

POLÍTICAS Y NORMATIVAS Y GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

POLÍTICAS Y NORMATIVAS Y GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Duración: 60 horas

Precio: consultar euros.

Modalidad: e-learning

Objetivos:

Descripción: Aprender los aspectos fundamentales de la legislación Española que afecta a los peritos judiciales informáticos Aplicar los distintos estándares para la elaboración de informes periciales informáticos. 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. QUE ES UNA POLITICA DE SEGURIDAD (PSI), DESARROLLO DE UN PLAN DE POLITICAS DE SEGURIDAD INFORMATICA

- FUNDAMENTOS DE SEGURIDAD: LOS CINCO PILARES
- CONSTRUYENDO UN PROGRAMA DE SEGURIDAD
- LA POLÍTICA ES LA PIEDRA ANGULAR
- DEFINICIONES
- ELEMENTOS CLAVES DE UNA POLÍTICA
- FORMATO DE UNA POLÍTICA
- COMPRENSIÓN DEL GOBIERNO DE LA SEGURIDAD DE LA INFORMACIÓN

TEMA 2. AUDITORIA DEL SISTEMA DE SEGURIDAD Y ANALISIS DE RIESGOS

- INTRODUCCIÓN
- CICLO DE VIDA DE LA GESTIÓN DEL RIEGO
- ESFUERZO DE PREPARACIÓN PARA LA GESTIÓN DE RIESGOS
- UNA CULTURA DE SEGURIDAD SOSTENIBLE
- INFORMACIÓN NECESARIA PARA MANEJAR RIESGOS
- FACTORES QUE AFECTAN A LOS RIESGOS DE SEGURIDAD
- METODOLOGÍA DE RIEGO ALE
- RIESGOS OPERACIONALES, FUNCIONALES Y ESTRATÉGICOS
- CÓMO, QUÉ, Y POR QUÉ AUDITAR

TEMA 3. LA NORMA ISO/IEC 27001 E IMPLANTACION DEL MODELO SG SI

- INTRODUCCIÓN
- COMO LAS ORGANIZACIONES INTERACTÚAN CON LAS NORMAS
- MARCO GENERAL ISMS
- MODELO DE ISMS
- ESTRATEGIA DE PROCESOS QUE ASEGURA LA MEJORA CONTINUA DEL ISMS
- DESARROLLO DEL SISTEMA GESTOR DE SEGURIDAD DE LA INFORMACIÓN
- DISEÑO DEL ISMS
- NECESIDADES DE UN INVENTARIO DE SEGURIDAD
- INTEGRACIÓN DE SUBSISTEMAS ISMS

© icaformación2026

AUTOEVALUACIÓN DE CUMPLIMIENTO
NUEVA VISITA AL ÁMBITO ISMS

TEMA 4. CUMPLIMIENTO Y GESTION DE LA SEGURIDAD

DIRECCIÓN DEL CUMPLIMIENTO
INTRODUCCIÓN A LA DIRECCIÓN DEL CUMPLIMIENTO
IA CMP

TEMA 5. GESTION DE RIESGOS E INDICADORES DE RIESGO TECNOLOGICO (KRI'S)

INTRODUCCIÓN
DESCRIPCIÓN DE FRAAP (ANÁLISIS DE RIEGOS Y PROCESO DE EVALUACIÓN FACILITADO)
HISTORIA DE FRAAP
PRESENTACIÓN DEL FRAAP
LA REUNIÓN PRE-FRAAP
LA SESIÓN FRAAP
IDENTIFICACIÓN DE AMENAZAS FRAAP
IDENTIFICACIÓN DE CONTROLES EXISTENTES
ESTABLECER EL NIVEL DE RIESGO
RIESGO RESIDUAL
RESUMEN DE LA SESIÓN FRAAP
COMPLETAR EL PLAN DE ACCIÓN

© icaformación2026