iTSecurity
INFORMATION SECURITY
EDUCATION CENTER

PROPUESTAS DE FORMACIÓN ACADÉMICA PARA TECNOLOGÍAS DE LA INFORMACIÓN

CURSOS INDIVIDUALES

2016

PROPUESTAS DE FORMACIÓN TECNOLÓGICA

(Precios Individuales) (*)

OFERTA DE CURSOS PARA SEPTIEMBRE Y OCTUBRE 2016

Preparación para Certificación CISA (Auditor de Sistemas)	40 horas	05Sep/04Oct	BsF. 126.000,00
Incluye: (Puede realizarse por módulos)			
El Proceso de Auditoría de Sistemas de Información	8 horas	05Sept	BsF. 32.760,00
El Gobierno y la gestión de Tecnologías de Información	8 horas	13Sept	BsF. 32.760,00
La Adquisición, desarrollo e implementación de SI	8 horas	21Sept	BsF. 32.760,00
La Operaciones, mantenimiento y soporte de SI	8 horas	29Sept	BsF. 32.760,00
La Protección de los activos de información	8 horas	04Oct	BsF. 32.760,00
Preparación para Certificación CISM (Gerente de Seguridad)	40 horas	06Sep/03Oct	BsF. 126.000,00
Incluye: (Puede realizarse por módulos)			
El Gobierno de la Seguridad de la Información	8 horas	06Sept	BsF. 32.760,00
La Gestión de Riesgos de la Información	8 horas	14Sept	BsF. 32.760,00
El Desarrollo del Programa de Seguridad de Información	8 horas	22Sept	BsF. 32.760,00
Implementación y gestión del Programa de S.I.	8 horas	30Sept	BsF. 32.760,00
La Gestión de Incidentes de Seguridad de la Información	8 horas	03Oct	BsF. 32.760,00
Preparación Certificación CRISC (Control de Riesgos & SI)	40 horas	10Sept/08Oct	BsF. 126.000,00
Incluye: (Puede realizarse por módulos)			
Identificación, valoración y evaluación de riesgos	8 horas	10Sept	BsF. 32.760,00
Respuesta a los riesgos tecnológicos	8 horas	17Sept	BsF. 32.760,00
Monitoreo de riesgos de Tecnología	8 horas	24Sept	BsF. 32.760,00
Diseño de control e implementación de S.I.	8 horas	01Oct	BsF. 32.760,00
Monitoreo de control y mantenimiento de SI	8 horas	08Oct	BsF. 32.760,00

(*) Todos los precios son en Bs. (Incluyen el IVA)

NOTA: NO SE ACEPTAN CARTAS AVAL, DE COMPROMISO NI ORDENES DE SERVICIO

NOTA: Todos nuestros Instructores cuentan con las mas prestigiosas certificaciones internacionales y acreditaciones nacionales, además de sólida experiencia en cada uno de los campos y especialidades; son Ingenieros, Contadores, Administradores de larga trayectoria y reconocimiento.

Condiciones:

1. Los cursos están sujetos en base a quorum mínimo 5 hasta un máximo de 12 participantes por curso.
2. Los Certificados por módulos son emitidos en digital, firmados en Electrónico y enviados a cada participante
3. Los Certificados de los cursos largos (40 horas) son emitidos impresos y firmados en forma autógrafa
4. Los cursos deben ser solicitados y pagados con anticipación al inicio de cada módulo
5. La reservación debe ser realizada con el pago del 100% del módulo o el 20% del monto del Curso largo (40 horas)
6. Los cursos deben ser confirmados por email con 30 días de anticipación
7. Un curso puede ser re-agendado solo 1 vez. Un curso no dictado por razones ajenas a INACOMP pierde reintegro de la reserva
8. La logística, así como los gastos de alojamiento, traslado y viáticos deben ser cubiertos por el Cliente
9. Todo gasto o daño incurrido en la ejecución del curso de los materiales, equipos e instalaciones deberá ser reembolsado por el Cliente
10. Es responsabilidad del Cliente suministrar todos los datos exactos para la facturación

Formas de Pago: Beneficiario: INACOMP CONSULTORES S.A. RIF. J-31398990-8
Transferencias: Cuenta Corriente en Banco de Venezuela Nro. 0102-0221-38-0000201582

Avenida Urdaneta, Esquina Jesuítas, Torre Bandagro, Piso 7, Oficina 71, Municipio Libertador, Caracas—Venezuela
Email: cursos@inacomp.com.ve www.inacomp.com.ve . Teléfonos: 58 212 8613604 / 212 5374258 / 0412 3328072

iT Security
INFORMATION SECURITY
EDUCATION CENTER

CISA

Curso NO Oficial Solo para Grupos de Auto estudio.

No está relacionado con ningún Capítulo Oficial.

Certificación Internacional en Auditoría de Sistemas de Información

ISACA, CISA, CISM, CGEIT, CRISC and COBIT are trademarks of ISACA registered in the U.S. and around the world

La Certificación de Auditor de Sistemas de Información (CISA®) de ISACA® es actualmente la de mayor reconocimiento profesional a nivel global y adoptada como un símbolo de excelencia. Este curso modular de nuestro programa de formación de especialistas está dirigido al personal clave de las organizaciones, responsables de las gestiones de auditoría, control y aseguramiento de las TIC's, con este curso lograrás

CONTENIDO

El examen CISA se ofrece todos los años y consta de 200 preguntas de selección múltiple que cubren los cinco dominios de práctica profesional creados a partir de los análisis más recientes de las prácticas de Auditoría. Los dominios de práctica y los porcentajes que se encuentran a continuación indican el énfasis de preguntas que aparecerán en el examen.

1 El Proceso de auditoría de sistemas de la información (14 %)

OBJETIVO: Proporcionar servicios de auditoría de acuerdo con los estándares de auditoría de TI para ayudar a la organización a proteger y controlar los sistemas de información.

CONTENIDO:
Administración de la función de Auditoría - estándares y directrices ISACA - Análisis de Riesgo - Controles internos - Ejecución de auditorías - CSA - Cambios emergentes

2 Gobierno y gestión de TI (14 %)

OBJETIVO: Garantizar la operatividad de las estructuras organizativas y de liderazgo necesarias para conseguir los objetivos y apoyar la estrategia de la organización.

CONTENIDO:
Gobierno corporativo - monitoreo y aseguramiento de la gerencia - estrategias - políticas y procedimientos - administración del riesgo - prácticas de gerencia de SI – auditoría del gobierno de TI

3 Adquisición, desarrollo e implementación de sistemas de Información (19 %)

OBJETIVO: Garantizar que las prácticas para adquirir, desarrollar, probar e implementar los sistemas de información cumplen las estrategias y los objetivos de la organización.

CONTENIDO:
Ciclo de vida de sistemas e infraestructuras - gerencia de proyectos - desarrollo y mantenimiento de aplicaciones - estrategias alternativas - prácticas de mejoras - controles de aplicación – auditoría a controles - auditoría del desarrollo, adquisición y mantenimiento

4 Operaciones, mantenimiento y soporte de sistemas de información (23%)

OBJETIVO: Garantizar que las operaciones, el mantenimiento y el soporte de los sistemas de información cumplen las estrategias y los objetivos de la organización.

CONTENIDO:
Entrega y soporte de servicio de TI – Operaciones de los sistemas de información - hardware de sistemas – la arquitectura y software de SI - infraestructura de redes - auditorías de la infraestructura y de las operaciones

5 Protección de los activos de información (30%)

OBJETIVO: Garantizar que las políticas de seguridad, los estándares, los procedimientos y los controles de la organización aseguran la confidencialidad, la integridad y la disponibilidad de los activos de información.

CONTENIDO:
Gestión de la seguridad de la información - diseño, implementación y el monitoreo de controles de seguridad - gestión y respuesta a incidentes - controles de acceso lógico - riesgos y controles en virtualización - herramientas de detección de amenazas y controles - riesgos asociados a internet - seguridad de la infraestructura de la red - auditoría de la administración de la SI - auditoría de la seguridad de la infraestructura de red - pruebas de seguridad - exposiciones y controles ambientales - exposiciones y controles de acceso físico - computación móvil - PKI

Duración: 40 horas **Lugar**: INCOMPANY

Modalidad: 16 Hrs de contenido teórico y 24 Hrs. distribuidas en actividades presenciales, talleres en grupo, seminarios online, videos, simulacros de exámenes, etc.
Actividades Presenciales: de 09:00 am-12:00m y 1:30pm-5:30 pm
Materiales: Resúmenes del Manual CISA para su lectura Online, Guías y lecturas relacionadas con el manual CISA, directrices, estándares, etc.
Recursos: Simulacros de Exámenes en línea, CD's de autoevaluación
Instructores: CISA, CISM, CRISC, CGEIT, ITSM, ISO LA, CISSP
Inscripciones: Todo el año **Calendario**: Ver página WEB

Derecho a Éxámen (*): NO incluido.

Cheque: **INACOMP CONSULTORES S.A. - RIF. J-31398990-8**
Banco de Venezuela: Cuenta Corriente 0102-0221-38-00002011582
(*) El participante deberá gestionarlo en www.isaca.org

Descuentos: INCOMPANY y/o por grupos

http://www.inacomp.com.ve/ve/cisacursovenezuela.pdf

Avenida Urdaneta Esquina Jesuita Torre Bandagro Piso 7 Oficina 71 Caracas-Venezuela
Teléfonos +58212 8613604 +58212 2759171 +58412 3328072
cursos@inacomp.com.ve inacomp.venezuela@gmail.com www.inacomp.com.ve

Inacomp Consultores
Administración Comercio Tecnología
Auditoría de Sistemas y Seguridad de Datos
La gestión de seguridad empresarial empieza y termina aquí.

iT Security
INFORMATION SECURITY
EDUCATION CENTER

CISM

Curso NO Oficial Solo para Grupos de Auto estudio.

No está relacionado con ningún Capítulo Oficial.

Certificación Internacional en Gestión de la Seguridad de la Información

ISACA, CISA, CISM, CGEIT, CRISC and COBIT are trademarks of ISACA registered in the U.S. and around the world

La Certificación en Gestión de Seguridad de la Información (CISM®) es la certificación de ISACA® introducida desde el año 2002 y dirigida específicamente a profesionales experimentados en la Seguridad de la Información. La Certificación CISM® está orientada a la gerencia de riesgos y gestión de seguridad de la información. Los profesionales con experiencia en temas de Seguridad de la Información encontraron en esta Certificación, una herramienta de gran valor para las empresas. , con este curso lograrás obtener la orientación y la formación necesaria para aplicar en los exámenes de Junio y Diciembre.

CONTENIDO

El examen CISM se ofrece todos los años y consta de 200 preguntas de selección múltiple que cubren los cuatro dominios de práctica profesional creados a partir de los análisis más recientes de las prácticas en Seguridad de la Información. Los dominios de práctica y los porcentajes que se encuentran a continuación indican el énfasis de preguntas que aparecerán en el examen.

CONTENIDO:

1 Gobierno de la Seguridad de la Información (24 %)

OBJETIVO: Establecer y mantener un marco para proporcionar un entorno en que las estrategias de la seguridad de la información están alineadas con objetivos de negocio y se mantienen dentro de los parámetros marcados por las leyes y regulaciones aplicables.

CONTENIDO:
Conceptos de Gobierno - métricas - estrategias - estado del arte - recursos - planes de acción

2 Gestión de Riesgos de la Información (33 %)

OBJETIVO: Identificar y gestionar los riesgos de la Seguridad de la Información para alcanzar objetivos de negocio.

CONTENIDO:
Visión y estrategia de la gestión de riesgos - riesgos en la seguridad informática - implementación de la gestión - análisis de brechas - metodologías de evaluación y análisis de riesgos - tiempo objetivo de recuperación - integración con procesos del ciclo de vida - monitoreo y comunicación de riesgos - capacitación y concientización

3 Desarrollo y gestión del Programa de Seguridad de la Información (25 %)

OBJETIVO: Crear y mantener un programa para implementar la estrategia de la Seguridad de la Información.

CONTENIDO:
Gestión del Programa de Seguridad de la Información - Objetivos de un programa de seguridad de la información - marco de gestión - Plan de acción - Infraestructura y arquitectura - controles y contramedidas - métricas y monitoreo

4 Gestión de Incidentes de Seguridad de la Información (18%)

OBJETIVO: Planificar, establecer y administrar la capacidad de detectar, investigar, responder y recuperarse de incidentes de seguridad de la información para minimizar el impacto en el negocio
.

CONTENIDO:
Gestión de Incidentes - respuesta a incidentes - recursos para la gestión - métricas e indicadores de gestión de incidentes - procedimientos de gestión de incidentes

Duración: 40 horas LUGAR: INCOMPANY

Modalidad: 16 Hrs. intensivas y Presenciales, y 24 Hrs. distribuidas en actividades presenciales, talleres en grupo, seminarios online, simulacros de exámenes, etc.
Actividades Presenciales: de 09:00 am-12:00m y 1:30pm-5:30 pm
Materiales: Resúmenes del Manual CISM para su lectura Online, Guías y lecturas relacionadas con el manual CISM, directrices, estándares, etc.
Recursos: Simulacros de Exámenes en línea, CD's de autoevaluación
Instructores: CISM, CISA, CRISC, CGEIT, ITSM, ISO LA, CISSP
Inscripciones: Todo el año **Calendario**: Ver página WEB

Derecho a Éxámen (*): NO incluido.

Cheque: **INACOMP CONSULTORES S.A. - RIF. J-31398990-8**
Banco de Venezuela: Cuenta Corriente 0102-0221-38-00002011582

Descuentos: INCOMPANY y/o por grupos

http://www.inacomp.com.ve/ve/cismcursovenezuela.pdf

Avenida Urdaneta Esquina Jesuita Torre Bandagro Piso 7 Oficina 71 Caracas-Venezuela
Teléfonos +58212 8613604 +58212 2759171 +58412 3328072
cursos@inacomp.com.ve inacomp.venezuela@gmail.com www.inacomp.com.ve

inacomp consultores
Administración Comercio Tecnología
Auditoría de Sistemas y Seguridad de Datos
La gestión de seguridad empresarial empieza y termina aquí.

iTSecurity
INFORMATION SECURITY
EDUCATION CENTER

CRISC

Curso NO Oficial Solo para Grupos de Auto estudio
No está relacionado con ningún Capítulo Oficial

Certificación Internacional en Riesgo Tecnológico

ISACA, CISA, CISM, CGEIT, CRICS and COBIT are trademarks of ISACA registered in the U.S and around the word.

Este curso está diseñado para profesionales de TI, Profesionales de riesgo, Análisis económico, Gerentes de proyecto y Oficiales de Cumplimiento. CRISC se centra en: Identificación, evaluación y la evaluación de Respuesta a los riesgos, y la supervisión de riesgos.

CONTENIDO

El examen CRISC se ofrece todos los años y consta de 200 preguntas de selección múltiple que cubren los cinco dominios de la práctica profesional creados a partir de los análisis más recientes de las prácticas en RIESGO. Cada uno de los dominios de práctica y los porcentajes que se encuentran a continuación indican el énfasis de preguntas que aparecerán en el examen.

1 Identificación, valoración y evaluación de riesgos (31%)

OBJETIVO: Determinar correctamente el riesgo que enfrenta la empresa y formular recomendaciones a la alta dirección sobre cómo mantener eficazmente el riesgo a un nivel aceptable, apoyando la ejecución de una estrategia de gestión del riesgo empresarial.

CONTENIDO:
Clasificación de Riesgos - Factores de Riesgos - Metodologías - Inventario de Activos - Amenazas - Vulnerabilidades - Sensibilización - Criticidad - Valoración - Impacto - Evaluación de Riesgos

2 Respuesta al riesgo (17 %)

OBJETIVO: Desarrollar e implementar respuestas a los riesgos para garantizar que los factores de riesgo y los eventos se tratan de una manera costo-efectiva y de acuerdo con los objetivos de negocio. Asegurando que el riesgo residual esté dentro de los límites de tolerancia al riesgo de la empresa.

CONTENIDO:
Análisis de entornos– Análisis de brechas– medición de desempeño de los controles - Revisión del riesgo - RTO- ALE - SLE - Tratamiento - BIA

3 Monitoreo de riesgos (17 %)

OBJETIVO: Monitoreo de riesgos e información y así poder comunicarlo a las partes interesadas, para garantizar la continua efectividad de la estrategia de la empresa en la gestión de riesgos, (usando extracción de datos, herramientas y técnicas de análisis a un alto nivel, apoyándose en diversas normas, marcos de trabajo y prácticas relacionadas con el monitoreo de los riesgos).

CONTENIDO:
Monitoreo de riegos– Gestión de notificación – medición de desempeño de los controles - Revisión del riesgo

4 Diseño de control e implementación de sistemas de información (17%)

OBJETIVO: Diseñar o supervisar el diseño de los controles para los sistemas de información y que éstos estén alineados con el apetito y la tolerancia al riesgo, definidos por la organización para apoyar los objetivos de negocio.

CONTENIDO:
Técnicas de elicitación, Identificación de roles - Diseño de controles efectivos para prevención - costo Vs beneficio de controles - Niveles mínimos de control

5 Monitoreo de control y mantenimiento de SI (18%)

OBJETIVO: Supervisar y mantener los controles de sistemas de información que aseguren su funcionamiento de manera eficaz y eficiente, verificando que los controles claves están en uso, que la administración proporciona supervisión de las actividades de control, que revisa las actividades y se reporta a las partes interesadas de la efectividad de los controles claves.

CONTENIDO:
Monitoreo de controles- Supervisión de eventos– medición de desempeño de los controles - Revisión del riesgo - Comunicación del riesgo a la gerencia - Capacitación y concientización

Duración: 40 horas **Lugar**: INCOMPANY
Modalidad: 16 Hrs. intensivas y Presenciales, y 24 Hrs. distribuidas en actividades presenciales, talleres en grupo, seminarios online, simulacros de exámenes, etc.
Actividades presenciales: de 09:00 am-12:00m y 1:30pm-5:30 pm
Materiales: Resúmenes del Manual CRISC para su lectura Online, Guías y lecturas relacionadas con el manual CRISC, matrices de análisis y evaluación, etc.
Recursos: Simulacros de Exámenes en línea, CD's de autoevaluación
Instructores: CRISC, CISA, CISM, CGEIT, ITSM, ISO LA, CISSP
Inscripciones: Todo el año **Calendario**: Ver página WEB

Opción a Exámen: No Incluido

Cheque: **INACOMP CONSULTORES S.A. - RIF. J-31398990-8**
Banco de Venezuela: Cuenta Corriente 0102-0221-38-00002011582

Avenida Urdaneta Esquina Jesuita Torre Bandagro Piso 7 Oficina 71 Caracas-Venezuela
Teléfonos +58212 8613604 +58212 2759171 +58412 3328072
cursos@inacomp.com.ve inacomp.venezuela@gmail.com www.inacomp.com.ve

inacomp consultores
Administración Comercio Tecnología
Auditoría de Sistemas y Seguridad de Datos
La gestión de seguridad empresarial empieza y termina aquí.