CURSO DE ESPECIALIZACIÓN EN CIBERSEGURIDAD EN ENTORNOS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

PROGRAMACIÓN ANUAL

Parte específica del módulo:
5024. Análisis Forense Informático

Departamento de Familia Profesional de Informática

Curso: 2023-24
Nivel: Curso de Especialización
Turno: Tarde
Profesor: Ignacio García Manotas

Índice

1 CARACTERÍSTICAS GENERALES DEL CURSO DE ESPECIALIZACIÓN DE CIBERSEGURIDAD EN ENTORNOS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

1.1 OBJETO DE ESTA PROGRAMACIÓN

El objeto de esta programación didáctica es el Curso de especialización en ciberseguridad en entornos de las tecnologías de la información.

1.2 MARCO LEGAL

La legislación aplicable a este curso procede del Real Decreto 479/2020, de 7 de abril, “Curso de especialización en ciberseguridad en entornos de las tecnologías de la información y se fijan los aspectos básicos del currículo”.

No existe actualmente publicado currículo del presente curso en el ámbito de la Comunidad Autónoma de la Región de Murcia.

1.3 UBICACIÓN DEL CICLO

- Denominación: Ciberseguridad en entornos de las tecnologías de la información.
- Nivel: Curso de Especialización
- Duración: 720 horas.
- Familia Profesional: Informática y Comunicaciones (únicamente a efectos de clasificación de las enseñanzas de formación profesional).
- Rama de conocimiento: Ingeniería y Arquitectura.
- Créditos ECTS: 43.
- Referente en la Clasificación Internacional Normalizada de la Educación: P-5.5.4.

1.4 COMPETENCIA GENERAL

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

1.5 COMPETENCIAS PROFESIONALES, PERSONALES Y SOCIALES

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

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

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

El módulo de Análisis Forense Informático se centra en la parte de ciberseguridad que permite reconstruir lo que ha sucedido en un sistema tras un incidente de seguridad. Este análisis puede determinar quién, desde dónde, cómo, cuándo y qué acciones ha llevado a cabo un intruso en los sistemas afectados por un incidente de seguridad.

Normalmente, los estudiantes del curso no tienen los conocimientos altos en sistemas operativos, siendo más habitual el perfil de administradores de sistemas.

3 UBICACIÓN, OBJETIVOS, CONTENIDOS Y DISTRIBUCIÓN TEMPORAL DEL MÓDULO

3.1 UBICACIÓN, DISTRIBUCIÓN TEMPORAL Y CARACTERÍSTICAS

En la Región de Murcia el módulo *Análisis Forense Informático* se desarrolla durante los tres trimestres contando con 120 horas (No disponiendo actualmente de currículo) a 7 créditos ECTS[1] , lo que se traduce en 4 horas semanales de clase.

3.2 OBJETIVOS/RESULTADOS DE APRENDIZAJE Y CRITERIOS DE EVALUACIÓN

El citado Real Decreto 479/2020, de 7 de abril, "Curso de especialización en ciberseguridad en entornos de las tecnologías de la información y se fijan los aspectos básicos del currículo", establece los siguientes objetivos, expresados como resultados de aprendizaje previsibles y sus correspondientes criterios de evaluación.

3.2.1 OBJETIVO/RESULTADO 1

3.2.1.1 Enunciado

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

3.2.1.2 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.

3.2.2 OBJETIVO/RESULTADO 2

3.2.2.1 Enunciado

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

3.2.2.2 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.

[1] Sistema Europeo de Transferencia de Créditos por el que se establece el reconocimiento de créditos entre los títulos de técnico superior y las enseñanzas conducentes a títulos universitarios y viceversa.

3.2.3 OBJETIVO/RESULTADO 3

3.2.3.1 Enunciado

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

3.2.3.2 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.

3.2.4 OBJETIVO/RESULTADO 4

3.2.4.1 Enunciado

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

3.2.4.2 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.

3.2.5 OBJETIVO/RESULTADO 5

3.2.5.1 Enunciado

Documenta análisis forenses elaborando informes que incluyan la normativa aplicable

3.2.5.2 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.

3.3 OBJETIVOS/RESULTADOS DE APRENDIZAJE Y CRITERIOS DE EVALUACIÓN. MÍNIMOS O ESENCIALES

Todos los los objetivos/resultados de aprendizaje y criterios de evaluación indicados en el apartado anterior 3.2 se consideran mínimos o esenciales, de acuerdo al Real Decreto 479/2020, de 7 de abril, por el que se establece el título del Curso de especialización en ciberseguridad en entornos de las tecnologías de la información y se fijan los aspectos básicos del currículo.

RA1. 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.

RA2. 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

RA3. 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.

RA4. 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.

RA5. 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.

4 UNIDADES DE TRABAJO

Para cada Unidades de Trabajo vamos a ver los objetivos y resultados de aprendizaje, contenidos, distribución temporal, metodología concreta y criterios de evaluación aplicables.

El primer periodo lectivo se dedica a la introducción del módulo y su ubicación dentro del título (y el currículo cuando sea publicado). Así mismo, se ven todos los aspectos relevantes de la programación como por ejemplo los criterios de evaluación. Además se utilizarán algunos periodos lectivos para la realización de las pruebas de evaluación.

4.1 LA CUESTIÓN DE LOS MÍNIMOS

Todos los contenidos se consideran esenciales para alcanzar los objetivos

4.2 UT0: PRESENTACIÓN DEL MÓDULO

4.2.1 OBJETIVOS

1. Ubicar el módulo dentro del título.
2. Ubicar el módulo en el currículo.
3. Determinar como el módulo ayuda a conseguir los objetivos generales del ciclo.
4. Conocer la programación del módulo y sus distintas partes.
5. Conocer las normas de funcionamiento del centro y aula.

4.2.2 CONTENIDOS

- Cualificaciones que constituyen el ciclo y relación con el módulo.
- Contribución del módulo al logro de los objetivos del ciclo
- Objetivos del módulo
- Criterios de evaluación del módulo y de las unidades didácticas.

4.3 UT1. INTRODUCCIÓN. CONCEPTOS BÁSICOS

4.3.1 OBJETIVOS

1. Preparar entorno de trabajo
2. Conocer metodología a seguir
3. Conocer proceso para crear imágenes forenses

4.3.2 CONTENIDOS BÁSICOS Y NO BÁSICOS

– Identificación de los dispositivos a analizar.
– Recolección de evidencias (trabajar un escenario).

4.3.3 RESULTADOS DE APRENDIZAJE

RA1

4.4 UT2. ANÁLISIS FORENSE DE SISTEMAS WINDOWS

4.4.1 OBJETIVOS

1. Analizar evidencias volátiles y no volátiles de sistemas Windows
2. Analizar volcados de RAM de sistemas Windows
3. Analizar imágenes forenses de sistemas Windows

4.4.2 CONTENIDOS BÁSICOS Y NO BÁSICOS

– 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.

4.4.3 RESULTADOS DE APRENDIZAJE

RA1. RA5

4.5 UT3. ANÁLISIS FORENSE DE SISTEMAS LINUX/UNIX

4.5.1 OBJETIVOS

1. Analizar evidencias volátiles y no volátiles de sistemas Linux/Unix
2. Analizar volcados de RAM de sistemas Linux/Unix
3. Analizar imágenes forenses de sistemas Linux/Unix

4.5.2 CONTENIDOS BÁSICOS Y NO BÁSICOS

– 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.

4.5.3 RESULTADOS DE APRENDIZAJE

RA1

4.6 UT4. ANÁLISIS FORENSE DE DISPOSITIVOS MÓVILES

4.6.1 OBJETIVOS

Conocer de forma general el análisis forense en dispositivos móviles.

4.6.2 CONTENIDOS BÁSICOS Y NO BÁSICOS

– Métodos para la extracción de evidencias.
– Herramientas de mercado más comunes.

4.6.3 RESULTADOS DE APRENDIZAJE

RA1, RA2

4.7 UT5. ANÁLISIS FORENSE EN ENTORNOS CLOUD

4.7.1 OBJETIVOS

Conocer de forma general el análisis forense en entornos Cloud

4.7.2 CONTENIDOS BÁSICOS Y NO BÁSICOS

– 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

4.7.3 RESULTADOS DE APRENDIZAJE

RA1, RA3

4.8 UT6. ANÁLISIS FORENSE EN ENTORNOS IOT

4.8.1 OBJETIVOS

Conocer de forma general el análisis forense en entornos iOT

4.8.2 CONTENIDOS BÁSICOS Y NO BÁSICOS

– 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.

4.8.3 RESULTADOS DE APRENDIZAJE

RA1, RA4

4.9 UT7. DOCUMENTACIÓN Y ELABORACIÓN DE INFORMES DE ANÁLISIS FORENSE

4.9.1 OBJETIVOS

Aprender a hacer informes forenses técnicos y ejecutivos

4.9.2 CONTENIDOS BÁSICOS Y NO BÁSICOS

– 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.

4.9.3 RESULTADOS DE APRENDIZAJE

RA1, RA5

5 DISTRIBUCIÓN TEMPORAL

5.1 DISTRIBUCIÓN TEÓRICA PREVISTA

UT	Título	Horas	Ev
0	UT0: PRESENTACIÓN DEL MÓDULO	2	1
1	UT1. ANÁLISIS FORENSE. INTRODUCCIÓN. CONCEPTOS BÁSICOS	30	1
2	UT2. ANÁLISIS FORENSE DE SISTEMAS WINDOWS	20	1
3	UT3. ANÁLISIS FORENSE DE SISTEMAS LINUX/UNIX	20	2
4	UT4. ANÁLISIS FORENSE DE DISPOSITIVOS MÓVILES	14	2
5	UT5. ANÁLISIS FORENSE EN ENTORNOS CLOUD	14	2/3
6	UT6. ANÁLISIS FORENSE EN ENTORNOS IoT	14	3
7	UT7. DOCUMENTACIÓN Y ELABORACIÓN DE INFORMES DE ANÁLISIS FORENSE	6	3
	Total	120	

6 METODOLOGÍA

Generalmente en cada unidad de trabajo se comenzará con teoría y se pasará a la práctica en cualquier momento del proceso de enseñanza-aprendizaje. Las actividades de aprendizaje que desarrollen simularán ambientes reales. Cuando se estime oportuno se fomentará el debate entre el grupo de estudiantes, de tal forma que estos podrán reflexionar sobre la importancia de lo que se haya tratado. La metodología a utilizar en este módulo estará orientada a promover en los estudiantes:

1) Su **participación** en los procesos de enseñanza y aprendizaje, de forma que mediante la metodología activa se desarrolle su capacidad de autonomía y responsabilidad personales, de creciente importancia en el mundo profesional. Con este enfoque metodológico activo se evitará la presentación de soluciones únicas y exclusivas a los problemas o situaciones planteados, que quitan al alumnado la posibilidad del descubrimiento propio. De forma que cuando se integren profesionalmente, sepan intervenir activamente en procesos de decisión compartida de forma creativa y positiva, desarrollando un espíritu crítico constructivo y aportando soluciones alternativas.

Al ser el alumnado quien construye su propio aprendizaje, el profesor actuará como guía y mediador para facilitar la construcción de capacidades nuevas sobre la base de las ya adquiridas. También se contribuirá a que el alumnado descubra su capacidad potencial en relación con las ocupaciones implicadas en el perfil profesional correspondiente, reforzando y motivando la adquisición de nuevos hábitos de trabajo.

2) El desarrollo de la capacidad para **aprender por sí mismos**, de modo que adquieran una identidad y madurez profesionales motivadoras de futuros aprendizajes y adaptaciones al cambio de las cualificaciones.

7 MATERIALES, RECURSOS, ESPACIO DOCENTE

7.1 MATERIALES Y RECURSOS DIDÁCTICOS

- Sistemas informáticos adecuados con el software correspondiente que será fundamentalmente:
  - Herramientas gratuitas opensouce, software libre o freeware.
  - Herramientas comerciales en su versión de evaluación.
  - Distribuciones forense en entorno Linux.
  - Máquina virtuales para la realización de instalaciones y pruebas en un entorno seguro.
  - Plataforma de e-learning Moodle que dará soporte a todos los materiales y actividades que se vayan trabajando/realizando. El módulo dispondrá de un curso completo Moodle que se irán actualizando permanentemente para que refleje la realidad del proceso docente.

7.2 DISTRIBUCIÓN DEL ESPACIO Y EL TIEMPO DOCENTE

Con los equipos de los estudiantes situados en filas paralelas a la mesa del profesor, dejando un pasillos para el acceso a cada una de las filas.

Se solicita también la agrupación de las sesiones de clase en bloques de al menos 2 horas seguidas, pues está comprobado que en módulos de tipo informático agrupaciones de menor duración no son prácticas.

8 MEDIDAS PARA ESTIMULAR EL INTERÉS Y EL HÁBITO DE LECTURA Y LA CAPACIDAD DEL ESTUDIANTE PARA EXPRESARSE CORRECTAMENTE

Se hará hincapié en leer los manuales, guías y how to's del hardware y software utilizados. Se utilizará vocabulario técnico y se corregirá el uso de vocabulario indebido.

9 CRITERIOS, PROCEDIMIENTOS E INSTRUMENTOS DE EVALUACIÓN

9.2.2.4.3 CRITERIOS DE CALIFICACIÓN GENERALES A TODAS LAS UNIDADES DE TRABAJO

Para la calificación del módulo se utilizará se tendrá en cuenta la siguiente ponderación:

N	Apartado	Ponderación	Ponderación
P1	Realización de trabajo y, supuestos prácticos de las unidades de trabajo.	40 %	100%
P2	Pruebas objetivas teórico-prácticas	60 %	

La nota máxima de un trabajo o supuesto práctico del apartado P1, entregado fuera de plazo será un 5 (siempre que esté justificado). Se realizarán pruebas objetivas teórico-prácticas a lo largo del curso que tendrán carácter eliminatorio, siempre y cuando se superen con una calificación igual o superior a 5 y se hayan presentado los trabajos relativos a las unidades de que se compone el examen, habiendo obtenido igualmente una calificación igual o superior a 5 en los mismos. Cada una de las partes que conforman las pruebas escritas se evaluará independientemente de las anteriores, por lo que la superación de una prueba (teniendo en cuenta que también se haya superado sus respectivas prácticas) no implica la superación de las anteriores, y por tanto cada prueba no superada tendrá su

correspondiente examen de recuperación. Siendo necesario aprobarlas todas para poder aprobar la evaluación. En caso de que no hayan pruebas teórico-prácticas, P1 será el 100% de la nota.

La calificación de cada trimestre se calculará a partir de las notas de las pruebas escritas y los ejercicios prácticos de acuerdo a la cuantificación anteriormente indicada y teniendo en cuenta la ponderación que el profesor determine para cada prueba escrita o ejercicio práctico.

El estudiante se presentará a la evaluación ordinaria de junio de aquellos trimestres que no haya superado. Para la evaluación extraordinaria el estudiante irá con toda la materia del curso, independientemente si tenía o no aprobado algún trimestre.

9.2.2.4.3.2 Cálculo de la calificación final

La calificación final será calculada como la media aritmética ponderada de todas las notas obtenidas y acumulas durante el curso.

9.2.2.4.3.3 Recuperación

Evaluación ordinaria. Una recuperación para la primera evaluación y otra para la segunda (los estudiantes se examinarán de las unidades de trabajo que no hayan superado.). Para la tercera evaluación no habrá recuperación. Los estudiantes que aprueben las dos primeras evaluaciones y suspendan la tercera se examinarán en junio solamente de la tercera evaluación.

Extraordinaria. La prueba de recuperación final de junio será sobre las evaluaciones pendientes. Para la calificación final de junio se tendrán en cuenta los resultados obtenidos durante todas las evaluaciones.

Cabe la posibilidad de que se puedan hacer 2 tipos de exámenes, unos para los que han asistido regularmente a clase y otros para los que han perdido la evaluación continua, garantizando así la igualdad de oportunidades.

10 ATENCIÓN A LA DIVERSIDAD DEL ALUMNADO EN LOS CICLOS FORMATIVOS

10.1 CUESTIONES GENERALES

Atender a la diversidad del alumnado es una labor en la que hay que anticiparse, incorporando en la planificación docente recursos y estrategias variadas para dar respuesta a las diversas necesidades que de hecho se van a producir. Los mejores proyectos y programaciones serán aquellos que favorezcan estos cambios habituales y den respuestas a estas diferencias individuales (estilos de aprendizaje, motivaciones, intereses o dificultades de aprendizaje transitorias).

La individualización se plasmará en los siguientes aspectos:

- Utilización de una evaluación individualizada en la que se fijan las metas partiendo de criterios individualizados (evaluación inicial).
- Uso de estrategias diferenciadas que permitan ritmos distintos y niveles de consecución diferentes.

- Actuación del profesor como mediador y organizador del proceso enseñanza-aprendizaje de acuerdo con la progresión de cada estudiante.
- Colaboración y coordinación con los demás profesores del equipo docente para conseguir el cumplimiento de los objetivos generales de etapa.

Habrá que asumir las diferencias individuales como algo característico del quehacer pedagógico.

Las medidas que se adopten para ello deben de caracterizarse por:

- Tener un carácter ordinario y no precisar una organización muy diferente de la habitual.
- No afectar a los componentes prescriptivos del currículo.

Según las circunstancias y manteniendo los mismos objetivos educativos es posible:

- Plantear metodologías y niveles de ayuda diversos.
- Proporcionar actividades de aprendizaje diferenciadas
- Prever adaptaciones de material didáctico.
- Organizar grupos de trabajo flexibles.
- Acelerar o frenar el ritmo de introducción de nuevos contenidos
- Organizar o secuenciar los contenidos de forma distinta.

Cambiar la prioridad y la profundización de los contenidos.

Las diferencias metodológicas provocarán variaciones en la forma de enfocar o presentar los contenidos y/o actividades y su elección se basará entre otros en:

- El grado de conocimiento previo detectado.
- El grado de autonomía y responsabilidad.
- Las dificultades detectadas previamente.

Por otro lado, es importante ofrecer una amplia gama de actividades asociadas a diferentes grados de aprendizaje ajustando la ayuda pedagógica a la variedad de necesidades educativas de la siguiente forma:

- Estableciendo en cada unidad de trabajo los diferentes grupos de actividades.
- Representando las actividades de forma secuencial y a modo de actividades graduadas, lo que permitirá desmenuzar los contenidos y trabajar un mismo contenido de diversas maneras, a la par que ir caminando hacia actividades más significativas.

Otras medidas pueden consistir en la organización de grupos de trabajo flexibles en el seno del grupo básico, lo que permitirá establecer tareas de refuerzo, de profundización, etc., en función de las diferentes necesidades del grupo. Para ello es necesario reflexionar sobre:

- Los aprendizajes básicos e imprescindibles para seguir progresando.
- La evaluación que detecte las necesidades de cada grupo.
- El uso de materiales didácticos específicos diseñados en este sentido.

10.2 PROCEDIMIENTOS

Todas las adaptaciones que se realicen serán del tipo "Acceso al Currículo" ya que la legislación vigente no permite otra cosa para el nivel educativo donde nos encontramos.

11 PREVENCIÓN DE RIESGOS LABORALES

Respecto a la prevención de riesgos laborales, considerando que el ámbito laboral más común va a ser el de las oficinas y centros de procesos de datos, habrá que haber insistido a diario de la importancia de conocer y prevenir los posibles riesgos.

12 INTERDISCIPLINARIEDAD

En este caso, al tratarse de un módulo de contenidos eminentemente prácticos, centrado en el análisis forense informático, surgen relaciones de interdisciplinariedad evidentes con el resto de módulos del curso.

13 TRANSVERSALIDAD

La transversalidad significa que ciertos elementos cognitivos o valorativos, que reflejan, a su vez, ciertas consideraciones sociales apreciadas como fundamentales para la formación de los ciudadanos, deben estar presentes en el proceso educativo. Sin embargo esta presencia tiene un carácter especial, ya que esos elementos han de servir de guía y orientación de todas las acciones educativas a emprender, al tiempo que reclama una actuación educativa más horizontal frente a la tradicional verticalidad que presidía las relaciones en el seno del Sistema Educativo.

Los temas transversales son un conjunto de contenidos educativos y ejes conductores de la actividad escolar que, no estando ligados a ninguna materia en particular, se puede considerar que son comunes a todas, de forma que, más que crear disciplinas nuevas, se ve conveniente que su tratamiento sea transversal en el currículum global del centro. La alta presencia de contenidos actitudinales en estos temas, junto al hecho del carácter prescriptivo de las actitudes y valores, como componentes de los objetivos de etapa y contenidos de áreas curriculares, convierte a estos temas en un elemento esencial del desarrollo curricular.

Estos temas transversales se organizan en los siguientes ámbitos:

- Educación del consumidor
- Educación para la igualdad de oportunidades de ambos sexos
- Educación para la paz
- Educación ambiental
- Educación para la salud
- Educación sexual
- Educación moral y cívica

Tratándose de un curso de especialización, a veces, la conexión con un tema transversal parece clara, pero en ocasiones es muy difícil casarlos con determinados módulos, resultando una tarea ardua incorporar en su currículo temas transversales. Eso es lo que ocurre en casi todos los módulos de este ciclo formativo. No vemos, en general y salvo casos especiales que se indican en la programación modular, la forma de integrar esa educación en valores con la programación de unos módulos cuyo desarrollo es absolutamente técnico y, casi siempre, de elevado nivel.

Pensamos que es en el desarrollo en el aula donde cabe hablar de valores y comportamientos, así como de su aprendizaje, pues este tipo de elementos forma parte de los que se conoce como currículo oculto. Por ejemplo, respecto a la educación para el consumidor el uso razonable de los dispositivos informáticos, sin caer en el abuso, el evitar actitudes de compra compulsiva para los nuevos desarrollos tecnológicos, etc. En la educación para la paz, tratar el tema de la violencia en los juegos informáticos. En la educación para la salud los efectos perniciosos del uso de sistemas informáticos

cuando se abusa de ellos en lugar de realizar otras tareas más dinámicas, así como el uso adecuado desde el punto de vista postural. En la educación ambiental el valor del reciclaje y del consumo razonable de los recursos y materiales fungibles, como papel, energía eléctrica, etc. En la igualdad de oportunidades de ambos sexos comentar el por qué de la alta "masculinización" de los puestos de trabajo informáticos. En la educación moral y cívica la no discriminación frente a cuestiones de índole religiosa, sexual, política, etc., así como el respeto a la confidencialidad de la información y el rechazo a actividades no cívicas, como la propagación de virus informáticos, el hackeo de aplicaciones con fines diferentes al aprendizaje, o el pirateo con fines lucrativos de contenidos informáticos. También se puede tratar en este tema el valor intrínseco del movimiento de software libre y abierto respecto al software propietario.

En definitiva, aunque en los decretos que establecen el currículo de los ciclos formativos no han sido incorporados los temas transversales, desde la docencia de los módulos formativos se pueden hacer algunas recomendaciones y sugerencias para que se tengan en cuenta a lo largo del desarrollo curricular los valores y actitudes recogidos en los temas transversales.

14 ACTIVIDADES COMPLEMENTARIAS Y EXTRAESCOLARES

Como actividad extraescolar se prevé que expertos en ciberseguridad y/o peritaje forense den alguna charla. También nos sumaremos a las actividades generales del Departamento.

15 USO DE LAS TICS

Al tratarse de módulos de un ciclo formativo de Informática, con contenidos, procedimientos, etc., totalmente inmersos dentro del ámbito de las Tecnologías de la Información y las Comunicaciones, podemos decir que prácticamente el cien por cien de su desarrollo se hace con utilización plena y sistemática de este tipo de tecnologías y recursos.

16 BIBLIOGRAFÍA

16.1 BIBLIOGRAFÍA CERCANA AL CURRÍCULO OFICIAL

En este módulo no hay un libro de texto que se vaya a seguir de forma habitual. Los materiales de clase se irán depositando bien en el servidor Moodle del Centro, bien en un servidor FTP accesible al alumnado o indicándose el URL donde pueden ser accedidos.

16.2 BIBLIOGRAFÍA COMPLEMENTARIA

El problema de la bibliografía en un entorno tan inmensamente cambiante como es el de la ciberseguridad es la obsolescencia acelerada que hace que un texto que hoy es plenamente válido deje de serlo en pocos meses. En el campo de la ciberseguridad en general ocurre que la bibliografía disponible en español no es ni muy extensa ni se adapta especialmente a los contenidos de este módulo. La bibliografía utilizada proviene principalmente de internet.

16.3 WEBGRAFÍA

Enunciar aquí un conjunto de enlaces web relacionados con el módulo que nos ocupa podría ser tan interminable como inútil, dada la alta variabilidad de estos enlaces de Internet e incluso de los ele-

mentos de interés sobre los que se indican enlaces. No obstante el uso de los recurso disponibles en la web se hace imprescindible en este módulo.