Misión

Promover la formación humanista y profesional en el área de los negocios, con responsabilidad social, y capacidad de gestión integral, mediante la investigación, la docencia y la acción social, para generar 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

- ✓ Prudencia
- ✓ Tolerancia
- ✓ Solidaridad
- ✓ Integridad
- ✓ Perseverancia
- ✓ Alegría

CATEDRA DE AUDITORÍA

PROGRAMA DEL CURSO PC-0423 AUDITORÍA INFORMÁTICA I

II CICLO, 2012

Información general:

Curso del VIII Ciclo del plan de estudios del 2002
Requisitos: PC-0381 Informática I para Gerencia de Negocios
PC-0422 Normas de Auditoría
Co-requisitos: PC-0424 Laboratorio de Auditoría Informática I
Créditos: 03
Horas por semana: 3 presenciales
4 extra clase
La Cátedra está compuesta por:
Grupo 01: M. Sc. Xiomar Delgado Rojas, Coordinador
Grupo 02: Dr. Sergio Espinoza Guido
Grupo 03: MSI Roberto Porras León
Sede Regional del Atlántico: MBA César Solano León
Sede Regional de Limón: Lic. Néstor Anderson Salomons

I. Descripción del curso:

El curso permite al estudiante adquirir los conceptos, herramientas, técnicas y habilidades básicas para realizar auditorías en Tecnologías de Información y Comunicaciones (TIC's).

II. Objetivo General:

Proporcionar a los estudiantes los conocimientos generales sobre la Auditoría a las Tecnologías de Información y Comunicaciones (TIC's), de las normativas que regulan esta actividad en el país, de las mejores prácticas internacionales, que conozca y aplique a nivel básico herramientas y técnicas para evaluar la gestión y control de las tecnologías de información.

Teléfonos: 2511-9180 / 2511-6482 Fax. 2511-9181
Correo Electrónico: negocios@ucr.ac.cr Página Web: http://www.ean.ucr.ac.cr

III. Objetivos específicos:

- Comprensión de los conceptos básicos relacionados con la auditoría de tecnologías de información y comunicaciones.
- Conocer y manejar los aspectos esenciales de la normativa dictada tanto por organismos locales como internacionales en relación con esta área.
- Conocer los aspectos generales de COBIT, ITIL y otros, como marcos de control y auditoría de las tecnologías de información.
- Conocer en forma básica y aplicar las guías de aseguramiento de la ISACA como una de las herramientas útiles para la evaluación de la gestión y control de las tecnologías de información.
- Obtener destrezas para la aplicación de herramientas para evaluar el cumplimiento de la normativa relacionada con el control y la auditoría de la gestión de TI, apoyándose en el uso de las guías de aseguramiento ISACA.

IV. CONTENIDO PROGRAMÁTICO

TEMA I- CONTROL INTERNO Y AUDITORÍA DE SISTEMAS DE INFORMACIÓN

Tiempo estimado: 1 sesión.

1. Las funciones de control interno y auditoría informáticos
1.1. Control interno informático
1.2. Auditoría informática
1.3. Control interno y auditoría informáticos
2. Sistemas de control interno informático
2.1. Definición y tipos de controles internos
2.2. Implantación de un sistema de control interno informático
3. Ética en Auditoría de Tecnologías de Información
3.1. Código de Ética de ISACA
4. Crimen informático
4.1. Delito Informático
4.2. Tipos de delincuentes informáticos
4.3. Software malicioso (MALWARE)

TEMA II. EL DEPARTAMENTO DE AUDITORÍA DE TECNOLOGÍAS DE INFORMACIÓN: ORGANIZACIÓN Y FUNCIONES.

Tiempo estimado: 2 sesiones.

1. Misión del departamento de Auditoría de Tecnologías de Información
2. Organización del departamento de Auditoría de TI
2.1. Objetivos
2.2. Ubicación en la organización
2.3. Recursos necesarios
2.4. Estructura del departamento de auditoría de TI
2.5. El estatuto de auditoría de las TI
2.6. Referencias sobre la función de auditoría de TI
3. Planificación del trabajo de auditoría de TI

3.1. Definir el universo de TI
3.2. Análisis de riesgos
3.3. Planificación a largo plazo
3.4. Planificación a corto plazo
4. Metodología del trabajo de auditoría de TI
5. El equipo de auditoría de TI

TEMA III. METODOLOGÍA PARA REALIZAR AUDITORÍAS DE SISTEMAS COMPUTACIONALES

Tiempo estimado: 3 sesiones.

1. Marco conceptual de la metodología para realizar auditorías de sistemas computacionales
2. Metodología para realizar auditorías de sistemas computacionales
3. Primera etapa: Planeación de la auditoría de sistemas computacionales
4. Segunda etapa: Ejecución de la auditoría de sistemas computacionales
5. Tercera etapa: Informe de la auditoría de sistemas computacionales

TEMA IV. PANORAMA GENERAL DE GOBIERNO DE TI, COBIT Y PROPUESTAS ASOCIADAS.

Tiempo estimado: 2 sesiones.

1. La ISACA y el ITGI
2. Áreas del Gobierno de TI
3. Diagrama de contenidos de COBIT
4. Interrelación de los componentes de COBIT
5. Misión de COBIT
6. Marco general de COBIT
6.1. La necesidad de un marco de control para el Gobierno de TI
6.2. Principios básicos y componentes de COBIT
6.3. Procesos y controles de COBIT
6.4. El cubo COBIT
6.5. Modelos genéricos de madurez
6.6. Cómo se usa COBIT
6.7. Otros documentos de ISACA relacionados a COBIT

TEMA V. NORMATIVA SOBRE TI EN COSTA RICA

Tiempo estimado: 1 sesión.

1. Normas técnicas para gestión y control de la tecnologías de información, Contraloría General de la República (**N-2-2007-CO-DFOE)**
2. Acuerdo SUGEF 14-09, "Reglamento sobre la Gestión de la Tecnología de Información".

TEMA VI. USO DE LAS GUÍAS DE ASEGURAMIENTO DE LA ISACA

Tiempo estimado: 2 sesiones.

1. Marco de riesgos de TI
2. Objetivos de la Guía y audiencia objetivos
3. Guía de COBIT para las actividades de aseguramiento de TI

4. Componentes de las guías de aseguramiento de TI
5. Enfoque de riesgo en las guías de aseguramiento de TI
6. Relación con las prácticas de control de COBIT
7. Cómo usar las guías de aseguramiento (Un ejemplo práctico)

TEMA VII. AUDITORÍA DE COMPUTACIÓN EN LA NUBE

Tiempo estimado: 1 sesión.

1. Impactos de computación en la nube y la virtualización
2. ¿Qué es computación en la nube?
3. Los beneficios de negocio de la computación en la nube
4. Riesgos y preocupaciones de seguridad relacionados con la computación en la nube
5. Estrategias para tratar riesgos relacionados con la computación en la nube
6. Problemas de gobierno y cambios relacionados con la computación en la nube
7. Consideraciones sobre el aseguramiento en relación con la computación en la nube

TEMA VIII. CONCEPTOS Y ESTRUCTURA DE COBIT 5

Tiempo estimado: 1 sesión.

1. Resumen ejecutivo
2. Los Principios de COBIT 5
3. Habilitadores de COBIT 5
4. El Marco Estructural de COBIT 5

V. SISTEMA DE EVALUACIÓN Y CRONOGRAMA

EXAMEN	CONTENIDO	Porcentaje	FECHA
Primer examen parcial	Temas 1, 2 y 3 del contenido	20%	17/09/12
Segundo examen parcial	Temas 4, 5 6, 7 y 8 del contenido	20%	26/11/12
Proyecto Aplicación de la normativa y mejores prácticas de control de TI	Según esquema adjunto	20%	19/11/12
Trabajos de Investigación	Según esquema adjunto	25%	Según cronograma
Exámenes cortos, lecturas y tareas	Según esquema adjunto	15%	Según cronograma

No se efectuará examen final, la nota final según la estructura de evaluación, será la que obtenga una vez sumados todos los porcentajes; si esa nota es igual o superior a 70 aprueba el curso; se aplica prueba de ampliación a aquellos estudiantes que obtengan una calificación final entre 6,0 y 6,74. El estudiante que

obtenga en la prueba de ampliación una nota de 7,0 o superior, tendrá una nota final de 7,0. (art.26 Reglamento de Régimen Académico Estudiantil).

EXAMEN DE REPOSICIÓN:

Sólo se repondrán exámenes parciales por motivos de fuerza mayor, conforme lo estable el artículo 24 del Reglamento de Régimen Académico Estudiantil en los plazos establecidos en el mismo.

Exámenes cortos no se reponen.

FECHA	ACTIVIDAD
06/08/12	Control interno y auditoría de sistemas de información
13/08/12	El departamento de auditoría de los Sistemas de Información: Organización y funciones
20/08/12	El departamento de auditoría de los Sistemas de Información: Organización y funciones. (Quiz lectura 1)
27/08/12	Metodología para realizar auditorías de sistemas computacionales
03/09/12	Metodología para realizar auditorías de sistemas computacionales
10/09/12	Metodología para realizar auditorías de sistemas computacionales
17/09/12	**Primer examen parcial**
24/09/12	Panorama General de COBIT 4.1 (Quiz lectura 2)
01/10/12	Panorama General de COBIT 4.1 (exposición tema de investigación 2)
8/10/12	Normativa aplicable a TI – Contraloría General de la República y Sugef
15/10/12	**Feriado (corresponde al traslado del 12 de octubre)**
22/10/12	Guías de aseguramiento de ISACA (Quiz lectura 3)
29/10/12	Guías de aseguramiento de ISACA
05/11/12	Auditoría de computación en la nube
12/11/12	Conceptos y estructura de COBIT 5 (exposición tema de investigación 3)
19/11/12	Exposición trabajo de aplicación de la normativa de TI en Costa Rica- Tema Auditoría de la Gestión de TI, apoyándose en el uso de las guías de aseguramiento ISACA.
26/11/12	**Segundo examen parcial**

VI. METODOLOGÍA

a- Lecciones impartidas por el profesor en tres horas lectivas semanales para analizar el material teórico relacionado con los temas de estudio, en clases de exposición dictadas por el profesor, complementadas con la participación activa y positiva de los estudiantes en la que se discutirá sobre la aplicación de la normativa y mejores prácticas en las empresas seleccionadas, producto del análisis de lo investigado por los estudiantes.

b- Es obligatorio que los estudiantes hagan una lectura e investigación previa de los temas a desarrollar en cada lección, que serán sujetas de evaluación corta a criterio del profesor.

c- Para los trabajos grupales se deberán conformar grupos de no más de seis (6) estudiantes ni menos de tres (3), que serán comunicados al profesor a más tardar al inicio de la segunda sesión de clases por el medio que el profesor indique. No se aceptarán trabajos individuales. En la portada de cada trabajo se consignará una matriz en orden alfabético de apellidos, calificando la participación de cada uno de los miembros.

d- Lecturas e investigaciones individuales o grupales asignadas de capítulos de libros, artículos de revistas, noticias de la prensa y otros relacionados con los temas a discutir en clase.

e- Discusión en clase de lo investigado y comparación de lo que plantea la teoría con lo determinado al respecto en la empresa que su grupo de estudio ha elegido como referencia.

f- Todas las tareas y trabajos solicitados, cualquiera que sea su nombre, deberán ser entregados, por escrito (en papel o medio electrónico, según lo determine el profesor), en las fechas que se indiquen, sin excepciones de ninguna naturaleza el profesor NO los solicitará, si no los presentan, tendrán un cero (0) como nota y deberán respetar la estructura propuesta de redacción de ensayo (p. ej. la propuesta en http://www.spanish.fau.edu/gamboa/ensayo.pdf") así como contar con referencia de las fuentes de información utilizadas, respetando el formato APA sexta edición.

g- Trabajo práctico realizado por el estudiante dentro y fuera del aula.

h- Pruebas cortas para evaluar los temas del curso, investigaciones, lecturas asignadas y cualquier otro conocimiento tratado en el curso.

i- Exámenes teóricos para evaluar la comprensión de los conceptos desarrollados durante el curso.

j- Los grupos de alumnos realizarán las investigaciones que se detallan en este documento. Cada grupo deberá investigar sobre cada uno de todos los temas, preparar un resumen de lo investigado y preparará una presentación; ambos documentos deberán ser entregados al profesor en el medio que este indique. Se expondrán los resultados de los temas investigados, según lo determine el profesor en la sesión que corresponde a la exposición.

k- La exposición de las asignaciones que así lo requieran deben realizarse por la totalidad de los integrantes del grupo, el estudiante que no participe perderá el puntaje respectivo. En la calificación de cada uno de los trabajos se evaluarán tanto aspectos de contenido, como de calidad que incluyen redacción y ortografía

l- Cada grupo realizará una práctica de campo: que consiste en evaluar el comportamiento o situación de la empresa de referencia respecto a la normativa relacionada con la auditoría de la gestión de TI y las mejores prácticas, apoyándose en las propuestas planteadas por las organizaciones líderes de referencia como ISACA, el Instituto de Auditores Internos (Global), comisión COSO e ITIL, de la cual deben desarrollar durante el

semestre, un legajo de papeles de trabajo, considerando la aplicación de la normativa de TI en Costa Rica o las mejores prácticas propuestas por el IT Governance Institute en COBIT, y las guías de aseguramiento que le permitan evaluar el cumplimiento del control interno relacionado con la gestión de TI en la empresa, según la regulación a que responda la empresa. El programa de este trabajo se adjunta al final de este documento.

m- No existe un libro base ni antología, pero deben estudiar los temas revisados en clases, en los libros citados en la bibliografía, que los contengan y complementarlo con investigación en otras fuentes.

n- Atención de consultas por parte del profesor o del asistente según horario a convenir entre profesor y estudiantes.

o- Exposiciones de los estudiantes de temas asignados

p- Participación de los estudiantes en charlas y conferencias.

NOTA: El plagio de tareas y otros será sancionado según lo establece la normativa vigente en la Universidad. Podrá utilizarse referencia de material publicado por otro autor, siempre que se haga la respectiva cita de su referencia y no constituya el objetivo principal de investigación o estudio de un tema.

ATENCIÓN A LOS ESTUDIANTES

Se atenderán las consultas de orden personal de los estudiantes previa coordinación con cada uno de los profesores.

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 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 profesor en donde se justifican estos aspectos.

Para que cada grupo disponga de acceso a los documentos disponibles en ISACA, que son material básico de estudio en los diferentes temas, se recomienda que al menos un estudiante de cada grupo se inscriba como miembro estudiantil según las indicaciones que se brindan en www.isaca.org/studentmember

VII. BIBLIOGRAFIA

a) COBIT 4.1 –IT Governance Institute , 2007, Edición en español.

b) Delgado R, Xiomar. (1997). Auditoría informática. (1ª. ed.). San José, Costa Rica: Editorial UNED.

c) Derrien, Y. (1995). Técnicas de la auditoría informática. (1ª. ed.). México D F, México: Ediciones Alfaomega.

d) Echenique G, J. A. (2001). Auditoría en informática. (2ª. ed.). México D F, México: Mc Graw Hill.

e) Espinoza G, Sergio. (2009). Auditoría de aplicaciones informáticas –Factores relevantes. (1ª. ed.). San José, Costa Rica: Editorial U C R.

f) IT Assurance Guide using COBIT ; IT Governance Institute, (Guías de aseguramiento de TI usando Cobit), 2007 (resumen traducido por Prof. Roberto Porras L.)

g) Ley general de Control Interno No. **8292** de 31 de julio del 2002. Publicado en La Gaceta No. 169 de 4 de setiembre del 2002

h) Normas técnicas para la gestión y control de las tecnologías de información. Contraloría General de la República de C. R., 2007.

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

j) Piattini, M, Del Peso, E y Del Peso, M. (2008). Auditoría de tecnologías y sistemas de información. (1ª. ed.). México D F, México: Alfaomega Grupo Editor.

k) Reglamento Sobre La Gestión De La Tecnología De Información Sugef 14-09, Superintendencia General de Entidades Financieras, San José, Costa Rica, 12 de marzo de 2009 y sus modificaciones

l) RISK IT - ISACA (Marco de Riesgo de TI), 2009

m) http://sibdi.ucr.ac.cr/bibliotecas.htm (varios trabajos finales de graduación)

n) *www.**intypedia**.com*

o) www.isaca.org – documentos relacionados con los temas de estudio

p) http://www.isaca.org/About-ISACA/History/Documents/ISACA-Glossary-English-Spanish.pdf

q) http://www.isaca.org/Knowledge-Center/Research/Documents/Guiding-Principles-for-Cloud-Computing-Adoption-and-Use-WP-Spanish.pdf

r) http://www.isaca.org/About-ISACA/History/Korean/Documents/ISACA-Code-of-Ethics-Spanish.pdf

s) http://www.isaca.org/Certification/CISA-Certified-Information-Systems-Auditor/Prepare-for-the-Exam/Documents/2011-2012-CISA-Term-Spanish.pdf

t) http://www.isaca.org/About-ISACA/History/Espanol/Documents/11v6-Technology-Risk-Measurement-and-Reporting-spanish.pdf

u) http://www.isaca.org/About-ISACA/History/Espanol/Documents/Virtualization-WP-Spanish-4Feb2011.pdf

v) http://www.isaca.org/Journal/Past-Issues/2011/Volume-1/Documents/jpdf11v1-how-the-IT-auditor-spanish.pdf

PRÁCTICA DIRIGIDA - TRABAJO A REALIZAR

Objetivo: Evaluar el cumplimiento de la normativa nacional o mejores prácticas relacionada con el control de la gestión de TI aplicables en una empresa.

1. Formar grupos de trabajo de cuatro (3) a seis (6) personas. NO se aceptan trabajos individuales.
2. Seleccionar una empresa en donde realizar el trabajo.
3. Identificar la normativa de TI nacional aplicable (SUGEF o CGR) o las mejores prácticas de control de TIC aplicables a la empresa
4. Seleccionar de la normativa seleccionada, los apartados aplicables a la evaluación de la gestión informática y los temas que se van tratando.
5. Seleccionar los procesos de COBIT 4.1 relacionados con los aparatados anteriores.
6. Identificar las guías de aseguramiento aplicables a los procesos de COBIT 4.1 seleccionados.
7. Aplicar las guías respectivas, recopilar y evaluar los resultados obtenidos.
8. Preparar un informe con los resultados de la evaluación.
9. Fecha límite para realizar consultas sobre este trabajo: 12 de Noviembre del 2012.
10. Fecha de presentación y exposición: 19 – Noviembre – 2012.
11. Presentar los resultados al profesor en un medio físico (papel, empastado), un medio magnético o electrónico, según lo determine cada profesor.

LECTURAS ASIGNADAS

FUENTE DE LECTURA	AUTOR	TEMA	FECHA
Auditoría de aplicaciones Informáticas (Factores relevantes). Primera Edición, 2009. Edit. UCR, San José, Costa Rica	Sergio Espinoza Guido	1. Papeles de trabajo. (de 1.1 a 1.6 inclusive).	20/08/12
Cómo el Auditor de TI Puede Hacer Contribuciones Sustanciales a una Auditoria Financiera	Tommie W. Singleton, ISACA	Todo el documento	3/09/12
COBIT 4.1, 2007	IT Governance Institute	Resumen ejecutivo	24/09/12
Implementación de COBIT 4.0 en Scotibank Costa Rica	Francisco Herrera Hernández y Manuel Vargas Roldán - ISACA	Todo el documento	8/10/12
Guías de Aseguramiento de ISACA (Resumen)	IT Governance Institute	Todo el documento	22/10/12
Virtualización – Beneficios y desafíos	ISACA	Todo el documento	05/11/12
Cobit 5	IT Governance Institute	Resumen ejecutivo	12/11/12

Trabajos a realiza respecto a cada lectura:

1. Estudio individual de cada documento, el cual será objeto de examen corto en la fecha de entrega del resumen.

2. Presentar un resumen por grupo de la lectura en la fecha indicada en la columna de la derecha, incluir los siguientes elementos: portada, introducción; resumen de las ideas principales y relevantes del documento y las conclusiones del grupo respecto a la aplicabilidad e importancia de lo expuesto por el autor a la realidad empresarial costarricense.

3. Los trabajos deben ser bien presentados, en formato físico o electrónico, según lo solicite el profesor y la evaluación considera redacción y ortografía.

4. Anotar en la portada (al externo): título del libro; nombre del autor; nombre y número del capítulo, la fecha de entrega y datos de los estudiantes que participaron con calificación en escala de 0 a 100 de la participación de cada uno.

- **No se revisarán los trabajos, si no cumplen con el formato anterior.**

TEMAS DE INVESTIGACIÓN

Nº	Tema	Aspectos básicos a tratar	Fecha sugerida de exposición[1]
1	Perfil y actividades del ATIC.	Realizar estudio en varias empresas que tengan el departamento o sección de ATIC; cuál fue el perfil de contratación; qué labores realiza; cuál es su preparación académica; a quién le reporta; en qué normativa se apoya, qué importancia le dan en la empresa.	27-8-2012
3	Gobierno de TI.	¿Qué es el gobierno de TI?; ¿Cuál es el marco de referencia que se emplea para la implementación del gobierno de TI?, ¿En qué consiste?; qué están haciendo en las empresas y entidades para su desarrollo; cómo se mide el grado de madurez de una organización con respecto a la implementación del gobierno de TI.	10-10-2011
7.	RISK IT (marco de riesgos de TI)	¿Qué es el RISK IT?; ¿Cuál es el marco de referencia que se emplea para la implementación del RISK IT?, ¿En qué consiste?; qué están haciendo en las empresas y entidades para su desarrollo; cómo se mide el grado de madurez de una organización con respecto a la implementación del RISK IT.	14-11-2011

Este es un trabajo grupal. Todos los grupos desarrollarán los tres trabajos de investigación. Deben tener los siguientes elementos:

- introducción,
- objetivos,
- problema,
- el cuerpo del trabajo,
- el resultado del estudio y análisis efectuado,
- las conclusiones, y
- las recomendaciones (solo si procediere).

[1] Como propuesta se sugiere una fecha de presentación que queda a criterio de cada profesor modificar según haya avanzado en el tratamiento de la materia, haciendo la indicación oportuna a sus estudiantes.

Si se realizó una investigación bibliográfica, incluir la bibliografía, así como las referencias a las citas incluidas.

Incluir en la portada: tema; número del grupo; participantes y su porcentaje de participación; fecha y cualquier otro dato de interés.

El estudio y su respectivo informe deben ser orientados esencialmente identificando implicaciones y aportes del tema objeto de estudio al campo de la auditoría, evitando el planteamiento de aspectos técnicos propios de los cursos de TIC's.

Deberá realizarse una exposición oral del resultado de la investigación, con una duración máxima de 15 minutos, con exposición y preguntas.