



Programa de Especialización en Auditoría de Sistemas

La Especialización en Auditoría de Sistemas proporciona los conocimientos necesarios para identificar los riesgos y diseñar controles en un ambiente computarizado, realizar la evaluación independiente del sistema de control y liderar el departamento de Auditoría de Sistemas en cualquier tipo de organización.

Es innegable la importancia de la tecnología de información como factor crítico de éxito para las organizaciones. La toma de conciencia en las empresas de los riesgos inherentes a la actividad informática y de la necesidad de protección de altas inversiones que se dedican al diseño e implementación de Sistemas de Información, han permitido el desarrollo de la Auditoría de Sistemas en nuestro medio y ha creado una demanda constante de profesionales idóneos en esta área.

Es la AUDITORÍA DE SISTEMAS la encargada de liderar el montaje y desarrollo de la función de control en los ambientes computarizados, integrar la Auditoría de Sistemas con las demás áreas de la auditoría para contribuir a la modernización y eficiencia de esta función, realizar evaluaciones de riesgos en ambientes de sistemas y diseñar los controles apropiados para disminuir esos riesgos, además de participar en el desarrollo de los Sistemas de información, aportando el elemento de control y evaluar la administración de los recursos de información en cualquier organización.

Objetivo

El objetivo de la Especialización es lograr que sus egresados:

- Adquieran un conocimiento amplio de las metodologías y herramientas necesarias para realizar la auditoría en el campo de la informática.
- Desarrollen las habilidades necesarias para identificar y evaluar situaciones de riesgo propios de la organización y operación de una división de informática.
- Desarrollen la capacidad para participar y dar conceptos en el proceso de planeación estratégica de informática aportando el elemento de control.
- Obtengan el conocimiento necesario para evaluar cualquier tipo de operación y sugerir mejoras para el logro de la eficiencia, la efectividad, la economía y la calidad en los sistemas de información.

Dirigido a

La Especialización de AUDITORÍA DE SISTEMAS está dirigida a Ingenieros de Sistemas, informáticos y afines Auditores internos, Jefes de departamentos vinculados a las áreas de control, auditorios o sistemas.



Perfil del egresado

El egresado de la Especialización de Auditoría de Sistemas al culminar el programa, estará en capacidad de identificar los riesgos inherentes al manejo de la información empresarial, proponer los controles necesarios para manejar dichos riesgos, construir un modelo de seguridad informática, evaluar la administración de los recursos informáticos y gerenciar efectivamente el área de Auditoría de Sistemas.

Plan de estudios

CURSOS	HORAS
Modulo I	
Procesos de Auditoría en Sistemas de Información	10
Gobierno en tecnología de la información	10
COSO y Control Interno	12
Modulo II	
Infraestructura de Tecnología de Información	14
Objetivos de Control en Tecnología de Información COBIT v. 4	18
Modulo III	
Herramientas automatizadas en auditoría - I (Laboratorio)	12
Herramientas automatizadas en auditoría - II (Laboratorio)	12
Auditoría de SGSI	18
Horas Totales	106

Temario Detallado

1. Procesos de Auditoría en Sistemas de Información

- a. Estándares de Auditoría de Sistemas
- b. Prácticas y técnicas de auditoría de sistemas
- c. Técnicas para recopilar la información y preservación de evidencias
- d. Ciclo de vida de la evidencia
- e. Análisis de riesgo en el contexto de la auditoría
- f. Técnicas de planeamiento y gestión de la auditoría
- g. Técnicas de informes y Comunicación
- h. Objetivos de control y controles relacionados a sistemas de información.



2. Gobierno en tecnología de la información

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

3. COSO y Control Interno

- a. INTRODUCCIÓN Y CONCEPTOS GENERALES
 - Marco Conceptual de Control Interno. El informe COSO.
 - Sistema de Control Interno
 - Roles y Responsabilidades
- b. COMPONENTES DEL CONTROL INTERNO
 - Ambiente de Control
 - Evaluación de riesgos
 - Actividades de control
 - Información y Comunicación
 - Supervisión
- c. GESTIÓN DE RIESGOS
 - Análisis conceptual y práctico de la diferente tipología de riesgos: ¿Qué son?, ¿Cómo se gestionan.
 - Los Procesos de Negocios.
 - Elaboración de Mapas de Riesgos

4. Infraestructura de Tecnología de Información

- a. Funcionalidad del Hardware y Componentes de RED.
- b. Enlaces WAN, LAN, Inalámbricos, hardware de comunicaciones.
- c. Firewalls, IDS, IPS, Equipos integrados (Appliances).
- d. Sistemas Operativos de servidores.
- e. Planeamiento de la capacidad y técnicas de monitoreo.
- f. Dispositivos de red y de seguridad de Internet, protocolos y técnicas
- g. Sistemas de detección de intrusos y configuración, implementación, operación y mantenimiento de Firewall.
- h. Encriptación.
- i. Llaves publicas y firma digital.
- j. Técnicas y herramientas de detección y control antivirus.
- k. Procesos, herramientas y técnicas de supervisión de la performance de sistemas.



5. Objetivos de Control en Tecnología de Información COBIT v. 4

- a. Presentación General del COBIT 4,0
- b. Introducción a las Directrices de Auditoría
- c. Planeación y organización
- d. Adquisición e Implementación
- e. Entrega y Soporte
- f. Monitoreo y Evaluación
- g. COBIT Implantación
- h. Taller de Elaboración de Programas de Trabajo COBIT

6. Auditorías de Sistemas de Seguridad de Información (SGSI)

- a. Introducción a la norma ISO 27001
- b. Sistemas de Gestión de Seguridad de Información
- c. Dominios de ISO 27001 y su comparación con ISO 27002
 - ⇒ Metodología de Auditorías
 - ⇒ Análisis de brechas
 - ⇒ Listas de verificación
 - ⇒ Informes de no conformidad
 - ⇒ No conformidad Mayor
 - ⇒ No conformidad Menor
 - ⇒ Caso taller de auditoría de seguridad de información

7. Herramientas automatizadas en auditoría – I

- a. Uso de herramientas CATT (Software de apoyo de auditoría)
 - ⇒ Taller de uso de la herramienta ACL

8. Herramientas automatizadas en auditoría – II

- a. Auditoría de Seguridad en Redes
 - ⇒ Introducción a las Redes y Ataques contra las redes TCP/IP
 - ⇒ Evaluación de Vulnerabilidades
 - ⇒ Herramientas para evaluar la seguridad de redes
 - ⇒ Auditoría básica de enrutadores
 - ⇒ Auditando un Firewall y una DMZ
 - ⇒ Revisión de un Sistema de Detección de Intrusos
 - ⇒ Auditoría de Redes inalámbricas
- b. Auditoría de Seguridad en Aplicaciones
 - ⇒ Auditoría de Aplicaciones cliente/servidor
 - ⇒ Auditoría de Servidores de correo, Web y aplicaciones
 - ⇒ Auditoría de Auditoría en Windows 2000/2003
 - ⇒ Auditoría de base de datos