



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

### **Programa Auditor Certificado de Sistemas de Información (CISA)**

La certificación CISA goza de gran reputación tanto a nivel nacional como internacional, donde existen más de 35.000 profesionales certificados. Actualmente es una certificación de referencia en nuestro País para las empresas auditoras y consultoras, e incluso en numerosos concursos públicos.

#### **Objetivos:**

El objetivo principal de este programa de formación es preparar al alumno para que supere con éxito el examen CISA. Para ello se analizará en profundidad el contenido de los seis 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, y financieros, interesados o con responsabilidad en el campo de la auditoria de sistemas de información.

- Responsables o gerentes de sistemas de información.
- Responsables de organización y calidad de empresas y administraciones Públicas.
- Consultores y asesores en TI de empresas públicas y privadas.
- Auditores contables y financieros y asesores jurídicos, que quieran ampliar conocimientos y adquirir una especialización en la auditoria de sistemas de Información.
- En general, toda persona interesada en adquirir los conocimientos técnicos relacionados con la auditoria de sistemas de información y su repercusión en el negocio de las organizaciones, y que desee obtener el certificado CISA otorgado por ISACA internacional.

#### **Programa:**

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

##### **• Procesos de Auditoria en Sistemas de Información:**

- Estándares de Auditoria de Sistemas
- Practicas y técnicas de auditoria de sistemas
- Técnicas para recopilar la información y preservación de evidencias
- Ciclo de vida de la evidencia
- Análisis de riesgo en el contexto de la auditoria
- Técnicas de planeamiento y gestión de la auditoria
- Técnicas de informes y Comunicación
- Objetivos de control y controles relacionados a sistemas de información.



• **Gobierno en tecnología de la información:**

- Estrategias de TI, Políticas, Procedimientos y estándares para una organización.
- Marco de Gobernabilidad de las TI
- Procesos para el desarrollo, la implantación y el mantenimiento de las estrategias de TI.
- Estrategias y políticas de gerencia.
- Estructura de la organización, roles y responsabilidades, relacionadas con el uso y la administración de TI.
- Estándares y lineamientos de TI generalmente aceptados.
- La arquitectura de TI de la empresa, y sus implicancias en el establecimiento de direcciones estratégicas de largo plazo.
- Metodologías y herramientas para la gestión y administración de riesgos.
- Uso de los marcos de control (COBIT, COSO, 17799)
- Uso de modelos de madurez y mejoramiento de procesos
- Gestión de RRHH de TI

• **Ciclo de vida de los sistemas e infraestructura**

- Beneficios de las practicas gerenciales
- Mecanismos de gobernabilidad del proyecto
- Practicas, herramientas y marco de control para la administración de proyectos.
- Practicas de gestión de riesgos aplicadas a los proyectos.
- Criterios y riesgos para el éxito de los proyectos
- Administración de la configuración y los cambios, respecto al desarrollo y mantenimiento de los sistemas e infraestructura.
- Objetivos de control y técnicas que aseguran la integridad, exactitud, validez y autorización de las transacciones y los datos dentro de las aplicaciones informáticas
- Arquitectura de la empresa en relación a los datos, aplicaciones y tecnologías.
- Practicas de análisis y administración de requerimientos
- Procesos de administración de contratos y adquisiciones
- Metodologías y herramientas de desarrollo, ventajas y debilidades
- Métodos de aseguramiento de calidad
- Gestión de procesos de prueba
- Herramientas, técnicas y procedimientos de conversión de datos
- Procedimientos para dar de baja a sistemas e infraestructura
- Practicas para la certificación, y acreditación de SW y HW
- Evaluaciones post-implementación



• **Entrega y soporte de los servicios de TI**

- Practicas de administración de nivel de servicio
- Mejores practicas en la administración de operaciones
- Procesos, herramientas y técnicas de supervisión de la performance de sistemas
- Funcionalidad del HW y Componentes de RED
- Practicas de administración de la base de datos
- Funcionalidad del Software del Sistema
- Planeamiento de la capacidad y técnicas de monitoreo
- Procesos para manejar cambios programados y de emergencia a los sistemas de producción.
- Practicas de administración de cambios a la infraestructura.
- Administración de incidentes y problemas
- Licencia de SW y Practicas de inventarios

• **Protección de los Activos de Información**

- Técnicas para el diseño, la implantación y el monitoreo de la seguridad.
- Controles de acceso lógico para la identificación, la autenticación.
- Métodos y técnicas de ataque.
- Procesos de monitoreo y de respuesta a incidentes de seguridad
- Dispositivos de red y de seguridad de Internet, protocolos y técnicas
- Sistemas de detección de intrusos y configuración, implementación, operación y mantenimiento de Firewall
- Encriptación
- Llaves publicas y firma digital
- Técnicas y herramientas de detección y control antivirus
- Pruebas de seguridad y herramientas de evaluación
- Sistemas y practicas de seguridad física
- Esquemas de clasificación de datos
- Seguridad de las comunicaciones de voz
- Controles y riesgos asociados al uso de dispositivos portátiles e inalámbricos.

• **Recuperación ante Desastres y Continuidad de Operación**

- Procesos y prácticas de respaldo, almacenamiento, retención y restauración.
- Aspectos legales, contractuales y de seguros relacionados con la continuidad de negocios y recuperación de desastres.
- Practicas de gestión de recursos humanos, con respecto a la continuidad y recuperación de desastres.
- Procedimientos para la activación de los planes de continuidad y recuperación de desastres
- Sitios de procesamiento alternativo y métodos para monitorear los acuerdos contractuales.



Las sesiones de preparación constan de una completa revisión de los conceptos 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 oficial, material de estudio, resúmenes de las guías oficiales para el examen y documentos complementarios (artículos y whitepapers adicionales de cada uno de los dominios del examen preparados por los docentes CISA), todas las preguntas tipo test analizadas durante el programa de preparación.

**Duración:**

- 6 dominios, 5 horas por dominio, 30 horas

**Certificado:**

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