"Se você está lendo este documento em mídia impressa, esta é uma cópia Não-Controlada"

## 1. OBJETIVO

Esta Política tem por objetivo estabelecer os princípios, diretrizes e responsabilidades para o Gerenciamento de Riscos, assegurando sua integração à estratégia, à governança e aos controles internos, de modo a apoiar a tomada de decisão, o alcance dos objetivos institucionais, a proteção e geração de valor e a melhoria contínua, em conformidade com a ABNT NBR ISO 31000:2018.

## 2. DEFINIÇÕES GERAIS

- **Risco:** Efeito da incerteza nos objetivos presentes nas melhores informações da organização, advindas da estratégia, linhas de negócios e áreas corporativas das entidades do Sistema FIEC.]
- **Gestão de Riscos:** atividades coordenadas para dirigir e controlar uma organização no que se refere a riscos.
- **Apetite ao Risco:** É o nível de risco que o Sistema FIEC (FIEC, SESI, SENAI e IEL) está disposto a assumir para alcançar seus objetivos estratégicos.
- **Tolerância ao Risco:** O nível máximo de exposição ao risco que a organização está disposta ou é capaz de suportar.
- **Resposta ao Risco:** Ações adotadas para tratar um risco, visando alterar sua probabilidade ou consequência, remover a fonte de risco, compartilhar, reter ou evitar o risco.
- **Nível de Risco Inerente:** representa o nível de exposição ao risco antes da consideração dos controles existentes e das demais respostas adotadas pela gestão para reduzir a probabilidade de ocorrência e/ou o impacto do evento sobre os objetivos organizacionais. É determinado pela combinação da probabilidade de ocorrência do risco e de seu impacto (consequência). .

Jurandir Francisco Juaçaba Estev
Diretor Administrativo do SFIEC



Livia Souza Sales
Gerente de Compliance SFIEC
Mat. 2628

Natali Cabral Nunes
Gerente SFIEC - SESI
OAB CE 21345

"Se você está lendo este documento em mídia impressa, esta é uma cópia Não-Controlada"

- **Nível de Risco Residual:** é o nível de risco que permanece para a organização após serem considerados os efeitos das respostas adotadas pela gestão para modificar o risco, incluindo controles internos, ações de tratamento, medidas preventivas, detectivas ou corretivas e outras formas de resposta ao risco.
- **Fatores de Risco:** São causas ou situações que podem levar à materialização dos riscos identificados.
- **Controle:** Medidas adotadas que modificam o risco. Os controles incluem quaisquer práticas que modifiquem a inerência do risco.
- **Cultura de riscos:** A cultura de riscos são os valores, princípios, conhecimento e compreensão sobre risco, que é compartilhado por um grupo de pessoas que tem um propósito comum.
- **Proprietário de risco:** pessoa que detém a responsabilidade primária e a autoridade para gerenciar determinado risco, devendo assegurar que o risco seja adequadamente identificado, avaliado e tratado, bem como monitorar sua evolução, a efetividade das respostas adotadas e o respectivo nível de risco residual, promovendo, quando necessário, o escalonamento das situações que excedam os limites de exposição estabelecidos pela organização.

## 2.1. DESCRIÇÃO DAS ATIVIDADES

### 2.1.1. Abrangência

Esta Política aplica-se a todas as entidades, unidades, processos, projetos e atividades do Sistema FIEC, em todos os níveis organizacionais, devendo a gestão de riscos estar integrada à governança, ao planejamento estratégico e à tomada de decisão.

"Se você está lendo este documento em mídia impressa, esta é uma cópia Não-Controlada"

### 2.1.2. Princípios da Gestão de Riscos

A Gestão de Riscos do Sistema FIEC deve observar os princípios estabelecidos pela ABNT NBR ISO 31000 aplicável, estando integrada à governança, ao planejamento, aos processos e à tomada de decisão, de modo a contribuir para o alcance dos objetivos organizacionais, a criação e proteção de valor e a melhoria contínua.

I. **Cria e protege valor:** contribui para o alcance dos objetivos organizacionais e para a criação, proteção e geração de valor.

II. **É parte integrante dos processos organizacionais:** está incorporada às atividades, processos, projetos e iniciativas do Sistema FIEC, não constituindo atividade isolada.

III. **É parte da tomada de decisões:** subsidia decisões estratégicas, táticas e operacionais, considerando os riscos, as oportunidades e seus potenciais efeitos sobre os objetivos.

IV. **Aborda explicitamente a incerteza:** considera a natureza da incerteza e seus possíveis efeitos sobre os objetivos organizacionais.

V. **É sistemática, estruturada e oportuna:** utiliza abordagem organizada, consistente e tempestiva, com metodologia e critérios definidos.

VI. **É baseada nas melhores informações disponíveis:** considera informações relevantes, confiáveis e atualizadas, reconhecendo suas limitações e incertezas.

VII. **É feita sob medida:** considera o contexto, a natureza, a complexidade, os objetivos e as características das entidades, processos e atividades.

VIII. **Considera fatores humanos e culturais:** reconhece a influência de comportamentos, competências, cultura e valores na gestão dos riscos.

IX. **É transparente e inclusiva:** promove a participação e o compartilhamento adequado de informações com as partes interessadas pertinentes.

X. **É dinâmica, interativa e capaz de reagir a mudanças, promovendo a melhoria contínua:** considera alterações nos ambientes interno e externo e



Livia Souza Sales
Gerente de Compliance SFIEC
Mat. 2628

Natali Chimarão Nunes
Gerente GEJUR - SFIEC
OAB CE 21345

"Se você está lendo este documento em mídia impressa, esta é uma cópia Não-Controlada"

responde tempestivamente aos novos riscos, às mudanças nos riscos existentes e às oportunidades de melhoria.

### 2.1.3. Diretrizes da Gestão de Riscos

A Gestão de Riscos do Sistema FIEC deve:

I. estar integrada à governança, ao planejamento estratégico e aos processos de tomada de decisão;
II. observar o apetite a risco e os limites de exposição estabelecidos pela organização;
III. atribuir aos gestores e proprietários dos riscos a responsabilidade pela gestão dos riscos sob sua esfera de atuação;
IV. promover a atuação coordenada entre as instâncias de gestão, a segunda linha e a terceira linha, respeitadas suas respectivas responsabilidades, competências e independência;
V. direcionar esforços para os riscos que possam comprometer de forma relevante o alcance dos objetivos organizacionais;
VI. assegurar o monitoramento e o reporte dos riscos relevantes, especialmente daqueles que apresentem níveis de exposição superiores aos parâmetros estabelecidos; e
VII. promover o fortalecimento contínuo da cultura, da conscientização e da maturidade em gestão de riscos.

### 2.1.4. Estrutura de Governança de Gestão de Riscos

A Gestão de Riscos deve observar o modelo de governança definido pela Organização, assegurando a adequada segregação entre gestão, orientação, monitoramento e avaliação independente.

Livia Souza Sales
Gerente de Compliance SFIEC
Mat. 2628

"Se você está lendo este documento em mídia impressa, esta é uma cópia Não-Controlada"

A responsabilidade pela gestão dos riscos deve permanecer nas áreas e instâncias responsáveis pelos respectivos processos e objetivos, enquanto as funções de segunda e terceira linhas devem atuar de acordo com suas respectivas competências.

A estrutura de governança deve assegurar, no mínimo:

- definição clara de papéis e responsabilidades;
- adequado fluxo de informações sobre riscos;
- supervisão dos riscos relevantes;
- escalonamento de situações que ultrapassem os níveis de exposição estabelecidos;
- acompanhamento da evolução da maturidade em Gestão de Riscos;
- integração entre riscos, controles, Compliance e demais mecanismos de governança.

### 2.1.5. Integração com o Sistema de Governança

A Gestão de Riscos deve atuar de forma integrada com os demais mecanismos de governança, incluindo:

- planejamento estratégico;
- Compliance e Integridade;
- controles internos;
- auditoria interna;
- gestão de processos;
- gestão de projetos;
- segurança da informação e proteção de dados;
- continuidade e gestão de crises;
- gestão de terceiros;
- gestão financeira e orçamentária;
- gestão de pessoas;

Livia Souza Sales
Gerente de Compliance SFIEC
Mat. 2628

"Se você está lendo este documento em mídia impressa, esta é uma cópia Não-Controlada"

- demais funções que possam contribuir para a identificação, avaliação ou tratamento de riscos.

### 2.1.6. Cultura de Riscos

O Sistema FIEC deve promover uma cultura na qual a identificação e a comunicação de riscos sejam compreendidas como parte da responsabilidade de todos.

A Organização deve estimular:

- comportamento ético e responsável;
- comunicação tempestiva de riscos e vulnerabilidades;
- aprendizado a partir de incidentes e ocorrências;
- tomada de decisão consciente quanto aos riscos;
- responsabilização compatível com os papéis exercidos;
- ambiente que favoreça a identificação de riscos sem receio de retaliação pela comunicação de boa-fé.

A cultura de riscos deve estar associada à cultura de integridade e aos valores institucionais do Sistema FIEC.

### 2.1.7. Gestão de Riscos na tomada de decisão

As decisões estratégicas e relevantes da Organização devem, sempre que aplicável, considerar os riscos associados às alternativas avaliadas, seus potenciais impactos, oportunidades, limites de exposição e capacidade de resposta.

A existência de riscos não deve, por si só, impedir a tomada de decisão, devendo ser considerada a relação entre risco, oportunidade, custo, benefício e objetivos institucionais.

Livia Souza Sales
Gerente de Compliance SFIEC
Mat. 2628

"Se você está lendo este documento em mídia impressa, esta é uma cópia Não-Controlada"

### 2.1.8. Apetite e Tolerância a Riscos

O Sistema FIEC deve estabelecer parâmetros de apetite e tolerância ao risco compatíveis com seus objetivos, estratégias, capacidade de gestão e contexto organizacional.

A exposição aos riscos deve ser monitorada em relação aos parâmetros estabelecidos, de modo a orientar as decisões quanto à aceitação, tratamento, monitoramento ou escalonamento dos riscos.

Os critérios, níveis, parâmetros e demais aspectos metodológicos relacionados ao apetite e a tolerância serão definidos em documento específico, aprovado pelo Comitê de Compliance, nos termos previstos na **NP 24 - Novo Regimento Interno do Comitê de Compliance.**

### 2.1.9. Comunicação, Monitoramento e Reporte

A Gestão de Riscos deve assegurar comunicação e reporte tempestivos e adequados sobre os riscos relevantes às instâncias responsáveis pela tomada de decisão.

O monitoramento deve possibilitar a identificação de mudanças no contexto, nos níveis de exposição e na efetividade das respostas adotadas, subsidiando a adoção de medidas necessárias.

Os critérios, periodicidades, instrumentos, fluxos e responsabilidades operacionais de monitoramento e reporte serão estabelecidos em instrumento específico.

### 2.1.10. Gestão de Crises

O comitê de crises é uma estrutura formada para gerir riscos tempestivos, oriundos de casos fortuitos ou forças maiores, que sejam caracterizados de alto impacto, advindos de eventos políticos, sociais, econômicos, legais, ambientais,

"Se você está lendo este documento em mídia impressa, esta é uma cópia Não-Controlada"

tecnológicos ou de natureza interna, que possuam consequências relevantes à imagem da organização. Este é constituído apenas para lidar com eventos dessa natureza.

Tal comitê é regido pela presente Política de Gestão de Riscos, com participação incisiva da direção, comunicação e gestores, a fim de apresentar soluções para tratamentos céleres e efetivos. O comitê deverá:

- Escrever os procedimentos e fornecer alternativas de como tratar o evento imediatamente;
- Executar o fluxo de como tratar cada evento de crise na empresa e fora dela;
- Fazer rapidamente o levantamento de investimentos, se necessário;
- Resolver a crise.

Quando o risco do evento se tornar residual, segue para a base histórica do Compliance e o Comitê de Crises é dissolvido.

### 2.1.11. Disposições Finais

A metodologia, os critérios, procedimentos, instrumentos, fluxos, periodicidades e demais aspectos operacionais da Gestão de Riscos serão estabelecidos no **PC148 – Procedimento de Gestão de Riscos do Sistema FIEC**.

Esta Política deve ser revisada periodicamente ou sempre que houver alterações relevantes no contexto organizacional, na legislação, na regulamentação ou nas referências aplicáveis.

Os casos omissos serão tratados pelas instâncias competentes, observadas as diretrizes de governança do Sistema FIEC.

Luiz Francisco Juaçaba Esteves
Diretor Administrativo do SFIEC

"Se você está lendo este documento em mídia impressa, esta é uma cópia Não-Controlada"

## 2.2. AUTORIDADES E RESPONSABILIDADES

### 2.2.1. Compete à Alta Administração:

I. assegurar o direcionamento e o apoio institucional à Gestão de Riscos;
II. promover a integração da Gestão de Riscos à estratégia, à governança e à tomada de decisão;
III. aprovar ou validar, conforme as competências estabelecidas, o apetite a risco e os limites de exposição;
IV. deliberar sobre riscos relevantes ou situações de exposição que demandem sua atuação; e
V. promover condições para o fortalecimento da cultura de gestão de riscos.

### 2.2.2. Compete ao Comitê de Compliance:

I. Acompanhar a implementação e a evolução da Gestão de Riscos no Sistema FIEC;
II. Apreciar informações consolidadas sobre os riscos relevantes e os respectivos níveis de exposição;
III. Acompanhar os riscos que apresentem exposição superior ao apetite ou aos limites estabelecidos, deliberando ou recomendando as medidas cabíveis, conforme sua competência;
IV. Avaliar questões relevantes relacionadas à Gestão de Riscos e, quando necessário, encaminhá-las à Alta Administração;
V. Acompanhar informações sobre a efetividade das respostas aos riscos e dos controles relevantes; e
VI. Promover o fortalecimento da integração entre Gestão de Riscos, Compliance, governança e demais mecanismos de integridade e controles.

Livia Souza Sales
Gerente de Compliance SFIEC
Mat. 2628

"Se você está lendo este documento em mídia impressa, esta é uma cópia Não-Controlada"

**2.2.3. Compete à Área de Compliance:**

I. Estabelecer orientações e metodologia para a Gestão de Riscos;
II. Prestar suporte técnico às áreas e aos proprietários dos riscos;
III. Monitorar a aplicação das diretrizes e a evolução da Gestão de Riscos;
IV. Realizar avaliação e desafio sobre a adequação das informações, avaliações e respostas apresentadas pelos proprietários dos riscos;
V. Consolidar e reportar informações relevantes sobre riscos às instâncias competentes; e
VI. Promover ações de conscientização e fortalecimento da cultura e da maturidade em Gestão de Riscos.

**2.2.4. Compete à Auditoria Interna:**

I. Fornecer avaliação e asseguração independentes sobre a adequação e efetividade da governança, da Gestão de Riscos e dos controles internos.

**2.2.5. Compete aos Gestores e Proprietários de Riscos**

I. Gerenciar os riscos sob sua esfera de atuação;
II. Assegurar a adequada identificação, avaliação, tratamento e monitoramento dos riscos;
III. Implementar e manter respostas e controles adequados;
IV. Acompanhar a evolução dos riscos e a efetividade das respostas adotadas;
V. Comunicar e escalar tempestivamente situações que possam resultar em exposição superior aos limites estabelecidos;
VI. Avaliar e monitorar continuadamente os riscos associados à contratação de terceiros, fornecedores e parceiros estratégicos no âmbito de suas unidades, exigindo a aplicação de processos de Due Diligência (Devida Diligência) de Integridade e Riscos; e

Livia Souza Sales
Gerente de Compliance SFIEC
Mat. 2528

"Se você está lendo este documento em mídia impressa, esta é uma cópia Não-Controlada"

VII. Fornecer as informações e evidências necessárias ao monitoramento e reporte.

**2.2.6. Compete aos colaboradores em geral**

I. Observar as diretrizes estabelecidas, contribuir para a identificação e comunicação de riscos e apoiar a implementação das medidas aplicáveis.

## 3. LEGISLAÇÃO E DOCUMENTAÇÃO COMPLEMENTAR


- Lei nº 12.846, de 1º de agosto de 2013 - Dispõe sobre a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira, e dá outras providências (Lei Anticorrupção Brasileira).
- Decreto nº 11.129, de 11 de julho de 2022 - regulamenta a Lei nº 12.846/2013.
- INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ISO 31000:2018. 2015b. Disponível em: < https://www.iso.org/standard/43170.html>. Acesso em: 20 de fevereiro de 2018.
- INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ISO 31010:2012. 2015b. Disponível em: https://www.iso.org/standard/51073.html>. Acesso em: 24 de fevereiro de 2018.
- INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ISO 73:2009. 2015b. Disponível em: < https://www.iso.org/standard/44651.html>. Acesso em: 24 de fevereiro de 2018.
- INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA. Guia de orientação para o gerenciamento de riscos corporativos. São Paulo: IBGC, 2007 (série de cadernos de governança corporativa, 3).

"Se você está lendo este documento em mídia impressa, esta é uma cópia Não-Controlada"


- MANUAL METODOLOGIA DE GESTÃO DE RISCOS. Ministério da Transparência e Controladoria Geral da União. Brasília-DF: 2018.
- BRASIL. TRIBUNAL DE CONTAS DA UNIÃO. Roteiro de Avaliação de Maturidade da Gestão de Riscos. Brasília: TCU – Secretaria de Métodos e Suporte ao Controle Externo, 2018.
- NP11 – Política de Compliance.
- NP 13 – Política de Controles Internos.
- PC148 – Gestão de Riscos do Sistema FIEC.


## 4. RECURSOS NECESSÁRIOS

Colaboradores capacitados nas Normas e Políticas que fazem parte do Programa de Compliance, ferramentas de arquivo em meio físico para guarda de documentos.

## 5. CONTROLE DE REGISTROS

| Identificação | Armazenamento | Proteção | Recuperação | Retenção | Disposição |
|---|---|---|---|---|---|
| Não Aplicável | | | | | |

## 6. HISTÓRICO DE ALTERAÇÕES

| Versão | Data de emissão | Descrição da alteração |
|---|---|---|
| 00 | 28/10/2021 | Versão Inicial |
| 01 | 16/11/2022 | **a) Alteração do item 2.1.5.1 – Estabelecimento do contexto, critério e escopo:**<br>- Inclusão da descrição relativa ao critério e ao escopo relativo ao processo de gestão de riscos, com base na ABNT NBR ISO 31.000:2018.<br>**b) Alteração do item 2.1.5.3 – Análise dos riscos:**<br>- Alteração do quadro referente a escala de probabilidade em consonância com o que preconiza o Roteiro de Avaliação de |

"Se você está lendo este documento em mídia impressa, esta é uma cópia Não-Controlada"

| | | |
|---|---|---|
| | | Maturidade da Gestão de Riscos, do Tribunal de Contas da União (TCU).<br>- Alteração do quadro referente a escala de consequência, em consonância com o que preconiza o Roteiro de Avaliação de Maturidade da Gestão de Riscos, do Tribunal de Contas da União (TCU).<br>- Inclusão da escala para classificação de níveis de risco, em consonância com o que preconiza o Roteiro de Avaliação de Maturidade da Gestão de Riscos, do Tribunal de Contas da União (TCU).<br>- Inclusão do quadro de avaliação do desenho e implementação dos controles (atributos do controle), em consonância com o que preconiza o Roteiro de Avaliação de Maturidade da Gestão de Riscos, do Tribunal de Contas da União (TCU).<br>- Inclusão da matriz de risco residual, em consonância com o que preconiza o Roteiro de Avaliação de Maturidade da Gestão de Riscos, do Tribunal de Contas da União (TCU).<br>**c) Alteração do item 2.1.5.4 – Avaliação de riscos:**<br>- Inclusão do quadro critérios para priorização e tratamento de riscos, em consonância com o que preconiza o Roteiro de Avaliação de Maturidade da Gestão de Riscos, do Tribunal de Contas da União (TCU).<br>**d) Alteração do item 2.1.5.5 - Tratamento dos riscos:**<br>- Retirada da classificação de tratamento dos riscos inerentes.<br>**e) Alteração do texto do item 2.1.5.6 - Monitoramento e Análise Crítica.**<br>**f) Alteração do texto do item 2.1.5.7 - Comunicação e Consulta.**<br>**g) Inclusão do item 2.1.5.8 – Registro e Relato.**<br>**h) Inclusão de informações no item 3. Legislação e Documentação Complementar.** |
| 02 | 19/10/2026 | **a) Alteração do item 1. Objetivo:**<br>**- Ajuste de redação.** |

"Se você está lendo este documento em mídia impressa, esta é uma cópia Não-Controlada"

| | | |
|---|---|---|
| | | **b) Alteração do item 2. Definições Gerais:**<br>**- Ajustes nos conceitos indicados.**<br>**c) Alteração do item 2.1. Descrição das atividades:**<br>**- Ajuste nos itens para contemplar os princípios, diretrizes, estrutura e cultura de gestão de riscos.**<br>**d) Alteração no item 2.2. Autoridades e Responsabilidades:**<br>**- Ajuste nas atribuições de todos os stakeholders envolvidos.** |

## 7. APÊNDICE

- Não Aplicável

Cientifique-se e cumpra-se.

Fortaleza, 19 de outubro de 2026.

**José Ricardo Montenegro Cavalcante**
Presidente da FIEC
Presidente do Conselho Regional do SENAI/DR-CE
Diretor Regional do SESI/DR-CE
Diretor-Presidente do IEL/CE
Condômino do Condomínio Edifício Casa da Indústria

Livia Souza Sales
Gerente de Compliance SFIEC
Mat. 2628

"Se você está lendo este documento em mídia impressa, esta é uma cópia Não-Controlada"

**Paulo André de Castro Holanda**

Diretor Regional do SENAI/DR-CE

Superintendente Regional do SESI/DR-CE

Condômino do Condomínio Edifício Casa da Indústria