

Versión 1.0

Última actualización: 15 de Junio del 2022

certm:nd

 Syllabus

Cybersecurity

Essentials

www.certmind.org

2022



Contenido

• Descripción del Esquema	3
• Competencias requeridas y descripción del trabajo	4
• Evaluación de las competencias	5
• ¿Quién debería tomar este examen?	6
• Proceso de certificación	7
• Niveles de dificultad: Taxonomía de Bloom	8
• Renovación, vigilancia y retiro de la certificación	9

Cybersecurity Essentials

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: Security management

Subcategoría: Information security



Alcance de la certificación

El propósito de la Certificación en Cybersecurity Essentials es garantizar que el profesional tiene una comprensión práctica de los conceptos básicos, terminología, análisis de la seguridad de la información, las políticas y la normatividad de la ciberseguridad.

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 Cybersecurity Essentials de mínimo 12 horas, segmentado en 4 sesiones de 3 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:

Módulo	Descripción del trabajo	Competencias requeridas
1. Cimientos de la ciberseguridad	Entender el contexto tecnológico y de seguridad, la importancia de la triada cibernética, los requerimientos complementarios y descubrirás el concepto y aplicación de la ingeniería social.	<ol style="list-style-type: none">1. Definición e importancia2. Conceptos básicos3. Triada4. Requerimientos5. Hablemos de privacidad6. Ingeniería social
2. Análisis de la seguridad de la información	Identificar el propósito, la importancia, los actores involucrados y la manera en que se puede evaluar el análisis de vulnerabilidades, comprendiendo los controles de seguridad en las organizaciones; además aprenderás los tipos de cifrado y su funcionalidad y el proceso para realizar el análisis de riesgos.	<ol style="list-style-type: none">1. Análisis de vulnerabilidades2. Controles de seguridad generales3. Criptografía4. Gestión del riesgo
3. Políticas y normatividad	Comprender las políticas de seguridad y los aspectos fundamentales de las mismas, conociendo las normas internacionales más importantes sobre la protección y tratamiento de la información y el sistema de seguridad de la información basado en ISO 27001.	<ol style="list-style-type: none">1. Políticas de seguridad de la información2. Normatividad internacional

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)
Entender el contexto tecnológico y de seguridad, la importancia de la triada cibernética, los requerimientos complementarios y descubrirás el concepto y aplicación de la ingeniería social.	X	
Identificar el propósito, la importancia, los actores involucrados y la manera en que se puede evaluar el análisis de vulnerabilidades, comprendiendo los controles de seguridad en las organizaciones; además aprenderás los tipos de cifrado y su funcionalidad y el proceso para realizar el análisis de riesgos.	X	X
Comprender las políticas de seguridad y los aspectos fundamentales de las mismas, conociendo las normas internacionales más importantes sobre la protección y tratamiento de la información y el sistema de seguridad de la información basado en ISO 27001.	X	

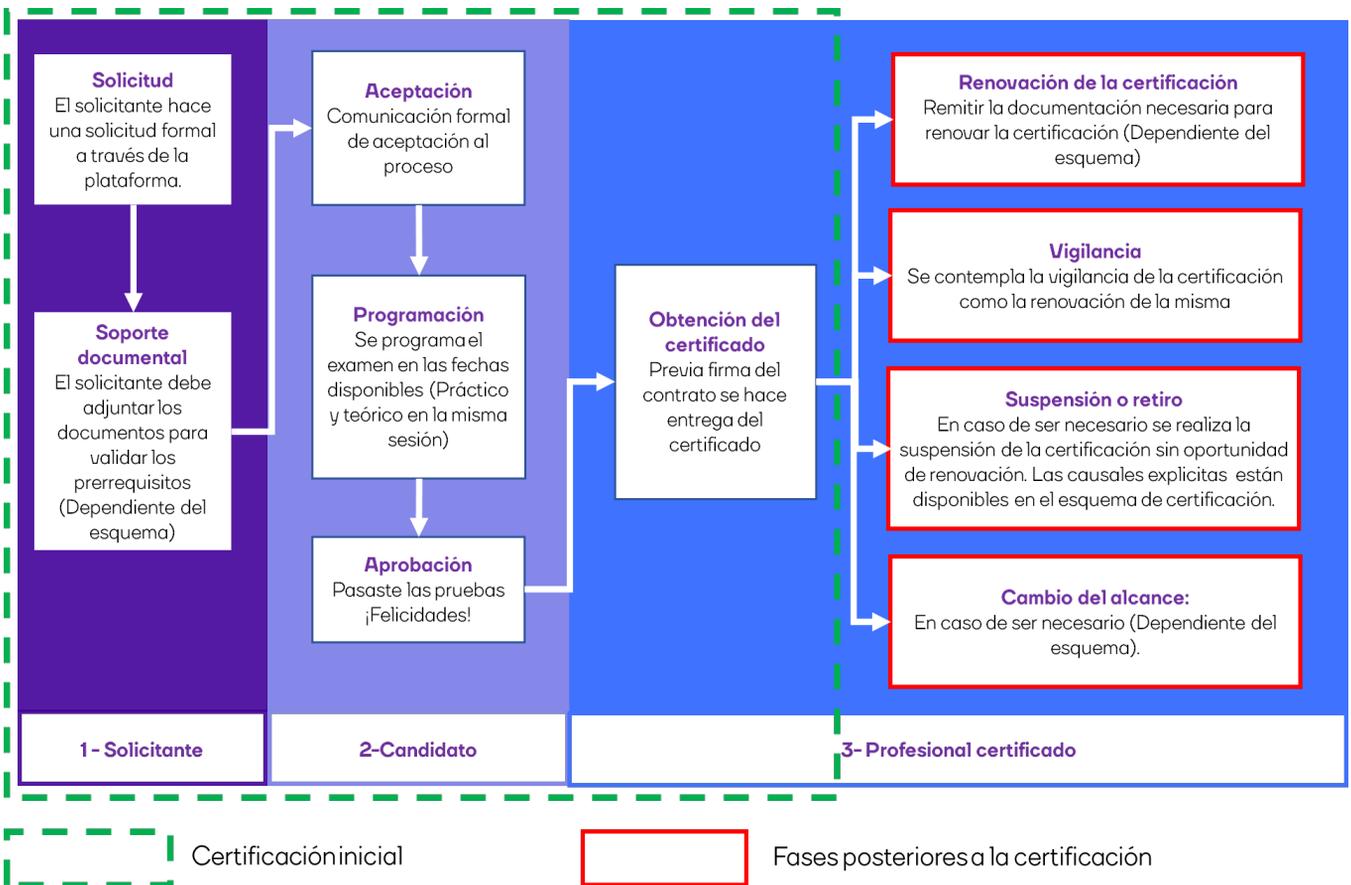
¿Quién debería tomar este examen?

Este examen es ideal para todas las personas y equipos involucrados o familiarizados con las herramientas y los dispositivos de computo de una organización.

Roles como: Gerentes, analistas, líderes, especialistas, emprendedores, personal del área de T.I, ingenieros de software, desarrolladores de aplicaciones y productos, arquitectos de T.I, analistas de negocio, desarrolladores e integradores de sistemas, entre otros.

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 25 preguntas, opción múltiple y única respuesta.
- **Duración:** 60 minutos.
- **Nota mínima para aprobar:** 18/25 o 72%.
- **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	40%	40%	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 necesitan 12 PUC's (Professional Update Credits) 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 Cybersecurity Essentials 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

CertMind is a registered trademark of CertMind - Netherlands