

				Introduzca aquí la denominación de la entidad jurídica registrada							
Número de documento: PII19				Título del documento: Política de Privacidad de Empleados							
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

Aviso legal (derechos de autor y restricciones de uso)
(C) 2025 Clarysec LLC. All rights reserved.

Este documento es propiedad intelectual de Clarysec LLC. Ninguna parte de este documento podrá copiarse, reutilizarse, distribuirse ni modificarse con fines comerciales o de implantación sin autorización previa y expresa por escrito.

El uso no autorizado está estrictamente prohibido y puede dar lugar a acciones legales.

Para cuestiones de licenciamiento, contacte con: info@clarysec.com

Alineación con normas y reglamentos

Norma / Reglamento	Cláusula / Control / Artículo	Applicability	Coverage Type	Comentario
ISO/IEC 27701:2025	Clause 7.5; Clause 8.1	Both	Primary	Evidencias de privacidad de empleados y control operacional
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Seguimiento, 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	Finalidades de RR. HH., vinculación con la base jurídica, activación de EIPD, responsabilidad conjunta y registros
ISO/IEC 27701:2025	Annex A.1.2.7; Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.6; Annex A.2.2.7	Both	Supporting	Contratos de encargados del tratamiento de RR. HH., instrucciones, asistencia y registros
ISO/IEC 27701:2025	Annex A.1.3.2; Annex A.1.3.6; Annex A.1.3.7; Annex A.1.3.10; Annex A.1.3.11	Controller	Supporting	Obligaciones, derechos y encaminamiento de decisiones automatizadas relativos a empleados
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 y vinculación con el calendario de conservación
ISO/IEC 27701:2025	Annex A.1.5.4; Annex A.1.5.5; Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6	Both	Supporting	Registros de divulgación y gestión de divulgaciones jurídicamente vinculantes
ISO/IEC 27701:2025	Annex A.3.14; Annex A.3.25	Both	Supporting	Protección de registros de RR. HH. y evidencias de 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 de privacidad de empleados y responsabilidad proactiva
GDPR	Article 6; Article 9; Article 10	Controller	Supporting	Licitud, categorías especiales de datos y datos de comprobación de antecedentes
GDPR	Article 12; Article 13; Article 14	Controller	Primary	Transparencia y avisos para empleados
GDPR	Article 15; Article 16; Article 17; Article 18; Article 21; Article 22	Controller	Supporting	Derechos de empleados y encaminamiento de decisiones automatizadas
GDPR	Article 24; Article 26; Article 28; Article 30; Article 32; Article 35; Article 39	Both	Supporting	Gobernanza, corresponsables del tratamiento, 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, uso, 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 29151:2022	Annex A.3; Annex A.4; Annex A.5; Annex A.7; Annex A.10	Controller	Supporting	Finalidad de PII, recogida, minimización, conservación y participación del interesado
ISO/IEC 29151:2022	Clause 7.1.2; Clause 7.1.3; Clause 7.2.4; Clause 7.3.2	Controller	Supporting	Controles del ciclo de vida laboral protectores de PII

ISO/IEC 29151:2022	Clause 15.1.2; Clause 15.2.2; Clause 15.2.3	Both	Supporting	Evaluación, seguimiento y control de cambios de encargados del tratamiento de RR. HH.
ISO/IEC 29134:2020	Clause 5.1; Clause 6.2	Controller	Supporting	Riesgo de privacidad de RR. HH. y vinculación con activación de EIPD
ISO/IEC 27002:2022	Controls 5.34; 6.1; 6.2; 6.5; 6.6	Both	Supporting	Protección de PII y ciclo de vida de seguridad de la información de la plantilla
ISO/IEC 27002:2022	Controls 8.15; 8.16	Both	Supporting	Actividades de registro de eventos y seguimiento

1. Alcance

- 1.1 Esta política define los requisitos de privacidad de empleados para la recogida, uso, divulgación, vinculación con el calendario de conservación, aviso, gestión de derechos, monitorización, soporte de encargados del tratamiento y gestión de evidencias de datos personales de los empleados dentro del Sistema de Gestión de la Privacidad de la Información.
- 1.2 A efectos de esta política, “datos personales de los empleados” incluye la PII relativa a empleados, candidatos a empleo, exempleados, contratistas, personal temporal, becarios, personal en comisión de servicio y otros miembros de la plantilla cuando la organización trate su PII con fines de plantilla, contratación, empleo, relación profesional, remuneración, prestaciones, seguridad, cumplimiento, administración del lugar de trabajo u otros fines de negocio relacionados.
- 1.3 Esta política se aplica a contextos de responsable del tratamiento y corresponsable del tratamiento en los que la organización determina los fines y medios del tratamiento de datos personales de los empleados.
- 1.4 Esta política también se aplica a contextos de encargado del tratamiento y subencargado del tratamiento en los que la organización trata datos personales de los empleados en nombre de un cliente, encargado ascendente u otro responsable del tratamiento conforme a instrucciones documentadas.

1.5 Esta política cubre:

- 1.5.1 recogida de datos de empleados;
 - 1.5.2 finalidades del tratamiento de RR. HH.;
 - 1.5.3 avisos de privacidad de empleados;
 - 1.5.4 gestión de derechos de empleados;
 - 1.5.5 vinculación con el calendario de conservación;
 - 1.5.6 monitorización de empleados;
 - 1.5.7 divulgación interna;
 - 1.5.8 controles de encargados del tratamiento de RR. HH., nóminas, sistema de información de recursos humanos, prestaciones, comprobación de antecedentes y servicios de RR. HH. externalizados, cuando proceda;
 - 1.5.9 incidentes de datos personales de los empleados, no conformidades, acciones correctivas y evidencias de mejora.
- 1.6 Esta política no crea un registro de privacidad de RR. HH., registro de privacidad de empleados, registro de tratamiento de RR. HH., registro de monitorización de empleados, registro de comprobación de antecedentes, registro de proveedores de RR. HH., registro de derechos de empleados ni registro de incidentes de empleados separados. Las evidencias del tratamiento de empleados se registran en REG02, REG04, REG06, REG07, REG08, REG10 y REG12.
 - 1.7 Esta política no proporciona asesoramiento en derecho laboral, asesoramiento en relaciones laborales, comentarios jurídicos sobre comités de empresa, contenido de procedimientos disciplinarios, contenido de procedimientos operativos de nómina ni plantillas documentales laborales específicas de una jurisdicción.

1.8 Esta política no duplica:

- 1.8.1 la gobernanza del PIMS en PII01;
- 1.8.2 la responsabilidad de roles en PII02;
- 1.8.3 la titularidad del inventario de tratamientos y de la base jurídica en PII03;
- 1.8.4 la gobernanza del contenido de avisos de privacidad en PII04;
- 1.8.5 la operación de consentimiento y preferencias en PII05;

- 1.8.6 el flujo de trabajo de derechos del interesado en PII06;
- 1.8.7 la metodología de riesgos de privacidad y EIPD en PII07;
- 1.8.8 las puertas de control de privacidad desde el diseño en PII08;
- 1.8.9 las reglas base de recogida, uso, divulgación e intercambio en PII09;
- 1.8.10 la ejecución de conservación, supresión y eliminación en PII10;
- 1.8.11 la gobernanza de exactitud y calidad en PII11;
- 1.8.12 la gobernanza del ciclo de vida de encargados, subencargados y terceros en PII12;
- 1.8.13 los controles de mecanismos de transferencia internacional en PII13;
- 1.8.14 la implementación de seguridad y control de acceso en PII14;
- 1.8.15 la gestión de incidentes y brechas de seguridad en PII15;
- 1.8.16 la gestión de formación y concienciación en PII16;
- 1.8.17 el control de información documentada en PII17;
- 1.8.18 la gobernanza de seguimiento, auditoría y mejora del PIMS en PII18;
- 1.8.19 los controles de IA y toma de decisiones automatizada en PII21, cuando se incluya esa política opcional.

2. Propósito

- 2.1 El propósito de esta política es asegurar que los datos personales de los empleados se traten únicamente para finalidades de plantilla documentadas, aprobadas, transparentes, proporcionadas y sujetas a responsabilidad proactiva, y que las evidencias de privacidad de empleados se mantengan en los registros canónicos del PIMS sin crear una capa separada de evidencias de privacidad de RR. HH.
- 2.2 Esta política respalda una gestión coherente del tratamiento de empleados mediante la vinculación de las actividades de tratamiento de empleados con REG02, los avisos de privacidad de empleados con REG07, las solicitudes de derechos de empleados con REG06, los riesgos de privacidad de RR. HH. y los criterios de activación de EIPD con REG04, los encargados del tratamiento de RR. HH. y los proveedores de nómina o sistema de información de recursos humanos con REG08, los incidentes de datos personales de los empleados con REG10, y las excepciones, no conformidades, acciones correctivas y evidencias de seguimiento con REG12.

3. Objetivos

3.1 Los objetivos de esta política son:

- 3.1.1 mantener evidencias del inventario de tratamientos de empleados en REG02;
- 3.1.2 documentar las fuentes de recogida de datos de empleados, categorías de PII, finalidades, sistemas, destinatarios y vinculación con el calendario de conservación;
- 3.1.3 mantener evidencias de avisos de privacidad de empleados en REG07;
- 3.1.4 encaminar los riesgos de privacidad de empleados y los criterios de activación de EIPD a través de REG04;
- 3.1.5 encaminar las solicitudes de derechos de empleados a través de REG06;
- 3.1.6 mantener evidencias de encargados del tratamiento de RR. HH., nóminas, sistema de información de recursos humanos, prestaciones, comprobación de antecedentes y servicios de RR. HH. externalizados en REG08;
- 3.1.7 asegurar que la monitorización de empleados esté documentada, sea proporcionada, sea revisada y se escale a través de REG04 y REG12 cuando proceda;
- 3.1.8 encaminar los incidentes sospechosos de datos personales de los empleados a través de REG10;

- 3.1.9 registrar las excepciones, no conformidades, acciones correctivas y acciones de mejora de privacidad de empleados en REG12;
- 3.1.10 evitar el asesoramiento en derecho laboral y los comentarios jurídicos sobre comités de empresa dentro de las cláusulas operativas;
- 3.1.11 evitar registros, roles, formularios, paneles u objetos de evidencia duplicados específicos de RR. HH.

4. Declaraciones de política

4.1 Inventario de tratamientos de empleados y finalidades del tratamiento de RR. HH.

- 4.1.1 [Controller] The Process Owner / Business Owner MUST registrar cada actividad de tratamiento de empleados en REG02 antes de que los datos personales de los empleados sean recogidos, generados, importados, utilizados o divulgados.
- 4.1.2 [Controller] The Process Owner / Business Owner MUST documentar las categorías de datos personales de los empleados, la población de empleados, la fuente de recogida, la finalidad del tratamiento, el sistema, la categoría de destinatario interno, la categoría de destinatario externo y la vinculación con el calendario de conservación en REG02 antes de aprobar la actividad de tratamiento.
- 4.1.3 [Controller] The Privacy Lead / PIMS Manager MUST revisar cada actividad de tratamiento de empleados nueva o modificada materialmente en REG02 antes de que la actividad de tratamiento sea aprobada para operar.
- 4.1.4 [Conditional] The Data Protection Officer / Privacy Advisor MUST registrar el asesoramiento de privacidad en REG04 antes de la aprobación del tratamiento de empleados que implique PII de categorías especiales, datos de infracciones penales, comprobación de antecedentes, datos de salud laboral, datos biométricos, datos de ubicación, monitorización de empleados o tratamiento que pueda afectar materialmente a un empleado.
- 4.1.5 [Processor] The Privacy Lead / PIMS Manager MUST registrar la instrucción del cliente, la finalidad del servicio, las categorías de datos personales de los empleados del cliente y la vinculación del rol de encargado del tratamiento en REG08 antes de tratar datos personales de los empleados del cliente como servicio externalizado de RR. HH., nómina, prestaciones, sistema de información de recursos humanos, comprobación o soporte de plantilla.
- 4.1.6 [Joint Controller] The Privacy Lead / PIMS Manager MUST registrar la asignación de responsabilidades de corresponsables del tratamiento para el tratamiento de datos personales de los empleados en REG08 antes de que comience la actividad conjunta de tratamiento de empleados.

4.2 Recogida de datos de empleados y avisos de privacidad de empleados

- 4.2.1 [Controller] The Process Owner / Business Owner MUST limitar la recogida de datos personales de los empleados a las categorías documentadas en REG02 antes de que comience la recogida para contratación, alta, administración del empleo, administración de prestaciones, operación de nómina, comprobación, monitorización o baja.
- 4.2.2 [Controller] The Process Owner / Business Owner MUST registrar en REG02 la fuente de los datos personales de los empleados recogidos de terceros antes de utilizar la fuente de recogida de terceros.
- 4.2.3 [Controller] The Privacy Lead / PIMS Manager MUST mantener un registro de aviso de privacidad de empleados en REG07 antes de que los datos personales de los empleados se recojan directa o indirectamente para una finalidad nueva o modificada materialmente.
- 4.2.4 [Controller] The Process Owner / Business Owner MUST confirmar que el aviso de privacidad de empleados vigente registrado en REG07 está disponible antes de la recogida

para contratación, recogida durante el alta, activación de la monitorización, inscripción en prestaciones, comprobación de antecedentes o un cambio material del tratamiento de empleados.

4.2.5 [Conditional] The Data Protection Officer / Privacy Advisor MUST revisar el registro de aviso de privacidad de empleados de REG07 antes de su publicación cuando el aviso cubra monitorización de empleados, comprobación de antecedentes, PII de categorías especiales, datos de infracciones penales, toma de decisiones automatizada o una finalidad de tratamiento de empleados modificada materialmente.

4.2.6 [Processor] The Vendor / Procurement Owner MUST registrar las responsabilidades de canales de recogida dirigidos a empleados en REG08 antes de que un servicio de RR. HH., nómina, sistema de información de recursos humanos, prestaciones, comprobación o RR. HH. externalizado operado por un encargado del tratamiento recoja datos personales de los empleados en nombre de un cliente.

[... 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] The Process Owner / Business Owner MUST registrar una solicitud de excepción en REG12 antes de desviarse de cualquier requisito de esta política.

9.1.2 [Conditional] The Data Protection Officer / Privacy Advisor MUST registrar asesoramiento en REG12 antes de la aprobación de una excepción que afecte a monitorización de empleados, gestión de derechos de empleados, comprobación de antecedentes, PII de categorías especiales, datos de infracciones penales o tratamiento de empleados de alto impacto.

9.1.3 [Conditional] Top Management MUST aprobar las excepciones de privacidad de empleados en REG12 antes de su activación cuando la excepción afecte a tratamiento de empleados de alto riesgo, monitorización de empleados, divulgación externa, dependencia de un encargado del tratamiento o acción correctiva no resuelta.

9.1.4 [All] The Privacy Lead / PIMS Manager MUST asignar una fecha de caducidad no superior a 90 días a cada excepción de privacidad de empleados en REG12 antes de que se active la excepción.

9.1.5 [All] The Privacy Lead / PIMS Manager MUST revisar cada excepción de privacidad de empleados en REG12 dentro de cinco días hábiles antes de su caducidad.

9.1.6 [All] The Privacy Lead / PIMS Manager MUST cerrar o escalar cada excepción de privacidad de empleados caducada en REG12 dentro de cinco días hábiles después de su caducidad.

10. Aplicación

10.1.1 [All] The Privacy Lead / PIMS Manager MUST registrar una no conformidad en REG12 dentro de cinco días hábiles cuando el tratamiento de datos personales de los empleados carezca de las evidencias requeridas en REG02, REG07, REG08, REG04 o REG06.

10.1.2 [Conditional] The Incident Response Coordinator MUST registrar la sospecha de acceso, divulgación, pérdida o compromiso no autorizados de datos personales de los empleados en REG10 dentro de un día hábil desde su identificación.

10.1.3 [Controller] The Privacy Lead / PIMS Manager MUST impedir la aprobación de nueva monitorización de empleados en REG12 cuando falten las evidencias requeridas en REG02, REG04 o REG07.

- 10.1.4 [Both] The Vendor / Procurement Owner MUST suspender la nueva divulgación de datos personales de los empleados a un proveedor de RR. HH. en REG08 cuando falten las evidencias requeridas de encargado del tratamiento, subencargado del tratamiento, instrucción o asistencia.
- 10.1.5 [All] Top Management MUST revisar las no conformidades repetidas de privacidad de empleados en REG12 cuando la misma categoría se produzca dos o más veces dentro de un período móvil de 12 meses.
- 10.1.6 [All] The Internal Audit / Compliance Reviewer MUST verificar las evidencias de cierre en REG12 antes de cerrar hallazgos de auditoría que impliquen tratamiento de privacidad de empleados, avisos de empleados, monitorización de empleados, derechos de empleados o proveedores de RR. HH.

11. Revisión y mantenimiento

- 11.1.1 [All] The Privacy Lead / PIMS Manager MUST revisar esta política en REG12 al menos anualmente.
- 11.1.2 [Conditional] The Privacy Lead / PIMS Manager MUST revisar esta política en REG12 dentro de 30 días desde un cambio material en el tratamiento de empleados, monitorización de empleados, sistemas de RR. HH., acuerdos de nómina, proveedores de sistema de información de recursos humanos, proveedores de prestaciones, proveedores de comprobación de antecedentes o servicios de RR. HH. externalizados.
- 11.1.3 [Conditional] The Data Protection Officer / Privacy Advisor MUST revisar los cambios materiales propuestos a esta política en REG12 antes de la aprobación por Top Management.
- 11.1.4 [All] Top Management MUST aprobar los cambios materiales de esta política en REG12 antes de su publicación.
- 11.1.5 [All] The Privacy Lead / PIMS Manager MUST actualizar REG02, REG07 o REG08 dentro de 15 días hábiles después de que un cambio aprobado de la política afecte a los registros de tratamiento de empleados, avisos de privacidad de empleados o evidencias de proveedores de RR. HH.
- 11.1.6 [All] The Internal Audit / Compliance Reviewer MUST registrar observaciones sobre la eficacia de la revisión de esta política en REG12 durante el ciclo programado de auditoría interna del PIMS.

12. Políticas relacionadas

- 12.1 Esta política está respaldada por las siguientes políticas relacionadas:
- 12.2 PII01 - Política del Sistema de Gestión de la Privacidad de la Información
- 12.3 PII02 - Política de Roles, Responsabilidades y Rendición de Cuentas de Privacidad
- 12.4 PII03 - Política de Inventario de Tratamientos de PII y Base Jurídica
- 12.5 PII04 - Política de Avisos de Privacidad y Transparencia
- 12.6 PII05 - Política de Gestión de Consentimiento y Preferencias
- 12.7 PII06 - Política de Gestión de Derechos del Interesado
- 12.8 PII07 - Política de Evaluación de Riesgos de Privacidad y EIPD
- 12.9 PII08 - Política de Privacidad desde el Diseño y por Defecto
- 12.10 PII09 - Política de Recogida, Uso, Divulgación e Intercambio de PII
- 12.11 PII10 - Política de Conservación, Supresión y Eliminación de PII
- 12.12 PII11 - Política de Exactitud y Calidad de PII
- 12.13 PII12 - Política de Gestión de Privacidad de Encargados, Subencargados y Terceros
- 12.14 PII13 - Política de Transferencia Internacional de PII

- 12.15 PII14 - Política de Seguridad y Control de Acceso de PII
- 12.16 PII15 - Política de Gestión de Incidentes y Brechas de Seguridad de PII
- 12.17 PII16 - Política de Formación, Concienciación y Competencia en Privacidad
- 12.18 PII17 - Política de Información Documentada y Gestión de Evidencias del PIMS
- 12.19 PII18 - Política de Supervisión, Auditoría y Mejora del PIMS
- 12.20 PII21 - Política de Privacidad de IA y Toma de Decisiones Automatizada, cuando se incluya en el alcance de la versión opcional complementaria

13. Normas y marcos de referencia

- 13.1 Esta política está mapeada con 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** - Mapeado con evidencias documentadas de privacidad de empleados, puertas de aprobación operacional, registros de encargados del tratamiento de RR. HH., avisos de empleados, registros de monitorización, gestión de excepciones y evidencias de implementación. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.2.3; 4.3.1; 4.4.1; 4.5.1; 4.7.1; 7.1.1; 7.1.3].
- 13.2.2 **Clause 9.1; Clause 10.2** - Mapeado con seguimiento de privacidad de empleados, métricas, evidencias de auditoría, muestreo de monitorización de empleados, gestión de no conformidades, acciones correctivas y mejora. Addressed by clauses [4.3.6; 4.4.5; 4.5.5; 4.6.7; 8.1.1; 8.1.4; 8.1.7; 10.1.1; 10.1.5].
- 13.2.3 **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** - Mapeado con finalidades de tratamiento de empleados, vinculación con la base jurídica, encaminamiento de riesgos de privacidad y EIPD, asignación de corresponsables del tratamiento y registros de tratamiento en REG02 y REG04. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.1.4; 4.1.6; 4.2.2; 4.6.1; 4.6.2].
- 13.2.4 **Annex A.1.2.7; Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.6; Annex A.2.2.7** - Mapeado con contratos de encargados del tratamiento de RR. HH., instrucciones documentadas, tratamiento de datos personales de los empleados del cliente, asistencia del encargado del tratamiento y registros del encargado del tratamiento en REG08. Addressed by clauses [4.1.5; 4.2.6; 4.4.4; 4.5.4; 4.7.1; 4.7.2; 4.7.3; 4.7.4; 4.7.5].
- 13.2.5 **Annex A.1.3.2; Annex A.1.3.6; Annex A.1.3.7; Annex A.1.3.10; Annex A.1.3.11** - Mapeado con gestión de derechos de empleados, asesoramiento en derechos complejos y encaminamiento de decisiones automatizadas o tratamiento de alto impacto a través de REG06 y REG04. Addressed by clauses [4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 4.6.3].
- 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** - Mapeado con limitación de recogida de empleados, uso interno aprobado, minimización, vinculación con el calendario de conservación y encaminamiento de excepciones de conservación. Addressed by clauses [4.2.1; 4.3.1; 4.3.2; 4.3.3; 4.4.1; 4.4.2; 4.4.3; 4.4.5; 4.6.1].
- 13.2.7 **Annex A.1.5.4; Annex A.1.5.5; Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6** - Mapeado con divulgaciones externas de datos personales de los empleados, registros de intercambio de datos, autorización de divulgación por el encargado del tratamiento y encaminamiento de incidentes relacionados con divulgación. Addressed by clauses [4.3.4; 4.3.5; 4.3.6; 4.7.6].
- 13.2.8 **Annex A.3.14; Annex A.3.25** - Mapeado con protección de registros de privacidad de empleados, evidencias de registros de monitorización de empleados y sospecha de uso

indebido o compromiso de datos de monitorización de empleados. Addressed by clauses [4.6.4; 4.6.6; 4.6.7; 7.1.2].

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)** - Mapeado con tratamiento de datos personales de los empleados lícito, leal, transparente, limitado a la finalidad, minimizado, vinculado con el calendario de conservación y sujeto a responsabilidad proactiva. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.2.3; 4.3.1; 4.3.3; 4.4.1; 4.4.5].

13.3.2 **Article 6; Article 9; Article 10** - Mapeado con vinculación con la base jurídica, encaminamiento de datos personales de los empleados de categorías especiales, encaminamiento de PII sensible de salud laboral y relacionada con el empleo, y encaminamiento de datos de infracciones penales o comprobación de antecedentes. Addressed by clauses [4.1.2; 4.1.3; 4.1.4; 4.2.2; 4.7.3].

13.3.3 **Article 12; Article 13; Article 14** - Mapeado con transparencia para empleados, registros de avisos de privacidad de empleados, activadores de aviso para recogida directa e indirecta, y evidencias de aviso de monitorización. Addressed by clauses [4.2.3; 4.2.4; 4.2.5; 4.6.5].

13.3.4 **Article 15; Article 16; Article 17; Article 18; Article 21; Article 22** - Mapeado con encaminamiento de derechos de empleados, evidencias de solicitudes, asesoramiento en solicitudes complejas y encaminamiento de decisiones automatizadas. Addressed by clauses [4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 4.6.3].

13.3.5 **Article 24; Article 26; Article 28; Article 30; Article 32; Article 35; Article 39** - Mapeado con gobernanza del responsable del tratamiento, asignación de corresponsables del tratamiento, gobernanza de encargados del tratamiento de RR. HH., registros de tratamiento, gestión segura, encaminamiento de EIPD e intervención de asesoramiento en privacidad. Addressed by clauses [4.1.3; 4.1.4; 4.1.5; 4.1.6; 4.3.4; 4.3.5; 4.6.2; 4.6.3; 4.6.6; 4.7.1; 4.7.6].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6** - Mapeado con especificación de finalidades de empleados, limitación de recogida, minimización, limitación de uso, limitación de conservación y limitación de divulgación. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.3.1; 4.3.2; 4.3.3; 4.4.1; 4.4.2; 4.6.1].

13.4.2 **Clause 5.8; Clause 5.9; Clause 5.10; Clause 5.11; Clause 5.12** - Mapeado con transparencia, participación de empleados, soporte de derechos de empleados, responsabilidad proactiva, seguridad de la información y evidencias de cumplimiento de privacidad. Addressed by clauses [4.2.3; 4.2.4; 4.5.1; 4.5.2; 4.5.5; 4.6.4; 4.6.6; 4.6.7; 4.7.6].

13.5 ISO/IEC 29151:2022

13.5.1 **Annex A.3; Annex A.4; Annex A.5; Annex A.7; Annex A.10** - Mapeado con registros de finalidad de PII, controles de recogida, minimización, vinculación con el calendario de conservación, limitación de divulgación y soporte de participación o acceso de empleados. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.3.1; 4.3.4; 4.4.1; 4.4.2; 4.5.1; 4.5.4].

13.5.2 **Clause 7.1.2; Clause 7.1.3; Clause 7.2.4; Clause 7.3.2** - Mapeado con controles del ciclo de vida laboral protectores de PII relevantes para comprobación, términos, vinculación con aplicación de brechas de privacidad y revisión de conservación por terminación o cambio de empleo. Addressed by clauses [4.1.4; 4.2.2; 4.4.2; 4.4.5; 10.1.1; 10.1.5].

13.5.3 **Clause 15.1.2; Clause 15.2.2; Clause 15.2.3** - Mapeado con evaluación de encargados del tratamiento de RR. HH., seguimiento de encargados del tratamiento de RR. HH., revisión de proveedores de RR. HH. y evidencias de cambio de servicio en REG08. Addressed by clauses [4.4.4; 4.7.1; 4.7.2; 4.7.3; 4.7.4; 4.7.5; 4.7.6].

13.6 ISO/IEC 29134:2020

13.6.1 **Clause 5.1; Clause 6.2** - Mapeado con beneficios de la evaluación de impacto relativa a la privacidad y determinación de riesgos de privacidad de RR. HH. o criterios de activación de EIPD para monitorización de empleados y tratamiento de datos de RR. HH. de alto impacto sin duplicar el método de EIPD. Addressed by clauses [4.1.4; 4.3.3; 4.6.2; 4.6.3].

13.7 ISO/IEC 27002:2022

13.7.1 Controls 5.34; 6.1; 6.2; 6.5; 6.6 - Mapeado con protección de PII, comprobación, términos de la plantilla, responsabilidades tras cambios en el empleo y expectativas de confidencialidad como controles del ciclo de vida laboral que respaldan PII. Addressed by clauses [4.1.4; 4.2.2; 4.4.2; 4.4.4; 4.7.2; 4.7.3].

13.7.2 Controls 8.15; 8.16 - Mapeado con registros de monitorización de empleados, actividades de monitorización, limitación de finalidad de registros y revisión de evidencias de monitorización. Addressed by clauses [4.6.1; 4.6.2; 4.6.4; 4.6.6; 4.6.7].