Escuela de Ingeniería y Ciencias
FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS UNIVERSIDAD DE CHILE

PROGRAMA DE CURSO

INTRODUCCIÓN A LA SEGURIDAD COMPUTACIONAL

A. Antecedentes generales del curso:

Departamento	Ciencias de la Computación					
Nombre del curso	Introducción a la Seguridad Computacional	**Código**	CC5327	**Créditos**	6	
Nombre del curso en inglés	Introduction to Computer Security					
Horas semanales	**Docencia**	3,0	**Auxiliares**	2,0	**Trabajo personal**	5,0
Carácter del curso	**Obligatorio**		**Electivo**	X		
Requisitos	CC4302 Sistema Operativos /AUTOR					

B. Propósito del curso:

El curso busca entregar a los y las estudiantes conocimientos transversales del área de la seguridad computacional en un gran número de contextos científicos y profesionales, tales como desarrollo y análisis de software de bajo y alto nivel, manejo de datos y uso de primitivas criptográficas; así como también conocimientos básicos sobre procesos de manejo de reportes de vulnerabilidades y privacidad de datos.

El curso tributa a las siguientes competencias específicas (CE) y genéricas (CG) del Plan de Formación de Ingeniería Civil en Computación:

CE2: Analizar, diseñar y/o adoptar, algoritmos y estructuras de datos que cumplan con las garantías requeridas de correctitud y eficiencia.

CE4: Extraer información relevante, utilizando el proceso de descubrimiento de conocimiento de datos.

CE6: Desarrollar software en una amplia variedad de plataformas y lenguajes de programación.

CG1 (Comunicación académica y profesional): Comunicar en español de forma estratégica, clara y eficaz, tanto en modalidad oral como escrita, puntos de vista, propuestas de proyectos y resultados de investigación fundamentados, en situaciones de comunicación compleja, en ambientes sociales, académicos y profesionales.

CG2 (Comunicación en inglés): Leer y escuchar de manera comprensiva en inglés una variedad de textos e informaciones sobre temas concretos o abstractos, comunicando experiencias y opiniones, adecuándose a diferentes contextos y a las características de la audiencia.

CG3 (Compromiso ético): Actuar de manera responsable y honesta, dando cuenta en forma crítica de

sus propias acciones y sus consecuencias, en el marco del respeto hacia la dignidad de las personas y el cuidado del medio social, cultural y natural.

CG4 (Trabajo en equipo): Trabajar en equipo, de forma estratégica y colaborativa, en diversas actividades formativas, a partir de la autogestión de sí mismo y de la relación con el otro, interactuando con los demás en diversos roles: de líder, colaborador u otros, según requerimientos u objetivos del trabajo, sin discriminar por género u otra razón.

C. Resultados de aprendizaje:

Competencias específicas	Resultados de aprendizaje
CE2	**RA1:** El o la estudiante identifica el uso correcto de algoritmos criptográficos basados en cifradores de bloque, funciones de hash y primitivas basadas en teoría de números, entre otros en cuanto a su aplicación en soluciones criptográficas para problemas de confidencialidad y autentificación en redes de computadores.
CE4	**RA2:** El o la estudiante maneja los conceptos básicos de seguridad computacional (como ataques, vulnerabilidades) y seguridad de sistemas, tanto en software de bajo nivel como en hardware, pudiendo evaluar informadamente la seguridad de un sistema computacional.
CE4, CE6	**RA3:** El o la estudiante identifica las causas y mecanismos detrás de las vulnerabilidades de software más comunes (incluído factores humanos), manejando detalles de implementación quecausan dichas vulnerabilidades. Además maneja las herramientas básicas para prevenir y mitigar dichos ataques.
CE2, CE4	**RA4:** El o la estudiante identifica los distintos problemas de seguridad y las medidas posibles de mitigación presentes en las redes de datos y protocolos de comunicación actuales.
CE2, CE4, CE6	**RA5:** El o la estudiante maneja los mecanismos y problemas detrás de la seguridad web y de dispositivos móviles, y diseña soluciones que mejoran la seguridad y/o los ataques en dichos sistemas.
Competencias genéricas	**Resultados de aprendizaje**
CG3	**RA6:** El o la estudiante identifica y maneja conceptos y mecanismos asociados a la respuesta a incidentes, privacidad de datos, reporte de vulnerabilidades responsable y anonimato en Internet.

CG1, CG2, CG4	**RA7:** El o la estudiante trabaja en equipos para la realización de una propuesta de proyecto y el desarrollo de una prueba de concepto.

D. Unidades temáticas:

Número	RA al que tributa	Nombre de la unidad	Duración en semanas
1	**RA1**	Conceptos Básicos y Criptografía	2,5 semanas
Contenidos		**Indicador de logro**	
1 Motivación, necesidad de seguridad informática, bugs de software y vulnerabilidades 2 Criptografía Simétrica (Encriptación, hashes, MACs, PRNG) 3 Criptografía Asimétrica (Encriptación, Firmas, PKI) 4 Aplicaciones Criptográficas (Acuerdo de llaves, TLS, etc)		El o la estudiante: 1 Identifica las motivaciones y conceptos fundamentales asociados a ataques de sistemas computacionales, y a las propiedades que se busca preservar. 2 Identifica los conceptos básicos asociados a la criptografía tales como confidencialidad y autentificación. 3 Maneja las distintas estrategias para proveer confidencialidad y autenticidad de datos en los casos de comunicación simétrica y asimétrica (clave pública). 4 Identifica mecanismos para proveer aleatoriedad y sus potenciales problemas.	
Bibliografía de la unidad		[1] Cap. 1 y 5, [2] Cap 1, 2 y 8, [3] Cap 6 y 8, [4], [a], [c]	

Número	RA al que tributa	Nombre de la unidad	Duración en semanas
2	**RA2**	Principios de Seguridad	1,5 semanas
Contenidos		**Indicador de logro**	
1. Conceptos de amenazas, adversarios, y propiedades u objetivos de seguridad 2. Modelo mental de la seguridad y modelamiento de amenazas 3. Principios básicos de la Seguridad 4. Autentificación		El o la estudiante: 1 Identifica correctamente los conceptos de amenazas, adversarios y las propiedades de seguridad. 2 Conoce algunos ejemplos de modelos mentales de seguridad y sistemas de modelamiento de amenazas. 3 Identifica principios básicos de seguridad. 4 Identifica correctamente los sistemas de autentificación y diferencia correctamente sus	

	distintos tipos.
Bibliografía de la unidad	[1] Cap. 1, 4 y 15, [2] Cap 3 y 4, [3] Cap 3, 7 y 8

Número	**RA al que tributa**	**Nombre de la unidad**	**Duración en semanas**
3	**RA2**	Seguridad de Software en Bajo Nivel	1,5 semanas
Contenidos		**Indicador de logro**	
1. Vulnerabilidades y Ataques de bajo nivel 2. Ataques de secuestro del flujo del programa (Buffer Overflows, Integer Overflow, Inyección de Código, ROP) 3. Estrategias de protección, Sandboxing, aislamiento		El o la estudiante: 1. Identifica y discrimina errores de vulnerabilidades de bajo nivel 2. Maneja los principales ataques de secuestro de flujo, siendo capaz de identificar instancias y de implementar alguno de ellos 3. Maneja estrategias de protección y mitigación para estos ataques	
Bibliografía de la unidad		[2] Cap 6	

Número	**RA al que tributa**	**Nombre de la unidad**	**Duración en semanas**
4	**RA5**	Seguridad Web	1,5 semanas
Contenidos		**Indicador de logro**	
1. Seguridad web, conceptos 2. Modelo de seguridad del cliente navegador 3. Ataques típicos del lado del cliente 4. Ataques típicos del lado del servidor		El o la estudiante: 1. Maneja los conceptos de seguridad web, y modelos de seguridad de este caso. 2. Identifica los principales ataques tanto en cliente como servidor y sus mecanismos de prevención y/o mitigación	
Bibliografía de la unidad		[2] Cap 9,	

Número	**RA al que tributa**	**Nombre de la unidad**	**Duración en semanas**

5	**RA4**	Seguridad de Redes y Sistemas Operativos	3 semanas

Contenidos	**Indicador de logro**
1. Control de acceso, mecanismos y políticas 2. Seguridad básica de Sistemas Operativos de Escritorio 3. Seguridad de Sistemas Operativos Móviles: Permisos y modelos de amenaza 4. Seguridad de protocolos de red, TCP/IP, DNS, ruteo 5. Seguridad perimetral, cortafuegos, IDS/IPS 6. Ataques de Denegación de Servicio	El o la estudiante: 1. Identifica mecanismos de control de acceso y políticas. 2. Identifica los principales mecanismos de seguridad de los sistemas operativos 3. Maneja mecanismos de autentificación 4. Identifica las principales fuentes de problemas de seguridad de protocolos de redes, y estrategias para su prevención y mitigación.
Bibliografía de la unidad	[1] Cap 3 y 21, [2] Cap 5, 10 y 11, [3] Cap 5 y 9, [b]. [d]

Número	**RA al que tributa**	**Nombre de la unidad**	**Duración en semanas**
6	**RA3**	Seguridad de Software	1,5 semanas

Contenidos	**Indicador de logro**
1. Técnicas de testeo de software: Análisis Estático y Dinámico, Verificación de Software, Fuzzing, Mutación. 2. Ingeniería reversa: Disassemblers y mitigaciones (Ofuscación) 3. Conceptos de seguridad de aplicaciones móviles y principales ataques	El o la estudiante: 1. Identifica las principales técnicas para testeo de software con el objetivo de disminuir la posibilidad de fallas de seguridad 2. Identifica técnicas para entender y modificar el funcionamiento de un programa a través de ingeniería reversa y sus mitigaciones 3. Identifica los principales problemas y soluciones para segurizar dispositivos móviles
Bibliografía de la unidad	

Número	RA al que tributa	Nombre de la unidad	Duración en semanas
7	**RA2**	Malware	1 semana
Contenidos		**Indicador de logro**	
1. Malware, su génesis e historia 2. Tipos de malware, causas y comportamiento 3. Estrategias de prevención de ataques de malware 4. Estrategias de detección de malware 5. El factor humano, ingeniería social		El o la estudiante: 1. Identifica los tipos de malware, sus causas, comportamiento y consecuencias 2. Maneja las distintas estrategias para prevenir el ataque de malware 3. Maneja estrategias comunes para detectar malware	
Bibliografía de la unidad		[1] Cap 21, [2] Cap 7, [3] Cap 4	

Número	RA al que tributa	Nombre de la unidad	Duración en semanas
8	**RA2**	Seguridad de Hardware	1,5 semanas
Contenidos		**Indicador de logro**	
1. BIOS, UEFI y Secure Boot 2. Apple y Secure Enclave, Cadena de Confianza en firmware, bootloaders y sistema operativo y vulnerabilidades. 3. Vulnerabilidades conocidas: Spectre, Meltdown, Rowhammer 4. Ataques de tipo Side-Channel sobre el hardware		El o la estudiante: 1. Conoce e identifica los distintos componentes de software que interactúan directamente con el hardware de un dispositivo, así como también vulnerabilidades históricas asociadas a ellos y sus mitigaciones. 2. Reconoce ejemplos básicos de ataques de tipo “Side Channel” y sabe cómo mitigarlos.	
Bibliografía de la unidad			

Número	RA al que tributa	Nombre de la unidad	Duración en semanas
9	**RA6, RA7**	Privacidad, Anonimato, Reportes de Vulnerabilidades y Temas Varios	1 semana
Contenidos		**Indicador de logro**	
1. Tipos de procedimientos reportes de vulnerabilidades, experiencias históricas, ventajas y desventajas y respuesta a incidentes. 2. Privacidad y Anonimato, problemas y herramientas. 3. Temas Varios: Copyright y DRM, Criptomondas, etc.		El o la estudiante: 1. Identifica las herramientas, procedimientos y mecanismos de reportes de vulnerabilidades. 2. Identifica los principales desafíos en proveer confidencialidad de datos personales y maneja herramientas que permiten resolver parcialmente el problema.	
Bibliografía de la unidad		[1] Cap 22,	

E. Estrategias de enseñanza:

La estrategia de enseñanza utilizada considera la realización de clases expositivas en horario de cátedra y de clases auxiliares y laboratorios guiados en horario de auxiliar.

Durante el transcurso del curso, se entregarán a los estudiantes referencias bibliográficas, *papers* y contenido audiovisual complementario, de forma de facilitar la comprensión de los contenidos cubiertos por el curso.

El curso contempla cinco horas de trabajo autónomo semanal.

F. Estrategias de evaluación:

El curso contempla distintas categorías de evaluación de proceso, todas reprobatorias por sí solas, es decir, requieren una nota igual o superior a 4 para aprobar:

- Ejercicios en clase, con un máximo de 6 por semestre
- Laboratorios individuales, con un máximo de 4 por semestre.
- Proyecto grupal dirigido, con un plazo de desarrollo mínimo de 5 semanas.

Así mismo, se planean realizar preguntas sin nota durante las cátedras para entender

mejor el nivel de comprensión general de los temas presentados.

La ponderación de cada evaluación respetará siempre los reglamentos de la Escuela.

G. Recursos bibliográficos:

Bibliografía obligatoria:

[1] Security Engineering, 3rd edition, Ross Anderson, 2010.
[2] Computer Security and the Internet, Paul C. van Oorschot, 2020
[3] Thinking Security: Stopping Next Year's Hackers, Steven M. Bellovin, 2015
[4] Cryptography Engineering, Ferguson, Schneier & Kohno, 2010

Bibliografía Recomendada:

[a] Practical Cryptography in Python, Monson Nielson, 2019
[b] Attacking Network Protocols, James Forshaw, 2017
[c] Ten laws of security, Eric Diehl, 2016
[d] The Shellcoder's Handbook, Varios Autores, 2007

H. Datos generales sobre elaboración y vigencia del programa de curso:

Vigencia desde:	Otoño 2022
Elaborado por:	Alejandro Hevia, Eduardo Riveros
Validado por:	Alejandro Hevia
Revisado por:	