

Criterios de calificación para el módulo profesional de Seguridad informática

El módulo profesional de **Seguridad informática** se imparte en el segundo curso, con una carga lectiva de 105 horas que se distribuyen a razón de **5 horas semanales durante 21 semanas**.

Al tratarse de un módulo de segundo curso, se realizarán **dos sesiones de evaluación parcial**, la primera al final del primer trimestre y la segunda a mediados de marzo, teniendo en cuenta que deben haber transcurrido 110 jornadas lectivas antes de poder celebrarse. Además de las evaluaciones parciales, se realizará una **sesión de evaluación final**, coincidiendo con la finalización del régimen ordinario de clases.

Este módulo tiene asociados **5 resultados de aprendizaje**, que debe alcanzar el alumnado a lo largo del curso, y que se trabajarán en las diferentes **unidades didácticas**, distribuidas en los dos trimestres, tal y como se muestra en la siguiente tabla. Se le ha asignado una **ponderación** a cada uno de los resultados de aprendizaje, según su importancia.

Temporalización	Unidad didáctica	Resultado de aprendizaje	Ponderación
Trimestre 1	UD 1: Aplicación de medidas de seguridad pasiva	1	25%
	UD: 2: Gestión de dispositivos de almacenamiento	2	20%
	UD3: Aplicación de medidas de seguridad activa	3	25%
Trimestre 2	UD4: Aseguramiento de la privacidad	4	15%
	UD5: Cumplimiento de la legislación y normas de seguridad	5	15%

De la temporalización anterior, sabiendo qué resultados de aprendizaje se van a trabajar y a evaluar en cada trimestre, y aplicando los pesos indicados, podemos así calcular las calificaciones, tanto de las evaluaciones parciales como de la evaluación final, como se resume en la siguiente tabla.

Resultados Aprendizaje	Unidad Didáctica	Calificación 1ª eval.	Calificación 2ª eval.	Calificación final
R. A. 1	UD 1	35%		25%
R. A. 2	UD 2	30%		20%
R. A. 3	UD 3	35%		25%
R. A. 4	UD 4		60%	15%
R. A. 5	UD 5		40%	15%
TOTAL		100%	100%	100%

La **calificación trimestral y final** de este módulo se expresará en cifras de 1 a 10 sin decimales, considerándose positivas las calificaciones iguales o superiores a 5 y negativas las restantes.

Cada uno de estos resultados de aprendizaje tiene asociados una serie de **criterios de evaluación**, que también se ponderan dada su relevancia. Cada uno de estos criterios se valorará mediante un **instrumento de evaluación**, obteniendo así una calificación numérica, tal y como se muestra en las siguientes tablas.

Resultados de Aprendizaje	1. Aplica medidas de seguridad pasiva en sistemas informáticos describiendo características de entornos y relacionando las con sus necesidades.		
Criterios de evaluación	Peso	UD	Instrumento de evaluación
a) Se ha valorado la importancia de mantener la información segura.	15%	1	Prueba escrita UD1
b) Se han descrito las diferencias entre seguridad física y lógica.	15%	1	Prueba escrita UD1
c) Se han definido las características de la ubicación física y condiciones ambientales de los equipos y servidores.	10%	1	Prueba tipo test UD1
d) Se ha identificado la necesidad de proteger físicamente los sistemas informáticos.	10%	1	Prueba escrita UD1
e) Se ha verificado el funcionamiento de los sistemas de alimentación ininterrumpida.	15%	1	Prueba escrita UD1
f) Se han seleccionado los puntos de aplicación de los sistemas de alimentación ininterrumpida.	10%	1	Prueba tipo test UD1
g) Se han esquematizado las características de una política de seguridad basada en listas de control de acceso.	10%	1	Práctica de aula UD1
h) Se ha valorado la importancia de establecer una política de contraseñas.	10%	1	Práctica de aula UD1
i) Se han valorado las ventajas que supone la utilización de sistemas biométricos.	5%	1	Prueba tipo test UD1
TOTAL	100%		

Resultados de Aprendizaje	2. Gestiona dispositivos de almacenamiento describiendo los procedimientos efectuados y aplicando técnicas para asegurar la integridad de la información.		
Criterios de evaluación	Peso	UD	Instrumento de evaluación
a) Se ha interpretado la documentación técnica relativa a la política de almacenamiento.	10%	2	Prueba escrita UD2
b) Se han tenido en cuenta factores inherentes al almacenamiento de la información (rendimiento, disponibilidad, accesibilidad, entre otros).	18%	2	Prueba escrita UD2
c) Se han clasificado y enumerado los principales métodos de almacenamiento incluidos los sistemas de almacenamiento en red.	17%	2	Prueba escrita UD2
d) Se han descrito las tecnologías de almacenamiento redundante y distribuido.	15%	2	Batería tareas UD2
e) Se han seleccionado estrategias para la realización de copias de seguridad.	10%	2	Prueba escrita UD2
f) Se ha tenido en cuenta la frecuencia y el esquema de rotación.	5%	2	Prueba escrita UD2
g) Se han realizado copias de seguridad con distintas estrategias.	5%	2	Práctica de aula UD2
h) Se han identificado las características de los medios de almacenamiento remotos y extraíbles.	5%	2	Batería tareas UD2
i) Se han utilizado medios de almacenamiento remotos y extraíbles.	5%	2	Batería tareas UD2
j) Se han creado y restaurado imágenes de respaldo de sistemas en funcionamiento.	10%	2	Práctica de aula UD2
TOTAL	100%		

Resultados de Aprendizaje	3. Aplica mecanismos de seguridad activa describiendo sus características y relacionándolas con las necesidades de uso del sistema informático.		
Criterios de evaluación	Peso	UD	Instrumento de evaluación
a) Se han seguido planes de contingencia ante fallos de seguridad.	18%	3	Prueba escrita UD3
b) Se han clasificado los principales tipos malicioso.	25%	3	Prueba escrita UD3
c) Se han realizado actualizaciones periódicas sistemas para corregir posibles vulnerabilidades.	14%	3	Práctica de aula UD3
d) Se ha verificado el origen y la autenticidad aplicaciones que se instalan en los sistemas.	11%	3	Batería tareas UD3

e) Se han instalado, probado y actualizado aplicaciones específicas para la detección y eliminación de software malicioso.	14%	3	Práctica de aula UD3
f) Se han aplicado técnicas de recuperación de datos.	18%	3	Prueba escrita UD3
TOTAL	100%		

Resultados de Aprendizaje	4. Asegura la privacidad de la información transmitida en redes informáticas describiendo vulnerabilidades e instalando software específico.		
Criterios de evaluación	Peso	UD	Instrumento de evaluación
a) Se ha identificado la necesidad de inventariar y controlar los servicios de red.	15%		Prueba escrita UD4
b) Se ha contrastado la incidencia de las técnicas de ingeniería social en los fraudes informáticos y robos de información.	15%	4	Prueba tipo test UD4
c) Se ha deducido la importancia de minimizar el volumen de tráfico generado por la publicidad y el correo no deseado.	10%	4	Prueba tipo test UD4
d) Se han aplicado medidas para evitar la monitorización de redes cableadas.	10%	4	Práctica de aula UD4
e) Se han clasificado y valorado las propiedades de seguridad de los protocolos usados en redes inalámbricas.	15%	4	Práctica de aula UD4
f) Se han descrito sistemas de identificación como la firma electrónica, certificado digital, entre otros.	10%	4	Batería tareas UD4
g) Se han utilizado sistemas de identificación como la firma electrónica, certificado digital, entre otros.	10%	4	Batería tareas UD4
h) Se ha instalado y configurado un cortafuegos en un equipo o servidor.	15%	4	Práctica de aula UD4
TOTAL	100%		

Resultados de Aprendizaje	5. Reconoce la legislación y normativa sobre seguridad y protección de datos analizando las repercusiones de su incumplimiento.		
Criterios de evaluación	Peso	UD	Instrumento de evaluación
a) Se ha descrito la legislación sobre protección de datos de carácter personal.	20%	5	Prueba escrita UD5
b) Se ha determinado la necesidad de controlar el acceso a la información personal almacenada.	25%	5	Batería tareas UD5

c) Se han identificado las figuras legales que intervienen en el tratamiento y mantenimiento de los ficheros de datos.	15%	5	Prueba escrita UD5
d) Se ha contrastado la obligación de poner a disposición de las personas los datos personales que les conciernen.	10%	5	Prueba escrita UD5
e) Se ha descrito la legislación actual sobre los servicios de la sociedad de la información y comercio electrónico.	15%	5	Prueba escrita UD5
f) Se han contrastado las normas sobre gestión de seguridad de la información.	15%	5	Batería tareas UD5
TOTAL	100%		

Recuperaciones

Los alumnos/as que inicialmente no alcancen los objetivos planteados, se beneficiarán de diferentes **actividades de refuerzo** donde se desarrollen los aspectos fundamentales de los contenidos y objetivos de las diferentes unidades didácticas.

Asimismo, en enero (tras la celebración de la primera sesión de evaluación parcial) y en marzo (antes de la sesión de evaluación parcial previa a la realización del módulo de FCT), el alumnado podrá **mejorar sus resultados obtenidos**, de forma que se volverán a utilizar los mismos instrumentos de evaluación, a excepción de las prácticas y trabajos grupales, que en este caso se realizarán de manera individual.

Una vez terminadas las evaluaciones parciales, los/as alumnos/as cuya **calificación final para el módulo sea menor de 5**, y por tanto tengan pendientes de superar algunos resultados de aprendizaje, así como también los estudiantes que deseen mejorar los resultados obtenidos, tendrán **obligación de asistir a clases** y continuar con las actividades lectivas **hasta el día 25 de junio**, dejando el módulo profesional de FCT para el curso siguiente.

En este **período de recuperación**, de marzo a junio, los estudiantes tendrán un número de horas de clase mayor o igual al 50% de las horas lectivas del módulo, es decir, 3 horas semanales. De esta forma, se realizarán diferentes **actividades de refuerzo** y se aplicarán de nuevo los **instrumentos de evaluación** considerados, a excepción de las actividades y prácticas grupales que se desarrollarán de forma individual, con el objetivo de que cada alumno/a pueda alcanzar los resultados de aprendizaje que tenga pendientes y obtener en última instancia una calificación final mayor o igual que 5 para el módulo profesional.