CertJoin
CERTIFIED PROFESSIONAL

CERTJOIN

Certification Body

SYLLABUS OFICIAL
ISO/IEC 27701 Implementer Certified
(27701:2025-ICE)

+1 (863) 591-0316
support@certjoin.com
www.certjoin.com
4300 Biscayne Blvd
Suite 203

Documento:	**CJ-SYL-27701:2025-ICE-v1.0**
Versión:	1.0
Fecha de emisión:	21/07/2026
Aprobado por:	Comité de Esquema de Certificación - CertJoin
Clasificación:	Público

Tabla de Contenidos

1. Introducción
2. Perfil del Candidato y Horas de Estudio Recomendadas
3. Estructura del Examen
4. Desglose de Dominios y Objetivos de Aprendizaje
   4.1 Dominio 1: Fundamentos de Privacidad y Marco Normativo
   4.2 Dominio 2: Contexto de la Organización y Liderazgo
   4.3 Dominio 3: Planificación del PIMS
   4.4 Dominio 4: Implementación Operativa del PIMS
   4.5 Dominio 5: Evaluación, Auditoría y Mejora Continua
   4.6 Dominio 6: Integración con SGSI y Cumplimiento Regulatorio
   4.7 Dominio 7: Herramientas, Técnicas y Mejores Practicas
5. Referencias Bibliográficas y Material de Estudio
6. Recomendaciones para la Preparación del Examen
7. Formato y Tipología de Preguntas del Examen
8. Condiciones de Administración del Examen

1. Introducción

Este documento constituye el syllabus oficial de referencia para la certificación ISO/IEC 27701 Implementer Certified (27701:2025-ICE) de CertJoin. Define de manera detallada los dominios de competencia, los objetivos de aprendizaje, las horas de estudio recomendadas, las referencias bibliográficas y la estructura del examen de certificación.
El syllabus ha sido desarrollado por el Comité de Esquema de CertJoin mediante un Job Task Analysis (JTA) con la participación de Expertos en la Materia (SMEs) en protección de datos, privacidad, sistemas de gestión de información de privacidad y legislación de protección de datos. Su propósito es servir como guía de estudio oficial para los candidatos y como marco de referencia para el desarrollo del banco de preguntas del examen.
La certificación 27701:2025-ICE evalúa las competencias necesarias para establecer, implementar, mantener y mejorar un Sistema de Gestión de Información de Privacidad (PIMS) conforme a los requisitos de la norma ISO/IEC 27701:2025, extendiendo y complementando un Sistema de Gestión de Seguridad de la Información (SGSI) basado en ISO/IEC 27001 o ISO/IEC 27002.

2. Perfil del Candidato y Horas de Estudio Recomendadas

Esta certificación está dirigida a profesionales que desempeñan o aspiran a desempeñar el rol de implementador de un PIMS. Se recomienda que el candidato cuente con experiencia previa en protección de datos, seguridad de la información o auditoría de sistemas de gestión, y conocimientos fundamentales de la normativa de protección de datos personales.
Horas de estudio recomendadas para la preparación del examen:

Modalidad	Horas Recomendadas	Descripción
Autodidacta	80 - 120 horas	Estudio individual basado en este syllabus y referencias bibliográficas.
Curso dirigido	40 - 56 horas	Curso oficial o programa de formación impartido por proveedores autorizados.
Blended learning	56 - 80 horas	Combinación de formación en línea con sesiones prácticas presenciales o virtuales.

3. Estructura del Examen

Distribución de preguntas por dominio:

ID	Dominio	Peso	Preguntas	Nivel Bloom	Horas Estudio
D1	Fundamentos de Privacidad y Marco Normativo	15%	8	Conocer / Comprender	12 - 16 h
D2	Contexto de la Organización y Liderazgo	10%	5	Comprender / Aplicar	8 - 12 h
D3	Planificación del PIMS	15%	8	Comprender / Aplicar	12 - 16 h
D4	Implementación Operativa del PIMS	25%	13	Aplicar / Analizar	18 - 24 h
D5	Evaluación, Auditoría y Mejora Continua	15%	8	Analizar / Evaluar	12 - 16 h
D6	Integración con SGSI y Cumplimiento Regulatorio	10%	5	Analizar / Evaluar	8 - 12 h
D7	Herramientas, Técnicas y Mejores Practicas	10%	5	Evaluar / Crear	8 - 12 h

4. Desglose de Dominios y Objetivos de Aprendizaje

4.1 Dominio 1: Fundamentos de Privacidad y Marco Normativo

Objetivos de aprendizaje del dominio:

Código	Objetivo de Aprendizaje	Nivel Bloom	Horas
D1.1	Comprender los principios fundamentales de protección de datos personales: licitud, lealtad, transparencia, limitación de la finalidad, minimización de datos, exactitud, limitación del almacenamiento, integridad y confidencialidad, responsabilidad proactiva.	Comprender	2 h
D1.2	Explicar la estructura y los requisitos de la norma ISO/IEC 27701:2025, incluyendo su relación con ISO/IEC 27001 e ISO/IEC 27002.	Comprender	2 h
D1.3	Comprender los roles y responsabilidades en la gestión de datos personales: controlador, procesador, subprocurador, DPO, titular de datos.	Comprender	1.5 h
D1.4	Identificar las diferencias y complementariedad entre ISO 27701 y los marcos regulatorios de protección de datos: RGPD (UE), CCPA/CPRA (California), LEY 1581 de 2012 (Colombia), LGPDPP (México) y	Conocer	2 h

	otras legislaciones nacionales.		
D1.5	Dominar la terminología de privacidad: datos personales, PII, tratamiento, consentimiento, anonimizarían, seudonimización, perfilado, decisión automatizada, transferencia internacional.	Conocer	2 h
D1.6	Comprender el ciclo PHVA (Planificar-Hacer-Verificar-Actuar) aplicado al PIMS.	Comprender	1.5 h
D1.7	Identificar los principios de privacidad por diseño y por defecto conforme al articulo 25 del RGPD y a ISO 27701.	Conocer	1.5 h

4.1.1 Temario Detallado

D1-A: Principios de Protección de Datos (2 h, nivel Bloom: Conocer)

- Los siete principios del RGPD y su aplicación en el PIMS
- Principio de licitud, lealtad y transparencia
- Principio de limitación de la finalidad
- Principio de minimización de datos
- Principio de exactitud
- Principio de limitación del almacenamiento
- Principio de integridad y confidencialidad
- Principio de responsabilidad proactiva (accountability)

D1-B: Estructura de ISO/IEC 27701 y su Relación con ISO 27001 (2 h, nivel Bloom: Comprender)

- Alcance y propósito de ISO/IEC 27701:2025
- Extensión de los requisitos de ISO/IEC 27001 e ISO/IEC 27002
- Estructura de alto nivel (HLS) y su aplicación en ISO 27701
- Cláusulas 4-10 de ISO 27701: requisitos para controladores y procesadores
- Anexo A: Objetivos de control y controles para controladores y procesadores
- Anexo B: Guía de implementación de controles
- Anexo C: Controles de seguridad de la información aplicables a PII

D1-C: Roles y Responsabilidades en Protección de Datos (1.5 h, nivel Bloom: Comprender)

- Responsable del tratamiento (controlador): definición y obligaciones
- Encargado del tratamiento (procesador): definición y obligaciones
- Subprocuradores: gestión y autorización
- Delegado de Protección de Datos (DPO): rol, funciones y requisitos de independencia
- Titular de datos: definición y derechos fundamentales

D1-D: Marcos Regulatorios de Protección de Datos (2 h, nivel Bloom: Conocer)

- Reglamento General de Protección de Datos (RGPD) - Reglamento (UE) 2016/679
- Ley Estatutaria 1581 de 2012 y Decreto 1377 de 2013 (Colombia)
- Ley Federal de Protección de Datos Personales en Posesión de los Particulares (México)
- California Consumir Privacy Act (CCPA) / California Privacy Rights Act (CPRA)
- Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales (España)
- Diferencias clave entre marcos regulatorios y complementariedad con ISO 27701

D1-E: Terminología de Privacidad y Ciclo PHVA (2.5 h, nivel Bloom: Conocer/Comprender)

- Definiciones clave: datos personales, PII, tratamiento, consentimiento, anonimización, seudonimización
- Conceptos avanzados: perfilado, decisión automatizada, transferencia internacional
- Ciclo PHVA aplicado al PIMS: Planificar, Hacer, Verificar, Actuar
- Privacidad por diseño y por defecto: principios y aplicación práctica
- ISO/IEC 29100:2011 - Marco de protección de la información privada
- ISO/IEC 27018:2019 - Protección de PII en servicios en la nube

4.2 Dominio 2: Contexto de la Organización y Liderazgo

Objetivos de aprendizaje del dominio:

Código	Objetivo de Aprendizaje	Nivel Bloom	Horas
D2.1	Analizar el contexto de la organización: partes interesadas, factores internos y externos, y requisitos de privacidad aplicables.	Analizar	2 h
D2.2	Definir el alcance del PIMS considerando los limites organizacionales, tecnológicos y normativos.	Aplicar	2 h
D2.3	Establecer la política de privacidad de la organización alineada con la estrategia del negocio y los requisitos normativos.	Aplicar	2 h
D2.4	Definir roles, responsabilidades y autoridades para la gestión de la privacidad (DPO, comité de privacidad, equipos de cumplimiento).	Aplicar	1.5 h
D2.5	Establecer mecanismos de comunicación interna y externa sobre políticas y procedimientos de privacidad.	Aplicar	1.5 h

4.2.1 Temario Detallado

D2-A: Contexto de la Organización (2 h, nivel Bloom: Analizar)

- Comprensión de la organización y su contexto: factores internos y externos
- Identificación de partes interesadas en materia de privacidad
- Requisitos de las partes interesadas: titulares, autoridades de control, proveedores, empleados
- Análisis de requisitos legales y regulatorios aplicables
- Documentación del contexto del PIMS

D2-B: Alcance y Política del PIMS (2 h, nivel Bloom: Aplicar)

- Definición del alcance del PIMS: limites organizacionales, tecnológicos y normativos
- Justificación del alcance definido
- Elementos de la política de privacidad: compromisos, principios, roles, marco de mejora continua
- Alineación de la política con la estrategia del negocio
- Aprobación, comunicación y revisión de la política de privacidad

D2-C: Liderazgo, Roles y Comunicación (2 h, nivel Bloom: Aplicar)

- Compromiso de la alta dirección con la protección de datos
- Designación formal del DPO o responsable de privacidad
- Definición de responsabilidades y autoridades en la gestión de privacidad
- Estructura de gobernanza de privacidad: comité de privacidad, equipos de cumplimiento
- Mecanismos de comunicación interna y externa sobre políticas y procedimientos

4.3 Dominio 3: Planificación del PIMS

Objetivos de aprendizaje del dominio:

Código	Objetivo de Aprendizaje	Nivel Bloom	Horas
D3.1	Identificar y evaluar los riesgos asociados al tratamiento de datos personales en la organización.	Aplicar	2 h
D3.2	Aplicar metodologías de evaluación de riesgos de privacidad adaptadas al contexto organizacional.	Aplicar	2 h
D3.3	Establecer objetivos de privacidad medibles y compatibles con la política de la organización.	Aplicar	1.5 h
D3.4	Planificar acciones para tratar los riesgos de privacidad, definiendo recursos, responsabilidades y cronogramas.	Aplicar	2 h
D3.5	Elaborar el inventario de tratamientos de datos personales (Récord o Processing Activities - ROPA).	Aplicar	1.5 h
D3.6	Definir criterios de Evaluación de Impacto a la Privacidad (PÍA/DPIA) conforme a ISO 27701 y al RGPD.	Comprender	2 h
D3.7	Diseñar el plan de implementación del PIMS con fases, hitos y criterios de aceptación.	Aplicar	2 h
D3.8	Establecer indicadores clave de desempeño (KPIs) para medir la eficacia del PIMS.	Aplicar	1.5 h

4.3.1 Temario Detallado

D3-A: Evaluación de Riesgos de Privacidad (2.5 h, nivel Bloom: Aplicar)

- Identificación de activos de información personal y procesos de tratamiento

- Identificación de amenazas y vulnerabilidades asociadas al tratamiento de datos
- Metodologías de evaluación de riesgos de privacidad adaptadas al contexto
- Criterios de aceptación del riesgo de privacidad
- Planificación de acciones de tratamiento de riesgos: recursos, responsabilidades, cronogramas

D3-B: Objetivos de Privacidad e Inventario de Tratamientos (2 h, nivel Bloom: Aplicar)

- Definición de objetivos de privacidad: coherencia con la política, medibilidad, monitoreo
- Elaboración del inventario de tratamientos de datos personales (ROPA)
- Categorías de datos, fines del tratamiento, destinatarios, transferencias, plazos de conservación
- Establecimiento de indicadores clave de desempeño (KPIs) para el PIMS

D3-C: Evaluación de Impacto y Plan de Implementación (2 h, nivel Bloom: Aplicar/Comprender)

- Criterios para la Evaluación de Impacto a la Privacidad (PÍA/DPIA)
- Metodologías de DPIA: ICO, CNIL, AEPD
- Elementos de la DPIA: descripción del tratamiento, necesidad, proporcionalidad, riesgos, mitigación
- Diseño del plan de implementación del PIMS: fases, hitos, criterios de aceptación
- Gestión de la transferencia internacional de datos en la planificación

4.4 Dominio 4: Implementación Operativa del PIMS

Objetivos de aprendizaje del dominio:

Código	Objetivo de Aprendizaje	Nivel Bloom	Horas
D4.1	Implementar controles del Anexo A (Tablas A.1, A.2 y A.3) de ISO 27701 para controladores de datos: gestión de la relación con titulares, obtención y registro de consentimiento, gestión de derechos, minimización de datos, notificación de brechas.	Aplicar	4 h
D4.2	Implementar controles del Anexo A (Tablas A.1, A.2 y A.3) de ISO 27701 para procesadores de datos: trato específico y seguro de datos personales, subprocesadores, auditorías y mejoras.	Aplicar	3 h
D4.3	Aplicar las directrices de implementación del Anexo B de ISO 27701 para la gestión de información de privacidad.	Aplicar	2 h
D4.4	Implementar los controles de seguridad de la información del Anexo C de ISO 27701 para la protección de datos personales.	Aplicar	3 h
D4.5	Establecer procesos para la gestión de derechos de los titulares: acceso, rectificación, supresión, portabilidad, oposición y decisiones automatizadas.	Aplicar	3 h
D4.6	Implementar mecanismos de gestión de incidentes de protección de datos y	Aplicar	2 h

	notificación a autoridades de control y titulares.		
D4.7	Gestionar la relación con proveedores y encargados de tratamiento: cláusulas contractuales, auditorías y evaluaciones de cumplimiento.	Aplicar	2 h
D4.8	Implementar mecanismos de transferencia internacional de datos: cláusulas contractuales estándar, decisiones de adecuación, normas corporativas vinculantes.	Aplicar	2 h
D4.9	Implementar controles de privacidad en el ciclo de vida del desarrollo de software (privacy by design).	Aplicar	2 h
D4.10	Establecer procesos de gestión de la información documentada del PIMS.	Aplicar	1.5 h
D4.11	Implementar formación y concienciación en materia de privacidad para todo el personal.	Aplicar	1.5 h
D4.12	Implementar controles de acceso y autenticación para sistemas que contienen datos personales.	Aplicar	1.5 h
D4.13	Implementar mecanismos de enmascaramiento, anonimización y seudonimización de datos personales.	Aplicar	1.5 h

4.4.1 Temario Detallado

D4-A: Controles del Anexo A para Controladores de Datos (4 h, nivel Bloom: Aplicar)

- Gestión de la relación con titulares de datos
- Obtención, registro y gestión del consentimiento
- Gestión de derechos de los titulares: acceso, rectificación, supresión, portabilidad, oposición
- Minimización de datos y limitación de la finalidad
- Notificación de brechas de datos personales a autoridades y titulares
- Decisiones automatizadas y perfilado: transparencia y derechos del titular

D4-B: Controles del Anexo A para Procesadores de Datos (3 h, nivel Bloom: Aplicar)

- Trato específico y seguro de datos personales
- Gestión de subprocesadores: autorización, contrato, verificación
- Auditorías y mejoras en la relación con el responsable del tratamiento
- Devolución o eliminación de datos al terminar el contrato
- Cooperación con autoridades de control

D4-C: Directrices del Anexo B y Controles del Anexo C (2.5 h, nivel Bloom: Aplicar)

- Uso del Anexo B como guía de implementación práctica
- Controles de seguridad de la información del Anexo C aplicables a datos personales
- Cifrado, control de acceso, gestión de incidentes, continuidad del negocio
- Evaluación de la efectividad de los controles implementados

D4-D: Gestión de Derechos, Incidentes y Proveedores (3 h, nivel Bloom: Aplicar)

- Procesos de atención a solicitudes de derechos de titulares
- Plazos legales de respuesta y documentación
- Gestión de incidentes: detección, clasificación, notificación, registro, lecciones aprendidas
- Gestión de proveedores y encargados de tratamiento: evaluación, contrato, auditoría

D4-E: Transferencia Internacional, Privacy by Design y Documentación (3 h, nivel Bloom: Aplicar)

- Mecanismos de transferencia internacional: SCC, BCR, decisiones de adecuación
- Evaluación de riesgos de transferencia internacional
- Privacidad por diseño y por defecto en el ciclo de vida del software
- Gestión de la información documentada del PIMS: políticas, procedimientos, registros
- Formación y concienciación en privacidad para todo el personal
- Controles de acceso, autenticación, anonimización y seudonimización

4.5 Dominio 5: Evaluación, Auditoría y Mejora Continua

Objetivos de aprendizaje del dominio:

Código	Objetivo de Aprendizaje	Nivel Bloom	Horas
D5.1	Establecer y gestionar el programa de evaluación del desempeño del PIMS.	Aplicar	2 h
D5.2	Preparar y ejecutar auditorías internas del PIMS conforme a ISO 19011 y a los requisitos de ISO 27701.	Aplicar	2.5 h
D5.3	Verificar la eficacia de los controles de privacidad implementados.	Analizar	2 h
D5.4	Elaborar informes de auditoría del PIMS con hallazgos, no conformidades y recomendaciones.	Analizar	2.5 h
D5.5	Implementar procesos de revisión por la dirección del PIMS.	Aplicar	2 h
D5.6	Gestionar no conformidades, acciones correctivas y preventivas.	Aplicar	2 h
D5.7	Evaluar la madurez del PIMS y definir planes de mejora continua.	Evaluar	2 h
D5.8	Preparar a la organización para auditorías de certificación externa del PIMS.	Aplicar	1.5 h

4.5.1 Temario Detallado

D5-A: Programa de Auditoría Interna del PIMS (2 h, nivel Bloom: Aplicar)

- Establecimiento del programa de auditoría interna basado en riesgos
- Frecuencia y alcance de las auditorías internas
- Criterios de selección de auditores internos: competencia e independencia
- Registros del programa de auditoría y seguimiento de resultados

D5-B: Preparación y Ejecución de Auditorías Internas (2.5 h, nivel Bloom: Aplicar)

- Preparación de listas de verificación (checklists) mapeadas a cláusulas de ISO 27701
- Definición del alcance, criterios y objetivos de cada auditoría
- Ejecución de la auditoría: entrevistas, revisión documental, observación, muestreo
- Técnicas de auditoría: entrevista efectiva, rastreo documental, verificación de evidencia
- Reunión de apertura y cierre de la auditoría interna

D5-C: Informes de Auditoría y Gestión de No Conformidades (2.5 h, nivel Bloom: Analizar)

- Elaboración de informes de auditoría del PIMS
- Redacción de no conformidades: hallazgo, requisito incumplido, evidencia objetiva, clasificación
- Clasificación de hallazgos: NC mayor, NC menor, observación, oportunidad de mejora
- Conclusiones y recomendaciones del informe

D5-D: Revisión por la Dirección y Mejora Continua (2.5 h, nivel Bloom: Aplicar/Evaluar)

- Proceso de revisión por la dirección del PIMS: entradas, salidas, eficacia
- Gestión de no conformidades: investigación de causa raíz, acción correctiva, verificación de eficacia
- Evaluación de la madurez del PIMS: modelos de escalera de madurez
- Planes de mejora continua basados en resultados de auditorías, indicadores y cambios normativos
- Preparación para auditorías de certificación externa del PIMS

4.6 Dominio 6: Integración con SGSI y Cumplimiento Regulatorio

Objetivos de aprendizaje del dominio:

Código	Objetivo de Aprendizaje	Nivel Bloom	Horas
D6.1	Integrar el PIMS con el SGSI basado en ISO 27001, aprovechando la estructura HLS y los controles comunes.	Analizar	2.5 h
D6.2	Evaluar la alineación del PIMS con otros sistemas de gestión: ISO 9001, ISO 22301.	Analizar	2 h
D6.3	Comprender la relación entre ISO 27701 y el RGPD, incluyendo la evidencia de cumplimiento que proporciona la certificación.	Comprender	2 h
D6.4	Evaluar escenarios de implementación en sectores regulados: salud, finanzas, educación, telecomunicaciones.	Analizar	2.5 h
D6.5	Gestionar el cumplimiento normativo en contextos de transferencia internacional de datos.	Aplicar	2 h

4.6.1 Temario Detallado

D6-A: Integración del PIMS con el SGSI (2.5 h, nivel Bloom: Analizar)

- Ventajas de integrar el PIMS con el SGSI basado en ISO 27001
- Aprovechamiento de la estructura HLS: procesos comunes (auditoría interna, revisión por la dirección, gestión de riesgos)
- Mapeo de controles de seguridad de ISO 27001 y controles de privacidad de ISO 27701
- Identificación de brechas y complementación de controles adicionales
- Documentación de la correlación entre ambos sistemas

D6-B: Integración con Otros Sistemas de Gestión (2 h, nivel Bloom: Analizar)

- Alineación con ISO 9001: gestión de documentos, auditoría interna, revisión por la dirección

- Alineación con ISO 22301: continuidad del negocio y protección de datos
- Evitación de duplicidades e inconsistencias entre sistemas de gestión
- Integración de procesos compartidos: no conformidades, acciones correctivas, gestión documental

D6-C: Relación entre ISO 27701 y el RGPD (2 h, nivel Bloom: Comprender)

- La certificación ISO 27701 como evidencia de buenas prácticas de cumplimiento
- Limitaciones de la certificación: no sustituye obligaciones directas del RGPD
- Mapeo de requisitos del RGPD a controles de ISO 27701
- Diferencias entre la certificación y la evaluación de conformidad por autoridades de control

D6-D: Sectores Regulados y Transferencia Internacional (2.5 h, nivel Bloom: Analizar)

- Implementación del PIMS en el sector salud: datos de salud, normativa sectorial, HIPAA
- Implementación del PIMS en el sector financiero: regulaciones prudenciales y de datos
- Implementación del PIMS en el sector educativo: datos de estudiantes, menores de edad
- Implementación del PIMS en el sector de telecomunicaciones: metadatos, geolocalización
- Gestión del cumplimiento normativo en transferencias internacionales de datos
- Evaluación de riesgos de transferencia y mecanismos de salvaguarda

4.7 Dominio 7: Herramientas, Técnicas y Mejores Practicas

Objetivos de aprendizaje del dominio:

Código	Objetivo de Aprendizaje	Nivel Bloom	Horas
D7.1	Aplicar herramientas de gestión de consentimiento y preferencias de privacidad.	Aplicar	2 h
D7.2	Utilizar herramientas de gestión de incidentes de datos personales y notificaciones regulatorias.	Aplicar	1.5 h
D7.3	Implementar herramientas de gestión de inventarios de datos y flujos de información personal.	Aplicar	1.5 h
D7.4	Aplicar técnicas de evaluación de impacto a la privacidad (PÍA/DPIA) con metodologías reconocidas.	Aplicar	2 h
D7.5	Identificar tendencias y mejores prácticas en gestión de privacidad: zero trust, PETs, federated learning.	Evaluar	1.5 h

4.7.1 Temario Detallado

D7-A: Herramientas de Gestión de Consentimiento y Preferencias (2 h, nivel Bloom: Aplicar)

- Centros de preferencias de privacidad: diseño, funcionalidades y experiencia del usuario
- Gestión granular de consentimientos por categoría de tratamiento
- Registro de consentimientos: fecha, versión, alcance, retiro
- Automatización de la gestión de consentimientos en aplicaciones web y móvil

D7-B: Herramientas de Gestión de Incidentes e Inventarios (1.5 h, nivel Bloom: Aplicar)

- Sistemas de registro y notificación de incidentes de datos personales
- Automatización de notificaciones a autoridades de control y titulares
- Herramientas de gestión de inventarios de datos personales y flujos de información

- Automatización de la generación de ROPA (Récord of Processing Activities)

D7-C: Evaluación de Impacto y Metodologías Reconocidas (2 h, nivel Bloom: Aplicar)

- Metodología del Information Commissioner's Office (ICO) del Reino Unido
- Marco de la Commission Nationale de l'Informatique et des Libertés (CNIL) de Francia
- Guía de la Agencia Española de Protección de Datos (AEPD)
- Elementos comunes de una DPIA: descripción, necesidad, proporcionalidad, riesgos, mitigación
- Integración de la DPIA en el ciclo de vida del proyecto

D7-D: Tendencias y Mejores Practicas en Gestión de Privacidad (1.5 h, nivel Bloom: Evaluar)

- Zero trust (confianza cero): principio y aplicación a la protección de datos
- Privacy Enhancing Technologies (PETs): seudonimización, anonimización, cifrado homomórfico
- Federated learning: aprendizaje federado como técnica de privacidad en IA
- Differential privacy: privacidad diferencial para análisis de datos
- Plataformas de automatización de cumplimiento de privacidad (privacy ops)
- Gobernanza de datos y arquitectura de privacidad

5. Referencias Bibliográficas y Material de Estudio

5.1 Referencias Obligatorias

- ISO/IEC 27701:2025 - Information technology - Security techniques - Extensión to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management - Requirements and guidelines.
- ISO/IEC 27001:2022 - Information security, cybersecurity and privacy protection - Information security management systems - Requirements.
- ISO/IEC 27002:2022 - Information security, cybersecurity and privacy protection - Information security controls.
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo - Reglamento General de Protección de Datos (RGPD).
- ISO/IEC 17024:2012 - Conformity assessment - General requirements for bodies operating certification of persons.

5.2 Referencias Recomendadas

- ISO/IEC 29100:2011 - Information technology - Security techniques - Privacy framework.
- ISO/IEC 27018:2019 - Information technology - Security techniques - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors.
- ISO/IEC 27002:2022 - Códigos de práctica para controles de seguridad de la información.
- Ley Estatutaria 1581 de 2012 y Decreto 1377 de 2013 (Colombia) - Protección de datos personales.
- Ley Federal de Protección de Datos Personales en Posesión de los Particulares (México).
- California Consumer Privacy Act (CCPA) y California Privacy Rights Act (CPRA).
- ISO/IEC 29134:2023 - Information security, cybersecurity and privacy protection - Privacy impact assessment guideline.
- ISO 31000:2018 - Risk management - Guidelines.
- ISO 9001:2015 - Quality management systems - Requirements.
- ISO 22301:2019 - Business continuity management systems - Requirements.

5.3 Material de Estudio CertJoin

- Guía de Estudio Oficial 27701:2025-ICE (disponible en portal del candidato).
- Simulador de examen 27701:2025-ICE con escenarios reales de implementación del PIMS.
- Caso práctico: Implementación del PIMS en una empresa de comercio electrónico.
- Caso práctico: Implementación del PIMS en una entidad del sector salud.
- Plantillas de trabajo: política de privacidad, ROPA, DPIA, plan de implementación.

- Webinars grabados: Técnicas de implementación de ISO 27701 y gestión de privacidad.

6. Recomendaciones para la Preparación del Examen

- Leer completamente la norma ISO/IEC 27701:2025, prestando especial atención a los Anexos A, B y C y a las cláusulas 4-10.
- Estudiar los requisitos de ISO/IEC 27001:2022 como base fundamental del PIMS.
- Comprender la estructura y los principios del RGPD, incluyendo los derechos de los titulares y las obligaciones de los responsables y encargados del tratamiento.
- Realizar ejercicios prácticos de implementación del PIMS utilizando casos de estudio de distintos sectores.
- Practicar la elaboración de documentación del PIMS: política de privacidad, ROPA, DPIA, procedimientos de gestión de derechos.
- Utilizar el simulador de examen oficial de CertJoin para familiarizarse con el formato y tipo de preguntas.
- Formar grupos de estudio con otros candidatos para simular escenarios de implementación.
- Mantenerse actualizado sobre la regulación de protección de datos (RGPD, leyes nacionales, sentencias del TJUE).
- Distribuir el tiempo de estudio proporcionalmente al peso de cada dominio en el examen.
- Dedicar especial atención al Dominio 4 (25%) que representa la mayor proporción del examen y evalúa competencias prácticas de implementación.
- Repasar la terminología técnica de privacidad según ISO/IEC 29100 y los conceptos de gestión de riesgos según ISO 31000.
- Estudiar los mecanismos de transferencia internacional de datos (SCC, BCR) y sus requisitos de implementación.

7. Formato y Tipología de Preguntas del Examen

El examen 27701:2025-ICE consta de 52 preguntas distribuidas en dos tipologías:

7.1 Tipo 1: Escenarios de Implementación (65% - 34 preguntas)

Estas preguntas presentan situaciones reales o simuladas de implementación del PIMS. El candidato debe:

- Determinar la acción más adecuada del implementador ante una situación dada

- Identificar los controles del Anexo A (Tablas A.1, A.2 y A.3) de ISO 27701 aplicables a una situación específica
- Diseñar o evaluar procedimientos de gestión de datos personales
- Resolver problemas específicos de privacidad en contextos organizacionales reales
- Seleccionar el mecanismo de transferencia internacional más apropiado
- Evaluar la suficiencia y adecuación de la evidencia de implementación

7.2 Tipo 2: Conceptuales / Normativas (35% - 18 preguntas)

Estas preguntas evalúan el conocimiento directo de:

- Requisitos específicos de las cláusulas 4-10 de ISO/IEC 27701
- Controles de los Anexos A, B y C de ISO 27701 y su propósito
- Terminología y definiciones según ISO/IEC 29100 y el RGPD
- Principios de protección de datos personales y sus aplicaciones
- Estructura y contenido de la documentación del PIMS
- Conceptos clave de regulación de protección de datos (RGPD, leyes nacionales)

8. Condiciones de Administración del Examen

Condición	Descripción
Formato	Online con proctoring remoto síncrono mediante Safe Exam Browser.
Duración	100 minutos continuos.
Número de preguntas	52 preguntas.
Tipos de preguntas	Escenarios de implementación (65%) y conceptuales/normativas (35%).
Puntaje de aprobación	70% (37 de 52 aciertos).
Intentos permitidos	2 intentos incluidos. Intentos adicionales requieren tarifa adicional.
Periodo entre intentos	Mínimo 14 días naturales entre intentos.
Idiomas disponibles	Español e ingles.
Requisitos técnicos	Computador con cámara y micrófono, conexión estable a internet, documento de identificación oficial vigente, espacio silencioso y privado.
Política de.cancelación	El candidato puede cancelar o reprogramar hasta 48 horas antes del examen sin penalización.

Fin del Documento

Copyright CertJoin. Todos los derechos reservados.