Programación didáctica del módulo: Seguridad y Alta Disponibilidad

Ciclo formativo: Administración de Sistemas Informáticos en Red

Curso: 2025/2026

Profesor: José Luis Amorós Pallarés

Índice

1. Introducción 4
2. Legislación aplicable 7
3. Ubicación 9
4. Resultados del aprendizaje 11
4.1 Objetivos comunes 11
4.2 Objetivos específicos del módulo 13
5. Contenidos 14
5.1.- Unidad de Trabajo 1: Introducción a la seguridad informática. 14
5.2.- Unidad de Trabajo 2: Seguridad lógica 15
5.5.- Unidad de Trabajo 5: Seguridad perimetral. 16
5.6.- Unidad de Trabajo 6: Cortafuegos. 16
5.7.- Unidad de Trabajo 7: El Proxy. 16
5.8.- Unidad de Trabajo 8: Alta disponibilidad. 17
5.9.- Unidad de Trabajo 9: Legislación y normas sobre seguridad 18
5.10.- Unidad de Trabajo 10: proyecto modular 18
6. Concordancia de las unidades de trabajo con los resultados del aprendizaje 18
7. Temporalización 19
8 Metodología 19
9 Evaluación 21
9.1 El proceso de evaluación 21
9.1.1 Evaluación inicial 21
9.1.2 Procedimientos para evaluar el proceso de aprendizaje del alumnado 22

9.1.3 Evaluación sumativa 22
9.2 Criterios de evaluación 23
9.3 Resultados de aprendizaje y criterios de evaluación necesarios para la formación en empresa 28
9.4 Criterios de calificación 31
9.5 Recuperación 33
9.5.1 Acceso a la segunda convocatoria ordinaria 33
9.5.2 Planificación de las actividades de recuperación de los módulos no superados 34
9.6 Pérdida de la evaluación continua 34
9.6.1 Sistemas e instrumentos de evaluación para los alumnos que han perdido el derecho a la evaluación continua 35
9.6.2 Procedimiento de notificación de la pérdida de la evaluación continua 35
9.6.3 Casos específicos 36
9.7 Autoevaluación del profesorado 37
10 Alumnado con necesidades específicas de apoyo educativo 38
11 Material didáctico 39
12 Actividades extraescolares 40
13 Bibliografía 40

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 2024/2025, 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. **FP Básica**
   - "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 del 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 "Seguridad y Alta Disponibilidad" de 2º curso del ciclo formativo "Administración de Sistemas Informáticos en Red" 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 1629/2009, de 30 de octubre, por el que se establece el título de Técnico Superior en Administración de Sistemas Informáticos en Red y se fijan sus enseñanzas mínimas. (B.O.E. de 18 de noviembre del 2009)
14. Decreto 200/2010, de 03/08/2010, por el que se establece el currículo de Ciclo Formativo de Grado Superior correspondiente al título de Técnico o

Técnica Superior en Administración de Sistemas Informáticos en Red, en la Comunidad Autónoma de Castilla-La Mancha [2010/13389].

15. Decreto 80/2024, de 5 de noviembre, por el que se modifican determinados decretos que establecen los currículos de los ciclos formativos de grado superior correspondientes a los títulos de Técnico o Técnica Superior de Formación Profesional en la comunidad autónoma de Castilla-La Mancha.
16. Real Decreto 1629/2009, de 30 de octubre, por el que se establece el título de Técnico Superior en Administración de Sistemas Informáticos en Red y se fijan sus enseñanzas mínimas. (B.O.E. de 18 de noviembre del 2009)
17. Decreto 200/2010, de 03/08/2010, por el que se establece el currículo de Ciclo Formativo de Grado Superior correspondiente al título de Técnico o Técnica Superior en Administración de Sistemas Informáticos en Red, en la Comunidad Autónoma de Castilla-La Mancha [2010/13389].
18. Decreto 80/2024, de 5 de noviembre, por el que se modifican determinados decretos que establecen los currículos de los ciclos formativos de grado superior correspondientes a los títulos de Técnico o Técnica Superior de Formación Profesional en la comunidad autónoma de Castilla-La Mancha. [2024/8907]

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 2º de ASIR suele ser un grupo homogéneo de alumnos, sin problemas de conducta y con interés por la informática (aunque sea principalmente por alguna de sus ramas). Algunos de los alumnos de este curso muestran normalmente interés por acceder directamente al mercado laboral, y otros muestran predisposición acceder a la Universidad.

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.

En la mayoría de las aulas debido al gran número de alumnos matriculados en algunos cursos (principalmente en los cursos de primero), las aulas están formadas por hileras de ordenadores para intentar aprovechar el espacio de la forma más óptima posible. Aunque en algunos casos cuando hay pocos alumnos es posible distribuirlas en forma de U para realizar las clases prácticas, permitiendo un control visual rápido de los ordenadores por parte del profesor, y en el centro de la clase disponer de mesas adicionales para realizar las clases teóricas.

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

Adicionalmente, los objetivos comunes para este ciclo formativo son los descritos en el Real Decreto 1629/2009:

1. Analizar la estructura del software de base, comparando las características y prestaciones de sistemas libres y propietarios, para administrar sistemas operativos de servidor.

2. Instalar y configurar el software de base, siguiendo documentación técnica y especificaciones dadas, para administrar sistemas operativos de servidor.
3. Instalar y configurar software de mensajería y transferencia de ficheros, entre otros, relacionándolos con su aplicación y siguiendo documentación y especificaciones dadas, para administrar servicios de red.
4. Instalar y configurar software de gestión, siguiendo especificaciones y analizando entornos de aplicación, para administrar aplicaciones.
5. Instalar y administrar software de gestión, relacionándolo con su explotación, para implantar y gestionar bases de datos.
6. Configurar dispositivos hardware, analizando sus características funcionales, para optimizar el rendimiento del sistema.
7. Configurar hardware de red, analizando sus características funcionales y relacionándolo con su campo de aplicación, para integrar equipos de comunicaciones.
8. Analizar tecnologías de interconexión, describiendo sus características y posibilidades de aplicación, para configurar la estructura de la red telemática y evaluar su rendimiento.
9. Elaborar esquemas de redes telemáticas utilizando software especifico para configurar la estructura de la red telemática.
10. Seleccionar sistemas de protección y recuperación, analizando sus características funcionales, para poner en marcha soluciones de alta disponibilidad.
11. Identificar condiciones de equipos e instalaciones, interpretando planes de seguridad y especificaciones de fabricante, para supervisar la seguridad física.
12. Aplicar técnicas de protección contra amenazas externas, tipificándolas y evaluándolas para asegurar el sistema.
13. Aplicar técnicas de protección contra pérdidas de información, analizando planes de seguridad y necesidades de uso para asegurar los datos.

14. Asignar los accesos y recursos del sistema, aplicando las especificaciones de la explotación, para administrar usuarios
15. Aplicar técnicas de monitorización interpretando los resultados y relacionándolos con las medidas correctoras para diagnosticar y corregir las disfunciones.
16. Establecer la planificación de tareas, analizando actividades y cargas de trabajo del sistema para gestionar el mantenimiento.
17. Identificar los cambios tecnológicos, organizativos, económicos y laborales en su actividad, analizando sus implicaciones en el ámbito de trabajo, para resolver problemas y mantener una cultura de actualización e innovación.
18. Identificar formas de intervención en situaciones colectivas, analizando el proceso de toma de decisiones y efectuando consultas para liderar las mismas.
19. Identificar y valorar las oportunidades de aprendizaje y su relación con el mundo laboral, analizando las ofertas y demandas del mercado para gestionar su carrera profesional.
20. Reconocer las oportunidades de negocio, identificando y analizando demandas del mercado para crear y gestionar una pequeña empresa.
21. Reconocer sus derechos y deberes como agente activo en la sociedad, analizando el marco legal que regula las condiciones sociales y laborales para participar como ciudadano democrático.

4.2 Objetivos específicos del módulo

El módulo profesional “Seguridad y alta disponibilidad” contribuye a alcanzar los objetivos generales: j), k), l), m), o), y p) del ciclo formativo y las competencias profesionales, personales y sociales e), f), i), j), k), m), n), o), r) y s) del título.

Además, este módulo tiene los siguientes objetivos específicos:

1. Adopta pautas y prácticas de tratamiento seguro de la información, reconociendo las vulnerabilidades de un sistema informático y la necesidad de asegurarlo.
2. Implanta mecanismos de seguridad activa, seleccionando y ejecutando contramedidas ante amenazas o ataques al sistema.
3. Implanta técnicas seguras de acceso remoto a un sistema informático, interpretando y aplicando el plan de seguridad.
4. Implanta cortafuegos para asegurar un sistema informático, analizando sus prestaciones y controlando el tráfico hacia la red interna.
5. Implanta servidores «proxy», aplicando criterios de configuración que garanticen el funcionamiento seguro del servicio.
6. Implanta soluciones de alta disponibilidad empleando técnicas de virtualización y configurando los entornos de prueba.
7. Reconoce la legislación y normativa sobre seguridad y protección de datos valorando su importancia.

5. Contenidos

5.1.- Unidad de Trabajo 1: Introducción a la seguridad informática.

- Fiabilidad, confidencialidad, integridad y disponibilidad.
- Elementos vulnerables en el sistema informático: hardware, software y datos.
- Análisis de las principales vulnerabilidades de un sistema informático.
- Amenazas. Tipos: Amenazas físicas. Amenazas lógicas.
- Seguridad física y ambiental:
    - Ubicación y protección física de los equipos y servidores.
    - Sistemas de alimentación ininterrumpida.
- Análisis forense en sistemas informáticos:
    - Funcionalidad y fases de un análisis forense.

- Respuesta a incidentes.
- Análisis de evidencias digitales.
- Herramientas de análisis forense.

5.2.- Unidad de Trabajo 2: Seguridad lógica.

- Medidas de seguridad.
- Listas de control de acceso.
- Establecimiento de políticas de contraseñas.
- Políticas de almacenamiento.
- Copias de seguridad e imágenes de respaldo.
- Medios de almacenamiento.

5.3.- Unidad de Trabajo 3: Criptografía.

- Sistemas de cifrado
- Sistemas biométricos
- Protocolos seguros
- Firma electrónica y certificado digital

5.4.- Unidad de Trabajo 4: Seguridad activa.

- Ataques y contramedidas en sistemas personales:
  - Clasificación de los ataques.
  - Anatomía de ataques y análisis de software malicioso.
  - Herramientas preventivas y paliativas.
  - Actualización de sistemas y aplicaciones.
  - Seguridad en la conexión con redes públicas.
  - Pautas y prácticas seguras.
- Seguridad en la red corporativa:
  - Monitorización del tráfico en redes.
  - Seguridad en los protocolos para comunicaciones inalámbricas.
  - Riesgos potenciales de los servicios de red.

- Intentos de penetración.

5.5.- Unidad de Trabajo 5: Seguridad perimetral.

- Elementos básicos de la seguridad perimetral.
- Perímetros de red. Zonas desmilitarizadas. Router frontera.
- Arquitectura débil/ fuerte de subred protegida.
- Políticas de defensa en profundidad:
  - Defensa perimetral, defensa interna, factor Humano.
- Redes privadas virtuales. VPN.
- Servidores de acceso remoto:
  - Protocolos de autenticación.
  - Configuración de parámetros de acceso.
  - Servidores de autenticación

5.6.- Unidad de Trabajo 6: Cortafuegos.

- Utilización de cortafuegos.
- Filtrado de paquetes de datos.
- Tipos de cortafuegos. Características. Funciones principal.
- Instalación de cortafuegos. Ubicación.
- Reglas de filtrado de cortafuegos.
- Pruebas de funcionamiento. Sondeo.
- Registros de sucesos de un cortafuegos.
- Cortafuegos integrados en los sistemas operativos.
- Cortafuegos libres y propietarios.
- Cortafuegos hardware.

5.7.- Unidad de Trabajo 7: El Proxy.

- Tipos de «proxy». Características y funciones.

- Instalación de servidores «proxy».
- Instalación y configuración de clientes «proxy».
- Configuración del almacenamiento en la caché de un «proxy».
- Configuración de filtros.
- Métodos de autenticación en un «proxy».
- «proxys» inversos.
- «proxys» encadenados.
- Pruebas de funcionamiento. Herramientas gráficas.

5.8.- Unidad de Trabajo 8: Alta disponibilidad.

- Definición y objetivos.
- Análisis de configuraciones de alta disponibilidad:
    - Funcionamiento ininterrumpido.
    - Integridad de datos y recuperación de servicio.
    - Servidores redundantes.
    - Sistemas de «clusters».
    - SAN, NAS, FiberChannel
    - Balanceadores de carga.
- Instalación y configuración de soluciones de alta disponibilidad.
- Vitalización de sistemas.
- Posibilidades de la virtualización de sistemas.
- Herramientas para la virtualización.
- Configuración y utilización de maquinas virtuales.
- Alta disponibilidad y virtualización.
- Simulación de servicios con virtualización.

5.9.- Unidad de Trabajo 9: Legislación y normas sobre seguridad.

- Legislación sobre protección de datos.
- Legislación sobre los servicios de la sociedad de la información y correo electrónico.
- Normas ISO sobre gestión de seguridad de la información.
- Organismos de gestión de incidencias.

5.10.- Unidad de Trabajo 10: proyecto modular

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 aprendizaje	RA. 1	RA. 2	RA. 3	RA. 4	RA. 5	RA. 6	RA. 7
U.T. 1	X						
U.T. 2	X						
U.T. 3	X	X					
U.T. 4	X	X					
U.T. 5	X	X					
U.T. 6	X	X	X	X			
U.T. 7	X	X	X		X		
U.T. 8	X		X			X	
U.T. 9							X

U.T. 10	X	X	X	X	X	X	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**
1	Introducción a la seguridad informática.	10 h	1
2	Seguridad lógica.	16 h	1
3	Criptografía.	11 h	1
4	Seguridad activa.	16h	1
5	Seguridad perimetral.	15 h	2
6	Cortafuegos.	13 h	2
7	El Proxy.	13 h	2
8	Alta disponibilidad.	15 h	2
9	Legislación y normas sobre seguridad.	10 h	3
10	Proyecto modular	40	3
Duración total:		159 h	

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

Los criterios de evaluación asociados a cada uno de los resultados del aprendizaje son los siguientes:

1. Adopta pautas y prácticas de tratamiento seguro de la información, reconociendo las vulnerabilidades de un sistema informático y la necesidad de asegurarlo.
   a. Se ha valorado la importancia de asegurar la privacidad, coherencia y disponibilidad de la información en los sistemas informáticos.
   b. Se han descrito las diferencias entre seguridad física y lógica.
   c. Se han clasificado las principales vulnerabilidades de un sistema informático, según su tipología y origen.
   d. Se ha contrastado la incidencia de las técnicas de ingeniería social en los fraudes informáticos.
   e. Se han adoptado políticas de contraseñas.
   f. Se han valorado las ventajas que supone la utilización de sistemas biométricos.
   g. Se han aplicado técnicas criptográficas en el almacenamiento y transmisión de la información.
   h. Se ha reconocido la necesidad de establecer un plan integral de protección perimetral, especialmente en sistemas conectados a redes públicas.
   i. Se han identificado las fases del análisis forense ante ataques a un sistema.
   j. Se han identificado las herramientas hardware y software para realizar un análisis forense.

2. Implanta mecanismos de seguridad activa, seleccionando y ejecutando contramedidas ante amenazas o ataques al sistema.

a. Se han clasificado los principales tipos de amenazas lógicas contra un sistema informático.
b. Se ha verificado el origen y la autenticidad de las aplicaciones instaladas en un equipo, así como el estado de actualización del sistema operativo.
c. Se han identificado la anatomía de los ataques más habituales, así como las medidas preventivas y paliativas disponibles.
d. Se han analizado diversos tipos de amenazas, ataques y software malicioso, en entornos de ejecución controlados.
e. Se han implantado aplicaciones específicas para la detección de amenazas y la eliminación de software malicioso.
f. Se han utilizado técnicas de cifrado, firmas y certificados digitales en un entorno de trabajo basado en el uso de redes públicas.
g. Se han evaluado las medidas de seguridad de los protocolos usados en redes inalámbricas.
h. Se ha reconocido la necesidad de inventariar y controlar los servicios de red que se ejecutan en un sistema.
i. Se han descrito los tipos y características de los sistemas de detección de intrusiones.

3. Implanta técnicas seguras de acceso remoto a un sistema informático, interpretando y aplicando el plan de seguridad.
   a. Se han descrito escenarios típicos de sistemas con conexión a redes públicas en los que se precisa fortificar la red interna.
   b. Se han clasificado las zonas de riesgo de un sistema, según criterios de seguridad perimetral.
   c. Se han identificado los protocolos seguros de comunicación y sus ámbitos de utilización.

d. Se han configurado redes privadas virtuales mediante protocolos seguros a distintos niveles.
e. Se ha implantado un servidor como pasarela de acceso a la red interna desde ubicaciones remotas.
f. Se han identificado y configurado los posibles métodos de autenticación en el acceso de usuarios remotos a través de la pasarela.
g. Se ha instalado, configurado e integrado en la pasarela un servidor remoto de autenticación.

4. Implanta cortafuegos para asegurar un sistema informático, analizando sus prestaciones y controlando el tráfico hacia la red interna.
   a. Se han descrito las características, tipos y funciones de los cortafuegos.
   b. Se han clasificado los niveles en los que se realiza el filtrado de tráfico.
   c. Se ha planificado la instalación de cortafuegos para limitar los accesos a determinadas zonas de la red.
   d. Se han configurado filtros en un cortafuegos a partir de un listado de reglas de filtrado.
   e. Se han revisado los registros de sucesos de cortafuegos, para verificar que las reglas se aplican correctamente.
   f. Se han probado distintas opciones para implementar cortafuegos, tanto software como hardware.
   g. Se han diagnosticado problemas de conectividad en los clientes provocados por los cortafuegos.
   h. Se ha elaborado documentación relativa a la instalación, configuración y uso de cortafuegos.

5. Implanta servidores «proxy», aplicando criterios de configuración que garanticen el funcionamiento seguro del servicio.

a. Se han identificado los tipos de «proxy», sus características y funciones principales.
b. Se ha instalado y configurado un servidor «proxy-cache».
c. Se han configurado los métodos de autenticación en el «proxy».
d. Se ha configurado un «proxy» en modo transparente.
e. Se ha utilizado el servidor «proxy» para establecer restricciones de acceso Web.
f. Se han solucionado problemas de acceso desde los clientes al «proxy».
g. Se han realizado pruebas de funcionamiento del «proxy», monitorizando su actividad con herramientas gráficas.
h. Se ha configurado un servidor «proxy» en modo inverso.
i. Se ha elaborado documentación relativa a la instalación, configuración y uso de servidores «proxy».

6. Implanta soluciones de alta disponibilidad empleando técnicas de vitalización y configurando los entornos de prueba.
   a. Se han analizado supuestos y situaciones en las que se hace necesario implementar soluciones de alta disponibilidad.
   b. Se han identificado soluciones hardware para asegurar la continuidad en el funcionamiento de un sistema.
   c. Se han evaluado las posibilidades de la vitalización de sistemas para implementar soluciones de alta disponibilidad.
   d. Se ha implantado un servidor redundante que garantice la continuidad de servicios en casos de caída del servidor principal.
   e. Se ha implantado un balanceador de carga a la entrada de la red interna.
   f. Se han implantado sistemas de almacenamiento redundante sobre servidores y dispositivos específicos.

g. Se ha evaluado la utilidad de los sistemas de «clúster» para aumentar la fiabilidad y productividad del sistema.
h. Se han analizado soluciones de futuro para un sistema con demanda creciente.
i. Se han esquematizado y documentado soluciones para diferentes supuestos con necesidades de alta disponibilidad.

7. Reconoce la legislación y normativa sobre seguridad y protección de datos valorando su importancia.
   a. Se ha descrito la legislación sobre protección de datos de carácter personal.
   b. Se ha determinado la necesidad de controlar el acceso a la información personal almacenada.
   c. Se han identificado las figuras legales que intervienen en el tratamiento y mantenimiento de los ficheros de datos.
   d. Se ha contrastado el deber de poner a disposición de las personas los datos personales que les conciernen.
   e. Se ha descrito la legislación actual sobre los servicios de la sociedad de la información y comercio electrónico.
   f. Se han contrastado las normas sobre gestión de seguridad de la información.
   g. Se ha comprendido la necesidad de conocer y respetar la normativa legal aplicable.

9.3 Resultados de aprendizaje y criterios de evaluación necesarios para la formación en empresa

Los siguientes resultados de aprendizaje y sus correspondientes criterios de evaluación deben ser necesariamente alcanzados en su totalidad para poder incorporarse a la fase de formación en empresa u organismo equiparado, de esta forma se garantiza que el desempeño del alumnado en la empresa no va suponer un riesgo para sí mismo, para la seguridad de los trabajadores o trabajadoras, sus instalaciones o para el tratamiento de la información confidencial de la empresa.

1. Adopta pautas y prácticas de tratamiento seguro de la información, reconociendo las vulnerabilidades de un sistema informático y la necesidad de asegurarlo.
   a. Se ha valorado la importancia de asegurar la privacidad, coherencia y disponibilidad de la información en los sistemas informáticos.
   b. Se han descrito las diferencias entre seguridad física y lógica.
   c. Se han clasificado las principales vulnerabilidades de un sistema informático, según su tipología y origen.
   d. Se ha contrastado la incidencia de las técnicas de ingeniería social en los fraudes informáticos.
   e. Se han adoptado políticas de contraseñas.
   f. Se han valorado las ventajas que supone la utilización de sistemas biométricos.
   g. Se han aplicado técnicas criptográficas en el almacenamiento y transmisión de la información.
   h. Se ha reconocido la necesidad de establecer un plan integral de protección perimetral, especialmente en sistemas conectados a redes públicas.
   i. Se han identificado las fases del análisis forense ante ataques a un sistema.

j. Se han identificado las herramientas hardware y software para realizar un análisis forense.

2. Implanta mecanismos de seguridad activa, seleccionando y ejecutando contramedidas ante amenazas o ataques al sistema.
   a. Se han clasificado los principales tipos de amenazas lógicas contra un sistema informático.
   b. Se ha verificado el origen y la autenticidad de las aplicaciones instaladas en un equipo, así como el estado de actualización del sistema operativo.
   c. Se han identificado la anatomía de los ataques más habituales, así como las medidas preventivas y paliativas disponibles.
   d. Se han analizado diversos tipos de amenazas, ataques y software malicioso, en entornos de ejecución controlados.
   e. Se han implantado aplicaciones específicas para la detección de amenazas y la eliminación de software malicioso.
   f. Se han utilizado técnicas de cifrado, firmas y certificados digitales en un entorno de trabajo basado en el uso de redes públicas.
   g. Se han evaluado las medidas de seguridad de los protocolos usados en redes inalámbricas.
   h. Se ha reconocido la necesidad de inventariar y controlar los servicios de red que se ejecutan en un sistema.
   i. Se han descrito los tipos y características de los sistemas de detección de intrusiones.

3. Implanta técnicas seguras de acceso remoto a un sistema informático, interpretando y aplicando el plan de seguridad.
   a. Se han descrito escenarios típicos de sistemas con conexión a redes públicas en los que se precisa fortificar la red interna.

b. Se han clasificado las zonas de riesgo de un sistema, según criterios de seguridad perimetral.
c. Se han identificado los protocolos seguros de comunicación y sus ámbitos de utilización.
d. Se han configurado redes privadas virtuales mediante protocolos seguros a distintos niveles.
e. Se ha implantado un servidor como pasarela de acceso a la red interna desde ubicaciones remotas.
f. Se han identificado y configurado los posibles métodos de autenticación en el acceso de usuarios remotos a través de la pasarela.
g. Se ha instalado, configurado e integrado en la pasarela un servidor remoto de autenticación.

4. Implanta cortafuegos para asegurar un sistema informático, analizando sus prestaciones y controlando el tráfico hacia la red interna.
   a. Se han descrito las características, tipos y funciones de los cortafuegos.
   b. Se han clasificado los niveles en los que se realiza el filtrado de tráfico.
   c. Se ha planificado la instalación de cortafuegos para limitar los accesos a determinadas zonas de la red.
   d. Se han configurado filtros en un cortafuegos a partir de un listado de reglas de filtrado.
   e. Se han revisado los registros de sucesos de cortafuegos, para verificar que las reglas se aplican correctamente.

5. Implanta servidores «proxy», aplicando criterios de configuración que garanticen el funcionamiento seguro del servicio.
   a. Se han identificado los tipos de «proxy», sus características y funciones principales.

b. Se ha instalado y configurado un servidor «proxy-cache».
c. Se han configurado los métodos de autenticación en el «proxy».
d. Se ha configurado un «proxy» en modo transparente.
e. Se ha utilizado el servidor «proxy» para establecer restricciones de acceso Web.

6. Implanta soluciones de alta disponibilidad empleando técnicas de vitalización y configurando los entornos de prueba.
   a. Se han analizado supuestos y situaciones en las que se hace necesario implementar soluciones de alta disponibilidad.
   b. Se han identificado soluciones hardware para asegurar la continuidad en el funcionamiento de un sistema.
   c. Se han evaluado las posibilidades de la vitalización de sistemas para implementar soluciones de alta disponibilidad.
   d. Se ha implantado un servidor redundante que garantice la continuidad de servicios en casos de caída del servidor principal.
   e. Se ha implantado un balanceador de carga a la entrada de la red interna.
   f. Se han implantado sistemas de almacenamiento redundante sobre servidores y dispositivos específicos.

9.4 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.

RESULTADOS DE APRENDIZAJE	% Asignado Evaluación
RA 1. Adopta pautas y prácticas de tratamiento seguro de la información, reconociendo las vulnerabilidades de un sistema informático y la necesidad de asegurarlo.	18
RA 2. Implanta mecanismos de seguridad activa, seleccionando y ejecutando contramedidas ante amenazas o ataques al sistema.	18
RA 3. Implanta técnicas seguras de acceso remoto a un sistema informático, interpretando y aplicando el plan de seguridad.	18
RA 4. Implanta cortafuegos para asegurar un sistema informático, analizando sus prestaciones y controlando el tráfico hacia la red interna.	18
RA 5. Implanta servidores «proxy», aplicando criterios de configuración que garanticen el funcionamiento seguro del servicio.	18
RA 6. Implanta soluciones de alta disponibilidad empleando técnicas de vitalización y configurando los entornos de prueba.	10

9.5 Recuperación

El alumno 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 poder realizar este examen es necesario haber presentado todos los trabajos prácticos obligatorios solicitados por el profesor a lo largo de todo el curso y tener una calificación de 5 en estos.

9.5.1 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).

Antes de la realización de la segunda convocatoria ordinaria si el profesor lo considera oportuno se programarán ejercicios de recuperación que se deberán de entregar en la fecha establecida por cada profesor.

El examen de la segunda convocatoria ordinaria incluirá solo aquellos contenidos que no se hayan conseguido superar en la primera.

La segunda convocatoria ordinaria se realizará en junio.

9.5.2 Planificación de las actividades de recuperación de los módulos no superados

Dado que se utiliza la plataforma Moodle a lo largo del módulo/asignatura, 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.

Se realizará una prueba final por cada una de las convocatorias ordinarias, esta prueba supondrá el 100% de la calificación, estado está comprendida entre 1-10. El alumno deberá obtener una calificación final igual o superior a 5 sobre 10 para superar el módulo.

9.6 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: 40 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.

9.6.1 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.

9.6.2 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.

9.6.3 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.

9.7 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 Oracle Virtual Box
- Conexión a Internet
- Teams y portal Educamos
- Impresoras

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

Las actividades extraescolares muy importantes para la motivación del alumnado, por tanto, 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

Seguridad y alta disponibilidad
Autor: Ignacio Triviño Mosquera
Editorial: Síntesis
ISBN: 978-84-917184-8-2

Seguridad y alta disponibilidad

Autor: Jesús Costas Santos

Editorial: Ra-Ma

ISBN: 978-84-7897-979-0

Seguridad informática.

Autores: César Seoane Ruano, Ana Belén Saiz Herrero, Emilio Fernández Álvarez,

Laura Fernández Aranda.

Editorial: McGrawHill

ISBN: 978-84-9964-089-1

Seguridad informática

Autor: Purificación Aguilera

Editorial: Editex

ISBN: 978-84-9771-657-4