Índice

5.1 Descrição do gerenciamento de riscos e riscos de mercado

5. Política de gerenciamento de riscos e controles internos

5.1. Em relação aos riscos indicados nos itens 4.1 e 4.3, informar:

(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 Gestão de Riscos Corporativos, aprovada em 14 de janeiro de 2021 e revisada em 6 de dezembro de 2022 pelo Conselho de Administração da Companhia ("Política de Gestão de Riscos") e que pode ser consultada nos seguintes endereços:

- Site de Relações com Investidores da Companhia (https://ri.assai.com.br/), clicando em "Governança Corporativa", "Estatutos e Políticas" e, por fim, "Política de Gestão de Riscos Corporativos" ou diretamente por meio do link https://api.mziq.com/mzfilemanager/v2/d/ec14f0ab-c5d4-4b12-a413-b6cc7475ed98/5b310e2c-2f23-55c6-ab56-098e7886a34a?origin=1; e
- Site da Comissão de Valores Mobiliários ("CVM") (https://www.rad.cvm.gov.br/ENET/frmExibirArquivoIPEExterno.aspx?NumeroProtocoloEntrega=823026).

A Companhia possui, também, a Política de Aplicação, Captação e Câmbio, aprovada em 14 de janeiro de 2021 pelo Conselho de Administração da Companhia, que define as principais estratégias a serem adotadas para mitigar os riscos de mercado.

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

A Política de Gestão de Riscos tem o objetivo de estabelecer princípios, diretrizes do processo e responsabilidades da gestão de riscos da Companhia, bem como orientar os processos de identificação, avaliação, tratamento, monitoramento e comunicação dos riscos inerentes às atividades, incorporando a visão de riscos à tomada de decisões estratégicas e em conformidade com as melhores práticas de mercado, contribuindo com a proteção do valor da Companhia, apoiando o cumprimento dos objetivos do negócio, reduzindo de forma preventiva as incertezas e potencializando a identificação de oportunidades.

i. riscos para os quais se busca proteção

Nos termos da Política de Gestão de Riscos, os quatro principais riscos para os quais se busca proteção são:

a) Estratégicos: Riscos que afetam a estratégia ou os objetivos estratégicos da Companhia. Estão ligados a cenários de incertezas e/ou oportunidades e estão no foco prioritário da alta administração.

b) Operacionais: Riscos decorrentes da inadequação ou falha na gestão de processos internos, de pessoas ou tecnologias que possam dificultar ou impedir o alcance dos objetivos.

5.1 Descrição do gerenciamento de riscos e riscos de mercado

c) Externo: Riscos provenientes de eventos externos a Companhia e estão além da sua influência ou controle. Estão ligados a fatores externos como cenário econômico, crises sanitárias, ambiente regulatório, hábito do consumidor, entre outros.

d) Responsabilidade Social Corporativa: Riscos relacionados a qualquer questão de natureza ambiental, social e/ ou de governança, vinculada a reputação e/ ou à imagem da Companhia.

Os principais **riscos de mercado** aos quais a Companhia está exposta, elencados no item 4.3 deste Formulário de Referência, são:

Risco de taxa de juros

A Companhia e suas controladas obtêm empréstimos e financiamentos com as principais instituições financeiras para atender às necessidades de caixa para suportar os investimentos. Consequentemente, a Companhia e sua controlada estão expostas, principalmente, ao risco de flutuações relevantes na taxa de juros, especialmente a taxa relativa à parte passiva das operações com derivativos (*hedge* de exposição cambial) e às dívidas referenciadas em CDI. O saldo de caixa e equivalentes de caixa, indexado ao CDI, neutraliza parcialmente o risco de flutuações nas taxas de juros.

Risco de crédito

- Caixa e equivalentes de caixa

A fim de minimizar o risco de crédito são adotadas políticas de investimentos em instituições financeiras aprovadas pelo Comitê Financeiro e de Investimentos da Companhia, considerando-se os limites monetários as avaliações de instituições financeiras, as quais são constantemente atualizados.

- Contas a receber

O risco de crédito relativo às contas a receber é minimizado pelo fato de grande parte das vendas serem realizadas por meio de cartões de crédito onde as contrapartes são as principais adquirentes do mercado, ligadas a bancos de primeira linha. Parte desses recebíveis são antecipados junto a bancos e às administradoras de cartões de crédito, com o objetivo de prover o capital de giro e isso proporciona o desconhecimento das contas a receber em virtude da transferência do risco de crédito, benefícios e controle sobre tais ativos. Adicionalmente, principalmente para às contas a receber parceladas, a Companhia monitora o risco pela concessão de crédito e pela análise constante dos saldos de provisão para créditos de liquidação duvidosa.

Risco de liquidez

A Companhia gerencia o risco de liquidez através do acompanhamento diário do fluxo de caixa, controle dos vencimentos dos ativos e dos passivos financeiros. Para maiores informações, vide item 4.3 deste Formulário de Referência.

ii. instrumentos utilizados para proteção

5.1 Descrição do gerenciamento de riscos e riscos de mercado

O processo de gestão de riscos corporativos da Companhia, é conhecido como ERM (*Enterprise Risk Management*) e tem início em reunião anual de apresentação/atualização para o CEO e Diretores Executivos da Companhia. Contempla a captura e entendimento dos objetivos estratégicos de curto e longo prazo da Companhia e o ambiente em que esses objetivos são perseguidos.

Este "estabelecimento do contexto" é uma etapa fundamental para garantir que o processo de gestão de riscos esteja alinhado aos ciclos de gestão e de planejamento estratégico de curto e longo prazo da Companhia, identificando assim as suas capacidades e tolerâncias para maior amadurecimento dos conceitos de gestão de riscos.

A abordagem de identificação de riscos para o ERM na Companhia é *top-down*, partindo de entrevistas com os diretores e principais executivos de todas as áreas da Companhia, tendo em vista os principais processos pelos quais são responsáveis. O produto da identificação é uma lista abrangente de riscos baseada nos eventos que possam ameaçar a realização dos objetivos de cada unidade de negócio e consequentemente da Companhia. Nesta etapa também deve ser definido o dono e o ponto focal por cada um dos riscos identificados, assim como uma descrição que orientará as próximas etapas do mapeamento.

A análise de riscos é conduzida em seguida e consiste na definição das causas e níveis de probabilidade e impacto dos riscos, classificando os fatores agravantes desses riscos, para gerar uma lista de riscos abrangente e relevante para prosseguir com o mapeamento.

A fase de avaliação dos riscos e de seus potenciais de materialização é realizada com o suporte da alta administração, dos executivos e dos líderes de processos da Companhia. Os eventos são avaliados dentro das perspectivas de probabilidade ou frequência e impactos, buscando variáveis para combinar métodos de avaliação qualitativos e quantitativos. Combinando todas as variáveis de avaliação, é definida a criticidade dos riscos identificados, permitindo a construção de uma lista de riscos priorizados (da maior exposição para a menor exposição).

A fase de tratamento de riscos envolve a identificação, formalização e implementação de um ou mais planos de ação para mitigar os fatores de risco, que não possuem iniciativas de mitigação efetivas. Para cada ação, é imprescindível que seja definido um responsável e um cronograma de implementação. O objetivo é que, uma vez concluídos, os planos de ação gerem novas iniciativas de mitigação ou melhorem as existentes, consequentemente, reduzindo o nível de risco residual. As alternativas possíveis para tratamento dos riscos são:

(a) Reduzir ou mitigar a probabilidade e/ou o impacto de um risco até um nível aceitável, de acordo com o apetite a riscos da Companhia;

(b) Eliminar o fator de risco, eliminando o processo ou o projeto que o gera;

(c) Transferir ou compartilhar parte do risco com terceiros;

(d) Aceitá-lo.

5.1 Descrição do gerenciamento de riscos e riscos de mercado

O monitoramento dos riscos é feito através do acompanhamento dos planos de ação estabelecidos junto às áreas de negócio, mas principalmente através do acompanhamento dos indicadores de riscos (KRIs) e de performance (KPIs). O monitoramento do status dos planos de ação é realizado pelos donos dos riscos e o suporte da área Gestão de Riscos, de acordo com as responsabilidades definidas na Política de Gestão de Riscos com periodicidade que pode variar de mensal, bimestral, trimestral, semestral, chegando até a anual, dependendo das necessidades de gestão de risco de maneira a atender o fluxo de validações que resulta na apresentação para o CEO, para o Comitê de Auditoria e para o Conselho de Administração da Companhia. Os riscos priorizados das áreas de negócio são monitorados a partir dos status dos planos de ação, refletindo a comparação entre redução de risco planejada e a realizada.

Em conjunto com a área de comunicação interna, a disseminação da cultura de gestão de riscos é realizada continuamente através da divulgação da Política de Gestão de Riscos da Companhia, bem como de campanhas internas e treinamentos sobre Código de ética, *compliance* e boas práticas de gestão na Companhia, quando necessários.

Adicionalmente, a Companhia aplica sua metodologia baseada nos frameworks COSO e ISO 31000; através desta metodologia foram identificados os principais riscos de negócio e de ESG, considerando, fundamentalmente, a visão dos executivos da Companhia.

Em relação aos **riscos de mercado**, a estrutura de proteção da exposição cambial (*hedge*) adotada pela Companhia é a associação de um contrato de *swap* em que a posição dada (ponta ativa) é idêntica à remuneração do contrato de captação acrescida de custos acessórios, tais como IR e custos de estruturação, ou seja, indexada à variação cambial e a uma taxa anual de juros pré-fixada. A posição tomada, neste mesmo contrato, está indexada à variação de um percentual da Taxa DI.

Em todas as situações, a operação em moeda estrangeira somente poderá ser contratada se for possível realizar tal operação de *swap* em condições que a Companhia considerar favoráveis e observando o fluxo total da operação.

A estrutura de *hedge* busca neutralizar a variação da cotação da moeda estrangeira ao longo da operação. O instrumento financeiro derivativo, associado a esta estrutura, destina-se a compensar riscos decorrentes da exposição à variação no valor de mercado do item objeto da operação.

Os instrumentos utilizados para proteção patrimonial (hedge) da Companhia são os contratos de *swap* de taxas de juros e taxas de câmbio no mercado local.

iii. estrutura organizacional de gerenciamento de riscos

A estrutura de governança em riscos da Companhia e as suas respectivas responsabilidades são, dentre outras, como segue:

(a) Conselho de Administração da Companhia:

- Estabelecer as diretrizes gerais de riscos alinhadas ao contexto de negócio e do

5.1 Descrição do gerenciamento de riscos e riscos de mercado

ciclo de planejamento estratégico;

- Avaliar, deliberar e aprovar a matriz de riscos estratégicos e priorizados;
- Influenciar e patrocinar dentro dos fóruns de gestão o monitoramento dos riscos priorizados;
- Influenciar e patrocinar a cultura de Riscos dentro da Companhia;
- Avaliar, anualmente, a suficiência da estrutura e do orçamento da área de Gestão de Riscos e da Auditoria Interna para o desempenho das suas funções;
- Revisar e aprovar as definições gerais das estratégias de Gestão de Riscos; e
- Aprovar o orçamento destinado ao Comitê de Auditoria, visando assegurar sua autonomia operacional e a cobertura das despesas de seu funcionamento.

(b) Comitê de Auditoria:

- Acompanhar as atividades das áreas de Controles Internos, Gestão de Riscos e de Auditoria Interna e Externa da Companhia;
- Acompanhar as exposições de risco da Companhia;
- Avaliar a elegibilidade dos fóruns, definições e diretrizes para compor o modelo de Gestão de Riscos dentro da Companhia;
- Acompanhar os indicadores de riscos na aplicáveis ao contexto de negócio e as diretrizes do Conselho de Administração;
- Aferir a regular realização das atividades de Gestão de Riscos, seguindo o cumprimento das legislações legais, das políticas, normas e procedimentos internos da Companhia;
- Avaliar, monitorar e informar periodicamente o Conselho de Administração sobre os riscos priorizados identificados pelas revisões da área de Gestão de Riscos auxiliando na avaliação dos planos de ação e cumprimento das recomendações;
- Avaliar, aprovar e acompanhar a execução do tratamento e monitoramento dos riscos priorizados;
- Avaliar, aprovar e recomendar à administração a correção ou aprimoramento das políticas internas da Companhia; e

5.1 Descrição do gerenciamento de riscos e riscos de mercado

- Avaliar as informações trimestrais, demonstrações intermediárias e demonstrações financeiras da Companhia.

(c) Comitê de Governança Corporativa, Sustentabilidade e Indicação:

- Elaborar o planejamento e assegurar a operacionalização da Gestão de Riscos, considerando todas as dimensões da estrutura definida, englobando atividades estratégicas, táticas e operacionais da Companhia;

- Assessorar o Conselho de Administração na aplicação da metodologia de Gestão de Riscos na Companhia;

- Apoiar o Conselho de Administração na definição dos riscos priorizados da Companhia;

- Apoiar a Companhia na análise e aprovação da estratégia de Gestão de Risco;

- Assessorar o Comitê de Auditoria e o Conselho de Administração sobre os níveis de exposições dos Riscos;

- Avaliar a eficácia do processo de Gestão de Risco na Companhia; e

- Identificar os Riscos decorrentes das mudanças estratégicas e diretivas da Companhia sob decisão do Conselho de Administração.

(d) Presidência Executiva / COMEX / DirEx (Diretoria Executiva):

- Promover a integração e a cultura de Riscos na Companhia e nos ciclos de gestão e planejamento estratégico;

- Aprovar a Política de Gestão de Riscos e apoiar as iniciativas da área de Gestão de Riscos e Continuidade de Negócios, visando contribuir com a eficácia de sua atuação;

- Promover a implantação de um modelo eficiente de Gestão de Riscos, alinhado aos objetivos de negócios e metas de negócio. Aplicar as diretrizes gerais estabelecidas pelo Conselho de Administração;

- Acompanhar os riscos gerenciados no nível de cada processo e operações para garantir a efetividade das medidas de controle;

- Participar dos rituais da identificação, de validações e priorização dos Riscos da Companhia;

- Acompanhar os KRIs, KPIs e as estratégias de mitigação dos riscos priorizados;

5.1 Descrição do gerenciamento de riscos e riscos de mercado

- Avaliar e monitorar o tratamento dos riscos de negócio alinhados à execução do planejamento estratégico;

- Avaliar, tempestivamente, a eficácia a aplicabilidade das diretrizes da Política de Gestão de Riscos;

- Avaliar e apoiar as adequações da estrutura destinada ao processo de gerenciamento, considerando recursos humanos, financeiros e tecnológicos;

- São responsáveis pela pertinente gestão de risco da Companhia, devendo envidar todos os esforços necessários para mitigar os riscos considerados com impacto significativo no cumprimento dos objetivos do negócio; e

- Assumir e autorizar riscos que estejam acima do nível de aceitação que justifiquem iniciativas estratégicas e decisões corporativas.

(e) Área de Gestão de Riscos:

- Estabelecer a Política de Gestão de Riscos e os Procedimentos de gerenciamento de riscos;

- Fomentar a adoção de boas práticas de gerenciamento de riscos, considerando a necessidade do negócio da Companhia;

- Promover treinamentos e campanhas de conscientização sobre Gestão de Riscos;

- Definir, estabelecer e aprimorar a metodologia de Gestão de Riscos alinhada à cadeia de valor e integrada dentro da estratégia, da tática e da operação da Companhia;

- Gerir o ciclo do processo de Gestão de Riscos na Companhia, em conjunto com as áreas e respectivas atividades de negócio da Companhia;

- Conduzir a gestão do fluxo de informações dentro de todas as áreas e atividades de negócio, alinhada aos conceitos, a metodologia e aos prazos estabelecidos a cada ciclo de Gestão de Riscos;

- Apoiar a todas áreas e atividades de negócio no ciclo de identificação, avaliação, tratamento e monitoramento dos riscos para auxiliá-los na redução dos níveis de exposição dos Riscos;

- Gerir a Matriz de Riscos, comunicando dentro dos principais fóruns de gestão seus status e níveis de exposições;

- Auxiliar as áreas de negócio na identificação e avaliação do impacto dos Riscos;

5.1 Descrição do gerenciamento de riscos e riscos de mercado

- Reportar/Informar o status dos riscos mais significativos ao Comitê de Auditoria do Assaí, tempestivamente;

- Analisar riscos potenciais a partir de vulnerabilidades informadas pelas áreas de negócio, auditoria, segurança, controles internos ou compliance;

- Notificar os donos de riscos sempre que exista uma variação significativa dos riscos sob sua responsabilidade; e

- Assessorar a Alta Administração no processo de aprovação de riscos acima do nível de aceitação estabelecido.

(f) Área de Compliance:

Implementar um Programa de Integridade abrangente:

- Criar políticas e procedimentos: para prevenir, detectar e remediar violações de leis, regulamentos e normas internas.
- Realizar treinamentos periódicos para os colaboradores: sobre ética, compliance e leis anticorrupção.
- Criar uma cultura de ética e compliance na empresa: onde os colaboradores se sintam à vontade para reportar violações sem medo de retaliação.
- Supervisionar o canal de denúncias: para contribuir que os colaboradores possam reportar violações de forma anônima e equânime.
- Realizar monitoramento dos processos regularmente: para verificar o cumprimento das políticas, procedimentos e mitigação de riscos de compliance.

Monitorar o cumprimento das leis e regulamentos:

- Manter-se atualizado sobre as leis e regulamentos aplicáveis: à empresa, incluindo leis anticorrupção, leis de proteção ambiental, leis trabalhistas e leis de defesa do consumidor.
- Monitorar o ambiente regulatório: para identificar mudanças nas leis e regulamentos que podem afetar a empresa nos temas relacionados a Compliance
- Efetuar testes e controles dos processos: para verificar o cumprimento das leis e regulamentos relacionados bem como materialização dos riscos
- Implementar e acompanhar medidas corretivas em caso de violações de leis e regulamentos.

Gerenciar os riscos de compliance:

- Identificar e avaliar os riscos de compliance que a empresa enfrenta.
- Implementar medidas de controle para mitigar esses riscos como políticas e procedimentos de compliance, treinamentos para colaboradores e canais de denúncias.
- Monitorar os riscos de compliance para garantir que as medidas de controle sejam eficazes.

5.1 Descrição do gerenciamento de riscos e riscos de mercado

- Comunicar os riscos de compliance à alta administração para que a empresa possa tomar decisões informadas sobre como gerenciar esses riscos.

Investigar e remediar violações de compliance:

- Realizar investigações rigorosas: de todas as violações de compliance.
- Apoiar na aplicação de medidas disciplinares cabíveis: em caso de violações de compliance.
- Implementar medidas corretivas: para evitar que violações de compliance se repitam.
- Comunicar as violações de compliance à alta administração: para que a empresa possa tomar as medidas cabíveis.

Promover a ética e a transparência na empresa:

- Responsável pelo Código de Ética e Disseminação de cultura de integridade e valores da empresa.
- Promover a cultura de compliance através de treinamentos, campanhas de conscientização e canais de comunicação.
- Incentivar o diálogo e a participação dos colaboradores na construção de um ambiente de negócios ético.
- Prestar contas aos stakeholders sobre o desempenho da empresa em relação ao compliance e à integridade corporativa.

(g) Área de Controles Internos:

- Revisão dos controles da matriz SOx junto as áreas de negócio;

- Realização dos testes de SOx;

- Apoiar as áreas na implementação dos planos de ação e na remediação de pontos identificados antes e após as fases do processo de auditoria SOx;

- Atender a Auditoria Externa;

- Auxiliar na elaboração de políticas, processos, normas, e manuais de procedimentos;

- Mapear e avaliar aderência às Políticas, Normas e Procedimentos e adequar os processos para as melhores práticas de mercado;

- Acompanhar e controlar o follow-up dos principais aspectos reportados (auditoria externa, auditoria interna, controles internos e gestão de riscos);

5.1 Descrição do gerenciamento de riscos e riscos de mercado

- Apoiar a Gestão de Riscos e Continuidade de Negócios quanto ao mapeamento de riscos relacionados a não aderência dos requisitos da SOx; e

- Dar suporte às demais áreas para melhorar o ambiente de controles internos dos processos.

(h) Área de Segurança da Informação:

- Identificar vulnerabilidades e riscos de segurança da informação e comunicar as áreas responsáveis para que tomem as devidas tratativas;

- Manter comunicação efetiva com o time de Gestão de Riscos sobre possíveis vulnerabilidades, ameaças, falhas, anomalias, violações e novos controles de segurança;

- Monitorar os acessos às informações e aos ativos de tecnologia (sistemas, bancos de dados, recursos de rede), tendo como referência a Política e as Normas de Segurança da Informação;

- Implantar e manter funcionais os controles e padrões de segurança definidos para os ativos de tecnologia;

- Definir controles para tratamento de riscos, vulnerabilidades, ameaças e não conformidades identificadas pelos processos de Segurança da Informação;

- Propor as metodologias e processos referentes à segurança da informação, como classificação da informação, avaliação de risco e análise de vulnerabilidades;

- Classificar e reclassificar o nível de acesso às informações sempre que necessário;

- Estabelecer e manter a Política de Segurança da Informação;

- Estabelecer, controlar, implementar, divulgar, e manter atualizados a Política de Segurança da Informação, demais políticas, normas e padrões de Segurança da Informação aplicáveis;

- Desenvolver e estabelecer, com o envolvimento da área de Comunicação Interna, programas de conscientização e treinamentos de Segurança da Informação;

- Realizar trabalhos de análise de vulnerabilidades, com intuito de assegurar o nível de segurança dos sistemas de informações e dos demais ambientes em que armazenam, processam ou transmitem as informações de interesse da empresa;

- Tratar os riscos e vulnerabilidades identificados em ativos, sistemas ou processos sob responsabilidade da área de Segurança da Informação;

5.1 Descrição do gerenciamento de riscos e riscos de mercado

- Conduzir a gestão de incidentes de segurança da informação, incluindo as investigações para determinação de causas e responsáveis e a comunicação dos fatos ocorridos;

- Propor ações corretivas para os incidentes de segurança da informação;

- Solicitar informações às demais áreas da empresa e realizar testes e avaliações de segurança, no intuito de verificar o cumprimento e aderência da Política de Segurança da Informação, sempre que necessário;

- Realizar a avaliação dos projetos das áreas de negócio e do TI do Assaí realizando os apontamentos de segurança necessários para implantação/contratação do Software/Serviço/Solução;

- Propor projetos e iniciativas para melhoria do nível de segurança das informações do Assai; e

- Propor investimentos relacionados à segurança da informação com o intuito de minimizar os riscos.

(i) Dono do risco/ responsável: É o principal responsável pela gestão do risco e responde pelo status do mesmo. Estão sob sua responsabilidade as seguintes funções:

- Identificar, classificar e gerenciar os Riscos das respectivas áreas de acordo com as estratégias de mitigação, em conjunto com a área de Gestão de Riscos;

- Indicar o profissional que responderá como ponto focal da área na gestão do Risco junto à área de Gestão de Risco;

- Assegurar a implementação dos planos de ação e acompanhamento dos KRIs e KPIs;

- Prestar contas dos níveis de exposição, dos planos de ações e dos indicadores que descrevem o status do risco residual para os fóruns de governança e gestão; e

- Notificar a Gestão de Riscos sobre riscos, eventos similares, ou mudanças no atual contexto de riscos que tenham sido identificados na rotina de trabalho.

(j) Ponto focal da área: É o detentor do conhecimento técnico a respeito do risco e o principal responsável pela atualização das informações do mapeamento e tratamento dos riscos. Estão sob sua responsabilidade as seguintes funções:

- Deter o conhecimento técnico dos processos no qual os Riscos estão inseridos;

- Ser o responsável pela atualização das informações do mapeamento e tratamento

5.1 Descrição do gerenciamento de riscos e riscos de mercado

dos Riscos da sua área / unidade do negócio (lojas, CDs, regionais, áreas da sede);

- Manter as informações atualizadas tempestivamente, respeitando o calendário de planejamento do ciclo de Gestão de Riscos;

- Monitorar o status dos planos de ação junto aos responsáveis pela implementação dos dispositivos de controles; e

- Notificar a Gestão de Riscos sobre riscos ou eventos similares que tenham sido identificados na rotina de trabalho.

(k) Área de Auditoria Interna:

- Aferir a qualidade e a efetividade dos processos de gerenciamento de riscos, controle e governança da Companhia;

- Identificar e apontar oportunidades de melhorias nos processos de Controle Internos e de Gestão de Risco;

- Auditar as informações e controles relacionados aos KRIs e KPIs desenvolvidos e monitorados pelas áreas funcionais; e

- Reportar periodicamente ao COAUD, órgão ao qual a área de auditoria interna se vincula funcionalmente, e aos seus clientes auditados os resultados de avaliações independentes, imparciais e tempestivas sobre a efetividade da Gestão de Riscos na Companhia.

(l) Colaboradores:

- Assegurar a operacionalização da Gestão de Riscos, fazendo parte do processo de identificação, avaliação e mensuração, implementando ações preventivas e corretivas;

- Elaborar e cumprir planos de ação destinados a tratar adequadamente os riscos sob sua responsabilidade; e

- Notificar a Gestão de Riscos sobre riscos ou eventos similares que tenham sido identificados na rotina de trabalho.

Ademais, a Companhia poderá contratar Auditoria Externa, a qual tem por missão profissional avaliar a qualidade dos controles internos voltados para o preparo de demonstrações financeiras da Companhia, reportando à Companhia as fragilidades em tais controles, se encontrarem.

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

5.1 Descrição do gerenciamento de riscos e riscos de mercado

A área de Controles Internos e a área de Gestão de Riscos da Companhia revisam periodicamente os processos da Companhia, avaliando os riscos inerentes a estes processos, e mantêm uma matriz de riscos e controles com as devidas validações por partes das gestões das áreas de negócio e da Administração, a qual é submetida, anualmente, para avaliação de procedimentos de auditoria interna e externa, além de trabalhar em cooperação com a auditoria interna da Companhia nos assuntos internos. Para maiores detalhes sobre o histórico da estrutura da área de Controles Internos, vide item 5.2 deste Formulário de Referência.

O Conselho de Administração deverá, anualmente, avaliar a suficiência da estrutura e orçamento das áreas de Gestão de Riscos e da Auditoria Interna para o desempenho de suas funções. Tendo em vista que a áreas de Gestão de Riscos e da Auditoria Interna próprias foram recentemente constituídas, tais avaliações serão feitas oportunamente pelo Comitê de Auditoria da Companhia e, posteriormente, pelo Conselho de Administração.

A Administração da Companhia acredita que, atualmente, a estrutura, metodologia e procedimentos de controles internos adotados são adequados para verificar a efetividade tanto da Política de Gestão de Riscos da Companhia quanto da Política de Aplicação, Captação e Câmbio aplicada para a Companhia.

5.2 Descrição dos controles internos

5.2. Em relação aos controles adotados pelo emissor para assegurar a elaboração de demonstrações financeiras confiáveis, indicar:

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

A Companhia, com o objetivo de manter o adequado monitoramento do ambiente de controles internos atrelados aos processos operacionais e financeiros mantém as principais práticas de controles internos a seguir apresentadas.

A Companhia, atualmente, possui diversas práticas de controles internos, como a condução de treinamentos para colaboradores acerca das principais normas de *Compliance* da Companhia, o desenvolvimento de planos de ação junto às áreas de negócios da Companhia para mitigar potenciais riscos reputacionais e perdas financeiras relevantes futuras, a avaliação periódica dos principais riscos relacionados ao ambiente tecnológico e aos processos operacionais da Companhia, dentre outros, sendo que cada uma dessas práticas está sob responsabilidade primária de uma das áreas de controle da Companhia, conforme descritas no item 5.2(b) abaixo.

A Administração da Companhia acredita que os procedimentos e controles internos adotados são adequados e suficientes para assegurar a qualidade, precisão e confiabilidade das demonstrações financeiras da Companhia. Por essa razão, as demonstrações financeiras da Companhia apresentam adequadamente o resultado de suas operações e sua situação patrimonial e financeira nas respectivas datas.

(b) as estruturas organizacionais envolvidas

(a) Área de Gestão de Riscos da Companhia, a qual é responsável pela identificação, avaliação e monitoramento dos riscos corporativos junto aos administradores e diretores;

(b) Área de *Compliance* é dedicada à estruturação, gestão e aprimoramento constante do Programa de Integridade através de atividades e controles que visam prevenir, detectar e corrigir potenciais situações que possam contribuir para a ocorrência de riscos relacionados à Compliance. A atuação da área de Compliance via Programa de Integridade é bem ampla, podendo atingir qualquer área da Companhia onde um risco relacionado possa ocorrer;

(c) Área de segurança da informação que cria políticas e monitora a proteção do ambiente tecnológico;

(d) Área de prevenção de perdas responsável pelo monitoramento e controle de estoque;

(e) Área de controles internos responsável pela inclusão e guarda dos controles, além da avaliação dos riscos dos processos operacionais, financeiros, tecnológicos; e

(f) Auditoria interna da Companhia que é responsável por aferir a qualidade e a efetividade dos processos de gerenciamento de riscos, controle e governança.

A área de Controles Internos, que se reporta à Diretoria Administrativa Financeira, é responsável por coordenar e monitorar os testes nos controles internos visando atendimento aos requisitos da Lei Sarbanes–Oxley (“SOx”).

5.2 Descrição dos controles internos

A Companhia adota a estrutura conceitual do *Committee of Sponsoring Organizations of the Treadway Commission* – Coso, emitido em 2013, para desempenhar e testar os controles para fins de Sox.

Vale ressaltar, ainda, que cabe ao Comitê de Auditoria acompanhar as atividades de Gestão de Riscos, da Auditoria Interna e da área de controles internos e *compliance* da Companhia.

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

A área de Auditoria Interna da Companhia, que se reporta ao Comitê de Auditoria, atua de forma independente e objetiva para aferir a qualidade e a efetividade dos processos de gerenciamento de riscos, controle e governança da Companhia. O plano atual da auditoria é revisado e validado pela Presidência e Comitê de Auditoria da Companhia, tendo o seu cumprimento supervisionado pelo Comitê de Auditoria e reportado ao Conselho de Administração.

A Área de Gestão de Riscos da Companhia avalia periodicamente os riscos inerentes aos processos e mantém uma matriz de riscos e controles com as devidas validações por parte dos donos dos processos e da Administração, a qual é submetida, anualmente, para avaliação de procedimentos de auditoria interna.

A Administração da Companhia contrata ainda uma firma Independente para efetuar os testes de controles para fins de SOx sob supervisão da administração, de forma a suportar sua conclusão sobre os controles internos.

(d) deficiências e recomendações sobre os controles internos presentes no relatório circunstanciado, preparado e encaminhado ao emissor pelo auditor independente, nos termos da regulamentação emitida pela CVM que trata do registro e do exercício da atividade de auditoria independente

De acordo com o relatório de deficiências (relatório circunstanciado) preparado e encaminhado pelos auditores independentes da Companhia, relativo às demonstrações financeiras do exercício social encerrado em 31 de dezembro de 2023, foi identificada deficiência significativa sobre os controles internos da Companhia relativas a:

Revisão e aprovação de lançamentos manuais

A Companhia desenhou e implementou o controle AT-153 com o objetivo de assegurar que todos os lançamentos manuais originados por certas transações existentes no sistema SAP passem por processo de revisão e aprovação antes que sejam registrados no razão contábil. Entretanto, a Companhia constatou que o controle foi desenhado para capturar somente lançamentos manuais originados na transação FBV0, não capturando, portanto, lançamentos manuais originados em outras transações padronizadas e/ou customizadas do sistema SAP que permitem a criação de lançamentos manuais.

Adicionalmente, ao realizarem os testes de implementação do controle, os auditores independentes constataram que o revisor dos lançamentos manuais não demonstrou conhecimento suficiente para suportar a revisão do lançamento registrado e concluíram que a deficiência estaria relacionada à ausência de conhecimento detalhado dos assuntos respectivos.

5.2 Descrição dos controles internos

comentários dos diretores sobre as deficiências apontadas no relatório circunstanciado preparado pelo auditor independente e sobre as medidas corretivas adotadas

Em relação à deficiência apontada no item “d” acima, a Administração entende que:

Revisão e aprovação de lançamentos manuais:

A Administração fez aprimoramentos importantes no escopo do controle AT153, implementando em dezembro de 2023 políticas de alçadas para aprovação de lançamentos manuais, reforçando a importância de o aprovador possuir o conhecimento suficiente e toda a documentação suporte necessária quando realizasse a aprovação sistêmica do lançamento.

Adicionalmente, a Administração implementou mudanças nos controles existentes em 2022 e implementação de novos controles, assegurando: i) confirmação de que os limites de alçada definidos foram seguidos; ii) aprimoramento dos controles manuais sobre a totalidade dos lançamentos manuais; e iii) controles qualitativos de observância dos requerimentos de suporte do lançamento manual.

Para o ano de 2024 a Companhia está trabalhando em uma melhoria sistêmica para que a aprovação das alçadas esteja no sistema SAP.

5.3 Programa de integridade

5.3. Em relação aos mecanismos e procedimentos internos de integridade adotados pelo emissor para prevenir, detectar e sanar desvios, fraudes, irregularidades e atos ilícitos praticados contra a administração pública, nacional ou estrangeira, informar:

(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 pelo emissor, informando com que frequência os riscos são reavaliados e as políticas, procedimentos e as práticas são adaptadas

A Companhia implantou o seu Programa de Integridade, o qual foi estruturado nos termos da Lei nº 12.846/13, Decreto nº 11.129/22, Portarias da Controladoria Geral da União, do *Foreign Corrupt Practices Act* (FCPA), que conta com supervisão periódica pelo Conselho de Administração da Companhia, via Comitê de Auditoria e pela Diretoria Executiva através do Comite de Ética.

Dentre os principais mecanismos e procedimentos adotados pela Companhia, destacam-se:

a. Código de Ética, com as principais diretrizes, relacionadas à condução dos negócios e relacionamento com Poder Público, parceiros comerciais e os colaboradores;

b. Adoção de diversas políticas e procedimentos, com destaque para: Anticorrupção https://api.mziq.com/mzfilemanager/v2/d/ec14f0ab-c5d4-4b12-a413-b6cc7475ed98/8bbbe10c-c4bb-04e8-85df-597380181723?origin=1;Conflito de Interesses; Doações, Contribuições e Patrocínios; Acionamento e Apuração da Ouvidoria; Consequências e Medidas Disciplinares https://api.mziq.com/mzfilemanager/v2/d/ec14f0ab-c5d4-4b12-a413-b6cc7475ed98/eb49eb6c-280d-e3db-e904-14c53a6c6c81?origin=1;Brindes, Presentes, Viagens e Entretenimento; Gestão do Comitê de Ética; Relacionamento e Acordos com o Poder Público; e Atendimento a Fiscalização;

c. Comitê de Ética, composto pelo Diretor Presidente, Diretora Administrativo Financeira, Diretora de Gestão de Gente e Ouvidoria, Diretor de Auditoria, Riscos e Investigações, Diretor Jurídico e Gerente de Compliance, é a instância responsável por deliberar sobre questões que atentem contra o Código de Ética da Companhia bem como determinar a pronta interrupção e aplicar medidas corretivas sobre atividades nas quais for identificado que os riscos envolvidos não são aceitáveis. Além dos membros descritos anteriormente, VP Operações, VP Comercial, Gerente de Ouvidoria e Secretária do Comitê são convidados permanentes e participam de todas as reuniões;

d. Área de Compliance, dedicada à estruturação, gestão e aprimoramento constante do Programa de Integridade através de atividades e controles que visam prevenir, detectar e corrigir potenciais situações que possam contribuir para a ocorrência de riscos relacionados à Compliance;

e. Treinamentos periódicos acerca do Código de Ética, Direitos Humanos, Compliance, Lei Anticorrupção e outras regulamentações correlatas, políticas e procedimentos internos, realizados presencialmente e via *e-learning*, divididos por tema e abrangência, conforme o público-alvo;

5.3 Programa de integridade

f. Canal de Ouvidoria, responsável por esclarecimento de dúvidas, recebimento de reclamações e/ou denúncias internas e externas, assim como pela gestão do processo de apuração e tratativas de consequência;

g. Avaliação de risco periódica sobre fornecedores de acordo com o seu grau de risco e das atividades econômicas, com foco no histórico ético, reputacional e cultura de integridade;

h. Mapeamento e acompanhamento de atividades em que exista relacionamento com agentes públicos, bem como pessoas politicamente expostas a fim de mitigar riscos de corrupção, conflitos de interesse e problemas ligados a integridade e improbidade administrativa;

i. Avaliação e supervisão sobre doações e patrocínios para mitigar os riscos relacionados à marca, imagem e reputação;

j. Acompanhamento das atividades das áreas ligadas às linhas de defesa da Companhia, tais como Auditoria Interna, Controles Internos a fim de monitorar e mitigar riscos decorrentes de ausência de controles, falhas de controle interno, impacto em demonstrações financeiras, fraudes dentre outros problemas nos diversos processos da companhia; e

k. Monitoramento contínuo do Programa de Integridade visando seu aperfeiçoamento na prevenção, detecção e no combate de atos lesivos previstos nas legislações anticorrupção Brasileira e FCPA (EUA).

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 do emissor a que se reportam, e os mecanismos de garantia da independência de seus dirigentes, se existentes

As seguintes áreas são envolvidas diretamente na supervisão, monitoramento e funcionamento do Programa de Integridade, tendo suas atribuições definidas por políticas internas:

a. Conselho de Administração, via Comitê de Auditoria: é responsável pela supervisão do Programa de Integridade;

b. Comitê de Ética: tem como principal atribuição zelar pelo cumprimento das diretrizes estabelecidas no Código de Ética da Companhia, incluindo análises de suspeita de corrupção, fraude ou outras violações ao Código de Ética ou Política Anticorrupção por parte de colaboradores, fornecedores, prestadores de serviço e agentes intermediários, para definição dos procedimentos a serem adotados. Em sua atuação o Comitê de Ética pode contar com a contribuição eventual da Ouvidoria e dos departamentos de recursos humanos, compliance e qualquer outra área que seja pertinente;

c. Área de Compliance, dedicada à estruturação, gestão e aprimoramento constante do Programa de Integridade através de atividades e controles que visam prevenir, detectar e corrigir potenciais situações que possam contribuir para a ocorrência de riscos relacionados à Compliance. A atuação

5.3 Programa de integridade

da área de Compliance via Programa de Integridade é bem ampla, podendo atingir qualquer área da Companhia onde um risco relacionado possa ocorrer;

d. Ouvidoria: área responsável por receber e dar tratativa às denúncias envolvendo violações ao Código de Ética, políticas e procedimentos internos, bem como violações à legislação vigente por colaboradores, fornecedores e clientes, ou qualquer parte interessada, independentemente do cargo ou situação de quem tenha praticado a violação e envio para apuração de áreas específicas. A Ouvidoria também acompanha a conclusão das apurações e planos de ação gerados para mitigar os riscos, medidas corretivas e disciplinares e reportará, periodicamente, os seus indicadores ao Comitê de Ética e ao Comitê de Auditoria;

e. Áreas Apuradoras: possuem a atribuição de apurar a procedência das ocorrências reportadas à Ouvidoria; e

f. Auditoria Interna: realiza a auditoria do Programa de Integridade, apontando necessidade de melhorias nos processos, políticas e procedimentos. Reporte ao Comitê de Auditoria.

iii. se o emissor possui código de ética ou de conduta formalmente aprovado, indicando:

a. 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 da Companhia se aplica a administradores e colaboradores da Companhia, bem como a parceiros comerciais, tais como fornecedores, prestadores de serviço e agentes intermediários.

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

A Política de Consequências e Medidas Disciplinares da Companhia estabelece as sanções aplicáveis no caso de violação ao Código de Ética, políticas e procedimentos internos. Essas sanções consistem em medidas disciplinares educativas (advertência e suspensão) ou punitivas de rompimento contratual, e desligamento dos colaboradores envolvidos, sem ou por justa causa.

c. órgão que aprovou o código, data da aprovação e, caso o emissor divulgue o código de conduta, locais na rede mundial de computadores onde o documento pode ser consultado

O Código de Ética foi aprovado pelo Conselho de Administração da Companhia em 14 de janeiro de 2021 com posterior revalidação de seu conteúdo em 31 de maio de 2022. O Código de Ética e a Política de Consequências e Medidas Disciplinares da Companhia podem ser consultados nos seguintes endereços:

5.3 Programa de integridade

- Site de Relações com Investidores da Companhia (https://ri.assai.com.br/), clicando em "Governança Corporativa", "Estatutos e Políticas" e, por fim, "Código de Ética Assaí" ou diretamente por meio do link https://api.mziq.com/mzfilemanager/v2/d/ec14f0ab-c5d4-4b12-a413-b6cc7475ed98/0035ec06-01b9-f0b4-2f5d-fa11b0f2816f?origin=1;
- Site de Relações com Investidores da Companhia (https://ri.assai.com.br/), clicando em "Governança Corporativa", "Estatutos e Políticas" e, por fim, "Política de Consequências e Medidas Disciplinares" ou diretamente por meio do link https://api.mziq.com/mzfilemanager/v2/d/ec14f0ab-c5d4-4b12-a413-b6cc7475ed98/eb49eb6c-280d-e3db-e904-14c53a6c6c81?origin=1; e
- Site da Comissão de Valores Mobiliários ("CVM") (Site da Comissão de Valores Mobiliários ("CVM") (https://www.rad.cvm.gov.br/ENET/frmExibirArquivoIPEExterno.aspx?NumeroProtocoloEntrega=823166).

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

- **se o canal de denúncias é interno ou se está a cargo de terceiros**
- **se o canal está aberto para o recebimento de denúncias de terceiros ou se recebe denúncias somente de empregados**
- **se há mecanismos de anonimato e de proteção a denunciantes de boa-fé**
- **órgão do emissor responsável pela apuração de denúncias**

A Companhia possui canal de denúncias interno, contando também com linha confidencial para recebimento de denúncias operacionalizada por terceiros, sendo que ambos os canais estão sob a responsabilidade da Ouvidoria e eventuais reportes são realizados ao Comitê de Ética. O canal está apto a receber denúncias internas e externas, de forma anônima, de colaboradores, de clientes, parceiros comerciais e ou qualquer outro público de relacionamento da Companhia.

Prestador de serviço terceiro é responsável pelo recebimento das ocorrências, e o time interno dedicado a ouvidoria é responsável pela análise e distribuição para as Áreas apuradoras, de ocorrências relacionadas à Ética, conforme o tema e políticas impactadas.

O Código de Ética da Companhia, legislações vigentes aplicadas no país e políticas internas relacionadas ao Programa de *Compliance* ou demais áreas estabelecem as premissas para recebimento de denúncias, que podem ser feitas de forma anônima, de modo a garantir a imparcialidade e equidade na apuração e aplicações de sanções, assim como impedir qualquer tipo de retaliação aos denunciantes.

e. 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

5.3 Programa de integridade

Não há casos confirmados de desvios, fraudes ou atos ilícitos praticados contra a administração pública no período entre 2021 e 2023

f. 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.

Não aplicável, conforme respostas acima.

5.4 Alterações significativas

5.4. Informar se, em relação ao último exercício social, houve alterações significativas nos principais riscos a que o emissor está exposto ou na política de gerenciamento de riscos adotada, comentando, ainda, eventuais expectativas de redução ou aumento na exposição do emissor a tais riscos

Não houve, no exercício social encerrado em 31 de dezembro de 2023, alterações significativas nos principais riscos aos quais a Companhia está sujeita.

5.5 Outras informações relevantes

5.5. Fornecer outras informações que o emissor julgue relevantes

Na data deste Formulário de Referência, na busca pela segurança e boas práticas no manuseio de dados pessoais para adequação às disposições da LGPD, a Companhia já havia realizado o mapeamento de seus fluxos de dados pessoais, inserido práticas de Governança como elaboração de relatórios de impacto, e capacitado mais de 60 mil colaboradores(as) para que sigam as melhores orientações em privacidade e proteção de dados pessoais. Adicionalmente, foram elaborados os documentos obrigatórios e de boas práticas de acordo com a LGPD, incluindo, mas não se limitando, a Políticas de Privacidade interna e externa, Política de Gestão de Incidentes de Segurança com Dados Pessoais, Política de Segurança da Informação, Política de Gestão de Vulnerabilidades e Política de Utilização de Credenciais de Acesso e Senhas.

Também foi realizada a revisão de contratos de produtos e/ou serviços, bem como os contratos com colaboradores, para adequação de acordo com as exigências da LGPD. Além disso, a Companhia, ressaltando a preocupação da Companhia com sua segurança cibernética, contratou seguro contra incidentes desta natureza, bem como realiza periodicamente testes de intrusão para identificação de vulnerabilidades.

Por fim, para atender não só requisitos da LGPD, como também do Marco Civil da Internet, contratou ferramenta para gestão e registro dos *cookies* dos seus *websites*.