

Seguridad en Redes de Comunicación

Número total de créditos ECTS		6
Tipología		Obligatoria
Organización temporal		Semestre 1
Modalidad		Virtual
Idioma		Castellano
Contenidos	<ul style="list-style-type: none"> • Estructura de comunicaciones, modelo OSI y principales protocolos <ul style="list-style-type: none"> ○ Capa de red: IPv4, IPv6 y protocolos auxiliares ○ Capa de transporte: TLS y VPN ○ Capa de aplicación: DNS, HTTP, FTP, RDP y correo electrónico • Ataques <ul style="list-style-type: none"> ○ Spoofing ○ Sniffing ○ DDoS ○ Hijacking ○ Inyecciones de código ○ Intrusiones físicas • Mitigaciones <ul style="list-style-type: none"> ○ IPSec ○ BGPSec ○ HTTPS ○ SFTP ○ SMTPS ○ IMAPS 	
Resultados de aprendizaje TÍTULO	Conocimientos contenidos	CC02 Identificar vulnerabilidades en sistemas clave de información y comunicación distinguiendo y categorizando las principales amenazas relacionadas con dichas vulnerabilidades 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 destrezas	HD01 Realizar análisis de las vulnerabilidades tanto manuales como automatizados a sistemas informáticos y redes para determinar las principales amenazas que puedan afectarles 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. 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 ASIGNATURA		
<ul style="list-style-type: none"> • Elaborar un plan de migración de protocolos tradicionales a sus alternativas recientes más seguras. • Identificar los protocolos empleados en un entorno práctico y sus principales vulnerabilidades y contramedidas específicas de cada caso. • Mitigar los ataques más comunes a los diferentes niveles de la capa OSI. 		

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