

BOAS PRÁTICAS DE CONTROLE INTERNO, GESTÃO DE RISCOS E COMPLIANCE

1. INTRODUÇÃO

O presente documento tem como premissa apresentar as diretrizes básicas acerca das boas práticas de controle interno, gerenciamento de riscos e *compliance*, buscando fomentar e despertar nos gestores a importância dessas ferramentas para a melhoria da gestão da EPAGRI.

As boas práticas de controle interno, gerenciamento de riscos e *compliance* visam a preservação e a geração de valor da EPAGRI e devem estar alinhadas à missão, visa, valores e objetivos estratégicos da empresa.

2. OBJETIVOS

Os objetivos do presente documento são:

- a) Instituir diretrizes básicas e competências em relação às boas práticas de controle interno, gerenciamento de riscos e *compliance*.
- b) Difundir a importância desses mecanismos de gestão entre os gestores de modo a auxiliar e incorporar os seus resultados à tomada de decisão da EPAGRI.
- c) Promover uma linguagem comum de boas práticas de controle interno, gerenciamento de riscos e *compliance* a todos os gestores e empregados da EPAGRI.

3. ABRANGÊNCIA

Este documento se aplica a todos os empregados da EPAGRI, incluindo membros do Conselho de Administração e Fiscal, Comitês e Diretoria Executiva.

4. CONTROLES INTERNOS

A atividade de controles internos constitui-se numa ferramenta de gestão, composta por um conjunto de procedimentos, com o objetivo de conferir confiabilidade aos dados e informações, promover a eficiência operacional, assegurar a aderência à legislação e demais regulamentos internos, bem como avaliar se os objetivos da EPAGRI estão sendo alcançados.

A atividade de controles internos é de competência de todas as áreas da EPAGRI, cada qual em seu nível de atuação, uma vez que está intrinsecamente ligada ao processo de gerenciamento de riscos corporativos.

Os princípios fundamentais do controle interno são:

- a) **Responsabilidade:** definição clara e objetiva das atribuições de cada empregado, com vistas a assegurar que todos os procedimentos da empresa serão cumpridos, evitando e detectando possíveis erros, bem como identificando as responsabilidades por eventuais omissões na realização das atividades da EPAGRI.
- b) **Rotinas internas:** definição das rotinas de controles internos nos manuais e regulamentos internos. As rotinas compreendem: formulários internos e externos, evidências das execuções dos procedimentos de controle e dos procedimentos internos.
- c) **Segregação de funções:** consiste em estabelecer que um empregado não deva atuar em todas as etapas de um processo, de modo a se reduzir o risco de erros, fraudes e conflito de interesses.
- d) **Confronto dos ativos com os registros:** definição de procedimentos em que as operações sob a responsabilidade de um empregado sejam sempre confrontadas com os registros da contabilidade.
- e) **Auditoria interna:** setor responsável pela verificação dos controles internos.
- f) **Custos x benefícios:** o custo do controle interno não pode ser superior aos benefícios que este pode trazer para empresa.

4.1. ATIVIDADES DE CONTROLE INTERNO

As atividades de controle interno quando executadas a tempo e de modo adequado permitem a redução ou administração dos riscos.

As atividades de controle interno podem ser de **prevenção**, **detecção** ou **correção**.

- a) **Atividades de prevenção:** controles preventivos são aqueles que têm a finalidade de evitar a ocorrência de erros ou irregularidades. São exemplos de atividades de prevenção: *autorizações competentes, sistemas informatizados, segurança de acesso, normatização, segregação de funções.*

- b) Atividades de detecção:** são atividades projetadas para detectar erros, ou irregularidades depois que já tenham ocorrido, permitindo a adoção de medidas tempestivas de correção. São exemplos de atividades de detecção: *conciliação, revisões de desempenho, segurança física, sistemas informatizados, controles de aplicativos, avaliação de conformidade.*
- c) Atividades de correção:** são controles que eliminam a causa da ocorrência do evento indesejado.

4.2. IMPLANTAÇÃO DO SISTEMA DE CONTROLES INTERNOS

A implantação do sistema de controles internos tem como base a identificação dos riscos que podem comprometer o alcance dos objetivos da empresa. Embora sejam muito parecidos e possam se confundir, não trataremos aqui do gerenciamento de riscos corporativos, mas sim, dos riscos de processo.

A significância dos riscos e a probabilidade de sua ocorrência permitirão decidir sobre as respostas e ações a serem realizadas.

As etapas para a implantação do sistema de controles internos correspondem a: *alcance e planejamento, mapeamento da área operacional que apresenta riscos relevantes, identificação e avaliação dos riscos, planejamento das respostas aos riscos, monitoramento e controle dos riscos.*

4.2.1. Alcance e Planejamento

- a)** Definição dos processos críticos e estabelecimentos de ferramentas de gestão;
- b)** Definição da equipe de trabalho, composta por um coordenador para cada área e empregados que executem no dia a dia as tarefas das áreas analisadas;
- c)** Criação de um plano de ação para execução do projeto;
- d)** Planejamento de um cronograma com datas de início e término para cada etapa do processo.

4.2.2. Mapeamento da Área Operacional que Apresenta Riscos Relevantes

O mapeamento dos processos permite um melhor entendimento das atividades, bem como a definição de atribuições e responsabilidades, além de identificar possíveis falhas dos processos atuais.

Todos os processos da empresa devem ser examinados em todas as etapas e, depois desse levantamento, deve ser elaborado relatório de avaliação e sugerir melhorias para as deficiências encontradas no processo.

Os levantamentos do sistema de controle interno podem ser obtidos da seguinte maneira:

- a) Leitura dos manuais e regulamentos internos;
- b) Conversa com empregados, colaboradores e acionistas;
- c) Acompanhamento da execução da operação do início até a sua finalização.

As formas utilizadas para o registro dos procedimentos dos controles internos correspondem a: *descritiva, utilização de fluxogramas, utilização de questionários.*

4.2.3. Identificação e Avaliação dos Riscos

Cada risco identificado e apresentado deve conter a probabilidade de ocorrência do mesmo e o grau do impacto previsto, conforme tabela abaixo:

PROBABILIDADE		
	Baixa (entre 0 e 35%)	É improvável a ocorrência do risco
	Média (entre 35% e 65%)	É provável a ocorrência do risco Com ou sem histórico de perda anterior
	Alta (entre 65% e 100%)	É muito provável a ocorrência do risco. Há histórico de perda anterior
IMPACTO		
	Baixo (entre 0 e 35%)	Baixo impacto na reputação Perdas assimiladas
	Médio (entre 35% e 65%)	Perda temporária da reputação Perdas financeiras significativas
	Alto (entre 65% e 100%)	Elevado risco de perda da reputação Elevada perda financeira

4.2.4. Planejamento das Respostas ao Risco

As respostas aos riscos buscam opções e ações para aumentar as oportunidades e reduzir as ameaças aos objetivos da EPAGRI, podendo ser classificadas em quatro categorias: *evitar, reduzir, compartilhar ou aceitar*.

- a) **Evitar:** descontinuar as atividades que geram risco.
- b) **Reduzir:** adotar medidas para reduzir a probabilidade e/ou o impacto dos riscos.
- c) **Compartilhar:** ações para reduzir a probabilidade ou o impacto dos riscos pela transferência ou pelo compartilhamento de uma parcela do risco.
- d) **Aceitar:** não adotar nenhuma medida que possa afetar a probabilidade e o grau do impacto dos riscos.

4.2.5. Monitoramento e Controle dos Riscos

Deve ser realizado por meio de acompanhamento contínuo das atividades, bem como por avaliações pontuais.

O sistema de monitoramento deve ser incorporado às atividades rotineiras de cada uma das áreas da empresa.

4.3. AVALIAÇÃO DO SISTEMA DE CONTROLES INTERNOS

Os controles internos devem ser periodicamente revisados e atualizados, de forma que sejam a eles incorporadas medidas relacionadas a riscos novos ou riscos não abordados anteriormente.

A Auditoria Interna é responsável por aferir a adequação dos controles internos.

5. COMPLIANCE

Os procedimentos de *compliance* têm o objetivo de assegurar a aderência às legislações, normas, regulamentos, políticas internas e às boas práticas de gestão, sempre alinhadas aos objetivos da empresa, bem como identificar eventuais condutas inadequadas.

A função de *compliance* atua como um instrumento de gestão preventiva de riscos legais e de reputação.

O risco de *compliance* configura-se como o risco de perda financeira por sanções legais, regulatórias ou por dano na reputação que a EPAGRI pode sofrer como resultado de falhas no cumprimento das leis, regulamentações, regras e das boas práticas de gestão.

Para que a função de *compliance* possa atingir o resultado esperado na EPAGRI é importante a observação das seguintes premissas:

- a) A estrutura de *compliance* deverá interagir com diversas áreas da empresa para a execução de suas atividades;
- b) Definir formalmente quais as legislações, regulamentos e normas internas irão compor o Programa de *Compliance*, e, portanto, serão o escopo de atuação da área de *Compliance*, incluindo o Código de Conduta e Integridade;
- c) Por meio de método formal, verificar na empresa a aderência em relação a cada uma das legislações, regulamentos e normas internas que fizerem parte do escopo do Programa de *Compliance*;
- d) Propor formalmente ações em conjunto com as áreas envolvidas para atendimento das legislações, regulamentos e normas internas;
- e) Monitorar o cumprimento do Programa de *Compliance* e reportar para a Diretoria Executiva sobre o seu desenvolvimento;
- f) Revisar periodicamente o escopo do Programa de *Compliance*, observando o surgimento de novas legislações, regulamentações e normas internas;
- g) Zelar pelo cumprimento de leis, regulamentos, normas internas e por padrões éticos;
- h) Analisar políticas e normas internas com objetivo de evitar conflitos com outras já existentes e com a legislação;
- i) Os responsáveis pelos processos de negócios são os donos dos riscos de *compliance*, cabendo a estes o papel de estar em conformidade nos processos sob sua responsabilidade.

6. GESTÃO DE RISCOS CORPORATIVOS

A Gestão Integrada de Riscos Corporativos é um processo estruturado e contínuo, desenhado para identificar e responder de maneira proativa a eventos em potencial capazes de afetar os objetivos da EPAGRI, buscando a manutenção dos riscos em níveis adequados.

O processo pode ser dividido em cinco macro etapas: *identificação, avaliação, resposta ao risco, monitoramento e comunicação*.

As informações devem ser registradas em uma matriz de riscos, que deverá ser revisada, no mínimo, anualmente, levando em consideração eventuais mudanças em relação aos objetivos estratégicos da empresa, bem como em relação ao aumento ou diminuição no grau de impacto e probabilidade de ocorrência dos riscos.

A EPAGRI utilizará como base o modelo do COSO – ERM (*Committee of Sponsoring Organizations of the Treadway Commission – Enterprise Risk Management*) e o Código das Melhores Práticas de Governança Corporativa do Instituto Brasileiro de Governança Corporativa – IBGC.

6.1. Princípios da Gestão de Riscos Corporativos

- a) Salvaguarda e geração de valor para EPAGRI;
- b) Alinhamento da gestão de riscos corporativos com os objetivos estratégicos da EPAGRI;
- c) Definição formal de atuação e responsabilidades no processo de gestão de riscos corporativos;
- d) Constituição e manutenção de infraestrutura adequada;
- e) Definição clara e objetiva de metodologia de gestão de riscos corporativos.

6.2. Diretrizes da Gestão de Riscos Corporativos

- a) Manter a política de gestão de riscos corporativos alinhada com os objetivos e estratégias da EPAGRI;
- b) Promover a gestão de riscos corporativos em todos os níveis hierárquicos e áreas de atuação da EPAGRI;
- c) Integrar e manter os níveis de apetite ao risco alinhados com os objetivos e estratégias da EPAGRI;
- d) Direcionar as oportunidades identificadas às áreas competentes para análise e implementação das ações necessárias à sua realização;
- e) Assegurar que os riscos e controles associados sejam revisados, no mínimo, anualmente;
- f) Assegurar que o processo de identificação e análise geral de riscos seja monitorado e aprimorado;

6.3. Categorias de Risco

Considerando as quatro classes de objetivos do COSO – ERM, a natureza de suas operações e a relação com suas atividades, as categorias de risco da EPAGRI classificam-se em: *risco estratégico, risco financeiro, risco operacional e risco de compliance.*

6.3.1. Risco Estratégico

- a) **Estratégia:** riscos que estão associados à tomada de decisão da Diretoria Executiva e ao planejamento estratégico;
- b) **Reputação:** possibilidade de perdas em razão deterioração da marca EPAGRI junto à sociedade, às famílias rurais ou ao Governo, em virtude de publicidade negativa.

6.3.2. Risco Financeiro

- a) **Liquidez:** possibilidade de insuficiência de recursos, caixa ou outro ativo financeiro para liquidar as obrigações nas datas previstas;
- b) **Crédito:** risco de incorrer em perdas decorrentes do não recebimento das receitas programadas;
- c) **Divulgação:** risco associado à possibilidade de emissão de relatórios financeiros, gerenciais, regulatórios, fiscais, estatutários incompletos, inexatos ou intempestivos, expondo a EPAGRI a multas, penalidades ou outras sanções.

6.3.3. Risco Operacional

- a) **Processos:** risco relacionado à eficácia e eficiência das atividades da EPAGRI, inclusive as metas de desempenho financeiros e operacional e a salvaguarda de perda de ativos e à possibilidade de ocorrência de perdas resultantes da falha, deficiência ou inadequação de processos internos, pessoas e sistemas ou de eventos externos;
- b) **Tecnologia da informação:** riscos de acesso não autorizado a dados e informações da companhia, decorrente de vulnerabilidades de controles de acesso, falha de segregação de funções, violação de políticas, acarretando ataques externos, paradas no ambiente de TI, alteração ou divulgação indevida de informações;

- c) **Socioambiental:** riscos relacionados aos impactos que as atividades da EPAGRI podem gerar na sociedade e no meio ambiente, podendo afetar a reputação e gerar atuação de órgãos fiscalizadores. Está relacionado, também, com o efeito das intempéries climáticas severas, escassez de recursos naturais ou mobilização de comunidades, podendo causar interrupção na prestação dos serviços;

6.3.4. Risco de *Compliance*

- a) **Leis e normas:** não conformidade com leis ambientais, trabalhistas, tributárias, e regulatórias às quais a EPAGRI está sujeita, incluindo políticas e normas internas, expondo a empresa à atuação por órgãos fiscalizadores;
- b) **Fraude e corrupção:** riscos relacionados ao roubo de ativos físicos, agenciamento de informações, desvio de recursos financeiros, conflito de interesses, tráfico de influência, suborno, propina, conluio com fornecedores e clientes, entre outros, podendo implicar em perdas financeiras, multas, sanções e penalidades por órgãos fiscalizadores e deterioração da imagem da EPAGRI.