unie
Universidad

# GUÍA DOCENTE

## SEGURIDAD EN REDES DE COMUNICACIÓN

Planeta Formación y Universidades

## Seguridad En Redes De Comunicación

| | | |
|---|---|---|
| **Número total de créditos ECTS** | | 6 |
| **Tipología** | | Obligatoria |
| **Organización temporal** | | Semestre 1 |
| **Modalidad** | | Presencial y virtual |
| **Idioma** | | Castellano |
| **Contenidos** | | • Estructura de comunicaciones, modelo OSI y principales protocolos<br>  ○ Capa de red: IPv4, IPv6 y protocolos auxiliares<br>  ○ Capa de transporte: TLS y VPN<br>  ○ Capa de aplicación: DNS, HTTP, FTP, RDP y correo electrónico<br>• Ataques<br>  ○ Spoofing<br>  ○ Sniffing<br>  ○ DDoS<br>  ○ Hijacking<br>  ○ Inyecciones de código<br>  ○ Intrusiones físicas<br>• Mitigaciones<br>  ○ IPSec<br>  ○ BGPSec<br>  ○ HTTPS<br>  ○ SFTP<br>  ○ SMTPS<br>  ○ IMAPS |
| **Resultados de aprendizaje TÍTULO** | **Conocimientos y contenidos** | CC02 Identificar vulnerabilidades en sistemas clave de información y comunicación distinguiendo y categorizando las principales amenazas relacionadas con dichas vulnerabilidades<br>CC03 Identificar las alternativas seguras de los principales protocolos usados en los diferentes niveles del modelo OSI, que garanticen la integridad, confidencialidad y disponibilidad de la información. |
| | **Habilidades y destrezas** | HD01 Realizar análisis de las vulnerabilidades tanto manuales como automatizados a sistemas informáticos y redes para determinar las principales amenazas que puedan afectarles<br>HD09 Aplicar técnicas y herramientas avanzadas de bastionado de redes y sistemas informáticos, destacando en la implementación de estrategias de fortificación de redes de vanguardia |
| | **Competencias** | CP04 Comunicar las causas, consecuencias, mecanismos de contención empleados y medidas de prevención implementadas a raíz de un ataque informático.<br>CP05 Elaborar un plan integral de ciberseguridad para organizaciones, proponiendo mejoras a sus mecanismos de seguridad informática que atiendan a su naturaleza, recursos, fortalezas, debilidades y necesidades. |
| **Resultados de aprendizaje MATERIA** | | |
| • Elaborar un plan de migración de protocolos tradicionales a sus alternativas recientes más seguras.<br>• Identificar los protocolos empleados en un entorno práctico y sus principales vulnerabilidades y contramedidas específicas de cada caso.<br>• Mitigar los ataques más comunes a los diferentes niveles de la capa OSI. | | |

| | | | |
|---|---|---|---|
| **Modalidad Presencial** | **Actividades formativas** | **Horas totales** | |
| | Clases Expositivas | 22 | |
| | Seminarios | 2 | |
| | Clases prácticas | 10 | |
| | Prácticas de laboratorio | 12 | |
| | **Trabajo autónomo** | **102** | |
| | **Prueba de evaluación final** | **2** | |
| | **Total** | **150** | |
| | **Sistemas de evaluación** | **MÍNIMO** | **MÁXIMO** |
| | Evaluación final: prueba o examen | 50 | 50 |
| | Resolución problemas | 10 | 30 |
| | Estudio casos - Proyectos | 10 | 30 |
| | Otras actividades de evaluación continua | 0 | 10 |
| | **Total** | **70** | **120** |
| **Modalidad virtual** | **Actividades formativas** | **Horas totales** | |
| | Clases expositivas síncronas | 10 | |
| | Recursos didácticos audiovisuales | 6 | |
| | Seminarios síncronos | 2 | |
| | Clases prácticas síncronas | 10 | |
| | Resolución de ejercicios, casos y proyectos | 6 | |
| | Prácticas de laboratorio asíncronas | 12 | |
| | **Trabajo autónomo** | 102 | |
| | **Prueba de evaluación final** | 2 | |
| | **Total** | **150** | |
| | **Sistemas de evaluación** | **MÍNIMO** | **MÁXIMO** |
| | Evaluación final: prueba o examen virtual | 50 | 50 |
| | Resolución problemas | 10 | 30 |
| | Estudio casos / Proyectos | 10 | 30 |
| | Otras actividades de evaluación continua | 0 | 10 |
| | **Total** | **70** | **120** |
| **Observaciones** | | | |