PROGRAMACIÓN DIDÁCTICA DEL MÓDULO

Bastionado de redes y sistemas

Curso de experto en Ciberseguridad en entornos de las tecnologías de la información

Curso 2023/2024

Arturo José Puentes Castellanos

Modalidad: **presencial**
Turno: **tarde**
IES Aguadulce
Aguadulce (Almería)

UNIÓN EUROPEA
Fondo Social Europeo
El FSE invierte en tu futuro

Contenido

1. Introducción

El presente documento plasma la programación didáctica (objetivos, contenidos, criterios de evaluación, planificación, etc.) del módulo de **Bastionado de Redes y Sistemas** (BRS), incluido entre las enseñanzas del **Curso de Especialización en Ciberseguridad en Entornos de las Tecnologías de la Información**. Las **características generales** del curso son:

CARACTERÍSTICAS GENERALES DEL **CURSO**	
Denominación:	Curso de Especialización en Ciberseguridad en Entornos de las Tecnologías de la Información
Fecha de comienzo:	29/09/2023
Fecha de finalización:	20/05/2024
Duración:	720 horas
Familia profesional:	Informática y Comunicaciones
Modalidad:	Presencial
Turno:	Tarde
CARACTERÍSTICAS ESPECÍFICAS DEL **MÓDULO BRS**	
Horas totales:	150
Horas por semana:	5
Semanas:	30

El presente curso está enfocado al alumnado que está en posesión de un título de **Formación Profesional de Grado Superior** de la familia profesional de **Informática y Comunicaciones**, ya que puede proporcionar una formación adicional que mejore sus competencias para acceder al mercado laboral, además de introducirle en esta rama profesional en pleno auge.

2. Marco legal.

El diseño de esta planificación docente se ha hecho atendiendo a la jerarquía normativa, desde la que abarca el ámbito nacional, su contextualización en nuestra comunidad autonómica y, por último, la que se establece en el centro y se plasma en el Proyecto Educativo de Centro (PEC). Así, la normativa específica a la que obedece el diseño de esta programación es:

- Ámbito nacional:

- **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.
- **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.**
- **Real Decreto 1147/2011**, de 29 de julio, por el que se establece la ordenación general de la formación profesional del sistema educativo.

- Ámbito autonómico:
  - **Resolución de 9 de septiembre de 2022**, de la Dirección General de Formación Profesional de la Consejería de Desarrollo Educativo y Formación Profesional de la Junta de Andalucía, por la que se establecen aspectos organizativos de los cursos de especialización de Formación Profesional para el curso escolar **2022-2023**.

    En ella se establece el **calendario escolar** del curso y la carga lectiva en horas de cada uno de sus módulos, así como la forma de evaluación, entre otros aspectos que se describen en el presente documento.
  - **Orden de 29 de septiembre de 2010**, por la que se regula la evaluación, certificación, acreditación y titulación académica del alumnado que cursa enseñanzas de formación profesional inicial que forma parte del sistema educativo en la Comunidad Autónoma de Andalucía.

- Ámbito de centro:
  - **Proyecto Educativo de Centro** del IES Aguadulce.

El Real Decreto 1147/2011, de 29 de julio, dispone en su artículo 27 los aspectos generales referentes a los cursos de especialización de formación profesional. Estos aspectos se especifican para este curso en el Real Decreto 479/2020, de 7 de abril, donde se establecen los resultados aprendizaje y sus respectivos criterios de evaluación para el presente curso.

3. Contexto.

El grupo clase está formado por 11 **estudiantes**, 10 chicos y 1 chica. Partiendo de los resultados obtenidos en la evaluación inicial, podemos afirmar que el nivel de conocimientos relacionados con el módulo es medio-bajo. No se distinguen diferencias significativas entre el alumnado, conformando un grupo más o menos homogéneo, aunque de procedencias diferentes. La mitad provienen de ASIR y la otra mitad de ciclos de desarrollo DAW/DAM.

El nivel de conocimientos de sus respectivos títulos es el normal, al igual que el ritmo de aprendizaje que demuestran. Además, demuestran un alto nivel de motivación e interés por la materia, según se ha podido observar tras las primeras semanas de clase.

Ninguno tiene experiencia laboral en el sector relacionado con sus estudios.

En definitiva y según lo observado en el aula, el grupo clase es **homogéneo** y demuestra una actitud **participativa** y **colaborativa**.

4. Competencias y objetivos.

Las competencias y objetivos son elementos a alcanzar por el alumnado que cursa los estudios del presente curso. Ambos vienen recogidos en el RD 479/2020, de 7 de abril, tal y como se indican a continuación.

4.1. Competencias.

4.1.1. Competencia general del curso.

El Real Decreto 479/2020, en su artículo 3, indica que el perfil profesional de este curso de especialización queda determinado por su competencia general y sus competencias profesionales, personales y sociales. El artículo 4 dicta que la **competencia general** de este curso de especialización consiste en:

"*Definir e implementar estrategias de seguridad en los sistemas de información realizando diagnósticos de ciberseguridad, identificando vulnerabilidades e implementando las medidas necesarias para mitigarlas aplicando la normativa vigente y estándares del sector, siguiendo los protocolos de calidad, de prevención de riesgos laborales y respeto ambiental.*"

4.1.2. Competencias profesionales, personales y sociales.

El artículo 5 del mismo Real Decreto enumera, para este curso, las siguientes competencias profesionales, personales y sociales (CPPS):

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

b) Detectar e investigar incidentes de ciberseguridad, documentándolos e incluyéndolos en los planes de securización de la organización.

c) Diseñar planes de securización contemplando las mejores prácticas para el bastionado de sistemas y redes.

d) Configurar sistemas de control de acceso y autenticación en sistemas informáticos, cumpliendo los requisitos de seguridad y minimizando las posibilidades de exposición a ataques.

e) Diseñar y administrar sistemas informáticos en red y aplicar las polV≠ticas de seguridad establecidas, garantizando la funcionalidad requerida con un nivel de riesgo controlado.

f) Analizar el nivel de seguridad requerido por las aplicaciones y los vectores de ataque más habituales, evitando incidentes de ciberseguridad.

g) Implantar sistemas seguros de desplegado de software con la adecuada coordinación entre los desarrolladores y los responsables de la operación del software.

h) Realizar análisis forenses informáticos analizando y registrando la información relevante relacionada.

i) Detectar vulnerabilidades en sistemas, redes y aplicaciones, evaluando los riesgos asociados.

j) Definir y aplicar procedimientos para el cumplimiento normativo en materia de ciberseguridad y de protección de datos personales, implementándolos tanto internamente como en relación con terceros.

k) Elaborar documentación técnica y administrativa cumpliendo con la legislación vigente, respondiendo a los requisitos establecidos.

l) Adaptarse a las nuevas situaciones laborales, manteniendo actualizados los conocimientos científicos, técnicos y tecnológicos relativos a su entorno profesional, gestionando su formación y los recursos existentes en el aprendizaje a lo largo de la vida.

m) Resolver situaciones, problemas o contingencias con iniciativa y autonomía en el ámbito de su competencia, con creatividad, innovación y espíritu de mejora en el trabajo personal y en el de los miembros del equipo.

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

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

4.2. Objetivos.

El RD 479/2020, de 7 de abril, establece para este curso los objetivos que se indican en los siguientes apartados.

4.2.1. Objetivos generales del curso.

Según el artículo 8 del RD 479/2020, de 7 de abril, los objetivos generales del curso son:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

4.2.2. Objetivos específicos del módulo.

La formación en el módulo de **Bastionado de Redes y Sistemas (BRS)** contribuye a alcanzar aquellos objetivos generales resaltados en negrita, que son: **e, f, g, h, i, j, q, r, s, t, u** y **v**. Además, ayuda en la adquisición de las competencias **c, d, e, k, l, m, n** y **ñ**.

Para la consecución de dichos objetivos, el proceso de enseñanza seguirá las líneas de actuación relacionadas con:

- El diseño de planes de securización de la organización.
- El diseño de redes de computadores.
- La administración de los sistemas de control de acceso.

5. Resultados de aprendizaje y criterios de evaluación.

Los resultados de aprendizaje (RA) que se pretenden alcanzar con las enseñanzas de este módulo profesional (BRS) vienen expresados como **resultados de aprendizaje** (RA) en el RD 479/2020, de 7 de abril, junto a los criterios para su evaluación. Así, cada RA dispone de sus respectivos criterios de evaluación de la forma siguiente:

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

Criterios de evaluación:

a) Se han identificado los activos, las amenazas y vulnerabilidades de la organización.

b) Se ha evaluado las medidas de seguridad actuales.

c) Se ha elaborado un análisis de riesgo de la situación actual en ciberseguridad de la organización

d) Se ha priorizado las medidas técnicas de seguridad a implantar en la organización teniendo también en cuenta los principios de la Economía Circular.

e) 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.

f) 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.

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

Criterios de evaluación:

a) Se han definido los mecanismos de autenticación en base a distintos / múltiples factores (físicos, inherentes y basados en el conocimiento), existentes.

b) Se han definido protocolos y políticas de autenticación basados en contraseñas y frases de paso, en base a las principales vulnerabilidades y tipos de ataques.

c) Se han definido protocolos y políticas de autenticación basados en certificados digitales y tarjetas inteligentes, en base a las principales vulnerabilidades y tipos de ataques.

d) Se han definido protocolos y políticas de autenticación basados en tokens, OTPs, etc., en base a las principales vulnerabilidades y tipos de ataques.

e) Se han definido protocolos y políticas de autenticación basados en características biométricas, según las principales vulnerabilidades y tipos de ataques.

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

a) Se han identificado los tipos de credenciales más utilizados.

b) Se han generado y utilizado diferentes certificados digitales como medio de acceso a un servidor remoto.

c) Se ha comprobado la validez y la autenticidad de un certificado digital de un servicio web.

d) Se han comparado certificados digitales válidos e inválidos por diferentes motivos.

e) Se ha instalado y configurado un servidor seguro para la administración de credenciales (tipo RADIUS - *Remote Access Dial In User Service*).

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

a) Se ha incrementado el nivel de seguridad de una red local plana segmentándola físicamente y utilizando técnicas y dispositivos de enrutamiento.

b) Se ha optimizado una red local plana utilizando técnicas de segmentación lógica (VLANs).

c) Se ha adaptado un segmento de una red local ya operativa utilizando técnicas de subnetting para incrementar su segmentación respetando los direccionamientos existentes.

d) Se han configurado las medidas de seguridad adecuadas en los dispositivos que dan acceso a una red inalámbrica (*routers*, puntos de acceso, etc.).

e) Se ha establecido un túnel seguro de comunicaciones entre dos sedes geográficamente separadas.

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

a) Se han configurado dispositivos de seguridad perimetral acorde a una serie de requisitos de seguridad.

b) Se han detectado errores de configuración de dispositivos de red mediante el análisis de tráfico.

c) Se han identificado comportamientos no deseados en una red a través del análisis de los registros (Logs), de un cortafuego.

d) Se han implementado contramedidas frente a comportamientos no deseados en una red.

e) Se han caracterizado, instalado y configurado diferentes herramientas de monitorización.

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

a) Se ha configurado la BIOS para incrementar la seguridad del dispositivo y su contenido minimizando las probabilidades de exposición a ataques.

b) Se ha preparado un sistema informático para su primera instalación teniendo en cuenta las medidas de seguridad necesarias.

c) Se ha configurado un sistema informático para que un actor malicioso no pueda alterar la secuencia de arranque con fines de acceso ilegítimo.

d) Se ha instalado un sistema informático utilizando sus capacidades de cifrado del sistema de ficheros para evitar la extracción física de datos.

e) Se ha particionado el sistema de ficheros del sistema informático para minimizar riesgos de seguridad.

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

a) Se han enumerado y eliminado los programas, servicios y protocolos innecesarios que hayan sido instalados por defecto en el sistema.

b) Se han configurado las características propias del sistema informático para imposibilitar el acceso ilegítimo mediante técnicas de explotación de procesos.

c) Se ha incrementado la seguridad del sistema de administración remoto SSH y otros.

d) Se ha instalado y configurado un Sistema de detección de intrusos en un Host (HIDS) en el sistema informático.

e) Se han instalado y configurado sistemas de copias de seguridad.

6. Contenidos.

6.1. Contenidos básicos.

Los contenidos propuestos para lograr los resultados de aprendizaje indicados en el apartado anterior se expresan como **contenidos básicos** en el RD 479/2020, de 7 de abril:

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.

Configuración de sistemas de control de acceso y autenticación de personas:

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

Administración de credenciales de acceso a sistemas informáticos:

- Gestión de credenciales.
- Infraestucturas 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.

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.).

Configuración de dispositivos y sistemas informáticos:

- Seguridad perimetral. Firewalls de Próxima Generación.
- Seguridad de portales y aplicativos web. Soluciones WAF (Web Aplication 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 SOCs.

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.

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.

6.2. Unidades didácticas.

Cada uno de los bloques de contenidos básicos que se han desglosado en el apartado anterior se tomará como **unidad didáctica** (UD) y los contenidos de cada UD se corresponderán con los contenidos básicos de cada una de ella. Así, las UD para el presente curso son:

- UD1. Diseño de planes de securización.
- UD2. Configuración de sistemas de control de acceso y autenticación de personas.
- UD3. Administración de credenciales de acceso a sistemas informáticos.
- UD4. Diseño de redes de computadores seguras.
- UD5. Configuración de dispositivos y sistemas informáticos.
- UD6. Configuración de dispositivos para la instalación de sistemas informáticos.
- UD7. Configuración de los sistemas informáticos.

En el siguiente apartado se explica la planificación temporal de las UD y la relación de cada una de ellas con su respectivo RA.

6.3. Temporalización.

La carga lectiva del curso se extiende a **30 semanas** de clase, desde el 30-09-2022 hasta el 21-05-2023. Como se indicaba en la **introducción**, la duración total del módulo es de **150 horas**, a impartir en **tres evaluaciones**, y con una carga semanal de **5 horas**. Así, la planificación temporal aproximada propuesta para este curso es:

Resultados de aprendizaje	Unidad didáctica	Duración	Evaluación parcial
RA1	UD1	8	1er trimestre
RA2	UD2	8	
RA3	UD3	14	
RA4	UD4	11	2º trimestre
RA5	UD5	24	
RA6	UD6	8	3er trimestre
RA7	UD7	22	
Total		**95**	

A partir de **21-05-2023**, el alumnado que no haya superado alguno de los módulos deberá ceñirse a los establecido en el **apartado de evaluación** del presente documento.

7. Evaluación

En lo referente a la evaluación, la Resolución de 9 de septiembre de 2022 establece en su apartado "**Sexto. Evaluación del alumnado**" (en adelante **apdo. 6º**) los siguientes puntos:

- **Punto 1**. El alumnado dispondrá de **dos convocatorias finales** por curso escolar, para cada uno de los módulos profesionales, a excepción del módulo profesional de Formación en Centros de Trabajo en el que dispondrá de una convocatoria final.
- **Punto 2**. El alumnado de cursos de especialización que, tras la primera evaluación final, **tenga módulos profesionales no superados**, tendrá **obligación de asistir a clases** y continuar con las actividades lectivas hasta la fecha de finalización del régimen ordinario de clase que no será anterior al día **22 de junio de 2023**.
- **Punto 4**. Cuando el régimen ordinario de clases sea superior a 400 horas, se realizarán **dos evaluaciones parciales** y **dos evaluaciones finales**.
- **Punto 6**. En aquellos cursos de especialización que no contengan el módulo profesional de Formación en Centros de Trabajo se realizará **una convocatoria final a la finalización del régimen ordinario de clases**.

  La **segunda evaluación final se realizará antes del 30 de junio**, fecha de finalización del curso escolar.
- **Punto 7**. La obtención del Certificado que acredita la superación del curso de especialización requiere tener calificación positiva en todos los módulos profesionales y se certifica mediante el Anexo III de la presente Resolución.

Por otra parte, el apartado "**Octavo. Normativa supletoria**" (en adelante **apdo. 8º**) aclara que todos los aspectos relativos a ordenación curricular y a la evaluación no recogidos en esta Resolución **se regirán por las normas que con carácter general regulan las enseñanzas de formación profesional del sistema educativo**.

7.1. Criterios, estrategias y procedimientos de evaluación.

La evaluación, en sus diversas vertientes, constituye un análisis de los factores y elementos que intervienen en el proceso educativo, valorando su adecuación y eficacia. En función del momento en que se realice, se pueden distinguir los siguientes tipos:

a) **Evaluación inicial**. Se realiza antes de comenzar el proceso de enseñanza-aprendizaje para diagnosticar el punto de partida del nivel de conocimientos y destrezas del alumnado, así como las posibles dificultades de aprendizaje que puedan presentar.

b) **Evaluación formativa**. Será una evaluación continua, haciendo un seguimiento constante de los progresos del alumnado, teniendo en cuenta sus capacidades, esfuerzo realizado y los criterios de evaluación que marca la legislación. Se llevará a cabo en el aula virtual, que el alumnado podrá consultar en todo momento (autoevaluación).

c) **Evaluación sumativa**. Tiene por objeto medir el resultado al finalizar el proceso de enseñanza-aprendizaje.

El alumnado debe alcanzar la consecución de los RA del módulo. Para valorar el grado de consecución de cada RA de forma cuantitativa (calificaciones), se van a usar los **criterios de evaluación** de cada uno de ellos.

Las **calificaciones** se harán ponderando los pesos de los **criterios de evaluación**, que se indican en la siguiente tabla:

1er trimestre:

CE y sus pesos respecto al RA	Peso RA en la evaluación	UD	Peso de evaluación en el curso
a – 16% b – 16% c – 17% d – 17% e – 17% f – 17%	RA 1 3% de la evaluación total	UD 1. Diseño de planes de securización.	1ª evaluación parcial 21% del módulo
a – 20% b – 20% c – 20% d – 20% e – 20%	RA 2 7% de la evaluación total	UD 2. Configuración de sistemas de control de acceso y autenticación de personas.	
a – 20% b – 20% c – 20% d – 20% e – 20%	RA 3 11% de la evaluación total	UD 3. Administración de credenciales de acceso a sistemas informáticos.	

- Las actividades se realizarán y evaluarán en base a los criterios de evaluación.
- La ponderación de los criterios de evaluación dará la nota resultante de los correspondientes RA.
- La nota de la **1ª evaluación parcial** (1er trimestre) se hará mediante la ponderación de los RA en la evaluación.

Esto se aplicará al resto de trimestres.

2º trimestre:

CE y sus pesos respecto al RA	Pes RA en la evaluación	UD	Peso de evaluación en el curso
a – 20% b – 20% c – 20% d – 20% e – 20%	RA 4 15% de la evaluación total	UD4. Diseño de redes de computadores seguras.	2ª evaluación parcial 47% del módulo
a – 20% b – 20% c – 20% d – 20% e – 20%	RA 5 32% de la evaluación total	UD5. Configuración de dispositivos y sistemas informáticos.	

- La nota de la **2ª evaluación parcial** (2º trimestre) se hará mediante la ponderación de los RA en la evaluación.

3er trimestre:

CE y sus pesos respecto al RA	Peso RA en la evaluación	UD	Peso de evaluación en el curso
a – 20% b – 20% c – 20% d – 20% e – 20%	RA 6 7% de la evaluación	UD6. Configuración de dispositivos para la instalación de sistemas informáticos.	1ª evaluación final 32% del módulo
a – 20% b – 20% c – 20% d – 20% e – 20%	RA 7 25% de la evaluación	UD7. Configuración de los sistemas informáticos.	

- Las actividades se realizarán y evaluarán en base a los criterios de evaluación.
- La ponderación de los criterios de evaluación dará la nota resultante de los correspondientes RA.
- La nota de la **1ª evaluación final** (3er trimestre) se hará mediante la ponderación global de **todo el curso**.
- Si la nota resultante es negativa (menor que 5), le alumnado deberá presentarse a la 2ª convocatoria final para superar aquellos criterios de evaluación no superados.

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 lo siguiente:

- **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.

7.2. Instrumentos de evaluación:

Se usarán 4 instrumentos de evaluación:

a) **Ejercicios teóricos (ET)** o cuestionarios para responder a una serie de preguntas.

b) **Ejercicios prácticos (EP)**, a modo de práctica o proyecto.

c) **Exámenes (EX)**, que podrán ser teóricos o prácticos, según la naturaleza de los contenidos a evaluar.

Todos ellos se proporcionarán al alumnado a través del **aula virtual**, aunque en algún caso y solo si fuese necesario se podría hacer en **papel**.

Cada criterio o conjunto de criterios de los expuestos en la tabla anterior se podrán evaluar con **uno o varios instrumentos** (ET, EP y/o EX), pero los exámenes teóricos serán un 10% del RA.

Se valorará la iniciativa, originalidad y participación del alumnado, la exactitud y precisión en el desarrollo de los ejercicios y prácticas realizadas.

Referencia normativa:

La **Orden de 29 de septiembre de 2010**, establece en su **Artículo 2**, **Apartado 5**, que el departamento de familia profesional, a través del equipo educativo de cada uno de los ciclos formativos, desarrollará el currículo mediante la elaboración de las correspondientes programaciones didácticas de los módulos profesionales. Su elaboración se realizará siguiendo las directrices marcadas en el proyecto educativo del centro, especialmente en lo referente a los **procedimientos y criterios de evaluación** comunes para las enseñanzas de formación profesional inicial.

Procedimientos y criterios de evaluación comunes para las enseñanzas de formación profesional inicial.

- Se evaluarán los criterios de evaluación, según los pesos o ponderaciones expuestos en la tabla anterior, haciendo media aritmética de los distintos instrumentos de evaluación (ET, EP y/o EX) que se usen para cada criterio o conjunto de criterios.
- Para **aprobar el módulo** la nota media ponderada final debe ser **superior o igual a 5** (sobre 10).
- Las actividades no entregadas, o entregadas fuera de plazo, **se puntuarán con un 0**.
- La información sobre objetivos, contenidos y criterios de evaluación y calificación será facilitada por el profesorado de cada módulo profesional al alumnado durante el primer trimestre del curso académico.

Período final de recuperación / mejora de calificaciones.

El período final de **recuperación** o **mejora de calificaciones** se corresponde con las semanas siguientes al final de las clases (21-05-2024) y siempre antes de la finalización del curso (21-06-2024).

Mejora de calificaciones

El alumnado que desee mejorar sus calificaciones podrá realizar trabajos para los criterios de evaluación donde quiera incrementar su nota. La nota final de dichos criterios será la más alta de las obtenidas en régimen ordinario y en el extraordinario (mejora de calificaciones).

Recuperación

Aquellas/os estudiantes que deban **recuperar el módulo**, deberán asistir obligatoriamente a clase desde el 22-05-2024 hasta la prueba de la 2ª evaluación final, que se realizará antes del final del curso (21-06-2024). En dichas pruebas **se evaluarán solamente los criterios de evaluación no superados**. La nota final se obtendrá teniendo en cuenta los criterios de evaluación superados y los recuperados, prevaleciendo en estos últimos la máxima nota obtenida.

Por tanto, no hay que establecer criterios de evaluación diferentes para ese período, sino que durante el mismo el alumnado podrá:

- Volver a ser evaluado de los **criterios de evaluación no superados**, a través de los instrumentos de evaluación anteriormente descritos.
- Realizar las tareas que estén **suspensas** o **no entregadas**, o realizar otras tareas donde se evalúen los criterios de evaluación no superados.
- Obtener notas de mejora de sus competencias personales y sociales y su participación en clase, que permitan mejorar la nota en ese apartado.

De acuerdo con la Orden de 29 de septiembre de 2010, el carácter de la evaluación será continua por tanto la **asistencia del alumnado** durante todo este periodo de recuperación es **obligatoria**.

"En caso de comprobarse que el alumno no ha realizado su trabajo (cuestionarios, tareas, etc.) de **manera legítima** (copia de otro compañero, falsificación de resultados, plagio de otras fuentes, etc.), tendrá una **puntuación de 0** en dicho trabajo. El uso de IA no autorizado supondrá también una **puntuación de 0** en dicho trabajo. Para asegurarse de esto, el profesor podrá hacer las comprobaciones y preguntas que considere convenientes **pudiendo exigir si fuera necesario una defensa de su trabajo** delante de él. Este tipo de comportamientos no estarán exentos de otras medidas disciplinarias que se puedan acometer en función de la gravedad del acto realizado".

7.3. Superación del módulo.

El/La estudiante superará el módulo si iguala o supera la calificación de 5 sobre 10. Para ello, deberá trabajar en clase y entregar los ejercicios y exámenes planteados en el aula virtual.

Para el cálculo de la nota final del trimestre, se ponderarán las notas según lo indicado en la **tabla de ponderaciones** de criterios de evaluación. La obtención de la **nota final** del módulo vendrá dada por la media ponderada de las notas de ambas evaluaciones. Así, es conveniente entender que, si se aprueba una de las evaluaciones, pero se suspende otra y la media ponderada es negativa (inferior a 5), el/la estudiante **no habrá superado el módulo**.

8. Metodología.

8.1. Orientaciones metodológicas.

Esta planificación plantea una metodología **flexible**, **dinámica** y **eminentemente práctica**, adaptada a los objetivos y contenidos expuestos en apartados anteriores, y orientada a un proceso de evaluación continua y formativa. En resumen, una metodología que se adecúa al tipo de alumnado y a sus necesidades para conseguir la consecución de los objetivos marcados.

A priori no se descarta ninguno de los recursos metodológicos comúnmente admitidos: charlas, ejercicios prácticos, debates, conferencias, medios audiovisuales, formulación de problemas, exposiciones, orientaciones, trabajos individuales y grupales, investigación en el medio, visitas técnicas, etc.

Las pautas básicas serán las siguientes:

- Las actividades de enseñanza y aprendizaje seguirán el aprendizaje significativo.
- Se darán clases magistrales solamente para explicaciones teóricas que sean necesarias sobre determinados contenidos.
- El enfoque de estudio y trabajo del módulo será **eminentemente práctico**.
- Salvo que la naturaleza de algunos contenidos exija una actividad teórica, los trabajos a entregar serán **actividades prácticas**, para las que se entregará al alumnado las correspondientes **guías**.

En cualquier caso, la metodología se enfocará hacia la adquisición de hábitos de autonomía y autosuficiencia en el alumnado, mediante la resolución de los problemas que vayan surgiendo

y dando especial relevancia a la **iniciativa**, la **lógica**, el **método**, la **acumulación de experiencia** y la **capacidad de adaptación y reacción**; en definitiva, el desarrollo de habilidades, destrezas y criterios propios que producirán un gradual aumento de la independencia del alumnado respecto del profesor.

La organización del espacio físico está hecha para el uso individualizado de ordenadores, aunque no dificulta en modo alguno el trabajo en equipos.

Se fomentará la **lectura** a través del **aula virtual**, mediante la publicación de contenidos actualizados y de fácil búsqueda y acceso en Internet, con temáticas relacionadas con los contenidos estudiados.

Para finalizar, el trabajo con el alumnado irá destinado a desarrollar sus capacidades para la resolución práctica de problemas y situaciones que se pueden encontrar en el sector productivo, incluyendo en dichas capacidades el conocimiento técnico y teórico necesario para ello.

8.2. Actividades.

El tipo de trabajo a realizar se define a través de las siguientes actividades:

- **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-prácticas**. 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.

8.3. Agrupamientos.

Uno de los recursos que cuida y fomenta la diversidad en el entorno de trabajo es el agrupamiento de estudiantes para una mayor interacción.

El grupo clase consta de 11 estudiantes, lo que supone un grupo pequeño y bien cohesionado que favorece el **aprendizaje cooperativo**.

Así pues, el trabajo se hará de **forma individual**, permitiendo la **colaboración** entre el alumnado. 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.

8.4. 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.

8.5. Materiales didácticos y recursos.

El equipamiento informático con el que se cuenta para este módulo es el siguiente:

- Un ordenador portátil para cada estudiante.
- Ordenador del profesor.
- Una pantalla táctil gigante, con la que el profesorado podrá dar instrucciones o hacer ejercicios guiados.
- Red con acceso a Internet.
- El aula virtual **de** Plataforma Moodle Centros de la Consejería de Educación y Deporte, donde se pondrá a disposición del alumnado el material didáctico necesario para el desarrollo de la clase y donde, además, subirá las tareas exigidas en esta misma plataforma.

9. Atención al alumnado con necesidades específicas de atención educativa (NEAE).

Se debe regular la atención al alumnado con necesidades específicas de atención educativas. Por este motivo en este módulo se tendrán en cuenta, en caso de necesidad, la utilización del material adecuado para el alumnado con deficiencias auditivas, visuales o motoras.

- Para los alumnos o alumnas con deficiencia visual se adaptarán el hardware y el software a sus necesidades.
- Los alumnos o alumnas con deficiencia motora estarán ubicados en las mesas y sillas que pertinentemente se soliciten a tal efecto.
- Para los alumnos/as con TDAH se remite al documento que se encuentra en el departamento de orientación de este centro.
- Para las posibles adaptaciones NO SIGNIFICATIVAS se cambiará la metodología adaptándola a las necesidades del alumno.

10. Conexión con los temas transversales.

Durante el desarrollo de este módulo profesional se intentará fomentar en el alumnado actitudes relacionadas con:

- La educación para la **igualdad** entre los sexos, mediante trabajos con grupos mixtos.
- La educación para el cuidado del medio ambiente, mediante reciclado de papel y tóner.
- La educación moral y cívica, mediante una actitud de respeto en clase.
- La educación para la salud, mediante ergonomía y hábitos posturales.

11. Planes y proyectos.

11.1. Coeducación.

En el presente curso tenemos una chica en el grupo clase. Se integra bien con el resto de los compañeros y las relaciones interpersonales son fluidas, respetuosas y colaborativas. Para ayudar a este ambiente, de por si respetuoso y equitativo entre sexos, se hará hincapié en **figuras relevantes de ambos sexos** en el sector informático.

Las medidas que se tomarán serán las siguientes:

- Visibilizar el papel de la mujer: destacar las figuras femeninas que han contribuido en el desarrollo de la materia, en nuestro caso en Informática.
- Utilizar el lenguaje **no sexista**: usar un lenguaje (oral y escrito) igualitario e inclusivo que no excluya a ninguna persona por su sexo.
- Evitar estereotipos: evitar los estereotipos asociados al sexo, en concreto, explicando todas aquellas situaciones que se planteen a lo largo del curso.

- Participación en las actividades del plan de Igualdad: intentar participar en talleres, charlas, presentaciones, etc., que se realicen en el centro para ayuda a la concienciación de la plena igualdad entre hombres y mujeres.

11.2. Plan lector.

Desde el módulo fomentamos la lectura de las siguientes formas:

- Realización de prácticas sobre texto de actualidad (periódicos digitales, prensa escrita, manuales de informática). Leemos los textos en voz alta, analizamos el vocabulario, y por último elaboramos la práctica en el ordenador lo que lleva al alumnado a un segundo análisis del texto.

Como lecturas recomendadas:

- Prensa técnica en formato digital.
- Lectura de contenidos relacionados con la tecnología en general y, más concretamente, con la materia de este módulo para identificar vocabulario informático: noticias, artículos técnicos, posts, etc.
- Foros de actualidad.

12. Actividades extraescolares y complementarias.

En el presente curso se propondrá la asistencia virtual a alguna charla ofrecida en *streaming* por distintas entidades (Cajamar o la Universidad de Almería entre otras) si realizan algún evento relacionado con la materia de estudio de este módulo.

Se va a intentar ir al tercer congreso de ciberseguridad de Andalucía, pero de momento no se saben fechas.

Y por último las Jornadas Orientate 2024.

13. Bibliografía de aula y departamento.

En este momento no hay ningún libro publicado que cubra directamente el módulo. El profesor está realizando apuntes para cada unidad, pero siempre se podrá utilizar la documentación del INCIBE, EOI, etc, estándares, oficiales de configuración de servicios, etc..