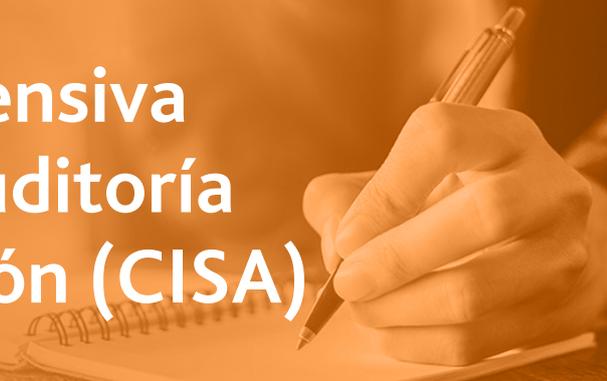


◦ Curso de preparación para certificación

Curso de preparación intensiva para la certificación de auditoría en sistemas de información (CISA)



Duración
12 encuentros de
2 horas c/u (total 24hs)



Plataforma:
Microsoft Teams

Módulos

Dominio 1: Proceso de auditoría de Sistemas de Información

Proporcionar servicios de auditoría de acuerdo con las normas para ayudar a las organizaciones para proteger y controlar los sistemas de información. El Dominio 1 afirma su credibilidad para ofrecer conclusiones sobre el estado de las soluciones de seguridad, riesgo y control de IS/IT de una organización.

A. Planificación

- Normas, directrices y códigos de ética de auditoría de IS
- Procesos de Negocio
- Tipos de controles
- Planificación de auditoría basada en riesgos
- Tipos de auditorías y evaluaciones

B. Ejecución

- Gestión de Proyectos de Auditoría
- Metodología de muestreo
- Técnicas de recolección de evidencia de auditoría
- Análisis de datos
- Técnicas de Reporting y Comunicación
- Aseguramiento de la Calidad y Mejora del Proceso de Auditoría

Dominio 2: Gobernanza y gestión de TI

El dominio 2 confirma a las partes interesadas sus habilidades para identificar problemas críticos y recomendar prácticas específicas de la empresa para apoyar y salvaguardar la gobernanza de la información y las tecnologías relacionadas.

A. Gobierno de TI

- Gobierno de TI y estrategia de TI
- Marcos relacionados con TI

POWERED BY



BDO
Academy

Requisitos:

Cinco (5) o más años de experiencia en auditoría, control, aseguramiento o seguridad de SI/IT. Existen convalidaciones por experiencia disponibles, hasta un máximo de tres (3) años.

Alianza educativa:



Metodología de evaluación:

Se realiza un examen de muestra, con análisis de las preguntas y respuestas más importantes, con el fin de construir y afianzar su confianza y hacer los preparativos finales para el día de la certificación.

- Estructura Organizacional
- Arquitectura empresarial
- Gestión de riesgos empresariales
- Modelos de madurez
- Leyes, Reglamentos y Estándares de la Industria que afectan a la Organización

B. Gestión de TI

- Gestión de recursos de TI
- Adquisición y gestión de proveedores de servicios de TI
- Supervisión y generación de informes sobre el rendimiento de TI
- Aseguramiento de la Calidad y Gestión de la Calidad de TI

Dominio 3: Adquisición, Desarrollo e Implementación de Sistemas de Información

A. Adquisición y desarrollo de sistemas de información

- Gobierno y gestión de proyectos
- Caso de Negocio y Análisis de Factibilidad
- Metodologías de desarrollo de sistemas
- Identificación y diseño de controles

B. Implementación de sistemas de información

- Metodologías de prueba
- Gestión de la configuración y la versión
- Migración de sistemas, implementación de infraestructura y conversión de datos
- Examen posterior a la aplicación

Dominio 4: Operaciones de Sistemas de Información y resiliencia empresarial

Los dominios 3 y 4 ofrecen pruebas no solo de su competencia en controles de TI, sino también de su comprensión de cómo TI se relaciona con el negocio.

A. Operaciones de sistemas de información

- Componentes tecnológicos comunes
- Gestión de activos de TI
- Programación de trabajos y automatización de procesos de producción
- Interfaces del sistema
- Informática para el usuario final
- Gobierno de datos
- Gestión del rendimiento de los sistemas
- Gestión de problemas e incidentes
- Administración de cambios, configuraciones, versiones y parches
- Gestión del nivel de servicio de TI
- Administración de bases de datos

B. Resiliencia empresarial

- Análisis de Impacto en el Negocio (BIA)
- Resiliencia del sistema
- Copia de seguridad, almacenamiento y restauración de datos
- Plan de Continuidad del Negocio (BCP)
- Planes de recuperación ante desastres (DRP)

Dominio 5—Protección de activos de información - (27%)

- Estándares, políticas y procedimientos de TI
- Marcos, estándares y directrices de seguridad de activos de información
- Principios de privacidad
- Acceso físico y controles ambientales
- Gestión de identidades y accesos
- Seguridad de red y punto final
- Clasificación de datos
- Cifrado de datos y técnicas relacionadas con el cifrado
- Infraestructura de clave pública (PKI)
- Técnicas de comunicación basadas en la web
- Entornos virtualizados
- Dispositivos móviles, inalámbricos e Internet de las cosas (IoT)

B. Gestión de eventos de seguridad

- Capacitación y programas de concientización sobre seguridad
- Métodos y técnicas de ataque al sistema de información
- Herramientas y técnicas de pruebas de seguridad
- Herramientas y técnicas de monitoreo de seguridad
- Gestión de respuesta a incidentes
- Recopilación de pruebas y análisis forense

Equipo docente:

Docentes de ISACA certificados