# CURSO DE ESPECIALIZACIÓN EN CIBERSEGURIDAD EN ENTORNOS DE TECNOLOGÍAS DE LA INFORMACIÓN

**PROGRAMACIÓN ANUAL**

Parte específica del módulo:
5025. Hacking Ético

**Departamento de Familia Profesional de Informática**

Curso: 2022-23
Turno: tardes

# ESQUEMA DE CONTENIDOS

# 1 CARACTERÍSTICAS GENERALES DEL CURSO DE ESPECIALIZACIÓN EN CIBERSEGURIDAD EN ENTORNOS DE TECNOLOGÍAS DE LA INFORMACIÓN

Se relacionan en la parte general de la programación de los ciclos formativos.

# 2 DESCRIPCIÓN DEL MÓDULO

El módulo profesional de Hacking Ético, al cual hace referencia esta programación didáctica, está enmarcado dentro de las enseñanzas del Curso de Especialización en Ciberseguridad en Entornos de las Tecnologías de la Información.

# 3 UBICACIÓN, OBJETIVOS, CONTENIDOS Y DISTRIBUCIÓN TEMPORAL DEL MÓDULO

## 3.1 UBICACIÓN, DISTRIBUCIÓN TEMPORAL Y CARACTERÍSTICAS

El Real Decreto 479/2020, de 7 de abril (BOE nº134 de 13 de mayo), establece los aspectos básicos del currículo para este curso de especialización que cuenta con un total de 720 horas de duración, de las cuales al módulo profesional de Hacking Ético le corresponden 65 horas. Todo esto teniendo en consideración el Real Decreto 1147/2011, de 29 de julio, por el que se establece la ordenación general de la formación profesional del sistema educativo.

Para este módulo, se han asignado 4 horas semanales en el horario propuesto por la Consejería de Educación de la Región de Murcia que en el calendario actual lectivo de 2022-2023 para el municipio de Murcia llegan a sumar 150 horas de clase y equivalentes sin embargo a 7 ECTS en el RD de Título.

## 3.2 OBJETIVOS/RESULTADOS DE APRENDIZAJE Y CRITERIOS DE EVALUACIÓN

De conformidad con lo regulado en el Real Decreto 479/2020, de 7 de abril, por el que se establece el Curso de especialización en Ciberseguridad, el módulo de Hacking Ético contribuye a alcanzar las siguientes **competencias profesionales del curso de especialización**:

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

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

**También contribuye a conseguir los siguientes objetivos generales:**

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.

**En cuanto a resultados de aprendizaje y criterios de evaluación:**

El módulo profesional de Hacking Ético está formado por una serie de resultados de aprendizaje descritos en términos de competencias y que el alumnado debe adquirir como resultado del proceso de enseñanza-aprendizaje. Con cada uno de estos resultados de aprendizaje se encuentran relacionados los criterios de evaluación, mediante los cuales se acredita la consecución de las competencias.

**RA1. Determina herramientas de monitorización para detectar vulnerabilidades aplicando técnicas de *hacking* ético.**

Criterios de evaluación:

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.**

Criterios de evaluación:

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.**

Criterios de evaluación:

a) Se ha recopilado información sobre la red y sistemas objetivo mediante técnicas pasivas.

b) Se ha creado un inventario de equipos, cuentas de usuario y potenciales vulnerabilidades de la red y sistemas objetivo mediante técnicas activas.

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.**

Criterios de evaluación:

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.**

Criterios de evaluación:

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

# 4 UNIDADES DE TRABAJO

De las Unidades de Trabajo vamos a prever, en lo posible, los objetivos y resultados de aprendizaje, contenidos, distribución temporal, metodología concreta y criterios de evaluación aplicables.

**UT01. Determinación de las herramientas de monitorización para detectar vulnerabilidades**

− Elementos esenciales del *hacking* ético.

− Diferencias entre *hacking*, *hacking* ético, tests de penetración y hacktivismo.

− Recolección de permisos y autorizaciones previos a un test de intrusión.

− Fases del *hacking*.

− Auditorías de caja negra y de caja blanca.

− Documentación de vulnerabilidades.

− Clasificación de herramientas de seguridad y *hacking*.

− *ClearNet*, *Deep Web*, *Dark Web*, *Darknets*. Conocimiento, diferencias y herramientas de acceso: *Tor*. *ZeroNet*, *FreeNet*.

**UT02. 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*).

− Monitorizacion 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.

**UT03. 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.

**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 DISTRIBUCIÓN TEMPORAL

## 5.1 DISTRIBUCIÓN TEÓRICA PREVISTA (A 2 HORAS SEMANALES > 60 HORAS)

**Primer Trimestre (14 semanas, 56 horas)**

U.T. 0. Presentación del módulo (6 horas)

U.T. 1. 25 horas

U.T. 2. 25 horas

**Segundo Trimestre (11 semanas, 44 horas)**

U.T. 3. 25 horas

U.T. 4. 25 horas

**Tercer Trimestre (9 semanas, 36 horas)**

U.T.5 36 horas

## 5.2 ANÁLISIS DE LA VIABILIDAD DEL CURRÍCULO PREVISTO

Los contenidos planificados se pueden impartir con bastante hogura ya que el módulo en el RD correspondiente consta de un asignación de 30 horas y en la distribución temporal realizada por la administración educativa de la Comunidad Autónoma de la Región de Murcia para 2022-2023 se le asigna un cómputo de horas de 2 horas semanas que llegan a unas 60 horas anuales mayorando casi al doble la imputación horaria del RD.

# 6 METODOLOGÍA

## 6.1 CRITERIOS

## 6.2 ASPECTOS CONCRETOS

Los aspectos metodológicos que se pretenden aplicar en este módulo descansan en la idea de que el alumno se considere parte activa de la actividad docente, con esto se pretende involucrarlo en el proceso de asimilación de nuevos conceptos y adquisición de capacidades no como un mero contenedor de éstas sino como un productor directo de estos conocimientos y habilidades en sí mismo. De igual forma se pretende que el alumno respete al profesor y a sus compañeros, respectando igualmente el material de la clase.

- La metodología didáctica favorecerá, mediante la integración de los contenidos científicos tecnológicos y organizativos una visión global y coordinada de los procesos productivos en los que debe intervenir el alumnado.

- El trabajo en el aula consistirá en la exposición oral de cada unidad de trabajo, para que, posteriormente, los alumnos desarrollen los ejercicios y prácticas propuestos.
- La metodología será participativa, favoreciendo el aprendizaje por descubrimiento. Partiendo de los conocimientos iniciales de los alumnos/as, estos deberán construir sus aprendizajes significativos.
- La metodología será teórico-práctica (debida a la alta carga normativa del módulo), acompañada de situaciones que reflejen la realidad en la mayor medida posible, huyendo de ejemplos y ejercicios abstractos.
- Estos aspectos prácticos del módulo se desarrollarán en la forma de:
  .1. Experiencias didácticas: las realiza el profesor.
  .2. Experiencias prácticas: las realizan los alumnos, el profesor corrige técnicas de trabajo y evalúa resultados.

Para el trabajo en el aula, los alumnos dispondrán de toda la documentación que se considere oportuna, además de la asistencia permanente del profesor.

# 7 MATERIALES, RECURSOS, ESPACIO DOCENTE

## 7.1 MATERIALES Y RECURSOS DIDÁCTICOS

Los recursos necesarios para impartir este módulo son los siguientes:

Para las explicaciones de contenidos teóricos:

Aula con medios audiovisuales:

- Pizarra.
- Retroproyector y pantalla.
- Ordenador con Linux Mint, LibreOffice
- Distribuciones Linux de seguridad y testeo.
- Impresoras.

Para la confección de los trabajos de los alumnos:

- Conexión a Internet en el aula.
- Correo electrónico
- Moodle

## 7.2 DISTRIBUCIÓN DEL ESPACIO Y EL TIEMPO DOCENTE

Se opta por la “organización tipo A” que se explica en la parte general de la programación del ciclo formativo.

# 8 MEDIDAS PARA ESTIMULAR EL INTERÉS Y EL HÁBITO DE LECTURA Y LA CAPACIDAD DEL ALUMNO PARA EXPRESARSE CORRECTAMENTE

Este apartado se estudia en la parte general de la programación del ciclo.

# 9 CRITERIOS, PROCEDIMIENTOS E INSTRUMENTOS DE EVALUACIÓN

9.2.2.3.3.1 Aspectos y apartados a ponderar.

**Se sigue el Modelo 6 (original, sin cambios) de la Programación General del Ciclo Formativo ASIR.**

Partiendo de las Realizaciones de aprendizaje dispuestas en el currículo, y para cada una de ellas, se valorarán los siguientes aspectos y ponderaciones:

| Apartado | Ponderación |
|---|---|
| Pruebas objetivas basadas en:<br>● cuestionarios<br>● enunciados teórico-prácticos de aplicación amplia de los contenidos<br>● prácticas de laboratorio<br>● prácticas reales sobre el terreno<br>● actividades de investigación<br>● actividades de documentación<br>● actividades extraescolares directamente conectadas con el currículo<br>● participación en actividades cooperativas<br>● otras pruebas | 100 % (*) |

Hay que tener en cuenta las consideraciones:

- Todas las prácticas propuestas en el curso son de entrega obligatoria. La no entrega en plazo y forma de un porcentaje igual o superior al 20% implica la no superación del módulo correspondiente, que podrá evaluarse como máximo con la calificación "4".
- Las pruebas y prácticas que no se realicen íntegramente durante el periodo lectivo en el aula (por abarcar más de un día.) no se considerarán para el cálculo de la calificación, aunque tienen la misma consideración de obligatorias.
- (*) La calificación de cada periodo trimestral de evaluación será la media ponderada de las notas obtenidas en todas las pruebas objetivas de aprendizaje acumulas durante dicho periodo (multiplicando cada calificación por el número de periodos lectivos que dicha prueba abarque, y dividiendo la suma por total de periodos que tenga el módulo en la evaluación considerada)
- En caso de falta de asistencia justificada la nota no influirá en la media ponderada, ni negativa ni positivamente.

### *Cálculo de la calificación final*

***Calificación final***: se seguirá el **método 1 (original, sin cambios) de la Programación General del Ciclo ASIR**. La calificación final del módulo se expresa en cifras de 1 a 10 sin decimales, y MH en su caso. Consistirá en la media aritmética de la calificación obtenida en cada una de las tres evaluaciones, en el caso de haberlas superado todas. En caso contrario, la calificación final será la calificación menor de las tres.

### *Recuperación*

Se seguirá lo dispuesto en el método 6 (ampliada para pendientes del curso anterior) de la Programación General de ASIR.

***Recuperaciones parciales***

- Al final de cada evaluación trimestral (excepto en el último trimestre) o al comienzo de la siguiente se realizará una prueba objetiva de recuperación.
- La nota máxima que se puede obtener en una recuperación es 5.
- En el caso del 2º curso, que no tiene clase durante el tercer trimestre por la realización de la FCT, se propondrán durante el tercer trimestre actividades de repaso para el alumnado asistente a clases de recuperación, que sean de utilidad para la recuperación de los módulos pendientes de primer y segundo curso que puedan tener.

***Recuperación en convocatoria ordinaria***

Se guardarán las evaluaciones superadas ***dentro del mismo curso académico hasta la convocatoria extraordinaria***, de forma que el alumnado que ha superado una evaluación no tiene que volver a presentarse.

La nota máxima que se puede obtener en cada evaluación pendiente en esta recuperación es 5.

***Recuperación en convocatoria extraordinaria***

Este módulo ***tiene convocatoria extraordinaria***. Para acceder a dicha prueba deben entregarse previamente todas las prácticas y actividades que se hayan realizado durante el curso en la plataforma moodle.

La nota máxima que se puede obtener en cada evaluación pendiente en esta recuperación es 5.

***Alumnado que repite el módulo***

El alumnado que haya promocionado a 2º curso con este módulo pendiente se **examinará al final del segundo trimestre (antes de los exámenes de 2º curso) de la totalidad del mismo**, con la finalidad de que pueda alcanzar en su caso la FCT en convocatoria ordinaria. **Para acceder a dicha prueba deberá haber realizado y entregado (en el plazo y forma que se especifique) previamente tres pruebas específicas que le serán comunicadas a comienzos del primer trimestre por el profesor, mediante convocatoria oficial en tablón de anuncios**. Dichas prácticas **deberán ser evaluadas positivamente** por el profesor **para poder concurrir al examen**. El profesor examinará dichas pruebas y entrevistará al alumno si lo considera necesario.

*9.2.2.3.3.2. Cálculo de la calificación final*

Usaremos el Modelo 1 usando una ponderación por defecto de 33%.

9.2.2.3.3.3. Recuperación

Usaremos el Modelo 1.

# 10 ALUMNOS MATRICULADOS EN 2º CON MÓDULOS DE 1º SUSPENSOS

No aplica

# 11 ATENCIÓN A LA DIVERSIDAD DEL ALUMNADO EN LOS CICLOS FORMATIVOS

No aplica.

# 12 PREVENCIÓN DE RIESGOS LABORALES

Este apartado se estudia en la parte general de la programación de los ciclos de la misma familia profesional del centro.

# 13 INTERDISCIPLINARIEDAD

Al ser un módulo general y transversal se relaciona con todos los módulos del curso de especialización.

# 14 TRANSVERSALIDAD

Al ser un módulo general y transversal se relaciona con todos los módulos del curso de especialización.

## 15 ACTIVIDADES COMPLEMENTARIAS Y EXTRAESCOLARES

No se han previsto.

## 16 USO DE LAS TICS

Al ser un curso de especialización post-ciclo las TIC’s vienen incluidas en todas y cada una de los trabajos y tareas a realizar.

## 17 BIBLIOGRAFÍA


- Apuntes de clase
- Videos públicos propuestos por el profesor