Cuerpo Académico / Individual	Individual
Nombre del Proyecto de Investigación / Vinculación / PLADEA-FEI / No registrado	No registrado
LGAC que alimenta	
Línea de Investigación	
Duración aproximada	12 meses
Modalidad de Trabajo Recepcional	Monografía
Nombre del Trabajo Recepcional	Estado del arte de Adversarial Machine Learning
Requisitos	Seguridad Pruebas de penetración Desarrollo de Sistemas Web
Responsables del Trabajo Recepcional	
Director	Dr. Héctor Xavier Limón Riaño
Codirector	
Alumnos participantes	Uno

Descripción del Proyecto de Investigación

La seguridad en servicios de red es un tema de suma importancia cuyo impacto se ve reflejado en la reciente currícula de la ACM sobre ciberseguridad, destacándose la necesidad de formar a los nuevos profesionistas de esta área, puesto cuya demanda se encuentra y encontrará en creciente aumento en los próximos años.

Desde un punto de vista académico, debe buscarse la investigación y generación de conocimientos referentes a temas de impacto social actual como es el caso de ciberseguridad en todos los aspectos que conlleva, haciendo especial incapié en nuevos desarrollos y tendencias, para mantenerse al ritmo del avance de esta área en
creciente y constante expansión.

Descripción del Trabajo Recepcional

En la actualidad la integración de métodos de aprendizaje máquina para robustecer la seguridad de sistemas informáticos se ha vuelto una práctica común, desde aquellos métodos que detectan posibles ataques de denegación de servicio, hasta aquellos que detectan patrones de comportamiento anómalos por parte de usuarios. Sin embargo, a la par de estos nuevos desarrollos, también han surgido técnicas para burlar métodos de aprendizaje máquina, a este conjunto de técnicas se le denomina "Adversarial Machine Learning".

En este trabajo de investigación se plantea realizar una revisión sistemática de la literatura, donde se cubran los siguientes aspectos referentes a Adversarial Machine Learning

- Contextos donde es aplicado
- Técnicas existentes
- Mitigaciones y mejores prácticas
- Retos abiertos

Resultados esperados

Reporte monográfico con los hallazgos de la investigación
Artículo publicado en congreso o revista afín al área de seguridad informática

Bibliografía recomendada

Duddu, V. (2018). A survey of adversarial machine learning in cyber warfare. *Defence Science Journal*, *68*(4), 356.

Wang, X., Li, J., Kuang, X., Tan, Y. A., & Li, J. (2019). The security of machine learning in an adversarial setting: A survey. *Journal of Parallel and Distributed Computing*, *130*, 12-23.

Xalapa, Ver., a fecha

Nombre y firma del director del trabajo

Vo. Bo.

Nombre y firma del co-director del trabajo

Vo. Bo.

Nombre y firma del Responsable del CA si aplica, en otro caso nombre y firma del Director de la Facultad

Nombre y firma del Coordinador de Academia Servicio Social y Practicas de Redes