Título:

POLÍTICA DE GESTÃO DE RISCOS DE COMPLIANCE

Revisão	Data	Histórico da Revisão
00	07/02/2024	Emissão Inicial.

Elaborado por	Verificado por	Aprovado por
Ana Cristina Carvalho Gerente Jurídico	Marco Aurélio Vargas Danemberg Diretor Superintendente	Marcelo Noto Bonilha Diretor Presidente

ÍNDICE:

1. Objetivo

A EBSE está inserida em um ambiente de negócio cada vez mais complexo e em constantes mudanças, o que impõe o desafio de se adaptar continuamente, de forma acelerada e com elevado grau de sucesso.

Estar preparada para as incertezas é a única forma de evitar ser surpreendida por situações repentinas e sobre as quais não se tem controle, em qualquer ramo de atividade econômica, em especial nas entidades do terceiro setor, cujos serviços e entregas dependem da sociedade.

A atuação da EBSE envolve riscos relacionados a incertezas que pode impactar no alcance de resultados e no cumprimento da missão e na imagem institucional, bem como, na segurança das pessoas.

Uma abordagem estruturada e sistemática de gestão de riscos, em nível institucional, além de ser uma importante ferramenta de governança, aumenta a capacidade da EBSE em lidar com incertezas, aprimora a transparência organizacional e contribui para o uso eficiente, eficaz e efetivo dos recursos.

A presente política de gestão de riscos faz parte do Programa de Integridade da EBSE e é fruto do trabalho desenvolvido no Planejamento Estratégico e o primeiro documento institucional produzido para formalizar o processo sistematizado de gestão de riscos.

2. Aplicabilidade

A Política de Gestão de Riscos de Compliance se aplica a todos os diretores, e profissionais da EBSE, além dos que a representam em suas subsidiárias, aos consultores, aos distribuidores, aos agentes e aos prestadores de serviços independentes, ainda que temporários, que além de cumpri-la deverá alavancar seu aprimoramento.

3. Definições e Siglas

Não aplicável.

4. Documentos de Referência

4.1 Documentos Externos

Lei 12.846/2013 – lei anticorrupção de 01/08/2013.
Decreto Regulamentador nº 11.129/2022

4.2 Documentos Internos

POP.COMP.001 - Procedimento do Comitê Diretivo de Compliance
POP.COMP.002 - Código de Conduta e Ética Empresarial
POP.COMP.003 - Procedimento de canais de Comunicações e Denúncia
POP.COMP.004 - Procedimento de Apuração de Denúncias
POP.COMP.005 - Política de Anticorrupção
POP.COMP.006 - Política de Relacionamento Externo
POP.COMP.007 - Política de Compras de Materiais e Serviços
POP.COMP.008 - Política Gestão de Compliance
POP.COMP.009 - Procedimento de Treinamento de Compliance
POP.COMP.010 - Procedimento de Gestão de Fornecedores – Terceiros

5. Finalidade

Incorporar a visão de riscos à tomada de decisões estratégicas, em conformidade com as regulamentações aplicáveis e as melhores práticas de mercado, estabelecendo princípios, diretrizes, processos e responsabilidade na gestão de riscos da EBSE, primordialmente, no que tange à identificação e tratamento dos riscos que possam afetá-la, e estabelecendo controles e procedimentos de monitoramento para a efetiva criação, proteção, crescimento do valor institucional, cumprimento integral da sua missão e aprimoramento dos mecanismos de controles internos.

6.Sistemática

6.1 Princípios fundamentais desta política:

a) **A gestão de riscos deve ser coerente ao Planejamento Estratégico** e à cadeia de valor da EBSE, bem como, ser sistemática, racional, transparente, dinâmica, interativa, adaptável a mudanças e considerar também o risco como oportunidade de melhoria;

b) **Os riscos devem ser considerados em todas as decisões** e sua gestão deve ser realizada de maneira integrada em todos os processos da instituição, em diferentes níveis, respeitadas as normas internas;

c) **A gestão de riscos deve considerar, explicitamente, as incertezas, a natureza dessas incertezas**, e como elas podem ser tratadas;

d) **As ações de resposta devem considerar as possíveis consequências de curto, médio e longo prazos** e devem ser priorizadas de acordo com a agregação ou preservação de valor para a EBSE e a sociedade;

e) **A Equipe de Gestão de Riscos**, estrutura que fica dentro da Gerência Jurídica, deve assegurar a eficácia do gerenciamento dos riscos por meio de revisões frequentes, favorecendo o cumprimento dos seus objetivos.

6.2. Conteúdo

6.2.1 Diretrizes Gerais

As diretrizes apresentadas nesta Política definem e caracterizam macro etapas do processo de gestão de riscos.

A implementação da gestão de riscos deve tratar prioritariamente os processos e decisões de maior criticidade e relevância estratégica, tendo as deliberações do Planejamento Estratégico como principal instrumento norteador.

É responsabilidade de todos os colaboradores atuar de forma integra, preservar valores éticos, bem como com a disseminar a cultura de gestão de riscos da EBSE de forma a contribuir para uma gestão eficaz.

6.3 O processo de gestão de riscos

O processo de gestão de riscos fortalece a imagem da EBSE e encoraja a gestão proativa na cultura da instituição.

Figura 01: Processo de gestão de riscos da EBSE

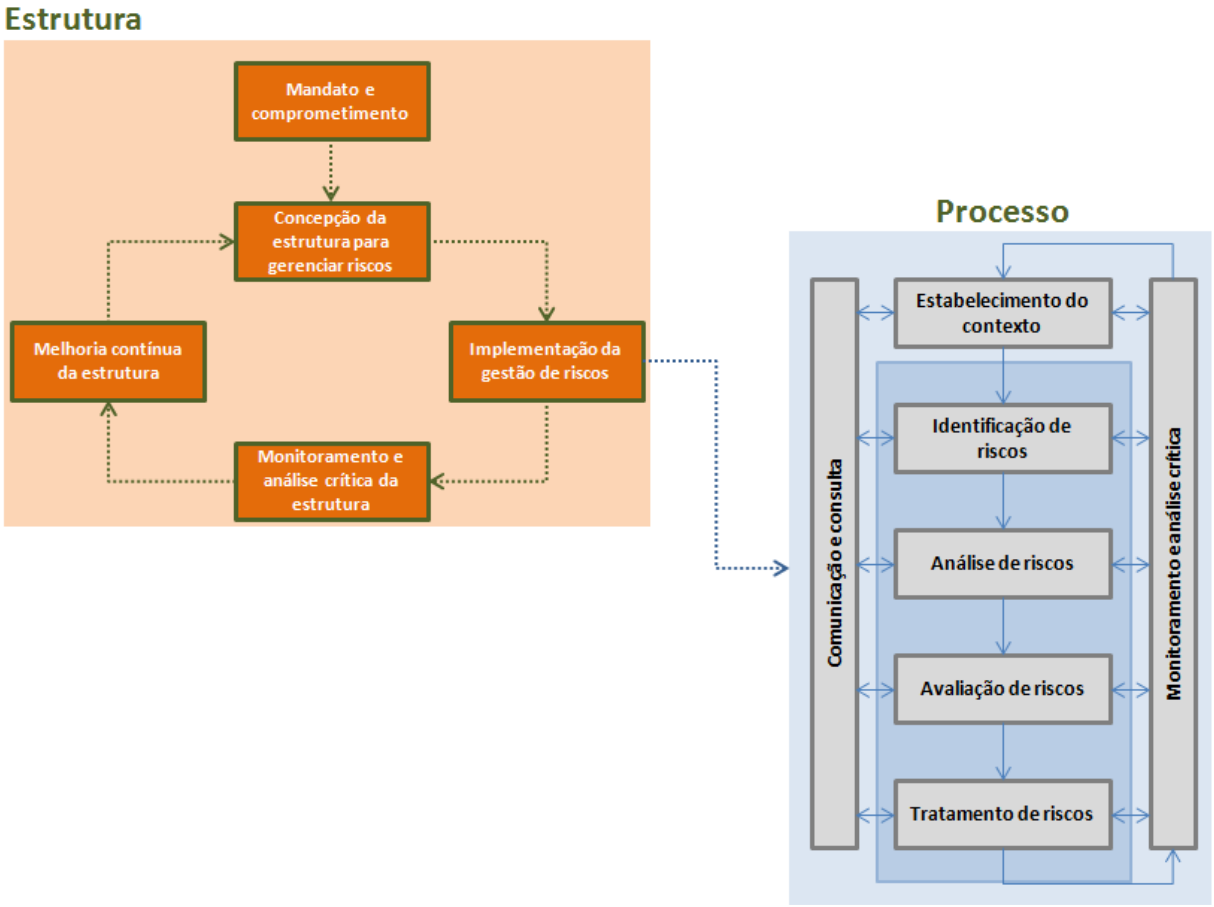
	ETAPAS	DESCRIÇÃO
1	Estabelecimento do contexto	Etapa de identificação e definição dos parâmetros internos e externos a serem levados em consideração ao gerenciar riscos e ao estabelecimento do escopo e das categorias de riscos;
2	Identificação de riscos	Etapa de busca, reconhecimento e descrição de riscos, mediante a identificação das fontes, eventos, suas causas e as consequências potenciais. Possui como produto uma lista abrangente de riscos baseada nos eventos que possam criar, aumentar, evitar, reduzir, acelerar ou atrasar a realização dos objetivos da Fiotec;
3	Análise de riscos	Etapa de desenvolvimento da compreensão sobre o risco e a determinação do nível do risco. Nesta etapa são elaborados os mapas de riscos. Envolve a apreciação das causas e das fontes de risco, suas consequências positivas e negativas, e a probabilidade de que essas consequências possam ocorrer.
4	Avaliação de riscos	Etapa de comparação entre o nível de risco encontrado, durante a etapa de análise, com o limite de tolerância estabelecido pela instituição. Nesta etapa são elaborados os planos 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. Compara o nível de risco encontrado durante o processo de análise com os critérios de risco estabelecidos quando o contexto foi considerado.
5	Tratamento	Etapa de implementação de uma ou mais ações para modificar o nível do risco, ou seja, é a execução dos planos de riscos.
6	Monitoramento	Etapa de verificação, supervisão, observação crítica ou identificação da situação de risco, realizadas de forma contínua, é nesta etapa que são elaborados os relatórios de riscos.
7	Comunicação	Etapa de comunicação contínua com as partes interessadas, que ocorre durante todas as etapas do processo de gestão de riscos.

A estrutura para garantir a avaliação e tratamento dos riscos, doravante denominada Equipe de Gestão de Riscos, deverá estruturar e garantir a existência de um processo desenhado para avaliação, monitoramento e direcionamento da gestão de riscos.

Ficará a cargo da Equipe de Gestão de Riscos garantir o estabelecimento do contexto (universo, apetite e tolerância), a comunicação e consulta junto às partes interessadas e por fim o monitoramento e análise crítica de todo o processo.

As etapas de identificação, análise, avaliação e tratamento dos riscos de TI ficarão sob a responsabilidade das áreas internas da EBSE, que deverão utilizar como norte a direção fornecida pela Equipe de Gestão de Riscos. Já as etapas de identificação, análise, avaliação e tratamento dos riscos corporativos ficarão sob a responsabilidade da Gerência Jurídica conforme a necessidade

O macroprocesso se utiliza da estrutura que será a apresentada pela ISO31000, representada logo abaixo:



6.4 Introdução ao processo de avaliação de riscos

Todos os colaboradores nomeados pela Equipe de Gestão de Riscos terão autonomia para identificar e reportar riscos para a Equipe de Gestão de Riscos, para isto bastará utilizar os artefatos que serão apresentados neste documento.

Importante registrar que todo evento de risco ocorrido deve ser reportado imediatamente para a Equipe de Gestão de Riscos.

Outra possibilidade de identificação de riscos será através da construção de cenários de riscos. Estes visam identificar possíveis falhas futuras e com isso garantir o seu tratamento de forma preventiva.

6.5 Processo de registro, aprovação e tratamento de risco

O processo de registro, aprovação e tratamento de risco será composto por três etapas, conforme a seguir:

Na primeira etapa onde ocorre o registro do risco serão considerados os fatores de risco envolvidos e a categorização do evento. Em seguida serão levantados e analisados dados históricos relevantes para a avaliação de impacto e probabilidade visando classificar o grau do risco. Nesta fase de análise deverá constar também as ações de tratamento do risco propostas acompanhadas da estimativa de custo-benefício de cada uma.

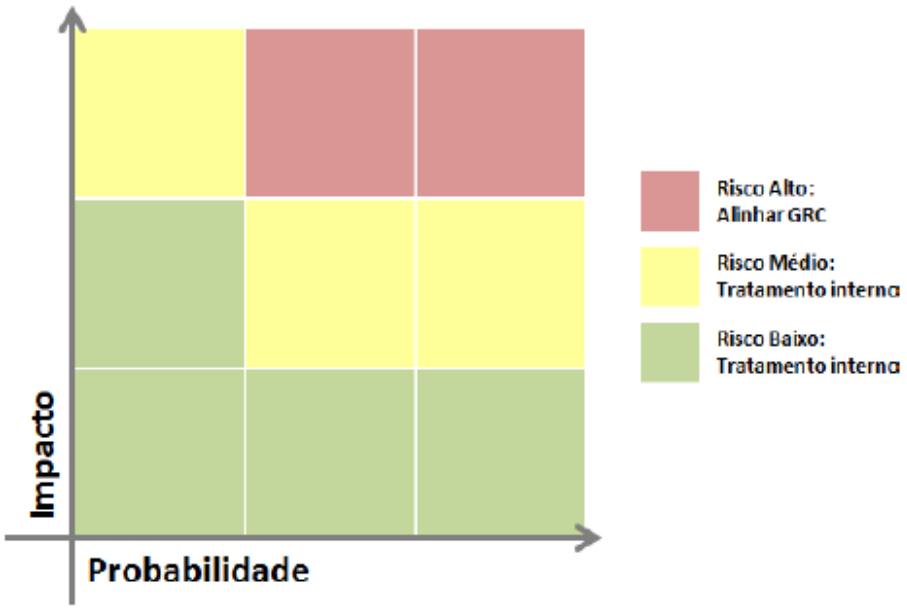
6.6 Probabilidade do risco

Para concluir a classificação do grau do risco será necessário cruzar o impacto do risco com a probabilidade de ocorrência do evento em questão. Para calcular esta probabilidade será atribuído pela Equipe de Gestão de Riscos uma pontuação com as seguintes classificações:
Probabilidade de ocorrência podem ser: Muito Alta, Alta, Média, Baixa e Muito baixa.

CLASSIFICAÇÃO DA PROBABILIDADE POR EVENTO	
CLASSIFICACÃO	**DESCRIÇÃO**
1-Remoto	Menos de uma vez por ano
2-Improvável	Uma vez por ano
3-Possível	Uma vez por semestre
4-Provável	Uma vez por mês
5-Quase Certo	Uma vez por semana ou mais

6.7 Grau do risco

Após a avaliação do impacto e do cálculo da probabilidade do risco basta cruzar estas duas informações, conforme a matriz abaixo, para obter o grau do risco. De acordo com este grau calculado será definido o envolvimento da Diretoria como também a alçada de aprovação do tratamento deste evento.



6.8 Tratamento do risco

Por fim, o tratamento do risco conforme a estratégia definida. Os Riscos identificados e classificados conforme as estratégias citadas acima: Evitar, Mitigar, Compartilhar e Aceita, devem ser registradas e as ações de tratamentos serão registradas na ferramenta de controle de documentos pela Comitê Diretivo de Compliance e acompanhados pela parte interessada

Devendo sempre seguir as seguintes etapas: planejamento da ação, execução da ação e encerramento da ação, com a devida apresentação da evidência de avaliação da eficácia da ação implementada, e da devida verificação do risco residual remanescente do tratamento realizado.

O tratamento do risco pode ser: Treinamentos para todos os colaboradores ou para grupos específicos, cancelamento de contratos ou qualquer outra ação que mitigue o risco

OBSERVAÇÃO: Se o risco residual ainda for considerado alto, podem ser feitas outras rodadas de avaliação de novas ações para mitigar o risco.

6.9 Planos de ação

Será de responsabilidade do Comitê diretivo de Compliance a consolidação dos planos de ação e acompanhamento das ações corretivas oriundas das análises e tratamento de riscos, bem como da avaliação da eficácia da ação de implementação.

7. Considerações de Qualidade, Segurança, Meio Ambiente e Saúde

Para executar as atividades que constam neste procedimento, o colaborador deverá estar integrado à Política de QSMS da empresa, seguindo as normas e procedimentos de Qualidade, Meio Ambiente, Saúde Ocupacional e Segurança do Trabalho. Além disso, deve, conforme aplicável:

- Estar autorizado a executar as atividades aqui descritas;
- Receber treinamento prévio quanto às atividades a exercer;
- Possuir a capacitação técnica legal pertinente (caso aplicável);
- Seguir as orientações de segurança e utilizar EPI adequados para a realização das atividades;
- Interromper suas atividades em casos de riscos graves e iminentes;
- Gerenciar resíduos conforme procedimentos internos pertinentes;
- Atender às normas e procedimentos pertinentes a emergências.

8. Registros

Não se aplica.

9. Anexos

9.1. Planilha de riscos de Compliance

Título:

POLÍTICA DE GESTÃO DE RISCOS DE COMPLIANCE