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
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 tiene</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>Horas Cátedra Semanal : 1</td><td>Ayudantía:
Sí tiene</td><td>Laboratorio:
Sí tiene</td><td colspan="4">Semestre en que se dicta</td></tr>
<tr><td colspan="3"></td><td>Impar
X</td><td>Par</td><td colspan="2">Ambos</td></tr>
<tr><td colspan="3">Eje formativo</td><td colspan="4">: Ciencias de la Ingeniería Aplicada</td></tr>
<tr><td colspan="3">Tiempo total de dedicación a la asignatura</td><td colspan="4">: 141 horas</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

- Implementar servicios de red, resolviendo necesidades concretas.
- Optimizar configuraciones de redes y servicios.
- Resolver problemas de redes y servicios.
- Dimensionar recursos para soluciones tecnológicas.
- Analizar la seguridad de las primitivas criptográficas.
- Utilizar las primitivas criptográficas correctamente dentro de soluciones complejas.

Contribución al perfil de egreso

COMPETENCIAS DE EGRESO

- 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.
- 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.

COMPETENCIAS TRANSVERSALES SELLO USM

- Responsabilidad Social y Ética:
  Se hace responsable de que los conocimientos adquiridos y habilidades desarrolladas sean puestos 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 Carrera.
- Manejo de las Tecnologías de Información y Comunicaciones:
  Utiliza las tecnologías de información y comunicaciones en la gestión de proyectos, la resolución de problemas y en la forma de colaborar con otras personas.
- Compromiso con la Calidad:

Ejecuta las actividades profesionales con excelencia, que le permitan enfrentar los retos que se presentan, guiado por un aprendizaje continuo, una autoevaluación sistemática y una cultura de calidad.

Resultados de Aprendizaje que se esperan lograr en esta asignatura

- **Utiliza** los conceptos y términos específicos en la seguridad de la información, **evaluando** su pertinencia en situaciones específicas.
- **Evalúa** el impacto de los *malware*, ataques de tipo *social engineering*, ataques de aplicación, ataques de red, **seleccionando** los métodos de protección del ámbito aislado.
- **Realiza** un análisis de vulnerabilidades de un servicio web o una red de computadores, **utilizando** herramientas que prueban un conjunto de vulnerabilidades conocidas.
- **Evalúa** varios métodos de mitigación de ataques, **considerando** la creación de una postura de seguridad, configuración de controles, endurecimiento, presentación de informes.
- **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 del punto de vista de la seguridad, **identificando** aspectos como zonas desmilitarizadas, *subnetting*, redes LAN virtuales.
- **Aplica** ataques contra redes Wireless, **atendiendo** a las variables de un ámbito controlado y aislado.
- **Explica** los fundamentos de control de acceso, de autenticación y de gestión de cuentas, **distinguiendo** varias técnicas que se pueden utilizar para lograrlo.
- **Administra** una red segura, **considerando** la limitación razonable de los riesgos.
- **Explicita** el funcionamiento de protocolos de seguridad, **señalando** las características de protocolos como SSL/TLS, WEP/WPA/WPA2, IPSec.

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- N°1)

Requisitos de aprobación y calificación

Proceso de evaluación y calificación:

Instrumentos de evaluación.	Nro.	%
Certamen (C)	1	40
Promedio Controles (PC)	3	20
Proyecto (PY)	1	40

- 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 virtual

Bibliografía:

Texto Guía	No tiene
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	Cantidad de semanas	Cantidad total de horas
PRESENCIAL			
Cátedra o Clases teóricas	1,5	16	24
Ayudantía/Ejercicios	1,5	16	24
Visitas industriales (de Campo)			
Laboratorios / Taller	1,5	16	24
Evaluaciones (certámenes, otros)	2	1	2
Otras (Especificar) Presentación de proyecto	3	1	3
NO PRESENCIAL			
Ayudantía			
Proyecto	2	16	32
Estudio Personal (Individual o grupal)	2	16	32
Otras (Especificar)			
TOTAL (HORAS RELOJ)			**141**
Número total en CRÉDITOS TRANSFERIBLES			**5**