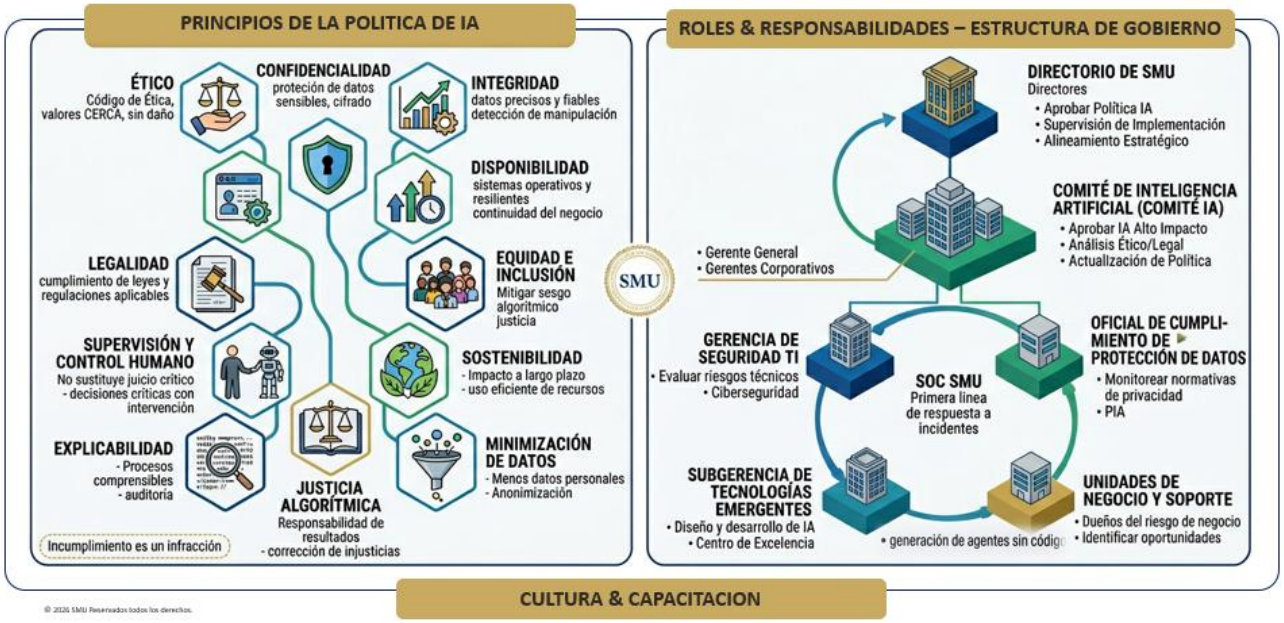
POLÍTICA CORPORATIVA DE INTELIGENCIA ARTIFICIAL

I. MARCO GENERAL DE INTELIGENCIA ARTIFICIAL EN SMU

A continuación, se presenta un diagrama que resume de manera integral el marco general de gobernanza, principios, riesgos y uso de la Inteligencia Artificial en SMU.

Este esquema tiene por finalidad entregar una visión ejecutiva e introductoria de los elementos clave que conforman la presente política, facilitando su comprensión y aplicación por parte de los distintos actores de la Compañía.



II. OBJETIVO

Establecer un marco institucional robusto que establezca los lineamientos estratégicos de ética, gobernanza y seguridad para el desarrollo, adquisición, despliegue y uso de tecnologías de Inteligencia Artificial (IA) en SMU S.A. y sus filiales (en adelante, para todos los efectos, "SMU" o la "Compañía").

Esta política promueve que la innovación impulsada por la IA se alinee con los valores corporativos, la estrategia de negocio y el marco legal vigente en Chile y en todos los países donde opere SMU, con tres fines principales:

- Contribuir a la generación de valor para la compañía, impulsando la eficiencia operativa, la personalización de la oferta y la competitividad, así como el desarrollo de nuevas capacidades que respalden los objetivos estratégicos presentes y futuros.
- Gestionar y mitigar los riesgos asociados a la IA, mediante la identificación, evaluación y mitigación de amenazas de seguridad (ej. ataques adversariales), brechas de datos, sesgos en la toma de decisiones, "alucinaciones" de los modelos y potenciales impactos reputacionales, económicos, legales u otros.

- Contribuir a la confianza de clientes, colaboradores, proveedores, inversionistas, reguladores y demás partes interesadas, mediante la promoción de un uso responsable, transparente y ético de la IA.

III. ALCANCE

Esta política rige el uso de todos los sistemas, plataformas, algoritmos, modelos y activos de información vinculados a la Inteligencia Artificial (IA) definidos por la Compañía. Incluye los datos para su entrenamiento, operación o mejora y comprende su ciclo de vida completo: diseño, desarrollo, entrenamiento, implementación, operación, monitoreo y retiro.

Para mitigar riesgos como la exposición de información confidencial, el tratamiento inadecuado de datos y la generación de contenido no fiable, se establece que, directores, ejecutivos y trabajadores de la Compañía deberán utilizar única y exclusivamente las herramientas y plataformas de Inteligencia Artificial que la Compañía haya autorizado previamente para el desempeño de sus funciones. Esta directriz es de carácter obligatorio para toda tecnología de IA, ya sea desarrollada internamente, adquirida a terceros o utilizada mediante servicios de software (SaaS).

IV. DEFINICIONES

Para asegurar un entendimiento común de los términos utilizados en esta política se establecen las siguientes definiciones:

- Inteligencia Artificial (IA): Conjunto de tecnologías, sistemas y métodos computacionales capaces de realizar tareas que normalmente requieren inteligencia humana, como razonamiento, aprendizaje, percepción, toma de decisiones e interacción con el entorno. Incluye, entre otros, el Aprendizaje Automático (Machine Learning), el procesamiento del lenguaje natural, la visión por computador, las bases de conocimiento y el reconocimiento visual.
- Sistema(s) de IA: Sistema basado en IA que, para un conjunto de objetivos definidos por humanos, infiere resultados tales como predicciones, recomendaciones o decisiones que pueden influir en entornos físicos o virtuales.
- IA Generativa: Tipo de Inteligencia Artificial capaz de crear contenido nuevo y original, como texto, imágenes, audio o código, a partir de los patrones y estructuras aprendidas de grandes volúmenes de datos.
- Datos Personales: Información que permite identificar o hacer identificable a una persona natural (ej. nombre, RUT, correo electrónico, dirección, dirección IP, datos biométricos, etc.).
- Datos Sensibles: Subcategoría de datos personales que incluye información sobre salud, religión, origen racial o étnico, opiniones políticas, orientación sexual, entre otros, y que requieren una protección especial.
- Anonimización: Proceso de transformar datos personales de tal manera que el titular de los datos ya no pueda ser identificado o sea irreversiblemente imposible de re-identificar, sin utilizar recursos desproporcionados.
- PIA (Privacy Impact Assessment): Evaluación de Impacto en la Privacidad. Es un proceso sistemático para identificar y evaluar los riesgos que un proyecto, sistema o tecnología puede representar para la privacidad de las personas.
- Alucinación (Hallucination): Resultado o información generada por un sistema de IA (particularmente IA Generativa) que aparenta ser correcto y fáctico, pero que en

realidad carece de fundamento real, es inventado o es inconsistente con la información de origen, pudiendo inducir a error o desinformación.

- Sesgo Algorítmico (Bias): Una tendencia sistemática, injusta o discriminatoria en los resultados de un sistema de IA, que puede surgir de sesgos en los datos de entrenamiento, en el diseño del algoritmo o en la forma en que se utiliza el sistema, afectando negativamente a ciertos grupos o individuos.
- Ataque Adversarial: Una técnica maliciosa que consiste en realizar pequeñas y a menudo imperceptibles modificaciones en los datos de entrada de un sistema de IA con el objetivo de engañarlo y provocar que clasifique incorrectamente una información, genere un resultado erróneo o se comporte de manera inesperada.
- Shadow AI: Se refiere al uso no autorizado, no supervisado o informal de herramientas, sistemas o servicios de Inteligencia Artificial dentro de una organización por parte de sus colaboradores, sin la aprobación, control o visibilidad de las áreas responsables, lo que puede generar riesgos significativos de seguridad, cumplimiento y uso indebido de información.
- Toma de Decisiones Automatizada: Proceso en el cual un sistema de IA llega a una conclusión o ejecuta una acción que tiene un impacto significativo, sin intervención humana directa en la validación o autorización de esa decisión específica.
- RPA (Robotic Process Automation): Tecnología que utiliza robots de software (bots) para automatizar tareas digitales repetitivas y basadas en reglas, imitando la interacción humana con sistemas y aplicaciones de software para ejecutar procesos de negocio.
- Deepfake: Contenido multimedia sintético (video, audio o imagen) que ha sido manipulado y generado mediante técnicas de IA, a menudo con el objetivo de suplantar la apariencia o la voz de una persona, haciendo que parezca que dice o hace algo que en realidad nunca hizo.
- SOC (Security Operation Center SMU) Equipo de Respuesta ante Incidentes de Seguridad Informática de SMU, responsable de coordinar la detección, análisis, contención, erradicación y recuperación de incidentes de ciberseguridad, incluyendo aquellos que afecten a sistemas de IA.
- Decisión Crítica: Decisión, asistida o automatizada por IA, que tiene un impacto significativo y directo sobre los derechos, oportunidades o seguridad de clientes o colaboradores, o sobre la estabilidad financiera, reputacional u operacional de SMU.
- Evaluar Críticamente: Obligación de todo usuario de IA de no aceptar ciegamente sus resultados. Implica usar el juicio profesional, verificar la coherencia y lógica del resultado, contrastarlo con otras fuentes si es necesario, y cuestionarlo si parece ilógico, incorrecto, sesgado o potencialmente una "alucinación".

V. MARCO NORMATIVO REFERENCIAL

Esta política se alinea con la legislación y normativa vigente en la República de Chile y políticas internas y estándares éticos definidos por la Compañía, tales como:

- Ley 19.628 sobre protección de la vida privada
- Ley 21.459 de delitos informáticos
- Ley 21.719 sobre protección de datos personales
- Ley 21.663 de Ciberseguridad
- Ley 19.496 sobre protección de los derechos de los consumidores
- Política Corporativa de Gestión de Riesgos
- Política de Protección de Datos Personales
- Política General de Seguridad de la Información

VI. POLÍTICA

1. PRINCIPIOS DE LA INTELIGENCIA ARTIFICIAL EN SMU

El desarrollo, adopción, despliegue y uso de tecnologías de Inteligencia Artificial (IA) en SMU, estará basado en los siguientes principios rectores. El incumplimiento de cualquiera de ellos es una infracción a esta política y podrá dar lugar a las medidas disciplinarias correspondientes.

Principio	Descripción y Aplicación en SMU
Ético	La IA se desarrollará y utilizará siempre en consonancia con el Código de Ética y Conducta de Negocios de SMU y los valores CERCA. Se prohíbe el uso de IA para fines que puedan dañar la dignidad humana, la privacidad, la seguridad, la libertad, o que promuevan algún tipo de violencia, la discriminación o la desinformación. Toda aplicación de IA debe contribuir positivamente al negocio y los objetivos definidos por SMU.
Confidencialidad	Se implementarán medidas para la protección de la información sensible y confidencial de SMU y de sus clientes, proveedores y personas trabajadoras, tanto en los datos de entrada como en los modelos y resultados generados por la IA. Se implementarán controles de acceso estrictos y cifrado de datos en todo el ciclo de vida de la IA para prevenir accesos no autorizados y filtraciones.
Integridad	Los datos utilizados para entrenar y operar los sistemas de IA, así como los modelos de IA y sus resultados, deben ser precisos, completos y fiables. Se implementarán mecanismos para detectar y prevenir la manipulación (ej. Ataques Adversariales) o alteración no autorizada de datos y modelos, asegurando la robustez y confiabilidad de los sistemas de IA.
Disponibilidad	Los sistemas de IA críticos y la infraestructura subyacente deben estar disponibles y operativos cuando sean requeridos por las operaciones de SMU. Se implementarán planes de continuidad del negocio y recuperación ante desastres para garantizar la resiliencia de los servicios de IA frente a fallos técnicos o ataques.
Legalidad	Todo uso de IA en SMU debe cumplir estrictamente con todas las leyes, regulaciones y normativas aplicables en las jurisdicciones donde opera la Compañía, incluyendo la legislación sobre protección de datos personales, derechos del consumidor y ciberseguridad. La política se adaptará a los futuros marcos regulatorios sobre IA.
Equidad e Inclusión	Se buscará activamente identificar, medir y mitigar el Sesgo Algorítmico en los datos de entrenamiento y en los modelos de IA, para asegurar que los sistemas operen de manera justa y equitativa, sin perpetuar ni amplificar la discriminación o exclusión de ningún grupo de personas. Se promoverá la diversidad en los equipos de desarrollo de IA.

Supervisión y Control Humano	La IA debe ser una herramienta para potenciar las capacidades humanas, no para sustituir el juicio crítico. Las Decisiones Críticas tomadas por sistemas de IA siempre requerirán un nivel de supervisión y control humano significativo y proporcional al riesgo, con la posibilidad de intervención y reversión.
Sostenibilidad	Se evaluará el impacto a largo plazo de la IA en la organización, en la sociedad y en el medio ambiente. Se promoverá el uso eficiente de los recursos computacionales y energéticos, y se considerará la viabilidad económica y el retorno de la inversión de las iniciativas de IA para asegurar su crecimiento orgánico y sostenido.
Explicabilidad	Para los sistemas de IA de Riesgo de Medio Impacto y Riesgo de Alto Impacto, especialmente aquellos que influyen en Decisiones Críticas, se buscará que sus procesos y resultados sean comprensibles para los supervisores humanos. Esto implica poder entender por qué un sistema de IA llegó a una conclusión o recomendación específica, facilitando la auditoría y la rendición de cuentas.
Justicia Algorítmica	Este principio complementa la Equidad, enfocándose en la responsabilidad sobre los resultados de la IA. Implica que SMU se compromete a investigar y corregir activamente cualquier resultado injusto o discriminatorio derivado del uso de sus Sistemas de IA, y a establecer mecanismos claros para la rendición de cuentas y la reparación cuando sea necesario.
Minimización de Datos	Los Sistemas de IA deben diseñarse y operarse utilizando la menor cantidad posible de datos personales. Se priorizará la Anonimización o seudonimización de los datos cuando sea factible y se limitará el acceso a la información estrictamente necesaria para el propósito definido, reduciendo así los riesgos de privacidad.

2. ROLES Y RESPONSABILIDADES

Para la adecuada implementación, supervisión y ejecución de esta política, se establece una estructura de gobernanza clara, con roles y responsabilidades definidos que permiten una gestión coherente y efectiva en todos los niveles de la organización, desde la definición de la estrategia hasta la operación diaria, según se detalla a continuación:

Rol	Integrantes / Responsables	Funciones Clave
Directorio de SMU	Directores	- Aprobar la Política de Inteligencia Artificial de SMU y supervisar su implementación, asegurando que el uso de la IA se mantenga alineado con la estrategia corporativa, la gestión de riesgos y las obligaciones legales y éticas de la Compañía.
Comité de Inteligencia Artificial (Comité IA)	Gerente General SMU, Gerentes Corporativos de Tecnología y Digital, Fiscalía y Asuntos Externos, Personas y Sostenibilidad, Operaciones y	- Aprobar el desarrollo y/o adquisición y uso de IA de Alto Impacto, sujeto a la política de aprobación de inversiones de SMU. - Analizar implicancias éticas, sociales, legales y reputacionales de nuevos desarrollos. - Proponer

	Ventas, Administración y Finanzas, Inmobiliaria, Ecommerce, Marketing y Clientes, Marcas Propias y Nuevos Negocios, Gerente General de Unicard, Gerente General SMU Perú, Gerente de Seguridad de la Información, y el Oficial de Cumplimiento de Protección de Datos.	actualizaciones periódicas a esta política. - Coordinar con otras áreas de la compañía como el Comité de Ética y Cumplimiento materias relacionadas a IA. - Coordinar con la Encargada de Prevención de Delitos de SMU, la identificación y mitigación de riesgos penales asociados al uso de Sistemas de IA. – Reportar, a lo menos trimestralmente, al Comité de Auditoría y Riesgos el estado del uso de la Inteligencia Artificial en la Compañía, incluyendo los principales riesgos, los sistemas de mayor impacto, los incidentes relevantes, el cumplimiento normativo, los resultados de auditoría y los cambios o riesgos emergentes.
Gerencia de Seguridad TI	Lidera la estrategia de ciberseguridad, incluyendo la seguridad de Sistemas de IA.	- Evaluar y monitorear los riesgos técnicos asociados a modelos de IA, incluyendo IA Generativa, Alucinaciones, Ataques Adversariales y Sesgos Algorítmicos. -Dar cuenta al Comité IA de los hallazgos de sus evaluaciones y monitoreos. - Coordinar con el SOC SMU en caso de incidentes críticos relacionados con IA. - Asegurar el cumplimiento de los principios de seguridad de esta política. - Integrar controles de seguridad en todo el ciclo de vida del sistema de IA.
SOC (Security Operation Center SMU)	Equipo de Respuesta a Incidentes de Seguridad Informática de SMU.	- Actuar como primera línea de respuesta y coordinación ante incidentes de ciberseguridad que afecten a Sistemas de IA, garantizando una contención, erradicación y recuperación efectivas y rápidas.
Subgerencia de Tecnologías Emergentes	Área responsable del desarrollo e implementación de IA.	- Proponer, diseñar y desarrollar soluciones de IA alineadas a la estrategia de la compañía. - Asegurar que los desarrollos cumplan con los principios y controles de esta política desde la fase de concepción (Security & Privacy by Design). - Actuar como el centro de excelencia técnica en IA para la organización, explorando nuevas capacidades y usos responsables.
Oficial de Cumplimiento de Protección de Datos	Gerente de Cumplimiento de SMU.	- Monitorear que los Sistemas de IA que traten, procesan o usen datos personales cumplan con las normativas legales vigentes de privacidad y derechos de los titulares, y en general con cualquier normativa que regle esta materia. - Participar activamente en la evaluación de impacto (PIA) de todos los Sistemas de IA que involucren datos personales o sensibles.

Unidades de Negocio y Soporte	Gerentes y usuarios de las distintas áreas de SMU.	- Identificar oportunidades de uso de IA en sus respectivos procesos y áreas. - Ser los dueños del riesgo asociado al proceso de negocio donde se implementa la IA. - Evaluar Críticamente los resultados generados por los sistemas de IA y reportar cualquier anomalía.

3. RIESGOS DE LA IA Y MARCO DE USO

a. CLASIFICACIÓN DE RIESGO SEGÚN ALCANCE DE LA IA

La evaluación de todo riesgo asociado a un Sistema de IA se regirá íntegramente por la metodología y las herramientas definidas en la Política de Gestión del Riesgo de SMU. Esto asegura un enfoque unificado para la identificación, evaluación y tratamiento de todos los riesgos de la Compañía. Las dimensiones de impacto a considerar (Continuidad, Financiero, Reputacional, Cumplimiento, etc.) serán siempre las establecidas en dicho marco general.

Los siguientes criterios de riesgo específicos para la IA dan una guía complementaria al marco de la Política de Gestión de Riesgos, sirviendo, así como una orientación de casos de uso y su evaluación de riesgo.

- Riesgo Bajo: Se considera de Riesgo Bajo a aquel cuya materialización, incluso considerando los controles existentes, tendría un impacto mínimo o insignificante en la operación, las finanzas o las personas. Estos riesgos son aceptables para la Compañía y se gestionan mediante los procedimientos de control estándar.
- Riesgo Medio: Se define como Riesgo Medio a aquel que, a pesar de los controles, podría generar un impacto moderado y acotado. Requiere de medidas de control específicas y un monitoreo periódico por parte del dueño del riesgo para asegurar que se mantiene en un nivel tolerable.
- Riesgo Medio Alto: Un Riesgo Medio Alto es aquel que representa una amenaza significativa para los objetivos del negocio, la seguridad de la información o la reputación. Su gestión exige atención prioritaria, con planes de acción robustos y detallados para su mitigación, además de una aprobación formal por parte de los comités especializados.
- Riesgo Alto: Se cataloga como Riesgo Alto a aquel que posee el potencial de causar un impacto severo y extendido en la Compañía, afectando críticamente los objetivos estratégicos, la estabilidad financiera o el cumplimiento normativo. Estos riesgos exigen una respuesta inmediata, medidas de mitigación urgentes y la supervisión directa de la alta dirección y los comités de riesgo.

En caso de detectarse un riesgo o clasificarse alguna herramienta de IA de Riesgo Medio Alto o Alto, deberá efectuarse una evaluación de impacto reputacional y legal y establecerse un plan de mitigación documentado y aprobado por el Comité IA.

Nivel de Riesgo	Descripción General	Ejemplos de Uso	Gobernanza Requerida
Riesgo Bajo	Sistemas para productividad personal o procesos internos no críticos. No procesan datos personales y su impacto financiero es insignificante.	Asistentes de IA Generativa para borradores no confidenciales, RPA para tareas administrativas, traducción de documentos públicos, organización de información o bases de conocimiento.	Si el Riesgo Residual es Bajo: Se gestiona según procedimiento estándar de Gestión de Riesgo. Supervisión a nivel de Jefatura. No requiere escalamiento al Comité de IA.
Riesgo Medio	Sistemas que apoyan la toma de decisiones operativas con supervisión humana y cuyo impacto financiero es limitado.	Análisis de patrones de compra para segmentación de clientes. Modelos básicos de recomendación de productos en un canal.	Si el Riesgo Residual es Medio: El análisis de riesgo debe incluir validación de controles por Gerencia de Seguridad TI y Oficial de Cumplimiento y Protección de Datos. Debe ser informado al Comité de IA.
Riesgo Medio Alto	Sistemas que apoyan la toma de decisiones relevantes para la operación, con impacto financiero significativo o uso de datos personales a escala.	Modelos de demanda para optimización de stock a nivel cadena. Sistemas de apoyo a la optimización de rutas de distribución. Reconocimiento visual para control de inventario a gran escala.	Si el Riesgo Residual es Medio Alto: Requiere aprobación explícita del Comité de IA antes de su desarrollo o adquisición. Exige un análisis de riesgos exhaustivo y planes de mitigación a detallar según sistema de Gestión de Riesgos.
Riesgo Alto	Sistemas que toman o influyen en "decisiones críticas" sobre personas, procesan datos sensibles, o tienen un impacto reputacional o financiero severo.	Sistemas de fijación de precios dinámicos. Modelos para concesión de crédito. Herramientas de preselección de candidatos. Reconocimiento facial para seguridad.	Si el Riesgo Residual es Alto: Además de lo requerido para Medio Alto, exige una PIA completa obligatoria. El caso debe ser presentado por el Comité de IA al Comité de Riesgos de la Administración para su supervisión.

b. USO DE LA INTELIGENCIA ARTIFICIAL POR PARTE DE LOS(AS) TRABAJADORES(AS) Y TERCEROS

El uso de tecnologías de Inteligencia Artificial por parte de los trabajadores(as) en el cumplimiento de sus labores, y terceros relacionados con SMU, ya sea en la prestación de servicios, consultorías o asesorías o similares, debe realizarse de manera informada, alineado con los valores CERCA y los principios definidos en esta política, además de cumplir con los procedimientos internos y la normativa legal vigente. Esta directriz también aplica a los directores de la Compañía en el cumplimiento de sus funciones de director.

La IA se utilizará por todos ellos, exclusivamente como herramienta complementaria y bajo supervisión humana, sin delegar decisiones críticas, regulatorias o sensibles a sistemas automatizados sin evaluación y aprobación previa correspondiente.

Cada trabajador(a), director(a) y tercero que se relacione con SMU será responsable de:

- Proteger la información de la Compañía durante el uso de IA.
- Evaluar críticamente los resultados generados por los sistemas de IA.
- Reportar cualquier anomalía, alucinación, sesgo algorítmico o uso indebido de estas herramientas.
- No utilizar herramientas de IA no aprobadas (evitar el Shadow AI).
- Está prohibido implementar sistemas de vigilancia masiva sin base legal válida.
- Utilizar datos sensibles sin fundamento legal o consentimiento.

Se prohíbe ingresar información confidencial o estratégica en herramientas no autorizadas y que todo contenido que vaya a ser difundido externamente debe ser revisado y autorizado por una jefatura responsable.

La Gerencia de Seguridad TI mantendrá y actualizará un registro oficial de herramientas de IA autorizadas, clasificadas según su nivel de riesgo y tipo de uso permitido (Autorizadas, Condicionales o Prohibidas).

4. GESTIÓN DE SISTEMAS DE IA DE TERCEROS

La incorporación de tecnologías, servicios o componentes de Inteligencia Artificial (IA) por parte de proveedores de SMU deberá cumplir igualmente con los principios definidos en esta política, asegurando que su uso no represente riesgos para los activos y procesos de SMU ni para los derechos de las personas.

Todo proveedor que ofrezca una solución de IA o un servicio que integre modelos de IA deberá someterse a un proceso de evaluación formal previo a su contratación, conforme al procedimiento definido por la Compañía. Esta evaluación deberá incluir, al menos, los siguientes aspectos:

- Transparencia y Explicabilidad: El proveedor deberá explicar su sistema, incluyendo su arquitectura general, nivel de autonomía, técnicas de aprendizaje, y su capacidad de explicabilidad.
- Control de Sesgos: El proveedor debe detallar sus procesos y controles para identificar y mitigar el Sesgo Algorítmico en sus modelos.
- Manejo de Decisiones Automatizadas: El proveedor debe dar a entender cómo gestiona las “decisiones críticas” o “automatizadas”, y cuáles son los mecanismos de

supervisión humana implementados.
- Seguridad y Calidad: El proveedor debe demostrar su gestión sobre normas de calidad y vulnerabilidad sistémica, según requiera la Compañía (ej. certificaciones ISO/IEC 27001, implementación de NIST AI RMF).
- Trazabilidad del Uso y Manejo de Información: El proveedor debe garantizar la trazabilidad del uso y manejo de la información incluyendo la identificación de subcontratistas y proveedores de datos para evitar fugas de información a terceros no autorizados y/o infracciones legales.
- Requisitos Contractuales Mínimos: Todo contrato que SMU suscriba con proveedores de IA deberá incorporar, como mínimo:
    - Controles técnicos y organizativos de seguridad para el tratamiento de la información de SMU.
    - Garantía de uso exclusivo de los datos proporcionados por SMU para el servicio contratado, prohibiendo su utilización para entrenamiento adicional del modelo, su reutilización por parte del proveedor, transmisión a terceros no autorizados o almacenamiento indebido.

SMU mantendrá la titularidad sobre los datos entregados al proveedor y sobre los resultados generados con los Sistemas de IA.
La propiedad del modelo resultante (en caso de ser entrenado con datos de SMU) no podrá transferirse sin cláusula explícita aprobada previamente por el Comité de IA.

5. SEGURIDAD Y TRAZABILIDAD DE LA INTELIGENCIA ARTIFICIAL

a. MARCO DE SEGURIDAD TI PARA LA IA

SMU asegurará que la seguridad de los Sistemas de IA será abordada desde una perspectiva integral, considerando la protección de datos, seguridad, algoritmos, infraestructuras, entornos de ejecución, usuarios y flujos de inferencia.
Esta protección debe contemplar no solo la prevención de brechas tradicionales, sino también riesgos emergentes como: la manipulación de entradas (Ataques Adversariales), la generación de inferencias incorrectas o alucinaciones, la exposición de datos a través de re-identificación indirecta, sesgos algorítmicos persistentes, regresiones de comportamiento, y la integridad y disponibilidad del modelo ante cambios maliciosos.

Para ello, la Gerencia de Seguridad TI deberá implementar, como mínimo controles organizados en los siguientes niveles:
- Protección de Datos y Privacidad: Aplicación obligatoria de privacidad por diseño y privacidad por defecto en todo Sistema de IA que procese datos personales o sensibles. Cifrado de datos en reposo y en tránsito (ej. AES-256, TLS 1.3). Anonimización o seudonimización de conjunto de datos, especialmente en fases de entrenamiento y testeo.
- Seguridad del Modelo y Algoritmos: Evaluación periódica de robustez ante Ataques Adversariales y desviación del comportamiento esperado. Validación de Explicabilidad y transparencia de resultados. Versionamiento seguro de modelos entrenados, con firma digital y validación de integridad.
- Control de Acceso y Entorno: Aplicación del principio de mínimo privilegio en accesos a datos de entrenamiento, entornos de ejecución y outputs. Trazabilidad completa de accesos administrativos y operaciones sobre el modelo. Separación lógica y física de entornos de desarrollo, testing y producción.
- Ciclo de Vida Seguro y Monitoreo: Auditorías regulares de código, datasets y comportamiento de inferencia. Implementación de herramientas de monitoreo

continuo y alertas sobre anomalías, errores o Sesgos Algorítmicos emergentes. Evaluación continua de cumplimiento frente a políticas internas y marcos regulatorios externos.

Todas las soluciones basadas en IA deberán estar sujetas a un plan de pruebas de seguridad, que incluya pruebas funcionales, de estrés, de manipulación y de escenarios adversos, asegurando que el comportamiento del sistema se mantenga confiable, explicable y alineado con los objetivos del negocio.

Los Sistemas de IA clasificados de Riesgo Alto deberán someterse, al menos anualmente, a auditorías internas, y podrán ser objeto de auditorías externas cuando así lo determine el Comité IA, el Directorio o el Comité de Auditoría y Riesgos.

SMU mantendrá un registro corporativo de sistemas de IA donde se indicará la finalidad del sistema, clasificación de riesgo, área o persona responsable, tipo de datos utilizados, versión del modelo, fecha de aprobación y fecha de última revisión.

b. TRAZABILIDAD Y MONITOREO

SMU asegurará que todos los Sistemas de IA, especialmente aquellos clasificados como de "Riesgo Medio", "Riesgo Medio-Alto" y "Riesgo Alto", deberán implementar capacidades robustas de registro (logging) y auditoría que permitan:

- Trazabilidad completa de sus operaciones,
- Seguimiento de las decisiones tomadas o influenciadas por la IA,
- La identificación de los datos utilizados en el proceso y
- El control de las versiones de los modelos desplegados.

La información generada por estos mecanismos de trazabilidad será esencial para la investigación de incidentes, la auditoría interna y externa, y para sustentar la mejora continua del desempeño y la seguridad de los Sistemas de IA.

6. GESTIÓN DEL CICLO DE VIDA DE LOS DATOS

El ciclo de vida completo de los datos utilizados por Sistemas de IA (recolección, almacenamiento, procesamiento, uso y eliminación) deberá cumplir con la normativa vigente, así como con la Política de Protección de Datos Personales y la Política General de Seguridad de la Información de SMU.

Se establecerán procedimientos formales para la eliminación segura o la anonimización de datos una vez que ya no sean necesarios para el propósito para el que fueron recopilados, o cuando lo exija la normativa legal. Se prestará especial atención a la gobernanza de datos en entornos de entrenamiento y producción.

7. CULTURA, CAPACITACIÓN Y CONCIENTIZACIÓN

SMU promoverá una cultura organizacional basada en la ética, la seguridad y el uso responsable de las tecnologías de Inteligencia Artificial, como parte de su compromiso con la sostenibilidad digital, el respeto a los derechos de las personas y la innovación confiable.
SMU asegurará que todo colaborador (a) independientemente de su cargo o función, reciba información que permita un uso seguro, ético y responsable de la IA y que participe en procesos de formación y concientización orientados a:

- Comprender los riesgos asociados al uso de IA en relación con la privacidad de las personas, la integridad de los datos, la equidad en la toma de decisiones y los efectos sociales o reputacionales.
- Reconocer sus responsabilidades individuales y colectivas frente al uso ético de IA, incluyendo la prohibición de herramientas no autorizadas (Shadow AI), la Evaluación Crítica de resultados generados por IA y la obligación de reporte frente a anomalías (ej. Alucinaciones, Deepfakes no autorizados).
- Identificar señales de Sesgo Algorítmico, discriminación indirecta o fallos en los modelos predictivos que puedan tener impacto humano, operacional o legal.

Los programas de capacitación se diferenciarán según el nivel de exposición, responsabilidad y uso de IA por parte de cada trabajador(a), e incluirán evaluaciones obligatorias y una validación interna de conocimientos para asegurar la comprensión y cumplimiento de esta política.

SMU fomentará el reporte oportuno de vulnerabilidades, sesgos, errores en modelos o usos indebidos de herramientas IA, a través de canales internos de consultas o denuncias seguros, protegidos y libres de represalias.

VII. DIVULGACIÓN, VIGENCIA Y APLICACIÓN

La presente política fue aprobada por el Directorio de SMU en su sesión de fecha 18 de mayo de 2026, sobre la base de las recomendaciones del Comité de IA, dada su relevancia estratégica y transversal para la organización.

Esta política es un documento vivo y será revisada y, si es necesario, actualizada, como mínimo una vez al año, o cuando exista un evento crítico que lo justifique (por ejemplo, cambios regulatorios, incidente de seguridad mayor, introducción de una nueva tecnología de IA disruptiva en la compañía, entre otros).

El Comité de IA propondrá al Directorio las actualizaciones que correspondan, mientras que la Gerencia de Seguridad TI coordinará este proceso para asegurar que SMU se mantenga a la vanguardia en la gobernanza de la IA.

Esta Política se presume conocida desde que se publique en el repositorio de la Compañía y su vigencia será de carácter indefinido. La misma regla se aplicará en caso de cualquier modificación.

Esta Política es obligatoria para todos los trabajadores(as) de SMU S.A y sus filiales.