Aprobado por resolución N°113 del CFI de fecha 04.07.2017

FACULTAD DE INGENIERIA

UNIVERSIDAD DE LA REPÚBLICA URUGUAY

Programa de
Fundamentos de la Seguridad Informática

1. NOMBRE DE LA UNIDAD CURRICULAR

Fundamentos de la Seguridad Informática (FSI)

2. CRÉDITOS

12 créditos

3. OBJETIVOS DE LA UNIDAD CURRICULAR

Capacitar al estudiante para:

1. Asimilar la seguridad informática como un conjunto de metodologías.
2. Analizar la seguridad de una red o sistema informático, identificando los puntos débiles de la misma para su protección.
3. Conocer los principales ataques de los que puede ser objeto un sistema informático, así como los posibles métodos de protección, detección y políticas de seguridad que permitan evitar el daño al sistema o minimizar su repercusión.
4. Entender el funcionamiento de diferentes protocolos criptográficos que se utilizan en la actualidad.
5. Conocer los sistemas de autenticación más importantes identificando sus características

4. METODOLOGÍA DE ENSEÑANZA

- Horas clase (teórico): 44
- Horas clase (práctico): 0
- Horas clase (laboratorio): 4
- Horas consulta: 16
- Horas evaluación: 6
  - Subtotal horas presenciales:70
- Horas estudio: 50
- Horas resolución ejercicios/prácticos: 60
- Horas proyecto final/monografía: 0
  - Total de horas de dedicación del estudiante:180

5. TEMARIO

Módulo 1. Bases y motivación

Introducción. Motivación, definiciones y objetivos de la seguridad informática. Motivación. Ejemplos históricos. Ejemplos actuales.Quién precisa seguridad informática. Definición de seguridad informática. Objetivos. Propiedades de seguridad: confidencialidad (secreto), disponibilidad, integridad, autenticación, no repudio. Motivación y herramientas del atacante. Principios de seguridad informática.

Módulo 2. Criptografía Aplicada

Introducción a la Criptografía.Definiciones. Criptografía moderna. Algoritmo público, clave secreta. Objetivos de un algoritmo. Tipos de ataques a los que debe ser inmune un algoritmo. Cifrado perfecto. "One time pads".Clasificaciones: Cifrados de clave simétrica, de clave pública, en bloque, en flujo.Encadenamiento de algoritmos en bloques.Otras funciones criptográficas. Hashes. Diffie-Hellman. Gestión de claves.Firma electrónica.Ejemplo de protocolos: SL.Importancia de los números aleatorios en criptografía. Infraestructura declave pública (PKI). Certificados digitales. Ejemplo: X.509. Protocolos criptográficos.

Módulo 3. Seguridad de Sistemas

Identificación, Autenticación: mecanismos tradicionalmente utilizados en los sistemas operativos comunes, y ganar una noción razonable de los nuevos mecanismos que ya se están implementando (y que se implementan hace
tiempo en sistemas especializados en seguridad). Métodos de Autenticación. Algoritmos y protocolos de autenticación. Políticas de seguridad y mecanismos de control de acceso. Modelos de políticas de seguridad: Bell - La Padula. BIBA. Clark-Wilson. Chinese Wall. Modelos de control de acceso: IBAC (Identity Based Access Control). DAC (Discretionary Access Control). MAC (Mandatory Access Control). RBAC (Role Based Access Control). Mecanismos de control de acceso: ACL, Control de acceso centralizado (AAA), RADIUS, TACACS, Single Sign- On. Seguridad en Windows. Seguridad en Unix.

Módulo 4. Seguridad en Bases de Datos

Bases de datos Relacionales: claves, reglas de integridad. Control de acceso: el modelo de seguridad de SQL, privilegios, vistas como control de acceso. Bases estadísticas: seguridad, agregación e inferencia, ataques, contramedidas. Integración con el SO. Privacidad.

Módulo 5. Seguridad en Redes TCP/IP

Introducción a la seguridad en redes TCP/IP. Problemas en las distintas capas del modelo OSI simplificado. Seguridad por debajo de la capa 3. Seguridad física. Seguridad en los protocolos de capa 2 y capa MAC. Ataques a estos protocolos. Redes inalámbricas. (IN)Seguridad en capa 3 y 4. Ataques a los protocolos IP, TCP, UDP, ICMP. Qué provee IPSec y qué no. Seguridad en los protocolos de aplicación. Servicios de infraestructura críticos: DNS Ataques a las aplicaciones. Seguridad de la infraestructura. Ataques a la infraestructura. (IN)Seguridad en los protocolos de ruteo. Herramientas para la seguridad en redes TCP/IP: Firewalls, VPNs, IDS, Honeypots. El estado de la seguridad en Internet: DdoS, Ataques "Man in the middle", Ataques a las aplicaciones. Botnets, Canales encubiertos, Ataques "sociales". El factor humano. Phishing, etc.

Módulo 6. Seguridad en las Aplicaciones

Errores en los programas y defensas: Ataques al Stack, Bugs en el formato de los strings, Ataques de Timing, Defensas contra estos ataques. Diseño de código seguro: Diseño modular, Herramientas para hacer código seguro, Verificadores de modelos. Manejando código inseguro: Sandboxing, Máquinas virtuales. Seguridad en los browsers: Cookies, Privacidad y multitudes, Java Script, Java Applets y ActiveX. Secure Coding.

6. BIBLIOGRAFÍA

Tema	Básica	Complementaria
Módulo 1	(1)(2)	
Módulo 2	(3)	
Módulo 3	(1)(2)	
Módulo 4	(1)(2)	
Módulo 5	(1)	(4)(5)
Módulo 6.	(1)	

6.1 Básica

1. Gollman, Dieter (2009), Computer Security, Wiley Computing Publishing, 3rd. Edition.
2. Anderson, Ross (2008), Security Engineering: A Guide to Building Dependable Distributed Systems, 2nd edition, Wiley Computing Publishing, 2008. ISBN: 0470068523.
3. Stallings, W. (2006), Cryptography and Network Security, Prentice Hall.

6.2 Complementaria

4. Garfinkel,S.; Spafford, G. & Schuartz, A., Practical Unix & Internet Security,,Ed. O'Reilly, 3rd Edition.
5. Zwicky,E.; Cooper, S. & Chapman, B., Building Internet Firewalls,, Ed. O'Reilly, 2nd Edition.

7. CONOCIMIENTOS PREVIOS EXIGIDOS Y RECOMENDADOS

7.1 Conocimientos Previos Exigidos: Fundamentos de programación estructurada, de bases de datos y de sistemas operativos y redes de computadores.

7.2 Conocimientos Previos Recomendados: Lógica y matemática discreta

ANEXO A
Para todas las Carreras

A1) INSTITUTO

Instituto de Computación.

A2) CRONOGRAMA TENTATIVO

Consiste en un cronograma de avance semanal con detalle de las horas de clase asignadas a cada tema.

Semana 1	Presentación del curso(2 hs de clase). Introducción (2 hs de clase).
Semana 2	Criptografía aplicada (4 hs de clase).
Semana 3	Criptografía aplicada (2 hs de clase).
Semana 4	Identificación, Autenticación, Autorización (4hs de clase)
Semana 5	Modelos de Control de Acceso I (2hs de clase), Modelos de Control de Acceso II (2hs de clase)
Semana 6	Seguridad de Bases de Datos (2hs de clase)
Semana 7	Seguridad de Sistemas operativos (4hs)
Semana 8	Seguridad de Sistemas operativos (4hs)
Semana 9	Seguridad de Redes TCP/IP (4hs)
Semana 10	Seguridad de Redes TCP/IP (4hs)
Semana 11	Seguridad de Aplicaciones (4hs)
Semana 12	Seguridad de Aplicaciones (4hs)
Semana 13	
Semana 14	
Semana 15	

A3) MODALIDAD DEL CURSO Y PROCEDIMIENTO DE EVALUACIÓN

La unidad curricular se evaluará por medio de dos parciales y trabajos de laboratorio. El nivel mínimo de suficiencia en los trabajos de laboratorio es eliminatorio, ya que esta parte del trabajo del curso no puede ser evaluada mediante exámenes. Por otra parte, dependiendo de las condiciones de dictado del curso, el trabajo de laboratorio se evalúa según las opciones aprobado/no aprobado, o con puntaje diferenciado en el caso de aprobación. En este último caso, el puntaje del laboratorio se integraría al puntaje total del curso, prorrateándose en los de las pruebas parciales.

En todos los casos de los resultados obtenidos surgen dos posibilidades:

1. Exoneración del curso
2. Insuficiencia en el curso; el estudiante reprueba el curso

Se presenta a continuación el esquema de evaluación del curso

Exoneración.
El estudiante debe cumplir los siguientes requisitos:

- llegar al nivel mínimo y en cada uno de los trabajos de laboratorio, y
- reunir al menos el 60% del puntaje de parciales,
- obtener al menos el 25% en cada prueba parcial

Insuficiencia. El estudiante no obtiene los puntajes de alguna de las franjas anteriores.

A4) CALIDAD DE LIBRE

No se adhiere a la resolución de calidad de libre.

A5) CUPOS DE LA UNIDAD CURRICULAR

No tiene cupo.

ANEXO B para la(s) carrera(s) **Ingeniería en Computación (plan 97) y Licenciatura en Computación.**

B1) ÁREA DE FORMACIÓN

Arquitectura,Sistemas Operativos y Redes de Computadoras

B2) UNIDADES CURRICULARES PREVIAS

Para el Curso: Exámenes aprobados de:

Lógica y
Programación 3 y
Fundamentos de Bases de Datos
Redes de Computadoras
Sistemas Operativos

Para el Examen: No aplica

Aprobado por resolución N°113 del CFI de fecha 04.07.2017

ANEXO B para la(s) carrera(s) Ingeniería en Computación (plan 87)

B1) ÁREA DE FORMACIÓN

No corresponde

B2) UNIDADES CURRICULARES PREVIAS

Para el Curso: Previas comunes a las electivas
y exámenes aprobados de:
Lógica y
Programación III y
Bases de Datos y
Sistemas Operativos.

Para el Examen: **No Aplica**

Observación: Esta unidad curricular se corresponde con una electiva

APROB. RES. CONSEJO DE FAC. ING.
de fecha 5.12.17 Exp. 060120-004595-13