Guía didáctica

Ciberseguridad

INTRODUCCIÓN

La Ciberseguridad es un tema cada vez más relevante en nuestra sociedad actual, donde la tecnología es parte fundamental de nuestras vidas. La creciente interconexión de dispositivos y sistemas, así como el aumento de las amenazas cibernéticas, hacen que la seguridad digital sea una prioridad para empresas y usuarios.

En este curso de Ciberseguridad, se abordarán los principales conceptos y técnicas para proteger los sistemas y datos de posibles amenazas. Se explorarán las vulnerabilidades más comunes en el entorno digital y se proporcionarán recomendaciones para mitigarlas. Además, se analizarán casos reales de incidentes de seguridad y se desarrollarán habilidades en la elaboración de informes detallados.

OBJETIVO GENERAL

Proporcionar a los estudiantes los conocimientos y habilidades necesarias para proteger sistemas y datos contra amenazas cibernéticas, promoviendo la conciencia sobre la importancia de la seguridad en el entorno digital.

CONTENIDO FORMATIVO

	Ciberseguridad	20 horas
UA1	**Introducción a la seguridad en sistemas de información** • Conceptos de seguridad en los sistemas • Clasificación de las medidas de seguridad • Requerimientos de seguridad en los sistemas de información	2
	Test de evaluación	0,5
	Tiempo total de la unidad de aprendizaje	**2,5**
UA2	**Ciberseguridad** • Concepto de ciberseguridad • Amenazas más frecuentes a los sistemas de información • Tecnologías de seguridad más habituales • Gestión de la seguridad informática	2
	Test de evaluación	0,5
	Tiempo total de la unidad de aprendizaje	**2,5**
UA3	**Software dañino** • Conceptos sobre software dañino • Clasificación del software dañino • Amenazas persistentes y avanzadas • Ingeniería social y redes sociales	2
	Test de evaluación	0,5
	Tiempo total de la unidad de aprendizaje	**2,5**
UA4	**Seguridad en redes inalámbricas** • Concepto de seguridad en redes inalámbricas • Ataques a redes inalámbricas	1,5
	Test de evaluación	0,5
	Tiempo total de la unidad de aprendizaje	**2**
UA5	**Herramientas de Ciberseguridad** • Medidas de protección • Control de acceso de los usuarios al sistema operativo • Gestión segura de comunicaciones, carpetas y otros recursos • compartidos	2

	Ciberseguridad	20 horas
	• Protección frente a código malicioso	
	Test de evaluación	0,5
	Tiempo total de la unidad de aprendizaje	**2,5**
UA6	**Conocimientos avanzados sobre nuestra identidad digital.** • Capacidad de identificación personal en el ámbito digital. • Conocimiento sobre la protección de nuestra identidad digital. • Conocimiento sobre los derechos asociados a la identidad digital. • Conocimiento avanzado de los aspectos de navegación segura por internet. • Capacidad de identificación y uso de protocolos seguros en internet. • Conocimiento avanzado sobre el proceso de reporte y comunicación de ciberincidentes.	2
	Test de evaluación	0,5
	Tiempo total de la unidad de aprendizaje	**2,5**
UA7	**Conocimiento de las ciberamenazas y aplicación de técnicas de defensa.** • Conocimiento de los incidentes de seguridad (robo, filtrado y secuestro de información) y sus características. • Capacidad para la implementación de las estrategias de protección contra los ciberataques. • Capacidades para aplicar técnicas de defensa en el ciberentorno. • Capacidad para minimizar los daños causados por los posibles ciberincedentes.	2
	Test de evaluación	0,5
	Tiempo total de la unidad de aprendizaje	**2,5**
	Actividad final de evaluación	**2**
	Test de evaluación final	**1**