

PROGRAMA DE ASIGNATURA

I. IDENTIFICACIÓN DE LA ASIGNATURA

Asignatura: Criptografía y Seguridad en la Información		Sigla: TEL-252	Fecha de aprobación 11/06/2019 (CCDD Acuerdo 13/2019)		
Créditos UTFSM : 3	Prerrequisitos: ELO-204 + ELO-321	Examen: No tiene	Unidad Académica que la imparte		
Créditos SCT : 5			Departamento de Electrónica		
Horas Cátedra Semanal : 1,5	Ayudantía: Sí tiene	Laboratorio: Sí tiene	Semestre en que se dicta		
			Impar	Par X	Ambos
Eje formativo		: Ciencias de la Ingeniería Aplicada			
Tiempo total de dedicación a la asignatura		: 139 horas			

Descripción de la Asignatura

El estudiante utiliza los principales algoritmos criptográficos utilizados en seguridad de la información, obteniendo una panorámica de las debilidades y fortalezas de los diferentes métodos de cifrado y sus implicancias en los procesos y usuarios que las aplican.

Los aprendizajes en torno a las temáticas antes anunciadas, posibilita al futuro profesional, integrar elementos esenciales de seguridad a los productos y servicios tecnológicos que se le demanden.

Requisitos de entrada

- Implementar programas utilizando una metodología algorítmica.
- Identificar situaciones prácticas de naturaleza aleatoria con la teoría de probabilidades.
- Relacionar los conceptos fundamentales de probabilidades y los conceptos básicos de procesos aleatorios con los sistemas de Telecomunicaciones y Computación (TIC).
- Redactar informes en lenguaje técnico propio de la especialidad profesional.

Contribución al perfil de egreso

COMPETENCIAS DE EGRESO

- 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.
- Resolución de Problemas:
Resuelve problemas complejos, analizando y evaluando soluciones efectivas y eficientes, en función de su impacto en la organización, las personas y el medio ambiente.



Resultados de Aprendizaje que se esperan lograr en esta asignatura

- **Analiza** los riesgos de seguridad/privacidad en el área de Internet para implementar servicios de seguridad, **evaluando** escenarios en donde la seguridad es un punto crítico.
- **Analiza** la seguridad de las primitivas criptográficas, **evaluando** la seguridad de varias soluciones que la utilizan (protocolos de seguridad, sistemas de autenticación, etc.).
- **Utiliza** las primitivas criptográficas correctamente, **aplicando** soluciones complejas.

Contenidos temáticos

1. Criptografía y seguridad.
2. Encriptación por flujo.
3. Encriptación por bloque.
4. Criptografía asimétrica.
5. Firmas digitales.
6. Funciones hash.
7. Códigos de autenticación de mensajes.
8. Gestión de la claves y planificación de la seguridad.
9. Implementación de servicios de seguridad ya sea en forma móvil o web.

Metodología de enseñanza y aprendizaje

- Clases expositivas interactivas utilizando diapositivas.
- Ejercicios de laboratorio grupales e individuales.
- Creación de un proyecto grupal y presentación oral.

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

Requisitos de aprobación y calificación	Proceso de evaluación y calificación: <table border="1" style="margin: 10px auto;"> <thead> <tr> <th>Instrumentos de evaluación.</th> <th>Nro.</th> <th>%</th> </tr> </thead> <tbody> <tr> <td>Certamen (C)</td> <td>1</td> <td>40</td> </tr> <tr> <td>Promedio Controles (PC)</td> <td>4</td> <td>20</td> </tr> <tr> <td>Presentación de Avance Proyecto (PA)</td> <td>1</td> <td>10</td> </tr> <tr> <td>Presentación Final Proyecto (PP)</td> <td>1</td> <td>30</td> </tr> </tbody> </table> <ul style="list-style-type: none"> • <u>Promedio semestral</u> (PS) se calcula según: $PS = C * 0,40 + PC * 0,20 + PA * 0,1 + PP * 0,30$ • Los estudiantes que obtengan PS mayor o igual a 55 aprobarán la asignatura con nota final (NF) $NF = PS$ 	Instrumentos de evaluación.	Nro.	%	Certamen (C)	1	40	Promedio Controles (PC)	4	20	Presentación de Avance Proyecto (PA)	1	10	Presentación Final Proyecto (PP)	1	30
Instrumentos de evaluación.	Nro.	%														
Certamen (C)	1	40														
Promedio Controles (PC)	4	20														
Presentación de Avance Proyecto (PA)	1	10														
Presentación Final Proyecto (PP)	1	30														

Recursos para el aprendizaje.

- Plataforma virtual

Bibliografía:

Texto Guía	<ul style="list-style-type: none"> • Doukas, Charalampos (2012). Building Internet of Things with the Arduino. North Charleston SC: Createspace.
Complementaria u Opcional	<ul style="list-style-type: none"> • Ferguson N., Schneier B., Kohno T., (2010) "Cryptography Engineering", Wiley, EEUU. • Paar C., Pelzl J. (2010) "Understanding Cryptography", Springer-Verlag Berlin Heidelberg. • Vermesan, O. & Friess, P. Editors. (2013). Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems. River Publisher (River Publishers' Series in Information Science and Technology). ISBN: 8792982735



**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	15	22,5
Ayudantía/Ejercicios	1,5	16	24
Visitas industriales (de Campo)			
Laboratorios / Taller	1,5	16	24
Evaluaciones (certámenes, otros)	1,5	1	1,5
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)			139
Número total en CRÉDITOS TRANSFERIBLES			5

[Handwritten signature]



[Handwritten signature]