



 GOBIERNO DE ESPAÑA  MINISTERIO DE EDUCACIÓN, CULTURA Y DEPORTE  JUNTA DE ANDALUCÍA CONSEJERÍA DE EDUCACIÓN  FONDO SOCIAL EUROPEO "El FSE invierte en tu futuro"	<b>PLANIFICACIÓN DOCENTE</b>		<b>IES VIRGEN DEL CARMEN</b> Paseo de la Estación nº 44. 23008 Jaén Tel. 953366942 – Fax: 953366944 www.iesvirgendelcarmen.com		 INSTITUTOS DE EDUCACIÓN SECUNDARIA DE CALIDAD DE ANDALUCÍA
	<b>PROGRAMACIÓN</b>				
	<b>MD850202</b>	<b>Rev. 7</b>	<b>06/09/23</b>	<b>Página 1 de 33</b>	

<b>MÓDULO:</b>	<b>HACKING ÉTICO</b>
<b>CURSO:</b>	<b>2024/2025</b>

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

ÍNDICE

1.INTRODUCCIÓN ..... 5

1.1.PRESENTACIÓN DEL MÓDULO PROFESIONAL ..... 5

1.2.MARCO LEGISLATIVO ..... 5

1.3.ENTORNO PROFESIONAL DEL TÍTULO ..... 6

2.CONTEXTO ..... 6

2.1.CONTEXTO SOCIOECONÓMICO..... 7

3.PERFIL PROFESIONAL ..... 7

3.1.COMPETENCIA GENERAL DEL TÍTULO ..... 7

3.2.COMPETENCIAS PROFESIONALES, PERSONALES Y SOCIALES ..... 7

4.OBJETIVOS..... 8

4.1.OBJETIVOS GENERALES DEL CICLO QUE SE TRABAJAN EN EL MÓDULO..... 8

4.2.RESULTADOS DE APRENDIZAJE..... 10

5.CONTENIDOS ..... 11

5.1.TEMPORALIZACIÓN DE CONTENIDOS ..... 11

5.2.SECUENCIACIÓN DE CONTENIDOS ..... 12

5.2.1.Unidad didáctica 1: Introducción al Hacking Ético..... 13

5.2.2.Unidad didáctica 2: Hacking en redes inalámbricas..... 15

5.2.3.Unidad didáctica 3: Reconocimiento..... 17

5.2.4.Unidad didáctica 4: Escaneo de red..... 18

5.2.5.Unidad didáctica 5: Análisis de vulnerabilidades..... 20

5.2.6.Unidad didáctica 6: Explotación de vulnerabilidades..... 21

5.2.7.Unidad didáctica 7: Postexplotación..... 22

5.2.8.Unidad didáctica 8: Ingeniería social y phishing..... 24

5.2.9.Unidad didáctica 9: Hacking de servicios Web..... 25

5.3.ELEMENTOS TRANSVERSALES DEL CURRÍCULO ..... 26

5.3.1.ÁREAS DE INTERÉS EN LA FP ..... 27

Código	Rev .	Fecha Implantación	Entregar a:	Página 2 de 33
MD850202	7	16/09/22	Jefa/e depto. → Jefatura estudios	

5.3.2. EDUCACIÓN EN VALORES.....	27
6. METODOLOGÍA.....	28
6.1. LINEAS DE ACTUACIÓN.....	28
6.2. ACTIVIDADES DE ENSEÑANZA-APRENDIZAJE.....	28
6.3. ESTRATEGIAS DIDÁCTICAS.....	28
6.4. ACTIVIDADES COMPLEMENTARIAS Y EXTRAESCOLARES.....	28
6.5. MATERIALES Y RECURSOS DIDÁCTICOS.....	28
6.6. BIBLIOGRAFÍA.....	29
6.6.1. BIBLIOGRAFÍA DE DEPARTAMENTO.....	29
6.6.2. BIBLIOGRAFÍA DE AULA.....	29
7. EVALUACIÓN.....	29
7.1. ¿QUÉ, CUÁNDO Y CÓMO EVALUAR ?.....	29
7.2. CALIFICACIÓN Y CRITERIOS DE CALIFICACIÓN.....	30
7.2.1. CRITERIOS DE CALIFICACIÓN.....	30
7.3. RECUPERACIÓN Y MEJORA DE CALIFICACIÓN.....	32
Procedimiento para subida de nota.....	32
8. ATENCIÓN A LA DIVERSIDAD.....	33
8.1. Alumnos de admisión tardía.....	33
8.2. Alumnos con necesidades educativas especiales.....	34
8.3. Alumnos con compatibilidad laboral y/o modularidad.....	34
8.4. Alumnado con altas capacidades.....	34

## Índice de tablas

Tabla 1: Temporalización de bloques de contenidos y unidades didácticas.....	11
Tabla 2: Ponderaciones de los RA y unidades didácticas donde se evalúan.....	30

Código	Rev	Fecha Implantación	Entregar a:	Página 3 de 33
MD850202	7	16/09/22	Jefa/e depto. → Jefatura estudios	

## 1. INTRODUCCIÓN

En el contexto del actual sistema educativo (LOMLOE, Ley Orgánica 3/2020, de 29 de diciembre), la programación es la planificación del proceso de enseñanza y el aprendizaje. Es decir, programar es planificar, concretar y secuenciar los distintos elementos curriculares, partiendo de la normativa propuesta por la administración educativa, en el marco de la autonomía pedagógica a través de la herramienta de planificación docente, reguladas por el Decreto 327/2010 (Plan de Centro: Proyecto Educativo, Proyecto de Gestión y ROF).

Una programación minimiza la necesidad de improvisación en el aula y evita el azar a la vez que atiende a las necesidades y características específicas del alumnado.

La eficacia de la programación didáctica como instrumento de planificación de la actividad en el aula dependerá de la adecuación al contexto, la concreción al currículo oficial, el nivel de flexibilidad que presenta y que sea factible, es decir, viable.

La finalidad de esta programación será la consecución de las capacidades propuestas en los objetivos del currículo y la adquisición de las competencias profesionales, personales y sociales. Por lo tanto, esta programación del postgrado **CETIC**, del módulo de **HACKING ÉTICO**, se ha realizado de acuerdo a los objetivos y contenidos de la normativa vigente.

La programación educativa se concreta en tres niveles denominados niveles de concreción curricular que, según la propuesta de César Coll (2012), son los siguientes:

- ! **Currículo:** Es dado por la administración educativa.
- ! **Programación Didáctica:** Se incluye en el Proyecto Educativo y hace referencia a las líneas generales de programación para el curso.
- ! **Programación de aula:** Es la concreción y secuenciación del currículo a nivel de aula, pormenoriza los elementos curriculares y establece los ejercicios, actividades y tareas a desarrollar.

En los distintos niveles de programación se debe tener en cuenta las fuentes epistemológica, sociológica, pedagógica y psicológica.

En esta programación didáctica se desarrollan objetivos, contenidos, competencias profesionales, personales y sociales, metodología, criterios de evaluación y resultados de aprendizaje evaluables, así como la atención a la diversidad y a las necesidades específicas de apoyo educativo.

### 1.1. PRESENTACIÓN DEL MÓDULO PROFESIONAL

Esta programación didáctica estructura la enseñanza correspondiente al módulo de HACKING ÉTICO correspondiente al curso de especialización de CETIC.

Dicho curso de formación profesional tiene una duración de 720 horas.

Este curso de especialización dispone de una organización modular. El módulo de HACKING ÉTICO dispone de una carga lectiva de **120 horas** que se distribuyen a razón de **4 horas semanales**.

### 1.2. MARCO LEGISLATIVO

Código	Rev	Fecha Implantación	Entregar a:	Página 4 de 33
MD850202	7	16/09/22	Jefa/e depto. → Jefatura estudios	

La Constitución Española de 1.978 establece en su artículo 27 el derecho universal a la educación que queda también regulado en la Ley Orgánica del Derecho a la Educación (LODE, 1985). Asimismo, el Estatuto Andalúz del 2007 garantiza a través del artículo 21 que esta educación será permanente y de carácter compensatorio. Sobre estas bases, el Sistema Educativo se ordena a través de la Ley de Educación LOMLOE, Ley Orgánica 3/2020, de 29 de diciembre, que se publicó en el BOE de 30 de diciembre de 2020 y por la que se modifica la Ley Orgánica 2/2006, de 3 de mayo de Educación (LOE), modificada por la Ley Orgánica 8/2013 de Mejora de la Calidad Educativa (LOMCE). En el caso concreto de Andalucía, esta concreción se hace a través de la Ley de Educación de Andalucía (LEA 17/2007).

La Ley Orgánica 3/2022, de 31 de marzo, de ordenación e integración de la Formación Profesional, establece un marco integral para la FP en España. Esta ley deroga la anterior Ley Orgánica 5/2002, de 19 de junio, de las Cualificaciones y de la Formación Profesional, y el Real Decreto 1147/2011, de 29 de julio, que establecía la ordenación general de la FP del sistema educativo. La nueva ley promueve una formación adaptada a las necesidades del mercado laboral y facilita la acreditación de competencias profesionales adquiridas por vías no formales.

Para el desarrollo de esta ley, se ha promulgado el Real Decreto 659/2023, de 18 de julio, por el que se desarrolla la ordenación del Sistema de Formación Profesional. Este real decreto establece la estructura y organización de las ofertas formativas de FP, incluyendo los cursos de especialización.

Este curso de especialización queda regulado a través del Real Decreto 479/2020 de 7 de abril, por el que se establece el Curso de Especialización en Ciberseguridad en Entornos de las Tecnologías de la Información. Posteriormente, el Real Decreto 497/2024, de 21 de mayo, modifica determinados aspectos para adaptarlo al nuevo marco regulatorio.

Entre otras cosas, este primer Real Decreto nos muestra las Unidades de Competencia que se trabajarán en el curso de especialización, de modo que se relacione de forma efectiva con el mundo laboral. Este es uno de los grandes objetivos del nuevo sistema de la Formación Profesional que pretende que la formación se entienda como una actividad que se desarrolla a lo largo de toda la vida y que se adapta a las situaciones concretas del individuo.

Este objetivo se instrumentaliza a través de la Ley Orgánica 3/2022 sobre ordenación e integración de la Formación Profesional, que, basándose en las necesidades del mercado laboral actual, organiza las Cualificaciones Profesionales en Unidades de Competencia necesarias para alcanzarlas. Toda esta información, junto con el contenido de la formación profesional asociada, se estructura en el nuevo Catálogo Nacional de Estándares de Competencias Profesionales, que sigue vigente según el esquema del Catálogo Nacional de Cualificaciones Profesionales establecido por el Real Decreto 1128/2003, hasta que se complete el desarrollo reglamentario. Estas Unidades de Competencia pueden adquirirse en el ámbito laboral, mediante certificados de profesionalidad o a través de cualquiera de los subsistemas de la Formación Profesional: la formación profesional del sistema educativo, donde trabajamos, y la formación profesional para el empleo.

### 1.3. ENTORNO PROFESIONAL DEL TÍTULO

Las ocupaciones y puestos de trabajo más relevantes en los que desarrollarán su actividad profesional los alumnos/as que cursen este ciclo, según lo dispuesto en la normativa que lo regula son las siguientes:

- a) Experto en ciberseguridad.
- b) Auditor de ciberseguridad.
- c) Consultor de ciberseguridad.
- d) Hacker ético.

Código	Rev	Fecha Implantación	Entregar a:	Página 5 de 33
MD850202	7	16/09/22	Jefa/e depto. → Jefatura estudios	

## 2. CONTEXTO

Una de las características de la ley educativa, es que se proporciona autonomía pedagógica a los centros educativos para adaptar la enseñanza de los ciclos formativos a la realidad social y económica del centro donde se impartirán.

Si bien el contexto socioeconómico se trata ampliamente en el Proyecto Educativo, se señala en este apartado el marco socioeconómico, así como el tipo de alumnado al que se dirige esta programación didáctica.

### 2.1. CONTEXTO SOCIOECONÓMICO

El actual modelo curricular, abierto y flexible, posibilita adecuar la programación didáctica a distintos contextos educativos teniendo en cuenta las características del entorno escolar del Centro y de los alumnos y alumnas.

Esta programación se ha elaborado considerando el siguiente contexto educativo: un centro docente donde se imparte el curso de especialización de CETIC, situado en Jaén, una ciudad de aproximadamente 110.000 habitantes. El centro se encuentra en una zona habitada por una población de clase media/alta mayoritariamente.

Al tratarse de un tipo de enseñanza pos-obligatoria, en este centro se encuentran alumnos/as de otras poblaciones próximas de la ciudad, así como de zonas de la periferia de la misma.

La principal actividad económica en la ciudad proviene de los **sectores de servicios y de industria**. El centro educativo se sitúa en el centro de la ciudad. Fruto de la transformación digital en la que estamos inmersos no solo surgen nuevos sectores económicos, sino también nuevas profesiones que van ganando peso en la estructura organizativa de las compañías a medida que las nuevas tecnologías entran en todos sus departamentos. Es por ello que cada día más, las empresas situadas en las proximidades del centro educativo requieren de personal informático cualificado del que se forma en este ciclo.

## 3. PERFIL PROFESIONAL

### 3.1. COMPETENCIA GENERAL DEL TÍTULO

La **competencia general de este título** 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.

### 3.2. COMPETENCIAS PROFESIONALES, PERSONALES Y SOCIALES

Las **competencias profesionales, personales y sociales** describen el conjunto de conocimientos, destrezas y competencias, entendida éstas en términos de autonomía y responsabilidad, que permiten responder a los requerimientos del sector productivo, aumentar la empleabilidad y favorecer la cohesión social.

Las competencias profesionales, personales y sociales del curso de especialización vienen descritas en el currículo que regula título. Son las siguientes:

a) Elaborar e implementar planes de prevención y concienciación en ciberseguridad en la organización, aplicando la normativa vigente.

Código	Rev	Fecha Implantación	Entregar a:	Página 6 de 33
MD850202	7	16/09/22	Jefa/e depto. → Jefatura estudios	

- 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.
- 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.

Concretamente, y tal y como se indica en la Orden que regula el título, de ese total de competencias profesionales, personales y sociales, el módulo que se está programando trabaja las competencias i), k), l), m), n) y ñ) del curso de especialización

#### 4. OBJETIVOS

Los objetivos educativos expresan el nivel de desarrollo que se espera alcance el alumnado como consecuencia de la intervención educativa y se expresan en términos de competencias, es decir, que la meta educativa no debe ser que el alumnado aprenda meros datos, sino que sean capaces de manejarse con ellos. Toda intervención educativa persigue en última instancia el desarrollo integral del individuo, por ello, el objetivo de la educación es el desarrollo de las competencias.

##### 4.1. OBJETIVOS GENERALES DEL CICLO QUE SE TRABAJAN EN EL MÓDULO

Para el curso de especialización de CETIC se han definido una serie de objetivos generales, que se describen a continuación:

Código	Rev	Fecha Implantación	Entregar a:	Página 7 de 33
MD850202	7	16/09/22	Jefa/e depto. → Jefatura estudios	

- 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.

Código	Rev.	Fecha Implantación	Entregar a:	Página 8 de 33
MD850202	7	16/09/22	Jefa/e depto. → Jefatura estudios	



- 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.
- 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.

La formación de nuestro módulo contribuye a alcanzar los objetivos generales de este curso de especialización, tal como se indica en la Orden que regula el título, que se relacionan a continuación: los objetivos generales ñ), q), r), s), t), u) y v)

#### 4.2. RESULTADOS DE APRENDIZAJE

Dentro de la programación, según el grado de concreción, se habla de objetivos a nivel del módulo que se pretenden conseguir durante el transcurso del mismo y los cuales vienen expresados en la correspondiente Orden de 16 de junio de 2011 en términos de **resultados de aprendizaje**, que pasamos a citar:

Código	Rev	Fecha Implantación	Entregar a:	Página 9 de 33
MD850202	7	16/09/22	Jefa/e depto. → Jefatura estudios	

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.

Por otra parte, en cada una de las unidades didácticas en que queda dividida esta programación, se detallarán los objetivos específicos o didácticos de cada una.

## 5. CONTENIDOS

Los objetivos anteriormente planteados serán abordados a través de los contenidos que se describen a continuación. Se toman como fuentes para construir los contenidos: el Real Decreto y la Orden que establece el título de nuestro ciclo y el entorno socioeconómico del centro.

### 5.1. TEMPORALIZACIÓN DE CONTENIDOS

A continuación se esquematizan las unidades didácticas en las que se ha dividido el módulo.

Código	Rev.	Fecha Implantación	Entregar a:	Página 10 de 33
MD850202	7	16/09/22	Jefa/e depto. → Jefatura estudios	

UNIDADES DIDÁCTICAS	HORAS	TRIMESTRE
<b>1. Introducción al Hacking Ético</b>	12	1
<b>2. Hacking en redes inalámbricas</b>	18	1
<b>3. Reconocimiento</b>	10	1
<b>4. Escaneo de red</b>	18	2
<b>5. Análisis de vulnerabilidades</b>	18	2
<b>6. Explotación de vulnerabilidades</b>	16	2
<b>7. Postexplotación</b>	18	3
<b>8. Ingeniería social y phishing</b>	4	3
<b>9. Hacking de servicios Web</b>	6	3

Tabla 1: Temporalización de bloques de contenidos y unidades didácticas

## 5.2. SECUENCIACIÓN DE CONTENIDOS

En este apartado se pasan a esquematizar las unidades didácticas en las que se ha dividido el módulo. Para cada una de ellas se expresan sus contenidos didácticos específicos.

El módulo de HACKING ÉTICO Tiene una carga lectiva de 120 horas que se distribuyen a razón de 4 horas semanales.

Código	Rev	Fecha Implantación	Entregar a:	Página 11 de 33
MD850202	7	16/09/22	Jefa/e depto. → Jefatura estudios	

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.		
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 hacktivismo.</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 hacking 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>
Resultados de aprendizaje	RA1-Determina herramientas de monitorización para detectar vulnerabilidades aplicando técnicas de <i>hacking</i> ético

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

## Unidad didáctica 2: Hacking en redes inalámbricas

Núm.	2	Título	Hacking en redes inalámbricas
Objetivos Didácticos	Ataque y defensa en entorno de pruebas, de las comunicaciones inalámbricas		

Código	Rev	Fecha Implantación	Entregar a:	Página 14 de 33
MD850202	7	16/09/22	Jefa/e depto. → Jefatura estudios	

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

Código	Rev.	Fecha Implantación	Entregar a:	Página 15 de 33
MD850202	7	16/09/22	Jefa/e depto. → Jefatura estudios	

Criterios de 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>
Competencias profesionales	l,k,l,m,n,ñ

### Unidad didáctica 3: Reconocimiento

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	<p>- Fase de reconocimiento (<i>footprinting</i>).</p> <p>- Monitorización de tráfico.</p>		

Código	Rev.	Fecha Implantación	Entregar a:	Página 16 de 33
MD850202	7	16/09/22	Jefa/e depto. → Jefatura estudios	



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

## Unidad didáctica 4: Escaneo de red

Núm.	4	Título	Escaneo de red
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 17 de 33
MD850202	7	16/09/22	Jefa/e depto. → Jefatura estudios	

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

Código	Rev.	Fecha Implantación	Entregar a:	Página 18 de 33
MD850202	7	16/09/22	Jefa/e depto. → Jefatura estudios	

**Unidad didáctica 5: Análisis de vulnerabilidades**

Núm.	5	Título	Análisis de vulnerabilidades
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>	
Resultados de aprendizaje		RA3-Ataca y defiende en entornos de prueba, redes y sistemas consiguiendo acceso a información y sistemas de terceros.	

Código	Rev.	Fecha Implantación	Entregar a:	Página 19 de 33
MD850202	7	16/09/22	Jefa/e depto. → Jefatura estudios	

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

## 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		
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 phishing e ingeniería social</li> </ul>
Resultados de aprendizaje	RA3-Ataca y defiende en entornos de prueba, redes y sistemas consiguiendo acceso a información y sistemas de terceros.
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>
Competencias profesionales	I,k,l,m,n,ñ

## Unidad didáctica 7: Postexplotación

Núm.	7	Título	Postexplotación
Objetivos Didácticos	Consolida y utiliza sistemas comprometidos garantizando accesos futuros		

Código	Rev.	Fecha Implantación	Entregar a:	Página 21 de 33
MD850202	7	16/09/22	Jefa/e depto. → Jefatura estudios	

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 metasploit</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>
Resultados de aprendizaje	RA4-Consolida y utiliza sistemas comprometidos garantizando accesos futuros.

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

## Unidad didáctica 8: Ingeniería social y phishing

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>
Resultados de aprendizaje	RA3-Ataca y defiende en entornos de prueba, redes y sistemas consiguiendo acceso a información y sistemas de terceros.
Criterios de Evaluación	a) Se ha recopilado información sobre la red y sistemas objetivo mediante técnicas pasivas. e) Se han comprometido sistemas remotos explotando sus vulnerabilidades.
Competencias profesionales	l,k,l,m,n,ñ

## Unidad didáctica 9: Hacking de servicios Web

Núm.	9	Título	Hacking de servicios Web
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 interceptación.</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>
Resultados de aprendizaje	RA5-Ataca y defiende en entornos de prueba, aplicaciones web consiguiendo acceso a datos o funcionalidades no autorizadas.
Criterios de Evaluación	<p>a) Se han identificado los distintos sistemas de autenticación web, 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 web.</p> <p>c) Se ha analizado el flujo de las interacciones realizadas entre el navegador y la aplicación web durante su uso normal.</p> <p>d) Se han examinado manualmente aplicaciones web en busca de las vulnerabilidades más habituales.</p> <p>e) Se han usado herramientas de búsquedas y explotación de vulnerabilidades web.</p> <p>f) Se ha realizado la búsqueda y explotación de vulnerabilidades web mediante herramientas software.</p>
Competencias profesionales	l,k,l,m,n,ñ

### 5.3. ELEMENTOS TRANSVERSALES DEL CURRÍCULO

Código	Rev	Fecha Implantación	Entregar a:	Página 25 de 33
MD850202	7	16/09/22	Jefa/e depto. → Jefatura estudios	

### 5.3.1.ÁREAS DE INTERÉS EN LA FP

Asimismo, se debe de prestar atención a las áreas prioritarias o de especial interés, existentes en la Formación Profesional: TIC, idiomas y prevención de riesgos laborales.

### 5.3.2.EDUCACIÓN EN VALORES

El Sistema Educativo incluye en el currículo una serie de saberes actualmente demandados por la sociedad: son los llamados temas transversales.

Se denominan transversales porque 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 del centro.

La LOMLOE y, más concretamente la LEA refuerzan el uso en los currículos de las enseñanzas no universitarias de estos temas transversales.

Las materias transversales que se tratarán son:

- Accesibilidad de las personas con discapacidad a las tecnologías de la información
  - LEY 51/2003, de 2 de diciembre, de igualdad de oportunidades, no discriminación y accesibilidad universal de las personas con discapacidad. (BOE nº 289, 3 diciembre 2003)
  - Se considerará el "Diseño para Todos" como criterio general a aplicar en todas las unidades.
- Educación para la convivencia.
  - 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 para la salud.
  - Seguridad e higiene en el trabajo
  - Prevención de riesgos laborales.
  - Ergonomía del puesto de trabajo.
- 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 26 de 33
MD850202	7	16/09/22	Jefa/e depto. → Jefatura estudios	

## 6. METODOLOGÍA

### 6.1. LINEAS DE ACTUACIÓN

Las líneas de actuación en el proceso de enseñanza-aprendizaje vienen determinadas en la Orden correspondiente por la que se regula el curso de especialización CETIC, versarán sobre:

- Los objetivos y las fases del *hacking* ético.
- Las herramientas de seguridad y *hacking*.
- La administración remota de sistemas.
- El ataque ético a redes de comunicaciones, a sistemas y a las aplicaciones *web*.

### 6.2. ACTIVIDADES DE ENSEÑANZA-APRENDIZAJE

Para las actividades de enseñanza-aprendizaje expresadas en las unidades didácticas (*se ha utilizado la metodología de Tyler y Wheeler, que distingue entre varios tipos de actividades*). En concreto se utilizan los siguientes tipos de actividades:

- Exposición oral de la parte teórica de cada UD.
- Explicación de las prácticas de cada UD.
- Realización de las prácticas de cada UD tutorizadas por el profesor.
- Realización de pruebas de cada UD para comprobar el grado de asimilación de contenidos.

### 6.3. ESTRATEGIAS DIDÁCTICAS

### 6.4. ACTIVIDADES COMPLEMENTARIAS Y EXTRAESCOLARES

Se consideran actividades complementarias las organizadas durante el horario escolar por los Centros, y que tienen un carácter diferenciado de las propiamente lectivas, por el momento, espacio o recursos que utilizan. Estas actividades son fundamentalmente las salidas y celebraciones y se organizarán de forma coordinada con los profesores del equipo docente.

Este curso escolar se han previsto las siguientes actividades:

### 6.5. MATERIALES Y RECURSOS DIDÁCTICOS

Código	Rev	Fecha Implantación	Entregar a:	Página 27 de 33
MD850202	7	16/09/22	Jefa/e depto. → Jefatura estudios	

Todas las sesiones correspondientes a este módulo se desarrollarán en el aula-taller de informática de dotación del ciclo. Además de los recursos tradicionales como la pizarra para explicaciones teóricas, se necesitarán los siguientes recursos tecnológicos en el aula:

- Sistema de proyección o pantalla táctil.
- Ordenadores personales para cada alumno.

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 de cada unidad didáctica en moodle

## 6.6. BIBLIOGRAFÍA

### 6.6.1. BIBLIOGRAFÍA DE DEPARTAMENTO

### 6.6.2. BIBLIOGRAFÍA DE AULA

- Documentos pdf elaborados por el profesor para la parte teórica de cada UD
- Documentos elaborados por el profesor para la realización de las diferentes prácticas

## 7. EVALUACIÓN

La evaluación tendrá en cuenta el progreso del alumno/a respecto a la formación adquirida en los distintos módulos que componen el curso de especialización. La superación del curso de especialización requerirá la evaluación positiva de todos los módulos que lo componen.

La evaluación es **criterial** y **continua**. En primer lugar, es criterial, ya que a través del cumplimiento de los criterios de evaluación, se valida si se alcanzan las metas. En segundo lugar, se dice que es continua porque continuamente se está evaluando y cuando se detecta un problema en clase, se intenta solucionar. Por tanto, permite resolver el problema que tenga un alumno/a en un momento dado. Además, que la evaluación sea continua implica que sea formativa, puesto que permite cambiar aspectos determinados si se detectan fallos en el proceso de enseñanza.

### 7.1. ¿QUÉ, CUÁNDO Y CÓMO EVALUAR ?

- La evaluación inicial:

Código	Rev	Fecha Implantación	Entregar a:	Página 28 de 33
MD850202	7	16/09/22	Jefa/e depto. → Jefatura estudios	

- Se realizará el primer día de clase un cuestionario que pretende recoger el estado inicial de conocimientos previos del alumno.
- Durante las primeras semanas se observarán las aptitudes, actitudes y comportamiento de los alumnos.

-Evaluación final (y trimestral):

En los sucesivos apartados se describe el procedimiento para obtener la nota de evaluación final y trimestral.

## **7.2. CALIFICACIÓN Y CRITERIOS DE CALIFICACIÓN**

Teniendo en cuenta la Orden de 29 de septiembre de 2010, la evaluación final de este módulo profesional el módulo se evaluará por resultados de aprendizaje, complementando con las competencias profesionales, personales y sociales.

### **7.2.1. CRITERIOS DE CALIFICACIÓN**

A continuación, se visualiza una tabla donde se relacionan las ponderaciones estimadas en esta programación didáctica (PD) para cada resultado de aprendizaje (RA) y las unidades didácticas implicadas en cada uno de ellos:

Código	Rev	Fecha Implantación	Entregar a:	Página 29 de 33
MD850202	7	16/09/22	Jefa/e depto. → Jefatura estudios	

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%
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 3 (Reconocimiento) /11,111% UD 4 (Escaneo de red) /11,111% UD 5 (Análisis de vulnerabilidades) /11,111% 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 web consiguiendo acceso a datos o funcionalidades no autorizadas)	UD 9 (Hacking de Servicios Web) /11,111%

Tabla 2: Ponderaciones de los RA y unidades didácticas donde se evalúan

Los Criterios de Evaluación usados en cada unidad didáctica ponderarán por igual.

Teniendo en cuenta las ponderaciones de la tabla anterior, la nota media para la **calificación final del módulo** es la siguiente:

$$\text{Nota final} = (\text{RA1} \cdot 11,111\%) + (\text{RA2} \cdot 11,111\%) + \text{RA3} \cdot 55,555\% + \text{RA4} \cdot 11,111\% + (\text{RA5} \cdot 11,111\%)$$

La nota final del módulo será una media ponderada por RA's teniendo en cuenta los porcentajes de la fórmula anterior aunque puede variar en caso de que se imparta alguna RA menos de las planificadas, en cuyo caso se hará la media ponderada en función de las RA's impartidas en el curso repartiendo la ponderación de la RA no impartida entre las demás y siguiendo la misma proporción que éstas tienen en el módulo.

Código	Rev	Fecha Implantación	Entregar a:	Página 30 de 33
MD850202	7	16/09/22	Jefa/e depto. → Jefatura estudios	

La nota final de la primera evaluación se obtendrá realizando la media ponderada en función de las UD's y RA's impartidas en ese trimestre repartiendo la ponderación de las UD's impartidas al 100% y siguiendo la misma proporción que éstas tienen en el módulo.

La nota final de la segunda evaluación se obtendrá realizando la media ponderada en función de las UD's y RA's impartidas desde el comienzo del curso y repartiendo la ponderación de las UD's impartidas al 100% y siguiendo la misma proporción que éstas tienen en el módulo.

Las notas de los boletines se obtendrán por redondeo al entero más cercano siempre que la nota obtenida con la media ponderada de las RA sea mayor o igual que 5, ya que en caso contrario se considera que el alumno está suspenso.

La nota mínima obtenida en una unidad didáctica que posibilita que se compute la media ponderada del alumno por RA's y UD's es un 4, de forma que si el alumno obtiene menos de un 4 en la nota de una UD deberá recuperar dicha UD con los procedimientos indicados en el apartado de recuperación.

El alumno sólo se considerará aprobado si la nota media ponderada por UD's y RA's es mayor o igual que 5 y no tiene ninguna UD pendiente de recuperación (tanto en la primera evaluación como en la segunda y en la evaluación final)

### 7.3. RECUPERACIÓN Y MEJORA DE CALIFICACIÓN

Para la recuperación en el periodo ordinario, los alumnos podrán realizar las siguientes actividades:

- Repetir los exámenes de las unidades didácticas que cuya nota sea inferior a 4. Sólo se puede recuperar una vez cada examen en el periodo ordinario.
- Repetir las prácticas de la UD que tenga que recuperar.

Se establece un periodo de recuperación que comprende desde finales de mayo a finales de junio. Dicha recuperación consistirá:

- Se realizarán de nuevo algunas de las prácticas propuestas en el módulo.
- Repetir los exámenes de las unidades didácticas que cuya nota sea inferior a 4. Sólo se puede recuperar una vez cada examen en el periodo extraordinario.
- Se impartirán clases teóricas -mas reducidas- debido al acortamiento de tiempo.

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 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.

#### Procedimiento para subida de nota

Código	Rev	Fecha Implantación	Entregar a:	Página 31 de 33
MD850202	7	16/09/22	Jefa/e depto. → Jefatura estudios	

Si los alumnos realizan durante el curso algunos retos propuestos relacionados con el hacking ético, éstos serán tenidos en cuenta para el procedimiento de subida de nota, cuantificándose esta subida a criterio del profesor y en función de la dificultad de los mismos.

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.

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.

## 8. ATENCIÓN A LA DIVERSIDAD

La diversidad está presente en todos los colectivos sociales. El reto de los centros educativos y del profesorado en relación con el alumnado que atienden, es proporcionar el desarrollo de las capacidades en función de sus características diferenciales.

Es una realidad que los alumnos/as del grupo-clase se diferencian en cuanto a sus capacidades, conocimientos previos, motivaciones e intereses. Por ello en el aula, existen alumnos/as que van a presentar distintas necesidades educativas.

La LOMLOE, entiende por alumnado con **necesidades específicas de apoyo educativo (NEAE)** a aquel alumnado, que requiera una atención educativa diferente a la ordinaria, por presentar necesidades educativas especiales, por dificultades específicas de aprendizaje, TDAH, por sus altas capacidades intelectuales, por haberse incorporado tarde al sistema educativo, o por condiciones personales o de historia escolar.

El alumnado con **necesidades educativas especiales**, es aquel alumnado con discapacidad o trastornos graves de conducta.

Los principios de actuación con estos alumnos/as son la no discriminación y la normalización educativa, a fin de lograr la igualdad de oportunidades para todos.

En esta programación se van a adoptar una serie de medidas para atender a los diferentes ritmos de aprendizaje del alumnado y al alumnado con necesidades específicas de apoyo educativo (NEAE).

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 y de retos, los 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.

Código	Rev	Fecha Implantación	Entregar a:	Página 32 de 33
MD850202	7	16/09/22	Jefa/e depto. → Jefatura estudios	



**8.1. 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 se le dará la oportunidad de realizar dichas pruebas siempre y cuando el motivo de la incorporación tardía esté justificado.

**8.2. 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.

**8.3. Alumnos con compatibilidad laboral y/o modularidad**

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

**8.4. Alumnado con altas capacidades**

Para este tipo de alumnado se propondrá la realización de prácticas de ampliación y de retos según se explica en el apartado relativo a la subida de nota.

Código	Rev	Fecha Implantación	Entregar a:	Página 33 de 33
MD850202	7	16/09/22	Jefa/e depto. → Jefatura estudios	