



UNIVERSIDAD  
POLITÉCNICA  
DE MADRID

PROCESO DE  
COORDINACIÓN DE LAS  
ENSEÑANZAS PR/CL/001



E.T.S. de Ingenieros  
Informaticos

# ANX-PR/CL/001-01

## GUÍA DE APRENDIZAJE

### ASIGNATURA

**105000030 - Seguridad De Las Tecnologias De La Informacion**

### PLAN DE ESTUDIOS

10II - Grado En Ingenieria Informatica

### CURSO ACADÉMICO Y SEMESTRE

2023/24 - Primer semestre

## Índice

---

### Guía de Aprendizaje

1. Datos descriptivos.....	1
2. Profesorado.....	1
3. Conocimientos previos recomendados.....	2
4. Competencias y resultados de aprendizaje.....	2
5. Descripción de la asignatura y temario.....	3
6. Cronograma.....	5
7. Actividades y criterios de evaluación.....	7
8. Recursos didácticos.....	9
9. Otra información.....	11

## 1. Datos descriptivos

### 1.1. Datos de la asignatura

<b>Nombre de la asignatura</b>	105000030 - Seguridad de las Tecnologías de la Información
<b>No de créditos</b>	6 ECTS
<b>Carácter</b>	Obligatoria
<b>Curso</b>	Tercero curso
<b>Semestre</b>	Quinto semestre
<b>Período de impartición</b>	Septiembre-Enero
<b>Idioma de impartición</b>	Castellano
<b>Titulación</b>	10II - Grado en Ingeniería Informática
<b>Centro responsable de la titulación</b>	10 - Escuela Técnica Superior De Ingenieros Informaticos
<b>Curso académico</b>	2023-24

## 2. Profesorado

### 2.1. Profesorado implicado en la docencia

<b>Nombre</b>	<b>Despacho</b>	<b>Correo electrónico</b>	<b>Horario de tutorías</b> *
Maria Del Socorro Bernardos Galindo	5206	mariadelsocorro.bernardos@upm.es	M - 08:00 - 11:00 J - 08:00 - 11:00
Jorge Davila Muro (Coordinador/a)	5205	jorge.davila@upm.es	J - 12:00 - 14:00 V - 12:00 - 14:00
Alberto Juan Sebastian Lombraña	5206	aj.sebastian@upm.es	L - 15:30 - 17:30 X - 15:30 - 17:30

\* Las horas de tutoría son orientativas y pueden sufrir modificaciones. Se deberá confirmar los horarios de tutorías con el profesorado.

## 3. Conocimientos previos recomendados

---

### 3.1. Asignaturas previas que se recomienda haber cursado

El plan de estudios Grado en Ingeniería Informática no tiene definidas asignaturas previas recomendadas para esta asignatura.

### 3.2. Otros conocimientos previos recomendados para cursar la asignatura

- Saber programar suficientemente bien en algún lenguaje como C, Python o Java
- Saber escribir y compilar programas que utilicen utilizar librerías de código tanto de forma dinámica como estática.

## 4. Competencias y resultados de aprendizaje

---

### 4.1. Competencias

CG-1/21 - Capacidad de resolución de problemas aplicando conocimientos de matemáticas, ciencias e ingeniería.

CG-19 - Capacidad de usar las tecnologías de la información y la comunicación.

Ce 22 - Capacidad de aplicar sus conocimientos e intuición para diseñar el hardware/software que cumple unos requisitos especificados.

Ce 26/27 - Definir, evaluar y seleccionar plataformas hardware y software, incluyendo el sistema operativo, y concebir, llevar a cabo, instalar y mantener arquitecturas informáticas centralizadas o distribuidas integrando hardware, software y redes.

Ce 29 - Diseñar, desarrollar, y evaluar la seguridad de los sistemas, aplicaciones, servicios informáticos y sistemas operativos sobre los que se ejecutan, así como de la información que proporcionan.

Ce 6 - Comprender intelectualmente el papel central que tienen los algoritmos y las estructuras de datos, así como una apreciación del mismo.

Ce 8 - Poseer destrezas fundamentales de la programación que permitan la implementación de los algoritmos y las estructuras de datos en el software.

## 4.2. Resultados del aprendizaje

RA506 - Conocer y comprender la importancia de la seguridad para la empresa.

RA358 - Identificar riesgos y posibles ataques

RA360 - Conocimiento actualizado de soluciones de seguridad para la Sociedad de la Sociedad de la Información

RA317 - Fundamentos, criptografía y criptoanálisis.

RA359 - Conocer, comprender y saber utilizar servicios criptográficos para la obtención de seguridad.

RA318 - Seguridad de los Datos de carácter Personal.

RA319 - Arquitectura de Seguridad y de Red frente a incidencias y ataques.

## 5. Descripción de la asignatura y temario

---

### 5.1. Descripción de la asignatura

El objetivo de esta asignatura es hacer comprender a los alumnos el papel central que tienen los algoritmos y las estructuras de datos en la seguridad de los sistemas informáticos. Con ella se pretende que el alumno adquiera destrezas fundamentales en el uso, programación e implementación de algoritmos y sistemas que proporcionen seguridad a las TIC. Para ello el alumno habrá que aplicar conocimientos e intuición en el diseño de soluciones válidas según requisitos de seguridad especificados.

El objetivo global es que el alumno pueda llegar a diseñar, desarrollar y evaluar la Seguridad de sistemas, aplicaciones y servicios informáticos de todo tipo. Los conocimientos adquiridos siempre apuntarán al desarrollo, despliegue, organización y gestión de servicios informáticos en contextos empresariales que realmente puedan mejorar los procesos de negocio. En esta asignatura se favorecerá la capacidad del alumno en la resolución de problemas de seguridad recurriendo a los conocimientos que sean necesarios (matemáticas, ciencias, ingeniería, etc.).

Al final, el alumno conocerá y comprenderá la importancia que tiene la seguridad informática para las Administraciones y Empresas, serán capaces de identificar riesgos y posibles ataques. Para ello conocerá, comprenderá y sabrá utilizar servicios criptográficos para proporcionar seguridad TIC y conocerá algunas soluciones de seguridad que están disponibles y son válidas para la protección de la Sociedad de la Información.

## 5.2. Temario de la asignatura

1. Soluciones Criptográficas
  - 1.1. Metodos de Sustitución
  - 1.2. Métodos de Transposición
  - 1.3. Máquinas de Cifrado
2. Criptoanálisis Clásico
3. Algoritmos de Cifrado Actuales
  - 3.1. Cifradores Simétricos
  - 3.2. Funciones Hash
  - 3.3. Cifradores Asimétricos
4. Control de Accesos y Autenticación
5. Código Malicioso y medidas en contra
6. Uso de Librerías Criptográficas.
  - 6.1. Scripting y Criptografía/Criptoanálisis clásico
  - 6.2. OpenSSL, GnuPG, y otras librerías
  - 6.3. Correo Electronico Cifrado y Autenticado (PGP y sMIME)
  - 6.4. Identidad Digital, PKIs y Certificados x509v3

## 6. Cronograma

### 6.1. Cronograma de la asignatura \*

Sem	Actividad en aula	Actividad en laboratorio	Tele-enseñanza	Actividades de evaluación
1	<b>Clase de teoría</b> Duración: 02:00 LM: Actividad del tipo Lección Magistral			
2	<b>Clase de teoría</b> Duración: 04:00 LM: Actividad del tipo Lección Magistral			
3	<b>Clase de teoría</b> Duración: 04:00 LM: Actividad del tipo Lección Magistral			
4	<b>Clase de teoría</b> Duración: 04:00 LM: Actividad del tipo Lección Magistral			
5	<b>Clase de teoría</b> Duración: 04:00 LM: Actividad del tipo Lección Magistral			
6	<b>Clase de teoría</b> Duración: 04:00 LM: Actividad del tipo Lección Magistral			<b>Ejercicio Telemático Individual</b> <b>Evaluacion Progresiva del Bloque I del Temario</b> ET: Técnica del tipo Prueba Telemática Evaluación continua No presencial Duración: 01:00
7	<b>Clase de teoría</b> Duración: 04:00 LM: Actividad del tipo Lección Magistral			
8	<b>Clase de teoría</b> Duración: 04:00 LM: Actividad del tipo Lección Magistral			
9	<b>Clase de teoría</b> Duración: 04:00 LM: Actividad del tipo Lección Magistral			
10	<b>Clase de teoría</b> Duración: 04:00 LM: Actividad del tipo Lección Magistral			
11	<b>Clase de teoría</b> Duración: 04:00 LM: Actividad del tipo Lección Magistral			
12	<b>Clase de teoría</b> Duración: 04:00 LM: Actividad del tipo Lección Magistral			<b>Ejercicio Telemático Individual</b> <b>Evaluacion Progresiva del Bloque II del Temario</b> ET: Técnica del tipo Prueba Telemática Evaluación continua No presencial Duración: 01:00

13	<b>Clase de teoría</b> Duración: 04:00 LM: Actividad del tipo Lección Magistral			
14	<b>Clase de teoría</b> Duración: 02:00 LM: Actividad del tipo Lección Magistral			
15	<b>Clase de teoría</b> Duración: 04:00 LM: Actividad del tipo Lección Magistral			
16	<b>Clase de teoría</b> Duración: 02:00 LM: Actividad del tipo Lección Magistral			<b>Ejercicio Telemático Individual</b> <b>Evaluación Progresiva del Bloque III del Temario</b> ET: Técnica del tipo Prueba Telemática Evaluación continua No presencial Duración: 01:00
17				<b>Examen Presencial de aquellas pruebas/Bloques que no haya aprobado previamente mediante Evaluación Progresiva</b> EX: Técnica del tipo Examen Escrito Evaluación sólo prueba final Presencial Duración: 02:00

Para el cálculo de los valores totales, se estima que por cada crédito ECTS el alumno dedicará dependiendo del plan de estudios, entre 26 y 27 horas de trabajo presencial y no presencial.



## 7. Actividades y criterios de evaluación

### 7.1. Actividades de evaluación de la asignatura

#### 7.1.1. Evaluación (progresiva)

Sem.	Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
6	Ejercicio Telemático Individual Evaluación Progresiva del Bloque I del Temario	ET: Técnica del tipo Prueba Telemática	No Presencial	01:00	38%	0 / 10	CG-1/21 CG-19 Ce 6 Ce 8 Ce 22 Ce 26/27 Ce 29
12	Ejercicio Telemático Individual Evaluación Progresiva del Bloque II del Temario	ET: Técnica del tipo Prueba Telemática	No Presencial	01:00	38%	0 / 10	CG-1/21 CG-19 Ce 6 Ce 8 Ce 22 Ce 26/27 Ce 29
16	Ejercicio Telemático Individual Evaluación Progresiva del Bloque III del Temario	ET: Técnica del tipo Prueba Telemática	No Presencial	01:00	24%	0 / 10	CG-1/21 CG-19 Ce 6 Ce 8 Ce 22

#### 7.1.2. Prueba evaluación global

Sem	Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
17	Examen Presencial de aquellas pruebas/Bloques que no haya aprobado previamente mediante Evaluación Progresiva	EX: Técnica del tipo Examen Escrito	Presencial	02:00	100%	0 / 10	CG-1/21 CG-19 Ce 6 Ce 8 Ce 22 Ce 26/27 Ce 29

#### 7.1.3. Evaluación convocatoria extraordinaria

Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
Examen Presencial de Toda la Asignatura (Bloques I y II)	EX: Técnica del tipo Examen Escrito	Presencial	02:00	100%	0 / 10	CG-1/21 CG-19 Ce 6 Ce 8 Ce 22 Ce 26/27 Ce 29

## 7.2. Criterios de evaluación

La evaluación progresiva de esta asignatura estará organizada en TRES ejercicios telemáticos individuales obligatorios.

Los ejercicios SUSPENSOS de Evaluación Progresiva deberán volverse a examinar en la prueba presencial de la Convocatoria Ordinaria.

La nota final de la asignatura será la media aritmética ponderada de las mejores calificaciones obtenidas en cada bloque tanto si se ha examinado en Evaluación Progresiva como en la Convocatoria Ordinaria.

Las pruebas obligatorias son TRES exámenes no presenciales en los que el alumno deberá responder correctamente y por escrito a las preguntas y enunciados que se le planteen. Estos exámenes se celebraran en las fechas y plataformas (Moodle) establecidas para ello en el calendario de la asignatura y disponibles en cada momento.

En el caso de no aprobarse la asignatura y tener que concurrir al examen de la Convocatoria Extraordinaria, el alumno/a tendrá que examinarse de todo el temario. No se guardan resultados entre convocatorias.

La puntuación correspondiente a cada examen por Evaluación Progresiva (Bloque I, Bloque II y Bloque III) supondrá un 38 %, 38 % y 24 % de la nota final del alumno respectivamente.

Es criterio de evaluación es la correcta respuesta a las preguntas planteadas a cada alumno, así como correcta satisfacción de los objetivos marcados en cualquier ejercicio práctico individual que se le plantee.

Cumplir las normas que se establezcan para la asignación de tareas así como para la entrega de materiales y resultados.

Podrán acudir a la Convocatoria Ordinaria aquellos alumnos que no hayan superado alguna de la pruebas de la Evaluación Progresiva, en cuyo caso se examinarán solo de las pruebas que no tenga aprobadas.

Acudirán a la Convocatoria Extraordinaria, aquellos alumnos que no hayan aprobado la asignatura ni mediante la Evaluación Progresiva ni en la Convocatoria Ordinaria. En este caso, los alumnos se examinarán de todo el temario de la asignatura, independientemente de los resultados que haya podido obtener en Evaluación Progresiva o en la Convocatoria Ordinaria.

## 8. Recursos didácticos

---

### 8.1. Recursos didácticos de la asignatura

Nombre	Tipo	Observaciones
Applied Cryptography. Protocols, Algorithms, and Source Code in C	Bibliografía	2nd Edition, Bruce Schneier (Author) ISBN-10: 0471117099 ISBN-13: 978-0471117094
Practical Cryptography	Bibliografía	Niels Ferguson (Author), Bruce Schneier (Author) ISBN-10: 0471223573 ISBN-13: 978-0471223573
Handbook of Applied Cryptography. Discrete Mathematics and Its Applications	Bibliografía	Alfred Menezes, Paul van Oorschot y Scott Vanstone (Editores) ISBN-10: 0849385237 ISBN-13: 978-0849385230
Cryptography and Network Security. Principles and Practice,	Bibliografía	5th Edition, William Stallings (Author) ISBN-10: 0136097049 ISBN-13: 978-0136097044
Cryptography for Developers,	Bibliografía	Tom St Denis (Author) ISBN-10: 1597491047 ISBN-13: 978-1597491044

BigNum Math: Implementing Cryptographic Multiple Precision Arithmetic.	Bibliografía	Tom St Denis (Author) ISBN-10: 1597491128 ISBN-13: 978-1597491129
Codes, Ciphers, Secrets and Cryptic Communication. Making and Breaking Secret Messages from Hieroglyphs to the Internet,	Bibliografía	Fred B. Wrixon (Author) ISBN-10: 1579124852 ISBN-13: 978-1579124854
The Code Book. The Science of Secrecy from Ancient Egypt to Quantum Cryptography,	Bibliografía	Simon Singh (Author) ISBN-10: 0385495323 ISBN-13: 978-0385495325
The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet,	Bibliografía	David Kahn (Author) ISBN-10: 0684831309 ISBN-13: 978-0684831305
Security in Computing	Bibliografía	(4ª ed.). Charles P. Pfleeger y Shari Lawrence Pfleeger. Prentice Hall (2006) ISBN-10: 0132390779, ISBN-13: 978-0132390774
Network Security: Private Communication in a Public World	Bibliografía	(2ª ed). Charlie Kaufman, Radia Perlman y Mike Speciner. Prentice Hall (2002) ISBN-10: 0130460192, ISBN-13: 978-0130460196
Computer Security Basics	Bibliografía	(2ª ed.) Rick Lehtinen y G.T. Gangemi. O'Reilly Media, Inc. (2006) ISBN-10: 0596006691, ISBN-13: 978-0596006693
Computer Security	Bibliografía	(2ª ed.). Dieter Gollmann. Wiley (2006) ISBN-10: 0470862939, ISBN-13: 978-0470862933
Introduction to Computer Security.	Bibliografía	Matt Bishop. Addison-Wesley Professional (November 5, 2004) ISBN-10: 0321247442, ISBN-13: 978-0321247445
Fundamentals Of Computer	Bibliografía	Security, Josef Pieprzyk, Thomas Hardjono, Jennifer Seberry ISBN: 3540431012, ISBN-13: 9783540431015, 978-3540431015. Springer 2003

## 9. Otra información

---

### 9.1. Otra información sobre la asignatura

En el desarrollo de los **Bloques I y II** la asistencia a clase **NO es obligatoria**, sin embargo, en el desarrollo del **Bloque III** de la asignatura, la asistencia a clase **SI es OBLIGATORIA**. En cualquier caso, el comportamiento de los asistentes deberá ser respetuoso y correcto con todos los demás.

El alumno deberá colaborar en el adecuado desarrollo de las clases y demás actividades formativas del curso.

Antes de acudir a una tutoría, el alumno deberá solicitar cita para ello con el profesorado mediante un **correo electrónico** indicando tal interés.

El profesorado de la asignatura se reserva la potestad de dividir o reunir grupos para el desarrollo de temas específicos si el desarrollo del temario y sus actividades asociadas así lo aconsejan.

Si el desarrollo de la asignatura así lo requiriese o aconsejase, el profesorado de reserva la potestad de cambiar el orden en el que se exponen y desarrollan los distintos bloques que constituyen el temario de la asignatura.

Para el correcto desarrollo de esta asignatura, todos los alumnos deberán utilizar la plataforma Moodle en la que están registrados automáticamente como consecuencia de su matrícula en ella.

Tanto en las **pruebas/exámenes telemáticas** como en las **pruebas/exámenes presenciales**, queda **terminantemente PROHIBIDO** el uso de **cualquier material o información que no este contenida en el enunciado** de la prueba.

Está prohibido el plagio tanto en las memorias, como en los códigos o en el software que se desarrolle. En todos los casos el alumno deberá indicar explícitamente y con detalle de dónde han salido y cuál es el origen de los materiales que utiliza.

Está prohibida la mera traducción de artículos académicos o de cualquier otra índole. El uso de traductores

automáticos está completamente prohibido.

Las incorrecciones sintácticas, ortográficas y semánticas del lenguaje utilizado podrán ser penalizadas.

Cualquier sospecha sobre la autoría de un examen, un ejercicio individual o una práctica, llevará inexorablemente al Examen Oral de la asignatura y parte del cuál será la defensa de lo expuesto en su entrega (examen, memoria, código, ejecutables, etc.).