EXTRACTO PROGRAMACIÓN DOCENTE

Principado de Asturias | Consejería de Educación

Centro Integrado de Formación Profesional

AVILÉS

Principado de Asturias

DEPARTAMENTO DE FAMILIA PROFESIONAL:

INFORMÁTICA Y COMUNICACIONES

CICLO FORMATIVO:

IFC401 – CURSO DE ESPECIALIZACIÓN EN CIBERSEGURIDAD EN ENTORNOS TIC

MODULO FORMATIVO:

5025 – HACKING ÉTICO

DOCENTE:

JUAN CARLOS MARTINEZ FERNÁNDEZ

CURSO:

2026 – 2027

Identificación de la programación

Centro Educativo

Código	Centro	Año académico
33028684	**CIFP Avilés**	**2026/2027**

Ciclo formativo

Familia profesional	Ciclo formativo	Código	Curso
Informática y Comunicaciones	**Curso de Especialización en CIBERSEGURIDAD en ENTORNOS TIC**	**IFCE01**	**1º**
Regulación legal	- Ley Orgánica 2/2006, de 3 de mayo, de Educación. - Ley Orgánica 3/2020, de 29 de diciembre, por la que se modifica la anterior. - 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 - Ley Orgánica 3/2022, de 31 de marzo, de ordenación e integración de la Formación Profesional.		

Módulo profesional

Código	**5025**
Nombre	**Hacking ético**
Horas/curso	**120**
Horas/semana	**4**
Especialidad del profesorado	**Profesorado de Enseñanza Secundaria – Informática (0590 - 107)**

Índice

1. Resultados de aprendizaje 2

2. Contenidos y criterios 4

UT 1: Introducción al hacking ético 4

UT 2: Recogida de información (footprinting) 5

UT 3: Enumeración de servicios (fingerprinting) 5

UT 4: Hacking de aplicaciones web 6

UT 5: Hacking de redes y sistemas informáticos 6

UT 6: Mantenimiento del acceso, escalada de privilegios y pivotaje 7

UT 7: Hacking de redes inalámbricas 7

3. Evaluación 8

3.1. Criterios de evaluación 8

3.2. Procedimientos e instrumentos de evaluación 8

3.3. Criterios de calificación 10

3.4. Ponderación 12

4. Actividades de recuperación 12

4.1. Actividades de recuperación del primer cuatrimestre 12

4.2. Programas de recuperación de módulos no superados 13

5. Sistema extraordinario de evaluación para aquellos alumnos a los que, como consecuencia de sus faltas de asistencia, no se les puedan aplicar los criterios generales de evaluación ni la propia evaluación continua 13

6. Criterios de elaboración de pruebas extraordinarias 13

7. Mínimos exigibles 14

1. Resultados de aprendizaje

Los resultados de aprendizaje y los criterios de evaluación del módulo que se detallan a continuación son los mencionados en el *Real Decreto 479/2020* por el que se establece el título y las enseñanzas mínimas.

1) 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.

2) 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.

3) 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.

4) 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.

5) 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.

2. Contenidos y criterios

Los criterios de evaluación son los descritos en el apartado de anterior. Los contenidos se desarrollan en base a los dispuestos por el Real Decreto 479/2020. Se enumeran a continuación enmarcados en las unidades de trabajo que los comprenden.

UT 1: Introducción al hacking ético

Resultado de aprendizaje asociado**: 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.

Contenidos

- 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.

UT 2: Recogida de información (footprinting)

Resultado de aprendizaje asociado**: 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.

Contenidos:

- ClearNet, Deep Web, Dark Web, Darknets. Conocimiento, diferencias y herramientas de acceso: Tor. ZeroNet, FreeNet.
- Fase de reconocimiento (*footprinting*).

UT 3: Enumeración de servicios (fingerprinting)

Resultado de aprendizaje asociado**: RA3.** *Ataca y defiende en entornos de prueba, redes y sistemas consiguiendo acceso a información y sistemas de terceros.*

Criterios de evaluación:

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.

Contenidos:

- Fase de escaneo (fingerprinting).
    - Escaneo de redes locales y direcciones IP.
    - Escaneo de puertos abiertos.
    - Escaneo de servidores.
    - Recolección de información en redes abiertas OSINT (Open Source Intelligence).
    - Uso y configuración de herramientas enfocadas a OSINT.
- Monitorización de tráfico.
- Interceptación de comunicaciones utilizando distintas técnicas.

UT 4: Hacking de aplicaciones web

Resultado de aprendizaje asociado**: RA5.** *Ataca y defiende en entornos de prueba, aplicaciones web consiguiendo acceso a datos no 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.

Contenidos:

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

UT 5: Hacking de redes y sistemas informáticos

Resultado de aprendizaje asociado**: RA3.** *Ataca y defiende en entornos de prueba, redes y sistemas consiguiendo acceso a información y sistemas de terceros.*

Criterios de evaluación:

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.

Contenidos:

- Manipulación e inyección de tráfico.
- Herramientas de búsqueda y explotación de vulnerabilidades.
- Ingeniería social. *Phising*.

UT 6: Mantenimiento del acceso, escalada de privilegios y pivotaje

Resultado de aprendizaje asociado**: 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.

Contenidos:

- Escalada de privilegios.
- Administración de sistemas de manera remota.
- Pivotaje en la red.
- Instalación de puertas traseras con troyanos (*RAT, Remote Access Trojan*).

UT 7: Hacking de redes inalámbricas

Resultado de aprendizaje asociado**: 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.

Contenidos:

- Comunicación inalámbrica.
    - Tipos de redes inalámbricas. Estándares.
    - Modos de autenticación con wifi.
    - Cifrados en entornos inalámbricos. Estándares y protocolos.
- 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.
- Ataques y auditorías de contraseñas.

3. Evaluación

Los siguientes apartados recogen los distintos aspectos de la evaluación.

3.1. Criterios de evaluación

Son criterios de evaluación a tener en consideración todos los detallados previamente. Las capacidades personales y sociales podrán ser evaluadas como parte de otras actividades que integren los mencionados criterios.

3.2. Procedimientos e instrumentos de evaluación

Principios generales

El proceso de evaluación del aprendizaje programado debe atender a los siguientes puntos:

- En el desarrollo de las unidades de trabajo en que se divide el módulo, se realizara un proceso de **evaluación continua**.

- La evaluación continua, dentro de cada unidad de trabajo, se realiza valorando la participación del alumnado en la clase, los trabajos y actividades, tanto individuales como en grupo, y la resolución de ejercicios y cuestionarios que en cada caso se realicen.
- Los criterios de evaluación específicos de cada unidad de trabajo han sido mostrados previamente junto con la descripción de sus contenidos.

Métodos específicos

En cada una de las unidades de trabajo enumeradas en la programación se realizarán las siguientes actividades de evaluación:

- **Pruebas objetivas**:
  - ✓ Cuestionario tipo **test**: Se podrán realizar cuestionarios en las unidades de trabajo. La nota mínima para superar el cuestionario es de 5.
  - ✓ Pruebas **teórico-prácticas**: se podrán realizar pruebas teórico-prácticas en las unidades de trabajo, en la que se evaluará la comprensión de los diferentes conceptos y procedimientos. La nota mínima de superación de la prueba es de 5.
  - ✓ **Prácticas**: en las unidades de trabajo se podrán realizar trabajos prácticos, cuya nota mínima de superación es de 5.
- Entrega de informes de **actividades prácticas** en diferentes formatos.

Los trabajos y prácticas **deberán ser originales**, **se penalizará la copia entre el alumnado calificando con 0 puntos a cada persona implicada**, independientemente si ha copiado o se ha dejado copiar. En el caso de utilizar distintas fuentes para realizar las prácticas se deberá indicar en el informe las mismas a modo de **referencias bibliográficas**, así como el **uso de cualquier herramienta de IA** para la realización de las mismas. En caso de no hacerlo también se penalizará con una calificación de 0 puntos.

Con el fin de realizar una evaluación del alumnado lo más precisa y justa posible, y teniendo presente un carácter continuo de la evaluación, se van a utilizar los siguientes **instrumentos de evaluación**:

Procedimientos	Aspectos Considerados
Pruebas tipo test	- Conceptos - Procedimientos
Prácticas/Informes	- Conceptos - Procedimientos - Organización - Planteamiento correcto - Originalidad - Contenido
Observación sistemática del trabajo	- Capacidad organizativa - Comportamiento
Diálogo con el alumnado	- Conceptos - Procedimientos
Interpretación de datos	- Conceptos - Procedimientos

3.3. Criterios de calificación

Siguiendo el proceso de evaluación descrito, la calificación del alumnado para cada evaluación puede concretarse a través de la suma de tres componentes: **pruebas objetivas (30%), actividades prácticas (60%) y trabajo en el aula (10%).**

A continuación se especifica cómo se calificará cada uno de los tipos de pruebas que se realizarán a lo largo del curso:

a) **Pruebas objetivas:** Resolución de cuestionarios y pruebas individuales prácticas: Cada una de estas pruebas se valorará de 0 a 10 considerándose aprobada si el alumno obtiene una valoración igual o superior a 5.

b) **Actividades prácticas**: cada prueba se valorará de 0 a 10. Si a lo largo del periodo de evaluación se hubieran realizado varias de estas pruebas se calculará la media entre ellas, siempre y cuando el alumno haya superado los contenidos mínimos exigibles para aprobar cada una de ellas. Esta media será ponderada en función de la importancia dada a cada ejercicio.

Alternativamente, en las actividades prácticas también se utilizará la forma de calificación consistente en tres niveles de corrección:

- **No satisfactoria/presentada.** Equivale a una calificación de 0 puntos. Esto ocurre cuando no se ha procedido a la entrega de la tarea o no tiene contenido mínimo evaluable.
- **Satisfactoria.** Equivale a una calificación de 7 puntos. Se califica como tal cuando la tarea cumple unos mínimos, pero contiene fallos que suponen no llegar al máximo.
- **Supera lo esperado**. Equivale a una calificación de 10 puntos. Si la tarea cumple con todo lo pedido y además añade elementos que la enriquecen.

c) **Trabajo en el aula:** se valorarán las aportaciones realizadas en el aula, la actitud de trabajo y colaboración con los compañeros, cuestionarios gamificados que se realicen durante las clases, participación en los foros que se dispondrán en el aula virtual, etc.

Las entregas han de realizarse en el plazo marcado por el profesor para ello. **No se permite la entrega fuera de plazo.** En este caso, la puntuación será de 0 puntos.

Para el alumnado que no supere el módulo profesional en la evaluación final ordinaria se realizará una **evaluación final extraordinaria**. Durante el periodo comprendido entre ambas evaluaciones finales se desarrollarán las actividades de refuerzo destinadas a superar el módulo en la evaluación extraordinaria. La docencia impartida entre la evaluación ordinaria y la extraordinaria estará dedicada a que el alumnado que no haya superado el módulo en la evaluación final ordinaria pueda afianzar sus conocimientos y afrontar con garantías de éxito la prueba o pruebas de la evaluación final extraordinaria.

3.4. Ponderación

UT	Ponderación
UT 1: Introducción al hacking ético	10%
UT 2: Recogida de información (*footprinting*)	15%
UT 3: Enumeración de servicios (*fingerprinting*)	15%
UT 4: Hacking de aplicaciones web	15%
UT 5: Hacking de redes y sistemas informáticos	15%
UT 6: Mantenimiento del acceso, escalada de privilegios y pivotaje	15%
UT 7: Hacking de redes inalámbricas	15%

4. Actividades de recuperación

Los siguientes apartados detallan los distintos tipos de actividades de recuperación.

4.1. Actividades de recuperación del primer cuatrimestre

Este punto se refiere a las actividades que realizará el alumnado que obtenga calificación negativa en la evaluación parcial intermedia de febrero.

Al tratarse de un sistema de evaluación totalmente continua, en el cual al final del curso se emplean todos los contenidos que se han ido desarrollando durante el curso, no es necesaria la realización de actividades específicas de recuperación tras el primer cuatrimestre. El alumnado tendrá la oportunidad de recuperar en la segunda evaluación todas las evaluaciones con calificación negativa por medio de:

- Repetición de todas las pruebas objetivas con calificación negativa
- Realización de las prácticas no superadas

4.2. Programas de recuperación de módulos no superados

El alumnado que no haya superado el módulo a través del procedimiento de evaluación continua ni mediante la prueba de recuperación anterior a la sesión de evaluación ordinaria podrá recuperarlo en una o varias pruebas teórico-prácticas a desarrollar con anterioridad a la sesión de evaluación extraordinaria.

5. Sistema extraordinario de evaluación para aquellos alumnos a los que, como consecuencia de sus faltas de asistencia, no se les puedan aplicar los criterios generales de evaluación ni la propia evaluación continua

Para la planificación de este sistema extraordinario se siguen las directrices establecidas en el Proyecto Curricular de Ciclo Formativo.

Al alumnado a quien no se pueda aplicar los criterios de evaluación continua a causa de un elevado número de faltas de asistencia se les realizará **a final de cada evaluación** (febrero y junio) una **prueba extraordinaria** de evaluación teórico-práctica.

En dicha prueba se incluirán:

- cuestionarios de tipo test
- preguntas teóricas
- actividades prácticas

Así mismo, se deberán entregar todas las prácticas propuestas a lo largo del módulo, que se encontrarán en el Aula Virtual.

6. Criterios de elaboración de pruebas extraordinarias

En la prueba extraordinaria podrán incluirse ejercicios y cuestiones sobre todos los contenidos de las unidades de trabajo incluidas en esta programación, además de la presentación de los trabajos exigidos con carácter general para el resto del alumnado y/o trabajos específicos para el alumnado que se presente a la prueba extraordinaria. Los criterios de calificación de estas pruebas son los mismos que se aplican durante el curso.

En las pruebas extraordinarias, las cuestiones planteadas se diseñarán de forma que el 50% de ellas versen sobre contenidos mínimos, de forma que si el alumnado resuelve satisfactoriamente dichas cuestiones sobre contenidos mínimos pueda ser evaluado con un 5.

En el caso de las **pruebas extraordinarias de junio**, siempre incluirá, **al menos**:

- Examen tipo test.
- Presentación y defensa de las **Prácticas asociadas del módulo**.

7. Mínimos exigibles

Son mínimos exigibles todos los criterios de evaluación detallados en esta programación.