# Proyecto de Tesis de Maestría

(Ramón René Palacio Cinco)

**Título:** Modelo de protección a la privacidad en el contexto de aprendizaje automatizado.

**Problema a resolver:** Realizar la implementación y análisis de un algoritmo de Machine Learning (ML) considerando dos perspectivas para proteger la privacidad de los datos (homomorfica y diferencial) considerando que: El objetivo de ML [1] es extraer información útil de los datos, tales como la forma de clasificar los datos, cómo predecir una cantidad, o cómo encontrar grupos de muestras similares. Dada una familia de modelos de aprendizaje, los algoritmos de ML seleccionan y presentan el mejor basado en algunos datos dados. El modelo de salida puede ser usado en ya sea tratando con datos futuros o interpretando la distribución de los datos. Aun que el modelo de salida es típicamente mucho más compacto que el conjunto de datos fundamental, debe capturar alguna información que describa el conjunto de datos. La privacidad [2, 3], por otro lado, se refiere a la protección de datos privados que puedan filtrarse, especialmente la información de los individuos. Sería razonable preguntar, "¿por qué es insuficiente anonimizar los datos?" Uno podría eliminar los nombres y otra información obviamente identificable de una base de datos. Podría entonces parecer difícil, para un atacante identificar a un individuo. Las reglas actuales de HIPAA [4] promueven un enfoque de este tipo, listando 18 categorías de información de identificación personal que debe ser redactada en el caso de datos de investigación para su publicación. Desafortunadamente, el método puede filtrar información cuando el atacante ya tenga cierta información sobre los individuos en cuestión. Un esquema de encriptación homomórfica total es un esquema normal de encriptación (dos funciones "enc" y "dec" para encriptar y decriptar) con una función adicional, la cual podemos llamar "eval". En términos generales, eval acepta como entrada el texto de un programa y un texto cifrado, y produce como salida un texto cifrado [5, 6].

Un esquema de encriptación verdaderamente homomórfico tiene la habilidad de correr cualquier función de cálculo en los datos encriptados. No hay pérdida de funcionalidad en preservar la privacidad del corredor de programa. El uso principal de esto es mantener la privacidad mientras se realizan grandes cálculos en la nube, por ejemplo, una consulta de búsqueda, pero también aplica para grandes sitios web como Reddit, que operan exclusivamente en Servicios Web de Amazon. Una simple aplicación del esquema de encriptación homomórfica total es la evaluación de la media y varianza de un conjunto de datos [5]. Hay muchos algoritmos diferencialmente privados conocidos, y son más fuertes de lo que uno puede imaginarse a primera vista. Uno puede correr bosques de árboles de decisión al azar, análisis de red de seguimiento, análisis de consultas-clic, ciertas formas de agrupamiento, y toda una serie de problemas de optimización combinatoria. Por lo que realizar un análisis entre estas dos perspectivas de protección de la privacidad, resulta muy conveniente ya que nos permitiría definir un modelo.

**Productos acádemicos comprometidos:** Estancia de dos meses en la Universidad Autónoma de Baja California, con el objetivo de realizar el análisis comparativo entre los dos procesos para proteger la privacidad implementados. *Responsable durante la estancia*: Dra. María de los Ángeles Cosío León, FIAD UABC Ensenada.

**Conferencia del estudiante:**
Un paper para congreso Congreso Nacional de Ingeniería Biomédica (http://cnib.somib.org.mx/)

**Referencias**


[1] C. Task (2012, March 29th, 2016). *A Practical Beginners' Guide to Differential Privacy*. Available: http://www.cerias.purdue.edu/news_and_events/events/security_seminar/details/flash/j9cvs3as2h1qds1jrdqfdc3hu8

[2] C. Dwork "A firm foundation for private data analysis.," *Commun. ACM* vol. 54, pp. 1-8, 2011.

[3 ] Ji, Z., Lipton, Z. C., Elkan, C., 2014b. Differential privacy and machine learning: a survey and review. arXiv preprint arXiv:1412.7584

[4] HIPAA. The HIPAA Privacy Rule. Available: http://www.hhs.gov/hipaa/for-professionals/privacy/

[5] Gentry, Craig. *A fully homomorphic encryption scheme*. Diss. Stanford University, 2009.

[6] Waziri, Victor Onomza, et al. "Big data analytics and data security in the cloud via fully homomorphic encryption." *International Journal of Computer, Control, Quantum and Information Engineering* 9.3 (2015).