Fecha del CVA	02/12/2023

Parte A. DATOS PERSONALES

Nombre	Luis		
Apellidos	Hernández Encinas		
Sexo	Hombre	Fecha de Nacimiento	02/10/1957
DNI/NIE/Pasaporte	08950984M		
URL Web	http://www.itefi.csic.es/es/personal/hernandez-encinas-luis		
Dirección Email	luis.h.encinas@csic.es		
Open Researcher and Contributor ID (ORCID)	0000-0001-6980-2683		

A.1. Situación profesional actual

Puesto	Profesor de Investigación de OPI		
Fecha inicio	2023		
Organismo / Institución	Consejo Superior de Investigaciones Científicas		
Departamento / Centro	Tecnologías de la Información y Comunicaciones / Instituto de Tecnologías y de la Información (ITEFI)		
País		Teléfono	
Palabras clave	Criptografía		

A.3. Formación académica

Grado/Master/Tesis	Universidad / País	Año
Doctor en Ciencias Matemáticas	Universidad de Salamanca / España	1992

Parte B. RESUMEN DEL CV

La mayor parte de mis últimos artículos científicos han sido publicados en revistas indexadas (Journal Citation Report —JCR— y SCImago Journal & Country Rank —SJR—), muchas de ellas situadas en los primeros cuartiles de las áreas de: Matemáticas (Aplicadas y Aplicaciones interdisciplinares) y Ciencias de la Computación (Sistemas de información, Teoría y métodos). Además, he publicado 14 libros y editado otros 8, he sido editor asociado de la revista Information Sciences (Q1 del JCR), miembro del editorial board de otras revistas y recensor de varias revistas de reconocido prestigio. Tengo numerosas publicaciones en las actas de congresos internacionales y nacionales. La Comisión Nacional Evaluadora de la Actividad Investigadora (CNEAI) me ha evaluado positivamente cinco Tramos de Actividad Investigadora (sexenios: 1993-1998, 1999-2004, 2005-2010, 2011-2016, 2017-2022) y un Tramo de Actividad Investigadora Transferencia de Conocimiento e Innovación (sexenio tecnológico: 2001/2011) y los seis Tramos de Méritos Investigadores (quinquenios: (1987-1991), 1992-1996, 1997-2001, 2002-2006, 2007-2011 y 2012-2016 y 2017-2021).

He sido galardonado con el Premio “CCN-2021 a la trayectoria profesional en favor de la Ciberseguridad”, del Centro Criptológico Nacional (CCN) del Centro Nacional de Inteligencia (CNI); Ministerio de Defensa y condecorado con la “Cruz al Mérito Policial con distintivo blanco”, del Ministerio del Interior, 2022.

Mis índices de impacto en investigación científica son: h = 17 en Scopus y en Google Scholar son h = 26 e i10 = 52, número de citas = 2.401. He participado en 10 proyectos internacionales y en 24 de plan nacional de I+D+I, siendo el investigador principal en 22 de ellos (7 internacionales). Además de otros 20 proyectos regionales.

He sido Profesor de Enseñanza Secundaria (1980-1990) y Profesor Titular de la Universidad de Salamanca (1990-2000). En el CSIC he sido Científico Titular (2000-2018), Investigador Científico (2018-2022) y actualmente Profesor de Investigación (2022-), además de haber sido el director del Instituto de Tecnologías Físicas y de la Información entre 2014 y 2022.

En transferencia de tecnología, destacan 9 patentes publicadas en colaboración con otros investigadores, 6 de las cuales están licenciadas por Telefónica Investigación y Desarrollo. Además, he sido responsable de numerosos contratos de apoyo tecnológico, tanto con empresas y organismos del sector público, como con empresas privadas. Estos contratos son una importante vía de financiación y de transferencia tecnológica de la investigación realizada. Son de destacar los sucesivos contratos técnicos, desde 2010, en materia de evaluación de la seguridad de productos criptográficos firmados con el CCN del CNI; para el análisis de vulnerabilidades en el marco de evaluaciones de seguridad Common Criteria firmado con LGAI, Epoche, Winbond, Lesikar y Samsung; así como de apoyo tecnológico a otras empresas líderes en seguridad y tecnologías de la Información como Indra, Epicom, Tecnobit, Ferrovial, Airtel y Visa.

También he firmado contratos, en concurrencia competitiva, con centros de investigación europeos, en 2014, 2015 y 2016, con la European Union Agency for Cybersecurity (ENISA) relacionados con la seguridad de datos personales, la confiabilidad en herramientas de privacidad para el público en general y la confiabilidad en herramientas de privacidad en línea.

En formación y divulgación, he sido profesor en numerosos cursos de postgrado y másteres, he impartido numerosas conferencias invitadas nacionales e internacionales, y he dirigido nueve tesis doctorales (actualmente dirijo otras tres). También soy miembro de los Comités de Programa de varios congresos nacionales e internacionales.

Soy Jefe de Seguridad del Servicio de Protección de Información Clasificada nacional del CSIC (JSSP) y Jefe de Seguridad del Servicio Central de Protección de Información Clasificada nacional del CSIC (SCPIC), nombrado por la Presidencia del CSIC (22/12/2019). Soy el representante del CSIC en varias comisiones: desde 2010 en la Comisión Mixta del Acuerdo Marco CSIC-CNI para la Investigación de vulnerabilidades Criptográficas en el ámbito de la Seguridad de las Tecnologías de la Información; desde 2014 en la Comisión Mixta del Acuerdo Marco CSIC-INCIBE (Instituto Nacional de Ciberseguridad) para llevar a cabo actividades relacionadas con la investigación científica y el desarrollo tecnológico; desde 2018 en el Comité Técnico de UNE (antes AENOR) CTN320 “Ciberseguridad y protección de datos personales”, siendo secretario del Subcomité CTN/SC2 “Criptografía y mecanismos de seguridad"; desde 2016, como socio fundador en la Red de Excelencia Nacional de Investigación en Ciberseguridad (RENIC, http://www.renic.es/es/index.html); desde 2020 como patrono de la persona jurídica CSIC en el Patronato de la Fundación Círculo de Tecnologías para la Defensa y la Seguridad.

Parte C. LISTADO DE APORTACIONES MÁS RELEVANTES

C.1. Publicaciones más importantes en libros y revistas con “peer review” y conferencias

AC: Autor de correspondencia; (nº x / nº y): posición firma solicitante / total autores. Si aplica, indique el número de citaciones

1 **Artículo científico**. Luis Hernández Álvarez; Elena Barbierato; Stefano Caputo; José María de Fuentes; Lorena González Manzano; (6/7) Luis Hernández Encinas; Lorenzo Mucchi. 2023. Key Encoder: A secure and usable EEG-based cryptographic key generation mechanism.Pattern Recognition Letters. 173, pp.1-9. https://doi.org/10.1016/j.patrec.2023.07.008

2 **Artículo científico**. Luis Hernández Álvarez; Elena Barbierato; Stefano Caputo,; Lorenzo Mucchi; (5/5) Luis Hernández Encinas (AC). 2022. EEG Authentication System Based on One- and Multi-Class Machine Learning Classifiers. Sensors. Special Issue “Feature Papers in Smart and Intelligent Sensors Systems.23 (1)-186, pp.1-19. https://doi.org/10.3390/s23010186

3 **Artículo científico**. Miguel Ángel González de la Torre; (2/3) Luis Hernández Encinas (AC); Araceli Queiruga Dios. 2022. Analysis of the FO Transformation in the Lattice-Based Post-Quantum Algorithms. Mathematics. 10-16. ISSN 2227-7390. https://doi.org/10.3390/math10162967

4 **Artículo científico**. Victor Gayoso Martínez; Luis Hernández Encinas; Agustín Martín Muñoz. 2022. A modification proposal for the reconciliation mechanism of the key exchange algorithm NewHope.Logic Journal of the IGPL.

5 **Artículo científico**. LuisHernández Álvarez; José María de Fuentes; Lorena González Manzano; Luis Hernández Encinas. 2021. SmartCAMPP - Smartphone-based Continuous Authentication leveraging Motion sensors with Privacy Preservation. Pattern Recognition Letters. Special Issue “Implicit Biometric Authentication and Monitoring through Internet of Things. Elsevier. 147, pp.189-196. https://doi.org/10.1 016/j.patrec.2021.04.013

6 **Artículo científico**. Luis Hernández Álvarez; José María de Fuentes; Lorena González Manzano; Luis Hernández Encinas. 2020. Privacy-Preserving Sensor-Based Continuous Authentication and User Profiling: A Review. Sensors. 21(1)-92, pp.1-23. https://doi.org/10.3390/s21010092

7 **Capítulo de libro**. Luis Hernández Álvarez; Lorena González Manzano; José Marí Fuentes; (4/4) Luis Hernández Encinas (AC). 2022. Biometrics and Artificial Intelligence: Attacks and Challenges. Breakthroughs in Digital Biometrics and Forensics.Springer. pp.213-240. ISBN 978-3-031-10705-4. https://doi.org/10.1007/978-3-031-10706-1_10

8 **Libro o monografía científica**. Luis Hernández Encinas. 2023. Manual Básico de Criptología.Manual Básico de Criptología. Pinolia. ISBN 9788418965883.

9 **Libro o monografía científica**. Kevin Daimi; Guillermo Francia III; Luis Hernández Encinas. 2022. Breakthroughs in Digital Biometrics and Forensics.Breakthroughs in Digital Biometrics and Forensics.Springer International Publishing. pp.213-240. ISBN 978-3-031-10705-4.

10 **Informe científico-técnico**. (1/1) Luis Hernández Encinas (AC). 2023. Guía de Mecanismos Criptográficos autorizados por el CCN. Guía de Seguridad de las TIC (CCN-STIC-221. Centro Criptológico Nacional.

11 **Informe científico-técnico**. (1/1) Luis Hernández Encinas (AC). 2022. Recomendaciones para una transición postcuántica segura. Guía/Norma (CCN-TEC 009). CCN-PYTEC del Centro Criptológico Nacional. pp.1-23.

12 **Artículo científico**. Victor Gayoso Martínez; Luis Hernández Encinas; Agustín Martín Muñoz. 2021. Using Free Mathematical Software in Engineering Classes. Axioms. MDPI. 10 (4)-253. https://doi.org/10.3390/axioms10040253

C.2. Congresos

1 Luis Hernández Álvarez; Miguel Angel González de la Torre; E. Iglesias Hernandez; Luis Hernández Encinas. How to attack a galaxy: from Star Wars to Star Trek. International Conference on Security and Management (Worldcomp-SAM’23). 2023. Estados Unidos de América. Participativo - Ponencia oral (comunicación oral). Congreso.

2 Miguel Angel González de la Torre; Luis Hernández Encinas. About the Fujisaki-Okamoto Transformation in the Code-based Algorithms of the NIST Post-Quantum Call. 14th International Conference on Computational Intelligence in Security for Information Systems (CISIS'2022). Universidad de Salamanca. 2022. España. Participativo - Ponencia oral (comunicación oral). Congreso.

3 O. Castillo Campo; Victor Gayoso Martinez; Luis Hernández Encinas; Agustín Martín Muñoz; R. Álvarez Fernández. State of the art of cybersecurity in cooperative, connected and automated mobility.. 14th International Conference on Computational Intelligence in Security for Information Systems (CISIS'2022). Universidad de Salamanca. 2022. España. Participativo - Ponencia oral (comunicación oral). Congreso.

4 J. Espinosa García; Luis Hernández Encinas; Alberto Peinado Domínguez. Challenges and Competences in Master Degrees from a Comprehensive Security Perspective. 14th International Conference on Computational Intelligence in Security for Information Systems and 12th International Conference on European Transnational Educational (CISIS 2021 and ICEUTE 2021). 2021. España. Participativo - Ponencia oral (comunicación oral). Congreso.

5 V. Gayoso Martínez; L. Encinas; A. Martín Muñoz. A Study of the Reconciliation Mechanism of NewHope. 13th International Conference on Computational Intelligence in Security for Information Systems (CISIS’2020). Universidad de Burgos. 2020. España. Participativo - Ponencia oral (comunicación oral). Congreso.

C.3. Proyectos o líneas de investigación

1 **Proyecto**. 1011091638, EuroQCI deployment in Spain (EuroQCI-Spain).. European Comission. Luis Hernández Encinas. (Instituto de Tecnologías Fisicas y de la Información "Leonardo Torres Quevedo" (ITEFI) CSIC). 01/01/2023-31/07/2025. 154.905 €. Miembro de equipo.

2 **Proyecto**. TED2021-130369BC33., QUantum-based Resistant Architectures and Techniques. Integration QKD+PQC (QURSA).. MICIIN, Convocatoria 2021 de Proyectos Orientados a la Transición Ecológica y a la Transición Digital, del Plan Estatal de Investigación Científica, Técnica y de Innovación 2021- 2023, en el Marco del. Verónica Fernández Marmól. (Instituto de Tecnologías Físicas y de la Información "Leonardo Torres Quevedo" (ITEFI) del CSIC). 01/12/2022-30/11/2024. 154.905 €. Investigador principal.

3 **Proyecto**. H2020-SU-ICT-2018-2020. ID:952622, Secure Platform for ICT Systems Rooted at the Silicon Manufacturing Process (SPIRS).. Cybersecurity. P. Brox Jiménez. (Instituto de Tecnologías Físicas y de la Información "Leonardo Torres Quevedo" (ITEFI) CSIC). 01/10/2021-30/09/2024. 5.041.091,25 €. Miembro de equipo.

4 **Proyecto**. PID2020-112586RB-I00, Protocolos, Mecanismos y Tecnologías Pre y Postcuánticas para la Ciberseguridad y la Privacidad (P2QProMeTe). Fondo Europeo de Desarrollo Regional de la U.E. MInisterio de Ciencia e Innovación (MICIIN). Luis Hernández Encinas. (Instituto de Tecnologías Físicas y de la Información "Leonardo Torres Quevedo"(ITEFI) CSIC). 01/09/2021-31/08/2024. 101.640 €. Investigador principal.

5 **Proyecto**. PCI2020-120691-2, Organically Resilient and Secure Wireless Networks for Next-Generation IoT Technologies to serve Future Connected Societies (ORACLE). EIG CONCERT-Japan 7th Joint Call ICT for Resilient, Safe and Secure Society; Agencia Española de Investigación. Luis Hernández Encinas. (Instituto de Tecnologías Fisicas y de la Información "Leonardo Torres Quevedo" (ITEFI) CSIC). 01/04/2021-30/03/2024. 120.000 €. Investigador principal.

6 **Proyecto**. TSI-020100-2009-44., Reconocimiento Mediante Olor Corporal en la Internet del futurO y su securizaciÓN, EMOCION. Ministerio de Industria Turismo y Comercio, Subprograma AVANZA I+D (Ingenio 2010), TSI-020100-2009-44. L. Hernández Encinas. (Instituto de Tecnologías Físicas y de la Información "Leonardo Torres Quevedo". CSIC.). 01/07/2009-30/06/2012. 112.350 €. Investigador principal.

7 **Contrato**. Estudio del estado del arte de la seguridad de librerías de criptografía postcuántica, incluyendo ataques por canal lateral a sus implementaciones y posibles contramedidas EPICOM. Luis Hernández Encinas. (Instituto de Tecnologías Fisicas y de la Información "Leonardo Torres Quevedo"). 01/06/2023-31/12/2023. 72.600 €.

8 **Contrato**. Revision of the AVA report corresponding to the evaluation carried out by LGAI of the Winbond's product SpiFlash® TrustMETM W75F40W [W/R] [I/J/W] [B/C] & W75F40W [BY/Q3] [I/J/W] [C/B]G Secure Serial Flash Memory Version: AA. Winbond Electronics Corporation.. Agustín Martín Muñoz. (Instituto de Tecnologias Físicas y de la Información "Leonardo Torres Quevedo". CSIC). 06/03/2023-06/06/2024. 2.000 €.

9 **Contrato**. Technical Support Project for CC Evaluation of Tongxin Microelectronics Co., Ltd. THD89 Secure Microcontroller, version 1.0.5, with Crypto Library. LGAI TECHNOLOGICAL CENTER S.A. Agustín Martín Muñoz. (Instituto de Tecnologias Físicas y de la Información "Leonardo Torres Quevedo". CSIC). 30/01/2023-30/01/2025. 18.150 €.

10 **Contrato**. Asistencia Técnica para la Evaluación de la Seguridad de Productos Criptográficos para el Centro Criptológico Nacional Ministerio de Defensa. Centro Nacional de Inteligencia (CNI). L. Hernández Encinas. (Instituto de Tecnologias Físicas y de la Información "Leonardo Torres Quevedo". CSIC). 01/01/2023-01/01/2024. 148.830 €.

11 **Contrato**. Asistencia Técnica para la Evaluación de la Seguridad de Productos Criptográficos para el Centro Criptológico Nacional Ministerio de Defensa. Centro Nacional de Inteligencia (CNI). L. Hernández Encinas. (Instituto de Tecnologias Físicas y de la Información "Leonardo Torres Quevedo". CSIC). 01/01/2022-01/01/2023. 148.830 €.

12 **Contrato**. SEGUR@: Seguridad y Confianza en la Sociedad de la Información Telefónica I+D (Ministerio de Turismo, Industria y Comercio, CENIT-2007 2004). L. Hernández Encinas. (Instituto de Tecnologías Físicas y de la Informacion "Leonardo Torres Quevedo". CSIC.). 2007-01/01/2011. 684.418,56 €.