Universidad de Puerto Rico en Bayamón
#170 Carr. 174 Parque Industrial Minillas
Bayamón, PR 00959
Tels. (787) 993-8853, (787) 993-0000, Ext. 3035 o 3037, Fax (787) 993-8900

Senado Académico
Secretaría

CERTIFICACIÓN NÚM. 39-2015-2016

Yo, Arnaldo Rodríguez Rivera, secretario ejecutivo del Senado Académico de la Universidad de Puerto Rico en Bayamón, **CERTIFICO QUE**:

> El Senado Académico, en reunión ordinaria celebrada el 18 de febrero de 2016, encomendó al *Comité de evaluación de cursos* evaluar el curso *COTI 4260 – Seguridad de la Información*, sometido por el Departamento de Ciencias de Computadoras.

Y PARA QUE ASÍ CONSTE, expido la presente certificación en Bayamón, Puerto Rico, hoy 26 de febrero de 2016.

Arnaldo Rodríguez Rivera
Secretario Ejecutivo

Vo.Bo. Margarita Fernández Zavala
Rectora

Universidad de Puerto Rico en Bayamón
Decanato de Asuntos Académicos
Departamento de Ciencias Computadoras
Programa de Bachillerato en Ciencias Computadoras

PRONTUARIO

A. TÍTULO DEL CURSO: Seguridad de la Información

B. CODIFICACIÓN: COTI 4260

C. CRÉDITOS: 3

D. HORAS DE CONTACTO: 3 horas semanales

E. PRERREQUISITOS: SICI 4036 Estructuras de Datos

F. COREQUISITOS: Ninguno

G. DESCRIPCIÓN DEL CURSO:

Este curso provee un vistazo general de la seguridad de la información. El contenido técnico del curso discute conceptos esenciales y métodos para proveer y evaluar la seguridad en sistemas de procesamiento de información, incluyendo la seguridad de los sistemas operativos, redes, aplicaciones y el web. Además, casos de estudio serán utilizados para presentar la ética del manejo de la información y el impacto que las decisiones administrativas tienen en nuestra sociedad.

H. OBJETIVOS DEL CURSO:

Al finalizar el curso, el estudiante:

1. Conocerá el desarrollo histórico relacionado a la seguridad de la información.
2. Conocerá la los conceptos de "information assurance", seguridad de la información, seguridad de las computadoras, seguridad en las redes, y seguridad en la Internet.
3. Podrá explicar los conceptos relacionados a la criptografía, las cuatro técnicas de criptoanálisis, criptografía simétrica y asimétrica, firmas digitales, códigos de autenticación de mensajes, funciones "hash" y modos de encriptación y des encriptación.
4. Conocerá y podrá distinguir la diferencia entre las distintas definiciones sobre el concepto de "hackers" y la terminología relacionada a la seguridad de la información
5. Comprenderá los conceptos sobre código malicioso y cómo protegerse del mismo.
6. Podrá analizar las implicaciones legales, éticas y sociales del manejo de los sistemas de información.
7. Podrá entender el concepto de desbordamiento de "buffer" y cómo crear programado que reduzca este efecto.
8. Conocerá conceptos sobre la seguridad de los sistemas operativos.
9. Conocerá la diferencia entre cifradores en bloque y de ráfagas
10. Podrá entender los conceptos de confusión y difusión que se utilizan en los cifradores actuales.

11. Conocerá los conceptos de seguridad en las redes actuales con especial énfasis en los protocolos HTTPS, Secure HTTP, Secure Socket Layer (SSL), Transport Layer Security (TLS) y Secure Shell (SSH).
12. Podrá explicar los conceptos y maneras en las cuales los sistemas operativos y los anti-virus manejan el código confiable y no confiable.
13. Tendrá la capacidad de analizar, diseñar e implementar tecnologías relacionadas a la protección de la información.
14. Podrá describir los requisitos de seguridad para los sistemas de información, garantizando confiabilidad, integridad y secretividad.
15. Podrá analizar la pertinencia en la aplicabilidad de los mecanismos y servicios enfocados a proteger la información.

I. CONTENIDO DEL CURSO:

Tema	*Horas*
1. Introducción a la seguridad de la información y campos relacionados	6

a. Definiciones de los campos de: seguridad de la información, seguridad de la computación, seguridad en las redes y seguridad de la Internet
b. El concepto de "information assurance" y su importancia
c. Confiabilidad, integridad y disponibilidad
d. Seguridad comprometida y su nivel de impacto
e. Ataques comunes
f. Relación entre servicios y mecanismos
g. Modelo general de la seguridad de la información

2. Conceptos básicos y definiciones — 6

a. "Hackers" y su real definición
b. Botnet y su impacto
c. Adware, spyware, malware
d. Ataque del día cero
e. Mpack y el ataque del banquero silencioso
f. La economía subterránea relacionada a los "hackers"
g. Vulnerabilidades comunes

3. Ética del manejo de la seguridad de la información computadorizada — 6

a. Responsabilidades que acarrea la seguridad
b. El uso del conocimiento para propósitos benévolos
c. Consecuencias criminales
d. El virus Melissa y la convicción de su creador
e. Dmitry Sklyarov vs. Adobe
f. La convicción de "The Analyzer" y el fraude bancario
g. Estudio de casos: Ron Harris y Gaming Control Board
h. Estudio de casos: El escándalo de la copa "Breeders"

4. Criptografía, Criptoanálysis y cifradores 3.5
    a. Definiciones y conceptos básicos sobre criptografía y criptoanálisis
    b. Ataques cripto analíticos
    c. Ataques de fuerza bruta
    d. Encriptación de llave privada o simétrica

5. Evolución de los cifradores y decifradores 4.5
    a. Historia de los cifradores
    b. Ventajas y desventajas de los cifradores y decifradores
    c. El cifrador de Julio Cesar
    d. Cifradores mono-alfabéticos
    e. Los idiomas humanos y la peculiaridad del uso de las letras
    f. Dígrafos, Triglifos y sus frecuencias
    g. Seguridad incondicional y seguridad computacional
    h. El cifrador de Playfair y su importancia en la Primera y Segunda Guerra Mundial
    i. Cifradores poli-alfabéticos
    j. Cifrador de Vigeneré
    k. El metodo de Kasiski
    l. Cifradores de autoclave
    m. Cifradores Vernam
    n. Cifradores "one-time pad"
    o. Cifradores de transposición
    p. Máquinas rotativas y su relación con la historia.

6. Cifradores Modernos y en Bits 3
    a. Cifradores en bloque vs. cifradores de ráfagas
    b. Principios de cifradores en bloque
    c. Servicios de autenticación y secretividad
    d. Cifradores de permutación y sustitución de Claude Shannon
    e. Principios de confusión y difusión
    f. La creación de servicios combinados
    g. Estructura y elementos del cifrador de Feistel
    h. "DES Data Encryption Standard"
    i. El efecto avalancha
    j. Ataques comunes al DES
    k. RC4

7. Teoría de números y bases matemáticas para los mecanismos de seguridad modernos 6
    a. Generación de números aleatorios y su relación con los sistemas de seguridad
    b. Usando cifradores para generar números aleatorios
    c. Números y factorización prima
    d. Primos relativos y el mayor común divisor
    e. Teorema de Fermat
    f. La función y teorema de Euler
    g. Algoritmo Miller Rabin
    h. La distribución de los números primos

i. Teorema chino del residuo
j. Las raíces primitivas
k. Logaritmos discretos

8. Llaves Publicas y Privadas 4
   a. Llaves publicas vs encriptación simétrica
   b. Intercambio de llaves Diffie-Hellman
   c. Protocolos de intercambio de llaves
   d. Criptografía de curva elíptica

9. "Firewalls" y Posibles Amenazas 3
   a. Amenazas modernas a la seguridad de la información
   b. Políticas de seguridad
   c. Sistemas de detección de Intrusos
   d. Firewalls
   e. Firewalls sencillo, doble y paralelo

10. Seguridad para el Web 3
   a. Seguridad para la capa de HTTP
   b. Seguridad en la capa de IP
   c. El protocolo SSL y seguridad en la capa de transporte
   d. Importancia de los cifradores y el protocolo SSL
   e. Protocolo de transferencia de hipertexto seguro (HTTPS)
   f. "Secure Shell vs. Telnet"
   g. Códigos de autenticación del medio
   h. Funciones de hash importantes para seguridad de la Web

11. Esteganografía 3
   a. Historia
   b. Conceptos
   c. Maneras análogas
   d. Esconder un mensaje dentro de una imagen
   e. Esconder una imagen dentro de una imagen
   f. Estenografía usando la red

J. ESTRATEGIAS INSTRUCCIONALES:
   1. Conferencias
   2. Presentaciones en PowerPoint
   3. Material didáctico Web 2.0 : videos, animaciones y artículos en línea
   4. Debate sobre casos reales

K. RECURSOS DE APRENDIZAJE O INSTITUCIONALES:

1. Laboratorio con una computadora asignada a cada estudiante
2. Herramientas de desarrollo de programas
3. Disco o *USB Flash Drive* personal para almacenar los programas escritos

L. ESTRATEGIAS DE EVALUACIÓN:

1. Exámenes parciales y/o pruebas cortas	40%
2. Proyectos y/o programas	40%
3. Asignaciones	20%
TOTAL	100%

M. INTEGRIDAD ACADÉMICA:

La Universidad de Puerto Rico promueve los más altos estándares de integridad académica y científica. El Artículo 6.2 del Reglamento General de Estudiantes de la UPR (Certificación Núm. 13, 2009-2010, de la Junta de Síndicos) establece que "la deshonestidad académica incluye, pero no se limita a: acciones fraudulentas, la obtención de notas o grados académicos valiéndose de falsas o fraudulentas simulaciones, copiar total o parcialmente la labor académica de otra persona, plagiar total o parcialmente el trabajo de otra persona, copiar total o parcialmente las respuestas de otra persona a las preguntas de un examen, haciendo o consiguiendo que otro tome en su nombre cualquier prueba o examen oral o escrito, así como la ayuda o facilitación para que otra persona incurra en la referida conducta". Cualquiera de estas acciones estará sujeta a sanciones disciplinarias en conformidad con el procedimiento disciplinario establecido en el Reglamento General de Estudiantes de la UPR vigente.

N. SISTEMA DE CALIFICACIÓN:

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

O. TEXTO Y REFERENCIAS:

Texto:

Stallings, W. (2011). *Cryptography and network security: Principles and practice* (5th ed.). Upper Saddle River, N.J.: Prentice Hall.

Referencias:

Anderson, R. (2009). *Security engineering: A guide to building dependable distributed systems* (2nd ed.). New York: Wiley. Disponible electrónicamente en http://www.cl.cam.ac.uk/~rja14/book.html

Baase, S. (2013). *A gift of fire: Social, legal, and ethical issues for computing technology* (4th ed.). Upper Saddle River, NJ: Pearson.

Bishop, M. (2005). *Introduction to computer security.* Boston: Addison-Wesley.

Bynum, T. (2004). *Computer ethics and professional responsibility.* Malden, MA: Blackwell Pub.

Easttom, W. (2012). *Computer Security Fundamentals (2nd Edition). Paperback.* Pearson Certification

Gollmann, D. (2011). *Computer Security Paperback (3rd Edition).* John Wiley & Sons.

Hodeghatta U. (2014). *The Infosec Handbook: An Introduction to Information Security Paperback.* Apress open.

Infosecurity. (2015). *Infosecurity Magazine Webminars.* Disponible electrónicamente en http://www.infosecurity-magazine.com

ISF. (2015). *Information Security Forum.* Disponible electrónicamente en https://www.securityforum.org/

ISSA forum (2015). *Information System Security Association.* Disponible electrónicamente en https://www.issa.org/

Pfleeger, C. (2003). *Security in computing* (3rd ed.). Upper Saddle River, NJ: Prentice Hall PTR.

Stallings, W. (2014). *Computer Security: Principles and Practice* (3rd Edition). Upper Saddle River, NJ: Prentice Hall PTR.

P. LEY ADA Y LEY 51:

La Universidad de Puerto Rico en Bayamón está comprometida con el cumplimiento de la Ley de Rehabilitación Vocacional de 1973, Sección 504 (Acomodo Razonable), y la Ley ADA (*American with Disabilities Act*) de 1990, las cuales aseguran que los estudiantes con impedimentos tengan igual acceso a las oportunidades educacionales en la universidad. Todo estudiante que requiera un acomodo razonable debido al impacto de su impedimento, deberá visitar la Oficina de Servicios para Estudiantes Universitarios con Impedimentos (OSEUI), ubicada en el primer piso del Centro de Estudiantes, al lado de la Cafetería, para someter evidencia médica actualizada que le requiera la oficina para la otorgación de los acomodos razonables y otros servicios.

A solicitud del estudiante, la OSEUI preparará una carta individualizada para cada profesor. Esta carta certifica que el estudiante tiene un impedimento y presenta los acomodos razonables que requiere el estudiante para la obtención de un adecuado aprovechamiento académico. Los estudiantes son responsables de reunirse con cada uno de sus profesores al inicio de cada semestre académico para discutir las implicaciones académicas de su impedimento, cómo está relacionado con algunos cursos en específico y a solicitar los acomodos razonables.