Redes de ordenadores

Grado en Ingeniería Informática



UNIVERSIDAD NEBRIJA

GUÍA DOCENTE

Asignatura: Redes de ordenadores

Titulación: Grado en Ingeniería Informática

Carácter: Obligatoria

Idioma: Español

Modalidad: Presencial

Créditos: 6

Curso: 2º

Semestre: 2º

Profesores/Equipo docente: D. Oscar Alberto Gru, D. Elam Uceda Herrero (prácticas)

1. COMPETENCIAS Y RESULTADOS DE APRENDIZAJE

1.1. Competencias

Competencias básicas

- CB1, CB2, CB3, CB4, CB5

Competencias específicas

- CEC11. Conocer y aplicar las características, funcionalidades y estructura de los sistemas distribuidos, las redes de computadores e Internet y diseñar e implementar aplicaciones basadas en ellas.
- CEIC06. Comprender, aplicar y gestionar la garantía y seguridad de los sistemas informáticos.
- CEIC08. Diseñar, desplegar, administrar y gestionar redes de computadores.

Competencias generales

- CGT1. Analizar y sintetizar la información necesaria para realizar su trabajo plasmando los resultados en informes o en la toma de decisiones en proyectos del ámbito de la ingeniería informática.
- CGT2. Organizar y planificar los recursos e ideas necesarias para realizar su trabajo ideando acciones e hitos en proyectos del ámbito de la ingeniería informática.
- CGT3. Comunicar de forma oral y escrita en la lengua nativa pudiendo expresar sus opiniones de forma clara para transmitir conceptos y soluciones dentro del ámbito de la ingeniería informática.

- CGT5. Aplicar conocimientos de informática relativos al ámbito de estudio al trabajar en proyectos del ámbito de la ingeniería informática.
- CGT6. Gestionar la información, conociendo su importancia y la forma de procesarla generando los recursos necesarios para facilitar su acceso y provisión en el ámbito de la ingeniería informática.
- CGT7. Resolver problemas en el entorno de trabajo, dentro del ámbito de la ingeniería informática, enfrentándose a situaciones complejas en cuanto a problemas técnicos y a las relaciones personales y profesionales.
- CGT8. Tomar decisiones basadas en la información disponible en el ámbito de la ingeniería informática.
- CGS2. Razonar de forma crítica ante los problemas que surjan en el ámbito de la ingeniería informática, contando con la información disponible, y explicar dicho razonamiento.
- CGS3. Aplicar su compromiso ético en la actividad diaria y en el ejercicio de su profesión dentro del campo de la ingeniería informática, sabiendo justificar el porqué de sus acciones.
- CGS4. Aprender de forma autónoma conceptos relativos a la profesión ingenieril para facilitar la mejora continua ya sea mediante el acceso a información disponible o cualquier otro medio.
- CGS5. Adaptarse a nuevas situaciones en el entorno de la ingeniería informática, reconociendo dichas situaciones y expresando formas de afrontarlas.
- CGS6. Aplicar la creatividad ante las diferentes circunstancias generando soluciones novedosas dentro del ámbito de la ingeniería informática.
- CGP1. Trabajar en equipo contribuyendo de forma activa al resultado de los proyectos u operaciones del ámbito de la ingeniería informática.

1.2. Resultados de aprendizaje

Esta asignatura contribuye a los siguientes resultados de aprendizaje de la materia en la que se engloba:

- Describir las características, funcionalidades y estructura de los sistemas basados en redes de computadores, incluidos los diferentes niveles del modelo de capas.
- Diseñar e implementar aplicaciones basadas en redes de computadores.
- Diseñar y gestionar redes de computadores.

2. CONTENIDOS

2.1. Requisitos previos

Ninguno.

2.2. Descripción de los contenidos

- Introducción a las redes de paquetes. Conceptos de transmisión de datos. Medios de transmisión y tecnologías de nivel físico. La capa de enlace de datos. Acceso múltiple y redes de área local. Capa de red y protocolo IP. Servicios y protocolos básicos de red. Seguridad en redes.

2.3. Contenido detallado

Presentación de la asignatura.

Explicación de la **guía docente**.

Tema 1: Introducción a las redes de ordenadores

Definición y tipos de redes.

Modelos de referencia: El modelo OSI vs. el modelo TCP/IP.

Mecanismos de comunicación: servicios, interfaces y protocolos.

Cloud: Modelos de servicio (IaaS, PaaS, SaaS) y el concepto de computación elástica.

Tema 2: Capa de aplicación (L7)

Arquitecturas Cliente-Servidor y P2P.

Protocolos estándar: DNS (Dominios), SMTP/POP3/IMAP (Correo), HTTP (Web).

Servicios multimedia: Vídeo y audio streaming.

Application Programming Interfaces (APIs): Formato JSON y métodos REST.

Cloud: Microservicios y Service Discovery. El rol del DNS dinámico en la nube.

Tema 3: Capa de transporte (L4)

Comunicación lógica entre procesos: Sockets y Multiplexación.

Protocolo UDP: Transmisión no orientada a conexión.

Protocolo TCP: Control de flujo, control de congestión y establecimiento de conexión (3 way handshake).

Cloud: Balanceo de carga en L4 (Network Load Balancers) y terminación SSL.

Tema 4: Capa de red (L3)

El plano de datos: Forwarding (Reenvío) vs. Routing (Enrutamiento).

Datagramas IP: Estructura de cabecera en IPv4 e IPv6.

Direccionamiento: Subnetting, máscaras de red y NAT.

Protocolos de control: ICMP, ARP y DHCP.

Introducción al enrutamiento jerárquico: Conceptos de OSPF y BGP.

Cloud: Redes Definidas por Software (SDN) y la Virtual Private Cloud (VPC). Anatomía de una caída global (Caso Cloudflare/BGP).

Tema 5: Capas de enlace y física (L2/L1)

Función de las capas L1 y L2 en la transmisión de datos.

Señales y ancho de banda: limitaciones físicas (Nyquist y Shannon).

Codificación y sincronización: Manchester, 4B/5B, MLT-3.

Medios de transmisión: par trenzado y fibra óptica.

Tramado y control de errores: preámbulo, delimitadores y CRC.

Protocolos de acceso al medio: CSMA/CD y evolución hacia redes conmutadas.

Dispositivos: Hub vs Switch, VLANs y enlaces troncales (802.1Q).

Prevención de bucles: Spanning Tree Protocol (STP) y agregación de enlaces.

Aspectos prácticos: MTU, priorización (CoS), autonegociación.

Cloud: Segmentación lógica y redes virtualizadas en entornos cloud.

Tema 6: Seguridad en redes

Principios básicos: Confidencialidad, Integridad y Disponibilidad.

Defensa en profundidad: seguridad multicapa.

Ataques y mitigación en L7: SQL Injection, XSS, WAF.

Firewalls avanzados: NGFW y DPI.

Sistemas IDS/IPS: detección por firmas y análisis de anomalías.

Cifrado extremo a extremo: TLS/SSL y certificados digitales (PKI).

VPNs: IPsec y SSL/TLS.

Ataques clásicos: IP Spoofing, ARP Poisoning, MAC Flooding, VLAN Hopping.

Ataques DoS/DDoS y técnicas de mitigación.

Cloud: Seguridad en redes definidas por software y entornos virtualizados.

2.4. Actividades dirigidas

Durante el curso se desarrollarán actividades dirigidas en forma de cinco prácticas de laboratorio. El contenido de dichas prácticas irá enfocado al aprendizaje del diseño, el despliegue, la organización y la gestión redes y servicios, incluyendo tanto la puesta en marcha como la mejora continua y la resolución de problemas en redes y sistemas.

El contenido de las prácticas podrá modificarse con el fin de afianzar aquellos aspectos para los que se detecte una mayor dificultad de aprendizaje.

2.5 Actividades formativas

CÓDIGO	ACTIVIDAD FORMATIVA	HORAS	PORCENTAJE DE PRESENCIALIDAD
AF1	Clases de teoría, evaluación y problemas	45	100%
AF2	Tutorías	12,5	100%
AF3	Prácticas	15	100%
AF4	Estudio individual	77,5	0%

3. SISTEMA DE EVALUACIÓN

3.1. Sistema de calificaciones

El sistema de calificaciones (R.D. 1125/2003, de 5 de septiembre) será el siguiente:

0 - 4,9 Suspenso (SS)

5,0 - 6,9 (Aprobado (AP)

7,0 - 8,9 Notable (NT)

9,0 - 10 Sobresaliente (SB)

La mención de «Matrícula de Honor» podrá ser otorgada a alumnos que hayan obtenido una calificación igual o superior a 9.0. Su número no podrá exceder del cinco por ciento de los alumnos matriculados en una materia en el correspondiente curso académico, salvo que el número de alumnos matriculados sea inferior a 20, en cuyo caso se podrá conceder una sola «Matrícula de Honor».

3.2. Criterios de evaluación

Convocatoria ordinaria

Sistemas de evaluación	Porcentaje
SE1 Prueba parcial	15%
SE2 Examen final	65%

SE3 Evaluación de la participación del estudiante	5%
SE4 Actividades dirigidas, prácticas y memorias de prácticas, trabajos (obligatorios y voluntarios) y proyectos a realizar	15%

Convocatoria extraordinaria

Sistemas de evaluación	Porcentaje
SE2 Examen final	70%
SE4 Actividades dirigidas, prácticas y memorias de prácticas, trabajos (obligatorios y voluntarios) y proyectos a realizar	30%

3.3. Restricciones

Calificación mínima

Para aprobar la asignatura es preciso obtener una nota de 5 o superior en la media ponderada de los distintos criterios del sistema de evaluación. La ponderación tanto del examen parcial como de los conceptos de participación y trabajos escritos/prácticas, sólo se aplicará si el estudiante obtiene al menos un 5 en el examen final (ordinaria/extraordinaria).

La no superación del bloque de prácticas comportará el suspenso automático de la asignatura en las convocatorias ordinaria y extraordinaria. Para considerar superado dicho bloque se requerirá cumplir simultáneamente los siguientes criterios:

- Obtener en cada una de las prácticas una calificación igual o superior a 3 puntos, condición necesaria para el cálculo de la media.
- Obtener una media aritmética igual o superior a 5 puntos en el conjunto de todas las prácticas.

La calificación del bloque de prácticas no se conservará para cursos académicos posteriores.

Asistencia

El alumno que, injustificadamente, deje de asistir a más de un 25% de las clases presenciales podrá verse privado del derecho a examinarse en la convocatoria ordinaria.

Normas de escritura

Se prestará especial atención en los trabajos, prácticas y proyectos escritos, así como en los exámenes tanto a la presentación como al contenido, cuidando los aspectos gramaticales y ortográficos. El no cumplimiento de los mínimos aceptables puede ocasionar que se resten puntos en dicho trabajo.

3.4. Advertencia sobre plagio

La Universidad Antonio de Nebrija no tolerará en ningún caso el plagio o copia. Se considerará plagio la reproducción de párrafos a partir de textos de autoría distinta a la del estudiante (Internet, libros, artículos, trabajos de compañeros…), cuando no se cite la fuente original de la que provienen. El uso de las citas no puede ser indiscriminado. El plagio es un delito.

En caso de detectarse este tipo de prácticas, se considerará Falta Grave y se podrá aplicar la sanción prevista en el Reglamento del Alumno.

3.5. Uso de la inteligencia artificial (IA) generativa en las actividades formativas

La adopción de herramientas de IA en la docencia debe basarse en un enfoque transparente, responsable, ético y seguro, que fomente el desarrollo de competencias digitales en el estudiantado:

- El profesor incluirá en cada actividad formativa si tiene previsto el uso de IA Generativa, con qué objetivo y los requisitos de aplicación de esta.
- Es responsabilidad del estudiante mostrar una conducta transparente, ética y responsable con el uso de IA Generativa, y adaptarse a los criterios de aplicación dictados por el profesor en cada actividad.
- La detección de cualquier conducta fraudulenta con respecto al uso de IA Generativa, no atendiendo a las indicaciones del profesorado, aplicará las sanciones previstas en el Reglamento Disciplinario.

4. BIBLIOGRAFÍA

Bibliografía básica

- Tanenbaum, A. (2021). *Computer Networks*. 6th ed. Pearson.
- Tanenbaum, A. (2013). *Redes de Computadoras*. 5ª ed. Pearson.
- Stallings, W. (2013). *Data and computer communications*. 10th ed. Pearson.
- Kurose, J., Ross, K. (2017). *Computer Networking: A Top-Down Approach*. 7th ed. Pearson.

Bibliografía complementaria

- Sanders, C. (2017). *Practical Packet Analysis, using Wireshark to solve real-work network problems*. No Starch Press.
- Bejtlich, R. (2013). *The Practice of Networking Security Monitoring: understanding incident detection and response*. No Starch Press