

	<b>PLANIFICACIÓN DOCENTE</b>		<b>IES VIRGEN DEL CARMEN</b>	
	<b>PROGRAMACIÓN</b>		Paseo de la Estación nº 44 23008 Jaén Tel. 953366942 – Fax: 953366944 <a href="http://www.iesvirgendelcarmen.com">www.iesvirgendelcarmen.com</a>	
	MD850401	Rev. 4	15/02/2018	Página 1 de 32

<b>MÓDULO:</b>	<b>HACKING ÉTICO</b>
<b>CURSO:</b>	<b>2022/2023</b>

<b>DEPARTAMENTO</b>	<b>INFORMÁTICA</b>
<b>CICLO FORMATIVO</b>	<b>CETIC</b>
<b>PROFESORES</b>	<b>MIGUEL ÁNGEL PALOMARES ORTEGA</b>

# ÍNDICE DE CONTENIDO

NOTA: Se genera/actualiza automáticamente desde “Insertar → Índice y tablas→ tabla de contenido”

1.	Objetivos Generales.....	4
2.	Metodología.....	6
3.	Competencias Profesionales Generales .....	7
4.	Evaluación y Recuperación .....	9
4.1.	Procedimientos de Evaluación.....	9
4.2.	Criterios de ponderación.....	9
4.3.	Criterios de evaluación .....	10
4.4.	Criterios de recuperación.....	10
4.5.	Procedimiento para subida de nota .....	11
4.6.	Evaluación de Competencias Profesionales .....	12
5.	Atención a la diversidad .....	13
5.1.	Alumnos de admisión tardía .....	13
5.2.	Alumnos con necesidades educativas especiales.....	13
5.3.	Alumnos con compatibilidad laboral y/o modularidad .....	13
5.4.	Alumnado con altas capacidades .....	13
6.	Contenidos .....	14
6.1.	Relación de bloques temáticos.....	14
6.2.	Secuenciación de contenidos .....	14
6.2.1.	Unidad didáctica 1: Introducción al Hacking Ético.....	14
6.2.2.	Unidad didáctica 2: Hacking en redes inalámbricas.....	16
6.2.3.	Unidad didáctica 3: Reconocimiento.....	17
6.2.4.	Unidad didáctica 4: Escaneo de red.....	18
6.2.5.	Unidad didáctica 5: Análisis de vulnerabilidades.....	19
6.2.6.	Unidad didáctica 6: Explotación de vulnerabilidades .....	20
6.2.7.	Unidad didáctica 7: Postexplotación .....	22
6.2.8.	Unidad didáctica 8: Ingeniería social y phishing.....	23
6.2.9.	Unidad didáctica 9: Hacking de servicios Web.....	24
7.	Ponderación de Resultados de Aprendizaje.....	27
8.	Materias Transversales .....	29
9.	Actividades Complementarias y Extraescolares.....	31
10.	Bibliografía, Materiales y Recursos .....	32
10.1.	Bibliografía de departamento .....	32
10.2.	Materiales, recursos y laboratorios .....	32

Código:	Rev.:	Fecha Implantación:	Entregar a:	Página 2 de 32
MD850401	4	15/02/2018	Jefa/e depto. → Jefatura estudios	

<b>Código:</b>	<b>Rev.:</b>	<b>Fecha Implantación:</b>	<b>Entregar a:</b>	<b>Página 3 de 32</b>
MD850401	4	15/02/2018	Jefa/e depto. → Jefatura estudios	

# 1. OBJETIVOS GENERALES

Los objetivos generales de este ciclo formativo, especificados en el Real Decreto 479/2020, del 7 de abril, son los siguientes:

a) Identificar los principios de la organización y normativa de protección en ciberseguridad, planificando las acciones que es preciso adoptar en el puesto de trabajo para la elaboración del plan de prevención y concienciación.

b) Auditar el cumplimiento del plan de prevención y concienciación de la organización, definiendo las acciones correctoras que puedan derivarse para incluirlas en el plan de securización de la organización.

c) Detectar incidentes de ciberseguridad implantando los controles, las herramientas y los mecanismos necesarios para su monitorización e identificación.

d) Analizar y dar respuesta a incidentes de ciberseguridad, identificando y aplicando las medidas necesarias para su mitigación, eliminación, contención o recuperación.

e) Elaborar análisis de riesgos para identificar activos, amenazas, vulnerabilidades y medidas de seguridad.

f) Diseñar e implantar planes de medidas técnicas de seguridad a partir de los riesgos identificados para garantizar el nivel de seguridad requerido.

g) Configurar sistemas de control de acceso, autenticación de personas y administración de credenciales para preservar la privacidad de los datos.

h) Configurar la seguridad de sistemas informáticos para minimizar las probabilidades de exposición a ataques.

i) Configurar dispositivos de red para cumplir con los requisitos de seguridad.

j) Administrar la seguridad de sistemas informáticos en red aplicando las políticas de seguridad requeridas para garantizar la funcionalidad necesaria con el nivel de riesgo de red controlado.

k) Aplicar estándares de verificación requeridos por las aplicaciones para evitar incidentes de seguridad.

l) Automatizar planes de despliegado de software respetando los requisitos relativos a control de versiones, roles, permisos y otros para conseguir un despliegado seguro.

m) Aplicar técnicas de investigación forense en sistemas y redes en los ámbitos del almacenamiento de la información no volátil, de los dispositivos móviles, del Cloud y de los sistemas IoT (Internet de las cosas), entre otros, para la elaboración de análisis forenses.

n) Analizar informes forenses identificando los resultados de la investigación para extraer conclusiones y realizar informes.

ñ) Combinar técnicas de *hacking* ético interno y externo para detectar vulnerabilidades que permitan eliminar y mitigar los riesgos asociados.

o) Identificar el alcance de la aplicación normativa dentro de la organización, tanto internamente como en relación con terceros para definir las funciones y responsabilidades de todas las partes.

Código:	Rev.:	Fecha Implantación:	Entregar a:	Página 4 de 32
MD850401	4	15/02/2018	Jefa/e depto. → Jefatura estudios	

p) Revisar y actualizar procedimientos de acuerdo con normas y estándares actualizados para el correcto cumplimiento normativo en materia de ciberseguridad y de protección de datos personales.

q) Desarrollar manuales de información, utilizando herramientas ofimáticas y de diseño asistido por ordenador para elaborar documentación técnica y administrativa.

r) Analizar y utilizar los recursos y oportunidades de aprendizaje relacionados con la evolución científica, tecnológica y organizativa del sector y las tecnologías de la información y la comunicación, para mantener el espíritu de actualización y adaptarse a nuevas situaciones laborales y personales.

s) Desarrollar la creatividad y el espíritu de innovación para responder a los retos que se presentan en los procesos y en la organización del trabajo y de la vida personal.

t) Evaluar situaciones de prevención de riesgos laborales y de protección ambiental, proponiendo y aplicando medidas de prevención personales y colectivas, de acuerdo con la normativa aplicable en los procesos de trabajo, para garantizar entornos seguros.

u) Identificar y proponer las acciones profesionales necesarias para dar respuesta a la accesibilidad universal y al «diseño para todas las personas».

v) Identificar y aplicar parámetros de calidad en los trabajos y actividades realizados en el proceso de aprendizaje, para valorar la cultura de la evaluación y de la calidad y ser capaces de supervisar y mejorar procedimientos de calidad.

<b>Código:</b>	<b>Rev.:</b>	<b>Fecha Implantación:</b>	<b>Entregar a:</b>	<b>Página 5 de 32</b>
MD850401	4	15/02/2018	Jefa/e depto. → Jefatura estudios	

## 2. METODOLOGÍA

La metodología empleada se basa en los siguientes principios:

### a.- Flexible

En esta asignatura se aplican varias metodologías. La técnica utilizada normalmente para las clases teóricas es la lección magistral del método expositivo, para transmitir los conocimientos básicos del módulo y los conceptos a utilizar posteriormente.

### b.- Activa y participativa

Como en este método el profesor lleva la iniciativa, se intenta evitar que el alumnado permanezca pasivo utilizando normalmente una metodología activa y participativa, como la técnica del torbellino de ideas y la realización de trabajos en grupos pequeños, para que el alumno/a participe en el proceso de enseñanza aprendizaje y se habitúe a la búsqueda y consulta de material bibliográfico, manuales, Internet, etc., así como a la exposición de dichos trabajos.

### c.- Explicativa demostrativa

Para las clases prácticas, en las que se utiliza el ordenador, la metodología utilizada, además de la activa participativa, es la explicativa demostrativa, en la que el profesor transmite el conocimiento a través de la realización práctica de las tareas en el ordenador, la cual el alumnado observa. Luego propone al alumno/a resolver un problema en el que se tiene que aplicar la información recibida y descubrir por sí mismo algunos conocimientos a través del ensayo – error para obtener la solución.

### d.- Motivadora e interactiva

El profesor intenta crear un ambiente que favorezca la interacción profesor-alumno/a, integrando aspectos informativos, formales y socio-afectivos que estimulen el desarrollo del aprendizaje. También se utilizan como ejes del planteamiento metodológico el diálogo, el debate y la confrontación de ideas e hipótesis, entendiendo el proceso de enseñanza como la mejor forma en que el alumno/a es capaz de aprender y asimilar conceptos e informaciones.

### e.- Aprendizaje significativo

El profesor favorece el aprendizaje significativo, facilitando que los alumnos/as sean capaces de establecer relaciones entre conocimientos y experiencias que ya poseen y la nueva información. También debe ser capaz de estimular y regular las interacciones entre profesor-alumno/a, alumno/a-alumno/a, facilitando el trabajo individual y alentando la investigación en grupo.

Código:	Rev.:	Fecha Implantación:	Entregar a:	Página 6 de 32
MD850401	4	15/02/2018	Jefa/e depto. → Jefatura estudios	

### 3. COMPETENCIAS PROFESIONALES GENERALES

La competencia general de este curso de especialización consiste en definir e implementar estrategias de seguridad en los sistemas de información realizando diagnósticos de ciberseguridad, identificando vulnerabilidades e implementando las medidas necesarias para mitigarlas aplicando la normativa vigente y estándares del sector, siguiendo los protocolos de calidad, de prevención de riesgos laborales y respeto ambiental.

Las competencias profesionales, personales y sociales de este curso de especialización son las que se relacionan a continuación:

- a) Elaborar e implementar planes de prevención y concienciación en ciberseguridad en la organización, aplicando la normativa vigente.
- b) Detectar e investigar incidentes de ciberseguridad, documentándolos e incluyéndolos en los planes de securización de la organización.
- c) Diseñar planes de securización contemplando las mejores prácticas para el bastionado de sistemas y redes.
- d) Configurar sistemas de control de acceso y autenticación en sistemas informáticos, cumpliendo los requisitos de seguridad y minimizando las posibilidades de exposición a ataques.
- e) Diseñar y administrar sistemas informáticos en red y aplicar las políticas de seguridad establecidas, garantizando la funcionalidad requerida con un nivel de riesgo controlado.
- f) Analizar el nivel de seguridad requerido por las aplicaciones y los vectores de ataque más habituales, evitando incidentes de ciberseguridad.
- g) Implantar sistemas seguros de despliegado de software con la adecuada coordinación entre los desarrolladores y los responsables de la operación del software.
- h) Realizar análisis forenses informáticos analizando y registrando la información relevante relacionada.
- i) Detectar vulnerabilidades en sistemas, redes y aplicaciones, evaluando los riesgos asociados.
- j) Definir y aplicar procedimientos para el cumplimiento normativo en materia de ciberseguridad y de protección de datos personales, implementándolos tanto internamente como en relación con terceros.
- k) Elaborar documentación técnica y administrativa cumpliendo con la legislación vigente, respondiendo a los requisitos establecidos.
- l) Adaptarse a las nuevas situaciones laborales, manteniendo actualizados los conocimientos científicos, técnicos y tecnológicos relativos a su entorno profesional, gestionando su formación y los recursos existentes en el aprendizaje a lo largo de la vida.
- m) Resolver situaciones, problemas o contingencias con iniciativa y autonomía en el ámbito de su competencia, con creatividad, innovación y espíritu de mejora en el trabajo personal y en el de los miembros del equipo.

<b>Código:</b>	<b>Rev.:</b>	<b>Fecha Implantación:</b>	<b>Entregar a:</b>	<b>Página 7 de 32</b>
MD850401	4	15/02/2018	Jefa/e depto. → Jefatura estudios	

n) Generar entornos seguros en el desarrollo de su trabajo y el de su equipo, supervisando y aplicando los procedimientos de prevención de riesgos laborales y ambientales, de acuerdo con lo establecido por la normativa y los objetivos de la organización.

ñ) Supervisar y aplicar procedimientos de gestión de calidad, de accesibilidad universal y de «diseño para todas las personas», en las actividades profesionales incluidas en los procesos de producción o prestación de servicios.

<b>Código:</b>	<b>Rev.:</b>	<b>Fecha Implantación:</b>	<b>Entregar a:</b>	<b>Página 8 de 32</b>
MD850401	4	15/02/2018	Jefa/e depto. → Jefatura estudios	



## 4. EVALUACIÓN Y RECUPERACIÓN

### 4.1. Procedimientos de Evaluación

Para llevar a cabo el proceso de evaluación descrito anteriormente, se deberá tener en cuenta la evolución personal del alumnado y su participación en el grupo. Se realizará una evaluación cuantitativa y cualitativa, llevándose a cabo mediante la observación, el diálogo y el intercambio constante entre el docente y el alumno, además de los trabajos habituales de clase propuestos en las actividades. Entre los procedimientos de evaluación, podemos distinguir los siguientes:

- Técnicas
  - Observación directa. Valorarán la implicación del alumnado en el trabajo individual, en los conocimientos, habilidades y destrezas relacionadas con el módulo, en el trabajo en grupo y en las actitudes personales
  - Medición. Se realizarán a través de pruebas escritas (u orales, en su caso), cuestionarios, informes, trabajos y presentaciones
  - Técnicas de autoevaluación y coevaluación. Permitirán favorecer la reflexión y valoración del alumnado sobre sus propias dificultades, así como la participación de sus compañeros junto con el profesor en la regulación del proceso de enseñanza-aprendizaje
- Instrumentos. Para poner en prácticas las técnicas anteriores es necesario emplear procedimientos de evaluación que nos permitan registrar la información sobre el proceso de aprendizaje del alumnado, como las que se indican:
  - Pruebas escritas y orales
  - Rúbricas.
  - Cuaderno docente, que incluirá:
    - Escalas de observación, listas de control y registro anecdótico.
    - Guías y fichas para el registro y revisión de las tareas de los alumnos
    - Guiones más o menos estructurados para registrar los diálogos y entrevistas realizados con los alumnos, sobre todo con los que presentan mayores problemas o dificultades
  - Cuestionarios de autoevaluación, inicio de una unidad o fase de aprendizaje.

A continuación en los siguientes apartados se describe el procedimiento de evaluación, indicando los criterios de ponderación, evaluación en competencias, criterios de calificación, criterios de recuperación y el proceso de evaluación de la enseñanza

### 4.2. Criterios de ponderación

Las herramientas de evaluación serán las siguientes:

- Exámenes realizados en la plataforma Moodle.

Para aprobar el módulo es imprescindible obtener una media de 5 entre todos los exámenes de todas las unidades didácticas, así como obtener como mínimo un 4 en los exámenes de cada unidad didáctica, esto es, es necesario obtener un 4 como mínimo para acceder a la media general.

Código:	Rev.:	Fecha Implantación:	Entregar a:	Página 9 de 32
MD850401	4	15/02/2018	Jefa/e depto. → Jefatura estudios	

### 4.3. Criterios de evaluación

Criterios de Calificación		
Criterio (marcar con una X debajo de SI o NO)	SI	NO
La ortografía resta puntuación		X
Entregar fuera de plazo resta puntuación		X
Los alumnos/as deben llegar a un mínimo de la calificación para acceder a la media <b>Sí, un 4</b>	X	
Los alumnos/as deben superar todas las evaluaciones para aprobar el módulo (si procede, determinar qué evaluaciones debe superar el alumnado para obtener las competencias mínimas)		X
La NO entrega de un número mínimo de prácticas supone directamente que esa parte se recupera con un examen (en caso afirmativo explicar el número de prácticas -el 100%, el 80%, el 50%...-)		X
La NO entrega de ejercicios de clase supone directamente que esa parte se recupera con examen		X

### 4.4. Criterios de recuperación

Criterios de recuperación		
Criterio (marcar con una X debajo de SI o NO)	SI	NO
La calificación final será la misma que la del examen (en caso negativo, explicar las diferencias)	X	
Puede eliminar materia previamente al examen		X
Existen criterios de corrección diferentes entre convocatoria ordinaria y extraordinaria (explicar en caso afirmativo las diferencias)		X
Existe una nota máxima en la recuperación independientemente de la calificación que se obtenga en la misma		X
Otros (a completar):		

#### 4.4.1 Recuperaciones en el período ordinario de clases (antes de la FCT):

Código:	Rev.:	Fecha Implantación:	Entregar a:	Página 10 de 32
MD850401	4	15/02/2018	Jefa/e depto. → Jefatura estudios	

Los alumnos que no hayan superado alguna de las evaluaciones podrán presentarse a las siguientes actividades de recuperación:

- Un examen realizado en la plataforma moodle. Estos exámenes de recuperación se realizarán sólo una vez en el período ordinario.

El alumno que no haya podido asistir regularmente a clase por motivos debidamente justificados realizará los exámenes que no hubiera realizado debido a su falta de asistencia justificada. Para estos alumnos se aplicarán los mismos criterios que los aplicados a los demás alumnos en lo que respecta a las condiciones necesarias para aprobar el módulo.

#### **4.4.2 Recuperaciones en el período no ordinario de clases: (período de recuperación)**

Los alumnos que no hayan superado el módulo en el período ordinario de clases tendrán la oportunidad de realizar las prácticas no efectuadas durante el período ordinario en las clases de recuperación. En este período los alumnos realizarán las siguientes actividades de recuperación:

- Un examen realizado en la plataforma moodle. Estos exámenes de recuperación se realizarán sólo una vez en este periodo.

Al igual que en el período ordinario de clases, para aprobar el módulo en el período de recuperación es imprescindible obtener una media superior o igual a 5 entre todos los exámenes realizados así como un 4 en cada unidad didáctica para acceder a la media.

El alumno que no haya podido asistir regularmente a clase por motivos debidamente justificados realizará las prácticas y ejercicios posteriormente al resto del grupo, así como los exámenes de recuperación no realizados. Para estos alumnos se aplicarán los mismos criterios que los aplicados a los demás alumnos en lo que respecta a las condiciones necesarias para aprobar el módulo.

### **4.5. Procedimiento para subida de nota**

Si los alumnos realizan durante el curso algunas prácticas de ampliación, éstas serán tenidas en cuenta para el procedimiento de subida de nota, cuantificándose esta subida a criterio del profesor y en función de la dificultad de las mismas.

El otro procedimiento de subida de nota, que no es excluyente con el anterior, consiste en la realización de cursos relacionados con los contenidos del módulo en la plataforma formativa de OpenWebinars, de forma que se subirá la nota multiplicando el número de horas totales de los cursos por 0,01. Por ejemplo, si un alumno acredita 40 horas de formación conseguirá una subida de nota de 0,4 puntos.

El alumno podrá subir como máximo 1,5 puntos en la nota final sumando los dos procedimientos anteriores.

<b>Código:</b>	<b>Rev.:</b>	<b>Fecha Implantación:</b>	<b>Entregar a:</b>	<b>Página 11 de 32</b>
MD850401	4	15/02/2018	Jefa/e depto. → Jefatura estudios	

Ambos procedimientos de subida de nota NO servirán para aprobar el módulo sino que la subida de nota se aplicará sólo en el caso en el que el alumno haya aprobado el módulo según los criterios expuestos en apartados anteriores.

#### **4.6. Evaluación de Competencias Profesionales**

La formación del módulo contribuye a alcanzar las competencias profesionales, personales y sociales de este título que se relacionan a continuación:

- i) Detectar vulnerabilidades en sistemas, redes y aplicaciones, evaluando los riesgos asociados.
- k) Elaborar documentación técnica y administrativa cumpliendo con la legislación vigente, respondiendo a los requisitos establecidos.
- l) Adaptarse a las nuevas situaciones laborales, manteniendo actualizados los conocimientos científicos, técnicos y tecnológicos relativos a su entorno profesional, gestionando su formación y los recursos existentes en el aprendizaje a lo largo de la vida.
- m) Resolver situaciones, problemas o contingencias con iniciativa y autonomía en el ámbito de su competencia, con creatividad, innovación y espíritu de mejora en el trabajo personal y en el de los miembros del equipo.
- n) Generar entornos seguros en el desarrollo de su trabajo y el de su equipo, supervisando y aplicando los procedimientos de prevención de riesgos laborales y ambientales, de acuerdo con lo establecido por la normativa y los objetivos de la organización.
- ñ) Supervisar y aplicar procedimientos de gestión de calidad, de accesibilidad universal y de «diseño para todas las personas», en las actividades profesionales incluidas en los procesos de producción o prestación de servicios.

Código:	Rev.:	Fecha Implantación:	Entregar a:	Página 12 de 32
MD850401	4	15/02/2018	Jefa/e depto. → Jefatura estudios	

## **5. ATENCIÓN A LA DIVERSIDAD**

Los casos más corrientes a los que nos enfrentamos en estas enseñanzas son los de aquellos alumnos/as que van más adelantados al resto del grupo, bien sea porque ya conocen el tema como es el caso de repetidores o bien porque lo comprenden rápidamente; estos alumnos serán atendidos con actividades de ampliación, las cuales les proporcionarán puntuación adicional. Por otro lado pueden existir otros alumnos/as a los que por el contrario, les pueda costar más trabajo llegar a los mínimos exigidos, y a éstos se les mandarán también ejercicios adicionales, pero en este caso de refuerzo.

### ***5.1. Alumnos de admisión tardía***

Si por cualquier motivo se incorporara algún alumno de forma tardía, se le dará acceso a todo el material impartido hasta ese momento. Además se le hará un seguimiento aparte en el cual el alumno podrá preguntar todas las posibles dudas que le surgieran respecto a la materia ya dada.

En caso de que ya se hubiesen hecho exámenes o prácticas se le dará la oportunidad de realizar dichas pruebas siempre y cuando el motivo de la incorporación tardía esté justificado.

### ***5.2. Alumnos con necesidades educativas especiales***

La evaluación de otros alumnos/as con necesidades educativas especiales, de existir algún caso, se realizarán tomando como referencia los criterios y evaluación establecidos en las adaptaciones curriculares, que, para ello se hubieran realizado y valorando las recomendaciones que por parte del Departamento de Orientación pudieran dictarse.

### ***5.3. Alumnos con compatibilidad laboral y/o modularidad***

En este apartado se seguirán las directrices de la programación de departamento.

### ***5.4. Alumnado con altas capacidades***

Para este tipo de alumnado se propondrá la realización de prácticas de ampliación según se explica en el apartado 4.5.

<b>Código:</b>	<b>Rev.:</b>	<b>Fecha Implantación:</b>	<b>Entregar a:</b>	<b>Página 13 de 32</b>
MD850401	4	15/02/2018	Jefa/e depto. → Jefatura estudios	

## 6. CONTENIDOS

A continuación se detallan las diferentes unidades didácticas con sus correspondientes criterios de evaluación.

### 6.1. Relación de bloques temáticos

Horas totales de módulo: 120

Distribución de las horas

No se contempla agrupamiento en bloques temáticos en este módulo.

### 6.2. Secuenciación de contenidos

#### 6.2.1. Unidad didáctica 1: Introducción al Hacking Ético

Se desarrolla con dos temas: 1. Introducción al hacking ético y 2. Ocultación de la identidad.

Núm.	1	Título	Introducción al Hacking Ético
Objetivos Didácticos		Determina herramientas de monitorización para detectar vulnerabilidades aplicando técnicas de <i>hacking</i> ético.	

Código:	Rev.:	Fecha Implantación:	Entregar a:	Página 14 de 32
MD850401	4	15/02/2018	Jefa/e depto. → Jefatura estudios	

Contenidos Conceptuales	<ul style="list-style-type: none"> <li>- Objetivos de la seguridad informática.</li> <li>- Elementos esenciales del <i>hacking</i> ético.</li> <li>- Diferencias entre <i>hacking</i>, <i>hacking</i> ético, tests de penetración y hacktivismismo.</li> <li>- Recolección de permisos y autorizaciones previos a un test de intrusión.</li> <li>- Fases del <i>hacking</i>.</li> <li>- Auditorías de caja negra y de caja blanca.</li> <li>- Tipos de ataque.</li> <li>- Clasificación de herramientas de seguridad y <i>hacking</i>.</li> <li>- <i>ClearNet</i>, <i>Deep Web</i>, <i>Dark Web</i>, <i>Darknets</i>. Conocimiento, diferencias y herramientas de acceso: <i>Tor</i>, <i>ZeroNet</i>, <i>FreeNet</i>.</li> </ul>
Contenidos Procedimentales	<ul style="list-style-type: none"> <li>• Diferenciar los distintos tipos de hackers</li> <li>• Diferenciar cada una de las fases del <i>hacking</i> ético.</li> <li>• Configurar un proxy TOR</li> <li>• Configurar un servicio oculto en TOR</li> </ul>
Contenidos Actitudinales	<ul style="list-style-type: none"> <li>• Concienciación sobre la importancia de la Ciberseguridad en el mundo actual</li> <li>• Concienciación sobre la necesidad del uso del anonimato en el acceso a internet en ciertas circunstancias</li> </ul>

<b>Código:</b>	<b>Rev.:</b>	<b>Fecha Implantación:</b>	<b>Entregar a:</b>	<b>Página 15 de 32</b>
MD850401	4	15/02/2018	Jefa/e depto. → Jefatura estudios	

Criterios de Evaluación	<p>a) Se ha definido la terminología esencial del <i>hacking</i> ético.</p> <p>b) Se han identificado los conceptos éticos y legales frente al ciberdelito.</p> <p>c) Se ha definido el alcance y condiciones de un test de intrusión.</p> <p>d) Se han identificado los elementos esenciales de seguridad: confidencialidad, autenticidad, integridad y disponibilidad.</p> <p>e) Se han identificado las fases de un ataque seguidas por un atacante.</p> <p>f) Se han analizado y definido los tipos vulnerabilidades.</p> <p>g) Se han analizado y definido los tipos de ataque.</p> <p>h) Se han determinado y caracterizado las diferentes vulnerabilidades existentes.</p> <p>i) Se han determinado las herramientas de monitorización disponibles en el mercado adecuadas en función del tipo de organización.</p>
Competencias profesionales	l,k,l,m,n,ñ

### 6.2.2. Unidad didáctica 2: Hacking en redes inalámbricas

Núm.	2	Título	<b>Hacking en redes inalámbricas</b>
Objetivos Didácticos	Ataque y defensa en entorno de pruebas, de las comunicaciones inalámbricas		
Contenidos Conceptuales	<ul style="list-style-type: none"> <li>– Comunicación inalámbrica.</li> <li>– Modo infraestructura, ad-hoc y monitor.</li> <li>– Análisis y recolección de datos en redes inalámbricas.</li> <li>– Técnicas de ataques y exploración de redes inalámbricas.</li> <li>– Ataques a otros sistemas inalámbricos.</li> <li>– Realización de informes de auditoría y presentación de resultados.</li> <li>– Interceptación de comunicaciones utilizando distintas técnicas.</li> <li>– Manipulación e inyección de tráfico.</li> </ul>		

Código:	Rev.:	Fecha Implantación:	Entregar a:	Página 16 de 32
MD850401	4	15/02/2018	Jefa/e depto. → Jefatura estudios	



Contenidos Procedimentales	<ul style="list-style-type: none"> <li>• Realizar un ataque capturando el Handshake en entorno de pruebas</li> <li>• Realizar un ataque Evil Twin en entorno de pruebas</li> <li>• Realizar un ataque MIM con ARP poisoning y DNS spoofing en entorno de pruebas.</li> <li>• Configurar una red con seguridad WPA empresarial</li> </ul>
Contenidos Actitudinales	<ul style="list-style-type: none"> <li>• Concienciación sobre la importancia de la Ciberseguridad en el mundo actual</li> <li>• Concienciación sobre la importancia de las buenas prácticas a la hora de configurar una red wifi.</li> </ul>
Criterios Evaluación	<p>a) Se han configurado los distintos modos de funcionamiento de las tarjetas de red inalámbricas.</p> <p>b) Se han descrito las técnicas de encriptación de las redes inalámbricas y sus puntos vulnerables.</p> <p>c) Se han detectado redes inalámbricas y se ha capturado tráfico de red como paso previo a su ataque.</p> <p>d) Se ha accedido a redes inalámbricas vulnerables.</p> <p>e) Se han caracterizado otros sistemas de comunicación inalámbricos y sus vulnerabilidades.</p> <p>f) Se han utilizado técnicas de “Equipo Rojo y Azul”.</p> <p>g) Se han realizado informes sobre las vulnerabilidades detectadas.</p> <p>h) Se ha realizado un ataque de intermediario, leyendo, insertando y modificando, a voluntad, el tráfico intercambiado por dos extremos remotos.</p> <p>b) Se han comprometido contraseñas a través de ataques de diccionario, tablas rainbow y fuerza bruta contra sus versiones encriptadas.</p>
Competencias profesionales	l,k,l,m,n,ñ

### 6.2.3. Unidad didáctica 3: Reconocimiento

<b>Código:</b>	<b>Rev.:</b>	<b>Fecha Implantación:</b>	<b>Entregar a:</b>	<b>Página 17 de 32</b>
MD850401	4	15/02/2018	Jefa/e depto. → Jefatura estudios	

Núm.	3	Título	Reconocimiento
Objetivos Didácticos	Ataca y defiende en entornos de prueba, redes y sistemas consiguiendo acceso a información y sistemas de terceros.		
Contenidos Conceptuales	<ul style="list-style-type: none"> <li>– Fase de reconocimiento (<i>footprinting</i>).</li> <li>– Monitorización de tráfico.</li> </ul>		
Contenidos Procedimentales	<ul style="list-style-type: none"> <li>• Footprinting usando whois</li> <li>• Footprinting usando theharvester</li> <li>• Footprinting usando web.archive.org</li> <li>• Footprinting usando Maltego</li> <li>• Footprinting usando recon-ng</li> </ul>		
Contenidos Actitudinales	<ul style="list-style-type: none"> <li>• Concienciación sobre la importancia de las técnicas de reconocimiento</li> </ul>		
Criterios de Evaluación	<p>a) Se ha recopilado información sobre la red y sistemas objetivo mediante técnicas pasivas.</p> <p>c) Se ha interceptado tráfico de red de terceros para buscar información sensible.</p>		
Competencias profesionales	l,k,l,m,n,ñ		

#### 6.2.4. Unidad didáctica 4: Escaneo de red

Núm.	4	Título	Escaneo de red
Objetivos Didácticos			

<b>Código:</b>	<b>Rev.:</b>	<b>Fecha Implantación:</b>	<b>Entregar a:</b>	<b>Página 18 de 32</b>
MD850401	4	15/02/2018	Jefa/e depto. → Jefatura estudios	

	Ataque y defensa en entorno de pruebas, de redes y sistemas para acceder a sistemas de terceros
Contenidos Conceptuales	<ul style="list-style-type: none"> <li>– Fase de escaneo (<i>fingerprinting</i>).</li> <li>– Monitorización de tráfico.</li> </ul>
Contenidos Procedimentales	<ul style="list-style-type: none"> <li>• Fingerprinting usando fping</li> <li>• Fingerprinting usando nmap</li> <li>• Fingerprinting usando zenmap</li> <li>• Fingerprinting usando shodan</li> <li>• Fingerprinting usando greynoise y zoomeye</li> </ul>
Contenidos Actitudinales	<ul style="list-style-type: none"> <li>• Concienciación sobre la importancia de las técnicas de escaneo</li> </ul>
Criterios de Evaluación	<p>a) Se ha recopilado información sobre la red y sistemas objetivo mediante técnicas pasivas.</p> <p>b) Se ha creado un inventario de equipos, cuentas de usuario y potenciales vulnerabilidades de la red y sistemas objetivo mediante técnicas activas.</p> <p>c) Se ha interceptado tráfico de red de terceros para buscar información sensible.</p>
Competencias profesionales	l,k,l,m,n,ñ

### 6.2.5. Unidad didáctica 5: Análisis de vulnerabilidades

Núm.	5	Título	Análisis de vulnerabilidades		
<b>Código:</b>	<b>Rev.:</b>	<b>Fecha Implantación:</b>	<b>Entregar a:</b>	<b>Página 19 de 32</b>	
MD850401	4	15/02/2018	Jefa/e depto. → Jefatura estudios		

Objetivos Didácticos	Ataque y defensa en entorno de pruebas, de redes y sistemas para acceder a sistemas de terceros
Contenidos Conceptuales	<ul style="list-style-type: none"> <li>– Documentación de vulnerabilidades</li> <li>– Tipos de vulnerabilidades</li> <li>– Monitorización de tráfico</li> <li>– Interceptación de comunicaciones utilizando distintas técnicas.</li> <li>– Herramientas de búsqueda y explotación de vulnerabilidades.</li> </ul>
Contenidos Procedimentales	<ul style="list-style-type: none"> <li>• Análisis de vulnerabilidades usando nmap</li> <li>• Análisis de vulnerabilidades usando nessus</li> <li>• Análisis de vulnerabilidades usando openvas</li> <li>• Análisis de vulnerabilidades buscando en internet</li> </ul>
Contenidos Actitudinales	<ul style="list-style-type: none"> <li>• Concienciación sobre la importancia de las técnicas de análisis de vulnerabilidades</li> <li>• Concienciación sobre las medidas necesarias para minimizar las vulnerabilidades de los sistemas</li> </ul>
Criterios de Evaluación	<p>b) Se ha creado un inventario de equipos, cuentas de usuario y potenciales vulnerabilidades de la red y sistemas objetivo mediante técnicas activas.</p> <p>c) Se ha interceptado tráfico de red de terceros para buscar información sensible.</p>
Competencias profesionales	l,k,l,m,n,ñ

### 6.2.6. Unidad didáctica 6: Explotación de vulnerabilidades

Núm.	6	Título	Explotación de vulnerabilidades
Objetivos Didácticos	Ataque y defensa en entorno de pruebas, de redes y sistemas para acceder a sistemas de terceros		

Código:	Rev.:	Fecha Implantación:	Entregar a:	Página 20 de 32
MD850401	4	15/02/2018	Jefa/e depto. → Jefatura estudios	

Contenidos Conceptuales	<ul style="list-style-type: none"> <li>– Interceptación de comunicaciones utilizando distintas técnicas.</li> <li>– Manipulación e inyección de tráfico.</li> <li>– Herramientas de búsqueda y explotación de vulnerabilidades.</li> <li>– Ingeniería social. <i>Phising</i>.</li> <li>– Escalada de privilegios.</li> <li>– Ataques MIM.</li> </ul>
Contenidos Procedimentales	<ul style="list-style-type: none"> <li>• Aprender a usar metaexploit de manera fluida</li> <li>• Explotación de vulnerabilidades usando metaexploit</li> <li>• Explotación de vulnerabilidades usando exploits de fuentes públicas (internet)</li> <li>• Uso de Cain y Ettercap para realizar ataques MIM</li> </ul>
Contenidos Actitudinales	<ul style="list-style-type: none"> <li>• Concienciación sobre la importancia de las técnicas de explotación de vulnerabilidades</li> <li>• Valorar la importancia de la formación de los usuarios para minimizar el riesgo de ataques por medio de phising e ingeniería social</li> </ul>
Criterios de Evaluación	<p>c) Se ha interceptado tráfico de red de terceros para buscar información sensible.</p> <p>d) Se ha realizado un ataque de intermediario, leyendo, insertando y modificando, a voluntad, el tráfico intercambiado por dos extremos remotos.</p> <p>e) Se han comprometido sistemas remotos explotando sus vulnerabilidades.</p> <p>h) Se ha realizado un ataque de intermediario, leyendo, insertando y modificando, a voluntad, el tráfico intercambiado por dos extremos remotos</p> <p>c) Se ha interceptado tráfico de red de terceros para buscar información sensible.</p>
Competencias profesionales	I,k,l,m,n,ñ

<b>Código:</b>	<b>Rev.:</b>	<b>Fecha Implantación:</b>	<b>Entregar a:</b>	<b>Página 21 de 32</b>
MD850401	4	15/02/2018	Jefa/e depto. → Jefatura estudios	

### 6.2.7. Unidad didáctica 7: Postexplotación

Núm.	7	Título	Postexplotación
Objetivos Didácticos		Consolida y utiliza sistemas comprometidos garantizando accesos futuros	
Contenidos Conceptuales		<ul style="list-style-type: none"> <li>– Administración de sistemas de manera remota.</li> <li>– Ataques y auditorías de contraseñas.</li> <li>– Pivotaje en la red.</li> <li>– Instalación de puertas traseras con troyanos (<i>RAT, Remote Access Trojan</i>).</li> <li>– Ingeniería social. Phishing.</li> </ul>	
Contenidos Procedimentales		<ul style="list-style-type: none"> <li>• Uso de herramientas de fuerza bruta para averiguar las contraseñas (John the ripper y hashcat)</li> <li>• Creación de RATs usando metaexploit</li> <li>• Uso de Cain y Ettercap para realizar ataques MIM</li> </ul>	
Contenidos Actitudinales		<ul style="list-style-type: none"> <li>• Concienciación sobre la importancia de las técnicas de explotación de vulnerabilidades</li> <li>• Valorar la importancia de la formación de los usuarios para minimizar el riesgo de ataques por medio de phishing e ingeniería social</li> <li>• Valorar la importancia de la formación de los usuarios para la elección de contraseñas seguras</li> </ul>	

Criterios de Evaluación	<p>a) Se han administrado sistemas remotos a través de herramientas de línea de comandos.</p> <p>b) Se han comprometido contraseñas a través de ataques de diccionario, tablas rainbow y fuerza bruta contra sus versiones encriptadas.</p> <p>c) Se ha accedido a sistemas adicionales a través de sistemas comprometidos.</p> <p>d) Se han instalado puertas traseras para garantizar accesos futuros a los sistemas comprometidos.</p>
Competencias profesionales	l,k,l,m,n,ñ

### 6.2.8. Unidad didáctica 8: Ingeniería social y phishing

<b>Código:</b>	<b>Rev.:</b>	<b>Fecha Implantación:</b>	<b>Entregar a:</b>	<b>Página 23 de 32</b>
MD850401	4	15/02/2018	Jefa/e depto. → Jefatura estudios	

Núm.	8	Título	Ingeniería social y phishing
Objetivos Didácticos	Determina herramientas de monitorización para detectar vulnerabilidades aplicando técnicas de <i>hacking</i> ético.		
Contenidos Conceptuales	<ul style="list-style-type: none"> <li>– Ingeniería social.</li> <li>– Phishing.</li> <li>– Tipos de ataques de phishing.</li> <li>– Herramientas para la explotación de phishing: gophish</li> </ul>		
Contenidos Procedimentales	<ul style="list-style-type: none"> <li>• Configuración de una campaña usando gophish</li> <li>• Prueba de una campaña usando gophish</li> <li>• Determinar las medidas a adoptar para reducir el riesgo de ataques de phishing en la organización</li> </ul>		
Contenidos Actitudinales	<ul style="list-style-type: none"> <li>• Concienciación sobre la importancia de las técnicas de phishing</li> <li>• Valoración de la importancia de una buena formación para reducir los ataques de phishing</li> </ul>		
Criterios de Evaluación	<ul style="list-style-type: none"> <li>e) Se han identificado las fases de un ataque seguidas por un atacante.</li> <li>f) Se han analizado y definido los tipos vulnerabilidades.</li> <li>g) Se han analizado y definido los tipos de ataque.</li> <li>h) Se han determinado y caracterizado las diferentes vulnerabilidades existentes.</li> <li>i) Se han determinado las herramientas de monitorización disponibles en el mercado adecuadas en función del tipo de organización.</li> </ul>		
Competencias profesionales	l,k,l,m,n,ñ		

### 6.2.9. Unidad didáctica 9: Hacking de servicios Web

Núm.	9	Título	Hacking de servicios Web
------	---	--------	--------------------------

Código:	Rev.:	Fecha Implantación:	Entregar a:	Página 24 de 32
MD850401	4	15/02/2018	Jefa/e depto. → Jefatura estudios	



Objetivos Didácticos	Ataca y defiende en entornos de prueba, aplicaciones <i>web</i> consiguiendo acceso a datos o funcionalidades no autorizadas
Contenidos Conceptuales	<ul style="list-style-type: none"> <li>– Negación de credenciales en aplicaciones <i>web</i>.</li> <li>– Recolección de información.</li> <li>– Automatización de conexiones a servidores <i>web</i> (ejemplo: <i>Selenium</i>).</li> <li>– Análisis de tráfico a través de proxies de intercepción.</li> <li>– Búsqueda de vulnerabilidades habituales en aplicaciones <i>web</i>.</li> <li>– Herramientas para la explotación de vulnerabilidades <i>web</i>.</li> </ul>
Contenidos Procedimentales	<ul style="list-style-type: none"> <li>• Ataques a los servicios web usando XSS</li> <li>• Ataques a los servicios web usando inyección SQL</li> <li>• Ataques a los servicios web usando LFI (Local File Inclusion) y RFI (Remote File Inclusion)</li> </ul>
Contenidos Actitudinales	<ul style="list-style-type: none"> <li>• Concienciación sobre la importancia de las técnicas de explotación de vulnerabilidades web</li> <li>• Valoración de la importancia de una buena configuración del servidor Web para minimizar riesgos</li> <li>• Valoración de la importancia de buenas prácticas en la programación orientada a servicios Web para minimizar riesgos</li> </ul>
Criterios de Evaluación	<p>a) Se han identificado los distintos sistemas de autenticación <i>web</i>, destacando sus debilidades y fortalezas.</p> <p>b) Se ha realizado un inventario de equipos, protocolos, servicios y sistemas operativos que proporcionan el servicio de una aplicación <i>web</i>.</p> <p>c) Se ha analizado el flujo de las interacciones realizadas entre el navegador y la aplicación <i>web</i> durante su uso normal.</p> <p>d) Se han examinado manualmente aplicaciones <i>web</i> en busca de las vulnerabilidades más habituales.</p> <p>e) Se han usado herramientas de búsquedas y explotación de vulnerabilidades <i>web</i>.</p> <p>f) Se ha realizado la búsqueda y explotación de vulnerabilidades <i>web</i> mediante herramientas software.</p>

<b>Código:</b>	<b>Rev.:</b>	<b>Fecha Implantación:</b>	<b>Entregar a:</b>	<b>Página 25 de 32</b>
MD850401	4	15/02/2018	Jefa/e depto. → Jefatura estudios	

Competencias profesionales	l,k,l,m,n,ñ

<b>Código:</b>	<b>Rev.:</b>	<b>Fecha Implantación:</b>	<b>Entregar a:</b>	<b>Página 26 de 32</b>
MD850401	4	15/02/2018	Jefa/e depto. → Jefatura estudios	

## 7. PONDERACIÓN DE RESULTADOS DE APRENDIZAJE

RA1-Determina herramientas de monitorización para detectar vulnerabilidades aplicando técnicas de *hacking* ético.

RA2-Ataca y defiende en entornos de prueba, comunicaciones inalámbricas consiguiendo acceso a redes para demostrar sus vulnerabilidades.

RA3-Ataca y defiende en entornos de prueba, redes y sistemas consiguiendo acceso a información y sistemas de terceros.

RA4-Consolida y utiliza sistemas comprometidos garantizando accesos futuros.

RA5-Ataca y defiende en entornos de prueba, aplicaciones *web* consiguiendo acceso a datos o funcionalidades no autorizadas.

RESULTADO DE APRENDIZAJE	UNIDAD DIDÁCTICA/Ponderación
RA1 (Determina herramientas de monitorización para detectar vulnerabilidades aplicando técnicas de <i>hacking</i> ético)	UD 1 (Introducción al hacking ético) /11,111%  UD 3 (Reconocimiento) /11,111%  UD 4 (Escaneo de red) /11,111%  UD 5 (Análisis de vulnerabilidades) /11,111%
RA2 (Ataca y defiende en entornos de prueba, comunicaciones inalámbricas consiguiendo acceso a redes para demostrar sus vulnerabilidades)	UD 2 (Hacking de redes inalámbricas) /11,111%
RA3 (Ataca y defiende en entornos de prueba, redes y sistemas consiguiendo acceso a información y sistemas de terceros)	UD 6 (Explotación) /11,111%  UD 8 (Ingeniería Social y Phising) /11,111%
RA4 (Consolida y utiliza sistemas comprometidos garantizando accesos futuros)	UD7 (Postexplotación) /11,111%
RA5 (Ataca y defiende en entornos de prueba, aplicaciones <i>web</i> consiguiendo acceso a datos o funcionalidades no autorizadas)	UD 9 (Hacking de Servicios Web) /11,111%

<b>Código:</b>	<b>Rev.:</b>	<b>Fecha Implantación:</b>	<b>Entregar a:</b>	<b>Página 28 de 32</b>
MD850401	4	15/02/2018	Jefa/e depto. → Jefatura estudios	

## 8. MATERIAS TRANSVERSALES

Según los artículos 39 y 40 de la LEA 17/2007 y el artículo 3 del Decreto 436/2008 por el que se establece la ordenación de la Formación Profesional, en todas las enseñanzas han de incorporarse valores transversales y educación en valores. Éstos son un conjunto de saberes basados en actitudes, valores y normas que dan respuesta a algunos problemas sociales existentes en la actualidad. Deben ser tratados en todas las áreas de forma global y programada, aunque también se transmiten a través del currículo oculto que cada docente, equipo o centro transmite con sus opiniones. Por ello se denominan transversales, ya que no surgen como un programa paralelo al desarrollo del currículo sino insertado en la dinámica diaria del proceso de enseñanza – aprendizaje. Son complementarios y deben impregnar la totalidad de actividades. En relación a ellos se plantean los siguientes objetivos de los valores transversales para el módulo:

- Fomentar la tolerancia y el respeto hacia los demás.
- Asignar responsabilidades al alumnado.
- Fomentar el consumo inteligente, especialmente de componentes informáticos.
- Fomentar la responsabilidad ante problemas ambientales, especialmente aquellos relacionados con la informática
- Trabajar en equipo.
- Aprender a ver y escuchar a los demás.
- Conocer y respetar las distintas culturas y etnias
- Favorecer actitudes y hábitos no sexistas.
- Desarrollar hábitos de lectura y escritura.
- Utilizar libros, manuales técnicos y prensa escrita como fuente de información.
- Aplicar las TIC al proceso de enseñanza-aprendizaje.
- Conocer cómo buscar de manera eficiente información en Internet.

Para la consecución de estos objetivos se planteará el desarrollo habitual de las actividades de clase utilizando técnicas que los favorezcan, impregnando el proceso de enseñanza-aprendizaje. Además, hay un conjunto de fechas idóneas para motivar la reflexión sobre dicha temática, tanto mediante actividades diarias como extraordinarias (Día de la Mujer, contra la Violencia de Género, Día de Andalucía, de la Constitución, Día Europeo de la protección de datos, etc.)

Tomando como referencia los incluidos en el Proyecto Educativo del Centro y adaptándolos a estos alumnos y alumnas en concreto, y por su relación con este módulo, se desarrolla de la siguiente manera:

- Educación para la salud:
  - Ergonomía del puesto de trabajo: se harán consideraciones de tipo ergonómico sobre la forma más adecuada de utilizar el ordenador, para disfrutar de una mejor salud postural.
  - Seguridad e higiene en el trabajo
  - Prevención de riesgos laborales.
- Educación para la paz y convivencia:

Código:	Rev.:	Fecha Implantación:	Entregar a:	Página 29 de 32
MD850401	4	15/02/2018	Jefa/e depto. → Jefatura estudios	

- Se harán consideraciones relacionadas con adoptar situaciones de diálogo y consenso frente a situaciones conflictivas en el trabajo en grupo.
- Fomento del diálogo e intercambio razonado de puntos de vista cuando se realicen prácticas en parejas o grupos.
- Importancia del trabajo en equipo para conseguir un objetivo común.
- Respeto del trabajo de todos y su influencia en el funcionamiento de cualquier organización.
- Educación medioambiental: Se harán consideraciones relacionadas con el medioambiente y con acciones que ayuden a preservarlo.
  - Accesibilidad de las personas con discapacidad a las tecnologías de la información
  - Real Decreto Legislativo 1/2013, de 29 de noviembre, por el que se aprueba el Texto Refundido de la Ley General de derechos de las personas con discapacidad y de su inclusión social (BOE nº 289, 3 diciembre 2013)
  - Se considerará el "Diseño para Todos" como criterio general a aplicar en todas las unidades.
- Respeto al material, derecho a la intimidad y a la privacidad. Rechazo a las intrusiones, virus. Cuidado en el uso de los ordenadores y respeto a las normas del aula.
  - LEY ORGÁNICA 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (BOE nº 298, 14 diciembre 1999)
  - REAL DECRETO 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (BOE nº 17, 19 enero 2008)

Código:	Rev.:	Fecha Implantación:	Entregar a:	Página 30 de 32
MD850401	4	15/02/2018	Jefa/e depto. → Jefatura estudios	

## 9. ACTIVIDADES COMPLEMENTARIAS Y EXTRAESCOLARES

Se realizarán las actividades recogidas en la programación de departamento.

Código:	Rev.:	Fecha Implantación:	Entregar a:	Página 31 de 32
MD850401	4	15/02/2018	Jefa/e depto. → Jefatura estudios	

## **10. BIBLIOGRAFÍA, MATERIALES Y RECURSOS**

### **10.1. *Bibliografía de departamento***

### **10.2. *Materiales, recursos y laboratorios***

El material didáctico utilizado consta de:

- Presentaciones teóricas de cada unidad didáctica en moodle proporcionados por el profesor
- Relación de prácticas en moodle proporcionadas por el profesor
- Exámenes de evaluación en moodle o escritos
- Internet como medio frecuente de búsqueda de información
- Cursos de OpenWebinars

<b>Código:</b>	<b>Rev.:</b>	<b>Fecha Implantación:</b>	<b>Entregar a:</b>	<b>Página 32 de 32</b>
MD850401	4	15/02/2018	Jefa/e depto. → Jefatura estudios	