					Introduzca aquí la denominación de la entidad jurídica registrada							
Número de documento: PII24					Título del documento: **Política de privacidad de CCTV y monitorización física**							
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 reglamentos

Norma / Reglamento	Cláusula / Control / Artículo	Aplicabilidad	Tipo de cobertura	Comentario
ISO/IEC 27701:2025	Clause 7.5; Clause 8.1	Both	Primary	Controles documentados y operativos
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Seguimiento y acción correctiva
ISO/IEC 27701:2025	Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.6; Annex A.1.2.9	Controller	Primary	Finalidad, base jurídica, activador de riesgo y registros
ISO/IEC 27701:2025	Annex A.1.2.7; Annex A.1.2.8	Controller	Supporting	Asignación de encargado del tratamiento y corresponsable del tratamiento
ISO/IEC 27701:2025	Annex A.1.3.2; Annex A.1.3.6; Annex A.1.3.7; Annex A.1.3.10	Controller	Supporting	Obligaciones y solicitudes de los interesados
ISO/IEC 27701:2025	Annex A.1.4.2; Annex A.1.4.3; Annex A.1.4.5; Annex A.1.4.8; Annex A.1.4.9	Controller	Primary	Recogida, tratamiento, minimización, conservación y eliminación
ISO/IEC 27701:2025	Annex A.1.5.4; Annex A.1.5.5	Controller	Primary	Registros y solicitudes de divulgación
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.6; Annex A.2.2.7	Processor	Supporting	Acuerdos de encargado del tratamiento, instrucciones, soporte y registros
ISO/IEC 27701:2025	Annex A.2.3.2; Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6	Processor	Supporting	Derechos del encargado del tratamiento y soporte para divulgaciones
ISO/IEC 27701:2025	Annex A.3.14; Annex A.3.25	Both	Supporting	Protección de registros y registro de eventos
GDPR	Article 5(1)(a); Article 5(1)(b); Article 5(1)(c); Article 5(1)(e); Article 5(2)	Controller	Primary	Principios y responsabilidad proactiva

GDPR	Article 6	Controller	Primary	Base jurídica
GDPR	Article 12; Article 13; Article 14	Controller	Primary	Transparencia y avisos
GDPR	Article 15; Article 16; Article 17; Article 18; Article 21	Controller	Supporting	Solicitudes de derechos
GDPR	Article 24; Article 26; Article 28; Article 30; Article 32; Article 35; Article 39	Both	Supporting	Gobernanza, encargados del tratamiento, registros, seguridad, EIPD y asesoramiento
ISO/IEC 29100:2020	Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6	Controller	Supporting	Finalidad, recogida, minimización, conservación y divulgación
ISO/IEC 29100:2020	Clause 5.8; Clause 5.9; Clause 5.10; Clause 5.11; Clause 5.12	Both	Supporting	Transparencia, participación, responsabilidad proactiva, seguridad y cumplimiento
ISO/IEC 29134:2020	Clause 5.1; Clause 6.2	Controller	Supporting	Riesgo de privacidad y activadores de EIPD
ISO/IEC 29151:2022	Annex A.3; Annex A.4; Annex A.5; Annex A.7; Annex A.10	Both	Supporting	Controles de privacidad para la protección de PII
ISO/IEC 29151:2022	Clause 9.2.3; Clause 9.4.2; Clause 11.1.3	Both	Supporting	Controles de acceso y entrada física
ISO/IEC 27002:2022	Controls 5.34; 7.2; 7.4; 8.2; 8.3; 8.15	Both	Supporting	PII, monitorización física, restricción de acceso y registro de eventos

1. Alcance

1.1 Esta política se aplica a CCTV, videovigilancia, monitorización de visitantes, registros de control de acceso físico, registros de monitorización operados por personal de seguridad, sistemas de monitorización de instalaciones y actividades de monitorización física relacionadas que recojan o traten de otro modo PII.

1.2 Esta política se aplica a las organizaciones que actúan como responsables del tratamiento de PII para sus propias instalaciones y actividades de monitorización física. También se aplica a las actividades de soporte como encargado del tratamiento o subencargado del tratamiento cuando la organización opera, aloja, revisa, almacena, divulga, suprime o trata de otro modo grabaciones de videovigilancia, datos de visitantes o registros de acceso físico por cuenta de un cliente.

1.3 Esta política cubre la definición de la finalidad de la monitorización, la aprobación, los avisos y la señalización, las restricciones de acceso, la divulgación, la conservación, la supresión, la externalización, el escalado de incidentes, el enrutamiento de solicitudes de derechos, la revisión y la gestión de evidencias.

1.4 Esta política no proporciona asesoramiento en materia de derecho laboral, comentarios jurídicos sobre comités de empresa, procedimientos de las fuerzas y cuerpos de seguridad ni un registro específico de CCTV. Las evidencias específicas de monitorización se mantienen en los objetos de evidencia canónicos del PIMS identificados en esta política.

2. Finalidad

2.1 La finalidad de esta política es establecer controles de privacidad para CCTV y la monitorización física, de modo que las actividades de monitorización tengan una finalidad definida, sean transparentes, proporcionadas, sujetas a control de acceso, conservadas durante periodos definidos, divulgadas únicamente a través de canales aprobados y respaldadas por evidencias auditables del PIMS.

2.2 Esta política respalda el tratamiento coherente de grabaciones de videovigilancia, registros de visitantes, registros de acceso físico y PII de monitorización relacionada sin crear registros, comités, paneles ni roles no canónicos adicionales.

3. Objetivos

3.1 Los objetivos de esta política son:

3.1.1 definir las finalidades de monitorización y el alcance del tratamiento antes de que comience la monitorización;

3.1.2 documentar en REG02 las actividades de CCTV, acceso físico, monitorización de visitantes y monitorización física;

3.1.3 identificar en REG04 las actividades de monitorización que requieren una revisión de riesgos de privacidad o una evaluación preliminar de EIPD;

3.1.4 mantener evidencias de avisos y señalización transparentes en REG07;

3.1.5 restringir el acceso, la visualización, la exportación, la divulgación y la conservación de PII de monitorización;

3.1.6 enrutar las solicitudes de los interesados a través de REG06;

3.1.7 gestionar en REG08 las evidencias de proveedores de monitorización externalizados y de intercambio de datos;

3.1.8 escalar a través de REG10 los incidentes de PII sospechados relacionados con la monitorización;

3.1.9 registrar en REG12 revisiones, excepciones, no conformidades, acciones correctivas, hallazgos de auditoría y mejoras.

4. Declaraciones de la política

4.1 Inventario, finalidad y aprobación de la monitorización

4.1.1 [Controller] The Process Owner / Business Owner DEBE registrar en REG02 cada actividad de CCTV, monitorización de visitantes, registro de control de acceso físico o monitorización física antes de que comience la actividad.

4.1.2 [Controller] The Privacy Lead / PIMS Manager DEBE validar la entrada de REG02 respecto de la finalidad, la base jurídica, la ubicación monitorizada, las categorías de PII, las categorías de interesados, la conservación, el aviso, el acceso y los campos de divulgación antes de la activación de una actividad de monitorización nueva o modificada sustancialmente.

4.1.3 [Controller] The Process Owner / Business Owner DEBE registrar en REG02 las zonas monitorizadas aprobadas, las zonas excluidas y los límites de recogida antes de habilitar cámaras, sensores, registros de visitantes o registros de control de acceso.

4.1.4 [Conditional] The Process Owner / Business Owner DEBE obtener una decisión de riesgos de privacidad en REG04 antes de activar una monitorización que implique monitorización sistemática, grabación de audio, identificación biométrica, detección habilitada mediante analítica, ubicaciones sensibles, personas vulnerables o monitorización no evidente.

4.1.5 [Joint Controller] The Privacy Lead / PIMS Manager DEBE registrar en REG08 la asignación de responsabilidades de monitorización conjunta antes de que comience la monitorización compartida con un arrendador, socio de instalaciones, cliente u otro corresponsable del tratamiento.

4.1.6 [Processor] The Privacy Lead / PIMS Manager DEBE registrar en REG08 las instrucciones del cliente sobre monitorización y los límites del tratamiento permitido antes de tratar grabaciones de videovigilancia, registros de visitantes o registros de acceso físico por cuenta de un cliente.

4.2 Aviso y transparencia

4.2.1 [Controller] The Process Owner / Business Owner DEBE asegurar que la señalización de videovigilancia o las evidencias equivalentes de aviso justo a tiempo se registren en REG07 antes de que las áreas monitorizadas se abran a los interesados.

4.2.2 [Controller] The Privacy Lead / PIMS Manager DEBE vincular cada aviso de monitorización en REG07 con la finalidad del tratamiento correspondiente en REG02 antes de su publicación o cambio sustancial.

4.2.3 [Processor] The Privacy Lead / PIMS Manager DEBE proporcionar en REG08 información de soporte para avisos de monitorización cuando la organización opere servicios de monitorización bajo instrucciones del cliente.

4.2.4 [Conditional] The Process Owner / Business Owner DEBE registrar en REG07 y REG04 medidas alternativas de transparencia antes de activar monitorización no evidente o de emergencia.

[... 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 [All] The Privacy Lead / PIMS Manager DEBE registrar en REG12 cada excepción a esta política antes de que se utilice la excepción.

9.2 [Conditional] The Data Protection Officer / Privacy Advisor DEBE documentar el asesoramiento en privacidad en REG04 o REG12 antes de la aprobación de excepciones que impliquen monitorización no evidente, grabación de audio, identificación biométrica, monitorización habilitada mediante analítica o ubicaciones de monitorización sensibles.

9.3 [All] Top Management DEBE aprobar en REG12 las excepciones que superen 90 días antes de su ampliación más allá del periodo inicial de excepción.

9.4 [All] The Privacy Lead / PIMS Manager DEBE revisar en REG12 las excepciones de monitorización abiertas al menos mensualmente hasta su cierre.

10. Aplicación

10.1 [All] The Privacy Lead / PIMS Manager DEBE registrar como no conformidades en REG12 los fallos de controles de monitorización dentro de los cinco días hábiles desde su confirmación.

10.2 [Both] The Information Security Lead DEBE suspender el acceso no autorizado al sistema de monitorización dentro de un día hábil desde su confirmación y registrar la acción en REG10 o REG12.

10.3 [All] Top Management DEBE asignar en REG12 la propiedad de las acciones correctivas dentro de 10 días hábiles para incumplimientos de la política repetidos o sustanciales.

10.4 [Conditional] The Incident Response Coordinator DEBE iniciar el flujo de trabajo de incidentes de PII en REG10 ante la sospecha de divulgación, pérdida o compromiso no autorizados de PII de monitorización.

11. Revisión y mantenimiento

11.1 [All] The Privacy Lead / PIMS Manager DEBE revisar esta política y las evidencias de monitorización relacionadas en REG12 al menos anualmente.

11.2 [Controller] The Process Owner / Business Owner DEBE revalidar cada finalidad de monitorización activa, aviso, alcance de ubicación y entrada de conservación en REG02 y REG07 al menos anualmente.

11.3 [Both] The System Owner / Application Owner DEBE revalidar en REG12 los controles de acceso, registro de eventos, supresión y exportación del sistema de monitorización al menos anualmente y después de un cambio sustancial del sistema.

11.4 [Conditional] The Vendor / Procurement Owner DEBE revalidar las evidencias de proveedores de monitorización externalizados en REG08 al menos anualmente y antes de la renovación contractual.

11.5 [All] The Privacy Lead / PIMS Manager DEBE actualizar las evidencias relacionadas de REG02, REG04, REG07, REG08, REG10 o REG12 dentro de los 30 días naturales posteriores a los cambios aprobados de la política.

12. Políticas relacionadas

12.1 PII02 - Política de roles, responsabilidades y responsabilidad proactiva de privacidad

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

12.3 PII04 - Política de avisos de privacidad y transparencia

12.4 PII06 - Política de gestión de derechos de los interesados

12.5 PII07 - Política de evaluación de riesgos de privacidad y EIPD

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

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

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

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

12.10 PII13 - Política de transferencia internacional de datos personales

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

12.12 PII15 - Política de incidentes y brechas de PII

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

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

12.15 PII19 - Política de privacidad de empleados

12.16 PII21 - Política de privacidad de IA y toma de decisiones automatizada

12.17 PII23 - Política de encargado del tratamiento de PII en la nube

13. Normas y marcos de referencia

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

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 7.5; Clause 8.1** - Mapeadas a evidencias documentadas de monitorización, planificación operacional, controles de activación, registros de finalidad, vinculación de avisos, configuración de acceso, configuración de conservación y control de cambios para actividades de CCTV y monitorización física. Addressed by clauses [4.1.1; 4.1.2; 4.2.2; 4.3.1; 4.4.1; 6.2; 7.1; 11.5].

13.2.2 **Clause 9.1; Clause 10.2** - Mapeadas a medición de controles de monitorización, revisión de proveedores, revisión de accesos, hallazgos de auditoría, no conformidades, acciones correctivas, escalado de acciones vencidas y evidencias de mejora. Addressed by clauses [4.6.4; 6.4; 6.5; 6.6; 8.1; 8.7; 10.1; 11.1].

13.2.3 **Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.6; Annex A.1.2.9** - Mapeadas a la definición por el responsable del tratamiento de la finalidad de monitorización, la documentación de la base jurídica, las decisiones sobre activadores de riesgos de privacidad y los registros de actividades de tratamiento de monitorización en REG02 y REG04. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.4.1; 6.2; 7.1; 11.2].

13.2.4 **Annex A.1.2.7; Annex A.1.2.8** - Mapeadas a la asignación de proveedores de monitorización externalizados, la asignación de responsabilidades de monitorización conjunta y las evidencias de encargado del tratamiento o corresponsable del tratamiento en REG08. Addressed by clauses [4.1.5; 4.6.1; 4.6.2; 5.7; 6.2; 7.6].

13.2.5 **Annex A.1.3.2; Annex A.1.3.6; Annex A.1.3.7; Annex A.1.3.10** - Mapeadas a obligaciones de interesados relacionadas con la monitorización, enrutamiento de solicitudes, preservación necesaria para evaluar solicitudes y evidencias de gobernanza para el soporte de derechos. Addressed by clauses [4.5.1; 4.5.2; 5.2; 7.2; 11.5].

13.2.6 **Annex A.1.4.2; Annex A.1.4.3; Annex A.1.4.5; Annex A.1.4.8; Annex A.1.4.9** - Mapeadas a limitación de la recogida de monitorización, límites del tratamiento, minimización, periodos de conservación, supresión, sobrescritura, retenciones de conservación y control de copias extraídas. Addressed by clauses [4.1.3; 4.3.1; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 7.3; 7.5; 8.4].

13.2.7 **Annex A.1.5.4; Annex A.1.5.5** - Mapeadas a registros de divulgación externa, gestión de solicitudes de divulgación, minimización antes de la divulgación y divulgaciones vinculadas a incidentes que impliquen PII de monitorización. Addressed by clauses [4.3.4; 4.5.4; 7.8; 10.4].

13.2.8 **Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.6; Annex A.2.2.7** - Mapeadas a instrucciones del cliente para encargados del tratamiento, límites del tratamiento permitido, soporte de avisos, instrucciones de conservación y supresión, asistencia en derechos y registros del encargado del tratamiento para servicios de monitorización externalizados. Addressed by clauses [4.1.6; 4.2.3; 4.4.5; 4.5.3; 4.6.3].

13.2.9 **Annex A.2.3.2; Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6** - Mapeadas al soporte del encargado del tratamiento para las obligaciones del cliente, autorización de divulgación, registros de divulgación, notificación de solicitudes de divulgación y gestión de divulgaciones

legalmente vinculantes para PII de monitorización. Addressed by clauses [4.3.5; 4.5.3; 4.6.2; 4.6.3].

13.2.10 **Annex A.3.14; Annex A.3.25** - Mapeadas a protección de registros de monitorización, acceso restringido, revisión de acceso privilegiado, registro de accesos, contención de accesos no autorizados y evidencias de registro de eventos para sistemas de monitorización. Addressed by clauses [4.3.2; 4.3.3; 4.5.5; 5.4; 7.4; 10.2; 11.3].

13.3 GDPR

13.3.1 **Article 5(1)(a); Article 5(1)(b); Article 5(1)(c); Article 5(1)(e); Article 5(2)** - Mapeados a licitud, lealtad, transparencia, limitación de la finalidad, minimización de datos, limitación del plazo de conservación y evidencias de responsabilidad proactiva para actividades de monitorización. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.2.1; 4.4.1; 4.4.2; 4.4.3; 6.1; 8.1; 11.2].

13.3.2 Article 6 - Mapeado a documentación de la base jurídica para CCTV, monitorización de visitantes, registros de acceso físico y otras actividades de monitorización física. Addressed by clauses [4.1.2; 4.1.4; 7.1].

13.3.3 **Article 12; Article 13; Article 14** - Mapeados a avisos de monitorización transparentes, evidencias de señalización, vinculación de avisos con finalidades del tratamiento, información de soporte para avisos por parte del encargado del tratamiento y medidas alternativas de transparencia. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 7.2; 8.2; 11.2].

13.3.4 **Article 15; Article 16; Article 17; Article 18; Article 21** - Mapeados a acceso, rectificación, supresión, limitación, oposición, enrutamiento de solicitudes, preservación necesaria para evaluar solicitudes y asistencia al cliente relacionada con la monitorización. Addressed by clauses [4.5.1; 4.5.2; 4.5.3; 7.8; 11.5].

13.3.5 **Article 24; Article 26; Article 28; Article 30; Article 32; Article 35; Article 39** - Mapeados a gobernanza del responsable del tratamiento, asignación entre corresponsables del tratamiento, gobernanza de encargados del tratamiento, registros de tratamiento, seguridad de sistemas de monitorización, revisión de riesgos de privacidad, activadores de EIPD y asesoramiento en privacidad. Addressed by clauses [4.1.4; 4.1.5; 4.1.6; 4.3.2; 4.3.3; 4.5.4; 4.6.1; 4.6.2; 4.6.4; 5.1; 5.3; 6.3; 8.5; 10.4].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6** - Mapeadas a especificación de la finalidad, limitación de la recogida, minimización de datos, limitación del uso, limitación de la conservación y limitación de la divulgación para PII de monitorización. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.3.4; 4.4.1; 4.4.2; 4.4.4; 7.8].

13.4.2 **Clause 5.8; Clause 5.9; Clause 5.10; Clause 5.11; Clause 5.12** - Mapeadas a transparencia, participación individual, responsabilidad proactiva, seguridad de la información, revisión de cumplimiento, revisión de accesos, enrutamiento de derechos, escalado de incidentes y evidencias de acciones correctivas. Addressed by clauses [4.2.1; 4.2.2; 4.3.2; 4.3.3; 4.5.1; 4.5.4; 6.1; 8.7; 10.1].

13.5 ISO/IEC 29134:2020

13.5.1 **Clause 5.1; Clause 6.2** - Mapeadas a riesgos de privacidad y evaluación preliminar de activadores de EIPD para monitorización física sistemática, no evidente, de audio, biométrica, habilitada mediante analítica, en ubicaciones sensibles, de personas vulnerables u otra monitorización física de mayor riesgo. Addressed by clauses [4.1.4; 4.2.4; 5.3; 6.3; 7.5; 9.2].

13.6 ISO/IEC 29151:2022

13.6.1 **Annex A.3; Annex A.4; Annex A.5; Annex A.7; Annex A.10** - Mapeadas a controles de protección de PII para finalidad, recogida, minimización, conservación, divulgación y

participación de los interesados en contextos de monitorización. Addressed by clauses [4.1.1; 4.1.3; 4.2.1; 4.4.1; 4.4.3; 4.5.1; 7.2; 8.2].

13.6.2 **Clause 9.2.3; Clause 9.4.2; Clause 11.1.3** - Mapeadas a aprovisionamiento de accesos, restricción de acceso a la información y controles de entrada física relevantes para el acceso a sistemas de monitorización y registros de control de acceso físico. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.5.5; 5.4; 7.4; 10.2; 11.3].

13.7 ISO/IEC 27002:2022

13.7.1 Controls 5.34; 7.2; 7.4; 8.2; 8.3; 8.15 - Mapeados a privacidad y protección de PII, entrada física, monitorización de seguridad física, acceso privilegiado, restricción de acceso a la información y controles de registro de eventos para CCTV y sistemas de monitorización física. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.5.5; 5.4; 7.3; 7.4; 8.3; 10.2; 11.3].