

DATOS GENERALES DE LA ASIGNATURA

ASIGNATURA: Delitos Informáticos

PLAN DE ESTUDIOS: Grado en Criminología (SGR-CRIM)

GRUPO: 2425-01

CENTRO: Facultad de Ciencias Sociales

CARÁCTER DE LA ASIGNATURA: Obligatorio

ECTS: 6,0

CURSO: 3º

SEMESTRE: 2º Semestre

IDIOMA EN QUE SE IMPARTE:

Castellano, excepto las asignaturas de idiomas que se impartirán en el idioma correspondiente

DATOS DEL PROFESOR

NOMBRE Y APELLIDOS: PABLO LUIS GÓMEZ SIERRA

EMAIL: plgomez@uemc.es

TELÉFONO: 983 00 10 00

CV DOCENTE:

FORMACIÓN:

Doctorando Universidad de Alcalá. Medidas especiales LECrim lucha contra el crimen organizado.

Graduado en Criminología (Universidad a Distancia de Madrid-UDIMA).

Máster Universitario en Proyectos Informáticos (Universidad de Alcalá).

Máster Universitario en Ingeniería de Sistemas de Información (Universidad Rey Juan Carlos).

Especialización Universitaria en Seguridad e Investigación Digital (Universidad de Alcalá).

Especialización Universitaria en Ciberseguridad (Universidad de León).

Especialización Profesional en Inteligencia Artificial.

EXPERIENCIA DE FORMACIÓN ONLINE:

Profesor en la Asignatura de Técnicas de Investigación y Análisis en Ciberdelincuencia en el Máster Universitario en Análisis e Investigación Criminal (Universidad a Distancia de Madrid-UDIMA).

Ponente en el Congreso de Nuevos Cibertalentos (Centro de Estudios Financieros-CEF).

Formador en el Taller de la Conducta Delictiva en el Ciberespacio de la Cátedra de Análisis de Conducta Behavior & Law.

Ponente en el Congreso Internacional de Sociología en Castilla La Mancha titulada "La investigación tecnológica y su vinculación con el ordenamiento jurídico español. Medidas Especiales" (ACMS).

Formador en Talleres Técnicos de disciplinas relacionadas con la Investigación Tecnológica, Inteligencia de Fuentes Abiertas y Seguridad Digital.

Ponente en Congreso de Seguridad Digital "CiberWall" (dos ediciones).

Ponente en el Congreso de Criminología Prospectiva "Criminología Corporativa". Universidad Complutense de Madrid.

Ponente en el Congreso de Criminología del Colegio Profesional de la Criminología de la Comunidad de Madrid.

Ponente en el Congreso Internacional "Evidentia University International" EEUU

CV PROFESIONAL:

15 años de experiencia en el sector relacionado con el “Espacio Red”, en disciplinas como la Investigación en Entornos de Alta Tecnología, Inteligencia en Fuentes Abiertas y sucesos de cibercrimen relacionados con las TICs.

Miembro del Grupo de Investigación Universitaria sobre Cibercriminología, Ciberseguridad y Ciberinteligencia (GRICCI) de la Universidad a Distancia de Madrid.

Miembro del Grupo de Trabajo de Cibercriminología de Colegio Profesional de la Criminología de la Comunidad de Madrid.

Colegiado de número del Colegio Profesional de la Criminología de la Comunidad de Madrid.

CERTIFICACIONES:

- Certificación HOL-SEG10 R1 Hacking Ético. Microsoft TechNet.
- Certificación HOL-SEG10 R2 Contramedidas Hacker. Microsoft TechNet.

CV INVESTIGACIÓN:

Gómez, P. L. (2024). "Explorando la inteligencia artificial y el pensamiento arborescente. Resolución de problemas complejos en la investigación tecnológica". Dykinson. ISBN: 9788410704503

Gómez, P. L y Lominchar J.. Libro (2023). "Principios de Ciberinteligencia". Centro de Estudios Financieros. ISBN 9788445444696

Gómez, P. L. (2023). "Explorando la inteligencia artificial y el pensamiento arborescente. Resolución de problemas complejos en la investigación tecnológica".

Gómez, P. L. (2022). *Diligencias de investigación tecnológica policial contra acciones de ciberdelincuencia en entornos de alta tecnología*. Madrid: Dykinson.

Gómez, P.L. (2021). “Medidas especiales de lucha contra el crimen organizado. La monitorización silenciosa de equipos informáticos”. Número 1, enero-marzo 2021 "LA LEY Privacidad" Wolters Kluwer. ISSN 2659-8698.

Gómez, P.L. (2020). “Infiltrados en el Ciberespacio. El Agente Encubierto Online”. Número 6, diciembre 2020 "LA LEY Privacidad" Wolters Kluwer. ISSN 2659-8698.

Gómez, P.L., varios autores (2020). “Diseño operativo de un Ciberataque a una Smart City”. Manual básico en Ciberseguridad y Protección de Datos. Exit Editorial S.L. ISBN: 978-84-9744-320-3, DL: M-28229-2020.

Gómez, P.L., varios autores (2020). “El estallido de la información abierta”. Manual básico en Ciberseguridad y Protección de Datos. Exit Editorial S.L. ISBN: 978-84-9744-320-3, DL: M-28229-2020.

Gómez, P.L. (2018). “Las smart cities como espacio propicio de acciones ofensivas de ciberdelincuencia”, en Martínez Paricio, J. y Moreno Carrillo, J.M. (Coords.). *Comprender el presente, imaginar el futuro: nuevas y viejas brechas sociales*. Roma-Messina (Italia): CORISCO Edizione, pp. 680-696. ISBN: 9788898138326.

Gómez, P.L., varios autores (2017). “Ciberseguridad en el Sector Público”. Documento de Conclusiones del Observatorio Sector Público - OSPI”. Madrid. IECISA.

García, A. y Gómez, P.L. (2016). "Amenazas Persistentes Avanzadas; producir el terror y el caos en las estructuras esenciales de la sociedad". Madrid: Jornadas de Seguridad y Defensa UDIMA.

DATOS ESPECÍFICOS DE LA ASIGNATURA

DESCRIPTOR DE LA ASIGNATURA:

La asignatura "Delitos Informáticos" se centra en el estudio de las nuevas formas de criminalidad que han surgido con el auge de las tecnologías de la información y la comunicación (TIC). Se analizarán los delitos informáticos, también conocidos como ciberdelitos, que representan un desafío para el Derecho penal moderno.

Al finalizar la asignatura, los alumnos serán capaces de:

Identificar y clasificar los diferentes tipos de delitos informáticos. Analizar las conductas típicas y los elementos constitutivos de los delitos informáticos. Conocer las medidas de investigación tecnológica empleadas en la investigación de los delitos informáticos. Aplicar los conocimientos adquiridos para resolver casos prácticos

relacionados con delitos informáticos. Comprender las técnicas de inteligencia en fuentes abiertas (OSINT) y su aplicación en la lucha contra el cibercrimen. Conocer el marco legal español e internacional en materia de ciberdelincuencia. Argumentar sobre la adecuación de la legislación actual a los desafíos que plantean las nuevas tecnologías.

CONTENIDOS DE LA ASIGNATURA:

1. Delitos Informáticos

1. Delitos Informáticos en el Código Penal Español : El estudio de esta unidad proporcionará a los alumnos una comprensión profunda de cómo el Código Penal español aborda los delitos informáticos y las estrategias legales para combatirlos.
2. Procedimientos de Investigación Tecnológica en la Ley de Enjuiciamiento Criminal : El alumno conocerá que la investigación tecnológica es esencial para garantizar que las tecnologías se utilicen de manera responsable, ética y si fuera necesario ser eficaces en la lucha contra la delincuencia en la era digital.
3. Metodología operativa realizada a través de medios Informáticos. Parte I : Se analizan las principales conductas operativas del cibercrimen y los cibercriminales.
4. Metodología operativa realizada a través de medios Informáticos. Parte II : Se abordará como los ingenieros sociales son a menudo personas extrovertidas con una notable capacidad para interactuar y manipular a otras personas.
5. OSINT. Técnicas de inteligencia en fuentes abiertas para la lucha contra el cibercrimen. : Se pretende dar una visión global sobre cómo se puede obtener información utilizando procedimientos y herramientas tecnológicas.

OBSERVACIONES CONTENIDO DE LA ASIGNATURA:

Esta asignatura ofrece una visión detallada de los delitos informáticos en el Código Penal español, las medidas de investigación y las técnicas operativas del cibercrimen. Se exploran los delitos contra la intimidad, el honor, el patrimonio y la propiedad intelectual en el entorno digital. Se analizan técnicas de ingeniería social, ataques de denegación de servicio (DDoS), malware, phishing y spam. También se abordan los procedimientos de investigación tecnológica en la Ley de Enjuiciamiento Criminal (LECrim), incluyendo la intervención de comunicaciones, el registro de dispositivos y la cadena de custodia. Se examinan las técnicas OSINT para la recopilación y análisis de información en fuentes abiertas, junto con herramientas como Maltego, Google, Bing y Shodan.

RECURSOS DE APRENDIZAJE:

Los recursos de aprendizaje que se utilizarán en todas las asignaturas de la titulación (salvo las prácticas externas) para facilitar el proceso de enseñanza-aprendizaje, son:

- Campus online de la UEMC (Open Campus)
- Plataforma de Webconference(Zoom work place)

Las comunicaciones con el profesor serán a través de Open Campus vía Mi correo, Tablón o/y Foro.

COMPETENCIAS Y RESULTADOS DE APRENDIZAJE A ADQUIRIR POR EL ALUMNO

COMPETENCIAS GENERALES:

- RD 822/2021. Según el Real Decreto 822/2021, el marco competencial del título se define a través de grandes competencias (GC), ubicadas temporalmente en esta categoría de "competencias generales".
- GC02. Adquirir la capacidad de reconocer y analizar las teorías criminológicas y las distintas técnicas de investigación desarrolladas como fuentes de estudio y formulación de estrategias de actuación

COMPETENCIAS ESPECÍFICAS:

- RD 822/2021. Según el Real Decreto 822/2021, el marco competencial del título se concreta en los resultados de aprendizaje de cada materia y asignatura

COMPETENCIAS TRANSVERSALES:

- RD 822/2021. Según el Real Decreto 822/2021, el marco competencial del título se concreta en los resultados de aprendizaje de cada materia y asignatura

RESULTADOS DE APRENDIZAJE:

El alumno será capaz de:

- SbC2.3_Subcompetencia_Acomodar las investigaciones a la normativa europea legal existente
- SbC2.4_Subcompetencia_Proponer soluciones concretas relacionadas con los contenidos de la materia
- SbC2.6_Subcompetencia_El alumno asume la importancia del Derecho en la regulación de Internet y las redes sociales
- SbC2.7_Subcompetencia_Entiende y conoce el impacto que las nuevas tecnologías de la comunicación han asumido en todos los ámbitos del derecho
- SbC2.8_Subcompetencia_El alumno asume la relevancia que las nuevas tecnologías de la comunicación y su nueva regulación tiene para la vigencia de los derechos fundamentales y principios y valores democráticos
- C2.3_Conocimiento_Adquirir conocimientos que habiliten al alumno para la investigación operativa, para el esclarecimiento de determinados casos, con capacidad crítica, aplicada a la práctica profesional
- C2.5_Conocimiento_Influencia de los factores socioeconómicos en el desarrollo de nuevas actividades delictivas
- C2.6_Conocimiento_Conoce el régimen jurídico básico de Internet y las redes sociales
- C2.7_Conocimiento_Conoce las problemática y principales implicaciones que las nuevas tecnologías tienen en las diferentes ramas del ordenamiento jurídico
- H2.2_Habilidad o destreza_Actualización científica
- CT2.2_Competencia transversal, valor o actitud_Interés en la actualización de las novedades tecnológicas de apoyo a la investigación
- CT2.3_Competencia transversal, valor o actitud_Conocimiento de los nuevos delitos y su investigación práctica

BIBLIOGRAFÍA Y RECURSOS DE REFERENCIA GENERALES

BIBLIOGRAFÍA BÁSICA:

- Velasco Núñez, E., & Sanchis Crespo, C (2019): Delincuencia informática tipos delictivos e investigación con jurisprudencia tras la reforma procesal y penal de 2015.. Tirant lo Blanch. ISBN: 9788413133560
- BALLESTEROS, M. C. (2019): Medidas de investigación tecnológica en el proceso penal: la nueva redacción de la Ley de Enjuiciamiento Criminal operada por la Ley Orgánica 13/2015.. Anuario Jurídico y Económico Escurialense.. ISBN: ISSN: 1133-3677
- Maíllo Fernández, J. A. (2020): Hackers: Técnicas y herramientas para atacar y defendemos.. RAMA. ISBN: 978-84-9964-895-8

BIBLIOGRAFÍA COMPLEMENTARIA:

- Aldawood, H., & Skinner, G. (2019): Reviewing cyber security social engineering training and awareness programs—Pitfalls and ongoing issues.. Future Internet. ISBN: 10.3390/fi11030073

WEBS DE REFERENCIA:

Web / Descripción

[INCIBE](https://www.incibe.es/aprendeciberseguridad/ingenieria-social)(<https://www.incibe.es/aprendeciberseguridad/ingenieria-social>)

Campaña "Ingeniería social: que no te engañen": Recursos educativos de la Oficina de Seguridad del Internauta (OSI) de INCIBE.

Formulario de colaboración sobre "delitos telemáticos" (https://www.guardiacivil.es/es/colaboracion/form_contacto/delitos_telematicos.html)
 Grupo de Delitos Telemáticos de la Guardia Civil

Brigada Central de Investigación Tecnológica (B.C.I.T.) (https://www.policia.es/_es/tupolicia_conocenos_estructura_dao_cgpoliciajudicial_bcit.php)
 Sección de delitos telemáticos de la Policía Nacional

Poder Judicial (<https://www.poderjudicial.es/cgpj/>)
 Portal oficial que contiene jurisprudencia y documentación sobre investigación tecnológica en procesos penales.

PLANIFICACIÓN DEL PROCESO DE ENSEÑANZA-APRENDIZAJE DE LA ASIGNATURA

METODOLOGÍAS:

Valor del parámetro TEXTO_FIJO_ONLINE_GRADO_METODOLOGIA

MÉTODO DIDÁCTICO:

El papel del profesor cobra importancia a través de la impartición de clases magistrales en tiempo real por videoconferencia que podrá utilizar para explicar los contenidos teóricos, resolver dudas que se planteen durante la sesión, ofrecer retroalimentación sobre las actividades de evaluación continua o realizar sesiones de tutoría de carácter grupal.

MÉTODO DIALÉCTICO:

Se caracteriza por la participación de los alumnos en las actividades de evaluación continua de debate y la intervención de éstos a través del diálogo y de la discusión crítica (seminarios, grupos de trabajo, etc.). Utilizando este método el alumno adquiere conocimiento mediante la confrontación de opiniones y puntos de vista. El papel del profesor consiste en proponer a través de Open Campus temas referidos a la materia objeto de estudio que son sometidos a debate para, posteriormente, evaluar el grado de comprensión que han alcanzado los alumnos.

MÉTODO HEURÍSTICO:

Este método puede desarrollarse de forma individual o en grupo a través de las actividades de evaluación continua (entregas de trabajos, resolución de ejercicios, presentaciones, etc.). El objetivo es que el alumno asuma un papel activo en el proceso de aprendizaje adquiriendo los conocimientos mediante la experimentación y la resolución de problemas.

CONSIDERACIONES DE LA PLANIFICACIÓN:

Las ACTIVIDADES FORMATIVAS que se realizan en la asignatura son las siguientes:

Clases teóricas: Actividad dirigida por el profesor que se desarrollará de forma sincrónica en grupo. Para la realización de esta actividad en Open Campus, la UEMC dispone de herramientas de Webconference que permiten una comunicación unidireccional en las que el docente puede desarrollar sesiones en tiempo real con posibilidad de ser grabadas para ser emitidas en diferido.

Actividades prácticas: Actividades supervisadas por el profesor que se desarrollarán fundamentalmente de forma asincrónica, y de forma individual o en grupo:

- Actividades de debate. Se trata de actividades desarrolladas en el foro de Open Campus, en las que se genera conocimiento mediante la participación de los estudiantes en discusiones alrededor de temas de interés en las distintas asignaturas.
- Entregas de trabajos individuales o en grupo a partir de un enunciado o unas pautas de trabajo que establecerá el profesor.
- Resolución de ejercicios y problemas que el alumno debe realizar a través de Open Campus en un periodo de tiempo determinado. Esta actividad puede ser en formato test de evaluación.

Tutorías: Las tutorías podrán tener un carácter sincrónico o asincrónico y podrán desarrollarse de manera individual o en grupos reducidos.

Están previstas tres sesiones de tutoría por videoconferencia, una al inicio y otra antes del examen parcial, y una más al final del semestre. En la primera se presentará la asignatura y la guía docente y en la segunda, en las semanas previas a la evaluación final, se dedicará a la resolución de dudas de los estudiantes.

Además, el docente utiliza el Tablón, el Foro y el Sistema de correo interno de Open Campus para atender las necesidades y dudas académicas de los estudiantes.

SESIONES EN TIEMPO REAL

En la asignatura se planifican clases magistrales y tutorías a través de videoconferencias.

La asistencia a las videoconferencias no será obligatoria, pero si recomendable para un adecuado seguimiento de la asignatura, la comprensión de los materiales y el desarrollo óptimo de las actividades de aprendizaje. En cualquier caso, salvo circunstancias excepcionales, será posible acceder a ellas en diferido a las 48 horas máximo desde su celebración.

SESIONES EN TIEMPO REAL :

Título	
TU1	Presentación asignatura y Guía docente
CM1	- TEMA 1 Delitos Informáticos en el Código Penal Español.
CM2	- TEMA 2 Procedimientos de Investigación Tecnológica en la Ley de Enjuiciamiento Criminal.
CM3	- TEMA 3 Metodología operativa realizada a través de medios Informáticos. Parte I
CM4	- TEMA 4 Metodología operativa realizada a través de medios Informáticos. Parte II
CM5	- Tema 5: OSINT. Técnicas de inteligencia en fuentes abiertas para la lucha contra el cibercrimen.
CM6	TU. Parc. Resolución de dudas y preparación de la prueba parcial
CM7	- Herramientas y procedimientos online. Parte I
CM8	- Herramientas y procedimientos online. Parte II
TU2	Resolución de dudas antes de la evaluación

EVALUACIÓN CONVOCATORIA ORDINARIA:

Evaluación continua	60%
Evaluación final	40%

ACTIVIDADES Y SISTEMAS DE EVALUACIÓN :

Tipo Evaluación	Nombre Actividad	% Calif.
Evaluación continua (60 %)	1. Actividad 1 (Entrega individual)	25
	2. Actividad 2 (Entrega individual)	25
	3. Test (Test de evaluación)	10
Evaluación final (40 %)	1. Prueba de evaluación final (Prueba de evaluación final)	40

CONSIDERACIONES EVALUACIÓN CONVOCATORIA ORDINARIA:

A lo largo de la planificación de la asignatura el alumno realizará **actividades de evaluación continua** que forman parte de la calificación de la asignatura con un peso del 60% sobre la nota final.

Para superar la evaluación continua, el alumno debe obtener una media de igual o superior a 5 entre todas las actividades. En el caso de no superar la evaluación continua, se guardan para la convocatoria extraordinaria las notas de aquellas actividades aprobadas, no pudiendo volver a presentarlas.

El sistema de evaluación de esta asignatura acentúa el desarrollo gradual de competencias y resultados de aprendizaje y, por tanto, se realizará una evaluación continua a través de las distintas actividades de evaluación propuestas. El resultado de la evaluación continua se calcula a partir de las notas obtenidas en cada actividad teniendo en cuenta el porcentaje de representatividad en cada caso.

Todas las actividades deberán entregarse en las fechas previstas para ello, teniendo en cuenta:

- Las actividades de evaluación continua (entrega de trabajos) se desarrollarán según se indica y, para ser evaluadas, los trabajos deberán ser entregados en la forma y fecha prevista y con la extensión máxima señalada. No se evaluarán trabajos entregados posteriormente a esta fecha o que no cumplan con los criterios establecidos por el profesor.
- La no entrega de una actividad de evaluación continua en forma y plazo se calificará con un 0 y así computarán en el cálculo de la nota de evaluación continua y final de la asignatura.
- Cualquier tipo de copia o plagio por mínimo que sea, así como un uso inapropiado de herramientas de inteligencia artificial, supondrá una calificación de 0 en la actividad correspondiente. Esta actuación podría suponer la apertura de un expediente disciplinario.
- Las actividades de evaluación continua (tipo test) se desarrollarán con anterioridad a la realización de las pruebas de evaluación final de la asignatura

Los alumnos accederán a través de Open Campus a las calificaciones de las actividades de evaluación continua en un plazo aproximado de 20 días lectivos desde la fecha fin de fecha de entrega, excepto causas de fuerza mayor en cuyo caso se informará al alumno a través del Tablón.

La evaluación continua se complementará con una **evaluación final** que se realizará al finalizar el periodo lectivo en cada asignatura. La prueba constará de parte práctica y teórica, suponiendo un 40% de la calificación sobre la nota final.

La evaluación final de la asignatura se desarrollará del siguiente modo:

- A mitad de cada semestre se ofrece al alumno el poder realizar de forma voluntaria un parcial para eliminar materia.
- Para eliminar la materia es necesario que el alumno lo supere al menos con un 5. En este caso, se le guardaría la nota del parcial hasta la convocatoria extraordinaria. El alumno sólo podrá presentarse a la segunda parte de la asignatura bien en convocatoria ordinaria o extraordinaria.
- En convocatoria ordinaria, la prueba final constará de dos exámenes (primera y segunda parte de la asignatura)
 - En el caso de que el alumno hubiera superado y eliminado materia con el primer parcial, sólo se presentará a la segunda parte. Para superar la asignatura se hará la media siempre que en la segunda parte se obtenga al menos un 4 y la media supere el 5.
 - En el caso de que el alumno no hubiera superado el primer parcial, se podrá presentar a ambas partes. Para superar la asignatura se hará la media de ambas partes siempre que se obtenga al menos un 4 en cada una y la media supere el 5.
- El alumno tendrá la posibilidad, siempre dentro de los tres días siguientes a la publicación de las notas, a renunciar a su calificación, y presentarse en la siguiente convocatoria
- El alumno tendrá hasta 3 días después de la calificación para solicitar al docente más información sobre su calificación por el correo de la plataforma.
- Cualquier tipo de irregularidad o fraude en la realización de una prueba, así como un uso inapropiado de herramientas de inteligencia artificial, supondrá una calificación de 0 en la prueba/convocatoria correspondiente. Esta actuación podría suponer la apertura de un expediente disciplinario.
- El aplazamiento concedido por la Universidad para la realización de una evaluación final se registrará por lo

establecido en el Manual de "Directrices y plazos para la tramitación de una solicitud"

La nota final se corresponderá con la media aritmética del resultado obtenido en cada una de las partes. En caso de no superación, se guarda la parte aprobada para la convocatoria extraordinaria.

La **nota global** de la asignatura se obtiene ponderando la calificación de la evaluación continua y de la evaluación final según los siguientes porcentajes, y debiendo tener aprobadas ambas partes, continua y final, para superar la asignatura.

Si un alumno no se presenta a la prueba de evaluación final, su calificación en la convocatoria será de "No presentado", con independencia de que haya realizado alguna actividad de evaluación continua.

De igual modo si el alumno no entrega ninguna actividad de evaluación continua, obtendrá la calificación de "No presentado", con independencia de que haya aprobado la prueba de evaluación final, en cuyo caso, se le guardaría su calificación para la convocatoria extraordinaria

EVALUACIÓN CONVOCATORIA EXTRAORDINARIA:

Evaluación continua	60%
Evaluación final	40%

ACTIVIDADES Y SISTEMAS DE EVALUACIÓN :

Tipo Evaluación	Nombre Actividad	% Calif.
Evaluación continua (60 %)	1. Actividad 1 (Entrega individual)	25
	2. Actividad 2 (Entrega individual)	25
	3. Test (Test de evaluación)	10
Evaluación final (40 %)	1. Prueba de evaluación final (Prueba de evaluación final)	40

CONSIDERACIONES EVALUACIÓN CONVOCATORIA EXTRAORDINARIA:

Los estudiantes que no hayan superado la asignatura en la convocatoria ordinaria, porque hayan suspendido la evaluación continua o la prueba de evaluación final, podrán presentarse a las pruebas establecidas por el profesor en la convocatoria extraordinaria.

Para la convocatoria extraordinaria se guardan las calificaciones de las actividades de evaluación continua y pruebas de evaluación (parcial y final), superadas por el estudiante (nota superior o igual a 5), no permitiéndose volver a realizarlas.

- En convocatoria extraordinaria, la prueba final también constará de dos exámenes (primera y segunda parte de la asignatura)
 - En el caso de que el alumno hubiera superado el parcial (al menos un 5) o una de las partes en convocatoria ordinaria (al menos un 5), esta calificación se mantiene para la extraordinaria, presentándose el alumno sólo a lo suspenso. Para superar la asignatura se hará la media entre lo aprobado en ordinaria y la calificación que haya sacado en extraordinaria siempre que se obtenga al menos un 4 y la media supere el 5.
 - En el caso de que el alumno tuviera que presentarse a ambas partes, para superar la asignatura se hará la media siempre que se obtenga al menos un 4 en cada parte y la media supere el 5.
- En convocatoria extraordinaria, el alumno solo podrá entregar las actividades de evaluación continua no superadas, guardándose la calificación de las aprobadas.
- El alumno tendrá hasta 3 días después de la calificación para solicitar al docente más información sobre su calificación por el correo de la plataforma.
- Cualquier tipo de irregularidad o fraude en la realización de una prueba, supondrá una calificación de 0 en

la prueba/convocatoria correspondiente.

- El aplazamiento concedido por la Universidad para la realización de una evaluación final se regirá por lo establecido en el Manual de "Directrices y plazos para la tramitación de una solicitud".

En la convocatoria extraordinaria, la **nota global** de la asignatura se obtiene ponderando la calificación de la evaluación continua y de la evaluación final, de la misma forma que en la convocatoria ordinaria.

Al igual que en la convocatoria ordinaria, en la convocatoria extraordinaria es necesario superar tanto la evaluación continua como la evaluación final para aprobar la asignatura.

Si un alumno no se presenta a la prueba de evaluación final, su calificación en la convocatoria será de "No presentado", con independencia de que haya realizado alguna actividad de evaluación continua.

SISTEMAS DE EVALUACIÓN:

SISTEMA DE EVALUACIÓN	PORCENTAJE (%)
Ejecución de prácticas	50%
Pruebas escritas	50%