

---

**Curso Académico: ( 2021 / 2022 )****Fecha de revisión: 10/06/2021 23:54:32**

---

**Departamento asignado a la asignatura: Departamento de Tecnología Electrónica****Coordinador/a: SANCHEZ REILLO, RAUL****Tipo: Obligatoria Créditos ECTS : 3.0****Curso : 1 Cuatrimestre : 2**

---

## REQUISITOS (ASIGNATURAS O MATERIAS CUYO CONOCIMIENTO SE PRESUPONE)

Ninguno más allá de los necesarios para ser admitido en el Máster.

## OBJETIVOS

CB6: Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación .

CG7: Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio.

CB8: Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios.

CB9: Que los estudiantes sepan comunicar sus conclusiones y los conocimientos y razones últimas que las sustentan a públicos especializados y no especializados de un modo claro y sin ambigüedades.

CB10: Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando.

CG2: Concebir, diseñar, poner en práctica y mantener un sistema global de Ciberdefensa en un contexto definido.

CG3: Elaborar concisa, clara y razonadamente documentos, planes y proyectos de trabajo en el ámbito de la Ciberseguridad.

CG4: Conocer la normativa técnica y las disposiciones legales de aplicación en la materia de ciberseguridad, sus implicaciones en el diseño de sistemas y en la aplicación de herramientas de seguridad.

CE4: Analizar sistemas para encontrar evidencias de ataques en los mismos y adoptar las medidas precisas para mantener la cadena de custodia de dichas evidencias.

CE5: Aplicar los servicios, mecanismos y protocolos de seguridad oportunos en un caso concreto.

CE6: Diseñar y evaluar arquitecturas de seguridad de sistemas y redes.

CE7: Conocer y aplicar los mecanismos de cifrado y esteganografiado pertinentes para proteger los datos residentes en un sistema o en tránsito por una red.

CE8: Analizar los riesgos de la introducción de dispositivos personales en un entorno profesional. Conocer y aplicar las medidas para controlar dichos riesgos.

## DESCRIPCIÓN DE CONTENIDOS: PROGRAMA

En esta asignatura el alumno adquirirá los conocimientos técnicos sobre los procesos de identificación y autenticación. Se familiarizará con distintos esquemas y dispositivos de identificación y autenticación, incluyendo las principales técnicas biométricas utilizadas hoy en día y los sistemas de gestión de identidades. Finalmente se introducirán conceptos claves de privacidad y legislación relacionados con los procesos de identificación y manejo de información personal.

Programa:

1. Autenticación de usuarios
  - 1.1. Conceptos y definiciones
  - 1.2. Esquemas de autenticación. Autenticación de varios factores

- 1.3. Autenticación robusta. Autenticación mediante la firma digital
- 1.4. Análisis de seguridad
- 1.5. Arquitecturas de autenticación. Kerberos
  
2. Identificación biométrica
  - 2.1. Definiciones y principios de funcionamiento
  - 2.2. Sistemas biométricos
  - 2.3. Seguridad, privacidad y aspectos prácticos
  
3. Gestión de identidades
  - 3.1. Ciclo de vida de la identidad digital
  - 3.2. Gestión de la identidad en sistemas distribuidos
  - 3.3. Estándares y sistemas federados
  
4. Aspectos éticos y legislación asociada a la privacidad.
  - 4.1. Normativa sobre identificación
  - 4.2. LOPD y Reglamento de desarrollo

## ACTIVIDADES FORMATIVAS, METODOLOGÍA A UTILIZAR Y RÉGIMEN DE TUTORÍAS

### ACTIVIDADES FORMATIVAS

- Clase teórica
- Clases teórico prácticas
- Tutorías
- Trabajo en grupo
- Trabajo individual del estudiante

### METODOLOGÍAS DOCENTES

- Exposiciones en clase del profesor con soporte de medios informáticos y audiovisuales, en las que se desarrollan los conceptos principales de la materia y se proporciona la bibliografía para complementar el aprendizaje de los alumnos.
- Lectura crítica de textos recomendados por el profesor de la asignatura:
- Artículos de prensa, informes, manuales y/o artículos académicos, bien para su posterior discusión en clase, bien para ampliar y consolidar los conocimientos de la asignatura.
- Resolución de casos prácticos, problemas, etc. planteados por el profesor de manera individual o en grupo
- Exposición y discusión en clase, bajo la moderación del profesor de temas relacionados con el contenido de la materia, así como de casos prácticos
- Elaboración de trabajos e informes de manera individual o en grupo

## SISTEMA DE EVALUACIÓN

<b>Peso porcentual del Examen/Prueba Final:</b>	50
<b>Peso porcentual del resto de la evaluación:</b>	50

Los Trabajos Prácticos solicitados a los alumnos, así como el examen serán puntuados bajo el siguiente baremo:

- P1 (Tarjetas): 10%
- P2 (Biometría): 20%
- P3 (Gestión de Identidad): 20%

Examen: 50%, requiriendo una nota mínima de 3 sobre 10 para aprobar la asignatura.

## BIBLIOGRAFÍA BÁSICA

- A. Sigüenza, M. Tapiador Tecnologías biométricas aplicadas a la seguridad, Ra-Ma, 2005
- Anil K. Jain Biometrics : personal identification in networked society, Kluwer Academic, 2005
- Anil K. Jain, Raúl Sánchez Reillo, et. al. Encyclopedia of Biometrics, Springer, 2015

- Finkenzeller, Klaus. RFID handbook : fundamentals and applications in contacless smart cards and identification, Wiles and Sons.
- Li, Stan Z. Encyclopedia of Biometrics, vols. 1 and 2, Springer, 2009
- Patrizio Campisi Security and Privacy in Biometrics, Springer, 2013
- Rankl, Wolfgang Smart card handbook, John & Wiley & Sons.
- Raúl Sánchez Reíllo, et. al. User-Centric Privacy and Security in Biometrics, IET, 2017
- Raúl Sánchez Reíllo, et. al. Iris and Periocular Biometric Recognition , IET, 2017
- Wayman, James. Biometric systems : technology, design, and performance evaluation., Springer.