INPI INSTITUTO NACIONAL DA PROPRIEDADE INDUSTRIAL	SISTEMA DE PADRONIZAÇÃO DO INPI MANUAL	**Código**	GEQU – GRI – MN- 0001
		Revisão	01
		Elaboração	26/03/2020
	MANUAL DE GESTÃO DE RISCOS DO INPI	**Aprovação**	31/03/2020
		Processo	Gestão de Riscos

1 Sumário

2 Introdução

O modelo de gestão de riscos do INPI tem como premissa básica a avaliação de riscos dentro dos processos organizacionais, e está apoiado em diretrizes da norma ABNT NBR ISO 31000:2009 e do Guia de Gestão de Riscos do Ministério da Economia, publicado por meio da Resolução CRTCI n° 5, de 29 de agosto de 2019.

Assim, a Instituição adota uma estrutura de governança baseada em um processo contínuo de tratamento de riscos, planejado para identificar, avaliar, tratar e monitorar eventos que possam comprometer ou impossibilitar o atingimento dos objetivos organizacionais.

Como forma de operacionalizar a metodologia apresentada neste Manual, a Divisão de Gestão de Riscos disponibiliza uma planilha para sistematizar a aplicação do processo e a organização dos dados, visando também contribuir para a formação de um Banco de Riscos do Instituto, e para o monitoramento das ações de tratamento propostas.

Adicionalmente, o INPI, enquanto entidade vinculada ao Ministério da Economia, utilizará o sistema “AGATHA” como forma de documentar a gestão de riscos, sem prejuízo da solução mencionada e em funcionamento.

3 Objetivo

Gerenciar riscos é uma das funções essenciais da governança. Assim, a Alta Administração do INPI, com o apoio e assessoramento técnico da DIGER deve direcionar e monitorar o sistema de gestão de riscos, estabelecendo diretrizes para implementação e monitoramento das medidas de gerenciamento dos riscos e controle interno. O comprometimento e as diretrizes gerais para a Gestão de Riscos no INPI estão estabelecidos na Política de Riscos, documento GEQU - GRI - PL-0001.

Para se cumprir um objetivo ou compromisso, algumas ações devem ser adotadas visando este fim. Porém, toda ação tem uma (ou mais) consequência(s). E, toda consequência, traz consigo, inúmeras possibilidades de impacto (risco) no negócio ou objeto que se pretende realizar, que podem cooperar positivamente no alcance do objetivo (oportunidades, fonte de ganhos) ou, do contrário, prejudicar ou até mesmo impedir seu atingimento (ameaças, fonte de perdas).

Os controles internos nos processos de trabalho devem ser criados para diminuir ou eliminar os riscos. Ele devem ser, portanto, cuidadosamente dimensionados, uma vez que a implementação de controles complexos e demasiadamente burocráticos para eventos com nível de risco baixo, por exemplo, podem gerar um alto e desnecessário custo administrativo ao processo, podendo comprometer, inclusive, o alcance dos objetivos da organização – o que não se justificaria.

Os níveis de riscos vêm aumentando globalmente, e esta nova realidade vem exigindo cada vez mais das organizações a capacidade de lidar com altos graus de riscos em seus Projetos e Processos. Por isso, diante desta realidade, é fundamental a utilização de um Plano de Gestão de Riscos institucional, que permita tanto seu tratamento corretivo, mas, principalmente, preventivo.

Em resumo, uma boa gestão de riscos resulta em:

I- aumentar a probabilidade de atingir os objetivos;

II- estar atento para a necessidade de identificar e tratar os riscos através de toda a organização;

III- melhorar a identificação de oportunidades e ameaças;

IV-melhorar a governança;

V- melhorar a confiança das partes interessadas;

VI-estabelecer uma base confiável para a tomada de decisão e o planejamento;

VII- melhorar os controles;

VIII- alocar e utilizar eficazmente os recursos para o tratamento de riscos;

IX-melhorar a eficácia e a eficiência operacional; e

X- aumento de produtividade.

4 Abrangência

Todos os processos do Instituto.

5 Documentos complementares

GEQU – GRI – PL– 0001 Política de Gestão de Riscos do INPI.

6 Descrição dos processos ou atividades

6.1 Gestão de Riscos

O risco é o resultado da combinação da probabilidade de ocorrência de um determinado evento indesejado e de sua consequência.

O risco ocorre quando uma fonte potencial de um evento indesejado é concretizada por uma vulnerabilidade (causa), que implicará em um efeito (ou consequência) no fluxo do trabalho.

O evento de risco identificado é considerado uma ameaça quando pode prejudicar o desenvolvimento da atividade ou processo e, em última instância, comprometer o alcance dos objetivos institucionais; por outro lado, é considerado uma oportunidade quando existe a possibilidade de que um evento afete positivamente o alcance destes objetivos.

Figura 1 Componentes do Risco

Sintaxe para a descrição de riscos:

“Devido a <CAUSAS/FONTES/VULNERABILIDADES>, poderá acontecer <DESCRIÇÃO DA INCERTEZA/EVENTO DE RISCO>, o que poderá levar a <DESCRIÇÃO DA CONSEQUÊNCIA/ IMPACTO/PERDA> impactando no/na <DIMENSÃO DE OBJETIVO IMPACTADA>”.

Os riscos são medidos em termos de probabilidade de ocorrência e do impacto resultante da concretização do evento de risco.

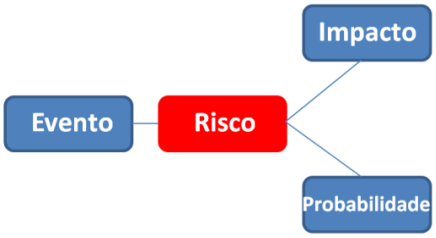


Figura 2 Fatores para a análise do risco

A mensuração da probabilidade de ocorrência está ligada a uma investigação das causas do risco. O dimensionamento do impacto está ligado às consequências do risco.

Para tanto, são atribuídas pontuações de probabilidade e impacto de ocorrência para cada risco, chegando-se ao nível do risco – que no caso do INPI poderá ser: baixo, médio, alto e crítico. A depender do resultado desta análise, propõe-se um plano de ação para mitigação dos riscos – os detalhes serão explicados ao longo deste Manual.

6.1.1 Processos da gestão de riscos no INPI

No processo de gestão de riscos do INPI serão consideradas apenas as ameaças e não os riscos positivos.

O INPI organizará sua gestão de riscos de acordo com os processos a seguir:

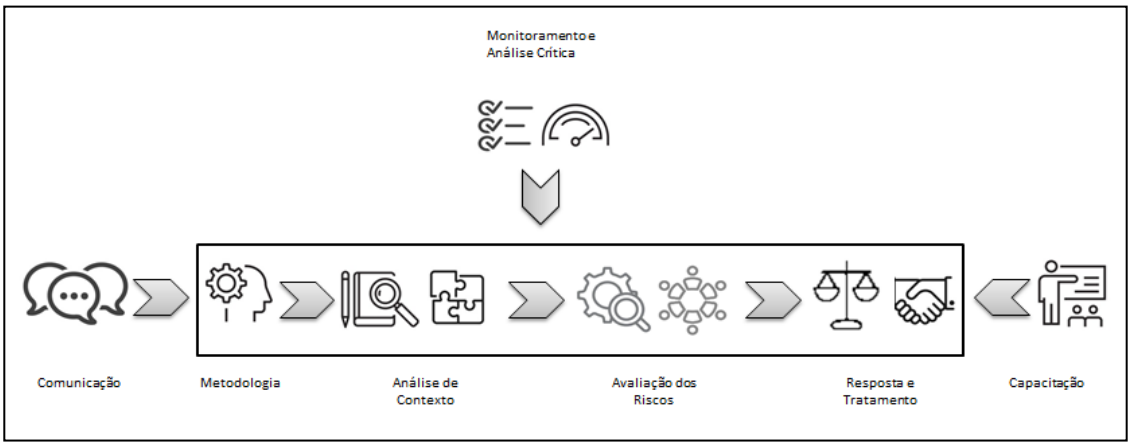


Figura 3 Processo de Gestão de Riscos do INPI

- Desenvolvimento da Metodologia de Gestão de Riscos: é o processo que define como será feita a gestão de riscos, o escopo de suas atividades, e os papéis e responsabilidades no gerenciamento de riscos.
- Análise de Contexto: é o processo onde serão realizados o levantamento e registro dos aspectos externos e internos essenciais ao alcance dos objetivos institucionais, compreendendo o contexto em que a organização está inserida.
- Avaliação dos Riscos: é o processo para identificar, avaliar os riscos e registrar seus eventuais controles existentes.
- Resposta e Tratamento dos Riscos: é o processo para definir as respostas aos riscos e, eventualmente, estabelecer medidas de controle, visando modificar o nível dos

riscos, sempre buscando sua redução. **O Plano de Tratamento dos Riscos é o principal resultado deste processo**.

- Monitoramento e Análise Crítica: é o processo para monitorar os riscos identificados, verificar possíveis melhorias e gerar dados e informações com vistas a subsidiar atualizações, caso necessário.
- Capacitação: é o processo para treinar gestores e servidores nos processos da gestão de riscos e em assuntos relacionados ao tema.
- Comunicação: é o processo para orientar e divulgar informações da gestão de riscos permitindo a interação e comunicação entre as instâncias internas e externas.

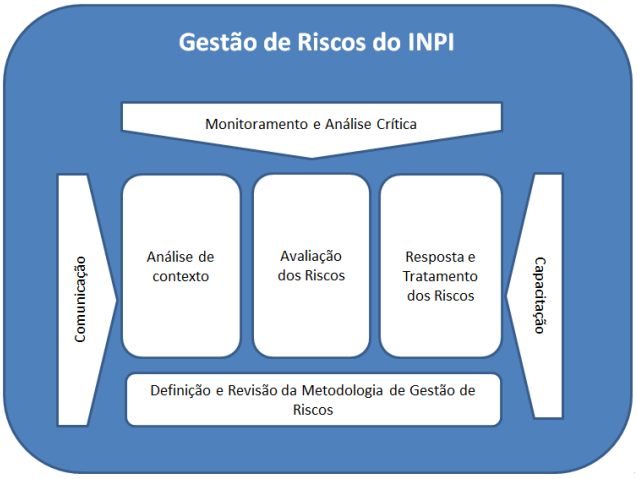


Figura 4 Estrutura de Gestão de Riscos do INPI

6.2 Elaboração do Plano de Gestão de Riscos

Para a elaboração do Plano de Gestão de Riscos, o dirigente máximo de cada unidade determinará a ordem dos processos sob sua responsabilidade a serem analisados, designando aos gestores diretamente responsáveis por eles a responsabilidade pela elaboração deste Plano.

Caso os gestores julguem pertinente, os mesmos poderão designar um servidor que detenha profundo conhecimento no processo em análise para elaborar este Plano, exercendo a função de “analista de risco”; de toda forma, esta delegação não afasta dos gestores dos processos (que são também os gestores dos riscos a eles associados) a responsabilidade pelo resultado da análise.

O Plano de Gestão de Riscos é elaborado através da execução de alguns processos, em um ciclo de melhoria contínua, quais sejam:

6.2.1 Análise de Contexto

Análise de Contexto é desenvolvida para registrar as informações coletadas sobre os aspectos afetos ao processo em que o risco se manifesta, definir os objetivos do processo em questão e o alinhamento destes aos objetivos institucionais mais amplos.

Além disso, refere-se, também, ao entendimento do contexto em que a organização se insere, por meio da identificação dos fatores externos e internos que podem influenciar a capacidade institucional de alcance de resultados planejados, uma vez que as informações obtidas sobre o ambiente, além de contribuir ao entendimento do processo, ajudarão na identificação das fraquezas e riscos, e na escolha das ações para mitigá-los.

O estabelecimento do contexto deve seguir os seguintes passos:

- identificar a qual objetivo institucional o processo está associado;
- identificar quais metas ou resultados associados a este objetivo devem ser alcançados;
- identificar as pessoas envolvidas nos processos e especialistas na área; e,
- mapear os principais fatores internos e externos que podem afetar o alcance dos objetivos/resultados (pessoas, sistemas informatizados, estruturas organizacionais, legislação, recursos, *stakeholders* etc.).

A análise de contexto é uma precondição à identificação de evento, à avaliação de riscos e às respostas aos riscos. Em primeiro lugar, é necessário que os objetivos existam para que se possa identificar e avaliar os riscos quanto a sua realização, bem como adotar as medidas necessárias para administrá-los.

Os resultados do processo de análise do contexto devem ser registrados em planilha e/ou software próprio da gestão de riscos, contendo atributos como:

- Identificação do processo e macroprocesso associado;

- Objetivos, legislação, entradas do processo, partes envolvidas e interessadas, sistemas associados, resultados esperados do processo em análise (Matriz SIPOC do processo); e

- Análise do ambiente interno e externo (Matriz SWOT da organização).

6.2.2 Avaliação dos Riscos

6.2.2.1 Identificação dos Riscos

Este processo consiste em identificar, para cada processo da unidade, os riscos associados, considerando os contextos em que estão inseridos (ambiente interno e externo) e os objetivos do processo.

A identificação dos riscos é de responsabilidade dos gestores dos processos (“donos dos processos”) em que eles se manifestam, e deve-se buscar gerar uma lista que abranja as ameaças ao atingimento do objetivo do processo em análise.

Embora o processo de identificação dos riscos deva ocorrer ao longo da vida do objeto de gestão selecionado – pois antigos riscos podem ser eliminados e novos poderão surgir –, o(s) novo(s) risco(s) identificado(s) deve(m) ser anotado(s) em registros internos e incluído(s) no plano de gestão de riscos nas ocasiões estabelecidas para a revisão do mesmo. Todavia, tal recomendação não afasta do gestor do risco, enquanto gestor público, o dever de tomar as providências imediatas para atuar de forma preventiva (idealmente) ou corretiva quanto à eventual materialização de qualquer novo risco identificado ao longo da execução do plano em vigência (registrando em documento próprio as ações tomadas), pois sua responsabilidade sobre as ameaças ao processo independe de um processo formal de gestão de riscos. De toda forma, é facultado ao gestor do risco, sempre que entender necessário, solicitar a inclusão de novos riscos em seu plano, acompanhado da devida aprovação do dirigente máximo da unidade, sem necessidade de aguardar para fazê-lo somente nas ocasiões estabelecidas para a revisão formal do plano.

A identificação de riscos, segundo a norma ABNT NBR ISO 31000:2009, contempla a busca, o reconhecimento e a descrição de eventos que possam afetar objetivos, as fontes que possam originar tais eventos, as possíveis causas e consequências.

No processo de identificação de riscos, deve-se buscar a participação das pessoas que conheçam bem o objeto de gestão de riscos, além de consultar as partes interessadas para eventuais contribuições.

Vale lembrar que, ainda segundo esse normativo, a identificação de riscos pode envolver dados históricos, análises teóricas, opiniões de pessoas informadas ou especialistas, e as necessidades das partes interessadas.

Ferramentas adequadas devem ser utilizadas para a coleta de informações que auxiliem neste processo de identificação dos riscos. Entre as técnicas que podem ser utilizadas na atividade de identificação de riscos, citamos: entrevistas com as partes interessadas, *brainstormings* a partir de reuniões com uma equipe multidisciplinar, entrevistas com especialistas, questionários e consultas a relatórios contendo histórico de lições aprendidas ou recomendações de Auditoria e Corregedoria do Instituto, elaboração de diagramas de causa e efeito (Diagrama de *Ishikawa*), *Bow Tie*, listas de verificação, análise de cenários, elaboração das matrizes SIPOC e SWOT, por exemplo.

Outra ferramenta muito importante para identificar os riscos é a utilização de processos mapeados como subsídio, que podem ser desenhados em diferentes níveis, chegando até a identificação dos procedimentos, do fluxo de atividades, suas interferências e interdependências mais relevantes para o alcance dos objetivos/resultados que compõem o processo em análise, de modo a obter as informações necessárias sobre o processo de trabalho.

A gestão de riscos dos processos não depende do seu mapeamento[1], embora o mapeamento de processos seja desejável e possa contribuir para a identificação dos riscos, a aplicação desta metodologia independe de os processos estarem formalmente mapeados. O que se pretende, para fins de gestão de riscos, é conhecer o processo de trabalho avaliado, os seus objetivos e as fontes de riscos presentes em suas atividades, sendo certo que quanto mais detalhada for a descrição do processo de trabalho, e quanto mais detalhado for o seu mapeamento (quando houver), mais fácil será a visualização dos eventos que podem ocorrer e afetar os objetivos.

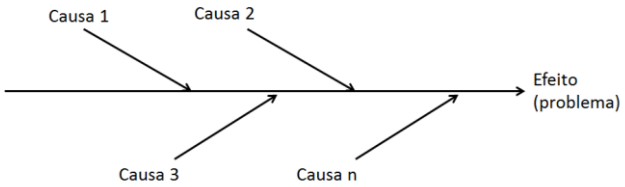


Figura 5 Diagrama de Causa e Efeito *(Ishikawa*)

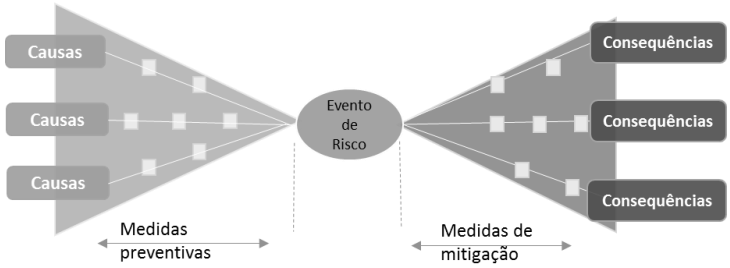


Figura 6 *Bow Tie* para identificar o evento de risco

Como fonte de informação para identificação dos riscos é desejável que se verifique, também, a existência de determinações e recomendações expedidas por meio de Acórdãos ou Decisões do TCU, de recomendações emanadas da CGU, de reclamações registradas na Ouvidoria e de processos judiciais relacionados aos objetos em análise.

Esta análise servirá para embasar, na etapa seguinte, a avaliação sobre o quão provável o risco pode ocorrer (dependendo das causas identificadas, que poderão estar associadas a

1 Conforme afirmado no item 6.2 FUNCIONAMENTO DO SISTEMA DE GESTÃO DE RISCOS do Manual de Gestão de Riscos do TCU (Segepres/Seplan – Brasília, Maio, 2018), disponível na Biblioteca digital do Portal TCU (https://portal.tcu.gov.br/biblioteca-digital/manual-de-gestao-de-riscos.htm).

pessoas, sistemas, processos, infraestrutura, tecnologia e eventos externos, por exemplo) e o grau do impacto que o risco pode gerar (dependendo das consequências identificadas).

Caso o evento de risco esteja associado a duas ou mais categorias de classificação, deverá ser escolhida a categoria que reflita o aspecto mais relevante quanto ao impacto que o evento de risco poderá trazer, caso se materialize. No entanto, sempre que o risco estiver também associado a um aspecto de integridade, este deverá estar registrado em conjunto à sua categoria principal.

6.2.2.1.1 Categoria dos Riscos

A categorização de riscos no INPI seguirá as definições[2] contidas neste manual, quais sejam:

Estratégico: eventos de potencial impacto na missão, metas ou objetivos estratégicos da unidade/Instituto.

Operacional: eventos que podem comprometer as atividades da unidade, normalmente associados a falhas, deficiência ou inadequação de processos internos, pessoas, infraestrutura e sistemas, afetando o esforço da gestão quanto à eficácia e à eficiência dos processos organizacionais.

Orçamentário: eventos que podem comprometer a capacidade da unidade de contar com os recursos orçamentários necessários à realização de suas atividades, ou eventos que possam comprometer a própria execução orçamentária.

Reputação: eventos que podem comprometer a confiança da sociedade em relação à capacidade da unidade em cumprir sua missão institucional; interferem na imagem do INPI.

Social: eventos que podem comprometer o valor público esperado ou percebido pela sociedade em relação ao resultado da prestação de serviços públicos da instituição.

Conformidade: eventos que podem afetar o cumprimento de leis e regulamentos aplicáveis.

Integridade: vulnerabilidade que pode favorecer ou facilitar a ocorrência de práticas de corrupção, fraudes, irregularidades e/ou desvios éticos e de conduta, podendo comprometer os objetivos da instituição[3].

O risco para a integridade, em especial, deve ser classificado segundo as seguintes subcategorias[4]:

- Subcategoria 1: Desvio Ético ou de Conduta
- Subcategoria 2: Ameaças à Isenção e à Autonomia Técnicas
- Subcategoria 3: Conflito de Interesses
- Subcategoria 4: Uso indevido ou manipulação de dados/informações
- Subcategoria 5: Desvio de pessoal ou de recursos materiais
- Subcategoria 6: Corrupção, Fraude, Desvio Irregular de Verbas Públicas

[2] Com base nas recomendações extraídas do Manual de Gestão de Integridade, Riscos e Controles Internos da Gestão, do Ministério Público e na Guia de Gestão de Riscos do Ministério da Economia (2019).
[3] Conforme conceito trazido pelo Art. 2°, inciso II, da Portaria CGU nº 57, de 04 de janeiro de 2019.
[4] Exemplos para cada subcategoria apresentados no Anexo B.

Caso o evento de risco esteja associado a duas ou mais categorias de classificação, recomenda-se que seja analisada a causa de maior relevância para sua ocorrência[5].

Os riscos identificados devem ser registrados em planilha e/ou software próprio de gestão de riscos contendo atributos como:

- Processo no qual o risco foi identificado
- Descrição do Risco
- Causa(s) do Risco
- Consequência(s) do Risco
- Categoria dos Riscos

6.2.2.2 Análise de Riscos

Após a identificação dos riscos, devemos compreender, analisar, e estimar o nível de criticidade de cada um, que pode ser determinado com base na probabilidade (chance de ocorrência) e no impacto (consequências) sobre um ou mais objetivos do processo.

6.2.2.2.1 Matriz de Probabilidade e Impacto (Matriz de Riscos)

A análise dos riscos fornece uma base para a etapa posterior, de planejamento de respostas e tratamento dos riscos, e podemos utilizar como ferramenta para a avaliação global de um conjunto de riscos a Matriz de Probabilidade e Impacto (ou "Matriz de Riscos"), na qual posicionamos e avaliamos as combinações de probabilidade e impacto, gerando, como resultado, uma classificação quanto ao nível de risco para cada evento identificado.

Deve-se buscar compreender o funcionamento das atividades e processos da organização para, então, fazer uma melhor análise qualitativa e quantitativa no momento de "traduzir" em números as chances de ocorrência dos riscos e suas consequências, atribuindo-lhes uma pontuação para cada parâmetro.

Cabe ao gestor do risco (ou ao analista de risco, quando designado) realizar entrevistas internas com a equipe técnica, buscando entender o contexto e analisando indicadores, estatísticas e dados existentes, antes de conferir o grau de relevância.

A utilização de uma escala para probabilidade e impacto pode ser suficiente, vinculando cada nível a uma pontuação de referência.

Avaliação de a **probabilidade** de um risco ocorrer, através da escala:

Grau	Escala	Definições da Escala	Frequência Observada/Esperada
5	Muito alta	Evento esperado que ocorra na maioria das circunstâncias	> 90%
4	Alta	Evento provavelmente ocorra na maioria das circunstâncias	> 50% <= 90%
3	Média	Evento deve ocorrer em algum momento	> 30% <= 50%
2	Baixa	Evento pode ocorrer em algum momento	> = 10% <= 30%
1	Muito baixa	Evento pode ocorrer apenas em circunstâncias excepcionais	< 10%

Tabela 1 Escala de probabilidade

A probabilidade escala-se em cinco níveis, com base em avaliação quantitativa ou qualitativa que utilizará o conhecimento técnico e experiências vivenciadas dos partícipes no processo a ser avaliado, e sempre que possível, será feita uma avaliação quantitativa, com base nos dados estatísticos de eventos de riscos já materializados, por determinado período de tempo ou

[5] Exceto para os casos em que uma das naturezas possíveis do risco for a de integridade, quando esta e a outra categoria mais relevante deverão ser selecionadas no momento da elaboração do plano de gestão de riscos.

média histórica disponível. Nesse caso, é também possível o uso de técnicas de apoio à coleta estruturada de informações.

Avaliação de **impacto** na organização, dada a ocorrência do risco, através da escala:

Grau	Escala	Impacto – fatores para análise		
		Conformidade	Reputação	Negócios/Serviços à Sociedade
		25%	25%	50%
5	Extremo	Impacto no cumprimento de atos que determinam a interrupção das atividades	Com destaque na mídia nacional e internacional, podendo atingir os objetivos estratégicos e a missão	Prejudica o alcance da missão institucional
4	Alto	Impacto no cumprimento de atos de caráter pecuniário (multas)	Com algum destaque na mídia nacional, provocando exposição significativa	Prejudica o alcance da missão da Unidade
3	Médio	Impacto no cumprimento de atos de caráter corretivo	Pode chegar à mídia provocando a exposição por um curto período de tempo	Prejudica o alcance dos objetivos estratégicos
2	Baixo	Impacto no cumprimento de atos de caráter orientativo	Tende a limitar-se às partes envolvidas	Prejudica o alcance das metas do processo
1	Insignificante	Nenhum impacto no cumprimento de normativos que regulamentam o objeto	Impacto apenas interno / sem impacto	Pouco ou nenhum impacto nas metas do processo

Tabela 2 Escala de impacto

Em relação ao impacto, podem ser considerados fatores específicos de análise e respectivos pesos de distribuição, caso o evento de risco ocorra, como:

- Conformidade: refere-se ao tipo de ato normativo que rege o objeto da análise (ou medida correlacionada determinada pelos órgãos de controle) impactado (peso de 25%);
- Reputação: refere-se à imagem institucional (peso de 25%); e,
- Serviços: refere-se à execução das competências institucionais, com reflexo no valor público, resultados e serviços esperados pela sociedade (peso de 50%).

A pontuação dada por escala de criticidade possibilita organizar os riscos em níveis, resultando em uma ordem de priorização: quanto maior sua pontuação, mais crítico e, portanto, maior prioridade deve ser dada ao seu tratamento/gerenciamento.

A análise e classificação quanto ao grau de criticidade dos riscos também é o instrumento que subsidiará a estabelecer respostas preliminarmente definidas para cada nível de risco, de acordo com a atitude da organização perante o risco.

Além disso, sempre que possível, a análise riscos deve ser baseada em evidências objetivas e fundamentadas em informações institucionais e em dados rastreáveis, como documentos, relatórios ou qualquer outra evidência que confira maior confiabilidade na definição dos graus de probabilidade e impacto (e, consequentemente, no nível do risco estimado).

6.2.2.3 Avaliação de Criticidade dos Riscos

Os valores de Probabilidade e Impacto, uma vez aferidos, formam os eixos da Matriz de Riscos, em que se classifica e se avalia o nível do risco, com a combinação dos valores encontrados, podendo resultar em quatro níveis: baixo, médio, alto e crítico.

No processo de avaliação de riscos, deve-se identificar, na matriz probabilidade x impacto, os riscos de acordo com seu respectivo nível e comparar os resultados da análise de riscos

com o limite de exposição a riscos definido pelo INPI, a fim de determinar se o risco é aceitável ou não.

NÍVEL DE RISCO			PROBABILIDADE				
			1	2	3	4	5
			Muito baixa	Baixa	Média	Alta	Muito alta
IMPACTO	1	Insignificante	B	B	B	M	M
	2	Baixo	B	M	M	A	A
	3	Médio	B	M	A	A	C
	4	Alto	M	A	A	C	C
	5	Extremo	M	A	C	C	C

Tabela 3 Modelo de avaliação do risco, considerando probabilidade e impacto

A avaliação dos riscos fornece subsídios para a tomada de decisão, não se constituindo em fator determinante para eventual tratamento do risco.

6.2.2.3.1 Apetite a Riscos

O apetite a risco está diretamente relacionado à estratégia da organização e é levado em conta na ocasião de definir as estratégias, visto que a estas expõem a organização a diferentes riscos. Por isso, o mesmo é definido pelo colegiado designado, e em sua ausência, pelo Presidente do INPI, e seus efeitos se estendem a toda instituição.

Uma operação dentro dos parâmetros de apetite a riscos possibilita à administração maior garantia de que esta permanecerá dentro do limite que está disposta a aceitar, o qual, por sua vez, possibilita um grau mais elevado de confiança para que os seus objetivos possam ser atingidos.

Este limite entre riscos aceitáveis ou não pode ser visualizado graficamente através de uma **linha limite de exposição a riscos** indicada na própria Matriz de Riscos. Este limite de exposição a riscos representa o nível de risco acima do qual é desejável o tratamento do risco.

Assim, as respostas deverão observar o limite de exposição a riscos previamente definido.

No caso do INPI, por ser uma autarquia federal que visa atender à sociedade, prestando serviço público, serão considerados como acima deste limite aqueles riscos classificados como de níveis alto e crítico.

Podemos visualizar a linha limite de exposição a riscos através da Matriz de Riscos a seguir:

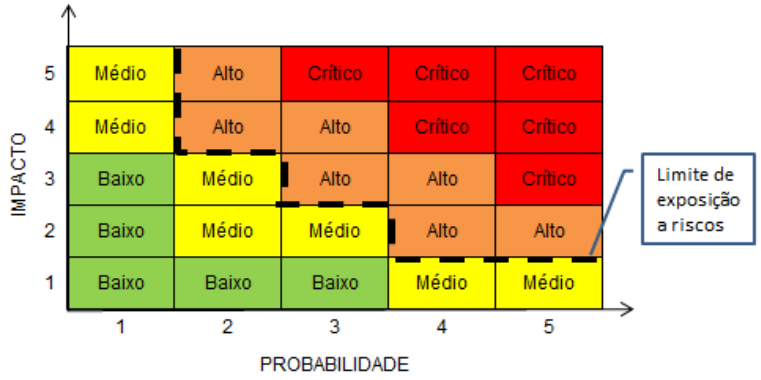


Figura 7 Matriz de Probabilidade x Impacto, demonstrando o apetite a risco do INPI

6.2.2.3.2 Tolerância ao risco

A tolerância ao risco está relacionada à meta do processo ao qual ele pertence, representa a flexibilidade, a margem aceitável tendo a meta do processo em si enquanto referência, sendo, por isso, definida por cada gestor para os resultados dos seus próprios processos.

Assim, o apetite está relacionado aos objetivos da organização (e poderá ser reavaliado quando houver mudança na estratégia do Instituto), e a tolerância, às metas de cada processo.

6.2.2.3.3 Riscos inerentes e residuais

No processo de avaliação dos riscos, é interessante observar a dimensão inerente e residual dos mesmos.

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. Após o levantamento dos riscos inerentes, é necessário levantar e avaliar os controles adotados nos processos.

Risco residual é o risco a que uma organização está exposta após a implementação de ações gerenciais para o tratamento do risco (controles).

Os riscos para os quais não forem verificadas, no momento da análise, medidas de controle existentes, serão classificados como INERENTES ao processo avaliado. Isso ocorre, muitas vezes, quando se está avaliando um processo de trabalho novo, para os quais ainda não foram implementados controles.

Para aqueles em que for possível identificar medida(s) de controle existente(s) e em operação (ou não), serão classificados como RESIDUAIS que, por sua vez, ainda poderão ter seus níveis de criticidade diminuídos através da implementação de controles adicionais – que poderão ser novos ou melhorias de controles já existentes.

No processo de gestão de riscos do INPI, o responsável pela análise pode optar por identificar apenas os riscos residuais ou ambos os riscos.

No entanto, caso o responsável pela análise não tenha muita experiência no processo de gestão de riscos, ainda que não se trate da análise de um processo de trabalho novo, é recomendado que este realize a identificação de ambos os riscos (inerentes e residuais), para fins de fixar os conceitos e amadurecer o entendimento do processo de análise, até que se sinta seguro para realizar a identificação somente dos riscos residuais.

6.2.2.3.4 Controles internos

Controles internos são as ações que a unidade já adota (ou passará a adotar) para responder ao evento de risco, são barreiras implementadas nos processos em que os riscos se manifestam a fim de reduzir a probabilidade e/ou impacto dos mesmos.

A Instrução Normativa Conjunta MP/CGU Nº 01/2016, em seu Art. 2º, inciso V, assim o define os 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.*

6.2.2.3.4.1 Eficácia dos controles e sua maturidade

Devemos classificá-los quanto ao grau de eficácia em relação aos respectivos riscos, conforme as tabelas a seguir.

Desenho
Há procedimento de controle suficiente e formalizado?
a. Não há procedimento de controle;
b. Há procedimentos de controle, mas insuficiente e não formalizado;
c. Há procedimentos de controle formalizado, mas insuficientes;
d. Há procedimentos de controle suficientes, mas não formalizados; ou
e. Há procedimentos de controle suficientes e formalizados.

Operação
Há procedimento de controle sendo executado? Há evidências de sua execução?
a. Não há procedimento de controle;
b. Há procedimentos de controle, mas não são executados;
c. Há procedimentos de controle, mas parcialmente executados;
d. Há procedimentos de controle executados, mas não evidenciados; e
e. Há procedimentos de controle executados de forma evidenciável.

Tabela 4 Desenho e Operação dos controles existentes

Adicionalmente, devemos realizar uma avaliação da maturidade dos controles, a fim de indicar em que medida a Administração gerencia os riscos, que podem ser avaliados quanto a:

Tipo:

• Preventivo: tem como objetivo prevenir a materialização do evento de risco; ou

• Corretivo: tem como objetivo mitigar falha que já ocorreu, apurada após o processamento inicial ter ocorrido.

Natureza:

• Manual: controle realizado por pessoa;

• Automático: controle processado por sistema;

• Híbrido: controle que mescla atividades manuais e automáticas.

Frequência:

• Anual, semestral, bimestral, mensal, diária ou sob demanda.

Os resultados dos processos de análise e avaliação de riscos devem ser registrados em planilha e/ou software próprio de gestão de riscos contendo atributos como:

- Probabilidade de ocorrência de evento de risco;

- Impacto do evento de risco;

- Classificação do risco (nível de risco);

- Matriz de Probabilidade e Impacto (Matriz de Riscos);

- Controles existentes (incluindo tipo e maturidade dos controles).

6.2.3 Resposta e Tratamento dos Riscos

Este processo contempla a definição das respostas aos riscos comparando os resultados encontrados com os critérios para tratamento de riscos previamente definidos neste Manual. A resposta escolhida determina se o risco identificado exige tratamento.

A definição desta resposta deve ser baseada em uma **análise de custo e benefício**, de forma a otimizar a alocação de recursos, e permitir maior alcance do valor público gerado; e, posteriormente, a elaboração das ações de respostas aos riscos, com o objetivo de reduzir a níveis aceitáveis as ameaças levantadas.

O INPI adotará em seu planejamento, as seguintes respostas aos riscos identificados:

- Aceitar (ou tolerar): a organização decide, deliberadamente, não tomar nenhuma medida em relação ao risco. A sua probabilidade e impacto são tão baixos que não justificam a criação de controles para mitigação (o custo de tomar uma ação pode ser desproporcional ao benefício potencial gerado), ou os controles existentes já resguardam boa parte de suas consequências. Ocorre quando o risco está dentro do limite de exposição a risco da organização. Esta opção pode ser suplementada por um plano de contingência – é um plano de ação para conter/minimizar os impactos (consequências) que adviriam caso a ameaça acorra.
- Mitigar (ou reduzir): Mitigar um risco é provavelmente a técnica de gerenciamento de riscos mais utilizada. Também é a mais fácil de compreender e de implementar. Mitigar significa atuar para reduzir a probabilidade e/ou impacto do risco, de modo que mesmo que ele ocorra, o problema gerado é menor e mais fácil de corrigir. Significa restringi-los a um determinado nível aceitável, tornando-o menor ou mesmo removendo-o da lista dos principais riscos. Exemplo: Redundância de recursos.
- Transferir (ou compartilhar): transferência é uma opção de gerenciamento de risco que não é utilizada muito frequentemente, e tende a ser mais comum em projetos onde há várias partes. É o caso especial de se reduzir a consequência e/ou probabilidade de ocorrência do risco por meio da transferência ou compartilhamento de uma parte do risco. Isso pode ser feito através de contratação de seguros ou de cláusulas específicas e garantias em contratos, ou, ainda, através da terceirização de atividades das quais a organização não tem suficiente domínio. É importante notar que alguns riscos não são totalmente transferíveis, como, por exemplo, transferir risco de reputação e imagem, mesmo se a entrega dos serviços foi contratada para um terceiro.
- Evitar (ou eliminar): significa alterar ou reduzir escopos/requisitos, ou não iniciar ou descontinuar atividades/processos para eliminar o objeto sujeito ao risco, eliminando a ameaça na origem. Exemplo: cancelar o projeto.

6.2.3.1 Plano de Tratamento

É um **plano de ação** sobre como mitigar os riscos, definindo para cada risco quem é responsável por implementar os controles.

O propósito do Plano de Tratamento de Risco é exatamente o de definir quais controles precisam ser implementados, quem são os responsáveis por eles, quais são os prazos e quais recursos (i.e. financeiros e humanos) requeridos.

É o gestor do risco o responsável pela elaboração da proposta de tratamento dos riscos associados ao processo sob sua responsabilidade, visando à modificação do nível do risco, de forma a reduzi-lo. Espera-se que, com os resultados do tratamento, o nível de risco residual fique abaixo do limite de exposição.

Para o Processo de Gestão de Riscos do INPI, consideraremos as seguintes ações:

- Nível Baixo: é possível conviver com o risco, mantendo as práticas e controles existentes;
- Nível Médio: é possível promover ações que atenuem causas e/ou consequências;
- Nível Alto: é desejável promover ações para mitigar ou eliminar as causas e/ou consequências;
- Nível Crítico: o nível crítico é aferido nos níveis mais altos de probabilidade e impacto, hipótese em que os gestores responsáveis podem considerar a necessidade de mobilização imediata de recursos, materiais e pessoal capacitado, com vistas ao tratamento desse risco.

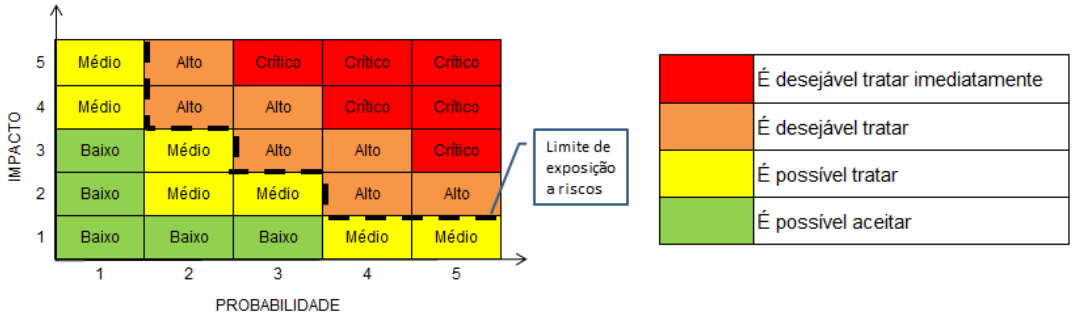


Figura 8 Respostas de acordo com o nível do risco

De todo modo, como já mencionado, a avaliação dos riscos não se constitui em fator determinante para eventual tratamento do risco, sendo permitido ao gestor do processo 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 e validação pelo dirigente máximo da unidade responsável pelo processo.

Por exemplo, quando o nível do risco estiver acima do limite de exposição aceitável, a resposta mais adequada, sempre que possível, deveria ser “evitar”; no entanto, em muitos casos, o processo em que ele se manifesta, existe como atendimento a alguma exigência legal ou por outro motivo inescusável, de modo que não é possível simplesmente “eliminar o objeto sujeito ao risco, eliminando a ameaça na origem” e, assim, evitá-lo. Nesses casos, a recomendação é a de promover ações para mitigar ou eliminar as causas e/ou consequências do risco (tratá-lo), sendo mais urgente quanto mais crítico for o risco.

Da mesma forma, um gestor também pode optar por “aceitar” um risco tido como crítico quando não houver nenhuma ação que possa ser implementada como controle no processo – nestes casos, o gestor pode planejar um “plano B”, ou seja, um plano de contingência que amenize os impactos, caso o risco se concretize.

Assim, deve-se definir a estratégia de tratamento considerando:

- Evitar o risco acima do limite de exposição aceitável quando possível;
- Modificar o nível de exposição por meio de plano de tratamento, conforme estratégia de resposta adotada: transferir ou mitigar o risco;
- Assumir o risco (aceitar) e monitorá-lo dentro do limite de exposição aceitável.

Caso as iniciativas definidas no Plano de Tratamento envolvam mais de uma unidade, o gestor do risco deve encaminhar previamente a proposta de plano à análise e anuência dos gestores das demais unidades; e, após validação pelos mesmos, submeter à aprovação do dirigente máximo da unidade responsável pelo processo.

Após aprovação, o gestor do risco deverá monitorar e assegurar a implementação do Plano de Tratamento (1ª linha de defesa – item 6.3.1.1 Fundamentos do Monitoramento de Riscos - Três Linhas de Defesa).

Destaca-se que é o dirigente máximo da unidade o responsável pelo processo de gestão de riscos daqueles associados aos seus processos de negócio (vide definições apresentadas na Tabela 5 Atribuições e responsabilidades por atividades); sendo, de responsabilidade do dirigente máximo do INPI, o dever de patrocinar, estruturar e efetivar a gestão de riscos do Instituto.

6.3 Monitoramento e Análise Crítica

6.3.1 Monitoramento e Análise Crítica

Identificados os riscos, tendo-os analisados, classificados por criticidades e tendo sido definidas as ações com seus respectivos planejamentos e a priorização, chega-se à etapa em que é necessário ter um controle sobre a execução das ações planejadas, monitorar o comportamento dos riscos ao longo do tempo (se o perfil de risco está mudando), verificar se os riscos identificados ainda existem (ou se novos apareceram), e realizar um constante monitoramento quanto à adequação do perfil de apetite ao risco definido pela organização.

Este processo também inclui tomar as medidas de correção que se mostrarem necessárias na revisão dos Planos de Tratamento e da própria metodologia, estrutura e governança da Gestão de Riscos do INPI; atualizar os registros e documentos gerados; garantir que a gestão de riscos esteja sendo efetiva; e, finalmente, documentar as lições aprendidas.

Desta forma, o processo de monitoramento e análise crítica deve contemplar as seguintes ações:

- monitorar se as ações propostas no Plano de Tratamento de riscos estão sendo executadas conforme planejado;

- analisar se o Plano de Tratamento de riscos está sendo efetivo;

- analisar se o Plano de Tratamento de riscos se precisa sofrer alterações, informando o responsável e frequência de revisão;

- monitorar se houve alguma mudança no contexto ou no processo no qual o risco está associado, no seu nível de risco ou, ainda, se existem novos riscos identificados;

- propor ações corretivas e registrar lições aprendidas, dentre outras informações relevantes (como atividades não programadas e decisões tomadas durante o processo de tratamento dos riscos);

- analisar se o Processo de Gestão de Riscos do INPI está sendo efetivo ou se precisa sofrer alterações; e,

- observar as recomendações das 2ª e 3ª linhas de defesa com vistas a melhorias na gestão dos riscos do processo em análise.

Importante observar que neste processo, novos riscos podem ser criados, excluídos ou modificados riscos já existentes.

6.3.1.1 Fundamentos do Monitoramento de Riscos - Três Linhas de Defesa

É importante observar os seguintes fundamentos para um efetivo processo de monitoramento e controle de riscos, quais sejam:

- que o monitoramento seja realizado de forma contínua, pelos próprios responsáveis pelas atividades e pelos respectivos gestores.

- que haja segregação de funções, tanto na execução de atividades como, também, nas atividades de monitoramento.

Este último é tido como primordial para a excelência do processo de gestão de riscos da organização, e está alinhado com o princípio das “três linhas de defesa”, o qual preconiza a formação de instâncias distintas de monitoramento e revisão da gestão de riscos para garantir a qualidade do processo.

O Modelo das Três Linhas de Defesa separa as responsabilidades administrativas de gestão de riscos (primeira linha de defesa) do papel de outras funções no apoio e supervisão do gerenciamento de riscos (segunda linha) e do papel da auditoria interna em prestar avaliação objetiva (terceira linha).

Primeira linha de defesa: formada pelos gestores da unidade;

Segunda linha de defesa: formada pelas áreas funcionais especializadas em risco, o *Chief Risk Officer*, representado no INPI pela Divisão de Gestão de Riscos – DIGER, bem como colegiados responsáveis pela coordenação da gestão de riscos que venham a ser constituídos; e,

Terceira linha de defesa: formada pela Auditoria Interna do INPI – AUDIT.

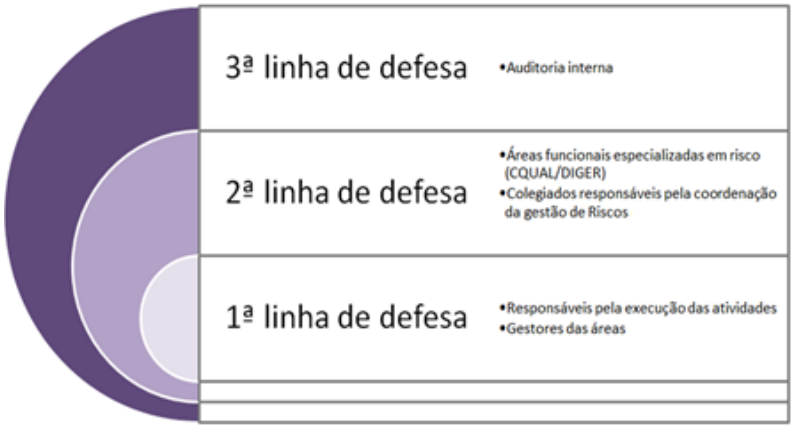


Figura 9 Níveis de Defesa para o Monitoramento e Controle da Gestão de Riscos

6.3.1.2 Reuniões de Monitoramento

Cada unidade deve realizar reuniões de acompanhamento, onde serão discutidas e verificadas as questões mencionadas anteriormente. Nos casos em que os riscos sejam classificados como de nível acima do limite de exposição a riscos do INPI, é importante que essas reuniões ocorram com maior frequência, e produzindo relatórios de monitoramento mais detalhados.

Essas reuniões devem ser convocadas pelos gestores dos processos com a frequência a ser definida no Plano de Gestão de Riscos da própria unidade, assim como, a nível institucional, pelos colegiados relacionados à gestão de riscos, em consonância com suas atribuições previstas em normativos próprios. Além disso, o monitoramento dos Planos de Tratamento dos riscos mais críticos deve ser acompanhado em conjunto ao planejamento estratégico da organização.

Os resultados do processo de monitoramento e análise crítica de riscos devem ser registrados em planilha e/ou software próprio de gestão de riscos contendo atributos como:

- Relatórios de monitoramento e análise crítica;
- Notas técnicas; e
- Recomendações às unidades.

6.4 Capacitação

Este processo tem como objetivo capacitar na metodologia e uso de ferramentas os servidores diretamente envolvidos no processo de gestão de riscos de suas unidades, através da execução de um Plano de Capacitação – que deve ser elaborado pela DIGER/CQUAL – em parceria com a CGRH, registrando as ações realizadas e pessoal capacitado.

Estas capacitações também deverão ocorrer em temas correlatos à gestão de riscos cujo conhecimento adquirido agregará valor à execução da gestão de riscos por esses agentes públicos.

6.5 Comunicação

Conforme apresentado na Norma ABNT NBR ISO 31000:2009, este processo consiste em um método interativo que uma organização realiza para fornecer, compartilhar ou obter informações necessárias para dialogar com as partes interessadas, relacionadas com a gestão de riscos.

Neste processo, o objetivo é estabelecer e manter a comunicação com as partes interessadas (internas e externas), para informá-las ou consultá-las sobre riscos.

Importante destacar que todos os agentes públicos do Instituto devem conhecer a estrutura de governança em gestão de riscos do INPI, suas diretrizes e política, uma vez que para garantir a eficiência do processo, é necessário que possam ter um nível de conhecimento mínimo que lhes permita contribuir reportando aos gestores dos riscos de sua unidade quaisquer mudanças ou fragilidades identificadas no(s) processo(s) em que está inserido; para tanto, deve ser elaborado e executado um Plano de Comunicação, de responsabilidade da CQUAL/DIGER, que deverá contemplar o planejamento das ações de comunicação e disseminação.

Assim como sugerido nas etapas anteriores, convém que esta atividade seja realizada continuamente, desde a fase inicial de planejamento do processo de gestão de riscos e durante toda a sua implementação e controle, para que seja, de fato, efetiva.

7 Atribuições e Responsabilidades

No INPI, todas as diretorias e unidades ligadas à Presidência deverão identificar os riscos de seus processos conforme relevância, e seguindo as diretrizes apresentadas em todas as etapas anteriores.

Todo o material referente à gestão dos riscos das unidades deverá estar disponível para ciência e formação de banco de dados da CQUAL (especialmente quanto às estatísticas de ocorrência dos eventos de risco previstos e realizados), que também atuará dando suporte e assessoramento técnico em todas as etapas do processo de Gestão de Riscos, oferecendo capacitação e prestando o apoio quando demandado pelas áreas.

Os papéis e atribuições podem ser visualizados na tabela a seguir:

Responsável	Atribuições
Todas as unidades do INPI	• Devem **identificar e avaliar** os riscos de todos os seus processos, priorizando os mais críticos, podendo tratá-los se for o caso.
Todos os servidores do INPI	• Operacionalizam os Planos de Tratamento de riscos definidos para os processos em que estiverem envolvidos; • Reportam aos gestores de processos quaisquer mudanças ou fragilidades identificadas naquele(s) processo(s) em que estiverem envolvidos.
Analista de riscos	• Servidor designado pelo gestor do risco (quando julgar pertinente) e que atua sob sua supervisão no apoio à elaboração do Plano de Gestão de riscos em que estiver envolvido (seguindo os procedimentos estabelecidos neste Manual).
Gestor do risco	• Servidor ocupante de cargo em comissão ou função comissionada responsável pela elaboração (e revisão) dos Planos de Gestão de riscos dos processos sob sua gerência imediata, podendo delegar esta atividade ao analista de risco; • É o gestor do processo em que o risco se manifesta; • Atua como a "1ª linha de defesa" do processo de gestão de riscos de suas unidades (monitoramento contínuo); • Acompanha e assegura que os Planos de Tratamento estejam sendo executados e efetivos; • Responsável por manter atualizados os registros de trabalho e documentos gerados, registrando, inclusive, as lições aprendidas; • Propõe ao dirigente máximo da unidade a revisão dos Planos de Gestão de riscos sob sua gerência imediata ao final do ciclo do processo de gestão de riscos.
Dirigente máximo da unidade	• É quem aprova os Planos de Gestão de Riscos associados aos processos sob sua responsabilidade; • Determina a ordem dos processos sob sua responsabilidade para a realização da gestão de riscos; • Deve integrar e utilizar as informações e resultados gerados pela gestão de riscos na elaboração do planejamento estratégico e na melhoria contínua dos processos organizacionais de sua unidade.
Interlocutor da unidade organizacional	• Atua como "ponto focal", faz a interlocução entre os Gestores dos Processos de sua unidade e a CQUAL/DIGER.
DIGER	• Atua como a "2º linha de defesa" do processo (apoio e supervisão) de gestão de riscos do INPI, indicando eventuais atrasos, alterações etc.; • Emite recomendações para o aprimoramento da governança, gestão de riscos e dos controles internos; • Apoia, tecnicamente, o processo de elaboração dos Planos de

	Gestão de Riscos das unidades, quando solicitado; • Acompanha e monitora a execução dos Planos de Tratamento para os riscos que estiveram situados acima do limite de exposição a riscos do INPI, juntos aos interlocutores das unidades organizacionais; • Mantém atualizado o Banco de Riscos do INPI.
CQUAL	• Elabora propostas de política, diretrizes, metodologias e mecanismos para a comunicação e institucionalização da gestão de riscos do INPI; • Assessorar tecnicamente a instância colegiada e ao Presidente do INPI em matéria de gestão de riscos; • Garante que as informações adequadas sobre os riscos estejam disponíveis em todos os níveis da organização.
Instância colegiada formada pelo Dirigente Máximo e dirigentes a ele diretamente subordinados	• Aprovar, quando necessária, política de gestão de riscos do INPI, bem como normas e métodos complementares; • Promover o desenvolvimento contínuo dos agentes e incentivar a adoção de boas práticas de governança e de gestão de riscos; • Promover a integração dos agentes responsáveis pela gestão de riscos; • Estabelecer limites de exposição a riscos e de alçada para gerenciamento dos riscos; • Aprovar e supervisionar método de priorização de processos para gerenciamento de riscos; • Zelar pela eficácia, eficiência e efetividade do processo de gerenciamento de riscos.
Presidente do INPI	• Aprova política de gestão de riscos do INPI, bem como normas e métodos complementares, quando na ausência do colegiado designado para tal; • Patrocinar, estruturar e efetivar a gestão de Riscos do INPI.
Auditoria Interna	• Avaliar os processos de gestão de riscos e controles, em especial: adequação e suficiência dos mecanismos de gestão de riscos e de controles estabelecidos; eficácia da gestão dos principais riscos; e conformidade das atividades executadas em relação à Política de Gestão de Riscos do INPI.

Tabela 5 Atribuições e responsabilidades por atividades

8 Considerações finais

A gestão de riscos é um processo dinâmico, contínuo e essencial para a boa governança de qualquer organização. Além disso, ela auxilia sobremaneira os gestores na tomada de decisões.

É fortemente recomendável que todas as organizações tenham um controle estratégico bem estruturado e competente, capaz de gerir os seus diversos indicadores de desempenho e qualidade. E a definição de uma política e procedimentos para a gestão de riscos possibilita diagnosticar, priorizar, monitorar e gerir as possíveis ameaças aos objetivos estratégicos.

Estar atento e preparado para as incertezas é a única forma de evitar ser surpreendido por situações repentinas e sobre as quais não se tem controle, em qualquer ramo de negócio, mas em especial, no setor público, de cujos serviços e entregas dependem toda a sociedade.

Os casos omissos e/ou não previstos neste manual devem ser encaminhados à Coordenação-Geral de Qualidade, para avaliação e proposições de ajustes.

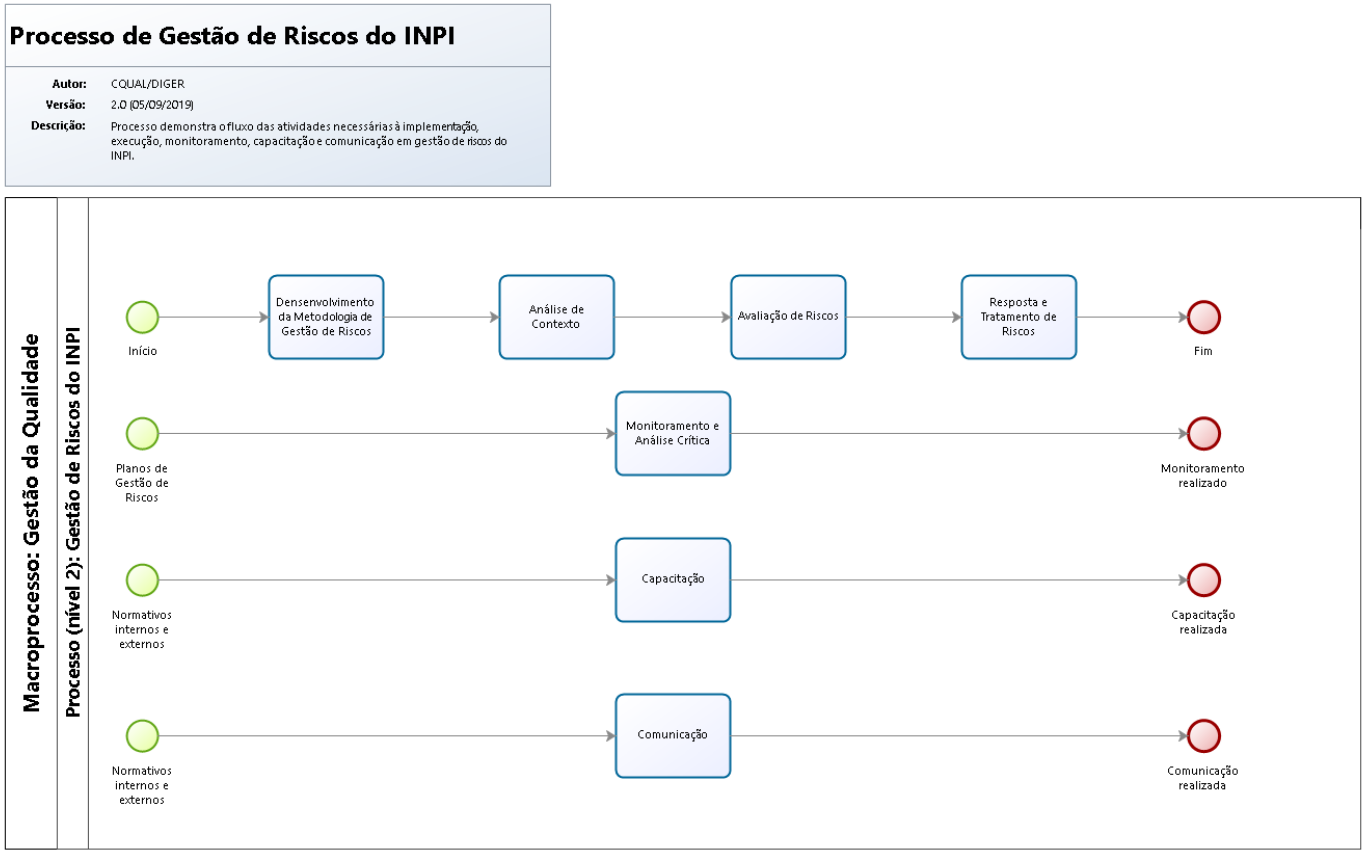
9 Entradas do processo

As entradas do processo são apresentadas na Matriz SIPOC de Gestão de Riscos – Anexo C.

10 Saídas do processo / resultados esperados

As saídas do processo são apresentadas na Matriz SIPOC de Gestão de Riscos – Anexo C.

11 Fluxo do processo



12 Indicadores do processo

Ainda não existem indicadores deste processo.

13 Governança

N/D

14 Glossário

Siglas

INPI – Instituto Nacional da Propriedade Industrial

ABNT – Associação Brasileira de Normas Técnicas

NBR – Norma Brasileira

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

CQUAL – Coordenação-Geral da Qualidade

DIGER – Divisão de Gestão de Riscos

TCU – Tribunal de Contas da União

CGU – Controladoria-Geral da União

COSO – The Comitee of Sponsoring Organizations

AUDIT – Auditoria Interna do INPI

Termos e Definições

Processo: conjunto ordenado de atividades de trabalho, no tempo e espaço, com início e fim, além de entradas e saídas bem definidas, que são executadas para alcançar produto, resultado ou serviço predefinido.

Governança: conjunto de mecanismos de liderança, estratégia e controle postos em prática para avaliar, direcionar e monitorar a gestão, com vistas à condução de políticas públicas e à prestação de serviços de interesse da sociedade.

Objetivo organizacional: situação que se deseja alcançar de forma a se evidenciar êxito no cumprimento da missão e no atingimento da visão de futuro da organização.

Meta: alvo ou propósito com que se define um objetivo a ser alcançado.

Risco: possibilidade de ocorrência de um evento que venha a ter impacto no cumprimento dos objetivos dos processos ou institucionais. O risco é medido em termos de impacto e de probabilidade.

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

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

Gestão de riscos: conjunto de princípios, estruturas, alçadas, processos e atividades coordenados para dirigir e controlar uma organização no que se refere a riscos.

Gerenciamento dos riscos: processo para identificar, avaliar, administrar e controlar potenciais eventos ou situações e fornecer segurança razoável no alcance dos objetivos organizacionais.

Estrutura da gestão de riscos: 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.

Política de Gestão de Riscos: declaração das intenções e diretrizes gerais de uma organização relacionadas à gestão de riscos.

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 dos riscos.

Atitude perante o risco: abordagem da organização para avaliar e eventualmente buscar, reter, assumir ou afastar-se do risco.

Limite de exposição a riscos: representa o nível de risco acima do qual é desejável o tratamento do risco.

Apetite a risco: nível máximo de risco que a Instituição aceita incorrer para atingir seus objetivos.

Tolerância a risco: nível máximo de risco e as restrições específicas aplicáveis a cada tipo que o gestor do risco está disposto a assumir.

Contexto externo: ambiente externo no qual a organização busca atingir seus objetivos.

Contexto interno: ambiente interno no qual a organização busca atingir seus objetivos.

Identificação de riscos: processo de busca, reconhecimento e descrição de riscos.

Fonte de risco: elemento que, individualmente ou combinado, tem o potencial intrínseco para dar origem ao risco.

Evento: ocorrência ou mudança em um conjunto específico de circunstâncias (pode ser positivo/benéfico ou negativo/prejudicial).

Impacto: efeito resultante da ocorrência do evento.

Consequência: resultado de um evento que afeta positiva ou negativamente os objetivos.

Probabilidade: chance de um evento ocorrer.

Gestor do risco: Servidor ocupante de cargo em comissão ou função comissionada responsável pela elaboração (e revisão) dos Planos de Gestão de riscos dos processos sob sua gerência imediata; é também o gestor do processo em que o risco se manifesta.

Analista de riscos: Servidor designado pelo gestor do risco e que atua sob sua supervisão no apoio à elaboração do Plano de Gestão de riscos em que estiver envolvido.

Análise de riscos: processo de compreender a natureza do risco e determinar o nível de risco.

Nível de risco: magnitude de um risco ou combinação de riscos, expressa em termos da combinação das consequências e de suas probabilidades.

Tratamento de riscos: processo para modificar o risco.

Controle: medida que está modificando o risco.

Controle interno: conjunto de processos estruturados para mitigar os possíveis riscos com vistas ao alcance dos objetivos institucionais, e para garantir a execução ordenada, ética, econômica, eficiente e eficaz das atividades da organização, com preservação da legalidade e da economicidade no dispêndio de recursos públicos.

Medida de controle: medida aplicada pela organização para tratar os riscos, aumentando a probabilidade de que os objetivos e as metas organizacionais estabelecidos sejam alcançados.

Monitoramento: verificação, supervisão, observação crítica ou identificação da situação, executadas de forma contínua, a fim de identificar mudanças no nível de desempenho requerido ou esperado.

15 Dono do documento

Helena Acácio Santini Pereira, Chefe da Divisão de Gestão de Riscos, DIGER/CQUAL/DIREX.

16 Elaborador(es) do documento

Pedro Henrique Fernandes Pinto, Analista de Planejamento, Gestão e Infraestrutura em PI, servidor da Divisão de Gestão de Riscos, DIGER/CQUAL/DIREX;

Helena Acácio Santini Pereira, Chefe da Divisão de Gestão de Riscos, DIGER/CQUAL/DIREX;

Alessandro Bunn Bergamaschi, Coordenador-Geral da Qualidade, CQUAL/DIREX.

17 Aprovador do documento

Cláudio Vilar Furtado, Presidente do INPI.

18 Bibliografia

Guia de Gestão de Riscos do Ministério da Economia, 2019.

Manual de Gestão de Riscos do TCU, Segepres/Seplan – Brasília, Maio, 2018.

Manual para Implementação de Programas de Integridade (Orientações para o setor público) – CGU, 2017.

Manual de Gestão de Integridade, Riscos e Controles Internos da Gestão – Ministério do Planejamento, 2017.

Modelo de Gestão de Riscos para o TCU – Tribunal de Contas da União, 2015.

Projeto de Desenvolvimento do Guia de Orientação para o Gerenciamento de Riscos – Ministério do Planejamento, 2013.

ABNT NBR ISO 31000:2009 – Gestão de riscos – Princípios e diretrizes, 2009.

The Orange Book Management of Risk - Principles and Concepts. Londres, Reino Unido: Her Magesty's Treasury, 2004.

Internal Control - Integrated Framework. The Committee of Sponsoring Organizations of the Treadway Commission - COSO, 2004.

MODELO DE EXCELÊNCIA DO SISTEMA DE GESTÃO PÚBLICA – Secretaria de Gestão Publica – Ministério do Planejamento, Orçamento e Gestão.

19 Histórico das alterações

A cada revisão no procedimento, a tabela abaixo deverá ser preenchida de forma a manter o histórico das alterações.

Data	Nº revisão	Item	Descrição
26/03/2020	0001	Todos	Este documento refere-se à segunda edição do Manual de Gestão de Riscos do INPI (embora esta seja a primeira versão no formato definido pelo Sistema de Padronização de Documentos), tendo sido substancialmente revisado com o objetivo de se alinhar às orientações emitidas pelo Ministério da Economia, através do Guia de Gestão de Riscos do Ministério da Economia, 2019.

20 Anexos

Anexo A – Exemplos de Riscos à Integridade

Conjunto de 29 riscos que podem ser considerados como insumo para a gestão de riscos para a integridade em cada órgão e entidade do Ministério da Economia:

- Subcategoria 1: **Desvio Ético ou de Conduta**

1. Atraso no andamento dos trabalhos, por conduta profissional dissonante dos interesses institucionais.

2. Execução de atividades alheias ao serviço, durante o expediente.

3. Uso do cargo ou função para favorecimento pessoal ou de terceiros.

4. Não realização das atribuições com zelo, dedicação, presteza, responsabilidade e qualidade.

5. Não cumprimento da carga horária, ou ausência do trabalho, sem prévio aviso ou autorização da chefia.

6. Omissão do servidor em denunciar ou representar ocorrência de irregularidade.

7. Assédio moral ou sexual, preconceito (raça, gênero, religião, origem, orientação sexual).

- Subcategoria 2: **Ameaças à Isenção e à Autonomia Técnicas**

8. Desconsideração da posição técnica na tomada de decisão.

9. Direcionamento na seleção de pessoas ou empresas prestadoras de serviços.

10. Emissão de parecer técnico tendencioso, em desconsideração às evidências constantes em processo.

11. Omissão deliberada de informações relevantes em parecer ou instrução técnica encaminhada para tomada de decisão.

12. Emissão de pareceres quando há impedimento ou suspeição.

13. Fragilização ou desconsideração da atuação da Gestão de Risco.

- Subcategoria 3: **Conflito de Interesses**

14. Prestação de serviços profissionais particulares pelo agente público, em conflito com as atribuições da função pública ou do órgão.

15. Ato ou omissão do servidor por influência externa, em detrimento do interesse público – “risco de captura”.

16. Influência indevida na contratação de terceiros – nepotismo.

17. Designação de funções críticas a um mesmo servidor – falta de segregação de funções.

18. Participação do servidor ou gestor em decisão de que é beneficiário particular – conflito de interesses.

- Subcategoria 4: **Uso indevido ou manipulação de dados/informações**

19. Acesso ou concessão de acesso indevido aos dados e informações, inclusive com uso de persuasão e eventual ingenuidade dos usuários – "engenharia social" –, devido à ausência de cultura de segurança da informação e comunicação.

20. Acesso ou concessão de acesso a dados ou informações restritas para uso ou divulgação indevida.

21. Manipulação e alteração de dados e informações para benefício próprio ou de terceiros.

- Subcategoria 5: **Desvio de pessoal ou de recursos materiais**

22. Desvio de função de estagiários, servidores, terceirizados e contratados.

23. Utilização de recursos logísticos e materiais em finalidade estranha às necessidades do serviço.

24. Ingerência em contratações, a fim de obter benefícios próprios ou em favor de terceiros.

25. Utilização da administração pública para fins eleitorais.

- Subcategoria 6: **Corrupção, Fraude, Desvio Irregular de Verbas Públicas**

26. Influência indevida de interesses privados nas decisões ou procedimentos de órgãos singulares ou colegiados.

27. Direcionamento de normas ou da atuação do órgão para favorecimento de interesses privados.

28. Indícios de enriquecimento ilícito e/ou lavagem de dinheiro.

29. Indícios de fraudes em processos licitatórios.

Fonte: Resolução CRTCI nº 3, de 27 jun. 2018.

Anexo B – Exemplos de Eventos de Risco Operacional

Conjunto exemplificativo de eventos de risco operacional, quanto aos fatores de processos, pessoas, ambiente tecnológico e eventos externos.

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; e
- 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 avaliações periódica sobre a adequabilidade do desenho do processo;
- Ausência ferramenta para análise e melhoria contínua do processo; e
- 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; e
- 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[6]
- Descumprimento de prazo judicial na execução do processo; e
- 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; e
- 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; e
- 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; e

[6] Este evento também pode se enquadrar como um exemplo de risco para a integridade, segundo conceito trazido pela Portaria CGU nº 57, de 07 de janeiro de 2019.

- 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; e
- 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; e
- 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; e
- 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; e
- 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; e
- Incompatibilidade e/ou indisponibilidade de informações afetando a execução do processo.

EVENTOS EXTERNOS

DESASTRES NATURAIS E CATASTROFE:

- 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; e
- 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; e
- 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; e
- Falhas ou indisponibilidade de serviços públicos que afeta a execução do processo.

Fonte: Resolução CRTCI nº 3, de 27 jun. 2018.

Anexo C – Matriz SIPOC da Gestão de Riscos

INSTITUTO NACIONAL DA PROPRIEDADE INDUSTRIAL

Atualizado em: 09/10/2019

Macroprocesso Gestão da Qualidade

Processo (nível 2) Gestão de Riscos

Objetivos do Processo Gerenciar os riscos de forma integrada com os agentes responsáveis pela governança, a fim de alcançar os objetivos do INPI e garantir a qualidade dos serviços.

Fornecedores (S)	Entradas (I)	Processos / Atividades críticas (nível 3)	Saídas (O)	Clientes (C)
- Ministério da Economia - Órgãos de controle - Comitês internos de governança e gestão de riscos - Auditoria interna - CGPE	- Política de Gestão de Riscos - Definições e recomendações exaradas pelos Comitês de Gestão de Riscos - Normativos externos referentes à governança e gestão de riscos - Regimento Interno do INPI	Desenvolvimento da metodologia de gestão de riscos	- Metodologia de gestão de riscos do INPI definida e aprovada - Manual de Gestão de Riscos publicado e atualizado	- Comitês de gestão de riscos - Gestores - Corpo funcional do INPI
- CGPE - Auditoria Interna - Corregedoria - Ouvidoria - Diretorias e órgãos seccionais	- Ordem de priorização de processos da unidade - Planejamento Estratégico do INPI (Matriz SWOT) - Planejamento setorial da unidade - Relatórios das instâncias de integridade - Normativos internos e externos referentes ao processo em análise - Estrutura de governança do Instituto - Política de Gestão de Riscos - Metodologia de Gestão de Riscos	Análise de Contexto	- Diagnóstico do ambiente interno e externo (incluindo manutenção ou atualização da Matriz SWOT do INPI) - Identificação das principais partes interessadas no objetivo do processo	- Gestores - Pessoas envolvidas - Dirigente máximo da unidade
- Gestores	- Diagnóstico do ambiente interno e externo - Manual de Gestão de Riscos do INPI - Processo mapeado Relatórios com os riscos para a integridade Normas internas e externas relacionadas ao processo	Avaliação de riscos	Riscos identificados, analisados e avaliados: Processos; Iniciativas; Ações;	- Dirigentes - Gestores - Pessoas envolvidas - Comitês de Governança
- Gestores	- Riscos identificados, analisados e avaliados	Resposta e Tratamento de Riscos	- Plano de Tratamento dos riscos elaborado e aprovado - Plano de Gestão de Riscos elaborada e/ou atualizada (completo, incluindo os planos de tratamento) - Banco de Riscos do INPI atualizado (contendo até a avaliação de riscos)	- Gestores - Pessoas envolvidas - Agentes públicos das unidades impactadas pelo risco - Comitês de Governança
- Gestores	- Planos de Tratamento dos riscos aprovados - Plano de Gestão de Riscos da unidade atualizada - Banco de Riscos do INPI atualizado - Processo mapeado	Monitoramento e Análise Crítica	- Relatórios de monitoramento e análise crítica - Relatórios de Status dos Riscos - Notas técnicas - Recomendações às unidades - Verificação de necessidade de atualização/revisão da estrutura de governança e metodologia de gestão de riscos do INPI	- Comitês de Governança - Gestores - Corpo funcional do INPI
- DIGER - Órgãos de controle - Gestores - Instâncias de governança	- Relatórios de monitoramento e análise crítica - Notas técnicas - Recomendações às unidades - Manual de Gestão de Riscos - Normativos internos e externos	Capacitação	- Planejamento de Capacitações - Capacitação realizada - Relatórios das capacitações	- Pessoas envolvidas - Gestores - Órgãos de controle e Auditoria Interna
- DIGER - Órgãos de controle - Gestores - Instâncias de governança	- Relatórios de monitoramento e análise crítica - Notas técnicas - Recomendações às unidades - Política de Gestão de Riscos - Manual de Gestão de Riscos - Normativos internos e externos	Comunicação	- Planejamento das ações de comunicação - Comunicação realizada - Relatórios das ações de comunicação - Intranet e Portal atualizados	- Corpo funcional do INPI - Gestores - Órgãos de controle e Auditoria Interna - Fornecedores, usuários e demais partes interessadas