Universidad Nacional de San Agustín
VICE RECTORADO ACADÉMICO
SILABO

CODIGO DEL CURSO: CS336

1 Datos Generales

FACULTAD : Ingeniería de Producción y Servicios						
DEPARTAMENTO : Ingeniería de Sistemas e Informática			**ESCUELA :** Ciencia de la Computación			
PROFESOR : **TÍTULO :**						
ASIGNATURA : Seguridad en Computación						
PREREQUISITO: CS103O	**CREDITOS:** 4		**Año**: 2010-1 **Sem:** 7^{mo} Semestre.		**Total Horas:** 2 HT; 2 HT	2 HP 2 HL
Horario	Lun	Mar	Mie	Jue	Vie	Sáb
Total Semanal						
Aula						

2 Exposición de Motivos

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

2 Objetivo

- 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.

3 Contenido Temático

3 PF/Fundamentos de seguridad de la Información.(4 horas)

Objetivos Específicos

- Explicar los objetivos de
  dad de la información.
- Analizar los puntos de equ
  herentes a la seguridad.
- Explicar la importancia y
  caciones de la confidencia
  tegridad y disponibilidad.
- Entender las categorías l
  las amenazas a las compu
  redes.
- Discutir problemas para e
  ticas de seguridad para u
  zación de gran tamaño.
- Defender la necesidad d
  tección y la seguridad y
  consideraciones éticas en
  computadores.

3 PF/Programación segura.(4 horas)

Objetivos Específicos	Contenidos
▪ 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 ev tar desbordes en array y cadenas. ▪ Construcciones en lenguajes de pro gramación para evitar problemas d seguridad. ▪ ¿Cómo los atacantes usan el desbo de para destruir la pila (*stack*) e tiempo de ejecución. [11]

3 OS/Modelos de seguridad.(4 horas)

Objetivos Específicos	Contenidos
▪ 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: oblig torio, a discresión, controlado por origen, basado en el rol. ▪ Modelo de matriz de control de a ceso. ▪ El modelo Harrison-Russo-Ullman la indecisión en temas de segurida ▪ Modelos de confidencialidad tal como Bell-LaPadula. ▪ Modelos de integridad tales con Biba y Clark-Wilson. ▪ Modelos de conflicto de interés tal como la muralla china. [11]

3 AL/Algoritmos Criptográficos.(4 horas)

Objetivos Específicos	Contenidos
▪ 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 criptosistema 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 cript ▪ Criptografía de llaves privad problema del intercambio de ▪ Criptografía de llaves públic ▪ Firmas digitales. ▪ Protocolos de seguridad. ▪ Aplicaciones (pruebas de conocimiento, autenticaci otros). [11], [16], [14], [2], [6]

3 NC/Seguridad de Red.(8 horas)

Objetivos Específicos	Contenidos
▪ 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*. [1], [5], [19], [7], [9]

3 NC/Administración de Redes.(8 horas)

Objetivos Específicos	Contenidos
▪ 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 administ de redes. ▪ Uso de contraseñas y mecanis control de acceso. ▪ Nombres de dominio y servic nombre. ▪ Proveedores de servicio de In (ISPs). ▪ Seguridad y muros de fuego *walls*). ▪ Asuntos de calidad de se desempeño, recuperación de e [4], [8], [13], [18]

3 Factores humanos y seguridad.(2 horas)

Objetivos Específicos	Contenidos
▪ 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 guridad. ▪ Diseño pensando en usabilida guridad. ▪ Ingeniería social. ▪ Suplantación de indentidad. ▪ Adquisición de información dencial de forma fraudulenta *hing*. [3]

3 SP/Operaciones de seguridad.(8 horas)

Objetivos Específicos	Contenidos
▪ 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 mas/redes. ▪ Recuperación y respuesta. ▪ Manejando problemas técni humanos. [11]

3 PL/Máquinas Virtuales.(3 horas)

Objetivos Específicos	Contenidos
▪ 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. [11]

4 Actividades

- Asignaciones
- Controles de Lectura
- Exposiciones

5 Recursos Materiales

- Apuntes del curso
- Libro(s) de la bibliografía

6 Metodología

- Clase Magistral.
- Taller didáctico.
- Social Constructivismo.
- Prácticas personales y en grupo.

7 Evaluación

La nota final (NF) se obtiene de la siguiente manera:

NE Nota de Exámenes 60 %, esta nota se divide en
- Exámen Parcial 40 %
- Examen Final 60 %

NT Nota de Trabajos e Intervención en clase 40 %

$$NF = 0{,}6 * NE + 0{,}4 * NT$$

Referencias

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

[2] Pino Caballero. *Introducción a la Criptografia*, volume Textos Universitarios. Ra-Ma, 1996.

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

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

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

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

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

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

[9] B. Clifford Neuman and Theodore Ts'o. Kerberos: An autentication service for computer networks. *IEEE Communications Magazine*, 32(9):33–38, September 1994.

[10] Dept. of Computer Engineering. A structured approach to computer security. Technical report, Chalmers University of Tecnology, Feb 1995.

[11] Jorge Ramió Aguirre. *Aplicaciones Criptográficas.* Dpto. de Publicaciones EUI-UPM, segunda edición edition, Junio 1999.

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

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

[14] Jennifer Seberry and Josef Pieprzyk. *Cryptography. An Introduction to Computer Security.* Prentice-Hall, 1989.

[15] Eugene H. Spafford. The internet worm program: An analysis. Technical report, Purdue, Noviembre 1998. CSD-TR-823.

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

[17] Mario Tinto. Computer viruses: prevention, detection and treatment. Technical Report 001, National Computer Security Center, June 1989.

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

[19] Stallings William. *Network and Internetwork Security, Principles and Practice.* Prentice-Hall, 1995.

Docente del curso