Universitat Autònoma de Barcelona

2022/2023

Privacidad de Datos y Seguridad

Código: 104369
Créditos ECTS: 6

Titulación	Tipo	Curso	Semestre
2503758 Ingeniería de Datos	OT	4	1

Contacto

Nombre: Guillermo Navarro Arribas
Correo electrónico: guillermo.navarro@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

Equipo docente

Cristina Perez Sola

Prerequisitos

En esta asignatura se hará uso de conocimientos adquiridos durante la carrera. No hay ningún requisito obligatorio, pero sí que se asumirá que los estudiantes tienen una base de Criptografía (correspondiente a la asignatura criptografía y Seguridad) y conocimientos básicos sobre estadística, grafos, o programación.

Objetivos y contextualización

Los objetivos de la asignatura son:

- Entender la problemática de la privacidad en entornos digitales.
- Conocer de forma global herramientas que proporcionan privacidad a varios niveles.
- Entender los principales modelos de privacidad de datos.
- Entender y conocer mecanismos para la evaluación y protección de datos.
- Conocer algunos mecanismos criptográficos avanzados para la privacidad.
- Conocer mecanismos por la comunicación privada.

Competencias

- Demostrar sensibilidad hacia los temas éticos, sociales y medioambientales.
- Trabajar cooperativamente, en entornos complejos o inciertos y con recursos limitados, en un contexto multidisciplinar, asumiendo y respetando el rol de los diferentes miembros del equipo.

Resultados de aprendizaje

1. Demostrar sensibilidad hacia los temas éticos, sociales y medioambientales.
2. Trabajar cooperativamente, en entornos complejos o inciertos y con recursos limitados, en un contexto multidisciplinar, asumiendo y respetando el rol de los diferentes miembros del equipo.

Contenido

- Introducción a la privacidad
- Privacidad de datos
  - Modelos: k-anonimidad, privacidad diferencial
  - Métodos de protección por la privacidad de datos
  - Privacidad y aprendizaje automático
- Comunicaciones privadas
- Protocolos criptográficos por la privacidad

Metodología

La asignatura se imparte en sesiones de dos horas. Estas sesiones se organizarán de forma dinámica y requerirán una participación activa del alumnado. A lo largo del curso habrá sesiones de tipología más teórica y otro
de tipología práctica.

Las sesiones de tipo teórico se podrán estructurar de diversas maneras. En unos casos, el profesorado, previamente a la sesión, pondrá a disposición del alumnado material sobre el tema a tratar. Basándonos en este material, se estructurarán dos tipologías distintas de sesiones. Por un lado, sesiones de preguntas y respuestas donde los estudiantes formularán las dudas que les hayan surgido del trabajo previo sobre el material proporcionado. En estas sesiones, el profesorado también interpelará a los estudiantes para aflorar los aspectos más relevantes del material que se está trabajando. Por otra parte, habrá sesiones donde los estudiantes, en grupos de dos, presentarán algún estudio más detallado de alguno de los temas tratados en la asignatura. Dependiendo del tema concreto en tratar la sesión de teoría, también podrá estructurarse como clase magistral.

Las sesiones de tipo práctico incluyen la resolución de cuestiones o ejercicios, como la resolución de trabajos más técnicos de tipo prácticas.

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.

Actividades

Título	Horas	ECTS	Resultados de aprendizaje
Tipo: Dirigidas			
Clases prácticas	25	1	1, 2
Clases teóricas	25	1	1, 2
Tipo: Supervisadas			
Tutorías y consultas	10	0,4	1, 2
Tipo: Autónomas			
Preparación de clases prácticas	25	1	1, 2
Preparación de clases teóricas	37,5	1,5	1, 2

Evaluación

Esta asignatura utiliza un modelo de evaluación continua de forma única. Dado el dinamismo de la misma y la implicación que se pide al alumnado en todas las sesiones de clase (tanto las de carácter más teórico como las más
prácticas) el profesorado tendrá múltiples elementos para poder evaluar a los alumnos. La participación activa en las clases preguntando dudas al profesor y respondiendo dudas de los demás estudiantes o de las cuestiones del profesor supondrá es un ejemplo de evidencia por la evaluación. Es por este motivo que la asistencia a clase de esta asignatura es obligatoria.

Más allá de la evaluación en base a las aportaciones en las clases, los estudiantes también tendrán que entregar diferentes trabajos más prácticos que se irán proponiendo a lo largo del curso en el campus virtual de la UAB, entregas que complementarán las evidencias de evaluación del estudiante.

Por otra parte, la presentación del tema que los estudiantes harán en las sesiones teóricas de la asignatura también formará parte de las evidencias de evaluación.

Evaluación final: La evaluación final lo calcula ponderando las actividades de evaluación de la siguiente modo:

- Participación en clase: 20%
- Trabajos prácticos: 50%
- Preparación y presentación tema: 30%

Tanto los trabajos prácticos como la presentación de tema requieren una nota mínima de 5. En caso de no superar alguna de estas partes se podrá recuperar, aunque en este caso la nota máxima de la parte recuperada será un 5.

En caso de no superar la evaluación de la participación en clase, esta no se podrá recuperar.

Losalumnos que logren el número mínimo de puntos para aprobar, pero la asignatura no hayan alcanzado la nota mínima en alguna de las actividades de evaluación, serán evaluados con una nota final de 4.5. En caso de que no se halla aprobado la asignatura por la calificación de un cero de una actividad por motivo de copia, la nota final de la asignatura será un 3, lo que no permitirá compensar esta asignatura.

Obtendrán la calificación de "No Evaluable" aquellos estudiantes que no entreguen ninguna de las actividades prácticas que se propongan. La participación en alguna de estas actividades de evaluación supondrá recibir una calificación diferente de "No Evaluable".

Alumnado repetidor:No se contempla ningún tipo de convalidación de ninguna de las actividades evaluables para los estudiantes repetidores. Esta medida se podría relajarse dependiendo del curso y actividad concreta. Si así fuera el caso, a principio de curso se anunciará las condiciones y mecanismos para ello.

Calendario de actividades: Las fechas de evaluación continua y entrega de trabajos se publicarán en el campus virtual y pueden estar sujetos a cambios de programación por motivos de adaptación a posibles incidencias. Siempre se informará en el campus virtual y en clase sobre estos posibles cambios, ya que estos son los canales de intercambio de información entre profesores y estudiantes.

Concesión de MH: Solo podrán obtener una MH los estudiantes que tengan una nota igual o superior a los 9 puntos. Debido a que el número de MH no puede superar el 5% de los estudiantes matriculados, se concederán a los estudiantes que tengan las notas finales más altas.

Otros aspectos importantes de la evaluación: 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 en una actividad evaluable se calificarán 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. Estas irregularidades incluyen, entre otras:

- la copia total o parcial de una práctica, informe, o cualquier otra actividad de evaluación;
- dejar copiar;

- presentar un trabajo de grupo no realizado íntegramente por los miembros del grupo (aplicado a todos los miembros, no solo a los que no han trabajado);
- presentar como propios materiales elaborados por un tercero, aunque sean traducciones o adaptaciones, y por lo general trabajos con elementos no originales y exclusivos del estudiante;
- tener dispositivos de comunicación (como teléfonos móviles, smart watches, bolígrafos con cámara, etc.) accesibles durante las pruebas de evaluación;
- hablar con compañeros durante las pruebas de evaluación;
- copiar o intentar copiar de otros alumnos durante las pruebas de evaluación;
- usar o intentar utilizar escritos relacionados con la materia durante la realización de las pruebas de evaluación, cuando estos no hayan sido explícitamente permitidos.

La nota numérica del expediente será el valor menor entre 3.0 y la media ponderada de las notas en caso de que elestudiante haya cometido irregularidades en un acto de evaluación (y, por tanto, no será posible el aprobado por compensación). En ediciones futuras de esta asignatura, al estudiante que haya cometido irregularidades en un acto de evaluación no se le convalidará ninguna de las actividades de evaluación realizadas.

En resumen: copiar, dejar copiar o plagiar (o el intento de) en cualquiera de las actividades de evaluación equivale a un SUSPENSO, no compensable y sin convalidaciones de partes de la asignatura en cursos posteriores.

Actividades de evaluación

Título	Peso	Horas	ECTS	Resultados de aprendizaje
Actividades prácticas	50	12,5	0,5	1, 2
Participación en clase	20	14	0,56	1, 2
Preparación y presentación de un tema	30	1	0,04	1, 2

Bibliografía

Dado el dinamismo de la asignatura, muchas referencias bibliográficas y material se irá proporcionando durante el curso. Aquí se incluyen algunas referencias más genéricas:

- Vicenç Torra (2017) Data Privacy: Foundations, New Developments and the Big Data Challenge. Springer.
- Cynthia Dwork, Aaron Roth (2014) The Algorithmic Foundations of Differential Privacy. Foundations and Trends in Theoretical Computer Science (vol. 9, núm. 3-4, págs. 211-407).
- Solon Barocas, Moritz Hardt, Arvind Narayanan (2009) Fairness and Machine Learning. https://fairmlbook.org/
- Yevgeniy Vorobeychik, Murat Kantarcioglu. (2018) Adversarial Machine Learning. Synthesis Lectures on Artificial Intelligence and Machine Learning #38. Morgan & Claypool.
- Molnar, Christoph (2020). Interpretable Machine Learning: A Guide for Making Black Box Models Explainable.
- Christof Paar, Pelzl Jan. (2010) Understanding Cryptography: A Textbook for Students and Practitioners. Springer Berlin Heidelberg, 2010.

Software

Dada la multidiciplinaridad de esta asignatura se utilizarán diferentes herramientas y lenguajes de programación dependiendo de la actividad concreta a realizar, tanto para las prácticas como por las actividades y ejercicios.