Programación didáctica del módulo: Incidentes de Ciberseguridad

Curso de Especialización Ciberseguridad en Entornos de las Tecnologías de la Información

Curso: 2025/2026

Profesora: Celeste Rhodes Rodríguez

Índice

1. Introducción

La Formación Profesional está orientada tanto al desarrollo y satisfacción personal del alumno como a la obtención de unos conocimientos de tipo técnico y/o humanístico que han de ser preparatorios para el mundo laboral o la Universidad.

La reforma educativa promulgada por la L.O.G.S.E. (Ley Orgánica de Ordenación General del Sistema Educativo) supuso un cambio radical en el sistema educativo existente hasta entonces. La Formación Profesional tradicional pasó a denominarse Ciclos Formativos, quedando estructurada en familias y niveles. Así, los Ciclos Formativos de Grado Medio permiten obtener el título de Técnico, mientras que los Ciclos Formativos de Grado Superior permiten obtener el título de Técnico Superior.

Posteriormente, la L.O.E. (Ley Orgánica de la Educación) estableció una nueva ordenación de los ciclos formativos, estableciendo el nuevo catálogo de la formación profesional, las unidades de competencia y los módulos formativos asociados del Catálogo Modular de Formación Profesional. Este nuevo marco formativo no hace sino acercar la Formación Profesional a las necesidades actuales de la sociedad del conocimiento, donde la movilidad laboral, las nuevas tecnologías, la cohesión e inserción laboral exigen un nuevo planteamiento del mercado laboral. Así pues se pretende proporcionar a las personas la formación requerida por el sistema productivo y de acercar los títulos de formación profesional a la realidad del mercado laboral. Los Ciclos Formativos ofertados por la LOE están separados por familias, siendo una de ellas la Informática.

Con la entrada en vigor de la LOMCE en el curso 2014-2015 la FP Básica vino a sustituir a los PCPI, o Programas de Cualificación Profesional Inicial, desvinculando la Formación Profesional Básica de la obtención del Título de ESO. En este centro se lleva

impartiendo la formación Básica en la rama de "Informática y Comunicaciones" desde el curso 2014-2015. Con la promulgación de la Ley Orgánica 3/2022, de 31 de marzo, de ordenación e integración de la Formación Profesional la formación básica pasa a denominarse Ciclo Formativo de Grado Básico

De acuerdo a la Ley Orgánica 3/2020, de 29 de diciembre, por la que se modifica la Ley Orgánica 2/2006, de 3 de mayo, de Educación, se establecen las titulaciones de los cursos de especialización, cuyo acceso requiere como mínimo de una titulación de grado superior.

A partir del curso 2024/2025, en Castilla-La Mancha se implantarán, con carácter obligatorio y de forma progresiva, las medidas establecidas en el Real Decreto 659/2023, de 18 de julio, que desarrolla la Ley Orgánica 3/2022, de 31 de marzo, de ordenación e integración de la formación profesional.

En este curso 2025/2026, el Departamento de Informática impartirá los siguientes cursos:

a) <u>Ciclos formativos:</u>

1. **<u>Grado Medio</u>**
   - Sistemas Microinformáticos y Redes (primer y segundo curso en turnos de mañana y vespertino).

2. **<u>Grado Superior</u>**

- Administración de Sistemas Informáticos en Red (primer y segundo curso).
- Desarrollo de Aplicaciones Web (primer y segundo curso en turnos de mañana y vespertino).
- Desarrollo de Aplicaciones Web (primer y segundo curso) en la modalidad Virtual).

3. **Grado Básico**
   - "Informática y Comunicaciones" (Primer y segundo curso)

b) **Cursos de Especialización (en horario vespertino):**

- Ciberseguridad en Entornos de las Tecnologías de la Información.
- Inteligencia Artificial y Big Data.

c) Las siguientes asignaturas en Bachillerato y la ESO

- Digitalización. (4º ESO)
- Desarrollo Digital. (1º Bachillerato)

d) Además, el departamento también será encargado de llevar a cabo las tareas de:

- Responsable de Formación y TIC
- Jefatura de estudios adjunta de FP

- Responsable de aula ATECA
- Responsable de aula APE

Dado el extraordinario auge de la informática, y su gran implantación en la gran mayoría de trabajos actualmente, no es de extrañar que estos ciclos formativos sean considerados por los alumnos como una buena alternativa profesional para su futuro.

Para la inserción de los alumnos en el mundo laboral de modo rápido y eficaz, el alumno debe aprender las técnicas y métodos más adecuados que garanticen la adquisición de los conocimientos y destrezas para desenvolverse en el sector informático.

Esta programación está referida al módulo de “Incidentes de ciberseguridad” del curso de especialización “Ciberseguridad en entornos de las tecnologías de la información” en el centro I.E.S. Arcipreste de Hita de Azuqueca de Henares (Guadalajara).

2. Legislación aplicable

La legislación en la que se basa esta programación didáctica es la siguiente:

1. Ley 5/2002, de 19 de junio, donde se establece el sistema integral de la Formación Profesional.
2. Ley Orgánica 2/2006, de 3 de mayo, donde se regula la Formación Profesional en el sistema educativo, organizándola en ciclos formativos de grado medio y grado superior.

3. Real Decreto 1538/2006, de 15 de diciembre, por el que se establece la ordenación general de la Formación Profesional del sistema educativo, incluyendo los aspectos básicos de la evaluación y efectos de los títulos de Formación Profesional.
4. Orden de 29/07/2010, de la Consejería de Educación, Ciencia y Cultura, por la que se regula la evaluación, promoción y acreditación académica del alumnado de formación profesional inicial del sistema educativo de la Comunidad Autónoma de Castilla-La Mancha [2010/14361].
5. Orden de 12 de marzo de 2010, de la Consejería de Educación y Ciencia.
6. Ley 3/2012, de 10 de mayo, de autoridad del profesorado [2012/7512].
7. Ley Orgánica 3/2020, de 29 de diciembre, por la que se modifica la Ley Orgánica 2/2006, de 3 de mayo, de Educación.
8. Orden de 30/07/19, de la Cons. de Educación, Cultura y Deportes, por la que se modifican varias órdenes que regulan la evaluación de alumnado que cursa enseñanzas de FP y otras, para adecuar las fechas de evaluación anuales al calendario de evaluaciones.
9. Ley Orgánica 3/2022, de 31 de marzo, de ordenación e integración de la formación profesional.
10. RD 659/2023, de 18 de julio, por el que se desarrolla la ordenación del Sistema de Formación Profesional.
11. Real Decreto 500/2024, de 21 de mayo, por el que se modifican determinados reales decretos por los que se establecen títulos de Formación Profesional de grado superior y se fijan sus enseñanzas mínimas.
12. Real Decreto 405/2023, de 29 de mayo, por el que se actualizan los títulos de la formación profesional del sistema educativo de Técnico Superior en Desarrollo de Aplicaciones Multiplataforma y Técnico Superior en Desarrollo

de Aplicaciones Web, de la familia profesional Informática y Comunicaciones, y se fijan sus enseñanzas mínimas.

13. 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.
1. Resolución de 11/06/2021, de la Vicecons de Educación, por la que se establece con carácter experimental la distribución horaria de determinados cursos de especialización de Formación Profesional y otros aspectos de organización y desarrollo de los mismos.

3. Ubicación

Tradicionalmente, el alumnado que se matricula es consciente de que las enseñanzas que va a recibir están muy ligadas a un entorno laboral, y que el objetivo principal de los ciclos formativos es formar trabajadores en un campo específico. Al tratarse de enseñanzas dedicadas a la informática, los alumnos tienen claro que el trabajo fundamental se desarrolla con ordenadores, aunque desgraciadamente asocian los contenidos con la ofimática, en lugar de la informática.

El grupo de alumnos es realmente heterogéneo, existiendo una importante presencia de alumnos procedentes de los grados superiores que se imparten en el centro. La mayoría de ellos desconocen realmente el contenido de los módulos (dado su carácter específico). En contraste, existe también un reducido número de alumnos que proceden de entornos profesionales que presentan unos altos conocimientos previos.

En el curso 2020-2021 se impartió por primera vez el curso de especialización correspondiente al título Ciberseguridad en Entornos de las Tecnologías de la Información.

El Departamento de Informática dispone de las siguientes aulas:

a) <u>Aulas para ciclos y cursos de especialización:</u>

a. Formado por 6 aulas situadas en el aulario en las que se imparten los seis cursos de Formación Profesional (dos aulas para el ciclo de SMR, dos para el ciclo de ASIR y dos para el ciclo de DAW) de aproximadamente 50 metros cuadrados cada una de ellas.
b. El tamaño de las aulas no es el adecuado para realizar clases teóricas y prácticas cuando el grupo de alumnos es superior a 26 alumnos.
c. Para el grupo Distancia, no será necesaria la utilización de ningún aula, pero si sería útil que el profesor pudiera tener una sala disponible con conexión a Internet donde pudiera trabajar.
d. Los cursos de especialización se imparten en horario de tarde y ocupan las mismas aulas que los grados superiores.

b) <u>Aulas APE</u>

a. La asignatura de Bachillerato y de la ESO se imparte en las aulas APE del centro o en aulas tradicionales con el apoyo de ordenadores portátiles.

c) <u>Aulas para CFG Báscio</u>

a. La formación profesional básica se imparte en otras aulas independientes de los Ciclos.
b. El aula de primero está en la planta baja del aulario.
c. El aula de segundo está en el edificio principal del instituto, un aula situada entre las aulas APE y ATECA.

d) <u>Aula ATECA</u>

a. Aula de dotación europea para el desarrollo de proyectos de innovación.

Al disponer de horario vespertino, los cursos se imparten en las mismas aulas que los ciclos con turno de mañana, por lo que presentan la misma distribución. Existe un importante número de alumnos que acuden al aula con su propio equipo portátil, se les facilita bajo su responsabilidad una toma de corriente y acceso a la red wifi del aula.

El módulo cuenta con una parte teórica ya que el alumnado debe conocer y manejar conceptos relacionados con la ciberseguridad, pero al mismo tiempo tiene un carácter muy práctico. El alumnado que acude muestra un alto interés por el módulo y éste cuenta con un nivel de dificultad medio. En este módulo el alumno/a conseguirá 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. Por otra parte, de cara al mercado laboral, la superación de este módulo y del resto de módulos que componen el curso de especialización, proporcionará el título para desempeñar funciones en las organizaciones como pueden ser: experto en ciberseguridad, auditor de ciberseguridad o consultor de ciberseguridad.

4. Resultados del aprendizaje

Son objetivos comunes los descritos en el Proyecto educativo del centro, en los que respecta a la convivencia, integración, trabajo en equipo y respeto mutuo entre los integrantes de la comunidad docente.

4.1 Objetivos comunes

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

1. 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.
2. 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.
3. Detectar incidentes de ciberseguridad implantando los controles, las herramientas y los mecanismos necesarios para su monitorización e identificación.
4. Analizar y dar respuesta a incidentes de ciberseguridad, identificando y aplicando las medidas necesarias para su mitigación, eliminación, contención o recuperación.
5. Elaborar análisis de riesgos para identificar activos, amenazas, vulnerabilidades y medidas de seguridad.
6. Diseñar e implantar planes de medidas técnicas de seguridad a partir de los riesgos identificados para garantizar el nivel de seguridad requerido.
7. Configurar sistemas de control de acceso, autenticación de personas y administración de credenciales para preservar la privacidad de los datos.
8. Configurar la seguridad de sistemas informáticos para minimizar las probabilidades de exposición a ataques.
9. Configurar dispositivos de red para cumplir con los requisitos de seguridad.
10. 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.

11. Aplicar estándares de verificación requeridos por las aplicaciones para evitar incidentes de seguridad.
12. Automatizar planes de desplegado de software respetando los requisitos relativos a control de versiones, roles, permisos y otros para conseguir un desplegado seguro.
13. 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.
14. Analizar informes forenses identificando los resultados de la investigación para extraer conclusiones y realizar informes.
15. ñ) Combinar técnicas de hacking ético interno y externo para detectar vulnerabilidades que permitan eliminar y mitigar los riesgos asociados.
16. 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.
17. 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.
18. Desarrollar manuales de información, utilizando herramientas ofimáticas y de diseño asistido por ordenador para elaborar documentación técnica y administrativa.
19. 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.

20. 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.
21. 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.
22. Identificar y proponer las acciones profesionales necesarias para dar respuesta a la accesibilidad universal y al «diseño para todas las personas».
23. 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.

4.2 Resultados de aprendizaje específicos del módulo

Los objetivos específicos del módulo descritos en el Real Decreto 479/2020, de 7 de abril, como resultados de aprendizaje son:

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

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

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

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

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

5. Contenidos

Los contenidos de esta programación se desarrollarán en 5 unidades de trabajo.

5.1. UT 1: 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.

5.2. UT 2: 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.

5.3. UT 3: 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.

5.4. UT 4: 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 restablecer los servicios afectados por incidentes.
− Documentación.
− Seguimiento de incidentes para evitar una situación similar.

5.5. UT 5: 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.

6. Concordancia de las unidades de trabajo con los resultados del aprendizaje

En el siguiente cuadro resumen, se especifica la concordancia entre los objetivos específicos de este módulo y las unidades de trabajo (la X muestra correspondencia):

Unidad de Trabajo / Resultados de aprendizaje	**RE 1**	**RE. 2**	**RE. 3**	**RE. 4**	**RE. 5**
U.T. 1	X				
U.T. 2		X			
U.T. 3			X		
U.T. 4				X	
U.T. 5					X

7. Temporalización

A continuación, se plantea el calendario de ejecución de las unidades de trabajo ya descritas, la **duración asignada es orientativa** y puede modificarse y adaptarse durante el curso dependiendo del tipo de alumnado, recursos con los que se pueda contar en clase o posibles imprevistos:

Unidad de Trabajo	Duración prevista	Trimestre
UT1	20	1º
UT2	28	1º y 2º
UT3	26	2º
UT4	30	2º y 3º
UT5	16	3º
Duración total:	120	

8. Metodología

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, respectando igualmente el material de la clase. Dado el poco material disponible para

impartir este módulo, esta última premisa se convierte en vital para poder realizar un aprendizaje correcto de la materia.

Los medios que se implantarán en la medida de lo posible para conseguir estos fines son:

- Estructuración de la clase de la forma más óptima posible para aprovechar el espacio según el número de alumnos en el aula.
- Utilización de la pantalla digital o el proyector para realizar las explicaciones prácticas de software.
- Agrupación de algunas horas de clase en bloques de 2 sesiones lectivas, con el fin de poder planificar teoría y ejercicios prácticos en el mismo día.
- Realización de actividades en grupo que permitan, de una forma próxima y fácil, el aporte de distintos puntos de vista sobre un tema concreto.
- Agrupaciones de alumnos para realizar proyectos o ejercicios conjuntos.
- Planteamiento de actividades creativas donde el alumno pueda aportar su criterio a los temas comentados.
- Por otra parte se plantea la necesidad de motivar e incentivar el interés del alumno por los temas referenciados en clase, esto se concreta en los puntos siguientes:
  - Acercamiento de los temas didácticos al mundo real, aportando publicaciones y documentación de productos lo más conocidos y asequibles posible.
  - Desmitificando la teoría más abstracta y convirtiéndola en cosas tangibles. Es decir, analizando el punto de vista práctico de los conceptos expresados en clase.

- Planteando ejemplos de aplicación de los trabajos en clase en el mundo laboral real (o lo más cercano posible) de forma que se vaya formando la imagen, en cada alumno, de su perfil profesional.
- Se utilizará en la medida de lo posible la plataforma Moodle proporcionada por la Junta de comunidades, integrado en Educamos CLM, para proporcionar a los alumnos materiales de consulta, así como ejercicios y tareas.

9. Evaluación

La evaluación será continua, formativa y sumativa, considerándose además de las pruebas objetivas, el trabajo en clase, el progreso, el interés por el módulo, la atención, etc.

9.1. El proceso de evaluación

9.1.1. Evaluación inicial

Al comienzo de cada Unidad de Trabajo se realizará un pequeño debate que permitirá saber cuál es el nivel de conocimientos del alumno sobre cada tema, realizando introducciones sobre aquellos aspectos necesarios para el tema que el alumno no tiene o no ha adquirido completamente, o una pequeña introducción al tema. Se orientará a los alumnos acerca de los contenidos del tema para que los ubiquen dentro de los conocimientos informáticos adquiridos en el curso pasado, o bien en unidades de trabajo anteriores.

En el caso de que Unidades de Trabajo anteriores sirvan como base a una nueva Unidad de Trabajo, los alumnos en esta fase realizarán un repaso de esos conceptos.

9.1.2. Procedimientos para evaluar el proceso de aprendizaje del alumnado

Utilizando la observación y el análisis de los trabajos desarrollados, se utilizarán los siguientes instrumentos de evaluación:

1. El trabajo en equipo
2. La investigación de los contenidos
3. La asistencia regular a clase
4. La puntualidad
5. La correcta utilización del material y equipos
6. Participación en clase
7. Realización y presentación de los trabajos obligatorios solicitados por el profesor.
8. La elaboración de los trabajos optativos
9. Pruebas escritas, con contenidos teóricos y prácticos

Se considera que estos instrumentos de evaluación son adecuados para los criterios de evaluación de este módulo.

9.1.3. Evaluación sumativa

Al final de ciertos bloques de unidades de trabajo, fundamentales para proseguir el desarrollo del módulo, se realizarán pruebas específicas de evaluación escritas llevadas a cabo por el alumno de forma individual. En ciertas unidades de trabajo se realizarán proyectos o ejercicios de síntesis que deberán ser entregados en una fecha límite que serán calificados en ese trimestre.

9.2. Criterios de evaluación

Teniendo en cuenta los Resultados de Aprendizaje, los Criterios de Evaluación son los siguientes:

RA1. 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.

RA2. 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.

RA3. 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.

RA4. 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.

RA5. 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.

9.3. Criterios de calificación

Para la superación del módulo es requisito indispensable que el alumno supere **todos y cada uno de los resultados de aprendizaje** del módulo de acuerdo a los criterios de calificación establecidos.

Una vez superados todos los resultados de aprendizaje, la calificación final del módulo se obtendrá sumando la calificación obtenida en cada uno de los RRAA, de acuerdo con los porcentajes de ponderación.

Del resultado se tomará la parte entera, redondeando por exceso la cifra si la parte decimal resultase ser igual o superior a 5.

La calificación final del módulo, por lo tanto, se establecerá según los siguientes puntos:

- El rango de calificación será de 1 a 10 valor entero
- El peso de las calificaciones de los RRAA se realizará mediante una media ponderada.
- El valor mínimo en los RRAA para considerar que las capacidades profesionales han sido alcanzadas será de 5. En el caso, que algún RRAA presente una puntuación inferior a 5, entonces la calificación final del módulo no podrá ser superior a 4.
- Para obtener la calificación de cada RA se ponderarán los criterios de evaluación asociados.

RESULTADOS DE APRENDIZAJE	% Asignado Evaluación
RA1	20%
RA2	20%
RA3	20%
RA4	20%
RA5	20%
TOTAL	100%

9.4. Recuperación

El alumno/a deberá recuperar los RRAA no superadas en el examen final que se realizará en la primera convocatoria ordinaria. Solo se deberán recuperar **únicamente** aquellos RRAA no superados. En el caso de no recuperar los RRAA, entonces la calificación final del módulo no podrá ser superior a 4, considerándose el mismo suspenso.

Para recuperar los RRAA suspensos, se deberán realizar los trabajos o exámenes escritos correspondientes a sus criterios de evaluación. Aquellos criterios que se hayan calificado como superados durante la evaluación no será obligatorio recuperarlos.

Acceso a la segunda convocatoria ordinaria

Los alumnos que, después de la primera convocatoria tengan módulos no superados, accederán a la segunda convocatoria de cada curso académico. No obstante, si el alumno no se presenta a la prueba de evaluación preparada por los profesores para la segunda convocatoria, se entenderá que el alumno renuncia a la misma, sin necesidad de haberlo solicitado previamente.

El acceso a la segunda convocatoria ordinaria se realizará independientemente del tipo de matrícula del alumno (ordinaria o modular).

Para la recuperación de los RRAA no superados en la segunda convocatoria ordinaria se seguirán los mismos criterios que para la primera: “se deberán realizar los trabajos o exámenes escritos correspondientes a sus criterios de evaluación. Aquellos criterios que se hayan calificado como superados durante la evaluación no será obligatorio recuperarlos.”

9.4.1. Planificación de las actividades de recuperación de los módulos no superados

Dado que se utiliza la plataforma Moodle a lo largo del módulo, los alumnos tienen a su disposición el conjunto de ejercicios que les pueden servir de refuerzo para superar el examen de la segunda convocatoria ordinaria

Se realizarán sesiones de repaso en el centro con el fin de que los alumnos puedan reforzar los contenidos no superados.

9.5. Pérdida de la evaluación continua

En el caso de que un alumno no asista a clase, puede perder el derecho a ser evaluado de forma continua. En concreto aquellos alumnos que tengan un 25% de faltas de asistencia injustificadas POR MÓDULO perderán el derecho a la evaluación continua de ese módulo, por lo que deberán presentarse a una prueba objetiva al finalizar el módulo.

En este módulo, el porcentaje de faltas injustificadas que puede tener un alumno antes de perder el derecho a la evaluación continua es: **30 horas.**

La pérdida de la evaluación continua se realiza únicamente para el módulo en el que se hayan detectado las faltas de asistencia injustificadas, y no para todo el ciclo formativo.

La justificación válida para los alumnos se realizará mediante un justificante médico expedido por autoridades médicas o por causas de fuerza mayor que el alumno pueda alegar y sean aceptadas por el profesor.

Adicionalmente, para fomentar el cuidado y corresponsabilidad del material de clase y prepararles para el trabajo en empresa de forma responsable, los alumnos que causen daño intencionado o por negligencia no cuiden el mismo deberán reparar el daño causado al amparo de la Ley de Autoridad del Profesorado. En el caso de que no reparen el daño causado **perderán el derecho a la evaluación continua en todos los módulos en los que estén matriculados**. Los alumnos volverán a ser evaluados de forma continuada cuando reparen el daño causado.

9.5.1. Sistemas e instrumentos de evaluación para los alumnos que han perdido el derecho a la evaluación continua

En el caso de que un alumno pierda el derecho a evaluación continua, deberá presentarse al examen final del curso que se realizará la última semana del curso. En base a ese examen final se calificará el módulo en la primera sesión de evaluación ordinaria. Aun así, el alumno deberá entregar los trabajos prácticos que considere el profesor PREVIA realización del examen. En el caso de no entregar los trabajos prácticos, el alumno no podrá realizar el examen final.

La calificación final obtenida se calculará según lo descrito en el apartado 9.3 de esta programación didáctica.

9.5.2. Procedimiento de notificación de la pérdida de la evaluación continua

El procedimiento de notificación de la pérdida de la evaluación continua es el siguiente:

1. Una vez el alumno haya perdido el derecho a la evaluación continua, al alcanzar el 25% de las faltas injustificadas, el profesor notificará del hecho al tutor del grupo.
2. El tutor del grupo contactará con el resto de los profesores, por si hubiera algún módulo con alguna circunstancia similar.
3. En el menor tiempo posible se notificará por carta al alumno o a sus tutores legales (en el caso de menores de edad), enviada por el tutor desde la secretaría del centro (con registro de entrada) con el visto bueno de la Dirección del centro. La comunicación se realizará según el modelo establecido en el Anexo I de la orden 29/07/2010 de la Consejería de Educación, Ciencia y Cultura de CLM, por la que se regula la evaluación del alumnado de Formación Profesional.
4. La realización del examen final de curso será posible si el alumno entrega los trabajos prácticos indicados por el profesor.

9.5.3. Casos específicos

Aquellos alumnos que presenten una justificación a las faltas de asistencia (únicamente debida a causas justificadas), **no perderán el derecho a la evaluación continua**, pero deberán igualmente presentarse a los exámenes parciales y entregar los trabajos prácticos. En el caso de que no lo hagan deberán presentarse al examen final de curso.

Independientemente de lo anterior, es responsabilidad del alumno realizar un seguimiento de las explicaciones realizadas en clase, para poder entregar los proyectos y realizar los exámenes con el resto de la clase.

9.6. Autoevaluación del profesorado

La autoevaluación del profesorado está englobada en el Proyecto Educativo del Centro (según su plan de autoevaluación del centro), y se percibe como una forma de mejora y calidad de la enseñanza.

La autoevaluación del profesorado es una práctica constante y continua en el Departamento de Informática, que demuestra a lo largo de cada curso escolar una innovación de metodologías y capacidad de inventiva para poder impartir enseñanzas a pesar de los escasos recursos materiales de los que dispone. Esta autoevaluación del trabajo docente suele ser un proceso interno, de reflexión intrínseca y de necesidad esencial en el trabajo del profesorado. Conviene sin embargo realizar una reflexión escrita de forma periódica, por lo que, una vez terminadas las evaluaciones del primer y segundo trimestre, el profesorado realiza una autoevaluación de su trabajo y metodología empleada. En esa autoevaluación se recogerán los siguientes aspectos:

Medidas tomadas durante el trimestre que se deben autoevaluar:

1. Medidas metodológicas (clase magistral, libro de texto, nuevas tecnologías,…)
2. Organizativas del aula
3. Agrupamientos del alumnado
4. Evaluación
5. Actividades de recuperación
6. Acción tutorial
7. Material
8. Problemas encontrados
9. Correcciones
10. Departamentales

Medidas que se deben tomar durante el siguiente trimestre:

1. Medidas metodológicas (clase magistral, libro de texto, nuevas tecnologías,…)
2. Organizativas del aula
3. Agrupamientos del alumnado
4. Evaluación
5. Actividades de recuperación
6. Acción tutorial
7. Material
8. Problemas encontrados
9. Correcciones

Resultados académicos:

1. Porcentaje de alumnos por tramos de calificación.
2. Porcentaje de abandonos o renuncias de convocatorias
3. Número de faltas de asistencia

10. Alumnado con necesidades específicas de apoyo educativo

Se realizarán las adaptaciones necesarias en los medios y procedimientos de evaluación para el alumnado con necesidades específicas de apoyo educativo, con el fin de garantizar su accesibilidad a las pruebas y que sea evaluado con los medios apropiados a sus posibilidades y características.

En todo caso, en el proceso de evaluación se comprobará que el alumnado ha conseguido los resultados de aprendizaje establecidos para cada uno de los módulos que forman parte del ciclo formativo.

En ningún caso se realizarán adaptaciones curriculares significativas.

11. Material didáctico

Los recursos necesarios para impartir este módulo son los siguientes:

- Pizarra
- Retroproyector y pantalla.
- Ordenador con Windows, Microsoft Office, Acrobat Reader, Winrar y programas de software específicos del módulo.
- Conexión a Internet
- Teams y portal Educamos
- Impresoras
- Aula virtual

Cuidado del material

En la situación actual en la que nos encontramos, con unos presupuestos ajustados y un material escaso, se hace IMPRESCINDIBLE en el Departamento de Informática exigir un cuidado del material a los alumnos. Afortunadamente, esta necesidad viene incluso amparada por ley de CLM, por lo que, en el caso de rotura del material por parte de un alumno, se exigirá el cumplimiento de la Ley de Autoridad del Profesorado, donde se especifica, en su Artículo 7:

"*Artículo 7. Responsabilidad y reparación de daños.*

Los alumnos/as o personas con él relacionadas que individual o colectivamente causen, de forma intencionada o por negligencia, daños a las instalaciones, equipamientos informáticos, incluido el software, o cualquier material del centro, así como a los bienes de los miembros de la comunidad educativa, quedarán obligados a reparar el daño causado o hacerse cargo del coste económico de su reparación o restablecimiento,

cuando no medie culpa in vigilando de los/as profesores/as. Asimismo, deberán restituir los bienes sustraídos, o reparar económicamente el valor de estos.

2. En todo caso, quienes ejerzan la patria potestad o la tutela de los menores de edad serán responsables civiles en los términos previstos por la legislación vigente."

En el caso de que un alumno cause daño a las instalaciones o material, se amonestará de la acción por escrito informando a Jefatura de Estudios para que tome las medidas disciplinarias oportunas, y gestione la aplicación del artículo mencionado anteriormente.

Como se ha comentado en el apartado 9.6, los alumnos que causaran daño a las instalaciones o material y no reparen el daño causado perderán el derecho a la evaluación continua.

12. Actividades extraescolares

Siempre que sea posible se organizarán salidas que sean provechosas para los alumnos (Como ferias de informática, empresas de informática, etc.). Incluso si es posible se contactará con antiguos alumnos para que den una charla a los alumnos actuales sobre su visión del mundo laboral después de haber obtenido el título.

13. Bibliografía

- **Incidentes de ciberseguridad**. Editorial Paraninfo. ISBN: 9788428365413