

EL PERITAJE INFORMATICO DESDE EL AMBITO JUDICIAL

EL PERITAJE INFORMATICO DESDE EL AMBITO JUDICIAL

Duración: 60 horas

Precio: consultar euros.

Modalidad: e-learning

Objetivos:

Descripción: Conocer los fundamentos teórico-prácticos para la realización de informes periciales informáticos. Conocer los ámbitos de actuación de un Perito Judicial en Seguridad Informática. Fundamentación: Ataques contra la protección de datos personales, fraudes digitales, espionaje industrial, phising… El contexto jurídico actual requiere de estudios e investigaciones orientados a la obtención de pruebas informáticas como argumentos judiciales sobre la culpabilidad o inocencia de una de las partes. El temario y los contenidos del curso compaginan contenido teórico (aspectos formales del peritaje informático, legislación y estándares) con material práctico basado en las últimas técnicas y herramientas de análisis forense.

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:

TEMA 1. DERECHOS, DEBERES Y CODIGO DEONTOLOGICO DEL PERITO INFORMATICO

1. INTRODUCCIÓN
2. SITUACIÓN JURÍDICA Y NUEVAS TECNOLOGÍAS
3. PERITO JUDICIAL INFORMÁTICO Y EL ANÁLISIS FORENSE
4. DERECHOS DEL PERITO INFORMÁTICO JUDICIAL
5. DEBERES DEL PERITO INFORMÁTICO JUDICIAL
6. ÁREAS DE ACTUACIÓN DEL PERITO
7. RESPONSABILIDADES DEL PERITO INFORMÁTICO JUDICIAL
8. CÓDIGO DEONTOLÓGICO
9. AUTORIZACIÓN PROFESIONAL EN ESPAÑA

TEMA 2. EVIDENCIAS DIGITALES Y EVIDENCIAS JUDICIALES

1. INTRODUCCIÓN
2. INFORMÁTICA FORENSE
3. EVIDENCIAS Y EQUIPAMIENTO FORENSE
4. METODOLOGÍA DE ANÁLISIS FORENSE
5. EVALUACIÓN DE LA SITUACIÓN
6. EVIDENCIAS Y PRUEBAS JUDICIALES
7. BÚSQUEDA Y EXTRACCIÓN DE EVIDENCIAS
8. PROCESO DE ADQUISICIÓN DE EVIDENCIAS

TEMA 3. ORGANISMOS RELACIONADOS CON LA CIBERSEGURIDAD INTERNACIONALES

1. INTRODUCCIÓN
2. INFORMES DE CIBERSEGURIDAD
3. ENISA
4. UIT-D UNIÓN EUROPEA

TEMA 4. ORGANISMOS RELACIONADOS CON LA CIBERSEGURIDAD NACIONAL

1. INTRODUCCIÓN

© icaformación2026

2. INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA INFORMACIÓN (INTECO)
3. OFICINA DE SEGURIDAD DEL INTERNAUTA (OSI)
4. UIT-D UNIÓN TELECOMUNICACIONES
5. SECRETARIA DE ESTADO TELECOMUNICACIONES (SETSI)
6. CENATIC
7. COMISIÓN DEL MERCADO DE LAS TELECOMUNICACINES (CMT)

TEMA 5. ASPECTOS LEGALES Y REGULATORIOS

1. INTRODUCCIÓN
2. REGULACIÓN SOBRE LA PROTECCIÓN DE DATOS
3. PRINCIPIOS RELATIVOS A LA PROTECCIÓN DE DATOS
4. AGENCIA DE PROTECCIÓN DE DATOS Y EL REGISTRO GENERAL

TEMA 6. REGULACION NACIONAL. LOPD Y Rº DE LA LOPD

1. INTRODUCCIÓN
2. DERECHOS DE LOS CIUDADANOS EN LA LOPD
3. ADAPTACIÓN A LA NORMATIVA VIGENTE
4. CREACIÓN, MODIFICACIÓN Y SUPRESIÓN DE FICHEROS
5. NOTIFICACIÓN E INSCRIPCIÓN DE LOS FICHEROS DE TITULARIDAD
6. SEGURIDAD EN EL TRATAMIENTO DE DATOS PERSONALES
7. NIVELES DE FICHEROS Y MEDIDAS DE SEGURIDAD
8. SANCIONES POR INCUMPLIMIENTO

© icaformación2026