NATURA &CO HOLDING S.A.

POLÍTICA DE GERENCIAMENTO DE RISCOS

1. Propósito

O objetivo desta Política de Gestão de Riscos ("Política") é estabelecer diretrizes padrão e definir os princípios, papéis e responsabilidades relativamente às práticas de Gestão de Riscos Empresariais (ERM) para a Natura &Co, apoiando os processos de tomada de decisão e fornecendo conhecimentos relevantes tendo em conta o equilíbrio entre o risco e o desempenho.

2. Abrangência e aplicação

Esta Política aplica-se a todas as entidades do Grupo Natura &Co, independentemente do país de constituição, registo ou localização do escritório.

3. Definição

Plano de Ação: Uma ação, ou um conjunto de ações, desenvolvido para reduzir uma exposição ao risco.

Empresa ou Grupo: Natura &Co Holding S.A. e as suas empresas controladas, conhecidas como Business Units (BUs), nomeadamente Natura Cosméticos e Avon Products, Inc ("Avon").

Committee of Sponsoring Organizations of the Treadway Commission (COSO): Iniciativa conjunta composta por organizações especializadas e reconhecidas do setor privado, dedicadas a fornecer liderança de pensamento através do desenvolvimento de frameworks e orientações sobre Gestão de Riscos Empresariais, Controles Internos e dissuasão de Fraudes.

Riscos Emergentes: Riscos que podem ter a sua exposição aumentada, apesar dos seus níveis atuais, tal como indicado no atual Mapa de Riscos, devido a uma mudança abrupta de fatores internos e/ou externos que afetam o seu cenário.

Liderança Executiva: Representada pela Direção Executiva do Grupo e das Unidades de Negócios e pelos membros dos Comitês do Grupo, tais como ELT, Comex,. São responsáveis pela gestão da Companhia e pela condução do negócio e dos seus processos operacionais e financeiros.

IIA (The Institute of Internal Auditors): Associação profissional internacional e autoridade para assuntos de Auditoria Interna, Gestão de Riscos Empresariais, Governança Corporativa, Controles Internos e Auditoria de Tecnologia de Informação.

Impacto: A medida em que um Risco pode afetar a Empresa. Uma consequência potencial de uma materialização do risco é medida em termos financeiros e/ou não financeiros.

ISO (International Organization for Standardization): Federação mundial que prepara normas internacionais baseadas no consenso e relevantes para o mercado através de comitês técnicos.

ISO 31000: Norma Internacional emitida pela ISO com diretrizes para a Gestão do Risco.

Probabilidade: Probabilidade de ocorrência de um evento. Na terminologia de Gestão do Risco, é utilizada para referir a probabilidade de que algo aconteça, independentemente de ser definido, medido ou determinado de forma objetiva ou subjetiva, qualitativa ou quantitativa, ou

de ser descrito com a utilização de termos gerais ou matemáticos, tais como probabilidade ou frequência durante um determinado período.

Risco: A possibilidade de que os eventos ocorram e afetam a realização de objetivos estratégicos e empresariais, impedindo a criação ou mesmo destruindo o valor existente, ou contribuindo potencialmente para o processo de tomada de decisão para uma oportunidade estratégica ou empresarial.

Apetite de risco: Nível agregado de exposição e tipos de Risco que a empresa está disposta a assumir a fim de atingir os seus objetivos estratégicos.

Exposição ao risco: Combinação de Impacto e Probabilidade que representa efeitos adversos dos Riscos.

Mapa dos Riscos: Representação gráfica dos níveis de exposição ao risco em dois eixos de análise (Impacto e Probabilidade), compreendendo uma matriz 4x4.

Gestão de Riscos: Conjunto de atividades e procedimentos definidos para gerir os riscos e oportunidades. No contexto desta Política, refere-se especificamente à abordagem de Gestão de Riscos (ERM) do Grupo.

Proprietários dos Riscos (Risk Owners): Gestores ou executivos que têm a responsabilidade e autoridade para gerir riscos e oportunidades em diferentes áreas de negócio e operacionais dentro da Empresa. São designados pela Liderança Executiva como responsáveis pela identificação e aplicação eficaz dos procedimentos de Gestão de Riscos, em conformidade com o Apetite pelo Risco acordado.

Resposta ao risco: Ação tomada quando um Risco é identificado, após a decisão de o atenuar, rejeitar ou reter. A estratégia global do Grupo indica a mitigação como a resposta ao risco definidos, o que resultará na necessidade de definir um Plano de Ação para mitigar esse risco.

4. Princípios e Diretrizes

O Grupo está empenhado em manter um modelo de governação robusto e integrado para assegurar, em benefício das suas partes interessadas, a realização dos objetivos corporativos e o desempenho das suas responsabilidades com responsabilidade, cumprimento, divulgação e equidade.

As práticas de Gestão de Riscos, que incluem a identificação de oportunidades e ameaças, são vistas pelo Grupo como uma componente central do compromisso aqui declarado. É um processo constante e transparente que incumbe a todos os profissionais que trabalham para o Grupo em todos os níveis hierárquicos. Cada um é responsável por tomar consciência dos Riscos envolvidos na sua área, considerando aspectos de curto, médio e longo prazo, juntamente com a sua gestão e comunicação, de acordo com conceitos, diretrizes e instruções brevemente descritas nesta Política e detalhadas nos seus documentos complementares.

A abordagem metodológica da Natura &Co ERM baseia-se no quadro integrado sugerido pelo COSO e nas diretrizes definidas na ISO 31000 para a Gestão do Risco, observando também os conceitos estabelecidos no Modelo de Três Linhas, desenvolvido pelo IIA, que é ilustrado abaixo na figura 1.

Figura 1 - Adaptado do Modelo de Três Linhas do IIA

O Modelo de Três Linhas do IIA garante a segregação entre a responsabilidade direta: decisões de risco (Primeira Linha); supervisão independente sobre decisões de risco juntamente com definições para o quadro de Gestão de Risco (Segunda Linha); e garantia independente sobre a eficácia da Gestão de Risco, controle e processos de governação (Terceira Linha).

A Primeira Linha é responsável pela execução diária da estratégia e propriedade do risco, e é formada pelas áreas de negócio, incluindo filiais e empresas controladas. A Segunda Linha é formada por áreas independentes como a Gestão de Riscos e Controles Internos, Conformidade, Regulamentação e Segurança da Informação, que fornecem instrumentos para os gestores da Primeira Linha gerirem eficazmente os Riscos de forma preventiva. A Terceira Linha é formada pela Auditoria Interna, trabalhando de forma independente para verificar a eficácia do modelo de forma detectiva. Funções e responsabilidades mais abrangentes de cada linha podem ser encontradas no item 5 (Funções e Responsabilidades) desta Política.

4.1 Natura &Co ERM Framework

A metodologia ERM do Grupo está resumida no quadro apresentado na figura 2. É um processo contínuo que engloba quatro etapas principais: i) Identificação e Análise; ii) Avaliação; iii) Resposta; iv) e Supervisão. O quadro contempla as diretrizes ISO 31000 segregadas em diferentes grandes grupos de atividades.

Figura 2 - Representação gráfica do quadro de gestão de riscos da Natura &Co

Onde:

Identificação e Análise

Identificação e Análise é um processo interativo que contempla a verificação de fatores internos e externos que contribuem para o debate de eventos que podem afetar o âmbito dos objetivos empresariais a curto, médio e longo prazo, de forma preventiva, durante na tomada de decisão, bem como avaliar as suas implicações.

Para estabelecer o contexto de identificação, é importante considerar tanto o ambiente interno como externo, capturado e refletido na estratégia do Grupo. Os fatores internos a observar incluem a visão e missão da Empresa, objetivos estratégicos, iniciativas para apoiar a realização de metas, governança (normas, procedimentos e diretrizes), relação com os intervenientes internos e questões contratuais, cultura e estruturas organizacionais, dados e processos. Os fatores externos compreendem as circunstâncias que rodeiam a Empresa nos contextos internacionais, nacionais, regionais e locais, tais como fatores sociais, culturais, políticos, legais, regulamentares, financeiros, tecnológicos, econômicos, ambientais e de relacionamento com as partes interessadas externas.

Os Proprietários de Riscos, juntamente com outras áreas da empresa, e tendo em conta a sua capacidade de contribuir com informação relevante, devem proceder à análise dos Riscos para identificar as causas, processos e áreas que possam ser afetadas em caso de materialização, alinhadas com as causas e consequências potenciais para a Empresa.

Avaliação

As avaliações de risco analisarão o impacto potencial e a probabilidade de uma materialização, o que definirá o nível de Exposição ao Risco. A representação gráfica dos níveis de Exposição aos Riscos da Empresa compreenderá uma matriz 4x4 (Mapa de Risco) para apoiar o processo de tomada de decisão e a priorização dos temas.

Os riscos devem ser devidamente identificados, avaliados e priorizados, a fim de assegurar que os temas mais relevantes serão periodicamente monitorados nos fóruns de governança

adequados, as iniciativas de resposta serão tratadas tempestivamente, e as exposições serão geridas dentro de níveis aceitáveis.

Resposta

A resposta refere-se à estratégia de resposta aos Riscos, ou à forma como a Empresa optará por lidar com os Riscos. Deve ser alinhada ao Apetite de Risco da Empresa, orientada pelos níveis de Exposição ao Risco, como o seu posicionamento no Mapa de Riscos. A definição de ações e iniciativas de Resposta ao Risco e concepção de mitigação visará uma tomada de decisão consciente para as melhores alternativas de resposta, considerando os resultados a curto, médio e longo prazo. O prazo da mitigação dos riscos deve ser compatível com a sua criticidade e velocidade de materialização, a fim de permitir uma redução adequada da exposição.

As respostas devem ser a melhor alternativa de reação à luz das possibilidades, considerando o Apetite de Risco da Empresa, o que melhor equilibrará a redução da exposição e custos relacionados. Após a implementação de uma Resposta ao Risco, é importante considerar iniciativas de mitigação prospectivas (Planos de Ação) propostas e executadas pelos Proprietários do Risco.

Os Planos de Ação serão implementados, executados e geridos pela Primeira Linha, serão monitorados e apoiados pela Segunda Linha, e serão discutidos em fóruns de governança, quando aplicável.

Monitoramento

O monitoramento e a análise crítica consistem nos processos de verificação, supervisão, observação crítica e implantação de melhorias a partir da identificação de mudanças no nível de desempenho requerido ou esperado. Fóruns onde os riscos são monitorados são inicialmente classificados pela sua origem e pela área funcional.

É importante que o monitoramento ocorra em todos os aspectos do processo de gerenciamento de Riscos visando (i) garantir que os controles e as práticas de gerenciamento sejam eficazes e eficientes no desenho e na operação; (ii) obter informações que possam melhorar o processo de avaliação de Riscos; (iii) aprimorar o processo através da análise de eventos, mudanças, tendências, sucessos e fracassos; (iv) identificar mudanças no contexto externo e interno, que podem inclusive influenciar escolhas de respostas passadas e priorizações realizadas; (v) identificar Riscos emergentes.

5. Funções e Responsabilidades

5.1 Conselho de Administração

• Definir a filosofia de gestão do risco da organização de acordo com a missão, valores e princípios estabelecidos;

• Definir os níveis de Apetite ao Risco do Grupo com base nos objetivos empresariais de curto, médio e longo prazo;

• Rever e aprovar as definições gerais das estratégias de gestão do risco, incluindo esta Política;

• Monitorar os alinhamentos críticos: estratégia, riscos, controles, conformidade, incentivos e pessoas;

• Tomar conhecimento e avaliar periodicamente se os processos de gestão do risco incluindo os riscos priorizados, permitem ao Conselho de Administração atingir os seus objetivos de supervisão do risco; bem como, se necessário, recomendar alterações.

5.2 Comitê de Auditoria, Gestão de Riscos e Finanças

• Supervisionar a adequação dos processos relacionados com a gestão de riscos e com o sistema de controle interno, em conformidade com as diretrizes estabelecidas pelo Conselho de Administração;

• Apoiar os gestores na formulação de conceitos e metodologias utilizadas na gestão do Risco Corporativo, bem como do Mapa de Risco e da régua de Risco, que os classifica de acordo com a gravidade dos seus potenciais impactos;

• Avaliar e monitorar a exposição ao risco da Empresa;

• Acompanhar a evolução da gestão dos riscos identificados, bem como a conformidade com a legislação, políticas, regras e procedimentos aplicáveis do Grupo, e a eficácia dos controles e das ações de resposta abordadas;

• Avaliar a adequação dos recursos humanos e financeiros atribuídos ao processo de gestão dos riscos corporativos do Grupo.

• Manter o Conselho de Administração devidamente informado sobre a eficácia dos processos de gestão dos Riscos, incluindo os Riscos priorizados, bem como, sempre que necessário, recomendar alterações aos conceitos e aos níveis de apetite pelo risco.

5.3 Liderança executiva (Grupo e Unidades de Negócio)

• Submeter ao Comitê de Auditoria, Gestão de Riscos e de Finanças e ao Conselho de Administração a aprovação das diretrizes gerais para a gestão de riscos e os limites de exposição;.

• Avaliar o desempenho do processo de gerenciamento de Riscos

• Garantir os recursos necessários à operacionalização das diretrizes gerais para a gerenciamento de Riscos

• Validar as revisões periódicas do mapeamento dos Riscos com Impacto nas estratégias do Grupo

• Acompanhar o comportamento das exposições dos Riscos prioritários

5.4 Diretor Presidente (Chief Executive Officer – CEO) Grupo e Unidades de Negocio

Promover a integração entre o ERM e os ciclos de revisão e construção do plano estratégico do Grupo e das Unidades de Negócio.

5.5 Área de Gestão de Riscos e Controles Internos (Grupo e Unidades de Negocio)

A Área de Risco e Controles Internos assume várias responsabilidades relativamente à sua Gestão de Risco, Controles Internos, Segurança da Informação e Estrutura de Seguros. As principais responsabilidades da Área de Gestão de Riscos Empresariais são:

• Desenvolvimento e implementação da estratégia e metodologia de Gestão de Riscos Empresariais em conformidade com as leis, regulamentos, políticas, regras, procedimentos

internos e melhores práticas de gestão aplicáveis;

• Em conjunto com 2ª e 3ª linhas (ref. IIA), conciliar as análises de risco, impacto e probabilidade, de modo a que os mesmos conceitos de classificação de risco sejam utilizados em todas as atividades;

• Manter esta Política, o Procedimento de Gestão de Risco da Empresa e outros documentos complementares de Risco atualizados (Mapa de Risco, etc.).

• Promoção de uma cultura de gestão do risco na organização;

• Fornecer ferramentas para os proprietários de Risco identificarem, analisarem, avaliarem o Risco e darem o melhor conjunto de respostas adequadas e tempestiva;

• Monitorar periodicamente os níveis de exposição aos Riscos;

• Relatar à Direção Executiva e ao Comitê de Auditoria, Gestão de Riscos e Finanças os níveis de exposição potencial dos principais Riscos;

• Monitoramento da implementação dos planos de ação dos proprietários do risco, sempre que aplicável, a fim de verificar a sua atenuação ou redução, comunicando-a Liderança Executiva e ao Comitê de Auditoria, Gestão de Riscos e Finanças.

5.6 Auditoria Interna

• Avaliar e rever a eficácia e eficiência das transações e das informações por elas produzidas e proteger os bens da Companhia assegurando o cumprimento de leis, regulamentos e contratos;

• Examinar o sistema de controles internos, fornecendo uma avaliação da sua eficácia à alta gerência;

• Prestar aconselhamento ao Diretor Presidente do Grupo e ao Conselho de Administração, através do Comitê de Auditoria, Gestão de Riscos e Finanças, monitorando, examinando, avaliando, informando e recomendando melhorias para o ambiente interno e eficácia do processo de Gestão de Riscos;

• Identificação e indicação dos Riscos que possam não ter sido mapeados pela organização, através de uma avaliação independente do ambiente dos controles internos;

• Avaliar a qualidade e eficácia dos processos de gestão dos riscos da empresa, monitorar periodicamente as ações de mitigação dos riscos e as fragilidades registadas nos relatórios de auditoria e alimentar o modelo de gestão dos riscos com informações.

5.7 Proprietários de risco

• Identificação, avaliação, mitigação e monitoramento dos Riscos dos processos e negócios sob a sua responsabilidade, com base nos critérios estabelecidos pelo Grupo;

• Definir e implementar ações atenuantes e práticas de gestão da exposição aos Riscos;

• Criação e atualização dos indicadores-chave utilizados para monitorar os Riscos;

• Assegurar o desempenho e eficácia dos Controles Internos existentes utilizados para mitigar os Riscos;

• Formalização de exposições ocasionais a Riscos identificados devido à monitoramento de transações que são desconhecidas da Administração.

6. Comunicação de riscos

Os fóruns de compartilhamento e monitoramento das exposições são inicialmente definidos tendo em conta a classificação de cada risco, tal como descrito abaixo:

Nível de Exposição do Risco	Fórum de compartilhamento e monitoramento
4. Severo (Severe)	Conselho de Administração, Comitê de Auditoria, Gestão de Riscos e Finanças e Liderança Executiva.
3. Alto (High)	Comitê de Auditoria, Gestão de Riscos e Finanças, Liderança Executiva e Vice-presidências responsáveis pela(s) unidade(s) de negócio.
2. Moderado (Moderate)	Oficiais responsáveis pelas unidades de negócio
4. Baixo (Low)	Oficiais responsáveis pelas unidades de negócio

Os fóruns criados podem, em qualquer altura, solicitar que os sujeitos de risco sejam registrados para controle e reconhecimento, independentemente dos níveis de exposição indicados, e os proprietários dos sujeitos (riscos) devem preparar documentação que permita a compreensão tempestiva das exposições atuais, da fase de implementação das ações e do prazo para a conclusão dessas ações, bem como restrições ou eventos extraordinários responsáveis por extensões ocasionais.

7. Considerações Finais

Devido à dimensão do Grupo, às suas particularidades empresariais, complexidade das estruturas, contextos operacionais e localizações geográficas diversas, juntamente com diferentes jurisdições e ambientes regulamentares onde as Unidades de Negócio operam, esta Política pode ser complementada por procedimentos específicos (procedimento ERM, e outros documentos complementares) aplicáveis e/ou necessários. A revisão desta Política foi aprovada em maio de 2024 pelo Conselho de Administração do Grupo Natura &Co, substituindo a sua versão anterior, entrando imediatamente em vigor, na data da sua publicação e divulgação, e permanecerá em vigor por um período indeterminado, até que seja resolvido o contrário.