

				Introduzca aquí la denominación de la entidad jurídica registrada							
Número de documento: PII08				Título del documento: Política de privacidad desde el diseño y por defecto							
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

Aviso legal (derechos de autor y restricciones de uso)
(C) 2025 Clarysec LLC. All rights reserved.

Este documento es propiedad intelectual de Clarysec LLC. Ninguna parte de este documento podrá copiarse, reutilizarse, distribuirse ni modificarse con fines comerciales o de implantación sin autorización previa y expresa por escrito.

El uso no autorizado está estrictamente prohibido y puede dar lugar a acciones legales.

Para cuestiones de licenciamiento, contacte con: info@clarysec.com

Alineación con normas y regulaciones

Norma / Regulación	Cláusula / Control / Artículo	Aplicabilidad	Tipo de cobertura	Comentario
ISO/IEC 27701:2025	Clause 6.1.2; Clause 6.1.3	Both	Supporting	Vinculación de la evaluación y el tratamiento de riesgos de privacidad
ISO/IEC 27701:2025	Clause 6.3; Clause 8.1	Both	Primary	Cambios planificados y control operacional
ISO/IEC 27701:2025	Clause 7.5	Both	Supporting	Evidencias documentadas de privacidad desde el diseño
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Supervisión y acción correctiva
ISO/IEC 27701:2025	Annex A.1.2.2; Annex A.1.2.6; Annex A.1.2.9	Controller	Supporting	Finalidades, activador de PIA y registros
ISO/IEC 27701:2025	Annex A.1.4.2; Annex A.1.4.3	Controller	Primary	Limitar la recogida y el tratamiento
ISO/IEC 27701:2025	Annex A.1.4.4; Annex A.1.4.5	Controller	Supporting	Objetivos de exactitud y minimización
ISO/IEC 27701:2025	Annex A.1.4.6; Annex A.1.4.7	Controller	Supporting	Diseño de desidentificación, supresión y archivos temporales
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.6; Annex A.2.2.7	Processor	Supporting	Acuerdo con el cliente, apoyo y registros del encargado
ISO/IEC 27701:2025	Annex A.2.4.2; Annex A.2.4.3; Annex A.2.4.4	Processor	Supporting	Capacidades de diseño del encargado
ISO/IEC 27701:2025	Annex A.3.27; Annex A.3.29	Both	Supporting	Ciclo de vida del desarrollo y principios de ingeniería
GDPR	Article 5(1)(b); Article 5(1)(c); Article 5(2)	Controller	Supporting	Limitación de la finalidad, minimización y responsabilidad proactiva

GDPR	Article 24	Controller	Supporting	Medidas del responsable del tratamiento
GDPR	Article 25	Controller	Primary	Protección de datos desde el diseño y por defecto
GDPR	Article 28	Both	Supporting	Instrucciones y asistencia del encargado del tratamiento
GDPR	Article 30	Both	Supporting	Registros de tratamiento
GDPR	Article 35	Controller	Supporting	Vinculación con el activador de la EIPD
ISO/IEC 29100:2020	Clause 4.7	Both	Supporting	Controles de privacidad desde el diseño
ISO/IEC 29100:2020	Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6	Both	Primary	Finalidad, recogida, minimización y limitación del uso
ISO/IEC 29100:2020	Clause 5.7; Clause 5.10; Clause 5.12	Both	Supporting	Exactitud, responsabilidad proactiva y cumplimiento
ISO/IEC 29151:2022	Annex A.3; Annex A.4; Annex A.5; Annex A.7; Annex A.8	Both	Primary	Principios y controles de protección de la PII

1. Alcance

- 1.1 Esta política define los requisitos para incorporar la privacidad desde el diseño y la privacidad por defecto en actividades nuevas y modificadas de tratamiento de PII, proyectos, productos, servicios, sistemas, aplicaciones, integraciones, actividades de adquisición y cambios en procesos de la organización dentro del alcance del PIMS.
- 1.2 Esta política se aplica a contextos de responsable del tratamiento, corresponsable del tratamiento, encargado del tratamiento y subencargado.
- 1.3 Las obligaciones del encargado del tratamiento y del subencargado se aplican cuando la organización diseña, configura, modifica u opera tratamientos por cuenta de un cliente, responsable del tratamiento o encargado del tratamiento aguas arriba bajo instrucciones documentadas.

1.4 Esta política cubre lo siguiente:

- 1.4.1 requisitos de privacidad al inicio del proyecto;
- 1.4.2 controles de diseño relativos a finalidad, minimización de datos y configuración por defecto;
- 1.4.3 revisión de privacidad desde el diseño antes de la entrada en producción;
- 1.4.4 revisión de privacidad desde el diseño activada por cambios;
- 1.4.5 comprobaciones de privacidad desde el diseño en adquisiciones;
- 1.4.6 vinculación con riesgos de privacidad, evaluación preliminar de EIPD y evidencias de acciones correctivas.

1.5 Esta política no sustituye lo siguiente:

- 1.5.1 PII03 para el inventario de tratamientos, finalidades, base jurídica y registros ROPA;
- 1.5.2 PII04 para el contenido y la publicación del aviso de privacidad;
- 1.5.3 PII05 para los controles de consentimiento y preferencias;
- 1.5.4 PII06 para la gestión de derechos de los interesados;
- 1.5.5 PII07 para la metodología de evaluación de riesgos de privacidad y EIPD;
- 1.5.6 PII09 para los controles de recogida, uso, comunicación y compartición;
- 1.5.7 PII10 para la ejecución de conservación, supresión y eliminación;
- 1.5.8 PII11 para la operación de exactitud y calidad;
- 1.5.9 PII12 para la gobernanza del ciclo de vida de encargados, subencargados y terceros;
- 1.5.10 PII13 para los mecanismos de transferencia internacional;
- 1.5.11 PII14 para la operación de seguridad de PII y control de acceso;
- 1.5.12 PII18 para la supervisión, auditoría, acción correctiva y gobernanza de mejora en todo el PIMS.

2. Finalidad

- 2.1 La finalidad de esta política es asegurar que los requisitos de privacidad se identifiquen, implementen y evidencien antes de que comience el tratamiento de PII o cambie materialmente, y que los sistemas y procesos se configuren por defecto para limitar la recogida, el uso, la exposición, la dependencia de conservación, la dependencia de comunicación y la identificabilidad de la PII a lo necesario para la finalidad documentada.

3. Objetivos

3.1 Los objetivos de esta política son:

- 3.1.1 incorporar requisitos de privacidad en las decisiones de inicio de proyecto, diseño, adquisición, cambio y entrada en producción;

- 3.1.2 asegurar que los diseños de tratamiento de PII estén vinculados a finalidades documentadas y a registros de tratamiento REG02;
- 3.1.3 implementar la minimización de datos y ajustes por defecto protectores de la privacidad antes de que comience el tratamiento;
- 3.1.4 asegurar que se active la evaluación preliminar de riesgos de privacidad y de EIPD sin duplicar la metodología de PII07;
- 3.1.5 asegurar que los requisitos de diseño de adquisiciones y de encargados se registren sin duplicar la gobernanza del ciclo de vida de PII12;
- 3.1.6 asegurar que los problemas de diseño no resueltos se escalen mediante REG12;
- 3.1.7 mantener evidencias de diseño preparadas para auditoría en REG02, REG04, REG08 y REG12.

4. Declaraciones de la política

4.1 Inicio de proyectos y requisitos de privacidad

- 4.1.1 [Both] The Process Owner / Business Owner MUST registrar una entrada de privacidad desde el diseño en REG04 antes de iniciar cualquier proyecto, producto, servicio, sistema, aplicación, integración o cambio de proceso de la organización que implique PII.
- 4.1.2 [Both] The Process Owner / Business Owner MUST vincular cada entrada de privacidad desde el diseño en REG04 a una actividad de tratamiento REG02 existente o en borrador antes de que se aprueben los requisitos funcionales.
- 4.1.3 [Controller] The Privacy Lead / PIMS Manager MUST registrar los requisitos de privacidad desde el diseño del responsable del tratamiento en REG04 antes de la aprobación del diseño funcional del responsable del tratamiento.
- 4.1.4 [Processor] The Vendor / Procurement Owner MUST registrar las instrucciones de diseño de privacidad del cliente y las restricciones contractuales de diseño en REG08 antes de la aprobación del diseño del servicio del encargado del tratamiento o de un cambio material del servicio.
- 4.1.5 [Conditional] The Data Protection Officer / Privacy Advisor MUST registrar asesoramiento en REG04 antes de la aprobación de un diseño de PII de alto riesgo, novedoso, sensible, automatizado, a gran escala o materialmente modificado.
- 4.1.6 [Both] The Information Security Lead MUST registrar en REG04 las dependencias de controles de seguridad de PII que respaldan el diseño de privacidad antes de la aprobación de la arquitectura.

4.2 Minimización de datos y diseño de privacidad por defecto

- 4.2.1 [Controller] The Process Owner / Business Owner MUST documentar las categorías mínimas de PII, categorías de interesados, fuentes y finalidades en REG02 y REG04 antes de la aprobación del diseño de recogida o importación.
- 4.2.2 [Both] The System Owner / Application Owner MUST configurar los ajustes de tratamiento por defecto para la recogida y el tratamiento mínimos de PII necesarios para la finalidad documentada y registrar evidencias en REG04 antes de la entrada en producción.
- 4.2.3 [Controller] The Process Owner / Business Owner MUST documentar los campos opcionales de PII, las opciones de tratamiento opcionales y los ajustes desactivados por defecto en REG02 y REG04 antes de la aprobación de la interfaz de usuario, formulario o flujo de trabajo.
- 4.2.4 [Both] The System Owner / Application Owner MUST documentar en REG04 los ajustes por defecto de exposición de privacidad para vistas, informes, exportaciones, interfaces y flujos de trabajo automatizados antes de la entrada en producción.

- 4.2.5 [Both] The Process Owner / Business Owner MUST documentar en REG04 la viabilidad de desidentificación, seudonimización, agregación o tratamiento no identificable antes de aprobar PII identificable para pruebas, analítica, informes o uso operativo secundario.
- 4.2.6 [Both] The System Owner / Application Owner MUST documentar en REG04 la gestión de artefactos temporales de PII, incluidos archivos temporales, cachés, registros de eventos o registros de preproducción, antes de la entrada en producción.
- 4.2.7 [Both] The Process Owner / Business Owner MUST dirigir los requisitos de diseño asignados a PII10, PII11, PII13 o PII14 a la vía de evidencias de la política relacionada en REG04 en un plazo de cinco días hábiles desde la identificación de la dependencia.

[... 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 Excepciones de diseño de privacidad

- 9.1.1 [Both] The Process Owner / Business Owner MUST solicitar una excepción de diseño de privacidad en REG12 antes de aprobar un diseño o cambio que no pueda cumplir un requisito de diseño de privacidad aplicable.
- 9.1.2 [Both] The Privacy Lead / PIMS Manager MUST evaluar en REG12 el impacto, los controles compensatorios y la caducidad de cada excepción de diseño de privacidad en un plazo de cinco días hábiles desde la solicitud.
- 9.1.3 [Conditional] The Data Protection Officer / Privacy Advisor MUST registrar asesoramiento en REG12 antes de la aprobación de una excepción de diseño de privacidad que implique tratamiento de alto riesgo, sensible, automatizado, a gran escala, controvertido o legalmente material.
- 9.1.4 [All] Top Management MUST aprobar en REG12 una excepción de diseño de privacidad que afecte a tratamientos de alto impacto, alcance de certificación, riesgo mayor no resuelto u obligación legal antes de que la excepción surta efecto.
- 9.1.5 [Both] The Privacy Lead / PIMS Manager MUST establecer en REG12 una fecha de caducidad no superior a 90 días para cada excepción de diseño de privacidad aprobada antes de la aprobación.
- 9.1.6 [Both] The Privacy Lead / PIMS Manager MUST cerrar o reevaluar cada excepción de diseño de privacidad en REG12 en un plazo de cinco días hábiles desde su caducidad.

10. Aplicación

10.1 Aplicación y gestión de no conformidades

- 10.1.1 [Both] The Privacy Lead / PIMS Manager MUST registrar en REG12 la ausencia de revisión de privacidad desde el diseño, la falta de evidencias de minimización, el fallo no resuelto de ajustes por defecto o la entrada en producción no autorizada como una no conformidad en un plazo de cinco días hábiles desde su identificación.
- 10.1.2 [Both] The System Owner / Application Owner MUST impedir la entrada en producción de un sistema que trate PII cuando la revisión de privacidad desde el diseño REG04 esté incompleta y registrar la decisión en REG12 antes de la entrada en producción.
- 10.1.3 [Both] The Vendor / Procurement Owner MUST impedir la incorporación de proveedores o la firma del contrato cuando falten las evidencias de diseño de privacidad REG08 requeridas y registrar la decisión en REG12 antes de la incorporación o firma.
- 10.1.4 [Both] The Process Owner / Business Owner MUST suspender el uso de un diseño de tratamiento de PII nuevo o modificado hasta que la revisión REG04, las actualizaciones REG02 y las excepciones REG12 requeridas estén completas.

- 10.1.5 [All] Top Management MUST requerir una acción correctiva en REG12 en un plazo de 10 días hábiles para fallos de diseño de privacidad repetidos, prolongados o de alto impacto.
- 10.1.6 [All] The Internal Audit / Compliance Reviewer MUST verificar la eficacia de las acciones correctivas relativas a no conformidades de diseño de privacidad en REG12 en la siguiente auditoría PIMS programada o en un plazo de 60 días desde el cierre, lo que ocurra primero.

11. Revisión y mantenimiento

11.1 Revisión de la política y de los controles de diseño

- 11.1.1 [All] The Privacy Lead / PIMS Manager MUST revisar esta política en REG12 anualmente y en un plazo de 30 días desde un cambio material legal, de tratamiento, tecnológico, del alcance de certificación o de control del PIMS.
- 11.1.2 [Both] The Process Owner / Business Owner MUST revisar anualmente y en un plazo de 30 días desde un cambio material del tratamiento las actividades de tratamiento REG02 activas para detectar cambios en dependencias de diseño de privacidad.
- 11.1.3 [Both] The System Owner / Application Owner MUST revisar anualmente y en un plazo de 30 días desde un cambio material del sistema las evidencias de configuración de privacidad por defecto en REG04.
- 11.1.4 [Both] The Vendor / Procurement Owner MUST revisar en REG08 las obligaciones de diseño de privacidad de proveedores, encargados del tratamiento, subencargados y terceros antes de la renovación y en un plazo de 30 días desde un cambio material de la relación.
- 11.1.5 [Conditional] The Data Protection Officer / Privacy Advisor MUST revisar el impacto en la privacidad de los cambios materiales de la política en REG12 antes de la aprobación.
- 11.1.6 [All] Top Management MUST aprobar los cambios materiales de esta política en REG12 antes de su publicación.

12. Políticas relacionadas

- 12.1 PII01 - Política del Sistema de Gestión de la Privacidad de la Información
- 12.2 PII02 - Política de funciones, responsabilidades y rendición de cuentas de privacidad
- 12.3 PII03 - Política de inventario de tratamientos de PII y base jurídica
- 12.4 PII04 - Política de aviso de privacidad y transparencia
- 12.5 PII05 - Política de gestión del consentimiento y preferencias
- 12.6 PII06 - Política de gestión de derechos de los interesados
- 12.7 PII07 - Política de evaluación de riesgos de privacidad y EIPD
- 12.8 PII09 - Política de recogida, uso, comunicación y compartición de PII
- 12.9 PII10 - Política de conservación, supresión y eliminación de PII
- 12.10 PII11 - Política de exactitud y calidad de PII
- 12.11 PII12 - Política de gestión de privacidad de encargados, subencargados y terceros
- 12.12 PII13 - Política de transferencias internacionales de PII
- 12.13 PII14 - Política de seguridad de PII y control de acceso
- 12.14 PII17 - Política de información documentada y gestión de evidencias del PIMS
- 12.15 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 regulaciones. 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 6.1.2; Clause 6.1.3** - Mapeado con la evaluación preliminar de riesgos de privacidad, la vinculación de acciones de tratamiento, el análisis de dependencias de diseño, el escalado y la acción correctiva sin duplicar la metodología completa de evaluación de riesgos de privacidad y EIPD. Addressed by clauses [4.1.5; 4.3.1; 4.3.2; 4.3.4; 4.5.5; 5.1.3; 7.1.7].
- 13.2.2 **Clause 6.3; Clause 8.1** - Mapeado con cambios de privacidad planificados, inicio de proyectos, revisión operacional del diseño de privacidad, control de entrada en producción y revisión de cambios materiales. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.3.3; 4.3.5; 4.5.1; 4.5.3; 4.5.4; 4.5.6; 7.1.2; 7.1.5; 10.1.2].
- 13.2.3 **Clause 7.5** - Mapeado con evidencias documentadas de diseño de privacidad conservadas en REG02, REG04, REG08 y REG12. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.2.1; 4.2.3; 4.4.1; 4.4.2; 4.4.3; 5.1.2; 5.1.5; 5.1.6; 5.1.7; 7.1.1; 7.1.3; 7.1.4].
- 13.2.4 **Clause 9.1; Clause 10.2** - Mapeado con métricas de diseño de privacidad, muestreo de evidencias, registro de no conformidades, acciones correctivas y verificación de eficacia. Addressed by clauses [4.3.6; 4.4.5; 4.5.5; 6.1.1; 6.1.2; 6.1.4; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 10.1.1; 10.1.5; 10.1.6].
- 13.2.5 **Annex A.1.2.2; Annex A.1.2.6; Annex A.1.2.9** - Mapeado con la documentación de finalidades de tratamiento, registros de tratamiento, vinculación del diseño de privacidad y activadores de evaluación preliminar de riesgos de privacidad o EIPD para el tratamiento del responsable del tratamiento. Addressed by clauses [4.1.2; 4.2.1; 4.3.1; 4.4.2; 4.5.2; 5.1.5; 7.1.3; 11.1.2].
- 13.2.6 **Annex A.1.4.2; Annex A.1.4.3** - Mapeado con la limitación de la recogida y el tratamiento de PII mediante requisitos mínimos de datos basados en la finalidad, tratamiento opcional desactivado por defecto y ajustes mínimos de tratamiento por defecto. Addressed by clauses [4.1.3; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.5.4; 7.1.5; 11.1.3].
- 13.2.7 **Annex A.1.4.4; Annex A.1.4.5** - Mapeado con el direccionamiento de dependencias de exactitud, objetivos de minimización, viabilidad de desidentificación y evidencias de diseño para minimizar la PII identificable. Addressed by clauses [4.2.5; 4.2.7; 4.3.2; 4.5.2; 7.1.3; 11.1.2].
- 13.2.8 **Annex A.1.4.6; Annex A.1.4.7** - Mapeado con la identificación en fase de diseño de desidentificación, dependencia de supresión, artefactos temporales de PII y direccionamiento a controles del ciclo de vida sin duplicar la ejecución de conservación o eliminación. Addressed by clauses [4.2.5; 4.2.6; 4.2.7; 4.3.3; 4.5.4; 7.1.5; 11.1.3].
- 13.2.9 **Annex A.2.2.2; Annex A.2.2.6; Annex A.2.2.7** - Mapeado con instrucciones del cliente al encargado, información de apoyo al cliente, registros de diseño del encargado y cambios de diseño del servicio autorizados por el cliente. Addressed by clauses [4.1.4; 4.4.1; 4.4.3; 4.4.6; 5.1.7; 7.1.4; 11.1.4].
- 13.2.10 **Annex A.2.4.2; Annex A.2.4.3; Annex A.2.4.4** - Mapeado con capacidades de diseño del encargado para archivos temporales, dependencia de devolución o eliminación, y dependencia de controles de transmisión registradas como evidencias de diseño sin duplicar procedimientos operativos de supresión o controles de seguridad. Addressed by clauses [4.2.6; 4.2.7; 4.4.3; 4.4.4; 4.4.6; 7.1.4; 7.1.6; 11.1.4].
- 13.2.11 **Annex A.3.27; Annex A.3.29** - Mapeado con requisitos de privacidad en el ciclo de vida del desarrollo, principios de ingeniería, puntos de control de protección de PII y evidencias de configuración de privacidad por defecto. Addressed by clauses [4.1.6; 4.3.3; 4.3.4; 4.4.4; 4.5.1; 4.5.4; 5.1.4; 5.1.6; 7.1.5; 7.1.6; 10.1.2; 11.1.3].

13.3 GDPR

- 13.3.1 **Article 5(1)(b); Article 5(1)(c); Article 5(2)** - Mapeado con la limitación de la finalidad, el diseño de PII mínima, la vinculación con registros de tratamiento, la minimización por defecto, las evidencias y la responsabilidad proactiva. Addressed by clauses [4.1.2; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.4.2; 4.5.2; 5.1.5; 8.1.1; 10.1.1].
- 13.3.2 **Article 24** - Mapeado con medidas del responsable del tratamiento, revisión de gobernanza, aprobación de excepciones, acción correctiva y mantenimiento de la política para la implementación de privacidad desde el diseño. Addressed by clauses [4.1.3; 4.5.6; 5.1.1; 6.1.2; 9.1.2; 9.1.4; 10.1.5; 11.1.6].
- 13.3.3 **Article 25** - Mapeado con inicio de proyectos, requisitos de privacidad en fase de diseño, ajustes de privacidad por defecto, minimización, comprobaciones de diseño en adquisiciones, revisión de entrada en producción y revisión activada por cambios. Addressed by clauses [4.1.1; 4.1.3; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.3.5; 4.4.1; 4.5.1; 4.5.3; 4.5.4; 10.1.2].
- 13.3.4 **Article 28** - Mapeado con instrucciones al encargado, apoyo de diseño del encargado, evidencias de diseño de privacidad de proveedores y cambios de diseño autorizados por el cliente. Addressed by clauses [4.1.4; 4.4.1; 4.4.3; 4.4.5; 4.4.6; 5.1.7; 7.1.4; 10.1.3; 11.1.4].
- 13.3.5 **Article 30** - Mapeado con vinculación de registros de tratamiento, actualizaciones REG02, dependencias de diseño de actividades de tratamiento y evidencias de registros de tratamiento. Addressed by clauses [4.1.2; 4.2.1; 4.4.2; 4.5.2; 5.1.5; 7.1.3; 11.1.2].
- 13.3.6 **Article 35** - Mapeado con activadores de evaluación preliminar de riesgos de privacidad y EIPD en fase de diseño, asesoramiento de alto riesgo y comprobaciones posteriores a la implementación sin duplicar la metodología de EIPD. Addressed by clauses [4.1.5; 4.3.1; 4.3.6; 5.1.3; 6.1.3; 9.1.3].

13.4 ISO/IEC 29100:2020

- 13.4.1 **Clause 4.7** - Mapeado con la identificación de controles de privacidad en la fase de diseño, la vinculación con riesgos de privacidad y evidencias de diseño para la implementación de controles. Addressed by clauses [4.1.1; 4.1.3; 4.1.5; 4.3.1; 4.3.2; 4.3.3; 4.3.5; 4.5.1].
- 13.4.2 **Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6** - Mapeado con la especificación de finalidades, la limitación de la recogida, la minimización de datos, el uso limitado y los ajustes de tratamiento por defecto. Addressed by clauses [4.1.2; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.4.2; 4.5.2].
- 13.4.3 **Clause 5.7; Clause 5.10; Clause 5.12** - Mapeado con el direccionamiento de dependencias de exactitud, evidencias de responsabilidad proactiva, supervisión del diseño de privacidad, auditoría y acción correctiva. Addressed by clauses [4.2.7; 4.3.6; 4.5.5; 6.1.1; 6.1.4; 8.1.1; 8.1.2; 10.1.1; 10.1.6].

13.5 ISO/IEC 29151:2022

- 13.5.1 **Annex A.3; Annex A.4; Annex A.5; Annex A.7; Annex A.8** - Mapeado con la legitimidad de la finalidad, la limitación de la recogida, la minimización de datos, la limitación del uso y la comunicación, la dependencia de conservación, la gestión de archivos temporales y los controles de diseño de dependencias de exactitud. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.2.6; 4.2.7; 4.4.2; 4.5.2; 4.5.4; 7.1.3; 7.1.5].