Universidad Católica San Pablo
Facultad de Ingeniería y Computación
Escuela Profesional de
Ciencia de la Computación
SILABO

CS336. Seguridad en Computación (Obligatorio)

2010-1

1. DATOS GENERALES		
1.1 CARRERA PROFESIONAL	:	Ciencia de la Computación
1.2 ASIGNATURA	:	CS336. Seguridad en Computación
1.3 SEMESTRE ACADÉMICO	:	7^{mo} Semestre.
1.4 PREREQUISITO(S)	:	CS103O. Algoritmos y Estructuras de Datos. (4^{to} Sem)
1.5 CARÁCTER	:	Obligatorio
1.6 HORAS	:	1 HT; 2 HP; 2 HL;
1.7 CRÉDITOS	:	3

2. DOCENTE

3. FUNDAMENTACIÓN DEL CURSO

Hoy en dia la información es uno de los activos más preciados en cualquier organización. Este cursos está orientado a poder brindar al alumno los elementos de seguridad orientados a proteger la información de la organización y principalmente poder preveer los posibles problemas relacionados con este rubro. Esta materia involucra el desarrollo de una actitud preventiva por parte del alumno en todas las áreas relacionadas al desarrollo de software.

4. SUMILLA

1. PF/Fundamentos de seguridad de la Información.2. PF/Programación segura.3. OS/Modelos de seguridad.4. AL/Algoritmos Criptográficos.5. NC/Seguridad de Red.6. NC/Administración de Redes.7. Factores humanos y seguridad.8. SP/Operaciones de seguridad.9. PL/Máquinas Virtuales.

5. OBJETIVO GENERAL

- Discutir a un nivel intermedio avanzado los los fundamentos de la Seguridad Informática.
- Brindar los diferentes aspectos que presenta el código malicioso.
- Que el alumno conozca los conceptos de criptografía y seguridad en redes de computadoras.
- Discutir y analizar junto con el alumno los aspectos de la Seguridad en Internet.

6. CONTRIBUCIÓN A LA FORMACIÓN PROFESIONAL Y FORMACIÓN GENERAL

Esta disciplina contribuye al logro de los siguientes resultados de la carrera:

a) Aplicar conocimientos de computación y de matemáticas apropiadas para la disciplina. [**Nivel Bloom: 3**]

b) Analizar problemas e identificar y definir los requerimientos computacionales apropiados para su solución. [**Nivel Bloom: 4**]

c) Diseñar, implementar y evaluar un sistema, proceso, componente o programa computacional para alcanzar las necesidades deseadas. [**Nivel Bloom: 4**]

g) Analizar el impacto local y global de la computación sobre los individuos, organizaciones y sociedad. [**Nivel Bloom: 4**]

h) Incorporarse a un proceso de aprendizaje profesional continuo. [**Nivel Bloom: 3**]

i) Utilizar técnicas y herramientas actuales necesarias para la práctica de la computación. [**Nivel Bloom: 4**]

j) Aplicar la base matemática, principios de algoritmos y la teoría de la Ciencia de la Computación en el modelamiento y diseño de sistemas computacionales de tal manera que demuestre comprensión de los puntos de equilibrio involucrados en la opción escogida. [**Nivel Bloom: 3**]

7. CONTENIDOS

UNIDAD 1: PF/Fundamentos de seguridad de la Información.(4 horas)

Nivel Bloom: 4

OBJETIVO GENERAL	**CONTENIDO**
▪ Explicar los objetivos de lse seguridad de la información. ▪ Analizar los puntos de equilibrio inherentes a la seguridad. ▪ Explicar la importancia y las aplicaciones de la confidencialidad, integridad y disponibilidad. ▪ Entender las categorías básicas de las amenazas a las computadoras y redes. ▪ Discutir problemas para crear políticas de seguridad para una organización de gran tamaño. ▪ Defender la necesidad de ls protección y la seguridad y el rol de consideraciones éticas en el uso de computadores.	▪ Rol y propósito de de la seguridad en las computadoras y redes. ▪ Objetivos de seguridad: confidencialidad, integridad y disponibilidad. ▪ Políticas y estándares de seguridad. ▪ Mentalidad orientada a la seguridad. ▪ Defensa en profundidad. ▪ Amenazas comunes: *worms*, virus, troyanos, bloqueo de acceso a servicios. ▪ Estimación de riesgos y análisis de costo beneficio. ▪ Seguridad vs usabilidad.

Lecturas: [Department of Defense, 1985], [Spafford, 1998], [Tinto, 1989], [Russel and Gangemi, 1991], [of Computer Engineering, 1995]

UNIDAD 2: PF/Programación segura.(4 horas)	
Nivel Bloom: 4	
OBJETIVO GENERAL	**CONTENIDO**
▪ Reescribir un simple programa para remover una simple vulnerabilidad. ▪ Explicar porque es o no es posible el desborde en un lenguaje de programación de dominio del estudiante. ▪ Explicar porque una o más construcciones de lenguaje pueden originar problemas de seguridad como desborde.	▪ Validaciones importantes para evitar desbordes en array y cadenas. ▪ Construcciones en lenguajes de programación para evitar problemas de seguridad. ▪ ¿Cómo los atacantes usan el desborde para destruir la pila (*stack*) en tiempo de ejecución.
Lecturas: [Ramió Aguirre, 1999]	

UNIDAD 3: OS/Modelos de seguridad.(4 horas)	
Nivel Bloom: 4	
OBJETIVO GENERAL	**CONTENIDO**
▪ Comparar y contrastar métodos existentes para la implementación de seguridad. ▪ Comparar y contrastar las fortalezas y debilidades de dos o más sistemas operativos actuales con respecto a la seguridad. ▪ Comparar y contrastar las fortalezas y debilidades en seguridad de dos o más sistemas operativos actuales con respecto a la gestión de la recuperación. ▪ Describir la matriz de control de accesos y como esta se relaciona la Lista de control de accesos (*Access Control Lists*-ACLs.) y a las listas de capacidades (C-*Lists*) ▪ Aplicar el modelo de Biba para el chequeo de las entradas de un programa (contaminada y descontaminada por ejemplo). ▪ Describir como el modelo Bell-LaPadula combina mecanismos de control de acceso obligatorios y a discresión así como explicar la formulación de *lattice* de Bell-LaPadula y Biba. ▪ Comparar y contrastar dos modelos de seguridad. ▪ Relacionar modelos de seguridad particular con los modelos del ciclo de desarrollo de software. ▪ Aplicar modelos particulares a diferentes entornos y seleccionar el modelo que mejor captura el entorno.	▪ Modelos de protección. ▪ Protección de memoria. ▪ Encriptación. ▪ Gestión de la recuperación. ▪ Tipos de control de acceso: obligatorio, a discresión, controlado por el origen, basado en el rol. ▪ Modelo de matriz de control de acceso. ▪ El modelo Harrison-Russo-Ullman y la indecisión en temas de seguridad. ▪ Modelos de confidencialidad tales como Bell-LaPadula. ▪ Modelos de integridad tales como Biba y Clark-Wilson. ▪ Modelos de conflicto de interés tales como la muralla china.
Lecturas: [Ramió Aguirre, 1999]	

UNIDAD 4: AL/Algoritmos Criptográficos.(4 horas)	
Nivel Bloom: 3	
OBJETIVO GENERAL	**CONTENIDO**
▪ Describir algoritmos numérico-teóricos básicos eficientes, incluyendo el máximo común divisor, inversa multiplicativa mod n y elevar a potencias mod n. ▪ Describir al menos un cripto-sistema de llave pública, incluyendo una suposición necesaria de complejidad teórica sobre su seguridad. ▪ Crear extensiones simples de protocolos criptográficos, usando protocolos conocidos y primitivas criptográficas.	▪ Revisión histórica de la criptografía. ▪ Criptografía de llaves privadas y el problema del intercambio de llaves. ▪ Criptografía de llaves públicas. ▪ Firmas digitales. ▪ Protocolos de seguridad. ▪ Aplicaciones (pruebas de cero-conocimiento, autenticación y otros).
Lecturas: [Ramió Aguirre, 1999], [Stallings, 1999], [Seberry and Pieprzyk, 1989], [Caballero, 1996], [Fúster et al., 1997]	

UNIDAD 5: NC/Seguridad de Red.(8 horas)	
Nivel Bloom: 3	
OBJETIVO GENERAL	**CONTENIDO**
▪ Describir las mejoras hechas por el IPSec al IPv4. ▪ Identificar protocolos usados para mejorar la comunicación en Internet y escoger el protocolo apropiado para un determinado caso. ▪ Entender y detectar intrusiones. ▪ Discutir las ideas fundamentales de criptografía de clave pública. ▪ Describir como la criptografía de clave pública trabaja. ▪ Distinguir entre el uso de algoritmos de clave privada y pública. ▪ Resumir los protocolos comunes de autenticación. ▪ Generar y distribuir un par de claves PGP y usar el paquete PGP para enviar un mensaje de correo electrónico encriptado. ▪ Resumir las capacidades y limitaciones del significado de criptografía que se encuentran disponibles para el público en general. ▪ Describir y discutir recientes ataques de seguridad exitosos. ▪ Resumir las fortalezas y debilidades asociadas con diferentes abordajes de seguridad.	▪ Fundamentos de criptografía: a) Algoritmos de clave pública. b) Algoritmos de clave privada. ▪ Protocolos de autenticación. ▪ Firmas digitales y ejemplos. ▪ Tipos de ataques por red: negación de servicio (*Denial of service*), desborde *flooding*, *sniffing* y desvio de tráfico, ataques de integridad de mensajes, usurpación de identidad, ataques de vulnerabilidades (desborde de *buffers*, caballos de troya, puertas traseras), por dentro del ataque, infraestructura (secuestro de DNS, ruteo nulo- *route blackholing*, comportamiento inadecuado de ruteadores que descartan tráfico), etc. ▪ Uso de contraseñas y mecanismos de control de acceso. ▪ Herramientas y estrategias de defensa básica. a) Detección de intrusos. b) *Firewalls*. c) Detección de *malware*. d) Kerberos. e) IPSec. f) Redes privadas virtuales (*Virtual Private Networks*). g) Traducción de direcciones de red. ▪ Políticas de gerenciamiento de recursos en redes. ▪ Auditoría y *logging*.
Lecturas: [Bellovin, 1989], [FIPS PUB, 1994], [William, 1995], [ICSA Inc., 1998], [Neuman and Ts'o, 1994]	

UNIDAD 6: NC/Administración de Redes.(8 horas)	
Nivel Bloom: 3	
OBJETIVO GENERAL	**CONTENIDO**
▪ Explicar los asuntos de la administración de redes resaltando amenazas de seguridad, virus, gusanos, troyanos y ataques de negación de servicios. ▪ Desarrollar una estrategia para asegurar niveles apropiados de seguridad en un sistema diseñado para un propósito particular. ▪ Implementar un muro de fuego (*firewall*) de red.	▪ Vista general de la administración de redes. ▪ Uso de contraseñas y mecanismos de control de acceso. ▪ Nombres de dominio y servicios de nombre. ▪ Proveedores de servicio de Internet (ISPs). ▪ Seguridad y muros de fuego (*firewalls*). ▪ Asuntos de calidad de servicio: desempeño, recuperación de errores.
Lecturas: [Department of Defense, 1985], [NCSC, 1987], [Sandhu and Samarati, 1994], [Venerma, 1998]	

UNIDAD 7: Factores humanos y seguridad.(2 horas)	
Nivel Bloom: 4	
OBJETIVO GENERAL	**CONTENIDO**
▪ Explicar el concepto de *phishing* y como reconocerlo. ▪ Explicar el concepto de robo de identidad y cómo dificultarlo. ▪ Diseñar una interfaz de usuario con mecanismos de seguridad. ▪ Discutir procedimientos que ayuden a reducir un ataque de ingeniería social. ▪ Analizar una política de seguridad y/o procedimientos para mostrar donde funcionan y donde fallan. Hacer consideraciones de valor práctico.	▪ Psicología aplicada y políticas de seguridad. ▪ Diseño pensando en usabilidad y seguridad. ▪ Ingeniería social. ▪ Suplantación de indentidad. ▪ Adquisición de información confidencial de forma fraudulenta *Phishing*.
Lecturas: [Cano, 1998]	

UNIDAD 8: SP/Operaciones de seguridad.(8 horas)	
Nivel Bloom: 4	
OBJETIVO GENERAL	**CONTENIDO**
▪ Desarrollar un plan de recuperación de incidentes para manejar los compromisos de una organización. ▪ Analizar los procedimientos de seguridad establecidos en busca de puntos débiles que un atacante podría explotar y explicar como los mismos podrían fallar. ▪ Proponer medidas de seguridad apropiadas para diferentes situaciones. ▪ Explicar para una comunidad de usuarios no expertos en seguridad que medidas ellos deben seguir y porque en una situación en la que sus trabajos no sean realacionados con seguridad.	▪ Seguridad física. ▪ Control de acceso físico. ▪ Control de acceso de personal. ▪ Seguridad Operativa. ▪ Políticas de seguridad para sistemas/redes. ▪ Recuperación y respuesta. ▪ Manejando problemas técnicos y humanos.
Lecturas: [Ramió Aguirre, 1999]	

UNIDAD 9: PL/Máquinas Virtuales.(3 horas)	
Nivel Bloom: 2	
OBJETIVO GENERAL	**CONTENIDO**
▪ Explicar como los programas ejecutables pueden violar la seguridad de sistema computacional accediendo a archivos de disco y memoria.	▪ Temas de seguridad relacionados a ejecutar código sobre una máquina externa.
Lecturas: [Ramió Aguirre, 1999]	

8. METODOLOGÍA

El profesor del curso presentará clases teóricas de los temas señalados en el programa propiciando la intervención de los alumnos.

El profesor del curso presentará demostraciones para fundamentar clases teóricas.

El profesor y los alumnos realizarán prácticas

Los alumnos deberán asistir a clase habiendo leído lo que el profesor va a presentar. De esta manera se facilitará la comprensión y los estudiantes estarán en mejores condiciones de hacer consultas en clase.

9. EVALUACIONES

Evaluación Permanente 1 : 20 %

Examen Parcial : 30 %

Evaluación Permanente 2 : 20 %

Examen Final : 30 %

Referencias

[Bellovin, 1989] Bellovin, S. (1989). Security problems in the tcp/ip protocol suite. *ACM Computer Communications Review*, 19(2):32–48.

[Caballero, 1996] Caballero, P. (1996). *Introducción a la Criptografia*, volume Textos Universitarios. Ra-Ma.

[Cano, 1998] Cano, J. J. (1998). Pautas y recomendaciones para elaborar políticas de seguridad informática. Technical report, Universidad de Los Andes.

[Department of Defense, 1985] Department of Defense (1985). *Password Management Guideline (Green Book)*. Department of Defense. CSC-STD-002-85.

[FIPS PUB, 1994] FIPS PUB (1994). Guideline for the analysis of local area network security. Technical Report 191, FIPS PUB.

[Fúster et al., 1997] Fúster, A., De la Guía, D., Hernández, L., Montoya, F., and Muñoz, J. (1997). *Técnicas Criptográficas de Protección de Datos*. Ra-Ma.

[ICSA Inc., 1998] ICSA Inc. (1998). An introduction to intrusion detection and assessment. Technical report, ICSA Inc.

[NCSC, 1987] NCSC (1987). A guide to understanding discretionary access control in trusted systems. Technical report, National Computer Security Center. NCSC-TG-003.

[Neuman and Ts'o, 1994] Neuman, B. C. and Ts'o, T. (1994). Kerberos: An autentication service for computer networks. *IEEE Communications Magazine*, 32(9):33–38.

[of Computer Engineering, 1995] of Computer Engineering, D. (1995). A structured approach to computer security. Technical report, Chalmers University of Tecnology.

[Ramió Aguirre, 1999] Ramió Aguirre, J. (1999). *Aplicaciones Criptográficas*. Dpto. de Publicaciones EUI-UPM, segunda edición edition.

[Russel and Gangemi, 1991] Russel, D. and Gangemi, G. (1991). *Computer Security Basics*. O'Reilly and Associates.

[Sandhu and Samarati, 1994] Sandhu, R. S. and Samarati, P. (1994). Authentication, access control and intrusion detection. *IEEE Communications*, 32(9).

[Seberry and Pieprzyk, 1989] Seberry, J. and Pieprzyk, J. (1989). *Cryptography. An Introduction to Computer Security*. Prentice-Hall.

[Spafford, 1998] Spafford, E. H. (1998). The internet worm program: An analysis. Technical report, Purdue. CSD-TR-823.

[Stallings, 1999] Stallings, W. (1999). *Cryptography and Network Security. Principles and Practice*. Prentice Hall International Editions, segunda edición edition.

[Tinto, 1989] Tinto, M. (1989). Computer viruses: prevention, detection and treatment. Technical Report 001, National Computer Security Center.

[Venerma, 1998] Venerma, W. (1998). Tcpwrapper: networking monitoring, access control and booby traps. Technical report, Mathematics and Computing Science, Eindhoven University of Technology.

[William, 1995] William, S. (1995). *Network and Internetwork Security, Principles and Practice*. Prentice-Hall.