Curso 2024 / 2025

Programación Didáctica

Curso de especialización en ciberfffffffffffffffffffffff ffffffffffffffffff

---

Departamento de informática

IES Rafael Alberti, Cádiz

Índice

1. Introducción

1.1 Justificación del curso

La sociedad actual está inmersa en una imparable transformación tecnológica y digital que está cambiando la forma de trabajar, de vivir, de comunicarnos, de relacionarnos o de hacer negocios. Y para todo ello necesitamos estar conectados mediante todo tipo de dispositivos que, a través de Internet, intercambian datos personales o profesionales. En este escenario digital, la información se convierte en uno de los bienes más preciados y la seguridad de la información en un punto crítico.

Por ello, la demanda de perfiles formados en ciberseguridad ha crecido de manera espectacular en los últimos años. El experto en ciberseguridad se ha convertido en un perfil fundamental para proteger la integridad digital de cualquier organización.

La competencia general de este curso de especialización consiste en definir e implementar estrategias de seguridad en los sistemas de información realizando diagnósticos de ciberseguridad, identificando vulnerabilidades e implementando las medidas necesarias para mitigarlas aplicando la normativa vigente y estándares del sector, siguiendo los protocolos de calidad, de prevención de riesgos laborales y respeto ambiental.

1.2 Situación del currículo

El Curso de Especialización en Ciberseguridad en entornos de las tecnologías de la información queda identificado por los siguientes elementos:

- **Nivel:** Formación Profesional de Grado Superior.
- **Duración:** 720 horas.
- **Familia Profesional:** Informática y Comunicaciones (únicamente a efectos de clasificación de las enseñanzas de formación profesional).
- **Rama de conocimiento:** Ingeniería y Arquitectura.
- **Créditos ECTS:** 43.

Referente en la Clasificación Internacional Normalizada de la Educación: P-5.5.4.

La referencia al sistema productivo, de este módulo profesional, se encuentra en 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.

1.3 Justificación del currículo

El artículo 5 del Real Decreto 479/2020, de 7 de abril, establece las competencias profesionales, personales y sociales de este curso de especialización.

“El equipo educativo responsable del desarrollo del curso de especialización elaborará de forma coordinada las programaciones didácticas para los módulos profesionales, teniendo en cuenta la adecuación de los diversos elementos curriculares a las características del entorno social y cultural del centro docente, así como a las del alumnado para alcanzar la adquisición de la competencia general y de las competencias profesionales, personales y sociales del título.”

Por ello, es el Departamento de la Familia Profesional correspondiente el encargado de elaborar y aprobar dichas programaciones.

Dicho esto, cabe decir que la programación es un proceso a través del cual se diseña y planifica el trabajo que el profesorado ha de desarrollar con sus alumnos. Este dará como resultado un conjunto de unidades didácticas ordenadas y secuenciadas, teniendo siempre como referente el proyecto curricular del ciclo formativo, así como la realidad laboral del sector informático. Elimina la improvisación, el azar y permite adaptarse al contexto de los alumnos. En definitiva, es una guía de qué y cuándo hay que impartir y cómo calificar a nuestros alumnos.

El profesorado debe evaluar los aprendizajes de los alumnos, los procesos de enseñanza y su propia práctica docente. Igualmente evaluará el Proyecto Curricular, las programaciones didácticas de los módulos profesionales y el desarrollo real del currículo en relación a las necesidades educativas del Centro, a las características específicas de los alumnos y al entorno socio-económico, cultural y profesional, adaptando esta programación a la realidad social del entorno.

Por ello, la programación debe estar en continua evolución dependiendo de los resultados del proceso de enseñanza-aprendizaje de los alumnos, no solo del curso para el que se ideó, sino también para los posteriores.

2. Marco legal

2.1 Leyes Orgánicas

Ley Orgánica 2/2006, de 3 de mayo (BOE 106 de 4 de mayo), de Educación. https://www.boe.es/boe/dias/2013/12/10/pdfs/BOE-A-2013-12886.pdf de 9 de diciembre (BOE 295, de 10 de diciembre) para la Mejora de la Calidad Educativa (LOMCE).

Ley Orgánica 5/2002, de 19 de junio (BOE 147, de 20 de junio), de las Cualificaciones y de la Formación Profesional.

2.2 Leyes de Andalucía

Ley 17/2007, de 10 de diciembre (BOJA 252 de 17 de diciembre y BOE 13 de febrero de 2008), de Educación en Andalucía.

Decreto 436/2008, de 2 septiembre (BOJA 182, de 12 de septiembre), por el que se establecen las enseñanzas de la Formación Profesional inicial.

Instrucciones de 25 de septiembre 2024, de la Dirección General de Formación Profesional y Educación Permanente de la Consejería de Desarrollo Educativo y Formación Profesional de la Junta de Andalucía, por las que se ordenan los grados E de Formación Profesional para el curso 2024/2025, y se establecen aspectos organizativos.

2.3 Calendario de implantación

Real Decreto 806/2006, de 30 de junio (BOE 167, de 14 de julio), por el que se establece el calendario de aplicación de la nueva ordenación del sistema educativo establecido por la Ley Orgánica 2/2006, de 3 de mayo, de Educación.

2.4 Requisitos de centros

Real Decreto 132/2010, de 12 de febrero (BOE 62, de 12 de marzo), por el que se establecen los requisitos mínimos de los centros que impartan las enseñanzas del segundo ciclo de la educación infantil, la educación primaria y la educación secundaria.

2.5 Desarrollo curricular de la materia

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.

2.6 Organización y funcionamiento de los centros

Decreto 327/2010, de 13 de julio (BOJA 139, de 16 de julio), por el que se establece el Reglamento Orgánico de los IES.

Orden de 20 de agosto de 2010 (BOJA 169, 30 de agosto), por la que se regula la organización y el funcionamiento de los institutos de educación secundaria, así como el horario de los centros, del alumnado y del profesorado.

2.7 Contextualización

Real Decreto 1147/2011, de 29 de julio, (BOE 182, de 30 de julio) por el que se establece la ordenación general de la formación profesional del sistema educativo. Deroga el Decreto 1538/2006.

2.8 Regulación y evaluación

Orden de 29 de septiembre de 2010 (BOJA 202, de 15 octubre), 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.

Orden de 28 de septiembre de 2011 (BOJA 206, de 20 de octubre), por la que se regulan los módulos profesionales de formación en centros de trabajo y de proyecto para el alumnado matriculado en centros docentes de la Comunidad Autónoma de Andalucía. Deroga la Orden de 9 de diciembre de 1998 sobre regulación y la de 31 de julio de 2001 sobre exención de la FCT.

Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas. En lo referente a la utilización de tecnologías telemáticas y audiovisuales para el proceso de seguimiento y evaluación.

2.9 Calendario escolar

Decreto 301/2009, de 14 de julio, (BOJA 139, de 20 de julio de 2009) por el que se regula el calendario y la jornada escolar en los centros, a excepción de los universitarios.

3. Contexto del centro educativo

El I.E.S. Rafael Alberti está ubicado en Cádiz, con una población que gira alrededor de 122.990 habitantes. Su economía está basada principalmente en el sector del comercio, debido a la presencia de los astilleros y las actividades en la zona portuaria y la Zona Franca. Otro sector clave es el turismo, gracias a su importante patrimonio histórico, así como sus playas, fiestas locales y gastronomía.

El centro oferta estudios de ESO, Bachillerato, CFGM de Gestión Administrativa, CFGS de Técnico Superior en Administración y Finanzas, CFGB de Informática de Oficina, CFGBE de Informática de Oficina, CFGM de Sistemas Microinformáticos y Redes, CFGS de Desarrollo de Aplicaciones Web, CFGS de Desarrollo de Aplicaciones Multiplataforma, y los cursos de especialización en Ciberseguridad en entornos de las tecnologías de la información, Desarrollo de Videojuegos y Realidad Virtual, e Inteligencia Artificial y Big Data.

3.1 Características del grupo

La distribución del alumnado es variada, habiendo accedido a través de los ciclos formativos de grado superior de la familia profesional de informática y comunicaciones, como ASIR, DAW y DAM, así como del ciclo formativo de grado superior de Técnico Superior en Sistemas de Telecomunicaciones e Informáticos, de la familia profesional de Electricidad y Electrónica.

4. Objetivos

4.1 Objetivos generales del curso de especialización

El Real Decreto 479/2020, de 7 de abril, fija los objetivos generales de este curso.

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 de securización de la organización.

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

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

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

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

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

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

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

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

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

l) Automatizar planes de despliegue 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) Desarrollar manuales de información, utilizando herramientas ofimáticas y de diseño asistido por ordenador para elaborar documentación técnica y administrativa.

q) 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.

r) 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.

s) 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.

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

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

4.2 Competencias profesionales, personales y sociales

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) Implementar sistemas seguros de despliegue 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.

5. Metodología

5.1 Principios metodológicos

La metodología a emplear tomará como eje el diálogo, el debate y la confrontación de ideas e hipótesis, ya que no podemos olvidar que el aprendizaje es un proceso social y personal que cada individuo construye al relacionarse, activamente, con las personas y la cultura en las que vive. Como orientaciones metodológicas se utilizarán las siguientes:

- Partir del nivel de desarrollo del alumno/a y los conocimientos previos que posee.
- Favorecer la adquisición de aprendizajes significativos y funcionales, trasladables a las situaciones de trabajo relacionadas con su Ciclo Formativo. De este modo, se crean relaciones entre los nuevos contenidos y lo que ya se sabe.
- Contribuir al desarrollo de la capacidad de “aprender a aprender”, permitiendo que el alumno/a se adapte a nuevas situaciones de aprendizaje.
- Crear un clima de aceptación mutua y cooperación.

En definitiva, la metodología a utilizar será activa, participativa, creativa y reflexiva; para que el alumno/a sea protagonista de su propio aprendizaje. Además, será importante hacer ver al alumnado la funcionalidad de los contenidos, de manera que puedan utilizarlos en situaciones reales de la vida cotidiana en relación con sus intereses y motivaciones. Es por ello que en la medida de

lo posible intentaremos no hacer clases magistrales salvo en casos excepcionales en los que los contenidos a explicar requieran una mayor utilización de estas.

Basándonos en un aprendizaje significativo, en las unidades didácticas se ha utilizado la metodología de Tyler y Wheeler, que distingue entre varios tipos de actividades. En concreto, se utilizan los siguientes tipos de actividades:

- Actividades de evaluación de conocimientos previos.
- Actividades de presentación – motivación.
- Actividades de desarrollo de contenidos o explicación.
- Actividades de refuerzo y ampliación.
- Actividades de evaluación.
- Actividades de recuperación.

5.2 Aspectos organizativos

5.2.1 Trabajo en equipo y colaboración

Tal y como se establece en los Objetivos de la formación Profesional, ser capaces de realizar trabajo en equipo es uno de los objetivos. Es por ello necesario para el proceso de enseñanza-aprendizaje, y conviene señalar el tipo de agrupamiento de los alumnos mediante el cual se desarrollarán dichas actividades.

Los diferentes bloques de la materia permiten que se pueda trabajar tanto individualmente (resolución de actividades) como en pequeños grupos (discusión y resolución de casos prácticos) y en gran grupo.

Individualmente, como actividad de aprendizaje propia de cada alumno/a, favorecemos la capacidad intelectual de aprender por sí mismo.

- Realiza actividades y tareas programadas.
- Crea sus propias pautas o ritmos de aprendizaje.
- Organiza sus tiempos. Es puntual en la entrega de trabajos.
- Es autocrítico y tiene autoestima. Tiene iniciativa ante problemas que se le plantean.
- Es perseverante y responsable.
- Cuida los recursos que utiliza (instalaciones, equipos, bibliografía, etc.), evita riesgos medioambientales. Aplica las normas de seguridad e higiene en el trabajo.

El trabajo individual nos permitirá, por tanto, desarrollar las competencias personales y profesionales programadas.

En grupo, “el conocimiento que se comparte, se multiplica”. Se procurará que el alumnado logre entre sí, un buen clima de cooperación y trabajo en equipo. El desarrollo de estas actitudes en la Formación Profesional es básico para que el alumno/a en el futuro se integre fácilmente en su puesto de trabajo y pueda participar en un equipo profesional. Los trabajos en grupo nos permiten desarrollar las competencias personales y sociales del alumnado.

Usaremos el agrupamiento de pequeño grupo, entre 2 y 4 componentes, y en menor medida el trabajo individualizado, tanto para los trabajos de clase, autodidacta como en casa. Esto mismo es aplicable a la realización de las prácticas obligatorias, y también cuando la actividad a desempeñar sea la de dudas, cierre o repaso.

5.3 Desarrollo de las unidades didácticas

El proceso que se seguirá es el siguiente:

- Presentación de la unidad, indicando los Resultados de Aprendizaje y Criterios de Evaluación asociados a la unidad.
- Cada sesión comenzará con un breve resumen de los contenidos vistos en la sesión anterior, resolviendo cualquier tipo de duda que haya surgido.
- A continuación se explicarán los nuevos contenidos con ayuda de diapositivas, resolución de ejercicio práctico o algún material de apoyo, como vídeos, imágenes, audios, enlaces a otros contenidos, etc.
- Puesta en práctica de aquellos contenidos en actividades que se podrá comenzar en clase y seguir practicando en casa.
- Al finalizar la unidad se realizarán actividades de refuerzo y ampliación para resolución de las dudas que aún les puedan surgir o ampliar los conocimientos, de forma que atendamos a la atención a la diversidad y en concreto a los diferentes ritmos de aprendizaje.

5.4 Materiales y recursos didácticos

Se utilizarán los siguientes recursos:

- Para el desarrollo de los contenidos conceptuales se emplearán textos, ejemplos y apuntes en formato digital.
- Para el desarrollo de los contenidos prácticos se utilizarán los ordenadores del aula-grupo.

En cuanto al espacio utilizado para el desarrollo de esta programación, será el aula del grupo usando los ordenadores disponibles. Será necesario el uso de Internet como complemento a las actividades.

- **Hardware:**
- Televisión.
- Ordenadores.
- Red de área local.
- Dispositivos IoT.
- Raspberry Pi.
- USB Rubber Ducky.
- WiFi Pineapple y similares.
- HackRF One.
- USB Killer Pro Kit.
- AirDrive Forensic Keylogger Pro.
- Servidor Proxmox.
- **Software:**
- Sistema operativo.
- Navegador.
- Software de virtualización.
- PNETLab.

Se usará la plataforma educativa online Moodle Centros que proporciona la Consejería de Educación de la Junta de Andalucía, como lugar de consulta y presentación de trabajos, así como medio principal de comunicación con el alumnado.

5.5 Actividades complementarias y extraescolares

Las visitas programadas por el departamento se recogen en el plan anual del centro, y las actividades que se han programado para el presente curso lectivo se han incluido en dicho documento.

5.6 Fomento de la lectura

Dada la particular naturaleza de las enseñanzas relacionadas con la informática, es frecuente que los profesionales de la informática deban leer documentación técnica en inglés, ya que o la documentación en castellano está anticuada o bien las traducciones son deficientes, y los detalles técnicos traducidos resultan con frecuencia incomprensibles, incompletos o erróneos.

Por tanto, es necesario que el alumno que cursa estudios de informática se acostumbre a utilizar documentación técnica en inglés, en primer lugar para "perder el miedo" a consultar documentación en inglés u otra lengua y en segundo lugar porque es frecuente que no haya otra alternativa si se quiere tener información actualizada.
El alumno debe evitar utilizar permanentemente traductores automáticos, no solo porque las traducciones de textos técnicos la mayoría de las veces no son comprensibles, sino porque también se pierde demasiado tiempo si cada vez que se necesite comprender algo escrito en otro idioma haya que copiar el texto al software traductor, el cual frecuentemente origina problemas relacionados con el formato del texto copiado (viñetas, etc.) que dificultan la comprensión del texto traducido. Sin contar que es posible que lo que sea necesario traducir sea un texto impreso en papel, o una conversación hablada.

6. Medidas de atención a la diversidad

Es un hecho indiscutible que los alumnos y alumnas son diferentes por su cultura, intereses, estilos de aprendizaje, motivaciones y tiempo que necesitan para aprender y esta necesidad, requiere diferentes grados de atención educativa.

El art 5.3 del Real Decreto 1147/2011, indica que las enseñanzas de formación profesional se adaptarán al alumnado con necesidad específica de apoyo educativo para que se garantice su acceso, permanencia y progresión.

En la Formación Profesional Inicial no se contemplan adaptaciones curriculares significativas, es por ello que, solo se podrán contemplar medidas no significativas de acceso al currículo. Por este motivo, la forma de atender a la diversidad desde este módulo será sobre todo metodológica.

Los ajustes deben ser flexibles para atender a las dificultades, con la metodología, actividades, materiales y agrupamientos que no entorpezcan al resto del alumnado. Estas pueden ser:

- Adaptaciones de acceso, no solo movilidad sino también acceso a la información. Que pueden afectar a la metodología, recursos y métodos de evaluación, pero jamás a los contenidos, ya que la Ley lo impide.
- Adaptaciones metodológicas que no afectarán a los componentes del currículo.

El Departamento didáctico solicitará asesoramiento al Departamento de Orientación del Centro respecto al alumnado que soliciten apoyo, para en caso de no tener apoyo externo intentar asesorar a las familias y/o alumnado solicitante, con el objeto de facilitar alcanzar los objetivos fijados por el diseño curricular.

6.1 Atención a la diversidad

Se realizará un seguimiento individual del alumnado con el objeto de adecuar el proceso de enseñanza-aprendizaje a las características del mismo. Se pueden emplear los siguientes métodos:

- Planteamiento de actividades y cuestionarios para fijar el nivel de conocimientos previos.
- Observación de la actitud diaria del alumnado.
- Evaluación de la capacidad del educando para realizar procedimientos técnicos con el equipo y su habilidad para la resolución de los problemas.
- Elaboración de trabajos que hagan uso de la capacidad creativa y de los medios y recursos del Centro.
- Integración de los alumnos y alumnas con problemas en grupos de trabajo mixtos y diversos para que en ningún momento se sientan discriminados.

6.2 Adaptaciones de acceso

Adaptaciones de acceso al currículo, condiciones físicas del Centro y del aula y recursos materiales, dentro de las condiciones y medidas previstas por el Centro.

Medidas metodológicas, curriculares y organizativas, que básicamente serán:

- Modificación de la organización espacial: para que puedan sacar más partido de lo que se vea o se oiga en clase y garantizando su comodidad y movilidad.
- Priorización y secuenciación de contenidos (resaltando los procedimientos), con posibilidad de eliminar contenidos secundarios.
- En los agrupamientos: fomentando la integración y la ayuda entre compañeros.
- Adaptando los tiempos y ritmos de aprendizaje, a cada alumno/a.
- Variedad de recursos didácticos en función de las necesidades, uso de técnicas de estudio (con el Dpto. de Orientación) y alterando el nivel de abstracción o complejidad.
- Actividades alternativas y/o complementarias que respondan progresivamente a los diferentes ritmos de aprendizaje del alumnado del grupo:
- Las *actividades de refuerzo* se orientan a la superación de posibles dificultades de alumnos que no han alcanzado los objetivos, a través de la repetición de explicaciones y la búsqueda de ejemplos y casos prácticos.
- Las *actividades de ampliación*, se orientan a que el alumno/a que haya adquirido perfectamente los contenidos del tema, desarrolle al máximo los resultados de aprendizaje, usando todos los recursos disponibles. Consistirán en la investigación, de entre varios temas propuestos por el profesor, en la búsqueda de información y realización de trabajos.
- Empleo de variedad de técnicas e instrumentos de evaluación de los aprendizajes.

7. Evaluación

El art. 3.3 de la ORDEN de 29 de septiembre de 2010 establece que al término del proceso de enseñanza-aprendizaje, el alumnado obtendrá una calificación final para cada uno de los módulos profesionales en que esté matriculado y que para establecer dicha calificación los miembros del equipo docente considerarán el grado y nivel de adquisición de los resultados de aprendizaje establecidos para cada módulo profesional, de acuerdo con sus correspondientes criterios de evaluación.

En base al artículo anterior, en el apartado 9 de esta programación, se especifican los resultados de aprendizaje asociados a cada uno de los módulos profesionales, así como la ponderación asignada a cada uno de ellos. Igualmente, se especifica el peso de cada uno de los CE, para así poder medir si se ha logrado o por el contrario se han presentado dificultades en el proceso.

7.1 Instrumentos de evaluación

Se utilizarán los siguientes instrumentos de evaluación para comprobar el progreso y las dificultades del alumnado:

- Actividades teórico-prácticas sobre los contenidos tratados en el aula.
- Proyectos aplicados.
- Pruebas de aplicación teóricas y prácticas.

7.2 Calificación

Según establece el artículo 3, punto 3 de 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:

"Al término del proceso de enseñanza-aprendizaje, el alumnado obtendrá una calificación final para cada uno de los módulos profesionales en que esté matriculado. Para establecer dicha calificación los miembros del equipo docente considerarán el grado y nivel de adquisición de los resultados de aprendizaje establecidos para cada módulo profesional, de acuerdo con sus correspondientes criterios de evaluación y los objetivos generales relacionados, así como de la competencia general y las competencias profesionales, personales y sociales del título, establecidas en el perfil profesional del mismo y sus posibilidades de inserción en el sector profesional y de progreso en los estudios posteriores a los que pueda acceder."

7.2.1 Evaluación inicial

Durante el primer mes del curso, se realizará una evaluación inicial sobre los contenidos del módulo profesional con la finalidad de detectar posibles problemas que podamos tener durante el curso y adaptar los contenidos al nivel del alumnado.

Los resultados serán obtenidos a través de una prueba inicial en los primeros días de clase y observación directa del alumnado desde el inicio del curso hasta la evaluación.

Esta evaluación no afectará a la calificación final, solo tendrá carácter informativo.

7.2.2 Evaluaciones parciales

A lo largo del curso tendremos dos momentos en los que se evaluará al alumnado de manera parcial: una en enero y otra en mayo.

Para calcular la **calificación de cada evaluación parcial**, y dado que según la normativa vigente debe ser un número entero comprendido entre el 1 y el 10, se procederá de la siguiente manera:

La calificación de cada evaluación parcial será la media aritmética de las calificaciones obtenidas en todos los Resultados de Aprendizaje evaluados hasta el momento. A su vez, la calificación de cada Resultado de Aprendizaje se obtendrá mediante la media aritmética de las calificaciones de los Criterios de Evaluación que lo componen.

Esta calificación solo será efectiva en el caso de que el alumno haya superado todos y cada uno de los Resultados de Aprendizaje impartidos en la evaluación. En el caso de que el alumno no haya superado algún Resultado de Aprendizaje y el resultado de la anterior fórmula sea un número entero mayor o igual que 5, la calificación efectiva de la evaluación será igual a 4 hasta que el alumno supere todos los Resultados de Aprendizaje pendientes, momento en el que se realizará el recálculo de las calificaciones tal y como se indica en el apartado **Evaluación Ordinaria**.

7.2.3 Evaluación final ordinaria

La calificación de la evaluación final se expresa en la escala de 1 a 10 sin decimales considerándose superado el módulo a las alumnas o alumnos que obtengan una puntuación igual o superior a 5.

Para la evaluación final, la calificación será la media aritmética de todos los Resultados de Aprendizaje evaluados a lo largo del curso. La superación de un trimestre no implica la superación de los anteriores. Si el alumnado supera el segundo trimestre, pero no el primero, se considerará el curso no superado.

7.2.4 Periodo de refuerzo y/o recuperación

Al finalizar el periodo ordinario podemos encontrarnos con alumnos o alumnas que no hayan superado el módulo, por lo que contaremos con un amplio plazo para intentar dotar a los estudiantes de los Resultados de Aprendizajes del módulo para obtener una calificación positiva en la evaluación final. En este periodo se ha considerado oportuno llevar a cabo las siguientes acciones:

- Se analizarán a modo de síntesis los conceptos fundamentales.
- Los alumnos y alumnas resolverán supuestos prácticos.
- Posteriormente se celebrará una prueba de evaluación.

Igualmente, podemos encontrarnos con la situación de alumnos o alumnas que han superado las dos evaluaciones parciales, no estén satisfechos con su calificación y soliciten una oportunidad de intentar mejorarlas. El docente, tal como establece la normativa, atenderá a dicha demanda y planificará actividades para tal fin:

- Se efectuarán aportaciones de situaciones más complejas de los supuestos prácticos.
- Posteriormente, se presentarán a una prueba de evaluación.

7.2.5 Reclamación del alumnado

El alumnado tiene derecho a formular reclamaciones sobre las decisiones y calificaciones del proceso de evaluación. Así lo establece el artículo 19 de la Orden de 29 de septiembre de 2010, que concede un plazo de 2 días hábiles posteriores a la

publicación o notificación de las notas para hacerla efectiva y encarga al departamento correspondiente resolver, emitiendo un informe al efecto.

8. Evaluación y seguimiento de la programación

8.1 Evaluación del proceso de enseñanza

En este caso se pretende valorar la idoneidad de la programación didáctica y el entorno donde se pone en práctica, comparando los resultados alcanzados con los objetivos que se pretendían conseguir.

También es conveniente la evaluación del profesorado como parte del proceso de enseñanza. Esto permite garantizar la calidad del mismo, pues la propia revisión del trabajo realizado por el docente, es el mejor camino para detectar los puntos débiles del proceso de enseñanza-aprendizaje, siempre para tomar las medidas oportunas que permitan reforzar esos puntos débiles con el fin de mejorar la calidad de la enseñanza impartida.

La autoevaluación posibilita:

- Tener una técnica apropiada de percepción de la actuación docente.
- Una ayuda para reflexionar sobre éxitos y fracasos. Para modificar la forma de enseñar y evaluar.
- Un método que facilita el crecimiento y desarrollo profesional.
- Una herramienta que permite identificar las necesidades de formación del docente.
- Un instrumento para la evaluación del docente, por y para él.

La evaluación del proceso de enseñanza no debe ser considerada por el profesorado como un método de inspección que detecte la competencia o no. Debe entenderse como una práctica de auto sensibilización en los valores más adecuados para la enseñanza:

- Colaboración frente a individualismo.
- Autonomía frente a dependencia.
- Comunicación frente al aislamiento.
- Autorregulación y crítica colaborativa frente a directrices externas.

Hemos de considerar la autoevaluación como un componente esencial dentro del proceso general de la evaluación académica. Esta se llevará a cabo fundamentalmente por la realimentación proporcionada por el propio alumnado, en forma de resultados de las prácticas, exámenes, proyectos, trabajos de investigación, etc. También por las opiniones que podamos recibir de otros compañeros del Departamento y del Equipo Directivo.

Además, está previsto realizar un cuestionario que se pasará a todos los alumnos y alumnas al final del curso, para conocer la impresión que han tenido y aspectos que mejorarían o cambiarían.

9. Módulos profesionales

Los módulos profesionales de este curso de especialización quedan desarrollados en el anexo I de este real decreto, cumpliendo lo previsto en el artículo 10, apartado 3 del Real Decreto 1147/2011, de 29 de julio, por el que se establece la ordenación general de la formación profesional del sistema educativo. Son los que a continuación se relacionan:

- Incidentes de ciberseguridad.
- Bastionado de redes y sistemas.
- Puesta en producción segura.
- Análisis forense informático.
- Hacking ético.
- Normativa de ciberseguridad.

10. Módulo Profesional. Incidentes de ciberseguridad (5021)

10.1 Resultados de aprendizaje

El Real Decreto 479/2020, de 7 de abril, establece los siguientes Resultados de aprendizaje, que se presentan desglosados según sus elementos:

RA	LOGRO	OBJETO	ACCIONES EN EL CONTEXTO DE APRENDIZAJE
RA 1	Desarrolla	planes de prevención y concienciación en ciberseguridad	estableciendo normas y medidas de protección
RA 2	Analiza	incidentes de ciberseguridad	utilizando herramientas, mecanismos de detección y alertas de seguridad
RA 3	Investiga	incidentes de ciberseguridad	analizando los riesgos implicados y definiendo las posibles medidas a adoptar
RA 4	Implementa	medidas de ciberseguridad en redes y sistemas	respondiendo a los incidentes detectados y aplicando las técnicas de protección adecuadas
RA 5	Detecta y documenta	incidentes de ciberseguridad	siguiendo procedimientos de actuación establecidos.

10.2 Contenidos

10.2.1 Contenidos del currículo

Los contenidos son el conjunto de conocimientos, habilidades, destrezas y actitudes cuya asimilación y apropiación por los que aprenden se consideran esenciales para su ejercicio profesional.

La concreción de los mismos y su secuenciación de aprendizaje se han realizado atendiendo a los siguientes criterios:

- Adecuación a los contenidos básicos reflejados en la normativa estatal, el Real Decreto 479/2020, de 7 de abril.
- Adecuación de los contenidos al requerido en el entorno laboral local.
- Adaptación de los contenidos a los conocimientos previos del alumnado.
- Continuidad y progresión en los contenidos.
- Equilibrio entre las secuencias de conceptos, objetivos y capacidades.
- Interrelación entre contenidos.

10.2.2 Selección y secuencia de contenidos

Unidades didácticas		Sesiones	RA	Criterios	Trimestre
UD1	Desarrollo de planes de prevención y concienciación	30	RA1	a)..e)	1º
UD2	Analiza incidentes de ciberseguridad	35	RA2	a)..e)	1º
UD3	Investiga incidentes de ciberseguridad	30	RA3	a)..e)	2º
UD4	Implementa medidas de ciberseguridad en redes y sistemas	35	RA4	a)..f)	2º
UD5	Documenta y notifica incidentes de ciberseguridad	20	RA5	a)..e)	2º

10.2.3 Tratamiento de temas transversales

Los temas transversales -no específicos de la materia- y su tratamiento, están vinculados a las situaciones que se presenten en las actividades propuestas, distribuidos a lo largo del módulo.

- Se considerarán los siguientes temas transversales:
- Sostenibilidad medioambiental.
- Educación del consumidor.
- Salud laboral.
- Educación para la igualdad de oportunidades entre ambos sexos.
- Igualdad de oportunidades y respeto a personas de otras culturas y credos.
- Inserción laboral.
- Creación de empleo.
- Educación para la paz y la convivencia.
- Educación para la ciudadanía.
- Manejo de documentación técnica en irrors fixed rv3@slimbnglés.

10.2.4 Interdisciplinaridad

En el curso, todos los módulos se relacionan íntimamente con el presente, con cuyo profesorado debemos coordinarnos:

- 5022. Bastionado de redes y sistemas.
- 5023. Puesta en producción segura.
- 5024. Análisis forense informático.
- 5025. Hacking ético.
- 5026. Normativa de ciberseguridad.

10.3 Evaluación

A continuación, se especifica el peso de cada uno de los resultados de aprendizaje, así como el de los criterios de evaluación que lo componen. La mayor o menor ponderación de los criterios se obtiene en base al nivel de dificultad y contenidos a desarrollar

para cada criterio. La calificación de cada resultado de aprendizaje será la media ponderada de los distintos criterios de evaluación.

RA	Criterios de evaluación	Peso RA	Peso CE	Técnica
RA1	a) Se han definido los principios generales de la organización en materia de ciberseguridad, que deben ser conocidos y apoyados por la dirección de la misma.	15%	6,0%	Actividades teórico - prácticas
	b) Se ha establecido una normativa de protección del puesto de trabajo.		3,0%	
	c) Se ha definido un plan de concienciación de ciberseguridad dirigido a los empleados.		3,0%	
	d) Se ha desarrollado el material necesario para llevar a cabo las acciones de concienciación dirigidas a los empleados.		2,0%	
	e) Se ha realizado una auditoría para verificar el cumplimiento del plan de prevención y concienciación de la organización.		1,0%	
RA2	a) Se ha clasificado y definido la taxonomía de incidentes de ciberseguridad que pueden afectar a la organización.	25%	2,0%	Actividades teórico - prácticas
	b) Se han establecido controles, herramientas y mecanismos de monitorización, identificación, detección y alerta de incidentes.		11,0%	
	c) Se han establecido controles y mecanismos de detección e identificación de incidentes de seguridad física.		1,0%	
	d) Se han establecido controles, herramientas y mecanismos de monitorización, identificación, detección y alerta de incidentes a través de la investigación en fuentes abiertas (OSINT: Open Source Intelligence).		6,0%	
	e) Se ha realizado una clasificación, valoración, documentación y seguimiento de los incidentes detectados dentro de la organización.		5,0%	
RA3	a) Se han recopilado y almacenado de forma segura evidencias de incidentes de ciberseguridad que afectan a la organización.	20%	3,0%	Actividades teórico - prácticas
	b) Se ha realizado un análisis de evidencias.		4,0%	
			5,0%	

RA	Criterios de evaluación	Peso RA	Peso CE	Técnica
	c) Se ha realizado la investigación de incidentes de ciberseguridad.			
	d) Se ha intercambiado información de incidentes, con proveedores y/o organismos competentes que podrían hacer aportaciones al respecto.		4,0%	
	e) Se han iniciado las primeras medidas de contención de los incidentes para limitar los posibles daños causados.		4,0%	
RA4	a) Se han desarrollado procedimientos de actuación detallados para dar respuesta, mitigar, eliminar o contener los tipos de incidentes de ciberseguridad más habituales.	30%	6,0%	Actividades teórico - prácticas
	b) Se han preparado respuestas ciberresilientes ante incidentes que permitan seguir prestando los servicios de la organización y fortaleciendo las capacidades de identificación, detección, prevención, contención, recuperación y cooperación con terceros.		6,0%	
	c) Se ha establecido un flujo de toma de decisiones y escalado de incidentes interno y/o externo adecuados.		6,0%	
	d) Se han llevado a cabo las tareas de restablecimiento de los servicios afectados por un incidente hasta confirmar la vuelta a la normalidad.		6,0%	
	e) Se han documentado las acciones realizadas y las conclusiones que permitan mantener un registro de “lecciones aprendidas”.		3,0%	
	f) Se ha realizado un seguimiento adecuado del incidente para evitar que una situación similar se vuelva a repetir.		3,0%	
RA5	a) Se ha desarrollado un procedimiento de actuación detallado para la notificación de incidentes de ciberseguridad en los tiempos adecuados.	10%	6,0%	Actividades teórico - prácticas
	b) Se ha notificado el incidente de manera adecuada al personal interno de la organización		1,0%	

RA	Criterios de evaluación	Peso RA	Peso CE	Técnica
	responsable de la toma de decisiones.			
	c) Se ha notificado el incidente de manera adecuada a las autoridades competentes en el ámbito de la gestión de incidentes de ciberseguridad en caso de ser necesario.		1,0%	
	d) Se ha notificado formalmente el incidente a los afectados, personal interno, clientes, proveedores, etc., en caso de ser necesario.		1,0%	
	e) Se ha notificado el incidente a los medios de comunicación en caso de ser necesario.		1,0%	

Para el cálculo de la calificación de cada evaluación parcial se tendrán en cuenta únicamente los criterios impartidos hasta la finalización de dicha evaluación. Dado que según la normativa vigente la calificación debe ser un entero numérico comprendido entre el 1 y el 10, el cálculo se realizará de la siguiente manera:

La calificación de cada criterio se obtendrá sobre su peso, es decir si un criterio tiene un peso del 1% su nota será un número real comprendido entre el 0 y el 1. Por otra parte, la calificación de cada uno de los resultados de aprendizaje se obtendrá mediante el redondeo de lo que resulte al aplicar la siguiente fórmula a los CE pertenecientes al RA:

Calificación Ev. Parcial \=(Calificación CE *%)

Esta misma fórmula permitirá obtener la nota parcial, no obstante esta calificación sólo será efectiva en el caso de que el alumno haya superado todos y cada uno de los Resultados de Aprendizaje impartidos en la evaluación. En el caso de que el alumno no haya superado algún Resultado de Aprendizaje y el resultado de la anterior fórmula sea un número entero mayor o igual que 5, la calificación efectiva de la evaluación será igual a 4 hasta que el alumno supere todos los Resultados de Aprendizaje pendientes, momento en el que se realizará el recálculo de las calificaciones tal y como se indica en el apartado Evaluación Ordinaria.

La superación de una evaluación, no implica la superación del resto. Si llegado el caso de que alguna alumna o alumno superará la segunda evaluación, pero no hubiere superado la anterior, implica la no superación del curso, y por ello en el informe de evaluación se consignará como no superada. No se conservan partes -aprobadas o suspensas- de un curso a otro. Para el alumnado que no supere alguna de las evaluaciones, se prepararon actividades personalizadas de refuerzo/recuperación para el periodo de recuperación de fin de curso, siendo estas actividades de carácter obligatorio.

Se utilizarán los siguientes instrumentos de evaluación para comprobar el progreso y las dificultades del alumnado:

Trabajo diario individual y grupal:

- Observación sistemática sobre el trabajo en clase.
- Anotaciones sobre participación.
- Seguimiento de las actividades programadas y realizadas en el aula.
- Puntualidad y asistencia.

Prácticas y proyectos, individuales y grupales:

- Realización de prácticas planteadas durante el curso.
- Presentaciones sobre proyectos generados.

Pruebas teórico/prácticas individuales:

- Pruebas con ejercicios escritos y/o en el ordenador.

10.4 Bibliografía y referencias

10.4.1 Bibliografía de departamento

- Cómo protegerse de los peligros en internet, Jose Carlos Gallego Cano. Ed. 0xWORD
- Blue Team. Centro de operaciones de ciberseguridad. Numa Editorial.
- Incident Response in the Age of Cloud. Erdal Ozkaya. Packt .
- Applied Incident Response. Steve Anson. Wiley.

10.4.2 Bibliografía de aula

Al alumnado se le facilitará en cada unidad didáctica unos apuntes/presentaciones elaborados por el profesor, basados en los libros de texto que encontramos en la bibliografía de departamento y en las referencias web.

10.4.3 Referencias web

Todas las referencias usadas, se encuentran disponibles en la extensión virtual del aula que proporciona la plataforma Moodle del Centro, destacando:

- https://www.incibe.es/
- https://www.ccn-cert.cni.es/

11. Módulo Profesional. Bastionado de redes y sistemas (5022)

11.1 Resultados de aprendizaje

El Real Decreto 479/2020, de 7 de abril, establece los siguientes Resultados de aprendizaje, que se presentan desglosados según sus elementos:

RA	LOGRO	OBJETO	ACCIONES EN EL CONTEXTO DE APRENDIZAJE
RA 1	Diseña	Planes de securización	Incorporando buenas prácticas para el bastionado de sistemas y redes
RA 2	Configura	Sistemas de control de acceso y autenticación de personas	Preservando la confidencialidad y privacidad de los datos
RA 3	Administra	Credenciales de acceso a sistemas informáticos	Aplicando los requisitos de funcionamiento y seguridad establecidos
RA 4	Diseña	Redes de computadores	Contemplando los requisitos de seguridad
RA 5	Configura	Dispositivos y sistemas informáticos	Cumpliendo los requisitos de seguridad
RA 6	Configura	Dispositivos para la instalación de sistemas informáticos	Minimizando las probabilidades de exposición a ataques
RA 7	Configura	Sistemas informáticos	Minimizando las probabilidades de exposición a ataques

11.2 Contenidos

11.2.1 Contenidos del currículo

Los contenidos son el conjunto de conocimientos, habilidades, destrezas y actitudes cuya asimilación y apropiación por los que aprenden se consideran esenciales para su ejercicio profesional.

La concreción de los mismos y su secuenciación de aprendizaje se han realizado atendiendo a los siguientes criterios:

- Adecuación a los contenidos básicos reflejados en la normativa estatal, el Real Decreto 479/2020, de 7 de abril.
- Adecuación de los contenidos al requerido en el entorno laboral local.
- Adaptación de los contenidos a los conocimientos previos del alumnado.
- Continuidad y progresión en los contenidos.
- Equilibrio entre las secuencias de conceptos, objetivos y capacidades.
- Interrelación entre contenidos.

11.2.2 Selección y secuencia de contenidos

Unidades didácticas		Sesiones	RA	Criterios	Timestre
UD1	Zero Trust	20	RA4, RA6	6a), 6b), 6c), 6d), 6e), 4a), 4b), 4c)	1º
UD2	Least-Privilege	20	RA2, RA3, RA4, RA7	2a), 2b), 2c), 2d), 2e). 3a), 4e), 7a) 7b)	1º
UD3	Reduce Attack Surface	20	RA5	5b)	1º
UD4	Under Control	40	RA3, RA4, RA5, RA7	3b), 3c), 3d), 3e), 4d), 5a), 5e), 7c), 7d), 7e)	2º
UD5	Risk Management	10	RA1	1a), 1b), 1c), 1d), 1e), 1f)	2º
UD6	Defense in Depth	40	RA5	5c), 5d)	2º

11.2.3 Tratamiento de temas transversales

Los temas transversales -no específicos de la materia- y su tratamiento, están vinculados a las situaciones que se presenten en las actividades propuestas, distribuidos a lo largo del módulo.

Se considerarán los siguientes temas transversales:

- Sostenibilidad medioambiental.
- Educación del consumidor.
- Salud laboral.
- Educación para la igualdad de oportunidades entre ambos sexos.
- Igualdad de oportunidades y respeto a personas de otras culturas y credos.
- Inserción laboral.
- Creación de empleo.
- Educación para la paz y la convivencia.
- Educación para la ciudadanía.
- Manejo de documentación técnica en inglés.

11.2.4 Interdisciplinaridad

En el curso, todos los módulos se relacionan íntimamente con el presente, con cuyo profesorado debemos coordinarnos:

- 5021. Incidentes de ciberseguridad.
- 5022. Bastionado de redes y sistemas.
- 5023. Puesta en producción segura.
- 5025. Hacking ético.
- 5026. Normativa de ciberseguridad.

11.3 Evaluación

A continuación, se especifica el peso de cada uno de los resultados de aprendizaje, así como el de los criterios de evaluación que lo componen. La mayor o menor ponderación de los criterios se obtiene en base al nivel de dificultad y contenidos a desarrollar para cada criterio.

Resultados de Aprendizaje	Criterios de evaluación	% RA	Peso C.E.	Técnica
RA1. Diseña planes de securización incorporando buenas prácticas para el bastionado de sistemas y redes.	a) Se han identificado los activos, las amenazas y vulnerabilidades de la organización.	15%	B	Proyectos aplicados y pruebas teórico-prácticas
	b) Se ha evaluado las medidas de seguridad actuales.		B	
	c) Se ha elaborado un análisis de riesgo de la situación actual en ciberseguridad de la organización		I	
	d) Se ha priorizado las medidas técnicas de seguridad a implantar en la organización teniendo también en cuenta los principios de la Economía Circular.		A	
	e) Se ha diseñado y elaborado un plan de medidas técnicas de seguridad a implantar en la organización, apropiadas para garantizar un nivel de seguridad adecuado en función de los riesgos de la organización.		I	
	f) Se han identificado las mejores prácticas en base a estándares, guías y políticas de securización adecuadas para el bastionado de los sistemas y redes de la organización.		I	
RA2. Configura sistemas de control de acceso y autenticación de personas preservando la confidencialidad y privacidad de los datos.	a) Se han definido los mecanismos de autenticación en base a distintos / múltiples factores (físicos, inherentes y basados en el conocimiento), existentes.	7,5%	B	Proyectos aplicados y pruebas teórico-prácticas
	b) Se han definido protocolos y políticas de autenticación basados en contraseñas y frases de paso, en base a las		B	

Resultados de Aprendizaje	Criterios de evaluación	% RA	Peso C.E.	Técnica
	principales vulnerabilidades y tipos de ataques.			
	c) Se han definido protocolos y políticas de autenticación basados en certificados digitales y tarjetas inteligentes, en base a las principales vulnerabilidades y tipos de ataques.		B	
	d) Se han definido protocolos y políticas de autenticación basados en tokens, OTPs, etc., en base a las principales vulnerabilidades y tipos de ataques.		B	
	e) Se han definido protocolos y políticas de autenticación basados en características biométricas, según las principales vulnerabilidades y tipos de ataques.		B	
RA3. Administra credenciales de acceso a sistemas informáticos aplicando los requisitos de funcionamiento y seguridad establecidos.	a) Se han identificado los tipos de credenciales más utilizados.	7,5%	B	Proyectos aplicados y pruebas teórico-prácticas
	b) Se han generado y utilizado diferentes certificados digitales como medio de acceso a un servidor remoto.		I	
	c) Se ha comprobado la validez y la autenticidad de un certificado digital de un servicio web.		I	
	d) Se han comparado certificados digitales válidos e inválidos por diferentes motivos.		I	
	e) Se ha instalado y configurado un servidor seguro para la administración de credenciales (tipo RADIUS -		I	

Resultados de Aprendizaje	Criterios de evaluación	% RA	Peso C.E.	Técnica
	Remote Access Dial In User Service).			
RA4. Diseña redes de computadores contemplando los requisitos de seguridad.	a) Se ha incrementado el nivel de seguridad de una red local plana segmentándola físicamente y utilizando técnicas y dispositivos de enrutamiento.	15%	B	Proyectos aplicados y pruebas teórico-prácticas
	b) Se ha optimizado una red local plana utilizando técnicas de segmentación lógica (VLANs).		I	
	c) Se ha adaptado un segmento de una red local ya operativa utilizando técnicas de subnetting para incrementar su segmentación respetando los direccionamientos existentes.		I	
	d) Se han configurado las medidas de seguridad adecuadas en los dispositivos que dan acceso a una red inalámbrica (routers, puntos de acceso, etc.).		B	
	e) Se ha establecido un túnel seguro de comunicaciones entre dos sedes geográficamente separadas.		I	
RA5. Configura dispositivos y sistemas informáticos cumpliendo los requisitos de seguridad.	a) Se han configurado dispositivos de seguridad perimetral acorde a una serie de requisitos de seguridad.	20%	B	Proyectos aplicados y pruebas teórico-prácticas
	b) Se han detectado errores de configuración de dispositivos de red mediante el análisis de tráfico.		I	
	c) Se han identificado comportamientos no deseados en una red a través del análisis de los registros (Logs), de un cortafuego.		I	
	d) Se han implementado contramedidas frente a		B	

Resultados de Aprendizaje	Criterios de evaluación	% RA	Peso C.E.	Técnica
	comportamientos no deseados en una red.			
	e) Se han caracterizado, instalado y configurado diferentes herramientas de monitorización.		B	
RA6. Configura dispositivos para la instalación de sistemas informáticos minimizando las probabilidades de exposición a ataques.	a) Se ha configurado la BIOS para incrementar la seguridad del dispositivo y su contenido minimizando las probabilidades de exposición a ataques.	15%	B	Proyectos aplicados y pruebas teórico-prácticas
	b) Se ha preparado un sistema informático para su primera instalación teniendo en cuenta las medidas de seguridad necesarias.		B	
	c) Se ha configurado un sistema informático para que un actor malicioso no pueda alterar la secuencia de arranque con fines de acceso ilegítimo.		I	
	d) Se ha instalado un sistema informático utilizando sus capacidades de cifrado del sistema de ficheros para evitar la extracción física de datos.		B	
	e) Se ha particionado el sistema de ficheros del sistema informático para minimizar riesgos de seguridad.		B	
RA7. Configura sistemas informáticos minimizando las probabilidades de exposición a ataques.	a) Se han enumerado y eliminado los programas, servicios y protocolos innecesarios que hayan sido instalados por defecto en el sistema.	20%	B	Proyectos aplicados y pruebas teórico-prácticas
	b) Se han configurado las características propias del sistema informático para imposibilitar el acceso ilegítimo mediante técnicas de explotación de procesos.		I	
	c) Se ha incrementado la seguridad del sistema de		I	

Resultados de Aprendizaje	Criterios de evaluación	% RA	Peso C.E.	Técnica
	administración remoto SSH y otros.			
	d) Se ha instalado y configurado un Sistema de detección de intrusos en un Host (HIDS) en el sistema informático.		B	
	e) Se han instalado y configurado sistemas de copias de seguridad.		B	

La calificación de cada resultado de aprendizaje será la media ponderada de los distintos criterios de evaluación, repartidos en los siguientes pesos:
- Básicos (B): 4.
- Intermedios (I): 2.
- Avanzados (A): 1.
Por ejemplo, si un resultado de aprendizaje tiene 6 criterios de evaluación repartidos de la siguiente forma: c1 (básico), c2 (básico), c3 (básico), c4 (intermedio), c5 (intermedio) y c6 (avanzado), se calcularía la calificación sumando las multiplicaciones de la nota de cada criterio por su peso correspondiente y dividiendo el resultado por la suma de todos los pesos. La fórmula matemática sería la siguiente:

$$ \text{Calificación del RA} = c_{14} + c_{24} + c_{34} + c_{42} + c_{52} + c_{614} + 4 + 4 + 2 + 2 + 1 $$

El alumnado que supere o iguale la calificación de 5 en cada uno de los Resultados de Aprendizaje tras aplicar estas ponderaciones, aprueba el módulo.
El alumno también tendrá posibilidad de subir nota y podrá solicitar al profesor un plan de mejora que consistirá en un conjunto de trabajos, prácticas o pruebas sobre los contenidos a los que están asociados los resultados de aprendizaje en los que desea mejorar su calificación.
Si no se han superado los contenidos del módulo a finales del mes de mayo, se desarrollará la recuperación de los R.A pendientes durante el mes de junio y consistirá en un conjunto de prácticas y/o pruebas sobre los contenidos a los que están asociados los resultados de aprendizaje no superados.

11.4 Bibliografía y referencias

11.4.1 Bibliografía de departamento

- Hardening de servidores GNU/Linux. 4ªEdición. Ed. 0xWORD
- Máxima Seguridad en Windows: Secretos Técnicos. 5ª Edición. Ed. 0xWORD
- Mastering Linux Security and Hardening. 2ª Edición. Ed. Packt.
- Mastering Windows Security and Hardening. Ed. Packt.
- Network Security Strategies. Ed. Packt.

11.4.2 Bibliografía de aula

Al alumnado se le facilitará en cada unidad didáctica unos apuntes/presentaciones elaborados por el profesor, basados en los libros de texto que encontramos en la bibliografía de departamento y en las referencias web.

11.4.3 Referencias web

Todas las referencias usadas, se encuentran disponibles en la extensión virtual del aula que proporciona la plataforma Moodle del Centro.

12. Módulo Profesional. Puesta en producción segura (5023)

12.1 Resultados de aprendizajes

Los Resultados de Aprendizaje establecidos por la normativa para este módulo de Puesta en producción segura son 5 que se enumeran a continuación y se presentan desglosado según sus elementos:

RA	LOGRO	OBJETO	ACCIONES EN EL CONTEXTO DE APRENDIZAJE
RA 1	Prueba	Aplicaciones web y aplicaciones para dispositivos móviles	Analizando la estructura del código y su modelo de ejecución
RA 2	Determina	El nivel de seguridad requerido por aplicaciones	Identificando los vectores de ataque habituales y sus riesgos asociados
RA 3	Detecta y corrige	Vulnerabilidades de aplicaciones web	Analizando su código fuente y configurando servidores web
RA 4	Detecta	Problemas de seguridad en las aplicaciones móviles	Monitorizando su ejecución y analizando ficheros y datos
RA 5	Implanta	Sistemas seguros de desplegado de software	Utilizando herramientas para la automatización de la construcción de sus elementos.

12.2 Contenidos

12.2.1 Contenidos del currículo

Los contenidos son el conjunto de conocimientos, habilidades, destrezas y actitudes cuya asimilación y apropiación por los que aprenden se consideran esenciales para su ejercicio profesional.

La concreción de los mismos y su secuenciación de aprendizaje se han realizado atendiendo a los siguientes criterios:

- Adecuación a los contenidos básicos reflejados en la normativa estatal, el Real Decreto 479/2020, de 7 de abril.
- Adecuación de los contenidos al requerido en el entorno laboral local.
- Adaptación de los contenidos a los conocimientos previos del alumnado.
- Continuidad y progresión en los contenidos.
- Equilibrio entre las secuencias de conceptos, objetivos y capacidades.
- Interrelación entre contenidos.

12.2.2 Selección y secuencia de contenidos

Unidades didácticas		Sesiones	RA	Criterios	Trimestre
UT1	Fundamentos del Software	16	RA1	a, b, c, d, e	1º
UT2	Verificación de seguridad en las aplicaciones	15	RA 2	a, b, c, d	1º
UT4	Detección y corrección vulnerabilidades	30	RA3	a, b, c, d, e, f, g	2º
					2º
UT3	Desplegado de software seguro	44	RA5	a, b, c, d, e	2º
UT5	Seguridad en aplicaciones móviles	15	RA4	a, b, c, d, e	2º

12.2.3 Tratamiento de temas transversales

Los temas transversales -no específicos de la materia- y su tratamiento, están vinculados a las situaciones que se presenten en las actividades propuestas, distribuidos a lo largo del módulo.

Se considerarán los siguientes temas transversales:

- Sostenibilidad medioambiental.
- Educación del consumidor.
- Salud laboral.
- Educación para la igualdad de oportunidades entre ambos sexos.
- Igualdad de oportunidades y respeto a personas de otras culturas y credos.
- Inserción laboral.
- Creación de empleo.
- Educación para la paz y la convivencia.
- Educación para la ciudadanía.
- Manejo de documentación técnica en inglés.

12.2.4 Interdisciplinaridad

En el curso, todos los módulos se relacionan íntimamente con el presente, con cuyo profesorado debemos coordinarnos:

- 5021. Incidentes de ciberseguridad.
- 5022. Bastionado de redes y sistemas.
- 5024. Análisis Forense Informático.
- 5025. Hacking ético.
- 5026. Normativa de ciberseguridad.

12.3 Evaluación

Resultados de Aprendizaje	Criterios de evaluación	% RA	Peso C.E.	Técnicas
RA1 Prueba aplicaciones web y aplicaciones para dispositivos móviles analizando la estructura del código y su modelo de ejecución.	a) Se han comparado diferentes lenguajes de programación de acuerdo a sus características principales.	11 %	2 %	Proyecto de desarrollo y testing
	b) Se han descrito los diferentes modelos de ejecución de software.		2%	
	c) Se han reconocido los elementos básicos del código fuente, dándoles significado.		2 %	
	d) Se han ejecutado diferentes tipos de prueba de software.		3 %	
	e) Se han evaluado los lenguajes de programación de acuerdo a la infraestructura de seguridad que proporcionan.		2 %	
RA2 Determina el nivel de seguridad requerido por aplicaciones identificando los vectores de ataque habituales y sus riesgos asociados.	a) Se han caracterizado los niveles de verificación de seguridad en aplicaciones establecidos por los estándares internacionales (ASVS, “Application Security Verification Standard”).	12 %	2 %	Trabajo: Análisis y verificación de software
	b) Se ha identificado el nivel de verificación de seguridad requerido por las aplicaciones en función de sus riesgos de acuerdo a estándares reconocidos.		2 %	
	c) Se han enumerado los requisitos de verificación necesarios asociados al nivel de seguridad establecido.		4 %	
	d) Se han reconocido los principales riesgos de las aplicaciones desarrolladas, en función de sus características.		4 %	
RA3 Detecta y corrige vulnerabilidades de aplicaciones web	a) Se han validado las entradas de los usuarios.	35 %	5 %	Actividades teórico / prácticas

Resultados de Aprendizaje	Criterios de evaluación	% RA	Peso C.E.	Técnicas
analizando su código fuente y configurando servidores web.				
	b) Se han detectado riesgos de inyección tanto en el servidor como en el cliente.		5 %	
	c) Se ha gestionado correctamente la sesión del usuario durante el uso de la aplicación.		5 %	
	d) Se ha hecho uso de roles para el control de acceso.		5 %	
	e) Se han utilizado algoritmos criptográficos seguros para almacenar las contraseñas de usuario.		5 %	
	f) Se han configurado servidores web para reducir el riesgo de sufrir ataques conocidos.		5 %	
	g) Se han incorporado medidas para evitar los ataques a contraseñas, envío masivo de mensajes o registros de usuarios a través de programas automáticos (bots).		5 %	
RA4 Detecta problemas de seguridad en las aplicaciones para dispositivos móviles, monitorizando su ejecución y analizando ficheros y datos	a) Se han comparado los diferentes modelos de permisos de las plataformas móviles.	10%	2 %	Actividades teórico / prácticas
	b) Se han descrito técnicas de almacenamiento seguro de datos en los dispositivos, para evitar la fuga de información.		2 %	
	c) Se ha implantado un sistema de validación de compras integradas en la aplicación haciendo uso de validación en el servidor.		2 %	
	d) Se han utilizado herramientas de monitorización de tráfico de red para detectar el uso de protocolos inseguros de		2 %	

Resultados de Aprendizaje	Criterios de evaluación	% RA	Peso C.E.	Técnicas
	comunicación de las aplicaciones móviles.			
	e) Se han inspeccionado binarios de aplicaciones móviles para buscar fugas de información sensible.		2 %	
RA5 Implanta sistemas seguros de desplegado de software, utilizando herramientas para la automatización de la construcción de sus elementos.	a) Se han identificado las características, principios y objetivos de la integración del desarrollo y operación del software.	32 %	2%	Proyecto de puesta en producción
	b) Se han implantado sistemas de control de versiones, administrando los roles y permisos solicitados.		6%	
	c) Se han instalado, configurado y verificado sistemas de integración continua, conectándolos con sistemas de control de versiones.		6%	
	d) Se han planificado, implementado y automatizado planes de desplegado de software.		6%	
	e) Se ha evaluado la capacidad del sistema desplegado para reaccionar de forma automática a fallos.		4%	
	f) Se han documentado las tareas realizadas y los procedimientos a seguir para la recuperación ante desastres.		4%	
	g) Se han creado bucles de retroalimentación ágiles entre los miembros del equipo.		4%	

Todas las actividades son evaluables, sin entender la evaluación como un proceso de recogida de información, pero no todas son objeto de calificación, sólo aquellas recogidas en la tabla anterior y que hemos asociado a los criterios de evaluación y a los resultados de aprendizaje y se suelen denominar actividades de evaluación.

Además, llevaremos un registro en Excel de la calificación de cada RA, unidad, por actividad y criterio.

A la puntuación obtenida en la unidad se le aplicará la ponderación correspondiente a los Resultados de Aprendizaje, los cuales los RA 3 y 5 tienen mayor peso en la nota final, un 35% y 28% y los RA 1, 2 y 4 tienen entre 10-15%. Esta elección es debida a la

dedicación profesional que harán de este módulo, ya que los dos primeros resultados de aprendizaje comentados anteriormente, atañan un gran peso a nivel profesional, debido a que son parte del proceso habitual en el trabajo de la puesta en producción segura, y el resto de unidades componen recursos complementarios para ayudar a esa puesta en producción.

Para calificar cada unidad utilizaremos aquellas actividades de evaluación planteadas, en la que se ponderan los CE y para establecer la nota de cada evaluación, atenderemos a las siguientes consideraciones:

- En el primer trimestre se evaluarán completos los RA 1, 2 clasificando con el sistema de ponderación establecido, llevándolo al 100% para puntuar en Séneca por el sistema tradicional. Es decir, un alumno/a que tenga un diez en todas las unidades del primer trimestre habrá obtenido un 27% de los RA, pero nosotros puntuaremos con un 10 la evaluación.
- En la segunda se evaluarán del mismo modo los criterios que nos resten de los RA 3 y de forma completa 4 y 5 .
- Para calcular la nota final, como ya hemos comentado, se aplicarán los porcentajes de los todos Resultados de Aprendizaje (RA).
- Para obtener la nota de la evaluación extraordinaria se deberá realizar un plan de recuperación personalizado a cada alumno o alumna, dependiendo de los RA que no haya superado.

Para obtener una calificación positiva en los trimestres y en la nota final todos los RA deben ser alcanzados, tras aplicar el sistema de ponderación, en un 50% cada uno de los RA, lo que es lo mismo si traducimos al lenguaje de calificación tradicional la puntuación deberá ser al menos un 5, de forma excepcional el alumnado que obtenga un 5 en la valoración global, pero tenga algún RA con puntuación entre 4 y 4,99 habría superado el módulo, sin necesidad de recuperar ese RA. No obstante, los alumnos que alcance unos RA y otros no se le dará diferentes oportunidades de obtenerlos, realizándose pruebas de recuperación y oportunidades de mejoras del proyecto.

12.4 Bibliografía y referencias

12.4.1 Bibliografía de departamento

Ortega Candel, J. M. (2020). *Desarrollo seguro en ingeniería del software. Aplicaciones seguras con Android, NodeJS, Python y C++*. Marcombo.

12.4.2 Bibliografía de aula

Al alumnado se le facilitará en cada unidad didáctica unos apuntes/presentaciones elaborados por el profesor, basados en los libros de texto que encontramos en la bibliografía de departamento y en las referencias web.

12.4.3 Referencias web

Todas las referencias usadas, se encuentran disponibles en la extensión virtual del aula que proporciona la plataforma Moodle del Centro.

13. Módulo Profesional. Análisis forense informático (5024)

13.1 Resultados de aprendizaje

El Real Decreto 479/2020, de 7 de abril, establece para este módulo profesional, los siguientes Resultados de aprendizaje:

RA	LOGRO	OBJETO	ACCIONES EN EL CONTEXTO DE APRENDIZAJE
RA 1	Aplica	Metodologías de análisis forense	Caracterizando las fases de preservación, adquisición, análisis y documentación
RA 2	Realiza	Análisis forenses en dispositivos móviles	Aplicando metodologías establecidas, actualizadas y reconocidas
RA 3	Realiza	Análisis forenses en Cloud	Aplicando metodologías establecidas, actualizadas y reconocidas
RA 4	Realiza	Análisis forense en dispositivos de IoT	Aplicando metodologías establecidas, actualizadas y reconocidas
RA 5	Documenta	Análisis forenses	Elaborando informes que incluyan la normativa aplicable

13.2 Contenidos

13.2.1 Contenidos del currículo

Los contenidos son el conjunto de conocimientos, habilidades, destrezas y actitudes cuya asimilación y apropiación por los que aprenden se consideran esenciales para su ejercicio profesional.

La concreción de los mismos y su secuenciación de aprendizaje se han realizado atendiendo a los siguientes criterios:

- Adecuación a los contenidos básicos reflejados en la normativa estatal, el Real Decreto 479/2020, de 7 de abril.
- Adecuación de los contenidos al requerido en el entorno laboral local.
- Adaptación de los contenidos a los conocimientos previos del alumnado.
- Continuidad y progresión en los contenidos.
- Equilibrio entre las secuencias de conceptos, objetivos y capacidades.
- Interrelación entre contenidos.

Para una mejor compresión de contenido global, dividiremos el módulo en 9 bloques de contenido, intentando agrupar ordenadamente conceptos intrínsecamente conectados.

13.2.2 Selección y secuencia de contenidos

Unidades didácticas		Sesiones	RA	Criterios	Trimestre
UD1	Evidence Acquisition and Preservation	12	1	a, b, c	1º
UD2	Windows Forensics	32	1	d, e	1º
UD3	Documentation and Reporting	4	5	a, b, c, d, e, f	1º
UD4	Memory Forensics	12	1	g	2º
UD5	Linux Forensics	20	1	f	2º
UD6	Cloud Forensics	8	3	a, b, c, d, e, f	2º
UD7	Mobile Device Forensics	16	2	a, b, c, d	2º
UD8	IoT Forensics	16	4	a, b, c, d, e, f, g, h, i	2º

13.2.3 Tratamiento de temas transversales

Los temas transversales -no específicos de la materia- y su tratamiento, están vinculados a las situaciones que se presenten en las actividades propuestas, distribuidos a lo largo del módulo.

Se considerarán los siguientes temas transversales:

- Sostenibilidad medioambiental.
- Educación del consumidor.
- Salud laboral.
- Educación para la igualdad de oportunidades entre ambos sexos.
- Igualdad de oportunidades y respeto a personas de otras culturas y credos.
- Inserción laboral.
- Creación de empleo.
- Educación para la paz y la convivencia.
- Educación para la ciudadanía.
- Manejo de documentación técnica en inglés.

13.2.4 Interdisciplinaridad

En el curso, todos los módulos se relacionan íntimamente con el presente, con cuyo profesorado debemos coordinarnos:

- 5021. Incidentes de ciberseguridad.
- 5022. Bastionado de redes y sistemas.
- 5023. Puesta en producción segura.
- 5025. Hacking ético.
- 5026. Normativa de ciberseguridad.

13.3 Evaluación

A continuación, se especifica para cada unidad didáctica los resultados de aprendizaje y los criterios de evaluación correspondientes a la misma, así como los instrumentos de evaluación que se usarán para calificar cada uno de ellos.

Resultados de Aprendizaje	Criterios de evaluación	Instrumentos
RA1. Aplica metodologías de análisis forense caracterizando las fases de preservación, adquisición, análisis y documentación.	a) Se han identificado los dispositivos a analizar para garantizar la preservación de evidencias.	Proyecto integrado y actividades teórico-prácticas
	b) Se han utilizado los mecanismos y las herramientas adecuadas para la adquisición y extracción de las evidencias.	
	c) Se ha asegurado la escena y conservado la cadena de custodia.	
	d) Se ha documentado el proceso realizado de manera metódica.	
	e) Se ha considerado la línea temporal de las evidencias.	
	f) Se ha elaborado un informe de conclusiones a nivel técnico y ejecutivo.	
	g) Se han presentado y expuesto las conclusiones del análisis forense realizado.	
RA2. Realiza análisis forenses en dispositivos móviles, aplicando metodologías establecidas, actualizadas y reconocidas.	a) Se ha realizado el proceso de toma de evidencias en un dispositivo móvil.	Proyecto integrado y actividades teórico-prácticas
	b) Se han extraído, decodificado y analizado las pruebas conservando la cadena de custodia.	
	c) Se han generado informes de datos móviles, cumpliendo con los requisitos de la industria forense de telefonía móvil.	
	d) Se han presentado y expuesto las conclusiones del análisis forense realizado a quienes proceda.	
RA3. Realiza análisis forenses en Cloud, aplicando metodologías establecidas, actualizadas y reconocidas.	a) Se ha desarrollado una estrategia de análisis forense en Cloud, asegurando la disponibilidad de los recursos y capacidades necesarios una vez ocurrido el incidente.	Proyecto integrado y actividades teórico-prácticas
	b) Se ha conseguido identificar las causas, el alcance y el impacto real causado por el incidente.	
	c) Se han realizado las fases del análisis forense en Cloud.	
	d) Se han identificado las características intrínsecas de la nube (elasticidad, ubicuidad, abstracción, volatilidad y compartición de recursos).	
	e) Se han cumplido los requerimientos legales en vigor, RGPD (Reglamento general de protección de datos) y directiva NIS (Directiva de la UE sobre seguridad de redes y sistemas de información) o las que eventualmente pudieran sustituirlas.	
	f) Se han presentado y expuesto las conclusiones del análisis forense realizado.	

Resultados de Aprendizaje	Criterios de evaluación	Instrumentos
RA4. Realiza análisis forense en dispositivos de IoT, aplicando metodologías establecidas, actualizadas y reconocidas.	a) Se han identificado los dispositivos a analizar garantizando la preservación de las evidencias.	Proyecto integrado y actividades teórico-prácticas
	b) Se han utilizado mecanismos y herramientas adecuadas para la adquisición y extracción de evidencias	
	c) Se ha garantizado la autenticidad, completitud, fiabilidad y legalidad de las evidencias extraídas.	
	d) Se han realizado análisis de evidencias de manera manual y mediante herramientas.	
	e) Se ha documentado el proceso de manera metódica y detallada.	
	f) Se ha considerado la línea temporal de las evidencias.	
	g) Se ha mantenido la cadena de custodia	
	h) Se ha elaborado un informe de conclusiones a nivel técnico y ejecutivo.	
	i) Se han presentado y expuesto las conclusiones del análisis forense realizado.	
RA5. Documenta análisis forenses elaborando informes que incluyan la normativa aplicable.	a) Se ha definido el objetivo del informe pericial y su justificación.	Proyecto integrado y actividades teórico-prácticas
	b) Se ha definido el ámbito de aplicación del informe pericial.	
	c) Se han documentado los antecedentes.	
	d) Se han recopilado las normas legales y reglamentos cumplidos en el análisis forense realizado.	
	e) Se han recogido los requisitos establecidos por el cliente.	
	f) Se han incluido las conclusiones y su justificación.	

13.4 Bibliografía y referencias

13.4.1 Bibliografía de departamento

- Técnicas de Análisis Forense informático para Peritos Judiciales profesionales. Ed.0xword
- Análisis Forense Digital en Entornos Windows. 3ª Edición revisada
- Incident Response & Computer Forensics, Third Edition. McGraw-Hill Education.

13.4.2 Bibliografía de aula

Al alumnado se le facilitará en cada unidad didáctica unos apuntes/presentaciones elaborados por el profesor, basados en los libros de texto que encontramos en la bibliografía de departamento y en las referencias web.

13.4.3 Referencias web

Todas las referencias usadas, se encuentran disponibles en la extensión virtual del aula que proporciona la plataforma Moodle del Centro.

14. Módulo Profesional. Hacking ético (5025)

14.1 Resultados de aprendizaje

El Real Decreto 479/2020, de 7 de abril, establece para este módulo profesional, los siguientes Resultados de aprendizaje:

RA	LOGRO	OBJETO	ACCIONES EN EL CONTEXTO DE APRENDIZAJE
RA 1	Determina	Herramientas de monitorización para detectar vulnerabilidades	Aplicando técnicas de hacking ético
RA 2	Ataca y defiende	Comunicaciones inalámbricas	Consiguiendo acceso a redes para demostrar sus vulnerabilidades
RA 3	Ataca y defiende	Redes y sistemas	Consiguiendo acceso a información y sistemas de terceros
RA 4	Consolida y utiliza	Sistemas comprometidos	Garantizando accesos futuros
RA 5	Ataca y defiende	Aplicaciones web	Consiguiendo acceso a datos o funcionalidades no autorizadas

14.2 Contenidos

14.2.1 Contenidos del currículo

Los contenidos son el conjunto de conocimientos, habilidades, destrezas y actitudes cuya asimilación y apropiación por los que aprenden se consideran esenciales para su ejercicio profesional.

La concreción de los mismos y su secuenciación de aprendizaje se han realizado atendiendo a los siguientes criterios:

- Adecuación a los contenidos básicos reflejados en la normativa estatal, el Real Decreto 479/2020, de 7 de abril.
- Adecuación de los contenidos al requerido en el entorno laboral local.
- Adaptación de los contenidos a los conocimientos previos del alumnado.
- Continuidad y progresión en los contenidos.
- Equilibrio entre las secuencias de conceptos, objetivos y capacidades.
- Interrelación entre contenidos.

Para una mejor compresión de contenido global, dividiremos el módulo en 9 bloques, intentando agrupar ordenadamente conceptos intrínsecamente conectados.

14.2.2 Selección y secuencia de contenidos

Unidades didácticas		Sesiones	RA	Criterios	Trimestre
UD1	Cybersecurity Audit Fundamentals	12	1	a), b), c), d), e), f), g), h), i)	1º
UD2	Web app penetration testing	36	5	a), b), c), d), e), f)	1º
UD3	Host & Network Penetration Testing	40	3	a), b), c), d), e)	2º
UD4	Post Exploitation	20	4	a), b), c), d)	2º
UD5	Reporting	4	2	g)	2º
UD6	Wi-Fi Security and Pentesting	8	2	a), b), c), d), e), f)	2º

14.2.3 Tratamiento de temas transversales

Los temas transversales -no específicos de la materia- y su tratamiento, están vinculados a las situaciones que se presenten en las actividades propuestas, distribuidos a lo largo del módulo.

Se considerarán los siguientes temas transversales:

- Sostenibilidad medioambiental.
- Educación del consumidor.
- Salud laboral.
- Educación para la igualdad de oportunidades entre ambos sexos.
- Igualdad de oportunidades y respeto a personas de otras culturas y credos.
- Inserción laboral.
- Creación de empleo.
- Educación para la paz y la convivencia.
- Educación para la ciudadanía.
- Manejo de documentación técnica en inglés.

14.2.4 Interdisciplinaridad

En el curso, todos los módulos se relacionan íntimamente con el presente, con cuyo profesorado debemos coordinarnos:

- 5021. Incidentes de ciberseguridad.
- 5022. Bastionado de redes y sistemas.
- 5023. Puesta en producción segura.
- 5024. Análisis Forense Informático.
- 5025. Hacking ético.

14.3 Evaluación

A continuación, se especifica para cada unidad didáctica los resultados de aprendizaje y los criterios de evaluación correspondientes a la misma, así como los instrumentos de evaluación que se usarán para calificar cada uno de ellos.

Resultados de Aprendizaje	Criterios de evaluación	Técnica
RA1. Determina herramientas de monitorización para detectar vulnerabilidades aplicando técnicas de hacking ético.	a) Se ha definido la terminología esencial del hacking ético.	Proyecto integrado y actividades teórico-prácticas
	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 de 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.	Proyecto integrado y actividades teórico-prácticas
	b) Se han descrito las técnicas de encriptación de las redes inalámbricas y sus puntos vulnerables.	
	c) Se han generado informes de datos móviles, cumpliendo con los requisitos de la industria forense de telefonía móvil.	
	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.	Proyecto integrado y actividades teórico-prácticas

Resultados de Aprendizaje	Criterios de evaluación	Técnica
	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.	a) Se han administrado sistemas remotos a través de herramientas de línea de comandos.	Proyecto integrado y actividades teórico-prácticas
	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.	Proyecto integrado y actividades teórico-prácticas
	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.	
	f) Se ha realizado la búsqueda y explotación de vulnerabilidades web mediante herramientas software.	

14.4 Bibliografía y referencias

14.4.1 Bibliografía de departamento

- Hacking: The Art of Exploitation.
- The Basics of Hacking and Penetration Testing.

- The Hacker Playbook 2: Practical Guide to Penetration Testing.
- Penetration Testing – A Hands-On Introduction to Hacking.

14.4.2 Bibliografía de aula

Al alumnado se le facilitará en cada unidad didáctica unos apuntes/presentaciones elaborados por el profesor, basados en los libros de texto que encontramos en la bibliografía de departamento y en las referencias web.

14.4.3 Referencias web

Todas las referencias usadas, se encuentran disponibles en la extensión virtual del aula que proporciona la plataforma Moodle del Centro.

15. Módulo Profesional. Normativa de ciberseguridad (5026)

15.1 Resultados de aprendizaje

El Real Decreto 479/2020, de 7 de abril, establece para este módulo profesional, los siguientes Resultados de aprendizaje:

RA	LOGRO	OBJETO	ACCIONES EN EL CONTEXTO DE APRENDIZAJE
RA 1	Identifica	Los puntos principales de aplicación para asegurar el cumplimiento normativo	Reconociendo funciones y responsabilidades
RA 2	Diseña	Sistemas de cumplimiento normativo	Seleccionando la legislación y jurisprudencia de aplicación
RA 3	Relaciona	La normativa relevante para el cumplimiento de la responsabilidad penal de las organizaciones y personas jurídicas con los procedimientos establecidos	Recopilando y aplicando las normas vigentes
RA 4	Aplica	La legislación nacional de protección de datos de carácter personal	Relacionando los procedimientos establecidos con las leyes vigentes y con la jurisprudencia existente sobre la materia
RA 5	Recopila y aplica	La normativa vigente de ciberseguridad de ámbito nacional e internacional	Actualizando los procedimientos establecidos de acuerdo con las leyes y con la jurisprudencia existente sobre la materia

15.2

15.3 Contenidos

15.3.1 Contenidos del currículo

Los contenidos son el conjunto de conocimientos, habilidades, destrezas y actitudes cuya asimilación y apropiación por los que aprenden se consideran esenciales para su ejercicio profesional.

La concreción de los mismos y su secuenciación de aprendizaje se han realizado atendiendo a los siguientes criterios:

- Adecuación a los contenidos básicos reflejados en la normativa estatal, el Real Decreto 479/2020, de 7 de abril.
- Adecuación de los contenidos al requerido en el entorno laboral local.
- Adaptación de los contenidos a los conocimientos previos del alumnado.
- Continuidad y progresión en los contenidos.
- Equilibrio entre las secuencias de conceptos, objetivos y capacidades.
- Interrelación entre contenidos.

Para una mejor compresión de contenido global, dividiremos el módulo en 9 bloques, intentando agrupar ordenadamente conceptos intrínsecamente conectados.

15.3.2 Selección y secuencia de contenidos

Unidades didácticas		Sesiones	RA	Criterios	
UD1	Fundamentos Jurídicos de la Seguridad Informática	4	1	a	1er trimestre (22 horas)
UD2	Principios y Buenas Prácticas de la Seguridad de la Información	8	1	b, c, d, e	
UD3	Gestión de Riesgos	10	2	a, b, c, d	
UD4	Normativas, Regulaciones y Legislación	14	4	a, b, c, d, e, f, g	2o trimestre (38 horas)
UD5	Sistemas de Gestión de la Seguridad de la Información	16	5	a, b, c, d, e	
UD6	Legislación para el Cumplimiento de la Responsabilidad Penal	8	3	a, b, c, d	

15.3.3 Tratamiento de temas transversales

Los temas transversales -no específicos de la materia- y su tratamiento, están vinculados a las situaciones que se presenten en las actividades propuestas, distribuidos a lo largo del módulo.

Se considerarán los siguientes temas transversales:

- Sostenibilidad medioambiental.
- Educación del consumidor.
- Salud laboral.
- Educación para la igualdad de oportunidades entre ambos sexos.
- Igualdad de oportunidades y respeto a personas de otras culturas y credos.
- Inserción laboral.
- Creación de empleo.
- Educación para la paz y la convivencia.
- Educación para la ciudadanía.
- Manejo de documentación técnica en inglés.

15.3.4 Interdisciplinaridad

En el curso, todos los módulos se relacionan íntimamente con el presente, con cuyo profesorado debemos coordinarnos:

- 5021. Incidentes de ciberseguridad.
- 5022. Bastionado de redes y sistemas.
- 5023. Puesta en producción segura.
- 5024. Análisis Forense Informático.
- 5025. Hacking ético.

15.4 Evaluación

A continuación, se especifica el peso de cada uno de los resultados de aprendizaje, así como el de los criterios de evaluación que lo componen. La mayor o menor ponderación de los criterios se obtiene en base al nivel de dificultad y contenidos a desarrollar

para cada criterio. La calificación de cada resultado de aprendizaje será la media ponderada de los distintos criterios de evaluación.

Resultados de Aprendizaje	Criterios de evaluación	Peso RA	Peso CE	Técnica
RA1. Identifica los puntos principales de aplicación para asegurar el cumplimiento normativo reconociendo funciones y responsabilidades.	a) Se han identificado las bases del cumplimiento normativo a tener en cuenta en las organizaciones.	20%	4%	Proyecto integrado y actividades teórico-prácticas
	b) Se han descrito y aplicado los principios de un buen gobierno y su relación con la ética profesional.		4%	
	c) Se han definido las políticas y procedimientos, así como la estructura organizativa que establezca la cultura del normativo dentro de las organizaciones.		4%	
	d) Se han descrito las funciones o competencias del responsable del cumplimiento normativo dentro de las organizaciones.		4%	
	e) Se han establecido las relaciones con terceros para un correcto cumplimiento normativo.		4%	
RA2. Diseña sistemas de cumplimiento normativo seleccionando la legislación y jurisprudencia de aplicación.	a) Se han recogido las principales normativas que afectan a los diferentes tipos de organizaciones.	25%	5%	Proyecto integrado y actividades teórico-prácticas
	b) Se han establecido las recomendaciones válidas para diferentes tipos de organizaciones de acuerdo con la normativa vigente (ISO 19.600 entre otras).		5%	
	c) Se han realizado análisis y evaluaciones de los riesgos de diferentes tipos de organizaciones de acuerdo con la normativa vigente (ISO 31.000 entre otras).		7,5%	

Resultados de Aprendizaje	Criterios de evaluación	Peso RA	Peso CE	Técnica
	d) Se ha documentado el sistema de cumplimiento normativo diseñado.		7,5%	
RA3. Relaciona la normativa relevante para el cumplimiento de la responsabilidad penal de las organizaciones y personas jurídicas con los procedimientos establecidos, recopilando y aplicando las normas vigentes.	a) Se han identificado los riesgos penales aplicables a diferentes organizaciones.	10%	2%	Proyecto integrado y actividades teórico-prácticas
	b) Se han implantado las medidas necesarias para eliminar o minimizar los riesgos identificados.		2%	
	c) Se ha establecido un sistema de gestión de cumplimiento normativo penal de acuerdo con la legislación y normativa vigente (Código Penal y UNE 19.601, entre otros).		3%	
	d) Se han determinado los principios básicos dentro de las organizaciones para combatir el soborno y promover una cultura empresarial ética de acuerdo con la legislación y normativa vigente (ISO 37.001 entre otros).		3%	
RA4. Aplica la legislación nacional de protección de datos de carácter personal, relacionando los procedimientos establecidos con las leyes vigentes y con la jurisprudencia existente sobre la materia.	a) Se han reconocido las fuentes del Derecho de acuerdo con el ordenamiento jurídico en materia de protección de datos de carácter personal.	20%	2%	Proyecto integrado y actividades teórico-prácticas
	b) Se han aplicado los principios relacionados con la protección de datos de carácter personal tanto a nivel nacional como internacional.		3%	

Resultados de Aprendizaje	Criterios de evaluación	Peso RA	Peso CE	Técnica
	c) Se han establecido los requisitos necesarios para afrontar la privacidad desde las bases del diseño.		2%	
	d) Se han configurado las herramientas corporativas contemplando el cumplimiento normativo por defecto.		3%	
	e) Se ha realizado un análisis de riesgos para el tratamiento de los derechos a la protección de datos		3%	
	f) Se han implantado las medidas necesarias para eliminar o minimizar los riesgos identificados en la protección de datos.		4%	
	g) Se han descrito las funciones o competencias del delegado de protección de datos dentro de las organizaciones.		3%	
RA5.Recopila y aplica la normativa vigente de ciberseguridad de ámbito nacional e internacional, actualizando los procedimientos establecidos de acuerdo con las leyes y con la jurisprudencia existente sobre la materia.	a) Se ha establecido el plan de revisiones de la normativa, jurisprudencia, notificaciones, etc. jurídicas que puedan afectar a la organización.	25%	5%	Proyecto integrado y actividades teórico-prácticas
	b) Se ha detectado nueva normativa consultando las bases de datos jurídicas siguiendo el plan de revisiones establecido.		5%	
	c) Se ha analizado la nueva normativa para determinar si aplica a la actividad de la organización.		5%	
	d) Se ha incluido en el plan de revisiones las modificaciones		5%	

Resultados de Aprendizaje	Criterios de evaluación	Peso RA	Peso CE	Técnica
	necesarias, sobre la nueva normativa aplicable a la organización, para un correcto cumplimiento normativo.			
	e) Se han determinado e implementado los controles necesarios para garantizar el correcto cumplimiento normativo de las nuevas normativas. incluidas en el plan de revisiones.		5%	

15.5 Bibliografía y referencias

15.5.1 Bibliografía de departamento

- Aspectos jurídicos de la ciberseguridad. Ofelia Tejerina. Ed. Ra-Ma

15.5.2 Bibliografía de aula

Al alumnado se le facilitará en cada unidad didáctica unos apuntes/presentaciones elaborados por el profesor, basados en los libros de texto que encontramos en la bibliografía de departamento y en las referencias web.

15.5.3 Referencias web

Todas las referencias usadas, se encuentran disponibles en la extensión virtual del aula que proporciona la plataforma Moodle del Centro.

16. Registro de versiones

Responsable	Acción (Redactado, Revisado)	Fecha	Versión
Carmona Martos, Alejandro Fenández Oliver, Eduardo Rivas Sández, Manuel Romero Santos, David	Redactado	28/10/2022	1.0
Carmona Martos, Alejandro Fenández Oliver, Eduardo Rivas Sández, Manuel Romero Santos, David	Revisado		1.1
Fenández Oliver, Eduardo Rivas Sández, Manuel Romero Santos, David Ureña Lara, Fernando	Revisado	06/11/2023	1.2
Fenández Oliver, Eduardo Ortega Nogueras, Francisco Javier Rivas Sández, Manuel Romero Santos, David	Revisado	31/10/2024	2