UAB
Universitat Autònoma de Barcelona

Seguridad y Privacidad de los Sistemas de Información

Código: 106951
Créditos ECTS: 6

2025/2026

Titulación	Tipo	Curso
Gestión de Ciudades Inteligentes y Sostenibles	OB	3

Contacto

Nombre: Enric Alibech Romero

Correo electrónico: enric.alibech@uab.cat

Idiomas de los grupos

Puede consultar esta información al final del documento.

Prerrequisitos

No hay

Objetivos y contextualización

Proporcionar a los estudiantes los conocimientos fundamentales sobre seguridad informática aplicada a entornos urbanos inteligentes, capacitándolos para identificar, evaluar y mitigar riesgos de ciberseguridad en infraestructuras críticas urbanas, así como para proteger la privacidad de los ciudadanos en ecosistemas digitales complejos.

Resultados de aprendizaje

1. CM05 (Competencia) Relacionar los conocimientos y habilidades informáticas con los aportados por otros técnicos en equipos interdisciplinarios.
2. KM09 (Conocimiento) Entender el funcionamiento y la correcta gestión de las bases de datos.
3. SM06 (Habilidad) Emplear herramientas informáticas de transmisión de datos ajustados a los estándares internacionales.

Contenido

1. Seguridad de la Información 1.1. El valor de la información 1.2. Nociones básicas de seguridad de la información 1.3. Tipos de seguridad

2. Estrategias de seguridad práctica 2.1. Qué es la seguridad informática 2.2. Medidas básicas de seguridad 2.3. Seguridad en datos y aplicaciones 2.4. Entidades responsables de seguridad

3. Criptografía. Firma digital 3.1. Introducción y fundamentos de la criptografía 3.2. Claves públicas y privadas 3.3. Claves simétricas y asimétricas 3.4. Entidades certificadoras 3.5. La firma digital

4. Seguridad en redes de comunicaciones 4.1. Internet, funcionamiento, aplicaciones
5. Introducción al análisis de vulnerabilidades 5.1. Intrusión informática: explotación de vulnerabilidades 5.2. Explotación de vulnerabilidades. Etapas de una intrusión
6. Análisis forense 6.1. Ciencias forenses 6.2. Informática forense 6.3. Etapas del análisis forense informático 6.4. Análisis e investigación de los delitos informáticos. El marco legal
7. Cumplimiento normativo y Estándares internacionales 7.1. Planes de seguridad 7.2. Auditoría de sistemas de información 7.3. Normativa

Actividades formativas y Metodología

Título	Horas	ECTS	Resultados de aprendizaje
Tipo: Dirigidas			
Teoria	28	1,12	CM05, CM05
Tipo: Supervisadas			
Problemas y Prácticas	24	0,96	CM05, KM09, SM06, CM05
Tipo: Autónomas			
Trabajo autónomo (problemas y prácticas)	70	2,8	CM05, KM09, SM06, CM05

Los conocimientos teóricos se introducen y se refuerzan a través de la exposición oral del profesor, así como por medio del trabajo autónomo del alumno con el estudio de los materiales específicos o con actividades de aprendizaje propuestas por el profesor de la asignatura. Todos los datos y materiales de la asignatura estarán disponibles en el Campus Virtual. Esta misma plataforma será usada para lograr una comunicación fluida entre el alumnado y el profesor. La metodología docente estará basada en tres tipos de actividad:

- Actividad dirigida: clases teóricas, prácticas y de análisis de problemas.
- Actividad supervisada: asistencia a tutorías y realización de ejercicios con seguimiento pautado.
- Actividad autónoma: parte de estudio del alumno y resolución de casos, individualmente o en grupo

Nota: se reservarán 15 minutos de una clase dentro del calendario establecido por el centro o por la titulación para que el alumnado rellene las encuestas de evaluación de la actuación del profesorado y de evaluación de la asignatura o módulo.

Evaluación

Actividades de evaluación continuada

Título	Peso	Horas	ECTS	Resultados de aprendizaje
Elaboración de trabajos de prácticas con memoria descriptiva y defensa	30	20	0,8	CM05, KM09, SM06

Evaluación de los contenidos teóricos	60	4	0,16	CM05, KM09, SM06
Realización de las actividades de la clase de problemas	10	4	0,16	CM05, SM06

La evaluación del aprendizaje será de tipo continuo y consta de los siguientes elementos:

a) Dos pruebas sobre el contenido del temario. Estos exámenes se realizarán a mitad y al final del semestre. Representarán el 60% de la nota final (30% + 30%).

b) El estudiante realizará los trabajos prácticos en un grupo de dos personas. La realización del trabajo representa un 20% y la habilidad para buscar soluciones a problemas técnicos un 10%.

c) La evaluación de la participación activa del estudiante en los debates y las actividades del curso y la presentación de la documentación de defensa de los trabajos. Representará el 10% de la nota final.

1. Pruebas de evaluación continua

Hay dos pruebas que incluyen los seis bloques de materia (1, 2 y 3 en la primera prueba y 4, 5, 6 y 7 en la segunda prueba). Las fechas de evaluación continua se fijan al inicio del curso y no tienen fecha alternativa de recuperación en caso de inasistencia. En caso de producirse algún cambio de programación por motivos de adaptación a posibles incidencias, siempre se informará sobre estos cambios.

Proves d'avaluació continuada	Pes nota avaluació continuada	Nota mínima per fer promig
1,2,3	50%	4.0
4,5,6,7	50%	4.0

2. Nota final de l'avaluació

Nota final	Pes nota final
Avaluació continuada	60%
Treball Laboratori	30%
Habilitats de resolució de problemes de les sessions de problemes.	10%

1. Se considera aprobado todo aquel que:

Haya superado los dos exámenes con una nota mínima por examen de 4 y una calificación media mínima de 5. Tenga todos los entregables de los trabajos prácticos aprobados (nota mínima de 5 en todos y cada uno de los trabajos). Haya participado de manera regular en las actividades del curso. Alcance una calificación mínima global igual o superior a 5.

1. Calificación:

La calificación final de la asignatura resultará del promedio ponderado de todas las evidencias de evaluación: exámenes (60%), trabajo (20%), evaluación de las habilidades de resolución de problemas (10%) y participación y presentación (10%). Consistirá en una calificación entre 0 y 10. Para aprobar la asignatura es necesario haber obtenido una calificación mínima total de 5.

1. Re-evaluación

Una vez finalizada la evaluación ordinaria, el alumno/a tendrá la posibilidad de realizar un examen de re-evaluación dentro de las fechas que programe la Facultad.

a) Para poder optar a re-evaluación es necesario haber participado en las pruebas de evaluación y entregado los trabajos prácticos. b) Los resultados de los entregables de los trabajos prácticos no serán re-evaluables. c) En la re-evaluación, la nota máxima que se podrá obtener para cada una de las pruebas re-evaluadas es de 5.

1. Repetidores.

Al inicio del curso académico, en caso de que sea posible, se notificará si hay convalidación del trabajo y su defensa. En caso de ser así, la convalidación solo se realizará a aquellos alumnos que lo soliciten y hayan aprobado el trabajo y la defensa en el curso anterior. Para poder optar a esta evaluación diferenciada, el alumnado repetidor debe solicitarlo al profesor mediante correo electrónico (enric.alibech@uab.cat) como muy tarde 5 días después del inicio de las clases.

1. Casos no evaluables

En caso de que no se haga ninguna entrega, no se asista a ninguna sesión de laboratorio y no se realice ningún examen, la nota correspondiente será un "no evaluable". En cualquier otro caso, los "no presentados" computan como un 0 para el cálculo del promedio ponderado que, como máximo, será 4,5. Es decir, la participación en alguna actividad evaluada implica que se tengan en cuenta los "no presentados" en otras actividades como ceros. Por ejemplo, una ausencia en una sesión de laboratorio implica una nota de cero para esa actividad.

1. Matrículas de honor

Las matrículas de honor se concederán a quienes obtengan una nota superior o igual a 9,5 en cada parte, hasta el 5% de los matriculados según orden descendente de nota final. A criterio del profesorado, también se podrán conceder en otros casos.

1. Copias, plagios e irregularidades

Para esta asignatura, se permite el uso de tecnologías de Inteligencia Artificial (IA) exclusivamente en tareas de apoyo, como la búsqueda bibliográfica o de información, la corrección de textos o las traducciones. El estudiante deberá identificar claramente qué partes han sido generadas con esta tecnología, especificar las herramientas empleadas e incluir una reflexión crítica sobre cómo estas han influido en el proceso y el resultado final de la actividad. La no transparencia del uso de la IA en esta actividad evaluable se considerará falta de honestidad académica y puede conllevar una penalización parcial o total en la nota de la actividad, o sanciones mayores en casos de gravedad.

Sin perjuicio de otras medidas disciplinarias que se estimen oportunas, y de acuerdo con la normativa académica vigente, las irregularidades cometidas por un estudiante que puedan conducir a una variación de la calificación se calificarán con un cero (0). Por ejemplo, plagiar, copiar, dejar copiar, el uso no autorizado de la IA (p. ej., no hacer uso correcto tal y como se estipula en el párrafo anterior), etc., una actividad de evaluación, implicará suspender esta actividad de evaluación con un cero (0). Las actividades de evaluación calificadas de esta forma y por este procedimiento no serán recuperables. Si es necesario superar cualquiera de estas actividades de evaluación para aprobar la asignatura, esta asignatura quedará suspendida directamente, sin oportunidad de recuperarla en el mismo curso.

1. Evaluación única

Esta asignatura no prevé el sistema de evaluación única.

Bibliografía

- Colobran, M. Arques, J. Iparraguirre, J. Com s'ha de fer l'informe pericial d'un delicte informàtic? Editorial UOC (2012)
- Guia del Reglamento General de Protección de Datos para Responsables de Tratamiento. Agencia Espanyola de Protección de Datos. https://www.aepd.es/media/guias/guia-rgpd-para-responsables-de-tratamiento.pdf
- Guia práctica para las evaluaciones de impacto en la protección de los datos sujetas al RGPD. Agencia Espanyola de Protección de Datos. https://www.aepd.es/media/guias/guia-evaluaciones-de-impacto-rgpd.pdf
- GUÍA PRÁCTICA para la evaluación de impacto relativa a la protección de datos. Agencia Espanyola de Protección de Datos (2018) http://apdcat.gencat.cat/web/.content/03-documentacio/Reglament_general_de_proteccio_de_dades/docu
- Garcia, E. Lopez, M. Ortega,J Una introducción a la CRIPTOGRAFIA (2005) http://www.criptored.upm.es/guiateoria/gt_m182a.htm
- Smart Cities. Development and Governance Frameworks. Editors: Mahmood, Zaigham (Ed.) (2018)
- Smart Cities Cybersecurity and Privacy. Editors: Danda Rawat Kayhan Zrar Ghafoor. (1st November 2018)

Software

Se trabajará con amb la distribución actual de Kali Linux.

Grupos e idiomas de la asignatura

La información proporcionada es provisional hasta el 30 de noviembre de 2025. A partir de esta fecha, podrá consultar el idioma de cada grupo a través de este enlace. Para acceder a la información, será necesario introducir el CÓDIGO de la asignatura

Nombre	Grupo	Idioma	Semestre	Turno
(PAUL) Prácticas de aula	1	Catalán	segundo cuatrimestre	tarde
(PAUL) Prácticas de aula	2	Catalán	segundo cuatrimestre	tarde
(PLAB) Prácticas de laboratorio	1	Catalán	segundo cuatrimestre	tarde
(PLAB) Prácticas de laboratorio	2	Catalán	segundo cuatrimestre	tarde
(PLAB) Prácticas de laboratorio	3	Catalán	segundo cuatrimestre	tarde
(TE) Teoría	1	Catalán	segundo cuatrimestre	tarde