CISM®, Certified Information Security Manager® + Preguntas Prácticas (QAE)

Duración: 4 Días **Código del Curso: CISM** **Método de Impartición: Curso Cerrado (In-Company)**

Temario:

El curso Certified Information Security Manager (CISM) le ayuda a conseguir la certificación CISM. Esta certificación de ISACA es la certificación líder y reconocida internacionalmente para gestores de seguridad de la información con experiencia. Desplácese hacia abajo para obtener más información sobre esta certificación. **Continuing Professional Education (CPE) :** 31**Preguntas Prácticas (QAE = Questions, Answers and Explanations) :** Acceso durante 12 meses

Curso Cerrado (In-Company)

Debido a que nuestra formación es modular, nuestros responsables de formación e instructores pueden trabajar con usted y su equipo para detectar las necesidades formativas y adaptar un temario de forma rápida y rentable. Durante una formación cerrada, usted recibirá una formación de expertos en un curriculum adaptado a sus necesidades.

Dirigido a:

ISACA's Certified Information Security Manager (CISM) certification is for those with technical expertise and experience in IS/IT security and control and wants to make the move from team player to manager. CISM can add credibility and confidence to your interactions with internal and external stakeholders, peers and regulators.
Experienced information security managers and those who have information security management responsibilities, including IT consultants, auditors, managers, security policy writers, privacy officers, information security officers, network administrators, security device administrators, and security engineers.

Objetivos:

- **Módulo 1: Gobierno de seguridad de la informaciónMódulo**
- Describir la función del gobierno en la generación de valor para la empresa.
- Explicar la importancia del gobierno de la seguridad de la información en el contexto del
- gobierno general de la empresa.
- Describir la influencia de la dirección, la estructura y la cultura de la empresa en la
- efectividad de una estrategia de la seguridad de la información.
- Identificar los requisitos legales, legales y contractuales que afectan a la empresa.
- Describir los efectos de la estrategia de seguridad de la información en la gestión de
- riesgos de la empresa.
- Evaluar los marcos y las normas comunes que se usan para gobernar un estrategia de
- seguridad de la información.
- Explicar la importancia de las métricas en el desarrollo y la evaluación de la estrategia
- Describir el proceso de definición de una hoja de ruta para el programa de SI.
- Resumir las métricas del programa de SI que se utilizan para hacer el seguimiento e
- informar del progreso a la alta gerencia.
- Explicar cómo gestionar el programa de SI con los controles.
- Crear una estrategia para mejorar el conocimiento y la concienciación sobre el
- programa de seguridad de la información.
- Describir el proceso de integración del programa de seguridad dentro de las
- operaciones de TI y los proveedores externos.
- Comunicar información clave del programa de SI a las partes interesadas pertinentes.
- **Módulo 4: Gestión de incidentes de seguridad de la información**
- Distinguir entre la gestión de incidentes y la respuesta a incidentes
- Resumir los requisitos y procedimientos necesarios para desarrollar un plan de respuesta

- de seguridad de la información
- **Módulo 2: Gestión de riesgos de la seguridad de la información**
- Aplicar las estrategias de evaluación de riesgos para reducir el impacto del riesgo de
- seguridad de la información.
- Evaluar los tipos de amenazas a los que se enfrenta la empresa.
- Explicar cómo las referencias de control de la seguridad afectan al análisis de
- vulnerabilidades y deficiencias de controles.
- Diferenciar entre la aplicación de los diferentes tipos de tratamiento de riesgos desde el
- punto de vista de la seguridad de la información.
- Describir la influencia de la propiedad del riesgo y del control en el programa de
- seguridad de la información.
- Describir el proceso de supervisión y registro del riesgo de seguridad de la información.
- **Módulo 3: Desarrollo y gestión del programa de seguridad de la información**
- Resumir los componentes y los recursos utilizados para elaborar un programa de
- seguridad de la información.
- Distinguir entre las normas y marcos comunes de SI disponibles para elaborar un
- programa de seguridad de la información.
- Explicar cómo alinear las políticas de SI, los procedimientos y las directrices con las
- necesidades de la empresa.
- a incidentes.
- Identificar las técnicas utilizadas para clasificar o categorizar los incidentes.
- Resumir los tipos de funciones y responsabilidades necesarios para tener un equipo
- efectivo de gestión y respuesta a incidentes
- Distinguir entre los tipos de herramientas y tecnologías para la gestión de incidentes
- disponibles en una empresa.
- Describir los procesos y los métodos utilizados para investigar, evaluar y contener un
- incidente.
- Identificar los tipos de comunicaciones y las notificaciones utilizadas para informar a las
- partes interesadas clave de los incidentes y las pruebas.
- Resumir los procedimientos y los procesos utilizados para erradicar incidentes y
- recuperarse de ellos.
- Describir los requisitos y los beneficios de la documentación de eventos.
- Explicar la relación entre impacto sobre el negocio, continuidad y respuesta a incidentes.
- Describir los procesos y los resultados relacionados con la recuperación en caso de
- desastre.
- Explicar el impacto de las métricas y las pruebas al evaluar el plan de respuesta ante
- incidentes

Exámenes y certificación

Las preguntas de práctica (QAE = Preguntas, Respuestas y Explicaciones) están disponibles en línea mediante un bono. El vale forma parte del material del curso. Te permite practicar durante la formación y está disponible hasta 12 meses después de la formación

Para obtener la certificación oficial CISM, debe cumplir los requisitos que se indican a continuación:

aprobar el examen oficial CISM
tener al menos 5 años de experiencia laboral pertinente en al menos dos ámbitos de CISM (o 4 años de experiencia complementados con una formación en HBO+).
El examen CISM se centra en los cuatro dominios definidos por ISACA. El examen real dura 4 horas y consta de 150 preguntas de opción múltiple en inglés. Para más información sobre la certificación, visite: https://www.isaca.org/credentialing/cism

El bono de examen para el examen oficial CISM dejará de estar incluido en el precio del curso a partir de enero de 2023. Puede solicitar este examen como un producto independiente.

Siguientes cursos recomendados:

- GK9840 - CISSP Certification Preparation
- CISAU - CISA, Certified Information Systems Auditor

Contenido:

Módulo 1: Gobierno de seguridad de la informaciónMódulo

Temas de la sesión:

- Descripción general del gobierno de la empresa
- Cultura, estructura, roles y responsabilidades organizativas
- Requisitos legales, normativos y contractuales
- Estrategia de seguridad de la información
- Marcos y normas de gobierno de la información
- Planificación estratégica

Módulo 2: Gestión de riesgos de la seguridad de la información

- Escenarios de riesgos y amenazas
- Análisis de vulnerabilidades y deficiencias de controles
- Evaluación, valoración y análisis del riesgo
- Respuesta al riesgo de la información
- Presentación de informes, comunicación y supervisión de riesgos

Módulo 3: Desarrollo y gestión del programa de seguridad de la información

- Desarrollo de programas y recursos de SI
- Marcos y normas de SI
- Definición de una hoja de ruta para el programa de SI
- Métricas del programa de SI
- Gestión de programas de SI
- Concienciación y formación en SI
- Integración del programa de seguridad en las operaciones de TI
- Comunicaciones del programa, notificación y gestión del rendimiento

Módulo 4: Gestión de incidentes de seguridad de la información

- Descripción general de la gestión y la respuesta a incidentes
- Planes de gestión y respuesta a incidentes
- Clasificación y categorización de incidentes
- Operaciones, herramientas y tecnologías para la gestión de incidentes
- Investigación, evaluación, contención y comunicación de incidentes
- Erradicación, recuperación y revisión de incidentes
- Impacto y continuidad en el negocio
- Planificación de recuperación en caso de desastre
- Formación, pruebas y evaluación

Más información:

Para más información o para reservar tu plaza llámanos al (34) 91 425 06 60

info.cursos@globalknowledge.es

www.globalknowledge.com/es-es/

Global Knowledge Network Spain, C/ Retama 7, 6ª planta, 28045 Madrid