PLAN DOCENTE DE LA ASIGNATURA

Curso académico: 2026/27

Identificación y características de la asignatura					
Código	501283				
Denominación (español)	Biometría y Seguridad de Sistemas				
Denominación (inglés)	Biometrics and Systems Security				
Titulaciones	Grado en Ingeniería Informática en Ingeniería de Computadores (GIIIC), Grado en Ingeniería Informática en Ingeniería del Software (GIIIS)				
Centro	Escuela Politécnica				
Módulo	De Tecnología Específica en Ingeniería de Computadores				
Materia	Biometría y Seguridad de Sistemas				
Carácter	GIIIC: Obligatoria, GIIIS: Optativa	ECTS	6	Semestre	6

Profesor/es		
Nombre	Despacho	Correo-e
Rafael Martín Espada	Nº 70, Informática	rmmartin@unex.es
Área de conocimiento	Ingeniería Telemática	
Departamento	Ingeniería de Sistemas Informáticos y Telemáticos	
Nombre	Despacho	Correo-e
David Rodríguez Lozano		drlozano@unex.es
Área de conocimiento	Arquitectura y Tecnología de los Computadores	
Departamento	Tecnología de los Computadores y las Comunicaciones	
Profesor/a coordinador/a	Rafael Martín Espada	

Competencias / Resultados de aprendizaje

Básicas:

CB1 - Que los estudiantes hayan demostrado poseer y comprender conocimientos en un área de estudio que parte de la base de la educación secundaria general, y se suele encontrar a un nivel que, si bien se apoya en libros de texto avanzados, incluye también algunos aspectos que implican conocimientos procedentes de la vanguardia de su campo de estudio.

CB2 - Que los estudiantes sepan aplicar sus conocimientos a su trabajo o vocación de una forma profesional y posean las competencias que suelen demostrarse por medio de la elaboración y defensa de argumentos y la resolución de problemas dentro de su área de estudio.

CB3 - Que los estudiantes tengan la capacidad de reunir e interpretar datos relevantes (normalmente dentro de su área de estudio) para emitir juicios que incluyan una reflexión sobre temas relevantes de índole social, científica o ética.

CB4 - Que los estudiantes puedan transmitir información, ideas, problemas y soluciones a un público tanto especializado como no especializado.

CB5 - Que los estudiantes hayan desarrollado aquellas habilidades de aprendizaje necesarias para emprender estudios posteriores con un alto grado de autonomía.

Generales:

CG03 - Capacidad para diseñar, desarrollar, evaluar y asegurar la accesibilidad, ergonomía, usabilidad y seguridad de los sistemas, servicios y aplicaciones informáticas, así como de la información que gestionan.

CG05 - Capacidad para concebir, desarrollar y mantener sistemas, servicios y aplicaciones informáticas empleando los métodos de la ingeniería del software como instrumento para el

aseguramiento de su calidad, de acuerdo con los conocimientos adquiridos según lo establecido en el apartado 5 del anexo II de la resolución de la Secretaria General de Universidades de 8 de junio de 2009 (BOE de 4 de agosto de 2009) para la tecnología específica de Ingeniería de Computadores. CG07 - Capacidad para conocer, comprender y aplicar la legislación necesaria durante el desarrollo de la profesión de Ingeniero Técnico en Informática y manejar especificaciones, reglamentos y normas de obligado cumplimiento. CG11 - Capacidad para analizar y valorar el impacto social y medioambiental de las soluciones técnicas, comprendiendo la responsabilidad ética y profesional de la actividad del Ingeniero Técnico en Informática. Específicas de Ingeniería de Computadores: CIC06: Capacidad para comprender, aplicar y gestionar la garantía y seguridad de los sistemas informáticos. Específicas de Ingeniería del Software: CIS05 - Capacidad de identificar, evaluar y gestionar los riesgos potenciales asociados que pudieran presentarse. Transversales: CT04 - Capacidad de comunicación escrita efectiva. CT10: Habilidades de relaciones interpersonales.

Contenidos
Breve descripción del contenido
Fundamentos de la seguridad de la información y su aplicación a la seguridad de los sistemas informáticos. Principios fundamentales de las políticas de seguridad en los sistemas y su aplicación en la administración segura, usando las herramientas actuales. Sistemas biométricos actuales (basados en iris, retina, huella dactilar, geometría de la mano, escritura, voz, facial, …). Seguridad contra ataques biométricos. Estudio y comparativa entre los diferentes sistemas de seguridad. Aplicación de estos sistemas a la seguridad de los distintos sistemas operativos y web en base a sus capacidades.
Temario de la asignatura
Denominación del tema 1: Fundamentos de Seguridad de la Información y de los Sistemas. **Contenidos del tema 1**: Fundamentos de Seguridad. Herramientas para la seguridad: La política de seguridad.
Denominación del tema 2: Fundamentos de Criptografía. **Contenidos del tema 2**: Introducción a la criptografía. Criptografía de clave privada y secreto de mensajes. Criptografía de clave pública y Autenticación de Mensajes. Distribución de claves y Autenticación de usuarios.
Denominación del tema 3: Seguridad en los Sistemas. **Contenidos del tema 3**: Software malicioso. Intrusos
Denominación del tema 4: Seguridad en los Sistemas y en las redes. **Contenidos del tema 4**: Cortafuegos.
Denominación del tema 5: Aspectos generales de la biometría. **Contenidos del tema 5**: Introducción a la biometría - Tipos de biometría - Introducción a la biometría aplicada a la seguridad.
Denominación del tema 6: Biometría estática. **Contenidos del tema 6:** Características de los sistemas biométricos estáticos - Biometría de la huella dactilar, iris y retina - Geometría de la mano - Combinación de tecnologías.
Denominación del tema 7: Biometría dinámica: **Contenidos del tema 7:** Características de los sistemas biométricos dinámicos - Reconocimiento de voz - Reconocimiento de firma escrita y escritura - Dinámica de tecleo - Combinación de tecnologías.
Denominación del tema 8: Aplicaciones biométricas en la seguridad: **Contenidos del tema 8:** Biometría en la seguridad informática - Aplicaciones - Estándares biométricos.
Actividades prácticas:

- 1. Herramientas de seguridad de la información I
- 2. Herramientas de seguridad de la información II
- 3. Algoritmos criptográficos de la JCA I
- 4. Algoritmos criptográficos de la JCA II
- 5. Herramientas de seguridad de sistemas.
- 6. Firewalls
- 7. Algoritmos biométricos I.
- 8. Algoritmos biométricos II.

Actividades formativas

Horas de trabajo del alumno/a por tema		Horas Gran grupo	Actividades prácticas				Actividad de seguimiento	No presencial
Tema	**Total**	**GG**	**CH**	**L**	**O**	**S**	**TP**	**EP**
1	16,5	3		1,5			0	12
2	20,75	5		3			0	12,75
3	18,5	5		3			1	9.5
4	18,5	4,5		3			0,5	10,5
5	14,25	3		2			0	9,25
6	18,5	5		3			0	10,5
7	19,5	5		3			1	10,5
8	19,5	4		3			0,5	12
Evaluación	4	3		1			0	0
Total	**150**	**37,5**		**22,5**			**3**	**87**

GG: Grupo Grande (85 estudiantes).
CH: Actividades de prácticas clínicas hospitalarias (7 estudiantes)
L: Actividades de laboratorio o prácticas de campo (15 estudiantes)
O: Actividades en sala de ordenadores o laboratorio de idiomas (20 estudiantes)
S: Actividades de seminario o de problemas en clase (40 estudiantes).
TP: Tutorías Programadas (seguimiento docente, tipo tutorías ECTS).
EP: Estudio personal, trabajos individuales o en grupo, y lectura de bibliografía.

Metodologías docentes

Clases teórico-prácticas en el aula, para el desarrollo de los contenidos fundamentales de la materia; actividades breves, individuales o en grupo que permitan aplicar los conceptos expuestos y resolver problemas, facilitando la participación activa de los estudiantes.

Sesiones de laboratorio, actividades prácticas, sesiones de laboratorio guiadas, seminarios de resolución de problemas, etc. en grupos bajo la dirección de un profesor.

Tutorías programadas, individuales o en grupos pequeños se realizará un seguimiento más individualizado del estudiante, con actividades de formación y orientación. Principalmente, se utilizarán para el seguimiento de los trabajos planteados, debate sobre alternativas y evaluación de los objetivos alcanzados.

Realización de actividades, trabajos y estudio por parte del estudiante, de manera autónoma, individualmente o en grupo. Las actividades que el estudiante desarrollará de manera no presencial estarán orientadas principalmente al desarrollo de los proyectos y trabajos solicitados, bien individualmente o en grupo.

Resultados de aprendizaje

- Conoce los aspectos fundamentales sobre los distintos sistemas biométricos (basados en iris, retina, huella dactilar, geometría de la mano, escritura, voz, facial, etc.).
- Entiende las etapas básicas para el diseño de los distintos sistemas biométricos, teniendo en cuenta la seguridad contra ataques biométricos.

- Comprende los fundamentos de la seguridad de sistemas, sabiendo aplicar dichas técnicas a la seguridad avanzada de sistemas operativos y web.
- Conoce los fundamentos de la seguridad de la información y de los sistemas informáticos. Domina los conceptos relacionados con las políticas de seguridad en sistemas.
- Conoce las metodologías, las técnicas y las herramientas para proporcionar seguridad a los sistemas.
- Conoce y aplica en actividades de nivel medio las competencias transversales indicadas.

Sistemas de evaluación

De acuerdo a la *Normativa de Evaluación de las Titulaciones oficiales de Grado y Máster de la Universidad de Extremadura*, la asignatura puede superarse siguiendo un sistema de evaluación continua o con una prueba final global.
De acuerdo a dicha normativa, el estudiante debe elegir el sistema de evaluación a seguir siguiendo el procedimiento indicado que se pondrá a disposición del estudiante (campus virtual de la asignatura, en las primeras semanas del semestre). Por omisión, se entiende que el estudiante elige la evaluación continua.

La evaluación de la asignatura consistirá en la valoración tanto de los conceptos teóricos como de los supuestos prácticos planteados. Esta evaluación se hará de forma continuada a lo largo del curso, pudiendo realizarse también mediante una evaluación global final.

Evaluación de contenidos teóricos. Consistirá en varias pruebas compuestas de preguntas teóricas y ejercicios relativos al contenido del programa teórico de la asignatura, y en la realización y entrega de varias actividades.

Evaluación de supuestos prácticos. Consistirá en la entrega y evaluación de supuestos prácticos propuestos en las sesiones prácticas de la asignatura. Para superar la parte práctica se exige una asistencia mínima al 80% de las clases prácticas. Se podrá realizar un examen de prácticas.

Evaluación final de la asignatura. La calificación final de la asignatura consistirá en la suma ponderada de las evaluaciones teórico-prácticas. Es condición imprescindible haber superado ambas partes por separado, con una nota mínima de 5 sobre 10. La ponderación final se establece considerando 2/3 de la nota final para la parte teórica, y 1/3 de la nota final para la parte práctica. Se establece la posibilidad de compensar ambas partes a partir de una nota mayor o igual a 4, siempre y cuando la parte aprobada haya obtenido una calificación mayor o igual a 7.

Cada una de las partes, teoría y práctica, podrá aprobarse por separado y su nota se guardará a lo largo de las convocatorias dentro de un mismo curso académico, sólo si se obtiene una calificación mínima de 5 sobre 10.

Los estudiantes que no superen la evaluación continua o no deseen seguirla, tendrán una prueba de evaluación final de las dos partes, teoría y práctica.

Bibliografía (básica y complementaria)

Bibliografía:

- *Effective Cybersecurity. A guide to using best practices and standards*. William Stallings, Ed. Addison-Wesley, 2019.
- *Network Security Essentials. Applications and Standards*, William Stallings, Ed. Pearson, 6ª Ed., 2017.
- *Seguridad en Redes*, Chris McNab, Ed. Anaya-Multimedia, 2ª edición, 2008. *Tecnologías biométricas aplicadas a la seguridad*, Marino Tapiador y Juan A. Sigüenza, Ed. Ra-ma, 2005.
- *Seguridad en Redes*, Chris McNab, Ed. Anaya-Multimedia, 2ª edición, 2008.

Otros recursos y materiales docentes complementarios

Recursos: Espacio virtual de la asignatura, disponible en el Campus Virtual de la Universidad de Extremadura.