DATOS GENERALES DE LA ASIGNATURA

ASIGNATURA: Informática Aplicada
PLAN DE ESTUDIOS: Grado en Criminología (SGR-CRIMINOL)
GRUPO: 2324-02
CENTRO: Facultad de Ciencias Sociales
CARÁCTER DE LA ASIGNATURA: Básico
ECTS: 6,0
CURSO: 2º
SEMESTRE: 1º 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:

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)

Experiencia en 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 el Congreso de Seguridad Digital CiberWall.

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.

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 relacionados con las TICs.

Miembro del Grupo de InvestigaciónUniversitaria 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.

Certificación HOL-SEG10 R1 Hacking Ético. Microsoft TechNet.

Certificación HOL-SEG10 R2 Contramedidas Hacker. Microsoft TechNet.

CV INVESTIGACIÓN:

Gómez, P. L. (2022). Diligencias de investigación tecnológica policialcontra 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, ima-ginar 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 Conclu-siones 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:

En un mundo donde todo gira en torno a internet, el ámbito delictivo también se está aprovechando y sacando partido de los beneficios que ofrece cometer hechos delictivos a través de este medio, por todo ello, en esta asignatura pretendemos que el usuario entienda que internet es un territorio hostil, ofrecer luz a todos aquellos que se desconocen del mismo, con la finalidad de que pueda adoptar decisiones correctas en el día a día para prevenir o erradicar el fenómeno de la delincuencia a través de estos medios.

Partimos de la base de que la gran mayoría de ordenadores, smartphones y demás dispositivos están conectados a internet, una zona que se encuentre en permanente conflicto, por lo que el nivel de desconfianza ante dichos medios debe ser el adecuado a cada caso.

A través de esta asignatura, aprenderemos a analizar ese escenario de riesgo que se produce en cada comunicación a través de medios electrónicos, detectar y analizar las amenazas posibles, así como las consecuencias por la falta de aplicación de medidas de prevención.

Estudiaremos las diferentes medidas de prevención, tanto las que deben llevarse a cabo en el momento de la instalación del sistema operativo, y las medidas de contención y reparación, que serán aquellas que ejecutaremos cuando el ordenador se encuentre comprometido por malware.

CONTENIDOS
Para poder afrontar todas las competencias necesarias en la presente asignatura, se empezará estudiando los diferentes sistemas operativos y sus características, entendiendo su funcionamiento, vulnerabilidades y fortalezas.

Acto seguido, realizaremos un estudio pormenorizado de internet y los estándares de Internet, los RFC´s así como

los diferentes códigos que se utilizan en la web para crear una página web.

En el tema 3, aprenderemos a encontrar información y a su tratamiento adecuado, la recopilación de la información existente en internet es una de las tareas más importantes, ya que vivimos en una época en la que tenemos acceso a muchísima información, pero no sabemos qué hacer con ella.

En el tema destinado a Sistemas de seguridad informática, aprenderemos las diferentes amenazas que podemos encontrarnos en internet, y las posibles medidas de seguridad que podemos utilizar para ser menos vulnerables.

En el tema 4 estudiaremos las redes informáticas y los sistemas de conexión entre las mismas. Y en el último tema, aprenderemos a monitorizar la actividad delictiva en internet para prevenir los posibles delitos, o detectar aquellos que se hayan cometido.

Para poder afrontar todas las competencias necesarias en la presente asignatura, se empezará estudiando los diferentes sistemas operativos y sus características, entendiendo su funcionamiento, vulnerabilidades y fortalezas.

Acto seguido, realizaremos un estudio pormenorizado de internet y los estándares de Internet, los RFC´s así como los diferentes códigos que se utilizan en la web para crear una página web.

En el tema 3, aprenderemos a encontrar información y a su tratamiento adecuado, la recopilación de la información existente en internet es una de las tareas más importantes, ya que vivimos en una época en la que tenemos acceso a muchísima información, pero no sabemos
qué hacer con ella.

En el tema destinado a Sistemas de seguridad informática, aprenderemos las diferentes amenazas que podemos encontrarnos en internet, y las posibles medidas de seguridad que podemos utilizar para ser menos vulnerables.

En el tema 4 estudiaremos las redes informáticas y los sistemas de conexión entre las mismas.

Y en el último tema, aprenderemos a monitorizar la actividad delictiva en internet para prevenir los posibles delitos, o detectar aquellos que se hayan cometido.

CONTENIDOS DE LA ASIGNATURA:

1. **Informática Aplicada**
    1. Sistemas operativos
    2. Internet
    3. Hojas de cálculo y bases de datos
    4. Sistemas de seguridad informática
    5. Redes informáticas
    6. Monitorización de los delitos cometidos a través de internet

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 (Adobe Connect)

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 BÁSICAS:

- CB1. Que los estudiantes hayan demostrado poseer y comprender conocimientos en un área de estudio que parte de la base de la educación secundaria general, y se suele encontrar a un nivel que, si bien se apoya en libros de texto avanzados, incluye también algunos aspectos que implican conocimientos procedentes de la vanguardia de su campo de estudio

- CB2. Que los estudiantes sepan aplicar sus conocimientos a su trabajo o vocación de una forma profesional y posean las competencias que suelen demostrarse por medio de la elaboración y defensa de argumentos y la resolución de problemas dentro de su área de estudio
- CB3. Que los estudiantes tengan la capacidad de reunir e interpretar datos relevantes (normalmente dentro de su área de estudio) para emitir juicios que incluyan una reflexión sobre temas relevantes de índole social, científica o ética
- CB4. Que los estudiantes puedan transmitir información, ideas, problemas y soluciones a un público tanto especializado como no especializado
- CB5. Que los estudiantes hayan desarrollado aquellas habilidades de aprendizaje necesarias para emprender estudios posteriores con un alto grado de autonomía

COMPETENCIAS GENERALES:

- CG01. Adquirir la capacidad de búsqueda, análisis y sistematización de la información
- CG02. Adquirir la capacidad de organización y planificación
- CG03. Adquirir la capacidad para trabajar en equipos de carácter interdisciplinar
- CG04. Desarrollar estrategias de aprendizaje autónomo.
- CG05. Desarrollar hábitos de excelencia y calidad en el ejercicio profesional
- CG06. Desarrollar la capacidad de crítica y autocrítica del estudiante
- CG07. Desarrollar la capacidad para la toma de decisiones, aplicando los conocimientos a la práctica.
- CG08. Desarrollar un compromiso ético en la práctica profesional en todos los ámbitos en los que se desarrolle
- CG09. Desarrollar un pensamiento y un razonamiento crítico y saber comunicarlo, de manera efectiva.

COMPETENCIAS ESPECÍFICAS:

- CE22. Manejar las nuevas tecnologías en el ámbito criminológico y de la seguridad: bases de datos, legislación, software específico.

RESULTADOS DE APRENDIZAJE:

El alumno será capaz de:

- Buscar y seleccionar recursos bibliográficos relevantes, impresos o electrónicos de manera autónoma.
- Práctica en el análisis de datos cuantitativos y cualitativos.
- Reconoce y utiliza los principales recursos documentales e informáticos
- Utiliza adecuadamente las bases de datos fundamentales y obtiene información relevante.

BIBLIOGRAFÍA Y RECURSOS DE REFERENCIA GENERALES

BIBLIOGRAFÍA BÁSICA:

- DIAZ ORUETA, GABRIEL (2004): Seguridad en las comunicaciones y en la información. ES UNED. ISBN: 9788436247893
- COCERO MATESANZ, DAVID et al (2017): Informática aplicada. Herramientas digitales para la investigación y el tratamiento de información en humanidades. ES UNED. ISBN: 9788436272765
- CASTRO GIL, MANUEL ALONSO (2014): Procesos y herramientas para la seguridad de redes. ES UNED. ISBN: 9788436272765

BIBLIOGRAFÍA COMPLEMENTARIA:

- José Luis Verdeguer Navarro (2013): Hacking y seguridad VolP. Informática 64. ISBN: 9788461622573
- FLORES PRADA, IGNACIO (2012): Criminalidad informática. Tirant Lo Blanch. ISBN: 978-84-9033-570-3
- VALDIVIA MIRANDA, CARLOS (2014): Sistemás informáticos y redes locales. Ediciones Paraninfo. ISBN: 978-8497324496
- RAMOS VARÓN, ANTONIO ÁNGEL (2015): Hacking práctico en internet y redes de ordenadores y redes de ordenadores.. RA-MA S.A.. ISBN: 978-8499642949

WEBS DE REFERENCIA:

Web / Descripcion
Guardia Civil(https://www.guardiacivil.es/es/index.html) Web oficial Cuerpo de la Guardia Civil
Policía Nacional(https://www.policia.es/_es/denuncias.php) Web oficial Cuerpo Nacional Policía
Incibe(https://www.incibe.es/) Web oficial Instituto Nacional de CIberseguridad
CN-CERT(https://www.ccn-cert.cni.es/) Web oficial Centro Criptológico Nacional
OSI(https://www.osi.es/es) Web oficial Oficina Seguridad Internauta
CSIRT(https://www.csirt.es/index.php/es/) Web oficial Equipos de CIberseguridad y Gestión de Incidentes
OTRAS FUENTES DE REFERENCIA:
Artículos científicos enlazados en el Aula VIrtual

PLANIFICACIÓN DEL PROCESO DE ENSEÑANZA-APRENDIZAJE DE LA ASIGNATURA

METODOLOGÍAS:

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 OpenCampus, 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 asíncrona, 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 asíncrono y podrán desarrollarse de manera individual o en grupos reducidos.

Están previstas tres sesiones de tutoría por videoconferencia, una al inicio, otra antes de la evaluación parcial y otra 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	Sistemas Operativos
CM2	Internet
CM3	Hojas de cálculo y bases de datos
CM4	Sistemas de seguridad informática y redes informáticas
CM5	Monitorización de delitos cometidos a través de internet
CM6	TU. Parc. Resolución de dudas y preparación de la prueba parcial
CM7	Uso de herramientas para los casos prácticos
CM8	Resolución de los casos prácticos planteados en la asignatura
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.
Evaluacion contínua (60 %)	1. Actividad 1 (Entrega individual)	25

Tipo Evaluación	Nombre Actividad	% Calif.
	2. Actividad 2 (Entrega grupal)	25
	3. Test de evaluación (Test de evaluación)	10
Evaluacion final (40 %)	1. Prueba de evaluación final Online (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.
- Las actividades de entrega de trabajos en grupo se diseñan para que se desarrolle la competencia de trabajo en equipo por lo que cada equipo dispone de un espacio de trabajo y una única entrega para todos los integrantes. Salvo decisión del profesor, todos los integrantes del grupo obtendrán la misma calificación en la actividad.
- 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, supondrá una calificación de 0 en la actividad correspondiente.
- 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 OpenCampus a las calificaciones de las actividades de evaluación continua en un plazo no superior a 15 días lectivos desde su 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 a 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, 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"

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.
Evaluacion contínua (60 %)	1. Actividad 1 (Entrega individual)	25
	2. Actividad 2 (Entrega individual)	25
	3. Test de evaluación (Test de evaluación)	10
Evaluacion final (40 %)	1. Prueba de evaluación final Online (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 (%)
Pruebas de ejecución de tareas reales y/o simuladas	25%
Pruebas de respuesta corta	20%
Pruebas objetivas	30%
Trabajos y proyectos	25%