



**EUROINNOVA**  
BUSINESS  
SCHOOL



**FORMACIÓN  
ONLINE**

Titulación certificada por EUROINNOVA BUSINESS SCHOOL



## Master en Informática Forense y Delitos Informáticos + Titulación Universitaria

[www.euroinnova.edu.es](http://www.euroinnova.edu.es)



LLAMA GRATIS: (+34) 900 831 200





EUROINNOVA FORMACIÓN

## Especialistas en **Formación Online**

### **SOBRE EUROINNOVA BUSINESS SCHOOL**

Bienvenidos/as a EUROINNOVA BUSINESS SCHOOL, una escuela de negocios apoyada por otras entidades de enorme prestigio a nivel internacional, que han visto el valor humano y personal con el que cuenta nuestra empresa; un valor que ha hecho que grandes instituciones de reconocimiento mundial se sumen a este proyecto.



EUROINNOVA BUSINESS SCHOOL es la mejor opción para formarse ya que contamos con años de experiencia y miles de alumnos/as, además del reconocimiento y apoyo de grandes instituciones a nivel internacional.

Como entidad acreditada para la organización e impartición de formación de postgrado, complementaria y para el empleo, Euroinnova es centro autorizado para ofrecer formación continua bonificada para personal trabajador, **cursos homologados y baremables** para Oposiciones dentro de la Administración Pública, y cursos y acciones formativas de **máster online** con título propio.



**CERTIFICACIÓN  
EN CALIDAD**

Euroinnova Business School es miembro de pleno derecho en la Comisión Internacional de Educación a Distancia, (con estatuto consultivo de categoría especial del Consejo Económico y Social de NACIONES UNIDAS), y cuenta con el Certificado de Calidad de la Asociación Española de Normalización y Certificación (AENOR) de acuerdo a la normativa ISO 9001, mediante la cual se Certifican en Calidad todas las acciones formativas impartidas desde el centro.





## DESCUBRE EUROINNOVA FORMACIÓN

# Líderes en Formación Online



### APOSTILLA DE LA HAYA

Además de disponer de formación avalada por universidades de reconocido prestigio y múltiples instituciones, Euroinnova posibilita certificar su formación con la Apostilla de La Haya, dotando a sus acciones formativas de Titulaciones Oficiales con validez internacional en más de 160 países de todo el mundo.



### PROFESIONALES A TU DISPOSICION

La metodología virtual de la formación impartida en Euroinnova está completamente a la vanguardia educativa, facilitando el aprendizaje a su alumnado, que en todo momento puede contar con el apoyo tutorial de grandes profesionales, para alcanzar cómodamente sus objetivos.



### DESCUBRE NUESTRAS METODOLOGÍAS

Desde Euroinnova se promueve una enseñanza multidisciplinar e integrada, desarrollando metodologías innovadoras de aprendizaje que permiten interiorizar los conocimientos impartidos con una aplicación eminentemente práctica, atendiendo a las demandas actuales del mercado laboral.





### NUESTRA EXPERIENCIA NOS AVALA

Más de 15 años de experiencia avalan la trayectoria del equipo docente de Euroinnova Business School, que desde su nacimiento apuesta por superar los retos que deben afrontar los/las profesionales del futuro, lo que actualmente lo consolida como el centro líder en formación online.




## Master en Informática Forense y Delitos Informáticos + Titulación Universitaria

 **DURACIÓN:**  
725 horas

 **MODALIDAD:**  
Online

 **PRECIO:**  
1.495 € \*

 **CRÉDITOS:**  
5,00 ECTS

\* Materiales didácticos, titulación y gastos de envío incluidos.

### CENTRO DE FORMACIÓN:

Euroinnova Business  
School



EUROINNOVA  
BUSINESS  
SCHOOL

## TITULACIÓN

Doble Titulación: - Titulación de Master en Informática Forense y Delitos Informáticos con 600 horas expedida por EUROINNOVA INTERNATIONAL ONLINE EDUCATION, miembro de la AEEN (Asociación Española de Escuelas de Negocios) y CLADEA (Consejo Latinoamericano de Escuelas de Administración) - Titulación Universitaria en Consultor en Seguridad Informática IT: Ethical Hacking con 5 Créditos Universitarios ECTS. Formación Continua baremable en bolsas de trabajo y concursos oposición de la Administración Pública.



EUROINNOVA  
BUSINESS  
SCHOOL

TITULACIÓN EXPEDIDA POR  
EUROINNOVA BUSINESS SCHOOL  
CENTRO DE ESTUDIOS DE POSTGRADO



3ª Mejor Escuela de Negocios  
España  
(RANKING EL ECONOMISTA)





Una vez finalizado el curso, el alumno recibirá por parte de Euroinnova Formación vía correo postal, la titulación que acredita el haber superado con éxito todas las pruebas de conocimientos propuestas en el mismo.

Esta titulación incluirá el nombre del curso/master, la duración del mismo, el nombre y DNI del alumno, el nivel de aprovechamiento que acredita que el alumno superó las pruebas propuestas, las firmas del profesor y Director del centro, y los sellos de la instituciones que avalan la formación recibida (Euroinnova Formación, Instituto Europeo de Estudios Empresariales y Comisión Internacional para la Formación a Distancia de la UNESCO).



## DESCRIPCIÓN

La informática forense se trata de una disciplina que consiste en uso de técnicas científicas y analíticas con la finalidad de identificar, analizar y presentar pruebas que sean válidas dentro de un proceso legal en relación al uso de tecnologías informáticas. Por medio del presente master informática forense podrás realizar análisis forenses e informes periciales de manera profesional que sirvan como pruebas judiciales en cualquier juicio donde se investiguen delitos informáticos.



## OBJETIVOS

Entre los principales objetivos del master informática forense podemos destacar los siguientes:

- Descubrir la importancia del peritaje informático y el papel del perito informático.
- Utilizar las principales técnicas de ciberseguridad y hacking ético para el análisis forense.
- Evitar la cibercriminalidad mediante la búsqueda de pruebas periciales en los análisis forenses.
- Conocer las etapas que se desarrollan en un análisis forense.
- Seguir el marco normativo actual que rige la ciberseguridad y los delitos informáticos.
- Realizar informes periciales gracias a pruebas periciales extraídas del análisis forense.
- Identificar los elementos funcionales de un sistema informático.
- Conocer aspectos tan importantes como lo son la ciberseguridad y la cibercriminalidad.
- Indicar las etapas implicadas en un análisis forense.
- Implantar un Sistema de Gestión de Seguridad en la Información SGSI.
- Conocer las funciones, procedimientos, técnicas e instrumentos de la Peritación judicial.
- Conocer los diferentes tipos de Peritaje que podemos encontrarnos.
- Interpretar el sistema de mediación y la importancia de éste en la implicación de los afectados.
- Conocer la definición precisa de los diferentes tipos de hackers y de sus objetivos.
- Aprender sobre la metodología de un ataque y los medios para identificar las vulnerabilidades o fallos de seguridad a través de los que introducirse en un sistema.
- Conocer los fallos físicos, que permiten un acceso directo a ordenadores, y los fallos de red y Wi-Fi se presentan e ilustran cada uno con propuestas de contramedidas.
- Saber sobre el Cloud Computing (su historia, su funcionamiento) para dominar mejor la seguridad.
- Tener en cuenta la seguridad en la web y los fallos actuales identificados gracias a la ayuda de herramientas que el lector puede implantar fácilmente en sus propios sistemas.
- Identificar siempre los posibles fallos para establecer después la estrategia de protección adecuada.
- Conocer algunos ejemplos los fallos de sistemas en Windows o Linux y los fallos de aplicación, para familiarizarse con el lenguaje ensamblador y comprender mejor las posibilidades de ataque.

## A QUIÉN VA DIRIGIDO

El master informática forense se dirige tanto a estudiantes como a profesionales del mundo informático o jurídico y otros afines que tengan interés en formarse para aprender a realizar análisis forense e informes periciales permitiendo la mejora de la ciberseguridad y asegurando la aplicación de la legislación mediante pruebas periciales.





## PARA QUÉ TE

Gracias al master infromatica forense conocerás las mejores técnicas utilizadas en la realización de análisis forenses e informes periciales que sirvan como prueba en un proceso legal.

## SALIDAS LABORALES

Perito informático forense, Experto en Ciberseguridad o Auditor de Sistemas de Seguridad.

## MATERIALES DIDÁCTICOS



- Maletín porta documentos
- Manual teórico 'Derecho y Nuevas Tecnologías'
- Manual teórico 'Cibercrimen: Delitos contra la Protección de Datos y la Identidad en Internet'





- Manual teórico 'Perito Judicial'
- Manual teórico 'Informática y Electrónica Forense'
- Manual teórico 'Ethical Hacking'
- Manual teórico 'Informática Forense'
- Subcarpeta portafolios
- Dossier completo Oferta Formativa
- Carta de presentación
- Guía del alumno
- Bolígrafo

## FORMAS DE PAGO

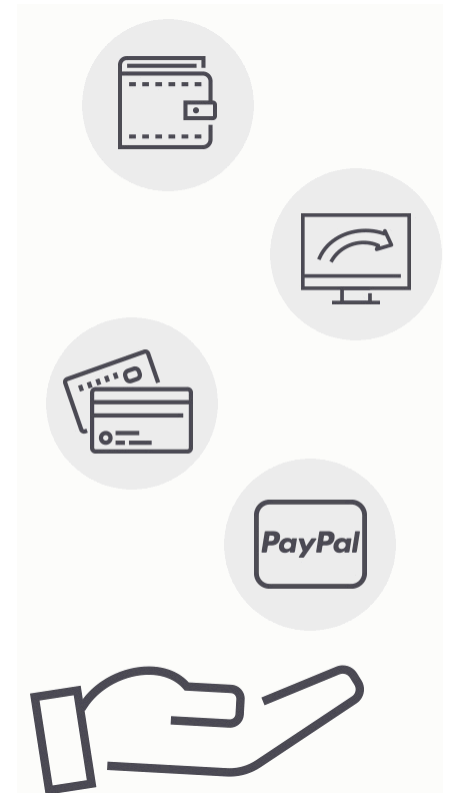
Contrareembolso / Transferencia / Tarjeta de Crédito / Paypal

Tarjeta de Crédito / PayPal Eligiendo esta opción de pago, podrá abonar el importe correspondiente, cómodamente en este mismo instante, a través de nuestra pasarela de pago segura concertada con Paypal Transferencia Bancaria Eligiendo esta opción de pago, deberá abonar el importe correspondiente mediante una transferencia bancaria. No será aceptado el ingreso de cheques o similares en ninguna de nuestras cuentas bancarias.

Contrareembolso Podrá pagar sus compras directamente al transportista cuando reciba el pedido en su casa . Eligiendo esta opción de pago, recibirá mediante mensajería postal, en la dirección facilitada

Otras: PayU, Sofort, Western Union / SafetyPay

Fracciona tu pago en cómodos Plazos sin Intereses + Envío







Llama gratis al 900 831 200 e infórmate de nuestras facilidades de pago.

## FINANCIACIÓN Y BECAS

Facilidades  
económicas y  
financiación  
100% sin  
intereses

En EUROINNOVA, ofrecemos a nuestros alumnos facilidades económicas y financieras para la realización de pago de matrículas, todo ello 100% sin intereses.

10% Beca Alumnos :Como premio a la fidelidad y confianza ofrecemos una beca a todos aquellos que hayan cursado alguna de nuestras acciones formativas en el pasado.

### 10% PARA ANTIGUOS ALUMNOS

.....  
Queremos agradecer tu fidelidad y la confianza depositada en Euroinnova Formación.

10  
%

BECA  
Antiguos  
Alumnos

## METODOLOGÍA Y TUTORIZACIÓN





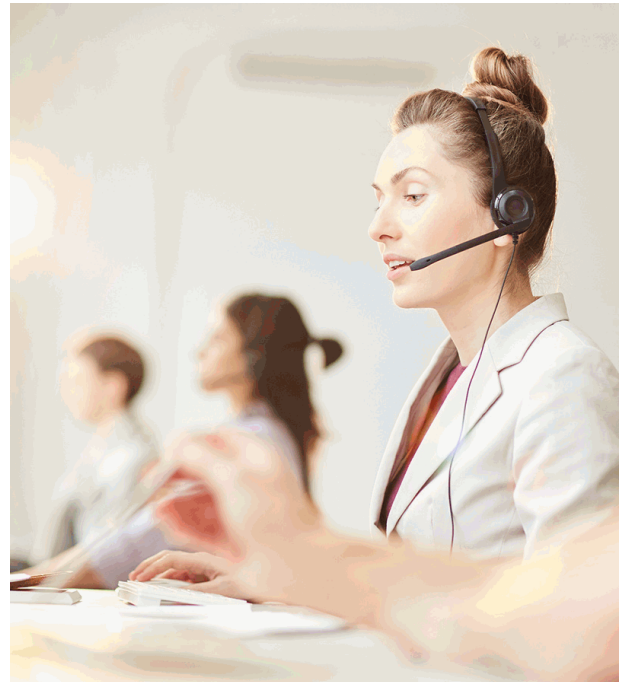
El modelo educativo por el que apuesta Euroinnova es el aprendizaje colaborativo con un método de enseñanza totalmente interactivo, lo que facilita el estudio y una mejor asimilación conceptual, sumando esfuerzos, talentos y competencias.

El alumnado cuenta con un equipo docente especializado en todas las áreas.

Proporcionamos varios medios que acercan la comunicación alumno tutor, adaptándonos a las circunstancias de cada usuario.

Ponemos a disposición una plataforma web en la que se encuentra todo el contenido de la acción formativa. A través de ella, podrá estudiar y comprender el temario mediante actividades prácticas, autoevaluaciones y una evaluación final, teniendo acceso al contenido las 24 horas del día.

Nuestro nivel de exigencia lo respalda un acompañamiento



## CARÁCTER OFICIAL DE LA FORMACIÓN

La presente formación no está incluida dentro del ámbito de la formación oficial reglada (Educación Infantil, Educación Primaria, Educación Secundaria, Formación Profesional Oficial FP, Bachillerato, Grado Universitario, Master Oficial Universitario y Doctorado). Se trata por tanto de una formación complementaria y/o de especialización, dirigida a la adquisición de determinadas competencias, habilidades o aptitudes de índole profesional, pudiendo ser baremable como mérito en bolsas de trabajo y/o concursos oposición, siempre dentro del apartado de Formación Complementaria y/o Formación Continua siendo siempre imprescindible la revisión de los requisitos específicos de baremación de las bolsa de trabajo público en concreto a la que deseemos presentarnos.

## REDES SOCIALES



Síguenos en nuestras redes sociales y pasa a formar parte de nuestra gran comunidad educativa, donde podrás participar en foros de opinión, acceder a contenido de interés, compartir material didáctico e interactuar con otros alumnos, ex alumnos y profesores.

Además serás el primero en enterarte de todas las promociones y becas mediante nuestras publicaciones, así como también podrás contactar directamente para obtener información o resolver tus dudas.



## LÍDERES EN FORMACION ONLINE

### Somos Diferentes



#### Ampio **Catálogo** Format

Nuestro catálogo está formado por más de 18.000 cursos de múltiples áreas de conocimiento, adaptándonos a las necesidades formativas de nuestro alumnado.



#### Confianza

Contamos con el Sello de Confianza Online que podrás encontrar en tus webs de confianza. Además colaboramos con las más prestigiosas Universidades, Administraciones Públicas y Empresas de Software a nivel





## Campus Online

Nuestro alumnado puede acceder al campus virtual desde cualquier dispositivo, contando con acceso ilimitado a los contenidos de su programa formativo.



## Profesores/as Especialis

Contamos con un equipo formado por más de 50 docentes con especialización y más de 1.000 colaboradores externos a la entera disposición de nuestro alumnado.



## Bolsa de Empleo

Disponemos de una bolsa de empleo propia con diferentes ofertas de trabajo correspondientes a los distintos cursos y masters. Somos agencia de colaboración N° 9900000169 autorizada por el Ministerio de Empleo y Seguridad Social.



## Garantía de Satisfacción

Más de 15 años de experiencia con un récord del 96% de satisfacción en atención al alumnado y miles de opiniones de personas satisfechas nos avalan.



## Precios Competitivos

Garantizamos la mejor relación calidad/precio en todo nuestro catálogo formativo.



## Calidad AENOR

Todos los procesos de enseñanza aprendizaje siguen los más rigurosos controles de calidad extremos, estando certificados por AENOR conforme a la ISO 9001, llevando a cabo auditorías externas que garantizan la máxima calidad.



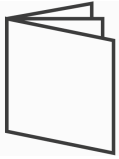
## Club de Alumnos/as

Servicio Gratuito que permitirá al alumnado formar parte de una extensa comunidad virtual que ya disfruta de múltiples ventajas: beca, descuentos y promociones en formación. En esta, el alumnado podrá relacionarse con personas que estudian la misma área de conocimiento, compartir opiniones, documentos, prácticas y un sinfín de



## Bolsa de Prácticas

Facilitamos la realización de prácticas de empresa gestionando las ofertas profesionales dirigidas a nuestro alumnado, para realizar prácticas relacionadas con la formación que ha estado recibiendo



### Revista Digital

El alumnado podrá descargar artículos sobre e-learning, publicaciones sobre formación a distancia, artículos de opinión, noticias sobre convocatorias de oposiciones, concursos públicos de la administración, ferias sobre formación, y otros recursos



### Innovación y Calidad

Ofrecemos el contenido más actual y novedoso, respondiendo a la realidad empresarial y al entorno cambiante con una alta rigurosidad académica combinada con formación práctica.

## ACREDITACIONES Y RECONOCIMIENTOS





## TEMARIO

# PARTE 1. INFORMÁTICA Y ELECTRÓNICA FORENSE

## UNIDAD DIDÁCTICA 1. INFORMÁTICA, CONECTIVIDAD E INTERNET

1. La informática
  - 1.- Conceptos básicos
2. Componentes de un sistema informático
3. Estructura básica de un sistema informático
4. Unidad central de proceso en un sistema informático
  - 1.- Estructura
5. Periféricos más usuales: conexión
6. Sistema operativo
7. Internet
8. Conectividad a Internet
  - 1.- Tipos de redes
  - 2.- Red inalámbrica

## UNIDAD DIDÁCTICA 2. FUNDAMENTOS DE LA INFORMÁTICA Y ELECTRÓNICA FORENSE

1. Concepto de informática forense
2. Objetivos de la informática forense
3. Usos de la informática forense
4. El papel del perito informático
5. El laboratorio informático forense
6. Evidencia digital
  - 1.- Evidencias volátiles y no volátiles
  - 2.- Etiquetado de evidencias
7. Cadena de custodia

## UNIDAD DIDÁCTICA 3. CIBERSEGURIDAD

1. El ciberespacio y su seguridad
2. Riesgos y amenazas de la ciberseguridad
  - 1.- Amenazas internas y externas
  - 2.- Principales riesgos y amenazas
3. Objetivos de la ciberseguridad
4. Líneas de acción de la ciberseguridad nacional
5. Instituto Nacional de Ciberseguridad

## UNIDAD DIDÁCTICA 4. CIBERCRIMINALIDAD

1. Delito informático
  - 1.- Principales características del delito informático
2. Tipos de delito informático
3. Cibercriminalidad
  - 1.- Evolución de la sociedad española en el empleo de las nuevas tecnologías. Los delitos cibernéticos





### **UNIDAD DIDÁCTICA 5. HACKING ÉTICO**

1. ¿Qué es el hacking ético?
  - 1.- Ética hacker
  - 2.- Valores de la ética hacker
  - 3.- Fases del Hacking Ético
  - 4.- Tipo de Hacking Ético
2. Aspectos legales del hacking ético
3. Perfiles del hacker
  - 1.- Hacker de sombrero negro
  - 2.- Hacker de sombrero blanco
  - 3.- Hacker de sombrero gris
  - 4.- Otros perfiles
4. Hacktivismo

### **UNIDAD DIDÁCTICA 6. ANÁLISIS FORENSE**

1. El análisis forense
2. Etapas de un análisis forense
  - 1.- Estudio preliminar
  - 2.- Adquisición de datos
  - 3.- Análisis e investigación
  - 4.- Presentación y realización del informe pericial
3. Tipos de análisis forense
4. Requisitos para el análisis forense
5. Principales problemas

### **UNIDAD DIDÁCTICA 7. SOPORTE DE DATOS**

1. Adquisición de datos: importancia en el análisis forense digital
2. Modelo de capas
3. Recuperación de archivos borrados
  - 1.- Dinámica del borrado de archivos
  - 2.- Características exigibles para recuperación de archivos y datos borrados
  - 3.- Principales herramientas para recuperación de datos
  - 4.- La acción de recuperación
4. Análisis de archivos
  - 1.- Firmas características
  - 2.- Documentos
  - 3.- Archivos gráficos y multimedia
  - 4.- Archivos ejecutables

### **UNIDAD DIDÁCTICA 8. SISTEMA DE GESTIÓN DE SEGURIDAD EN LA INFORMACIÓN SGSI**

1. La sociedad de la información
2. ¿Qué es la seguridad de la información?





- 3.Importancia de la seguridad de la información
- 4.Principios básicos de seguridad de la información: confidencialidad, integridad y disponibilidad
  - 1.- Principio Básico de Confidencialidad
  - 2.- Principio Básico de Integridad
  - 3.- Disponibilidad
- 5.Descripción de los riesgos de la seguridad
- 6.Selección de controles
- 7.Factores de éxito en la seguridad de la información
- 8.Introducción a los sistemas de gestión de seguridad de la información
- 9.Beneficios aportados por un sistema de seguridad de la información

#### **UNIDAD DIDÁCTICA 9. MARCO NORMATIVO**

- 1.Marco normativo
- 2.Normativa sobre seguridad de la información
  - 1.- Planes de acción para la utilización más segura de Internet
  - 2.- Estrategias para una sociedad de la información más segura
  - 3.- Ataques contra los sistemas de información
  - 4.- La lucha contra los delitos informáticos
  - 5.- La Agencia Europea de Seguridad de las Redes y de la información (ENISA)
- 3.Normativa relacionada con la ciberseguridad
- 4.Legislación sobre delitos informáticos

## **PARTE 2. INFORMÁTICA FORENSE**

#### **UNIDAD DIDÁCTICA 1. FUNDAMENTOS DE LA INFORMÁTICA Y ELECTRÓNICA FORENSE**

- 1.Concepto de informática forense
- 2.Objetivos de la informática forense
- 3.Usos de la informática forense
- 4.El papel del perito informático
- 5.El laboratorio informático forense
- 6.Evidencia digital
- 7.Cadena de custodia

#### **UNIDAD DIDÁCTICA 2. CIBERSEGURIDAD**

- 1.El ciberespacio y su seguridad
- 2.Riesgos y amenazas de la ciberseguridad
- 3.Objetivos de la ciberseguridad
- 4.Líneas de acción de la ciberseguridad nacional
- 5.Instituto Nacional de Ciberseguridad

#### **UNIDAD DIDÁCTICA 3. CIBERCRIMINALIDAD**

- 1.Delito informático
- 2.Tipos de delito informático







3. Cibercriminalidad

#### **UNIDAD DIDÁCTICA 4. HACKING ÉTICO**

1. ¿Qué es el hacking ético?
2. Aspectos legales del hacking ético
3. Perfiles del hacker
4. Test de vulnerabilidades
5. Sniffing
6. Tipos de test de seguridad en entornos web

#### **UNIDAD DIDÁCTICA 5. ANÁLISIS FORENSE**

1. El análisis forense
2. Etapas de un análisis forense
3. Tipos de análisis forense
4. Requisitos para el análisis forense
5. Principales problemas

#### **UNIDAD DIDÁCTICA 6. SOPORTE DE DATOS**

1. Adquisición de datos: importancia en el análisis forense digital
2. Modelo de capas
3. Recuperación de archivos borrados
4. Análisis de archivos

#### **UNIDAD DIDÁCTICA 7. MARCO NORMATIVO**

1. Marco normativo
2. Normativa sobre seguridad de la información
3. Normativa relacionada con la ciberseguridad
4. Legislación sobre delitos informáticos

## **PARTE 3. PERITO JUDICIAL**

### **MÓDULO 1. PERITO JUDICIAL**

#### **UNIDAD DIDÁCTICA 1. PERITACIÓN Y TASACIÓN**

1. Delimitación de los términos peritaje y tasación
2. La peritación
3. La tasación pericial

#### **UNIDAD DIDÁCTICA 2. NORMATIVA BÁSICA NACIONAL**

1. Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial
2. Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil
3. Ley de Enjuiciamiento Criminal, de 1882
4. Ley 1/1996, de 10 de enero, de Asistencia Jurídica Gratuita

#### **UNIDAD DIDÁCTICA 3. LOS PERITOS**

1. Concepto





2. Clases de perito judicial
3. Procedimiento para la designación de peritos
4. Condiciones que debe reunir un perito
5. Control de la imparcialidad de peritos
6. Honorarios de los peritos

#### **UNIDAD DIDÁCTICA 4. EL RECONOCIMIENTO PERICIAL**

1. El reconocimiento pericial
2. El examen pericial
3. Los dictámenes e informes periciales judiciales
4. Valoración de la prueba pericial
5. Actuación de los peritos en el juicio o vista

#### **UNIDAD DIDÁCTICA 5. LEGISLACIÓN REFERENTE A LA PRÁCTICA DE LA PROFESIÓN EN LOS TRIBUNALES**

1. Funcionamiento y legislación
2. El código deontológico del Perito Judicial

#### **UNIDAD DIDÁCTICA 6. LA RESPONSABILIDAD**

1. La responsabilidad
2. Distintos tipos de responsabilidad
  - 1.- Responsabilidad civil
  - 2.- Responsabilidad penal
  - 3.- Responsabilidad disciplinaria
3. El seguro de responsabilidad civil

#### **UNIDAD DIDÁCTICA 7. PERITACIONES**

1. La peritación médico-legal
  - 1.- Daño corporal
  - 2.- Secuelas
2. Peritaciones psicológicas
  - 1.- Informe pericial del peritaje psicológico
3. Peritajes informáticos
4. Peritaciones inmobiliarias

## **MÓDULO 2. LEGISLACIÓN NACIONAL APLICABLE AL SECTOR DEL PERITAJE**

# **PARTE 4. SEGURIDAD INFORMÁTICA IT: ETHICAL HACKING**

#### **UNIDAD DIDÁCTICA 1. INTRODUCCIÓN A LOS ATAQUES Y AL HACKING ÉTICO**

1. Introducción a la seguridad informática





- 2.El hacking ético
- 3.La importancia del conocimiento del enemigo
- 4.Seleccionar a la víctima
- 5.El ataque informático
- 6.Acceso a los sistemas y su seguridad
- 7.Análisis del ataque y seguridad

#### **UNIDAD DIDÁCTICA 2. SOCIAL ENGINEERING**

- 1.Introducción e historia del Social Engineering
- 2.La importancia de la Ingeniería social
- 3.Defensa ante la Ingeniería social

#### **UNIDAD DIDÁCTICA 3. LOS FALLOS FÍSICOS EN EL ETHICAL HACKING Y LAS PRUEBAS DEL ATAQUE**

- 1.Introducción
- 2.Ataque de Acceso físico directo al ordenador
- 3.El hacking ético
- 4.Lectura de logs de acceso y recopilación de información

#### **UNIDAD DIDÁCTICA 4. LA SEGURIDAD EN LA RED INFORMÁTICA**

- 1.Introducción a la seguridad en redes
- 2.Protocolo TCP/IP
- 3.IPv6
- 4.Herramientas prácticas para el análisis del tráfico en la red
- 5.Ataques Sniffing
- 6.Ataques DoS y DDoS
- 7.Ataques Robo de sesión TCP (HIJACKING) y Spoofing de IP
- 8.Ataques Man In The Middle (MITM).
- 9.Seguridad Wi-Fi
- 10.IP over DNS
- 11.La telefonía IP

#### **UNIDAD DIDÁCTICA 5. LOS FALLOS EN LOS SISTEMAS OPERATIVOS Y WEB**

- 1.Usuarios, grupos y permisos
- 2.Contraseñas
- 3.Virtualización de sistemas operativos
- 4.Procesos del sistema operativo
- 5.El arranque
- 6.Hibernación
- 7.Las RPC
- 8.Logs, actualizaciones y copias de seguridad
- 9.Tecnología WEB Cliente - Servidor
- 10.Seguridad WEB
- 11.SQL Injection





12.Seguridad CAPTCHA

13.Seguridad Akismet

14.Consejos de seguridad WEB

#### **UNIDAD DIDÁCTICA 6. ASPECTOS INTRODUCTORIOS DEL CLOUD COMPUTING**

1.Orígenes del cloud computing

2.Qué es cloud computing

1.- Definición de cloud computing

3.Características del cloud computing

4.La nube y los negocios

1.- Beneficios específicos

5.Modelos básicos en la nube

#### **UNIDAD DIDÁCTICA 7. CONCEPTOS AVANZADOS Y ALTA SEGURIDAD DE CLOUD COMPUTING**

1.Interoperabilidad en la nube

1.- Recomendaciones para garantizar la interoperabilidad en la nube

2.Centro de procesamiento de datos y operaciones

3.Cifrado y gestión de claves

4.Gestión de identidades

#### **UNIDAD DIDÁCTICA 8. SEGURIDAD, AUDITORÍA Y CUMPLIMIENTO EN LA NUBE**

1.Introducción

2.Gestión de riesgos en el negocio

1.- Recomendaciones para el gobierno

2.- Recomendaciones para una correcta gestión de riesgos

3.Cuestiones legales básicas. eDiscovery

4.Las auditorías de seguridad y calidad en cloud computing

5.El ciclo de vida de la información

1.- Recomendaciones sobre seguridad en el ciclo de vida de la información

#### **UNIDAD DIDÁCTICA 9. CARACTERÍSTICAS DE SEGURIDAD EN LA PUBLICACIÓN DE PÁGINAS WEB**

1.Seguridad en distintos sistemas de archivos.

1.- Sistema operativo Linux.

2.- Sistema operativo Windows.

3.- Otros sistemas operativos.

2.Permisos de acceso.

1.- Tipos de accesos

2.- Elección del tipo de acceso

3.- Implementación de accesos

3.Órdenes de creación, modificación y borrado.

1.- Descripción de órdenes en distintos sistemas

2.- Implementación y comprobación de las distintas órdenes.

#### **UNIDAD DIDÁCTICA 10. PRUEBAS Y VERIFICACIÓN DE PÁGINAS WEB**





1. Técnicas de verificación.
  - 1.- Verificar en base a criterios de calidad.
  - 2.- Verificar en base a criterios de usabilidad.
2. Herramientas de depuración para distintos navegadores.
  - 1.- Herramientas para Mozilla.
  - 2.- Herramientas para Internet Explorer.
  - 3.- Herramientas para Opera.
  - 4.- Creación y utilización de funciones de depuración.
  - 5.- Otras herramientas.
3. Navegadores: tipos y «plug-ins».
  - 1.- Descripción de complementos.
  - 2.- Complementos para imágenes.
  - 3.- Complementos para música.
  - 4.- Complementos para vídeo.
  - 5.- Complementos para contenidos.
  - 6.- Máquinas virtuales.

#### **UNIDAD DIDÁCTICA 11. LOS FALLOS DE APLICACIÓN**

1. Introducción en los fallos de aplicación
2. Los conceptos de código ensamblador y su seguridad y estabilidad
3. La mejora y el concepto de shellcodes
4. Buffer overflow
5. Fallos de seguridad en Windows

## **PARTE 5. DERECHO Y NUEVAS TECNOLOGÍAS**

#### **UNIDAD DIDÁCTICA 1. SERVICIOS DE LA SOCIEDAD DE LA INFORMACIÓN Y COMERCIO ELECTRÓNICO**

1. Ley de servicios de la sociedad de la información y de comercio electrónico
2. Servicios de la información
3. Servicios excluidos del ámbito de aplicación de la LSSI
4. Definiciones de la LSSI

#### **UNIDAD DIDÁCTICA 2. CONTRATACIÓN ELECTRÓNICA**

1. El contrato electrónico
2. La contratación electrónica
3. Tipos de contratos electrónicos
4. Perfeccionamiento del contrato electrónico

#### **UNIDAD DIDÁCTICA 3. PROTECCIÓN DE LOS CONSUMIDORES Y USUARIOS**

1. Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias
2. Protección de la salud y seguridad
3. Derecho a la información, formación y educación
4. Protección de los intereses económicos y legítimos de los consumidores y usuarios





#### **UNIDAD DIDÁCTICA 4. PUBLICIDAD**

1. Concepto de publicidad
2. Procesos de comunicación publicitaria
3. Técnicas de comunicación publicitaria

#### **UNIDAD DIDÁCTICA 5. LIBERTAD DE EXPRESIÓN E INFORMACIÓN**

1. Libertad de expresión
2. Libertad de información

#### **UNIDAD DIDÁCTICA 6. DERECHO AL HONOR, INTIMIDAD U PROPIA IMAGEN**

1. Derecho al honor, intimidad y propia imagen
2. Derecho a la intimidad
3. Derecho a la propia imagen
4. Derecho al honor
5. Acciones protectoras

## **PARTE 6. CIBERCRIMEN: DELITOS CONTRA LA PROTECCIÓN DE DATOS Y LA IDENTIDAD EN INTERNET**

#### **UNIDAD DIDÁCTICA 1. LOS DELITOS INFORMÁTICOS EN EL CÓDIGO PENAL**

1. Concepto y clasificación de los delitos informáticos
2. Características principales de los delitos informáticos

#### **UNIDAD DIDÁCTICA 2. COMPETENCIA PARA EL ENJUICIAMIENTO DE LOS DELITOS INFORMÁTICOS**

1. Principio de Universalidad
2. Efectos de cosa juzgada
3. Competencia judicial: teoría de la actividad, del resultado y de la ubicuidad
4. Temporalidad

#### **UNIDAD DIDÁCTICA 3. EL AUTOR TECNOLÓGICO**

1. Responsabilidad penal del autor
2. Proliferación de autores
3. La responsabilidad de intermediarios tecnológicos

#### **UNIDAD DIDÁCTICA 4. DELITOS CONTRA LA PROTECCIÓN DE DATOS Y LA IDENTIDAD EN INTERNET**

1. Delitos de estafa
2. Pornografía infantil, sexting y staking
3. Revelación de secretos
4. Delitos de amenaza y coacciones
5. Delito de falsificación documental
6. Delito de espionaje informático o hacking

#### **UNIDAD DIDÁCTICA 5. MEDIDAS CAUTELARES EN EL CIBERCRIMEN**

1. Retirada del contenido ilícito
2. El alejamiento informático
3. La Comiso cautelar

