					Introduzca aquí la denominación de la entidad jurídica registrada							
Número de documento: PII02					Título del documento: **Política de roles, responsabilidades y responsabilidad proactiva en materia de 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 4.1	Both	Primary	Contexto de roles del PIMS
ISO/IEC 27701:2025	Clause 5.1	Both	Primary	Liderazgo y responsabilidad proactiva
ISO/IEC 27701:2025	Clause 5.3	Both	Primary	Roles, responsabilidades y autoridades del PIMS
ISO/IEC 27701:2025	Clause 7.2	Both	Primary	Competencia del rol
ISO/IEC 27701:2025	Clause 7.3	Both	Primary	Concienciación sobre el rol
ISO/IEC 27701:2025	Clause 7.4	Both	Supporting	Comunicación del rol
ISO/IEC 27701:2025	Clause 7.5	Both	Primary	Información documentada sobre roles
ISO/IEC 27701:2025	Clause 8.1	Both	Primary	Titularidad del control operacional
ISO/IEC 27701:2025	Clause 9.2	Both	Supporting	Rol de auditoría independiente
ISO/IEC 27701:2025	Clause 9.3	Both	Supporting	Revisión por la dirección de la responsabilidad proactiva
ISO/IEC 27701:2025	Clause 10.2	Both	Supporting	No conformidad relacionada con roles y acción correctiva
ISO/IEC 27701:2025	Annex A.1.2.7	Controller	Supporting	Responsabilidad sobre contratos con encargados del tratamiento
ISO/IEC 27701:2025	Annex A.1.2.8	Joint Controller	Primary	Roles y responsabilidades del corresponsable del tratamiento
ISO/IEC 27701:2025	Annex A.1.2.9	Controller	Primary	Registros de responsabilidad proactiva

ISO/IEC 27701:2025	Annex A.2.2.2	Processor	Primary	Acuerdos con clientes e instrucciones del encargado del tratamiento
ISO/IEC 27701:2025	Annex A.2.2.3	Processor	Supporting	Alineación de finalidades del encargado del tratamiento
GDPR	Article 5(2)	Controller	Supporting	Evidencias de responsabilidad proactiva
GDPR	Article 24	Controller	Supporting	Responsabilidad y medidas del responsable del tratamiento
GDPR	Article 26	Joint Controller	Supporting	Acuerdos de corresponsabilidad del tratamiento
GDPR	Article 28	Both	Supporting	Gobernanza del encargado del tratamiento e instrucciones
GDPR	Article 30	Both	Supporting	Registros de tratamiento y evidencias de responsabilidad
GDPR	Article 37	Conditional	Referenced	Designación del DPO cuando sea aplicable
GDPR	Article 38	Conditional	Supporting	Posición e independencia del DPO cuando sea aplicable
GDPR	Article 39	Conditional	Supporting	Tareas del DPO cuando sea aplicable
ISO/IEC 29100:2020	Clause 4.1; Clause 4.2	Both	Supporting	Actores y roles del marco de privacidad
ISO/IEC 29100:2020	Clause 5.12	Both	Supporting	Responsabilidad proactiva sobre el cumplimiento de privacidad

ISO/IEC 29151:2022	Clause 6.1.2; Clause 6.1.3	Both	Supporting	Roles de protección de PII y segregación
ISO/IEC 27002:2022	Control 5.2	Both	Supporting	Roles y responsabilidades de seguridad de la información
ISO/IEC 27002:2022	Control 5.3	Both	Supporting	Segregación de funciones

1. Alcance

1.1 Esta política define el modelo de roles del PIMS, la estructura de responsabilidad proactiva, las reglas de asignación de responsabilidades, las reglas de combinación de roles, las expectativas de escalado y los requisitos de evidencias para la gobernanza de la privacidad.

1.2 Esta política se aplica al personal, funciones, sistemas, proveedores, encargados del tratamiento, subencargados y relaciones de corresponsabilidad del tratamiento que participan en el tratamiento de PII o influyen en él dentro del alcance del PIMS.

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

1.4 Esta política no crea nuevos cargos organizativos.

1.5 Esta política define roles canónicos del PIMS que pueden asignarse al personal o a las funciones existentes, siempre que se documenten los requisitos de asignación de roles, competencia, independencia y conflicto de intereses.

2. Propósito

2.1 El propósito de esta política es asegurar que las responsabilidades del PIMS estén claramente asignadas, comprendidas, comunicadas, evidenciadas, revisadas y mejoradas.

2.2 Esta política permite a la organización demostrar responsabilidad proactiva respecto de la gobernanza de la privacidad, la titularidad del tratamiento de PII, la determinación del rol de responsable del tratamiento y encargado del tratamiento, la asignación de responsabilidades entre corresponsables del tratamiento, la gestión de instrucciones del encargado del tratamiento, la responsabilidad de privacidad de proveedores, la revisión independiente y el escalado basado en roles.

3. Objetivos

3.1 Los objetivos de esta política son:

3.1.1 definir los roles canónicos del PIMS utilizados en el conjunto de políticas del PIMS;

3.1.2 asegurar que cada responsabilidad material del PIMS tenga asignado un rol responsable;

3.1.3 respaldar la responsabilidad proactiva del responsable del tratamiento, del corresponsable del tratamiento, del encargado del tratamiento y del subencargado;

3.1.4 permitir una combinación práctica de roles para pequeñas y medianas organizaciones, controlando al mismo tiempo los conflictos de intereses;

3.1.5 preservar la revisión independiente por parte de Internal Audit / Compliance Reviewer;

3.1.6 asegurar que las asignaciones de roles y los cambios de rol se registren en objetos de evidencia canónicos;

3.1.7 asegurar que los titulares de las funciones del PIMS reciban la comunicación y concienciación adecuadas;

3.1.8 asegurar que las brechas, conflictos y no conformidades relacionados con roles se escalen y corrijan.

4. Declaraciones de política

4.1 Modelo y asignación de roles del PIMS

4.1.1 [All] Top Management DEBE aprobar el modelo canónico de roles del PIMS en REG01 antes de la implementación inicial del PIMS y posteriormente con periodicidad anual.

4.1.2 [All] Privacy Lead / PIMS Manager DEBE mantener las asignaciones nominales de roles del PIMS en REG01 antes de la implementación del PIMS y dentro de los 10 días hábiles siguientes a cambios de personal u organizativos.

4.1.3 [All] Privacy Lead / PIMS Manager DEBE documentar el alcance de responsabilidad y el nivel de autoridad de cada rol del PIMS asignado en REG01 antes de que la asignación surta efecto.

4.1.4 [All] Process Owner / Business Owner DEBE asignar un propietario responsable para cada actividad de tratamiento de PII en REG02 antes de que comience la actividad de tratamiento.

4.1.5 [All] System Owner / Application Owner DEBE documentar el propietario del sistema responsable de cada sistema que trate PII en REG02 antes de la entrada en producción del sistema.

4.1.6 [All] Vendor / Procurement Owner DEBE documentar el responsable de la relación para cada encargado del tratamiento, subencargado, intercambio de datos con terceros o relación de corresponsabilidad del tratamiento en REG08 antes de la incorporación o aprobación del acuerdo.

4.2 Combinación de roles, segregación e independencia

4.2.1 [All] Privacy Lead / PIMS Manager DEBE documentar cada combinación de roles del PIMS en REG01 antes de que la combinación de roles surta efecto.

4.2.2 [All] Top Management DEBE aprobar en REG01, antes de la asignación, las combinaciones de roles que involucren a Privacy Lead / PIMS Manager, Data Protection Officer / Privacy Advisor, Information Security Lead, Incident Response Coordinator o Internal Audit / Compliance Reviewer.

4.2.3 [All] Internal Audit / Compliance Reviewer DEBE documentar en REG12 su independencia respecto del proceso del PIMS objeto de revisión antes de que comience cada auditoría del PIMS o revisión de cumplimiento.

4.2.4 [All] Privacy Lead / PIMS Manager DEBE registrar en REG12 los controles compensatorios para conflictos de segregación inevitables antes de aprobar una combinación de roles.

4.2.5 [All] Data Protection Officer / Privacy Advisor DEBE registrar en REG12 las preocupaciones sobre independencia del rol o conflictos de intereses dentro de los cinco días hábiles siguientes 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] Process Owner / Business Owner DEBE solicitar en REG12 una excepción de responsabilidad proactiva de roles antes de operar una actividad de tratamiento de PII sin un rol asignado requerido.

9.1.2 [All] Privacy Lead / PIMS Manager DEBE evaluar en REG12 el impacto y la mitigación de cada excepción de responsabilidad proactiva de roles dentro de los 10 días hábiles siguientes a la solicitud.

9.1.3 [All] Top Management DEBE aprobar en REG12 las excepciones de responsabilidad proactiva de roles que superen 30 días o afecten a tratamientos de alto riesgo antes de que la excepción surta efecto.

9.1.4 [All] Privacy Lead / PIMS Manager DEBE establecer en REG12 una fecha de caducidad que no exceda de 90 días para cada excepción de responsabilidad proactiva de roles aprobada antes de la aprobación.

9.1.5 [All] Privacy Lead / PIMS Manager DEBE cerrar o reevaluar cada excepción de responsabilidad proactiva de roles en REG12 dentro de los cinco días hábiles siguientes a su caducidad.

10. Aplicación

10.1.1 [All] Privacy Lead / PIMS Manager DEBE registrar en REG12 como no conformidades las asignaciones de roles del PIMS inexistentes, inexactas u obsoletas dentro de los cinco días hábiles siguientes a su identificación.

10.1.2 [All] Top Management DEBE exigir acciones correctivas en REG12 dentro de los 15 días hábiles siguientes para fallos de responsabilidad proactiva repetidos o prolongados.

10.1.3 [All] Process Owner / Business Owner DEBE impedir la entrada en producción de tratamientos de PII nuevos o modificados cuando las evidencias requeridas de roles y responsabilidad proactiva no consten en REG02 o REG08.

10.1.4 [All] Internal Audit / Compliance Reviewer DEBE verificar la eficacia de las acciones correctivas para no conformidades de responsabilidad proactiva de roles en REG12 en la siguiente auditoría programada o dentro de los 60 días siguientes al cierre, lo que ocurra primero.

11. Revisión y mantenimiento

11.1.1 [All] Privacy Lead / PIMS Manager DEBE revisar esta política anualmente y dentro de los 30 días siguientes a un cambio material del modelo de roles del PIMS.

11.1.2 [All] Data Protection Officer / Privacy Advisor DEBE revisar en REG12 los cambios propuestos a esta política para determinar su impacto en los roles de privacidad antes de la aprobación.

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

11.1.4 [All] Privacy Lead / PIMS Manager DEBE actualizar REG01 y REG11 dentro de los 15 días hábiles siguientes a los cambios aprobados en los roles, responsabilidades o requisitos de comunicación del PIMS.

12. Políticas relacionadas

12.1 Esta política se apoya en las siguientes políticas relacionadas:

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

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

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

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

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

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

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

12.9 PII16 - Política de formación, concienciación y competencia en privacidad

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

12.11 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 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 4.1** - Mapeada a la determinación del contexto de roles del PIMS, la aplicabilidad del responsable del tratamiento y del encargado del tratamiento, la titularidad del tratamiento y los registros de responsabilidad sobre relaciones. Addressed by clauses [4.3.5; 5.1.5; 5.1.7; 7.1.2].

13.2.2 **Clause 5.1** - Mapeada a la aprobación por Top Management, la supervisión de la responsabilidad proactiva, la revisión anual por la dirección, las métricas de responsabilidad proactiva y la acción correctiva ante fallos de roles. Addressed by clauses [4.1.1; 4.2.2; 5.1.1; 6.1.1; 8.1.6; 10.1.2; 11.1.3].

13.2.3 **Clause 5.3** - Mapeada a la asignación, documentación, comunicación y mantenimiento de roles, responsabilidades y autoridades del PIMS, titularidad de sistemas, titularidad del tratamiento, titularidad de relaciones con proveedores, titularidad del escalado de incidentes y responsabilidad de revisión independiente. Addressed by clauses [4.1.2; 4.1.3; 4.1.4; 4.1.5; 4.1.6; 4.4.2; 4.4.3; 5.1.2; 5.1.3; 5.1.4; 5.1.5; 5.1.6; 5.1.7; 5.1.8; 5.1.9].

13.2.4 **Clause 7.2** - Mapeada a las evidencias de competencia y concienciación específicas del rol para las responsabilidades asignadas del PIMS. Addressed by clauses [7.1.4; 8.1.5].

13.2.5 **Clause 7.3** - Mapeada a la concienciación sobre las responsabilidades asignadas del PIMS, las evidencias de reconocimiento y los informes anuales de concienciación de roles. Addressed by clauses [4.5.1; 4.5.2; 7.1.4; 8.1.5].

13.2.6 **Clause 7.4** - Mapeada a la comunicación de asignaciones de roles, cambios de rol, escalados e información de traspaso de rol. Addressed by clauses [4.5.1; 4.5.4; 6.1.5; 7.1.6].

13.2.7 **Clause 7.5** - Mapeada a la información documentada sobre asignaciones de roles del PIMS, alcances de responsabilidad, niveles de autoridad, conservación anual de evidencias y mantenimiento de la matriz de roles. Addressed by clauses [4.1.2; 4.1.3; 4.5.3; 7.1.1; 11.1.4].

13.2.8 **Clause 8.1** - Mapeada a la titularidad del control operacional de actividades de tratamiento, sistemas, proveedores, encargados del tratamiento, subencargados, relaciones de corresponsabilidad del tratamiento y controles de entrada en producción. Addressed by clauses [4.1.4; 4.1.5; 4.1.6; 7.1.2; 7.1.3; 7.1.5; 10.1.3].

13.2.9 **Clause 9.2** - Mapeada a la auditoría independiente y la revisión de cumplimiento de evidencias de asignación de roles, evidencias de combinación de roles, evidencias de independencia, hallazgos y cierre de acciones correctivas. Addressed by clauses [4.2.3; 5.1.9; 6.1.4; 8.1.4; 10.1.4].

13.2.10 **Clause 9.3** - Mapeada a la revisión por la dirección de la completitud de asignación de roles del PIMS, conflictos de roles, excepciones, métricas de responsabilidad proactiva y resultados de revisión de responsabilidad proactiva. Addressed by clauses [5.1.1; 6.1.1; 8.1.6; 11.1.1].

13.2.11 **Clause 10.2** - Mapeada al escalado, registro de no conformidades, acción correctiva, cierre de excepciones y verificación de eficacia para cuestiones de responsabilidad proactiva de roles. Addressed by clauses [4.2.5; 4.4.5; 6.1.5; 9.1.5; 10.1.1; 10.1.2; 10.1.4].

13.2.12 **Annex A.1.2.7** - Mapeada a la asignación y documentación de la responsabilidad sobre contratos con encargados del tratamiento y el escalado de responsabilidades de terceros antes de la aprobación o renovación del contrato. Addressed by clauses [4.1.6; 4.4.4; 5.1.7; 7.1.3].

13.2.13 **Annex A.1.2.8** - Mapeada a la documentación de la asignación de responsabilidades entre corresponsables del tratamiento y las evidencias de responsabilidad sobre la relación antes de que comience el tratamiento en corresponsabilidad. Addressed by clauses [4.3.2; 5.1.7; 7.1.3; 8.1.3].

13.2.14 **Annex A.1.2.9** - Mapeada al mantenimiento de registros de responsabilidad proactiva para la titularidad del tratamiento como responsable del tratamiento, la clasificación de roles y la titularidad de evidencias. Addressed by clauses [4.3.1; 4.3.5; 4.5.3; 8.1.1].

13.2.15 **Annex A.2.2.2** - Mapeada a la responsabilidad sobre acuerdos del encargado del tratamiento con clientes, la titularidad de instrucciones del cliente y las evidencias de relación con el encargado del tratamiento. Addressed by clauses [4.3.3; 5.1.7; 7.1.3; 8.1.3].

13.2.16 **Annex A.2.2.3** - Mapeada a la alineación de finalidad e instrucciones del encargado del tratamiento mediante la titularidad de instrucciones del cliente y la verificación del rol de responsable del tratamiento/encargado del tratamiento. Addressed by clauses [4.3.3; 4.3.5; 5.1.7].

13.3 GDPR

13.3.1 **Article 5(2)** - Mapeado a las evidencias de responsabilidad proactiva de asignaciones de roles, titularidad del tratamiento, revisiones de roles, no conformidades y hallazgos de auditoría. Addressed by clauses [4.5.3; 6.1.2; 8.1.1; 10.1.1].

13.3.2 **Article 24** - Mapeado a la responsabilidad del responsable del tratamiento, la titularidad responsable del tratamiento, la supervisión por Top Management, la revisión anual y las medidas de responsabilidad proactiva. Addressed by clauses [4.1.1; 4.3.1; 5.1.1; 6.1.1; 8.1.6].

13.3.3 **Article 26** - Mapeado a la documentación de la asignación de responsabilidades entre corresponsables del tratamiento y las evidencias de responsabilidad sobre la relación antes de que comience el tratamiento en corresponsabilidad. Addressed by clauses [4.3.2; 5.1.7; 7.1.3; 8.1.3].

13.3.4 **Article 28** - Mapeado a la asignación de responsabilidades del encargado del tratamiento y subencargado, la titularidad de instrucciones del cliente, la responsabilidad contractual y las vías de escalado de terceros. Addressed by clauses [4.3.3; 4.3.4; 4.4.4; 5.1.7; 7.1.3].

13.3.5 **Article 30** - Mapeado a los registros de tratamiento, la titularidad del tratamiento, la clasificación de roles del PIMS y la verificación del rol de responsable del tratamiento/encargado del tratamiento. Addressed by clauses [4.1.4; 4.3.1; 4.3.5; 8.1.1].

13.3.6 **Article 37** - Mapeado a la documentación del rol de Data Protection Officer / Privacy Advisor cuando la designación sea aplicable o se asigne voluntariamente. Addressed by clauses [4.1.2; 4.1.3; 5.1.3; 11.1.2].

13.3.7 **Article 38** - Mapeado a la posición, independencia, participación y gestión de conflictos de intereses de Data Protection Officer / Privacy Advisor cuando sea aplicable. Addressed by clauses [4.2.5; 5.1.3; 6.1.3; 11.1.2].

13.3.8 **Article 39** - Mapeado al asesoramiento en privacidad, las observaciones de supervisión, la revisión consultiva y la revisión del impacto en privacidad relacionado con roles por Data Protection Officer / Privacy Advisor cuando sea aplicable. Addressed by clauses [4.4.1; 5.1.3; 6.1.3; 11.1.2].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 4.1; Clause 4.2** - Mapeada a los actores del marco de privacidad y la asignación de roles para interesados, responsables del tratamiento de PII, encargados del tratamiento de PII, terceros y clasificación de roles del PIMS. Addressed by clauses [4.1.4; 4.1.6; 4.3.5; 5.1.5; 5.1.7].

13.4.2 **Clause 5.12** - Mapeada a la responsabilidad proactiva sobre el cumplimiento de privacidad, evidencias de roles, revisión, hallazgos de auditoría y verificación de acciones correctivas. Addressed by clauses [4.5.3; 6.1.2; 8.1.4; 10.1.4].

13.5 ISO/IEC 29151:2022

13.5.1 **Clause 6.1.2; Clause 6.1.3** - Mapeada a la definición de roles de protección de PII, documentación de roles, comunicación de roles, coordinación de seguridad/privacidad y

segregación de funciones para la protección de PII. Addressed by clauses [4.1.1; 4.2.1; 4.2.3; 4.2.4; 4.4.2; 5.1.4; 7.1.4].

13.6 ISO/IEC 27002:2022

13.6.1 Control 5.2 - Mapeado a la definición, asignación, documentación, comunicación y mantenimiento de responsabilidades del PIMS y de seguridad de la información. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.2.1; 4.4.2; 4.5.1; 5.1.4; 7.1.1].

13.6.2 Control 5.3 - Mapeado a la segregación de funciones, aprobación de combinación de roles, revisión independiente, controles de conflictos y verificación de acciones correctivas para conflictos de roles. Addressed by clauses [4.2.2; 4.2.3; 4.2.4; 9.1.2; 10.1.4].