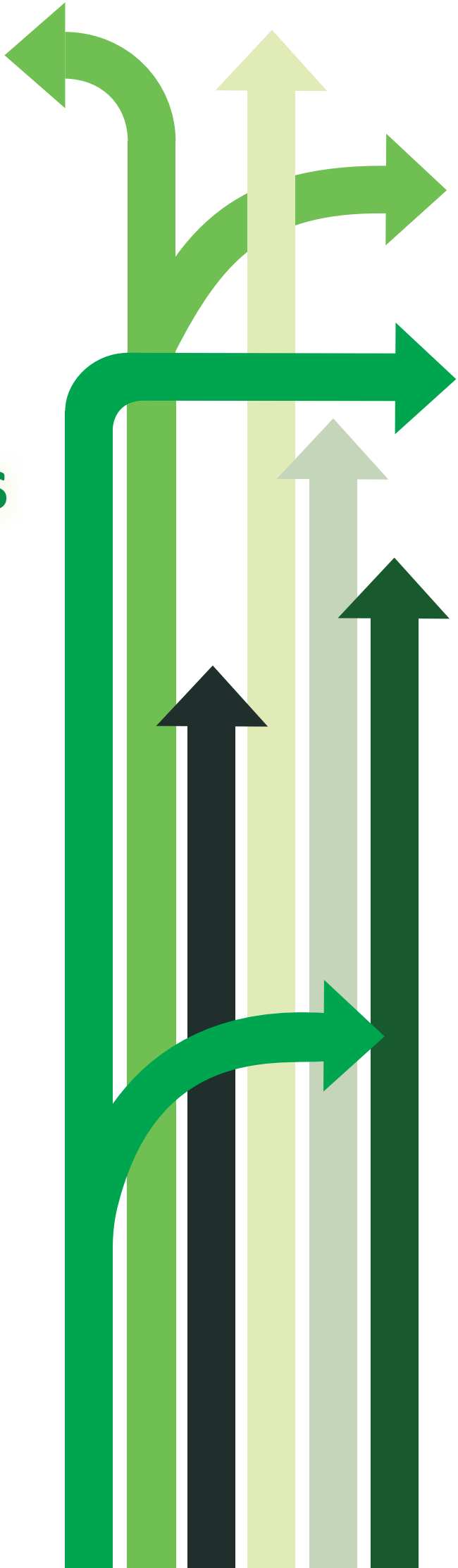
Política de Gestão de Riscos Corporativos

Manual de Procedimentos e Análise de Gestão de Riscos Corporativos



CORSAN

Versão 1.00

FOLHA DE CONTROLE

Título	Manual de Procedimentos e Análise de Gestão de Riscos Corporativos, anexo à Política de Gestão de Riscos Corporativos
Número de versão	1
Status	Lançamento
Autoria	Superintendência de Controles Internos e Gestão de Riscos
Pré-aprovação	Diretoria Colegiada
Data de aprovação	13.03.2017
Instrumento de homologação (pré-aprovação)	Ata 14/2017
Aprovação	Conselho de Administração
Data de aprovação	19.05.2017
Instrumento de homologação	Ata 09/2017

Histórico de versionamento

Versão	Motivo	Data	Autoria
1	Versão inicial	19.05.2017	SUCIR

SUMÁRIO

1. INTRODUÇÃO

A organização está comprometida com seus clientes, acionistas e com a sociedade em que atua, focando esforços em reduzir os riscos existentes e/ou os que possam se manifestar no futuro e também na maximização das oportunidades de negócio. Para tanto, é necessário conhecer os riscos que a afetam e seus impactos sobre todas as partes interessadas - os *stakeholders*. Os riscos permeiam todos os níveis das atividades do negócio e, se não forem gerenciados adequadamente, poderão resultar em perdas financeiras, deterioração da imagem e reputação da organização e ou desencadear uma crise. A gestão de riscos tem se tornado um assunto de suma importância no meio empresarial, uma vez que a conscientização da necessidade de administração dos riscos potenciais é, hoje, uma questão de competitividade e sobrevivência. Para que seja eficaz, a gestão de riscos deve fazer parte da cultura da organização e deve estar inserido em sua filosofia, nas práticas e nos processos de negócio. As organizações que gerenciam seus riscos de maneira eficaz e eficiente têm maior probabilidade de atingir seus objetivos, a um custo total menor.

2. POLÍTICA CORPORATIVA PARA A GESTÃO DE RISCOS

Cumprindo seu compromisso com seus clientes, acionistas, a sociedade, colaboradores diretos e indiretos, a organização posiciona a gestão de riscos como um desafio indispensável para as operações do negócio bem como para manter e melhorar seu valor corporativo. Como os riscos têm se diversificado e aumentado, estes serão aceitos como oportunidades para a criação de um sistema de gerenciamento fortalecido, visando o crescimento e a prosperidade da organização. Ao mesmo tempo, a organização cumprirá suas responsabilidades com relação aos seus *stakeholders* com o objetivo de conquistar ainda mais a confiança dos clientes com relação à marca organização.

3. VISÃO GERAL DA GESTÃO DE RISCOS

O método de gestão de riscos corporativos escolhido pela organização possui como elementos principais do processo o mostrado na figura 1, que estão alinhados com a Norma ISO 31000. Os elementos principais do processo estão integrados no ciclo do P (*plan*) D (*do*) C (*check*) A (*act*).

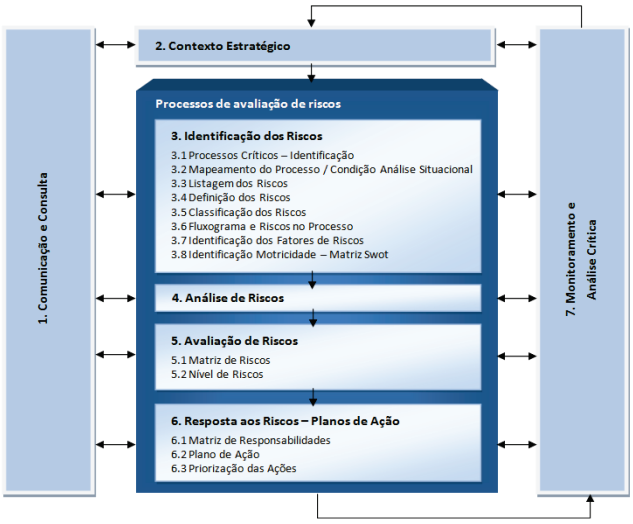


Figura 1: Adaptado da ISO 31000

4. REAVALIAÇÃO DO PROCESSO DE GESTÃO DE RISCOS

As áreas e departamentos da organização devem revisar seus riscos, através do processo de gestão de riscos corporativos descritos nesta política, a cada semestre, com o objetivo de monitorar os riscos e os fatores de riscos do ambiente interno e externo.

5. FASES DO PROCESSO DE GESTÃO DE RISCOS CORPORATIVOS

5.1. Comunicação e consulta

Trata-se, aqui, das formas como se vai estabelecer o processo e a estratégia de comunicação com as partes interessadas. É uma fase que permeia todo o processo de gestão e análise de riscos. É extremamente estratégico, pois sem a comunicação não vai existir processo de gestão de riscos tendo em vista não sensibilizar os usuários do processo. A organização decide utilizar sua área de comunicação corporativa para operacionalizar o processo de comunicação dos riscos corporativos.

5.2. Contexto estratégico

O estabelecimento do contexto é dividido em duas etapas:

A primeira etapa diz respeito ao entendimento da área que está fazendo a gestão de riscos em compreender os objetivos estratégicos e organizacionais da organização. Importante que essa etapa esteja alinhada ao planejamento estratégico da empresa (políticas, objetivos, missão, valores e estratégias implementadas na organização).

A segunda etapa aborda as variáveis externas incontroláveis que poderão interferir ou expor os objetivos estratégicos da organização, integrado com a gestão de riscos. Cada área da organização deverá construir seus cenários de riscos estratégicos. O resultado dessa construção de cenários deve ser incorporado no diagrama de causa e efeito, na macrocausa do ambiente externo.

5.3. Identificação dos riscos

A identificação dos riscos possui como subfases sete, todas interligadas e interdependentes, com o objetivo de as principais causas dos riscos versus os processos críticos de cada área da organização, mas alinhada com a visão estratégica e seus respectivos objetivos.

5.3.1. Processos críticos – identificação

O gestor de cada área da organização deve realizar a priorização dos seus processos de negócio ou atividade utilizando dois critérios:

a. Impacto no negócio

b. Tempo de tolerância

5.3.2. Mapeamento do processo/condição - análise situacional

O objetivo do mapeamento do processo é descrever passo a passo. A análise situacional é realizada no processo mapeado. O gestor deve percorrer o processo, ou seja, fazer o *walkthrough* com o objetivo de identificar pontos fortes e fracos, que sirvam de fatores para mitigar ou potencializar a concretização dos riscos, classificando como controles eficientes ou

ineficientes. Nessa fase é necessário evidenciar as fragilidades, mapear histórico de ocorrências (caso exista) e comprovar a funcionalidade dos controles.

Mapeamento do processo			Análise situacional		
Processo	Área	Atividade	Controle		Histórico/evidência
			Descrição da atividade e controles	Status (eficiente ou ineficiente)	
Nome do processo	Área em que ocorre o processo	1			
		2			
		3			
		4			
		5			

5.3.3. Listagem de Riscos

A listagem deve ser realizada através de reuniões do tipo *brainstorming*, levantando tanto os riscos conhecidos como os desconhecidos. Os riscos desconhecidos são aqueles que nunca aconteceram na organização, porém são riscos exequíveis, ou seja, poderão ocorrer.

5.3.4. Definição dos Riscos

Os riscos devem ser definidos e classificados de acordo com o dicionário de riscos de cada área da organização, aplicáveis ao seu negócio.

5.3.5. Classificação dos Riscos

Os riscos identificados devem ser classificados em categorias e para cada um deve-se dar um nome para codificação e referência. A organização decidiu a seguinte classificação de riscos:

5.3.5.1. **Estratégicos:** Os riscos estratégicos estão associados à tomada de decisão da alta administração e podem gerar perda substancial no valor econômico da organização. Os riscos decorrentes da má gestão empresarial muitas vezes resultam em fraudes relevantes nas demonstrações financeiras.

Exemplos: falhas na antecipação ou reação ao movimento dos concorrentes causadas por fusões e aquisições; diminuição de demanda do mercado por produtos e serviços da empresa causada por obsolescência em função de desenvolvimento de novas tecnologias/produtos pelos concorrentes.

5.3.5.2. **Financeiros:** Os riscos financeiros são aqueles associados à exposição das operações financeiras da organização. É o risco de que os fluxos de caixa não sejam administrados efetivamente para maximizar a geração de caixa operacional, gerenciar os riscos e retornos específicos das transações financeiras e captar e aplicar recursos financeiros de acordo com as políticas estabelecidas. São ocorrências tais como a administração financeira inadequada, que conduz a endividamento elevado, podendo causar prejuízo frente à exposição cambial ou aumentos nas taxas de juros, etc. Incluem-se neste grupo operações no mercado de derivativos de *commodities*. Abrangendo tanto a área de crédito como de mercado.

5.3.5.3. **Operacional:** Os riscos operacionais estão associados à possibilidade de ocorrência de perdas (de produção, ativos, clientes, receitas) resultantes de falhas, deficiências ou inadequação de processos internos, pessoas e sistemas, assim como de eventos externos como catástrofes naturais, fraudes, greves e atos terroristas. Os riscos operacionais geralmente acarretam redução, degradação ou interrupção, total ou parcial, das atividades, com impacto negativo na reputação da sociedade, além da potencial geração de passivos contratuais, regulatórios e ambientais.

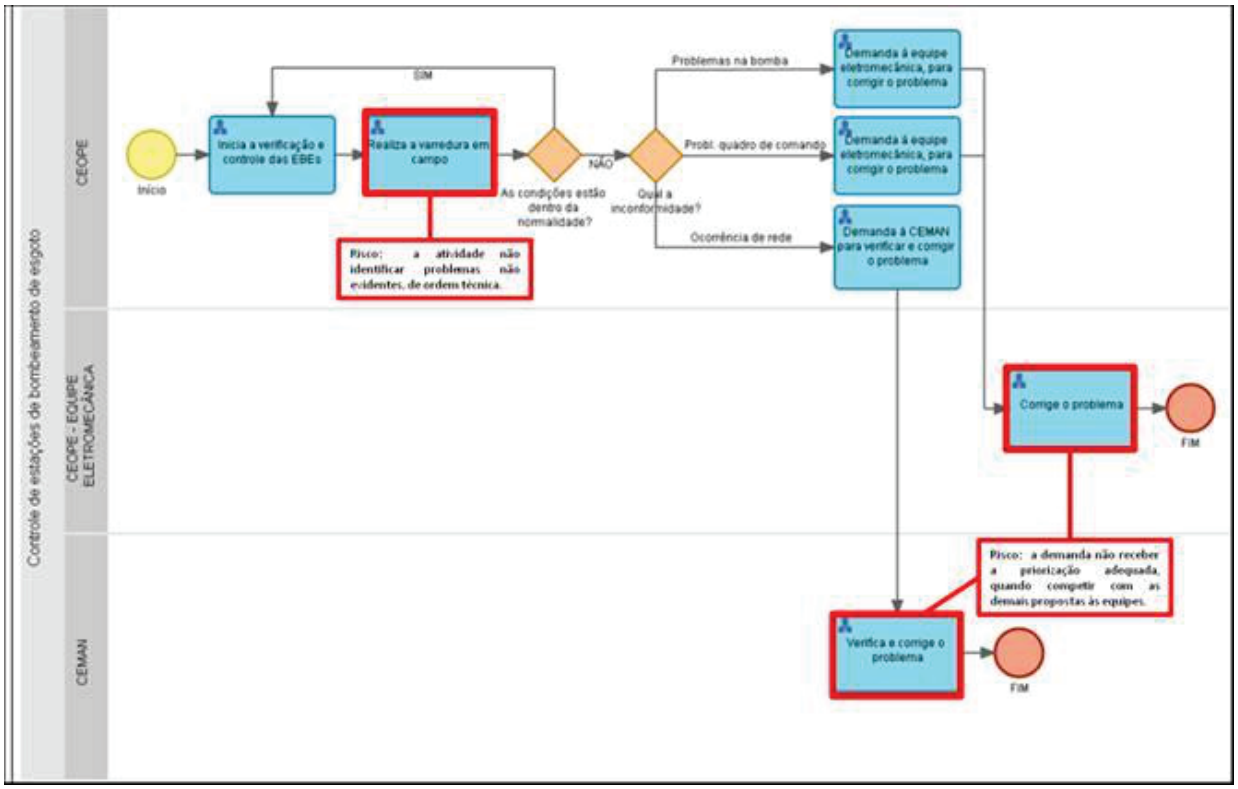
5.3.5.4. **Conformidade/legal:** Relacionadas com temas ligados a Agência reguladora, saúde e segurança, meio ambiente, práticas comerciais, proteção do consumidor, proteção de dados, entre outros. O risco legal pode também ser definido como uma medida numérica da incerteza dos retornos da organização, caso seus contratos não possam ser legalmente amparados por: falta de representatividade por parte de um negociador, documentação insuficiente, insolvência ou ilegalidade. As principais sub-áreas do risco legal são:

Risco de legislação	Risco tributário	Risco de contrato
É o risco de perdas decorrentes de sanções aplicadas por reguladores e indenizações por danos a terceiros por violação da legislação vigente. Exemplos:	É risco de perdas resultantes da criação de tributos ou de nova interpretação de sua incidência. Exemplos:	É o risco de perdas decorrentes de julgamentos desfavoráveis devido a contratos omissos, mal redigidos ou sem o devido amparo legal. Exemplos
1. Multas por não cumprimento de exigibilidades;	1. Criação de impostos novos sobre ativos e/ou produtos;	1. Pessoa sem o poder de assinar contratos representando a instituição;
2. Indenizações pagas a clientes por não cumprimento da legislação.	2. Recolhimento de novas contribuições sobre receitas, não mais sobre lucros.	2. Não execução pronta de garantias, requerendo o acionamento do Jurídico.
		3. Responsabilidades cobertas nos contratos de terceirização, mas colocadas de forma pouco objetiva.

RISCOS			
N°	Listagem	Definição	Classificação
R1	Risco de suspensão indevida	O risco está ligado a possíveis falhas sistemáticas e não controladas/verificadas pela área comercial	Operacional
R2	Risco de atraso na entrega das faturas	O risco está ligado ao atraso dos cumprimentos dos prazos por parte das equipes de leitura/faturamento	Financeiro
R3	Risco de perda de contratos de programa	O risco está ligado ao não cumprimento por falta de gestão das obrigações firmadas com os municípios na assinatura dos contratos de programa	Legal

5.3.6. Fluxograma e riscos no processo

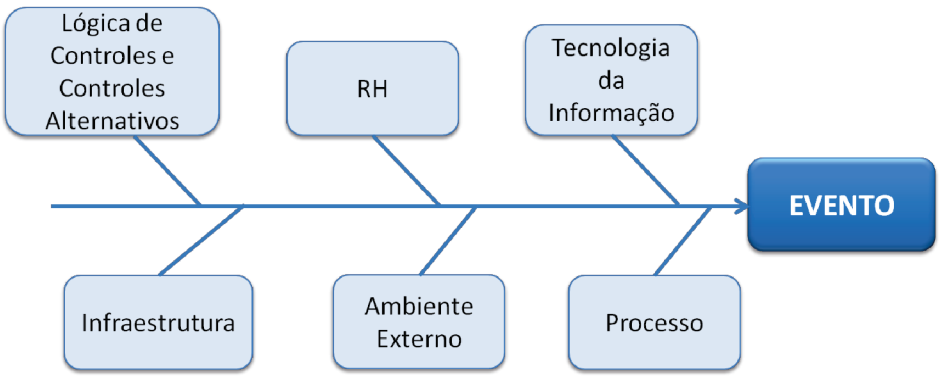
Com base na análise situacional/mapeamento do processo e os seus respectivos riscos levantados, o gestor da área ou departamento, deve demonstrar nos fluxogramas desenhados pela organização os riscos existentes em cada atividade. Abaixo exemplo.



5.3.7. Identificação dos fatores de riscos

Os fatores de risco são na realidade a origem e ou causa de cada evento identificado em cada processo. Para compreender o risco – a condição – a soma de todos os fatores, há a necessidade de dissecar o evento e ou ameaça. A organização optou pela técnica do Diagrama de Causa e Efeito, o chamado Diagrama de Ishikawa e ou de Espinha de Peixe para poder entender quais são os fatores que influenciam a concretização de cada risco. Esta técnica é uma notação simples para identificar fatores que causam o evento estudado. Em 1953 o Professor Karou Ishikawa, da Universidade de Tóquio Japão, sintetizou as opiniões dos engenheiros de uma fábrica na forma de um diagrama de causa e efeito, enquanto eles discutiam problemas de qualidade. O diagrama bem detalhado apresenta a forma de uma espinha de peixe.

Para compreender o risco e o cenário no qual ele está inserido, é importante considerar os diversos fatores que impactam o processo. Neste contexto, foi adaptado o diagrama de causa e efeito da qualidade para a área de riscos, inserindo os seguintes fatores de riscos, específicos para a organização. O diagrama de causa e efeito fica assim exemplificado:



Ressaltamos que para cada evento identificado há a necessidade da elaboração de um diagrama de causa e efeito específico. Se estivermos estudando 10 eventos em um determinado processo, teremos que elaborar 10 diagramas de causa e efeito.

5.3.8. Identificação Motricidade – Matriz SWOT

Após a identificação dos vários fatores de riscos de cada processo, os gestores da área precisam enxergar estrategicamente quais são os fatores comuns a todos os riscos e quais são os mais motrizes. Ou seja, quais são os que podem de fato potencializar os perigos estudados. A organização optou em utilizar a matriz SWOT, conhecida dos gestores para identificar os pontos fracos, fortes, oportunidades e ameaças do contexto empresarial. A ferramenta é a matriz SWOT - FOFA, que em inglês significa SWOT - *Strengths - Weaknesses - Opportunities – Threats* e em português – Força – Oportunidade – Fraqueza - Ameaça. A avaliação das forças e fraquezas diz respeito às condições dos nossos controles e nível de operacionalização, são processos que a organização possui domínio de ação e decisão. São os chamados fatores de riscos internos, variáveis internas. Os fatores de riscos considerados incontroláveis dizem respeito ao ambiente externo, podendo ser negativa – ameaças e ou positivas – oportunidades. Visando identificar a motricidade dos fatores de riscos, os gestores possuem dois critérios de avaliação:

5.3.8.1. **Magnitude**: significa o tamanho ou grandeza que a variável ou evento possui perante a empresa. Caso aconteça, positivamente ou negativamente, o quanto ela vai influenciar no contexto como um todo. A magnitude é ranqueada, utilizando-se uma pontuação, que varia de –3 a +3, dentro do seguinte parâmetro: + 3 (alto); + 2 (médio); + 1 (baixo), para cada elemento positivo (força ou oportunidade) e –1 (baixo); -2 (médio); -3 (alto) para cada variável negativa (fraqueza e ameaça). No nosso caso podemos ter como parâmetro para poder dar a nota da magnitude na célula da fraqueza e ameaça o número de vezes que as variáveis aparecem no diagrama de causa e efeito. É uma forma mais objetiva de saber a magnitude do fator de risco, pois se um fator de risco aparece 5 vezes em seis riscos estudados, significa que esta variável é de "grande"magnitude.

5.3.8.2. **Importância**: significa a prioridade que esta variável deve possuir perante a conjuntura do processo estudado interagindo com a área do gestor. É uma nota subjetiva com base na experiência da equipe que está avaliando. Utilizamos também três níveis de pontuação: 3 (muito importante); 2 (média importância); 1 (pouca importância). Neste caso, não há contagem negativa, pois o critério Importância sempre é positivo.

Para ranquear os itens em cada célula, podemos multiplicar a avaliação da magnitude e da importância. Os fatores de riscos ranqueados com maior numeração, positiva e negativa, são considerados motrizes. Motrizes porque devem receber maior atenção. A matriz SWOT - FOFA demonstra o conjunto de Fatores de Riscos (Fraquezas e Ameaças), e seus pontos fortes e oportunidades. Com esta fotografia o gestor enxergará seus pontos de maior fragilidade. Se formos observar sob o ponto de vista das fraquezas e ameaças contidas na Matriz SWOT, podemos afirmar que a Matriz SWOT é um resumo de todos os diagramas de causa e efeito, sem listar os fatores repetidos.

				FRAQUEZAS E AMEAÇAS								
ID	ÍTEM	Magnitude	mportância	TOTAL	Qte		ID	ÍTEM	Magnitude	mportância	TOTAL	Qte
1							1					
2							2					
3							3					
4							4					
5							5					
6							6					
7							7					
8							8					
9							9					
10							10					
11							11					
12							12					

Ponto importante na matriz SWOT – FOFA é que as fraquezas são oriundas dos diagramas de causa e efeito, são os resumos dos fatores de riscos que cada área possui. As ameaças são as variáveis incontroláveis do ambiente externo, também oriundas do diagrama de causa e efeito. As variáveis negativas (fraquezas e ameaças) da matriz SWOT – FOFA são o resumo dos vários diagramas de causa e efeito, sendo a base do Plano de Ação. A matriz é uma ferramenta de gestão, fácil de enxergar as principais deficiências e quais são as possibilidades de reversão da situação existente. A matriz SWOT – FOFA adaptada para a gestão de riscos visualiza o todo, enquanto que o diagrama de causa e efeito visualiza somente o risco estudado.

6. ANÁLISE DE RISCOS

A avaliação de riscos visa promover o entendimento do nível de risco e de sua natureza, auxiliando na definição de prioridades e opções de tratamento aos riscos identificados. Por meio dela, é possível saber qual a chance, a probabilidade dos riscos virem a acontecer e calcular seus respectivos impactos nos processos da empresa. A organização optou, neste momento, na avaliação de riscos qualitativa (subjetiva), que consiste na utilização de critérios pré-estabelecidos com uma escala de valoração para a determinação do nível do risco. A metodologia a ser utilizada para a avaliação de riscos possui dois parâmetros claros a serem estudados:

Saber qual a chance, a probabilidade, dos riscos virem a acontecer, frente à condição existente de cada processo e área de negócio. Calcular o impacto, as consequências para o processo impactado.

A avaliação de riscos é uma forma do gestor acompanhar a evolução de suas ameaças de maneira geral

6.1. Determinação do Grau de Probabilidade - GP

Para elaborar o Grau de Probabilidade – GP, temos dois critérios: O Critério dos Fatores de Riscos (FR) e o Critério da Exposição (E). O GP está alicerçado em uma fórmula simples, que calcula de forma direta, através da multiplicação dos dois critérios, o nível de possibilidade de o evento vir a acontecer, frente a sua condição e exposição. Com base nesta classificação e cruzando com o grau da relevância do impacto, o gestor possuirá a Matriz de Riscos de seu processo, priorizando desta forma o tratamento dos riscos.

6.1.1. Determinação do Critério Fator de Riscos – Grau de Probabilidade

Os seis macro fatores de riscos identificados no Diagrama de causa e Efeito, (Lógica de Controle e Controles alternativos, RH/Pessoas, Tecnologia – TI, Infraestrutura, Ambiente

Externo, Processos), possuem uma escala de valoração que mede o nível de influência de cada aspecto para a materialização do risco, conforme pode ser observado na tabela abaixo:

Nível do Fator de Risco	
Escala	**Pontuação**
Melhoria completa necessária nos controles e processo	5
Melhoria parcial necessária nos controles e processos	4
Nível suficiente dos controles e processos	3
Nível Alto dos controles e processos	2
Nível Muito Alto dos controles e processos	1

Para cada um dos 6 (seis) fatores damos uma nota de 1 a 5, de acordo com o nível de influência de concretização, em função do nível de controle/segurança existente no processo estudado. Após a pontuação das questões pertinentes aos respectivos fatores de risco, é necessário efetuar a soma do resultado/média dos seis fatores e dividir por seis para determinar o grau final (média) desta variável, conforme demonstrado a seguir:

FR = (LCCA + RS + TI + IE + AE + P / 6)

6.1.2. Determinação do Critério da Exposição – Grau de Probabilidade

Assim como no tópico anterior, o critério de Exposição (E) possui uma escala de valoração que mede a frequência que o processo costuma-se manifestar-se na organização. É importante visualizar que a escala de valores deve levar em conta o histórico, a condição atual e a futura. Deve ter uma visão não só projetiva, mas sim prospectiva. A tabela abaixo:

Critério de Exposição	
Escala	Pontuação
Dia/Semana	5
Quinzenal	4
Mensal	3
Anual	2
Eventual	1

6.1.3. Determinação do Grau de Probabilidade

O GP é o resultado da multiplicação do valor final do fator de risco versus o critério da exposição, conforme demonstrado abaixo:

GP = FR x E

Esta multiplicação direta representa o grau de probabilidade, sendo que o valor máximo obtido é 25, com a classificação dividida em cinco níveis (escala 1). No entanto, para que o valor do GP seja lançado na matriz de riscos, cuja escala máxima permitida é 5 (escala 2), é necessário efetuar a equivalência entre as duas escalas utilizadas, conforme tabela a seguir:

Escala 1	Escala 2	Nível de Probabilidade	
1 - 5	1	Muito baixa	4%-20%
5,1 – 10	2	Baixa	20,4%-40%

10,1 – 15	3	Média	40,4%-60%
15,1 – 20	4	Alta	60,4%-80%
20,1 - 25	5	Muito Alta	80,4%-100%

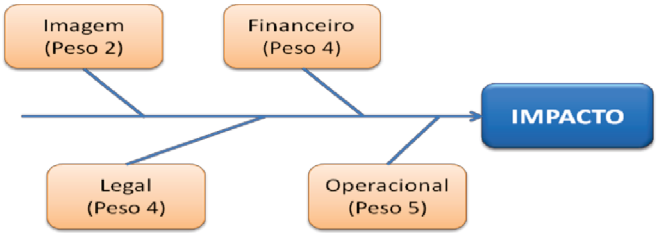
Resultado da multiplicação GP = FR x E

Equivalência para matriz de riscos

Equivalência em Probabilidade Fator de Multiplicação 4%

6.2. Determinação do Nível de Impacto – Consequências

Para mensurar o impacto, não devemos levar em consideração somente a questão financeira. Com o objetivo de o gestor obter uma visão holística do impacto há a necessidade de projetar todas as consequências que os eventos causam. Utilizaremos o mesmo critério adotado para identificar o processo crítico. Cada fator de impacto terá um peso diferenciado, tendo em vista seu grau de importância para a organização. Cada fator de impacto possui um valor e também será dada uma nota de valoração, tendo em vista o nível de consequência. O objetivo é a obtenção de uma média ponderada, equalizando desta forma o nível de impacto. Os fatores de Impacto – FI são:



Fator de impacto - Imagem	
Escala	Pontuação
De caráter nacional – Brasil	5
De caráter estadual – RS	4
De caráter local – Região Metropolitana	3
De caráter interno – Dentro da organização	2
De caráter interno – Dentro da área	1

Nota - Imagem: *No critério impacto na imagem, considerar visões distintas, ou seja, Cooperado e Cliente, considerando sempre a maior nota. Exemplo – Imagem na visão do cooperado 3 e imagem na visão do cliente 5, considerar a maior nota.*

Fator de impacto - Financeiro	
Escala	Pontuação
Catastrófico – Acima de R$5.000.001,00	5
Severo – De R$500.001,00 a R$5.000.000,00	4
Moderado – De R$50.001,00 a R$500,000,00	3
Leve – De R$25.001,00 a R$50.000,00	2
Insignificante – Até R$25.000,00	1

Fator de impacto - Legal	
Escala	Pontuação
Perturbações muito graves	5
Perturbações graves	4
Perturbações limitadas	3
Perturbações leves	2
Perturbações muito leves	1

Nota - Legal: Deverão ser avaliadas as consequências para a organização no âmbito de responsabilidade civil, regulatório

(multa e civil), tributário e criminal.

Fator de impacto - Operacional	
Escala	Pontuação
Perturbações muito graves (impacta outros processos muito fortemente)	5
Perturbações graves (impacta outros processos de forma direta)	4
Perturbações limitadas (só impacta o próprio processo, consideravelmente)	3
Perturbações leves (só impacta o próprio processo, levemente)	2
Perturbações muito leves (em nada impacta)	1

O nível de impacto é o resultado da soma dos resultados de cada fator de impacto (multiplicação do peso versus a nota), dividido pela soma dos pesos, conforme demonstrado abaixo:

$$\text{Nível de Impacto} = \frac{\text{Imagem} + \text{Financeiro} + \text{Operacional} + \text{Legislação}}{\text{15 (soma dos pesos 2+4+4+5)}}$$

O resultado do nível de impacto é a tabela abaixo:

Grau de impacto	Escala	Nível de impacto
4,51 – 5,00	5	Catastrófico
3,51 – 4,50	4	Severo
2,51 – 3,50	3	Moderado
1,51 – 2,50	2	Leve
1,00 – 1,50	1	Insignificante

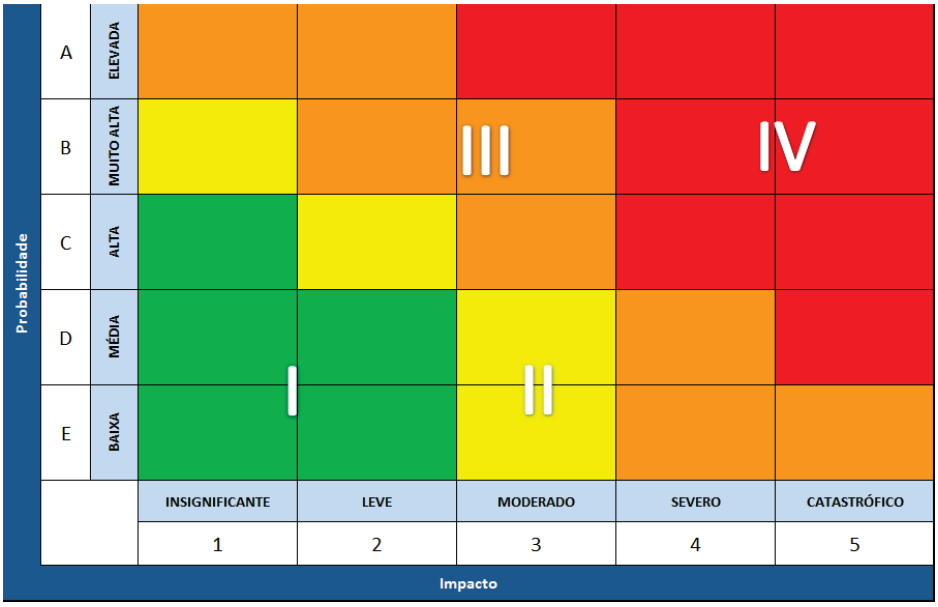
7. AVALIAÇÃO DE RISCOS

Comparar os níveis de riscos em relação ao critério pré-estabelecido. A relevância dos riscos possui como parâmetro a matriz de riscos. O resultado da matriz de riscos é o grau de criticidade, ou seja, qual é a priorização que a empresa deve tratar cada risco, frente ao seu apetite ao risco. A matriz é dividida em quadrantes e para cada quadrante há uma estratégia de tratamento e priorização. Cabe ressaltar que é nesta fase também que estabelece o grau de riscos dos processos estudados e ou das unidades organizacionais

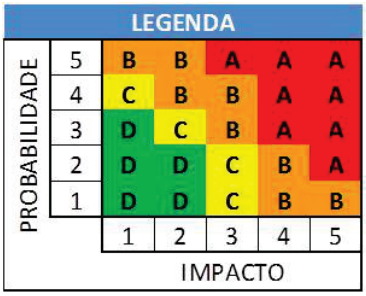
7.1. Matriz de riscos

Com o objetivo de visualizar e, ao mesmo tempo, implementar uma forma de tratamento de cada risco, o resultado da avaliação dos riscos será apresentado em um mapa de

riscos (matriz de monitoramento de riscos), permitindo o acompanhamento da mitigação ou elevação dos riscos.



A matriz de riscos demonstra os pontos de cruzamento (horizontal e vertical) da probabilidade de ocorrência e impacto. Desta forma, pela divisão da matriz em quatro quadrantes, podemos avaliar o nível de vulnerabilidade do processo estudado ou do departamento. Quanto maior for à probabilidade e o impacto de um risco, maior será o nível do risco. Temos a seguinte classificação de priorização de tratamento, de acordo com o nível de risco:



NÍVEIS DE TRATAMENTO	
A	AÇÃO IMEDIATA - INTOLERÁVEL
B	AÇÃO MÉDIA E CURTO PRAZO
C	MONITORAMENTO E GESTÃO
D	RISCO TOLERÁVEL

Os riscos terão os seguintes tratamentos, de acordo com o quadrante em que estiver localizado:

Quadrante IV (Vermelho): Os riscos existentes no quadrante IV são aqueles que têm alta probabilidade de ocorrência e poderão resultar em impacto extremamente severo, caso ocorram. Exigem a implementação imediata das estratégias de proteção e prevenção, ou seja, ação imediata. Ações de 0 a 30 dias.

Quadrante III (laranja): No quadrante III, localizam-se ameaças que poderão ser muito danosas à empresa, podendo possuir muito baixa probabilidade e alto impacto como baixo impacto e alta probabilidade. Estas ameaças devem possuir respostas rápidas, que para isso devem estar planejadas e testadas em um plano de contingência, emergência, continuidade de negócios, além de ações preventivas. A diferença do quadrante IV é que as ações podem ser implementadas com mais planejamento e tempo. São eventos que devem ser constantemente monitorados. Ações de 0 a 90 dias.

Quadrante II (amarelo): No quadrante II, estão os riscos com alta probabilidade de ocorrência, mas que causam consequências gerenciáveis à empresa. Os riscos classificados neste quadrante devem ser monitorados de forma rotineira e sistemática, podendo também possuir planos de emergência. Ponto de monitoramento 1 vez a cada 60 dias.

Quadrante I (verde): Os riscos classificados no quadrante I possuem baixa probabilidade e pequeno impacto, representando pequenos problemas e prejuízos. Estes riscos somente devem ser gerenciados e administrados, pois estão na zona de conforto. Ponto de monitoramento 1 vez a cada 90 dias.

7.2. Nível de Riscos

Após a finalização da etapa de avaliação de riscos, é iniciado o processo de avaliação do nível do risco por processo estudado. O nível do risco é um índice calculado semestralmente para mensurar o grau de risco dos processos e/ou unidades/sites analisados, com o objetivo de facilitar o monitoramento e acompanhamento da evolução do risco no processo. Para calcular o nível do risco, é necessário utilizar as variáveis já identificadas na etapa anterior de avaliação de riscos – Grau de Probabilidade (GP) e Impacto (I), conforme metodologia de cálculo abaixo:

Nível do Risco = GP x Impacto
Média do Nível de Risco: Média do GP x Média do Impacto

Para identificarmos o nível de risco (MGP X MI) é necessário utilizar a tabela de conversão abaixo:

NÍVEL DE RISCO			TRATAMENTO
1 a 5	1	Verde	Áreas ou departamentos que estão na zona de conforto, devendo ser gerenciadas e administradas.
5,1 a 10	2	Amarelo	Áreas ou departamentos com algum grau de riscos, mas que causam consequências gerenciáveis à empresa. Essas áreas ou departamentos devem ser monitoradas de forma rotineira ou sistemática.
10,1 a 15	3	Laranja	Áreas ou departamentos que devem receber tratamento com médio e curto prazo. Possuem cruzamento do grau de risco com médio e grande nível de riscos e elevados impactos. São áreas ou departamentos que devem ser constamente monitoradas.
15,1 a 25	4	Vermelho	Áreas ou departamentos que tem alto grau de risco e poderão resultar em impacto extremamente severo. Exigem implementação imediata das estratégias de proteção e prevenção, ou seja, ação imediata.

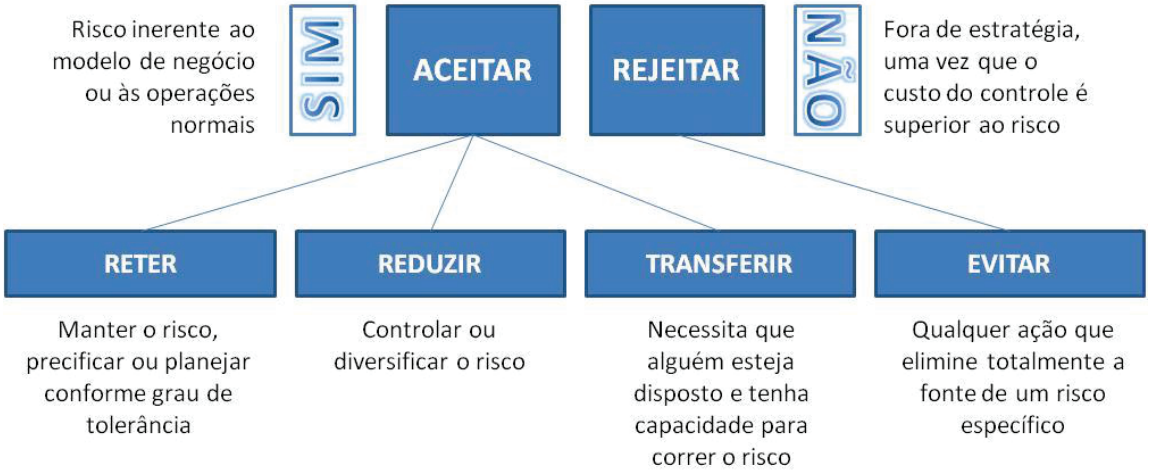
É importante ressaltar que quanto maior o nível do risco, maior sua criticidade para o processo. O nível de risco serve para a organização determinar seu apetite ao risco. A organização não admite nível de risco de seus processos acima do nível 2. Isto significa que os riscos plotados no quadrante IV – Vermelho - são considerados como *intoleráveis* para a organização. Estes riscos terão ação e tratamento imediatos por parte dos gestores.

8. RESPOSTAS AOS RISCOS – PLANO DE AÇÃO

8.1. Matriz de Responsabilidades

É importante que haja conscientização e comprometimento com o gerenciamento de riscos por parte da alta administração. Nesse contexto, Diretores e executivos são os responsáveis finais pelo gerenciamento de riscos na organização, ou seja, mediante a matriz de

riscos deve-se identificar qual a resposta a ser adotada para tratamento do risco. O diagrama abaixo exemplifica as estratégias de tratamento dos riscos.



Evitar o risco: Decisão de não se envolver ou agir de forma a se retirar de uma situação de risco. Necessário preencher o formulário padrão de Risco Assumido.

Aceitar o risco: Neste caso, apresentam-se três alternativas: reter, reduzir ou transferir/compartilhar o risco.

Reter: Manter o risco no nível atual de impacto e probabilidade. Necessário preencher o formulário padrão de risco assumido – Ver anexo 6.11.

Reduzir: Ações são tomadas para minimizar a probabilidade e/ou o impacto do risco.

Transferir e/ou compartilhar: atividades que visam reduzir o impacto e/ou a probabilidade de ocorrência do risco através da transferência ou, em alguns casos, do compartilhamento de uma parte do risco.

8.2. Risco Assumido

O risco é assumido quando o gestor do processo, com o nível de risco igual ou inferior a 3, decide, tendo em vista relação custo benefício ou por questões estratégicas, por não implementar medidas de médio e ou curto prazo. A área e ou departamento deve preencher um documento assumindo o risco e projetando as consequências. Este documento deve ter a assinatura de um diretor. Ressaltamos que não há possibilidade de risco assumido com grau de risco superior a 3. É contra a Política de Riscos da Organização.

8.3. Plano de Ação

É o tratamento dos riscos, ou seja, qual será a resposta que a empresa terá que operacionalizar. Aceitar, Reter, Reduzir, Transferir ou Evitar? O Plano de Ação é o conjunto de medidas organizacionais, sistemas técnicos de prevenção e monitoração, recursos humanos que gerenciarão os riscos. O Plano de Ação é elaborado com base nos Fatores de Riscos visando mitigar riscos. Para cada risco identificado, deve-se identificar qual a resposta a ser adotada para tratamento do risco de acordo com as possibilidades adotadas na matriz de responsabilidade. O Plano de Ação deverá ser elaborado utilizando-se a técnica das perguntas: 5W e 2H.

What?	*Who?*	*When?*	*Where?*	*Why?*	*How?*	*How much?*
O quê?	Quem?	Quando?	Onde?	Por quê?	Como?	Quanto custa?

Medida em relação à causa prioritária.	Nome do responsável pela implantação da ação.	Data limite para implantação da ação.	Onde a ação será implantada.	Qual o motivo para realização da ação.	Descrever como será executada a ação proposta.	Qual o valor do investimento.

O plano de ação formal, denominado *Ação Corretiva Negociada* (PDCA), deve ser elaborado em conjunto com o gestor do processo a que o risco estiver relacionado e deve conter, obrigatoriamente, os prazos e os responsáveis pela implementação das ações recomendadas.

Compartilhar riscos (transferir) pode gerar novos riscos ou modificar um risco existente, uma vez que a organização para qual o risco foi transferido pode não gerenciá-lo de maneira eficaz.

A ação corretiva negociada possui a seguinte estrutura:

Número da recomendação proposta pela Auditoria Interna e ou pelo Usuário (ex.: Rec 1);

Codificação do risco e respectivo grau (ex. R1 – risco alto);

Unidade e ou Departamento a que o risco se aplica (ex. Financeira)

Descrição do aspecto identificado (situação atual);

Descrição da recomendação proposta (situação proposta);

Áreas envolvidas (ex. Alta Administração, Recursos Humanos, Contábil e Financeira, outras áreas);

Responsável: gestor responsável pela implementação das recomendações nas respectivas unidades;

Prazo (mês/ano): data negociada para a efetiva implementação da recomendação.

8.4. Priorização das Ações - critérios

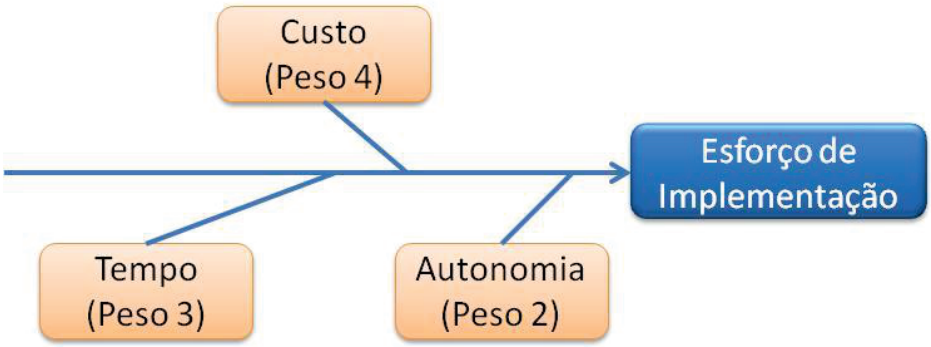
A ferramenta de apoio à decisão – priorização das ações tem por objetivo fazer com que o gestor e ou analista possa de forma mais prática e objetiva enxergar, através de critérios preestabelecidos e plotados em uma matriz, as ações que são prioritárias em termos de benefício. Os dois macro critérios são:

a. Esforço de Implementação;

b. Benefício Estimado.

8.4.1. Esforço de implementação

O macro critério esforço de implementação é conseguido através da medida ponderada de três sub critérios, com os seguintes pesos:



Abaixo subcritérios e definições:

Subcritério	Definição
Custo	Significa quanto a empresa vai ter que investir. É uma visão financeira.
Tempo	Visa identificar qual o horizonte temporal estimado para a real implantação da ação e/ou sistema.
Autonomia	É em termos de nível de aprovação, se dependera de uma diretoria ou do próprio departamento.

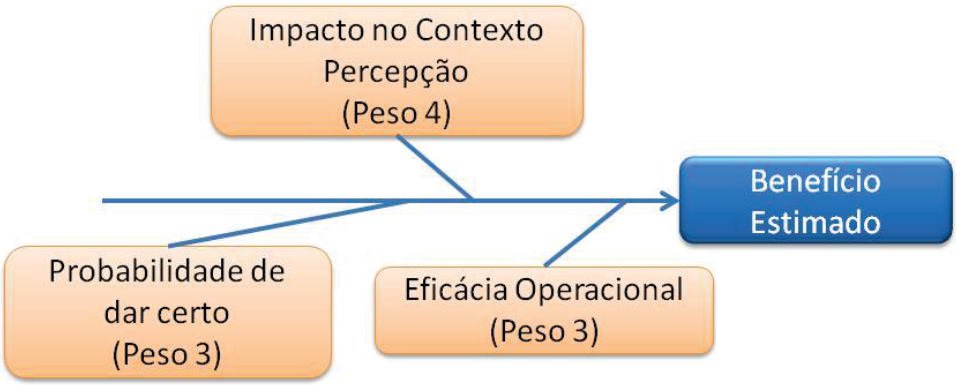
A nota varia de 1 a 5, de acordo com o nível de esforço. Quanto maior o esforço maior a nota. O grau de esforço de implementação é conseguido somando-se as notas de cada sub critério, e dividindo por 09 (somatório dos pesos). A partir daí temos a média ponderada:

$$\text{Esforço de Implementação} = \frac{\text{Custo + Tempo + Autonomia}}{\text{9 (soma dos pesos 4+3+2)}}$$

Grau de impacto	Nível
4,51 – 5,00	Insatisfatório
3,51 – 4,50	Ruim
2,51 – 3,50	Bom
1,51 – 2,50	Muito bom
1,00 – 1,50	Excelente

8.4.2. Benefício estimado

O macro critério benefício estimado é conseguido através da média ponderada de três subcritérios, com os seguintes pesos:



Abaixo subcritérios e definições:

Subcritério	Definição
Impacto no contexto	Significa quanto a ação pode gerar de resultado no contexto estabelecido
Probabilidade (de dar certo)	É a estimativa de a ação ser operacionalizada com sucesso diante da estrutura e dos recursos da empresa.
Eficácia operacional	É a estimativa do quanto a ação pode continuar gerando de resultado após sua implantação.

A nota varia de 1 a 5, de acordo com o nível de benefício. Quanto maior o benefício maior a nota. O grau de benefício estimado é conseguido somando-se as notas de cada subcritério, e dividindo por 10 (somatório dos pesos). A partir daí temos a média ponderada.

$$\text{Benefício estimado} = \frac{\text{Impacto no contexto} + \text{Probabilidade de dar certo} + \text{Eficácia operacional}}{10 \text{ (soma dos pesos 4+3+3)}}$$

Grau de impacto	Nível
4,51-5,00	Muito bom
3,51-4,50	Bom
2,51-3,50	Regular
1,51-2,50	Ruim
1,00-1,50	Muito ruim

8.5. Matriz de Priorização de Ações

O resultado do cruzamento dos dois macrocritérios é uma Matriz, com três quadrantes, onde temos as priorizações. O quadrante azul é onde as ações devam ser operacionalizadas; o quadrante laranja exige reavaliação e ou ação a médio prazo, e o quadrante vermelho as ações devem ser descartadas.

9. MONITORAMENTO

O monitoramento proporciona o acompanhamento rotineiro do desempenho real, para que possa ser comparado ao desempenho esperado ou requerido. A auditoria envolve a investigação periódica da situação atual, normalmente com um foco específico. O resultado desse trabalho proporciona a identificação de *gaps* de controle existentes, permitindo o endereçamento destes em um plano de ação formal, contendo prazos e responsabilidades pela implementação das ações recomendadas. O monitoramento e a auditoria são partes integrantes e essenciais da gestão dos riscos, é uma das etapas mais importantes do processo de gestão de riscos no âmbito organizacional, devendo ser realizados continuamente. É necessário que sejam monitorados os riscos, a eficácia e a adequação das estratégias e dos sistemas de gestão estabelecidos para a implementação dos tratamentos dos riscos, bem como o plano e o sistema de gestão de riscos como um todo.

9.1. Execução de cada plano

Após a elaboração dos planos e a escolha da ação a ser executada, as atividades pertinentes deverão ser efetuadas em consonância com os gestores envolvidos e as práticas descritas nesta política.

9.2. Monitoramento

O monitoramento da execução de cada plano segue o processo definido pela organização, executada por meio do processo “Monitoramento de Riscos”, que consiste em um questionário cujas questões estão organizadas conforme relação a seguir:

1) O plano/meta do gerenciamento de risco de determinado processo.
   a) O plano de gerenciamento de risco está montado?
   b) A meta do gerenciamento de risco está estabelecida?
   c) O plano e a meta acima são conhecidos por todos os membros do staff do departamento envolvido?
2) A organização.
   a) A organização de gerenciamento de risco está montada?
   b) O responsável pelo gerenciamento do risco está definido?
   c) Há uma regra para elaboração de relatórios de gerenciamento de risco. Ela é seguida?
3) A identificação do risco.
   a) O risco é conhecido é investigado?
   b) As normas, políticas e/ou procedimentos internos existentes são perioridicamente revisados/atualizados e conhecidos por todos os colaboradores envolvidos?
4) A avaliação e importância do risco.
   a) Pode-se rever o grau (existência e danos) da influência do risco?
   b) Pode-se prever a frequência de ocorrência do risco?
   c) A importância do risco está clara?
5) A resposta ao risco.
   a) Estabeleceu alguma medida para os riscos de maior importância?
   b) O plano de resposta aos riscos (reter, transferir, reduzir e evitar) está claro?
   c) A meta a ser alcançada está clara?
   d) O ambiente no qual foi gerado o risco está pronto para ser mudado?
6) O plano de ação.
   a) O plano de ação para o risco está estabelecido (PDCA)?
   b) A pessoa responsável pela organização está envolvida na elaboração do plano de resposta ao risco?
   c) O plano de ação para o risco está na direção certa para se adequar ao plano e meta da empresa?
   d) O plano de resposta ao risco completou o ciclo PDCA até a data desta avaliação?
7) O progresso do plano de ação.
   a) A forma de execução do plano de ação está clara?
   b) A pessoa responsável pelo plano de ação está definida?
   c) O progresso do plano de ação para o risco é reportado e acompanhado pelo responsável da organização?
   d) O plano de ação para o risco progride com o planejado?

e) Há uma medida a ser utilizada quando há atrasos no cumprimento do plano de ação?

8) A identificação e relação das informações de risco.

a) As informações sobre o risco podem ser identificadas e relacionadas de acordo com o manual básico de gerenciamento de riscos?

9) As medidas em momento de emergência.

a) A organização para emergência (sério risco de que riscos de nível 4 e 5 ocorram) está pronta?

b) O padrão de conduta em emergência (sério risco de que riscos de nível 4 ou 5 ocorram) está pronto?

10) Educação e treinamento.

a) Existe um plano de ação de educação e/ou treinamento para membros da equipe?

b) O plano de educação e/ou treinamento é realizado?

c) Os conteúdos de educação e/ou treinamento são revisados e utilizados?

11) Auditoria (ou monitoramento).

a) Existem regulamentos e/ou normas de auditoria (ou monitoramento)?

b) Existe uma estrutura e plano de auditoria (ou monitoramento)?

c) A auditoria (ou monitoramento) é realizada?

d) O relatório de auditoria é revisado pela alta administração?

12) Correção e melhoria contínua.

a) Com base no resultado da auditoria, são realizadas as correções e melhorias necessárias.

b) O resultado da correção / melhoria é verificado e acompanhado?

13) Eficácia de custo.

a) O custo – benefício está equilibrado?

As questões pertinentes a cada tópico deverão ser pontuadas de acordo com o padrão de avaliação que aborda a seguinte escala de valoração:

Monitoramento de risco		
Escala	Pontuação	Descrição
Nível muito alto	5	O nível mais alto realizável; O nível que não precisa de mais nenhuma melhoria.
Nível suficiente	4	Nível alto, mesmo não sendo o mais alto; O nível que chegará ao mais alto, se melhorado.
Nível necessário	3	O risco, a gama de gerenciamento e a classe abrangem a área necessária; É feita a quantificação, regularização, convenção regular, documentação, etc; É decidido “quem faz” (pessoa reconhecida, pessoa responsável, etc); Gerenciamento de progresso executado. O padrão de avaliação e o índice do gerenciamento foram decididos; O resultado se equilibrou ao custo.
Melhorias parciais necessárias	2	Necessita de melhorias parciais; O nível que irá alcançar o “nível de necessidade” se melhorar; Se algo não for feito, não alcançará o “nível de necessidade”.
Melhorias significativas necessárias	1	É necessária uma porção maior de melhorias; Torna-se um problema se continuar no mesmo nível.

Melhoria completa necessária	0	O nível do qual nada foi feito ou perdeu-se o objetivo; O nível que necessita uma reavaliação completa e novas medidas.

Para identificar o resultado do nível de monitoramento, após a pontuação de todas as questões, calcula-se o valor total dos tópicos de todas as questões (185), dividido pelos 4 (quatro) níveis de tratamento já adotados pela organização, chegando a média 46,25. Para a criação dos critérios de escalas foi necessário dividir novamente por 4 (quatro). Abaixo, ilustração de cálculo.

Nível de monitoramento = $\frac{\text{185 total da pontuação (considerar a maior nota)/4 = 46,25}}{4}$

NÍVEL DE MONITORAMENTO			TRATAMENTO
34,70 - 46,25	4	Verde	Áreas ou departamentos que estão na zona de conforto, devendo ser gerenciadas e administradas.
23,14 - 34,69	3	Amarelo	Áreas ou departamentos com algo grau de riscos, mas que causam consequências gerenciáveis à empresa. Essas áreas ou departamentos devem ser monitoradas de forma rotineira ou sistemática.
11,57 - 23,13	2	Laranja	Áreas ou departamentos que devem receber tratamento com médio e curto prazo. Possuem cruzamento do grau de risco com médio e grande nível de riscos e elevados impactos. São áreas ou departamentos que devem ser constamente monitoradas.
0 - 11,56	1	Vermelho	Áreas ou departamentos que tem alto grau de risco e poderão resultar em impacto extremamente severo. Exigem implementação imediata das estratégias de proteção e prevenção, ou seja, ação imediata.

A organização não admite nível de monitoramento abaixo do nível 3. Isto significa que as avaliações com resultado menor que 23,13, são considerados como *intoleráveis* para a organização e devem sofrer ações e tratamento imediatos por parte dos gestores. Abaixo,

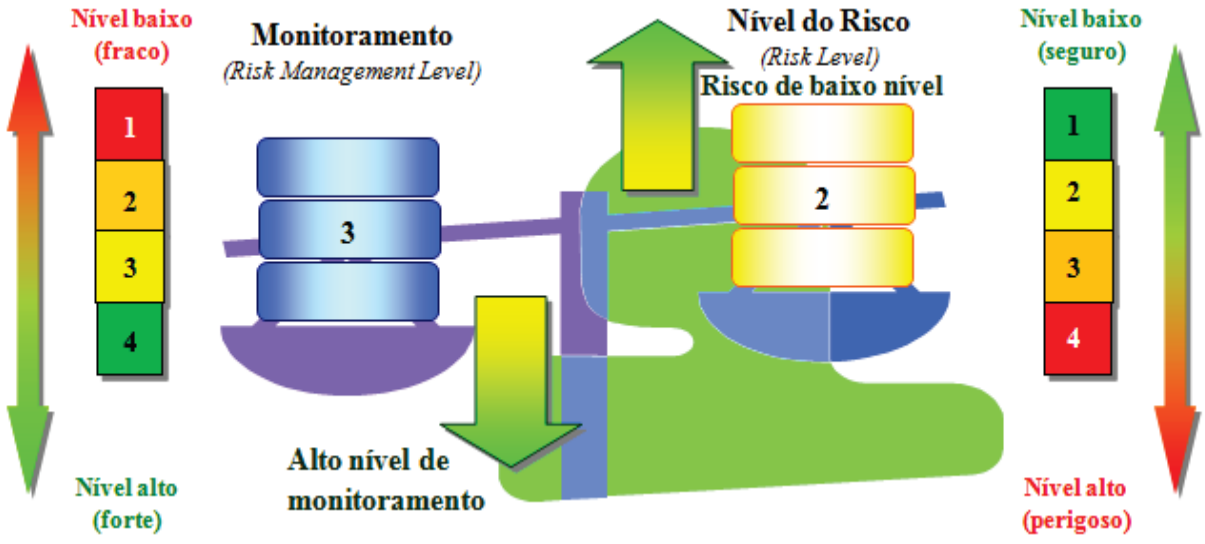


ilustração do resultado comparativo da avaliação nível de monitoramento e nível de risco.

A identificação do nível de Monitoramento do Risco, assim como o Nível do Risco, deve ser executada anualmente com o objetivo de monitorar e acompanhar a evolução do risco e/ou processo.

9.3. Checagem (*follow-up*)

A checagem da execução de cada plano, denominado *follow-up*, consiste na verificação do nível de implementação das recomendações apresentadas no relatório detalhado de auditoria, considerando os prazos e as responsabilidades previamente definidas. As informações/observações identificadas durante o follow-up, bem como a verificação do nível de implementação das recomendações, são definidas com base nas entrevistas realizadas com os principais gestores envolvidos no processo. Adicionalmente, para as recomendações implementadas, são conduzidos testes e exames complementares, visando constatar a efetiva implementação dos controles propostos.

A partir das recomendações não implementadas, são definidos novos prazos para implementação das recomendações, que devem ser devidamente discutidos com os diversos gestores envolvidos no processo. Adicionalmente, o sucesso da mitigação dos diversos riscos identificados dependerá da designação de recursos (humanos, de sistemas e financeiros). Além disso, é necessário alto grau de comprometimento dos referidos gestores, a fim de viabilizar a implementação das ações de forma objetiva.

9.3.1. Reavaliação

A realização do follow-up culmina com a reavaliação do grau dos riscos a partir da análise do nível de implementação das recomendações propostas. Com o intuito de possibilitar uma análise comparativa, elabora-se um novo mapa de riscos por meio do qual é possível verificar a evolução dos riscos.

9.3.2. Correções

A partir do resultado do follow-up, identificam-se novas oportunidades de melhoria que são formalizadas por meio de novas recomendações propostas. Tais recomendações dão origem a um novo PDCA para mitigar os riscos residuais.

10. DICIONÁRIO DE RISCOS

Anteriormente à avaliação dos riscos, os aspectos identificados no decorrer dos trabalhos de monitoramento devem ser definidos. Para auxiliar a definição dos riscos, elaboramos o dicionário de riscos, conforme segue abaixo:

Riscos estratégicos	
Risco	Definição do risco
1. Planejamento estratégico	Um processo de planejamento estratégico moroso e confuso pode resultar em informações irrelevantes que ameaçam a capacidade da organização de formular estratégias de negócios viáveis.
2. Estrutura organizacional	Ausência de informações necessárias para a gerência avaliar a eficácia da estrutura organizacional da empresa, que ameaça sua capacidade para mudar ou executar suas estratégias em longo prazo.
3. Indicadores estratégicos	Indicadores de *performance* inexistentes, irrelevantes ou não confiáveis são inconsistentes com as estratégias de negócio estabelecidas, ameaçando a capacidade da empresa em executar suas estratégias em longo prazo.
4. Imagem	Este pode ser definido como o risco de perdas em decorrência de alterações da reputação junto a clientes, concorrentes, órgãos governamentais, etc. Exemplo: boatos sobre a saúde de uma instituição, desencadeando corrida para saques.

Riscos financeiros	
Risco	Definição do risco
1. Planejamento **e orçamento**	Informações de Planejamento e Orçamento inexistentes, irreais, irrelevantes ou não confiáveis podem causar conclusões ou decisões financeiras não apropriadas.
2. **Avaliação de**	Fracasso em acumulação de informações externas e internas pertinentes e seguras para avaliar se

relatórios financeiros	ajustes requeridos nas demonstrações financeiras podem resultar na emissão de relatórios financeiros enganosos para a futura apreciação dos acionistas da empresa.
3. In**formações contábeis**	Excesso de ênfase nas informações contábeis e financeiras para administrar o negócio pode resultar na manipulação dos resultados para o atingimento de metas financeiras ao custo de não atender requisitos como satisfação do cliente, qualidade e eficiência.
4. **Fiscal**	Falhas ao acumular e considerar informações pertinentes de impostos podem resultar em descumprimento de regulamentos ou consequências de impostos adversos, que poderiam ter sido evitados, caso transações tivessem sido estruturadas diferentemente.
5. Relatórios regulamentares	Relatórios de informações financeiras e operacionais requeridos por agências de regulamentação incompletos, imprecisos e/ou atrasados podem expor a empresa a multas, penalidades e sanções.

Riscos operacionais	
Risco	Definição do risco
1. Obrigações contratuais	Falta de informações relevantes e/ou confiáveis em relação aos compromissos contratuais que estão sendo tratados no período podem gerar decisões adicionais sobre compromissos contratuais subsequentes que não são de interesse da empresa.
2. Precificação	Falta de informações relevantes ou que apoiem as estimativas para as decisões podem resultar em preços ou taxas insatisfatórias para os clientes.
3. Indicadores de desempenho/risco	Medidas não-financeiras inexistentes, irrelevantes e incertas podem causar avaliações e conclusões errôneas sobre o desempenho operacional.
4. Congruência	Fracasso no alinhamento dos objetivos dos processos de negócio e indicadores de performance com os objetivos e estratégias organizacionais pode resultar em atividades conflitantes e desordenadas em toda a empresa.
5. Presteza e confiabilidade	Este pode ser definido como o risco de perdas, pelo fato de informações não poderem ser recebidas, processadas, armazenadas e transmitidas em tempo hábil e de forma confiável.
6. Equipamento	Este pode ser definido como o risco de perdas por falhas nos equipamentos elétricos, de processamento e transmissão de dados, telefônicos, de segurança, etc.
7. Erro não intencional	Este pode ser definido como o risco de perdas em decorrência de equívoco, omissão, distração ou negligência de funcionários.

Riscos **legais e de conformidade**	
Risco	Definição do risco
1. Legislação	Este pode ser definido como o risco de perdas decorrentes de sanções por reguladores e indenizações por danos a terceiros por violação da legislação vigente. Exemplos: 1) Multas por não cumprimento de exigibilidades; 2) Indenizações pagas a clientes por não cumprimento da legislação.
2. Tributário	Este pode ser definido como o risco de perdas devido à criação ou nova interpretação da incidência de tributos. Exemplos: 1) Criação de impostos novos sobre ativos e/ou produtos; 2) Recolhimento de novas contribuições sobre receitas, não mais sobre lucros.
3. Contrato	Este pode ser definido como o risco de perdas decorrentes de julgamentos desfavoráveis por contratos omissos, mal redigidos ou sem o devido amparo legal. Exemplos: 1) Pessoa sem poder para assinar contratos representando a instituição; 2) Não execução pronta de garantias, requerendo o acionamento do jurídico; 3) Responsabilidades cobertas nos contratos de terceirização colocadas de forma pouco objetivas.

11. TERMOS E DEFINIÇÕES

Para os efeitos deste documento, aplicam-se os seguintes termos e definições.

Nota: Os termos/definições foram retirados da Norma ABNT ISO GUIA 73:2009, Gestão de riscos – Vocabulário .

Análise crítica: Atividade realizada para determinar a adequação, suficiência e eficácia do assunto em questão para atingir os objetivos estabelecidos.

Nota: A análise crítica pode ser aplicada à estrutura da gestão de riscos, ao processo de riscos, ao risco ou aos controles.

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

Nota 1: A análise de riscos fornece a base para a avaliação de riscos e para as decisões sobre o tratamento de riscos.

Nota 2: A análise de riscos inclui a estimativa de riscos.

Apetite pelo risco: Quantidade e tipo de riscos que uma organização está preparada para buscar, manter ou assumir.

Atitude perante o risco: Abordagem da organização para avaliar e eventualmente aceitar, reter, reduzir, transferir ou evitar o risco.

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

Nota: A avaliação de riscos auxilia na decisão sobre o tratamento de riscos.

Aversão ao risco: Atitude de afastar-se de riscos.

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

Nota: O contexto externo pode incluir:

- *os ambientes cultural, social, político, legal, regulamentar, financeiro, tecnológico, econômico, natural e competitivo, seja internacional, nacional, regional ou local;*
- *os fatores chaves e as tendências que tem impacto sobre os objetivos da organização;*
- *as relações com partes interessadas externas, e suas percepções e valores.*

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

Nota: O contexto interno pode incluir:

- *governança, estrutura organizacional, funções e responsabilidades;*
- *políticas, objetivos e as estratégias implementadas para atingi-los;*
- *as capacidades, compreendidas em termos de recursos e conhecimento (por exemplo, capital, tempo, pessoas, processos, sistemas e tecnologias);*
- *percepções e valores das partes interessadas internas;*
- *sistema de informação, fluxos de informação e processos de tomada de decisão (tanto como informais);*
- *relações com partes interessadas internas, e suas percepções e valores;*
- *a cultura da organização;*
- *normas, diretrizes e modelos adotados pela organização, e*
- *forma e extensão das relações contratuais.*

Comunicação e consulta: Consulta processos contínuos e interativos que uma organização conduz para fornecer, compartilhar ou obter informações e se envolver no diálogo com as partes interessadas e outros, com relação a gerenciar riscos.

Controle: Medida que está modificando o risco.

Nota 1: Os controles incluem qualquer processo, política, dispositivo, prática ou outras ações que modificam o risco.

Nota 2: Os controles nem sempre conseguem exercer o efeito de modificação pretendido ou presumido.

Critérios de riscos: Termos de referência contra a qual o significado de um risco é avaliado.

Nota 1: Os critérios de riscos são baseados nos objetivos organizacionais e no contexto externo e interno.
Nota 2: Os critérios de risco podem ser derivados de normas, leis, políticas e outros requisitos.

Consequência: Resultado de um evento que afeta os objetivos.

Nota 1: Um evento pode levar a uma série de consequências.
Nota 2: Um consequência pode ser certa ou incerta e pode ter efeitos positivos ou negativos sobre os objetivos.
Nota 3: As consequências podem ser expressas qualitativa ou quantitativamente..
Nota 4: As consequências inicias podem desencadear reações em cadeia.

Estabelecimento do contexto: Definição dos parâmetros externos e internos a serem levados em consideração ao gerenciar riscos, e estabelecimento do escopo e dos critérios de risco para a política de gestão de riscos.

Nota 1: As informações podem referir-se à existência, natureza, forma, probabilidade, severidade, avaliação, aceitabilidade, tratamento ou outros aspectos da gestão de riscos.

Nota 2: A consulta é um processo bidirecional de comunicação sistematizada entre uma organização e suas partes interessadas ou outros, antes de tomar uma decisão ou definir a direção a respeito de questão específica. A consulta é:

- *um processo que impacta uma decisão através da influência ao invés do poder; e*
- *uma entrada para o processo de tomada de decisão, e não uma tomada de decisão em conjunto.*

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 continua da gestão de riscos através de toda a organização.

Nota 1: Os fundamentos incluem a política, objetivos mandatos e comprometimento para gerenciar riscos.
Nota 2: Os arranjos organizacionais incluem planos, relacionamentos, responsabilidades, recursos, processos e atividades.
Nota 3: A estrutura da gestão de riscos está incorporada no âmbito das políticas e práticas estratégicas e operacionais para toda a organização.

Evento: Ocorrência ou alteração em um conjunto específico de circunstancias.

Nota 1: Um evento pode consistir de uma ou mais ocorrências, e pode ter várias causas.
Nota 2: Um evento pode consistir em alguma coisa não acontecer.
Nota 3: Um evento pode algumas vezes ser referido como "incidente" ou um "acidente".
Nota 4: Um evento sem consequência também pode ser referido como "quase acidente", ou um "incidente" ou "quase sucesso".

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

Nota: Uma fonte de risco pode ser tangível ou intangível.

Gestão de riscos: Atividades coordenadas para dirigir e controlar uma organização no que se refere ao risco.

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

Nota 1: A identificação de riscos envolve a identificação das fontes de risco, evento, suas causas e suas consequências potenciais.
Nota 2: A identificação de riscos pode envolver dados históricos, análises teóricas, opiniões de pessoas informadas e especialistas, e as necessidades das partes interessadas.

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

Nota: O monitoramento pode ser aplicado a estrutura da gestão de riscos, ao processo de gestão de riscos, ao risco ou aos controles.

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

Parte interessada: Pessoa ou organização que pode afetar, ser afetada, ou perceber–se afetada por uma decisão ou atividade.

Nota: Um tomador de decisão pode ser uma parte interessada.

Perfil do risco: Descrição de um conjunto qualquer de riscos.

Nota: O conjunto de riscos pode conter riscos que dizem respeito à toda a organização, à parte da organização, ou referente ao qual tiver sido definido.

Plano de gestão de riscos: Esquema dentro da estrutura da gestão de riscos, especificando a abordagem, os componentes de gestão e os recursos a serem aplicados para gerenciar riscos.

Nota 1: Os componentes de gestão tipicamente incluem procedimentos, práticas, atribuição de responsabilidades, sequencia e a cronologia das atividades.
Nota 2: O plano de gestão de riscos pode ser aplicado a um determinado produto, processo e projeto, em parte ou em toda a organização.

Política de gestão de riscos: Declaração das intenções e diretrizes gerais de uma organização relacionadas à gestão de riscos.

Probabilidade: Chance de algo acontecer.

Nota 1: Na terminologia de gestão de riscos, a palavra "probabilidade" é utilizada para referir-se à chance de algo acontecer, não importando se definida, medida ou determinada objetiva ou subjetivamente, qualitativa ou quantitativamente, ou se descrita utilizando-se termos gerais ou matemáticos (tal como uma probabilidade ou uma frequência durante um determinado período de tempo).

Nota 2: O termo em Inglês likelihood *não tem um equivalente direto em algumas línguas; em vez disso, o equivalente do termo* probability *é frequentemente utilizado. Entretanto, em Inglês,* probability *é muitas vezes interpretado estritamente como uma expressão matemática. Portanto, na terminologia de gestão de riscos,* likelihood *é utilizado com a mesma ampla interpretação de que o termo* probability *tem em muitos outros idiomas além do Inglês.*

Processo de avaliação de riscos: Processo global de identificação de riscos, análise de riscos e avaliação 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.

Proprietário do risco: Pessoa ou entidade com a responsabilidade e a autoridade para gerenciar o risco.

Risco: Efeito da incerteza nos objetivos

Nota 1: Um efeito é um desvio em relação ao esperado – positivo e/ou negativo.

Nota 2: Os efeitos podem ter diferentes aspectos (tais como metas financeiras, de saúde e segurança e ambientais) e podem aplicar-se em diferentes níveis (tais como estratégico, em toda a organização, de projeto,d e produto e de processo).

Nota 3: O risco é muitas vezes caracterizado pela referência aos eventos potenciais e às consequências, ou uma condição destes.

Nota 4: O risco é muitas vezes expresso em termos de uma combinação de consequências de um evento (incluindo mudanças nas circunstanciais) e a probabilidade de ocorrência associada.

Nota 5: A incerteza é o estado, mesmo que parcial, da deficiência das informações relacionadas a um evento, sua compreensão, conhecimento, sua consequência ou probabilidade.

Risco residual: Risco remanescente após o tratamento do risco.

Nota 1: O risco residual pode conter riscos não identificados.

Nota 2: O risco residual também pode ser conhecido como "risco retido".

Tratamento de riscos: Processo para modificar o risco.

Nota 1: O tratamento de risco pode incluir:

- *a ação de evitar o risco pela decisão de não iniciar ou descontinuar a atividade que dá origem ao risco;*
- *assumir ou aumentar o risco a fim de buscar uma oportunidade;*
- *a remoção da fonte de risco;*
- *a alteração da probabilidade;*
- *a alteração das consequências;*
- *o compartilhamento do risco com outra parte ou partes (incluindo contratos e financiamento do risco), e;*
- *a retenção do risco por uma escolha consciente.*

Nota 2: Os tratamentos de riscos relativos a consequências negativas são muitas vezes referidos como "mitigação de riscos", "eliminação de riscos", "prevenção de riscos" e "redução de riscos".

Nota 3: O tratamento de riscos pode criar novos riscos ou modificar riscos existentes.