Manual de **Gestão de Riscos e Controles Internos**

CORSAN

Controle de Alterações

Versão	Data	Descrição
1	19.05.2017	Lançamento da Política de Gestão de Riscos Corporativos
2	02.09.2020	Revisão, adequação ao Código Brasileiro de Governança e ao Regulamento do Novo Mercado da B3, incorporação dos procedimentos de Controles Internos

Alçadas de Aprovação

Função	Responsável	Instrumento de Homologação	Data de Aprovação
Pré-aprovação Versão 1	Diretoria Colegiada	Ata 14/2017	13.03.2017
Aprovação Versão 1	Conselho de Administração	Ata 09/2017	19.05.2017
Pré-aprovação Versão 2	Diretoria Colegiada	Ata 46/2020	24.08.2020
Aprovação Versão 2	Conselho de Administração	Ata 14/2020	02.09.2020

Versão 1 elaborada e revisada por:

Departamento de Gestão de Riscos – DEGER/SUCORP

Versão 2 revisada e adequada por:

Departamento de Gestão de Riscos – DEGER/SUCORP

Aprovado por:

Conselho de Administração

1 OBJETIVO

Este Manual é parte integrante da Política de Gestão de Riscos e Controles Internos – PGERCI – e tem por finalidade auxiliar os profissionais responsáveis por aplicar a metodologia de gestão de riscos e controles internos nos diversos níveis gerenciais da Corsan, estabelecendo os procedimentos para identificar, analisar, avaliar, tratar e monitorar os riscos e os controles internos nos processos da Companhia, em consonância com os objetivos, princípios e diretrizes lançados pela PGERCI, e de acordo com padrões definidos pela norma ISO 31.000/2018.

2 PROCESSO DE GESTÃO DE RISCOS

As unidades organizacionais, sob supervisão do Comitê Executivo de Riscos – CER – devem identificar, analisar, avaliar, tratar e monitorar os riscos dos ambientes interno e externo, associados aos seus processos de negócio, de acordo com o esquema geral do processo ilustrado na figura 1, abaixo. As etapas do processo de gestão de riscos são descritas com maiores detalhes a seguir:

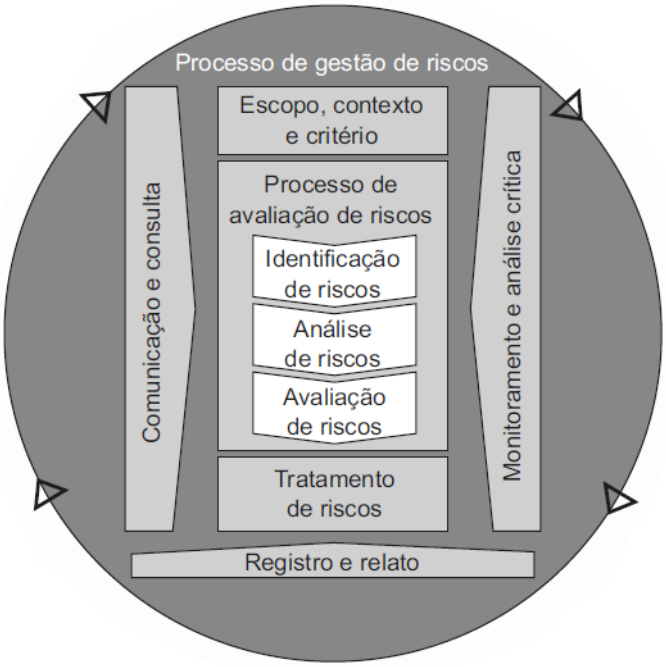


Figura 1: Esquema do Processo de Gestão de Riscos
Fonte: Framework ISO 31.000:2018

2.1 Comunicação e Consulta

A constante e efetiva comunicação e consulta entre as três linhas de atuação, bem como a contextualização estratégica, são fases que permeiam todo o processo de gestão de riscos. O estabelecimento de uma comunicação eficaz é de suma importância, uma vez que a gestão de riscos precisa acontecer em todos os níveis da Companhia, sendo necessário sensibilizar todos os atores envolvidos. A etapa de comunicação e consulta depende do protagonismo do CER na capilarização e execução efetiva dos procedimentos junto às unidades organizacionais representadas por seus membros.

Os planos de comunicação e consulta devem ser desenvolvidos em um estágio inicial, abordando questões relacionadas aos riscos propriamente ditos, suas causas, consequências, quando os conhecemos e as medidas que estão sendo tomadas para tratá-los. A comunicação e consulta internas e externas, quando eficazes, têm como objetivo assegurar que os responsáveis pela implementação do processo de gestão de riscos e as partes interessadas compreendam os fundamentos sobre os quais as decisões são tomadas e as razões pelas quais ações específicas são requeridas.

A abordagem da equipe consultiva pode auxiliar a estabelecer o contexto apropriadamente e garantir que os interesses das partes sejam compreendidos e considerados. É necessário assegurar que os riscos sejam identificados adequadamente, reunindo diferentes áreas de especialização em conjunto para análise de riscos, a qual possa avaliar os diferentes pontos de vista que sejam devidamente considerados, garantidos o aval da Administração e o apoio para uma agenda de treinamento e encontros periódicos, a fim de desenvolver e aprimorar constantemente o processo de comunicação e consulta.

2.2 Estabelecimento do Escopo, Contexto e Critérios

O estabelecimento do contexto estratégico refere-se ao alinhamento necessário entre a definição dos riscos e como estes afetam o atingimento dos objetivos estratégicos e organizacionais. Nesta etapa, são definidos os objetivos, responsabilidade, escopo das atividades a serem realizadas, sua profundidade e amplitude, os processos a serem identificados e mapeados, a relação entre projetos/processo/atividades, metodologias a adotar, estabelecimento de indicadores e dados de desempenho, especificação e definição de estudos necessários, extensão dos recursos requeridos.

Na gestão de riscos, é necessário avaliar como o nível de risco deve ser determinado e os pontos de vista das diferentes partes interessadas, pois todo o processo deve ser discutido à exaustão, tendo em vista que nenhum processo de gestão de riscos e controles, sem que haja engajamento, promove sucesso à organização. Além disso, é fundamental o apoio da alta Administração ao processo, inclusive porque é ela que determina, em última instância, o nível em que um risco se torna aceitável ou tolerável para a organização.

2.3 Identificação de riscos

Na etapa de identificação de riscos, são definidos os eventos, externos ou internos, que podem impactar (positiva ou negativamente) os objetivos estratégicos da organização, inclusive os relacionados aos ativos intangíveis. A finalidade é produzir uma lista abrangente de riscos, baseada nos eventos que possam criar, reduzir, acelerar ou atrasar a realização dos objetivos da Companhia. Deve-se estabelecer uma sinergia produtiva entre a área de gestão de riscos e controles com as demais unidades organizacionais, por intermédio da atuação do Comitê Estratégico de Riscos – CER, ente interdepartamental que possui uma representatividade transversal e auxilia na detecção ou construção de fontes tangíveis e intangíveis de risco, causas e eventos, ameaças e oportunidades, vulnerabilidades e capacidades, mudanças nos contextos externo e interno, indicadores de riscos emergentes, natureza e valor dos ativos e recursos, consequências e seus impactos nos objetivos, limitações de conhecimento e de confiabilidade da informação, fatores temporais, vieses, hipóteses e crenças dos envolvidos.

Abaixo, são descritas as sub etapas adotadas pela Companhia para auxiliar na identificação dos riscos:

2.3.1 Listagem de riscos

A listagem deve ser construída pela realização de reuniões do tipo *brainstorming*, a fim de desenvolver a compreensão dos riscos, tanto dos conhecidos quanto dos desconhecidos, e fornecer um ponto de partida para a avaliação dos riscos e para as decisões sobre o tratamento dos riscos. Os riscos desconhecidos são aqueles que nunca aconteceram na organização, porém são riscos exequíveis, ou seja, poderão ocorrer em algum momento.

2.3.2 Classificação de riscos

Os riscos identificados devem ser classificados em categorias, e para cada um deve-se dar um nome para codificação e referência. A Corsan optou pela seguinte classificação:

a. **Riscos estratégicos:** atrelados à tomada de decisão da Administração, podem gerar perda substancial no valor econômico da organização. Exemplos: falhas na antecipação ou reação ao movimento dos concorrentes; diminuição de demanda do mercado por produtos e serviços da empresa causada por obsolescência em função de desenvolvimento de novas tecnologias ou alteração do ambiente regulatório da prestação de serviços;

b. **Riscos financeiros:** associados à exposição das operações financeiras da organização. É, por exemplo, o risco de liquidez, que ocorre quando os fluxos de caixa não são administrados efetivamente, para maximizar a geração de caixa operacional, gerenciar os riscos e retornos específicos das transações financeiras, de forma a manter um nível satisfatório de disponibilidades para honrar os compromissos assumidos, e também para facilitar a captação e aplicação de recursos conforme as políticas

estabelecidas e o plano de investimentos da Companhia. Pode ser também o risco de liquidez;

c. **Riscos operacionais:** associados à possibilidade de ocorrência de perdas (de produção, ativos, clientes, receitas) resultantes de falhas, deficiências ou inadequação de processos e sistemas internos, assim como a influência de eventos externos, como catástrofes naturais, alterações no ambiente regulatório, greves, pandemias e outros. Os riscos operacionais geralmente acarretam redução, degradação ou interrupção, total ou parcial, das atividades da Companhia, com impacto negativo em sua reputação, além da potencial geração de passivos contratuais, fiscais, trabalhistas e ambientais;

d. **Riscos de conformidade legal:** também chamados de riscos de *compliance*, são relacionados a temas ligados ao ambiente regulatório e normativo no qual a Corsan atua, que engloba regramentos das mais variadas esferas, desde saúde e segurança do trabalhador, passando por meio ambiente, práticas comerciais, proteção do consumidor, proteção de dados, e diversos 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.

2.4 Análise de riscos

O propósito da análise de riscos é compreender a natureza dos riscos e suas características, incluindo o nível do risco, onde for apropriada a sua aplicação. A análise de riscos envolve a consideração detalhada de

incertezas, dos fatores de risco, suas consequências, probabilidades, eventos associados, cenários possíveis, eficácia dos controles aplicados, caso existentes, ou criação de mecanismos de controle. Um evento pode ter múltiplas causas e consequências e pode afetar múltiplos objetivos. A Companhia optou, neste momento, pela análise 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 análise de riscos possui dois parâmetros centrais:

a. Conhecer, ou tentar prever, a chance, a **probabilidade** de riscos concretizarem-se, consideradas as condições atuais e futuras dos processos e áreas de negócio aos quais os riscos se associam;

b. Calcular o **impacto**, as consequências de cada risco para os processos associados.

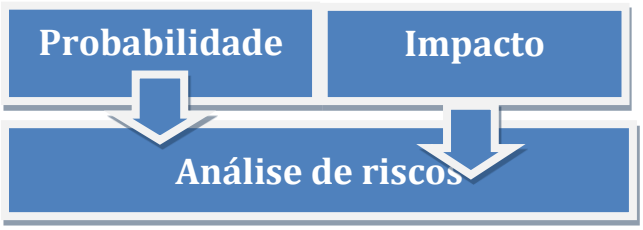


Figura 2: Probabilidade e impacto na avaliação de riscos

2.4.1 Probabilidade

Para conhecer ou tentar prever a probabilidade de um risco concretizar-se, são utilizados dois critérios: fator de risco (FR) e exposição (E). O cruzamento desses dois critérios resulta no grau de probabilidade (GP). O GP

está alicerçado em uma fórmula simples, que calcula de forma direta, através da multiplicação dos dois critérios, o nível de possibilidade do evento vir a acontecer, frente a sua condição e exposição.

2.4.1.1 Fator de risco (FR):

Os fatores de risco, ou fontes de risco (definição da ISO 31000) são, na realidade, a origem e/ou causa de cada evento identificado em cada processo. Para compreender o risco ou as condições em que o risco ocorre ou pode ocorrer, faz-se necessário dissecar os eventos e levar em consideração a maior quantidade de fatores possível, buscando entender quais são os fatores que mais influenciam a ocorrência ou concretização de cada risco.

De forma a facilitar a identificação e composição dos fatores de risco, foram organizados seis agrupamentos de fatores de risco – Lógica de controle e controles alternativos (LCCA), Recursos Humanos (RH), Tecnologia da Informação (TI), Infraestrutura (IE), Ambiente Externo (AE) e Processos (P) – identificados no diagrama de causa e efeito da figura 3.

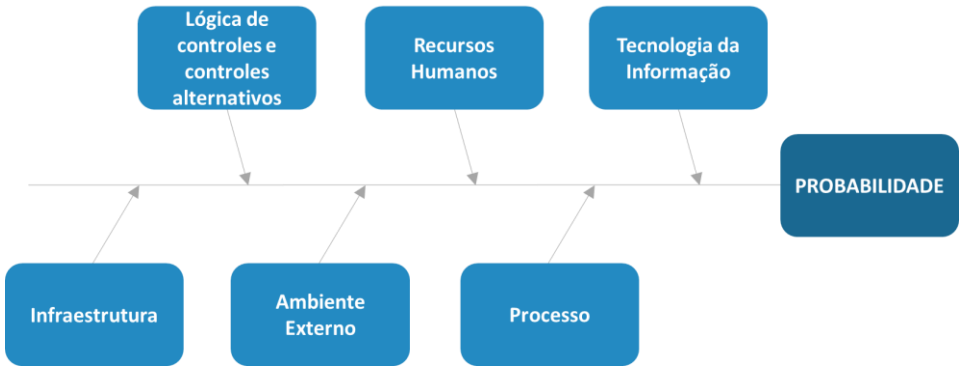


Figura 3: Diagrama de causa e efeito: fatores de risco x probabilidade

Os fatores possuem uma escala de valoração, que mede o nível de influência de cada aspecto para a concretização do risco, conforme descrito na tabela abaixo:

Nível de influência dos fatores na concretização do risco	
Escala	Pontuação
Melhoria completa necessária nos controles e processos	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 seis agrupamentos de fatores de risco, é atribuída 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 somar as notas atribuídas e dividir por seis, para determinar o grau final (média) da variável "fator de risco" (FR), conforme demonstrado na fórmula abaixo:

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

2.4.1.2 Exposição (E):

Assim como no tópico anterior, o critério de exposição (E) possui uma escala de valoração, que mede a frequência em que um evento costuma se manifestar, ao ser analisado um risco. É importante frisar que a escala de valores leva em conta o histórico de exposição, a condição atual e a previsão futura. Deve ter uma visão não só projetiva, mas também prospectiva. A tabela a seguir descreve os graus de exposição:

Graus de Exposição	
Frequência	Pontuação
Dia/Semana	5
Quinzenal	4
Mensal	3
Anual	2
Eventual	1

2.4.1.3 Grau de Probabilidade (GP):

O GP é o resultado da multiplicação do valor final do fator de risco (FR) versus o grau da exposição (E), conforme demonstrado a seguir:

GP = FR X E

Esta multiplicação direta representa o grau de probabilidade (valor máximo: 25), com a classificação dividida em cinco níveis (escala 1). 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 da Probabilidade	
≤ 5	1	Muito Baixa	≤ 20%
> 5 a ≤ 10	2	Baixa	> 20% a ≤ 40%
> 10 a ≤ 15	3	Média	> 40% a ≤ 60%
> 15 a ≤ 20	4	Alta	> 60% a ≤ 80%
> 20	5	Muito Alta	> 80%

Resultado da multiplicação GP = FR x E

Equivalência para matriz de riscos

Equivalência em Percentual: fator de multiplicação 4%

2.4.2 Impacto

Além da probabilidade, o outro parâmetro utilizado na análise de risco é o impacto. Para mensurá-lo, busca-se uma visão holística de causas e efeitos dos fatores que influenciam o grau de impacto de cada risco. Cada fator, ou dimensão de impacto, tem um peso diferenciado, de acordo com seu grau de importância para a organização: Legal (peso 4), Financeiro (peso 4), Operacional (Peso 5) e Imagem (Peso 2). Adicionalmente, é atribuída uma nota de 1 a 5, de acordo com uma escala de impacto atribuída a cada fator, a fim de se obter uma nota final, que expressa o nível de impacto total de cada risco. Os fatores de impacto (FI) são demonstrados no diagrama de causa e efeito da figura 4, e detalhados nas tabelas seguintes:

Figura 4: Diagrama de Causa e Efeito – Fatores de Impacto

Fator de Impacto - IMAGEM	
Escala	Pontuação
De Caráter Nacional – Brasil	5
Regional – Estado RS	4
Local – Região Metropolitana	3
De Caráter Interno – Dentro da Organização	2
De Caráter Interno – Dentro da Área	1

Nota - No impacto de imagem, levar em conta visões distintas, ou seja, sob o ponto de vista da Corsan (determinada área/localidade) e sob o ponto de vista do cliente, considerando sempre a maior nota. Por exemplo: imagem na visão do Corsan (determinada área/localidade) valorada como 3 e imagem na visão do cliente valorada como 5, considerar a maior nota (5).

Fator de Impacto - FINANCEIRO	
Escala	Pontuação
Catastrófico - Acima de R$ 5.000.001,00	5
Severo – De R$ 500.001,00 Até R$ 5.000.000,00	4
Moderado – De R$ 50.001,00 Até R$ 500.000,00	3
Leve – De R$ 25.001,00 Até R$ 50.000,00	2
Insignificante - Até R$ 25.000,00	1

Fator de Impacto - LEGAL	
Escala	Pontuação
Perturbações muito graves	5
Graves	4
Limitada	3
Leve	2
Muito Leve	1

Fator de Impacto - OPERACIONAL	
Escala	Pontuação
Perturbações muito graves (impacta outros processos muito fortemente)	5
Graves (impacta outros processos de forma direta)	4
Limitadas (Impacta somente o próprio processo consideravelmente)	3
Leves (Impacta somente o próprio processo levemente)	2
Muito Leves (não impacta nada)	1

Nota: no tocante ao fator de impacto Legal, deverão ser avaliadas, como consequências para a organização, as responsabilidades civil, regulatória, tributária, criminal e trabalhista.

O nível de impacto final do risco, ou simplesmente impacto, é a soma dos resultados de cada fator de impacto, multiplicados pelos seus respectivos pesos, e divididos por 15 (soma dos pesos dos 4 fatores), de forma que o valor final de cada nível de impacto não seja maior do que 5, conforme demonstrado na fórmula:

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

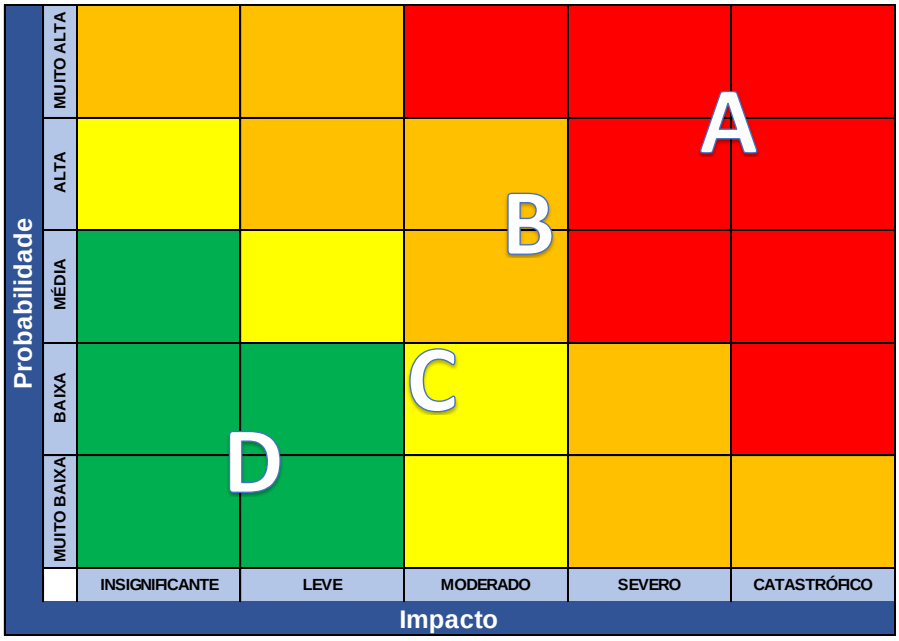
O resultado do nível de impacto é descrito na tabela abaixo:

Grau de Impacto	Escala	Nível de Impacto
> 4,50	5	Catastrófico
> 3,50 a ≤ 4,50	4	Severo
> 2,50 a ≤ 3,50	3	Moderado
> 1,51 a ≤ 2,50	2	Leve
≤ 1,50	1	Insignificante

2.4.3 Matriz de riscos

Com o objetivo de visualizar e, ao mesmo tempo, implementar uma forma de tratamento para cada risco, o resultado da análise de riscos é apresentado em um mapa de riscos (matriz de monitoramento de riscos). A matriz de riscos demonstra os pontos de cruzamento (horizontal e vertical)

da probabilidade de ocorrência e do impacto. Desta forma, pela divisão da matriz em quatro regiões, pode-se avaliar o nível de vulnerabilidade do processo impactado por determinado risco. Quanto maior a probabilidade e o impacto de um risco, maior será seu grau de criticidade, e maior deverá ser a prioridade de tratamento daquele risco. As tabelas abaixo ilustram a matriz de riscos e a escala de priorização de tratamento, de acordo com o grau de criticidade de cada risco:



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

2.5 Avaliação de riscos

Os riscos serão avaliados de acordo com o a região em que estiverem localizados na matriz de riscos. Quanto maior o nível de tratamento do risco, maior sua criticidade para o processo. O nível de tratamento serve para a organização determinar seu apetite ao risco, ao priorizar os riscos que

deverão ser tratados com mais urgência, e ao determinar os níveis de tratamento que serão admitidos. Por exemplo, os riscos plotados no quadrante A (vermelho) são considerados como intoleráveis para a organização, e deverão ter ação e tratamento imediatos por parte dos profissionais envolvidos no processo de gestão de riscos e controles, com o apoio da Administração. Abaixo estão descritos os 4 níveis de tratamento dos riscos, utilizados na fase de avaliação:

a. **Quadrante A (vermelho):** Os riscos localizados no quadrante A são aqueles que têm alta probabilidade de ocorrência e poderão resultar em impacto extremamente severo, caso ocorram. Exigem a implementação imediata de estratégias de proteção e prevenção – **ação imediata;**

b. **Quadrante B (laranja):** Os riscos localizados no quadrante B costumam ser muito danosos à empresa. Seu grau de probabilidade pode variar de muito baixo, mas com alto impacto, ou alta probabilidade de ocorrer, mas com baixo impacto. Devem ser providenciadas ações rápidas de tratamento a esses riscos, idealmente planejadas e testadas em um plano de contingência, além de ações preventivas. A diferença do quadrante A é que as ações podem ser implementadas com mais planejamento e tempo – **ação de curto a médio prazo;**

c. **Quadrante C (amarelo):** No quadrante C, estão os riscos com alta probabilidade de ocorrência, mas com consequências gerenciáveis à empresa. Os riscos classificados neste quadrante devem ser monitorados de forma rotineira e sistemática, podendo também possuir planos de emergência – **monitoramento e gestão;**

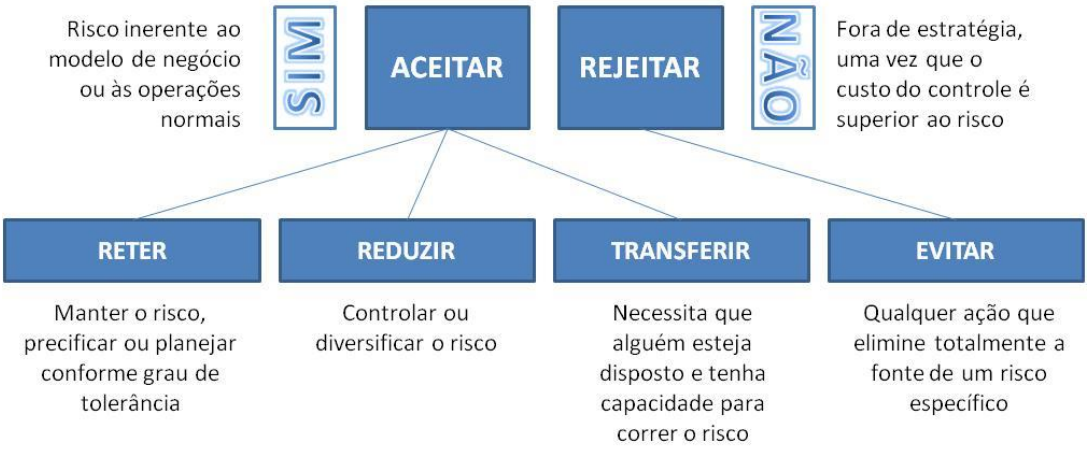
d. **Quadrante D (verde):** Os riscos classificados no quadrante D possuem baixa probabilidade e pequeno impacto, representando pequenos problemas e prejuízos. Estes riscos somente devem ser tratados caso os benefícios gerados pela sua mitigação sejam superiores aos custos de implementação de controles – **risco tolerável.**

2.6 Tratamento de Riscos

No tratamento de um risco, a Administração define qual será a resposta que a empresa terá que operacionalizar depois de avaliá-lo e decidir ser irá reter, reduzir, transferir ou evitar o risco. O enfrentamento aos riscos identificados pela Companhia dar-se-á pela aplicação de controles internos, cuja existência ou carência deverá ser identificada pela 1ª e 2ª linhas, em cada circunstância, com monitoramento e fiscalização da 3ª linha. Em todo caso, cabe à Administração definir se deve instituir novos controles internos, a partir da ponderação da relação entre os esforços de implementação e os benefícios estimados. Os controles internos atacam as causas (fatores) dos riscos, por isso a identificação dos controles pressupõe a definição dos fatores de riscos.

2.6.1 Matriz de Responsabilidades

A Administração é responsável pelo gerenciamento de riscos da Corsan e, portanto, por definir a resposta a ser adotada para seu tratamento. O diagrama a seguir exemplifica as estratégias de tratamento dos riscos:



- **Evitar o risco**: decisão de não iniciar ou continuar com a atividade que dá origem ao risco;

- **Aceitar o risco**: neste caso, apresentam-se três alternativas:

  a. **Reter**: manter o risco no nível atual de impacto e probabilidade;

  b. **Reduzir**: ações são tomadas para minimizar a probabilidade e/ou o impacto do risco;

  c. **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 parte do risco

2.6.2 Estrutura de Controles Internos

A estrutura conceitual de controles internos, desenvolvida pelo COSO (*Committee of Sponsoring Organizations of the Treadway Commission)*, atualmente é a mais aceita entre as companhias abertas nacionais e

internacionais, tendo sido também a estrutura recomendada pelo PCAOB (*Public Company Accounting Oversight Board*) e pela SEC (*Security and Exchange Comission* – Comissão de Títulos e Câmbio dos Estados Unidos). Os cinco componentes de um sistema de controles internos são caracterizados da seguinte maneira:

a. **Ambiente de controle**: estabelece a base para o sistema de controles internos, por meio do fornecimento de disciplina e estrutura fundamentais, em que a organização demonstra ter comprometimento com a integridade e os valores éticos; estabelecendo as estruturas, os níveis de subordinação e as autoridades e responsabilidades adequadas, fazendo com que as pessoas assumam responsabilidade por suas funções de controle interno na busca pelos objetivos. Além disso, a estrutura de governança deve demonstrar independência em relação aos seus executivos e supervisionar o desenvolvimento e o desempenho dos controles internos.

b. **Avaliação de riscos**: envolve a identificação e a análise pela gestão – não pelo auditor interno – dos riscos relevantes para o alcance dos objetivos predeterminados. A organização deve considerar o potencial de fraude na avaliação dos riscos, além de identificar e avaliar as mudanças que podem afetar, de forma significativa, o sistema de controles internos.

c. **Atividades de controle** (ou políticas, procedimentos e práticas): asseguram que os objetivos da gestão sejam alcançados e que as estratégias de mitigação dos riscos sejam implementadas, ou seja, a organização seleciona e desenvolve atividades de controle que contribuem para a redução, a níveis aceitáveis, dos riscos à realização dos objetivos.

d. **Informação e comunicação**: suporta todos os outros componentes de controle, por meio da comunicação das responsabilidades de controle aos empregados e por meio do fornecimento de informações que permitam às pessoas o cumprimento das suas responsabilidades. Diz respeito à produção de relatórios, tanto operacionais, quanto financeiros, necessários para o controle e gestão da organização;

e. **Monitoramento:** a organização seleciona, desenvolve e realiza avaliações contínuas para se certificar da efetividade do sistema de controles internos. Inclui a supervisão externa dos controles por parte da gestão ou de outras partes externas ao processo. Também pode consistir na aplicação de metodologias independentes (como procedimentos customizados ou listas de verificação padronizadas) por parte das pessoas envolvidas em um processo.

De acordo com o COSO, os três principais objetivos de um sistema de controles internos são:

- assegurar **operações** eficazes e eficientes;
- produção de **relatórios financeiros** corretos e confiáveis; e
- **conformidade** com as leis e regulamentos.

A figura 5 apresenta as três dimensões da estrutura de controles internos, segundo o modelo COSO:

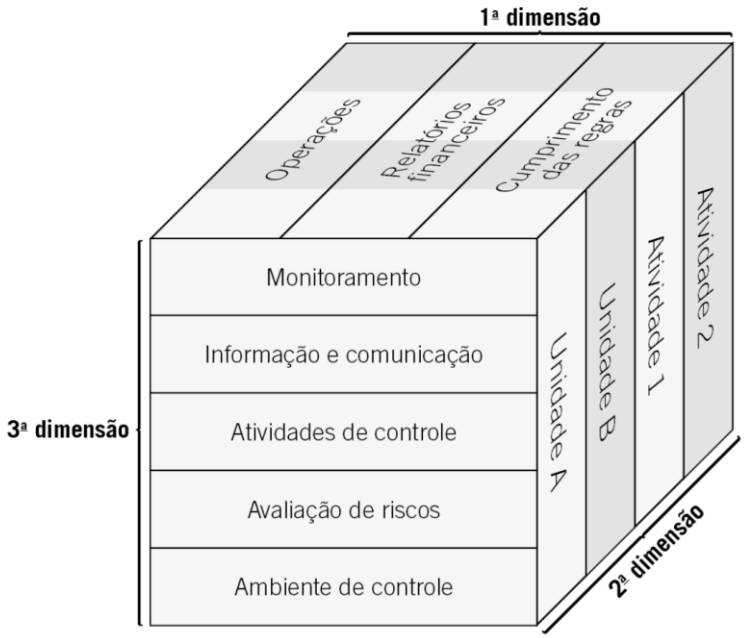


Figura 5: *COSO CUBE – Internal Control – Integrated Framework*

A partir da estrutura de controles internos, deve-se verificar se os procedimentos ou atos que possibilitam segurança quanto aos aspectos lógicos e técnicos dos processos são realizados de forma eficiente e tempestiva e, neste contexto, mesmo que a estrutura seja implantada de forma adequada em todas as suas dimensões, não é possível assegurar um nível de conformo pleno, porque há limitações inerentes. Dessa maneira, faz-se necessária a aplicação das seguintes etapas, de forma a se alcançar maior otimização da estrutura de controles internos na Companhia:

a. **Mapeamento de processos** - Primeira etapa, na qual se identificam as necessidades de controle, com definição de pontos de controle, periodicidade e responsáveis pelo monitoramento;

b. **Auto-avaliação dos pontos de controle** – Nesta etapa são realizadas auto-avaliações sobre o nível de conformidade dos pontos de controle e enviadas para consolidação à SUCORP;

c. **Consolidação das auto-avaliações** - As avaliações reportadas no período à SUCORP serão consolidadas e analisadas em conjunto com o Departamento de Gestão de Riscos – DEGER;

d. **Avaliação de pontos críticos** – A SUCORP, em conjunto com o CER, avalia quais pontos possuem necessidade de maior atenção, podendo ser endereçados diretamente ao diretor responsável, ao Conselho de Administração e ao Comitê de Auditoria, ou apenas terem seus resultados monitorados;

e. **Revisão de pontos de controle** – Com base nos reportes consolidados, o Departamento de Gestão de Riscos – DEGER, fará análise amostral de pontos em conformidade para comprovação dos resultados e dos pontos em não conformidade recorrentes para endereçamento;

f. **Monitoramento** – As áreas responsáveis devem aplicar o plano de ação e monitorar os pontos de controle sob sua responsabilidade;

g. **Acompanhamento** – Os planos de ação implementados pelas áreas responsáveis serão acompanhados pela SUCORP, e o nível de conformidade dos processos deverá ser acompanhado periodicamente pelo Conselho de Administração e Comitê de Auditoria, possibilitando a identificação da necessidade de endereçamentos.

Os controles já instituídos na Companhia devem ser identificados pelos gestores responsáveis por cada processo (1ª linha), com apoio do CER. Os controles identificados devem ser cadastrados em rol destinado a registrar características intrínsecas a cada qual e, sistematicamente, deverão sujeitar-se a verificações de efetividade na mitigação dos riscos e da vantajosidade em sua implementação, quando for o caso. Para facilitar essa identificação, estão descritas a seguir algumas naturezas de controles internos:

a. **Controles automatizados**: executados por sistema seguros e confiáveis, não dependendo de julgamentos pessoais para garantir a consistência, precisão e tempestividade:

b. **Controles compensatórios**: executados quando da ausência de implantação dos demais controles;

c. **Controles detectivos**: executados ao longo do processo. Detectam erros que são difíceis de definir ou prever;

d. **Controles diretivos**: controles que direcionam para os comportamentos desejados, porém não garantem ou previnem a ocorrência de falhas e erros intencionais ou não;

e. **Controles manuais**: executados por pessoas, sem suporte sistêmico;

f. **Controles preventivos**: executados no início do processo. Previnem o acontecimento de erros ou irregularidades e minimizam os riscos na fonte.

2.6.3 Planos de ação

O plano de ação é o conjunto de medidas organizacionais, sistemas técnicos de prevenção e monitoramento e recursos humanos que protagonizarão a implantação de controles/ações para a gestão dos riscos. É elaborado com base nos fatores de riscos visando mitigá-los, e deverá ser constituído utilizando-se o modelo 5W2H.

What?	Who?	When?	Where?	Why?	How?	How Much?
O que?	Quem?	Quando?	Onde?	Por quê?	Como?	Quanto Custa?
Medida em relação à causa prioritária	Nome do responsável pela implementação da ação	Data limite para implementação da ação	Onde a ação será implementada	Qual o motivo para realização da ação	Descrever como será executada ação proposta	Qual o valor do investimento

- O plano de ação formal 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 unidade organizacional para qual o risco foi transferido pode não o gerenciar de maneira eficaz.

O plano de ação apresentará a seguinte estrutura:

- Número da recomendação proposta por qualquer das 3 linhas;
- Risco e respectivo grau;
- Unidade e/ou departamento a que o risco se aplica;

- Descrição da situação atual;
- Descrição da recomendação proposta (situação proposta);
- Áreas envolvidas;
- Responsável: gestor responsável pela implementação das recomendações nas respectivas unidades;
- Prazo (mês/ano): data negociada para a efetiva implementação da recomendação.

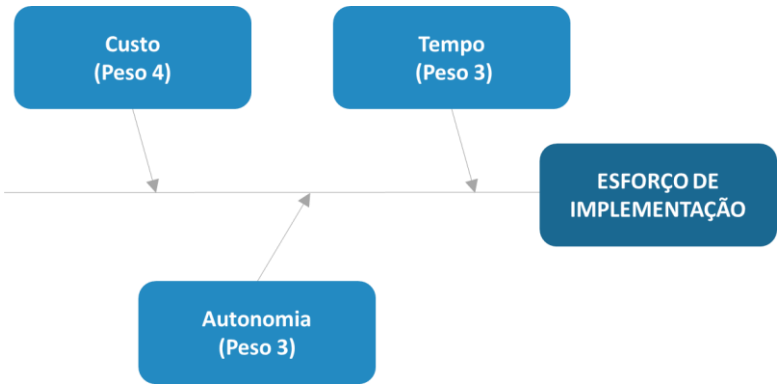
2.6.4 Priorização de implementação de controles

Ferramenta que objetiva fazer com que o gestor e/ou o analista possam enxergar, de forma mais prática e objetiva, através de critérios preestabelecidos e plotados em uma matriz, as ações que serão prioritárias em termos de benefício. Os dois macro critérios são:

- Esforço de implementação
- Benefício Estimado

2.6.4.1 Esforço de implementação

O esforço de implementação é obtido da média ponderada de três subcritérios, com os seguintes pesos:



Abaixo estão descritos os subcritérios e definições:

Sub-critério	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 dependerá de uma diretoria ou do próprio departamento.

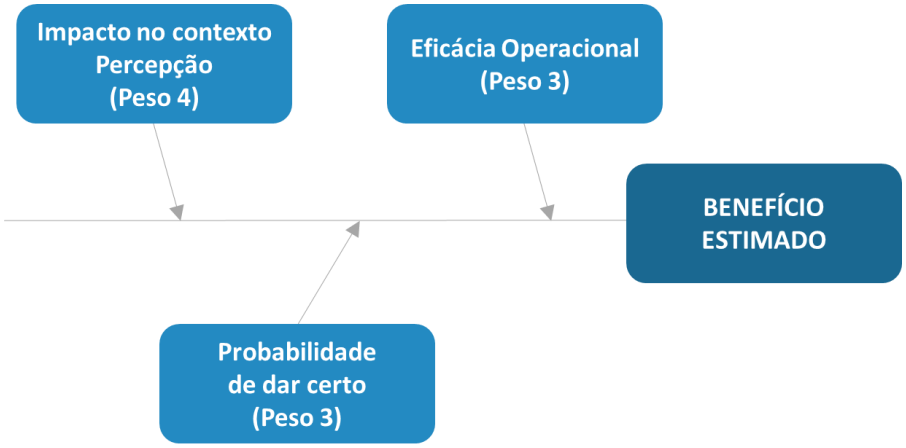
A nota varia de 1 a 5, de acordo com o nível de esforço. Quanto maior o esforço maior a nota. O grau de esforço de implementação é conseguido somando-se as notas de cada subcritério, e dividindo por 09 (somatório dos pesos). A partir daí temos a média ponderada:

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

Grau Impacto	Nível
> 4,50	Insatisfatório
> 3,51 a ≤ 4,50	Ruim
> 2,51 a ≤ 3,50	Bom
> 1,51 a ≤ 2,50	Muito Bom
≤ 1,50	Excelente

2.6.4.2 Benefício Estimado

O benefício estimado é medido a partir da média ponderada de três subcritérios, em que são aplicados os seguintes pesos:



Abaixo estão descritos os subcritérios e definições:

Subcritério	Definição
Impacto no Contexto	Significa quanto a ação pode gerar de resultado no contexto estabelecido.
Probabilidade	É a estimativa da ação ser operacionalizada com sucesso diante da estrutura e recursos da empresa.
Eficácia Operacional	É a estimativa do quanto a ação pode continuar gerando de resultado, após sua implantação.

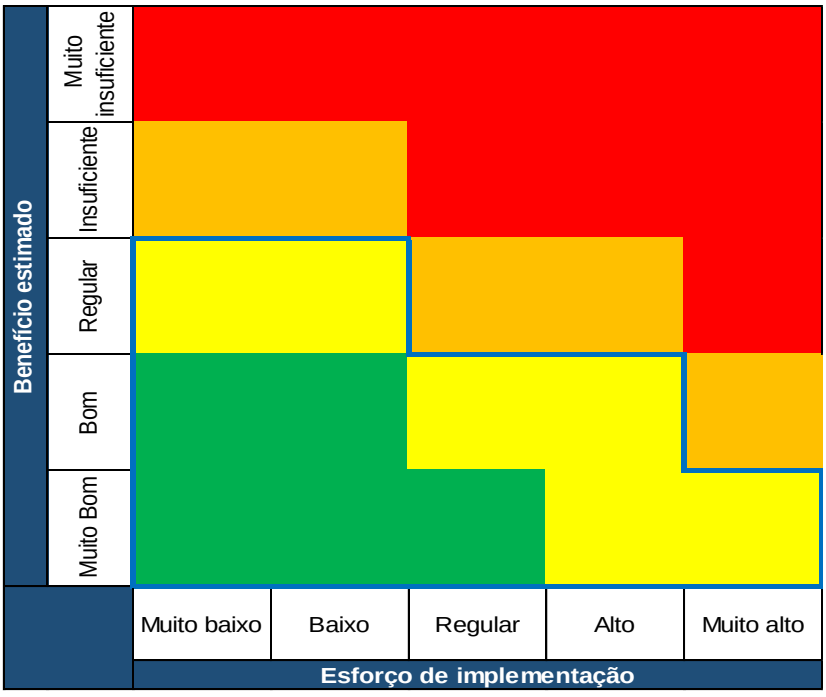
A nota varia de 1 a 5, de acordo com o nível de benefício. Quanto maior o benefício maior a nota. O grau de benefício estimado é conseguido somando-se as notas de cada subcritério, e dividindo por 10 (somatório dos pesos). A partir daí temos a média ponderada:

$$\text{Benefício Estimado} = \frac{\text{Impacto Contexto + Prob. de Dar Certo + Eficácia Op.}}{\text{10 (soma dos pesos 4+3+3)}}$$

Grau Impacto	Nível
> 4,50	Excelente
> 3,51 a ≤ 4,50	Muito Bom
> 2,51 a ≤ 3,50	Bom
> 1,51 a ≤ 2,50	Regular
≤ 1,50	Insuficiente

2.6.4.3 Matriz de Priorização de Ações

O resultado do cruzamento dos dois macrocritérios (esforço de implementação x benefício estimado) resulta no grau de priorização do controle em análise, mediante esse resultado identificamos se a ação deve ou não ser operacionalizada. O recorte delimitado com linha azul, abaixo, indica as situações prioritárias.



OPERACIONALIZAÇÃO DE CONTROLE			
AÇÃO DEVE SER ADOTADA PRIORITARIAMENTE	AÇÃO DEVE SER ADOTADA	AÇÃO DEVE SER REAVALIADA OU ADOTADA MÉDIO E LONGO PRAZO	AÇÃO NÃO DEVE SER ADOTADA

2.6.4.4 Execução dos planos de ação

Após a elaboração dos planos e a escolha da ação a ser executada, as atividades pertinentes deverão ser efetuadas em consonância com práticas descritas na Política de Gestão de Riscos e neste Manual, devidamente alinhadas entre os gestores envolvidos e com o apoio da SUCORP e do CER.

2.7 Monitoramento e análise crítica

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, sendo 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 os planos de ação e os sistemas de controles internos.

Uma das formas de monitoramento e análise crítica dá-se através da aplicação de questionários, nos quais são avaliados diversos aspectos do gerenciamento de riscos e controles internos, tais como o efetivo estabelecimento, progresso e eficácia dos planos de ação, a identificação de novos fatores de risco e sua importância nos respectivos riscos, as respostas aos riscos, incluindo eventuais planos de contingência, a relação custo x benefício na implementação dos controles internos, bem como o papel da auditoria na avaliação e monitoramento dos riscos e controles internos, e até mesmo as necessidades de treinamento dos membros das equipes responsáveis pela gestão de riscos de cada processo.

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

Monitoramento e Análise Crítica		
Escala	**Pontuação**	**Descrição**
Nível muito alto de controle	5	• O nível mais alto realizável; • O nível que não precisa de mais nenhuma melhoria.
Nível suficiente de controle	4	• Nível alto, mesmo não sendo o mais alto; • O nível que chegará ao nível mais alto se for melhorado.
Nível mínimo necessário de controle	3	• O risco, a gama de gerenciamento e 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 nos controles	2	• Necessita de melhorias parciais; • O nível que irá alcançar o "Nível da necessidade" se melhorar; • Se algo não for feito, não alcançará o "Nível da necessidade".
Melhorias significativas nos controles	1	• É necessária uma porção maior de melhorias; • Torna-se um problema se continuar no mesmo nível.
Melhoria completa nos controles	0	• O nível no 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 a soma total de todas as pontuações. Na escala abaixo, que vai de 0 a 100 por cento, são exemplificados os níveis de monitoramento e os respectivos tratamentos:

NÍVEL DE MONITORAMENTO			TRATAMENTO
> 75% e ≤ 100%	4	Verde	Áreas ou departamentos que estão na zona de conforto, devendo ser gerenciadas e administradas.
> 50% e ≤ 75%	3	Amarelo	Áreas ou departamentos com alto grau de riscos, mas que causam consequências gerenciáveis à empresa. Essas áreas ou departamentos devem ser monitoradas de forma rotineira ou sistemática.
> 25% e ≤ 50%	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 constantemente monitoradas.
≤ 25 %	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 ou igual a 50%, são considerados como *intoleráveis* para a organização e devem sofrer ações e tratamento por parte dos gestores. A identificação do nível de monitoramento do risco, assim como o nível do risco, deve ser executada no mínimo anualmente, com o objetivo de monitorar e acompanhar a evolução dos risco e/ou controles.

2.8 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.

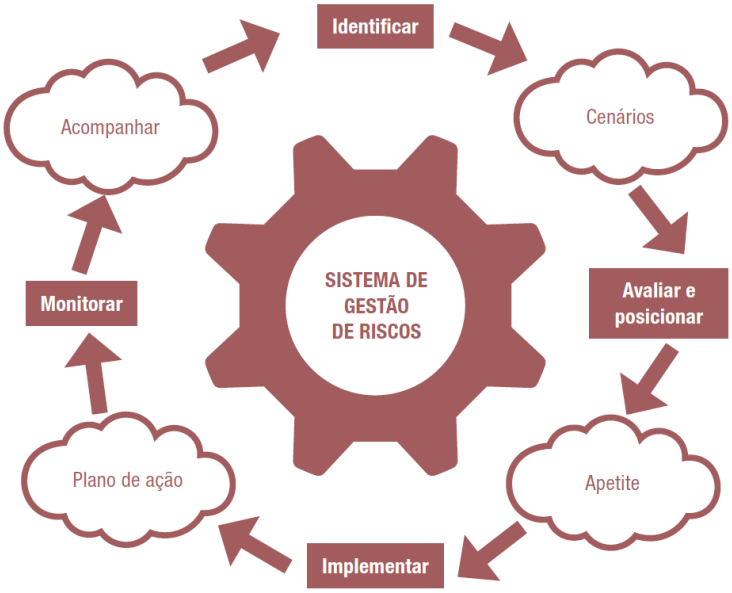
A partir das recomendações não implementadas, são definidos novos prazos para implementação das recomendações, que devem ser devidamente discutidos com os diversos gestores envolvidos nos processos. Adicionalmente, o sucesso da mitigação dos diversos riscos identificados dependerá da designação de recursos (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. 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 uma nova Matriz de Riscos, por meio da qual é possível verificar a evolução dos riscos.

2.8.1 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 ciclo de monitoramento e análise crítica, de forma a mitigar os riscos residuais.

2.8.2 Aprimoramento contínuo

O processo de gestão de riscos e controles internos deve ser continuamente aprimorado e alinhado ao planejamento estratégico e à identidade da organização. Os processos de tomada de decisão, de supervisão, monitoramento e asseguração do funcionamento efetivo da estrutura de gestão de riscos e controle internos, agregados aos conhecimentos dos gestores e diretores sobre o negócio, viabilizam o desenvolvimento de mecanismos de tomada de decisão e de controle da exposição a riscos. Nas empresas inovadoras, a assunção de riscos é incentivada. A criatividade, a flexibilidade e, principalmente, a rapidez de respostas criativas trazem a necessidade de uma cultura de gestão de riscos e controles internos inovadora, e uma governança diferenciada e condizente com os desafios de um ambiente em constante mudança. O esquema abaixo sintetiza o modelo de gestão de riscos e controles internos proposto neste Manual:



Fonte: *Cadernos de Governança Corporativa – Gerenciamento de Riscos Corporativos – IBGC 2017*

2.9 Registro e Relato

Todo o processo de gestão de riscos e seus resultados devem ser documentados e relatados por meio de mecanismos apropriados. O registro e o relato objetivam comunicar as atividades e resultados da gestão de riscos em toda a organização, além de fornecer informações para a tomada de decisão e também proporcionar a melhora contínua da gestão de riscos e controles internos. Além disso, o registro e relato auxilia na interação com as partes interessadas, incluindo aquelas com responsabilidade e com responsabilização por atividades de gestão de riscos.

As decisões relativas à criação, retenção e manuseio de informação documentada levam em consideração, mas não se limitam a, o seu uso, a sensibilidade da informação e os contextos externo e interno. O relato é parte

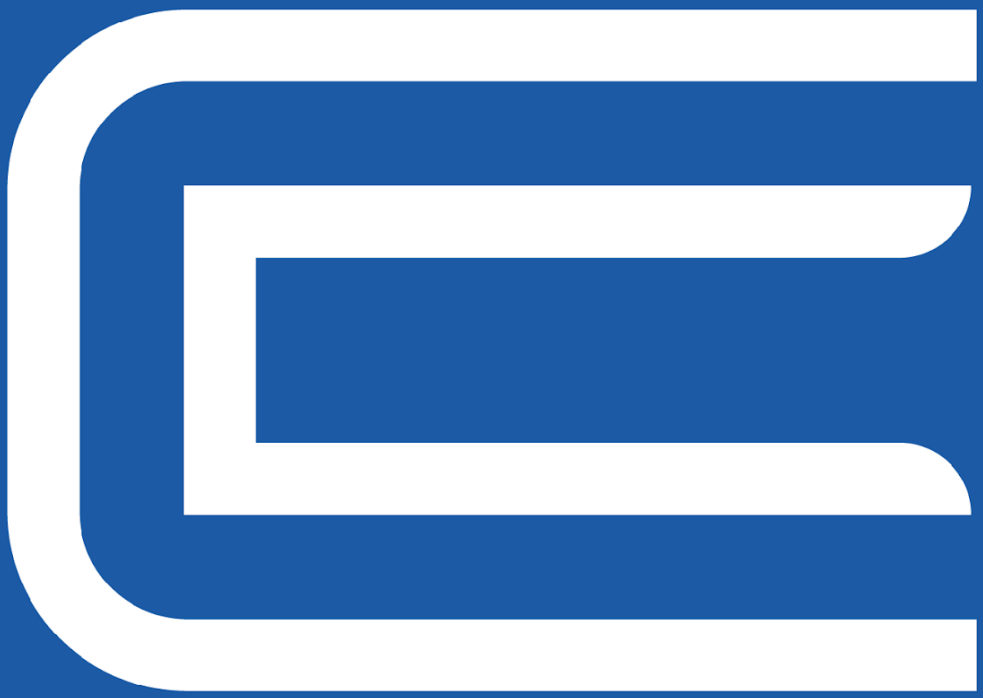
integrante da governança da organização e convém que melhore a qualidade do diálogo com as partes interessadas e apoie a Administração e os órgãos de supervisão a cumprirem suas responsabilidades. Os fatores a considerar para o relato incluem as diferentes partes interessadas e suas necessidades específicas de informação e requisitos; o custo, frequência e pontualidade do relato, o método de relato e a pertinência da informação para os objetivos organizacionais e para a tomada de decisão.

3 DISPOSIÇÕES FINAIS

Este documento deverá ser revisado, no mínimo anualmente, e aprovado pela Diretoria Colegiada e pelo Conselho de Administração.

4 REFERÊNCIAS

- Modelo internacional COSO ERM (*Committee of Sponsoring Organizations of the Treadway Commission* - Enterprise Risk Management) - Framework 2004;
- *The Institute of Internal Auditors – Standards and Guidelines* (O Instituto dos Auditores Internos – Padronização e Orientação) – América do Norte, 2020
- Guia de Boas Práticas da Função Controles Internos – FEBRABAN 2020
- Assi, Marcos. *Gestão de riscos com controles internos: ferramentas, certificações e métodos para garantir a eficiência dos negócios* | São Paulo: Saint Paul Editora, 2013;
- Regulamento do Novo Mercado da B3;
- ABNT NBR ISO 31000:2018;
- ABNT NBR GUIA 73:2009;
- IEC 31010:2019.



corsan

COMPANHIA RIOGRANDENSE DE SANEAMENTO – CORSAN
Rua Caldas Júnior, 120 / 18º andar
CEP 90010-260 – Porto Alegre – RS
www.corsan.com.br