Protección de Sistemas Informáticos

Número total de créditos ECTS		6
Tipología		Obligatoria
Organización temporal		Semestre 1
Modalidad		Virtual
Idioma		Castellano

Contenidos		• Herramientas de detección y prevención de ciberataques
		  ○ Logs
		  ○ Firewalls y políticas de seguridad
		  ○ IDS y configuración de reglas
		  ○ IPS
		  ○ SIEM/SOAR y desarrollo de playbooks
		  ○ EDR/XDR
		• Técnicas estadísticas para la detección de outliers
		  ○ Z-Score
		  ○ IQR
		• Uso de Inteligencia Artificial en IDS y IPS

Resultados de aprendizaje TÍTULO	**Conocimientos y contenidos**	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	HD02 Aplicar las medidas correctivas necesarias para eliminar o mitigar las consecuencias de un ataque informático. HD05 Evaluar diferentes ataques informáticos gracias a las trazas que dejan los mismos en los diferentes mecanismos de detección y registro de los sistemas. HD06 Configurar diferentes herramientas de detección, prevención, contención y recuperación de ciberincidentes. HD07 Extraer evidencias de diversas fuentes de dispositivos involucrados en un ciberincidente. 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	CP01 Realizar un análisis forense detallado de los diferentes elementos que pueden estar involucrados en un incidente informático, desde sistemas informáticos convencionales hasta redes complejas y dispositivos móviles, identificando, recopilando y examinando de manera sistemática diversas evidencias digitales. 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		
• Decidir qué herramientas de defensa frente a ciberataques implementar, teniendo en cuenta las características y las necesidades del sistema a proteger, así como las particularidades y opciones de cada una de ellas. • Usar técnicas estadísticas y de inteligencia artificial para detectar comportamientos anómalos en un sistema e integrar esta información en las herramientas de defensa del mismo.		

Actividades formativas	Horas totales
Clases expositivas síncronas	6
Recursos didácticos audiovisuales	4
Seminarios síncronos	2
Clases prácticas síncronas	14
Resolución de ejercicios, casos y proyectos	4
Prácticas de laboratorio asíncronas	16
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**