POLÍTICA DE GESTÃO DE RISCOS

Fevereiro/2025

HISTÓRICO DE VERSÕES

Data	Versão	Descrição	Autor	Aprovação
06/11/2024	V1.0	Primeira versão da Política de Gestão de Riscos.	Equipe Lara Martins Advogados	Anna Bastos
21/02/2025	V1.1	Primeira versão da Política de Gestão de Riscos.	Equipe Técnica de Elaboração	Deborah Montenegro e Alexandre de Abreu e Silva

SUMÁRIO

POLÍTICA DE GESTÃO DE RISCOS

1. APRESENTAÇÃO

A Política de Gestão de Riscos do Sesc Goiás tem como objetivo estabelecer diretrizes e critérios para um gerenciamento eficaz dos riscos de *compliance*, promovendo uma cultura organizacional baseada na integridade, transparência e conformidade.

Os riscos de *compliance* podem surgir a partir de diversas fontes, como operações cotidianas, falhas humanas, mudanças no ambiente regulatório, deficiências de infraestrutura e desafios na adaptação às legislações e normativas aplicáveis.

Em conformidade com a ABNT NBR ISO 37301:2021, a identificação das obrigações e riscos de *compliance* é um componente essencial do Sistema de Gestão de *Compliance* (SGC). Esse processo segue o ciclo PDCA (Planejar, Executar, Verificar e Agir), garantindo a melhoria contínua e a eficácia das medidas adotadas.

Para que a gestão de riscos seja efetiva, é imprescindível que os responsáveis compreendam o contexto estratégico e operacional da instituição, estabeleçam critérios objetivos para avaliação e categorização dos riscos e implementem ações preventivas e corretivas de maneira estruturada.

Dessa forma, esta política se compromete a fortalecer a governança, aprimorar os controles internos e contribuir para um ambiente organizacional resiliente, permitindo que o Sesc Goiás alcance seus objetivos estratégicos com segurança, ética e responsabilidade.

2. DOCUMENTOS DE REFERÊNCIA

Para a elaboração desta política foram utilizados os seguintes modelos de gestão de riscos:

- Norma ABNT ISO/IEC 31000:2018 – Sistema de gestão de riscos.
- Norma ABNT ISO/IEC 37001:2017 – Sistema de gestão antissuborno – Requisitos com orientações para uso.
- Norma ABNT ISO/IEC 37301:2021 - Sistema de Gestão de *Compliance*.
- Metodologia de Gestão de Riscos da Controladoria-Geral da União (CGU).
- Declaração de Posicionamento do IIA – Gerenciamento de Risco Eficaz.
- Documento Referencial de Gerenciamento de Riscos do Sesc – Departamento Nacional.

3. ABRANGÊNCIA

Esta Política é aplicável à Diretoria Jurídica e de *Compliance*, responsável pelo gerenciamento de riscos ligados à *compliance*, bem como às demais diretorias executivas, gerências e funcionários que, no exercício de suas funções, realizem a gestão de riscos relacionados à conformidade em suas respectivas áreas de atuação.

Além disso, esta política estende-se aos membros da Comissão de Ética e *Compliance*, encarregada da governança e supervisão do Programa de *Compliance*, assegurando sua efetividade e alinhamento com as diretrizes institucionais.

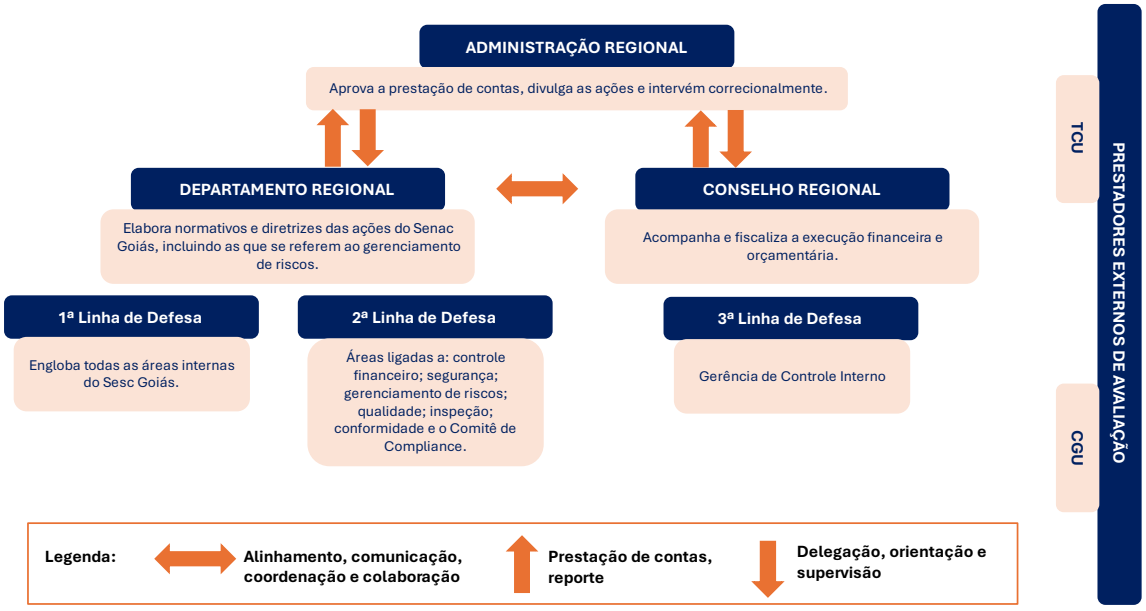
O desconhecimento desta política não exime ninguém de suas responsabilidades e poderá resultar na aplicação de medidas disciplinares e sancionatórias, conforme previsto neste documento.

4. ESTRUTURA DA GESTÃO DE RISCOS NO SESC GOIÁS

O Sesc Goiás adota em seu gerenciamento de riscos e controles internos, o modelo das três linhas de defesa do The IIA (*The Institute of Internal Auditors*), com o objetivo de aprimorar a comunicação e a eficácia no gerenciamento de riscos e controles internos.

Esse modelo estabelece a segregação de responsabilidades entre as diferentes áreas da instituição, garantindo uma abordagem estruturada e colaborativa para a identificação, mitigação e monitoramento dos riscos. Além disso, reforça a interação entre os atores internos e os órgãos fiscalizadores externos, que atuam como supervisores desse processo.

A estrutura é definida conforme descrito abaixo:



1

i. Primeira linha de defesa: Esta linha inclui as áreas de negócios e operações da instituição, onde os riscos são identificados e gerenciados diariamente. São as equipes operacionais, diretores, gerentes e funcionários que têm responsabilidade direta pela execução das atividades e processos finalísticos da instituição. Essas pessoas deverão implementar e monitorar os controles internos em suas áreas de responsabilidade. Eles são os principais responsáveis por:

- Identificar e avaliar os riscos dentro de suas áreas de atuação.
- Implementar medidas de mitigação de riscos, a depender do caso.
- Monitorar a efetividade dos controles internos.
- Monitorar as operações do processo de gestão de riscos realizadas na área.
- Sugerir os processos ou objetivos prioritários para gerenciamento dos riscos.
- Validar e contribuir na tomada de decisões dos planos de ação definidos na gestão dos riscos de sua área.
- Monitorar, propor e incentivar práticas referentes ao processo de gestão de riscos, tais como identificação, análise, avaliação e tratamento dos riscos na área sob sua responsabilidade.
- Relatar à segunda linha de defesa sobre os riscos e controles encontrados.

[1] Referências: Modelo das Três Linhas do The Institute of Internal Auditors e Documento Referencial de Gerenciamento de Riscos do Sesc – Departamento Nacional.

- Manter um diálogo contínuo com a diretoria e reportar resultados planejados, reais e esperados, vinculados aos objetivos da organização e riscos
- Garantir a conformidade com as expectativas legais, regulatórias e éticas.

ii. Segunda linha de defesa: Esta linha é composta pelas funções de apoio, conformidade e supervisão do gerenciamento de riscos. Essas funções fornecem orientação e supervisão sobre a forma como os riscos são gerenciados pela primeira linha de defesa. Isso inclui áreas envolvidas com: *compliance*, gestão de riscos, controle interno, jurídico dentre outros. Eles ajudam a:

- Supervisionar o Programa de *Compliance* do Sesc Goiás.
- Acompanhar o mapeamento de riscos realizado, por meio do monitoramento contínuo.
- Definir, gerenciar, comunicar e assessorar a Administração Regional quanto à implementação da gestão de riscos e à avaliação de controles internos, propondo ajustes e medidas preventivas e proativas.
- Convocar reuniões da Comissão de Ética e *Compliance*.
- Desenvolver políticas, procedimentos e controles para mitigar riscos.
- Garantir conformidade com leis, regulamentos e políticas internas.
- Dirimir dúvidas quanto à identificação de determinados riscos no âmbito interno com os gestores das áreas.
- Fornecer análises e reportar sobre a adequação e eficácia do gerenciamento de riscos.

iii. Terceira linha de defesa: Esta linha é composta pela área responsável pelo controle interno, que fornece uma avaliação independente e objetiva dos controles internos, processos de gerenciamento de riscos e governança da instituição. Eles avaliam a eficácia das atividades de gerenciamento de riscos e controles internos nas outras duas linhas de defesa e fornecem recomendações para melhorias, se necessário.

Posto isso, o modelo das três linhas de defesa facilita uma abordagem estruturada e colaborativa para o gerenciamento de riscos e controles internos dentro da instituição, ajudando a garantir que os riscos sejam identificados, avaliados e gerenciados de forma eficaz.

5. DIRETRIZES PARA GESTÃO DE RISCOS NO SESC GOIÁS

A Gestão de Riscos no Sesc Goiás é composta por uma estrutura integrada, fundamentada em princípios, objetivos, competências e processos que possibilitam o gerenciamento eficaz dos riscos organizacionais. Esse sistema institucional, de caráter permanente, é estruturado e monitorado principalmente pela alta administração e pela Diretoria Jurídica e de *Compliance*.

Seu foco está na identificação, análise e avaliação de riscos, bem como na definição de estratégias de resposta e na implementação de ações voltadas ao tratamento desses riscos. Além disso, contempla o monitoramento contínuo e a comunicação clara sobre o processo de gerenciamento de riscos, com o objetivo de subsidiar a tomada de decisões em todos os níveis hierárquicos.

Devido à natureza multidisciplinar da gestão de riscos, é importante que o processo seja conduzido de forma colaborativa, por meio de oficinas de trabalho, envolvendo pessoas que possuam conhecimento específico sobre o processo, projeto ou atividade em questão.

Essa abordagem visa assegurar o alcance efetivo dos objetivos estratégicos da instituição, fortalecendo a governança, a transparência e a sustentabilidade das ações realizadas pelo Sesc Goiás.

5.1. Entendendo a instituição e suas obrigações

Para o desenvolvimento de um sistema de gestão de *compliance* eficaz, é essencial que a instituição compreenda tanto questões internas quanto externas que possam afetar suas obrigações de *compliance*. O primeiro passo para identificar essas obrigações é dialogar com as áreas que lidam com matérias regulatórias da instituição e com o gestor responsável.

As obrigações de *compliance* podem ser mandatórias ou voluntárias. Os requisitos mandatórios são aqueles que a instituição deve cumprir para estar em conformidade com as leis, regulamentos e normas aplicáveis ao seu setor, sob o risco de sanções legais, multas e danos reputacionais. Estes incluem, entre outros:

- Leis e regulamentos;
- Permissões, licenças ou outras autorizações;
- Ordens ou diretrizes emitidas por agências reguladoras;
- Decisões de cortes de justiça ou tribunais administrativos;
- Tratados, convenções e protocolos.

Por outro lado, os requisitos voluntários são adotados por iniciativa da própria instituição, com o objetivo de promover uma cultura de ética, integridade e responsabilidade social, além de aprimorar sua reputação e atender às expectativas dos *stakeholders*. Esses requisitos podem incluir:

- Políticas e procedimentos internos;
- Princípios voluntários ou códigos de conduta e ética;
- Rótulos voluntários ou compromissos ambientais;
- Obrigações contratuais assumidas pela instituição;
- Normas setoriais e organizacionais.

A consideração dessas obrigações, mandatórias e voluntárias, forma a base para o estabelecimento, desenvolvimento, implementação, avaliação, manutenção e melhoria do sistema de gestão de *compliance*, ajudando a instituição a identificar os riscos aos quais está exposta, avaliá-los e tratá-los.

5.1.1. Identificação e análise de riscos

O propósito da identificação de riscos é encontrar, reconhecer e descrever riscos que possam evitar, atrasar, prejudicar ou impedir que o Sesc Goiás alcance seus objetivos, ou ainda, trazer consequências severas para a instituição.

O processo de identificação deve incluir riscos cujas fontes estejam ou não sob o controle da instituição. Consiste em identificar riscos potenciais associados a uma determinada atividade, operação ou processo, levando em consideração todos os fatores relevantes, tais como meio ambiente, tecnologia, recursos humanos, entre outros

É importante que o processo de identificação de riscos seja conduzido de forma sistemática, interativa e colaborativa, com base no conhecimento e nos pontos de vista de todos os envolvidos. Para tanto, é necessário:

i. Analisar o fluxo dos processos da instituição;
ii. Inserir os gestores das áreas envolvidas na etapa de identificação;
iii. Levantar as obrigações de *compliance* mandatórias e voluntárias;
iv. Analisar os riscos identificados.

Cada área deverá ter seu próprio mapa de risco para registro dos riscos identificados, bem como as seguintes informações:

i. Natureza do risco e suas características;
ii. Causas e eventos;

iii. A probabilidade de eventos e consequências;

iv. A natureza e magnitude das consequências;

v. Complexidade e conectividade;

vi. Fatores temporais e volatilidade;

vii. Controles existentes.

5.1.2. Classificação de riscos

Os riscos identificados e analisados serão classificados em conformidade com as seguintes categorias:

i. **Riscos Legais e Regulatórios (Riscos Jurídicos)**: Inclui os riscos jurídicos decorrentes da não conformidade com leis, regulamentos, contratos e outras normas, que podem resultar em sanções ou penalidades.

ii. **Riscos de Imagem e Reputação**: Envolve riscos relacionados à percepção da instituição por terceiros, afetando sua credibilidade, ética, transparência e confiança em seus compromissos.

iii. **Riscos Operacionais**: Abrange riscos de falhas em processos internos, gestão de recursos, infraestrutura e sistemas de informação, impactando a eficiência operacional.

iv. **Riscos Financeiros**: Riscos que podem afetar o setor financeiro da instituição, tais como:

- ***Riscos de Crédito***: Perda resultante da incerteza quanto ao recebimento, ou não, de valores contratados junto a terceiros.
- ***Riscos de Liquidez****:* Incapacidade da instituição em honrar com seus compromissos nos prazos pactuados, em razão do descasamento entre ativos e passivos.
- ***Riscos de Mercado***: Perdas financeiras resultantes de mudanças no comportamento do mercado financeiro, como, variação cambial e taxa de juros, dentre outros.

v. **Riscos Estratégicos**: Ligados a mudanças externas (legais, sociais, políticas, econômicas) que podem impactar as estratégias e objetivos da instituição.

vi. **Riscos Socioambientais**: Referem-se aos impactos adversos sobre o meio ambiente, comunidades e pessoas, comprometendo a sustentabilidade da instituição.

vii. **Conformidade Interna e Externa:** Esta categoria inclui:

- ***Conformidade Interna***: Relacionada ao cumprimento de políticas, procedimentos e padrões internos.
- ***Conformidade de Terceiros***: Riscos associados às práticas de fornecedores, parceiros e contratados que possam comprometer a conformidade da instituição.

viii. **Riscos de integridade e conduta ética**: Esta categoria inclui:

- ***Corrupção e Suborno***: Riscos associados às práticas antiéticas de suborno, corrupção e lavagem de dinheiro que podem ocorrer dentro da instituição ou envolvendo terceiros.
- ***Conflito de Interesses***: Riscos que abrangem situações em que interesses pessoais ou financeiros de funcionários, diretores ou partes relacionadas entram em conflito com os interesses da instituição.
- ***Fraude***: Riscos que englobam atividades fraudulentas que podem ocorrer em várias áreas da instituição.

ix. **Privacidade de Dados Pessoais e Segurança da Informação:** Engloba riscos relacionados a violações de dados, acesso não autorizado, falhas de segurança cibernética e proteção de dados pessoais.

5.1.3. Identificação dos controles

É importante destacar que o nível de risco é inicialmente determinado para os riscos inerentes[2]. Após entender as causas e consequências dos riscos, é fundamental mapear quais são os controles mitigatórios já existentes.

Uma vez identificados os controles, analisa-se sua eficácia e suficiência, para então analisar se os riscos residuais[3] estão alinhados com o apetite ao risco da instituição e definir a resposta adequada. Essas estratégias de mitigação formam a base do plano de ação, que deverá ser acompanhado por novos controles a serem implementados, podendo estes ser do tipo:

- **Preventivos**: Têm por objetivo reduzir a probabilidade de ocorrência de um evento. Os controles preventivos são executados antes de possíveis eventos e abordam suas causas. Ex.: Alçada de níveis de aprovação.
- **Detectivos**: Estes ocorrem durante ou logo após um evento e, graças à detecção precoce, podem reduzir o seu impacto. Ex.: Canal de Denúncias.
- **Corretivos**: Estes ocorrem após o incidente, para mitigar os impactos que já ocorreram. Ex. Tratamento de reclamação dos clientes.

[2] Risco inerente é o que se apresenta a uma organização na ausência de qualquer medida gerencial que possa alterar a probabilidade ou o impacto de um risco.
[3] Risco residual é aquele que ainda permanece após a definição de resposta da administração.

- **Diretivos**: Estes cobrem todas as ações e regras necessárias para executar um processo, ou seja, políticas e procedimentos, formação e orientação, estrutura de governança, papéis e responsabilidades.

Essas análises permitem ao Sesc Goiás aprimorar continuamente seus mecanismos de controle, promovendo eficiência, eficácia e alinhamento com os objetivos estratégicos da instituição. O resultado dessa etapa será utilizado na construção do Plano de Tratamento de Riscos, contribuindo para um processo de gestão de riscos mais robusto e integrado.

5.1.4. Avaliação de riscos

A avaliação de risco consiste no cálculo dos níveis de risco a partir de critérios de probabilidade e impacto de cada evento. A probabilidade refere-se à chance de o evento ocorrer e o risco se materializar, enquanto o impacto diz respeito às consequências da materialização do risco, sendo preferencialmente mensurado por critérios quantitativos.

Essa avaliação orienta não apenas a resposta aos riscos, mas também pode influenciar atividades de controle e revisar as necessidades de informação, comunicação e monitoramento da instituição.

Vejamos o quadro de definições da Probabilidade x Impacto, responsável por estimar a incerteza de eventos em potencial:

ESCALA DE PROBABILIDADE		
PROBABILIDADE	**DESCRIÇÃO DA PROBABILIDADE**	**PESO**
Muito baixa	**Improvável:** Em situações excepcionais, o evento poderá até ocorrer, mas nada nas circunstâncias indica essa possibilidade.	**1**
Baixa	**Rara:** De forma inesperada ou casual, o evento poderá ocorrer, pois as circunstâncias pouco indicam essa possibilidade.	**2**
Média	**Possível:** De alguma forma, o evento poderá ocorrer, pois as circunstâncias indicam moderadamente essa possibilidade.	**3**
Alta	**Provável:** De forma até esperada, o evento poderá ocorrer, pois as circunstâncias indicam fortemente essa possibilidade.	**4**
Muito alta	**Praticamente certa:** De forma inequívoca, o evento ocorrerá, as circunstâncias indicam claramente essa possibilidade.	**5**

Fonte: Metodologia de Gestão de Riscos CGU versão 2.0

ESCALA DE IMPACTO		
Impacto	**Descrição do impacto nos objetivos, caso o evento ocorra**	**Peso**
Muito baixo	**Mínimo** impacto nos objetivos do processo.	**1**
Baixo	**Pequeno** impacto nos objetivos do processo. forma inesperada ou casual, o evento poderá ocorrer, pois as circunstâncias pouco indicam essa possibilidade.	**2**
Médio	**Moderado** impacto nos objetivos do processo, porém recuperável.	**3**
Alto	**Significativo** impacto nos objetivos do processo, de difícil reversão.	**4**
Muito alto	**Catastrófico** impacto nos objetivos do processo, de forma irreversível.	**5**

Fonte: Metodologia de Gestão de Riscos CGU versão 2.0

O nível de risco (NR) será o resultado da equação probabilidade(P) x impacto(I), ou seja, NR = P x I. A partir do resultado do cálculo, o risco poderá ser classificado dentro das seguintes faixas e é representado visualmente pela Matriz de Riscos, abaixo evidenciada, a qual deverá ser utilizada na gestão dos riscos, guiando a instituição sobre quais riscos merecem maior atenção:

MATRIZ DE RISCOS						
IMPACTO	**Muito Alto 5**	5 RM	10 RM	15 RA	20 RE	25 RE
	Alto 4	4 RB	8 RM	12 RA	16 RA	20 RE
	Médio 3	3 RB	6 RM	9 RM	12 RA	15 RA
	Baixo 2	2 RB	4 RB	6 RM	8 RM	10 RM
	Muito Baixo 1	1 RB	2 RB	3 RB	4 RB	5 RM
		Muito Baixa 1	**Baixa 2**	**Média 3**	**Alta 4**	**Muito Alta 5**
		PROBABILIDADE				

Fonte: Metodologia de Gestão de Riscos CGU versão 2.0

CLASSIFICAÇÃO DO RISCO	
Classificação	**Faixa**
Risco baixo - RB	0 – 4,99
Risco médio - RM	5 – 11,99
Risco alto - RA	12 – 19,99
Risco extremo - RE	20 – 25

Fonte: Metodologia de Gestão de Riscos CGU versão 2.0

Assim, feita a avaliação de probabilidade e impacto, em conformidade com os critérios da Matriz de Riscos, os seguintes riscos serão identificados como:

i. **Riscos extremos**: são riscos de impacto crítico e probabilidade muito alta. Devem ser considerados inaceitáveis pelo Sesc Goiás e tratados imediatamente, pois podem afetar drasticamente o alcance das metas determinadas pela instituição. Esse nível de risco costuma ficar muito além do apetite de risco da instituição;

ii. **Riscos altos**: são riscos de impacto alto e probabilidade alta. Ou seja, tratam de eventos prováveis ou muito prováveis de acontecer. Normalmente são riscos derivados de perdas frequentes e que usualmente acabam sendo incorporados ao custo da operação da instituição. Esse nível de risco costuma ficar além do apetite ao risco da instituição;

iii. **Riscos médios**: são riscos de impacto mediano e probabilidade de ocorrência possível ou provável. Geralmente nenhuma medida especial é necessária, porém requer atividades de monitoramento para manter o risco nesse nível, ou reduzi-lo sem custos adicionais. Esse nível de risco fica dentro do apetite ao risco;

iv. **Riscos baixos:** são riscos de baixo impacto e probabilidade remota ou possível. Trata-se de riscos aceitáveis onde as perdas são baixas. Esse nível de risco fica dentro do apetite ao risco da instituição.

É fundamental que as decisões sejam tomadas com base nesses critérios, pois a partir deles será possível a indicação da medida de segurança e o direcionamento adequado para cada ação frente aos riscos identificados.

Convém que os riscos de *compliance* sejam reavaliados periodicamente e quando houver:

- Atividades, produtos ou serviços novos ou alterados;
- Mudanças na estrutura ou estratégia da instituição;
- Mudanças externas significativas, como circunstâncias econômicas e financeiras, condições de marketing, responsabilidades e relacionamento com clientes;

- Mudanças nas obrigações de *compliance*;
- Fusões e aquisições;
- Não *compliance*(s) (mesmo um simples incidente de não *compliance* pode constituir uma mudança material nas circunstâncias) e quase falhas.

Por fim, após avaliação dos riscos, faz-se necessário:

- Reuniões periódicas com equipe diretamente ligada à alta direção da instituição ou funcionários indicados por ela para identificação de novos riscos;
- Reuniões periódicas com funcionários responsáveis por áreas com riscos já identificados e funcionários relacionados às respectivas áreas;
- Reuniões periódicas com a Comissão de Ética e *Compliance*;
- Reuniões periódicas com a área de controles internos.

5.1.5. Plano de ação e tratamento de riscos

Uma vez avaliados os riscos inerentes e residuais, um plano de ação deve ser desenvolvido para mitigar os riscos identificados, levando em consideração a criticidade de cada um e o apetite ao risco da instituição. Esse plano de ação deve detalhar as medidas necessárias para tratar os riscos, priorizando as ações de acordo com a sua relevância, e com os recursos disponíveis.

Além da avaliação inicial dos riscos, o Sesc Goiás deverá analisar as alternativas de mitigação, ponderando o custo-benefício de cada uma, para selecionar a opção de tratamento mais eficaz e sustentável. A seguir, são apresentadas as principais estratégias de tratamento de risco, que podem ser aplicadas isoladamente ou em combinação, conforme for adequado:

- **Evitar**: Esta estratégia é aplicada a atividades com alto potencial de risco, para as quais nenhuma alternativa é viável para reduzir, de forma aceitável, o impacto ou a probabilidade do risco. Nesses casos, a atividade deverá ser interrompida ou descontinuada para eliminar totalmente o risco.
- **Compartilhar**: Neste caso, o risco é transferido ou compartilhado com terceiros, o que pode ocorrer por meio de contratação de seguros, parcerias, terceirização de atividades ou de transações de hedge, entre outras medidas. Essa abordagem reduz a exposição da instituição ao risco, distribuindo os possíveis impactos.
- **Mitigar/Reduzir**: Para riscos nos quais é possível adotar medidas que diminuam a probabilidade de ocorrência ou minimizem seus impactos, podem ser implementadas ações como aprimoramento de

processos, uso de sistemas de controle, treinamentos de funcionários, desenvolvimento de políticas, normas e procedimentos, além da criação de controles internos eficazes.

- **Aceitar**: Em casos em que os riscos são considerados toleráveis e não justificam ações de mitigação adicionais, a instituição pode optar pela aceitação do risco. É importante ressaltar que aceitar um risco não significa negligenciá-lo; o risco deve ser monitorado e reavaliado periodicamente para garantir que sua criticidade permaneça dentro dos níveis aceitáveis. Quando a aceitação do risco for escolhida, a decisão deve ser formalizada e aprovada conforme as alçadas definidas pela alta direção.

5.2. Comunicação

A comunicação busca promover a conscientização e o entendimento do risco. O objetivo da comunicação dos riscos é alcançar um consenso sobre como os riscos devem ser gerenciados, compartilhando essas informações com tomadores de decisão e demais partes interessadas.

A comunicação dos riscos deve ser feita tanto para as operações rotineiras quanto para as emergenciais. Trata-se de uma atividade realizada continuamente.

Ademais, a comunicação dos riscos é realizada a fim de:

i. Compartilhar resultados e apresentar o plano de tratamento;
ii. Permitir que todos compreendam o contexto das situações, as decisões tomadas, e ações necessárias a serem realizadas;
iii. Dar suporte ao processo decisório;
iv. Dar a todos um senso de responsabilidade sobre os riscos;
v. Facilitar a obtenção de informações relevantes para a gestão dos riscos;
vi. Auxiliar na promoção da cultura de gestão de riscos.

Assim, as informações compartilhadas devem ser claras e objetivas, de modo que permitam a todos a compreensão e o contexto das situações. Recomenda-se os seguintes questionamentos previamente à publicação ou divulgação de informações:

- O conteúdo é apropriado – está no nível de detalhe adequado?
- As informações são oportunas – estarão disponíveis quando necessário?
- As informações são atuais – são as mais recentes?
- As informações são exatas – os dados estão corretos?
- As informações são de fácil acesso – são de fácil obtenção por quem delas necessita?

A comunicação eficaz deve ocorrer em todos os níveis da instituição. É fundamental que uma mensagem seja transmitida a todos os funcionários, em nome da alta administração, destacando as responsabilidades individuais em relação aos processos de gerenciamento de riscos corporativos.

Além disso, a instituição deve disseminar comunicações específicas, com delegação clara de autoridade e definição precisa da abordagem adotada para o gerenciamento de riscos corporativos.

5.3. Monitoramento e análise crítica

Após a definição do plano de ação e das medidas de mitigação, os riscos devem ser monitorados continuamente e de forma periódica, visando avaliar a eficácia dos controles internos implementados. Esse monitoramento contínuo tem como objetivo assegurar que a gestão de riscos do Sesc Goiás esteja operando conforme planejado, além de identificar oportunidades de aprimoramento, alinhadas a possíveis mudanças nas condições internas e externas, que possam alterar o nível de exposição ao risco.

O monitoramento deve ocorrer com uma periodicidade de 06 (seis) meses a 01 (um) ano. Todos os relatórios e atas resultantes dos mapeamentos de riscos devem ser submetidos à apreciação do Presidente e Diretor Regional e, posteriormente, arquivados como informação documentada, garantindo o registro histórico e a transparência do processo de gestão de riscos.

5.3.1. Monitoramento pela primeira linha de defesa

Os gerentes de operação, com base nas informações recebidas, devem assumir a responsabilidade pelo monitoramento contínuo dos riscos ligados à sua área, podendo contar com o apoio de outras pessoas. Os responsáveis pelo monitoramento deverão focar em relacionamentos, inconsistências ou outras questões relevantes, avaliando se há necessidade de ações corretivas ou outras medidas.

Cumpre destacar que o monitoramento contínuo difere das atividades voltadas ao cumprimento de políticas nos processos de negócio. Por exemplo, ações como aprovações de transações, conciliações de saldos de contas e verificações da precisão de alterações em bancos de dados, realizadas como etapas essenciais em sistemas de informação ou processos contábeis, são atividades de controle que visam garantir o cumprimento de obrigações de *compliance*.

6. PAPÉIS E RESPONSABILIDADES

6.1. Alta Direção

i. Coordenar e definir os padrões referentes aos processos de gestão de riscos, com a finalidade de implantar uma Política de Gestão de Riscos eficaz no Sesc Goiás;

ii. Designar os papéis e responsabilidades de todas as pessoas responsáveis pela gestão de áreas sensíveis da instituição. Cada tipo de risco será designado a uma área adequada;

iii. Avaliar e aprovar a Matriz de Riscos e o Plano de Ação elaborados;

iv. Estabelecer o apetite de risco, bem como os limites aceitáveis para suportar e gerenciar riscos;

v. Apoiar e garantir a identificação e monitoramento dos riscos e seus respectivos planos de ação;

vi. Realizar a consolidação dos riscos e controles internos;

vii. Monitorar os riscos altos e críticos, junto à Comissão de Ética e *Compliance*;

viii. Avaliar a adequação dos recursos destinados à implementação e estruturação da gestão de riscos;

ix. Disseminar a cultura de gerenciamento de riscos e controles internos na instituição.

6.2. Sessão de Conformidade

i. Realizar a operação do sistema de gestão de *compliance*;

ii. Facilitar a identificação das obrigações de *compliance*;

iii. Assegurar que as responsabilidades, para alcançar as obrigações de *compliance* identificadas, estejam adequadamente alocadas ao longo de toda a instituição;

iv. Documentar a avaliação dos riscos de *compliance*;

v. Propor um plano anual de controle, com o escopo de verificar a eficácia, eficiência e efetividade da gestão de riscos do Sesc Goiás;

vi. Analisar e avaliar o desempenho do sistema de gestão de *compliance,* para identificar quais são as necessidades de ação corretiva;

vii. Identificar e apontar melhorias nos processos de controle interno e de gestão de riscos;

viii. Garantir que os indicadores de desempenho do *compliance* estejam estabelecidos.

ix. Avaliar as estratégias e informações relacionadas aos indicadores chaves de riscos (KRI's), que serão desenvolvidos e monitorados pelos departamentos;

x. Estabelecer um sistema de documentação e reporte de *compliance*;

xi. Assegurar que o sistema de gestão de *compliance* seja analisado criticamente, a intervalos planejados;

xii. Estabelecer um sistema para levantamento de preocupações, assegurando que as questões sejam endereçadas.

xiii. Comunicar à Alta Direção os resultados das avaliações, que deverão ser independentes e imparciais.

6.3. Comissão de Ética e *Compliance*

i. Propor à Alta Direção as definições e estratégias para a gestão de riscos;

ii. Acompanhar, supervisionar e gerenciar o processo de gestão de riscos do Sesc Goiás;

iii. Avaliar, monitorar e comunicar periodicamente a Alta Direção sobre os riscos altos e críticos, assim como os planos de tratamento e monitoramento;

iv. Promover a cultura de gestão de riscos dentro da instituição.

6.4. Diretorias Executivas

Cada direção de área é responsável pelo *compliance* dentro da sua área de responsabilidade, devendo:

i. Cooperar e apoiar a Diretoria de *Compliance*, bem como encorajar seu pessoal a fazer o mesmo;

ii. Assegurar que todo o pessoal dentro de seu controle esteja cumprindo os procedimentos, os processos, as políticas e as obrigações de *compliance* da instituição;

iii. Identificar e comunicar os riscos de *compliance* nas suas operações;

iv. Integrar as obrigações de *compliance* às práticas e aos procedimentos de negócio existentes em suas áreas de responsabilidade;

v. Apoiar e atender as atividades de treinamento de *compliance*;

vi. Desenvolver a conscientização junto ao pessoal sobre as obrigações de *compliance*, e orientá-los a cumprir os requisitos de competência e treinamento;

vii. Encorajar seu pessoal a levantar preocupações de *compliance,* apoiando-os e impedindo quaisquer formas de retaliação;

viii. Participar ativamente na gestão e na resolução de incidentes relacionados a *compliance* e outras questões, conforme requerido;

ix. Assegurar que, uma vez identificada a necessidade de ação corretiva, a ação corretiva apropriada seja recomendada e implementada.

6.5. Funcionários

i Auxiliar a operacionalização da Política de Gestão de Riscos;

ii Colaborar com a implementação das ações preventivas e/ou corretivas dos riscos;

iii Comunicar os riscos identificados ao superior hierárquico;

iv Participar ativamente da disseminação da cultura de gestão de riscos;

v Participar dos treinamentos;

vi Auxiliar na identificação e no mapeamento dos riscos do seu departamento;

vii Identificar, analisar, avaliar, propor tratamento aos riscos identificados em sua área.

7. CANAL DE DENÚNCIAS

O Canal de Denúncias do Sesc Goiás é um instrumento seguro e confidencial, acessível a qualquer pessoa, seja ela funcionário, aluno, fornecedor, parceiro ou membro da comunidade externa, que tenha conhecimento ou suspeita de condutas antiéticas, ilícitas ou irregulares, em violação a esta Política de Gestão de Riscos, às normas internas da instituição ou à legislação brasileira.

Garantimos o anonimato do denunciante e a proteção da identidade de todos os envolvidos no relato. Todas as denúncias recebidas são tratadas com a máxima seriedade, imparcialidade e sigilo, assegurando a devida apuração dos fatos e a adoção de medidas corretivas adequadas. O Sesc Goiás se compromete a proteger o denunciante contra qualquer forma de retaliação, promovendo um ambiente de confiança e transparência.

Para realizar uma denúncia, acesse o nosso canal online:

https://faleconoscosesc.sescgo.com.br/?tipoFormulario=denuncia.

Importante:

Denúncias realizadas de má-fé, com informações falsas ou com o intuito de prejudicar injustamente alguém, podem configurar crime de calúnia, conforme previsto no Art. 138 do Código Penal Brasileiro.

8. MEDIDAS DISCIPLINARES

A violação desta Política de Gestão de Riscos poderá acarretar a aplicação das seguintes medidas disciplinares:

Funcionários	Terceiros
1. Advertência (verbal ou escrita); 2. Suspensão; 3. Demissão; 4. Outras medidas judiciais na esfera cível, criminal e administrativa.	1. Suspensão do direito de licitar, nos termos do Regulamento de Licitações e Contratos; 2. Rescisão contratual; 3. Outras medidas judiciais na esfera cível, criminal e administrativa.

As penalidades serão aplicadas de forma imparcial e proporcional, com base na comprovação dos fatos e na responsabilidade dos envolvidos. A análise levará em consideração:

- A gravidade da infração;
- Os danos causados à instituição ou a terceiros;
- A reincidência de condutas inadequadas.

Em todos os casos, será assegurado o direito à ampla defesa e ao contraditório ao acusado.

No caso de violações cometidas por parceiros comerciais, o não cumprimento das regras poderá resultar na rescisão contratual e, se necessário, na adoção de medidas legais cabíveis, incluindo ação rescisória ou outras providências judiciais e administrativas.

9. INFORMAÇÕES E DÚVIDAS

Para maiores informações, reclamações, elogios ou dúvidas, o Sesc Goiás disponibiliza em seu website - https://sescgo.com.br/ - aba de comunicação direta com a Ouvidoria, além de diversos canais de atendimento.

10. ATUALIZAÇÃO E REVISÃO

O Sesc Goiás está comprometido com a melhoria contínua. Por isso, esta Política pode ser revisada e atualizada a qualquer momento. Recomendamos que você a consulte regularmente para se manter informado sobre possíveis alterações.

ANEXO I – DEFINIÇÕES PARA GESTÃO DE RISCOS

- **Sistema de Gestão** – conjunto de elementos interligados, que estabelecem políticas, objetivos e processos para alcançar os objetivos da instituição. Os elementos do sistema de gestão incluem a estrutura da instituição, papéis e responsabilidades, planejamento e operação.
- **Processo** – conjunto de atividades inter-relacionadas, que são executadas para alcançar produto, resultado ou serviço predefinido.
- **Governança** – combinação de processos e estruturas implantadas pela alta administração da instituição, para informar, dirigir, administrar, avaliar e monitorar atividades organizacionais, com o intuito de alcançar os objetivos e prestar contas dessas atividades para a sociedade.
- **Gestão de Riscos** – atividades coordenadas e estruturadas de um sistema de gestão, com o objetivo de mapear, avaliar e responder riscos que podem ser prejudiciais a instituição na busca de realização de suas metas e objetivos.
- **Riscos** – é a possibilidade da ocorrência de um evento que possa atingir os objetivos da instituição.
- **Riscos de *compliance*** – probabilidade da ocorrência e as consequências de não atendimento das obrigações de *compliance* da instituição.
- **Obrigações de *compliance*** – requisitos que uma instituição mandatoriamente tem que cumprir, como também os que uma instituição voluntariamente escolhe cumprir.
- ***Compliance*** – atendimento a todas as obrigações de *compliance* da instituição.
- **Não *compliance*** – não atendimento de obrigações de *compliance*.
- **Não conformidade** – não atendimento de um requisito. Uma não conformidade não é, necessariamente, um não *compliance*.
- **Objetivo organizacional** – situação que se deseja alcançar de forma a se evidenciar êxito no cumprimento da missão e no atingimento da visão de futuro da organização.
- **Meta** – alvo ou propósito com que se define um objetivo a ser alcançado.
- **Riscos** – é a possibilidade da ocorrência de um evento que possa atingir os objetivos da instituição.
- **Tolerância a Risco** – nível máximo de riscos aceitável pela instituição. Capacidade limite em lidar com os riscos.
- **Risco inerente** – risco a que uma organização está exposta sem considerar quaisquer medidas de controle que possam reduzir a probabilidade de sua ocorrência ou seu impacto.

- **Risco residual –** risco a que uma organização está exposta após a implementação de medidas de controle para o tratamento do risco.
- **Matriz de Riscos –** representação gráfica de probabilidade *versus* impacto dos riscos identificados pela Política de Gestão de Risco.
- **Probabilidade –** é a possibilidade de materialização de um risco, aponta o nível de exposição ao risco considerando a atual estrutura de controles da instituição.
- **Impacto –** resultado ou efeito de um evento que afeta de forma positiva ou negativa o Sesc Goiás considerando seus objetivos de negócio.
- **Evento –** fato ou acontecimento que materializa o risco. Um evento pode consistir em uma ou mais ocorrências, bem como pode ter várias causas.
- **Fonte do Risco –** elemento que, individualmente ou combinado, tem potencial para dar origem ao risco.
- **Plano de Contingência –** compreende-se no conjunto de medidas a serem adotadas diante da materialização do risco a fim de minimizar as consequências negativas que podem recair sobre a instituição.
- **Plano de Tratamento de Riscos –** compreende-se no conjunto de medidas a serem adotadas diante da possibilidade de materialização do risco, diminuindo o impacto para um nível que esteja de acordo com o apetite a riscos da instituição.
- **Consequência –** resultado de um evento que afeta os objetivos.
- **Controle –** medida que mantém e/ou modifica o risco.