

POLÍTICA DE GERENCIAMENTO DE RISCOS

1. OBJETIVO

A presente Política de Gerenciamento de Riscos (“Política”), visa estabelecer os princípios, as diretrizes e responsabilidades a serem observadas no processo de gerenciamento de riscos corporativos e de controles internos, assegurando a adequada identificação, análise, avaliação, tratamento, monitoramento e comunicação dos riscos corporativos inerentes às atividades da Anima Holding S.A. e suas controladas, incluindo coligadas e filiais (Companhia), buscando reduzir os níveis de exposição para efetiva criação, proteção e crescimento de valor.

2. ABRANGÊNCIA

A presente Política de Gerenciamento de Riscos aplica-se à Anima e à todas as empresas do Grupo, incluindo suas controladas, coligadas e filiais que, direta ou indiretamente, participam do processo de Gestão de Riscos.

3. DEFINIÇÕES

Apetite ao Risco: nível de risco que a Companhia está disposta a incorrer e gerenciar para atingir seus objetivos e criar valor para seus acionistas.

Compliance: prevenção e detecção de falta de conformidade com leis, regulamentações nacionais e estrangeiras e com as normas internas da Companhia, que possa ser cometida pelos administradores, colaboradores e parceiros de negócios da Companhia.

Controles: políticas, normas, procedimentos, atividades e mecanismos desenvolvidos para assegurar que os objetivos de negócios sejam atingidos e que eventos indesejáveis sejam prevenidos ou detectados e corrigidos.

Controles internos: é o conjunto de atividades de controles manuais e sistêmicos que compõem uma barreira de proteção para que as atividades operacionais e tomadas de decisões sejam realizadas em um ambiente seguro e para que os riscos sejam rapidamente identificados e tratados.

Dono do Risco (Risk Owner): Pessoa que realiza ou gerencia determinado processo e que possui responsabilidade e autoridade para gerenciar determinado risco em tal processo.

Gestão de Riscos: o gerenciamento de riscos corporativos é um processo conduzido em uma organização pelo Conselho de Administração, Diretoria e demais empregados, aplicado no estabelecimento de estratégias, formuladas para identificar em toda a organização eventos em potencial, capazes de afetá-la, e administrar os riscos de modo a mantê-los compatíveis com o apetite a risco da organização e possibilitar garantia razoável do cumprimento dos seus objetivos.

KRIs: Key Risk Indicators - principais indicadores de risco da Companhia. Funcionam como sinais de alerta, indicando as mudanças no nível de risco de uma organização ou de seus negócios.

Matriz de Riscos: visa estabelecer uma comparação individual dos Riscos a partir dos impactos e probabilidades de ocorrência para fins de priorização e gestão. A matriz de riscos é uma ferramenta em constante evolução e atualizada, no mínimo, anualmente, por ocasião da revisão de planejamento estratégico da Companhia e tempestivamente com o surgimento de eventos de riscos emergentes.

Órgãos de Gestão: Conselho de Administração e Diretoria

Planos de Ação: ações ou conjunto de ações visando a mitigação ou redução do nível de exposição de um risco identificado.

Resposta ao Risco: decisão que será tomada após a identificação do risco inerente ou avaliação do ambiente de controle dos riscos residuais, com objetivo de promover discussões que assegurem a eficiência do ambiente de Controles internos da Ânima.

Risco(s): ameaça de eventos ou ações que possam impactar o atingimento dos objetivos da Companhia. É inerente a qualquer atividade e pode afetar os ativos, resultados, imagem ou continuidade dos negócios.

4. DIRETRIZES

O processo de gerenciamento de riscos segue os princípios éticos da Companhia, valores e cultura, e as informações geradas pelo sistema de gestão de riscos devem ser confiáveis, seguir as orientações legais, e fornecer subsídios para tomada de decisões visando a mitigação ou redução do nível de exposição aos riscos e a adequada priorização de ações, em especial com relação aos seguintes aspectos:

- (i) As políticas e processos de gerenciamento de riscos devem ser conhecidos de todos os colaboradores de forma a garantir que todos eles entendam seu papel dentro da estrutura de controle e os realizem a contento;
- (ii) As informações utilizadas para gerenciamento dos riscos e controles internos devem ser íntegras e corretas, representando a situação atual das operações da Companhia, para que todos os colaboradores tenham disponíveis as informações necessárias e assertivas para a gestão de seus riscos;
- (iii) Os riscos da Companhia devem ser comunicados e conhecidos por todos os envolvidos em seu gerenciamento e monitoramento, bem como reportados tempestivamente. O processo de comunicação dos riscos deve ser claro e eficiente, e conter informações suficientes para a apropriada tomada de decisão;
- (iv) Cabe aos Órgãos de Gestão garantir recursos adequados para a operacionalização dos processos de identificação, avaliação, análise, tratamento, monitoramento e controle dos riscos da Companhia.

Todas as informações e reportes resultantes do processo de gestão de riscos são classificadas como restritas ao uso interno e devem possuir repositório e guarda adequada. As informações cujo reporte será externo, como Formulário de Referência ou Informe do Código Brasileiro de Governança Corporativa, devem refletir a metodologia e os resultados de exposição identificada no processo de gestão de riscos.

4.1. Categorias de Riscos

Os riscos da Companhia são categorizados de acordo com a seguinte classificação:

- (i) **Riscos Estratégicos** - riscos associados com as decisões estratégicas da organização para atingir os seus objetivos de negócios, e/ou decorrentes da falta de capacidade ou habilidade da empresa para proteger-se ou adaptar-se a mudanças no ambiente. Consistem de: (a) **Riscos acadêmicos** - impactos que decorrem das estratégias adotadas para conteúdo programático, grade curricular, qualificação dos docentes, marcas e patentes e satisfação do cliente; (b) **Riscos de governança** - possibilidade de impactos resultante de incertezas quanto a comunicação e divulgação, cultura organizacional, incentivos de desempenho, questões de mercado, relacionamento com investidores, reputação e imagem, responsabilidade social e sucessão ou controle acionário;

- (c) **Riscos de modelo de negócio** - consequência das indefinições quanto à concorrência e mercado, continuidade do negócio, inovações, estrutura organizacional, fusão e aquisições, investimento, orçamento, planejamento financeiro e precificação; (d) **Riscos políticos econômicos** - relacionados às indeterminações que decorrem do cenário econômico, mudança governamental, FIES e ProUni;
- (ii) **Riscos Financeiros** - consistem de: (a) **Riscos de mercado** - que decorrem da possibilidade de perdas que podem ser ocasionadas por mudanças no comportamento das taxas de juros, do câmbio, dos preços das ações e dos preços de *commodities*; (b) **Riscos de crédito** - possibilidade de perda resultante da incerteza quanto ao recebimento de valores pactuados com tomadores de empréstimos, contrapartes de contratos ou emissões de títulos; (c) **Riscos de liquidez** - possibilidade de perda decorrente da incapacidade de realizar uma transação em tempo razoável e sem perda significativa de valor ou a possibilidade de falta de recursos para honrar os compromissos assumidos em função do descasamento entre os ativos e passivos;
- (iii) **Riscos de Compliance / Regulamentar** - riscos de sanções legais ou regulatórias que a empresa pode sofrer como resultado da falha no cumprimento da aplicação de leis, acordos, regulamentos, código de conduta e/ou de suas políticas e que poderão resultar em perda financeira ou danos à reputação da Companhia;
- (iv) **Riscos de Tecnologia da Informação e Cyber Security** – possibilidade de perda resultante de insegurança nas operações dos recursos tecnológicos quanto ao acesso, confidencialidade, credibilidade, disponibilidade e integridade das informações, como a ocorrência de ataques cibernéticos por hackers, vazamento e/ou perda de integridade de informações, indisponibilidade do ambiente de TI e obsolescência tecnológica, que podem impactar nos negócios da Companhia, podendo ocasionar inclusive a interrupção de operações e sanções pelo descumprimento de leis e normas, a exemplo da Lei Geral de Proteção de Dados (LGPD).
- (v) **Riscos Operacionais** - referem-se às possíveis perdas resultantes de falhas, deficiências ou inadequação de processos internos, pessoas, ambiente tecnológico ou provocadas por eventos externos. Consistem de: (a) **Riscos acadêmicos** – relacionados as incertezas de procedimentos da companhia quanto a capacidade operacional, emissão de diplomas e certificados, divulgação de resultados do ENADE, efetividade e eficiência, execução da grade curricular, cumprimento do conteúdo didático, efetivação do conteúdo programático, obrigação com alunos, padrão de qualidade e satisfação dos alunos; (b) **Riscos de pessoal** - possibilidade de impactos decorrente de ineficiência quanto à capacitação dos funcionários, contratação e retenção de talentos, bem como a dependência de pessoal; (c) **Riscos do processo** - que derivam da eventualidade de prejuízos que podem ser ocasionados devido a erros na execução de processos como captação e retenção de alunos, expansão, fornecimento, práticas comerciais, terceirizações, segurança patrimonial e outros; (d) **Riscos de ameaças à vida** tais como: incêndios, atentados, suicídios, epidemias e pandemias.
- (vi) **Risco de Imagem** - possibilidade de ocorrência de evento, geralmente ocasionado por outros riscos, que possa causar danos à reputação, credibilidade ou marca da Companhia, inclusive em razão de publicidade negativa, verdadeira ou não;

4.2- Processo de Gestão de Riscos

4.2.1- Fixação de Objetivos

Consiste da definição e documentação dos objetivos e metas da gestão de riscos com base na estratégia de gestão de riscos e no plano estratégico da Companhia, deixando claros ao menos os objetivos e metas (1) estratégicas, (2) financeiras, (3) de abordagem aos clientes, (4) operacionais, (5) objetivos de aprendizado e desenvolvimento contínuo, (6) de comunicação interna e externa e (7) de conformidade.

4.2.2- Identificação dos Riscos

O processo de captura e identificação de riscos consiste na execução de atividades específicas, como mapeamento de processos, entrevistas com os gestores responsáveis de cada área/segmento de negócio e o levantamento de perdas ocorridas no passado, com o intuito de estabelecer as matrizes de riscos e controles e mantê-las constantemente atualizadas, com base nos eventos que possam impactar os objetivos estratégicos e de negócio da Companhia.

A Diretoria de Gestão de Riscos e *Compliance* atuará como facilitadora e consolidadora no processo de identificação e atualização dos riscos da Companhia.

4.2.3- Avaliação de Riscos

Nesta etapa do processo a Companhia refina o entendimento do nível e natureza dos riscos, quantificando estes em termos de probabilidade e impacto de acordo com sua capacidade de afetar as atividades da Companhia em curto, médio e longo prazo.

Toda a metodologia de avaliação, ponderação e priorização dos riscos será proposta pela Diretoria de Gestão de Riscos e *Compliance* e validada pelo Comitê de Auditoria, Governança e Gestão de Riscos da Companhia, contemplando minimamente (podendo ser utilizada uma combinação de cada uma delas) as etapas de (1) Categorização (2) Estabelecimento de Critério para Cálculo da Severidade e (3) Elaboração de Mapa dos Riscos.

4.2.4- Respostas (tratamento) aos Riscos

Após avaliar e classificar os riscos a administração determinará como pretende responder aos riscos. Tais respostas devem estar em linha com o apetite de riscos definido pelo Conselho de Administração. Cada risco identificado e avaliado pode ter uma ou mais respostas. A administração pode adotar as seguintes respostas aos riscos:

- (i) **Evitar:** descontinuação das atividades que geram os riscos. Evitar riscos pode implicar, como por exemplo, a descontinuação de uma linha de serviços;
- (ii) **Reduzir:** são adotadas medidas, por meio de planos de ação, para reduzir a probabilidade ou o impacto dos riscos, ou, até mesmo, ambos;
- (iii) **Compartilhar:** redução da probabilidade ou do impacto dos riscos pela transferência ou pelo compartilhamento de uma parte do risco, como por exemplo, a terceirização de uma atividade ou a contratação de seguros;
- (iv) **Aceitar:** nenhuma medida é adotada para afetar a probabilidade ou o grau de impacto dos riscos.

4.2.5- Atividades de Controle

As áreas de negócio possuem o papel de implementar e garantir a continuidade operacional dos controles internos associados às suas atividades, garantindo que os riscos residuais estejam alinhados ao nível de apetite e tolerância estabelecidos e validados pelo Conselho de Administração. A Diretoria de Gestão de Riscos e *Compliance* atuará ativamente no processo de identificação e avaliação de controles internos por meio de revisões de processos, investigações pontuais e auditorias internas.

4.2.6- Comunicação

As informações pertinentes devem ser identificadas, coletadas e comunicadas de forma coerente e em prazo hábil, a fim de permitir que as pessoas cumpram as suas responsabilidades. A comunicação eficaz deve ocorrer em todos os níveis da organização, de modo que cada colaborador entenda a sua função no gerenciamento de riscos corporativos, assim como as atividades individuais que se relacionam com o

trabalho dos demais. Deve haver, também, uma comunicação eficaz com terceiros, como clientes, fornecedores, órgãos reguladores e acionistas. Os sistemas de gestão de riscos devem permitir o acompanhamento através de indicadores e *dashboards*, possibilitando a tomada de decisão baseadas em dados relacionados aos objetivos.

4.2.7- Monitoramento e Análise Crítica

A estrutura de controles internos deve ser monitorada para avaliar a qualidade e a atualização dos controles no tempo. Esse objetivo é atingido mediante atividades recorrentes de monitoramento ou avaliações independentes periódicas, ou, ainda, por uma combinação desses dois mecanismos. As principais atividades de monitoramento incluem conciliações, acompanhamento de comunicações de agentes externos, inventários, auditorias, auto avaliações e verificação contínua.

5. RESPONSABILIDADES

Esta política envolve a responsabilidade direta das seguintes áreas e instâncias:

Conselho de Administração

- (i) Aprovar a Política de Gerenciamento de Riscos da Companhia e suas futuras revisões;
- (ii) Estabelecer o nível de apetite a risco para a Companhia em função da relação risco / retorno que ela pretende assumir;
- (iii) Monitorar o processo de gerenciamento de Riscos e de Controles internos, bem como do programa de *Compliance* da Companhia, recomendando eventuais alterações.
- (iv) Avaliar (mínimo anualmente) a qualidade e adequação da Matriz de Riscos da Companhia;
- (v) Discutir, contribuir e opinar sobre os riscos estratégicos da Companhia.

Comitê de Auditoria, Governança e Gestão de Riscos

- (i) Analisar a Política de Gerenciamento de Riscos Corporativos da Companhia, assim como quaisquer revisões, submetendo-a à aprovação do Conselho de Administração;
- (ii) Supervisionar e avaliar as atividades e planejamento de Gerenciamento de Riscos da Companhia (incluindo as atividades de auditoria interna e controles internos), bem como o cumprimento da legislação aplicável, das políticas, normas e procedimentos internos da Companhia (*Compliance*), em todos os seus níveis;
- (iii) Avaliar a adequação dos recursos humanos e financeiros destinados à gestão de riscos da Organização;
- (iv) Monitorar o andamento dos planos de ação de melhorias de controles internos oriundos da área de Gestão de Riscos Corporativos;
- (v) Avaliar as informações trimestrais, demonstrações intermediárias e demonstrações financeiras;

Área de Gestão de Riscos:

- (i) Avaliar os riscos da Companhia por unidades de negócio e/ou portfólio;
- (ii) Consolidar e comunicar o portfólio de riscos relevantes da organização;

- (iii) Coordenar e definir os padrões a serem seguidos no que tange os processos de controles internos, *compliance* e risco corporativo, os sistemas de suporte e as formas e a periodicidade dos seus reportes;
- (iv) Avaliar e propor estratégias de resposta aos riscos;
- (v) Assessorar os *Risk Owners* na identificação e avaliação do impacto dos diversos tipos de riscos envolvidos;
- (vi) Suportar os *Risk Owners* na definição do plano de ação/contingência.

Área de *Compliance*:

- (i) Elaborar e/ou contribuir na elaboração das políticas e normas de conduta e anticorrupção para os colaboradores, fornecedores e clientes, atuando ativamente na sua divulgação e conscientização junto aos respectivos públicos;
- (ii) Garantir o funcionamento e idoneidade dos canais de denúncias em todos os níveis e para todos os públicos da organização, assim como a apuração e resolução adequada de todos os casos de desvios comprovados;
- (iii) Garantir a existência de procedimentos, indicadores e controles nas áreas operacionais que garantam a manutenção do atendimento das leis e normas educacionais, tributárias, cíveis e trabalhistas.

Área de Controles Internos

- (i) Elaborar e/ou contribuir na elaboração dos procedimentos e normas de *cybersecurity*;
- (ii) Desenhar os perfis de acesso a sistemas internos e externos (p. ex bancos) por funções e setores, bem como auxiliar as áreas nas definições de alçadas de aprovação por cargos. Atuar na validação da concessão de tais acessos e revisão tempestiva dos mesmos;
- (iii) Revisar e desenhar junto às áreas operacionais os controles nos processos de negócio e *back-office* que minimizem a possibilidade de ocorrência de erros e seguindo metodologia que permita a auditoria e certificação de processos de controles, evitando burocracias desnecessárias;
- (iv) Disseminar na Companhia e suas controladas a cultura de controles com o intuito de minimizar erros e retrabalhos;
- (v) Suportar as áreas de negócio na definição e acompanhamento do plano de ação/contingência para a melhoria dos controles internos;
- (vi) Garantir que os controles internos desenhados estejam em funcionamento em todas as áreas, obtendo evidências sobre o funcionamento dos mesmos e atuando corretivamente nos casos de mau funcionamento.

Auditoria Interna

- (i) Proceder a avaliação e entendimento do ambiente de riscos e controles da Companhia e suas controladas, incluindo as operações que ocorrem nos *campi*;
- (ii) Verificar o funcionamento dos controles internos da organização através de testes sobre os mesmos, sempre com uma abordagem de parceria com as áreas auditadas e com objetivo de incentivar as melhorias de qualidade dos processos e redução de riscos, evitando abordagens meramente punitivas;
- (iii) Realizar auditoria contínua dos processos críticos de negócio, em conjunto com as respectivas áreas operacionais.

Diretoria Executiva

- (i) A diretoria é a responsável pelo gerenciamento dos riscos, bem como pelo estabelecimento de um sistema de controles Internos adequado ao apetite a riscos definido pelo Conselho de Administração;
- (ii) Estabelecer priorização dos Riscos a partir do impacto e probabilidade, visando estabelecer uma comparação individual dos riscos para fins de priorização e gestão;
- (iii) Acompanhar os KRI's e as estratégias de mitigação dos riscos prioritários;
- (iv) Definir diretrizes, recursos e metas que garantam o bom funcionamento da gestão de riscos;
- (v) Promover a integração da gestão de riscos com os ciclos de gestão e planejamento das empresas do grupo Ânima.

Gestores das Áreas de Negócio

- (i) Elaborar o planejamento e assegurar a operacionalização da gestão de riscos, considerando todas as dimensões da estrutura definida, englobando atividades estratégicas, táticas e operacionais;
- (ii) Identificar e gerenciar os riscos das respectivas áreas de acordo com as estratégias de resposta aos riscos;
- (iii) Implementar e acompanhar as ações corretivas e/ou preventivas (plano de ação / resposta aos riscos).

6. DISPOSIÇÕES FINAIS

Esta Política entra em vigor quando de sua aprovação pelo Conselho de Administração.