LOJAS AMERICANAS S.A.

POLÍTICA DE GERENCIAMENTO DE RISCOS

1. Objetivo

1.1. Esta Política de Gerenciamento de Riscos ("Política") tem por objetivo estabelecer princípios, diretrizes e responsabilidades a serem observados no processo de gerenciamento de riscos inerentes às atividades de negócio da Lojas Americanas S.A. ("Companhia"), de forma a identificar e monitorar os riscos relacionados à Companhia ou seu setor de atuação.

2. Abrangência

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

3. Conceitos

3.1. Para fins de aplicação desta Política, os seguintes conceitos devem ser utilizados:

Limite (ou apetite) do Risco: é a exposição e/ou impacto máximo do Risco que a Companhia está disposta a aceitar, na busca dos seus objetivos e geração de valor. Nem todos os tipos de Riscos são passíveis de aceitação. Portanto, a proposta de limites deverá obrigatoriamente ser fundamentada e formalizada pelas seguintes análises: (i) avaliação do retorno tangível e intangível relacionado ao limite de Risco proposto; (ii) capacidade da Companhia de suportar o impacto do limite de Risco proposto; (iii) decisão se o Risco deve ou não ser aceito conforme sua tipologia; (iv) viabilidade da implantação das iniciativas de mitigação (custo e esforço) versus efeito na mitigação do Risco e respectivo retorno; e (v) disponibilidade de recursos (investimento e esforço) para implantação.

Matriz/Modelagem de Riscos: visa estabelecer uma comparação individual dos Riscos a partir dos impactos e probabilidades de ocorrência para fins de priorização e gestão. A

matriz de riscos é um organismo em constante evolução e atualizada, no mínimo, anualmente, por ocasião da revisão de planejamento estratégico da Companhia e tempestivamente com o surgimento de eventos de Risco emergentes.

Definição de Risco(s): a possibilidade de que um evento ocorra e afete adversamente a realização dos objetivos da Companhia ou a probabilidade de insucesso, malogro de determinada coisa, em função de acontecimento eventual, incerto, cuja ocorrência não depende exclusivamente dos interessados.

3.1.1. Para fins de aplicação desta Política, os Riscos serão classificados nas seguintes categorias:

Riscos Prioritários: são Riscos com probabilidade e impacto potencialmente elevado para o negócio, cuja gestão deve ser priorizada e os seus indicadores devem ser monitorados regularmente.

Riscos Estratégicos: são Riscos associados à tomada de decisão da alta administração que podem gerar perda substancial no valor econômico da organização.

Riscos Operacionais: são Riscos associados à possibilidade de ocorrência de perdas de ativos, clientes ou receitas, resultantes de falhas, deficiências ou da inadequação de processos internos, pessoas e sistemas, assim como de eventos externos como catástrofes naturais, fraudes, greves e atos terroristas. Os Riscos Operacionais geralmente acarretam redução ou interrupção total ou parcial das atividades.

Riscos de Conformidade: são Riscos relacionados à falta de habilidade ou disciplina da Companhia para cumprir com a legislação e/ou regulamentação externa aplicáveis ao negócio, bem como às normas e procedimentos internos. Os Riscos de Conformidade também incluem as regras internas do negócio, possuindo um caráter mais amplo do que o conceito usualmente atribuído como risco legal ou regulatório, decorrente da aplicação da legislação trabalhista, tributária, fiscal e contratual, dentre outras.

Riscos de Conduta: são Riscos associados ao ferimento da moral e da ética da Companhia, por descumprimento do Código de Ética e Conduta e das políticas associadas, tais como: ações que caracterizem assédio, corrupção, conflitos de interesse, discriminação,

posicionamento político-partidário ou religioso, uso inadequado dos recursos da Companhia, dentre outros.

Riscos de Tecnologia e de Informação: são Riscos associados a fragilidades e/ou obsolescência dos sistemas de informação, controle e gestão da Companhia. Nessa categoria, incluem-se possíveis invasões externas aos sistemas para captura de dados e informações internas e/ou da cadeia de valor (clientes, fornecedores, parceiros de negócio etc.), Riscos de fraudes internas e/ou externas decorrentes dessas falhas, uso ou distribuição inadequada das informações e as falhas sistêmicas que prejudiquem a assertividade dos indicadores da Companhia.

Riscos de Crédito: são Riscos decorrentes de caixa e equivalentes de caixa, instrumentos financeiros derivativos, depósitos em bancos e outras instituições financeiras, bem como de exposições de crédito a clientes.

Riscos de Liquidez: são os Riscos relacionados à possibilidade de a Companhia não ser capaz de honrar eficientemente suas obrigações esperadas e inesperadas, correntes e futuras, inclusive decorrentes de vinculação de garantias, sem afetar suas operações diárias e sem incorrer em perdas significativas.

Riscos de Mercado: são os Riscos relacionados a perdas resultantes da flutuação nos valores de mercado de posições próprias da Companhia, incluindo os Riscos das operações sujeitas à variação cambial, das taxas de juros, dos preços de ações e preços de mercadorias (*commodities*).

Riscos Macroeconômicos e Sociais: são Riscos que envolvem fatores externos à Companhia provenientes de instabilidade econômica e mudanças do ambiente social. Como exemplo, pode-se citar o risco de segurança, associado ao problema de segurança pública em determinada região, que pode impedir a continuidade ou expansão de um determinado negócio naquele território.

Riscos Ambientais: são os Riscos associados à gestão inadequada de questões ambientais, causando efeitos como: contaminação de solo, água ou ar, decorrentes da operação ou da disposição inadequada de resíduos. Os Riscos Ambientais também incluem os efeitos decorrentes do aquecimento global sobre os negócios, que podem inviabilizar a expansão

do negócio.

Riscos de Imagem: são os Riscos associados à reputação da Companhia, quando o mau gerenciamento dos demais Riscos se torna público.

4. Referências

4.1. Esta Política tem como referências: (i) as regras de governança corporativa do Estatuto Social da Companhia; (ii) o Código de Ética e Conduta da Companhia; (iii) Política de Divulgação e Uso de Informações e de Negociação de Valores Mobiliários; e (iv) o Código Brasileiro de Governança Corporativa – Companhias Abertas.

5. Diretrizes

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

5.2. O objetivo da gestão de Riscos é entendê-los, avaliar e definir ações de resposta para que eventuais perdas sejam previstas e reduzidas, visando manter os Riscos em níveis aceitáveis. A análise de Riscos deve auxiliar o processo de tomada de decisão nos diversos níveis de gestão da Companhia.

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

(a) tomada de decisão consciente através de melhor conhecimento e consideração dos Riscos, contextos, impactos diretos e indiretos em todas as suas atividades;
(b) alocação de recursos de forma adequada para melhor controle dos Riscos Prioritários;
(c) transferência para o mercado de seguros de certos Riscos e de uma política de retenção adaptada a cada tipo de Risco; e
(d) gerenciamento adequado e coordenado de incidentes por meio do fornecimento de informação confiável e rápida à Diretoria em caso de grandes acontecimentos que possam impactar a Companhia.

5.4. O sistema adotado pela Companhia baseia-se, principalmente, em:

(a) identificação dos fatores (causas) de Riscos e implicações nos objetivos (metas e resultados) projetados;
(b) avaliação dos principais Riscos e incertezas suscetíveis de afetar os seus objetivos, por meio do cálculo de impacto e probabilidade de ocorrência dos Riscos;
(c) proposta de limites de Risco que a Companhia e seus acionistas estão dispostos a correr na busca pelo retorno e geração de valor;
(d) integração do gerenciamento de Riscos nos processos de tomada de decisão, incluindo o planejamento estratégico, as decisões de investimento e a gestão de projetos, desde o momento em que são criados e ao longo de todo o seu desenvolvimento; e
(e) utilização de ferramentas e mecanismos que objetivam a mitigação dos Riscos, por meio de inciativas definidas e implantadas pela Diretoria, com auxílio da área de gestão de Risco da Companhia, de forma a adequar a exposição da Companhia aos limites do Risco aprovado.

5.5. As Modelagens de Risco devem compor as ferramentas de análise e apoio às decisões da Diretoria, cabendo ao Comitê de Riscos da Companhia fornecer o apoio necessário à Diretoria para o desenvolvimento da gestão de Risco.

5.6. É fundamental o entendimento e disseminação entre os órgãos e executivos envolvidos da correta diferenciação de impactos causados por eventos e situações que não envolvem diretamente a gestão de Riscos como: (i) falhas de controles internos em processos; (ii) decisões estratégicas malsucedidas; ou (iii) falha na governança. Este entendimento visa aperfeiçoar e fortalecer o modelo de governança corporativa da Companhia.

5.7. Todos os Riscos, bem como os limites aprovados, deverão ser formalizados em relatórios detalhados, explicativos, com planos de ação, se for o caso, bem como a identificação dos responsáveis e prazos de conclusão dos planos de ação.

6. Tratamento dos Riscos:

6.1. Os Riscos identificados devem ser abordados de acordo com a sua criticidade. A área de Controles Internos da Companhia, juntamente com as áreas relacionadas ao Risco

identificado devem determinar como responder ao Risco, e definir os instrumentos de proteção para a Companhia, equilibrando os efeitos de resposta ao Risco com a eventual relação de custo/benefício decorrente de requisitos legais, regulatórios ou quaisquer outros que sejam relevantes a Companhia. A Comissão de Riscos, formada pelas áreas de Riscos, Jurídico, Controles Internos e Auditoria Interna de forma permanente, e por áreas convidadas de acordo com o Risco analisado, observará as seguintes alternativas para tratamento dos Riscos:

(i) Aceitar o Risco. Nenhuma ação é tomada para influenciar a probabilidade de ocorrência e/ou severidade do Risco. Riscos cujo impacto seja menor que o custo/benefício do seu gerenciamento podem ser mantidos, desde que conhecidos e aceitos pela Comissão de Riscos. No entanto, o monitoramento destes Riscos deve ser contínuo de modo a assegurar que, caso haja uma mudança de conjuntura que justifique alteração no tratamento do Risco, a Companhia implemente referido tratamento.

(ii) Rejeitar o Risco. Caso seja determinado que a Companhia não deverá conviver com o Risco nas condições em que este se apresenta, a Comissão de Riscos aplicará um dos tratamentos a seguir:

(a) *Evitar*: não correr o Risco e descontinuar as atividades que o geram. Evitar o Risco pode implicar na descontinuação de uma linha de produtos, divisão de negócios ou processos.

(b) *Mitigar*: ações são tomadas para reduzir a probabilidade de materialização e/ou severidade do Risco. Esta resposta envolve o aprimoramento ou criação de controles e melhorias em processos.

(c) *Compartilhar*: atividades que visam reduzir a probabilidade de ocorrência e/ou severidade do Risco, por meio da transferência ou compartilhamento de uma parte do Risco a terceiros, como, por exemplo, contratação de apólices de seguro, *outsourcing* e *hedging*.

7. Cargos e Responsabilidades

7.1. Compete ao Conselho de Administração da Companhia:

(a) aprovar as políticas, diretrizes, Matriz/Modelagem de Risco, limites de exposição e

impactos conforme apresentado pela Diretoria;
(b) fornecer à Diretoria, quando necessário, sua percepção do grau de exposição a Riscos da Companhia e influenciar na priorização dos Riscos a serem tratados;
(c) avaliar, quando necessário, mudanças nos limites de exposição de riscos que tenham sido aprovados pela Diretoria; e
(d) avaliar a adequação da estrutura operacional e de controles internos na avaliação da efetividade desta Política.

7.2. Compete à Diretoria da Companhia:

(a) validar as diretrizes, Matriz/Modelagem de Risco, determinando os limites de exposição, impactos, e a tolerância de exposição aos Riscos;
(b) definir a estrutura para o sistema de gerenciamento de Riscos dentro da Companhia;
(c) definir, em conjunto com a Comissão de Riscos, os planos de ação para mitigação dos Riscos;
(d) supervisionar o processo de avaliação de Riscos e monitorar a evolução da exposição aos Riscos e os sistemas de gerenciamento de Risco;
(e) disseminar a cultura da gestão de Risco em toda Companhia; e
(f) avaliar, pelo menos anualmente, a eficácia das políticas e dos sistemas de gerenciamento de Riscos e de controles internos, bem como do programa de *compliance* da Companhia e prestar contas ao Conselho de Administração sobre essa avaliação.

7.3. Compete à Área de Riscos da Companhia:

(a) interagir com as áreas críticas da Companhia, de modo a se antecipar aos Riscos decorrentes de novos projetos ou de processos investigatórios;
(b) estudar os processos atuais sob a ótica de Riscos;
(c) discriminar para a área de Controles Internos os Riscos identificados;
(d) apresentar, quando solicitado, sua percepção quanto à exposição ao Risco (magnitude de impacto e probabilidade de ocorrência), se possível, pautada também em indicadores de mercado;
(e) comunicar, tempestivamente, os eventos de Risco que apresentarem tendência de ocorrência e/ou eventual extrapolação de limites, para discussão nos fóruns e alçadas apropriadas;
(f) assegurar as informações disponibilizadas à Diretoria sobre Riscos ou incidentes, bem como coordenar o sistema de gerenciamento dos Riscos em momentos de crises em caso

de grandes acontecimentos.

7.4. Compete à área de Controles Internos da Companhia:

(a) avaliar, implantar e monitorar as ações com o objetivo de reduzir a exposição ao Risco;
(b) redesenhar os processos críticos recebidos da área de Riscos ou de outras áreas;
(c) normatizar os processos redesenhados;
(d) estabelecer os controles para cada um dos Riscos mapeados;
(e) cumprir nesses controles os limites de Riscos aprovados pelo Conselho de Administração;
(f) fornecer apoio metodológico aos departamentos operacionais e funcionais da Companhia por meio de ferramentas e serviços sob demanda;
(g) acompanhar a Diretoria na implantação desta Política por meio da disseminação de ferramentas e boas práticas.

7.5. Compete à área de Auditoria Interna da Companhia:

(a) auditar os controles estabelecidos pela área de Controles Internos em cada um dos processos críticos;
(b) aferir a qualidade e a efetividade dos processos de gerenciamento de Riscos da Companhia, sugerindo alterações ao Conselho de Administração e à Diretoria, quando necessário;
(c) discutir sobre os prós e contras de se correr determinados Riscos em projetos estratégicos e apresentar relatório final à Diretoria e ao Conselho de Administração, se necessário, para a tomada de decisão.
(d) propor limites para exposição aos Riscos.
(e) supervisionar o processo de avaliação de riscos e assegurar monitoramento constante de Riscos de fontes externas, com visão prospectiva sobre os Riscos emergentes.
(f) auditar os processos e controles internos, de acordo com a metodologia estabelecida, a fim de verificar o cumprimento de normas, políticas e procedimentos.
(g) avaliar a confiabilidade e a integridade das informações e os meios usados para identificar, mensurar, classificar e reportar tais informações.
(h) avaliar os sistemas estabelecidos para garantir a conformidade com as políticas, processos, leis e regulamentos que poderiam ter impacto significativo na Companhia.
(i) analisar os controles adotados para garantir o cumprimento das metas e objetivos

estabelecidos pela Companhia.

(j) monitorar e avaliar os processos de governança.

(k) avaliar os apontamentos realizados pelos auditores externos e o grau de coordenação com as áreas envolvidas.

(l) reportar periodicamente ao Conselho de Administração o desempenho da atividade de auditoria interna em relação ao seu plano.

(m) elaborar, ao menos anualmente, e submeter ao Conselho um Plano Anual de Auditoria Interna para revisão e aprovação.

(n) elaborar um relatório após a conclusão de cada trabalho com a resposta da gerência, contendo os planos de ação devidamente formalizados e aprovados.

7.6. Compete ao Departamento de Prevenção e Perdas:

(a) mitigar os Riscos e minimizar prejuízos relacionados a possíveis desvios de mercadorias e também à segurança patrimonial da Companhia.

(b) fiscalizar os processos de movimentação física da mercadoria, verificando se os procedimentos estão sendo cumpridos, identificando fragilidades para possíveis desvios e propondo as alterações necessárias para eliminá-las.

(c) buscar soluções de equipamentos e tecnologia quando necessário para minimizar os Riscos identificados relacionados às perdas de mercadorias e à segurança patrimonial da Companhia.

7.7. Compete ao Departamento Jurídico:

(a) assegurar a legalidade da condução dos negócios da Companhia, buscando prevenir Riscos regulatórios (com relação ao Código de Defesa do Consumidor, por exemplo), Riscos de fraude e os Riscos inerentes às políticas dos sites da Companhia (Política de Privacidade, Política de Uso, dentre outras), Código de Ética e Conduta e demais políticas relacionadas.

(b) controlar os contratos, ações judiciais e assessorar a Companhia em questões legais.

(c) alertar e auxiliar outras áreas sobre riscos trabalhistas e criminais, atuando na prevenção das relações existentes entre a Companhia, associados e parceiros de negócio.

7.8. Compete ao Departamento de Controladoria:

(a) zelar pela integridade e precisão dos registros financeiros da Companhia de acordo com as normas aplicáveis.

(b) revisar periodicamente, por equipe interna os registros financeiros da Companhia a fim de garantir segurança das informações.
(c) reportar à Diretoria e ao Conselho de Administração qualquer deficiência encontrada no processo de Auditoria Externa.

7.9. Compete ao Departamento de Segurança da Informação:

(a) monitorar os principais processos, fluxos financeiros, infraestrutura tecnológica, aplicações e serviços de tecnologia verificando se os procedimentos e/ou controles sistêmicos estão sendo cumpridos.
(b) identificar possíveis fragilidades ou desvios de comportamento, propondo as alterações necessárias para eliminá-las e/ou mitigá-las.
(c) fazer a gestão centralizada de vulnerabilidade.
(d) garantir testes frequentes de invasão, proteção contra negação de serviço, serviços de CDN (*Content Delivery Network*) de alta disponibilidade e capacidade, soluções anti-phishing e anti-fraudes.
(e) garantir o processo interno e formal de gestão continua de vulnerabilidade contemplando scans de vulnerabilidade e de testes de invasão (Pen Test), bem como ferramentas tradicionais, como: IPS, Antivírus, Firewalls Waff e monitoria de redes.
(f) correlacionar todas as ferramentas e eventos de negócio ou técnico gerados com ferramenta própria integrada ao centro de operações de segurança (SOC).

8. Vigência

Esta Política entra em vigor na data de sua aprovação e somente poderá ser modificada por deliberação do Conselho de Administração da Companhia.

*****