

**UNIVERSIDAD INTERAMERICANA DE PUERTO RICO  
RECINTO METROPOLITANO  
DEPARTAMENTO DE GRADUADO  
FACULTAD DE EMPRESAS**

**PRONTUARIO**

**I. INFORMACIÓN GENERAL**

<b>Título del Curso</b>	:	Seguridad de la Información, la Privacidad y el Cumplimiento Normativo
<b>Código y Número</b>	:	BADM 6285
<b>Créditos</b>	:	Tres (3)
<b>Término Académico</b>	:	
<b>Profesor</b>	:	
<b>Lugar y Horas de Oficina</b>	:	
<b>Teléfono de la Oficina</b>	:	
<b>Correo Electrónico</b>	:	

**II. DESCRIPCIÓN**

Análisis de las tecnologías de información existentes para hacer cumplir con las políticas, procedimientos y controles en el manejo de los riesgos de la información de acuerdo con las exigencias legales y éticas. Énfasis en la seguridad y auditoría de la información en las empresas, la privacidad y el cumplimiento normativo de la Gobernabilidad de la Información (GI) emergente que se aplica a la gerencia de documentos electrónicos y a la entrada y a la salida de información.

**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 sistemas de información y su desarrollo como disciplina:
2. Explicar los aspectos reglamentarios que rigen la práctica de la Auditoría de sistemas de información:
3. Explicar las fases del proceso de Auditoría de los sistemas de información:
4. Entender desde una perspectiva histórica los fundamentos e importancia de la Seguridad de sistemas de información y su desarrollo como disciplina
5. Entender el concepto de análisis de riesgo:

6. Explicar los aspectos reglamentarios que rigen seguridad de sistemas de información:
7. Comparar el modelo de Auditoría de sistemas de información basado en la evaluación y análisis de riesgo Vs. El modelo de análisis de riesgo dictado por el campo de seguridad de sistemas de información:
8. Comparación de la metodología y herramientas actuales en un proyecto de Auditoría Vs la metodología de los mecanismos de seguridad en los sistemas de información:
9. Evaluar y recomendar desde el punto de vista de auditoría sobre las políticas de seguridad y control diseñadas para los sistemas de información, redes de comunicación y redes sociales en aquellos ambientes que son operacionales integrando aquellos procedimientos recomendados en el área de seguridad:

#### **IV. CONTENIDO**

- A. Introducción a la Auditoría de Sistemas de Información
  1. Definición e historia de la auditoría y de la seguridad de los sistemas de información
  2. La función de la auditoría y de la seguridad dentro de la organización
  3. La administración de los recursos de auditoría y de seguridad
  4. Planificación de la función de auditoría de los sistemas de información
  5. Planificación de la seguridad en los sistemas de información
- B. Estructura reglamentaria
  1. Reglamentación a nivel internacional: ISACA
  2. Reglamentaciones de los profesionales de seguridad en los sistemas de información
  2. Certificaciones profesionales
  3. Código de Ética para los profesionales de la auditoría y de seguridad
  4. Leyes, Estándares, guías y procedimientos
- C. Introducción a la Seguridad de Sistemas de Información
  1. Definición e historia de Seguridad en los sistemas de Información
  2. El papel que juega la función de la Seguridad de los sistemas de información dentro de la organización
  3. La administración de los recursos de la seguridad de sistemas de información
  4. Planificación de la función de Seguridad
  5. Planificación de proyectos: Consideraciones legales y reglamentarias
- D. El proceso de Auditoría de sistemas de información
  - 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. Control interno
- 1. Definición de control dentro del ambiente de sistemas de información
  - 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 sistemas de información
  - 6. Procedimientos generales de control
  - 7. Procedimientos de control de las aplicaciones
- E. Seguridad Lógica
- 1. Fundamentos de seguridad de la información
  - 2. Diseño, implementación y mantenimiento de políticas de seguridad
    - a. "*Security awareness*"
    - b. "*Security development and contributors*"
    - c. "*Security security policies*"
    - d. "*Security network policies*"
  - 4. Organización de Seguridad
  - 5. Autenticación y autorización
  - 6. Manejo de las políticas derecho de la información
  - 7. Seguridad para el almacenamiento de los datos e información
  - 8. Modalidades actuales de seguridad de la información
- F. Seguridad Física
- 1. tipos de activos (assets)
  - 2. Avalúo de vulnerabilidades físicas
  - 3. Selección de sitios seguros
  - 4. plan de seguridad de activos
  - 5. Cumplimiento de estándares
- G. Nuevas tendencias en la práctica Seguridad
- 1. Seguridad en infraestructuras de servicios:
    - a. Email
    - b. Web Servers
    - c. DNS Servers
    - d. Proxy Servers
  - 2. Virtual Machines and Cloud Computing

3. Dispositivos Móviles

**V. 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

### A. 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 la Oficina de la Coordinadora de servicios a estudiantes con impedimentos, la Dra. María de los Ángeles Cabello. Ella está ubicada en el Programa de Orientación y Consejería, Oficina 111, en el primer piso del edificio John Will Harris, extensión 2306.

### B. 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.

### C. 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.

### D. Cumplimiento con las disposiciones del Título IX

La Ley de Educación Superior Federal, según enmendada, prohíbe el discrimen por razón de sexo en cualquier actividad académica, educativa, extracurricular, atlética o en cualquier otro programa o empleo, auspiciado o controlado por una institución de educación superior independientemente de que esta se realice dentro o fuera de los predios de la institución, si la institución recibe fondos federales.

Conforme dispone la reglamentación federal vigente, en nuestra unidad académica se ha designado un(a) Coordinador(a) Auxiliar de Título IX que brindará asistencia y orientación con relación a cualquier alegado incidente constitutivo de discrimen por sexo o género, acoso sexual o agresión sexual. Se puede comunicar con el Coordinador(a) Sr. George Rivera, extensión 2262 – 2147, o al correo electrónico [\\_griverar@metro.inter.edu](mailto:_griverar@metro.inter.edu).

El Documento Normativo titulado **Normas y Procedimientos para Atender Alegadas Violaciones a las Disposiciones del Título IX** es el documento que contiene las reglas

institucionales para canalizar cualquier querrela que se presente basada en este tipo de alegación. Este documento está disponible en el portal de la Universidad Interamericana de Puerto Rico ([www.inter.edu](http://www.inter.edu)).

## **VIII. RECURSOS EDUCATIVOS**

### **Textos**

Mark Rhodes-Ousley, (2013), *The Complete Reference Information Security*, 2<sup>nd</sup>. ed. McGraw Hill Osborne, ISBN-978-0-07-178435

### **Lecturas Suplementarias**

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

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

## **IX. BIBLIOGRAFÍA (O REFERENCIAS)**

### **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)