UNIVERSIDAD DE COSTA RICA

ESCUELA DE ADMINISTRACIÓN DE NEGOCIOS
UNIVERSIDAD DE COSTA RICA

PROGRAMA DEL CURSO

PC-0526
AUDITORÍA INFORMÁTICA 2

SINAES CARRERA ACREDITADA COSTA RICA

La Escuela de Administración de Negocios

Fundada en 1943, es una de las Escuelas con mayor trayectoria en Costa Rica y Centroamérica en la formación de profesionales de alto nivel en las carreras de Dirección de Empresas y Contaduría Pública. Cuenta con un equipo docente altamente capacitado, así como un curriculum actualizado según las necesidades y cambios actuales del mercado. Actualmente ambas carreras se encuentran acreditadas por el SINAES en la Sede Rodrigo Facio.

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 Humanistas

Ética Tolerancia Solidaridad
Perseverancia Alegría

Valores Empresariales

Innovación Liderazgo Excelencia
Trabajo en equipo Emprendedurismo
Responsabilidad Social

Una larga trayectoria de excelencia...

2511-9180 / 2511-9188 www.ean.ucr.ac.cr negocios@ucr.ac.cr /eanucr

PROGRAMA DEL CURSO

PC-0526
CÁTEDRA AUDITORÍA INFORMÁTICA 2
I CICLO 2017

DATOS DEL CURSO						
Carrera (s):	Contaduría Pública					
Curso del IX ciclo del Plan de Estudios 2002.						
Requisitos:	PC-0423: Auditoría Informática I y PC-0424: Laboratorio de Auditoría Informática I					
Correquisitos	PC-0527: Laboratorio de Auditoría Informática II					
Créditos	03					
Horas de teoría:	03 horas	**Horas de laboratorio:**	03 horas	**Horas de práctica:**	05 horas	

PROFESORES DEL CURSO				
SEDE RODRIGO FACIO				
GR	**Docente**	**Horario**	**Aula**	**Horario de Atención***
01	MSI. Roberto Porras León, CPA. Coordinador	**K: 19 a 21:50**	126 CE	K: 17 a 18:50
02	MBA. Gino Ramírez Solís	**K: 19 a 21:50**	128 CE	M: 18 a 21:00
RECINTO SANTA CRUZ				
01	Lic. Olger Obando Fonseca	**S: 13 a 15:50**	Lab.	A convenir
SEDE DEL CARIBE				
01	MBA. Néstor Anderson Salomons	**K: 17 a 19:50**	14	J: 16:30 a 20:30
SEDE DEL ATLÁNTICO				
01	MBA. César Solano León	**K: 18 a 20:50**	15RA	M y V 11 a 11:50

***A solicitud del estudiante, el profesor podrá atender consultas según la hora, lugar y día acordado para cada caso particular, dentro del marco de la normativa de la Universidad de Costa Rica.**

I. DESCRIPCIÓN DEL CURSO

El curso permite al estudiante dar continuidad a lo aprendido en el curso de Auditoría Informática I, conocer los conceptos generales sobre la auditoría de la administración de riesgos de TI y el proceso de auditoría del desarrollo y operación de sistemas de información automatizados. Además, se informará sobre temas de actualidad en el campo de la seguridad informática, del control en sistemas en operación y continuidad de las operaciones.

Se busca que la persona profesional de Contaduría Pública sea además de una persona preparada en las áreas técnicas de este curso, alguien emprendedor, con sentido de la ética y la responsabilidad social, que se desempeñe y tome decisiones tomando en cuenta valores como la solidaridad, la tolerancia y la perseverancia, y destrezas tales como la comunicación asertiva y el trabajo en equipo. La población estudiantil debe dirigir su actuar durante el curso acorde con dichos valores y competencias, y aplicarlos en su desarrollo del curso.

El uso de la plataforma virtual será baja, como apoyo a la consulta de información de los tema del curso y la realización de algunas evaluaciones en línea.

II. OBJETIVO GENERAL

Proporcionar a los futuros profesionales en Contaduría los conocimientos generales sobre la auditoría de administración de riesgos informáticos y la auditoría del desarrollo de sistemas automatizados y en operación, así como conocer de la seguridad informática y su impacto para las organizaciones.

III. OBJETIVOS ESPECÍFICOS

1. Integrar la ética y la responsabilidad social en el análisis del contenido programático del curso, y profundizar en el diálogo y la reflexión sobre los valores de solidaridad, tolerancia y perseverancia, así como sobre la importancia de desarrollar y aplicar las competencias de comunicación asertiva y trabajo en equipo.
2. Aprender los conceptos generales de la auditoría de la administración de riesgos de TI.
3. Aprender el proceso general de auditoría del desarrollo de sistemas de información.
4. Conocer aspectos generales sobre temas de actualidad en seguridad informática y su impacto en las organizaciones.
5. Aprender el proceso de auditoría de sistemas de información en operación
6. Conocer el panorama general de la continuidad de las operaciones de TI

IV. CONTENIDO PROGRAMÁTICO

TEMA 1. Auditoría de la administración de riesgos de tecnologías de información
El estudiante revisará el proceso de administración de riesgos de TI y conocerá la guía de auditoría de COBIT relacionada.

TEMA 2. Auditoría del proceso de adquisición, desarrollo e implementación de sistemas de información automatizados
El estudiante aprenderá los conceptos generales del proceso de auditoría de la adquisición, desarrollo e implementación de sistemas de información automatizados.

TEMA 3. Temas de actualidad en seguridad informática
Mediante el trabajo de investigación y exposición el estudiante se informará de temas de actualidad en seguridad informática y su impacto en las organizaciones.(ver detalle al final del programa)

TEMA 4. Evaluación de sistemas de información en operación
El estudiante aprenderá los conceptos generales de la auditoría de sistemas de información en operación

TEMA 5. Auditoría del plan de continuidad de TI
El estudiante conocerá los criterios generales para la auditoría del proceso de continuidad de TI.

A través de los siguientes componentes de la evaluación, en lo que resulte pertinente en cada uno de los temas, se integrarán aspectos sobre ética, responsabilidad social y emprendedurismo. También se tomará en consideración la aplicación de los valores y competencias referidos en la descripción del curso.

V. ASPECTOS METODOLÓGICOS

a. El personal docente y la población estudiantil desarrollarán las clases dentro de un ambiente de tolerancia, respeto y comunicación asertiva. El profesorado promoverá el trabajo en equipo, en un plano de igualdad de oportunidades y sin discriminación de ninguna especie de forma tal que se garantice un ambiente de diálogo y libre expresión de las ideas y opiniones.
b. Tres horas semanales para analizar el material teórico relacionado con los temas de estudio.
c. 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.
d. Lectura previa a cada clase, según el tema a tratar, de capítulos específicos en los documentos recomendados y material adicional recomendado por el profesor.
e. Participación de los estudiantes en la clase, sobre los temas analizados.
f. 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.
g. Resolución y exposición de casos, con el apoyo de recursos multimedia.
h. Lecturas y actividades complementarias recomendadas por el profesor.

Objetivos de los aspectos metodológicos
a. Fomentar el aprendizaje colaborativo
b. Fortalecer el trabajo en equipo
c. Fortalecer el análisis crítico-constructivo

Objetivos de las competencias Éticas
a. Fomentar el respeto entre los compañeros, en la relación profesor-estudiante y demás miembros de la comunidad universitaria.
b. Fortalecer la responsabilidad en el cumplimiento de tareas y compromisos.

VI. SISTEMA DE EVALUACIÓN

Rubro	Contenido	Porcentaje	Fecha
Primer examen parcial	Temas 1 y 2	20%	16 de mayo
Segundo examen parcial	Temas 4 y 5	25%	04 de julio
Trabajo de investigación	Tema 3	15 %	30 de mayo
Quices y tareas	Todos los temas	20%	En las fechas que defina el profesor
Desarrollo de guías de auditoría	Todos los temas	20%	En las fechas que defina el profesor
NOTA		**100%**	

Primer examen parcial
Incluye los temas de auditoría de la administración de riesgos y el proceso de adquisición, desarrollo e implementación de sistemas de información automatizados

Segundo examen parcial
Incluye los temas de la evaluación de sistemas en operación y continuidad de las operaciones de TI

Trabajo de Investigación
Mediante la metodología que defina el profesor, los estudiantes investigarán sobre temas de actualidad en seguridad informática, preparan un informe sobre el tema y presentan una exposición al respecto.

Quices y Tareas
Pruebas y actividades de corta duración que sirven para evaluar periódicamente el proceso de aprendizaje de los estudiantes.

Desarrollo de guías de auditoría
Los estudiantes preparan las guías de auditoría relacionadas con algunos de los temas del curso. En el campus virtual del curso se encuentra un instructivo general para la elaboración de las guías de auditoría.

Los exámenes de reposición se regirán según el Art. 24 del Reglamento Académico
Los examen de reposición se aplicarán una semana después de la fecha del examen ordinario y tratará sobre los mismos temas del examen ordinario, previa presentación del comprobante respectivo.

VII. CRONOGRAMA

SEMANA	FECHA	TEMA
Semana 1	Del 13 al 17 de marzo	Discusión del programa del curso y Tema 1
Semana 2	Del 20 al 24 de marzo	Tema 1
Semana 3	Del 27 al 31 de marzo	Tema 1
Semana 4	Del 03 al 07 de abril	Tema 2
Semana 5	Del 10 al 14 de abril	Semana Santa – 11 de abril
Semana 6	Del 17 al 21 de abril	Tema 2
Semana 7	Del 24 al 28 de abril	Semana Universitaria
Semana 8	Del 01 al 05 de mayo	Tema 2
Semana 9	Del 08 al 12 de mayo	Tema 2
Semana 10	Del 15 al 19 de mayo	Primer examen Parcial
Semana 11	Del 22 al 26 de mayo	Tema 3
Semana 12	Del 29 de mayo al 02 de junio	Tema 3 – Trabajo de investigación
Semana 13	Del 05 al 09 de junio	Tema 4
Semana 14	Del 12 al 16 de junio	Tema 4
Semana 15	Del 19 al 23 de junio	Tema 5
Semana 16	Del 26 al 30 de junio	Tema 5
Semana 17	Del 03 al 07 de julio	Segundo Examen Parcial
Semana 18	Del 10 al 14 de julio	Exámenes finales
Semana 19	Del 17 al 21 de julio	Exámenes finales

VIII. BIBLIOGRAFÍA

Bibliografía principal:
ISACA (2015), Administración del ciclo de vida de la infraestructura y los sistemas. Manual para la Preparación del Examen CISA

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

Bibliografía complementaria:

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

Estupiñán G, R. (2003). Control interno y fraudes. (1ª. ed.). Bogotá, Colombia: Ecoe Ediciones.

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 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.

IX. INFORMACIÓN DE CONTACTO DE LOS PROFESORES

SEDE RODRIGO FACIO		
GR	**Docente**	**Correo**
01	MSI. Roberto Porras León, CPA Coordinador	roberto.porras@ucr.ac.cr
02	MBA. Gino Ramírez Solís	gino.ramirez@ucr.ac.cr
GR	**Docente**	**Correo**
RECINTO SANTA CRUZ		
01	Prof. Olger Obando Fonseca	olger.obando@gmail.com
SEDE DEL CARIBE		
01	MBA. Néstor Anderson Salomon	nestor.anderson@gmail.com
SEDE DEL ATLÁNTICO		
01	MBA. César Solano León	cesar.solano@sa.ucr.ac.cr

PC-0526 – CÁTEDRA AUDITORÍA INFORMÁTICA 2
I CICLO 2017
TRABAJO DE INVESTIGACIÓN – Entrega: 30 DE MAYO 2017 – 7:00 p.m.

INCIDENTES DE SEGURIDAD INFORMÁTICA EN COSTA RICA Y SUS IMPLICACIONES
(Un análisis de Casos Reales)

Como parte del desarrollo del tema de Seguridad Informática del curso de Auditoría Informática 2, para el primer semestre del 2017, los estudiantes desarrollarán, en grupos, el trabajo de investigación y análisis que se describe a continuación, con un valor del 15% de la nota del curso.

Introducción:

La seguridad informática es una disciplina que se encarga de proteger la integridad y la privacidad de la información almacenada en un sistema informático. De todas formas, no existe ninguna técnica que permita asegurar la inviolabilidad de un sistema.

Un sistema informático puede ser protegido desde un punto de vista lógico (con el desarrollo de software) o físico (vinculado al mantenimiento eléctrico, por ejemplo). Por otra parte, las amenazas pueden proceder desde programas dañinos que se instalan en la computadora del usuario (como un virus) o llegar por vía remota (los delincuentes que se conectan a Internet e ingresan a distintos sistemas). La amenazas a la seguridad informática pueden también venir de personal interno.

Un sistema seguro debe ser íntegro (con información modificable sólo por las personas autorizadas), confidencial (los datos tienen que ser legibles únicamente para los usuarios autorizados), irrefutable (el usuario no debe poder negar las acciones que realizó) y tener buena disponibilidad (debe ser estable).

De todas formas, como en la mayoría de los ámbitos de la seguridad, lo esencial sigue siendo la capacitación de los usuarios. Una persona que conoce cómo protegerse de las amenazas sabrá utilizar sus recursos de la mejor manera posible para evitar ataques o accidentes.

En otras palabras, puede decirse que la seguridad informática busca garantizar que los recursos de un sistema de información sean utilizados tal como una organización o un usuario lo ha decidido, sin intromisiones.

Trabajo a realizar:

En grupos, cuyo tamaño lo define el profesor del curso, los estudiantes deben hacer una investigación, a través de hechos noticiosos acontecidos o con afectación en Costa Rica, sobre incidentes relacionados con el tema de la seguridad e inseguridad informática.

Deben ser casos reales que hayan afectado organizaciones, privadas o públicas, individuos o sistemas de información, información personal de las personas, seguridad física o lógica de los equipos informáticos, robo de identidad, malware, ransonware, phishing, espionaje electrónico,

chantaje o extorsión informática, mal uso de redes sociales, ciberbulling, ciberacoso, ciberamenazas, estafas con medios informáticos, robo de información, alteración no autorizada de sitios web, daño a la información de bases de datos, ciberterrorismo, ciberguerra, ciberdelincuencia, afectación de dispositivos móviles, suplantación de identidad, robo de contraseñas, etc..etc.

Como parte del proceso de investigación se deben identificar 10 hechos que hayan sido noticia en Costa Rica, en los últimos 5 años, a través de cualquier medio de comunicación, incluyendo sitios web y redes sociales.

Para cada uno de ellos se debe hacer un breve resumen identificando los siguientes componentes:

1. ¿Cuál fue el objetivo? - persona, institución, sistema informático, etc.
2. ¿Quién fue el responsable? (si es posible identificarlo)
3. ¿Cuál fue el modus operandi? (cómo lo hicieron, en qué consistió el ataque o incidente)
4. ¿Cuáles fueron las implicaciones del ataque o incidente? (En términos monetarios, sociales, pérdida de credibilidad, afectación a la dignidad de una persona, dificultades operacionales o afectación en el servicio, despido de personal, etc.)
5. ¿Cómo se resolvió o medidas adoptadas al respecto?
6. Lecciones aprendidas de este incidente desde el punto de vista del control interno informático y recomendaciones del grupo para que un incidente de este tipo no se vuelva a repetir. (para este apartado se recomienda utilizar los aprendido en los cursos de auditoría informática, los marcos de referencia normativos en Costa Rica sobre Tecnologías de Información, Ley de delitos informáticos, COBIT, las guías de aseguramiento u otras fuentes de mejores prácticas de control interno informático.)

- Además de la información solicitada, se deben incluir los links de los sitios consultados y referencias bibliográficas para que el profesor puede revisarlos en caso de ser necesario.

- El trabajo debe ser remitido vía electrónica al profesor respectivo, según el cronograma del curso, y este escogerá dos casos por grupo para que sean expuestos en clase en la fecha que este indique.

<u>CONSEJOS</u>:

- Para hacer una análisis apropiado de cada uno de los casos, se recomienda revisar la misma noticia en varios medios de comunicación, de forma que sea posible tener un mejor panorama de cómo sucedió el incidente, qué implicaciones tuvo y como se resolvió.

- Algunos casos pueden haber llegado hasta instancias judiciales, por lo que puede existir una sentencia que sea posible revisar.
- Otros casos pueden haber llegado hasta la Sala Cuarta, lo cual sugiere un pronunciamiento de la misma que sea posible conocer.

2511-9180 / 2511-9188 www.ean.ucr.ac.cr negocios@ucr.ac.cr /eanucr