UNIVERSIDAD DE COSTA RICA

EAN Escuela de Administración de Negocios

Programa de Curso

PC-0526
AUDITORÍA INFORMÁTICA II

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 de docentes altamente capacitado, así como un currículum actualizado según las necesidades actuales del mercado. A partir de junio 2016, el SINAES otorgó acreditación de ambas carreras a 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...

SINAES CARRERA ACREDITADA COSTA RICA

¡Para proteger el ambiente, no imprima este documento si no es necesario!

PROGRAMA DEL CURSO
PC-0526 AUDITORÍA INFORMÁTICA II
II CICLO 2021

DATOS DEL CURSO

Carrera (s): Contaduría Pública
Curso del IX ciclo del Plan de Estudios 2016.
Requisitos: PC-0423 Auditoría Informática I; PC-0424 Laboratorio de Auditoria Informática I
Correquisitos PC-0527 Laboratorio de Auditoría Informática II
Créditos 3

Horas de teoría:	3 horas	**Horas de laboratorio: 0**	**Horas de práctica: 0**

PROFESORES DEL CURSO

GR	Docente	Horario	Aula	Horario de Atención*
	SEDE RODRIGO FACIO			
1	MSI Roberto Porras León, CPA, CISA	**K: 19 A 21:50**	Virtual	K:17 A 18:50
2	Msc. Fabián Cordero Navarro, CISA	**K: 19 A 21:50**	Virtual	K:17 A 18:50
	SEDE CARIBE			
1	MBA. Néstor Anderson Salomons	**K: 17 A 19:50**	Virtual	L:16 A 18:00
	SEDE ATLÁNTICO			
1	MBA. William Bonilla Madriz, CISA	**K: 18 A 20:50**	Virtual	K:16 A 18:00

Coordinador de la Cátedra: Msc. Fabián Cordero Navarro.

*A solicitud del estudiante, el profesor podrá atender consultas según la hora y día acordado para cada caso particular mediante modalidad virtual, 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.

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

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. Integrar la ética y la responsabilidad social en el estudio del contenido programático del curso, y profundizar en el diálogo y la reflexión sobre los valores de ética, tolerancia, solidaridad, perseverancia, en un marco de respeto y responsabilidad, así como sobre la importancia de desarrollar y aplicar las competencias de comunicación asertiva, trabajo en equipo, hábitos de orden, disciplina, búsqueda de soluciones y construcción autodidacta del conocimiento.

2. Repasar el proceso de auditoría de TI.

3. Aprender los conceptos generales de la auditoría de la administración de riesgos de TI.

4. Aprender el proceso general de auditoría del desarrollo, implementación y operación de sistemas de información.

5. Conocer aspectos generales sobre temas de actualidad en seguridad informática y su impacto en las organizaciones.

6. 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:

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

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

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:

- Perspectiva de Cobit 5 para riesgos
- Factores impulsadores de la gestión de riesgos
- 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:

- El proceso de auditoría de la adquisición, desarrollo, implementación (el proceso de compras de SW y HW).
- 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:

- 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:

- Que es seguridad informática
- Confidencialidad, integridad y disponibilidad de la información.
- Objetivos de la seguridad informática.
- Amenazas actuales a la seguridad informática
- Enfoques para la ciberseguridad
- Vulnerabilidades, riesgos y amenazas de la tecnología móvil
- Riesgos y beneficios de la "computación en la nube"
- 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 involucrará 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:

- 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).

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

A través de los siguientes componentes de la evaluación, en lo que resulte pertinente en cada uno de los temas, se integrarán lecturas en inglés y casos.

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. 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.

c. Lectura previa a cada clase, según el tema a tratar, de material suministrado por el profesor.

d. Participación de los estudiantes en la clase, mediante la discusión de los temas analizados.

e. Desarrollo de trabajos de investigación 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.

f. Resolución y exposición de casos, con el apoyo de recursos multimedia.

g. 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.

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

VI. SISTEMA DE EVALUACIÓN

Rubro	Contenido	Porcentaje	Fecha
Pruebas cortas		25%	Ver Cronograma
Casos		20%	Ver Cronograma
Trabajo Investigación		25%	Ver Cronograma
Material en inglés		5%	Ver Cronograma
Examen Final		25%	Ver Cronograma
NOTA		**100%**	

a. Pruebas cortas

Los exámenes cortos quedan anunciados desde el primer día de clase y se aplicarán de forma en horario de clase o bien extraclase. La materia puede derivarse de cualquiera de los temas previamente discutidos y estudiados en clase. Éstos estarán conformados por pruebas de corta duración que sirven para evaluar periódicamente el aprendizaje de los estudiantes. Deberán ser realizados en forma individual, y de manera virtual por medio de la plataforma Mediación Virtual de la UCR. Se realizarán cinco exámenes cortos de cátedra. Los exámenes cortos no se reponen; sin embargo, para efectos de determinar el porcentaje asignado a este rubro se eliminará la prueba corta con menor nota.

b. Casos

El desarrollo grupal o individual de casos prácticos permitirá la aplicación de los contenidos teóricos a un contexto empresarial y fomentará la habilidad de toma de decisiones del estudiante. Durante el curso se desarrollará por parte de los estudiantes tres casos de temas relacionados con el contenido del curso.

c. Trabajo de investigación

Los estudiantes deberán realizar una investigación de acuerdo con los siguientes términos:

- La investigación **se realizará en grupos** de máximo 5 estudiantes, no se permiten trabajos individuales, ello con la intención de promover el trabajo en equipo.
- Los resultados de la investigación se deben presentar en forma escrita o formato electrónico (según lo disponga el profesor) en formato de “nota técnica” con una extensión entre 10 y 20 páginas máximo, en un formato de “nota técnica”.
- Cada grupo deberá realizar una **exposición oral**, ante la clase y el profesor; y deben exponer todos los miembros del grupo. La exposición se realizará según el calendario establecido y en un tiempo máximo de 20 minutos.
- Al finalizar la exposición oral **el profesor realizará una serie de preguntas** sobre la materia a investigar y sobre lo expuesto por el equipo de trabajo.
- La **calificación de la investigación** se asignará de la siguiente manera:
    - 60% corresponde al trabajo escrito (se considerará: cobertura de los aspectos mínimos

establecidos para el tema de investigación, alcance y certeza del contenido, calidad del documento, presentación y ortografía, uso de diagramas y gráficos).

25% sobre la exposición (calidad expositores (voz, seguridad, uso de la plataforma, dominio del tema, vocabulario apropiado, gestión del tiempo, uso adecuado de la plataforma, creatividad)).

- 15% sobre la calidad de las respuestas por parte del equipo de trabajo a las preguntas realizadas por el profesor posterior a la exposición.

- El profesor podrá requerir tanto un **avance** del trabajo como la **entrega en borrador** del documento escrito en las fechas que designará oportunamente a fin de revisar su contenido y preparar las preguntas a realizar, después de la exposición de los estudiantes.
- La investigación se realizará sobre el siguiente tema; el cual será asignado en la primera clase del curso.

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 II, para el segundo semestre del 2021, los estudiantes desarrollarán, en grupos de máximo 5 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 y en el resto del mundo en los últimos 3 años, 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 3 hechos que hayan sido noticia en Costa Rica y 3 hechos en el resto del mundo, en los últimos 3 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.

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

- 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 en el caso de Costa Rica, 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.

d. Material en inglés

El profesor entregará a los estudiantes 2 materiales en inglés (lecturas, videos, presentaciones, etc.) con la finalidad de que el estudiante comprenda el contenido del material. El profesor realizará ejercicios, prácticas, talleres o exámenes cortos para verificar la comprensión del material asignado.

e. Examen Final

El **examen final** se realizará en forma virtual y por medio de mediación virtual; se efectuará de conformidad con los contenidos señalados en el cuadro de evaluación y lo que establece la normativa universitaria. Este se realizará en las fechas indicadas e incorporará toda la materia explicada por el profesor en clase hasta ocho días antes de la fecha de la prueba.

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).

En caso de ausencia al examen final antes indicado, 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.

VII. CRONOGRAMA

SEMANA	FECHA	TEMA
1	Agosto 17	Programa del curso. Tema1: Repaso del proceso de auditoría de TI Asignación material en inglés tema 1
2	Agosto 24	Tema1: Repaso del proceso de auditoría de TI Semana del 23 al 27 de agosto comprobación material en inglés tema 1
3	Agosto 31	Semana del 30 de agosto al 03 de setiembre **examen corto#1** tema 1 Tema 2: Auditoría de la administración de riesgos de TI Asignación lectura en inglés tema 2 Entrega caso #1 tema 2 por pate del profesor
4	Setiembre 07	Tema 2: Auditoría de la administración de riesgos de TI Semana del 06 de setiembre al 10 de setiembre comprobación material en inglés tema 2
5	Setiembre 14	Semana del 13 al 17 de setiembre **examen corto #2** tema 2 Tema:3 Auditoría del proceso de adquisición, desarrollo, implementación y evaluación operativa de SI automatizados **Entrega resolución caso #1 tema 2 por parte de los estudiantes**
6	Setiembre 21	Tema:3 Auditoría del proceso de adquisición, desarrollo, implementación y evaluación operativa de SI automatizados Entrega caso #2 tema 3 por parte del profesor
7	Setiembre 28	Tema:3 Auditoría del proceso de adquisición, desarrollo, implementación y evaluación operativa de SI automatizados
8	Octubre 05	Tema:3 Auditoría del proceso de adquisición, desarrollo, implementación y evaluación operativa de SI automatizados **Entrega resolución caso #2 tema 3 por parte de los estudiantes**
9	Octubre 12	Semana de la Desconexión Tecnológica
10	Octubre 19	Semana del 18 al 22 de octubre **examen corto #3** tema 3 Tema 4: Temas de actualidad en seguridad informática
11	Octubre 26	Tema 4: Temas de actualidad en seguridad informática
12	Noviembre 02	**Exposiciones trabajo investigación** tema 4 Semana del 01 al 05 de noviembre **examen corto #4** tema 4
13	Noviembre 09	**Exposiciones trabajo investigación** tema 4 Entrega caso #3 tema 5 por parte del profesor
14	Noviembre 16	Tema 5: Auditoría del plan de continuidad de TI
15	Noviembre 23	**Entrega resolución caso #3 tema 5 por parte de estudiantes** Tema 5: Auditoría del plan de continuidad de TI Semana del 22 al 26 de noviembre **examen corto #5** tema 5 (lo visto hasta el 16 de noviembre)
16	Noviembre 30	**Examen Final**

VIII. BIBLIOGRAFÍA

El material principal del curso será distribuido por los profesores de la cátedra y estará fundamentado en otros textos y material disponibles.

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: 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 DEL PROFESOR

SEDE RODRIGO FACIO		
GR	**Docente**	**Correo**
1	MSI Roberto Porras León, CPA, CISA	roberto.porras@ucr.ac.cr
2	Msc. Fabián Cordero Navarro, CISA	fabian.cordero@ucr.ac.cr
SEDE CARIBE		
1	MBA. Néstor Anderson Salomons	nestor.anderson@ucr.ac.cr
SEDE ATLÁNTICO		
1	MBA. William Bonilla Madriz, CISA	william.bonillamadriz@ucr.ac.cr

X. ENTORNO VIRTUAL

Este curso es virtual. Se utilizará la plataforma institucional Mediación Virtual para colocar los documentos, vídeos del curso, hacer evaluaciones. Además, se usará para que los estudiantes puedan realizar consultas en forma virtual al docente.

Importante:
Tomando como base lo establecido por la Vicerrectoría de Docencia de la Universidad de Costa Rica todas las evaluaciones del curso se llevarán a cabo por medio del sitio Mediación Virtual. En este contexto la Cátedra de Auditoría Informática II ha establecido los siguientes criterios para el uso del citado sitio de Mediación Virtual:

1. Prácticas, casos, temas varios: en cada una de las semanas que corresponda (según se indica en el cronograma del curso) en el sitio Mediación Virtual se habilitará un repositorio en el cual los estudiantes deben colocar la solución de cada uno de los casos, prácticas, etc., indicados en el curso por el profesor.

   Dicho repositorio indicará de forma clara y precisa la fecha y hora que los estudiantes tendrán como límite para hacer entrega de la solución de sus prácticas, casos, ejercicios, etc. Una vez expirado ese plazo, el sitio Mediación Virtual no permitirá la carga de archivos y en consecuencia el o los grupos de estudiantes o los estudiantes individuales (según sea el caso) que eventualmente no hubiesen entregado la solución de sus trabajos, perderán los puntos asignados a los mismos. La cátedra ha designado al sitio Medición Virtual como el único medio a través del cual se llevará a cabo la recepción de la solución de las prácticas, casos, etc., del curso, en consecuencia, no se tomará como válido el que los estudiantes hagan envío de la solución de los trabajos asignados por medios alternativos tales como correo electrónico, What's App u otros similares.

2. Exámenes, comprobación de lecturas en inglés y pruebas cortas: en cada una de las semanas que corresponda (según se indica en el cronograma del curso) en el sitio Mediación Virtual se habilitará cada una de las evaluaciones. Para la solución de las citadas evaluaciones, los estudiantes contarán con un único intento el cual se cerrará y enviará de forma automática una vez que expire el tiempo asignado a la prueba. En todas las evaluaciones el modo de navegación será secuencial, lo cual implica que los estudiantes deben iniciar la prueba dando respuesta a la pregunta No. 1 y avanzar en la prueba haciendo uso del botón "siguiente página" de manera que den respuesta una a una a la totalidad de las preguntas que conforman la evaluación. El sitio Mediación Virtual no permitirá al estudiante regresar a las páginas anteriores en ningún punto de la evaluación. En el caso de que un estudiante pase de una pregunta a la siguiente sin dar respuesta a la primera, automáticamente perderá el puntaje asignado a la pregunta a la cual no dio respuesta.

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.**