# Guía Docente

Modalidad A Distancia

# Seguridad en Redes de Computadores

## Curso 2017/18

## Curso de adaptación al Grado en Ingeniería de Sistemas de Información

UCAV

www.ucavila.es

## 1 Datos descriptivos de la Asignatura

| | |
|---|---|
| **Nombre:** | SEGURIDAD EN REDES DE COMPUTADORES |
| **Carácter:** | OPTATIVA |
| **Código:** | 40304GH |
| **Curso:** | 4º |
| **Duración (Semestral/Anual):** | SEMESTRAL |
| **Nº Créditos ECTS:** | 6 |
| **Prerrequisitos:** | NINGUNO |
| **Responsable docente:** | FERNANDO PACHÓN GARCÍA<br>Doctor en Física,<br>Ingeniero de Telecomunicación. |
| **Email:** | fernando.pachon@ucavila.es |
| **Departamento (Área Departamental):** | TECNÓLOGICO |
| **Lengua en la que se imparte:** | ESPAÑOL |
| **Módulo:** | **CONTENIDOS COMUNES A LA INGENIERÍA INFORMÁTICA** |
| **Materia:** | **SISTEMAS OPERATIVOS Y REDES** |

# 2 Objetivos y competencias

## 2.1. COMPETENCIAS BÁSICAS Y GENERALES

- Capacidad para concebir, redactar, organizar, planificar, desarrollar y firmar proyectos en el ámbito de la ingeniería en informática que tengan por objeto la concepción, el desarrollo o la explotación de sistemas, servicios y aplicaciones informáticas.
- Capacidad para diseñar, desarrollar, evaluar y asegurar la accesibilidad, ergonomía, usabilidad y seguridad de los sistemas, servicios y aplicaciones informáticas, así como de la información que gestionan.
- Capacidad para definir, evaluar y seleccionar plataformas hardware y software para el desarrollo y la ejecución de sistemas, servicios y aplicaciones informáticas.
- Capacidad para concebir y desarrollar sistemas o arquitecturas informáticas centralizadas o distribuidas integrando hardware, software y redes.
- Conocimiento de las materias básicas y tecnologías, que capaciten para el aprendizaje y desarrollo de nuevos métodos y tecnologías, así como las que les doten de una gran versatilidad para adaptarse a nuevas situaciones.
- Capacidad para resolver problemas con iniciativa, toma de decisiones, autonomía y creatividad. Capacidad para saber comunicar y transmitir los conocimientos, habilidades y destrezas de la profesión de Ingeniero Técnico en Informática.

## 2.2. COMPETENCIAS ESPECÍFICAS

- Capacidad para diseñar, desarrollar, seleccionar y evaluar aplicaciones y sistemas informáticos, asegurando su fiabilidad,

seguridad y calidad, conforme a principios éticos y a la legislación y normativa vigente.

- Capacidad para participar activamente en la especificación, diseño, implementación y mantenimiento de los sistemas de información y comunicación.
- Capacidad para seleccionar, diseñar, desplegar, integrar y gestionar redes e infraestructuras de comunicaciones en una organización.

### 2.3. RESULTADOS DE APRENDIZAJE

- Conocimiento y aplicación de las características, funcionalidades y estructura de los Sistemas Distribuidos, las Redes de Computadores e Internet y diseñar e implementar aplicaciones basadas en ellas.
- Conocimiento, administración y mantenimiento sistemas, servicios y aplicaciones informáticas.

## 3 Contenidos de la asignatura

### 3.1. PROGRAMA

UNIDAD 1. SEGURIDAD EN SISTEMAS INFORMÁTICOS.

1.1. Seguridad de la información

1.2. Seguridad en el tratamiento automatizado de la Información

1.3. Servicios de seguridad

1.4. Políticas de seguridad

1.5. Amenazas

1.6. Seguridad en Redes

UNIDAD 2. CONFIDENCIALIDAD: CRIPTOGRAFÍA.

2.1. Introducción a la Criptografía

2.1.2. Principios criptográficos fundamentales

2.2. Criptografía clásica

2.2.1. Cifrado por sustitución

2.2.2. Cifrado por transposición

2.3. Criptografía moderna

2.3.1. Cifrado con clave simétrica

2.3.2. Cifrado con clave asimétrica

2.3.3. Localización de los dispositivos de cifrado

2.3.4. Comentario clave asimétrica vs clave simétrica

UNIDAD 3. IDENTIFICACIÓN: PROTOCOLOS DE AUTENTICACIÓN

3.1. Validación de la identificación: autenticación

3.2. Validación de identificación de clave secreta

3.2.1. Validación de identificación basada en clave secreta compartida

3.2.2. Establecimiento de una clave compartida: intercambio de claves DiffieHellman

3.2.3. Validación de identificación usando un centro de distribución de claves

3.2.4. Protocolo de autenticación Kerberos

3.3. Validación de identificación usando criptografía de clave pública

3.3.1. TACACS, XTACACS, TACACS+, RADIUS y otros

UNIDAD 4. INTEGRIDAD Y NO REPUDIO

4.1. Control de integridad

4.1.1. Compendio de mensaje MD5

4.1.2. Compendio de mensaje SHA

4.2. No repudio: firmas digitales

4.2.1. Firmas de clave secreta

4.2.2. Firmas de clave pública

4.3. El certificado digital

4.4. Aplicaciones Seguras

4.4.1. El protocolo SSH

4.4.2. Confidencialidad del correo electrónico

4.4.3. Aplicaciones seguras basadas en tarjetas inteligentes y PKI (Public Key infraestructura)

4.4.4. Secure Socket Layer

UNIDAD 5. MECANISMOS DE PROTECCIÓN DE REDES

5.1. Seguridad en Redes

5.1.1. Peligros y modos de ataque

5.1.2. Elementos de seguridad

5.2. Seguridad basada en criptografía

5.2.1. Túneles

5.2.2. Redes Privadas Virtuales (VPNs)

5.2.3. IPSEC

5.3. Seguridad en red perimetral

5.3.1. Cortafuegos (firewalls)

5.3.2. Traducción de direcciones (NAT)

5.3.3. Detección de intrusos o IDS (Intrusión Detection System)

5.4. Seguridad en red basada en sistema centralizado

5.4.1. Encapsuladores (proxies) y pasarelas

5.5. Seguridad en redes inalábricas

5.5.1. WEP

5.5.2. WPA

5.5.3. WPA

UNIDAD 6. DETECCIÓN DE INTRUSOS

6.1. Necesidad de mecanismos adicionales en la prevención y protección

6.2. Sistemas de detección de intrusos

6.2.1. Arquitectura general de un sistema de detección de intrusiones

6.3. Escáneres de vulnerabilidades

6.4. Sistemas de Decepción

6.4.1. Equipos de decepción

6.5. Prevención de intrusos

6.5.1. Sistemas de detección en línea

6.5.2. Sistemas cortafuegos a nivel de aplicación

6.6. Detección de ataques distribuidos

6.6.1. Esquemas tradicionales

6.6.2. Análisis descentralizado

6.6.3. Análisis descentralizado mediante código móvil

6.6.4. Análisis descentralizado mediante paso de mensajes

## 3.2. BIBLIOGRAFÍA

- Manual de la asignatura. RODRIGUEZ LLORENTE, Javier (2011). Seguridad en Redes de Computadores. Avila: Servicio de Publicaciones de la Universidad Católica de Avila.

- AREITIO, J. (2012). Seguridad de la Información: Redes, Informática y Sistemas de Información. Cengage Learning. Madrid.
- CARRACEDO GALLARDO, Justo. (2004). Seguridad en Redes Telemáticas. McGraw Hill, 2004
- RAMIÓ AGUIRRE, Jorge. Libro Electrónico de Seguridad Informática y Criptografía. Versión 4.1 publicada en Internet y de libre distribución. http://www.lpsi.eui.upm.es/SInformatica/diapositivas.htm
- Libros electrónicos de libre distribución que puede descargar desde "Criptored" http://www.criptored.upm.es/paginas/docencia.htm#librose


## 4 Indicaciones metodológicas

La asignatura se desarrollará a través de los siguientes métodos y técnicas generales, que se aplicarán diferencialmente según las características propias de la asignatura:

- **Manual de la asignatura y sistema de tutorización online:** El alumno tendrá a su disposición un manual de estudio de la asignatura elaborado por el profesor de la misma. Además contará con la tutorización personalizada del profesor de la asignatura, como principal responsable docente.

- **Estudio personal dirigido:** el alumno acometerá de forma individual el estudio de la asignatura de modo que le permita adquirir las competencias de la misma.

- **Ejercicios y problemas prácticos:** Se propondrá al alumno la realización de ejercicios y/o casos prácticos para que resuelva y lo confronte con las soluciones dadas por el profesor y que encontrará en la plataforma virtual.

- **Trabajo académico dirigido**: el alumno realizará individualmente un trabajo académico individual conforme a las indicaciones y enunciado que el profesor mediante la plataforma virtual facilitará al alumno, el cual deberá realizar y entregar para su corrección en los periodos establecidos por el profesor.

- **Actividades de evaluación.**

## 5 Evaluación

La evaluación es un componente fundamental de la formación del alumno. Está compuesta por un examen final escrito y la evaluación continua, que consta de ejercicios y actividades evaluables.

La evaluación de esta asignatura se realiza mediante la media del examen (valorado en un 60%) y la realización de un trabajo obligatorio individual (con valor del 40%).

- Examen (60 % de la nota final)

La superación de dicho examen constituye un requisito indispensable para la superación de la asignatura. El alumno deberá tener en el examen al menos un 5 para poder realizar la ponderación de notas. El alumno con nota inferior se considerará suspenso. El alumno dispondrá de dos convocatorias de examen por curso académico.

No se guardará la nota del examen, si éste estuviera aprobado, para una convocatoria posterior.

- Trabajo obligatorio (40% de la nota final)

No es necesario superar el trabajo obligatorio para superar la asignatura. El trabajo obligatorio constará de una serie de ejercicios o trabajo teórico (35% de la nota total) y de prácticas obligatorias presenciales (5% de la nota total). En el caso de tener el trabajo obligatorio superado y no aprobar el examen, se guardará su nota hasta la segunda convocatoria de examen perteneciente al curso académico actual.

No se admitirán trabajos fuera de la fecha límite de entrega, que será comunicada al alumno con suficiente antelación. Con la no

presentación del trabajo obligatorio se considerará suspensa la asignatura, independientemente de la nota obtenida en el examen.

- Práctica voluntaria (10% extra en la nota final)

Se propondrá una práctica voluntaria adicional que computará un 10 % extra de la calificación final. En realidad servirá para subir la calificación de la asignatura.

| EJERCICIOS Y ACTIVIDADES EVALUABLES | PROPORCIÓN |
|---|---|
| Trabajo obligatorio | 40% |
| Examen final escrito | 60% |
| **TOTAL** | **100%** |

## Criterios de calificación de la evaluación continua

Los criterios para la evaluación del trabajo obligatorio se presentan en la siguiente tabla, donde se resumen los aspectos a valorar y el porcentaje que representa cada uno de los mismos:

| COMPONENTES EVALUABLES | PROPORCIÓN |
|---|---|
| Contenidos generales | 10% |
| Desarrollo | 50% |
| Otras aportaciones | 40% |
| **TOTAL** | **100%** |

Los criterios para la evaluación de la evaluación continua son los siguientes:

| ASPECTO DEL TEXTO | CARACT. POSTIVAS | 1 | 0,75 | 0,5 | 0,25 | 0 | CARACT. NEGATIVAS |
|---|---|---|---|---|---|---|---|
| Estructura (orden lógico) | Bien organizado | | | | | | Sin orden, índice o esquema |
| Formato | Adecuado | | | | | | Inadecuado |
| Objetivos | Fundamentados y claros | | | | | | No se especifican |
| Expresión escrita | Corrección gramatical y ortografía | | | | | | Incorrección y faltas |
| Metodología | Bien expuesta | | | | | | Mal o no se explica |
| Bibliografía | Se utiliza la necesaria | | | | | | No hay indicios de ello |
| Terminología | Adecuado uso | | | | | | Uso inadecuado |
| Análisis | Corrección | | | | | | Incorrección |
| Interpretación | Rigurosa | | | | | | Defectuosa o inexistente |
| Conclusión | Existe, clara y correcta | | | | | | Confusa, errada o ausente |
| Argumentación | Coherente y acertada | | | | | | Afirmaciones poco coherentes |

## 6 Apoyo tutorial

Para el apoyo tutorial, el alumno tendrá a su disposición un equipo docente encargado de acompañar al alumno durante toda su andadura en el proceso formativo, prestando una atención personalizada al alumno. Sus funciones están claramente diferenciadas complementándose al mismo tiempo. Las dos personas principales de este acompañamiento tutorial son:

- **Orientador Académico Personal:** encargado de planificar al alumno el estudio de la asignatura en función del tiempo disponible, incluso realiza nuevas planificaciones ajustándose a nuevos periodos marcados por el alumno según sus circunstancias personales y familiares. Otra de sus funciones es la de realizar un seguimiento del estudio del alumno, así como de dar al alumno información de carácter general necesaria en su proceso formativo.
- **Profesor docente:** encargado de resolver todas las dudas específicas de la asignatura y de informar al alumno de todas las pautas que debe seguir para realizar el estudio de la asignatura.

El alumno dispondrá de un horario de tutorías para contactar con estas figuras durante toda su formación académica. La información sobre el horario la encontrará el alumno en la plataforma virtual.

## 7 Horario de la asignatura y Calendario de temas

**Horario de tutorías de la asignatura: martes de 16:00 a 18:00 horas.**

El peso de cada unidad formativa dentro de cada asignatura queda determinado en el cronograma por el tiempo dedicado a la misma. El alumno deberá acometer el estudio marcado por la herramienta de planificación utilizada en el campus virtual, después de la planificación realizada con su tutor. A continuación se muestra una tabla con las unidades didácticas que componen la asignatura y las unidades de tiempo que se requieren para su estudio.

| UNIDADES DIDÁCTICAS | UNIDAD DE TIEMPO | HORAS DEDICACIÓN |
|---|---|---|
| Unidad 1 | 10 | 13,5 HORAS |
| Unidad 2 | 22 | 32,5 HORAS |
| Unidad 3 | 17 | 26 HORAS |
| Unidad 4 | 17 | 26 HORAS |
| Unidad 5 | 17 | 26 HORAS |
| Unidad 6 | 17 | 26 HORAS |
| **TOTAL** | **100** | **150** |