Programación didáctica del módulo: Puesta en Producción Segura

Curso de Especialización Ciberseguridad en Entornos de las Tecnologías de la Información

Curso: 2025/2026

Profesor:

Alexis Manuel Melián Segura

Índice

1. Introducción

La Formación Profesional está orientada tanto al desarrollo y satisfacción personal del alumno como a la obtención de unos conocimientos de tipo técnico y/o humanístico que han de ser preparatorios para el mundo laboral o la Universidad.

La reforma educativa promulgada por la L.O.G.S.E. (Ley Orgánica de Ordenación General del Sistema Educativo) supuso un cambio radical en el sistema educativo existente hasta entonces. La Formación Profesional tradicional pasó a denominarse Ciclos Formativos, quedando estructurada en familias y niveles. Así, los Ciclos Formativos de Grado Medio permiten obtener el título de Técnico, mientras que los Ciclos Formativos de Grado Superior permiten obtener el título de Técnico Superior.

Posteriormente, la L.O.E. (Ley Orgánica de la Educación) estableció una nueva ordenación de los ciclos formativos, estableciendo el nuevo catálogo de la formación profesional, las unidades de competencia y los módulos formativos asociados del Catálogo Modular de Formación Profesional. Este nuevo marco formativo no hace sino acercar la Formación Profesional a las necesidades actuales de la sociedad del conocimiento, donde la movilidad laboral, las nuevas tecnologías, la cohesión e inserción laboral exigen un nuevo planteamiento del mercado laboral. Así pues se pretende proporcionar a las personas la formación requerida por el sistema productivo y de acercar los títulos de formación profesional a la realidad del mercado laboral. Los Ciclos Formativos ofertados por la LOE están separados por familias, siendo una de ellas la Informática.

Con la entrada en vigor de la LOMCE en el curso 2014-2015 la FP Básica vino a sustituir a los PCPI, o Programas de Cualificación Profesional Inicial, desvinculando la Formación Profesional Básica de la obtención del Título de ESO. En este centro se lleva

impartiendo la formación Básica en la rama de "Informática y Comunicaciones" desde el curso 2014-2015. Con la promulgación de la Ley Orgánica 3/2022, de 31 de marzo, de ordenación e integración de la Formación Profesional la formación básica pasa a denominarse Ciclo Formativo de Grado Básico.

De acuerdo a la Ley Orgánica 3/2020, de 29 de diciembre, por la que se modifica la Ley Orgánica 2/2006, de 3 de mayo, de Educación, se establecen las titulaciones de los cursos de especialización, cuyo acceso requiere como mínimo de una titulación de grado superior.

A partir del curso 2024/2025, en Castilla-La Mancha se implantarán, con carácter obligatorio y de forma progresiva, las medidas establecidas en el Real Decreto 659/2023, de 18 de julio, que desarrolla la Ley Orgánica 3/2022, de 31 de marzo, de ordenación e integración de la formación profesional.

En este curso 2025/2026, el Departamento de Informática impartirá los siguientes cursos:

a) Ciclos formativos:

1. **Grado Medio**
   - Sistemas Microinformáticos y Redes (primer y segundo curso en turnos de mañana y vespertino).

2. **Grado Superior**

- Administración de Sistemas Informáticos en Red (primer y segundo curso).
- Desarrollo de Aplicaciones Web (primer y segundo curso en turnos de mañana y vespertino).
- Desarrollo de Aplicaciones Web (primer y segundo curso) en la modalidad Virtual).

3. **Grado Básico**
   - "Informática y Comunicaciones" (Primer y segundo curso)

b) **Cursos de Especialización (en horario vespertino):**

- Ciberseguridad en Entornos de las Tecnologías de la Información.
- Inteligencia Artificial y Big Data.

c) Las siguientes asignaturas en Bachillerato y la ESO

- Digitalización. (4º ESO)
- Desarrollo Digital. (1º Bachillerato)

d) Además, el departamento también será encargado de llevar a cabo las tareas de:

- Responsable de Formación y TIC
- Jefatura de estudios adjunta de FP

- Responsable de aula ATECA
- Responsable de aula APE

Dado el extraordinario auge de la informática, y su gran implantación en la gran mayoría de trabajos actualmente, no es de extrañar que estos ciclos formativos sean considerados por los alumnos como una buena alternativa profesional para su futuro.

Para la inserción de los alumnos en el mundo laboral de modo rápido y eficaz, el alumno debe aprender las técnicas y métodos más adecuados que garanticen la adquisición de los conocimientos y destrezas para desenvolverse en el sector informático.

Esta programación está referida al módulo de "Puesta en Producción Segura" del Curso de Especialización de Ciberseguridad en Entornos de las Tecnologías de la Información en el centro I.E.S. Arcipreste de Hita de Azuqueca de Henares (Guadalajara).

2. Legislación aplicable

La legislación en la que se basa esta programación didáctica es la siguiente:

1. Ley 5/2002, de 19 de junio, donde se establece el sistema integral de la Formación Profesional.
2. Ley Orgánica 2/2006, de 3 de mayo, donde se regula la Formación Profesional en el sistema educativo, organizándola en ciclos formativos de grado medio y grado superior.

3. Real Decreto 1538/2006, de 15 de diciembre, por el que se establece la ordenación general de la Formación Profesional del sistema educativo, incluyendo los aspectos básicos de la evaluación y efectos de los títulos de Formación Profesional.
4. Orden de 29/07/2010, de la Consejería de Educación, Ciencia y Cultura, por la que se regula la evaluación, promoción y acreditación académica del alumnado de formación profesional inicial del sistema educativo de la Comunidad Autónoma de Castilla-La Mancha [2010/14361].
5. Orden de 12 de marzo de 2010, de la Consejería de Educación y Ciencia.
6. Ley 3/2012, de 10 de mayo, de autoridad del profesorado [2012/7512].
7. Ley Orgánica 3/2020, de 29 de diciembre, por la que se modifica la Ley Orgánica 2/2006, de 3 de mayo, de Educación.
8. Orden de 30/07/19, de la Cons. de Educación, Cultura y Deportes, por la que se modifican varias órdenes que regulan la evaluación de alumnado que cursa enseñanzas de FP y otras, para adecuar las fechas de evaluación anuales al calendario de evaluaciones.
9. Ley Orgánica 3/2022, de 31 de marzo, de ordenación e integración de la formación profesional.
10. RD 659/2023, de 18 de julio, por el que se desarrolla la ordenación del Sistema de Formación Profesional.
11. Real Decreto 500/2024, de 21 de mayo, por el que se modifican determinados reales decretos por los que se establecen títulos de Formación Profesional de grado superior y se fijan sus enseñanzas mínimas.
12. 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 y se fijan los aspectos básicos del currículo.

13. Decreto 77/2022, de 12 de julio, por el que se establece el currículo del Curso de Especialización de Formación Profesional en Ciberseguridad en Entornos de las Tecnologías de la Información en la comunidad autónoma de Castilla-La Mancha.
14. Resolución de 11/06/2021, de la Vicecons de Educación, por la que se establece con carácter experimental la distribución horaria de determinados cursos de especialización de Formación Profesional y otros aspectos de organización y desarrollo de los mismos.

3. Ubicación

Tradicionalmente, el alumnado que se matricula es consciente de que las enseñanzas que va a recibir están muy ligadas a un entorno laboral, y que el objetivo principal de los ciclos formativos es formar trabajadores en un campo específico. Al tratarse de enseñanzas dedicadas a la informática, los alumnos tienen claro que el trabajo fundamental se desarrolla con ordenadores, aunque desgraciadamente asocian los contenidos con la ofimática, en lugar de la informática.

El grupo de alumnos es realmente heterogéneo, existiendo una importante presencia de alumnos procedentes de los grados superiores que se imparten en el centro. La mayoría de ellos desconocen realmente el contenido de los módulos (dado su carácter específico). En contraste, existe también un reducido número de alumnos que proceden de entornos profesionales que presentan unos altos conocimientos previos.

En el curso 2020-2021 se impartió por primera vez el curso de especialización correspondiente al título Ciberseguridad en Entornos de las Tecnologías de la

Información. Durante el curso 2021-2022 se implantó el curso de especialización correspondiente al título Inteligencia Artificial y Big Data.

El Departamento de Informática dispone de las siguientes aulas:

a) <u>Aulas para ciclos y cursos de especialización:</u>

a. Formado por 6 aulas situadas en el aulario en las que se imparten los seis cursos de Formación Profesional (dos aulas para el ciclo de SMR, dos para el ciclo de ASIR y dos para el ciclo de DAW) de aproximadamente 50 metros cuadrados cada una de ellas.
b. El tamaño de las aulas no es el adecuado para realizar clases teóricas y prácticas cuando el grupo de alumnos es superior a 26 alumnos.
c. Para el grupo Distancia, no será necesaria la utilización de ningún aula, pero si sería útil que el profesor pudiera tener una sala disponible con conexión a Internet donde pudiera trabajar.
d. Los cursos de especialización se imparten en horario de tarde y ocupan las mismas aulas que los grados superiores.

b) **<u>Aulas APE</u>**

a. La asignatura de Bachillerato y de la ESO se imparte en las aulas APE del centro o en aulas tradicionales con el apoyo de ordenadores portátiles.

b) <u>Aulas para CFG Básico</u>

a. La formación profesional básica se imparte en otras aulas independientes de los Ciclos.
b. El aula de primero está en la planta baja del aulario.

c. El aula de segundo está en el edificio principal del instituto, un aula situada entre las aulas APE y ATECA.

c) <u>Aula ATECA</u>

a. Aula de dotación europea para el desarrollo de proyectos de innovación.

En la mayoría de las aulas debido al gran número de alumnos matriculados en algunos cursos (principalmente en los cursos de primero), las aulas están formadas por hileras de ordenadores para intentar aprovechar el espacio de la forma más óptima posible. Aunque en algunos casos cuando hay pocos alumnos es posible distribuirlas en forma de U para realizar las clases prácticas, permitiendo un control visual rápido de los ordenadores por parte del profesor, y en el centro de la clase disponer de mesas adicionales para realizar las clases teóricas.

Al disponer de horario vespertino, los cursos se imparten en las mismas aulas que los ciclos con turno de mañana, por lo que presentan la misma distribución. Existe un importante número de alumnos que acuden al aula con su propio equipo portátil, se les facilita bajo su responsabilidad una toma de corriente y acceso a la red wifi del aula.

El módulo de Puesta en Producción Segura se caracteriza por tener un enfoque eminentemente práctico, aunque requiere también una sólida base teórica para comprender los fundamentos de la seguridad en entornos de producción. A lo largo del curso, los alumnos trabajan con situaciones reales o simuladas en las que deben aplicar procedimientos seguros para el despliegue de software, la gestión de cambios y la supervisión de servicios en producción.

En general, los estudiantes muestran un alto nivel de interés por esta materia, ya que les permite acercarse al mundo profesional de forma directa, enfrentándose a retos similares a los que encontrarán en su futuro laboral. Aunque puede presentar cierta dificultad técnica (especialmente en lo relativo a la gestión de sistemas, automatización de procesos y buenas prácticas de seguridad), se convierte en una materia especialmente motivadora por su aplicación práctica inmediata.

En cuanto a su relevancia en el mercado laboral, este módulo es de gran importancia, ya que responde a una necesidad creciente de perfiles técnicos capaces de garantizar despliegues seguros, eficientes y controlados en entornos empresariales. Los conocimientos adquiridos permiten desempeñar funciones como técnico de sistemas, administrador de entornos de producción, DevOps o especialista en seguridad informática, entre otros.

La materia también se presta especialmente al trabajo colaborativo, ya que muchas de las tareas que se desarrollan en entornos reales implican la coordinación entre distintos equipos (desarrollo, operaciones, seguridad…). Por ello, se fomenta el trabajo en grupo como metodología habitual, lo que favorece el desarrollo de habilidades transversales como la comunicación, la toma de decisiones conjunta y la resolución de problemas en equipo.

4. Resultados del aprendizaje

Son objetivos comunes los descritos en el Proyecto educativo del centro, en los que respecta a la convivencia, integración, trabajo en equipo y respeto mutuo entre los integrantes de la comunidad docente.

4.1 Objetivos comunes

Los objetivos generales de este curso de especialización son los siguientes:

1. 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.
2. Auditar el cumplimiento del plan de prevención y concienciación de la organización, definiendo las acciones correctoras que puedan derivarse para incluirlas en el plan se securización de la organización.
3. Detectar incidentes de ciberseguridad implantando los controles, las herramientas y los mecanismos necesarios para su monitorización e identificación.
4. Analizar y dar respuesta a incidentes de ciberseguridad, identificando y aplicando las medidas necesarias para su mitigación, eliminación, contención o recuperación.
5. Elaborar análisis de riesgos para identificar activos, amenazas, vulnerabilidades y medidas de seguridad.
6. Diseñar e implantar planes de medidas técnicas de seguridad a partir de los riesgos identificados para garantizar el nivel de seguridad requerido.
7. Configurar sistemas de control de acceso, autenticación de personas y administración de credenciales para preservar la privacidad de los datos.
8. Configurar la seguridad de sistemas informáticos para minimizar las probabilidades de exposición a ataques.
9. Configurar dispositivos de red para cumplir con los requisitos de seguridad.
10. 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.

11. Aplicar estándares de verificación requeridos por las aplicaciones para evitar incidentes de seguridad.
12. Automatizar planes de desplegado de software respetando los requisitos relativos a control de versiones, roles, permisos y otros para conseguir un desplegado seguro.
13. 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.
14. Analizar informes forenses identificando los resultados de la investigación para extraer conclusiones y realizar informes.
15. ñ) Combinar técnicas de hacking ético interno y externo para detectar vulnerabilidades que permitan eliminar y mitigar los riesgos asociados.
16. 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.
17. 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.
18. Desarrollar manuales de información, utilizando herramientas ofimáticas y de diseño asistido por ordenador para elaborar documentación técnica y administrativa.
19. 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.

20. 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.
21. 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.
22. Identificar y proponer las acciones profesionales necesarias para dar respuesta a la accesibilidad universal y al «diseño para todas las personas».
23. 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.

4.2 Objetivos específicos del módulo

De los objetivos comunes del ciclo formativo son aplicables a este módulo los puntos 11), 12), 17), 18), 19), 20), 21) y 22). Por otra parte, los resultados de aprendizaje para este módulo son:

1. Prueba aplicaciones web y aplicaciones para dispositivos móviles analizando la estructura del código y su modelo de ejecución.
2. Determina el nivel de seguridad requerido por aplicaciones identificando los vectores de ataque habituales y sus riesgos asociados.
3. Detecta y corrige vulnerabilidades de aplicaciones web analizando su código fuente y configurando servidores web.
4. Detecta problemas de seguridad en las aplicaciones para dispositivos móviles, monitorizando su ejecución y analizando ficheros y datos.

5. Implanta sistemas seguros de desplegado de software, utilizando herramientas para la automatización de la construcción de sus elementos.

5. Contenidos

5.1 Unidad de Trabajo 1. Prueba de aplicaciones web y para dispositivos móviles

Contenidos	**Objetivos**
1. Fundamentos de la programación. 2. Lenguajes de programación interpretados y compilados. 3. Código fuente y entornos de desarrollo. 4. Ejecución de software. 5. Elementos principales de los programas. 6. Pruebas. Tipos. 7. Seguridad en los lenguajes de programación y sus entornos de ejecución (“sandboxes”).	1. Comparar diferentes lenguajes de programación de acuerdo a sus características principales. 2. Describir los diferentes modelos de ejecución software. 3. Reconocer los elementos básicos del código fuente, dándoles significado. 4. Ejecutar diferentes tipos de prueba de software. 5. Evaluar los lenguajes de programación de acuerdo con la infraestructura de seguridad que proporcionan.
Resultados y Criterios de Evaluación asociados a los Contenidos y Objetivos:	
RA1: Prueba aplicaciones web y aplicaciones para dispositivos móviles analizando la estructura del código y su modelo de ejecución. a) Se han comparado diferentes lenguajes de programación de acuerdo a sus características principales. b) Se han descrito los diferentes modelos de ejecución de software.	

c) Se han reconocido los elementos básicos del código fuente, dándoles significado.

d) Se han ejecutado diferentes tipos de prueba de software.

e) Se han evaluado los lenguajes de programación de acuerdo a la infraestructura de seguridad que proporcionan.

5.2 Unidad de Trabajo 2. Determinación del nivel de seguridad requerido por aplicaciones

Contenidos	**Objetivos**
1. Fuentes abiertas para el desarrollo seguro. 2. Listas de riesgos de seguridad habituales: OWASP Top Ten (web y móvil). 3. Requisitos de verificación necesarios asociados al nivel de seguridad establecido 4. Comprobaciones de seguridad a nivel de aplicación: ASVS (Application Security Verification Standard).	1. Caracterizar los niveles de verificación de seguridad en aplicaciones establecidas por los estándares internacionales (ASVS, “Application Security Verification Standard”). 2. Identificar el nivel de verificación de seguridad requerido por las aplicaciones en función de sus riesgos de acuerdo a estándares reconocidos. 3. Enumerar los requisitos de verificación necesarios asociados al nivel de seguridad establecido. 4. Reconocer los principales riesgos de las aplicaciones desarrolladas, en función de sus características.
Resultados y Criterios de Evaluación asociados a los Contenidos y Objetivos:	
RA2: Determina el nivel de seguridad requerido por aplicaciones identificando los vectores de ataque habituales y sus riesgos asociados.	

a) Se han caracterizado los niveles de verificación de seguridad en aplicaciones establecidos por los estándares internacionales (ASVS, "Application Security Verification Standard").

b) Se ha identificado el nivel de verificación de seguridad requerido por las aplicaciones en función de sus riesgos de acuerdo a estándares reconocidos.

c) Se han enumerado los requisitos de verificación necesarios asociados al nivel de seguridad establecido.

d) Se han reconocido los principales riesgos de las aplicaciones desarrolladas, en función de sus características.

5.3 Unidad de Trabajo 3. Detección y corrección de vulnerabilidades de aplicaciones web

Contenidos	Objetivos
1. Desarrollo seguro de aplicaciones web. 2. Listas públicas de vulnerabilidades de aplicaciones web. OWASP Top Ten. 3. Entrada basada en formularios. Inyección. Validación de la entrada. 4. Estándares de autenticación y autorización. 5. Robo de sesión. 6. Vulnerabilidades web. 7. Almacenamiento seguro de contraseñas.	1. Validar las entradas de los usuarios. 2. Detectar riesgos de inyección tanto en el servidor como en el cliente. 3. Gestionar correctamente la sesión del usuario durante el uso de la aplicación. 4. Hacer uso de roles para el control de acceso. 5. Utilizar algoritmos criptográficos seguros para almacenar las contraseñas de usuario. 6. Configurar servidores web para reducir el riesgo de sufrir ataques conocidos.

8. Contramedidas. HSTS, CSP, CAPTCHAs, entre otros. 9. Seguridad de portales y aplicativos webs. Soluciones WAF (Web Application Firewall).	7. Incorporar medidas para evitar los ataques a contraseñas, envío masivo de mensajes o registros de usuarios a través de programas automáticos (bots).
Resultados y Criterios de Evaluación asociados a los Contenidos y Objetivos:	
RA3: Detecta y corrige vulnerabilidades de aplicaciones web analizando su código fuente y configurando servidores web. a) Se han validado las entradas de los usuarios. b) Se han detectado riesgos de inyección tanto en el servidor como en el cliente. c) Se ha gestionado correctamente la sesión del usuario durante el uso de la aplicación. d) Se ha hecho uso de roles para el control de acceso. e) Se han utilizado algoritmos criptográficos seguros para almacenar las contraseñas de usuario. f) Se han configurado servidores web para reducir el riesgo de sufrir ataques conocidos. g) Se han incorporado medidas para evitar los ataques a contraseñas, envío masivo de mensajes o registros de usuarios a través de programas automáticos (bots).	

5.4 Unidad de Trabajo 4. Detección de problemas de seguridad en aplicaciones para dispositivos móviles

Contenidos	Objetivos
1. Modelos de permisos en plataformas móviles. Llamadas al sistema protegidas.	1. Comparar los diferentes modelos de permisos de las plataformas móviles.

2. Firma y verificación de aplicaciones. 3. Almacenamiento seguro de datos. 4. Validación de compras integradas en la aplicación. 5. Fuga de información en los ejecutables. 6. Soluciones CASB.	2. Describir técnicas de almacenamiento seguro de datos en los dispositivos, para evitar la fuga de información. 3. Implantar un sistema de validación de compras integradas en la aplicación haciendo uso de validación en el servidor. 4. Utilizar herramientas de monitorización de tráfico de red para detectar el uso de protocolos inseguros de comunicación de las aplicaciones móviles. 5. Inspeccionar binarios de aplicaciones móviles para buscar fugas de información sensible.

Resultados y Criterios de Evaluación asociados a los Contenidos y Objetivos:

RA4: Detecta problemas de seguridad en las aplicaciones para dispositivos móviles, monitorizando su ejecución y analizando ficheros y datos.

a) Se han comparado los diferentes modelos de permisos de las plataformas móviles.

b) Se han descrito técnicas de almacenamiento seguro de datos en los dispositivos, para evitar la fuga de información.

c) Se ha implantado un sistema de validación de compras integradas en la aplicación haciendo uso de validación en el servidor.

d) Se han utilizado herramientas de monitorización de tráfico de red para detectar el uso de protocolos inseguros de comunicación de las aplicaciones móviles.

e) Se han inspeccionado binarios de aplicaciones móviles para buscar fugas de información sensible.

5.5 Unidad de Trabajo 5. Implantación de sistemas seguros de desplegado de software

Contenidos	Objetivos
1. Puesta segura en producción. 2. Prácticas unificadas para el desarrollo y operación del software (DevOps). 3. Sistema de control de versiones. 4. Sistemas de automatización de construcción (build). 5. Integración continua y automatización de pruebas. 6. Escalado de servidores. Virtualización. Contenedores. 7. Gestión automatizada de configuraciones de sistemas. 8. Herramientas de simulación de fallos. 9. Orquestación de contenedores.	1. Identificar las características, principios y objetivos de la integración del desarrollo y operación del software. 2. Implantar sistemas de control de versiones, administrando los roles y permisos solicitados. 3. Instalar, configurar y verificar sistemas de integración continua, conectándolos con sistemas de control de versiones. 4. Planificar, implementar y automatizar planes de desplegado de software. 5. Evaluar la capacidad del sistema desplegado para reaccionar de forma automática a fallos. 6. Documentar las tareas realizadas y los procedimientos a seguir para la recuperación ante desastres. 7. Crear bucles de retroalimentación ágiles entre los miembros del equipo.
Resultados y Criterios de Evaluación asociados a los Contenidos y Objetivos:	
RA5: Implanta sistemas seguros de desplegado de software, utilizando herramientas	

para la automatización de la construcción de sus elementos.

a) Se han identificado las características, principios y objetivos de la integración del desarrollo y operación del software.

b) Se han implantado sistemas de control de versiones, administrando los roles y permisos solicitados.

c) Se han instalado, configurado y verificado sistemas de integración continua, conectándolos con sistemas de control de versiones.

d) Se han planificado, implementado y automatizado planes de desplegado de software.

e) Se ha evaluado la capacidad del sistema desplegado para reaccionar de forma automática a fallos.

f) Se han documentado las tareas realizadas y los procedimientos a seguir para la recuperación ante desastres.

g) Se han creado bucles de retroalimentación ágiles entre los miembros del equipo

6. Concordancia de las unidades de trabajo con los resultados del aprendizaje

En el siguiente cuadro resumen, se especifica la concordancia entre los objetivos específicos de este módulo y las unidades de trabajo (la X muestra correspondencia):

Unidad de Trabajo / Resultados del aprendizaje	**RA1**	**RA2**	**RA3**	**RA4**	**RA5**
UT01	x				
UT02		x			
UT03			x		
UT04				x	
UT05					x

7. Temporalización

A continuación, se plantea el calendario de ejecución de las unidades de trabajo ya descritas, la **duración asignada es orientativa** y puede modificarse y adaptarse durante el curso dependiendo del tipo de alumnado, recursos con los que se pueda contar en clase o posibles imprevistos:

Unidad de Trabajo		**Duración prevista**	**Trimestre**
UT01	**Prueba de aplicaciones web y para dispositivos móviles**	26	1
UT02	**Determinación del nivel de seguridad requerido por aplicaciones**	22	1

UT03	**Detección y corrección de vulnerabilidades de aplicaciones web**	26	2
UT04	**Detección de problemas de seguridad en aplicaciones para dispositivos móviles**	26	2, 3
UT05	**Implantación de sistemas seguros de desplegado de software**	20	3
Duración total:		120	

8. Metodología

Los aspectos metodológicos que se pretenden aplicar en este módulo descansan en la idea de que el alumno se considere parte activa de la actividad docente, con esto se pretende involucrarlo en el proceso de asimilación de nuevos conceptos y adquisición de capacidades no como un mero contenedor de éstas sino como un productor directo de estos conocimientos y habilidades en sí mismo.

De igual forma se pretende que el alumno respete al profesor y a sus compañeros, respectando igualmente el material de la clase. Dado el poco material disponible para impartir este módulo, esta última premisa se convierte en vital para poder realizar un aprendizaje correcto de la materia.

Los medios que se implantarán en la medida de lo posible para conseguir estos fines son:

- Estructuración de la clase de la forma más óptima posible para aprovechar el espacio según el número de alumnos en el aula.
- Utilización de la pantalla digital o el proyector para realizar las explicaciones prácticas de software.
- Agrupación de algunas horas de clase en bloques de 2 sesiones lectivas, con el fin de poder planificar teoría y ejercicios prácticos en el mismo día.
- Realización de actividades en grupo que permitan, de una forma próxima y fácil, el aporte de distintos puntos de vista sobre un tema concreto.
- Agrupaciones de alumnos para realizar proyectos o ejercicios conjuntos.
- Planteamiento de actividades creativas donde el alumno pueda aportar su criterio a los temas comentados.
- Por otra parte se plantea la necesidad de motivar e incentivar el interés del alumno por los temas referenciados en clase, esto se concreta en los puntos siguientes:
  - Acercamiento de los temas didácticos al mundo real, aportando publicaciones y documentación de productos lo más conocidos y asequibles posible.
  - Desmitificando la teoría más abstracta y convirtiéndola en cosas tangibles. Es decir, analizando el punto de vista práctico de los conceptos expresados en clase.
  - Planteando ejemplos de aplicación de los trabajos en clase en el mundo laboral real (o lo más cercano posible) de forma que se vaya formando la imagen, en cada alumno, de su perfil profesional.
  - Se utilizará en la medida de lo posible la plataforma Moodle proporcionada por la Junta de comunidades, integrado en Educamos CLM, para proporcionar a los alumnos materiales de consulta, así como ejercicios y tareas.

9. Evaluación

La evaluación será continua, formativa y sumativa, considerándose además de las pruebas objetivas, el trabajo en clase, el progreso, el interés por el módulo, la atención, etc.

9.1 El proceso de evaluación

9.1.1 Evaluación inicial

Al comienzo de cada Unidad de Trabajo se realizará un pequeño debate que permitirá saber cuál es el nivel de conocimientos del alumno sobre cada tema, realizando introducciones sobre aquellos aspectos necesarios para el tema que el alumno no tiene o no ha adquirido completamente, o una pequeña introducción al tema. Se orientará a los alumnos acerca de los contenidos del tema para que los ubiquen dentro de los conocimientos informáticos adquiridos en el curso pasado, o bien en unidades de trabajo anteriores.

En el caso de que Unidades de Trabajo anteriores sirvan como base a una nueva Unidad de Trabajo, los alumnos en esta fase realizarán un repaso de esos conceptos.

9.1.2 Procedimientos para evaluar el proceso de aprendizaje del alumnado

Utilizando la observación y el análisis de los trabajos desarrollados, se utilizarán los siguientes instrumentos de evaluación:

1. El trabajo en equipo

2. La investigación de los contenidos
3. La asistencia regular a clase
4. La puntualidad
5. La correcta utilización del material y equipos
6. Participación en clase
7. Realización y presentación de los trabajos obligatorios solicitados por el profesor.
8. La elaboración de los trabajos optativos
9. Pruebas escritas, con contenidos teóricos y prácticos

Se considera que estos instrumentos de evaluación son adecuados para los criterios de evaluación de este módulo.

9.1.3 Evaluación sumativa

Al final de ciertos bloques de unidades de trabajo, fundamentales para proseguir el desarrollo del módulo, se realizarán pruebas específicas de evaluación escritas llevadas a cabo por el alumno de forma individual. En ciertas unidades de trabajo se realizarán proyectos o ejercicios de síntesis que deberán ser entregados en una fecha límite que serán calificados en ese trimestre.

9.2 Criterios de evaluación

Los criterios de evaluación, agrupados por resultados del aprendizaje, son los siguientes:

1. Prueba aplicaciones web y aplicaciones para dispositivos móviles analizando la estructura del código y su modelo de ejecución.

Criterios de evaluación:

a) Se han comparado diferentes lenguajes de programación de acuerdo a sus características principales.
b) Se han descrito los diferentes modelos de ejecución de software.
c) Se han reconocido los elementos básicos del código fuente, dándoles significado.
d) Se han ejecutado diferentes tipos de prueba de software.
e) Se han evaluado los lenguajes de programación de acuerdo a la infraestructura de seguridad que proporcionan.

2. Determina el nivel de seguridad requerido por aplicaciones identificando los vectores de ataque habituales y sus riesgos asociados.

Criterios de evaluación:

a) Se han caracterizado los niveles de verificación de seguridad en aplicaciones establecidos por los estándares internacionales (ASVS, “Application Security Verification Standard”).
b) Se ha identificado el nivel de verificación de seguridad requerido por las aplicaciones en función de sus riesgos de acuerdo a estándares reconocidos.
c) Se han enumerado los requisitos de verificación necesarios asociados al nivel de seguridad establecido.
d) Se han reconocido los principales riesgos de las aplicaciones desarrolladas, en función de sus características.

3. Detecta y corrige vulnerabilidades de aplicaciones web analizando su código fuente y configurando servidores web.

Criterios de evaluación:

a) Se han validado las entradas de los usuarios.

b) Se han detectado riesgos de inyección tanto en el servidor como en el cliente.
c) Se ha gestionado correctamente la sesión del usuario durante el uso de la aplicación.
d) Se ha hecho uso de roles para el control de acceso.
e) Se han utilizado algoritmos criptográficos seguros para almacenar las contraseñas de usuario.
f) Se han configurado servidores web para reducir el riesgo de sufrir ataques conocidos.
g) Se han incorporado medidas para evitar los ataques a contraseñas, envío masivo de mensajes o registros de usuarios a través de programas automáticos (bots).

4. Detecta problemas de seguridad en las aplicaciones para dispositivos móviles, monitorizando su ejecución y analizando ficheros y datos.

Criterios de evaluación:

a) Se han comparado los diferentes modelos de permisos de las plataformas móviles.
b) Se han descrito técnicas de almacenamiento seguro de datos en los dispositivos, para evitar la fuga de información.
c) Se ha implantado un sistema de validación de compras integradas en la aplicación haciendo uso de validación en el servidor.
d) Se han utilizado herramientas de monitorización de tráfico de red para detectar el uso de protocolos inseguros de comunicación de las aplicaciones móviles.
e) Se han inspeccionado binarios de aplicaciones móviles para buscar fugas de información sensible.

5. Implanta sistemas seguros de desplegado de software, utilizando herramientas para la automatización de la construcción de sus elementos.

Criterios de evaluación:

a) Se han identificado las características, principios y objetivos de la integración del desarrollo y operación del software.
b) Se han implantado sistemas de control de versiones, administrando los roles y permisos solicitados.
c) Se han instalado, configurado y verificado sistemas de integración continua, conectándolos con sistemas de control de versiones.
d) Se han planificado, implementado y automatizado planes de desplegado de software.
e) Se ha evaluado la capacidad del sistema desplegado para reaccionar de forma automática a fallos.
f) Se han documentado las tareas realizadas y los procedimientos a seguir para la recuperación ante desastres.
g) Se han creado bucles de retroalimentación ágiles entre los miembros del equipo.

9.3 Criterios de calificación

Es requisito indispensable para la superación del módulo que el alumno supere cada uno de los resultados de aprendizaje del módulo de acuerdo a los criterios de calificación establecidos.

Una vez superados todos los resultados de aprendizaje, la calificación final del módulo se obtendrá sumando la calificación obtenida en cada uno de los Resultados de Aprendizaje, de acuerdo con los porcentajes de ponderación.

Del resultado se tomará la parte entera, redondeando por exceso la cifra si la parte decimal resultase ser igual o superior a 5.

La calificación final del módulo, por lo tanto, se establecerá según los siguientes puntos:

- El rango de calificación será de 1 a 10 valor entero (Delphos)
- El peso de las calificaciones de los RRAA se realizará mediante una media ponderada. (Véase Tabla siguiente)
- El valor mínimo en los RRAA para considerar que las capacidades profesionales han sido alcanzadas será de 5, para poder realizar la media.

RESULTADOS DE APRENDIZAJE	UNIDAD DE TRABAJO	% ASIGNADO A CADA RA
RA1. Prueba aplicaciones web y aplicaciones para dispositivos móviles analizando la estructura del código y su modelo de ejecución.	UT01	20%
RA2. Determina el nivel de seguridad requerido por aplicaciones identificando los vectores de ataque habituales y sus riesgos asociados.	UT02	20%
RA3. Detecta y corrige vulnerabilidades de aplicaciones web analizando su código fuente y configurando servidores web.	UT03	20%
RA4. Detecta problemas de seguridad en las aplicaciones para dispositivos móviles, monitorizando su ejecución y analizando ficheros y datos.	UT04	20%
RA5. Implanta sistemas seguros de desplegado de software, utilizando herramientas para la automatización de la construcción de sus	UT05	20%

elementos		
	TOTAL	100%

Cada resultado de aprendizaje está dividido en criterios de evaluación que serán evaluados mediante varios instrumentos de evaluación, pudiendo un instrumento de evaluación evaluar diferentes criterios de evaluación.

El rango de calificación de un criterio de evaluación será de 0 a 10 y el valor mínimo para considerar que el criterio de evaluación está logrado será de 5.

Para la evaluación de cada uno de los resultados de aprendizaje se tendrán en cuenta los diferentes criterios de evaluación que tienen asociados, donde cada uno de estos podrá ser evaluado con un instrumento de evaluación, donde el cómputo global asociado a cada resultado de aprendizaje se podría resumir en los siguientes porcentajes asociados a los instrumentos y criterios de evaluación:

- Pruebas de contenido: 40 % de la nota
- Actividades de clase y prácticas: 60 % de la nota

Para superar cada evaluación es necesario:

- Haber obtenido al menos un 4,5 en las pruebas de contenido realizados.
- Haber obtenido al menos un 5 de media en el conjunto de las diferentes actividades de clase y prácticas.
- No haber perdido el derecho a la evaluación continua.

No se considera la evaluación superada si no se cumplen los criterios anteriores.

El alumno deberá superar cada uno de los Resultados de Aprendizaje. La nota final del módulo corresponde a la media ponderada de la nota obtenida en las evaluaciones de cada uno de los resultados de aprendizaje.

Si el alumno no supera uno o varios Resultados de Aprendizaje, la nota final será:

- **Si la media aritmética de las calificaciones obtenidas en los Resultados de Aprendizaje es superior o igual a 5 sobre 10, la calificación final será de 4 sobre 10.**
- **Si la media aritmética de las calificaciones obtenidas en los Resultados de Aprendizaje es inferior a 5 sobre 10 está será la calificación final.**

En el caso de que la calificación obtenida tenga decimales, se realizará el redondeo para la evaluación. Por ejemplo, si el alumno tiene un 5,8 se le redondea al siguiente entero superior, es decir a 6. En cambio, sí tiene un 7,2 se le redondea a un 7. En calificaciones inferiores a 5, se redondea a la baja siempre.

Protocolo de actuación ante plagio en pruebas y proyectos:

Tanto las actividades de clase, como las pruebas prácticas y los proyectos son individuales y deben ser realizados por el alumno con los recursos y tiempo que se dispongan.

En el caso en el que el alumno utilice material que no esté permitido en pruebas prácticas y sea utilizado de manera visible para la realización de la prueba, el alumno será informado de tal evento y la prueba que esté realizando tendrá calificación de 1, independiente de lo que presente el alumno.

Asimismo, si uno o más alumnos son susceptibles de haber incurrido en copia o plagio de una prueba práctica de otro alumno y/o alumnos, el profesor podrá someterlos a una prueba y entrevista específicas después del examen para verificar la propiedad individual de cada una de las pruebas. El contenido de dicha verificación está a disposición del profesor que realizará las preguntas pertinentes. Si dicha entrevista individual o colectiva es satisfactoria, se mantendrá la nota de las pruebas. Por el contrario, las pruebas prácticas y/o proyectos de los alumnos sometidos a dicha verificación tendrán una calificación de 1 en cada una de las pruebas plagiadas.

9.4 Recuperación

El alumno deberá recuperar los Resultados de Aprendizaje no superados en el examen final que se realizará en la primera convocatoria ordinaria. Solo se deberán recuperar únicamente aquellos Resultados de Aprendizaje no superados. En el caso de no recuperar los Resultados de Aprendizaje, entonces la calificación final del módulo no podrá ser superior a 4, considerándose el mismo suspenso.

Se debe tener en cuenta que la evaluación por Resultados de Aprendizaje y Criterios de Evaluación conlleva que las recuperaciones se deben realizar sobre los Resultados de Aprendizaje no logrados.

Para poder realizar este examen es necesario haber presentado todos los trabajos prácticos solicitados por el profesor a lo largo de todo el curso.

En la recuperación la calificación será igual que en primera instancia (0-10).

Acceso a la segunda convocatoria ordinaria

Los alumnos que, después de la primera convocatoria tengan módulos no superados, accederán a la segunda convocatoria de cada curso académico. No obstante, si el alumno no se presenta a la prueba de evaluación preparada por los profesores para la segunda convocatoria, se entenderá que el alumno renuncia a la misma, sin necesidad de haberlo solicitado previamente.

El acceso a la segunda convocatoria ordinaria se realizará independientemente del tipo de matrícula del alumno (ordinaria o modular).

Antes de la realización de la segunda convocatoria ordinaria si el profesor lo considera oportuno se programarán ejercicios de recuperación que se deberán de entregar en la fecha establecida. Dichos ejercicios consistirán en la realización de trabajos, resúmenes y/o ejercicios extra para potenciar los conocimientos del módulo, y su entrega será requisito previo a la realización de la prueba de recuperación.

En el examen de la segunda convocatoria ordinaria, los alumnos deberán examinarse de los resultados de aprendizaje que no se hayan conseguido superar en la primera convocatoria, a través de una prueba única.

9.4.1. Planificación de las actividades de recuperación de los módulos no superados

Dado que se utiliza la plataforma educamosCLM a lo largo del módulo, los alumnos tienen a su disposición el conjunto de ejercicios que les pueden servir de refuerzo para superar el examen de la segunda convocatoria ordinaria.

Se realizarán sesiones de repaso en el centro con el fin de que los alumnos puedan reforzar los contenidos no superados.

Se realizará una prueba final por cada una de las convocatorias ordinarias, esta prueba supondrá el 100% de la calificación, estando está comprendida entre 1-10. El alumno deberá obtener una calificación final igual o superior a 5 sobre 10 para superar el módulo.

9.5 Pérdida de la evaluación continua

En el caso de que un alumno no asista a clase, puede perder el derecho a ser evaluado de forma continua. En concreto aquellos alumnos que tengan un 25% de faltas de asistencia injustificadas POR MÓDULO perderán el derecho a la evaluación continua de ese módulo, por lo que deberán presentarse a una prueba objetiva al finalizar el módulo.

En este módulo, el porcentaje de faltas injustificadas que puede tener un alumno antes de perder el derecho a la evaluación continua es: 30 horas.

La pérdida de la evaluación continua se realiza únicamente para el módulo en el que se hayan detectado las faltas de asistencia injustificadas, y no para todo el ciclo formativo.

La justificación válida para los alumnos se realizará mediante un justificante médico expedido por autoridades médicas o por causas de fuerza mayor que el alumno pueda alegar y sean aceptadas por el profesor.

Adicionalmente, para fomentar el cuidado y corresponsabilidad del material de clase y prepararles para el trabajo en empresa de forma responsable, los alumnos que causen daño intencionado o por negligencia no cuiden el mismo deberán reparar el daño causado al amparo de la Ley de Autoridad del Profesorado. En el caso de que no reparen el daño causado **perderán el derecho a la evaluación continua en todos los módulos en los que estén matriculados**. Los alumnos volverán a ser evaluados de forma continuada cuando reparen el daño causado.

9.5.1 Sistemas e instrumentos de evaluación para los alumnos que han perdido el derecho a la evaluación continua

En el caso de que un alumno pierda el derecho a evaluación continua, deberá presentarse al examen final del curso que se realizará la última semana del curso. En base a ese examen final se calificará el módulo en la primera sesión de evaluación ordinaria. Aun así, el alumno deberá entregar los trabajos prácticos que considere el

profesor PREVIA realización del examen. En el caso de no entregar los trabajos prácticos, el alumno no podrá realizar el examen final.

La calificación final obtenida se calculará según lo descrito en el apartado 9.3 de esta programación didáctica.

9.5.2 Procedimiento de notificación de la pérdida de la evaluación continua

El procedimiento de notificación de la pérdida de la evaluación continua es el siguiente:

1. Una vez el alumno haya perdido el derecho a la evaluación continua, al alcanzar el 25% de las faltas injustificadas, el profesor notificará del hecho al tutor del grupo.
2. El tutor del grupo contactará con el resto de los profesores, por si hubiera algún módulo con alguna circunstancia similar.
3. En el menor tiempo posible se notificará por carta al alumno o a sus tutores legales (en el caso de menores de edad), enviada por el tutor desde la secretaría del centro (con registro de entrada) con el visto bueno de la Dirección del centro. La comunicación se realizará según el modelo establecido en el Anexo I de la orden 29/07/2010 de la Consejería de Educación, Ciencia y Cultura de CLM, por la que se regula la evaluación del alumnado de Formación Profesional.
4. La realización del examen final de curso será posible si el alumno entrega los trabajos prácticos indicados por el profesor.

9.5.3 Casos específicos

Aquellos alumnos que presenten una justificación a las faltas de asistencia (únicamente debida a causas justificadas), **no perderán el derecho a la evaluación continua**, pero deberán igualmente presentarse a los exámenes parciales y entregar los trabajos prácticos. En el caso de que no lo hagan deberán presentarse al examen final de curso.

Independientemente de lo anterior, es responsabilidad del alumno realizar un seguimiento de las explicaciones realizadas en clase, para poder entregar los proyectos y realizar los exámenes con el resto de la clase.

9.6 Autoevaluación del profesorado

La autoevaluación del profesorado está englobada en el Proyecto Educativo del Centro (según su plan de autoevaluación del centro), y se percibe como una forma de mejora y calidad de la enseñanza.

La autoevaluación del profesorado es una práctica constante y continua en el Departamento de Informática, que demuestra a lo largo de cada curso escolar una innovación de metodologías y capacidad de inventiva para poder impartir enseñanzas a pesar de los escasos recursos materiales de los que dispone. Esta autoevaluación del trabajo docente suele ser un proceso interno, de reflexión intrínseca y de necesidad esencial en el trabajo del profesorado. Conviene sin embargo realizar una reflexión escrita de forma periódica, por lo que una vez terminadas las evaluaciones del primer y segundo trimestre, el profesorado realiza una autoevaluación de su trabajo y metodología empleada. En esa autoevaluación se recogerán los siguientes aspectos:

Medidas tomadas durante el trimestre que se deben autoevaluar:

1. Medidas metodológicas (clase magistral, libro de texto, nuevas tecnologías,…)
2. Organizativas del aula
3. Agrupamientos del alumnado
4. Evaluación
5. Actividades de recuperación
6. Acción tutorial
7. Material
8. Problemas encontrados
9. Correcciones
10. Departamentales

Medidas que se deben tomar durante el siguiente trimestre:

1. Medidas metodológicas (clase magistral, libro de texto, nuevas tecnologías,…)
2. Organizativas del aula
3. Agrupamientos del alumnado
4. Evaluación
5. Actividades de recuperación
6. Acción tutorial
7. Material
8. Problemas encontrados
9. Correcciones

Resultados académicos:

1. Porcentaje de alumnos por tramos de calificación.
2. Porcentaje de abandonos o renuncias de convocatorias

3. Número de faltas de asistencia

10. Alumnado con necesidades específicas de apoyo educativo

Se realizarán las adaptaciones necesarias en los medios y procedimientos de evaluación para el alumnado con necesidades específicas de apoyo educativo, con el fin de garantizar su accesibilidad a las pruebas y que sea evaluado con los medios apropiados a sus posibilidades y características.

En todo caso, en el proceso de evaluación se comprobará que el alumnado ha conseguido los resultados de aprendizaje establecidos para cada uno de los módulos que forman parte del ciclo formativo.

En ningún caso se realizarán adaptaciones curriculares significativas.

11. Material didáctico

Los recursos necesarios para impartir este módulo son los siguientes:

- Pizarra
- Retroproyector y pantalla.
- Ordenador con Windows, Microsoft Office, Acrobat Reader, Winrar, Visual Studio Code, Virtual Box, Docker, Git y Herramientas OSINT (Maltego, Shodan, etc.).
- Conexión a Internet
- Teams y portal Educamos
- Impresoras

Cuidado del material

En la situación actual en la que nos encontramos, con unos presupuestos ajustados y un material escaso, se hace IMPRESCINDIBLE en el Departamento de Informática exigir un cuidado del material a los alumnos. Afortunadamente, esta necesidad viene incluso amparada por ley de CLM, por lo que, en el caso de rotura del material por parte de un alumno, se exigirá el cumplimiento de la Ley de Autoridad del Profesorado, donde se especifica, en su Artículo 7:

"*Artículo 7. Responsabilidad y reparación de daños.*

Los alumnos/as o personas con él relacionadas que individual o colectivamente causen, de forma intencionada o por negligencia, daños a las instalaciones, equipamientos informáticos, incluido el software, o cualquier material del centro, así como a los bienes de los miembros de la comunidad educativa, quedarán obligados a reparar el daño causado o hacerse cargo del coste económico de su reparación o restablecimiento, cuando no medie culpa in vigilando de los/as profesores/as. Asimismo, deberán restituir los bienes sustraídos, o reparar económicamente el valor de estos.

2. En todo caso, quienes ejerzan la patria potestad o la tutela de los menores de edad serán responsables civiles en los términos previstos por la legislación vigente."

En el caso de que un alumno cause daño a las instalaciones o material, se amonestará de la acción por escrito informando a Jefatura de Estudios para que tome las medidas disciplinarias oportunas, y gestione la aplicación del artículo mencionado anteriormente.

Como se ha comentado en el apartado 9.6, los alumnos que causarán daño a las instalaciones o material y no reparen el daño causado perderán el derecho a la evaluación continua.

12. Actividades extraescolares

Las actividades extraescolares son muy importantes para la motivación del alumnado, por lo tanto, siempre que sea posible se organizarán salidas que sean provechosas para los alumnos (Como ferias de informática, empresas de informática, etc.). Incluso si es posible se contactará con antiguos alumnos para que den una charla a los alumnos actuales sobre su visión del mundo laboral después de haber obtenido el título.

13. Bibliografía

- “Puesta en producción segura”. Máximo Fernández Riera. Edición Ra-Ma.
- “Puesta en Producción Segura”. María del Carmen Romero Ternero, Pilar Pavón Rosano, Ángel Jesús Varela Vaca, Francisco José de Haro Olmo. Paraninfo.
- Material elaborado por el profesor.