

PECB · CERTIFICACIÓN PROFESIONAL

VERSIÓN 2023

ISO/IEC 27032:2023
Gerente Líder en Ciberseguridad

Programa de certificación acreditado según ISO/IEC 17024

Desarrolle las competencias para implementar, gestionar y mejorar un programa de ciberseguridad basado en ISO/IEC 27032 y el Marco de Ciberseguridad del NIST

¿Por qué debería asistir?

Las amenazas cibernéticas evolucionan cada día y las organizaciones necesitan profesionales capaces de dirigir un programa de ciberseguridad sólido. Este curso oficial de PECB le brinda los conceptos, estrategias, métodos y técnicas para iniciar, gobernar, operar y mejorar un programa de ciberseguridad, gestionar los riesgos cibernéticos y fortalecer la resiliencia de su organización.

El curso lo imparte un instructor certificado PECB Titanium de Savant Consultores, PECB Authorized Gold Partner, y combina la teoría con ejercicios prácticos, un caso de estudio y cuestionarios similares al examen.

Al finalizar podrá presentar el examen y optar por la credencial **Gerente Líder en Ciberseguridad Certificado PECB ISO/IEC 27032**.

5 días	7	31	Prácticos	Líder
DURACIÓN	DOMINIOS	CRÉDITOS CPD	EJERCICIOS Y CASOS	NIVEL



¿Quién debería participar?

Líderes de ciberseguridad
Gerentes y responsables de ciberseguridad que dirigen o desarrollan el programa de ciberseguridad de la organización.

Profesionales de TI y seguridad
Personas que implementan estrategias y medidas de ciberseguridad y buscan avanzar en su carrera.

Riesgo y cumplimiento
Profesionales responsables de gestionar los riesgos cibernéticos y el cumplimiento, y consultores del área.

Alta dirección
Ejecutivos que participan en la toma de decisiones de ciberseguridad, continuidad del negocio e incidentes.

Objetivos de aprendizaje

- Explicar los conceptos, estrategias, métodos y técnicas para implementar y gestionar un programa de ciberseguridad
- Explicar la relación entre ISO/IEC 27032, el Marco de Ciberseguridad del NIST y otras normas y marcos de referencia
- Iniciar el programa de ciberseguridad y establecer su gobernanza
- Definir los roles y las responsabilidades, y gestionar los riesgos de ciberseguridad
- Seleccionar los controles de ciberseguridad adecuados según los riesgos identificados
- Establecer programas de comunicación, concienciación y formación en ciberseguridad
- Integrar el programa con la gestión de incidentes y la continuidad del negocio
- Medir el desempeño del programa de ciberseguridad y mejorarlo de forma continua

Áreas de habilidad del programa

Conceptos de ciberseguridad | ISO/IEC 27032 y NIST CSF | Gobernanza de la ciberseguridad | Roles y responsabilidades | Gestión de activos | Gestión de riesgos cibernéticos | Mecanismos de ataque | Controles de ciberseguridad | Concienciación y formación | Continuidad del negocio | Gestión de incidentes | Métricas y mejora continua

Programa del curso

Duración: 5 días

Modalidades de formación

- **Presencial** — En aula, con instructor
- **Online** — En vivo, con instructor
- **Híbrida** — Aula y online combinadas

Módulo	Contenido
Día 1 **Módulo 1** Dominios 1 y 2	**Introducción a la ciberseguridad e inicio de la implementación del programa** ▶ Objetivos y estructura del curso ▶ Normas y marcos regulatorios ▶ Conceptos fundamentales de ciberseguridad ▶ Programa de ciberseguridad ▶ Contexto de la organización ▶ Gobernanza de la ciberseguridad
Día 2 **Módulo 2** Dominio 3	**Roles y responsabilidades, gestión de riesgos y mecanismos de ataque** ▶ Roles y responsabilidades en ciberseguridad ▶ Gestión de activos ▶ Gestión de riesgos de ciberseguridad ▶ Mecanismos de ataque
Día 3 **Módulo 3** Dominios 4 y 5	**Controles de ciberseguridad, comunicación, concienciación y formación** ▶ Controles de ciberseguridad ▶ Comunicación en ciberseguridad ▶ Programas de concienciación y formación
Día 4 **Módulo 4** Dominios 6 y 7	**Gestión de incidentes, monitoreo y mejora continua** ▶ Preparación de las TIC para la continuidad del negocio ▶ Gestión de incidentes de ciberseguridad ▶ Pruebas de ciberseguridad ▶ Medición del desempeño y métricas ▶ Mejora continua ▶ Cierre del curso
Día 5 **Examen** Dominios 1 al 7	**Examen de certificación** ▶ Examen PECB ISO/IEC 27032 Gerente Líder en Ciberseguridad ▶ 80 preguntas de opción múltiple ▶ 3 horas de duración, a libro abierto ▶ Costos del examen y de la certificación incluidos

El programa cubre los 7 dominios de competencia del examen con ejercicios prácticos y un caso de estudio. Los detalles del examen están en la página 4.

Examen y certificación

Duración: 3 horas

Título	Gerente Líder en Ciberseguridad Certificado PECB ISO/IEC 27032 – Versión 2023
Preguntas	80
Formato	Opción múltiple, con escenarios
Modalidad	Libro abierto
Duración	3 horas
Aprobación	70 %
Idioma	Español, inglés y otros idiomas
Plataforma	PECB Exams (en línea, con supervisión remota)

Requisitos de elegibilidad

- **Gerente Líder en Ciberseguridad:** cinco años de experiencia profesional (dos en ciberseguridad) y 300 horas en actividades de ciberseguridad.
- **Gerente Provisional en Ciberseguridad:** sin experiencia previa; podrá ascender de nivel al acumular la experiencia, sin repetir el curso.
- **Gerente en Ciberseguridad / Gerente Líder Sénior en Ciberseguridad:** 2 años y 200 horas, o 10 años y 1,000 horas, respectivamente.
- Todos los niveles requieren aprobar el examen y firmar el Código de Ética de PECB.

Ruta profesional en ciberseguridad

Quien aprueba el examen sin la experiencia requerida obtiene el nivel Provisional. El Gerente Líder en Ciberseguridad le permite dirigir un programa de ciberseguridad; con más experiencia puede avanzar al nivel Sénior y, sumando otras credenciales de ciberseguridad de PECB, optar por el nivel Máster.



Información general

- Más de 400 páginas de material oficial de PECB y constancia de 31 créditos CPD
- Instructor certificado PECB Titanium; Savant Consultores es PECB Authorized Gold Partner
- Examen y certificación incluidos; reintento gratuito dentro de los 12 meses siguientes