Junta de Andalucía
Consejería de Educación y Deporte

IES AGUADULCE

UNIÓN EUROPEA
Fondo Social Europeo
El FSE invierte en tu futuro

PROGRAMACIÓN DIDÁCTICA

MÓDULO

HACKING ÉTICO

IES AGUADULCE

CURSO DE ESPECIALIZACIÓN EN CIBERSEGURIDAD

EN ENTORNOS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

CURSO 2023/2024

PROFESOR: DIOSDADO SÁNCHEZ HERNÁNDEZ

ÍNDICE

1. Introducción.

Este documento establece la programación didáctica del módulo de **Hacking Ético** que se imparte en el curso de especialización en **Ciberseguridad en Entornos de las Tecnologías de la Información**. Dicho módulo, tal como establece el 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, se debe impartir por profesores del cuerpo de Enseñanza Secundaria de la especialidad de Informática. La duración del módulo es de **120 horas lectivas** y se desarrolla a lo largo de los tres trimestres del curso (**cuatro horas semanales**). Su equivalencia en créditos ECTS es de 7 y su código el 5025.

La Formación Profesional debe ofrecer una respuesta eficaz y competente a las necesidades del actual mundo laboral, con un esquema flexible que permita la adecuación a los cambios tecnológicos que se están experimentando en los diferentes procesos productivos.

El Curso de especialización en ciberseguridad en entornos de las tecnologías de la información está regulado por los siguientes documentos:

- El 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**.
- Las **instrucciones de 30 de agosto de 2023**, 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 ordenan los cursos de especialización de Formación Profesional para el curso 2023/2024, y se establecen aspectos organizativos.
- La **Orden de 29 de septiembre de 2010 (BOJA 202)**, la cual **regula la evaluación**, certificación, acreditación y titulación académica del alumnado que cursa enseñanzas de FP en Andalucía..

Este módulo profesional contiene la formación necesaria para desempeñar las funciones de **detectar las vulnerabilidades de la organización mediante *hacking* ético**.

La función de *hacking* incluye aspectos como el **ataque programado a las redes y a las aplicaciones web de la organización**.

Las actividades profesionales asociadas a esta función se aplican en el **ataque de las redes de comunicaciones para acceder a datos o funcionalidades no autorizadas con el propósito de encontrar vulnerabilidades**.

Las líneas de actuación en el proceso de enseñanza aprendizaje que permiten alcanzar los objetivos del módulo versarán sobre:

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

2. Contextualización de la Programación.

El entorno profesional, social, cultural y económico del centro, su ubicación geográfica y las características y necesidades del alumnado, constituyen los ejes prioritarios en la planificación de procesos de enseñanza y aprendizaje. Los centros, departamentos y profesorado deberán tener en cuenta dicho entorno y las posibilidades de desarrollo de éste a la hora de establecer las programaciones de cada uno de los módulos profesionales y del ciclo formativo en su conjunto. Esta programación se ha diseñado teniendo en cuenta los principios y contenidos del **Plan de Centro** y del **Proyecto Educativo** del IES Aguadulce.

2.1. Características del Grupo.

En base a la normativa vigente, el grupo lo forman, como máximo, 20 alumnos y alumnas. La experiencia nos muestra que el factor más determinante en el proceso de enseñanza-aprendizaje es la heterogeneidad del grupo, podemos destacar los siguientes grupos:

- Alumnado que procede del ciclo de grado superior Administración de Sistemas Informáticos en Red, impartido en el propio centro IES Aguadulce, así como en centros de localidades cercanas (Vícar, Almería). Este alumnado tiene un buen bagaje tecnológico en cuanto a la implantación y administración de sistemas operativos, así como de planificación y gestión de redes, aunque suele presentar algunas dificultades en el desarrollo de scripts y programas al no haber cursado módulos relacionados con el desarrollo de aplicaciones.
- Alumnado que procede de los ciclos de grado superior Desarrollo de Aplicaciones Multiplataforma o Desarrollo de Aplicaciones Web, impartido en el propio centro IES Aguadulce, así como en centros de localidades cercanas (Vícar, Almería). Este alumnado tiene un buen bagaje tecnológico en cuanto al desarrollo de aplicaciones y la escritura de código, aunque suele presentar algunas dificultades en cuanto a la implantación y administración de sistemas operativos, así como en la planificación y gestión de redes.
- Alumnado que procede del ciclo de grado superior Sistemas de Telecomunicación e Informáticos en Red. Este alumnado tiene un buen bagaje tecnológico en cuanto a la planificación y gestión de redes, aunque puede presentar algunas dificultades en la implantación y administración de sistemas operativos, así como en el desarrollo de scripts y programas.
- Alumnado que procede del ciclo de grado superior Mantenimiento Electrónico. Este alumnado tiene un buen bagaje tecnológico en cuanto a la gestión y el mantenimiento del hardware, aunque puede presentar dificultades en la implantación y administración de sistemas operativos y redes, así como en el desarrollo de scripts y programas.

Aunque las procedencias del alumnado ya vemos que pueden resultar heterogéneas, las motivaciones suelen ser bastante coincidentes y se pueden resumir en dos: la **incorporación al mercado laboral con una cualificación superior** y la **posible continuación de estudios** (universidad, formación más específica, cuerpos y fuerzas de seguridad del estado, etc.)

Obviamente la heterogeneidad (diversidad de procedencias e intereses) introduce un factor de dificultad para el docente y su programación, pero al mismo tiempo representa una oportunidad de enriquecimiento mutuo de los diferentes subgrupos dentro del grupo.

3. Competencias y Objetivos Generales.

La **competencia general del curso** 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.*

Las **competencias profesionales, personales y sociales** de este curso de especialización son las que se relacionan a continuación:

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 políticas de seguridad establecidas, garantizando la funcionalidad requerida con un nivel de riesgo controlado.

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

g) Implantar sistemas seguros de 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**.

Según normativa, **la formación de este módulo contribuye a alcanzar las competencias i), k), l), m), n) y ñ) del curso de especialización**.

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

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 sesecurización 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**.

Según normativa, **la formación de este módulo contribuye a alcanzar los objetivos generales ñ), q), r), s), t), u) y v) de este curso de especialización**.

4. Resultados de Aprendizaje.

El Real Decreto de 7 de abril de 2020 establece los siguientes resultados de aprendizaje (RA) y sus correspondientes criterios de evaluación (CE):

RA01. Determina herramientas de monitorización para detectar vulnerabilidades aplicando técnicas de hacking ético.

RA02. Ataca y defiende en entornos de prueba, comunicaciones inalámbricas consiguiendo acceso a redes para demostrar sus vulnerabilidades.

RA03. Ataca y defiende en entornos de prueba, redes y sistemas consiguiendo acceso a información y sistemas de terceros.

RA04. Consolida y utiliza sistemas comprometidos garantizando accesos futuros.

RA05. Ataca y defiende en entornos de prueba, aplicaciones web consiguiendo acceso a datos o funcionalidades no autorizadas.

(Ver los CE en el Real Decreto de 7 de abril de 2020, BOE del 13 de mayo de 2020)

5. Unidades de Trabajo.

5.1. Contenidos y Secuencia de las Unidades de Trabajo.

Los contenidos básicos del módulo se especifican en el Real Decreto **479/2020**. Estos contenidos se han agrupado en **cinco unidades de trabajo** para su tratamiento. A continuación, se detalla dicha agrupación:

UT01. Introducción al hacking ético. Herramientas de monitorización.

- 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.

UT02. 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.

UT03. 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.
- Herramientas de búsqueda y explotación de vulnerabilidades.
- Ingeniería social. Phising.
- Escalada de privilegios.

UT04. Consolidación y utilización de sistemas comprometidos.

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

UT05. Ataque y defensa en entorno de pruebas, a aplicaciones web.

- Negación de credenciales en aplicaciones web.
- Recolección de información.
- Automatización de conexiones a servidores web (ejemplo: Selenium).
- Análisis de tráfico a través de proxies de intercepción.
- Búsqueda de vulnerabilidades habituales en aplicaciones web.
- Herramientas para la explotación de vulnerabilidades web.

5.2. Relación de Resultados de Aprendizaje con las Unidades de Trabajo Propuestas.

A continuación, se detalla la relación de cada una de las unidades de la programación con los RA establecidos en la legislación vigente:

UT01. Introducción al hacking ético. Herramientas de monitorización.

- RA01. Determina herramientas de monitorización para detectar vulnerabilidades aplicando técnicas de hacking ético.

UT02. Ataque y defensa en entorno de pruebas, de las comunicaciones inalámbricas.

- RA02. Ataca y defiende en entornos de prueba, comunicaciones inalámbricas consiguiendo acceso a redes para demostrar sus vulnerabilidades.

UT03. Ataque y defensa en entorno de pruebas, de redes y sistemas para acceder a sistemas de terceros.

- RA03. Ataca y defiende en entornos de prueba, redes y sistemas consiguiendo acceso a información y sistemas de terceros.

UT04. Consolidación y utilización de sistemas comprometidos.

- RA04. Consolida y utiliza sistemas comprometidos garantizando accesos futuros.

UT05. Ataque y defensa en entorno de pruebas, a aplicaciones web.

- RA05. Ataca y defiende en entornos de prueba, aplicaciones web consiguiendo acceso a datos o funcionalidades no autorizadas.

5.3. Temporalización.

La temporalización prevista para las unidades de trabajo se presenta en la siguiente tabla resumen:

- **Primer trimestre**:
  - UT01. Introducción al *hacking* ético. Determinación de las herramientas de monitorización para detectar vulnerabilidades.
  - UT03. Ataque y defensa en entorno de pruebas, de redes y sistemas para acceder a sistemas
  - de terceros.
- **Segundo trimestre**:
  - UT02. Ataque y defensa en entorno de pruebas, de las comunicaciones inalámbricas.
  - UT04. Consolidación y utilización de sistemas comprometidos.
- **Tercer trimestre**:
  - UT05. Ataque y defensa en entorno de pruebas, a aplicaciones web.

En cualquier caso, esta temporalización está condicionada al alumnado que integre el grupo, por lo que esta programación tiene una naturaleza dinámica que se irá adaptando a la evolución en el proceso de enseñanza-aprendizaje de los alumnos y alumnas del módulo.

6. Metodología.

Según el R**eal 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, las **líneas de actuación en el proceso de enseñanza-aprendizaje** que permiten alcanzar los objetivos del módulo versarán sobre:

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

6.1. Utilización del aula virtual como apoyo a la docencia

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.

6.2. Estrategias metodológicas en el aula

La **metodología didáctica** que se va a seguir para llevar a cabo el proceso de enseñanza-aprendizaje se regirá bajo las siguientes pautas, aunque éstas podrán sufrir las excepciones que se requieran en función de las necesidades del momento:

1. Se realiza una **breve introducción general** a la utilidad de las herramientas, metodologías, conceptos, procesos, etc. que se van a emplear.
2. Se comienza a trabajar con algunos **ejemplos básicos** que vayan usando poco a poco esas nuevas herramientas, comenzando con los casos más elementales.
3. Mediante el planteamiento de ciertos problemas y situaciones, se intenta **crear la necesidad de nuevas herramientas más sofisticadas** para que el propio alumnado intuya que sería útil la existencia de esa herramienta o concepto para mejorar el modo en que se podría resolver el problema planteado. De este modo el propio alumnado está de alguna manera anticipando lo que va a venir a continuación.
4. Se **introduce ese nuevo concepto o herramienta** en los ejemplos que se están desarrollando para **facilitar la resolución de un problema**, provocando que sea el propio alumnado quien lo pida o necesite.
5. Se procura que el alumnado **experimente con esas nuevas herramientas o conceptos de manera intuitiva e incompleta** para resolver nuevos problemas más complejos y así **descubra la necesidad de una mayor sistematización y documentación** en la explicación de esas nuevas herramientas y conceptos. De este modo el alumnado se encontrará **motivado y preparado para asimilar y aplicar esos nuevos conocimientos sin que le parezcan ajenos, extraños o innecesarios**.
6. Se lleva a cabo una **exposición más sistemática y demostrativa** de esos conceptos o herramientas para **sistematizar**, **completar** y **documentar** lo que el alumnado ya ha aprendido a utilizar de manera práctica e intuitiva.
7. Se plantean diversos problemas y ejercicios donde el alumnado podrá **poner en práctica todo lo aprendido tanto de manera intuitiva como sistemática**.

Todo el proceso de enseñanza-aprendizaje estará guiado por la realización práctica de los contenidos de cada unidad, introduciendo siempre los conceptos teóricos por medio de prácticas guiadas que darán paso posteriormente a prácticas autónomas.
De lo anterior se concluye que el alumnado tendrá que realizar trabajos y actividades, algunos de los cuales serán de carácter obligatorio, y otros de carácter opcional. Se procurará que existan prácticas individuales, pero también grupales, ya que tan importante es alcanzar los resultados de aprendizaje del módulo, como lo es alcanzar las soft skills (competencias personales y sociales).

Se dispone de un ordenador personal portátil para cada alumno o alumna. Dadas las particularidades de este curso de especialización, este ordenador será utilizado únicamente por ese alumno o alumna y será responsable de su uso y cuidado durante el curso.

El alumnado es responsable de salvaguardar las actividades y trabajos que va realizando a lo largo de todo el curso. El profesorado solicitará al alumnado las actividades y trabajos realizados para su posterior evaluación. El alumnado deberá utilizar algún soporte de almacenamiento propio (memoria USB, conexión con la nube o similar) para salvaguardar el trabajo de cara a continuar con él en sesiones posteriores o para la entrega al profesorado. De esta forma se evita que el alumnado pierda el trabajo si el equipo en el que trabaja habitualmente se estropea.

Se fomentará la realización de trabajos de investigación en los que habrá que contrastar informaciones de diferentes fuentes (material proporcionado en clase, documentación técnica, y búsquedas por Internet). También se fomentará el intercambio de información entre los miembros del grupo.

Tanto para la realización de actividades como para la realización de trabajos de investigación, se dejará tiempo suficiente en clase para su realización. Se hará un seguimiento en clase del trabajo del alumnado, con el fin de evaluar apropiadamente la adquisición de los resultados de aprendizaje. Así mismo, se fomentará que el alumnado haga exposiciones de uno o varios de los trabajos que haya realizado con el mismo fin anterior. Se incluirán exposiciones orales para mejorar la destreza comunicativa.

Los trabajos o actividades en grupo se fundamentarán en los principios del **aprendizaje cooperativo**, buscando la implicación en el desarrollo de la actividad práctica o trabajo, sin perjuicio de la distribución de roles entre los participantes.

A modo de síntesis y sin perjuicio del necesario rigor conceptual, se tendrá siempre presente la consideración de que **lo importante es desarrollar las capacidades para abordar realizaciones prácticas similares a aquellas que se va a tener que afrontar en la vida profesional**, una vez concluida la etapa formativa.

7. Evaluación.

La 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, 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.
A tal efecto, el **Proyecto Educativo,** en su apartado de Evaluación, recoge los puntos principales sobre el proceso de evaluación en los ciclos formativos de la familia de Informática y Comunicaciones. El proceso de evaluación explicitado en esta programación se ajusta a esos puntos, que a continuación son desarrollados de manera concreta para este módulo.

7.1. Criterios de Evaluación.

A continuación, se indican los criterios de evaluación (a partir de ahora CE) asociados a los diferentes resultados de aprendizaje (a partir de ahora RA) según normativa.

Resultado de aprendizaje	Criterios de evaluación
RA1. 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. 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.
RA2. 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.
RA3. 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

Resultado de aprendizaje	Criterios de evaluación
	objetivo mediante técnicas activas. 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.
RA4. 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.
RA5. 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. f) Se ha realizado la búsqueda y explotación de vulnerabilidades web mediante herramientas software.

7.2. Instrumentos de Evaluación.

Entendiendo como Instrumentos de Evaluación aquellos recursos que permiten la recogida o registro de información sobre el desarrollo del aprendizaje por parte del alumnado, se determina que para el presente módulo se tendrán en cuenta los siguientes instrumentos:

- **Tareas y actividades obligatorias de carácter práctico** (conocidas a partir de ahora como "tareas" o "prácticas") que el alumnado deberá realizar para demostrar la adquisición de los resultados de aprendizaje. En algunos casos estas tareas se realizarán durante una sesión de clase con un tiempo límite predefinido. En otros casos, para tareas más extensas, éstas se realizarán tanto en el aula como en casa, a lo largo de uno o varios días, debiendo ser entregadas en un determinado plazo.
- **Cuestionarios teórico/prácticos** (conocidos a partir de ahora como "cuestionarios") que el alumnado deberá realizar también para demostrar la adquisición de los resultados de aprendizaje.
- **Tareas de ampliación (voluntarias)**, que el alumnado podrá realizar para ampliar y reforzar sus conocimientos en un área concreta.

Se procurará que todas estas actividades puedan llevarse a cabo a través del aula virtual aunque, en algún caso y solo si se considerase necesario, se podría hacer en papel.

En relación con lo anterior:

- **Cada actividad o instrumento de evaluación que se realice recogerá los RA cubiertos por la unidad que se pretenden evaluar**, ya sea total o parcialmente, detallando los CE específicos que se evaluarán para cada RA.
- El conjunto de actividades prácticas a realizar, dependerá de la evolución del alumnado y de la unidad que se esté trabajando en cada momento. No obstante, **se procurará desarrollar, siempre que sea posible, al menos una actividad o tarea práctica por unidad**, versando dicha actividad sobre los RA de la unidad en curso o recién finalizada y, dada la naturaleza acumulativa de la materia, parte de los RA/CE cubiertos por en unidades anteriores.
- Cada actividad o trabajo práctico tendrá un **plazo de entrega** fuera del cual, dicha actividad no puede ser entregada por el alumnado, salvo circunstancias concretas: enfermedad o circunstancias personales justificables que hayan impedido que el alumno o la alumna realice la actividad en el periodo previsto. Si se dieran dichas circunstancias concretas, el alumnado debería justificar apropiadamente el motivo de manera documental. Esas actividades podrán realizarse en clase y, en algunos casos, fuera de clase. Para cada actividad concreta se indicará cómo se va a proceder. En cualquier caso, el profesorado siempre se reserva la posibilidad de exigir, si lo considera necesario, una defensa del trabajo haciendo que el alumno o alumna conteste a algunas preguntas sobre la realización de la práctica o bien que complete la práctica con algunos detalles adicionales basándose en lo que se ha presentado.
- Las actividades podrán tener un diseño **individual o grupal**, aunque lo habitual será el trabajo individual.
- Normalmente se procurará realizar al menos **un cuestionario o trabajo teórico/práctico por unidad**. En cualquier caso, como mínimo, se realizará **al menos un cuestionario teórico/práctico por trimestre**, en cuyo caso se englobarían los RA y CE cubiertos por todas las unidades impartidas en ese trimestre.
- A efectos de cómputo de la calificación final, **una tarea (voluntaria u obligatoria) no entregada** computará como **cero (0)**. De igual forma, un **cuestionario teórico/práctico no realizado computará** como **cero (0)**.
- **En caso de comprobarse que el alumno/a no ha realizado su trabajo (cuestionario, tarea, etc.) de manera legítima o fraudulenta** (copia de otro compañero/a, falsificación de resultados, plagio de otras fuentes, etc.), tendrá una puntuación de **un cero (0) en dicho trabajo**. Para asegurarse de esto, el profesorado podrá hacer las comprobaciones y preguntas que estime convenientes, pudiendo exigir, si lo considera necesario, una defensa de su trabajo delante de él. Este tipo de comportamientos fraudulentos **no estarán exentos**

de otras medidas disciplinarias que se puedan acometer en función de la gravedad del acto realizado.

- En el caso de las **tareas o actividades prácticas**, si no se consigue superar algún RA, habrá que acudir al periodo de **recuperación y mejora de calificaciones** del mes de junio para poder hacerlo.
- **El conjunto de las actividades de evaluación realizadas para cada unidad permitirá discernir si los RA cubiertos por esa unidad han sido superados o no.** Algunos CE de esos RA serán evaluados mediante tareas prácticas y otros mediante cuestionarios, o bien mediante ambos tipos de instrumentos, ponderándose en tal caso la calificación obtenida en cada uno..
  - En el caso de aquellos CE que sean evaluados mediante cuestionarios, será necesario superarlos los CE a través del cuestionario asociado a una unidad (o a varias, si se ha decidido hacer un único cuestionario para varias unidades).
  - Del mismo modo, para los CE evaluados mediante tareas, será necesario superarlos a través de una tarea práctica.
- Para que el alumnado esté siempre apropiadamente informado, **se detallará, en cada actividad que se desarrolle, qué RA/CE pueden superarse (o recuperarse) con ella.** Se informará de ello anticipadamente, al planificarse la actividad, así como en el propio enunciado o texto de la actividad.

7.3. Criterios de calificación.

La siguiente tabla muestra la **ponderación de resultados de aprendizaje (RA) y criterios de evaluación (CE) , así como su relación con las unidades**. Dicha tabla es un referente inicial y puede actualizarse para adaptarse al contexto y a las características particulares del grupo o al progreso del curso.

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

RA1. Determina herramientas de monitorización para detectar vulnerabilidades aplicando técnicas de hacking ético.	**Peso total %**
	15%
1.a) Se ha definido la terminología esencial del hacking ético.	**1,00 %**
1.b) Se han identificado los conceptos éticos y legales frente al ciberdelito.**1,00 %**	**1,00 %**
1.c) Se ha definido el alcance y condiciones de un test de intrusión.	**1,00 %**
1.d) Se han identificado los elementos esenciales de seguridad: confidencialidad, autenticidad, integridad y disponibilidad.	**1,00 %**
1.e) Se han identificado las fases de un ataque seguidas por un atacante.	**1,00 %**
1.f) Se han analizado y definido los tipos vulnerabilidades.	**2,00%**
1.g) Se han analizado y definido los tipos de ataque.	**2,00%**
1.h) Se han determinado y caracterizado las diferentes	**2,00%**

vulnerabilidades existentes.	
1.i) Se han determinado las herramientas de monitorización disponibles en el mercado adecuadas en función del tipo de organización.	**4,00%**
RA2. Ataca y defiende en entornos de prueba, comunicaciones inalámbricas consiguiendo acceso a redes para demostrar sus vulnerabilidades.	**Peso total %**
	25%
2.a) Se han configurado los distintos modos de funcionamiento de las tarjetas de red inalámbricas.	**3,00%**
2.b) Se han descrito las técnicas de encriptación de las redes inalámbricas y sus puntos vulnerables.	**5,00%**
2.c) Se han detectado redes inalámbricas y se ha capturado tráfico de red como paso previo a su ataque.	**3,00%**
2.d) Se ha accedido a redes inalámbricas vulnerables.	**4,00%**
2.e) Se han caracterizado otros sistemas de comunicación inalámbricos y sus vulnerabilidades.	**3,00%**
2.f) Se han utilizado técnicas de “Equipo Rojo y Azul”.	**4,00%**
2.g) Se han realizado informes sobre las vulnerabilidades detectadas.	**3,00%**
RA3. Ataca y defiende en entornos de prueba, redes y sistemas consiguiendo acceso a información y sistemas de terceros.	**Peso total %**
	25%
3.a) Se ha recopilado información sobre la red y sistemas objetivo mediante técnicas pasivas.	**5%**
3.b) Se ha creado un inventario de equipos, cuentas de usuario y potenciales vulnerabilidades de la red y sistemas objetivo mediante técnicas activas.	**5%**
3.c) Se ha interceptado tráfico de red de terceros para buscar información sensible.	**5%**
3.d) Se ha realizado un ataque de intermediario, leyendo, insertando y modificando, a voluntad, el tráfico intercambiado por dos extremos remotos.	**5%**
3.e) Se han comprometido sistemas remotos explotando sus vulnerabilidades.	**5%**
RA4. Consolida y utiliza sistemas comprometidos garantizando accesos futuros.	**Peso total %**
	10%
4.a) Se han administrado sistemas remotos a través de herramientas de línea de comandos.	**2,50%**

4.b) Se han comprometido contraseñas a través de ataques de diccionario, tablas rainbow y fuerza bruta contra sus versiones encriptadas.	**2,50%**
4.c) Se ha accedido a sistemas adicionales a través de sistemas comprometidos.	**2,50%**
4.d) Se han instalado puertas traseras para garantizar accesos futuros a los sistemas comprometidos.	**2,50%**
RA5. Ataca y defiende en entornos de prueba, aplicaciones web consiguiendo acceso a datos o funcionalidades no autorizadas.	**Peso total %**
	25%
5.a) Se han identificado los distintos sistemas de autenticación web, destacando sus debilidades y fortalezas.	**4,00%**
5.b) Se ha realizado un inventario de equipos, protocolos, servicios y sistemas operativos que proporcionan el servicio de una aplicación web.	**4,00%**
5.c) Se ha analizado el flujo de las interacciones realizadas entre el navegador y la aplicación web durante su uso normal.	**4,00%**
5.d) Se han examinado manualmente aplicaciones web en busca de las vulnerabilidades más habituales.	**4,00%**
5.e) Se han usado herramientas de búsquedas y explotación de vulnerabilidades web.	**5,00%**
5.f) Se ha realizado la búsqueda y explotación de vulnerabilidades web mediante herramientas software.	**4,00%**

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.
A efectos de **cómputo de la nota final del módulo**, se tendrán en cuenta las siguientes pautas:

- **Todos los RA (para aquellos CE que han sido evaluados) deben ser superados con un grado de consecución de al menos un 5.**
- **Si no se alcanza la calificación mínima de un 5 en cada RA**, la calificación máxima alcanzable al calcular la nota de una evaluación será de 4, pues **no se podrá superar el módulo si no se han superado todos sus Resultados de Aprendizaje**.
- Para el **cálculo de las calificaciones correspondientes al primer, segundo y tercer trimestre**, así como la calificación final, se aplicará lo siguiente:
    - El **grado de consecución de cada RA** se calculará **en función de los CE evaluados hasta el momento**.
    - La **calificación trimestral** se calculará **en función de los CE evaluados hasta el momento**. Eso significa que al final de algunos de los trimestres, algunos de los RA habrán sido evaluados solo parcialmente (porque no todos sus CE han sido evaluados aún). **El cálculo del grado de consecución de un RA se llevará a cabo basándonos únicamente en esos CE evaluados**. Ahora bien, **si alguno de los RA**

impartidos hasta el momento (en el grado en el que hayan sido evaluados hasta el momento) **no ha sido superado, la calificación trimestral será como máximo de un 4**.

- Esto significa que la nota obtenida en cada evaluación es una especie de "fotografía" de cómo se encuentra el alumno o alumna justo en ese momento de curso, reflejando de la manera más fiel posible el concepto de **evaluación continua**.
- Para el **cálculo de la calificación final** no se realizará la nota media de los trimestres, sino que se seguirá el proceso antes descrito, teniendo en cuenta la calificación obtenida en cada uno de los CE y RA a través de los diferentes instrumentos utilizados durante el curso. Si se han podido impartir y evaluar apropiadamente todos los RA/CE, se tendrán todos en cuenta. Si hay algún RA que no haya sido impartido o alguno que haya sido evaluado parcialmente (no se pudieron evaluar todos sus CE), solo se tendrá en cuenta todo aquello que haya podido ser evaluado. Recordemos una vez más que **cada RA impartido y evaluado (tanto total como parcialmente) debe obtener un grado de consecución mínimo de un 5 para poderse considerar el módulo como superado**. En caso contrario, la máxima calificación alcanzable será de un 4.

- **Redondeo de la calificación final:** cuando el alumnado tenga una nota superior a 5, las calificaciones finales que arrojen números decimales se redondearán a la unidad, eliminando la parte decimal y aproximando la unidad a la más cercana. De este modo, si la parte decimal fuera inferior a 0,500 se aproximará a la unidad inferior. Si esta fuera igual o superior a 0,500, se aproximará a la unidad superior. **Si el cálculo de la calificación final es inferior a 5, el módulo no se considerará como superado y su calificación máxima podría llegar como mucho hasta el 4**.
- La realización de **actividades de ampliación voluntarias** puede conllevar un incremento en la calificación final. En ningún caso, su no realización o mala resolución supondrá un detrimento en la evaluación. Para calcular el incremento de calificación proporcionado por las tareas de ampliación, el profesorado tendrá en cuenta los RA/CE que se evalúen en la actividad propuesta y se actualizarán en aquellos casos en los que se mejoren.

7.4. Criterios de corrección de la expresión escrita

Tal y como se establece en el Proyecto Educativo del 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 cualquier instrumento de evaluación deberá de cumplir lo siguiente:

- El documento debe seguir las pautas marcadas referentes a formato, estructura, organización y ortografía.
- Se incluyen las capturas de pantalla propias necesarias para aclarar las explicaciones textuales y, a su vez, para demostrar la autoría del trabajo.
- Se realizan los comentarios necesarios para aclarar las explicaciones.
- Seguimos rigurosamente la petición expuesta en el enunciado de cada ejercicio.

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

7.5. Proceso de recuperación y mejora de calificaciones

Una vez finalizado el periodo de evaluación ordinario, existe un **período final de recuperación o mejora de calificaciones**, comprendido entre la 3ª evaluación y la evaluación final, que se utilizará para intentar que el alumnado consiga alcanzar los resultados de aprendizaje no superados o mejore las competencias relacionadas con el módulo. Durante este periodo:

- El alumnado podrá volver a ser **evaluado de los RA no superados**, a través de los instrumentos de evaluación anteriormente descritos (tareas de carácter práctico y cuestionarios teórico/prácticos). Estos instrumentos de evaluación incorporarán los CE de los RA aún pendientes por superar.
- En el caso de los **cuestionarios** teórico/prácticos, se requerirá que el alumnado realice una o más pruebas donde se le vuelva a evaluar, mediante los CE asociados, aquellos RA que no lograra superar durante el curso.
- En el caso de las **tareas**, se requerirá que el alumnado realice una serie de tareas (diferentes a las realizadas durante el curso, aunque de un nivel similar de dificultad) donde se evalúen los RA no superados mediante los CE asociados.
- De la misma manera, el alumnado que desee **optar a una mejora de su calificación** podrá acogerse también a este proceso preparándose para éste instrumentos de evaluación específicos basados en los CE de los RA en los que se quiera intentar mejorar.

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 para poder recuperar o mejorar la calificación. Las faltas de asistencia durante este período por parte del alumnado que necesite recuperar dará lugar a la no superación del módulo, pues no se trata de venir un día a realizar un examen de recuperación, sino de asistir durante este período a una serie de sesiones en las que se llevarán a cabo diversas actividades de recuperación.
La **nota final después de este periodo de recuperación** se obtendrá teniendo en cuenta todo el trabajo realizado durante el curso, pero considerando las calificaciones de las partes recuperadas o mejoradas en lugar de las calificaciones obtenidas y registradas inicialmente. Por tanto, las pautas para calcular la calificación en el periodo de recuperación o mejora de nota, y poder considerar el módulo por superado o mejorado, a través de sus RA y CE, son las mismas que se han descrito para el resto del curso.

8. Fomento de la Lectura.

Para el desarrollo de la **competencia en comunicación lingüística** de los centros educativos públicos se desarrollarán las siguientes actuaciones:

- **Lectura en clase** de artículos relacionados con la materia del módulo al final de las unidades de trabajo, dichas lecturas se complementarán con coloquios o debates sobre la temática de la lectura, que también podrá ser apoyada por otro material multimedia.
- Realización de trabajos de investigación comparando diversos artículos y contenidos, redactando finalmente **resúmenes y esquemas** con la información obtenida.
- Realización de **presentaciones orales** sobre algunas de las tareas realizadas fomentando así la lectura desde la oralidad, con lo que se potencia y enriquece la capacidad de expresión del alumnado y se desarrolla su capacidad de atención y comunicación.

9. Medidas previstas para la consecución de la plena igualdad entre hombres y mujeres.

Teniendo en cuenta que habitualmente la presencia de alumnas en este ciclo es mínima, no es tarea fácil llevar a cabo este punto, pues partimos de una importante desproporción de género desde la misma matriculación. No obstante, se trabaja ponderando la labor y la figura de la mujer en la sociedad como elemento indispensable para la convivencia, la mejora y la integración en la sociedad.

Las medidas que se tomarán serán las siguientes:

- **Visibilizar el papel de la mujer**: se destacarán las figuras femeninas que han contribuido en el desarrollo de la materia, en nuestro caso en Informática, y en particular en Programación.
- Utilizar el **lenguaje igualitario, inclusivo, y no sexista**: se procurará utilizar la lengua tanto oral como escrita para identificar una realidad que no excluya a las mujeres.
- **Evitar estereotipos**: se evitarán los estereotipos asociados al sexo en los enunciados de prácticas, ejercicios, tareas, etc.
- Participación en las actividades del **plan de Igualdad**: Se instará a participar en talleres, charlas, presentaciones, etc., que se realicen en el centro para la consecución de la plena igualdad entre hombres y mujeres.

10. Medidas de Atención a la Diversidad.

La atención a la diversidad hace referencia a las **adaptaciones curriculares no significativas**. Una adaptación curricular no significativa establece medidas de refuerzo o de ampliación para determinados alumnos y alumnas sin cambiar los objetivos y contenidos establecidos por el módulo. Esto habitualmente se debe a que el alumnado parte con distintos niveles de conocimientos y experiencia dependiendo de su procedencia (otros ciclos formativos de grado medio o superior de la misma u otras familias profesionales, bachilleratos tecnológicos, bachilleratos de ciencias sociales, estudios universitarios, etc.).
Por otro lado, también habrá que tener en cuenta que no todos los alumnos y alumnas superarán los objetivos establecidos con la misma facilidad pudiendo necesitar en algunos casos dichos refuerzos o ampliaciones, según los supere con dificultad o por el contrario los supere con notable facilidad y estén preparados para poder aprender algo más.
Dado que es probable que los niveles sean diferentes podemos disponer de varios recursos que se pueden emplear para atender esta diversidad, pudiéndose plantear un seguimiento individual de cada alumno o alumna a través de propuestas del tipo:

- Realización de las actividades propuestas al final de cada unidad, que siguen un orden creciente de dificultad.
- Integración del alumnado con problemas en grupos de trabajo de nivel heterogéneo para que en ningún momento se sienta discriminado. Si se crea un buen ambiente de grupo, los mismos compañeros y compañeras se ayudarán entre ellos favoreciendo el proceso de aprendizaje.
- Apoyo del profesorado cuando lo consideren necesario y en la forma que se estime oportuna.
- A través de la lectura del material complementario (libros, apuntes, ejercicios resueltos, revistas, artículos, etc.) que se encuentra en el aula.
- Realización de actividades complementarias propuestas y/o coordinadas por los profesores.
- Realizaciones de trabajos haciendo uso de la capacidad creativa y los medios y recursos con que cuenta el centro.
- Planteamiento por parte de los profesores/as de ejercicios y cuestionarios al alumnado con la consiguiente supervisión.
- Exposición de algunos de los trabajos que se van desarrollando en clase.
- Adaptación de la programación, delimitando aquellos que sean considerados como mínimo exigible según el currículo.

10.1. Tratamiento del alumnado con NEE

En relación al **tratamiento del alumnado con NEE**, se estará a lo dispuesto en los **acuerdos adoptados en la sesión de evaluación inicial** para cada caso, reflejados en el acta de la reunión del equipo educativo, o si se detectan a posteriori, en una **reunión del equipo educativo convocada al efecto**.
En caso de que se detectara algún caso de NEE tanto en la evaluación inicial como durante el resto del curso, el tutor del grupo, en colaboración con el equipo educativo y el departamento de orientación, elaborará un informe sobre las medidas a adoptar.

11. Actividades complementarias y extraescolares.

Las posibles actividades propuestas para este curso son:

- Aquellas actividades relacionadas con la **ciberseguridad** que se realicen durante las tradicionales **jornadas "Orientate".**
- Aquellas actividades relacionadas con la **ciberseguridad** que se realicen durante la **"Feria de Orientación Académica y Profesional".**
- Participación en **talleres** y **concursos** relacionados con la **ciberseguridad** que se convoquen a lo largo del curso por diversos organismos públicos o privados. Las convocatorias las pueden realizar instituciones como la Universidad de Almería, el INCIBE (Instituto Nacional para la Ciberseguridad), etc.

12. Recursos Didácticos.

Para el desarrollo normal de la clase se disponen de los siguientes recursos:

- Pizarra y accesorios.
- Ordenador de de dotación TDE para el profesorado.
- Proyector para conectar a ordenador o recursos audiovisuales.
- Sistema de altavoces.
- Libros de consulta (no están el aula, pero en un momento dado se pueden consultar del departamento).
- Curso alojado en la plataforma Moodle Centros.
- Aula con ordenadores para alumnado.
- Conexión a Internet.
- Software de red, software de documentación (paquete ofimático), navegadores web y utilidades para el acceso a los servicios de red.

13. Bibliografía.

- Herrero Pérez, Luis. "*Hacking Ético*". 2022. Ra-Ma.
- Material del INCIBE: https://www.incibe.es/
- Material del CCN-CERT: https://www.ccn-cert.cni.es
- Material de TryHackMe: https://tryhackme.com/
- Material de HackTheBox: https://www.hackthebox.com/
- Material de Vulnhub: https://www.vulnhub.com/
- Castillo, Fernando. "*Hacking. Curso completo*". 2022. Ra-Ma.
- Ortega Candel, José Manuel. "*Hacking Ético con herramientas Python*". 2018. Ra-Ma.
- Astudillo B., Karina. "*Hacking Ético. ¡Cómo convertirse en hacket ético en 21 días o menos!*". 2018. Ra-Ma.
- Mata, Arturo E. "Kali Linux para *hackers. Técnicas y metodologías avanzadas de seguridad informática ofensiva*". 2023. Ra-Ma.