Disposición Decanal FMC N° 64/2026

C.A. de Buenos Aires, **31** de agosto de 2026

VISTO la Disposición Decanal FMC N° 45/2025, la renuncia de la Mg. Adriana BARAVALLE (DNI: 21.382.808) a la dirección del Proyecto de Investigación "Escudo cuántico: Arquitecturas híbridas de IA y Criptografía Post-Cuántica para la protección resiliente de infraestructuras críticas de información", la propuesta de reemplazo presentada por el Secretario de Investigación; y

CONSIDERANDO:

Que el desarrollo del proyecto "Escudo cuántico: Arquitecturas híbridas de IA y Criptografía Post-Cuántica para la protección resiliente de infraestructuras críticas de información", fue aprobado por DD FMC N° 45/2025.

Que los integrantes del equipo de trabajo inicial con asignación de horas eran: la Mg. Adriana BARAVALLE (Directora) y el Mg. Eduardo FOGLIATO (Asistente).

Que la Mg. Adriana BARAVALLE presenta su renuncia con fecha 13 de agosto de 2026, por su designación en cargo de mayor jerarquía en el orden nacional. (Secretaria de Innovación, Ciencia y Tecnología de la JEFATURA DE GABINETE DE MINISTROS).

Que el Secretario de Investigación propone en su reemplazo al Mg. Eduardo FOGLIATO, quién formaba parte del equipo.

Que la Asesoría Legal ha tomado la intervención de su competencia.

Disposición Decanal FMC N° 64/2026

Que la presente Disposición responde a las atribuciones conferidas por el Artículo 53 del Estatuto Universitario de la Universidad de la Defensa Nacional (UNDEF),

Por ello,

EL DECANO DE LA FACULTAD MILITAR CONJUNTA

DISPONE:

ARTÍCULO 1ro.– Apruébese el nuevo equipo del Proyecto de Investigación "Escudo cuántico: Arquitecturas híbridas de IA y Criptografía Post-Cuántica para la protección resiliente de infraestructuras críticas de información", conforme al ANEXO adjunto a la presente Disposición.

ARTÍCULO 2do.– Regístrese, comuníquese y remítase copia al Rector (UNDEF), al Vicerrector de Educación Militar Conjunta (EMCO), a los Directores de las SEU ESGC, SEU IIFA y SEU ICFA, y a los Secretarios de Investigación y Académico (FMC).

ARTÍCULO 3ro.– Archívese el original en la Secretaría General de la Facultad Militar Conjunta.

CR (R) VGM ALBERTO VICTORIO APARICIO
DECANO
FACULTAD MILITAR CONJUNTA

Disposición Decanal FMC N° 64/2026

Disposición Decanal FMC N° 64/2026

ANEXO

FORMULARIO PARA LA PRESENTACIÓN DE PROYECTOS DE INVESTIGACIÓN

1. IDENTIFICACIÓN DEL PROYECTO

a. **Título:**
"Escudo cuántico: Arquitecturas híbridas de IA y Criptografía Post-Cuántica para la protección resiliente de infraestructuras críticas de información"

b. Tipo de actividad:
(Investigación básica, aplicada, exploratoria, desarrollo técnico, otra):
Investigación aplicada.

c. Campo o área temática/disciplinar en la que se encuadra el proyecto:

Ciberdefensa.

d. Área de conocimiento en la que se enmarcará el proyecto: *(RR UNDEF N° 307/23 Art.4):*

Ciberdefensa y Operaciones Militares Cibernéticas.

e. Fundamentación o justificación del proyecto:*(RR UNDEF N° 307/23 Art.3)*

El objetivo general de este trabajo es investigar y desarrollar un enfoque integral para la optimización de la arquitectura y gestión de riesgos en sistemas avanzados de ciberseguridad. Se busca aprovechar las sinergias entre la inteligencia artificial y la criptografía post-cuántica para fortalecer la seguridad de la información crítica en el contexto de la computación cuántica.
La investigación propuesta es relevante por múltiples factores críticos interconectados.
El avance de la computación cuántica ya no es teórico sino inminente. Los avances de Google, IBM y otros actores en demostrar la "supremacía cuántica" representan un punto de inflexión para la seguridad informática global. Los algoritmos de Shor y Grover tienen el potencial de comprometer nuestros sistemas criptográficos actuales en un horizonte temporal de menos de una década, creando una vulnerabilidad sistémica sin precedentes. Estudios prospectivos de hace 5 años esperaban que el grado de madurez de esta tecnología se alcance a partir de 2030, avances actuales hacen prever que se concrete en 2027.
Las infraestructuras críticas vitales para nuestra sociedad (redes energéticas, sistemas sanitarios, infraestructura financiera y plataformas de defensa nacional)

dependen actualmente de protocolos criptográficos que se volverán obsoletos ante computadoras cuánticas funcionales. Esta vulnerabilidad constituye un riesgo socioeconómico para el cual debemos prepararnos.
En mi trayectoria profesional he observado que nos encontramos en una ventana temporal crítica. La transición hacia sistemas post-cuánticos no es instantánea y requiere años de investigación, desarrollo e implementación coordinada. Ya estamos presenciando estrategias de "Harvestnow, Decryptlater", donde actores maliciosos almacenan datos cifrados actuales con la intención de descifrarlos cuando dispongan de capacidades cuánticas operativas.
Se identifica un déficit significativo en la integración sinérgica entre la inteligencia artificial y los métodos criptográficos post-cuánticos. Si bien ambos campos avanzan separadamente, existe una escasez notable de investigación sobre cómo pueden complementarse para crear sistemas de defensa adaptativos y resilientes.
La complejidad arquitectónica para implementar soluciones post-cuánticas presenta desafíos sustanciales de rendimiento, interoperabilidad y gestión que mis años de trabajo en el sector me han permitido comprender en profundidad. Estos retos demandan nuevos paradigmas arquitectónicos optimizados que este proyecto de investigación busca desarrollar.
Nos encontramos en un momento formativo para los estándares y normativas post-cuánticas. Las iniciativas del NIST están evolucionando, lo que crea una oportunidad única para que esta investigación contribuya significativamente a la formación de estos marcos conceptuales y prácticos que definirán la ciberseguridad de la próxima década.
Este proyecto aborda esta intersección crítica de desafíos, con el objetivo de desarrollar soluciones arquitectónicas y metodologías de gestión de riesgos que sean técnicamente viables, económicamente sostenibles y adaptables al panorama evolutivo de las amenazas cuánticas y las capacidades de la IA en el ámbito de la ciberdefensa.

f. Carrera con la que se vincula:

Maestría en Estrategia Militar

g. Unidad ejecutora:
Facultad Militar Conjunta

h. Director/a del proyecto: (*acompañar CVar actualizado*):

Nombre y apellido	Eduardo FOGLIATO				
CUIL	20-14892287-3				
Dirección	Puerto Rico			Nro.	2148
Localidad	Martínez	CP	1640	Provincia	Bs. As.

Tel	11-6365-1619	E-MAIL	Fliafog1@hotmail.com

2. DURACIÓN DEL PROYECTO

a. Fecha de inicio: 01-06-2025
b. Fecha de finalización: Fase I: 30-06-2027
c. Duración prevista en meses: 24 meses

3. PRESENTACIÓN DEL PROYECTO

a. Resumen sobre el propósito del proyecto:

En el Congreso del Consorcio de Clave Pública de 2023, se destacó la importancia de integrar la criptografía post-cuántica (PQC) y la inteligencia artificial (IA) para fortalecer los sistemas criptográficos frente a la amenaza de la computación cuántica. Esta sinergia promete mejorar la detección de amenazas, la identificación de anomalías, la adaptación dinámica de algoritmos y la optimización de la rotación de claves.

El algoritmo de Shor, un pilar de la computación cuántica representa un riesgo significativo para los sistemas criptográficos actuales, poniendo en peligro datos sensibles en sectores como finanzas, salud y gobierno. La transición a soluciones PQC con capacidades predictivas impulsadas por IA se vuelve urgente para fortalecer las defensas cibernéticas.

El aprendizaje automático (ML) mejora significativamente la detección de amenazas y anomalías, analizando grandes volúmenes de datos en tiempo real, optimizando la selección e intercambio de algoritmos criptográficos permitiendo mejorar la rotación de claves y, fortaleciendo la seguridad contra ataques de fuerza bruta.

Sin embargo, el reciente quiebre del mecanismo CRYSTALS-Kyber mediante el uso de Inteligencia Artificial y ataques de canal lateral subraya la necesidad de seguir investigando alternativas donde la IA se use para proteger contra ataques diseñados con la misma tecnología.

Esta investigación busca desarrollar un marco arquitectónico integrado que resuelva las vulnerabilidades expuestas por el reciente compromiso del mecanismo CRYSTALS-Kyber mediante ataques de canal lateral asistidos por IA. Nuestro objetivo es crear un sistema adaptativo de defensa que utilice la IA no solo como herramienta de detección, sino como componente activo en la generación de contramedidas frente a ataques cuánticos.

La convergencia de la computación cuántica, la IA y la PQC promete un cambio de paradigma en la seguridad digital, requiriendo una infraestructura de software

robusta para soportar estos sistemas avanzados de ciberseguridad y allanar el camino hacia un ecosistema cibernético más seguro.

Nuestra propuesta incluye el análisis y diseño de una arquitectura multicapa que combine: (1) algoritmos PQC resistentes a ataques de canal lateral, (2) sistemas de detección de anomalías basados en aprendizaje profundo que identifiquen patrones de exfiltración cuántica, y (3) mecanismos auto adaptativos que modifiquen dinámicamente los parámetros criptográficos según el nivel de amenaza detectado.

La investigación abordará específicamente el problema de optimización computacional en dispositivos con recursos limitados, la interoperabilidad con infraestructuras criptográficas existentes, y el desarrollo de métricas estandarizadas para evaluar la resistencia de sistemas híbridos IA-PQC. Esperando arribar como resultado final al diseño de un marco implementable en infraestructuras críticas que proporcione resistencia cuántica verificable mientras mantiene niveles de rendimiento aceptables en entornos de producción.

b. Estado actual del conocimiento sobre el tema:

La convergencia entre Inteligencia Artificial y criptografía post-cuántica es un área de investigación emergente, y representa actualmente uno de los frentes más dinámicos en la evaluación de sistemas avanzados de ciberseguridad. Ha experimentado una aceleración significativa desde que el NIST completó en 2023 su primera fase de estandarización, seleccionando CRYSTALS-Dilithium para firmas digitales (NIST, 2023). Sin embargo, la identificación posterior de vulnerabilidades de canal lateral en Kyber mediante técnicas de IA ha catalizado una segunda fase de evaluación que continúa actualmente (Wang et al., 2024).

Las arquitecturas híbridas surgen como solución práctica, investigadores de Micorsoft Research y ETH Zürich han desarrollado esquemas que integran algoritmos clásicos con post-cuánticos que proporcionan una estrategia de seguridad en capas y mitigan las penalizaciones de rendimiento (Bernstein & Lange, 2023). Por otro lado, fabricantes con Intel, IBM y Qualcomm han introducido aceleradores de hardware que reducen la sobrecarga computacional asociada con primitivas post-cuánticas (Intel Labs, 2024).

El esfuerzo en el desarrollo de algoritmos y protocolos resistentes a los ataques cuánticos, incluyen la exploración de esquemas de cifrado basados en retículas, códigos de corrección de errores y funciones hash resistentes a este tipo de ataques. Por su parte, la Inteligencia Artificial no sólo se aplica como herramienta de análisis, sino que se ha convertido en componente estructural de los sistemas defensivos avanzados. Modelos de Aprendizaje Profundo como los desarrollados por Zhang y colaboradores han demostrado mejorar la capacidad de detección de ataques de canal lateral con una precisión superior al 97%, basados en el análisis de patrones sutiles ene el consumo energético durante operaciones criptográficas (Wang et al., 2024). La Universidad de Stanford se encuentra trabajando en frameworks

autoadaptativos que ajustan dinámicamente parámetros criptográficos según la amenaza detectada.

En relación con la gestión de riesgos se ha incorporado el paradigma "Zero-Trust Cuántico", extendiendo los principios clásicos mediante validaciones criptográficas post-cuánticas en cada punto de la infraestructura.

Como respuesta ante la amenaza "HarvestNow, DecryptLater", donde actores maliciosos almacenan datos cifrados actualmente para su desencriptación futura mediante computadores cuánticos, el consorcio Quantum-Ready ha propuesto arquitecturas con rotación predictiva de claves y fragmentación estratégica de datos sensibles.

La interacción de estas tecnologías está fomentando la colaboración entre investigadores de diferentes disciplinas, incluyendo matemáticos, informáticos, físicos y expertos en ciberseguridad. Se encuentran trabajos relevantes sobre la integración de ambas tecnologías para la protección de sistemas de información crítica haciendo búsquedas en bases de datos académicas como IEEE Xplore, ACM Digital Library y Google Scholarcentradas en términos clave como "post-quantumcryptography", "quantum artificial intelligence", "cybersecurityarchitecture", "riskmanagement", y combinaciones de estos términos.

Los desafíos actuales se centran en tres áreas principales: la eficiencia computacional en dispositivos con recursos limitados, la interoperabilidad durante la migración de infraestructuras críticas, y la validación rigurosa de implementaciones.

Particularmente prometedor resulta el avance en computación homomórfica post-cuántica, que permite procesar datos cifrados sin descifrarlos, manteniendo seguridad incluso ante atacantes con capacidades cuánticas. Esta tecnología podría revolucionar el procesamiento seguro en entornos compartidos y nubes públicas.

El ritmo acelerado de innovación en este campo refleja su criticidad estratégica, las organizaciones que implementen proactivamente estos avances no solo mitigarán riesgos emergentes, sino que establecerán ventajas competitivas significativas en un entorno digital cada vez más complejo y amenazado por capacidades computacionales sin precedentes.

c. Marco teórico (opcional para desarrollo técnico):

Esta investigación tiene como bases conceptuales un marco teórico multidisciplinario que proporciona los fundamentos para desarrollar sistemas resistentes a amenazas cuánticas integrando las capacidades de la IA y PQC.

La criptografía post-cuántica (PQC) como paradigma emergente diseñado para resistir ataques de computadoras cuánticas. A diferencia de los sistemas criptográficos clásicos basados en factorización de números primos (RSA) o logaritmos discretos (ECC), que son vulnerables al algoritmo de Shor (1994), la PQC se fundamenta en problemas matemáticos considerados difíciles incluso para computadoras cuánticas (Bernstein & Lange, 2023). Entre estos destacan los

sistemas basados en retículas, códigos y funciones hash multivariables, cada uno con distintas características de seguridad, eficiencia y tamaño de claves.

La inteligencia artificial se aplicada en ciberseguridad avanzada para la detección, adaptación y predicción. En el nivel de detección, los modelos de aprendizaje profundo analizan patrones en tráfico de red, uso de sistema y comportamiento de aplicaciones para identificar anomalías que escapan a métodos estadísticos tradicionales. El nivel adaptativo comprende sistemas que modifican dinámicamente parámetros de seguridad basados en la inferencia de niveles de amenaza, optimizando el equilibrio entre seguridad y rendimiento. Finalmente, el nivel predictivo utiliza modelos generativos para anticipar variantes de ataques antes de su manifestación en entornos reales. (https://postquantum.com/post-quantum/pqc-quantum-ai-qai/).

El concepto de arquitecturas híbridas representa un constructo esencial dentro de este marco, integrando estratégicamente algoritmos clásicos y post-cuánticos durante el período de transición (https://repositorio.ufsc.br/handle/123456789/251847). Estas arquitecturas implementan el principio de defensa en profundidad mediante capas redundantes pero diferenciadas de protección criptográfica, mitigando riesgos asociados a vulnerabilidades desconocidas en nuevos algoritmos.

El marco de optimización arquitectónica se sustenta en la teoría de compensación (trade-off) entre múltiples variables: resistencia cuántica, eficiencia computacional, interoperabilidad con sistemas legados y escalabilidad. Los aceleradores hardware específicos (Intel Labs, 2024) representan una manifestación tecnológica de este equilibrio teórico, permitiendo implementaciones eficientes de algoritmos computacionalmente intensivos.

d. Objetivos general y específicos contribuyentes:

- Analizar el estado del arte de la criptografía post-cuántica (PQC) y la inteligencia artificial (IA) en el ámbito de la ciberseguridad, centrada en sus aplicaciones, desafíos y sinergias potenciales integrándola con las capacidades predictivas y adaptativas impulsadas por IA.
- Investigar las amenazas emergentes asociadas con la computación cuántica, especialmente el algoritmo de Shor, y evaluar su impacto en la seguridad de los sistemas criptográficos actuales.
- Identificar y probar algoritmos y técnicas de inteligencia artificial para la detección de anomalías en sistemas de ciberseguridad avanzados.
- Diseñar una arquitectura de alto nivel sobre una infraestructura de software robusto y escalable capaz de soportar sistemas avanzados de ciberseguridad que aprovechen las capacidades de la inteligencia artificial cuántica y la criptografía post-cuántica.

- Evaluar experimentalmente el rendimiento y la eficacia de modelos de inteligencia artificial utilizando datos de logs de acceso a servidores para detectar patrones de comportamiento de usuarios y funcionamiento de la red.
- Contribuir al avance del conocimiento en el campo de la ciberseguridad mediante la generación de resultados significativos y la divulgación de hallazgos a través de publicaciones científicas y presentaciones en conferencias especializadas.

e. Método:

El marco metodológico previsto para el presente trabajo se basará en las técnicas cualitativas de revisión bibliográfica, descripción de casos y diseño de una metodología para la elaboración de estrategias de defensa contra amenazas cuánticas para la ciberseguridad de la interoperabilidad de sistemas de inteligencia artificial. En este sentido se emplean las herramientas de exploración de documentos como libros, artículos e informes de prensa sobre las cuestiones relevantes para el desarrollo de este trabajo. Este trabajo de investigación prevé el análisis de las tres áreas de interacción en distintas fases:

- Revisión exhaustiva de la literatura existente en materia de ciberseguridad, computación cuántica e interoperabilidad de sistemas de inteligencia artificial. Identificando claramente el teorías, metodologías y brechas de conocimiento.
- Luego se refinará la definición del problema de investigación y se formularán las preguntas específicas.
- Desarrollo del marco conceptual que integre los conceptos de los tres campos para elegir las metodologías de investigación apropiadas que pueden incluir: análisis cuantitativos, cualitativos, estudio de casos o simulaciones.
- Recolección y análisis de datos mediante técnicas de minería de datos.
- Modelado de datos utilizando algoritmos de inteligencia artificial cuántica para la detección de patrones anómalos.
- Análisis comparativo de algoritmos de encriptación post-cuánticos.
- Se analizará la implementación de prototipos o simulaciones si corresponde para evaluar la efectividad de las soluciones propuestas e interpretar los resultados.
- Propuesta de futuras líneas de investigación.

f. Resultados esperados:

Como puede observarse a priori en la revisión de publicaciones y patentes, la integración de la inteligencia artificial cuántica y la criptografía post-cuántica representa una línea de investigación de vanguardia en materia de seguridad digital. La tesis aborda esta convergencia, reconociendo su potencial para fortalecer sistemas criptográficos y mejorar la detección de amenazas y anomalías.

Reconociendo la necesidad de contar una infraestructura sólida y segura para sistemas críticos, con este trabajo de investigación se pretende aprovechar la sinergia entre la inteligencia artificial y la criptografía post-cuántica para diseñar estrategias de defensa proactiva de sistemas críticos contra actores maliciosos.

Esta convergencia de tecnologías en el contexto cuántico promete un cambio de paradigma en los protocolos de seguridad digital, contribuyendo al diseño de una arquitectura robusta para el desarrollo de este nuevo ecosistema cibernético más seguro.

Con este trabajo se pretende contribuir en la reducción de riesgos en el contexto cuántico, utilizando modelos de detección de anomalías de inteligencia artificial y proponiendo el diseño de una arquitectura segura robusta para la defensa proactiva de sistemas e información crítica mediante la recomendación de uso de algoritmos post-cuánticos.

g. Formación de recursos humanos:

Se espera incorporar al proyecto a alumnos de grado y posgrado interesados en la temática que puedan contribuir en la investigación.

h. Interdisciplinariedad y colaboraciones:

El equipo de investigación interactúa con investigadores internacionales y nacionales de otras universidades que siguen esta línea de investigación.

i.Bibliografía inicial (de acuerdo con normas APA):

- Abdullah Aydeger; Engin Zeydan; Awaneesh Kumar Yadav; Kasun T. Hemachandra; Madhusanka Liyanage.Towards a Quantum-Resilient Future: StrategiesforTransitioningto Post-Quantum Cryptography. IEEE. https://ieeexplore.ieee.org/document/10741441
- Bernstein, D. J., & Lange, T. (2023). Hybridpost-quantumcryptosystems. JournalofCryptographicEngineering, 13(2), 56-73. https://doi.org/10.1007/s13389-022-00305-x
- J. Wang, W. Cao, H. Chen and H. Li, "Blink: Breaking Parallel Implementation of Crystals-Kyber with Side-Channel Attack," 2024 IEEE 42nd International Conference on Computer Design (ICCD), Milan, Italy, 2024, pp. 105-113, doi: 10.1109/ICCD63220.2024.00026.
- European Telecommunications Standards Institute [ETSI]. (2024). Quantum Safe Cryptography and Security. https://www.etsi.org/technologies/quantum-safe-cryptography
- Gentry, C., &Boneh, D. (2023). Advances in quantum-resistantfullyhomomorphicencryption. Advances in Cryptology – CRYPTO 2023, 12954, 311-335. https://doi.org/10.1007/978-3-031-38548-3_11

- Intel Labs. (2024). Performance analysisoflattice-basedcryptographyonspecialized hardware. Intel TechnicalJournal, 28(1), 41-58. https://www.intel.com/content/www/us/en/research/technical-journal/2024/lattice-cryptography-hardware.html
- NationalInstituteofStandards and Technology [NIST]. (2023). Post-quantumcryptographystandardization. U.S. Departmentof Commerce. https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization
- Stanford Cyber Initiative. (2023). Adaptive cryptographic systems: Integrating AI and post-quantum primitives. Stanford Security Research Series.Cryptography | Stanford Emerging Technology Review
- Eric Yocam et. Al. (2024), Aprendizaje automático cuántico adversarial y estrategias de defensa: desafíos y oportunidades.Arxiv. https://arxiv.org/html/2412.12373v1
- Zhang, W., Smith, J., & Patel, K. (2024). Deep learningforside-channelattackdetection in post-quantumcryptographicimplementations. IEEE TransactionsonInformationForensics and Security, 19(1), 1890-1905.
- Machine Learning and Deep Learning Methods for Cybersecurity | IEEE Journals & Magazine | IEEE Xplore
- Zhuang Xu ID, Owen Pemberton ID, SujoySinha Roy ID, David Oswald ID, Wang Yao ID, and Zhiming Zheng: MagnifyingSide-ChannelLeakageofLattice-BasedCryptosystemswithChosenCiphertexts: The Case StudyofKyber. 2021. https://ieeexplore.ieee.org/document/9591340/

4. CRONOGRAMA DE ACTIVIDADES

(Hoja de ruta detallando las tareas principales y su duración en meses)

TAREAS		MESES DE TRABAJO											
		1	2	3	4	5	6	7	8	9	10	11	12
A	**1.** Inicio de las actividades y organización del trabajo (previsto).					**X**							
B	Presentación de estado de avance.							**X**			**X**		
C	Presentación del informe final. (previsto)												**X**

5. INTEGRANTES DEL EQUIPO DE TRABAJO (acompañar CVar actualizado)

Nombre y Apellido	Docente / Investigador (cargo, área de trabajo, facultad)	Función	Categorización (UNDEF, Conicet, otras - especificar)	Dedicación (horas semanales)
Mg. Fogliato, Eduardo	Investigador, Maestría en Ciberdefensa y Ciberseguridad, FCE UBA	Director	-	3
Mg. Baravalle, Adriana	Investigador, Docente Maestría en Estrategia Militar – ESGC - UNDEF	Asistente	Clase LI Grupo C – RPIDFA CONVOCATORIA 2024 (en evaluación)	"Ad Honorem"
Giorgio, Juan	Ingeniería Informática, Facultad de Ingeniería, Universidad Austral	Estudiante	-	--

(Los estudiantes que participen como colaboradores, no reciben asignación horaria remunerada).

6. FUENTES DE FINANCIAMIENTO DEL PROYECTO

(Especificar si cuenta con financiamiento propio, institucional, externo, becas o subsidios)

FMC

Director/a del proyecto: Mg. Eduardo FOGLIATO

(solo aclarar nombre y apellido/s completos)

CR (R) VGM Alberto Victorio APARICIO
DECANO
FACULTAD MILITAR CONJUNTA