

**GUÍA DOCENTE**  
**EXPERIENCIA PILOTO DE APLICACIÓN DEL SISTEMA EUROPEO DE CRÉDITOS (ECTS)**  
**UNIVERSIDADES ANDALUZAS**

**TITULACIÓN: INGENIERÍA TÉCNICA EN INFORMÁTICA DE GESTIÓN**  
**(MODALIDAD PRESENCIAL)**

**DATOS BÁSICOS DE LA ASIGNATURA**

NOMBRE: SEGURIDAD Y MEDIOS DE PAGO

CÓDIGO: 939

AÑO DE PLAN DE ESTUDIO: 2004

TIPO (troncal/obligatoria/optativa): Optativa

Créditos totales (LRU/ECTS):  
4.5

Créditos LRU/ECTS teóricos:  
2.5

Créditos LRU/ECTS prácticos:  
2

CURSO: 3º

CUATRIMESTRE(S): 1C

CICLO: 1º

**EQUIPO DOCENTE**

**Responsable / Coordinador de la asignatura:**

NOMBRE: Francisco Javier Duque Pintor

CENTRO/DEPARTAMENTO: Escuela Politécnica Superior / Deporte e Informática

ÁREA: Lenguajes y Sistemas Informáticos

CATEGORÍA:

| POD |                   | GRUPOS | CRÉDITOS | TOTAL |
|-----|-------------------|--------|----------|-------|
|     | Gran Grupo        |        |          |       |
|     | Grupo de Docencia |        |          |       |
|     | Activ. Dirigidas  |        |          |       |

HORARIO DE TUTORÍAS:

Nº DESPACHO:

E-MAIL:

TF: +34

URL WEB:

**Otros profesores:**

NOMBRE: Eloy R. Sanz Tapia

CENTRO/DEPARTAMENTO: Escuela Politécnica Superior / Deporte e Informática

ÁREA: Lenguajes y Sistemas Informáticos

CATEGORÍA:

| POD |                   | GRUPOS | CRÉDITOS | TOTAL |
|-----|-------------------|--------|----------|-------|
|     | Gran Grupo        |        |          |       |
|     | Grupo de Docencia |        |          |       |
|     | Activ. Dirigidas  |        |          |       |

HORARIO DE TUTORÍAS:

Nº DESPACHO:

E-MAIL:

TF: +34

URL WEB:

## LA ASIGNATURA EN EL PROGRAMA FORMATIVO

### 1. DESCRIPTOR.

Infraestructura pública de seguridad, criptografía y esteganografía, certificación, protocolos, claves secretas y públicas, claves simétricas y asimétricas, e-Cash, privacidad.

### 2. UBICACIÓN EN EL PROGRAMA FORMATIVO.

#### 2.1. PRERREQUISITOS:

Ninguno.

#### 2.2. CONTEXTO DENTRO DE LA TITULACIÓN:

La asignatura de Seguridad y medios de pago se posiciona como un complemento formativo a las asignaturas de Redes Telemáticas y Seguridad Informática. En esta asignatura se tratan con profundidad aspectos relacionados con la seguridad en redes y, en concreto, temas de criptografías y se profundiza en protocolos seguros tales como SSL. Esta asignatura tiene como reto el proporcionar al alumno de los conocimientos suficientes para el diseño de sistemas de pago seguros, dado el auge que se está dando en los pagos vía internet

#### 2.3. RECOMENDACIONES:

Ninguna.

### 3. LA ASIGNATURA EN LA ADQUISICIÓN DE COMPETENCIAS.

#### 3.1. COMPETENCIAS TRANSVERSALES/GENÉRICAS:

- Conocimientos generales básicos.
- Solidez en los conocimientos básicos de la profesión.
- Resolución de problemas.
- Capacidad de aprender.
- Habilidad para trabajar de forma autónoma.

#### 3.2. COMPETENCIAS ESPECÍFICAS:

- **Cognitivas (Saber):** Enseñar al alumno unos conocimientos generales básicos sobre seguridad en medios de pago: algoritmos de encriptación, tecnologías y legislación.
- **Procedimentales/Instrumentales (Saber hacer):** Enseñar al alumno los métodos actuales para la realización de pagos seguros por internet. Enseñar al alumno el procedimiento necesario para el diseño de sitios web que permitan este tipo de pago de manera fiable.
- **Actitudinales (Ser):** Fomentar la disciplina en el diseño de sitios seguros para el pago electrónico, siguiendo planteamientos que desarrollen la capacidad analítica del alumno para enfrentarse a problemas reales.

### 4. OBJETIVOS.

- Conocer las técnicas de seguridad existentes en relación a los medios de pago electrónico
- Conocer los estándares de seguridad.
- Adquirir conocimientos suficientes para el desarrollo de entornos web seguros.

#### DISTRIBUCIÓN DEL TRABAJO PRESENCIAL.

|                | Gran Grupo | Grupo de Docencia | Actividades dirigidas<br>(seminarios) |
|----------------|------------|-------------------|---------------------------------------|
| Nº de grupos   | 1          | 2                 | 2                                     |
| Nº de horas    | 12         | 12                | 4                                     |
| Nº de sesiones | 12         | 8                 | 2                                     |

## 5. METODOLOGÍA.

### NÚMERO TOTAL DE HORAS DE TRABAJO DEL ALUMNO: 116

#### PRIMER SEMESTRE: 116 horas de trabajo

Nº de Horas:

- Enseñanzas básicas (Gran Grupo): 12
- Enseñanzas prácticas y de desarrollo (Grupo de Docencia): 12
- Actividades académicas dirigidas (Seminarios-Grupo de Trabajo): 4
- Tutorías especializadas (presenciales o virtuales):
  - A) Colectivas:
  - B) Individuales:
- Trabajo personal autónomo:
  - A) Horas de estudio de enseñanzas básicas: 24
  - B) Horas de estudio-preparación de las enseñanzas prácticas y de desarrollo: 48
  - C) Horas de trabajo personal o en grupo derivadas de las actividades académicas dirigidas: 14
- Otras actividades (visitas, excursiones, etc.)
- Realización de pruebas de evaluación y/o exámenes:
  - A) Prueba de evaluación y/o exámenes escritos: 2
  - B) Pruebas de evaluación y/o exámenes orales (control del Trabajo Personal)

**6. TÉCNICAS DOCENTES.** (Señale con una X las técnicas que va a utilizar en el desarrollo de su asignatura. Puede señalar más de una).

|                                  |                        |                                     |
|----------------------------------|------------------------|-------------------------------------|
| Sesiones académicas teóricas: X  | Exposición y debate: X | Tutorías especializadas: X          |
| Sesiones académicas prácticas: X | Visitas y excursiones: | Controles de lecturas obligatorias: |

Otras (especificar):

#### DESARROLLO Y JUSTIFICACIÓN:

Todas las Actividades Prácticas y de Desarrollo así como las Actividades Académicas Dirigidas llevarán asociada una documentación que se proporcionará al alumno a través de la página Web de la asignatura dentro del aula virtual WebCT.

**7. BLOQUES TEMÁTICOS.** (Dividir el temario en grandes bloques temáticos; no hay número mínimo ni máximo).

- BLOQUE 1: INTRODUCCIÓN A LOS MEDIOS DE PAGO
- BLOQUE 2: SEGURIDAD Y TECNOLOGÍAS

## 8. BIBLIOGRAFÍA.

### 8.1 GENERAL:

- Apuntes del curso proporcionados por los profesores de la asignatura
- Simson Garfinkel y Gene Spafford: Seguridad y Comercio en el Web. Editorial Osborne McGraw-Hill, 1999.

### 8.2 ESPECÍFICA: (con remisiones concretas en lo posible)

A lo largo del curso se irán dando referencias concretas que deberán ser usadas para complementar las explicaciones que se den en clase.

## 9. TÉCNICAS DE EVALUACIÓN.

- La evaluación se basará principalmente en los conocimientos adquiridos tanto en clase de teoría como en aula de informática. La participación también será evaluada.
- Para la realización de cualquier prueba evaluable no se permitirá el uso o consulta de documentación, salvo indicación expresa del profesor en convocatoria oficial

### Criterios de evaluación y calificación: (referidos a las competencias trabajadas durante el curso)

La nota estará comprendida entre 0 y 10 puntos, los cuales se acumularán en función de los porcentajes descritos a continuación:

- Enseñanzas básicas: 30%
- Actividades prácticas y de desarrollo: 45%
- Actividades académicas dirigidas: 25%

Nota: Título II. Capítulo II. Artículo 14.2 y 14.3 de la Normativa de Régimen Académico y de Evaluación del Alumnado (aprobada en Consejo de Gobierno de la UPO el 18 de julio de 2006): "En la realización de trabajos, el **plagio** y la utilización de material no original, incluido aquél obtenido a través de Internet, sin indicación expresa de su procedencia y, si es el caso, permiso de su autor, podrá ser considerada causa de calificación de **suspenso** de la asignatura, sin perjuicio de que pueda derivar en **sanción académica**."

Corresponderá a la Dirección del Departamento responsable de la asignatura, oídos el profesorado responsable de la misma, los estudiantes afectados y cualquier otra instancia académica requerida por la Dirección del Departamento, decidir sobre la posibilidad de solicitar la apertura del correspondiente **expediente sancionador**".

| <b>10. ORGANIZACIÓN DOCENTE SEMANAL.</b> (Sólo hay que indicar el número de horas que a ese tipo de sesión va a dedicar el estudiante cada semana) |   |  |   |                                     |  |   |          |                            |
|--|---|--|---|-------------------------------------|--|---|----------|----------------------------|
| SEMANA   | Enseñanzas básicas<br>(Gran Grupo)<br>Nº de horas | Enseñanzas básicas y de desarrollo<br>(Grupo de Docencia)<br>Nº de horas | Actividades académicas dirigidas<br>(Seminarios-Grupos de Trabajo)<br>Nº de horas | Visita y excursiones<br>Nº de horas | Tutorías especializadas<br>Nº de horas | Control de lecturas obligatorias<br>Nº de horas | Exámenes | Temas del temario a tratar |
| <b>Primer Cuatrimestre</b>   |   |  |   |                                     |  |   |          |                            |
| <b>SEMANA 1 (26 sep – 30 sep)</b>  | 1   |  |   |                                     |  |   |          | T1(1)                      |
| <b>SEMANA 2 (3-7 oct)</b>  | 1   | 1.5  |   |                                     |  |   |          | T1(2) / APD1               |
| <b>SEMANA 3 (10,12-14 oct)</b>   | 1   |  |   |                                     |  |   |          | T2                         |
| <b>SEMANA 4 (17-21 oct)</b>  | 1   | 1.5  |   |                                     |  |   |          | T3 / APD2                  |
| <b>SEMANA 5 (24-28 oct)</b>  | 1   | 1.5  | 2   |                                     |  |   |          | T4(1) / APD3 / AAD1        |
| <b>SEMANA 6 (31 oct,1-4 nov)</b>   |   |  |   |                                     |  |   |          |                            |
| <b>SEMANA 7 (7-11 nov)</b>   | 1   |  |   |                                     |  |   |          | T4(2)                      |
| <b>SEMANA 8 (14-18 nov)</b>  | 1   | 1.5  |   |                                     |  |   |          | T4(3) / APD4               |
| <b>SEMANA 9 (21-25 nov)</b>  | 1   |  |   |                                     |  |   |          | T5                         |
| <b>SEMANA 10 (28 nov - 2 dic)</b>  | 1   | 1.5  | 2   |                                     |  |   |          | T6(1) / APD5 / AAD2        |
| <b>SEMANA 11 (5,6,7,8-9 dic)</b>   |   |  |   |                                     |  |   |          | T6(2)                      |
| <b>SEMANA 12 (12-16 dic)</b>   | 1   | 1.5  |   |                                     |  |   |          | T6(3) / APD6               |
| <b>SEMANA 13 (19,23 dic)</b>   | 1   |  |   |                                     |  |   |          | T7(1)                      |
| <b>SEMANA 14 (9-13 ene)</b>  | 1   | 1.5  |   |                                     |  |   |          | T7 (2) / APD7              |
| <b>SEMANA 15 (16-20 ene)</b>   |   | 1.5  |   |                                     |  |   |          | APD8                       |
| <b>SEMANA 16, 17 y 18 (23 ene – 10 feb)</b>  |   |  |   |                                     |  |   |          |                            |
| <b>Evaluaciones finales</b>  |   |  |   |                                     |  |   |          |                            |

|  |
|--|
| <b>11. TEMARIO DESARROLLADO.</b> (Con indicación de las competencias que se van a trabajar en cada tema).  |
| <b>BLOQUE 1: INTRODUCCIÓN A LOS MEDIOS DE PAGO</b>   |
| <b>Tema 1. Introducción a los medios de pago</b>   |
| 1.1 Conceptos sobre comercio electrónico<br>1.2 Definición de medios de pago<br>1.3 Evolución de los medios de pago  |
| <b>Tema 2. Conceptos de seguridad de la información</b>  |
| 2.1 Definiciones<br>2.2 Aspectos de la seguridad<br>2.3 Análisis y gestión de riesgos<br>2.4 Controles de seguridad  |
| <b>Tema 3. Aspectos de seguridad en medios de pago</b>   |
| 3.1 Aspectos de seguridad aplicables a los medios de pago<br>3.2 Principales vulnerabilidades<br>3.3 Casos reales  |
| <b>BLOQUE 2: SEGURIDAD Y TECNOLOGÍAS</b>   |
| <b>Tema 4. Criptografía</b>  |
| 4.1 Introducción<br>4.2 Criptografía de la clave privada (clásica y moderna)<br>4.3 Criptografía de clave pública<br>4.5 Funciones hash<br>4.6 Firma electrónica<br>4.7 Certificados digitales<br>4.8 Infraestructura de clave pública (PKI) |
| <b>Tema 5. Protocolos seguros</b>  |
| 5.1 Repaso: TCP/IP, HTTP<br>5.2 Mantenimiento de sesiones<br>5.3 SSL/TLS<br>5.4 SET  |
| <b>Tema 6. Tecnologías para medios de pago</b>   |
| 6.1 Tarjetas de crédito/débito<br>6.2 Características, identificación<br>6.3 TPV y TPV virtuales: configuración y protocolos<br>6.4 Micropagos<br>6.5 E-cash<br>6.6 Pagos mediante teléfonos móviles<br>6.7 RFID                             |

|  |
|--|
| <b>Tema 7. Legislación aplicable</b>   |
| 7.1 LSSI<br>7.2 LFE<br>7.3 LOPD<br>7.4 PCI-DSS   |
| <b>ACTIVIDADES PRÁCTICAS Y DE DESARROLLO</b>   |
| APD1. Criptografía: métodos clásicos<br>APD2. Criptografía moderna de clave privada<br>APD3. Criptografía de clave pública<br>APD4. SSL<br>APD5. Certificados digitales<br>APD6. Firma electrónica, PKI<br>APD7. Vulnerabilidades (I): keyloggers<br>APD8. Vulnerabilidades (II): sniffers / secuestro de sesión |
| <b>ACTIVIDADES ACADÉMICAS DIRIGIDAS</b>  |
| AAD 1: Criptografía<br>AAD 2: Protocolos de seguridad  |

**12. MECANISMOS DE CONTROL Y SEGUIMIENTO.** (Al margen de los contemplados a nivel general para toda la Experiencia Piloto, se recogerán aquí los mecanismos concretos que los docentes propongan para el seguimiento de cada asignatura).