					Introduzca aquí la denominación de la entidad jurídica registrada							
Número de documento: PII14					Título del documento: **Política de Seguridad y Control de Acceso 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 6.1.3; Clause 8.1	Both	Primary	Planificación y operación de controles de seguridad de PII
ISO/IEC 27701:2025	Clause 7.5; Clause 9.1; Clause 10.2	Both	Supporting	Evidencias, supervisión y acción correctiva
ISO/IEC 27701:2025	Annex A.3.8; Annex A.3.9	Both	Primary	Identidad y derechos de acceso para el tratamiento de PII
ISO/IEC 27701:2025	Annex A.3.22; Annex A.3.23	Both	Primary	Protección de endpoints y autenticación segura
ISO/IEC 27701:2025	Annex A.3.25; Annex A.3.26	Both	Primary	Registro de eventos y protección criptográfica
ISO/IEC 27701:2025	Annex A.3.28; Annex A.3.29	Both	Supporting	Seguridad de aplicaciones y arquitectura segura
ISO/IEC 27701:2025	Annex A.3.14; Annex A.3.15; Annex A.3.16	Both	Supporting	Protección y revisión de registros
GDPR	Article 5(1)(f); Article 5(2); Article 24; Article 28; Article 32	Both	Primary	Seguridad, responsabilidad proactiva y controles del encargado del tratamiento
ISO/IEC 27001:2022	Clause 6.1.3; Clause 8.1; Annex A controls 8.1, 8.2, 8.3, 8.5, 8.8, 8.9, 8.15, 8.16, 8.20, 8.24	Both	Supporting	Integración de controles del SGSI
ISO/IEC 27002:2022	Controls 8.1, 8.2, 8.3, 8.5, 8.8, 8.9, 8.15, 8.16, 8.20, 8.24	Both	Supporting	Orientación para la implementación de controles de seguridad
ISO/IEC 29100:2020	Clause 5.11; Clause 5.12	Both	Supporting	Principios de seguridad de la información y

				cumplimiento de privacidad
ISO/IEC 29151:2022	Clause 9.4.2; Clause 9.4.3; Clause 9.4.4; Clause 9.4.5; Clause 10.1.2; Clause 10.1.3; Clause 12.1.5; Clause 18.1.5; Clause 18.2.2; Clause 18.2.3; Clause 18.2.4	Both	Supporting	Controles de seguridad para la protección de PII

1. Alcance

1.1 Esta política define los requisitos específicos de seguridad y control de acceso de PII para sistemas, aplicaciones, servicios, dispositivos, entornos en la nube y procesos operativos que almacenen, transmitan, traten, accedan a, administren o protejan PII.

1.2 Esta política se aplica a contextos de responsable del tratamiento, corresponsable del tratamiento, encargado del tratamiento y subencargado del tratamiento en los que la organización determine, opere, apoye o dependa de controles de seguridad para el tratamiento de PII.

1.3 Esta política cubre los siguientes dominios de control de seguridad de PII:

1.3.1 línea base de seguridad de datos personales e integración con las políticas de seguridad de la información existentes;

1.3.2 control de acceso;

1.3.3 autenticación;

1.3.4 acceso privilegiado;

1.3.5 cifrado y almacenamiento seguro;

1.3.6 registro de eventos y supervisión;

1.3.7 configuración segura y gestión de vulnerabilidades;

1.3.8 controles de acceso a endpoints y a la nube;

1.3.9 vinculación de evidencias mediante REG02, REG08, REG10 y REG12.

1.4 Esta política no sustituye a un sistema completo de gestión de la seguridad de la información, una política de seguridad de redes, una política de desarrollo seguro, una política de copias de seguridad, una política de endpoints, una política de seguridad en la nube, un estándar criptográfico, un procedimiento de gestión de vulnerabilidades o un procedimiento de respuesta a incidentes. Cuando dichas políticas ya existan, esta política define la vinculación específica de PII y los requisitos de evidencias necesarios para el aseguramiento de PIMS.

1.5 Esta política no duplica:

1.5.1 la titularidad del inventario de tratamientos de PII y de la base jurídica en PII03;

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

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

1.5.4 las reglas de recogida, uso, comunicación y uso compartido en PII09;

1.5.5 la ejecución de conservación, supresión y eliminación en PII10;

1.5.6 la gobernanza del ciclo de vida del encargado del tratamiento en PII12;

1.5.7 los controles de mecanismos de transferencia internacional en PII13;

1.5.8 el flujo de trabajo de incidentes y brechas de seguridad en PII15;

1.5.9 la gobernanza de la información documentada en PII17;

1.5.10 la gobernanza de supervisión, auditoría y mejora de PIMS en PII18.

1.6 A los efectos de esta política, los registros operativos, las salidas de herramientas de seguridad, las exportaciones de revisiones de acceso, los informes de vulnerabilidades y las evidencias de configuración son fuentes de evidencias que se adjuntan a, se resumen en, o se referencian en los objetos de evidencia canónicos. No son registros PIMS separados.

2. Finalidad

2.1 La finalidad de esta política es asegurar que PII esté protegida mediante controles de seguridad y acceso adecuados, alineados con el riesgo y auditables durante todo el tratamiento.

2.2 Esta política permite a la organización demostrar que los controles de seguridad de PII se planifican, implementan, revisan, supervisan y mejoran mediante REG02, REG08, REG10 y

REG12 sin crear registros de seguridad duplicados ni sustituir las políticas de seguridad de la información existentes.

3. Objetivos

3.1 Los objetivos de esta política son:

3.1.1 definir una línea base de control de acceso de PII para sistemas y actividades de tratamiento;

3.1.2 asegurar que los controles de autenticación sean adecuados para la sensibilidad y el contexto de acceso de PII;

3.1.3 definir requisitos de revisión para el acceso privilegiado y ordinario a PII;

3.1.4 definir expectativas de cifrado y almacenamiento seguro para PII en reposo, en tránsito y en contextos pertinentes de nube o endpoint;

3.1.5 definir expectativas de registro de eventos y supervisión para el acceso a PII, los cambios en PII y la administración de PII;

3.1.6 definir requisitos de evidencias de configuración segura y vulnerabilidades para sistemas que tratan PII;

3.1.7 definir expectativas de acceso a endpoints y a la nube sin crear una política completa de seguridad de endpoints o de seguridad en la nube;

3.1.8 vincular los incidentes de seguridad de PII sospechados a REG10 sin duplicar el flujo de trabajo de incidentes;

3.1.9 integrarse con las políticas de seguridad de la información existentes cuando estén disponibles;

3.1.10 mantener evidencias preparadas para auditoría utilizando únicamente REG02, REG08, REG10 y REG12.

4. Declaraciones de la política

4.1 Línea base de seguridad de datos personales e integración con el SGSI

4.1.1 [Both] Information Security Lead DEBE definir la línea base de seguridad de datos personales para cada sistema o servicio que trate PII en REG12 antes de que el sistema o servicio entre en producción o cambie materialmente.

4.1.2 [Both] System Owner / Application Owner DEBE registrar la ubicación de las evidencias de los controles de seguridad de PII implementados en REG12 antes de basarse en un control de seguridad de la información existente para el aseguramiento de PIMS.

4.1.3 [Controller] Process Owner / Business Owner DEBE identificar la sensibilidad de PII, el contexto del tratamiento y la necesidad de acceso en REG02 antes de solicitar acceso nuevo o materialmente modificado a PII.

4.1.4 [Processor] Vendor / Procurement Owner DEBE registrar las instrucciones de seguridad del cliente, los límites de responsabilidad del cliente y los compromisos de seguridad del encargado del tratamiento en REG08 antes de que comience o cambie materialmente el acceso del encargado del tratamiento a la PII del cliente.

4.1.5 [Both] Privacy Lead / PIMS Manager DEBE verificar que las evidencias de seguridad de PII estén vinculadas a REG02, REG08, REG10 o REG12 antes de aceptar la actividad de tratamiento como auditable en PIMS.

4.2 Línea base de control de acceso

4.2.1 [Both] System Owner / Application Owner DEBE restringir el acceso a PII a roles aprobados y usuarios autorizados registrados o trazables en REG02 o REG12 antes de habilitar el acceso.

4.2.2 [Both] Process Owner / Business Owner DEBE aprobar la finalidad de negocio para el acceso a PII en REG02 o REG12 antes de que System Owner / Application Owner aprovisione el acceso.

4.2.3 [Both] System Owner / Application Owner DEBE revisar el acceso de usuarios a sistemas que tratan datos personales de alto impacto o PII sensible al menos trimestralmente y registrar el resultado de la revisión en REG12.

4.2.4 [Both] System Owner / Application Owner DEBE revisar el acceso de usuarios a otros sistemas que tratan PII al menos anualmente y registrar el resultado de la revisión en REG12.

4.2.5 [Both] System Owner / Application Owner DEBE eliminar o modificar el acceso a PII en REG12 en el plazo de un día hábil tras un cambio de rol, terminación, finalización de contrato o cuando el acceso ya no sea necesario.

4.2.6 [Processor] Vendor / Procurement Owner DEBE confirmar en REG08 que el acceso del encargado del tratamiento a la PII del cliente se limita a instrucciones documentadas del cliente antes de habilitar o cambiar el acceso.

4.2.7 [Subprocessor] Vendor / Procurement Owner DEBE confirmar en REG08 que el acceso del subencargado del tratamiento a PII se limita a actividades de subtratamiento autorizadas antes de habilitar o cambiar el acceso del subencargado del tratamiento.

[... 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 [Both] Information Security Lead DEBE registrar cada excepción a un requisito de seguridad o control de acceso de PII en REG12 antes de activar la excepción.

9.1.2 [Both] Data Protection Officer / Privacy Advisor DEBE asesorar sobre las excepciones de seguridad de PII de mayor riesgo en REG12 antes de la aprobación.

9.1.3 [Both] Top Management DEBE aprobar las excepciones de seguridad de PII en REG12 antes de la activación cuando la excepción afecte a datos personales de alto impacto, PII sensible, acceso privilegiado, cifrado, registro de eventos o vulnerabilidades de alto riesgo no resueltas.

9.1.4 [Both] Information Security Lead DEBE definir la caducidad de la excepción, el control compensatorio y la fecha de revisión en REG12 antes de la aprobación de la excepción.

9.1.5 [Both] System Owner / Application Owner DEBE remediar, renovar o cerrar las excepciones de seguridad de PII vencidas en REG12 en el plazo de cinco días hábiles desde su vencimiento.

9.1.6 [Processor] Vendor / Procurement Owner DEBE registrar las excepciones de seguridad del encargado del tratamiento o subencargado del tratamiento que afecten a la PII del cliente en REG08 y REG12 antes de la aceptación.

10. Aplicación

10.1.1 [Both] Privacy Lead / PIMS Manager DEBE registrar las no conformidades por evidencias de seguridad de PII ausentes o incompletas en REG12 en el plazo de cinco días hábiles desde su identificación.

10.1.2 [Both] Information Security Lead DEBE asignar la titularidad de la remediación para fallos de controles de seguridad de PII en REG12 en el plazo de cinco días hábiles desde la validación.

10.1.3 [Both] System Owner / Application Owner DEBE deshabilitar o restringir el acceso no autorizado, excesivo o no respaldado a PII en el plazo de un día hábil desde la validación y registrar la acción en REG12.

10.1.4 [Conditional] Incident Response Coordinator DEBE vincular las medidas de aplicación a REG10 en el plazo de un día hábil cuando el asunto de aplicación implique un incidente de PII sospechado o confirmado.

10.1.5 [Both] Top Management DEBE revisar las no conformidades de seguridad de PII repetidas o de alto riesgo en REG12 antes de la revisión por la dirección.

11. Revisión y mantenimiento

11.1.1 [All] Privacy Lead / PIMS Manager DEBE revisar esta política con Information Security Lead al menos anualmente y registrar el resultado de la revisión en REG12.

11.1.2 [Both] Information Security Lead DEBE revisar la línea base de seguridad de datos personales en REG12 en el plazo de 30 días tras un cambio material tecnológico, de amenazas, auditoría, incidente o regulatorio que afecte a la seguridad de PII.

11.1.3 [Both] System Owner / Application Owner DEBE actualizar las evidencias de seguridad de PII a nivel de sistema en REG12 en el plazo de 30 días tras un cambio material de arquitectura, acceso, configuración, vulnerabilidades o registro de eventos.

11.1.4 [Processor] Vendor / Procurement Owner DEBE revisar las evidencias de responsabilidades de seguridad de PII de encargados del tratamiento y subencargados del tratamiento en REG08 en el plazo de 30 días tras un cambio material del servicio, de instrucciones del cliente o de subencargado del tratamiento.

11.1.5 [All] Internal Audit / Compliance Reviewer DEBE verificar las evidencias de revisión de la política y evidencias seleccionadas de controles de seguridad de PII en REG12 de acuerdo con el plan de auditoría aprobado.

12. Políticas relacionadas

12.1 Esta política debería 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 PII07 - Política de Evaluación de Riesgos de Privacidad y DPIA;

12.1.5 PII08 - Política de Privacidad desde el Diseño y por Defecto;

12.1.6 PII09 - Política de Recogida, Uso, Comunicación y Uso Compartido de PII;

12.1.7 PII10 - Política de Conservación, Supresión y Eliminación de PII;

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

12.1.9 PII13 - Política de Transferencias Internacionales de PII;

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

12.1.11 PII16 - Política de Formación, Concienciación y Competencia en Privacidad;

12.1.12 PII17 - Política de Información Documentada y Gestión de Evidencias de PIMS;

12.1.13 PII18 - Política de Supervisión, Auditoría y Mejora de PIMS.

13. Normas y marcos de referencia

13.1 ISO/IEC 27701:2025 - Clause 6.1.3; Clause 8.1. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.1.4; 4.1.5; 4.7.1; 4.7.2; 4.7.3; 4.7.4; 4.7.5; 4.7.7; 4.8.1; 4.8.2; 4.8.3; 4.8.4; 4.8.5; 5.1.4; 5.1.6; 6.1.2; 7.1.1; 7.1.2].

13.2 ISO/IEC 27701:2025 - Clause 7.5; Clause 9.1; Clause 10.2. Addressed by clauses [4.1.5; 4.2.3; 4.2.4; 4.4.2; 4.4.3; 4.5.5; 4.6.3; 4.6.4; 4.7.5; 5.1.2; 6.1.1; 6.1.3; 6.1.4; 7.1.3; 7.1.6; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 9.1.1; 10.1.1; 10.1.2; 11.1.1; 11.1.5].

13.3 ISO/IEC 27701:2025 - Annex A.3.8; Annex A.3.9. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.2.6; 4.2.7; 4.3.1; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 4.4.6; 10.1.3].

13.4 ISO/IEC 27701:2025 - Annex A.3.22; Annex A.3.23. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 4.8.1; 4.8.2; 4.8.3; 4.8.4; 4.8.5].

13.5 ISO/IEC 27701:2025 - Annex A.3.25; Annex A.3.26. Addressed by clauses [4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 4.6.1; 4.6.2; 4.6.3; 4.6.4; 4.6.5; 4.6.6].

13.6 ISO/IEC 27701:2025 - Annex A.3.28; Annex A.3.29. Addressed by clauses [4.1.1; 4.1.2; 4.7.1; 4.7.2; 4.7.3; 4.7.4; 4.7.5; 4.7.6; 4.7.7; 4.8.4; 7.1.1; 7.1.2].

13.7 ISO/IEC 27701:2025 - Annex A.3.14; Annex A.3.15; Annex A.3.16. Addressed by clauses [4.1.5; 4.2.3; 4.2.4; 4.4.2; 4.4.3; 4.6.2; 4.6.3; 4.6.4; 4.7.2; 4.7.3; 5.1.9; 6.1.6; 8.1.4; 10.1.1; 11.1.5].

13.8 GDPR - Article 5(1)(f); Article 5(2); Article 24; Article 28; Article 32. Addressed by clauses [4.1.1; 4.1.4; 4.2.1; 4.2.5; 4.2.6; 4.2.7; 4.3.2; 4.4.4; 4.5.1; 4.5.2; 4.6.1; 4.6.6; 4.7.5; 4.7.6; 4.7.7; 4.8.4; 4.8.5; 5.1.1; 5.1.7; 6.1.4; 7.1.4; 9.1.3; 10.1.4].

13.9 ISO/IEC 27001:2022 - Clause 6.1.3; Clause 8.1; Annex A controls 8.1, 8.2, 8.3, 8.5, 8.8, 8.9, 8.15, 8.16, 8.20, 8.24. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.2.3; 4.3.2; 4.4.1; 4.4.2; 4.5.1; 4.5.2; 4.6.1; 4.6.3; 4.7.1; 4.7.4; 4.7.5; 4.8.1; 4.8.2; 7.1.1; 7.1.2].

13.10 ISO/IEC 27002:2022 - Controls 8.1, 8.2, 8.3, 8.5, 8.8, 8.9, 8.15, 8.16, 8.20, 8.24. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.2.3; 4.3.2; 4.4.1; 4.4.2; 4.5.1; 4.5.2; 4.6.1; 4.6.3; 4.7.1; 4.7.4; 4.7.5; 4.8.1; 4.8.2; 7.1.1; 7.1.2].

13.11 ISO/IEC 29100:2020 - Clause 5.11; Clause 5.12. Addressed by clauses [4.1.5; 4.2.1; 4.5.1; 4.6.2; 4.6.6; 4.7.6; 5.1.2; 6.1.1; 8.1.4; 10.1.1; 11.1.1].

13.12 ISO/IEC 29151:2022 - Clause 9.4.2; Clause 9.4.3; Clause 9.4.4; Clause 9.4.5; Clause 10.1.2; Clause 10.1.3; Clause 12.1.5; Clause 18.1.5; Clause 18.2.2; Clause 18.2.3; Clause 18.2.4. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.4.1; 4.4.2; 4.4.5; 4.5.1; 4.5.2; 4.5.3; 4.6.1; 4.6.2; 4.7.1; 4.7.2; 4.7.4; 4.8.1; 4.8.2; 6.1.6; 11.1.5].