PROGRAMACIÓN DEL MÓDULO:

Análisis Forense Informático

PROFESOR:	Felipe Pablos Lamas
GRUPO/S Y CICLO/S:	CECETI
CURSO:	2020-2021

ÍNDICE

1. INTRODUCCIÓN

Para la elaboración de esta programación se ha considerado la "Guía general para la organización y desarrollo de la actividad educativa para el curso 2020/2021 en todos los centros sostenidos con fondos públicos de la Comunidad Autónoma de Extremadura", la instrucción 13/2020 de la Secretaría general de educación, referente a la organización de las actividades lectivas semipresenciales y no presenciales, la evaluación del aprendizaje del alumnado y otros aspectos de la organización de los centros educativos y del sistema educativo en su conjunto durante el curso 2010-2021, las instrucciones y recomendaciones elaboradas por los distintos órganos de coordinación didáctica y lo indicado en el apartado "Medidas a adoptar ante la suspensión de las actividades lectivas presenciales" en la Programación General Anual.

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 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.

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 se 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.

3. CONTENIDOS

Previa a la impartición de los contenidos se realizará una unidad 0 en la que se explicará la metodología, los criterios y procedimientos de evaluación, **incluyendo la eventualidad de tener que abandonar la enseñanza presencial por modelos semipresenciales o a distancia.**

De forma frecuente se refrescará la metodología y se practicará con las herramientas a utilizar en caso de paso a enseñanza semipresencial o a distancia, algunas de las cuales se integrarán también en la clase presencial para facilitar una migración rápida y el seguimiento de las clases por parte del alumnado que no pueda asistir.

Aplicación de metodologías de análisis forenses:

- **Identificación de los dispositivos a analizar.**
- **Recolección de evidencias (trabajar un escenario).**
- **Análisis de la línea de tiempo (TimeStamp).**
- **Análisis de volatilidad**
- **Extracción de información (Volatility).**
- Análisis de Logs, herramientas más usadas.

Realización de análisis forenses en dispositivos móviles:

- **Métodos para la extracción de evidencias.**
- **Herramientas de mercado más comunes.**

Realización de análisis forenses en Cloud:

- **Nube privada y nube pública o híbrida.**
- Retos legales, organizativos y técnicos particulares de un análisis en Cloud.
- **Estrategias de análisis forense en Cloud.**
- **Realizar las fases relevantes del análisis forense en Cloud.**
- Utilizar herramientas de análisis en Cloud (Cellebrite UFED Cloud Analyzer, Cloud Trail, Frost, OWADE, ...).

Realización de análisis forenses en IoT:

- **Identificar los dispositivos a analizar.**
- Adquirir y extraer las evidencias.

- Analizar las evidencias de manera manual y automática.
- Documentar el proceso realizado.
- Establecer la línea temporal.
- Mantener la cadena de custodia.
- Elaborar las conclusiones.
- Presentar y exponer las conclusiones.

Documentación y elaboración de informes de análisis forenses. Apartados de los que se compone el informe:

- **Hoja de identificación (título, razón social, nombre y apellidos, firma).**
- **Índice de la memoria.**
- **Objeto (objetivo del informe pericial y su justificación).**
- **Alcance (ámbito de aplicación del informe pericial - resumen ejecutivo para una supervisión rápida del contenido y resultados).**
- **Antecedentes (aspectos necesarios para la comprensión de las alternativas estudiadas y las conclusiones finales).**
- **Normas y referencias (documentos y normas legales y reglamentos citados en los distintos apartados).**
- **Definiciones y abreviaturas (definiciones, abreviaturas y expresiones técnicas que se han utilizado a lo largo del informe).**
- **Requisitos (bases y datos de partida establecidos por el cliente, la legislación, reglamentación y normativa aplicables).**
- **Análisis de soluciones – resumen de conclusiones del informe pericial (alternativas estudiadas, qué caminos se han seguido para llegar a ellas, ventajas e inconvenientes de cada una y cuál es la solución finalmente elegida y su justificación).**
- **Anexos.**

4. DISTRIBUCIÓN TEMPORAL DE CONTENIDOS

El orden de impartición de los contenidos y la duración planificada para cada uno de los bloques puede variar en función de las necesidades del grupo y **de la eventualidad del paso a enseñanza semipresencial o a distancia**. Dentro de cada bloque se impartirán contenidos de forma paralela, trabajando varios conceptos a la vez.

Debido a que este módulo no cuenta con la adaptación al decreto extremeño en la actualidad, por comparativa de la asignación 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 con otros reales decretos parecidos, se ha establecido que la asignación horaria rondará las 120 horas. En concreto, la adaptación para el curso 2020-21, teniendo en cuenta las particularidades del curso y la distribución horaria del módulo, es de 129 periodos lectivos. 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	Unidad 0 - Enseñanza de la metodología y de la plataforma en línea	16/11/2020 17/11/2020	3h
	Unidad 1 - Introducción al Análisis Forense Informático	17/11/2020 25/11/2020	7h
	Unidad 2 - Identificación de evidencias	26/11/2020 16/12/2020	12h
	Unidad 3 - Herramientas para adquisición de evidencias	17/12/2020 13/01/2021	8h
	Unidad 4 - El informe y la comunicación	14/01/2021 01/02/2021	13h
	Unidad 5 - Adquisición de evidencias	02/02/2021 08/03/2021	22h
		% AVANCE EN CONTENIDOS	**51%**
2ª	Unidad 6 - Análisis de evidencias	09/03/2021 03/05/2021	39h
	Unidad 7 - Contrapericial	15/05/2021 23/05/2021	5h
	Unidad 8 - Forense Cloud	24/05/2021 06/06/2021	10h
	Unidad 9 - Forense IoT	07/06/2021 18/06/2021	10h
		% 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 ciclo formativo 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 ciclo formativo.

1. Aplica metodologías de análisis forense caracterizando las fases de preservación, adquisición, análisis y documentación.

Criterios de evaluación:

a) Se han identificado los dispositivos a analizar para garantizar la preservación de evidencias.

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.

2. Realiza análisis forenses en dispositivos móviles, aplicando metodologías establecidas, actualizadas y reconocidas.

Criterios de evaluación:

a) Se ha realizado el proceso de toma de evidencias en un dispositivo móvil.

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.

3. Realiza análisis forenses en Cloud, aplicando metodologías establecidas, actualizadas y reconocidas.

Criterios de evaluación:

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.

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.

4. Realiza análisis forense en dispositivos del IoT, aplicando metodologías establecidas, actualizadas y reconocidas.

Criterios de evaluación:

a) Se han identificado los dispositivos a analizar garantizando la preservación de las evidencias.

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.

5. Documenta análisis forenses elaborando informes que incluyan la normativa aplicable.

Criterios de evaluación:

a) Se ha definido el objetivo del informe pericial y su justificación.

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.

6. RELACIÓN CON OTROS MÓDULOS DEL CICLO

Este módulo está muy relacionado con los siguientes módulos del mismo ciclo de especialización:

- Incidentes de ciberseguridad.
- Normativa de ciberseguridad.
- Hacking ético.

7. METODOLOGÍA DIDÁCTICA

La metodología será adaptada en función de la evolución de la pandemia COVID19, pudiendo contemplar los escenarios de educación a distancia o semipresencial. 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 cueste 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.
- Cuando sea necesario, se contará con la colaboración de expertos para realizar alguna de las prácticas. Esa colaboración será por vía telemática.

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 a las clases o sesiones virtuales.
- Observación directa del trabajo diario en clase o desde casa.

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 septiembre, 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): 70%.
  - Prácticas/Trabajos/Ejercicios: 20% .
  - Asistencia/Comportamiento/Puntualidad/Asistencia: 10%

- **Asistencia, comportamiento, puntualidad y actitud.**

En este apartado cada alumno parte con 1 punto que irán sumando o restando de acuerdo al siguiente baremo:

– 0,1 por cada falta de asistencia. (Máximo de 10 faltas)

– 0,1 por cada retraso. (Máximo de 10 retrasos)

– 0,5 por negarse a hacer las tareas o salir a la pizarra.

– 0,5 por mal comportamiento o actitud pasiva.

– 0,5 por maltratar los equipos (instalar programas, saltarse claves, etc.)

+ 0,5 por actitud positiva

- 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 notas parciales se guardan para el cálculo final de la nota de la evaluación y para ello será necesario haber obtenido una calificación igual o mayor a 5.
- 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 dos evaluaciones** para superar el curso. Se calculará aplicando la media aritmética de las calificaciones de las dos 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

- Los alumnos podrán realizar una prueba de recuperación de la primera evaluación al inicio de la segunda. 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, etc) encaminadas a asegurar que comprenden los distintos contenidos. Para aquellos alumnos que vayan más avanzados se plantearán ejercicios prácticos que profundicen en los contenidos y que sean lo más motivadores posible.

11. MATERIALES Y RECURSOS DIDÁCTICOS, HERRAMIENTAS Y EQUIPAMIENTOS

El desarrollo del módulo se hará en el aula dotada con 1 ordenador por alumno y también en el taller y en el CPD de los ciclos formativos. Se facilitará a los alumnos la utilización de los diferentes materiales y recursos disponibles (discos duros, pendrives, clonadoras, bloqueadoras, software, etc).

Bibliografía:

- Manuales de las aplicaciones utilizadas.
- Especificaciones de organismos nacionales/internacionales.
- 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.

Se pondrá especial interés en que el alumnado no comparta recursos físicos atendiendo a las recomendaciones sanitarias a causa de la pandemia.

12. ACTIVIDADES COMPLEMENTARIAS Y EXTRAESCOLARES

Las programadas por el departamento y que estén relacionadas con los contenidos de este módulo.

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 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 salud
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
Los aspectos básicos a trabajar en la educación para la salud en relación a COVID-19 son los aspectos de la enfermedad, cómo actuar ante la aparición de síntomas, medidas de distancia física y limitación de contactos, higiene de manos y resto de medidas de prevención personal, uso adecuado de la mascarilla, conciencia de la interdependencia entre los seres humanos y el entorno y fomento de la corresponsabilidad en la salud propia y en la salud de los otros, prevención del estigma.

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.

Ecología y medioambiente

La utilización de la informática en general, y sobre todo en el ámbito empresarial, hace que grandes volúmenes de información puedan ser almacenadas en soportes informáticos y enviados a otros usuarios a través de las redes informáticas evitando de esta manera el consumo de papel y su correspondiente impacto medioambiental, contribuyendo a la conservación de los medios naturales y la conservación de la naturaleza.

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.