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, 2013

Información general:

Curso del VIII Ciclo del plan de estudios del 2002
Requisitos: PC-0381 Informática II 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.

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.

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

- Obtener destrezas para la aplicación de herramientas para evaluar el cumplimiento de la normativa relacionada con gobierno, riesgo y cumplimiento de TIC (GRC).

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
   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. PANORAMA GENERAL DE GOBIERNO DE TI, COBIT, VAL IT E ITIL.

Tiempo estimado: 3 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
   6.8. VAL IT
   6.9. ITIL

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

Tiempo estimado: 1 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 IV. 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 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. GUÍAS DE ASEGURAMIENTO DE ISACA

Tiempo estimado: 3 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)
8. ¿Qué es computación en la nube?
9. Impactos de computación en la nube y la virtualización

10. Riesgos y preocupaciones de seguridad relacionados con la computación en la nube
11. Consideraciones sobre el aseguramiento en relación con la computación en la nube

TEMA VII. 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 3 y 4 del contenido	20%	07/10/13
Segundo examen parcial	Temas 5, 6 y 7 del contenido	20%	18/11/13
Proyecto Aplicación de la normativa y mejores prácticas de control de TI	Según esquema adjunto	20%	25/11/13
Trabajos de Investigación	Según esquema adjunto	25%	Según cronograma
Exámenes cortos y tareas	En todas las sesiones	15%	Según cronograma

EXAMEN DE REPOSICIÓN:

Los exámenes de reposición se realizarán según lo que se establece estable en el artículo 24 del Reglamento de Régimen Académico Estudiantil.

Los exámenes cortos no se reponen, su justificación razonable hace que no se considere en el promedio, la no presentación genera una nota de cero.

FECHA	ACTIVIDAD
12/08/13	Control interno y auditoría de sistemas de información
19/08/13	COBIT 4.1, Gobierno de TI, VAL IT e ITIL
26/08/13	COBIT 4.1, Gobierno de TI, VAL IT e ITIL
02/09/13	COBIT 4.1, Gobierno de TI, VAL IT e ITIL – CASO TIBO
09/09/13	El departamento de auditoría de los Sistemas de Información: Organización y funciones.
16/09/13	Metodología para realizar auditorías de sistemas computacionales
23/09/13	Metodología para realizar auditorías de sistemas computacionales

30/0913	Metodología para realizar auditorías de sistemas computacionales
07/10/13	**Primer examen parcial**
14/10/13	Normativa aplicable a TI – Contraloría General de la República y SUGEF
21/10/13	Guías de aseguramiento de ISACA
28/10/13	Guías de aseguramiento de ISACA
04/11/13	Guías de aseguramiento de ISACA
11/11/13	Conceptos y estructura de COBIT 5
18/11/13	**Segundo examen parcial**
25/11/13	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.
09/12/13	**Examen Extraordinario**

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://datateca.unad.edu.co/contenidos/358016/GUIA_PARA_LA_ESCRITURA_DEL_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, en el horario publicado por el profesor.

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.
2. Seleccionar una empresa en donde realizar el trabajo.
3. El líder de grupo debe comunicar al profesor la conformación de grupo y la empresa seleccionada a más tardar el 19 de agosto en formulario establecido para ese efecto, acompañado de una nota de aceptación de la empresa.
4. Identificar la normativa de TI nacional aplicable (SUGEF o CGR) o las mejores prácticas de control de TIC aplicables a la empresa
5. Seleccionar de la normativa seleccionada, los apartados aplicables a la evaluación de la gestión informática y los temas que se van tratando.
6. Seleccionar los procesos de COBIT 4.1 relacionados con los apartados anteriores.
7. Identificar las guías de aseguramiento aplicables a los procesos de COBIT 4.1 seleccionados.
8. Aplicar las guías respectivas, recopilar y evaluar los resultados obtenidos.
9. Preparar un informe con los resultados de la evaluación.
10. Fecha límite para realizar consultas sobre este trabajo: 19 de agosto del 2013.
11. Entrega del informe final 18 de noviembre de 2013.
12. Fecha de presentación y exposición: 25 de noviembre de 2013.
13. Presentar los resultados al profesor en un medio físico (papel, empastado), un medio magnético o electrónico, según lo determine cada profesor.

TEMAS DE INVESTIGACIÓN

Nº	Tema	Aspectos básicos a tratar	Fecha de exposición
1	Gobierno de TI.	Qué están haciendo en las empresas y entidades para su desarrollo; cómo miden el grado de madurez de una organización con respecto a la implementación del gobierno de TI.	09/09/13
2	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.	23/09/13
3.	RISK IT (marco de riesgos de TI)	¿Qué están haciendo en las empresas y entidades para gestionar el riesgo deTIC?; ¿cómo miden el grado de madurez de la organización con respecto a la implementación del RISK IT?.	04-11-2013

Cada grupo desarrollará los tres trabajos, aplicando investigación comparativa de al menos 3 organizaciones (al menos una presencial y el resto se puede investigar por INTERNET) y

presentará para cada uno de ellos un informe ejecutivo y una presentación digital del resultado. Uno de los grupos será seleccionado para presentar a la clase los resultados de su investigación.

Se debe incluir en la portada: tema; número del grupo; participantes en orden ascendente por apellidos 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 prepararse una exposición oral del resultado de la investigación, con una duración máxima de 15 minutos.

VII. BIBLIOGRAFIA

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

b) COBIT 5 - IT Governance Institute , 2012, Edición en español

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

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

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

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

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

h) IT_Gov_Using_COBIT_and_ValIT_Student_Book_2ndEd_Research - IT Governance Institute , 2007

i) 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

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

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

l) 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.

m) 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

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

o) The 2013 Data Breach Investigations Report, VERIZON

REFERENCIAS DIGITALES

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

b) www.**intypedia**.com

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

d) www.isacacr.org

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

f) http://www.isaca.org/Certification/Code-of-Professional-Ethics/Pages/default.aspx

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

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

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

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

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

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

m) http://www.verizonenterprise.com/DBIR/2013/

En razón de que parte importante del material de estudio corresponde a documentos con derechos de autor propiedad de ISACA, para cumplir el principio ético respectivo de adquisición cada estudiante debe adquirir su derecho al registrarse como miembro estudiantil de ISACA según las indicaciones que se brindan en www.isaca.org/studentmember aprovechando el beneficio que tanto la organización local e internacional brindan a los estudiantes de nuestra Facultad. La inversión en este registro tiene un costo de US$25 (inferior al de cualquier libro de texto que pudiera usarse) y le da derecho al estudiante de obtener todo el material del curso de esa organización durante el segundo semestre de 2014 y el año 2014 (acceso al material de Auditoría Informática II).