POLÍTICA DE GESTÃO DE RISCOS E CONTROLES INTERNOS

ÁREA PROPONENTE

1.1 Coordenadoria de Riscos e Controles Internos – CORIS

OBJETIVO

2.1 Esta política tem como objetivo estabelecer e apresentar os princípios e características da Gestão de Riscos da FUSESC, sendo ferramenta de desenvolvimento, disseminação e aplicação de abordagens de Gestão de Riscos e Controles internos, atestando o comprometimento de todas as partes envolvidas, sob liderança da Diretoria Executiva e Conselho Deliberativo e monitoramento do Conselho Fiscal, de maneira integrada a Governança Corporativa.

2.2 O objetivo da FUSESC em adotar Gestão de Riscos e Controles Internos é instituir prática que subsidie a melhoria contínua dos processos, para a tomada de decisão através da melhor informação disponível, visando o cumprimento da sua missão e visão, se mantendo aderente a seus valores.

CLASSIFICAÇÃO DA INFORMAÇÃO

3.1 As informações contidas nesta Política são de acesso público.

GLOSSÁRIO E DEFINIÇÕES

4.1 Risco: Efeito da incerteza nos objetivos;

4.2 Risco Original ou Inerente: Nível de exposição ao risco antes da aplicação de

controles;

4.3 Risco Residual: Risco remanescente após a implementação de controles que visam a reduzir a probabilidade e/ou impacto de ocorrência;

4.4 Apetite a Risco: Está associado ao nível de risco aceitável pela Entidade na busca e realização de sua missão e visão;

4.5 Fonte de Risco: Elemento que, individualmente ou combinado, tem o potencial para dar origem ao risco;

4.6 Probabilidade: Critério de avaliação da chance de materialização do risco;

4.7 Impacto: Critério de avaliação da consequência de materialização do risco;

4.8 Consequência: Resultado percebido de um evento de materialização de risco;

4.9 Evento: Ocorrência ou mudança em um conjunto específico de circunstâncias;

4.10 Controles Internos: Práticas que mitigam os impactos e/ou probabilidades dos riscos;

4.11 Controle Preventivo: Práticas que mitigam a probabilidade dos eventos de risco;

4.12 Controle Detectivo: Práticas que mitigam o impacto dos eventos de risco;

4.13 Partes Interessadas: Pessoa ou organização que pode afetar, ser afetada ou perceber-se afetada por uma decisão ou atividade;

4.14 Plano de Ação: Compreende um conjunto de ações definidas por gestores, com indicação de responsáveis e prazo para implementação, visando melhorar processos, minimizar riscos ou solucionar problemas identificados nas avaliações das áreas. Podem ser criados a qualquer momento e ou ser decorrentes da avaliação de riscos.

DIRETRIZES GERAIS

5.1 O modelo de gestão de riscos e controles internos adotado pela FUSESC baseia-se nas diretrizes da Norma ABNT NBR ISO 31000 e se aplicada a toda a Entidade.

5.2 Para que a Gestão de Riscos cumpra seus objetivos, a Alta Gestão deve

proporcionar os recursos e diretrizes necessárias, a fim de, não somente atender

as legislações e normas setoriais, mas também, garantir a geração e proteção de

valor da Entidade.

5.3 A Cadeia de Valor da FUSESC é entrada estrutural da Gestão de Riscos, de modo que os Planos de Risco são alocados por processo. Sua atualização é dinâmica, estando disponível para consulta pelos funcionários e membros da Governança no sistema SoftExpert.

PRINCÍPIOS

6.1 Os princípios fornecem orientações sobre os atributos da gestão de riscos eficaz e eficiente, comunicando seu valor e elucidando sua intenção e propósito. Os princípios são a base para gerenciar riscos e devem ser considerados na estruturação dos processos da gestão de riscos:

6.1.1 **Integrada:** A Gestão de Riscos deve ser parte integrante de todas as atividades e processos da Entidade;

6.1.2 **Estruturada e abrangente:** A gestão de riscos deve ser estruturada de forma

sistematizada, abrangendo a Entidade como um todo, em seus diversos níveis e processos , proporcionando entregas consistentes;

6.1.3 **Personalizada:** A gestão dos riscos deve ser compatível com a missão e visão da Entidade, como também ao seu contexto interno e externo, considerando sempre seu porte e complexidade;

6.1.4 **Inclusiva:** O envolvimento oportuno das partes interessadas abastece o processo com seus diversos pontos de vista, gerando senso de pertencimento, resultando em melhor conscientização e fundamentação;

6.1.5 **Dinâmica:** A gestão de riscos deve ser tempestiva com as mudanças internas e externas, abastecendo-se dos processos cotidianos por suas diversas entradas;

6.1.6 **Melhor informação disponível**: As entradas para gestão de riscos são claras e consistentes, alicerçando as tomadas de decisão por informações precisas, estruturadas e relevantes;

6.1.7 **Fatores humanos e culturais**: O nível de engajamento e conhecimento pelas pessoas e a cultura na qual estão inseridas influenciam significativamente todos os aspectos da gestão de riscos;

6.1.8 **Melhoria contínua:** A estrutura de gestão de riscos é revisitada sempre que o passado ou novos conhecimentos proporcionam oportunidades de aperfeiçoamento adequadas ao porte e complexidade da Entidade, buscando se manter eficiente, eficaz e relevante;

ESTRUTURA

7.1 A estrutura de gestão de riscos é desenvolvida de modo a realizar sua integração com a Governança, atuando com maior inserção nos processos mais críticos. A eficácia da estrutura depende do cumprimento de todos os alicerces por todas as partes envolvidas, principalmente a Gestão. São seus alicerces de maneira cíclica:

7.1.1 **Liderança e Comprometimento:** O comprometimento dos Órgãos Estatutários visa garantir a eficácia da estrutura e processos da cultura de gestão de riscos. Evidência deste comprometimento é a criação de área específica, com a atribuição de apoiar às demais áreas na identificação, análise, avaliação e tratamento dos riscos dos processos;

7.1.2 **Integração**: A gestão de riscos deve estar integrada aos processos, estando presente em todos os níveis organizacionais. Todos os funcionários são

proprietários dos riscos vinculados a suas atividades e contribuem com sua percepção e controle;

7.1.3 **Concepção**: A gestão de riscos utiliza o Planejamento Estratégico vigente da FUSESC para abastecer os fatores internos e externos de relevância. O relacionamento entre Gestão de Riscos e Planejamento Estratégico / Análise SWOT é recíproco, sendo ambos utilizados como entradas e saídas em suas revisões;

7.1.4 **Implementação:** A Gestão de Riscos está implementada através do software SoftExpert, garantindo o cumprimento de metodologia, com confiabilidade auditável. Sua funcionalidade bem-sucedida depende do correto abastecimento e envolvimento das partes interessadas, garantindo o dinamismo necessário para constante aderência as diversas mudanças de contexto e utilização como fonte de informação adequada para tomadas de decisões;

7.1.5 **Avaliação:** A estrutura de gestão de riscos é avaliada constantemente, através dos indicadores estabelecidos e criticada conforme nível de maturidade pela Diretoria Executiva. Além de manter reporte mensal a todos os Órgãos Estatutários, disponibilizando suas atualizações e recepcionando as dúvidas e oportunidades geradas;

7.1.6 **Melhorias**: As oportunidades identificadas através da avaliação, desde que aderentes ao porte e complexidade da Entidade, com adequado custo benefício e pautadas na perseguição de proteção e criação de valor devem ser implementadas, de modo a manter a Gestão de Riscos adequada com as necessidades de Contexto Interno e Externo;

PROCESSO DE GESTÃO DE RISCOS

8.1 O processo de gestão de riscos deve estar incorporado à cultura organizacional, e apesar de ser apresentado em sequência, este é iterativo e dinâmico:

8.1.1 Comunicação e consulta: Para garantir a adequada integração da gestão de riscos na Entidade, as partes interessadas internas são parte inclusa do processo de desenvolvimento e abastecimento, participando ativamente de todas as etapas do Processo de Avaliação de Riscos, inclusive na validação de critérios de impacto, levantamento de ocorrências, mensuração de consequências e comunicações e consultas específicas para acurácia de informações;

8.1.2 Escopo, contexto e critérios: A gestão de riscos se aplica a toda a FUSESC, desse modo, o contexto é analisado através do Planejamento Estratégico vigente.

8.1.2.1 Os critérios para avaliação de riscos operacionais são baseados em Probabilidade e Impacto, sendo a probabilidade medida padrão que leva em consideração a quantidade de Fontes de Risco e a biblioteca de ocorrências, e o impacto medida personalizada para cada processo, podendo ser quantitativo, qualitativo ou a mescla de ambos.

8.1.2.2 Os critérios para avaliação de riscos estratégicos são baseados em impacto e horizonte de tempo.

8.1.3 Processo de Avaliação de Riscos: Inclui as etapas de identificação, análise e avaliação de riscos.

8.1.3.1: Identificação de riscos: a identificação de riscos acontece por entradas diversas, considerando fontes de risco que estão ou não sob controle da Entidade, causas, eventos, consequências e mudanças de contextos ou objetivos;

8.1.3.2 Análise: os riscos devem ser compreendidos, em relação a sua natureza e características. É levada em consideração sua relevância, logo que, se o risco for considerando irrelevante para a FUSESC seu mapeamento não se faz necessário. 8.1.3.2.1 Riscos irrelevantes são aqueles que em caso de ocorrência não impactariam o processo, nem mesmo no impacto mínimo dos critérios de avaliação do processo em questão.

8.1.3.3 As naturezas dos riscos são classificadas em categorias, sendo essas:

8.1.3.3.1 Atuarial: O risco atuarial se caracteriza pela ausência de solidez econômico-financeira, comprometendo a liquidez, solvência e o equilíbrio dos planos de benefícios, ou seja, a incapacidade de os planos de benefícios saldarem as obrigações previstas com os participantes.

8.1.3.3.2 Crédito: O risco de crédito refere-se ao risco de um devedor não liquidar integralmente seus compromissos em tempo hábil (Inadimplência).

8.1.3.3.3 Legal / Compliance: O risco legal/compliance está relacionado a não conformidade com a Legislação e normativos internos e externos.

8.1.3.3.4 Liquidez: O risco de liquidez envolve o descasamento entre o fluxo do ativo e do passivo do Plano.

8.1.3.3.5 Mercado: O risco de mercado pode ser definido como o risco decorrente de flutuações nos preços e taxas de mercado.

8.1.3.3.6 Operacional: O risco operacional é a possibilidade de ocorrência de perdas resultantes de falha, deficiência ou inadequação de processos internos, pessoas e sistemas.

8.1.3.3.7 Reputação/Imagem: O risco de reputação/imagem remete a alteração da credibilidade e confiança das partes interessadas em relação a Fundação.

8.1.3.3.8 Socioambiental: O risco socioambiental é caracterizado por origem social ou ambiental.

8.1.3.3.9 Tecnologia e Segurança da Informação: O risco de tecnologia e segurança da informação está diretamente ligado a proteção das informações sob guarda da Entidade, assim como seu correto manejo e confiabilidade.

8.1.3.3.10 Estratégico: São os riscos vinculados ao Planejamento Estratégico.

8.1.3.3.11 Os riscos emergentes devem ser identificados através de atributo específico, não sendo considerados uma categoria específica, logo que, pode haver riscos emergentes de diversas naturezas.

8.1.3.4 O resultado final da análise de riscos relevantes deve gerar registro do risco, suas fontes, controles (quando existentes) e nível de risco original e residual, de acordo com os critérios definidos para o processo em questão.

8.1.4. Avaliação: os riscos devem ser alocados perante sua significância e seus controles já existentes em três possíveis níveis de risco, gerando diretrizes conforme abaixo:

Nível de Risco Residual	**Apetite**	**Diretriz**
ALTO	Acima do apetite desejável	O Conselho Deliberativo deve tomar conhecimento do risco e seus controles existentes acompanhados de planos de ação aprovados pela Diretoria Executiva.
MÉDIO	Dentro do apetite desejável	Análise de custo / benefício de planos de melhoria de controles existentes ou implantações de novos controles.
BAIXO	Dentro do apetite desejável	Manutenção de controles existentes, com possibilidade de flexibilidade nos prazos de ações de melhorias planejadas.

8.1.4.1 A tabela acima representa a Declaração de Apetite a Riscos da FUSESC.

8.1.4.1.1 Levando em consideração a premissa de que quanto maior a exposição, maior o nível de controle desejado, as tabelas abaixo trazem os endereçamentos de controle de acordo com os níveis de Risco Real, para garantia de manutenção de Risco Residual conforme avaliado:

Riscos Operacionais	
Nível de Risco Real	**Diretriz**
ALTO	Monitoramento de todos os controles
MÉDIO	Adoção de monitoramento por amostragem/histórico
BAIXO	Monitoramento eventual de controles

Riscos Estratégicos	
Nível de Risco Real	**Diretriz**
ALTO	Priorizar ações e análise de viabilidade de planos de resposta/contingência
MÉDIO	Programar ações dentro do horizonte de tempo do Planejamento Estratégico
BAIXO	Analisar custo / benefício de ações, com possibilidade de repactuações

8.1.5. **Tratamento:** é o ato de abordar o risco residual, e sua decisão deve levar em consideração as diretrizes com base no nível e apetite a riscos. As ações escolhidas podem ser:

a. Assumir ou reter: nenhuma ação é tomada para mudar a magnitude do risco, mas um plano de contingência pode ser desenvolvido;

b. Evitar: remover o risco, sendo necessário eliminar as fontes de risco, envolve descontinuar determinada atividade/objetivo;

c. Mitigar: reduzir o impacto através de controles detectivos e/ou reduzir a probabilidade através de controles preventivos;

d. Compartilhar: compartilhamento através de mecanismo que diminua ou imunize o impacto gerado em ocorrência do risco.

8.1.6. **Monitoramento riscos operacionais:** A partir das do resultado do risco residual, após aplicação dos tratamentos, deve ser criado plano de

monitoramento anual, através de amostragem, conforme diretrizes de nível de risco. As mudanças de contexto e ocorrências geram novas entradas para o processo de avaliação de riscos e são monitoradas constantemente.

8.1.7 **Monitoramento riscos estratégicos**: Realizado conforme reporte do Planejamento Estratégico.

8.2 **Registro e Relato:** Os registros e relatos da gestão de riscos são controlados por meio do sistema e seus relatórios, devendo ser a divulgação tempestiva, levando em consideração que a comunicação dos resultados deve ser difundida em toda a Entidade, bem como fornecer informações para tomada de decisão das partes interessadas e servir de base para a melhoria contínua dos processos da Entidade.

8.2.1 Todas as partes internas possuem acesso constante a todas as informações atualizadas através do SoftExpert. Em rotina mensal, é emitido o Relatório Gerencial, trazendo de forma consolidada aos Órgãos Estatutários os dados modificados no último mês.

8.2.2 Anualmente, em toda conclusão de ciclo de avaliação anual de riscos, é emitido Relatório específico, divulgado a todas as partes relacionadas internas, e mantido para consulta no sistema de gestão.

PAPÉIS E RESPONSABILIDADES

9.1 A FUSESC deverá referenciar a Gestão de Riscos ao modelo das Três Linhas do Instituto de Auditores Internos (IIA). O modelo estrutura as responsabilidades em:

9.1.1 Primeira Linha: gestores e operacionais responsáveis pela execução, incluindo riscos e controles de suas atividades;

9.1.2 Segunda Linha: gestores e operacionais ligados as funções de monitoramento e estruturação de regras/ritos;

9.1.3 Terceira Linha: componentes independentes de avaliação da atuação das primeiras e segundas linhas;

9.1.4 Órgãos de Governança: estruturas de liderança, fiscalização e direcionamento institucional.

9.2 A delimitação das funções e obrigações se fundamenta na abordagem integrada, harmonizada e segregada, possibilitando que cada grupo de profissionais compreenda seu papel dentro do contexto abrangente na gestão de riscos e controles internos da Entidade.

9.3 Todos os Colaboradores e Dirigentes são responsáveis pelo conjunto de

componentes e arranjos organizacionais na concepção, implementação, monitoramento, comunicação, análise crítica e melhorias contínuas da gestão de riscos. Suas responsabilidades são:

9.3.1 **Órgãos de Governança** – Mantenedor da estrutura de gestão de riscos quanto a:

a) Política de Gestão de Riscos e Controles Internos;

b) Apetite organizacional aos riscos e supervisão do gerenciamento de riscos (incluindo controle interno);

c) Recursos necessários sejam alocados para gerenciar riscos e controles internos;

d) Estruturas e processos para a gestão de riscos e controles internos;

e) Prestação de contas, transparência e monitoramento dos interesses das partes interessas;

f) Cultura de comportamento ético e responsabilidade, demonstrando liderança e comprometimento com o sistema de gestão de riscos e controles internos;

g) Delegação de responsabilidades e de recursos à gestão de riscos e aos controles internos;

h) Supervisão da conformidade com as expectativas legais, regulatórias e éticas.

i) Incorporação de práticas de gestão de riscos e controles internos ao processo decisório;

9.3.2 **Primeira linha** - Gerenciamento e propriedade do risco:

a) Identificação dos riscos dos processos sob sua gestão;

b) Análise e avaliação dos riscos, atribuindo impacto e fontes de risco;

c) Identificação e avaliação da eficácia dos controles aplicados aos riscos;

d) Definição e aplicação de formas de tratamento;

e) Registro tempestivo de riscos concretizados e as alterações de contexto sob sua responsabilidade;

9.3.3 **Segunda linha** - Supervisão dos riscos:

a) Sugestão aos órgãos de governança de métodos e práticas de gestão de riscos

e controles internos, implantando e estruturando as práticas aprovadas;

b) Reporte de informações e movimentações realizadas;

c) Promoção e disseminação da cultura de riscos a implementação de

práticas eficazes de gerenciamento de riscos e controles internos;

d) Gerenciamento de ciclos de avaliações periódicas de riscos em conjunto com as áreas;

e) Monitoramento de indicadores de riscos, auxiliando as primeiras linhas no levantamento/desenvolvimento de soluções, quando aplicável;

f) Consolidação de sistema de gestão de riscos em conformidade com esta

Política e disponibilizar em local apropriado informações referentes à gestão de

riscos e controles internos;

9.4 As responsabilidades específicas dos Órgãos de Governança na gestão de riscos se definem em:

9.4.1 **Conselho Deliberativo:**

a) Definir e monitorar a gestão de riscos, determinando o apetite a riscos, de modo a preservar e agregar valor;

b) Aprovar a Política de Gestão de Riscos e Controles Internos;

c) Acompanhar a evolução dos níveis de riscos e a efetividade das medidas de

controles implementadas e as ações de conformidade;

9.4.2 **Conselho Fiscal:**

a) Supervisionar a conformidade da gestão de riscos e dos controles internos ao

apetite ao risco;

b) Reportar ao Conselho Deliberativo eventuais deficiências identificadas na

gestão de riscos e controles internos;

c) Monitorar o nível de exposição aos riscos, a eficácia dos controles internos e

ações de conformidade adotadas pela Diretoria Executiva.

9.4.3 **Diretoria Executiva:**

a) Executar as diretrizes estabelecidas pelo Conselho Deliberativo;

b) Monitorar os riscos e respectivas medidas de mitigação;

c) Avaliar periodicamente a maturidade da Gestão de Riscos;

e) Promover a cultura organizacional voltada para gestão de riscos, controles internos e conformidade, alocando recursos e patrocinando capacitações.

DISPOSIÇÕES FINAIS

10.1 Periodicidade: deve ser revisada sempre que se fizer necessário, não excedendo o período máximo de 02 (dois) anos.

10.2 Abrangência: esta Política aplica-se aos Dirigentes, Colaboradores e Prestadores de Serviços.

10.3 Divulgação: Esta Política deve ser divulgada nos meios institucionais da FUSESC.

10.4 Vigência: esta Política terá vigência a partir de 01 de julho de 2025.

10.5 Os casos omissos devem ser apreciados pelo Conselho Deliberativo.

Pedro Bramont

Presidente do Conselho Deliberativo