UNIVERSIDAD DE LAS PALMAS DE GRAN CANARIA

GUÍA DOCENTE *CURSO: 2018/19*

40824 - SERVICIOS Y SEGURIDAD EN RED

CENTRO: *180 - Escuela de Ingeniería Informática*

TITULACIÓN: *4008 - Grado en Ingeniería Informática*

ASIGNATURA: *40824 - SERVICIOS Y SEGURIDAD EN RED*

Vinculado a : (Titulación - Asignatura - Especialidad)
4801-Doble Grado en Ingeniería Informática y - 48142-SERVICIO Y SEGURIDAD EN LA RED - 00
4801-Doble Grado en Ingeniería Informática y - 48354-SERVICIOS Y SEGURIDAD EN RED - 00

CÓDIGO UNESCO: *1203* **TIPO:** *Obligatoria* **CURSO:** *3* **SEMESTRE:** *2º semestre*

CRÉDITOS ECTS: *6* **Especificar créditos de cada lengua:** **ESPAÑOL:** *6* **INGLÉS:**

SUMMARY

While we believe that the reference model proposed by I.S.O. they reflect the most adequate, both methodologically and functionally, to address the problem of interconnection of Open Systems, we must recognize the prominence of the Internet network that has been imposed
both in the Academic-Scientific and in the Commercial field and that bases its architecture on the protocols known as TCP / IP, ARPA or DoD. From this perspective they should be studied therefore, the applications developed in this field. Finally, it is worth highlighting the need currently exists for the protection of information that is exchanged between two users or distributed applications, given the different physical paths that it must travel and that are not susceptible to being physically protected by the users in question. For said we will introduce the students to the best known mechanisms for data encryption and the way that such mechanisms can be introduced into communication processes through of computer networks.

REQUISITOS PREVIOS

Redes de Computadores.

Plan de Enseñanza (Plan de trabajo del profesorado)

Contribución de la asignatura al perfil profesional:

Esta asignatura complementa la formación recibida en la asignatura de Redes de Computadores. Extiende la formación del alumno estudiando las aplicaciones más importantes existentes en la actualidad que complementa el modelo de Referencia para la Arquitectura de Sistemas Abiertos propuesto por I.S.O. y C.C.I.T.T.

Si bien creemos que el modelo de referencia propuesto por I.S.O. reflejan la forma más adecuada, tanto metodológica como funcionalmente, de abordar el problema de la interconexión de Sistemas Abiertos, debemos reconocer el protagonismo de la red Internet que se ha impuesto tanto en el ámbito Académico-Científico como en el Comercial y que basa su arquitectura en los protocolos conocidos como TCP/IP, ARPA o DoD. Desde esta perspectiva deben estudiarse por tanto las aplicaciones desarrolladas en dicho ámbito. Por último cabe resaltar la necesidad

existente en la actualidad de protección de la información que se intercambia entre dos usuarios o aplicaciones distribuidas, dado los diferentes caminos físicos que debe recorrer la misma y que no son susceptibles de ser protegidos físicamente por los usuarios en cuestión. Por dichos motivos introduciremos al alumnado en los mecanismos más conocidos de cifrado de datos y de la forma que dichos mecanismos pueden introducirse en los procesos de comunicación a través de redes de computadores.

Competencias que tiene asignadas:

G1.
G2.
G3.
G4.
G5.
N1.
N2.
N3.
N4.
N5.
T3.
T5.
T6.
T7.
T8.
T9.
CII01.
CII05.
CII011.
CII014.

Objetivos:

Ob1: El alumno conozca los protocolos más utilizados
Ob2: El alumno conozca la implementación de servicios
Ob3: El alumno tenga capacidad práctica de poner los servicios en funcionamiento.
Ob4: El alumno conozca y maneje las técnicas básicas de la criptografía
Ob5: Seguridad a los sistemas en su relación con la red así como los mecanismos de control de acceso a los sistemas más relevantes.

Contenidos:

PARTE TEÓRICA
****

Modulo I: Protocolos ARPA

Competencias: G1, G2, G3, G4, G5, N1, N2, N3, N4, N5, T3, T5, T6, T7, T8, T9, CII01, CII05,CII11, CII14.
Horas Presenciales: 16
Horas no Presenciales: 24

Bibliografía: D. Comer, RFC´s

Tema 1:Modelo de interacción Cliente-Servidor
Tema 2:Sistema de Nombre de Dominio
Tema 3:Protocolos y servicio de correo Electrónico
Tema 4:Protocolos para la compartición de Ficheros en Red
Tema 5:Mecanismos de Autenticación Única
Tema 6:Acceso Seguro
Tema 7:Protocolos para acceso Web.

Modulo II: Seguridad en Redes de Computadores

Competencias:G1, G2, G3, G4, G5, N1, N2, N3, N4, N5, T3, T5, T6, T7, T8, T9, CII01, CII05, CII11, CII14.
Horas Presenciales: 14
Horas no Presenciales: 21
Bibliografía: Stallings, Muñoz, Zwicky

Tema 1:Introducción a la Criptografía; Sistemas Simétricos y Asimétricos.
Tema 2:Aplicaciones Criptográficas
Tema 3:Técnicas de Intrusión
Tema 4:Mecanismos de Control de Acceso

PARTE PRÁCTICA
****

PRÁCTICA 1.- Cortafuego.

Implementación de supuestos prácticos que enseñen al alumno a realizar las tareas necesarias para alcanzar el objetivo enunciado en el título de la práctica.

Competencias:G1, G2, G3, G4, G5, N1, N2, N3, N4, N5, T3, T5, T6, T7, T8, T9, CII01, CII05, CII11, CII14.
Horas Presenciales: 4
Horas no Presenciales: 6

PRÁCTICA 2.- Servicio de Nombres de Dominio

Implementación de supuestos prácticos que enseñen al alumno a realizar las tareas necesarias para alcanzar el objetivo enunciado en el título de la práctica.

Competencias:G1, G2, G3, G4, G5, N1, N2, N3, N4, N5, T3, T5, T6, T7, T8, T9, CII01, CII05, CII11, CII14.
Horas Presenciales: 4
Horas no Presenciales: 6

PRÁCTICA 3.- Servicio de Correo Electrónico

Implementación de supuestos prácticos que enseñen al alumno a realizar las tareas necesarias para alcanzar el objetivo enunciado en el título de la práctica.

Competencias:G1, G2, G3, G4, G5, N1, N2, N3, N4, N5, T3, T5, T6, T7, T8, T9, CII01, CII05, CII11, CII14.
Horas Presenciales: 4
Horas no Presenciales: 6

PRÁCTICA 4.- Servicios de acceso a recursos compartidos

Implementación de supuestos prácticos que enseñen al alumno a realizar las tareas necesarias para alcanzar el objetivo enunciado en el título de la práctica.

Competencias:G1, G2, G3, G4, G5, N1, N2, N3, N4, N5, T3, T5, T6, T7, T8, T9, CII01, CII05, CII11, CII14.
Horas Presenciales: 2
Horas no Presenciales: 4

PRÁCTICA 5.- Acceso a través de proxy

Implementación de supuestos prácticos que enseñen al alumno a realizar las tareas necesarias para alcanzar el objetivo enunciado en el título de la práctica.

Competencias: G1, G2, G3, G4, G5, N1, N2, N3, N4, N5, T3, T5, T6, T7, T8, T9, CII01, CII05, CII11, CII14.
Horas Presenciales: 2
Horas no Presenciales: 4

PRÁCTICA 6.- Acceso seguro

Implementación de supuestos prácticos que enseñen al alumno a realizar las tareas necesarias para alcanzar el objetivo enunciado en el título de la práctica.

Competencias: G1, G2, G3, G4, G5, N1, N2, N3, N4, N5, T3, T5, T6, T7, T8, T9, CII01, CII05, CII11, CII14.
Horas Presenciales: 4
Horas no Presenciales: 6

PRÁCTICA 7.- Trabajo de curso

Implementación de supuestos prácticos que enseñen al alumno a realizar las tareas necesarias para alcanzar el objetivo enunciado en el título de la práctica.

Competencias: G1, G2, G3, G4, G5, N1, N2, N3, N4, N5, T3, T5, T6, T7, T8, T9, CII01, CII05, CII11, CII14.
Horas Presenciales: 10
Horas no Presenciales: 14

Metodología:

Actividades formativas presenciales:

AF1. Sesiones académicas teóricas: exposición de los conceptos fundamentales necesarios para la realización de las actividades prácticas.

AF2. Sesiones académicas prácticas: trabajo de diseño, instalación y administración de una

intranet.

AF3. Trabajos de curso dirigidos: Realización de un trabajo de curso basado en los conocimientos y habilidades desarrolladas durante el curso.

AF4. Tutorías colectivas o individuales:Esta actividad se realiza de forma presencial en el despacho del profesor (tutoría individual) o en un aula, seminario o laboratorio (para las tutorías colectivas) donde se las resuelven dudas que tengan los alumnos y se proponen supuestos donde el alumno tenga que decidir como resolver el la situación propuesta.

Actividades formativas no presenciales

AF5: Realización de pruebas de trabajo personal orientadas a consolidar los conceptos expuestos en las sesiones teóricas.
AF6: Realización de pruebas de trabajo personal orientadas a adquirir las habilidades necesarias para la realización de las prácticas
AF7: Tutorías mediante el uso de las tecnologías de la información y las comunicaciones (TICs)

Evaluacion:

Criterios de evaluación

Durante el curso se realizaran pruebas de trabajos personal y casos de estudio que se realizan de forma no presencial pero con el apoyo tutorizado de los profesores de las asignaturas. En estas tareas se persigue el objetivo de reafirmar los conocimientos impartidos en las clases presenciales.

Actividades formativas: AF1, AF2, AF3, AF5, AF6, AF7
Competencias: G1, G2, G3, G4, G5, N1, N2, N3, N4, N5, T3, T5, T6, T7, T8, T9, CII01, CII05,CII11, CII14.
En cada convocatoria se realizará:

FE1: Examen de la parte teórica de la asignatura. En él se preguntará por los contenidos teorícos-prácticos de la asignatura. Se valorará la exactitud y concreción de las respuestas. Actividades formativas AF1, AF2, AF3, AF5, AF7

FE2: Un examen práctico. Se realizará un examen de prácticas en el laboratorio. Se valorará la correcta aplicación de las técnicas estudiadas. Actividades formativas AF1, AF2, AF3, AF5, AF6, AF7

FE3: Un trabajo de curso en el que se trabajaba forma conjunta los conocimientos obtenidos durante el curso. Actividades formativas AF1, AF2, AF3, AF4, AF5, AF6, AF7

FE4: Pruebas de trabajo personal. Actividades formativas AF1, AF2, AF3, AF5, AF6, AF7

Sistemas de evaluación

La evaluación del alumno se realiza a través de pruebas que determinen los conocimientos adquiridos. Se realizan pruebas de trabajo personal, evaluación de tareas asignadas al alumno, exposición oral de trabajos, realización y defensa de trabajos prácticos en el laboratorio y resolución casos prácticos.
Se realizaran exámenes teóricos y prácticos.
Criterios de calificación

NF: Nota Final

Bloque Básico
NT: Nota de exámenes (FE1)
NP: Nota de practicas (FE2, FE3)

Bloque complementario
PTP: Pruebas de trabajo personal (FE4)

Hay que superar (>= 5) las pruebas del bloque básico.

Si alguno de los criterios no supera los mínimos, la nota final será el valor del criterio de menor puntuación.

Evaluación en todas convocatorias
NF= 0.2*PTP + 0.5*NT+0.5*NP

La NF máxima es un 10.

Las partes superadas en la convocatoria ordinaria se mantienen hasta la convocatoria extraordinaria

Plan de Aprendizaje (Plan de trabajo de cada estudiante)

Tareas y actividades que realizará según distintos contextos profesionales (científico, profesional, institucional, social)

Asistencia a clases teóricas y a clases prácticas:

TA1 : Adquirir conocimientos teóricos y prácticos sobre protocolos y servicios TCP/IP

TA2 : Adquirir conocimientos teóricos y prácticos sobre mecanismos de seguridad en redes de computadores

Temporalización semanal de tareas y actividades (distribución de tiempos en distintas actividades y en presencialidad - no presencialidad)

Semana 01 : Actividad 1 (presencial)
Teoría 2 horas. Práctica 2 horas. Trabajo no presencial 6 horas.
Semana 02 : Actividad 1 (presencial)
Teoría 2 horas. Práctica 2 horas. Trabajo no presencial 6 horas.
Semana 03 : Actividad 1 (presencial)
Teoría 2 horas. Práctica 2 horas. Trabajo no presencial 6 horas.
Semana 04 : Actividad 1 (presencial)
Teoría 2 horas. Práctica 2 horas. Trabajo no presencial 6 horas.
Semana 05 : Actividad 1 (presencial)
Teoría 2 horas. Práctica 2 horas. Trabajo no presencial 6 horas.
Semana 06 : Actividad 1 (presencial)
Teoría 2 horas. Práctica 2 horas. Trabajo no presencial 6 horas.
Semana 07 : Actividad 1 (presencial)
Teoría 2 horas. Práctica 2 horas. Trabajo no presencial 6 horas.

Semana 08 : Actividad 1 (presencial)
Teoría 2 horas. Práctica 2 horas. Trabajo no presencial 6 horas.
Semana 09 : Actividad 2 (presencial)
Teoría 2 horas. Práctica 2 horas. Trabajo no presencial 6 horas.
Semana 10 : Actividad 2 (presencial)
Teoría 2 horas. Práctica 2 horas. Trabajo no presencial 6 horas.
Semana 11 : Actividad 2 (presencial)
Teoría 2 horas. Práctica 2 horas. Trabajo no presencial 6 horas.
Semana 12 : Actividad 2 (presencial)
Teoría 2 horas. Práctica 2 horas. Trabajo no presencial 6 horas.
Semana 13 : Actividad 2 (presencial)
Teoría 2 horas. Práctica 2 horas. Trabajo no presencial 6 horas.
Semana 14 : Actividad 2 (presencial)
Teoría 2 horas. Práctica 2 horas. Trabajo no presencial 6 horas.
Semana 15 : Actividad 2 (presencial)
Teoría 2 horas. Práctica 2 horas. Trabajo no presencial 6 horas.

Recursos que tendrá que utilizar adecuadamente en cada uno de los contextos profesionales.

Re1: Infraestructura de red de comunicaciones, donde se incluyen switchs y router.

Re2: Computadores ejecutándose bajos los sistemas operativos Linux y Windows.

RE3: Software de aplicaciones.

Resultados de aprendizaje que tendrá que alcanzar al finalizar las distintas tareas.

Actividades formativas AF1, AF2, AF3, AF4, AF5, AF6, AF7
Tarea formativa TA1
RA1: Explicar en detalle el concepto de modelo Cliente-Servidor.
RA2: Analizar, comparar y describir distintos protocolos de aplicación de Internet.
RA3: Analizar, comparar y describir los servicios de aplicación más difundidos en Internet.

Tarea formativa TA2
RA4: Describir los conceptos fundamentales de la criptografía.
RA5: Plantear los aspectos más relevantes sobre la problemática de la seguridad informática, tanto en los aspectos teóricos como prácticos.
RA6: Conocer las distintas alternativas para aportar seguridad a los Sistemas de Información.

Plan Tutorial

Atención presencial individualizada (incluir las acciones dirigidas a estudiantes en 5ª, 6ª y 7ª convocatoria)

Resolución de dudas y orientación en el proceso de aprendizaje.
Para los alumnos de 5ª, 6ª y 7ª convocatoria se llevara a cabo el siguiente plan tutorial:

En la parte teórica de la asignatura, tras realizar de cada una de las Tareas de Trabajo Personal que se les proponen a lo largo del curso, y al finalizar las mismas se realizará una tutoría individual con el alumno para validar la realización de las mismas y corregir errores de concepto si los hubiere.

En la parte práctica de la asignatura. al finalizar de cada práctica y tras realizar el proceso de autovalidación, tendrá que exponérsela al tutor para verificar su correcta realización.

Atención presencial a grupos de trabajo

Resolución de dudas y orientación en el proceso de aprendizaje.

Atención telefónica

Mediante el teléfono del despacho del profesor.

Atención virtual (on-line)

Mediante el Campus Virtual y el correo electrónico

Datos identificativos del profesorado que la imparte.

Datos identificativos del profesorado que la imparte

Dr./Dra. Francisco Javier Alayón Hernández *(RESPONSABLE DE PRACTICAS)*

Departamento: *260 - INFORMÁTICA Y SISTEMAS*

Ámbito: *075 - Ciencia De La Comp. E Intel. Artificial*

Área: *075 - Ciencia De La Comp. E Intel. Artificial*

Despacho: *INFORMÁTICA Y SISTEMAS*

Teléfono: *928458756* **Correo Electrónico:** *francisco.alayon@ulpgc.es*

Dr./Dra. José Antonio Muñoz Blanco

Departamento: *260 - INFORMÁTICA Y SISTEMAS*

Ámbito: *075 - Ciencia De La Comp. E Intel. Artificial*

Área: *075 - Ciencia De La Comp. E Intel. Artificial*

Despacho: *INFORMÁTICA Y SISTEMAS*

Teléfono: *928458754* **Correo Electrónico:** *joseantonio.munoz@ulpgc.es*

Bibliografía

[1 Básico] Internetworking with TCP/IP: vol. I

Comer, Douglas E.

Prentice-Hall Internacional,, London : - (3rd ed.)

0132169878

[2 Básico] Building Internet firewalls /

D. Brent Chapman and Elizabeth D. Zwicky.

O'Reilly and Associates,, Sebastopol, CA : (1995)

1565921240

[3 Básico] Request for comments [

Internet Engineering Task Force.

[4 Básico] Seguridad de sistemas en red /

José Antonio Muñoz Blanco, Víctor Manuel Henríquez Henríquez.
Universidad de Las Palmas de Gran Canaria, Servicio de Publicaciones,, Las Palmas de Gran Canaria : (2007)
97884969710305

[5 Básico] Network security essentials: applications and standards /

William Stallings.
Prentice Hall,, Upper Saddle River, NJ : (2000)
0130160938

[6 Recomendado] Network security with OpenSSL /

John Viega, Matt Messier and Pravir Chandra.
O'Reilly,, Sebastopol (California) : (2002)
978-0-596-00270-1

[7 Recomendado] Linux: administración del sistema y explotación de los servicios de red /

Philippe Banquet, Sébastien Bobillier.
ENI,, Cornellà de Llobregat, Barcelona : (2015) - (3ª ed.)
978-2-7460-9612-7

[8 Recomendado] Linux preparación para la certificación LPIC-2: exámenes LPI 201 y LPI 202 /

[Sébastien Bobillier, Philippe Banquet].
ENI,, Barcelona : (2015) - (3ª ed.)
978-2-7460-9512-0

[9 Recomendado] Linux preparación para la certificación LPIC-1: exámenes LPI 101 y LPI 102 /

[Sébastien Rohaut].
ENI,, Barcelona : (2015) - (3ª ed.)
978-2-7460-9513-7