

PROGRAMA DE LA ASIGNATURA

Curso académico: 2017/18

Identificación y características de la asignatura			
Código	501283	Créditos ECTS	6
Denominación (español)	Biometría y Seguridad de Sistemas		
Denominación (inglés)	Biometrics and Systems Security		
Titulaciones	Grado en Ingeniería Informática en Ingeniería de Computadores (GIISC), Grado en Ingeniería Informática en Ingeniería del Software (GIIS)		
Centro	Escuela Politécnica		
Semestre	6º	Carácter	GIIC: Obligatoria, GIIS: Optativa
Módulo	De Tecnología Específica en Ingeniería de Computadores		
Materia	Biometría y Seguridad de Sistemas		
Profesor/es			
Nombre	Despacho	Correo-e	Página web
Lorenzo M. Martínez Bravo	3 (Edificio Informática)	lorenzom@unex.es	http://gitaca.unex.es
Área de conocimiento	Ingeniería Telemática		
Departamento	Ingeniería de Sistemas Informáticos y Telemáticos		
Nombre	Despacho	Correo-e	Página web
David Rodríguez Lozano		drlozano@unex.es	http://arco.unex.es/documentos_arco/articulos/member.html
Área de conocimiento	Arquitectura y Tecnología de los Computadores		
Departamento	Tecnología de los Computadores y las Comunicaciones		
Profesor coordinador	Lorenzo M. Martínez Bravo		
Competencias			
<p><u>Básicas:</u></p> <p>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.</p> <p>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.</p> <p>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.</p> <p>CB4 - Que los estudiantes puedan transmitir información, ideas, problemas y soluciones a un público tanto especializado como no especializado.</p> <p>CB5 - Que los estudiantes hayan desarrollado aquellas habilidades de aprendizaje necesarias</p>			

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 antes mencionada 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
<p>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.</p> <p>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.</p>
Temario de la asignatura
<p>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.</p>
<p>Denominación del tema 2: Fundamentos de Criptografía. Contenidos del tema 6: Introducción a la criptografía. Criptografía de clave privada y secreto de mensajes.</p>
<p>Denominación del tema 3: Criptografía avanzada. Contenidos del tema 3: Criptografía de clave pública y Autenticación de Mensajes. Distribución de claves y Autenticación de usuarios.</p>
<p>Denominación del tema 4: Seguridad en los Sistemas. Contenidos del tema 4: Software malicioso. Intrusos. Cortafuegos.</p>
<p>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.</p>
<p>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.</p>
<p>Denominación del tema 7: Biometría dinámica: Contenidos del tema 7: Características de los sistemas biométricos dinámicos -</p>

Reconocimiento de voz - Reconocimiento de firma escrita y escritura - Dinámica de teclado - 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. Uso de algunas herramientas de seguridad.
- 2 y 3. Uso de algoritmos criptográficos de la JCA.
- 4. Uso de algoritmos biométricos.

Temporización de temas

	Enero		Febrero			Marzo			Abril			Mayo			
Tema/ Semana	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1															
2															
3															
4															
5															
6															
7															
8															
Exámenes															Final

Actividades formativas

Horas de trabajo del alumno por tema		Presencial		Actividad de seguimiento	No presencial
Tema	Total	GG	SL	TP	EP
1	16,5	3	1	0,25	10
2	20,75	4	2	0,5	14,25
3	18,5	4	2	0,5	13
4	18,5	4	2	0,5	13
5	14,25	3	1	0,25	12
6	18,5	4	2	0,5	12
7	19,5	4	2	0,5	12
8	19,5	4	2	0,5	12
Evaluación del conjunto	4	3	1		
Total	150	33	15	3,75	98,25

GG: Grupo Grande (100 estudiantes).

SL: Seminario/Laboratorio (prácticas clínicas hospitalarias = 7 estudiantes; prácticas laboratorio o campo = 15; prácticas sala ordenador o laboratorio de idiomas = 30, clases problemas o seminarios o casos prácticos = 40).

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 las normas básicas de comportamiento, en su actividad diaria como estudiante, puntualidad en la asistencia a clase, respeto al compañero, etc.
- Conoce las habilidades como empatía, comprensión y tolerancia.
- Reconoce los gestos de discriminación por razón de raza, sexo, etnia, religión y los rechaza. Comprende la necesidad de la discriminación positiva en la lucha por la igualdad de género.
- Aplica las habilidades sociales en todas las facetas de su vida académica.

Sistemas de evaluación

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 una prueba compuesta de preguntas relativas al contenido del programa teórico de la asignatura.

Evaluación de supuestos prácticos. Consistirá en la evaluación de los 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.

Evaluación final de la asignatura. La evaluación final de la asignatura consistirá en la suma ponderada de las evaluaciones teórico-prácticas. Para considerar la nota final 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 de que consta el examen 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)
<p>Bibliografía:</p> <ul style="list-style-type: none"> • <i>Network Security Essentials. Applications and Standards</i>, William Stallings, Ed. Prentice-Hall, 5ª Edición, 2013. • <i>Seguridad de la Información</i>, Javier Areitio. Ed. Paraninfo, 2008. • <i>Tecnologías biométricas aplicadas a la seguridad</i>, Marino Tapiador y Juan A. Sigüenza, Ed. Ra-ma, 2005. • <i>Seguridad en Redes</i>, Chris McNab, Ed. Anaya-Multimedia, 2ª edición, 2008.
Otros recursos y materiales docentes complementarios
<p>Recursos: Aula virtual de la asignatura, disponible en el Campus Virtual de la Universidad de Extremadura.</p>
Horario de tutorías
<p>Tutorías programadas: Los horarios se publicarán en la primera semana de clase.</p> <p>Tutorías de libre acceso (horarios provisionales):</p> <p>Lorenzo M. Martínez Bravo Lunes: 9:30 a 11:30 h, Martes: 9:30 a 11:30 h y Miércoles: 9:30 a 11:30 h.</p> <p>David Rodríguez Lozano Miércoles: de 19 a 21h y Viernes: de 18 a 21</p>
Recomendaciones
<p>Se recomienda la asistencia a las clases de teoría, sesiones prácticas y tutorías programadas. Igualmente, se recomienda llevar al día la asignatura, dado que los conceptos (tanto teóricos como prácticos) se fundamentan en la asimilación de otros expuestos en temas anteriores. Se recomienda tener una actitud abierta, crítica y participativa en las discusiones y debates propuestos en las clases.</p>