

Escuela Superior de Ingeniería y Tecnología

Grado en Ingeniería Informática

GUÍA DOCENTE DE LA ASIGNATURA :

**Seguridad de Sistemas Informáticos
(2022 - 2023)**

1. Datos descriptivos de la asignatura

Asignatura: Seguridad de Sistemas Informáticos	Código: 139264213
<ul style="list-style-type: none">- Centro: Escuela Superior de Ingeniería y Tecnología- Lugar de impartición: Escuela Superior de Ingeniería y Tecnología- Titulación: Grado en Ingeniería Informática- Plan de Estudios: 2010 (Publicado en 2011-03-21)- Rama de conocimiento: Ingeniería y Arquitectura- Itinerario / Intensificación:- Departamento/s: Ingeniería Informática y de Sistemas- Área/s de conocimiento: Ciencia de la Computación e Inteligencia Artificial Lenguajes y Sistemas Informáticos- Curso: 4- Carácter: Obligatoria- Duración: Primer cuatrimestre- Créditos ECTS: 6,0- Modalidad de impartición: Presencial- Horario: Enlace al horario- Dirección web de la asignatura: http://www.campusvirtual.ull.es- Idioma: Español e Inglés	

2. Requisitos para cursar la asignatura

No existen requisitos para cursar la asignatura

3. Profesorado que imparte la asignatura

Profesor/a Coordinador/a: VICENTE JOSE BLANCO PEREZ
- Grupo: 1
General <ul style="list-style-type: none">- Nombre: VICENTE JOSE- Apellido: BLANCO PEREZ- Departamento: Ingeniería Informática y de Sistemas- Área de conocimiento: Lenguajes y Sistemas Informáticos

<p>Contacto</p> <ul style="list-style-type: none"> - Teléfono 1: 922 318 637 - Teléfono 2: - Correo electrónico: vblanco@ull.es - Correo alternativo: - Web: http://www.campusvirtual.ull.es 						
<p>Tutorías primer cuatrimestre:</p>						
Desde	Hasta	Día	Hora inicial	Hora final	Localización	Despacho
Todo el cuatrimestre		Lunes	11:00	13:00	Escuela Superior de Ingeniería y Tecnología - Módulo A - AN.4A ESIT	P3.015
Todo el cuatrimestre		Viernes	11:00	13:00	Escuela Superior de Ingeniería y Tecnología - Módulo A - AN.4A ESIT	P3.015
Todo el cuatrimestre		Miércoles	15:00	17:00	Escuela Superior de Ingeniería y Tecnología - Módulo A - AN.4A ESIT	P3.015
<p>Observaciones: Visitar aula virtual o http://goo.gl/CyVIUw. Las dos horas de tutoría de los viernes serán online debido a la participación en el Programa de Apoyo a la Docencia Presencial mediante Herramientas TIC, modalidad B Tutorías Online. Para llevar a cabo la tutoría online, usaremos la herramienta Hangouts, enlazada con los eventos de mi calendario de tutorías con reserva de cita</p>						
<p>Tutorías segundo cuatrimestre:</p>						
Desde	Hasta	Día	Hora inicial	Hora final	Localización	Despacho
Todo el cuatrimestre		Lunes	11:00	13:00	Escuela Superior de Ingeniería y Tecnología - Módulo A - AN.4A ESIT	P3.015

Todo el cuatrimestre		Viernes	11:00	13:00	Escuela Superior de Ingeniería y Tecnología - Módulo A - AN.4A ESIT	P3.015
Todo el cuatrimestre		Miércoles	15:00	17:00	Escuela Superior de Ingeniería y Tecnología - Módulo A - AN.4A ESIT	P3.015

Observaciones: Visitar aula virtual o <http://goo.gl/CyVIUw>. Las dos horas de tutoría de los viernes serán online debido a la participación en el Programa de Apoyo a la Docencia Presencial mediante Herramientas TIC, modalidad B Tutorías Online. Para llevar a cabo la tutoría online, usaremos la herramienta Hangouts, enlazada con los eventos de mi calendario de tutorías con reserva de cita

Profesora/a: MARIA CANDELARIA HERNANDEZ GOYA

- Grupo: 1

General

- Nombre: **MARIA CANDELARIA**
- Apellido: **HERNANDEZ GOYA**
- Departamento: **Ingeniería Informática y de Sistemas**
- Área de conocimiento: **Ciencia de la Computación e Inteligencia Artificial**

Contacto

- Teléfono 1: **922 316 502 Ext 6827**
- Teléfono 2: **922 316 502 Ext 6827**
- Correo electrónico: **mchgoya@ull.es**
- Correo alternativo:
- Web: **<http://www.campusvirtual.ull.es>**

Tutorías primer cuatrimestre:

Desde	Hasta	Día	Hora inicial	Hora final	Localización	Despacho
Todo el cuatrimestre		Martes	10:00	12:00	Escuela Superior de Ingeniería y Tecnología - Módulo A - AN.4A ESIT	P2.026

Todo el cuatrimestre		Jueves	10:00	12:00	Escuela Superior de Ingeniería y Tecnología - Módulo A - AN.4A ESIT	P2.026
Todo el cuatrimestre		Miércoles	10:00	12:00	Escuela Superior de Ingeniería y Tecnología - Módulo A - AN.4A ESIT	P2.026

Observaciones: Las modificaciones de este horario por causas sobrevenidas se comunicarán a través del campus virtual. Las tutorías de los jueves, de 10:00 a 12:00, serán en línea. Para llevar a cabo la tutoría en línea se hará uso del Google Meet <https://meet.google.com/rrii-asrj-dxt>

Tutorías segundo cuatrimestre:

Desde	Hasta	Día	Hora inicial	Hora final	Localización	Despacho
Todo el cuatrimestre		Martes	12:00	14:00	Escuela Superior de Ingeniería y Tecnología - Módulo A - AN.4A ESIT	P2.026
Todo el cuatrimestre		Miércoles	12:00	14:00	Escuela Superior de Ingeniería y Tecnología - Módulo A - AN.4A ESIT	P2.026
Todo el cuatrimestre		Viernes	10:00	12:00	Escuela Superior de Ingeniería y Tecnología - Módulo A - AN.4A ESIT	P2.026

Observaciones: Las modificaciones de este horario por causas sobrevenidas se comunicarán a través del campus virtual. Las tutorías de los viernes, de 10:00 a 12:00, serán en línea. Para llevar a cabo la tutoría en línea se hará uso del Google Meet <https://meet.google.com/bfv-ajyu-xhe>.

4. Contextualización de la asignatura en el plan de estudio

Bloque formativo al que pertenece la asignatura: **Itinerario 2: Ingeniería de Computadores**
 Perfil profesional: **Ingeniero Técnico en Informática**

5. Competencias

Tecnología Específica / Itinerario: Ingeniería de Computadores

C36 - Capacidad para comprender, aplicar y gestionar la garantía y seguridad de los sistemas informáticos.

Competencias Generales

CG4 - Capacidad para definir, evaluar y seleccionar plataformas hardware y software para el desarrollo y la ejecución de sistemas, servicios y aplicaciones informáticas, de acuerdo con los conocimientos adquiridos según lo establecido en el apartado 5 de este anexo.

CG6 - Capacidad para concebir y desarrollar sistemas o arquitecturas informáticas centralizadas o distribuidas integrando hardware, software y redes de acuerdo con los conocimientos adquiridos según lo establecido en el apartado 5 de este anexo.

Transversales

T1 - Capacidad de actuar autónomamente.

T2 - Tener iniciativa y ser resolutivo.

T3 - Tener iniciativa para aportar y/o evaluar soluciones alternativas o novedosas a los problemas, demostrando flexibilidad y profesionalidad a la hora de considerar distintos criterios de evaluación.

T4 - Actuar en el desarrollo profesional con responsabilidad y ética profesional y de acuerdo con la legislación vigente.

T6 - Capacidad de comunicación efectiva en inglés.

T9 - Capacidad para argumentar y justificar lógicamente las decisiones tomadas y las opiniones.

T16 - Capacidad de planificación y organización del trabajo personal.

T18 - Tener motivación por la calidad y la mejora continua y actuar con rigor en el desarrollo profesional.

T19 - Capacidad de adaptación a los cambios organizativos o tecnológicos.

T25 - Capacidad de análisis, síntesis y evaluación.

Módulo Redes de Computadores y Seguridad

E4 - Capacidad para dimensionar y gestionar adecuadamente servicios de red.

E5 - Capacidad para plantear, defender y ejecutar un proyecto de red.

Módulo Sistemas Operativos Avanzados, Redes y Seguridad

E6 - Conocer, comprender y saber implementar y gestionar una PKI.

E7 - Conocer y comprender los tipos de ataques más habituales para desarrollar medidas de protección contra ellos.

E8 - Conocer y comprender las aplicaciones y protocolos criptográficos más utilizados.

E9 - Conocer, comprender y saber gestionar los algoritmos que conforman la arquitectura de seguridad de los sistemas informáticos actuales.

E10 - Conocer y comprender los procedimientos criptográficos que se utilizan al gestionar una red informática de modo seguro.

6. Contenidos de la asignatura

Contenidos teóricos y prácticos de la asignatura

- Profesor/a: Candelaria Hernández Goya

- Temas (epígrafes):

- 1.- Preliminares y Conceptos Básicos: Introducción a la Criptografía. Confidencialidad de la información: clave secreta y clave pública. Integridad de la Información: funciones Hash. Firma Digital.
- 2.- Infraestructura de Clave Pública (PKI): Despliegue, certificación y revocación. Estándar X.509. OpenPGP
- 3.- Comercio Electrónico: Medios de pago en Internet. Dinero electrónico

- Profesor/a: José Ángel Concepción Sánchez

Contenidos prácticos en los temas Temas (epígrafes):

- 1.- Preliminares y Conceptos Básicos: Introducción a la Criptografía. Confidencialidad de la información: clave secreta y clave pública. Integridad de la Información: funciones Hash. Firma Digital.
- 2.- Infraestructura de Clave Pública (PKI): Despliegue, certificación y revocación. Estándar X.509. OpenPGP
- 3.- Comercio Electrónico: Medios de pago en Internet. Dinero electrónico

- Profesor/a: Vicente José Blanco Pérez

- Temas (epígrafes):

- 4.- Comunicaciones Seguras: Protocolos: IPsec. Seguridad Perimetral: firewalls. Interceptación de comunicaciones: tipos. Redes privadas virtuales (VPNs).
- 5.- Esquemas de Control de Accesos y Autenticación: Contraseñas (fijas y de un solo uso). Esquemas Reto-Respuesta. Kerberos. Modelos DAC y MAC. Sistemas de Ficheros. Hardening Sistema Operativo.
- 6.- Evaluación y Protección de la Seguridad: Monitorización y Auditoría. Sistemas de detección de intrusos. Informática Forense

Actividades a desarrollar en otro idioma

Se visualizarán en las sesiones de prácticas vídeos y screencast (5h) en inglés relacionados con las actividades propuestas en estas sesiones. La bibliografía y la documentación así como algunas presentaciones estarán disponibles en inglés.

7. Metodología y volumen de trabajo del estudiante

Descripción

- * Enseñanza expositiva: clases teóricas donde el profesor expone los conceptos teóricos de la asignatura y clases prácticas o de problemas donde se estudiarán ejemplos prácticos. Se espera que tanto las clases teóricas como las prácticas sean participativas
- * Tutorías individuales presenciales o virtuales a través del portal de la asignatura.
- * Realización de trabajos/proyectos propuestos por el profesor que serán de tipo práctico y podrán realizarse dentro o fuera del aula virtual, y que serán el material utilizado para la evaluación continua.
- * La asignatura participa en el Programa de Apoyo a la Docencia Presencial en la modalidad A: asignaturas. La metodología de trabajo a desarrollar en el aula virtual se centra en realizar las actividades de evaluación de respuesta corta para cada tema, que se llevarán a cabo durante 30m en cada sesión de laboratorio. Se utilizarán foros en la plataforma virtual como

herramienta de trabajo colaborativo. Se realizará alguna píldora educativa como soporte para la instalación de la infraestructura virtual (varias máquinas virtuales conectadas en red simulando una red corporativa) en la que se realizarán las prácticas de la asignatura. También participa en el Programa de Apoyo a la Docencia Presencial en la Modalidad C: Tutorías.

Actividades formativas en créditos ECTS, su metodología de enseñanza-aprendizaje y su relación con las competencias que debe adquirir el estudiante

Actividades formativas	Horas presenciales	Horas de trabajo autónomo	Total horas	Relación con competencias
Clases teóricas	15,00	0,00	15,0	[E10], [E9], [E8], [E7], [E6], [E5], [E4], [T25], [T19], [T18], [CG6], [CG4]
Clases prácticas (aula / sala de demostraciones / prácticas laboratorio)	35,00	0,00	35,0	[E10], [E9], [E8], [E7], [E6], [E5], [E4], [T25], [T19], [T18], [T16], [T9], [C36]
Realización de seminarios u otras actividades complementarias	0,00	10,00	10,0	[E8], [E7], [E6], [E5], [E4], [T25], [T19], [T18], [T16], [T9], [T4], [T3], [C36]
Realización de trabajos (individual/grupal)	0,00	40,00	40,0	[E10], [E9], [E8], [E7], [E6], [T25], [T19], [T16], [T9], [T6], [T3], [T1], [CG6], [CG4], [C36]
Estudio/preparación de clases teóricas	0,00	10,00	10,0	[E10], [E9], [E8], [E7], [E6], [T25], [T19], [T16], [T9], [T6], [T3], [T1], [CG6], [CG4], [C36]
Realización de exámenes	2,00	0,00	2,0	[E9], [E8], [E7], [E6], [T25], [T19], [T18], [T16], [T9], [T4], [T3], [CG6], [CG4], [C36]
Asistencia a tutorías	8,00	0,00	8,0	[E10], [E9], [E8], [E7], [E6], [T25], [T16], [T9], [CG6], [CG4], [C36]

Estudio autónomo individual o en grupo	0,00	30,00	30,0	[E10], [E9], [E8], [E7], [E6], [T25], [T18], [T16], [T9], [T6], [T4], [T3], [T2], [T1], [CG6], [CG4], [C36]
Total horas	60,00	90,00	150,00	
Total ECTS			6,00	

8. Bibliografía / Recursos

Bibliografía Básica

- * PKI Uncovered: Certificate-Based Security Solutions for Next-Generation Networks. Andre Karamanian, Srinivas Tenneti, Francois Dessart, 2011. Cisco Press. ISBN 978-1-58705-916-2
- * Network Security, Firewalls, and VPNs (Jones & Bartlett Learning Information Systems Security & Assurance) J. Michael Stewart. 2010 ISBN 978-0763791308
- * Security Strategies in Linux Platforms and Applications. Michael Jango. 2010 ISBN 978-0763791896

Bibliografía Complementaria

- * Security Strategies in Windows Platforms and Applications (J & B Learning Information Systems Security & Assurance Series) Michael G. Solomon. 2010 ISBN 978-0763791933
- * Hands-On Ethical Hacking and Network Defense. Michael T. Simpson, Kent Backman, James Corley 2010 ISBN 978-1435486096
- * Guide to Computer Forensics and Investigations. Bill Nelson, Amelia Phillips, Christopher Steuart. 2009 ISBN 978-1435498839
- * Digital Evidence and Computer Crime, Third Edition: Forensic Science, Computers, and the Internet Eoghan Casey BS MA. 2011 ISBN 978-0123742681

Otros Recursos

Campus virtual de la ULL

9. Sistema de evaluación y calificación

Descripción

La Evaluación de la asignatura se rige por el Reglamento de Evaluación y Calificación (REC) de la Universidad de La Laguna (Boletín Oficial de la Universidad de La Laguna de 23 de junio de 2022), o el que la Universidad tenga vigente, además de por lo establecido en la Memoria de Verificación o Modificación vigente. En virtud de dicho reglamento, todo el alumnado está sujeto a evaluación continua en la primera convocatoria de la asignatura, salvo el que se acoja a la evaluación única, lo que tendrá que ser comunicado por el propio alumnado en el plazo de un mes a partir del inicio del cuatrimestre correspondiente (ver art. 5.4 del REC), o transcurrido ese mes solo por circunstancias sobrevenidas (ver art. 5.5 del REC).

La asignatura de Seguridad en Sistemas Informáticos se enmarca dentro del módulo "Sistemas Operativos Avanzados, Redes y Seguridad" del Itinerario "Ingeniería de Computadores". El sistema de evaluación especificado en la Memoria del Título es 50% prueba final y 50% evaluación continua.

Evaluación Continua:

La asignatura se organiza en dos módulos en los que se aplica el sistema de evaluación según la Memoria de Verifica/Modifica para la titulación y que se desglosa en las siguientes pruebas:

Módulo I (34% del peso en la nota final obtenida).

- Prácticas Individuales (hasta 5), con un peso del 9% en la nota final obtenida.
- Cuestionarios sobre aspectos teóricos (hasta 5), con un peso del 9% en la nota final obtenida.
- Exámen final, con un peso del 17% en la nota final obtenida.

Módulo II (66% del peso en la nota final obtenida)

- Prácticas individuales (hasta 5), con un peso del 20% en la nota final obtenida.
- Prácticas grupales (hasta 4), con un peso del 13% en la nota final obtenida.
- Exámen final, con un peso del 33% en la nota final obtenida.

Todos estos epígrafes con sus correspondientes pesos están configurados en el calificador de Moodle de la asignatura.

Es obligatoria la asistencia a las clases, hacer uso de los foros y la realización de las actividades prácticas, informes y exámenes. Se podrá llevar a cabo control de asistencia.

Es necesario superar cada una de estas partes (prácticas, informes y exámenes) para superar la asignatura mediante evaluación continua.

La modalidad de evaluación continua se mantendrá en la segunda convocatoria. Por lo tanto, la segunda convocatoria (podrá utilizarse para recuperar las pruebas de evaluación continua no superadas antes del fin de la primera convocatoria de la asignatura).

Agotamiento de la Evaluación Continua:

En relación a la evaluación continua, conforme al artículo 4.7 del REC "se entenderá agotada la convocatoria desde que el alumnado se presente, al menos, a las actividades cuya ponderación compute el 50% de la evaluación continua, salvo en los casos recogidos en el artículo 5.5". Por lo tanto, una vez realizado cualquier conjunto de actividades cuya suma de ponderaciones alcance el 50% supone el agotamiento de la evaluación continua de la asignatura. Una vez agotada la evaluación continua la calificación en el acta no podrá ser "No presentado".

Obligatoriedad de las actividades:

Será obligatorio realizar todas las pruebas de evaluación propuestas. En ese caso, la calificación final (CF) o calificación en el acta se obtiene tras la aplicación de la siguiente fórmula:

- Si se realizan todas las pruebas de evaluación, entonces $CF = 0.25 * \text{Prácticas Individuales} + 0.25 * \text{Cuestionarios/Prácticas Grupales} + 0.5 \text{ Exámen}$.
- Si no se realizan todas las pruebas de evaluación, entonces:
 - Si se ha agotado la evaluación continua (se han realizado pruebas cuya suma de ponderaciones es mayor o igual al 50%), entonces $CF = \min(4.5 ; 0.25 * \text{Prácticas Individuales} + 0.25 * \text{Cuestionarios/Prácticas Grupales} + 0.5 \text{ Exámen})$
 - Si no se ha agotado la evaluación continua, entonces $CF = \text{"No Presentado"}$.

Evaluación única:

Si el alumnado no se evalúa de forma continua (por las circunstancias que se describen en el REC), debe evaluarse de todo el contenido teórico y práctico de la asignatura en la fecha oficial de convocatoria que figure en el calendario académico, circunstancia que debe ser comunicada al profesorado de la asignatura con una antelación mínima de 10 días respecto a la fecha oficial en la que el/la estudiante quiera presentarse.

La evaluación única se compondrá de dos pruebas:

Una prueba Teórica donde se evaluarán los contenidos impartidos en la asignatura, con una ponderación del 50% en la nota final obtenida y una prueba Práctica que consistirá en el desarrollo de un ejercicio práctico relacionado con los contenidos de la asignatura. Este ejercicio tendrá una ponderación del 50% en la nota final obtenida.

Si la realización de estas pruebas no puede realizarse el mismo día debido a su extensión, el profesorado convendrá con el alumnado una fecha alternativa para su realización. La ponderación de las distintas pruebas de evaluación en la CF de la asignatura es: $CF = 0.5 * C.Teórica + 0.5 * C.Práctica$.

Evaluación del 5% de inglés:

Las actividades en inglés de la asignatura que se describen en el apartado 6 serán evaluadas a través de la misma metodología que el resto de actividades, teniendo en cuenta que el inglés pudiera ser utilizado en la propia evaluación, tanto a la hora de formular las preguntas y/o ejercicios como a la hora de responderlas/resolverlos por parte del alumnado.

La estrategia evaluativa se detalla en la tabla que aparece a continuación. En ella se establecen los criterios de evaluación de las competencias que se desarrollan en esta asignatura, así como la ponderación de los mismos dentro de los distintos tipos de calificación descritos en los párrafos anteriores. En ningún caso se guardarán actividades para siguientes cursos académicos.

Estrategia Evaluativa

Tipo de prueba	Competencias	Criterios	Ponderación
Valoración de las actividades prácticas en el laboratorio	[E10], [E9], [E8], [E7], [E6], [T19], [T4], [T3], [T2], [T1], [CG6], [CG4], [C36]	* Adecuación a lo solicitado. * Participación activa e interés demostrado. * Calidad e interés de las implementaciones	25,00 %
Elaboración de informes	[E10], [E9], [E8], [E7], [E6], [T18], [T6], [T4], [T3], [T2], [T1], [CG6], [CG4], [C36]	* Adecuación a lo solicitado. * Concreción en la redacción. * Nivel de conocimientos adquiridos.	25,00 %
Examen final	[E10], [E9], [E8], [E7], [E6], [E5], [E4], [T25], [T16], [T9], [CG6], [CG4], [C36]	* Adecuación a lo solicitado. * Concreción en la redacción. * Nivel de conocimientos adquiridos.	50,00 %

10. Resultados de Aprendizaje

Conocer algoritmos criptográficos más utilizados, su implementación y su uso en protocolos de comunicación, autenticación e infraestructura de clave pública (PKI)

Configurar, administrar y utilizar un entorno basado en máquinas virtuales para simular una red corporativa con sus servicios y políticas de seguridad

Instalar y administrar aplicaciones y servicios sobre la infraestructura de máquinas virtuales para implementar cortafuegos, sistemas de autenticación, sistemas de monitorización, auditoría y análisis forense

En el contexto de un grupo de trabajo, simular sobre la infraestructura virtual distintos tipos de ataques, auditar los efectos y plantear las contramedidas.

Recopilar y analizar información técnica sobre técnicas, medidas y políticas de seguridad para realizar una síntesis por escrito de los conocimientos adquiridos

11. Cronograma / calendario de la asignatura

Descripción

*La distribución de los temas por semana es orientativo, puede sufrir cambios según las necesidades de organización docente.

Primer cuatrimestre

Semana	Temas	Actividades de enseñanza aprendizaje	Horas de trabajo presencial	Horas de trabajo autónomo	Total
Semana 1:	1T	1CT + 2,5CP + 0,5CP (online)	4.00	5.00	9.00

Semana 2:	1T	1CT + 2,5CP + 0,5CP (on-line)	4.00	5.00	9.00
Semana 3:	2T	1CT + 2,5CP + 0,5CP (online)	4.00	5.00	9.00
Semana 4:	2T	1CT + 1,5CP + 0,5CP (online)	4.00	6.00	10.00
Semana 5:	3T	1CT, 2CP + 1 proyecto (online)	4.00	6.00	10.00
Semana 6:	4T	1CT + 2,5CP + 0,5CP (on-line)	4.00	6.00	10.00
Semana 7:	4T	1CT + 2,5CP + 0,5CP (on-line)	4.00	7.00	11.00
Semana 8:	4T	1CT + 1,5CP + 0,5CP (on-line)	4.00	6.00	10.00
Semana 9:	4T	1CT y 2CP + proyecto (on-line)	4.00	6.00	10.00
Semana 10:	5T	1CT + 2,5CP + 0,5CP (online)	4.00	6.00	10.00
Semana 11:	5T	1CT + 2,5CP + 0,5CP (online)	4.00	6.00	10.00
Semana 12:	5T	1CT + 2,5CP + 0,5CP (online)	4.00	6.00	10.00
Semana 13:	5T	1CT + 2,5CP + 0,5CP (online)	4.00	6.00	10.00
Semana 14:	6T	1CT + 2,5CP + 0,5CP (online)	4.00	6.00	10.00
Semana 15:	Semanas 15 a 16. Exámenes y revisión	Evaluación.	4.00	8.00	12.00
Total			60.00	90.00	150.00