SAN LUIS, 11 de septiembre de 2026.-

VISTO:

El EXPE: 12037/2026, mediante el cual se solicita la protocolización del Curso de Posgrado TÓPICOS AVANZADOS DE SEGURIDAD Y PRIVACIDAD EN SISTEMAS DE SOFTWARE; y

CONSIDERANDO:

Que el Curso de Posgrado se propone dictar en el ámbito de la Facultad de Ciencias Físico Matemáticas y Naturales desde el 04 de septiembre al 25 de septiembre de 2026 con un crédito horario de SESENTA (60) horas presenciales y bajo la coordinación de la Dra. Ana Gabriela GARIS.

Que la Comisión Asesora de Investigación, actuando en su carácter de Comisión de Posgrado, en su sesión del día 12 de agosto de 2026, analizó el expediente de referencia y recomienda aprobar el dictado del mencionado curso de posgrado.

Que el Consejo de Posgrado de la Universidad Nacional de San Luis en su reunión del 27 de agosto de 2026, analizó la propuesta y observa que el programa del curso, bibliografía, metodología de evaluación y docentes a cargo constituyen una propuesta de formación de posgrado de calidad en su campo específico de estudio.

Que, por lo expuesto, el Consejo de Posgrado aprueba la propuesta como Curso de Posgrado, según lo establecido en Ordenanza CS Nº 35/2016.

Que corresponde su protocolización.

Por ello; y en uso de sus atribuciones:

EL RECTOR DE LA UNIVERSIDAD NACIONAL DE SAN LUIS

RESUELVE:

ARTÍCULO 1º.- Protocolizar el dictado del Curso de Posgrado TÓPICOS AVANZADOS DE SEGURIDAD Y PRIVACIDAD EN SISTEMAS DE SOFTWARE, en el ámbito de la Facultad de Ciencias Físico Matemáticas y Naturales desde el 4 de septiembre al 25 de septiembre de 2026 con un crédito horario de SESENTA (60) horas presenciales.

ARTÍCULO 2º.- Protocolizar el cuerpo docente del curso Responsable: Dr. Mario Marcelo BERÓN, DU N.º 22140238; Colaborador: Enrique Alfredo MIRANDA, DU N.° 32456631, ambos de la Universidad Nacional de San Luis.

ARTÍCULO 3º.- Aprobar el programa del Curso de referencia, de acuerdo al Anexo de la presente disposición.

ARTÍCULO 4º.- Comuníquese, notifíquese, publíquese en el Digesto Administrativo de la Universidad Nacional de San Luis, insértese en el Libro de Resoluciones y archívese. -

RC

Documento firmado digitalmente según Ordenanza Rectoral Nº 15/2021 por: Subsecretario de Formación de Posgrado FAVIER, Sergio José – Rector GIL, Raúl Andrés.

ANEXO

IDENTIFICACIÓN DEL CURSO

UNIDAD ACADÉMICA RESPONSABLE: Facultad de Ciencias Físico Matemáticas y Naturales

DENOMINACIÓN DEL CURSO: TÓPICOS AVANZADOS DE SEGURIDAD Y PRIVACIDAD EN SISTEMAS DE SOFTWARE

CATEGORIZACIÓN: perfeccionamiento

FECHA DE DICTADO DEL CURSO: desde el 4 de septiembre al 25 de septiembre de 2026

MODALIDAD DE DICTADO: Presencial.

CRÉDITO HORARIO TOTAL: 60 horas (20 hs. teóricas, 20 hs. de prácticas de aula, 20 hs. de prácticas de laboratorio)

COORDINADOR: Dra. Ana Gabriela GARIS, DU N.° 25700407

EQUIPO DOCENTE

RESPONSABLE: Dr. Mario Marcelo BERÓN

COLABORADOR: Dr. Enrique Alfredo MIRANDA

PROGRAMA ANALÍTICO

FUNDAMENTACIÓN:

El curso se plantea como una actividad curricular optativa correspondiente al Doctorado en Ingeniería Informática. Como aspecto clave en la formación de profesionales altamente capacitados en el área de la ingeniería informática, se hace necesario estudiar y analizar los fundamentos básicos relacionados a la seguridad informática y la privacidad. Así mismo, se vuelve imprescindible dotar a los estudiantes de herramientas vinculadas a la Criptografía y la Teoría de la Información para abordar problemáticas actuales y encontrar óptimas soluciones.

OBJETIVOS:

Dotar al estudiante con capacidades para:

- Profundizar en la relación entre la Criptografía y la Seguridad Informática, y entre la Calidad de Información y Programas Maliciosos.
- Estudiar los métodos de ataque y defensa, junto con el análisis estático y dinámico de programas.

- Consolidar conceptos, generar habilidades y formular propuestas en el ámbito de la Gestión de la Seguridad.
- Estudiar el aporte de la Teoría de la Información, de los Números y de la Complejidad Algorítmica a la Seguridad Informática.
- Consolidar conceptos, generar habilidades y formular propuestas en el ámbito de los Sistemas de Cifrado.
- Profundizar y efectuar propuestas en el ámbito de las Funciones Hash en Criptografía, de la Autenticación y la Firma Digital, de los Certificados Digitales y Estándar PKCS, y de Aplicaciones de Correo Seguro.
- Adquirir una sólida base para el desarrollo de herramientas de análisis.
- Estudiar casos reales de cibercrimen, ciberterrorismo y guerra cibernética, y efectuar propuestas conceptuales e instrumentales para mitigar los efectos negativos en los tres ámbitos.

CONTENIDOS MÍNIMOS:

Seguridad Informática. Conceptos de Seguridad de Informática. Gestión de la Seguridad. Vulnerabilidades. Estrategias de Detección de Vulnerabilidades. Estrategias de Ataque. Estrategias de Defensa. Codificación Segura. Criptografía. Calidad de Información y Programas Malignos. Teoría de la Información. Teoría de los Números. Teoría de la Complejidad Algorítmica. Sistemas de Cifrado Clásicos. Introducción al Cifrado Moderno. Sistemas de Cifrado en Flujo. Cifrado Simétrico en Bloque. Cifrado Asimétrico con Mochilas. Cifrado Asimétrico Exponencial. Funciones Hash en Criptografía. Autenticación y Firma Digital. Certificados Digitales y Estándar PKCS. Aplicaciones de Correo Seguro. Protocolos y Esquemas Criptográficos. Cifrado con Curvas Elíptica. Crimen cibernético, terrorismo cibernético y guerra cibernética

PROGRAMA DETALLADO:

Unidad 1: Seguridad Informática.

Conceptos de Seguridad de Informática. Gestión de la Seguridad. Vulnerabilidades. Crimen cibernético, terrorismo cibernético y guerra cibernética. Delitos complejos e Informática forense. Evidencia Digital.

Unidad 2: Criptografía.

Teoría de la Información. Teoría de los Números. Teoría de la Complejidad Algorítmica. Sistemas de Cifrado Clásicos. Introducción al Cifrado Moderno. Sistemas de Cifrado en Flujo. Cifrado Simétrico en Bloque. Cifrado Asimétrico con Mochilas. Cifrado Asimétrico Exponencial. Funciones Hash en Criptografía. Autenticación y Firma Digital. Certificados

Digitales y Estándar PKCS. Protocolos y Esquemas Criptográficos. Cifrado con Curvas Elíptica.

Unidad 3: Protección de Software.

Software subrepticio. La escena. Ataque y Defensa. Análisis de Programas. Ingeniería Reversa. Ofuscación de Código. Aplicaciones de la Ofuscación de Código. Transformaciones que Ofuscan. Ofuscación de Código de Sombrero Negro. Prueba de Manipulaciones. Aplicaciones de la Prueba de Manipulaciones. Marca de Agua. Software forense. Ataques sobre sistemas de Marca de Agua. Similaridad de Software. Plagio. Marca de Nacimiento. Técnicas de Protección por Hardware. Distribución de un Token Físico. Vincular el Programa a la CPU. Ambiente de Ejecución Segura. Ejecución Encriptada. Barreras Físicas.

Unidad 4: Métodos de Ataque y Defensa.

Estrategias de Ataque. Prototipo de Cracking. Motivación del Adversario. Tareas del Adversario para Crackear un Programa. Metodología de Ataque del Adversario. Herramientas de Ataque. Técnicas que usa el Adversario. Estrategias de Defensa. Primitivas de Protección.

Unidad 5: Análisis Estático y Dinámico.

Concepto. Análisis de Control de Flujo. Análisis de Dependencia de Dato. Análisis de Alias. Slicing. Interpretación Abstracta. Representaciones de Programas. Visualización de Software. Análisis Dinámico. Depuración. Profiling. Trazas. Emulación. Reconstrucción del Fuente. Desensamble. Decompilación. Análisis Pragmático. Métricas de Estilo. Métricas de Complejidad de Software. Visualización de Software.

Unidad 6: Herramientas para la Construcción de Estrategias de Análisis Estático y Análisis Dinámico

ANTLR4. Generalidades. Implementación de Parsers. Construcción de Aplicaciones de Lenguajes usando Árboles. Oyentes y Visitantes. La Herramienta ANTLR4. Tiempo de Ejecución. Código Generado. Prueba de los Módulos Generados. Integración de los Módulos Generados con la Aplicación. Construcción de Aplicaciones Basadas en Lenguajes. Ejemplos de Aplicación.

El curso combinará clases teóricas con prácticas en las que los estudiantes podrán aplicar los conceptos y técnicas aprendidas. Además, se proporcionarán materiales de lectura complementarios y se promoverá la discusión y el debate sobre temas actuales en el campo de la seguridad informática y la privacidad.

SISTEMA DE EVALUACIÓN: Para aprobar el curso, el estudiante deberá desarrollar los casos prácticos correspondientes a cada tópico y deberá presentar un proyecto integrador,

en el que se evaluará si se ha logrado adquirir las capacidades esperadas. La evaluación es individual.

BIBLIOGRAFÍA:

- Abhijit Mohanta, Anoop Saldanha (2020). Malware Analysis and Detection Engineering: A Comprehensive Approach to Detect and Analyze Modern Malware. Editorial: Apress; 1st ed. edición (23 septiembre 2020). Idioma: Inglés. Tapa blanda: 948 páginas. ISBN-10:1484261925. ISBN-13:978- 1484261927.
- Adkins, Heather; Beyer, Betsy; Blankinship Paul; Lewandowski, Piotr; Oprea Ana. (2020). Building Secure and Reliable Systems: Best Practices for Designing, Implementing, and Maintaining Systems. Editorial O'Reilly Media; 1er edición.
- ANTLR, Sitio web oficial https://www.antlr.org/ (última visita 24/7/2026)
- Banescu S., Ochoa M., y Pretschner A. (2015), "A framework for measuring software obfuscation resilience against automated attacks," in 2015 IEEE/ACM 1st International Workshop on Software Protection, May 2015, pp. 45–51.
- Bayrak A. G., Regazzoni F., Novo D., Brisk P., Standaert F. y Ienne P. (2015), "Automatic application of power analysis countermeasures," IEEE Transactions on Computers, vol. 64, no. 2, pp. 329–341.
- Basile C., Canavese D., D'Annoville J., Sutter B. D. y Valenza F. (2015) "Automatic discovery of software attacks via backward reasoning," in 2015 IEEE/ACM 1st International Workshop on Software Protection, pp. 52–58.
- Ceccato M., Tonella P., Basile C., Coppens B., De Sutter B., Falcarin P. y Torchiano M. (2017). How professional hackers understand protected code while performing attack tasks, in 2017 IEEE/ACM 25th International Conference on Program Comprehension (ICPC), May 2017, pp. 154–164.
- Chuck Easttom (2021). Computer Security Fundamentals (Pearson IT Cybersecurity Curriculum (ITCC)). 4th edición. Editorial: Pearson IT Certification; 4a edición. ISBN de origen: 0135774772.
- Dalai A. K., Das S. S., y Jena S. K. (2017). A code obfuscation technique to prevent reverse engineering, in 2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), March 2017, pp. 828–832.
- Jawalkar M. K., Gokhale P. S., y Dixit A. M. (2015). "Jiid: Java input injection detector for pre-deployment vulnerability detection," in 2015 IEEE International Conference on Research in Computational Intelligence and Communication Networks (ICRCICN), pp. 444–449.

- Kuang K., Tang Z., Gong X., Fang D., Chen X., Zhang H., Liu J., y Wang Z. (2017). Exploit dynamic data flows to protect software against semantic attacks in 2017 IEEE SmartWorld, Ubiquitous Intelligence Computing, Advanced Trusted Computed, Scalable Computing Communications, Cloud Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI), Aug 2017,pp.1-6.
- Long, Fred, Mohindra, Dhruv, Seacord, Robert C., Sutherland, Dean F., y Svoboda, David (2014). JavaTM Coding Guidelines: 75 Recommendations for Reliable and Secure Programs. Long, Fred, 1947: Addison Wesley.
- Oliveira L., Pereira F., Misoczki R., Aranha D., Borges F., y Liu J. (2017) "The computer for the 21st century: Security, privacy challenges after 25 years,"in 2017 26th International Conference on Computer Communication and Networks (ICCCN). IEEE, 2017., 07 2017, pp. 1–10.
- Protsenko M., Kreuter S. y Müller T. (2015). "Dynamic self-protection and tamperproofing for android apps using native code," in 2015 10th International Conference on Availability, Reliability and Security, pp. 129–138.
- Seacord, Robert (2014). CERT® C Coding Standard, Second Edition. The 98 Rules for Developing Safe, Reliable, and Secure Systems (SEI Series in Software Engineering). Editorial: Addison-Wesley Professional; 2nd edición.
- Stalling, William; Brown, Lawrie (2017). Computer Security: Principles and Practices. Editorial: Pearson. 4a edición. • Seacord R. (2013) Secure Coding in C and C++, 2nd ed. Addison-Wesley.
- Software Engineering Institute (2016) SEI CERT C Coding Standard, Rules for Developing Safe, Reliable and Secure Systems. Carnegie Mellon University.
- Vacca, John (2009). Computer and Information Security Handbook (Morgan Kaufmann Series in Computer Security).
- Villalba de Benito, M.Teresa; Fernández, Luis (2012). Modelos de Calidad del Software: Un modelo práctico para medir la calidad de los productos de Seguridad Informática. Editorial Académica Española.
- Oracle software security assurance (2026). [En línea]. Disponible: https://www.oracle.com/ar/corporate/security-practices/assurance/ (última visita 24/7/2026)
- Wang H., Fang D., Li J., Chang Y., y Yu L. (2016). "The research and discussion on effectiveness evaluation of software protection," in 2016 12th International Conference on Computational Intelligence and Security (CIS), pp. 62

CARACTERISTICAS DEL CURSO

DESTINATARIOS Y REQUISITOS DE INSCRIPCIÓN

Los aspirantes deben ser graduados con título universitario de grado. Profesionales en Informática y títulos de grado similares correspondientes a carreras con planes de estudio que impliquen 4 o más años de duración.

PROCESO DE ADMISIÓN: Se evaluará el CV de los postulantes y su formación previa.

CUPO: mínimo de 5 y máximo 20 estudiantes.

CRONOGRAMA DE ACTIVIDADES:

Fecha	Tipo de actividad/Temas a desarrollar	Docente/s	Ámbito
04/09/26	Clases teórico-prácticos / Unidad 1	Dr. Mario Berón Dr. Enrique Miranda.	Aula Posgrado Dpto. Informática
05/09/26	Clases teórico-prácticos / Unidad 2	Dr. Mario Berón Dr. Enrique Miranda	Aula Posgrado Dpto. Informática
11/09/26	Clases teórico-prácticos / Unidad 3	Dr. Mario Berón Dr. Enrique Miranda	Aula Posgrado Dpto. Informática
12/09/26	Clases teórico-prácticos / Unidad 4	Dr. Mario Berón Dr. Enrique Miranda	Aula Posgrado Dpto. Informática
18/09/26	Clases teórico-prácticos / Unidad 5.	Dr. Mario Berón Dr. Enrique Miranda	Aula Posgrado Dpto. Informática
19/09/26	Clases teórico-prácticos / Unidad 6.	Dr. Mario Berón Dr. Enrique Miranda	Aula Posgrado Dpto. Informática
25/09/26	Evaluación final	Dr. Mario Berón Dr. Enrique Miranda	Aula Posgrado Dpto. Informática

LUGAR DE DICTADO: 1° piso del Bloque II. Departamento de Informática-Aula de Posgrado Facultad de Ciencias Físico Matemáticas y Naturales - UNSL. Av. Ejército de los Andes 950.

FECHA PREVISTA PARA ELEVAR LA NÓMINA DE ESTUDIANTES APROBADOS: diciembre de 2026

FINANCIAMIENTO DEL CURSO

COSTOS: Honorarios Docentes.

FUENTES DE FINANCIAMIENTO: El curso es autofinanciado mediante arancel.

ARANCEL GENERAL: PESOS CIEN MIL ($100.000).

BECA A DOCENTES DE LA UNSL: Los docentes no abonan arancel, será gratuito.

BECA A ESTUDIANTES DE LA UNSL: Los estudiantes de posgrado no abonan arancel, será gratuito.

Hoja de firmas

Sistema: SUDOCU UNSL
Firmado por: SUDOCU UNSL
Fecha: 11/09/2026 09:33:18
Razon: Cargado por SIU-Documentos

Sistema: SUDOCU UNSL
Firmado por: SUDOCU UNSL
Fecha: 11/09/2026 11:30:58
Razon: Autorizado por Sergio Jose Favier

Sistema: SUDOCU UNSL
Firmado por: SUDOCU UNSL
Fecha: 11/09/2026 14:55:12
Razon: Autorizado por Raul Andres Gil