

ISO/IEC 27001:2022 Implementer

Certification Syllabus

Última revisión: Octubre 23 del 2026

Contenido

- Descripción del Esquema 3
- Competencias requeridas y descripción del trabajo 4
- Evaluación de las competencias 7
- ¿Quién debería tomar este examen? 8
- Proceso de certificación 8
- Niveles de dificultad: Taxonomía de Bloom 10
- Renovación, vigilancia y retiro de la certificación 12

certm:nd

ISO/IEC 27001:2022 Implementador

Nuestro objetivo en CertMind es certificar las habilidades de los profesionales que se desempeñan en el contexto de Tecnología. Para lograrlo, buscamos asegurar que los profesionales demuestren sus habilidades y conocimientos mediante la aplicación de un Examen de Certificación Internacional.

Categoría de la certificación



Categoría principal: Estándares ISO/IEC

Categoría: Sistema de Gestión de Seguridad de la Información

Subcategoría: Implementación

Alcance de la certificación

El propósito de la Certificación de ISO/IEC 27001 Implementador es demostrar que el profesional comprende la terminología, estructura y consideraciones para la definición, implementación, operación, seguimiento y mejora de un Sistema de Gestión de Seguridad de la Información (SGSI), según la norma ISO/IEC 27001:2022.

Prerrequisitos



- Ser mayor de edad, según la edad mínima determinada por Ley (Según el Documento Nacional de Identidad que deberá ser subido a la plataforma).
- Tener conocimientos básicos de lectura, escritura y aritmética básica: suma, resta, multiplicación y división.
- Lectura y aceptación del Código de ética disponible en la plataforma antes de la presentación del examen de certificación.

Código de ética

Todos los profesionales certificados deben conocer, aceptar y acogerse al Código de ética que está disponible para su consulta en la plataforma.

Recomendaciones

- Es altamente recomendable que el profesional asista a una capacitación formal de ISO/IEC 27001:2022 Implementador de mínimo 18 horas, segmentada en 9 sesiones de 2 horas aproximadamente.

Competencias requeridas y descripción del trabajo

Con el fin de asegurar que el profesional cuenta con las competencias y conocimientos mínimos que pueden ser aplicados en un entorno real, en el examen se abordan los siguientes temas:

1. Introducción y contexto de la organización

Habilidad evaluada	Competencias requeridas
Comprender el propósito de la norma y determinar el contexto, las partes interesadas y el alcance del SGSI.	1. Marco normativo: propósito, estructura y términos 2. Cuestiones externas e internas 3. Partes interesadas y sus requisitos 4. Alcance y sistema de gestión de seguridad de la información

2. Liderazgo

Habilidad evaluada	Competencias requeridas
Establecer el compromiso de la alta dirección, la política de seguridad de la información y la asignación de roles.	1. Liderazgo y compromiso 2. Política de seguridad de la información 3. Roles, responsabilidades y autoridades

3. Planificación

Habilidad evaluada	Competencias requeridas
Evaluar y tratar los riesgos de seguridad de la información, elaborar la Declaración de Aplicabilidad y fijar los objetivos de seguridad.	1. Riesgos y oportunidades 2. Evaluación de riesgos de seguridad de la información 3. Tratamiento de riesgos y Declaración de Aplicabilidad 4. Objetivos de seguridad y planificación de los cambios

4. Apoyo y operación

Habilidad evaluada	Competencias requeridas
Asegurar los recursos, la competencia, la comunicación y la documentación del SGSI, y planificar y controlar su operación.	1. Recursos, competencia y toma de conciencia 2. Comunicación 3. Información documentada 4. Planificación y control de la operación 5. Evaluación y tratamiento de riesgos en la operación

5. Evaluación del desempeño y mejora

Habilidad evaluada	Competencias requeridas
Evaluar el desempeño del SGSI y gestionar su mejora continua.	1. Seguimiento, medición, análisis y evaluación 2. Auditoría interna 3. Revisión por la dirección 4. Mejora continua y acciones correctivas

6. Anexo A: controles organizacionales

Habilidad evaluada	Competencias requeridas
Aplicar los 37 controles organizacionales del Anexo A y justificar su inclusión o exclusión en la Declaración de Aplicabilidad.	1. Gobierno y organización 2. Activos, información y acceso 3. Terceros e incidentes 4. Cumplimiento y revisión

7. Anexo A: controles de personas

Habilidad evaluada	Competencias requeridas
Aplicar los 8 controles de personas del Anexo A y su relación con la competencia y la toma de conciencia.	1. Incorporación y compromiso 2. Conciencia y reporte 3. Trabajo remoto y salida

8. Anexo A: controles físicos

Habilidad evaluada	Competencias requeridas
Aplicar los 14 controles físicos del Anexo A y justificar su inclusión o exclusión en la Declaración de Aplicabilidad.	1. Perímetro y acceso 2. Protección del puesto 3. Equipos y soportes

9. Anexo A: controles tecnológicos

Habilidad evaluada	Competencias requeridas
Aplicar los 34 controles tecnológicos del Anexo A y completar la Declaración de Aplicabilidad de los 93 controles con su justificación.	1. Acceso y sistemas 2. Vulnerabilidades y datos 3. Trazabilidad y redes 4. Desarrollo, cifrado y cambios

Evaluación de las competencias

CertMind realiza dos tipos de evaluación para garantizar que el profesional cuenta con las competencias requeridas:

1. Preguntas de opción múltiple con única respuesta: esta modalidad de evaluación consiste en preguntas teóricas de opción múltiple única respuesta que buscan medir el grado en el que el profesional ha comprendido los conceptos teóricos de la certificación.

2. Caso de estudio: su estructura es similar a la que tienen las preguntas de las que se habló en el numeral anterior, la diferencia radica en que, en lugar de preguntar por un concepto particular, se presenta la descripción de una situación que tiene lugar en el contexto real y que debe ser analizada por el profesional de tal manera que pueda en primer lugar identificar el problema y posteriormente evaluar cuál de las opciones presentadas refleja la mejor solución a dicha situación problema.

Competencia	Preguntas (1)	Caso de estudio (2)
Comprender el propósito de la norma ISO/IEC 27001:2022 y determinar el contexto y el alcance del SGSI.	X	
Establecer el liderazgo, la política y los roles del SGSI.	X	
Evaluar y tratar los riesgos de seguridad de la información y elaborar la Declaración de Aplicabilidad.	X	X
Determinar los recursos, la documentación y el control operacional del SGSI.	X	X
Evaluar el desempeño del SGSI y gestionar su mejora continua.	X	

Competencia	Preguntas (1)	Caso de estudio (2)
Aplicar los controles organizacionales y de personas del Anexo A.		X
Aplicar los controles físicos y tecnológicos del Anexo A y completar la Declaración de Aplicabilidad.		X

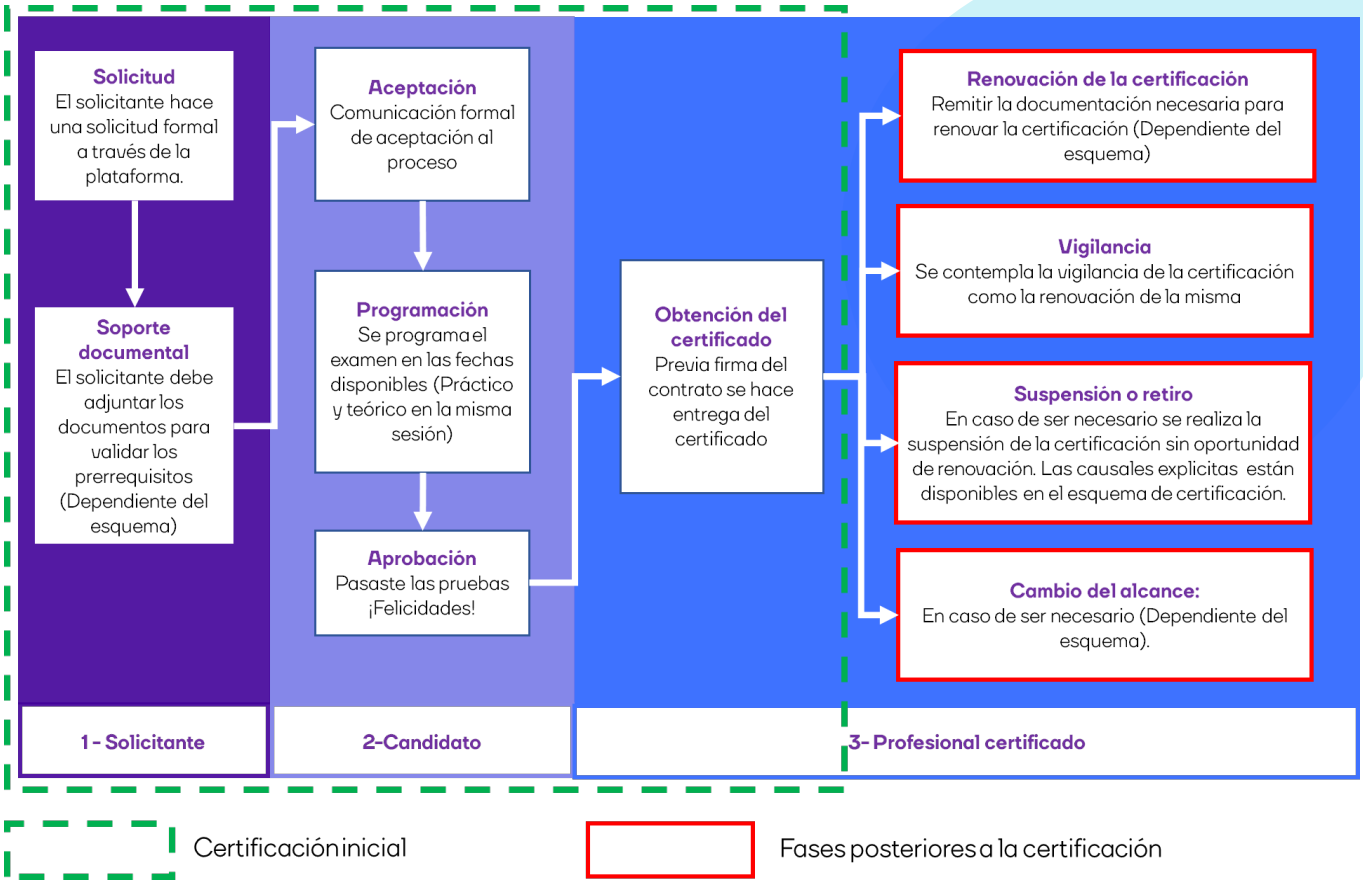
¿Quién debería tomar este examen?

Este examen es ideal para personas o equipos responsables que buscan implementar un Sistema de Gestión de Seguridad de la Información (SGSI) conforme a la norma ISO/IEC 27001, o que se relacionan con su definición, operación y mejora.

Roles como: Oficiales de seguridad de la información, administradores de redes, ingenieros de soporte, analistas de riesgos en sistemas de información, consultores e implementadores del SGSI.

Proceso de certificación

El siguiente gráfico, presenta el ciclo de vida general para la obtención de una certificación:



A continuación, se describe cada una de las fases para la obtención de la certificación por primera vez, las fases posteriores a la obtención del certificado (recuadros de borde rojo) serán explicadas más adelante.

1. Solicitud de certificación: el solicitante remite su solicitud de certificación, en la plataforma QuizLab o a través de la empresa aliada (donde el solicitante haya tomado su capacitación). Una vez aprobada la solicitud se procede a la creación del perfil del solicitante en CertMind.

2. Soporte documental: el solicitante debe adjuntar en la plataforma de CertMind su documento de identidad y adicionalmente completar el registro de su hoja de vida.

3. Verificación y aceptación: la plataforma verifica el cumplimiento de los prerrequisitos del solicitante, una vez verificados es aceptada la solicitud el postulante y se convierte en candidato para el proceso de certificación.

4. Programación: se procede a realizar la convocatoria para la presentación del examen, directamente en la plataforma o a través de su representante. El formato del examen se explica a continuación:

- **Tipo:** Examen en línea de 40 preguntas, opción múltiple y única respuesta.
- **Duración:** 60 minutos.
- **Nota mínima para aprobar:** 28/40 o 70%.
- **Tiempo adicional:** Si el profesional no presenta el examen en su idioma nativo, contará con 15 minutos adicionales y además se le permite utilizar un diccionario.
- **Supervisión:** CertMind realiza el monitoreo de los exámenes asegurando que se realizan de manera correcta y transparente a través de Invigilator Program (también conocido como "Proctor"). Para conocer más sobre este mecanismo de vigilancia consultar la página web www.certmind.org
- **Libro abierto:** No.
- **Modalidad:** Disponible únicamente en línea en la plataforma de CertMind.
- **Vigencia:** 5 Años.
- **Otros:** Se requiere a todos los postulantes la lectura y aceptación del código de ética de la compañía y términos y condiciones.

Niveles de dificultad: Taxonomía de Bloom

La Taxonomía de Bloom es una teoría conocida en el sector educativo porque muchos docentes la consideran idónea para evaluar el nivel cognitivo adquirido en una asignatura. El objetivo de esta teoría es que después de realizar un proceso de aprendizaje, el aprendiente adquiera nuevas habilidades y conocimientos. La siguiente tabla presenta una descripción de las categorías de la taxonomía de Bloom presentes en el examen de certificación, así como el porcentaje de cada tipo de pregunta dentro del examen.

Módulo	Nivel 1	Nivel 2	Nivel 3
Descripción	Conocimiento. Este puede comprender, recordar una amplia gama de elementos, desde datos específicos, hasta teoría completa. Pero todo lo que se necesita es traer a la mente la información apropiada.	Compresión. Esto se puede demostrar pasando o traduciendo, material de una forma a otra (palabras a números), interpretar el material (explicar o resumir), y estimando tendencias futuras (prediciendo consecuencias o efectos).	Aplicación. Hace referencia a la habilidad o capacidad de utilizar el material aprendido en situaciones concretas, nuevas.
Porcentaje de preguntas presente en el examen	50%	30%	20%

Nota: Para obtener más información sobre el sistema de supervisión visita nuestro sitio web https://certmind.org

5. Obtención del certificado: una vez aprobado en examen y aceptado el contrato de términos y condiciones se hace entrega de la certificación.

Renovación, vigilancia y retiro de la certificación

Esta fase se da luego de que el profesional ha obtenido su certificación. La renovación hace referencia a la reexpedición de la certificación una vez la vigencia de la misma ha llegado a su fin. La vigilancia se refiere a la supervisión que realiza CertMind al desempeño que realiza el profesional durante el período transcurrido entre la certificación y la recertificación para asegurar el cumplimiento de lo estipulado en el presente esquema de certificación. A continuación, se describen las actividades que debe realizar el profesional certificado con el objetivo de obtener su recertificación:

1. Solicitud de recertificación: antes de que la certificación pierda su vigencia, el profesional certificado remite su solicitud de recertificación, en la plataforma QuizLab. En caso de que la certificación pierda su vigencia, el profesional debe realizar el proceso de certificación nuevamente.

2. Registro de PUC's: se requiere que el profesional certificado registre 30 PUC's cada 5 años para la renovación de la certificación.

Para obtener más información sobre el sistema de Créditos de Actualización Profesional (PUC) visita nuestro sitio web https://certmind.org. El profesional certificado debe adjuntar los soportes que acreditan las PUC's en la plataforma CertMind.

3. Validación de la documentación: la plataforma verifica el cumplimiento de las PUC's del profesional certificado, una vez verificados es aceptada la solicitud de recertificación.

4. Obtención de la recertificación: una vez validados los documentos se hace entrega de la nueva certificación.

Criterios para la suspensión o retiro de la certificación

La certificación le será retirada al profesional en los siguientes casos:

1. El incumplimiento al código de ética o a los requisitos del esquema.
2. Resultados insatisfactorios del proceso de vigilancia.
3. Incapacidad para cumplir de forma continuada los requisitos de competencia del esquema.

Cambios al esquema de certificación

CertMind revisa continuamente sus esquemas de certificación para incorporar las actualizaciones de la norma ISO/IEC 27001:2022 (nuevas ediciones, enmiendas y correcciones), actualizaciones regulatorias relevantes, y retroalimentación de participantes (resultados de evaluaciones, métricas de desempeño y quejas). Las modificaciones se notifican con al menos 2 meses de antelación a través del sitio web y correo a certificados, y se documentan con versión, fecha e impacto. Cuando un cambio requiera verificación adicional (ej. nuevos controles o requisitos de la norma), se especifican mecanismos públicos de transición, como recertificación focalizada o módulos complementarios, garantizando cumplimiento justo y validez continua sin afectar indebidamente a los ya certificados.



certm:nd

www.certmind.org

b2b@certmind.org – partner@certmind.org

CertMind is a registered trademark of CertMind - Netherlands