**UNIVERSIDAD INTERAMERICANA DE PUERTO RICO**

**RECINTO METROPOLITANO**

**ESCUELA DE ECONOMIA**

**SISTEMAS COMPUTADORIZADOS DE INFORMACIóN GERENCIAL**

**Prontuario**

**I. INFORMACIÓN GENERAL**

**Título del Curso : Auditoría y Seguridad de los Sistemas de Información**

**Código y Número : CMIS 4500**

**Créditos : 3**

**Término Académico : 2010-33**

**Profesor : Juan C. Karman**

**Horas de Oficina : Martes y Jueves 6-8 PM**

**Teléfono de la Oficina : (787) 250-1912 XT: 2493**

**Correo Electrónico :** [**jkarman@metro.inter.edu**](mailto:jkarman@metro.inter.edu)

**II. Descripción**

Análisis de los procedimientos y métodos de la auditoría aplicados a los sistemas de información incluyendo los aspectos de seguridad y controles físicos y lógicos.

**III.** **Objetivos**

Al terminar el curso el estudiante estará capacitado para:

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

1.1 se define lo que comprende la Auditoría de SI y se distingue de otras disciplinas relacionadas

1.2 se presenta un breve recuento histórico acerca del surgimiento y desarrollo hasta el presente de la profesión de Auditoría de SI

1.3 se define el rol de la función de la Auditoría de SI dentro de las organizaciones y su importancia para el logro de metas y objetivos

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

2.1 se discute la estructura reglamentaria que rige internacionalmente la práctica de la profesión de Auditoría de SI

2.2 se presentan y discuten las versiones actualizadas del Código de Ética y los estándares, guías y procedimientos

2.3 se enfatiza sobre el rol y responsabilidades del auditor de SI

3. Explicar las fases del proceso de Auditoría de SI

3.1 se enumeran y explican las fases del proceso de Auditoría de SI

3.2 se enfatiza sobre la importancia de considerar como parte del análisis de auditoría aspectos tales como seguridad, eficiencia, eficacia y cumplimiento con leyes y reglamentos

3.3 se discuten las reglas y procedimientos generales para la recopilación, evaluación y documentación de la evidencia de auditoría

3.4 se discute sobre la importancia del informe final de auditoría, la opinión y las recomendaciones

3.5 se introduce el concepto de *auditoría continua* a través del proceso de seguimiento o “*follow up*”

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

4.1 se definen riesgo, control y otros conceptos clave relacionados dentro del ambiente de SI

4.2 se explica en qué consiste el modelo de Auditoría de SI basado en la evaluación y análisis de riesgo y su importancia para la planificación de proyectos

4.3 se define el concepto de *Gobierno Corporativo* y se explica su relación con el ambiente de control interno

4.4 se presentan y discuten ejemplos específicos de procedimientos de control y seguridad, tanto generales como los aplicables a los distintos sub-sistemas dentro de los SI o redes

4.5 se explica la importancia de los procesos de resguardo, planes de contingencia, planes de respuesta a emergencias y recuperación en caso de desastres y su relación con la continuidad de las operaciones

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

5.1 se presentan y discuten ejemplos comunes de la metodología y herramientas actuales para llevar a cabo un proyecto de Auditoría de SI

5.2 se expone brevemente sobre las nuevas tendencias y el futuro de la profesión

5.3 se desarrollan ejercicios prácticos de evaluación y recomendaciones sobre aspectos específicos dentro de los SI o redes

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

6.1 se discuten aspectos relacionados al diseño e implementación de las políticas de seguridad de SI o redes

6.2 se definen conceptos relacionados a seguridad de la información tales como privacidad, confidencialidad, integridad y disponibilidad

6.2 se estudian ejemplos de leyes actuales que rigen la implementación de mecanismos de seguridad de la información

6.3 se desarrollan ejercicios prácticos de evaluación y recomendaciones sobre políticas de seguridad de 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

a. Tipos de auditoría

b. Programas de auditoría

c. Metodología de la auditoría

d. Detección de fraude

e. Materialidad y riesgo de auditoría

f. Técnicas para el análisis de riesgo

g. Objetivos de la auditoría

h. Pruebas de auditoría: cumplimiento / detalle

i. Evidencia y muestreo

j. Herramientas computarizadas para asistir en la auditoría (CAAT’s)

k. Evaluación de los resultados de la auditoría: limitaciones, debilidades y fortalezas

l. Comunicación de resultados

m. Recomendaciones y seguimiento (“follow up”)

n. Documentación

o. 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.** ESTRATEGIAS DE ENSEÑANZA Y **Actividades**

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 |

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 XT. 2306.*

* 1. 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.*

* 1. 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**

**Textos**

Gallegos, F., [et al.], (2004). *Information Technology Control and Audit*

*2ed.* Auerbach Publications, CRC Press LLC.

Merkow M., Breithaupt, J., (2006). *Information Security Principles and*

*Practices 1ed.* Upper Saddle River, NJ. Prentice Hall.

**Lecturas Suplementarias**

*CISA Review Manual*. (2006). Information Systems Audit and Control

Association.

*CobiT Framework, 4 ed.* (2005). IT Governance Institute.

**IX. Bibliografía**

**Libros**

Whitman, M., Mattord, H., (2005). *Readings and Cases in the*

*Management of Information Security.* Boston, MA. Course Technology.

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

Prentice Hall.

*Information Technology Controls.* (2006). The Institute of Internal Auditors.

**Recursos Electrónicos**

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

**OPAC/VAAEPS**

**Rev. 10/2004; 08/2008; 03/2009; 08/2009**