# Protección de Datos

**Curso Académico: ( 2021 / 2022 )** **Fecha de revisión: 29-06-2021**

**Departamento asignado a la asignatura: Departamento de Ingeniería Telemática**

**Coordinador/a: LOPEZ GARCIA, SERGIO**

**Tipo: Obligatoria Créditos ECTS : 3.0**

**Curso : 1 Cuatrimestre : 1**

## OBJETIVOS

COMPETENCIAS Y RESULTADOS DEL APRENDIZAJE
En relación a las competencias, durante el curso se trabajarán las siguientes:

- 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.
- 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.
- Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando.
- Elaborar concisa, clara y razonadamente documentos, planes y proyectos de trabajo en el ámbito de la Ciberseguridad.
- Aplicar los servicios, mecanismos y protocolos de seguridad oportunos en un caso concreto.
- Diseñar y evaluar arquitecturas de seguridad de sistemas y redes.
- Conocer y aplicar los mecanismos de cifrado y esteganografiado pertinentes para proteger los datos residentes en un sistema o en tránsito por una red.

Con respecto a los resultados del aprendizaje, a la superación de esta materia los estudiantes serán capaces de:
- Dado un sistema con unos requisitos de seguridad establecidos, proponer mecanismos y protocolos necesarios para proporcionar algunos de los servicios básicos de seguridad: autenticación, autorización, privacidad y control de acceso. Dar una medida de su eficacia y limitaciones.
- Diseñar y evaluar medidas apropiadas para la identificación y autenticación de usuarios, así como la gestión de las identidades y las autorizaciones asociadas.

## DESCRIPCIÓN DE CONTENIDOS: PROGRAMA

PROGRAMA

Esta asignatura cubre los diferentes aspectos relacionados con la protección de la información, centrándose especialmente en los servicios de confidencialidad, integridad y autenticidad de la información intercambiada o almacenada. La asignatura aborda dichos aspectos desde un punto de vista eminentemente práctico, mediante la realización de un caso de estudio a lo largo del curso consistente en el desarrollo de una aplicación de protección de datos.

El programa de la asignatura se divide en cuatro partes:

* Parte I: introducción.
  - Presentación del curso: temario, normativa, descripción del caso de estudio práctico.
  - Introducción a la protección de la información: definiciones, dimensiones de la seguridad de la información.
  - Clasificación de los sistemas de cifrado (simétrico/asimétrico)

* Parte II: cifrado simétrico
  - Cifradores de bloque y de flujo.
  - Algoritmos de cifrado: DES, modos de operación, 2DES, 3DES, AES.
  - Gestión de claves criptográficas.

* Parte III: Cifrado asimétrico
  - RSA, Diffie-Hellman, ECC.

* Parte IV: autenticación y firma digital

- Autenticación y funciones unidireccionales: funciones hash criptográficas, códigos de Autenticación de Mensajes (MAC).
- Firma Digital. Estándares.
- Certificados digitales e infraestructuras de clave pública (PKI) (certificados digitales. ITU-T X.509v3, Autoridades de confianza (CA) e infraestructuras de clave pública (PKI), legislación de firma electrónica.

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

ACTIVIDADES FORMATIVAS

La metodología docente incluirá:

- 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

CRITERIOS DE EVALUACIÓN

La nota de la asignatura está formada por los siguientes bloques:

- Caso de estudio práctico (evaluación continua): 60%.
- Examen final: 40%.

Para aprobar la asignatura es necesario obtener al menos 50 puntos en la suma de los dos bloques (sin ser necesario un mínimo de puntos en ninguno de los mismos).

De acuerdo con la normativa de evaluación continua establecida por la Universidad, en la convocatoria ordinaria se permitirá a los estudiantes que no hayan seguido la evaluación continua realizar un examen final con un valor del 60% de la asignatura. En la convocatoria extraordinaria, el estudiante tendrá derecho a ser calificado mediante un examen final con un valor del 100% de la asignatura.

| | |
|---|---|
| **Peso porcentual del Examen Final:** | 40 |
| **Peso porcentual del resto de la evaluación:** | 60 |

## BIBLIOGRAFÍA BÁSICA


- Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone Handbook of applied cryptography, http://www.cacr.math.uwaterloo.ca/hac/, 2001
- C. Kaufman, R. Perlman, M. Speciner, E. Cliffs. Network security : private communication in a public world , Prentice Hall, 1995
- Manuel José Lucena López Criptografía y seguridad en computadores, Universidad de Jaén, 2011
- Stallings, William Cryptography and network security. Principles and Practice. Sixth Edition, Prentice Hall, 2014