JUSTIFICACIÓN
PROYECTO DE FLEXIBILIZACIÓN CeCIB

“Curso de Especialización en Ciberseguridad en las Tecnologías de la Información”

Marzo 2022

ÍNDICE

1 INTRODUCCIÓN

Los cursos de especialización se consideran un programa secuencial de los títulos de referencia que dan acceso a los mismos y responden de forma rápida a las innovaciones que se producen en el sistema productivo, así como a ámbitos emergentes que complementen la formación incluida en los títulos de referencia. Es por todo ello, que la oferta de cursos de especialización se ve necesaria para preparar profesionales a lo largo de su vida que asuman los retos del sistema económico y productivo de la Comunitat Valenciana.

En el curso académico 2020-2021, se implanta con carácter experimental en nuestro centro, el curso de especialización en ciberseguridad en las tecnologías de la información (CeCIB). En la *RESOLUCIÓN de la Secretaría Autonómica de Educación y Formación Profesional, en la que se determina el procedimiento de admisión y aspectos de la organización para los cursos de especialización en el curso 2021-2022*, justifica la utilización de metodologías activas de aprendizaje que cambien las estructuras rígidas de aprendizaje y posibilite que los alumnos puedan diseñar su itinerario formativo dentro de las competencias generales y especificas del curso de especialización

La *Ley orgánica 2/2006, de 3 de mayo*, en su artículo 120.4 dice que los centros, en el ejercicio de su autonomía, pueden adoptar experimentaciones, innovaciones pedagógicas, programas educativos, planes de trabajo, formas de organización, normas de convivencia o ampliación del calendario escolar o del horario lectivo de ámbitos, áreas o materias, en los términos que establezcan las administraciones educativas.

Finalmente, la *RESOLUCIÓN de 17 de enero de 2022 de la Consellería de Educación*, establece los requisitos y procedimientos para la implantación de proyectos propios de flexibilización de la oferta modular de los ciclos formativos con el objetivo de promover la innovación y mejorar la empleabilidad. En esta misma resolución se establecen diferentes opciones de flexibilización. En concreto, el **proyecto de flexibilización para el Curso de especialización en Ciberseguridad se basa en la reorganización de contenidos**.

El objetivo y justificación de solicitar este proyecto de flexibilización es el empleo de nuevas metodologías, las llamadas activas, que ponen al alumnado en el centro del aprendizaje, fomentan el trabajo en equipo e incentivan el espíritu crítico, dejando a un lado los procesos memorísticos de repetición de contenidos; **una forma de trabajar que prepara al alumnado para situaciones de la vida real y para su vida profesional**.

2 ANÁLISIS PRECEPTIVO

2.1 IDENTIFICACIÓN DEL TÍTULO

El Real Decreto 479/2020, de 7 de abril, establece el Curso de especialización en ciberseguridad en entornos de las tecnologías de la información y se fijan los aspectos básicos del currículo. Con carácter autonómico no se ha desarrollado ninguna norma que complemente dicho decreto.

El Curso de Especialización en Ciberseguridad en entornos de las tecnologías de la información queda identificado para todo el territorio nacional por los siguientes elementos:

- Denominación: Ciberseguridad en entornos de las tecnologías de la información.
- Nivel: Formación Profesional de Grado Superior.
- Duración: 720 horas.
- Familia Profesional: Informática y Comunicaciones.
- Rama de conocimiento: Ingeniería y Arquitectura.
- Créditos ECTS: 43.
- Referente en la Clasificación Internacional Normalizada de la Educación: P-5.5.4.

2.2 PERFIL PROFESIONAL

El perfil profesional del Curso de Especialización en Ciberseguridad en entornos de las tecnologías de la información queda determinado por su competencia general, sus competencias profesionales, personales y sociales.

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.

En la tabla siguiente se muestran las competencias profesionales, sociales y personales.

Competencias profesionales:

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

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

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

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

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

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

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

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

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

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

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

Competencias personales y sociales:

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.

Las competencias describen una serie de capacidades y conocimientos que tienen que conseguir los titulados del curso de especialización para dar respuesta a los requerimientos del sector productivo, aumentar la ocupación y favorecer la cohesión social.

2.3 CONTEXTO LABORAL. ¿Qué demandan las empresas?

Según el RD, este profesional ejercerá su actividad en entidades de los sectores donde sea necesario establecer mecanismos y medidas para la protección de los sistemas de información y redes de comunicaciones. Las ocupaciones y puestos de trabajo más relevantes son los siguientes:

a. Experto en ciberseguridad.
b. Auditor de ciberseguridad.

c. Consultor de ciberseguridad.
d. Hacker ético.

Tras un análisis de las ofertas de empleo (*Linkedin*), encontramos una definición poco clara de las funciones de cada una de las ocupaciones anteriores. La ciberseguridad es un área de conocimiento bastante compleja y al mismo tiempo, nos encontramos en un mundo cada vez más digital que afecta a todos los ámbitos de la vida, no solo empresariales, lo que se plasma en la creación de nuevos perfiles laborales asociados a la protección de entornos digitales. Según distintas fuentes pueden llegar hasta 15 (*Elevenpath*). Para las empresas es más fácil crear nuevos perfiles en las que encajan varios roles que depender de un perfil dado.

Atendiendo a la competencia general del curso de especialización y a sus competencias profesionales podemos concluir que los perfiles más cercanos que el alumnado sería capaz de desempeñar son[1]:

Administrador De Sistemas.

El administrador de sistemas es en realidad una de las profesiones más importantes en el camino hacia una carrera en ciberseguridad, aunque no se describen estrictamente como profesionales de la ciberseguridad. Sin embargo, necesitan tener importantes conocimientos en seguridad para realizar su trabajo correctamente.

Los administradores de sistemas son indispensables para la mayoría de las empresas, ya que son responsables de la configuración, mantenimiento, operación y seguridad de los sistemas informáticos y servidores, así como de solucionar problemas y brindar apoyo a otros empleados. Alguno de los requisitos para ser administrador de sistemas son el conocimiento de Linux y de los principales hardware de red, ingeniería de redes y soporte técnico.

Ingeniero De Ciberseguridad.

Es quien se encarga de llevar a cabo el plan de ciberseguridad a nivel técnico, construyendo la red a partir de las decisiones tomadas por la dirección, con el fin de garantizar la seguridad de todos los procedimientos que lleve a cabo la empresa. Se trata de un perfil esencial de carácter preventivo, por tanto, sus funciones están orientadas a proteger redes, sitios web, bases de datos, aplicaciones y otros sistemas tecnológicos de cualquier ataque. Los

[1] (https://www.welivesecurity.com/la-es/2020/11/13/perfiles-profesionales-en-seguridad-informatica-que-camino-elegir/):

https://www.ironhack.com/es/ciberseguridad/las-salidas-profesionales-de-un-experto-en-ciberseguridad

podríamos dividir en dos categorías; los ingenieros de ciberseguridad de sistemas y los de aplicaciones.

Analista De Seguridad.

El principal objetivo como analista de seguridad será detectar las debilidades técnicas que puedan sufrir las empresas. En esta área tendrás que llevar a cabo una labor técnica pero también tareas de gestión, localizando puntos vulnerables, respondiendo a los incidentes, estableciendo planes y políticas eficientes, además de asegurarte de su correcta ejecución.

Especialista en Incidentes.

Es el responsable de coordinar las acciones de una empresa en caso de que aparezcan problemas de seguridad, encargándose de accionar un plan de control para que todo un equipo trabaje en la misma línea y tratando de que un ataque tenga las menores consecuencias posibles. Se trata, por tanto, de un puesto más organizativo que de investigación, ideal para aquellos con madera de líder que quieran dirigir personas y sepan ganarse la confianza de los distintos equipos.

Especialista Forense o Analista de Ataques.

Los especialistas en informática forense pueden describirse como los detectives del ciberespacio. Son responsables de investigar diversas violaciones de datos e incidentes de seguridad, recuperar y examinar datos almacenados en dispositivos electrónicos y reconstruir sistemas dañados para recuperar datos perdidos. También se espera que los especialistas forenses ayuden a las autoridades a evaluar la credibilidad de los datos y proporcionen asesoramiento experto a los profesionales del derecho cuando se utilicen pruebas electrónicas en un caso legal.

Hacker Ético.

El hacking ético se ha convertido en una práctica esencial para poner a prueba la seguridad de los servidores y sistemas de las empresas, simulando ataques para comprobar hasta qué punto una compañía está preparada o es vulnerable a los ciberataques. Son profesionales que bien pueden formar parte de un equipo o trabajar de forma externa. En cualquier caso, se trata de un perfil muy demandado que puede ahorrar pérdidas millonarias, filtraciones y ataques irreparables.

Como hemos comentado anteriormente y se evidencia en los perfiles profesionales descritos, la ciberseguridad requiere unos conocimientos avanzados sobre distintas áreas técnicas, por lo que las ofertas de empleo suelen requerir certificaciones de reconocido prestigio, como puede ser:

- CISSP (Certified Information Systems Security Professional).
- CISM (Certified Information Security Manager).
- CISA (Certified Information Systems Auditor).

- OSCP (Offensive Security Certified Professional).
- CEH (Certified Ethical Hacker).

Además, se suele requerir una experiencia profesional de alrededor de 4 años, aunque debido a la gran demanda de personal con formación en ciberseguridad, se ofertan estas mismas ocupaciones con el adjetivo *junior,* eliminando así el requisito de la experiencia.

(CyberSeek, un sitio que proporciona una variedad de información acerca de la planificación de carrera en ciberseguridad)

2.4 Objetivos generales del Título

Los objetivos expresan los resultados esperados del alumnado como consecuencia del proceso formativo. Se obtienen a partir de las competencias, y su finalidad es facilitar la planificación didáctica. Así pues, **los objetivos generales son una herramienta muy importante en el proceso de aprendizaje y en la planificación docente**.

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

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

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

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

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

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

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

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

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

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

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

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

2.5 CUADRO HORARIO.

Los contenidos son un elemento básico en la programación de cualquier módulo, ya que son el objeto del proceso de enseñanza-aprendizaje. Los **contenidos** se utilizan como medios para alcanzar las capacidades contenidas en los objetivos generales. De ahí que **debamos de dejarlos de considerar como un fin en sí mismos, y convertirlos en meros instrumentos para alcanzar esas capacidades**.

Los contenidos del currículo de CECIB se distribuyen en 6 módulos formativos:

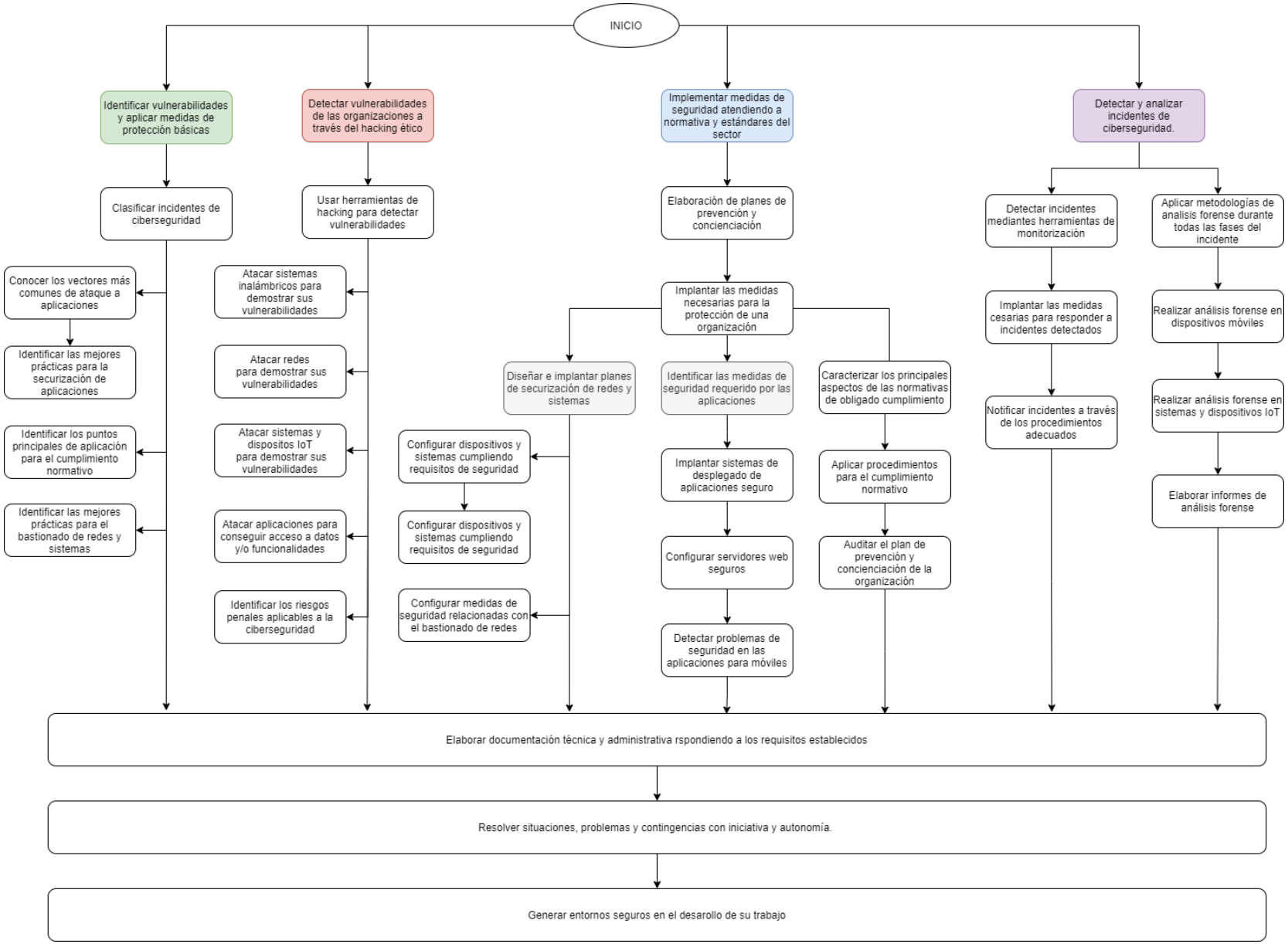
Módulos profesionales	**Horas**
5021. Incidentes de ciberseguridad	120
5022. Bastionado de redes y sistemas	185
5023. Puesta en producción segura	120
5024. Análisis forense informático	120
5025. Hacking ético	120
5026. Normativa de ciberseguridad	55
Total	**720**

3 JUSTIFICACIÓN PROPUESTA DE FLEXIBILIZACIÓN

3.1 PROCESO TECNOLÓGICO

Teniendo en cuenta el perfil del Título, sus competencias y objetivos, así como los resultados de aprendizaje y orientaciones pedagógicas de cada uno de los módulos, representamos en el siguiente diagrama las relaciones que a nuestro entender tienen las diferentes realizaciones profesionales asociadas al curso de especialización. Tal como se representa en el proceso tecnológico, las diferentes realizaciones profesionales se agrupan en cuatro bloques con poca interdependencia entre sí. En concreto:

- En el primero, orientado a identificar y aplicar medidas de protección básicas, el alumnado adquirirá los conocimientos generales a aplicar en las organizaciones y empresas para proteger la información y dispositivos empresariales.
- El objetivo del bloque “Detectar vulnerabilidades de las organizaciones a través del hacking ético” es analizar el comportamiento y la resistencia de los sistemas de una organización ante ataques externos.
- La finalidad del tercer bloque es proteger la organización bajo cualquier concepto, desde el completo bastionado de la infraestructura de red de la organización hasta el diseño de un plan de seguridad que permita garantizar la efectividad de los controles desplegados.
- El último está orientado a la gestión de incidentes. Además de implementar prácticas y soluciones de seguridad efectivas, toda organización necesita identificar y abordar rápidamente ataques para minimizar daños, interrupciones y costes. Al mismo tiempo se debe asegurar que durante toda la gestión del incidente se preserve y tomen las evidencias necesarias para su posterior análisis y/o consecuencias legales.


INICIO
Identificar vulnerabilidades y aplicar medidas de protección básicas
Detectar vulnerabilidades de las organizaciones a través del hacking ético
Implementar medidas de seguridad atendiendo a normativa y estándares del sector
Detectar y analizar incidentes de ciberseguridad.
Clasificar incidentes de ciberseguridad
Usar herramientas de hacking para detectar vulnerabilidades
Elaboración de planes de prevención y concienciación
Detectar incidentes mediantes herramientas de monitorización
Aplicar metodologías de analisis forense durante todas las fases del incidente
Conocer los vectores más comunes de ataque a aplicaciones
Identificar las mejores prácticas para la securización de aplicaciones
Identificar los puntos principales de aplicación para el cumplimiento normativo
Identificar las mejores prácticas para el bastionado de redes y sistemas
Atacar sistemas inalámbricos para demostrar sus vulnerabilidades
Atacar redes para demostrar sus vulnerabilidades
Atacar sistemas y dispositos IoT para demostrar sus vulnerabilidades
Atacar aplicaciones para conseguir acceso a datos y/o funcionalidades
Identificar los riesgos penales aplicables a la ciberseguridad
Implantar las medidas necesarias para la protección de una organización
Diseñar e implantar planes de securización de redes y sistemas
Identificar las medidas de seguridad requerido por las aplicaciones
Caracterizar los principales aspectos de las normativas de obligado cumplimiento
Configurar dispositivos y sistemas cumpliendo requisitos de seguridad
Configurar dispositivos y sistemas cumpliendo requisitos de seguridad
Configurar medidas de seguridad relacionadas con el bastionado de redes
Implantar sistemas de desplegado de aplicaciones seguro
Configurar servidores web seguros
Detectar problemas de seguridad en las aplicaciones para móviles
Aplicar procedimientos para el cumplimiento normativo
Auditar el plan de prevención y concienciación de la organización
Implantar las medidas cesarias para responder a incidentes detectados
Notificar incidentes a través de los procedimientos adecuados
Realizar análisis forense en dispositivos móviles
Realizar análisis forense en sistemas y dispositivos IoT
Elaborar informes de análisis forense
Elaborar documentación técnica y administrativa rspondiendo a los requisitos establecidos
Resolver situaciones, problemas y contingencias con iniciativa y autonomía.
Generar entornos seguros en el desarollo de su trabajo

3.2 UNIDADES FORMATIVAS

El proyecto de flexibilización por reorganización de contenidos afectará a todos los módulos y durante la totalidad del horario lectivo. Evidentemente esto supone necesariamente un trabajo en equipo de todo el profesorado, una cierta flexibilidad, así como una reflexión, que realizaremos durante este tercer trimestre, sobre las capacidades y competencias que buscamos en el perfil profesional asociado a este curso.

En concreto, todos los resultados de aprendizaje se reorganizarán en cuatro unidades formativas correspondientes a los cuatro bloques identificados en el proceso tecnológico y **que se impartirán de forma secuencial**. En concreto:

- **UF1. Warm-up**, corresponde a identificar vulnerabilidades y aplicar medidas de protección básica.
- **UF2. Seguridad ofensiva**. Detectar vulnerabilidades de las organizaciones a través del hacking ético.
- **UF3. Seguridad defensiva**. Implementar medidas de seguridad atendiendo a normativa y estándares.
- **UF4. Gestión de incidentes**. Detectar, responder y analizar incidentes de ciberseguridad.

Resultados de aprendizaje por unidad formativa.

Por cada resultado de aprendizaje indicamos el %de relevancia que tiene por unidad formativa. La codificación de cada RA es con dos dígitos, el primero indica el módulo y el segundo, la posición que ocupa dentro del módulo.

		UF1	UF2	UF3	UF4
INCIDENTES DE CIBERSEGURI.	RA1.1	20		80	
	RA1.2	20		80	
	RA1.3	20			80
	RA1.4			40	60
	RA1.5				100
BASTIONADO DE REDES	RA2.1	20		80	
	RA2.2	20		80	
	RA2.3	40		60	
	RA2.4	40		60	
	RA2.5	40		60	
	RA2.6	40		60	
	RA2.7	40		60	
PUESTA DE PRODUCCIÓN SEGURA	RA3.1	100			
	RA3.2	20		80	
	RA3.3	20		80	
	RA3.4			100	
	RA3.5	20		80	
ANALÍSIS FORENSE INFORMÁTICO	RA4.1				100
	RA4.2				100
	RA4.3				100
	RA4.4				100
	RA4.5				100

		UF1	UF2	UF3	UF4
HACKING ÉTICO	RA5.1		100		
	RA5.2		100		
	RA5.3		100		
	RA5.4		100		
	RA5.5		100		
NORMATIVA DE CIBERSEGURI.	RA6.1	40		60	
	RA6.2			100	
	RA6.3	20	20	60	
	RA6.4	20		80	
	RA6.5			100	

3.3 PRINCIPIOS METODOLÓGICOS

Nuestro Centro tiene gran experiencia en el Aprendizaje Basado en Proyectos y en el trabajo por ámbitos, ambos aplicados desde 2008 en la ESO. En este curso académico, compañeros/as pertenecientes a las **familias profesionales de Marketing y Publicidad, y a la de Informática y Comunicaciones están participando en el programa InnovaTec**. Al mismo tiempo, se están realizando **cuatro seminarios** en el que participan más de cuarenta docentes de FP **relacionados con el Aprendizaje Competencial y el Aprendizaje Colaborativo Basado en Retos (ACbR).**

El aprendizaje colaborativo basado en retos bebe de dos metodologías interrelacionadas: el aprendizaje basado en problemas y proyectos y el aprendizaje colaborativo.

La primera es una tendencia constructivista que se rige por los siguientes principios: la formulación de una problemática a partir de la cual los procesos de aprendizaje son dirigidos por las personas participantes, están basados en la experiencia y la actividad, son interdisciplinares, relacionan teoría y práctica, y se realizan en grupo.

La segunda se refiere a la adquisición de destrezas que ocurren como resultado de la interacción en grupo. Sus elementos clave son: responsabilidad individual, interdependencia positiva, habilidades de colaboración, interacción promotora y proceso de grupo.

El **equipo educativo del CECIB asume** los principios del aprendizaje constructivista y cooperativo para el diseño de actividades formativas transversales significativas, utilizando como referencia **el modelo ACbR**.

Este modelo supone un cambio sustancial tanto en el proceso de enseñanza-aprendizaje como en la organización modular y del profesorado del curso de especialización.

El **aprendizaje basado en retos será implementado íntegramente en todo el curso de especialización y por tanto afectará a todos los módulos y durante la totalidad del horario lectivo**. Evidentemente esto supone necesariamente un **trabajo en equipo de todo el profesorado**, una cierta flexibilidad, así como una reflexión, que realizaremos durante este tercer trimestre, sobre las capacidades y competencias que buscamos en el perfil profesional asociado a este curso.

3.4 ESTRATÉGIA METODOLÓGICA

El curso de especialización se enfocará a través de la implantación de varios aspectos desde un enfoque innovador, a saber:

- **PROGRAMACIÓN**: Se realiza una **organización curricular supramodular** que combina los diferentes resultados de aprendizaje de los diferentes módulos para que las secuencias didácticas puedan tener un sentido mucho más práctico e intuitivo. Todo ello estará contextualizado a través de **propuestas prácticas basadas**

en retos. Se fomentará la participación de empresas en la definición, planteamiento y/o evaluación de los mismos. Al mismo tiempo, se buscará que parte de las actividades se desarrollen en las empresas **a través de convenios Dual**.

Cada uno de los retos contextualizará el resto de acciones formativas que se desarrolle, haciendo que estas tengan sentido y por tanto que sean significativas para el alumnado.

- **ESTRUCTURA.** Como ya hemos dicho, las acciones formativas se agruparán en cuatro bloques formativos secuenciales. Por tanto, la creación de las aulas en el portal e-learning de la Consellería (Aules) no se realizará por módulos, habrá un curso por cada uno de las unidades formativas en donde todos los profesores especialistas estarán matriculados. La organización de contenidos de estos cursos será semanal.

  Por cada uno de los bloques se dispondrá de una actividad central o reto. El resto de las actividades, píldoras formativas, actividades prácticas y de evaluación, se diseñan para que el esfuerzo estimado del alumno/a sea de 24 horas por semana. La planificación docente sigue el modelo hibrido invertido; lunes y miércoles se dedicarán a la impartición de contenidos teóricos (píldoras formativas) y, martes y jueves estará enfocado a que el alumnado trabaje de forma colaborativa aplicando lo aprendido, realización actividades propuestas o en la resolución del reto. El viernes estará destinada a la realización de la evaluación formativa y formadora entre el alumnado y profesorado.

  Semanalmente, para realizar un seguimiento del proceso formativo, el alumnado deberá realizar una prueba corta a través de la plataforma Aules sobre los contenidos tratados. La prueba contendrá 20 preguntas aleatorias con cuatro opciones de selección única o múltiple. Permanecerá abierta desde el viernes hasta el domingo, con tres intentos y se seleccionará la de mayor puntuación.

4 CALENDARIO GENERAL

Posible distribución temporal de las unidades formativas, pendiente de un análisis más detallado.

Mes			L	M	X	J	V	S	D	Actividad
Septiembre	4	s0	27	28	29	30	1	2	3	Presentación CECIB
Octubre	5	s1	4	5	6	7	8	9	10	WARM-UP
	6	s2	11	12	13	14	15	16	17	
	7	s3	18	19	20	21	22	23	24	
	8	s4	25	26	27	28	29	30	31	
Noviembre	9	s5	1	2	3	4	5	6	7	
	10	s6	8	9	10	11	12	13	14	
	11	EV1	15	16	17	18	19	20	21	
	12	s1	22	23	24	25	26	27	28	SEGURIDAD OFENSIVA
Diciembre	13	s2	29	30	1	2	3	4	5	
	14	s3	6	7	8	9	10	11	12	
	15	s4	13	14	15	16	17	18	19	
	16	s5	20	21	22	23	24	25	26	
Enero	17		27	28	29	30	31	1	2	
	18		3	4	5	6	7	8	9	
	19	s6	10	11	12	13	14	15	16	
	20	s7	17	18	19	20	21	22	23	
	21	s8	24	25	26	27	28	29	30	
Febrero	22	EV2	31	1	2	3	4	5	6	
	23	s1	7	8	9	10	11	12	13	SEGURIDAD DEFENSIVA
	24	s2	14	15	16	17	18	19	20	
	25	s3	21	22	23	24	25	26	27	
Marzo	26	s4	28	1	2	3	4	5	6	
	27	s5	7	8	9	10	11	12	13	
	28	s6	14	15	16	17	18	19	20	
	29	s7	21	22	23	24	25	26	27	
Abril	30	s8	28	29	30	31	1	2	3	
	31	EV3	4	5	6	7	8	9	10	
	32	s1	11	12	13	14	15	16	17	GESTIÓN DE INCIDENTES
	33		18	19	20	21	22	23	24	
Mayo	34		25	26	27	28	29	30	1	
	35	s2	2	3	4	5	6	7	8	
	36	s3	9	10	11	12	13	14	15	
	37	s4	16	17	18	19	20	21	22	
	38	s5	23	24	25	26	27	28	29	
Junio	39	s6	30	31	1	2	3	4	5	
	40	EV4	6	7	8	9	10	11	12	

5 TIPIFICACIÓN DE LAS ACCIONES FORMATIVAS

Trabajar por retos o proyectos no quiere decir que sean las únicas actividades prácticas, ya que por necesidad se deberán desarrollar otras cuyo objetivo sea facilitar la adquisición de una determinada competencia, como pueden ser:

- **Actividades de introducción**, orientadas a averiguar las ideas y conocimientos previos sobre el tema y a motivar.
- **Actividades PoC (pruebas de conceptos)**. Se harán de forma paralela a las explicaciones, de modo que se ponga en práctica lo aprendido, mediante pequeños ejercicios.
- **Actividades de evaluación**. Es complejo diseñar retos que contemplen todos los RAs de un bloque, por lo que puede ser necesario completar la evaluación con algún otro instrumento.
- **Actividades de refuerzo y/o recuperación**. La función de estas actividades es evaluar contenidos pendientes de evaluación positiva, así como repasar antes de estas pruebas. Las realizarán únicamente los alumnos que tengan alguna parte de la materia pendiente.

5.1 PROPUESTA INICIAL DE RETOS/PROYECTOS

RETO 1: Plan de prevención y concienciación para PYMES

Aunque los ciberataques más conocidos son a grandes empresas, lo cierto es que las pymes son más vulnerables porque en general se encuentran más desprotegidas. Según datos del INCIBE, en 2021, el aumento a ataques a empresas pequeñas ha crecido un 80%, y lo que es peor: el coste medio al que tiene que hacer frente una pyme en caso de un ataque es de 35.000 euros, una cantidad responsable de que el 60% de las empresas atacadas termine por cerrar el negocio.

Hay que tener en cuenta que el cibercrimen está completamente profesionalizado, y como tal podemos encontrar diferentes modelos de negocio. En el caso de ciberataques que afectan a las grandes empresas, son habituales las intrusiones extremadamente sofisticadas, siguiendo un modelo en el que se dedican muchos recursos a un gran objetivo mayor, ya que el retorno de esa inversión también será más elevado.

Sin embargo, en el caso de las pymes no encontraremos habitualmente ese tipo de ataques tan personalizados; en la mayoría de las ocasiones los ciberdelincuentes lanzan **ataques más masivos a gran escala**. No por ello son menos apetecibles o rentables para ellos, al contrario, ya que el botín de cada una de las víctimas será proporcionalmente menor en comparación, pero lograrán muchas más.

La pregunta ¿quién me va atacar a mí, si yo no soy nadie? es la principal vulnerabilidad que tiene las PYMEs. Las PYMEs pueden mitigar la mayoría de las amenazas mediante concienciación y buenas prácticas en ciberseguridad.

En este reto, el alumnado tendrá que desarrollar una serie de consejos, orientación y controles de seguridad sobre cómo las PYMES pueden prevenir o en su caso mitigar los ciberincidentes más frecuentes y relevantes sufridos por este tipo de organizaciones.

RETO 2: Prueba de Pentesting

O, dicho de otra forma, **hacking al servicio de la ciberseguridad**.

El principal objetivo de este reto es analizar el comportamiento y la resistencia de los sistemas de una organización ante ataques externos. El pentester (alumno/a) deberá realizar un informe donde documente ordenadamente las diferentes acciones que ha realizado para explotar las vulnerabilidades detectadas en un entorno simulado en la nube.

RETO 3: Controles de ciberseguridad

En el reto 2, el alumnado ha realizado un informe (auditoría) sobre las diferentes vulnerabilidades encontradas en un supuesto sistema informático de una organización. En el reto actual, atendiendo a las debilidades anteriormente detectadas, se deberá proponer las **medidas técnicas** correctivas correspondientes, junto con aquellos **controles físicos, administrativos y legales** que consideren esenciales para asegurar el nivel de seguridad de la organización. Para ello durante este bloque se presentarán diferentes frameworks relacionados con la seguridad de la información.

RETO 4: DFIR (Digital Forensic and Incident Response)

En el mundo DFIR el entrenamiento es fundamental ya que permite detectar carencias y áreas de mejora, así como afianzar conceptos y aprender nuevas formas de hacer las cosas.

Al alumnado se presentarán retos clasificados en las siguientes 4 categorías que deberá resolver exponiendo en un informe las acciones realizadas. Los escenarios están relacionados con los incidentes más frecuentes, estos son:

- Ataques de phishing.
- Malware.
- Ataques de DDoS
- Usuarios no autorizados sobre la red.