1. OBJETIVO

Esta política rige el uso de toda técnica computacional y proceso de Inteligencia Artificial, conocida como IA, que sea utilizado para potenciar y mejorar las capacidades humanas en la prestación de los servicios de Nativo.

2. ALCANCE.

Esta Política aplica para todas las personas que colaboren en la prestación de servicios de Nativo incluyendo Directivos, Trabajadores, Proveedores por Honorarios y *Freelancers*.

3. TÉRMINOS DEFINIDOS

- **Nativo:** Se refiere a las sociedades debidamente constituidas en la legislación mexicana con las denominaciones: Nativo Priority, S.C., The Packshot, S.A. de C.V. y Creative Data Lab, S.A.P.I. de C.V.

- **Trabajadores:** Son las personas físicas que prestan servicios de manera personal y subordinada a Nativo.

- **Proveedores**: Son las personas físicas que prestan servicios profesionales de manera independiente, ya sea por honorarios o como *freelancers* a Nativo, a través de la celebración y firma de un contrato de prestación de servicios profesionales e independientes.

- **Alucinación.** Se refiere a la información incorrecta, engañosa o totalmente inventada generada por un modelo de IA que parece ser cierta.

- **Anonimización:** Se refiere al proceso mediante el cual se desvincula toda aquella Información que permita la identificación del titular, por lo que la Información no puede vincularse a una persona determinada o determinable.

- **Auditoría interna:** Se refiere a la evaluación interna, que realiza el Comité de Ética, de los sistemas de IA, los algoritmos y las prácticas de datos para identificar riesgos como sesgos, problemas de privacidad, infracciones a la propiedad intelectual y cuestiones éticas.

- **Comité de Ética:** Es el equipo conformado por el director general, el área legal que supervisa y audita regularmente los procesos que utiliza Nativo con la inteligencia artificial y la correcta aplicación de la presente política.

- ***Deepfake*:** Se refiere a la inteligencia artificial que crea imágenes, sonidos y videos engañosos convincentes, al combinar el aprendizaje profundo con información falsa.

- **Ética**: Se refiere a la facultad de las personas de normar las acciones morales y los principios encaminados hacia la realización del bien y el "deber hacer" lo correcto.

- **IA.** Se refiere a la Inteligencia Artificial como la capacidad de un sistema de interpretar correctamente los datos externos, de aprender de ellos y de utilizar esos aprendizajes para lograr objetivos y tareas específicas mediante una adaptación flexible y que pretende dotar de autonomía y adaptabilidad a las computadoras, con la finalidad de que realicen tareas de forma eficiente e innovadora y sin la necesidad de supervisión humana.

- **Política.** Se refiere a esta política que es de cumplimiento obligatorio.

- **Privacidad de la información:** Se refiere a la capacidad que tiene una persona (física o moral) para controlar la forma en la que se recopilan, usan, almacenan y comparten sus datos personales, enfocándose en la regulación del acceso y uso de los datos para asegurar que se manejen de acuerdo con las leyes y los derechos individuales.

- ***Prompt*:** Se refiere a la entrada proporcionada por un usuario para interactuar con un modelo de IA y generar una respuesta, o salida, del modelo. Las indicaciones suelen incluir instrucciones específicas que debe seguir el modelo o preguntas que debe responder.

- **Propiedad Intelectual:** Se refiere a la protección del producto del intelecto humano que concede a los creadores, autores e inventores un derecho.

4. PRINCIPIOS EN EL USO DE LA IA.

a. Transparencia y divulgación.

- Divulgar el uso de sistemas de IA a los usuarios y las partes interesadas.
- Proporcionar información clara sobre cómo funciona el sistema de IA, incluyendo su finalidad, capacidades y limitaciones.

b. Privacidad y protección de datos:

- Limitar la recopilación de datos a lo necesario e implementar prácticas sólidas de anonimización y cifrado de datos.
- Obtener el consentimiento adecuado para la recopilación y el procesamiento de datos

c. Equidad y no discriminación.

- Evitar sesgos y discriminación en los resultados de la IA.
- Auditar periódicamente los algoritmos de IA para garantizar la equidad y la imparcialidad.
- Implementar medidas para prevenir impactos discriminatorios en clases de personas protegidas.

d. Responsabilidad y gobernanza.

- Asignar claramente la responsabilidad de las decisiones y los resultados relacionados con la IA.
- Mantener una documentación detallada del desarrollo, el uso y los procesos de toma de decisiones del sistema de IA.
- Establecer mecanismos de supervisión interna.

e. Precisión y fiabilidad.

- Garantizar que los sistemas de IA proporcionen resultados precisos y fiables.
- Probar y validar los modelos de IA periódicamente para minimizar los errores y las imprecisiones.
- Comunicar a los usuarios cualquier limitación del sistema de IA.

f. Seguridad y protección.

- Implementar medidas de seguridad para evitar el uso indebido, la piratería informática u otras vulnerabilidades de seguridad.
- Supervisar y actualizar periódicamente los sistemas de IA para hacer frente a las amenazas en constante evolución.
- Garantizar que los sistemas de IA funcionen dentro de los parámetros de seguridad predefinidos.

g. Supervisión y control humanos.

- Diseñar/utilizar sistemas de IA que permitan la intervención y la supervisión humanas cuando sea necesario.
- Evitar la automatización total de las decisiones críticas o de alto riesgo sin revisión humana.

h. Cumplimiento de la propiedad intelectual (PI).

- Garantizar que los sistemas de IA no infrinjan los derechos de propiedad intelectual de los clientes (por ejemplo, patentes, derechos de autor o marcas comerciales).
- Abordar la propiedad del contenido generado por la IA y aclarar los derechos de propiedad intelectual en los contratos.

i. Cumplimiento normativo.

- Cumplir con las normativas de IA específicas del sector en el que se encuentren nuestros clientes y la jurisdicción aplicable.
- Supervisar las normativas de IA emergentes y adaptar los sistemas a medida que evolucionen las leyes.

j. Consideraciones éticas.

- Alinear el desarrollo y el uso de la IA con principios éticos, como promover el beneficio social y evitar daños.
- Considerar el impacto más amplio de la IA en las partes interesadas, incluidos los empleados, los clientes y la sociedad.

k. Explicabilidad.

- Garantizar que los sistemas de IA proporcionen resultados que sean interpretables y explicables para los usuarios.
- Evitar los modelos de IA de “caja negra” que carecen de transparencia en sus procesos de toma de decisiones.

l. Responsabilidad y gestión de riesgos.

- Definir la responsabilidad por daños relacionados con la IA en los contratos con clientes y proveedores.
- Contratar un seguro adecuado para cubrir los riesgos potenciales asociados al despliegue de la IA.

m. Consentimiento para el uso de la IA.

- Obtener el consentimiento informado al desplegar herramientas de IA que afecten directamente a los usuarios, como los *chatbots* o los sistemas de recomendación.
- Informar claramente a los clientes de sus derechos, incluida la posibilidad de excluirse de las interacciones con la IA.

5. LINEAMIENTOS INTERNOS PARA EL USO DE LA IA:

1. **Responsabilidad Final:** Nativo es el máximo responsable de todas las decisiones tomadas con el apoyo de la IA.

2. **Autoridad Humana:** Los humanos deben permanecer como los últimos responsables de todas las decisiones y acciones, incluidas las realizadas/sugeridas por la IA.

3. **Función de la IA:** Las herramientas de IA deben ser utilizadas únicamente para potencializar los servicios y optimizar las horas de trabajo, y no como un sustituto de la creatividad, el conocimiento y la experiencia humana.

4. **Supervisión:** Todos los diseños, servicios y resultados presentados por Nativo deben ser creados y supervisados por humanos.

5. **Ampliación Creativa:** Las herramientas de IA deben ser vistas como un impulsor de la transformación creativa en la publicidad, que permitan a Nativo explorar nuevas fronteras creativas y responder a las necesidades de los clientes con soluciones innovadoras.

6. **Optimización y Calidad de Vida:** Nativo promoverá el uso de nuevas herramientas de IA que ayuden a mejorar la calidad del trabajo y, con ello, la calidad de vida y la optimización de tiempo del equipo de trabajo.

7. **Resultados Únicos:** Todos nuestros servicios son supervisados y aprobados por diferentes áreas y con el empleo de múltiples herramientas, lo que nos permite presentar resultados únicos, innovadores y creativos

8. **Mantenimiento del Estatus:** El uso de IA en Nativo se limita a tareas de procedimiento delimitadas, a la mejora de actividades humanas previamente realizadas, o a la detección de patrones de toma de decisiones sin influir sustancialmente en el resultado final.

9. **Evaluación de Impacto:** En caso de que Nativo, o alguno de sus Proveedores, decidan modificar la finalidad prevista de un sistema de IA de uso general de manera que se considere un sistema de alto riesgo, se deberá realizar inmediatamente una nueva evaluación de la conformidad y un análisis de impacto de derechos fundamentales.

6. COMPETENCIA, FORMACIÓN Y ALFABETIZACIÓN EN IA

1. **Capacitación:** Nativo establecerá un programa de capacitación periódica y especializada en las capacidades, limitaciones, riesgos éticos y requisitos legales de los sistemas de IA utilizados para todos sus Trabajadores.

2. **Conocimiento de Riesgos:** Los Trabajadores y Proveedores de Nativo deben entender la correcta aplicación de los elementos técnicos, las medidas que deben aplicarse durante el uso, las formas adecuadas de interpretar los resultados de salida del sistema de IA, y estar conscientes de los posibles perjuicios físicos, psíquicos, sociales o económicos que puede generar la IA.

7. TRANSPARENCIA Y PROPIEDAD INTELECTUAL (PI)

1. **Información del Proceso:** Se informará a los clientes con toda claridad en qué momento del proceso se hace uso de herramientas de IA y cuál es el propósito de su empleo para cada caso específico.

2. **Identificación de Material:** Todo el material, la Información y las creaciones obtenidas mediante IA serán plenamente identificados y se harán del conocimiento del cliente.

3. **Autorización de Uso:** Previo a su empleo, se solicitará la autorización por parte del cliente para hacer uso de herramientas de IA en la creación de contenido.

4. **Trazabilidad de Contenido Generativo:** Cuando los sistemas de IA generen contenido sintético (audio, imagen, video o texto que pueda constituir una ultra suplantación o *deepfake*), Nativo deberá asegurar que los resultados de salida estén marcados en un formato legible por máquina (metadatos o marcas de agua) de forma que sea posible detectar que han sido generados o manipulados de manera artificial. Esta solución técnica deberá ser, en la medida de lo técnicamente viable, eficaz, interoperable, robusta y fiable.

5. **Adopción de IA:** Nativo adoptará las posibilidades de la IA generativa para la creación de contenido (textos, gráficos, logotipos, audio, etc.), asegurando que todas las partes interesadas estén debidamente informadas.

6. **Publicidad:** La divulgación de trabajos obtenidos por medio de IA no se hará pública, salvo en los casos en los que se acuerde expresamente lo contrario con el cliente.

7. **Diligencia en la Información:** Nativo se compromete a asegurar que todas las partes interesadas estén debidamente informadas sobre el uso de tecnologías de IA en los procesos creativos.

8. DEBIDA DILIGENCIA EN LA CADENA DE SUMINISTRO Y DERECHOS DE AUTOR

1. **Diligencia en Modelos de IA de Uso General:** Nativo, al adquirir o integrar modelos de IA de uso general (GPAI) que puedan formar parte de un sistema de IA, revisara, solicitará y conservará la documentación técnica y la información relevante del proveedor del modelo para entender sus capacidades y limitaciones.

2. **Reserva de Derechos (Opt-Out):** Nativo incluirá en los acuerdos contractuales con los Proveedores de IA que utilizan técnicas de prospección de textos y datos (Text and Data Mining), cláusulas que aseguren la transparencia y el cumplimiento de las obligaciones de derechos de autor. Nativo exigirá que el proveedor de IA cumpla con la obligación de identificar y respetar la reserva de derechos (opt-out) expresada por los titulares de derechos, de conformidad con las mejores prácticas internacionales en PI.

9. VERIFICACIÓN DE LA INFORMACIÓN

1. **Revisión Obligatoria:** Toda la información y los resultados obtenidos con ayuda de la IA deben ser revisados y confirmados por algún trabajador de Nativo de forma minuciosa, previo a su presentación al cliente, para garantizar que sean certeros, confiables y demostrables.

2. **Autenticidad:** Nativo se compromete a trabajar en contra de la desinformación, asegurando la autenticidad y precisión de todos sus contenidos.

3. **Sinceridad:** Los Trabajadores y Proveedores se comprometen a conducirse de manera sincera, no permitiendo mentir, modificar datos o alterarlos, bajo ningún motivo.

4. **Promoción Positiva:** Nativo se compromete a utilizar el lenguaje, imágenes y videos para educar, influir y promover un cambio positivo.

10. LINEAMIENTOS DE CONDUCTA Y COMPLIANCE

1. Legalidad: Queda estrictamente prohibido realizar o propiciar actividades que contravengan el espíritu de la Ley.
2. Software: No se utilizarán programas o archivos piratas o que no hayan sido previamente autorizados por Nativo.
3. Integridad Documental: Queda prohibido alterar, destruir u ocultar Información que pueda afectar a Nativo, sus Clientes o Proveedores.
4. Proveedores: Nativo únicamente trabajará con proveedores de herramientas de IA que se encuentren en cumplimiento de toda la normatividad aplicable a su uso.
5. Revisión Periódica: Nativo periódicamente realiza revisiones a todos los procesos, haciendo énfasis en aquellos en los que hacemos uso de herramientas de Inteligencia Artificial, para poder identificar los riesgos que puedan llegar a existir en cada proceso.
6. Alineación Ética: Cada decisión tomada con el apoyo de la IA deberá estar alineada con los más altos estándares éticos y profesionales.

11. SISTEMA DE GESTIÓN DE RIESGOS Y CALIDAD (SGC)

1. Formalización del SGC: Nativo establecerá, implementará y documentará un Sistema de Gestión de la Calidad (SGC) formal, que asegure el cumplimiento continuo con la presente Política y los más altos estándares éticos, siendo este un proceso iterativo continuo planificado y ejecutado durante todo el ciclo de vida del uso de la IA.
2. Proceso Iterativo: El SGC incluirá la determinación y el análisis de los riesgos conocidos y previsibles, así como la adopción de medidas adecuadas y específicas de gestión de riesgos para hacer frente a los riesgos detectados, teniendo en cuenta la finalidad prevista y el uso indebido razonablemente previsible del sistema de IA.

12. PROTECCIÓN DE LA INFORMACIÓN CONFIDENCIAL Y PERSONAL

1. Restricción de Uso: Se prohíbe incluir información confidencial y/o información personal de los clientes en las herramientas de IA.
2. Excepción con Consentimiento: Solo se permitirá incluir información confidencial y/o personal en herramientas de IA cuando se cuente con la autorización previa y por escrito del cliente.
3. Anonimización Obligatoria: Toda información confidencial que deba ser utilizada en herramientas de IA deberá pasar previamente por un proceso de Anonimización.

4. Confidencialidad: Los Trabajadores y Proveedores tienen la obligación de no divulgar información que pueda ser considerada como confidencial o restringida.

5. Estándares y Técnicas de Anonimización para Robustez Legal: Para asegurar la robustez del proceso de Anonimización y el cumplimiento estricto con la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), Nativo implementará las siguientes medidas técnicas para desvincular la Información de cualquier titular identificado o identificable:

6. Supresión de Identificadores Directos: Eliminación de datos que identifiquen de forma única al individuo (ej. nombres, correos, números de identificación).

7. Generalización y Agregación: Reducción de la precisión de los datos (ej. sustitución de fechas exactas por rangos, agrupación de ubicaciones por región) para crear conjuntos de información amplios y evitar la re-identificación.

8. Verificación de Riesgo de Re-identificación: Nativo realizará pruebas internas de riesgo de re-identificación de forma periódica. Este proceso tiene como objetivo asegurar que la Información Confidencial anonimizada, incluso al ser cotejada con otras fuentes de información, no pueda ser vinculada a una persona determinada o determinable.

9. Gestión de la Privacidad desde el Diseño: Se garantiza que los sistemas de IA se desarrollen y utilicen de conformidad con normas en materia de protección de la intimidad y de los datos, aplicando los principios de minimización de datos y de protección de datos desde el diseño.

13. INCLUSIÓN Y NO DISCRIMINACIÓN

1. Mandato de No Discriminación: Nativo actuará de forma decidida contra cualquier forma de discriminación conforme a lo establecido en el artículo Primero de la Constitución Política de los Estados Unidos Mexicanos.

2. Mitigación de Sesgos: Se realizarán esfuerzos continuos para evitar y mitigar los sesgos en los sistemas de IA.

3. Verificación de Resultados: Se verifican las respuestas brindadas por la IA, asegurando que cumplan respetuosamente con los estándares de exclusividad y diversidad en México.

4. Audiencias: Se buscará presentar a los clientes resultados que atiendan a una amplia gama de audiencias y necesidades, respetando la riqueza de la experiencia humana.

5. *Prompts* Libres de Prejuicios: Los Trabajadores y Proveedores se esforzarán por evitar y mitigar los sesgos en los sistemas de IA, asegurándose de que los *prompts* sean inclusivos y libres de prejuicios.

6. Verificación de Resultados Culturales: Se verifican activamente las respuestas brindadas por la IA, asegurando que cumplan con los estándares de exclusividad y diversidad en México.

7. Representación Amplia: Nativo buscará presentar a los clientes resultados que atiendan a una amplia gama de audiencias y necesidades, reflejando y respetando la riqueza de la experiencia humana.

14. ANÁLISIS DE RIESGOS Y CONTROL DE CALIDAD

1. Nativo realizará permanentemente controles de seguridad y revisiones periódicas a los procesos que utilizan IA, con el fin de identificar posibles riesgos en materia de seguridad, integridad y confiabilidad de la Información, e implementar medidas para mitigarlos.

2. El área de control de calidad supervisará que el trabajo final que se comparte con el Cliente se encuentre íntegro y sea confiable.

3. Los Trabajadores deben informar al Comité de Ética, de forma inmediata, cualquier incumplimiento a esta Política por otros trabajadores y/o los Proveedores.

Proceso de Corrección y Mitigación de Sesgos

1. Detección Humana: El Trabajador y/o Proveedor que utiliza la herramienta de IA debe verificar las respuestas brindadas por la IA para asegurar que cumplen con los estándares de exclusividad y diversidad.
2. Si identifica un contenido (texto, imagen, video, dato) que sea discriminatorio, sesgado, o que contravenga lo establecido en el artículo Primero de la Constitución Política de los Estados Unidos Mexicanos o el Código de Ética de Nativo, el resultado se clasifica como "No Apto para Cliente".
3. El Trabajador deberá, de manera inmediata, revisar el *prompt* utilizado y la herramienta de IA específica que lo generó.
    a. La revisión del *prompt* debe asegurar que las instrucciones iniciales sean inclusivas y libres de prejuicios.
    b. El contenido sesgado debe ser eliminado o modificado por el equipo humano (Corrección Ética) y pasar por una revisión adicional para garantizar que el sesgo ha sido completamente mitigado antes del uso del contenido generado.
4. El tratamiento de categorías especiales de datos personales (sensibles) para detectar y corregir sesgos solo se permite en la medida en que sea estrictamente necesario y tras aplicar garantías adecuadas, quedando prohibida su transmisión a terceros y debiendo ser eliminados una vez corregido el sesgo.

5. El contenido discriminatorio o sesgado debe ser eliminado o modificado por el equipo humano para alinearse con el compromiso de Nativo de actuar contra cualquier forma de discriminación. Este proceso se fundamenta en la visión humana y la integridad y confiabilidad de la información.
6. El Trabajador y/o Proveedor utilizará el *prompt* revisado y éticamente corregido para re-generar el contenido, buscando presentar resultados que atiendan a una amplia gama de audiencias y necesidades, reflejando y respetando la riqueza de la experiencia humana.

Registro de Incidencias

1. Todos los incidentes, la causa raíz identificada y las acciones correctivas tomadas se registrarán para futuras revisiones a todos los procesos.
2. Los resultados de este análisis serán utilizados para actualizar la capacitación de los Trabajadores en la formulación de *prompts* inclusivos y en la detección de sesgos, como parte del compromiso de Nativo de usar la IA para empoderar a las personas.
3. La información recopilada informará el Análisis de Riesgos que Nativo realiza permanentemente, permitiendo la implementación de medidas preventivas más sólidas para futuros usos de la IA.

4. SANCIONES.

Los Trabajadores y/o Proveedores que se determine que han violado esta Política podrán sujetarse a las medidas disciplinarias que para tal efecto determine Nativo. Éstas incluyen, mas no se limitan a: reprimendas verbales o por escrito (actas Administrativas), suspensión, reasignación, relevo del cargo y/o terminación de la relación laboral, conforme a lo establecido en el Reglamento Interior de Trabajo conforme a su gravedad:

Faltas Graves (Sujetas a Sanción Inmediata)

Se consideran faltas graves aquellas que **violentan un principio legal o de derechos fundamentales**, o que exponen a Nativo a riesgos de Privacidad y Legalidad o de Propiedad Intelectual (PI). Son consideradas faltas graves, entre otras:

1. **Violación de la Privacidad de Datos:** Incluir información confidencial y/o información personal de los Clientes en los *prompts* o en cualquier herramienta de IA sin la autorización previa y por escrito del cliente.
2. **Omisión de Anonimización Obligatoria:** Utilizar información confidencial, incluso con consentimiento, sin haber realizado el proceso de Anonimización obligatoria, exponiendo datos sensibles a riesgos de reidentificación.
3. **Fraude y Desinformación (Sinceridad):** Alterar, destruir u ocultar Información que pueda afectar a Nativo, sus clientes o Proveedores. También se incluye el incumplimiento del compromiso de sinceridad, el cual prohíbe mentir, modificar o alterar datos, así como el uso de técnicas subliminales o deliberadamente manipuladoras con el objetivo de alterar el comportamiento de manera sustancial.

4. **Incumplimiento de PI Grave:** Infringir los derechos de Propiedad Intelectual de los clientes o utilizar *software* o archivos piratas o no autorizados.
5. **Violación del Mandato de No Discriminación:** La omisión deliberada de aplicar el proceso de corrección y mitigación de sesgos ante la detección de un resultado discriminatorio o sesgado.
6. **Ausencia de Trazabilidad Digital:** La omisión intencional de marcar en un formato legible por máquina (metadatos o marcas de agua) el contenido sintético generado por IA (como un *deepfake* o *ultrasuplantación*).

Faltas Menores o Repetidas (Sujetas a Proceso Correctivo)

Se consideran faltas menores aquellas que no implican un riesgo inmediato de daño legal o reputacional, pero que demuestran negligencia en los procesos operativos.

1. **Omisión de la Revisión Obligatoria:** Fallar en la revisión y confirmación minuciosa de la Información y los resultados obtenidos con ayuda de la IA, siempre y cuando esto no resulte en una "Alucinación" o resultado sesgado presentado al cliente.
2. **Uso de *Prompts* No Inclusivos:** Fallar recurrentemente en el uso de *prompts* inclusivos y libres de prejuicios.

Procedimiento de Aplicación y Recurso

1. El Trabajador o tercero que detecte un incumplimiento debe reportarlo de forma inmediata, por escrito al Comité de Ética.
2. El Comité de Ética iniciará una Auditoría interna para analizar la causa raíz del incidente.
3. Se notificará al Trabajador/Proveedor sobre el incumplimiento detectado, otorgándole un plazo razonable para presentar su defensa y las pruebas que considere pertinentes.
4. Con base en la investigación y el derecho de audiencia, el Comité de Ética emitirá una resolución y, de ser necesario, procederá a la aplicación de la sanción correspondiente, notificando formalmente al Trabajador/Proveedor, la cual puede ser inclusive la terminación de la relación laboral o contractual, según corresponda.

5. DOCUMENTO RELACIONADOS.

- Reglamento Interior de Trabajo.
- Código de Ética en el uso de inteligencia artificial

6. MODIFICACIONES.

Esta política podrá ser modificada en cualquier momento; cualquier cambio o modificación será comunicado de forma oportuna.

7. CONTROL DE CAMBIOS.

VERSIÓN NO.	ELABORADO	REVISADO	APROBADO	FECHA DE APROBACIÓN	MODIFICACIÓN REALIZADA
01	Adda Lizbeth Solis Huerta	Jennifer Córdoba	*****		* Creación

MAPA DE RIESGOS EN EL USO DE LA INTELIGENCIA ARTIFICIAL

Categoría de Riesgo	Riesgos Potenciales (Amenazas)	Estrategias de Mitigación
Transformación Económica y Social	La existencia de normas nacionales divergentes puede fragmentar el mercado y reducir la seguridad jurídica.	• Nativo trabaja bajo lineamientos de conducta para evitar actividades que contravengan la ley. • El objetivo de la política es establecer un marco jurídico uniforme para el desarrollo de contenido basado en IA.
Optimización y Creatividad	Riesgo de pérdida de autonomía personal si el control humano es insuficiente.	• Los humanos deben permanecer como los últimos responsables de todas las decisiones y acciones. • La IA se utiliza únicamente para potencializar los servicios y no como un sustituto de la creatividad y el conocimiento humano.
Sesgo y Discriminación	Los datos utilizados para el entrenamiento, la validación y la prueba deben ser relevantes y suficientemente representativos, y estar en la mayor medida posible, libres de errores.	• Se prohíben las prácticas que van en contra de la no discriminación y el respeto de la dignidad humana. • Se aplica el Proceso de Corrección y Mitigación de Sesgos si la revisión humana detecta un sesgo o resultado discriminatorio. • Revisión Obligatoria de los resultados para asegurar que cumplen con la diversidad en México.
Manipulación Subliminal	Sistemas de IA con el objetivo de alterar de manera sustancial el comportamiento, mermando la capacidad de tomar una decisión informada y provocando perjuicios considerables.	• Las prácticas de IA que se sirvan de técnicas subliminales o deliberadamente manipuladoras con el objetivo de alterar el comportamiento de manera sustancial quedan prohibidas. • Nativo se compromete a conducirse con sinceridad, no permitiendo mentir o alterar datos.
Explotación de Vulnerabilidades	Explotación de vulnerabilidades de personas físicas o colectivos (edad, discapacidad, situación socioeconómica) para alterar su comportamiento y provocar perjuicios considerables.	• Nativo se compromete a realizar esfuerzos continuos para evaluar y prevenir los perjuicios de los sistemas de IA para las personas vulnerables o los colectivos de personas vulnerables.
Contenido Generativo No Identificado	Contenido sintético difícil de distinguir del auténtico, creando riesgos de desinformación y suplantación de identidad.	• Todo material generado por la IA debe ser plenamente identificado y hecho del conocimiento del Cliente. • Se exige que los resultados de salida estén marcados en un formato legible por máquina.
Infracción de Derechos de Autor	El desarrollo y entrenamiento de modelos IA requiere acceder a grandes cantidades de datos que pueden estar protegidos por derechos de autor.	• Se requiere la autorización previa del Cliente para usar IA en la creación de Contenido. • Nativo debe exigir a sus proveedores un resumen suficientemente detallado del contenido utilizado para el entrenamiento.
Precisión y Solidez Técnica	Un sistema de IA que no está entrenado con datos de buena calidad o que no cumple los requisitos de precisión y solidez puede dar lugar a resultados sesgados, incorrectos o injustos.	• Los sistemas de IA utilizados por Nativo deben alcanzar un nivel adecuado de precisión, solidez y ciberseguridad y funcionar de manera uniforme. • Se utilizarán soluciones de redundancia técnica (copias de seguridad o planes de prevención contra fallos).
Ciberseguridad	La IA puede ser vulnerable a ataques dirigidos a conjuntos de datos de entrenamiento (envenenamiento de datos) o modelos entrenados (ataques adversarios).	• Los sistemas de IA de alto riesgo deben ser resistentes a los intentos de terceros no autorizados de alterar su funcionamiento. • Se exige la adopción de medidas técnicas y organizativas adecuadas, como controles de seguridad.
Violación de la Privacidad de Datos	El diseño, desarrollo o uso de sistemas de IA puede implicar el tratamiento de datos personales, lo que conlleva riesgos de violación de la intimidad.	• Se aplica la gestión de la privacidad y de los datos. • Se prohíbe incluir Información Confidencial y/o Personal de los Clientes sin consentimiento. • Anonimización Obligatoria de Información Confidencial antes de su uso.
Riesgo de Uso Indebido	El uso indebido razonablemente previsible puede generar riesgos si no se mitigan adecuadamente.	• El sistema de gestión de riesgos debe ser un proceso iterativo continuo que se planifica y ejecuta durante todo el ciclo de vida del sistema de IA, revisándose periódicamente. • La gestión de riesgos debe tener en cuenta el uso indebido razonablemente previsible.