

**Resumen****DESCRIPCIÓN GENERAL DE LA ASIGNATURA**

La asignatura permite adquirir unos conocimientos fundamentales sobre las necesidades de seguridad y como se debe diseñar cualquier protocolo de comunicación si se desea que sea seguro. Para ello, se presentan los ataques más habituales en el diseño de protocolos (man-in-the-middle, ataques de DoS, y DDoS) y el uso de algoritmos criptográficos como elemento clave para garantizar la autenticación, integridad y confidencialidad de los documentos intercambiados. También se tratan las dificultades añadidas que conlleva las limitaciones de los dispositivos al diseñar un protocolo de seguridad; se analizará brevemente la situación en redes de sensores inalámbricas y en dispositivos RFID. Este entorno permitirá enlazar con otro aspecto clave: la privacidad del individuo. De la misma forma que un buen sistema de seguridad no debería ir en detrimento de la disponibilidad de servicios, tampoco debería ir en contra de la privacidad de los usuarios. Se presentarán distintas herramientas, y un nuevo entorno en el que se puede identificar fácilmente esta necesidad de privacidad: las votaciones por Internet. En este nuevo escenario se presentarán las distintas soluciones con ejemplos prácticos

**OBJETIVOS, COMPETENCIAS Y DESTREZAS****CONOCIMIENTOS RECOMENDADOS****SELECCIÓN Y ESTRUCTACIÓN LAS UNIDADES DIDÁCTICAS**

## 1. Seguridad en redes

## 1. Introducción a la seguridad en redes□

- Mecanismos de seguridad□
- Conceptos básicos de criptografía

## 2. Servicios de seguridad□

- Confidencialidad□
- Integridad□
- Autenticidad□
- Control de acceso□
- No repudio

## 3. PKI/PMI Infraestructuras de clave pública y gestión de privilegios

## 4. Seguridad en IP

## 5. Seguridad perimetral

## 6. Seguridad en pagos

## 7. Seguridad en comunicaciones de grupo

## 8. Seguridad en redes de sensores

## 9. Votaciones electrónicas seguras

**DISTRIBUCIÓN DE LAS UNIDADES DIDÁCTICAS****Unidad didáctica****Trab.**  
**Presencial****Trab.no**  
**Presencial**

Seguridad en redes

30,00

45,00

**Total:****30,00****45,00**

**METODOLOGIA DE ENSEÑANZA-APRENDIZAJE*****Autónomas***

<b><u>Nombre</u></b>	<b><u>Descripción</u></b>	<b><u>Horas</u></b>
Estudio teórico	Estudio de contenidos relacionados con las "clases teóricas": Incluye cualquier actividad de estudio que no se haya computado en el apartado anterior (estudiar exámenes, trabajo en biblioteca, lecturas complementarias, hacer problemas y ejercicios, etc.).	45
<b>Total:</b>		<b>45,00</b>

***Presenciales***

<b><u>Nombre</u></b>	<b><u>Descripción</u></b>	<b><u>Horas</u></b>
Clase magistral	Exposición de contenidos mediante presentación o explicación por parte de un profesor (posiblemente incluyendo demostraciones).	25
Aprendizaje basado en problemas	Enfoque educativo en el que los alumnos partiendo de problemas reales, aprenden a buscar la información necesaria para comprender dichos problemas y obtener soluciones; todo ello bajo la supervisión de un tutor.	5
<b>Total:</b>		<b>30,00</b>

**EVALUACIÓN**

<b><u>Nombre</u></b>	<b><u>Descripción</u></b>
Prueba escrita de respuesta abierta	Prueba cronometrada, efectuada bajo control, en la que el alumno construye su respuesta. Se le puede conceder o no el derecho a consultar material de apoyo.
Pruebas objetivas (tipo test)	Examen escrito estructurado con diversas preguntas o ítems en los que el alumno no elabora la respuesta; sólo ha de señalarla o completarla con elementos muy precisos.

**RECURSOS**

copia de las transparencias  
pizarra  
transparencias

**BIBLIOGRAFÍA**