RESPONSABLE(S) DE TUTORIZACIÓN				TRABAJO FIN DE GRADO			DETALLE DEL TFG			
Número	DPTO	RESPONSABLE DE TUTORIZACIÓN	RESPONSABLE DE COTUTORIZACIÓN si procede	TIPOLOGÍA	TÍTULO	ESTUDIANTE	Descripción, resumen de contenidos y actividades a desarrollar en el ámbito de la Informática	Descripción, resumen de contenidos y actividades a desarrollar en el ámbito de las Matemáticas	Materias del Grado relacionadas	HARDWARE/SOFTWARE/BIBLIOGRAFÍA
21	**CCIA / AM**	Francisco Javier Meri de la Maza	Nuria Rodríguez Barroso	Complementario de profundización / Iniciación a la investigación	Sistemas de optimización para el balance entre resiliencia a ataques a la privacidad y rendimiento en Aprendizaje Federado.	Julio Pérez Cabeza	Uno de los principales problemas de los modelos de Inteligencia Artificial más usados en la actualidad, es la privacidad de los datos cuando estos provienen de contextos sensibles. Como solución a este problema surge el Aprendizaje Federado [I1], un paradigma de aprendizaje distribuido en el cual los datos de entrenamiento nunca salen de los dispositivos originales. Aún así, este paradigma es vulnerable a diferentes ataques a la privacidad [I2]. En este TFG se propone el estudio de los diferentes ataques a la privacidad que puede sufrir el Aprendizaje Federado así como el desarrollo de mecanismos de defensa frente a estos ataques. Para ello, se usarán mecanismos de programación lineal para optimizar la cantidad de Privacidad Diferencial [I3] empleada, encontrando un balance entre privacidad, resiliencia a ataques y rendimiento.	Se propone realizar un desarrollo teórico de distintos tipos de optimización, desde los modelos más simples a los más complejos. Se propone comenzar recordando el teorema de Minkowski-Carathéodory y su aplicación en programación lineal. Se propone también desarrollar algunos aspectos de programación convexa y presentar algunos resultados clásicos de optimización de funciones convexas como el principio del máximo de Bauer, que se puede obtener como consecuencia del Teorema de Krein Milman [M1,M2].	Análisis Matemático I y II, Análisis Funcional. Inteligencia Artificial. Visión por Computador. Aprendizaje Automático.	[M1] L. Berkowitz, Convexity and optimization in R^n, John Wiley & Sons, Inc., New York, 2002 [M2] H. Tuy, Convex analysis and global optimization (second edition), Springer International Publishing, 2016 [I1] Kairouz, P., McMahan, H. B., Avent, B., Bellet, A., Bennis, M., Bhagoji, A. N., ... & Zhao, S. (2021). Advances and open problems in federated learning. Foundations and trends® in machine learning, 14(1–2), 1-210. [I2] Rodríguez-Barroso, N., Jiménez-López, D., Luzón, M. V., Herrera, F., & Martínez-Cámara, E. (2023). Survey on federated learning threats: