

	PLANIFICACIÓN DOCENTE		IES VIRGEN DEL CARMEN		
	PROGRAMACIÓN		Paseo de la Estación nº 44 23008 Jaén Tel. 953366942 – Fax: 953366944 www.iesvirgendelcarmen.com		
	MD75010201	Rev. 4	18/09/20	Página 1 de 29	

MÓDULO:	INCIDENTES DE CIBERSEGURIDAD
CURSO:	2022/2023

DEPARTAMENTO	INFORMÁTICA
CURSO DE ESPECIALIZACIÓN	CURSO DE ESPECIALIZACIÓN EN CIBERSEGURIDAD EN ENTORNOS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN
PROFESORES	JUAN GUALBERTO GUTIÉRREZ MARÍN

Índice de contenido

Objetivos Generales.....	3
Metodología.....	7
Competencias Profesionales Generales.....	10
Resultados de aprendizaje, Evaluación y Recuperación.....	12
Resultados de Aprendizaje.....	12
Procedimientos de Evaluación.....	12
Criterios de ponderación.....	13
Criterios de evaluación.....	14
Criterios de recuperación.....	19
Evaluación de Competencias Profesionales.....	19
Atención a la diversidad.....	21
Alumnos con compatibilidad laboral y/o modularidad.....	21
Alumnado con altas capacidades.....	21
Contenidos.....	22
Relación de bloques temáticos.....	22
Secuenciación de contenidos.....	24
Unidad didáctica 1: Introducción a la ciberseguridad, Plan Director de Seguridad y Auditoría Informática.....	24
Unidad didáctica 2: Análisis de incidentes de Ciberseguridad.....	25
Unidad didáctica 3: Investigación de los incidentes de ciberseguridad.....	25
Unidad didáctica 4: Implementación de medidas de ciberseguridad.....	26
Unidad didáctica 5: Detección y documentación de incidentes de ciberseguridad:.....	26
Materias Transversales.....	28
Actividades Complementarias y Extraescolares.....	29
Bibliografía, Materiales y Recursos.....	30
Bibliografía.....	30
Materiales, recursos y laboratorios.....	30

[Escriba aquí]

Código:	Rev.:	Fecha Implantación:	Entregar a:	Página 2 de 29
MD75010201	4	18/09/2020	Jefa/e depto. → Jefatura estudios	

1. OBJETIVOS GENERALES

La **normativa** que regula tanto el título de Desarrollo de Aplicaciones Web como el módulo de Entornos de desarrollo:

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.

OBJETIVOS GENERALES DEL CURSO DE ESPECIALIZACIÓN EN CIBERSEGURIDAD EN ENTORNOS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN.

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 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.

[Escriba aquí]

Código:	Rev.:	Fecha Implantación:	Entregar a:	Página 3 de 29
MD75010201	4	18/09/2020	Jefa/e depto. → Jefatura estudios	

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.

COMPETENCIA GENERAL DEL Curso de especialización en ciberseguridad en entornos de las tecnologías de la información

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.

La formación del módulo contribuye a alcanzar los objetivos generales de este curso de especialización que se relacionan a continuación:

- Identificar los principios de la organización y normativa de protección en ciberseguridad, planificando las acciones que es preciso adoptar en el puesto de trabajo para la elaboración del plan de prevención y concienciación.
- Auditar el cumplimiento del plan de prevención y concienciación de la organización, definiendo las acciones correctoras que puedan derivarse para incluirlas en el plan de securización de la organización.
- Detectar incidentes de ciberseguridad implantando los controles, las herramientas y los mecanismos necesarios para su monitorización e identificación.

[Escriba aquí]

Código:	Rev.:	Fecha Implantación:	Entregar a:	Página 4 de 29
MD75010201	4	18/09/2020	Jefa/e depto. → Jefatura estudios	

- Analizar y dar respuesta a incidentes de ciberseguridad, identificando y aplicando las medidas necesarias para su mitigación, eliminación, contención o recuperación.
- Elaborar análisis de riesgos para identificar activos, amenazas, vulnerabilidades y medidas de seguridad.
- Diseñar e implantar planes de medidas técnicas de seguridad a partir de los riesgos identificados para garantizar el nivel de seguridad requerido.
- Configurar sistemas de control de acceso, autenticación de personas y administración de credenciales para preservar la privacidad de los datos.
- Configurar la seguridad de sistemas informáticos para minimizar las probabilidades de exposición a ataques.
- 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.
- Aplicar estándares de verificación requeridos por las aplicaciones para evitar incidentes de seguridad.
- Automatizar planes de despliegado de software respetando los requisitos relativos a control de versiones, roles, permisos y otros para conseguir un despliegado seguro.
- Analizar informes forenses identificando los resultados de la investigación para extraer conclusiones y realizar informes.
- 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.
- Desarrollar manuales de información, utilizando herramientas ofimáticas y de diseño asistido por ordenador para elaborar documentación técnica y administrativa.
- Analizar y utilizar los recursos y oportunidades de aprendizaje relacionados con la evolución científica, tecnológica y organizativa del sector y las tecnologías de la información y la comunicación, para mantener el espíritu de actualización y adaptarse a nuevas situaciones laborales y personales.
- Desarrollar la creatividad y el espíritu de innovación para responder a los retos que se presentan en los procesos y en la organización del trabajo y de la vida personal.
- Evaluar situaciones de prevención de riesgos laborales y de protección ambiental, proponiendo y aplicando medidas de prevención personales y colectivas, de

[Escriba aquí]

Código:	Rev.:	Fecha Implantación:	Entregar a:	Página 5 de 29
MD75010201	4	18/09/2020	Jefa/e depto. → Jefatura estudios	

acuerdo con la normativa aplicable en los procesos de trabajo, para garantizar entornos seguros.

- Identificar y proponer las acciones profesionales necesarias para dar respuesta a la accesibilidad universal y al «diseño para todas las personas».
- Identificar y aplicar parámetros de calidad en los trabajos y actividades realizados en el proceso de aprendizaje, para valorar la cultura de la evaluación y de la calidad y ser capaces de supervisar y mejorar procedimientos de calidad.

[Escriba aquí]

Código:	Rev.:	Fecha Implantación:	Entregar a:	Página 6 de 29
MD75010201	4	18/09/2020	Jefa/e depto. → Jefatura estudios	

PRINCIPIOS METODOLÓGICOS

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 informática mediante una prueba inicial que, aunque se supone conocidos en este nivel, permita fijar el punto de partida de la asignatura. Por otra parte se pretende establecer conflictos cognitivos en el alumnado, que modifiquen sus esquemas de conocimiento para producir saltos de conocimiento; enseñar al alumnado a aprender a aprender, fomentando su autonomía didáctica y su implicación en el aprendizaje de manera activa y constructivista; y finalmente se busca que el aprendizaje sea funcional, de manera que puedan aplicar los conocimientos adquiridos en su vida cotidiana y su desempeño profesional. El esquema de trabajo que se seguirá en cada clase será el siguiente:

- ☐ 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 los alumnos.
- ☐ Orientación y resolución de dudas que surjan en la realización de dichos ejercicios
- ☐ Supervisión y corrección del trabajo realizado por los alumnos
- ☐ Asesoramiento para el estudio de los alumnos incidiendo en los conceptos.

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 video proyector.
- ☐ Acceso a internet y a la plataforma educativa on-line (moodle)
- ☐ Consulta de manuales, apuntes y tutoriales on-line evitando el gasto de papel
- ☐ Red de área local para compartir recursos

TIPOS DE ACTIVIDADES DE ENSEÑANZA Y APRENDIZAJE.

Las actividades tienen como meta la consecución de los objetivos a través de los contenidos y la adquisición de las competencias profesionales. Entre los tipos de actividades que se desarrollarán a lo largo del curso, destacan:

a) Actividades introductorias o de motivación: para que el aprendizaje sea significativo es que el alumno esté motivado por aprender, para lo que se deben presentar actividades atractivas que capten su interés. Este tipo de actividades se realizarán, normalmente, en las primeras sesiones de trabajo de la unidad y seguirán estrategias como, por ejemplo:

[Escriba aquí]

Código:	Rev.:	Fecha Implantación:	Entregar a:	Página 7 de 29
MD75010201	4	18/09/2020	Jefa/e depto. → Jefatura estudios	

- ☐ Planteamiento de problemáticas relacionadas con la materia.
- ☐ Comentarios sobre material informático presentado a clase.
- ☐ Visualización de vídeos y presentaciones.
- ☐ Curiosidades sobre los temas a tratar.
- ☐ Lectura de artículos en prensa y revistas especializadas.
- ☐ Falsos mitos en la informática.

b) Actividades diagnósticas o de revisión de conocimientos previos: se utilizarán para conocer los conocimientos previos del alumnado como base del aprendizaje significativo. Las estrategias más utilizadas son los debates y torbellinos de ideas que se alternan con preguntas y diálogos para que participe la totalidad del alumnado.

c) Actividades de desarrollo: tienen como finalidad desarrollar los distintos contenidos propuestos para la consecución de los objetivos y la adquisición de las competencias profesionales. Para ello, y tras haber realizado las exposiciones precisas, se realizarán actividades de descubrimiento dirigido o de tipo comprobatorio, para analizar el estado del proceso de enseñanza-aprendizaje:

- ☐ Explicación de conceptos de cada unidad de trabajo.
- ☐ Definición y diferenciación de los conceptos de la unidad de forma oral o escrita.
- ☐ Cuestiones de respuesta alternativa con una o varias opciones válidas.
- ☐ Realización de mapas conceptuales, cuadros sinópticos y organigramas.
- ☐ Resolución de problemas y supuestos prácticos aplicando los conceptos aprendidos.
- ☐ Realización de prácticas.
- ☐ Trabajos monográficos y búsquedas en Internet.

d) Actividades de refuerzo y ampliación: se trata de un mecanismo de atención a la diversidad y a las distintas capacidades intelectuales y ritmos de aprendizaje del alumnado. Partiendo de un diagnóstico previo del alumnado, se irá adecuando el grado de complejidad de la actividad y los requerimientos de la tarea a sus posibilidades. Entre las actividades de refuerzo destacan:

- ☐ Repaso de actividades que no han realizado con el resto del grupo.
- ☐ Participación en diálogos sobre los procedimientos de resolución de tareas.
- ☐ Elaboración de mapas conceptuales sencillos.

Entre las actividades de ampliación destacan:

[Escriba aquí]

Código:	Rev.:	Fecha Implantación:	Entregar a:	Página 8 de 29
MD75010201	4	18/09/2020	Jefa/e depto. → Jefatura estudios	

- ☐ Trabajos de investigación sobre determinados aspectos de cada unidad de trabajo.
- ☐ Trabajos monográficos interdisciplinarios.

e) Actividades de evaluación: se utilizan para valorar el proceso de aprendizaje del alumno a través de preguntas orales o escritas, tareas sobre los contenidos o actividades trabajados a lo largo de las diferentes unidades de trabajo. Tendrán como referentes los criterios de evaluación y se realizarán utilizando los procedimientos de evaluación.

[Escriba aquí]

Código:	Rev.:	Fecha Implantación:	Entregar a:	Página 9 de 29
MD75010201	4	18/09/2020	Jefa/e depto. → Jefatura estudios	

COMPETENCIAS PROFESIONALES Y SOCIALES DEL MÓDULO DE INCIDENTES DE CIBERSEGURIDAD

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

- Implantar procedimientos para la respuesta ante incidentes y mecanismos para la detección de intrusos según directrices de los equipos de respuesta ante incidentes nacionales e internacionales.
- Detectar incidentes de seguridad de forma activa y preventiva para minimizar el riesgo según directrices de los equipos de respuesta ante incidentes nacionales e internacionales.
- Coordinar la respuesta ante incidentes de seguridad entre las distintas áreas implicadas para contener y solucionar el incidente según los requisitos de servicio y dentro de las directivas de la organización.

ENTORNO PROFESIONAL

Ámbito Profesional: Desarrolla su actividad profesional en el área de sistemas del departamento de informática de empresas públicas o privadas que utilizan equipamiento informático, desempeñando tareas de auditoría, configuración y temas relacionados con la seguridad informática, tanto por cuenta ajena como por cuenta propia. **Sectores Productivos:** Está presente en múltiples sectores productivos, sobre todo en el sector servicios, aunque se percibe una marcada característica de transectorialidad.

Este profesional ejercerá su actividad en entidades de los sectores donde sea necesario establecer mecanismos y medidas para la protección de los sistemas de información y redes de comunicaciones.

Las ocupaciones y puestos de trabajo más relevantes son los siguientes:

- Experto en ciberseguridad.
- Auditor de ciberseguridad.
- Consultor de ciberseguridad
- Hacker ético.

Esta relacionado con los siguiente medios de producción:

- Aplicaciones ofimáticas corporativas
- Analizadores de vulnerabilidades.
- Herramientas para garantizar la confidencialidad de la información.

[Escriba aquí]

Código:	Rev.:	Fecha Implantación:	Entregar a:	Página 10 de 29
MD75010201	4	18/09/2020	Jefa/e depto. → Jefatura estudios	

- Programas que garantizan la confidencialidad e integridad de las comunicaciones.
- Aplicaciones para gestión de proyectos.
- Programas de análisis de contraseñas.

Y genera los siguientes productos y resultados:

- Informes de análisis de vulnerabilidades
- Relación de contraseñas débiles.
- Registro de ficheros de datos de carácter personal, según normativa vigente
- Informe de auditoría de servicios y puntos de acceso al sistema informático.

La información que utiliza o genera:

- Normativa sobre protección de datos personales.
- Política de seguridad de la empresa.
- Metodologías de análisis de seguridad (OSSTM, BS7799/ISO17799).
- Boletines de seguridad y avisos de vulnerabilidades disponibles en formato electrónico.
- Topología del sistema informático a proteger

Las líneas de actuación en el proceso de enseñanza-aprendizaje que permiten alcanzar los objetivos del módulo están relacionados con:

- La interpretación de documentación técnica.
- La instalación, configuración y personalización de diversos entornos de desarrollo.
- La utilización de distintos entornos de desarrollo para la edición y prueba de aplicaciones.
- La utilización de herramientas de depuración, optimización y documentación de aplicaciones.
- La generación de diagramas técnicos.
- La elaboración de documentación interna de la aplicación

[Escriba aquí]

Código:	Rev.:	Fecha Implantación:	Entregar a:	Página 11 de 29
MD75010201	4	18/09/2020	Jefa/e depto. → Jefatura estudios	

Además de la normativa citada en el apartado primero hay que tener presente:

ORDEN de 29 de septiembre de 2010, por la que se regula la evaluación, certificación, acreditación y titulación académica del alumnado que cursa enseñanzas de formación profesional inicial que forma parte del sistema educativo en la Comunidad Autónoma de Andalucía.

4.1. Resultados de Aprendizaje

1. Desarrolla planes de prevención y concienciación en ciberseguridad, estableciendo normas y medidas de protección.
2. Analiza incidentes de ciberseguridad utilizando herramientas, mecanismos de detección y alertas de seguridad.
3. Investiga incidentes de ciberseguridad analizando los riesgos implicados y definiendo las posibles medidas a adoptar.
4. Implementa medidas de ciberseguridad en redes y sistemas respondiendo a los incidentes detectados y aplicando las técnicas de protección adecuadas.
5. Detecta y documenta incidentes de ciberseguridad siguiendo procedimientos de actuación establecidos.

4.2. Procedimientos 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

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.

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.

Evaluación continua: Es la evaluación realizada desde que comenzamos la unidad hasta acabarla. Permite corregir errores y reorientar el proceso de enseñanza-aprendizaje.

La superación de este módulo mediante evaluación continua requiere la asistencia regular a clase y el desarrollo de todas las actividades programadas para el mismo.

Evaluación final o sumativa: Es la realizada al final de una unidad didáctica o al final de un bloque de unidades y nos permite conocer el grado de consecución de los objetivos. De acuerdo con la **Orden de evaluación del 29 de Septiembre de 2010**, se

[Escriba aquí]

Código:	Rev.:	Fecha Implantación:	Entregar a:	Página 12 de 29
MD75010201	4	18/09/2020	Jefa/e depto. → Jefatura estudios	

debe realizar una evaluación parcial o sumativa al menos tres veces al año (al final de cada evaluación) para informar al alumnado.

Además para el alumnado que participa en el proyecto dual:

- seguimiento del tutor docente en la empresa correspondiente
- información del tutor laboral
- registro de actividades del alumnado en el curso moodle de cada empresa

4.3. Criterios de ponderación

Teniendo en cuenta la Orden 29/9/2010 de evaluación de ciclos formativos y en el marco de la autonomía pedagógica, se establecen los criterios de calificación de sus módulos, teniendo en cuenta el grado de consecución de los resultados de aprendizaje establecidos en la ORDEN de 16 de junio de 2011, así como la adquisición de competencias y objetivos generales del título. Para calificar los módulos se tendrán en cuenta:

- Los criterios de evaluación establecidos en la programación.
- Los procedimientos de evaluación expuestos en el apartado 4.1
- Los siguientes criterios de calificación:

Pruebas prácticas	Supuestos prácticos y ejercicios	Trabajo diario en clase	TOTAL
40%	40%	20%	100%

Esta ponderación tendrá las siguientes matizaciones:

- Para las unidades o grupos de unidades en que la prueba práctica pudiera ser sustituida por un trabajo individual, dicho trabajo tendrá la misma ponderación que si se tratara de una prueba práctica.
- Para aquellas unidades o grupos de unidades sin prácticas, ejercicios o trabajos, este porcentaje se sumaría al de “*Pruebas teórico - prácticas*”.
- Las actividades prácticas escritas se realizarán de manera individual.
- El apartado de trabajo diario en el aula comprende aspectos tales como la participación, respeto, buen uso de materiales e instalaciones, estilo y forma en las actividades prácticas....
- Cualquier prueba de copia o plagio en los documentos evaluables implicará una calificación negativa a los alumnos/as implicados.
- Las pruebas parciales serán eliminatorias. Aquellos alumnos/as que superen las pruebas parciales (en aquellas evaluaciones planteadas de

[Escriba aquí]

Código:	Rev.:	Fecha Implantación:	Entregar a:	Página 13 de 29
MD75010201	4	18/09/2020	Jefa/e depto. → Jefatura estudios	

esta manera) no estarán obligados a realizar la prueba final de evaluación para obtener una nota positiva. Sin embargo podrán presentarse para mejorar la nota obtenida, no siendo esto óbice para disminuir la nota obtenida según el resultado de la prueba.

- Los alumnos/as que superen las tres evaluaciones quedan exentos de la evaluación ordinaria y tendrán superado el módulo.
- Para el alumnado que participa en el proyecto dual la calificación de observación diaria vendrá dada, en su mayor parte, por el seguimiento realizado por el tutor docente.

Calificación final:

La calificación final de cada evaluación se obtendrá como la **nota promedio** de las unidades evaluadas y finalizadas hasta el día de la evaluación.

Como las calificaciones son numéricas enteras, se **redondeará** (únicamente para calificaciones finales mayores de 5) al entero mayor cuando el decimal sea mayor o igual a 7. En otro caso, la nota será el entero obtenido. En el caso en que los alumnos hayan realizado actividades de ampliación de forma continua a lo largo de todo el curso, destacando sobre el resto de sus compañeros se podría redondear hacia arriba desde cualquier decimal, incluyendo aquellos inferiores a 7.

La nota final del curso corresponderá a la nota media (sin decimales) de todas las evaluaciones (redondeando de la misma manera que los casos anteriores), siempre que se hayan superado todos los trimestres.

Aquellas evaluaciones o pruebas superadas como resultado de una prueba o actividades de **recuperación**, serán calificadas con la nota obtenida en dicha prueba salvo que para dicha superación se hayan modificado objetivos, contenidos...

4.4. 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) <ul style="list-style-type: none"> • Aunque no reste puntuación se llamará la atención sobre este tema. 		X
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

[Escriba aquí]

Código:	Rev.:	Fecha Implantación:	Entregar a:	Página 14 de 29
MD75010201	4	18/09/2020	Jefa/e depto. → Jefatura estudios	

Criterios de Calificación		
Criterio (marcar con una X debajo de SI o NO)	SI	NO
<p>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)</p> <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	
<p>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)</p> <ul style="list-style-type: none"> Para superar cada evaluación se deben haber superado cada una de 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 media aritmética (redondeo al entero más cercano) de todas las calificaciones obtenidas en el curso. 	X	
<p>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%...-)</p> <ul style="list-style-type: none"> Todas las prácticas planteadas deben ser realizadas obligatoriamente. 		X
<p>La NO entrega de ejercicios de clase supone directamente que esa parte se recupera con examen (en caso afirmativo explicar los criterios)</p> <ul style="list-style-type: none"> Todos los ejercicios de clase deben ser realizados, en caso contrario dejaría de puntuar en ese apartado. 		X

- Se prevé una prueba específica de evaluación para cada una de las unidades didácticas.
- Las pruebas de evaluación podrán ser realizadas tanto de forma escrita como en el ordenador.

[Escriba aquí]

Código:	Rev.:	Fecha Implantación:	Entregar a:	Página 15 de 29
MD75010201	4	18/09/2020	Jefa/e depto. → Jefatura estudios	

A partir de las calificaciones obtenidas en cada una de las unidades didácticas obtendremos la calificación en las diferentes evaluaciones del módulo utilizando las ponderaciones descritas en las tablas A, B y C que se muestran a continuación.

TABLA A: PONDERACIONES PARA OBTENER LA CALIFICACIÓN EN LA EVALUACIÓN FINAL DEL MÓDULO EN FUNCIÓN DE LAS UNIDADES DIDÁCTICAS O DE LOS RESULTADOS DE APRENDIZAJE

	EV1	EV2		EV3		
	UD1	UD2	UD3	UD4	UD5	CALIFICACIÓN EV FINAL
RA1	5					18,5%
RA2		6				22,25%
RA3			5			18,5%
RA4				6		22,25%
RA5					5	18,5%
CALIFICACIÓN EV FINAL	18,5%	22,25%	18,5%	22,25%	18,5%	
CALIFICACION 1º EVAL	100%					
CALIFICACION 2º EVAL	31,25%	37,5%	31,25%			

Esta tabla A se indica el número de criterios de evaluación que forma cada resultado de aprendizaje, nos permite observar la importancia que tiene cada Resultado de aprendizaje y cada unidad didáctica en el módulo profesional y nos servirá para evaluar al

Código:	Rev.:	Fecha Implantación:	Entregar a:	Página 16 de 29
MD75010201	4	18/09/2019	Jefa/e depto. → Jefatura estudios	

alumnado en la evaluación final. Sin embargo, al trabajar un único RA en cada unidad podemos observar que la calificación por RA y por UD será idéntica.

La ponderación indicada en la TABLA A no es aleatoria sino que surge a partir del número de veces que se evalúan los criterios de evaluación respecto al total de la carga lectiva del módulo y considerando que todos los criterios de evaluación en DEWC tienen el mismo peso. Podemos ver que los criterios de evaluación se evalúan 27 veces en las diferentes unidades didácticas. Por lo tanto, el peso de una unidad didáctica se obtendrá al dividir el número de criterios de evaluación de dicha unidad respecto del total (27).

Los porcentajes se han redondeado para no utilizar decimales. Si se ha tenido que ajustar un porcentaje para que la suma sea el 100% siempre se ha hecho con el de menor valor para incrementar su peso o el de mayor valor para reducir su peso.

$$\text{Calificación de la evaluación final en base a RA} = \text{RA1} \cdot 0,185 + \text{RA2} \cdot 0,2225 + \text{RA3} \cdot 0,185 + \text{RA4} \cdot 0,2225 + \text{RA5} \cdot 0,185$$

$$\text{Calificación de la evaluación final en base a UD} = \text{UD1} \cdot 0,185 + \text{UD2} \cdot 0,14 + \text{UD3} \cdot 0,185 + \text{UD4} \cdot 0,16 + \text{UD5} \cdot 0,185$$

$$\text{Calificación de la primera evaluación en base a RA} = \text{RA1} \cdot$$

$$\text{Calificación de la primera evaluación en base a UD} = \text{UD1} \cdot$$

$$\text{Calificación de la segunda evaluación en base a RA} = \text{RA1} \cdot 0,3125 + \text{RA2} \cdot 0,375 + \text{RA3} \cdot 0,3125$$

$$\text{Calificación de la segunda evaluación en base a UD} = \text{UD1} \cdot 0,3125 + \text{UD2} \cdot 0,375 + \text{UD3} \cdot 0,3125$$

Código:	Rev.:	Fecha Implantación:	Entregar a:	Página 17 de 29
MD75010201	4	18/09/2019	Jefa/e depto. → Jefatura estudios	

La calificación de la tercera Evaluación coincide con la nota de la Evaluación final.

Código:	Rev.:	Fecha Implantación:	Entregar a:	Página 18 de 29
MD75010201	4	18/09/2019	Jefa/e depto. → Jefatura estudios	

4.5. 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) <i>No, se evalúa mediante un examen único.</i>		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):	X	

La recuperación de cada unidad didáctica no superada 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 (evaluación parcial en mayo) ya sea por no tener asistencia regular o por no haber superado una o varias unidades didácticas deberán asistir y superar todas las unidades en el periodo de recuperación de junio. Para poder superar cada unidad es necesario haber completado con evaluación positiva todas las actividades prácticas propuestas para dicha unidad durante el curso.

Los alumnos que, habiendo superado el módulo por evaluación continua, deseen mejorar su calificación deberán asistir a clase en el periodo de junio y 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.

4.6. Evaluación de Competencias Profesionales

Para cada unidad didáctica se incluyen los criterios de evaluación correspondientes que contribuyen a la evaluación de las competencias profesionales, personales y sociales para este módulo que se citan a continuación:

Código:	Rev.:	Fecha Implantación:	Entregar a:	Página 19 de 29
MD75010201	4	18/09/20	Jefa/e depto. → Jefatura estudios	

- Implantar procedimientos para la respuesta ante incidentes y mecanismos para la detección de intrusos según directrices de los equipos de respuesta ante incidentes nacionales e internacionales.
- Detectar incidentes de seguridad de forma activa y preventiva para minimizar el riesgo según directrices de los equipos de respuesta ante incidentes nacionales e internacionales.
- Coordinar la respuesta ante incidentes de seguridad entre las distintas áreas implicadas para contener y solucionar el incidente según los requisitos de servicio y dentro de las directivas de la organización.

Código:	Rev.:	Fecha Implantación:	Entregar a:	Página 20 de 29
MD75010201	4	18/09/20	Jefa/e depto. → Jefatura estudios	

5.1. Alumnos con compatibilidad laboral y/o modularidad

Al tratarse de un curso de especialización presencial se requiere la asistencia regular a clase.

5.2. Alumnado con altas capacidades

Proposición de actividades complementarias que amplíen sus conocimientos tanto sobre los contenidos tratados como de otros relacionados.

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.

Código:	Rev.:	Fecha Implantación:	Entregar a:	Página 21 de 29
MD75010201	4	18/09/20	Jefa/e depto. → Jefatura estudios	

6. CONTENIDOS

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

6.1. Relación de bloques temáticos

Nº U.D	Título Unidad Didáctica	Horas	Trimestre		
			1º	2º	3º
1	Introducción a la ciberseguridad, Plan Director de Seguridad y Auditoría Informática	18	X		
2	Análisis de incidentes de Ciberseguridad	42	X	X	
3	Investigación de los incidentes de ciberseguridad	21		X	
4	Implementación de medidas de ciberseguridad	42		X	X
5	Detección y documentación de incidentes de ciberseguridad	21			X

Distribución de las horas de clase previstas según calendario (incluye período de recuperación):

1ª Eval (21 h)			2ª Eval (48 h)			3ª Eval (48 h)		Fin(24 h)
Oct.	Nov.	Dic.	Ene.	Feb.	Mar.	Abril	Mayo	Junio
15	15	13	18	18	20	15	18	18

Código:	Rev.:	Fecha Implantación:	Entregar a:	Página 22 de 29
MD75010201	4	18/09/20	Jefa/e depto. → Jefatura estudios	

6.2. Secuenciación de contenidos

6.2.1. Unidad didáctica 1: Introducción a la ciberseguridad, Plan Director de Seguridad y Auditoría Informática

RA1. Selecciona las arquitecturas y tecnologías de programación sobre clientes Web, identificando y analizando las capacidades y características de cada una.

Criterios de evaluación:

- Se han definido los principios generales de la organización en materia de ciberseguridad, que deben ser conocidos y apoyados por la dirección de la misma.
- Se ha establecido una normativa de protección del puesto de trabajo.
- Se ha definido un plan de concienciación de ciberseguridad dirigido a los empleados.
- Se ha desarrollado el material necesario para llevar a cabo las acciones de concienciación dirigidas a los empleados.
- Se ha realizado una auditoría para verificar el cumplimiento del plan de prevención y concienciación de la organización.

Contenidos Integrados

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

Código:	Rev.:	Fecha Implantación:	Entregar a:	Página 23 de 29
MD75010201	4	18/09/20	Jefa/e depto. → Jefatura estudios	

6.2.2. Unidad didáctica 2: Análisis de incidentes de Ciberseguridad

RA2. Analiza incidentes de ciberseguridad utilizando herramientas, mecanismos de detección y alertas de seguridad.

Criterios de evaluación:

- Se ha clasificado y definido la taxonomía de incidentes de ciberseguridad que pueden afectar a la organización.
- Se han establecido controles, herramientas y mecanismos de monitorización, identificación, detección y alerta de incidentes
- Se han establecido controles y mecanismos de detección e identificación de incidentes de seguridad física.
- Se han establecido controles, herramientas y mecanismos de monitorización, identificación, detección y alerta de incidentes a través de la investigación en fuentes abiertas (*OSINT: Open Source Intelligence*).
- Se ha realizado una clasificación, valoración, documentación y seguimiento de los incidentes detectados dentro de la organización.

Contenidos Integrados

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

6.2.3. Unidad didáctica 3: Investigación de los incidentes de ciberseguridad

RA3. Investiga incidentes de ciberseguridad analizando los riesgos implicados y definiendo las posibles medidas a adoptar..

Criterios de evaluación:

- Se han recopilado y almacenado de forma segura evidencias de incidentes de ciberseguridad que afectan a la organización.
- Se ha realizado un análisis de evidencias.
- Se ha realizado la investigación de incidentes de ciberseguridad.
- Se ha intercambiado información de incidentes, con proveedores y/o organismos competentes que podrían hacer aportaciones al respecto.
- Se han iniciado las primeras medidas de contención de los incidentes para limitar los posibles daños causados.

Código:	Rev.:	Fecha Implantación:	Entregar a:	Página 24 de 29
MD75010201	4	18/09/20	Jefa/e depto. → Jefatura estudios	

Contenidos Integrados

- Recopilación de evidencias.
- Análisis de evidencias.
- Investigación del incidente
- Intercambio de información del incidente con proveedores u organismos competentes.
- Medidas de contención de incidentes.

6.2.4. Unidad didáctica 4: Implementación de medidas de ciberseguridad

RA4.Implementa medidas de ciberseguridad en redes y sistemas respondiendo a los incidentes detectados y aplicando las técnicas de protección adecuadas.

Criterios de evaluación:

- a) Se han desarrollado procedimientos de actuación detallados para dar respuesta, mitigar, eliminar o contener los tipos de incidentes de ciberseguridad más habituales.
- b) Se han preparado respuestas ciberresilientes ante incidentes que permitan seguir prestando los servicios de la organización y fortaleciendo las capacidades de identificación, detección, prevención, contención, recuperación y cooperación con terceros.
- c) Se ha establecido un flujo de toma de decisiones y escalado de incidentes interno y/o externo adecuados.
- d) Se han llevado a cabo las tareas de restablecimiento de los servicios afectados por un incidente hasta confirmar la vuelta a la normalidad.
- e) Se han documentado las acciones realizadas y las conclusiones que permitan mantener un registro de “lecciones aprendidas”.
- f) Se ha realizado un seguimiento adecuado del incidente para evitar que una situación similar se vuelva a repetir.

Contenidos Integrados

- Desarrollar procedimientos de actuación detallados para dar respuesta, mitigar, eliminar o contener los tipos de incidentes.
- Implantar capacidades de ciberresiliencia.
- Establecer flujos de toma de decisiones y escalado interno y/o externo adecuados.
- Tareas para reestablecer los servicios afectados por incidentes.
- Documentación
- Seguimiento de incidentes para evitar una situación similar.

6.2.5. Unidad didáctica 5: Detección y documentación de incidentes de ciberseguridad:

Código:	Rev.:	Fecha Implantación:	Entregar a:	Página 25 de 29
MD75010201	4	18/09/20	Jefa/e depto. → Jefatura estudios	

RA6. Detecta y documenta incidentes de ciberseguridad siguiendo procedimientos de actuación establecidos..

Criterios de evaluación:

- a) Se ha desarrollado un procedimiento de actuación detallado para la notificación de incidentes de ciberseguridad en los tiempos adecuados.
- b) Se ha notificado el incidente de manera adecuada al personal interno de la organización responsable de la toma de decisiones.
- c) Se ha notificado el incidente de manera adecuada a las autoridades competentes en el ámbito de la gestión de incidentes de ciberseguridad en caso de ser necesario.
- d) Se ha notificado formalmente el incidente a los afectados, personal interno, clientes, proveedores, etc., en caso de ser necesario.
- e) Se ha notificado el incidente a los medios de comunicación en caso de ser necesario.

Contenidos Integrados

- – Desarrollar procedimientos de actuación para la notificación de incidentes.
- – Notificación interna de incidentes.
- – Notificación de incidentes a quienes corresponda.

Código:	Rev.:	Fecha Implantación:	Entregar a:	Página 26 de 29
MD75010201	4	18/09/20	Jefa/e depto. → Jefatura estudios	

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. 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.
- Conocer cómo buscar de manera eficiente información en Internet.

Para la consecución de estos objetivos se planteará el desarrollo habitual de las clases actividades utilizando técnicas que lo permitan y haciendo referencias a habituales y, más concretamente, en fechas señaladas (Día de la Mujer, contra la Violencia de Género, Día de Andalucía, de la Constitución, del Libre, 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: Se harán consideraciones de tipo ergonómico sobre la forma más adecuada de utilizar el ordenador, para disfrutar de una mejor salud postural.
- Educación para la paz: Se harán consideraciones relacionadas con adoptar situaciones de diálogo y consenso frente a situaciones conflictivas en el trabajo en grupo.
- Educación medioambiental: Se harán consideraciones relacionadas con el medioambiente y con acciones que ayuden a preservarlo.

Código:	Rev.:	Fecha Implantación:	Entregar a:	Página 27 de 29
MD75010201	4	18/09/20	Jefa/e depto. → Jefatura estudios	

8. ACTIVIDADES COMPLEMENTARIAS Y EXTRAESCOLARES

El departamento de informática colaborará en todas aquellas actividades complementarias y extraescolares que se proponga en el Centro que afecten al alumnado del curso de especialización.

El alumnado que participa en la modalidad dual del curso de especialización deberá realizar la formación complementaria que determinen tanto la empresa como el departamento de informática a través del equipo educativo del grupo.

Código:	Rev.:	Fecha Implantación:	Entregar a:	Página 28 de 29
MD75010201	4	18/09/20	Jefa/e depto. → Jefatura estudios	

9. BIBLIOGRAFÍA, MATERIALES Y RECURSOS

9.1. Bibliografía

- MF0488_3:Gestión de incidentes de seguridad informática, Esther Chicano Tejada, IC Editorial
- INSTITUTO NACIONAL DE CIBERSEGURIDAD : <https://www.incibe.es/>
- ISACA <https://www.isaca.org/>
- Cómo implantar un SGSI según UNE-EN ISO/IEC 27001 y su aplicación en el Esquema Nacional de Seguridad, Luis Gómez Fernández y pedro Pablo Fernández Rivero, AENOR ediciones

9.2. Materiales, recursos y laboratorios

La LOE 2/2006 establece que las Tecnologías de la Información y la Comunicación (T.I.C.) se han de trabajar en todas las enseñanzas a todos los niveles. En el caso de este módulo y, de forma general en los ciclos formativos de la familia profesional de Informática y Comunicaciones, las TIC forman parte del propio currículo. De cualquier forma, se fomenta su uso diario utilizando recursos, además de los propios de un aula y la bibliografía de aula y departamento, como:

- *Recursos audiovisuales*: proyector digital, impresora láser conectados en red.
- *Red de ordenadores*: puestos con un ordenador por persona conectados en red, con el sistema operativo Windows 7 o 10 y Ubuntu instalados.
- *Acceso a Internet*: se fomenta especialmente la búsqueda de información en la red, enseñando cómo realizarlo de forma eficiente.
- *Correo electrónico*: se utilizan listas de distribución para el intercambio de información instantánea a un grupo amplio de receptores.
- *Plataforma Virtual*: el módulo cuenta con una plataforma virtual Moodle, accesible a través de Internet, que permite al alumnado acceder a los recursos que ofrece utilizando un usuario y clave personalizado y único. A través de la plataforma se distribuirá material de consulta del módulo y se realizará la entrega de ejercicios resueltos, trabajos y, en caso de ser posible, prácticas siendo por tanto, el mecanismo principal de comunicación profesor-alumno.

Código:	Rev.:	Fecha Implantación:	Entregar a:	Página 29 de 29
MD75010201	4	18/09/20	Jefa/e depto. → Jefatura estudios	