					Introduzca aquí la denominación de la entidad jurídica registrada							
Número de documento: PII21					Título del documento: **Política de privacidad de IA y toma de decisiones automatizada**							
Versión: 1.0		Fecha de entrada en vigor: 01.01.2025			Propietario del documento:							
X	Política		Norma		Procedimiento		Formulario		Registro		Otro	

Historial de revisiones				
Número de revisión	**Fecha de revisión**	**Cambios**	**Revisado por**	**Propietario del proceso**

Aprobaciones			
Nombre	**Cargo**	**Fecha**	**Firma**

Alineación con normas y reglamentos

Norma / Reglamento	Cláusula / Control / Artículo	Aplicabilidad	Tipo de cobertura	Comentario
ISO/IEC 27701:2025	Clause 7.5; Clause 8.1	Both	Primary	Información documentada y control operacional para evidencias del tratamiento mediante IA, elaboración de perfiles y toma de decisiones automatizada
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Seguimiento, no conformidad y acción correctiva para controles de privacidad de IA
ISO/IEC 27701:2025	Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.6; Annex A.1.2.9	Controller	Primary	Finalidad, base jurídica, evaluación de impacto sobre la privacidad y registros del responsable del tratamiento
ISO/IEC 27701:2025	Annex A.1.2.7; Annex A.1.2.8	Controller	Supporting	Contratos con encargados del tratamiento y responsabilidades de corresponsables del tratamiento para el tratamiento de PII relacionado con IA
ISO/IEC 27701:2025	Annex A.1.3.2; Annex A.1.3.3; Annex A.1.3.4	Controller	Primary	Obligaciones frente a interesados y transparencia para el tratamiento relacionado con IA
ISO/IEC 27701:2025	Annex A.1.3.6; Annex A.1.3.7; Annex A.1.3.10; Annex A.1.3.11	Controller	Primary	Obligaciones de oposición, acceso, rectificación, supresión, gestión de solicitudes y toma de decisiones automatizada
ISO/IEC 27701:2025	Annex A.1.4.2; Annex A.1.4.3; Annex A.1.4.5	Controller	Primary	Límites de recogida, tratamiento y

				minimización para entradas, salidas y datos derivados de IA
ISO/IEC 27701:2025	Annex A.1.5.2; Annex A.1.5.3; Annex A.1.5.4; Annex A.1.5.5	Conditional	Supporting	Enrutamiento de transferencias internacionales, comunicaciones y solicitudes de divulgación para PII relacionada con IA
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.6; Annex A.2.2.7	Processor	Primary	Acuerdo del encargado del tratamiento, instrucciones documentadas, apoyo a las obligaciones del cliente y registros
ISO/IEC 27701:2025	Annex A.2.3.2; Annex A.2.5.2; Annex A.2.5.3; Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6	Processor	Supporting	Apoyo del encargado del tratamiento a obligaciones frente a interesados, enrutamiento de transferencias y gestión de divulgaciones
ISO/IEC 27701:2025	Annex A.3.14; Annex A.3.25	Both	Supporting	Protección de registros y registro de eventos relacionados con el tratamiento de PII relacionado con IA
GDPR	Article 4(4); Article 5(1)(a); Article 5(1)(b); Article 5(1)(c); Article 5(1)(d); Article 5(2)	Controller	Primary	Elaboración de perfiles, equidad, transparencia, limitación de la finalidad, minimización, exactitud y responsabilidad proactiva
GDPR	Article 6; Article 9; Article 10	Controller	Primary	Licitud, datos de categorías especiales y salvaguardas para datos de condenas

				o infracciones penales
GDPR	Article 12; Article 13; Article 14; Article 15	Controller	Primary	Información transparente, acceso e información significativa sobre la toma de decisiones automatizada
GDPR	Article 16; Article 17; Article 18; Article 21; Article 22	Controller	Primary	Derechos de rectificación, supresión, limitación, oposición y toma de decisiones automatizada
GDPR	Article 24; Article 25; Article 26; Article 28; Article 30; Article 32; Article 35; Article 39	Both	Supporting	Responsabilidad del responsable del tratamiento, diseño/por defecto, corresponsables del tratamiento, encargados del tratamiento, registros, seguridad, DPIA y tareas del DPO
GDPR	Article 44	Conditional	Referenced	Enrutamiento de transferencias internacionales para el tratamiento de PII relacionado con IA
ISO/IEC 29100:2020	Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6; Clause 5.7	Both	Primary	Principios de finalidad, recogida, minimización, uso, conservación, divulgación, exactitud y calidad
ISO/IEC 29100:2020	Clause 5.8; Clause 5.9; Clause 5.10; Clause 5.11; Clause 5.12	Both	Supporting	Transparencia, participación individual, responsabilidad proactiva, seguridad de la información y cumplimiento de privacidad

ISO/IEC 29134:2020	Clause 5.1; Clause 6.2; Clause 6.3	Both	Supporting	Beneficio de la PIA, determinación del umbral y preparación para la evaluación de riesgos de privacidad relacionados con IA
ISO/IEC 29151:2022	Annex A.4; Annex A.5; Annex A.7; Annex A.8; Annex A.10	Both	Supporting	Controles de finalidad, recogida, minimización, uso, conservación, divulgación, exactitud y participación del interesado

1. Alcance

1.1 Esta política define los requisitos obligatorios de privacidad para las actividades de tratamiento de inteligencia artificial, elaboración de perfiles, puntuación, recomendación, apoyo a la toma de decisiones y toma de decisiones automatizada que utilicen, infieran, generen, divulguen o traten de otro modo PII dentro del alcance del PIMS.

1.2 Esta política se aplica a lo siguiente:

1.2.1 sistemas, aplicaciones, modelos, servicios, flujos de trabajo, motores de decisión, herramientas de puntuación, sistemas de recomendación, modelos analíticos y procesos de toma de decisiones automatizada habilitados por IA que traten PII;

1.2.2 elaboración de perfiles, segmentación, clasificación, predicción, inferencia, personalización, ordenación, elegibilidad, detección de fraude, puntuación de riesgos, decisiones de acceso, evaluación relacionada con el empleo, elaboración de perfiles relativa a menores, personalización de marketing y tratamientos similares en los que intervenga PII;

1.2.3 PII relacionada con IA utilizada para entrenamiento, pruebas, validación, ajuste, seguimiento, inferencia en producción, revisión de salidas, medición del desempeño, investigación de incidentes o retirada del modelo;

1.2.4 contextos de responsable del tratamiento, corresponsable del tratamiento, encargado del tratamiento y subencargado del tratamiento;

1.2.5 proveedores relacionados con IA, encargados del tratamiento, subencargados del tratamiento, destinatarios de intercambio de datos y rutas de transferencia internacional que traten PII.

1.3 Esta política no crea un marco completo de gobernanza de IA, sistema de gestión de IA, inventario de IA, inventario de modelos, registro de riesgos de modelos, registro de equidad, registro de algoritmos, registro de incidentes de IA, comité de IA, rol de propietario del modelo, rol de propietario del sistema de IA, flujo de trabajo de asesoramiento jurídico ni formulario separado de aprobación de IA.

1.4 Esta política no sustituye a lo siguiente:

1.4.1 PII03 para el inventario de tratamientos, la base jurídica y la titularidad del ROPA;

1.4.2 PII04 para la gobernanza de los avisos de privacidad;

1.4.3 PII05 para la gestión de consentimientos y preferencias;

1.4.4 PII06 para el flujo de trabajo de derechos de los interesados;

1.4.5 PII07 para la evaluación de riesgos de privacidad y la metodología de DPIA;

1.4.6 PII08 para las puertas de control de privacidad desde el diseño y por defecto;

1.4.7 PII09 para los controles de recogida, uso, divulgación e intercambio;

1.4.8 PII10 para la ejecución de conservación, supresión y eliminación;

1.4.9 PII11 para los controles de exactitud y calidad;

1.4.10 PII12 para la gobernanza del ciclo de vida de encargados del tratamiento, subencargados del tratamiento y terceros;

1.4.11 PII13 para los controles de transferencias internacionales;

1.4.12 PII14 para seguridad y control de acceso;

1.4.13 PII15 para la gestión de incidentes y brechas de seguridad;

1.4.14 PII18 para seguimiento, auditoría y mejora;

1.4.15 PII19 para privacidad de empleados;

1.4.16 PII20 para privacidad de menores;

1.4.17 PII22 para privacidad de marketing y cookies.

2. Propósito

2.1 El propósito de esta política es asegurar que las actividades de IA, elaboración de perfiles y toma de decisiones automatizada que impliquen PII se identifiquen, documenten, evalúen en cuanto a riesgos, sean transparentes, puedan impugnarse, sean objeto de seguimiento y se controlen a través del PIMS sin crear artefactos duplicados de gobernanza específicos de IA.

2.2 Esta política asegura que las obligaciones de privacidad para el tratamiento de PII relacionado con IA se evidencien mediante REG02, REG04, REG06, REG07, REG08, REG09, REG10 y REG12.

3. Objetivos

3.1 Los objetivos de esta política son:

3.1.1 identificar en REG02 el tratamiento mediante IA, elaboración de perfiles y toma de decisiones automatizada que implique PII;

3.1.2 documentar en REG02 las finalidades relacionadas con IA, la base jurídica, las categorías de PII, las fuentes de datos, los datos inferidos, las salidas, los destinatarios y los efectos de las decisiones;

3.1.3 activar la evaluación preliminar de riesgos de privacidad y el enrutamiento de DPIA mediante REG04;

3.1.4 asegurar que los avisos de privacidad relacionados con IA y la información significativa se registren en REG07;

3.1.5 enrutar las solicitudes de derechos, oposición, revisión humana y posibilidad de impugnación mediante REG06;

3.1.6 controlar mediante REG08 los encargados del tratamiento, subencargados del tratamiento, proveedores y acuerdos de intercambio de datos relacionados con IA;

3.1.7 enrutar las transferencias internacionales relacionadas con IA mediante REG09;

3.1.8 escalar los incidentes sospechosos de PII relacionados con IA, el uso indebido, la divulgación no autorizada y los resultados adversos para la privacidad mediante REG10 y REG12;

3.1.9 registrar en REG12 el seguimiento, las excepciones, las no conformidades, las acciones correctivas y las mejoras.

4. Declaraciones de la política

4.1 Identificación de IA, elaboración de perfiles y toma de decisiones automatizada

4.1.1 [Controller] Cuando se proponga un sistema, aplicación, modelo, flujo de trabajo, servicio o proceso de la organización nuevo o con cambios materiales, el Process Owner / Business Owner debe determinar si utiliza IA, elaboración de perfiles, puntuación, recomendación, apoyo a la toma de decisiones o toma de decisiones automatizada que implique PII y registrar la determinación en REG02.

4.1.2 [Controller] Antes de que comience el tratamiento de PII relacionado con IA, el Process Owner / Business Owner debe documentar la finalidad del tratamiento, las categorías de PII, las categorías de interesados, las fuentes de datos, las categorías de datos inferidos o derivados, las categorías de salidas, las categorías de destinatarios, la base jurídica y la vinculación con el calendario de conservación en REG02.

4.1.3 [Controller] Antes de utilizar en producción la elaboración de perfiles, la puntuación, la recomendación, el apoyo a la toma de decisiones o la toma de decisiones automatizada, el Process Owner / Business Owner debe documentar el contexto de la decisión, el efecto esperado sobre los interesados, la intervención humana y la ruta de derechos en REG02 y REG04.

4.1.4 [Joint Controller] Antes de realizar tratamiento de PII relacionado con IA con un corresponsable del tratamiento, el Privacy Lead / PIMS Manager debe documentar en REG08 la responsabilidad sobre la definición de finalidad, el aviso, la gestión de derechos, el apoyo a la DPIA, la gobernanza de encargados del tratamiento y el escalado de incidentes.

4.1.5 [Processor] Antes de tratar PII mediante un servicio relacionado con IA para un cliente, el Process Owner / Business Owner debe confirmar que las instrucciones del cliente, las finalidades permitidas, los usos prohibidos, la gestión de la información de salida y las obligaciones de asistencia estén documentados en REG08.

4.1.6 [Both] Antes de activar el tratamiento de PII relacionado con IA, el Privacy Lead / PIMS Manager debe confirmar que el tratamiento esté vinculado a los objetos de evidencia canónicos aplicables y que no se cree ningún registro separado específico de IA fuera de REG02, REG04, REG06, REG07, REG08, REG09, REG10 o REG12.

4.2 Evaluación de riesgos de privacidad y enrutamiento de DPIA

4.2.1 [Controller] Antes de lanzar o modificar materialmente el tratamiento de PII relacionado con IA, el Privacy Lead / PIMS Manager debe completar la evaluación preliminar de riesgos de privacidad y registrar la decisión de DPIA en REG04.

4.2.2 [Conditional] Cuando el tratamiento relacionado con IA implique elaboración de perfiles, decisiones automatizadas, evaluación a gran escala, datos de categorías especiales, datos de infracciones penales, interesados vulnerables, evaluación de empleados, menores, seguimiento del comportamiento, datos de localización, datos biométricos, puntuación de alto impacto o efectos significativos, el Data Protection Officer / Privacy Advisor debe revisar el riesgo de privacidad y registrar el asesoramiento en REG04.

4.2.3 [Controller] Antes de la entrada en producción del tratamiento de PII relacionado con IA, el Process Owner / Business Owner debe documentar las acciones de tratamiento de riesgos, el estado del riesgo residual y las evidencias de preparación para la entrada en producción en REG04 o REG12.

4.2.4 [Controller] Antes de reutilizar PII para entrenamiento, pruebas, validación, ajuste, seguimiento o mejora de modelos con una finalidad nueva o modificada materialmente, el Process Owner / Business Owner debe completar la revisión de privacidad y registrar la decisión en REG02 y REG04.

4.2.5 [Conditional] Cuando el riesgo residual de privacidad siga siendo alto tras el tratamiento planificado, Top Management debe aprobar, rechazar o requerir tratamiento adicional antes del uso en producción y registrar la decisión en REG04 y REG12.

[... Las secciones 4.3–8 no están incluidas en esta vista previa. Adquiera el documento completo para acceder al contenido íntegro. ...]

9. Excepciones

9.1 [All] Antes de desviarse de un requisito de privacidad relacionado con IA de esta política, el Process Owner / Business Owner solicitante debe presentar en REG12 una justificación de excepción y evidencias de controles compensatorios.

9.2 [Conditional] Cuando una excepción afecte a la elaboración de perfiles, la toma de decisiones automatizada, la revisión humana, la posibilidad de impugnación, la transparencia, el resultado de DPIA, la puntuación de alto impacto, el tratamiento relativo a menores, el tratamiento relativo a empleados, las restricciones de encargados del tratamiento o las transferencias internacionales, el Data Protection Officer / Privacy Advisor debe revisar la excepción y registrar el asesoramiento en REG04 o REG12.

9.3 [Conditional] Cuando una excepción cree o preserve un alto riesgo residual de privacidad, Top Management debe aprobar o rechazar la excepción y registrar la decisión en REG04 y REG12.

9.4 [All] Antes de que venza una excepción de privacidad relacionada con IA aprobada, el Privacy Lead / PIMS Manager debe revisar el estado de cierre, renovación o acción correctiva y registrar el resultado en REG12.

10. Aplicación

10.1 [All] Cuando se identifique incumplimiento de esta política, el Privacy Lead / PIMS Manager debe registrar la no conformidad y la acción correctiva en REG12.

10.2 [Both] Cuando se sospeche tratamiento, divulgación o acceso no autorizados a PII relacionada con IA, uso indebido del modelo, fallo de derechos o resultado adverso para la privacidad, el Incident Response Coordinator debe iniciar el escalado de incidentes y registrar evidencias en REG10 y REG12.

10.3 [Both] Cuando un encargado del tratamiento, subencargado del tratamiento, proveedor o destinatario de intercambio de datos incumpla las obligaciones de privacidad relacionadas con IA, el Vendor / Procurement Owner debe registrar las acciones de remediación, escalado o terminación en REG08 y REG12.

10.4 [All] Cuando se produzcan no conformidades de privacidad relacionadas con IA repetidas o sistémicas, Top Management debe revisar la cuestión y registrar la acción de gestión en REG12.

11. Revisión y mantenimiento

11.1 [All] Al menos anualmente, el Privacy Lead / PIMS Manager debe revisar esta política para asegurar su idoneidad continuada y registrar el resultado de la revisión en REG12.

11.2 [Conditional] Cuando cambien materialmente las leyes, servicios, modelos, fuentes de datos, prácticas de elaboración de perfiles, lógica de toma de decisiones automatizada, acuerdos con proveedores, rutas de transferencia o riesgos de privacidad, el Privacy Lead / PIMS Manager debe revisar los controles de privacidad relacionados con IA afectados y registrar el resultado en REG02, REG04 o REG12.

11.3 [Controller] Al menos anualmente y después de cambios materiales en el recorrido del usuario relacionado con IA, el Process Owner / Business Owner debe revisar las evidencias de transparencia, información significativa, revisión humana y ruta de derechos, y registrar la revisión en REG06 y REG07.

11.4 [All] Una vez cerradas las acciones correctivas de privacidad relacionadas con IA, el Internal Audit / Compliance Reviewer debe verificar su eficacia y registrar evidencias de verificación en REG12.

12. Políticas relacionadas

12.1 PII01 - Política del Sistema de Gestión de la Privacidad de la Información

12.2 PII02 - Política de roles, responsabilidades y responsabilidad proactiva en privacidad

12.3 PII03 - Política de inventario de tratamientos de PII y base jurídica

12.4 PII04 - Política de avisos de privacidad y transparencia

12.5 PII05 - Política de gestión de consentimientos y preferencias

12.6 PII06 - Política de gestión de derechos de los interesados

12.7 PII07 - Política de evaluación de riesgos de privacidad y DPIA

12.8 PII08 - Política de privacidad desde el diseño y por defecto

12.9 PII09 - Política de recogida, uso, divulgación e intercambio de PII

12.10 PII10 - Política de conservación, supresión y eliminación de PII

12.11 PII11 - Política de exactitud y calidad de PII

12.12 PII12 - Política de gestión de privacidad de encargados del tratamiento, subencargados del tratamiento y terceros

12.13 PII13 - Política de transferencia internacional de PII

12.14 PII14 - Política de seguridad y control de acceso de PII

12.15 PII15 - Política de gestión de incidentes y brechas de seguridad de PII

12.16 PII17 - Política de información documentada y gestión de evidencias del PIMS

12.17 PII18 - Política de seguimiento, auditoría y mejora del PIMS

12.18 PII19 - Política de privacidad de empleados

12.19 PII20 - Política de privacidad de menores

12.20 PII22 - Política de privacidad de marketing y cookies

13. Normas y marcos de referencia

13.1 ISO/IEC 27701:2025 - Clause 7.5; Clause 8.1. Addressed by clauses [4.1.6; 4.8.1; 6.1; 7.1; 7.5; 11.1].

13.2 ISO/IEC 27701:2025 - Clause 9.1; Clause 10.2. Addressed by clauses [4.6.2; 4.6.5; 4.8.2; 6.5; 8.1; 8.2; 8.3; 8.4; 8.5; 10.1; 11.4].

13.3 ISO/IEC 27701:2025 - Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.6; Annex A.1.2.9. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.2.1; 4.2.3; 4.2.4; 4.8.1; 7.1; 7.2].

13.4 ISO/IEC 27701:2025 - Annex A.1.2.7; Annex A.1.2.8. Addressed by clauses [4.1.4; 4.7.1; 4.7.2; 4.7.3; 5.7; 6.3; 7.6].

13.5 ISO/IEC 27701:2025 - Annex A.1.3.2; Annex A.1.3.3; Annex A.1.3.4. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 7.3; 11.3].

13.6 ISO/IEC 27701:2025 - Annex A.1.3.6; Annex A.1.3.7; Annex A.1.3.10; Annex A.1.3.11. Addressed by clauses [4.1.3; 4.3.2; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 7.4; 11.3].

13.7 ISO/IEC 27701:2025 - Annex A.1.4.2; Annex A.1.4.3; Annex A.1.4.5. Addressed by clauses [4.2.4; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 7.1; 7.5].

13.8 ISO/IEC 27701:2025 - Annex A.1.5.2; Annex A.1.5.3; Annex A.1.5.4; Annex A.1.5.5. Addressed by clauses [4.7.3; 4.7.4; 4.7.5; 7.7].

13.9 ISO/IEC 27701:2025 - Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.6; Annex A.2.2.7. Addressed by clauses [4.1.5; 4.3.5; 4.5.5; 4.7.1; 4.7.2; 5.7; 6.3; 7.6].

13.10 ISO/IEC 27701:2025 - Annex A.2.3.2; Annex A.2.5.2; Annex A.2.5.3; Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6. Addressed by clauses [4.3.5; 4.5.5; 4.7.1; 4.7.2; 4.7.4; 4.7.5; 7.6; 7.7].

13.11 ISO/IEC 27701:2025 - Annex A.3.14; Annex A.3.25. Addressed by clauses [4.4.4; 4.6.1; 4.6.3; 4.8.1; 5.4; 7.5; 7.8; 10.2].

13.12 GDPR - Article 4(4); Article 5(1)(a); Article 5(1)(b); Article 5(1)(c); Article 5(1)(d); Article 5(2). Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.3.1; 4.4.1; 4.4.2; 4.4.5; 4.8.1; 8.1].

13.13 GDPR - Article 6; Article 9; Article 10. Addressed by clauses [4.1.2; 4.2.4; 4.4.3; 4.7.3; 7.1].

13.14 GDPR - Article 12; Article 13; Article 14; Article 15. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.5.2; 4.5.3; 7.3; 11.3].

13.15 GDPR - Article 16; Article 17; Article 18; Article 21; Article 22. Addressed by clauses [4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 7.4].

13.16 GDPR - Article 24; Article 25; Article 26; Article 28; Article 30; Article 32; Article 35; Article 39. Addressed by clauses [4.1.4; 4.1.5; 4.2.1; 4.2.2; 4.2.5; 4.4.4; 4.7.1; 4.8.2; 5.3; 6.2; 6.4; 7.2].

13.17 GDPR - Article 44. Addressed by clauses [4.7.4; 7.7; 8.4].

13.18 ISO/IEC 29100:2020 - Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6; Clause 5.7. Addressed by clauses [4.1.2; 4.2.4; 4.4.1; 4.4.2; 4.4.4; 4.4.5; 4.7.5].

13.19 ISO/IEC 29100:2020 - Clause 5.8; Clause 5.9; Clause 5.10; Clause 5.11; Clause 5.12. Addressed by clauses [4.3.1; 4.3.2; 4.5.1; 4.5.2; 4.6.3; 4.8.1; 4.8.2; 8.5; 10.1].

13.20 ISO/IEC 29134:2020 - Clause 5.1; Clause 6.2; Clause 6.3. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.5; 4.6.4; 6.4; 7.2; 9.2].

13.21 ISO/IEC 29151:2022 - Annex A.4; Annex A.5; Annex A.7; Annex A.8; Annex A.10. Addressed by clauses [4.3.1; 4.3.2; 4.4.1; 4.4.2; 4.4.4; 4.4.5; 4.5.2; 4.5.4; 4.7.5].