




 GOBIERNO DE ESPAÑA  MINISTERIO DE EDUCACIÓN, CULTURA Y DEPORTE  JUNTA DE ANDALUCÍA CONSEJERÍA DE EDUCACIÓN  FONDO SOCIAL EUROPEO "El FSE invierte en tu futuro"	PLANIFICACIÓN DOCENTE		IES VIRGEN DEL CARMEN		 IESCA INSTITUTO DE EDUCACIÓN SECUNDARIA "VICENTE YUCRA" 
	PROGRAMACIÓN		Paseo de la Estación nº 44 23008 Jaén Tel. 953366942 – Fax: 953366944 www.iesvirgendelcarmen.com		
	MD850401	Rev. 4	15/02/2018	Página 1 de 31	

MÓDULO:	BASTIONADO DE REDES Y SISTEMAS
CURSO:	2022/2023

DEPARTAMENTO	INFORMÁTICA Y COMUNICACIONES
CURSO DE ESPECIALIZACIÓN EN	CIBERSEGURIDAD EN ENTORNOS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN
PROFESORES	MANUEL JESÚS HIDALGO GALERA

ÍNDICE DE CONTENIDO

1. Objetivos Generales.....	3
2. Metodología.....	8
3. Competencias Profesionales Generales.....	9
4. Evaluación y Recuperación.....	10
4.1. Momentos y procedimientos de Evaluación.....	10
4.2. Criterios de ponderación.....	10
4.3. Criterios de evaluación.....	10
4.4. Criterios de recuperación.....	11
4.5. Evaluación de Competencias Profesionales.....	12
5. Atención a la diversidad.....	13
5.1. Alumnos de admisión tardía.....	13
5.2. Alumnos con necesidades educativas especiales.....	13
5.3. Alumnos con compatibilidad laboral y/o modularidad.....	13
5.4. Alumnado con altas capacidades.....	13
6. Contenidos.....	14
6.1. Relación de bloques temáticos.....	17
6.2. Secuenciación de contenidos.....	22
6.2.0. Unidad didáctica 0: Introducción del módulo.....	22
6.2.1. Unidad didáctica 1: Diseño de planes de securización.....	23
6.2.2. Unidad didáctica 2: Configuración de sistemas de control de acceso y autenticación de personas.....	24
6.2.3. Unidad didáctica 3: Administración de credenciales de acceso a sistemas informáticos.....	25
6.2.4. Unidad didáctica 4: Diseño de redes de computadores seguras.....	26
6.2.5. Unidad didáctica 5: Configuración de dispositivos y sistemas informáticos.....	27
6.2.6. Unidad didáctica 6: Configuración de dispositivos para la instalación de sistemas informáticos.....	28
6.2.7. Unidad didáctica 7: Configuración de los sistemas informáticos.....	29
7. Materias Transversales.....	30
8. Actividades Complementarias y Extraescolares.....	31
9. Bibliografía, Materiales y Recursos.....	32
9.1. Bibliografía de departamento.....	32
9.2. Materiales, recursos y laboratorios.....	32

Código:	Rev.:	Fecha Implantación:	Entregar a:	Página 2 de 31
MD850401	4	15/02/2018	Jefa/e depto. → Jefatura estudios	

1. OBJETIVOS GENERALES

1. Descripción

Este módulo tiene estipulada una duración de 95 horas, que se imparten en el Curso de especialización en ciberseguridad en entornos de las tecnologías de la información.

El módulo se desarrolla durante los tres trimestres, a razón de 7 horas semanales durante unas 23 semanas.

2. Referencia normativa

La normativa que regula tanto este módulo, como el Curso de especialización es:

1. Real Decreto 479/2020, de 7 de abril, por el que se establece el Curso de especialización en ciberseguridad en entornos de las tecnologías de la información y se fijan los aspectos básicos del currículo (BOE nº 134 de 13 de mayo de 2020).

3. Objetivos generales del Curso de especialización

Los objetivos generales de este curso de especialización son los que se indican a continuación, siendo los marcados en negrita los que más contribuye a alcanzar este módulo:

- a) Identificar los principios de la organización y normativa de protección en ciberseguridad, planificando las acciones que es preciso adoptar en el puesto de trabajo para la elaboración del plan de prevención y concienciación.
- b) Auditar el cumplimiento del plan de prevención y concienciación de la organización, definiendo las acciones correctoras que puedan derivarse para incluirlas en el plan de securización de la organización.
- c) Detectar incidentes de ciberseguridad implantando los controles, las herramientas y los mecanismos necesarios para su monitorización e identificación.
- d) Analizar y dar respuesta a incidentes de ciberseguridad, identificando y aplicando las medidas necesarias para su mitigación, eliminación, contención o recuperación.
- e) **Elaborar análisis de riesgos para identificar activos, amenazas, vulnerabilidades y medidas de seguridad.**
- f) **Diseñar e implantar planes de medidas técnicas de seguridad a partir de los riesgos identificados para garantizar el nivel de seguridad requerido.**
- g) **Configurar sistemas de control de acceso, autenticación de personas y administración de credenciales para preservar la privacidad de los datos.**
- h) **Configurar la seguridad de sistemas informáticos para minimizar las probabilidades de exposición a ataques.**
- i) **Configurar dispositivos de red para cumplir con los requisitos de**

Código:	Rev.:	Fecha Implantación:	Entregar a:	Página 3 de 31
MD850401	4	15/02/2018	Jefa/e depto. → Jefatura estudios	

seguridad.

j) Administrar la seguridad de sistemas informáticos en red aplicando las políticas de seguridad requeridas para garantizar la funcionalidad necesaria con el nivel de riesgo de red controlado.

k) Aplicar estándares de verificación requeridos por las aplicaciones para evitar incidentes de seguridad.

l) Automatizar planes de despliegado de software respetando los requisitos relativos a control de versiones, roles, permisos y otros para conseguir un despliegado seguro.

m) Aplicar técnicas de investigación forense en sistemas y redes en los ámbitos del almacenamiento de la información no volátil, de los dispositivos móviles, del Cloud y de los sistemas IoT (Internet de las cosas), entre otros, para la elaboración de análisis forenses.

n) Analizar informes forenses identificando los resultados de la investigación para extraer conclusiones y realizar informes.

ñ) Combinar técnicas de hacking ético interno y externo para detectar vulnerabilidades que permitan eliminar y mitigar los riesgos asociados.

o) Identificar el alcance de la aplicación normativa dentro de la organización, tanto internamente como en relación con terceros para definir las funciones y responsabilidades de todas las partes.

p) Revisar y actualizar procedimientos de acuerdo con normas y estándares actualizados para el correcto cumplimiento normativo en materia de ciberseguridad y de protección de datos personales.

q) Desarrollar manuales de información, utilizando herramientas ofimáticas y de diseño asistido por ordenador para elaborar documentación técnica y administrativa.

r) Analizar y utilizar los recursos y oportunidades de aprendizaje relacionados con la evolución científica, tecnológica y organizativa del sector y las tecnologías de la información y la comunicación, para mantener el espíritu de actualización y adaptarse a nuevas situaciones laborales y personales.

s) Desarrollar la creatividad y el espíritu de innovación para responder a los retos que se presentan en los procesos y en la organización del trabajo y de la vida personal.

t) Evaluar situaciones de prevención de riesgos laborales y de protección ambiental, proponiendo y aplicando medidas de prevención personales y colectivas, de acuerdo con la normativa aplicable en los procesos de trabajo, para garantizar entornos seguros.

u) Identificar y proponer las acciones profesionales necesarias para dar respuesta a la accesibilidad universal y al «diseño para todas las personas».

v) Identificar y aplicar parámetros de calidad en los trabajos y actividades realizados en el proceso de aprendizaje, para valorar la cultura de la evaluación y de la calidad y ser capaces de supervisar y mejorar procedimientos de calidad.

4. Resultados de aprendizaje y criterios de evaluación.

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

En el Real Decreto 479/2020 indicado anteriormente, se indican los siguientes resultados de aprendizaje y criterios de evaluación del presente módulo:

1. Diseña planes de securización incorporando buenas prácticas para el bastionado de sistemas y redes.

Criterios de evaluación:

- a) Se han identificado los activos, las amenazas y vulnerabilidades de la organización.
- b) Se ha evaluado las medidas de seguridad actuales.
- c) Se ha elaborado un análisis de riesgo de la situación actual en ciberseguridad de la organización
- d) Se ha priorizado las medidas técnicas de seguridad a implantar en la organización teniendo también en cuenta los principios de la Economía Circular.
- e) Se ha diseñado y elaborado un plan de medidas técnicas de seguridad a implantar en la organización, apropiadas para garantizar un nivel de seguridad adecuado en función de los riesgos de la organización.
- f) Se han identificado las mejores prácticas en base a estándares, guías y políticas de securización adecuadas para el bastionado de los sistemas y redes de la organización.

2. Configura sistemas de control de acceso y autenticación de personas preservando la confidencialidad y privacidad de los datos.

Criterios de evaluación:

- a) Se han definido los mecanismos de autenticación en base a distintos / múltiples factores (físicos, inherentes y basados en el conocimiento), existentes.
- b) Se han definido protocolos y políticas de autenticación basados en contraseñas y frases de paso, en base a las principales vulnerabilidades y tipos de ataques.
- c) Se han definido protocolos y políticas de autenticación basados en certificados digitales y tarjetas inteligentes, en base a las principales vulnerabilidades y tipos de ataques.
- d) Se han definido protocolos y políticas de autenticación basados en tokens, OTPs, etc., en base a las principales vulnerabilidades y tipos de ataques.
- e) Se han definido protocolos y políticas de autenticación basados en características biométricas, según las principales vulnerabilidades y tipos de ataques.

3. Administra credenciales de acceso a sistemas informáticos aplicando los requisitos de funcionamiento y seguridad establecidos.

Criterios de evaluación:

- a) Se han identificado los tipos de credenciales más utilizados.
- b) Se han generado y utilizado diferentes certificados digitales como medio de acceso a un servidor remoto.
- c) Se ha comprobado la validez y la autenticidad de un certificado digital de un servicio web.
- d) Se han comparado certificados digitales válidos e inválidos por diferentes motivos.
- e) Se ha instalado y configurado un servidor seguro para la administración de credenciales (tipo RADIUS - Remote Access Dial In User Service)

4. Diseña redes de computadores contemplando los requisitos de seguridad.

Criterios de evaluación:

- a) Se ha incrementado el nivel de seguridad de una red local plana segmentándola

Código:	Rev.:	Fecha Implantación:	Entregar a:	Página 5 de 31
MD850401	4	15/02/2018	Jefa/e depto. → Jefatura estudios	

físicamente y utilizando técnicas y dispositivos de enrutamiento.

b) Se ha optimizado una red local plana utilizando técnicas de segmentación lógica (VLANs).

c) Se ha adaptado un segmento de una red local ya operativa utilizando técnicas de subnetting para incrementar su segmentación respetando los direccionamientos existentes.

d) Se han configurado las medidas de seguridad adecuadas en los dispositivos que dan acceso a una red inalámbrica (routers, puntos de acceso, etc.).

e) Se ha establecido un túnel seguro de comunicaciones entre dos sedes geográficamente separadas.

5. Configura dispositivos y sistemas informáticos cumpliendo los requisitos de seguridad.

Criterios de evaluación:

a) Se han configurado dispositivos de seguridad perimetral acorde a una serie de requisitos de seguridad.

b) Se han detectado errores de configuración de dispositivos de red mediante el análisis de tráfico.

c) Se han identificado comportamientos no deseados en una red a través del análisis de los registros (Logs), de un cortafuegos.

d) Se han implementado contramedidas frente a comportamientos no deseados en una red.

e) Se han caracterizado, instalado y configurado diferentes herramientas de monitorización.

6. Configura dispositivos para la instalación de sistemas informáticos minimizando las probabilidades de exposición a ataques.

Criterios de evaluación:

a) Se ha configurado la BIOS para incrementar la seguridad del dispositivo y su contenido minimizando las probabilidades de exposición a ataques.

b) Se ha preparado un sistema informático para su primera instalación teniendo en cuenta las medidas de seguridad necesarias.

c) Se ha configurado un sistema informático para que un actor malicioso no pueda alterar la secuencia de arranque con fines de acceso ilegítimo.

d) Se ha instalado un sistema informático utilizando sus capacidades de cifrado del sistema de ficheros para evitar la extracción física de datos.

e) Se ha particionado el sistema de ficheros del sistema informático para minimizar riesgos de seguridad.

7. Configura sistemas informáticos minimizando las probabilidades de exposición a ataques.

Criterios de evaluación:

a) Se han enumerado y eliminado los programas, servicios y protocolos innecesarios que hayan sido instalados por defecto en el sistema.

b) Se han configurado las características propias del sistema informático para imposibilitar el acceso ilegítimo mediante técnicas de explotación de procesos.

c) Se ha incrementado la seguridad del sistema de administración remoto SSH y otros.

d) Se ha instalado y configurado un Sistema de detección de intrusos en un Host (HIDS) en el sistema informático.

e) Se han instalado y configurado sistemas de copias de seguridad.

Código:	Rev.:	Fecha Implantación:	Entregar a:	Página 6 de 31
MD850401	4	15/02/2018	Jefa/e depto. → Jefatura estudios	

2. METODOLOGÍA

La metodología básica a utilizar será el aprendizaje significativo, el lenguaje utilizado en clase debe ser comprensible por los alumnos, para ello habrá que determinar el dominio del vocabulario informático y el conocimiento de conceptos básicos de ciberseguridad, que, aunque se supone conocidos en este nivel, permita fijar el punto de partida del módulo.

El esquema de trabajo que se seguirá en cada clase será el siguiente:

- Exposición de los contenidos teóricos para cada unidad didáctica.
- Planteamiento de ejercicios prácticos y resolución de los mismos por parte de los alumnos.
- Orientación y resolución de dudas que surjan en la realización de dichos ejercicios.
- Supervisión y corrección del trabajo realizado por los alumnos.

Código:	Rev.:	Fecha Implantación:	Entregar a:	Página 7 de 31
MD850401	4	15/02/2018	Jefa/e depto. → Jefatura estudios	

3. COMPETENCIAS PROFESIONALES GENERALES

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

Las Competencias profesionales, personales y sociales de este curso son las indicadas a continuación; siendo las marcados en negrita las que más contribuye a alcanzar este módulo:

- a) Elaborar e implementar planes de prevención y concienciación en ciberseguridad en la organización, aplicando la normativa vigente.
- b) Detectar e investigar incidentes de ciberseguridad, documentándolos e incluyéndolos en los planes de securización de la organización.
- c) Diseñar planes de securización contemplando las mejores prácticas para el bastionado de sistemas y redes.**
- d) Configurar sistemas de control de acceso y autenticación en sistemas informáticos, cumpliendo los requisitos de seguridad y minimizando las posibilidades de exposición a ataques.**
- e) Diseñar y administrar sistemas informáticos en red y aplicar las políticas de seguridad establecidas, garantizando la funcionalidad requerida con un nivel de riesgo controlado.**
- f) Analizar el nivel de seguridad requerido por las aplicaciones y los vectores de ataque más habituales, evitando incidentes de ciberseguridad.
- g) Implantar sistemas seguros de despliegado de software con la adecuada coordinación entre los desarrolladores y los responsables de la operación del software.
- h) Realizar análisis forenses informáticos analizando y registrando la información relevante relacionada.
- i) Detectar vulnerabilidades en sistemas, redes y aplicaciones, evaluando los riesgos asociados.
- j) Definir y aplicar procedimientos para el cumplimiento normativo en materia de ciberseguridad y de protección de datos personales, implementándolos tanto internamente como en relación con terceros.
- k) Elaborar documentación técnica y administrativa cumpliendo con la legislación vigente, respondiendo a los requisitos establecidos.**
- l) Adaptarse a las nuevas situaciones laborales, manteniendo actualizados los conocimientos científicos, técnicos y tecnológicos relativos a su entorno profesional, gestionando su formación y los recursos existentes en el aprendizaje a lo largo de la vida.**
- m) Resolver situaciones, problemas o contingencias con iniciativa y autonomía en el ámbito de su competencia, con creatividad, innovación y espíritu de mejora en el trabajo personal y en el de los miembros del equipo.**
- n) Generar entornos seguros en el desarrollo de su trabajo y el de su equipo, supervisando y aplicando los procedimientos de prevención de riesgos laborales y ambientales, de acuerdo con lo establecido por la normativa y los objetivos de la organización.**
- ñ) Supervisar y aplicar procedimientos de gestión de calidad, de accesibilidad universal y de «diseño para todas las personas», en las actividades profesionales incluidas en los procesos de producción o prestación de servicios.**

Código:	Rev.:	Fecha Implantación:	Entregar a:	Página 8 de 31
MD850401	4	15/02/2018	Jefa/e depto. → Jefatura estudios	

4. EVALUACIÓN Y RECUPERACIÓN

4.1. Momentos y procedimientos de Evaluación

Procedimientos de evaluación, podemos distinguir los siguientes:

- Observación diaria del trabajo y progreso del alumnado
- Revisión de las tareas y ejercicios encomendados
- Pruebas de evaluación

Para la superación del módulo, los alumnos deberán de obtener una calificación superior o igual a 5 en todos y cada uno de los RA evaluados.

Para recuperar, deberán repetir/presentar las pruebas/actividades necesarias para alcanzar la calificación indicada en el párrafo anterior

Para el periodo de recuperación de junio, el profesor determinará para cada alumno, de forma personalizada las pruebas/actividades a realizar/presentar, que podrán ser de partes de evaluaciones, de evaluaciones completas o de todo el módulo.

Para el periodo de mejora, se propondrá al alumnado la realización de varios cursos en la plataforma OpenWebinars, Amazon Web Services, etc. y/o la superación de pruebas adicionales que pueden permitir al alumnado subir hasta 1 punto en la nota final del módulo.

4.2. Criterios de ponderación

Cada ítem evaluable se asocia a un criterio de evaluación. El peso de cada criterio de evaluación será proporcional al número de ítems asociados a dicho criterio de evaluación a lo largo del curso, ponderado teniendo en cuenta que el peso de cada evaluación es $\frac{1}{3}$ sobre la nota final.

4.3. Criterios de evaluación

Criterios de Calificación		
Criterio (marcar con una X debajo de SI o NO)	SI	NO
La ortografía resta puntuación (en caso afirmativo explicar los criterios)		X
Entregar fuera de plazo resta puntuación (en caso afirmativo explicar debajo los criterios)		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) Aprobar todos los RAs	X	

Código:	Rev.:	Fecha Implantación:	Entregar a:	Página 9 de 31
MD850401	4	15/02/2018	Jefa/e depto. → Jefatura estudios	

Criterios de Calificación		
Criterio (marcar con una X debajo de SI o NO)	SI	NO
Los alumnos/as deben superar todas las evaluaciones para aprobar el módulo (si procede, determinar qué evaluaciones debe superar el alumnado para obtener las competencias mínimas)		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
La NO entrega de ejercicios de clase supone directamente que esa parte se recupera con examen (en caso afirmativo explicar los criterios)		X

4.4. Criterios de recuperación

Criterios de recuperación		
Criterio (marcar con una X debajo de SI o NO)	SI	NO
La calificación final será la misma que la del examen (en caso negativo, explicar las diferencias). La calificación final se obtiene realizando la media entre todas las notas de las pruebas, actividades, prácticas, ... obtenidas y superadas durante el curso, incluyendo como tal la que se obtiene en la prueba, actividad, práctica, ... de recuperación de la parte no superada.		X
Puede eliminar materia previamente al examen	X	
Existen criterios de corrección diferentes entre convocatoria ordinaria y extraordinaria (explicar en caso afirmativo las diferencias)		X
Existe una nota máxima en la recuperación independientemente de la calificación que se obtenga en la misma		X
Otros (a completar):		

Código:	Rev.:	Fecha Implantación:	Entregar a:	Página 10 de 31
MD850401	4	15/02/2018	Jefa/e depto. → Jefatura estudios	

4.5. Evaluación de Competencias Profesionales

Las competencias profesionales que se evalúan en este módulo, de entre las indicadas en el Real Decreto 479/2020, de 7 de abril (BOE nº 134 de 13 de mayo de 2020), son las siguientes:

- c) Diseñar planes de securización contemplando las mejores prácticas para el bastionado de sistemas y redes.
- d) Configurar sistemas de control de acceso y autenticación en sistemas informáticos, cumpliendo los requisitos de seguridad y minimizando las posibilidades de exposición a ataques.
- e) Diseñar y administrar sistemas informáticos en red y aplicar las políticas de seguridad establecidas, garantizando la funcionalidad requerida con un nivel de riesgo controlado.
- k) Elaborar documentación técnica y administrativa cumpliendo con la legislación vigente, respondiendo a los requisitos establecidos.
- m) Resolver situaciones, problemas o contingencias con iniciativa y autonomía en el ámbito de su competencia, con creatividad, innovación y espíritu de mejora en el trabajo personal y en el de los miembros del equipo.
- n) Generar entornos seguros en el desarrollo de su trabajo y el de su equipo, supervisando y aplicando los procedimientos de prevención de riesgos laborales y ambientales, de acuerdo con lo establecido por la normativa y los objetivos de la organización.
- ñ) Supervisar y aplicar procedimientos de gestión de calidad, de accesibilidad universal y de «diseño para todas las personas», en las actividades profesionales incluidas en los procesos de producción o prestación de servicios.

Código:	Rev.:	Fecha Implantación:	Entregar a:	Página 11 de 31
MD850401	4	15/02/2018	Jefa/e depto. → Jefatura estudios	

5. ATENCIÓN A LA DIVERSIDAD

5.1. Alumnos de admisión tardía

Los alumnos que se incorporen una vez iniciado el curso escolar, tendrán que repasar en su casa el temario ya impartido, debiendo realizar también en su casa las actividades y prácticas ya realizadas. No obstante se atenderán en clase las cuestiones planteadas, relativas a dicho temario.

En caso de no haber asistido a pruebas, se presentarán a las recuperaciones establecidas de forma general.

5.2. Alumnos con necesidades educativas especiales

Se aplicarán las medidas que estén a nuestro alcance, para que el alumno pueda acceder de forma adecuada al currículo.

5.3. Alumnos con compatibilidad laboral y/o modularidad

Los alumnos que puedan compatibilizar sus actividades laborales con este módulo, deberán de asistir con regularidad a clase y realizar las actividades en casa, que hayan hecho sus compañeros en clase. No obstante, se tendrá en cuenta su situación a la hora de consultar dudas sobre el contenido del temario.

5.4. Alumnado con altas capacidades

Los alumnos con altas capacidades podrán realizar actividades adicionales para ampliar sus capacidades profesionales.

Así mismo, aquellos alumnos que muestran conocimientos avanzados en diversas áreas del presente módulo se les permitirá ayudar a los compañeros para fomentar su autoestima, a la vez que la cohesión y buen ambiente de trabajo, que, a su vez, mejora las competencias de trabajo en grupo.

Código:	Rev.:	Fecha Implantación:	Entregar a:	Página 12 de 31
MD850401	4	15/02/2018	Jefa/e depto. → Jefatura estudios	

6. CONTENIDOS

El Real Decreto 479/2020, de 7 de abril (BOE nº 134 de 13 de mayo de 2020), que desarrolla el currículo del presente curso de especialización, establece los siguientes contenidos básicos:

- Diseño de planes de securización:
 - Análisis de riesgos.
 - Principios de la Economía Circular en la Industria 4.0.
 - Plan de medidas técnicas de seguridad.
 - Políticas de securización más habituales.
 - Guías de buenas prácticas para la securización de sistemas y redes.
 - Estándares de securización de sistemas y redes.
 - Caracterización de procedimientos, instrucciones y recomendaciones.
 - Niveles, escalados y protocolos de atención a incidencias.
- Configuración de sistemas de control de acceso y autenticación de personas:
 - Mecanismos de autenticación. Tipos de factores.
 - Autenticación basada en distintas técnicas:
- Administración de credenciales de acceso a sistemas informáticos:
 - Gestión de credenciales.
 - Infraestructuras de Clave Pública (PKI).
 - Acceso por medio de Firma electrónica.
 - Gestión de accesos. Sistemas NAC (Network Access Control, Sistemas de Gestión de Acceso a la Red).
 - Gestión de cuentas privilegiadas.
 - Protocolos RADIUS y TACACS, servicio KERBEROS, entre otros.
- Diseño de redes de computadores seguras:
 - Segmentación de redes:
 - Subnetting.
 - Redes virtuales (VLANs).
 - Zona desmilitarizada (DMZ).
 - Seguridad en redes inalámbricas (WPA2, WPA3, etc.).
 - Protocolos de red seguros (IPSec, etc.).
- Configuración de dispositivos y sistemas informáticos:
 - Seguridad perimetral. Firewalls de Próxima Generación.
 - Seguridad de portales y aplicativos web. Soluciones WAF (Web Application Firewall).
 - Seguridad del puesto de trabajo y endpoint fijo y móvil. AntiAPT, antimalware.
 - Seguridad de entornos cloud. Soluciones CASB.
 - Seguridad del correo electrónico
 - Soluciones DLP (Data Loss Prevention)
 - Herramientas de almacenamiento de logs.
 - Protección ante ataques de denegación de servicio distribuido (DDoS).
 - Configuración segura de cortafuegos, enrutadores y proxies.

Código:	Rev.:	Fecha Implantación:	Entregar a:	Página 13 de 31
MD850401	4	15/02/2018	Jefa/e depto. → Jefatura estudios	

- Redes privadas virtuales (VPNs), y túneles (protocolo IPSec).
 - Monitorización de sistemas y dispositivos.
 - Herramientas de monitorización (IDS, IPS).
 - SIEMs (Gestores de Eventos e Información de Seguridad).
 - Soluciones de Centros de Operación de Red, y Centros de Seguridad de Red: NOCs y SOCs.
- Configuración de dispositivos para la instalación de sistemas informáticos:
 - Precauciones previas a la instalación de un sistema informático: aislamiento, configuración del control de acceso a la BIOS, bloqueo del orden de arranque de los dispositivos, entre otros.
 - Seguridad en el arranque del sistema informático, configuración del arranque seguro.
 - Seguridad de los sistemas de ficheros, cifrado, particionado, entre otros.
- Configuración de los sistemas informáticos:
 - Reducción del número de servicios, Telnet, RSSH, TFTP, entre otros.
 - Hardening de procesos (eliminación de información de depuración en caso de errores, aleatorización de la memoria virtual para evitar exploits, etc.).
 - Eliminación de protocolos de red innecesarios (ICMP, entre otros).
 - Securización de los sistemas de administración remota.
 - Sistemas de prevención y protección frente a virus e intrusiones (antivirus, HIDS, etc.).
 - Configuración de actualizaciones y parches automáticos.
 - Sistemas de copias de seguridad.
 - Shadow IT y políticas de seguridad en entornos SaaS.

Código:	Rev.:	Fecha Implantación:	Entregar a:	Página 14 de 31
MD850401	4	15/02/2018	Jefa/e depto. → Jefatura estudios	

CALENDARIO ESCOLAR. CURSO 2022-2023

IES VIRGEN DEL CARMEN DE JAÉN

SEPTIEMBRE							OCTUBRE							NOVIEMBRE						
			1	2	3	4						1	2		1	2	3	4	5	6
5	6	7	8	9	10	11	3	4	5	6	7	8	9	7	8	9	10	11	12	13
12	13	14	15	16	17	18	10	11	12	13	14	15	16	14	15	16	17	18	19	20
19	20	21	22	23	24	25	17	18	19	20	21	22	23	21	22	23	24	25	26	27
26	27	28	29	30			24	25	26	27	28	29	30	28	29	30				
							31													
DICIEMBRE							ENERO							FEBRERO						
			1	2	3	4							1			1	2	3	4	5
5	6	7	8	9	10	11	2	3	4	5	6	7	8	6	7	8	9	10	11	12
12	13	14	15	16	17	18	9	10	11	12	13	14	15	13	14	15	16	17	18	19
19	20	21	22	23	24	25	16	17	18	19	20	21	22	20	21	22	23	24	25	26
26	27	28	29	30	31		23	24	25	26	27	28	29	27	28					
							30	31												
MARZO							ABRIL							MAYO						
		1	2	3	4	5						1	2	1	2	3	4	5	6	7
6	7	8	9	10	11	12	3	4	5	6	7	8	9	8	9	10	11	12	13	14
13	14	15	16	17	18	19	10	11	12	13	14	15	16	15	16	17	18	19	20	21
20	21	22	23	24	25	26	17	18	19	20	21	22	23	22	23	24	25	26	27	28
27	28	29	30	31			24	25	26	27	28	29	30	29	30	31				
JUNIO							JULIO							AGOSTO						
			1	2	3	4						1	2		1	2	3	4	5	6
5	6	7	8	9	10	11	3	4	5	6	7	8	9	7	8	9	10	11	12	13
12	13	14	15	16	17	18	10	11	12	13	14	15	16	14	15	16	17	18	19	20
19	20	21	22	23	24	25	17	18	19	20	21	22	23	21	22	23	24	25	26	27
26	27	28	29	30			24	25	26	27	28	29	30	28	29	30	31			
							31													

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

Los contenidos del módulo se agrupan en las unidades didácticas que junto a los criterios de evaluación se detallan a continuación.

El Real Decreto 479/2020, de 7 de abril (BOE nº 134 de 13 de mayo de 2020), establece una duración mínima de **95** horas lectivas para este módulo. Debido a la distribución horaria semanal del módulo (5h/sem) y a la ubicación de los días no lectivos, el número total de horas lectivas que dispone el módulo durante el presente curso escolar es de **145** horas; distribuidas en evaluaciones según los meses de la siguiente manera:

1ª Evaluación			2ª Evaluación			3ª Evaluación		Total
Oct.	Nov.	Dic.	Ene.	Feb.	Mar.	Abr.	May.	
21	20	19	20	15	20	15	20	
60			55			35		145

6.1. Relación de bloques temáticos

Bloque Temático 1	Nº U.D.	Título Unidad Didáctica	Horas (según calendario)	Evaluación (marcar)		
				1º	2º	3º
Planes de seguridad	0	Introducción al módulo.	2	x		
	1	Diseño de planes de securización	23			x

Bloque Temático 2	Nº U.D.	Título Unidad Didáctica	Horas (según calendario)	Evaluación (marcar)		
				1º	2º	3º
Autenticación	2	Configuración de sistemas de control de acceso y autenticación de personas	7			x
	3	Administración de credenciales de acceso a sistemas informáticos	19	x		

Bloque Temático 3	Nº U.D.	Título Unidad Didáctica	Horas (según calendario)	Evaluación (marcar)		
				1º	2º	3º
Securización de redes	4	Diseño de redes de computadores seguras	19	x		
	5	Configuración de dispositivos y sistemas informáticos	40		x	

Código:	Rev.:	Fecha Implantación:	Entregar a:	Página 16 de 31
MD850401	4	15/02/2018	Jefa/e depto. → Jefatura estudios	

Bloque Temático 4	Nº U.D.	Título Unidad Didáctica	Horas (según calendario)	Evaluación (marcar)		
				1º	2º	3º
Securización de sistemas	6	Configuración de dispositivos para la instalación de sistemas informáticos	12		x	
	7	Configuración de los sistemas informáticos	23		x	

Código:	Rev.:	Fecha Implantación:	Entregar a:	Página 17 de 31
MD850401	4	15/02/2018	Jefa/e depto. → Jefatura estudios	

Resultado de aprendizaje	Criterios Evaluación
RA1: Diseña planes de securización incorporando buenas prácticas para el bastionado de sistemas y redes.	a) Se han identificado los activos, las amenazas y vulnerabilidades de la organización.
	b) Se ha evaluado las medidas de seguridad actuales.
	c) Se ha elaborado un análisis de riesgo de la situación actual en ciberseguridad de la organización.
	d) Se ha priorizado las medidas técnicas de seguridad a implantar en la organización teniendo también en cuenta los principios de la Economía Circular.
	e) Se ha diseñado y elaborado un plan de medidas técnicas de seguridad a implantar en la organización, apropiadas para garantizar un nivel de seguridad adecuado en función de los riesgos de la organización.
	f) Se han identificado las mejores prácticas en base a estándares, guías y políticas de securización adecuadas para el bastionado de los sistemas y redes de la organización.
RA2: Configura sistemas de control de acceso y autenticación de personas preservando la confidencialidad y privacidad de los datos.	a) Se han definido los mecanismos de autenticación en base a distintos / múltiples factores (físicos, inherentes y basados en el conocimiento), existentes.
	b) Se han definido protocolos y políticas de autenticación basados en contraseñas y frases de paso, en base a las principales vulnerabilidades y tipos de ataques.
	c) Se han definido protocolos y políticas de autenticación basados en certificados digitales y tarjetas inteligentes, en base a las principales vulnerabilidades y tipos de ataques.
	d) Se han definido protocolos y políticas de autenticación basados en tokens, OTPs, etc., en base a las principales vulnerabilidades y tipos de ataques.
	e) Se han definido protocolos y políticas de autenticación basados en características biométricas, según las principales vulnerabilidades y tipos de ataques.
RA3: Administra credenciales de acceso a sistemas informáticos aplicando los requisitos de funcionamiento y seguridad establecidos.	a) Se han identificado los tipos de credenciales más utilizados.
	b) Se han generado y utilizado diferentes certificados digitales como medio de acceso a un servidor remoto.
	c) Se ha comprobado la validez y la autenticidad de un certificado digital de un servicio web.
	d) Se han comparado certificados digitales válidos e inválidos por diferentes motivos.
	e) Se ha instalado y configurado un servidor seguro para la administración de credenciales (tipo RADIUS - Remote Access Dial In User Service)
RA4: Diseña redes de computadores	a) Se ha incrementado el nivel de seguridad de una red local plana segmentándola físicamente y utilizando técnicas y dispositivos de enrutamiento.

Código:	Rev.:	Fecha Implantación:	Entregar a:	Página 18 de 31
MD850401	4	15/02/2018	Jefa/e depto. → Jefatura estudios	

contemplando los requisitos de seguridad.	b) Se ha optimizado una red local plana utilizando técnicas de segmentación lógica (VLANs).
	c) Se ha adaptado un segmento de una red local ya operativa utilizando técnicas de subnetting para incrementar su segmentación respetando los direccionamientos existentes.
	d) Se han configurado las medidas de seguridad adecuadas en los dispositivos que dan acceso a una red inalámbrica (routers, puntos de acceso, etc.).
	e) Se ha establecido un túnel seguro de comunicaciones entre dos sedes geográficamente separadas.
RA5: Configura dispositivos y sistemas informáticos cumpliendo los requisitos de seguridad.	a) Se han configurado dispositivos de seguridad perimetral acorde a una serie de requisitos de seguridad.
	b) Se han detectado errores de configuración de dispositivos de red mediante el análisis de tráfico.
	c) Se han identificado comportamientos no deseados en una red a través del análisis de los registros (Logs), de un cortafuegos.
	d) Se han implementado contramedidas frente a comportamientos no deseados en una red.
	e) Se han caracterizado, instalado y configurado diferentes herramientas de monitorización.
RA6: Configura dispositivos para la instalación de sistemas informáticos minimizando las probabilidades de exposición a ataques.	a) Se ha configurado la BIOS para incrementar la seguridad del dispositivo y su contenido minimizando las probabilidades de exposición a ataques.
	b) Se ha preparado un sistema informático para su primera instalación teniendo en cuenta las medidas de seguridad necesarias.
	c) Se ha configurado un sistema informático para que un actor malicioso no pueda alterar la secuencia de arranque con fines de acceso ilegítimo.
	d) Se ha instalado un sistema informático utilizando sus capacidades de cifrado del sistema de ficheros para evitar la extracción física de datos.
	e) Se ha particionado el sistema de ficheros del sistema informático para minimizar riesgos de seguridad.
RA7: Configura sistemas informáticos minimizando las probabilidades de exposición a	a) Se han enumerado y eliminado los programas, servicios y protocolos innecesarios que hayan sido instalados por defecto en el sistema.
	b) Se han configurado las características propias del sistema informático para imposibilitar el acceso ilegítimo mediante técnicas de explotación de procesos.
	c) Se ha incrementado la seguridad del sistema de administración remoto SSH y otros.
	d) Se ha instalado y configurado un Sistema de detección de intrusos en un Host (HIDS) en el sistema informático.
	e) Se han instalado y configurado sistemas de copias de seguridad.

Código:	Rev.:	Fecha Implantación:	Entregar a:	Página 19 de 31
MD850401	4	15/02/2018	Jefa/e depto. → Jefatura estudios	

Reparto de los criterios de evaluación según las distintas unidades didácticas

	Criterio de evaluación					
	a)	b)	c)	d)	e)	f)
RA1	1	1	1	1	1	1
RA2	2	2	2	2	2	-
RA3	3	3	3	3	3	-
RA4	4	4	4	4	4	-
RA5	5	5	5	5	5	-
RA6	6	6	6	6	6	-
RA7	7	7	7	7	7	-

Código:	Rev.:	Fecha Implantación:	Entregar a:	Página 20 de 31
MD850401	4	15/02/2018	Jefa/e depto. → Jefatura estudios	

6.2. Secuenciación de contenidos

6.2.0. Unidad didáctica 0: Introducción del módulo.

0.a. Objetivos Didácticos

Conocer los objetivos del módulo, temario, exámenes y demás aspectos.

0.b. Contenidos Conceptuales

Objetivos del módulo.

Bloques temáticos.

0.c. Contenidos Procedimentales

Proceso de evaluación.

0.d. Contenidos Actitudinales

Trabajar asiduamente.

Consultar las dudas.

0.e. Criterios de Evaluación

Código:	Rev.:	Fecha Implantación:	Entregar a:	Página 21 de 31
MD850401	4	15/02/2018	Jefa/e depto. → Jefatura estudios	

6.2.1. Unidad didáctica 1: Diseño de planes de securización.

1.a. Objetivos Didácticos

Conocer los elementos integrantes de un Plan de seguridad
Aplicar metodologías para el análisis de riesgos
Conocer los documentos asociados a las políticas de seguridad
Conocer el proceso de atención a incidencias

1.b. Contenidos Conceptuales

Análisis de riesgos.
Principios de la Economía Circular en la Industria 4.0.
Plan de medidas técnicas de seguridad.
Políticas de securización más habituales.
Guías de buenas prácticas para la securización de sistemas y redes.
Estándares de securización de sistemas y redes.
Caracterización de procedimientos, instrucciones y recomendaciones.
Niveles, escalados y protocolos de atención a incidencias.

1.c. Contenidos Procedimentales

Identificar los activos, las amenazas y vulnerabilidades de la organización.
Evaluar las medidas de seguridad.
Elaborar un análisis de riesgo.
Priorizar las medidas técnicas de seguridad a implantar.
Diseñar y elaborar un plan de medidas técnicas de seguridad.
Identificado las mejores prácticas para el bastionado de los sistemas y redes.

1.d. Contenidos Actitudinales

Tener interés en la mejora de conocimientos relativos a esta unidad didáctica.
Tener predisposición para trabajar utilizando la plataforma Moodle.
Tener predisposición para trabajar utilizando máquinas virtuales.
Tener predisposición para trabajar bajo la interfaz de línea de comandos.
Valorar los distintos ejemplos presentados en la unidad didáctica.
Valorar las distintas herramientas presentadas en esta unidad didáctica.
Mostrar actitud de aplicar medidas de seguridad presentadas en esta unidad didáctica
Mostrar voluntad de ayudar a los demás.
Presentar disposición de trabajo en equipo.
Respetar las opiniones manifestadas libremente por los compañeros.

1.e. Criterios de Evaluación

Los indicados en el "Reparto de los criterios de evaluación".

Código:	Rev.:	Fecha Implantación:	Entregar a:	Página 22 de 31
MD850401	4	15/02/2018	Jefa/e depto. → Jefatura estudios	

6.2.2. Unidad didáctica 2: Configuración de sistemas de control de acceso y autenticación de personas.

2.a. Objetivos Didácticos

Conocer diversos mecanismos de autenticación
Definir protocolos y políticas de autenticación

2.b. Contenidos Conceptuales

Mecanismos de autenticación. Tipos de factores.
Autenticación basada en distintas técnicas.

2.c. Contenidos Procedimentales

Definir los mecanismos de autenticación en base a distintos / múltiples factores.
Definir protocolos y políticas de autenticación basados en contraseñas y frases de paso.
Definir protocolos y políticas de autenticación basados en certificados digitales y tarjetas inteligentes.
Definir protocolos y políticas de autenticación basados en tokens, OTPs, etc..
Definir protocolos y políticas de autenticación basados en características biométricas.

2.d. Contenidos Actitudinales

Tener interés en la mejora de conocimientos relativos a esta unidad didáctica.
Tener predisposición para trabajar utilizando la plataforma Moodle.
Tener predisposición para trabajar utilizando máquinas virtuales.
Tener predisposición para trabajar bajo la interfaz de línea de comandos.
Valorar los distintos ejemplos presentados en la unidad didáctica.
Valorar las distintas herramientas presentadas en esta unidad didáctica.
Mostrar actitud de aplicar medidas de seguridad presentadas en esta unidad didáctica
Mostrar voluntad de ayudar a los demás.
Presentar disposición de trabajo en equipo.
Respetar las opiniones manifestadas libremente por los compañeros.

2.e. Criterios de Evaluación

Los indicados en el "Reparto de los criterios de evaluación".

Código:	Rev.:	Fecha Implantación:	Entregar a:	Página 23 de 31
MD850401	4	15/02/2018	Jefa/e depto. → Jefatura estudios	

6.2.3. Unidad didáctica 3: Administración de credenciales de acceso a sistemas informáticos.

3.a. Objetivos Didácticos

Conocer mecanismos para la gestión de credenciales

Aplicar mecanismos de autenticación de dispositivos y usuarios

3.b. Contenidos Conceptuales

Gestión de credenciales.

Infraestructuras de Clave Pública (PKI).

Acceso por medio de Firma electrónica.

Gestión de accesos. Sistemas NAC (Network Access Control, Sistemas de Gestión de Acceso a la Red).

Gestión de cuentas privilegiadas.

Protocolos RADIUS y TACACS, servicio KERBEROS, entre otros.

3.c. Contenidos Procedimentales

Identificar los tipos de credenciales.

Generar y utilizar diferentes certificados digitales como medio de acceso a un servidor remoto.

Comprobar la validez y la autenticidad de un certificado digital de un servicio web.

Comparar certificados digitales válidos e inválidos por diferentes motivos.

Instalar y configurar un servidor seguro para la administración de credenciales tipo RADIUS.

3.d. Contenidos Actitudinales

Tener interés en la mejora de conocimientos relativos a esta unidad didáctica.

Tener predisposición para trabajar utilizando la plataforma Moodle.

Tener predisposición para trabajar utilizando máquinas virtuales.

Tener predisposición para trabajar bajo la interfaz de línea de comandos.

Valorar los distintos ejemplos presentados en la unidad didáctica.

Valorar las distintas herramientas presentadas en esta unidad didáctica.

Mostrar actitud de aplicar medidas de seguridad presentadas en esta unidad didáctica

Mostrar voluntad de ayudar a los demás.

Presentar disposición de trabajo en equipo.

Respetar las opiniones manifestadas libremente por los compañeros.

3.e. Criterios de Evaluación

Los indicados en el "Reparto de los criterios de evaluación".

Código:	Rev.:	Fecha Implantación:	Entregar a:	Página 24 de 31
MD850401	4	15/02/2018	Jefa/e depto. → Jefatura estudios	

6.2.4. Unidad didáctica 4: Diseño de redes de computadores seguras.

4.a. Objetivos Didácticos

Conocer los mecanismos para mejorar la seguridad en las redes locales.

Aplicar metodologías para la mejora de la seguridad en las redes locales cableadas e inalámbricas.

4.b. Contenidos Conceptuales

Segmentación de redes

Subnetting.

Redes virtuales (VLANs).

Zona desmilitarizada (DMZ).

Seguridad en redes inalámbricas (WPA2, WPA3, etc.).

Protocolos de red seguros (IPSec, etc.).

4.c. Contenidos Procedimentales

Segmentar una red local plana físicamente, incluyendo enrutamiento.

Segmentar una red local plana utilizando técnicas de segmentación lógica (VLANs).

Adaptar un segmento de una red local ya operativa utilizando técnicas de subnetting para incrementar su segmentación.

Configurar medidas de seguridad en los dispositivos que dan acceso a una red inalámbrica (routers, puntos de acceso, etc.).

Establecer un túnel seguro de comunicaciones entre dos sedes separadas.

4.d. Contenidos Actitudinales

Tener interés en la mejora de conocimientos relativos a esta unidad didáctica.

Tener predisposición para trabajar utilizando la plataforma Moodle.

Tener predisposición para trabajar utilizando máquinas virtuales.

Tener predisposición para trabajar bajo la interfaz de línea de comandos.

Valorar los distintos ejemplos presentados en la unidad didáctica.

Valorar las distintas herramientas presentadas en esta unidad didáctica.

Mostrar actitud de aplicar medidas de seguridad presentadas en esta unidad didáctica

Mostrar voluntad de ayudar a los demás.

Presentar disposición de trabajo en equipo.

Respetar las opiniones manifestadas libremente por los compañeros.

4.e. Criterios de Evaluación

Los indicados en el "Reparto de los criterios de evaluación".

Código:	Rev.:	Fecha Implantación:	Entregar a:	Página 25 de 31
MD850401	4	15/02/2018	Jefa/e depto. → Jefatura estudios	

6.2.5. Unidad didáctica 5: Configuración de dispositivos y sistemas informáticos.

5.a. Objetivos Didácticos

Aplicar mecanismos de hardening de redes, sistemas y servicios.

Conocer la problemática asociada al uso de la nube.

Valorar la importancia de los datos de carácter personal que gestiona una organización.

Establecer túneles seguros.

Conocer herramientas avanzadas de análisis de tráfico.

5.b. Contenidos Conceptuales

Seguridad perimetral. Firewalls de Próxima Generación.

Seguridad de portales y aplicativos web. Soluciones WAF (Web Application Firewall).

Seguridad del puesto de trabajo y endpoint fijo y móvil. AntiAPT, antimalware.

Seguridad de entornos cloud. Soluciones CASB.

Seguridad del correo electrónico

Soluciones DLP (Data Loss Prevention)

Herramientas de almacenamiento de logs.

Protección ante ataques de denegación de servicio distribuido (DDoS).

Configuración segura de cortafuegos, enrutadores y proxies.

Redes privadas virtuales (VPNs), y túneles (protocolo IPSec).

Monitorización de sistemas y dispositivos.

Herramientas de monitorización (IDS, IPS).

SIEMs (Gestores de Eventos e Información de Seguridad).

Soluciones de Centros de Operación de Red, y Centros de Seguridad de Red: NOCs y SOCs.

5.c. Contenidos Procedimentales

Configurar dispositivos de seguridad perimetral.

Detectar errores de configuración de dispositivos de red mediante el análisis de tráfico.

Identificar comportamientos no deseados en una red a través del análisis de los registros (Logs), de un cortafuegos.

Implementar contramedidas frente a comportamientos no deseados en una red.

Caracterizar, instalar y configurar diferentes herramientas de monitorización.

5.d. Contenidos Actitudinales

Tener interés en la mejora de conocimientos relativos a esta unidad didáctica.

Tener predisposición para trabajar utilizando la plataforma Moodle.

Tener predisposición para trabajar utilizando máquinas virtuales.

Tener predisposición para trabajar bajo la interfaz de línea de comandos.

Valorar los distintos ejemplos presentados en la unidad didáctica.

Valorar las distintas herramientas presentadas en esta unidad didáctica.

Mostrar actitud de aplicar medidas de seguridad presentadas en esta unidad didáctica

Mostrar voluntad de ayudar a los demás.

Presentar disposición de trabajo en equipo.

Respetar las opiniones manifestadas libremente por los compañeros.

5.e. Criterios de Evaluación

Los indicados en el "Reparto de los criterios de evaluación".

Código:	Rev.:	Fecha Implantación:	Entregar a:	Página 26 de 31
MD850401	4	15/02/2018	Jefa/e depto. → Jefatura estudios	

6.2.6. Unidad didáctica 6: Configuración de dispositivos para la instalación de sistemas informáticos.

6.a. Objetivos Didácticos

Aplicar mecanismos de seguridad en ordenadores personales y servidores usados en las empresas.

6.b. Contenidos Conceptuales

Precauciones previas a la instalación de un sistema informático: aislamiento, configuración del control de acceso a la BIOS, bloqueo del orden de arranque de los dispositivos, entre otros.

Seguridad en el arranque del sistema informático, configuración del arranque seguro.

Seguridad de los sistemas de ficheros, cifrado, particionado, entre otros.

6.c. Contenidos Procedimentales

Configurar la BIOS para incrementar la seguridad del dispositivo.

Preparar un sistema informático para su primera instalación teniendo en cuenta las medidas de seguridad.

Configurar un sistema informático para que un actor malicioso no pueda alterar la secuencia de arranque.

Instalar un sistema informático utilizando sus capacidades de cifrado del sistema de ficheros.

Particionar el sistema de ficheros del sistema informático para minimizar riesgos.

6.d. Contenidos Actitudinales

Tener interés en la mejora de conocimientos relativos a esta unidad didáctica.

Tener predisposición para trabajar utilizando la plataforma Moodle.

Tener predisposición para trabajar utilizando máquinas virtuales.

Tener predisposición para trabajar bajo la interfaz de línea de comandos.

Valorar los distintos ejemplos presentados en la unidad didáctica.

Valorar las distintas herramientas presentadas en esta unidad didáctica.

Mostrar actitud de aplicar medidas de seguridad presentadas en esta unidad didáctica

Mostrar voluntad de ayudar a los demás.

Presentar disposición de trabajo en equipo.

Respetar las opiniones manifestadas libremente por los compañeros.

6.e. Criterios de Evaluación

Los indicados en el "Reparto de los criterios de evaluación".

Código:	Rev.:	Fecha Implantación:	Entregar a:	Página 27 de 31
MD850401	4	15/02/2018	Jefa/e depto. → Jefatura estudios	

6.2.7. Unidad didáctica 7: Configuración de los sistemas informáticos.

7.a. Objetivos Didácticos

Reducir el número de vulnerabilidades en un equipo y de sus servicios.

Valorar la importancia de las copias de seguridad

7.b. Contenidos Conceptuales

Reducción del número de servicios, Telnet, RSSH, TFTP, entre otros.

Hardening de procesos (eliminación de información de depuración en caso de errores, aleatorización de la memoria virtual para evitar exploits, etc.).

Eliminación de protocolos de red innecesarios (ICMP, entre otros).

Securización de los sistemas de administración remota.

Sistemas de prevención y protección frente a virus e intrusiones (antivirus, HIDS, etc.).

Configuración de actualizaciones y parches automáticos.

Sistemas de copias de seguridad.

Shadow IT y políticas de seguridad en entornos SaaS.

7.c. Contenidos Procedimentales

Enumerar y eliminar programas, servicios y protocolos innecesarios que hayan sido instalados por defecto.

Configurar las características propias del sistema informático para imposibilitar el acceso ilegítimo mediante técnicas de explotación de procesos.

Incrementar la seguridad del sistema de administración remoto SSH y otros.

Instalar y configurar un Sistema de detección de intrusos en un Host.

Instalar y configurar un sistemas de copias de seguridad.

7.d. Contenidos Actitudinales

Tener interés en la mejora de conocimientos relativos a esta unidad didáctica.

Tener predisposición para trabajar utilizando la plataforma Moodle.

Tener predisposición para trabajar utilizando máquinas virtuales.

Tener predisposición para trabajar bajo la interfaz de línea de comandos.

Valorar los distintos ejemplos presentados en la unidad didáctica.

Valorar las distintas herramientas presentadas en esta unidad didáctica.

Mostrar actitud de aplicar medidas de seguridad presentadas en esta unidad didáctica

Mostrar voluntad de ayudar a los demás.

Presentar disposición de trabajo en equipo.

Respetar las opiniones manifestadas libremente por los compañeros.

7.e. Criterios de Evaluación

Los indicados en el "Reparto de los criterios de evaluación".

Código:	Rev.:	Fecha Implantación:	Entregar a:	Página 28 de 31
MD850401	4	15/02/2018	Jefa/e depto. → Jefatura estudios	

7. MATERIAS TRANSVERSALES

En las diversas unidades, se trabajarán los siguientes temas transversales:

Coeducación

Educación para la vida en sociedad y convivencia

Educación del consumidor

Educación ambiental

Educación para la salud

Código:	Rev.:	Fecha Implantación:	Entregar a:	Página 29 de 31
MD850401	4	15/02/2018	Jefa/e depto. → Jefatura estudios	

8. ACTIVIDADES COMPLEMENTARIAS Y EXTRAESCOLARES

Durante el presente curso se podrán realizar las siguientes actividades:

1. Asistencia a charlas/coloquios/conferencias de personas relacionadas con las tecnologías de la información y la comunicación.
2. Visitas y/o actividades que durante el presente curso escolar se programen a nivel de departamento, y se consideren aptas para el alumnado del curso de especialización.

Código:	Rev.:	Fecha Implantación:	Entregar a:	Página 30 de 31
MD850401	4	15/02/2018	Jefa/e depto. → Jefatura estudios	

9. BIBLIOGRAFÍA, MATERIALES Y RECURSOS

9.1. Bibliografía de departamento

Hardening de servidores GNU/Linux. Editorial OxWord.

Máxima seguridad en Windows: Secretos técnicos

9.2. Materiales, recursos y laboratorios

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. Esto permitirá utilizar de forma ágil los siguientes recursos:

- Pizarra blanca
- Cañón de proyección.
- Sistema de audio en el aula.
- Ordenador Personal
- Red de área local.
- Acceso a servidores y servicios del departamento
- Acceso a Internet.
- Manuales, apuntes y tutoriales on-line.

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