					Introduzca aquí la denominación de la entidad jurídica registrada							
Número de documento: PII18					Título del documento: **Política de seguimiento, auditoría y mejora del PIMS**							
Versión: 1.0		Fecha de entrada en vigor: 01.01.2025			Propietario del documento:							
X	Política		Norma		Procedimiento		Formulario		Registro		Otro	

Historial de revisiones				
Número de revisión	**Fecha de revisión**	**Cambios**	**Revisado por**	**Propietario del proceso**

Aprobaciones			
Nombre	**Cargo**	**Fecha**	**Firma**

Alineación con normas y regulaciones

Standard / Regulation	Clause / Control / Article	Applicability	Coverage Type	Comment
ISO/IEC 27701:2025	Clause 6.2	Both	Supporting	Medición de objetivos de privacidad
ISO/IEC 27701:2025	Clause 7.5	Both	Primary	Información documentada de seguimiento, auditoría y mejora
ISO/IEC 27701:2025	Clause 8.1	Both	Supporting	Seguimiento de la planificación y el control operacional
ISO/IEC 27701:2025	Clause 9.1	Both	Primary	Seguimiento, medición, análisis y evaluación
ISO/IEC 27701:2025	Clause 9.2	Both	Primary	Auditoría interna
ISO/IEC 27701:2025	Clause 9.3	Both	Primary	Revisión por la dirección
ISO/IEC 27701:2025	Clause 10.1	Both	Primary	Mejora continua
ISO/IEC 27701:2025	Clause 10.2	Both	Primary	No conformidad y acción correctiva
ISO/IEC 27701:2025	Annex A.1.2.9	Controller	Supporting	Registros de tratamiento del responsable del tratamiento utilizados para auditoría
ISO/IEC 27701:2025	Annex A.2.2.2	Processor	Supporting	Evidencias de acuerdo del encargado del tratamiento y de cooperación en auditorías
GDPR	Article 5(2)	Controller	Supporting	Evidencias de responsabilidad proactiva
GDPR	Article 24	Controller	Supporting	Medidas del responsable del tratamiento y revisión de eficacia
GDPR	Article 28	Both	Supporting	Gobernanza de auditoría y

				cooperación del encargado del tratamiento
GDPR	Article 30	Both	Supporting	Registros de tratamiento utilizados para auditoría
GDPR	Article 32	Both	Supporting	Pruebas y evaluación de medidas de seguridad
GDPR	Article 39	Conditional	Supporting	Seguimiento del DPO y asesoramiento sobre auditoría cuando corresponda
ISO/IEC 29100:2020	Clause 5.12	Both	Supporting	Cumplimiento de privacidad, auditoría y supervisión independiente
ISO/IEC 29151:2022	Clause 18.2.2; Clause 18.2.3; Clause 18.2.4	Both	Supporting	Revisión de la protección de PII y comprobaciones de cumplimiento
ISO/IEC 27001:2022	Clause 9.1	Both	Supporting	Seguimiento y evaluación de la seguridad de la información
ISO/IEC 27001:2022	Clause 9.2	Both	Supporting	Soporte a la auditoría interna del SGSI
ISO/IEC 27001:2022	Clause 9.3	Both	Supporting	Soporte a la revisión por la dirección del SGSI
ISO/IEC 27001:2022	Clause 10.1	Both	Supporting	Soporte a la mejora continua del SGSI
ISO/IEC 27001:2022	Clause 10.2	Both	Supporting	Soporte a no conformidades y acciones correctivas del SGSI
ISO/IEC 27002:2022	Control 5.35	Both	Supporting	Revisión independiente de la seguridad de la información

ISO/IEC 27002:2022	Control 5.36	Both	Supporting	Revisión del cumplimiento de políticas y normas
ISO 19011:2018	Clause 4; Clause 5; Clause 6; Clause 7	Both	Supporting	Principios, programa, realización y competencia de auditorías de sistemas de gestión

1. Alcance

1.1 Esta política define los requisitos de la organización para el seguimiento, la medición, el análisis, la evaluación, la auditoría interna, la revisión por la dirección, la gestión de no conformidades, las acciones correctivas y la mejora continua del PIMS.

1.2 Esta política se aplica a:

1.2.1 todos los procesos, controles, políticas, registros, objetos de evidencia, sistemas, proveedores, encargados del tratamiento, subencargados del tratamiento y acuerdos de intercambio de datos incluidos en el alcance del PIMS;

1.2.2 los contextos de la organización como responsable del tratamiento, corresponsable del tratamiento, encargado del tratamiento y subencargado del tratamiento;

1.2.3 el seguimiento consolidado del desempeño del PIMS, los objetivos de privacidad, el estado de implantación de controles, los hallazgos de auditoría, las no conformidades, las acciones correctivas, las acciones de revisión por la dirección y las acciones de mejora;

1.2.4 las evidencias conservadas en REG12 y las evidencias fuente de soporte conservadas en REG01 a REG11.

1.3 Esta política no sustituye los requisitos de seguimiento operativo definidos en otras políticas del PIMS. Establece el ciclo consolidado de evaluación del desempeño, auditoría, revisión y mejora del PIMS.

1.4 A efectos de esta política, una no conformidad grave del PIMS significa un fallo que afecta materialmente al alcance del PIMS, a los objetivos de privacidad, a la responsabilidad proactiva del tratamiento de PII, al tratamiento de riesgos de privacidad, a los derechos del interesado, a la seguridad del tratamiento, a la gobernanza de encargados del tratamiento o subencargados del tratamiento, a la preparación ante brechas de seguridad, a la integridad de las evidencias documentadas, al alcance de certificación o a la repetición del incumplimiento del mismo requisito dentro de un período de 12 meses.

1.5 A efectos de esta política, un cambio material significa cualquier cambio que afecte al alcance del PIMS, a las finalidades del tratamiento de PII, a las categorías de PII, a las categorías de interesados, a las ubicaciones de tratamiento, a la asignación de roles de responsable del tratamiento o encargado del tratamiento, a la arquitectura del sistema, a los acuerdos con proveedores o subencargados del tratamiento, al perfil de riesgo de privacidad, a las obligaciones legales o contractuales aplicables, al alcance de auditoría, al método de seguimiento o al alcance de certificación.

2. Finalidad

2.1 La finalidad de esta política es asegurar que la organización evalúe el desempeño del PIMS, verifique la conformidad del PIMS, identifique no conformidades, corrija debilidades de control y mejore continuamente el PIMS utilizando evidencias objetivas.

2.2 Esta política permite a la organización demostrar que las actividades de seguimiento, auditoría, revisión por la dirección y mejora del PIMS están planificadas, son independientes cuando se requiera, se basan en evidencias, son oportunas y son trazables a roles responsables y objetos de evidencia canónicos.

3. Objetivos

3.1 Los objetivos de esta política son:

3.1.1 definir un proceso consolidado de seguimiento y medición del PIMS;

3.1.2 asegurar que los objetivos de privacidad y el desempeño de los controles del PIMS se midan utilizando evidencias documentadas;

3.1.3 establecer un programa de auditoría interna del PIMS basado en riesgos;

3.1.4 preservar la independencia y la objetividad en las actividades de auditoría del PIMS;

3.1.5 asegurar que la revisión por la dirección reciba entradas completas y actuales sobre el desempeño del PIMS;

3.1.6 asegurar que las no conformidades se registren, evalúen, corrijan y verifiquen;

3.1.7 asegurar que las acciones correctivas se supervisen hasta su cierre y se revisen en cuanto a su eficacia;

3.1.8 identificar debilidades recurrentes y oportunidades de mejora;

3.1.9 respaldar la preparación para la certificación y la gestión responsable de evidencias;

3.1.10 evitar la duplicación de métricas operativas ya definidas en políticas del PIMS relacionadas.

4. Declaraciones de política

4.1 Marco de seguimiento y medición del PIMS

4.1.1 [Both] The Privacy Lead / PIMS Manager DEBE definir el programa de seguimiento consolidado del PIMS en REG12 antes de la operación inicial del PIMS y anualmente a partir de entonces.

4.1.2 [Both] The Privacy Lead / PIMS Manager DEBE definir el método de medición, la frecuencia, la fuente de evidencia, el objetivo y el rol responsable de cada métrica del PIMS en REG12 antes de que comience el ciclo de medición.

4.1.3 [Both] The Process Owner / Business Owner DEBE proporcionar al Privacy Lead / PIMS Manager entradas de seguimiento de las actividades de tratamiento de PII procedentes de REG02 trimestralmente.

4.1.4 [Both] The Information Security Lead DEBE proporcionar al Privacy Lead / PIMS Manager entradas sobre el estado de los controles de seguridad de PII procedentes de REG03 trimestralmente.

4.1.5 [Both] The Vendor / Procurement Owner DEBE proporcionar al Privacy Lead / PIMS Manager entradas sobre el estado de aseguramiento de encargados del tratamiento, subencargados del tratamiento, intercambio con terceros y proveedores procedentes de REG08 trimestralmente.

4.1.6 [All] The Incident Response Coordinator DEBE proporcionar al Privacy Lead / PIMS Manager entradas sobre tendencias de incidentes de privacidad y brechas de seguridad procedentes de REG10 mensualmente y dentro de los 10 días hábiles posteriores al cierre de un incidente grave.

4.1.7 [Both] The Privacy Lead / PIMS Manager DEBE consolidar los resultados de seguimiento del PIMS en REG12 trimestralmente.

4.2 Programa de auditoría interna del PIMS

4.2.1 [All] The Internal Audit / Compliance Reviewer DEBE preparar un programa de auditoría interna del PIMS basado en riesgos en REG12 anualmente antes del primer ciclo de auditoría del PIMS planificado.

4.2.2 [All] The Internal Audit / Compliance Reviewer DEBE definir el objetivo, los criterios, el alcance, el método, la base de muestreo y el plazo de presentación de informes de cada auditoría del PIMS en REG12 antes de que comience el trabajo de campo de auditoría.

4.2.3 [All] The Internal Audit / Compliance Reviewer DEBE registrar en REG12 las comprobaciones de independencia del auditor y de conflicto de intereses antes de cada asignación de auditoría.

4.2.4 [All] The Privacy Lead / PIMS Manager DEBE poner a disposición la información documentada controlada del PIMS y las evidencias de registros solicitadas a través de REG12 dentro de los 10 días hábiles siguientes a una solicitud de auditoría aprobada.

4.2.5 [Both] The Internal Audit / Compliance Reviewer DEBE comprobar el estado de implantación de los controles del PIMS aplicables frente a REG03 durante cada auditoría del PIMS.

4.2.6 [Both] The Internal Audit / Compliance Reviewer DEBE registrar en REG12 la muestra seleccionada de evidencias de tratamiento de PII durante cada auditoría del PIMS.

4.2.7 [All] The Internal Audit / Compliance Reviewer DEBE registrar los resultados de auditoría del PIMS en REG12 dentro de los 15 días hábiles posteriores a la finalización de la auditoría.

4.2.8 [All] The Privacy Lead / PIMS Manager DEBE asignar propietarios de acciones correctivas para los hallazgos de auditoría del PIMS aceptados en REG12 dentro de los 10 días hábiles siguientes a la aceptación de los resultados de auditoría.

[... 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 seguimiento, auditoría y mejora

9.1.1 [All] The Process Owner / Business Owner DEBE solicitar cualquier excepción a esta política en REG12 antes de que se produzca la desviación.

9.1.2 [All] The Privacy Lead / PIMS Manager DEBE evaluar el impacto en privacidad, certificación, auditoría y acciones correctivas de cada excepción solicitada en REG12 dentro de los 10 días hábiles siguientes a la solicitud.

9.1.3 [All] The Data Protection Officer / Privacy Advisor DEBE registrar asesoramiento en REG12 antes de la aprobación de cualquier excepción que afecte a obligaciones legales, derechos del interesado, compromisos de DPIA, obligaciones de auditoría de clientes o tratamientos de alto riesgo.

9.1.4 [All] Top Management DEBE aprobar en REG12 las excepciones que afecten a la finalización del calendario de auditoría, la revisión por la dirección, las no conformidades graves, el alcance de certificación o los tratamientos de alto riesgo antes de que la excepción surta efecto.

9.1.5 [All] The Privacy Lead / PIMS Manager DEBE establecer en REG12 una fecha de caducidad que no supere los 90 días para cada excepción de seguimiento, auditoría o mejora aprobada.

9.1.6 [All] The Privacy Lead / PIMS Manager DEBE cerrar o reevaluar cada excepción de seguimiento, auditoría o mejora en REG12 dentro de los cinco días hábiles posteriores a su vencimiento.

10. Aplicación

10.1 Aplicación de los requisitos de seguimiento, auditoría y mejora

10.1.1 [All] The Privacy Lead / PIMS Manager DEBE registrar un ciclo de seguimiento omitido, una auditoría del PIMS omitida, una revisión por la dirección vencida, evidencias de auditoría faltantes, una acción correctiva vencida o una acción de mejora vencida como no conformidad en REG12 dentro de los cinco días hábiles siguientes a su identificación.

10.1.2 [All] The Internal Audit / Compliance Reviewer DEBE registrar la severidad del hallazgo de auditoría en REG12 antes de la emisión del informe de auditoría.

10.1.3 [All] Top Management DEBE requerir una acción correctiva para cada no conformidad grave del PIMS en REG12 dentro de los 10 días hábiles siguientes al escalado.

10.1.4 [All] The Process Owner / Business Owner DEBE impedir la entrada en producción o la presentación de aseguramiento externo de tratamientos de alto riesgo cuando falten en REG12 las evidencias de acción correctiva requeridas antes de la entrada en producción o de la presentación.

10.1.5 [All] The Privacy Lead / PIMS Manager DEBE escalar a Top Management en REG12 los incumplimientos repetidos de plazos de seguimiento o acciones correctivas dentro de los cinco días hábiles posteriores a la segunda ocurrencia en un período de 12 meses.

10.1.6 [All] The Internal Audit / Compliance Reviewer DEBE verificar el cierre de la medida de aplicación en REG12 en la siguiente auditoría programada o dentro de los 60 días siguientes al cierre comunicado, lo que ocurra primero.

11. Revisión y mantenimiento

11.1 Revisión y mantenimiento de la política

11.1.1 [All] The Privacy Lead / PIMS Manager DEBE revisar esta política en REG12 anualmente y dentro de los 30 días posteriores a un cambio material en los requisitos de seguimiento, auditoría, revisión por la dirección, acción correctiva o certificación del PIMS.

11.1.2 [All] The Internal Audit / Compliance Reviewer DEBE revisar anualmente la eficacia del programa de auditoría del PIMS en REG12 después de la última auditoría programada del año operativo del PIMS.

11.1.3 [All] The Data Protection Officer / Privacy Advisor DEBE revisar los cambios significativos para la privacidad en esta política en REG12 antes de su aprobación.

11.1.4 [All] Top Management DEBE aprobar los cambios materiales en esta política en REG12 antes de su publicación.

11.1.5 [All] The Privacy Lead / PIMS Manager DEBE actualizar REG01 y REG03 dentro de los 15 días hábiles posteriores a los cambios aprobados en esta política que alteren el alcance del PIMS o la aplicabilidad de los controles.

11.1.6 [All] The Privacy Lead / PIMS Manager DEBE registrar la comunicación de los cambios aprobados en esta política en REG11 dentro de los 30 días posteriores a la publicación.

12. Políticas relacionadas

12.1 Esta política está respaldada por las siguientes políticas relacionadas:

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 PII05 - Política de gestión del consentimiento y las preferencias

12.1.6 PII06 - Política de gestión de derechos del interesado

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

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

12.1.9 PII09 - Política de recogida, uso, divulgación e intercambio de PII

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

12.1.11 PII11 - Política de exactitud y calidad de PII

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

12.1.13 PII13 - Política de transferencia internacional de datos personales

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

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

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

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

13. Normas y marcos de referencia

13.1 Esta política se mapea con las siguientes normas y regulaciones. El mapeo explica cómo la política respalda los requisitos citados e identifica las cláusulas internas que los implantan o respaldan.

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 6.2** - Mapeada a la definición, medición, comunicación y revisión de los objetivos del PIMS y las métricas de desempeño del PIMS. Addressed by clauses [4.1.2; 4.3.4; 8.1.1].

13.2.2 **Clause 7.5** - Mapeada al mantenimiento de información documentada para resultados de seguimiento, programas de auditoría, resultados de auditoría, evidencias de revisión por la dirección, no conformidades, acciones correctivas y acciones de mejora. Addressed by clauses [4.1.7; 4.2.4; 4.2.7; 4.3.1; 4.4.1; 7.1.8; 11.1.1].

13.2.3 **Clause 8.1** - Mapeada a la operación del ciclo planificado de seguimiento, auditoría, acción correctiva y mejora del PIMS como parte del control operacional del PIMS. Addressed by clauses [4.1.1; 4.2.1; 7.1.1; 7.1.6].

13.2.4 **Clause 9.1** - Mapeada a la definición de qué se supervisa y mide, la consolidación de resultados de seguimiento, la evaluación del desempeño del PIMS y el mantenimiento de evidencias de medición. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.1.4; 4.1.5; 4.1.6; 4.1.7; 8.1.1; 8.1.2; 8.1.4; 8.1.7].

13.2.5 **Clause 9.2** - Mapeada al mantenimiento del programa de auditoría interna, la planificación de auditoría, las comprobaciones de independencia del auditor, el muestreo de evidencias, los resultados de auditoría y el seguimiento de hallazgos de auditoría. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.2.6; 4.2.7; 8.1.3; 10.1.2].

13.2.6 **Clause 9.3** - Mapeada a la planificación de la revisión por la dirección, la revisión del desempeño del PIMS, la revisión de tendencias de auditoría y acciones correctivas, la aprobación de resultados y las decisiones sobre recursos. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 4.3.6; 6.1.7].

13.2.7 **Clause 10.1** - Mapeada a la identificación, aprobación, implantación y seguimiento de oportunidades de mejora continua para la idoneidad, adecuación y eficacia del PIMS. Addressed by clauses [4.3.7; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 4.5.6; 7.1.6].

13.2.8 **Clause 10.2** - Mapeada al registro de no conformidades, análisis de causa raíz, planificación de acciones correctivas, implantación de acciones correctivas, verificación de eficacia, escalado y aplicación. Addressed by clauses [4.2.8; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 4.4.6; 4.4.7; 4.4.8; 10.1.1; 10.1.3; 10.1.6].

13.2.9 **Annex A.1.2.9** - Mapeada a los registros de tratamiento del responsable del tratamiento utilizados como fuentes de evidencia para seguimiento, muestreo de auditoría y métricas de actualización del inventario de tratamientos. Addressed by clauses [4.1.3; 4.2.6; 8.1.7].

13.2.10 **Annex A.2.2.2** - Mapeada a las evidencias de acuerdos del encargado del tratamiento, auditorías de clientes, respuestas de aseguramiento y cooperación del encargado del tratamiento supervisadas mediante procesos de aseguramiento de proveedores y clientes. Addressed by clauses [4.1.5; 5.1.7; 7.1.5; 8.1.8].

13.3 GDPR

13.3.1 **Article 5(2)** - Mapeada a evidencias de responsabilidad proactiva para seguimiento, auditoría, revisión por la dirección, acción correctiva y mejora continua. Addressed by clauses [4.1.7; 4.2.7; 4.3.2; 4.4.2; 4.5.1].

13.3.2 **Article 24** - Mapeada a medidas de gobernanza del responsable del tratamiento, revisión de eficacia, revisión por la dirección, acción correctiva y evidencias documentadas de mejora. Addressed by clauses [4.3.4; 4.3.5; 4.3.6; 4.5.2; 10.1.3].

13.3.3 **Article 28** - Mapeada a evidencias de encargados del tratamiento, subencargados del tratamiento, auditorías de clientes, aseguramiento de terceros y cooperación de proveedores. Addressed by clauses [4.1.5; 5.1.7; 7.1.5; 8.1.8].

13.3.4 **Article 30** - Mapeada a registros de tratamiento utilizados como evidencias de seguimiento, muestreo de auditoría, integridad de objetos de evidencia y actualización del inventario de tratamientos. Addressed by clauses [4.1.3; 4.2.6; 8.1.7].

13.3.5 **Article 32** - Mapeada al seguimiento y evaluación del estado de controles de seguridad de PII, evidencias de controles técnicos y evidencias de eficacia relacionadas con seguridad. Addressed by clauses [4.1.4; 4.2.5; 5.1.4; 7.1.4; 8.1.2].

13.3.6 **Article 39** - Mapeada al asesoramiento sobre privacidad, observaciones de seguimiento, soporte de auditoría y revisión de tendencias de cumplimiento de privacidad por parte del Data Protection Officer / Privacy Advisor cuando corresponda. Addressed by clauses [5.1.3; 6.1.6; 9.1.3; 11.1.3].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 5.12** - Mapeada a la verificación del cumplimiento de privacidad, auditorías internas o independientes, controles internos, mecanismos de supervisión y evidencias de evaluación de riesgos de privacidad. Addressed by clauses [4.2.1; 4.2.3; 4.2.7; 4.5.1; 6.1.6; 8.1.7].

13.5 ISO/IEC 29151:2022

13.5.1 **Clause 18.2.2; Clause 18.2.3; Clause 18.2.4** - Mapeada a la revisión independiente de la seguridad de la información relacionada con PII, el cumplimiento de políticas y normas, y la revisión de cumplimiento técnico para la protección de PII. Addressed by clauses [4.2.3; 4.2.5; 7.1.4; 8.1.2; 10.1.6].

13.6 ISO/IEC 27001:2022

13.6.1 **Clause 9.1** - Mapeada a entradas de seguimiento y evaluación de la seguridad de la información que respaldan la medición del desempeño del PIMS y el estado de controles de seguridad de PII. Addressed by clauses [4.1.4; 8.1.2].

13.6.2 **Clause 9.2** - Mapeada al soporte de auditoría interna del SGSI para la planificación de auditorías del PIMS, evidencias de auditoría, resultados de auditoría y finalización del programa de auditoría. Addressed by clauses [4.2.1; 4.2.2; 4.2.7; 8.1.3].

13.6.3 **Clause 9.3** - Mapeada a entradas y salidas de revisión por la dirección para la supervisión integrada del desempeño del PIMS y de la seguridad de la información. Addressed by clauses [4.3.1; 4.3.2; 4.3.5; 4.3.6].

13.6.4 **Clause 10.1** - Mapeada a la mejora continua del PIMS y del entorno de controles de seguridad de la información de soporte. Addressed by clauses [4.5.1; 4.5.2; 4.5.6].

13.6.5 **Clause 10.2** - Mapeada a la gestión de no conformidades, planificación de acciones correctivas, implantación de acciones correctivas y verificación de eficacia. Addressed by clauses [4.4.2; 4.4.4; 4.4.6; 4.4.7; 10.1.1].

13.7 ISO/IEC 27002:2022

13.7.1 Control 5.35 - Mapeada a la revisión independiente, comprobaciones de independencia del auditor, pruebas de evidencias de auditoría y verificación independiente de la eficacia de acciones correctivas. Addressed by clauses [4.2.3; 4.2.5; 4.4.7; 10.1.6].

13.7.2 Control 5.36 - Mapeada a la revisión del cumplimiento de políticas del PIMS y de seguridad de la información, el estado de implantación de controles y evidencias de conformidad con normas. Addressed by clauses [4.1.4; 4.2.5; 4.5.3; 8.1.2].

13.8 ISO 19011:2018

13.8.1 **Clause 4; Clause 5; Clause 6; Clause 7** - Mapeada a principios de auditoría, gestión del programa de auditoría, realización de auditorías, informes de auditoría basados en evidencias, seguimiento de auditoría y expectativas de competencia de auditores para auditorías del PIMS. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.6; 4.2.7; 4.4.7; 5.1.9; 11.1.2].