					Introduzca aquí la denominación de la entidad jurídica registrada							
Número de documento: PII17					Título del documento: **Política de Gestión de la Información Documentada y Evidencias del PIMS**							
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 6.1.3	Both	Supporting	Información documentada del SoA
ISO/IEC 27701:2025	Clause 7.5	Both	Primary	Información documentada del PIMS
ISO/IEC 27701:2025	Clause 8.1	Both	Primary	Control de evidencias operativas
ISO/IEC 27701:2025	Clause 9.1	Both	Supporting	Evidencias de seguimiento
ISO/IEC 27701:2025	Clause 9.2	Both	Supporting	Evidencias de auditoría
ISO/IEC 27701:2025	Clause 9.3	Both	Supporting	Evidencias de revisión por la dirección
ISO/IEC 27701:2025	Clause 10.2	Both	Supporting	Evidencias de no conformidades y acciones correctivas
ISO/IEC 27701:2025	Annex A.1.2.9	Controller	Primary	Registros de tratamiento del responsable del tratamiento
ISO/IEC 27701:2025	Annex A.2.2.2	Processor	Supporting	Evidencias de acuerdos e instrucciones del encargado del tratamiento
ISO/IEC 27701:2025	Annex A.3.14	Both	Primary	Protección de registros
GDPR	Article 5(2)	Controller	Supporting	Evidencias de responsabilidad proactiva
GDPR	Article 24	Controller	Supporting	Medidas y evidencias del responsable del tratamiento
GDPR	Article 28	Both	Supporting	Documentación del encargado del tratamiento

GDPR	Article 30	Both	Supporting	Registros de tratamiento
GDPR	Article 32	Both	Supporting	Protección de evidencias
ISO/IEC 29100:2020	Clause 5.12	Both	Supporting	Evidencias de cumplimiento de privacidad
ISO/IEC 29151:2022	Clause 18.1.4	Both	Supporting	Protección de registros
ISO/IEC 27001:2022	Clause 7.5	Both	Supporting	Control de la información documentada
ISO/IEC 27002:2022	Control 5.33	Both	Supporting	Protección de registros
ISO/IEC 27002:2022	Control 5.34	Both	Supporting	Protección de la privacidad y de la PII

1. Alcance

1.1 Esta política define requisitos obligatorios para crear, aprobar, controlar versiones, proteger, conservar, recuperar, traducir, retirar y evidenciar la información documentada del PIMS.

1.2 Esta política se aplica a las políticas del PIMS, registros, aprobaciones documentadas, registros de evidencias, evidencias de auditoría, registros de revisión por la dirección, evidencias de acciones correctivas y traducciones controladas utilizadas para demostrar la conformidad del PIMS.

1.3 Esta política se aplica a contextos de responsable del tratamiento, corresponsable del tratamiento, encargado del tratamiento y subencargado del tratamiento.

1.4 Esta política no crea un registro independiente de control documental. Las evidencias de control de la información documentada se mantienen mediante los objetos de evidencia canónicos del PIMS REG01 a REG12, utilizando REG03 y REG12 para evidencias de aplicabilidad de los controles, auditoría, no conformidades, acciones correctivas y mejora.

2. Propósito

2.1 El propósito de esta política es asegurar que la información documentada del PIMS sea exacta, esté controlada, sea accesible para los usuarios autorizados, esté protegida frente a cambios o divulgaciones no autorizados, se conserve para garantizar su auditabilidad y se retire cuando quede obsoleta.

2.2 Esta política apoya la preparación para la certificación asegurando que las evidencias necesarias para demostrar la conformidad del PIMS puedan localizarse, verificarse, recuperarse y vincularse con las políticas, controles, actividades de tratamiento, riesgos, auditorías y acciones correctivas aplicables.

3. Objetivos

3.1 Los objetivos de esta política son:

3.1.1 definir los requisitos de control de la información documentada del PIMS;

3.1.2 mantener la integridad de las evidencias en REG01 a REG12;

3.1.3 asegurar que la aprobación de políticas y evidencias sea trazable;

3.1.4 asegurar que el historial de versiones y las decisiones de retirada estén documentados;

3.1.5 vincular las evidencias del PIMS con la Declaración de Aplicabilidad y los mapeos de políticas;

3.1.6 controlar el acceso a los documentos del PIMS y a los registros de evidencias;

3.1.7 respaldar el control de versiones multilingüe de políticas y evidencias;

3.1.8 permitir la recuperación oportuna de evidencias de auditoría;

3.1.9 evitar burocracia innecesaria de control documental;

3.1.10 conservar registros preparados para auditorías con fines de certificación, aseguramiento de clientes y mejora continua.

4. Declaraciones de política

4.1 Control de la información documentada del PIMS

4.1.1 [All] El Privacy Lead / PIMS Manager DEBE mantener un índice de información documentada del PIMS en REG12 antes de la publicación inicial del PIMS y, posteriormente, con periodicidad trimestral.

4.1.2 [All] El Process Owner / Business Owner DEBE identificar en REG02 la información documentada requerida para cada actividad de tratamiento de PII de su propiedad antes de que comience la actividad de tratamiento y, posteriormente, con periodicidad anual.

4.1.3 [All] El Privacy Lead / PIMS Manager DEBE vincular las políticas, controles y obligaciones de evidencia aplicables del PIMS con REG03 antes de cada publicación de política y dentro de los 15 días hábiles siguientes a cualquier cambio material en la aplicabilidad de los controles.

4.1.4 [All] El Privacy Lead / PIMS Manager DEBE asignar un nivel de acceso y una clasificación de sensibilidad de las evidencias a cada categoría de información documentada del PIMS en REG12 antes de utilizar la categoría.

4.2 Creación, aprobación, control de versiones y publicación

4.2.1 [All] El Privacy Lead / PIMS Manager DEBE asignar un identificador de documento, propietario, número de versión, estado de aprobación, fecha de entrada en vigor y fecha de revisión en REG12 antes de publicar información documentada del PIMS.

4.2.2 [All] Top Management DEBE aprobar las políticas esenciales del PIMS y los cambios materiales de políticas en REG12 antes de su publicación.

4.2.3 [All] El Privacy Lead / PIMS Manager DEBE aprobar las plantillas de evidencias del PIMS o las secciones integradas de registros en REG12 antes de su uso operativo.

4.2.4 [All] El Privacy Lead / PIMS Manager DEBE registrar el historial de versiones y la justificación de los cambios en REG12 antes de publicar información documentada actualizada del PIMS.

4.2.5 [All] El Privacy Lead / PIMS Manager DEBE registrar la comunicación de los cambios aprobados en la información documentada del PIMS en REG11 dentro de los 30 días posteriores a la publicación.

[... 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] El Process Owner / Business Owner DEBE solicitar en REG12 excepciones de información documentada o de control de evidencias antes de desviarse de esta política.

9.1.2 [All] El Privacy Lead / PIMS Manager DEBE evaluar cada excepción de información documentada o de control de evidencias en REG12 dentro de los 10 días hábiles siguientes a la solicitud.

9.1.3 [All] El Data Protection Officer / Privacy Advisor DEBE registrar asesoramiento en REG12 antes de aprobar cualquier excepción que implique divulgación de evidencias con PII, discrepancias de traducción, conflictos de conservación o limitaciones de evidencias de auditoría.

9.1.4 [All] Top Management DEBE aprobar en REG12 las excepciones de información documentada que superen los 30 días o afecten a la certificación, al tratamiento de alto riesgo o al aseguramiento externo antes de que la excepción surta efecto.

9.1.5 [All] El Privacy Lead / PIMS Manager DEBE establecer en REG12 una fecha de caducidad no superior a 90 días para cada excepción aprobada de información documentada o de control de evidencias.

9.1.6 [All] El Privacy Lead / PIMS Manager DEBE cerrar o reevaluar cada excepción de información documentada o de control de evidencias en REG12 dentro de los cinco días hábiles siguientes a su caducidad.

10. Aplicación

10.1.1 [All] El Privacy Lead / PIMS Manager DEBE registrar la información documentada del PIMS ausente, inexacta, no controlada, obsoleta o no recuperable como una no conformidad en REG12 dentro de los cinco días hábiles siguientes a su identificación.

10.1.2 [All] El Privacy Lead / PIMS Manager DEBE impedir la publicación de información documentada del PIMS cuando falten en REG12 las evidencias requeridas de aprobación, versión, propietario o fecha de entrada en vigor.

10.1.3 [All] El Process Owner / Business Owner DEBE impedir la presentación a auditoría de evidencias de tratamiento cuando falten en REG02 las evidencias requeridas de propietario, fecha, estado o aprobación.

10.1.4 [All] El System Owner / Application Owner DEBE retirar el acceso no autorizado a los repositorios de información documentada del PIMS y registrar la retirada en REG12 dentro de un día hábil desde su identificación.

10.1.5 [All] El Internal Audit / Compliance Reviewer DEBE verificar la eficacia de las acciones correctivas relativas a no conformidades de información documentada en REG12 en la siguiente auditoría programada o dentro de los 60 días posteriores al cierre, lo que ocurra primero.

11. Revisión y mantenimiento

11.1.1 [All] El Privacy Lead / PIMS Manager DEBE revisar esta política anualmente y dentro de los 30 días posteriores a un cambio material en los requisitos de información documentada del PIMS.

11.1.2 [All] El Privacy Lead / PIMS Manager DEBE revisar esta política dentro de los 30 días posteriores a un hallazgo de auditoría mayor, una no conformidad de certificación, un cambio en la plataforma de repositorio o un cambio en el proceso de publicación multilingüe.

11.1.3 [All] El Data Protection Officer / Privacy Advisor DEBE revisar en REG12 los cambios con impacto significativo en la privacidad de esta política antes de la aprobación.

11.1.4 [All] Top Management DEBE aprobar los cambios materiales de esta política en REG12 antes de su publicación.

11.1.5 [All] El Privacy Lead / PIMS Manager DEBE registrar la comunicación de los cambios aprobados de esta política en REG11 dentro de los 30 días posteriores a la publicación.

12. Políticas relacionadas

12.1 Esta política está respaldada por las siguientes políticas relacionadas:

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

12.3 PII02 - Política de Roles, Responsabilidades y Responsabilidad Proactiva de Privacidad

12.4 PII03 - Política de Inventario de Tratamientos de PII y Base Jurídica

12.5 PII04 - Política de Aviso de Privacidad y Transparencia

12.6 PII05 - Política de Gestión del Consentimiento y Preferencias

12.7 PII06 - Política de Gestión de Derechos del Interesado

12.8 PII07 - Política de Evaluación de Riesgos de Privacidad y DPIA

12.9 PII08 - Política de Privacidad desde el Diseño y por Defecto

12.10 PII09 - Política de Recogida, Uso, Divulgación e Intercambio de PII

12.11 PII10 - Política de Conservación, Supresión y Eliminación de PII

12.12 PII11 - Política de Exactitud y Calidad de PII

12.13 PII12 - Política de Gestión de Privacidad de Encargados del Tratamiento, Subencargados del Tratamiento y Terceros

12.14 PII13 - Política de Transferencias Internacionales de PII

12.15 PII14 - Política de Seguridad y Control de Acceso de PII

12.16 PII15 - Política de Gestión de Incidentes y Brechas de Seguridad de PII

12.17 PII16 - Política de Formación, Concienciación y Competencia en Privacidad

12.18 PII18 - Política de Seguimiento, Auditoría y Mejora del PIMS

13. Normas y marcos de referencia

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

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 6.1.3** - Mapeada con el mantenimiento de la Declaración de Aplicabilidad del PIMS, los registros de aplicabilidad de los controles y la vinculación entre políticas y evidencias. Addressed by clauses [4.1.3; 4.3.3; 6.1.3; 7.1.2].

13.2.2 **Clause 7.5** - Mapeada con la identificación de información documentada, aprobación, control de versiones, acceso, recuperación, conservación, retirada, vinculación de versiones de traducción y metadatos de conservación. Addressed by clauses [4.1.1; 4.1.4; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.3.1; 4.3.5; 4.4.1; 4.4.2; 4.4.4; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.6.1; 4.6.2; 4.6.3; 4.6.4].

13.2.3 **Clause 8.1** - Mapeada con las evidencias de planificación y control operacional para registros de tratamiento, plantillas de evidencias, calidad de evidencias operativas y evidencias proporcionadas externamente. Addressed by clauses [4.1.2; 4.2.3; 4.3.2; 7.1.3; 7.1.4].

13.2.4 **Clause 9.1** - Mapeada con el mantenimiento de evidencias documentadas de medición, desempeño de recuperación, deficiencias de evidencias, discrepancias de traducción y finalización de la revisión de accesos al repositorio. Addressed by clauses [8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 8.1.6].

13.2.5 **Clause 9.2** - Mapeada con la recuperación de evidencias de auditoría, el muestreo de auditoría, la trazabilidad de evidencias de auditoría y los hallazgos de auditoría relacionados con el control de información documentada. Addressed by clauses [4.3.4; 4.4.4; 6.1.3; 8.1.3; 10.1.5].

13.2.6 **Clause 9.3** - Mapeada con evidencias de revisión por la dirección, la consideración del control de información documentada en la revisión por la dirección y la revisión por Top Management del desempeño del control de evidencias. Addressed by clauses [6.1.2; 8.1.1; 8.1.2; 11.1.4].

13.2.7 **Clause 10.2** - Mapeada con no conformidades de información documentada, acciones correctivas, gestión de excepciones, cierre y verificación de eficacia. Addressed by clauses [4.3.4; 6.1.4; 9.1.1; 9.1.2; 9.1.4; 9.1.5; 9.1.6; 10.1.1; 10.1.5].

13.2.8 **Annex A.1.2.9** - Mapeada con registros de tratamiento del responsable del tratamiento, registros de responsabilidad proactiva, calidad de evidencias de tratamiento y conservación de evidencias que respaldan las obligaciones del responsable del tratamiento. Addressed by clauses [4.1.2; 4.3.2; 4.5.1; 7.1.3].

13.2.9 **Annex A.2.2.2** - Mapeada con acuerdos del encargado del tratamiento, instrucciones de clientes, evidencias proporcionadas externamente y control de evidencias de relaciones con encargados del tratamiento. Addressed by clauses [5.1.7; 7.1.4].

13.2.10 **Annex A.3.14** - Mapeada con la protección de registros del PIMS frente a pérdida, cambios no autorizados, acceso no autorizado, divulgación no autorizada y eliminación indebida. Addressed by clauses [4.1.4; 4.4.1; 4.4.2; 4.4.3; 4.4.5; 4.5.2; 4.5.4; 4.5.5; 10.1.4].

13.3 GDPR

13.3.1 **Article 5(2)** - Mapeado con evidencias de responsabilidad proactiva, trazabilidad de evidencias, recuperación de evidencias, registros de no conformidades y registros preparados

para auditorías que demuestran el cumplimiento. Addressed by clauses [4.1.1; 4.3.2; 4.3.3; 4.4.4; 4.5.4; 6.1.3; 8.1.3; 10.1.1].

13.3.2 **Article 24** - Mapeado con evidencias de gobernanza del responsable del tratamiento, registros de aprobación, control de políticas, medidas de responsabilidad proactiva, revisión documentada y supervisión por Top Management. Addressed by clauses [4.2.2; 4.3.3; 6.1.2; 9.1.4; 11.1.4].

13.3.3 **Article 28** - Mapeado con documentación de encargado del tratamiento y subencargado del tratamiento, evidencias de instrucciones de clientes, evidencias de procesos proporcionadas externamente y control de divulgación de evidencias. Addressed by clauses [4.4.5; 5.1.7; 7.1.4].

13.3.4 **Article 30** - Mapeado con evidencias de registros de tratamiento, requisitos de calidad de evidencias, referencias de actividades de tratamiento y metadatos de propietario/estado de evidencias de tratamiento. Addressed by clauses [4.1.2; 4.3.2; 7.1.3; 10.1.3].

13.3.5 **Article 32** - Mapeado con la protección de repositorios de evidencias, restricciones de acceso, aprobaciones de acceso, revisión de la protección de repositorios y retirada de accesos no autorizados. Addressed by clauses [4.1.4; 4.4.1; 4.4.2; 4.4.3; 4.4.5; 4.5.5; 10.1.4].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 5.12** - Mapeada con evidencias de cumplimiento de privacidad, recuperación de evidencias de auditoría, trazabilidad de evidencias, soporte para revisión independiente y evidencias de acciones correctivas. Addressed by clauses [4.3.3; 4.4.4; 4.6.3; 6.1.3; 8.1.3; 10.1.5].

13.5 ISO/IEC 29151:2022

13.5.1 **Clause 18.1.4** - Mapeada con la protección de registros relacionados con PII, conservación de registros y controles de acceso y supresión de repositorios de evidencias. Addressed by clauses [4.1.4; 4.4.1; 4.4.2; 4.4.3; 4.5.2; 4.5.5; 10.1.4].

13.6 ISO/IEC 27001:2022

13.6.1 **Clause 7.5** - Mapeada con la identificación de información documentada, aprobación, disponibilidad, protección, control de versiones, conservación, disposición y control de información documentada requerida externamente. Addressed by clauses [4.1.1; 4.2.1; 4.2.4; 4.3.1; 4.4.1; 4.5.1; 4.5.2; 4.5.3; 4.6.1; 4.6.2; 4.6.4].

13.7 ISO/IEC 27002:2022

13.7.1 Control 5.33 - Mapeado con la protección de registros del PIMS frente a pérdida, destrucción, falsificación, acceso no autorizado, divulgación no autorizada y eliminación indebida. Addressed by clauses [4.1.4; 4.4.1; 4.4.2; 4.4.3; 4.4.5; 4.5.5; 10.1.4].

13.7.2 Control 5.34 - Mapeado con la protección de la privacidad y de la PII en información documentada, repositorios de evidencias, divulgaciones y registros con control de acceso. Addressed by clauses [4.1.4; 4.4.2; 4.4.3; 4.4.5; 4.5.5; 6.1.5].