PROPUESTA DE TRABAJO FIN DE MÁSTER (Modalidad B)
Curso 2023-2024
MÁSTER EN TÉCNICAS ESTADÍSTICAS

Título	Estudio de ataques prácticos a la privacidad de algoritmos de ML en entornos de aprendizaje federado
Nombre de la Empresa **Tutor/a en la empresa** **Tutor/a académico/a**	Centro tecnológico de telecomunicaciones de Galicia (GRADIANT) Inés Ortega Marta Sestelo
Descripción del trabajo a realizar	El federated learning (FL) es un enfoque de aprendizaje automático distribuido que permite que varias entidades realicen entrenamiento local de modelos, compartiendo los parámetros en lugar de los datos de entrenamiento en sí. Si bien el Federated Learning ofrece muchas ventajas, como la privacidad de los datos, también es susceptible a ciertos ataques basados en técnicas estadísticas y de inteligencia artificial que pueden comprometer la privacidad. Los ataques a la privacidad en FL se basan en el uso de modelos estadísticos que permitan identificar las diferencias en las predicciones realizadas por el modelo de la víctima entre ejemplos que pertenecen al conjunto de entrenamiento y ejemplos que no. Otros enfoques explotan vulnerabilidades en el algoritmo de descenso del gradiente que permiten extraer información relevante para la ejecución del ataque. Este TFM plantea el estudio, documentación e implementación de ataques basados en técnicas estadísticas que permitan demostrar la vulnerabilidad de un esquema de FL, como pueden ser ataques de inferencia o re-identificación. El estudiante se integrará en el equipo de trabajo del proyecto europeo de investigación TRUMPET, donde GRADIANT lidera un consorcio de 9 instituciones europeas para la investigación de nuevos métodos de protección de la privacidad de entornos de aprendizaje federado.
Recomendaciones	Machine Learning/Inteligencia Artificial

Fechas de las practicas	Septiembre (a concretar con el alumno/a)
Lugar de trabajo y horario	Carretera do Vilar 56-58, Vigo, Pontevedra, 36214 Horario a concretar con el alumno/a
Convenio	Convenio de Cooperación Educativa
Otras observaciones	Remuneración 965€ brutos/jornada completa