Universitat Autònoma de Barcelona

2019/2020

Seguridad y Privacidad de los Sistemas de Información

Código: 104539
Créditos ECTS: 6

Titulación	Tipo	Curso	Semestre
2503743 Gestión de Ciudades Inteligentes y Sostenibles	OB	2	2

Contacto

Nombre: Pedro Luis Pons Pons
Correo electrónico: Pere.Pons@uab.cat

Uso de idiomas

Lengua vehicular mayoritaria: catalán (cat)
Algún grupo íntegramente en inglés: No
Algún grupo íntegramente en catalán: No
Algún grupo íntegramente en español: No

Prerequisitos

No hay.

Objetivos y contextualización

En esta materia se introducirán los conceptos básicos relativos a al uso de las Tecnologías de la Información y las Comunicaciones (TIC) dentro de la sociedad, así como su uso e impacto en la privacidad y seguridad de los ciudadanos.

Se introducirán conceptos básicos de herramientas de ciberseguridad, auditorías, informática forense y una base legal.

Competencias

- Desarrollar plataformas de gestión, integración de servicios a los ciudadanos y a la gobernanza aplicando tecnologías y sistemas de sensorización, adquisición, procesado y comunicación de datos.
- Generar propuestas innovadoras y competitivas en la actividad profesional.
- Prevenir y solucionar problemas, adaptarse a situaciones imprevistas y tomar decisiones.
- Que los estudiantes hayan desarrollado aquellas habilidades de aprendizaje necesarias para emprender estudios posteriores con un alto grado de autonomía.
- Que los estudiantes puedan transmitir información, ideas, problemas y soluciones a un público tanto especializado como no especializado.
- 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.
- Resolver problemas de gestión urbana utilizando conocimientos, metodologías y procedimientos de diseño e implementación de aplicaciones informáticas para diferentes tipos de entornos (web, móvil, nube) y con diferentes paradigmas.

Resultados de aprendizaje

1. Describir las necesidades de seguridad de una aplicación informática como base para la gestión de un servicio donde se almacenen, se gestionen y se transmitan datos sensibles.
2. Describir los mecanismos esenciales de la transmisión de datos, y los estándares internacionales.
3. Generar propuestas innovadoras y competitivas en la actividad profesional.
4. Prevenir y solucionar problemas, adaptarse a situaciones imprevistas y tomar decisiones.
5. Que los estudiantes hayan desarrollado aquellas habilidades de aprendizaje necesarias para emprender estudios posteriores con un alto grado de autonomía.
6. Que los estudiantes puedan transmitir información, ideas, problemas y soluciones a un público tanto especializado como no especializado.
7. 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.

Contenido

Introducción

1. Seguridad de la información
1.1. El valor de la información
1.2. Nociones básicas de la seguridad de la información
1.3 Seguridad técnica y seguridad jurídica
1.4 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 la seguridad

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

4. Seguridad en redes de comunicaciones
4.1 Internet, funcionamiento y aplicaciones
4.2 Intrusión informática: explotación de vulnerabilidades
4.3 Explotación de vulnerabilidades: etapas de una intrusión

5. Análisis forense
5.1 Ciencias forenses
5.2 Informática forense
5.3 Etapas de un análisis forense informático
5.4 Análisis y investigación de delitos informáticos. El marco legal.

6. Cumplimiento normativo y estándares internacionales
6.1 Planes de seguridad
6.2 Auditoria de sistemas de información
6.3 Normativa

Metodología

Los conocimientos teóricos se introducen y se refuerzan a través de la exposición oral del profesor, así como por medio de 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.

Competencias transversales

T03. Generar propuestas innovadoras y competitivas en la actividad profesional.
T05. Evaluar de manera crítica el trabajo realizado y demostrar espíritu de superación.

Se tratarán y evaluarán las actividades supervisadas.

Actividades

Título	Horas	ECTS	Resultados de aprendizaje
Tipo: Dirigidas			
Teoria	26	1,04	2, 1, 5
Tipo: Supervisadas			
Problemas y prácticas	24	0,96	1, 3, 6, 7
Tipo: Autónomas			
Trabajo autónomo (prácticas, actividades)	96	3,84	3, 5

Evaluación

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 un trabajo solo o en un grupo de dos personas que al final se expondrá en clase. El docente propondrá una relación de varios temas a desarrollar, pero el estudiante puede proponer otros, siempre dentro del ámbito de la asignatura. La realización del trabajo representa un 20% y la exposición en clase un 10%.

c) La evaluación de la participación activa del estudiante en los debates y las actividades del curso. 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 y 6 en la segunda prueba). Las fechas de evaluación continua se fijan a inicio de curso y no tienen fecha alternativa de recuperación en caso de inasistencia. Caso de producirse algún cambio de programación por motivos de adaptación a posibles incidencias, siempre se informará sobre estos cambios.

Pruebas de evaluación continua	Peso nota avaluación continua	Nota mínima para hacer media

	50%	
1,2,3	50%	4.0
4,5,6		4.0

2. Nota final de la evaluación

Nota final	Peso nota final
Evaluación continua	60%
Trabajo	20%
Defensa del trabajo	10%
Participación del estudiante	10%

3. Se considera aprobado todo aquel que:

- Haya superado el dos exámenes (pruebas de evaluación continua) con una calificación media mínima de 5.
- Tenga el trabajo y su defensa aprobado (mínimo tener un 4 para poder hacer media).
- Haya participado de manera regular alas actividades del curso.
- Logre una calificación mínima global igual / superior a 5.

4. Calificación

La calificación final de la asignatura resultará de la media ponderada de todas las evidencias de evaluación: exámenes (60%), Trabajo (20%), defensa (10%) y participación (10%). Consistirá en una calificación entre 0 y 10. Para aprobar la asignatura es necesario haber obtenido una calificación mínima total de 5.

5.Reevaluación

Una vez terminada la evaluación ordinaria, el alumno / a tendrá la posibilidad de realizar un examen de reevaluación en las fechas que programe la Facultad.

a) Para poder optar a una reevaluación necesario haber participado en las pruebas de evaluación y entregado el trabajo así como haber hecho la defensa.
b) Los resultados del trabajo y de la defensa no serán reavaluables.
c) En la reevaluación, la nota máxima que se podrá obtener para cada una de las pruebas reavaluades es de 5.

6. Repetidores.
Al inicio de curso académico, en caso de que sea posible, se notificará si hay convalidación del trabajo y su defensa. Caso de estar, la convalidación sólo se realizará a aquellos alumnos que lo soliciten y hayan aprobado el trabajo y la defensa en el curso anterior.

7. Casos no evaluables

En caso de que no se haga ninguna entrega, no se asista a ninguna sesión de laboratorio y no se haga ningún examen, la nota correspondiente será un "no evaluable". En otro caso, los "no presentados" computan como un 0 para el cálculo de la media ponderada 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.

8. 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 otroscasos.

9. Copias, plagios e irregularidades

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, ..., 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.

Actividades de evaluación

Título	Peso	Horas	ECTS	Resultados de aprendizaje
Evaluación de los contenidos teóricos	60	4	0,16	2, 4, 6, 7
Participation	10	0	0	3, 7
Preparación de la memoria del trabajo y defensa	30	0	0	1, 3, 5

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)