

ASIGNATURA: SEGURIDAD DE DATOS

ÁREA DEL CONOCIMIENTO:	TRATAMIENTO DE LA INFORMACIÓN	CLAVE:	I5SD1
ETAPA FORMATIVA:	ETAPA DISCIPLINAR	TOTAL HRS. SEMANA:	5
DURACIÓN:	SEMESTRAL	HRS. TEÓRICAS:	3
TIPO DE CURSO:	OBLIGATORIO	HRS. PRÁCTICAS:	2
REQUISITOS:	NINGUNA	CRÉDITOS:	8
SEMESTRE:	5º	HORAS POR CLASE:	1

OBJETIVO GENERAL:

Al finalizar el curso el alumno comprenderá y valorará la problemática de la seguridad de la información, así como las técnicas criptográficas y los distintos mecanismos que se utilizan como soporte a la seguridad de la información.

TIEMPO (HORAS)	TEMÁTICA	OBJETIVOS DE APRENDIZAJE	MODALIDADES DE CONDUCCIÓN DEL PROCESO ENSEÑANZA APRENDIZAJE	REFERENCIAS BIBLIOGRÁFICAS
5	1. Planteamientos generales sobre la seguridad en la información 1.1 Problemática de seguridad: amenazas y ataques 1.2 Servicios y mecanismos de seguridad	Al término de la unidad, el alumno tendrá los conceptos básicos para entender y analizar la problemática en la seguridad de la información.	E.M. C.L. M.A. P.R. D.T.	Libro: 1,2

10	2. Técnicas de criptográficas para servicios de seguridad Introducción a la criptografía Criptosistemas del secreto perfecto Criptosistemas de clave secreta Introducción a la aritmética modular Criptosistemas de clave pública Legislación sobre criptografía	El alumno integrará los elementos de la criptografía en la seguridad de la información.	E.M. C.L. M.A. P.R. D.T.	Libros: 1,4,5
15	3. Firma digital Concepto de firma digital Funciones HASH Algoritmos de firma digital Legislación sobre firma digital	El alumno conocerá los elementos que integran la firma digital para la protección de los datos-	E.M. C.L. M.A. P.R. D.T.	Libros: 3, 4
20	4. Infraestructuras de clave pública Problemática de la distribución segura de claves Infraestructuras de certificación: X.509 Normas Otras soluciones	El alumno conocerá la problemática y soluciones en cuanto a las claves públicas, para la protección de los datos.	E.M. C.L. M.A. P.R. D.T.	Libros: 3, 4,5
10	5. Tokens criptográficos Concepto de token criptográfico Tarjetas inteligentes Protecciones biométricas Normas	El tendrá los conceptos básicos acerca de tokens criptográficos para la protección de los datos.	E.M. C.L. M.A. P.R. D.T.	Libros: 2,3,4,5
20	6. Seguridad en las aplicaciones de Internet Seguridad en el nivel de transporte: SSL/TLS Seguridad en correo electrónico: PGP, PE; y S/MIME	El alumno tendrá los conceptos básicos acerca de la seguridad de los datos a través de Internet, sus riesgos y soluciones.	E.M. C.L. M.A. P.R. D.T.	Libros: 4,5

20	7. Problemática de la seguridad en los sistemas de gestión de la información Virus, troyanos y gusanos Técnicas de spoofing Vulnerabilidad de los sistemas informáticos Sistemas de defensa: Firewalls, IDS Sistemas de gestión de la seguridad: ISO17799 y UNE71502	El alumno conocerá la problemática de la seguridad de los sistemas de gestión de información: sus riesgos y soluciones.	E.M. C.L. M.A. P.R. D.T	Libros 1,5
----	---	---	-------------------------------------	------------

PERFIL PROFESIOGRÁFICO DEL DOCENTE

ESTUDIOS REQUERIDOS: Licenciado en Informática, Ingeniero en Sistemas Computacionales, en Computación o en Informática, Licenciatura en Sistemas Computacionales
EXPERIENCIA PROFESIONAL DESEABLE: En Áreas de Seguridad de Sistemas o afín.
OTROS REQUERIMIENTOS: Ninguno

MODALIDADES DE CONDUCCIÓN DEL PROCESO ENSEÑANZA APRENDIZAJE

Exposición oral
Exposición audiovisual
Ejercicios dentro de la clase
Seminarios
Trabajos de investigación

CRITERIOS DE EVALUACIÓN

Exámenes parciales	30%
Proyecto Final	50%
Trabajos y tareas fuera del aula	10%
Participación en clase	10%
Asistencia a clases	

BIBLIOGRAFÍA BÁSICA:

1. Stallings, W., *Fundamentos de seguridad en redes: aplicaciones y estándares*, 2ª. Ed. Pearson-Prentice-Hall, 2004
2. Fuster, A., de la Guía., D. Hernández, H. Montoya, F. y Muñoz, J, *Técnicas criptográficas de protección de datos*, 2ª. Ed. 2000, 2002
3. Housley, R., Ford, W. and Solo, D. *Internet X.509 Public Key Infrastructure Certificate and CRL Profile*, RFC 3280, 2002
4. McClure, S. Scambray, J and Kurts , G. Hackers, *Secretos y soluciones para la seguridad en redes*, McGraw-Hill, 2002
5. Cariacedo, J., *Seguridad en Redes Telemáticas*, McGraw-Hill, 2004

CLAVE DE MODALIDADES DE CONDUCCIÓN DEL PROCESO ENSEÑANZA APRENDIZAJE

E.M.	EXPOSICIÓN DEL MAESTRO	E.D.	EXPOSICIÓN DIALÉCTICA	E.P.	EJERCICIO PRÁCTICO
C.L.	CONTROL DE LECTURA	M.A.	MATERIAL AUDIOVISUAL	P.R.	PREGUNTAS Y RESPUESTAS
I.A.	INVESTIGACIÓN POR PARTE DE LOS ALUMNOS	V.C.	VISITA DE CAMPO	D.T.	DISCUSIÓN DE TEMAS
		E.A.	EXPOSICIÓN DE LOS ALUMNOS	C.D.	CONFERENCIA DIALÉCTICA