

PROGRAMACIÓN DEL MÓDULO:

PUESTA EN PRODUCCIÓN SEGURA

PROFESOR/ES:	Tomás Montero Ripoll
GRUPO/S Y CICLO/S:	CECETI
CURSO:	2020-2021

ÍNDICE

[INTRODUCCIÓN](#)

[OBJETIVOS](#)

[CONTENIDOS](#)

[DISTRIBUCIÓN TEMPORAL DE CONTENIDOS](#)

[CRITERIOS DE EVALUACIÓN](#)

[RELACIÓN CON OTROS MÓDULOS DEL CURSO DE ESPECIALIZACIÓN](#)

[METODOLOGÍA DIDÁCTICA](#)

[PROCEDIMIENTOS DE EVALUACIÓN DEL APRENDIZAJE DE LOS ALUMNOS](#)

[CRITERIOS DE CALIFICACIÓN](#)

[ATENCIÓN A LA DIVERSIDAD](#)

[MATERIALES Y RECURSOS DIDÁCTICOS, HERRAMIENTAS Y EQUIPAMIENTOS](#)

[ACTIVIDADES COMPLEMENTARIAS Y EXTRAESCOLARES](#)

[TEMAS TRANSVERSALES](#)

1. INTRODUCCIÓN

Este módulo se incluye en el **Curso de Especialización en Ciberseguridad en entornos de las tecnologías de la información**, perteneciente a la Familia Profesional de Informática y Comunicaciones, que queda establecido y regulado por 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.

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

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

- a) Elaborar e implementar planes de prevención y concienciación en ciberseguridad en la organización, aplicando la normativa vigente.
- b) Detectar e investigar incidentes de ciberseguridad, documentándolos e incluyéndolos en los planes de securización de la organización.
- c) Diseñar planes de securización contemplando las mejores prácticas para el bastionado de sistemas y redes.
- d) Configurar sistemas de control de acceso y autenticación en sistemas informáticos, cumpliendo los requisitos de seguridad y minimizando las posibilidades de exposición a ataques.
- e) Diseñar y administrar sistemas informáticos en red y aplicar las políticas de seguridad establecidas, garantizando la funcionalidad requerida con un nivel de riesgo controlado.
- f) Analizar el nivel de seguridad requerido por las aplicaciones y los vectores de ataque más habituales, evitando incidentes de ciberseguridad.**
- g) Implantar sistemas seguros de despliegado 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.**

2. OBJETIVOS

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

- a) Identificar los principios de la organización y normativa de protección en ciberseguridad, planificando las acciones que es preciso adoptar en el puesto de trabajo para la elaboración del plan de prevención y concienciación.
- b) Auditar el cumplimiento del plan de prevención y concienciación de la organización, definiendo las

acciones correctoras que puedan derivarse para incluirlas en el plan 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 despliegado de software respetando los requisitos relativos a control de versiones, roles, permisos y otros para conseguir un despliegado 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.

3. CONTENIDOS

Prueba de aplicaciones *web* y para dispositivos móviles:

- Fundamentos de la programación.
- Lenguajes de programación interpretados y compilados.
- Código fuente y entornos de desarrollo.
- Ejecución de *software*.

- Elementos principales de los programas.
- Pruebas. Tipos.
- **Seguridad en los lenguajes de programación y sus entornos de ejecución (“sandboxes”).**

Determinación del nivel de seguridad requerido por aplicaciones:

- Fuentes abiertas para el desarrollo seguro.
- **Listas de riesgos de seguridad habituales: OWASP Top Ten (web y móvil).**
- Requisitos de verificación necesarios asociados al nivel de seguridad establecido
- Comprobaciones de seguridad a nivel de aplicación: *ASVS (Application Security Verification Standard)*.

Detección y corrección de vulnerabilidades de aplicaciones *web*:

- Desarrollo seguro de aplicaciones *web*.
- Listas públicas de vulnerabilidades de aplicaciones *web*. *OWASP Top Ten*.
- Entrada basada en formularios. Inyección. Validación de la entrada.
- Estándares de autenticación y autorización.
- **Robo de sesión.**
- **Vulnerabilidades *web*.**
- Almacenamiento seguro de contraseñas.
- **Contra medidas. HSTS, CSP, CAPTCHAs, entre otros.**
- Seguridad de portales y aplicativos *web*. Soluciones *WAF (Web Application Firewall)*.

Detección de problemas de seguridad en aplicaciones para dispositivos móviles:

- Modelos de permisos en plataformas móviles. Llamadas al sistema protegidas.
- **Firma y verificación de aplicaciones.**

- **Almacenamiento seguro de datos.**
- Validación de compras integradas en la aplicación.
- Fuga de información en los ejecutables.
- Soluciones *CASB*.

Implantación de sistemas seguros de despliegado de *software*:

- **Puesta segura en producción.**
- Prácticas unificadas para el desarrollo y operación del *software* (*DevOps*).
- Sistemas de control de versiones.
- Sistemas de automatización de construcción (*build*).
- **Integración continua y automatización de pruebas.**
- Escalado de servidores. Virtualización. Contenedores.
- Gestión automatizada de configuración de sistemas
- Herramientas de simulación de fallos.
- Orquestación de contenedores.

4. DISTRIBUCIÓN TEMPORAL DE CONTENIDOS

A pesar de que el número de horas asignadas al módulo es de 117, ocurre que por cuestiones de calendario escolar y aspectos como el impacto de los días festivos respecto al horario generado para el módulo, el número total de horas exceda las 117. La distribución temporal de los contenidos contemplará este hecho, dedicando ese excedente de horas a tareas de repaso, refuerzo y profundización de algunos de los contenidos vistos en el curso.

El orden de impartición de los contenidos puede variar en función de las necesidades del grupo, así como la duración planificada para cada uno de los bloques.

]

EVALUACIÓN	TEMA, BLOQUE O UNIDAD DIDÁCTICA	FECHA INICIO ---- FECHA FIN	Nº HORAS LECTIVAS
1ª	0 - Enseñanza de la metodología y de la plataforma en línea	16/11/2020 16/11/2020	1h
	1 - Fundamentos de software y seguridad informática	17/11/2020 01/12/2020	12h
	2 - Tipos de pruebas software	02/12/2020 22/12/2020	12h
	3 - Niveles de seguridad de las aplicaciones	11/01/2021 02/02/2021	18h
	4 - Vulnerabilidades de aplicaciones web. Detección y corrección	03/02/2021 10/03/2021	24h
% AVANCE EN CONTENIDOS			51%
2ª	5 - Desarrollo seguro en Java	15/03/2021 07/04/2021	14h
	6 - Vulnerabilidades en aplicaciones para dispositivos móviles	12/04/2021 28/04/2021	15h
	7 - Implantación de sistemas seguros	03/05/2021 25/05/2021	18h
	8 - Despliegue de software	26/05/2021 16/06/2021	17h
% AVANCE EN CONTENIDOS			100%

5. CRITERIOS DE EVALUACIÓN

El profesorado evaluará los aprendizajes del alumnado, los procesos de enseñanza y su propia práctica docente. La evaluación en el curso de especialización se realizará teniendo en cuenta los resultados de aprendizaje y los criterios de evaluación establecidos en los módulos profesionales, así como los objetivos generales del curso de especialización.

Resultados de Aprendizaje y Criterios de Evaluación según recoge el Decreto 257/2011 de 7 de octubre:

1. Prueba aplicaciones *web* y aplicaciones para dispositivos móviles analizando la estructura del código y su modelo de ejecución.

Criterios de evaluación:

- a) Se han comparado diferentes lenguajes de programación de acuerdo a sus características principales.
- b) Se han descrito los diferentes modelos de ejecución de software.
- c) Se han reconocido los elementos básicos del código fuente, dándoles significado.
- d) Se han ejecutado diferentes tipos de pruebas de software.
- e) Se han evaluado los lenguajes de programación de acuerdo a la infraestructura de seguridad que proporcionan.

2. Determina el nivel de seguridad requerido por aplicaciones identificando los vectores de ataque habituales y sus riesgos asociados.

Criterios de evaluación:

- a) Se han caracterizado los niveles de verificación de seguridad en aplicaciones establecidos por los estándares internacionales (*ASVS*, "*Application Security Verification Standard*").
- b) Se ha identificado el nivel de verificación de seguridad requerido por las aplicaciones en función de sus riesgos de acuerdo a estándares reconocidos.
- c) Se han enumerado los requisitos de verificación necesarios asociados al nivel de seguridad establecido.
- d) Se han reconocido los principales riesgos de las aplicaciones desarrolladas, en función de sus características.

3. Detecta y corrige vulnerabilidades de aplicaciones *web* analizando su código fuente y configurando servidores *web*.

Criterios de evaluación:

- a) Se han validado las entradas de los usuarios.
- b) Se han detectado riesgos de inyección tanto en el servidor como en el cliente.
- c) Se ha gestionado correctamente la sesión del usuario durante el uso de la aplicación.
- d) Se ha hecho uso de roles para el control de acceso.
- e) Se han utilizado algoritmos criptográficos seguros para almacenar las contraseñas de usuario.
- f) Se han configurado servidores *web* para reducir el riesgo de sufrir ataques conocidos.
- 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*).

4. Detecta problemas de seguridad en las aplicaciones para dispositivos móviles, monitorizando su ejecución y analizando ficheros y datos.

Criterios de evaluación:

- a) Se han comparado los diferentes modelos de permisos de las plataformas móviles.
- b) Se han descrito técnicas de almacenamiento seguro de datos en los dispositivos, para evitar la fuga de información.
- c) Se ha implantado un sistema de validación de compras integradas en la aplicación haciendo uso de validación en el servidor.
- d) Se han utilizado herramientas de monitorización de tráfico de red para detectar el uso de protocolos inseguros de comunicación de las aplicaciones móviles.
- e) Se han inspeccionado binarios de aplicaciones móviles para buscar fugas de información sensible.

5. Implanta sistemas seguros de despliegado de software, utilizando herramientas para la automatización de la construcción de sus elementos.

Criterios de evaluación:

- a) Se han identificado las características, principios y objetivos de la integración del desarrollo y operación del software.
- b) Se han implantado sistemas de control de versiones, administrando los roles y permisos solicitados.

- c) Se han instalado, configurado y verificado sistemas de integración continua, conectándolos con sistemas de control de versiones.
- d) Se han planificado, implementado y automatizado planes de despliegado de software.
- e) Se ha evaluado la capacidad del sistema desplegado para reaccionar de forma automática a fallos.
- f) Se han documentado las tareas realizadas y los procedimientos a seguir para la recuperación ante desastres.
- g) Se han creado bucles de retroalimentación ágiles entre los miembros del equipo.

6. RELACIÓN CON OTROS MÓDULOS DEL CURSO DE ESPECIALIZACIÓN

Este módulo está muy relacionado con el módulo de Hacking Ético del mismo curso de especialización.

7. METODOLOGÍA DIDÁCTICA

La metodología didáctica se adaptará a las peculiaridades colectivas del grupo, así como a las individuales. En el caso de las individuales se apoyarán mayoritariamente en la entrega de material, documentación, prácticas, etc. adicionales que sirvan de apoyo y refuerzo de los contenidos no asimilados.

En lo posible se buscará reproducir entornos reales de producción que puedan ayudar en la formación para la inserción laboral del alumno y en lo referido a la prevención de riesgos laborales.

La metodología encaminada a que el alumno alcance los contenidos estará compuesta por los siguientes procesos:

- Cada tema comienza con una explicación teórica, en la mayoría de los casos apoyada en diapositivas/documentos que se entregarán al alumno. Le siguen un conjunto de ejercicios, algunos opcionales de ampliación, y la corrección de los mismos, bien de forma personalizada o en común. El objetivo de estos ejercicios es llevar a la práctica los conceptos teóricos que se asimilaron en la exposición teórica.
- Algunos temas son totalmente prácticos. Cada práctica está apoyada en un documento que contiene el enunciado y en algunos casos explicaciones teóricas. Se explica mediante demostraciones.
- El profesor resolverá todas las dudas que puedan tener los alumnos, tanto teóricas como prácticas.

Incluso si se considera necesario se realizarán ejercicios específicos que aclaren los conceptos que más cuesten comprender a los alumnos.

- El profesor entregará apuntes a los alumnos, cuando lo crea conveniente, para poder concentrar la atención del alumno en las explicaciones teóricas.
- Debido a las características de la asignatura, algunos temas se explicarán de forma directa sobre el ordenador.
- Cuando el tema a tratar lo requiera el alumno deberá realizar ejercicios prácticos en pizarra, papel y ordenador.
- El alumno que finalice las prácticas del aula con antelación deberá dedicar el tiempo sobrante a la realización de sus proyectos, bien obligatorios o voluntarios.

8. PROCEDIMIENTOS DE EVALUACIÓN DEL APRENDIZAJE DE LOS ALUMNOS

La evaluación será continua, según lo establecido en la normativa vigente y pretenderá comprobar si el alumno ha alcanzado las capacidades terminales y los objetivos del módulo.

Como *instrumentos de evaluación*, se considerarán los siguientes:

- Pruebas escritas individuales.
- Resolución y presentación de los ejercicios propuestos en el modo y tiempo previstos.
- Ejercicios y trabajos prácticos individuales o en grupo.
- Asistencia regular y puntual.
- Observación directa del trabajo diario en clase.

Se evaluará cada evaluación de acuerdo a los instrumentos expresados anteriormente, asignando una nota final que será la correspondiente a la evaluación trimestral.

Se realizará una prueba de recuperación para cada una de las evaluaciones, de manera que aquellos alumnos que la hubieran suspendido o quisieran presentarse a subir nota pudieran hacerlo. Los procedimientos de evaluación y criterios de calificación serán los mismos que en las pruebas ordinarias.

Aquellos alumnos que al finalizar el curso cuenten con alguna evaluación suspensa, podrán realizar un

examen final en el que se evaluarán todos los contenidos del módulo, al finalizar el último trimestre.

En caso de no superar la convocatoria ordinaria se examinarán en la extraordinaria de junio, en la que se evaluarán todos los contenidos del módulo.

9. CRITERIOS DE CALIFICACIÓN

Se calificará a los alumnos/as en sesiones de evaluación una vez al final de cada trimestre.

La calificación de cada alumno/a se elaborará en base a:

- Serán evaluados los contenidos de la o las unidades, de acuerdo con lo expuesto en el punto anterior, calificando de 0 a 10 puntos, de acuerdo a los siguientes elementos:
 - Pruebas teórico/prácticas.
 - Prácticas o trabajos.
- La calificación obtenida en las **pruebas** teórico/prácticas realizadas en la evaluación estará comprendida entre los valores 0 y 10.
- La calificación obtenida en las **prácticas y/o trabajos** realizados en la evaluación estará comprendida entre los valores 0 y 10 o con la calificación APTO y NO APTO.
- Algunos criterios que se tienen en cuenta en la valoración de las prácticas y/o trabajos son:
 - Cumplir los plazos de entrega.
 - Formato y limpieza del documento.
 - La autoría del contenido por parte del alumno.
 - Que incluya las referencias bibliográficas (libros, páginas Web, documentos electrónicos, ...) y respete los derechos de autor.
 - Entrega ordenada de todos los ficheros implicados en la práctica o proyecto.
 - La práctica/trabajo se debe ajustar a los requisitos solicitados por el profesor, incluyendo todos los puntos solicitados y se ponga de manifiesto que el alumno ha asimilado los conceptos desarrollados en el trabajo.
- El porcentaje de cada parte irá en función del desarrollo de la evaluación y de las características de la materia a evaluar (hay evaluaciones con mayor contenido teórico y otras con mayor contenido práctico). Los porcentajes a aplicar serán:
 - Pruebas (teórico-prácticas): 60%.
 - Prácticas/Trabajos/Ejercicios: 40%.
- Al finalizar cada tema, y a criterio del profesor, se puede llevar a cabo una **prueba parcial** de los contenidos impartidos a lo largo de ese tema. Estas pruebas parciales se guardarían para el cálculo

final de la nota de la evaluación y cada una de ellas tendría un peso del 20% sobre la parte de Prácticas/Trabajos/Ejercicios.

- En caso de detectar **plagios** en tareas y pruebas (sea de compañeros o de otras fuentes) la calificación de la tarea o prueba será de 0.
- Para poder aplicar los porcentajes descritos anteriormente es necesario obtener un **mínimo de un 4** en cada uno de los apartados y que al calcular la calificación final resulte superior a un 5. En caso de no obtener un mínimo de un 4 en algún apartado:
 - La evaluación no estará superada.
 - El alumno deberá recuperar la/s parte/s correspondiente/s.
- El alumno/a superará la evaluación con la obtención de una calificación **igual o mayor a 5**.
- Las prácticas/trabajos voluntarios solamente subirán calificación, siempre y cuando esté aprobada la evaluación. Podrán sumar, como máximo, 1 punto más en la calificación de la evaluación.
- La **calificación final** del módulo se calculará teniendo en cuenta las calificaciones de cada una de las evaluaciones, siendo requisito necesario y obligatorio el **haber superado las tres evaluaciones** para superar el curso. Se calculará aplicando la media aritmética de las calificaciones de las tres evaluaciones.

INSTRUCCIONES DE PRUEBAS Y PRÁCTICAS

- Las pruebas se realizarán en la fecha y hora indicadas por la profesora del módulo.
- La no asistencia a la prueba supone la calificación de **No presentado**.
- Sólo se considerarán justificantes válidos los emitidos por órganos oficiales que explícitamente indiquen que no es posible o recomendable la asistencia en la fecha y hora de la prueba. A los estudiantes que aporten tales justificantes de ausencia a la prueba se les propondrá otra fecha y hora de realización.
- En las pruebas no se podrá hablar ni realizar preguntas en voz alta, ni comentarios o ruidos que distraigan a los demás compañeros. En el caso de que estos se produzcan se expulsará al alumno del aula, suponiendo la anulación del examen y la calificación de 0.

RECUPERACIONES

- Primera evaluación no superada: A criterio del profesor, los alumnos podrían realizar una prueba de recuperación al inicio de la siguiente evaluación. En ese caso, el alumno estaría obligado igualmente a entregar todas las prácticas y trabajos de carácter obligatorio propuestos para conseguir una calificación positiva.

- Alguna/s evaluación/es (1ª y/o 2ª) no superada/s en junio: los alumnos podrán realizar **una prueba de recuperación**, cuyo **contenido** será **todo** el que se haya impartido y tratado en la evaluación a recuperar. El alumno está obligado igualmente a entregar todas las prácticas y trabajos de carácter obligatorio propuestos para conseguir una calificación positiva.

CONVOCATORIA EXTRAORDINARIA DE SEPTIEMBRE

Si el módulo no es superado en la convocatoria de junio, los alumnos podrán realizar una prueba en la **convocatoria extraordinaria de septiembre** de todos los contenidos del curso.

10. ATENCIÓN A LA DIVERSIDAD

Si se detectan alumnos con necesidades especiales, por una parte se les ofrecerá la posibilidad de ampliar el número de ejercicios prácticos y por otra se abordarán otras metodologías (elaboración de posters, trabajos sobre el tema, etc) encaminadas a asegurar que comprenden los distintos contenidos.

Para aquellos alumnos que vayan más avanzados se plantearán ejercicios prácticos optativos que profundicen en los contenidos y que sean lo más motivadores posibles.

11. MATERIALES Y RECURSOS DIDÁCTICOS, HERRAMIENTAS Y EQUIPAMIENTOS

El desarrollo del módulo se hará en un aula-taller dotada con pizarra, cañón-proyector, 15 equipos informáticos (1 ordenador por alumno) conectados en red y con salida a Internet. Se facilitará a los alumnos la utilización de los diferentes materiales y recursos disponibles.

- Libros relacionados con los contenidos y disponibles en la biblioteca del departamento.
- Revistas especializadas, disponibles en la biblioteca del departamento.
- Manuales, ejercicios resueltos, etc. obtenidos de Internet. El desarrollo del módulo se hará en un aula-taller dotada con pizarra, cañón proyector, 26 equipos informáticos (1 ordenador por alumno) conectados en red y con salida a Internet. Se facilitará a los alumnos la utilización de los diferentes materiales y recursos disponibles.

12. ACTIVIDADES COMPLEMENTARIAS Y EXTRAESCOLARES

Se fomentará entre el alumnado la labor de investigación personal sobre los diferentes temas tratados a lo largo del curso y la realización de actividades complementarias que permitan conocer casos reales de

implantación de los diversos aspectos abordados en el módulo.

A lo largo del curso se podrían organizar charlas de expertos, empresarios, trabajadores del sector y ex-alumnos para que aprendan cómo se desarrollará su profesión, la importancia de este módulo en el desempeño correcto de las labores encomendadas en su futuro puesto de trabajo y las últimas tendencias del sector.

13. TEMAS TRANSVERSALES

De los temas transversales aconsejados por los departamentos de IyC y FOL para los módulos de la familia profesional de Informática y Comunicaciones, se trabajarán los siguientes:

Educación ambiental

La utilización de la informática en general, y sobre todo en los negocios, hace que grandes volúmenes de información puedan ser almacenados en soportes informáticos, y enviados de unos lugares a otros a través de las redes informáticas, autopistas de la información, evitándose de esta manera el consumo de grandes cantidades de papel y por consiguiente la destrucción de bosques, contribuyendo de alguna manera a la preservación de los medios naturales y medioambientales.

Educación para la igualdad de oportunidades entre ambos sexos

Desde este módulo contamos con elementos para concienciar al alumnado sobre la igualdad de oportunidades entre los sexos, formando grupos mixtos de trabajo, distribuyendo iguales tareas entre alumnos y alumnas, haciendo que todos utilicen iguales o similares materiales y fomentando la participación de todos, sin distinciones de sexo.

Educación para la prevención de riesgos laborales

Cuando se utilizan equipos informáticos uno de los objetivos es que los alumnos y alumnas conozcan unas normas básicas de higiene y seguridad en el trabajo, así como a tomar las debidas precauciones en el empleo de dichos equipos. Es necesario conocer unos principios de ergonomía en el puesto de trabajo, para que la actividad frente al ordenador no sea motivo de problemas físicos. Estos aspectos cobran especial importancia en la Prevención de riesgos laborales. Considerando que el ámbito laboral más común de los Técnicos va a ser las oficinas y centros de procesos de datos, habrá que insistir a diario en la existencia de los siguientes riesgos y de sus correspondientes medidas de prevención

Fomento de la capacidad emprendedora

La capacidad emprendedora se define como la capacidad de actuar con iniciativa y perseverancia, para modificar la realidad siendo un agente de cambio, junto a los que lo rodean, aportando soluciones innovadoras a organizaciones productivas y sociales desde su profesión. Debemos fomentar en nuestros alumnos esta capacidad inculcando en ellos valores tales como:

- La autoconfianza, tener fe en nuestras posibilidades, sin olvidar que los objetivos marcados deben ser

realistas.

- La tolerancia a la frustración, saber sobreponerse a la frustración que suponen las expectativas no cumplidas, sabiendo extraer un análisis positivo de las situaciones negativas.
- La gestión del riesgo, mediante un enfoque adecuado para manejar los posibles riesgos y mitigar su impacto.
- La búsqueda de recursos, de todo aquello que puede contribuir a llevar un proyecto a buen término.
- La productividad, saber explotar los recursos al máximo.
- La creatividad, en un mundo cambiante, necesitamos plantear soluciones, formular hipótesis, tener iniciativas novedosas, y todo ello está íntimamente ligado con el proceso creativo.

Educación del consumidor

El análisis y la utilización de diferentes herramientas informáticas favorecen la capacidad del alumno/a para decidir sobre los productos informáticos que debe adquirir y utilizar de la manera más apropiada, valorando de manera crítica las distintas ofertas, campañas de publicidad, etc.