Guía docente de la asignatura

Asignatura	GARANTÍA Y SEGURIDAD DE LA INFORMACIÓN		
Materia	SISTEMAS DE INFORMACIÓN Y BASES DE DATOS		
Módulo			
Titulación	GRADO EN INGENIERÍA INFORMÁTICA DE SISTEMAS (464)		
Plan	464	**Código**	45267
Periodo de impartición	1er. CUATRIMESTRE	**Tipo/Carácter**	OBLIGATORIA
Nivel/Ciclo	GRADO	**Curso**	3º
Créditos ECTS	6 ECTS		
Lengua en que se imparte	CASTELLANO		
Profesor/es responsable/s	VALENTÍN CARDEÑOSO PAYO (Coordinador) CÉSAR LLAMAS BELLO PABLO DE LA FUENTE REDONDO		
Datos de contacto (E-mail, teléfono…)	TELÉFONO: 983 423000 ext. 5601 / ext. 5609 E-MAIL: valen@infor.uva.es, cllamas@infor.uva.es		
Horario de tutorías	Véase www.uva.es → Centros → Campus de Valladolid → Escuela Técnica Superior de Ingeniería Informática → Tutorías		
Departamento	DEPARTAMENTO DE INFORMÁTICA (ATC, CCIA, LSI)		

1. Situación / Sentido de la Asignatura

1.1 Contextualización

La Ingeniería de la Seguridad se ocupa del desarrollo de sistemas que se mantengan fiables (*dependable*) frente a errores, usos maliciosos o mala fortuna. Como disciplina, se centra en el estudio de los métodos, procesos y herramientas necesarios para diseñar, implementar y probar sistemas completos y para adaptar los sistemas existentes a entornos que evolucionan. Aunque la mayor parte de las tecnologías que sirven de base para garantizar la seguridad de la información (criptología, fiabilidad de software, resistencia a intrusos, …) están relativamente maduras, aún falta conocimiento y experiencia sobre cómo aplicarlas de forma eficiente y eficaz.

En un entorno digital como el que nos movemos, el graduado en Ingeniería Informática de Sistemas, con un perfil profesional orientado a la gestión de las Tecnologías de la Información en todos los ámbitos debe contar con una formación sólida en los aspectos fundamentales de ingeniería de la seguridad. Ese es el objetivo que pretende esta asignatura, enmarcada en la materia de Sistemas de Información y Bases de Datos.

La asignatura pretende cubrir tanto los aspectos conceptuales más básicos del ámbito de la seguridad como los aspectos metodológicos relacionados con la garantía y protección de la información. Las técnicas relacionadas con la protección de recursos, a los diversos niveles de organización de los sistemas de cómputo, y las técnicas de identificación segura de usuarios y control de acceso forman parte central de los contenidos de esta asignatura.

1.2 Relación con otras materias

La asignatura pertenece a la materia de Sistemas de Información y Bases Datos, estando relacionada en términos de competencias con el Diseño de Bases de Datos y la Administración de Bases de Datos. Además, tiene relación transversal con diferentes asignaturas del plan de estudios, entre las que destacamos las de la materia Plataforma Tecnológica: Administración de Sistemas Operativos, Diseño Administración y Seguridad de Redes.

1.3 Prerrequisitos

Se recomienda que los alumnos hayan superado las competencias básicas de las asignaturas Fundamentos de Redes, Fundamentos de Computadoras y Fundamentos de Redes.

2. Competencias

2.1 Generales

Código	Descripción
G03	Capacidad de análisis y síntesis
G04	Capacidad de organizar y planificar
G05	Comunicación oral y escrita en la lengua propia
G06	Conocimiento de una segunda lengua (preferentemente inglés)
G08	Habilidades de gestión de la información
G09	Resolución de problemas
G10	Toma de decisiones
G11	Capacidad crítica y autocrítica
G12	Trabajo en equipo
G14	Responsabilidad y compromiso ético
G15	Liderazgo
G16	Capacidad de aplicar los conocimientos en la práctica
G17	Habilidades de investigación
G18	Capacidad de aprender
G19	Capacidad de adaptarse a nuevas situaciones
G20	Capacidad de generar nuevas ideas
G21	Habilidad para trabajar de forma autónoma
G22	Diseño y gestión de proyectos

2.2 Específicas

Código	Descripción
TI7	**Capacidad para comprender, aplicar y gestionar la garantía y seguridad de los sistemas informáticos.**
SI2	**Capacidad para determinar los requisitos de los sistemas de información y comunicación de una organización atendiendo a aspectos de seguridad y cumplimiento de la normativa y la legislación vigente.**

3. Objetivos

Código	Descripción
SI2.1	Evaluar los riesgos que afectan a los recursos de información de una organización y ser capaz de catalogarlos y clasificarlos.
TI7.1	Analizar las necesidades de garantía de la información en un sistema informático.
TI7.2	Adoptar modelos, gestores y políticas de seguridad adecuadas, incluyendo los servicios de seguridad necesarios

4. Tabla de dedicación del estudiante a la asignatura

ACTIVIDADES PRESENCIALES	HORAS	ACTIVIDADES NO PRESENCIALES	HORAS
Clases teórico-prácticas (T/M)	**28**	Estudio y trabajo autónomo individual	48
Clases prácticas de aula (A)			
Laboratorios (L)	**20**	Estudio y trabajo autónomo grupal	30
Prácticas externas, clínicas o de campo			
Seminarios (S)	**6**	Estudio y trabajo autónomo grupal	12
Tutorías grupales (TG)			
Evaluación (fuera del periodo oficial de exámenes)	**6**		
Total presencial	**60**	**Total no presencial**	**90**

5. Bloques temáticos

Bloque 1: Fundamentos de Seguridad de la Información

Carga de trabajo en créditos ECTS: 1,2

a. Contextualización y justificación

En este primer bloque se analizan las diferentes facetas de la ingeniería de la seguridad y se introducen los conceptos y objetivos básicos de la seguridad y de la garantía de la información. Se presentan los doce principios básicos de seguridad introducidos ya hace más de tres décadas por Saltzer y Schroeder en un artículo de referencia en el área.

b. Objetivos de aprendizaje

Código	Descripción
SI2.1	Evaluar los riesgos que afectan a los recursos de información de una organización y ser capaz de catalogarlos y clasificarlos.
TI7.1	Analizar las necesidades de garantía de la información en un sistema informático.

Tras completar satisfactoriamente este bloque, el alumno:

- Conocerá los posibles riesgos que afectan a la seguridad e integridad de la información que se maneja las organizaciones.
- Podrá detectar las repercusiones de la seguridad de la información de la organización en un sistema informático vinculado a dicha organización, para poder analizar posteriormente las necesidades de garantía de la información.
- Será capaz de confeccionar una lista de criterios que le permitirán evaluar los posibles riesgos que afectan a un sistema informático.
- Conocerá los mecanismos que se emplean para hacer frente a los ataques a la integridad y seguridad de la información, como los planes de contingencia y los métodos de defensa al alcance del ingeniero informático.

c. Contenidos

TEORÍA

TEMA 1: Visión panorámica
- 1.1 Marco sistémico de ingeniería de la seguridad.
- 1.2 Visión funcional de la seguridad.
- 1.3 El problema de la seguridad en computación.

TEMA 2: Conceptos básicos de seguridad de la información
- 2.1 Objetivos básicos: confidencialidad, integridad y disponibilidad
- 2.2 Vulnerabilidad, ataques y riesgo.
- 2.3 Formas de ataque y métodos de defensa.

TEMA 3: Principios básicos de seguridad
- 3.1 Contexto del problema.
- 3.2 Los doce principios básicos de la seguridad de Saltzer y Schroeder.

PRÁCTICAS

P0. Instalación y Configuración del entorno de trabajo práctico.
P1. Primer supuesto práctico: Servicios y seguridad de red
PROYECTO PRÁCTICO: Enunciado, análisis y planificación del trabajo.

d. Métodos docentes

- Ver anexo

e. Plan de trabajo

- Ver anexo

f. Evaluación

- Ver punto 7 de esta guía.

g. Bibliografía básica

- Stuart Jacobs, *Engineering Information Security*. IEEE Press, 2011. ISBN 978-0-470-56512-4.
- Charles P. PFleeger, *Security in Computing*, 2nd. ed., Prentice-Hall, 1997. ISBN 0-13-185794-0.

h. Bibliografía complementaria

- Ross Anderson, *Security Engineering*, 2nd ed. Wiley, 2008. ISBN 978-0-470-06852-6.
- David Basin, Patrick Schaller y Michael Schläpfer, *Applied Information Security*. Springer, 2011. ISBN 978-3-642-24473-5.
- William Stallings, Network and Internetwork Security. Prentice Hall, 1995. ISBN 0-02-415483-0.
- J.H. Saltzer y M.D. Schroeder, *The Protection of Information in Computer Systems*. Proceedings of the IEEE, volume 63, pag. 1278-1308, 1975.

i. Recursos necesarios

Todas las referencias web y el software necesario se pondrá a disposición de los alumnos a través de la página de la asignatura en el campus virtual.

Bloque 2: Protección y Garantía de la Información

Carga de trabajo en créditos ECTS: 3,2

a. Contextualización y justificación

En este bloque, que constituye la parte central de la asignatura, se analizan los diferentes mecanismos de protección frente a problemas de seguridad: la protección de recursos (información) y la protección de acceso (usuarios), que incluye los problemas de autenticación e identificación segura.

La protección de acceso se presenta de forma ascendente por niveles, desde el entorno físico al nivel de aplicación. En cada uno de ellos se analizarán las alternativas que se han ido desarrollando para proporcionar mecanismos de protección que garanticen la fiabilidad de los sistemas y de la información.

La protección de la información no protegida usando técnicas criptográficas se aborda en la segunda parte de este bloque. Se presentarán, de forma resumida pero útil, los fundamentos de la criptografía de clave privada y de clave pública y se discutirán desde un enfoque funcional los problemas relacionados con el intercambio de claves. Se ilustrarán todos estos conceptos con referencias constantes a las posibles aplicaciones prácticas de estas técnicas.

El bloque termina con un apartado esencial desde el punto de vista de la elaboración sistematica de soluciones de seguridad: los diversos modelos de seguridad que se han ido introduciendo a lo largo de los años. Estos modelos proporcionan la base de trabajo para elaborar las políticas y planes de seguridad que forman parte del proceso de ingeniería de la seguridad.

b. Objetivos de aprendizaje

Código	Descripción
TI7.1	Analizar las necesidades de garantía de la información en un sistema informático.
TI7.2	Adoptar modelos, gestores y políticas de seguridad adecuadas, incluyendo los servicios de seguridad necesarios

Tras completar satisfactoriamente este bloque, el alumno:

- Podrá identificar los principales servicios de seguridad que se pueden incluir en un sistema informático.
- Será capaz de cubrir las necesidades de garantía de la información de un sistema mediante estos servicios de seguridad.
- Conocerá los principales modelos de seguridad conocidos aplicables a los sistemas informáticos.
- Será capaz de identificar los mecanismos criptográficos más habituales: algoritmos y protocolos de encriptación, firma y contrato
- Podrá decidir por sí mismo qué modelo de seguridad es apropiado para un sistema concreto.
- Será capaz de analizar la seguridad que proporciona este modelo de seguridad con relación a las necesidades de garantía de la información del sistema, lo que incluye la identificación de cada elemento y sus relaciones, y los mecanismos criptográficos apropiados.

c. Contenidos

TEORÍA

TEMA 1: Protección de acceso
- 1.1 Identificación de usuarios y control de acceso.
- 1.2 Diseño y gestión de listas de control de acceso.

TEMA 2: Protección y garantía de recursos de informaciónn
- 2.1 Entorno físico.
- 2.2 Mecanismos de nivel arquitectónico: procesador.
- 2.3 Mecanismos de nivel sistema operativo.
- 2.4 Mecanismos de los niveles de red.
- 2.5 Mecanismos de nivel de aplicación.

TEMA 3: Criptografía básica
- 3.1 Terminología y escenarios.
- 3.2 Criptografía de clave privada.
- 3.3 Criptografía de clave pública.
- 3.4 Protocolos y práctica de la criptografía.

TEMA 4: Modelado de seguridad

4.1 Modelo Bell-LaPadula y extensiones.
4.2 Modelo Muralla China
4.3 Modelo Biba
4.4 Modelo Clark Wilson
4.5 Estándares relacionados.

PRÁCTICAS

P2. Segundo supuesto práctico: Usuarios, grupos y relaciones de confianza.
P3. Tercer supuesto práctico: Configuración y seguimiento de ficheros de bitácora del sistema.
P4. Cuarto supuesto práctico: Creación, distribución y uso de certificados.
P5. Quinto supuesto práctico: Análisis y configuración de seguridad web.
PROYECTO PRÁCTICO: Se avanza en el desarrollo del mismo, en paralelo.

d. Métodos docentes

- Ver anexo

e. Plan de trabajo

- Ver anexo

f. Evaluación

- Ver punto 7 de esta guía.

g. Bibliografía básica

- Stuart Jacobs, *Engineering Information Security*. IEEE Press, 2011. ISBN 978-0-470-56512-4.
- Charles P. PFleeger, *Security in Computing*, 2nd. ed., Prentice-Hall, 1997. ISBN 0-13-185794-0.

h. Bibliografía complementaria

- Ross Anderson, *Security Engineering*, 2nd ed. Wiley, 2008. ISBN 978-0-470-06852-6.
- David Basin, Patrick Schaller y Michael Schläpfer, *Applied Information Security*. Springer, 2011. ISBN 978-3-642-24473-5.
- William Stallings, Network and Internetwork Security. Prentice Hall, 1995. ISBN 0-02-415483-0.

i. Recursos necesarios

Todas las referencias web y el software necesario se pondrá a disposición de los alumnos a través de la página de la asignatura en el campus virtual.

Bloque 3: Gestión de la seguridad de la información

Carga de trabajo en créditos ECTS: 1,6

a. Contextualización y justificación

La asignatura termina con un bloque íntegramente dedicado a los aspectos metodológicos y de planificación de ingeniería de la seguridad, con especial atención a las normas y estándares que se aplican en este dominio. Desde un enfoque práctico, se analizarán los aspectos clave relacionados con el diseño de políticas de seguridad y los aspectos metodológicos para asegurar un diseño, despliegue, evaluación y mantenimiento de soluciones de seguridad correctas y conformes con los estándares de mercado.

b. Objetivos de aprendizaje

Código	Descripción
SI2.1	Evaluar los riesgos que afectan a los recursos de información de una organización y ser capaz de catalogarlos y clasificarlos.
TI7.1	Analizar las necesidades de garantía de la información en un sistema informático.
TI7.2	Adoptar modelos, gestores y políticas de seguridad adecuadas, incluyendo los servicios de seguridad necesarios

Tras completar satisfactoriamente este bloque, el alumno:

- Será capaz de identificar las líneas generales de un proceso de ingeniería de seguridad, y reconocerá los más habituales.
- Será capaz de interpretar un proyecto concreto de seguridad práctico.
- Podrá identificar los aspectos más importantes de una política de seguridad, y diseñará una concreta para un caso práctico.
- Evaluará los riesgos prácticos asociados a un modelo de seguridad concreto y una política concreta de seguridad para un caso práctico.
- Será capaz de integrarse en un equipo de trabajo que implanta la política de seguridad de la información de una organización.
- Conocerá las tareas involucradas en la operación de un dispositivo de seguridad práctico asociado a un sistema informático.

c. Contenidos

TEORÍA

TEMA 1: Proceso de ingeniería de la seguridad
- 1.1 Cuerpo común de conocimiento sobre dominios de seguridad
- 1.2 Modelo de proceso en ingeniería de la seguridad.
- 1.3 Esquema del ISO 27001 e ISO 27002.

TEMA 2: Diseño de políticas de seguridad
- 2.1 Aspectos clave de una política de seguridad.
- 2.2 Aspectos éticos y legales.
- 2.3 Aspectos organizativos.

TEMA 3: Metodología de trabajo en ingeniería de seguridad
- 3.1 Inventario de bienes y servicios.
- 3.2 Detección y valoración de vulnerabilidades, riesgos y amenazas.
- 3.3 Plan de gestión de riesgos.

TEMA 4: Gestión y mantenimiento de la seguridad
- 4.1 Mecanismos operacionales.
- 4.2 Evaluación y aseguramiento de los sistemas de seguridad.

PRÁCTICAS

PROYECTO PRÁCTICO: Finalización y puesta en común (presentación y debate). Evaluación entre pares de los proyectos presentados.

d. Métodos docentes

- Ver anexo

e. Plan de trabajo

- Ver anexo

f. Evaluación

- Ver punto 7 de esta guía.

g. Bibliografía básica

- Stuart Jacobs, *Engineering Information Security*. IEEE Press, 2011. ISBN 978-0-470-56512-4.
- Ross Anderson, *Security Engineering*, 2nd ed. Wiley, 2008. ISBN 978-0-470-06852-6.

h. Bibliografía complementaria

- Charles P. PFleeger, *Security in Computing*, 2nd. ed., Prentice-Hall, 1997. ISBN 0-13-185794-0.
- David Basin, Patrick Schaller y Michael Schläpfer, *Applied Information Security*. Springer, 2011. ISBN 978-3-642-24473-5.

i. Recursos necesarios

Todas las referencias web y el software necesario se pondrá a disposición de los alumnos a través de la página de la asignatura en el campus virtual, incluyendo las herramientas de evaluación cruzada entre pares que requiere la evaluación de los proyectos de seguridad elaborados por los grupos de trabajo formados por alumnos de la asignatura.

6. Temporalización (por bloques temáticos)

BLOQUE TEMÁTICO	CARGA ECTS	PERIODO PREVISTO DE DESARROLLO
Bloque 1: Fundamentos de Seguridad de la Información	1,2 ECTS	Semanas 1 a 3
Bloque 2: Protección y Garantía de la Información	3,2 ECTS	Semanas 4 a 11
Bloque 3: Gestión de la seguridad de la Información	1,6 ECTS	Semanas 12 a 15

7. Sistema de calificaciones – Tabla resumen

Cada una de las actividades dirigidas que realizará el alumno, será objeto de valoración y será tenida en cuenta en el momento de medir la consecución de los resultados de aprendizaje contenidos en esta asignatura. Se procurará que el alumno tenga a su disposición lo antes posible una realimentación adecuada que le permita dirigir su trabajo y sus actividades de estudio. Entre los instrumentos que se contemplan con este fin se incluyen los siguientes elementos: Cuestionarios de teoría, entregas de ejercicios prácticos, el desarrollo documental de un proyecto práctico de seguridad, y la subsiguiente presentación pública del proyecto desarrollado.

Mediante los cuestionarios, el alumnado recibe una realimentación de los objetivos cognitivos conseguidos hasta el momento, sobre preguntas similares a las que se propondrán en el Examen de teoría normativo, y su influencia en la nota se presenta como algo atractivo, pero no es imprescindible para conseguir la evaluación final positiva. Las entregas de ejercicios prácticos y la realización y presentación del proyecto son instrumentos de progreso colaborativo e individual, deben ser evaluados para constatar los resultados de aprendizaje correspondientes a las habilidades específicas que cubre la asignatura, además de los objetivos transversales de aprendizaje como son la capacidad de planificación, de trabajar en grupo y de comunicación. Es preciso obtener una calificación suficiente en esta parte, para obtener una evaluación final positiva en la convocatoria ordinaria.

Finalmente, se propondrá una prueba de competencias teóricas (Examen de teoría) como viene siendo habitual que habrá que superar satisfactoriamente para superar la asignatura, si bien su peso en la nota final en la convocatoria ordinaria es del 40%.

Tal y como exige el reglamento de ordenación académica de la Uva se proponen instrumentos de evaluación alternativos para la convocatoria extraordinaria, con el fin de proporcionar criterios de calificación para el caso de que el alumno no supere la convocatoria extraordinaria.

En este caso la prueba de competencias teóricas cobra mayor importancia supliendo la imposibilidad de medir por otros cauces la consecución de ciertas habilidades que se encomendaban a la entrega de ejercicios de laboratorio. La parte práctica queda relegada a la elaboración de un proyecto, con la misma importancia que en la convocatoria ordinaria. Tanto en la parte teórica como en la práctica es preciso conseguir un nivel satisfactorio en cada una de las dos partes.

INSTRUMENTO/PROCEDIMIENTO	PESO EN LA NOTA FINAL	OBSERVACIONES
Cuestionarios Teoría (2 x 1 hora)	15 %	Examen parcial contenidos teóricos. Semana 4 y Semana 12
Entregas ejercicios prácticos (5 x 3%)	15 %	Trabajo contínuo práctico. Semanas 2, 5, 7, 9 y 11
Proyecto práctico seguridad	20 %	Informe de desarrollo del proyecto. Semana 16
Presentación Proyecto Práctico	10 %	Presentación y defensa del proyecto Semana 15
Examen de teoría	40 %	Ver calendario exámenes

CRITERIOS DE CALIFICACIÓN
Para superar la asignatura deben cumplirse todas las condiciones siguientes: • Superar satisfactoriamente la parte práctica, es decir obtener al menos el 50% de la máxima calificación en la parte práctica (entregas ejercicios + proyecto práctico + presentación). • Superar satisfactoriamente la parte teórica, en concreto obtener al menos el 40% de la máxima calificación en el examen de teoría o al menos el 50% de la máxima calificación del examen de teoría más los cuestionarios. • Obtener al menos una calificación final de 5,0. **Convocatoria extraordinaria**: • El examen de teoría representará el 70% de la calificación final. Es preciso superar esta prueba satisfactoriamente. • Se desarrollará un supuesto práctico que representará el 30% de la calificación final. Es preciso superar esta prueba satisfactoriamente. • El enunciado del supuesto práctico se publicará al finalizar el periodo de convocatoria ordinaria. • Obtener al menos una calificación final de 5,0.

8. Anexo: Métodos docentes

Actividad	Metodología
Clase de teoría	• Clase magistral participativa. • Estudio de casos en aula. • Resolución de problemas.
Clase práctica	• Resolución de problemas prácticos en laboratorio. • Realización de un proyecto guiado por el profesor, que encargará y guiará el trabajo que se realizará en grupos de 3 alumnos siguiendo un enfoque colaborativo.
Seminarios	• Talleres de presentación de trabajos monográficos y revisión de proceso de aprendizaje.
Tutoría	• Seguimiento de trabajo del alumno y atención de consultas y dudas.

9. Anexo: Cronograma de actividades previstas

El **plan de trabajo detallado definitivo estará disponible antes del comienzo de clases**.

Sem	FECHA	T	L	S	E	CONTENIDOS/ACTIVIDADES	ENTREGAS	EVAL (%)	HP	HNP
S1	24/09/12	2	2			**Bloque 1. Fundamentos de Seguridad de la Información**			4	6
S2	01/10/12	2	2			**Bloque 1. Fundamentos de Seguridad de la Información**	Práctica P1 Red	**3%**	4	6
S3	08/10/12	2	2			**Bloque 1. Fundamentos de Seguridad de la Información**			4	6
S4	15/10/12	2		2		**Bloque 2. Protección y Garantía de la Información** ***Entrega del enunciado de Proyecto***	**Cuestionario C1**	**5%**	4	6
S5	22/10/12	2	2			**Bloque 2. Protección y Garantía de la Información**	Práctica P2 Usuarios	**3%**	4	6
S6	29/10/12	2	2			**Bloque 2. Protección y Garantía de la Información**			4	6
S7	05/11/12	2	2			**Bloque 2. Protección y Garantía de la Información**	Práctica P3 Logs	**3%**	4	6
S8	12/11/12	2	2			**Bloque 2. Protección y Garantía de la Información**			4	5
S9	19/11/12	2		2		**Bloque 2. Protección y Garantía de la Información**	Práctica P4 Certificados	**3%**	4	6
S10	26/11/12	2	2			**Bloque 2. Protección y Garantía de la Información**			4	4
S11	03/12/12	2	2			**Bloque 2. Protección y Garantía de la Información**	Práctica P5 Web	**3%**	4	4
S12	10/12/12	2	2			**Bloque 3. Gestión de la seguridad de la Información**	**Cuestionario C2**	**10%**	4	6
S13	17/12/12	2	2			**Bloque 3. Gestión de la seguridad de la Información**			4	6
S14	07/01/13	2	2			**Bloque 3. Gestión de la seguridad de la Información**			4	6
S15	14/01/13	2		2		**Bloque 3. Gestión de la seguridad de la Información**	**Presentación Proyecto**	**10%**	4	8
S16	21/01/13					***ENTREGAS Y EVALUACIÓN FINAL***	**Entrega Informe Proyecto**	**20%**	0	
S17	28/01/13				2	***ENTREGAS Y EVALUACIÓN FINAL***	**Examen**	**40%**	2	
S18	04/02/13					***ENTREGAS Y EVALUACIÓN FINAL***			0	
TOTALES		30	24	6	2			**100%**	62	87

PRESENCIAL **62** ***DEDICACIÓN ALUMNO*** **149**