UNIVERSIDAD DE LAS PALMAS DE GRAN CANARIA

GUÍA DOCENTE *CURSO: 2014/15*

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

CÓDIGO UNESCO: *1203* **TIPO:** *Obligatoria* **CURSO:** *3* **SEMESTRE:** *2º semestre*
CRÉDITOS ECTS: *6* **Especificar créditos de cada lengua:** **ESPAÑOL:** *6* **INGLÉS:**

SUMMARY

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.- Configuración dinámica TCP/IP.

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: 5
Horas no Presenciales: 8

PRÁCTICA 4.- Generación y distribución de claves simétricas, asimétricas y certificados

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 5.- Acceso Seguro a sistemas remotos

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: 5
Horas no Presenciales: 8

PRÁCTICA 6.- Conexión segura

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.- Control de Acceso

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

Metodología:

- Sesiones académicas teóricas con debates y participación
- Sesiones académicas de problemas.
- Sesiones académicas prácticas.
- Trabajos colaborativos en grupo e individuales dirigidos.
- Exposición y defensa oral de trabajos en el ámbito de la clase.
- Lecturas obligatorias.
- Búsqueda, análisis, síntesis y generación de la información.
- Ejercicios de autoevaluación.
- Exámenes de control y aprendizaje
- Tutorías colectivas e individuales.
- Uso de las tecnologías de la información.
- Foros, debates y discusiones en el ámbito de la clase
- Actividades para conexión de la clase como grupo, conocer a los individuos y servicios al colectivo.

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.

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.

FE2: Un examen práctico. Se realizará un examen de prácticas en el laboratorio. Se valorará la correcta aplicación de las técnicas estudiadas.

FE3: Un trabajo de curso en el que se trabajaba forma conjunta los conocimientos obtenidos durante el curso.

FE4: Pruebas de trabajo personal

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)

Bloque complementario
PTP: Pruebas de trabajo personal (FE4)
CE: Casos de estudio (FE3)

Hay que superar (>= 5) las pruebas del bloque básico.
Del bloque complementario es necesario obtener al menos un 4 en cada uno de ellos.

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 + 0.4*NT+0.3*NP+0.3*CE

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:

AF1 : Adquirir conocimientos teóricos y prácticos sobre protocolos y servicios TCP/IP

AF2 : 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.

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.
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.

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. José Antonio Muñoz Blanco *(COORDINADOR)*
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*

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*

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] Beginning OpenVPN 2.0.9 :build and integrate Virtual Private Networks using OpenVPN /

Markus Feilner, Norbert Graf.
Packt Publishing,, Birmingham : (2009)
978-1-84719-706-1