de gestão de riscos que compilasse, pelo menos, os conceitos básicos, o processo da gestão de riscos e a estrutura organizacional envolvida.

Um manual de procedimentos é um eficiente instrumento de controle interno uma vez que condensa as informações mais relevantes para determinado assunto, permitindo, assim, a implementação mais difusa e uniforme na organização.

Como o objetivo chave desta ação de consultoria é a disseminação da cultura de riscos em todos os níveis do IFPB, a propositura de um modelo de manual de gestão de riscos demonstra-se como uma medida eficiente para alcance amplo na instituição.

Serviram de orientação para a elaboração da proposta de Manual de Gestão de Riscos as seguintes experiências e órgãos da Administração Pública:

1. Manual de Gestão de Integridade, Riscos e Controles Internos da Gestão, do Ministério do Planejamento, Desenvolvimento e Gestão - MP;
2. Manual de Gestão de Riscos do TCU;
3. Plano de Gestão de Riscos da Secretaria do Tribunal Superior do Trabalho - TST;
4. Manual de Gestão de Riscos do INPI;
5. Manual de Gestão de Riscos da Agência Nacional de Saúde Suplementar;
6. Referencial Básico de Gestão de Riscos do TCU; e
7. Metodologia de Gestão de Riscos da CGU.

É preciso ressaltar, entretanto, que o manual ora proposto não tem qualquer caráter vinculativo, cabendo a gestão adotá-lo ou não bem como modificá-lo às suas necessidades.

Da Revisão do Processo de Gestão de Riscos

O segundo eixo desta ação de consultoria consiste na revisão do processo de gestão de riscos. As recomendações resultantes desta revisão estão contidas na proposta do Manual de Gestão de Riscos.

Na formulação da proposta de Manual de Gestão de Riscos, bem como considerando as recomendações emitidas na ação de avaliação executada no processo Gerir Riscos, constatou-se a necessidade de propor medidas diversas daquelas registradas nos documentos da gestão de riscos do IFPB. Merecem destaque os pontos a seguir.

Apetite a Risco

A declaração de apetite a riscos presente no sistema PLANEDE determina:

> Para fins de aplicação ao PLANEDE 2025, adota-se um apetite ao risco único, aqui declarado formalmente como "nulo apetite ao risco" para toda a instituição, consubstanciado nos parâmetros de forte exposição do IFPB a riscos relacionados a requisitos legais (e.g., leis, políticas, regulamentações, contratos) e dependência umbilical de orçamento público federal para o funcionamento (e.g., despesa com pessoal, expansão de oferta de vagas), fazendo com que se internalize o uso de controles que sejam rígidos em busca de prevenir perdas e assim fomentar um estilo de gestão institucional em "estado de alerta" em cada tomada de decisão para o alcance dos objetivos estratégicos.

O apetite a risco é o nível de risco que uma organização está disposta a aceitar. Não deve, contudo, ser compreendido como a anuência com o resultado do risco, mas sim como uma aceitação de perseguir determinados objetivos mesmo considerando um determinado grau de exposição a riscos.

Da forma que está declarado o apetite a riscos do IFPB, nenhuma atividade, processo ou objetivo deve ser assumido ou continuado uma vez que não há risco nulo. Há sempre algum risco residual, independente da sua probabilidade, de seu impacto e dos níveis de controle.

Diante disso, a proposta do manual considera a necessidade de determinação do apetite a riscos diferente da proposta no PLANEDE de apetite nulo.

Comitê de Gestão de Riscos na 3ª Linha 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 da seguinte forma:

- 1ª linha de defesa: controles internos da gestão executados por todos os agentes públicos responsáveis pela condução de atividades e tarefas, no âmbito dos macroprocessos finalísticos e de apoio;
- 2ª linha de defesa: supervisão e monitoramento dos controles internos executados por instâncias específicas, como comitês, diretorias ou assessorias específicas para tratar de riscos, controles internos, integridade e compliance;
- 3ª linha de defesa: constituída pelas auditorias internas no âmbito da Administração Pública, uma vez que são responsáveis por proceder à avaliação da operacionalização dos controles internos da gestão (primeira linha ou camada de defesa) e da supervisão dos controles internos (segunda linha ou camada de defesa).

O documento SGE004 - Governança, Risco e Compliance (GRC), presente no sistema PLANEDE e que detalha a gestão de riscos na instituição aloca o Comitê de Gestão de Riscos na mesma camada de defesa da Unidade de Auditoria Interna ao mesmo tempo que a Política de Gestão de Riscos determina que o referido Comitê tem a responsabilidade primária pelo processo de Gestão de Riscos.

O Referencial Básico de Gestão de Riscos do TCU aponta que a 3ª linha de defesa fica a cargo de órgãos que fornecem avaliações independentes.

> **Funções que fornecem avaliações independentes**: a auditoria interna constitui a terceira linha de defesa na gestão de riscos ao fornecer avaliações (asseguraçõ̃es) independentes e objetivas sobre os processos de gestão de riscos, controles internos e governança aos órgãos de governança e à alta administração. Tais avaliações devem abranger uma grande variedade de objetivos (incluindo eficiência e eficácia das operações; salvaguarda de ativos; confiabilidade e integridade dos processos de reporte; conformidade com leis e regulamentos) e elementos da estrutura de gestão de riscos e controle interno em todos os níveis da estrutura organizacional da entidade.

Considerando as atribuições de supervisão da gestão de riscos por parte do Comitê de Gestão de Riscos, na proposta do Manual compreendeu-se como este sendo um órgão da 2ª linha de defesa.

Das demais análises

Os demais resultados da revisão do processo de gestão de riscos não carecem de mais fundamentações que não as já declaradas no próprio corpo da proposta do Manual de Gestão de Riscos, que faz parte deste relatório.

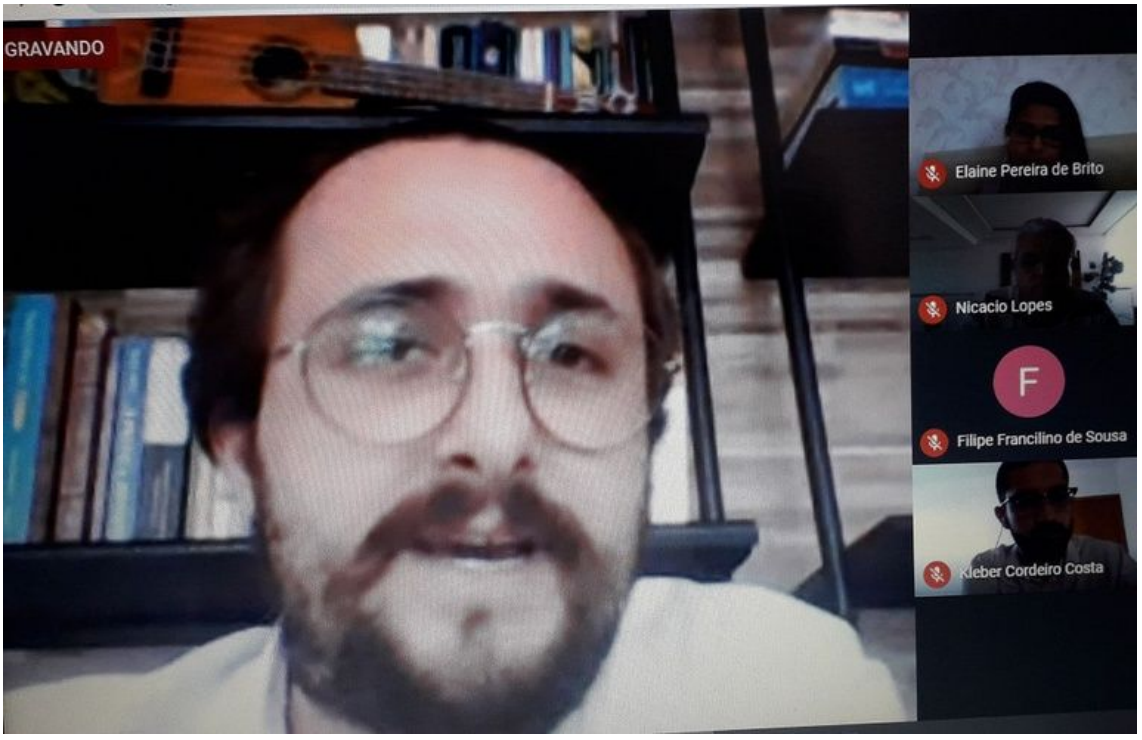
Da Ação de Capacitação dos Membros do Comitê de Gestão de Riscos

Segundo a Política de Gestão de Riscos do IFPB o processo de gestão de risco do IFPB é de responsabilidade primária do Comitê de Gestão de Riscos. Tendo o Comitê papel chave na condução de qualquer medida de disseminação da cultura de riscos na instituição, vislumbrou-se a necessidade de direcionamento da ação de capacitação aos seus membros, de forma a possibilitar um entendimento inicial sobre a importância da gestão de riscos bem como sobre conceitos chaves, para que se possa facilitar a adoção de iniciativas de disseminação da cultura de riscos para toda a instituição.

A referida ação de capacitação foi realizada no dia 27 de agosto de 2020, das 14h às 18h, remotamente via plataforma Google Meet. No evento foram explanados conceitos básicos da gestão de riscos e apresentada a minuta do manual de gestão de riscos bem como foi demonstrado o preenchimento da planilha de gestão de riscos anexa ao manual.

Matéria publicada no sítio eletrônico do IFPB:
https://www.ifpb.edu.br/noticias/2020/08/gestores-realizam-capacitacao-sobre-gerenciamento-de-crise

Imagem 1. Auditor Geral apresentou a ação de consultoria e abordou conceitos da gestão de riscos.

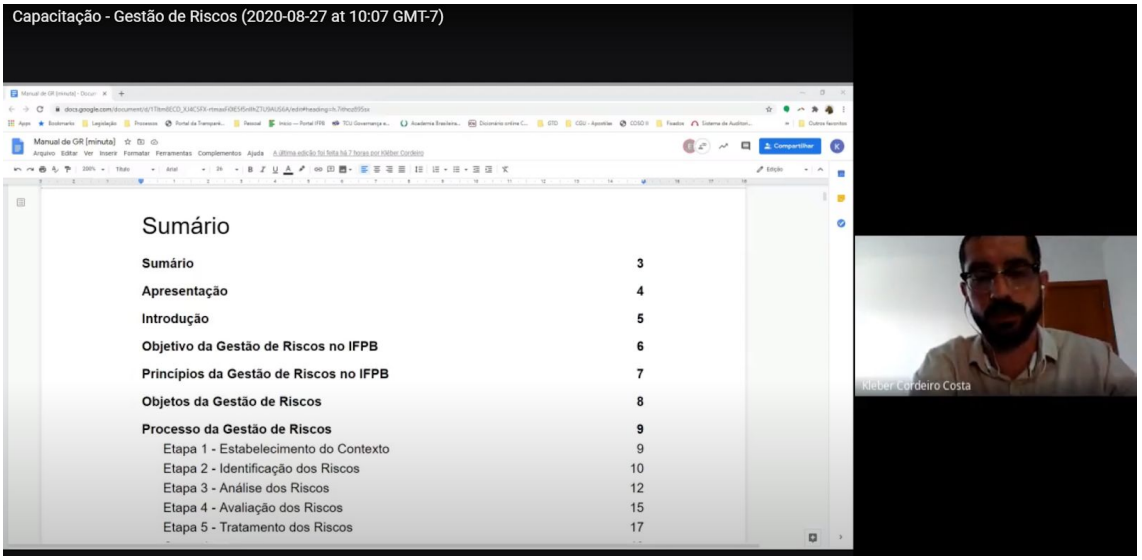


Fonte: Elaboração própria (2020) a partir da reunião realizada através do Google Meet.

Imagem 2. Magnífico Reitor realizou a abertura do evento.

Fonte: Elaboração própria (2020) a partir da reunião realizada através do Google Meet.

Imagem 3. Apresentação da minuta do manual de gestão de riscos.



Fonte: Elaboração própria (2020) a partir da reunião realizada através do Google Meet.

Como encaminhamentos da referida reunião definiu-se a Unidade de Auditoria Interna remeteria ao Comitê de Gestão de Riscos, por intermédio da Diretoria de Planejamento Institucional, a Minuta do Manual e a gravação da reunião.

Plano de ação pactuado

Conforme relatado, a participação da equipe da Unidade de Auditoria Interna encerrou-se no dia 27/08/2020 com a ação de capacitação dos membros do Comitê de Gestão de Riscos. Após essa data, as ações necessárias para a continuidade do trabalho passaram a ser coordenadas pelas equipes da Diretoria de Planejamento Institucional, do Comitê de Gestão de Riscos bem como do Comitê de Governança, Integridade, Riscos e Controles (GIRC) do IFPB.

Dessa forma, no sentido de guiar a execução dos trabalhos e permitir um acompanhamento por parte da UAIG-IFPB, foi pactuado um Plano de Ação prevendo as atividades a serem executadas após o encerramento da participação da equipe da UAIG-IFPB.

O referido Plano de Ação prevê, de modo geral, as seguintes atividades (detalhadas no próprio documento):

- Deliberação e aprovação de manual de gestão de riscos (21/10/2020);
- Disseminação do manual de gestão de riscos ao servidores (após aprovação)

Conclusão

O amadurecimento da gestão de riscos no IFPB irá favorecer o alcance dos objetivos da instituição e permitirá otimização de recursos públicos na elaboração de controles internos cada vez mais eficientes e adequados aos riscos geridos.

Espera-se que a adoção de instrumentos hábeis a disseminar a gestão de riscos entre os diversos níveis da organização, a exemplo do manual de gestão de riscos, tenha se tornado uma realidade mais aplicável após a realização desta ação de consultoria em soma de esforços com a gestão, na figura da Diretoria de Planejamento Institucional e do Comitê de Gestão de Riscos do IFPB.

João Pessoa, 22/12/2020

Bruno Rodrigues Cabral
Matrícula 1115863

Kléber Cordeiro Costa
Matrícula 2736382

Manual de Gestão de Riscos do IFPB

Instituto Federal de Educação, Ciência e Tecnologia da Paraíba

Reitor
Cícero Nicácio do Nascimento Lopes

Comitê de Gestão de Riscos

Elaboração:

Colaboração:

Sumário

Apresentação

O objetivo deste manual é apresentar, de forma sintética, os conceitos e princípios que norteiam a Gestão de Riscos no IFPB, além de servir como guia para os agentes e gestores na realização do processo de avaliação de riscos. Tem por finalidade orientar a identificação, a avaliação e a adoção de respostas aos eventos de riscos dos processos da unidade bem como instruir sobre o monitoramento e reporte.

A proposta do manual é que o gestor possa encontrar, de maneira rápida e simples, tudo o que precisa para compreender o assunto em um só documento.

A expectativa é que este Manual atenda às necessidades dos gestores e colaboradores, auxiliando-os a controlar e mitigar riscos e contribuindo para a melhoria dos processos internos, fazendo com que o processo de gestão de riscos seja incorporado à cultura do IFPB.

Inicialmente, até que seja desenvolvido sistema específico para a gestão de riscos, a aplicação poderá ser realizada por meio de planilha, parte integrante deste Manual.

Introdução

A incerteza ou o risco é inerente a praticamente todas as atividades humanas. Uma das funções da gestão de riscos é assegurar o alcance dos objetivos, por meio da identificação antecipada dos possíveis eventos que poderiam ameaçar o atingimento dos objetivos, o cumprimento de prazos, leis e regulamentos etc, e, implementar uma estratégia evitando o consumo intenso de recursos para solução de problemas quando estes surgem inesperadamente, bem como a melhoria contínua dos processos organizacionais. Independentemente da área em que se atua, e até na vida pessoal, os riscos (ameaças ou oportunidades) podem afetar o andamento da ação, levando-a a uma direção completamente diferente daquela inicialmente planejada.

A iniciativa de implantar a gestão de riscos no setor público é relativamente recente no Brasil. Nesse contexto, é importante lembrar a Emenda Constitucional nº 19, de 1998, que acrescentou o conceito da eficiência no rol dos princípios que regem toda a administração pública federal (CF, art. 37, caput). O objetivo principal da gestão de riscos é aumentar o grau de certeza na consecução dos objetivos, o que tem impacto direto na eficiência.

O Ministério do Planejamento, Desenvolvimento e Gestão (MP), Ministério da Transparência e Controladoria-Geral da União (CGU) expediram, em 2016, a Instrução Normativa Conjunta nº 01, que dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo Federal. O MP lançou, em 2017, o Manual de Gestão de Integridade, Riscos e Controles Internos da Gestão.

Ainda em 2017, foi editado 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.

A gestão de riscos é um importante instrumento de apoio para garantir que os eventos identificados com potencial impacto negativo sobre a atividade ou processo sejam tratados de forma apropriada e tempestiva de modo a não prejudicar o atingimento dos objetivos ou metas institucionais. Portanto, ela pode e deve ser aplicada a toda a organização (ou em todos os processos e atividades do IFPB).

Objetivo da Gestão de Riscos no IFPB

A gestão de riscos no IFPB tem como objetivo auxiliar a tomada de decisão, com vistas a prover razoável segurança no cumprimento da missão e no alcance dos objetivos institucionais.

Não considerar explicitamente os riscos na tomada de decisões pode acarretar o não alcance dos objetivos ou resultados que poderiam ser atingidos.

Conceitos Básicos
Risco – possibilidade de que um evento afete negativamente o alcance dos objetivos.
Oportunidade – possibilidade de que um evento afete positivamente o alcance de objetivos.

Princípios da Gestão de Riscos no IFPB

Conforme a Política de Gestão de Riscos do IFPB, que absorve as definições da Instrução Normativa Conjunta MP-CGU nº 1, de 10 de maio de 2016 , são os seguintes os princípios que regem a gestão de riscos no IFPB.

- Gestão de riscos de forma sistemática, estruturada e oportuna,subordinada ao interesse público;
- Estabelecimento de níveis de exposição a riscos adequados;
- Estabelecimento de procedimentos de controle interno proporcionais ao risco, observada a relação custo-benefício, e destinado a agregar valor à organização;
- Utilização do mapeamento de riscos para apoio à tomada de decisão e à elaboração do planejamento estratégico; e
- Utilização da gestão de riscos para apoio à melhoria contínua dos processos organizacionais.

Objetos da Gestão de Riscos

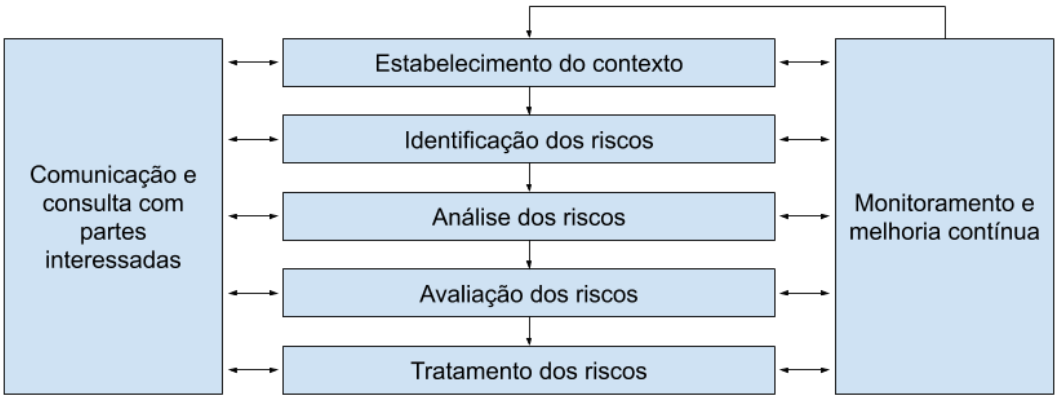
São objetos da gestão de riscos qualquer **processo de trabalho**, **atividade**, **função**, **projeto**, **iniciativa** ou **ação de plano institucional**, assim como os recursos que dão suporte à realização dos objetivos do IFPB. Unidades organizacionais também podem ser objeto da gestão de riscos.

Processo da Gestão de Riscos

Após a definição do processo a ser trabalhado, da definição da equipe responsável com seus papéis e responsabilidades, da identificação das partes intervenientes/interessadas no processo, são realizadas as etapas a seguir:

1. Estabelecimento do contexto;
2. Identificação dos riscos;
3. Análise dos riscos;
4. Avaliação dos riscos;
5. Tratamento dos riscos;
6. Monitoramento; e
7. Melhoria contínua.

O processo de gestão de riscos pode ser visualizado na figura abaixo.



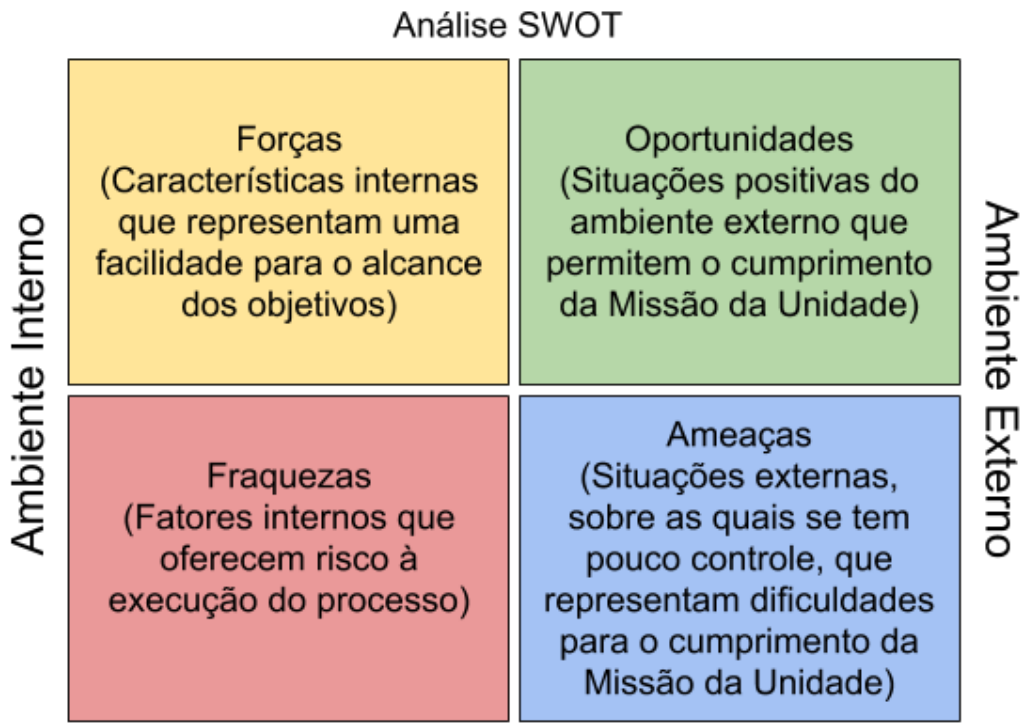
Etapa 1 - Estabelecimento do Contexto

Consiste em **compreender** o **ambiente externo** e **interno** no qual o objeto de gestão de riscos se encontra inserido e em identificar parâmetros e critérios a serem considerados no processo de gestão de riscos. A definição desses fatores servirá de insumo à atuação das demais atividades que compõem este manual.

O estabelecimento do contexto deve seguir os seguintes passos:

- identificar quais objetivos ou resultados devem ser 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.).

Para auxiliar nesta etapa, considere a adoção da ferramenta análise SWOT:



Análise SWOT é uma ferramenta utilizada para fazer análise de cenário (ou análise de ambiente). As informações obtidas sobre o ambiente interno e externo, contribuem na identificação dos riscos e na escolha das respostas aos riscos.

As informações coletadas, em conjunto com as informações do processo (normas, fluxograma das atividades, descrição das tarefas, responsáveis), são fundamentais para a realização das demais etapas do gerenciamento de riscos.

Etapa 2 - Identificação dos Riscos

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.

Riscos são situações em potencial – **que ainda não ocorreram** – que podem causar impacto na consecução dos objetivos da organização, caso venham a ocorrer.

A identificação dos riscos deve ser realizada em oficinas de trabalho ou, dependendo do objeto, pelo próprio gestor do risco.

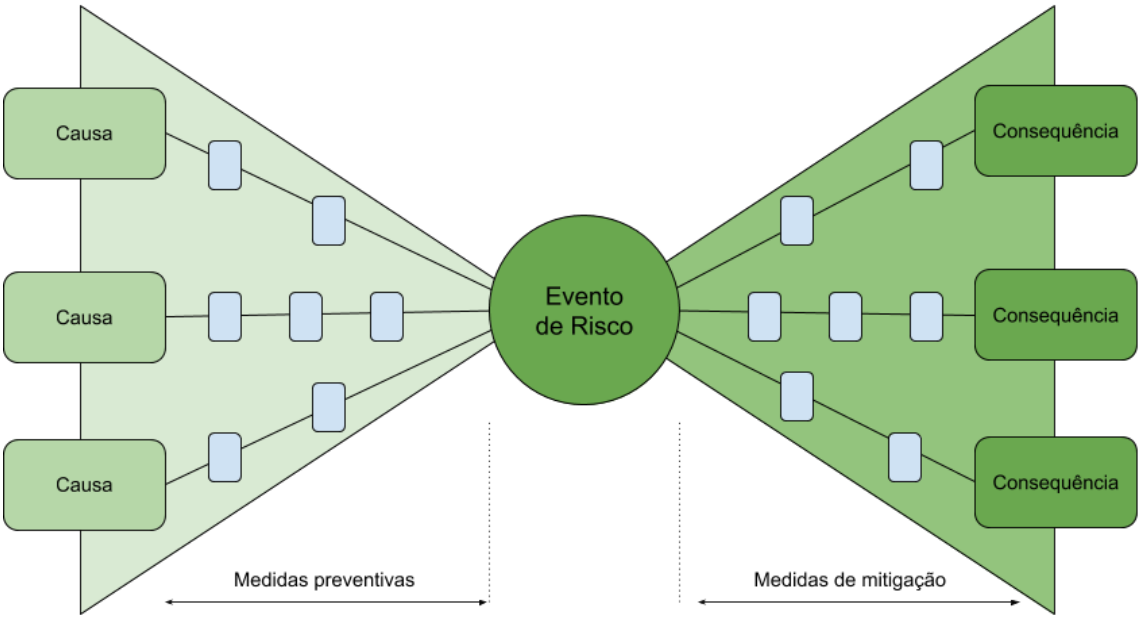
No processo de identificação de riscos, deve-se buscar a participação de pessoas que conheçam bem o objeto de gestão de riscos.

Devem ser utilizadas técnicas/ferramentas que permitam a coleta do maior número de riscos, tais como *brainstorming*, entrevistas, visitas técnicas, pesquisas, diagrama de causa e efeito, *bow-tie* etc.

São dicas que facilitam a identificação dos riscos:

- 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.

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. 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 a seguir para uma melhor compreensão.



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>

Os eventos de riscos identificados devem ser registrados de forma a permitir o levantamento das possíveis causas e consequências e a sua classificação quanto à categoria e natureza, bem como a sua avaliação quanto à probabilidade x impacto.

Etapa 3 - Análise dos 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**. Normalmente as causas se relacionam à probabilidade de o evento ocorrer e as consequências ao impacto, caso o evento se materialize.

A avaliação de riscos geralmente é feita por meio de análises quantitativas e qualitativas ou da combinação de ambas e, ainda, quanto à sua condição de *inerentes* (risco bruto, sem considerar qualquer controle) e *residuais* (considerando os controles identificados e avaliados quanto ao desenho e a sua execução).

Risco inerente é o risco a que uma organização está exposta sem considerar quaisquer ações gerenciais que possam reduzir a probabilidade de sua ocorrência ou seu impacto.

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

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

São calculados os níveis dos riscos identificados pela equipe técnica designada, a partir de critérios de probabilidade e impacto.

A seguir, as escalas de probabilidade e impacto:

Escala de probabilidade:

1. **muito baixa**: acontece apenas em situações excepcionais. Não há histórico conhecido do evento ou não há indícios que sinalizem sua ocorrência. **Peso 1**.
2. **baixa**: o histórico conhecido aponta para baixa frequência de ocorrência no prazo associado ao objetivo. **Peso 2**.
3. **média**: repete-se com frequência razoável no prazo associado ao objetivo ou há indícios que possa ocorrer nesse horizonte. **Peso 5**.

4. **alta**: repete-se com elevada frequência no prazo associado ao objetivo ou há muitos indícios que ocorrerá nesse horizonte. **Peso 8**.
5. **muito alta**: ocorrência quase garantida no prazo associado ao objetivo. **Peso 10**.

Escala de impacto:

1. **muito baixo**: compromete minimamente o atingimento do objetivo; para fins práticos, não altera o alcance do objetivo/resultado. **Peso 1**.
2. **baixo**: compromete em alguma medida o alcance do objetivo, mas não impede o alcance da maior parte do objetivo/resultado. **Peso 2**.
3. **médio**: compromete razoavelmente o alcance do objetivo/resultado. **Peso 5**.
4. **alto**: compromete a maior parte do atingimento do objetivo/resultado. **Peso 8**.
5. **muito alto**: compromete totalmente ou quase totalmente o atingimento do objetivo/resultado. **Peso 10**.

A multiplicação entre os valores de probabilidade e impacto define o **nível do risco inerente**, ou seja, o nível do risco sem considerar quaisquer controles que reduzem ou podem reduzir a probabilidade da sua ocorrência ou do seu impacto.

A seguinte matriz representa os possíveis resultados da combinação das escalas de probabilidade e impacto.

Impacto						
	Muito alto 10	10 RM	20 RM	50 RA	80 RE	100 RE
	Alto 8	8 RB	16 RM	40 RA	64 RA	80 RE
	Médio 5	5 RB	10 RM	25 RM	40 RA	50 RA
	Baixo 2	2 RB	4 RB	10 RM	16 RM	20 RM
	Muito baixo 1	1 RB	2 RB	5 RB	8 RB	10 RM
		Muito baixa 1	Baixa 2	Média 5	Alta 8	Muito alta 10
		Probabilidade				

Onde:

Classificação	Faixa
Risco baixo - RB	0 a 9,99
Risco médio - RM	10 a 39,99
Risco alto - RA	40 a 79,99
Risco extremo - RE	80 a 100

Em seguida, a equipe técnica designada deve avaliar a eficácia dos controles internos existentes em relação aos objetivos do processo organizacional. Ou seja, é necessário verificar se os controles existentes têm auxiliado no tratamento adequado desse risco.

O quadro abaixo mostra os níveis de avaliação da eficácia dos controles existentes.

Nível	Descrição	Fator de avaliação dos controles
Inexistente	Controles inexistentes, mal desenhados ou mal implementados, isto é, não funcionais.	1
Fraco	Controles têm abordagens *ad hoc*, tendem a ser aplicados caso a caso, a responsabilidade é individual, havendo elevado grau de confiança no conhecimento das pessoas.	0,8
Mediano	Controles implementados mitigam alguns aspectos do risco, mas não contemplam todos os aspectos relevantes do risco devido a deficiências no desenho ou nas ferramentas utilizadas.	0,6
Satisfatório	Controles implementados e sustentados por ferramentas adequadas e, embora passíveis de aperfeiçoamento, mitigam o risco satisfatoriamente.	0,4
Forte	Controles implementados podem ser considerados a “melhor prática”, mitigando todos os aspectos relevantes do risco.	0,2

O valor final da multiplicação entre o valor do **risco inerente** e o **fator de avaliação dos controles** corresponde ao nível de **risco residual**.

RR = RI x FC
em que:
RR = nível do risco residual
RI = nível do risco inerente
FC = fator de avaliação dos controles existentes

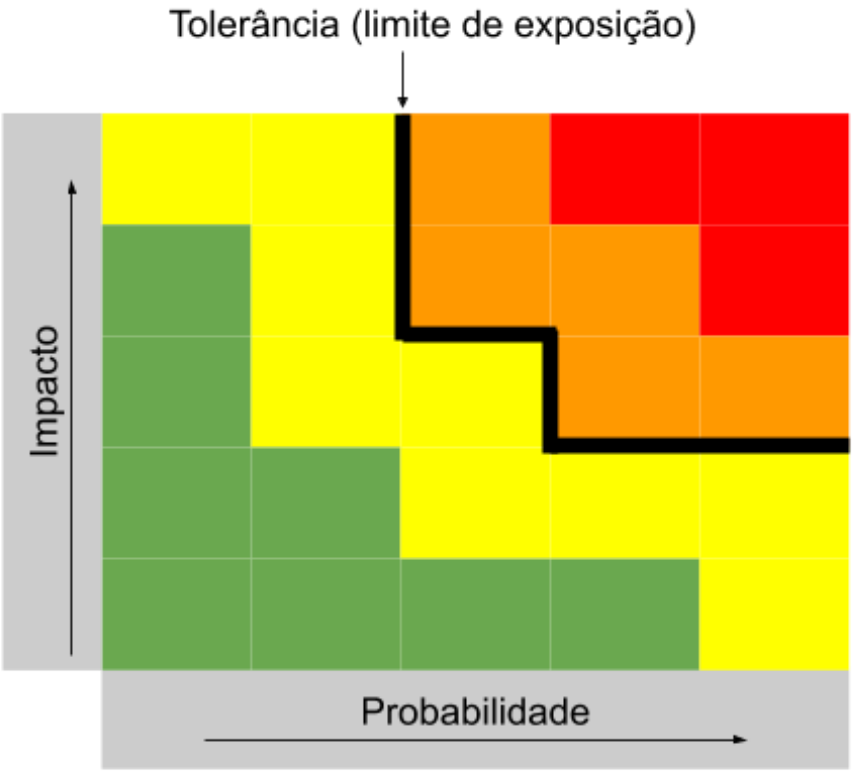
O valor de risco residual pode fazer com que o risco se enquadre em uma faixa de classificação diferente da faixa definida para o risco inerente.

Etapa 4 - Avaliação dos Riscos

A **avaliação do risco** envolve a **comparação do seu nível com o limite de exposição a riscos**, a fim de determinar se o risco é aceitável.

O limite de exposição a riscos representa o nível de risco acima do qual é desejável o tratamento do risco. Espera-se que, com os resultados do tratamento, o nível de **risco residual** fique abaixo do limite de exposição.

Matriz Simples de Risco e Tolerância ao Risco



A avaliação de riscos utiliza os resultados da análise de riscos como subsídio para a tomada de decisões sobre quais riscos necessitam ser tratados e quais terão prioridade no tratamento.

O quadro abaixo mostra, por classificação, quais ações devem ser adotadas em relação ao risco e suas exceções.

Classificação	Ação necessária	Exceção
Risco Baixo	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.	Caso o risco seja priorizado para implementação de medidas de tratamento, essa priorização deve ser justificada pela unidade e aprovada pelo seu dirigente máximo.
Risco Médio	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.	Caso o risco seja priorizado para implementação de medidas de tratamento, essa priorização deve ser justificada pela unidade e aprovada pelo seu dirigente máximo.
Risco Alto	Nível de risco além do apetite a risco. Qualquer risco neste nível deve ser comunicado ao dirigente máximo da unidade e ter uma ação tomada em período determinado. Postergação de medidas só com autorização do dirigente máximo da unidade.	Caso o risco não seja priorizado para implementação de medidas de tratamento, a não priorização deve ser justificada pela unidade e aprovada pelo seu dirigente máximo.
Risco Extremo	Nível de risco muito além do apetite a risco. Qualquer risco neste nível deve ser objeto de Avaliação Estratégica, comunicado ao Conselho Superior e ao dirigente máximo da unidade e ter uma resposta imediata. Postergação de medidas só com autorização do Comitê de Gestão Estratégica.	Caso o risco não seja priorizado para implementação de medidas de tratamento, a não priorização deve ser justificada pela unidade e aprovada pelo seu dirigente máximo e pelo Conselho Superior.

Sobre o Apetite a Risco do Processo Organizacional

A unidade organizacional pode definir, em conformidade com o contexto do processo organizacional em avaliação, faixas de classificação distintas das apontadas neste documento para refletir o nível de apetite a risco desse processo. Apetite a risco é o "nível de risco que a unidade está disposta a aceitar". Além disso, esse apetite deve ser aprovado pelo Conselho Superior.

É importante que o apetite a risco do processo organizacional 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 tratados e monitorados, e uma possível falta de tratamento deve ser justificada.

Etapa 5 - Tratamento dos 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 quadro a seguir.

Opção de Tratamento	Descrição
Mitigar	Um risco normalmente é mitigado quando é classificado como "Alto" ou "Extremo". A implementação de controles, neste caso, apresenta um custo/benefício adequado. Mitigar o risco significa implementar controles que possam diminuir as causas 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 "Extremo", 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 “Extremo”, e a implementação de controles apresenta um custo muito elevado, inviabilizando sua mitigação, ou não há entidades dispostas a compartilhar o risco. Evitar o risco significa encerrar o processo organizacional. Nesse caso, essa opção deve ser aprovada pelo Conselho Superior
Aceitar	Um risco normalmente é aceito quando seu nível está nas faixas de apetite a risco. Nessa situação, nenhum novo controle precisa ser implementado para mitigar o risco.

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 “Baixo” ou “Médio”).

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, com a participação de pessoas que conheçam bem o objeto de gestão de riscos.

São dicas que facilitam a identificação de medidas de resposta ao risco:

- 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.

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.

Validação do Resultado das Etapas do Processo de Gerenciamento de Riscos

Os resultados das etapas anteriores do processo de gerenciamento de riscos (entendimento do contexto, identificação e análise dos riscos, avaliação dos riscos, priorização dos riscos e definição de respostas aos riscos) devem ser avaliados e aprovados pelo dirigente máximo da unidade organizacional.

Após a aprovação desses resultados, o responsável pelo processo de gerenciamento de riscos ou o dirigente da unidade deve:

- Encaminhar esses resultados ao Comitê de Gestão de Riscos;
- Encaminhar o Plano de Tratamento aprovado às unidades corresponsáveis pelas iniciativas para que essas também incluam as ações em seu Plano Operacional corrente.

A implementação do Plano de Tratamento 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 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.

Comunicação

Refere-se à **identificação das partes interessadas** e ao **compartilhamento de informações relativas à gestão de riscos** sobre determinado objeto, observada a classificação da informação quanto ao sigilo.

Comunicar riscos é fornecer as informações relativas ao risco e ao seu tratamento para todos aqueles que possam influenciar ou ser influenciados por esse risco, sob pena de ele se materializar plenamente.

Dentro do escopo de um processo de gerenciamento de riscos, deve ser observada a Matriz de Responsabilidade RACI. A Matriz de Responsabilidade RACI define Responsável, Autoridade, Consultado e Informado para o processo de gerenciamento de riscos. São elementos da Matriz RACI:

- Responsável: quem executa a atividade;
- Autoridade: quem aprova a tarefa ou produto. Pode delegar a função, mas mantém a responsabilidade;
- Consultado: quem pode agregar valor ou é essencial para a implementação;
- Informado: quem deve ser notificado de resultados ou ações tomadas, mas não precisa se envolver na decisão.

Durante as etapas do processo de gerenciamento de riscos, é importante que a comunicação observe os agentes ou unidades apontadas como consultados ou informados na Matriz RACI a seguir.

Matriz RACI para o processo de gerenciamento de riscos no IFPB

	Conselho Superior	Diretoria Colegiada	Comitê de Riscos	Pró-Reitor / Diretor de Campus	Responsável pelo gerenciamento de riscos (Dono do riso)	Equipe Técnica Designada	Responsável pela implementação	Servidores do IFPB
Definir Plano de Gestão de Riscos da Unidade	A	C	I	R	C	I	I	I
Selecionar Processo Organizacional	A	I	C	R	C	I		
Realizar o Entendimento do Contexto	I	I	C	A	R	R		
Realizar a Identificação e Análise dos Riscos	I	I	C	A	R	R		
Realizar a Avaliação dos Riscos	I	I	C	A	R	R		
Realizar a Priorização dos Riscos	I	I	C	A	R	R		
Realizar a Definição de Respostas aos Riscos	I	I	C	A	R	R		
Validar os Riscos Levantados	I	I	C	R	C	C		
Implementar o Plano de Tratamento	I	I	C	A	I	C	R	

Monitorar	I/R	I	C	A	R	I	C	R
Realizar Avaliação Estratégica	A	C	R	C	C	R		

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, no âmbito do processo de gerenciamento de riscos, deve ser realizado principalmente pela unidade responsável pelo processo organizacional, de forma a:

- Garantir que os controles sejam eficazes e eficientes;
- Analisar as ocorrências dos riscos;
- Detectar mudanças que possam requerer revisão dos controles e/ou do Plano de Tratamento;
- Identificar os riscos emergentes.

Mudanças identificadas durante o monitoramento devem ser encaminhadas ao Comitê de Gestão de Riscos, a quem compete supervisionar os resultados de todos os processos de gerenciamento de riscos já realizados nos processos organizacionais do IFPB.

Trimestralmente, o Comitê de Gestão de Riscos produzirá um boletim com o resultado do acompanhamento das ações relacionadas ao Plano de Gestão de Riscos de cada unidade, que será enviado ao Comitê Gerencial e ao Comitê de Gestão Estratégica.

Além disso, o Comitê elaborará o Relatório de Monitoramento da Gestão de Riscos do IFPB com a consolidação desses resultados, que deve ser encaminhado, no mínimo, uma vez por ano ao Conselho Superior.

Sistema de Gestão de Riscos do IFPB

O Sistema de Gestão de Riscos do IFPB é o conjunto de componentes que fornecem os fundamentos e os arranjos organizacionais para a concepção, implementação, monitoramento, análise crítica e melhoria contínua da gestão de riscos através de toda a organização.

A ISO 31000:2009 trata dos componentes Mandato e Comprometimento, Concepção da Estrutura para Gerenciar Riscos, Implementação da Gestão de Riscos, Monitoramento e Análise Crítica da Estrutura e Melhoria Contínua da Estrutura.

No IFPB, o componente Mandato e Comprometimento é demonstrado pelas ações do Conselho Superior e da alta administração em promover a Gestão de Riscos do IFPB; primeiro, pela aprovação da Política de Gestão de Riscos; segundo, por definir suas competências e responsabilidades naquela.

Na Concepção da estrutura para gerenciar riscos, além da publicação da sua Política de Gestão de Riscos, o IFPB definiu a responsabilização das suas unidades e agentes, a forma de integração dos processos organizacionais, os recursos necessários e as formas de comunicação no âmbito de sua Gestão de Riscos.

O Monitoramento e a Análise Crítica da estrutura de Gestão de Riscos são constantes, por meio da comparação da Gestão de Riscos do IFPB com bases normativas, estruturas de trabalho, contextos de Governo e do IFPB, percepção de servidores, entre outros.

Com o entendimento de que os resultados do Monitoramento e da Análise Crítica podem impactar na estrutura e na metodologia de Gestão de Riscos do IFPB, é prevista uma revisão anual desses componentes (Melhoria Contínua da Estrutura). Porém, mudanças no contexto podem provocar a necessidade de implantação de melhorias de forma antecipada.

Instâncias e Responsabilidades

De acordo com a Política de Gestão de Riscos do IFPB, são instâncias responsáveis pelo Sistema de Gestão de Riscos:

- Conselho Superior;
- Comitê de Gestão de Riscos;
- Diretorias colegiadas;
- Gestores estatutários (Pró-reitores e Diretores);
- Gestores de riscos; e

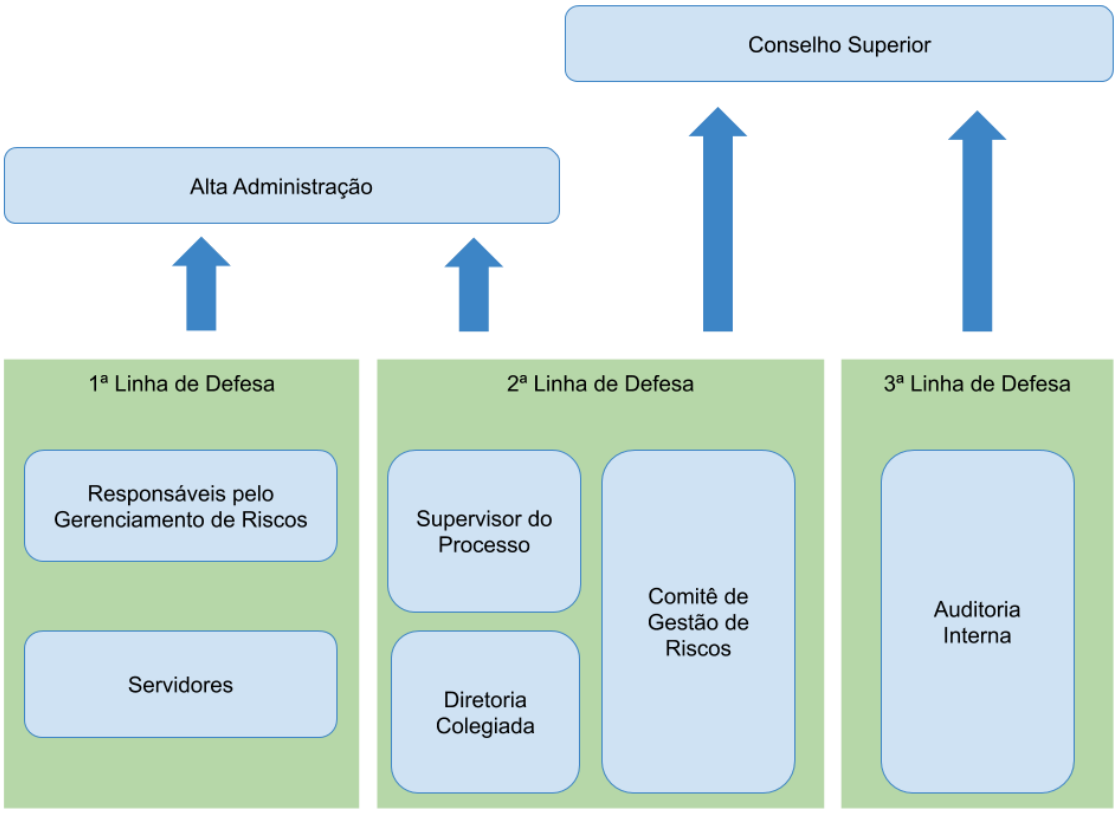
- Auditoria Interna.

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 da seguinte forma:

- 1ª linha de defesa: controles internos da gestão executados por todos os agentes públicos responsáveis pela condução de atividades e tarefas, no âmbito dos macroprocessos finalísticos e de apoio;
- 2ª linha de defesa: supervisão e monitoramento dos controles internos executados por instâncias específicas, como comitês, diretorias ou assessorias específicas para tratar de riscos, controles internos, integridade e compliance;
- 3ª linha de defesa: constituída pelas auditorias internas no âmbito da Administração Pública, uma vez que são responsáveis por proceder à avaliação da operacionalização dos controles internos da gestão (primeira linha ou camada de defesa) e da supervisão dos controles internos (segunda linha ou camada de defesa).

No IFPB, de acordo com O SGE004 - Governança, Risco e Compliance (Planede), a 1ª linha de defesa é composta pelo “dono do processo”, que é o gestor do processo e responsável pela execução operacional e o reporte da mensuração. Na 2ª linha, atuam: o "Supervisor do Processo", que é o gestor de nível hierárquico imediatamente superior ao do dono do processo; a "Diretoria Colegiada", constituída por todos os servidores da área que se reúnem para a avaliação conjunta dos indicadores de desempenho e de indicadores de risco, para se atestar a conformidade; o "Presidência do Órgão Colegiado Estatutário", que atua direta e especificamente na regulamentação do macroprocesso; e o “Comitê de Gestão de Riscos”. A 3ª linha de defesa fica a cargo da Unidade de Auditoria Interna Governamental.

A figura a seguir demonstra as linhas de defesa na Gestão de Riscos do IFPB.



O **Comitê de Gestão de Riscos** tem a responsabilidade primária sobre o processo de gestão de riscos do IFPB, o qual deve articular periodicamente com o Conselho Superior do IFPB (CONSUPER) para avaliar processo e procedimentos e de propor as melhores alternativas.

As competências dos atores envolvidos na Gestão de Riscos são as seguintes:

Conselho Superior

- 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;
- Definir indicadores de desempenho para a Gestão de Riscos, alinhados com os indicadores de desempenho do IFPB;
- 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 do IFPB; e
- Supervisionar a atuação das demais instâncias da Gestão de Riscos.

Diretorias Colegiadas

- Auxiliar o CONSUPER 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;
- Monitorar a evolução dos níveis de riscos e a efetividade das medidas de controle implementadas;
- Auxiliar na avaliação do desempenho e da conformidade legal e normativa da Gestão de Riscos; e
- Auxiliar na definição dos indicadores de desempenho para a Gestão de Riscos, alinhados com os indicadores de desempenho do IFPB.

Comitê de Gestão de Riscos

- Propor a Metodologia de Gestão de Riscos e suas revisões;
- Definir 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 Gerencial e ao Comitê de Gestão Estratégica;
- Oferecer capacitação continuada em Gestão de Riscos para os servidores do IFPB;
- Elaborar Plano de Comunicação de Gestão de Riscos;

- Medir o desempenho da Gestão de Riscos objetivando a sua melhoria contínua;
- Construir e propor ao Conselho Superior os indicadores de desempenho para a Gestão de Riscos, alinhados com os indicadores de desempenho do IFPB; e
- Requisitar aos responsáveis pelo gerenciamento de riscos dos processos organizacionais as informações necessárias para a consolidação dos dados e a elaboração dos relatórios gerenciais.

Responsáveis pelo gerenciamento de riscos dos processos organizacionais

- Identificar, analisar e avaliar os riscos dos processos sob sua responsabilidade, em conformidade ao que define a Política de Gestão de Riscos;
- 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 ao Comitê de Gestão de Riscos sobre mudanças significativas nos processos organizacionais sob sua responsabilidade;
- Responder às requisições do Comitê de Gestão de Riscos; e
- Disponibilizar as informações adequadas quanto à gestão dos riscos dos processos sob sua responsabilidade a todos os níveis do IFPB e demais partes interessadas.

Servidores do IFPB

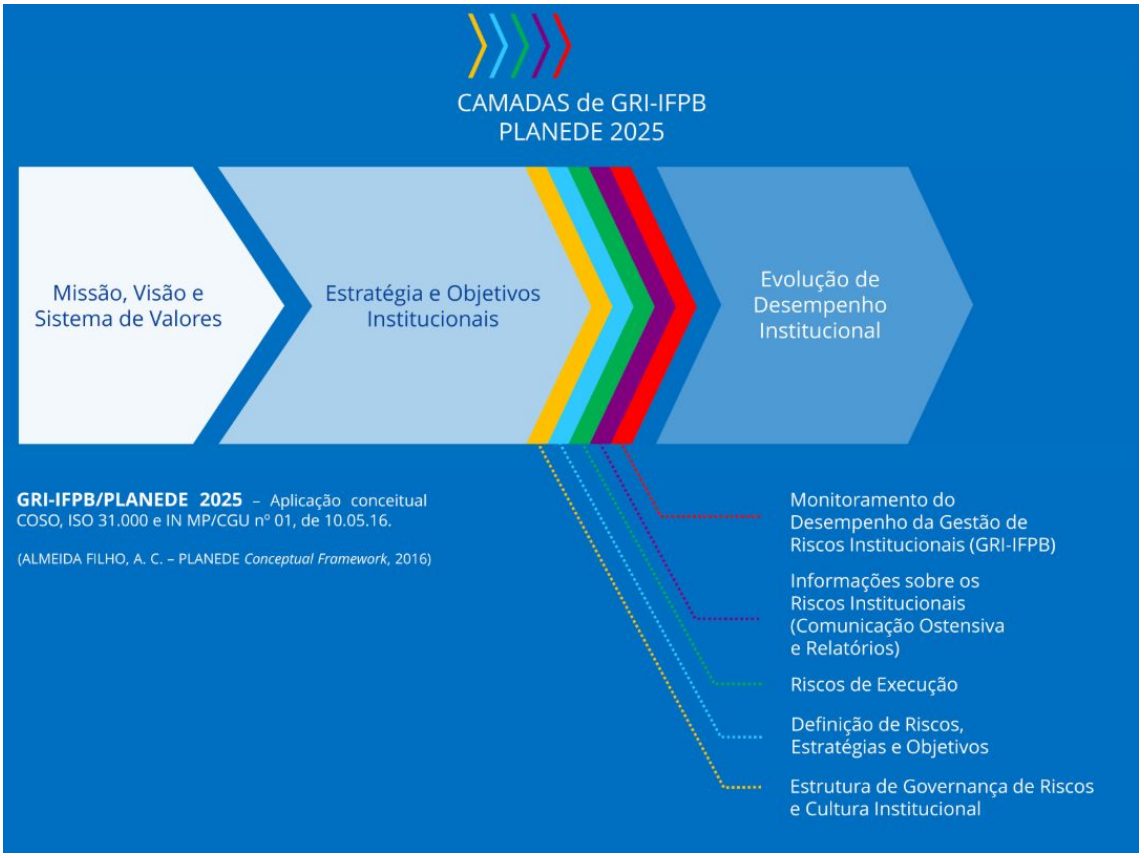
- Monitoramento da evolução dos níveis de riscos e da efetividade das medidas de controles implementadas nos processos organizacionais em que estiverem envolvidos ou que tiverem conhecimento.

Integração nos Processos Organizacionais

Os riscos constituem insumo para o diagnóstico institucional do processo de planejamento estratégico.

Ao se formular a estratégia institucional, deverão ser considerados os riscos intrínsecos àquela estratégia (COSO 2017). Deve ser considerado, também, o risco de a estratégia não estar alinhada à missão, à visão e às competências constitucionais do IFPB.

Depois de estabelecida a estratégia, as medidas mitigadoras constituirão ações constantes dos planos operacionais.


CAMADAS de GRI-IFPB
PLANEDE 2025
Missão, Visão e Sistema de Valores
Estratégia e Objetivos Institucionais
Evolução de Desempenho Institucional
GRI-IFPB/PLANEDE 2025 – Aplicação conceitual COSO, ISO 31.000 e IN MP/CGU nº 01, de 10.05.16.
(ALMEIDA FILHO, A. C. – PLANEDE Conceptual Framework, 2016)
Monitoramento do Desempenho da Gestão de Riscos Institucionais (GRI-IFPB)
Informações sobre os Riscos Institucionais (Comunicação Ostensiva e Relatórios)
Riscos de Execução
Definição de Riscos, Estratégias e Objetivos
Estrutura de Governança de Riscos e Cultura Institucional

Referências bibliográficas

BRASIL. Agência Nacional de Saúde Suplementar. Manual de Gestão de Riscos. Rio de Janeiro, 2018. Disponível em: <http://www.ans.gov.br/images/stories/A_ANS/Transparencia_Institucional/gestao_de_riscos/manual-de-gestao-de-riscos-da-ans.pdf>. Acesso em: abril, 2020.

_____. Associação Brasileira de Normas Técnicas - ABNT. Gestão de Riscos: Princípios e Diretrizes. Norma Brasileira ABNT NBR ISO 31000: Primeira Edição, 2009.

_____. Instituto Federal de Educação, Ciência e Tecnologia da Paraíba - IFPB. Portaria nº 2025/2017 - Reitoria, de 24 de agosto de 2017. .

_____. Instituto Nacional da Propriedade Industrial. Manual de gestão de riscos do INPI. Rio de Janeiro, 2018. Disponível em: <http://www.inpi.gov.br/sobre/estrutura/manual-gestao-de-riscos-inpi.pdf/view>. Acesso em: abril de 2020.

_____. Ministério da Transparência e Controladoria-Geral da União - CGU. Metodologia de Gestão de Riscos. Brasília, 2018. Disponível em: <https://www.gov.br/cgu/pt-br/centrais-de-conteudo/publicacoes/institucionais/arquivos/cgu-metodologia-gestao-riscos-2018.pdf>. Acesso em: abril, 2020.

_____. Ministério do Planejamento, Orçamento e Gestão. Manual de Gestão de Integridade, Riscos e Controles Internos da Gestão. Assessoria Especial de Controles Internos - AECI. Brasília, 2017. Disponível em <http://www.planejamento.gov.br/assuntos/gestao/controle-interno/manual-de-girc>. Acesso em: abril 2020.

_____. _____ e Controladoria-Geral da União. Instrução Normativa Conjunta Nº 1, de 10 de maio de 2016. Dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo federal. Brasília, 2016. Disponível em <http://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?jornal=1&data=11/05/2016&pagina=14> . Acesso em: abril 2020.

_____. Tribunal de Contas da União. Manual de Gestão de Riscos: TCU, 2018. Disponível em: <https://portal.tcu.gov.br/planejamento-governanca-e-gestao/gestao-de-riscos/manual-de-gestao-de-riscos/> . Acesso em: abril, 2020.

_____. _____. Referencial Básico de Gestão de Riscos: TCU, 2018. Disponível em <https://portal.tcu.gov.br/biblioteca-digital/referencial-basico-de-gestao-de-riscos.htm>: . Acesso em: abril, 2020.

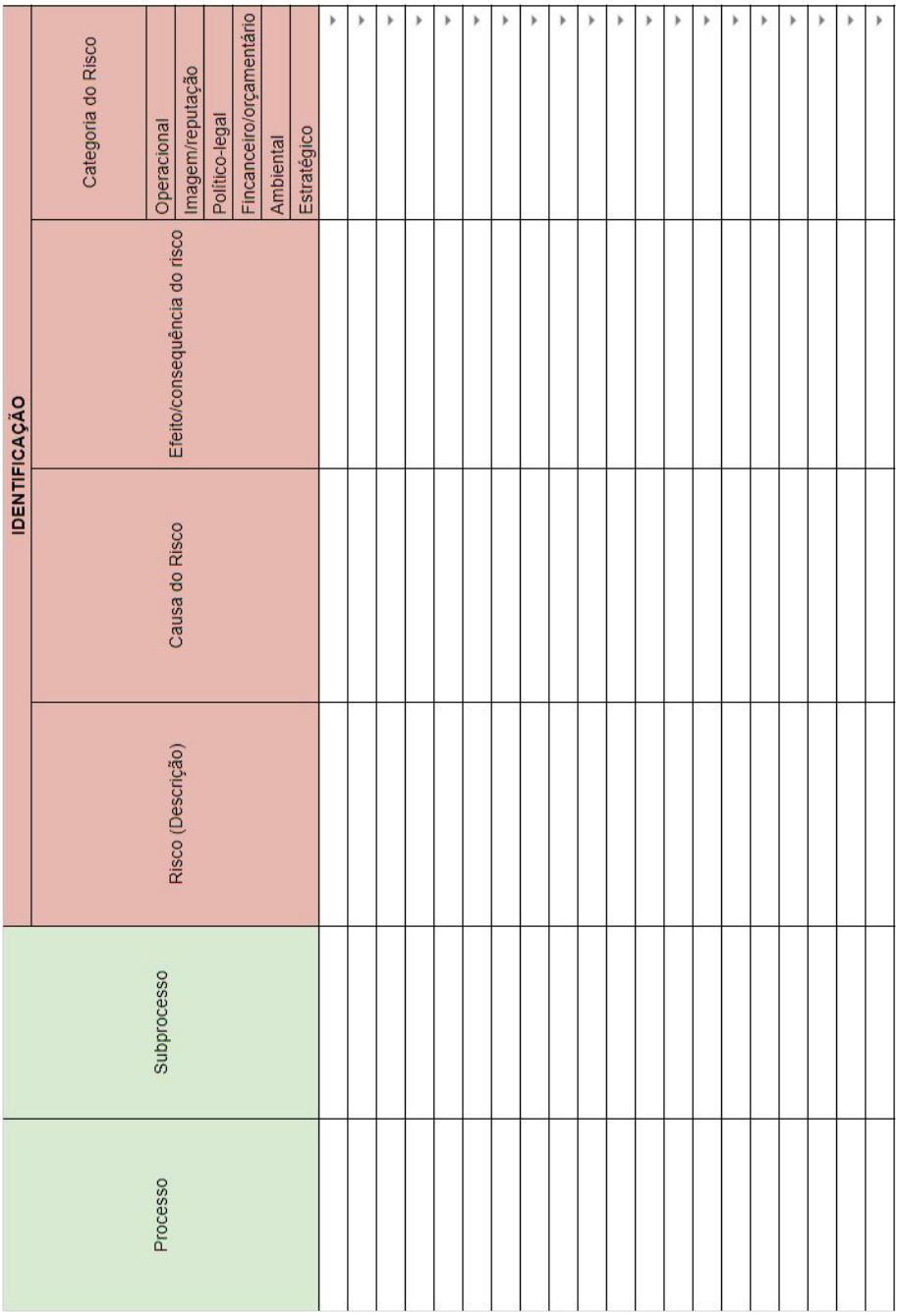
_____. Tribunal Superior do Trabalho. Plano de Gestão de Riscos da Secretaria do Tribunal Superior do Trabalho. Brasília, 2015. Disponível em: <https://juslaboris.tst.jus.br/handle/20.500.12178/73831>. Acesso em: abril, 2020.

COSO. 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.

Anexos

Modelo de planilha de apoio ao processo de gerenciamento de riscos

Parte 1 - Identificação dos riscos



ANÁLISE E AVALIAÇÃO									
Probabilidade (P)	Impacto (I)	Risco Inerente (RI) RI=P x I	Nível do Risco Inerente	Controles existentes				Risco Residual (RR) RR = RI x FC	Nível do Risco Residual
				Medidas de controles		Maturidade	Fator (FC)		
1. Muito baixa	1. Muito baixo					Inexistente	1,00		
2. Baixa	2. Baixo		Risco Baixo			Fraco	0,80		Risco Baixo
5. Média	5. Médio		Risco Médio	Preventivo	Atenuação e recuperação	Mediano	0,60		Risco Médio
8. Alta	8. Alto		Risco Alto			Satisfatório	0,40		Risco Alto
10. Muito alta	10. Muito alto		Risco Extremo			Forte	0,20		Risco Extremo
		0	Risco Baixo					0	Risco Baixo
		0	Risco Baixo					0	Risco Baixo
		0	Risco Baixo					0	Risco Baixo
		0	Risco Baixo					0	Risco Baixo
		0	Risco Baixo					0	Risco Baixo
		0	Risco Baixo					0	Risco Baixo
		0	Risco Baixo					0	Risco Baixo
		0	Risco Baixo					0	Risco Baixo
		0	Risco Baixo					0	Risco Baixo
		0	Risco Baixo					0	Risco Baixo
		0	Risco Baixo					0	Risco Baixo
		0	Risco Baixo					0	Risco Baixo
		0	Risco Baixo					0	Risco Baixo
		0	Risco Baixo					0	Risco Baixo
		0	Risco Baixo					0	Risco Baixo
		0	Risco Baixo					0	Risco Baixo
		0	Risco Baixo					0	Risco Baixo
		0	Risco Baixo					0	Risco Baixo
		0	Risco Baixo					0	Risco Baixo
		0	Risco Baixo					0	Risco Baixo
		0	Risco Baixo					0	Risco Baixo
		0	Risco Baixo					0	Risco Baixo

RESPOSTA E TRATAMENTO									
Resposta ao Risco	Plano de Tratamento			Data de início	Data de conclusão		Custo previsto	Proprietário do Risco	Situação
	Controles propostos	Tipo de Controle Proposto	Objetivo do Controle proposto						
Aceitar									Não iniciado
Mitigar		Preventivo							Em andamento
Compartilhar		Detectivo	Adotar novo						Atrasado
Evitar		Corretivo	Melhorar existente		Programada	Realizada			Concluído no prazo
									Concluído fora do prazo

Parte 3 - Resposta e Tratamento dos Riscos

Parte 4 - Monitoramento e Revisão

MONITORAMENTO E REVISÃO					
Plano de Revisão		Houve mudança no processo?	Novos riscos identificados?	Ações corretivas	Lições aprendidas
Responsável	Frequência				
	Por evento				
	Semanal				
	Mensal				
	Trimestral				
	Semestral				
	Anual	Sim	Sim		
	Aleatório	Não	Não		

Lista de Eventos de Risco Operacional

Segue uma lista sugestiva e não exaustiva de eventos de risco operacional.

Risco Operacional	
Fator	Subfator e Exemplos de Riscos
PROCESSOS	COMUNICAÇÃO INTERNA: ● Os insumos e as informações não são recebidos em tempo adequado para a execução do processo ● Ausência de padrões mínimos definidos para a execução do processo ● Erros e falhas de informações que afetam a execução do processo MODELAGEM: ● Fluxo desatualizado e não reflete a prática atual utilizada na execução do processo ● Ausência de avaliação periódica sobre a adequabilidade do desenho do processo ● Ausência ferramenta para análise e melhoria contínua do processo ● Falha ou falta de metodologia que auxilie no mapeamento do processo SEGURANÇA FÍSICA: ● Falha ou falta de segurança no ambiente de trabalho que afeta a execução do processo ● Acesso a áreas consideradas como críticas sem que as pessoas estejam devidamente credenciadas e identificadas ADEQUAÇÃO À LEGISLAÇÃO: ● Descumprimento de prazos legais na execução do processo ● Ausência de compilação e distribuição de legislação pertinente ao processo em execução ● Execução do processo em desacordo com o regimento interno/normas ● Descumprimento de prazo judicial na execução do processo ● Descumprimento de obrigação regulatória na execução do processo
PESSOAS	CARGA DE TRABALHO: ● Rotatividade (turnover) de pessoal acima do esperado que afeta a execução do processo ● Capacidade operacional insuficiente para a execução do processo ● Falha ou falta de dimensionamento da capacidade operacional com impacto na execução do processo COMPETÊNCIAS:

	● Capacitação da equipe é insatisfatória para a execução do processo ● Concentração de conhecimentos em determinados servidores afetando a execução do processo ● Falha ou falta de disseminação de conhecimento afetando a execução do processo ● Falha ou falta de capacitação que afeta a execução do processo AMBIENTE ORGANIZACIONAL: ● Ausência de satisfação e/ou de bem-estar do servidor na execução de sua tarefa ● Desconhecimento dos objetivos do processo por parte dos Servidores Servidores desconhecem as suas responsabilidades individuais na execução do processo ● Ausência de recursos necessários para execução das tarefas ● Resistência de Servidores em promover alterações nas condições de trabalho CONDUTA: ● Ausência de postura ética nas atividades e nos relacionamentos interpessoais ● Falta de atenção e zelo na execução do processo ● Ausência de imparcialidade, cumprimento das leis e normas/regulamentares, confidencialidade e comprometimento na execução do processo ● Quebra de sigilo e confidencialidade
AMBIENTE TECNOLÓGICO	SEGURANÇA LÓGICA: ● Ausência de estrutura de perfis de acesso aos sistemas para execução do processo ● Ausência de controle de acesso lógico ● Ausência de logon próprio na rede institucional ● Falha ou falta de meios seguros de acesso aos sistemas ● Inexistência de registro nos sistemas (log) das transações críticas ● Ausência de formalização que defina as responsabilidades do usuário externo do sistema ● Incapacidade do sistema de prover informações confiáveis e suficientes sobre o processo em execução INFRAESTRUTURA TECNOLÓGICA: ● Grau de informatização do processo inadequado para execução do processo ● Informações e dados armazenados em diretórios não protegidos e sem controle de acesso ● Ausência de backup de arquivos, planilhas e bancos de dados essenciais à execução do processo ● A estação de trabalho não possui acionado

	dispositivo de time-out ● Descarte de mídias sem antes terem apagados os com conteúdo reservado ● Sobrecarga de sistemas de processamento de dados no momento da execução do processo ● Inadequação de sistemas operacionais/aplicativos para execução do processo ● Falhas de hardware, faltas de backup e de legalização do software afetando a execução do processo ● Obsolescência dos sistemas e equipamentos afetando a execução do processo ● Ataques lógicos à rede de computadores afetando a execução do processo SOLUÇÃO DE TI: ● Inexistência de controle nas requisições e nas melhorias requeridas nos sistemas cuja falta de implementação afeta a execução do processo ● Falha ou falta de homologação de sistema impedindo a execução do processo de forma automatizada COMUNICAÇÃO: ● Instabilidade nos sistemas operacionais que afeta a execução do processo ● Incompatibilidade e/ou indisponibilidade de informações afetando a execução do processo
EVENTOS EXTERNOS	DESASTRES NATURAIS E CATÁSTROFE: ● Ação Humana: ações intencionais executadas por terceiros para lesar o órgão, como por exemplo: (i) roubos, falsificações, furtos, atos de vandalismos, fraudes externas; (ii) degradação do meio ambiente; e (iii) alterações no ambiente econômico, político e social ● Força Maior: (i) enchentes, terremotos, catástrofes (queda de prédio) e outros desastres naturais AMBIENTE REGULATÓRIO: ● Alterações inesperadas na legislação ou em marcos regulatórios pelos órgãos fiscalizadores e reguladores AMBIENTE SOCIAL: ● Cenário socioeconômico interfere na execução do processo ● Retrações ou não-aproveitamento de oportunidades de mercado provocadas por eventos relacionados a segurança patrimonial que impede a execução do processo FORNECEDORES: ● Indisponibilidade de recursos em virtude de concentração em um único fornecedor que impede a

	execução do processo ● Falhas ou indisponibilidade de serviços públicos que afeta a execução do processo

Controles básicos

Segue uma lista sugestiva e não exaustiva de controles básicos.

Categoria de Risco	Fatores	Subfatores	Controles básicos
Risco de Integridade			Postura da alta administração
			Políticas e procedimentos anticorrupção
			Mapeamento de Riscos de Corrupção
			Criação de indicadores de riscos de corrupção dos passos decisórios
Risco de conformidade			Acompanhamento e Análise de Normas e Regulamentos Externos
			Pareceres da Assessoria Jurídica
			Atividades de Treinamento
			Normas e Procedimentos
Risco Operacional	Pessoas	Carga de Trabalho	Planejamentos de longo, médio e curto prazos
			Acordo de Trabalho
			Pesquisa de Clima Organizacional
			Reuniões Participativas
		Competências	Identificação da Necessidade de Conhecimento / Habilidades

			Atividades de Treinamento
			Normas e Procedimentos
			Ferramentas de autoavalização de Conhecimentos / Habilidades
		Qualidade de Vida no Trabalho	Pesquisa de Clima Organizacional
			Condições Ambientais
			Comunicação com a Administração
			Processo de Gerenciamento de Equipes
Risco Operacional	Processos	Comunicação Interna	Canais de Comunicação – Com os Servidores
			Normas e Procedimentos
		Modelagem	Ferramentas para Análise e Melhoria Contínua de Processos
			Metodologia de Autoavalização de Riscos e Controles
			Validações – Backtesting
		Segurança Física	Mecanismos de Segurança Física
			Controles de Acesso Físico
			Manutenção de Equipamentos
		Pontos de Controle	Normas e Procedimentos
			Metodologia de Autoavalização de Riscos e Controles
			Mecanismos de Monitoramento e Reporte
		Adequação à	Testes de Conformidade

		Legislação	Normas e Procedimentos
Risco Operacional	Sistemas	Segurança Lógica	Políticas e Diretrizes
			Controles de Acesso Lógico
			Arquivo e Preservação de Registros
		Hardware e Software	Manutenção de Equipamentos
			Layout de formulários e Sistemas
			Planos de Contingência
		Análise e Programação	Layout de Formulários e Sistemas
			Validações - Backtesting
			Atividades de Treinamento
		Rede de Comunicação	Planos de Contingência
			Manutenção de Equipamentos
Risco Operacional	Eventos Externos	Desastres Naturais e Catástrofes	Planos de Contingência
			Atividades de Treinamento
		Ambiente Regulatório	Análise da Conjuntura Política e Econômica Nacional e Internacional
		Ambiente Social	Análise da Conjuntura Política e Econômica Nacional e Internacional
		Fornecedores	Controles de Serviços Terceirizados
			Planos de Contingência
		Clientes	Controles de Acesso Lógico
		Meio Ambiente	Valores Éticos e Normas de Conduta da Empresa
Risco de Imagem			Valores Éticos e Normas de Conduta da Empresa

			Normas e Procedimentos
			Controles de Serviços Terceirizados
			Pesquisa de Satisfação
			Canais de Comunicação - Com a Sociedade
			Canais de Comunicação – Com os Servidores