



Unión Europea

Fondo Social Europeo

"El FSE invierte en tu futuro"

Formación
Financiada
por el Fondo
Social Europeo

I.E.S. AGUADULCE

Aguadulce (Almería)

PROGRAMACIÓN DIDÁCTICA

PUESTA EN PRODUCCIÓN SEGURA

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

CURSO 2023/24

PROFESOR: Ismael López García

Contenido

Introducción	3
Contexto	4
1.- Marco Legal.....	5
2.- Competencias, objetivos y resultados de aprendizaje.	6
2.1.- Competencias profesionales, personales y sociales.	6
2.2.- Objetivos generales.....	6
2.3.- Resultados de aprendizaje.	7
3.- Secuenciación y temporalización de las unidades didácticas.	9
4.- Contenidos.	10
5.- Evaluación.	11
5.1. Evidencias: técnicas e instrumentos	11
5.2. Ponderación Criterios de Evaluación	12
5.3. Evaluación inicial.....	16
5.4. Criterios de calificación	16
5.4.1.- Calificación de cada unidad.....	16
5.4.2.- Calificación de cada evaluación	18
5.4.3.- Criterios de evaluación de la expresión escrita.....	19
5.4.4.- Calificación final.....	19
5.5. Evaluación extraordinaria	19
5.6. Periodo entre la 3ª evaluación parcial y la evaluación final:	20
6.- Metodología y materiales didácticos.	21
6.1. Agrupamientos.....	21
6.2. Tipos de tareas.....	22
6.3. Recursos y materiales	22
6.4. Utilización del aula Virtual como apoyo a la docencia reglada.....	23
7.- Atención a la diversidad.....	23
8.- Materiales y recursos didácticos.....	24
9.- Bibliografía	24

Introducción

Se ha realizado la programación didáctica del módulo profesional de **Puesta en Producción Segura** (en adelante **PPS**), que forma parte del curso de especialización **Ciberseguridad en Entornos de las Tecnologías de la Información** (en adelante **CETI**), cuya duración total es de 720 horas impartidas en un curso:

MÓDULOS PROFESIONALES	HORAS TOTALES	HORAS SEMANALES
5021. Incidentes de ciberseguridad.	150	5
5022. Bastionado de redes y sistemas.	150	5
5023. Puesta en producción segura.	120	4
5024. Análisis forense informático.	120	4
5025. Hacking ético.	120	4
5026. Normativa de ciberseguridad.	60	2
TOTALES	720	30

El citado módulo profesional es impartido en el mencionado curso de especialización CETI con una duración de **120 horas** impartándose a un ritmo de **4 horas semanales**.

La organización del curso se realizará en 30 semanas de clase con fecha de 29/09/23 y finalizará el 19/05/24. La mejora de resultados se realizará desde el 20/05/24 hasta fin de curso.

Contexto

El IES Aguadulce está situado en la barriada del mismo nombre perteneciente al municipio de Roquetas de Mar (Almería). Cuenta con una población estimada de 90.000 habitantes. Concretamente Aguadulce es un barrio residencial que cuenta con un gran atractivo turístico en la época estival ya que cuenta con playa, puerto deportivo etc.

En cuanto al centro educativo es de importancia señalar que cuenta con amplia oferta formativa en la familia profesional de informática y comunicaciones. En el mismo se imparten los ciclos formativos siguientes:

Nivel	Nombre de Ciclo Formativo	Turno
Grado básico	Informática de Oficina	Mañana
Grado medio	Sistemas Microinformáticos y Redes	Mañana y tarde
Grado superior	Desarrollo de Aplicaciones Web	Mañana y distancia
Grado superior	Desarrollo de Aplicaciones Multiplataforma	Mañana, tarde y distancia
Grado superior	Administración de Sistemas Informáticos y en Red	Tarde y distancia

Este curso de especialización, está dirigido a alumnado que ya cuenta con una titulación de Formación Profesional de Grado Superior de la Familia Profesional de Informática y Comunicaciones, lo que supone una continuidad en su formación y adaptación al mercado profesional y las demandas formativas emergentes y la especialización cada vez más requerida, así como el aumento de competencias profesionales en materia de ciberseguridad.

En particular, este módulo profesional contiene la formación necesaria para desempeñar la función de puesta en producción mediante el desarrollo de un sistema de despliegue de software seguro.

La función de implantación de un sistema de despliegue seguro incluye aspectos como la monitorización de aplicaciones y dispositivos para detectar los vectores de ataque más comunes.

Las actividades profesionales asociadas a esta función se aplican en el análisis de las aplicaciones web y dispositivos móviles, así como en la configuración de servidores web.

Este curso se cuenta con un grupo de 11 alumnos, de los cuales 10 son alumnos y 1 es una alumna. La procedencia del alumnado es predominante del mismo centro (4 alumnos provienen de DAM/DAW y 4 alumnos de ASIR). El resto vienen de institutos de la provincia titulados 2 en DAW y 1 en ASIR.

Si bien el nivel general es bastante elevado en el área de la informática hay que mencionar que tenemos dos perfiles profesionales distintos. Por un lado, el programador Web y de Aplicaciones (DAW y DAM) y por otro los Administradores de Sistemas y Redes (ASIR).

1.- Marco Legal

Para la elaboración de esta programación didáctica se han utilizado los siguientes textos de legislación vigente para la formación profesional específica:

- **Ley Orgánica 3/2020**, de 29 de diciembre, por la que se modifica la Ley Orgánica 2/2006, de 3 de mayo, de Educación (LOMLOE).
- **Ley 17/2007**, de 10 de diciembre de Educación de Andalucía (LEA).
- **Real Decreto 659/2023**, de 18 de julio, por el que se desarrolla la ordenación del Sistema de Formación Profesional que está en vigor, pero no detalla las enseñanzas mínimas.

Nuestro sistema educativo en el Real Decreto 659/2023, de 18 de julio, desarrolla la ordenación del Sistema de Formación Profesional y **deroga** el anterior **Real Decreto 1147/2011**, de 29 de julio.

El Real Decreto 659/2023 en su Disposición transitoria segunda: Vigencia de la ordenación de los títulos de formación profesional, establece que “Hasta tanto no se proceda reglamentariamente a su modificación, permanecerá vigente la ordenación de los títulos de formación profesional básica, de grado medio o de grado superior recogida en cada uno de los reales decretos por los que se establecen”.

- **Real Decreto 479/2020, de 7 de abril** y por el que se establece el Curso de especialización en CITE y fijan los aspectos básicos del currículo.
- A falta de orden autonómica específica referente al currículo en Andalucía en el curso académico actual 2023/24, se ha tomado como referencia las **Instrucciones de 30 de agosto de 2023**, de la Dirección General de Formación Profesional de la Consejería de Educación y Deporte de la Junta de Andalucía, por la que se ordena de forma experimental los cursos de especialización de Formación Profesional en el curso 2022/2023, se regulan los criterios y el procedimiento de admisión del alumnado, así como se establecen otros aspectos organizativos.

2.- Competencias, objetivos y resultados de aprendizaje.

2.1.- Competencias profesionales, personales y sociales.

Este módulo profesional contribuye a la adquisición de las Competencias Profesionales, Personales y Sociales siguientes que se incluyen en el artículo 5 del **Real Decreto** que regula el curso de especialización CETI:

- f) Analizar el nivel de seguridad requerido por las aplicaciones y los vectores de ataque más habituales, evitando incidentes de ciberseguridad.*
- g) Implantar sistemas seguros de despliegado de software con la adecuada coordinación entre los desarrolladores y los responsables de la operación del software.*
- k) Elaborar documentación técnica y administrativa cumpliendo con la legislación vigente, respondiendo a los requisitos establecidos.*
- l) Adaptarse a las nuevas situaciones laborales, manteniendo actualizados los conocimientos científicos, técnicos y tecnológicos relativos a su entorno profesional, gestionando su formación y los recursos existentes en el aprendizaje a lo largo de la vida.*
- m) Resolver situaciones, problemas o contingencias con iniciativa y autonomía en el ámbito de su competencia, con creatividad, innovación y espíritu de mejora en el trabajo personal y en el de los miembros del equipo.*
- n) Generar entornos seguros en el desarrollo de su trabajo y el de su equipo, supervisando y aplicando los procedimientos de prevención de riesgos laborales y ambientales, de acuerdo con lo establecido por la normativa y los objetivos de la organización.*
- ñ) Supervisar y aplicar procedimientos de gestión de calidad, de accesibilidad universal y de «diseño para todas las personas», en las actividades profesionales incluidas en los procesos de producción o prestación de servicio.*

2.2.- Objetivos generales.

Este módulo profesional contribuye a la adquisición de los Objetivos Generales siguientes que se incluyen en el artículo 8 del **Real Decreto** que regula el curso de especialización CETI:

- k) Aplicar estándares de verificación requeridos por las aplicaciones para evitar incidentes de seguridad.*
- l) Automatizar planes de despliegado de software respetando los requisitos relativos a control de versiones, roles, permisos y otros para conseguir un despliegado seguro.*
- q) Desarrollar manuales de información, utilizando herramientas ofimáticas y de diseño asistido por ordenador para elaborar documentación técnica y administrativa.*

- r) *Analizar y utilizar los recursos y oportunidades de aprendizaje relacionados con la evolución científica, tecnológica y organizativa del sector y las tecnologías de la información y la comunicación, para mantener el espíritu de actualización y adaptarse a nuevas situaciones laborales y personales.*
- s) *Desarrollar la creatividad y el espíritu de innovación para responder a los retos que se presentan en los procesos y en la organización del trabajo y de la vida personal.*
- t) *Evaluar situaciones de prevención de riesgos laborales y de protección ambiental, proponiendo y aplicando medidas de prevención personales y colectivas, de acuerdo con la normativa aplicable en los procesos de trabajo, para garantizar entornos seguros.*
- u) *Identificar y proponer las acciones profesionales necesarias para dar respuesta a la accesibilidad universal y al «diseño para todas las personas».*
- v) *Identificar y aplicar parámetros de calidad en los trabajos y actividades realizados en el proceso de aprendizaje, para valorar la cultura de la evaluación y de la calidad y ser capaces de supervisar y mejorar procedimientos de calidad.*

2.3.- Resultados de aprendizaje.

RA1: Prueba aplicaciones web y aplicaciones para dispositivos móviles analizando la estructura del código y su modelo de ejecución.

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

RA 2: 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.

RA 3: 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).

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

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

RA 5: 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.

3.- Secuenciación y temporalización de las unidades didácticas.

El módulo tiene una duración de 120 horas y lo componen un total de 6 unidades didácticas, cada una con la siguiente denominación y carga horaria:

Unidad Didáctica	Denominación	Carga Horaria
UD 01	Fundamentos del desarrollo del software. Scripts en GNU/Linux	22
UD 02	Introducción a la puesta en producción segura. (GIT)	22
UD 03	Despliegue de software (Dockers).	24
UD 04	Determinación del nivel de seguridad requerido por las aplicaciones (OWASP).	24
UD 05	Detección y corrección de vulnerabilidades de aplicaciones web.	14
UD 06	Detección de problemas de seguridad en aplicaciones para dispositivos móviles.	14

La temporalización de las Unidades didácticas se realizará conforme a la siguiente tabla donde se indican los trimestres en los que se impartirán las mismas:

TRIMESTRE	UNIDADES
Primero	UD1 y UD2
Segundo	UD3 y UD4
Tercero	UD5 y UD6

4.- Contenidos.

Los contenidos básicos recogidos en la orden agrupados por las Unidades Didácticas anteriores quedarían de la siguiente forma:

Unidad Didáctica	Contenidos
1. Fundamentos del desarrollo del software. Scripts en GNU/Linux	<ul style="list-style-type: none">• Fundamentos de la programación.• Lenguajes de programación interpretados y compilados.• Código fuente y entornos de desarrollo.• Ejecución de software.• Elementos principales de los programas.• Pruebas. Tipos.• Seguridad en los lenguajes de programación y sus entornos de ejecución (“sandboxes”).
2. Introducción a la puesta en producción segura. (GIT)	<ul style="list-style-type: none">• Puesta segura en producción.• Prácticas unificadas para el desarrollo y operación del software (DevOps).• Sistemas de control de versiones.• Sistemas de automatización de construcción (build).• Integración continua y automatización de pruebas.
3. Despliegue de software (Dockers).	<ul style="list-style-type: none">• Escalado de servidores. Virtualización. Contenedores. Gestión automatizada de configuración de sistemas Herramientas de simulación de fallos.• Orquestación de contenedores.
4. Determinación del nivel de seguridad requerido por las aplicaciones (OWASP).	<ul style="list-style-type: none">• Fuentes abiertas para el desarrollo seguro.• Listas de riesgos de seguridad habituales: OWASP Top Ten (web y móvil).• Requisitos de verificación necesarios asociados al nivel de seguridad establecido• Comprobaciones de seguridad a nivel de aplicación: ASVS (Application Security Verification Standard).
5. Detección y corrección de vulnerabilidades de aplicaciones web.	<ul style="list-style-type: none">• Desarrollo seguro de aplicaciones web.• Listas públicas de vulnerabilidades de aplicaciones web.• OWASP Top Ten.• Entrada basada en formularios. Inyección. Validación de la entrada.• Estándares de autenticación y autorización.• Robo de sesión.• Vulnerabilidades web.• Almacenamiento seguro de contraseñas.• Contramedidas. HSTS, CSP, CAPTCHAs, entre otros.• Seguridad de portales y aplicativos webs. Soluciones WAF (Web Application Firewall).
6. Detección de problemas de seguridad en aplicaciones para dispositivos móviles.	<ul style="list-style-type: none">• Modelos de permisos en plataformas móviles. Llamadas al sistema protegidas.• Firma y verificación de aplicaciones.• Almacenamiento seguro de datos.• Validación de compras integradas en la aplicación.• Fuga de información en los ejecutables.

5.- Evaluación.

En este apartado se verá sobre **qué se va a evaluar**, en **qué momento**, los **instrumentos usados**, los **criterios de evaluación** así de saber **cómo** vamos a evaluar nuestra propia intervención docente y en particular la programación.

Las características se pueden encontrar en el **artículo 2** de la **orden 29 septiembre de 2010** de evaluación de Formación Profesional y (RD 1147/2011. Art.51)

- La evaluación de los aprendizajes del alumnado que cursa ciclos formativos **será continua** y se realizará por **módulos** profesionales.
- La aplicación del proceso de evaluación continua del alumnado requerirá, en la modalidad presencial, su **participación en las actividades** programadas para los distintos módulos profesionales del ciclo formativo.
- La evaluación del alumnado será realizada por el profesorado que imparta cada **módulo** profesional del ciclo formativo, de acuerdo con los **resultados de aprendizaje**, los **criterios de evaluación** y **contenidos de cada módulo** profesional, así como las competencias y objetivos generales del ciclo asociados a los mismos.

5.1. Evidencias: técnicas e instrumentos

Evidencias: técnicas e instrumentos de evaluación: Las técnicas e instrumentos propuestos para usar en los distintos resultados de aprendizaje son:

Se usarán una serie de instrumentos y técnicas ajustadas a los criterios de evaluación y a las características específicas del alumnado en **las unidades de trabajo (RA)**, destacando:

- Técnicas **escritas** cuyos instrumentos **son**:
 - Pruebas objetivas de **preguntas cortas**, textos incompletos, correspondencia, **test** de respuesta única, de verdadero o falso, de relacionar, de elección múltiple, etc. **Pruebas de desarrollo**
- **Técnicas de observación o Rúbricas, escalas de valoración, listas de control**
 - (cuaderno del profesor) **Observación directa** de trabajo diario de los alumnos/as en la realización de tareas, actividades y cuaderno. Participación, motivación, interés, etc. en las actividades programadas. ○ **Exposiciones** de temas, **debates**, **entrevista** con el profesorado, sistemas de preguntas, presentación de trabajos al grupo...
- **Técnica de ejecución práctica** ○ **casos prácticos**/actividades/tareas/supuestos
 - **Cuaderno de clase** (ejercicios, resúmenes, esquemas, **mapas conceptuales**, guiones.)
 - **Trabajos de investigación** ○ **Portfolio** digital en plataforma Moodle: técnica de recopilación de evidencias (ejercicios, problemas resueltos, mapas conceptuales, grabaciones, etc.) que permiten al alumnado demostrar el cumplimiento de los objetivos.

5.2. Ponderación Criterios de Evaluación

En las siguientes tablas se ponderan los criterios de evaluación asociados a cada uno de sus Resultados de Aprendizaje, aplicando para ellos las técnicas e instrumentos de evaluación explicadas con anterioridad, dependiendo de las circunstancias en cada caso:

RA1. Prueba aplicaciones web y aplicaciones para dispositivos móviles analizando la estructura del código y su modelo de ejecución. 14 %				
Criterios de Evaluación	%	UDs	INSTRUMENTO	Trimestre
a) Se han comparado diferentes lenguajes de programación de acuerdo a sus características principales.	20	1	Tareas y Actividades, Exposiciones, Prueba Escrita y/o Práctica, Observación Directa	1
b) Se han descrito los diferentes modelos de ejecución de software.	20	1		1
c) Se han reconocido los elementos básicos del código fuente, dándoles significado.	20	1		1
d) Se han ejecutado diferentes tipos de prueba de software.	20	1		1
e) Se han evaluado los lenguajes de programación de acuerdo a la infraestructura de seguridad que proporcionan.	20	1		1

RA2. Determina el nivel de seguridad requerido por aplicaciones identificando los vectores de ataque habituales y sus riesgos asociados. 14%

Criterios de Evaluación	%	UDs	INSTRUMENTO	Trimestre
a) Se han caracterizado los niveles de verificación de seguridad en aplicaciones establecidos por los estándares internacionales (ASVS, "Application Security Verification Standard").	25	4	Tareas y Actividades, Exposiciones, Prueba Escrita y/o Práctica, Observación Directa	2
b) Se ha identificado el nivel de verificación de seguridad requerido por las aplicaciones en función de sus riesgos de acuerdo con los estándares reconocidos.	25	4		2
c) Se han enumerado los requisitos de verificación necesarios asociados al nivel de seguridad establecido.	25	4		2
d) Se han reconocido los principales riesgos de las aplicaciones desarrolladas, en función de sus características.	25	4		2

RA3. Detecta y corrige vulnerabilidades de aplicaciones web analizando su código fuente y configurando servidores web. 24%

Criterios de Evaluación	%	UDs	INSTRUMENTO	Trimestre
a) Se han validado las entradas de los usuarios.	14,3	5	Tareas y Actividades, Exposiciones, Prueba Escrita y/o Práctica, Observación Directa	3
b) Se han detectado riesgos de inyección tanto en el servidor como en el cliente.	14,3	5		3
c) Se ha gestionado correctamente la sesión del usuario durante el uso de la aplicación.	14,3	5		3
d) Se ha hecho uso de roles para el control de acceso.	14,3	5		3
e) Se han utilizado algoritmos criptográficos seguros para almacenar las contraseñas de usuario.	14,3	5		3
f) Se han configurado servidores web para reducir el riesgo de sufrir ataques conocidos.	14,3	5		3
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).	14,3	5		3

RA4. Detecta problemas de seguridad en aplicaciones para dispositivos móviles, monitorizando su ejecución y analizando ficheros y datos. 24%

Criterios de Evaluación	%	UDs	INSTRUMENTO	Trimestre
a) Se han comparado los diferentes modelos de permisos de las plataformas móviles	20	6	Tareas y Actividades, Exposiciones, Prueba Escrita y/o Práctica, Observación Directa	3
b) Se han descrito técnicas de almacenamiento seguro de datos en los dispositivos, para evitar la fuga de información.	20	6		3
c) Se ha implantado un sistema de validación de compras integradas en la aplicación haciendo uso de validación en el servidor.	20	6		3
d) Se han utilizado herramientas de monitorización de tráfico de red para detectar el uso de protocolos inseguros de comunicación de las aplicaciones móviles.	20	6		3
e) Se han inspeccionado binarios de aplicaciones móviles para buscar fugas de información sensible.	20	6		3

RA5. Implanta sistemas seguros de despliegado de software, utilizando herramientas para la automatización de la construcción de sus elementos. 24%

Criterios de Evaluación	%	UDs	INSTRUMENTO	Trimestre
a) Se han identificado las características, principios y objetivos de la integración del desarrollo y operación del software.	14,3	2	Tareas y Actividades, Exposiciones, Prueba Escrita y/o Práctica, Observación Directa	1
b) Se han implantado sistemas de control de versiones, administrando los roles y los permisos solicitados.	14,3	2		1
c) Se han instalado, configurado y verificado sistemas de integración continua, conectándolos con sistemas de control de versiones.	14,3	2		1
d) Se han planificado, implementado y automatizado planes de despliegado de software.	14,3	3		2
e) Se ha evaluado la capacidad del sistema desplegado para reaccionar de forma automática a fallos.	14,3	3		2
f) Se han documentado las tareas realizadas y los procedimientos a seguir para la recuperación ante desastres.	14,3	3		2
g) Se han creado bucles de retroalimentación ágiles entre los miembros del equipo.	14,3	3		2

5.3. Evaluación inicial

La evaluación inicial o diagnóstica, es de vital importancia ya que nos va a proporcionar información sobre la situación de partida del alumnado del módulo. Para poder realizar dicha evaluación se usará como instrumento una prueba objetiva de preguntas cortas relacionada con los contenidos más generales del módulo.

Una vez analizados los resultados, podemos obtener información referente a posibles carencias o ciertas dificultades del alumnado.

También, al comenzar cada unidad de trabajo, se realizará una actividad de iniciación para conocer los conocimientos de partida del alumnado sobre aspectos específicos de la unidad

5.4. Criterios de calificación

Según la orden 29 de septiembre 2010 artículo 16, la evaluación conllevará una calificación que reflejará los resultados obtenidos por el alumno o alumna en su proceso de enseñanza-aprendizaje. La calificación de los módulos profesionales de formación en el centro educativo y del módulo profesional de proyecto se expresará en valores numéricos de 1 a 10, sin decimales. Se considerarán positivas las iguales o superiores a 5 y negativas las restantes.

En la evaluación del proceso de Enseñanza/Aprendizaje, para valorar el progreso del alumnado, evaluaremos las distintas actividades de las unidades didácticas, utilizando para ello alguno de los instrumentos de evaluación establecidos.

Tomando como referencia los **CRITERIOS DE EVALUACIÓN** y los objetivos del módulo, se tendrá que obtener una **CALIFICACIÓN** en los siguientes momentos del curso académico

- **A la finalización de las evaluaciones (primera, segunda)**
- **Al finalizar el curso académico.**

5.4.1.- Calificación de cada unidad

Cada una de las **unidades** corresponde con **un resultado de aprendizaje (RA)**, por lo que la calificación de una unidad será la calificación del RA asociado.

Hay que tener en cuenta que los **criterios de evaluación** relacionados a los **RA** están ponderados de manera global al módulo. Para que el alumno vea en cada unidad una calificación de 1 a 10 se realizará la ponderación oportuna.

Para comprobar si cada **criterio de evaluación** es superado, se emplearán **los instrumentos** mencionados con anterioridad. Cada criterio de evaluación se considerará **evaluado** positivamente cuando la calificación obtenida sea **de 5 puntos o superior. Se considera un RA superado si se obtiene una nota mayor o igual a 5**

Si se emplean diferentes **técnicas (evidencias e instrumentos)** asociadas al **mismo resultado de aprendizaje**, se tomará como nota, la siguiente

- **Técnicas escritas (TE)**: valdrán el 60% del RA y en caso de realizar varias en un mismo resultado se realizará la media de las mismas
- **Técnica de ejecución práctica (TEP)**: valdrán el 30% del RA y en caso de realizar varias en un mismo resultado se realizará la media de las mismas
- **Técnicas de observación (TO)**: valdrán el 10% del RA y en caso de realizar varias en un mismo resultado se realizará la media de las mismas
- Nota: si para un RA o unidad solo se aplica una de las técnicas, ésta tendrá el valor del 100%. Si hay varios instrumentos se realizará la media aritmética de los mismas.

Para aplicar la ponderación anterior indicada, es obligatorio para el alumnado **realizar la entrega de todas las actividades prácticas de carácter obligatorio requeridas**.

Calificación final del RA o unidad = Media aritmética de las tareas TE + TEP + TO.

Aspectos a tener en cuenta en la entrega de tareas

Las actividades prácticas deberán ser entregadas en el **plazo** indicado por el profesor. No se aceptarán prácticas fuera de plazo. Por ello, se habilitará al final de la evaluación un periodo para la entrega de todas las actividades y practicas pendientes.

Si se detecta que un **alumno copia de un compañero**, su nota automáticamente pasará a ser un 1. Si se detecta que ha habido varios alumnos implicados en la copia, todos ellos tendrán 1 en la calificación. Se aplicará también la nota de 1 si se detecta que un alumno realiza una prueba con materiales no permitidos.

5.4.2.- Calificación de cada evaluación

En cada una de las evaluaciones parciales, se tendrán en cuenta los RA que se han visto en cada una de ellas. Para ello, utilizaremos el **peso** que tiene cada **RA** dentro del módulo completo para ajustarlo a cada una de las evaluaciones. El peso de cada **RA** se observa en la siguiente tabla. Se han obtenido mediante los pesos de cada uno de sus criterios de evaluación asociados

Resultados de aprendizaje	Peso
RA1: Prueba aplicaciones web y aplicaciones para dispositivos móviles analizando la estructura del código y su modelo de ejecución.	14%
RA 2: Determina el nivel de seguridad requerido por aplicaciones identificando los vectores de ataque habituales y sus riesgos asociados.	14%
RA 3: Detecta y corrige vulnerabilidades de aplicaciones web analizando su código fuente y configurando servidores web.	24%
RA 4: Detecta problemas de seguridad en las aplicaciones para dispositivos móviles, monitorizando su ejecución y analizando ficheros y datos.	24%
RA 5: Implanta sistemas seguros de despliegado de software, utilizando herramientas para la automatización de la construcción de sus elementos.	24%
Total	100%

Para realizar el cálculo de las calificaciones parciales de cada evaluación se tomará como **100%** el total de RA impartidos hasta el momento en cada evaluación, aplicando los porcentajes sobre ese total.

Nota: Si alguno de los RA impartidos no ha sido adquirido por el alumno en el momento de la calificación parcial, su calificación será inferior a 5 puntos.

Calificaciones por evaluaciones

La calificación de cada evaluación se realizará la media ponderada de todos los criterios de evaluación de los resultados de aprendizaje de las unidades que componen el trimestre.

Se tendrán 2 evaluaciones parciales (Primer y Segundo Trimestre) y 2 evaluaciones Finales:

- En mayo, donde se obtendrá la nota final de los aprobados y suspensos.
- En junio, donde se podrán recuperar los criterios de evaluación no superados, y si el alumnado quiere subir la nota final.

5.4.3.- Criterios de evaluación de la expresión escrita

Tal y como se establece en el Proyecto Educativo de Centro, los aspectos formales de la expresión escrita serán objeto de valoración por parte de todos los departamentos didácticos en las diferentes pruebas que realice el alumnado.

La correcta entrega de la tarea deberá cumplir los siguientes términos:

- Redacción: estructura con párrafos, conectores, oraciones completas, puntuación (comas y puntos), concordancias. El máximo de penalización será de -0,25. Este criterio se denominará como CEEE1.
- Ortografía: faltas ortográficas (grafías y uso de mayúsculas) y del uso de las tildes. El máximo de penalización será de -0,75. Este criterio se denominará como CEEE2.

Estos criterios se valorarán con un 10% sobre la nota obtenida en cada uno de los instrumentos de evaluación utilizados.

5.4.4.- Calificación final

Para el cálculo de la calificación final se **ponderará la calificación obtenida en cada Resultado de Aprendizaje RA** y se le aplicará el **peso asignado a dicho resultado de aprendizaje sobre el total del módulo**, según la tabla expuesta con anterioridad

Para poder **superar el módulo profesional** de forma ordinaria, es necesario que el alumno/a obtenga una calificación **final igual o superior a 5** en cada uno de los **resultados de aprendizaje**.

5.5. Evaluación extraordinaria

En el caso de que el alumno no supere **una unidad o RA** podrá recuperarla los primeros días de la evaluación siguiente, excepto en el periodo de recuperación (a partir del 20 de mayo). Es necesario que entregue todas las tareas pendientes y se utilizarán diferentes técnicas e instrumentos.

En el caso en que el/la alumno/a no supere el **módulo por evaluaciones**, tiene la posibilidad de recuperar las evaluaciones pendientes en la convocatoria **ordinaria de junio**. Este plan de recuperación será elaborado por el profesor/a atendiendo a las circunstancias de cada alumno/a. Para poder realizar esta prueba es necesario haber presentado todos los ejercicios solicitados por el profesor a lo largo del curso, organizándole actividades de refuerzo hasta la evaluación final (3 semanas aproximadamente).

Respecto a la mejora de la calificación: el alumnado que quiera mejorar su calificación, deberá hacerlo en el periodo establecido junto con las recuperaciones finales de junio. Se deberá diseñar uno o varios instrumentos de evaluación que contemplen todos los criterios de evaluación de los RA presentes en el módulo profesional.

5.6. Periodo entre la 3ª evaluación parcial y la evaluación final:

Se realizarán las mismas prácticas que el alumnado no haya realizado y también se apoyará el aprendizaje de los mismos resolviendo las dudas y problemas que éstos puedan presentar. En caso de que hayan realizado las prácticas, se propondrán nuevas prácticas.

El profesor establecerá un calendario personalizado para cada alumno indicando las fechas límite de entrega de las prácticas pendientes y exámenes a desarrollar.

Se aplicará el mismo porcentaje a cada uno de los criterios y resultados de aprendizaje que en las evaluaciones ordinarias

6.- Metodología y materiales didácticos.

A lo largo de todo el curso y para cada una de las unidades didácticas, se procederá de la siguiente forma:

- Utilizaremos el aprendizaje significativo.
- Se hará el módulo muy práctico.
- Se darán explicaciones teóricas sobre los temas necesarios.
- Se presentarán actividades prácticas.
- Se darán guías para la elaboración de prácticas.

La metodología tendrá un carácter fundamentalmente activo, motivador y participativo, partirá de los intereses del alumnado, favorecerá el trabajo individual, cooperativo y el **APRENDIZAJE SIGNIFICATIVO**, e integrará en todas las áreas referencias a la vida cotidiana y al entorno inmediato.

6.1. Agrupamientos

Uno de los recursos que permite aportar diversidad en la forma de trabajar en el aula es el agrupamiento de los estudiantes, lo que permite que interactúen de forma **diferente y con compañeros distintos**.

Así, es probable que ofrezcamos a todos los estudiantes la oportunidad de trabajar y participar según sus preferencias, intereses y potencial: escuchar, hablar ante un grupo grande, hablar en grupo pequeño, hacer las tareas personales, trabajar con un amigo o con un grupo de compañeros.

En los grupos pequeños y medianos es donde mejor se consigue el **APRENDIZAJE COOPERATIVO** (resulta verdaderamente efectivo para trabajar la ayuda mutua entre compañeros y fomentar así la inclusión de todos los alumnos de un mismo grupo clase)

El modo de trabajo será individual pero colaborativo entre el alumnado. Es decir, las prácticas se deberán realizar y entregar individualmente, pero el alumnado tiene la posibilidad de resolver dudas, evidentemente, con el docente, pero también pueden colaborar entre ellos.

Si las circunstancias lo permiten se **realizarán trabajos en pareja, pequeños grupos o grupo clase**.

Algunas reglas para trabajar en grupos son:

- Identificar los puntos fuertes o especialidades de cada componente del grupo.
- Definir los objetivos o tarea final a lograr entre todo el grupo.
- Determinar el tiempo de trabajo y hacer una planificación temporal.
- Establecer claramente las reglas y organización del grupo.
- Establecer la forma de trabajo como equipo dentro de cada grupo.
- Distribuir las responsabilidades individuales de cada miembro del grupo.

6.2. Tipos de tareas

Entre los tipos de actividades a realizar destacamos:

- **De introducción.** Saber los conocimientos previos. (coloquios, vídeos, etc.)
- **Interdisciplinares.** Trabajar al mismo tiempo con otros módulos.
- **Debate.** Poner un tema de discusión para defender diferentes puntos de vista.
- **De síntesis.** Realizar resúmenes o mapas conceptuales de la unidad.
- **De desarrollo.** Consisten en el desarrollo de los contenidos de una unidad.
- **De motivación.** Se intenta despertar el interés del alumno.
- **De indagación.** investigar para completar los contenidos (búsquedas, lecturas, etc.)
- **De ampliación y refuerzo.** Ampliar o repasar criterios de evaluación • **Teórico práctico.** Se mezclan parte de teoría como de práctica de un módulo.
- **De autoevaluación.** conocer si se están alcanzando los objetivos propuestos.
- **De consolidación.** Se comprueba que se han conseguido los objetivos propuestos: repasos, exposiciones, resúmenes, trípticos o mapas mentales, etc.
- **De gamificación:** uso de herramientas, motivándolos e implicándolos con unos retos a superar, obteniendo unos logros o recompensas (puntos, clasificación, insignias)

6.3. Recursos y materiales

Los recursos usados en la metodología son muy diversos, agrupando en tres los más usados, siendo los tecnológicos/electrónicos motivadores para el alumnado.



- Ordenadores con GNU/Linux como sistema anfitrión.
- Sistemas operativos y software necesario (en el caso de software propietario trabajaremos con las demos de los sistemas operativos).
- Acceso a internet, Plataforma Moodle, Proyector multimedia.
- Pizarra.
- Manuales y libros de ciberseguridad en internet.

6.4. Utilización del aula Virtual como apoyo a la docencia reglada

A lo largo del curso se utilizará el Aula Virtual como apoyo a la docencia reglada. Se fomentará un mayor uso conforme el alumnado vaya promocionando de curso. En general, su utilización responderá a las siguientes pautas:

- Se definirá la estructura del curso en unidades, temas, secciones, etc.
- Se procurará que el desarrollo de los contenidos del curso esté disponible en el Aula Virtual, sobre todo en los niveles en los que no se disponga de un libro de texto o materiales de referencia.
- Se proporcionarán recursos educativos para el tratamiento de los contenidos programados (documentos explicativos, materiales audiovisuales, cuestionarios, actividades resueltas, recursos de refuerzo y de ampliación, modelos de pruebas, etc.).
- Se podrán establecer tareas y otras actividades de evaluación cuya entrega quede registrada en el Aula Virtual.

7.- Atención a la diversidad

La atención a la diversidad, debe estar presente en todo el proceso de aprendizaje, y debe servir al profesor para:

- Comprobar los conocimientos previos de los alumnos al comienzo de cada tema. Cuando se detecte alguna laguna en los conocimientos de determinados alumnos, deben proponerse actividades destinadas a subsanar.
- Procurar que los contenidos nuevos conecten con los conocimientos previos de la clase y que sean adecuados a su nivel cognitivo. En este punto es del máximo valor la actuación del profesor, la persona más capacitada para servir de puente entre los contenidos y los alumnos, y el mejor conocedor de las capacidades de su clase.
- Propiciar que el ritmo de aprendizaje sea marcado por el propio alumno. Es evidente que, con los amplios programas de las materias es difícil impartir los contenidos mínimos dedicando a cada uno el tiempo necesario. Pero hay que llegar a un equilibrio que garantice un ritmo no excesivo para el alumno y suficiente para la extensión de la materia.
- Los contenidos de cada tema se presentarán de la forma más categorizada y organizada posible, sin violentar la orientación disciplinar ni alterar la lógica de la materia.
- Las actividades serán abundantes y su grado de complejidad, variable. La selección, realizada por el profesor, de estas actividades permite atender a las diferencias individuales en el alumnado.

En los casos de absoluta desmotivación del alumno se aplicarán adaptaciones curriculares con el fin de conocer lo que el alumno busca y a partir de ahí conseguir que tenga experiencias de triunfo mediante prácticas o ejercicios complementarios más adecuados a su nivel e intereses. En estos casos nunca se perderán de vista los contenidos mínimos que marca la legislación en este sentido.

Si el alumno presenta dificultades en la asimilación de los contenidos se intercalan actividades de refuerzo y se le prestará un seguimiento especial.

8.- Materiales y recursos didácticos

El aprendizaje significativo ha de ser eminentemente activo, por lo que el profesor utilizará material didáctico diverso:

1. Aula Virtual de la Junta de Andalucía Moodle Centro.
 - Libro de texto recomendado (no obligatorio) para los alumnos será: Puesta en producción segura (MÁXIMO FERNÁNDEZ RIERA). Editorial RA-MA, con abundantes recursos web y documentación en formato digital. El libro no será obligatorio porque el profesor dejará en el aula virtual del módulo todos los apuntes y recursos necesarios.
2. Material audiovisual (por ejemplo, con procedimientos/minitutoriales/conferencias grabados en soporte digital: .avi,.mov,.mp3,.wav etc.) que se proyectará al igual que el tutorial seleccionado como base para la exposición de las clases mediante un cañón conectado a un ordenador. En su defecto se podrá utilizar el VNC (disponible tanto en Windows como en Linux) o cualquier programa de gestión remota de escritorio para que todos los alumnos desde sus propios puestos puedan ver la pantalla del equipo donde actúa el profesor.
3. Fotocopias de apuntes elaborados por el Departamento.
4. Catálogos comerciales y revistas especializadas del sector.

El aula está equipada con el siguiente material informático:

- 11 ordenadores portátiles Pentium Core i3 equipados con 24GB de RAM, disco duro de 1 TB M.2 SSD.
- Conexión por Wi-Fi a la red Andared del centro.
- Un cañón para proyectar la imagen de cualquier ordenador.
- El software básico está compuesto Ubuntu 21.04 con KDE Plasma y diferente software ofimático y de virtualización (VirtualBox).

9.- Bibliografía

En este apartado podríamos distinguir la que debe residir en el aula y la que es propia del departamento, pero, en este caso, considero innecesaria esta distinción ya que cualquiera de estos libros debería estar disponible tanto para profesores como alumnos como material de consulta y ampliación.

- Puesta en producción segura (MÁXIMO FERNÁNDEZ RIERA). Editorial RA-MA
- Desarrollo seguro en ingeniería del software. Aplicaciones seguras con Android, NodeJS, Python y C++ (José Manuel Ortega Candel). Editorial Marcombo
- Aprender Docker, un enfoque práctico (José Juan Sánchez Hernández). Editorial Marcombo.