1. OBJETIVO

Esta política tem por objetivo estabelecer princípios, diretrizes e responsabilidades a serem observados no processo de Gerenciamento de Riscos (GR), de forma a possibilitar a adequada identificação, análise, avaliação, controle, monitoramento, análise crítica, melhoria contínua, comunicação e consulta, nos termos da ABNT NBR ISO 31.000:2018.

2. DEFINIÇÕES GERAIS

- GR: Gerenciamento de Riscos
- SGC: Sistema de Gestão de Compliance
- Risco: Efeito da incerteza nos objetivos presentes nas melhores informações da organização, advindas da estratégia, linhas de negócios e área corporativa das entidades do Sistema FIEC.
- Riscos Corporativos: Abrange os principais eventos de riscos advindos das áreas de apoio das entidades do Sistema FIEC, que impactam nas atividades previstas nas linhas de negócio e na estratégia da Organização.
- Riscos Estratégicos: Representa a possibilidade de ocorrência de restritivos ante a execução de atividades previstas do Mapa Estratégico e dos processos das linhas de negócio. Podem acarretar impeditivos na execução das atividades dos núcleos de operações das entidades, bem como falhas em processos gerenciais, sistemas e infraestruturas.
- Riscos de Compliance: São riscos oriundos das obrigações de compliance.
- Atitude Perante ao Risco: É o nível de risco que o Sistema FIEC (FIEC, SESI, SENAI e IEL) se sujeita a aceitar na realização prioritária dos controles para a execução dos riscos. Atualmente, está aprovado pela direção que todo e qualquer risco acima do nível médio deverá receber especial atenção nos procedimentos de controle.
- Nível de Risco: Relacionamento entre as probabilidades e as consequências de um risco se materializar.

- Fatores de Risco: São causas que levam à materialização dos riscos identificados.
- Critérios de risco: São direcionamentos decisórios para cada nível de risco, aplicado mediante a aprovação da direção da organização.
- Controle: Medidas adotadas que modificam o risco. Os controles incluem quaisquer práticas que modifiquem a inerência do risco.
- Critérios de controles: São direcionamentos que atestam a eficácia do controle aplicado, a cada risco avaliado.
- 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. Por meio dela, são identificados os elementos culturais adversos ou conflitantes e formas para tratamentos. A maturidade do processo de avaliação de riscos é conquistada mediante a prática constante da organização, para dirimir vieses de interpretação, mediante comunicação e consulta a todas as partes interessadas.
- Proprietário de risco: O proprietário responsabiliza-se pelo risco inerente, até que o mesmo seja transformado em residual, incluindo seu monitoramento pós execução de controles. Porém, o proprietário apenas gerencia o risco, não se responsabiliza por quaisquer problemas legais, nem financeiros que possam estar atrelados ao risco.

2.1. DESCRIÇÃO DAS ATIVIDADES

2.1.1. Apresentação

O Sistema FIEC busca assegurar o mais alto nível de integridade e ética em suas atividades. Para tal, promove ações de prevenção e controle fundadas em seu Sistema de Gerenciamento de Riscos.

O Sistema de Gestão de Compliance (SGC) do Sistema FIEC está fundado na manutenção de uma estrutura formal, com uma instância responsável, na determinação de normas e políticas e padrões de Gerenciamento de Riscos e

Controles Internos, no treinamento e na comunicação, e também no processo de monitoramento e suporte à Ouvidoria, através do Canal de Denúncias para avaliação e apuração de potenciais desvios de conduta ou procedimentos estabelecidos, por meio de investigações internas.

2.1.2. Abrangência

Aplica-se ao Sistema FIEC (FIEC, SESI, SENAI e IEL), as atividades de Gerenciamento de Riscos (GR) que impactam no seu ambiente, de acordo com as diretrizes do Planejamento Estratégico vigente, obrigações de compliance, processos operacionais, assim como a organização das atividades corporativas e projetos das linhas de negócio.

A presente Política de Gestão de Riscos está alinhada e subordinada às diretrizes da Política de Compliance da organização.

2.1.3. Princípios da Gestão de Riscos

Para a garantia dos objetivos estratégicos, o Gerenciamento de Riscos (GR) das entidades do Sistema FIEC possui, de acordo com a ABNT NBR ISO 31.000:2018, dez princípios que norteiam a efetividade de ações.

As entidades que compõem o Sistema FIEC farão o uso desses princípios para tratar riscos, pois são diretrizes que nortearão as ações previstas na Política de Gestão de Riscos:

Cria e protege valor: A organização adota o Gerenciamento de Riscos (GR) como parte integrante da tomada de decisões, o que possibilita a criação de valor para o ambiente organizacional, na medida que reconhece as incertezas que permeiam suas atividades gerenciais diárias.

Parte integrante dos processos organizacionais: A organização toma o Gerenciamento de Riscos (GR) como parte integrante dos processos organizacionais a partir da promulgação desta política.

Parte da tomada de decisões: A organização executa o Gerenciamento de Riscos (GR) como parte da tomada de decisões estratégicas, corporativas, dos processos das linhas de negócio e atividades operacionais, com a execução de reuniões pelo Comitê de Compliance, a fim de acompanhar as atividades de controle especificadas nos riscos mapeados pelas áreas/setores/unidades, bem como o acompanhamento dos orçamentos aprovados para gestão de riscos.

Aborda explicitamente a incerteza: As áreas/setores/unidades do Sistema FIEC (FIEC, SESI, SENAI e IEL) buscam identificar riscos, de forma que aborde explicitamente as incertezas em toda atividade de planejamento.

Sistemática, estruturada e oportuna: A organização tem no Gerenciamento de Riscos (GR) uma ferramenta para oportunizar discussões, de forma estruturada e sistemática por meio da metodologia aplicada, reconhecida internacionalmente pela sua efetividade.

Baseada nas melhores informações disponíveis: A organização utiliza as melhores informações de gestão disponíveis, oriundas do desenvolvimento dos objetivos estratégicos presentes no mapa, bem como das operações das linhas de negócio e da área corporativa, para estruturar o acompanhamento dos riscos identificados.

Feita sob medida: A organização utiliza as diretrizes presentes na ABNT NBR ISO 31.000:2018 para ajustar de forma adequada o Gerenciamento de Riscos (GR) nas suas atividades diárias.

Considera fatores humanos e culturais: A organização considera, para fins de desenvolvimento do Gerenciamento de Riscos (GR), as questões humanas e culturais presentes nas atividades do seu dia a dia e promove a melhoria contínua de suas ações, com o objetivo de promover um ciclo constante de melhorias para promover a eficiência do Gerenciamento de Riscos (GR).

Transparente e inclusiva: A organização publica, de forma transparente e inclusiva, todas as ações tomadas para identificar riscos e diminuir a criticidade dos mesmos, a todas as partes interessadas, incluindo seus colaboradores.

Dinâmica, interativa, capaz de reagir a mudanças e promover a melhoria contínua da organização: A organização utiliza o Gerenciamento de Riscos (GR) para envolver todos os colaboradores em busca do alcance das diretrizes traçadas no planejamento, provendo condições para o desenvolvimento perene das ações e estabelecer meios de reação a mudanças que porventura possam existir de forma segura e confortável a todos os envolvidos.

2.1.4. Estruturação da Gestão de Riscos

A abordagem das três linhas de defesa, embora não seja um modelo de gestão de riscos, é uma forma simples e eficaz para melhorar a comunicação e a conscientização sobre os papeis e as responsabilidades essenciais de gestão de riscos e controles. De acordo com essa abordagem, há três grupos (ou linhas) envolvidos no gerenciamento eficaz de riscos, como explanado a seguir:

Primeira linha de defesa: São funções que gerenciam e têm propriedade de riscos. A gestão operacional e os procedimentos rotineiros de riscos e controles internos constituem a primeira linha de defesa na gestão de riscos. A gestão operacional serve naturalmente como a primeira linha de defesa porque os controles internos são desenvolvidos como sistemas e processos sob sua orientação e responsabilidade. Nesse nível se identificam, avaliam e tratam riscos por meio do

desenvolvimento e da implementação de normas, políticas e procedimentos que possam oferecer garantia razoável de que as atividades estejam de acordo com as metas e objetivos.

Segunda linha de defesa: São funções que implementam o gerenciamento de riscos. A segunda linha de defesa é constituída por comitês ou outras estruturas organizacionais estabelecidas para garantir que a primeira linha funcione como pretendido no que diz respeito à gestão e controle de riscos. Seu papel é coordenar as atividades de gestão de riscos, orientar e monitorar a implementação das práticas de gestão de riscos por parte da gestão operacional, apoiar a definição de metas de exposição a risco, monitorar riscos específicos (de compliance, por exemplo), bem como ajudar a definir controles e/ ou monitorar riscos e controles da primeira linha de defesa.

Terceira linha de defesa: São funções que fornecem avaliações independentes. A auditoria interna constitui a terceira linha de defesa na gestão de riscos ao fornecer avaliações independentes e objetivas sobre os processos de gestão de riscos, controles internos e governança aos órgãos de governança e à alta administração. Tais avaliações devem abranger uma grande variedade de objetivos (incluindo eficiência e eficácia das operações; salvaguarda de ativos; confiabilidade e integridade dos processos de reporte; conformidade com leis e regulamentos) e elementos da estrutura de gestão e controle de riscos em todos os níveis da estrutura organizacional da entidade.

Embora a instância máxima de governança e a alta administração não sejam consideradas entre as três linhas de defesa desse modelo, nenhuma consideração sobre o Gerenciamento de Riscos (GR) estaria completa sem levar em consideração, em primeiro lugar, os papéis essenciais dessas que são as principais partes interessadas e as que estão em melhor posição para instituir e assegurar o bom funcionamento das linhas de defesa no processo de gestão de riscos e controles da organização. A alta administração é a responsável maior pela gestão de

riscos e a ela cabe estabelecer, avaliar, direcionar e monitorar o sistema de gestão de riscos e controle interno, bem como assegurar que os gestores implementem práticas de gestão de riscos e controle interno, no âmbito da instituição.

Órgãos de controle externo, reguladores, auditores externos e outras instâncias externas de governança estão fora da estrutura da organização, devendo desempenhar o controle externo na estrutura geral de governança, fornecendo avaliações tanto às partes interessadas externas da organização, como às instâncias internas de governança e à alta administração da entidade.

Transversalmente, a área jurídica permeia todas as linhas de defesa, captura, interpreta e analisa impactos de leis e regulamentos, bem como auxilia na aprovação da execução de treinamentos em temas de Compliance/Gerenciamento de Riscos (GR), junto às áreas e colaboradores da instituição. As atribuições de todas as funções das linhas de defesa estão discriminadas no item "Autoridades e Responsabilidades".

2.1.5. Processo de Gestão de Riscos

As entidades do Sistema FIEC adotam um modelo de processo de Gerenciamento de Riscos (GR), seguindo as diretrizes da norma ABNT NBR ISO 31.000:2018. O fluxo de processo e seu procedimento operacional padrão (**PC148 – Gestão de Riscos do Sistema FIEC**) estão sob responsabilidade da área de compliance. Compreende as seguintes etapas:

2.1.5.1. Estabelecimento do contexto, critério e escopo

É imprescindível que o escopo das atividades de gestão de riscos, definido pelo Sistema FIEC, esteja em completo alinhamento com os objetivos organizacionais.
Para isso, o processo organizacional e seus objetivos são analisados considerando os seus ambientes interno e externo, incluindo todos os documentos que de alguma

forma influenciem no processo de gestão estratégica das entidades do Sistema FIEC.

O estabelecimento do contexto do Gerenciamento de Riscos (GR) deve seguir os seguintes passos:

- Utilizar o Mapa Estratégico vigente para identificar riscos que possam afetar o alcance dos objetivos/resultados (pessoas, sistemas informatizados, estruturas organizacionais, recursos, partes interessadas, dentre outros);

- Utilizar informações de contexto interno, advindas da gestão dos processos corporativos, das obrigações de compliance, das linhas de negócio e da gestão dos processos operacionais das Unidades de Negócios.

Além disso, é salutar a especificação da quantidade e do tipo de risco que a Instituição pode ou não assumir com relação aos objetivos, estabelecendo critérios para avaliar a significância dos riscos, sendo conveniente o seu estabelecimento no início do processo de avaliação de riscos, devendo ser continuamente analisados e alterados, se necessário, em razão de sua dinamicidade.

2.1.5.2. Identificação dos Riscos

Os eventos em potencial que podem gerar consequências à organização devem ser identificados de acordo com os objetivos presentes no planejamento das entidades do Sistema FIEC, uma vez que esses possíveis eventos, gerados por fontes internas ou externas, afetam a realização desses objetivos.

Durante o processo de identificação de eventos, estes poderão caracterizar riscos. O objetivo é produzir uma lista abrangente de riscos, que possam ter um impacto na consecução dos objetivos identificados na etapa de "Estabelecimento do contexto, critério e escopo".

São formas que facilitam a identificação dos riscos:

- Quais eventos podem EVITAR o atingimento de um ou mais objetivos do processo organizacional?
- Quais eventos podem ATRASAR o atingimento de um ou mais objetivos do processo organizacional?
- Quais eventos podem PREJUDICAR o atingimento de um ou mais objetivos do processo organizacional?
- Quais eventos podem IMPEDIR o atingimento de um ou mais objetivos do processo organizacional?

Os eventos identificados inicialmente podem ser analisados e revisados, reorganizados, reformulados e até eliminados nesta etapa, e, para tanto, podem ser utilizadas as seguintes questões:

- O evento analisado é um risco que pode comprometer claramente um objetivo do processo?
- O evento analisado é um risco ou uma falha no desenho do processo organizacional?
- À luz dos objetivos do processo organizacional, o evento analisado é um risco ou uma causa potencial para um risco?
- O evento analisado é um risco ou uma fragilidade em um controle para tratar um risco de um processo?

Para fins de agrupamento dos riscos identificados, deve-se discriminar seu tipo, da seguinte forma:

Estratégico: Riscos que possam comprometer o atingimento dos objetivos estratégicos, vinculados ao Mapa Estratégico do Sistema FIEC, associados aos Projetos Estratégicos;

Operacional: Riscos que possam comprometer as atividades das entidades do Sistema FIEC, normalmente associados a falhas, deficiência ou inadequação de processos internos, pessoas, infraestrutura e sistemas;

Financeiro: Riscos que possam comprometer a capacidade das entidades do Sistema FIEC de contar com os recursos orçamentários e financeiros necessários à realização de suas atividades ou eventos que possam comprometer a própria execução orçamentária;

TI: A gestão de risco em TI evita desperdício de recursos, bem como potencializa a efetividade de processos, garantindo que ações preventivas sejam feitas sempre que forem necessárias à saúde de uma empresa. Além disso, permite criar uma estratégia para gerir os riscos envolvidos na falha de sistemas críticos ou de segurança.

Compliance: Riscos relacionados à corrupção, fraudes, irregularidades e/ou desvios éticos e de conduta que podem comprometer os valores e padrões preconizados pelas entidades do Sistema FIEC, na realização de seus objetivos. O Código de Ética e Conduta serve de base regulatória para tal fim, e está vinculado diretamente à **NP11 - Política de Compliance**.

2.1.5.3. Análise dos Riscos

A análise de riscos fornece uma compreensão sobre os riscos presentes nas entidades do Sistema FIEC. Envolve a apreciação das causas potenciais e fontes de risco, suas consequências positivas e negativas, e também a probabilidade de que essas consequências possam ocorrer. O nível de risco é mensurado, mediante a matriz formada entre a probabilidade e a consequência (impacto) de cada risco traçado na identificação.

O Sistema FIEC utiliza-se de escalas qualitativas de probabilidade e de consequência que têm uma amplitude de cinco níveis. Os quadros abaixo demonstram as escalas, respectivamente:

a) Escala de Probabilidades

PROBABILIDADE	DESCRIÇÃO DA PROBABILIDADE, DESCONSIDERANDO OS CONTROLES	PESO
Muito baixa	**Improvável**. Em situações excepcionais, o evento poderá até ocorrer, mas nada nas circunstâncias indica essa possibilidade.	**1**
Baixa	**Rara**. De forma inesperada ou casual, o evento poderá ocorrer, pois as circunstâncias pouco indicam essa possibilidade.	**2**
Média	**Possível**. De alguma forma, o evento poderá ocorrer, pois as circunstâncias indicam moderadamente essa possibilidade.	**5**
Alta	**Provável**. De forma até esperada, o evento poderá ocorrer, pois as circunstâncias indicam fortemente essa possibilidade.	**8**
Muito alta	**Praticamente certa**. De forma inequívoca, o evento ocorrerá, as circunstâncias indicam claramente essa possibilidade.	**10**

Fonte: 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

b) Escala de Consequências

CONSEQUÊNCIA	DESCRIÇÃO DA CONSEQUÊNCIA NOS OBJETIVOS , CASO O EVENTO OCORRA	PESO
Muito baixo	**Mínimo** impacto nos objetivos (estratégicos, operacionais, de informação/comunicação/divulgação ou de conformidade).	**1**
Baixo	**Pequeno** impacto nos objetivos (idem).	**2**
Médio	**Moderado** impacto nos objetivos (idem), porém recuperável.	**5**
Alto	**Significativo** impacto nos objetivos (idem), de difícil reversão	**8**
Muito alto	**Catastrófico** impacto nos objetivos (idem), de forma irreversível.	**10**

Fonte: 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.

O resultado final do processo de análise de riscos será o de atribuir, para cada risco identificado, uma classificação tanto para a probabilidade como para a consequência (impacto) do evento, cuja combinação determinará o nível do risco inerente.

O nível de risco inerente (NRI) de um evento é o nível de risco antes da consideração das respostas que a gestão adota, incluindo controles internos, para reduzir a probabilidade do evento e ou sua consequência (impactos) nos objetivos. Resulta na combinação da probabilidade com a consequência (impacto).

NRI=NP X NC

Em que:

NRI = nível de risco inerente

NP = nível de probabilidade do risco

NC = nível de consequência (impacto) do risco

ESCALA PARA CLASSIFICAÇÃO DE NÍVEIS DE RISCO			
RB (Risco Baixo)	**RM** (Risco Médio)	**RA** (Risco Alto)	**RE** (Risco Extremo)
0 - 9,99	**10 - 39,99**	**40 - 79,99**	**80 - 100**

Os resultados dos cálculos da multiplicação da probabilidade versus a consequência, classificados de acordo com a escala de níveis de risco, podem ser expressos em uma matriz, da seguinte forma:

MATRIZ DE RISCO

IMPACTO						
10 Muito Alto	10 Risco Médio	20 Risco Médio	50 Risco Alto	80 Risco Extremo	100 Risco Extremo
8 Alto	8 Risco Baixo	16 Risco Médio	40 Risco Alto	64 Risco Alto	80 Risco Extremo
5 Médio	5 Risco Baixo	10 Risco Médio	25 Risco Médio	40 Risco Alto	50 Risco Alto
2 Baixo	2 Risco Baixo	4 Risco Baixo	10 Risco Médio	16 Risco Médio	20 Risco Médio
1 Muito baixo	1 Risco Baixo	2 Risco Baixo	5 Risco Baixo	8 Risco Baixo	10 Risco Médio
	1 **Muito baixa**	**2** **Baixa**	**5** **Média**	**8** **Alta**	**10** **Muito alta**
	PROBABILIDADE				

Fonte: Adaptado da Gestão de Riscos – Avaliação da Maturidade (TCU, 2018), Metodologia de Gestão de Riscos - (CGU, 2018) e Modelo_Matriz_de_Riscos.xlsx (CGU, 2020).

A análise de riscos só se completa quando as ações que a gestão adota para respondê-los são também avaliadas, chegando-se ao nível de risco residual, o risco que remanesce depois de considerado o efeito das respostas adotadas pela gestão para reduzir a probabilidade e/ou o impacto dos riscos, incluindo controles internos e outras ações.

A avaliação das respostas a riscos e atividades de controle correspondentes – ou simplesmente controles – é parte integrante da análise de riscos.

Os controles incluem qualquer processo, política, dispositivo, prática ou outras ações e medidas que a gestão adota com o objetivo de modificar o nível de risco inerente (ABNT NBR ISSO 31.000:2018).

Uma forma de avaliar o efeito dos controles na mitigação de riscos consiste em determinar um nível de confiança (NC), mediante análise dos atributos do desenho e da implementação dos controles, utilizando a escala abaixo:

NÍVEL DE CONFIANÇA (NC)	AVALIAÇÃO DO DESENHO E IMPLEMENTAÇÃO DOS CONTROLES (ATRIBUTOS DO CONTROLE)	RISCO DO CONTROLE (RC)
Inexistente NC = 0% (0,0)	Controles inexistente, mal desenhados ou mal implementados, isto é, não funcionais	**Muito Alto 1,0**
Fraco NC = 20% (0,2)	Controles têm abordagens ad hoc, tendem a ser aplicados caso a caso, a responsabilidade é individual,havendo elevado grau de confiança no conhecimento das pessoas	**Alto 0,8**
Mediano NC = 40% (0,4)	Controles implementados mitigam alguns aspectos do risco, mas não contemplam todos os aspectos relevantes do risco devido a deficiências no desenho ou nas ferramentas utilizadas.	**Médio 0,6**
Satisfatório NC = 60% (0,6)	Controles implementados e sustentados por ferramentas adequadas e, embora passíveis de aperfeiçoamento, mitigam o risco satisfatoriamente.	**Baixo 0,4**
Forte NC = 80% (0,8)	Controles implementados podem ser considerados a "melhor prática", mitigando todos os aspectos relevantes do risco.	**Muito Baixo 0,2**

Fonte: 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

Quadro 11: Níveis de Avaliação dos Controles Internos Existentes		
Nível	Descrição	Fator de Avaliação dos Controles
Inexistente	Controles inexistentes, mal desenhados ou mal implementados, isto é, não funcionais.	1
Fraco	Controles têm abordagens ad hoc, tendem a ser aplicados caso a caso, a responsabilidade é individual, havendo elevado grau de confiança no conhecimento das pessoas.	0,8
Mediano	Controles implementados mitigam alguns aspectos do risco, mas não contemplam todos os aspectos relevantes do risco devido a deficiências no desenho ou nas ferramentas utilizadas.	0,6
Satisfatório	Controles implementados e sustentados por ferramentas adequadas e, embora passíveis de aperfeiçoamento, mitigam o risco satisfatoriamente.	0,4
Forte	Controles implementados podem ser considerados a "melhor prática", mitigando todos os aspectos relevantes do risco.	0,2

Fonte: Gestão de Riscos – Avaliação da Maturidade (TCU, 2018, adaptado)

Uma vez determinado o nível de confiança (NC), pode-se determinar o risco de controle (RC), isto é, a possibilidade de que os controles adotados pela gestão não sejam eficazes para prevenir, detectar e permitir corrigir, em tempo hábil, a ocorrência de eventos que possam afetar adversamente a realização de objetivos. O RC é definido como complementar ao NC.

Uma vez estabelecido o RC, é possível estimar o nível de risco residual (NRR), ou seja, o risco que permanece após o efeito das respostas adotadas pela gestão, incluindo controles internos e outras ações, para reduzir a probabilidade e ou o impacto do evento. Para isso, deduz-se do nível de risco inerente (NRI) o percentual de confiança (NC) atribuído ao controle, o que equivale a multiplicar o NRI pelo RC, utilizando a seguinte fórmula:

NRR = NRI x RC

Em que:

NRR = nível de risco residual

NRI = nível de riscos inerente

RC = risco de controle

Os resultados dos cálculos da multiplicação do nível de risco inerente versus o risco do controle, podem ser expressos em uma matriz de riscos residuais que tem o propósito de demonstrar o efeito dos controles (RC) sobre os riscos inerentes (NRI), da seguinte forma:

MATRIZ DE RISCO						
NÍVEL DE RISCO INERENTE (NRI)	100 Extremo	20 RM	40 Risco Alto	60 Risco Alto	80 Risco Extremo	100 Risco Extremo
	80 Extremo	16 Risco Médio	32 Risco Médio	48 Risco Alto	64 Risco Alto	80 Risco Extremo
	50 Alto	10 Risco Médio	20 Risco Médio	30 Risco Médio	40 Risco Alto	50 Risco Alto
	25 Médio	5 Risco Baixo	10 Risco Médio	15 Risco Médio	20 Risco Médio	25 Risco Médio
	8 Baixo	2 Risco Baixo	3 Risco Baixo	5 Risco Baixo	6 Risco Baixo	8 Risco Baixo
		0,2 Muito baixo	**0,4 Baixo**	**0,6 Médio**	**0,8 Alto**	**1 Muito alto**
		RISCO DE CONTROLE (RC)				

Fonte: Adaptado da Gestão de Riscos – Avaliação da Maturidade (TCU, 2018), Metodologia de Gestão de Riscos - (CGU, 2018) e Modelo_Matriz_de_Riscos.xlsx (CGU, 2020).

A análise de riscos fornece uma entrada para a avaliação de riscos, para decisões sobre se o risco necessita ser tratado e como, sobre a estratégia e os métodos mais apropriados para o tratamento de riscos.

2.1.5.4. Avaliação de Riscos

A finalidade da avaliação de riscos é auxiliar na tomada de decisões com base nos resultados da análise de riscos, sobre quais riscos necessitam de tratamento e a prioridade para a implementação do tratamento.

Compreende a identificação e a análise dos riscos relevantes que comprometam o atendimento dos objetivos das entidades, formando uma base para determinar como os riscos devem ser gerenciados.

Nesse escopo, foi sugerida uma avaliação de riscos qualitativa trabalhada numa matriz de Gerenciamento de Riscos, proporcionando um mecanismo para tratamento de riscos. Consequentemente, é uma ferramenta de direcionamento dos esforços para tratar os riscos quantificar melhor a estrutura de controles internos.

Uma boa prática para apoiar o processo de avaliação de riscos é estabelecer critérios para priorização e tratamento associados aos níveis de risco, conforme o quadro abaixo:

a) Diretrizes para priorização e tratamento de riscos

NÍVEL DE RISCO	CRITÉRIOS PARA PRIORIZAÇÃO E TRATAMENTO DE RISCOS
Risco Extremo	Nível de risco muito além do apetite a risco. Qualquer risco nesse nível deve ser comunicado à governança e alta administração e ter uma resposta imediata. Postergação de medidas só com autorização do dirigente máximo
Risco Alto	Nível de risco além do apetite a risco. Qualquer risco nesse nível dever ser comunicado a alta administração e ter uma ação tomada em período determinado. Postergação de medidas só com autorização do dirigente de área
Risco Médio	Nível de risco dentro do apetite a risco. Geralmente nenhuma medida especial é necessária, porém requer atividades de monitoramento específicas e atenção da gerência na manutenção de respostas e controles para manter o risco nesse nível, ou reduzi-lo sem custos adicionais.
Risco Baixo	Nível de risco dentro do apetite a risco, mas é possível que existam oportunidades de maior retorno que podem ser exploradas assumindo-se mais riscos, avaliando a relação custos x benefícios, como diminuir o nível de controles.

Fonte: 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

2.1.5.5. Tratamento dos Riscos

O tratamento de riscos envolve a seleção de uma ou mais opções para modificar o nível do risco (a probabilidade ou o impacto) e a elaboração de planos de tratamento que, uma vez implementados, implicarão a introdução de novos controles ou a modificação dos existentes. Um dos benefícios da gestão de riscos é exatamente o rigor que proporciona ao processo de identificação e seleção de alternativas de respostas aos riscos.

Segundo a ISO 31000, (2018 p. 19) *"o tratamento de riscos envolve a seleção de uma ou mais opções para modificar os riscos e a implementação dessas opções. Uma vez implementado, o tratamento fornece novos controles ou modifica os existentes".*

A implementação dos planos de ação para tratamento dos riscos compreende atividades específicas que visam transformar quaisquer riscos inerentes em riscos residuais.

Os orçamentos propostos para cada risco avaliado devem ser inseridos nesse momento, para posterior aprovação das alçadas, cujo procedimento específico está instruído no mapeamento do processo de riscos.

2.1.5.6. Monitoramento e Análise Crítica

As atividades de monitoramento de riscos compreendem planos elaborados para assegurar que as diretrizes e os objetivos, definidos pelas entidades do Sistema FIEC, para minimizar os riscos, estão sendo observados nas atividades executadas.

As atividades de monitoramento ocorrem em todos os níveis das entidades e abrangem atividades como aprovações, autorizações, limites de alçada, verificações, reconciliações, revisões de performance operacional, segurança de ativos e segregação de funções e será executada pelo Controle Interno.

O Controle Interno executa o monitoramento e solicita as entregas previstas pelos agentes (responsáveis) de risco, de acordo com a periodicidade definida pela área de Compliance.

A análise crítica é executada pela área de Compliance que referendará com o Comitê de Compliance as ações previstas para o tratamento de riscos, numa

periodicidade trimestral, em especial com relação àqueles que forem classificados acima da atitude perante aos riscos.

As principais atividades de monitoramento incluem conciliações, acompanhamento de comunicações de agentes externos e internos, inventários, autoavaliações e verificação contínua, bem como a avaliação constante da matriz de riscos, com intuito de fortalecer ainda mais as Entidades, em busca da melhoria contínua.

2.1.5.7. Comunicação e Consulta

A forma e o prazo em que as informações relevantes são identificadas, colhidas e comunicadas permite que as partes interessadas cumpram com suas atribuições. Para identificar, avaliar e responder ao risco, a organização necessita das informações em todos os níveis hierárquicos.

A comunicação eficaz ocorre quando esta flui na organização em todas as direções e quando os colaboradores recebem informações claras quanto às suas funções e responsabilidades.

O propósito da comunicação e consulta é auxiliar as partes interessadas pertinentes na compreensão do risco, na base sobre a qual decisões são tomadas e nas razões pelas quais ações específicas são requeridas.

A comunicação busca promover a conscientização e o entendimento do risco, enquanto a consulta envolve obter retorno e informação para auxiliar a tomada de decisão.

Convém que uma coordenação estreita entre as duas facilite a troca de informações factuais, oportunas, pertinentes, precisas e compreensíveis, levando em consideração a confidencialidade e integridade da informação, bem como os direitos de privacidade dos indivíduos.

2.1.5.8. Registro e Relato

O processo de gestão de riscos e seus resultados devem ser documentados e relatados por meio de mecanismos apropriados.

Nos termos da ANBT NBR ISO 31.000:2018*, "o registro e o relato visam:*

a) comunicar atividades e resultados de gestão de riscos em toda a organização;

b) fornecer informações para a tomada de decisão;

c) melhorar as atividades de gestão de riscos;

d) auxiliar a interação com as partes interessadas, incluindo aquelas com responsabilidade e com responsabilização por atividades de gestão de riscos."

2.1.6. Comitê 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, 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.

2.2. AUTORIDADES E RESPONSABILIDADES

2.2.1 Responsabilidades das áreas com relação ao Gerenciamento de Riscos (GR)

COMITÊ DE COMPLIANCE

✓ Deliberar com relação ao nível de Atitude Perante ao Risco na condução dos negócios;

- ✓ Propor alterações e revisões na Política de Gestão de Riscos e demais normativos relacionados ao tema;
- ✓ Referendar os relatórios de Compliance;
- ✓ Propor a aplicação de recursos para tratamentos de Riscos,
- ✓ Buscar o alinhamento da cultura da organização com a Política de Gestão de Riscos;
- ✓ Buscar o alinhamento dos objetivos da Gestão de Riscos com os objetivos e estratégias da organização;
- ✓ Analisar e propor sugestões para o aperfeiçoamento dos processos de Gestão de Riscos;
- ✓ Sugerir o líder do Comitê de Crises;
- ✓ Validar os relatórios de monitoramento da gestão da matriz de riscos;
- ✓ Recomendar a realização de treinamentos e atualizações;
- ✓ Participar da atualização da gestão de riscos a ser realizada por cada área, em caso de reestruturação com consequente alterações de competências;
- ✓ Efetuar outras análises e propor outras medidas que entender cabíveis;
- ✓ Acompanhar a matriz de Riscos do Sistema FIEC.

ÁREA DE COMPLIANCE

- ✓ Monitorar os processos chaves e críticos, verificando, através de suas revisões periódicas, se os controles praticados pelos proprietários de riscos atendem às necessidades de controle do processo;
- ✓ Informar ao Comitê de Compliance sobre os resultados dos controles estabelecidos para cada um dos riscos identificados nos processos, na forma de um relatório trimestral;
- ✓ Reportar aos gestores as falhas observadas, oferecendo recomendações para saná-las;
- ✓ Intensificar ações que promovam a melhoria do Gerenciamento de Riscos (GR) do Sistema FIEC;

✓ Buscar proteger os ativos, analisar dados contábeis, com o apoio da Gerência de Contabilidade do SFIEC, ajudando a gestão na condução ordenada do negócio da Instituição;

✓ Prevenir, sempre que possível, antecipadamente o acontecimento de erros, desperdícios, abusos, práticas antieconômicas, fraudes e negociações internas com informações privilegiadas (*insider trading*);

✓ Propiciar informações oportunas e confiáveis, inclusive de caráter administrativo e operacional, sobre os resultados e efeitos atingidos;

✓ Apoiar a implementação de programas, projetos, atividades, sistemas e operações, visando à eficiência, eficácia e economia de recursos;

✓ Gerenciar o Processo de Avaliação e Monitoramento de Riscos;

✓ Monitorar os desdobramentos dos controles de riscos e relacionar os níveis e os fatores de avaliação dos controles existentes;

✓ Controlar os tempos de execução dos planos de ação para residualização dos riscos pelos proprietários;

✓ Monitorar os recursos destinados ao tratamento dos riscos, a partir do que foi estipulado pelos proprietários de riscos;

✓ Validar a inserção de riscos residuais propostos à operação das entidades para os processos de Gerenciamento de Riscos, levando em consideração sua relevância;

✓ Propor ao Comitê de Compliance o nível de Atitude Perante ao Risco das entidades.

AGENTE (RESPONSÁVEL) DE CONTROLE

✓ Informar e executar os planos de ação referente aos controles atribuídos a cada risco;

✓ Identificar as ações propostas e defendê-las junto ao Controle Interno;

✓ Definir a residualidade dos riscos inerentes sob sua responsabilidade;

✓ Executar as ações dentro do orçamento proposto;

✓ Modificar e propor novos controles, a partir da classificação realizada pelo Controle Interno;

AUDITORIA

✓ Auditar controles que geraram inconformidades e sugerir a implementação de ações referentes ao Gerenciamento de Riscos (GR);

✓ Revisar de forma independente aspectos operacionais e financeiros relativos ao Gerenciamento de Riscos (GR);

✓ Avaliar de forma independente os controles do Gerenciamento de Riscos (GR);

✓ Realizar a Auditoria Baseada em Riscos dos controles;

JURÍDICO

✓ Capturar, interpretar e analisar impactos de leis e regulamentos na gestão de riscos;

✓ Participar, quando necessário, da execução de treinamentos em temas de Compliance.

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).
- 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.
- NP 15 – Política de *Due Diligence* de Integridade de Terceiros.
- PC148 – Gestão de Riscos do Sistema FIEC.
- PC150 – *Due Diligence* de Integridade de Terceiros
- Políticas, Normas, Procedimentos e Portarias correlatas 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: - 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. **b) Alteração do item 2.1.5.3 – Análise dos riscos:** **-** - Alteração do quadro referente a escala de probabilidade em consonância com o que preconiza o Roteiro de Avaliação de Maturidade da Gestão de Riscos, do Tribunal de Contas da União (TCU). **-** 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). - 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). - 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). - 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). **c) Alteração do item 2.1.5.4 – Avaliação de riscos:** **-** 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). **d) Alteração do item 2.1.5.5 - Tratamento dos riscos:** **-** Retirada da classificação de tratamento dos riscos inerentes. **e) Alteração do texto do item 2.1.5.6 - Monitoramento e Análise Crítica.** **f) Alteração do texto do item 2.1.5.7 - Comunicação e Consulta.**

		g) Inclusão do item 2.1.5.8 – Registro e Relato. **h) Inclusão de informações no item 3. Legislação e Documentação Complementar.**

7. APÊNDICE

- Não Aplicável

Cientifique-se e cumpra-se.

Fortaleza, 16 de novembro de 2022.

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

Paulo André de Castro Holanda
Diretor Regional do SENAI/DR-CE
Superintendente Regional do SESI/DR-CE
Condômino do Condomínio Edifício Casa da Indústria