MANUAL DE CONFORMIDADE E AVALIAÇÃO DE RISCO

EMDEC

CAMPINAS

2022

EMPRESA MUNICIPAL DE DESENVOLVIMENTO DE CAMPINAS

EMDEC

Vinicius Issa Lima Riverete
Diretor-Presidente da Emdec

Fernando de Caires Barbosa
Secretário Municipal de Transportes

Elaboração:
Comissão de Conformidade e Gerenciamento de Risco
Alan Wiezel de Andrade Battaglin
Jeany Lucia da Silva Oliveira
José Renato Giacobbe Júnior
Fernanda Sartori Marques Vieira *(membro da comissão no exercício 2021)*

comite.compliance@emdec.com.br

CAMPINAS
2022

MANUAL DE CONFORMIDADE E AVALIAÇÃO DE RISCO

EMDEC

EMPRESA MUNICIPAL DE
DESENVOLVIMENTO DE CAMPINAS

CAMPINAS

2022

APRESENTAÇÃO

Vinicius Issa Lima Riverete

Diretor-Presidente da Emdec

A gestão dos recursos públicos e a condução dos processos da organização com responsabilidade e eficiência é um compromisso que assumimos diariamente com a população. Para nortear nossos colaboradores e garantir que os processos internos estejam alinhados às políticas públicas definidas e à legislação vigente, lançamos o presente Manual de Gestão de Riscos.

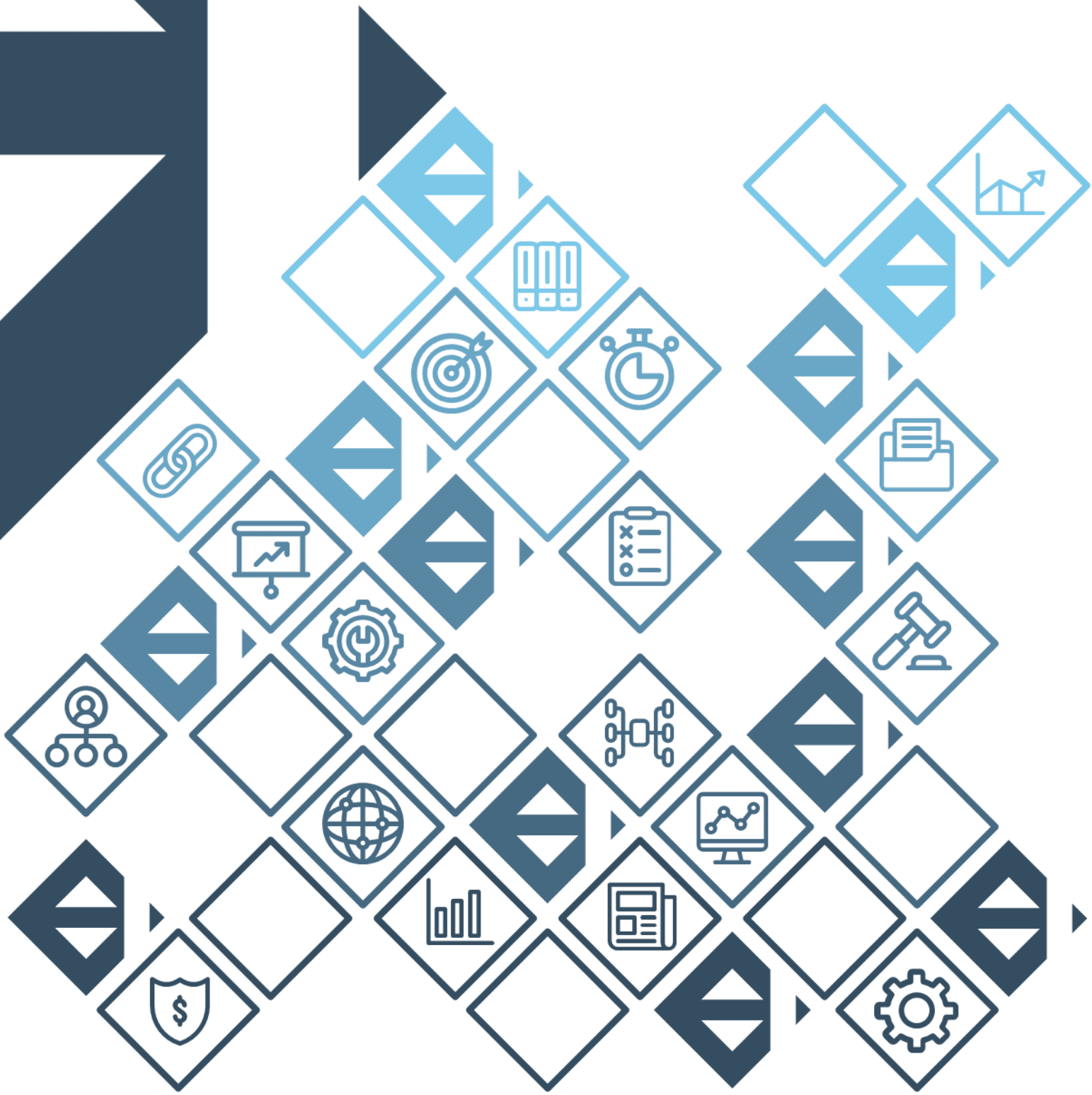
Trata-se de uma ferramenta de monitoramento para que nossa conduta, como servidores da população, seja sempre pautada pela ética, normas legais e lisura; e alinhada à missão e aos valores da Emdec.

Ao instituirmos uma metodologia para gestão de riscos e adotarmos boas práticas de governança corporativa, buscamos guiar os colaboradores na tomada de decisões estratégicas e no cumprimento de nossa missão institucional.

Que possamos buscar sempre a melhoria contínua e ajustar as rotas necessárias em favor de um desempenho mais eficiente. Tudo com o propósito do desenvolvimento de uma mobilidade urbana mais acessível, inclusiva, sustentável e, principalmente, mais humana.

SUMÁRIO

PARTE I
CONTEXTUALIZAÇÃO



1. INTRODUÇÃO

O Manual de Gestão de Riscos da EMDEC se presta a sintetizar as premissas e conceitos adotados para gestão de riscos da EMDEC, tornando-se um guia prático e objetivo para os administradores e gestores que atuarão no processo de análise de riscos.

Buscou-se, de forma resumida e com linguagem acessível, detalhar as etapas a serem seguidas pelos responsáveis por cada uma das áreas e/ou processos de trabalho, para maior compreensão e facilitação das ações durante o processo de avaliação de riscos.

Com o presente trabalho objetiva-se auxiliar os responsáveis por cada área/processo de trabalho para o maior controle e mitigação dos seus respectivos riscos, fomento da melhoria contínua dos processos e incorporação permanente da metodologia de gestão de riscos no cotidiano da EMDEC para criação, preservação e percepção de valores corporativos.

2. BASE LEGAL E NORMATIVA

A gestão de riscos da EMDEC possui seu principal eixo na Lei Federal nº 6.404/76 que dita as normas sobre as sociedades anônimas, como também na Lei Federal nº 13.303/2016 e Lei Anticorrupção - Lei Federal nº 12.846/2013.

O presente Manual de Gestão de Riscos, baseia-se nos seguintes instrumentos legais e normativos:

a) Estatuto Social Consolidado da EMDEC aprovado pela A.G.O.E. de 30/04/2021;
b) Regimento Interno da EMDEC;
c) Lei Municipal nº 4.092/1972 que cria o Fundo para o desenvolvimento de Campinas, transforma o escritório municipal de planejamento em Empresa Pública - Empresa Municipal De Desenvolvimento De Campinas - Emdec, institui o plano comunitário municipal, atribui à EMDEC competência para executá-lo e dá outras providências;
d) Decreto municipal nº 4.016/1972 que transforma a Empresa Pública criada pela Lei nº 4.092, de 11 de janeiro de 1972 e denomina Empresa Municipal De Desenvolvimento de Campinas - EMDEC em sociedade de economia mista;
e) Lei Municipal nº 10.248/1999 que dispõe sobre a reorganização da Estrutura Administrativa da Prefeitura Municipal de Campinas e dá outras providências;

f) Decreto nº 19.369/2016 - Regulamenta o estatuto jurídico das empresas públicas e de economia mista, da administração indireta do Município de Campinas;
g) Lei Municipal nº 11.263/2002 que dispõe sobre a organização dos Serviços de Transporte Público Coletivo de Passageiros no Município de Campinas e dá outras providências, e legislações regulamentadoras correlatas;
h) Código de Conduta e Integridade da EMDEC;
i) Regulamento de Licitações e Contratos da EMDEC;
j) Comunicados do Presidente, emitidos pela Presidência, que dispõe sobre a instituição de procedimentos e práticas a serem observadas na condução de matérias diversas;
k) ABNT NBR ISO 31000:2018, Gestão de riscos – Princípios e diretrizes;
l) Comunicado do Presidente nº 60/2020 – nomeação do Comitê de Conformidade e Gerenciamento de Riscos;
m) Política de Gestão de Riscos da EMDEC – aprovada na 201ª Reunião do Conselho de Administração.

3. Objetivos da Gestão de Riscos

A gestão de riscos busca o estabelecimento de regras e princípios para identificação, análise, tratamento, monitoramento e comunicação dos riscos inerentes às atividades da EMDEC, sendo um instrumento de controle essencial para promover a conformidade dos atos praticados.

4. Princípios da Gestão de Riscos

Conforme a Política de Gestão de Riscos da EMDEC, são os seguintes os princípios e premissas que regem a gestão de riscos na EMDEC:

a) **Estabelecer a gestão de Riscos como parte da cultura empresarial da EMDEC objetivando a geração de valor para a EMDEC**.

A EMDEC reconhece que a gestão integrada de riscos corporativos está diretamente relacionada ao crescimento sustentável, criação de valor e proteção do ambiente institucional, por permitir a identificação não só de ameaças, como também de oportunidades de negócio, além de apoiar a tomada de decisões.

b) Adotar boas práticas de governança corporativa

Buscar adotar as melhores práticas de governança corporativa quanto à gestão de riscos e às políticas e práticas antifraude e anticorrupção, com o intuito de aprimorar e manter a transparência e a qualidade das suas informações, divulgadas interna e externamente. Como, por exemplo, o cuidado com estabelecimento de regras sobre coleta, armazenamento, tratamento e compartilhamento de dados pessoais em atendimento à Lei Geral de Proteção de Dados.

c) Definir uma linguagem comum sobre riscos na EMDEC

A adoção de uma linguagem padrão de gestão de riscos na empresa é essencial ao processo, possibilitando um melhor entendimento entre as partes e um processo livre de interferências.

d) Utilizar padrões e metodologias reconhecidos pelo mercado

Com um modelo baseado em metodologias e padrões formalizados, reconhecidos pelo mercado e disseminados na empresa, a gestão integrada de riscos é capaz de se adequar a estratégias, iniciativas e estruturas organizacionais, além de atender às exigências setoriais e dos órgãos reguladores e fiscalizadores.

e) Integração dos Conselhos de Administração e Fiscal, Diretoria Executiva, Comitê de Conformidade e Gestão de Riscos "Compliance", Auditoria Interna, Comitê de Auditoria Estatutário e Controladoria Interna.

A integração dos atores de controle interno e da alta Administração da EMDEC são crucias para o alcance dos objetivos e metas traçadas pela instituição.

f) Estabelecer e manter a infraestrutura necessária para a gestão integrada de Riscos

O gerenciamento de riscos requer uma infraestrutura adequada e integrada de processos, pessoas e tecnologia, estabelecendo mecanismos de comunicação claros e objetivos.

g) Integrar a gestão de riscos aos processos organizacionais

A gestão integrada de riscos deve permear todas as práticas e processos organizacionais da EMDEC de forma a garantir a identificação de eventos de riscos inerentes a todas as suas áreas de negócio.

h) Analisar periodicamente a gestão de riscos na EMDEC.

O Comitê de Conformidade e Gestão de Riscos "Compliance" juntamente com a Auditoria Interna, deverá assegurar a eficácia do gerenciamento de riscos por meio de monitoramento e revisões frequentes, favorecendo o cumprimento de seus objetivos

5. DEFINIÇÕES E CONCEITOS

a) Apetite a riscos: grau de exposição a Riscos que a Companhia está disposta a aceitar para atingir seus objetivos e criar valor para seus acionistas, respeitando as partes interessadas.

b) Compliance: designação utilizada na prevenção e detecção de falta de conformidade com leis e regulamentações, que possa ser cometida pelos administradores, colaboradores e parceiros de negócios da Companhia.

c) Controles: políticas, normas, procedimentos, atividades e mecanismos desenvolvidos para assegurar que os objetivos de negócios sejam atingidos e que eventos indesejáveis sejam prevenidos ou detectados e corrigidos.

d) **Fraude**: quaisquer atos ilegais caracterizados por desonestidade, dissimulação ou quebra de confiança. Estes atos não implicam o uso de ameaça de violência ou de força física;

e) **Gestão de riscos**: atividades realizadas com a finalidade de identificar, classificar, formalizar, monitorar e/ou administrar os Riscos identificados. A Gestão de Riscos deve estar alinhada aos objetivos, estratégias e negócios da Companhia.

f) **Evento**: ocorrência ou alteração em um conjunto específico de circunstâncias. Um evento pode consistir em uma ou mais ocorrências, e pode ter várias causas. Também pode consistir em não ocorrência de alguma coisa.

g) **Plano(s) de ação**: definição das ações corretivas para reduzir a exposição aos Riscos residuais, a partir da identificação das deficiências ao longo do ciclo de avaliação do ambiente de controle/Riscos.

h) **Resposta(s) ao(s) risco(s**): decisão que será tomada após a identificação do Risco inerente ou avaliação do ambiente de controle dos Riscos residuais, com objetivo de promover discussões que assegurem a eficiência do ambiente de Controles internos da EMDEC.

i) **Key Risk Indicators (KRI's):** métricas que possibilitam a identificação do grau de Risco ao qual a organização está sujeita ou ao qual tem alta probabilidade de estar sujeita e que exceda o Apetite a Riscos. Funcionam como sinais de alerta, indicando as mudanças no nível de Risco da organização ou de seus negócios.

j) **Risco(s)**: ameaça de eventos ou ações que possam impactar o atingimento dos objetivos da Companhia. É inerente a qualquer atividade e pode afetar os ativos,

resultados, imagem/reputação, aspectos legais, regulatórios, socioambientais ou continuidade dos negócios.

k) **Risco inerente**: risco a que uma organização está exposta sem considerar quaisquer ações gerenciais que possam reduzir a probabilidade dos riscos ou seu impacto;

l) **Risco residual**: risco a que uma organização está exposta após a implementação de ações gerenciais para o tratamento do risco;

m) **Tolerância ao Risco**: é o nível de variação aceitável quanto à realização dos objetivos;

n) **Tratamento de riscos**: processo de estipular uma resposta a risco;

o) **Responsável pelo controle**: Consiste na identificação do responsável por alertar e gerenciar determinado controle, que obrigatoriamente, deverá estar alinhado com todos os assuntos relacionados à Gestão de Riscos sob sua responsabilidade

6. METODOLOGIA

A norma ABNT NBR ISO 31000:2018 estabelece um roteiro para que seja feita a identificação, análise, avaliação e tratamento dos riscos identificados, selecionando a opção de tratamento que melhor se adequar às características da empresa, com base nos benefícios, custos, vantagens e desvantagens de sua implementação. Destaca-se abaixo, a ilustração de como é realizado o processo de gestão de riscos, com base na ISO 31000-2018 que é "parte integrante da gestão e

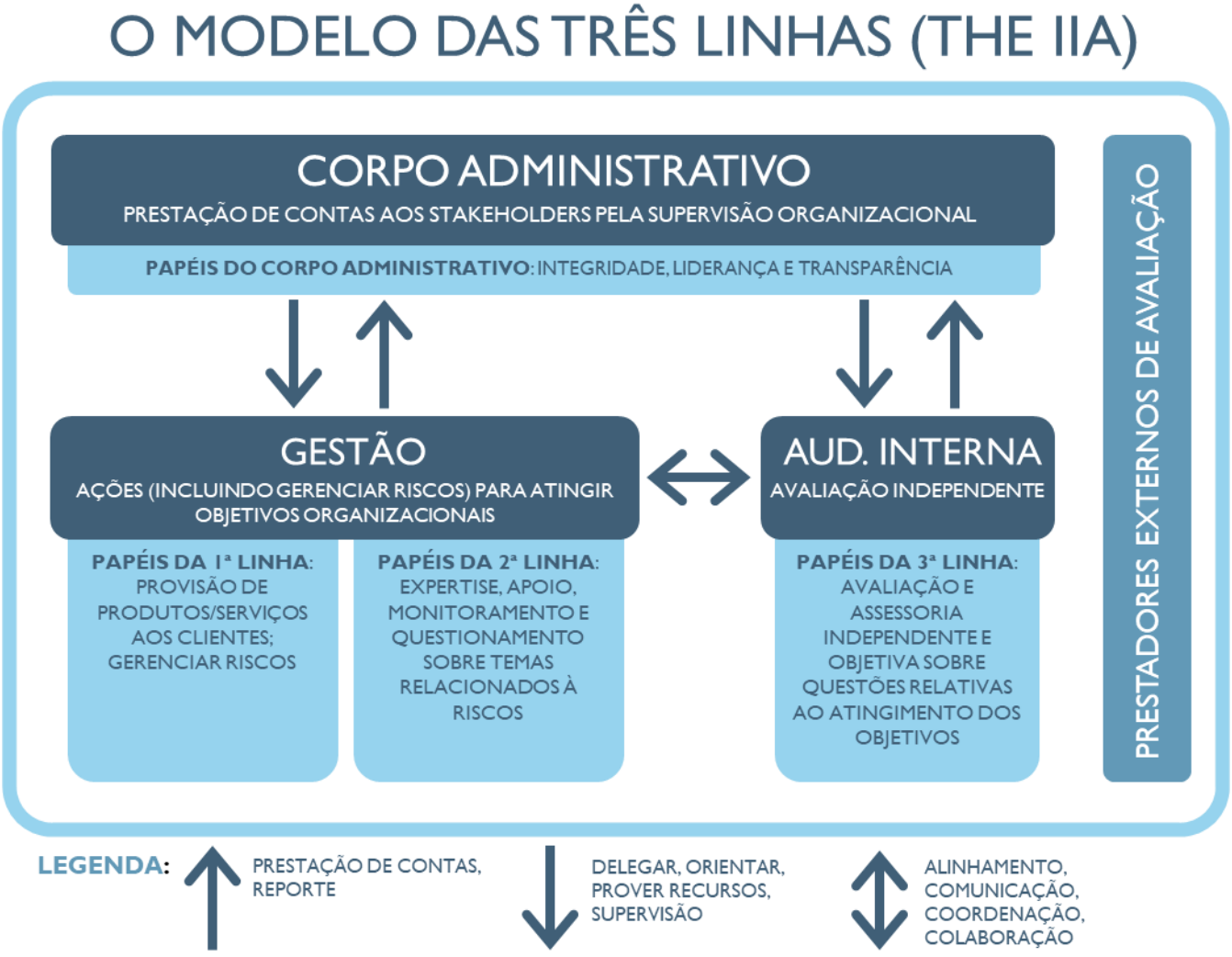
da tomada de decisão, e seja integrado na estrutura, operações e processos da organização[1]":

Com o diagnóstico e plano de ação idealizado, será proposto pelo Comitê de Conformidade e Gerenciamento de Riscos ao Conselho de Administração da EMDEC que terá por responsabilidade aprovar ou não a implementação proposta, realizando os ajustes que forem necessários.

A Comissão de Conformidade e Gestão de Riscos adotará o "Modelo de Três Linhas" (anteriormente conhecido como "Modelo de Três Linhas de Defesa") desenvolvido pelo The Institute of Internal Auditors (The IIA)

[1] ABNT NBR 31000-2018, p. 9

e mundialmente adotado por empresas e governos. O modelo apresenta uma abordagem baseada em princípios adaptáveis aos objetivos da Organização, oferece clareza nas atribuições e relações entre as partes envolvidas e possibilita a implantação de medidas para garantir que a atividade e objetivos estejam alinhados com as normas de conformidade estabelecidas.



Adaptando o modelo à estrutura organizacional da EMDEC, os processos proprietários de riscos juntamente com a alta Administração devem atuar como primeira linha de defesa, realizando o gerenciamento dos riscos específicos de suas atividades.

A comissão de Conformidade e Gestão de Riscos atua como segunda linha de defesa, desenvolvendo e monitorando os controles referentes à primeira linha e

sendo responsável por fornecer orientações e treinamentos e auxiliar no desenvolvimento de processos e controles para gerenciamento de riscos.

Na terceira linha encontra-se a Auditoria Interna e Comitê de Auditoria Estatutário, responsável pela avaliação geral, de forma independente e objetiva, sobre a adequação dos controles internos e efetividade da gestão de riscos.

7. Atores da Gestão de Risco

GESTORES DE RISCOS

Todos aqueles que são responsáveis pelo gerenciamento de um processo de trabalho ou um projeto é considerado um "Gestor de Riscos". A ele é atribuída a competência de informar o início do processo de avaliação de riscos, com apoio dos demais atores envolvidos da Gestão de Riscos e dos servidores e colaboradores envolvidos nas atividades sob sua gestão.

Os Gestores de Riscos também são responsáveis pela classificação dos riscos envolvidos nos seus processos de trabalho. Para os casos no qual o nível de risco residual esteja acima do nível de risco tolerável, ele deverá estabelecer um plano de tratamento, a fim de reduzir os riscos a níveis aceitáveis.

COMITÊ DE COMPLIANCE E GESTÃO DE RISCOS

O Comitê tem por objetivo auxiliar as tomadas de decisões do Gestores de Riscos, assim minimizando os riscos operacionais, legais, financeiros, orçamentários e de imagem da EMDEC.

Terão também o papel de "facilitadores" desse processo, promovendo e acompanhando todas as fases definidas nesse manual e atuando para a consolidação e divulgação das informações levantadas durante a execução do trabalho.

AUDITORIA INTERNA

A Auditoria Interna tem como objetivo avaliar e prestar ajuda à alta Administração proporcionando análises, recomendações e comentários objetivos acerca das atividades examinadas.

COMITÊ DE AUDITORIA

Órgão de suporte ao Conselho de Administração no que se refere ao exercício de suas funções de auditoria e de fiscalização sobre a qualidade das demonstrações contábeis e efetividade dos sistemas de controle interno e de auditorias interna e independente

CONTROLE INTERNO

Atua nas atividades de controle e cumprimento das metas traçadas pelas áreas, buscando eficiência dos resultados, orientando e estruturando os processos.

CONSELHO DE ADMINISTRAÇÃO

Implementar e supervisionar a gestão de riscos e controle interno visando a mitigação dos principais riscos elencados, sobretudo àqueles relacionados à ocorrência de corrupção e fraude e integridade de informações contábeis e financeiras.

PARTE II

PROCESSO DE GESTÃO DE RISCOS

8. Processo de Gestão de Riscos

8.1. Etapas Preliminares

Inicialmente, é necessário que a **Cadeia de Valor** e os **Processos de Trabalho** estejam mapeados, pois serão a base para o gerenciamento de riscos.

Cadeia de Valor é o modelo (representação gráfica) que permite a visão do sequenciamento lógico dos processos organizacionais, enquanto os Processos de Trabalho descrevem detalhadamente as atividades, interações, processamento, entradas e saídas de cada processo.

Ambas são essenciais para que a aplicação da metodologia de gerenciamento de integridade, riscos e controles internos da gestão tenha maior efetividade.

Por se tratar de um processo complexo e inédito na EMDEC, também se sugere a priorização dos processos mais suscetíveis a eventos de risco. Nesse contexto, pode ser utilizado o **Método de Priorização de Processos** (Ministério do Planejamento, Desenvolvimento e Gestão) para classificação dos processos em função de seu grau de exposição, analisados com enfoque quantitativo e qualitativo.

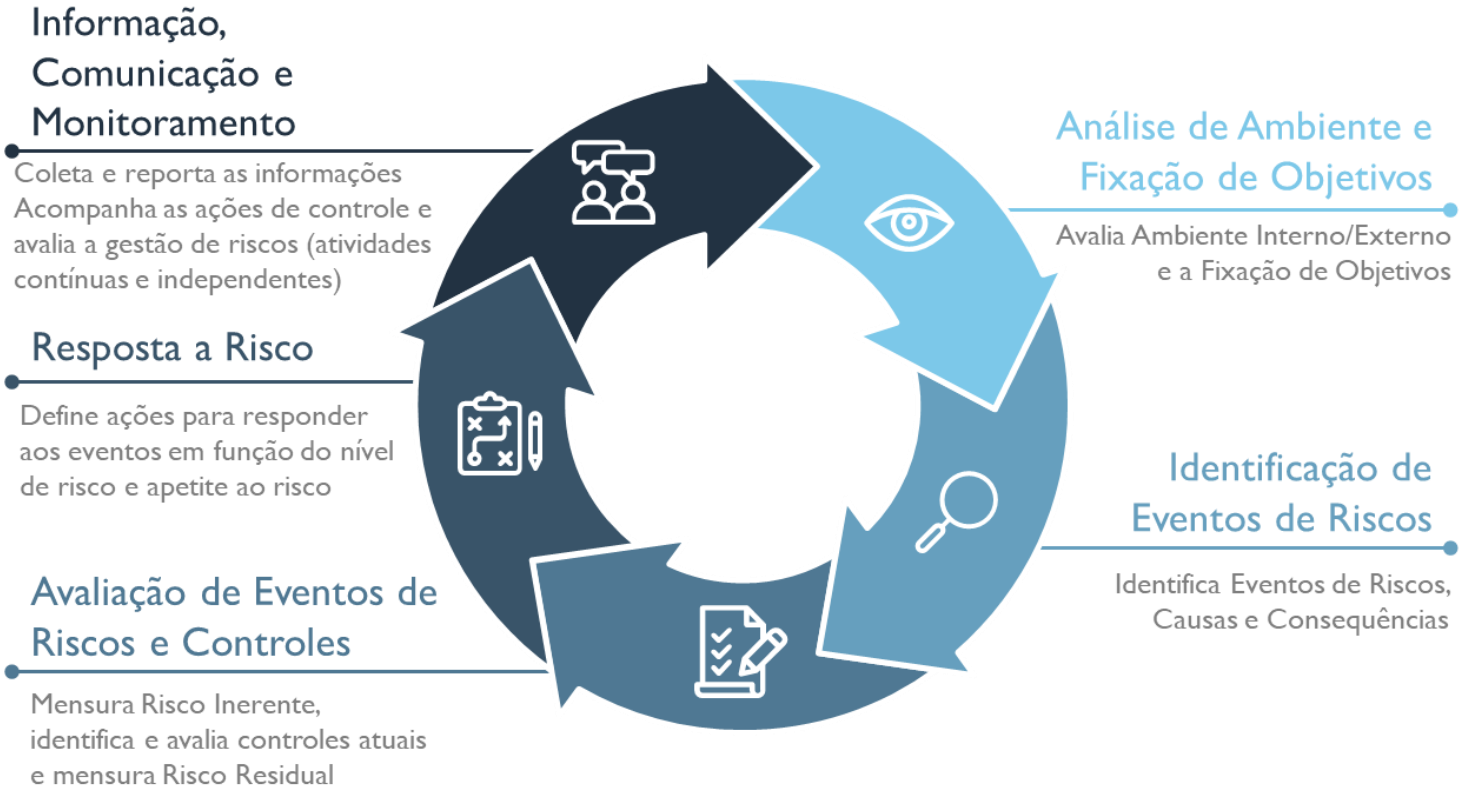
Assim, de maneira resumida, o processo se inicia com a avaliação da Cadeia de Valor e dos Processos de Trabalho, a classificação dos processos através do Método de Priorização, a definição da equipe responsável e identificação das partes intervenientes/interessadas no processo.

8.2. Planilha Documentadora

Deste ponto do documento em diante, será frequente a menção à **Planilha Documentadora**. Trata-se de um arquivo do MS Excel, com campos disponíveis para preenchimento e fórmulas que auxiliarão na identificação, mensuração e organização dos eventos de riscos e seus controles. Seu preenchimento deve ser realizado pelas áreas proprietárias dos riscos.

8.3. Etapas do Gerenciamento de Riscos

A metodologia de gestão de riscos adotada, baseada sobretudo no COSO ERM, é dividida em 5 etapas e correspondem às fases que devem ser percorridas para a avaliação de riscos de cada processo.



8.3.1. Análise de Ambiente e Fixação de Objetivos

A etapa inicial do processo de Gestão de Riscos consiste na coleta de informações referentes ao Ambiente em que o processo está inserido e a Fixação de Objetivos.

A **Análise do Ambiente** inclui as ferramentas de gestão e controles existentes, políticas, estrutura de governança, valores éticos, integridade, delegação de autoridade e competências e práticas de recursos humanos.

A **Fixação de Objetivos** é fundamental para a Gestão de Riscos, pois os objetivos devem estar previamente estabelecidos para que a Administração identifique as situações em potencial que possam afetar sua realização e deve verificar se os objetivos de todos os processos da organização estão alinhados à Missão, Visão e Valores, estejam claramente definidos, documentados e comunicados aos colaboradores envolvidos

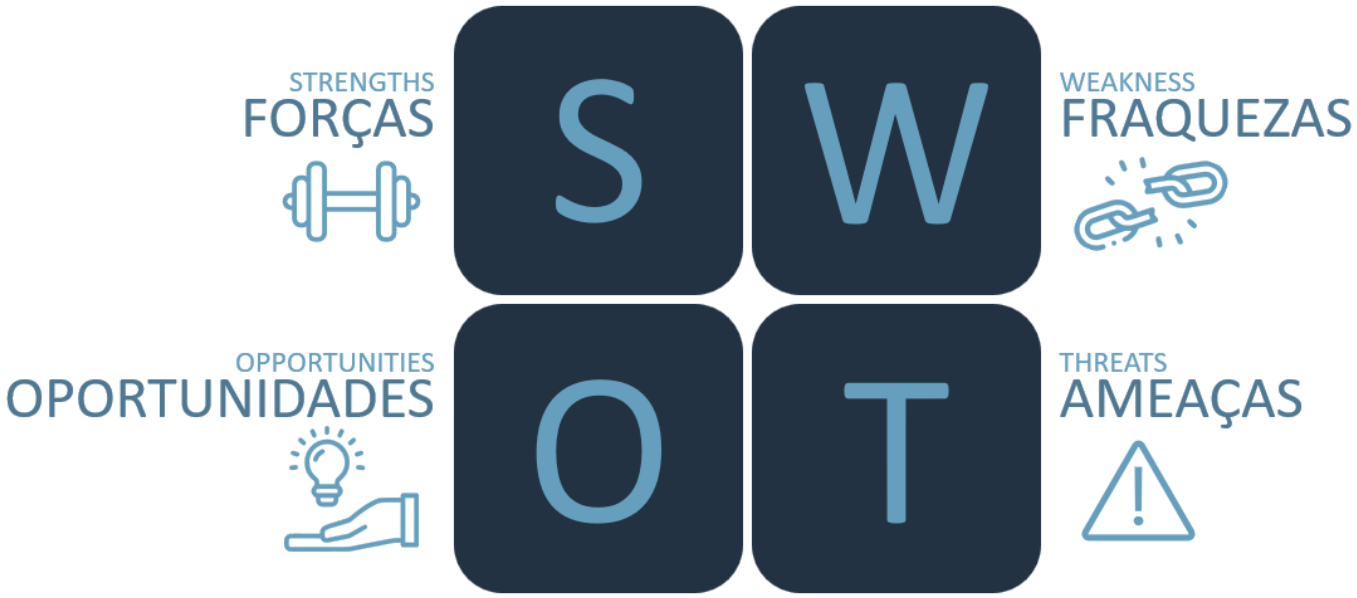
Esta etapa não tem por objetivo mapear ou redesenhar o processo de trabalho, mas sim conhecer seus objetivos e fontes de risco presentes em suas atividades. Eventuais propostas de mudanças poderão ser oportunamente discutidas em etapas subsequentes.

Para simplificar a obtenção e visualização de informações que facilitem a identificação de eventos de risco e permitam escolher as ações mais adequadas para assegurar o alcance dos objetivos do processo sugere-se a utilização da ferramenta Análise de SWOT.

A análise **SWOT** (Strengths, Weaknesses, Opportunities e Threats ou Forças, Fraquezas, Oportunidades e Ameaças, em tradução para o português), é o método de análise de cenários ou ambientes e permite uma identificação assertiva dos fatores que influenciam seu funcionamento.

A análise SWOT de um processo ou macroprocesso pode ser dividida em duas partes:

- Ambiente interno, onde serão identificados os pontos fortes e as fraquezas de uma empresa, macroprocesso ou processo;
- Análise do ambiente externo, onde estão as ameaças (questões impostas por forças externas, não passíveis de controle, que podem prejudicar o processo), e as oportunidades (fatores externos que podem beneficiar o processo).



PREENCHIMENTO DA PLANILHA

Aba "Ambiente e Fixação de Objetivos"

- *Leis e Regulamentos: listar as leis, regulamentos e normas que afetam ou influenciam o macroprocesso/processo. Essas informações são importantes para verificar se há riscos e descumprimento de leis, regulamentos e normas, bem como para auxiliar na adoção de ações de controle.*
- *Sistemas: listar os sistemas e ferramentas (planilhas, formulários, checklists) utilizadas pelo o processo. Essas informações são importantes para verificar se os controles são manuais ou eletrônicos.*

8.3.2. IDENTIFICAÇÃO DE EVENTOS DE RISCO

Com os resultados da análise do Ambiente e fixação dos Objetivos, é possível iniciar a etapa de Identificação de eventos de risco, com a finalidade de registrar eventos que podem comprometer a execução de um ou vários objetivos do processo, suas causas e consequências. A identificação desses eventos permite planejar a forma de tratamento adequada e a melhor resposta para o risco.

EVENTO: situações potenciais (que ainda não ocorreram) que podem causar impacto na consecução dos objetivos da organização/macroprocesso/processo caso ocorram. Esse impacto pode ser positivo (oportunidade) ou negativo (riscos). Este manual tratará apenas dos eventos negativos.

É importante destacar que eventos de risco devem ser considerados em seu contexto, nunca isoladamente.

CAUSA: Condição que dá origem à possibilidade de um evento ocorrer; podem ter origem no ambiente interno ou externo.

CAUSA = FONTE DE RISCO + VULNERABILIDADE

EVENTO DE RISCO: incidente decorrente de erro, falha, deficiência ou inadequação de processos que resulta em perdas ou impacto.

EVENTO DE RISCO = IRREGULARIDADE + INCIDENTE

EFEITO / CONSEQUÊNCIA: resultado de um evento de risco sobre os objetivos do processo.

EFEITO = IMPACTO EM OBJETIVO + PERDA

Baseado nos conceitos acima podemos afirmar que:

UMA OU MAIS CAUSAS GERAM UM EVENTO DE RISCO;

UM EVENTO DE RISCO GERA UMA CONSEQUÊNCIA;

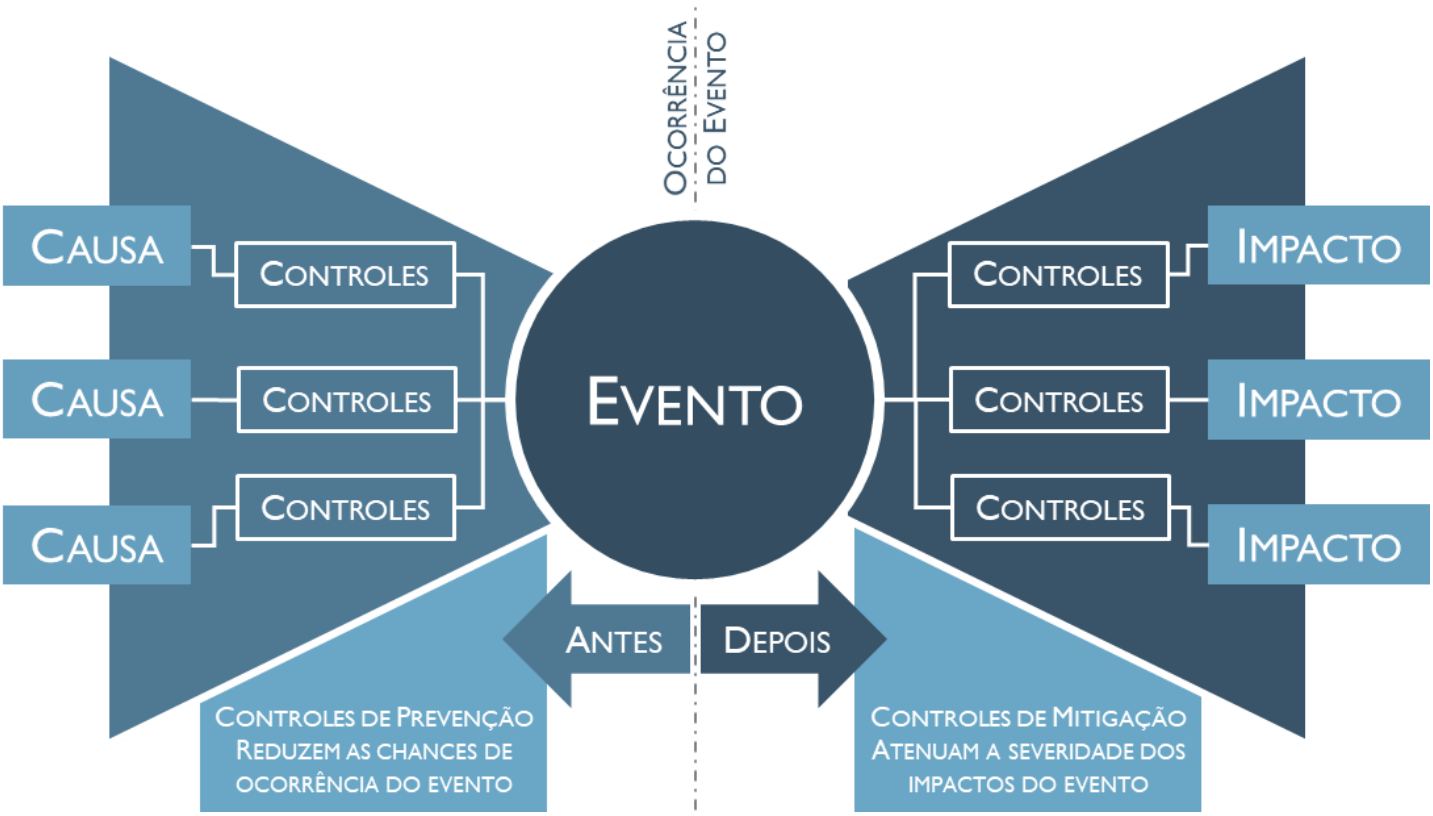
UMA CAUSA SOZINHA NÃO GERA UMA CONSEQUÊNCIA;

UMA CAUSA IDENTIFICADA PODE GERAR UM EVENTO DE RISCO E ESSE EVENTO, SE CONCRETIZADO, PODE GERAR UMA CONSEQUÊNCIA.

A identificação dos riscos requer a participação de colaboradores com profundo conhecimento do processo e que, além disso, possuam ampla visão dos serviços da organização em seus diferentes níveis.

Os métodos para a identificação de risco são variados e devem se adaptar ao grupo de trabalho. Algumas das técnicas utilizadas são: questionários e checklist; workshop e brainstorming; inspeções e auditorias, fluxogramas, diagrama de causa e efeito etc.

Uma ferramenta bastante utilizada nesse tipo de análise é o diagrama **Bow Tie**. Considerado uma evolução dos diagramas de causa e efeito, ele permite uma visão geral e bastante clara da inter-relação entre causas e consequências tendo como ponto central o evento de risco. Seu nome provém da semelhança com uma gravata borboleta (bow tie em inglês).



Nesta etapa devem ser levantados o máximo possível de eventos de risco, sem um julgamento aprofundado sobre a probabilidade e o impacto associados ao risco. Porém deve-se evitar os **"CISNES NEGROS"**, eventos de impacto devastador, porém com probabilidades baixíssimas (como a queda de um meteoro, por exemplo).

Um erro bastante frequente nessa etapa é a identificação de uma causa ou efeito como um evento. Uma ferramenta para a correta identificação de um evento de risco é sua aplicação na sentença abaixo:

Devido a [CAUSA], poderá ocorrer [EVENTO DE RISCO], o que poderá levar à [EFEITO/CONSEQUÊNCIA] impactando no [OBJETIVO DO PROCESSO].

8.3.2.1. CAUSAS

Conforme já visto, uma causa é uma fonte (parte integrante do processo) associada à uma vulnerabilidade (requisito não atendido). As causas de eventos de risco variam enormemente entre os diversos processos da organização. Outrossim, a tabela abaixo apresenta algumas causas, associando fontes com possíveis vulnerabilidades:

FONTE	VULNERABILIDADE
PROCESSOS	Ausência de manual ou instruções formalizadas
	Fluxo de processos mal concebidos ou desatualizados
	Ausência de padrões mínimos de execução
	Ausência de ferramenta de análise e melhoria contínua do processo
	Falha ou ausência de metodologia que auxilie no mapeamento do processo
	Ausência de segregação de funções
	Recebimento de Insumos ou informações em descompasso com o tempo de execução do processo
	Erros ou falhas de informação que impactem no processo
	Descumprimento de obrigação legal ou regulatória
	Falta de divulgação da legislação e normas aplicadas ao processo
	Descumprimento de prazos legais ou judiciais

FONTE	VULNERABILIDADE
PESSOAS	Número insuficiente de funcionários
	Capacitação inadequada para execução do processo
	Concentração de conhecimentos afetando a execução e continuidade do processo
	Falha na disseminação de conhecimentos
	Alta rotatividade (*turnover*)
	Comportamentos antiéticos nas atividades e relacionamentos interpessoais
	Falta de comprometimento, atenção ou zelo na execução do processo
	Falta de motivação ou perfil adequado para as atividades desenvolvidas no processo
	Parcialidade e/ou descumprimentos de leis e normas reguladoras
	Quebras de sigilo e confidencialidade
	Resistência em aceitar alterações nas condições e ferramentas de trabalho
INFRAESTRUTURA ORGANIZACIONAL	Deficiências nos fluxos de informação e comunicação
	Desconhecimento dos objetivos do processo e responsabilidades individuais
	Centralização de responsabilidades
	Delegações exorbitantes
	Recursos insuficientes para execução do processo
	Resistência em promover alterações nos processos de trabalho
INFRAESTRUTURA FÍSICA	Localização Inadequada
	Instalações ou layout inadequados
	Falha ou falta de segurança no ambiente de trabalho
	Inexistência de controles de acesso físico
AMBIENTE TECNOLÓGICO	Ausência de estrutura de perfis de acesso aos sistemas para execução do processo
	Ausência de *logon* próprio na rede institucional
	Falha ou falta de meios seguros de acesso aos sistemas
	Falha ou inexistência de registros de transações críticas

FONTE	VULNERABILIDADE
AMBIENTE TECNOLÓGICO	Utilização de sistemas e equipamentos obsoletos e/ou sem integração
	Informações e dados armazenados em diretórios não protegidos e sem controle de acesso
	Ausência de backup de arquivos, planilhas e bancos de dados essenciais à execução do processo
	Sobrecarga de sistemas de processamento de dados
	Falhas de hardware, faltas de backup e de legalização do software
	Instabilidade nos sistemas operacionais que afeta a execução do processo
	Inexistência de investimentos em pesquisa e desenvolvimento
EVENTOS EXTERNOS	Ações humanas intencionais para lesar o órgão como roubos, furtos, falsificações, atos de vandalismo e fraudes externas
	Alterações no ambiente econômico, político e social
	Alterações inesperadas na legislação ou marcos regulatórios
	Indisponibilidade de recursos necessários
	Falhas ou indisponibilidade de serviços públicos que afetem a execução do processo
	Desastres naturais

Eventos externos também são considerados fontes de risco, porém, via de regra, não é possível gerenciar a situação para reduzir sua probabilidade.

8.3.2.2. CATEGORIA DO RISCO

Não existe consenso na literatura sobre a categorização de riscos, assim será considerada neste manual a classificação adotada pelo Comitê Técnico de Riscos do Ministério do Planejamento, Desenvolvimento e Gestão, dividindo os eventos de risco em sete categorias:

ESTRATÉGICO: eventos que possam impactar na missão, nas metas ou nos objetivos estratégicos do macroprocesso/processo, caso venham ocorrer.

OPERACIONAL: eventos que podem comprometer as atividades do processo ou divisão, normalmente associados a falhas, deficiência ou inadequação de processos internos, pessoas, infraestrutura e sistemas,

afetando o esforço da gestão quanto à eficácia e eficiência dos processos organizacionais.

ORÇAMENTÁRIO: eventos que podem comprometer a capacidade da EMDEC de contar com os recursos orçamentários necessários à realização de suas atividades, ou eventos que possam comprometer a própria execução orçamentária.

REPUTAÇÃO: eventos que podem comprometer a confiança da sociedade em relação à capacidade da EMDEC em cumprir sua missão institucional; interferem diretamente na imagem da empresa.

INTEGRIDADE: eventos que podem afetar a probidade da gestão dos recursos públicos e das atividades da organização, causados pela falta de honestidade e desvios éticos.

FISCAL: eventos que podem afetar negativamente afetar as contas da empresa, comprometendo o alcance dos resultados fiscais estabelecidos como metas e objetivos.

CONFORMIDADE: eventos que podem afetar o cumprimento de leis e regulamentos aplicáveis.

8.3.2.3. NATUREZA DO RISCO

Além desta classificação, os riscos serão agrupados conforme sua Natureza, diretamente relacionada à categoria de risco escolhida. Se a categoria de risco for fiscal ou orçamentária, a natureza do risco será **ORÇAMENTÁRIO-FINANCEIRA**. Se a categoria do risco for estratégica, operacional, reputacional, integridade ou conformidade, a natureza do risco será **NÃO ORÇAMENTÁRIO-FINANCEIRA**.

PREENCHIMENTO DA PLANILHA

Aba "Mapa de Riscos"

- *Subprocesso/atividade: indica o nível em que se realizará a identificação dos eventos de riscos do macroprocesso/processo escolhido para a análise.*
- *Evento de Risco: descreve os eventos de riscos identificados, a partir da utilização da técnica escolhida para essa atividade.*
- *Causas: descreve as possíveis causas, condições que dão origem à possibilidade de um evento ocorrer, também chamadas de fatores de riscos e podem ter origem no ambiente interno e externo.*
- *Efeitos/consequências: descreve os/as possíveis efeitos/consequências de um possível evento de risco sobre os objetivos do processo.*
- *Categoria do Risco: escolher no menu suspenso a categoria de risco.*
- *Natureza do Risco: preenchido automaticamente em função da Categoria de Risco*

8.3.3. AVALIAÇÃO DO RISCO

Nesta etapa, os riscos identificados serão avaliados quanto seu impacto e probabilidade considerando suas causas e consequências.

A avaliação deve ser feita por meio de análises quantitativas e qualitativas e quanto à condição de Inerente e Residual:

RISCO INERENTE: desconsidera a aplicação de nenhum controle gerencial que possa reduzir a probabilidade ou impacto.

RISCO RESIDUAL: risco remanescente após a implementação dos controles gerenciais existentes incluindo a avaliação do desenho e execução desses controles.

Entende-se por **CONTROLES INTERNOS** todas as regras, procedimentos, diretrizes, protocolos, rotinas de sistemas informatizados, conferências e trâmites de documentos e informações, entre outros, operacionalizados de forma integrada

pela direção e corpo de servidores da organização, com o objetivo de enfrentamento a riscos e alcance de razoável segurança para a consecução da missão da empresa.

A realização desta etapa ocorres em três subetapas, todas utilizando a **PLANILHA DOCUMENTADORA**.

8.3.3.1. CÁLCULO DO RISCO INERENTE

O Risco inerente será calculado de acordo com a probabilidade e impacto de sua ocorrência, observando as matrizes abaixo:

	Impacto - Fatores para Análise						
	Estratégico-Operacional					Econômico/ Financeiro	Peso
	Esforço de Gestão	Regulação	Reputação	Negócios/ Serviços à Sociedade	Intervenção Hierárquica	Orçamentário	
	15%	17%	12%	18%	13%	25%	100%
Orientações para atribuição de pesos	Evento com potencial para levar o negócio ou serviço ao colapso	Determina interrupção das atividades	Com destaque na mídia nacional e internacional, podendo atingir os objetivos estratégicos e a missão	Prejudica o alcance da missão da EMDEC	Exigiria a intervenção do Presidente	> = 25%	5 CATASTRÓFICO
	Evento crítico, mas que com a devida gestão pode ser suportado	Determina ações de caráter pecuniários (multas)	Com algum destaque na mídia nacional, provocando exposição significativa	Prejudica o alcance da missão da Diretoria	Exigiria a intervenção do Diretor	> = 10% < 25%	4 GRANDE
	Evento significativo que pode ser gerenciado em circunstâncias normais	Determina ações de caráter corretivo	Pode chegar à mídia provocando a exposição por um curto período de tempo	Prejudica o alcance dos objetivos estratégicos	Exigiria a intervenção do Gerente da Divisão	> = 3% < 10%	3 MODERADO
	Evento cujas consequências podem ser absorvidas, mas carecem de esforço da gestão para minimizar o impacto	Determina ações de caráter orientativo	Tende a limitar-se às partes envolvidas	Prejudica o alcance das metas do processo	Exigiria a intervenção do Líder do Processo	> = 1% < 3%	2 PEQUENO
	Evento cujo impacto pode ser absorvido por meio de atividades normais	Pouco ou nenhum impacto	Impacto apenas interno / sem impacto	Pouco ou nenhum impacto nas metas	Seria alcançada no funcionamento normal da atividade	< 1%	1 INSIGNIFICANTE

Probabilidade					
Aspectos Avaliativos	Evento pode ocorrer apenas em circunstâncias excepcionais	Evento pode ocorrer em algum momento	Evento deve ocorrer em algum momento	Evento provavelmente ocorra na maioria das circunstâncias	Evento esperado que ocorra na maioria das circunstâncias
Frequência Observada/ Esperada	MUITO BAIXA (< 10%)	BAIXA (>=10% <= 30%)	MÉDIA (>=30% <= 50%)	ALTA (>=50% <= 90%)	MUITO ALTA (>90%)
Peso	1	2	3	4	5

PREENCHIMENTO DA PLANILHA

Aba "Cálculo do Risco Inerente"

- *Para cada evento identificado atribuir o peso referente ao impacto de sua ocorrência para cada um dos seis aspectos avaliados (Esforço de Gestão, Regulação, Reputação, Negócios/Serviços à Sociedade, Intervenção Hierárquica e Orçamentário) na respectiva coluna.*
- *Na coluna "Frequência Prevista", incluir o peso referente à probabilidade de ocorrência do evento.*
- *As células só aceitam a digitação de valores numéricos entre um e cinco.*
- *O nível de riscos será calculado automaticamente e aparecerá nas colunas "Nível de Risco" ("Impacto x Probabilidade" e "Descrição) e na aba "Mapa de Riscos"*

8.3.3.2. AVALIAÇÃO DO CONTROLE

Após a mensuração do Risco inerente é necessário identificar e avaliar os controles atribuídos aos riscos identificados quanto ao seu desenho e operação, conforme apresentado abaixo:

AVALIAÇÃO DO DESENHO DO CONTROLE

1. Não há procedimento de controle;
2. Há procedimentos de controles, mas não são adequados e nem estão formalizados;
3. Há procedimentos de controles formalizados, mas não estão adequados (insuficientes);
4. Há procedimentos de controles adequados (suficientes), mas não estão formalizados;
5. Há procedimentos de controles adequados (suficientes) e formalizados.

AVALIAÇÃO DA OPERAÇÃO DO CONTROLE

1. Não há procedimento de controle;
2. Há procedimentos de controle, mas não são executados;
3. Os procedimentos de controle estão sendo parcialmente executados;
4. Os procedimentos de controle são executados, mas sem evidência de sua realização;
5. Procedimentos de controle são executados e com evidência de sua realização.

PREENCHIMENTO DA PLANILHA

Aba "Mapa de Riscos"

- *Os controles existentes deverão ser listados.*
- *Proceder com a Avaliação do Desenho e Operação dos Controles existentes utilizando os respectivos menus suspensos.*

8.3.3.3. CÁLCULO DO RISCO RESIDUAL

O Risco residual será calculado da mesma forma que o **RISCO INERENTE**, porém nesta etapa, serão considerados os controles identificados e o resultado da avaliação destes controles quanto ao desenho e operação.

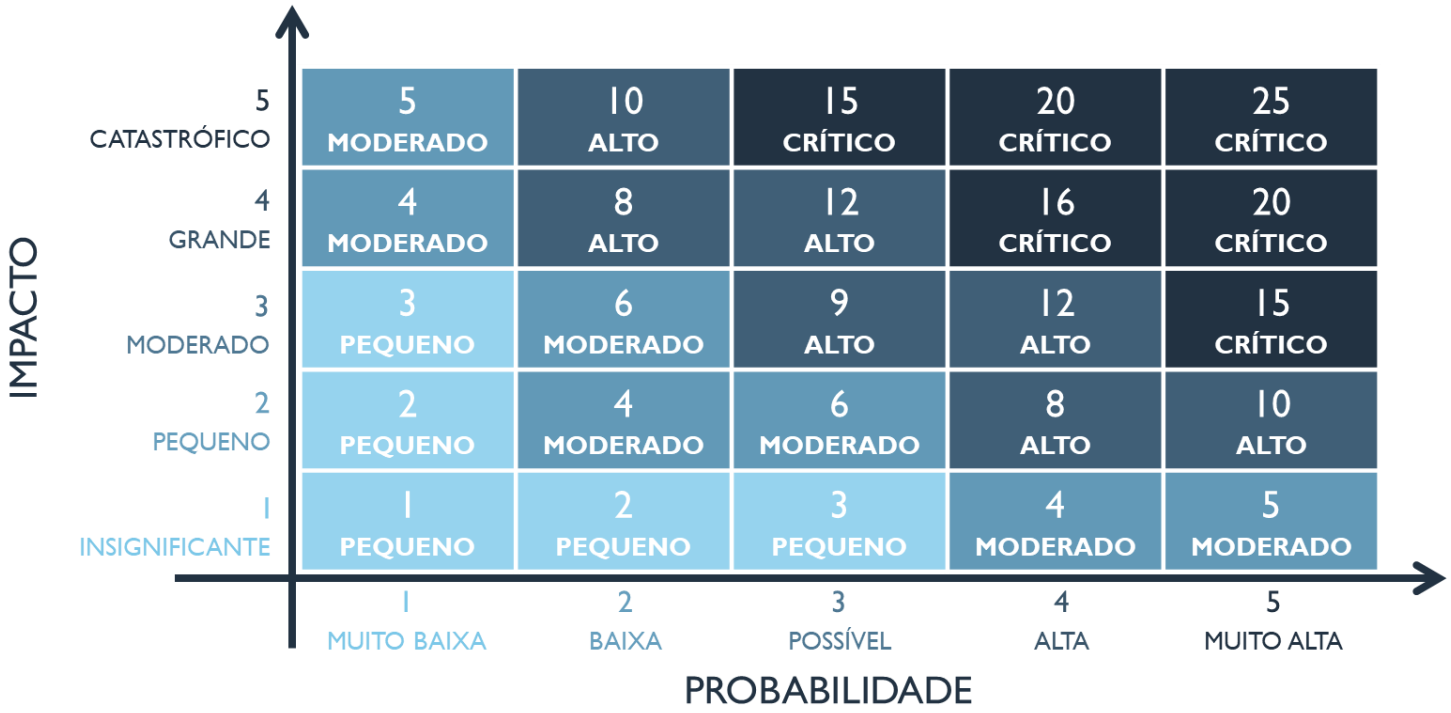
PREENCHIMENTO DA PLANILHA

Aba "Cálculo do Risco Residual"

- *Como realizado na etapa anterior para os Riscos Inerentes, deverão ser atribuídos pesos para o Impacto e Probabilidade de ocorrência dos eventos, porém considerando a efetividade dos controle existentes*
- *As células só aceitam a digitação de valores numéricos entre um e cinco.*
- *O nível de riscos será calculado automaticamente e aparecerá nas colunas "Nível de Risco" ("Impacto x Probabilidade" e "Descrição) e na aba "Mapa de Riscos".*

8.3.3.4. MATRIZ IMPACTO X PROBABILIDADE

Ao final dessas três etapas a Planilha Documentadora terá efetuado o cálculo do nível de risco para evento identificado e classificado o risco conforme a Matriz de Impacto x Probabilidade



8.3.4. Resposta ao Risco

Após a definição do Risco Residual, e considerando a Política de Gestão de Riscos da organização e seu apetite ao risco, deverá ser verificada a estratégia adotada para responder ao evento de risco identificado. A resposta deve considerar também a relação custo-benefício e se o efeito da resposta afeta a probabilidade, impacto, ou ambos e designar os responsáveis pela resposta.

A tabela abaixo sugere as **Respostas ao Risco** e **Ações de Controle**, em função do Risco Residual determinado:

Nível de Risco	Descrição do Nível de Risco	Parâmetro de Análise para Adoção de Resposta	Tipo de Resposta	Ação de Controle
Risco Crítico	Indica que nenhuma opção de resposta foi identificada para reduzir a probabilidade e o impacto a nível aceitável	Custo desproporcional, capacidade limitada diante do risco identificado	**Evitar**	Promover ações que evitem/eliminem as causas e/ou efeitos
Risco Alto	Indica que o risco residual será reduzido a um nível compatível com a tolerância a riscos	Nem todos os riscos podem ser transferidos. Exemplo: Risco de Imagem, Risco de Reputação	**Reduzir**	Adotar medidas para reduzir a probabilidade ou impacto dos riscos, ou ambos
Risco Moderado	Indica que o risco residual será reduzido a um nível compatível com a tolerância a riscos	Reduzir probabilidade ou impacto, ou ambos	**Compartilhar ou Transferir**	Reduzir a probabilidade ou impacto pela transferência ou compartilhamento de uma parte do risco. (seguro, transações de hedge ou terceirização da atividade).
Risco Pequeno	Indica que o risco inerente já está dentro da tolerância a risco	Verificar a possibilidade de retirar controles considerados desnecessários	**Aceitar**	Conviver com o evento de risco mantendo práticas e procedimentos existentes

8.3.4.1. Atividades de Controle

Atividades de Controle são políticas e procedimentos estabelecidos para reduzir os riscos que o Macroprocesso/Processo tenha optado por responder e devem estar distribuídas em todos os níveis e funções dos processos proprietários de riscos.

Uma mesma atividade de controle pode abranger vários riscos, da mesma forma que um único risco pode demandar diversas atividades de controle.

As Atividade de Controle incluem os controles internos e a preparação prévia de planos de contingência e/ou continuidade no caso da materialização de determinados eventos de risco.

8.3.4.1.1. CLASSIFICAÇÃO DOS CONTROLES

No **PLANO DE AÇÃO**, os Controles adotados deverão ser classificados quanto ao seu **TIPO** e seu **OBJETIVO.**

TIPO DE CONTROLE

1. PREVENTIVO: tem o objetivo de prevenir falhas, evitando a ocorrência de eventos ou resultados indesejados (atuação na causa);

2. CORRETIVO: tem o objetivo de detectar falhas já ocorridas e anular ou atenuar seus efeitos (atuação na consequência);

3. COMPENSATÓRIO: tem o objetivo de mitigar os eventos de risco temporariamente, até a implementação de um controle definitivo. Utilizado apenas em situações em que a ação ideal não pode ser implementada ou não pode ser implantada no curto prazo em função de sua complexidade, alto custo ou alto nível de interveniência.

OBJETIVO

1. IMPLEMENTAÇÃO DE UM NOVO CONTROLE: criação de ou adoção de nova ferramenta de gestão;

2. MELHORIA DE UM CONTROLE EXISTENTE: revisão ou adequação de controles existentes.

Outros aspectos dos controles também deverão ser levados em consideração como:

Natureza do Controle

- **Manual**: controles realizados por pessoas (exemplo: checklist, conferência);
- **Automático**: controles processados por um sistema, sem interferência humana;
- **Híbridos**: controles que mesclam atividades manuais e automáticas.

Frequência do Controle

- **Anual**
- **Semestral**
- **Mensal**
- **Semanal**
- **Diário**
- **Várias vezes ao dia**

Relação com risco

- **Direto**: tem objetivo de mitigar o risco; geralmente relacionados a controles operacionais
- **Indireto**: têm como objetivo a prevenção e detecção de eventos de risco; mais relacionados ao ambiente de controle (exemplo: treinamentos)

8.3.4.1.2. PLANO DE IMPLEMENTAÇÃO DOS CONTROLES

Definidos os tipos de controles a serem adotados, deve ser elaborado um **PLANO DE AÇÃO** para a implementação desses controles, descrevendo as ações necessárias e seu encadeamento para reduzir os riscos a níveis aceitáveis, sempre levando em consideração o custo-benefício dessas propostas, já que custo de um controle não pode ser mais alto do que o benefício gerado por ele.

Outros pontos de atenção na proposição de ações incluem:

- A substituição de controles manuais por controles automatizados sempre que for possível/viável
- Estabelecer indicadores de desempenho
- Segregar funções com a finalidade de reduzir erros, riscos ou a possibilidade de fraudes

PREENCHIMENTO DA PLANILHA

Aba "Plano de Ação"

As propostas podem ser registradas seguindo o modelo de cinco perguntas: O quê? Onde? Quem? Como? Quando?

O QUÊ?
- *Descrição do controle ou ação para resposta ao evento de risco;*
- *Tipo de controle proposto: preventivo, corretivo ou compensatório (Menu Suspenso);*
- *Objetivo: adoção de novo controle ou melhoria de controle existente (Menu Suspenso).*

ONDE?
- *Área responsável pela implementação do controle/ação proposta; informar Divisão/Processo/Subprocesso.*

QUEM?
- *Responsável pela implementação; gestor do processo ou colaborador designado.*

COMO?
- *Descrição o modo de implementação do controle/ação proposta, seja por meio de projeto, melhoria de sistema, criação de norma, plano de contingência;*
- *Intervenientes: outras áreas ou pessoas que participam da ação.*

QUANDO?
- *Data prevista de início;*
- *Data prevista para conclusão;*
- *Status.*

Os dados inseridos nessa aba serão automaticamente atualizados na aba "Mapa de Riscos".

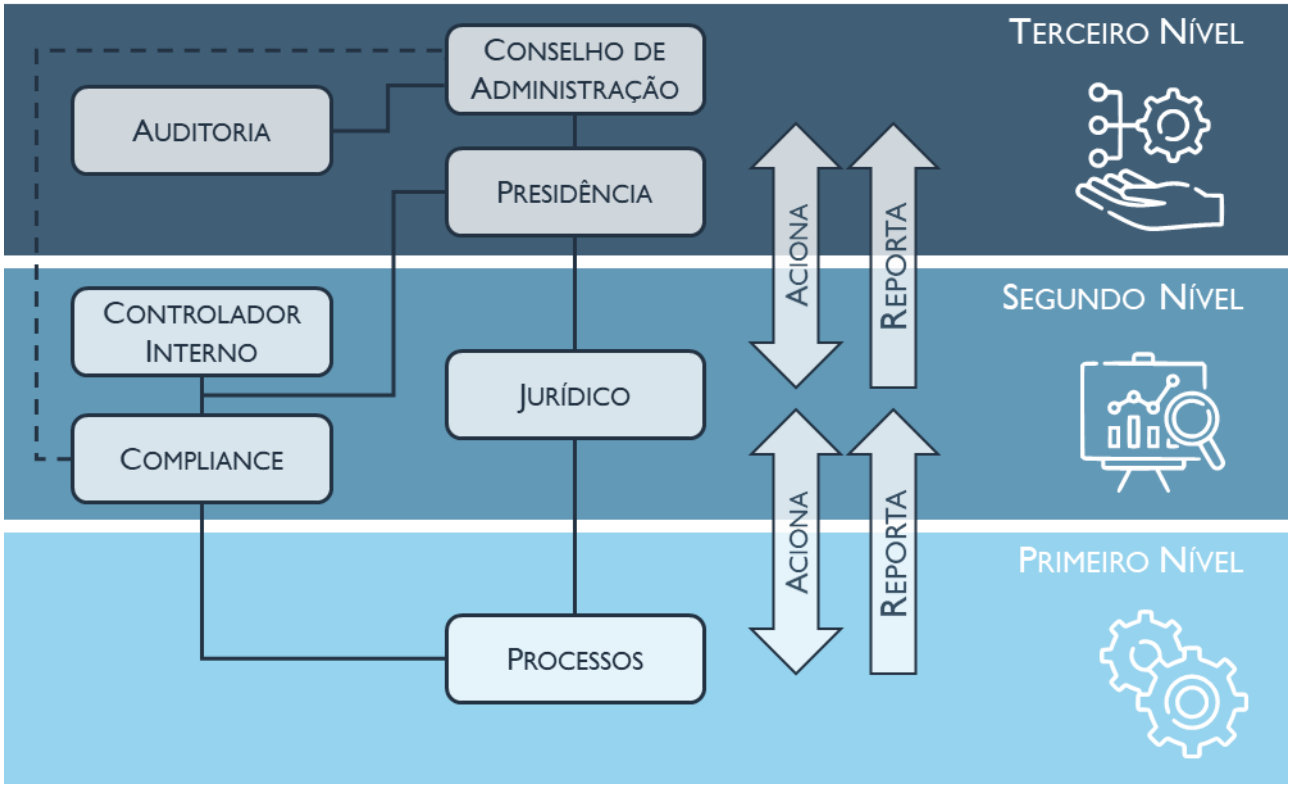
8.3.5. Informação, Comunicação e Monitoramento

O acesso a informações confiáveis, íntegras e tempestivas é indispensável para a efetividade da Gestão de Riscos, de modo que os direcionamentos estratégicos oriundos da alta administração alcancem todos os processos e, da mesma forma, as informações geradas e coletadas pelos processos de trabalho, bem como as informações externas relevantes, cheguem até os decisores. A comunicação direcionada à sociedade também deve ser controlada, evitando-se respostas inadequadas ou equivocadas à população.

No tocante à gestão de riscos, o primeiro nível, representado pelos gestores dos processos e demais colaboradores envolvidos, serão responsáveis pelo reporte ao segundo nível sobre o monitoramento das ações definidas no plano de implementação de controles e demais ações referentes à gestão de integridade, riscos e controles. O primeiro nível também pode acionar, a qualquer tempo o segundo nível para orientações técnicas relativas ao modelo de gestão de riscos

O segundo nível, composto por colaboradores com capacitação em temas afetos à Gestão de Integridade, Riscos e Controles internos e representado pelo Comitê de Compliance e Gerenciamento de Riscos, Controlador Interno e, nos casos fortuitos, o departamento Jurídico, poderá acionar o nível operacional durante as etapas de monitoramento de ações de integridade e controles, sendo também responsável pelo reporte realizado ao terceiro nível sobre o andamento das ações definidas para o plano de gestão de riscos.

O segundo nível também poderá, a qualquer momento, acionar e ser acionado pelo terceiro nível, composto pela Alta Administração (Presidência e Conselho de Administração) para o monitoramento das ações definidas na Política de Gestão de Riscos. Em casos extraordinários, onde recaiam sobre o presidente suspeitas de ilícitos ou má conduta, o Comitê de Compliance poderá acionar diretamente o Conselho de Administração.



8.3.5.1. MONITORAMENTO

O monitoramento é parte integrante do processo de gestão e tomada de decisão. Visando garantir que a estrutura de governança e gestão de riscos e controles estejam adequadas aos objetivos estratégicos da EMDEC, o processo deve ser continuamente monitorado e avaliado. O Mapa de Riscos (Planilha Documentadora) é a principal ferramenta de monitoramento da gestão de integridade, riscos e controle dos processos, permitindo uma visualização rápida do status de implementação dos controles.

Além dele, sugere-se que a cada seis meses seja apresentado o Relatório de Implementação do Plano de Controles às instâncias de supervisão, contendo o detalhamento das ações implementadas, deficiências e vulnerabilidades percebidas e ajustes ou aperfeiçoamento necessários.

De modo a tornar o processo de implementação mensurável, o relatório também deve conter indicadores de monitoramento. Alguns desses indicadores são sugeridos na tabela abaixo, porém os processos proprietários dos riscos têm autonomia para desenvolver indicadores próprios para os controles planejados:

- % PROCESSOS MAPEADOS = processos mapeados/total de processos
- % PROCESSOS COM RISCOS MAPEADOS = processos com riscos mapeados/ total de processos
- % CONTROLES IMPLEMENTADOS POR PROCESSO = controles concluídos/total de controles do processo
- % CONTROLES EM ANDAMENTO POR PROCESSO = controles em andamento/total de controles do processo
- % CONTROLES ATRASADOS POR PROCESSO = controles atrasados/total de controles do processo
- % CONTROLES NÃO INICIADOS POR PROCESSO = controles não iniciados/total de controles do processo

8.3.5.2. REVISÃO DO PROCESSO DE GESTÃO DE RISCOS

Outrossim, o Processo de Gestão de Riscos deve ser revisado nos seguintes casos:

- Sempre que ocorrer mudança significativa no processo de trabalho;
- Quando a última avaliação atingiu o prazo de dois anos (embora processos com maior exposição possam ser avaliados com menor intervalo).

9. REFERÊNCIAS BIBLIOGRÁFICAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS - ABNT. NBR ISO 31000: Gestão de Riscos - Diretrizes. Rio de Janeiro, 2018

BRASIL. Ministério do Planejamento, Desenvolvimento e Gestão. Manual de Gestão de Integridade, Riscos e Controles Internos da Gestão. Brasília, 2017b. Disponível em:<https://www.gov.br/economia/pt-br/centrais-de-conteudo/publicacoes/planejamento/controle-interno/manual_de_girc___versao_2_0.pdf>

COSO ERM. Gerenciamento de Riscos Corporativos - Estrutura Integrada, 2004.

COSO. Gerenciamento de Riscos Corporativos – Estrutura Integrada. 2007. Tradução: Instituto dos Auditores Internos do Brasil (Audibra) e Pricewaterhouse Coopers Governance, Risk and Compliance, Estados Unidos da América, 2007.

IIA. As Três Linhas de Defesa no Gerenciamento Eficaz de Riscos e Controles. Disponível em https://na.theiia.org/standards-guidance/Public%20Documents. Acesso em 13.out.2021.

IBGC, Guia de Orientação para Gerenciamento de Riscos Corporativos.

EMDEC

EMPRESA MUNICIPAL DE
DESENVOLVIMENTO DE CAMPINAS

CAMPINAS

2022