



Región de Murcia

Consejería de Educación
y Universidades



Unión Europea
Fondo Social Europeo



C/ La Iglesia, s/n

30012 Patiño (Murcia)

968266922 968342085

DEPARTAMENTO DE FP DE INFORMÁTICA. PROGRAMACIÓN DIDÁCTICA

Ciberseguridad

Pág: 1 de 18

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

PROGRAMACIÓN ANUAL

Parte específica del módulo:
5021. Incidentes de Ciberseguridad

Departamento de Familia Profesional de Informática

Curso: 2023-24
Turno: vespertino



Región de Murcia

Consejería de Educación
y Universidades



Unión Europea
Fondo Social Europeo



C/ La Iglesia, s/n

30012 Patiño (Murcia)

968266922 968342085

DEPARTAMENTO DE FP DE INFORMÁTICA. PROGRAMACIÓN DIDÁCTICA

MÓDULO : Incidentes de Ciberseguridad

Pág: 2 de 18

ESQUEMA DE CONTENIDOS

1 CARACTERÍSTICAS GENERALES DEL CURSO DE ESPECIALIZACIÓN EN CIBERSEGURIDAD EN ENTORNOS DE TECNOLOGÍAS DE LA INFORMACIÓN.....	3
2 DESCRIPCIÓN DEL MÓDULO.....	3
3 UBICACIÓN, OBJETIVOS, CONTENIDOS Y DISTRIBUCIÓN TEMPORAL DEL MÓDULO.....	3
3.1 UBICACIÓN, DISTRIBUCIÓN TEMPORAL Y CARACTERÍSTICAS.....	3
3.2 OBJETIVOS/RESULTADOS DE APRENDIZAJE Y CRITERIOS DE EVALUACIÓN.....	3
4 UNIDADES DE TRABAJO.....	6
5 DISTRIBUCIÓN TEMPORAL.....	8
5.1 DISTRIBUCIÓN TEÓRICA PREVISTA (a 4 horas semanales).....	8
5.2 ANÁLISIS DE LA VIABILIDAD DEL CURRÍCULO PREVISTO.....	8
6 METODOLOGÍA.....	8
6.1 CRITERIOS.....	8
6.2 ASPECTOS CONCRETOS.....	8
7 MATERIALES, RECURSOS, ESPACIO DOCENTE.....	9
7.1 MATERIALES Y RECURSOS DIDÁCTICOS.....	9
7.2 DISTRIBUCIÓN DEL ESPACIO Y EL TIEMPO DOCENTE.....	9
8 MEDIDAS PARA ESTIMULAR EL INTERÉS Y EL HÁBITO DE LECTURA Y LA CAPACIDAD DEL ALUMNO PARA EXPRESARSE CORRECTAMENTE.....	9
9 CRITERIOS, PROCEDIMIENTOS E INSTRUMENTOS DE EVALUACIÓN.....	10
9.2.2.3.3.2. Cálculo de la calificación final.....	10
10 ALUMNOS MATRICULADOS EN 2º CON MÓDULOS DE 1º SUSPENSOS.....	10
11 ATENCIÓN A LA DIVERSIDAD DEL ALUMNADO EN LOS CICLOS FORMATIVOS....	10
12 PREVENCIÓN DE RIESGOS LABORALES.....	10
13 INTERDISCIPLINARIEDAD.....	10
14 TRANSVERSALIDAD.....	10
15 ACTIVIDADES COMPLEMENTARIAS Y EXTRAESCOLARES.....	10
16 USO DE LAS TICS.....	11
17 BIBLIOGRAFÍA.....	11

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

Se relacionan en la parte general de la programación de los ciclos formativos.

2 DESCRIPCIÓN DEL MÓDULO

Este módulo profesional, al cual hace referencia esta programación didáctica, está enmarcado dentro de las enseñanzas del Curso de Especialización en Ciberseguridad en Entornos de las Tecnologías de la Información.

No existe actualmente publicado currículum del presente curso en el ámbito de la Comunidad Autónoma de la Región de Murcia por lo que no hay ninguna base que sustente los contenidos ya que el número de horas de los módulos es muy diferente de lo legislado en territorio MEC donde sí se ajusta al número de horas del RD 479/20.

Se entiende, al menos por el que redacta esta programación, que, en este caso más que nunca, la programación no puede ser válida hasta que haya legislación de currículum por parte de la CARM, apoyada esta afirmación por la ya indicada extraordinaria diferencia en horas con lo dispuesto en el RD siendo por tanto una mera declaración de intenciones.

3 UBICACIÓN, OBJETIVOS, CONTENIDOS Y DISTRIBUCIÓN TEMPORAL DEL MÓDULO

3.1 UBICACIÓN, DISTRIBUCIÓN TEMPORAL Y CARACTERÍSTICAS

El Real Decreto 479/2020, de 7 de abril (BOE nº134 de 13 de mayo), establece los aspectos básicos del currículum para este curso de especialización que cuenta con un total de 720 horas de duración, de las cuales a este módulo profesional le corresponden 80 horas. Todo esto teniendo en consideración el Real Decreto 1147/2011, de 29 de julio, por el que se establece la ordenación general de la formación profesional del sistema educativo y única referencia oficial aprobada al día de entrega de esta programación didáctica.

Para este módulo, se han asignado 4 horas semanales en el horario propuesto por la Consejería de Educación de la Región de Murcia que en el calendario actual lectivo de 2022-2023 para el municipio de Murcia llegan a sumar 150 horas de clase y equivalentes sin embargo a solamente 9 ECTS en el RD de Título. Sin otra legislación al respecto el que redacta esta programación entiende que el alumnado solamente tendría que cursar la parte proporcional horaria del módulo para superarlo.

3.2 OBJETIVOS/RESULTADOS DE APRENDIZAJE Y CRITERIOS DE EVALUACIÓN

De conformidad con lo regulado en el Real Decreto 479/2020, de 7 de abril, por el que se establece el Curso de especialización en Ciberseguridad, este módulo contribuye a alcanzar las siguientes **competencias profesionales del curso de especialización**:

- Elaborar e implementar planes de prevención y concienciación en ciberseguridad en la organización, aplicando la normativa vigente.
- Detectar e investigar incidentes de ciberseguridad, documentándolos e incluyéndolos en los planes de securización de la organización.
- Elaborar documentación técnica y administrativa cumpliendo con la legislación vigente, respondiendo a los requisitos establecidos.
- 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.
- 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.

- 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.
- 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

También contribuye a conseguir los siguientes objetivos generales:

- 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.
- 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.
- Detectar incidentes de ciberseguridad implantando los controles, las herramientas y los mecanismos necesarios para su monitorización e identificación.
- Analizar y dar respuesta a incidentes de ciberseguridad, identificando y aplicando las medidas necesarias para su mitigación, eliminación, contención o recuperación.
- Desarrollar manuales de información, utilizando herramientas ofimáticas y de diseño asistido por ordenador para elaborar documentación técnica y administrativa.
- 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
- 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.
- 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.
- Identificar y proponer las acciones profesionales necesarias para dar respuesta a la accesibilidad universal y al «diseño para todas las personas».
- 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.

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, se indica la competencia general, así como las **competencias profesionales**, personales y sociales del mismo. Las competencias correspondientes a este módulo son las siguientes:

- Elaborar e implementar planes de prevención y concienciación en ciberseguridad en la organización, aplicando la normativa vigente.
- Detectar e investigar incidentes de ciberseguridad, documentándolos e incluyéndolos en los planes de securización de la organización.
- Elaborar documentación técnica y administrativa cumpliendo con la legislación vigente, respondiendo a los requisitos establecidos.
- 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.
- 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.
- 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.
- 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

En cuanto a resultados de aprendizaje y criterios de evaluación:

Este módulo profesional está formado por una serie de resultados de aprendizaje descritos en términos de competencias y que el alumnado debe adquirir como resultado del proceso de enseñanza-aprendizaje. Con cada uno de estos resultados de aprendizaje se encuentran relacionados los criterios de evaluación, mediante los cuales se acredita la consecución de las competencias.

1. Desarrolla planes de prevención y concienciación en ciberseguridad, estableciendo normas y medidas de protección.

Criterios de evaluación:

- a) Se han definido los principios generales de la organización en materia de ciberseguridad, que deben ser conocidos y apoyados por la dirección de la misma.
- b) Se ha establecido una normativa de protección del puesto de trabajo.
- c) Se ha definido un plan de concienciación de ciberseguridad dirigido a los empleados.

d) Se ha desarrollado el material necesario para llevar a cabo las acciones de concienciación dirigidas a los empleados.

e) Se ha realizado una auditoría para verificar el cumplimiento del plan de prevención y concienciación de la organización.

2. Analiza incidentes de ciberseguridad utilizando herramientas, mecanismos de detección y alertas de seguridad.

Criterios de evaluación:

a) Se ha clasificado y definido la taxonomía de incidentes de ciberseguridad que pueden afectar a la organización.

b) Se han establecido controles, herramientas y mecanismos de monitorización, identificación, detección y alerta de incidentes

c) Se han establecido controles y mecanismos de detección e identificación de incidentes de seguridad física.

d) Se han establecido controles, herramientas y mecanismos de monitorización, identificación, detección y alerta de incidentes a través de la investigación en fuentes abiertas (OSINT: Open Source Intelligence).

e) Se ha realizado una clasificación, valoración, documentación y seguimiento de los incidentes detectados dentro de la organización.

3. Investiga incidentes de ciberseguridad analizando los riesgos implicados y definiendo las posibles medidas a adoptar.

Criterios de evaluación:

a) Se han recopilado y almacenado de forma segura evidencias de incidentes de ciberseguridad que afectan a la organización.

b) Se ha realizado un análisis de evidencias.

c) Se ha realizado la investigación de incidentes de ciberseguridad.

d) Se ha intercambiado información de incidentes, con proveedores y/o organismos competentes que podrían hacer aportaciones al respecto.

e) Se han iniciado las primeras medidas de contención de los incidentes para limitar los posibles daños causados.

4. Implementa medidas de ciberseguridad en redes y sistemas respondiendo a los incidentes detectados y aplicando las técnicas de protección adecuadas.

Criterios de evaluación:

a) Se han desarrollado procedimientos de actuación detallados para dar respuesta, mitigar, eliminar o contener los tipos de incidentes de ciberseguridad más habituales.

b) Se han preparado respuestas ciberresilientes ante incidentes que permitan seguir prestando los servicios de la organización y fortaleciendo las capacidades de identificación, detección, prevención, contención, recuperación y cooperación con terceros.

c) Se ha establecido un flujo de toma de decisiones y escalado de incidentes interno y/o externo adecuados.

d) Se han llevado a cabo las tareas de restablecimiento de los servicios afectados por un incidente hasta confirmar la vuelta a la normalidad.

e) Se han documentado las acciones realizadas y las conclusiones que permitan mantener un registro de “lecciones aprendidas”.

f) Se ha realizado un seguimiento adecuado del incidente para evitar que una situación similar se vuelva a repetir.

5. Detecta y documenta incidentes de ciberseguridad siguiendo procedimientos de actuación establecidos.

Criterios de evaluación:

a) Se ha desarrollado un procedimiento de actuación detallado para la notificación de incidentes de ciberseguridad en los tiempos adecuados.

b) Se ha notificado el incidente de manera adecuada al personal interno de la organización responsable de la toma de decisiones.

c) Se ha notificado el incidente de manera adecuada a las autoridades competentes en el ámbito de la gestión de incidentes de ciberseguridad en caso de ser necesario.

d) Se ha notificado formalmente el incidente a los afectados, personal interno, clientes, proveedores, etc., en caso de ser necesario.

e) Se ha notificado el incidente a los medios de comunicación en caso de ser necesario.

Duración: 80 horas.

Contenidos básicos:

Desarrollo de planes de prevención y concienciación en ciberseguridad:

- Principios generales en materia de ciberseguridad.
- Normativa de protección del puesto del trabajo.
- Plan de formación y concienciación en materia de ciberseguridad.
- Materiales de formación y concienciación.
- Auditorías internas de cumplimiento en materia de prevención.

Auditoría de incidentes de ciberseguridad:

- Taxonomía de incidentes de ciberseguridad.
- Controles, herramientas y mecanismos de monitorización, identificación, detección y alerta de incidentes: tipos y fuentes
- Controles, herramientas y mecanismos de detección e identificación de incidentes de seguridad física.
- Controles, herramientas y mecanismos de monitorización, identificación, detección y alerta de incidentes a través de la investigación en fuentes abiertas (OSINT).
- Clasificación, valoración, documentación, seguimiento inicial de incidentes de ciberseguridad.

Investigación de los incidentes de ciberseguridad:

- Recopilación de evidencias.
- Análisis de evidencias.
- Investigación del incidente

- Intercambio de información del incidente con proveedores u organismos competentes.

- Medidas de contención de incidentes.

Implementación de medidas de ciberseguridad:

- Desarrollar procedimientos de actuación detallados para dar respuesta, mitigar, eliminar o contener los tipos de incidentes.

- Implantar capacidades de ciberresiliencia.

- Establecer flujos de toma de decisiones y escalado interno y/o externo adecuados.

- Tareas para reestablecer los servicios afectados por incidentes.

- Documentación

- Seguimiento de incidentes para evitar una situación similar.

Detección y documentación de incidentes de ciberseguridad:

- Desarrollar procedimientos de actuación para la notificación de incidentes.

- Notificación interna de incidentes.

- Notificación de incidentes a quienes corresponda.

4 UNIDADES DE TRABAJO

De las Unidades de Trabajo vamos a prever, en lo posible, los objetivos y resultados de aprendizaje, contenidos, distribución temporal, metodología concreta y criterios de evaluación aplicables.

1. Desarrollo de planes de prevención y concienciación en ciberseguridad:

1.1 Principios generales en materia de ciberseguridad.

1.2 Normativa de protección del puesto del trabajo.

1.3 Plan de formación y concienciación en materia de ciberseguridad.

1.4 Materiales de formación y concienciación.

1.5 Auditorías internas de cumplimiento en materia de prevención.

2. Elaboración de un entorno para dar respuesta a incidentes. Backups

2.1 Backups multiplataforma

2.2 Sistemas de ficheros con snapshots y sincronización incremental entre hosts

3. Auditoría de incidentes de ciberseguridad:

3.1 Taxonomía de incidentes de ciberseguridad.

3.2 Controles, herramientas y mecanismos de monitorización, identificación, detección y alerta de incidentes: tipos y fuentes

3.2.1. Elaboración de un entorno para dar respuesta a incidentes. Logs

3.2.1.1 Puesta en marcha de sistemas de detección de intrusos.

3.2.1.2 Puesta en marcha de sistemas de recolección de logs

3.2.1.3 Puesta en marcha de sistemas de análisis y tratamiento de logs

3.3 Controles, herramientas y mecanismos de detección e identificación de incidentes de seguridad física.

3.4 Controles, herramientas y mecanismos de monitorización, identificación, detección y alerta de incidentes a través de la investigación en fuentes abiertas (OSINT).

3.5 Clasificación, valoración, documentación, seguimiento inicial de incidentes de ciberseguridad.

4. Investigación de los incidentes de ciberseguridad:

4.1 Recopilación de evidencias.

4.2 Análisis de evidencias.

4.3 Investigación del incidente

4.4 Intercambio de información del incidente con proveedores u organismos competentes.

4.5 Medidas de contención de incidentes.

5. Implementación de medidas de ciberseguridad:

5.1 Desarrollar procedimientos de actuación detallados para dar respuesta, mitigar, eliminar o contener los tipos de incidentes.

5.2 Implantar capacidades de ciberresiliencia.

5.3 Establecer flujos de toma de decisiones y escalado interno y/o externo adecuados.

5.4 Tareas para reestablecer los servicios afectados por incidentes.

5.5 Documentación

5.6 Seguimiento de incidentes para evitar una situación similar.

6. Detección y documentación de incidentes de ciberseguridad:

6.1 Desarrollar procedimientos de actuación para la notificación de incidentes.

6.2 Notificación interna de incidentes.

6.3 Notificación de incidentes a quienes corresponda.

5 DISTRIBUCIÓN TEMPORAL

5.1 DISTRIBUCIÓN TEÓRICA PREVISTA (A 4 HORAS SEMANALES > 80 HORAS)

Primer Trimestre

U.T. 0: Presentación del módulo (2 horas)

U.T. 1: 6 horas

U.T. 2: 12 horas

Segundo Trimestre

U.T. 3: 30 horas

U.T. 4: 10 horas

Tercer Trimestre

U.T. 5: 12 horas

U.T. 6: 10 horas

5.2 ANÁLISIS DE LA VIABILIDAD DEL CURRÍCULO PREVISTO

Los contenidos planificados se pueden impartir con bastante holgura ya que el módulo en el RD correspondiente consta de un asignación de 80 horas y en la distribución temporal realizada por la administración educativa de la Comunidad Autónoma de la Región de Murcia para 2022-2023 se le asigna un cómputo de horas de 4 horas semanales que llegan a unas 150 horas anuales mayorando casi al doble la imputación horaria del RD sin una normativa legal adecuada por parte de esta CA.

No se ha dotado al curso de especialización con materiales al respecto a pesar de que el Departamento de Informática, al que está adscrita esta enseñanza, fue requerido a finales del pasado curso para que expresase las necesidades para su correcta impartición. Tras enviar la solicitud de material no solamente no se ha dotado con absolutamente nada del material solicitado sino que se ha ignorado totalmente la petición hasta el punto de ni siquiera hacer sido respondida la petición por parte de nuestra Conejería.

6 METODOLOGÍA

6.1 CRITERIOS

6.2 ASPECTOS CONCRETOS

Los aspectos metodológicos que se pretenden aplicar en este módulo descansan en la idea de que el alumno se considere parte activa de la actividad docente, con esto se pretende involucrarlo en el proceso de asimilación de nuevos conceptos y adquisición de capacidades no como un mero contenedor de éstas sino como un productor directo de estos conocimientos y habilidades en sí mismo. De igual forma se pretende que el alumno respete al profesor y a sus compañeros, respetando igualmente el material de la clase.

- ✓ La metodología didáctica favorecerá, mediante la integración de los contenidos científicos tecnológicos y organizativos una visión global y coordinada de los procesos productivos en los que debe intervenir el alumnado.

El trabajo en el aula consistirá en la exposición oral de cada unidad de trabajo, para que, posteriormente, los alumnos desarrollen los ejercicios y prácticas propuestos.

La metodología será participativa, favoreciendo el aprendizaje por descubrimiento.

Partiendo de los conocimientos iniciales de los alumnos/as, estos deberán construir sus aprendizajes significativos.

La metodología será teórico-práctica, acompañada de situaciones que reflejen la realidad en la mayor medida posible, huyendo de ejemplos y ejercicios abstractos.

Estos aspectos prácticos del módulo se desarrollarán en la forma de:

- 1 Experiencias didácticas: las realiza el profesor.
- 2 Experiencias prácticas: las realizan los alumnos, el profesor corrige técnicas de trabajo y evalúa resultados.

Para el trabajo en el aula, los alumnos dispondrán de toda la documentación que se considere oportuna, además de la asistencia permanente del profesor.

7 MATERIALES, RECURSOS, ESPACIO DOCENTE

7.1 MATERIALES Y RECURSOS DIDÁCTICOS

NOTA IMPORTANTE: No se ha enviado ni un euro en materia de dotación específica para este curso de especialización. El material necesario para impartir este módulo dista mucho del material existente en los centros por lo que no es posible desarrollar los contenidos adecuadamente mientras no se dote a los centros de unos recursos mínimos.

Los recursos con los que se cuenta para impartir este módulo son los siguientes:

Para las explicaciones de contenidos teóricos:

Aula con medios audiovisuales:

- ✓ Pizarra.
- ✓ Proyector y pantalla.
- ✓ Ordenador con Linux Mint, LibreOffice
- ✓ Distribuciones Linux de seguridad y testeo.

Para la confección de los trabajos de los alumnos:

- ✓ Conexión a Internet en el aula.
- ✓ Correo electrónico
- ✓ Moodle en el IES, con carga de trabajo extra para el profesorado, ya que la conexión al supuestamente facilitado por educación es peor que inestable.

Como se puede ver no hay ningún material especializado para un curso de especialización.

7.2 DISTRIBUCIÓN DEL ESPACIO Y EL TIEMPO DOCENTE

Se opta por la “organización tipo A” que se explica en la parte general de la programación del Dpto.

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

Este apartado se estudia en la parte general de la programación del Dpto.

9 CRITERIOS, PROCEDIMIENTOS E INSTRUMENTOS DE EVALUACIÓN

9.2.2.3.3.1 Aspectos y apartados a ponderar.

Se sigue el Modelo 6 (original, sin cambios) de la Programación General del Dpto.

Partiendo de las Realizaciones de aprendizaje dispuestas en el currículo, y para cada una de ellas, se valorarán los siguientes aspectos y ponderaciones:

Apartado	Ponderación
Pruebas objetivas basadas en: <ul style="list-style-type: none">○ cuestionarios○ enunciados teórico-prácticos de aplicación amplia de los contenidos○ prácticas de laboratorio○ prácticas reales sobre el terreno○ actividades de investigación○ actividades de documentación○ actividades extraescolares directamente conectadas con el currículo○ participación en actividades cooperativas○ otras pruebas	100 % (*)

Hay que tener en cuenta las consideraciones:

- Todas las prácticas propuestas en el curso son de entrega obligatoria. La no entrega en plazo y forma de un porcentaje igual o superior al 20% implica la no superación del módulo correspondiente, que podrá evaluarse como máximo con la calificación "4".
- Las pruebas y prácticas que no se realicen íntegramente durante el periodo lectivo en el aula (por abarcar más de un día.) no se considerarán para el cálculo de la calificación, aunque tienen la misma consideración de obligatorias.
- (*) La calificación de cada periodo trimestral de evaluación será la media ponderada de las notas obtenidas en todas las pruebas objetivas de aprendizaje acumuladas durante dicho periodo (multiplicando cada calificación por el número de periodos lectivos que dicha prueba abarque, y dividiendo la suma por total de periodos que tenga el módulo en la evaluación considerada)
- En caso de falta de asistencia justificada la nota no influirá en la media ponderada, ni negativa ni positivamente.

Calcúlo de la calificación final

Calificación final: se seguirá el **método 1 (original, sin cambios) de la Programación General del Dpto.** La calificación final del módulo se expresa en cifras de 1 a 10 sin decimales, y MH en su caso. Consistirá en la media ponderada de la calificación obtenida en cada una de las tres evaluaciones, en el caso de haberlas superado todas. En caso contrario, la calificación final será la calificación menor de las tres.

Recuperación

1 La recuperación consistirá en la entrega de prácticas iguales o similares a las desarrolladas a lo largo del curso. Los criterios serán los mismos que los llevados a cabo durante el curso.

Recuperaciones parciales

- Al final de cada evaluación trimestral (excepto en el último trimestre) o al comienzo de la siguiente se realizará una prueba objetiva de recuperación.

Recuperación en convocatoria ordinaria

Se guardarán las evaluaciones superadas **dentro del mismo curso académico hasta la convocatoria extraordinaria**, de forma que el alumnado que ha superado una evaluación no tiene que volver a presentarse.

La nota máxima que se puede obtener en cada evaluación pendiente en esta recuperación es 5.

Recuperación en convocatoria extraordinaria

Este módulo **tiene convocatoria extraordinaria**. Para acceder a dicha prueba deben entregarse previamente todas las prácticas y actividades que se hayan realizado durante el curso en la plataforma moodle.

La nota máxima que se puede obtener en cada evaluación pendiente en esta recuperación es 5.

2 Alumnado que repite el módulo

Se evalúa igual que el resto

10 ALUMNOS MATRICULADOS EN 2º CON MÓDULOS DE 1º SUSPENSOS

No aplica

11 ATENCIÓN A LA DIVERSIDAD DEL ALUMNADO EN LOS CICLOS FORMATIVOS

No aplica.

12 PREVENCIÓN DE RIESGOS LABORALES

Este apartado se estudia en la parte general de la programación de los ciclos de la misma familia profesional del centro.

13 INTERDISCIPLINARIEDAD

Al ser un módulo general y transversal se relaciona con todos los módulos del curso de especialización.

14 TRANSVERSALIDAD

Al ser un módulo general y transversal se relaciona con todos los módulos del curso de especialización.

15 ACTIVIDADES COMPLEMENTARIAS Y EXTRAESCOLARES

No se han previsto.

16 USO DE LAS TICS

Al ser un curso de especialización post-ciclo las TIC's vienen incluidas en todas y cada una de los trabajos y tareas a realizar aunque hay que contar con el material del resto de ciclos que se imparten en el IES, dotaciones por otro lado obsoletas y sin renovar en, al menos, el último lustro, ya que no se ha enviado dotación alguna.

17 BIBLIOGRAFÍA

- ✓ Apuntes de clase
- ✓ Videos públicos propuestos por el profesor

18 LABORATORIO

- ✓ Inexistente por no enviar dotación alguna la administración ni atender (ni siquiera responder) los requerimientos realizados.
- ✓ Como consta en las actas del Dpto de Informática, este profesor que redacta esta programación didáctica (responsabilidad por otra parte del Dpto) ha solicitado en la práctica totalidad de las reuniones el material necesario para una correcta impartición del ciclo sin tener conocimiento alguno de que haya servido para nada. De hecho la consideración de que no existan desviaciones se hace a partir de lo que se puede hacer sin material del ciclo de cara a la evaluación y seguimiento de las programaciones. Se considera que no hay desviación al no existir el material requerido. Así que no puede haber desviación ya que se hace lo que buenamente se puede en un curso de especialización sin dotación que en otras Comunidades Autónomas ha sido dotado, al parecer, con decenas de miles de euros.

ANEXO I

Normativa de exámenes

Los exámenes se realizarán en la fecha y hora indicadas por el profesor de la asignatura.

Los alumnos podrán sugerir realizar cambios en la fecha y hora indicadas, sugerencia que deberá ser trasladada al profesor mediante el delegado o el subdelegado del grupo, y sólo en el caso de que la propuesta sea secundada por una amplia mayoría de la clase.

Si algún alumno desea oponerse al cambio de fecha/hora podrá hacerlo bien públicamente en clase o bien en privado dirigiéndose directamente al profesor. El profesor tomará la decisión intentando no perjudicar a los alumnos que se hayan preparado la materia para la fecha de examen inicialmente prevista.

La **no asistencia** a examen supone la calificación de **No presentado**. Un alumno no puede aprobar este módulo si en alguno de los exámenes que componen el curso tiene finalmente la calificación de No Presentado, es decir, si nunca se ha presentado a examen de una parte en concreto.

En caso de no asistencia por causas debidamente justificadas, al alumno se le podrá examinar en otra fecha siempre y cuando justifique debidamente su ausencia, mediante justificante médico, de trabajo, asistencia a exámenes de otras enseñanzas oficiales, justificante del padre o tutor (sólo para menores de edad), etc. En cualquier caso la aceptación del justificante quedará a elección del profesor, que podrá rechazar dicho justificante.

En caso de que la realización del examen a un alumno que no haya asistido en su fecha suponga, a juicio del profesor, perjuicio para el desarrollo normal de la asignatura, no se le realizará el cambio de examen a otra fecha.

El alumno sólo podrá hacer uso en cada examen, práctica o prueba del material expresamente autorizado en cada caso, o bien autorizado implícitamente porque sea necesario para la realización del examen: bolígrafo, folio en blanco, ordenador si es necesario, etc. El uso o tenencia de cualquier otro material no autorizado expresamente supone la nulidad de todo lo realizado por el alumno en dicho examen hasta ese momento, y la correspondiente calificación de 0 (cero) en dicho examen, práctica o prueba.

Igualmente, se considera material no autorizado cualquier tipo de ayuda o comunicación que no haya sido previa y expresamente autorizada. En exámenes prácticos el profesor podrá autorizar el acceso del alumno a Internet. En ningún caso se permitirá la

comunicación entre alumnos durante la realización de un examen, ya sea de forma oral o a través de otros dispositivos. El profesor podrá hacer uso de herramientas de monitorización de la red para detectar comunicaciones entre diferentes hosts en el aula u otros comportamientos contrarios a normativa o enfocados a burlar el proceso normal de evaluación, quedando los alumnos advertidos mediante este párrafo de esta programación didáctica que los alumnos tienen deber de conocer, sin perjuicio de que se les informe verbalmente en el aula.

Las conductas que supongan perjuicio para la realización de un examen o práctica por parte de los alumnos asistentes serán objeto de expulsión inmediata y supondrán de forma implícita la renuncia del alumno a continuar el examen o práctica, asumiendo el alumno la consiguiente calificación de 0 (cero) o de No Presentado si procede, o la calificación correspondiente a lo que haya realizado hasta el momento del incidente, todo ello sin perjuicio de que se puedan adoptar otras medidas disciplinarias contempladas en la normativa del centro.

Las faltas de ortografía por parte del alumno pueden dar lugar a una reducción de la nota correspondiente a la pregunta donde tengan lugar de hasta un 0.2 por falta ortográfica. Si se trata de una pregunta de respuesta corta, donde la respuesta sea de una sola palabra o como mucho una frase, la penalización en dicha pregunta a causa de incorrecciones ortográficas no será en ningún caso superior al 20 % de la calificación de la pregunta.

Para que un examen práctico pueda calificarse positivamente debe cumplir las premisas del enunciado del mismo si las hubiere. Esto significa que aunque contenga contenido técnicamente adecuado si dicho contenido no se ajusta al fin global del examen propuesto porque incumple alguna de sus premisas su calificación no podrá alcanzar la nota de corte o nota necesaria para aprobar dicho examen.

En caso de que el profesor considere que el alumno puede haber vulnerado la normativa de examen podrá requerir al alumno a la finalización del mismo o incluso a posteriori para que demuestre de forma clara que ha adquirido los conocimientos y destrezas que se evalúan en dicho examen, mediante una entrevista en la que puede solicitar al alumno que repita alguno de los procedimientos o explica cómo ha alcanzado alguna conclusión o resultado. La entrevista será determinante en la calificación definitiva del examen, debiendo el alumno demostrar de forma fehaciente que ha realmente ha adquirido la competencia necesaria para ser evaluado positivamente en dicho examen.

ANEXO II

Normativa específica de exámenes del módulo de RL

Se realizarán exámenes por partes, generalmente un examen por cada tema, salvo que el desarrollo de las clases aconseje, a juicio del profesor, que se realice un único examen para más de un tema o más de un examen para un mismo tema. En cualquier caso esto no es relevante para el desarrollo del módulo ni su evaluación.

Una vez realizado el examen final/global de cada evaluación se realizará media de las calificaciones de todas las partes para obtener la calificación correspondiente a los exámenes de dicha evaluación. Para poder ser evaluado positivamente el alumno deberá alcanzar al menos un 4 en cada una de las partes/exámenes. Cuando un examen se compone de dos partes (un examen teórico y otro práctico, por ejemplo) será necesario alcanzar un 4 como mínimo en cada una de ellas.

El examen final/global de todo el módulo que se realiza en la convocatoria ordinaria incluirá tantas partes como exámenes haya tenido el curso escolar.

El alumno que tenga una o más evaluaciones no superadas, deberá presentarse para poder superar dichas evaluaciones. El alumno podrá ser evaluado de TODOS los contenidos impartidos durante las sesiones lectivas correspondientes a cada evaluación que no tenga superada.

En la convocatoria extraordinaria los alumnos se examinarán de todos los contenidos de las evaluaciones no superadas salvo que el profesor estime oportuno otra cosa en beneficio de cada alumno, por ejemplo si la causa de no tener una evaluación superada ha sido una competencia no desarrollada por una práctica no entregada. Igualmente tendrá que presentar todas las prácticas que se hayan puesto durante el curso. Como algunas prácticas han sido resueltas y se ha publicado su solución, el profesor podrá poner nuevas prácticas para los alumnos que se presenten a evaluación extraordinaria, prácticas que serán igualmente consideradas que las desarrolladas durante el curso. Las prácticas no presentadas recibirán calificación de 0 (cero) y harán media como cualquier otra práctica.

Es condición necesaria para superar el módulo tener superadas todas las evaluaciones de que se componga.

NOTA: Se entiende por calificación o evaluación no superada, aquella que no alcanza un 5 sobre 10.

Referente a la entrega de prácticas y trabajos

Las prácticas serán entregadas en los plazos estipulados por el profesor de la asignatura. Sólo en casos justificados se permitirá su entrega fuera de los plazos establecidos.

Debido a que las prácticas de esta asignatura requieren en muchos casos de material que no está al alcance de los alumnos salvo en el propio instituto, así como de una comprobación 'in situ' e 'ipso facto', las prácticas que requieran de alguno de estos materiales sólo se realizarán en la fecha y hora indicadas por el profesor de la asignatura. No obstante el profesor intentará, en los casos en que sea posible, utilizar simuladores, máquinas virtuales, etc para minimizar el número de prácticas que sólo pueden ser realizadas en el centro.

Para aquellas prácticas en las que es imprescindible el uso del material del centro se establecerá, siempre que se pueda, más de un día para facilitar la asistencia de los alumnos a las prácticas.

La no realización y/o entrega de todas las prácticas supondrá la imposibilidad, por parte del alumno, de alcanzar la calificación de aprobado o apto.

Cada práctica no entregada por el alumno en tiempo y forma supondrá la calificación de 0 (cero) en dicha práctica.

La calificación total de las prácticas no podrá ser inferior a 4 para poder superar la asignatura.

En caso de no asistencia por causas debidamente justificadas, al alumno se le podrá realizar las prácticas en otra fecha siempre y cuando justifique debidamente su ausencia, mediante justificante médico, de trabajo, asistencia a exámenes de otras enseñanzas oficiales, justificante del padre o tutor (sólo para menores de edad), etc. En cualquier caso la aceptación del justificante quedará a elección del profesor, que podrá rechazar dicho justificante.

En caso de que la realización de las prácticas por parte de un alumno que no haya asistido en su fecha suponga, a juicio del profesor, perjuicio para el desarrollo normal de la asignatura o no haya tiempo material para realizarlas, no se le realizará el cambio a otra fecha.

Para llevar a cabo la evaluación y calificación de las prácticas se podrá requerir al alumno para una entrevista sobre cualquier práctica entregada, con objeto de comprobar que ha asimilado realmente los conceptos, procedimientos y aptitudes asociados a dicha práctica. Incluso se podrá exigir al alumno que repita la totalidad o parte de la misma en presencia del profesor. La entrevista será determinante en la calificación correspondiente a la práctica pudiendo incluso anular la práctica y ser calificada negativamente si el alumno demostrase no haber adquirido los conocimientos y habilidades inherentes a la realización de la misma.

Para que una práctica o tarea pueda calificarse positivamente debe cumplir las premisas de la misma si las hubiere. Esto significa que aunque la misma contenga contenido técnico adecuado si dicho contenido no se ajusta al fin global de la práctica porque incumple alguna de sus premisas su calificación no podrá alcanzar la nota de corte o nota necesaria para aprobar dicha práctica.