					Introduzca aquí la denominación de la entidad jurídica registrada							
Número de documento: PII16					Título del documento: **Política de Formación, Concienciación y Competencia en Privacidad**							
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 7.2; Clause 7.3	Both	Primary	Competencia y concienciación
ISO/IEC 27701:2025	Clause 7.4; Clause 7.5	Both	Supporting	Comunicación y evidencias documentadas
ISO/IEC 27701:2025	Clause 8.1; Clause 9.1; Clause 10.2	Both	Supporting	Control operacional, medición y mejora
ISO/IEC 27701:2025	Annex A.3.17	Both	Primary	Concienciación, educación y formación sobre el tratamiento de PII
GDPR	Article 5(2); Article 24; Article 28; Article 32; Article 39	Both	Supporting	Responsabilidad proactiva, gobierno de encargados del tratamiento, seguridad y tareas del DPO
ISO/IEC 27001:2022	Clause 7.2; Clause 7.3; Annex A control 6.3	Both	Supporting	Competencia, concienciación y formación
ISO/IEC 27002:2022	Control 6.3	Both	Supporting	Orientación sobre concienciación, educación y formación
ISO/IEC 29100:2020	Clause 5.11; Clause 5.12	Both	Supporting	Seguridad de la información y cumplimiento de privacidad

1. Alcance

1.1 Esta política define los requisitos de la organización para la formación, la concienciación y la competencia en privacidad dentro del Sistema de Gestión de la Privacidad de la Información.

1.2 Esta política se aplica al personal, contratistas, personal temporal, terceros relevantes, encargados del tratamiento, subencargados del tratamiento y otras partes interesadas cuyo trabajo pueda afectar al tratamiento de PII, al desempeño del PIMS, a los derechos de los interesados, al riesgo de privacidad, a la seguridad de la información relacionada con PII, a las instrucciones de encargados del tratamiento, a incidentes de privacidad, a información documentada o a evidencias de cumplimiento.

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

1.4 Esta política cubre:

1.4.1 la identificación de los destinatarios de la formación en privacidad;

1.4.2 la formación de incorporación;

1.4.3 la formación de actualización anual;

1.4.4 la formación basada en roles y activada por eventos;

1.4.5 las evidencias de finalización de la formación;

1.4.6 el escalado por no finalización;

1.4.7 la revisión de la eficacia de la formación;

1.4.8 las evidencias de aseguramiento de la formación de encargados del tratamiento, subencargados del tratamiento y terceros.

1.5 Esta política no crea una matriz de formación, un panel de formación, un registro de recursos humanos, un registro de competencias, un registro disciplinario ni un registro de formación de clientes separados. Las asignaciones de formación, las finalizaciones, los recordatorios, las evidencias de competencia y las evidencias de concienciación se registran en REG11, y las excepciones, escalados, no conformidades, acciones correctivas y evidencias de revisión se registran en REG12. Las evidencias de aseguramiento de la formación de encargados del tratamiento, subencargados del tratamiento y terceros se registran en REG08 cuando sea pertinente.

1.6 Esta política no duplica:

1.6.1 la asignación de responsabilidad proactiva por rol en PII02;

1.6.2 el inventario de tratamientos y los requisitos de base jurídica en PII03;

1.6.3 la metodología de riesgos de privacidad y DPIA en PII07;

1.6.4 las puertas de control de privacidad desde el diseño en PII08;

1.6.5 el gobierno del ciclo de vida de encargados del tratamiento en PII12;

1.6.6 la operación de seguridad de PII y control de acceso en PII14;

1.6.7 el flujo de trabajo de incidentes y brechas de seguridad de PII en PII15;

1.6.8 el gobierno de la información documentada en PII17;

1.6.9 la supervisión, la auditoría interna y el gobierno de la mejora en PII18.

2. Propósito

2.1 El propósito de esta política es asegurar que las personas cuyo trabajo afecta al tratamiento de PII comprendan sus responsabilidades de privacidad, completen la formación adecuada con una cadencia definida, mantengan la competencia pertinente para su rol y generen evidencias auditables de formación, concienciación y escalado.

2.2 Esta política respalda una implantación coherente del PIMS mediante el uso de REG11 como objeto principal de evidencias de formación y concienciación, y de REG08, REG10 y REG12 como objetos de evidencias de apoyo.

3. Objetivos

3.1 Los objetivos de esta política son:

3.1.1 definir los destinatarios de la formación en privacidad;

3.1.2 definir los requisitos de formación de incorporación;

3.1.3 definir los requisitos de formación de actualización anual;

3.1.4 definir los requisitos de formación en privacidad basada en roles;

3.1.5 registrar las evidencias de finalización en REG11;

3.1.6 escalar la no finalización mediante REG12;

3.1.7 mantener en REG08 las evidencias de aseguramiento de la formación de encargados del tratamiento, subencargados del tratamiento y terceros cuando sea pertinente;

3.1.8 revisar la eficacia de la formación sin crear métricas excesivas ni registros duplicados;

3.1.9 asegurar que el contenido de la formación permanezca alineado con las políticas PIMS vigentes y las obligaciones materiales de privacidad.

4. Declaraciones de política

4.1 Destinatarios y asignación de la formación

4.1.1 [All] The Privacy Lead / PIMS Manager MUST definir en REG11 las categorías de destinatarios de la formación del PIMS antes de que comience cada ciclo anual de formación.

4.1.2 [All] The Process Owner / Business Owner MUST identificar en REG11 al personal cuyas funciones impliquen tratamiento de PII antes de la incorporación, la asignación de rol o un cambio material de funciones.

4.1.3 [Conditional] The System Owner / Application Owner MUST identificar en REG11 a los usuarios que requieran formación de privacidad sobre sistemas PII, acceso privilegiado o administración antes de habilitar o modificar materialmente el acceso.

4.1.4 [Joint Controller] The Privacy Lead / PIMS Manager MUST registrar en REG11 o REG08 la asignación de responsabilidades de formación entre corresponsables del tratamiento antes de que comience o cambie materialmente la actividad de tratamiento conjunto.

4.1.5 [Conditional] The Data Protection Officer / Privacy Advisor MUST identificar en REG11 las necesidades reforzadas de formación en privacidad antes de asignar formación a roles que gestionen tratamientos de alto riesgo, PII de categorías especiales, derechos de los interesados, DPIAs, transferencias internacionales o evaluación de brechas de seguridad.

4.1.6 [All] The Privacy Lead / PIMS Manager MUST registrar en REG11 los destinatarios de la formación asignados, el tipo de formación, la fecha de finalización requerida y el propietario de las evidencias antes de que comience cada ciclo anual de formación.

4.2 Cadencia de formación de incorporación y anual

4.2.1 [All] The Privacy Lead / PIMS Manager MUST asignar en REG11 formación básica de concienciación en privacidad dentro de los 10 días laborables posteriores a la incorporación para el personal con acceso a PII o responsabilidades PIMS.

4.2.2 [All] The Process Owner / Business Owner MUST asegurar que el personal asignado complete en REG11 la formación de privacidad de incorporación antes de que se apruebe el acceso no supervisado a PII o dentro de los 30 días posteriores a la incorporación, lo que ocurra primero.

4.2.3 [All] The Privacy Lead / PIMS Manager MUST asignar en REG11 la formación anual de actualización en privacidad al menos una vez cada 12 meses.

4.2.4 [All] The Process Owner / Business Owner MUST confirmar en REG11 el estado de finalización de la actualización anual del personal asignado antes de la fecha límite anual publicada.

4.2.5 [Conditional] The Privacy Lead / PIMS Manager MUST asignar en REG11 formación de actualización específica dentro de los 30 días posteriores a un cambio material de la política de privacidad, un cambio material de proceso del PIMS, un hallazgo de auditoría, un fallo recurrente de formación o una lección pertinente de un incidente 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] The Process Owner / Business Owner MUST registrar en REG12 una solicitud de excepción de formación en privacidad antes de que se prorrogue una fecha límite de finalización requerida.

9.1.2 [All] The Privacy Lead / PIMS Manager MUST aprobar o rechazar en REG12 las solicitudes de excepción de formación en privacidad antes de que la excepción se active.

9.1.3 [Conditional] The Data Protection Officer / Privacy Advisor MUST asesorar sobre las excepciones de formación en REG12 antes de la aprobación cuando la excepción afecte a tratamientos de alto riesgo, PII de categorías especiales, gestión de derechos, gestión de incidentes, transferencias internacionales o evidencias de certificación.

9.1.4 [Conditional] Top Management MUST aprobar en REG12 las excepciones de formación en privacidad antes de su activación cuando la excepción afecte a la no finalización repetida, al acceso privilegiado a PII, al tratamiento de PII de alto impacto o a evidencias de cara a autoridades reguladoras.

9.1.5 [All] The Privacy Lead / PIMS Manager MUST definir en REG12 el propietario de la excepción, la fecha de caducidad, la acción compensatoria y la fecha de revisión antes de aprobar cualquier excepción de formación en privacidad.

9.1.6 [All] The Process Owner / Business Owner MUST cerrar o renovar en REG12 las excepciones aprobadas de formación en privacidad 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 de formación en REG12 dentro de los cinco días laborables cuando las evidencias de formación obligatoria en privacidad falten, estén incompletas, estén vencidas o no sean trazables hasta REG11.

10.1.2 [All] The Process Owner / Business Owner MUST asegurar que la formación obligatoria en privacidad vencida se complete o se escale en REG11 o REG12 dentro de los 10 días laborables posteriores al registro del estado vencido.

10.1.3 [Conditional] The System Owner / Application Owner MUST restringir en REG12 el nuevo acceso de alto impacto a PII cuando la formación de incorporación o la formación en privacidad basada en roles requerida siga incompleta después del escalado.

10.1.4 [Processor] The Vendor / Procurement Owner MUST escalar en REG08 y REG12 las evidencias ausentes de aseguramiento de la formación de encargados del tratamiento, subencargados del tratamiento o plantilla externa dentro de los cinco días laborables posteriores a su identificación.

10.1.5 [Conditional] The Incident Response Coordinator MUST vincular las medidas de aplicación relacionadas con la formación a REG10 dentro de un día laborable cuando el fallo de formación haya contribuido a un incidente de PII sospechado o confirmado.

10.1.6 [All] The Internal Audit / Compliance Reviewer MUST verificar las evidencias de cierre de las acciones correctivas de formación 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] The Privacy Lead / PIMS Manager MUST revisar esta política y el contenido de formación al menos anualmente y registrar el resultado de la revisión en REG11 o 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 el alcance del PIMS, la legislación de privacidad, las actividades de tratamiento, el modelo de roles, las lecciones de incidentes, los hallazgos de auditoría o los resultados de eficacia de la formación.

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

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

11.1.5 [All] The Privacy Lead / PIMS Manager MUST actualizar en REG11 el contenido de formación y las evidencias de asignación dentro de los 30 días posteriores a un cambio material aprobado de la política.

12. Políticas relacionadas

12.1 Esta política debe leerse junto con:

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 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 de los Interesados;

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

12.13 PII13 - Política de Transferencias Internacionales de PII;

12.14 PII14 - Política de Seguridad de PII y Control de Acceso;

12.15 PII15 - Política de Gestión de Incidentes y Brechas de Seguridad de PII;

12.16 PII17 - Política de Gestión de Información Documentada y Evidencias del PIMS;

12.17 PII18 - Política de Supervisión, Auditoría y Mejora del PIMS.

13. Normas y marcos de referencia

13.1 ISO/IEC 27701:2025 - Clause 7.2; Clause 7.3; Clause 7.4. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.1.4; 4.1.5; 4.1.6; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 4.3.6; 5.1.2; 5.1.3; 5.1.4; 5.1.5; 7.1.1; 7.1.2; 7.1.3; 11.1.1; 11.1.5].

13.2 ISO/IEC 27701:2025 - Clause 7.5; Clause 9.1; Clause 10.2. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 4.6.1; 4.6.4; 4.6.5; 6.1.1; 6.1.2; 6.1.3; 6.1.5; 7.1.7; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 9.1.1; 9.1.2; 9.1.5; 10.1.1; 10.1.2; 10.1.6; 11.1.1; 11.1.2; 11.1.4].

13.3 ISO/IEC 27701:2025 - Annex A.3.17. Addressed by clauses [4.1.6; 4.2.1; 4.2.3; 4.2.5; 4.3.1; 4.3.5; 4.3.6; 4.4.1; 4.4.3; 4.5.5; 4.6.1; 4.6.2; 4.6.3; 5.1.2; 5.1.4; 5.1.8; 7.1.1; 7.1.2; 7.1.6; 8.1.5; 11.1.5].

13.4 GDPR - Article 5(2); Article 24; Article 28; Article 32; Article 39. Addressed by clauses [4.1.3; 4.1.5; 4.2.1; 4.2.2; 4.2.3; 4.2.5; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 4.3.6; 4.4.1; 4.4.4; 4.5.3; 4.5.4; 4.5.5; 5.1.1; 5.1.3; 5.1.7; 6.1.2; 6.1.3; 6.1.4; 7.1.4; 7.1.5; 9.1.3; 9.1.4; 10.1.3; 10.1.4; 10.1.5; 11.1.3].

13.5 ISO/IEC 27001:2022 - Clause 7.2; Clause 7.3; Annex A control 6.3. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.1.6; 4.2.1; 4.2.3; 4.3.1; 4.3.5; 4.4.1; 4.4.3; 4.5.1; 4.5.2; 4.6.1; 4.6.4; 5.1.2; 5.1.4; 6.1.1; 7.1.1; 7.1.2; 8.1.1; 8.1.2; 8.1.3; 11.1.1].

13.6 ISO/IEC 27002:2022 - Control 6.3. Addressed by clauses [4.1.6; 4.2.1; 4.2.3; 4.2.5; 4.3.1; 4.3.5; 4.3.6; 4.4.1; 4.4.3; 4.5.5; 4.6.1; 4.6.4; 5.1.2; 5.1.4; 5.1.8; 7.1.1; 7.1.2; 7.1.6; 8.1.5; 10.1.2].

13.7 ISO/IEC 29100:2020 - Clause 5.11; Clause 5.12. Addressed by clauses [4.1.5; 4.2.5; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 4.3.6; 4.4.1; 4.5.5; 4.6.4; 4.6.5; 5.1.3; 6.1.2; 6.1.3; 6.1.5; 8.1.5; 9.1.3; 10.1.1; 10.1.6; 11.1.2].