Seguridad en los Sistemas de Información
Planificación Ciclo lectivo 2026

1. Datos administrativos de la asignatura

Departamento:	Sistemas de Información	Carrera	Ing. en Sistemas de Información
Asignatura:	**Seguridad en los Sistemas de Información**		
Nivel de la carrera	5to Año	Duración	Cuatrimestral
Plan	2023 Ord. 1877	Modalidad	Presencial
Bloque Curricular:	Tecnologías Aplicadas		
Área	Gestión Ingenieril	RTF	6
Horas cátedra semanal:	3	Horas reloj anual total:	72
Carga horaria no presencial semanal	----------	% horas no presenciales	----------
Profesor/es Titular/Asociado/Adjunto:		Dedicación:	Exclusiva
Auxiliar/es de 1°/JTP		Dedicación:	Simple
Competencias	Específicas	Genéricas	
	CE1.1 – CE2.1 – CE3.1 - CE4.1 – CE5.1 – CE7.1	CG3 – CG6 – CG7 – CG8 - CG10	

2. Presentación, Fundamentación

La asignatura Seguridad en los Sistemas de Información tiene como objetivo la formación del estudiante para la toma de decisiones y la gestión de los aspectos de seguridad en lo normativo, riesgos, continuidad en el negocio y el proceso de auditoria según necesidades.

La seguridad de la información ha tomado un papel altamente relevante ante la ubicuidad de internet. Los datos personales y privados de los ciudadanos son almacenados y resguardados por sistemas de información de distintas organizaciones, como empresas industriales, comerciales, de servicios, instituciones gubernamentales, etc.

Relación de la asignatura con el perfil de egreso.

La Seguridad en los sistemas de información aporta al Ingeniero en Sistemas de Información las metodologías y herramientas necesarias para identificar problemas y oportunidades en el entorno en el que se desenvuelva, actuando de manera responsable y logrando un equilibrio entre la protección de estos recursos y la satisfacción de las necesidades básicas de la población.

Relación de la asignatura con los alcances del título.

La asignatura responde a las actividades reservadas de la carrera haciendo un fuerte aporte a proyectar y dirigir lo referido a seguridad informática

3. Relación de la asignatura con las competencias de egreso de la carrera

Se detalla en la siguiente tabla, la relación de la asignatura con las competencias de egreso específicas, genéricas tecnológicas, sociales, políticas y actitudinales de la carrera. Indicando a cuáles competencias de egreso tributa y en qué nivel (No Tributa, 1=bajo, 2=medio, 3=alto).

Competencias	Nivel
Competencias genéricas tecnológicas (CG):	
CG. 1. Identificar, formular y resolver problemas de ingeniería.,	No Tributa
CG. 2. Concebir, diseñar y desarrollar proyectos de ingeniería.	No Tributa
CG. 3. Gestionar, planificar, ejecutar y controlar proyectos de ingeniería.	3
CG. 4. Utilizar de manera efectiva las técnicas y herramientas de aplicación en la ingeniería.	No Tributa
CG. 5. Contribuir a la generación de desarrollos tecnológicos y/o innovaciones tecnológicas.	No Tributa

Competencias Genéricas Sociales Políticas y Actitudinales (CG):	
CG. 6. Desempeñarse de manera efectiva en equipos de trabajo.	2
CG. 7. Comunicarse con efectividad	2
CG. 8. Actuar con ética, responsabilidad profesional y compromiso social, considerando el impacto económico, social y ambiental de su actividad en el contexto local y global.	3
CG. 9. Aprender en forma continua y autónoma.	No Tributa
CG. 10. Actuar con espíritu emprendedor	1
Competencias Específicas (CE):	
CE. 1.1. Especificar, proyectar y desarrollar sistemas de información para concebir soluciones tecnológicas que permitan resolver situaciones en las organizaciones mediante el empleo de metodologías de sistemas y tecnologías asociadas a los sistemas de información	3
CE. 1.2. Especificar, proyectar y desarrollar sistemas de comunicación de datos, evaluando posibles soluciones tecnológicas disponibles para dar soporte a los sistemas de información en lo referido al procesamiento y comunicación de datos.	No Tributa
CE. 1.3. Especificar, proyectar y desarrollar software para la elaboración de soluciones informáticas con el propósito de resolver problemas estratégicos y operativos, así como de servicios y de negocios, en el marco de una actividad económica que sea social y ambientalmente sustentable.	No Tributa
CE. 2.1. Proyectar y dirigir lo referido a seguridad informática para seleccionar y aplicar técnicas, herramientas, métodos y normas, garantizando la seguridad y privacidad de la información procesada y generada por los sistemas de información.	3
CE. 3.1. Establecer métricas y normas de calidad de software para medir, evaluar, controlar y monitorear el rendimiento, impulsando mejoras de acuerdo a técnicas y normas vigentes definidas por los organismos de estandarización.	3
CE. 4.1. Certificar el funcionamiento, condición de uso o estado de sistemas de información, sistemas de comunicación de datos, software, seguridad informática y calidad de software para asegurar la generación de los resultados deseados en función de restricciones de tiempo y recursos establecidos.	3
CE. 5.1. Dirigir y controlar la implementación, operación y mantenimiento de sistemas de información, sistemas de comunicación de datos, software, seguridad informática y calidad de software, a los fines de alcanzar los objetivos fijados por la organización.	3

CE. 6.1. Asesorar y capacitar a organizaciones, empresas, organismos públicos o privados en la adquisición, instalación y uso, en lo que respecta a sistemas de información, sistemas de comunicación de datos, software, seguridad informática y calidad de software, a los fines de un uso correcto de los sistemas intervinientes.	No Tributa
CE. 7.1. Realizar pericias, tasaciones y arbitrajes relacionados con su actividad profesional, respetando marcos normativos y jurídicos con el objeto de asesorar a las partes o a los tribunales de Justicia.	3

4. Propósito

Brindar al estudiante herramientas para la gestión de los aspectos de seguridad en los sistemas de información en referencia a lo normativo, al riesgos, a la continuidad en el negocio y el proceso de auditoría.

5. Objetivos establecidos en el Diseño Curricular

- Aplicar modelos de referencia en la gestión de la seguridad de la información según las normativas vigentes.
- Planificar controles de seguridad basados en la gestión de riesgo.
- Desarrollar un plan de seguridad asegurando la continuidad del negocio.
- Comprender el proceso de auditoría y tratamiento de evidencias

6. Contenidos Mínimos establecidos en el Diseño Curricular

- Seguridad de la Información.
- Marco Normativo.
- Gestión de Riesgos.
- Sistemas de gestión de seguridad.
- Auditoría de Sistemas de Información.
- Peritaje informático forense

7. Resultados de aprendizaje

Se describen los Resultados de aprendizaje (RA) a promover en el desarrollo de la asignatura.

Identificador del RA	Redacción
RA1	[Distingue] [los componentes propios de la seguridad de la información] para [su abordaje y gestión según los casos de estudio], en contextos profesionales reales e hipotéticos.
RA2	[Evalúa] [los riesgos de un sistema de información] para [identificar potenciales vulnerabilidades en el contexto de un caso real o hipotético.]
RA3	[Desarrolla] [un Plan de Gestión de la Seguridad de la información según las normas vigentes y buenas prácticas], para [lograr los resultados previstos en diferentes casos de estudio.]

RA4	[Interpreta] [la Auditoría de Seguridad] para [detectar que se cumplan las normativas y/o buenas prácticas en casos de estudio de la vida real o escenarios posibles].
RA5	[Experimenta] [el peritaje de Sistema de Información] para [identificar los aspectos éticos de la profesión a través de una situación que simula la realidad]

8. Asignaturas correlativas previas

Para cursar debe tener cursada:

- Redes de Datos
- Administración de Sistemas de Información

Para cursar debe tener aprobada:

- Desarrollo de Software
- Comunicación de Datos

9. Asignaturas correlativas posteriores

-

10. Programa analítico, Contenidos temáticos

Ejes temáticos	Contenidos
Seguridad de la información	Seguridad de la Información: Conceptos, herramientas, tecnologías, metodologías. Marco Normativo. Estrategia de la Seguridad de SI/TI Compromiso de la Gerencia Roles y Responsabilidades Cuestiones Legales y Reglamentarias Requisitos para el contenido y preservación de registros del negocio y su cumplimiento Políticas de seguridad de SI/TI Glosario
Gestión de Riesgos	Proceso de Administración de riesgos Métodos de Identificación y Análisis de Riesgos Identificación de los activos de una organización Mitigando el Riesgo Plan de Contingencia Marco Normativo Herramientas e indicadores Glosario
Sistemas de Gestión de Seguridad de la Información	Políticas de seguridad de SI Procesos de negocio Roles y Funciones Documentación (procedimientos e instructivos) Estándares Uso de Métricas para medir, monitorear e informar Indicadores de Seguridad. Proveedores Tercerizados Evaluaciones de Vulnerabilidades Cultura, Comportamiento y Educación del usuario y Conciencia de Seguridad de SI/TI Gestión de seguridad en nuevas tecnologías.
Auditoría y Peritaje	Auditoría: Concepto, Plan de auditoría, Criterios de auditoría, tipos de auditorías, Objetivo alcance, tipos de auditor, Hallazgos, evidencias. Perito informático: Deberes, Deontología y ética profesional, tipos de peritajes informáticos, requisitos, informes. Informática forense: fases del análisis forense, evidencias, metodologías.

Cuadro de Carga Horaria de Formación Práctica

Tipo de Formación Práctica	Carga horaria	
	Presencial	A Distancia
Instancias supervisadas de formación práctica (prácticas en diferentes ámbitos tales como aula, laboratorios, campo u otros)	32	
Proyecto Integrador		
Práctica profesional supervisada		
Carga horaria total	32	

11. Metodología de enseñanza

La metodología de enseñanza está focalizada principalmente en el análisis de casos y la resolución de problemas. Se presentará en las clases una serie de casos de estudio, reales o simulados, en los que quien estudia, conformando grupos de trabajos, analizará y utilizará diferentes procedimientos para la solución de los problemas planteados.

Otra estrategia, que se propone, es el Aprendizaje Basado en Investigación. Se busca promover la autogestión y el aprendizaje colaborativo. El estudiante investigará sobre diferentes temas de seguridad reales y de actualidad. Deberá seleccionar y construir glosarios para luego de manera colaborativa, integrar y organizar en mapas conceptuales e informes. Se utilizarán recursos disponibles del aula virtual como método de comunicación asíncrono y aplicaciones de mensajería instantánea para un intercambio de ideas y opiniones más fluidos con quien estudia.

Resumen de Competencias - Resultados de Aprendizaje - Metodologías de Enseñanza de la asignatura.

COMPETENCIA - NIVEL DE TRIBUTACIÓN	RESULTADO DE APRENDIZAJE (RA)
CE1.1(3) – CE2.1(3) – CE3.1(3) - CE4.1(3) – CE5.1(3) – CE7.1(3) - CG3(3) – CG62() – CG7(2) – CG8(3) - CG10(1)	RA1 - RA2 - RA3- RA4 - RA5

EJES TEMÁTICOS - CONTENIDOS

Seguridad de la información - Gestión de Riesgos - Sistemas de Gestión de Seguridad de la Información - Auditoría y Peritaje

ACTIVIDADES DEL ESTUDIANTE (FORMATIVAS)

El **estudiante** deberá realizar las siguientes actividades para alcanzar los **RA** propuestos:

- Lectura y análisis de material bibliográfico, diapositivas y videos.
- Participar activamente en clase.
- Resolver Casos de Estudios.
- Interpretar y debatir resultados obtenidos.
- Utilizar software de modelado como herramienta para la validación.
- Realizar el Trabajo Práctico Final
- Realizar Instancia de Evaluación de integración de saberes.
- Elaborar una exposición oral para presentar el TPI.

ESTRATEGIAS DE ENSEÑANZA

El **docente** diseñará las siguientes **actividades pedagógicas**:

- Clase expositiva dialogada
- Acompañamiento continuo.
- Diseño de casos de estudios
- Diseñar el Trabajo Práctico Final.
- Diseñar Instancia de evaluación individual de integración de saberes.
- Diseñar instrumentos de evaluación del TPF
- Retroalimentación formativa.
- Coordinación de trabajo colaborativo.

12. Recomendaciones para el estudio

- Antes de cada clase se recomienda al estudiante, realizar lectura y búsqueda de información sobre el tema que se abordará.
- Durante la clase es recomendable y necesario que participe de las actividades propuestas.

- Después de la clase se recomienda realizar resúmenes de los temas.

13. Metodología de evaluación

Los métodos de evaluación serán diversos, realizando un monitoreo de las actividades propuestas a los estudiantes fuera del aula, y analizando la participación en ejercicios durante las clases.
También se utilizarán recursos interactivos en tiempo real con incentivos reales sobre los efectos de la evaluación individual del estudiante, generando así una doble recompensa de efecto directo de su condición evaluativa y una a largo plazo de conocimiento aplicado, basado en actividades recreativas y de realización grupal.

Finalmente se realizarán tres evaluaciones parciales y directas de contenidos que permitan tener revisiones periódicas de las competencias esperadas.

Evaluación de cada resultado de aprendizaje
Para las actividades propuestas dentro y fuera del contexto del aula se evaluará el desarrollo y la participación activa en las mismas, sirviendo como un sensor general y sensor del desarrollo de las competencias en el estudiante. No se tomará en cuenta para esta etapa evaluativa el nivel y la calidad de lo realizado, si no el interés y la involucración en la asignatura.
Las actividades de tiempo real grupales tendrán una retroalimentación inmediata de los resultados y serán claros en los efectos evaluativos del alumno.
Las 8 evaluaciones parciales serán revisadas por el equipo docente y se hará una devolución numérica y retroalimentación de los contenidos que el estudiante desarrolle.
Condiciones de aprobación
- Asistencia del 75%
- Desarrollo de las actividades propuestas extra-áulicas.
- Desarrollo de las actividades propuestas en el aula.
- Realización de al menos el 80% de los cuestionarios de evaluación.
- Participación de las actividades en tiempo real y grupales.
- La nota se obtendrá en base a los cuestionarios realizados en clase y los trabajos grupales integradores que asignen créditos.
- Obtener nota mayor a seis.

Se considera en condición de ALUMNO REGULAR a quien cumpla las condiciones del punto anterior, u obtenga nota mayor a seis en la evaluación integradora final.
Se considera en condición de APROBACIÓN DIRECTA a quienes obtengan una nota mayor a

ocho y cumplan además las condiciones de ALUMNO REGULAR, u obtenga nota mayor a ocho en la evaluación integradora final y cumpla con las condiciones de asistencia.

Aquellos estudiantes que no cumplan las condiciones anteriores se consideran en condición de LIBRES, debiendo recursar la asignatura.

14. Cronograma de clases año 2026

Semana / Fecha	Contenido / Actividad
Semana 1	Definiciones (Confidencialidad, Integridad, Disponibilidad). Diferencia entre Seguridad Informática y de la Información.
Semana 2	Marco Normativo en Argentina (I). Ley 25.326 de Protección de Datos Personales. El rol de la Agencia de Acceso a la Información Pública (AAIP).
Semana 3	Marco Normativo en Argentina (II). Ley 26.388 de Delitos Informáticos y Ley 25.506 de Firma Digital. Estándares locales (Disposiciones de la ONTI para administración pública).
Semana 4	Introducción al Peritaje Informático. El rol del perito en la justicia argentina. Cadena de custodia y preservación de la prueba digital.
Semana 5	Adquisición de datos (discos, memoria RAM). Herramientas de análisis (Autopsy, FTK Imager, Volatility).
Semana 6	El Informe Pericial. Redacción de puntos de pericia y presentación ante juzgados. Ética profesional.
Semana 7	Seguridad en el Ciclo de Vida del Software. DevSecOps y seguridad por diseño. Controles técnicos fundamentales (Cifrado, Autenticación).
Semana 8	Auditoría de Sistemas de Información (I). Conceptos, objetivos y tipos de auditoría. Perfil del auditor. Marcos de referencia (COBIT/NIST).
Semana 9	Auditoría de Sistemas (II). Ejecución de la auditoría: recolección de evidencia, pruebas de cumplimiento y sustantivas. Informe de auditoría.
Semana 10	Seguridad en Redes y Cloud. Amenazas modernas y arquitecturas Zero Trust. El framework de ciberseguridad del NIST.
Semana 11	Gestión de Riesgos (Metodología). Identificación de activos, amenazas y vulnerabilidades. El proceso según IRAM-ISO/IEC 31000.
Semana 12	Análisis Cualitativo y Cuantitativo. Evaluación del impacto y probabilidad. Selección de estrategias de tratamiento del riesgo.
Semana 13	Sistemas de Gestión de Seguridad (SGSI). Introducción a la familia ISO/IEC 27000. Estructura de la norma IRAM-ISO/IEC 27001:2022.
Semana 14	Controles de Seguridad. Implementación de controles basados en el Anexo A de la ISO 27001. Políticas, organización y seguridad de RRHH.
Semana 15	Plan de Continuidad del Negocio (BCP). Gestión de incidentes y recuperación ante desastres (DRP).
Semana 16	Repaso General y Examen Final/Presentación de Proyecto.

15. Recursos necesarios

- Contar con un aula en la que se disponga de mesas de trabajo que se orienten al trabajo en equipo en donde los participantes puedan desarrollar sus actividades de los talleres. Facilitan la comunicación entre ellos fundamentalmente pero también con el cuerpo docente.
- Disponer de una muy buena conexión a Internet.
- Estudiantes provistos de notebooks o teléfonos móviles.
- Utilización de proyector.

16. Referencias bibliográficas (citadas según Normas APA)

Bibliografía Obligatoria

- InfoLeg Portal de Información Legislativa. Leyes 25.326, 26.388 y 25.506. https://www.infoleg.gob.ar/
- NIST (28 de noviembre de 2022). “COMPUTER SECURITY RESOURCE CENTER”. https://csrc.nist.gov/.
- Alvaro Gomez Vieites (2011). Enciclopedia de la Seguridad Informática. Alfaomega.
- IRAM-ISO/IEC. (2022). ISO/IEC 27001. https://www.iso.org
- IRAM-ISO/IEC 31000. https://www.iso.org
- Diseño y Gestión de un Sistema de Seguridad de Información: Optica ISO 27001:2005. Alfaomega. 2007 1a ed.

17. Función Docencia

- Dictado de las clases
- Elaboración de plan de trabajos de situaciones prácticas
- Disponibilidad en tiempo y forma de recursos materiales (infraestructura y equipamiento).
- Actualización de material bibliográfico
- Aprobación de instrumentos de evaluación.
- Dictado de las clases colaborativas en resolución de problemas.

18. Reuniones de asignatura y área

Reuniones periódicas de asignatura y se prevén dos reuniones de área en el año.

19. Atención y orientación a las y los estudiantes

Las clases de consultas se coordinan con los estudiantes según sus necesidades.

Se enfatiza el uso de los recursos de comunicación asincrónica y sincrónica que proporciona la plataforma virtual (Moodle).

Se planifican encuentros individuales o grupales por medio de videoconferencia por las diversas plataformas y/o presenciales.