					Introduzca aquí la denominación de la entidad jurídica registrada							
Número de documento: PII09					Título del documento: **Política de recogida, uso, divulgación e intercambio de PII**							
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 regulaciones

Standard / Regulation	Clause / Control / Article	Applicability	Coverage Type	Comment
ISO/IEC 27701:2025	Clause 7.5; Clause 8.1	Both	Primary	Control operacional documentado
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Supervisión y acción correctiva
ISO/IEC 27701:2025	Annex A.1.2.2; Annex A.1.2.9	Controller	Primary	Finalidad y registros de tratamiento
ISO/IEC 27701:2025	Annex A.1.2.3	Controller	Referenced	Vinculación con la base jurídica
ISO/IEC 27701:2025	Annex A.1.2.8	Joint Controller	Supporting	Responsabilidades de intercambio entre corresponsables del tratamiento
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
ISO/IEC 27701:2025	Annex A.1.5.2; Annex A.1.5.3	Conditional	Referenced	Vinculación de enrutamiento de transferencias
ISO/IEC 27701:2025	Annex A.1.5.4; Annex A.1.5.5	Controller	Primary	Registros de transferencia y divulgación
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.7	Processor	Primary	Instrucciones y registros del encargado del tratamiento
ISO/IEC 27701:2025	Annex A.2.5.2; Annex A.2.5.3	Processor	Referenced	Vinculación de enrutamiento de transferencias del encargado del tratamiento
ISO/IEC 27701:2025	Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6	Processor	Supporting	Registros y solicitudes de divulgación del encargado del tratamiento
GDPR	Article 5(1)(b); Article 5(1)(c); Article 5(2)	Controller	Primary	Limitación de la finalidad, minimización y responsabilidad proactiva

GDPR	Article 6	Controller	Referenced	Vinculación con la base jurídica
GDPR	Article 24	Controller	Supporting	Responsabilidad del responsable del tratamiento
GDPR	Article 26	Joint Controller	Supporting	Acuerdos de corresponsabilidad del tratamiento
GDPR	Article 28	Both	Supporting	Instrucciones del encargado del tratamiento y límites de divulgación
GDPR	Article 30	Both	Supporting	Registros de tratamiento y destinatarios
ISO/IEC 29100:2020	Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6	Both	Primary	Limitación de finalidad, recogida, minimización y divulgación
ISO/IEC 29100:2020	Clause 5.10; Clause 5.12	Both	Supporting	Responsabilidad proactiva y cumplimiento de privacidad
ISO/IEC 29151:2022	Annex A.3; Annex A.4; Annex A.5; Annex A.7	Both	Supporting	Controles de finalidad, recogida, minimización, uso y divulgación

1. Alcance

1.1 Esta política define los requisitos para recoger, usar, divulgar e intercambiar PII dentro del alcance del PIMS.

1.2 Esta política se aplica a:

1.2.1 la recogida de PII mediante canales directos, indirectos, automatizados, manuales, internos, externos y de terceros;

1.2.2 el uso interno aprobado de PII por procesos, sistemas y aplicaciones de la organización;

1.2.3 el uso secundario de PII para una finalidad nueva o modificada materialmente;

1.2.4 la divulgación externa de PII a destinatarios, socios, autoridades, encargados del tratamiento, subencargados, proveedores y otros terceros;

1.2.5 los acuerdos recurrentes de intercambio de datos y las divulgaciones puntuales;

1.2.6 los contextos de responsable del tratamiento, corresponsable del tratamiento, encargado del tratamiento y subencargado;

1.2.7 REG02 - Inventario de Tratamientos de PII / ROPA, REG08 - Registro de Encargados, Subencargados e Intercambio de Datos, REG09 - Registro de Transferencias Internacionales, y REG12 - Registro de Auditoría, No Conformidad, Acción Correctiva y Mejora.

1.3 Esta política no sustituye a:

1.3.1 PII03 en materia de inventario de tratamientos, base jurídica y titularidad del ROPA;

1.3.2 PII04 en materia de contenido del aviso de privacidad, publicación y control de versiones;

1.3.3 PII05 en materia de operación del consentimiento y las preferencias;

1.3.4 PII06 en materia de gestión de solicitudes de derechos de los interesados;

1.3.5 PII07 en materia de metodología de DPIA y evaluación de riesgos de privacidad;

1.3.6 PII08 en materia de puertas de control de privacidad desde el diseño;

1.3.7 PII10 en materia de ejecución de conservación, supresión y eliminación;

1.3.8 PII11 en materia de gestión de exactitud y calidad;

1.3.9 PII12 en materia de gobierno del ciclo de vida de encargados, subencargados y terceros;

1.3.10 PII13 en materia de selección del mecanismo de transferencia internacional y controles de riesgo de transferencia;

1.3.11 PII14 en materia de seguridad de PII y control de acceso;

1.3.12 PII15 en materia de gestión de incidentes y brechas;

1.3.13 PII18 en materia de gobierno de supervisión, auditoría, no conformidad, acción correctiva y mejora en todo el PIMS.

1.4 A efectos de esta política:

1.4.1 "uso aprobado" significa un uso de PII registrado en REG02 para una actividad de tratamiento, finalidad, categoría de PII, categoría de interesados, propietario de la empresa y rol PIMS aplicable específicos.

1.4.2 "recogida" significa la obtención de PII directamente de un interesado, indirectamente de otra parte, automáticamente desde un sistema o dispositivo, o mediante una fuente de datos interna o externa.

1.4.3 "uso secundario" significa usar PII para una finalidad que no esté ya registrada como finalidad aprobada en REG02 para la actividad de tratamiento correspondiente.

1.4.4 "verificación de compatibilidad" significa una evaluación documentada en REG02 de la finalidad original, la finalidad propuesta, la dependencia de la base jurídica, las categorías de

PII, las expectativas de los interesados, la justificación de minimización, el impacto de divulgación o transferencia, y el enrutamiento a otras políticas PIMS cuando sea necesario.

1.4.5 "divulgación externa" significa poner PII a disposición de una parte externa a la organización o fuera de la cadena documentada de instrucciones del cliente.

1.4.6 "intercambio de datos" significa un acuerdo recurrente o estructurado en virtud del cual PII se divulga, se transfiere, se accede a ella, se intercambia o se pone a disposición de otra parte.

1.4.7 "intercambio recurrente sensible" significa el intercambio recurrente que implique PII de categorías especiales, PII relativa a infracciones penales, PII de menores, registros de alto impacto, intercambio a gran escala, o intercambio externo que implique una ubicación de transferencia registrada en REG09.

2. Propósito

2.1 El propósito de esta política es garantizar que PII se recoja, use, divulgue e intercambie únicamente para finalidades documentadas, aprobadas, limitadas y sujetas a responsabilidad proactiva.

2.2 Esta política permite a la organización demostrar que la recogida y el uso están vinculados a los registros de tratamiento de REG02, que las divulgaciones y los acuerdos de intercambio de datos se registran en REG08, que el enrutamiento de transferencias internacionales está vinculado a REG09, y que las excepciones y no conformidades se gestionan mediante REG12.

3. Objetivos

3.1 Los objetivos de esta política son:

3.1.1 limitar la recogida a la PII necesaria para finalidades documentadas;

3.1.2 garantizar que el uso interno de PII se apruebe antes de que comience el tratamiento;

3.1.3 exigir verificaciones de compatibilidad antes del uso secundario;

3.1.4 exigir aprobación y evidencias antes de la divulgación externa;

3.1.5 mantener evidencias de intercambio de datos en REG08 sin crear un registro separado de intercambio de datos;

3.1.6 enrutar las dependencias de transferencia internacional a REG09 y PII13 sin duplicar los controles de mecanismos de transferencia;

3.1.7 definir la cadencia de revisión del intercambio recurrente;

3.1.8 mantener evidencias preparadas para auditoría sobre recogida, uso, divulgación, intercambio, excepciones y acciones correctivas.

4. Declaraciones de política

4.1 Limitación de la recogida

4.1.1 [Controller] Process Owner / Business Owner DEBE registrar en REG02 la finalidad de la recogida, la fuente o canal, las categorías de PII, las categorías de interesados y los elementos mínimos de datos antes de que comience cualquier nueva actividad de recogida o cambio material de la recogida.

4.1.2 [Controller] Privacy Lead / PIMS Manager DEBE revisar el registro de recogida de REG02 antes de que comience la recogida cuando se añada una nueva categoría de PII, fuente, canal o finalidad.

4.1.3 [Controller] Process Owner / Business Owner DEBE registrar una justificación de necesidad en REG02 para cada elemento de datos de PII antes de recoger dicho elemento.

4.1.4 [Processor] Process Owner / Business Owner DEBE registrar en REG02 la referencia de la instrucción del cliente procedente de REG08 antes de recoger PII por cuenta de un cliente.

4.1.5 [Joint Controller] Process Owner / Business Owner DEBE registrar en REG08 la asignación de responsabilidades de recogida entre corresponsables del tratamiento antes de que comience la recogida conjunta.

4.2 Controles de uso interno aprobado

4.2.1 [Controller] Process Owner / Business Owner DEBE registrar en REG02 las reglas de uso interno aprobado para cada actividad de tratamiento antes de que comience el uso.

4.2.2 [Controller] System Owner / Application Owner DEBE implementar únicamente campos de flujo de trabajo, informes o exportaciones de uso interno que tengan una regla de uso aprobado coincidente en REG02 antes de la liberación a producción.

4.2.3 [Processor] Process Owner / Business Owner DEBE registrar en REG08 la alineación con las instrucciones del cliente antes de usar PII del cliente para cualquier actividad de encargado del tratamiento o subencargado.

4.2.4 [Controller] Privacy Lead / PIMS Manager DEBE revisar las reglas de uso aprobado en REG02 al menos anualmente para cada actividad de tratamiento activa.

4.2.5 [All] Privacy Lead / PIMS Manager DEBE registrar una no conformidad en REG12 en un plazo de cinco días hábiles cuando se identifique un uso interno no documentado de PII.

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

9. Excepciones

9.1.1 [All] Process Owner / Business Owner DEBE registrar una solicitud de excepción en REG12 antes de desviarse de una regla aprobada de recogida, uso, divulgación o intercambio.

9.1.2 [All] Privacy Lead / PIMS Manager DEBE registrar una decisión de aprobación o rechazo en REG12 antes de activar una excepción.

9.1.3 [Conditional] Data Protection Officer / Privacy Advisor DEBE registrar asesoramiento en REG12 antes de aprobar una excepción que implique uso secundario incompatible, intercambio recurrente sensible, conflicto de divulgación jurídicamente vinculante o enrutamiento de transferencias.

9.1.4 [All] Top Management DEBE registrar la aprobación en REG12 antes de activar cualquier excepción con una duración superior a 30 días naturales o que afecte a más de una actividad de tratamiento.

9.1.5 [All] Process Owner / Business Owner DEBE cerrar una excepción en REG12 en la fecha de caducidad o en un plazo de cinco días hábiles después de que finalice la condición de excepción.

10. Aplicación

10.1.1 [All] Privacy Lead / PIMS Manager DEBE registrar la recogida, uso, divulgación o intercambio no aprobados como no conformidad en REG12 en un plazo de cinco días hábiles desde su identificación.

10.1.2 [Controller] Process Owner / Business Owner DEBE suspender la recogida, uso, divulgación o intercambio en un plazo de un día hábil cuando Privacy Lead / PIMS Manager registre en REG12 la ausencia de evidencias aprobadas de REG02 o REG08.

10.1.3 [Processor] Process Owner / Business Owner DEBE registrar una decisión de parada o escalado en REG08 y REG12 en un plazo de un día hábil cuando la PII del cliente se use o divulgue fuera de las instrucciones documentadas.

10.1.4 [All] Top Management DEBE revisar las no conformidades de alto impacto no resueltas relativas a recogida, uso, divulgación o intercambio en REG12 en un plazo de 30 días naturales desde su escalado.

10.1.5 [All] Internal Audit / Compliance Reviewer DEBE verificar en REG12 las evidencias de cierre de acciones correctivas en un plazo de 15 días hábiles después de que Privacy Lead / PIMS Manager marque el cierre.

11. Revisión y mantenimiento

11.1.1 [All] Privacy Lead / PIMS Manager DEBE revisar esta política al menos anualmente y registrar la decisión en REG12.

11.1.2 [All] Privacy Lead / PIMS Manager DEBE revisar esta política en un plazo de 30 días naturales desde un cambio material en el alcance del PIMS, las finalidades del tratamiento, el modelo de intercambio, el enrutamiento de transferencias o la obligación aplicable, y registrar el resultado en REG12.

11.1.3 [All] Process Owner / Business Owner DEBE recertificar los registros activos de REG02 y REG08 al menos anualmente y en un plazo de 30 días naturales desde un cambio material del tratamiento.

11.1.4 [All] Internal Audit / Compliance Reviewer DEBE incluir los controles de PII09 en el muestreo anual de auditoría y registrar la cobertura en REG12.

11.1.5 [All] Privacy Lead / PIMS Manager DEBE actualizar las referencias a políticas relacionadas en REG12 en un plazo de diez días hábiles cuando PII03, PII08, PII10, PII12, PII13, PII14 o PII18 modifiquen el límite operativo de esta política.

12. Políticas relacionadas

12.1 Esta política debe leerse junto con:

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

12.1.2 PII02 - Política de roles, responsabilidades y responsabilidad proactiva de privacidad

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

12.1.4 PII04 - Política de aviso de privacidad y transparencia

12.1.5 PII05 - Política de gestión del consentimiento y las preferencias

12.1.6 PII06 - Política de gestión de derechos de los interesados

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

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

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

12.1.10 PII11 - Política de exactitud y calidad de PII

12.1.11 PII12 - Política de gestión de privacidad de encargados, subencargados y terceros

12.1.12 PII13 - Política de transferencias internacionales de PII

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

12.1.14 PII15 - Política de gestión de incidentes y brechas de PII

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

12.1.16 PII18 - Política de supervisión, auditoría y mejora del PIMS

13. Normas y marcos de referencia

13.1 Esta política está mapeada con las siguientes normas y regulaciones. El mapeo explica cómo la política apoya los requisitos citados e identifica las cláusulas internas que los implementan o respaldan.

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 7.5; Clause 8.1** - Mapeado con registros operativos documentados y control sobre evidencias de recogida, uso aprobado, uso secundario, divulgación, intercambio y

enrutamiento de transferencias. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.2.1; 4.3.1; 4.3.3; 4.3.5; 4.4.1; 4.4.2; 4.5.1; 7.1.1; 7.1.4].

13.2.2 **Clause 9.1; Clause 10.2** - Mapeado con la supervisión, medición, revisión, gestión de excepciones, no conformidad y acción correctiva para controles de recogida, uso, divulgación e intercambio. Addressed by clauses [4.2.4; 4.2.5; 6.1.1; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 9.1.1; 10.1.1; 10.1.5; 11.1.4].

13.2.3 **Annex A.1.2.2; Annex A.1.2.9** - Mapeado con finalidades documentadas del responsable del tratamiento, registros de uso aprobado y evidencias de tratamiento en REG02. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.2.4; 4.3.1; 4.3.2; 4.3.4; 4.5.5].

13.2.4 **Annex A.1.2.3** - Mapeado con la vinculación de base jurídica para el enrutamiento de recogida, uso y uso secundario sin sustituir PII03. Addressed by clauses [4.3.4; 6.1.2; 7.1.1].

13.2.5 **Annex A.1.2.8** - Mapeado con evidencias de responsabilidad de recogida e intercambio entre corresponsables del tratamiento en REG08. Addressed by clauses [4.1.5; 4.4.4; 6.1.4].

13.2.6 **Annex A.1.4.2; Annex A.1.4.3; Annex A.1.4.5** - Mapeado con la limitación de la recogida, la limitación del tratamiento y la justificación de minimización antes de recoger o usar PII. Addressed by clauses [4.1.1; 4.1.3; 4.2.1; 4.2.2; 4.3.1; 4.3.2; 7.1.2].

13.2.7 **Annex A.1.5.2; Annex A.1.5.3** - Mapeado con la vinculación de enrutamiento de transferencias mediante REG09 sin sustituir los controles de mecanismos de transferencia de PII13. Addressed by clauses [4.5.1; 4.5.2; 7.1.4].

13.2.8 **Annex A.1.5.4; Annex A.1.5.5** - Mapeado con registros de transferencias, divulgaciones y acuerdos recurrentes de intercambio de datos en REG08. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.5.1; 4.5.3; 4.5.4; 4.5.5].

13.2.9 **Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.7** - Mapeado con la alineación con instrucciones del cliente del encargado del tratamiento y registros del encargado del tratamiento para límites de recogida, uso y uso secundario. Addressed by clauses [4.1.4; 4.2.3; 4.3.6; 7.1.3; 10.1.3].

13.2.10 **Annex A.2.5.2; Annex A.2.5.3** - Mapeado con la vinculación de enrutamiento de transferencias del encargado del tratamiento mediante REG09 sin sustituir los controles de mecanismos de transferencia de PII13. Addressed by clauses [4.5.1; 4.5.2; 7.1.4].

13.2.11 **Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6** - Mapeado con registros de divulgación del encargado del tratamiento, estado de notificación de solicitudes de divulgación y evidencias de autorización de divulgación en REG08. Addressed by clauses [4.4.5; 4.4.6; 4.4.7; 10.1.3].

13.3 GDPR

13.3.1 **Article 5(1)(b); Article 5(1)(c); Article 5(2)** - Mapeado con evidencias de limitación de la finalidad, minimización de datos y responsabilidad proactiva para recogida, uso, uso secundario, divulgación e intercambio. Addressed by clauses [4.1.1; 4.1.3; 4.2.1; 4.3.1; 4.3.2; 4.4.1; 4.4.2; 4.5.3; 8.1.3; 10.1.1].

13.3.2 Article 6 - Mapeado con la vinculación y el enrutamiento de base jurídica para uso secundario nuevo o incompatible sin sustituir PII03. Addressed by clauses [4.3.4; 6.1.2; 7.1.1].

13.3.3 **Article 24** - Mapeado con el gobierno del responsable del tratamiento, aprobaciones, revisión y medidas de responsabilidad proactiva para recogida, uso, divulgación e intercambio. Addressed by clauses [4.1.2; 4.2.4; 4.3.2; 4.3.3; 4.3.5; 4.4.1; 6.1.1; 9.1.2; 10.1.4; 11.1.1].

13.3.4 **Article 26** - Mapeado con evidencias de responsabilidad de recogida e intercambio entre corresponsables del tratamiento. Addressed by clauses [4.1.5; 4.4.4; 6.1.4].

13.3.5 **Article 28** - Mapeado con la alineación de instrucciones de encargados y subencargados, autorización del cliente y límites de divulgación. Addressed by clauses [4.1.4; 4.2.3; 4.3.6; 4.4.5; 4.4.6; 4.4.7; 7.1.3; 10.1.3].

13.3.6 **Article 30** - Mapeado con registros de tratamiento, destinatarios, divulgación e intercambio en REG02 y REG08. Addressed by clauses [4.1.1; 4.2.1; 4.4.2; 4.4.3; 4.5.1; 4.5.5; 8.1.1; 8.1.2].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6** - Mapeado con especificación de finalidad, limitación de la recogida, minimización de datos, limitación del uso y limitación de la divulgación. Addressed by clauses [4.1.1; 4.1.3; 4.2.1; 4.2.2; 4.3.1; 4.3.2; 4.4.1; 4.4.2; 4.5.3].

13.4.2 **Clause 5.10; Clause 5.12** - Mapeado con responsabilidad proactiva, evidencias de cumplimiento, revisión, gestión de excepciones, muestreo de auditoría y acción correctiva. Addressed by clauses [4.2.4; 4.2.5; 5.1.2; 6.1.1; 8.1.1; 9.1.1; 10.1.1; 11.1.4].

13.5 ISO/IEC 29151:2022

13.5.1 **Annex A.3; Annex A.4; Annex A.5; Annex A.7** - Mapeado con finalidad, limitación de la recogida, minimización, limitación del uso, limitación de la divulgación y soporte de registros de divulgación. Addressed by clauses [4.1.1; 4.1.3; 4.2.1; 4.2.2; 4.4.1; 4.4.2; 4.4.3; 4.4.5; 4.4.6; 4.5.3].