UNIVERSIDAD INTERAMERICANA DE PUERTO RICO
RECINTO METROPOLITANO
FACULTAD DE CIENCIAS ECONÓMICAS Y ADMINISTRATIVAS
ESCUELA DE ECONOMÍA
PROGRAMA DE TECNOLOGÍA DE LA INFORMACIÓN

PRONTUARIO

I. INFORMACIÓN GENERAL

Título del Curso	:	Auditoría y Seguridad en los Sistemas de Información
Código y Número	:	CMIS 4500
Créditos	:	3
Término Académico	:	
Profesor	:	
Horas de Oficina	:	
Teléfono de Oficina	:	(787) 250-1912
Correo Electrónico	:	

II. DESCRIPCIÓN

Análisis de los procedimientos y métodos de la auditoría aplicados a los sistemas de información. Incluye los aspectos de seguridad y los controles físicos y lógicos. Requisito: CMIS 3420.

III. OBJETIVOS

Se espera que al finalizar el curso, el estudiante pueda:

1. Entender desde una perspectiva histórica los fundamentos e importancia de la Auditoría de SI y su desarrollo como disciplina.

2. Explicar los aspectos reglamentarios que rigen la práctica de la Auditoría de SI.

3. Explicar las fases del proceso de Auditoría de SI.

4. Entender el modelo de Auditoría de SI basado en la evaluación y análisis de riesgo y su importancia para la fase de planificación de proyectos de auditoría de SI.

5. Relacionarse con la metodología y herramientas actuales para llevar a cabo un proyecto de Auditoría de SI.

6. Evaluar y recomendar desde el punto de vista de auditoría sobre las políticas de seguridad y control diseñadas para los SI o redes.

IV. CONTENIDO TEMÁTICO

A. Introducción a la Auditoría de Sistemas de Información

1. Definición e historia de la Auditoría de SI
2. El rol de la función de la Auditoría de SI dentro de la organización
3. La administración de los recursos de Auditoría de SI
4. Planificación de la función de Auditoría de SI
5. Planificación de proyectos: Consideraciones legales y reglamentarias

B. Estructura reglamentaria

1. Reglamentación a nivel internacional: ISACA
2. Certificaciones profesionales
3. El Código de Ética
4. Estándares, guías y procedimientos

C. El proceso de Auditoría de SI

1. Tipos de auditoría
2. Programas de auditoría
3. Metodología de la auditoría
4. Detección de fraude
5. Materialidad y riesgo de auditoría
6. Técnicas para el análisis de riesgo
7. Objetivos de la auditoría
8. Pruebas de auditoría: cumplimiento / detalle
9. Evidencia y muestreo
10. Herramientas computarizadas para asistir en la auditoría (CAAT's)
11. Evaluación de los resultados de la auditoría: limitaciones, debilidades y fortalezas
12. Comunicación de resultados
13. Recomendaciones y seguimiento ("follow up")
14. Documentación
15. Técnicas de administración de proyectos

D. Riesgo

1. Definición de riesgo dentro del ambiente de SI
2. Auditoría basada en riesgo y la planificación proyectos
3. Riesgos típicos de los SI o redes

E. Control Interno

1. Definición de control dentro del ambiente de SI
2. El *Gobierno Corporativo* y el ambiente de control interno
3. Objetivos del control interno
4. Modelos: CobiT / COSO / ISO
5. Objetivos del control de SI
6. Procedimientos generales de control
7. Procedimientos de control de las aplicaciones

F. Seguridad

1. Fundamentos de seguridad de la información
2. Análisis de riesgo aplicado a seguridad
3. Diseño, implementación y mantenimiento de políticas de seguridad

    a. "*Security awareness*"

4. Vulnerabilidades y amenazas comunes: accesos indebidos, ataques maliciosos y robo de identidad
5. Detección y respuesta a incidentes
6. Investigación forense
7. Leyes y reglamentación de seguridad
8. Modalidades actuales de seguridad de la información

G. Nuevas tendencias en la práctica de Auditoría de SI

1. Auto evaluación de controles
2. Automatización de los documentos de trabajo
3. Auditoría integrada
4. Auditoría continua
5. El futuro de la profesión

V. ACTIVIDADES

1. Esta es una lista de estrategias de enseñanza sugeridas para el curso:

Conferencias por el profesor
Ejercicios de práctica
Discusión de lecturas y ejercicios
Ejercicios de aplicación
Auto evaluación
Trabajo colaborativo
Vídeos
Lecturas y ejercicios suplementarios

2. Uso de estrategias de Calidad Total y “Assessment”:

Auto evaluación (*A, CT*)
Ejercicios de reflexión (*A*)
“One minute paper” (*A*)
Aprendizaje cooperativo (*A, CT*)
Resumir en una oración (*A*)
Resumir en una palabra (*A*)
Trabajos en grupos (*A*)
Torbellino de ideas (*A*)
Portafolio (*A*)

VI. EVALUACIÓN

El profesor (a) utilizará los criterios de evaluación que estime pertinentes para determinar el dominio de los estudiantes en cuanto a conocimientos y destrezas. Se utilizará la siguiente distribución para la asignación de calificaciones:

100 - 90	A
89 - 80	B
79 - 70	C
69 - 60	D
59 - 0	F

3 pruebas parciales	60%
Trabajo especial de revisión de caso	20%
Proyecto de evaluación de políticas de seguridad	20%
Total	100%

Se aplicará la curva normal

VII. NOTAS ESPECIALES

1. Servicios Auxiliares o Necesidades Especiales

Todo estudiante que requiera servicios auxiliares o asistencia especial deberá solicitar los mismos al inicio del curso o tan pronto como adquiera conocimiento de que los necesita, a través del registro correspondiente, en el programa de orientación con el Sr. José A. Rodríguez, Ext. 2306.

2. Honradez, Fraude y Plagio

La falta de honradez, el fraude, el plagio y cualquier otro comportamiento inadecuado con relación a la labor académica constituyen infracciones mayores sancionadas por el Reglamento General de Estudiantes. Las infracciones mayores, según dispone el Reglamento General de Estudiantes, pueden tener como consecuencia la suspensión de la Universidad por un tiempo definido mayor de un año o la expulsión permanente de la Universidad, entre otras sanciones.

3. Uso de Dispositivos Electrónicos

Se desactivarán los teléfonos celulares y cualquier otro dispositivo electrónico que pudiese interrumpir los procesos de enseñanza y aprendizaje o alterar el ambiente conducente a la excelencia académica. Las situaciones apremiantes serán atendidas, según corresponda. Se prohíbe el manejo de dispositivos electrónicos que permitan acceder, almacenar o enviar datos durante evaluaciones o exámenes.

VIII. RECURSOS EDUCATIVOS

Libros de Texto:

Davis, C., Schiller, M. & Wheeler, K., (2011), IT Auditing Using Control to Protect Information Assets, 2nd ed. McGraw Hill Osborne ISBN-13: 978-0071742382.

Stamp, M., (2011). Information Security: Principles and Practice, 2nd ed. John Wiley. ISBN-13: 978-0470626399.

Lecturas Suplementarias:

CISM Review Manaula (2012) Certified Information Security Manager ISBN13: 978-1604202137.

CISA Review Manual. (2012). Certified Information Systems Auditor ISBN13: 978-1604202007.

CobiT Framework, 4.1 ed. (2007). IT Governance Institute. ISBN10: 1033284722.

IX. BIBLIOGRAFÍA ACTUAL Y CLÁSICA

Libros:

Allen-Senft, S., (2008), Information Technology Control and Audit Auerbach Publications, ISBN-13: 978-1420065503.

Merkow M., Breithaupt, J., (2006). *Information Security Principles and Practices 1ed.* Upper Saddle River, NJ. Prentice Hall.

Information Technology Controls. (2006). The Institute of Internal Auditors.
Whitman, M., Mattord, H., (2005). *Readings and Cases in the Management of Information Security.* Boston, MA. Course Technology.

Gallegos, F., [et al.], (2004). *Information Technology Control and Audit 2ed.* Auerbach Publications, CRC Press LLC.

Weber, R., (1999). *Information Systems Auditing.* Upper Saddle River, NJ. Prentice Hall.

Recursos Electrónicos:

- IS Audit and Control Association (ISACA) Web Site. www.isaca.org
- The Institute of Internal Auditors (IIA) Web Site. www.theiia.org
- American Institute of CPAs (AICPA) Web Site. www.aicpa.org
- IT Governance Institute (ITGI) Web Page. www.itgi.org
- International IS Security Certification Consortium (ISC2) Web Site. www.isc2.org
- 2002 Sarbanes-Oxley Act (S-Ox) Web Site. www.sarbanes-oxley.com
- Securities and Exchange Commission (SEC) Web Site. www.sec.gov
- Audit Net Web Site. www.auditnet.org

Rev. 10/2004; 08/2008; 03/2009; 08/2009 06/2011; 04/2012; 10/2013