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 2019

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:**	0 horas	**Horas de práctica:**	0 horas

PROFESORES DEL CURSO				
SEDE RODRIGO FACIO				
GR	**Docente**	**Horario**	**Aula**	**Horario de Atención***
01	Lic. Olger Obando Fonseca	**K: 19 a 21:50**	0124 CE	L: 18:00 a 20:00
02	MSI. Roberto Porras León, CPA Master Walter Saborio Segura	**K: 19 a 21:50**	0308 AU	Roberto K: 17:00 a 19:00 Walter V: 18:00 a 20:00
03	MBA. Gino Ramírez Solís	**K: 19 a 21:50**	0218 CE	M: 18:00 a 20:00
04	MBA. William Bonilla Madriz	**K: 19 a 21:50**	0221 AU	K: 16:50 a 18:50
RECINTO SANTA CRUZ				
01	Lic. Olger Obando Fonseca	**S: 13:00 a 15:50**	0101 RS	S: 9:00 a 11:00
SEDE DEL CARIBE				
01	MBA. Néstor Anderson Salomons	**K: 17:00 a 19:50**	014 RL	J: 16:00 a 18:00
SEDE DEL ATLÁNTICO				
01	MSC. Fabián Cordero Navarro**	**K: 18:00 a 20:50**	009 RA	K: 16:00 a 18:00

Coordinador de la cátedra: Msc. Fabián Cordero Navarro, CISA

***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 los conocimientos adquiridos en el curso Auditoría Informática I, complementándolos con nuevos conceptos generales sobre la auditoría de la administración de riesgos de TI, los procesos de adquisición e implementación, los controles de operación, temas de actualidad en el campo de la seguridad informática, ciberseguridad y la 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 considerando valores tales como la solidaridad, la tolerancia y la perseverancia, y cuente con destrezas para 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 el desarrollo del curso.

II. OBJETIVO GENERAL

Proporcionar a los futuros profesionales en Contaduría Pública los conocimientos y habilidades necesarias para examinar la gestión de las tecnologías de información en las organizaciones, lo anterior, desde una perspectiva de control, y a efecto de este curso, específicamente en lo que corresponde a la gestión de riesgos informáticos, el desarrollo e implementación de sistemas de información, los controles de sistemas en operación, la seguridad informática y la continuidad de las operaciones.

III. OBJETIVOS ESPECÍFICOS

1. Repasar el proceso de auditoría de TI.
2. Aprender los conceptos generales de la auditoría de la administración de riesgos de TI.
3. Aprender el proceso general de auditoría del desarrollo, implementación y operación de sistemas de información.
4. Conocer aspectos generales sobre temas de actualidad en seguridad informática y su impacto en las organizaciones.
5. Conocer el panorama general de la continuidad de las operaciones de T.I.

IV. CONTENIDO PROGRAMÁTICO

TEMA 1. Repaso del Proceso de Auditoría de TI
Se repasará con los estudiantes el proceso de auditoría de la gestión de TI (tema desarrollado durante el curso Auditoría Informática I); específicamente en lo relativo a lo siguiente:

1. Objetivos y actividades principales de las etapas del proceso de auditoría (Planificación, Examen, Comunicación).
2. El programa de auditoría para la etapa de Planificación y para la etapa de Examen (componentes, objetivos, alcance y procedimientos típicos).
3. Consideraciones básicas en la construcción de procedimientos de auditoría y uso de técnicas.
4. Importancia y condiciones particulares de la evidencia de auditoría en pruebas sobre TI (TAAC).
5. El informe de auditoría (componentes, hallazgos, conclusiones).

TEMA 2. 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 5.0 relacionada; en detalle se analizarán los siguientes temas:

1. Importancia, aspectos a considerar, definiciones, proceso de evaluación y controles como contramedidas.
2. Enfoque de auditoría basado en riesgos.
3. Perspectiva de Cobit 5 para riesgos
4. Factores impulsadores de la gestión de riesgos
5. Ventajas del uso de Cobit 5 para riesgos

TEMA 3. Auditoría del proceso de adquisición, desarrollo, implementación y evaluación operativa de sistemas de información automatizados
El estudiante aprenderá los conceptos generales relativos a:

1. El proceso de auditoría de la adquisición, desarrollo, implementación (el proceso de compras de SW y HW).
2. El ciclo de vida del desarrollo de sistemas de información y metodologías de desarrollo y gestión de proyectos en la implementación de soluciones.

En lo correspondiente a la evaluación operativa de sistemas de información automatizados se estudiarán los conceptos relativos a:

1. Controles de aplicación (controles de entrada, procesamiento y salida) y su incidencia en la integridad de datos.

TEMA 4. Temas de actualidad en seguridad informática
El estudiante conocerá aspectos relativos a:

1. Que es seguridad informática
2. Confidencialidad, integridad y disponibilidad de la información.
3. Objetivos de la seguridad informática.
4. Amenazas actuales a la seguridad informática
5. Enfoques para la ciberseguridad
6. Vulnerabilidades, riesgos y amenazas de la tecnología móvil
7. Riesgos y beneficios de la "computación en la nube"
8. Cómo COBIT 5 puede ayudar a reducir la probabilidad y el impacto de las amenazas cibernéticas más importantes

Adicional el estudiante mediante la construcción, análisis y presentación de diversos casos prácticos se involucrarán en temas actuales sobre seguridad informática y el fraude asociado, así como su impacto en las organizaciones. **(Ver detalle en el apartado de "Estudio de Casos", ubicado al final de este programa).**

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

1. La auditoría del proceso de continuidad de TI (Plan de Continuidad, Plan de Recuperación y Planes de Contingencias, consideraciones generales, componentes y valoración riesgos y análisis de impacto de negocio - BIA).

V. ASPECTOS METODOLÓGICOS

1. 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.
2. Cada profesor podrá desarrollar un máximo de 2 lecciones en modo virtual, para el aprovechamiento de distintas actividades que no pueden ser desarrolladas en la lección magistral; por ejemplo, la realización de foros mediante el uso de la plataforma Moodle, a fin de que se evidencie la participación de la totalidad de los estudiantes del curso y se puedan utilizar sus participaciones para ampliar la discusión del tema en estudio.
3. Tres horas semanales para analizar el material teórico relacionado con los temas de estudio.
4. 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.
5. Lectura previa a cada clase, según el tema a tratar, de capítulos específicos en los documentos recomendados y material adicional recomendado por el profesor.

6. Participación de los estudiantes en la clase, sobre los temas analizados.
7. Desarrollo de trabajos prácticos sobre los contenidos del curso, por parte de grupos de alumnos no mayores a 4 integrantes, los cuales deberán exponer los resultados de los temas investigados, en las fechas que se determinan en el programa.
8. Resolución y exposición de casos, con el apoyo de recursos multimedia.
9. 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

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 y valores. También se tomará en consideración la aplicación de las competencias referidas en la descripción del curso.

Rubro	Contenido	Porcentaje
Primer examen parcial	Temas 1 y 2	20%
Segundo examen parcial	Temas 3, 4 y 5	30%
Dinámica de casos prácticos	Incidentes seguridad informática en Costa Rica	25%
Pruebas cortas	Los temas y en las fechas indicados en el cronograma	25%
NOTA		**100%**

Primer examen parcial

Incluye los temas de: **Repaso del proceso de auditoría de TI** y **Auditoría de la administración de riesgos de tecnologías de información**.

Se realizará en forma virtual y por medio del campus de la Facultad. El examen se efectuará en la fecha indicada e incorporará la materia detallada anteriormente y explicada por el profesor en clase hasta ocho días antes de la fecha de cada prueba.

Segundo examen parcial

Incluye los temas de: **Auditoría del proceso de adquisición, desarrollo, implementación y evaluación operativa de sistemas de información automatizados, Seguridad Informática y Auditoría del plan de continuidad de TI.**

Se realizará en forma virtual y por medio del campus de la Facultad. El examen se efectuará en la fecha indicada e incorporará la materia detallada anteriormente y explicada por el profesor en clase hasta ocho días antes de la fecha de cada prueba.

Estudio de Casos Prácticos

Haciendo uso de la metodología establecida en **el apartado de "Estudio de Casos" (ubicado al final de este programa)**, los estudiantes procederán a la construcción y análisis de diversos casos prácticos basados en situaciones fácticas de la vida real por medio de los cuales profundizarán sobre temas de actualidad relacionados con la seguridad informática.

Pruebas cortas
Pruebas y actividades que sirven para evaluar periódicamente el proceso de aprendizaje de los estudiantes. Quedan anunciados desde el primer día de clase y se aplicarán en horario de clase o bien extraclase. La materia puede derivarse de cualquiera de los temas previamente discutidos y estudiados en clase. Deberán ser realizados en forma individual, y ya sea de manera presencial y en papel o bien por medio del campus de la Facultad (Moodle). Se realizarán cinco exámenes cortos de cátedra. Los exámenes cortos no se reponen.

En caso de ausencia a alguno de los exámenes parciales antes indicados, se aplicará lo que establece el RRAE en su artículo 24:

> "ARTÍCULO 24. Cuando el estudiante se vea imposibilitado, por razones justificadas, para efectuar una evaluación en la fecha fijada, puede presentar una solicitud de reposición a más tardar en cinco días hábiles a partir del momento en que se reintegre normalmente a sus estudios. Esta solicitud debe presentarla ante el profesor que imparte el curso, adjuntando la documentación y las razones por las cuales no pudo efectuar la prueba, con el fin de que el profesor determine, en los tres días hábiles posteriores a la presentación de la solicitud, si procede una reposición. Si ésta procede, el profesor deberá fijar la fecha de reposición, la cual no podrá establecerse en un plazo menor de cinco días hábiles contados a partir del momento en que el estudiante se reintegre normalmente a sus estudios. Son justificaciones: la muerte de un pariente hasta de segundo grado, la enfermedad del estudiante u otra situación de fuerza mayor o caso fortuito."

Aquel estudiante o grupo de trabajo que incurra en alguna falta grave tal como, copia, plagio, utilización de material no autorizado o comunicación o actuación ilícita en cualquiera de la pruebas o parte de ellas, tendrá una calificación de 0%, con las consecuencias posteriores que establece la Universidad de Costa Rica.

Los exámenes 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.

La nota final será la que obtenga una vez sumados todos los porcentajes; si esa nota es igual o superior a 70 aprueba el curso; si está entre 60 y 69, tiene derecho al examen de ampliación; si es inferior a 60 pierde el curso. 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 del RRAE).

En todos los casos, se aplica el sistema de redondeo según el Reglamento de Régimen Académico Estudiantil (RRAE).

VII. CRONOGRAMA

SEMANA	FECHA	TEMA
Semana 1	Del 11 al 15 de marzo 2019	Discusión del programa del curso y Tema 1
Semana 2	Del 18 al 22 de marzo 2019	Tema 1
	29 de marzo 2019	Examen Corto #1 Tema 1
Semana 3	Del 25 al 29 de marzo 2019	Tema 2
Semana 4	Del 01 al 05 de abril 2019	Tema 2
	12 de abril 2019	Examen Corto #2 Tema 2
Semana 5	Del 8 al 12 de abril 2019	Tema 3
Semana 6	Del 15 al 19 de abril 2019	Semana Santa
Semana 7	Del 22 al 26 de abril 2019	Semana Universitaria / Tema 3 Sesión virtual
Semana 8	Del 29 abril al 03 de mayo 2019	Primer Examen Parcial
Semana 9	Del 06 al 10 de mayo 2019	Tema 3
Semana 10	Del 13 al 17 de mayo 2019	Tema 3
	24 mayo 2019	Examen Corto #3 Tema 3
Semana 11	Del 20 al 24 de mayo 2019	Tema 4
Semana 12	Del 27 al 31 de mayo 2019	Tema 4
	7 de junio 2019	Examen Corto #4 Tema 4
Semana 13	Del 03 al 07 de junio 2019	Tema 4 – Presentación construcción y análisis de casos
Semana 14	Del 10 al 14 de junio 2019	Tema 4 – Presentación construcción y análisis de casos - Tema 5
Semana 15	Del 17 al 21 de junio 2019	Tema 5
	28 de junio 2019	Examen Corto #5 Tema 5 (parcial)
Semana 16	Del 24 al 28 de junio 2019	Tema 5
Semana 17	Del 01 al 05 de julio 2019	Segundo Examen Parcial (Fin de Lecciones)
Semana 18	Del 8 al 12 de julio 2019	Exámenes finales
Semana 19	Del 15 al 19 de julio 2019	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)
COBIT® 5 for Risk
ISO 22301

Bibliografía complementaria:

Echenique G, J. A. (2001). Auditoría en informática. (2ª. ed.). México D F, México: McGraw 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	roberto.porras@ucr.ac.cr
02	MBA. Gino Ramírez Solís, CPA	gino.ramirez@ucr.ac.cr
03	Lic. Olger Obando Fonseca	olger.obando@gmail.com
04	Master Walter Saborio Segura	wbsaborio@gmail.com
05	MBA. William Bonilla Madriz, CISA	william@gti.co.cr
GR	**Docente**	**Correo**
RECINTO SANTA CRUZ		
01	Lic. Olger Obando Fonseca	olger.obando@gmail.com
SEDE DEL CARIBE		
01	MBA. Néstor Anderson Salomón	nestor.anderson@gmail.com
SEDE DEL ATLÁNTICO		
01	MSC. Fabián Cordero Navarro, CISA	fcordero@carvajalcr.com

PC-0526 – CÁTEDRA AUDITORÍA INFORMÁTICA 2
ESTUDIO DE CASOS PRÁCTICOS

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 2019, los estudiantes desarrollarán, en grupos de máximo 4 integrantes, el trabajo de investigación y análisis que se describe a continuación, con un valor del 25% 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). Las 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, 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.

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 lo 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.

CONSEJOS:
- Para hacer un 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.