

1. OBJETIVO

O objetivo desta Política Corporativa para Uso de Inteligência Artificial (“Política”) é definir princípios e diretrizes gerais que orientam o uso, desenvolvimento e a contratação de sistemas e ferramentas (“Soluções de IA”) de Inteligência Artificial (“IA”), na Ultrapar e suas controladas (“Negócios”, em conjunto com Ultrapar, “Grupo Ultra”).

Esta Política deve ser considerada em conjunto com o Código de Ética e as demais políticas corporativas do Grupo Ultra, sendo aplicável a todos os seus administradores e colaboradores, no Brasil e no exterior, bem como aos representantes externos, fornecedores, clientes e prestadores de serviço e parceiros de negócios, sempre que houver uso, desenvolvimento ou contratação de Soluções de IA ou que utilizem IA.

2. CONCEITOS

Para os fins desta Política, adotam-se estes conceitos:

- **IA Generativa:** Solução de IA capaz de criar conteúdo (como textos, imagens, sons, vídeos e códigos) a partir de comandos ou dados de entrada fornecidos pelos Usuários.
- **Usuário de IA:** quem utiliza soluções de IA no exercício das suas atividades profissionais, ainda que sem qualquer envolvimento técnico no seu desenvolvimento.
- **Avaliação de impacto de inteligência artificial:** documento prévio à aplicação de Soluções de IA, sempre que a Solução de IA for considerado como de alto risco pela avaliação preliminar das áreas de Segurança da Informação, Privacidade e Proteção de Dados e de Gestão de Riscos dos Negócios, para identificar, analisar e mitigar riscos.
- **Ciclo de vida da IA:** conjunto de fases relativas ao desenvolvimento e aplicação da Solução de IA, como planejamento, treinamento, retreinamento, testagem, validação, implantação, monitoramento, adaptações, uso e eventual descontinuidade.

3. PRINCÍPIOS ÉTICOS E RESPONSÁVEIS PARA USO E DESENVOLVIMENTO DE IA

Os princípios indicados abaixo devem orientar todas as decisões relacionadas à IA:

- **Auditabilidade, confiabilidade e robustez:** permitir que as Soluções de IA operem de forma segura, precisa e consistente, garantindo rastreabilidade das decisões, recomendações ou resultados (trilha de auditoria) e a manutenção do desempenho adequado.
- **Não discriminação, equidade e inclusão:** promover o desenvolvimento e uso de Soluções de IA sem vieses ou qualquer tipo de discriminação, garantindo a atuação da IA com imparcialidade e em conformidade com o Código de Ética.
- **Privacidade e proteção de dados:** assegurar que o tratamento realizado por Soluções de IA respeite a legislação e normas internas sobre privacidade e proteção de dados. Caso o uso seja indispensável, é necessário envolver previamente a área responsável por Privacidade e Proteção de Dados do respectivo Negócio.
- **Qualidade dos dados:** assegurar que os dados utilizados pelas Soluções de IA sejam obtidos de fontes legítimas e que sejam validados a fim de garantir a precisão, atualização e completude, bem como a confiabilidade dos resultados e a mitigação de riscos operacionais, regulatórios e reputacionais.
- **Responsabilidade e supervisão humana:** assegurar que todas as pessoas e áreas envolvidas no Ciclo de Vida das Soluções de IA compreendam e assumam a responsabilidade pelas suas ações, decisões e impactos decorrentes do uso da tecnologia, assim como garantir a supervisão humana sobre as decisões automatizadas.
- **Segurança:** garantir que as Soluções de IA sejam projetadas, implementadas e operadas de forma segura, resiliente e protegida contra falhas, vazamento de dados, ataques cibernéticos, manipulações ou usos indevidos.
- **Transparência e explicabilidade:** assegurar que a utilização de Soluções de IA, bem como suas recomendações, decisões e resultados, sejam comunicados de forma clara e acessível,

incluindo informações sobre finalidade, funcionamento, limitações e eventuais impactos, fortalecendo a confiança de colaboradores, de parceiros e da sociedade.

4. PRINCIPAIS RISCOS RELACIONADOS À IA

A adoção de Soluções de IA potencializa ganhos de eficiência e inovação, porém pode ocasionar impactos reputacionais, financeiros, legais e operacionais relevantes, demandando avaliação prévia criteriosa e implementação de medidas de mitigação.

Em caso de dúvida sobre o nível de risco da Solução de IA, as áreas responsáveis por Segurança da Informação, Privacidade e Proteção de Dados e de Gestão de Riscos da Ultrapar e/ou dos Negócios, conforme aplicável, devem ser consultadas previamente para apoiar na avaliação/indicação de medidas adicionais de governança, documentação e validação.

5. PAPÉIS E RESPONSABILIDADES

A depender do nível de interação com as Soluções de IA, os colaboradores do Grupo Ultra, além de cumprir integralmente a presente Política, devem observar as orientações aplicáveis ao seu papel, conforme estabelecido abaixo.

5.1. CONSELHO DE ADMINISTRAÇÃO DA ULTRAPAR

- Aprovar esta Política e suas revisões.
- Assegurar que riscos de IA estão capturados pela matriz de riscos da Ultrapar.

5.2. CONSELHO DE ADMINISTRAÇÃO DOS NEGÓCIOS

- Garantir a aplicação desta Política em seu negócio.
- Assegurar que os riscos de IA estão capturados pela matriz de riscos do seu Negócio, considerando eventuais riscos específicos e mitigadores.

5.3. ÁREA RESPONSÁVEL POR PRIVACIDADE E PROTEÇÃO DE DADOS DA ULTRAPAR E/OU DOS NEGÓCIOS

- Fornecer orientações sobre o tratamento de dados pessoais e dados pessoais sensíveis nas Soluções de IA.
- Apoiar a classificação e mitigação de riscos de privacidade.
- Apoiar na realização da Avaliação de Impacto de Inteligência Artificial.
- Apoiar na construção e atualização do inventário de Soluções de IA.

5.4. ÁREA DE RISCOS, INTEGRIDADE E AUDITORIA DA ULTRAPAR E/OU DOS NEGÓCIOS

- Avaliar o risco e reporte de vieses ou discriminação na utilização de Soluções de IA e sugerir medidas de mitigação e controle.
- Coordenar e apoiar nas discussões de identificação, avaliação, tratamento e monitoramento dos riscos de IA.
- Recomendar ações para tratamento dos riscos de IA.
- Apoiar na realização da Avaliação de Impacto de Inteligência Artificial.
- Apoiar na construção e atualização do inventário de Soluções de IA e classificação de risco.

5.5. ÁREA DE SEGURANÇA DA INFORMAÇÃO DA ULTRAPAR E/OU DOS NEGÓCIOS

- Avaliar riscos técnicos e cibernéticos associados ao uso de Soluções de IA.
- Conduzir a Avaliação de Impacto de Inteligência Artificial, quando aplicável, podendo contar com o apoio de outras áreas.
- Apoiar o processo de homologação de Soluções de IA.
- Apoiar os desenvolvedores de IA na elaboração de documentação de Soluções de IA.
- Revisar integrações das Soluções de IA com sistemas críticos.
- Colaborar na definição e na aplicação de controles técnicos e organizacionais de proteção da informação e mitigação de vulnerabilidades.

- Apoiar na construção e atualização do inventário de Soluções de IA e classificação de risco.
- Oferecer treinamento obrigatório acerca desta Política aos administradores e colaboradores do Grupo Ultra, bem como para seus parceiros de negócios, representantes externos, fornecedores e prestadores de serviços pertinentes.
- Verificar e acompanhar o tempo de guarda e local de armazenagem dos dados e informações.

5.6. DESENVOLVEDORES DE IA

- Observar os princípios éticos e responsáveis para o uso e desenvolvimento de IA desde a concepção de Soluções de IA, conforme definido nesta Política, e no Código de Ética de forma que decisões de alto impacto mantenham prioritariamente revisão humana.
- Garantir que a Solução de IA e sua utilização estejam em conformidade com as políticas corporativas, leis e normas aplicáveis.
- Não utilizar informações sensíveis ou confidenciais no desenvolvimento de IA, exceto se expressamente permitido e com salvaguardas definidas pelas áreas responsáveis pela salvaguarda dos dados.
- Implementar medidas para garantia de segurança e resiliência em Soluções de IA, com prevenção de falhas, manipulação, ataques cibernéticos e uso indevido.
- Garantir a documentação, com registros completos sobre *datasets*, algoritmos, modelos e decisões, permitindo a rastreabilidade do Ciclo de Vida das Soluções de IA e identificação dos limites de aplicabilidade do modelo.
- Realizar testes éticos e técnicos antes da implantação e após o uso periodicamente.
- Reportar em tempo adequado riscos, falhas, vieses ou violações éticas identificadas às áreas responsáveis por Segurança da Informação, Privacidade e Proteção de Dados e Gestão de Riscos dos Negócios.
- Realizar a zeladoria do conteúdo gerado pela IA, sustentação (retreino) e evolução dos modelos e aplicações de IA.

5.7. USUÁRIOS DE IA

- Utilizar exclusivamente Soluções de IA homologados pelo Grupo Ultra ou respectivo Negócio.
- Garantir que o uso de Soluções de IA esteja alinhado a esta Política, ao Código de Ética e às diretrizes do Grupo Ultra.
- Não utilizar informações sensíveis ou confidenciais nas Soluções de IA, salvo com a respectiva autorização (se aplicável) e/ou adoção de salvaguardas.
- Não reproduzir conteúdo gerado por IA sem validação humana prévia, especialmente se o tema tratar de decisões de alto impacto, se houver publicação externa das informações ou quando envolver análises relevantes aos negócios ou Grupo Ultra.
- Reportar comportamentos anômalos, fragilidades e novos riscos identificados às áreas responsáveis por Segurança da Informação, Privacidade e Proteção de Dados e Gestão de Riscos do respectivo Negócio ou ao Canal Aberto e zelar pela integridade e segurança das informações inseridas ou tratadas pela Solução de IA.

5.8. ÁREA JURÍDICA DOS NEGÓCIOS

- Apoiar a análise de riscos legais relacionados ao uso e à contratação de Soluções de IA.
- Revisar cláusulas contratuais com fornecedores e parceiros de Soluções de IA.
- Avaliar eventuais obrigações regulatórias relacionadas à utilização e desenvolvimento de IA.
- Contribuir na definição de modelos de responsabilidade aplicáveis às Soluções de IA.

As demais áreas do Grupo Ultra e dos respectivos Negócios poderão ser envolvidas conforme o contexto de uso, o tipo de Solução de IA, riscos identificados e especificidades de cada área de atuação, incluindo para fins de treinamento e conscientização.

6. DIRETRIZES PARA CONTRATAÇÃO DE SOLUÇÕES DE IA OU QUE ENVOLVAM UTILIZAÇÃO DE IA

Para realizar a contratação de Soluções de IA ou que envolvam utilização de IA, além de seguir as políticas corporativas relacionadas à contratação de serviços e/ou produtos, a Contratante deve:

- Informar a área de Segurança da Informação do respectivo Negócio para inventariar e apoiar na avaliação dos riscos associados as Soluções de IA.
- Avaliar a finalidade e os riscos da Solução de IA, com análise do objetivo da contratação e o potencial impacto sobre pessoas ou grupos afetados, processos produtivos, ativos do Grupo Ultra e dados estratégicos ou confidenciais.
- Garantir que a Solução de IA contratada seja aderente às políticas corporativas do Grupo Ultra e do respectivo Negócio.
- Assegurar que os Usuários de IA estejam capacitados e que a área de Segurança da Informação sempre seja envolvida antes da contratação para avaliação dos riscos.
- Prever mecanismos contratuais e técnicos de atualização tecnológica e adequação a novas regulações aplicáveis, assim como o desligamento seguro e a gestão de dados em casos de descontinuidade do fornecedor ou término contratual.
- Realizar a zelaroria do conteúdo gerado pela IA, sustentação (retreino) e evolução dos modelos e aplicações de IA.

7. TREINAMENTOS

Todo o público-alvo da presente Política deverá participar de treinamentos periódicos sobre os assuntos tratados no presente documento.

8. CANAL ABERTO

O Canal Aberto está disponível para esclarecimento de dúvidas e comunicação da existência e/ou de suspeita de violações a esta e outras políticas internas do Grupo Ultra ou legislação aplicável.

- Site: **canalabertoultra.com.br**
- Telefone: **0800 701 7172**

Os relatos poderão ser enviados de forma anônima. É proibido praticar qualquer ato de ameaça, intimidação ou retaliação a qualquer pessoa que: (i) reportar violações a esta Política e qualquer outra política ou legislação aplicável; ou (ii) manifestar suas dúvidas, suspeitas ou preocupações em relação a este assunto. O Canal é operado por empresa independente e todos os relatos são registrados e encaminhados para condução ou supervisão da apuração pela Diretoria de Riscos, Integridade e Auditoria.