


 <div>GOBIERNO DE ESPAÑA</div>		 <div>MINISTERIO DE EDUCACIÓN, CULTURA Y DEPORTE</div>		PLANIFICACIÓN DOCENTE		IES VIRGEN DEL CARMEN		 <div>IESCA INSTITUCIÓN DE SECUNDARIA COMUNIDAD DE MADRID DE EDUCACIÓN</div>	
 <div>JUNTA DE ANDALUCÍA CONSEJERÍA DE EDUCACIÓN</div>		 <div>FONDO SOCIAL EUROPEO "El FSE invierte en tu futuro"</div>		PROGRAMACIÓN		<p>Paseo de la Estación nº 44 23008 Jaén Tel. 953366942 – Fax: 953366944 www.iesvirgendelcarmen.com</p>			
MD850401		Rev. 4		16/09/2022		Página 1 de 36			

MÓDULO:	SEGURIDAD Y ALTA DISPONIBILIDAD
CURSO:	2022/2023
DEPARTAMENTO	INFORMÁTICA
CICLO FORMATIVO	ADMINISTRACIÓN DE SISTEMAS INFORMÁTICOS EN RED
PROFESORES	JUAN ANTONIO ROMERO OLMO

Código:	Rev.:	Fecha Implantación:	Entregar a:	Página 1 de 36
MD850401	4	15/02/2018	Jefa/e depto. → Jefatura estudios	

Tabla de Contenido

1. OBJETIVOS GENERALES	3
2. METODOLOGÍA	5
3. COMPETENCIAS PROFESIONALES GENERALES	6
4. EVALUACIÓN Y RECUPERACIÓN	7
4.1. Procedimientos y momentos de Evaluación	7
4.2. Criterios de ponderación	9
4.3. Criterios de evaluación.....	9
4.4. Criterios de recuperación	17
4.5. Evaluación de Competencias Profesionales.....	18
4.6. Evaluación del Proceso de la Enseñanza	19
5. ATENCIÓN A LA DIVERSIDAD.....	20
5.1. Alumnos de admisión tardía	20
5.2. Alumnos con necesidades educativas especiales	20
5.4. Alumnado con altas capacidades	20
6. CONTENIDOS	21
6.1. Relación de bloques temáticos	21
6.2. Secuenciación de contenidos.....	22
1.a. Resultado de Aprendizaje (RA1 y 7)	22
1.b. Contenidos Conceptuales	22
1.e. Criterios de Evaluación	23
2.b. Contenidos Conceptuales	24
2.e. Criterios de Evaluación	25
3.b. Contenidos Conceptuales	26
3.e. Criterios de Evaluación	26
6.2.4. Unidad didáctica 4: Alta Disponibilidad.....	27
6.2.8. Unidad didáctica 8: Seguridad activa en redes	32
6.3. Ponderación de Unidades Didácticas	33
7. MATERIAS TRANSVERSALES	34
8. ACTIVIDADES COMPLEMENTARIAS Y EXTRAESCOLARES	36
9. BIBLIOGRAFÍA, MATERIALES Y RECURSOS.....	36
9.2. Materiales, recursos y laboratorios	36

Código:	Rev.:	Fecha Implantación:	Entregar a:	Página 2 de 36
MD850401	4	16/09/2022	Jefa/e depto. → Jefatura estudios	

1. OBJETIVOS GENERALES

Los objetivos generales de este ciclo formativo, especificados en el artículo 9 del Real Decreto 1629/2009, de 30 de octubre, son los siguientes:

- a) Analizar la estructura del software de base, comparando las características y prestaciones de sistemas libres y propietarios, para administrar sistemas operativos de servidor.
- b) Instalar y configurar el software de base, siguiendo documentación técnica y especificaciones dadas, para administrar sistemas operativos de servidor.
- c) 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.
- d) Instalar y configurar software de gestión, siguiendo especificaciones y analizando entornos de aplicación, para administrar aplicaciones.
- e) Instalar y administrar software de gestión, relacionándolo con su explotación, para implantar y gestionar bases de datos.
- f) Configurar dispositivos hardware, analizando sus características funcionales, para optimizar el rendimiento del sistema.
- g) Configurar hardware de red, analizando sus características funcionales y relacionándolo con su campo de aplicación, para integrar equipos de comunicaciones.
- h) Analizar tecnologías de interconexión, describiendo sus características y posibilidades de aplicación, para configurar la estructura de la red telemática y evaluar su rendimiento.
- i) Elaborar esquemas de redes telemáticas utilizando software específico para configurar la estructura de la red telemática.
- j) Seleccionar sistemas de protección y recuperación, analizando sus características funcionales, para poner en marcha soluciones de alta disponibilidad.
- k) Identificar condiciones de equipos e instalaciones, interpretando planes de seguridad y especificaciones de fabricante, para supervisar la seguridad física.
- l) Aplicar técnicas de protección contra amenazas externas, tipificándolas y evaluándolas para asegurar el sistema.
- m) Aplicar técnicas de protección contra pérdidas de información, analizando planes de seguridad y necesidades de uso para asegurar los datos.
- n) Asignar los accesos y recursos del sistema, aplicando las especificaciones de la explotación, para administrar usuarios.
- ñ) Aplicar técnicas de monitorización interpretando los resultados y relacionándolos con las medidas correctoras para diagnosticar y corregir las disfunciones.
- o) Establecer la planificación de tareas, analizando actividades y cargas de trabajo del sistema para gestionar el mantenimiento.
- p) 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.
- q) Identificar formas de intervención en situaciones colectivas, analizando el proceso de toma de decisiones y efectuando consultas para liderar las mismas.

Código:	Rev.:	Fecha Implantación:	Entregar a:	Página 3 de 36
MD850401	4	16/09/2022	Jefa/e depto. → Jefatura estudios	

- r) 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.
- s) Reconocer las oportunidades de negocio, identificando y analizando demandas del mercado para crear y gestionar una pequeña empresa.
- t) 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.

Este módulo, Seguridad y Alta Disponibilidad, de 84 horas se imparte en el segundo curso del Ciclo Formativo de Grado Superior (CFGS) correspondiente al título de Técnico Superior en Administración de Sistemas Informáticos en Red (ASIR).

El módulo SAD se desarrolla durante los dos trimestres del segundo curso, a razón de 4 horas.

La **normativa** que regula tanto el título ASIR como el módulo SAD:

- 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. (BOE nº 278 de 18/11/2009)
- ORDEN de 19 de julio de 2010, por la que se desarrolla el currículo correspondiente al título de Técnico Superior en Administración de Sistemas Informáticos en Red. (BOJA nº 168 de 27/08/2010)

La **competencia general** del título ASIR está establecida como:

Configurar, administrar y mantener sistemas informáticos, garantizando la funcionalidad, la integridad de los recursos y servicios del sistema, con la calidad exigida y cumpliendo la reglamentación vigente.

*La formación del módulo contribuye a alcanzar los **objetivos generales** de este ciclo formativo que se relacionan a continuación:*

- j) Seleccionar sistemas de protección y recuperación, analizando sus características funcionales, para poner en marcha soluciones de alta disponibilidad.
- k) Identificar condiciones de equipos e instalaciones, interpretando planes de seguridad y especificaciones de fabricante, para supervisar la seguridad física.
- l) Aplicar técnicas de protección contra amenazas externas, tipificándolas y evaluándolas para asegurar el sistema.
- m) Aplicar técnicas de protección contra pérdidas de información, analizando planes de seguridad y necesidades de uso para asegurar los datos.

Código:	Rev.:	Fecha Implantación:	Entregar a:	Página 4 de 36
MD850401	4	16/09/2022	Jefa/e depto. → Jefatura estudios	

2. METODOLOGÍA

La metodología empleada se basa en los siguientes principios:

a.- Flexible

En esta asignatura se aplican varias metodologías. La técnica utilizada normalmente para las clases teóricas es la lección magistral del método expositivo, para transmitir los conocimientos básicos del módulo y los conceptos a utilizar posteriormente.

b.- Activa y participativa

Como en este método el profesor lleva la iniciativa, se intenta evitar que el alumnado permanezca pasivo utilizando normalmente una metodología activa y participativa, como la técnica del torbellino de ideas y la realización de trabajos en grupos pequeños, para que el alumno/a participe en el proceso de enseñanza aprendizaje y se habitúe a la búsqueda y consulta de material bibliográfico, manuales, Internet, etc., así como a la exposición de dichos trabajos.

c.- Explicativa demostrativa

Para las clases prácticas, en las que se utiliza el ordenador, la metodología utilizada, además de la activa participativa, es la explicativa demostrativa, en la que el profesor transmite el conocimiento a través de la realización práctica de las tareas en el ordenador, la cual el alumnado observa. Luego propone al alumno/a resolver un problema en el que se tiene que aplicar la información recibida y descubrir por sí mismo algunos conocimientos a través del ensayo – error para obtener la solución.

d.- Motivadora e interactiva

El profesor intenta crear un ambiente que favorezca la interacción profesor-alumno/a, integrando aspectos informativos, formales y socio-afectivos que estimulen el desarrollo del aprendizaje. También se utilizan como ejes del planteamiento metodológico el diálogo, el debate y la confrontación de ideas e hipótesis, entendiendo el proceso de enseñanza como la mejor forma en que el alumno/a es capaz de aprender y asimilar conceptos e informaciones.

e.- Aprendizaje significativo

El profesor favorece el aprendizaje significativo, facilitando que los alumnos/as sean capaces de establecer relaciones entre conocimientos y experiencias que ya poseen y la nueva información. También debe ser capaz de estimular y regular las interacciones entre profesor-alumno/a, alumno/a-alumno/a, facilitando el trabajo individual y alentando la investigación en grupo.

La metodología será la siguiente:

Código:	Rev.:	Fecha Implantación:	Entregar a:	Página 5 de 36
MD850401	4	16/09/2022	Jefa/e depto. → Jefatura estudios	

- Exposición de los contenidos teóricos para cada unidad didáctica
- Realización de ejercicios prácticos como modelo
- Planteamiento de ejercicios prácticos y resolución de los mismos por parte de los alumnos
- Orientación y resolución de dudas que surjan tanto en la realización de los ejercicios prácticos como de los conceptos teóricos tratados en cada unidad
- Supervisión y corrección del trabajo realizado por los alumnos
- Asesoramiento para el estudio de los alumnos incidiendo en los conceptos fundamentales de cada unidad

Se primará el uso de medios digitales tanto para la obtención y manejo de la información, apuntes y ejercicios como para las explicaciones teóricas y prácticas. Para ello las clases se desarrollarán en el aula-taller de informática de dotación del ciclo. Esto permitirá utilizar de forma ágil los siguientes recursos:

- el cañón de proyección
- el acceso a internet
- uso de la plataforma Moodle
- la consulta de manuales, apuntes y tutoriales on-line evitando el derroche de papel

3. COMPETENCIAS PROFESIONALES GENERALES

Según la ORDEN de 19 de julio de 2010, por la que se desarrolla el currículo correspondiente al título de Técnico Superior en Administración de Sistemas Informáticos en Red en Andalucía (BOJA 27-8-2010, página 9), la formación del módulo contribuye a alcanzar las *competencias profesionales, personales y sociales que se relacionan a continuación*:

- e) Optimizar el rendimiento del sistema configurando los dispositivos hardware de acuerdo a los requisitos de funcionamiento.
- f) Evaluar el rendimiento de los dispositivos hardware identificando posibilidades de mejoras según las necesidades de funcionamiento.
- i) Implementar soluciones de alta disponibilidad, analizando las distintas opciones del mercado, para proteger y recuperar el sistema ante situaciones imprevistas.
- j) Supervisar la seguridad física según especificaciones del fabricante y el plan de seguridad para evitar interrupciones en la prestación de servicios del sistema.

Código:	Rev.:	Fecha Implantación:	Entregar a:	Página 6 de 36
MD850401	4	16/09/2022	Jefa/e depto. → Jefatura estudios	

- k) Asegurar el sistema y los datos según las necesidades de uso y las condiciones de seguridad establecidas para prevenir fallos y ataques externos.
- m) Diagnosticar las disfunciones del sistema y adoptar las medidas correctivas para restablecer su funcionalidad.
- n) Gestionar y/o realizar el mantenimiento de los recursos de su área (programando y verificando su cumplimiento), en función de las cargas de trabajo y el plan de mantenimiento.
- o) Efectuar consultas, dirigiéndose a la persona adecuada y saber respetar la autonomía de los subordinados, informando cuando sea conveniente.
- r) Adaptarse a diferentes puestos de trabajo y nuevas situaciones laborales, originadas por cambios tecnológicos y organizativos.
- s) Resolver problemas y tomar decisiones individuales, siguiendo las normas y procedimientos establecidos, definidos dentro del ámbito de su competencia.

4. EVALUACIÓN Y RECUPERACIÓN

4.1. Procedimientos y momentos de Evaluación

Según la normativa indicada anteriormente, se establecen los siguientes momentos de evaluación:

- Evaluación inicial: Durante el **primer mes** desde el comienzo de las actividades lectivas se realizará una **evaluación inicial** que tendrá como objetivo fundamental indagar sobre las características y el nivel de competencias que presenta el alumnado en relación con los resultados de aprendizaje y contenidos de las enseñanzas que va a cursar. Durante dicha sesión, el tutor facilitará al equipo docente la información disponible sobre las características generales del grupo y las circunstancias específicamente académicas y personales con incidencia educativa del alumnado. La evaluación inicial también se realizará al inicio de cada Bloque de Contenidos y, en muchos casos, al comienzo de cada Unidad Didáctica con el fin de extraer información de las capacidades y conocimientos previos que nos permitan marcarnos objetivos concretos y determinar el grado de dificultad de las actividades. Mediante la observación y el desarrollo de las actividades de conocimientos previos, podremos evaluar el nivel de conocimiento, la actitud y la capacidad del alumnado tanto a nivel general como grupo como a nivel individual.
- Evaluación continua: el proceso de evaluación será continuo, ya que estará integrado en el proceso de enseñanza-aprendizaje y formativo, puesto que contribuye a formar la opinión del profesorado y la propia del alumnado sobre su aprendizaje. Para ello, se requerirá la participación en las actividades programadas para los distintos módulos profesionales del ciclo formativo.

Código:	Rev.:	Fecha Implantación:	Entregar a:	Página 7 de 36
MD850401	4	16/09/2022	Jefa/e depto. → Jefatura estudios	

- Evaluación sumativa o final: que determinará el grado de consecución de los objetivos al final de cada unidad didáctica o bloque temático. Dicha evaluación sumativa no se circunscribe a la obtención de una evaluación final, sino que la propia normativa establece que se realizará mediante las sesiones de evaluación parcial. Se expresará mediante la escala numérica de 1 a 10 sin decimales, considerándose positivas las calificaciones iguales o mayores que 5 y negativas las restantes. De acuerdo con **la Orden de evaluación del 29 de Septiembre de 2010**, se debe realizar una evaluación parcial o sumativa al menos tres veces al año (al final de cada evaluación) para informar al alumnado.

Para llevar a cabo el proceso de evaluación descrito anteriormente, se deberá tener en cuenta la evolución personal del alumnado y su participación en el grupo. Se realizará una evaluación cuantitativa y cualitativa, llevándose a cabo mediante la observación, el diálogo y el intercambio constante entre el docente y el alumno, además de los trabajos habituales de clase propuestos en las actividades. Entre los procedimientos de evaluación, podemos distinguir los siguientes:

- Técnicas observación directa. Valorarán la implicación del alumnado en el trabajo individual, en los conocimientos, habilidades y destrezas relacionadas con el módulo, en el trabajo en grupo y en las actitudes personales
- Medición. Se realizarán a través de pruebas escritas (u orales, en su caso), cuestionarios, informes, trabajos y presentaciones
- Técnicas de autoevaluación y coevaluación. Permitirán favorecer la reflexión y valoración del alumnado sobre sus propias dificultades, así como la participación de sus compañeros junto con el profesor en la regulación del proceso de enseñanza-aprendizaje
- Instrumentos. Para poner en prácticas las técnicas anteriores es necesario emplear procedimientos de evaluación que nos permitan registrar la información sobre el proceso de aprendizaje del alumnado, como las que se indican:
 - o Pruebas escritas y orales
 - o Rúbricas.
 - o Cuaderno docente, que incluirá:
 - Escalas de observación, listas de control y registro anecdótico.
 - Guías y fichas para el registro y revisión de las tareas de los alumnos
 - Guiones estructurados para registrar los diálogos y entrevistas realizados con los alumnos, sobre todo con los que presentan mayores problemas o dificultades
 - Cuestionarios de autoevaluación, inicio de una unidad o fase de aprendizaje.

A continuación en los siguientes apartados se describe el procedimiento de evaluación, indicando los criterios de ponderación, evaluación en competencias, criterios de calificación, criterios de recuperación y el proceso de evaluación de la enseñanza.

Código:	Rev.:	Fecha Implantación:	Entregar a:	Página 8 de 36
MD850401	4	16/09/2022	Jefa/e depto. → Jefatura estudios	

4.2. Criterios de ponderación

Las herramientas de evaluación serán las siguientes:

- Un Examen tipo test por cada Unidad Didáctica realizados en la plataforma Moodle
- Prácticas y ejercicios realizados en clase. Las prácticas deben realizarse en clase bajo la supervisión del profesor, excepto en el caso en el cual el alumno tenga muchas faltas de asistencia justificadas. En este último caso, el alumno podrá realizar las prácticas en casa pero debe entregarlas, éstas deben ser aptas y debe demostrar al profesor que las ha hecho él para superar este apartado.

4.3. Criterios de evaluación

Criterios de Calificación		
Criterio (marcar con una X debajo de SI o NO)	SI	NO
Entregar fuera de plazo resta puntuación (en caso afirmativo explicar debajo los criterios) <ul style="list-style-type: none"> • No resta, pero puede ser un ítem a tener en cuenta en las rúbricas de corrección. Por tanto, dejaría de puntuar ese apartado. 		X
Los alumnos/as deben llegar a un mínimo de la calificación para acceder a la media (en caso afirmativo determinar los mínimos, ya sea de la media, por criterio de evaluación, o por actividad) <ul style="list-style-type: none"> • La calificación mínima será de 5 sobre 10 en la primera oportunidad y 4,5 sobre 10 en la correspondiente recuperación. • En algunas pruebas de evaluación, como por ejemplo en controles tipo test, se podrá fijar el 5 sobre 10 en un número superior a la mitad de las cuestiones contestadas correctamente. 		X
Los alumnos/as deben superar todos los resultados de aprendizaje para aprobar el módulo (si procede, determinar qué resultados de aprendizaje debe superar el alumnado para obtener las competencias mínimas) <ul style="list-style-type: none"> • Para superar cada evaluación se deben haber superado cada uno de los resultados de aprendizaje asociados a las unidades impartidas en dicha evaluación. Es decir, para superar el módulo es necesario haber superado todas las unidades impartidas. La calificación final del módulo (mayo y junio) se obtiene mediante la ponderación de todos los resultados de aprendizaje obtenidos en el curso. 	X	
La NO entrega de un número mínimo de prácticas supone directamente que esa parte se recupera con un examen (en caso afirmativo explicar el número de prácticas -el 100%, el 80%, el 50%...-)		X

Código:	Rev.:	Fecha Implantación:	Entregar a:	Página 9 de 36
MD850401	4	16/09/2022	Jefa/e depto. → Jefatura estudios	

La NO entrega de ejercicios de clase supone directamente que esa parte se recupera con examen (en caso afirmativo explicar los criterios)		X
<ul style="list-style-type: none"> Todos los ejercicios de clase deben ser realizados, en caso contrario dejaría de puntuar en ese apartado. 		

Se prevé una prueba específica de evaluación para cada una de las unidades.

Los criterios de evaluación expresan el tipo y grado de aprendizaje que se espera que los alumnos hayan alcanzado respecto a los resultados de aprendizaje de cada uno de los módulos. Para el módulo de Seguridad y Alta disponibilidad desarrollado en esta programación, la Orden de 19 de julio de 2010 establece el conjunto de criterios de evaluación que se exponen a continuación.

1. Adopta pautas y prácticas de tratamiento seguro de la información, reconociendo las vulnerabilidades de un sistema informático y la necesidad de asegurarlo.

Criterios de evaluación:

- 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.

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

Criterios de evaluación:

- 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.

Código:	Rev.:	Fecha Implantación:	Entregar a:	Página 10 de 36
MD850401	4	16/09/2022	Jefa/e depto. → Jefatura estudios	

- 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.

Criterios de evaluación:

- 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.

Criterios de evaluación:

- 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.

Criterios de evaluación:

- a) Se han identificado los tipos de «proxy», sus características y funciones principales.
- b) Se ha instalado y configurado un servidor «proxy-caché».
- 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.

Código:	Rev.:	Fecha Implantación:	Entregar a:	Página 11 de 36
MD850401	4	16/09/2022	Jefa/e depto. → Jefatura estudios	

- 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 virtualización y configurando los entornos de prueba.

Criterios de evaluación:

- 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 virtualización 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 «clústeres» 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.

Criterios de evaluación:

- 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.

A continuación, las siguientes tablas muestran un resumen de la ponderación de las unidades didácticas sobre cada resultado de aprendizaje, pudiéndose observar en qué unidades se trabaja cada resultado de aprendizaje y qué ponderación tiene.

Código:	Rev.:	Fecha Implantación:	Entregar a:	Página 12 de 36
MD850401	4	16/09/2022	Jefa/e depto. → Jefatura estudios	

Resultado de aprendizaje	Criterio evaluación	UD. 1	UD. 2	UD. 3	UD. 4	UD. 5	UD. 6	UD. 7	UD. 8	Ponderación criterio	Total
1. Adopta pautas y prácticas de tratamiento seguro de la información, reconociendo las vulnerabilidades de un sistema informático y la necesidad de asegurarlo.	1.a)	6,25%								1,10%	10,00%
	1.b)	6,25%								1,10%	
	1.c)	6,25%								1,10%	
	1.d)	6,25%								1,10%	
	1.e)	6,25%								1,10%	
	1.f)	6,25%		20,00%						1,10%	
	1.g)	6,25%								1,10%	
	1.h)	6,25%								1,10%	
	1.i)	6,25%								1,10%	
2. Implanta mecanismos de seguridad activa, seleccionando y ejecutando contramedidas ante amenazas o ataques al sistema.	2.a)							11,11%	7,69%	1,55%	14,00%
	2.b)							11,11%	7,69%	1,55%	
	2.c)							11,11%	7,69%	1,55%	
	2.d)							11,11%	7,69%	1,55%	
	2.e)							11,11%	7,69%	1,55%	
	2.f)			20,00%				11,11%	7,69%	1,55%	
	2.g)							11,11%	7,69%	1,55%	
	2.h)			20,00%				11,11%	7,69%	1,55%	
	2.i)							11,11%	7,69%	1,55%	
3. Implanta técnicas seguras de acceso remoto a un sistema informático, interpretando y aplicando el plan de seguridad.	3.a)				14,3%				7,69%	2,85%	20,00%
	3.b)				14,3%				7,69%	2,85%	
	3.c)			20,00%	14,3%				7,69%	2,85%	
	3.d)				14,3%				7,69%	2,85%	

3.e)				14,3%					2,85%
3.f)			20,00%	14,3%					2,85%
3.g)				14,3%					2,85%

Tabla 1: Ponderación de los resultados de aprendizaje y criterios de evaluación sobre el curso

Resultado de aprendizaje	Criterio evaluación	UD. 1	UD. 2	UD. 3	UD. 4	UD. 5	UD. 6	UD. 7	UD. 8	Ponderación criterio	Total
4. Instala cortafuegos para asegurar un sistema informático, analizando sus prestaciones y controlando el tráfico hacia la red interna.	4.a)					7,14%				2,50%	20,00%
	4.b)					7,14%				2,50%	
	4.c)					7,14%				2,50%	
	4.d)					7,14%				2,50%	
	4.e)					7,14%				2,50%	
	4.f)					7,14%				2,50%	
	4.g)					7,14%				2,50%	
	4.h)					7,14%				2,50%	
5. Instala servidores «proxy», aplicando criterios de configuración que garanticen el funcionamiento seguro del servicio.	5.a)						11,11%			1,33%	12,00%
	5.b)						11,11%			1,33%	
	5.c)						11,11%			1,33%	
	5.d)						11,11%			1,33%	
	5.e)						11,11%			1,33%	
	5.f)						11,11%			1,33%	
	5.g)						11,11%			1,33%	
	5.h)						11,11%			1,33%	
	5.i)						11,11%			1,33%	
	6.a)		16,60%		14,28%					1,77%	16,00%

6. Instala soluciones de alta disponibilidad empleando técnicas de virtualización y configurando los entornos de prueba.	6.b)		16,60%		14,28%					1,77%	
	6.c)				14,28%					1,77%	
	6.d)		16,60%		14,28%					1,77%	
	6.e)				14,28%					1,77%	
	6.f)		16,60%							1,77%	
	6.g)				14,28%					1,77%	
	6.h)		16,60%		14,28%					1,77%	
	6.i)		16,60%		14,28%					1,77%	
Resultado de aprendizaje	Criterio evaluación	UD. 1	UD. 2	UD. 3	UD. 4	UD. 5	UD. 6	UD. 7	UD. 8	Ponderación criterio	Total
7. Reconoce la legislación y normativa sobre seguridad y protección de datos valorando su importancia.	7.a)	6,25%								1,14%	8,00%
	7.b)	6,25%								1,14%	
	7.c)	6,25%								1,14%	
	7.d)	6,25%								1,14%	
	7.e)	6,25%								1,14%	
	7.f)	6,25%								1,14%	
	7.g)	6,25%								1,14%	
Ponderación UD sobre el curso		10,00%	12,00%	18,00%	12,00%	18,00%	11,00%	11,00%	10,00%	100,00%	100,0%

	RA 1	RA 2	RA 3	RA 4	RA 5	RA 6	RA 7	Ponderación UD sobre el curso
UD 1	80,00%						100,00%	10,00%
UD 2						60,00%		12,00%
UD 3	20,00%	20,00%	28,00%					18,00%
UD 4			30,00%			40,00%		12,00%
UD 5				100,00%				18,00%
UD 6					100,00%			11,00%
UD 7		60,00%						11,00%
UD 8		20,00%	42,00%					10,00%
Ponderación de cada RA sobre el curso	10,00%	14,00%	20,00%	20,00%	12,00%	16,00%	8,00%	100,0%

Tabla 2: Ponderación de los resultados de aprendizaje y criterios de evaluación sobre el curso

4.4. Criterios de recuperación

La recuperación de cada resultado de aprendizaje no superado se planteará de manera individualizada para cada alumno o grupo de alumnos con una nueva prueba con los objetivos no alcanzados. Si no se superara esta segunda oportunidad se podrá recuperar dicha unidad en el periodo de recuperación de junio.

Las pruebas de recuperación se pueden plantear de dos maneras: completa y parcial. Para la completa se repite una nueva prueba con los mismos objetivos y contenidos que la prueba original. Con la parcial la prueba constaría solamente de los contenidos no superados por el alumno.

La calificación para las unidades recuperadas será la nota que el alumno obtenga.

Aquellos alumnos que no superen el módulo por evaluación continua por no haber superado una o varias unidades didácticas deberán asistir y superar todas las unidades en el periodo de recuperación de junio.

Los alumnos que, habiendo superado el módulo por evaluación continua, deseen mejorar su calificación deberán presentarse a un control de mejora. La calificación lograda reemplazaría la obtenida anteriormente. El control contaría con cuestiones prácticas y teóricas relativas a todas las unidades didácticas programadas para el módulo.

4.4.1 Recuperaciones en el período ordinario de clases (antes de la FCT):

Los alumnos que no hayan superado alguna de las evaluaciones (o que quieran subir nota) podrán presentarse a las siguientes actividades de recuperación:

- Un Examen de recuperación tipo test por cada Unidad Didáctica realizados en la plataforma Moodle. Podrán presentarse a los exámenes de las Unidades Didácticas que consideren oportunos. Estos exámenes de recuperación se realizarán sólo una vez en el período ordinario.
- Repetición de las prácticas que no hayan superado.

4.4.2 Recuperaciones en el período no ordinario de clases: (período de recuperación)

Los alumnos que no hayan superado el módulo en el período ordinario de clases tendrán la oportunidad de realizar las prácticas no efectuadas durante el período ordinario en las clases de recuperación que se iniciarán después de la segunda evaluación. En este período los alumnos realizarán las siguientes actividades de recuperación:

- Un Examen de recuperación tipo test por cada Unidad Didáctica realizados en la plataforma Moodle. Podrán presentarse a los exámenes de las Unidades Didácticas que consideren

Código:	Rev.:	Fecha Implantación:	Entregar a:	Página 17 de 36
MD850401	4	15/02/2018	Jefa/e depto. → Jefatura estudios	

oportunos, de forma que se les conserva la nota más alta que obtuvieron en el periodo ordinario de clases. Estos exámenes de recuperación se realizarán sólo una vez en este periodo.

- Repetición de las prácticas que no hayan superado.

El alumno que no haya podido asistir regularmente a clase por motivos debidamente justificados realizará las prácticas y ejercicios posteriormente al resto del grupo, así como los exámenes de recuperación de Moodle no realizados. Para estos alumnos se aplicarán los mismos criterios que los aplicados a los demás alumnos en lo que respecta a las condiciones necesarias para aprobar el módulo. La única salvedad es que las prácticas las puede realizar en casa y luego tendrán que ser defendidas delante del profesor para su calificación.

4.5. Evaluación de Competencias Profesionales

La formación del módulo contribuye a alcanzar las competencias profesionales, personales y sociales de este título que se relacionan a continuación:

- e) Optimizar el rendimiento del sistema configurando los dispositivos hardware de acuerdo a los requisitos de funcionamiento.
- f) Evaluar el rendimiento de los dispositivos hardware identificando posibilidades de mejoras según las necesidades de funcionamiento.
- i) Implementar soluciones de alta disponibilidad, analizando las distintas opciones del mercado, para proteger y recuperar el sistema ante situaciones imprevistas.
- j) Supervisar la seguridad física según especificaciones del fabricante y el plan de seguridad para evitar interrupciones en la prestación de servicios del sistema.
- k) Asegurar el sistema y los datos según las necesidades de uso y las condiciones de seguridad establecidas para prevenir fallos y ataques externos.
- m) Diagnosticar las disfunciones del sistema y adoptar las medidas correctivas para restablecer su funcionalidad.
- n) Gestionar y/o realizar el mantenimiento de los recursos de su área (programando y verificando su cumplimiento), en función de las cargas de trabajo y el plan de mantenimiento.
- o) Efectuar consultas, dirigiéndose a la persona adecuada y saber respetar la autonomía de los subordinados, informando cuando sea conveniente.
- r) Adaptarse a diferentes puestos de trabajo y nuevas situaciones laborales, originadas por cambios tecnológicos y organizativos.
- s) Resolver problemas y tomar decisiones individuales, siguiendo las normas y procedimientos establecidos, definidos dentro del ámbito de su competencia.

Código:	Rev.:	Fecha Implantación:	Entregar a:	Página 18 de 36
MD850401	4	15/02/2018	Jefa/e depto. → Jefatura estudios	

4.6. Evaluación del Proceso de la Enseñanza

Para ello debemos valorar, entre otros, los siguientes factores:

- ¿Los contenidos han sido los adecuados para alcanzar los objetivos?
- ¿Las actividades han estado bien secuenciadas y han atendido los conocimientos previos?
- ¿El tiempo utilizado ha sido suficiente?
- ¿La organización en grupos ha sido la adecuada?
- ¿Las pruebas realizadas al alumnado han sido adecuadas?
- ¿Los resultados obtenidos por el alumnado han sido los esperados?

Las conclusiones a las que lleguemos permitirán optimizar dicho proceso en el futuro y se deben reflejar en la memoria final del curso. Esta evaluación se realizará al terminar cada bloque de contenidos y, sobre todo, al finalizar cada sesión de evaluación.

Código:	Rev.:	Fecha Implantación:	Entregar a:	Página 19 de 36
MD850401	4	15/02/2018	Jefa/e depto. → Jefatura estudios	

5. ATENCIÓN A LA DIVERSIDAD

Los casos más corrientes a los que nos enfrentamos en estas enseñanzas son los de aquellos alumnos/as que van más adelantados al resto del grupo, bien sea porque ya conocen el tema como es el caso de repetidores o bien porque lo comprenden rápidamente; estos alumnos serán atendidos con actividades de ampliación, las cuales les proporcionarán puntuación adicional. Por otro lado pueden existir otros alumnos/as a los que por el contrario, les pueda costar más trabajo llegar a los mínimos exigidos, y a éstos se les mandarán también ejercicios adicionales, pero en este caso de refuerzo.

5.1. Alumnos de admisión tardía

El módulo objeto de esta programación se implanta en el segundo año del ciclo, por este motivo la admisión y matriculación debe estar completa al comienzo del curso. Si por cualquier motivo se incorporara algún alumno de forma tardía, se le dará acceso a todo el material impartido hasta ese momento. Además se le hará un seguimiento a parte en el cual el alumno podrá preguntar todas las posibles dudas que le surgieran respecto a la materia ya dada.

En caso de que ya se hubiesen hecho exámenes o trabajos se le dará la oportunidad de realizar dichas pruebas siempre y cuando el motivo de la incorporación tardía esté justificado.

5.2. Alumnos con necesidades educativas especiales

Aunque no hay alumnos con necesidades educativas especiales, en el caso de que así fuese, la evaluación de otros alumnos/as con necesidades educativas especiales, se realizarán tomando como referencia los criterios y evaluación establecidos en las adaptaciones curriculares, que, para ello se hubieran realizado y valorando las recomendaciones que por parte del Departamento de Orientación pudieran dictarse.

5.3. Alumnos con compatibilidad laboral y/o modularidad

En este apartado se seguirán las directrices de la programación de departamento.

5.4. Alumnado con altas capacidades

No hay alumnos con altas capacidades en el grupo, pero si los hubiese, se propondrían actividades complementarias que amplíen sus conocimientos tanto sobre los contenidos tratados como de otros relacionados.

Código:	Rev.:	Fecha Implantación:	Entregar a:	Página 20 de 36
MD850401	4	15/02/2018	Jefa/e depto. → Jefatura estudios	

Implicar a estos alumnos en la ayuda a sus compañeros de clase como monitores en aquellas actividades en las que demuestren mayor destreza. Con esta medida se pretende además reforzar la cohesión del grupo y fomentar el aprendizaje colaborativo.

6. CONTENIDOS

A continuación se detallan las diferentes unidades didácticas con sus correspondientes criterios de evaluación.

6.1. Relación de bloques temáticos

Bloque temático		Nº	Título Unidad Didáctica	Horas	Trimestre		
					1º	2º	3º
1	Introducción a la seguridad informática	1	Conceptos básicos de la seguridad informática	8	X		
Bloque temático		Nº	Título Unidad Didáctica	Horas	Trimestre		
					1º	2º	3º
2	Seguridad pasiva	2	Seguridad pasiva. Hardware de almacenamiento y recuperación de datos	10	X		
Bloque temático		Nº	Título Unidad Didáctica	Horas	Trimestre		
					1º	2º	3º
3	Criptografía	3	Sistemas de identificación. Criptografía	16	X		
Bloque temático		Nº	Título Unidad Didáctica	Horas	Trimestre		
					1º	2º	3º
4	Alta disponibilidad	4	Alta Disponibilidad	10	X		
Bloque temático		Nº	Título Unidad Didáctica	Horas	Trimestre		
					1º	2º	3º
5	Seguridad activa	5	Seguridad de alto nivel en redes: cortafuegos	16		X	
		6	Seguridad de alto nivel en redes: proxy	9		X	
		7	Seguridad activa en el sistema	9		X	
		8	Seguridad activa en redes	6		X	

Horas totales de módulo: 84 horas.

Código:	Rev.:	Fecha Implantación:	Entregar a:	Página 21 de 36
MD850401	4	15/02/2018	Jefa/e depto. → Jefatura estudios	

Distribución de las 84 horas de clase previstas:

1ª Evaluación (50 horas)				2ª Evaluación (34 horas)		
Sept.	Oct.	Nov.	Dic.	Ene.	Feb.	Mar.

6.2. Secuenciación de contenidos

6.2.1. Unidad didáctica 1: Conceptos básicos de la seguridad informática

1.a. Resultado de Aprendizaje (RA1 y 7)

RA 1. Adopta pautas y prácticas de tratamiento seguro de la información, reconociendo las vulnerabilidades de un sistema informático y la necesidad de asegurarlo.

RA 7. Reconoce la legislación y normativa sobre seguridad y protección de datos valorando su importancia.

1.b. Contenidos Conceptuales

- *Visión global de la seguridad informática. Conceptos*
- Servicios de seguridad
 - Confidencialidad
 - Integridad
 - Disponibilidad
 - No repudio
- Clasificación de seguridad
 - Seguridad física y seguridad lógica
 - Seguridad activa y seguridad pasiva
 - Modelo de seguridad. Amenazas y fraudes
 - Activos
 - Impactos
 - Riesgos
 - Vulnerabilidades
 - Tipos de amenazas
- Legislación
 - Protección de datos
 - Servicios de la sociedad de la información y correo electrónico

1.c. Contenidos Procedimentales

- Determinar los problemas que pueden surgir por no tener un acceso a Internet correctamente protegido.

Código:	Rev.:	Fecha Implantación:	Entregar a:	Página 22 de 36
MD850401	4	15/02/2018	Jefa/e depto. → Jefatura estudios	

- Valorar los problemas que pueden surgir por no tener protegidos los sistemas.
- Reconocer los certificados digitales.
- Verificar la integridad de los ficheros.
- Reconocer los activos, daños e impactos que pueden sufrir las empresas que no están bien protegidas.
- Determinar las pautas de protección de los sistemas.
- Identificar los ataques recibidos.
- Conocer el proceso legal para almacenar información personal de clientes.

1.d. Contenidos Actitudinales

- Apreciar la importancia de mantener los equipos informáticos y la información protegidos frente a posibles amenazas, tanto físicas como lógicas.
- Valorar la necesidad de utilizar todas las medidas de seguridad necesarias para proteger la información.
- Mostrar interés en la adquisición de conocimientos.
- Darse cuenta de lo importante que es saber proteger correctamente los equipos de las posibles amenazas, tanto físicas como lógicas.
- Utilizar el vocabulario correcto para referirse a los nuevos conceptos aprendidos.

1.e. Criterios de Evaluación

- 1a) Se ha valorado la importancia de asegurar la privacidad, coherencia y disponibilidad de la información en los sistemas informáticos.
- 1b) Se han descrito las diferencias entre seguridad física y lógica.
- 1c) Se han clasificado las principales vulnerabilidades de un sistema informático, según su tipología y origen.
- 1d) Se ha contrastado la incidencia de las técnicas de ingeniería social en los fraudes informáticos.
- 1e) Se han adoptado políticas de contraseñas.
- 1f) Se han valorado las ventajas que supone la utilización de sistemas biométricos.
- 1g) Se han aplicado técnicas criptográficas en el almacenamiento y transmisión de la información.
- 1h) Se ha reconocido la necesidad de establecer un plan integral de protección perimetral, especialmente en sistemas conectados a redes públicas.
- 1i) Se han identificado las fases del análisis forense ante ataques a un sistema.
- 7a) Se ha descrito la legislación sobre protección de datos de carácter personal.
- 7b) Se ha determinado la necesidad de controlar el acceso a la información personal almacenada.
- 7c) Se han identificado las figuras legales que intervienen en el tratamiento y mantenimiento de los ficheros de datos.
- 7d) Se ha contrastado el deber de poner a disposición de las personas los datos personales que les conciernen.

Código:	Rev.:	Fecha Implantación:	Entregar a:	Página 23 de 36
MD850401	4	15/02/2018	Jefa/e depto. → Jefatura estudios	

- 7e) Se ha descrito la legislación actual sobre los servicios de la sociedad de la información y comercio electrónico.
- 7f) Se han contrastado las normas sobre gestión de seguridad de la información.
- 7g) Se ha comprendido la necesidad de conocer y respetar la normativa legal aplicable.

6.2.2. Unidad didáctica 2: Seguridad pasiva. Hardware y almacenamiento. Recuperación de datos

2.a. Resultado de Aprendizaje (RA6)

RA 6. Implanta soluciones de alta disponibilidad empleando técnicas de virtualización y configurando los entornos de prueba.

2.b. Contenidos Conceptuales

- Ubicación y protección física de los equipos y servidores
- Sistemas de alimentación ininterrumpida (SAI)
- Almacenamiento de la información: rendimiento, disponibilidad, accesibilidad
- Almacenamiento redundante: RAID (Redundant Array of Independent Disk)
- NAS (Network Attached Storage)
- SAN (Storage Area Network)
- Copias de seguridad e imágenes de respaldo.
- Medios de almacenamiento en copias de seguridad.
- Políticas de copias de seguridad.
- Software de copias de seguridad.
- Recuperación de datos.

2.c. Contenidos Procedimentales

- Determinar los problemas que pueden surgir por no escoger correctamente la ubicación de un CPD.
- Valorar los problemas que pueden surgir por no considerar la seguridad necesaria en los centros de procesamiento de datos.
- Determinar la necesidad de los planes de recuperación en caso de desastre.
- Conocer las ventajas del uso de equipos SAI y seleccionarlos correctamente para satisfacer las necesidades concretas del sistema.
- Valorar la necesidad de utilizar sistemas de almacenamiento redundante o distribuido para proteger los datos de los equipos.
- Determinar qué tipo de sistema de almacenamiento redundante o distribuido es más adecuado para nuestros equipos.
- Configurar sistemas RAID.

Código:	Rev.:	Fecha Implantación:	Entregar a:	Página 24 de 36
MD850401	4	15/02/2018	Jefa/e depto. → Jefatura estudios	

- Determinar el tipo de copia a realizar.
- Realizar copias de seguridad.
- Restaurar las copias de seguridad.
- Definir la política de copias de seguridad.

2.d. Contenidos Actitudinales

- Apreciar la importancia de mantener los equipos informáticos y la información protegidos frente a amenazas físicas.
- Valorar la necesidad de utilizar todas las medidas necesarias para proteger nuestros sistemas.
- Valorar la necesidad de conocer software específico para recuperar información borrada.
- Valorar la necesidad de realizar copias de respaldo para recuperar la información en caso de perderla.
- Mostrar interés en la adquisición de conocimientos.
- Utilizar el vocabulario correcto para referirse a los nuevos conceptos aprendidos.

2.e. Criterios de Evaluación

- 6a) Se han analizado supuestos y situaciones en las que se hace necesario implementar soluciones de alta disponibilidad.
- 6b) Se han identificado soluciones hardware para asegurar la continuidad en el funcionamiento de un sistema.
- 6d) Se ha implantado un servidor redundante que garantice la continuidad de servicios en casos de caída del servidor principal.
- 6f) Se han implantado sistemas de almacenamiento redundante sobre servidores y dispositivos específicos.
- 6h) Se han analizado soluciones de futuro para un sistema con demanda creciente.
- 6i) Se han esquematizado y documentado soluciones para diferentes supuestos con necesidades de alta disponibilidad.

6.2.3. Unidad didáctica 3: Sistemas de identificación. Criptografía.

3.a. Resultado de Aprendizaje (RA1, 2 y 3)

RA 1. Adopta pautas y prácticas de tratamiento seguro de la información, reconociendo las vulnerabilidades de un sistema informático y la necesidad de asegurarlo.

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

RA 3. Implanta técnicas seguras de acceso remoto a un sistema informático, interpretando y aplicando el plan de seguridad.

Código:	Rev.:	Fecha Implantación:	Entregar a:	Página 25 de 36
MD850401	4	15/02/2018	Jefa/e depto. → Jefatura estudios	

3.b. Contenidos Conceptuales

- Métodos para asegurar la privacidad de la información transmitida.
- Criptografía:
- Cifrado de clave secreta (simétrica).
- Cifrado de clave pública (asimétrica).
- Funciones de mezcla o resumen (hash).
- Sistemas de identificación:
- Firma digital.
- Certificado digital.
- Distribución de claves. PKI.

3.c. Contenidos Procedimentales

- Cifrar textos mediante diversos algoritmos.
- Generar parejas de claves para el cifrado asimétrico.
- Exportar e importar certificados.
- Intercambiar claves o certificados.
- Revocar un certificado.
- Instalar una entidad emisora de certificados.
- Realizar peticiones de certificados a una entidad emisora.
- Retirar certificados.
- Firmar mensajes.
- Obtener certificados digitales.
- Enviar correos electrónicos haciendo uso del certificado digital.

3.d. Contenidos Actitudinales

- Apreciar la necesidad de cifrar la información para mantener la confidencialidad.
- Valorar la importancia del uso de los certificados y firmas digitales.
- Mostrar interés en la adquisición de los conocimientos.
- Utilizar el vocabulario correcto para referirse a los nuevos conceptos aprendidos.

3.e. Criterios de Evaluación

- 2f) Se han utilizado técnicas de cifrado, firmas y certificados digitales en un entorno de trabajo basado en el uso de redes públicas.
- 2i) Se han descrito los tipos y características de los sistemas de detección de intrusiones.
- 3c) Se han identificado los protocolos seguros de comunicación y sus ámbitos de utilización.
- 3f) Se han identificado y configurado los posibles métodos de autenticación en el acceso de usuarios remotos a través de la pasarela.

Código:	Rev.:	Fecha Implantación:	Entregar a:	Página 26 de 36
MD850401	4	15/02/2018	Jefa/e depto. → Jefatura estudios	

- 1f) Se han aplicado técnicas criptográficas en el almacenamiento y transmisión de la información.

6.2.4. Unidad didáctica 4: Alta Disponibilidad

4.a. Resultado de Aprendizaje (RA6)

RA 6. Implanta soluciones de alta disponibilidad empleando técnicas de virtualización y configurando los entornos de prueba.

4.b. Contenidos Conceptuales

- Alta disponibilidad
- Balanceo de carga
- Escalabilidad
- Clústeres de servidores

4.c. Contenidos Procedimentales

- Comprender el concepto de alta disponibilidad
- Instalar y configurar balanceadores de carga
- Comprender los conceptos básicos sobre clustering
- Instalar y configurar un clúster de Alta Disponibilidad

4.d. Contenidos Actitudinales

- Valorar la necesidad de utilizar técnicas de Alta Disponibilidad.
- Valorar la importancia de la Alta Disponibilidad en los sistemas actuales.
- Aprender la importancia de proteger los sistemas informáticos y la información frente a todo tipo de contingencias.
- Valorar la importancia de la escalabilidad en los sistemas actuales.
- Mostrar interés en la adquisición de conocimientos.
- Utilizar el vocabulario correcto para referirse a los nuevos conceptos y procedimientos aprendidos.

4.e. Criterios de Evaluación

- 6a) Se han analizado supuestos y situaciones en las que se hace necesario implementar soluciones de alta disponibilidad.
- 6b) Se han identificado soluciones hardware para asegurar la continuidad en el funcionamiento de un sistema.
- 6c) Se han evaluado las posibilidades de la virtualización de sistemas para implementar soluciones de alta disponibilidad.
- 6d) Se ha implantado un servidor redundante que garantice la continuidad de servicios en casos de caída del servidor principal.

Código:	Rev.:	Fecha Implantación:	Entregar a:	Página 27 de 36
MD850401	4	15/02/2018	Jefa/e depto. → Jefatura estudios	

- 6e) Se ha implantado un balanceador de carga a la entrada de la red interna.
- 6g) Se ha evaluado la utilidad de los sistemas de «clústeres» para aumentar la fiabilidad y productividad del sistema.
- 6h) Se han analizado soluciones de futuro para un sistema con demanda creciente.
- 6i) Se han esquematizado y documentado soluciones para diferentes supuestos con necesidades de alta disponibilidad.

6.2.5. Unidad didáctica 5: Seguridad de alto nivel en redes: cortafuegos

5.a. Resultado de Aprendizaje (RA4)

RA 4. Implanta cortafuegos para asegurar un sistema informático, analizando sus prestaciones y controlando el tráfico hacia la red interna.

5.b. Contenidos Conceptuales

- Las funciones principales de los cortafuegos.
- Los tipos de cortafuegos que existen.
- Las arquitecturas de cortafuegos.
- El filtrado de paquetes y reglas de filtrado.
- La instalación y utilización de cortafuegos.
- Los logs y registros de actividad.

5.c. Contenidos Procedimentales

- Conocer las ventajas del uso de cortafuegos.
- Elegir el cortafuegos idóneo para el sistema que se vaya a proteger.
- Establecer las reglas de filtrado adecuadas para la red.
- Instalar y configurar un cortafuegos.
- Identificar distintas arquitecturas de red, así como sus ventajas e inconvenientes.
- Reconocer la información recogida en los archivos de monitorización.

5.d. Contenidos Actitudinales

- Valorar la importancia de proteger nuestros equipos de accesos desde el exterior y el interior de nuestra red.
- Utilizar la lógica para establecer las reglas de filtrado más adecuadas en cada situación.
- Mostrar iniciativa para proteger la red doméstica.
- Mostrar interés en la adquisición de conocimientos.
- Utilizar el vocabulario correcto para referirse a los nuevos conceptos aprendidos.

Código:	Rev.:	Fecha Implantación:	Entregar a:	Página 28 de 36
MD850401	4	15/02/2018	Jefa/e depto. → Jefatura estudios	

5.e. Criterios de Evaluación

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

6.2.6. Unidad didáctica 6: Seguridad de alto nivel en redes: proxy**6.a. Resultado de Aprendizaje (RA5)**

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

6.b. Contenidos Conceptuales

- Características y funcionamiento de los proxy.
- Instalación y configuración de un proxy.
- Filtrar acceso y tráfico en el proxy.
- Métodos de autenticación en un proxy.
- Monitorización del proxy.

6.c. Contenidos Procedimentales

- Identificar las funciones de un proxy y aplicarlas en una situación concreta y definida.
- Conocer y manejar los principales proxys que hay en el mercado (WinGate y Squid).
- Configurar adecuadamente las reglas de acceso de un proxy WinGate y de un Squid.
- Utilizar clasificaciones de sitios de Internet para restringir el acceso a un determinado tipo de contenidos.
- Comprender y controlar los ficheros de log generados por los proxys.

6.d. Contenidos Actitudinales

- Organizar y analizar el trabajo, antes de realizarlo y durante su desarrollo.

Código:	Rev.:	Fecha Implantación:	Entregar a:	Página 29 de 36
MD850401	4	15/02/2018	Jefa/e depto. → Jefatura estudios	

- Tener una actitud crítica pero respetuosa con los compañeros, lo que favorece unas mejores relaciones laborales en un futuro puesto de trabajo.
- Resolver problemas y tomar decisiones siguiendo las normas y procedimientos establecidos.
- Participar de forma activa en la vida económica, social y cultural con una actitud crítica y responsable.
- Reconocer los derechos y deberes.
- Mostrar interés en la adquisición de conocimientos.
- Utilizar el vocabulario correcto para referirse a los nuevos conceptos y procedimientos aprendidos.

6.e. Criterios de Evaluación

- 5a) Se han identificado los tipos de proxy, sus características y funciones principales.
- 5b) Se ha instalado y configurado un servidor proxy-caché.
- 5c) Se han configurado los métodos de autenticación en el proxy.
- 5d) Se ha configurado un proxy en modo transparente.
- 5e) Se ha utilizado el servidor proxy para establecer restricciones de acceso web.
- 5f) Se han solucionado problemas de acceso desde los clientes al proxy.
- 5g) Se han realizado pruebas de funcionamiento del proxy, monitorizando su actividad con herramientas gráficas.
- 5h) Se ha configurado un servidor proxy en modo inverso.
- 5i) Se ha elaborado documentación relativa a la instalación, configuración y uso de servidores proxy.

6.2.7. Unidad didáctica 7: Seguridad activa en el sistema.

7.a. Resultado de Aprendizaje (RA2)

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

7.b. Contenidos Conceptuales

- La seguridad en el arranque y en particiones.
- Las actualizaciones y parches de seguridad en el sistema y en las aplicaciones.
- La autenticación de usuarios.
- Listas de control de acceso.
- La monitorización del sistema.
- El software que vulnera la seguridad del sistema.

Código:	Rev.:	Fecha Implantación:	Entregar a:	Página 30 de 36
MD850401	4	15/02/2018	Jefa/e depto. → Jefatura estudios	

7.c. Contenidos Procedimentales

- Proteger el arranque del sistema frente a intrusos.
- Cifrar particiones para que no sean accesibles a personal ajeno.
- Crear cuotas de disco.
- Definir políticas de contraseñas.
- Crear contraseñas seguras.
- Definir listas de control de acceso.
- Monitorizar el sistema.
- Hacer ARP spoofing y DNS spoofing.
- Comprometer una sesión telnet.
- Configurar un análisis con antivirus.
- Detectar las amenazas del sistema.

7.d. Contenidos Actitudinales

Apreciar la necesidad de proteger al sistema frente a los atacantes.

Valorar la importancia de definir cuotas de disco.

Valorar la importancia de monitorizar el sistema.

Valorar la repercusión del uso de antivirus para evitar la entrada de troyanos, gusanos y virus.

- Mostrar interés en la adquisición de los conocimientos.
- Utilizar el vocabulario correcto para referirse a los nuevos conceptos aprendidos.

7.e. Criterios de Evaluación

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

Código:	Rev.:	Fecha Implantación:	Entregar a:	Página 31 de 36
MD850401	4	15/02/2018	Jefa/e depto. → Jefatura estudios	

6.2.8. Unidad didáctica 8: Seguridad activa en redes

8.a. Resultado de Aprendizaje (RA2 y 3)

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

RA 3. Implanta técnicas seguras de acceso remoto a un sistema informático, interpretando y aplicando el plan de seguridad

8.b. Contenidos Conceptuales

- Seguridad en la conexión a redes no fiables
- Introducción a protocolos seguros
- Seguridad en redes cableadas
- Intrusiones externas vs. intrusiones internas
- Redes privadas virtuales (VPN)
 - Detección de intrusos
 - Seguridad en los accesos de red: Arranque de servicios y monitorización
- Seguridad en redes inalámbricas
- Tecnologías Wi-Fi
- Seguridad en los protocolos para comunicaciones inalámbricas
- Tipos de ataques
- Mecanismos de seguridad

8.c. Contenidos Procedimentales

- Conocer los riesgos que implica conectarse a redes no seguras como Internet.
- Reconocer los protocolos seguros y las ventajas de utilizarlos.
- Conocer las alternativas de conexión segura a través de redes inseguras.
- Valorar la necesidad de utilizar herramientas de detección de spyware, malware e intrusos.
- Determinar la necesidad de iniciar automáticamente o no determinados servicios del sistema operativo.
- Valorar los riesgos de seguridad de las conexiones inalámbricas.
- Conocer los distintos estándares IEEE 802.11.
- Conocer las alternativas de seguridad para redes inalámbricas.

8.d. Contenidos Actitudinales

- Valorar la importancia de proteger nuestros sistemas cuando se utilizan redes no seguras, ya sean cableadas o inalámbricas.
- Mostrar iniciativa para proteger la red doméstica.

Código:	Rev.:	Fecha Implantación:	Entregar a:	Página 32 de 36
MD850401	4	15/02/2018	Jefa/e depto. → Jefatura estudios	

- Mostrar interés en la adquisición de conocimientos.
- Utilizar el vocabulario correcto para referirse a los nuevos conceptos aprendidos.

8.e. Criterios de Evaluación

- 2a) Se han clasificado los principales tipos de amenazas lógicas contra un sistema informático.
- 2b) Se ha verificado el origen y la autenticidad de las aplicaciones instaladas en un equipo, así como el estado de actualización del sistema operativo.
- 2c) Se han identificado la anatomía de los ataques más habituales, así como las medidas preventivas y paliativas disponibles.
- 2d) Se han analizado diversos tipos de amenazas, ataques y software malicioso, en entornos de ejecución controlados.
- 2e) Se han implantado aplicaciones específicas para la detección de amenazas y la eliminación de software malicioso.
- 2f) Se han utilizado técnicas de cifrado, firmas y certificados digitales en un entorno de trabajo basado en el uso de redes públicas.
- 2g) Se han evaluado las medidas de seguridad de los protocolos usados en redes inalámbricas.
- 2h) Se ha reconocido la necesidad de inventariar y controlar los servicios de red que se ejecutan en un sistema.
- 2i) Se han descrito los tipos y características de los sistemas de detección de intrusiones.
- 3a) Se han descrito escenarios típicos de sistemas con conexión a redes públicas en los que se precisa fortificar la red interna.
- 3b) Se han clasificado las zonas de riesgo de un sistema, según criterios de seguridad perimetral.
- 3c) Se han identificado los protocolos seguros de comunicación y sus ámbitos de utilización.
- 3d) Se han configurado redes privadas virtuales mediante protocolos seguros a distintos niveles.

6.3. Ponderación de Unidades Didácticas

El criterio de ponderación de las unidades didácticas se ha efectuado en relación al número de horas dedicado a cada unidad didáctica junto a la importancia de las mismas y será usado para calcular la nota final.

Código:	Rev.:	Fecha Implantación:	Entregar a:	Página 33 de 36
MD850401	4	15/02/2018	Jefa/e depto. → Jefatura estudios	

UNIDAD DIDÁCTICA	PONDERACIÓN
UD 1- INTRODUCCIÓN	10%
UD 2 - SEG PASIVA	12%
UD 3 - CRIPTOGRAFÍA	18%
UD 4 - HA	12%
UD 5 - FIREWALL	18%
UD 6 - PROXY	11%
UD 7 - SEG ACTIVA SISTEMA	11%
UD 8 -SEG ACTIVA REDES	8%

7. MATERIAS TRANSVERSALES

Según los artículos 39 y 40 de la LEA 17/2007 y el artículo 3 del Decreto 436/2008 por el que se establece la ordenación de la Formación Profesional, en todas las enseñanzas han de incorporarse valores transversales y educación en valores. Éstos son un conjunto de saberes basados en actitudes, valores y normas que dan respuesta a algunos problemas sociales existentes en la actualidad. Deben ser tratados en todas las áreas de forma global y programada, aunque también se transmiten a través del currículo oculto que cada docente, equipo o centro transmite con sus opiniones. Por ello se denominan transversales, ya que no surgen como un programa paralelo al desarrollo del currículo sino insertado en la dinámica diaria del proceso de enseñanza-aprendizaje. Son complementarios y deben impregnar la totalidad de actividades. En relación a ellos se plantean los siguientes objetivos de los valores transversales para el módulo:

- Fomentar la tolerancia y el respeto hacia los demás.
- Asignar responsabilidades al alumnado.
- Fomentar el consumo inteligente, especialmente de componentes informáticos.
- Fomentar la responsabilidad ante problemas ambientales, especialmente aquellos relacionados con la informática
- Trabajar en equipo.
- Aprender a ver y escuchar a los demás.
- Conocer y respetar las distintas culturas y etnias
- Favorecer actitudes y hábitos no sexistas.
- Desarrollar hábitos de lectura y escritura.
- Utilizar libros, manuales técnicos y prensa escrita como fuente de información.
- Aplicar las TIC al proceso de enseñanza-aprendizaje.

Código:	Rev.:	Fecha Implantación:	Entregar a:	Página 34 de 36
MD850401	4	15/02/2018	Jefa/e depto. → Jefatura estudios	

- Conocer cómo buscar de manera eficiente información en Internet.

Para la consecución de estos objetivos se planteará el desarrollo habitual de las actividades de clase utilizando técnicas que los favorezcan, impregnando el proceso de enseñanza-aprendizaje. Además, hay un conjunto de fechas idóneas para motivar la reflexión sobre dicha temática, tanto mediante actividades diarias como extraordinarias (Día de la Mujer, contra la Violencia de Género, Día de Andalucía, de la Constitución, Día Europeo de la protección de datos, etc.)

Tomando como referencia los incluidos en el Proyecto Educativo del Centro y adaptándolos a estos alumnos y alumnas en concreto, y por su relación con este módulo, se desarrolla de la siguiente manera:

- Educación para la salud:
 - Ergonomía del puesto de trabajo: se harán consideraciones de tipo ergonómico sobre la forma más adecuada de utilizar el ordenador, para disfrutar de una mejor salud postural.
 - Seguridad e higiene en el trabajo
 - Prevención de riesgos laborales.
- Educación para la paz y convivencia:
 - Se harán consideraciones relacionadas con adoptar situaciones de diálogo y consenso frente a situaciones conflictivas en el trabajo en grupo.
 - Fomento del diálogo e intercambio razonado de puntos de vista cuando se realicen prácticas en parejas o grupos.
 - Importancia del trabajo en equipo para conseguir un objetivo común.
 - Respeto del trabajo de todos y su influencia en el funcionamiento de cualquier organización.
- Educación medioambiental: Se harán consideraciones relacionadas con el medioambiente y con acciones que ayuden a preservarlo.
 - Accesibilidad de las personas con discapacidad a las tecnologías de la información
 - Real Decreto Legislativo 1/2013, de 29 de noviembre, por el que se aprueba el Texto Refundido de la Ley General de derechos de las personas con discapacidad y de su inclusión social (BOE nº 289, 3 diciembre 2013)
 - Se considerará el "Diseño para Todos" como criterio general a aplicar en todas las unidades.
- Respeto al material, derecho a la intimidad y a la privacidad. Rechazo a las intrusiones, virus. Cuidado en el uso de los ordenadores y respeto a las normas del aula.
 - LEY ORGÁNICA 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (BOE nº 298, 14 diciembre 1999)
 - REAL DECRETO 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (BOE nº 17, 19 enero 2008)

Código:	Rev.:	Fecha Implantación:	Entregar a:	Página 35 de 36
MD850401	4	15/02/2018	Jefa/e depto. → Jefatura estudios	

8. ACTIVIDADES COMPLEMENTARIAS Y EXTRAESCOLARES

Se denominan actividades complementarias y extraescolares a todas aquellas actividades que se realizan fuera del aula. En la primera categoría se incluyen las organizadas durante el horario escolar por los institutos, mientras que el segundo tipo engloba todas aquellas actividades encaminadas a potenciar la apertura del centro a su entorno favoreciendo la convivencia de todos los sectores de la comunidad educativa y a facilitar la formación integral del alumnado a través del desarrollo de actividades. Las complementarias deben ser tenidas en cuenta en todas las programaciones didácticas y son evaluables. Las extraescolares, en cambio, tendrán carácter voluntario y, en ningún caso, formarán parte del proceso de evaluación del alumnado para la superación de las distintas áreas o materias que integran los currículos.

El departamento de informática colaborará en todas aquellas actividades complementarias y extraescolares que se proponga en el Centro que afecten al alumnado del ciclo formativo. Entre las previstas se incluyen la realización de charlas impartidas por empresas o antiguos alumnos que expliquen tecnologías y metodologías empleadas en el ámbito laboral relacionadas con el ciclo, así como la asistencia a jornadas o congresos relacionados con la informática, aunque debido al momento sanitario en el que nos encontramos, dichas actividades estarán supeditadas al estado de la pandemia y a lo que el departamento decida ateniéndose a las recomendaciones de las entidades sanitarias y del propio centro.

En cualquier caso, el grupo participará en aquellas actividades complementarias y extraescolares propuestas por el departamento que sean de interés para el módulo.

9. BIBLIOGRAFÍA, MATERIALES Y RECURSOS

9.1. Bibliografía de departamento

9.2. Materiales, recursos y laboratorios

El material didáctico utilizado consta de:

- Presentaciones teóricas de cada unidad didáctica en Moodle proporcionados por el profesor
- Relación de prácticas en Moodle proporcionadas por el profesor
- Exámenes de evaluación de cada unidad didáctica en Moodle
- Internet como medio frecuente de búsqueda de información

El libro usado como guía estructural por parte del profesor es “Seguridad informática” de Mac-Graw-Hill

Código:	Rev.:	Fecha Implantación:	Entregar a:	Página 36 de 36
MD850401	4	15/02/2018	Jefa/e depto. → Jefatura estudios	