Version 1.0

Last update: October 25, 2021

certm:nd

Syllabus

ISO 27001

Information Security Management System (ISMS) (ISO 27001:2013)

www.certmind.org

2021

Contenido

certm:nd

ISO 27001:2013 –Auditor Interno

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

Categoría: Sistema de Gestión de Seguridad de la Información (ISO 27001:2013)

Subcategoría: Auditoría Interna

Alcance de la certificación

El propósito de la Certificación de ISO 27001 – Auditor Interno es demostrar que el profesional tiene una comprensión práctica de la terminología, estructura, y consideraciones para la definición, implementación, seguimiento y auditoría de un Sistema de Gestión de Seguridad de la Información (SGSI); siguiendo los lineamientos de la norma ISO 27001:2013 (seguridad de la información) y la norma ISO 19011:2018 (auditoría).

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 27001:2013 Auditor Interno de mínimo 20 horas, segmentado en 5 sesiones de 4 horas aproximadamente.

• Es recomendable tener experiencia mínima de un (1) año en la definición, implementación, seguimiento, auditoría y/o mejora de un Sistema de Gestión de Seguridad de la Información (SGSI).

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:

Módulo	Descripción del trabajo	Competencias requeridas
1. Introducción	Identificar y dominar los conceptos básicos y el contexto de la organización, su importancia y aspectos generales para el desarrollo de un SGSI	1. Historia, contextualización y estructura de las normas ISO 2. Estructura de la familia ISO 27000 3. Esquema y proceso de certificación 4. Conceptos básicos 5. Objeto y campo de aplicación
2. Contexto de la organización	Planificar y ejecutar las actividades de seguimiento y revisión para identificar el contexto de la organización.	1. Conocimiento de la organización y su contexto. 2. Necesidades y expectativas de las partes interesadas. 3. Alcance del SGSI.
3. Liderazgo	Comprender y determinar si existe liderazgo dentro de la organización para crear un entorno de compromiso frente al SGSI y definir la política de seguridad de la información.	1. Liderazgo y compromiso frente a la definición del SGSI. 2. Consideraciones para la definición de la política para la seguridad de la información. 3. Roles, responsabilidades y autoridades de la organización frente a la definición del SGSI.
4. Planificación	Definir y evaluar los riesgos asociados al SGSI, y evaluar los objetivos de seguridad de la información con sus respectivos planes para alcanzarlos.	1. Consideraciones sobre riesgos 2. Planificación del tratamiento de riesgos y oportunidades 3. Definición de objetivos de la seguridad de la información 4. Planificación para lograr los objetivos de la seguridad de la información
5. Soporte	Identificar los recursos necesarios para la definición e implementación de un Sistema de Gestión de Seguridad de la Información.	1. Recursos necesarios 2. Competencia 3. Toma de conciencia 4. Comunicación 5. Información documentada 6. Recomendaciones para el control de la información.

Módulo	Descripción del trabajo	Competencias requeridas
6. Operación	Realizar la evaluación, planificación, implementación y control de todos los procesos involucrados en el logro de los objetivos del SGSI	1. Planificación y control operacional. 2. Valoración de riesgos de la seguridad de la información. 3. Tratamiento de riesgos de la seguridad de la información.
7. Evaluación de desempeño	Identificar y evaluar las acciones que contribuyan a la mejora continua del SGSI.	1. Seguimiento, medición, análisis y evaluación del SGSI. 2. Auditoría interna 3. Revisión por la alta dirección
8. Mejora	Identificar y evaluar las acciones que contribuyan a la mejora continua del SGSI	1. Las No conformidades y acciones correctivas. 2. La Mejora continua del Sistema de Gestión de Seguridad de la Información.
Anexo A	Identificar y entender los objetivos de control y controles enumerados en el Anexo A, y como se deben usar en contexto con el numeral 6.1 (Tratar Riesgos y Oportunidades)	1. A.5 Políticas de la seguridad de la información 2. A.6 Organización de la Seguridad de la información 3. A.7 Seguridad de los Recursos Humanos 4. A.8 Gestión de Activos 5. A.9 Control de Acceso 6. A.10 Criptografía 7. A.11 Seguridad Física y del Entorno 8. A.12 Seguridad de las operaciones 9. A.13 Seguridad de las Comunicaciones 10. A.14 Adquisición, desarrollo y mantenimiento de Sistemas 11. A.15 Relaciones con los proveedores 12. A.16 Gestión de incidentes de seguridad de la información 13. A.17 Aspectos de Seguridad de la información de la Gestión de Continuidad de negocio 14. A.18 Cumplimiento

Módulo	Descripción del trabajo	Competencias requeridas
9. Directrices para la auditoría. (Siguiendo los lineamientos de la norma ISO 19011 norma, para llevar a cabo la auditoría de un sistema de gestión)	• Definir, implementar, revisar y mejorar el programa de auditoría. • Preparar y divulgar el plan de auditorías. • Coordinar y realizar la reunión de Apertura • Elaborar las los reportes de Hallazgos. • Realizar entrevistas a los dueños y participantes de los procesos. • Clasificar los hallazgos de auditoria. • Elaborar el informe final de auditoría. • Coordinar y realizar la reunión de cierre. • Determinar y evaluar las competencias requeridas por un auditor.	**Gestión de un programa de auditoría** Entender claramente las consideraciones y los lineamientos de la norma para llevar a cabo la auditoría: 1. Principios de auditoría 2. Definición de los objetivos del programa de auditoría 3. Definición del programa de auditoría 4. Implementación del programa de auditoría 5. Seguimiento del programa de auditoría 6. Revisión y mejora del programa de auditoría **Realizar la auditoría** Comprende las fases para la realización de una auditoría interna: 1. Inicio de la auditoría 2. Preparación de las actividades de auditoría 3. Realización de las actividades de auditoría 4. Preparación y distribución del informe de auditoría 5. Finalización de la auditoría 6. Realización de las actividades de seguimiento de la auditoría **Competencia y evaluación de un auditor** Comprender la importancia de evaluar y mantener la competencia del auditor: 1. Determinar la competencia del auditor. 2. Establecer los criterios de evaluación del auditor 3. Selección del método de evaluación del auditor 4. Realización de la evaluación del auditor 5. Mantenimiento y mejora de la competencia del auditor.

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)
Dominar los conceptos básicos y el contexto de la norma ISO 27001:2013.	X	
Entender la importancia de comprender el contexto de la organización antes de poner en marcha una iniciativa de definición del SGSI.	X	X
Comprender la importancia del liderazgo y el involucramiento de la alta dirección de la organización, para crear un entorno de compromiso frente a la definición del SGSI .	X	
Comprender las consideraciones para llevar a cabo la planificación de la gestión de riesgos y de los objetivos del SGSI.	X	
Comprender las consideraciones y aspectos que son necesarios para la definición, implementación, mantenimiento y mejora del SGSI.	X	X

Competencia	Preguntas (1)	Caso de estudio (2)
Comprender la importancia de implementar y controlar los planes definidos para lograr los objetivos de seguridad de la información	X	X
Comprender cómo evaluar el desempeño de la seguridad de la información y la efectividad del SGSI, mediante la auditoría interna y la revisión de la alta dirección.	X	
Comprender la responsabilidad de la organización frente al mejoramiento continuo de la seguridad de la información, a partir de los hallazgos de auditoría, el seguimiento y la revisión por la alta dirección	X	
Identificar y entender los objetivos de control y controles enumerados en el Anexo A, y como se deben usar en contexto con el numeral 6.1 (Tratar Riesgos y Oportunidades)	X	
Entender claramente las consideraciones y los lineamientos de la norma para llevar a cabo la auditoría	X	X
Comprende las fases para la realización de una auditoría interna	X	X
Comprender la importancia de evaluar y mantener la competencia del auditor	X	X
Identificar y entender los objetivos de control y controles enumerados en el Anexo A, y como se deben usar en contexto con el numeral 6.1 (Tratar Riesgos y Oportunidades)	X	

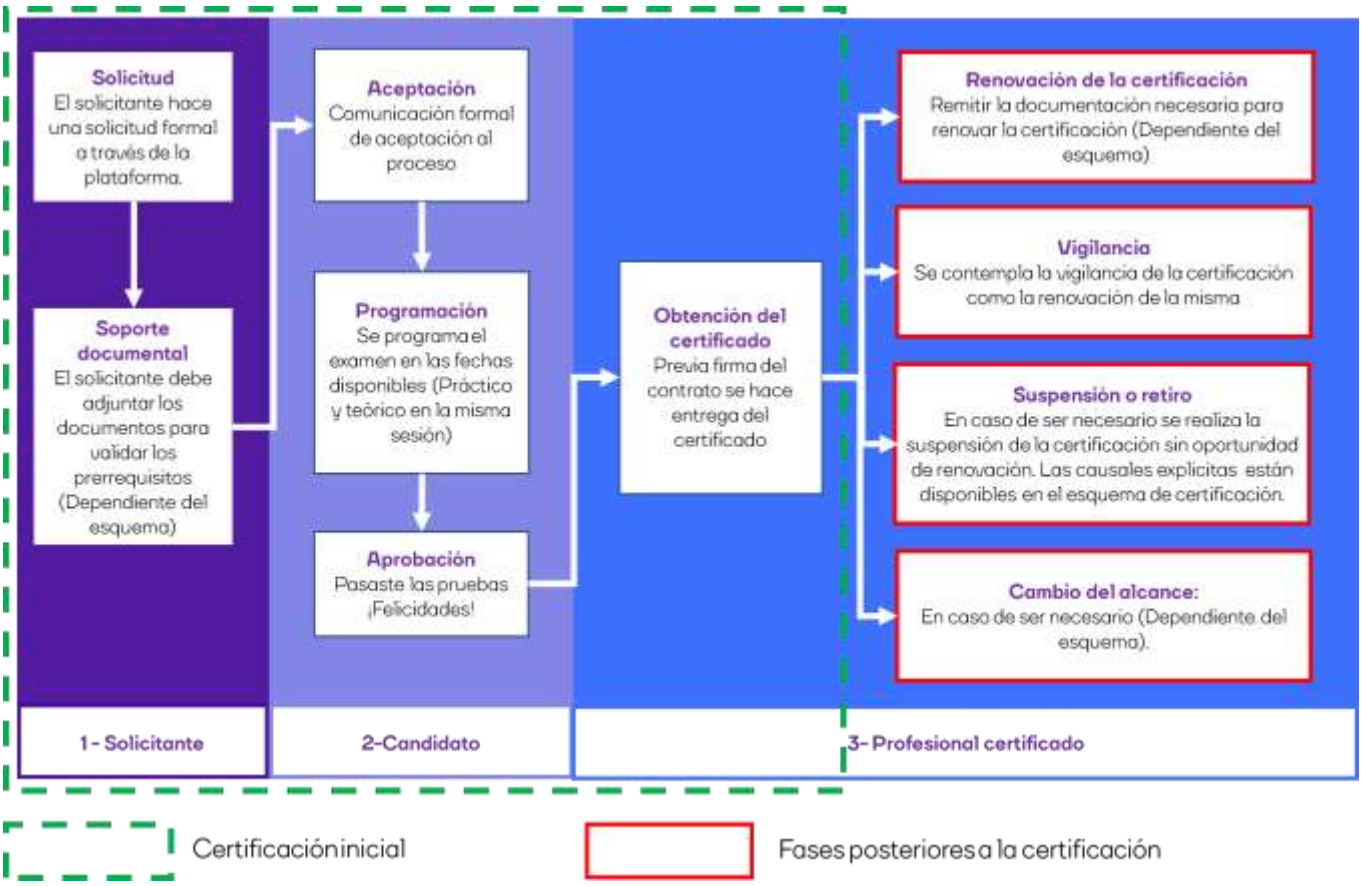
¿Quién debería tomar este examen?

Este examen es ideal para personas o equipos interesados en auditoría interna de seguridad de la información según la norma ISO 27001, o relacionados con un Sistema de Gestión de Seguridad de la Información (SGSI).

Roles como: Oficiales de seguridad de la información, administradores de redes, ingenieros de soporte, auditores, analistas de riesgos en sistemas de información.

Proceso de certificación

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



Proceso de 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 (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.
2. No cumplir con los requisitos del esquema.
3. Resultados insatisfactorios del proceso de vigilancia.
4. Incapacidad para cumplir de forma continuada los requisitos de competencia del esquema.

Cambios al esquema de certificación

El esquema de certificación ISO 27001 – Auditor Interno no contempla cambios en el alcance pues actualmente no aplican ampliaciones o reducciones en el alcance o nivel de la misma.

certm:nd

www.certmind.org

b2b@certmind.org – partner@certmind.org