					Introduzca aquí la denominación de la entidad jurídica registrada							
Número de documento: PII15					Título del documento: **Política de gestión de incidentes y brechas de seguridad 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

Norma / Regulación	Cláusula / Control / Artículo	Applicability	Coverage Type	Comentario
ISO/IEC 27701:2025	Clause 7.4; Clause 7.5	Both	Supporting	Comunicaciones del PIMS y evidencias documentadas de brechas de seguridad
ISO/IEC 27701:2025	Clause 8.1; Clause 8.2; Clause 8.3	Both	Supporting	Control operacional, evaluación de riesgos de privacidad y vínculo con el tratamiento
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Seguimiento, evaluación, no conformidad, acción correctiva y mejora
ISO/IEC 27701:2025	Annex A.3.11	Both	Primary	Planificación y preparación de la gestión de incidentes para el tratamiento de PII
ISO/IEC 27701:2025	Annex A.3.12	Both	Primary	Respuesta a incidentes de seguridad de la información que involucren PII
ISO/IEC 27701:2025	Annex A.3.13; Annex A.3.14	Both	Supporting	Requisitos legales, estatutarios, reglamentarios y contractuales, y protección de registros
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.6	Processor	Supporting	Acuerdo del encargado del tratamiento con el cliente y apoyo a las obligaciones del cliente
GDPR	Article 5(2); Article 24	Controller	Supporting	Responsabilidad proactiva y responsabilidad del responsable del tratamiento

GDPR	Article 26	Joint Controller	Supporting	Coordinación de la responsabilidad por brechas de seguridad entre corresponsables del tratamiento
GDPR	Article 28	Both	Supporting	Asistencia del encargado del tratamiento y obligaciones contractuales del encargado del tratamiento
GDPR	Article 32	Both	Supporting	Seguridad del tratamiento y capacidad de detección de brechas de seguridad
GDPR	Article 33	Both	Primary	Notificación de brechas de seguridad de datos personales y documentación de brechas de seguridad
GDPR	Article 34	Controller	Primary	Comunicación de brechas de seguridad de datos personales a los interesados afectados
GDPR	Article 39	Conditional	Supporting	Asesoramiento del DPO, supervisión, cooperación y apoyo como punto de contacto
ISO/IEC 29100:2020	Clause 5.11; Clause 5.12	Both	Supporting	Principios de seguridad de la información y cumplimiento de la privacidad
ISO/IEC 29151:2022	Clause 16.1.2; Clause 16.1.3	Both	Supporting	Responsabilidades de respuesta a incidentes de PII y notificación de eventos
ISO/IEC 27002:2022	Control 5.24; Control 5.25;	Both	Supporting	Planificación, evaluación,

	Control 5.26; Control 5.27; Control 5.28			respuesta, lecciones aprendidas y recopilación de evidencias de incidentes
ISO/IEC 27035-1:2023	Clause 5.2; Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6	Both	Supporting	Ciclo de vida del proceso de gestión de incidentes
ISO/IEC 27035-2:2023	Clause 4; Clause 6; Clause 10; Clause 11; Clause 12	Both	Supporting	Política, plan, concienciación, pruebas y lecciones aprendidas de incidentes
ISO/IEC 27035-3:2020	Clause 7; Clause 8; Clause 9; Clause 10; Clause 11; Clause 12	Both	Supporting	Operaciones de detección, notificación, triaje, análisis, respuesta e informes
ISO/IEC 27018:2020	Annex A.10.1	Conditional	Supporting	Expectativas de notificación y registro de brechas de seguridad para encargados del tratamiento en la nube
NIS2 Directive (EU) 2022/2555	Article 23	Conditional	Supporting	Notificación de incidentes significativos cuando sea aplicable
DORA Regulation (EU) 2022/2554	Article 17; Article 18; Article 19	Conditional	Supporting	Gestión, clasificación y notificación de incidentes de TIC cuando sea aplicable

1. Alcance

1.1 Esta política define los requisitos para identificar, notificar, triar, evaluar, contener, notificar externamente, documentar, cerrar y mejorar a partir de incidentes de PII y brechas de seguridad de PII dentro del alcance del PIMS.

1.2 Esta política se aplica a:

1.2.1 la organización cuando actúa como responsable del tratamiento de PII;

1.2.2 la organización cuando actúa como corresponsable del tratamiento cuando se requiere coordinación de la responsabilidad por brechas de seguridad;

1.2.3 la organización cuando actúa como encargado del tratamiento de PII;

1.2.4 la organización cuando actúa como subencargado del tratamiento;

1.2.5 sistemas, aplicaciones, servicios, procesos, proveedores, encargados del tratamiento, subencargados del tratamiento y terceros que traten, almacenen, transmitan, den soporte, accedan o afecten de otro modo a PII dentro del alcance del PIMS.

1.3 Esta política utiliza REG10 - Registro de Incidentes y Brechas de Seguridad de PII como objeto de evidencia principal para la gestión de incidentes y brechas de seguridad de PII.

1.4 Esta política utiliza objetos de evidencia de apoyo de la siguiente manera:

1.4.1 REG01 para el alcance del PIMS y el contexto aplicable de partes interesadas, legal, contractual, sectorial y de notificación a clientes.

1.4.2 REG02 para las actividades de tratamiento afectadas, categorías de PII, categorías de interesados, finalidades y sistemas.

1.4.3 REG03 para la Declaración de Aplicabilidad y las actualizaciones de aplicabilidad de controles.

1.4.4 REG04 para el vínculo con riesgos de privacidad, DPIA y riesgo residual.

1.4.5 REG08 para evidencias de interfaz de incidentes con encargados del tratamiento, subencargados del tratamiento, clientes, proveedores y terceros.

1.4.6 REG09 para el vínculo con transferencias internacionales cuando un incidente afecte al tratamiento transfronterizo.

1.4.7 REG11 para evidencias de formación, concienciación y competencia en respuesta a incidentes.

1.4.8 REG12 para evidencias de auditoría, no conformidad, acción correctiva y mejora.

1.5 Esta política se apoya en políticas PIMS relacionadas para controles especializados:

1.5.1 PII03 regula el inventario de tratamientos y los registros de base jurídica.

1.5.2 PII04 regula los controles de aviso de privacidad y transparencia fuera de las comunicaciones específicas de brechas de seguridad.

1.5.3 PII06 regula las solicitudes de derechos de los interesados que surgen antes, durante o después de un incidente.

1.5.4 PII07 regula la metodología de evaluación de riesgos de privacidad y DPIA.

1.5.5 PII08 regula los controles de privacidad desde el diseño y por defecto.

1.5.6 PII10 regula los controles de conservación, supresión y eliminación.

1.5.7 PII12 regula los controles de relaciones de privacidad con encargados del tratamiento, subencargados del tratamiento, proveedores y terceros.

1.5.8 PII13 regula los mecanismos de transferencia internacional de PII y los registros de riesgo de transferencia.

1.5.9 PII14 regula los controles preventivos y detectivos de seguridad y acceso de PII.

1.5.10 PII16 regula la formación, concienciación y competencia en privacidad.

1.5.11 PII17 regula la información documentada y la gestión de evidencias.

1.5.12 PII18 regula el seguimiento, la auditoría interna, la revisión por la dirección, la no conformidad, la acción correctiva y la mejora continua.

1.6 A efectos de esta política:

1.6.1 "Incidente de PII" significa un evento sospechado o confirmado que ha afectado, puede haber afectado o podría afectar razonablemente a la confidencialidad, integridad, disponibilidad, tratamiento lícito o manejo autorizado de PII.

1.6.2 "Brecha de seguridad de PII" significa un incidente de PII confirmado que involucra destrucción, pérdida, alteración, divulgación, acceso, indisponibilidad o compromiso de PII no autorizado, ilícito, accidental o no previsto.

1.6.3 "Evaluación de la brecha de seguridad" significa la evaluación documentada de si un incidente de PII es una brecha de seguridad de PII, qué PII e interesados están afectados, qué riesgos pueden surgir, qué notificaciones o comunicaciones son necesarias y qué acción correctiva se necesita.

1.6.4 "Conocimiento" significa el momento en que la organización tiene un grado razonable de certeza de que se ha producido un incidente de seguridad o privacidad y de que PII se ha visto o puede haberse visto comprometida.

1.6.5 "Incidente de datos personales de alto impacto" significa un incidente de PII que involucra tratamiento de alto riesgo, categorías especiales o PII altamente sensible, PII a gran escala, personas vulnerables, clientes regulados, impacto multijurisdiccional, impacto material en clientes, compromiso de acceso privilegiado, exposición pública, ransomware, indisponibilidad del servicio o impacto operacional o reputacional significativo.

1.6.6 "Cambio material del incidente" significa información nueva o modificada que afecta al alcance del incidente, la severidad, las categorías de PII, el impacto en los interesados, la decisión de notificación, el impacto en clientes, la causa raíz, la contención, la recuperación, la acción correctiva o las obligaciones de notificación externa.

2. Finalidad

2.1 La finalidad de esta política es asegurar que los incidentes y brechas de seguridad de PII se gestionen de forma coherente, oportuna, lícita, segura y con evidencias preparadas para auditoría.

2.2 Esta política respalda la responsabilidad proactiva al exigir que los incidentes y brechas de seguridad de PII se registren en REG10 y se vinculen, cuando se activen, con los registros de tratamiento afectados, riesgos de privacidad, relaciones con encargados del tratamiento y subencargados del tratamiento, registros de transferencia, acciones correctivas y registros de formación.

2.3 Esta política asegura que las obligaciones del responsable del tratamiento, corresponsable del tratamiento, encargado del tratamiento y subencargado del tratamiento se gestionen mediante reglas de aplicabilidad diferenciadas, manteniendo al mismo tiempo un modelo integrado de evidencias de incidentes y brechas de seguridad.

3. Objetivos

3.1 Los objetivos de esta política son:

3.1.1 asegurar que los incidentes de PII sospechados se notifiquen y registren oportunamente;

3.1.2 asegurar que los incidentes de PII se trien y clasifiquen utilizando criterios coherentes;

3.1.3 asegurar que las evaluaciones de brechas de seguridad consideren la PII afectada, los interesados, sistemas, actividades de tratamiento, encargados del tratamiento, subencargados del tratamiento, transferencias, riesgos y acciones correctivas;

3.1.4 asegurar que las decisiones de notificación del responsable del tratamiento y de comunicación a los interesados se documenten;

3.1.5 asegurar que las notificaciones de brechas de seguridad por parte de encargados del tratamiento y subencargados del tratamiento a clientes o partes ascendentes se realicen sin dilación indebida y conforme a los acuerdos aplicables;

3.1.6 asegurar que las evidencias se preserven y protejan durante la gestión de incidentes;

3.1.7 asegurar que la contención, erradicación, recuperación y validación se supervisen a través de REG10;

3.1.8 asegurar que se evalúen, cuando proceda, los desencadenantes de notificación regulados, contractuales, de clientes y sectoriales;

3.1.9 asegurar que las lecciones aprendidas de incidentes den lugar a acción correctiva y mejora continua;

3.1.10 asegurar que los registros de incidentes y brechas de seguridad estén disponibles para auditoría, revisión por la dirección, aseguramiento de clientes y revisión regulatoria cuando proceda.

4. Declaraciones de política

4.1 Preparación y recepción y registro de incidentes

4.1.1 [Both] Privacy Lead / PIMS Manager MUST mantener los criterios de gestión de incidentes y brechas de seguridad de PII en REG10 al menos anualmente y después de cualquier cambio material en el alcance del PIMS, el contexto legal, las obligaciones contractuales o el tratamiento de alto riesgo.

4.1.2 [All] Incident Response Coordinator MUST registrar cada incidente de PII sospechado que sea notificado o detectado en REG10 dentro de un día hábil desde su recepción, o antes cuando pueda activarse un plazo aplicable de notificación o de reporte a clientes.

4.1.3 [Both] System Owner / Application Owner MUST preservar los registros del sistema, alertas, registros de acceso, evidencias de configuración y evidencias de recuperación pertinentes vinculados a REG10 cuando un incidente sospechado afecte a un sistema o aplicación que trate PII.

4.1.4 [Both] Information Security Lead MUST completar el triaje técnico inicial de cualquier evento de seguridad que involucre PII dentro de las 24 horas siguientes a su detección y registrar en REG10 la severidad inicial, los activos afectados y el estado de contención.

4.2 Clasificación y evaluación de brechas de seguridad

4.2.1 [Both] Incident Response Coordinator MUST clasificar cada entrada de REG10 como evento no relacionado con PII, incidente de PII sospechado, incidente de PII confirmado o brecha de seguridad de PII confirmada dentro de las 24 horas desde la recepción, o actualizar el registro REG10 con la razón por la que la clasificación sigue pendiente.

4.2.2 [Both] Privacy Lead / PIMS Manager MUST identificar la actividad de tratamiento afectada, las categorías de PII, las categorías de interesados, los sistemas, encargados del tratamiento, subencargados del tratamiento, ubicaciones de transferencia y riesgos de privacidad en REG02, REG04, REG08, REG09 y REG10 antes de finalizar la decisión sobre la notificación de la brecha de seguridad.

4.2.3 [Controller] Data Protection Officer / Privacy Advisor MUST evaluar el riesgo para los interesados afectados por cada brecha de seguridad de PII confirmada o razonablemente sospechada y registrar la recomendación de notificación, la justificación del riesgo y el asesoramiento en REG10 antes de tomar la decisión de notificación externa.

4.2.4 [Processor] Privacy Lead / PIMS Manager MUST identificar al responsable del tratamiento o cliente afectado y los requisitos contractuales de notificación aplicables tan pronto como la organización tenga conocimiento de una brecha de seguridad de PII que afecte a PII del cliente, y MUST registrar el resultado en REG08 y REG10.

4.2.5 [Joint Controller] Privacy Lead / PIMS Manager MUST verificar la responsabilidad acordada por brechas de seguridad, la responsabilidad principal de comunicación y el acuerdo de coordinación antes de cualquier notificación o comunicación externa por parte de un corresponsable del tratamiento, y MUST registrar la decisión en REG08 y REG10.

4.2.6 [Conditional] Privacy Lead / PIMS Manager MUST evaluar los desencadenantes aplicables de notificación legal, sectorial, del sector financiero, de ciberseguridad, contractual, de clientes y de destinatarios del servicio para cada incidente de datos personales de alto impacto y registrar el resultado de aplicabilidad en REG01, REG08 y REG10.

[... 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] Privacy Lead / PIMS Manager MUST registrar cualquier excepción a esta política en REG12 antes de su implementación, o dentro de las 24 horas posteriores a una acción de emergencia cuando la aprobación previa no haya sido viable.

9.1.2 [Both] Top Management MUST aprobar cualquier excepción que afecte materialmente al plazo de notificación de brechas de seguridad, comunicación pública, compromiso con clientes, preservación de evidencias o riesgo para interesados antes de cerrar el incidente, con evidencias de aprobación conservadas en REG10 y REG12.

9.1.3 [Conditional] Data Protection Officer / Privacy Advisor MUST documentar asesoramiento para cualquier notificación demorada, decisión de no notificación o enfoque excepcional de comunicación antes del cierre del incidente, con el asesoramiento conservado en REG10.

9.1.4 [Both] Vendor / Procurement Owner MUST registrar en REG08 y REG12 las excepciones impulsadas por proveedores, encargados del tratamiento, subencargados del tratamiento o clientes que afecten a la respuesta a incidentes dentro de los cinco días hábiles posteriores a la identificación de la excepción.

10. Aplicación

10.1.1 [All] Process Owner / Business Owner MUST escalar el incumplimiento de notificar un incidente de PII sospechado, preservar evidencias, seguir acciones asignadas o cooperar con la evaluación de la brecha de seguridad a Privacy Lead / PIMS Manager dentro de los dos días hábiles posteriores a su descubrimiento, con evidencias conservadas en REG12.

10.1.2 [Both] Privacy Lead / PIMS Manager MUST registrar una no conformidad REG12 cuando un incumplimiento de esta política afecte a la recepción, triaje, contención, notificación, integridad de evidencias, comunicación o acción correctiva de incidentes.

10.1.3 [Both] Vendor / Procurement Owner MUST iniciar la remediación de proveedores o encargados del tratamiento a través de REG08 y REG12 dentro de los cinco días hábiles cuando un encargado del tratamiento, subencargado del tratamiento, proveedor u otro tercero no cumpla las obligaciones acordadas de incidentes o brechas de seguridad.

10.1.4 [Both] Top Management MUST revisar no conformidades materiales o recurrentes de gestión de incidentes en la siguiente revisión por la dirección programada, con decisiones y acciones requeridas conservadas en REG12.

11. Revisión y mantenimiento

11.1.1 [Both] Privacy Lead / PIMS Manager MUST revisar esta política al menos anualmente y registrar el resultado de la revisión, los cambios requeridos y el estado de aprobación en REG12.

11.1.2 [Both] Incident Response Coordinator MUST activar una revisión posterior al incidente de esta política dentro de los 30 días naturales posteriores al cierre de cualquier incidente de datos personales de alto impacto o brecha de seguridad de PII confirmada, con evidencias de revisión conservadas en REG10 y REG12.

11.1.3 [Conditional] Privacy Lead / PIMS Manager MUST revisar esta política dentro de los 30 días naturales posteriores a tener conocimiento de un cambio material en requisitos aplicables legales, sectoriales, de clientes, contractuales, de encargados del tratamiento, subencargados del tratamiento o relacionados con transferencias para la notificación de incidentes, con evidencias de revisión conservadas en REG01, REG08, REG09 y REG12.

11.1.4 [Both] Internal Audit / Compliance Reviewer MUST revisar la implementación de esta política al menos anualmente a través del programa de auditoría interna del PIMS, con hallazgos de auditoría y acciones correctivas conservados en REG12.

11.1.5 [Both] Top Management MUST revisar tendencias de incidentes, brechas de seguridad significativas, desempeño de notificación, acciones correctivas vencidas y eficacia de la política durante la revisión por la dirección programada, con resultados conservados en REG12.

12. Políticas relacionadas

12.1 Esta política debe 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 PII04 - Política de aviso de privacidad y transparencia

12.1.5 PII06 - Política de gestión de derechos de los interesados

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

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

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

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

12.1.10 PII13 - Política de transferencia internacional de PII

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

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

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

12.1.14 PII18 - Política de supervisión, auditoría y mejora del PIMS

13. Normas y marcos de referencia

13.1 ISO/IEC 27701:2025 - Clause 7.4; Clause 7.5. Addressed by clauses [4.4.7; 4.5.1; 4.5.3; 4.5.4; 5.2.2; 6.2.2; 7.1.1; 7.1.7; 11.1.3].

13.2 ISO/IEC 27701:2025 - Clause 8.1; Clause 8.2; Clause 8.3. Addressed by clauses [4.2.2; 4.3.4; 4.6.3; 6.3.1; 7.1.4; 11.1.2].

13.3 ISO/IEC 27701:2025 - Clause 9.1; Clause 10.2. Addressed by clauses [4.6.1; 4.6.2; 4.6.3; 4.6.4; 6.4.1; 6.5.1; 8.1.1; 8.1.4; 10.1.2; 11.1.4; 11.1.5].

13.4 ISO/IEC 27701:2025 - Annex A.3.11. Addressed by clauses [4.1.1; 4.1.2; 4.2.6; 4.4.1; 5.1.1; 5.4.1; 7.1.1; 7.1.2; 7.1.6].

13.5 ISO/IEC 27701:2025 - Annex A.3.12. Addressed by clauses [4.1.3; 4.1.4; 4.2.1; 4.2.3; 4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.4.1; 4.4.3; 4.4.4; 4.5.1; 4.5.4; 6.3.1].

13.6 ISO/IEC 27701:2025 - Annex A.3.13; Annex A.3.14. Addressed by clauses [4.2.6; 4.4.6; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.6.4; 6.2.2; 9.1.2; 11.1.3].

13.7 ISO/IEC 27701:2025 - Annex A.2.2.2; Annex A.2.2.6. Addressed by clauses [4.2.4; 4.4.4; 4.4.5; 4.5.5; 5.8.1; 7.1.5; 8.1.5; 10.1.3].

13.8 GDPR - Article 5(2); Article 24. Addressed by clauses [4.1.2; 4.2.2; 4.4.1; 4.5.1; 4.5.3; 4.5.4; 4.6.2; 5.2.1; 6.3.1; 8.1.3; 11.1.5].

13.9 GDPR - Article 26. Addressed by clauses [4.2.5; 4.4.1; 4.4.3; 5.3.1; 6.2.2; 11.1.3].

13.10 GDPR - Article 28. Addressed by clauses [4.2.4; 4.3.5; 4.4.4; 4.4.5; 4.5.5; 5.8.1; 7.1.5; 8.1.5; 10.1.3].

13.11 GDPR - Article 32. Addressed by clauses [4.1.3; 4.1.4; 4.3.2; 4.3.3; 4.5.2; 4.6.3; 5.5.1; 7.1.4; 8.1.2; 11.1.2].

13.12 GDPR - Article 33. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.4.1; 4.4.2; 4.4.4; 4.4.5; 4.5.1; 4.5.4; 8.1.3; 9.1.3].

13.13 GDPR - Article 34. Addressed by clauses [4.2.3; 4.2.5; 4.4.2; 4.4.3; 4.4.7; 4.5.4; 8.1.3; 9.1.3].

13.14 GDPR - Article 39. Addressed by clauses [4.2.3; 4.4.2; 5.3.1; 6.2.2; 9.1.3; 11.1.3].

13.15 ISO/IEC 29100:2020 - Clause 5.11; Clause 5.12. Addressed by clauses [4.2.2; 4.3.2; 4.3.3; 4.5.3; 4.6.2; 4.6.3; 5.2.2; 6.4.1; 8.1.4; 11.1.4].

13.16 ISO/IEC 29151:2022 - Clause 16.1.2; Clause 16.1.3. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.2.1; 4.2.3; 4.4.1; 4.4.3; 4.6.5; 7.1.3; 7.1.6].

13.17 ISO/IEC 27002:2022 - Control 5.24; Control 5.25; Control 5.26; Control 5.27; Control 5.28. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.1.4; 4.2.1; 4.3.1; 4.3.2; 4.3.3; 4.5.1; 4.5.2; 4.6.1; 4.6.2; 7.1.2; 7.1.6].

13.18 ISO/IEC 27035-1:2023 - Clause 5.2; Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.2.1; 4.3.1; 4.3.2; 4.4.7; 4.5.2; 4.6.1; 5.4.1; 7.1.6; 11.1.2].

13.19 ISO/IEC 27035-2:2023 - Clause 4; Clause 6; Clause 10; Clause 11; Clause 12. Addressed by clauses [4.1.1; 4.6.1; 4.6.5; 5.1.1; 7.1.1; 7.1.3; 7.1.6; 8.1.6; 11.1.1; 11.1.2].

13.20 ISO/IEC 27035-3:2020 - Clause 7; Clause 8; Clause 9; Clause 10; Clause 11; Clause 12. Addressed by clauses [4.1.2; 4.1.4; 4.2.1; 4.3.1; 4.3.2; 4.4.1; 4.4.4; 4.5.1; 5.4.2; 6.1.2; 8.1.2].

13.21 ISO/IEC 27018:2020 - Annex A.10.1. Addressed by clauses [4.2.4; 4.3.5; 4.4.4; 4.4.5; 4.5.5; 5.8.1; 7.1.5; 8.1.5].

13.22 NIS2 Directive (EU) 2022/2555 - Article 23. Addressed by clauses [4.2.6; 4.4.6; 4.4.7; 5.3.1; 6.2.2; 8.1.3; 11.1.3].

13.23 DORA Regulation (EU) 2022/2554 - Article 17; Article 18; Article 19. Addressed by clauses [4.2.1; 4.2.6; 4.4.6; 4.4.7; 5.1.2; 6.2.1; 8.1.3; 11.1.3; 11.1.5].