Descripción del anteproyecto **Facultad de Estadística e Informática**	**Junio 2023**

Xalapa, Veracruz, a 28 junio de 2023.

PROYECTO DE TITULACIÓN PARA REGISTRO.

Cuerpo Académico	**Ingeniería y Tecnología de Software**
Nombre del proyecto de Investigación VINCULACIÓN/PLADEA-FEI	
LGAC que alimenta	**LGAC 1. Gestión, modelado y desarrollo de Software**
Línea de Investigación	
Duración Aproximada	**12 meses**
Modalidad de Trabajo Recepcional	**Monografía**
Nombre del Trabajo Recepcional	**Prácticas y herramientas criptográficas orientadas al desarrollo seguro de software**
Requisitos	**Desarrollo de Sistemas en Red, Desarrollo de Sistemas Web, Programación segura**
RESPONSABLE DEL TRABAJO RECEPCIONAL.	
Director	**Dr. Héctor Xavier Limón Riaño**
Codirector	**MCC Juan Carlos Pérez Arriaga**
Alumnos Participantes	**1**
DESCRIPCIÓN DEL PROYECTO DE INVESTIGACIÓN	
DESCRIPCIÓN DEL TRABAJO RECEPCIONAL.	
La seguridad se ha posicionado en la actualidad como uno de los atributos de calidad más importantes debido a las crecientes amenazas que los sistemas expuestos en Internet sufren. Gran parte de las vulnerabilidades que existen en los sistemas son introducidos por desarrolladores de software, en ocasiones derivadas de su desconocimiento en temas de desarrollo seguro y falta de pruebas orientadas a la seguridad. Por otra parte, la criptografía es uno de los pilares principales de la seguridad en los sistemas	

modernos, reforzando propiedades de seguridad fundamentales como son la confidencialidad, integridad y autenticación, para datos tanto en tránsito como en reposo. Dada su relevancia y uso extensivo, es común encontrarse con sistemas que requieran aspectos criptográficos para reforzar la seguridad, sin embargo, la implementación de aspectos criptográficos seguros a menudo requiere de conocimientos, prácticas y herramientas específicas, esto debido aque muchos algoritmos criptográficos, aun siendo considerados seguros, son propensos a debilitarse si no se configuran o usan correctamente, originando vulnerabilidades en los sistemas.

En este trabajo se plantea realizar una investigación monográfica que recopile los prácticas y herramientas específicas de criptografía que los desarrolladores de software pueden requerir, o en los que se pueden apoyar, para reforzar la seguridad de los sistemas que desarrollan.

RESULTADOS ESPERADOS.

- Monografía
- Publicación de artículo de los resultados de la investigación

BIBLIOGRAFÍA RECOMENDADA.

Braga, A., Dahab, R., Antunes, N., Laranjeiro, N., & Vieira, M. (2019). Understanding how to use static analysis tools for detecting cryptography misuse in software. *IEEE Transactions on Reliability*, *68*(4), 1384-1403.

Hazhirpasand, M., & Ghafari, M. (2021, November). Crypto Experts Advise What They Adopt. In *2021 36th IEEE/ACM International Conference on Automated Software Engineering Workshops (ASEW)* (pp. 179-184). IEEE.

Braga, A., Dahab, R., Antunes, N., Laranjeiro, N., & Vieira, M. (2017, October). Practical evaluation of static analysis tools for cryptography: Benchmarking method and case study. In *2017 IEEE 28th International Symposium on Software Reliability Engineering (ISSRE)* (pp. 170-181). IEEE.

Dr. Héctor Xavier Limón Riaño **Nombre y Firma del Director del Trabajo**	**MCC. Juan Carlos Pérez Arriaga** **Nombre y Firma del Codirector del Trabajo**
Vo. Bo. **Dr. Ángel Juan Sánchez García** **Responsable del CA-ITS**	**Vo. Bo.** **Dr. Jorge Octavio Ocharán Hernández** **Coordinación de Academia de Experiencia Recepcional**

NOTAS:

1) Casos excepcionales serán evaluados por la Academia de ER.
2) Tratando de un CA externo a la Licenciatura en Ingeniería de Software, el proyecto deberá llevar el aval de los CA de la misma que se asocie con el tema.

3) El Vo. Bo. del Responsable de CA se obtiene en la reunión de cada CA, donde se presentan los temas del mismo para su aprobación.
4) El Vo. Bo. de la Coordinación de ER se obtiene en una reunión de la academia que se programa para ello.