



**I-SEC Education Center Presenta el curso:**

## **Programa Gerente Certificado de Seguridad de la Información (CISM)**

### **Descripción**

El programa de certificación CISM (Certified Information Security Manager), está orientado a profesionales que buscan obtener una visión integral de la gestión, diseño, supervisión y evaluación de la seguridad de la información de las organizaciones. En sus dos años de existencia, se han certificado a más de 5.000 profesionales en todo el mundo, estando específicamente orientada a gestores de seguridad de la información con experiencia y a aquellos profesionales con responsabilidades diversas en dicha área.

### **Objetivos**

La certificación está diseñada para garantizar a las organizaciones que los responsables del área de seguridad de la información poseen el conocimiento y experiencia adecuados a la importancia del puesto de trabajo.

El objetivo principal de este programa de formación es preparar al alumno para que supere con éxito el examen CISM. Para ello se analizará en profundidad el contenido de los cinco dominios de conocimiento en que se divide la materia, con el doble objetivo de dotar al alumno de los conocimientos necesarios en cada uno de ellos y de familiarizarle con las peculiaridades de la certificación, siempre manteniendo un enfoque centrado en la superación de la prueba de examen.

### **A Quien va Dirigido**

Profesionales del sector de las TI, interesados o con responsabilidad en el campo de la gestión de la seguridad de la información.

- Responsables o gerentes de sistemas de información.
- Consultores y asesores en TI de empresas y administraciones públicas.
- En general, toda persona interesada en adquirir los conocimientos técnicos relacionados con la seguridad de los sistemas de información y su repercusión en el negocio de las organizaciones, y que desee obtener el certificado CISM.

### **Programa**

El programa incluye la preparación exhaustiva del alumno en cada uno de los cinco dominios de conocimiento exigidos para superar el examen CISM:

- Gobierno de la Seguridad de la Información
- Gestión del Riesgo
- Gestión del Programa de Seguridad de la Información
- Gestión de la Seguridad de la Información
- Gestión de la Respuesta ante Incidentes

Las sesiones de preparación constan de un repaso exhaustivo de los conceptos teóricos requeridos en cada dominio y del estudio de preguntas tipo test similares a las del examen.

La documentación que se entrega al alumno incluye material de apoyo, documentos complementarios (artículos y whitepapers adicionales de cada uno de los dominios del examen).



## **Certificado**

Además del certificado CISM que el alumno podrá obtener si supera el examen correspondiente, I-SEC Education Center expedirá un certificado acreditativo de su participación en el programa.

Duración  
30 horas

## **V. TEMARIO**

### **1. Estrategia de la Seguridad de información**

El profesional establece y mantiene un marco para proporcionar aseguramiento que las estrategias de la seguridad de la información están alineadas con los objetivos de negocio y sean compatibles con las leyes y regulaciones aplicables.

En este dominio se abordan los siguientes temas:

- Introducción a la gobernabilidad de la seguridad de la información.
- La estrategia de la seguridad de la información.
- Compromiso de la gerencia.
- Roles y responsabilidades.
- Canales de comunicación.
- Aspectos normativos.
- Políticas de seguridad de información.
- Procedimientos y lineamientos.
- Análisis de valor.

### **2. Administración de riesgos**

El profesional debe identificar y administrar los riesgos de la seguridad de la información para alcanzar objetivos de negocio.

En este dominio se abordan los siguientes temas:

- 2.1 Introducción a la administración de los riesgos.
- 2.2 El proceso de administración de riesgos.
- 2.3 Gestión de riesgos en el ciclo de vida de los procesos
- 2.4 Identificación de riesgos y métodos de análisis de riesgos.
- 2.5 Mitigación del riesgo.
- 2.6 Informe sobre cambios significativos en el riesgo.



### **3. Administración del programa de seguridad de la información**

El profesional desarrolla y administra un programa de la seguridad de la información para poner el marco de la gobernabilidad a la seguridad de la información.

En este dominio se abordan los siguientes temas:

- 3.1 Introducción a la administración del programa de seguridad de la información.
- 3.2 Creando y manteniendo los planes.
- 3.3 Líneas de base para la seguridad de la información.
- 3.4 Procesos de negocio.
- 3.5 Actividades de infraestructura de TI.
- 3.6 Actividades de ciclo de vida.
- 3.7 Impacto en los usuarios finales.
- 3.8 Responsabilidad.
- 3.9 Métricas.
- 3.10 Recursos internos y externos para la seguridad de la información.

### **4. Administración de la seguridad de la información**

El profesional programa y ordena actividades de la seguridad de la información para ejecutar el programa de la seguridad de la información.

En este dominio se abordan los siguientes temas:

- 4.1 Introducción a la administración de la seguridad de la información.
- 4.2 Reglas de utilización para los sistemas de información.
- 4.3 Procedimientos administrativos para los sistemas de información.
- 4.4 Proveedores.
- 4.5 Uso de métricas para medir, monitorear e informar.
- 4.6 Procesos de administración de cambios.
- 4.7 Evaluación de vulnerabilidades.
- 4.8 Aspectos relativos al no cumplimiento.
- 4.9 Cultura, comportamiento y capacitación sobre la seguridad de información.

### **5. Administración de la respuesta**

El profesional desarrolla y administra una capacidad para responder y para recuperarse de acontecimientos inesperados y destructivos a la seguridad de la información.

En este dominio se abordan los siguientes temas:

- 5.1 Introducción a la administración de respuesta.
- 5.2 Procesos para detectar, identificar y analizar aspectos relacionados a la seguridad.
- 5.3 Desarrollo de planes de recuperación y respuesta.
- 5.4 Prueba de los planes de recuperación y respuesta.
- 5.5 Ejecución de los planes de recuperación y respuesta.
- 5.6 Procedimientos para documentar un evento.
- 5.7 Revisiones posteriores al evento.