					Introduzca aquí la denominación de la entidad jurídica registrada							
Número de documento: PII01					Título del documento: **Política del Sistema de Gestión de la Privacidad de la Información**							
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	Both	Primary	Contexto y determinación del rol en el PIMS
ISO/IEC 27701:2025	Clause 4.2	Both	Primary	Partes interesadas y requisitos
ISO/IEC 27701:2025	Clause 4.3	Both	Primary	Alcance del PIMS
ISO/IEC 27701:2025	Clause 4.4	Both	Primary	Establecimiento y mejora del PIMS
ISO/IEC 27701:2025	Clause 5.1	Both	Primary	Liderazgo y compromiso
ISO/IEC 27701:2025	Clause 5.2	Both	Primary	Política de privacidad
ISO/IEC 27701:2025	Clause 5.3	Both	Primary	Roles y autoridades
ISO/IEC 27701:2025	Clause 6.1.1	Both	Primary	Riesgos y oportunidades
ISO/IEC 27701:2025	Clause 6.1.2	Both	Primary	Evaluación de riesgos de privacidad
ISO/IEC 27701:2025	Clause 6.1.3	Both	Primary	Tratamiento de riesgos de privacidad y SoA
ISO/IEC 27701:2025	Clause 6.2	Both	Primary	Objetivos de privacidad
ISO/IEC 27701:2025	Clause 6.3	Both	Primary	Cambios planificados del PIMS
ISO/IEC 27701:2025	Clause 7.1	Both	Primary	Recursos
ISO/IEC 27701:2025	Clause 7.2	Both	Primary	Competencia
ISO/IEC 27701:2025	Clause 7.3	Both	Primary	Concienciación
ISO/IEC 27701:2025	Clause 7.4	Both	Primary	Comunicaciones
ISO/IEC 27701:2025	Clause 7.5	Both	Primary	Información documentada
ISO/IEC 27701:2025	Clause 8.1	Both	Primary	Planificación y control operacional

ISO/IEC 27701:2025	Clause 8.2	Both	Primary	Evaluación operacional de riesgos de privacidad
ISO/IEC 27701:2025	Clause 8.3	Both	Primary	Tratamiento operacional de riesgos de privacidad
ISO/IEC 27701:2025	Clause 9.1	Both	Primary	Seguimiento 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.1.2.2; Annex A.1.2.3; Annex A.1.2.6; Annex A.1.2.8; Annex A.1.2.9	Controller	Primary	Registros de gobierno del responsable del tratamiento
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.3	Processor	Primary	Acuerdo del encargado del tratamiento y finalidades
ISO/IEC 27701:2025	Annex A.3.3	Both	Primary	Vinculación con la política de seguridad de PII
GDPR	Article 5(2)	Controller	Supporting	Evidencias de responsabilidad proactiva
GDPR	Article 24	Controller	Supporting	Medidas y política del responsable del tratamiento
GDPR	Article 26	Joint Controller	Supporting	Acuerdos de corresponsables del tratamiento
GDPR	Article 28	Both	Supporting	Gobierno del encargado del tratamiento
GDPR	Article 30	Both	Supporting	Registros de tratamiento

GDPR	Article 32	Both	Supporting	Seguridad del tratamiento
GDPR	Article 35	Controller	Supporting	Gobierno de DPIA
ISO/IEC 29100:2020	Clause 4.7; Clause 5.1; Clause 5.11; Clause 5.12	Both	Supporting	Controles y principios de privacidad
ISO/IEC 29134:2020	Clause 1; Clause 5.1; Clause 6.2; Clause 6.3	Both	Supporting	Proceso y preparación de PIA
ISO/IEC 29151:2022	Clause 4.1; Clause 4.2; Annex A.2	Controller	Supporting	Programa y política de protección de PII
ISO/IEC 27557:2022	Clause 4; Clause 5.2; Clause 5.3; Clause 5.4.1	Both	Supporting	Integración organizativa de riesgos de privacidad

1. Alcance

1.1 Esta política establece el Sistema de Gestión de la Privacidad de la Información de la organización para el tratamiento de PII en contextos de responsable del tratamiento, corresponsable del tratamiento, encargado del tratamiento y subencargado.

1.2 Esta política se aplica a:

1.2.1 el alcance del PIMS, el contexto, las partes interesadas y los límites organizativos;

1.2.2 la determinación del rol en el PIMS para las actividades de tratamiento de PII;

1.2.3 la política de privacidad, los objetivos de privacidad, la evaluación de riesgos de privacidad, el tratamiento de riesgos de privacidad y la Declaración de Aplicabilidad del PIMS;

1.2.4 el gobierno, el seguimiento, la auditoría interna, la revisión por la dirección, la no conformidad, la acción correctiva y la mejora continua del PIMS;

1.2.5 la información documentada y las evidencias necesarias para demostrar la conformidad del PIMS y la responsabilidad proactiva.

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

2. Finalidad

2.1 Esta política define los requisitos obligatorios de gobierno para establecer, implementar, mantener, hacer seguimiento y mejorar continuamente el PIMS.

2.2 La finalidad de esta política es garantizar que la organización pueda demostrar una gestión del tratamiento de PII responsable, basada en riesgos y sustentada en evidencias en todos los roles PIMS aplicables.

3. Objetivos

3.1 Los objetivos de esta política son:

3.1.1 definir el alcance, el contexto, los límites y la aplicabilidad de roles del PIMS;

3.1.2 asignar la responsabilidad proactiva de gobierno del PIMS mediante roles PIMS canónicos;

3.1.3 establecer objetivos de privacidad y expectativas medibles de desempeño del PIMS;

3.1.4 mantener una Declaración de Aplicabilidad del PIMS para los controles seleccionados y excluidos;

3.1.5 integrar la evaluación de riesgos de privacidad, el tratamiento de riesgos de privacidad y el gobierno de DPIA en la operación del PIMS;

3.1.6 garantizar que las obligaciones de responsable del tratamiento, corresponsable del tratamiento, encargado del tratamiento y subencargado se identifiquen antes de que comience el tratamiento;

3.1.7 mantener evidencias preparadas para auditorías a efectos de preparación para la certificación y mejora continua;

3.1.8 evitar roles, registros, formularios y controles operativos duplicados que no sean necesarios.

4. Declaraciones de la política

4.1 Establecimiento, contexto y alcance del PIMS

4.1.1 [Both] Top Management DEBE aprobar el alcance del PIMS en REG01 antes de la implementación inicial del PIMS y dentro de los 30 días siguientes a cualquier cambio material.

4.1.2 [Both] Privacy Lead / PIMS Manager DEBE documentar las cuestiones externas e internas del contexto de privacidad en REG01 anualmente y dentro de los 30 días siguientes a cualquier cambio material.

4.1.3 [Both] Privacy Lead / PIMS Manager DEBE documentar las partes interesadas pertinentes y sus requisitos del PIMS en REG01 anualmente y dentro de los 30 días siguientes a cualquier cambio material.

4.1.4 [Both] Privacy Lead / PIMS Manager DEBE mantener el resumen de interacción de procesos del PIMS en REG01 antes de cada revisión por la dirección.

4.2 Determinación del rol en el PIMS

4.2.1 [Both] Process Owner / Business Owner DEBE clasificar el rol PIMS de la organización para cada actividad de tratamiento de PII en REG02 antes de que comience la actividad de tratamiento.

4.2.2 [Joint Controller] Vendor / Procurement Owner DEBE documentar la asignación de responsabilidades de corresponsables del tratamiento en REG08 antes de que comience el tratamiento conjunto.

4.2.3 [Processor] Vendor / Procurement Owner DEBE documentar las instrucciones de tratamiento del cliente para las actividades del encargado del tratamiento en REG08 antes de la incorporación del servicio.

4.2.4 [Subprocessor] Vendor / Procurement Owner DEBE documentar las instrucciones del cliente principal y los acuerdos de subtratamiento aprobados en REG08 antes de que comience el subtratamiento.

[... 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 Solicitud y aprobación de excepciones

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

9.1.2 [Both] Privacy Lead / PIMS Manager DEBE evaluar el riesgo de privacidad de cada excepción solicitada en REG04 antes de su aprobación.

9.1.3 [Both] Top Management DEBE aprobar en REG12 las excepciones que superen los umbrales de riesgo de privacidad aceptados antes de su implementación.

9.1.4 [Both] Privacy Lead / PIMS Manager DEBE revisar trimestralmente las excepciones activas del PIMS en REG12 hasta su cierre.

9.2 Cierre de excepciones

9.2.1 [All] Process Owner / Business Owner DEBE documentar las evidencias de cierre de excepciones en REG12 antes de la fecha de caducidad aprobada de la excepción.

9.2.2 [Both] Internal Audit / Compliance Reviewer DEBE verificar las evidencias de cierre de excepciones caducadas en REG12 durante la siguiente auditoría interna planificada.

10. Aplicación

10.1 Gestión de no conformidades

10.1.1 [All] Privacy Lead / PIMS Manager DEBE registrar las sospechas de no conformidad con esta política en REG12 dentro de los cinco días hábiles siguientes a su identificación.

10.1.2 [All] Process Owner / Business Owner DEBE implementar las acciones correctivas aprobadas en REG12 antes de la fecha límite asignada tras la aprobación de la no conformidad.

10.1.3 [All] Top Management DEBE revisar en REG12 las no conformidades mayores del PIMS no resueltas en cada revisión por la dirección.

10.1.4 [All] Internal Audit / Compliance Reviewer DEBE verificar la eficacia de las acciones correctivas en REG12 dentro de los 30 días siguientes al cierre notificado.

10.2 Escalado

10.2.1 [All] Privacy Lead / PIMS Manager DEBE escalar a Top Management las acciones correctivas mayores vencidas en REG12 dentro de los cinco días hábiles siguientes a la fecha límite.

10.2.2 [All] Top Management DEBE registrar las decisiones sobre acciones correctivas mayores vencidas en REG12 dentro de los 15 días hábiles siguientes al escalado.

11. Revisión y mantenimiento

11.1 Revisión de la política

11.1.1 [All] Privacy Lead / PIMS Manager DEBE revisar esta política en REG12 anualmente y dentro de los 30 días siguientes a cualquier cambio material legal, organizativo, de tratamiento, tecnológico o del alcance de certificación.

11.1.2 [All] Data Protection Officer / Privacy Advisor DEBE proporcionar asesoramiento documentado en REG12 antes de la aprobación de la política cuando cambien obligaciones materiales de privacidad.

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

11.1.4 [All] Privacy Lead / PIMS Manager DEBE actualizar REG01 y REG03 dentro de los 15 días hábiles siguientes a los cambios aprobados de la política que modifiquen el alcance del PIMS o la aplicabilidad de controles.

11.1.5 [All] Privacy Lead / PIMS Manager DEBE registrar la comunicación de los cambios aprobados de la política en REG11 dentro de los 30 días siguientes a su publicación.

12. Políticas relacionadas

12.1 Esta política está respaldada por las siguientes políticas relacionadas:

12.2 PII02 - Política de roles, responsabilidades y responsabilidad proactiva en materia de privacidad

12.3 PII03 - Política de inventario de tratamiento de PII y base jurídica

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

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

12.6 PII12 - Política de encargados del tratamiento, subencargados e intercambio de datos

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

12.8 PII15 - Política de gestión de incidentes y brechas de PII

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

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

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

13. Normas y marcos de referencia

13.1 Esta política está mapeada con las siguientes normas y regulaciones. El mapeo explica cómo la política apoya los requisitos citados e identifica las cláusulas internas que los implementan o respaldan.

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 4.1** - Mapeada con la determinación del contexto organizativo, las cuestiones del contexto de privacidad y la aplicabilidad del rol de responsable o encargado del tratamiento para las actividades del PIMS. Addressed by clauses [4.1.2; 4.2.1; 6.1.3].

13.2.2 **Clause 4.2** - Mapeada con la identificación de partes interesadas, interesados, clientes, autoridades de control, encargados del tratamiento, subencargados y sus requisitos pertinentes del PIMS. Addressed by clauses [4.1.3; 7.2.1; 11.1.1].

13.2.3 **Clause 4.3** - Mapeada con la definición, aprobación, mantenimiento y cambio del alcance documentado del PIMS. Addressed by clauses [4.1.1; 6.1.3; 11.1.4].

13.2.4 **Clause 4.4** - Mapeada con el establecimiento, la implementación, el mantenimiento y la mejora de los procesos del PIMS y sus interacciones. Addressed by clauses [4.1.4; 7.1.1; 7.2.1].

13.2.5 **Clause 5.1** - Mapeada con la aprobación de Top Management, los recursos, la revisión de gobierno y el liderazgo sobre la eficacia y la mejora del PIMS. Addressed by clauses [4.3.1; 5.1.1; 6.1.1; 8.1.4; 10.1.3].

13.2.6 **Clause 5.2** - Mapeada con el mantenimiento de esta política de privacidad como información documentada aprobada y la comunicación de cambios de la política. Addressed by clauses [4.3.1; 11.1.1; 11.1.3; 11.1.5].

13.2.7 **Clause 5.3** - Mapeada con la asignación y comunicación de roles, responsabilidades y autoridades del PIMS. Addressed by clauses [5.1.1; 5.1.2; 5.1.3; 5.1.4; 5.1.5; 5.1.6; 5.1.7; 5.1.8; 5.1.9].

13.2.8 **Clause 6.1.1** - Mapeada con la planificación de acciones para riesgos y oportunidades del PIMS utilizando el contexto, los requisitos de las partes interesadas, los objetivos y las entradas de mejora. Addressed by clauses [4.1.2; 4.1.3; 4.4.1; 6.1.1; 8.1.1].

13.2.9 **Clause 6.1.2** - Mapeada con la exigencia de evaluación de riesgos de privacidad antes de tratamientos nuevos o modificados materialmente y el mantenimiento de evidencias de riesgos de privacidad. Addressed by clauses [4.4.1; 5.1.3; 8.2.4; 9.1.2].

13.2.10 **Clause 6.1.3** - Mapeada con el tratamiento de riesgos de privacidad, la selección de controles, la vinculación con el programa de seguridad de la información y el mantenimiento de la Declaración de Aplicabilidad. Addressed by clauses [4.3.3; 4.3.4; 4.4.3; 7.1.3; 7.1.4; 8.2.2].

13.2.11 **Clause 6.2** - Mapeada con el establecimiento, la medición, el seguimiento, la comunicación y la actualización de los objetivos del PIMS. Addressed by clauses [4.3.1; 4.3.2; 8.1.2; 8.1.4].

13.2.12 **Clause 6.3** - Mapeada con los cambios planificados del PIMS y el control de los cambios que afectan al alcance, los roles, los controles y la información documentada. Addressed by clauses [4.1.1; 6.1.3; 7.1.1; 11.1.4].

13.2.13 **Clause 7.1** - Mapeada con la determinación y provisión de recursos para el establecimiento, la operación, el mantenimiento y la mejora del PIMS. Addressed by clauses [5.1.1; 6.1.1; 7.1.1].

13.2.14 **Clause 7.2** - Mapeada con las expectativas de competencia y las evidencias que respaldan las responsabilidades del PIMS y el desempeño de roles. Addressed by clauses [5.1.3; 5.1.8; 11.1.5].

13.2.15 **Clause 7.3** - Mapeada con la concienciación sobre la política de privacidad, la contribución a la eficacia del PIMS y las implicaciones de la no conformidad. Addressed by clauses [11.1.5; 10.1.1; 10.2.1].

13.2.16 **Clause 7.4** - Mapeada con las comunicaciones internas y externas pertinentes para el gobierno del PIMS, los cambios de la política y el escalado. Addressed by clauses [6.2.1; 10.2.1; 11.1.5].

13.2.17 **Clause 7.5** - Mapeada con la creación, el mantenimiento, el control, la preparación de evidencias y la conservación de información documentada. Addressed by clauses [4.5.1; 4.5.3; 7.1.6; 11.1.4].

13.2.18 **Clause 8.1** - Mapeada con la planificación, implementación y control de los procesos operativos del PIMS y de los procesos proporcionados externamente. Addressed by clauses [4.4.4; 7.1.3; 7.1.5; 7.2.1].

13.2.19 **Clause 8.2** - Mapeada con la realización de evaluaciones de riesgos de privacidad a intervalos planificados y cuando se propongan o se produzcan cambios significativos. Addressed by clauses [4.4.1; 8.2.4; 9.1.2].

13.2.20 **Clause 8.3** - Mapeada con la implementación de planes de tratamiento de riesgos de privacidad y la conservación de evidencias de los resultados del tratamiento. Addressed by clauses [4.4.3; 7.1.3; 8.2.2].

13.2.21 **Clause 9.1** - Mapeada con el seguimiento, la medición, el análisis, la evaluación, las métricas y los informes de eficacia del PIMS. Addressed by clauses [8.1.1; 8.1.2; 8.1.4; 8.2.1; 8.2.2; 8.2.3; 8.2.4].

13.2.22 **Clause 9.2** - Mapeada con la planificación de auditorías internas, el muestreo de evidencias, los resultados de auditoría y la revisión independiente. Addressed by clauses [5.1.9; 6.2.1; 8.1.3; 9.2.2].

13.2.23 **Clause 9.3** - Mapeada con las entradas de la revisión por la dirección, la revisión del desempeño, los resultados de la revisión por la dirección y las decisiones de mejora. Addressed by clauses [6.1.1; 6.1.2; 8.1.4; 10.1.3].

13.2.24 **Clause 10.1** - Mapeada con la mejora continua mediante revisión por la dirección, métricas, seguimiento de acciones correctivas y mantenimiento de la política. Addressed by clauses [6.1.1; 6.2.2; 10.1.4; 11.1.1].

13.2.25 **Clause 10.2** - Mapeada con la gestión de no conformidades, la acción correctiva, el escalado, el cierre y la verificación de eficacia. Addressed by clauses [4.5.2; 6.2.2; 6.2.3; 10.1.1; 10.1.2; 10.1.4; 10.2.1; 10.2.2].

13.2.26 **Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.6; Annex A.1.2.8; Annex A.1.2.9** - Mapeada con los registros de finalidades de tratamiento del lado del responsable del tratamiento, la vinculación con la base jurídica, la determinación de la necesidad de DPIA, la asignación de responsabilidades de corresponsables del tratamiento y los registros de evidencias de tratamiento. Addressed by clauses [4.2.1; 4.2.2; 4.4.2; 4.5.1; 7.1.2; 8.2.1].

13.2.27 **Annex A.2.2.2; Annex A.2.2.3** - Mapeada con los acuerdos de clientes para encargados del tratamiento, las instrucciones documentadas del cliente y las limitaciones de finalidad del encargado del tratamiento. Addressed by clauses [4.2.3; 4.2.4; 5.1.7; 7.1.5].

13.2.28 **Annex A.3.3** - Mapeada con la vinculación con la política de seguridad de PII, la propiedad de la configuración de referencia de controles de seguridad de PII y el estado de controles de seguridad de la información en la Declaración de Aplicabilidad del PIMS. Addressed by clauses [4.3.4; 5.1.4; 7.1.4].

13.3 GDPR

13.3.1 **Article 5(2)** - Mapeada con las evidencias de responsabilidad proactiva, la aprobación de la política, la clasificación del rol de tratamiento, la aplicabilidad de controles, el seguimiento, la auditoría y los registros de acciones correctivas. Addressed by clauses [4.3.1; 4.5.1; 4.5.2; 6.1.1; 8.1.3].

13.3.2 **Article 24** - Mapeada con las medidas de gobierno del responsable del tratamiento, la aprobación de la política, los objetivos del PIMS, la revisión de eficacia y las evidencias documentadas de responsabilidad proactiva del responsable del tratamiento. Addressed by clauses [4.3.1; 4.3.2; 6.1.1; 8.1.4; 11.1.1].

13.3.3 **Article 26** - Mapeada con la determinación y documentación de la asignación de responsabilidades de corresponsables del tratamiento antes de que comience el tratamiento conjunto. Addressed by clauses [4.2.2; 5.1.7; 7.1.5].

13.3.4 **Article 28** - Mapeada con los registros de gobierno de encargados del tratamiento y subencargados, las instrucciones de tratamiento del cliente y el control de procesos proporcionados externamente. Addressed by clauses [4.2.3; 4.2.4; 5.1.7; 7.1.5].

13.3.5 **Article 30** - Mapeada con los registros de actividades de tratamiento, la clasificación de roles, los registros de responsabilidad proactiva de tratamiento y las evidencias conservadas para la auditabilidad. Addressed by clauses [4.2.1; 5.1.5; 7.1.2; 8.2.1].

13.3.6 **Article 32** - Mapeada con el gobierno de la configuración de referencia de seguridad de PII, la propiedad de controles de seguridad, el estado de implementación de seguridad y la confirmación de controles operativos. Addressed by clauses [4.3.4; 4.4.4; 5.1.4; 7.1.4].

13.3.7 **Article 35** - Mapeada con la determinación de necesidad de DPIA y la evaluación de riesgos de privacidad antes de que prosiga un tratamiento como responsable del tratamiento de alto riesgo o modificado materialmente. Addressed by clauses [4.4.1; 4.4.2; 5.1.3; 8.2.4].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 4.7; Clause 5.1; Clause 5.11; Clause 5.12** - Mapeada con la identificación de controles de privacidad, los principios de privacidad, la seguridad de la información, el cumplimiento de privacidad, la auditoría, las evidencias y el gobierno de privacidad basado en riesgos. Addressed by clauses [4.3.3; 4.3.4; 4.4.1; 4.5.1; 8.1.3; 10.1.4].

13.5 ISO/IEC 29134:2020

13.5.1 **Clause 1; Clause 5.1; Clause 6.2; Clause 6.3** - Mapeada con el gobierno de PIA, la determinación de desencadenantes de DPIA, la preparación de PIA, los criterios de riesgos de privacidad y las evidencias documentadas de evaluación de riesgos de privacidad. Addressed by clauses [4.4.1; 4.4.2; 5.1.3; 8.2.4; 9.1.2].

13.6 ISO/IEC 29151:2022

13.6.1 **Clause 4.1; Clause 4.2; Annex A.2** - Mapeada con los requisitos del programa de protección de PII, la identificación de requisitos de protección de PII, la selección de controles basada en riesgos de privacidad y la orientación de la política de protección de PII. Addressed by clauses [4.3.3; 4.3.4; 4.4.3; 7.1.4].

13.7 ISO/IEC 27557:2022

13.7.1 **Clause 4; Clause 5.2; Clause 5.3; Clause 5.4.1** - Mapeada con los principios organizativos de riesgos de privacidad, el compromiso del liderazgo, la integración del riesgo de privacidad en el gobierno del PIMS y la comprensión del rol de la organización en el tratamiento de PII. Addressed by clauses [4.1.2; 4.2.1; 4.4.1; 4.4.3; 6.1.1].