



Programa de Especialización en Auditoria de Tecnología de Información (IT Audit)

Para las organizaciones en la actualidad, la información y la tecnología que las soportan representan sus más valiosos activos, aunque frecuentemente son poco entendidos. Las organizaciones exitosas reconocen los beneficios de la tecnología de información y la utilizan para impulsar su desarrollo y crear valor. Estas organizaciones también entienden y administran los riesgos asociados, tales como el aumento en requerimientos regulatorios, así como la dependencia crítica de muchos procesos de negocio en TI.

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

La Especialización en Auditoria de Tecnología de Información (IT Audit) proporciona los conocimientos necesarios para identificar las debilidades e incumplimientos de las áreas responsables de su gestión e implantación, para de esta forma proponer, recomendar y diseñar controles, proporcionar recomendaciones de valor y orientadas al negocio que son requeridas por las gerencias y directorio.

Es la Auditoria de Tecnología de Información la encargada de liderar el desarrollo de la función de control en los ambientes tecnológicos, integrar la Auditoria de TI con las demás funciones organizaciones de control.

Objetivo

El objetivo de la Especialización es lograr que sus egresados:

- Adquieran un conocimiento amplio de las metodologías y herramientas necesarias para realizar la auditoria en el campo de la tecnología de información.
- Desarrollen las habilidades necesarias para identificar y evaluar las debilidades propias de la organización gestión y operación del área de TI.
- Desarrollen la capacidad para participar y dar conceptos en el proceso de planeación estratégica de TI 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 en Auditoría de Tecnología de Información (IT Audit) está dirigida a Ingenieros de Sistemas, Ingenieros Informáticos y afines, Auditores Internos, Jefes de departamentos vinculados a las áreas de control, auditorías o sistemas.

Perfil del egresado

El egresado de La Especialización en Auditoría de Tecnología de Información (IT Audit) al culminar el programa, estará en capacidad de identificar las debilidades, riesgos y problemas inherentes a la gestión de la Tecnología de Información, proponer los controles necesarios para mitigar las debilidades, proponer recomendaciones de valor para el negocio y gerenciar efectivamente el área de Auditoría de Sistemas.

Plan de estudios

CURSOS	HORAS
Modulo I	
Procesos de Auditoría en Sistemas de Información	12
COSO y Control Interno	12
Gestión Integral en Riesgos Operaciones y de TI	15
Modulo II	
Infraestructura de Tecnología de Información	12
Objetivos de Control en Tecnología de Información COBIT v. 4	15
Auditoría de SGSI	12
Auditoría Forense Informática	9
Modulo III	
Herramientas automatizadas en auditoría – I (Laboratorio)	12
Herramientas automatizadas en auditoría – II (Laboratorio)	12
Horas Totales	111



Temario Detallado

1. Procesos de Auditoria en Sistemas de Información

- a. Estándares de Auditoria de Sistemas
- b. Practicas y técnicas de auditoria de sistemas
- c. Técnicas de planeamiento y gestión de la auditoria
- d. Técnicas de informes y Comunicación
- e. Objetivos de control y controles relacionados a sistemas de información
- f. El proceso de recolección de evidencias
- g. Listas de verificación
- h. Informes

2. 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



3. Infraestructura de Tecnología de Información

- a. Infraestructura de seguridad Firewalls, IDS, IPS, Equipos integrados (Appliances).
- b. Sistemas Operativos de servidores.
- c. Planeamiento de la capacidad y técnicas de monitoreo.
- d. Dispositivos de red y de seguridad de Internet, protocolos y técnicas
- e. Encriptación.
- f. Llaves publicas y firma digital.
- g. redes privadas virtuales, VPN, y redes inalámbricas, Wireless;
- h. Infraestructura de Virtualizacion
- i. Infraestructura de Storage
- j. Procesos, herramientas y técnicas de supervisión de la performance de sistemas.
- k. Introducción a las Redes y Ataques contra las redes TCP/IP; diversos tipos de ataques.
- l. Consideraciones para auditar la infraestructura de tecnología de Información.

4. Auditoria Forense Informática – Teoría

- a. Conceptos y campos de aplicación
- b. Cadena de custodia
- c. Fases de la auditoria informática
- d. Técnicas usadas
- e. Aspectos técnicos, procedimentales y legales a tener en cuenta.

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

- a. Presentación General del COBIT 4.1
- b. Introducción a las Directrices de Auditoria
- 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. Auditorias 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 Auditorias
 - ⇒ Análisis de brechas
 - ⇒ Listas de verificación
 - ⇒ Informes de no conformidad
 - ⇒ No conformidad Mayor
 - ⇒ No conformidad Menor
 - ⇒ Caso taller de auditoria a la seguridad de información



7. Herramientas automatizadas en auditoria – I

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

8. Herramientas automatizadas en auditoria – II

- a. Auditoria de Sistemas Operativos Windows Server 2003 y 2008
 - ⇒ Log de Auditoria, activación y revisión
 - ⇒ Registro de eventos, activación y reportes
 - ⇒ Auditoria de funcionamiento de las diversas funcionalidades del sistema.
 - ⇒ Técnicas para identificar problemas de configuración
 - ⇒ Uso del Microsoft Baseline Security Analyzer, interpretación de sus resultados.
 - ⇒ Auditoria del directorio activo
 - ⇒ Uso de utilitarios del S.O. para realizar verificaciones y auditoria
- b. Auditoria de sistemas operativos clientes
 - ⇒ Log de auditoría y revisión
 - ⇒ Uso de utilitarios de auditoria