## Misión

Promover la formación humanista y profesional en el área de los negocios, con ética y responsabilidad social, excelencia académica y capacidad de gestión global, mediante la docencia, la investigación y la acción social, para generar los líderes y los cambios que demanda el desarrollo del país.

**Visión**

Ser líderes universitarios en la formación humanista y el desarrollo profesional en la gestión integral de los negocios, para obtener las transformaciones que la sociedad globalizada necesita para el logro del bien común.

**Valores**

* Ética
* Tolerancia
* Solidaridad
* Perseverancia
* Alegría

**Ejes Transversales**

* Emprendedurismo
* Valores y Ética

### CATEDRA DE AUDITORIA INFORMATICA

### PROGRAMA DEL CURSO PC-0526 AUDITORIA INFORMATICA II

# I CICLO, 2016

**Información general:**

**Curso del IX Ciclo del plan de estudios del 2002**

**Requisitos**

 PC-0423: Auditoría Informática I

 PC-0424: Laboratorio de Auditoría Informática I

**Correquisito:** PC-0527: Laboratorio de Auditoría Informática II

**Créditos: 03**

**Horas por semana: 3**

**La Cátedra está compuesta por:**

Grupo 01: MSC Xiomar Delgado Rojas, CISA (Coordinador)

Grupo 02: MSI Roberto Porras León, CISA

Grupo 03: MSI Gino Ramírez Solís, CISA

Sede Regional del Atlántico: MBA César Solano León

Sede Regional de Limón: MBA. Néstor Anderson Salomon

Recinto Santa Cruz: MSC Xiomar Delgado Rojas, CISA

**I. Descripción del curso:**

El curso es teórico-práctico. Implica la exposición magistral de conceptos relacionados con la Auditoría de Tecnologías de Información por parte del profesor, complementado con una dinámica participativa de los estudiantes con base en la lectura previa de material asignado por el docente. Complementariamente, tales conocimientos son puestos en práctica por parte de los estudiantes mediante un trabajo de campo que involucra la ejecución de procedimientos de auditoría básicos que permitan un examen preliminar de áreas específicas relacionadas con el control y la gestión de las TI en una organización.

El curso utiliza ampliamente los conocimientos y técnicas aprendidas en el curso PC-0423 Auditoría Informática I y PC-0424 Laboratorio de Auditoría Informática I.

**II. Objetivo General:**

#### Proporcionar a los estudiantes de la carrera de Contaduría Pública conocimientos generales sobre la Auditoría de Tecnologías de Información, como complemento de los desarrollados en el curso PC-0423; en este caso sobre el Análisis de Riesgos Informáticos, el Ciclo

####

#### de Vida del Desarrollo de Sistemas y la evaluación de Sistemas en Operación. Lo cual se amplía con el estudio de técnicas y herramientas para evaluar las actividades relacionadas con esos temas.

#### III. Objetivos específicos:

#### Lograr que los estudiantes adquieran un dominio razonable sobre los temas indicados en el apartado “Contenido Programático”, mediante clases magistrales, complementadas con dinámicas, ejercicios prácticos, lecturas específicas y la participación motivada de los estudiantes.

#### Practicar el diseño y ejecución de procedimientos de auditoría para la evaluación del control interno aplicado a la gestión de las tecnologías de información en una organización, específicamente en los temas que ocupan este curso; lo cual incluye el estudio y puesta en práctica de técnicas y herramientas, y aspectos metodológicos. Se parte de la premisa de que los estudiantes han adquiridos el conocimiento suficiente sobre gestión de tecnologías y el proceso de auditoría, en cursos anteriores de la carrera.

#### Promover el conocimiento básico sobre el proceso documentación (evidencia- principalmente electrónica y de procesos electrónicos) y comunicación de resultados (informe); aspectos fundamentales para evidenciar el trabajo realizado por el auditor, y lograr que la organización implemente las acciones correctivas sugeridas por el auditor a partir de tales resultados.

**IV. Contenido programático**

# TEMA 1- Auditoría de la gestión de riesgo de TIC

- Principios y marco de los Riegos de TI

- Fundamentos del Gobierno de Riesgo de TI

- Evaluación y respuesta a Riesgos de TI

- Dominios y procesos del marco de riesgos de TI

- Gestión del riesgo en la práctica

- Desarrollo de un caso de estudio y discusión en clase.

**TEMA 2. Auditoría de la Seguridad Informática**

 Seguridad General

Seguridad Física

 .. Protecciones

 .. Ubicación

 .. Construcción

 .. Controles de Ambiente

Seguridad Lógica

 .. Claves de Acceso

 .. Segregación Electrónica de Funciones

 .. Técnicas de Protección

 .. Protección de datos, programas y documentación

Plan de continuidad de operaciones (PCO)

## TEMA 3. Auditoría de la adquisición, desarrollo e implementación de sistemas de información

 Realización del Negocio

 Estructura de la Gerencia de Proyectos

 Prácticas de Gestión de Proyectos

Desarrollo de Aplicaciones de Negocio

Sistemas de Aplicación del Negocio

 Desarrollo de Infraestructura / Prácticas de Adquisición

 Prácticas de Mantenimiento de Sistemas

Auditoría del Desarrollo Adquisición y Mantenimiento de Sistemas

## TEMA 4- Diseño de pistas de auditoría en sistemas automatizados

Propósito de las pistas de auditoría

Necesidad de las pistas de auditoría

Programas para la generación de las pistas de auditoría

Aspectos a considerar en el diseño de pistas de auditoría

Estructura de datos o registro extendido

Pistas de auditoría en las áreas de control de los sistemas de aplicación

Relación de las pistas de auditoría con el ciclo de vida de desarrollo de sistemas (CVDS)

## TEMA 5- Evaluación de sistemas en operación

 Sistemas de Aplicación

 .. En qué consisten

 .. Los cinco ciclos de proceso

Aplicación de Controles en las Diferentes Áreas de los Sistemas

 .. Preparación de Datos

 .. Entrada de Datos

 .. Proceso y Actualización

 .. Salida

 .. Documentación

 .. Respaldo y Recuperación

 .. Programas (Software) de Auditoría

 .. Usuario

## TEMA 6- AUDITORÍA DEL PLAN DE CONTINUIDAD DE TI

 Planeación de la continuidad de negocio SI

 .. En qué consisten

 .. Desastres y otros eventos que pueden causar interrupciones

Proceso de planificación y elementos de un plan de continuidad

 .. Análisis de impacto en el negocio

 .. Clasificación de operaciones

 .. Asignación de responsabilidades

Pruebas del plan

 .. Especificaciones

 .. Documentación y análisis de los resultados

**V. SISTEMA DE EVALUACIÓN Y CRONOGRAMA**

**Sistema de evaluación**

|  |  |  |  |
| --- | --- | --- | --- |
| TIPO DE EVALUACIÓN | CONTENIDO | Porcentaje | FECHA |
| I parcial | Temas 1 y 2 | 20% | 03-05-16 |
| II parcial | Temas 3 al 6 | 20% | 21/06/16 |
| Proyecto auditoría en la empresa (práctica dirigida) | Según esquema adjunto | 25% | 28-06-16 |
| Trabajo de investigación | Según esquema adjunto | 20% | Según fecha establecida |
| Exámenes cortos, tareas y casos | Material revisado y comprobación de lectura | 15% | En cualquier sesión |

\* No se repetirán exámenes cortos.

**Cronograma de actividades**

|  |  |
| --- | --- |
| **FECHA** | **CONTENIDO** |
| 8/03/16 |  Presentación del curso -Análisis del riesgo operativo y de TIC |
| 15/03/16 | Análisis del riesgo operativo de TIC |
| 22/03/16 | Semana Santa |
| 29/03/16 | Análisis del riesgo operativo de TIC |
| 5/04/16 | Auditoría de la Seguridad |
| 12/04/16 | Auditoría de la Seguridad |
| 19/04/16 | Auditoría de la Seguridad |
| 26/04/16 | Semana Universitaria |
| **03/05/16** | **Primer examen parcial** |
| 10/05/16 | Evaluación del Ciclo de Vida y adquisiciones de la infraestructura y sistemas |
| 17/05/16 | Evaluación del Ciclo de Vida y adquisiciones de la infraestructura y sistemas |
| 24/05/16 | Diseño de pistas de auditoría en sistemas automatizados |
| 31/05/16 | Evaluación de sistemas en operación |
| 7/06/16 | Evaluación de sistemas en operación |
| 14/06/16 | Auditoría del Plan de Continuidad de TI |
| **21/06/16** | **Segundo examen parcial** |
| 28/06/16 | Presentación resultado del proyecto de auditoría |
| 05/07/16 | Entrega de promedios |
| **12/07/16** | **Examen de ampliación** |

**VI. METODOLOGÍA**

1. Tres horas semanales para analizar el material teórico relacionado con los temas de estudio.
2. Las clases son de exposición, dictadas por el profesor, complementadas con la participación activa y positiva de los estudiantes y el desarrollo de ejercicios analíticos prácticos.
3. Lectura previa a cada clase, según el tema a tratar, de capítulos específicos en los documentos recomendados y material adicional recomendado por el profesor.
4. Participación de los estudiantes en la clase, sobre los temas analizados.
5. Desarrollo de trabajos prácticos sobre los contenidos del curso, por parte de grupos de alumnos no mayores a 5 integrantes, los cuales deberán exponer los resultados de los temas investigados, en las fechas que se determinan en el programa.
6. Resolución y exposición de casos, con el apoyo de recursos multimedia.
7. Desarrollo de pruebas de campo de auditoría informática, por parte de grupos de estudiantes no mayores a 5 integrantes, relacionadas con los temas de estudio, en una empresa previamente seleccionada y bajo la aprobación de un ejecutivo responsable de ella. El programa de este trabajo se adjunta al final de este documento.
8. Lecturas y actividades complementarias recomendadas por el profesor.

**VII. VALORES Y EJES TRANSVERSALES:**

El curso pretende la promoción de los valores y ejes trasversales establecidos por la Escuela motivando el trabajo ético en la aplicación práctica de campo, en la que el estudiante debe ser tolerante, solidario y perseverante con la empresa que colabora y sus compañeros de grupo, manteniendo en todo momento un espíritu alegre, que le ayude a ser un mejor auditor y alcanzar mayor aceptación por las personas con que interactúa.

Mediante la ejecución de una labor independiente en el trabajo de campo se pretende motivar la posibilidad de emprendedurismo que un futuro Contador Público puede tener en el campo laboral, reforzando siempre los valores y los principios éticos que son fundamentales de esta profesión, fortaleciendo el concepto generalmente aceptado en el Colegio de Contadores Públicos de Costa Rica que indica que esta es la profesión de la ética y la verdad.

**VIII ATENCIÓN A LOS Y LAS ESTUDIANTES**

Se atenderán las consultas, de orden personal, de los estudiantes inmediatamente después de terminadas las lecciones, previa coordinación de los estudiantes que soliciten apoyo, con cada uno de los instructores.

Solo se atenderán aquellas consultas, que por su naturaleza, no puedan ser atendidas durante el período normal de lecciones, y que sean exclusivas de un (a) estudiante o grupo de estudiantes, si son temas que interesan a todos los participantes, se atenderán durante las lecciones.

Si el tiempo de consulta se estima, por parte de los participantes, que pueda ser de larga duración, se ponen de acuerdo con cada instructor para que les asigne la hora y el tiempo en que los pueda atender.

Si los asuntos a tratar son problemas de no poder asistir, de llegadas tardías, o de irse antes de que terminen las lecciones, deben presentar una nota al instructor en donde se justifican estos aspectos.

**IX. PRACTICA DIRIGIDA – Metodología de trabajo**

El objetivo de la práctica dirigida es la ejecución de una auditoría sobre las prácticas relacionadas con alguno de los temas cubiertos en PC-0526 Auditoría Informática I o uno de los temas del 1 al 3 de este curso en la empresa seleccionada por el grupo de estudio, previa presentación al profesor de una propuesta durante la primera semana y su respectiva aprobación de alcance.

1. Formar grupos de trabajo. No más de cinco (5) personas por grupo. No se aceptan trabajos individuales. Estos grupos fueron conformados en el curso anterior, pero si alguna persona no matriculó esta materia o la matrícula los ubicó en otro grupo, pueden sufrir modificaciones.

2. La conformación de los grupos debe ser comunicada al profesor, en la segunda lección.

3. Efectuar la revisión o auditoría, con base en los siguientes aspectos:

- solicitar los documentos según la lista de verificación;

- efectuar la evaluación del control interno;

- realizar las pruebas de cumplimiento;

- llevar a cabo las pruebas sustantivas, si procediere;

- documentar y analizar los hallazgos;

- redactar el informe en borrador;

- discutir el informe en borrador con el auditado; y

- redactar y presentar el informe final.

4. Presentar el informe al auditado y obtener una carta en donde conste esta presentación.

5. Fases a completar en el ANALISIS DE LOS RESULTADOS DE LA AUDITORIA, que serán revisadas por el profesor conforme lo solicite

 - Programa de Trabajo de la Auditoría

 - Documentación y validación

 - Análisis

 - Desarrollo de las recomendaciones

 - Presentación y discusión preliminar

 - Presentación y discusión final

6. Presentar el informe al profesor. Debe ser por escrito, en un documento revisable (NO PDF), en medio magnético o papel según indique el profesor.

**X. TEMAS DE INVESTIGACIÓN – Guía de elaboración grupal**

|  |  |  |  |
| --- | --- | --- | --- |
| **Nº** | **Tema** | **Aspectos básicos a tratar** | **Fecha** |
| 1 | Forma de realizar el análisis de riesgos. | Procedimientos, metodologías empleadas, sectores o áreas en que se aplican, medición, evaluación, documentación de resultados. | 12-abr |
| 2 | Administración y aplicación de la seguridad. | Realizar estudio en varias empresas para determinar el grado de administración y aplicación de la seguridad en general; asignación de responsabilidades, cumplimiento de normativa; políticas y procedimientos. | 10-may |
| 3 | Estudios de Factibilidad de Proyectos de TIC | Revisar y analizar cómo diversas empresas gestionan el tema de los estudios de Factibilidad en los proyectos de TI. Establecer un análisis comparativo e identificar los principales controles aplicados. | 17-may |
| 4 | El control interno en el desarrollo de sistemas | Investigar en al menos tres organizaciones las metodologías de desarrollo o adquisición de sistemas de aplicación a la medida, estableciendo un análisis comparativo de los procedimientos de control | 24-may |
| 5 | Outsourcing de TI | Forma de gestionar el outsourcing de TI en diversas empresas. Razones para la contratación, resultados obtenidos, principales mecanismos de control aplicados. Realizar un análisis comparativo. | 31-may |
| 6 | Seguridad en transacciones electrónicas | Estudiar varias instituciones que ofrezcan este tipo de servicios, así como algunos de sus clientes, para determinar aspectos relativos a la seguridad en las transacciones; problemas que han tenido; cómo los han resuelto, timos o fraudes, protecciones, etc.  | 7-jun |
| 7 | Planes de continuidad de operación en las empresas | Investigar al menos en 3 organizaciones cómo se administran los planes de continuidad de negocio, enfatizando en planes de continuidad de las TIC´s, concluyendo en un análisis comparativo de prácticas y resultados obtenidos. | 14-jun |

* En la portada se debe indicar el porcentaje de participación de cada estudiante en la investigación.
* Cada investigación implica estudio en una o varias empresas.
* Deben tener: introducción, el cuerpo del trabajo, el resultado del estudio y análisis efectuado, y las conclusiones y recomendaciones.
* Debe detallar las fuentes de información (bibliografía y otras) según formato APA.
* Incluir en la portada: tema; número del grupo; participantes; fecha y cualquier otro dato de interés.
* Deben entregar el documento en el formato que el profesor lo solicite.
* Cada grupo dispondrá de un máximo 15 minutos para su exposición.

**XI. BIBLIOGRAFIA**

ISACA 2011 El Debido Cuidado en Seguridad de la Información

ISACA 2007 Inseguridad Informática y Computación Anti-forense: Dos Conceptos Emergentes en Seguridad de la Información

ISACA 2015,

 Manual para la Preparación del Examen CISA

ISACA 2009 Marco de Riesgos de TI (Risk-IT-framework-spanish)

ISACA 2009 - Seguridad Lógica y Seguridad Física: Dos Mundos Convergentes

Muñoz R, C. (2002). Auditoría en sistemas computacionales. (1ª. ed.). México D F, México: Pearson Prentice Hall.

Piattini V, M., Del Peso N, E y Del Peso R, M. (2008). Auditoría de Tecnologías y sistemas de información. (1ª. ed.). México D F, México: Ediciones Alfaomega.

**REFERENCIAS DIGITALES**

1. <http://sibdi.ucr.ac.cr/bibliotecas.htm> ( varios trabajos finales de graduación)
2. [www.**intypedia**.com](http://www.intypedia.com)
3. [www.isaca.org](http://www.isaca.org) – documentos relacionados con los temas de estudio
4. <http://www.isaca.org/About-ISACA/History/Espanol/Documents/11v6-Technology-Risk-Measurement-and-Reporting-spanish.pdf>
5. <http://www.isaca.org/About-ISACA/History/Espanol/Documents/Virtualization-WP-Spanish-4Feb2011.pdf>
6. <http://www.isaca.org/Journal/Past-Issues/2011/Volume-1/Documents/jpdf11v1-how-the-IT-auditor-spanish.pdf>
7. <http://www.verizonenterprise.com/DBIR/2015/>
8. <http://www.verizonenterprise.com/resources/reports/rp_dbir-2014-executive-summary_es_xg.pdf>
9. <http://www.mordecki.com/html/descargarlibro.php> Pensar primero