Resolución de Consejo Directivo **551 / 2026 - EXA -UNSa**
EXP 395/2025-EXA-UNSa: Tener por autorizado el dictado de la asignatura "Seminario de actualización tecnológica" (Seguridad de la información) de la carrera de Maestría en Informática, a cargo del Mag. Felipe David ORTIZ.
De: EXACTAS-Dirección de Posgrado

Salta,
26/08/2026

VISTO la presentación efectuada por el Mag Gustavo Daniel GIL, mediante la cual solicita autorización para dictar la asignatura "Seminario de actualización tecnológica" (Seguridad de la información), correspondiente a la carrera de Maestría en Informática - Plan 2023, a cargo del Mag. Felipe David ORTIZ y la coordinación del Mag. Gustavo Daniel GIL, y

CONSIDERANDO:

Que se cuenta con el visto bueno del Departamento de Informática y el despacho favorable de la Comisión de Posgrado.

Que la Comisión de Docencia e Investigación, desde el punto de vista académico, aconseja: 1) tener por autorizado el dictado de la asignatura "Seminario de actualización tecnológica" (Seguridad de la información), durante el primer cuatrimestre de 2026; y 2) tener por aprobado el programa analítico y el cuerpo docente propuesto.

Por ello y en uso de las atribuciones que le son propias.

EL CONSEJO DIRECTIVO DE LA FACULTAD DE CIENCIAS EXACTAS
(en su 9° Sesión Ordinaria del 10/06/2026)
RESUELVE

ARTÍCULO 1º: Tener por autorizado el dictado de la asignatura "Seminario de actualización tecnológica" (Seguridad de la información), correspondiente a la carrera de Maestía en Informática, a cargo del Mag. Felipe David ORTIZ y la coordinación del Mag. Gustavo Daniel GIL, a partir del 15 de mayo de 2026.

ARTÍCULO 2º: Tener por aprobado el programa analítico de la asignatura "Seminario de actualización tecnológica" (Seguridad de la información) y el plantel docente, de acuerdo a las características y requisitos que se explicitan en el anexo de la presente resolución.

ARTÍCULO 3º: Notifíquese al Mag. Felipe David ORTIZ y al Mag. Gustavo Daniel GIL. Comuníquese a las Autoridades y Secretarías de la Facultad, al Comité Académico de la Maestría en Informática, al Departamento de Informática, a la Comisión de Posgrado, a la Dirección General Administrativa Económica (Cr. Héctor FLORES), a la Dirección Administrativa Económica y Financiera (Sr. Oscar R. LESCANO) y a la Dirección Administrativa de Posgrado. Cumplido, archívese

ma

LIC. MARCELA F. LÓPEZ
SECRETARIA ACADÉMICA Y DE INVESTIGACIÓN
FACULTAD DE CS. EXACTAS - UNSa

Dr. JOSÉ RAMÓN MOLINA
DECANO
FACULTAD DE CS. EXACTAS - UNSa

ANEXO

Asignatura: "Seminario de actualización tecnológica" (Seguridad de la información)

Carrera: Maestría en Informática - Plan de Estudio 2023

Docente Responsable: Mg. Felipe David ORTIZ (UNAHUR)

Coordinador: Mag. Gustavo Daniel GIL (UNSa)

Objetivos:
Interiorizar a los/as alumnos/as en principios, tecnologías, metodologías y estándares empleados para asegurar y controlar la disponibilidad, integridad y confidencialidad de sistemas, equipos, redes y la información contenida o transmitidas a través de estos.
Dar a conocer los fundamentos de la seguridad de la información y su relación con las organizaciones y el ambiente laboral.

Modalidad: Curso teórico-práctico. Presencial con instancias de actividades asincrónicas

Carga horaria: 60 horas (24 hs. Teóricas y 36 hs. Prácticas).

Fecha de dictado: A partir del 15 de mayo de 2026.

Lugar de dictado: Laboratorio 4 del Departamento de Informática de la Facultad de Ciencias Exactas, UNSa.

Cronograma propuesto:

Nro. de clase	Fecha	Unidad analítica	Modalidad de dictado	Docente responsable
1	15/05/26 (19 a 22 hs)	Unidad 1	Virtual sincrónica	Felipe Ortiz
2	22/05/26 (19 a 22 hs)	Unidad 2	Virtual sincrónica	Felipe Ortiz
3	29/05/26 (19 a 22 hs)	Unidad 3	Virtual sincrónica	Felipe Ortiz
4	05/06/26 (19 a 22 hs)	Unidad 4	Virtual sincrónica	Felipe Ortiz.
5	12/06/26 (19 a 22 hs)	Unidad 5	Virtual sincrónica	Felipe Ortiz
6	19/06/26 (19 a 22 hs)	Unidad 6	Virtual sincrónica	Felipe Ortiz
7	26/06/26 (19 a 22 hs)	Unidad 7	Virtual sincrónica	Felipe Ortiz
8	03/07/27 (19 a 22 hs)	Defensa de trabajos y cierre	Virtual sincrónica	Felipe Ortiz

FACULTAD DE CIENCIAS EXACTAS UNSa

Metodología de enseñanza y aprendizaje:

Las estrategias de aprendizaje planeadas para los alumnos comprenden clases teóricas y prácticas, desarrollo de trabajos prácticos grupales que apliquen los conceptos teóricos presentados en clase.
La guía de trabajos prácticos del seminario incluirá, además de prácticas con casos de estudio, trabajos de lectura y análisis de herramientas del mercado.
Asimismo, los alumnos deberán elaborar en forma grupal un trabajo de integración de conceptos en base al documento de especificación de un sistema de información, generado por una organización real.

Sistema de Evaluación:

Todas las actividades solicitadas a los alumnos serán evaluadas de manera continua durante las clases y al final del seminario, deberán realizar una defensa oral del trabajo integrador y del trabajo de investigación de manera virtual.
El trabajo de investigación concluye un tema de investigación vinculado al seminario a definir por el docente a cargo.

Contenidos mínimos:

Introducción a la Seguridad de la Información. Conceptos fundamentales y objetivos. Gestión de la Seguridad de la Información. Riesgo: análisis y tratamiento. Seguridad en Redes, elementos de criptografía. Criptografía Simétrica y Asimétrica. Algoritmos de Hash. Infraestructura de Clave Pública. Certificados digitales. Seguridad en Redes. Objetivos. Ataques, Servicios y Mecanismos de Seguridad. Seguridad en Redes Inalámbricas. Control de Acceso Lógico. Controles físicos de seguridad: seguridad en el centro de cómputos. Seguridad en las operaciones. Gestión de usuarios. Control de cambios. Métodos de Evaluación de seguridad: Auditorías, Evaluaciones funcionales, Vulnerability Assessment y Penetration Test. Gestión de Incidentes. Seguridad en Aplicaciones. Vulnerabilidades. Software malicioso. Problemática de las aplicaciones WEB. Leyes, Regulaciones y Estándares. Marcos legales nacional e internacional. Privacidad, Integridad y seguridad en sistemas de información.

Programa Analítico

Unidad 1: Introducción a la seguridad de la información.
Introducción a la Seguridad de la Información. Confidencialidad, Integridad y Disponibilidad. Identificación, Autenticación, Autorización y Accountability. Definición de Activo de información, Vulnerabilidad, Amenazas y Riesgos.

Unidad 2: Sistemas de Gestión de la Seguridad de la Información (SGSI).
Introducción a los Sistemas de Gestión. Modelo PDCA. Enfoque Top Down Vs. Enfoque Bottom Up. Familia ISO/IEC 27.00X. Clasificación de la Información. Análisis de Riesgos como base de los SGSI.

Unidad 3: Seguridad en Redes.
Objetivos. Modelo OSI. Ataques, Servicios y Mecanismos de Seguridad. Modelo TCP/IP. Controles y dispositivos de seguridad. Seguridad en el perímetro. Firewalls y proxies. Redes Virtuales (VLANs). Redes Privadas Virtuales (VPNs). IPSec. Seguridad en redes inalámbricas. Seguridad en redes Wifi.

FACULTAD DE CIENCIAS EXACTAS UNSa

Unidad 4: Control de acceso físico y lógico.
Tipos de amenazas. Selección de la ubicación del datacenter. Protección en capas. Seguridad perimetral. Control de acceso lógico. Metodologías de control de acceso. Identificación, autenticación y autorización. Tipos de factores de autenticación. Gestión de identidades. SSO.

Unidad 5: Detección y análisis de vulnerabilidades.
Métodos de Evaluación de Seguridad. Tipos de análisis de vulnerabilidades. Aspectos legales. CVSS (common vulnerability scoring system). Escaneo de vulnerabilidades. Vulnerability Assessment y Test de Intrusiones. Tipos de hackers. Fases del hacking ético. Gestión del hacking ético.

Unidad 6: Seguridad en Aplicaciones.
Introducción a la seguridad en el software. Problemática del desarrollo de aplicaciones. Ciclo de vida del desarrollo del software. Software malicioso: Troyanos, backdoors, virus y gusanos. Otros tipos de malware. Niveles de maduración. Problemática de las aplicaciones WEB. OWASP Top 10.

Unidad 7: Ciberestafas.
Análisis de diferentes tipos de ciberestafas y metodologías de protección. Aplicación a sistemas empresariales y aplicación a nivel personal.

Bibliografía Obligatoria:

- ISC2 CISSP Certified Information Systems Security Professional Official Study Guide (Sybex Study Guide) 10th Edición. Mike Chapple (Author), James Michael Stewart (Author), Darril Gibson (Author)

Bibliografía Optativa:

- Albakri, Sameer-Hasan; Shanmugam, Bharanidharan; Samy, Ganthan-Narayana; Idris, Norbik-Bashah; Ahmed, Azuan (2014). "Security risk assessment framework for cloud computing environments". Security and communication networks, v. 7, n. 11, pp. 2114-2124. https://doi.org/10.1002/sec.923
- Mesquida, Antoni-Lluís; Mas, Antonia (2015). "Implementing information security best practices on software lifecycle processes: The ISO/IEC 15504 security extension". Computers and security, v. 48, pp. 19-34. https://goo.gl/BZt89n https://doi.org/10.1016/j.cose.2014.09.003

Repositorios de interés:

- Repositorio Institucional de la UNLP, https://sedici.unlp.edu.ar/
- Sistema Nacional de Repositorios Nacionales, https://repositoriosdigitales.mincyt.gob.ar/vufind/
- Open Digital Library of the Brazilian Computer Society - SOL (https://sol.sbc.org.br/index.php/anais).

LIC. MARCELA F. LÓPEZ
SECRETARIA ACADÉMICA Y DE INVESTIGACIÓN
FACULTAD DE CS. EXACTAS - UNSa

Dr. JOSÉ RAMÓN MOLINA
DECANO
FACULTAD DE CS. EXACTAS - UNSa