Guía didáctica

IFCT103. Ciberseguridad: Prevención, análisis y respuesta a incidentes de seguridad

INTRODUCCIÓN

En el actual panorama tecnológico, donde la información y la comunicación digital son elementos esenciales en la mayoría de las organizaciones y actividades cotidianas, la ciberseguridad se ha vuelto un aspecto crítico para salvaguardar la integridad, confidencialidad y disponibilidad de los datos y sistemas. La creciente sofisticación de las amenazas cibernéticas exige que tanto individuos como empresas adquieran habilidades avanzadas en ciberseguridad para prevenir, detectar y responder eficazmente a incidentes de seguridad.

El curso se erige como un pilar fundamental para comprender y abordar los desafíos emergentes en el ámbito de la ciberseguridad. Este curso está diseñado para dotar a los participantes con los conocimientos técnicos y las habilidades prácticas necesarias para identificar y contrarrestar diversas amenazas cibernéticas, así como para implementar medidas preventivas y estrategias de respuesta efectivas ante posibles incidentes de seguridad.

OBJETIVO GENERAL

Conocer y comprender las nociones fundamentales de ciberseguridad que permitan prevenir y dar respuesta a los incidentes de seguridad.

CONTENIDO FORMATIVO

IFCT103	Ciberseguridad: Prevención, análisis y respuesta a incidentes de seguridad	49 horas
UA1	**Conocimiento del Gobierno de seguridad de una organización** • Componentes del gobierno de seguridad • Establecimiento de políticas y procedimientos de seguridad • Cumplimiento de las normas de seguridad • Auditorias de seguridad y evaluación de cumplimento	9
	Cuestionario de evaluación	0,5
	Tiempo total de la unidad de aprendizaje	**9,5**
UA2	**Identificación de las acciones preventivas que se deben planificar para evitar incidentes** • Identificación de amenazas cibernéticas comunes • Análisis de riesgos y vulnerabilidades • Evaluación de impacto y probabilidad de incidentes • Selección de medidas preventivas y correctivas	9
	Cuestionario de evaluación	0,5
	Tiempo total de la unidad de aprendizaje	**9,5**
UA3	**Recolección de evidencias tras un ataque** • Identificación de diferentes tipos de ataques e incidentes que pueden darse en una empresa • Utilización de técnicas y recursos para el análisis de datos	8
	Cuestionario de evaluación	0,5
	Tiempo total de la unidad de aprendizaje	**8,5**
UA4	**Creación de un plan de respuesta ante incidentes** • Respuesta a incidentes de seguridad • Etapas de la respuesta a incidentes de seguridad • Criptografía • Plan de recuperación ante desastres • Beneficios de un plan de recuperación ante desastres	9,5
	Cuestionario de evaluación	0,5
	Tiempo total de la unidad de aprendizaje	**10**

IFCT103	Ciberseguridad: Prevención, análisis y respuesta a incidentes de seguridad	49 horas
UA5	**Práctica de Hacking Ético** • Introducción al hacking ético y su importancia • Metodología de hacking ético • Identificación y explotación de vulnerabilidades • Uso de herramientas de hacking ético • Elaboración de informes y recomendaciones de seguridad	9
	Cuestionario de evaluación	0,5
	Tiempo total de la unidad de aprendizaje	**9,5**
	Prueba final tipo test	**1**
	Prueba de evaluación práctica	**1**