SYLLABUS Extendido con cronograma

SEGURIDAD EN TI

TICS413 - Sección 1

Información General del Curso

Profesor:	
Email:	
Sigla:	TICS413
Sección:	
Semestre:	V-SEM. 2025/2
Créditos:	6
Unidad Académica:	Pregrado Viña del Mar/Santiago
Facultad:	Facultad de Ingeniería y Ciencias

Horas de Trabajo

Tipo de Actividad	Horas
Horas Presenciales	45
Horas Autónomas	135
Horas Laboratorio	22.5
Total	**180**

Descripción de la Asignatura

En la era digital actual, la seguridad de la información se ha convertido en un pilar fundamental para el funcionamiento de las organizaciones. Los continuos ataques cibernéticos perpetrados por actores maliciosos, junto con el manejo inadecuado de datos sensibles por parte de las empresas, han evidenciado la necesidad crítica de implementar estrategias robustas de ciberseguridad.

Este curso aborda la implementación y concientización en temas de seguridad de la información, dirigida tanto a usuarios finales como a especialistas tecnológicos y tomadores de decisiones. La asignatura proporciona una base sólida en ciberseguridad, considerando los desafíos actuales y futuros que enfrentan las organizaciones en el ámbito de las Tecnologías de la Información.

Resultados de Aprendizaje

Al finalizar el curso, los estudiantes serán capaces de:

RA1. **Comprender** los conceptos fundamentales de seguridad de la información aplicándolos en escenarios prácticos y casos empresariales reales.

RA2. **Identificar y analizar** vulnerabilidades y riesgos en redes de computadores, proponiendo e implementando controles de seguridad apropiados.

RA3. **Diseñar y proponer** soluciones seguras por diseño ante situaciones y riesgos que amenacen la confidencialidad, integridad y disponibilidad de la información empresarial, considerando aspectos éticos y legales.

RA4. **Evaluar** el impacto en la continuidad del negocio de las fallas de ciberseguridad en un entorno organizacional, desarrollando estrategias de mitigación.

RA5. **Colaborar** en la investigación de incidentes de seguridad, aplicando metodologías y herramientas especializadas en entornos simulados, manteniendo un comportamiento ético y respetando la privacidad y normativas legales vigentes.

Competencias del Egresado

Este curso contribuye al desarrollo de las siguientes competencias del egresado:

- **Competencia 2.3:** Diseñar, implementar y gestionar soluciones tecnológicas innovadoras que respondan a las necesidades de la sociedad y las organizaciones.
- **Competencia 3.1:** Comunicar efectivamente ideas, propuestas y resultados técnicos de manera oral y escrita, adaptándose a diferentes audiencias.
- **Competencia 4.2:** Actuar con responsabilidad social, ética y profesional, considerando el impacto de las decisiones tecnológicas en la sociedad y el medio ambiente.

Pre-requisitos

Para cursar esta asignatura, el estudiante debe tener conocimientos previos en:

- Fundamentos de redes de computadores

Es deseable que los estudiantes comprendan conceptos básicos de programación, arquitectura de sistemas informáticos y matemáticas discretas.

Objetivos de Desarrollo Sostenible (ODS)

La Facultad de Ingeniería y Ciencias está comprometida con la formación de ingenieros que contribuyan al bienestar de la sociedad y la protección del medioambiente. Este curso proporciona herramientas para cumplir con las siguientes metas de los Objetivos de Desarrollo Sostenible de las Naciones Unidas:

Objetivo	Nivel de Contribución
Educación de Calidad	Competencias
Trabajo Decente y Crecimiento Económico	Competencias
Industria, Innovación e Infraestructura	Competencias
Ciudades y Comunidades Sostenibles	Competencias
Consumo Responsable y Producción	Competencias
Paz, Justicia e Instituciones Fuertes	Competencias
Alianzas para los Objetivos	Competencias

Contenidos del Curso

Unidad 1: Seguridad en Protocolos y Redes

Esta unidad aborda los fundamentos de la seguridad informática y las tecnologías de protección en redes. Se estudian los conceptos básicos de seguridad y protocolos de seguridad de Internet. Se analizan las amenazas más comunes como software malicioso, ataques de denegación de servicio, técnicas de detección de intrusiones y sistemas de protección como firewalls para proteger la infraestructura de red.

Unidad 2: Seguridad de Aplicaciones y Datos

Esta unidad se enfoca en la seguridad a nivel de aplicación y datos, incluyendo autenticación de usuarios, herramientas criptográficas,, control de acceso, protección contra vulnerabilidades como desbordamiento de buffer, y en general desarrollo seguro de software. Se proporciona una visión integral de la protección de aplicaciones y sistemas operativos.

Unidad 3: Gestión de Riesgos y Continuidad del Negocio

Esta unidad aborda la gestión integral de la seguridad desde una perspectiva organizacional, incluyendo evaluación de riesgos, implementación de controles de seguridad y planificación de continuidad del negocio. Se estudian procesos de auditoría de seguridad y los aspectos legales y éticos que rigen la ciberseguridad en el contexto empresarial.

Metodología de Enseñanza y Aprendizaje

El curso emplea una metodología activa y experiencial que combina:

- **Estudio de Casos y Aprendizaje Basado en Problemas:** Análisis de incidentes reales de ciberseguridad para desarrollar pensamiento crítico.
- **Exposición Docente:** Presentación de conceptos teóricos fundamentales con ejemplos prácticos.
- **Aprendizaje Experiencial:**
  - Laboratorios semanales en horario de ayudantías donde los estudiantes practican técnicas de *purple team* para integración de técnicas ofensivas y defensivas

  - Tres ejercicios integradores tipo *capture the flag* donde ejercitan como *red team* en ambientes controlados, cerrados y seguros
  - Prácticas de *blue team* en ambientes simulados y controlados en clases.
- **Aprendizaje Basado en Juegos:** Simulaciones interactivas para reforzar conceptos de seguridad.

Sistema de Evaluación

La evaluación del curso se basa en tres notas evaluados con promedio simple:

$$\mathbf{NF = (T1 + T2 + T3) \ / \ 3}$$

Donde se tiene una nota por unidad temática (TX) la cual se calcula como:

$$\mathbf{TX = 0.8 \times PruebaX + 0.2 \times CTFX}$$

Nota: Las pruebas se realizan de forma simultánea para todos los grupos (a confirmar).
Examen: Solo se considera examen para aquellos alumnos que no aprueban el curso.

Política de Evaluaciones

- **Inasistencia Injustificada:** Resulta en nota mínima (1.0).
- **Inasistencia Justificada:** Para controles o actividades en clases, la nota del examen reemplaza la evaluación no rendida (máximo 2 reemplazos).
- **Pruebas Recuperativas:** Se deben rendir en la fecha oficial de exámenes si la inasistencia está justificada.
- **Falta a dos Pruebas o más:** Resulta en reprobación de la asignatura con nota 3.9 o menor según corresponda.

Reglamento y Políticas del Curso

Asistencia

Aunque la asistencia a clases no es obligatoria, se recomienda encarecidamente la participación regular, ya que el aprendizaje efectivo en esta asignatura depende significativamente de la práctica y el estudio continuo.

Comunicación y Recursos

1. **Webcursos:** El sitio web del curso es parte integral de la asignatura. Es responsabilidad del estudiante revisar periódicamente las novedades y comunicaciones.
2. **Comunicación con el Profesor:** Utilice exclusivamente el correo electrónico oficial para comunicaciones fuera de clases. Se pueden solicitar reuniones por correo electrónico cuando sea necesario.

3. **Comportamiento en Clases:** Dentro del aula de manera presencial y en el aula virtual fomente un ambiente de respeto a sus compañeros, al profesor, y conducente al aprendizaje.

Evaluaciones (fuera del horario de clases - a confirmar):

- **Evaluación Unidad Temática 1 - incluye CTF:** Semana del 29 de septiembre, 2025
- **Evaluación Unidad Temática 2 - incluye CTF:** Semana del 3 de noviembre, 2025
- **Evaluación Unidad Temática 3 - incluye CTF:** Semana del 24 de noviembre, 2025

Bibliografía

Bibliografía Obligatoria

1. Stallings, W., & Brown, L. (2023). *Computer security: Principles and practice* (5ta ed.). Pearson.

Bibliografía Complementaria

1. Kim, D., & Solomon, M. G. (2016). *Fundamentals of information systems security: Print bundle*. Jones & Bartlett Learning.
2. Anderson, R. (2020). *Security engineering: A guide to building dependable distributed systems*. John Wiley & Sons.

— Fin del Syllabus extendido con cronograma—

Cronograma Detallado del Curso

Sem.	Fecha	Unidad	Tema	Contenido	Lab
1	4-8-25	Unidad 1	Fundamentos de TI y Seguridad	Cap. 1: Conceptos básicos de seguridad, amenazas y activos y Cap. 6: Tipos de malware y contramedidas	
2	11-8-25	Unidad 1	Fundamentos de redes y protocolos	Repaso: Arquitectura de redes y protocolos TCP/IP	
3	18-8-25	Unidad 1	Fundamentos de redes y protocolos	Repaso: Arquitectura de redes y protocolos TCP/IP	Lab 1
4	25-8-25	Unidad 1	Protocolos de seguridad de Internet y Aplicaciones de autenticación	Cap. 23: Kerberos, X.509 y PKI y Cap. 22: SSL/TLS, HTTPS y seguridad de protocolos	Lab 2
5	1-9-25	Unidad 1	Seguridad de redes inalámbricas	Cap. 24: Seguridad WiFi y dispositivos móviles	Lab 3
6	8-9-25	Unidad 1	Firewalls e IDS	Cap. 9 y 8	Lab 4
7	15-9-25		Pausa Académica		
8	22-9-25	Unidad 2	2: Criptografía simétrica, asimétrica y hash	Cap. 2, 20 y 21: Criptografía simétrica, asimétrica y hash	Lab 5
9	29-9-25	Unidad 2	2: Criptografía simétrica, asimétrica y hash	Cap. 2, 20 y 21: Criptografía simétrica, asimétrica y hash	EVALUACIÓN T1 y CTF 1
10	6-10-25	Unidad 2	Autenticación de usuarios	Cap. 3: Métodos de autenticación y tokens	Lab 6
11	13-10-25	Unidad 2	Desbordamiento de buffer	Cap. 10: Buffer overflow y técnicas de explotación	Lab 7
12	20-10-25	Unidad 2	Control de acceso	Cap. 4: Modelos DAC, MAC, RBAC y ABAC	Lab 8
13	27-10-25	Unidad 2	Seguridad de software	Cap. 11: Desarrollo seguro y manejo de entrada/salida y Capítulo 5: Base de datos segura	~~lab 9~~
14	3-11-25	Unidad 2	Seguridad de software	Cap. 11: Desarrollo seguro y manejo de entrada/salida y Capítulo 5: Base de datos segura	Ayudantía previa a la evaluación T2
15	10-11-25	Unidad 3	Gestión de seguridad TI	Cap. 14 y 15: Gestión de seguridad y evaluación de riesgos y Planes de Continuidad de Negocio	Evaluación 2 y CTF 2
16	17-11-25	Unidad 3	Gestión de seguridad TI	Cap. 15 y 18: Planes y Auditoría de Seguridad	Ayudantía previa a la evaluación 3
17	24-11-25	Unidad 3	Gestión de seguridad TI	Cap. 18 y 19: Auditoría de Seguridad y Aspectos éticos y legales	Evaluación T3 y CTF 3
18	1-12-25			Recuperativos/Examen	