



1. **Código:** 35480 **Nombre:** Ciberseguridad
2. **Créditos:** 6,00 **--Teoría:** 3,00 **--Prácticas:** 3,00 **Carácter:** Obligatorio
- Titulación:** 2314-Máster Universitario en Ingeniería de Telecomunicación
- Módulo:** 1-Módulo de Tecnologías de Telecomunicación **Materia:** 2-Telemática
- Centro:** E.T.S.I. DE TELECOMUNICACIÓN
3. **Coordinador:** Aragonés Lozano, Mario
Departamento: COMUNICACIONES
4. **Bibliografía**

5. **Descripción general de la asignatura**

Objetivos de la asignatura

En la asignatura se partirá del análisis de incidentes de seguridad en sistemas reales para identificar las vulnerabilidades existentes en los mismos, los riesgos que éstas comportan y las tendencias actuales en materia de ciberataque. Para ello se valorarán las fuentes abiertas que ofrecen información relativa a las vulnerabilidades de los sistemas de información y a su explotación. Una vez definidos y estudiados los conceptos básicos como vulnerabilidad o incidente de seguridad, se abordará cómo gestionar de forma adecuada y eficiente incidentes de ciberseguridad en todas las fases del ciclo de vida del incidente, incluyendo las Amenazas Permanentes Avanzadas. La gestión de incidentes de seguridad incluirá el análisis de riesgos y la generación de planes de contingencia.

El objetivo de la asignatura es la adquisición de capacidades para el análisis y respuesta a los ciberincidentes en el contexto de un responsable del centro de operaciones de ciberseguridad. La gestión de ciberincidentes da una visión global y cohesionada de la seguridad al ser al momento en el coinciden los atacantes con los defensores y donde la mayoría de las técnicas tanto de ataque como de defensa adquieren su relevancia.

Contextualización de la asignatura

El contexto de la asignatura es la cada vez mayor peligrosidad e impacto de los incidentes de ciberseguridad, que afectan tanto a sistemas informáticos como a redes. En la asignatura se plantean las bases de las técnicas para abordar estos incidentes.

6. **Conocimientos recomendados**

La asignatura se basará en los conocimientos adquiridos durante los estudios del Grado en Ingeniería de Telecomunicaciones relacionados con en el campo de la telemática.

7. **Resultados**

Resultados fundamentales

G08(GE) Capacidad para la aplicación de los conocimientos adquiridos y resolver problemas en entornos nuevos o poco conocidos dentro de contextos más amplios y multidisciplinarios, siendo capaces de integrar conocimientos.

T06(ES) Capacidad para modelar, diseñar, implantar, gestionar, operar, administrar y mantener redes, servicios y contenidos.

G12(GE) Poseer habilidades para el aprendizaje continuado, autodirigido y autónomo.

Competencias transversales

(1) Compromiso social y medioambiental

- Actividades desarrolladas relacionadas con la adquisición de la competencia

Los alumnos, organizados por grupos de trabajo, plantearán la situación correspondiente a un ciberataque a una infraestructura crítica de depuración y distribución de aguas. Analizarán el efecto medioambiental y social de un incidente como este, y el valor que aporta la preparación para hacer frente a un ataque de este tipo

- Criterios de evaluación

Cada grupo expondrá de forma pública las conclusiones de la experiencia desarrollada.

Resultados de Aprendizaje Específicos

RA1.1 - Valorar las consecuencias éticas de las decisiones a tomar en una situación concreta, considerando el impacto en la sociedad y la responsabilidad en la práctica profesional.

(5) Responsabilidad y toma de decisiones

- Actividades desarrolladas relacionadas con la adquisición de la competencia

Los alumnos, organizados por grupos de trabajo, plantearán la situación correspondiente a la gestión de un incidente de ciberseguridad, con la correspondiente asignación de roles y distribución de tareas.

- Criterios de evaluación





7. Resultados

Competencias transversales

Cada grupo expondrá de forma pública las conclusiones de la experiencia desarrollada.

Resultados de Aprendizaje Específicos

RA5.4 - Aplicar de manera efectiva técnicas relacionadas con la búsqueda bibliográfica y el uso de fuentes de datos fiables u otros sistemas de información.

8. Unidades didácticas

1. Conceptos fundamentales de ciberseguridad
 1. Definiciones básicas
 2. Vulnerabilidades
 3. Amenazas
 4. Análisis de riesgos
2. Gestión de incidentes de ciberseguridad
 1. Incidentes de ciberseguridad
 2. Ciclo de vida de la gestión de incidentes de seguridad
 3. Coordinación y compartición de información
3. Respuesta frente a incidentes de ciberseguridad
 1. Preparación
 2. Detección y análisis
 3. Contención, erradicación y recuperación
 4. Lecciones aprendidas
4. Ciberinteligencia aplicada a la gestión de incidentes de ciberseguridad
 1. Ciberinteligencia
 2. Ciclo de vida de la generación de ciberinteligencia
 3. Fuentes de ciberinteligencia
5. Advanced Permanent Threats
 1. Caracterización de APTs
 2. Arquitectura de una APT
 3. Ciclo de vida de una APT
 4. Aplicación de técnicas de ciberinteligencia a APTs

9. Método de enseñanza-aprendizaje

A continuación se detalla el nombre de las sesiones de prácticas informáticas, teniendo cada una de ellas una duración de 2 horas.

Practica 01 - Virtualización

Practica 02 - Servidor

Practica 03 - Detección de intrusiones (parte 1)

Practica 04 - Detección de intrusiones (parte 2)

Practica 05 - Rúter Virtual

Practica 06 - Cortafuegos de nueva generación - Configuración de Red

Practica 07 - Cortafuegos de nueva generación - Políticas básicas

Practica 08 - Cortafuegos de nueva generación - Políticas avanzadas

Practica 09 - Cortafuegos de nueva generación - Perfiles de seguridad

Practica 10 - Honeypot SSH

Practica 11 - Analisis Wifi con Aircrack-ng

Practica 12 - Herramientas OSINT

<u>UD</u>	<u>TA</u>	<u>SE</u>	<u>PA</u>	<u>PL</u>	<u>PC</u>	<u>PI</u>	<u>EVA</u>	<u>TP</u>	<u>TNP</u>	<u>TOTAL HORAS</u>
1	4,00	--	--	--	--	--	--	4,00	8,00	12,00
2	4,00	--	--	--	--	--	--	4,00	12,00	16,00
3	8,00	--	--	--	--	12,00	--	20,00	40,00	60,00
4	8,00	--	--	--	--	12,00	--	20,00	20,00	40,00
5	6,00	--	6,00	--	--	--	--	12,00	40,00	52,00
TOTAL HORAS	30,00	--	6,00	--	--	24,00	--	60,00	120,00	180,00

UD: Unidad Didáctica. TA: Teoría de Aula. SE: Seminario. PA: Práctica de Aula. PL: Práctica de Laboratorio. PC: Práctica de Campo. PI: Práctica de Informática. EVA: Actividades de Evaluación. TP: Trabajo Presencial. TNP: Trabajo No Presencial.

Document signat electrònicament per
Documento firmado electrónicamente por
Electronically signed document by

UNIVERSITAT POLITÈCNICA DE VALÈNCIA

Data/Fecha/Date

06/06/2025

2 / 3

Autenticitat verificable mitjançant Codi Segur Verificació
Autenticidad verificable mediante Código Seguro Verificación
Original document can be verified by Secure Verification Code

ALUZEY0LXCP

<https://sede.upv.es/eVerificador>





10. Evaluación

Descripción

- (05) Trabajos académicos
(15) Prueba práctica de laboratorio/campo/informática/aula
(14) Prueba escrita

<u>Nº Actos</u>	<u>Peso (%)</u>
2	40
1	30
2	30

La asignatura se evaluará atendiendo a los siguientes criterios (alumnos con y sin dispensa):

- Dos exámenes (de desarrollo, test o híbridos) que tendrán un peso del 30% sobre la nota final en conjunto.
- Dos trabajos académicos relacionados con el contenido de la asignatura que tendrán un peso del 40% sobre la nota final en conjunto.
- Evaluación continua de las actividades prácticas de los alumnos que tendrá un peso del 30% sobre la nota final.

De acuerdo a las directrices de evaluación del primer curso del MUIT, en caso de no asistir al mínimo de asistencia a clase exigido, la evaluación se realizará atendiendo a los siguientes criterios (alumnos con y sin dispensa):

- Dos exámenes (de desarrollo, test o híbridos) que tendrán un peso del 70% sobre la nota final en conjunto.
- Evaluación continua de las actividades prácticas de los alumnos que tendrá un peso del 30% sobre la nota final.

La nota de los trabajos académicos podrá ser recuperada y se podrá subir volviendo a presentar los mismos. En caso de volverse a presentar éstos, se renuncia a la nota obtenida en la evaluación ordinaria.

La nota de las pruebas escritas puede ser recuperada y se puede subir presentándose a la prueba de evaluación extraordinaria. En caso de presentarse a dicha prueba, se renuncia a la nota obtenida en la evaluación ordinaria.

La evaluación continua de las actividades prácticas no es recuperable.

11. Porcentaje máximo de ausencia

<u>Actividad</u>	<u>Porcentaje</u>	<u>Observaciones</u>
Teoría Aula	20	
Teoría Seminario	0	
Práctica Aula	20	
Práctica Laboratorio	0	
Práctica Informática	20	
Práctica Campo	0	

