Resolución Consejo Directivo FCEyN N° 510 / 2025

Santa Rosa, 28 de noviembre de 2025

VISTO:

El Expediente. Nº 613/2025, iniciado por Secretaría Académica, Programas carrera Tecnicatura en Informática de Gestión - año 2025, y

CONSIDERANDO:

Que el docente Esp. Leandro Javier CASTRO, a cargo de la asignatura "Informática de Gestión II" que se dicta para la carrera Tecnicatura en Informática de Gestión (Plan 2023), eleva programa de la citada asignatura para su aprobación a partir del ciclo lectivo 2025 en adelante.

Que el mismo cuenta con el aval del Mg. Ruben PIZARRO y de la Mesa de Carrera de la Tecnicatura en Informática de Gestión.

Que en la sesión ordinaria del 27 de noviembre de 2025 el Consejo Directivo aprobó, por unanimidad, el despacho presentado por la Comisión de Enseñanza.

POR ELLO:

EL CONSEJO DIRECTIVO DE LA FACULTAD DE CIENCIAS EXACTAS Y NATURALES
RESUELVE:

ARTÍCULO 1º: Aprobar el programa de la asignatura "Informática de Gestión II" correspondiente a la carrera Tecnicatura en Informática de Gestión (Plan 2023), a partir del ciclo lectivo 2025 en adelante, que como Anexos I, II, III, IV, V, VI y VII forma parte de la presente Resolución.

ARTÍCULO 2º: Regístrese, comuníquese. Pase a conocimiento de Secretaría Académica, Departamento de Asuntos Estudiantiles, Departamento de Matemática y Computación, del docente Esp. Leandro Javier CASTRO, y del CENUP. Cumplido, archívese.

Gabriela Raquel VIDOZ – Secretaria Consejo Directivo – FCEyN - UNLPam

Nora Claudia FERREYRA – Decana – FCEyN - UNLPam

ANEXO I

DEPARTAMENTO: Matemática y Computación

ACTIVIDAD CURRICULAR: Informática de Gestión II

CARRERA-PLAN/ES: Tecnicatura en Informática de Gestión - 2023

CURSO
Segundo año

RÉGIMEN
Cuatrimestral (Segundo cuatrimestre)

CARGA HORARIA SEMANAL
Teórico-Práctico: 7 horas

CARGA HORARIA TOTAL
105 horas.

CICLO LECTIVO
2025 en adelante

EQUIPO DOCENTE
Prof. Esp. Leandro Javier CASTRO, Profesor Adjunto Interino, dedicación simple
Lic. Sofía FUNKNER, Jefa de Trabajos Prácticos Interina, dedicación simple.

FUNDAMENTACIÓN

En la actualidad, el uso cotidiano de Tecnologías de la Información y la Comunicación (TIC) constituye una práctica social y profesional indispensable. La gestión de datos personales, información organizacional y activos digitales estratégicos atraviesa todas las actividades humanas y productivas. En este contexto, los y las estudiantes deben reconocer la necesidad crítica de establecer y mantener un sistema integral, sistemático y permanente de seguridad de la información, orientado a garantizar la confidencialidad, integridad y disponibilidad de los datos.

La asignatura se propone brindar un enfoque formativo integral que articule los fundamentos teóricos con la práctica aplicada en entornos de simulación y administración real a partir del estudio de normas y marcos regulatorios nacionales e internacionales. Las y los estudiantes adquirirán competencias para analizar, diseñar e implementar políticas y medidas de seguridad efectivas en organizaciones públicas y privadas.

El programa contempla tanto los aspectos preventivos como los detectivos y correctivos, mediante el uso de herramientas de libre acceso para identificar activos, amenazas, ataques y vulnerabilidades en sistemas de información. Se promoverá la realización de prácticas de administración de sistemas y plataformas en la nube, gestión de accesos remotos seguros, instalación y configuración de sistemas de gestión de contenidos con criterios de seguridad, así como la ejecución de auditorías de redes y pruebas de penetración ética.

De esta manera, el grupo de estudiantes podrá trasladar los aprendizajes a situaciones reales de trabajo en equipo interdisciplinario, participando en la definición de estrategias de defensa organizacional y en la implementación de soluciones seguras para la protección de la información.

El curso se apoyará en el entorno virtual de la facultad, que centralizará el acceso a los materiales, actividades, espacios de comunicación y seguimiento personalizado de los avances del grupo. La propuesta didáctica combinará recursos teóricos, guías prácticas y entornos de simulación que aproximan la experiencia del aula a los desafíos actuales de la ciberseguridad en la gestión de la información.

OBJETIVOS Y/O ALCANCES DE LA ASIGNATURA

OBJETIVOS GENERALES

Objetivo General Principal: Desarrollar competencias técnicas y de gestión en seguridad informática para que cada estudiante pueda participar efectivamente en equipos interdisciplinarios, asesorando y colaborando en la implementación de soluciones seguras de información en organismos y empresas.

OBJETIVOS ESPECÍFICOS

- **Comprender** los fundamentos de la seguridad de la información y seguridad informática, diferenciando sistemas de información de sistemas informáticos.
- **Analizar** normas y políticas de seguridad informática aplicables en entornos organizacionales.
- **Identificar** mecanismos de seguridad.
- **Reconocer** diferentes tipos de amenazas informáticas.
- **Implementar** estrategias de defensa utilizando herramientas de monitoreo del sistema.
- **Gestionar** accesos remotos seguros.
- **Administrar** plataformas en la nube para soluciones empresariales.
- **Realizar** auditorías de redes para detectar vulnerabilidades.
- **Instalar y configurar** sistemas de gestión de contenidos con criterios de seguridad.

ANEXO II

ASIGNATURA

Informática de Gestión II

CICLO LECTIVO

2025 en adelante

PROGRAMA ANALÍTICO

BLOQUE TEMÁTICO 1

Sistemas de información y sistemas informáticos: arquitectura y componentes. Principios fundamentales: confidencialidad, integridad, disponibilidad. Gestión de riesgos: identificación, análisis, evaluación y tratamiento. Marco normativo: ISO 27000/27001, NIST Cybersecurity Framework, GDPR, Ley de Protección de Datos Personal. Mecanismos de seguridad: preventivos, detectivos y correctivos. Implementación de sistemas de backup y recuperación.

BLOQUE TEMÁTICO 2

Gestión de infraestructura de clave pública (PKI). Protocolos de acceso remoto seguro: SSH, VPN, RDP seguro. Administración de sistemas GNU/Linux: hardening y configuración segura. Servicios web seguros: HTTPS, certificados SSL/TLS. Sistemas de gestión de contenidos (CMS): instalación y configuración segura.

BLOQUE TEMÁTICO 3

Definición y características distintivas del software malicioso. Criterios de identificación: comportamiento anómalo, modificaciones no autorizadas, consumo irregular de recursos. Diferenciación entre software malicioso, software potencialmente no deseado y falsos positivos. Ciclo de vida del malware: creación, distribución, infección, ejecución y persistencia. Ingeniería social: phishing, pretexting, baiting. Explotación de vulnerabilidades: zero-day, exploit kits.

BLOQUE TEMÁTICO 4

Modelos de servicios cloud: IaaS, PaaS, SaaS y sus implicancias de seguridad. Configuración segura de plataformas cloud. Auditorías de seguridad: metodologías, herramientas y reporting. Pruebas de penetración ética: alcances, metodologías.

ANEXO III

ASIGNATURA

Informática de Gestión II

CICLO LECTIVO

2025 en adelante

BIBLIOGRAFÍA

International Organization for Standardization; International Electrotechnical Commission. (2022). *ISO/IEC 27001:2022 Tecnología de la información – Técnicas de seguridad – Sistemas de gestión de la seguridad de la información – Requisitos*. ISO. Recuperado de https://www.iso.org/es/norma/27001?frame=0&nav=1

National Institute of Standards and Technology. (2017). *An introduction to information security (NIST Special Publication 800-12 Revision 1)*. U.S. Department of Commerce. https://csrc.nist.gov/pubs/sp/800/12/r1/final

GDPRinfo. (s. f.). *Reglamento general de protección de datos*. Recuperado de https://gdprinfo.eu/es

Honorable Congreso de la Nación Argentina. (2000, 4 de octubre). *Ley 25.326 de Protección de los Datos Personales* [Texto actualizado]. Presidencia de la Nación Argentina. https://www.argentina.gob.ar/normativa/nacional/ley-25326-64790/actualizacion

Aguilera López, P. (2010). *Seguridad informática*. Editex. Recuperado de https://play.google.com/store/books/details?id=Mgvm3AYIT64C&hl=es

Romero Castro, M. I., Figueroa Morán, G. L., Vera Navarrete, D. S., Álava Cruzatty, J. E., Parrales Anzúles, G. R., Álava Mero, C. J., Murillo Quimiz, Á. L., & Castillo Merino, M. A. (2018, octubre). *Introducción a la seguridad informática y el análisis de vulnerabilidades*. 3Ciencias. Recuperado de https://play.google.com/store/books/details?id=5Z9yDwAAQBAJ&hl=es

Shotts, W. E., Jr. (2025). *The Linux Command Line* (Sixth Internet Edition) [Libro en línea]. https://linuxcommand.org/tlcl.php

Samaniego Mena, E. A., & Ponce Ordóñez, J. A. (2021). *Fundamentos de seguridad informática*. Editorial Grupo Compás. Universidad Técnica Estatal de Quevedo. ISBN 978-9942-33-426-8. Recuperado de https://www.researchgate.net/publication/354054517_Libro_Fundamentos_de_seguridad_informatica

Baca Urbina, G. (2016). *Introducción a la seguridad informática* [Versión e-book]. Grupo Editorial Patria. Recuperado de Academia.edu: https://www.academia.edu/40572652/Introduccion_a_la_seguridad_informatica_LIBRO

Caballero, M. A., Baus Lerma, L., & Cilleros Serrano, D. (2024). *Ciberseguridad paso a paso: Diseña tu estrategia* [Primer capítulo]. Anaya Multimedia. Recuperado de https://anayamultimedia.es/primer_capitulo/ciberseguridad-paso-a-paso.pdf

Agencia Española de Protección de Datos; Asociación Profesional Española de Privacidad; ISMS Forum España. (mayo de 2023). *Orientaciones para la validación de sistemas criptográficos en la protección de datos* [Guía]. Recuperado de https://www.aepd.es/guias/orientaciones-criptografia-aepd-isms-apep.pdf

Rifà Pous, H. (s. f.). *Infraestructura de clave pública (PKI)* [Documento PDF]. Universitat Oberta de Catalunya. Recuperado de

https://openaccess.uoc.edu/server/api/core/bitstreams/e939c10e-f9df-4f22-9f2d-b29430fdbc66/content

ANEXO IV

ASIGNATURA

Informática de Gestión II

CICLO LECTIVO

2025 en adelante

PROGRAMA DE TRABAJOS PRÁCTICOS

Trabajo Práctico 1: Análisis de riesgos y marco normativo

Este trabajo práctico se desarrollará en la primera parte de la cursada y tiene como finalidad que las y los estudiantes se introduzcan en la gestión de riesgos y en el conocimiento de las principales normas y marcos regulatorios de seguridad de la información. A partir de casos simulados, el grupo de estudiantes deberá identificar activos críticos, amenazas potenciales y vulnerabilidades. Este trabajo permitirá comprender la relación entre sistemas de información y sistemas informáticos, así como aplicar los principios de confidencialidad, integridad y disponibilidad de la información. Además, se analizarán los principales marcos regulatorios (ISO 27000, ISO 27001, NIST, GDPR, Ley 25.326 de Protección de Datos Personales), destacando su importancia para la implementación de políticas de seguridad en entornos organizacionales. Para guiar el proceso, en este y el resto de los trabajos, se proporcionarán los objetivos específicos de las actividades y se pondrán a disposición diferentes formatos de entrega según la actividad presentada (texto escrito, infografías, videos o audios). Se proporcionará retroalimentación escrita y oral, y el grupo de estudiantes contará con instancias de reentrega en caso de ser necesario. Asimismo, se ofrecerán rúbricas de evaluación que expliciten los aspectos a considerar.

Trabajo Práctico 2: Administración segura de servidores y accesos remotos

Este trabajo práctico se desarrollará durante el segundo bloque de la cursada y tiene como propósito que las y los estudiantes apliquen configuraciones básicas de seguridad en entornos GNU/Linux. Deberán instalar y configurar servicios de acceso remoto seguro utilizando SSH y RDP, implementar medidas de hardening en servidores y verificar la comunicación cifrada mediante certificados digitales. El trabajo se articulará con la práctica de gestión de sistemas y con el análisis de mecanismos preventivos y detectivos de seguridad. Su desarrollo permitirá al grupo de estudiantes reconocer la importancia de gestionar de forma segura los accesos remotos y fortalecer las competencias técnicas necesarias para la administración de plataformas y servicios empresariales.

Trabajo Práctico 3: Identificación de malware e ingeniería social

Este trabajo práctico se realizará en la tercera parte de la cursada y estará orientado a la identificación de software malicioso y técnicas de ingeniería social. El grupo de estudiantes trabajará con un material educativo, donde analizarán síntomas de infección en un sistema informático, como procesos anómalos, modificaciones no autorizadas o consumo irregular de recursos. Asimismo, deberán examinar ejemplos de phishing y otras estrategias de engaño, evaluando su impacto en las personas y organizaciones. Este trabajo permitirá reconocer diferentes tipos de amenazas informáticas, aplicar criterios de identificación y diseñar medidas preventivas, vinculando la práctica con los contenidos sobre ciclo de vida del malware, vulnerabilidades y técnicas de ataque.

Trabajo Práctico 4: Seguridad en entornos cloud y auditoría informática

Este trabajo práctico se desarrollará en la última etapa de la cursada y buscará integrar los aprendizajes anteriores en un entorno de aplicación realista. Las y los estudiantes deberán configurar y establecer controles de acceso y, proteger el almacenamiento de la información. Posteriormente, realizarán una auditoría de seguridad utilizando herramientas de libre acceso, elaborando un reporte con hallazgos y recomendaciones. Finalmente, se introducirán a la práctica de pruebas de penetración ética a través de escenarios simulados. Este trabajo permitirá comprender los riesgos y

responsabilidades en la gestión de servicios cloud, y aplicar metodologías de auditoría y defensa activa en seguridad informática.

ANEXO V

ASIGNATURA

Informática de Gestión II

CICLO LECTIVO

2025 en adelante

ACTIVIDADES ESPECIALES QUE SE PREVÉN

No se prevén actividades especiales

ANEXO VI

ASIGNATURA

Informática de Gestión II

CICLO LECTIVO

2025

PROGRAMA DE EXAMEN

Coincide con el programa analítico.

ANEXO VII

ASIGNATURA

Informática de Gestión II

CICLO LECTIVO

2025 en adelante

METODOLOGÍA DE EVALUACIÓN Y/O OTROS REQUERIMIENTOS

Según reglamentación vigente.

La evaluación será mediante un proceso formativo, continuo y participativo, en el que cada instancia de evaluación constituye, a la vez, una oportunidad de aprendizaje. Desde el inicio de la cursada se explicitarán los criterios de evaluación y se revisarán periódicamente, de manera conjunta con el grupo de estudiantes, en relación con los objetivos y contenidos de la asignatura.

El error se considerará un recurso pedagógico fundamental. Por ello, se brindará retroalimentación escrita y oral en cada entrega de los trabajos prácticos, y se habilitarán instancias de reentrega para favorecer la mejora y el aprendizaje progresivo.

La metodología contempla diferentes modalidades de evaluación:

- **Autoevaluación y autosupervisión:** las y los estudiantes reflexionarán sobre su propio proceso de aprendizaje, utilizando la plataforma Moodle para acceder a cuestionarios de autoevaluación y actividades diagnósticas.
- **Evaluación entre pares:** a través de foros y otras instancias colaborativas en el entorno virtual, se fomentará la revisión crítica y constructiva de los trabajos elaborados por el resto del grupo de estudiantes.
- **Evaluación por parte del equipo docente:** mediante una planilla de seguimiento previamente compartida, se detallarán los aspectos técnicos, metodológicos y comunicacionales a considerar en cada actividad.

Se propondrán distintos formatos de entrega (texto, infografía, presentación audiovisual, podcast, etc.) para favorecer la creatividad y la integración de competencias comunicacionales.

Criterios de evaluación

- Participación activa en las actividades asincrónicas.
- Entrega en tiempo y forma de los trabajos prácticos.
- Cumplimiento de los criterios mínimos específicos de cada actividad.

Requerimientos para la regularidad de la asignatura

- Aprobar el examen parcial.
- Entregar y aprobar el trabajo final integrador que articule los contenidos de los diferentes bloques temáticos en un contexto aplicado.

Requerimientos para la promoción de la asignatura

- Obtener una calificación de 6 (seis) o superior en el examen parcial.
- Aprobar las actividades evaluativas desarrolladas durante la cursada.
- Entregar, aprobar y defender el trabajo final integrador que articule los contenidos de los diferentes bloques temáticos en un contexto aplicado.

Hoja de firmas

Sistema: sudocu
Fecha: 03/12/2025 10:25:48
Cargado por: Gabriela Raquel Vidoz

Sistema: sudocu
Fecha: 03/12/2025 10:26:35
Autorizado por: Gabriela Raquel Vidoz

Sistema: sudocu
Fecha: 03/12/2025 11:26:56
Autorizado por: Nora Claudia Ferreyra