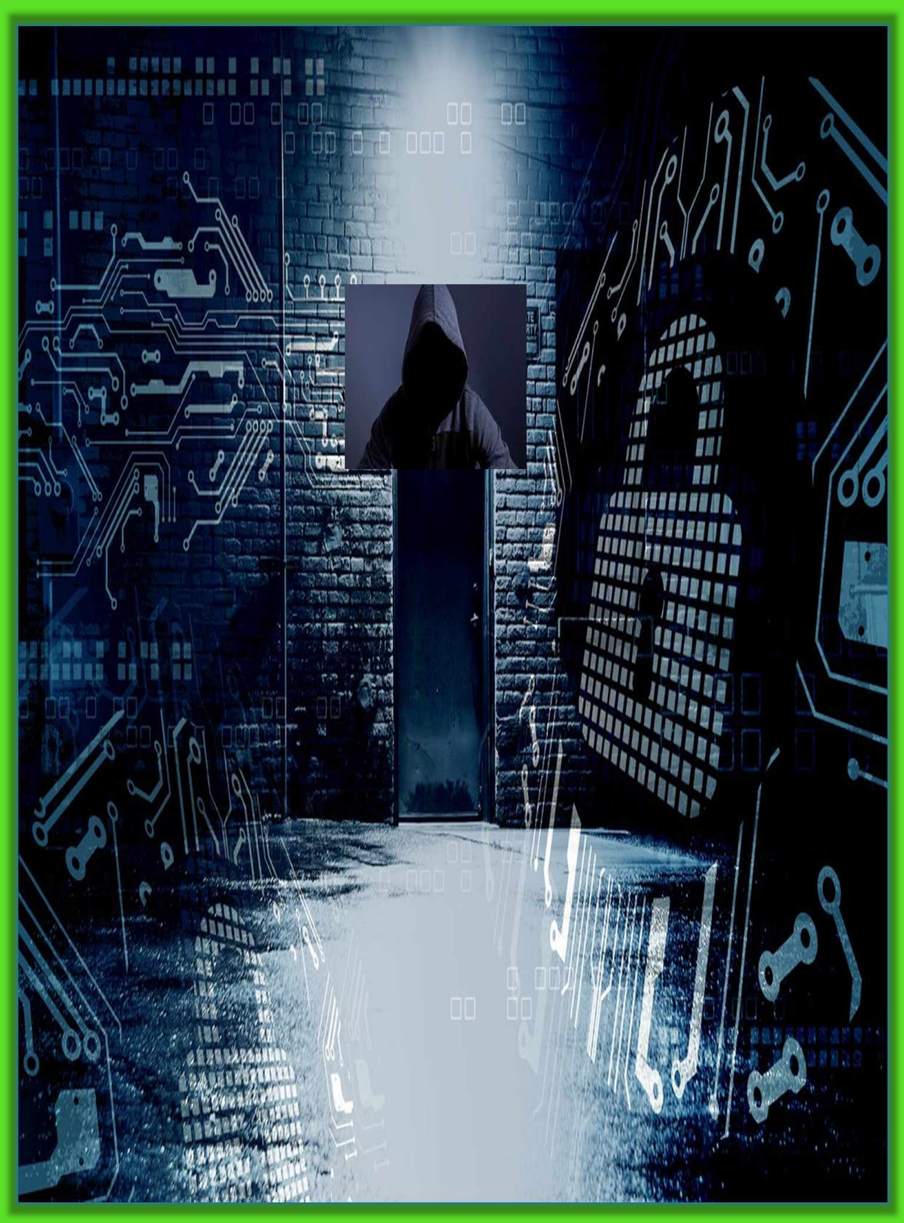
Criptología Maliciosa para la Ciberdefensa

[1]Laboratorio de Informática, Software Seguro y Criptografía.
Facultad de Ingeniería del Ejército (FIE), Universidad de la Defensa Nacional (UNDEF)
[2] Departamento de Ciencia y Tecnología, Universidad Nacional de Quilmes (UNQ)

Contexto

"Criptología Maliciosa para la Ciberdefensa" (CRIPTO-MC) es un *Proyecto de Desarrollo Tecnológico y Social* (PDTS) aprobado por la Disposición Decanal Nro 667/2022, perteneciente a la *Facultad de Ingeniería del Ejército (FIE) "Gral. Div. Manuel N. Savio"*, perteneciente a la *Universidad de la Defensa Nacional* (UNDEF).

Se encuentra enmarcado en el contexto de la carrera de grado de Ingeniería en Informática, la Especialización en Criptografía y Seguridad Teleinformática y la Maestría en Ciberdefensa, que se dictan en la citada unidad académica.



Formación RRHH

Se espera que los resultados previstos puedan enriquecer el capital de conocimiento y recursos humanos del espacio académico civil y militar de la Facultad de Ingeniería del Ejército, de la Universidad de la Defensa Nacional y de las Fuerzas Armadas en general.. Asimismo, se procura la difusión de estas temáticas en el ámbito de la Ciberdefensa Nacional, permitiendo dar a conocer nuestra maestría y logrando promocionar la misma.
Evitar un ciberataque que vulnere las capacidades de defensa, afecte la confidencialidad de la información y hasta impedir la afectación de una infraestructura crítica, en defensa de las vidas humanas involucradas

Resultados Obtenidos/Esperados

En línea con el trabajo realizado al momento, plasmado en las publicaciones del grupo de investigación en el XXIII Workshop de Investigadores en Ciencias de la Computación (WICC 2021) y en el XXVIII Congreso Argentino de Ciencias de la Computación (CACIC 2022), el proyecto tiene por finalidad la continuidad del estudio, análisis y aplicación de paradigmas y herramientas criptológicas modernas para el análisis y la creación de software malicioso y puertas traseras, como así también indagar técnicas de prevención, detección y protección para ser consideradas en el ámbito de la Ciberdefensa Nacional. Se planea la continuación del desarrollo de diferentes esquemas anti-kleptográficos para la experimentación y evaluación de su factibidad y eficacia. En particular, se intentará abordar el estudio de otras funcionalidades criptográficas como por ejemplo: generación de números aleatorios, funciones de hashing, y algoritmos de cifrado y firma asimétrico. Aunque comúnmente se entiende a la criptografía y a sus aplicaciones como herramientas de carácter defensivo, también pueden emplearse para usos ofensivos y maliciosos. En síntesis, los ataques basados en puertas traseras o *backdoors* pueden vulnerar la confidencialidad, integridad y disponibilidad de la información menoscabando la ciberdefensa de una nación.

Marcelo Cipriano[1 2], Edith García[1], Ariel Maiorano[1], Eduardo Malvacio[1],