Curso de Preparación para la Certificación CISM

Curso de Preparación para la Certificación CISM

Objetivo del Curso:

Apoyar al candidato a la certificación CISM en el proceso de preparación para aplicar el examen, utilizando el material oficial de la APMG (certificador) para tales efectos, incluyendo ejercicios similares a los del examen real.

Dirigido a:

Profesionales que tienen como objetivo certificar al nivel internacional su conocimiento en el área de Gobierno y Gestión de la Seguridad de la Información.

¿Que incluye el curso?

- Manual CISM.
- Certificado de participación.
- Material de apoyo
- Prácticas de examen.

Prerrequisitos:

- Conocimientos en Seguridad de la Información.
- Experiencia profesional en Seguridad de la Información

Modalidad: Virtual
Sesiones: 19
Fecha: 13,14,15,16,20,21,22,23,27,28,29,30 de octubre y 3,4,5,6,10,11,12 de noviembre 2025 – de lunes a jueves de cada semana una sesión de 2 horas.
Lugar: Plataforma ZOOM
Hora: 7 p.m. a 9 p.m.
Horas CPE´s: 38 horas.

***No incluye:** Examen de Certificación, el participante matricula el examen directamente en la página de ISACA Internacional: https://www.isaca.org/credentialing/cism

Costo de la certificación:
Miembros de ISACA: $575 dólares
No miembros: $760 dólares

Contenido:

17% DOMINIO 1 – GOBERNANZA DE LA SEGURIDAD DE LA INFORMACIÓN

Este dominio le proporcionará una visión completa de la cultura, las regulaciones y la estructura involucradas en la gobernanza empresarial, además de permitirle analizar, planificar y desarrollar estrategias de seguridad de la información. En conjunto, esto afirmará la credibilidad de alto nivel en la gobernanza de la seguridad de la información para las partes interesadas.

A–GOBERNANZA EMPRESARIAL

1. Cultura Organizacional
2. Requisitos legales, reglamentarios y contractuales
3. Estructuras Organizacionales, Roles y Responsabilidades

B–ESTRATEGIA DE SEGURIDAD DE LA INFORMACIÓN

1. Desarrollo de la estrategia de seguridad de la información
2. Marcos y estándares de gobernanza de la información
3. Planificación estratégica (por ejemplo, presupuestos, recursos, caso de negocio)

20% DOMINIO 2 – GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Este dominio le permite analizar e identificar posibles riesgos, amenazas y vulnerabilidades de seguridad de la información, además de brindarle toda la información sobre cómo identificar y contrarrestar los riesgos de seguridad de la información que deberá realizar a nivel de gestión.

A–EVALUACIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

1. Panorama emergente de riesgos y amenazas
2. Análisis de Vulnerabilidades y Deficiencias de Control
3. Evaluación y análisis de riesgos

B–RESPUESTA A LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

1. Tratamiento de Riesgos / Opciones de Respuesta al Riesgo
2. Propiedad de riesgo y control

3. Monitoreo de Riesgos e Informes

33% DOMINIO 3 – PROGRAMA DE SEGURIDAD DE LA INFORMACIÓN

Este dominio cubre los recursos, las clasificaciones de activos y los marcos para la seguridad de la información, además de permitirle administrar programas de seguridad de la información, incluido el control de seguridad, las pruebas, las comunicaciones y la generación de informes e implementación.

A–DESARROLLO DE PROGRAMAS DE SEGURIDAD DE LA INFORMACIÓN

1. Recursos del programa de seguridad de la información (p. ej., personas, herramientas, tecnologías)
2. Identificación y Clasificación de Activos de Información
3. Estándares y marcos de la industria para la seguridad de la información
4. Políticas, Procedimientos y Directrices de Seguridad de la Información
5. Métricas del programa de seguridad de la información

B–GESTIÓN DE PROGRAMAS DE SEGURIDAD DE LA INFORMACIÓN

1. Diseño y selección de controles de seguridad de la información
2. Implementación de control de seguridad de la información e integraciones
3. Pruebas y evaluación de control de seguridad de la información
4. Concienciación y formación en materia de seguridad de la información
5. Gestión de servicios externos (p. ej., proveedores, proveedores, terceros, terceros)
6. Comunicaciones e informes del programa de seguridad de la información

30% DOMINIO 4 – GESTIÓN DE INCIDENCIAS

Este dominio proporciona una formación en profundidad en gestión de riesgos y preparación, incluida la forma de preparar una empresa para responder a los incidentes y guiar la recuperación. El segundo módulo cubre las herramientas, los métodos de evaluación y contención para la gestión de incidentes.

A–PREPARACIÓN PARA LA GESTIÓN DE INCIDENTES

1. Plan de Respuesta a Incidentes
2. Análisis de Impacto en el Negocio (BIA)
3. Plan de Continuidad de Negocio (BCP)
4. Plan de recuperación ante desastres (DRP)
5. Clasificación/Categorización de Incidentes
6. Formación, pruebas y evaluación en gestión de incidentes

B–OPERACIONES DE GESTIÓN DE INCIDENTES

1. Herramientas y técnicas de gestión de incidentes
2. Investigación y evaluación de incidentes
3. Métodos de contención de incidentes
4. Comunicaciones de respuesta a incidentes (p. ej., informes, notificaciones, escalamientos)
5. Erradicación y recuperación de incidentes
6. Prácticas de revisión posterior al incidente

Instructor:

Arnoldo Le Roy Córdoba
CISM, CRISC, CGEIT, COBIT5f, ITILv3f, ISO-27001 e ISO-9001

Ingeniero en Sistemas con una maestría en Administración de Negocios, con más de 25 años de experiencia en las áreas de Gestión de Riesgos, Seguridad de la Información, Gobierno y Gestión de la T.I.C. e Inteligencia Empresarial. Ha desarrollado proyectos como consultor en diferentes industrias en México, Centroamérica y Sur América. Cuenta con las certificaciones CISM, CRISC, CGEIT, COBIT5f, ITILv3f, ISO-27001 e ISO-9001 y **es instructor certificado por APMG** para los cursos relacionados con las prácticas de CISM y CRISC. Actualmente labora para el grupo B-Solutions como Director de Consultoría e Innovación Tecnológica.

Inversión:

Miembros de ISACA: ₡ 390 000 colones
Convenios: ₡ 540 000 colones
Público General: ₡630 000 colones
***Precios incluyen en IVA**

Formas de Pago:

- ✓ Transferencia
- ✓ Depósito a la cuenta
- ✓ Tarjeta de Crédito o Débito.

A nombre de: Asociación Costarricense de Auditores en Informática
Cédula Jurídica: 3-002-045936

Cta. IBAN Colones -BCR CR69015201001013860853
Cta. IBAN Dólares - BCR CR96015201001022338943

Enviar copia del depósito / comprobante transferencia al correo capacitacion@isacacr.org