Título:

POLÍTICA DE GESTÃO DE RISCOS DE COMPLIANCE I INTEGRIDADE

Revisão	Data	Histórico da Revisão
00	07/02/2024	Emissão Inicial.
01	28/10/2024	Revisão - itens alterados face criação Conselho Consultivo da empresa
02	30/04/2026	Revisão geral

ÍNDICE:

Elaborado por	Verificado por	Aprovado por
ANA CRISTINA DA SILVA ALVES DE CARVALHO Assinado de forma digital por ANA CRISTINA DA SILVA ALVES DE CARVALHO Dados: 2026.05.06 12:31:00 -03'00'	HENRIQUE CORDEIRO GONCALVES:10348758766 Assinado de forma digital por HENRIQUE CORDEIRO GONCALVES:10348758766 Dados: 2026.05.12 09:41:04 -03'00'	MARCELO NOTO BONILHA:92731660759 Assinado de forma digital por MARCELO NOTO BONILHA:92731660759 Dados: 2026.05.08 09:01:13 -03'00'
Ana Cristina Carvalho Compliance Officer	Henrique Cordeiro Gonçalves Diretor Superintendente	Marcelo Noto Bonilha Diretor Presidente

1. Objetivo

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 Política de Gestão de Riscos de Compliance/Integridade da EBSE tem por finalidade estabelecer princípios, diretrizes, responsabilidades e metodologias para a identificação, análise, avaliação, tratamento, monitoramento e revisão dos riscos relacionados à integridade, corrupção, suborno e não conformidades regulatórias.

A gestão de riscos de compliance visa:

- prevenir, detectar e responder a riscos de suborno, fraude e corrupção;
- apoiar a tomada de decisão estratégica da Alta Direção;
- proteger a reputação institucional da EBSE;
- fortalecer os mecanismos de governança, controles internos e integridade organizacional;
- garantir a melhoria contínua da Gestão Antissuborno.

Nenhum objetivo comercial, pressão competitiva ou meta financeira justifica a exposição da empresa a riscos de corrupção ou suborno.

2. Aplicabilidade

A Política de Gestão de Riscos de Compliance I Integridade se aplica a todos os gestores, e profissionais da EBSE, acionistas, mas principalmente ao Comitê Diretivo de Compliance I Integridade, 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

Código Civil Brasileiro

Código Penal Brasileiro

ISO 31.000:2023 (Gestão de Risco)

ISO 37.001:2025 (Sistema de Gestão Antissuborno)

ISO 37.301:2021 (Sistema de Gestão de Compliance)

Lei nº 12.846/13 (Lei Anticorrupção) - Decreto Regulamentador 11.129/2022

Lei nº 13.303/16 (Lei das Estatais)

Lei nº 13.709/18 (Lei Geral de Proteção de dados)

Lei nº 14.133/21 (Nova Lei de Licitações)

Lei nº 9.613/98 (Lei da Lavagem de Dinheiro)

4.2 Documentos Internos

POP.COMP.001 – Procedimento do Comitê Diretivo de Compliance I Integridade

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 I Antissuborno

POP.COMP.006 - Política de Relacionamento Externo (Brindes, Entretenimento etc.)

POP.COMP.007 - Política de Compras de Materiais e Contratação de Serviços

POP.COMP.008 - Política Gestão de Compliance I Integridade

POP.COMP.009 - Procedimento de Treinamento de Compliance I Integridade

POP.COMP.010 - Procedimento de Gestão de Fornecedores – Terceiros

POP.COMP.011- Política de Gestão de Riscos de Compliance I Integridade

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 da Gestão de Riscos de Compliance/Integridade

A gestão de riscos da EBSE observará os seguintes princípios:

- Integridade – tolerância zero à corrupção e suborno.
- Transparência – decisões e registros auditáveis.
- Prestação de contas (Accountability) – responsabilização formal pelas decisões.
- Equidade – tratamento justo às partes interessadas.

- Supervisão eficaz – monitoramento permanente do programa de integridade.
- Melhoria contínua – revisão periódica do sistema de gestão.

Estes princípios estão alinhados aos fundamentos da ISO 37000 – Governança Organizacional e às diretrizes do Programa de Integridade da EBSE.

6.2 Estrutura de Governança da Gestão de Riscos

A gestão de riscos de compliance será conduzida pela seguinte estrutura organizacional:

Alta Direção

- Aprovar esta política;
- Garantir recursos para a gestão de riscos;
- Avaliar periodicamente o desempenho do sistema.

Comitê Diretivo de Compliance

- supervisionar a gestão de riscos;
- validar classificação de riscos moderados, altos e críticos;
- monitorar planos de mitigação;
- reportar resultados à Alta Direção.

Compliance Officer

- coordenar o processo de avaliação de riscos;
- manter atualizado o Mapa de Riscos de Compliance/Integridade;
- monitorar indicadores e planos de ação;
- assegurar alinhamento com a ISO 37001.

Gestores das áreas

- identificar riscos em seus processos;
- implementar controles internos;
- comunicar riscos ao Comitê de Compliance/Integridade.

6.3 Princípios fundamentais desta política:

a) **A gestão de riscos deve ser coerente ao Planejamento Estratégico** e à cadeia de valores 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 do Comitê Diretivo de Compliance/Integridade, deve assegurar a eficácia do gerenciamento dos riscos por meio de revisões frequentes, favorecendo o cumprimento dos seus objetivos.

6.4. Conteúdo/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.

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.

6.5 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.

O processo de gestão de riscos da EBSE seguirá as seguintes etapas:

a) Estabelecimento do contexto
b) Identificação dos riscos
c) Análise dos riscos
d) Avaliação e priorização
e) Tratamento e mitigação
f) Monitoramento
g) Revisão periódica

Este processo será aplicado a todas as áreas da empresa, especialmente aquelas com maior exposição a riscos de integridade, tais como:

- área comercial;
- área de suprimentos;
- relacionamento com agentes públicos;
- contratação de fornecedores e terceiros;
- execução de contratos;
- participação em licitações.

Ficará a cargo do Comitê Diretivo de Compliance/Integridade 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 da área de Planejamento Corporativo da EBSE, que deverá utilizar como norte a direção fornecida pelo Comitê Diretivo de Compliance/Integridade. Já as etapas de identificação, análise, avaliação e tratamento dos riscos corporativos ficarão sob a responsabilidade do Comitê Diretivo de Compliance/Integridade conforme a necessidade.

6.6 Introdução ao processo de avaliação de riscos

Todos os colaboradores nomeados pelo Comitê Diretivo de Compliance I Integridade terão autonomia para identificar e reportar 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 Comitê Diretivo de Compliance I Integridade.

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.

A identificação de riscos deverá considerar, entre outros:

- riscos de suborno;
- riscos de fraude;
- conflitos de interesse;
- relacionamento com agentes públicos;
- contratação de terceiros;
- processos de compras e licitações;
- pagamentos e controles financeiros;
- relacionamento externo e institucional.

A identificação poderá ocorrer por meio de:

- auditorias internas;
- análise de denúncias recebidas;
- avaliações de fornecedores;
- revisões de processos;
- reuniões do Comitê de Compliance.

6.7 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.

6.8 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 pelo Comitê Diretivo de Compliance I Integridade 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

6.9 Classificação 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.

Os riscos de compliance serão classificados conforme:

Classificação	Descrição
Baixo	impacto limitado, controlado por procedimentos existentes
Médio	impacto moderado, requer monitoramento
Alto	risco relevante com potencial impacto reputacional ou financeiro
Crítico	risco de suborno, corrupção ou responsabilização legal

Os riscos classificados como alto ou crítico deverão ser submetidos à análise do Comitê Diretivo de Compliance.

6.10 Mapa de Riscos de Compliance

A EBSE manterá atualizado um Mapa de Riscos de Compliance, contendo:

- descrição do risco;
- área responsável;
- probabilidade;
- impacto;
- nível de risco;
- controles existentes;
- plano de ação;
- responsável pela mitigação.

O Mapa de Riscos deverá ser:

- atualizado anualmente;
- revisado sempre que houver mudança significativa nos processos;
- apresentado ao Comitê Diretivo de Compliance/Integridade.

Esta medida atende aos requisitos de avaliação de riscos de suborno previstos na ISO 37001.

6.11 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 I Integridade 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

As respostas aos riscos poderão incluir:

- implementação de controles internos adicionais;
- revisão de procedimentos;
- treinamento específico;
- reforço de due diligence de terceiros;
- revisão contratual;
- auditorias específicas.

Todos os riscos classificados como alto ou crítico deverão possuir plano de mitigação formal.

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

6.12 Planos de ação

Será de responsabilidade do Comitê Diretivo de Compliance I Integridade 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.

6.13 Monitoramento e Revisão

A gestão de riscos deverá ser monitorada continuamente por meio de:

- indicadores de desempenho;
- auditorias internas;
- revisões do Comitê de Compliance;
- análise de denúncias;
- avaliações de fornecedores.

A revisão do mapa de riscos ocorrerá no mínimo uma vez por ano, ou sempre que ocorrer:

- mudança relevante na legislação;
- alteração significativa nos processos;
- ocorrência de incidentes relevantes.

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

Identificação	F-015 – Ata de Reunião
Armazenamento	Armário I Rede
Proteção	Armário I Rede
Recuperação	Ordem cronológica
Tempo de Retenção	05 anos
Descarte	Picotar I Reciclar I Deletar
Identificação	F-035 – Plano de Ação
Armazenamento	Armário I Rede
Proteção	Armário I Rede
Recuperação	Ordem cronológica
Tempo de Retenção	05 anos
Descarte	Picotar I Reciclar I Deletar
Identificação	F-218 – Planilha de Gerenciamento de Riscos e Oportunidades
Armazenamento	Armário I Rede
Proteção	Armário I Rede
Recuperação	Ordem cronológica
Tempo de Retenção	05 anos

Descarte	Picotar I Reciclar I Deletar
Identificação	Mapa de Riscos de Compliance
Armazenamento	Rede
Proteção	Rede
Recuperação	Ordem cronológica
Tempo de Retenção	05 anos
Descarte	Deletar
Identificação	Indicadores de Monitoramento
Armazenamento	Rede
Proteção	Rede
Recuperação	Ordem cronológica
Tempo de Retenção	05 anos
Descarte	Deletar

9. Anexos

9.1. Planilha de riscos de Compliance

9.1. Planilha de riscos de Compliance

COMPLIANCE AVALIAÇÃO DE RISCOS - MÊS / ANO

ID.	IDENTIFICAÇÃO			AVALIAÇÃO DO RISCO INERENTE			AVALIAÇÃO DE CONTROLES		AVALIAÇÃO DO RISCO RESIDUAL			GESTÃO DOS RISCOS			
	FATOR DE RISCO	PROCESSO AFETADO	ÁREA AFETADA	PROBABILI-DADE	IMPACTO	RISCO INERENTE	CONTROLES EXISTENTES	NÍVEL DE CONTROLE	PROBABILI-DADE	IMPACTO	RISCO RESIDUAL	MEDIDA	AÇÃO	RESPONSÁVEL	PRAZO