UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA
Dirección General de Docencia

PROGRAMA DE ASIGNATURA

I. IDENTIFICACIÓN DE LA ASIGNATURA

<table>
<tr><td colspan="2">Asignatura: SEGURIDAD EN REDES DE COMPUTADORES</td><td>Sigla: TEL-312</td><td colspan="4">Fecha de aprobación
14/11/2024
(CC.DD. Acuerdo 029/2024
10/12/2019
(CC.DD. Acuerdo 28/2019)</td></tr>
<tr><td>Créditos UTFSM: 3</td><td rowspan="2">Prerrequisitos:
TEL-342
TEL-252</td><td rowspan="2">Examen: No</td><td colspan="4">Unidad Académica que la imparte</td></tr>
<tr><td>Créditos SCT: 5</td><td colspan="4">Departamento de Electrónica</td></tr>
<tr><td rowspan="2">Horas Cátedra Semanal: 1,17</td><td rowspan="2">Ayudantía: Sí</td><td rowspan="2">Laboratorio: Sí</td><td colspan="3">Semestre en que se dicta</td></tr>
<tr><td>Impar
X</td><td>Par</td><td>Ambos</td></tr>
<tr><td colspan="6">Eje formativo: Ciencias de la Ingeniería Aplicada.</td></tr>
<tr><td colspan="6">Tiempo total de dedicación a la asignatura: 123,66 Horas Cronológicas.</td></tr>
</table>

Descripción de la Asignatura

El estudiante aplica conceptos y términos específicos en la seguridad de la información y el impacto de los *malware*, ataques de tipo *social engineering*, ataques de aplicación, ataques de red, etc. También, evalúa las vulnerabilidades de servicios específicos y de redes de computadores en general, incluyendo los métodos de mitigación de posibles ataques.

Requisitos de entrada

- Resolver problemas de redes y servicios, aplicando metodologías y buenas prácticas en la administración de redes.
- Dimensionar recursos para soluciones, evaluando productos de mercado para concretar dicha solución.
- Analizar los riesgos de seguridad/privacidad en el área de Internet para construir servicios de seguridad, evaluando escenarios en donde la seguridad es un punto crítico.
- Utilizar las primitivas criptográficas correctamente, aplicando soluciones complejas.

Contribución al perfil de egreso

Competencias específicas:

- Elaborar procedimientos de seguridad, disponibilidad, calidad de servicio y confiabilidad en redes de computadores, para proteger la transmisión y el acceso de la información y garantizar un buen servicio.
- Implementar procedimientos de seguridad, disponibilidad, calidad de servicio y confiabilidad en redes de computadores y servicios, para cumplir con los requerimientos de protección, acceso de la información y de calidad de servicio.
- Administrar plataformas y servicios de redes en organizaciones aplicando normas legales, técnicas y procedimentales específicas del área, para asegurar la comunicación, y conexión segura y confiable de los usuarios.
- Diseñar redes de computadores y servicios ["end to end"] en organizaciones, aplicando normas legales, técnicas y procedimentales, considerando protocolos y la tecnología, garantizando el nivel de calidad de servicio acordado, y cumpliendo estándares y recomendaciones de seguridad, para satisfacer los requerimientos de la sociedad.

Competencias Transversales Sello USM:

- **Responsabilidad Social y Ética:** El/la estudiante -de acuerdo con su nivel formativo- se hace responsable de que los conocimientos adquiridos y habilidades desarrolladas sean puestas al servicio de la comunidad y de la sociedad en pos de un bien común, por sobre el individual, en coherencia con el legado testamentario de Don Federico Santa María.
- **Tecnologías de Información y Comunicaciones:** El/la estudiante -de acuerdo con su nivel formativo- utiliza de forma pertinente y eficiente diversas herramientas tecnológicas y de comunicación para el análisis, comprensión y generación de información que le facilite un adecuado desenvolvimiento en sus actividades académicas y profesionales.
- **Compromiso con la Calidad:** El/la estudiante -de acuerdo con su nivel formativo- ejecuta actividades académicas profesionalizantes, demostrando un alto nivel de dedicación, excelen compromiso constante con su proceso de aprendizaje y/o el de sus pares.

Resultados de Aprendizaje que se esperan lograr en esta asignatura

Resultados de aprendizaje asociados a Competencias específicas:

- **Realiza** un análisis de vulnerabilidades de servicios web y de redes de computadores, **utilizando** herramientas que identifican un conjunto de amenazas conocidas.
- **Analiza** el funcionamiento de dispositivos de red dedicados a la seguridad, **considerando** firewall, proxy, Intrusión Prevención/Detección Sistemas, Gateway de seguridad y la contribución a la seguridad de varias tecnologías de red, como, Network Access Control.
- **Analiza** una arquitectura de red de punto de vista de la seguridad, **identificando** aspectos como zonas desmilitarizadas, segmentación, redes LAN virtuales.
- **Evalúa** varios métodos de mitigación de ataques, **considerando** la creación de una postura de seguridad, configuración de controles, endurecimiento, presentación de informes.
- **Evalúa** el impacto de códigos maliciosos, ataques de tipo ingeniería social, ataques de aplicación, ataques de red, **seleccionando** los métodos de protección del ámbito aislado.
- **Administra** una red segura, **considerando** la limitación razonable de los riesgos.

Resultados de Aprendizaje asociados a las CTS:

- Fundamenta su toma de decisiones conforme a principios éticos y dimensiones de la responsabilidad social, desde una perspectiva reflexiva y crítica, para promover un liderazgo ético y responsable.
- Diseña estrategias innovadoras para la sistematización de información técnica, evaluando críticamente su calidad, para generar información especializada que posibilite la toma de decisiones e innovación de procesos según los contextos disciplinares en los cuales se desenvuelve.
- Lidera actividades y/o proyectos académicos, considerando criterios de calidad preestablecidos por el equipo docente, tanto en el proceso como en los resultados, para la excelencia académica y profesional.

Contenidos temáticos

1. Contexto y nociones de la seguridad.
2. Malware e Ingeniería Social.
3. Ataques de aplicación y ataques de red.
4. Análisis de seguridad y mitigación de ataques.
5. Seguridad de anfitrión, aplicaciones y datos.
6. Seguridad de redes.
7. Control de acceso, autenticación y gestión de cuentas.
8. Protocolos de seguridad.
9. Análisis forense (análisis de paquetes IP, análisis de tráfico wireless, análisis de informes de los Intrusion Detection/Prevention Systems).

Metodología de enseñanza y aprendizaje

- Clases teóricas: exposición de contenidos de los capítulos, conceptos, estándares, técnicas y protocolos.
- Clases prácticas: estudiantes trabajan en un ámbito controlado y aislado, y realizan experiencias prácticas de ataques, medidas de defensa, y explotaciones de vulnerabilidades.

Evaluación y calificación de la asignatura (Ajustado a Reglamento Institucional-Rglto. N°1).

Requisitos de aprobación y calificación

El proceso de evaluación y calificación consiste en:

Instrumentos de evaluación	N°	%
Certamen (C)	**1**	**40**
Promedio Controles (PC)	**3**	**20**
Proyecto (PY)	**1**	**40**

Donde:
Promedio semestral (PS) se calcula según:

PS = C * 0,40 + PC * 0,20 + PY * 0,40

Nota final **NF = PS**

Recursos para el aprendizaje

- Plataforma Educativa Virtual AULA-USM.

Bibliografía:

Texto Guía	• Sin textos guía.
Complementaria u Opcional	• Davidoff S., Ham J., (2013) “Network Forensics – Tracking Hackers Through Cyberspace”, Pearson Education, EEUU. • Wu, C.-H., Irwin, J. D. (2013) “Introduction to Computer Networks and Cybersecurity”, CRC Press Taylor & Francis Group, EEUU. • Ciampa M. (2012), “Security+ Guide to Network Security Fundamentals”. Cengage Learning. EEUU. • Anderson R. (2008), “Security Engineering: A Guide to Building Dependable Distributed Systems ”. Wiley; 2nd Edition. • Versión digital en https://www.cl.cam.ac.uk/~rja14/book.html

II. CÁLCULO DE CANTIDAD DE HORAS DE DEDICACIÓN- (SCT-Chile)- CUADRO RESUMEN DE LA ASIGNATURA.

ACTIVIDAD	Cantidad de horas de dedicación		
	Cantidad de horas por semana[1]	Cantidad de semanas	Cantidad total de horas
PRESENCIAL			
Cátedra o Clases teóricas	1,17	16	18,72
Ayudantía/Ejercicios	1,17	16	18,72
Visitas industriales (de Campo)	-	-	-
Laboratorios / Taller	1,17	16	18,72
Evaluaciones (certámenes, otros)	1,17	1	1,17
Otras (Especificar)	2,33	1	2,33
NO PRESENCIAL			
Ayudantía	-	-	-
Tareas obligatorias / Proyecto	2	16	32
Estudio Personal (Individual o grupal: Certamen y controles de lectura)	2	16	32
Otras (Preparación Representación de obra seleccionada)	-	-	-
TOTAL (HORAS RELOJ)	-	-	**123,66**
Número total en CRÉDITOS ACADÉMICOS TRANSFERIBLES[2]			**5**

[1] DECRETO DE RECTORIA Nº 325/2020 VALPARAISO, 13 de noviembre de 2020. REF.: Establece duración hora pedagógica de clases en la Universidad Técnica Federico Santa María, a contar del Año Académico 2021.

[2] DECRETO DE RECTORIA Nº 324/2020 VALPARAISO, 13 de noviembre de 2020.
REF.: Establece equivalencia de crédito transferible SCT Chile con horas de trabajo cronológicas semestral en la Universidad Técnica Federico Santa María, a contar del Año Académico 2021.