UNIVERSIDAD INTERAMERICANA DE PUERTO RICO
RECINTO METROPOLITANO
FACULTAD DE CIENCIAS Y TECNOLOGÍA
DEPARTAMENTO DE CIENCIAS DE COMPUTADORAS Y MATEMÁTICAS

PROGRAMA DE CIENCIAS DE COMPUTADORAS

PRONTUARIO

I. INFORMACIÓN GENERAL

Título del Curso	**:**	**SEGURIDAD COMPUTACIONAL**
Código y Número	**:**	**COMP 4410**
Créditos	**:**	**Tres (3)**
Término Académico	**:**	
Profesor	**:**	
Horas de Oficina	**:**	
Teléfono de la Oficina	**:**	
Correo Electrónico	**:**	

II. DESCRIPCIÓN

Análisis de los fundamentos para la detección de riesgos y amenazas contra los sistemas computacionales. Evaluación de la vulnerabilidad de sistemas computacionales. Aplicación de controles y métodos de protección en el funcionamiento seguro y confiable en un sistema de información. Requiere 45 horas de conferencia-laboratorio. Requisito: COMP 3300.

III. OBJETIVOS

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

1. Identificar los riesgos, ataques, amenazas y vulnerabilidades involucrados en el uso de tecnología computacional.
2. Describir protocolos para el intercambio de información en forma segura.
3. Analizar formas de verificación de seguridad en la programación.
4. Analizar medidas y protocolos de seguridad de los sistemas operativos.
5. Señalar los tipos de defensas disponibles para controlar las amenazas a las que se expone un sistema computacional.
6. Investigar los aspectos éticos-legales y sus implicaciones en la seguridad de los sistemas computadorizados.
7. Manifestar una actitud crítica y creativa hacia la solución de problemas mediante la implementación de conocimientos relacionados con la seguridad computacional.

IV. CONTENIDO TEMÁTICO

A. Conceptos básicos de seguridad
   1. Confidencialidad, integridad, disponibilidad
   2. Riesgos, ataques, amenazas y vulnerabilidades
   3. Defensas y controles

B. Criptografía
   1. Tipos de cifrado: Simétricos, Asimétricos, de sustitución, de transposición
   2. Algoritmos; DES, AES, RSA, MD5
   3. Protocolos: Firmas digitales, Intercambio de llaves, certificados, funciones hash

C. Seguridad en programas
   1. Errores de programación: "buffer overflow", validación, tiempos de verificación y tiempo de utilización
   2. Código maligno: Virus, caballos de Troya, gusanos, puertas traseras
   3. Controles en el desarrollo y técnicas de verificación

D. Seguridad en Sistemas Operativos
   1. Métodos de protección
   2. Protección de memoria, archivos y ambiente de ejecución
   3. Controles de acceso físico
   4. Protección de archivos. Permisos. Protección basada en permisos por objeto, por usuario y localidad
   5. Identificación y autenticación

E. Políticas de seguridad
   1. Modelos de seguridad

F. Seguridad en redes
   1. Conceptos básicos: comunicación, medios, protocolos, direccionamiento, enrutamiento, topologías
   2. Amenazas: vulnerabilidades, fallas en protocolos, falsificación de identidad y conexiones
   3. Ataques: negación de servicio, robo de sesiones, modificación de datos, codificación de mensajes
   4. Controles: arquitectura, criptografía, acceso, alarmas, alertas
   5. Tecnologías de protección

G. Procesos corporativos de seguridad
   1. Análisis de riesgos
   2. Planificación

H. Aspectos legales y éticos
   1. Protección de programas y datos
   2. Privacidad
   3. Crimen computacional

V. ACTIVIDADES

A. Conferencia
B. Discusión socializada
C. Foros
D. Proyectos de investigación
E. Discusión de libros o artículos
F. Estudio de casos
G. Simulaciones
H. Trabajo individual
I. Informes orales
J. Informes escritos
K. Ejercicios de búsqueda de información

VI. EVALUACIÓN

Criterio	Puntuación	% de la Nota Final
Exámenes	100	80
Asignaciones	100	10
Proyectos	100	10
Total	300	100

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 _____.

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 Titulo 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) Auxiliar, George Rivera, Director de Seguridad, al teléfono 787-250-1912, extensión 2147, o al correo electrónico grivera@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 querella 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).

VIII. RECURSOS EDUCATIVOS

Libro(s) de Texto

Pfleeger, C. P. & Pfleeger, S. L. (2011). *Analyzing Computer Seciruty: A Threat / Vulnerability / Countermeasure Approach* (1st ed.). Upper Saddle River, NJ: Prentice Hall. ISBN-10: 0132789469, ISBN-13: 978-0132789462

Lecturas Suplementarias

Recursos Audiovisuales

Recursos Electrónicos (incluir título o nombre y dirección URL)

AV-Comparatives http://www.av-comparatives.org/

SANS.Org http://www.sans.org/

"CERT Coordination Center," at Carnegie Mellon University http://www.cert.org/

United State Computer Emergency Readiness Team (US-CERT) http://www.us-cert.gov/

"Information Security Group (ISG)," Royal Holloway, University of London http://www.isg.rhul.ac.uk/

Security Focus http://www.securityfocus.com/

Linux Security http://www.linuxsecurity.com/

Microsoft Security http://www.microsoft.com/security/

"Glossary," Microsoft Security http://www.microsoft.com/security/glossary.mspx

Threat Level http://www.wired.com/threatlevel.

IX. BIBLIOGRAFÍA

Stallings, W. (2010). Cryptography and Network Security: Principles and Practices (5th ed.). Upper Saddle River, NY: Prentice Hall. ISBN-10: 0136097049, ISBN-13: 978-0136097044

Stallings, W. (2010). Network Security Essentials: Applications and Standards (4th ed.). Upper Saddle River, NY: Prentice Hall. ISBN-10: 0136108059, ISBN-13: 978-0136108054

Gollmann, D. (2010). Computer Security (3rd ed.). United States: John Wiley & Sons. ISBN-10: 0470741155, ISBN-13: 978-0470741153

Goldreich O. (2009). Foundations of Cryptography: Volume 2, Basic Applications. Cambridge University Press. ISBN-10: 052111991X, ISBN-13: 978-0521119917
.