



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	Límites y retos de la criptografía moderna ante el cómputo cuántico
Requisitos	Seguridad Criptografía
Responsables del Trabajo Recepcional	
Director	Dr. Héctor Xavier Limón Riaño
Codirector	Dr. Ángel Juan Sánchez García
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 los métodos criptográficos juegan un papel central en la confidencialidad e integridad de los datos de la gran mayoría de los servicios y aplicaciones en red, así como de los propios sistemas operativos. Con la llegada de las primeras computadoras basadas en cómputo cuántico, que si bien aun no han alcanzado su máximo potencial ni llegado de forma práctica al mercado, se comienza a tomar seriamente el problema de sobrepasar la seguridad de los métodos criptográficos modernos, dando pie a lo que algunos autores denominan como “apocalipsis cuántico”. En este trabajo de investigación se plantea realizar una revisión sistemática de la literatura, donde se cubran los siguientes aspectos referentes a las implicaciones del cómputo cuántico en el contexto de criptografía: ⑩ Métodos y tecnologías criptográficas que se verán afectadas ⑩ Impacto social ⑩ Impacto de seguridad en los sistemas modernos ⑩ Propuestas de mitigación y nuevos métodos criptográficos ⑩ Áreas de oportunidad y retos abiertos	
Resultados esperados	
Trabajo escrito con investigación que de fundamento a la revisión sistemática realizada.	



Bibliografía recomendada

Bennett, C. H., Brassard, G., & Ekert, A. K. (1992). Quantum cryptography. *Scientific American*, 267(4), 50-57.
Furrer, F. J. Roger A. Grimes. Cryptography Apocalypse: Preparing for the Day When Quantum Computing Breaks Today's Crypto. *Informatik Spektrum*, 1-3.
Bernstein, D. J. (2009). Introduction to post-quantum cryptography. In *Post-quantum cryptography* (pp. 1-14). Springer, Berlin, Heidelberg.

Xalapa, Ver., a fecha

Nombre y firma del director del trabajo

Nombre y firma del co-director del trabajo

Vo. Bo.

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