PROGRAMACIÓN DEL MÓDULO:

Incidentes de ciberseguridad

PROFESOR/ES:	**Francisco Javier Rodrigo Rodríguez**
GRUPO/S Y CICLO/S:	**Curso de especialización en ciberseguridad en entornos de las tecnologías de la información**
CURSO:	**2020/2021**

UNION EUROPEA
Fondo Social Europeo
"Una manera de hacer Europa"

ÍNDICE

1. INTRODUCCIÓN

El módulo Incidentes de Ciberseguridad se engloba en el Curso de especialización en ciberseguridad en entornos de las tecnologías de la información, perteneciente a la Familia Profesional de Informática y Comunicaciones, que queda establecido por el Real Decreto 479/2020, de 7 de abril, estando por determinar el currículo del mismo.

2. OBJETIVOS

Objetivos generales del curso

Los objetivos para este curso son los descritos en el Real Decreto 479/2020:

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 se 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 desplegado de software respetando los requisitos relativos a control de versiones, roles, permisos y otros para conseguir un desplegado 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.

Objetivos específicos del módulo

De los objetivos comunes del curso son aplicables a este módulo los puntos siguientes:

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 se 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.
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.

Unidades de Competencia

Las competencias asociadas al módulo Incidentes de Ciberseguridad son:

- Elaborar e implementar planes de prevención y concienciación en ciberseguridad en la organización, aplicando la normativa vigente.
- Detectar e investigar incidentes de ciberseguridad, documentándolos e incluyéndolos en los planes de securización de la organización.
- Elaborar documentación técnica y administrativa cumpliendo con la legislación vigente, respondiendo a los requisitos establecidos.
- 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.
- 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.
- 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.
- 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.

CONTENIDOS

Los contenidos a tratar en el módulo se distribuyen en las siguientes unidades didácticas.

En negrita y cursiva están expresados aquellos contenidos y estándares de aprendizaje evaluables que se consideran como "imprescindibles o básicos" para un posible cambio a Escenario III. Esto se realiza atendiendo a la "GUÍA GENERAL PARA LA ORGANIZACIÓN Y DESARROLLO DE LA ACTIVIDAD EDUCATIVA PARA EL CURSO 2020/21 EN TODOS LOS CENTROS SOSTENIDOS CON FONDOS PÚBLICOS DE LA COMUNIDAD AUTÓNOMA DE EXTREMADURA" y a la "Instrucción 13/2020, de 2 de septiembre de 2020, de la Secretaría General de Educación, referente a la organización de las actividades lectivas semipresenciales y no presenciales, la evaluación del aprendizaje del alumnado y otros aspectos de la organización y funcionamiento de los centros educativos y del sistema educativo en su conjunto, durante el curso 2020-2021".

UNIDAD DIDÁCTICA 0. Presentación del módulo. Herramientas para el seguimiento de la enseñanza. Introducción:

- ***Presentación del módulo y de las herramientas para el seguimiento de la enseñanza.***
- ***Metodologías de trabajo en los escenarios de enseñanza presencial, semipresencial y a distancia. Manejo de las herramientas (plataforma on line, seguimiento de las clases, propuestas de trabajo y entrega de tareas).***
- ***Introducción a los Incidentes de Ciberseguridad***

UNIDAD DIDÁCTICA 1. La ciberseguridad y los centros de operaciones de seguridad

- El peligro
- Combatientes en la guerra contra la ciberdelincuencia

UNIDAD DIDÁCTICA 2. Sistema operativo Windows

- Descripción general de Windows
- ***Administración de Windows***

UNIDAD DIDÁCTICA 3. Sistema operativo Linux

- Uso de Linux
- ***Administración de Linux***
- Clientes Linux

UNIDAD DIDÁCTICA 4. Protocolos y servicios de red

- Protocolos de red
- ***Ethernet y protocolo de Internet (IP)***
- Verificación de conectividad
- Protocolo de resolución de direcciones
- La capa de transporte y los servicios de red
- ***Servicios de red***

UNIDAD DIDÁCTICA 5. Infraestructura de red

- Dispositivos de comunicación por redes
- ***Infraestructura de seguridad de redes***
- Representaciones de redes

UNIDAD DIDÁCTICA 6. Principios de la seguridad de redes

- Los atacantes y sus herramientas
- ***Amenazas y ataques comunes***

UNIDAD DIDÁCTICA 7. Ataques a redes

- Observación del funcionamiento de las redes
- ***Ataques a los pilares***
- ***Ataques a nuestra tarea***

UNIDAD DIDÁCTICA 8. Protección de la red

- La defensa
- ***Control de acceso***
- ***Los firewalls de redes y la prevención de intrusiones***
- ***Filtrado de contenido***
- ***Inteligencia de amenazas***

UNIDAD DIDÁCTICA 9. La criptografía y la infraestructura de claves públicas

- ***Criptografía***
- Criptografía de claves públicas

UNIDAD DIDÁCTICA 10. Seguridad y análisis de terminales

- ***Protección de terminales***
- ***Evaluación de vulnerabilidades de terminales***

UNIDAD DIDÁCTICA 11. Monitoreo de seguridad

- ***Tecnologías y protocolos***
- Archivos de registros

UNIDAD DIDÁCTICA 12. Análisis de datos de intrusiones

- ***Recopilación de datos***
- ***Preparación de datos***
- ***Análisis de datos***

UNIDAD DIDÁCTICA 13. Respuesta y manejo ante incidentes

- ***Modelos de respuesta ante incidentes***
- ***Los CSIRT y NIST 800-61r2***
- Práctica con casos

UNIDAD DIDÁCTICA 14. Plan De Seguridad. Prevención, Auditoría y Protección

3. DISTRIBUCIÓN TEMPORAL DE CONTENIDOS

Este módulo se imparte durante 6 horas semanales distribuidas a lo largo de dos trimestres lectivos, con un total de 157 horas lectivas.

EVALUACIÓN	TEMA, BLOQUE O UNIDAD DIDÁCTICA	FECHA INICIO ---- FECHA FIN *Diferenciar por grupo si son diferentes*	Nº HORAS LECTIVAS
1ª	Capítulo 0: Presentación del módulo. Herramientas para el seguimiento de la enseñanza. Introducción	16/11/2020 a 16/11/2020	1
	Capítulo 1: La ciberseguridad y el Centro de Operaciones de Seguridad	17/11/2020 a 26/11/2020	10
	Capítulo 2: Incidentes de Seguridad en Windows	30/11/2020 a 11/12/2020	9
	Capítulo 3: Incidentes de Seguridad en Linux	14/12/2020 a 22/12/2020	9
	Capítulo 4: Protocolos y servicios de red	11/01/2021 a 20/01/2021	10
	Capítulo 5: Infraestructura de la red	21/01/2021 a 01/02/2021	9
	Capítulo 6: Principios de la seguridad de la red	02/02/2021 a 12/02/2021	11
	Capítulo 7: Ataques a la red	17/02/2021 a 01/03/2021	10
	EXAMEN FINAL DEL TRIMESTRE y revisión del examen	02/03/2021 a 04/03/2021	4
		% AVANCE EN CONTENIDOS	**46%**
2ª	Capítulo 8: Protección de la red	05/03/2021 a 16/03/2021	10
	Capítulo 9: La criptografía y la infraestructura de claves públicas	17/03/2021 a 26/03/2021	8

	Capítulo 10: Seguridad y análisis de terminales	06/04/2021 a 16/04/2021	11
	Capítulo 11: Monitoreo de la seguridad	19/04/2021 a 30/04/2021	12
	Capítulo 12: Análisis de datos de intrusiones	03/04/2021 a 14/05/2021	12
	Capítulo 13: Manejo y respuesta ante los incidentes	17/05/2021 a 28/05/2021	12
	Capítulo 14: Plan De Seguridad. Prevención, Auditoría y Protección	31/05/2021 a 09/06/2021	10
	EXÁMENES FINALES DEL CURSO y REVISIÓN DE EXÁMENES FINALES DEL CURSO	14/06/2021 a 18/06/2021	6
	Actividades de ampliación, refuerzo y revisión	21/06/2021 a 22/06/2021	3
% AVANCE EN CONTENIDOS			**100%**

Destacar que esta planificación, realizada en base al calendario escolar del presente curso se podrá revisar a lo largo del mismo de forma periódica como consecuencia de la necesaria flexibilidad que suponen los distintos niveles de aprendizaje de contenidos que se presentan de forma natural en los distintos grupos de alumnos y también de otras circunstancias que puedan ocurrir de forma imprevista y que impida desarrollar de forma normal la impartición de estos contenidos.

La eventualidad del paso a enseñanza semipresencial o a distancia puede modificar el orden de impartición de los contenidos y la duración planificada para cada uno de los bloques.

Por otra parte, esta distribución no coincide en número de horas totales respecto a lo que marca el título oficial, ya que las horas reales vendrían definidas en el currículo que aún no está publicado. Se ha utilizado como criterio el calendario escolar oficial previsto para este curso.

4. CRITERIOS DE EVALUACIÓN

Los criterios de evaluación del módulo profesional Incidentes de Ciberseguridad están asociados a resultados de aprendizaje, definidos en el Real Decreto que establece el título.

Permiten comprobar el nivel de adquisición del resultado de aprendizaje correspondiente y constituyen la guía y el soporte para definir las actividades propias del proceso de evaluación. Aparecen aquí de forma general asociados a cada resultado de aprendizaje y concretados en cada

una de las unidades didácticas o de trabajo.

La unidad didáctica 0 es de presentación e introductoria para dar a conocer el contenido del módulo y las herramientas didácticas, por lo que no es evaluable ni calificable.

Criterios de evaluación del resultado de aprendizaje 1: *Desarrolla planes de prevención y concienciación en ciberseguridad, estableciendo normas y medidas de protección.*

- 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

Criterios de evaluación del resultado de aprendizaje 2: *Analiza incidentes de ciberseguridad utilizando herramientas, mecanismos de detección y alertas de seguridad.*

- 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.

Criterios de evaluación del resultado de aprendizaje 3: *Investiga incidentes de ciberseguridad analizando los riesgos implicados y definiendo las posibles medidas a adoptar.*

- 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.

Criterios de evaluación del resultado de aprendizaje 4: *Implementa medidas de ciberseguridad en redes y sistemas respondiendo a los incidentes detectados y aplicando las técnicas de protección adecuadas.*

- Se han desarrollado procedimientos de actuación detallados para dar respuesta, mitigar, eliminar o contener los tipos de incidentes de ciberseguridad más habituales.
- 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.
- Se ha establecido un flujo de toma de decisiones y escalado de incidentes interno y/o externo adecuados.
- Se han llevado a cabo las tareas de restablecimiento de los servicios afectados por un incidente hasta confirmar la vuelta a la normalidad.
- Se han documentado las acciones realizadas y las conclusiones que permitan mantener un registro de "lecciones aprendidas".
- Se ha realizado un seguimiento adecuado del incidente para evitar que una situación similar se vuelva a repetir.

Criterios de evaluación del resultado de aprendizaje 5: *Detecta y documenta incidentes de ciberseguridad siguiendo procedimientos de actuación establecidos.*

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

5. RELACIÓN CON OTROS MÓDULOS DEL CICLO

Es necesaria la coordinación con el resto de profesores de los restantes módulos para adaptarse y garantizar la unidad y coherencia de las enseñanzas de todos los módulos del ciclo, asegurando unos principios educativos y unos objetivos dentro del ciclo en su conjunto, evitando repetir contenidos pero sí complementándose.

6. METODOLOGÍA DIDÁCTICA

Los aspectos metodológicos que se pretenden aplicar en este módulo descansan en la idea de que el alumno se considere parte activa de la actividad docente, con esto se pretende involucrarlo en el proceso de asimilación de nuevos conceptos y adquisición de capacidades no como un mero contenedor de éstas sino como un productor directo de estos conocimientos y habilidades en sí mismo.

La metodología deberá ser eminentemente práctica, acompañada de situaciones que reflejen la realidad en la mayor medida posible, con el poco material disponible. Para el trabajo en el aula, los

alumnos dispondrán de toda la documentación que se considere oportuna, además de la asistencia permanente del profesor.

La metodología será participativa, favoreciendo el aprendizaje por descubrimiento. Partiendo de los conocimientos iniciales de los alumnos/as, estos deberán construir sus aprendizajes significativos.

El método de enseñanza-aprendizaje se articulará en torno a cuatro tipos de actividades interrelacionadas:

- Presentación de los contenidos. Se relacionan con los objetivos a conseguir y con la metodología a seguir. Se realizará una evaluación inicial al principio de cada unidad de trabajo para comprobar los conocimientos básicos que pueden tener algunos de los alumnos. Se hará por medio de preguntas espontáneas en el aula. Servirá para construir el aprendizaje sobre lo que saben los alumnos, también para detectar mitos o conceptos erróneos que puedan tener algunos alumnos de antemano.
- Descripción teórica de los contenidos conceptuales. Se utilizarán, en la medida de lo posible, los medios audiovisuales para facilitar su asimilación. Consistirá en la exposición en clase de las unidades de trabajo.
- Ejemplificación práctica de los contenidos expuestos. Se procurará relacionar los contenidos expuestos con situaciones concretas y cercanas al entorno sociolaboral del alumnado o, con carácter más general, a la actualidad regional, nacional o internacional.
- Se resolverán en clase ejercicios y supuestos. Los alumnos podrán utilizar sus equipos para verificar la corrección de tales supuestos.
- Realización de actividades de consolidación, individualmente y/o en grupos de trabajo. Se podrán realizar en clase y/o en casa (sin dar por supuesto que los alumnos disponen de ordenador en casa), posteriormente se corregirán por parte del profesor, ya sea mediante puesta en común en clase o individualmente fuera del horario lectivo.

7. PROCEDIMIENTOS DE EVALUACIÓN DEL APRENDIZAJE DE LOS ALUMNOS

Los distintos instrumentos de evaluación utilizados serán los siguientes para este módulo:

- Pruebas/exámenes escritos (preferentemente digital):
  - de preguntas cortas/tests o de desarrollo para evaluar contenidos conceptuales teóricos,
  - de resolución de problemas prácticos o casos prácticos de configuraciones para evaluar contenidos procedimentales prácticos.
  - de instalación y configuración de servicios en equipos reales o virtualizados para evaluar contenidos procedimentales prácticos.
- Trabajos prácticos obligatorios propuestos para realización en casa o clase. Se calificarán de 1 a 10.

- Trabajos prácticos voluntarios de ampliación de contenidos. Se calificarán de 1 a 10.
- Trabajo diario (participación y actitud en clase). Otra parte del proceso evaluador corresponde al trabajo desarrollado por el alumno de forma continua y durante todo el proceso. Se valora aquí la participación del alumno en su propio aprendizaje, demostrando la madurez suficiente para trabajar individualmente y en equipo, integrándose con los compañeros, siendo puntual y correcto en sus formas y siendo capaz de llegar a aprender o progresar por sí mismo, algo importantísimo en una rama tan cambiante como es la informática, donde una vez terminada la enseñanza reglada se debe seguir aprendiendo para evitar la obsolescencia de sus conocimientos. La calificación de este apartado se realizará teniendo en cuenta el comportamiento del alumno, su puntualidad y asistencia, el interés por mejorar y no estancarse en los mínimos necesarios y su nivel de participación en el aula. De todo esto tomará el profesor notas diarias.

Aquellos alumnos con evaluaciones suspensas podrán realizar un examen final, al finalizar el último trimestre, siempre que hayan entregado y superado, al menos con un 5, todos los proyectos y prácticas obligatorias del curso.

En caso de no superar la convocatoria ordinaria de junio tienen derecho a realizar una evaluación extraordinaria, que se llevará a cabo en el mes de septiembre.

8. CRITERIOS DE CALIFICACIÓN

Las calificaciones en este módulo vendrán dadas por la superación y el dominio de:

- Los contenidos básicos (hechos, conceptos y principios), recogidos en la programación, evaluados en términos de consecución de los resultados de aprendizaje y según los criterios de evaluación.
- Los procedimientos:
  - La adquisición de destrezas manuales relativas a la competencia
  - El desarrollo de la capacidad para aprender por sí mismos.
- Las actitudes («saber ser y estar»), que expresan la autorregulación del comportamiento en función del rol profesional. Se centrará en:
  - La participación en las propuestas de actividades que se programen para su realización
  - El desarrollo de la capacidad para trabajar en equipo.
  - El saber intervenir activamente en procesos de decisión compartida de profesional a la que se vincula la presente programación.
  - Trabajar los distintos contenidos de forma creativa, original y positiva.

En base a estos puntos a continuación se determinan los criterios de calificación.

Calificación de cada trimestre

Se calificará a los alumnos en sesiones de evaluación una vez al final de cada trimestre.
A lo largo del trimestre se realizarán exámenes para comprobar el grado de adquisición de conocimientos y destrezas sobre el o las unidades didácticas que se consideren oportunas.
Se utilizarán las siguientes ponderaciones para obtener la calificación del trimestre:

- Media de las calificaciones **obtenidas en las pruebas objetivas** realizadas, en las cuales el alumno demuestra la correcta asimilación de las materias impartidas, mediante exámenes, prácticas o trabajos obligatorios. Si alguna de las pruebas tuviera una valoración distinta a las demás, se indicará al alumno previamente. **(70%)**
- **Trabajos** prácticos voluntarios de ampliación de contenidos; en caso de que en la evaluación no haya trabajos prácticos voluntarios, este porcentaje se añade al apartado siguiente. **(10%)**
- La valoración del profesor sobre las **prácticas y actividades propuestas en el aula**, desarrolladas por el alumno bien en grupo o individualmente. Cada una de ellas se valorará con APTO o NO APTO. La puntuación se obtendrá según el número de APTOS obtenidos. **(20%)**

Para poder realizar el cálculo para obtener la calificación final del trimestre, se debe tener APTO en el 60% de las prácticas y actividades propuestas.

La calificación final del trimestre se redondea hacia arriba o abajo según la actitud y trabajo diario recogidos continuamente mediante anotaciones del profesor a lo largo del trimestre.

Cada actitud negativa recogida por el profesor descontará 0,25 puntos de la nota del trimestre. Se considera actitud negativa la falta de respeto en el aula hacia un compañero o profesor o la pasividad reiterada en la realización de ejercicios y aprovechamiento de las clases.

La calificación final será de aprobado si se obtiene una nota de 5 o superior.

Calificación final del módulo

La calificación final del módulo será la media aritmética obtenida en las evaluaciones trimestrales, siempre que se obtenga al menos 5 puntos en cada una.

En el caso de que en alguna de las evaluaciones no se obtenga una calificación de 5 puntos o superior, se realizará un examen de recuperación final en el mes de junio. La nota máxima que se puede obtener en las recuperaciones será de 5.

Si tras la la realización de los exámenes de recuperación final, la calificación de cada evaluación es 5 o mayor, el alumno habrá superado el módulo, recogiéndose dicha calificación en Rayuela en convocatoria Ordinaria. En caso contrario, deberá acudir a la convocatoria extraordinaria en el mes de septiembre.

En los casos excepcionales en los que un alumno, después de realizar las recuperaciones de las evaluaciones pendientes, todavía tenga suspensa una sola evaluación con nota igual o superior a 4 y la media de las dos evaluaciones salga aprobada, el alumno habrá aprobado el módulo.

Convocatoria extraordinaria

La convocatoria extraordinaria de este módulo se realizará en el mes de septiembre. Los alumnos que tengan que realizar dicha convocatoria extraordinaria se examinarán sólo de los contenidos de la evaluación pendiente.

Trabajos y prácticas de carácter obligatorio

En el caso de trabajos y prácticas de carácter obligatorio el alumno tendrá que presentarlos para poder obtener una evaluación positiva, entendiéndose que en caso de no presentarlos renuncia a ser evaluado positivamente (se entiende por calificación positiva un 5 o más). Los ejercicios y trabajos no entregados en los plazos fijados por el profesor se consideran no entregados en cualquier caso.

Dichos trabajos y prácticas de carácter obligatorio se contabilizarán con un porcentaje establecido previamente, informándose adecuadamente a los alumnos.

Los criterios de calificación descritos en este documento así como las ponderaciones son los que se planifican al iniciar el curso de forma objetiva, ahora bien, pueden depender en gran medida de los contenidos que se imparten de forma efectiva en cada momento y de posibles situaciones imprevistas que puedan hacer modificar estas ponderaciones. De cualquiera de las maneras, de ocurrir alguna modificación, se dará cumplida publicidad e información a los alumnos, por los medios que más garantías de difusión ofrezcan.

En caso de que por motivos imprevistos no se pueda desarrollar el temario con normalidad (parada anormal de las clases, huelgas, etc), cumpliendo los plazos previstos para ello, el profesor realizará los ajustes y modificaciones pertinentes que, a su entender, garanticen mejor una calificación más justa y un mejor desarrollo del proceso de enseñanza-aprendizaje.

Normativa de exámenes y tareas:

- Los exámenes se realizarán en la fecha y hora indicadas por la profesora del módulo.
- La no asistencia a examen supone la calificación de **No presentado.**
- Solo se considerarán justificantes válidos los emitidos por órganos oficiales que **explícitamente indiquen** que no es posible o recomendable la asistencia en la fecha y hora del examen. A los estudiantes que aporten tales justificantes de ausencia a examen se les propondrá otra fecha y hora de realización.
- En caso de detectar plagios en tareas y exámenes (sea de compañeros o de otras

fuentes) la calificación de la tarea o examen será de 0**.**

En los exámenes no se podrá hablar ni realizar preguntas en voz alta, ni comentarios o ruidos que distraigan a los demás compañeros. En el caso de que estos se produzcan se expulsará al alumno del aula, suponiendo la anulación del examen y la calificación de 0.

9. ATENCIÓN A LA DIVERSIDAD

En la Formación Profesional cualquier adaptación curricular debe ser no significativa, por lo que se realizarán adaptaciones sobre la metodología y sobre el proceso evaluador, pudiéndose modificar el formato de prácticas y exámenes, pero nunca supondrá modificación alguna sobre los contenidos mínimos del módulo.

Según las circunstancias y manteniendo los mismos objetivos educativos es posible:

- Establecer en cada unidad didáctica los diferentes grupos de actividades.
- Plantear metodologías y niveles de ayuda diversos, según el grado de conocimiento previo detectado, el grado de autonomía y responsabilidad y las dificultades detectadas previamente.
- Adaptar el material didáctico.
- Organizar grupos de trabajo flexibles, lo que permitirá establecer tareas de refuerzo, profundización, etc, en función de las diferentes necesidades del grupo.
- Organizar y secuenciar los contenidos de forma distinta, representando las actividades de forma secuencial y a modo de actividades graduadas, lo que permitirá desmenuzar los contenidos y trabajar un mismo contenido de diversas maneras, a la par que ir caminando hacia actividades más significativas.

10. MATERIALES Y RECURSOS DIDÁCTICOS, HERRAMIENTAS Y EQUIPAMIENTOS

Algunos materiales que utilizaremos en clase serán:

- Presentaciones elaboradas.
- Apuntes de clase y libros de consulta.
- Los manuales impresos y en línea, de todo el software instalado.
- Publicaciones periódicas relacionadas con el mundo de la ciberseguridad.
- Información accesible vía Internet.

En cuanto a recursos Hardware:

- Equipamiento del aula: ordenadores, periféricos.
- Cableado, switches y tarjetas de red.
- Equipos servidores de red y estaciones de trabajo.
- Acceso a Internet.
- Retroproyector y pantalla mural.

En cuanto a recursos Software:

- Máquinas virtuales con los sistema operativo de red necesarios (preferentemente los de mayor uso en el mercado (Ubuntu, Windows Server).
- Sistemas operativos en las estaciones de trabajo.
- Software de simulación de red Cisco Packet Tracer

11. ACTIVIDADES COMPLEMENTARIAS Y EXTRAESCOLARES

Se realizarán aquellas actividades extraescolares que, estando programadas a nivel del departamento de informática, estén relacionadas con los contenidos del módulo.

12. TEMAS TRANSVERSALES

De los temas transversales aconsejados por los departamentos de IyC y FOL para los módulos de la familia profesional de Informática y Comunicaciones se trabajarán los siguientes:

Educación ambiental
El análisis y la utilización de diferentes herramientas informáticas favorecen la capacidad del alumno/a para decidir sobre los productos informáticos que debe adquirir y utilizar de la manera más apropiada, valorando de manera crítica las distintas ofertas, campañas de publicidad, etc.

Educación para la igualdad de oportunidades entre ambos sexos
Desde este módulo contamos con elementos para concienciar al alumnado sobre la igualdad de oportunidades entre los sexos, formando grupos mixtos de trabajo, distribuyendo iguales tareas entre alumnos y alumnas, haciendo que todos utilicen iguales o similares materiales y fomentando la participación de todos, sin distinciones de sexo.

Educación para la paz
Concienciando a los alumnos y alumnas de la importancia de mantener un clima de respeto y de cooperación en el aula.

Educación para la salud
Cuando se utilizan equipos informáticos uno de los objetivos es que los alumnos y alumnas conozcan unas normas básicas de higiene y seguridad en el trabajo, así como a tomar las debidas precauciones en el empleo de dichos equipos. Es necesario conocer unos principios de ergonomía en el puesto de trabajo, para que la actividad frente al ordenador no sea motivo de problemas físicos. Estos aspectos cobran especial importancia en la Prevención de riesgos laborales. Considerando que el ámbito laboral más común de los Técnicos va a ser las oficinas y centros de procesos de datos, habrá que insistir a diario en la existencia de los siguientes riesgos y de sus correspondientes medidas de prevención

Educación del consumidor
El análisis y la utilización de diferentes herramientas informáticas favorecen la capacidad del alumno/a para decidir sobre los productos informáticos que debe adquirir y utilizar de la manera

más apropiada, valorando de manera crítica las distintas ofertas, campañas de publicidad, etc