Planificación de

Seguridad Informática

FACULTAD DE CIENCIAS EXACTAS, INGENIERIA Y AGRIMENSURA

Código/s: R-511

Identificación y características del Espacio Curricular

Carrera/s:	Licenciatura en Ciencias de la Computación		
Plan de Estudios:	2010, TO2024	Carácter:	Obligatoria
Bloque/Campo:		Área:	Ingeniería de Software, Bases de Datos y Sistemas de Información
Régimen de cursado:	Cuatrimestral		
Cuatrimestre:	9º [LCC], 9º [LCC]		
Carga horaria:	90 hs. / 6 hs. semanales	Formato curricular:	Asignatura
Escuela:	Ciencias Exactas y Naturales	Departamento:	Ciencias de la Computación
Docente responsable:	CRISTIA, Maximiliano		

Programa Sintético

Sistemas de Información. Teoría general de Sistemas. Privacidad, integridad y seguridad. en sistemas de información. Auditoría de sistemas informáticos. Protocolos de encriptación y autenticación: Kerberos, Leighton-Micali, pruebas de conocimiento cero, SHA.

Espacios Curriculares Relacionados

Previos Aprobados:	R-411 - Ingeniería del Software I
Simultaneos Recomendados:	R-521 - Tesina, R-513 - Taller de Tesina
Posteriores:	

Vigencia desde 2024

Firma Profesor	Fecha	Firma Aprob. Escuela	Fecha

Con el aval del Consejo Asesor:

Fundamentación

La Seguridad Informática se ha convertido en uno de los atributos de calidad más importantes de los sistemas de sofware. Muchas de las técnicas de la Ingeniería de Software pueden aplicarse a la Seguridad Informática, pero esta tiene aspectos específicos que deben ser abordados especialmente. Esto implica la necesidad de formar especialistas en la materia; esta asignatura es una introducción a partir del cual los egresados podrán ampliar sus conocimientos.

El programa que se presenta contempla aspectos tanto teóricos como prácticos con el fin de que los egresados puedan iniciar su actividad profesional en la industria o comenzar una carrera académica. El programa pone atención en cuestiones de Seguridad Informática relacionadas con la formalización de propiedades de seguridad de los sistemas de software, lo que la inserta de manera más clara con el espíritu general de la carrera.

El curso se relaciona estrechamente con Sistemas Operativos, Ingeniería de Software I y las materias dedicadas a programación. La seguridad de un sistema de software, por lo general, se implementa a nivel del sistema operativo. Las propiedades de seguridad informática complejas suelen especificarse formalmente con lenguajes de especificación similares a los mostrados en Ingeniería de Software I.

La seguridad informática es un aspecto crucial y esencial en los sistemas informáticos, radica en la prevención para evitar la pérdida de datos sensibles, amenazas de virus y riesgos en los sistemas de información, teniendo una vigencia en la actualidad por su impacto social y económico.

La seguridad de un sistema de software es en última instancia un problema de programación.

Resultados del aprendizaje

Al finalizar el cursado los/las estudiantes serán capaces de:

RA1 Comprender los modelos de confidencialidad conocidos como Bell-LaPadula, no-interferencia y multi-ejecución segura
RA2 Aplicar prácticas de programación segura
RA3 Detectar vulnerabilidades tales como desborde de arreglos e inyección de sentencias SQL en sistemas de complejidad reducida
RA4 Comprender las primitivas criptográficas relacionadas con la criptografía simétrica y asimétrica
RA5 Interpretar el problema de la verificación de protocolos criptográficos
RA6 Explicar la importancia de la confidencialidad de los datos y de la seguridad relacionadas al diseño, desarrollo, mantenimiento, supervisión y uso de sistemas informáticos

Competencias / Ejes transversales y Resultados del Aprendizaje

Competencia/Eje transversal al que tributa	Nivel	Resultados del Aprendizaje
CGT1-Identificación, formulación y resolución de problemas de informática	Bajo	RA1-RA2-RA3-RA4-RA5
CGT2-Concepción, diseño y desarrollo de proyectos de informática	Bajo	RA1-RA2-RA3-RA4-RA5
CGT4-Utilización de técnicas y herramientas de aplicación en la informática	Alto	RA1-RA2-RA3-RA4-RA5
CGS3-Fundamentos para la acción ética y responsable	Medio	RA6
CGS4-Fundamentos para la evaluación y actuación en relación con el impacto social de su actividad en el contexto global y local	Medio	RA6

Programa Analítico

Unidad II Confidencialidad en Sistemas de Cómputo
II.1. El problema de la confidencialidad en sistemas de cómputo
II.2. Control de acceso discrecional
II.3. Control de acceso obligatorio; seguridad multi-nivel
II.4. Flujo de información
II.5. Nointerferencia
II.6. Multi-ejecución nointerferente
II.7. Otras aproximaciones al problema

Unidad III Seguridad en Lenguajes de Programación
III.1. Evitar o detectar errores de seguridad en la implementación
III.2 Utilización de caracteristicas de los lenguajes para implementar políticas de seguridad
III.3. Ejemplos de errores de programación que producen fallas de seguridad: desbordamiento de arreglos e inyección de sentencias SQL
III.4. Prácticas de programación segura
III.5. Introducción a algunos tópicos avanzados
III.5.1. Código que incluye pruebas de corrección (proof-carrying code)
III 5.2. Monitores de referencia en linea
III.5.3. Ofuscación de código

Unidad IV Introduccion a la Criptografía
IV.1. Conceptos basicos de criptografía: relación entre criptografía y seguridad informática; algoritmo criptográfico; claves de encriptación; texto legible y encriptado; etc.
IV.2. Criptografía de clave simétrica; introducción al algoritmo DES
IV.3. Criptografia de clave aasimetrica; introduccion al algoritmo RSA
IV.4. Resumenes de mensajes y firmas electrónicas

Unidad V Introducción al Análisis de Protocolos Criptográficos
V.1. Protocolos criptográficos: aplicaciones y ejemplos.
V.2. Introducción a la lógica de Burrows, Abadi y Needham (BAN)

Unidad VI Introducción a la auditoría de Software
VI.1. Norma ISO 27001
VI.2. Normativa de la industria de pagos con tarjeta para auditoria de sistemas de pagos electrónicos
VI.3. Introducción a las comunicaciones A 4192 y A 4609 del Banco Central de la Republica Argentina.

Modalidades de enseñanza

Clases teóricas, clases prácticas, desarrollo de trabajos prácticos individuales.

Recursos

Aula de clase; ocasionalmente proyector multimedia, software específico relacionado con los contenidos.

Actividades de Formación Práctica

Nº	Título	Descripción
1	Práctica 1	Práctica correspondiente a las Unidades 1 y 2 del programa. Consiste en resolución de problemas prácticos y algunas preguntas sobre conceptos teóricos.
2	Práctica 2	Práctica correspondiente a los items III.3 (desbordamiento de arreglos e inyección de sentencias SQ) y III.5.1 (proof-carrying code). Consiste en resolución de problemas prácticos. Los alumnos deben elegir uno de los tres temas para el Trabajo Práctico 2.
3	Práctica 3	Práctica correspondiente a las unidades 4 y 5. Consiste en resolución de problemas prácticos y algunas preguntas sobre conceptos teóricos.

Evaluación

Se solicita la entrega de 3 problemas de cada práctica de ejercitación que cubren las primeras 5 unidades del programa. Si los problemas están correctamente resueltos el alumno queda en condición de regular. Para el examen final cada alumno debe seleccionar 2 artículos científicos de una lista provista por la cátedra. El día que se presenta a rendir el examen final el tribunal le solicitará presentar uno de esos dos artículos. Luego de la presentación el tribunal efectúa algunas preguntas sobre la presentación y sobre el contenido del curso. El examen final es oral.

Resultado de Aprendizaje	Actividades/Modalidad de Enseñanza	Modalidad de Evaluación
RA1	Clases teóricas y clases prácticas	Resolución de problemas
RA2	Clases teóricas y clases prácticas	Resolución de problemas
RA3	Clases teóricas y clases prácticas	Resolución de problemas
RA4	Clases teóricas y clases prácticas	Resolución de problemas
RA5	Clases teóricas y clases prácticas	Resolución de problemas
RA6	Clases teóricas y clases prácticas	Examen final oral

Bibliografía básica

Autores (Apellido, Inicial nombre)	Año de edición	Título de la obra	Editorial o Revista	Ejemplares disponibles o sitio web
Morrie Gasser	1988	Building a Secure Computer System	Van Nostrand Reinhold Co.	https://www.researchgate.net/publication/242363259_Building_a_Secure_Computer_System
Bell, E., LaPadula, L.	1973	Secure computer systems: Mathematical foundations	The MITRE Corporation	Poner: https://www.semanticscholar.org/paper/Secure-Computer-Systems-%3A-Mathematical-Foundations-L.-Field/a3f6208403fef265fd0e4ad2b4c7ed4c33d45ff2

M. Cristiá, P. Mata	2009	Runtime enforcement of noninterference by duplicating processes and their memories	Workshop de Seguridad Informática WSEGI 2009	https://www.fceia.unr.edu.ar/~mcristia/publicaciones/flowx-abs-model.pdf
Goguen, J., Meseguer, J.	1982	Security policies and security models	IEEE Symposium on Security and Privacy	https://www.semanticscholar.org/paper/Security-Policies-and-Security-Models-Goguen-Meseguer/4458b0a2247c658a9476b6b3774f3836c2c11e94
Aleph One	1990	Smashing the stack for fun and profit	Phrack 49	
George~C. Necula	1997	Proof-carrying code	24th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages	https://www.researchgate.net/publication/235940398_Proof_Carrying_Code
Michael Burrows, Martin Abadi, and Roger Needham	1990	A logic of authentication	ACM Transactions on Computer Systems	Poner: https://www.semanticscholar.org/paper/A-logic-of-authentication-Burrows-Abadi/c4767555e585afcbe982b228457c94a316ab84f1
Argencard		Payment Card Security Industry: Procedimientos de Auditoría		https://listings.pcisecuritystandards.org/pdfs/spanish_pci_dss_audit_procedures_v1-1.pdf
BCRA	2006	Comunicación A 4609	BCRA	https://www.bcra.gob.ar/pdfs/comytexord/a4609.pdf
BCRA	2004	Comunicación A 4192	BCRA	https://www.bcra.gob.ar/pdfs/comytexord/a4192.pdf
Sabelfeld, A., Myers, A.	2006	Language-based information-flow security	IEEE Journal on Selected Areas in Communications	https://www.semanticscholar.org/paper/Language-based-information-flow-security-Sabelfeld-Myers/cc076dcd0bbed4e019ea040a8cf0451d8717c476

Denning, D.	1976	A Lattice Model of Secure Information Flow	Communications of the ACM	https://www.semanticscholar.org/paper/A-lattice-model-of-secure-information-flow-Denning/5f2b22b77559ddb4f3734459d1ff66c58d22df12
Volpano, D., Smith, G., Irvine, C.	1996	A SOUND TYPE SYSTEM FOR SECURE FLOW ANALYSIS	Journal of Computer Security IOS Press	https://www.researchgate.net/publication/2619516_A_Sound_Type_System_For_Secure_Flow_Analysis
Cristiá, M.	2019	Seguridad Informática	Apunte de clase	http://www.fceia.unr.edu.ar/~mcristia/apunte-si.pdf

Bibliografía complementaria

Autores (Apellido, Inicial nombre)	Año de edición	Título de la obra	Editorial o Revista	Ejemplares disponibles o sitio web
Gao, H., Bodei, C., Degano, P., Nielson, H.	2007	A Formal Analysis for Capturing Replay Attacks in Cryptographic Protocols	Advances in Computer Science - ASIAN 2007	
Bathe, G., Rezk, T., Basu, A.	2007	Security types preserving compilation	Computer Languages, Systems & Structures	
Birgisson, A., Russo, A., Sabelfeld, A.	2011	Capabilities for information flow	Workshop on Programming Languages and Analysis for Security	
Adrian, D-, et al	2019	Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice	Communications of the ACM	
Checkoway, S., et al	2010	Return-Oriented Programming without Returns	17th ACM Conference on Computer and Communications Security	
Reed, M., et al	1998	Anonymous connections and onion routing	IEEE Journal on Selected Areas in Communications	
Wood, G.	2014	ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER	Ethereum Project Yellow Paper	
Russo, A.	2015	Functional Pearl: Two Can Keep a Secret, If One of Them Uses Haskell	20th ACM SIGPLAN International Conference on Functional Programming	

Chong, S., Myers, A.	2006	Decentralized Robustness	19th IEEE Computer Security Foundations Workshop	
Jaskelioff, M., Russo, A.	2011	Secure Multi-Execution in Haskell	8th Ershov Memorial Conference	
Barthe, G., et al	2008	Formal certification of ElGamal encryption: A gentle introduction to CertiCrypt	Formal Aspects in Security and Trust	

Distribución de la carga horaria

Presenciales

Teóricas		45 Hs.
Prácticas	Formación Experimental	
	Resolución de Problemas vinculados a la Profesión	
	Resolución de Problemas y Ejercicios	45 Hs.
	Actividades de Proyecto y Diseño	
	Formación en la Práctica Profesional	
Evaluaciones		
	Total	**90 Hs.**

Dedicadas por el alumno fuera de clase

Preparación Teórica	20 Hs.
Preparación Práctica	20 Hs.
Elaboración y redacción de informes, trabajos, presentaciones, etc.	20 Hs.
Total	**60 Hs.**

Cronograma de actividades

Semana	Unidad	Tema	Actividad
1	1-2		Clases teóricas y clases prácticas
2	2	Condifencialidad, Bell-LaPadula	Clases teóricas y clases prácticas
3	2	Condifencialidad, Bell-LaPadula	
4	2	No-interferencia, multi ejecución	Clases teóricas y clases prácticas
5	2	No-interferencia, multi ejecución segura	Clases teóricas y clases prácticas
6	2	No-interferencia, multi ejecución segura	Clases teóricas y clases prácticas, entrega
7	3	Desborde de arreglos, inyección de sentencias SQL	Clase de teoría y clase de práctica
8	3	Desborde de arreglos, inyección de sentencias SQL, proof-carrying code	Clase de teoría y clase de práctica
9	3	Proof-carrying code	Clases teóricas y clases prácticas, entrega TP 2
10	4	Criptografía simétrica	Clase de teoría y clase de práctica
11	4	Criptografía simétrica, criptografía	Clase de teoría y clase de práctica
12	4	Criptografía asimétrica	Clase de teoría y clase de práctica

13	5	Lógica BAN	Clase de teoría y clase de práctica
14	5	Lógica BAN	Clase de teoría y clase de práctica
15	6	Norma ISO 27001, normativa de la industria de pagos con tarjeta para electrónicos, introducción a las Comunicaciones A 4192 y A 4609 del Banco Central de la República Argentina	Clases teóricas y clases prácticas, entrega TP 3