Índice

5.1 Descrição do gerenciamento de riscos e riscos de mercado

5.1. - Descrição do gerenciamento de riscos e riscos de mercado

A Companhia informa que segue conduzindo esforços para revisar e aprimorar suas estruturas de governança de modo a fortalecer seu ambiente de controle e disseminar uma cultura de gerenciamento de riscos dentro do negócio. A Política de Gerenciamento de Riscos segue em revisão, com previsão para aprovação pela Alta Administração ainda no ano de 2024.

(a) se o emissor possui uma política formalizada de gerenciamento de riscos, destacando, em caso afirmativo, o órgão que a aprovou e a data de sua aprovação, e, em caso negativo, as razões pelas quais o emissor não adotou uma política

A Companhia possui uma política de gerenciamento de riscos, a qual foi formalmente atualizada e aprovada em Reunião do Conselho de Administração da Companhia, realizada em 09 de agosto de 2022 ("Política de Gerenciamento de Riscos").

Além disso, adotamos também políticas formais complementares destinadas ao gerenciamento de nossos riscos, tais como: Código de Ética e de Conduta, Política de Transações com Partes Relacionadas e Administração de Conflitos de Interesses, Política de Compliance, Política de Combate à Corrupção, Política de Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo dentre outras.

As nossas políticas, códigos e regimentos podem ser consultados em nosso *website* de relações com investidores: ri.americanas.io

(b) os objetivos e estratégias da política de gerenciamento de riscos, quando houver, incluindo:

A Política de Gerenciamento de Riscos tem por objetivo estabelecer princípios, diretrizes e responsabilidades a serem observados no processo de gerenciamento de riscos inerentes às atividades de negócio do Emissor, de forma a identificar e monitorar os riscos relacionados à mesma ou seu setor de atuação.

i. Riscos para os quais se busca proteção

A Companhia tem como escopo de sua política de gerenciamento de riscos a proteção contra riscos internos, ou seja, aqueles inerentes ao negócio, e externos, que dependem do contexto no qual o Emissor está inserido. Além disso, uma série de outros fatores de risco são monitorados no dia a dia por frentes específicas, como riscos associados às demonstrações financeiras ou a conduta de associados, parceiros e fornecedores.

i.i. 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:
a) Os riscos provenientes de aquisições, projetos e iniciativas;
b) Riscos observados nas atividades, plataformas tecnológicas e processos que compõem a cadeia de valor do negócio;
c) Riscos que possam impactar a continuidade do negócio e/ou resultar em perdas operacionais;
d) Riscos relacionados a conduta, integridade e conformidade;
e) Riscos relacionados à imagem e reputação da Companhia.

i.ii. Riscos de fontes externas

Para proteger e gerar valor para o negócio, o gerenciamento de riscos estende seu escopo ao ambiente externo, no qual 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.

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

5.1 Descrição do gerenciamento de riscos e riscos de mercado

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

i.iii. Riscos monitorados por frentes específicas

Em sua estrutura organizacional, 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:

a) Riscos de perda de mercadoria e patrimonial;
b) Riscos de conduta;
c) Riscos cibernéticos;
d) Riscos financeiros (crédito, liquidez, garantias, etc.)
e) Riscos nas demonstrações e reportes financeiros;
f) Riscos ambientais;
g) Riscos jurídicos.

ii. Instrumentos Utilizados para Proteção

O sistema de gerenciamento de riscos é composto por um processo definido com base nos principais *frameworks* para gerenciamento de riscos, como a ISO31000 e o COSO II, sendo ele composto pelas etapas de (a) identificação dos riscos e fatores de risco; (b) avaliação e priorização dos riscos (c) plano de ação para resposta ao risco e (d) monitoramento e reavaliação:

Durante esse processo são utilizadas ferramentas como a Matriz de probabilidade x impacto, onde os riscos identificados são avaliados com base em sua probabilidade (ou frequência esperado) e em seu potencial de impacto para os objetivos do Emissor para se chegar a uma pontuação denominada grau de risco. O Mapa de Riscos, também utilizado, concentra todos os riscos avaliados, listados com base em sua criticidade (grau de risco) e agrupados com base nas categorias citadas no tópico i. do Item 5.1 do presente formulário.

Essas ferramentas são operacionalizadas pela área de Riscos e Controles Internos, e o resultado, que pode ser visualizado através do mapa de riscos do Emissor, é apresentado uma vez por ano e sempre que necessário ao Conselho de Administração e Comitê de Auditoria, junto ao plano de ação de cada um dos riscos classificados como prioritários. As demais áreas componentes da segunda e primeira linha, em conjunto com a Administração, priorizam o acompanhamento das ações e os indicadores relacionados a esses riscos que são monitorados regularmente nas três linhas.

Além disso, o Emissor se utiliza de instrumentos formais como políticas, códigos e regimentos para assegurar que haja uma maior proteção de valor e um menor desvio em relação aos objetivos almejados, como é o caso do Código de Ética e de Conduta, que visa reduzir a ocorrência de riscos de Conduta.

Cabe ressaltar ainda que o Emissor possui um sistema de Controles Internos que objetiva não só aprimorar e assegurar a integridade das demonstrações financeiras, mas também fornecer a primeira e segunda linhas um importante mecanismo para a proteção de valor, que possibilita identificar e tratar erros e desvios nos processos que poderiam configurar riscos operacionais materializados. Além disso, a Companhia também conta com uma área de Auditoria Interna responsável por testar a eficiências dos controles.

5.1 Descrição do gerenciamento de riscos e riscos de mercado

iii. Estrutura Organizacional de Gerenciamento de Riscos

A estrutura organizacional do gerenciamento de riscos é composta das seguintes áreas/órgãos, além das áreas de primeira linha diretamente relacionadas ao risco priorizado, com as seguintes competências:

Conselho de Administração

O Conselho de Administração é responsável por:

- Validar as diretrizes gerais para o gerenciamento de riscos da americanas s.a.;
- 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.

Comitê de Auditoria:

Compete ao 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.

Diretoria

A Diretoria é responsável por:

- 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 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 e em suas controladas.

Área de Riscos e Controles Internos

A Área de Riscos e Controles Internos são responsáveis por:

- 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 e aquisições;
- 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;
- Operacionalizar e disponibilizar à Diretoria, ao Conselho de Administração e Comitê de Auditoria 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

5.1 Descrição do gerenciamento de riscos e riscos de mercado

de ferramentas e serviços sob demanda, apresentando, 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.

Auditoria Interna

A área de Auditoria Interna é responsável por:

- Aferir a qualidade e a efetividade dos processos de gerenciamento de Riscos da Companhia, sugerindo alterações ao Conselho de Administração, ao 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.

Investigações

A área de Investigações é responsável por:

- Apurar casos suspeitos de fraudes e de outras ações que possivelmente contrariem os valores, Código de Ética e Conduta e demais Políticas da Companhia;
- Utilizar técnicas de entrevista, forense e análise SCAN para levantamento de dados e apuração de suspeitas, que podem ser recebidas por meio de monitorias próprias, checagens da Auditoria Interna, acionamento das demais áreas da Companhia ou através do Canal de Denúncias;
- Gerenciar o canal de denúncias e as denúncias recebidas por meio deste.

c. a adequação da estrutura operacional e de controles internos para verificação da efetividade da política adotada

Ao longo do ano de 2023, a Companhia conduziu uma série de trabalhos com auxílio de consultorias externas para avaliar o sistema de controles internos e a metodologia de gerenciamento de riscos, considerando desde os processos em escopo até a adequação da estrutura responsável por conduzir as atividades. Os trabalhos realizados originaram uma série de melhorias nos controles internos, sobretudo nas frentes financeiras e contábeis, incluindo a implementação e revisão de controles existentes, adoção de boas práticas e mudanças nos fluxos dos processos. Parte dessas melhorias encontra-se em fase de implementação, sendo acompanhada diariamente em um fórum dedicado.

Nossa administração monitora e avalia se as operações que efetuamos estão de acordo com as políticas por nós adotadas e se representam exposição a riscos que comprometam o atendimento dos nossos objetivos. Além disto, na data deste Formulário de Referência, possuímos um Comitê de Auditoria instalado, conforme prática recomendada pelo Novo Mercado, e sempre que necessário revisamos nossos códigos e políticas internas para adequá-los e atualizá-los.

5.2 Descrição dos controles internos

5.2. Descrição dos Controles Internos

O monitoramento do nosso ambiente de controles internos é um processo contínuo que visa mitigar riscos, manter razoável segurança do atingimento dos objetivos, bem como suportar a preparação das demonstrações financeiras de acordo com as normas aplicáveis. Desta forma, a Companhia segue permanentemente fortalecendo seu ambiente de controles internos e disseminando a cultura de gerenciamento de riscos em todos os níveis da organização.

a) Principais práticas de controles internos e o grau de eficiência de tais controles, indicando eventuais imperfeições e providências adotadas para corrigi-las

Os processos de gestão de riscos e de controles internos da Companhia estão estabelecidos com base nas melhores práticas de mercado reconhecidas internacionalmente, entre elas premissas dos frameworks COSO (Committee of Sponsoring Organizations of the Treadway Commission) e COBIT (Control Objetctives for Information and related Technology). Neste sentido, a administração da Companhia possui um conjunto de normas, políticas e procedimentos que constituem a base para a prática de controles internos em toda a sua operação, incluindo: (i) Controles de alto nível (Entity Level Controls); (ii) Controles de Sistema de Informação (IT Level Controls); e (iii) Controles de nível dos processos (Process Level Controls) entre outros aspectos relevantes, tais como conduta, ética e compliance.

As práticas adotadas têm por objetivo promover um sistema de Controles Internos robusto em um ciclo de melhoria contínua, revisando os controles adotados e implementando novos sempre que necessário com o objetivo de aperfeiçoar os níveis de controle da organização e assegurar a integridade de todas as suas transações.

b) Estruturas organizacionais envolvidas

Nossas atividades de gerenciamento de riscos e controles realizadas têm como princípio a adoção do Modelo das Três Linhas de Defesa, que determina papéis e responsabilidade em 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:

- 1ª Linha: Áreas que executam atividades finais, sendo responsáveis por executar as atividades de controle relacionados a entrega de produtos e serviços aos clientes no dia-a-dia da operação;
- 2ª Linha: áreas especializadas que fornecem apoio à Primeira Linha, realizando monitorias e questionamentos quanto aos controles praticados e oferecendo mecanismos de proteção aos riscos identificados (como áreas de Riscos, Controles, Compliance, Segurança da Informação entre outras);
- 3ª Linha: área de Auditoria Interna, responsável por realizar avaliação e assessoria de forma independente e objetiva para mensurar a efetividade dos mecanismos de proteção e mitigação de riscos desenvolvidos e executados pelas Primeira e Segunda linhas, identificando e comunicando oportunidades de melhoria.
- 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.

5.2 Descrição dos controles internos

Neste modelo, são realizados reportes periódicos de riscos e controles internos à diretoria estatutária, ao Comitê de Auditoria e ao Conselho de Administração.

c) se e como a eficiência dos controles internos é supervisionada pela administração do emissor, indicando o cargo das pessoas responsáveis pelo referido acompanhamento

No nível das transações, as atividades de controles internos são implementadas, monitoradas e avaliadas em todos os estágios dos processos de negócios e no âmbito da tecnologia da informação. Estas atividades de controles variam em sua natureza e abrangem um conjunto de atividades manuais e automatizadas, tais como autorizações e aprovações, conferências, reconciliações e avaliações de desempenho de negócios. Os principais executivos da Companhia, incluindo cargos gerenciais e de diretoria, são responsáveis pelo acompanhamento da evolução das práticas e da evolução dos controles ao longo do tempo. A Companhia conta com uma área de Controles Internos responsável por gerenciar os controles executados pela primeira linha, de forma a identificá-los e auxiliar as áreas responsáveis pelos mesmos sanando eventuais deficiências.

Além disso, as atividades de testes e avaliação de efetividade de controles realizadas pela área de Controles Internos e pela Auditoria Interna são reportadas periodicamente para a diretoria estatutária, Comitê de Auditoria e Conselho de Administração que fornecem o apoio necessário para a priorização e implementação de ações que visem a aprimorar o sistema de Controles Internos da Companhia.

d) Deficiências e recomendações sobre os controles internos presentes no relatório circunstanciado do auditor independente

Em 11 de outubro de 2024, os auditores independentes emitiram relatório circunstanciado de recomendações sobre os trabalhos realizados relativos à auditoria das demonstrações financeiras de 2023 da Companhia e suas controladas. Conforme o relatório, os assuntos reportados não representaram riscos de distorções relevantes para as demonstrações financeiras e, portanto, não alteram o relatório de auditoria de 14 de agosto de 2024, quando da divulgação dos resultados.

A Administração da Companhia realizou todos os ajustes necessários nas demonstrações financeiras de 2023 e concluiu que as referidas demonstrações financeiras, apresentadas em 14 de agosto de 2024, com opinião sem ressalvas do auditor independente, apresentam adequadamente, em todos os aspectos relevantes, a condição financeira, os resultados de operações e o fluxo de caixa, uma vez que os efeitos de todos os fatos conhecidos pela administração até a conclusão das demonstrações financeiras já foram nelas refletidos.

Especificamente sobre o relatório do período, a Companhia tem como uma de suas principais prioridades o endereçamento das recomendações dos auditores e tem adotado todas as medidas necessárias (resumidas abaixo) visando o tratamento das deficiências significativas reportadas dividas em 3 blocos: (i) Contábil; (ii) Tecnologia da Informação; e (iii) Normas e Procedimentos Operacionais, quais sejam:

(i) Contábil:

• Controles de reconciliação de cartões e extratos de operadoras e terceiros:

Não foi identificado um procedimento uniforme de reconciliação de algumas transações e saldos existentes em Contas a Receber. Estamos revisando e reavaliando o controle executado pelas áreas de Conciliação e Contabilidade com o objetivo de tornar o processo de conciliação mais estruturado e assertivo, incluindo a implementação de um novo sistema de conciliação.

• Ausência de análise na preparação do relatório CAP para confrontar com a posição contábil:

Foi identificado que os controles de revisão das análises das contas contábeis não foram suficientes para detectar a ausência de algumas transações de cartão de crédito. O plano de ação em curso inclui revisar e atualizar os dados cadastrais dos fornecedores, eliminando eventuais inconsistências, padronizando as nomenclaturas e classificando contabilmente de maneira correta, o que irá sanar o apontamento.

(ii) Tecnologia da Informação:

• Gestão de Acessos:

Foi identificada ausência de processo apropriado de revisão de acessos para alguns sistemas, além de falhas na revogação de acessos. Estamos aprimorando o processo visando a integração dos sistemas e

5.2 Descrição dos controles internos

melhor gestão de acessos e identidades dentro do padrão de governança de tecnologia, o que tornará o processo mais eficaz, controlado e seguro.

• Trilhas de Auditoria:

O auditor recomendou ampliação dos controles de armazenamento dos logs de atividades sistêmicas, incluindo de log de acessos, ações e eventos dos usuários dos sistemas. Estamos avaliando a implementação dos controles adicionais relacionados nos respectivos sistemas.

• Segregação de Acessos de Ambientes Sistêmicos:

Embora a Companhia possua ambientes sistêmicos segregados, foram identificados acessos de mesmos usuários em ambientes de PRD (Produção) e DEV (Desenvolvimento). A Companhia está revisando os acessos e o processo respectivo visando garantir fluxo de aprovação apropriado entre outras iniciativas que garantam a segurança nos diferentes ambientes sistêmicos.

• Segregação de Acessos de Usuários:

Entendemos que a elaboração de uma matriz SOD irá sanar a deficiência apontada, pois será possível realizar o controle de segregação de acessos e a criação de um padrão de acesso definido por funções. Como plano de ação paliativo até a elaboração de uma matriz SOD, serão implementados controles compensatórios de revisões de perfis de acessos adotando critérios de periodicidade para os sistemas.

• Gestão de Mudanças:

Foram identificados chamados de mudanças sistêmicos já concluídas (em produção) como status "em aberto" na ferramenta de gestão dos chamados respectiva. Estamos aprimorando os fluxos para assegurar maior tempestividade do tratamento e controle dos chamados, incluindo análise prévia e sua baixa sistêmica.

• Plano de Continuidade de Negócios e Plano Recuperação de Desastres:

Para Americanas, não foram identificadas evidências apropriadas dos testes de simulação/efetividade dos planos de Recuperação de Desastres, e especificamente para a unidade de negócio HNT, não foi identificado um Plano de Continuidade do Negócio formalizado. Ambos os apontamentos estão sendo tratados, incluindo a documentação dos testes realizados e formalização da documentação dos planos envolvidos.

• Uso de contas genéricas e duplicadas:

Foi identificado ausência de gestão de identidade única e padronização de usuários. Entre os planos de ação em andamento, estamos revisando o processo de gestão de acesso com eliminação dos usuários duplicados e das contas genéricas.

• Ausência de processo de Gestão de Mudanças (Aplicável ao Negócio HNT):

Estamos revisando o processo de gestão de mudanças da HNT, incluindo normativos, processo e ferramentas de controles associadas.

(iii) Normas e Procedimentos Operacionais:

• Ausência de políticas e procedimentos:

Foi identificada ausência de formalização apropriada de algumas políticas e procedimentos operacionais, entre elas: (i) Estoque obsoleto, (ii) Compras; (iii) Fechamento Contábil; (iv) Vendas (Faturamento), entre outras. Todas estão sendo devidamente revisadas e formalizadas.

• Ausência de formalização de estrutura de responsabilidade de preparação e revisão em relação às contas contábeis:

A melhor formalização e documentação das aprovações e revisões da conciliação de todas as contas contábeis demonstrará que as análises das contas contábeis foram realizadas com o objetivo de garantir a

5.2 Descrição dos controles internos

precisão do saldo contábil, além disto a definição do novo plano de contas único e automatização do controles em curso trará as evidências necessárias para atestar a conformidade do processo.

• Ausência de registros contábeis que geraram a reapresentação das DFs 2022:

Foi identificado que determinados ajustes computados no mapa de consolidação para fins de apresentação das Demonstrações Financeiras, até o encerramento dos trabalhos de auditoria ainda não haviam sido reconhecidos nos livros contábeis da Companhia. O ponto já foi tratado, uma vez que a área Contábil realizou o registro dos ajustes respectivos.

e) Comentários dos diretores sobre as deficiências no relatório circunstanciado do auditor independente e sobre as medidas corretivas adotadas

Embora os riscos relacionados as deficiências reportadas pela auditoria independente não representem distorções relevantes nas demonstrações financeiras do período, trabalhamos continuamente na identificação de melhorias e aprimoramento do nosso ambiente de controles internos, definindo papéis e responsabilidades, redesenhando processos, revisando controles existentes, implementando controles adicionais, estruturando sistemas e aperfeiçoando nossa gestão e ambiente de controle.

Por ocasião da presente Carta de Controles a Companhia alcançou relevante redução de deficiências significativas em comparação com exercício anterior e já possui planos de ação em curso para tratamento de todas as demais, visando atendimento das recomendações dos auditores externos.

5.3 Programa de integridade

5.3. - Programa de integridade

a. Se o emissor possui regras, políticas, procedimentos ou práticas voltadas para a prevenção, detecção e remediação de desvios, fraudes, irregularidades e atos ilícitos praticados contra a administração pública, identificando, em caso positivo:

i. Os principais mecanismos e procedimentos de integridade adotados e sua adequação ao perfil e riscos identificados pela companhia, informando com que frequência os riscos são reavaliados e as políticas, procedimentos e as práticas são adaptadas

A Companhia possui uma Política de Gerenciamento de Riscos, ampla e abrangente, revisada e aprovada em Reunião do Conselho de Administração, realizada em 9 de agosto de 2022, cujo objetivo é formalizar e estabelecer princípios, diretrizes e responsabilidades para controle e mitigação qualitativa e quantitativa dos riscos que afetam o desempenho e o crescimento da Companhia e suas subsidiárias ("Política de Gerenciamento de Riscos").

As atividades de gerenciamento de Riscos têm como princípio a adoção do Modelo das Três Linhas do IIA (Instituto dos Auditores Internos), 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.

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 Riscos e Controles Internos e de Auditoria Interna.

São considerados na Política de Gerenciamento de Riscos, dentre outras categorias, os impactos provenientes de desvios de conduta, fraudes, corrupção e outros aspectos relacionados a conformidade e integridade. A existência de fatores de risco associados a esses aspectos é observada durante todo o processo de Gerenciamento de Riscos, composto pelas seguintes etapas:

1) Identificação de riscos

Riscos dessa natureza podem ser identificados durante o mapeamento de processos do negócio, em projetos e novos negócios, sobretudo onde há envolvimento de terceiros ou de órgãos públicos ou, ainda, durante apurações internas conduzidas pela área de Investigações.

2) Avaliação dos riscos

Os eventos de riscos dessa natureza são avaliados de acordo com a metodologia aplicada na Companhia, onde são descritos todos os possíveis fatores que podem levar a sua ocorrência e os impactos caso se materializem, sendo atribuída uma pontuação de probabilidade e outra de impacto, que juntas configuram o nível de criticidade do risco (multiplicação da probabilidade pelos impactos).

Na composição do mapa de riscos da Companhia, esses riscos são distinguidos dos demais, recebendo um atributo de identificação específico para fins de composição de relatórios e reportes, e são reavaliados pelo menos uma vez a cada ano.

3) Tratamento e resposta aos riscos

De acordo com a metodologia adotada, os riscos avaliados são priorizados com base em sua criticidade. Com isso, são tomadas ações para mitigar ou eliminar esses riscos, de modo a evitar ou reduzir sua probabilidade de ocorrência e/ou seus eventuais impactos.

4) Comunicação

O Mapa de Riscos é revisado sempre que necessário e pelo menos uma vez ao ano é apresentado pela Diretoria de Riscos, Auditoria e Compliance 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. Eventuais riscos relacionados a conformidade e integridade são discutidos em conjunto a Comissão de Compliance, que irá supervisionar a implementação das medidas.

Além da Política de Gerenciamento de Riscos, a Companhia conta ainda com diversas políticas, regimentos e Código de Ética e Conduta, adaptados e atualizados em Agosto de 2022 e sempre que necessário,

5.3 Programa de integridade

passando por aprovação das Diretorias e estruturas competentes, bem como os Comitês e o Conselho de Administração, de modo a promover as boas práticas, como as frentes de ética, Compliance e sustentabilidade, relacionamento com stakeholders, conduta interna, situações práticas, canais de denúncia e sanções. Em conjunto, esses instrumentos proíbem qualquer forma de suborno, implementam preceitos de governança corporativa, incentivam a legalidade e a transparência de sua gestão e todos stakeholders, cumprem a Lei Anticorrupção, além de fornecer canais de denúncia e prever sanções ao seu descumprimento.

O Código de Ética e Conduta é aplicável a todos os associados e parceiros, apresenta valores e compromissos que devem ser seguidos por todas as partes interessadas, ao longo da nossa cadeia de valor.

A Política de *Compliance* tem como objetivo estabelecer as diretrizes e principais responsabilidades associadas à função de Compliance, observando as boas práticas de mercado e regulamentações aplicáveis, bem como disseminar a cultura e a prática de integridade por todos os níveis da Companhia, demonstrando a importância do conhecimento e cumprimento das determinações legais e procedimentais, tantos externas quanto internas.

A Política de Combate à Corrupção, estabelece e formaliza as diretrizes, regras e procedimentos para prevenir, identificar, monitorar, comunicar e combater quaisquer práticas de corrupção dentro da Companhia.

A Política de Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo estabelece definições, diretrizes e responsabilidades na prevenção e combate a tais atos ilícitos, bem como informa canal para denúncia de irregularidades ou condutas suspeitas e apresenta as regulamentações de referência.

A Política de Transações com Partes Relacionadas e Administração de Conflitos de Interesses estabelece as regras que devem ser observadas em todas as transações comerciais. Fornece orientações à conduta dos administradores da Companhia e de suas controladas, de forma a zelar para que todas as Transações com Partes Relacionadas, e outras situações que envolvam potenciais conflitos de interesses, sejam realizadas de acordo com os interesses da Companhia, em condições estritamente comutativas ou com pagamento compensatório adequado, e de forma transparente aos acionistas e ao mercado em geral.

A Política de Segurança da Informação estabelece os princípios, diretrizes e regulamentos a fim de garantir o tratamento seguro das informações, dos dados e comunicações da Companhia e as Políticas de Privacidade demonstram o compromisso com a transparência, a privacidade e a segurança dos dados dos titulares, em linha com as disposições da Lei Geral de Proteção de Dados (Lei 13.709/18).

Além dos instrumentos já citados existe o Regulamento de Interações com Agentes Públicos, que reforça os padrões éticos e de conduta que devem ser adotados nas interações com agentes públicos, bem como estabelece medidas de cautela, de registro e controle dessas interações.

A Companhia adota ainda diversas ações preventivas de disseminação do Programa de Integridade, tais como: a) disponibilização de conteúdos na plataforma de treinamentos corporativa – Americanas Educa; b) inclusão da temática de integridade no programa interno de formação de lideranças; c) ações de comunicação na plataforma de colaboração corporativa através do grupo “Ética na Prática”; d) realização do evento “Mês da Ética”, promovendo lives temáticas para disseminar a cultura de ética e integridade entre os associados; e) divulgação de relatório anual para acionistas e demais partes interessadas pela Companhia estabelecendo métricas e indicadores do Programa de Integridade; bem como f) ampla divulgação do Canal de Denúncias, pilar do Programa de Integridade.

O Canal de Denúncias é independente, especializado e terceirizado, o Disk Alerta, onde as denúncias podem ser feitas de maneira anônima, estando disponível 24 horas por dia, sete dias por semana, online no site https://canaldedenuncias.com.br/universoamericanas e, gratuitamente, pelo telefone 0800 282 2550. As denúncias reportadas são tratadas de forma confidencial e os envolvidos tem preservados os seus direitos à privacidade e à confidencialidade, sendo inaceitáveis quaisquer formas de coação ou represálias. As denúncias recebidas são apuradas pela área de Investigações e classificadas, ao término da apuração, como: procedente, improcedente ou inconclusiva. Dentre as sanções aplicadas às denúncias apuradas como procedentes, estão: medidas disciplinares, demissões, demissões por justa causa ou até mesmo processos criminais, dependendo da gravidade da violação.

ii. As estruturas organizacionais envolvidas no monitoramento do funcionamento e da eficiência dos mecanismos e procedimentos internos de integridade, indicando suas atribuições, se sua criação foi formalmente aprovada, órgãos da Companhia a que se reportam, e os mecanismos de garantia da independência de seus dirigentes, se existentes

A despeito do acima descrito, a Companhia, por meio de sua Diretoria, do Comitê de Auditoria e do Conselho de Administração, monitora a eficiência dos mecanismos e procedimentos internos de integridade. Com o intuito de viabilizar o fortalecimento de sua cultura ética, de riscos e de conformidade com a legislação e com

5.3 Programa de integridade

os valores da Companhia, a Companhia mantém um Programa de Integridade (conhecido internamente como Programa "Ética na Prática") voltado para todos os seus associados, parceiros e fornecedores, sejam eles de natureza permanente, temporária, excepcional ou eventual. O Programa é baseado em pilares que englobam processos e atividades conduzidas por diferentes áreas e possuem o intuito de prevenir, detectar e corrigir desvios à legislação, externa e interna, e à cultura ética. É, portanto, por meio da atuação conjunta desses pilares que a Companhia conduz os seus negócios com integridade e conformidade.

Além disso, como já dito, a Companhia adota o Modelo das Três Linhas e acredita que as diversas áreas têm responsabilidade em monitorar os seus próprios riscos como primeira linha, e mantém áreas de controle, de segunda linha, como as áreas de Controladoria, Riscos e Controles Internos, Compliance, Controle e Prevenção de Perdas, Jurídico e Segurança da Informação e as áreas de terceira linha, Auditoria Interna e Investigações, fortalecendo o funcionamento e a eficiência dos mecanismos.

As áreas de controle são subordinadas operacionalmente às Diretorias Estatutárias e não Estatutárias da Companhia e pelo menos uma vez por ano, os riscos prioritários e seus planos de mitigação são reportados e discutidos junto ao Conselho de Administração e ao Comitê de Auditoria. O Conselho de Administração possui comitês de assessoramento que acompanham a estratégia de negócio e propõem recomendações para a gestão da Companhia. Ao todo, temos quatro Comitês – Auditoria, Financeiro, Nomeação, Gente & Sustentabilidade - nomeados pelo Conselho de Administração – formados por conselheiros e por membros externos e independentes convidados, que se reúnem a cada fechamento de trimestre ou sempre que houver convocação pelo seu Presidente em uma necessidade extraordinária.

Em 2021, em mais um passo em linha com as boas práticas de governança, a Companhia criou a Diretoria de Riscos, Auditoria e Compliance, no intuito de assegurar uma estrutura integralmente dedicada ao monitoramento do funcionamento e da eficiência dos mecanismos e procedimentos internos de integridade, com canal direto ao Comitê de Auditoria da Companhia, garantindo independência na prevenção e detecção de fraudes e erros, com o objetivo de mitigar os riscos inerentes ao negócio que desenvolve.

Em abril de 2023, com vistas a aprimorar a gestão de riscos e controles, incluindo as circunstâncias que ocasionaram as inconsistências em lançamentos contábeis identificadas neste ano, a Companhia criou a Vice-Presidência Jurídico e Compliance, responsável pela área jurídica e pela integridade corporativa da companhia, com autonomia em relação às demais estruturas de gestão da Americanas, reportando-se administrativamente ao Diretor Presidente.

iii. Se a Companhia possui código de ética ou de conduta formalmente aprovado, indicando:

Na data deste Formulário de Referência, possuímos um Código de Ética e Conduta, formalmente revisado e aprovado em Reunião do Conselho de Administração da Companhia, realizada em 9 de agosto de 2022.

- **se ele se aplica a todos os diretores, conselheiros fiscais, conselheiros de administração e empregados e se abrange também terceiros, tais como fornecedores, prestadores de serviço, agentes intermediários e associados**

O Código de Ética e Conduta da Companhia se aplica a todos os diretores, conselheiros fiscais, conselheiros de administração e associados e abrange também terceiros, tais como fornecedores e parceiros e está publicado em nosso site de Relações com Investidores que pode ser acessado através do link https://ri.americanas.io/governanca-corporativa/estatuto-codigos-e-politicas/

- **se e com que frequência os diretores, conselheiros fiscais, conselheiros de administração e empregados são treinados em relação ao código de ética ou de conduta e às demais normas relacionadas ao tema**

Os diretores, conselheiros e associados recebem o treinamento em relação ao Código de Ética e Conduta no processo de ambientação que ocorre no ingresso à Companhia, pelo menos uma vez ao ano ou a cada revisão deste.

- **as sanções aplicáveis na hipótese de violação ao código ou a outras normas relativas ao assunto, identificando o documento onde essas sanções estão previstas**

São previstas aplicações de sanções para cada tema aplicável no Código de Ética e Conduta, a depender da natureza da violação. Dentre as sanções possíveis de aplicação, estão medidas disciplinares, demissões, demissões por justa causa ou até mesmo processos criminais, dependendo da gravidade da violação.

- **órgão que aprovou o código, data da aprovação e, caso a Companhia divulgue o código de conduta, locais na rede mundial de computadores onde o documento pode ser consultado**

5.3 Programa de integridade

O Código de Ética e Conduta foi revisado e aprovado pelo Conselho de Administração, em reunião realizada em 9 de agosto de 2022 e pode ser acessado por meio do link https://ri.americanas.io/governanca-corporativa/estatuto-codigos-e-politicas/

b. se o emissor possui canal de denúncia, indicando, em caso positivo:

i. se o canal de denúncias é interno ou se está a cargo de terceiros

A Companhia possui um canal para realização de denúncias, o Disk Alerta, independente, especializado e terceirizado, onde as denúncias podem ser feitas de maneira anônima por qualquer associado ou cidadão que se relacione conosco, estando disponível 24 horas por dia, sete dias por semana, online no site https://canaldedenuncias.com.br/universoamericanas e, gratuitamente, pelo telefone 0800 282 2550.

ii. se o canal está aberto para o recebimento de denúncias de terceiros ou se recebe denúncias somente de empregados

O Disk Alerta é aberto a todos os stakeholders e tem como objetivo assegurar que todos os associados, fornecedores, parceiros, clientes ou qualquer cidadão ao observarem quaisquer desvios às diretrizes do Código de Ética e Conduta, políticas e regimentos internos ou atitudes suspeitas, possam reportá-los.

iii. se há mecanismos de anonimato e de proteção a denunciantes de boa-fé

As situações reportadas serão tratadas de forma sigilosa, sendo possível optar pelo anonimato. Todos os envolvidos têm reservados os seus direitos à privacidade e confidencialidade, sendo inaceitáveis quaisquer formas de coação ou represálias.

iv. órgão da companhia responsável pela apuração de denúncias

O canal é corporativo, ou seja, compreende a Companhia e suas controladas, e é administrado por uma empresa independente, terceirizada e especializada. Todas as informações necessárias para a apuração das denúncias são direcionadas para área de Investigações da Companhia, altamente treinada, imparcial e independente.

c.número de casos confirmados nos últimos 3 (três) exercícios sociais de desvios, fraudes, irregularidades e atos ilícitos praticados contra a administração pública e medidas corretivas adotadas

Não houve nenhum registro de desvios, fraudes, irregularidades e/ou atos ilícitos contra a administração pública nos últimos 3 anos.**d. caso o emissor não possua regras, políticas, procedimentos ou práticas voltadas para a prevenção, detecção e remediação de desvios, fraudes, irregularidades e atos ilícitos praticados contra a administração pública, identificar as razões pelas quais o emissor não adotou controles nesse sentido**

A Companhia possui Código de Ética e Conduta, políticas e regimentos internos e práticas voltadas para a prevenção, detecção e remediação de fraudes, conforme previsto no item 5.3 a) deste Formulário de Referência.

5.4 Alterações significativas

5.4. - Alteração significativa

Não houveram alterações significativas na política de gerenciamento de riscos, que segue em revisão com previsão de nova versão no ano de 2024.

5.5 Outras informações relevantes

5.5. - Outras informações relevantes

A Companhia informa que segue conduzindo trabalhos para fins de revisão e fortalecimento da sua governança, de modo que esta Política de gerenciamento de riscos poderá sofrer alterações.