

Ciberseguridad IFCT0023

Ciberseguridad IFCT0023

Duración: 60 horas

Precio: consultar euros.

Modalidad: e-learning

Metodología:

El Curso será desarrollado con una metodología a Distancia/on line. El sistema de enseñanza a distancia está organizado de tal forma que el alumno pueda compatibilizar el estudio con sus ocupaciones laborales o profesionales, también se realiza en esta modalidad para permitir el acceso al curso a aquellos alumnos que viven en zonas rurales lejos de los lugares habituales donde suelen realizarse los cursos y que tienen interés en continuar formándose. En este sistema de enseñanza el alumno tiene que seguir un aprendizaje sistemático y un ritmo de estudio, adaptado a sus circunstancias personales de tiempo

El alumno dispondrá de un extenso material sobre los aspectos teóricos del Curso que deberá estudiar para la realización de pruebas objetivas tipo test. Para el aprobado se exigirá un mínimo de 75% del total de las respuestas acertadas.

El Alumno tendrá siempre que quiera a su disposición la atención de los profesionales tutores del curso. Así como consultas telefónicas y a través de la plataforma de teleformación si el curso es on line. Entre el material entregado en este curso se adjunta un documento llamado Guía del Alumno dónde aparece un horario de tutorías telefónicas y una dirección de e-mail dónde podrá enviar sus consultas, dudas y ejercicios El alumno cuenta con un período máximo de tiempo para la finalización del curso, que dependerá del tipo de curso elegido y de las horas del mismo.

© icaformación2026

Profesorado:

Nuestro Centro fundado en 1996 dispone de 1000 m2 dedicados a formación y de 7 campus virtuales.

Tenemos una extensa plantilla de profesores especializados en las diferentes áreas formativas con amplia experiencia docentes: Médicos, Diplomados/as en enfermería, Licenciados/as en psicología, Licencidos/as en odontología, Licenciados/as en Veterinaria, Especialistas en Administración de empresas, Economistas, Ingenieros en informática, Educadodores/as sociales etc…

El alumno podrá contactar con los profesores y formular todo tipo de dudas y consultas de las siguientes formas:

-Por el aula virtual, si su curso es on line
-Por e-mail
-Por teléfono

Medios y materiales docentes

-Temario desarrollado.

-Pruebas objetivas de autoevaluación y evaluación.

-Consultas y Tutorías personalizadas a través de teléfono, correo, fax, Internet y de la Plataforma propia de Teleformación de la que dispone el Centro.



© icaformación2026

Titulación:

Una vez finalizado el curso, el alumno recibirá por correo o mensajería la titulación que acredita el haber superado con éxito todas las pruebas de conocimientos propuestas en el mismo.

Programa del curso:

OBJETIVOS 42120 IFCT0023 CIBERSEGURIDAD ? Objetivo principal: Proporcionar a los participantes los conocimientos teóricos y prácticos fundamentales sobre ciberseguridad, incluyendo la gestión de la seguridad en Internet, el uso crítico y seguro de las tecnologías digitales, la protección de datos, la identificación y prevención de ciberdelitos, y la implementación de medidas avanzadas para evitar el ingreso de intrusos, con el fin de mejorar la resiliencia digital en entornos personales y profesionales. ? Objetivos secundarios: Desarrollar habilidades en la gestión de la seguridad en Internet, identificando los elementos clave que garantizan una navegación y comunicación seguras, tanto a nivel individual como empresarial.. Aplicar estrategias de uso seguro y crítico en Internet, fomentando una actitud analítica ante la información, minimizando riesgos de ciberataques y mejorando la privacidad en el entorno digital. Analizar el marco legal, regulaciones y principios éticos en ciberseguridad y protección de datos, incluyendo la normativa vigente en 2025 y la regulación de la inteligencia artificial, para garantizar el cumplimiento normativo y la protección de la información personal y corporativa. Identificar y clasificar ciberdelitos y ciberincidentes, con base en la clasificación de ENISA y las amenazas emergentes en 2025, para desarrollar estrategias de prevención y mitigación de riesgos. Implementar medidas efectivas para protegerse del ingreso de intrusos, aplicando herramientas y metodologías de defensa en profundidad para fortalecer la seguridad de sistemas y redes ante accesos no autorizados. Asimilar la teoría de nodos y lazos en ciberseguridad, comprendiendo sus aplicaciones en la protección de infraestructuras digitales, la detección de vulnerabilidades y la optimización de la seguridad en redes de comunicación El curso incluye material educativo adicional para reforzar el aprendizaje, entre los que se encuentran: ? 24 vídeos explicativos ? 17 guías descargables ? 8 supuestos prácticos ? Glosario de términos y bibliografía especializada Este contenido complementario permitirá a los participantes profundizar en cada tema y aplicar los conocimientos adquiridos en situaciones reales.

TEMA 1 APROXIMACIÓN A LA CIBERSEGURIDAD ? Qué es la ciberseguridad ? Herramientas y plataformas nacionales de ciberseguridad ? Uso seguro de Inteligencia Artificial TEMA 2 GESTIÓN DE LA SEGURIDAD EN INTERNET ? En qué consiste la gestión de la seguridad en Internet ? Elementos clave de la gestión de la seguridad en Internet TEMA 3 USO SEGURO Y CRÍTICO EN INTERNET ? En qué consiste el uso seguro y crítico en Internet ? Elementos clave del uso seguro y crítico en Internet TEMA 4 CONOCIMIENTO DE ASPECTOS LEGALES, REGULATORIOS Y ÉTICOS RELACIONADOS CON LA PROTECCIÓN DE DATOS ? Marco legal en ciberseguridad ? Protección de datos. Ética y principios ? Regulación de la Inteligencia Artificial TEMA 5 CONOCIMIENTO SOBRE LOS CIBERDELITOS ? Clasificación de los ciberincidentes según ENISA ? Tipos de ciberdelitos en 2025 TEMA 6 ADAPTACIÓN DE MEDIDAS SOBRE CÓMO PROTEGERSE DEL INGRESO DE INTRUSOS ? Medidas para protegerse del ingreso de intrusos TEMA 7 ASIMILACIÓN DE

© icaformación2026

LA TEORÍA DE NODOS Y LAZOS ? Aplicaciones de la teoría de nodos y lazos ANEXO ? Glosario de términos ? Bibliografía ? Supuestos prácticos

© icaformación2026