GUIA

ISO 27701:2025

Sistemas de gestión de privacidad de la información — Requisitos.

La norma ISO/IEC 27701:2025 es la segunda edición del estándar internacional para los Sistemas de Gestión de Información de Privacidad (PIMS), publicada formalmente en octubre de 2025.

Su mayor cambio estratégico es que ahora es una norma independiente (*standalone*), lo que significa que las organizaciones pueden implementarla y certificarse en ella sin la obligación previa de contar con la certificación ISO/IEC 27001.

Cambios principales

Independencia operativa:

Elimina la dependencia estricta de una certificación previa de seguridad de la información.

Estructura Harmonizada (HLS):

Adopta las cláusulas estándar de la ISO (de la 4 a la 10), facilitando la compatibilidad nativa con marcos como ISO 9001 o ISO/IEC 42001 (Gobernanza de IA).

Nuevos riesgos tecnológicos:

Añade directrices específicas para mitigar amenazas modernas como la elaboración de perfiles con Inteligencia Artificial, flujos de datos transfronterizos, mecanismos de verificación de edad y datos biométricos.

Anexo B normativo:

Las guías detalladas para la implementación de controles pasan de ser informativas a ser requisitos obligatorios para fines de evaluación y auditoría.

Estructura de Cláusulas y Controles

El estándar organiza sus requisitos de la siguiente manera:

Cláusulas del Sistema de Gestión (4-10):

Definen el contexto de la organización, el liderazgo de la dirección, la planeación mediante análisis de riesgos, el soporte técnico, la operación diaria, la evaluación del desempeño y la mejora continua mediante el ciclo PDCA.

Controles para Encargados y Responsables:

Distribuye un conjunto optimizado de controles operativos enfocados en la protección de la información de identificación personal (PII), distinguiendo claramente si la organización actúa como controlador (*PII controller*) o procesador (*PII processor*) de los datos.

Equivalencias y Cumplimiento Regulatorio

A través de sus anexos de mapeo desarrollados por comités de la Organización Internacional de Normalización (ISO), la norma sirve como una herramienta técnica para demostrar conformidad frente a legislaciones globales:

Región/ Marco	Regulación Mapeada	Utilidad del PIMS
Unión Europea	**Reglamento General de Protección de Datos (RGPD)**	**El Anexo D ofrece un mapeo directo para estructurar el cumplimiento europeo.**
Estados Unidos	**Ley de Privacidad del Consumidor de California (CCPA)**	**Facilita auditorías de debida diligencia comerciales y contractuales.**
América Latina	**Leyes locales de privacidad (Chile, Colombia, México, Perú)**	**Sirve como evidencia medible de madurez organizativa ante reguladores locales.**

Plazos de Transición

Las empresas que posean una certificación bajo la versión anterior (ISO/IEC 27701:2019) cuentan con un periodo de transición de entre 18 y 24 meses a partir de la fecha de publicación para actualizar sus procesos internos, políticas y auditorías a las exigencias de la edición 2025.

Para ver el contenido completo de información específica contáctanos, la Norma **ISO 27701:2025 se incluye en Gap Analysis.**

Atención a Clientes

Lic. Alejandra Morales / Ing Gerardo García

Dirección Comercial WST / Dirección Operaciones WST

55 6581 0662 / 55 6581 0123

licmorales@iso-irca.com / inggarcia@iso-irca.com