

Certified Information Security Manager

Curso de preparación para presentar el examen de
certificación **CISM**



**Marzo 2 – Junio 1
2010**

La Certificación CISM.

La Certificación CISM (*Certified Information Security Manager*) esta diseñada para asegurar a la dirección ejecutiva que aquellos que lo obtengan cuentan con el conocimiento y la capacidad requeridas para proporcionar una gerencia y una asesoría efectivas sobre la seguridad de la información. Aun cuando el enfoque central está en la gerencia de la seguridad de la información, todos aquellos profesionales en las tecnologías de información que tengan experiencia en seguridad encontrarán sin duda un valor en CISM.

Los dominios de conocimiento de la certificación CISM están estructurados en cinco capítulos:

- Gobierno de la seguridad de información.
- Administración de riesgos de la información.
- Desarrollo de un programa de seguridad de información.
- Administración del programa de seguridad de información.
- Manejo y respuesta de incidentes.

El examen de conocimientos es uno de los principales requisitos para obtener la certificación y se aplica dos veces al año, una en junio y otra en diciembre.

Tanto la certificación **CISA** (*Certified Information Systems Auditor*) como **CISM** (*Certified Information Security Manager*) cumplen con el estándar internacional que la *American National Institute* (**ANSI**) les acredita bajo la norma **ISO/IEC 17024**.

Este estándar especifica los requerimientos a ser seguidos por las organizaciones que certifican a individuos contra requisitos específicos y se espera que juegue un rol prominente en la facilitación de estandarización global, seguridad pública y protección de consumidores. La acreditación por ANSI, significa que los procedimientos de ISACA cumplen con los requerimientos fundamentales de apertura, balance, consenso y diligencia.

EXAMEN DE PRÁCTICA

Adicionalmente a los ejercicios que se realicen durante las sesiones del curso, se ofrece a los participantes la aplicación de un examen de práctica que recrea de la forma más fidedigna posible, las condiciones reales que se encontrarán el día del examen de certificación. El examen se realizará una semana antes y en las mismas instalaciones del examen oficial, el cual es organizado por Isaca Capítulo México.

Programación del curso:

Capítulos y Temas de estudio	Horas
I. Gobierno de la seguridad de información	12 horas
a. Definición	
b. Objetivos	
c. Tareas	
d. Introducción al gobierno de la seguridad de información	
e. Gobierno eficaz de la seguridad de información	
f. Conceptos de seguridad de información	
g. Gerente de seguridad de información	
h. Alcance y estatutos del gobierno de la seguridad de información	
i. Métricas del gobierno de la seguridad de información	
j. Estrategia de seguridad de información	
k. Desarrollo de una estrategia de seguridad de información	
l. Objetivos de la estrategia de seguridad de información	
m. Determinación del estado actual de la seguridad	
n. Estrategia de seguridad de información	
o. Recursos de la estrategia	
p. Limitaciones a la estrategia	

<ul style="list-style-type: none"> q. Plan de acción para implementar la estrategia r. Implementación del gobierno de seguridad s. Metas intermedias del plan de acción t. Objetivos del programa de seguridad de información 	
II. Administración de Riesgos	8 horas
<ul style="list-style-type: none"> a. Definición b. Objetivo c. Tareas d. Introducción a la administración de riesgos e. Administración eficaz de riesgos de la seguridad de información f. Conceptos de la administración de riesgos de seguridad de información g. Implementación de la administración de riesgos 	
III. Desarrollo de un Programa de Seguridad de Información	16 horas
<ul style="list-style-type: none"> a. Definición b. Objetivo c. Tareas d. Introducción al desarrollo de un programa de seguridad de información e. Desarrollo de un programa eficaz de seguridad de información f. Conceptos del desarrollo del programa de seguridad de información g. Gerente de seguridad de información h. Alcance y estatutos del desarrollo de un programa de seguridad de información i. Objetivos del desarrollo de un programa de seguridad de información j. Definición de una directriz para el desarrollo de un programa de seguridad de la información 	

<ul style="list-style-type: none"> k. Recursos del programa de seguridad de información l. Implementación de un programa de seguridad de información m. Infraestructura de la información n. Controles físicos y ambientales o. Integración del programa de seguridad de información p. Métricas del desarrollo de un programa de seguridad de información 	
IV. Gerencia de la Seguridad de la Información	12 horas
<ul style="list-style-type: none"> a. Definición b. Objetivo c. Tareas d. Introducción a la gerencia de la seguridad de información e. Roles y responsabilidades organizacionales f. Componentes de un programa para la gerencia de la seguridad de información g. Medición del éxito de la gerencia de la seguridad de información h. Retos comunes de la gerencia de la seguridad de información i. Determinar el estado de la gerencia de la seguridad de información j. Recursos del programa de la gerencia de la seguridad de información k. Otras consideraciones de la gerencia de la seguridad de información l. Implementación de la gerencia de la seguridad de información <p>Implementación de la gerencia de la seguridad de información</p>	
V. Manejo y Respuesta de Incidentes	16 horas
<ul style="list-style-type: none"> a. Definición 	

- b. Objetivo
- c. Tareas
- d. Introducción al manejo de incidentes
- e. Conceptos del manejo de incidentes
- f. Alcance y cédula de manejo de incidentes
- g. Gerente de seguridad de información
- h. Objetivos del manejo de incidentes
- i. Métricas del manejo de incidentes
- j. Definición de los procedimientos del manejo de incidentes
- k. Recursos del manejo de incidentes
- l. Estado actual de la capacidad de respuesta a incidentes
- m. Desarrollo de un plan de respuesta a incidentes
- n. Desarrollo de planes de respuesta y recuperación
- o. Pruebas a los planes de respuesta y recuperación
- p. Ejecución de los planes de respuesta y recuperación
- q. Documentación de eventos
- r. Revisiones posteriores al incidente

Currícula de los Expositores

Gustavo Adolfo Solís Montes

El Sr. Solís es Licenciado en Contaduría con especialidad en finanzas, egresando de la Universidad Nacional Autónoma de México. Obtuvo el grado de Maestría en Sistemas de Información del Instituto Tecnológico y de Estudios Superiores de Monterrey. Actualmente se encuentra cursando el programa de Doctorado en Administración de la Universidad Nacional Autónoma de México.

Cuenta con las siguientes certificaciones:

- *CISA (Certified Information Systems Auditor) 1987.*
- *CISM (Certified Information Security Manager) 2004.*
- *ITIL (Foundation Certificate in IT Service Management) 2005.*
- *COBIT (Accredited Trainer for COBIT) 2005.*
- *CGETI (Certified in the Governance of Enterprise IT) 2009.*

Sr. Solís laboró en la Firma de Ernst & Young, de 1980 a 1996, tanto en la Ciudad de México como en la oficina de Nueva York, llegando a la Sociedad de dicha Firma en el año de 1992. En agosto de 1997 El Sr. Solís fundó Grupo Cynthus.

El Sr. Solís fue miembro titular del Comité de Auditoría de BANSEFI.

Actualmente es el Presidente del Capítulo de la Ciudad de México de la ISACA, cargo que ocupará en el período 2010-2011. En cuanto a su participación en la ISACA internacional, ésta ha incluido los siguientes puestos, entre otros:

- *Vicepresidente Internacional de ISACA*
- *Vicepresidente Regional para Latino América*
- *Miembro del IT Governance Committee.*
- *Miembro del IT Assurance Strategy Committee.*

Es autor del libro "Reingeniería de la Auditoría Informática" de Editorial Trillas y Coautor del libro "Seguridad de las Tecnologías de la Información" publicado por AENOR, España.

Israel Pichardo Camargo, CISA, CISSP

El Sr. Pichardo, es egresado de la Unidad Profesional Interdisciplinaria de Ingeniería y Ciencias Sociales (UPIICSA) del Instituto Politécnico Nacional donde cursó la carrera de Licenciatura en Informática. Cuenta con más de 15 años de experiencia profesional en el área de Tecnología de Información, de los cuales 11 ha dedicado al área de auditoría de sistemas tanto en empresas públicas como privadas.

En 1993 como líder de proyecto, desarrollo y coordinó la implantación del sistema de nóminas para las entidades foráneas de las Suprema Corte de Justicia de la Nación.

De 1994 a 1999, el Sr. Pichardo fungió como Supervisor de Auditoría de Sistemas de Información para la compañía Integradora de Servicios Operativos, teniendo como cliente al Servicio de Administración Tributaria. Como parte de los proyectos especiales en los que participó, se incluye la personalización de cuentas en el sistema aduanero y el desarrollo del área de auditoría forense.

En 2000, participó en el proyecto de Y2K liderando la etapa de certificación de los sistemas desarrollados por el Servicio de Administración Tributaria, así como de sus bases de datos.

El Sr. Israel Pichardo, actualmente ocupa la Gerencia de Auditoría de Sistemas para México y Brazil, en una compañía transnacional, donde fundó el área ha sido encargado de la realización de proyectos de auditoría en los negocios financieros de España, Inglaterra, USA, Suiza y Chile.

Estudios y Certificaciones:

- *Licenciado en Ciencias de la Informática - UPIICSA*
- *CISA, Certificado como Auditor en Sistemas de Información desde el 2002*
- *CISSP Certificado como Profesional en Seguridad en Sistemas.*

Diplomas de Postgrado

- *Consultoría aplicada a la administración de Tecnología de Información en la Universidad Iberoamericana (UIA)*
- *Seguridad Informática por el Instituto Tecnológico y de Estudios Superiores de Monterrey (ITESM)*
- *Comercio Electrónico en el Instituto Tecnológico Autónomo de México (ITAM)*
- *Administración de Proyecto en el Instituto Tecnológico Autónomo de México. (ITAM)*
- *Administración Estratégica por la Universidad Nacional Autónoma de México (UNAM)*

Jose Alfredo Torres Solano, MCC CISA OPST

Lic. en Informática por la Unidad Profesional Interdisciplinaria de Ingeniería y Ciencias Sociales y Administrativas (UPIICSA) perteneciente al Instituto Politécnico Nacional (IPN) y Maestría en Ciencias de la Computación por la Fundación Arturo Rosenblueth. Cuenta con más de 20 años de experiencia en las áreas de Desarrollo de Sistemas, Redes y Seguridad de TI. Trabajó durante diecisiete años para Banco de México (Banco Central), colaborando en los proyectos de Transferencia Electrónica Interbancaria y Transición Año 2000, entre otros. Actualmente es Socio Director de TECNINFO firma dedicada a la consultoría y capacitación en temas relacionados con la TI. De 1997 al 2004, impartió cátedra en la Fundación Arturo Rosenblueth en las maestrías de Ciencias de la Computación y Sistemas de Información en la especialidad de redes. Desde 2003 es profesor en el Instituto Tecnológico y de Estudios Superiores de Monterrey (ITESM) Campus Ciudad de México para las carreras de Ingeniería en Sistemas Computacionales (ISC), Licenciatura en Sistemas y Cómputo Administrativo (LSCA) y Licenciatura en Administración de la TI (LATI). Desde 2003 ha participado en talleres para la certificación CISA_{MR} impartidos a despachos, empresas y la Función Pública del Gobierno Federal. Ostenta la certificación CISA_{MR} desde 2002 y OPST_{MR} desde el 2004. Se desempeñó como Tesorero de ISACA_{TM} Capítulo México de (2003-2005).

Alexandro Fernández Rodríguez, CISSP, CISA

El Sr. Fernández es Licenciado en Informática Administrativa de la Universidad LatinoAmericana, siendo distinguido con el Diploma de alumno Meritorio.

Cuenta con un Diplomado en Telecomunicaciones.

Posee la Certificación CISA otorgado por la ISACA y la certificación CISSP que otorga ISC2.

En la empresa Avantel, se ha desarrollado profesionalmente como Auditor de Tecnología realizando auditorías internas de procesos y riesgos, revisiones tecnológicas a proveedores externos, además de coordinar auditorías con externos. También es Business Recovery Coordinator, donde es el responsable de coordinar los planes de continuidad, supervisar los planes, revisarlos y aprobarlos, desde el análisis de impacto al negocio y análisis de aplicaciones hasta los planes de contención de recuperación. Además coordina y ejecuta las pruebas anuales de sitio alterno en México, Guadalajara y Monterrey.

El Sr. Fernández se desempeña como Oficial de Seguridad de la Información, donde es el responsable de la implementación, revisión y seguimiento al cumplimiento de las Políticas Tecnológicas a través de Implementar el Programa de Concientización, el Programa de Seguridad de la Información, realizar evaluaciones de Seguridad, validar cumplimiento de estándares de seguridad para todas las Aplicaciones, los Sistemas y procesos de la empresa Avantel.

*En Wal*Mart fué Security Officer de Infraestructura, siendo el responsable de mantener y vigilar la confidencialidad, integridad y disponibilidad de la infraestructura del Grupo. Es el encargado de crear, actualizar y depurar las Políticas, Procedimientos y estándares para el uso y asignación de servicios.*

Actualmente es el Coordinador de Políticas y Lineamientos , responsable de mantener y vigilar la confidencialidad e integridad de Grupo Modelo, a través de establecer políticas, estándares, procedimientos, el programa de concientización, Controles de Cobit (SOX Compliance) y Administración de Riesgo Operativo.

Jorge Alejandro Luna Contreras, CISM, CISA, ISO/IEC 27001:2005 LA

El Sr. Jorge Alejandro Luna, es Licenciado en Informática Administrativa egresado de la Universidad Tecnológica de México. Cuenta con las certificaciones:

- *Certified Information Security Manager (CISM),*
- *Certified Information Systems Auditor (CISA),*
- *ISO/IEC 27001: 2005 Lead Auditor.*

Actualmente es especialista en gobierno de seguridad de la información, análisis de riesgos de seguridad de la información, auditoría en seguridad para las plataformas SAP, People Soft, T24, auditor de procesos de negocio y tecnológicos de clientes tanto en el sector público como privado. Líder en el establecimiento e implementación del estándar en seguridad de la información ISO/IEC 27001:2005 y su código de prácticas ISO/IEC 17799:2005.

Consultor pionero a nivel Latinoamérica en el establecimiento e implementación del estándar británico para la administración de la continuidad del negocio BS 25999 – 2 y BS 25999 – 1 laborando para la empresa Cerberian Consulting de 2006 a la fecha.

También es instructor certificado en el estándar de seguridad de la información ISO/IEC 27001:2005 para el British Standards Institution México en las ciudades de Monterrey y CD México, impartiendo los cursos de Implementación ISO/IEC 27001:2005 y Fundamentos ISO/IEC 27001:2005.

Durante 2005 y 2006, el Sr. Jorge Alejandro Luna trabajó para Moore Sthepens como Auditor SOX, siendo especialista en revisiones a diferentes áreas de tecnologías de información con el fin de establecer el cumplimiento con la regulación Sarbanes Oxley (SOX) así como de evaluaciones a procesos, tecnología, personas y gobierno en organizaciones públicas o privadas a través del modelo de control informático COBIT (Control Objectives For Information And Related Technology). Especialista en el establecimiento e implementación del modelo de control informático COBIT en sus versiones 3.2, 4.0 y 4.1.

Gerardo Mendoza Polo, CISM

El Sr. Mendoza es Ingeniero en Cibernética y en Sistemas Computacionales por la Universidad La Salle, colaborando desde el 2002 con esa misma institución como el responsable de la estrategia e implementación de la seguridad informática. Además, el Sr. Mendoza ha sido responsable de conducir auditorías informáticas a los procesos y sistemas de operación del departamento de T.I. de dicha institución.

El Sr. Mendoza obtuvo en 2004 y 2005 la aprobación de los exámenes correspondientes a las certificaciones CISM (Certified Information Systems Manager) y CISA (Certified Information Systems Auditor) emitidas por la ISACA (Information Systems Audit and Control Association).

Durante el período comprendido entre el año 2000 y 2003 el Sr. Mendoza se desempeñó como consultor en el diseño y administración de soluciones empresariales e infraestructura bajo ambientes UNIX, incluyendo los mecanismos, prácticas y herramientas de seguridad correspondientes.

El Sr. Mendoza ha impartido talleres de Administración de Sistemas Operativos en la carrera de Cibernética y Sistemas Computacionales de la Universidad La Salle.

Información General del Seminario

SEDE

Grupo Cynthus, S.A. de C.V.
W. T. C. México
Montecito No. 38 Col. Nápoles. C.P. 03810
Teléfono: 9000-5222

DURACIÓN, FECHAS Y HORARIO

El curso tendrá una duración de 64 horas, iniciando el 2 de Marzo y concluyendo el 1 de Junio de 2010.
Las sesiones se realizarán 3 sesiones en jueves del mes de marzo y todos los martes de 18:00 a 22:00 hrs.:

Marzo: 2, 4, 9, 11, 16, 18 y 23
Abril: 6, 13, 20 y 27
Mayo: 4, 11, 18 y 25
Junio: 1

INVERSIÓN TOTAL

Seminario \$ 16,500.00 + IVA por participante

MATERIAL

- Manual de preparación al examen CISM 2010 de ISACA.
- Carpeta con las presentaciones de los Expositores

POLÍTICA DE CANCELACIÓN

- No habrá cancelaciones de inscripción, solamente serán aceptadas sustituciones.
- Nos reservamos el derecho de cancelación en caso de no tener inscritos a más de 6 participantes antes del 20 de febrero de 2010

FORMA DE PAGO:

- **Depósito bancario.-**
Si el depósito es en moneda nacional, favor de hacerlo a nombre de Grupo Cynthus, S.A. de C.V., Banco BANORTE Número de Cta. 680 009 333 Suc. 680 CLABE 07218000680009333-4.
Si el pago es en dólares, favor de hacerlo a BBVA Bancomer, Nombre: Grupo Cynthus, S.A. de C.V. Cuenta: 0132395843 Clabe: 01218000132395843-2. . En ambos casos favor de enviar ficha de la transferencia o depósito.
- **Cheque.-** A nombre de Grupo Cynthus, S.A. de C.V., entregado en las instalaciones de Cynthus.
- **Tarjeta de Crédito.-** Aceptamos todas las tarjetas de crédito excepto American Express.

Favor de entregar el formato adjunto por cada participante

INFORMACIÓN E INSCRIPCIONES

Para mayores informes referentes a este seminario:

Favor de comunicarse a Grupo Cynthus, S. A. de C. V., al teléfono 90 00-52 22 ext 105 con Laura Ruelas.

O por mail a lruelas@cynthus.com.mx o info@cynthus.com.mx

LA INSCRIPCIÓN AL EXAMEN CISM 2010 O EN CUALQUIER FECHA SERA POR CUENTA DEL INTERESADO

Para mayores informes referentes al examen, consulte la página:
<http://www.isaca.org/cisa.htm>

Inscripción al curso de preparación para la certificación para CISA
Fecha: 3 de Febrero al 2 de Junio de 2010

Apellidos

Nombres

Cargo

Empresa

Dirección

Ciudad **CP**

País **Tel./ext.**

e-Mail

Facturación:

Nombre:

Dirección Fiscal:

R.F.C.:
