					Introduzca aquí la denominación de la entidad jurídica registrada							
Número de documento: PII15-FS					Título del documento: **Política de gestión de incidentes y brechas de seguridad de PII del sector financiero**							
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 7.4; Clause 7.5	Both	Supporting	Comunicaciones del PIMS y evidencias documentadas de incidentes
ISO/IEC 27701:2025	Clause 8.1; Clause 8.2; Clause 8.3	Both	Supporting	Control operacional y vinculación con la evaluación y el tratamiento de riesgos de privacidad
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Monitorización, 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 implican PII
ISO/IEC 27701:2025	Annex A.3.13; Annex A.3.14	Both	Supporting	Requisitos legales, estatutarios, regulatorios y contractuales, y protección de registros
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.6	Processor	Supporting	Acuerdo con el cliente del encargado del tratamiento y soporte 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 de incidentes 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 soporte como punto de contacto
DORA Regulation (EU) 2022/2554	Article 17	Conditional	Primary	Proceso de gestión de incidentes relacionados con las TIC para entidades financieras dentro del ámbito de aplicación
DORA Regulation (EU) 2022/2554	Article 18	Conditional	Primary	Criterios de clasificación de incidentes relacionados con las TIC y

				ciberamenazas significativas
DORA Regulation (EU) 2022/2554	Article 19	Conditional	Primary	Notificación de incidentes graves relacionados con las TIC y notificación de ciberamenazas significativas
DORA Regulation (EU) 2022/2554	Article 20	Conditional	Supporting	Contenido de la notificación, plazos, plantillas y procedimientos
NIS2 Directive (EU) 2022/2555	Article 23	Conditional	Supporting	Notificación de incidentes significativos cuando sea aplicable
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 ante incidentes de PII y notificación de eventos
ISO/IEC 27002:2022	Control 5.24; Control 5.25; Control 5.26; Control 5.27; Control 5.28	Both	Supporting	Planificación, evaluación, 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 sobre incidentes
ISO/IEC 27035-3:2020	Clause 7; Clause 8; Clause 9; Clause	Both	Supporting	Operaciones de detección,

	10; Clause 11; Clause 12			notificación, triaje, análisis, respuesta e informes
ISO/IEC 27018:2020	Annex A.10.1	Conditional	Supporting	Expectativas de notificación del encargado del tratamiento en nube pública y registros de brechas de seguridad

1. Alcance

1.1 Esta política define los requisitos para identificar, notificar, triar, clasificar, evaluar, contener, notificar formalmente, documentar, cerrar y mejorar a partir de incidentes de PII y brechas de seguridad de PII en alcances del PIMS del sector financiero.

1.2 **Aviso de implementación:** Esta política es una variante sustitutiva de PII15 para el sector financiero. No debe implementarse simultáneamente con PII15 para el mismo alcance del PIMS, unidad de negocio, producto, entorno de cliente, servicio regulado o perímetro de evidencias. Las organizaciones deben seleccionar PII15 o PII15-FS para el mismo alcance a fin de evitar obligaciones duplicadas de gestión de incidentes, registros duplicados y trabajo duplicado de evidencias de auditoría.

1.3 Esta política se aplica a:

1.3.1 la organización que actúa como responsable del tratamiento de PII en un contexto del sector financiero;

1.3.2 la organización que actúa como corresponsable del tratamiento cuando se requiere coordinación de responsabilidades por incidentes o brechas de seguridad;

1.3.3 la organización que actúa como encargado del tratamiento de PII para clientes del sector financiero;

1.3.4 la organización que actúa como subencargado del tratamiento para clientes del sector financiero o encargados del tratamiento aguas arriba;

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

1.4 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 del sector financiero.

1.5 Esta política utiliza objetos de evidencia de soporte de la siguiente manera:

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

1.5.2 REG02 para actividades de tratamiento afectadas, categorías de PII, categorías de interesados, finalidades, sistemas y servicios.

1.5.3 REG03 para la Declaración de Aplicabilidad y las actualizaciones de aplicabilidad de controles, incluida la sustitución de PII15 por PII15-FS para el mismo alcance.

1.5.4 REG04 para la vinculación con riesgos de privacidad, DPIA, riesgo residual y tratamiento de riesgos.

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

1.5.6 REG09 para la vinculación con transferencias internacionales cuando un incidente afecta al tratamiento transfronterizo.

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

1.5.8 REG12 para evidencias de auditoría, no conformidad, acción correctiva, revisión por la dirección y mejora.

1.6 Esta política se basa en políticas PIMS relacionadas para controles especializados:

1.6.1 PII03 rige el inventario de tratamientos y los registros de base jurídica.

1.6.2 PII04 rige los controles de aviso de privacidad y transparencia fuera de las comunicaciones específicas de brechas de seguridad.

1.6.3 PII06 rige las solicitudes de derechos de los interesados que surjan antes, durante o después de un incidente.

1.6.4 PII07 rige la metodología de evaluación de riesgos de privacidad y DPIA.

1.6.5 PII08 rige los controles de privacidad desde el diseño y por defecto.

1.6.6 PII10 rige los controles de conservación, supresión y eliminación.

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

1.6.8 PII13 rige los mecanismos de transferencia internacional de PII y los registros de riesgos de transferencia.

1.6.9 PII14 rige los controles preventivos y detectivos de seguridad de PII y control de acceso.

1.6.10 PII16 rige la formación, concienciación y competencia en privacidad.

1.6.11 PII17 rige la información documentada y la gestión de evidencias.

1.6.12 PII18 rige la monitorización, auditoría interna, revisión por la dirección, no conformidad, acción correctiva y mejora continua.

1.6.13 PII23 rige los controles del encargado del tratamiento de PII en la nube cuando las obligaciones del encargado en la nube estén dentro del alcance.

1.7 A efectos de esta política:

1.7.1 "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.

1.7.2 "Brecha de seguridad de PII" significa un incidente de PII confirmado que implica destrucción, pérdida, alteración, divulgación, acceso, indisponibilidad o compromiso de PII de forma no autorizada, ilícita, accidental o no prevista.

1.7.3 "Incidente de datos personales en el sector financiero" significa un incidente de PII que afecta, puede afectar o está razonablemente conectado con servicios financieros regulados, clientes del sector financiero, contrapartes financieras, transacciones financieras, operaciones financieras o tratamiento de PII del sector financiero.

1.7.4 "Incidente grave relacionado con las TIC en el sector financiero" significa un incidente de datos personales en el sector financiero o un incidente relacionado con las TIC que cumple criterios documentados de materialidad o notificación en REG10.

1.7.5 "Ciberamenaza significativa" significa una ciberamenaza registrada en REG10 que podría afectar materialmente a servicios del sector financiero, tratamiento de PII, clientes, contrapartes u operaciones dentro del alcance.

1.7.6 "Evaluación de la brecha de seguridad" significa la evaluación documentada de si un incidente de PII constituye una brecha de seguridad de PII, qué PII e interesados se ven afectados, qué riesgos pueden surgir, qué notificaciones o comunicaciones son necesarias y qué acción de remediación se requiere.

1.7.7 "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.

1.7.8 "Incidente de datos personales de alto impacto en el sector financiero" significa un incidente de PII que implica tratamiento de alto riesgo, categorías especiales o PII altamente sensible, PII a gran escala, personas vulnerables, clientes regulados, interrupción material del servicio, contrapartes financieras, transacciones financieras, impacto multijurisdiccional,

compromiso de acceso privilegiado, exposición pública, ransomware, indisponibilidad del servicio o impacto operacional, de cliente, financiero o reputacional significativo.

1.7.9 "Cambio material del incidente" significa información nueva o modificada que afecta al alcance del incidente, severidad, categorías de PII, impacto en interesados, impacto en el servicio, clasificación del sector financiero, decisión de notificación, impacto en clientes, causa raíz, contención, recuperación, acción correctiva u obligaciones de notificación externa.

2. Finalidad

2.1 La finalidad de esta política es garantizar que los incidentes y brechas de seguridad de PII en contextos del sector financiero se gestionen de forma coherente, pronta, 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 del sector financiero se registren en REG10 y se vinculen a registros de tratamiento afectados, riesgos de privacidad, relaciones con encargados y subencargados del tratamiento, registros de transferencia, acciones correctivas, registros de formación, decisiones de notificación del sector financiero y evidencias de revisión por la dirección cuando se activen.

2.3 Esta política garantiza 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 único modelo integrado de evidencias de incidentes y brechas de seguridad del sector financiero.

3. Objetivos

3.1 Los objetivos de esta política son:

3.1.1 garantizar que los incidentes de PII sospechados del sector financiero se notifiquen y registren con prontitud;

3.1.2 garantizar que los incidentes de PII del sector financiero se trien y clasifiquen utilizando criterios coherentes de privacidad, seguridad, operacionales y sectoriales;

3.1.3 garantizar que las evaluaciones de brechas de seguridad consideren PII afectada, interesados, sistemas, servicios, actividades de tratamiento, encargados del tratamiento, subencargados del tratamiento, transferencias, riesgos, clientes, contrapartes y acciones de remediación;

3.1.4 garantizar que las decisiones de notificación del responsable del tratamiento y de comunicación a los interesados queden documentadas;

3.1.5 garantizar que las notificaciones de brechas de seguridad del encargado del tratamiento y del subencargado del tratamiento a clientes o partes aguas arriba se realicen sin dilación indebida y de conformidad con los acuerdos aplicables;

3.1.6 garantizar que los desencadenantes de notificación del sector financiero se evalúen, documenten y supervisen cuando proceda;

3.1.7 garantizar que las evidencias se conserven y protejan durante la gestión de incidentes;

3.1.8 garantizar que la contención, erradicación, recuperación y validación se supervisen mediante REG10;

3.1.9 garantizar que las ciberamenazas significativas y los incidentes graves relacionados con las TIC en el sector financiero se dirijan a los flujos de decisión y notificación adecuados;

3.1.10 garantizar que las lecciones aprendidas de incidentes se traduzcan en acciones correctivas, formación, mejora de controles y revisión por la dirección;

3.1.11 garantizar 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;

3.1.12 garantizar que PII15-FS sustituya a PII15 para el mismo alcance del sector financiero y no duplique el trabajo de evidencias de PII15.

4. Declaraciones de la política

4.1 Activación de la variante, preparación y recepción y registro

4.1.1 [Conditional] Privacy Lead / PIMS Manager DEBE documentar la activación de PII15-FS en REG01 y REG03 antes de utilizar esta política para un alcance del PIMS del sector financiero.

4.1.2 [Conditional] Privacy Lead / PIMS Manager DEBE documentar en REG03 y REG12 que PII15 no se implementa simultáneamente para el mismo alcance del PIMS del sector financiero antes de que se apruebe PII15-FS.

4.1.3 [All] Incident Response Coordinator DEBE registrar cada incidente de PII sospechado del sector financiero que se notifique o detecte en REG10 en el plazo de un día hábil desde su recepción, o antes cuando pueda activarse un plazo aplicable de notificación, cliente o reporte.

4.1.4 [Conditional] Privacy Lead / PIMS Manager DEBE mantener criterios de gestión de incidentes y brechas de seguridad de PII del sector financiero en REG10 al menos anualmente y después de cualquier cambio material en el alcance del PIMS, contexto legal, obligaciones de clientes, obligaciones contractuales, contexto de reporte sectorial o tratamiento de alto riesgo.

4.1.5 [Both] Information Security Lead DEBE confirmar los requisitos de conservación de evidencias de incidentes en REG10 dentro de las 24 horas posteriores a que un incidente sospechado afecte a un sistema, servicio o aplicación que trate PII.

4.1.6 [Conditional] Vendor / Procurement Owner DEBE mantener los requisitos de contacto de incidentes de terceros del sector financiero y de encaminamiento de evidencias en REG08 antes de la incorporación y al menos anualmente para encargados del tratamiento, subencargados del tratamiento, proveedores y proveedores externalizados de reporte dentro del alcance.

4.2 Clasificación y evaluación de brechas de seguridad

4.2.1 [All] Incident Response Coordinator DEBE clasificar cada entrada de REG10 dentro de las 24 horas posteriores a la recepción y registro como evento no relacionado con PII, incidente de PII sospechado, incidente de PII confirmado, brecha de seguridad de PII confirmada, incidente de PII del sector financiero, incidente grave relacionado con las TIC en el sector financiero, ciberamenaza significativa o entrada pendiente de clasificación.

4.2.2 [Conditional] Information Security Lead DEBE evaluar en REG10 los servicios, clientes, contrapartes, transacciones, indisponibilidad del servicio, extensión geográfica, pérdida de datos, criticidad del servicio e impacto económico afectados cuando un incidente de PII pueda afectar a servicios u operaciones del sector financiero.

4.2.3 [Both] Privacy Lead / PIMS Manager DEBE identificar la actividad de tratamiento afectada, categorías de PII, categorías de interesados, 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.

4.2.4 [Controller] Data Protection Officer / Privacy Advisor DEBE evaluar el riesgo para los interesados afectados respecto de 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 adoptar la decisión de notificación externa.

4.2.5 [Joint Controller] Privacy Lead / PIMS Manager DEBE registrar la asignación de responsabilidades del corresponsable del tratamiento en REG08 y REG10 dentro de las 24

horas posteriores a la identificación de responsabilidad compartida por una brecha de seguridad de PII sospechada o confirmada.

4.2.6 [Processor] Privacy Lead / PIMS Manager DEBE evaluar las instrucciones del cliente, las obligaciones contractuales de notificación y las obligaciones de cooperación en REG08 y REG10 dentro de las 24 horas posteriores a que una brecha de seguridad de PII sospechada o confirmada afecte al tratamiento realizado como encargado del tratamiento.

4.2.7 [Subprocessor] Vendor / Procurement Owner DEBE identificar la cadena de notificación ascendente y el encaminamiento de evidencias requerido en REG08 y REG10 dentro de las 24 horas posteriores a que un incidente de PII sospechado o confirmado afecte al tratamiento realizado como 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 [All] Privacy Lead / PIMS Manager DEBE 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 [Conditional] Top Management DEBE aprobar cualquier excepción que afecte materialmente al calendario de notificación de brechas de seguridad, calendario de reporte del sector financiero, comunicación pública, compromiso con clientes, conservación de evidencias o riesgo para interesados antes del cierre del incidente, conservando evidencias de aprobación en REG10 y REG12.

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

9.1.4 [Both] Vendor / Procurement Owner DEBE registrar excepciones de proveedores, encargados del tratamiento, subencargados del tratamiento, clientes o proveedores externalizados que afecten a la respuesta a incidentes del sector financiero en REG08 y REG12 dentro de cinco días hábiles desde la identificación de la excepción.

9.1.5 [All] Privacy Lead / PIMS Manager DEBE revisar al menos mensualmente las excepciones abiertas a esta política hasta su cierre, conservando el estado de revisión en REG12.

10. Aplicación

10.1.1 [All] Process Owner / Business Owner DEBE escalar el incumplimiento de notificar un incidente de PII sospechado del sector financiero, conservar evidencias, seguir acciones asignadas o cooperar con la evaluación de brechas de seguridad a Privacy Lead / PIMS Manager dentro de dos días hábiles desde su descubrimiento, conservando evidencias en REG12.

10.1.2 [Both] Incident Response Coordinator DEBE escalar la notificación tardía, clasificación omitida, evidencias faltantes, escalado omitido o acción de contención vencida a Privacy Lead / PIMS Manager dentro de un día hábil desde la identificación del problema, conservando evidencias en REG10 y REG12.

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

10.1.4 [Both] Vendor / Procurement Owner DEBE iniciar la remediación de proveedores, encargados del tratamiento, subencargados del tratamiento o proveedores externalizados

mediante REG08 y REG12 dentro de cinco días hábiles cuando un tercero no cumpla las obligaciones acordadas de incidente, brecha de seguridad, evidencia o reporte.

10.1.5 [Conditional] Top Management DEBE revisar las no conformidades materiales o recurrentes de PII15-FS en la siguiente revisión por la dirección programada, conservando decisiones y acciones requeridas en REG12.

10.1.6 [All] Privacy Lead / PIMS Manager DEBE activar formación correctiva en REG11 dentro de los 30 días naturales cuando una no conformidad de la política implique concienciación del rol, notificación tardía, fallo de escalado, fallo en el manejo de evidencias o fallo de comunicación.

11. Revisión y mantenimiento

11.1.1 [Conditional] Privacy Lead / PIMS Manager DEBE 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 [Conditional] Incident Response Coordinator DEBE activar una revisión posterior al incidente de esta política dentro de los 30 días naturales posteriores al cierre de cualquier incidente de PII de alto impacto del sector financiero, brecha de seguridad de PII confirmada, incidente grave relacionado con las TIC en el sector financiero o ciberamenaza significativa, conservando evidencias de revisión en REG10 y REG12.

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

11.1.4 [Both] Internal Audit / Compliance Reviewer DEBE revisar la implementación de esta política al menos anualmente mediante el programa de auditoría interna del PIMS, conservando hallazgos de auditoría y acciones correctivas en REG12.

11.1.5 [Conditional] Top Management DEBE revisar tendencias de incidentes, brechas de seguridad significativas, desempeño de reporte, acciones correctivas vencidas y eficacia de la política durante la revisión por la dirección programada, conservando los resultados en REG12.

11.1.6 [Conditional] Privacy Lead / PIMS Manager DEBE revisar la relación de sustitución entre PII15-FS y PII15 al menos anualmente y después de cualquier cambio de alcance del PIMS para verificar que ambas políticas no se implementen para el mismo alcance del sector financiero, conservando evidencias de revisión en REG03 y 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 en 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 de PII y control de acceso

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

12.1.15 PII23 - Política de encargado del tratamiento de PII en la nube, cuando las obligaciones del encargado en la nube del sector financiero estén dentro del alcance

12.2 PII15 - Política de gestión de incidentes y brechas de seguridad de PII es la política de referencia de incidentes y brechas de seguridad. PII15-FS es una variante sustitutiva de PII15 para el sector financiero. PII15 y PII15-FS no deben implementarse simultáneamente para el mismo alcance del PIMS, unidad de negocio, producto, entorno de cliente, servicio regulado o perímetro de evidencias.

13. Normas y marcos de referencia

13.1 ISO/IEC 27701:2025 - Clause 7.4; Clause 7.5. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.4.8; 4.5.1; 4.5.4; 4.5.5; 5.2.2; 7.1.1; 11.1.3].

13.2 ISO/IEC 27701:2025 - Clause 8.1; Clause 8.2; Clause 8.3. Addressed by clauses [4.1.3; 4.2.3; 4.3.1; 4.3.4; 4.3.5; 4.7.3; 6.1.4; 7.1.4].

13.3 ISO/IEC 27701:2025 - Clause 9.1; Clause 10.2. Addressed by clauses [4.7.1; 4.7.2; 4.7.6; 6.1.3; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 8.1.6; 9.1.1; 10.1.1; 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; 4.1.4; 4.1.6; 5.1.1; 6.1.1; 7.1.2; 7.1.6; 7.1.7].

13.5 ISO/IEC 27701:2025 - Annex A.3.12. Addressed by clauses [4.1.3; 4.1.5; 4.2.1; 4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.6.1; 4.6.2].

13.6 ISO/IEC 27701:2025 - Annex A.3.13; Annex A.3.14. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 4.4.6; 4.4.7; 4.4.8; 4.4.9; 4.4.10; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 4.5.6; 4.5.7; 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 [4.2.6; 4.2.7; 4.3.6; 4.4.4; 4.4.5; 4.4.10; 4.5.6; 5.7.1; 7.1.3; 8.1.5; 10.1.4].

13.8 GDPR - Article 5(2); Article 24. Addressed by clauses [4.1.2; 4.2.3; 4.4.1; 4.5.1; 4.7.2; 5.2.1; 6.1.1; 8.1.2; 11.1.6].

13.9 GDPR - Article 26. Addressed by clauses [4.2.5; 4.4.6; 4.5.1].

13.10 GDPR - Article 28. Addressed by clauses [4.2.6; 4.2.7; 4.4.4; 4.4.5; 4.5.6; 7.1.3; 10.1.4].

13.11 GDPR - Article 32. Addressed by clauses [4.1.5; 4.3.1; 4.3.2; 4.3.4; 4.5.2; 4.7.3; 7.1.4].

13.12 GDPR - Article 33. Addressed by clauses [4.2.3; 4.2.4; 4.4.1; 4.4.2; 4.5.4; 8.1.2].

13.13 GDPR - Article 34. Addressed by clauses [4.4.3; 4.5.4].

13.14 GDPR - Article 39. Addressed by clauses [4.2.4; 4.4.3; 5.3.1; 6.1.4; 9.1.3].

13.15 DORA Regulation (EU) 2022/2554 - Article 17. Addressed by clauses [4.1.3; 4.1.4; 4.1.5; 4.2.1; 4.3.1; 4.3.3; 4.3.4; 4.3.6; 4.4.7; 4.5.1; 4.7.1; 5.4.1; 6.1.2; 7.1.7].

13.16 DORA Regulation (EU) 2022/2554 - Article 18. Addressed by clauses [4.2.1; 4.2.2; 4.6.1; 4.6.2; 4.6.3; 8.1.3].

13.17 DORA Regulation (EU) 2022/2554 - Article 19. Addressed by clauses [4.4.7; 4.4.8; 4.4.9; 4.4.10; 4.5.5; 8.1.3].

13.18 DORA Regulation (EU) 2022/2554 - Article 20. Addressed by clauses [4.4.8; 4.5.5; 6.1.4; 7.1.2; 8.1.3; 11.1.3].

13.19 NIS2 Directive (EU) 2022/2555 - Article 23. Addressed by clauses [4.4.7; 4.4.8; 4.5.5; 6.1.4; 8.1.3; 11.1.3].

13.20 ISO/IEC 29100:2020 - Clause 5.11; Clause 5.12. Addressed by clauses [4.1.2; 4.2.3; 4.4.1; 4.4.3; 4.5.1; 4.5.3; 4.7.2; 5.2.1; 8.1.2].

13.21 ISO/IEC 29151:2022 - Clause 16.1.2; Clause 16.1.3. Addressed by clauses [4.1.3; 4.1.5; 4.2.1; 4.3.1; 4.4.1; 4.5.1; 4.5.2; 4.7.1].

13.22 ISO/IEC 27002:2022 - Control 5.24; Control 5.25; Control 5.26; Control 5.27; Control 5.28. Addressed by clauses [4.1.4; 4.1.5; 4.2.1; 4.3.1; 4.3.2; 4.3.4; 4.3.6; 4.5.2; 4.7.1; 4.7.2; 7.1.7; 10.1.2].

13.23 ISO/IEC 27035-1:2023 - Clause 5.2; Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6. Addressed by clauses [4.1.4; 4.2.1; 4.3.1; 4.4.1; 4.5.1; 4.7.1; 7.1.7].

13.24 ISO/IEC 27035-2:2023 - Clause 4; Clause 6; Clause 10; Clause 11; Clause 12. Addressed by clauses [4.1.4; 4.1.6; 4.7.1; 4.7.5; 7.1.6; 7.1.7; 10.1.6].

13.25 ISO/IEC 27035-3:2020 - Clause 7; Clause 8; Clause 9; Clause 10; Clause 11; Clause 12. Addressed by clauses [4.1.3; 4.1.5; 4.2.1; 4.3.1; 4.3.2; 4.4.7; 4.5.1; 4.7.1].

13.26 ISO/IEC 27018:2020 - Annex A.10.1. Addressed by clauses [4.2.6; 4.2.7; 4.4.4; 4.4.5; 4.5.6; 7.1.3].