



IES ARCIPRESTE DE HIT. DEPARTAMENTO DE INFORMÁTICA  
Programación didáctica del módulo: Análisis Forense Informático  
Curso de Especialización Ciberseguridad en Entornos de las Tecnologías  
de la Información  
Curso 2025/2026

# **Programación didáctica del módulo: Análisis Forense Informático**

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

**Curso: 2025/2026**

**Profesor:**

**Alexis Manuel Melián Segura**



IES ARCIPRESTE DE HIT A. DEPARTAMENTO DE INFORMÁTICA  
Programación didáctica del módulo: Análisis Forense Informático  
Curso de Especialización Ciberseguridad en Entornos de las Tecnologías  
de la Información  
Curso 2025/2026

|  |    |
|--|----|
| 1. Introducción.....   | 4  |
| 2. Legislación aplicable .....   | 7  |
| 3. Ubicación .....   | 9  |
| 4. Resultados del aprendizaje.....   | 12 |
| 4.1. Objetivos comunes .....   | 12 |
| 4.2. Objetivos específicos del módulo.....   | 15 |
| 5. Contenidos.....   | 16 |
| 5.1. Unidad de Trabajo 1. Metodología de análisis forense.....                               | 16 |
| 5.2. Unidad de Trabajo 2. Aplicación de metodologías de análisis forense.....                | 17 |
| 5.3. Unidad de Trabajo 3. Realización de análisis forenses en dispositivos móviles .         | 18 |
| 5.4. Unidad de Trabajo 4. Realización de análisis forenses en cloud.....                     | 19 |
| 5.5. Unidad de Trabajo 5. Realización de análisis forense en IoT .....                       | 20 |
| 5.6. Unidad de Trabajo 6. Documentación y elaboración de informes de análisis forenses ..... | 22 |
| 6. Concordancia de las unidades de trabajo con los resultados del aprendizaje .....          | 24 |
| 7. Temporalización .....   | 24 |
| 8. Metodología .....   | 25 |
| 9. Evaluación.....   | 27 |
| 9.1. El proceso de evaluación .....  | 27 |
| 9.1.1. Evaluación inicial .....  | 27 |
| 9.1.2 Procedimientos para evaluar el proceso de aprendizaje del alumnado.....                | 28 |
| 9.1.3 Evaluación sumativa .....  | 28 |
| 9.2 Criterios de evaluación .....  | 29 |



|   |    |
|---|----|
| 9.3 Criterios de calificación.....  | 31 |
| 9.4 Recuperación .....  | 35 |
| 9.4.1 Planificación de las actividades de recuperación de los módulos no<br>superados .....                               | 36 |
| 9.5 Pérdida de la evaluación continua .....   | 37 |
| 9.5.1. Sistemas e instrumentos de evaluación para los alumnos que han perdido el<br>derecho a la evaluación continua..... | 38 |
| 9.5.2. Procedimiento de notificación de la pérdida de la evaluación continua .....  | 38 |
| 9.5.3. Casos específicos .....  | 39 |
| 9.6. Autoevaluación del profesorado .....   | 39 |
| 10. Alumnado con necesidades específicas de apoyo educativo.....  | 41 |
| 11. Material didáctico.....   | 41 |
| 12. Actividades extraescolares .....  | 43 |
| 13. Bibliografía.....   | 43 |



## 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



IES ARCIPRESTE DE HITA. DEPARTAMENTO DE INFORMÁTICA  
Programación didáctica del módulo: Análisis Forense Informático  
Curso de Especialización Ciberseguridad en Entornos de las Tecnologías  
de la Información  
Curso 2025/2026

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**



IES ARCIPRESTE DE HIT. DEPARTAMENTO DE INFORMÁTICA  
Programación didáctica del módulo: Análisis Forense Informático  
Curso de Especialización Ciberseguridad en Entornos de las Tecnologías  
de la Información  
Curso 2025/2026

- 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 “Análisis Forense Informático” 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.



IES ARCIPRESTE DE HITA. DEPARTAMENTO DE INFORMÁTICA  
Programación didáctica del módulo: Análisis Forense Informático  
Curso de Especialización Ciberseguridad en Entornos de las Tecnologías  
de la Información  
Curso 2025/2026

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) Aulas para ciclos y cursos de especialización:**

- 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) Aulas APE**

- 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.

**c) Aulas para CFG Básico**

- 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.



**d) Aula ATECA**

- 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.

La materia de Análisis Forense Informático se caracteriza por tener un enfoque teórico-práctico, con un marcado énfasis en la aplicación de herramientas y técnicas para la identificación, recolección, preservación, análisis y presentación de evidencia digital. A lo largo del curso, los estudiantes combinan el estudio de conceptos teóricos (como normativas legales, cadena de custodia, tipos de delitos informáticos y metodologías de investigación) con actividades prácticas orientadas a la simulación de casos reales.



En general, los alumnos muestran un alto grado de interés, ya que es una disciplina que despierta curiosidad por su vínculo con la ciberseguridad, la investigación criminal y el uso de tecnología avanzada. Además, la resolución de casos y la utilización de software especializado genera un entorno de aprendizaje dinámico y participativo.

Respecto a su nivel de dificultad, se considera medio-alto. Si bien no se requieren conocimientos extremadamente avanzados para iniciarse, sí se exige un manejo básico de sistemas operativos, redes y estructuras de archivos, así como habilidades analíticas y una gran atención al detalle.

La materia tiene una alta relevancia en el mercado laboral, dado el creciente número de incidentes relacionados con delitos informáticos. Las habilidades desarrolladas en esta asignatura permiten a los estudiantes desempeñarse en áreas como ciberseguridad, auditoría informática, respuesta a incidentes, consultoría en delitos digitales, o bien colaborar con fuerzas de seguridad y peritos judiciales en procesos legales.

## **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:



IES ARCIPRESTE DE HITA. DEPARTAMENTO DE INFORMÁTICA  
Programación didáctica del módulo: Análisis Forense Informático  
Curso de Especialización Ciberseguridad en Entornos de las Tecnologías  
de la Información  
Curso 2025/2026

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 de 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 despliegado de software respetando los requisitos relativos a control de versiones, roles, permisos y otros para conseguir un despliegado 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. 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 13), 14), 17), 18), 19), 20), 21), y 22). Por otra parte, los resultados de aprendizaje para este módulo son:

1. Aplica metodologías de análisis forense caracterizando las fases de preservación, adquisición, análisis y documentación.
2. Realiza análisis forenses en dispositivos móviles, aplicando metodologías establecidas, actualizadas y reconocidas.
3. Realiza análisis forenses en Cloud, aplicando metodologías establecidas, actualizadas y reconocidas.
4. Realiza análisis forense en dispositivos del IoT, aplicando metodologías establecidas, actualizadas y reconocidas.
5. Documenta análisis forenses elaborando informes que incluyan la normativa aplicable.



## 5. Contenidos

### 5.1. Unidad de Trabajo 1. Metodología de análisis forense

| Contenidos   | Objetivos   |
|--|---|
| <ol style="list-style-type: none"><li>1. Identificación de los dispositivos que se van a analizar.</li><li>2. Recolección de evidencias (trabajar un escenario).</li><li>3. Análisis de la línea de tiempo (timestamp).</li><li>4. Análisis de volatilidad y extracción de información (Volatility).</li><li>5. Análisis de logs, herramientas más usadas.</li></ol>   | <ol style="list-style-type: none"><li>1. Conocer las metodologías de análisis forense caracterizando las fases de preservación, adquisición, análisis y documentación.</li><li>2. Identificar los dispositivos que hay que analizar.</li><li>3. Garantizar la preservación de evidencias.</li><li>4. Asegurar la escena conservando la cadena de custodia.</li><li>5. Documentar todo el proceso realizado de forma metódica y sistemática.</li></ol> |
| <b>Resultados y Criterios de Evaluación asociados a los Contenidos y Objetivos:</b>  |   |
| <p>RA1: Aplica metodologías de análisis forense caracterizando las fases de preservación, adquisición, análisis y documentación.</p> <p>a) Se han identificado los dispositivos a analizar para garantizar la preservación de evidencias.</p> <p>b) Se han utilizado los mecanismos y las herramientas adecuadas para la adquisición y extracción de las evidencias.</p> <p>c) Se ha asegurado la escena y conservado la cadena de custodia.</p> <p>d) Se ha documentado el proceso realizado de manera metódica.</p> <p>e) Se ha considerado la línea temporal de las evidencias.</p> <p>f) Se ha elaborado un informe de conclusiones a nivel técnico y ejecutivo.</p> |   |





g) Se han presentado y expuesto las conclusiones del análisis forense realizado.

## ***5.2. Unidad de Trabajo 2. Aplicación de metodologías de análisis forense***

| <b>Contenidos</b>  | <b>Objetivos</b>  |
|--|---|
| <ol style="list-style-type: none"><li>1. Identificación de los dispositivos que se van a analizar.</li><li>2. Recolección de evidencias (trabajar un escenario).</li><li>3. Análisis de la línea de tiempo (timestamp).</li><li>4. Análisis de volatilidad y extracción de información (Volatility).</li><li>5. Análisis de logs, herramientas más usadas.</li></ol>   | <ol style="list-style-type: none"><li>1. Aplicar metodologías de análisis forense caracterizando las fases de preservación, adquisición, análisis y documentación.</li><li>2. Utilizar mecanismos y herramientas adecuadas para la adquisición y extracción de evidencias.</li><li>3. Analizar los artefactos forenses documentando todo el proceso.</li><li>4. Considerar la línea temporal de evidencias.</li><li>5. Mantener la cadena de custodia sobre las evidencias digitales.</li><li>6. Presentar y exponer los resultados obtenidos en el análisis forense realizado.</li></ol> |
| <b>Resultados y Criterios de Evaluación asociados a los Contenidos y Objetivos:</b>  |   |
| <p>RA1: Aplica metodologías de análisis forense caracterizando las fases de preservación, adquisición, análisis y documentación.</p> <p>a) Se han identificado los dispositivos a analizar para garantizar la preservación de evidencias.</p> <p>b) Se han utilizado los mecanismos y las herramientas adecuadas para la adquisición y extracción de las evidencias.</p> <p>c) Se ha asegurado la escena y conservado la cadena de custodia.</p> <p>d) Se ha documentado el proceso realizado de manera metódica.</p> <p>e) Se ha considerado la línea temporal de las evidencias.</p> |   |



f) Se ha elaborado un informe de conclusiones a nivel técnico y ejecutivo.

g) Se han presentado y expuesto las conclusiones del análisis forense realizado.

### ***5.3. Unidad de Trabajo 3. Realización de análisis forenses en dispositivos móviles***

| <b>Contenidos</b>  | <b>Objetivos</b>  |
|--|---|
| <ol style="list-style-type: none"><li>1. Métodos para la extracción de evidencias.</li><li>2. Herramientas de mercado más comunes.</li></ol> | <ol style="list-style-type: none"><li>1. Realizar análisis forenses en dispositivos móviles aplicando metodologías establecidas, actualizadas y reconocidas.</li><li>2. Desarrollar el proceso de toma de evidencias en un dispositivo móvil.</li><li>3. Extraer, decodificar y analizar las pruebas conservando la cadena de custodia.</li><li>4. Presentar y exponer las conclusiones de análisis forense sobre dispositivos móviles.</li><li>5. Recopilar y aplicar la normativa vigente de ciberseguridad de ámbito nacional e internacional, actualizando los procedimientos establecidos de acuerdo con las leyes y con la jurisprudencia existente sobre la materia.</li></ol> |
| <b>Resultados y Criterios de Evaluación asociados a los Contenidos y Objetivos:</b>  |   |
| RA2: Realiza análisis forenses en dispositivos móviles, aplicando metodologías establecidas, actualizadas y reconocidas.                     |   |
| a) Se ha realizado el proceso de toma de evidencias en un dispositivo móvil.   |   |



b) Se han extraído, decodificado y analizado las pruebas conservando la cadena de custodia.

c) Se han generado informes de datos móviles, cumpliendo con los requisitos de la industria forense de telefonía móvil.

d) Se han presentado y expuesto las conclusiones del análisis forense realizado a quienes proceda.

#### ***5.4. Unidad de Trabajo 4. Realización de análisis forenses en cloud***

##### **Objetivos específicos**

| <b>Contenidos</b>   | <b>Objetivos</b>   |
|---|--|
| <ol style="list-style-type: none"><li>1. Nube privada y nube pública o híbrida</li><li>2. Retos legales, organizativos y técnicos particulares de un análisis en cloud.</li><li>3. Estrategias de análisis forense en cloud.</li><li>4. Realizar las fases relevantes del análisis forense en cloud.</li><li>5. Utilizar herramientas de análisis en cloud (Cellebrite UFED Analyzer, Cloud, Trail, Frost y OWADE).</li></ol> | <ol style="list-style-type: none"><li>1. Realizar análisis forense en la nube (cloud), aplicando metodologías establecidas, actualizadas y reconocidas.</li><li>2. Desarrollar estrategias adecuadas de análisis forense en la nube.</li><li>3. Identificar las causas, el alcance y el impacto causado por un incidente.</li><li>4. Aplicar las fases del análisis forense en la nube.</li><li>5. Conocer las características intrínsecas de la nube.</li><li>6. Respetar los requerimientos legales en vigor: RGPD y directiva NIS.</li><li>7. Presentar y exponer las conclusiones del análisis forense</li></ol> |



|   |            |
|---|------------|
|   | realizado. |
| <b>Resultados y Criterios de Evaluación asociados a los Contenidos y Objetivos:</b>   |            |
| RA3: Realiza análisis forenses en Cloud, aplicando metodologías establecidas, actualizadas y reconocidas.   |            |
| a) Se ha desarrollado una estrategia de análisis forense en Cloud, asegurando la disponibilidad de los recursos y capacidades necesarios una vez ocurrido el incidente.   |            |
| b) Se ha conseguido identificar las causas, el alcance y el impacto real causado por el incidente.  |            |
| c) Se han realizado las fases del análisis forense en Cloud.  |            |
| d) Se han identificado las características intrínsecas de la nube (elasticidad, ubicuidad, abstracción, volatilidad y compartición de recursos).  |            |
| e) Se han cumplido los requerimientos legales en vigor, RGPD (Reglamento general de protección de datos) y directiva NIS (Directiva de la UE sobre seguridad de redes y sistemas de información) o las que eventualmente pudieran sustituirlas. |            |
| f) Se han presentado y expuesto las conclusiones del análisis forense realizado.  |            |

### **5.5. Unidad de Trabajo 5. Realización de análisis forense en IoT**

| <b>Contenidos</b>   | <b>Objetivos</b>   |
|---|--|
| 1. Identificar los dispositivos a analizar.               | 1. Realizar análisis forense en dispositivos IoT, aplicando metodologías establecidas, actualizadas y reconocidas. |
| 2. Adquirir y extraer las evidencias.                     | 2. Identificar los dispositivos y garantizar evidencias.   |
| 3. Analizar las evidencias de manera manual y automática. | 3. Emplear mecanismos y herramientas adecuadas para la adquisición y extracción de                                 |
| 4. Documentar el proceso realizado.                       |  |
| 5. Establecer la línea temporal.                          |  |



IES ARCIPRESTE DE HITA. DEPARTAMENTO DE INFORMÁTICA  
Programación didáctica del módulo: Análisis Forense Informático  
Curso de Especialización Ciberseguridad en Entornos de las Tecnologías  
de la Información  
Curso 2025/2026

|  |   |
|--|---|
| <ol style="list-style-type: none"><li>Mantener la cadena de custodia.</li><li>Elaborar las conclusiones.</li><li>Presentar y exponer las conclusiones.</li></ol>   | <p>evidencias.</p> <ol style="list-style-type: none"><li>Verificar la autenticidad, completitud, fiabilidad y legalidad de las evidencias extraídas.</li><li>Analizar evidencias manualmente y con herramientas específicas.</li><li>Documentar todo el proceso detalladamente y de forma metódica.</li><li>Considerar la línea temporal y garantizar la cadena de custodia.</li><li>Presentar y exponer las conclusiones del análisis forense realizado.</li></ol> |
| <b>Resultados y Criterios de Evaluación asociados a los Contenidos y Objetivos:</b>  |   |
| <p>RA4: Realiza análisis forense en dispositivos del IoT, aplicando metodologías establecidas, actualizadas y reconocidas.</p> <ol style="list-style-type: none"><li>Se han identificado los dispositivos a analizar garantizando la preservación de las evidencias.</li><li>Se han utilizado mecanismos y herramientas adecuadas para la adquisición y extracción de evidencias</li><li>Se ha garantizado la autenticidad, completitud, fiabilidad y legalidad de las evidencias extraídas.</li><li>Se han realizado análisis de evidencias de manera manual y mediante herramientas.</li><li>Se ha documentado el proceso de manera metódica y detallada.</li><li>Se ha considerado la línea temporal de las evidencias.</li></ol> |   |



- g) Se ha mantenido la cadena de custodia
- h) Se ha elaborado un informe de conclusiones a nivel técnico y ejecutivo.
- i) Se han presentado y expuesto las conclusiones del análisis forense realizado.

### ***5.6. Unidad de Trabajo 6. Documentación y elaboración de informes de análisis forenses***

| Contenidos   | Objetivos  |
|--|--|
| 1. Hoja de identificación (título, razón social, nombre y apellidos, firma).   | 1. Documentar análisis forenses elaborando informes que incluyan la normativa aplicable.           |
| 2. Índice de la memoria.   | 2. Registrar todo el proceso de análisis forense de forma metódica y sistemática.                  |
| 3. Objeto (objetivo del informe pericial y su justificación).  | 3. Elaborar un informe de conclusiones a nivel técnico y ejecutivo.                                |
| 4. Alcance (ámbito de aplicación del informe pericial - resumen ejecutivo para una supervisión rápida del contenido y resultados). | 4. Conocer los aspectos legales que hay que considerar al elaborar un dictamen o informe pericial. |
| 5. Antecedentes (aspectos necesarios para la comprensión de las alternativas estudiadas y las conclusiones finales).               | 5. Presentar y exponer las conclusiones del análisis forense realizado.                            |
| 6. Normas y referencias (documentos y normas legales y reglamentos citados en los distintos apartados).                            |  |
| 7. Definiciones y abreviaturas (definiciones, abreviaturas y expresiones técnicas que se han                                       |  |



IES ARCIPRESTE DE HIT. DEPARTAMENTO DE INFORMÁTICA

Programación didáctica del módulo: Análisis Forense Informático

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

Curso 2025/2026

|  |  |
|--|--|
| <p>utilizado a lo largo del informe).</p> <p>8. Requisitos (bases y datos de partida establecidos por el cliente, la legislación, reglamentación y normativa aplicables).</p> <p>9. Análisis de soluciones – resumen de conclusiones del informe pericial (alternativas estudiadas, qué caminos se han seguido para llegar a ellas, ventajas e inconvenientes de cada una y cuál es la solución finalmente elegida y su justificación).</p> <p>10. Anexos</p>  |  |
| <b>Resultados y Criterios de Evaluación asociados a los Contenidos y Objetivos:</b>  |  |
| <p>RA5: Documenta análisis forenses elaborando informes que incluyan la normativa aplicable.</p> <p>a) Se ha definido el objetivo del informe pericial y su justificación.</p> <p>b) Se ha definido el ámbito de aplicación del informe pericial.</p> <p>c) Se han documentado los antecedentes.</p> <p>d) Se han recopilado las normas legales y reglamentos cumplidos en el análisis forense realizado.</p> <p>e) Se han recogido los requisitos establecidos por el cliente.</p> <p>f) Se han incluido las conclusiones y su justificación.</p> |  |



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

En el siguiente cuadro resumen, se especifica la concordancia entre los resultados de aprendizaje 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   |     |
| UT06   |     |     |     |     | 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<br>prevista | Trimestre |
|-------------------|--|----------------------|-----------|
| UT01              | Metodología de análisis forense                              | 18                   | 1         |
| UT02              | Aplicación de metodologías de análisis forense               | 22                   | 1         |
| UT03              | Realización de análisis forense en dispositivos móviles      | 20                   | 2         |
| UT04              | Realización de análisis forense en cloud                     | 20                   | 2         |
| UT05              | Realización de análisis forense en IoT                       | 22                   | 2         |
| UT06              | Documentación y elaboración de informes de análisis forenses | 18                   | 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, respetando 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. Aplica metodologías de análisis forense caracterizando las fases de preservación, adquisición, análisis y documentación.**

Criterios de evaluación:

- a) Se han identificado los dispositivos a analizar para garantizar la preservación de evidencias.
- b) Se han utilizado los mecanismos y las herramientas adecuadas para la adquisición y extracción de las evidencias.
- c) Se ha asegurado la escena y conservado la cadena de custodia.
- d) Se ha documentado el proceso realizado de manera metódica.
- e) Se ha considerado la línea temporal de las evidencias.
- f) Se ha elaborado un informe de conclusiones a nivel técnico y ejecutivo.
- g) Se han presentado y expuesto las conclusiones del análisis forense realizado.

### **2. Realiza análisis forenses en dispositivos móviles, aplicando metodologías establecidas, actualizadas y reconocidas.**

Criterios de evaluación:

- a) Se ha realizado el proceso de toma de evidencias en un dispositivo móvil.
- b) Se han extraído, decodificado y analizado las pruebas conservando la cadena de custodia.
- c) Se han generado informes de datos móviles, cumpliendo con los requisitos de la industria forense de telefonía móvil.
- d) Se han presentado y expuesto las conclusiones del análisis forense realizado a quienes proceda.



**3. Realiza análisis forenses en Cloud, aplicando metodologías establecidas, actualizadas y reconocidas.**

Criterios de evaluación:

- a) Se ha desarrollado una estrategia de análisis forense en Cloud, asegurando la disponibilidad de los recursos y capacidades necesarios una vez ocurrido el incidente.
- b) Se ha conseguido identificar las causas, el alcance y el impacto real causado por el incidente.
- c) Se han realizado las fases del análisis forense en Cloud.
- d) Se han identificado las características intrínsecas de la nube (elasticidad, ubicuidad, abstracción, volatilidad y compartición de recursos).
- e) Se han cumplido los requerimientos legales en vigor, RGPD (Reglamento general de protección de datos) y directiva NIS (Directiva de la UE sobre seguridad de redes y sistemas de información) o las que eventualmente pudieran sustituirlas.
- f) Se han presentado y expuesto las conclusiones del análisis forense realizado.

**4. Realiza análisis forense en dispositivos del IoT, aplicando metodologías establecidas, actualizadas y reconocidas.**

Criterios de evaluación:

- a) Se han identificado los dispositivos a analizar garantizando la preservación de las evidencias.
- b) Se han utilizado mecanismos y herramientas adecuadas para la adquisición y extracción de evidencias
- c) Se ha garantizado la autenticidad, completitud, fiabilidad y legalidad de las evidencias extraídas.



- d) Se han realizado análisis de evidencias de manera manual y mediante herramientas.
- e) Se ha documentado el proceso de manera metódica y detallada.
- f) Se ha considerado la línea temporal de las evidencias.
- g) Se ha mantenido la cadena de custodia.
- h) Se ha elaborado un informe de conclusiones a nivel técnico y ejecutivo.
- i) Se han presentado y expuesto las conclusiones del análisis forense realizado.

**5. Documenta análisis forenses elaborando informes que incluyan la normativa aplicable.**

Criterios de evaluación:

- a) Se ha definido el objetivo del informe pericial y su justificación.
- b) Se ha definido el ámbito de aplicación del informe pericial.
- c) Se han documentado los antecedentes.
- d) Se han recopilado las normas legales y reglamentos cumplidos en el análisis forense realizado.
- e) Se han recogido los requisitos establecidos por el cliente.
- f) Se han incluido las conclusiones y su justificación.

**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.



IES ARCIPRESTE DE HIT. DEPARTAMENTO DE INFORMÁTICA  
Programación didáctica del módulo: Análisis Forense Informático  
Curso de Especialización Ciberseguridad en Entornos de las Tecnologías  
de la Información  
Curso 2025/2026

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.
- 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. Aplica metodologías de análisis forense caracterizando las fases de preservación, adquisición, análisis y documentación. | UT01              | 30%                  |
| RA2. Realiza análisis forenses en dispositivos móviles, aplicando metodologías establecidas, actualizadas y reconocidas.      | UT02              | 17,5%                |
| RA3. Realiza análisis forenses en Cloud, aplicando metodologías establecidas, actualizadas y reconocidas.                     | UT03              | 17,5%                |
| RA4. Realiza análisis forense en dispositivos del IoT, aplicando metodologías establecidas, actualizadas y reconocidas.       | UT04              | 17,5%                |
| RA5. Documenta análisis forenses elaborando informes que incluyan la normativa aplicable.                                     | UT05              | 17,5%                |
|   | 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.**



IES ARCIPRESTE DE HITA. DEPARTAMENTO DE INFORMÁTICA  
Programación didáctica del módulo: Análisis Forense Informático  
Curso de Especialización Ciberseguridad en Entornos de las Tecnologías  
de la Información  
Curso 2025/2026

**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 de suspenso.**

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, si 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 realizará una prueba final por cada una de las convocatorias ordinarias, esta prueba supondrá el 100% de la calificación, estando esta 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 renunciaciones 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.
- Ordenadores con Windows, Microsoft Office, Acrobat Reader, Winrar, Visual Studio Code, Autopsy, Virtual Box, Volatility.
- 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 causaran 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**

- “Análisis Forense Informático”. Francisco José de Haro Olmo, Ángel Jesús Varela Vaca, Pilar Pavón Rosana, María Carmen Romero Ternero. Edición Paraninfo.
- “Análisis Forense Informático”. Mario Guerra Soto. Edición Ra-Ma.
- Material elaborado por el profesor.



IES ARCIPRESTE DE HIT. DEPARTAMENTO DE INFORMÁTICA  
Programación didáctica del módulo: Bastionado de Redes y Sistemas  
Ciclo formativo: Curso de especialización en ciberseguridad  
Curso 2025/2026

# **Programación didáctica del módulo: Bastionado de Redes y Sistemas**

**Ciclo formativo: Curso de  
especialización de formación  
profesional en ciberseguridad en  
entornos de las tecnologías de la  
información**

**Curso: 2025/2026**

**Profesor: Juan José Rubio Atienza**



## Índice

|  |    |
|--|----|
| 1. Introducción.....   | 4  |
| 2. Legislación aplicable .....   | 7  |
| 3. Ubicación .....   | 10 |
| 4. Resultados del aprendizaje.....   | 11 |
| 4.1    Objetivos comunes .....   | 11 |
| 4.2    Objetivos específicos del módulo (Resultados de aprendizaje).....                     | 14 |
| 5. Contenidos.....   | 14 |
| 5.1    UT1: Diseño de planes de securización. ....   | 14 |
| 5.2    UT2: Configuración de sistemas de control de acceso y autenticación de personas. .... | 15 |
| 5.3    UT3: Administración de credenciales de acceso a sistemas informáticos. ....           | 15 |
| 5.4    UT4: Diseño de redes de computadores seguras.....                                     | 15 |
| 5.5    UT5: Configuración de dispositivos y sistemas informáticos. ....                      | 16 |
| 5.6    UT6: Configuración de dispositivos para la instalación de sistemas informáticos.....  | 16 |
| 5.7    UT7: Configuración de los sistemas informáticos: .....                                | 17 |
| 6. Concordancia de las unidades de trabajo con los resultados del aprendizaje .....          | 17 |
| 7. Temporalización .....   | 18 |
| 8. Metodología .....   | 18 |
| 9. Evaluación.....   | 20 |
| 9.1    El proceso de evaluación .....  | 20 |
| 9.1.1    Evaluación inicial .....  | 20 |
| 9.1.2    Procedimientos para evaluar el proceso de aprendizaje del alumnado                  | 21 |



IES ARCIPRESTE DE HIT. DEPARTAMENTO DE INFORMÁTICA  
Programación didáctica del módulo: Bastionado de Redes y Sistemas  
Ciclo formativo: Curso de especialización en ciberseguridad  
Curso 2025/2026

|       |  |    |
|-------|--|----|
| 9.1.3 | Evaluación sumativa .....  | 21 |
| 9.2   | Criterios de evaluación .....  | 22 |
| 9.3   | Criterios de calificación .....  | 24 |
| 9.4   | Recuperación .....   | 25 |
| 9.4.1 | Planificación de las actividades de recuperación de los módulos no superados .....                               | 26 |
| 9.5   | Pérdida de la evaluación continua .....  | 26 |
| 9.5.1 | Sistemas e instrumentos de evaluación para los alumnos que han perdido el derecho a la evaluación continua ..... | 27 |
| 9.5.2 | Procedimiento de notificación de la pérdida de la evaluación continua  | 28 |
| 9.5.3 | Casos específicos .....  | 28 |
| 9.6   | Autoevaluación del profesorado .....   | 29 |
| 10.   | Alumnado con necesidades específicas de apoyo educativo .....  | 30 |
| 11.   | Material didáctico.....  | 31 |
| 12.   | Actividades extraescolares .....   | 32 |
| 13.   | Bibliografía.....  | 32 |



## 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.

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. FP Básica**

- “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

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 “Bastionado de Redes y Sistemas” del ciclo formativo “*Curso de Especialización de formación profesional en 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 405/2023, de 29 de mayo, por el que se actualizan los títulos de la formación profesional del sistema educativo de Técnico Superior en Desarrollo de Aplicaciones Multiplataforma y Técnico Superior en Desarrollo de Aplicaciones Web, de la familia profesional Informática y Comunicaciones, y se fijan sus enseñanzas mínimas.
13. 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.
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.
15. Decreto 81/2024, de 5 de noviembre, por el que se modifican los decretos por los que se establecen los currículos de cursos de especialización de



Formación Profesional de grado medio y superior en la comunidad autónoma de Castilla-La Mancha.

El Departamento de Informática dispone de las siguientes aulas:

**a) Aulas para ciclos y cursos de especialización:**

- 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.

**b) Aulas para FP Básica**

- 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.

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

**c) Aula ATECA**

- 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.

### 3. Ubicación

El Departamento de Informática dispone de las siguientes aulas:

**a) Aulas para ciclos y cursos de especialización:**

- 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 de 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) Aulas APE**

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

**c) Aulas para CF Grado Básico**

- a. La formación básica se imparte en otra aula independiente 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 de APE y ATECA.

**d) Aula ATECA.**

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

## **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 de 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 despliegado de software respetando los requisitos relativos a control de versiones, roles, permisos y otros para conseguir un despliegado 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 (Resultados de aprendizaje)***

RA1. Diseña planes de securización incorporando buenas prácticas para el bastionado de sistemas y redes.

RA2. Configura sistemas de control de acceso y autenticación de personas preservando la confidencialidad y privacidad de los datos.

RA3. Administra credenciales de acceso a sistemas informáticos aplicando los requisitos de funcionamiento y seguridad establecidos.

RA4. Diseña redes de computadores contemplando los requisitos de seguridad.

RA5. Configura dispositivos y sistemas informáticos cumpliendo los requisitos de seguridad.

RA6. Configura dispositivos para la instalación de sistemas informáticos minimizando las probabilidades de exposición a ataques.

RA7. Configura sistemas informáticos minimizando las probabilidades de exposición a ataques.

La formación del módulo contribuye a alcanzar los objetivos generales e), f), g), h), i), j), q), r), s), t), u) y v) y las competencias profesionales, personales y sociales c), d), e), k), l), m), n) y ñ) del curso de especialización.

## **5. Contenidos**

### ***5.1 UT1: Diseño de planes de securización.***

- Análisis de riesgos.



- Principios de la Economía Circular en la Industria 4.0.
- Plan de medidas técnicas de seguridad.
- Políticas de securización más habituales.
- Guías de buenas prácticas para la securización de sistemas y redes.
- Estándares de securización de sistemas y redes.
- Caracterización de procedimientos, instrucciones y recomendaciones.
- Niveles, escalados y protocolos de atención a incidencias.

### ***5.2UT2: Configuración de sistemas de control de acceso y autenticación de personas.***

- Mecanismos de autenticación. Tipos de factores.
- Autenticación basada en distintas técnicas.

### ***5.3UT3: Administración de credenciales de acceso a sistemas informáticos.***

- Gestión de credenciales.
- Infraestructuras de Clave Pública (PKI).
- Acceso por medio de Firma electrónica.
- Gestión de accesos. Sistemas NAC (*Network Access Control*, Sistemas de Gestión de Acceso a la Red).
- Gestión de cuentas privilegiadas.
- Protocolos *RADIUS* y *TACACS*, servicio *KERBEROS*, entre otros.

### ***5.4UT4: Diseño de redes de computadores seguras.***

- Segmentación de redes.
- *Subnetting*.
- Redes virtuales (VLANs).
- Zona desmilitarizada (DMZ).



- Seguridad en redes inalámbricas (WPA2, WPA3, etc.).
- Protocolos de red seguros (IPSec, etc.).

### **5.5UT5: Configuración de dispositivos y sistemas informáticos.**

- Seguridad perimetral. Firewalls de Próxima Generación.
- Seguridad de portales y aplicativos web. Soluciones WAF (*Web Application Firewall*).
- Seguridad del puesto de trabajo y endpoint fijo y móvil. *AntiAPT*, antimalware.
- Seguridad de entornos cloud. Soluciones CASB.
- Seguridad del correo electrónico
- Soluciones DLP (*Data Loss Prevention*)
- Herramientas de almacenamiento de logs.
- Protección ante ataques de denegación de servicio distribuido (DDoS).
- Configuración segura de cortafuegos, enrutadores y proxies.
- Redes privadas virtuales (VPNs), y túneles (protocolo IPSec).
- Monitorización de sistemas y dispositivos.
- Herramientas de monitorización (IDS, IPS).
- SIEMs (Gestores de Eventos e Información de Seguridad).
- Soluciones de Centros de Operación de Red, y Centros de Seguridad de Red: NOCs y SOC.

### **5.6UT6: Configuración de dispositivos para la instalación de sistemas informáticos.**

- Precauciones previas a la instalación de un sistema informático: aislamiento, configuración del control de acceso a la BIOS, bloqueo del orden de arranque de los dispositivos, entre otros.
- Seguridad en el arranque del sistema informático, configuración del arranque seguro.



- Seguridad de los sistemas de ficheros, cifrado, particionado, entre otros.

### **5.7UT7: Configuración de los sistemas informáticos:**

- Reducción del número de servicios, *Telnet*, *RSSH*, *TFTP*, entre otros.
- *Hardening* de procesos (eliminación de información de depuración en caso de errores, aleatorización de la memoria virtual para evitar *exploits*, etc.).
- Eliminación de protocolos de red innecesarios (*ICMP*, entre otros).
- Securización de los sistemas de administración remota.
- Sistemas de prevención y protección frente a virus e intrusiones (antivirus, *HIDS*, etc.).
- Configuración de actualizaciones y parches automáticos.
- Sistemas de copias de seguridad.
- Shadow IT y políticas de seguridad en entornos SaaS.

## **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 | RE. 1 | RE. 2 | RE. 3 | RE. 4 | RE. 5 | RE. 6 | RE. 7 |
|--|-------|-------|-------|-------|-------|-------|-------|
| <b>U.T. 1</b>                                  | X     |       |       |       |       |       |       |
| <b>U.T. 2</b>                                  |       | X     |       |       |       |       |       |



|        |  |  |   |   |   |   |   |
|--------|--|--|---|---|---|---|---|
| U.T. 3 |  |  | X |   |   |   |   |
| U.T. 4 |  |  |   | X |   |   |   |
| U.T. 5 |  |  |   |   | X |   |   |
| U.T. 6 |  |  |   |   |   | X |   |
| U.T. 7 |  |  |   |   |   |   | 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/Tema |     | Duración prevista | Trimestre |
|------------------------|-----|-------------------|-----------|
| 1                      | UT1 | 15                | 1         |
| 2                      | UT2 | 25                | 1         |
| 3                      | UT3 | 30                | 1         |
| 4                      | UT4 | 30                | 2         |
| 5                      | UT5 | 30                | 2         |
| 6                      | UT6 | 30                | 3         |
| 7                      | UT7 | 25                | 3         |
| Duración total:        |     | 185               |           |

## 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, respetando 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. Prácticas
10. Exámenes teórico-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***

- 1) Se han identificado los activos, las amenazas y vulnerabilidades de la organización.
- 2) Se ha evaluado las medidas de seguridad actuales.
- 3) Se ha elaborado un análisis de riesgo de la situación actual en ciberseguridad de la organización
- 4) Se ha priorizado las medidas técnicas de seguridad a implantar en la organización teniendo también en cuenta los principios de la Economía Circular.
- 5) Se ha diseñado y elaborado un plan de medidas técnicas de seguridad a implantar en la organización, apropiadas para garantizar un nivel de seguridad adecuado en función de los riesgos de la organización.
- 6) Se han identificado las mejores prácticas en base a estándares, guías y políticas de securización adecuadas para el bastionado de los sistemas y redes de la organización.
- 7) Se han identificado los tipos de credenciales más utilizados.
- 8) Se han generado y utilizado diferentes certificados digitales como medio de acceso a un servidor remoto.
- 9) Se han identificado los tipos de credenciales más utilizados.
- 10) Se han generado y utilizado diferentes certificados digitales como medio de acceso a un servidor remoto.
- 11) Se ha comprobado la validez y la autenticidad de un certificado digital de un servicio web.
- 12) Se han comparado certificados digitales válidos e inválidos por diferentes motivos.
- 13) Se ha instalado y configurado un servidor seguro para la administración de credenciales (tipo RADIUS - Remote Access Dial In User Service)
- 14) Se ha incrementado el nivel de seguridad de una red local plana segmentándola físicamente y utilizando técnicas y dispositivos de enrutamiento.



- 15) Se ha optimizado una red local plana utilizando técnicas de segmentación lógica (VLANs).
- 16) Se ha adaptado un segmento de una red local ya operativa utilizando técnicas de subnetting para incrementar su segmentación respetando los direccionamientos existentes.
- 17) Se han configurado las medidas de seguridad adecuadas en los dispositivos que dan acceso a una red inalámbrica (routers, puntos de acceso, etc.).
- 18) Se ha establecido un túnel seguro de comunicaciones entre dos sedes geográficamente separadas.
- 19) Se han configurado dispositivos de seguridad perimetral acorde a una serie de requisitos de seguridad.
- 20) Se han detectado errores de configuración de dispositivos de red mediante el análisis de tráfico.
- 21) Se han identificado comportamientos no deseados en una red a través del análisis de los registros (Logs), de un cortafuego.
- 22) Se han implementado contramedidas frente a comportamientos no deseados en una red.
- 23) Se han caracterizado, instalado y configurado diferentes herramientas de monitorización.
- 24) Se ha configurado la BIOS para incrementar la seguridad del dispositivo y su contenido minimizando las probabilidades de exposición a ataques.
- 25) Se ha preparado un sistema informático para su primera instalación teniendo en cuenta las medidas de seguridad necesarias.
- 26) Se ha configurado un sistema informático para que un actor malicioso no pueda alterar la secuencia de arranque con fines de acceso ilegítimo.
- 27) Se ha instalado un sistema informático utilizando sus capacidades de cifrado del sistema de ficheros para evitar la extracción física de datos.



- 28) Se ha particionado el sistema de ficheros del sistema informático para minimizar riesgos de seguridad.
- 29) Se han enumerado y eliminado los programas, servicios y protocolos innecesarios que hayan sido instalados por defecto en el sistema.
- 30) Se han configurado las características propias del sistema informático para imposibilitar el acceso ilegítimo mediante técnicas de explotación de procesos.
- 31) Se ha incrementado la seguridad del sistema de administración remoto SSH y otros.
- 32) Se ha instalado y configurado un Sistema de detección de intrusos en un Host (HIDS) en el sistema informático.
- 33) Se han instalado y configurado sistemas de copias de seguridad.

### ***9.3 Criterios de calificación***

Dado el carácter eminentemente práctico de la Formación Profesional, la calificación del módulo se establecerá a partir de la evaluación continua del trabajo del alumnado y de las pruebas teórico-prácticas realizadas a lo largo del curso.

Para tener derecho a la evaluación continua será necesario contar con una asistencia igual o superior al 75 % de las horas impartidas en el período evaluado.

En cada una de las evaluaciones, la calificación se obtendrá aplicando dos posibles ponderaciones, eligiéndose para cada alumno aquella que resulte más favorable:

- Opción A: 70 % examen (teórico y/o práctico) y 30 % prácticas o actividades de enseñanza-aprendizaje.
- Opción B: 100 % examen (teórico y/o práctico).



El alumnado deberá realizar y entregar todas las prácticas programadas en el plazo establecido. Las prácticas no entregadas o no realizadas tendrán una calificación de 0 en la ponderación correspondiente.

Para considerar superada cada evaluación será necesario cumplir todas las condiciones siguientes:

- Obtener al menos un 4 en el examen teórico-práctico.
- Obtener una calificación final mínima de 5 puntos tras aplicar la ponderación más favorable.

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

La nota final del módulo profesional será la media aritmética de las calificaciones obtenidas en cada evaluación, siempre que todas ellas estén superadas.

En caso de no superar una o varias evaluaciones, la nota final del módulo será de suspenso.

### ***9.4 Recuperación***

El proceso de recuperación tiene como finalidad ofrecer al alumnado distintas oportunidades a lo largo del curso para alcanzar los resultados de aprendizaje no superados.

#### **Recuperaciones trimestrales**

Durante el curso se realizarán tres recuperaciones trimestrales, una al finalizar cada evaluación, con el objetivo de que el alumnado pueda recuperar los temas o resultados de aprendizaje pendientes del trimestre correspondiente.



Estas pruebas se realizarán durante la semana designada como primera convocatoria ordinaria de cada trimestre, una vez completadas las evaluaciones de todos los temas impartidos.

Las calificaciones obtenidas en la primera convocatoria se mantendrán para la segunda convocatoria del trimestre, salvo modificaciones derivadas de incidencias justificadas o mejoras puntuales.

#### **Convocatoria extraordinaria**

Al finalizar el curso, el alumnado que no haya superado el módulo dispondrá de una recuperación final en segunda convocatoria ordinaria (extraordinaria), que se celebrará en junio.

En esta convocatoria se evaluarán exclusivamente los contenidos o resultados de aprendizaje no superados durante el curso.

La no presentación a esta prueba implicará la renuncia a la convocatoria, sin necesidad de comunicación formal.

#### **9.4.1 Planificación de las actividades de recuperación de los módulos no superados**

Dado que se utiliza la plataforma Moodle a lo largo del módulo/asignatura, los alumnos tienen a su disposición el conjunto de ejercicios que les pueden servir de refuerzo para superar el examen de recuperación.

#### ***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



continúa 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: 47

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, en cada una de las evaluaciones su calificación seguirá la siguiente ponderación:

100% la nota del examen (teórico y/o práctico)



### 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 renunciaciones 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.

## 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
- 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 causaran 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**

Todo el material necesario para superar el módulo de Bastionado de Redes y Sistemas será suministrado al alumnado a través de las aulas virtuales.




IES ARCIPRESTE DE HITA. DEPARTAMENTO DE INFORMÁTICA  
Programación didáctica del módulo: Normativa de Ciberseguridad  
Curso de Especialización Ciberseguridad en Entornos de las Tecnologías  
de la Información  
Curso 2025/2026

# **Programación didáctica del módulo: Normativa de Ciberseguridad**

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

**Curso: 2025/2026**

**Profesor:  
Raquel Crespo Fuente**

|  |   |
|--|---|
|  | <p>IES ARCIPRESTE DE HITA. DEPARTAMENTO DE INFORMÁTICA</p> <p>Programación didáctica del módulo: Normativa de Ciberseguridad</p> <p>Curso de Especialización Ciberseguridad en Entornos de las Tecnologías de la Información</p> <p>Curso 2025/2026</p> |
|--|---|

|  |                                      |
|--|--------------------------------------|
| 1. Introducción.....   | 4                                    |
| 2. Legislación aplicable .....   | 7                                    |
| 3. Ubicación .....   | 9                                    |
| 4. Resultados del aprendizaje.....   | 12                                   |
| 4.1. Objetivos comunes .....   | 12                                   |
| 4.2. Objetivos específicos del módulo.....   | 15                                   |
| 5. Contenidos.....   | 16                                   |
| 5.1. Unidad de Trabajo 1. Metodología de análisis forense.....                               | 16                                   |
| 5.2. Unidad de Trabajo 2. Aplicación de metodologías de análisis forense.....                | 16                                   |
| 5.3. Unidad de Trabajo 3. Realización de análisis forenses en dispositivos móviles .         | 16                                   |
| 5.4. Unidad de Trabajo 4. Realización de análisis forenses en cloud.....                     | 16                                   |
| 5.5. Unidad de Trabajo 5. Realización de análisis forense en IoT                             | <b>¡Error! Marcador no definido.</b> |
| 5.6. Unidad de Trabajo 6. Documentación y elaboración de informes de análisis forenses ..... | <b>¡Error! Marcador no definido.</b> |
| 6. Concordancia de las unidades de trabajo con los resultados del aprendizaje .....          | 17                                   |
| 7. Temporalización .....   | 18                                   |
| 8. Metodología .....   | 19                                   |
| 9. Evaluación.....   | 20                                   |
| 9.1. El proceso de evaluación .....  | 20                                   |
| 9.1.1. Evaluación inicial .....  | 20                                   |
| 9.1.2 Procedimientos para evaluar el proceso de aprendizaje del alumnado.....                | 21                                   |
| 9.1.3 Evaluación sumativa .....  | 22                                   |



|   |    |
|---|----|
| 9.2 Criterios de evaluación .....   | 22 |
| 9.3 Criterios de calificación.....  | 25 |
| 9.4 Recuperación .....  | 28 |
| 9.4.1 Planificación de las actividades de recuperación de los módulos no superados<br>.....                               | 29 |
| 9.5 Pérdida de la evaluación continua .....   | 30 |
| 9.5.1. Sistemas e instrumentos de evaluación para los alumnos que han perdido el<br>derecho a la evaluación continua..... | 31 |
| 9.5.2. Procedimiento de notificación de la pérdida de la evaluación continua .....  | 31 |
| 9.5.3. Casos específicos .....  | 32 |
| 9.6. Autoevaluación del profesorado .....   | 32 |
| 10. Alumnado con necesidades específicas de apoyo educativo.....  | 34 |
| 11. Material didáctico.....   | 34 |
| 12. Actividades extraescolares .....  | 36 |
| 13. Bibliografía.....   | 36 |



## 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



IES ARCIPRESTE DE HITA. DEPARTAMENTO DE INFORMÁTICA  
Programación didáctica del módulo: Normativa de Ciberseguridad  
Curso de Especialización Ciberseguridad en Entornos de las Tecnologías  
de la Información  
Curso 2025/2026

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**





IES ARCIPRESTE DE HITA. DEPARTAMENTO DE INFORMÁTICA  
Programación didáctica del módulo: Normativa de Ciberseguridad  
Curso de Especialización Ciberseguridad en Entornos de las Tecnologías  
de la Información  
Curso 2025/2026

- 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

|  |   |
|--|---|
|  | <p>IES ARCIPRESTE DE HITA. DEPARTAMENTO DE INFORMÁTICA</p> <p>Programación didáctica del módulo: Normativa de Ciberseguridad</p> <p>Curso de Especialización Ciberseguridad en Entornos de las Tecnologías de la Información</p> <p>Curso 2025/2026</p> |
|--|---|

- 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 “Normativa de Ciberseguridad” 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:

|  |   |
|--|---|
|  | <p>IES ARCIPRESTE DE HITA. DEPARTAMENTO DE INFORMÁTICA</p> <p>Programación didáctica del módulo: Normativa de Ciberseguridad</p> <p>Curso de Especialización Ciberseguridad en Entornos de las Tecnologías de la Información</p> <p>Curso 2025/2026</p> |
|--|---|

**a) Aulas para ciclos y cursos de especialización:**

- 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) Aulas APE**

- 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.

**c) Aulas para CFG Básico**

- 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.

**d) Aula ATECA**

|  |  |
|--|--|
|  | <p>IES ARCIPRESTE DE HIT. DEPARTAMENTO DE INFORMÁTICA</p> <p>Programación didáctica del módulo: Normativa de Ciberseguridad</p> <p>Curso de Especialización Ciberseguridad en Entornos de las Tecnologías de la Información</p> <p>Curso 2025/2026</p> |
|--|--|


- 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.

La materia de Análisis Forense Informático se caracteriza por tener un enfoque teórico-práctico, con un marcado énfasis en la aplicación de herramientas y técnicas para la identificación, recolección, preservación, análisis y presentación de evidencia digital. A lo largo del curso, los estudiantes combinan el estudio de conceptos teóricos (como normativas legales, cadena de custodia, tipos de delitos informáticos y metodologías de investigación) con actividades prácticas orientadas a la simulación de casos reales.

En general, los alumnos muestran un alto grado de interés, ya que es una disciplina que despierta curiosidad por su vínculo con la ciberseguridad, la investigación

|  |   |
|--|---|
|  | <p>IES ARCIPRESTE DE HITA. DEPARTAMENTO DE INFORMÁTICA</p> <p>Programación didáctica del módulo: Normativa de Ciberseguridad</p> <p>Curso de Especialización Ciberseguridad en Entornos de las Tecnologías de la Información</p> <p>Curso 2025/2026</p> |
|--|---|

criminal y el uso de tecnología avanzada. Además, la resolución de casos y la utilización de software especializado genera un entorno de aprendizaje dinámico y participativo.

Respecto a su nivel de dificultad, se considera medio-alto. Si bien no se requieren conocimientos extremadamente avanzados para iniciarse, sí se exige un manejo básico de sistemas operativos, redes y estructuras de archivos, así como habilidades analíticas y una gran atención al detalle.

La materia tiene una alta relevancia en el mercado laboral, dado el creciente número de incidentes relacionados con delitos informáticos. Las habilidades desarrolladas en esta asignatura permiten a los estudiantes desempeñarse en áreas como ciberseguridad, auditoría informática, respuesta a incidentes, consultoría en delitos digitales, o bien colaborar con fuerzas de seguridad y peritos judiciales en procesos legales.

## 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 de 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 despliegado de software respetando los requisitos relativos a control de versiones, roles, permisos y otros para conseguir un despliegado 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. 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**

Como objetivos específicos para este módulo descritos en el DECRETO 77/2022 como resultados de aprendizaje:

1. Identifica los puntos principales de aplicación para asegurar el cumplimiento normativo reconociendo funciones y responsabilidades.
2. Diseña sistemas de cumplimiento normativo seleccionando la legislación y jurisprudencia de aplicación.
3. Relaciona la normativa relevante para el cumplimiento de la responsabilidad penal de las organizaciones y personas jurídicas con los procedimientos establecidos, recopilando y aplicando las normas vigentes.
4. Aplica la legislación nacional de protección de datos de carácter personal, relacionando los procedimientos establecidos con las leyes vigentes y con la jurisprudencia existente sobre la materia.
5. Recopila y aplica la normativa vigente de ciberseguridad de ámbito nacional e internacional, actualizando los procedimientos establecidos de acuerdo con las leyes y con la jurisprudencia existente sobre la materia.



## **5. Contenidos**

### ***5.1. Unidad de Trabajo 1. Cumplimiento normativo, funciones y responsabilidades***

- Introducción al cumplimiento normativo (Compliance: objetivo, definición y conceptos principales).
- Principios del buen gobierno y ética empresarial.
- Compliance Officer: funciones y responsabilidades.
- Relaciones con terceras partes dentro del Compliance.

### ***5.2. Unidad de Trabajo 2. Diseño de sistemas de cumplimiento normativo***


- Sistemas de Gestión de Compliance.
- Entorno regulatorio de aplicación.
- Análisis y gestión de riesgos, mapas de riesgos.
- Documentación del sistema de cumplimiento normativo diseñado.

### ***5.3. Unidad de Trabajo 3. Responsabilidad penal***

- Riesgos penales que afectan a la organización.
- Sistemas de gestión de Compliance penal.
- Sistemas de gestión anticorrupción.

### ***5.4. Unidad de Trabajo 4. Protección de datos***

- Principios de protección de datos.
- Novedades del RGPD de la Unión Europea.

|  |   |
|--|---|
|  | <p>IES ARCIPRESTE DE HITA. DEPARTAMENTO DE INFORMÁTICA</p> <p>Programación didáctica del módulo: Normativa de Ciberseguridad</p> <p>Curso de Especialización Ciberseguridad en Entornos de las Tecnologías de la Información</p> <p>Curso 2025/2026</p> |
|--|---|

- Privacidad por Diseño y por Defecto.
- Análisis de Impacto en Privacidad (PIA), y medidas de seguridad.
- Delegado de Protección de Datos (DPO).

### ***5.5. Unidad de Trabajo 5. Normativa vigente de ciberseguridad***

- Normas nacionales e internacionales.
- Sistema de Gestión de Seguridad de la Información (estándares internacionales) (ISO 27.001).
- Acceso electrónico de los ciudadanos a los Servicios Públicos
- Esquema Nacional de Seguridad (ENS).
  - Planes de Continuidad de Negocio (estándares internacionales) (ISO 22.301).
  - Directiva NIS.
  - Legislación sobre la protección de infraestructuras críticas.
  - Ley PIC (Protección de infraestructuras críticas).

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

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



| U.T / R.A. | 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              | <b>Cumplimiento normativo, funciones y responsabilidades.</b> | 11                | 1         |
| UT02              | <b>Diseño de sistemas de cumplimiento normativo.</b>          | 11                | 1         |
| UT03              | <b>Responsabilidad penal</b>                                  | 11                | 2         |
| UT04              | <b>Protección de datos</b>                                    | 11                | 2         |
| UT05              | <b>Normativa vigente de seguridad.</b>                        | 11                | 3         |
| Duración total:   |   | 55                |           |




## 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, respetando 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.

|  |   |
|--|---|
|  | <p>IES ARCIPRESTE DE HITA. DEPARTAMENTO DE INFORMÁTICA</p> <p>Programación didáctica del módulo: Normativa de Ciberseguridad</p> <p>Curso de Especialización Ciberseguridad en Entornos de las Tecnologías de la Información</p> <p>Curso 2025/2026</p> |
|--|---|

- 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,

|  |   |
|--|---|
|  | <p>IES ARCIPRESTE DE HITA. DEPARTAMENTO DE INFORMÁTICA</p> <p>Programación didáctica del módulo: Normativa de Ciberseguridad</p> <p>Curso de Especialización Ciberseguridad en Entornos de las Tecnologías de la Información</p> <p>Curso 2025/2026</p> |
|--|---|

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.



|  |   |
|--|---|
|  | <p>IES ARCIPRESTE DE HITA. DEPARTAMENTO DE INFORMÁTICA</p> <p>Programación didáctica del módulo: Normativa de Ciberseguridad</p> <p>Curso de Especialización Ciberseguridad en Entornos de las Tecnologías de la Información</p> <p>Curso 2025/2026</p> |
|--|---|

### **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. Identifica los puntos principales de aplicación para asegurar el cumplimiento normativo reconociendo funciones y responsabilidades.**

Criterios de evaluación:

- a) Se han identificado las bases del cumplimiento normativo a tener en cuenta en las organizaciones.
- b) Se han descrito y aplicado los principios de un buen gobierno y su relación con la ética profesional.
- c) Se han definido las políticas y procedimientos, así como la estructura organizativa que establezca la cultura del cumplimiento normativo dentro de las organizaciones.
- d) Se han descrito las funciones o competencias del responsable del cumplimiento normativo dentro de las organizaciones.
- e) Se han establecido las relaciones con terceros para un correcto cumplimiento normativo.

### **2. Diseña sistemas de cumplimiento normativo seleccionando la legislación y jurisprudencia de aplicación.**

|  |   |
|--|---|
|  | <p>IES ARCIPRESTE DE HITA. DEPARTAMENTO DE INFORMÁTICA</p> <p>Programación didáctica del módulo: Normativa de Ciberseguridad</p> <p>Curso de Especialización Ciberseguridad en Entornos de las Tecnologías de la Información</p> <p>Curso 2025/2026</p> |
|--|---|

Criterios de evaluación:

- a) Se han recogido las principales normativas que afectan a los diferentes tipos de organizaciones.
- b) Se han establecido las recomendaciones válidas para diferentes tipos de organizaciones de acuerdo con la normativa vigente (ISO 19.600 entre otras).
- c) Se han realizado análisis y evaluaciones de los riesgos de diferentes tipos de organizaciones de acuerdo con la normativa vigente (ISO 31.000 entre otras).
- d) Se ha documentado el sistema de cumplimiento normativo diseñado.

**3. Relaciona la normativa relevante para el cumplimiento de la responsabilidad penal de las organizaciones y personas jurídicas con los procedimientos establecidos, recopilando y aplicando las normas vigentes.**


Criterios de evaluación:

- a) Se han identificado los riesgos penales aplicables a diferentes organizaciones.
- b) Se han implantado las medidas necesarias para eliminar o minimizar los riesgos identificados.
- c) Se ha establecido un sistema de gestión de cumplimiento normativo penal de acuerdo con la legislación y normativa vigente (Código Penal y UNE 19.601, entre otros).
- d) Se han determinado los principios básicos dentro de las organizaciones para combatir el soborno y promover una cultura empresarial ética de acuerdo con la legislación y normativa vigente (ISO 37.001 entre otros).

**4. Aplica la legislación nacional de protección de datos de carácter personal, relacionando los procedimientos establecidos con las leyes vigentes y con la jurisprudencia existente sobre la materia.**

Criterios de evaluación:

- a) Se han reconocido las fuentes del derecho de acuerdo con el ordenamiento jurídico en materia

|  |   |
|--|---|
|  | <p>IES ARCIPRESTE DE HITA. DEPARTAMENTO DE INFORMÁTICA</p> <p>Programación didáctica del módulo: Normativa de Ciberseguridad</p> <p>Curso de Especialización Ciberseguridad en Entornos de las Tecnologías de la Información</p> <p>Curso 2025/2026</p> |
|--|---|


de protección de datos de carácter personal.

- b) Se han aplicado los principios relacionados con la protección de datos de carácter personal tanto a nivel nacional como internacional.
- c) Se han establecido los requisitos necesarios para afrontar la privacidad desde las bases del diseño.
- d) Se han configurado las herramientas corporativas contemplando el cumplimiento normativo por defecto.
- e) Se ha realizado un análisis de riesgos para el tratamiento de los derechos a la protección de datos.
- f) Se han implantado las medidas necesarias para eliminar o minimizar los riesgos identificados en la protección de datos.
- g) Se han descrito las funciones o competencias del delegado de protección de datos dentro de las organizaciones.

**5. Recopila y aplica la normativa vigente de ciberseguridad de ámbito nacional e internacional, actualizando los procedimientos establecidos de acuerdo con las leyes y con la jurisprudencia existente sobre la materia.**

Criterios de evaluación:

- a) Se ha establecido el plan de revisiones de la normativa, jurisprudencia, notificaciones, etc. jurídicas que puedan afectar a la organización.
- b) Se ha detectado nueva normativa consultando las bases de datos jurídicas siguiendo el plan de revisiones establecido.
- c) Se ha analizado la nueva normativa para determinar si aplica a la actividad de la organización.
- d) Se ha incluido en el plan de revisiones las modificaciones necesarias, sobre la nueva normativa aplicable a la organización, para un correcto cumplimiento normativo.

|  |  |
|--|--|
|  | <p>IES ARCIPRESTE DE HIT. DEPARTAMENTO DE INFORMÁTICA</p> <p>Programación didáctica del módulo: Normativa de Ciberseguridad</p> <p>Curso de Especialización Ciberseguridad en Entornos de las Tecnologías de la Información</p> <p>Curso 2025/2026</p> |
|--|--|

e) Se han determinado e implementado los controles necesarios para garantizar el correcto cumplimiento normativo de las nuevas normativas. incluidas en el plan de revisiones.

### 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 con 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.
- 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. Identifica los puntos principales de aplicación para asegurar el cumplimiento | UT01              | 20%                  |

|  |  |
|--|--|
|  | <p align="center"> <b>IES ARCIPRESTE DE HITA. DEPARTAMENTO DE INFORMÁTICA</b><br/> <b>Programación didáctica del módulo: Normativa de Ciberseguridad</b><br/> <b>Curso de Especialización Ciberseguridad en Entornos de las Tecnologías</b><br/> <b>de la Información</b><br/> <b>Curso 2025/2026</b> </p> |
|--|--|


|  |              |             |
|--|--------------|-------------|
| <b>normativo reconociendo funciones y responsabilidades.</b>   |              |             |
| <b>RA2. Diseña sistemas de cumplimiento normativo seleccionando la legislación y jurisprudencia de aplicación.</b>   | UT02         | 20%         |
| <b>RA3. Relaciona la normativa relevante para el cumplimiento de la responsabilidad penal de las organizaciones y personas jurídicas con los procedimientos establecidos, recopilando y aplicando las normas vigentes.</b>         | UT03         | 20%         |
| <b>RA4. Aplica la legislación nacional de protección de datos de carácter personal, relacionando los procedimientos establecidos con las leyes vigentes y con la jurisprudencia existente sobre la materia.</b>                    | UT04         | 20%         |
| <b>RA5. Recopila y aplica la normativa vigente de ciberseguridad de ámbito nacional e internacional, actualizando los procedimientos establecidos de acuerdo con las leyes y con la jurisprudencia existente sobre la materia.</b> | UT05         | 20%         |
|  | <b>TOTAL</b> | <b>100%</b> |

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

El rango de calificación de un CE será de 0 a 10.

Para realizar la evaluación de los resultados de aprendizaje mencionados en la tabla anterior, se disponen de una serie de instrumentos de evaluación para evaluar cada criterio asociado a los resultados de aprendizaje. Así se utilizarán habitualmente prácticas y pruebas escritas o exámenes.

Durante el desarrollo de la unidad de trabajo correspondiente se le indicará al alumno los criterios de evaluación asociados a esa unidad de trabajo. Además, se

|  |   |
|--|---|
|  | <p>IES ARCIPRESTE DE HITA. DEPARTAMENTO DE INFORMÁTICA</p> <p>Programación didáctica del módulo: Normativa de Ciberseguridad</p> <p>Curso de Especialización Ciberseguridad en Entornos de las Tecnologías de la Información</p> <p>Curso 2025/2026</p> |
|--|---|

indicará el instrumento o instrumentos (examen o practica) que se va a emplear para evaluar dichos criterios de evaluación.

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

Para realizar la calificación del alumno, se tendrá en cuenta el peso de cada resultado de aprendizaje mostrado anteriormente, realizando una media ponderada en base al peso de cada resultado de aprendizaje.

**Importante:**


Para aprobar la evaluación ordinaria hay que obtener una calificación numérica de 5 o superior en cada resultado de aprendizaje.

**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

|  |   |
|--|---|
|  | <p>IES ARCIPRESTE DE HITA. DEPARTAMENTO DE INFORMÁTICA</p> <p>Programación didáctica del módulo: Normativa de Ciberseguridad</p> <p>Curso de Especialización Ciberseguridad en Entornos de las Tecnologías de la Información</p> <p>Curso 2025/2026</p> |
|--|---|

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

|  |   |
|--|---|
|  | <p>IES ARCIPRESTE DE HITA. DEPARTAMENTO DE INFORMÁTICA</p> <p>Programación didáctica del módulo: Normativa de Ciberseguridad</p> <p>Curso de Especialización Ciberseguridad en Entornos de las Tecnologías de la Información</p> <p>Curso 2025/2026</p> |
|--|---|

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 realizará una prueba final por cada una de las convocatorias ordinarias, esta prueba supondrá el 100% de la calificación, estando esta comprendida entre 1-10. El



|  |   |
|--|---|
|  | <p>IES ARCIPRESTE DE HITA. DEPARTAMENTO DE INFORMÁTICA</p> <p>Programación didáctica del módulo: Normativa de Ciberseguridad</p> <p>Curso de Especialización Ciberseguridad en Entornos de las Tecnologías de la Información</p> <p>Curso 2025/2026</p> |
|--|---|

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: 14 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**

|  |   |
|--|---|
|  | <p>IES ARCIPRESTE DE HITA. DEPARTAMENTO DE INFORMÁTICA</p> <p>Programación didáctica del módulo: Normativa de Ciberseguridad</p> <p>Curso de Especialización Ciberseguridad en Entornos de las Tecnologías de la Información</p> <p>Curso 2025/2026</p> |
|--|---|

**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 renunciaciones 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.
- Ordenadores con Windows, Microsoft Office, Acrobat Reader, Winrar.
- 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 causaran daño a las instalaciones o material y no reparen el daño causado perderán el derecho a la evaluación continua.

## **12. Actividades extraescolares**

Desde este módulo no se proponen actividades extraescolares. Más allá de esto, se colaborará en la medida de lo posible con las actividades y los programas lanzados desde el centro, y de forma más específica, el Departamento de Informática y este grado en particular.

## **13. Bibliografía**

Normativa de ciberseguridad  
Editorial Paraninfo  
ISBN: 978-84-283-6545-1



IES ARCIPRESTE DE HITA. DEPARTAMENTO DE INFORMÁTICA

Programación didáctica del módulo: Hacking Ético

Ciclo formativo: Curso de Especialización en Ciberseguridad en Entornos  
de las Tecnologías de la Información

Curso 2025/2026

# **Programación didáctica del módulo:** **Hacking Ético**

## **Ciclo formativo:**

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

**Curso: 2025/2026**

**Profesor: *Rubén Avisón Melero***





## Índice

|   |    |
|---|----|
| 1. Introducción.....  | 4  |
| 2. Legislación aplicable .....  | 7  |
| 3. Ubicación .....  | 9  |
| 4. Resultados del aprendizaje.....  | 11 |
| 4.1    Objetivos comunes .....  | 11 |
| 4.2    Objetivos específicos del módulo (Resultados de aprendizaje) .....   | 14 |
| 5. Contenidos.....  | 15 |
| 6. Concordancia de las unidades de trabajo con los resultados del aprendizaje .....                                       | 17 |
| 7. Temporalización .....  | 17 |
| 8. Metodología .....  | 18 |
| 9. Evaluación.....  | 20 |
| 9.1    El proceso de evaluación .....   | 20 |
| 9.1.1    Evaluación inicial .....   | 20 |
| 9.1.2    Procedimientos para evaluar el proceso de aprendizaje del alumnado..   | 20 |
| 9.1.3    Evaluación sumativa .....  | 21 |
| 9.2    Criterios de evaluación .....  | 21 |
| 9.3    Criterios de calificación.....   | 24 |
| 9.4    Recuperación .....   | 25 |
| 9.5    Pérdida de la evaluación continua.....   | 26 |
| 9.5.1    Sistemas e instrumentos de evaluación para los alumnos que han perdido el derecho a la evaluación continua ..... | 27 |
| 9.5.2    Procedimiento de notificación de la pérdida de la evaluación continua .  | 27 |



IES ARCIPRESTE DE HIT. DEPARTAMENTO DE INFORMÁTICA

Programación didáctica del módulo: Hacking Ético

Ciclo formativo: Curso de Especialización en Ciberseguridad en Entornos  
de las Tecnologías de la Información

Curso 2025/2026

|       |  |    |
|-------|--|----|
| 9.5.3 | Casos específicos .....                                      | 28 |
| 9.6   | Autoevaluación del profesorado .....                         | 29 |
| 10.   | Alumnado con necesidades específicas de apoyo educativo..... | 30 |
| 11.   | Material didáctico.....                                      | 31 |
| 12.   | Actividades extraescolares .....                             | 32 |
| 13.   | Bibliografía.....  | 33 |



IES ARCIPRESTE DE HIT. DEPARTAMENTO DE INFORMÁTICA

Programación didáctica del módulo: Hacking Ético

Ciclo formativo: Curso de Especialización en Ciberseguridad en Entornos  
de las Tecnologías de la Información

Curso 2025/2026

## 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



IES ARCIPRESTE DE HIT. DEPARTAMENTO DE INFORMÁTICA

Programación didáctica del módulo: Hacking Ético

Ciclo formativo: Curso de Especialización en Ciberseguridad en Entornos  
de las Tecnologías de la Información

Curso 2025/2026

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).



IES ARCIPRESTE DE HITA. DEPARTAMENTO DE INFORMÁTICA  
Programación didáctica del módulo: Hacking Ético  
Ciclo formativo: Curso de Especialización en Ciberseguridad en Entornos  
de las Tecnologías de la Información  
Curso 2025/2026

## **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



IES ARCIPRESTE DE HITÁ. DEPARTAMENTO DE INFORMÁTICA

Programación didáctica del módulo: Hacking Ético

Ciclo formativo: Curso de Especialización en Ciberseguridad en Entornos  
de las Tecnologías de la Información

Curso 2025/2026

- 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 "Hacking Ético" del Curso de Especialización en 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.

|  |  |
|--|--|
|  | <p>IES ARCIPRESTE DE HIT. DEPARTAMENTO DE INFORMÁTICA</p> <p>Programación didáctica del módulo: Hacking Ético</p> <p>Ciclo formativo: Curso de Especialización en Ciberseguridad en Entornos de las Tecnologías de la Información</p> <p>Curso 2025/2026</p> |
|--|--|

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 405/2023, de 29 de mayo, por el que se actualizan los títulos de la formación profesional del sistema educativo de Técnico Superior en Desarrollo de Aplicaciones Multiplataforma y Técnico Superior en



IES ARCIPRESTE DE HIT. DEPARTAMENTO DE INFORMÁTICA

Programación didáctica del módulo: Hacking Ético

Ciclo formativo: Curso de Especialización en Ciberseguridad en Entornos  
de las Tecnologías de la Información

Curso 2025/2026

Desarrollo de Aplicaciones Web, de la familia profesional Informática y Comunicaciones, y se fijan sus enseñanzas mínimas.

13. 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.
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



|  |  |
|--|--|
|  | <p>IES ARCIPRESTE DE HIT. DEPARTAMENTO DE INFORMÁTICA</p> <p>Programación didáctica del módulo: Hacking Ético</p> <p>Ciclo formativo: Curso de Especialización en Ciberseguridad en Entornos de las Tecnologías de la Información</p> <p>Curso 2025/2026</p> |
|--|--|

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) Aulas para ciclos y cursos de especialización:**

- 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.
- 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.
- 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.
- Los cursos de especialización se imparten en horario de tarde y ocupan las mismas aulas que los grados superiores.

**b) Aulas APE**

- 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.

**c) Aulas para CFG Básico**

- La formación profesional básica se imparte en otras aulas independientes de los Ciclos.
- El aula de primero está en la planta baja del aulario.
- El aula de segundo está en el edificio principal del instituto, un aula situada entre las aulas APE y ATECA.



**d) Aula ATECA**

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

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.

Hacking Ético es un módulo donde la parte práctica puede ser más importante que la parte teórica, pero ambas son importantes para tener un dominio sobre el módulo. Además, como las aplicaciones de lo que se ve aquí se podría emplear tanto con fines éticos, como con otros fines, este módulo debería interesar una parte importante de la clase. Además, se tratan temas que se tratan continuamente en las noticias, así como en las películas. Es una disciplina que se está poniendo de moda y es fácil encontrar recursos en Internet.

## **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:



IES ARCIPRESTE DE HITA. DEPARTAMENTO DE INFORMÁTICA

Programación didáctica del módulo: Hacking Ético

Ciclo formativo: Curso de Especialización en Ciberseguridad en Entornos  
de las Tecnologías de la Información

Curso 2025/2026

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 de 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.



IES ARCIPRESTE DE HIT. DEPARTAMENTO DE INFORMÁTICA

Programación didáctica del módulo: Hacking Ético

Ciclo formativo: Curso de Especialización en Ciberseguridad en Entornos  
de las Tecnologías de la Información

Curso 2025/2026

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



IES ARCIPRESTE DE HIT. DEPARTAMENTO DE INFORMÁTICA

Programación didáctica del módulo: Hacking Ético

Ciclo formativo: Curso de Especialización en Ciberseguridad en Entornos  
de las Tecnologías de la Información

Curso 2025/2026

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 (Resultados de aprendizaje)**

1. Determina herramientas de monitorización para detectar vulnerabilidades aplicando técnicas de hacking ético.
2. Ataca y defiende en entornos de prueba, comunicaciones inalámbricas consiguiendo acceso a redes para demostrar sus vulnerabilidades.
3. Ataca y defiende en entornos de prueba, redes y sistemas consiguiendo acceso a información y sistemas de terceros.
4. Consolida y utiliza sistemas comprometidos garantizando accesos futuros.
5. Ataca y defiende en entornos de prueba, aplicaciones web consiguiendo acceso a datos o funcionalidades no autorizadas.



IES ARCIPRESTE DE HIT. DEPARTAMENTO DE INFORMÁTICA

Programación didáctica del módulo: Hacking Ético

Ciclo formativo: Curso de Especialización en Ciberseguridad en Entornos  
de las Tecnologías de la Información

Curso 2025/2026

## 5. Contenidos

### ***5.1 Unidad de Trabajo 1 - Determinación de las herramientas de monitorización para detectar vulnerabilidades:***

- Elementos esenciales del hacking ético.
- Diferencias entre hacking, hacking ético, tests de penetración y hacktivismo.
- Recolección de permisos y autorizaciones previos a un test de intrusión.
- Fases del hacking.
- Auditorías de caja negra y de caja blanca.
- Documentación de vulnerabilidades.
- Clasificación de herramientas de seguridad y hacking.
- ClearNet, Deep Web, Dark Web, Darknets. Conocimiento, diferencias y herramientas de acceso: Tor, ZeroNet, FreeNet.

### ***5.2 Unidad de Trabajo 2 - Ataque y defensa en entorno de pruebas, de las comunicaciones inalámbricas:***

- Comunicación inalámbrica.
- Modo infraestructura, ad-hoc y monitor.
- Análisis y recolección de datos en redes inalámbricas.
- Técnicas de ataques y exploración de redes inalámbricas.
- Ataques a otros sistemas inalámbricos.
- Realización de informes de auditoría y presentación de resultados.



IES ARCIPRESTE DE HIT. DEPARTAMENTO DE INFORMÁTICA

Programación didáctica del módulo: Hacking Ético

Ciclo formativo: Curso de Especialización en Ciberseguridad en Entornos  
de las Tecnologías de la Información

Curso 2025/2026

### ***5.3 Unidad de Trabajo 3 - Ataque y defensa en entorno de pruebas, de redes y sistemas para acceder a sistemas de terceros:***

- Fase de reconocimiento (footprinting).
- Fase de escaneo (fingerprinting).
- Monitorización de tráfico.
- Interceptación de comunicaciones utilizando distintas técnicas.
- Manipulación e inyección de tráfico.
- Administración de sistemas de manera remota.
- Ataques y auditorías de contraseñas.
- Pivoteo en la red.
- Instalación de puertas traseras con troyanos (RAT, Remote Access Trojan).

### ***5.4 Unidad de Trabajo 4 – Consolidación y utilización de sistemas comprometidos.***

- Administración de sistemas de manera remota.
- Ataques y auditorías de contraseñas.
- Pivoteo en la red.
- Instalación de puertas traseras con troyanos (RAT, Remote Access Trojan).

### ***5.5 Unidad de Trabajo 5 – Ataque y defensa en entorno de pruebas, a aplicaciones web:***

- Administración de sistemas de manera remota.
- Ataques y auditorías de contraseñas.
- Pivoteo en la red.
- Instalación de puertas traseras con troyanos (RAT, Remote Access Trojan).



## 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 | RE 1 | RE. 2 | RE. 3 | RE. 4 | RE. 5 |
|--|------|-------|-------|-------|-------|
| U.T. 1   | x    |       |       |       |       |
| U.T. 2   |      | x     |       |       |       |
| U.T. 3   |      |       | x     |       |       |
| U.T. 4   |      |       |       | x     |       |
| U.T. 5   |      |       |       |       | 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/Tema | Duración<br>prevista | Trimestre |
|------------------------|----------------------|-----------|
| U.T. 1                 | 44                   | 1º        |
| U.T. 2                 | 20                   | 2º        |
| U.T. 3                 | 20                   | 2º        |
| U.T. 4                 | 18                   | 3º        |
| U.T. 5                 | 18                   | 3º        |
| 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, respetando 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.



IES ARCIPRESTE DE HITA. DEPARTAMENTO DE INFORMÁTICA

Programación didáctica del módulo: Hacking Ético

Ciclo formativo: Curso de Especialización en Ciberseguridad en Entornos  
de las Tecnologías de la Información

Curso 2025/2026

- 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.



IES ARCIPRESTE DE HITÁ. DEPARTAMENTO DE INFORMÁTICA

Programación didáctica del módulo: Hacking Ético

Ciclo formativo: Curso de Especialización en Ciberseguridad en Entornos  
de las Tecnologías de la Información

Curso 2025/2026

## 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



IES ARCIPRESTE DE HITA. DEPARTAMENTO DE INFORMÁTICA

Programación didáctica del módulo: Hacking Ético

Ciclo formativo: Curso de Especialización en Ciberseguridad en Entornos  
de las Tecnologías de la Información

Curso 2025/2026

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**

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

- a) Se ha definido la terminología esencial del hacking ético.
- b) Se han identificado los conceptos éticos y legales frente al ciberdelito.
- c) Se ha definido el alcance y condiciones de un test de intrusión.
- d) Se han identificado los elementos esenciales de seguridad: confidencialidad, autenticidad, integridad y disponibilidad.



IES ARCIPRESTE DE HIT. DEPARTAMENTO DE INFORMÁTICA

Programación didáctica del módulo: Hacking Ético

Ciclo formativo: Curso de Especialización en Ciberseguridad en Entornos  
de las Tecnologías de la Información

Curso 2025/2026

- e) Se han identificado las fases de un ataque seguidas por un atacante.
- f) Se han analizado y definido los tipos vulnerabilidades.
- g) Se han analizado y definido los tipos de ataque.
- h) Se han determinado y caracterizado las diferentes vulnerabilidades existentes.
- i) Se han determinado las herramientas de monitorización disponibles en el mercado adecuadas en función del tipo de organización.

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

- a) Se han configurado los distintos modos de funcionamiento de las tarjetas de red inalámbricas.
- b) Se han descrito las técnicas de encriptación de las redes inalámbricas y sus puntos vulnerables.
- c) Se han detectado redes inalámbricas y se ha capturado tráfico de red como paso previo a su ataque.
- d) Se ha accedido a redes inalámbricas vulnerables.
- e) Se han caracterizado otros sistemas de comunicación inalámbricos y sus vulnerabilidades.
- f) Se han utilizado técnicas de "Equipo Rojo y Azul".
- g) Se han realizado informes sobre las vulnerabilidades detectadas.

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

- a) Se ha recopilado información sobre la red y sistemas objetivo mediante técnicas pasivas.
- b) Se ha creado un inventario de equipos, cuentas de usuario y potenciales vulnerabilidades de la red y sistemas objetivo mediante técnicas activas.



IES ARCIPRESTE DE HITA. DEPARTAMENTO DE INFORMÁTICA

Programación didáctica del módulo: Hacking Ético

Ciclo formativo: Curso de Especialización en Ciberseguridad en Entornos  
de las Tecnologías de la Información

Curso 2025/2026

c) Se ha interceptado tráfico de red de terceros para buscar información sensible.

d) Se ha realizado un ataque de intermediario, leyendo, insertando y modificando, a voluntad, el tráfico intercambiado por dos extremos remotos.

e) Se han comprometido sistemas remotos explotando sus vulnerabilidades.

#### 4. Consolida y utiliza sistemas comprometidos garantizando accesos futuros.

a) Se han administrado sistemas remotos a través de herramientas de línea de comandos.

b) Se han comprometido contraseñas a través de ataques de diccionario, tablas rainbow y fuerza bruta contra sus versiones encriptadas.

c) Se ha accedido a sistemas adicionales a través de sistemas comprometidos.

d) Se han instalado puertas traseras para garantizar accesos futuros a los sistemas comprometidos.

#### 5. Ataca y defiende en entornos de prueba, aplicaciones web consiguiendo acceso a datos o funcionalidades no autorizadas.


a) Se han identificado los distintos sistemas de autenticación web, destacando sus debilidades y fortalezas.

b) Se ha realizado un inventario de equipos, protocolos, servicios y sistemas operativos que proporcionan el servicio de una aplicación web.

c) Se ha analizado el flujo de las interacciones realizadas entre el navegador y la aplicación web durante su uso normal.

d) Se han examinado manualmente aplicaciones web en busca de las vulnerabilidades más habituales.

e) Se han usado herramientas de búsquedas y explotación de vulnerabilidades web.

|  |   |
|--|---|
|  | <p>IES ARCIPRESTE DE HITA. DEPARTAMENTO DE INFORMÁTICA</p> <p>Programación didáctica del módulo: Hacking Ético</p> <p>Ciclo formativo: Curso de Especialización en Ciberseguridad en Entornos de las Tecnologías de la Información</p> <p>Curso 2025/2026</p> |
|--|---|

f) Se ha realizado la búsqueda y explotación de vulnerabilidades web mediante herramientas software.

### **9.3 Criterios de calificación**


Para la superación del módulo es requisito indispensable que el alumno supere todos y 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 RRAA, 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
- El peso de las calificaciones de los RRAA se realizará mediante una media ponderada.
- El valor mínimo en los RRAA para considerar que las capacidades profesionales han sido alcanzadas será de 5. En el caso, que algún RRAA presente una puntuación inferior a 5, entonces la calificación final del módulo no podrá ser superior a 4.

|  |  |
|--|--|
|  | <p>IES ARCIPRESTE DE HIT. DEPARTAMENTO DE INFORMÁTICA</p> <p>Programación didáctica del módulo: Hacking Ético</p> <p>Ciclo formativo: Curso de Especialización en Ciberseguridad en Entornos de las Tecnologías de la Información</p> <p>Curso 2025/2026</p> |
|--|--|

| RESULTADOS DE APRENDIZAJE   | % Asignado Evaluación |
|---|-----------------------|
| RA1. Determina herramientas de monitorización para detectar vulnerabilidades aplicando técnicas de hacking ético.                         | 20%                   |
| RA2. Ataca y defiende en entornos de prueba, comunicaciones inalámbricas consiguiendo acceso a redes para demostrar sus vulnerabilidades. | 20%                   |
| RA3. Ataca y defiende en entornos de prueba, redes y sistemas consiguiendo acceso a información y sistemas de terceros.                   | 20%                   |
| RA4. Consolida y utiliza sistemas comprometidos garantizando accesos futuros.   | 20%                   |
| RA5. 5. Ataca y defiende en entornos de prueba, aplicaciones web consiguiendo acceso a datos o funcionalidades no autorizadas.            | 20%                   |
|   | 100%                  |


## 9.4 Recuperación

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

### 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.



|  |  |
|--|--|
|  | <p>IES ARCIPRESTE DE HIT. DEPARTAMENTO DE INFORMÁTICA</p> <p>Programación didáctica del módulo: Hacking Ético</p> <p>Ciclo formativo: Curso de Especialización en Ciberseguridad en Entornos de las Tecnologías de la Información</p> <p>Curso 2025/2026</p> |
|--|--|

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 por cada profesor.

El examen de la segunda convocatoria ordinaria incluirá solo aquellos contenidos que no se hayan conseguido superar en la primera.

### ***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.



IES ARCIPRESTE DE HITA. DEPARTAMENTO DE INFORMÁTICA

Programación didáctica del módulo: Hacking Ético

Ciclo formativo: Curso de Especialización en Ciberseguridad en Entornos  
de las Tecnologías de la Información

Curso 2025/2026

Adicionalmente, para fomentar el cuidado y corresponsabilidad del material de clase y prepararlos 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:



IES ARCIPRESTE DE HITA. DEPARTAMENTO DE INFORMÁTICA

Programación didáctica del módulo: Hacking Ético

Ciclo formativo: Curso de Especialización en Ciberseguridad en Entornos  
de las Tecnologías de la Información

Curso 2025/2026

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



IES ARCIPRESTE DE HIT. DEPARTAMENTO DE INFORMÁTICA

Programación didáctica del módulo: Hacking Ético

Ciclo formativo: Curso de Especialización en Ciberseguridad en Entornos  
de las Tecnologías de la Información

Curso 2025/2026

## 10. Departamentales

### **Medidas que se deben tomar durante el siguiente trimestre:**

1. Medidas metodológicas (clase magistral, libro de texto, nuevas tecnologías, etc)
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 renunciaciones 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.



IES ARCIPRESTE DE HITA. DEPARTAMENTO DE INFORMÁTICA

Programación didáctica del módulo: Hacking Ético

Ciclo formativo: Curso de Especialización en Ciberseguridad en Entornos  
de las Tecnologías de la Información

Curso 2025/2026

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, software de virtualización, máquinas virtuales (Kali Linux, Windows 7, Windows 10, etc.)
- Conexión a Internet
- Teams y portal Educamos
- Impresoras
- Adaptador de red capaz de ponerse en modo promiscuo

### 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.



IES ARCIPRESTE DE HITA. DEPARTAMENTO DE INFORMÁTICA

Programación didáctica del módulo: Hacking Ético

Ciclo formativo: Curso de Especialización en Ciberseguridad en Entornos  
de las Tecnologías de la Información

Curso 2025/2026

*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 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



IES ARCIPRESTE DE HIT. DEPARTAMENTO DE INFORMÁTICA

Programación didáctica del módulo: Hacking Ético

Ciclo formativo: Curso de Especialización en Ciberseguridad en Entornos  
de las Tecnologías de la Información

Curso 2025/2026

alumnos actuales sobre su visión del mundo laboral después de haber obtenido el título.

Durante este curso se plantea organizar y realizar si fuera posible alguna salida para participar en competiciones o eventos informáticos o visitar algún centro o empresa relacionado con el ciclo (Skills, CiberSeg, HoneyCon, Superordenador...).

### **13. Bibliografía**

- Gran parte del contenido de este curso está extraído del curso de Hacking Ético impartido por areaproject.
- Hacking Ético. J. L. Berenguel, P. Esteban. Paraninfo. 2023.





IES ARCIPRESTE DE HITA. DEPARTAMENTO DE INFORMÁTICA  
Programación didáctica del módulo: Incidentes de Ciberseguridad  
Curso de Especialización:  
Ciberseguridad en Entornos de las Tecnologías de la Información.  
Curso 2025/2026

# **Programación didáctica del módulo: Incidentes de Ciberseguridad**

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

**Curso: 2025/2026**

**Profesora: Celeste Rhodes Rodríguez**



IES ARCIPRESTE DE HITA. DEPARTAMENTO DE INFORMÁTICA  
Programación didáctica del módulo: Incidentes de Ciberseguridad  
Curso de Especialización:  
Ciberseguridad en Entornos de las Tecnologías de la Información.  
Curso 2025/2026

## Índice

|   |           |
|---|-----------|
| <b>1. Introducción .....</b>  | <b>4</b>  |
| <b>2. Legislación aplicable .....</b>   | <b>7</b>  |
| <b>3. Ubicación .....</b>   | <b>9</b>  |
| <b>4. Resultados del aprendizaje .....</b>  | <b>11</b> |
| 4.1    Objetivos comunes .....  | 12        |
| 4.2    Resultados de aprendizaje específicos del módulo.....                              | 14        |
| <b>5. Contenidos .....</b>  | <b>15</b> |
| 5.1.    UT 1: Desarrollo de Planes de prevención y Concienciación en Ciberseguridad ....  | 15        |
| 5.2.    UT 2: Auditoría de Incidentes de Ciberseguridad .....                             | 15        |
| 5.3.    UT 3: Investigación de los Incidentes de Ciberseguridad .....                     | 15        |
| 5.4.    UT 4: Implementación de Medidas de Ciberseguridad .....                           | 16        |
| 5.5.    UT 5: Detección y Documentación de Incidentes de Ciberseguridad .....             | 16        |
| <b>6. Concordancia de las unidades de trabajo con los resultados del aprendizaje.....</b> | <b>16</b> |
| <b>7. Temporalización .....</b>   | <b>17</b> |
| <b>8. Metodología.....</b>  | <b>17</b> |
| <b>9. Evaluación .....</b>  | <b>19</b> |
| 9.1.    El proceso de evaluación.....   | 19        |
| 9.2.    Criterios de evaluación .....   | 20        |
| 9.3.    Criterios de calificación .....   | 24        |
| 9.4.    Recuperación .....  | 25        |



IES ARCIPRESTE DE HITA. DEPARTAMENTO DE INFORMÁTICA  
Programación didáctica del módulo: Incidentes de Ciberseguridad  
Curso de Especialización:  
Ciberseguridad en Entornos de las Tecnologías de la Información.  
Curso 2025/2026

|      |  |           |
|------|--|-----------|
| 9.5. | Pérdida de la evaluación continua .....                              | 26        |
| 9.6. | Autoevaluación del profesorado .....                                 | 29        |
| 10.  | <i>Alumnado con necesidades específicas de apoyo educativo .....</i> | <i>30</i> |
| 11.  | <i>Material didáctico .....</i>                                      | <i>31</i> |
| 12.  | <i>Actividades extraescolares .....</i>                              | <i>32</i> |
| 13.  | <i>Bibliografía .....</i>  | <i>32</i> |



## 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



IES ARCIPRESTE DE HITA. DEPARTAMENTO DE INFORMÁTICA  
Programación didáctica del módulo: Incidentes de Ciberseguridad  
Curso de Especialización:  
Ciberseguridad en Entornos de las Tecnologías de la Información.  
Curso 2025/2026

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**



IES ARCIPRESTE DE HITA. DEPARTAMENTO DE INFORMÁTICA  
Programación didáctica del módulo: Incidentes de Ciberseguridad  
Curso de Especialización:  
Ciberseguridad en Entornos de las Tecnologías de la Información.  
Curso 2025/2026

- 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



IES ARCIPRESTE DE HITA. DEPARTAMENTO DE INFORMÁTICA  
Programación didáctica del módulo: Incidentes de Ciberseguridad  
Curso de Especialización:  
Ciberseguridad en Entornos de las Tecnologías de la Información.  
Curso 2025/2026

- 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 “Incidentes de ciberseguridad” del curso de especialización “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.



IES ARCIPRESTE DE HITA. DEPARTAMENTO DE INFORMÁTICA  
Programación didáctica del módulo: Incidentes de Ciberseguridad  
Curso de Especialización:  
Ciberseguridad en Entornos de las Tecnologías de la Información.  
Curso 2025/2026

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 405/2023, de 29 de mayo, por el que se actualizan los títulos de la formación profesional del sistema educativo de Técnico Superior en Desarrollo de Aplicaciones Multiplataforma y Técnico Superior en Desarrollo





de Aplicaciones Web, de la familia profesional Informática y Comunicaciones, y se fijan sus enseñanzas mínimas.

13. 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.
1. 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.



IES ARCIPRESTE DE HITA. DEPARTAMENTO DE INFORMÁTICA  
Programación didáctica del módulo: Incidentes de Ciberseguridad  
Curso de Especialización:  
Ciberseguridad en Entornos de las Tecnologías de la Información.  
Curso 2025/2026

El Departamento de Informática dispone de las siguientes aulas:

**a) Aulas para ciclos y cursos de especialización:**

- 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) Aulas APE**

- 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.

**c) Aulas para CFG Básico**

- 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.



**d) Aula ATECA**

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

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 cuenta con una parte teórica ya que el alumnado debe conocer y manejar conceptos relacionados con la ciberseguridad, pero al mismo tiempo tiene un carácter muy práctico. El alumnado que acude muestra un alto interés por el módulo y éste cuenta con un nivel de dificultad medio. En este módulo el alumno/a conseguirá 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. Por otra parte, de cara al mercado laboral, la superación de este módulo y del resto de módulos que componen el curso de especialización, proporcionará el título para desempeñar funciones en las organizaciones como pueden ser: experto en ciberseguridad, auditor de ciberseguridad o consultor de ciberseguridad.

## **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 de 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.



IES ARCIPRESTE DE HITA. DEPARTAMENTO DE INFORMÁTICA  
Programación didáctica del módulo: Incidentes de Ciberseguridad  
Curso de Especialización:  
Ciberseguridad en Entornos de las Tecnologías de la Información.  
Curso 2025/2026

11. Aplicar estándares de verificación requeridos por las aplicaciones para evitar incidentes de seguridad.
12. Automatizar planes de despliegado de software respetando los requisitos relativos a control de versiones, roles, permisos y otros para conseguir un despliegado 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 Resultados de aprendizaje específicos del módulo***

Los objetivos específicos del módulo descritos en el Real Decreto 479/2020, de 7 de abril, como resultados de aprendizaje son:

- 1) Desarrolla planes de prevención y concienciación en ciberseguridad, estableciendo normas y medidas de protección.
- 2) Analiza incidentes de ciberseguridad utilizando herramientas, mecanismos de detección y alertas de seguridad.
- 3) Investiga incidentes de ciberseguridad analizando los riesgos implicados y definiendo las posibles medidas a adoptar.
- 4) Implementa medidas de ciberseguridad en redes y sistemas respondiendo a los incidentes detectados y aplicando las técnicas de protección adecuadas.
- 5) Detecta y documenta incidentes de ciberseguridad siguiendo procedimientos de actuación establecidos.



## 5. Contenidos

Los contenidos de esta programación se desarrollarán en 5 unidades de trabajo.

### **5.1. UT 1: Desarrollo de Planes de prevención y Concienciación en Ciberseguridad**

- Principios generales en materia de ciberseguridad.
- Normativa de protección del puesto del trabajo.
- Plan de formación y concienciación en materia de ciberseguridad.
- Materiales de formación y concienciación.
- Auditorías internas de cumplimiento en materia de prevención.

### **5.2. UT 2: Auditoría de Incidentes de Ciberseguridad**

- Taxonomía de incidentes de ciberseguridad.
- Controles, herramientas y mecanismos de monitorización, identificación, detección y alerta de incidentes: tipos y fuentes.
- Controles, herramientas y mecanismos de detección e identificación de incidentes de seguridad física.
- Controles, herramientas y mecanismos de monitorización, identificación, detección y alerta de incidentes a través de la investigación en fuentes abiertas (OSINT).
- Clasificación, valoración, documentación, seguimiento inicial de incidentes de ciberseguridad.

### **5.3. UT 3: Investigación de los Incidentes de Ciberseguridad**

- Recopilación de evidencias.
- Análisis de evidencias.
- Investigación del incidente
- Intercambio de información del incidente con proveedores u organismos competentes.
- Medidas de contención de incidentes.



#### **5.4. UT 4: Implementación de Medidas de Ciberseguridad**

- Desarrollar procedimientos de actuación detallados para dar respuesta, mitigar, eliminar o contener los tipos de incidentes.
- Implantar capacidades de ciberresiliencia.
- Establecer flujos de toma de decisiones y escalado interno y/o externo adecuados.
- Tareas para restablecer los servicios afectados por incidentes.
- Documentación.
- Seguimiento de incidentes para evitar una situación similar.

#### **5.5. UT 5: Detección y Documentación de Incidentes de Ciberseguridad**

- Desarrollar procedimientos de actuación para la notificación de incidentes.
- Notificación interna de incidentes.
- Notificación de incidentes a quienes corresponda.

### **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 /<br>Resultados de aprendizaje | RE 1 | RE. 2 | RE. 3 | RE. 4 | RE. 5 |
|--|------|-------|-------|-------|-------|
| <b>U.T. 1</b>                                    | X    |       |       |       |       |
| <b>U.T. 2</b>                                    |      | X     |       |       |       |
| <b>U.T. 3</b>                                    |      |       | X     |       |       |
| <b>U.T. 4</b>                                    |      |       |       | X     |       |
| <b>U.T. 5</b>                                    |      |       |       |       | 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 |
|-------------------|-------------------|-----------|
| UT1               | 20                | 1º        |
| UT2               | 28                | 1º y 2º   |
| UT3               | 26                | 2º        |
| UT4               | 30                | 2º y 3º   |
| UT5               | 16                | 3º        |
| 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, respetando igualmente el material de la clase. Dado el poco material disponible para

|  |   |
|--|---|
|  | <p>IES ARCIPRESTE DE HITA. DEPARTAMENTO DE INFORMÁTICA</p> <p>Programación didáctica del módulo: Incidentes de Ciberseguridad</p> <p>Curso de Especialización:</p> <p>Ciberseguridad en Entornos de las Tecnologías de la Información.</p> <p>Curso 2025/2026</p> |
|--|---|

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**

Teniendo en cuenta los Resultados de Aprendizaje, los Criterios de Evaluación son los siguientes:



**RA1. Desarrolla planes de prevención y concienciación en ciberseguridad, estableciendo normas y medidas de protección.**

Criterios de evaluación:

- a) Se han definido los principios generales de la organización en materia de ciberseguridad, que deben ser conocidos y apoyados por la dirección de la misma.
- b) Se ha establecido una normativa de protección del puesto de trabajo.
- c) Se ha definido un plan de concienciación de ciberseguridad dirigido a los empleados.
- d) Se ha desarrollado el material necesario para llevar a cabo las acciones de concienciación dirigidas a los empleados.
- e) Se ha realizado una auditoría para verificar el cumplimiento del plan de prevención y concienciación de la organización.

**RA2. Analiza incidentes de ciberseguridad utilizando herramientas, mecanismos de detección y alertas de seguridad.**

Criterios de evaluación:

- a) Se ha clasificado y definido la taxonomía de incidentes de ciberseguridad que pueden afectar a la organización.
- b) Se han establecido controles, herramientas y mecanismos de monitorización, identificación, detección y alerta de incidentes
- c) Se han establecido controles y mecanismos de detección e identificación de incidentes de seguridad física.
- d) Se han establecido controles, herramientas y mecanismos de monitorización, identificación, detección y alerta de incidentes a través de la investigación en fuentes abiertas (OSINT: Open Source Intelligence).
- e) Se ha realizado una clasificación, valoración, documentación y seguimiento de los incidentes detectados dentro de la organización.



**RA3. Investiga incidentes de ciberseguridad analizando los riesgos implicados y definiendo las posibles medidas a adoptar.**


Criterios de evaluación:

- a) Se han recopilado y almacenado de forma segura evidencias de incidentes de ciberseguridad que afectan a la organización.
- b) Se ha realizado un análisis de evidencias.
- c) Se ha realizado la investigación de incidentes de ciberseguridad.
- d) Se ha intercambiado información de incidentes, con proveedores y/o organismos competentes que podrían hacer aportaciones al respecto.
- e) Se han iniciado las primeras medidas de contención de los incidentes para limitar los posibles daños causados.

**RA4. Implementa medidas de ciberseguridad en redes y sistemas respondiendo a los incidentes detectados y aplicando las técnicas de protección adecuadas.**

Criterios de evaluación:

- a) Se han desarrollado procedimientos de actuación detallados para dar respuesta, mitigar, eliminar o contener los tipos de incidentes de ciberseguridad más habituales.
- b) Se han preparado respuestas ciberresilientes ante incidentes que permitan seguir prestando los servicios de la organización y fortaleciendo las capacidades de identificación, detección, prevención, contención, recuperación y cooperación con terceros.
- c) Se ha establecido un flujo de toma de decisiones y escalado de incidentes interno y/o externo adecuados.
- d) Se han llevado a cabo las tareas de restablecimiento de los servicios afectados por un incidente hasta confirmar la vuelta a la normalidad.
- e) Se han documentado las acciones realizadas y las conclusiones que permitan mantener un registro de “lecciones aprendidas”.

|  |   |
|--|---|
|  | <p>IES ARCIPRESTE DE HITA. DEPARTAMENTO DE INFORMÁTICA</p> <p>Programación didáctica del módulo: Incidentes de Ciberseguridad</p> <p>Curso de Especialización:</p> <p>Ciberseguridad en Entornos de las Tecnologías de la Información.</p> <p>Curso 2025/2026</p> |
|--|---|

f) Se ha realizado un seguimiento adecuado del incidente para evitar que una situación similar se vuelva a repetir.

**RA5. Detecta y documenta incidentes de ciberseguridad siguiendo procedimientos de actuación establecidos.**

Criterios de evaluación:

- a) Se ha desarrollado un procedimiento de actuación detallado para la notificación de incidentes de ciberseguridad en los tiempos adecuados.
- b) Se ha notificado el incidente de manera adecuada al personal interno de la organización responsable de la toma de decisiones.
- c) Se ha notificado el incidente de manera adecuada a las autoridades competentes en el ámbito de la gestión de incidentes de ciberseguridad en caso de ser necesario.
- d) Se ha notificado formalmente el incidente a los afectados, personal interno, clientes, proveedores, etc., en caso de ser necesario.
- e) Se ha notificado el incidente a los medios de comunicación en caso de ser necesario.



### 9.3. Criterios de calificación

Para la superación del módulo es requisito indispensable que el alumno supere **todos y 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 RRAA, 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
- El peso de las calificaciones de los RRAA se realizará mediante una media ponderada.
- El valor mínimo en los RRAA para considerar que las capacidades profesionales han sido alcanzadas será de 5. En el caso, que algún RRAA presente una puntuación inferior a 5, entonces la calificación final del módulo no podrá ser superior a 4.
- Para obtener la calificación de cada RA se ponderarán los criterios de evaluación asociados.

| RESULTADOS DE APRENDIZAJE | % Asignado Evaluación |
|---------------------------|-----------------------|
| RA1                       | 20%                   |
| RA2                       | 20%                   |
| RA3                       | 20%                   |
| RA4                       | 20%                   |
| RA5                       | 20%                   |
| TOTAL                     | 100%                  |





#### **9.4. Recuperación**

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

Para recuperar los RRAA suspensos, se deberán realizar los trabajos o exámenes escritos correspondientes a sus criterios de evaluación. Aquellos criterios que se hayan calificado como superados durante la evaluación no será obligatorio recuperarlos.

#### **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).

Para la recuperación de los RRAA no superados en la segunda convocatoria ordinaria se seguirán los mismos criterios que para la primera: “se deberán realizar los trabajos o exámenes escritos correspondientes a sus criterios de evaluación. Aquellos criterios que se hayan calificado como superados durante la evaluación no será obligatorio recuperarlos.”



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

Dado que se utiliza la plataforma Moodle 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.

#### **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



IES ARCIPRESTE DE HITA. DEPARTAMENTO DE INFORMÁTICA  
Programación didáctica del módulo: Incidentes de Ciberseguridad  
Curso de Especialización:  
Ciberseguridad en Entornos de las Tecnologías de la Información.  
Curso 2025/2026

**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 renunciaciones 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 y programas de software específicos del módulo.
- Conexión a Internet
- Teams y portal Educamos
- Impresoras
- Aula virtual

### 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,*



IES ARCIPRESTE DE HITA. DEPARTAMENTO DE INFORMÁTICA  
Programación didáctica del módulo: Incidentes de Ciberseguridad  
Curso de Especialización:  
Ciberseguridad en Entornos de las Tecnologías de la Información.  
Curso 2025/2026

*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 causaran daño a las instalaciones o material y no reparen el daño causado perderán el derecho a la evaluación continua.

## **12. Actividades extraescolares**

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**

- **Incidentes de ciberseguridad.** Editorial Paraninfo. ISBN: 9788428365413





IES ARCIPRESTE DE HITA. DEPARTAMENTO DE INFORMÁTICA  
Programación didáctica del módulo Puesta en Producción Segura  
Curso de Especialización Ciberseguridad en Entornos de las Tecnologías  
de la Información  
Curso 2025/2026

# **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

|   |    |
|---|----|
| Índice .....  | 2  |
| 1. Introducción.....  | 4  |
| 2. Legislación aplicable .....  | 7  |
| 3. Ubicación .....  | 9  |
| 4. Resultados del aprendizaje.....  | 12 |
| 4.1 Objetivos comunes .....   | 13 |
| 4.2 Objetivos específicos del módulo.....   | 15 |
| 5. Contenidos.....  | 16 |
| 5.1 Unidad de Trabajo 1. Prueba de aplicaciones web y para dispositivos móviles                             | 16 |
| 5.2 Unidad de Trabajo 2. Determinación del nivel de seguridad requerido por aplicaciones .....              | 17 |
| 5.3 Unidad de Trabajo 3. Detección y corrección de vulnerabilidades de aplicaciones web .....               | 18 |
| 5.4 Unidad de Trabajo 4. Detección de problemas de seguridad en aplicaciones para dispositivos móviles..... | 19 |
| 5.5 Unidad de Trabajo 5. Implantación de sistemas seguros de despliegado de software.....                   | 21 |
| 6. Concordancia de las unidades de trabajo con los resultados del aprendizaje .....                         | 22 |
| 7. Temporalización .....  | 23 |
| 8. Metodología .....  | 24 |
| 9. Evaluación.....  | 26 |
| 9.1 El proceso de evaluación .....  | 26 |



IES ARCIPRESTE DE HIT. DEPARTAMENTO DE INFORMÁTICA  
Programación didáctica del módulo Puesta en Producción Segura  
Curso de Especialización Ciberseguridad en Entornos de las Tecnologías  
de la Información  
Curso 2025/2026

|        |  |    |
|--------|--|----|
| 9.1.1  | Evaluación inicial .....   | 26 |
| 9.1.2  | Procedimientos para evaluar el proceso de aprendizaje del alumnado ....  | 26 |
| 9.1.3  | Evaluación sumativa .....  | 27 |
| 9.2    | Criterios de evaluación .....  | 27 |
| 9.3    | Criterios de calificación .....  | 30 |
| 9.4    | Recuperación .....   | 34 |
| 9.4.1. | Planificación de las actividades de recuperación de los módulos no superados .....                               | 36 |
| 9.5    | Pérdida de la evaluación continua .....  | 36 |
| 9.5.1  | Sistemas e instrumentos de evaluación para los alumnos que han perdido el derecho a la evaluación continua ..... | 37 |
| 9.5.2  | Procedimiento de notificación de la pérdida de la evaluación continua ...  | 38 |
| 9.5.3  | Casos específicos .....  | 39 |
| 9.6    | Autoevaluación del profesorado .....   | 39 |
| 10.    | Alumnado con necesidades específicas de apoyo educativo.....   | 41 |
| 11.    | Material didáctico.....  | 41 |
| 12.    | Actividades extraescolares .....   | 43 |
| 13.    | Bibliografía.....  | 43 |



## 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



IES ARCIPRESTE DE HITA. DEPARTAMENTO DE INFORMÁTICA  
Programación didáctica del módulo Puesta en Producción Segura  
Curso de Especialización Ciberseguridad en Entornos de las Tecnologías  
de la Información  
Curso 2025/2026

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**



IES ARCIPRESTE DE HIT. DEPARTAMENTO DE INFORMÁTICA  
Programación didáctica del módulo Puesta en Producción Segura  
Curso de Especialización Ciberseguridad en Entornos de las Tecnologías  
de la Información  
Curso 2025/2026

- 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



IES ARCIPRESTE DE HIT. DEPARTAMENTO DE INFORMÁTICA  
Programación didáctica del módulo Puesta en Producción Segura  
Curso de Especialización Ciberseguridad en Entornos de las Tecnologías  
de la Información  
Curso 2025/2026

- 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.



IES ARCIPRESTE DE HITA. DEPARTAMENTO DE INFORMÁTICA  
Programación didáctica del módulo Puesta en Producción Segura  
Curso de Especialización Ciberseguridad en Entornos de las Tecnologías  
de la Información  
Curso 2025/2026

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



IES ARCIPRESTE DE HIT. DEPARTAMENTO DE INFORMÁTICA  
Programación didáctica del módulo Puesta en Producción Segura  
Curso de Especialización Ciberseguridad en Entornos de las Tecnologías  
de la Información  
Curso 2025/2026

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) Aulas para ciclos y cursos de especialización:**

- 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) Aulas APE**

- 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) Aulas para CFG Básico**

- 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.



IES ARCIPRESTE DE HIT. DEPARTAMENTO DE INFORMÁTICA  
Programación didáctica del módulo Puesta en Producción Segura  
Curso de Especialización Ciberseguridad en Entornos de las Tecnologías  
de la Información  
Curso 2025/2026

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

**c) Aula ATECA**

- 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 de 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.



IES ARCIPRESTE DE HITA. DEPARTAMENTO DE INFORMÁTICA  
Programación didáctica del módulo Puesta en Producción Segura  
Curso de Especialización Ciberseguridad en Entornos de las Tecnologías  
de la Información  
Curso 2025/2026

11. Aplicar estándares de verificación requeridos por las aplicaciones para evitar incidentes de seguridad.
12. Automatizar planes de despliegado de software respetando los requisitos relativos a control de versiones, roles, permisos y otros para conseguir un despliegado 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 despliegado 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   |
|---|---|
| <ol style="list-style-type: none"><li>1. Fundamentos de la programación.</li><li>2. Lenguajes de programación interpretados y compilados.</li><li>3. Código fuente y entornos de desarrollo.</li><li>4. Ejecución de software.</li><li>5. Elementos principales de los programas.</li><li>6. Pruebas. Tipos.</li><li>7. Seguridad en los lenguajes de programación y sus entornos de ejecución ("sandboxes").</li></ol> | <ol style="list-style-type: none"><li>1. Comparar diferentes lenguajes de programación de acuerdo a sus características principales.</li><li>2. Describir los diferentes modelos de ejecución software.</li><li>3. Reconocer los elementos básicos del código fuente, dándoles significado.</li><li>4. Ejecutar diferentes tipos de prueba de software.</li><li>5. Evaluar los lenguajes de programación de acuerdo con la infraestructura de seguridad que proporcionan.</li></ol> |
| <b>Resultados y Criterios de Evaluación asociados a los Contenidos y Objetivos:</b>   |   |
| RA1: Prueba aplicaciones web y aplicaciones para dispositivos móviles analizando la estructura del código y su modelo de ejecución.<br><br>a) Se han comparado diferentes lenguajes de programación de acuerdo a sus características principales.<br><br>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***

| <b>Contenidos</b>   | <b>Objetivos</b>  |
|---|---|
| <ol style="list-style-type: none"><li>1. Fuentes abiertas para el desarrollo seguro.</li><li>2. Listas de riesgos de seguridad habituales: OWASP Top Ten (web y móvil).</li><li>3. Requisitos de verificación necesarios asociados al nivel de seguridad establecido</li><li>4. Comprobaciones de seguridad a nivel de aplicación: ASVS (Application Security Verification Standard).</li></ol> | <ol style="list-style-type: none"><li>1. Caracterizar los niveles de verificación de seguridad en aplicaciones establecidas por los estándares internacionales (ASVS, "Application Security Verification Standard").</li><li>2. Identificar el nivel de verificación de seguridad requerido por las aplicaciones en función de sus riesgos de acuerdo a estándares reconocidos.</li><li>3. Enumerar los requisitos de verificación necesarios asociados al nivel de seguridad establecido.</li><li>4. Reconocer los principales riesgos de las aplicaciones desarrolladas, en función de sus características.</li></ol> |
| <b>Resultados y Criterios de Evaluación asociados a los Contenidos y Objetivos:</b>   |   |
| 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.                                  | 1. Validar las entradas de los usuarios.   |
| 2. Listas públicas de vulnerabilidades de aplicaciones web. OWASP Top Ten. | 2. Detectar riesgos de inyección tanto en el servidor como en el cliente.                |
| 3. Entrada basada en formularios. Inyección. Validación de la entrada.     | 3. Gestionar correctamente la sesión del usuario durante el uso de la aplicación.        |
| 4. Estándares de autenticación y autorización.                             | 4. Hacer uso de roles para el control de acceso.   |
| 5. Robo de sesión.   | 5. Utilizar algoritmos criptográficos seguros para almacenar las contraseñas de usuario. |
| 6. Vulnerabilidades web.   |  |
| 7. Almacenamiento seguro de contraseñas.                                   | 6. Configurar servidores web para reducir el riesgo de sufrir ataques conocidos.         |



|   |   |
|---|---|
| 8. Contramedidas. HSTS, CSP, CAPTCHAs, entre otros.   | 7. Incorporar medidas para evitar los ataques a contraseñas, envío masivo de mensajes o registros de usuarios a través de programas automáticos (bots). |
| 9. Seguridad de portales y aplicativos webs. Soluciones WAF (Web Application Firewall).   |   |
| <b>Resultados y Criterios de Evaluación asociados a los Contenidos y Objetivos:</b>   |   |
| 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***

| <b>Contenidos</b>  | <b>Objetivos</b>   |
|--|--|
| 1. Modelos de permisos en plataformas móviles. Llamadas al sistema protegidas. | 1. Comparar los diferentes modelos de permisos de las plataformas móviles. |



IES ARCIPRESTE DE HITA. DEPARTAMENTO DE INFORMÁTICA

Programación didáctica del módulo Puesta en Producción Segura

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

Curso 2025/2026

|  |   |
|--|---|
| <ol style="list-style-type: none"><li>2. Firma y verificación de aplicaciones.</li><li>3. Almacenamiento seguro de datos.</li><li>4. Validación de compras integradas en la aplicación.</li><li>5. Fuga de información en los ejecutables.</li><li>6. Soluciones CASB.</li></ol>   | <ol style="list-style-type: none"><li>2. Describir técnicas de almacenamiento seguro de datos en los dispositivos, para evitar la fuga de información.</li><li>3. Implantar un sistema de validación de compras integradas en la aplicación haciendo uso de validación en el servidor.</li><li>4. Utilizar herramientas de monitorización de tráfico de red para detectar el uso de protocolos inseguros de comunicación de las aplicaciones móviles.</li><li>5. Inspeccionar binarios de aplicaciones móviles para buscar fugas de información sensible.</li></ol> |
| <b>Resultados y Criterios de Evaluación asociados a los Contenidos y Objetivos:</b>  |   |
| <p>RA4: Detecta problemas de seguridad en las aplicaciones para dispositivos móviles, monitorizando su ejecución y analizando ficheros y datos.</p> <p>a) Se han comparado los diferentes modelos de permisos de las plataformas móviles.</p> <p>b) Se han descrito técnicas de almacenamiento seguro de datos en los dispositivos, para evitar la fuga de información.</p> <p>c) Se ha implantado un sistema de validación de compras integradas en la aplicación haciendo uso de validación en el servidor.</p> <p>d) Se han utilizado herramientas de monitorización de tráfico de red para detectar el uso de protocolos inseguros de comunicación de las aplicaciones móviles.</p> <p>e) Se han inspeccionado binarios de aplicaciones móviles para buscar fugas de información sensible.</p> |   |



### ***5.5 Unidad de Trabajo 5. Implantación de sistemas seguros de despliegado de software***

| Contenidos   | Objetivos   |
|--|---|
| <ol style="list-style-type: none"><li>1. Puesta segura en producción.</li><li>2. Prácticas unificadas para el desarrollo y operación del software (DevOps).</li><li>3. Sistema de control de versiones.</li><li>4. Sistemas de automatización de construcción (build).</li><li>5. Integración continua y automatización de pruebas.</li><li>6. Escalado de servidores. Virtualización. Contenedores.</li><li>7. Gestión automatizada de configuraciones de sistemas.</li><li>8. Herramientas de simulación de fallos.</li><li>9. Orquestación de contenedores.</li></ol> | <ol style="list-style-type: none"><li>1. Identificar las características, principios y objetivos de la integración del desarrollo y operación del software.</li><li>2. Implantar sistemas de control de versiones, administrando los roles y permisos solicitados.</li><li>3. Instalar, configurar y verificar sistemas de integración continua, conectándolos con sistemas de control de versiones.</li><li>4. Planificar, implementar y automatizar planes de despliegado de software.</li><li>5. Evaluar la capacidad del sistema desplegado para reaccionar de forma automática a fallos.</li><li>6. Documentar las tareas realizadas y los procedimientos a seguir para la recuperación ante desastres.</li><li>7. Crear bucles de retroalimentación ágiles entre los miembros del equipo.</li></ol> |

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

RA5: Implanta sistemas seguros de despliegado 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 despliegado 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            | <b>Detección y corrección de vulnerabilidades de aplicaciones web</b>                | 26  | 2    |
| UT04            | <b>Detección de problemas de seguridad en aplicaciones para dispositivos móviles</b> | 26  | 2, 3 |
| UT05            | <b>Implantación de sistemas seguros de despliegado de software</b>                   | 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, respetando 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:





IES ARCIPRESTE DE HITA. DEPARTAMENTO DE INFORMÁTICA  
Programación didáctica del módulo Puesta en Producción Segura  
Curso de Especialización Ciberseguridad en Entornos de las Tecnologías  
de la Información  
Curso 2025/2026

- 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 despliegado 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 despliegado 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.



IES ARCIPRESTE DE HIT. DEPARTAMENTO DE INFORMÁTICA  
Programación didáctica del módulo Puesta en Producción Segura  
Curso de Especialización Ciberseguridad en Entornos de las Tecnologías  
de la Información  
Curso 2025/2026

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. Instala sistemas seguros de despliegado de software, utilizando herramientas para la automatización de la construcción de sus           | UT05              | 20%                  |



IES ARCIPRESTE DE HITA. DEPARTAMENTO DE INFORMÁTICA  
Programación didáctica del módulo Puesta en Producción Segura  
Curso de Especialización Ciberseguridad en Entornos de las Tecnologías  
de la Información  
Curso 2025/2026

|           |       |      |
|-----------|-------|------|
| 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 esta 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, si 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.



IES ARCIPRESTE DE HITA. DEPARTAMENTO DE INFORMÁTICA  
Programación didáctica del módulo Puesta en Producción Segura  
Curso de Especialización Ciberseguridad en Entornos de las Tecnologías  
de la Información  
Curso 2025/2026

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 esta 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 renunciaciones 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 Terner, Pilar Pavón Rosano, Ángel Jesús Varela Vaca, Francisco José de Haro Olmo. Paraninfo.
- Material elaborado por el profesor.