UNIVERSIDAD NACIONAL DE SANTIAGO DEL ESTERO

FACULTAD DE CIENCIAS EXACTAS Y TECNOLOGÍAS

PLANIFICACIÓN ANUAL 2024

ASIGNATURA: CRIPTOGRAFÍA

LICENCIATURA EN SISTEMAS DE INFORMACIÓN
Plan de Estudio: 2011
(Innovación curricular 2022)

Equipo cátedra:
Profesora Titular: Costaguta Rosanna

PLANIFICACIÓN DE LA ASIGNATURA

1- IDENTIFICACIÓN:

1.1- Nombre de Asignatura: CRIPTOGRAFÍA (Optativa I)

1.2- Carrera/s: Licenciatura en Sistemas de Información

1.3- Plan de Estudios: 2011

1.4- Año académico: 2024

1.5- Carácter: (*Obligatoria/Optativa/Electiva):* Optativa

1.6- Ubicación de la Asignatura en el Plan de Estudios

1.6.1- Módulo – Año: 5to.año (noveno cuatrimestre)

1.6.2- Trayecto al que pertenece la Asignatura/Obligación Curricular

TRAYECTO	CARGA HORARIA PRESENCIAL
Ciencias Básicas y Específicas	
Algoritmos y Lenguajes	
Arquitectura, Sistemas Operativos y Redes	
Ingeniería de Software, Bases de Datos y Sistemas de Información	
Aspectos Sociales y Profesionales	
Otros contenidos	60
CARGA HORARIA TOTAL DE LA ACTIVIDAD CURRICULAR	60

Tabla 1: Carga horaria por trayecto

1.6.3-Correlativas

1.6.3.1 Anteriores: Simulación, Redes II e Ingeniería de Software (Regularizadas) - Sistemas de información II (Aprobada).

1.6.3.2. Posteriores: Optativa II.

1.7- Carga horaria:

1.7.1. **Carga horaria semanal total:** 4 horas

1.7.2. Carga horaria semanal destinada a la formación práctica: 2 horas

1.7.3. Carga horaria total dedicada a las distintas actividades de formación práctica: 30 horas

1.8. Ámbitos donde se desarrollan las actividades de formación práctica a las que se hace referencia en el punto anterior

Laboratorios de Informática del Departamento Académico de Informática de la FCEYT.

1.9. Indique la cantidad de comisiones en las que se dicta la asignatura: una

2- PRESENTACIÓN

2.1- Ubicación de la Asignatura como tramo de conocimiento de una disciplina

Esta asignatura corresponde al Segundo Ciclo de la carrera, dentro de un conjunto de asignaturas optativas, que tienen en general el objetivo de complementar la formación del egresado. En particular, esta asignatura está orientada principalmente a brindar a los alumnos fundamentos de la Criptografía, así como conocimientos sobre técnicas y metodologías propios de la disciplina que les permitan comprender los métodos de encriptado, programarlos y utilizarlos en los sistemas de información, así como también adquirir competencias para diseñar y programar nuevos algoritmos de encriptamiento.

2.2- Conocimientos y habilidades previas que permiten encarar el aprendizaje de la Asignatura.

Para el estudiante que cursa la asignatura se requieren conceptos previos adquiridos en las asignaturas Sistemas de información II, Simulación, Redes II e Ingeniería de Software. Contar con estos conocimientos previos permitirá al estudiante realizar una adecuada complementación con los que adquirirá en la cátedra, a fin de poder comprender, diseñar y programar algoritmos existentes y propios de la Criptografía en sistemas de información. Se espera además que los alumnos que ingresen a la cursada posean sentido de responsabilidad por el propio comportamiento, y cuenten con habilidades desarrolladas tanto respecto a un trabajo productivo en equipo como a un trabajo eficaz individual.

Dado que el contexto de post-pandemia nos permite retomar las actividades presenciales, y que a la vez disponemos de los medios tecnológicos necesarios para desarrollar las actividades de enseñanza y de aprendizaje soportadas adecuadamente por material disponible en el aula virtual, se espera que los estudiantes cuenten con el nivel de desarrollo adecuado de sus competencias digitales para sacar el máximo beneficio de las actividades que se lleven a cabo.

2.3- Aspectos del Perfil Profesional del Egresado a los que contribuye la asignatura

La asignatura brinda a los estudiantes:

- Profundos conocimientos sobre técnicas propias de la Criptografía, que le servirán para el diseño y programación de algoritmos específicos de la disciplina que den solución a problemas de seguridad de los datos.
- Práctica en la integración de técnicas y metodologías de la Criptografía con otras provenientes del área de los sistemas de información.
- Formación en pensamiento reflexivo.
- Ejercicio de una actitud crítica frente a su propio quehacer.
- Práctica en la manifestación de una actitud creativa en la búsqueda de respuestas originales a problemas específicos mediante la aplicación de técnicas y metodologías propias de la disciplina.

2.4- Integración horizontal y vertical con otras asignaturas.

Por ser asignatura del quinto y último año de la carrera, y tal como se explicitó en la sección 1.6.3., Criptografía (Optativa I) se integra verticalmente con las asignaturas: Sistemas de Información II, Simulación, Redes II, Ingeniería de Software y Optativa II. La integración horizontal se da con la asignatura Metodología de la Investigación I por cuanto podrán incluir temáticas de la asignatura en la formulación de sus trabajos finales de graduación. También se observa integración horizontal

con la asignatura Ingeniería Web por cuanto los estudiantes comprenderán y desarrollarán tópicos vinculados con los criterios de calidad web (específicamente criterios de seguridad).

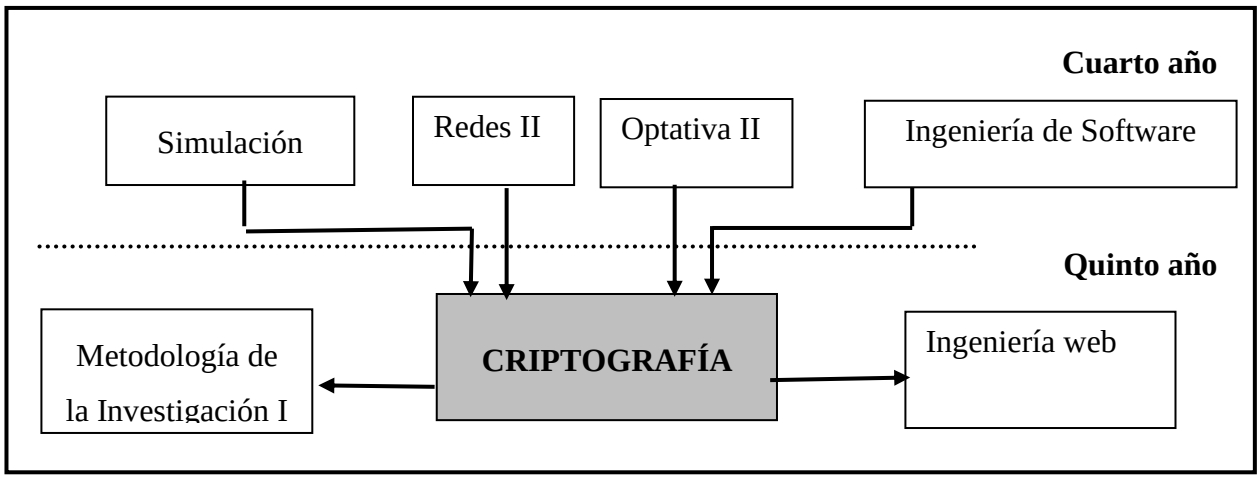

Figura 2. *Articulación horizontal y vertical de la asignatura*

3- OBJETIVOS

- Que el estudiante desarrolle las siguientes competencias básicas:
  - Representación de la Información
  - Lectura analítico-crítica
  - Resolución de Problemas

- Que el estudiante desarrolle las siguientes competencias específicas:
  - Reconocer el tipo de problemas que pueden ser estudiados con técnicas de Criptografía
  - Aplicar diferentes métodos de encriptamiento de información
  - Desarrollar destrezas interpretativas, tanto visuales como analíticas
  - Comprender y valorar los avances logrados en el campo de la Criptografía y su contribución a otras ramas de conocimiento

- Que el estudiante desarrolle las siguientes competencias digitales:
  - Buscar y seleccionar información relevante.
  - Comunicar sus ideas en diferentes formatos.
  - Utilizar adecuadamente distintas herramientas de la web 2.0.
  - Argumentar, negociar y consensuar posiciones en foros digitales.

- Que el estudiante desarrolle las siguientes competencias transversales:
  - Aplicar principios y generalizaciones ya aprendidas a la resolución de nuevos problemas y situaciones
  - Hacer inferencias razonables a partir de observaciones
  - Sintetizar e integrar informaciones e ideas
  - Pensar holísticamente (atendiendo tanto al todo como a las partes)
  - Organizar eficazmente su trabajo
  - Trabajar productivamente con otros
  - Desarrollar una actitud de apertura hacia nuevas ideas, una estima duradera por el aprendizaje, una comprensión informada de la ciencia y la tecnología, un sentido de

responsabilidad por el propio comportamiento, el respeto por el otro, y un compromiso por la honestidad

4- SELECCIÓN Y ORGANIZACIÓN DE CONTENIDOS

4.1- Contenidos mínimos establecidos en el Plan de Estudios para la Asignatura:

Criptografía: Definición y términos asociados. Necesidad de encriptar la información. Estructura de un criptosistema. Métodos clásicos de encriptación: Sustitución monoalfabética, Sustitución polialfabética, Transposición. Criptosistemas contemporáneos: Cifrados simétricos y asimétricos. Métodos de ataque conocidos. Autenticación de mensajes y autenticación de transmisores: conceptos y diferencias. Esquemas de autenticación. Criptografía en redes y bases de datos.

4.2- Programa Sintético sobre la base de los contenidos mínimos

UNIDAD 1: Fundamentos de la Criptografía

Definiciones. Términos asociados. Reseña histórica.

UNIDAD 2: Criptografía Clásica

Métodos clásicos de encriptación: por sustitución y por trasposición.

UNIDAD 3: Criptografía Moderna

Cifrados simétricos y asimétricos. Métodos de ataque conocidos.

UNIDAD 4: Métodos de autenticación

Autenticación de mensajes y autenticación de transmisores.

4.3- Articulación Temática de la Asignatura

La articulación temática de la asignatura se muestra en la Figura 3.

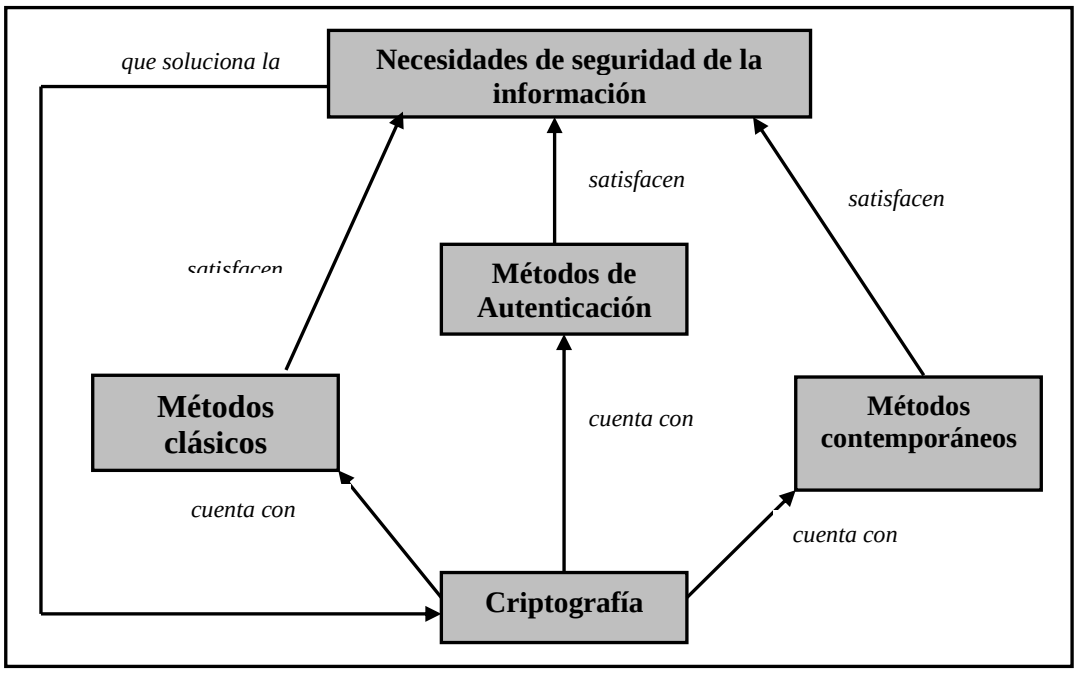

Figura 3. *Articulación temática de la asignatura*

4.4- Programa Analítico

UNIDAD 1: Fundamentos de la Criptografía
Criptografía: Etimología de la palabra. Definiciones. Términos asociados. Reseña histórica. Necesidad de encriptar la información. Estructura de los criptosistemas. Criptografía en redes y Bases de datos.

UNIDAD 2: Criptografía Clásica
Métodos clásicos de encriptación. Por sustitución monoalfabética: César, matricial simple, matricial ordenado por clave. Por sustitución polialfabética: Vigenere. Por trasposición.
Data Encryption Standard: origen, algoritmo implementado, encriptado y desencriptado.

UNIDAD 3: Criptografía Moderna
Criptosistemas contemporáneos: Cifrados simétricos y asimétricos. Condiciones de los criptosistemas asimétricos. Rivest-Shamir-Adleman (RSA): algoritmo implementado, seguridad del método, encubrimiento de los mensajes. Diffie-Hellman (D-H): algoritmo implementado. Merkle-Hellman (M-H): problema knapsack, algoritmo de encriptado y desencriptado, seguridad del método. Métodos de ataque conocidos.

UNIDAD 4: Métodos de Autenticación
Autenticación de mensajes & autenticación de transmisores: conceptos y diferencias. Esquemas de Ong-Schnorr-Shamir y Rivest-Shamir-Adleman. Prueba de mínimo conocimiento o de conocimiento cero.

4.5- Cronograma para el desarrollo de las Unidades Temáticas

UNIDADES	CARGA HORARIA	CRONOGRAMA DE DICTADO
1 - Fundamentos de la Criptografía	6	26//3, 28/3 y 4/4
2 – Criptografía Clásica	4	18/4 y 23/4
3 – Criptografía Moderna	2	16/5
4 – Métodos de Autenticación	2	11/6
	14	---

Tabla 2: Cronograma para el desarrollo teórico de las unidades temáticas

5. FORMACIÓN PRÁCTICA

5.1. Descripción de las actividades de formación práctica

En la asignatura se realizarán actividades de formación de tipo práctica orientadas a garantizar que el estudiante se introduzca en una temática importante en la Informática (creación y uso de algoritmos de encriptación para brindar seguridad a los datos), al mismo tiempo que se lo capacita para intervenir con éxito en la realidad de diferentes sistemas y organizaciones como futuro profesional del área.
Se desarrollarán 4 trabajos prácticos, el primero permitirá a los estudiantes reconocer la evolución de la disciplina, mientras que los 3 prácticos restantes les permitirán desarrollar soluciones a problemas del mundo real mediante la puesta en práctica de los temas teóricos vistos en clase (es decir, articulando la teoría con la práctica).
Específicamente, en el trabajo práctico 1 (TP1) los estudiantes generarán un infograma que muestre los hitos principales en la historia de la criptografía. En los trabajos prácticos 2 (TP2) y 3 (TP3) los estudiantes actuarán como transmisores de mensajes encriptados, como receptores habilitados capaces

de desencriptarlos, y también como receptores no habilitados (o atacantes) que desean quebrar el sistema y descubrir el contenido de los criptogramas. En el caso del TP2 se trabajará con los criptosistemas clásicos (basados en substitución y en transposición), mientras que en el TP3 será con los criptosistemas modernos o contemporáneos (basados en aritmética modular). En el trabajo práctico 4 (TP4) los estudiantes asumirán los roles de autenticador y de autenticado, poniendo en juego diferentes esquemas de autenticación de transmisores (basados en aritmética modular). Además, estos tres últimos prácticos incluirán el desarrollo de un producto software afín a la temática, es decir, en el TP2 un criptosistema clásico, en el TP3 un criptosistema moderno, y en el TP4 un esquema de autenticación de transmisores. Para realizar estos pequeños desarrollos los estudiantes podrán usar el lenguaje a su elección dentro de los vistos durante el cursado de su carrera.
Por otra parte, se concretarán pequeñas actividades individuales de investigación (ACT-INV) donde los estudiantes deberán desarrollar tareas de búsqueda de información sobre casos reales de aplicación de los métodos criptográficos vistos en clase. Producto de las investigaciones realizadas elaborarán y presentarán pequeños informes de carácter monográfico, y también presentaciones que socializarán en clase con sus compañeros, promoviendo el análisis y debate de los temas incluidos.
Se espera que la concreción de todas estas actividades permita capacitar a los estudiantes en el desempeño de sus roles profesionales futuros, mediante el desarrollo de las competencias específicas enunciadas en la sección 3 de este documento, al mismo tiempo que se propicie el desarrollo de las competencias básicas, digitales y transversales incluidas en la sección mencionada.

5.2.-Formación en Ejes Transversales

Explicite de qué manera las actividades de formación práctica descriptas en el punto 5.1 contribuyen a formar a los estudiantes en alguno/s de los siguientes ejes, indicando el grado de profundidad en el tratamiento de los mismos (Bajo, Medio, Alto, Ninguno) y los resultados de aprendizaje esperados.

Eje	**Actividades**	**Resultados de Aprendizaje**	**Grado de Profundidad en el tratamiento**
Identificación, formulación y resolución de problemas de informática	TP1: Analizar antecedentes históricos de la disciplina para conocer su evolución histórica	• **RA1**: Reconocen hitos históricos en la evolución del conocimiento (teórico y práctico) en el área de la Criptografía.	Alto
	TP2: Aplicar algoritmos de encriptación clásicos	• **RA2:** Reconocen situaciones problemáticas de la vida real donde se puedan aplicar métodos criptográficos • **RA3:** Aplican diferentes algoritmos de encriptación clásicos	
	TP3: Aplicar algoritmos de encriptación contemporáneos	• **RA2:** Reconocen situaciones problemáticas de la vida real donde se puedan aplicar métodos criptográficos • **RA4:** Aplican diferentes algoritmos de encriptación contemporáneos	
	TP4: Aplicar algoritmos de autenticación	• **RA2:** Reconocen situaciones problemáticas de la vida real donde se puedan aplicar métodos criptográficos	

		• **RA5:** Aplican diferentes algoritmos de autenticación de transmisores	
	ACT-INV: Buscar en fuentes digitales reconocidas (IEEE, ACM, etc.) artículos que describan casos reales de aplicación de algoritmos de encriptación y de autenticación de transmisores, analizarlos y generar pequeños informes monográficos, para luego socializar oralmente sus trabajos con sus compañeros	• **RA6**: Buscan casos relevantes y reales de aplicación de algoritmos de encriptación y de autenticación de transmisores. • **RA7:** Analizan como en esos casos se resuelven problemas de seguridad.	
Utilización de técnicas y herramientas de aplicación en la informática	TP2: Diseñar algoritmos de encriptación clásicos	• **RA8:** Diseñan diferentes algoritmos de encriptación clásicos	Alto
	TP3: Diseñar algoritmos de encriptación contemporáneos	• **RA9:** Diseñan diferentes algoritmos de encriptación contemporáneos	
	TP4: Diseñar algoritmos de autenticación	• **RA10:** Diseñan diferentes algoritmos de autenticación de transmisores	
	ACT-INV: Buscar en fuentes digitales reconocidas (IEEE, ACM, etc.) artículos que describan casos reales de aplicación algoritmos de encriptación y de autenticación de transmisores, analizarlos y generar pequeños informes monográficos, para luego socializar oralmente sus trabajos con sus compañeros	• **RA11**: Analizan las técnicas y herramientas informáticas utilizadas en casos reales	
Generación de desarrollos tecnológicos y/o innovaciones tecnológicas.	TP2: Programar una aplicación que encripte y desencripte mensajes usando algoritmos clásicos	• **RA12:** Crean aplicaciones para encriptar y desencriptar archivos con algoritmos clásicos	Alto
	TP3: Programar una aplicación que encripte y desencripte mensajes usando algoritmos contemporáneos	• **RA13:** Crean aplicaciones para encriptar y desencriptar archivos con algoritmos contemporáneos	
	TP4: Programar una aplicación que autentique transmisores	• **RA14:** Crean aplicaciones para autenticar transmisores	
Fundamentos para el desempeño en equipos de trabajo	ACT-INV: Buscar en fuentes digitales reconocidas (IEEE, ACM, etc.) artículos que describan casos reales de aplicación algoritmos de encriptación y de autenticación de	• **RA15**: Manifiestan apertura hacia nuevas ideas • **RA16**: Respetan las propuestas de otras personas • **RA17**: Consensuan opiniones y criterios con otras personas	Alto

	transmisores, analizarlos y generar pequeños informes monográficos, para luego socializar oralmente sus trabajos con sus compañeros	• **RA18**: Trabajan eficaz y productivamente en equipo • **RA19**: Elaboran productos digitales audiovisuales para presentar sus trabajos	
Fundamentos para la comunicación efectiva	TP1: Analizar antecedentes históricos de la disciplina para conocer su evolución histórica TP2: Aplicar algoritmos de encriptación clásicos TP3: Aplicar algoritmos de encriptación contemporáneos TP4: Aplicar algoritmos de autenticación ACT-INV: Buscar en fuentes digitales reconocidas (IEEE, ACM, etc.) artículos que describan casos reales de aplicación de algoritmos de encriptación y de autenticación de transmisores, analizarlos y generar pequeños informes monográficos, para luego socializar oralmente sus trabajos con sus compañeros	• **RA20**: Utilizan terminología propia de la disciplina y se expresan correctamente, tanto de manera oral como escrita, • **RA21**: Fundamentan, justifican y explican las actividades desarrolladas	Alto
Fundamentos para la acción ética y responsable.	TP1: Analizar antecedentes históricos de la disciplina para conocer su evolución histórica TP2: Aplicar algoritmos de encriptación clásicos TP3: Aplicar algoritmos de encriptación contemporáneos TP4: Aplicar algoritmos de autenticación ACT-INV: Buscar en fuentes digitales reconocidas (IEEE, ACM, etc.) artículos que describan casos reales de aplicación de algoritmos de encriptación y de autenticación de transmisores, analizarlos y generar pequeños informes monográficos, para luego socializar oralmente sus trabajos con sus compañeros	• **RA22**: Manifiestan un comportamiento honesto • **RA23**: Trabajan individualmente de manera responsable • **RA24**: Reconocen principios de la ética general aplicables	Alto
Fundamentos para evaluar y actuar en relación con el	TP2: Aplicar algoritmos de encriptación clásicos TP3: Aplicar algoritmos de	• **RA25:** Reconocen el importante impacto social que estas	Alto

impacto social de su actividad en el contexto global y local	encriptación contemporáneos TP4: Aplicar algoritmos de autenticación ACT-INV: Buscar en fuentes digitales reconocidas (IEEE, ACM, etc.) artículos que describan casos reales de aplicación de algoritmos de encriptación y de autenticación de transmisores, analizarlos y generar pequeños informes monográficos, para luego socializar oralmente sus trabajos con sus compañeros	tecnologías pueden provocar cuando son utilizadas para dar solución a situaciones problemáticas de la vida real • **RA26:** Reconocen aspectos de la actuación profesional que están en juego durante la aplicación de las técnicas	
Fundamentos para el aprendizaje continuo	TP1: Analizar antecedentes históricos de la disciplina para conocer su evolución histórica TP2: Aplicar algoritmos de encriptación clásicos TP3: Aplicar algoritmos de encriptación contemporáneos TP4: Aplicar algoritmos de autenticación ACT-INV: Buscar en fuentes digitales reconocidas (IEEE, ACM, etc.) artículos que describan casos reales de aplicación de algoritmos de encriptación y de autenticación de transmisores, analizarlos y generar pequeños informes monográficos, para luego socializar oralmente sus trabajos con sus compañeros	• **RA22**: Manifiestan un comportamiento honesto • **RA23**: Trabajan individualmente de manera responsable • **RA27**: Auto-aprenden familiarizándose con diferentes contextos reales donde se aplica la criptografía	Alto

Tabla 3: Formación en Ejes Transversales

Con el propósito de mostrar como los diferentes resultados de aprendizaje incluidos en la tabla anterior (Tabla 3), se incluye a continuación la Tabla 4 donde se evidencia la cobertura lograda sobre los diferentes objetivos de la asignatura enunciados en la sección 3 de este documento.

Resultados de aprendizaje	**Objetivos de la asignatura**			
	Competencias básicas	**Competencias específicas**	**Competencias digitales**	**Competencias transversales**
• **RA1**: Reconocen hitos históricos en la evolución del conocimiento (teórico y práctico) en el área de la Criptografía.	**X**			
• **RA2:** Reconocen situaciones problemáticas de la vida real donde se puedan aplicar métodos criptográficos		**X**	**X**	

Resultados de aprendizaje	Objetivos de la asignatura			
	Competencias básicas	**Competencias específicas**	**Competencias digitales**	**Competencias transversales**
• **RA3:** Aplican diferentes algoritmos de encriptación clásicos	**X**	**X**		
• **RA4:** Aplican diferentes algoritmos de encriptación contemporáneos	**X**	**X**		
• **RA5:** Aplican diferentes algoritmos de autenticación de transmisores		**X**	**X**	
• **RA6**: Buscan casos relevantes y reales de aplicación de algoritmos de encriptación y de autenticación de transmisores	**X**		**X**	
• **RA7:** Analizan como en esos casos se resuelven problemas de seguridad	**X**	**X**		
• **RA8:** Diseñan diferentes algoritmos de encriptación clásicos	**X**	**X**	**X**	
• **RA9:** Diseñan diferentes algoritmos de encriptación contemporáneos	**X**	**X**	**X**	
• **RA10:** Diseñan diferentes algoritmos de autenticación de transmisores	**X**	**X**	**X**	
• **RA11**: Analizan las técnicas y herramientas informáticas utilizadas en casos reales	**X**	**X**		
• **RA12:** Crean aplicaciones para encriptar y desencriptar archivos con algoritmos clásicos	**X**	**X**	**X**	
• **RA13:** Crean aplicaciones para encriptar y desencriptar archivos con algoritmos contemporáneos	**X**	**X**	**X**	
• **RA14:** Crean aplicaciones para autenticar transmisores	**X**	**X**	**X**	
• **RA15**: Manifiestan apertura hacia nuevas ideas				**X**
• **RA16**: Respetan las propuestas de otras personas				**X**
• **RA17**: Consensuan opiniones y criterios con otras personas	**X**			**X**
• **RA18**: Trabajan eficaz y productivamente en equipo				**X**
• **RA19**: Elaboran productos digitales audiovisuales para presentar sus trabajos	**X**		**X**	
• **RA20**: Utilizan terminología propia de la disciplina y se expresan correctamente, tanto de manera oral como escrita				**X**
• **RA21**: Fundamentan, justifican y explican las actividades desarrolladas	**X**			**X**
• **RA22**: Manifiestan un comportamiento honesto				**X**
• **RA23**: Trabajan individualmente de manera responsable				**X**

Resultados de aprendizaje	Objetivos de la asignatura			
	Competencias básicas	**Competencias específicas**	**Competencias digitales**	**Competencias transversales**
• **RA24**: Reconocen principios de la ética general aplicables				**X**
• **RA25:** Reconocen el importante impacto social que estas tecnologías pueden provocar cuando son utilizadas para dar solución a situaciones problemáticas de la vida real	**X**	**X**		**X**
• **RA26:** Reconocen aspectos de la actuación profesional que están en juego durante la aplicación de las técnicas	**X**	**X**		**X**
• **RA27**: Auto-aprenden familiarizándose con diferentes contextos reales donde se aplica la criptografía	X			X

Tabla 4. Cobertura de Objetivos por resultados de aprendizaje

5.3 Cronograma de formación práctica

Tabla 4: Cronograma para el desarrollo de las Actividades Prácticas

ACTIVIDAD	CARGA HORARIA	CRONOGRAMA DE DESARROLLO	Horas resolución problemas rutinarios	Horas form. experimental
TP 1: Historia de la criptografía	6	9/4, 11/4 y 16/4	6	-
TP 2: Criptografía clásica	8	25/4, 30/4, 2/5 y 7/5	3	5
TP 3: Criptografía moderna	10	21/5, 23/5, 28/5, 30/5 y 4/6	3	7
TP 4: Autenticación	6	13/6, 18/6 y 25/6	3	3
	30	**TOTALES**	**15**	**15**

5.4- Cuadro sintético

Teóricas	Formación Práctica					
	Formación experimental	Resolución de problemas del mundo real	Actividades de Proyectos y Diseño de Sistemas de Información	Instancias supervisadas de formación en la práctica profesional	Otras*	Total
14	**18**	**---**	**---**	**---**	**24***	**42**

* Corresponden a esta categoría las 18 horas de resolución de problemas rutinarios en trabajos prácticos, y las 12 horas de evaluaciones parciales y recuperatorias, y evaluación de trabajos de investigación (descriptas en apartado 7.3.1.)

Observación: las 4 horas faltantes para cumplimentar las 60 hs. total asignadas a la asignatura corresponden a los feriados de: martes 2/4 y jueves 20/5.

6. BIBLIOGRAFÍA

Título	Autor(es)	Editorial	Año y Lugar de edición	Disponible en	Cantidad de Ejemplares disponibles
Criptografía. Técnicas de desarrollo para profesionales	Ariel Maiorano	Alfaomega	Reimpresión 2013, México	Biblioteca Departamento de Informática FCEyT-UNSE	2
Criptografía y seguridad en computadoras	Manuel Lucena López	Universidad de Jaén	1999, España	Aula virtual CUV- FCEyT https://openlibra.com/es/collection	e-book
Cryptography: An Introduction to Computer Security	Jennifer Seberry y Josef Pieprzyk	Prentice-Hall	1988, Australia	Aula virtual CUV- FCEyT https://openlibra.com/es/collection	e-book
Teoría de códigos y Criptografía	Laura Colmenarejo, Marithania Silvero, M. Jesús Soto, José M. Tornero, José M. Ucha	Universidad de Sevilla	2014, España	Aula virtual CUV- FCEyT https://openlibra.com/es/collection https://cardbiss.com/libro-gratuito-teoria-de-codigos-y-criptografia-en-espanol/	e-book
Estudio y Aplicaciones de Esquemas Criptográficos	Carlos Rentería Marcos y Tlatoani de Jesús Reyes Bermejo	Instituto Politécnico Nacional	2012, México	Aula virtual CUV- FCEyT https://www.repositoriodigital.ipn.mx/handle/123456789/5922	e-book
¿Qué es la seguridad informática?	Hugo Scolnik	Paidos	2014, Argentina	Biblioteca Departamento de Informática FCEyT-UNSE	1
Criptografía. Desde los sistemas clásicos hasta el futuro de la privacidad.	Federico Pacheco	Red USERS	2014, Argentina	Biblioteca Departamento de Informática FCEyT-UNSE	1

7- ESTRATEGIAS METODOLÓGICAS.

7.1- Aspectos pedagógicos y didácticos

Describir la metodología de enseñanza que se adopta y las técnicas de trabajo áulico, de Laboratorio, etc. Explicite las estrategias empleadas para la formación práctica, la articulación e integración teoría y práctica y la formación en los ejes transversales.

En esta propuesta el aula se entiende como un espacio de diálogo y construcción, en el que se trabaja interactuando permanentemente. La comunicación se concreta con una estructura multipolar-

bidireccional, donde tanto los estudiantes como los docentes se consideran fuentes de información. En base a ello se han seleccionado las siguientes técnicas metodológicas para poner en juego durante el desarrollo de los contenidos programáticos:

a) Discusión dirigida
b) Aprendizaje colaborativo
c) Exposiciones abiertas
d) Resolución de casos
e) Uso de recursos educativos abiertos (REA)
f) Presentación de productos entregables

Por otra parte, al iniciar la asignatura se realizará una presentación global de la misma, consensuando objetivos y mostrando en un mapa conceptual la articulación temática de la asignatura, a fin de favorecer una comprensión global de la misma antes de entrar en el abordaje puntual de cada tema.

El enfoque principal dado a la asignatura será el aprendizaje colaborativo que permite promover la construcción compartida del conocimiento, mediante el cual no sólo se logra la apropiación activa del mismo por parte de los miembros de cada grupo de aprendizaje, sino también la indispensable socialización del estudiante que toda su vida deberá transcurrir en contacto y en colaboración con sus semejantes, lo que permitirá el desarrollo de sus competencias de trabajo en equipo.

Para incentivar habilidades de aprendizaje autónomo, así como para reforzar la apropiación de conocimientos logrado en las clases presenciales, se emplearán recursos educativos abiertos (REA) sobre diferentes temas del contenido programático. Estos REA serán especialmente desarrollados por la profesora responsable del espacio con el software eXe-learning, y no sólo contendrán desarrollo teórico, sino también ejemplos, material de actualidad vinculado, y tareas de autocomprobación. Los REA estarán disponibles en el aula virtual de la asignatura, la cual funcionará en la plataforma MOODLE del Centro Universitario Virtual perteneciente a la FCEyT. Allí, los estudiantes también encontrarán material didáctico, recursos bibliográficos, y foros de consulta especialmente creados, además de contar con las facilidades de comunicación con profesores y compañeros propias de Moodle.

En particular, considerando las actividades prácticas, los estudiantes resolverán 4 Trabajos prácticos cuyas temáticas están enunciadas en la Tabla 5 incluida en la sección 5.3. Cabe aclarar, además, que los TP2 a TP4 incluyen una actividad de desarrollo de software (con lenguaje a elección del estudiante acorde con el conocimiento que a este momento de la carrera posea).

Por otra parte, se concretarán pequeñas actividades individuales de investigación (ACT-INV) donde los estudiantes buscarán antecedentes relevantes que analizarán, documentarán y expondrán a sus compañeros para debate de los temas incluidos.

Completando las actividades de aprendizaje se desarrollarán otras actividades, como edición colaborativa de textos (en ACT-INV) y participación en foros grupales (dentro de los TP2, TP3 y TP4).

7.2- Mecanismos para la integración de docentes

Especificar los mecanismos y/o actividades para la integración de docentes, de diferentes asignaturas, en experiencias comunes

Considerando la integración vertical de esta asignatura con otras de la carrera, y a fin de facilitar la interrelación entre los docentes responsables de mismas, se prevé realizar al finalizar el cuatrimestre una reunión que permita evaluar lo ejecutado y acordar acciones de ajuste para el próximo año.

7.3- Recursos Didácticos

(Libros, revistas, publicaciones científicas, fotografías, videos, teleconferencias, software, página web, aula virtual, maquinarias, equipos, etc.). Describir en forma breve la importancia de los recursos didácticos que utiliza para favorecer un aprendizaje significativo y el logro de los objetivos.

Los recursos didácticos necesarios para el normal desenvolvimiento de la asignatura son los siguientes:

- Bibliografía actualizada tanto para facilitar a los estudiantes la apropiación de contenidos teóricos y prácticos.
- Aula virtual en Moodle para organizar y almacenar todo el material de la cursada (teórico y práctico), sociabilizar conocimientos a través del diálogo en foros evaluados, satisfacer consultas, coordinar actividades, resguardar actividades evaluadas, almacenar calificaciones, etc. Un uso adecuado del aula virtual promoverá en los estudiantes la apropiación de conocimientos y el desarrollo de distintas competencias (digitales, de trabajo individual responsable, de trabajo en equipo eficaz, etc.)
- REA, Libros digitales, y publicaciones disponibles en la Biblioteca de MINCYT para fomentar en los estudiantes el desarrollo de sus competencias digitales a la vez que se les facilita la apropiación de conocimientos.
- Tiza, pizarrón, PC, cañón y software PowerPoint para presentar los diferentes temas.

8- EVALUACIÓN

8.1- Evaluación Diagnóstica

Es recomendable para constatar la presencia o ausencia de ciertos conocimientos, capacidades y habilidades al inicio del curso o de unidades temáticas.

La evaluación diagnóstica permitirá evaluar el nivel de apropiación de los conocimientos previos por parte de los estudiantes. Esta evaluación será individual, escrita y de opción múltiple, y abarcará conceptos básicos desarrollados en las asignaturas Simulación, Redes II e Ingeniería de Software, y Sistemas de información II. El nivel de calificación será cualitativo politómico, según escala: Alto, Medio, Bajo. Esta instancia de evaluación se concretará durante la primera semana del cursado a través de un código QR disponible en el aula virtual de la asignatura.

8.2- Evaluación Formativa

Puede efectivizarse a través de tareas individuales o grupales. Posibilita detectar los aciertos, desaciertos, progresos y problemas que se presentan en el aula, permitiendo efectuar modificaciones o ajustes durante los procesos de enseñanza y de aprendizaje.

La evaluación formativa es de carácter continuo y está dirigida fundamentalmente a evaluar el proceso de enseñanza y de aprendizaje seguido por los estudiantes. Dado lo expuesto, tal evaluación se llevará a cabo durante todo el desarrollo de la asignatura a medida que los estudiantes concretan sus actividades de aprendizaje ya sea en modalidad individual o grupal.

8.3- Evaluación Parcial

8.3.1- Programa de Evaluaciones Parciales

Prueba oral o escrita en forma individual o grupal sobre determinados contenidos. Permite determinar el nivel de conocimientos y capacidades alcanzado por los alumnos. Incluir Cronograma de Evaluaciones Parciales, mediante un cuadro de doble entrada donde se visualice la semana estimativa de realización de cada parcial y recuperatorio. Incluir además la instancia de devolución de resultados, considerando la Resol CS. Nº 343/2017.

Evaluación	Contenidos	Tipo	Fecha Probable	Horas Resol. Problemas Rutinarios	Instrumento
DIAGNOSTICA	Conocimientos previos	Individual, escrita, prueba de desempeño, de carácter teórico	Semana del 26/3 (devolución de resultados instantánea)	---	Cuestionario Moodle especialmente diseñado
PARCIAL 1	Temas incluidos en Unidades 1 y 2	Especialmente diseñada, individual, escrita, prueba de desempeño, de contenido teórico y práctico	14/5	2	Resolución documentada de problemas Cuestionario multiple-choice
PARCIAL 2	Temas incluidos en Unidades 3 y 4	Especialmente diseñada, individual, escrita, prueba de desempeño, de contenido teórico y práctico	27/6	2	Resolución documentada de problemas Cuestionario multiple-choice
RECUPERATORIO 1	Temas incluidos en Unidades 1 y 2	Especialmente diseñada, individual, escrita, prueba de desempeño, de contenido práctico	4/7	2	Resolución documentada de problemas
RECUPERATORIO 2	Temas incluidos en Unidades 3 y 4	Especialmente diseñada, individual, escrita, prueba de desempeño, de contenido práctico			
ACT-INV	Temas incluidos en Unidad 2, 3 y 4	Grupal, documental y oral, de contenido teórico	9/5, 6/6 y 2/7	8	Monografía y Presentación digital
TOTAL				**14**	

8.3.2- Criterios de Evaluación

Explicite los criterios con que serán evaluados los estudiantes en cada instancia de evaluación indicada en el punto anterior. Estos criterios deben elaborarse teniendo presentes los objetivos definidos para la asignatura.

- ***En parciales y recuperatorios, y trabajos de investigación***

a) Adecuada interpretación de consignas a responder
b) Adecuado manejo de conocimiento y vocabulario técnico específico
c) Correcta formulación de respuestas a las consignas
d) Adecuada selección de ejemplos si son solicitados
e) Adecuada calidad de las respuestas considerando que sea clara, libre de errores de ortografía, ordenada y acotada a lo pedido.

Además, para el parcial 1 y su recuperatorio, considerando que corresponden a los contenidos establecidos para las Unidades 1 y 2, se evaluará específicamente si los estudiantes:

- **RA1**: Reconocen hitos históricos en la evolución del conocimiento (teórico y práctico) en el área de la Criptografía.
- **RA2:** Reconocen situaciones problemáticas de la vida real donde se puedan aplicar métodos criptográficos
- **RA3:** Aplican diferentes algoritmos de encriptación clásicos
- **RA20**: Utilizan terminología propia de la disciplina y se expresan correctamente, tanto de manera oral como escrita
- **RA21**: Fundamentan, justifican y explican las actividades desarrolladas
- **RA22**: Manifiestan un comportamiento honesto
- **RA23**: Trabajan individualmente de manera responsable
- **RA24**: Reconocen principios de la ética general aplicables

Además, para el parcial 2 y su recuperatorio, considerando que corresponden a los contenidos establecidos para las Unidades 3 y 4, se evaluará específicamente si los estudiantes:

- **RA2:** Reconocen situaciones problemáticas de la vida real donde se puedan aplicar métodos criptográficos
- **RA4:** Aplican diferentes algoritmos de encriptación contemporáneos
- **RA5:** Aplican diferentes algoritmos de autenticación de transmisores
- **RA20**: Utilizan terminología propia de la disciplina y se expresan correctamente, tanto de manera oral como escrita
- **RA21**: Fundamentan, justifican y explican las actividades desarrolladas
- **RA22**: Manifiestan un comportamiento honesto
- **RA23**: Trabajan individualmente de manera responsable
- **RA24**: Reconocen principios de la ética general aplicables

Además, para las actividades de investigación, considerando que corresponden a los contenidos establecidos para las unidades 2, 3 y 4, se evaluará específicamente si los estudiantes:

- **RA15**: Manifiestan apertura hacia nuevas ideas
- **RA16**: Respetan las propuestas de otras personas
- **RA17**: Consensuan opiniones y criterios con otras personas
- **RA18**: Trabajan eficaz y productivamente en equipo
- **RA19**: Elaboran productos digitales audiovisuales para presentar sus trabajos
- **RA20**: Utilizan terminología propia de la disciplina y se expresan correctamente, tanto de manera oral como escrita
- **RA21**: Fundamentan, justifican y explican las actividades desarrolladas
- **RA22**: Manifiestan un comportamiento honesto
- **RA24**: Reconocen principios de la ética general aplicables
- **RA25:** Reconocen el importante impacto social que estas tecnologías pueden provocar cuando son utilizadas para dar solución a situaciones problemáticas de la vida real
- **RA26:** Reconocen aspectos de la actuación profesional que están en juego durante la aplicación de las técnicas
- **RA27**: Auto-aprenden familiarizándose con diferentes contextos reales donde se aplica la criptografía

8.3.3- Escala de Valoración

Indicar el tipo de escala adoptada (numérica, conceptual, etc.). Si no coincide con la escala aprobada en Reglamento Alumnos, debe explicitar la correspondencia con la misma.

La escala de valoración a emplear para los parciales y recuperatorios será cuantitativa del 1 al 10.

8.4- Evaluación Integradora

No corresponde.

8.5- Evaluación Sumativa

8.5.1- Condiciones para lograr la promoción sin Examen Final

- Registrar un mínimo de 80 % de asistencia a las clases de la asignatura
- Aprobar el parcial 1 con un mínimo de 7 puntos.
- Aprobar el parcial 2 con un mínimo de 7 puntos.
- Aprobar actividades de investigación con un mínimo de 7 puntos.

8.5.2- Condiciones para lograr la Regularidad de la Asignatura.

- Registrar un mínimo de 70 % de asistencia a las clases de la asignatura
- Aprobar parciales prácticos o sus recuperatorios con un mínimo de 5 puntos.
- Aprobar actividades de investigación con un con un mínimo de 5 puntos.

8.6- Examen Final

La evaluación final será escrita u oral sobre los temas incluidos en la programación analítica.

8.7- Examen Libre

Los estudiantes libres deberán cumplir las siguientes etapas, cada una de ellas eliminatoria.

- Primera etapa: Aprobar una evaluación escrita de tipo práctica, de acuerdo con la temática de los parciales 1 y 2 de la asignatura.
- Segunda etapa: Aprobar una evaluación de tipo teórica, abarcando la totalidad del contenido programático, que podrá ser oral o escrita.

.....

Dra. Rosanna Costaguta
Prof. Responsable de Cátedra
Febrero de 2024.-