1. OBJETIVOS

O objetivo desta política é estabelecer as intenções, diretrizes e preceitos para implantação e gerenciamento de riscos da AeC.

2. CAMPO DE APLICAÇÃO

Este documento se aplica a todos aqueles que integram os quadros da AeC, sejam acionistas ou colaboradores, em todos os níveis hierárquicos, bem como para terceiros que agem em nome, interesse ou benefício da AeC.

3. REFERÊNCIAS

Código de Conduta AeC
Committee of Sponsoring Organizations of the Treadway Commission – Enterprise Risk Management (COSO-ERM)
ABNT NBR ISO 31000:2018 - Gestão de riscos — Diretrizes
ABNT NBR ISO 31073:2022 - Gestão de riscos — Vocabulário
REG-007 Controle de Documentos
POL 002 – Política de Segurança da Informação
POL 022 – Política Geral de Privacidade e Manuseio de Dados Pessoais
ABNT NBR ISO/IEC 27001:2022 - Sistema de gestão da segurança da informação - Requisitos
ABNT NBR ISO/IEC 27002:2022 - Código de prática para controles de segurança da informação
ABNT NBR ISO/IEC 27701:2019 - Técnicas de segurança — Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação — Requisitos e diretrizes
ABNT NBR ISO/IEC 27005:2019 – Técnicas de Segurança – Gestão de riscos de segurança da informação
Lei 12.965, de 23/4/2014 - Marco Civil da Internet.
Lei 13.709, de 14/08/208 – Lei Geral de Proteção de Dados.

4. DEFINIÇÕES

- ***Risco:*** *efeito da incerteza nos objetivos. Um efeito é um desvio em relação ao esperado. Pode ser positivo, negativo ou ambos, e pode abordar, criar ou resultar em oportunidades e ameaças.*
- ***Gestão de risco:*** *atividades coordenadas para dirigir e controlar uma organização no que se refere a riscos.*
- ***Apetite ao risco:*** *é a quantidade e tipo de risco que uma organização está disposta a buscar, reter ou assumir;*
- ***Matriz de Riscos:*** *ferramenta para classificar e apresentar riscos definindo faixas para consequência e probabilidade. A matriz de riscos é um organismo em constante evolução, atualizada e possui no mínimo os campos: risco, processo, probabilidade e impacto do risco inerente, probabilidade e impacto do risco residual, controles, frequências dos controles, entre outros.*
- ***Risk Owner:*** *pessoa ou entidade com a responsabilização e a autoridade para gerenciar riscos. É o proprietário do risco, responsável pelo gerenciamento dos riscos de suas operações, capaz de estabelecer e gerir os controles e planos de ação;*

- ***Control Owner:*** *É o colaborador responsável por identificar os riscos juntamente com a gestão dos riscos e executar, testar e fornecer periodicamente evidências das atividades de controle.*

5. CONTEÚDO

5.1 PREMISSAS E RESTRIÇÕES

A analise, avaliação e tratamento dos riscos é realizada por equipes de acordo com o assunto definido:

TIPO DE RISCO	*RESPONSÁVEL PELA AVALIAÇÃO*
Riscos de Segurança Da Informação	*Departamento de Segurança da Informação (GRC)*
Riscos de Privacidade de Dados	*Departamento de Privacidade de Dados*
Riscos Corporativos	*Departamento de Gestão de Riscos*

6. PAPÉIS E RESPONSABILIDADES

O gerenciamento de riscos não é um evento isolado de responsabilidade de uma única área. Faz parte do primeiro pilar do Sistema de Gestão da AeC e, por isso, requer o engajamento de todas as áreas da empresa, devendo ser realizado em todos os níveis (estratégico, tático e operacional).

A identificação dos riscos será realizada sempre que necessário e a reavaliação dos riscos será realizada no mínimo a cada 12 meses.

Abaixo, os papéis e responsabilidades dos principais agentes do processo de gestão de riscos na AeC.

6.1 Risk Owners (donos do risco)

São os diretores, executivos e gerentes responsáveis imediatos pelos riscos, membros da primeira linha de defesa da gestão de riscos, entre suas principais responsabilidades estão:

- Informar ao departamento responsável pelo gerenciamento dos riscos ao identificar riscos não mapeados.
- Avaliar e validar os riscos mapeados sob sua responsabilidade apresentando a percepção quanto à exposição ao risco (magnitude de impacto e probabilidade de ocorrência);
- Definir, gerir e controlar o plano de ação dos riscos sob sua responsabilidade;
- Implantar ações necessárias para a mitigação dos riscos juntamente com as demais áreas envolvidas;
- Informar ao departamento responsável pelo gerenciamento dos riscos acerca das mudanças na probabilidade e/ou impacto do risco ou sobre qualquer alteração na característica do mesmo;
- Fornecer informações precisas, íntegras e suficientes sobre os riscos;
- Identificar junto a Gestão de Riscos os indicadores para a mensuração e monitoramento dos riscos.
- Propor apetites para exposição aos riscos sob a sua responsabilidade;
- Comunicar, tempestivamente, os eventos de risco que apresentarem tendência de ocorrência e/ou eventual da extrapolação dos apetites ao risco, para discussão nos fóruns e alçadas apropriadas;
- *Garantir a aderência a conclusão dos planos de ação e entrega dos controles internos na data planejada;*
- *Participar dos treinamentos relacionados a Gestão de Riscos.*

6.2 ***Control Owners***

São os responsáveis pelos controles, membros da primeira linha de defesa da gestão de riscos, entre suas principais responsabilidades estão:

- *Fornecer informações precisas, íntegras e suficientes sobre os riscos;*
- *Informar ao departamento responsável pelo gerenciamento dos riscos ao identificar riscos não mapeados.*
- *Avaliar e validar os riscos mapeados sob sua responsabilidade apresentando a percepção quanto à exposição ao risco (magnitude de impacto e probabilidade de ocorrência);*
- *Definir, gerir e controlar o plano de ação dos riscos sob sua responsabilidade;*
- *Reunir as evidências necessárias para os controles e entregar na plataforma conforme data planejada;*
- *Informar ao departamento responsável pelo gerenciamento dos riscos ao identificar riscos não mapeados;*
- *Participar dos treinamentos relacionados a Gestão de Riscos.*

6.3 ***Departamento de Gestão de Riscos Corporativos***

A gestão de risco, *membro da segunda linha de defesa, realizará o processo de gerenciamento dos riscos corporativos*, além de estabelecer diretrizes e conduta requerida neste processo, devendo:

- Revisar a Política de Gestão de Riscos Corporativos da AeC, assim como outros documentos que suportem o processo de Gestão de Riscos Corporativos;
- Identificar os riscos corporativos de toda organização, junto ao Risk Owner sempre que necessário;
- Realizar a análise e avaliação dos riscos de forma recorrente e sempre que necessário;
- Avaliar a adequação e eficácia dos controles existentes indicados pelo Control Owner para mitigar os riscos conforme a periodicidade dos controles;
- Atuar como um integrador e facilitador das unidades de negócios nos assuntos de gestão de risco;
- Atualizar e revisar os riscos e seus fatores sempre que houver atualizações no planejamento estratégico ou quando fatos relevantes ocorrerem;
- Priorizar o tratamento dos riscos classificados como "altos" e "muito altos" e estes são passíveis de serem abordados na Reunião do Comitê de Compliance e Riscos Corporativos;
- Apoiar a Diretoria na atualização da Matriz de Riscos prioritários da Companhia.

6.4 Departamento de Auditoria Interna

O departamento de Auditoria Interna, membro da terceira linha de defesa, deverá:

- Monitorar e avaliar a eficácia dos processos de gerenciamento de riscos da organização;
- Prestar serviços de consultoria e aconselhamento relacionados a governança, gerenciamento de riscos e controle conforme apropriado para a organização;
- Participar dos treinamentos relacionados a Gestão de Riscos.

6.5 Departamento de Segurança da Informação (GRC)

- *Realizar a análise/avaliação dos riscos de segurança da informação de forma periódica e sob demanda;*
- *Classificar os riscos de segurança da Informação com base na Matriz de Risco definida em*

documento específico;
- *Reportar os riscos de segurança da informação com seus respectivos planos de tratamento ao Comitê de Segurança da Informação e Privacidade;*
- *Apoiar as áreas na elaboração dos planos de tratamentos dos riscos de segurança da informação;*
- *Monitorar os riscos de segurança da informação e acompanhar o status dos planos de tratamento para assegurar a implementação dos controles.*

6.6 Departamento de Privacidade de Dados

- *Realizar a análise/avaliação dos riscos de Privacidade nas atividades de processamento de Dados Pessoais;*
- *Classificar os riscos de Privacidade com base na Matriz de Risco definida em documento específico;*
- *Reportar os riscos de Privacidade com seus respectivos planos de tratamento ao Comitê de Segurança da Informação e Privacidade;*
- *Apoiar as áreas na elaboração dos planos de tratamentos dos riscos de Privacidade;*
- *Monitorar os riscos de Privacidade e acompanhar o status dos planos de tratamento para assegurar a implementação dos controles.*

6.7 Comitê de Segurança da Informação e Privacidade (CSIP)

- *Avaliar o resultado do processo de Gestão de Riscos de Segurança da Informação e de Privacidade, visando a melhoria contínua do SGPI;*
- *Avaliar e deliberar sobre os riscos críticos e altos de segurança da informação.*

6.8 Comitê de Compliance e Riscos Corporativos

- Disseminar a cultura da gestão de Riscos Corporativos em toda AeC;
- *Aprovar a política de Gestão de Riscos Corporativos;*
- Assessorar a Diretoria na definição do apetite e tolerância ao risco;
- Avaliar e validar políticas, procedimentos e o apetite ao risco;
- Recomendar a inclusão, avaliação e priorização na Matriz de Riscos da AeC;
- Solicitar análises complementares para entendimento e discussão na avaliação dos riscos, apetite ao risco, indicadores e planos de ação;
- *Efetuar reporte ao Conselho de Administração e à Diretoria Executiva acerca do gerenciamento dos riscos estratégicos.*

6.9 Alta Direção

- Tomar decisões em relação a exposição aos riscos (impacto e probabilidade) e aos apetites apresentados pelos Proprietários dos Riscos e recomendar ações de mitigação;
- Adotar os riscos avaliados como ferramenta na tomada de decisão e na revisão ou construção do plano estratégico;
- Acompanhar periodicamente a evolução da exposição aos riscos e planos de ação considerando os apetites aprovados dos riscos pelo Conselho de Administração;
- Propor a priorização dos riscos a partir do impacto e probabilidade, visando estabelecer uma comparação individual dos riscos para fins de gestão;
- Disponibilizar recursos adequados e apropriados necessários para a operação eficaz da Gestão de Riscos da AeC, além de apoiar outros papéis pertinentes da gestão para demostrar como sua liderança na prevenção e detecção do suborno se aplica às áreas sob sua responsabilidade;
- Disseminar a cultura da gestão de Risco em toda AeC;
- Participar dos treinamentos relacionados a Gestão de Riscos.

6.10 Conselho de Administração

- Receber e analisar criticamente, a intervalos planejados, os resultados do processo de gerenciamento dos riscos;
- Requerer que os recursos adequados e apropriados necessários para a operação eficaz do sistema de gestão de riscos estejam alocados e atribuídos;
- Exercer razoável supervisão eficaz do sistema de gestão de riscos da AeC.

6.11 Demais colaboradores

- *Reportar os riscos relevantes aos seus processos à Gestão de Riscos;*
- Participar dos treinamentos relacionados a Gestão de Riscos.

7. VIOLAÇÕES A ESTA POLÍTICA

Identificadas suspeitas de violações a esta política, essas deverão ser encaminhadas ao Canal de Denúncias *da AeC.*
Caso sejam apuradas desconformidades com as condutas previstas na presente política, poderão ser aplicadas as medidas disciplinares previstas no Código de Conduta da AeC