

POLÍTICA DE GESTÃO DE RISCO

HISTÓRICO DE VERSÕES

Data	Versão	Descrição	Autor	Aprovação
06/11/2024	v.1.0	Primeira versão da Política de Gestão de Riscos.	Equipe Lara Martins Advogados	Anna Bastos
21/02/2025	v.1.1	Primeira versão da Política de Gestão de Riscos.	Equipe Técnica de Elaboração	Deborah Montenegro e Alexandre de Abreu e Silva
18/08/2025	v.1.2	Alteração na estrutura da gestão de riscos.	Equipe Técnica de Elaboração	Deborah Montenegro e Alexandre de Abreu e Silva
10/09/2025	v.1.3	Alteração de formatação.	Equipe Técnica de Elaboração	Deborah Montenegro e Alexandre de Abreu e Silva
27/04/2026	v.2.0	Ajuste de Diretrizes, Controles Internos e integração com Programa de Privacidade.	Deborah Montenegro	Alexandre de Abreu e Silva

Nos termos da Resolução Sesc nº 747/2025, fica a presente Política aprovada por:



Alexandre de Abreu e Silva
OAB/GO 16.486 - OAB/DF 53.259
Diretor Jurídico e de Compliance Sesc/Senac



SUMÁRIO

MENSAGEM DA ALTA DIREÇÃO	3
1. APRESENTAÇÃO	4
2. DOCUMENTOS DE REFERÊNCIA	4
3. ABRANGÊNCIA	5
4. ESTRUTURA DA GESTÃO DE RISCOS NO SESC GOIÁS.....	5
5. DIRETRIZES PARA GESTÃO DE RISCOS NO SESC GOIÁS	8
5.1. Entendendo a instituição e suas obrigações	9
5.1.1. Identificação e Análise de Risco	10
5.1.2. Classificação de Riscos	10
5.1.3. Avaliação de Risco	12
5.1.4. Identificação dos Controles	14
5.1.5. Plano de Ação e Tratamento de Riscos	17
5.2. Comunicação	19
5.3. Monitoramento e Análise Crítica	20
5.3.1. Monitoramento pela primeira linha de defesa	21
5.4. Gestão de Riscos de Privacidade e Segurança da Informação	21
5.4.1. Escopo e Fundamentos Normativos	21
5.4.2. Especificidades Metodológicas	22
5.4.3. Instrumentos Específicos.....	23
5.4.4. Articulação com o Encarregado de Proteção de Dados	23
5.4.5. Integração com o Programa de Privacidade	24
6. PAPÉIS E RESPONSABILIDADES	24
6.1. Alta Direção	24
6.2. Seção de Conformidade	25
6.3. Núcleo de Gestão de Riscos	26
6.4. Comissão de Ética e <i>Compliance</i>	26
6.5. Diretorias Executivas	26
6.6. Colaboradores	27
7. CANAL DE DENÚNCIAS	27
8. MEDIDAS DISCIPLINARES	28
9. INFORMAÇÕES E DÚVIDAS.....	28
10. ATUALIZAÇÃO E REVISÃO	29
ANEXO I – DEFINIÇÕES PARA GESTÃO DE RISCOS.....	30



MENSAGEM DA ALTA DIREÇÃO

A gestão eficaz dos riscos é fundamental para a sustentabilidade, integridade e excelência de nossas ações. Com base nesse princípio, o Sesc Goiás aprova sua Política de Gestão de Riscos, reforçando o compromisso com a prevenção, o controle e a mitigação de ameaças que possam comprometer o alcance dos nossos objetivos institucionais.

A presente política representa mais do que uma diretriz operacional: ela é uma expressão do nosso compromisso com a ética, a transparência e a boa governança. Por meio dela, orientamos nossas equipes a identificar, avaliar e tratar os riscos com responsabilidade, colaborando para a segurança institucional e a confiança da sociedade nas nossas entregas.

Todos nós temos um papel ativo nesse processo. Cada colaborador, gestor e parceiro é chamado a contribuir para a construção de uma cultura organizacional resiliente, pautada pela integridade e pelo cumprimento das nossas obrigações de compliance.

Reafirmamos que a gestão de riscos não é uma tarefa isolada, mas um esforço coletivo que deve estar presente nas decisões do dia a dia. Contamos com o envolvimento de cada um para tornar o Sesc Goiás uma referência em governança, integridade e responsabilidade institucional.

Marcelo Baiocchi Carneiro

Marcelo Baiocchi Carneiro

Presidente do Conselho Regional do Sesc Goiás

José Leopoldo Veiga Jardim Filho

Leopoldo Veiga Jardim

Diretor Regional do Sesc Goiás

Alexandre de Abreu e Silva

Alexandre de Abreu e Silva

Diretor Jurídico e de Compliance do Sesc Goiás



POLÍTICA DE GESTÃO DE RISCOS

1. APRESENTAÇÃO

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

Os riscos 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* constitui componente relevante do Sistema de Gestão de *Compliance* (SGC), devendo estar integrada ao processo de gestão de riscos da instituição. 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 classificação dos riscos e implementem ações de tratamento de forma estruturada.

Dessa forma, esta Política contribui para o fortalecimento da governança, o aprimoramento dos controles internos e a promoção de 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 NBR ISO 31000:2018 – Sistema de gestão de riscos.
- Norma ABNT NBR ISO 31073:2022 – Sistema de gestão de riscos.
- Norma ABNT NBR ISO/IEC 27005:2019 – Gestão de Riscos de Segurança da Informação.
- Norma ABNT NBR ISO/IEC 27557:2023 – Aplicação da ABNT NBR ISO 31000:2018 para gestão de riscos de privacidade organizacional.
- Norma ABNT ISO 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.
- Política de Gestão de Riscos e Controles Internos 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 colaboradores 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 estrutura sua gestão de riscos e controles internos com base no Modelo das Três Linhas, conforme preconizado pelo *The Institute of Internal Auditors* (IIA). Esse modelo tem por objetivo fortalecer a governança institucional, aprimorar a comunicação interna e aumentar a eficácia na identificação, avaliação, tratamento e monitoramento de riscos.

O modelo estabelece a segregação de responsabilidades entre as diferentes áreas da instituição, promovendo uma atuação estruturada, coordenada e complementar. Reforça, igualmente, a interação entre os atores internos e os órgãos fiscalizadores externos, que atuam como supervisores desse processo.

A estrutura de gestão de riscos está organizada conforme as seguintes linhas de defesa:



i. Primeira linha de defesa — Gestão Operacional de Riscos:

A primeira linha de defesa é composta pelos gestores de negócios e líderes de equipe, responsáveis pela execução direta dos processos e atividades finalísticas. Sua atuação compreende a identificação, avaliação, mitigação e monitoramento cotidiano dos riscos inerentes às suas áreas, bem como a implementação e operacionalização dos controles internos.

Compete à primeira linha de defesa:

- a) identificar, analisar e avaliar os riscos associados aos seus processos;
- b) implementar e operacionalizar controles internos adequados;
- c) elaborar e executar planos de ação para o tratamento dos riscos identificados;
- d) monitorar a efetividade dos controles e das ações implementadas;
- e) reportar à segunda linha de defesa informações sobre riscos, controles e planos de ação;
- f) assegurar a conformidade dos processos com normas internas, requisitos legais e diretrizes institucionais;
- g) estabelecer e manter estruturas e processos adequados para o gerenciamento de operações e riscos, incluindo controles internos;
- h) manter diálogo contínuo com o órgão de governança, reportando resultados planejados, reais e esperados, vinculados aos objetivos institucionais.

ii. Segunda linha de defesa — Supervisão, Orientação e Controle:

A segunda linha de defesa é composta pelas funções de apoio, conformidade e supervisão do gerenciamento de riscos, integrando o Núcleo de Gestão de Riscos, a Gerência de Controle Interno, a área jurídica e demais funções correlatas.

Sua atuação tem por finalidade fornecer orientação, suporte metodológico, supervisão e avaliação sobre a forma como os riscos são gerenciados pela primeira linha, contribuindo para o fortalecimento da governança e dos controles internos da instituição.

No âmbito da segunda linha, as responsabilidades são exercidas de forma complementar, observando-se a seguinte segregação funcional:

a) Gestão de Riscos (função de coordenação e suporte metodológico)

A função de Gestão de Riscos tem caráter de coordenação e suporte metodológico, competindo-lhe:

- definir, manter e disseminar a metodologia institucional de gestão de riscos;
- coordenar o processo de identificação, análise, avaliação e tratamento de riscos;
- apoiar as áreas na realização do mapeamento de riscos e controles;



- consolidar as informações de riscos e controles em nível institucional;
- monitorar a evolução dos riscos e acompanhar a implementação das ações de tratamento;
- avaliar o nível de risco residual e seu alinhamento ao apetite ao risco institucional;
- assessorar a Administração Regional na tomada de decisões relacionadas à gestão de riscos;
- promover a cultura de gestão de riscos na instituição;
- fornecer análises e relatórios sobre a adequação e a eficácia do gerenciamento de riscos.

b) Controle Interno (função de avaliação e supervisão independente)

A função de Controle Interno, exercida pela Gerência de Controle Interno, atua na avaliação da qualidade dos controles internos e da conformidade dos processos, contribuindo para o fortalecimento da governança institucional.

Compete ao Controle Interno:

- avaliar a adequação, a suficiência e a efetividade dos controles internos adotados pelas áreas;
- analisar a consistência entre os riscos identificados e os controles implementados;
- identificar fragilidades, lacunas e oportunidades de melhoria nos controles internos;
- recomendar aprimoramentos nos processos de controle e na gestão de riscos;
- verificar a conformidade dos processos com normas internas, regulamentos e legislação aplicável;
- monitorar, de forma independente, a implementação das ações de tratamento de riscos;
- apoiar a Administração Regional com avaliações independentes sobre a eficácia dos controles internos;
- supervisionar o Programa de Compliance do Sesc Goiás no âmbito de suas competências.

iii. Terceira linha de defesa — Auditoria e Avaliação Independente:

A terceira linha de defesa é caracterizada pela atividade de auditoria, exercida com independência, autonomia técnica e objetividade, voltada à avaliação da governança, do gerenciamento de riscos e dos controles internos, com vistas ao aprimoramento contínuo da gestão institucional.

No âmbito do Sesc, o Conselho Fiscal — órgão colegiado autônomo da Administração Nacional — exerce as atribuições típicas desta linha, conforme previsto em Regimento Interno. Dentre suas competências, incluem-se a fiscalização contábil, financeira e patrimonial, o exame das demonstrações e prestações de contas, a realização de auditorias e a emissão de pareceres independentes, sem envolvimento na execução da gestão.



Tais atribuições são compatíveis, por analogia e como referencial de boas práticas, com os serviços de avaliação descritos no Referencial Técnico da Atividade de Auditoria Interna Governamental aprovado pela Instrução Normativa CGU nº 3/2017¹, o que reforça o posicionamento do Conselho Fiscal como instância independente de avaliação no âmbito da governança institucional do Sesc.

Compete à terceira linha de defesa:

- a) manter a prestação de contas primária perante o órgão de governança, com independência em relação às responsabilidades da gestão;
- b) comunicar avaliações e assessoramentos independentes e objetivos à gestão e ao órgão de governança sobre a adequação e a eficácia da governança e do gerenciamento de riscos, incluindo os controles internos, de forma a apoiar o atingimento dos objetivos organizacionais e promover a melhoria contínua;
- c) reportar ao órgão de governança eventuais riscos à sua independência e objetividade, implementando as salvaguardas necessárias;
- d) realizar avaliações independentes com base em evidências, abrangendo os aspectos de regularidade, economicidade, eficiência e eficácia da gestão;
- e) acompanhar os planos de ação voltados ao aprimoramento dos controles internos.

O Conselho Fiscal configura-se, assim, como a instância responsável pela terceira linha de defesa, atuando de forma complementar e independente em relação à gestão e às funções de controle exercidas pelas primeira e segunda linhas.

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 sistemático e eficaz dos riscos organizacionais.

Esse sistema institucional, de caráter permanente, é conduzido de forma coordenada pela área de Gestão de Riscos, com o apoio das demais instâncias da segunda linha de defesa, e supervisionado pela Alta Direção, no âmbito de suas atribuições.

Seu foco está na identificação, análise, avaliação e tratamento dos riscos, bem como no monitoramento contínuo e na comunicação das informações relevantes, com o objetivo de subsidiar a tomada de decisões em todos os níveis da instituição.

¹ A IN CGU nº 3/2017 destina-se formalmente ao Poder Executivo Federal. Sua menção neste documento tem caráter referencial, em razão da convergência entre as boas práticas que estabelece e as atribuições exercidas pelo Conselho Fiscal do Sesc, não implicando sujeição normativa direta da instituição a esse instrumento.



Considerando a natureza multidisciplinar da gestão de riscos, o processo deve ser conduzido de forma estruturada e colaborativa, preferencialmente por meio de oficinas de trabalho, envolvendo profissionais com conhecimento sobre os processos, projetos ou atividades avaliadas.

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

5.1. Entendendo a instituição e suas obrigações

A compreensão do contexto institucional, incluindo fatores internos, externos e as obrigações de *compliance*, constitui a base para a identificação dos riscos.

Nesse sentido, é essencial que a instituição compreenda tais elementos de forma estruturada. A identificação das obrigações de *compliance* deverá ser realizada em articulação com as áreas responsáveis pelos temas regulatórios e com os gestores dos processos envolvidos.

Para fins desta Política, os riscos de *compliance* são considerados uma categoria específica de riscos institucionais, relacionados ao descumprimento de obrigações legais, regulatórias, normativas e éticas, devendo ser gerenciados de forma integrada aos demais riscos da instituição.

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*, contribuindo para a identificação, análise e tratamento dos riscos aos quais a instituição está exposta.

5.1.1. Identificação e Análise de Risco

O propósito da identificação de riscos é encontrar, reconhecer e descrever eventos que possam evitar, atrasar, prejudicar ou impedir o alcance dos objetivos institucionais do Sesc Goiás, bem como gerar impactos negativos relevantes para a instituição.

O processo de identificação deve contemplar riscos cujas fontes estejam ou não sob o controle da instituição, consistindo no levantamento sistemático dos riscos potenciais associados a atividades, processos ou operações, considerando fatores internos e externos relevantes, tais como aspectos operacionais, tecnológicos, humanos, regulatórios e ambientais.

A identificação de riscos deve ser conduzida de forma estruturada, interativa e colaborativa, com base no conhecimento e na experiência dos envolvidos. Para tanto, recomenda-se:

- i. Analisar o fluxo dos processos da instituição;
- ii. Envolver os gestores e equipes das áreas relacionadas ao processo avaliado;
- iii. Levantar as obrigações de *compliance* mandatórias e voluntárias;
- iv. descrever e registrar os riscos identificados de forma clara e estruturada.

Cada área deverá manter seu respectivo mapa de riscos, contendo o registro dos riscos identificados e, no mínimo, as seguintes informações:

- i. Natureza do risco e suas características;
- ii. Causas e eventos associados;
- iii. Probabilidade de ocorrência e impacto das consequências;
- iv. Natureza e magnitude das consequências;
- v. Complexidade e interdependência dos riscos;
- 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:** Esta categoria inclui:
 - **Riscos de Crédito:** perda resultante da incerteza quanto ao recebimento, ou não, de valores junto a terceiros.
 - **Riscos de Liquidez:** incapacidade da instituição de 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, taxa de juros, entre 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. Avaliação de Risco

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.

Vejam os quadros 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.	1
Baixo	Pequeno impacto nos objetivos.	2
Médio	Moderado impacto nos objetivos, porém recuperável.	3
Alto	Significativo impacto nos objetivos de difícil reversão.	4
Muito alto	Catastrófico impacto nos objetivos 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, $NR = P \times I$. 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:

- 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;
- Riscos Alto:** 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 Médio:** 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:

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

5.1.4. Identificação dos Controles

Após a etapa de identificação e análise dos riscos, na qual são devidamente compreendidas suas causas, fatores de risco e potenciais consequências, procede-se à identificação dos controles internos existentes, com o objetivo de verificar em que medida os riscos identificados já se encontram mitigados no âmbito dos processos institucionais.



Para fins desta Política, consideram-se **controles internos** as medidas, práticas, mecanismos ou procedimentos instituídos pela organização com a finalidade de prevenir, detectar, corrigir ou direcionar eventos de risco, atuando sobre suas causas e/ou consequências.

Inicialmente, o nível de risco é determinado com base nos **riscos inerentes**², ou seja, aqueles avaliados na ausência de quaisquer medidas de controle. A partir dessa linha de base, são identificados os controles que incidem sobre os riscos mapeados, permitindo a análise da sua capacidade de mitigação e de sua efetividade.

A identificação dos controles deverá ser conduzida de forma **estruturada, sistemática e colaborativa**, envolvendo as áreas responsáveis pelos processos (primeira linha de defesa), com a devida coordenação metodológica do Núcleo de Gestão de Riscos, assegurando a adequada vinculação entre riscos, causas, controles e consequências.

i. Identificação dos controles existentes

As áreas gestoras deverão proceder ao mapeamento dos controles internos atualmente existentes, sejam eles formais ou informais, que contribuam para a mitigação dos riscos identificados, considerando, entre outros:

- procedimentos operacionais;
- políticas, normas e regulamentos internos;
- mecanismos de aprovação, validação e segregação de funções;
- sistemas de monitoramento, controle e registro de informações;
- práticas de supervisão, revisão e acompanhamento;
- quaisquer outras medidas que possam influenciar a probabilidade de ocorrência ou o impacto dos riscos.

Compete ao **Núcleo de Gestão de Riscos, Proteção de Dados e Ouvidoria**:

- conduzir metodologicamente o processo de identificação dos controles;
- apoiar as áreas na adequada vinculação entre riscos, suas causas e os controles correspondentes;
- assegurar a padronização das informações levantadas;
- consolidar os controles identificados nos registros de riscos da instituição.

² Risco inerente é o que se apresenta a uma instituição na ausência de qualquer medida gerencial que possa alterar a probabilidade ou o impacto de um risco.



ii. Análise dos controles identificados

Uma vez identificados, os controles deverão ser analisados quanto à sua **adequação, suficiência e efetividade**, verificando-se se são capazes de mitigar os riscos de forma compatível com o nível de exposição da instituição e com os objetivos dos processos envolvidos.

Compete ao **Núcleo de Gestão de Riscos, Proteção de Dados e Ouvidoria**:

- avaliar, em conjunto com as áreas, a relação entre riscos, suas causas e os controles existentes;
- analisar se os controles identificados atuam de forma adequada sobre as causas e/ou consequências dos riscos;
- apoiar as áreas na avaliação preliminar da efetividade dos controles mapeados.

Compete à **Gerência de Controle Interno**:

- realizar análise crítica dos controles mapeados, sob a perspectiva de controles internos;
- avaliar a suficiência, consistência e qualidade dos controles existentes;
- identificar fragilidades, lacunas ou inconsistências nos controles;
- recomendar melhorias e aperfeiçoamentos, quando necessário.

iii. Determinação do risco residual

Com base na análise dos controles identificados, será determinado o risco residual³, entendido como o nível de risco remanescente após a consideração da adequação e efetividade dos controles existentes.

Compete ao **Núcleo de Gestão de Riscos, Proteção de Dados e Ouvidoria**:

- Auxiliar na mensuração do nível de risco residual, considerando a efetividade dos controles identificados;
- Avaliar o grau de exposição residual dos riscos em relação ao apetite ao risco da instituição.

A Gerência de Controle Interno poderá contribuir com análises críticas e recomendações quanto à consistência da avaliação realizada, sem prejuízo de sua atuação independente.

Quando o risco residual não atingir um patamar de riscos aceitável, o risco deverá continuar sendo tratado por meio de novos controles.

iv. Classificação dos controles

Os controles identificados e/ou a serem implementados, deverão ser classificados conforme sua natureza, de modo a facilitar sua análise, avaliação e gestão no contexto do gerenciamento de riscos:

³ Risco residual é aquele que ainda permanece após a definição de resposta da administração.



- **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.
- **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.

v. Resultado da etapa

Como resultado da identificação e análise dos controles, a instituição deverá dispor de:

- mapeamento estruturado dos controles existentes;
- avaliação da adequação, suficiência e efetividade dos controles;
- identificação de lacunas, fragilidades e oportunidades de melhoria;
- determinação do nível de risco residual.

As informações consolidadas nesta etapa subsidiarão a definição das estratégias de tratamento dos riscos, conforme disposto no item 5.1.5 desta Política, contribuindo para a adoção de medidas proporcionais ao nível de exposição identificado.

5.1.5. Plano de Ação e Tratamento de Riscos

Uma vez avaliados os riscos inerentes e residuais, deverá ser elaborado um plano de ação para o tratamento dos riscos identificados, considerando a criticidade de cada risco e o apetite ao risco da instituição.

O plano de ação deverá detalhar as medidas necessárias para tratar os riscos, priorizando as ações de acordo com sua relevância, criticidade e os recursos disponíveis, de modo a promover a redução da exposição a níveis aceitáveis.

Além da avaliação dos riscos, o Sesc Goiás deverá analisar as alternativas de tratamento, ponderando o custo-benefício de cada medida, a viabilidade operacional e o impacto esperado, de forma a selecionar a estratégia mais adequada, eficaz e sustentável.

i. Estratégias de tratamento de riscos



As estratégias de tratamento de riscos poderão ser aplicadas isoladamente ou em combinação, conforme a natureza e criticidade dos riscos:

- **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.

ii. Elaboração do Plano de Ação

Para os riscos, sejam inerentes ou residuais, que demandem tratamento, deverá ser elaborado Plano de Ação contendo, no mínimo:

- ações a serem implementadas;
- controles a serem instituídos ou aprimorados;
- responsáveis pela execução;
- prazos para implementação;
- recursos necessários;
- forma de acompanhamento e evidências de execução.

Compete às **áreas responsáveis pelos processos (primeira linha de defesa):**



- elaborar e implementar os planos de ação;
- definir e operacionalizar os controles necessários ao tratamento dos riscos;
- assegurar a execução das ações nos prazos estabelecidos.

Compete ao **Núcleo de Gestão de Riscos**:

- apoiar metodologicamente a elaboração dos planos de ação;
- avaliar a aderência das medidas propostas aos riscos identificados;
- acompanhar a evolução das ações e seus efeitos sobre o nível de risco;
- consolidar e reportar as informações relativas ao tratamento dos riscos.

Compete à **Gerência de Controle Interno**:

- analisar criticamente os planos de ação propostos, sob a perspectiva de controles internos;
- avaliar a adequação e suficiência dos controles propostos para mitigação dos riscos;
- recomendar melhorias e aperfeiçoamentos nas medidas definidas;
- acompanhar, de forma independente, a consistência da implementação das ações.

iii. **Implementação e monitoramento**

A implementação das ações previstas no Plano de Ação é de responsabilidade das áreas gestoras dos processos, cabendo-lhes assegurar a efetiva execução das medidas definidas.

O monitoramento das ações deverá ser realizado de forma contínua, com o objetivo de:

- verificar a efetividade das medidas implementadas;
- identificar eventuais desvios ou atrasos;
- avaliar a necessidade de ajustes ou revisão das ações;
- assegurar que o risco residual permaneça dentro dos níveis aceitáveis.

O Núcleo de Gestão de Riscos atuará no acompanhamento sistemático da execução das ações e na atualização do nível de risco.

A Gerência de Controle Interno poderá realizar avaliações independentes quanto à efetividade das ações implementadas e à adequação dos controles, sem participação direta na execução.

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 aqueles que as necessitam?

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 e implementação do Plano de Ação e das medidas de tratamento de riscos, os riscos deverão ser monitorados de forma contínua e periódica, com o objetivo de avaliar a efetividade dos controles internos implementados e a evolução do nível de risco residual.

O monitoramento tem por finalidade assegurar que a gestão de riscos do Sesc Goiás esteja operando conforme planejado, bem como identificar eventuais desvios, fragilidades ou oportunidades de aprimoramento, considerando possíveis alterações nas condições internas e externas que possam impactar o nível de exposição aos riscos.



O monitoramento deverá ocorrer em ciclos periódicos, com intervalo mínimo de 06 (seis) meses e máximo de 01 (um) ano, podendo ser ajustado conforme a criticidade dos riscos e a dinâmica dos processos.

Os resultados do monitoramento, incluindo relatórios e registros das análises realizadas, deverão ser formalizados e submetidos à apreciação do Presidente e do Diretor Regional, sendo posteriormente mantidos como informação documentada, de modo a assegurar a rastreabilidade, a transparência e o histórico do processo de gestão de riscos.

5.3.1. Monitoramento pela primeira linha de defesa

Os gestores das áreas são responsáveis pelo monitoramento contínuo dos riscos associados aos seus processos, devendo acompanhar a execução dos controles implementados e a efetividade das ações previstas nos planos de tratamento.

O monitoramento deverá contemplar a identificação de desvios, inconsistências, falhas de controle ou quaisquer outras situações relevantes que possam comprometer a adequada gestão dos riscos, devendo, quando necessário, ser adotadas medidas corretivas ou de aprimoramento.

Os gestores poderão contar com o apoio de suas equipes e de outras áreas, quando pertinente, mantendo a responsabilidade pela supervisão e acompanhamento dos riscos sob sua gestão.

Cumprir destacar que o monitoramento contínuo dos riscos não se confunde com a execução rotineira de atividades de controle nos processos de negócio. Atividades como aprovações de transações, conciliações contábeis, validações sistêmicas ou verificações operacionais constituem controles internos, voltados ao cumprimento de normas e à integridade dos processos, enquanto o monitoramento de riscos possui caráter analítico e gerencial, voltado à avaliação da efetividade desses controles e da exposição ao risco.

5.4. Gestão de Riscos de Privacidade e Segurança da Informação

5.4.1. Escopo e Fundamentos Normativos

A gestão de riscos de privacidade e segurança da informação constitui subprocesso especializado da gestão de riscos institucional, integrado ao sistema descrito nesta Política e regido pelas disposições específicas da LGPD (Lei nº 13.709/2018, arts. 46 e 50), da ABNT NBR ISO/IEC 27005:2019 e da ISO/IEC 27701:2019, normas já referenciadas na Seção 2 deste documento.

O subprocesso é operacionalizado por meio dos instrumentos específicos do Programa de Governança em Privacidade do Sesc Goiás, em especial a Política de Avaliação de Riscos e Impactos, o Mapeamento de Riscos de Privacidade, o Relatório de Impacto à Proteção de Dados Pessoais (RIPD), o



Framework de Gestão de Terceiros e o Plano de Resposta a Incidentes, os quais integram o sistema normativo institucional e devem ser observados em conjunto com as disposições desta Política.

O Sesc Goiás deve ser capaz de demonstrar, perante o Departamento Nacional, a Autoridade Nacional de Proteção de Dados (ANPD) e demais partes interessadas, que o processo de avaliação de riscos de privacidade é estruturado, documentado e integrado à gestão institucional, em conformidade com o princípio da responsabilização e prestação de contas previsto no art. 6º, X, e no art. 50, § 2º, I, da LGPD e com a Res. CD/ANPD nº 15/2024.

5.4.2. Especificidades Metodológicas

Além dos critérios gerais de probabilidade e impacto previstos na Seção 5.1.3, a avaliação de riscos de privacidade e segurança da informação contempla elementos metodológicos específicos, decorrentes da natureza peculiar dos bens jurídicos protegidos e das exigências normativas aplicáveis, a saber:

- **Identificação e valoração dos ativos de informação pessoal:** compreende o mapeamento dos dados pessoais tratados (ativos primários) e dos sistemas, aplicações e infraestruturas que os processam (ativos de suporte), com avaliação de sua criticidade e das consequências da perda de confidencialidade, integridade ou disponibilidade;
- **Dupla dimensão do impacto:** a avaliação considera, de forma distinta e complementar, as consequências organizacionais para o Sesc Goiás (danos reputacionais, sanções regulatórias, custos de remediação, interrupção de operações) e os impactos sobre os titulares de dados pessoais (violação de direitos, danos materiais e imateriais, discriminação). O nível de impacto sobre titulares integra os critérios de priorização do tratamento do risco, independentemente do apetite ao risco institucional, em especial quando se tratar de dados sensíveis, dados de crianças e adolescentes ou operações de monitoramento sistemático;
- **Análise de ameaças e vulnerabilidades específicas:** abrange a identificação de ameaças com potencial de comprometer a confidencialidade, a integridade ou a disponibilidade de dados pessoais (acesso não autorizado, vazamento, alteração indevida, destruição, exfiltração externa ou uso desvirtuado por agentes internos), bem como das vulnerabilidades técnicas e organizacionais que possam ser exploradas, considerando os sistemas institucionais relevantes e os controles existentes;
- **Processo iterativo com pontos de decisão formalizados:** a aceitação formal do risco residual deve ser precedida da verificação da adequação da avaliação realizada e da suficiência das medidas de tratamento propostas. Caso o risco residual ainda não satisfaça os critérios de aceitação, uma nova iteração deve ser conduzida antes do encerramento do ciclo.



5.4.3. Instrumentos Específicos

A gestão de riscos de privacidade e segurança da informação se materializa por meio dos seguintes instrumentos:

- **Mapeamento de Riscos de Privacidade:** registro estruturado dos riscos identificados nas operações de tratamento de dados pessoais do Sesc Goiás, contendo a avaliação de probabilidade, impacto organizacional, impacto sobre os titulares, controles existentes, risco residual e plano de ação. Deve ser revisado em ciclos anuais ou quando identificadas novas operações de tratamento, mudanças relevantes nos sistemas ou alterações normativas;
- **Relatório de Impacto à Proteção de Dados Pessoais (RIPD/DPIA):** documento de avaliação aprofundada de impactos sobre a privacidade, obrigatório para operações de tratamento de alto risco. São consideradas operações de alto risco, entre outras, aquelas que envolvam dados sensíveis, dados biométricos, monitoramento sistemático por CFTV ou similares, dados de crianças e adolescentes e informações de saúde dos trabalhadores. O RIPD deve ser elaborado antes do início ou da alteração substancial da operação de tratamento, conforme diretrizes da ANPD e do art. 38 da LGPD;
- **Plano de Ação de Privacidade e Segurança da Informação:** conjunto estruturado de medidas de tratamento derivadas de cada ciclo avaliativo do Mapeamento de Riscos de Privacidade e dos RIPDs elaborados, contendo responsáveis, prazos e indicadores de efetividade. Deve ser integrado ao sistema de monitoramento da gestão de riscos institucional, com reporte periódico ao Núcleo de Gestão de Riscos e à Alta Direção.

5.4.4. Articulação com o Encarregado de Proteção de Dados

O Encarregado de Proteção de Dados (DPO), no exercício das atribuições previstas no art. 41 da LGPD e formalizadas no diagrama de governança institucional, integra em caráter consultivo o processo de avaliação de riscos de privacidade, em articulação com o Núcleo de Gestão de Riscos, Proteção de dados e Ouvidoria. Compete ao DPO, no âmbito deste processo:

- orientar a identificação e a análise dos riscos relacionados ao tratamento de dados pessoais, especialmente nas operações de alto risco;
- validar os RIPDs elaborados e emitir parecer técnico sobre a adequação das medidas de tratamento propostas às exigências legais e às boas práticas de proteção de dados;
- assessorar as áreas responsáveis na definição de medidas técnicas e administrativas de tratamento dos riscos de privacidade identificados; e



- comunicar à Alta Direção os riscos classificados como altos ou críticos no domínio da privacidade e da segurança da informação, em conjunto com o relatório consolidado elaborado pelo Núcleo de Gestão de Riscos.

5.4.5. Integração com o Programa de Privacidade

As saídas (os *outputs*) da gestão de riscos de privacidade e segurança da informação – mapas de riscos, RIPDs e planos de ação – alimentam e são alimentados pelos demais componentes do Programa de Governança em Privacidade do Sesc Goiás, configurando relações de interdependência que devem ser observadas na execução do processo, especialmente nos seguintes eixos:

- **Gestão de Terceiros:** os riscos identificados em operações que envolvam operadores e suboperadores devem refletir-se na classificação de risco dos fornecedores e na definição de cláusulas contratuais de proteção de dados, nos termos do Framework de Gestão de Terceiros vigente;
- **Resposta a Incidentes:** os cenários de incidentes identificados no Mapeamento de Riscos de Privacidade devem subsidiar a atualização dos gatilhos e procedimentos do Plano de Resposta a Incidentes, em especial os critérios para notificação obrigatória à ANPD e aos titulares; e
- **Matriz de Obrigações de Compliance LGPD:** os resultados dos ciclos avaliativos devem alimentar periodicamente a Matriz de Obrigações de Compliance LGPD, garantindo o alinhamento entre o nível de risco residual identificado e o status de implementação das obrigações legais correspondentes.

As informações consolidadas no âmbito desta seção constituem informação documentada do Sistema de Gestão de Privacidade do Sesc Goiás e devem ser mantidas com controle de versões, acesso restrito a pessoas autorizadas e disponibilidade para fins de auditoria interna, avaliações do Departamento Nacional e exames da ANPD.

6. PAPÉIS E RESPONSABILIDADES

6.1. Alta Direção

- Definir diretrizes e aprovar os padrões relacionados aos processos de gestão de riscos, com vistas à implementação e ao aprimoramento contínuo da Política de Gestão de Riscos do Sesc Goiás;
- Designar papéis e responsabilidades relativos à gestão de riscos, assegurando a adequada alocação dos riscos às áreas competentes;
- Avaliar e aprovar a Matriz de Riscos e os Planos de Ação correspondentes;



- iv. Estabelecer o apetite ao risco, bem como os níveis aceitáveis de exposição aos riscos;
- v. Assegurar o adequado funcionamento do processo de identificação, avaliação, tratamento e monitoramento dos riscos;
- vi. Acompanhar a consolidação das informações de riscos e controles internos em nível institucional;
- vii. Monitorar os riscos classificados como altos e extremos, em conjunto com a Comissão de Ética e Compliance;
- viii. Avaliar a adequação dos recursos destinados à implementação e ao fortalecimento da gestão de riscos;
- ix. Promover a cultura de gestão de riscos e controles internos na instituição.

6.2. Seção de Conformidade

A Seção de Conformidade, no âmbito da Gerência de Controle Interno, atua no suporte, monitoramento e avaliação dos processos de compliance e de gestão de riscos, sob a perspectiva de conformidade e controles internos.

No âmbito da gestão de riscos, sua atuação concentra-se na avaliação de conformidade e na análise crítica dos controles internos, sem atuação executiva no processo de gestão de riscos.

- i. Operacionalizar o 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. Apoiar a avaliação e o registro dos riscos de compliance, em articulação com o Núcleo de Gestão de Riscos;
- v. Propor plano anual de avaliação de controles internos, com foco na verificação da eficácia da gestão de riscos do Sesc Goiás;
- vi. Avaliar o desempenho do sistema de gestão de compliance, identificando a necessidade de ações corretivas;
- vii. Identificar e apontar oportunidades de melhoria nos processos de controle interno e de gestão de riscos;
- viii. Garantir que os indicadores de desempenho do *compliance* estejam estabelecidos.
- ix. Analisar criticamente os indicadores-chave de risco (KRI's), quanto à sua adequação e consistência;
- 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 mecanismos para o levantamento de preocupações, assegurando o adequado tratamento das questões reportadas;
- xiii. Comunicar à Alta Direção os resultados das avaliações realizadas, assegurando independência e imparcialidade.

6.3. Núcleo de Gestão de Riscos

No âmbito desta Política, as atribuições descritas referem-se especificamente à função de gestão de riscos desempenhada pelo Núcleo. Sua atuação possui caráter metodológico, de coordenação e de suporte, não incluindo a execução direta de controles ou a implementação de ações de tratamento, que são de responsabilidade das áreas operacionais.

- i. Coordenar a implementação, manutenção e aprimoramento da metodologia de gestão de riscos da instituição;
- ii. Conduzir, de forma estruturada, o processo de identificação, análise, avaliação e tratamento de riscos;
- iii. Apoiar as áreas na identificação de riscos, na análise de controles e na elaboração dos planos de ação;
- iv. Consolidar as informações de riscos e controles em nível institucional;
- v. Monitorar a evolução dos riscos e o andamento das ações de tratamento;
- vi. Avaliar o nível de risco residual e seu alinhamento ao apetite ao risco;
- vii. Elaborar relatórios gerenciais e reportar periodicamente à Alta Direção;
- viii. Promover a cultura de gestão de riscos na instituição.

6.4. Comissão de Ética e Compliance

- i. Propor à Alta Direção as diretrizes e estratégias para a gestão de riscos;
- ii. Acompanhar e supervisionar o processo de gestão de riscos do Sesc Goiás, sem atuação executiva;
- iii. Avaliar e acompanhar os riscos classificados como altos e extremos, bem como comunicar periodicamente à Alta Direção sua evolução e os respectivos planos de tratamento;
- iv. Promover a cultura de gestão de riscos na instituição.

6.5. Diretorias Executivas

Cada direção de área é responsável pela gestão de riscos, controles internos e compliance no âmbito de sua área de atuação, devendo:



- i. Cooperar e apoiar as áreas de gestão de riscos e compliance, bem como encorajar seu pessoal a fazer o mesmo;
- ii. Assegurar que todo o pessoal sob sua responsabilidade cumpra os processos, procedimentos, políticas internas e obrigações legais e regulatórias aplicáveis;
- iii. Identificar, analisar e comunicar os riscos associados às suas operações;
- iv. Integrar a gestão de riscos, controles internos e obrigações de compliance às práticas e aos processos de negócio de sua área;
- v. Apoiar e participar das ações de capacitação relacionadas à gestão de riscos, controles internos e compliance;
- vi. Promover a conscientização do pessoal quanto à gestão de riscos, controles internos e obrigações de compliance, assegurando o adequado nível de competência;
- vii. Incentivar a comunicação de riscos, desvios e preocupações, assegurando ambiente seguro e sem retaliações;
- viii. Atuar na gestão e na resolução de incidentes relacionados a riscos, controles e compliance, conforme aplicável;
- ix. Assegurar que as ações corretivas necessárias sejam devidamente definidas e implementadas;
- x. Monitorar os riscos e controles relacionados à sua área de atuação;
- xi. Elaborar e implementar planos de ação para tratamento dos riscos identificados;
- xii. Assegurar a efetividade dos controles internos sob sua responsabilidade;

6.6. Colaboradores

- i. Contribuir para a operacionalização da Política de Gestão de Riscos;
- ii. Colaborar com a implementação das ações de tratamento de riscos;
- iii. Comunicar riscos, desvios ou fragilidades identificadas ao superior hierárquico;
- iv. Participar da disseminação da cultura de gestão de riscos e controles internos;
- v. Participar das ações de capacitação e treinamento;
- vi. Auxiliar na identificação e no mapeamento dos riscos do seu departamento;
- vii. Contribuir para a melhoria contínua dos processos e controles internos.

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://www.contatoseguro.com.br/sescgo>

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

O descumprimento das diretrizes estabelecidas nesta Política sujeita os envolvidos à aplicação de medidas disciplinares, observados os critérios de classificação da infração (leve, média ou grave), os fatores agravantes e atenuantes e a matriz de dosimetria estabelecidos na **Política de Consequências e Medidas Disciplinares do [Senac/Sesc] Goiás**, instrumento normativo específico e vinculante para a definição, gradação e aplicação de sanções no âmbito do Programa de *Compliance*.

A medida disciplinar cabível observará a proporcionalidade entre a gravidade da conduta e a sanção aplicada, podendo abranger, conforme o vínculo da pessoa envolvida:

- **Colaboradores (CLT):** advertência verbal, advertência escrita, suspensão ou rescisão por justa causa, além de medidas complementares de caráter educativo ou corretivo;
- **Terceiros, parceiros e fornecedores:** advertência formal, multa contratual, suspensão temporária ou rescisão contratual, e inabilitação para novas contratações, conforme o caso.

Em todos os casos será assegurado o direito à ampla defesa e ao contraditório, sem prejuízo da apuração de responsabilidade civil, administrativa ou criminal pelas autoridades competentes.

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.

