



UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO
Facultad de Estudios Superiores Aragón
Plan de Estudios



Ingeniería en Computación
Seguridad Informática

Clave	Semestre	Créditos	Área	
	9	8.0	Redes	
Modalidad	Curso		Tipo	Teórico
Carácter	Obligatorio			
Horas				
Semana			Semestre	
Teóricas	4.0		Teóricas	64.0
Prácticas	0.0		Prácticas	0.0
Total	4.0		Total	64.0

Seriación indicativa

Asignatura antecedente	Redes de Computadoras 2 y Sistemas Operativos
Asignatura subsecuente	Ninguna

Objetivo general: Conocer los fundamentos básicos de la seguridad informática aplicables a todas las áreas de la Ingeniería en Computación.

Índice temático

No.	Tema	Horas Semestre	
		Teóricas	Prácticas
1	INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA	5.0	0.0
2	ARQUITECTURA DE SEGURIDAD DE LA INFORMACIÓN	10.0	0.0
3	CRİPTOGRAFÍA Y SUS APLICACIONES EN LA SEGURIDAD INFORMÁTICA	15.0	0.0
4	NORMATIVIDAD DE LA SEGURIDAD DE LA INFORMACIÓN	10.0	0.0
5	SEGURIDAD EN REDES DE COMPUTADORAS	10.0	0.0
6	LEGISLACIÓN NACIONAL E INTERNACIONAL EN TEMAS DIGITALES	4.0	0.0
7	ÁREAS DE ESPECIALIDAD DE SEGURIDAD INFORMÁTICA	10.0	0.0
Total		64.0	0.0
Suma total de horas		64.0	

Contenido Temático	
1. INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA	
Objetivo: Identificar los conceptos, objetivos, antecedentes y tendencias de la Seguridad Informática.	
1.1	Antecedentes.
1.2	Panorama de la Seguridad Informática.
1.3	Definiciones y conceptos básicos.
1.4	Amenazas.
1.5	Riesgos.
1.6	Vulnerabilidad.
1.7	Atacantes informáticos.

2. ARQUITECTURA DE SEGURIDAD DE LA INFORMACIÓN	
Objetivo: Conocer una arquitectura de seguridad y los servicios que la soportan.	
2.1	Servicios de seguridad.
2.2	Confidencialidad.
2.3	Integridad.
2.4	Autenticación.
2.5	No repudio.
2.6	Control de acceso.
2.7	Mecanismos de seguridad.

3. CRIPTOGRAFÍA Y SUS APLICACIONES EN LA SEGURIDAD INFORMÁTICA	
Objetivo: Entender la relación entre la criptografía y la seguridad moderna, así como sus aplicaciones.	
3.1	Historia.
3.2	Criptografía simétrica.
3.3	Criptografía asimétrica.
3.4	Estenografía.
3.5	Funciones HASH.
3.6	Protocolos criptográficos.
3.7	Huella digital.
3.8	Firma digital.
3.9	Certificado digital.

4. NORMATIVIDAD DE LA SEGURIDAD DE LA INFORMACIÓN	
Objetivo: Conocer los estándares, políticas y procedimientos para mantener la seguridad de la información en las organizaciones.	
4.1	Estándares: ISO 17799 y 27002, ISO 27001 y Familia 27000.
4.2	ISO 27002: COMPONENTES

5. SEGURIDAD EN REDES DE COMPUTADORAS	
Objetivo: Conocer y analizar la seguridad informática aplicada a las redes informáticas.	
5.1	Defensa en profundidad.
5.2	Sniffers y monitores.
5.3	Dispositivos de seguridad perimetral.

6. LEGISLACIÓN NACIONAL E INTERNACIONAL EN TEMAS DIGITALES

Objetivo: Conocer la legislación en delitos informáticos para encuadrar su relevancia en el ambiente ético y profesional.

- 6.1 Antecedentes históricos (Convenio de Budapest).
- 6.2 Categoría de leyes: criminal, civil y administrativa.
- 6.3 Crimen tecnológico.
- 6.4 Propiedad Intelectual.
- 6.5 Privacidad.
- 6.6 Cumplimiento.

7. ÁREAS DE ESPECIALIDAD DE SEGURIDAD INFORMÁTICA

Objetivo: Identificar los diferentes panoramas de las diferentes áreas en las que se puede desarrollar un profesional en seguridad informática.

- 7.1 Gestión de la seguridad.
- 7.2 Respuesta a incidentes y cómputo forense.
- 7.3 Seguridad ofensiva.
- 7.4 Seguridad en aplicaciones y software.
- 7.5 Seguridad en entornos industriales.
- 7.6 Ciber inteligencia.

Estrategias didácticas		Evaluación del aprendizaje		Recursos	
Exposición	(X)	Exámenes parciales	(X)	Aula interactiva	()
Trabajo en equipo	(X)	Examen final	(X)	Computadora	(X)
Lecturas	(X)	Trabajos y tareas	(X)	Plataforma tecnológica	(X)
Trabajo de investigación	(X)	Presentación de tema	(X)	Proyector o Pantalla LCD	(X)
Prácticas (taller o laboratorio)	()	Participación en clase	(X)	Internet	(X)
Prácticas de campo	()	Asistencia	()		
Aprendizaje por proyectos	()	Rúbricas	()		
Aprendizaje basado en problemas	(X)	Portafolios	()		
Casos de enseñanza	()	Listas de cotejo	()		
Otras (especificar)		Otras (especificar)		Otros (especificar)	

Perfil profesiográfico	
Título o grado	<ul style="list-style-type: none"> • Poseer un título a nivel licenciatura en Ingeniería en Computación, Ingeniería en Telecomunicaciones, Matemáticas Aplicadas a la Computación o carreras cuyo perfil sea afín al área de Redes.
Experiencia docente	<ul style="list-style-type: none"> • Poseer conocimientos y experiencia profesional relacionados con los contenidos de la asignación a impartir. • Tener la vocación para la docencia y una actitud permanentemente educativa a fin de formar íntegramente al alumno: <ul style="list-style-type: none"> ○ Para aplicar recursos didácticos. ○ Para motivar al alumno. ○ Para evaluar el aprendizaje del alumno, con equidad y objetividad.
Otra característica	<ul style="list-style-type: none"> • Poseer conocimientos y experiencia pedagógica referentes al proceso de enseñanza-aprendizaje. • Tener disposición para su formación y actualización, tanto en los conocimientos de su área profesional, como en las pedagógicas. • Identificarse con los objetivos educativos de la institución y hacerlos propios. • Tener disposición para ejercer su función docente con ética profesional: <ul style="list-style-type: none"> ○ Para observar una conducta ejemplar fuera y dentro del aula. ○ Para asistir con puntualidad y constancia a sus cursos. ○ Para cumplir con los programas vigentes de sus asignaturas.

Bibliografía básica	Temas para los que se recomienda
Maíllo, J. A. (2017). <i>Seguridad digital e informática</i> . Madrid: Ra-Ma.	1,2,3,4,5,6 y 7
Mollin, R. (2005). <i>Codes: The Guide to Secrecy From Ancient to Modern Times</i> . Florida: Chapman & Haxll/CRC.	1,2,3,4,5,6 y 7
Pfleeger, C. P. (2003). <i>Security in Computing</i> . New Jersey: Prentice- Hall.	1,2,3,4,5,6 y 7
Sigh, S. (2000). <i>The Code Book, The Science of Secrecy from Ancient Egypt to Quantum Cryptography</i> . New York:- Anchor Books & Random House Inc.	3
Stamp, M. (2001). <i>Information Security Principles and Practices</i> . John Wiley & Sons.	1,2,3,4,5 y 6



Bibliografía complementaria	Temas para los que se recomienda
Caballero, A. (2018) <i>El libro del hacker.</i> Madrid: Anaya Multimedia.	1,2,3,4,5,6 y 7
David, K. (1996). <i>The Codebreakers, The Comprehensive History of Secret Communication from Ancient Times to the Internet.</i> Ney York: Simon & Schuster.	1,2,3,4,5,6 y 7