GUIA DOCENTE DE LA ASIGNATURA

SEGURIDAD DE REDES Y TELECOMUNICACIONES

Curso 2019-2020

(Fecha última actualización: 28/04/2020)

(Fecha de aprobación en Consejo de Departamento: **Adenda** 28/04/2020 y **Guía** 27/05/2019)

MÓDULO	**MATERIA**	**CURSO**	**SEMESTRE**	**CRÉDITOS**	**TIPO**
Optativas	SEGURIDAD DE REDES Y TELECOMUNICACIONES	4º	7º	6	Optativa

PROFESORES	**DIRECCIÓN COMPLETA DE CONTACTO PARA TUTORÍAS** (Dirección postal, teléfono, correo electrónico, etc.)
• José Antonio Gómez Hernández: Teoría y prácticas COORDINADOR DE LA ASIGNATURA: José Antonio Gómez Hernández	Dpto. Lenguajes y Sistemas Informáticos, E.T.S. de Ingenierías Informática y de Telecomunicación. Despachos nº 10, 3ª planta Correo electrónico: jagomez@ugr.es Tfno: 958 240 572
	ENLACE A LA PÁGINA WEB DONDE PUEDAN CONSULTARSE LOS HORARIOS DE TUTORÍAS*
	https://lsi.ugr.es/lsi/jagomez

GRADO EN EL QUE SE IMPARTE	**OTROS GRADOS A LOS QUE SE PODRÍA OFERTAR**
Grado en Criminología	Cumplimentar con el texto correspondiente, si procede

PRERREQUISITOS Y/O RECOMENDACIONES (si procede)

Ninguno

BREVE DESCRIPCIÓN DE CONTENIDOS (SEGÚN MEMORIA DE VERIFICACIÓN DEL GRADO)

- Análisis técnico-profesional de la seguridad de las redes y telecomunicaciones.
- Protección de sistemas informáticos y certificados digitales. Seguridad en sistemas de tiempo real y distribuidos. Vulnerabilidad de sistemas operativos.

- Principales delitos cometidos en Internet: ciberterrorismo, ataques a la propiedad intelectual en Internet, intervención de las comunicaciones, intromisiones en la intimidad y el derecho a la propia imagen y tratamientos no autorizados de datos personales, ataques al honor y suplantación de personalidad, fraude de tarjetas de crédito en Internet, *phishing* o captación de datos para ser usados de manera fraudulenta, *bullying* o maltrato psicológico a menores en la Red, ciberacoso, difusión de material pornográfico en Internet, etc., virus y daños informáticos.

COMPETENCIAS GENERALES Y ESPECÍFICAS

Competencias básicas y generales

- G2. Dominar las técnicas e instrumentos para la evaluación y predicción de la criminalidad.
- G5. Comprender la complejidad y diversidad del fenómeno criminal en un mundo global.
- G11. Conocer y utilizar adecuadamente las Tecnologías de la Información y la Comunicación en la resolución de problemas y búsqueda de información en el ámbito de la Criminología y la Seguridad.
- G12. Ser capaz de trabajar en equipo con otros profesionales en las diferentes vertientes de la actividad criminológica.
- G13. Desarrollar una aptitud crítica frente a la realidad social respetando los principios de igualdad, derechos humanos, paz y accesibilidad universal.

Competencias específicas

- E2. Interpretar las fuentes de datos relacionados con la criminalidad: gráficos, estadísticas, etc.
- E5. Atender las necesidades de la víctima a nivel individual, grupal y comunitario, con especial referencia a colectivos muy victimizados como las víctimas de violencia de género, los menores o los incapaces.
- E7. Elaborar de informes para evaluar la situaciones de riesgo de los menores, medidas aplicables a los infractores y medidas de protección a los que estén en situación de abandono.
- E11. Aplicar las técnicas de investigación adecuadas para la persecución de delitos garantizando la seguridad ciudadana, los derechos fundamentales y la resolución de conflictos sociales.
- E16. Conocer y aplicar las técnicas y estrategias para la evaluación y predicción de la conducta criminal.
- E17. Capacidad de aplicar los conocimientos psicosociales al estudio y comprensión de las nuevas formas de criminalidad.

OBJETIVOS (EXPRESADOS COMO RESULTADOS ESPERABLES DE LA ENSEÑANZA)

- Conocer la tipología de delitos informáticos y la legislación vigente al respecto.
- Comprender los conceptos básicos de informática y de los componentes de un sistema informático y de redes de computadores.
- Utilizar las herramientas básicas para la detección y prevención de delitos frecuentes.
- Conocer las bases de la seguridad de sistemas informáticos.
- Profundizar en el método de investigación forense informática.
- Saber elaborar un informe pericial informático.

TEMARIO DETALLADO DE LA ASIGNATURA

TEMARIO TEÓRICO:

- **Tema 1**. Informática para criminólogos.

1.1. Conceptos básicos de Informática.
1.2. Componentes de un sistemas informático: hardware, *firmware* y software.
1.3. Redes de comunicaciones: hardware, protocolos y servicios.
1.4. Elementos avanzados de computación: computación en la nube, inteligencia artificial, etc.

- **Tema 2**. Cibercriminalidad.
  2.1. Definición y contexto.
  2.2 El crimen en el ciberespacio: características y cuantificación del problema.
  2.3. Clasificación y tipología de cibercrímenes.
  2.4. Los cibercriminales.
  2.5. Las cibervíctimas.
  2.6. Normativa.

- **Tema 3**. Prevención y detección del cibercrimen.
  3.1. Intrusiones y ataques a sistemas.
  3.2. Seguridad en sistemas operativos y redes de comunicaciones.
  3.3. Criptografía y certificados digitales.
  3.4. Técnicas y herramientas para la detección y prevención del cibercrimen.

- **Tema 4**. Peritaje informático
  4.1. El perito informático.
  4.2. Aspectos legales y jurídicos del peritaje
  4.3. Tipos y fases de peritajes.
  4.4. La prueba y el informe pericial.

- **Tema 5**. Informática forense.
  5.1. Fundamentos de la informática forense.
  5.2. La evidencia digital.
  5.3. Modelo de procesos de investigación forense informático.
  5.4. Laboratorio de Informática Forense.
  5.5. Metodologías, estándares y guías de buenas prácticas.
  5.6. Informática forense en la red, dispositivos móviles y en la nube.

TEMARIO PRÁCTICO:

Seminarios

- Realización de un trabajo trabajo grupal que se expondrá en clase relativo a un tipo de ciberdelitos y los medios técnicos para su detección y prevención.

Prácticas de Laboratorio

1. **Herramientas básicas de seguridad**:
   1.1. Información del sistema, administrador de tareas, borrado y recuperación de archivos y copias de

seguridad.

1.2. Desinstalar programas y servicios, edición y limpieza del registro, y compresión-descompresión de archivos y carpetas.

1.3. Gestión de contraseñas, gestión de eventos del sistema, y conexiones de red.

2. **Identidad digital y privacidad**.

2.1. Identidad digital, *egosurfing* y *google hacking*.

2.2. Navegación privada, rastreo (*cookies*) y complementos de seguridad/privacidad para la navegación.

2.3. Técnicas *anti-phishing*.

2.4. Cifrado de datos-dispositivos, y esteganografía.

2.5. Filtrado de correo y limpieza de metadatos.

3. **Herramientas para la prevención y detección de delitos informáticos**.

3.1. Configuración de cortafuegos y análisis de *malware*.

3.2. Análisis de vulnerabilidades, creación de listas blancas, análisis de la red y actualizaciones.

4. **Informática forense e informe pericial**.

4.1 Preservación y análisis forense de evidencias.

BIBLIOGRAFÍA

BIBLIOGRAFÍA FUNDAMENTAL:

- 1. Fernández Teruelo, J. G., Cibercrimen. Los delitos cometidos a través de Internet, Constitutio Criminalis Carolina, 2007.
- 2. Jonathan Clough, Principles of Cybercrime, Cambridge University Press, 2010.
- 3. P.W. Singer y Allan Friedman, Cybersecurity and Cyberware: What Everyone Needs to Know, Oxford University Press, 2014.
- 4. Raoul Chiesa, Stefania Ducci, y Silvio Ciappi, Profiling Hackers. The Science of Criminal Profiling ass Applied to the World of Hacking, CRC Press, 2009.
- 5. Debra Littlejohn y Michael Cross, Scene of the Cybercime, 2nd Ed., Syngress, 2008.
- 6. Chuch Easttom y Det Jeff Taylor, Computer Crime, Investigation, and the Law, Course Technology, CENGAGE Learning, 2011.
- 7. ITU, Comprensión del Ciberdelito: Fenómenos, Dificultades y Respuesta Jurídica, Unión Internacional de Telecomunicaciones (ITU), Sept. 2012. (disponible en http://www.itu.int/en/ITU-D/Cybersecurity/Documents/CybcrimeS.pdf).
- 8. K. Jaishandar, Ed., Cybercriminology. Exploring Internet crimes and Criminal Behavior, CRC Press, 2011.
- 9. Fernando Miró Llinares, El cibercrimen: Fenomenología y criminología de la delincuencia en el ciberespacio, Marcial Pons, 2012.
- 10. Ernesto Martínez de Carvajal Hedrich, Informática Forense. 44 casos reales, Editorial Ernesto Martínez de Carvajal Hedrich, 2012.
- 11. Rafael López Rivera, El peritaje informático y tecnológico, Editor Rafael López Rivera, 2012.
- 12. Juan Diego Pérez Villa, Guía Visual de Introducción a la Informática, Anaya, 2014.
- 13. Brett Shavers, Cybercrime Case Presentation. Using Digital Forensics and Investigative Techiques to Identify Cybercrime Suspects, Syngress, 2013.

- 14. Eoghan Casey, Digital Evidence and Computer Crime. Forensic Science, Computers and The Internet, 3th Ed., Academic Press, Elsevier, 2011.
- 15. Glenn Brookshear, J., Introducción a la Computación, Pearson Educación, 2012.
- 16. Barceló Ordinas, J.M., et al. Redes de Computadores, Universitat Oberta de Catalunya, 2004.
- 17. Stallings, W. Fundamentos de Seguridad en Redes, Aplicaciones y Estándares, Pearson Educación, 2004.
- 18. Stallings, W. y Brown, L., Computer Security. Principles and Practice, Pearson, 2012.
- 19. Tori, C. Hacking Ético, Carlos Tori, 2008.

BIBLIOGRAFÍA COMPLEMENTARIA:

- 1. Romero Casanova, C.M., El cibercrimen: nuevos retos juridicos-penales, nuevas respuestas político-criminales, Granada, 2006.
- 2. Tomasi, S. N., Peritaje judicial informático, Ediciones del Autor, 2010.
- 3. Michael G. Solomon et al., Computer Forensics Jumpstart, Indianopolis, IN : Wiley, 2011.
- 4. Velasco Núñez, E., Delitos cometidos a través de Internet : cuestiones procesales, Madrid, La Ley, 2010.
- 5. Seminario Duque de Ahumada, Seguridad y nuevas tecnologías, XX Seminario "Duque de Ahumada", (7 y 8 de mayo de 2008), Madrid, Ministerio del Interior, 2009
- 6. Bryant, R. (Ed.), Investigating digital crime, Chichester, England ; Hoboken, N.J. : J. Wiley & Sons, 2008.
- 7. Bejtlich, R.The Tao of Networking Security Monitoring. Beyond Instruction Detection, Addison-Wesley Professional, 2004.
- 8. Aissi, S., Dabbous, N. y Prasad, A. R., Security for Mobile Network and Platforms, Artech House, 2006.
- 9. Rash, M. et al., Intrusión Prevention and Active Response. Deploing Network and Host IPS, Syngress, 2005.
- 10. Cuesta Arzamendi, J. L. de la, Derecho Penal Informático, Civitas, 2010.
- 11. Marjie T. Britz, Computer Forensics and Cyber Crime: An Introduction, 2/E, Prentice Hall, 2009.
- 12. Altheide, C. y Carvey, H., Digital Forensics with Open Source Tools, Syngress, 2011.
- 13. Mahid Yar, Cybercrime and Society, Sage Publications, 2006.
- 14. Panagiotis Kanellis et al., Digital Crime and Forensic Science in Cyberspace, Idea Group Publishing, 2006.

ENLACES RECOMENDADOS

Plataforma docente: https://prado.ugr.es
Página web del Departamento: https://lsi.ugr.es/lsi/node/2844

METODOLOGÍA DOCENTE

La metodología que se propone parte de combinar distintas herramientas docentes –lección magistral, resolución de problemas, prácticas de laboratorio (informática), demostraciones, exposición de trabajos y tutorías académicas- con objeto de crear una metodología activa y participativa que permita que el estudiante

no solo adquiera los conceptos fundamentales de la Asignatura sino que pueda seguir profundizando en la materia de forma autónoma mediante la realización de actividades formativas teorico-prácticas, seminarios, actividades presenciales y no presenciales (individuales y grupales).

1) **Lección magistral y Actividades prácticas**:

- **Descripción**: El trabajo presencial estará repartido entre las clases de teoría y la prácticas de laboratorio. En teoría se presentan los conceptos propios de la materia haciendo uso de lecciones magistrales participativas con medios audiovisuales completadas con la resolución de ejercicios prácticos para reforzar los conocimientos. En las clases prácticas se plantean actividades para que el estudiante sepa como actuar a partir de los conocimientos adquiridos mediante el uso de una guía de laboratorio que describe las herramientas que se usan para resolver las actividades propuestas.
- **Propósito**: Transmitir los contenidos de la materia motivando al alumnado a la reflexión, facilitándole el descubrimiento de las relaciones entre diversos conceptos y formarlo una mentalidad crítica. Desarrollo en el alumnado de las habilidades instrumentales de la materia.
- **Contenido en ECTS**: 55 horas presenciales (2,2 ETCS).
- **Competencias**: G2, G5, G11, G12, G13, E2, E5, E7, E11, E16 y E17.
- **Metodologías**: Lección magistral, resolución de problemas, prácticas de laboratorio, demos y tutorías académicas.

3) **Actividades no presenciales grupales**:

- **Descripción**: Durante el desarrollo del curso, se propondrá el estudio monográfico por parte de los alumnos, en pequeños grupos, de algunas figuras delictivas informáticas así como las herramientas para prevenirlas y detectarlas. Tales trabajos serán supervisados por el profesor, suministrando bibliografía básica a utilizar, material jurisprudencial e informático, así como la metodología para su elaboración. Los mejores trabajos pueden ser expuestos y discutidos en clase.
- **Propósito**: Fomentar el estudio profundo y crítico de temas específicos mediante el trabajo en equipo.
- **Contenido en ECTS**: 45 horas no presenciales (1,8 ECTS):
- **Competencias**: G2, G5, G11, G12, G13, E2, E5, E7, E11, E16 y E17.
- **Metodologías**:

4) **Actividades no presenciales individuales**:

- **Descripción**: recoge tanto (1) actividades (guiadas o no) propuestas por el profesor a través de las cuales y de forma individual se profundiza en aspectos concretos de la materia de cara a avanzar en las adquisición de determinados conocimientos, (2) estudio y trabajo autónomo de los contenidos de la materia, y (3) Actividades de evaluación (informes, pruebas objetivas, etc.).
- **Propósito**: Favorecer en el estudiantes la capacidad de autoregulación de su aprendizaje: planificación, evaluación, adecuación al contexto e intereses.
- **Contenido en ECTS**: 45 horas no presenciales (1,8 ECTS).
- **Competencias**: G2, G5, G11, G12, G13, E2, E5, E7, E11, E16 y E17.

5) **Tutorías académicas**:

- **Descripción**: destinadas tanto a orientar el trabajo autónomo individual como grupal de los estudiantes como para profundizar o aclarar los contenidos de la materia.

- **Propósito**: (1) orientar el trabajo autónomo individual y grupal, (2) profundizar en elementos concretos, y (3) orientar en la formación académica del estudiante.
- **Contenidos en ECTS**: 5 horas presenciales, grupales e individuales (0.2 ECTS)
- **Competencias**: G2, G5, G11, G12, G13, E2, E5, E7, E11, E16 y E17.
- **Metodología docente**: Tutorías académicas.

EVALUACIÓN (INSTRUMENTOS DE EVALUACIÓN, CRITERIOS DE EVALUACIÓN Y PORCENTAJE SOBRE LA CALIFICACIÓN FINAL, ETC.)

Como establece el punto 2 del Artículo 6 de la Normativa de Evaluación y de calificación de los estudiantes de la Universidad de Granada (NCG71/2, accesible desde el enlace https://lsi.ugr.es/lsi/normativa_examenes), la evaluación de la asignatura será en la convocatoria ordinaria mediante la modalidad de evaluación continua. Quienes deseen la realización de un "Examen Único Final" deberán solicitarlo en los términos que establece la citada normativa (Art. 8).

- Convocatoria ordinaria

La evaluación continua constará de las siguientes actividades obligatorias:

- *Teoría*: Se realizarán dos pruebas objetivas individuales por escrito que constarán cuestiones concretas de respuesta corta sobre los contenidos teóricos del tema (similares a las existentes en la relaciones de ejercicios propuestos). Esta parte contribuye con un 40% de peso a la calificación final.
- *Prácticas*: Para cada una de las prácticas, que se realizan en individualmente, o en grupo dependiendo del número de matriculados, se deberá entregar una memoria de la misma donde se expliquen los pasos seguidos para la solución a un caso práctico propuesto en la Guía de Prácticas. Esta parte contribuye con un 40% a la calificación final si se realizan todos los supuestos.
- *Trabajo grupal tutorizado*: durante el semestre se realizará un trabajo en grupo tutorizado que será evaluado mediante rúbrica y se expondrá en clase. Esta parte contribuye con 20% a la calificación final: 10% para el trabajo y 10% la presentación del mismo.

La calificación final es la suma de las calificaciones de teoría, prácticas y seminarios y trabajos tutorizados. Condición previa para realizar la suma de cada parte calificable es que se debe obtener al menos un 2 sobre 5 de la calificación en teoría y, otro tanto, en prácticas.

Además se establecen las siguientes consideraciones generales:

- Para poder superar la evaluación continuada será necesario haber realizado un mínimo del 80% de todas las actividades propuestas, tanto para teoría como en prácticas.
- La calificación final de la asignatura es la suma de las calificaciones de cada una de las actividades descritas anteriormente.
- Para superar la Asignatura es necesario obtener un mínimo de 5 puntos en la calificación final.
- Se recomienda la asistencia tanto a clases teóricas como prácticas, si bien la misma no es obligatoria, y hacer uso de las tutorías (individuales o grupales) para resolver dudas surgidas en el desarrollo de la materia.

- En todas las actividades se tendrá especial cuidado en adjuntar, en virtud del Art. 15 de la Normativa, una declaración explícita de autoría.

- Convocatoria extraordinaria y convocatoria especial

Tanto en la convocatoria extraordinaria como en la Convocatoria Especial (Artículo 21 de la Normativa) se establece el mismo sistema y consideraciones que en el Examen Único Final que se describe en el siguiente Apartado.

DESCRIPCIÓN DE LAS PRUEBAS QUE FORMARÁN PARTE DE LA EVALUACIÓN ÚNICA FINAL ESTABLECIDA EN LA "NORMATIVA DE EVALUACIÓN Y DE CALIFICACIÓN DE LOS ESTUDIANTES DE LA UNIVERSIDAD DE GRANADA"

El sistema de evaluación que se describe a continuación es válido para las convocatorias de examen extraordinarias, especiales y exámenes únicos finales, y consta de:

- *Teoría* – examen final escrito sobre el temario de la Asignatura. Constará de preguntas cortas y/o ejercicios similares a los propuestos en clase. Su contribución a la calificación final es del 50% y para superarlo es necesario obtener un mínimo de 2 puntos sobre 5.
- *Prácticas* – examen final en laboratorio o con computador personal. Constará de preguntas relacionadas con los ejercicios propuestos en la Guía de Prácticas. Previo al examen el estudiante habrá tenido que realizar una memoria documentando las soluciones a los ejercicios propuestos en la Guía de prácticas. El examen de prácticas tiene un peso de 30% en la calificación final y la memoria de prácticas de un 20%. Para superarla es necesario obtener un mínimo de 2 puntos sobre 5.

Además se aplican las consideraciones generales:

- La calificación final de la asignatura es la suma de las calificaciones de cada una de las actividades descritas anteriormente.
- Para superar la Asignatura es necesario obtener un mínimo de 5 puntos en la calificación final.
- En todas las actividades se tendrá especial cuidado en adjuntar, en virtud del Art. 15 de la Normativa, una declaración explícita de autoría.

INFORMACIÓN ADICIONAL

ADENDA DE LA GUIA DOCENTE DE LA ASIGNATURA
SEGURIDAD EN REDES Y TELECOMUNICACIONES

Curso 2019-2020

(Fecha de aprobación de la adenda: 28/04/2020)

GRADO EN EL QUE SE IMPARTE		Grado en Criminología			
MÓDULO	MATERIA	CURSO	SEMESTRE	CRÉDITOS	TIPO
Optativas	Seguridad en Redes y Telecomunicaciones	4º	7º	6	Optativa

ATENCIÓN TUTORIAL	
HORARIO	HERRAMIENTAS PARA LA ATENCIÓN TUTORIAL
Martes y Miércoles 10:30-13:30 horas	Correo electrónico: jagomez@ugr.es Video-tutorías (concertarla previamente por correo): https://meet.google.com/amw-ogac-zho

ADAPTACIÓN DEL TEMARIO TEÓRICO Y PRÁCTICO

No es necesaria la adaptación de contenidos del temario. Para aquellos pocos supuestos prácticos que sea necesaria la sustitución de alguna herramienta de prácticas dependiendo del sistema operativo que use el estudiante, se buscará y cambiará a una herramienta equivalente a la que se propone en la Guía de Práctica.

MEDIDAS DE ADAPTACIÓN DE LA METODOLOGÍA DOCENTE
(Actividades formativas indicando herramientas para el desarrollo de la docencia no presencial, si procede)

- Dado que el estudiante dispone de todo el material en la plataforma docente tanto de teoría, guiones de prácticas y programas para el desarrollo de las prácticas, las video-tutorías permitirán solventar cualquier duda que el estudiante encuentre tanto en los contenidos teóricos como prácticos.
- Dado que no hay docencia presencial pues es del primer cuatrimestre, por lo que no es necesaria adaptación metodológica. Solo se adaptan las tutorías y el examen correspondiente a la convocatoria extraordinaria.

MEDIDAS DE ADAPTACIÓN DE LA EVALUACIÓN NO PRESENCIAL
(Herramientas alternativas de evaluación no presencial, indicando instrumentos, criterios de evaluación y porcentajes sobre la calificación final)

Convocatoria Ordinaria

Cerrada

Convocatoria Extraordinaria

- **Memoria de Prácticas**
  Realizar los ejercicios propuestos en las Guías de Prácticas, disponibles en Prado, y confeccionar una memoria con las soluciones a los ejercicios propuesto mostrando las evidencias necesarias que indiquen su realización. Esta memoria se sube a la actividad correspondiente en la plataforma docente.
  Criterio de evaluación: Se valora la correctitud de las soluciones de los ejercicios propuestos. Se deben completan al menos el 80% de las actividades.
  Porcentaje sobre calificación final: 40%
- **Trabajo escrito**
  Realizar un trabajo escrito de 6 páginas de extensión en el que se aborda el estudio de uno de los tipos de cibe-crimen estudiados en clase, a elección del estudiante, centrándose en cómo se materializa, caracterización de los actores que intervienen en el mismo, y estudiando las posibilidades de prevención o mitigación del mismo desde la tecnología (procedimientos o herramientas).
  Criterio de evaluación: Se valorará la claridad y exactitud de la exposición en su totalidad y, especialmente, la relativa a los procedimientos o herramientas que se pueden usar para prevenir o mitigar el ciber-delito seleccionado.
  Porcentaje sobre calificación final: 20%
- **Prueba oral**
  En la fecha prevista por el Centro, se realizará una prueba oral por video-conferencia (mismo enlace de tutorías) en la que se planteara a los estudiantes una pregunta por tema de teoría y el estudiante tendrá 10 minutos por pregunta. Cada pregunta aborda de forma concreta algunos de los aspectos más relevantes del tema correspondiente (al igual que en la convocatoria ordinaria y similares a las que aparecen en las relaciones de ejercicios). En caso de no ser posible realizar una video-conferencia, si realizarán las preguntas a través de Prado, en las que será posible usar material se exigirá un mayor detalle en las respuestas y el tiempo de la prueba será 50 minutos exactos.
  Criterio de evaluación: Las respuestas de ajustan a los contenidos impartidos de la materia.
  Porcentaje sobre calificación final: 40%

MEDIDAS DE ADAPTACIÓN DE LA EVALUACIÓN ÚNICA FINAL NO PRESENCIAL
(Herramientas alternativas de evaluación no presencial, indicando instrumentos, criterios de evaluación y porcentajes sobre la calificación final)

No procede por ser convocatoria extraordinaria.

RECURSOS Y ENLACES RECOMENDADOS PARA EL APRENDIZAJE Y EVALUACIÓN NO PRESENCIAL
(Alternativas a la bibliografía fundamental y complementaria recogidas en la Guía Docente)

RECURSOS:

- En caso de ser necesario y a petición del estudiante, se sustituirá aquella bibliográfica que no esté disponible por bibliografía accesible *online* a través de la Biblioteca electrónica de la UGR.

ENLACES:

- Las Guías de prácticas contienen los enlaces a los manuales de aquellas herramientas complejas que requieran más información de la suministrada en la propia guía.
- Tanto en Prado, como en https://lsi.ugr.es/jagomez/srt, están disponibles los programas para la realización de las prácticas.

INFORMACIÓN ADICIONAL
(Cumplimentar con el texto correspondiente, si procede)