Boas Práticas de Controle Interno, Gestão de Riscos e *Compliance*

1ª Revisão | 2021

Aprovação
Diretoria Colegiada dia 06/07/2021 - ATA 052/2021
Conselho de Administração dia 22/07/2021 - ATA 004/2021

Índice

1 Objetivo

Este manual tem o objetivo de fornecer suporte metodológico para execução das atividades de controle interno, gestão de riscos e *compliance* no âmbito do Centro de Informática e Automação do Estado de Santa Catarina – CIASC de forma a assegurar sua integração aos processos organizacionais, reduzir a exposição a riscos, danos ao patrimônio e à imagem empresarial, além de fortalecer os mecanismos de governança e o alcance dos objetivos estratégicos da empresa.

2 Conceitos básicos

2.1 Controle interno

Segundo COSO (*Committee of Sponsoring Organizations of the Treadway Commission)*, Controle interno é um processo conduzido pela estrutura de governança desenvolvido para proporcionar segurança razoável com respeito à realização dos objetivos relacionados a operações, divulgação e conformidade.

Neste sentido, o controle interno é:

- Conduzido para atingir objetivos em uma ou mais categorias – operacional, divulgação e conformidade.
- Um processo que consiste em tarefas e atividades contínuas – um meio para um fim, não um fim em si mesmo.
- Realizado por pessoas – não se trata simplesmente de um manual de políticas e procedimentos, sistemas e formulários, mas diz respeito a pessoas e às ações que elas tomam em cada nível da empresa para realizar o controle interno.
- Capaz de proporcionar segurança razoável - mas não absoluta, para a estrutura de governança e alta administração de uma empresa.
- Adaptável à estrutura da empresa – flexível na aplicação para toda a empresa ou para uma subsidiária, divisão, unidade operacional ou processo de negócio em particular.

2.2 Gestão de riscos corporativos

Risco é definido, pela *International Organization for Standardization – ISO,* como sendo o efeito da incerteza nos objetivos (ISO 31000).

O Risco também pode ser definido como o evento futuro e incerto que, caso ocorra, pode impactar negativamente o alcance dos objetivos da organização (COSO II - *Enterprise Risk Management*).

> O gerenciamento de riscos corporativos é um processo conduzido em uma organização pelo conselho de administração, diretoria e demais empregados, aplicado no estabelecimento de estratégias, formuladas para identificar em toda a organização eventos em potencial, capazes de afetá-la, e administrar os riscos de modo a mantê-los compatível com o apetite a risco da organização e possibilitar garantia razoável do cumprimento dos seus objetivos. (COSO)

Essas definições refletem certos conceitos fundamentais. O gerenciamento de riscos corporativos é:

- Um processo contínuo e estruturado, que flui através da empresa.
- Conduzido pelos profissionais em todos os níveis da empresa, considerando os fatores humanos e culturais.
- Aplicado à definição das estratégias, sendo base confiável para apoio de tomada de decisões e planejamento.
- Aplicado em toda a empresa, em todos os níveis e unidades, e inclui a formação de uma visão de portfólio de todos os riscos a que ela está exposta, abordando explicitamente as incertezas.
- Formulado para identificar eventos em potencial, cuja ocorrência poderá afetar a empresa, e para administrar os riscos de acordo com seu apetite a risco.
- Capaz de propiciar garantia razoável para o Conselho de Administração e a Diretoria Executiva da empresa.
- Orientado para a realização de objetivos em uma ou mais categorias distintas, mas dependentes, ou seja, o gerenciamento de riscos desdobra da estratégia e dos objetivos empresariais para os processos/atividades a eles vinculados, incorporando demais riscos existentes.

2.3 Compliance

Do verbo anglo-saxão "*to comply*", significa cumprir, executar, satisfazer, realizar o que foi imposto. *Compliance* é estar em conformidade, é o dever de cumprir regulamentações internas e externas impostas às atividades da instituição. "Estar em *compliance*" é estar em conformidade com leis e regulamentações internas e externas. "Ser e estar em *compliance*", é acima de tudo, uma obrigação individual de cada colaborador dentro da empresa.

3 Procedimentos gerais de controle interno

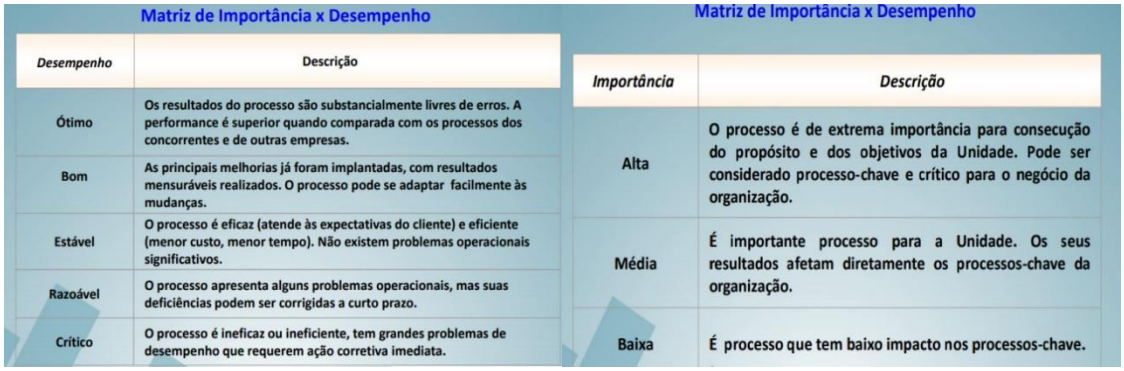
1. Seleção dos processos a serem trabalhados na empresa para documentar e implementar os controles. A empresa deve definir qual será o critério de seleção:
    a) por meio de materialidade das demonstrações contábeis;
    b) por julgamento profissional;
    c) por critérios de criticidade; e
    d) outros.
2. Conhecimento mínimo necessário dos processos selecionados. Esse conhecimento pode se dar por entrevistas, narrativas, fluxogramas. É importante conhecer o processo e identificar o que e em qual etapa algo pode dar errado (riscos do processo).
3. A partir da identificação dos riscos dos processos, deve-se documentar/formalizar os controles existentes e os controles necessários de serem implementados.
4. Um controle interno, necessariamente, precisa atender a 3 (três) quesitos:
    a) deve ser formalizado/documentado;
    b) deve ter evidência de sua execução; e
    c) deve ser mensurável.

5. Para cada controle identificado devem ser efetuados testes de efetividade, conforme amostras. Os testes confirmam se os controles são executados conforme sua descrição e se de fato são efetivos.
6. Os responsáveis pelos processos de negócios são os donos dos riscos e controles, cabendo a estes o papel de conduzir o processo e seus controles com efetividade.
7. O Processo de Controles Internos é um ciclo contínuo. Os processos trabalhados, seus riscos e controles devem ser revisados e atualizados sempre que houver alterações ou sempre que surgir um evento novo.

Figura I: *Ciclo de Gestão de Riscos de Processos e Controle Interno*

8. Na implementação da Gestão de Riscos de Processos a empresa poderá concentrar seus recursos e esforços nos processos considerados críticos e que impactam mais fortemente na eficiência e eficácia organizacional, ou seja, nas estratégias e objetivos empresariais desdobradas até a unidade, podendo se utilizar da Matriz de Importância e Desempenho, demonstrada na **Figura II**.

Figura II: *Matriz de Importância x Desempenho na Gestão de Riscos de Processos*



Matriz de Importância x Desempenho

Desempenho	Descrição
Ótimo	Os resultados do processo são substancialmente livres de erros. A performance é superior quando comparada com os processos dos concorrentes e de outras empresas.
Bom	As principais melhorias já foram implantadas, com resultados mensuráveis realizados. O processo pode se adaptar facilmente às mudanças.
Estável	O processo é eficaz (atende às expectativas do cliente) e eficiente (menor custo, menor tempo). Não existem problemas operacionais significativos.
Razoável	O processo apresenta alguns problemas operacionais, mas suas deficiências podem ser corrigidas a curto prazo.
Crítico	O processo é ineficaz ou ineficiente, tem grandes problemas de desempenho que requerem ação corretiva imediata.

Matriz de Importância x Desempenho

Importância	*Descrição*
Alta	O processo é de extrema importância para consecução do propósito e dos objetivos da Unidade. Pode ser considerado processo-chave e crítico para o negócio da organização.
Média	É importante processo para a Unidade. Os seus resultados afetam diretamente os processos-chave da organização.
Baixa	É processo que tem baixo impacto nos processos-chave.

9. Com base na matriz utiliza-se os seguintes fatores:

    a) Fator Importância:

        i. qual é a importância deste processo para atingirmos nossos objetivos?

        ii. este processo impacta diretamente nos nossos resultados?

        iii. é um processo-chave do nosso negócio?

        iv. é um processo de suporte “crítico” em relação aos processos finalísticos?

    b) Fator Desempenho:

        i. este processo tem atingido os resultados esperados?

        ii. qual o nível de satisfação dos clientes em relação a este processo?

        iii. têm sido registradas reclamações, elogios, sugestões de melhoria?

4 Procedimentos gerais de gestão de riscos corporativos

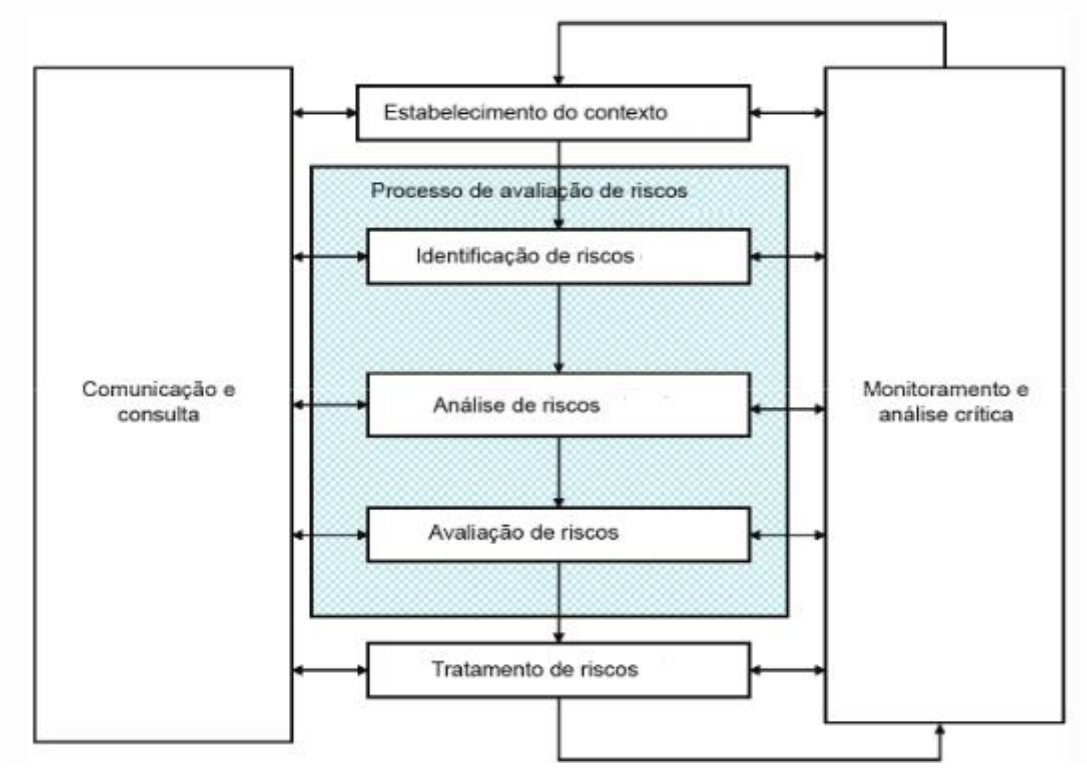
A empresa além da definição da missão e visão, também estabelece objetivos estratégicos, isto é, metas de alto nível que alinham e apoiam as decisões para o cumprimento destes.

O gerenciamento de riscos corporativos é um processo conduzido pelo Conselho de Administração, Diretoria Executiva e empregados, sendo aplicado no estabelecimento de estratégias no âmbito da empresa.

O gerenciamento de riscos corporativos requer que a empresa adote uma visão de portfólio dos riscos, procedimento que poderá exigir a participação de cada um dos gerentes responsáveis por unidades de negócios, funções, processos ou outras atividades que envolvam avaliação de risco, a qual poderá ser quantitativa ou qualitativa. Com uma visão combinada de cada nível da empresa, a alta administração é capaz de avaliar se a carteira de riscos é compatível com o apetite a risco da empresa.

O processo de gestão de riscos corporativos do CIASC é parte integrante da gestão, incorporado na cultura e nas práticas, e adaptado aos processos de negócios da empresa, utilizando o framework: ISO 31000

Figura III: *Framework ISO 31000*



4.1 Estabelecimento do contexto

Definir os objetivos estratégicos da empresa e identificar o contexto externo e interno a ser levado em consideração no gerenciamento dos riscos corporativos. Isto deverá acontecer em uma etapa anterior, durante a execução do planejamento estratégico.

O contexto no Processo de Gestão de Riscos ajuda a delimitar o escopo para a identificação dos riscos que poderão impactar no alcance dos objetivos estratégicos do CIASC.

4.1.1 Contexto externo

O contexto externo é o ambiente externo no qual o CIASC busca atingir seus objetivos.

O contexto externo pode incluir, mas não está limitado a:

- Ambientes cultural, social, político, legal, regulatório, financeiro, tecnológico, econômico e natural, quer seja internacional, nacional, regional ou local;
- Fatores–chave e tendências que tenham impacto sobre os objetivos da empresa; e
- Relações com as partes interessadas externas e suas percepções e valores.

4.1.2 Contexto interno

O contexto interno é o ambiente interno no qual o CIASC busca atingir seus objetivos.

O processo de gestão de riscos deve estar alinhado com a cultura, processos, estrutura e estratégia da empresa. O contexto interno é algo dentro da organização que pode influenciar a maneira pela qual ela gerenciará os riscos.

É necessário compreender o contexto interno. Isto pode incluir, mas não está limitado a:

- Governança, estrutura organizacional, funções e responsabilidades;

- Políticas, objetivos e estratégias implementadas para atingi-los;
- Capacidades, entendidas em termos de recursos e conhecimento (por exemplo, capital, tempo, pessoas, processos, sistemas e tecnologias);
- Sistemas de informação, fluxos de informação e processos de tomada de decisão (formais e informais);
- Relações com as partes interessadas internas, e suas percepções e valores;
- Cultura organizacional;
- Normas, diretrizes e modelos adotados pelo CIASC, e forma e extensão das relações contratuais.

4.1.3 Definição dos objetivos

A identificação dos objetivos não é parte integrante do processo de gestão de riscos, mas eles são parte do processo de planejamento estratégico e são de vital importância para que a atividade de identificação de riscos seja bem-sucedida.

4.2 Identificação de riscos

Riscos são incidentes ou ocorrências originadas a partir de fontes internas ou externas que afetam a implementação da estratégia ou a realização dos objetivos. Os riscos podem provocar impacto positivo, negativo ou ambos.

Durante a identificação dos riscos, existem diversas incertezas, uma vez que é difícil mensurar se um evento ocorrerá, quando poderá ocorrer, nem o impacto que terá caso ocorra. Inicialmente, devemos considerar uma faixa de eventos em potencial, originada de fontes internas e externas, sem levar em conta se o impacto será favorável ou desfavorável. Desse modo, podemos identificar não apenas riscos com potencial impacto negativo, mas também aqueles que representam oportunidades a serem aproveitadas.

Os riscos podem ser insignificantes ou altamente significativos, então é importante garantir que todos os riscos sejam identificados de forma

independente de sua avaliação, uma vez que riscos que pareçam pouco relevantes quanto à sua probabilidade de ocorrência podem resultar em impactos grandes para a organização.

4.2.1 Técnicas para identificação de riscos

- **Inventário de eventos:** trata-se da relação detalhada de eventos em potencial comuns às organizações de um mesmo cenário ou para um determinado tipo de processo, ou atividade, comum entre elas.
- **Análise interna:** Pode ser realizada como parte da rotina do ciclo de planejamento estratégico. A análise interna pode dispor das informações de outras partes interessadas, como clientes, fornecedores e outras unidades de negócios, ou da consulta a um especialista no assunto, e de fora da unidade.
- ***Brainstorming* estruturado:** Essas técnicas identificam eventos com base na experiência e no conhecimento acumulado da administração, do pessoal ou de outras partes interessadas por meio de discussões estruturadas. O facilitador envolvido irá iniciar um debate sobre os eventos que possam afetar os objetivos da empresa, procurando combinar o conhecimento e experiências dos envolvidos para a identificação dos potenciais eventos de risco.
- **Análise de fluxo de processo:** Permite identificar os riscos associados às entradas, saídas, processamentos e responsabilidades do processo.
- **Análise de dados e indicadores:** Analisar os dados e resultados de indicadores para a previsão de possíveis riscos. Por exemplo, a redução no número de multas pode gerar um risco direto ao caixa do CIASC.

4.2.2 Classificação de riscos

Os riscos precisam ser categorizados para facilitar o processo de gerenciamento, principalmente no que tange às possíveis áreas de impacto e tipos de riscos mais representativos para a gestão.

Visto isso, abaixo segue a classificação de riscos a ser adotada:

ORIGEM	
EXTERNA São ocorrências associadas ao ambiente macroeconômico, ambiental, social, tecnológico ou legal em que a organização opera. Em geral, a organização não consegue intervir diretamente, o que não significa que não possam ser gerenciados.	**INTERNA** São eventos originados na própria estrutura da organização, pelos seus processos, seus recursos financeiros, seu quadro de pessoal ou seu ambiente de tecnologia.
TIPO POR ORIGEM	
Macroeconômico Abrange disponibilidade de capital, inadimplência, concorrência, fornecedores, fusões/aquisições, política, etc.	**Financeiro** Associado a disponibilidade por parte da empresa de recursos e bens, acesso ao capital, etc.
Ambiental Relacionado a energia, emissões e dejetos, desenvolvimento sustentável, desastres naturais, etc.	**Ambiental** Abrange o ambiente interno da empresa, infraestrutura, segurança, etc.
Social Associado a características demográficas, comportamento do consumidor, terrorismo, etc.	**Social** Relacionado a capacidade e produtividade organizacional, execução das atividades, cultura e clima organizacional, saúde dos empregados, greves, etc.
Tecnológico Decorrente de interrupções tecnológicas, tecnologias emergentes, etc.	**Tecnológico** Deriva da disponibilidade dos sistemas, da integridade de dados, dos recursos técnicos existentes na empresa, etc.
Legal Deriva de mudanças na legislação, regulamentos ou normas, da possibilidade de aplicação de multas e sanções, de licenças de funcionamento, de Órgãos Normativos e Órgãos de Controle (GGG, SEF, CGE, TCE, PMF, Receita Federal...), etc.	***Compliance*** Decorrente da não aderência à legislação interna, regulamentos ou normas da estrutura, não adequação de processos e atividades, etc.

NATUREZA
ESTRATÉGICA Riscos associados à tomada de decisão da alta administração e que podem gerar perda substancial no valor econômico da organização.
OPERACIONAL Possibilidade de ocorrência de perdas ou redução de produção e ativos; geralmente acarretam redução, degradação ou interrupção, total ou parcial, das atividades, além da geração potencial de passivos contratuais, regulatórios e ambientais.
FINANCEIRA Caso o risco ocorra vai gerar um impacto direto com valor monetário.
INTEGRIDADE O risco está relacionado a vulnerabilidades institucionais que podem favorecer ou facilitar práticas de corrupção, fraudes, subornos, irregularidades e desvios éticos e de conduta.
PRIVACIDADE Riscos que estão associados ao cumprimento e descumprimento da Lei Geral de Proteção de Dados (LGPD).

4.2.3 Registro de riscos

Todo risco identificado deve ser cadastrado no sistema interno da empresa destinado ao registro dos riscos, devendo ser elaborado um Mapa de Riscos contendo as causas e consequências, a classificação de riscos e quais objetivos ele poderá impactar caso ocorra.

4.3 Análise de riscos

Analisar as causas do risco, suas consequências positivas e negativas, a probabilidade de que essas consequências possam ocorrer e o impacto delas caso ocorram.

4.3.1 Critérios para mensuração de riscos

Todos os riscos devem ser mensurados quanto à sua probabilidade de ocorrência, gerando uma escala que facilita a interpretação consistente dos níveis de riscos.

- **Probabilidade:** Representa a possibilidade de um risco acontecer.

Abaixo segue escala para mensuração da probabilidade.

Nível	Probabilidade	Descrição	
5	Muita alta	Quase certo	Evento esperado que ocorra na maioria das circunstâncias
4	Alta	Provável	Evento provavelmente ocorra na maioria das circunstâncias
3	Média	Possível	Evento deve ocorrer em algum momento
2	Baixa	Improvável	Evento pode ocorrer em algum momento
1	Muita baixa	Raro	Evento pode ocorrer apenas em circunstâncias excepcionais

- **Impacto:** Representa a consequência que o risco pode causar na empresa. O critério de avaliação do impacto pode incluir efeitos nos aspectos financeiros, operacionais, regulatórios, de imagem, de saúde, de segurança, ambiental, de recursos humanos, e de clientes.

Abaixo segue escala para mensuração do impacto:

Nível	Impacto	Descrição
5	Muito alto	Catastrófico
4	Alto	Grave
3	Médio	Moderado
2	Baixo	Fraco
1	Muito baixo	Irrelevante

4.3.2 Medida de risco

Uma vez que os riscos estão identificados e documentados com seus respectivos níveis de probabilidade e impacto, deve-se calcular o índice de risco através da equação abaixo.

Índice de Risco = Probabilidade X Impacto

O índice de risco poderá ter duas categorias, inerente ou residual. O índice de risco inerente é aquele calculado quando ainda não há qualquer tipo de controle

para tratamento do risco. Já o índice de risco residual é a medida de risco calculada após a implementação de mecanismos de controle.

Ambas as medidas, inerente e residual, devem ser mantidas documentadas para fins de comparação e análise da efetividade dos mecanismos de tratamento dos riscos corporativos.

4.3.3 Critérios de aceitação de riscos

Tendo todos os riscos com índice de risco calculado, o que poderá variar dentro de uma escala de 1 a 25, cabe à alta administração definir o grau de aceitação ao risco da instituição.

Ficam definidos os seguintes critérios de aceitação de riscos, conforme o índice de risco calculado:

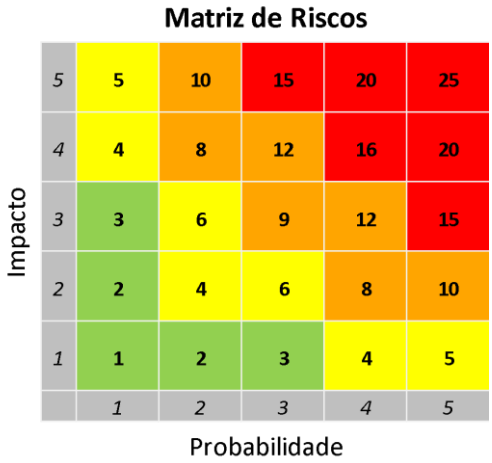
Índice de Risco	**Faixa de Risco**
1 a 3	Pequeno
4 a 6	Moderado
7 a 14	Alto
15 a 25	Crítico

Isto ajudará a definir os tratamentos adequados para cada faixa de risco na instituição.

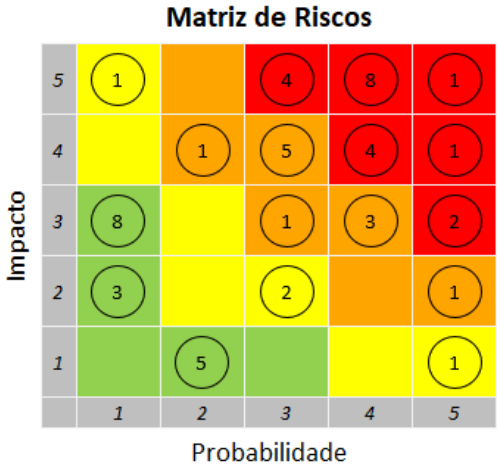
4.4 Avaliação de riscos

Esta etapa consiste em ranquear os índices de riscos calculados anteriormente e avaliar criteriosamente os aspectos de cada risco para a priorização do tratamento. Além disso, esta etapa permite obter uma visão geral quanto à exposição ao risco presente na instituição.

Para isto, poderão ser utilizados 2 modelos de matriz de riscos, uma que apresenta os quadrantes coloridos considerando as faixas de risco mencionadas na seção anterior. No interior dos quadrantes estão os índices de risco, conforme a seguir.



O outro modelo de matriz irá indicar a quantidade de riscos existentes em cada quadrante, conforme exemplo abaixo.



A matriz de riscos poderá ser apresentada considerando o índice de risco inerente ou residual.

Logo, considerando os critérios de aceitação definidos pela alta administração, identificam-se os riscos que serão aceitos e aqueles que deverão ser tratados. Também é importante ressaltar que os responsáveis pela análise dos riscos poderão analisar, de forma isolada, as variáveis que compõem o cálculo do índice de risco, para verificar se existem riscos que, mesmo com índice de risco baixo, devam ser tratados devido ao impacto que poderá gerar para os negócios da empresa.

4.5 Tratamento de riscos

Após identificados, analisados e mensurados, deve-se definir qual tipo de tratamento será dado a cada risco.

A área responsável pela gestão de riscos poderá determinar responsáveis de outras áreas para a elaboração e controle dos planos de ação, de acordo com as especificidades de cada risco.

Os responsáveis por cada risco deverão balancear os custos e esforços envolvidos com o potencial benefício que será alcançado com as soluções de tratamento.

4.5.1 Estratégias de tratamento de riscos

As respostas aos riscos devem ser definidas e planejadas utilizando-se as seguintes estratégias:

- **Evitar** - decidir em não iniciar ou descontinuar uma atividade ou processo que dá origem ao risco. Exemplo: uma organização decide se desfazer de uma unidade de negócios ou produto.
- **Reduzir** - alterar o fator probabilidade com a implementação de controles específicos. Por exemplo, o CIASC identificou e avaliou o risco de seus sistemas permanecerem inoperantes por um período superior a três horas e concluiu que não aceitaria o impacto dessa ocorrência. Sendo assim, investiu no aprimoramento de sistemas de autodetecção de falhas para reduzir a probabilidade de indisponibilidade do sistema.
- **Mitigar** - alterar o fator impacto com a implementação de controles específicos. Por Exemplo: O CIASC pode investir na redundância dos equipamentos que processam os sistemas críticos dos clientes. Havendo uma falha em algum desses equipamentos, a redundância implementada asseguraria a continuidade da operação dos respectivos sistemas, evitando o impacto nos negócios da empresa.
- **Reter** - aceitar manter o risco no nível atual de probabilidade e impacto. Exemplo: O CIASC decide não investir em melhorias de um respectivo sistema interno, assumindo que as perdas e erros atualmente sabidos e

esperados de informações internas deste sistema acarretam consequências toleráveis.

- **Transferir** – 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. Exemplo: o CIASC identificou e avaliou os riscos de falhas e desgaste natural dos veículos que compõem sua frota. Após analisar a melhor estratégia a ser adotada no que tange às despesas possíveis com manutenção, licenciamentos, seguros e eventualmente até a paralisação de algumas atividades em função da indisponibilidade de veículos, a empresa decide terceirizar a frota de forma que toda a manutenção, seguro e garantia de disponibilidade sejam de responsabilidade de um fornecedor externo.

Visando ao controle e acompanhamento das soluções, todas as estratégias de tratamento deverão ser documentadas em ações pelos responsáveis de cada risco.

Cabe à área responsável pela gestão de riscos fazer o acompanhamento do planejamento das estratégias de tratamento e sua devida execução pelos responsáveis.

4.6 Monitoramento e análise crítica

Envolve a checagem ou vigilância regulares. Pode ser periodicamente ou acontecer em resposta a um fato específico. Deve garantir que os riscos estejam sendo gerenciados conforme o planejado, possibilitar a detecção de mudanças no contexto interno e externo e identificar novos riscos.

Neste sentido, cabe aos responsáveis pelos riscos definir a periodicidade necessária para verificação de cada risco, de acordo com importância e tratamento definido para cada um.

É durante o monitoramento que os índices de risco residuais serão calculados e atualizados, identificando se as estratégias de tratamento estão reduzindo a exposição da empresa aos riscos.

4.6.1 Indicadores para gestão de risco

4.6.1.1 Índice de exposição ao risco - IER

- **Medida:** Soma dos índices de risco atualizados de todos os riscos.
- **Responsável:** Área responsável pela gestão de riscos.

4.6.1.2 Índice médio de risco inerente - IMRI

- **Medida:** Soma dos índices de risco inerentes de todos os riscos dividida pela quantidade de riscos.
- **Responsável:** Área responsável pela gestão de riscos.

4.6.1.3 Índice médio de risco residual - IMRR

- **Medida:** Soma dos índices de risco residuais de todos os riscos dividida pela quantidade de riscos.
- **Responsável:** Área responsável pela gestão de riscos.

4.6.2 Registros do processo de gestão de riscos

Todas as atividades de gestão de riscos devem ser registradas de forma a possibilitar a melhoria dos métodos e ferramentas, bem como de todo o processo.

4.7 Comunicação e consulta

Comunicação envolve compartilhar informação com públicos-alvo. A consulta também envolve o fornecimento de retorno pelos participantes, com a expectativa de que isto contribuirá para as decisões e sua formulação ou outras atividades.

Convém que a comunicação e a consulta sejam oportunas e assegurem que a informação pertinente seja coletada, consolidada, sintetizada e compartilhada, como apropriado, e que o retorno seja fornecido e as melhorias sejam implementadas.

5 Práticas gerais de *compliance*

Os procedimentos de *Compliance* têm o objetivo de avaliar a aderência às normas internas e externas e identificar condutas inadequadas. Para isto, a empresa deve:

1. A estrutura de *Compliance* deve interagir com diversas áreas da empresa para execução das suas atividades, principalmente com Jurídico, Gestão de Riscos, Controle Interno e Auditoria Interna.
2. Definir formalmente quais as leis, regulamentações e normas internas farão parte do Programa de *Compliance*, e, portanto, serão o escopo de atuação da área de *Compliance*, de acordo com o tamanho e complexidade do negócio, incluindo o Código de Conduta e Integridade.
3. Verificar, através de um método formal, a aderência em relação a cada uma das normas internas e externas que fizerem parte do escopo do Programa de *Compliance*.
4. Propor formalmente ações juntamente com as áreas envolvidas para atendimento das normas internas e externas.
5. Monitorar o cumprimento do programa e reportar para a administração da empresa sobre o seu desenvolvimento.
6. Revisar periodicamente o escopo do Programa de *Compliance*, observando novas leis, regulamentações e normas internas.
7. Zelar pelo cumprimento de leis, regulamentações e normas internas e por padrões éticos.
8. Analisar políticas e normas internas com objetivo de evitar conflitos com outras já existentes e com a legislação.
9. Os responsáveis pelos processos de negócios são os donos dos riscos de *compliance*, cabendo a estes o papel de estar em conformidade nos processos sob sua responsabilidade.

6 Disposições finais

1 As atividades de Controle Interno, Gestão de Riscos e *Compliance* serão vinculadas diretamente ao Presidente e conduzidas por ele, ou delegado por ele a outro Vice-presidente, devendo fazer parte dos processos da empresa, sendo formalizados em estrutura organizacional própria ou atribuída a uma determinada área que tenha outras competências, para que sejam dinâmicos, interativos e capazes de reagir a mudanças.

2 É responsabilidade do Conselho de Administração, aprovar a política de gerenciamento de riscos conforme a orientação estratégica da empresa, após aprovação pela Diretoria Colegiada. A definição de atribuições das atividades e responsabilidades nos processos de Controle Interno, Gestão de Riscos e *Compliance* deverão estar formalizadas em documento próprio.

3 Os treinamentos referentes à gestão de riscos, controles internos e *compliance* devem ser previstos para que todos na empresa participem, e sejam capazes de reagir a mudanças.

Histórico de versões

Aprovação	Versão gerada
Diretoria Colegiada dia 21/06/2018 - ATA 023/2018 e Conselho de Administração dia 28/06/2018 - ATA 005/2018	1