DISPOSICIÓN CONSEJO DIRECTIVO DEPARTAMENTAL DE CIENCIAS BÁSICAS DISPCD-CB : 255 / 2026

LUJAN, 10 DE AGOSTO DE 2026

VISTO: El programa de la asignatura Seguridad Informática (11292) para la carrera Licenciatura en Sistemas de Información presentado por la División Computación; y

CONSIDERANDO:

Que la Comisión Plan de Estudio ha tomado intervención en el trámite.

Que se ha tratado y aprobado por el Consejo Directivo Departamental de Ciencias Básicas en su Sesión Ordinaria del día 6 de agosto de 2026.

Por ello,

EL CONSEJO DIRECTIVO DEPARTAMENTAL

DE CIENCIAS BÁSICAS

D I S P O N E :

ARTÍCULO 1°.- Aprobar el programa de la asignatura Seguridad Informática (11292) para la carrera Licenciatura en Sistemas de Información presentado por la División Computación que como anexo I forma parte de la presente Disposición.-

ARTICULO 2°.- Establecer que el mismo tendrá vigencia para los años 2026-2027.-

ARTÍCULO 3°.- Regístrese, comuníquese, cumplido, archívese.-

CP. Ángel S. BERTOGLIO - Secretario Académico - Departamento de Ciencias Básicas

Dr. Carlos J. DI SALVO - Director Decano - Departamento de Ciencias Básicas

DENOMINACIÓN DE LA ACTIVIDAD: 11292 – Seguridad Informática
TIPO DE ACTIVIDAD ACADÉMICA: Asignatura

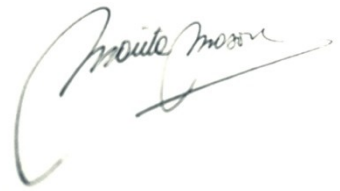
CARRERA: Licenciatura en Sistemas de Información
PLAN DE ESTUDIOS: 17:14

DOCENTE RESPONSABLE:
MASON María Rosana, Lic. en Sistemas de Información – Profesora Adjunta

OTROS DEPARTAMENTOS PARTICIPANTES DEL DICTADO:
EQUIPO DOCENTE:
CORSARO Alejandro, Ingeniero en Informática – Ayudante de 1ª
WAINERMAN Efraim, Lic. en Sistemas de Información - Jeje de Trabajos Prácticos

ACTIVIDADES CORRELATIVAS PRECEDENTES:
PARA CURSAR: 11260 – Sistemas de Información IV; 14029- Administración de Redes.
PARA APROBAR: 11260 – Sistemas de Información IV; 14029- Administración de Redes.

CARGA HORARIA TOTAL: HORAS SEMANALES: 4 (cuatro) - HORAS TOTALES 64 (sesenta y cuatro)
DISTRIBUCIÓN INTERNA DE LA CARGA HORARIA: 1 encuentro semanal de 4 horas
TEÓRICO: 44% - 28 hs.
PRÁCTICO: 44 % - 28 hs.
EVALUACIÓN: 12 % - 8 hs.



María Rosana Mason
Docente Responsable

PERÍODO DE VIGENCIA DEL PRESENTE PROGRAMA: 2026-2027

CONTENIDOS MÍNIMOS O DESCRIPTORES

Seguridad en los sistemas de información. Integridad, confidencialidad y disponibilidad. Políticas de seguridad de la información. Normativas. Estándares nacionales e internacionales. Análisis y gestión de riesgos. Gestión de incidentes de seguridad. Nociones de Auditoria y peritaje. Criptografía. Seguridad aplicada al desarrollo de software. Seguridad e higiene en el ámbito profesional informático.

FUNDAMENTACIÓN, OBJETIVOS, COMPETENCIAS

La utilización de redes de comunicaciones, en particular Internet, expone a las organizaciones a múltiples amenazas de seguridad de su información. Desde la pérdida de archivos hasta la denegación completa de un servicio, la cantidad de posibles debilidades es virtualmente infinita. Ya sea por fallas del software como por debilidades en la configuración, los sistemas pueden ser vulnerados y – por ende - requiere que el problema se aborde de manera global, concienzuda y metodológicamente. La gran cantidad de infraestructura y servicios interconectados, cada vez más distribuidas, plantea un importante desafío de como garantizar la seguridad informática, siendo la información uno de los activos más importantes que poseen las organizaciones.

La Seguridad Informática se ha convertido en uno de los atributos de calidad más importantes de los sistemas de software. Toda organización debe entonces contar con políticas para la correcta protección de su información. Esto incluye tanto buenas prácticas para el desarrollo de sistemas, la utilización de los mismos, así como la correcta implementación de los esquemas de recuperación ante incidentes. En algunos casos, la seguridad en la comunicación (por ejemplo, la confidencialidad) es un requerimiento por lo que hay que conocer los mecanismos que permiten lograr este tipo de servicio.

En todos los casos, la seguridad es un proceso que requiere el desarrollo de habilidades para la experimentación, como la identificación, manejo y control de herramientas de desarrollo de software, lenguajes de programación, herramientas especializadas para seguridad en redes, entre otras. Muchos de los fundamentos corresponden a modelos matemáticos (por ejemplo, la criptografía) y de redes (análisis de protocolos), como así también se involucran algunos aspectos relacionados con la ingeniería social, correspondiente al estudio del comportamiento de los usuarios de una red y cómo afectan la seguridad de la misma.

El profesional en Sistemas de Información debe contar con las competencias necesarias para poder llevar a cabo las actividades que son propias de la seguridad informática, sin omisión de los requisitos de seguridad e higiene necesarios en el ámbito profesional informático.

La materia está orientada a que el alumno pueda comenzar a desarrollar sus capacidades en los diferentes dominios de la Seguridad Informática, brindando un amplio abanico de conocimientos teóricos y prácticos. Se enfoca en que el alumno pueda comprender las diversas estándares, metodologías y funcionalidades para enfrentar las necesidades de las organizaciones en materia de seguridad informática, alineados con las mejores prácticas del mercado y posibilitando implementar sistemas de gestión de seguridad alineados con el contexto de riesgo de la organización y articulados para protegerse de riesgos emergentes.

Es primordial que los alumnos comprendan la importancia de prevenir y evitar los ataques informáticos y de la definición y puesta en marcha de planes de protección de todos los activos informáticos y sus correspondientes datos.

OBJETIVOS:

- Reconocer y valorar la importancia y complejidad que implica el concepto de seguridad de informática que genera y utiliza una organización.
- Implementar mecanismos de criptografía con el fin de proteger la información tanto almacenada como también en tránsito.
- Comprender el ámbito de utilización de los certificados y firmas digitales y cómo evaluar su uso e implementarlos.
- Analizar proactivamente posibles riesgos de seguridad en los sistemas de una organización y proponer soluciones.
- Definir e implementar políticas de seguridad basadas en metodologías y estándares.

- Adquirir los conocimientos necesarios para participar en proyectos de análisis, desarrollo e implementación de sistemas de información que contemplen la seguridad en su concepción, desarrollo, implementación, operación y retiro.
- Adquirir los conocimientos necesarios para incorporar requisitos fundamentales de seguridad e higiene en el ámbito profesional informático.
- Comprender el proceso de auditoría y las componentes claves que lo caracterizan.
- Desarrollar capacidades en la auditoría de gestión de seguridad Informática.
- Comprender los principios fundamentales de la informática forense.
- Conocer los protocolos, normas y guías de buenas prácticas, así como los fundamentos legales y procesales de la informática forense.
- Estudiar los diferentes procedimientos y metodologías en todo el ciclo de tratamiento de la evidencia digital.

CONTENIDOS

Unidad 1: Seguridad de la Información, conceptos básicos

Introducción a la Seguridad de la Información. Activos de información. Conceptos de integridad, confidencialidad, disponibilidad, autenticidad, control de acceso, no-repudio. Amenazas y su clasificación. Aumento de amenazas. Conceptos de vulnerabilidad, riesgo y daño. Objetivos de la seguridad de la información: prevención, detección, recuperación.

Unidad 2: Políticas - Normativa

Políticas y mecanismos de seguridad. Normativa vigente, leyes nacionales. Estándares nacionales e internacionales. Modelo de Política de Seguridad de la Información. Convenio de Confidencialidad. Ley 25.326 de Protección de los Datos Personales. Ley 25.506 de Firma Digital. Ley 26.388 de Delitos Informáticos. Serie de Normas ISO/IRAM 27.000. NIST Cybersecurity Framework. COBIT.

Unidad 3: Análisis y gestión de riesgos

Gestión de riesgos. Clasificación de activos de información. Identificación y análisis de riesgos. Tratamiento de los riesgos. Selección de controles y salvaguardas. Seguimiento y medición. Metodologías disponibles.

Unidad 4: Criptografía

Fundamentos. Esquemas simétricos y asimétricos. Aplicación en el software y redes de datos. Modelos clásicos de cifrado simétrico. Funciones de resumen o hash. Criptografía de clave pública. Infraestructura de Clave Pública. Gestión de claves. Firma electrónica y firma digital. Criptografía cuántica.

Unidad 5: Gestión de incidentes de seguridad - Seguridad de red

Concepto de incidente de seguridad. Gestión de incidentes de seguridad. Etapas de la gestión. Preparación y prevención. Detección y notificación. Análisis preliminar. Contención, erradicación y recupero. Investigación. Actividades posteriores.
Alertas y respuesta a incidentes de seguridad. Fuentes de alertas. Evaluación de alertas. Investigación de datos de red. Manejo de evidencia y atribución de ataques. Modelos de seguridad informática (Cyber Kill Chain. Mitre Att@ck) Respuesta ante incidentes.
Principios de la seguridad de red. Ataques a la red y a sus servicios. Defensa. Observación de la operación de red. Arquitectura de redes seguras. Protección de redes teleinformáticas. Hacking Ético - Análisis de Vulnerabilidades y Penetration Tests – Auditoría de redes LAN – Ejercitación con productos de Análisis de Vulnerabilidades.

Unidad 6: Auditoría y forensia

Trazabilidad y registros de auditoría. Paradigma actual, necesidad. Definición. Características, Independencia. Tipos, auditoría Informática. Auditoría interna. Auditoría externa. Consultoría. Funciones. Análisis de riesgos. Planificación. Evidencias. Pruebas de auditoría. Informes de auditoría. Control. Riesgos de auditoría. Metodologías. Herramientas. Interfaces de auditoría.

Recolección de evidencia en equipos y redes informáticas. Cadena de custodia. Proceso de análisis forense. Reportes.

Unidad 7: Seguridad en el desarrollo de software
Seguridad en el Ciclo de Vida de Desarrollo de Software. Modelo de Madurez para el Aseguramiento del Software. Requisitos de seguridad. Revisiones de diseño y de código. Vulnerabilidades y riesgos más comunes en el software y su mitigación. Pruebas de seguridad. Mejores prácticas de desarrollo y codificación. Administración de las vulnerabilidades y fortalecimiento del ambiente.

Unidad 8: Seguridad e higiene en el ámbito profesional informático.
Introducción a la higiene y seguridad laboral. Riesgos de seguridad física. Fuego. Energía eléctrica y medioambiente. Buenas prácticas en teletrabajo.

METODOLOGÍA DE ENSEÑANZA:
La actividad académica se desarrolla en la modalidad teórico-práctica. La interacción entre el equipo docente y quienes cursen la actividad académica se desarrollará de manera sincrónica, garantizando encuentros que cubran la totalidad de la carga horaria semanal mediante esta modalidad. Las actividades sincrónicas se desarrollaran en las aulas sedes de la universidad (50% de las clases) y mediatizadas a través de sistemas de videoconferencias (50%). Se desarrollan los conceptos teóricos y se trabaja mediante actividades prácticas para que los estudiantes logren el desarrollo de competencias. Los fundamentos y modelos teóricos son luego ejemplificados y demostrados en las implementaciones tecnológicas (cuando esto sea posible). En las actividades prácticas se resuelven ejercicios y casos respecto de conceptos teóricos.
Por otra parte, se pondrán a disposición de los estudiantes videos con la grabación de las clases teóricas y la resolución de trabajos prácticos, los que podrán consultar y acceder de manera asincrónica. Las consultas se atenderán tanto por correo electrónico como mediante un foro habilitado en el Aula virtual como en el aula una vez finalizada la clase.
Así mismo, se pondrá a disposición de los estudiantes y del equipo de trabajo un plan de trabajo y cronograma que describa el desarrollo de las distintas actividades de enseñanza, las consignas de aprendizaje, las mediaciones a utilizar y los instrumentos de evaluación.

TRABAJOS PRÁCTICOS
El equipo docente ha desarrollado un conjunto de actividades prácticas, con las que se va trabajando durante el desarrollo de la actividad académica. Estas actividades permiten llevar a la práctica los conocimientos que se van poniendo en juego buscando el desarrollo de competencias para la aplocación de los mismos en casos del mundo real.
Sobre el final del curso, se llevan a cabo prácticos integrados que permiten ver la interrelación de los distintos mecanismos de seguridad en el desarrollo de software. La cantidad de trabajos prácticos será de 8, uno por cada unidad del programa.

REQUISITOS DE APROBACION Y CRITERIOS DE CALIFICACIÓN:

CONDICIONES PARA PROMOVER (SIN EL REQUISITO DE EXAMEN FINAL)
DE ACUERDO AL ART.23 DEL RÉGIMEN GENERAL DE ESTUDIOS RESHCS 261-21 y su ANEXO PARA CARRERAS CON MODALIDAD PEDAGÓGICA A DISTANCIA

a) Tener aprobadas las actividades correlativas al finalizar el turno de examen extraordinario de ese cuatrimestre.
b) Cumplir con un mínimo del 75 % de asistencia para las actividades.
c) Aprobar el 100% de las evaluaciones previstas en este programa, con un promedio no inferior a seis (6) puntos sin recuperar ninguna.
d) Aprobar la evaluación integradora con calificación no inferior a siete (7) puntos.

CONDICIONES PARA APROBAR COMO REGULAR (CON REQUISITO DE EXAMEN FINAL)

DE ACUERDO AL ART.24 DEL RÉGIMEN GENERAL DE ESTUDIOS RESHCS 261-21 y su ANEXO PARA CARRERAS CON MODALIDAD PEDAGÓGICA A DISTANCIA

a) Estar en condición de regular en las actividades correlativas al momento de su inscripción al cursado de la asignatura.
b) Cumplir con un mínimo del 50 % de asistencia para las actividades prácticas.
c) Aprobar el 100% de las evaluaciones previstas en este programa, con un promedio no inferior a cuatro (4) puntos, pudiendo recuperar el 50% de las mismas. Cada evaluación solo podrá recuperarse en una oportunidad.

EXAMENES PARA ESTUDIANTES EN CONDICIÓN DE LIBRES

1) Para aquellos estudiantes que, habiéndose inscriptos oportunamente en la presente actividad hayan quedado en condición de libres por aplicación de los artículos 22, 25, 27, 29 o 32 del Régimen General de Estudios, SI podrán rendir en tal condición la presente actividad. Las características del examen libre son las siguientes: Sera un único examen (Teórico / Práctico) en el día, horario y llamado publicado.

BIBLIOGRAFÍA

OBLIGATORIA:

1. Apuntes de la asignatura Seguridad Informática. Material de estudio preparado por el equipo docente de la asignatura.
2. Leyes nacionales y Normas IRAM:
Ley 25.326 de Protección de los Datos Personales.
Ley 25.506 de Firma Digital.
Ley 26.388 de Delitos Informáticos.
Ley 19587 de Higiene y Seguridad en el Trabajo.
Ley 24557 de Riesgos del trabajo.
Ley 26773 reforma LRT.
Ley 27348 complementaria a la LRT.
Norma IRAM-ISO/IEC 27001, TI. Técnicas de seguridad. Sistema de gestión de seguridad de la Información, (2013), Cor 1:2014, Cor 2: 2015. Seguridad de la Información, Ciberseguridad y Protección de la Privacidad. Modificaciones 2018 y 2021. Rev. 2022.
Norma IRAM-ISO/IEC 27002, TI. Técnicas de seguridad. Código de Buenas Prácticas Controles de Seguridad de la Información, Seguridad de la Información, Ciberseguridad y Protección de la Privacidad. (2021). Rev. 2022.
Norma ISO/IEC 27000, Sistemas de Gestión de Seguridad de la Información, 5ta ed., (2018).
Modelo de Política de Seguridad de la Información. Disposición 1/2022. Modelo referencial de Política de Seguridad de la Información. DA 641/2021 JGM. Requisitos mínimos de Seguridad de la Información para Organismos. Resolución 1669/2022 CIN. Políticas de Seguridad de la Información. Guía de instrucciones.
BCRA COMUNICACIÓN "A" 7319 Requisitos mínimos de gestión, implementación y control de los riesgos relacionados con tecnología informática. https://www.bcra.gob.ar/pdfs/comytexord/A7319.pdf
3. STALLINGS, William. "Cryptography and Network Security Principles and Practices", 4ta ed., Editorial Prentice Hall (2005).
4. Cryptography: An Introduction (3rd Edition) Nigel Smart https://nigelsmart.github.io/Crypto_Book/
"3.0.1.4 10th April 2013 Minor correction in one of the attacks on RSA with a shared modulus."
5. PROSISE, Chis – MANDIA, Kevin. "Incident Response and Computer Forensics", 2da ed., Editorial McGraw-Hill (2003).
6. CHANDRA, Pravir. "Software Assurance Maturity Model (SAMM)"
7. The Open Web Application Security Project (2009).
8. WOOD, Charles Cresson, CISA, CISSP. "Information Security Policies Made Easy", 10th ed., Editorial Information Shield (2005).
9. PACHECO, Federico. "Criptografía", 1a ed., Cuidad Autónoma de Buenos Aires. Dalaga (2014).

COMPLEMENTARIA:

1. MENEZES, Alfred J., VAN OORSCHOT, Paul C., VANSTONE, Scott A. "Handbook of Applied Cryptography, CRC Press (2001).
   1996: https://cacr.uwaterloo.ca/hac/
   https://www.cs.umd.edu/~waa/414-F11/IntroToCrypto.pdf
2. MAGERIT versión 2. "Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información", Ministerio de Administraciones Públicas de España, (2006).
3. Guía para la Construcción de Aplicaciones y Servicios Web Seguros, The Open Web Application Security Project (OWASP), Free Software Foundation, 2005.
4. REVISTA (IN)SECURE MAGAZINE, HNS Consulting, 2005-2012.
5. Convenio Colectivo de Trabajo Sectorial del Personal del Sistema Nacional de Empleo Público (SINEP), homologado por Decreto 2098/2008.
6. eBooks
   a. Seguridad por Niveles, de Alejandro Corletti Estrada
   b. El arte de la intrusión, Kevin Mitnick
   c. La Ética de los Hackers, Pekka Himanen
7. Guidelines for digital forensics first responders. INTERPOL Digital 2021
8. Marco para la mejora de la seguridad cibernética en infraestructuras críticas
https://doi.org/10.6028/NIST.CSWP.04162018es
9. Security and Privacy Controls for Information Systems and Organizations https://doi.org/10.6028/NIST.SP.800-53r5
10. An Introduction to Information Security https://doi.org/10.6028/NIST.SP.800-12r1

DISPOSICIÓN DE APROBACIÓN: CD[A COMPLETAR POR EL DEPARTAMENTO]

Hoja de firmas

Sistema: sudocu
Fecha: 10/08/2026 09:12:50
Cargado por: BIBIANA LANNUTTI

Sistema: sudocu
Fecha: 10/08/2026 12:29:40
Autorizado por: ANGEL SEBASTIAN BERTOGLIO VIDAL

Sistema: sudocu
Fecha: 10/08/2026 15:59:36
Autorizado por: CARLOS JAVIER DI SALVO