Americanas S.A. – Em Recuperação Judicial

CNPJ nº 00.776.574/0006-60

POLÍTICA DE GESTÃO DE RISCOS

1. Objetivo

Esta política estabelece princípios, diretrizes e responsabilidade no processo de gerenciamento de riscos inerentes ao negócio, tendo como objetivo a geração e proteção de valor para a Companhia e o atingimento de seus objetivos estratégicos.

2. Campo de Aplicação

Esta política aplica-se à **Americanas**, membros do Conselho de Administração, membros de Comitês de Assessoramento, membros do Conselho Fiscal, Diretoria Estatutária, Associados e parceiros, direta ou indiretamente relacionados com a Companhia.

3. Definições

- **Americanas** ou **Companhia**: engloba Americanas S.A – em Recuperação Judicial e todas as demais empresas a ela relacionadas como controladas e/ou subsidiárias.
- **Associado:** menor aprendiz, estagiário, colaborador, que tenha acesso a informações e/ou recursos da Companhia.
- **Gestão de Riscos**: Processo sistematizado de identificação, avaliação e tratativa de riscos, incluindo a estrutura, normativos, metodologia, responsabilidades e recursos.
- **Risco**: Evento que pode comprometer total ou parcialmente, diminuindo, atrasando, alterando ou impedindo o alcance dos objetivos do negócio
- **Fator de Risco:** ocorrências que podem levar um risco a se materializar, representando deficiências e vulnerabilidades internas e externas.
- **Impacto**: Consequência da materialização de um risco, podendo gerar efeitos negativos operacionais, financeiros, regulatórios ou reputacionais.
- **Probabilidade**: Possibilidade de ocorrência de um determinado evento, podendo ser medida com base em estimativas ou no histórico/frequência de ocorrência.
- **Criticidade**: Métrica constituída pelo cruzamento entre probabilidade e impacto.
- **Matriz de Riscos**: Ferramenta utilizada para listar, detalhar e avaliar os riscos identificados, associando-os a controles existentes ou recomendações.
- **Apetite ao risco**: Limite máximo tolerável de exposição aos riscos.
- **Risk Owner**: responsável pelos riscos de sua área e respectivo gerenciamento.
- **Controle**: Mecanismo utilizado para reduzir o nível de risco de uma determinada atividade, processo ou sistema.
- **Plano de ação:** Conjunto de medidas a serem desenvolvidas de forma pontual ou contínua a fim de reduzir o grau de criticidade de um determinado risco.
- **KRI:** *Key Risk Indicator*. São indicadores quantitativos e/ou qualitativos que auxiliam no monitoramento dos riscos.

4. Diretrizes Gerais

A Companhia está comprometida com a dinâmica da Gestão de Riscos, de forma a preservar e desenvolver sua estratégia, valores, ativos, reputação, competitividade, integridade e resiliência.

O objetivo da Gestão de Riscos é **reduzir o nível de incerteza** nos negócios, **protegendo e gerando valor** e possibilitando uma **melhor tomada de decisão**. Isso ocorre através de um processo estruturado de identificação e análise de riscos, com escopo e critérios bem definidos e uma comunicação efetiva e transparente, assim como os registros e reportes relacionados.

A abordagem da Companhia tem ainda como premissas:

- Criação de uma **cultura de Gestão de Riscos** no longo prazo;
- Alinhamento com a **estratégia** e direcionamento "top-down";
- Definição de **escopo e critérios** personalizados como parâmetros para o processo de Gestão de Riscos na Companhia;
- Comunicação **abrangente, transparente e eficiente** e consulta às partes interessadas;
- Identificação de **oportunidades** de inovação e criação de valor para o negócio;
- Implementação e mantenimento de **estruturas e ferramentas** adequadas para operacionalização da Gestão de Riscos em linha com as melhores práticas;
- **Monitoramento e reavaliação** não só dos riscos, mas da **efetividade** da Gestão de Riscos como um todo, de modo a viabilizar a **melhoria contínua**.

5. Gestão de Riscos

As diretrizes estabelecidas na presente Política são operacionalizadas por meio de um modelo de trabalho integrado que inclui uma metodologia e ferramentas específicas, estruturas dedicadas, com papeis e funções atribuídas e um processo com etapas bem definidas e em linha com as melhores práticas de mercado.

5.1. Escopo e contexto

A Gestão de riscos considera em seu escopo uma série de aspectos do ambiente interno que vão do nível **estratégico ao transacional**, permeando **iniciativas e projetos** alinhados às diretrizes estratégicas e a **cadeia de valor**, incluindo atividades-chave e atividades de suporte e gestão.

Também considera a **influência direta e indireta** de fatores do **ambiente externo** no atingimento dos objetivos estratégicos, como mudanças no ambiente regulatório e legislação, mudanças climáticas, inovações tecnológicas, novos mecanismos de fraude, mercado e concorrência, saúde e segurança pública, transformações culturais, mudanças nos paradigmas de consumo e o contexto político, social e econômico.

5.2. Modelo de Atuação

A Companhia adota o **modelo das 3 linhas** como estrutura para Gestão de riscos, no qual estão envolvidas desde as áreas de negócio e operação, de suporte e de gestão, assim como o órgão de governança e a auditoria interna, sendo representadas na forma de camadas ou níveis:

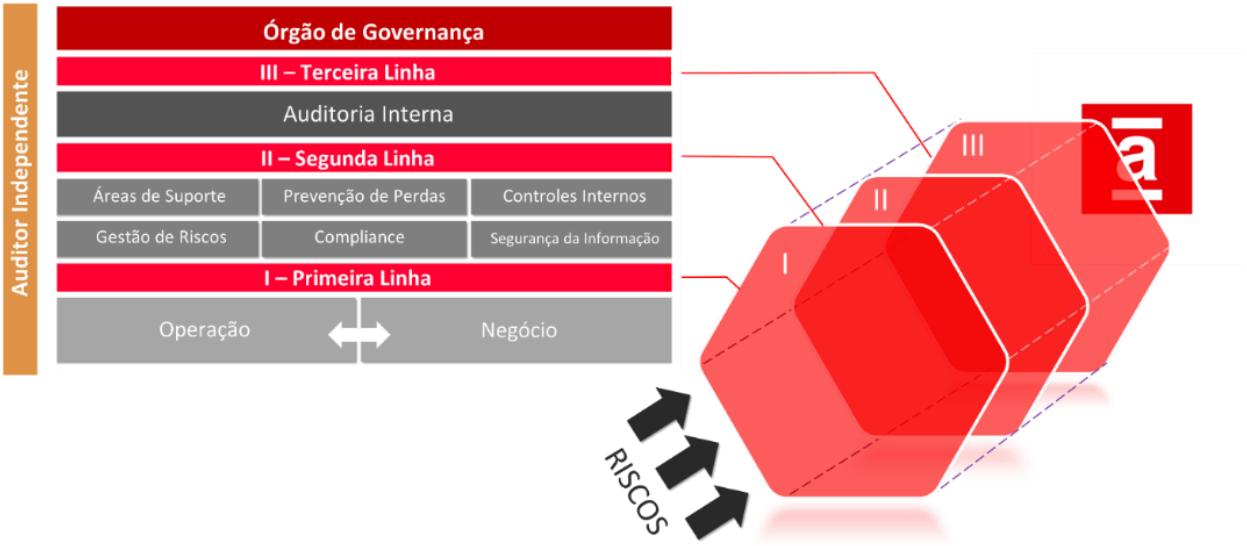

Figura 1: Modelo das 3 Linhas

Considerando esse modelo, as linhas possuem atribuições específicas no processo de gerenciamento de riscos:

- **1ª Linha:** áreas que executam atividades finais, sendo responsáveis por executar as atividades de controle relacionados ao negócio e operação;
- **2ª Linha:** áreas especializadas que fornecem apoio à primeira linha, realizando monitorias quanto aos controles e suporte na proteção dos riscos identificados;
- **3ª Linha:** Auditoria Interna, responsável por realizar avaliação de forma independente e objetiva para mensurar a efetividade dos mecanismos de proteção e mitigação de riscos.
- **Órgão de Governança:** presta contas às partes interessadas e supervisiona a atuação das três linhas, avaliando a efetividade do gerenciamento de riscos e controles.

5.4. Processo de Gestão de Riscos

O processo de gestão de riscos realizado na Companhia é baseado nas melhores práticas de mercado e considera 5 etapas principais, segundo a imagem 2:

Figura 2: Processo de Gestão de Riscos

5.4.1. Identificação

A identificação pode ocorrer de forma **estruturada e planejada**, por meio de mapeamentos de processo, análise de controles internos, na interação entre as áreas de primeira e segunda linha ou ainda de forma **responsiva**, tendo como base relatórios e comentários da terceira linha ou avaliadores externos, indicadores de desempenho, monitorias e outras fontes de dados.

Os riscos identificados são **detalhados e agrupados** com base nos processos em que foram identificados ou nos temas aos quais estão relacionados em uma Matriz de riscos correspondente, possuindo a ele associadas uma série de informações complementares, como responsável, subprocesso, fatores de risco, mecanismos de controle existentes etc.

5.4.1.1. Registro e reporte

Os riscos identificados são listados e detalhados por meio da Matriz de riscos, seguindo os modelos e critérios de metodologia estabelecidos no manual interno. Ao longo do processo, são apresentados **relatórios e informações**, com base nas linhas de reporte estabelecidas, elencando os **principais resultados e informações** sobre os riscos, incluindo detalhamento, responsáveis, controles associados, priorização e Planos de Ação.

Periodicamente, é gerado uma **Matriz de Riscos** com os **riscos prioritários**, que é apresentado e validado pelo Conselho de Administração e pelo Comitê de Auditoria. Para cada revisão, os riscos que o compõe são reavaliados com base no cenário e diretrizes vigentes

5.4.2. Análise

Uma vez listados e detalhados na matriz de risco, os riscos são individualmente avaliados através dos critérios **probabilidade** de ocorrência e **impacto**, que são atribuídos dentro de uma escala pré-definida e formalizada em manual interno com base em indicadores quantitativos e qualitativos:

(a) Probabilidade: Chance de ocorrência de um evento, podendo considerar a frequência esperada, projeções ou estimativas, bem como vulnerabilidades existentes. A pontuação é constituída por faixas de valores estabelecidos.

(b) Impacto: Corresponde aos efeitos ou consequências potenciais da materialização do risco na Companhia. Sua atribuição é feita por meio de uma escala gradativa, detalhada por tipo de impacto.

(c) Criticidade: O cálculo da criticidade, que mede o nível de risco, consiste na multiplicação das pontuações de probabilidade (eixo y) e impacto (eixo x), conforme mostra o exemplo abaixo:

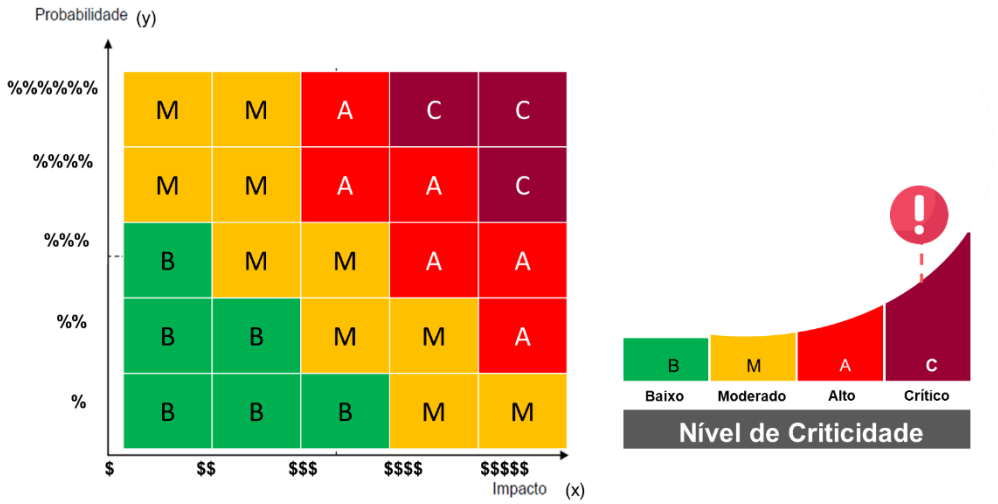

Figura 3: Modelo conceitual de classificação de criticidade (Heatmap)

5.4.3. Avaliação e Tratamento

O tratamento dos riscos busca reduzir seu nível de criticidade através da redução da probabilidade ou mitigação dos impactos, e tem como possibilidades de resposta, por padrão:: (a) a **eliminação** dos fatores que originam o risco, (b) a **mitigação** do risco por

meio da implementação ou aprimoramento de controles e processos, (c) a **transferência ou compartilhamento** do risco por meio de seguros, dispositivos contratuais e terceirização, (d) **exploração** do risco caso o mesmo represente uma oportunidade para o negócio, ou, em último caso, (e) a **aceitação** do risco em caráter excepcional e mediante justificativa, aprovação por alçada competente e reporte, observando os limites, formalização adequada e acompanhamento.

5.4.4. Revisão e Monitoramento Contínuo

As áreas de primeira e segunda linha acompanham os riscos por meio de atividades de **gestão, indicadores (KRIs) e análises internas**. Após a implementação das ações e controles para mitigação do risco, é atribuída uma nova pontuação para sua probabilidade e/ou impacto, resultando no **risco residual**. O fator utilizado para a revisão dos valores depende da **efetividade** das ações e controles relacionados.

Os riscos priorizados têm seus planos de ação acompanhados pelo Comitê de Auditoria e pelo Conselho de Administração por meio de seus Comitês de acordo com o tema ao qual está relacionado. **Mudanças** no contexto interno e externo também são **acompanhadas e refletidas** nas avaliações dos riscos e na Matriz de Riscos.

6. Papeis e Responsabilidades

6.1. Do Conselho de Administração

- Validar as diretrizes gerais para o gerenciamento de riscos da Companhia;
- Aprovar a Política de Gestão de Riscos e suas revisões futuras;
- Incentivar, direcionar e patrocinar o monitoramento dos riscos prioritários.

6.2. Do Comitê de Auditoria

- Analisar e opinar sobre as diretrizes e políticas de gestão de risco, principalmente no que tange ao apetite de risco e cultura de riscos;
- Fornecer ao Conselho de Administração assessoramento sobre o grau de exposição a riscos da Companhia e recomendar mecanismos de mitigação;
- Supervisionar a gestão de riscos e monitorar os riscos prioritários, bem como ações de mitigação e o ambiente de controle interno.

6.3. Da Diretoria de Riscos e Compliance

- Elaborar e revisar a política e procedimentos de gestão de riscos, bem como a metodologia e ferramentas utilizadas no processo.
- Operacionalizar a gestão de riscos, mapeando processos e elaborando a Matriz;
- Dar suporte as áreas do negócio na definição de planos de ação, controles internos e indicadores para monitoramento de riscos-chave;

- Disseminar a cultura da gestão de Riscos na Companhia;
- Acompanhar projetos e iniciativas críticas, suportando a tomada de decisão;
- Reportar ao Comitê de Auditoria quaisquer riscos emergentes que possam alterar a Matriz de Riscos ou que rompam os limites definidos;
- Interagir com a primeira linha e demais áreas de segunda linha quando uma vulnerabilidade ou ameaça é identificada e acompanhar e suportar a implementação de medidas de prevenção e mitigação;
- Conduzir treinamentos periódicos sobre as disposições previstas nesta política.

6.4. Da Auditoria Interna

- Aferir a qualidade e efetividade dos processos de gerenciamento de riscos e controles internos da Companhia, propondo melhorias e identificando vulnerabilidades.
- Reportar diretamente ao Comitê de Auditoria temas relacionados ao gerenciamento de riscos e efetividade do sistema de controles internos com base em suas avaliações independentes;

6.5. Das áreas de Negócio (Risk Owners)

- Aplicar as diretrizes da presente política na condução de suas atividades, zelando pela tratativa e comunicação dos riscos sob sua responsabilidade;
- Garantir a implementação das medidas de prevenção e mitigação de riscos;
- Prestar contas e fornecer informações, comunicando eventuais vulnerabilidades de forma transparente e tempestiva;

7. Treinamentos

A Diretoria de Riscos e Compliance será responsável por promover a disseminação da cultura de gestão de riscos na Companhia. Para isso, realizará treinamentos periódicos voltados ao engajamento e à conscientização dos públicos sujeitos a esta Política, reforçando a importância do cumprimento de suas diretrizes.

Eventuais dúvidas sobre o conteúdo deste documento poderão ser esclarecidas junto à Diretoria de Riscos e Compliance.

8. Disposições Finais

A presente Política deve ser interpretada e aplicada em harmonia com as demais políticas e procedimentos internos vigentes na Companhia, em especial aqueles voltados ao combate à corrupção, à prevenção e ao enfrentamento de fraudes, à promoção da conduta ética, à proteção dos direitos humanos e à preservação do meio ambiente.

9. Vigência

A Política terá vigência por prazo indeterminado e entrará em vigor na data de aprovação pelo Conselho de Administração. A política deverá ser revista no prazo máximo de 3 (três) anos a partir de sua publicação, podendo ocorrer em menor período, caso haja necessidade, e/ou em decorrência de alterações legislativas e regulatórias, ou em decorrência de revisão nos documentos de governança corporativa da Companhia.

10. Referências

- ISO 31.000:2018;
- COSO ERM (2017);
- Modelo das 3 Linhas – IIA (2020);
- Caderno 19 – Instituto Brasileiro de Governança Corporativa (IBGC);
- Código de Ética e Conduta;
- AMER-POL-SI-001 - Política de Segurança da Informação;
- AMER-POL-COMP-001 - Política de *Compliance*;
- AMER-POL-COMP-006 - Política de Combate à Corrupção;
- AMER-POL-COMP-008 - Política de Fornecedores e Parceiros;
- Diretriz de Consequências