					Introduzca aquí la denominación de la entidad jurídica registrada							
Número de documento: PII10					Título del documento: **Política de conservación, supresión y eliminación 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 reglamentos

Standard / Regulation	Clause / Control / Article	Applicability	Coverage Type	Comment
ISO/IEC 27701:2025	Clause 7.5; Clause 8.1	Both	Primary	Evidencia documentada de conservación y control operacional
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Supervisión, no conformidad y acción correctiva
ISO/IEC 27701:2025	Annex A.1.2.8; Annex A.1.2.9	Controller / Joint Controller	Supporting	Responsabilidad conjunta y registros de tratamiento
ISO/IEC 27701:2025	Annex A.1.3.7; Annex A.1.3.8	Controller	Supporting	Soporte para la ejecución de la supresión
ISO/IEC 27701:2025	Annex A.1.4.6; Annex A.1.4.7; Annex A.1.4.8; Annex A.1.4.9	Controller	Primary	Conservación, supresión y eliminación
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.7	Processor	Supporting	Instrucciones del cliente y registros del encargado del tratamiento
ISO/IEC 27701:2025	Annex A.2.3.2; Annex A.2.4.2; Annex A.2.4.3	Processor	Primary	Soporte de supresión y capacidad de eliminación
ISO/IEC 27701:2025	Annex A.3.20; Annex A.3.21; Annex A.3.24	Both	Supporting	Eliminación de soportes y gestión de copias de seguridad
GDPR	Article 5(1)(e); Article 5(2)	Controller	Primary	Limitación del plazo de conservación y responsabilidad proactiva
GDPR	Article 17	Controller	Supporting	Soporte para la ejecución de la supresión
GDPR	Article 24	Controller	Supporting	Medidas del responsable del tratamiento
GDPR	Article 26	Joint Controller	Supporting	Asignación de responsabilidad conjunta

GDPR	Article 28	Processor	Supporting	Supresión y devolución por el encargado del tratamiento
GDPR	Article 30	Both	Supporting	Registros de actividades de tratamiento
GDPR	Article 32	Both	Supporting	Seguridad del tratamiento y soporte para la eliminación
ISO/IEC 29100:2020	Clause 5.5; Clause 5.6; Clause 5.10	Both	Supporting	Minimización, limitación de la conservación y responsabilidad proactiva
ISO/IEC 29151:2022	Annex A.7; Annex A.7.2	Both	Supporting	Controles de conservación y supresión de archivos temporales
ISO/IEC 27555:2025	Clause 5.1; Clause 5.2; Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6; Clause 5.8	Both	Primary	Marco de supresión y documentación
ISO/IEC 27555:2025	Clause 7.2; Clause 7.3; Clause 8.3	Controller	Primary	Plazos de supresión y reglas de supresión
ISO/IEC 27555:2025	Clause 9.1; Clause 9.2; Clause 9.3; Clause 9.4; Clause 9.5; Clause 9.6; Clause 9.7	Both	Primary	Implantación y excepciones
ISO/IEC 27555:2025	Clause 10.1; Clause 10.2; Clause 10.3	Both	Primary	Responsabilidades y gobernanza de la implantación
ISO/IEC 27557:2022	Clause 4; Clause 5.2; Clause 5.3; Clause 5.4.1	Both	Supporting	Integración de riesgos de privacidad
ISO/IEC 27002:2022	Control 7.14; Control 8.10	Both	Supporting	Eliminación segura y supresión de información

1. Alcance

1.1 Esta política establece los requisitos de la organización para definir, revisar, ejecutar y evidenciar la conservación, supresión, anonimización, desidentificación, devolución, transferencia y eliminación de PII.

1.2 Esta política se aplica a PII tratada en contextos de responsable del tratamiento, corresponsable del tratamiento, encargado del tratamiento y subencargado, incluida PII mantenida en sistemas en producción, archivos, copias de seguridad, réplicas, registros, entornos de preproducción, archivos temporales, registros en papel y soportes de almacenamiento.

1.3 Esta política se aplica a las obligaciones de conservación y supresión derivadas de finalidades del tratamiento aprobadas, registros de base jurídica, instrucciones del responsable del tratamiento, requisitos contractuales, resultados de supresión de interesados, finalización del servicio, eliminación de soportes de almacenamiento y hallazgos de supervisión de PIMS.

1.4 Esta política no define la selección de la base jurídica, el contenido del aviso de privacidad, la gestión completa de los derechos de los interesados, la gobernanza del ciclo de vida del encargado del tratamiento, los mecanismos de transferencia internacional, la arquitectura de controles de seguridad, el flujo de trabajo de respuesta a incidentes ni la metodología de auditoría de PIMS. Estos controles se abordan en políticas relacionadas.

1.5 A efectos de esta política, un cambio material significa cualquier cambio en la finalidad del tratamiento, categoría de PII, categoría de interesado, ubicación de almacenamiento del sistema, ley o contrato de conservación, instrucción del cliente, arquitectura de copia de seguridad, enfoque de archivo, método de eliminación, acuerdo con encargado del tratamiento o subencargado, flujo de trabajo de supresión o alcance de certificación de PIMS que afecte a la conservación, la supresión o la eliminación.

2. Propósito

2.1 El propósito de esta política es asegurar que PII se conserve únicamente para finalidades y plazos aprobados, se suprima o elimine de otro modo cuando ya no sea necesaria, y esté respaldada por evidencias preparadas para auditoría.

2.2 Esta política permite a la organización demostrar limitación del plazo de conservación, gobernanza responsable de la conservación, ejecución controlada de la supresión, eliminación segura, alineación con las instrucciones del encargado del tratamiento, control de excepciones y mejora continua sin crear un registro de supresión separado.

3. Objetivos

3.1 Los objetivos de esta política son:

3.1.1 definir la titularidad de las reglas de conservación y los metadatos de conservación requeridos;

3.1.2 asegurar que las reglas de conservación se registren en el Inventario de Tratamientos de PII / ROPA;

3.1.3 asegurar que las acciones de supresión de encargados del tratamiento y subencargados se basen en la instrucción del cliente o en el contrato;

3.1.4 asegurar que PII caducada se suprima, devuelva, transfiera, anonimice, desidentifique o elimine mediante métodos aprobados;

3.1.5 distinguir sistemas en producción, archivos, copias de seguridad, réplicas, registros, áreas de preproducción y archivos temporales;

3.1.6 asegurar que las evidencias de supresión y eliminación se conserven en objetos de evidencia canónicos de PIMS;

3.1.7 asegurar que las excepciones de conservación tengan un plazo definido, estén aprobadas y se revisen;

3.1.8 integrar la supervisión de conservación y supresión con la no conformidad, la acción correctiva y la mejora.

4. Declaraciones de política

4.1 Asignación de reglas de conservación

4.1.1 [Controller] The Process Owner / Business Owner MUST asignar una regla de conservación documentada a cada actividad de tratamiento del responsable del tratamiento en REG02 antes de que comience la actividad de tratamiento.

4.1.2 [Joint Controller] The Process Owner / Business Owner MUST registrar la asignación de responsabilidades de conservación y supresión del corresponsable del tratamiento en REG02 y REG08 antes de que comience o cambie el tratamiento conjunto.

4.1.3 [Processor] The Vendor / Procurement Owner MUST registrar las instrucciones del cliente relativas a conservación, devolución, transferencia o supresión para las actividades del encargado del tratamiento en REG08 antes de que comience o cambie el tratamiento por el encargado del tratamiento.

4.1.4 [Subprocessor] The Vendor / Procurement Owner MUST registrar los requisitos de traslado a subencargados relativos a conservación, devolución, transferencia o supresión en REG08 antes de la incorporación del subencargado o del cambio de instrucción.

4.1.5 [Both] The Privacy Lead / PIMS Manager MUST verificar que cada regla de conservación aprobada en REG02 incluya el plazo de conservación, el desencadenante inicial, el propietario, la justificación, el destino final y la siguiente fecha de revisión antes de aprobar la regla.

4.1.6 [Both] The Data Protection Officer / Privacy Advisor MUST registrar el asesoramiento en REG02 o REG12 antes de la aprobación de cualquier regla de conservación que implique conflicto legal, tratamiento de alto riesgo, PII de categoría especial o conservación más allá de la finalidad original del tratamiento.

4.2 Revisión y limitación de la conservación

4.2.1 [Both] The Process Owner / Business Owner MUST revisar las reglas de conservación asignadas en REG02 al menos anualmente y dentro de los 30 días posteriores a un cambio material.

4.2.2 [Both] The Privacy Lead / PIMS Manager MUST aprobar o rechazar reglas de conservación nuevas o modificadas en REG02 dentro de los 10 días hábiles posteriores a su presentación.

4.2.3 [Both] The System Owner / Application Owner MUST confirmar el método de aplicación técnico o manual de cada regla de conservación en REG02 antes de la entrada en producción y durante cada revisión anual de conservación.

4.2.4 [Controller] The Process Owner / Business Owner MUST restringir el uso activo de PII conservada únicamente por motivos legales, contractuales, de auditoría o de disputa en REG02 dentro de los cinco días hábiles posteriores a la identificación de la condición de restricción.

4.2.5 [Both] The Privacy Lead / PIMS Manager MUST registrar el riesgo de conservación excesiva no resuelto o la revisión de conservación vencida en REG12 dentro de los cinco días hábiles posteriores a su identificación.

[... 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] The Process Owner / Business Owner MUST presentar cualquier solicitud para conservar PII más allá de la regla de conservación aprobada en REG02 en REG12 antes de que la excepción entre en vigor.

9.1.2 [All] The Privacy Lead / PIMS Manager MUST aprobar o rechazar las solicitudes de excepción de conservación en REG12 antes de que la excepción entre en vigor.

9.1.3 [All] The Data Protection Officer / Privacy Advisor MUST registrar el asesoramiento en REG12 antes de la aprobación de cualquier excepción que implique conflicto legal, denegación de supresión, PII de alto riesgo, intercambio externo o impacto en la certificación.

9.1.4 [All] Top Management MUST aprobar en REG12 las excepciones de conservación que superen los 90 días, afecten a tratamientos de alto riesgo o afecten al aseguramiento externo antes de que la excepción entre en vigor.

9.1.5 [All] The Privacy Lead / PIMS Manager MUST asignar un propietario, una fecha de caducidad, un control compensatorio y una frecuencia de revisión en REG12 para cada excepción aprobada de conservación, supresión o eliminación.

9.1.6 [All] The Privacy Lead / PIMS Manager MUST revisar cada excepción abierta en REG12 al menos mensualmente hasta su cierre.

9.1.7 [All] The Process Owner / Business Owner MUST cerrar o renovar cada excepción en REG12 antes de la fecha de caducidad de la excepción.

10. Aplicación

10.1.1 [All] The Privacy Lead / PIMS Manager MUST registrar una no conformidad en REG12 dentro de los cinco días hábiles posteriores a la identificación de metadatos de conservación faltantes, revisión de conservación vencida, conservación no respaldada, acción de destino final incumplida o evidencia faltante.

10.1.2 [All] The System Owner / Application Owner MUST suspender el nuevo uso en producción de una actividad de tratamiento en REG12 cuando falten los controles técnicos de conservación requeridos antes de la entrada en producción.

10.1.3 [All] The Process Owner / Business Owner MUST detener el uso activo no aprobado de PII conservada únicamente por motivos legales, contractuales, de auditoría o de disputa dentro de los cinco días hábiles y registrar la acción en REG02 o REG12.

10.1.4 [Processor] The Vendor / Procurement Owner MUST escalar las acciones de destino final dirigidas por el cliente que estén vencidas en REG08 y REG12 dentro de los cinco días hábiles posteriores al incumplimiento del plazo contractual.

10.1.5 [Subprocessor] The Vendor / Procurement Owner MUST escalar las evidencias faltantes de destino final del subencargado en REG08 y REG12 dentro de los cinco días hábiles posteriores al incumplimiento del plazo contractual de evidencia.

10.1.6 [All] The Internal Audit / Compliance Reviewer MUST verificar la eficacia de las acciones correctivas para no conformidades de conservación, supresión y eliminación en REG12 en la siguiente auditoría programada o dentro de los 60 días posteriores al cierre, lo que ocurra primero.

10.1.7 [Conditional] The Incident Response Coordinator MUST iniciar la gestión en REG10 cuando una no conformidad de conservación, supresión o eliminación indique un presunto incidente de PII.

11. Revisión y mantenimiento

11.1.1 [All] The Privacy Lead / PIMS Manager MUST revisar esta política anualmente y registrar el resultado de la revisión en REG12.

11.1.2 [All] The Privacy Lead / PIMS Manager MUST revisar esta política dentro de los 30 días posteriores a un cambio material en la ley de conservación, finalidad del tratamiento, instrucción del encargado del tratamiento, arquitectura del sistema, arquitectura de copia de seguridad, enfoque de archivo, flujo de trabajo de supresión, proceso de eliminación o requisitos de certificación de PIMS.

11.1.3 [All] The Data Protection Officer / Privacy Advisor MUST revisar los cambios significativos para la privacidad en esta política en REG12 antes de su aprobación.

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

11.1.5 [All] The Privacy Lead / PIMS Manager MUST registrar la comunicación de los cambios aprobados de la política en REG11 dentro de los 30 días posteriores a su 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 en materia 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 PII06 - Política de gestión de derechos de los interesados

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

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

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

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

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

12.12 PII17 - Política de información documentada y gestión de evidencias de PIMS

12.13 PII18 - Política de supervisión, auditoría y mejora de 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 7.5; Clause 8.1** - Mapeado con evidencias documentadas de conservación, planificación operacional, metadatos de conservación, evidencias de implantación y registros de ejecución del ciclo de vida. Addressed by clauses [4.1.5; 4.2.3; 4.3.5; 4.4.1; 7.1.1; 7.1.3; 7.1.4; 7.1.5; 7.1.6].

13.2.2 **Clause 9.1; Clause 10.2** - Mapeado con supervisión, métricas, revisión de acciones vencidas, no conformidad y acción correctiva para controles de conservación, supresión y eliminación. Addressed by clauses [4.2.5; 6.1.1; 6.1.2; 6.1.3; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 8.1.6; 8.1.7; 10.1.1; 10.1.6].

13.2.3 **Annex A.1.2.8; Annex A.1.2.9** - Mapeado con evidencias de responsabilidad del corresponsable del tratamiento y registros de tratamiento del responsable del tratamiento que contienen metadatos de conservación y destino final. Addressed by clauses [4.1.1; 4.1.2; 4.1.5; 4.2.1; 6.1.4; 7.1.2].

13.2.4 **Annex A.1.3.7; Annex A.1.3.8** - Mapeado con soporte para la ejecución de la supresión, enrutamiento de la evaluación de supresión y vinculación de evidencias de terceros cuando los resultados de supresión requieren acción. Addressed by clauses [4.3.2; 4.3.5; 7.1.8; 10.1.7].

13.2.5 **Annex A.1.4.6; Annex A.1.4.7; Annex A.1.4.8; Annex A.1.4.9** - Mapeado con la supresión o desidentificación al final del tratamiento, la gestión de archivos temporales, la limitación de la conservación y los controles documentados de destino final. Addressed by clauses [4.1.1; 4.1.5; 4.2.1; 4.2.3; 4.2.4; 4.3.1; 4.3.5; 4.3.6; 4.4.2; 4.4.5; 4.5.1; 4.5.2; 4.5.3].

13.2.6 **Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.7** - Mapeado con acuerdos de cliente del encargado del tratamiento, finalidades documentadas del cliente y registros de tratamiento del encargado del tratamiento. Addressed by clauses [4.1.3; 4.1.4; 4.3.3; 4.3.4; 6.1.5; 6.1.6; 7.1.7].

13.2.7 **Annex A.2.3.2; Annex A.2.4.2; Annex A.2.4.3** - Mapeado con el soporte del encargado del tratamiento para obligaciones del cliente, la gestión de archivos temporales y la capacidad de devolución, transferencia o destino final. Addressed by clauses [4.3.3; 4.3.4; 4.4.3; 4.4.4; 4.4.5; 6.1.5; 7.1.7; 10.1.4; 10.1.5].

13.2.8 **Annex A.3.20; Annex A.3.21; Annex A.3.24** - Mapeado con la gestión del ciclo de vida de soportes de almacenamiento, las comprobaciones de reutilización o liberación de equipos y la gestión de copias de seguridad para PII. Addressed by clauses [4.3.6; 4.3.7; 4.4.1; 4.4.3; 4.4.4; 4.4.6; 5.1.4].

13.3 GDPR

13.3.1 **Article 5(1)(e); Article 5(2)** - Mapeado con limitación del plazo de conservación, responsabilidad proactiva sobre la conservación, metadatos de conservación aprobados, evidencia y revisión. Addressed by clauses [4.1.1; 4.1.5; 4.2.1; 4.2.2; 4.2.4; 4.3.1; 4.3.5; 6.1.1; 8.1.1; 8.1.2; 10.1.1].

13.3.2 **Article 17** - Mapeado con enrutamiento del resultado de supresión aprobado, evidencias de ejecución y escalado de incidentes cuando los fallos de control de supresión indiquen un presunto incidente de PII. Addressed by clauses [4.3.2; 4.3.5; 7.1.8; 10.1.7].

13.3.3 **Article 24** - Mapeado con gobernanza del responsable del tratamiento, medidas de responsabilidad proactiva, revisiones, excepciones, acción correctiva y mantenimiento de políticas. Addressed by clauses [4.1.6; 6.1.2; 6.1.3; 9.1.2; 9.1.3; 9.1.4; 11.1.1; 11.1.2; 11.1.4].

13.3.4 **Article 26** - Mapeado con la asignación de responsabilidades de conservación y supresión del corresponsable del tratamiento. Addressed by clauses [4.1.2; 6.1.4].

13.3.5 **Article 28** - Mapeado con la alineación de instrucciones de encargados del tratamiento y subencargados, devolución, transferencia, destino final, evidencias y escalado. Addressed by clauses [4.1.3; 4.1.4; 4.3.3; 4.3.4; 6.1.5; 6.1.6; 7.1.7; 10.1.4; 10.1.5].

13.3.6 **Article 30** - Mapeado con metadatos de conservación y destino final en registros de tratamiento para actividades del responsable del tratamiento y del encargado del tratamiento. Addressed by clauses [4.1.1; 4.1.3; 4.1.5; 4.2.1; 4.4.1; 7.1.2].

13.3.7 **Article 32** - Mapeado con la gestión operacional segura de PII conservada, aplicación técnica, control de soportes de almacenamiento, gestión de copias de seguridad y escalado de incidentes. Addressed by clauses [4.2.3; 4.3.6; 4.4.3; 4.4.4; 4.4.6; 7.1.3; 7.1.4; 7.1.8].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 5.5; Clause 5.6; Clause 5.10** - Mapeado con minimización de datos, limitación de uso y conservación, destino final cuando ya no sea necesaria, restricción de PII conservada y evidencias de responsabilidad proactiva. Addressed by clauses [4.1.5; 4.2.1; 4.2.4; 4.3.1; 4.4.2; 4.5.1; 4.5.2; 6.1.1; 8.1.1; 10.1.1].

13.5 ISO/IEC 29151:2022

13.5.1 **Annex A.7; Annex A.7.2** - Mapeado con conservación limitada en el tiempo, destino final, aplicación automatizada o manual y gestión de archivos temporales. Addressed by clauses [4.2.3; 4.3.1; 4.4.5; 7.1.3; 7.1.4; 7.1.5; 7.1.6].

13.6 ISO/IEC 27555:2025

13.6.1 **Clause 5.1; Clause 5.2; Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6; Clause 5.8** - Mapeado con gobernanza del marco de supresión, agrupación de PII, períodos de conservación y supresión, distinción entre archivos y copias de seguridad, estructura de reglas de supresión y requisitos de procedimiento documentado. Addressed by clauses [4.1.1; 4.1.5; 4.2.1; 4.2.3; 4.4.1; 4.4.2; 4.4.3; 7.1.1; 7.1.2].

13.6.2 **Clause 7.2; Clause 7.3; Clause 8.3** - Mapeado con la especificación del período de supresión regular, la identificación del período de supresión estándar y la asignación de reglas de supresión a actividades de tratamiento de PII. Addressed by clauses [4.1.1; 4.1.5; 4.2.1; 4.2.2; 7.1.1; 7.1.2].

13.6.3 **Clause 9.1; Clause 9.2; Clause 9.3; Clause 9.4; Clause 9.5; Clause 9.6; Clause 9.7** - Mapeado con requisitos de implantación para sistemas, procesos manuales, aspectos de alcance organizativo, encargados del tratamiento, gestión de recuperación y gestión de excepciones. Addressed by clauses [4.3.1; 4.3.3; 4.3.4; 4.4.1; 4.4.3; 4.4.4; 4.4.5; 4.4.6; 7.1.3; 7.1.4; 7.1.5; 7.1.6; 9.1.1; 9.1.5; 9.1.6].

13.6.4 **Clause 10.1; Clause 10.2; Clause 10.3** - Mapeado con asignación de roles, documentación, integración operacional, auditoría y gobernanza de la implantación para conservación, supresión y eliminación. Addressed by clauses [5.1.2; 5.1.4; 5.1.5; 5.1.6; 5.1.7; 5.1.9; 6.1.7; 7.1.3; 7.1.4; 11.1.1; 11.1.2].

13.7 ISO/IEC 27557:2022

13.7.1 **Clause 4; Clause 5.2; Clause 5.3; Clause 5.4.1** - Mapeado con gobernanza de privacidad basada en riesgos, concienciación de la dirección, integración del riesgo de privacidad en el PIMS y contexto de riesgo relacionado con la conservación. Addressed by clauses [4.1.6; 4.2.5; 4.5.4; 6.1.2; 6.1.3; 9.1.3; 9.1.4].

13.8 ISO/IEC 27002:2022

13.8.1 Control 7.14; Control 8.10 - Mapeado con supresión de información, finalización controlada del ciclo de vida, liberación de soportes de almacenamiento y evidencias de destino final. Addressed by clauses [4.3.1; 4.3.5; 4.3.6; 4.3.7; 4.4.4; 4.4.5; 7.1.3; 7.1.4; 10.1.2].