Americanas S.A.

POLÍTICA DE GERENCIAMENTO DE RISCOS

1. Objetivo

Esta política estabelece princípios, diretrizes e responsabilidades no processo de gerenciamento de riscos inerentes às atividades de negócios da Companhia. As práticas de gerenciamento de riscos adotadas têm como finalidade:

- Proteger valor resguardando a Companhia contra os riscos identificados através da aplicação da metodologia de gerenciamento de riscos;
- Agregar valor fortalecendo as práticas de controle e governança e identificando oportunidades para o negócio diante de cenários de incerteza;
- Oferecer insumos para uma tomada de decisão mais assertiva;
- Identificar vulnerabilidades e cenários que possam impactar os objetivos estratégicos, resultando em desconformidade com a legislação, regulamentação ou com os procedimentos e regulamentos internos, que possam causar impactos nos custos e na eficiência da operação ou afetar a reputação da Companhia e suas marcas perante seus associados, parceiros, fornecedores, clientes, acionistas, o mercado e a sociedade.

2. Campo de aplicação

Esta Política aplica-se à Companhia, bem como a todos os seus associados, diretores estatutários e não estatutários, membros do Conselho de Administração, membros de comitês, membros do Conselho Fiscal, quando instalado, representantes e terceiros, direta ou indiretamente relacionados com a Companhia.

3. Definições

- **Apetite ao risco**: Limite máximo tolerável de exposição aos riscos considerados para os negócios da Companhia.
- **Companhia**: engloba americanas s.a. e todas as demais empresas a ela relacionadas como controladas diretas e indiretas, incluindo joint ventures

e subsidiárias, atuais e futuras, e se aplica individualmente a qualquer das empresas que compõem o mesmo Grupo Econômico.

- **Controle**: Ação ou mecanismo utilizado para reduzir o nível de risco de uma determinada atividade ou processo.
- **Criticidade**: Métrica constituída pelo cruzamento entre nível de probabilidade de ocorrência e nível de impacto potencial (probabilidade x impacto).
- **Evento**: Ocorrência na qual um risco se torna concreto.
- **Fator de risco**: Vulnerabilidade ou fragilidade interna ou decorrente de forças externas que pode, com maior ou menor probabilidade, se concretizar e prejudicar as empresas no atingimento de seus objetivos.
- **Gerenciamento de Riscos**: Estrutura composta por todas as ferramentas de governança que dão suporte às atividades relacionadas a identificação, avaliação e tratativa de riscos, incluindo a estrutura organizacional, políticas, regulamentos, metodologia, papéis e responsabilidades e recursos.
- **Gestão da Continuidade do Negócio**: Atividades voltadas para a identificação de fatores e cenários que possam comprometer a operação, seja na atividade fim (comercialização de produtos e oferta de serviços) ou nas atividades de suporte (processamento de informações, contabilização, infraestrutura tecnológica, etc.), bem como o planejamento das medidas de contingência para mitigar impactos, o teste contínuo dessas medidas e a garantia da continuidade.
- **Impacto**: Consequência da materialização de um risco, podendo gerar efeitos negativos de cunho operacional, financeiro, regulatório ou reputacional, em maior ou menor escala dependendo do seu grau.
- **Matriz de Riscos**: Ferramenta utilizada para listar, detalhar e avaliar os riscos identificados, associando-os a controles existentes ou recomendações de controle.
- **Mapa de Riscos**: Modelo que permite uma visualização clara e rápida dos riscos a serem priorizados com base em sua criticidade, medida por meio do cruzamento entre probabilidade e impacto.

- **Oportunidade**: Possibilidade de ganho de valor para o negócio a partir de cenários de incerteza que possuem aspectos favoráveis a serem explorados.
- **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.
- **Probabilidade**: Possibilidade de ocorrência de um determinado evento, podendo ser medida com base em estimativas ou no histórico/frequência de ocorrência.
- **Risco**: Incerteza quanto à ocorrência de um evento que pode diminuir, atrasar, alterar ou impedir o atingimento dos objetivos do negócio.
- **Risco prioritário**: Classificação dada a um risco que possui criticidade elevada perante os demais riscos listados na Matriz e no Mapa de Riscos, sendo, portanto, prioridade no desenvolvimento de planos de ação e no monitoramento da Gestão.

4. Diretrizes gerais

A Companhia está comprometida com a dinâmica de gerenciamento de Riscos, de forma a preservar e desenvolver sua estratégia, valores, ativos, reputação, competitividade, integridade e perenidade dos negócios.

O objetivo do gerenciamento de riscos é reduzir o nível de incerteza nos negócios através do detalhamento e melhor compreensão dos riscos, o que é feito por meio de um estudo de suas causas, do contexto no qual se materializam e das possíveis consequências, bem como das ações de resposta a serem definidas para que eventuais perdas ou danos sejam previstos e reduzidos, mantendo os riscos dentro dos limites estabelecidos.

A Gestão de Riscos deve auxiliar o processo de tomada de decisão nos diversos níveis de gestão da Companhia, estando presente no planejamento estratégico, nas decisões de investimento e na gestão de projetos. Além disso, é parte do processo de gerenciamento de riscos a identificação de oportunidades para o negócio a serem exploradas a partir de cenários de incerteza, sobretudo em relação a riscos de origem externa, como riscos associados a mudanças climáticas, ataques cibernéticos, disputa de mercado, de emergências em saúde

pública e desastre, transformações culturais e sociais, mudanças nos paradigmas de consumo, alterações em taxas e índices de mercado e outros possíveis cenários.

5. Aplicação e desdobramento

O gerenciamento de Riscos contribui para o monitoramento e para a realização dos objetivos da Companhia. A abordagem visa integrar o gerenciamento de Riscos no dia a dia e na conduta dos seus negócios por meio de:

- Tomada de decisão consciente através de melhor conhecimento e consideração dos Riscos, contextos, impactos diretos e indiretos em todas as suas atividades;
- Alocação de recursos de forma adequada para melhor controle dos riscos prioritários;
- Transferência de certos riscos ao mercado de Seguros, considerando os limites de exposição e o apetite ao risco;
- Gerenciamento adequado e coordenado de incidentes por meio do fornecimento de informação confiável e rápida à Diretoria, conselho de administração e comitês de assessoramento em caso de grandes acontecimentos que possam impactar a Companhia e a continuidade dos negócios;
- Identificação de oportunidades de inovação e criação de valor para o negócio a partir da existência de incerteza.

6. Riscos para os quais se busca proteção

6.1. Riscos inerentes às atividades do negócio

A abordagem do gerenciamento de riscos adotada pela Companhia tem por escopo primordial a identificação e a adoção de mecanismos de proteção aos riscos inerentes ao negócio e seu desenvolvimento. Esses riscos possuem diferentes fontes, podendo emergir desde o planejamento estratégico até os impactos externos projetados por meio da atividade fim.

Dentre estes, fazem parte do escopo do gerenciamento de riscos:

- Riscos provenientes de projetos e iniciativas, observados desde as etapas de planejamento e definição de escopo até a sua implementação e monitoramento;

- Riscos provenientes da aquisição de novos negócios, observados desde as modalidades de aquisição, incorporação, joint venture até a combinação de negócios;

- Riscos observados nas atividades, plataformas tecnológicas e processos que compõem a cadeia de valor do negócio, abrangendo tanto os processos finais quanto os processos de gestão e sustentação;

- Riscos ligados ao desenvolvimento das operações da Companhia e que possam impactar a continuidade do negócio e/ou resultar em perdas operacionais;

- Riscos relacionados à conduta, integridade e conformidade, considerando o respeito aos valores da Companhia e ao seu Código de Ética e Conduta, bem como as políticas, regimentos, normas e procedimentos internos, assim como a obediência à legislação vigente e às determinações dos órgãos reguladores e autoridades;

- Riscos relacionados à imagem e reputação da Companhia, considerando os impactos causados ao longo do desenvolvimento de sua atividade fim na sociedade, nas comunidades locais, no meio ambiente, e nas relações estabelecidas com as partes interessadas, incluindo acionistas, clientes, fornecedores, associados e outros parceiros de negócio.

6.2. Riscos de fontes externas

Para proteger e gerar valor para o negócio, o gerenciamento de riscos estende seu escopo aos ambientes externos no quais a Companhia e seus negócios estão inseridos, observando as constantes mudanças que ocorrem e na forma como elas podem afetar os objetivos do negócio, buscando ações que

permitam antecipar os impactos e reajustar o planejamento estratégico, de modo a mitigar riscos emergentes e explorar as oportunidades que surgem a partir desses cenários.

Para o gerenciamento dos riscos relacionados a esse ambiente são considerados aspectos como:

- As transformações na sociedade;
- Mudanças climáticas e questões ambientais;
- Pandemias, desastres naturais ou humanos;
- Incerteza quanto ao cenário político e econômico;
- Variações nas taxas e índices de mercado, como câmbio, inflação, PIB, dentre outras;
- Mudanças no ambiente regulatório, incluindo a legislação e a regulação de mercado vigentes e o surgimento de novas leis, jurisprudências ou determinações;
- Problemas de segurança pública;
- Aumento da competitividade;
- Avanços tecnológicos, mudanças nos padrões de consumo e comportamento e surgimento de novos nichos e segmentos;
- Aumento dos ataques cibernéticos.

6.3. Riscos monitorados por frentes específicas

A Companhia possui áreas e células dedicadas à proteção e ao controle de riscos específicos, abordados em paralelo às demais frentes citadas, mas também considerados no processo de gerenciamento de riscos, sendo eles:

- **Riscos de perda de mercadoria e patrimonial:** são riscos ligados a ocorrência de perdas operacionais e financeiras envolvendo os estoques de mercadoria e os ativos da Companhia, considerando perdas por obsolescência ou vencimento de itens perecíveis, quebra de mercadoria, desvios e furtos internos ou externos, arrombamentos, roubos ou ainda o mau uso;
- **Riscos de conduta:** são riscos associados ao ferimento da moral e da ética da Companhia, por descumprimento dos Códigos de Ética e

Conduta e das políticas associadas, tais como: ações que caracterizem assédio, corrupção, conflitos de interesse, discriminação, posicionamento político-partidário ou religioso, uso inadequado dos recursos da Companhia, dentre outros;

- **Riscos cibernéticos:** são riscos associados a vulnerabilidades desconhecidas, fragilidades e/ou obsolescência das plataformas tecnológicas, gestão de identidades e perfis de acesso, ao controle de hardware e software, gerenciamento de credenciais e ao tratamento de dados controlados e operados pela Companhia. Nessa categoria, incluem-se possíveis invasões externas ou acessos não autorizados as plataformas tecnológicas para roubo ou sequestro de dados, bem como falhas nas camadas de proteção, em procedimentos operacionais e/ou políticas internas ou ainda fraudes internas e/ou externas que afetem a disponibilidade de serviços e informações, a integridade dos dados controlados ou operados pela Companhia e a assertividade dos números e indicadores do negócio;
- **Riscos financeiros**: são riscos associados às finanças da Companhia, sendo preponderantes os riscos decorrentes de caixa e equivalentes de caixa, instrumentos financeiros derivativos, depósitos em bancos e outras instituições financeiras, bem como de exposições de crédito a clientes e os riscos relacionados a liquidez e a vinculação de garantias, sendo considerados, ainda, os riscos decorrentes de oscilações nas taxas de mercado e seus impactos no negócio;
- **Riscos nas demonstrações e reportes financeiros:** são considerados para esta classificação os riscos relacionados aos reportes financeiros da Companhia e a integridade das informações divulgadas ao mercado, sendo observados desde o momento em que são gerados os números para o fechamento contábil até sua efetiva divulgação e as posteriores retificações;
- **Riscos ESG:** são riscos decorrentes de uma má administração das questões socioambientais e dos impactos causados ao meio ambiente e à sociedade pelas atividades e operações do negócio, trazendo efeitos como: contaminação de solo, água ou ar, impactos negativos nas

comunidades próximas às operações da Companhia ou irregularidades no descarte de lixo e materiais ao longo da operação;

- **Riscos jurídicos:** riscos relacionados a questões de foro judicial, incluindo a ocorrência de causas trabalhistas individuais ou coletivas, multas por descumprimento da legislação aplicável ou de determinações e decisões judiciais, ocorrência de ações movidas contra a Companhia por responsabilidade civil ou infração ao Código de Defesa do Consumidor e demais regulamentações de mercado, bem como a existência de entraves legais ao desenvolvimento e a segurança jurídica do negócio.
- **Riscos de capital humano:** riscos relacionados à cultura corporativa, atratividade e retenção de talentos e garantia de que a Companhia tem as competências necessárias para viabilizar a estratégia de crescimento do negócio.

Os mecanismos e estruturas envolvidas na gestão dos riscos mencionados encontram-se descritos no item 4.5 desta Política.

7. Metodologia

7.1. Modelo das três linhas

As atividades de gerenciamento de Riscos têm como princípio a adoção do modelo das três linhas, que determina, de forma geral, as atribuições nos processos de gestão de riscos e de controles internos a três níveis organizacionais distintos que atuam de forma complementar nos esforços para proteção e mitigação de riscos.

O modelo e sua abordagem compreendem os seguintes componentes:

- **Primeira linha**: áreas que executam atividades finais, sendo responsáveis por gerenciar os riscos relacionados a entrega de produtos e serviços aos clientes no dia-a-dia da operação;
- **Segunda linha**: áreas especializadas que fornecem apoio a primeira linha, realizando monitorias e questionamentos quanto aos riscos gerenciados e oferecendo mecanismos de proteção a eles;

- **Terceira linha - Auditoria Interna**: realiza avaliação e assessoria de forma independente e objetiva para mensurar a efetividade dos mecanismos de proteção e mitigação de riscos desenvolvidos e executados pela primeira e segunda linhas;
- **Corpo Administrativo**: presta contas às partes interessadas e supervisiona a atuação das três linhas, avaliando a efetividade do gerenciamento de riscos e garantindo o comprometimento de todas as estruturas envolvidas por meio de integridade, liderança e transparência.

A atuação de todos os componentes do modelo também é avaliada periodicamente por prestadores externos de serviços de auditoria e avaliação independente. Com isso, busca-se o aprimoramento contínuo da estrutura de gerenciamento de riscos e das práticas de controle adotadas.

7.2. Identificação e classificação dos riscos

O processo de gerenciamento de riscos se inicia a partir da identificação de fatores de risco que podem, de alguma forma, impactar os objetivos do negócio. A etapa de identificação de riscos ocorre com base nas fontes de risco citadas no tópico 4.3 desta Política, podendo ocorrer de forma estruturada e planejada ou através da comunicação com outras áreas que identifiquem possíveis fatores de risco em seus processos e atividades.

Os riscos identificados são detalhados e agrupados em diferentes categorias com base no tipo de impacto que podem trazer, sendo eles:

- **Impacto Estratégico**: riscos cujo impacto está relacionado ao atingimento dos objetivos estratégicos do negócio, no curto, médio e longo prazo;
- **Impacto Operacional**: riscos decorrentes da inadequação ou falha na gestão de processos internos, tendo como principais impactos perdas financeiras e o comprometimento da produtividade e do nível de serviço;
- **Impacto na Conformidade**: riscos que se originam a partir do não cumprimento da legislação e/ou regulamentação externa, bem como às normas e procedimentos internos e contratos;

- **Impacto na Reputação**: riscos associados à imagem da Companhia e de suas marcas perante seus clientes, parceiros, fornecedores e demais partes interessadas.

A descrição dos fatores e das possíveis consequências passam a compor o detalhamento do risco, junto com informações sobre os processos e/ou atividades nos quais são observados e quem são as pessoas ou áreas responsáveis por elas.

7.3. Avaliação e priorização

Uma vez listados, detalhados e categorizados, os riscos são avaliados e priorizados com base em sua criticidade. Essa avaliação é feita por meio de uma escala qualitativa para medir a probabilidade de ocorrência e o nível de impacto caso o risco se materialize, sendo consideradas análises e estudos internos para precisar com maior assertividade a criticidade dos riscos.

A avaliação e mensuração do grau de criticidade são reunidas junto com as demais informações detalhadas na etapa de identificação e classificação e consolidadas na Matriz de Riscos. Os riscos listados com o maior grau de criticidade passam a assumir a classificação de risco prioritário.

7.4. Comunicação e resposta aos riscos

A Matriz de Riscos é compartilhada com a área responsável pelo processo ou atividade na qual o risco é observado, sendo posteriormente discutida em conjunto com a área de Riscos e Controles as medidas e ações de resposta aos riscos prioritários. Com isso, é montado um plano de ação para cada um desses riscos com o intuito de implementar medidas e controles que permitam reduzir a criticidade do risco por meio da diminuição de sua probabilidade de ocorrência e/ou através da mitigação dos impactos e consequências dele provenientes.
Os planos de ação são apresentados junto com o Mapa de Riscos da Companhia ao menos uma vez ao ano e sempre que necessário para a Diretoria, Conselho de Administração e Comitê de Auditoria com o intuito de fortalecer e garantir o andamento das ações e fornecer apoio na tomada de decisão.

7.5. Monitoramento e reavaliação

Os riscos mapeados são monitorados constantemente pela primeira e segunda linhas através de atividades gerenciais contínuas e/ou avaliações independentes, indicadores de riscos, implantação dos planos de ação e alcance de metas, sendo também acompanhadas as ações para mitigação e controle desses riscos como parte do escopo de atuação das áreas de Gestão de Riscos e Controles Internos e da Auditoria Interna.

Qualquer mudança significativa nos processos ou iniciativas que impactem a criticidade dos riscos implica em uma necessidade de reavaliação dos mesmos, e por consequência, da Matriz e do Mapa de riscos, podendo acontecer a qualquer momento. O mesmo se aplica no caso de mudanças não previstas no ambiente externo a organização ou na própria percepção e apetite de risco da Companhia.

O Mapa de Riscos é revisado sempre que necessário e pelo menos uma vez ao ano é apresentado e validado pelo Conselho de Administração e Comitê de Auditoria. Para cada revisão, os riscos que o compõe são reavaliados com base no cenário e diretrizes vigentes, podendo haver alteração nos riscos prioritários caso surjam riscos emergentes ou fatos e eventos de elevada magnitude que alterem as pontuações de criticidade de um ou mais riscos no mapa. Os riscos considerados prioritários têm seus planos de ação acompanhados pelo Conselho de Administração por meio de seus Comitês de Assessoramento.

8. Responsabilidades

As atividades de gerenciamento de riscos e as diretrizes e princípios descritos nesta Política são coordenadas e executadas por agentes presentes nas três linhas, sendo suas atribuições distribuídas da forma a seguir.

8.1. Do Conselho de Administração

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

8.2. Do Comitê de Auditoria

- Fornecer ao Conselho de Administração, sempre que necessário, sua percepção do grau de exposição a riscos da Companhia e influenciar na definição dos limites de apetite ao risco;
- Avaliar e validar a revisão anual do Mapa de Riscos, bem como os planos de ação para tratamento dos riscos prioritários;
- Monitorar os riscos prioritários que não estiverem sendo acompanhados pelos demais Comitês de Assessoramento conforme direcionamento do Conselho de Administração.

8.3. Da Diretoria

- Revisar as diretrizes, Matriz e Mapa de Riscos, determinando os limites de exposição e deliberando quanto às ações para mitigação dos riscos;
- Definir e dar suporte à estrutura de gerenciamento de Riscos da Companhia;
- Definir, em conjunto com a área de Riscos e Controles Internos e a primeira linha, os planos de ação para mitigação dos Riscos, dando suporte para a sua execução;
- Supervisionar o processo de avaliação de Riscos e monitorar a evolução da exposição aos Riscos e os sistemas de gerenciamento de Risco;
- Validar e garantir o cumprimento dos planos de contingência, de modo a garantir a Continuidade do Negócio;
- Disseminar a cultura da gestão de Riscos na Companhia.

8.4. Da área de Riscos e Controles Internos

- Definir e desenvolver a metodologia para gerenciamento de riscos internamente;
- Elaborar e atualizar a Matriz de Riscos, revisando as informações contidas sempre que houver mudanças relevantes na percepção de criticidade dos riscos;
- Interagir com as áreas críticas da Companhia, de modo a se antecipar aos Riscos decorrentes de iniciativas e projetos, bem como às vulnerabilidades identificadas em novos negócios;
- Analisar os processos atuais sob a ótica de Riscos e Controles Internos, avaliando, implantando e monitorando ações e controles com o objetivo de reduzir a exposição ao Risco;
- Identificar oportunidades para o negócio a serem exploradas nos processos e cenários analisados;
- Operacionalizar e disponibilizar à Diretoria, ao Comitê de Auditoria e ao Conselho de Administração o Mapa de Riscos da Companhia, contendo os riscos prioritários e os respectivos planos de ação para resposta;
- Identificar o potencial de impacto na continuidade do negócio dos riscos mapeados em cada uma das frentes de atuação, estruturando junto as áreas de negócio ações de contingência e procedimentos de resposta em um plano de contingência;
- Comunicar, tempestivamente, os eventos de Risco que apresentarem tendência de ocorrência e/ou eventual extrapolação de limites, para discussão nos fóruns e alçadas apropriadas;
- Fornecer apoio metodológico aos departamentos operacionais e funcionais da Companhia por meio de ferramentas e serviços sob demanda, apresentando, quando solicitado, sua percepção quanto à exposição ao Risco em um determinado processo, projeto ou iniciativa;
- Redesenhar processos críticos junto a primeira linha e normatizar os processos redesenhados.

8.5. Da área de Auditoria Interna

- Aferir a qualidade e a efetividade dos processos de gerenciamento de Riscos da Companhia, sugerindo alterações ao Conselho de Administração, Comitê de Auditoria e à Diretoria, quando necessário;
- Testar a efetividade dos controles e medidas implementadas para mitigação dos riscos;
- Identificar eventuais vulnerabilidades nos processos da Companhia e comunicá-las em tempo hábil para a área de Riscos e Controles Internos;
- Atuar junto a primeira e segunda linhas no tratamento de desvios e vulnerabilidades identificadas, supervisionando a implementação de ações corretivas para mitigação de riscos;
- Verificar e testar periodicamente a existência e a adequação do Plano de Continuidade do Negócio e dos planos de contingência para as principais atividades da Companhia.

8.6. Dos Gestores responsáveis pelos processos de negócio (primeira linha)

- Elaborar planos de ação e medidas para mitigação de riscos apontados em conjunto com a área de Riscos e Controles Internos;
- Operacionalizar os controles, ações e indicadores utilizados no gerenciamento e monitoramento dos riscos que incorrem em seus processos;
- Munir a área de Riscos e Controles Internos com os dados e informações necessários para desempenhar as atividades de mapeamento de processos e de identificação e avaliação de riscos;
- Comunicar mudanças significativas nos fluxos mapeados que possam alterar os níveis de criticidade dos riscos levantados, bem como informar o surgimento de novos riscos e vulnerabilidades, variações ou inovações em seus processos e sistemas.
- Comunicar a área de Riscos e Controles Internos, tempestivamente, caso controles para riscos críticos se tornem inoperantes, de modo a

desenvolverem, em conjunto, medidas e ações paliativas para que a indisponibilidade não aumente a exposição ao risco;

- Fornecer sua percepção sobre a adequação de controles e ações para mitigação dos riscos em seus processos para as áreas de Riscos e Controles Internos e para a Auditoria Interna;
- Implementar medidas de contingência e de resposta a crises na ocorrência de eventos que possam impactar a continuidade do negócio seguindo as diretrizes e planos previamente definidos.

9. Frentes de combate a riscos específicos

Além das áreas que atuam diretamente no processo de Gerenciamento de Riscos Corporativos mencionadas no tópico 7.1, a Companhia dispõe de outros mecanismos e estruturas responsáveis pelo monitoramento de riscos específicos ou que oferecem subsídio e insumos relevantes para a Gestão de Riscos, sendo eles:

- **Controle e Prevenção de Perdas**

O Departamento de Controle e Prevenção de Perdas é a principal frente no combate a riscos operacionais relacionados ao estoque e a segurança patrimonial, atuando continuamente para fiscalizar processos de movimentação de mercadorias, verificar o cumprimento de procedimentos, identificar fragilidades para possíveis perdas e propor as alterações necessárias para eliminá-las, sendo pioneiro na busca por soluções de equipamentos e tecnologia para mitigação de riscos que possam afetar as mercadorias, a segurança e o patrimônio da Companhia.

Sua atuação compreende desde a monitoria dos processos dos Centros de Distribuição, do Transporte e das lojas físicas até as medidas de resposta a incidentes e sinistros, além de ser a principal área responsável por disseminar a cultura de controle e de prevenção às perdas na Companhia estando presente ao longo de toda a Cadeia de valor do negócio.

- **Investigações**

A área de Investigações é altamente treinada, imparcial e independente para apurar casos suspeitos de fraudes e de outras ações que possivelmente contrariem os valores, Códigos de Ética e Conduta e demais Políticas e Regimentos da Companhia.

A partir do resultado das suas próprias monitorias, das checagens da Auditoria Interna, do acionamento das demais áreas da Companhia mediante a algum comportamento indevido ou caso suspeito ou das demandas que chegam a partir do Canal de Denúncias, a área de Investigações tem elementos para o início de suas apurações contando para isso com bastante experiência e especialização em técnicas de entrevista, forense e análise SCAN.

- **Canal de Denúncias**

A Companhia, disponibiliza um Canal de Denúncias, Disk Alerta, confidencial e sigiloso destinado e acessível a todos.
As denúncias sobre condutas que violem os princípios éticos e padrões de conduta e/ou a legislação vigente são recebidas por uma empresa terceirizada, independente e especializada, podendo ser feitas de maneira anônima, estando disponível 24 horas por dia, sete dias por semana, online no site https://canaldedenuncias.com.br/universoamericanas ou pelo telefone 0800 282 2550.

Todos os envolvidos em denúncias têm reservados os seus direitos à privacidade e confidencialidade, sendo inaceitáveis quaisquer formas de coação ou represálias para os denunciantes. Todas as denúncias recebidas são apuradas pela célula de Investigações da Companhia, e classificadas, ao término da apuração, como procedente, improcedente ou inconclusiva.

A Companhia buscará, sempre que possível e dentro da melhor diligência, individualizar e particularizar as condutas que possam vir a ser enquadradas como crime punível em conformidade com a Lei 12.846/13 (“Lei Anticorrupção”),

informando e colaborando com as autoridades competentes para a completa apuração e responsabilização dos indivíduos que as praticarem.

A responsabilidade dos indivíduos sujeitos às Políticas de Compliance, de Combate à Corrupção e de Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo da Companhia também será apurada e, caso confirmada, estes responderão pessoalmente pelos crimes cometidos, nos termos da Lei Anticorrupção, bem como pela eventual reparação de danos sofridos pela Companhia em decorrência da prática de tais atos.

Serão responsabilizados, de igual forma, os indivíduos sujeitos as Políticas de Compliance, de Combate à Corrupção e de Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo da Companhia que tiverem praticado o ato lesivo e também aqueles que tiverem conhecimento de sua prática, mas que, comprovadamente, tenham se omitido. Sem prejuízo das penalidades legais aplicáveis e também daquelas que decorrem do contrato de trabalho, do fornecimento de mercadorias e/ou de prestação de serviços, responderão pelos prejuízos eventualmente causados à Companhia e/ou a terceiros.

- **Segurança da Informação**

A área de Segurança da Informação atua continuamente na identificação e monitoramento de desvios, vulnerabilidades e ocorrências que envolvam as plataformas tecnológicas da Companhia, monitorando os principais processos, fluxos financeiros, infraestruturas, aplicações, serviços e ativos de tecnologia, de modo a assegurar o cumprimento de políticas, procedimentos e controles sistêmicos.

Dentro de escopo de suas atividades está a garantia da realização de testes frequentes de invasão, proteções contra negação de serviços, serviços de CDN (Content Delivery Network) de alta disponibilidade e capacidade, soluções anti-phishing (Brand Protection), Anti-Bot e antifraudes, monitoramento de ameaças e da deep e darkweb garantindo um processo de gestão contínua de vulnerabilidades e de identificação e mitigação de riscos cibernéticos,

operacionalizando também ferramentas tradicionais como IPS, EDRs, DLPs, Firewalls e monitoria de redes, ativos e clouds privados e públicos.

Com isso, é a principal estrutura responsável pela identificação de possíveis falhas e eventos ocasionados por agentes externos e internos que possam impactar na continuidade do negócio no que tange a disponibilidade das plataformas tecnológicas, agindo de forma preventiva na identificação de medidas de proteção e contingência, de forma detectiva e reativa nas atividades de recuperação de desastres, respostas a incidentes cibernéticos e retomada do negócio caso os cenários previstos se materializem.

- **Planejamento financeiro e Tesouraria**

As áreas de Planejamento Financeiro e Tesouraria monitoram continuamente os riscos relacionados à gestão do caixa, crédito e liquidez da Companhia, bem como os impactos provenientes das variações nas taxas praticadas no mercado. Para isso, monitora e reporta com frequência indicadores que refletem a saúde financeira da Companhia, tomando ações em conjunto com a Diretoria para ajustar o planejamento financeiro necessário.

Dentre os instrumentos utilizados com esse propósito estão as Reuniões de Caixa, realizadas semanalmente, e os Comitês Financeiros, realizados trimestralmente, com o objetivo de fornecer à Diretoria e aos Membros do Comitê Financeiro, respectivamente, informações financeiras atualizadas.

- **Controladoria**

A Controladoria representa uma das principais frentes de combate a riscos relacionados aos reportes e demonstrações financeiros e as atividades de divulgação de resultados, zelando pela integridade e precisão dos registros financeiros da Companhia de acordo com as normas aplicáveis através de controles e revisões periódicas.

- **Sustentabilidade**

A Companhia tem o compromisso com o desenvolvimento sustentável buscando, constantemente, a redução de impactos para o meio ambiente e o equilíbrio entre responsabilidade social e desenvolvimento econômico-

financeiro. Para isso, conta com a área de Sustentabilidade, que operacionaliza uma série de indicadores e monitora de forma contínua os impactos causados pelo negócio em comunidades locais, nas pessoas nelas inseridas e no meio-ambiente, desenvolvendo e implementando ações para evitar, minimizar ou reparar os impactos nelas causados.

A Companhia também prevê a realização de *due dilligence* em relação a impactos socioambientais. Nossa atuação contempla o monitoramento de riscos e oportunidades climáticos e ambientais, visando posicionar a Companhia de modo que possa gerenciar seus impactos e contribuir para sociedade e meio ambiente com medidas sustentáveis.

- **Comunicação Corporativa**

A área responsável pela Comunicação Corporativa atua para combater riscos ligados a imagem e reputação da Companhia e de suas marcas, monitorando notícias, publicações e movimentações e tendências em redes sociais que possam trazer impactos negativos nessa dimensão, como um aumento no número de reclamações, percepções negativas por parte do público e da sociedade ou ainda a perda de clientes.

- **Jurídico**

Dentre suas atribuições, o Jurídico atua de forma constante para assegurar a legalidade da condução dos negócios da Companhia, buscando prevenir riscos associados às leis e políticas externas, como o Código de Defesa do Consumidor, por exemplo, e também inerentes às políticas das plataformas da Companhia (Política de Privacidade, Termo de Uso, dentre outras), aos Códigos de Ética e Conduta e às demais políticas relacionadas.

O Jurídico também observa com a percepção de risco os contratos, ações judiciais e outras questões legais, dando subsídio para as áreas de negócio em relação a riscos decorrentes de processos trabalhistas e atividades ilegais ou criminosas que afetem a Companhia, atuando para garantir a integridade nas relações entre a Companhia, seus associados, fornecedores, parceiros, clientes e demais partes interessadas.

- **Gente**

A área de Gente é responsável por divulgar e disseminar o propósito, os valores e princípios da Companhia, bem como o Código de Ética e Conduta, o que é feito desde o processo de admissão e ao longo das etapas de desenvolvimento dos associados por meio de treinamentos e outras iniciativas. Além disso, é a área responsável por garantir a atratividade dos nossos programas de recrutamento e seleção, por apoiar o acompanhamento e desenvolvimento dos talentos da Companhia, por aperfeiçoar continuamente a estratégia está presente na tomada de decisão referente a qualquer risco relacionado especificamente aos associados, como desvios de conduta e causas trabalhistas.

- **Antifraude e Meios de pagamento**

Consiste em uma equipe que realiza análises dos pedidos realizados nas plataformas tecnológicas, atuando com métodos e ferramentas de monitoria voltados para a identificação de possíveis fraudes em meios de pagamento, impedindo perdas financeiras através do cancelamento de pedidos fraudulentos que ainda estão em análise.

- **Compliance**

É a área responsável por disseminar continuamente uma cultura de ética, riscos e conformidade com a legislação e com os seus valores e princípios, mantendo um Programa de Compliance, o Ética na Prática, voltado para todos os stakeholders da Companhia. Avalia e monitora, em conjunto com a área de Riscos e Controles Internos, as exposições de risco de Compliance da Companhia, tendo em vista o ambiente externo, leis, regulamentações e as normas internas inerentes à atuação dos seus stakeholders, combinando análises de indicadores com uma plataforma tecnológica própria para combater fraudes, utilizando algoritmos complexos de monitoramento e análises dados (Data Analytics e IA) e comportamentos, para bloquear a entrada, suspender ou remover da nossa cadeia de valor eventuais agentes inidôneos, bem como itens, ofertas ou serviços fora dos padrões estabelecidos.

- **Compliance Ame Digital**

Essa área é responsável por identificar e reportar riscos operacionais relacionados à Ame Digital sob a ótica de uma instituição financeira, estabelecendo controles internos voltados para a integridade das transações e dos números apurados, sendo também responsável por responder aos órgãos reguladores aplicáveis, como o Banco Central.

9. REFERÊNCIAS

Código de Ética e Conduta;

Política de Fornecedores;

Política de Segurança da Informação;

Política de Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo;

Política de Compliance.