Guía didáctica

IFCT121. Ciberseguridad. Riesgos y amenazas en la red

INTRODUCCIÓN

En este programa, exploraremos los desafíos y peligros que enfrentamos en el entorno digital actual. A lo largo del curso, adquirirás conocimientos avanzados sobre nuestra identidad digital, aprenderás sobre las ciberamenazas y técnicas de defensa, te familiarizarás con los lenguajes de programación en ciberseguridad, desarrollarás habilidades de detección y análisis de riesgos, y aprenderás a implementar buenas prácticas en el entorno digital.

OBJETIVO GENERAL

Concienciar a los usuarios de los posibles riesgos que pueden afectarle a nivel individual y de empresa, así como facilitarles una serie de “buenas prácticas” que puedan aplicar no sólo en su espacio de trabajo sino también en su vida personal.

CONTENIDO FORMATIVO

IFCT121	Ciberseguridad. Riesgos y amenazas en la red	10 horas
UA1	**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
UA2	**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 ciber-entorno. • Capacidad para minimizar los daños causados por los posibles ciberincedentes.	2
UA3	**Conocimiento avanzado de los lenguajes de programación en ciberseguridad** • Conocimiento del lenguaje común de los ciberriesgos. • Conocimiento de los principales lenguajes de programación orientados a la ciberseguridad. • Conocer los lenguajes que utilizan los hackers.	1
UA4	**Detección, análisis y anticipación a los riesgos de seguridad** • Conocimiento sobre las vulnerabilidades y riesgos de seguridad informática. • Detección, análisis y anticipación a los riesgos de seguridad. • Conocimiento sobre los comportamientos que ponen en riesgo nuestra seguridad en entornos digitales. • Capacidad de detección incipiente de los riesgos y minimización de los efectos de los daños producidos en la seguridad digital.	2

IFCT121	Ciberseguridad. Riesgos y amenazas en la red	10 horas
UA5	**Implementación de buenas prácticas en entorno digital.** • Capacidad de búsqueda y localización de información sobre buenas prácticas en las entidades oficiales de gestión de la ciberseguridad (CCN-CERT o INCIBE). • Capacidad de implementar buenas prácticas en el entorno digital a través del conocimiento de los principales mecanismos de protección (gestión segura de contraseñas, gestión y control de los sistemas de antivirus, control de accesos y aplicaciones críticas, etc.). • Capacidad de identificación y clasificación de la información que se maneja en entorno digital y aplicación de las medidas necesarias para su protección que se plasmará en distintas políticas de seguridad informática.	2
	Cuestionario de evaluación	0,5
	Actividad de evaluación	0,5
	Tiempo total de la unidad de aprendizaje	**10**