					Introduzca aquí la denominación de la entidad jurídica registrada							
Número de documento: PII23					Título del documento: **Política del encargado del tratamiento de PII en la nube**							
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 4.1; Clause 6.1.3	Processor	Supporting	Rol en el PIMS y aplicabilidad de los controles
ISO/IEC 27701:2025	Clause 7.5; Clause 8.1	Processor	Primary	Evidencias documentadas del encargado del tratamiento en la nube y control operacional
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Processor	Supporting	Seguimiento, no conformidad y acción correctiva
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.5; Annex A.2.2.6; Annex A.2.2.7	Processor	Primary	Acuerdos con clientes, instrucciones, asistencia y registros
ISO/IEC 27701:2025	Annex A.2.3.2	Processor	Primary	Asistencia al cliente para obligaciones relativas a interesados
ISO/IEC 27701:2025	Annex A.2.4.2; Annex A.2.4.3; Annex A.2.4.4	Processor	Primary	Controles sobre archivos temporales, devolución, transferencia, eliminación y transmisión
ISO/IEC 27701:2025	Annex A.2.5.2; Annex A.2.5.3	Processor	Supporting	Base de transferencia y ubicaciones
ISO/IEC 27701:2025	Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6	Processor	Supporting	Registros de divulgación y gestión de solicitudes de divulgación
ISO/IEC 27701:2025	Annex A.2.5.7; Annex A.2.5.8; Annex A.2.5.9	Processor	Primary	Divulgación, contratación y notificación de cambios de subencargados del tratamiento

ISO/IEC 27701:2025	Annex A.3.8; Annex A.3.9; Annex A.3.14; Annex A.3.24; Annex A.3.25	Processor	Supporting	Evidencias de acceso, registros, copia de seguridad y registro de eventos
GDPR	Article 28	Processor	Primary	Encargado del tratamiento, subencargado del tratamiento, asistencia, auditoría, supresión y devolución
GDPR	Article 30	Processor	Supporting	Registros del encargado del tratamiento
GDPR	Article 32; Article 33	Processor	Supporting	Seguridad y notificación de brechas de seguridad al responsable del tratamiento
GDPR	Article 44	Conditional	Referenced	Enrutamiento de transferencias internacionales
ISO/IEC 29100:2020	Clause 5.3; Clause 5.5; Clause 5.6	Processor	Supporting	Limitación de finalidad, minimización, uso, conservación y divulgación
ISO/IEC 29100:2020	Clause 5.10; Clause 5.11; Clause 5.12	Processor	Supporting	Responsabilidad proactiva, seguridad de la información y cumplimiento
ISO/IEC 29151:2022	Clause 15.1.2; Clause 15.2.2; Clause 15.2.3; Annex A.7; Annex A.7.2	Processor	Supporting	Evaluación del encargado del tratamiento, seguimiento, cambios y controles de conservación
ISO/IEC 27001:2022	Clause 6.1.3; Clause 8.1; Annex A controls 5.19; 5.20; 5.21; 5.22; 5.23	Processor	Supporting	Aplicabilidad de controles, control operacional y controles de proveedores/nube

ISO/IEC 27002:2022	Control 5.19; Control 5.20; Control 5.21; Control 5.22; Control 5.23; Control 8.10; Control 8.15; Control 8.16	Processor	Supporting	Controles de proveedores, nube, eliminación, registro de eventos y seguimiento
ISO/IEC 27018:2020	Annex A.2.1; Annex A.3.1	Processor	Primary	Asistencia al cliente del encargado del tratamiento en la nube y limitación de finalidad
ISO/IEC 27018:2020	Annex A.6.1; Annex A.6.2; Annex A.8.1	Processor	Primary	Notificación de divulgación en la nube, registros de divulgación y transparencia de subencargados del tratamiento
ISO/IEC 27018:2020	Annex A.10.1; Annex A.10.3; Annex A.11.11; Annex A.11.12; Annex A.12.1	Processor	Primary	Interfaz de brechas de seguridad en la nube, salida, medidas contractuales, subcontratos y registros de ubicación
ISO/IEC 27036-2:2022	Clause 6.1.1; Clause 6.1.2	Processor	Supporting	Estrategia y gobernanza de la relación de suministro
ISO/IEC 27036-2:2022	Clause 7.1; Clause 7.2; Clause 7.3; Clause 7.4; Clause 7.5	Processor	Supporting	Planificación, acuerdo, gestión, seguimiento y terminación de la relación con proveedores
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	Processor	Supporting	Marco y documentación 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	Processor	Supporting	Implementación de la supresión y excepciones

1. Alcance

1.1 Esta política define requisitos obligatorios de privacidad para servicios en la nube en los que la organización actúa como encargado del tratamiento o subencargado del tratamiento de PII, incluidos servicios SaaS, PaaS, IaaS, aplicaciones alojadas, nube gestionada, soporte en la nube, almacenamiento en la nube, analítica en la nube y servicios de infraestructura en la nube que tratan PII por cuenta de los clientes.

1.2 Esta política se aplica al tratamiento en la nube realizado en virtud de acuerdos con clientes, instrucciones documentadas del cliente, instrucciones de encargados del tratamiento ascendentes, acuerdos con subencargados del tratamiento, configuración de regiones de nube, acceso de soporte en la nube, administración del servicio, copia de seguridad, replicación, registro de eventos, seguimiento, supresión, devolución, soporte en caso de brecha de seguridad, soporte de auditoría y obligaciones de asistencia al cliente.

1.3 Esta política cubre:

1.3.1 el alcance del tratamiento de PII en la nube y los registros de instrucciones;

1.3.2 las evidencias de acuerdos con clientes y de responsabilidad compartida;

1.3.3 las evidencias de aislamiento entre tenants, acceso a la nube, acceso administrativo y registro de eventos;

1.3.4 la gobernanza de subencargados del tratamiento y de la cadena de suministro en la nube;

1.3.5 la ubicación, el acceso remoto y el enrutamiento de transferencias internacionales;

1.3.6 las evidencias de devolución, transferencia, supresión, eliminación y salida;

1.3.7 la asistencia al cliente respecto de derechos de los interesados, DPIA, auditorías y respuesta a brechas de seguridad;

1.3.8 las evidencias de seguimiento, excepción, aplicación y mejora.

1.4 Esta política no crea un registro independiente de contratos con clientes, registro de servicios en la nube, registro de aislamiento entre tenants, registro de accesos, registro de eventos, registro de supresión, registro de solicitudes de soporte, registro de evidencias de auditoría, registro de brechas de seguridad, registro de subencargados del tratamiento ni comité de gobernanza de la nube.

1.5 Esta política no sustituye a:

1.5.1 PII03 para el inventario de tratamientos y la titularidad de la base jurídica;

1.5.2 PII06 para el flujo de trabajo completo de derechos de los interesados;

1.5.3 PII07 para la metodología de riesgos de privacidad y DPIA;

1.5.4 PII08 para los controles de privacidad desde el diseño y por defecto;

1.5.5 PII09 para los controles generales de recogida, uso, divulgación y compartición;

1.5.6 PII10 para la metodología de conservación, supresión y eliminación;

1.5.7 PII12 para la gobernanza general del ciclo de vida de encargados del tratamiento, subencargados del tratamiento y terceros;

1.5.8 PII13 para la evaluación de mecanismos de transferencia internacional;

1.5.9 PII14 para la arquitectura completa de seguridad de PII y control de acceso;

1.5.10 PII15 para el flujo de trabajo de gestión de incidentes y brechas de seguridad;

1.5.11 PII17 para el control de información documentada;

1.5.12 PII18 para la gobernanza de seguimiento, auditoría y mejora del PIMS.

2. Propósito

2.1 El propósito de esta política es asegurar que los servicios de encargado del tratamiento y subencargado del tratamiento de PII en la nube operen conforme a instrucciones documentadas

del cliente, un alcance claro del tratamiento, acuerdos controlados con subencargados del tratamiento, responsabilidades adecuadas de seguridad en la nube, ubicación y enrutamiento de transferencias documentados, obligaciones de asistencia al cliente, soporte en caso de brecha de seguridad, capacidad de supresión/devolución y evidencias preparadas para auditoría.

2.2 Esta política respalda la preparación para la certificación PIMS ISO/IEC 27701:2025 para encargados del tratamiento en la nube y subencargados del tratamiento en la nube, manteniendo la integración con el conjunto existente de políticas PIMS y los objetos de evidencia canónicos.

3. Objetivos

3.1 Los objetivos de esta política son:

3.1.1 Definir el alcance del tratamiento de PII en la nube antes de la incorporación del cliente o de un cambio material.

3.1.2 Asegurar que las instrucciones del cliente se registren, revisen y sigan.

3.1.3 Mantener evidencias del encargado del tratamiento y subencargado del tratamiento en la nube en los registros canónicos del PIMS.

3.1.4 Definir evidencias de responsabilidad compartida, aislamiento entre tenants, acceso, registro de eventos y ubicación sin duplicar la política de seguridad de PII.

3.1.5 Controlar las evidencias de incorporación, cambio, obligaciones trasladadas contractualmente y seguimiento de subencargados del tratamiento.

3.1.6 Apoyar a los clientes en relación con derechos de los interesados, DPIA, solicitudes de auditoría y respuesta a brechas de seguridad.

3.1.7 Asegurar que las evidencias de devolución, supresión, transferencia y eliminación se conserven al finalizar el servicio.

3.1.8 Realizar el seguimiento de los controles del encargado del tratamiento en la nube e impulsar acciones correctivas mediante REG12.

4. Declaraciones de política

4.1 Alcance del tratamiento en la nube e instrucciones del cliente

4.1.1 [Processor] The Privacy Lead / PIMS Manager MUST registrar cada servicio de tratamiento de PII en la nube, rol de tratamiento del cliente, fuente de instrucciones del cliente, categorías de PII, categorías de interesados, finalidad del servicio, ubicación del tratamiento, dependencia de subencargados del tratamiento, dependencia de supresión e indicador de transferencia en REG02 y REG08 antes de la incorporación del cliente o de un cambio material del servicio.

4.1.2 [Processor] The Process Owner / Business Owner MUST registrar las instrucciones documentadas del cliente para el tratamiento de PII en la nube en REG08 antes de que comience el tratamiento.

4.1.3 [Subprocessor] The Process Owner / Business Owner MUST registrar las instrucciones del encargado del tratamiento ascendente o aprobadas por el cliente en REG08 antes de tratar PII como subencargado del tratamiento en la nube.

4.1.4 [Processor] The Privacy Lead / PIMS Manager MUST registrar la aplicabilidad de los controles del encargado del tratamiento en la nube en REG03 antes de que se libere o se modifique materialmente un nuevo servicio de tratamiento de PII en la nube.

4.1.5 [Processor] The Data Protection Officer / Privacy Advisor MUST revisar en REG12 cualquier instrucción del cliente que parezca incoherente con las obligaciones documentadas del cliente, los requisitos del PIMS o el alcance aprobado del servicio antes de que la organización actúe conforme a dicha instrucción.

4.1.6 [Processor] The Process Owner / Business Owner MUST registrar en REG12 cualquier tratamiento propuesto de PII del cliente fuera de las instrucciones documentadas del cliente y obtener la aprobación de Privacy Lead / PIMS Manager antes de que se realice el tratamiento.

4.2 Configuración de la nube, aislamiento entre tenants, acceso y registro de eventos

4.2.1 [Processor] The Information Security Lead MUST registrar el límite de responsabilidad compartida en la nube para el acceso a PII, la administración, el registro de eventos, la copia de seguridad, el cifrado, la gestión de vulnerabilidades y la supresión en REG08 antes de la incorporación del cliente o de un cambio material del servicio.

4.2.2 [Processor] The System Owner / Application Owner MUST validar en REG12 los controles de aislamiento entre tenants o segregación de clientes antes del uso en producción y después de un cambio material de arquitectura.

4.2.3 [Processor] The System Owner / Application Owner MUST conceder acceso administrativo en la nube a PII del cliente solo después de que la necesidad de negocio aprobada, el alcance del acceso, la duración del acceso y la frecuencia de revisión se registren en REG12.

4.2.4 [Processor] The Information Security Lead MUST revisar en REG12 el acceso privilegiado en la nube, el acceso de soporte, el acceso a PII del cliente y la cobertura de registro de eventos al menos trimestralmente.

4.2.5 [Processor] The System Owner / Application Owner MUST validar en REG12 la separación de los entornos de producción, preproducción, prueba y soporte para PII del cliente antes de la liberación y después de un cambio material del entorno.

4.2.6 [Processor] The System Owner / Application Owner MUST registrar las ubicaciones de copia de seguridad, replicación, almacenamiento de registros y acceso de soporte para PII de clientes en la nube en REG02, REG08 o REG09 antes de habilitar o cambiar dichas ubicaciones.

[... 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 [Processor] The Process Owner / Business Owner MUST solicitar en REG12 una excepción del encargado del tratamiento en la nube antes de la incorporación, liberación, renovación o uso continuado cuando estén incompletas las evidencias requeridas de instrucciones del cliente, subencargados del tratamiento, ubicación, acceso, registro de eventos, supresión o interfaz de incidentes.

9.2 [Processor] The Data Protection Officer / Privacy Advisor MUST revisar en REG12 las solicitudes de excepción del encargado del tratamiento en la nube significativas para la privacidad antes de la aprobación cuando la excepción afecte a instrucciones del cliente, asistencia a interesados, transferencias, subencargados del tratamiento, supresión, soporte de brechas de seguridad o PII de alto impacto.

9.3 [Processor] Top Management MUST aprobar en REG12 las excepciones de alto riesgo o materiales del encargado del tratamiento en la nube antes de que la excepción surta efecto.

9.4 [Processor] The Privacy Lead / PIMS Manager MUST asignar una fecha de caducidad, responsable de remediación, fecha de revisión y nota de riesgo residual en REG12 para cada excepción aprobada del encargado del tratamiento en la nube antes de la aprobación.

10. Aplicación

10.1 [Processor] The Privacy Lead / PIMS Manager MUST bloquear la incorporación del cliente, la liberación del servicio, la renovación o la continuación del tratamiento cuando falten evidencias

requeridas de REG02, REG03, REG08, REG09, REG10 o REG12 antes de que el tratamiento comience o continúe.

10.2 [Processor] The System Owner / Application Owner MUST deshabilitar el acceso a la nube no aprobado, el uso de regiones no aprobado, la replicación no aprobada, el acceso de soporte no aprobado o el flujo de datos a subencargados del tratamiento no aprobado dentro de un día hábil tras una decisión de aplicación, y registrar la finalización en REG08 o REG12.

10.3 [Processor] The Vendor / Procurement Owner MUST suspender el nuevo tratamiento de PII por un subencargado del tratamiento en la nube no aprobado o no conforme hasta que se completen las evidencias de acción correctiva en REG08.

10.4 [Processor] The Incident Response Coordinator MUST escalar los incumplimientos de plazos de notificación de incidentes al cliente en REG10 y REG12 dentro de un día hábil desde su identificación.

10.5 [Processor] The Internal Audit / Compliance Reviewer MUST verificar la eficacia de las acciones correctivas para no conformidades mayores o repetidas del encargado del tratamiento en la nube en REG12 dentro de los 60 días posteriores al cierre de la acción correctiva.

11. Revisión y mantenimiento

11.1 [Processor] The Privacy Lead / PIMS Manager MUST revisar esta política en REG12 anualmente y dentro de los 30 días posteriores a un cambio material en las obligaciones del encargado del tratamiento en la nube, la arquitectura de la nube, la gobernanza de subencargados del tratamiento, la asistencia al cliente, la capacidad de supresión o los requisitos de certificación.

11.2 [Processor] The Vendor / Procurement Owner MUST revisar los registros de subencargados del tratamiento en la nube y dependencias de servicios en la nube en REG08 al menos anualmente y antes de la renovación.

11.3 [Processor] The System Owner / Application Owner MUST revisar las evidencias de aislamiento entre tenants, acceso privilegiado, registro de eventos, copia de seguridad, replicación y supresión en REG12 al menos anualmente y después de un cambio material de arquitectura.

11.4 [Processor] The Privacy Lead / PIMS Manager MUST revisar los registros de ubicación en la nube y enrutamiento de transferencias de REG09 al menos anualmente y dentro de los 15 días hábiles posteriores a un cambio material de ubicación, acceso de soporte, copia de seguridad o subencargado del tratamiento.

11.5 [Processor] The Privacy Lead / PIMS Manager MUST actualizar REG03 dentro de los 15 días hábiles posteriores a cambios de política aprobados que afecten a la aplicabilidad de los controles del encargado del tratamiento en la nube.

11.6 [All] Top Management MUST aprobar las revisiones materiales de esta política en REG12 antes de su publicación.

12. Políticas relacionadas

12.1 Esta política cuenta con el respaldo de 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 rendición de cuentas en materia de privacidad

12.4 PII03 - Política de inventario de tratamientos de PII y base jurídica

12.5 PII06 - Política de gestión de derechos de los interesados

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

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

12.8 PII09 - Política de recogida, uso, divulgación y compartición de PII

12.9 PII10 - Política de conservación, supresión y eliminación de PII

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

12.11 PII13 - Política de transferencia internacional de PII

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

12.13 PII15 - Política de gestión de incidentes y brechas de seguridad de PII

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

12.15 PII18 - Política de seguimiento, auditoría y mejora del PIMS

12.16 PII20 - Política de privacidad de menores

12.17 PII21 - Política de privacidad de AI y toma de decisiones automatizada

12.18 PII22 - Política de privacidad de marketing y cookies

12.19 PII24 - Política de privacidad de CCTV y monitorización física

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 - Clause 4.1; Clause 6.1.3. Addressed by clauses [4.1.1; 4.1.4; 5.2; 7.1; 11.5].

13.3 ISO/IEC 27701:2025 - Clause 7.5; Clause 8.1. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.2.1; 4.3.1; 4.4.1; 4.6.1; 4.7.1; 4.8.1; 7.1; 7.2; 7.3].

13.4 ISO/IEC 27701:2025 - Clause 9.1; Clause 10.2. Addressed by clauses [4.3.5; 4.6.6; 4.8.1; 4.8.2; 4.8.4; 6.1; 6.2; 8.1; 8.2; 8.3; 8.4; 8.5; 10.5; 11.1].

13.5 ISO/IEC 27701:2025 - Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.5; Annex A.2.2.6; Annex A.2.2.7. Addressed by clauses [4.1.2; 4.1.3; 4.1.5; 4.1.6; 4.3.1; 4.7.5; 7.2].

13.6 ISO/IEC 27701:2025 - Annex A.2.3.2. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.3.5].

13.7 ISO/IEC 27701:2025 - Annex A.2.4.2; Annex A.2.4.3; Annex A.2.4.4. Addressed by clauses [4.6.1; 4.6.2; 4.6.3; 4.6.4; 4.6.5; 4.6.6].

13.8 ISO/IEC 27701:2025 - Annex A.2.5.2; Annex A.2.5.3. Addressed by clauses [4.2.6; 4.4.4; 4.5.1; 4.5.2; 7.5; 11.4].

13.9 ISO/IEC 27701:2025 - Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6. Addressed by clauses [4.5.3; 4.5.4; 4.7.2; 4.7.5].

13.10 ISO/IEC 27701:2025 - Annex A.2.5.7; Annex A.2.5.8; Annex A.2.5.9. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 4.4.6].

13.11 ISO/IEC 27701:2025 - Annex A.3.8; Annex A.3.9; Annex A.3.14; Annex A.3.24; Annex A.3.25. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.2.6; 4.7.3; 5.4; 5.6; 11.3].

13.12 GDPR - Article 28. Addressed by clauses [4.1.2; 4.1.3; 4.3.1; 4.3.2; 4.3.4; 4.4.2; 4.4.3; 4.4.5; 4.6.1; 4.6.3; 4.6.5; 4.7.2].

13.13 GDPR - Article 30. Addressed by clauses [4.1.1; 4.1.3; 4.4.1; 4.8.1; 7.1].

13.14 GDPR - Article 32; Article 33. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.7.1; 4.7.2; 4.7.3; 4.7.4; 4.7.5; 7.6].

13.15 GDPR - Article 44. Addressed by clauses [4.2.6; 4.4.4; 4.5.1; 4.5.2; 7.5; 11.4].

13.16 ISO/IEC 29100:2020 - Clause 5.3; Clause 5.5; Clause 5.6. Addressed by clauses [4.1.1; 4.1.2; 4.1.6; 4.2.6; 4.5.1; 4.6.1; 4.6.3].

13.17 ISO/IEC 29100:2020 - Clause 5.10; Clause 5.11; Clause 5.12. Addressed by clauses [4.1.4; 4.1.5; 4.2.1; 4.2.4; 4.3.5; 4.8.1; 4.8.4; 6.1; 8.5; 10.5].

13.18 ISO/IEC 29151:2022 - Clause 15.1.2; Clause 15.2.2; Clause 15.2.3; Annex A.7; Annex A.7.2. Addressed by clauses [4.4.1; 4.4.6; 4.6.1; 4.6.2; 4.6.3; 4.6.4; 4.8.3].

13.19 ISO/IEC 27001:2022 - Clause 6.1.3; Clause 8.1; Annex A controls 5.19; 5.20; 5.21; 5.22; 5.23. Addressed by clauses [4.1.4; 4.2.1; 4.4.1; 4.4.3; 4.4.6; 4.8.1; 4.8.3; 6.1; 7.1; 11.5].

13.20 ISO/IEC 27002:2022 - Control 5.19; Control 5.20; Control 5.21; Control 5.22; Control 5.23; Control 8.10; Control 8.15; Control 8.16. Addressed by clauses [4.2.1; 4.2.4; 4.4.1; 4.4.3; 4.4.6; 4.6.1; 4.6.3; 4.7.3; 4.8.3; 11.3].

13.21 ISO/IEC 27018:2020 - Annex A.2.1; Annex A.3.1. Addressed by clauses [4.1.2; 4.1.6; 4.3.1; 4.3.2; 4.3.3; 4.3.5].

13.22 ISO/IEC 27018:2020 - Annex A.6.1; Annex A.6.2; Annex A.8.1. Addressed by clauses [4.4.1; 4.4.2; 4.4.5; 4.5.3; 4.5.4].

13.23 ISO/IEC 27018:2020 - Annex A.10.1; Annex A.10.3; Annex A.11.11; Annex A.11.12; Annex A.12.1. Addressed by clauses [4.2.6; 4.4.3; 4.4.4; 4.6.1; 4.6.3; 4.6.5; 4.7.1; 4.7.2; 4.7.5].

13.24 ISO/IEC 27036-2:2022 - Clause 6.1.1; Clause 6.1.2. Addressed by clauses [4.1.1; 4.2.1; 4.4.1; 4.4.6; 6.1; 7.2].

13.25 ISO/IEC 27036-2:2022 - Clause 7.1; Clause 7.2; Clause 7.3; Clause 7.4; Clause 7.5. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.4.5; 4.4.6; 4.8.2; 4.8.3; 10.3; 11.2].

13.26 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. Addressed by clauses [4.6.1; 4.6.2; 4.6.3; 4.6.4; 4.6.5; 4.6.6].

13.27 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. Addressed by clauses [4.6.2; 4.6.3; 4.6.4; 4.6.5; 4.6.6; 9.1; 9.4].